Escuela Politécnica Superior

Implementación y creación de escenarios de pruebas con el NAC PacketFence

Máster Ciber Seg

Máster Universitario en Ciberseguridad

Trabajo Fin de Máster

Autor:

Ruslan Baltazar Nguema Ngua Nsee

Tutor/es:

Julio Antonio Jornet Monteverde

Mayo 2023

Universitat d'Alacant
Universidad de Alicante

Página dejada en blanco intencionadamente

Resumen

En la actualidad, está en constante aumento los ataques cibernéticos y las amenazas a las infraestructuras de red, esto hace que cada vez más la seguridad de las redes sea un tema fundamental e importante para las empresas.

Este trabajo fin de master se centra en encontrar una posible solución de seguridad para este tipo de casos. La solución de seguridad elegida es el NAC de packetfence, un sistema de control de acceso a la red que permite crear roles y políticas para la autenticación del usuario y detección de posibles amenazas en la red.

Este trabajo se ha ejecutado en la plataforma google cloud, y he utilizado EVE-NG como entorno de virtualización para integrar los dispositivos con los que he trabajado como los Router, Switch, máquinas virtuales.

En primer lugar, he implementado el NAC de packetfence en una máquina virtual Debían y he configurado los pasos necesarios previos para que funcione correctamente, luego he procedido a integrar este sistema de control en una red corporativa.

En segundo lugar, he integrado el controlador de dominio Active Directory en una LAN para crear los usuarios y grupos, y que packetfence filtre esos usuarios y los autentique según las reglas establecidas. Los protocolos de autenticación y autorización han sido RADIUS, IEEE 802.1X, MAB y EAP-PEAP. Por otro lado, está una segunda LAN que he configurado en una segunda interface de packetfence para realizar otro tipo de escenario de prueba.

Finalmente, he configurado los dispositivos para poder realizar los dos escenarios de pruebas, he documentado los resultados y los problemas encontrados durante la implementación.

Background

Currently, cyber-attacks and threats to network infrastructures are constantly increasing; this makes network security a fundamental and important issue for companies.

This master's paper focuses on finding a possible security solution for this type of case. The security solution chosen is NAC of packetfence, a network access control that allows you to create roles and policies for user authentication and detection of possible threats in the network.

I have executed this work on the google cloud platform, and I used EVE-NG as a virtualization environment to integrate the devices that I have worked with such as Router, Switch, virtual machines.

First, I have implemented the NAC in a Debían virtual machine and followed the configuration of necessary previous steps to make it work properly. Then I have integrated this control system into a corporate network.

Secondly, I have integrated Active Directory domain controller into a LAN to create the users and groups that packetfence will filter to authenticate according to the established rules, and the authentication and authorization protocols are RADIUS, IEEE 802.1X, MAB and EAP-PEAP. On the other hand, I have configured a packetfence second interface to perform another type of scenario.

Finally, I have configured the devices to be able to perform the two test scenarios, I have documented the results and the problems encountered during the implementation.

Resum

En l'actualitat, està en constant augment els atacs cibernètics i les amenaces a les infraestructures de xarxa, això fa que cada vegada més la seguretat de les xarxes sigui un tema fonamental i important per a les empreses.

Aquest treball fi de màster se centra a trobar una possible solució de seguretat per a aquest tipus de casos. La solució de seguretat escollida és el NAC de packetfence, un sistema de control d'accés a la xarxa que permet crear rols i polítiques per a l'autenticació de l'usuari i detecció de possibles amenaces a la xarxa.

Aquest treball s'ha executat a la plataforma google cloud, i he utilitzat EVE-NG com a entorn de virtualització per integrar els dispositius amb els he que he treballat com Router, Switch, màquines virtuals.

En primer lloc, he implementat el NAC de packetfence en una màquina virtual Debian i he configurat els passos necessaris previs perquè funcioni correctament, i després he procedit a integrar aquest sistema de control en una xarxa corporativa.

En segon lloc, he integrat el controlador de domini Active Directory en una LAN per crear els usuaris i grups, i que packetfence filtri aquests usuaris i els autentiqui segons les regles establertes, i els protocols d'autenticació i autorització han estat RADIUS, IEEE 802.1X, MAB i EAP-PEAP. D'altra banda, aquesta una segona LAN que he configurat en una segona interfície de packetfence per realitzar un altre tipus d'escenari de prova.

Finalment, he configurat els dispositius per poder realitzar els dos escenaris de proves, he documentat els resultats i els problemes trobats durant la implementació.

Motivación

La motivación principal que me ha conducido a realizar este trabajo viene de la idea que me planteó mi tutor de como poder crear soluciones de seguridad que sirvieran para fortalecer el acceso seguro de los dispositivos en una red corporativa. Soy consciente de que hay empresas que no gestionan de manera efectiva sus redes, y esto puede dar lugar a que existan vulnerabilidades o brechas de seguridad lo cual puede ocasionar la perdida de datos, información, fondos económicos e incluso dañar la reputación de empresa.

La solución planteada es el NAC de Packetfence y los objetivos que se quieren conseguir es de cómo aplicarlo en una red para asegurar el acceso y evitar brechas de seguridad. Este trabajo me permitirá aplicar conceptos aprendidos durante el master y mejorar mi experiencia y conocimientos en el mundo de la ciberseguridad.

Agradecimientos

La finalización de este trabajo fin de master marca uno de los mejores momentos de mi vida hasta entonces, y quiero agradecer a Dios por darme la fortaleza, sabiduría e inspiración para completar este proyecto.

Mi más sincero agradecimiento a mi tutor del TFM Julio Antonio Jornet Monteverde, por haber estado siempre pendiente de mis pasos. Su asistencia significativa, su sabia orientación y su experiencia han sido claves y me han sabido guiar para superar los desafíos que se me han presentado a lo largo del camino.

También quiero agradecer a la Universidad de Alicante, por darme la oportunidad de conseguir mis estudios de Master, al coordinador del Master José Vicente Berná, y al cuerpo docente por su compromiso con la excelencia académica y su gran aporte en mi formación académica y personal.

Un especial agradecimiento de todo corazón a mi padre Nemesio Ngua Mba, a mi madre Mariana Nsee Nguema, y a mi familia gracias por vuestro amor, paciencia y apoyo en mis estudios, por aconsejarme siempre y hacerme mejor persona.

A mis amigos y a mis compañeros del Master, gracias por formar parte de este camino, nuestros intercambios de ideas y debates han mejorado mi experiencia y han creado recuerdos inolvidables que siempre llevare conmigo.

Gracias a la bondad de estas personas mi trabajo puede ver la luz al final del túnel, y amablemente la presento con gran humildad.

Citas

El saber no ocupa lugar.

Unknown.

Dedicatoria

A mi padre y a mi madre

Índice de contenidos

Índice de figuras

Índice de tablas

Índice de abreviaturas

- **NAC:** Network Access Control (Control de Acceso a la red)
- **DAFO:** Destrezas, Amenazas, Fortalezas y Oportunidades
- **DDoS:** Distributed Denial of Service (Denegación de Servicio Distribuido)
- **Cisco ISE:** Cisco Identify Service Engine (Motor de Servicios de Identidad de Cisco)
- **TFM:** Trabajo Fin de Master
- **IEEE:** Institute of Electrical and Electronics Engineers (Instituto de Ingeniería Electrica y Electronica)
- **LAN:** Local Area Network (Red de Area Local)
- **WAN:** Wide Area Network (Red de area Amplia)
- **EAP:** Extensible Authentication Protocol (Protocolo de Autenticación Extensible)
- **PEAP:** Protected Extensible Authentication protocol (Protocolo de Autenticación Extensible protegido)
- **TCP:** Transmission Control Protocol (Protocolo de Control de Transmisión)
- **UDP:** User Datagram Protocol (Protocolo de Datagramas de Usuario)
- **ID:** Identification, Identifier (Identificación, Identificador)
- **EAPOL:** Extensible Authentication Protocol Over Local Área Network (Protocolo de Autenticación Extensible Sobre la Red de Área Local)
- **NAK:** Negative Acknowledgement (Reconocimiento Negativo)
- **BYOD:** Bring You Own Device (Trae Tu Propio Dispositivo)
- **EVE-NG:** Emulated Virtual Environment – Next Generation (Entorno Virtual Emulado – próxima Generación)
- **MAC:** Media Access Control (Control de Acceso al Medio)
- **LDAP:** Lightwight Directory Access Control (Protocolo Ligero de Acceso a Directorios)
- **VPN:** Virtual Private Network (Red Privada Virtual)
- **VM:** Virtual Machine (Máquina Virtual)

- **SFTP:** Secure File Transfer Protocol (Protocolo Seguro de Transferencia de Archivos)
- **SSH:** Secure Shell (Shell Seguro)
- **OVA:** Open Virtualization Appliance (Appliance de Virtualización Abierta)
- **CPU:** Central Processing Unit (Unidad Central de Procesamiento)
- **IP:** Internet Protocol (Protocolo de Internet)
- **NAT:** Network Address Translation (Traducción de Direcciones de Red)
- **AAA:** Authentication, Authorization and Acconting (Autenticación, Autorización y Contabilización)
- **MAB:** Media Access Control by pass (Control de Acceso al Medio por Pase)
- **RHEL:** Red Hat Enterprise Linux
- **ZEN:** Zero Effort NAC
- **DNS:** Domain Name System (Sistema de Nombres de Dominio)

1. Introducción

En la actualidad, el aumento de los ataques cibernéticos y las amenazas a las infraestructuras de red hace que cada vez más la seguridad de las redes sea un tema fundamental e importante para las empresas. Estas empresas trabajan con herramientas tecnológicas para poder ejecutar diariamente los trabajos que corresponden, la interconexión de sus activos en red, las aplicaciones que se manejan y los datos que se comparten pueden experimentar ciertas vulnerabilidades las cuales permiten a los ciberdelincuentes tomar ventaja y acción para acceder a la información que se maneja y los datos confidenciales de la empresa.

La poca seguridad que se puede experimentar en el entorno empresarial o en su defecto la no seguridad del sistema de redes puede generar que se pierdan datos valiosos, interrumpir en las tareas cotidianas, crear desconfianza para los usuarios y clientes. Otros aspectos a considerar son el cómo esto puede afectar a la reputación, los costes económicos que suponen y los daños generados adicionalmente. Por lo consiguiente, es fundamental para las empresas asegurar y proteger su entorno de red implementando buenas prácticas de seguridad e incorporar sistemas de control de acceso, y adoptar otras soluciones de seguridad según los requerimientos.

La solución de seguridad elegida para este proyecto es el NAC de PacketFence. Se puede implementar tecnología basada en roles para el aseguramiento de nuestro entorno de red empresarial, emplear estas técnicas de control de acceso basado en roles para preservar que tanto los usuarios como los dispositivos electrónicos que pretenden establecer conexión a nuestra red tengan los accesos necesarios y permisos adecuados para poder realizar sus correspondientes actividades. Desde esta perspectiva prevenimos que los usuarios no autorizados accedan a la red, reducimos de manera favorable el riesgo frente a las posibles amenazas cibernéticas.

En PacketFence, las políticas de control de acceso basado en roles pueden ser implementadas por el administrador de red de tal forma que este puede limitar el acceso a un cierto empleado dependiendo del área de trabajo en la empresa y el nivel de autorización, restringir el acceso al usuario invitado, o a los dispositivos. Como ejemplo, supongamos que un usuario invitado puede tener acceso a la red empresarial, pero este no podrá tener acceso a la red o a los recursos de empleados ya que la política implementada le limita el acceso.

Las tecnologías que se utiliza para la detección y prevención del acceso no autorizado a la red son varias en PacketFence, esto incluye monitorear el tráfico que pasa por la red, identificar los dispositivos que se conectan, autenticar debidamente a los usuarios y la implementación de las políticas de seguridad. De esta forma se fomenta que la red este correctamente protegida contra ataques tanto internas como externas y se ofrece a los usuarios un acceso seguro y controlado a la red empresarial.

2. Estudio de viabilidad

Antes de profundizar en el proyecto, es importante realizar un estudio de viabilidad. Para ello, es importante tener cierto rigor y plantearse de manera estratégica que es lo necesario que se deberá hacer para poder alcanzar los objetivos a los cuales se definen en este trabajo, se conseguirá o no tener éxito, se podrán encontrar posibles soluciones o no habrá soluciones. Los resultados de este estudio servirán para identificar las debilidades, fortalezas, amenazas y oportunidades; y en base a eso desarrollar un plan de acción para ejecutar el proyecto de manera eficiente. Esta es la idea que quiero enfatizar en este capítulo.

2.1. Análisis DAFO

El análisis DAFO es una herramienta que nos permite realizar un análisis completo sobre un producto para tener conocimiento de su situación presente, y en función de ello, tomar decisiones de cara al futuro. Un DAFO funciona como diagnóstico, después de realizar un estudio y radiografiar los puntos claves internos y externos del producto [2].

El análisis DAFO sobre PacketFence que he realizado es el siguiente:

Figura 1. Análisis DAFO [2] [3] (Fuente propia)

En la Figura 1, tenemos dos componentes uno interno y otro externo que afectan al NAC de manera positiva o negativa y que son imprescindibles para su correcta operatividad, y por lo consiguiente, para su posterior análisis. En cuanto a los componentes internos destacamos las debilidades y fortalezas que nos ayudan a ver de forma precisa para saber los puntos débiles y fuertes en el NAC. También nos permite determinar criterios concisos desde el conocimiento interno total. Para ello, voy a definir detalladamente cada uno de los aspectos que integran los componentes internos.

Debilidades

- **Costos:** Para implementar el NAC es de carácter necesario disponer de hardware y software específico, al igual que personal con habilidades en redes y seguridad para poderlo configurar y mantener adecuadamente.
- **Desafíos en la implementación:** Especialmente en los sistemas de red más grandes implementar PacketFence puede ser desafiante.
- **Dificultad de integración:** Anteriormente he mencionado que PacketFence es compatible con diferentes sistemas, aunque así sea, también pueden ocurrir problemas de integración con ciertos sistemas operativos y dispositivos.

Fortalezas

- **Gestión de permisos:** Este nos permite implantar políticas de seguridad para limitar el acceso a los recursos de la red según el usuario, el dispositivo, el tiempo.
- **Compatibilidad con diferentes sistemas:** Un punto importante de este apartado es que se puede integrar con tecnologías de seguridad ya existentes, así permitiendo su implementación con una variedad de dispositivos y sistemas operativos.
- **Escalabilidad:** Nos permite la adaptabilidad a las redes de cualquier tamaño.

En cuanto a los componentes externos, cuando es negativo destacamos que es una amenaza que resulta difícil gestionar el control, pero cuando el componente externo es positivo resulta ser una oportunidad la cual se puede aprovechar. Para ello, voy a definir detalladamente cada uno de los aspectos que integran los componentes externos.

Amenazas

- **Indisponibilidad de la red:** Ningún sistema es seguro al cien por cien. No se puede garantizar la protección y seguridad completa contra las amenazas de carácter externo como los existentes ataques DDoS, ataques de malware o desastres naturales que afecten directamente a los dispositivos físicos de red. Estos pueden crear lo no disponibilidad de red.
- **Otras plataformas:** Existen otras plataformas en el mercado para soluciones de seguridad como el Cisco ISE, el cual puede ser una fuerte competencia para PacketFence.

Oportunidades

- **Cumplimiento normativo:** Un aspecto muy importante en la seguridad de la información es el cumplimiento de las normas. PacketFence ayuda a las empresas a que puedan ajustarse a los requisitos normativos de la seguridad de la información.
- **Consolidación de la seguridad de la red:** Gracias a los sistemas de gestión de incidentes que se pueden implementar, esto favorece la fácil detección y respuesta frente a los posibles ataques cibernéticos.

3. Planificación

La planificación me sirve de guía y pasos marcados para conseguir los objetivos trazados del TFM. Además, me permitirá una vez terminado, analizar junto a los resultados la adecuación de la planificación al desarrollo completo del proyecto [4]. Eso me dará experiencia ya que al planificar se realiza una estimación de costes temporales en función de capacidades y habilidades supuestas [4]. Planificar el tiempo de ejecución de mi TFM me proporciona una perspectiva organizada que me ayude a no tener retrasos ni invertir mucho tiempo en aquello que se considera que no debería, y fraccionar el tiempo de tal forma que, este se ajuste a la carga del proyecto para poder finalizar y entregarlo en la fecha establecida por la universidad.

A continuación, en la figura 2 proporciono la planificación del proyecto:

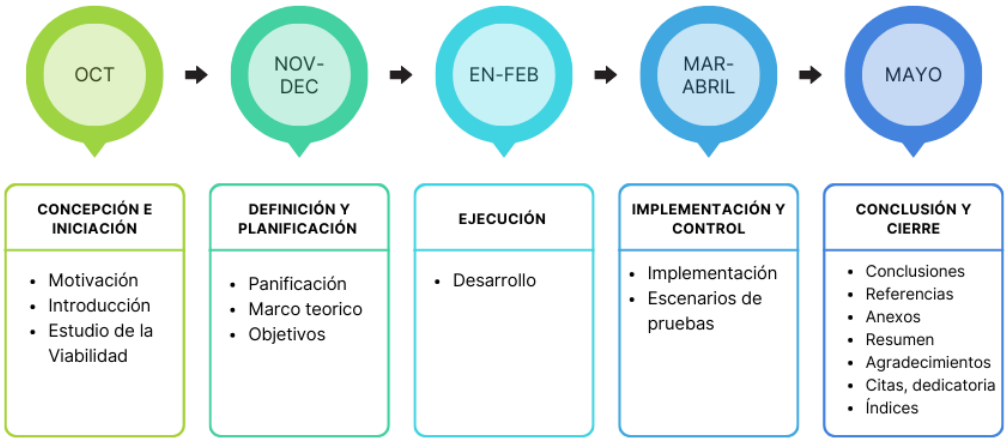

Figura 2. Planificación del TFM [3] (Fuente propia)

He realizado la planificación del proyecto con la herramienta canva. Los capítulos del TFM han sido agrupados en plazos por meses y grupos. En octubre, el grupo "Concepción e Iniciación" trata de la apertura, conceptos básicos y la motivación del proyecto. En noviembre y diciembre, se planifica el proyecto, se quiere definir conceptos que se consideran más importantes los cuales se basan en recoger toda la información de interés

para el desarrollo e implementación, así mismo como definir los objetivos concretos que se persiguen, y el marco teórico.

En enero y febrero, el grupo "Ejecución" se estima que es donde empezare a tocar el corazón del proyecto ya que se trata del proceso de recolección de todas las herramientas necesarias y útiles, la configuración del laboratorio de trabajo. Este punto es clave ya que al disponer de herramientas y el laboratorio correctamente configurado podré continuar con el capítulo de implementación. En marzo y abril. El grupo "Implementación y Control" está precisamente destinado a la implementación del proyecto, de las políticas y los controles de acceso basado en roles así mismo como mostrar los escenarios de pruebas.

En mayo, el grupo "Conclusión y cierre" hace referencia a la parte final del proyecto abarcando así aspectos como las conclusiones y trabajo futuro, las fuentes donde se va a extraer toda la información, los agradecimientos a las personas que han contribuido, estan contribuyendo directa o indirectamente a la consecución de mis objetivos, las citas. En resumen, esta planificación es para tener una versión legada la fecha 31 de mayo y así poder entregar adecuadamente para esta convocatoria [4]. Cada mes marca específicamente los capítulos que debo completar y coordinar en paralelo con mi tutor para que él pueda guiar y corregirme sobre la marcha.

3.1. Organización en trello

Trello es una herramienta flexible de gestión de trabajo donde se puede idear planes, colaborar proyectos, organizar flujos de trabajo y realizar un seguimiento del proceso de una manera visual, productiva y gratificante [5]. Para la ejecución de las tareas, he preparado en trello un tablero donde he ido creando una serie de tarjetas que explico a continuación sus correspondientes funciones:

- **Listado de tareas:** Son las respectivas tareas que estan por realizarse y las he ordenado según las fechas de ejecución.
- **En proceso:** Hacen referencia a las tareas que estan en curso, y la fecha en rojo es porque existen retrasos con lo inicialmente planeado.
- **Bloqueado:** Las tareas que permanecen en esta columna es porque existen dependencias con otras tareas, necesidad de asesoramiento del tutor, o necesitan más investigación para finalizarlas.

- **Finalizado:** En esta columna se sitúan las tareas que se han completado correctamente.

A continuación, en la figura 3 proporciono visualización del flujo de trabajo:

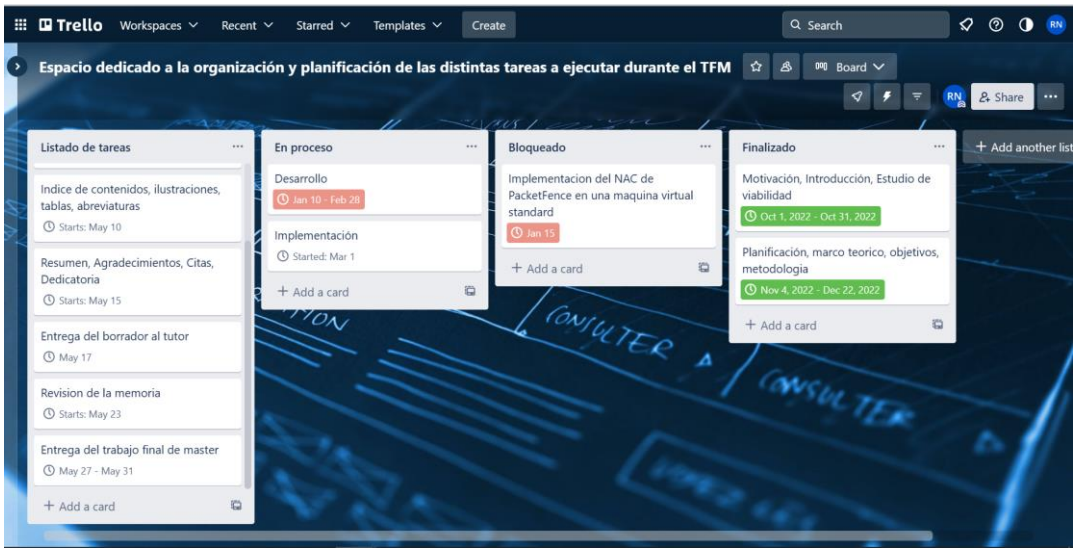

Figura 3. Tablero kanban en trello [5] (Fuente propia)

4. Marco Teórico

En este capítulo realizaré una revisión de la literatura, sobre teorías, conceptos, investigaciones y previos estudios que guardan relación con el tema de mi trabajo. Para ello, me voy a centrar en la identificación de los tópicos y conceptos fundamentales, proporcionaré referencias de donde se ha extraído la información, sintetizaré esa información relevante y elaboraré resúmenes de las teorías que se aplican directamente al trabajo. Mi objetivo en este capítulo es facilitar al lector información precisa y compresión detallada de aspectos y teorías esenciales.

4.1. Conceptos

4.1.1. Componentes AAA

Los servicios de seguridad de red AAA presentan una estructura principal para la implementación y control de acceso en un dispositivo que está conectado a la red. Implementar AAA nos permite administrar los permisos de acceso de un usuario a la red, Autorizar lo que se le permite hacer mientras dure su estancia en la red y por ultimo llevar a cabo un registro de las actividades que el usuario haya realizado mientras disponía de acceso a la red. Estos componentes se explican en detalles a continuación:

- **Autenticación:** En este procedimiento se comprueba la identidad del usuario, es decir, se debe demostrar que son quienes dicen ser.
- **Autorización:** Cuando ya se tiene autenticado al usuario, determinar los recursos a los que tiene acceso y las actividades que puede realizar.
- **Contabilización:** Registrar todo lo que hace el usuario, como por ejemplo a qué lugares tiene acceso, el tiempo que dura la conexión de acceso, cualquier modificación que pueda realizar.

4.1.2. MAB

La autenticación por MAB no es método seguro, pero es una técnica de control de acceso basado en puertos mediante el uso de la dirección MAC de un punto final [6]. MAB se usa típicamente como una alternativa a 802.1X para los puntos finales que no admiten IEEE 802.1X, como las impresoras y teléfonos, MAB proporciona visibilidad y control

de acceso basado en la identidad en el perímetro de la red. MAB no puede comprobar nada más que la MAC del punto final, por lo tanto, no ofrece autenticación segura porque las direcciones MAC son fáciles de falsificar [6]. Existen ataques como la suplantación de la MAC o IP, y una alternativa para evitar que no se pueda tener acceso a una cantidad considerable de la información es dedicarle una VLAN específica para mantener aislada la red.

4.1.3. EAP

Fue diseñado para utilizarse en la autenticación de acceso a la red [7]. Uno de los beneficios de este protocolo de autenticación es su flexibilidad ya que es compatible con diferentes métodos. Dado que EAP no requiere conectividad IP, solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación y nada más. Con base a como se quiere realizar la configuración de la red, se puede elegir un protocolo u otro de los siguientes: EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST, EAP-LEAP.

4.1.4. RADIUS

Es un protocolo que destaca por ofrecer un mecanismo de seguridad, flexibilidad, capacidad expansión y una administración simplificada de las credenciales de acceso a un recurso de la red. Es un protocolo de autenticación y autorización para el acceso a la red, este protocolo utiliza un esquema cliente servidor, es decir, un usuario con unas credenciales de acceso al recurso se conecta contra un servidor que será el que se encargue de verificarla autenticidad de la información, y será el encargado de determinar si el usuario accede o no al recurso compartido. Los servidores RADIUS también se puede usar para autenticar a los clientes que hagan uso del protocolo 802.1X para Ethernet [8].

4.1.5. Autenticación 802.1X

El contenido completo de este apartado y su sub-apartados ha sido extraído de Wikipedia y se ha proporcionado el enlace con numero [9] en el capítulo de referencias de este trabajo.

La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puerto. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto previniendo el acceso por ese puerto si la autenticación falla.

802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que estan equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos. La autenticación 802.1X implica a tres partes: un suplicante, un autenticador y un servidor de autenticación. El solicitante es un dispositivo cliente (como una computadora portátil) que desea conectarse a la red LAN/WAN. El termino suplicante también se usa indistintamente para referirse al software que se ejecuta en el cliente que proporciona credenciales al autenticador.

El autenticador es un dispositivo de red que proporciona un enlace de datos entre el cliente y la red y puede permitir o bloquear el tráfico de red entre los dos, como un conmutador ethernet o un punto de acceso inalámbrico; y el servidor de autenticación suele ser un servidor de confianza que puede recibir y responder a solicitudes de acceso a la red, y puede indicar al autenticador si se debe permitir la conexión, y varias configuraciones que deben aplicarse a la conexión o configuración de ese cliente. Los servidores de autenticación suelen ejecutar software con los protocolos RADIUS y EAP. En algunos casos, el software del servidor de autenticación puede estar ejecutándose en el hardware del autenticador.

El autenticador actúa como guardia de seguridad para una red protegida. El solicitante (es decir, el dispositivo cliente) no se le permite el acceso a través del autenticador al lado protegido de la red hasta que la identidad del suplicante haya sido validada y autorizada. Con la autenticación basada en puertos 802.1X, el solicitante debe proporcionar inicialmente las credenciales requeridas al autenticador, que habrán sido especificadas de antemano por el administrador de red y podrían ser nombre de usuario / contraseña o un certificado digital permitido. El autenticador reenvía estas credenciales al servidor de autenticación para decidir si se concede acceso. Si el servidor de autenticación determina que las credenciales son válidas, informa al autenticador, lo que a su vez permite al solicitante (dispositivo cliente) acceder a los recursos ubicados en lado protegido de la red.

4.1.5.1. Proceso de Autenticación 802.1X

El proceso de autenticación 802.1X típico consta de los siguientes pasos:

- **Inicialización:** Al detectar un nuevo suplicante, el puerto del conmutador (autenticador) se habilita y se establece en el estado “no autorizado”. En este

estado solo se permite el trafico 802.1X; otro tráfico, como el protocolo de internet (y con eso TCP y UDP), se elimina.

- **Iniciación:** Para iniciar la autenticación, el autenticador transmitirá periódicamente tramas de identidad EAP-Request a una dirección especial de capa 2 (01:80:C3:00:00:03) en el segmento de red local. El solicitante escucha en esta dirección y, al recibir el marco de identidad de solicitud EAP, responde con un marco de identidad EAP-Response que contiene un identificador para el solicitante, como un ID de usuario. A continuación, el autenticador encapsula esta respuesta de identidad en un paquete de solicitud de acceso RADIUS y la reenvía al servidor de autenticación. El solicitante también puede iniciar o reiniciar la autenticación enviando una trama EAPOL-Start al autenticador, que luego responderá con una trama EAP-Request Identity.
- **Negociación:** (Negociación técnica EAP) El servidor de autenticación envía una respuesta (encapsulada en un paquete de desafío de acceso RADIUS) al autenticador, que contiene una solicitud EAP que especifica el método EAP (el tipo de autenticación basada en EAP que desea que realice el solicitante). El autenticador encapsula la solicitud EAP en una trama EAPOL y la transmite al suplicante. En este punto, el solicitante puede comenzar a usar el método EAP solicitado, o hacer un NAK ("Reconocimiento negativo") y responder con los métodos EAP que está dispuesto a realizar.
- **Autenticación:** Si el servidor de autenticación y el solicitante acuerdan un método EAP, las solicitudes y respuestas EAP se envían entre el solicitante y el servidor de autenticación (traducido por el autenticador) hasta que el servidor de autenticación responde con un mensaje EAP-Success (encapsulado en un paquete RADIUS Access-Accept) o un mensaje EAP-Failure (encapsulado en un paquete RADIUS Acceso-rechazo). Si la autenticación es exitosa, el autenticador establece el puerto en el estado "autorizado" y se permite el trafico normal, si no tiene éxito, el puerto permanece en el estado "no autorizado".

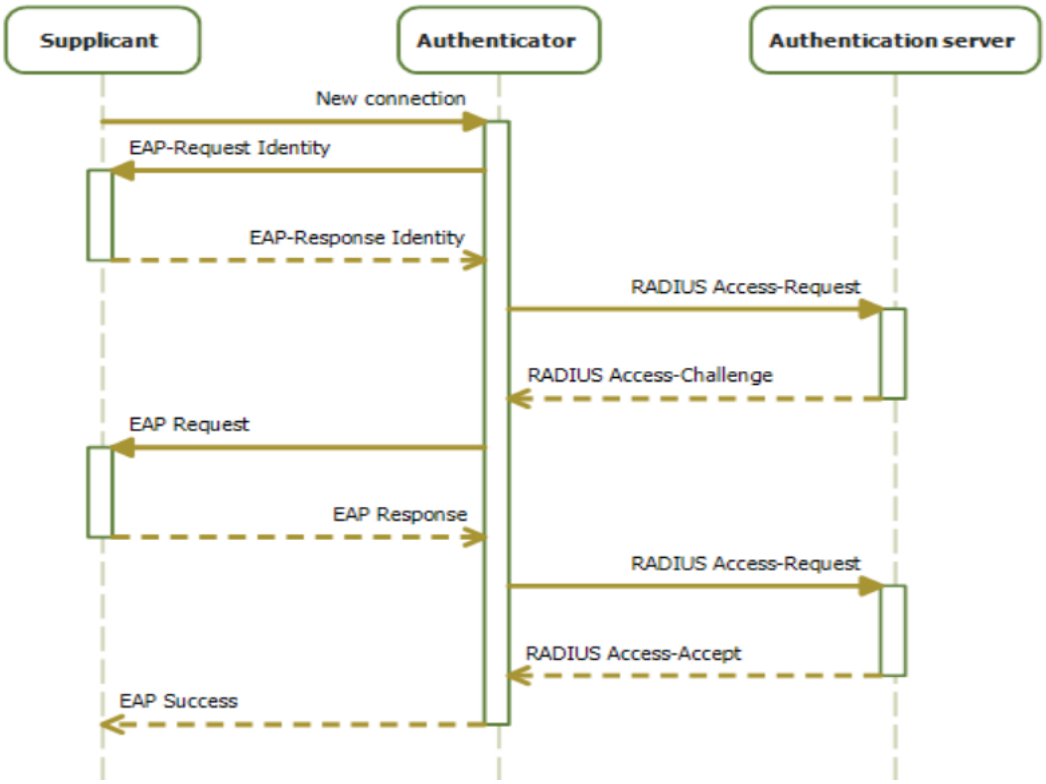

Figura 4. Proceso de autenticación 802.1X

(Fuente IEEE 802.1X https://en.wikipedia.org/wiki/IEEE_802.1X)

4.2. Sistema de Control de Acceso a la Red

El control de acceso a la red es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusos host, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de acceso [10]. Permite al administrador configurar políticas de acceso contextuales en el NAC para controlar el acceso a la nube y al centro de datos en función de dispositivos, localizaciones, recursos, usuarios y grupos o incluso el perfilado de endpoint [11]. NAC puede integrar proceso de remedio automático (corrigiendo nodos que no cumplen las normativas antes de permitirles acceso) en el sistema de red, permitiendo a la infraestructura de red como routers, switches y firewalls trabajar en conjunto con el back office y el equipamiento informático del usuario final para asegurar que el sistema de información está operando de manera segura antes de permitir el acceso a la red [10].

4.3. NAC de Packetfence

El contenido completo de este apartado y sub-apartado ha sido extraído de la página oficial de packetfence con referencia [1].

Packetfence es un sistema de control de acceso a la red totalmente compatible, confiable, gratuito y de código abierto. Impulsa un impresionante conjunto de características que incluye un portal cautivo para registro y corrección, administración centralizada cableada e inalámbrica, soporte 802.1X, aislamiento de capa 2 de dispositivos problemáticos, integración con IDS, escáneres de vulnerabilidades y firewalls; se puede utilizar para proteger eficazmente las redes, desde redes heterogéneas pequeñas hasta muy grandes.

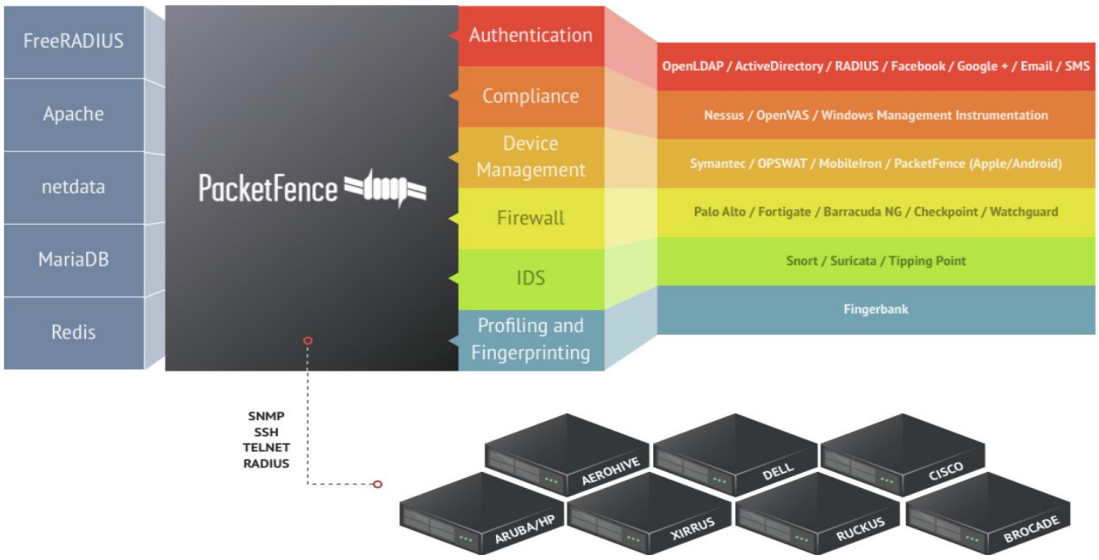

Figura 5. Arquitectura de componentes (Fuente https://www.packetfence.org)

En la figura 5, se ve que packetfence reutiliza muchos componentes en una infraestructura. No obstante, instalará los siguientes componentes y los gestionará él mismo:

- Servidor de base de datos (MariaDB)
- Servidor web (Apache)
- Servidor DHCP (Packetfence)
- Servidor RADIUS (FreeRADIUS)

- Firewall (IPTables)

Se asume que todos esos componentes se ejecutan en el mismo servidor en el que se instalará Packetfence.

4.3.1. Registro y autenticación

Para el registro y autenticación, el estándar 802.1X inalámbrico y cableado es compatible a través de un módulo FreeRADIUS que se incluye en packetfence. Se pueden utilizar PEAP-TLS, EAP-PEAP y muchos más mecanismos EAP.

4.3.2. Arquitectura de red

La figura 6 muestra la arquitectura de red de packetfence el cual es en gran medida escalable y que puede ser adaptada a una gama de entornos de red.

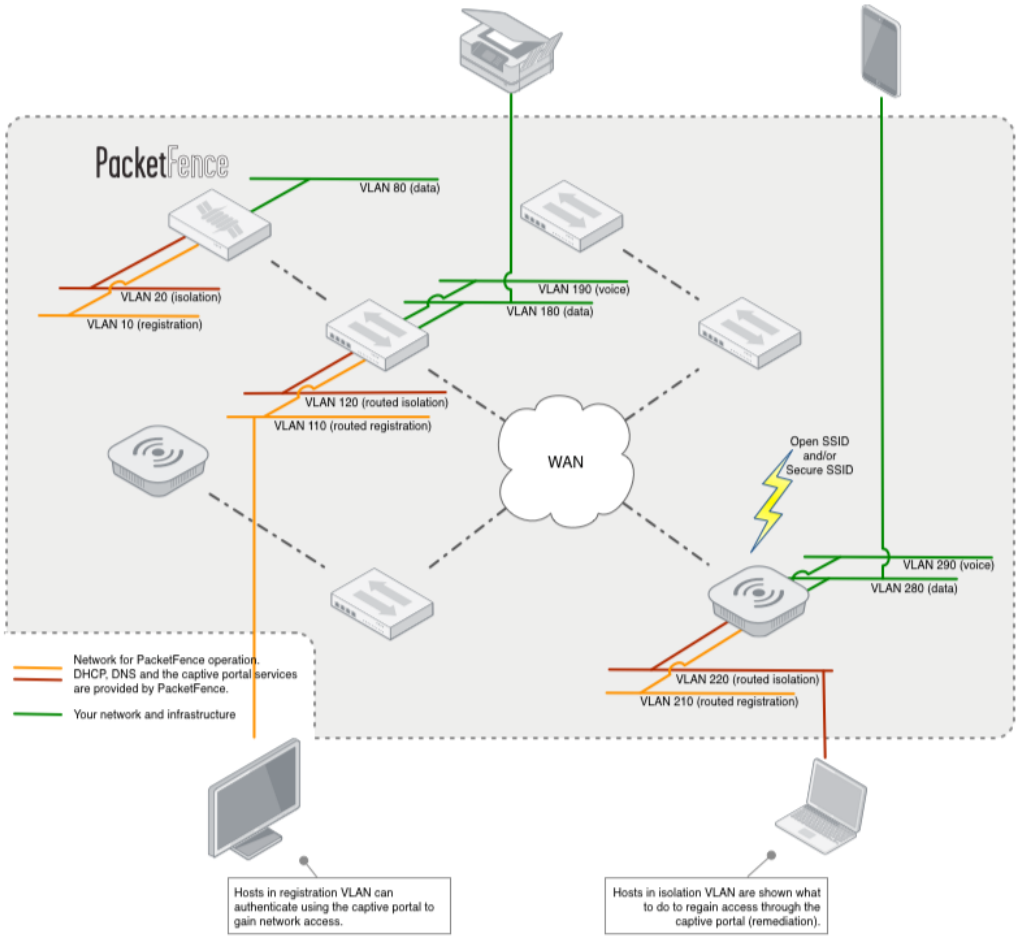

Figura 6. Arquitectura de red (Fuente https://www.packetfence.org)

4.3.3. Requisitos mínimos de hardware

A continuación, se proporcionan una lista de las recomendaciones mínimas de hardware del servidor:

- CPU Intel o AMD 3 GHz, 4 núcleos de CPU
- 16 GB de RAM
- 200 GB de espacio en disco (se recomienda RAID-1)
- 1 tarjeta de red (se recomiendan 2)

4.3.4. Requisitos del sistema operativo

Packetfence admite los siguientes sistemas operativos en la arquitectura x86_64:

- Servidor Red Hat Enterprise Linux 8.x
- Debian 11.x (diana)

Es importante asegurarse de que se puede instalar paquetes adicionales desde su distribución estándar. Por ejemplo, si se está utilizando Red Hat Enterprise Linux, debe estar suscrito a Red Hat Network antes de continuar con la instalación de Packetfence. Se sabe que otras distribuciones, como derivados de RHEL (o Debian), funcionan, pero no son compatibles con el equipo de Akamai/Inverse.

4.3.5. Métodos de instalación

Packetfence ofrece distintos métodos para su instalación, y pueden ser los siguientes:

- ZEN: Esta edición permite la instalación rápida del NAC, ya que es una versión que ya viene instalada y pre-configurada completamente.
- Desde la ISO: Permite la instalación del NAC en Debían 11 con mínimo esfuerzo, en lugar de instalar manualmente Debían 11 e instalar el NAC después.
- Desde Linux existente: Packetfence ofrece repositorio de paquetes para RHEL 8, al igual que ofrece repositorios para Debían. Con estos repositorios se tienen todas las dependencias que se necesitan para instalarlo.
- En Linode.

4.4. Análisis de los Sistemas de Autenticación

A modo de resumen, la tabla 1 muestra las características y ventajas cada uno de los métodos de autenticación. Haciendo uso en conjunto de cada una de estas características se puede establecer una solución de seguridad.

Tabla 1. Análisis de sistemas de autenticación

EAP	RADIUS	NAC	802.1X
autenticación	autenticación y autorización	Sistema de control de acceso	Estándar IEEE basado en control de acceso por puertos
LAN o WLAN	LAN o WLAN	LAN o WLAN	LAN o WLAN
Utiliza RADIUS como medio de comunicación	Utiliza EAP, NAC y 802.1X como medio de comunicación	Utiliza RADIUS, MAB y EAP como medio de comunicación	Hace uso de NAC, RADIUS y EAP
Múltiples formas para la autenticación	Múltiples formas para la autenticación	Distintos tipos de NAC	Se determina según la configuración
-	Asignación automática de roles	Asignación automática de roles	Asignación automática de roles
Se puede configurar con o sin certificados	Se puede configurar con o sin certificados	Se puede configurar con o sin certificados	Se puede configurar con o sin certificados

Cada uno de los sistemas de autenticación presenta una solución diferente, y que juntos se puede obtener una solución de seguridad más potente. El protocolo EAP solo autentica a los usuarios, pero no gestiona el control sobre la autorización al recurso. Si se quiere gestionar la autorización, se puede hacer uso del protocolo RADIUS o el sistema NAC. El punto importante es que pueden comunicarse entre ellos, y con eso se puede configurar distintas capas de control en la red. Para controlar los puertos de acceso está el estándar IEEE 802.1X, y con la ayuda de RADIUS y NAC para hacerlo más seguro. Un punto importante es que, en estos cuatro métodos, se puede conseguir la configuración de certificados para la autenticación de los usuarios.

5. Objetivos

Este proyecto se implementará mediante la herramienta de virtualización EVE-NG y máquinas virtuales. Los objetivos concretos que se persiguen conseguir se determinan a continuación:

- La implementación del NAC de packetfence en una máquina virtual estándar
- Integración del NAC de packetfence en una red estándar
- El planteamiento de una posible solución de seguridad con el NAC de PacketFence para una red corporativa que garantice un acceso seguro de los usuarios a la red.

Para cumplir con estos objetivos se va a integrar el active directory que es un controlador de dominio y método para asegurar el acceso de los usuarios a la red. En él se puede crear los usuarios por grupos y administrarlos de tal forma que Packetfence vaya a recopilar esa información para filtrar e implementar las políticas y los roles de acceso que le corresponde a cada usuario o grupo.

Otro método que voy probar es el fortalecimiento en línea para el registro de usuarios. Con este método el tráfico de la red es interceptada y se inspecciona para comprobar que cumple con las reglas y políticas de seguridad de la red.

6. Desarrollo

En este capítulo voy a detallar y hacer énfasis del proceso completo que se ha llevado a cabo para la puesta en marcha del laboratorio en EVE-NG, incluyendo las herramientas y tecnologías utilizadas, los requisitos previos, las imágenes ISO necesarias que se ejecutarán en el laboratorio, la experiencia obtenida, el motivo por el cual he migrado el proyecto de un entorno local a Google cloud y como logré establecer conexión en EVE-NG con Google Cloud hacia internet.

6.1. Herramientas y tecnologías para el desarrollo

Tabla 2. Inventario de herramientas y tecnologías

Nombre	Versión o Tipo	Formato
VMWare Workstation	17.0.0 pro	
EVE-NG	Community Edition	
Google cloud		
Putty	0.77.0.0	
WinScp	5.21.5	
Imagen-ISO Windows	7	hda.qcow2
Imagen-ISO Linux-Debian	11.6.0-amd64-netinst	virtioa.qcow2
Imagen-ISO Winserver	2019	virtioa.qcow2
Cisco Router	vios-IOS.156-2	virtioa.qcow2
Cisco Switch	viosl2-IOSL2m.03.2017	virtioa.qcow2
VPN Zerotier	1.10.5	
Ultra VNC Viewer	1.2.3.0	

A continuación, voy a detallar cada una de las herramientas y tecnologías, y su función en el proyecto.

- **VMware Workstation:** Es una plataforma para ejecutar múltiples sistemas operativos simultáneamente en la misma computadora [13]. Se ha utilizado inicialmente en este proyecto para alojar las máquinas virtuales.
- **Google cloud:** Es una plataforma en la nube utilizada para crear ciertos tipos de soluciones [14]. Ha sido utilizada en el proyecto como la mejor alternativa al no poder continuar utilizando VMware Workstation. Las razones se mencionan detalladamente en el apartado 6.3.
- **EVE-NG:** Es un entorno virtual emulado para profesionales de redes seguridad y DevOps. Tiene capacidad de aprendizaje para entrenarse con herramientas Cisco, Juniper y también una gran cantidad de proveedores como Checkpoint, PaloAlto, F5 y más. En él se puede construir los requisitos de red en consecuencia y planificar el diseño correcto para validar la solución, por su eficiencia y flexibilidad [15]. Es el laboratorio donde voy a desplegar el diagrama de red y las configuraciones de este trabajo.
- **Putty:** Es una implementación gratuita de SSH y Telnet para Windows y plataformas Unix, junto con un emulador de terminal [16].
- **WinScp:** Es una aplicación de software libre, cliente SFTP grafico para Windows que emplea SSH. Su función principal es facilitar la transferencia segura de archivos entre dos sistemas informáticos, el local y uno remoto que ofrezca servicios SSH [17]. Ha servido como aplicación para la transferencia de las imágenes ISO y los dispositivos de red desde mi pc a EVE-NG.
- **Imagen-ISO Windows:** Las imágenes ISO son un tipo de formato que se utilizan para hacer copias de sistemas operativos como Windows, ya que al descargarlo sería como si se descargase el disco original en el que se pudieran distribuir [18]. Con esta imagen podré tener las máquinas virtuales con el sistema operativo Windows en el emulador.
- **Imagen-ISO Linux-Debian:** Se ha utilizado como máquina virtual para la descarga, instalación e implementación del NAC de PacketFence.
- **Imagen-ISO Winserver:** Es una disposición que Microsoft ofrece para el uso de servidores. En este proyecto se utilizará para integrar el controlador de dominio, y para la creación de usuarios y establecer políticas de conexión a la red.

- **Cisco Router:** Dispositivo de red para guiar y gestionar los paquetes de datos de las transmisiones. Ha sido utilizado para conectar la red local hacia internet.
- **Cisco Switch:** Utilizado para poder crear red de área local, este dispositivo de red conectará diferentes dispositivos para la transmisión de paquetes entre sí mismos.
- **VPN Zerotier:** Es una solución de red de confianza cero ZeroTier que proporciona seguridad escalable de extremo a extremo de 256 bits [19]. Ha sido útil porque me ha facilitado la conexión remota de los dispositivos de red del entorno a mi dispositivo físico.
- **Ultra VNC Viewer:** Gracias a este software me ha resultado más fácil visualizar las máquinas virtuales en pantalla completa, eso cuando el estado se encuentra en modo "consola nativa".

Los formatos hda.qcow2 y virtoa.qcow2, son tipos de formatos en los que deben encontrarse las máquinas virtuales y los dispositivos de red antes de subirlos a EVE-NG.

A modo de resumen, estas son las herramientas y tecnologías necesarias que he utilizado para poder preparar y configurar el laboratorio de trabajo. El siguiente apartado detalla detenidamente las razones por las cuales se ha desplegado el proyecto en cloud.

6.2. Experiencia

Para la consecución de los objetivos de este proyecto, mi plan inicial era desplegar las herramientas y tecnologías en un entorno local. La elección de la herramienta para alojar las máquinas virtuales fue VMWare Workstation, ya que esta es una de las opciones más conocidas para la visualización de entornos que permite la creación de distintas máquinas virtuales y sistemas operativos en el equipo físico para poder aprovechar de su amplio espectro de funcionalidades y características, como la viabilidad de crear redes virtuales y clonar máquinas virtuales.

En el punto 1 del anexo he adjuntado detalles sobre la máquina virtual de EVE-NG, y PacketFence que ya se tenía alojadas correctamente.

Primero que todo, con la imagen de PacketFence ya se podía acceder al portal web de configuración del NAC, pero era necesario un dispositivo que lo enlace a EVE-NG como por ejemplo un switch para realizar las configuraciones. Este es el motivo por el cual se ha integrado el NAC directamente en el emulador.

Para ello, exporté la OVA de Packetfence y la convertí al formato compatible para así integrarla directamente a EVE-NG, pero comenzaron a surgir problemas durante el proceso, los cuales me han retrasado el tiempo planificado para la finalización de este capítulo. Uno de los problemas consistía en que, al exportar, convertir y subir la OVA a EVE-NG se corrompían los archivos porque no se terminaban de subir correctamente por cuestiones de memoria y CPU.

Utilicé otra técnica que era crear una máquina virtual en EVE-NG y desde ahí descargar e instalar PacketFence directamente, pero tampoco era posible por los mismos problemas. VMWare Workstation es una herramienta bastante útil para alojar máquinas virtuales, pero tuve limitaciones en términos de capacidad de procesamiento y memoria, y tenía que buscar otros recursos ya que no disponía de un equipo físico potente que me permita el funcionamiento correcto de PacketFence. La solución que me pareció viable era migrar el proyecto a una plataforma en la nube. Para elegir la plataforma, tenía que optar por una que me facilitara los requisitos específicos de memoria y CPU que necesitaba, y en paralelo teniendo en cuenta del coste económico que pudiera suponer trabajar en cloud.

6.3. Migración del proyecto a Google cloud

He elegido migrar el proyecto a google cloud por ofrecerme recursos que necesitaba, además me permite hacer uso de la plataforma con un coste económico gratuito durante un periodo de tiempo y en base a la utilización de la instancia. En el punto 2 del anexo proporciono un informe de los créditos de prueba gratuita. En google cloud hay un servicio informático personalizable “Compute Engine” en donde voy a poder crear y ejecutar una instancia en función de mis necesidades.

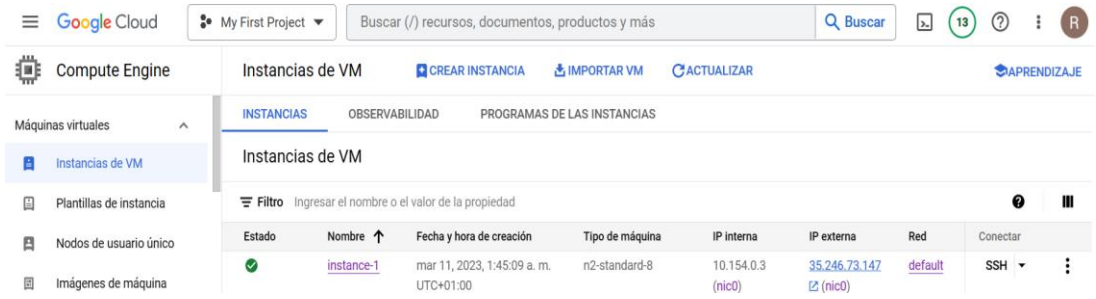

Figura 7. Vista de la instancia creada en google cloud

Una vez finalizado la creación de la instancia, lo siguiente viene a ser la instalación de EVE-NG, donde se subirán las imágenes y dispositivos de red para trabajar. Para ello, me conectaré por SSH con permisos privilegiados e introduciré el siguiente comando para su descarga:

```
“wget -O - https://www.eve-ng.net/focal/install-eve.sh | bash -i”
```

Ahora que se ha completado la descarga y se ha instalado correctamente EVE-NG, pasamos a las configuraciones del firewall para crear las reglas de entrada y salida. Estas reglas servirán para tener el control del tráfico que entra y sale de la instancia. En el punto 3 del anexo va adjuntado más detalles. Normalmente se deben bloquear todo el tráfico que viene del exterior de mi red, pero como esto es una prueba voy a crear la regla *“permitall”* para permitir el tráfico y que no me cree complicaciones más a delante cuando esté con las configuraciones e implementaciones.

6.4. Configuración inicial del entorno

En la figura 7 disponemos de la IP externa con la que se accede a EVE-NG, esta IP solía cambiarse automáticamente. *“admin y eve”* son las credenciales por defecto para acceder. En el punto 4 del anexo se muestra más detalles. Ya que se puede acceder perfectamente al emulador, lo siguiente es empezar a agregar los nodos; en otras palabras, agregar las máquinas virtuales y dispositivos de red con los que voy a trabajar. El método utilizado ha sido mediante la herramienta Winscp, lo que implica conectarse remotamente con la IP publica de EVE-NG, seleccionar SFTP como tipo de protocolo, el puerto número 22, y proporcionar las credenciales para establecer la conexión.

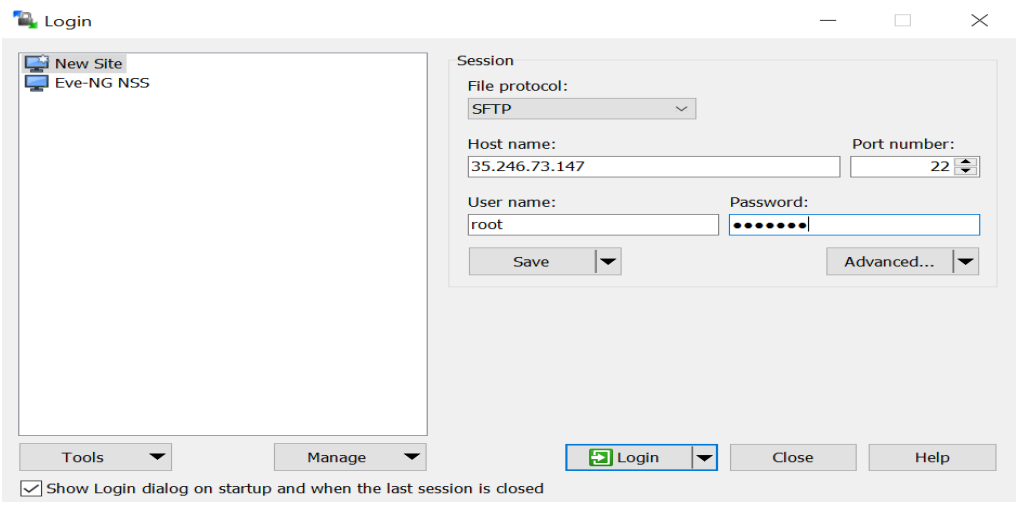

Figura 8. Conexión entre eve-ng y winscp

Una vez haber establecido la conexión remota entre EVE-NG y Winscp en mi equipo físico, se procede a transferir los archivos. Es importante subir los archivos como recomienda la página oficial de EVE-NG. Por ejemplo, a la hora de subir un archivo, crear una carpeta con el nombre seguido de la versión y guardar el archivo dentro de esa carpeta; estas carpetas se hospedan en la ruta "`/opt/unetlab/addons/qemu/`". También se pueden comprobar en la página oficial de EVE-NG los pasos específicos para subir la imagines o crear las tuyas propias y subirlas. En el capítulo de referencias numero [21] y [22] se ha proporcionado enlace con información sobre ello. En el punto 4 del anexo se muestran más detalles sobre la trasferencia de archivos.

6.5. Conexión a internet

En el punto anterior me he centrado en acceder al entorno virtual y subir tanto las máquinas virtuales como los dispositivos de red con los que voy a trabajar. En este punto voy a hacer mayor énfasis de como conectar a EVE-NG y los dispositivos hacia internet. En primer lugar, algo muy importante que se debe hacer es realizar una configuración en el sistema operativo Linux por el cual se está ejecutando EVE-NG. Es de carácter esencial tener en cuenta que, estos cambios se deben realizar correctamente para que no cause problemas más adelante, ya que en caso contrario podría generar errores y esto haría que se tenga que desplegar la máquina virtual nuevamente para que funcione bien. Para que las máquinas virtuales tengan acceso a internet se necesita habilitar EVE-NG como un router. A continuación, me conectaré por SSH y realizaré las siguientes configuraciones:

1. En la pnet9 asignaré una IP estática y mascara de red, y reiniciaré la red para que la IP se actualice correctamente en la interface. Esto se realiza en el archivo: `/etc/network/interfaces`

Para que surta efecto esta configuración y que los cambios se realicen correctamente se ejecuta el comando: `systemctl restart networking`

2. Habilitación de IPv4 forwading: esto permite que EVE-NG reenvié el trafico IP a los destinos que no conoce. Esto se realiza en el archivo: `/etc/sysctl.conf`

Este archivo avisa al kernel si habilitar o no ciertas características. Basta con dejar sin comentar la línea para que el trafico pueda ser enviado. Esto permitirá que cuando se reciba un paquete que no es enviado por él, mire por el destino en su tabla de enrutamiento

y lo reenvie. Para que surta efecto esta configuración se ejecuta el comando: `sysctl -p /etc/sysctl.conf`

3. Crear la regla (outbound nat iptables) para el tráfico saliente de EVE-NG, eso es necesario para la subred que voy a definir posteriormente.

Lo que he hecho ha sido modificar la tabla NAT, para que los paquetes salientes de la red de eve-ng se enruten a través la interfaz. *'iptables' '198.18.18.0/24' 'pnet0'.*

Para más detalles de la regla establecida, tenemos lo siguiente:

- **Iptables:** modifica las reglas de firewall netfilter.
- **-t nat:** determina la tabla NAT, que es la que se va a modificar.
- **-A POSTROUTING:** determina la secuencia de la tabla NAT. donde deberán ser añadidas las reglas. procesa los paquetes cuando van saliendo del sistema.
- **-o pnet0:** determina la interfaz que deben enviarse los paquetes.
- **-s 198.18.18.0/24:** determina el origen de la red.
- **-j MASQUERADE:** determina la conducta de destino a realizar en los paquetes que guardan coincidencia con la regla establecida.

Como ya se tiene configurado la dirección IP que es el origen de la red, el Ipv4 forwading y la NAT que permitirán la comunicación entre la LAN en EVE-NG hacia internet, voy a realizar una siguiente configuración en el Router para habilitar la conexión de los dispositivos en la LAN a internet. En la figura 9 se muestra la dirección estática, la ruta por defecto, y la IP asignada al nodo que conecta al router con internet.

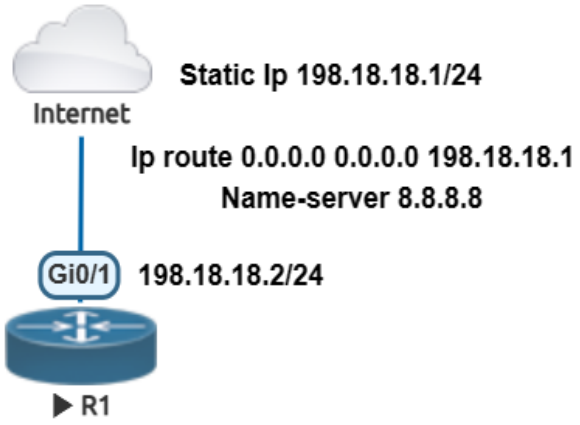

Figura 9. Conexión del router hacia internet

Los detalles de la configuración que se han realizado en el router se muestran en el punto 12 del anexo al final de esta documentación.

Una vez hecha la configuración, la verificamos haciendo un ping al 8.8.8.8 para confirmar que ya se dispone de internet en el dispositivo router. Ahora puedo proceder a crear la LAN para la implementación, pero antes de continuar voy a establecer una conexión de red privada triangulada con Zerotier para poder acceder a los dispositivos con aplicaciones locales en mi pc en lugar de *CLI* vía navegador. Los detalles se muestran en punto 9 del anexo.

7. Implementación y creación de políticas y roles de control de acceso

7.1. Implementación de packetfence en una máquina virtual

Para este trabajo he elegido implementar Packetfence en la distribución Debían. En primer lugar, agregaré a la topología el nodo de la máquina virtual de Debían la cual será conectada al router, y crearé una LAN para asignarle una dirección IP a la máquina virtual para que tenga acceso a internet y poder realizar la implementación. Una vez tenido la máquina virtual debían lista, se recomienda deshabilitar AppArmor y desactivar resolvconf, ya que tenerlo activado puede crear dificultades a la hora de la instalación.

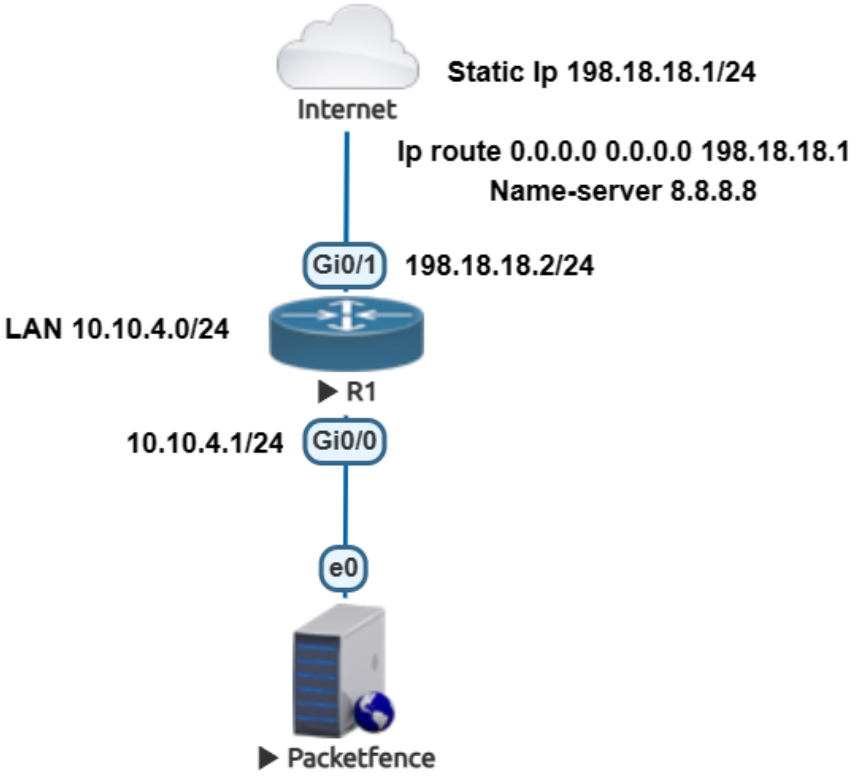

Figura 10. Implementación de packetfence en Debían.

Es importante tener en cuenta y asegurarse de que se esté ejecutando la versión más reciente de kernel. Desde el terminal de debían el siguiente comando para instalar el paquete de desarrollo del kernel: `Apt install Linux-headers-$(uyname -r)`

Para instalar el software y utilizar el repositorio que proporciona Packetfence, desde el terminal de debían generaré un archivo denominado:

```
/etc/apt/sources.list.d/packetfence.list
```

Para definir el siguiente repositorio dentro de él:

```
'deb http://inverse.ca/downloads/PacketFence/debian/12.2
bullseye bullseye'
```

Cuando ya se tiene definido el repositorio, lo siguiente es instalar el NAC con todas sus dependencias incluidas así mismo como los servicios externos necesarios (Base de datos servidor DHCP, servidor RADIUS) con los siguientes comandos: `Apt install gnupg sudo Wget –q -0 – https:// inverse.ca/downloads/GPG_PUBLIC_KEY | sudo apt-key add – Apt-get update Apt-get install packetfence`

Ahora que se ha completado la implementación del NAC en la debían, se debe realizar una primera configuración para acceder al portal de administración web. Esto se hace a través de la dirección *https://@ip_of_packetfence:1443/*, en este caso *https://10.10.4.8:1443* que es la dirección IP asignada. Estas configuraciones se dividen en los siguientes pasos:

1. **Configuración de la red:** Para definir la interfaz de red que será la que se comunicará con el switch de acceso, esta interfaz será de tipo ‘management”.
2. **Configuración de packetfence:** En este paso, se define toda la información que se requiere para generar la base de datos. Igualmente, el host, el nombre de dominio y las credenciales de gestión del administrador.
3. **FingerBank:** Este paso es opcional, sirve para la identificación precisa de dispositivos médicos, IoT, robóticos y más en la red. No se ha realizado ninguna configuración para este trabajo.
4. **Confirmación:** Después de realizar las configuraciones, se inicia packetfence, y ya se puede acceder al portal con la IP de gestión e introducir las credenciales definidas en el paso 2 para acceder como administrador.

7.2. Diseño del diagrama de la red

Después de haber implementado correctamente Packetfence en Debían y de conseguir el acceso al portal como administrador, el siguiente paso se centra en la integración del NAC a la red para posteriormente crear las políticas y roles de control de acceso de los usuarios. En la figura 11 se muestra el diagrama de la red y de cómo están interconectados todos los dispositivos.

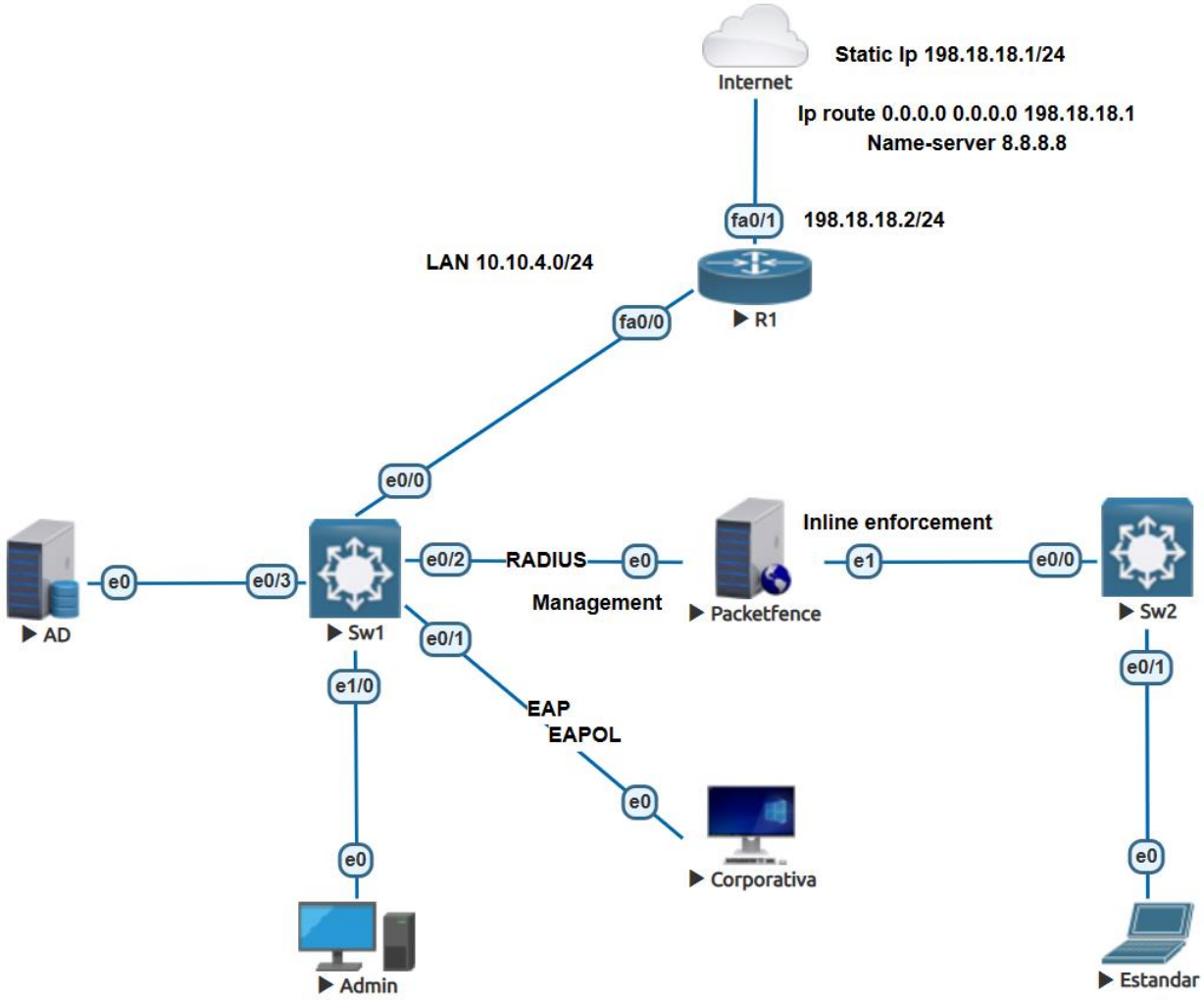

Figura 11. Diagrama de la red

Como se puede observar en la figura 11, se ha diseñado una red donde el principal actor es el NAC y lo que se quiere conseguir es configurar a los usuarios para realizar pruebas de control de acceso a la red. En este diagrama, se ha configurado dos redes. Una primera que es la red de gestión en la LAN 10.10.4.0/24 donde he configurado un solo puerto o interface e0/1 para realizar las pruebas.

En esta interface se ha configurado los protocolos EAP-PEAP y MAB para que cuando un dispositivo se conecte a esta interface, el packetfence lo que hará como primer paso es solicitar que este se autentique vía EAP-PEAP, y si no se pudiera autenticarse por qué no lo soporte, automáticamente pasara a MAB en caso de que sean dispositivos como teléfonos, impresoras. También se ha configurado el 802.1X para controlar el acceso al puerto.

Entre el switch 1 y packetfence el protocolo de autenticación que se va a utilizar es RADIUS el cual actuará de puente entre los dos nodos y permitirá conducir la petición del usuario que quiera autenticarse. Entre El switch 1 y el usuario también está una trama EAP-EAPOL que es el responsable de transportar la petición del usuario al switch 1. Otras configuraciones claves se proporcionan en el anexo. Configurando la red de esta manera garantizamos que los usuarios puedan tener que autenticarse, y tener autorización de manera segura.

Por otro lado, está el switch 2 que se ha integrado como una red normal en donde el usuario estándar solo necesita conectarse a internet y nada más. He configurado la red de esta forma como métodos de pruebas para ir descubriendo la cantidad de servicios que se pueden realizar en packetfence. En resumen, este diagrama de red determina como estan organizados y conectados los distintos dispositivos para que se tenga una comunicación optima de datos entre sí.

7.2.1. Direccionamiento IP

La tabla 3 resume las asignaciones de direcciones IP, la máscara de red, las rutas por defecto y las interfaces que se han configurado en cada dispositivo. Se puede observar a través de la dirección IP tanto del switch 2 como del usuario estándar que estos se encuentran completamente en una red distinta.

Tabla 3. Tabla de enrutamiento

Dispositivo	interfaces					IP Address	SubnetMask	Gateway
Router	0/1					198.18.18.2	255.255.255.0	198.18.18.1
	0/0					10.10.4.1		
Switch 1	0/0	0/1	0/2	0/3	1/0	10.10.4.2		10.10.4.1
Switch 2	0/0					11.11.5.2	255.255.255.0	11.11.5.1
	0/1							
Packetfence	E0					10.10.4.8	255.255.255.0	10.10.4.1
	E1					11.11.5.8		
Admin	E0					10.10.4.3	255.255.255.0	10.10.4.1
Active Directory	E0					10.10.4.19	255.255.255.0	10.10.4.1
Usuario Corporativo	E0							10.10.4.1
Usuario estándar	E/0					DHCP	255.255.255.0	11.11.5.1

7.3. Configuraciones

Packetfence es el principal actor de este trabajo y como se ha mencionado anteriormente es el responsable del control de acceso a la red. Para que se tenga un mejor entendimiento de como se ha ejecutado los ajustes, voy a detallar los pasos con mayor importancia en la configuración realizada en packetfence y en los dispositivos de este sistema. En el apartado 7.1 se ha realizado una primera configuración para tener acceso como administrador al portal web. En este apartado se va a realizar las siguientes configuraciones:

- Configurar los switches e integrarlos a packetfence
- Configurar packetfence para actué como servidor RADIUS
- Configurar active directory y conectarlo a packetfence
- Configurar 802.1X, MAB y los perfiles de conexión.

7.3.1. Switch 1 de gestión

En el switch de gestión lo primero que voy hacer es configurarlo para que se integre con packetfence. Para ello, en el fichero "dot1x system-auth-control" habrá que habilitar 802.1X globalmente en el switch para la autenticación basada en puertos. Algunos de los pasos que se van a seguir para la correcta configuración del switch serán los siguientes:

- Generar un método que permita que la autenticación local pueda ser aplicada a todas las líneas e interfaces.
- Establecer un nuevo grupo de servidor que será packetfence como nombre y se utilizará su IP para configurarlo.
- Ya que se tiene establecido el grupo, establecer la autenticación y autorización para que los usuarios puedan ser autenticados y autorizados y ganar acceso al grupo.
- Establecer los protocolos para la autenticación y autorización que se van a utilizar
- Configuracion de la VLAN.
- Configuracion del puerto de conexión para el escenario de la prueba.
- Definir el orden por el cual se realizará la autenticación. El primer protocolo de autenticación será el estándar 802.1X, cuando no se pueda el siguiente será MAB.

También se puede agregar a la configuración el tiempo en que un usuario debería autenticarse de nuevo. Evaluar la situación cuando al mismo puerto se estan conectando más de un dispositivo, se puede configurar de tal manera que cuando existe un dispositivo que desea establecer conexión a un puerto donde previamente ya existía un dispositivo, el dispositivo viejo sea sustituido por el nuevo y de este modo ningún dispositivo tendrá un puerto específico para poder acceder.

Si se tratase de un caso real esta configuración debe realizarse en todos los puertos, pero en este trabajo se va a realizar la configuración en un solo puerto. En este caso la configuración de MAB y la habilitación de 802.1X se van a realizar en la interface 0/1 del switch 1. Estos son los dos parámetros primordiales que deben ser configurados.

En el anexo irán adjuntadas las configuraciones completas de los switches.

7.3.2. Packetfence

El primer paso a realizar es unir el servidor packetfence al dominio active directory. Esto se hace en *Configuración → Políticas y Control de Acceso → Dominios → Dominio de Active Directory*. Entre los campos a rellenar nos solicitara las credenciales del administrador de Active Directory.

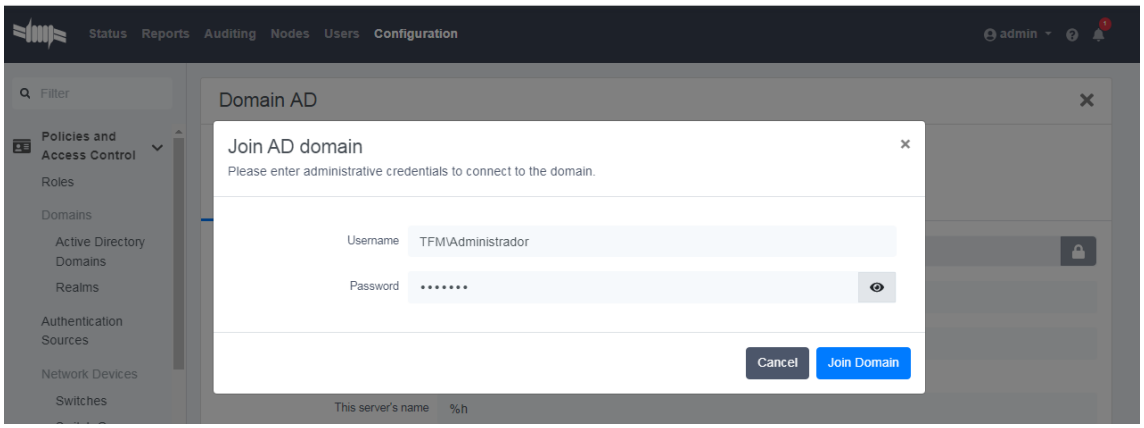

Figura 12. Solicitud de las credenciales del dominio

Es importante destacar que existen campos de carácter obligatorio a rellenar. A continuación, se muestra una vista más amplia de la información necesaria que se ha proporcionado para crear el dominio.

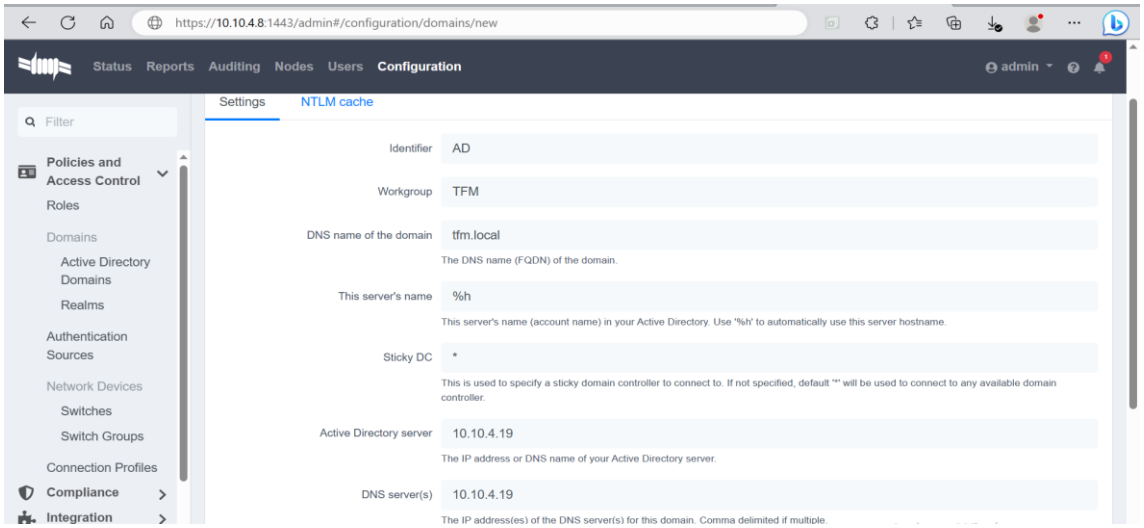

Figura 13. Configuracion del dominio packetfence

Una vez se haya unido correctamente el dominio y se tenga conexión con él, el siguiente paso es hacer que packetfence lo utilice por defecto para la autenticación. Para ello, generare un nuevo origen de autenticación. Este ajuste se realiza en *Configuracion →*

Políticas → Orígenes de autenticación. Gran parte de los campos a rellenar son de la configuración realizada de LDAP del AD.

En la figura 14 se tiene mayor visión de los campos a rellenar, una vez que se haya rellenado los campos es importante verificar con el botón test para confirmar que la información que se está proporcionando es válida. Cuando le damos al botón test y sale el mensaje "Success LDAP connect, bind and search successfull" esto significa que se ha tenido éxito en la conexión de enlace y búsqueda LDAP y que se ha configurado adecuadamente el nuevo origen de autenticación.

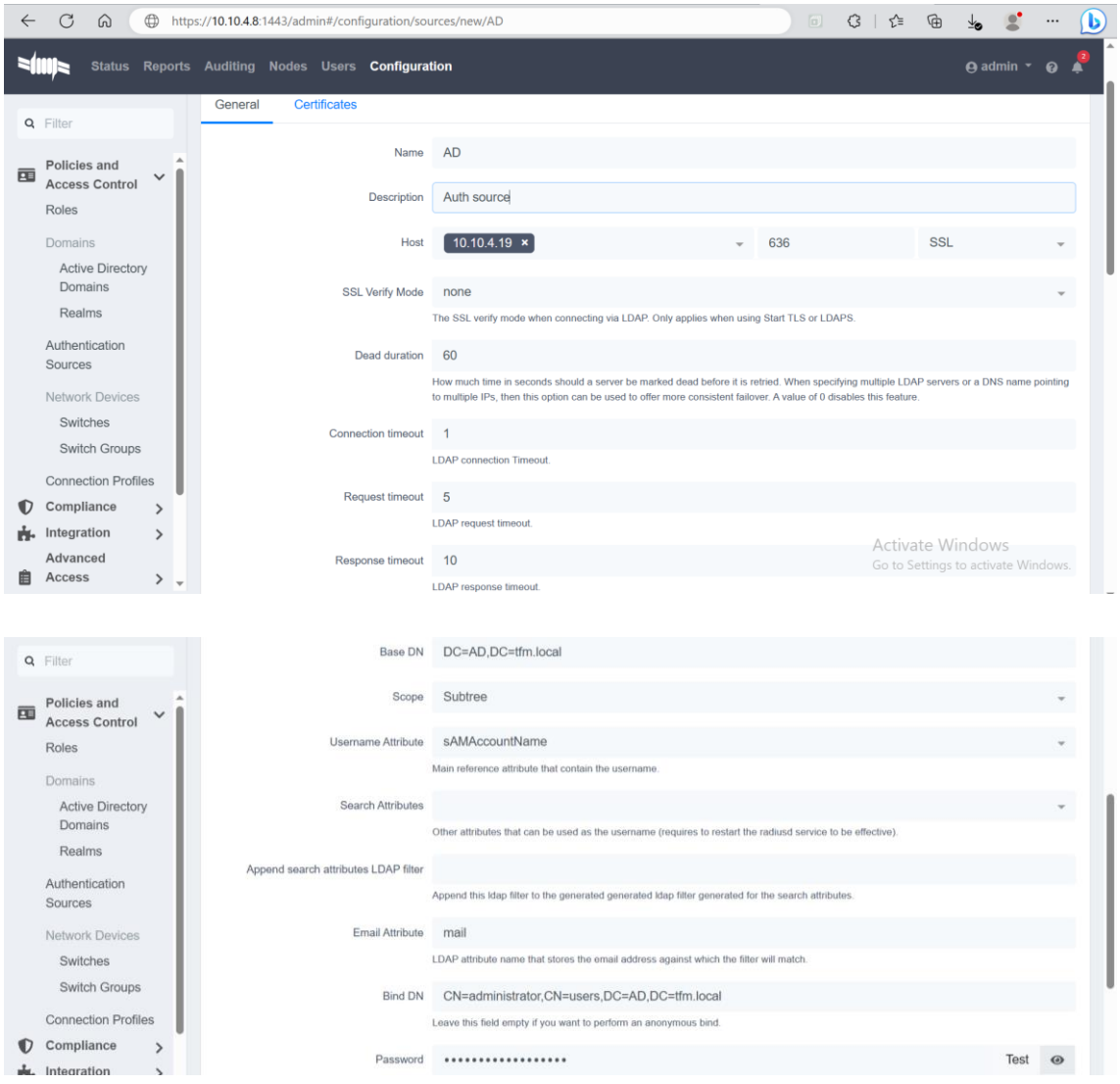

Figura 14. Configuracion de la fuente AD

7.3.2.1. Integración del switch 1

Para integrar el switch a packetfence nos dirigiremos a Configuración → *Políticas y Control de Acceso* → *Dispositivos de red* → *Switches* e introduciremos la dirección IP del switch, el tipo de dispositivo, y el modo. En la pestaña de los roles es importante marcar el 'Rol por ID de VLAN' y configurar la VLAN que serán asignadas a los usuarios para que estos puedan autenticarse contra el servidor.

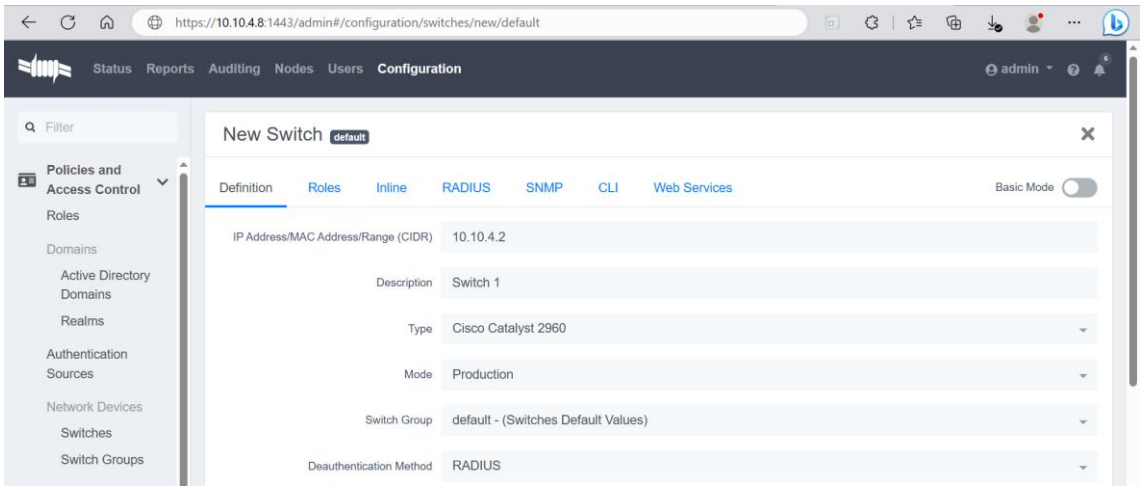

Figura 15. Datos para la integración del Switch 1

En la pestaña RADIUS se establecerá la "Frase de contraseña secreta" que se va a utilizar. Por otro lado, está la pestaña "SNMP" y en ella se proporcionan los valores de Community Read y Community Write. Una vez se haya finalizado con esta configuración, se ha integrado el switch correctamente.

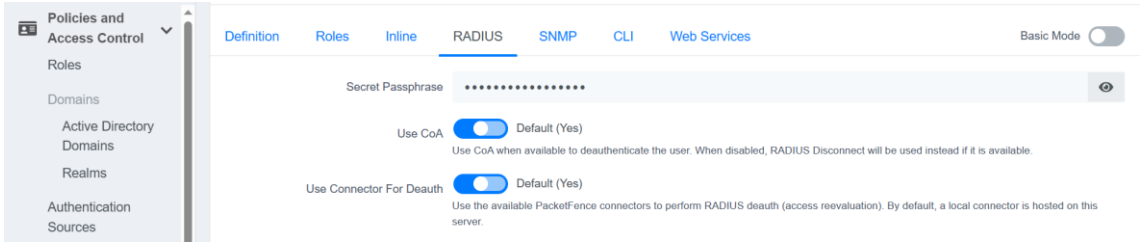

Figura 16. Switch 1, pestana RADIUS

Una vez se tiene integrado el switch, el siguiente paso es realizar la configuración de los perfiles de conexión para que packetfence pueda saber gestionar si la conexión entrante es via por 802.1X o si es por MAB. La primera regla que voy a configurar es la autenticación 802.1X para poder utilizar nuestra fuente de autenticación AD y además para que packetfence también sepa registrar de forma automática cualquier dispositivo que se autentique exitosamente utilizando este método de conexión. Esto se realiza en *Configuración → Políticas y Control de Acceso → perfiles de conexión.* En la figura 17 se muestra un resumen de la información que se ha proporcionado para crear el filtro 802.1X.

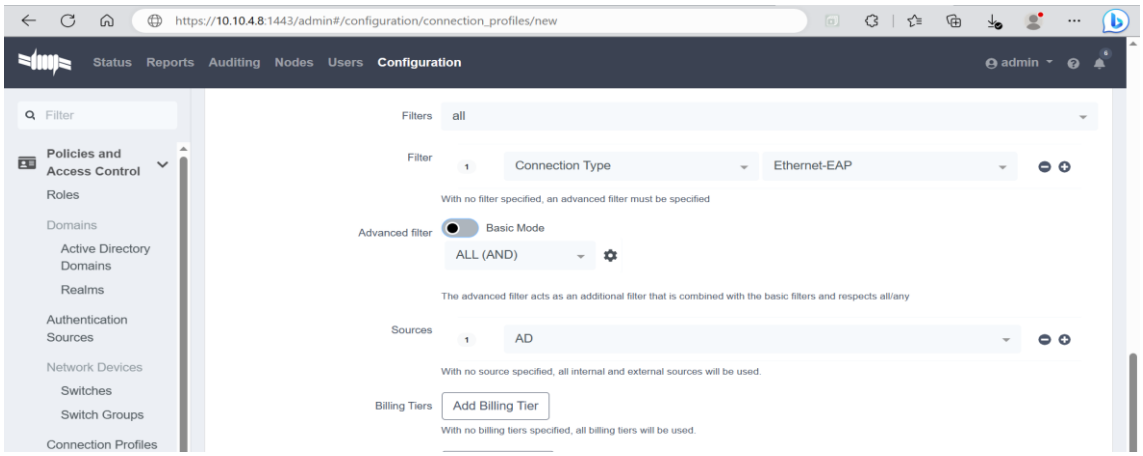

Figura 17. Configuracion del filtro 802.1X

La segunda regla que voy a configurar es para la autenticación vía MAC. Los pasos son prácticamente los mismos que lo realizado anteriormente, pero a diferencia de que esta vez el tipo de conexión será Ethernet-NoEAP, de esta manera este filtro evitará usar la versión EAP.

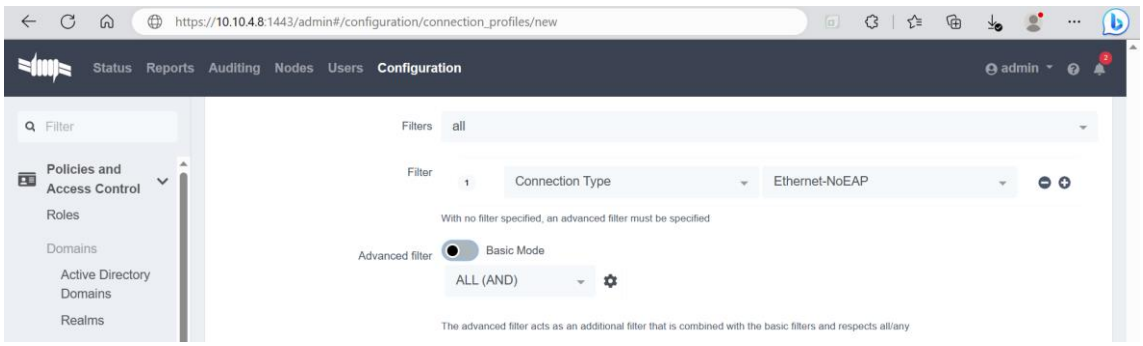

Figura 18. Configuracion del filtro MAB

En la figura 19 se muestra tres perfiles de conexión, el primer perfil es el que viene por defecto en el NAC y de hecho está protegido y no se puede eliminar. En la segunda y tercera columna se puede observar los dos perfiles de conexión que acabo de configurar en el apartado anterior.

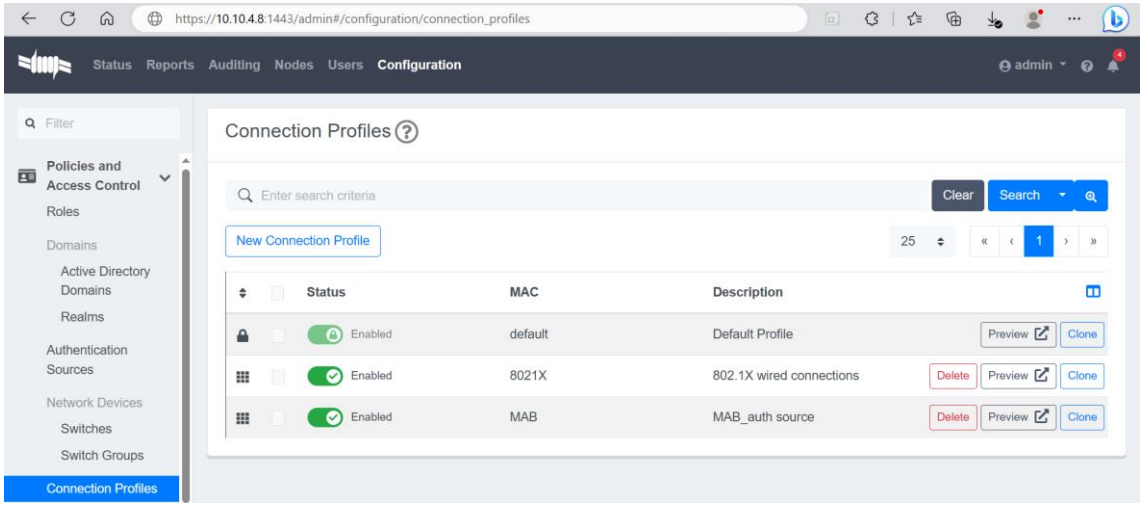

Figura 19. Perfiles de conexión configurados

7.3.3. El controlador de dominio Active Directory

Los usuarios en la red han de ser gestionados de manera eficiente. Para ello, es importante tener un servidor que agrupe en un solo lugar a todos los usuarios, de esta manera no tengo que crearlos localmente en cada uno de los dispositivos y tampoco tendría que mantenerlos individualmente. Administrándolo de esta forma, también realizamos buenas prácticas de seguridad. En el punto 7.3.2 se ha integrado el dominio AD a packetfence y es el que voy a utilizar para integrar adecuadamente los dispositivos y los usuarios (Corporativo e invitado) en la red. Por el lado de AD se ha hecho las siguientes configuraciones:

- En Windows server 2019 he implementado el controlador de dominio AD y he configurado el DNS para que se ajuste a la red en la que estoy trabajando. Como se muestra en la figura 20 se puede observar estos componentes, el AD DS permitirá el acceso tanto a la red como a los recursos a los usuarios que voy a crear posteriormente.

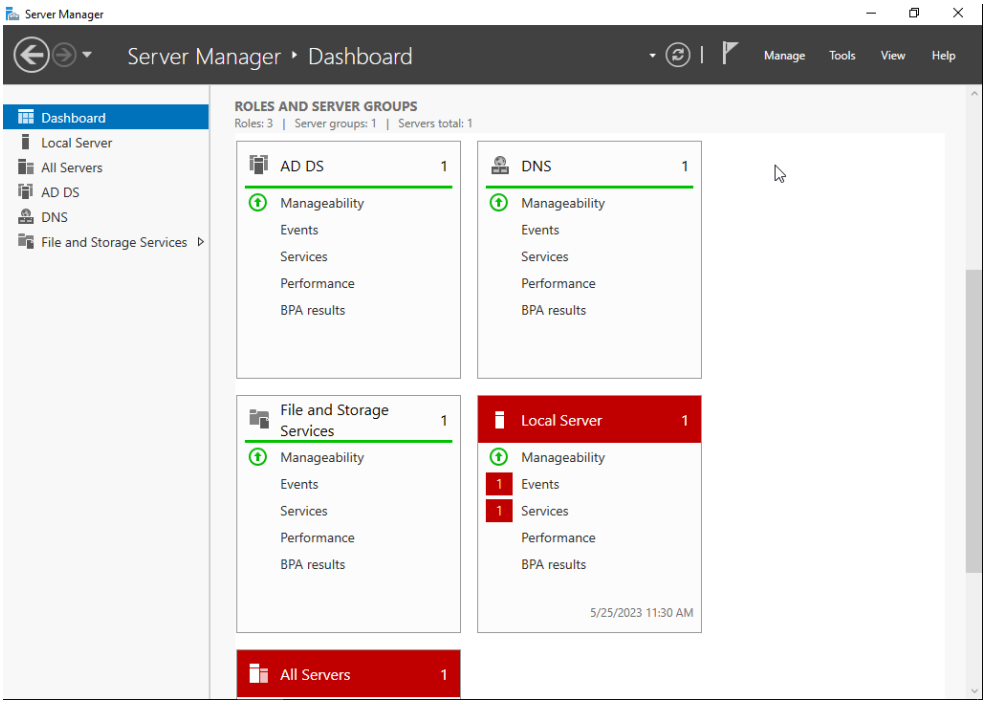

Figura 20. Configuración de AD DS

- He creado el dominio *tfm.local* para agrupar a los usuarios en grupos según el tipo de rol que se le asigne. El usuario Ruslan Nguema se le ha asignado el rol que se ha configurado para los usuarios corporativos, ya que pertenece a este grupo.

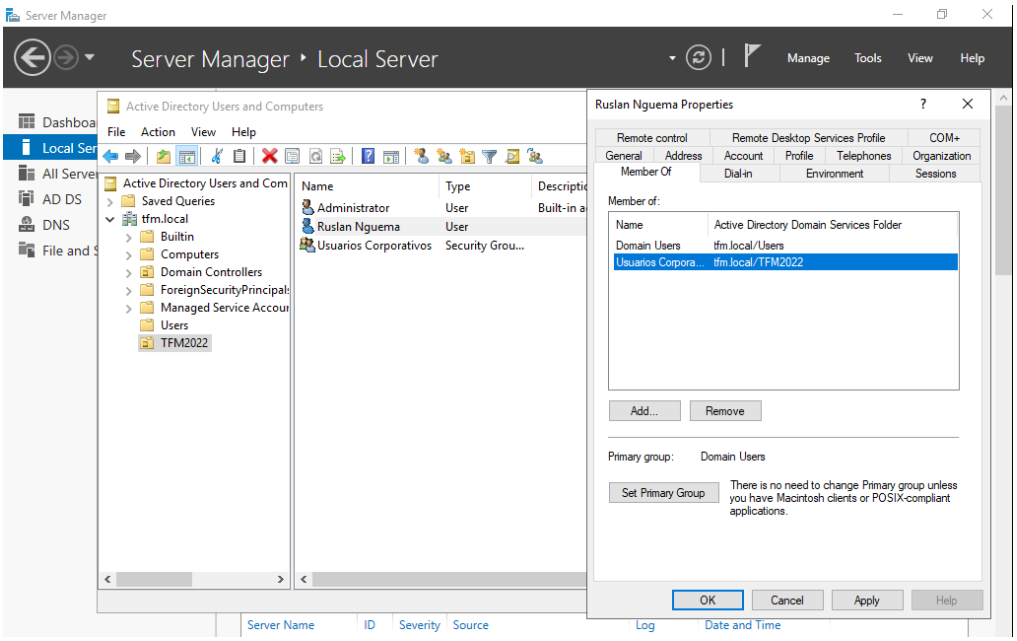

Figura 21. Creación del grupo y usuario corporativo

- Otro usuario que he creado ha sido el invitado Ngua Nsee, y le he agregado el rol de usuarios invitados. Lo que pretendo conseguir es que, este usuario podrá acceder a la red, y a los recursos que se le permite acceder como invitado, y no tendrá acceso a los recursos de los usuarios corporativos. El usuario administrador es el encargado de gestionar la red corporativa, por lo tanto, tiene asignado todos los roles y acceso a todos los grupos para gestionarlos ya que es la cuenta integrada para la administración del equipo y dominio.

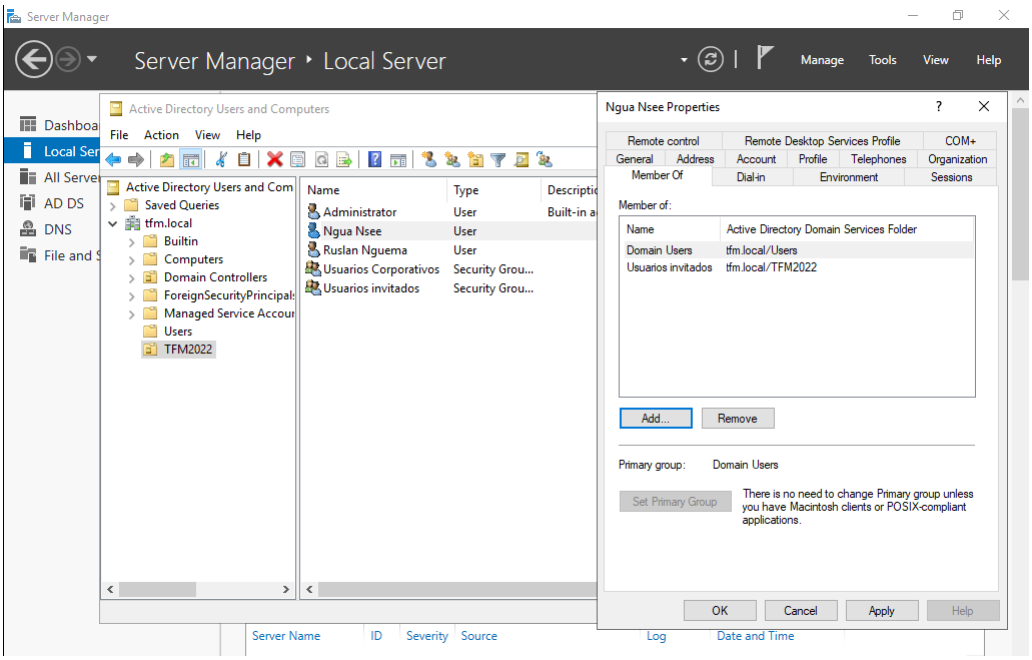

Figura 22. Creación del grupo y usuario invitado

8. Escenarios de pruebas

8.1. Escenario de Prueba 1: Usuario corporativo

En el diagrama de red de la figura 11, la maquina corporativa actúa como suplicante, y el objetivo que se persigue detrás es que este pueda simular una computadora de trabajo que quiera establecer conexión con la red y acceder a los recursos. La configuración que voy a realizar en este endpoint es habilitar la autenticación 802.1X, y para ello, primero habrá que iniciar el servicio Windows dot3svc Wired Autoconfig "Configuracion automática de redes cableadas". Este servicio nos permitirá autenticar las conexiones tanto si hacen por ethernet o a través de Wi-Fi a los dispositivos antes de que consigan ganar el acceso a la red.

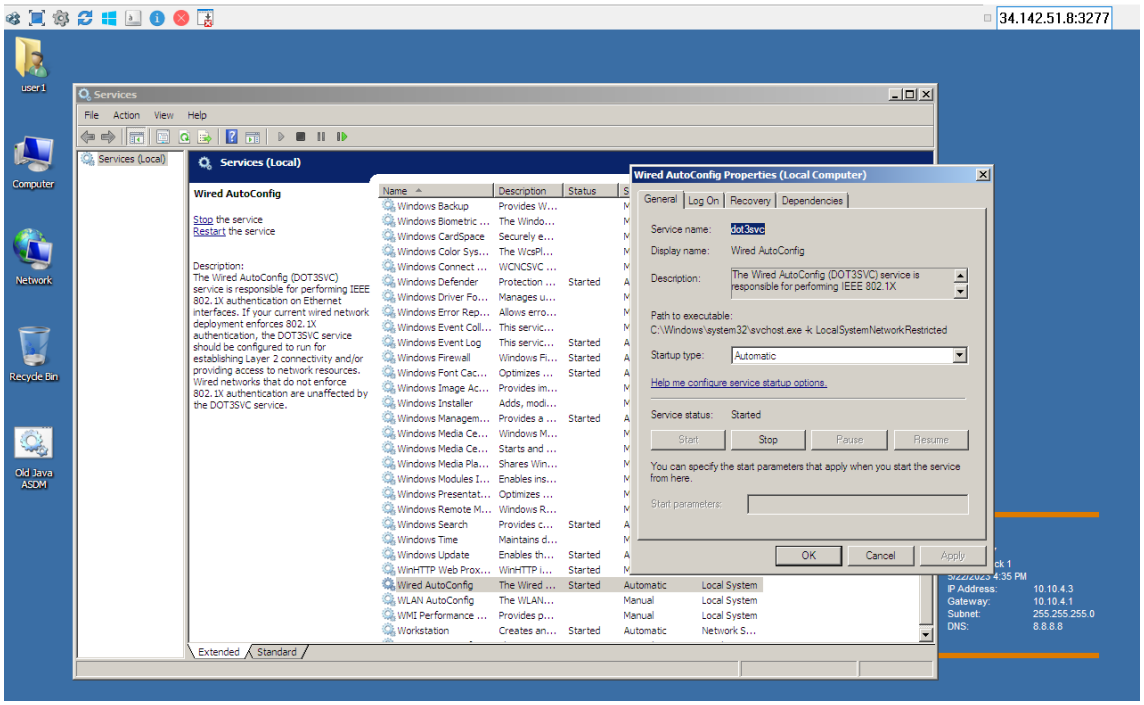

Figura 23. Habilitación del servicio Windows dot3svc

Ahora que se tiene iniciado este servicio, nos dirigimos al panel de configuración de red en las propiedades de la LAN, concretamente en la pestaña de autenticación habilitamos la autenticación IEEE 802.1X y seleccionamos Microsoft: protected EAP (PEAP) como método de autenticación.

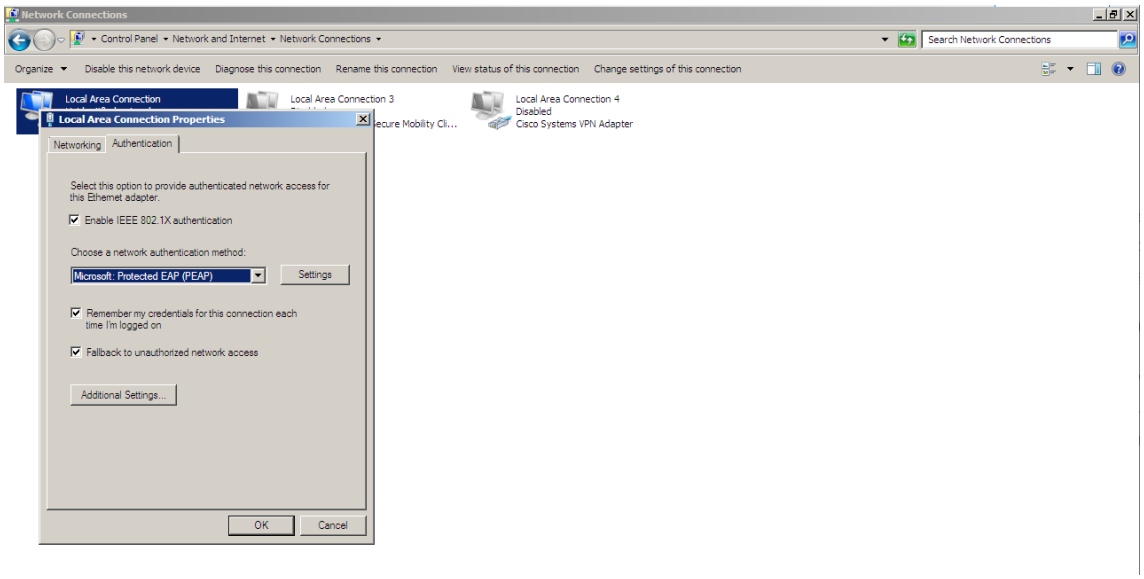

Figura 24. Habilitación de la autenticación IEEE 802.1X

Accedemos a las configuraciones de este método de autenticación para asegurarnos que se tiene seleccionada la opción Secured password (EAP-MSCHAPv2) “Contraseña segura (EAP-MSCHAPv2)” para encriptar las contraseñas, prevenir el acceso no autorizado, proporcionar seguridad en la red inalámbrica y cumplir con los estándares de seguridad.

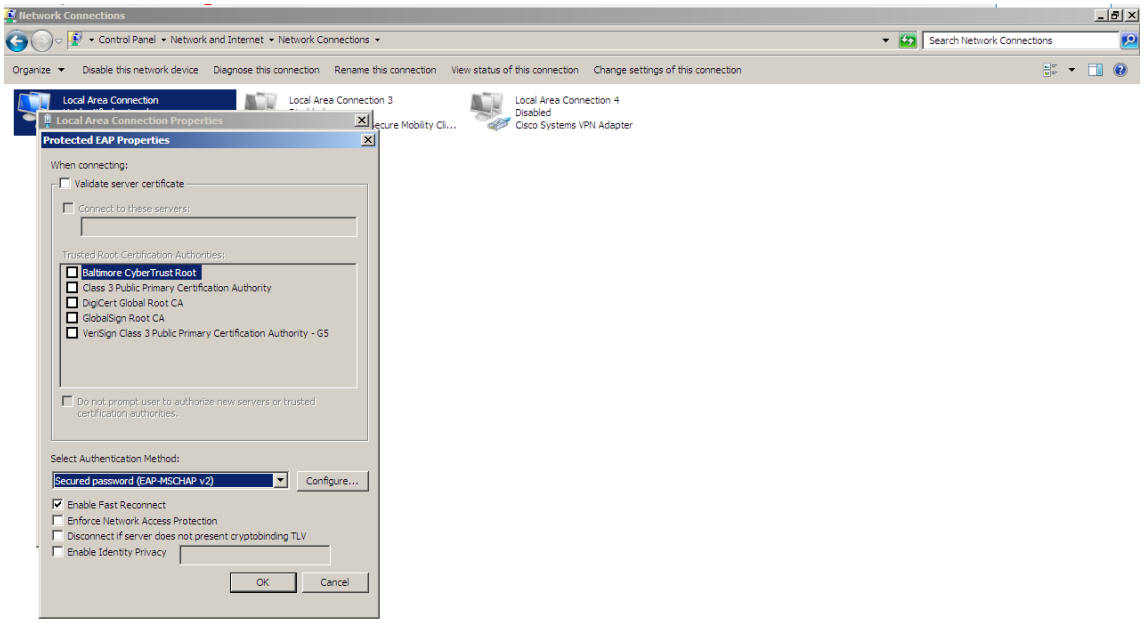

Figura 25. Propiedades EAP

Como ya se tiene listo la configuración por el lado del suplicante queremos realizar una prueba. Primero que todo ha de asegurarse desde packetfence de reiniciar el servicio "radiusd", esto es muy importante ya que se ha unido el controlador de dominio AD. Para ello, en la pestaña Estado → Servicios hacemos click el botón del servicio "radiusd" y de esta manera packetfence asumirá en control de que este servicio se reinicie así mismo como los subservicios "radiusd-acct" y "radius-auth".

Una vez realizado esto, podemos proceder a conectar la maquina corporativa al puerto e/0 donde se ha realizado las configuraciones del switch para simular la conexión. Desde esta máquina nos debería aparecer una ventana solicitando las credenciales del usuario, estas credenciales deben ser validas de nuestro AD configurado, lo que debería iniciar la autenticación 802.1X(EAP-PEAP).

Para verificar el estado de la conexión he de dirigirse a la pestaña de auditing, auditoria en la interfaz administradora de packetfence. Normalmente debería aparecer una entrada de la MAC de la maquina corporativa, y haciendo clic en la MAC se podría ver los intercambios de RADIUS. Si se da el caso de que la autenticación estándar IEEE 802.1X se efectué correctamente debería tener un "Aceptar" como "Estado de autenticación".

8.1.1. Posibles problemas en la prueba 1

Como tal es caso de que se han realizado las configuraciones y se han activado los protocolos de autenticación, el objetivo de este apartado es descubrir la problemática de que no se haya autenticado correctamente el usuario. Para ello accedemos a packetfence para comprobar los servicios si se han iniciado correctamente. Desde *status → servicios*, en la figura 26 observamos que tenemos algunas deficiencias como el fallo en el reinicio del servicio "radiusd-acct".

Figura 26. Fallo en el inicio del servicio radius-acct

Desde *status → servicios*, accedemos para reiniciar el servicio “iptables”. En la figura 27 observamos que se ha reiniciado correctamente, pero con un aviso de que necesita una configuración.

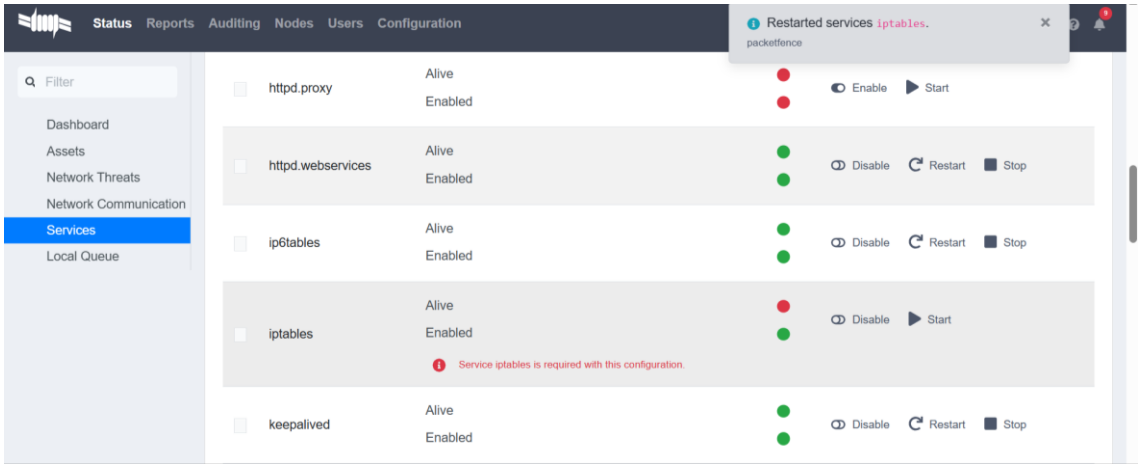

Figura 27. Requerimiento de configuración Iptables

Desde *status → servicios*, accedemos para reiniciar servicio “radiusd-auth”. En la figura 28 también se poder observar que se ha reiniciado correctamente, pero al igual que la figura 27 existe un aviso de que se necesita una configuración.

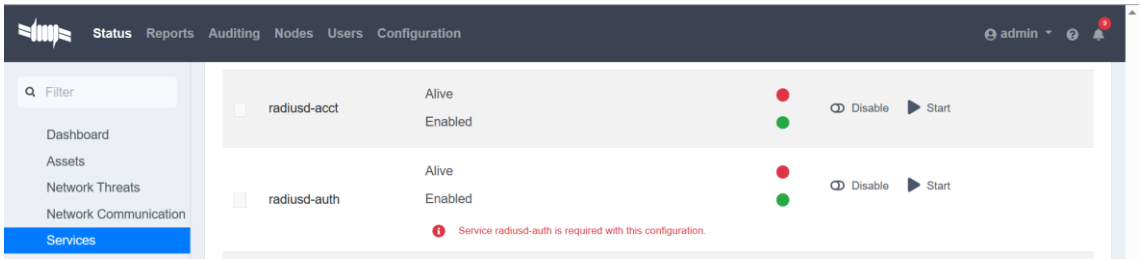

Figura 28. Requerimiento de configuración radius-auth

8.2. Switch 2

He integrado el switch 2 en la red para configurar una segunda LAN destinada a los usuarios que solo se conectaran a internet. Estos usuarios no tendrán acceso a la red de gestión donde se encuentran los recursos ya que se encuentran en LAN distintas. Parte de esta configuración se realiza en packetfence, ya que es el que se encargara de controlar el acceso, definir el rango IP que posteriormente se designaran por DHCP a través de switch a los dispositivos que se conectan a esta LAN. En la figura 28 se muestra la configuración del tipo de conexión, la configuración del DNS y la habilitación del servidor DHCP y NAT.

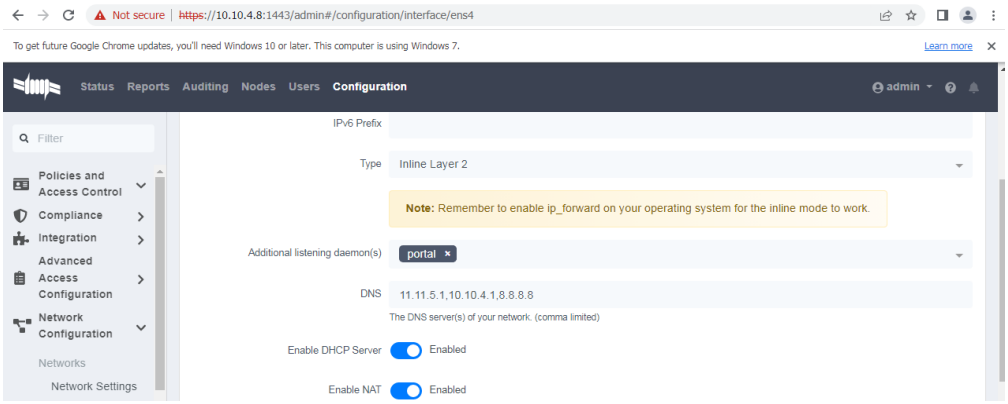

Figura 29. Habilitación del servidor DHCP packetfence

Por otro lado, lo siguiente es configurar la red específica a la que se conectaran tanto el switch 2 como los puntos finales, en este caso el usuario estándar. El filtro de red que se ha establecido es la LAN 11.11.5.0/24 y se muestra en la figura 30.

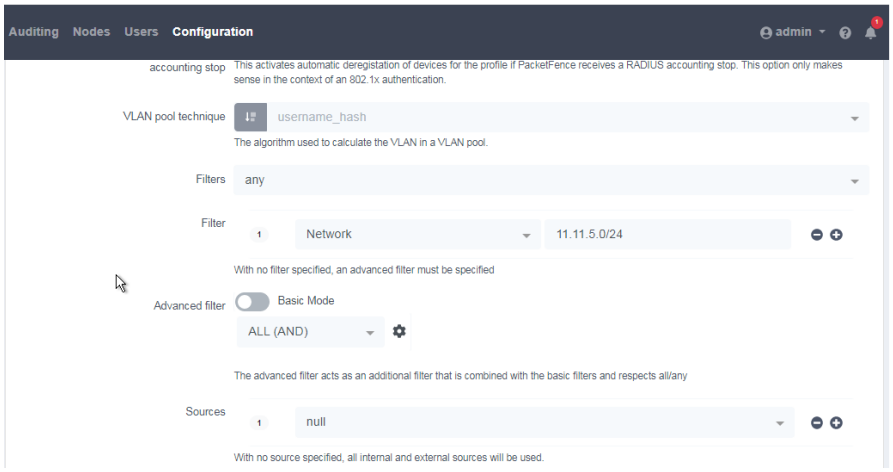

Figura 30. Configuracion rol IP en Switch 2

Este switch se ha integrado y se ha conectado con la segunda interface habilitado en packetfence que es la ens4. La primera intrface en packetfence es la ens3. En la figura 30 se puede ver que se encuentran en LAN distintas, lo que puede ayudar a que, en el hipotético caso de que un atacante suplante la dirección MAC o IP del dispositivo en esta red, esto no significa automáticamente que pueda acceder a la LAN privada donde se encuentra los recursos, ya que esa se ha implementado buenas prácticas de seguridad mediante protocolos de autenticación.

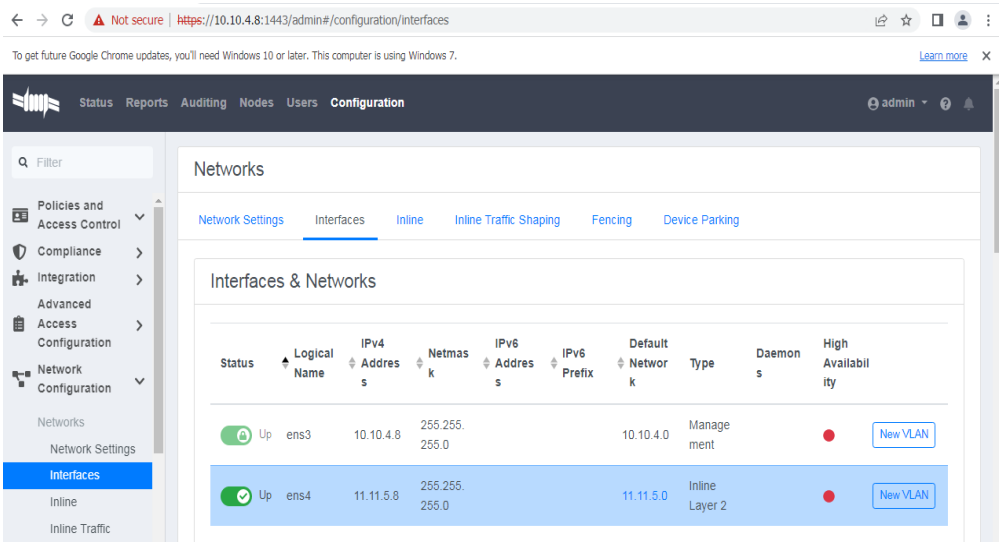

Figura 31. Packetfence interface 2 habilitado

8.2.1. Escenario de Prueba 2: Usuario Estándar

En esta segunda prueba se ha utilizado otra máquina Windows 7 y se ha denominado como usuario estándar. La configuración que se va a realizar aquí es relativamente Sencilla. Si retrocedemos a la figura 28 nos aparece un aviso en packetfence que es de habilitar IP_forwading en la máquina para que este modo inline funcione, y es lo que se va a realizar posteriormente que esta pueda recibir una IP. Cuando este modo está habilitado, packetfence hace de punto control entre la red interna y externa. Todos los paquetes de red van a transitar a través de él, y esto permitirá que se pueda inspeccionar el tráfico para poder garantizar la seguridad en nuestra red. Para ello, desde el "Registry editor", accedemos a la ruta que a continuación se define:

"Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters"

Una vez accedido a esta ruta, buscamos por la función “IPEnableRouter” y su valor lo seleccionamos a 1 para que se active.

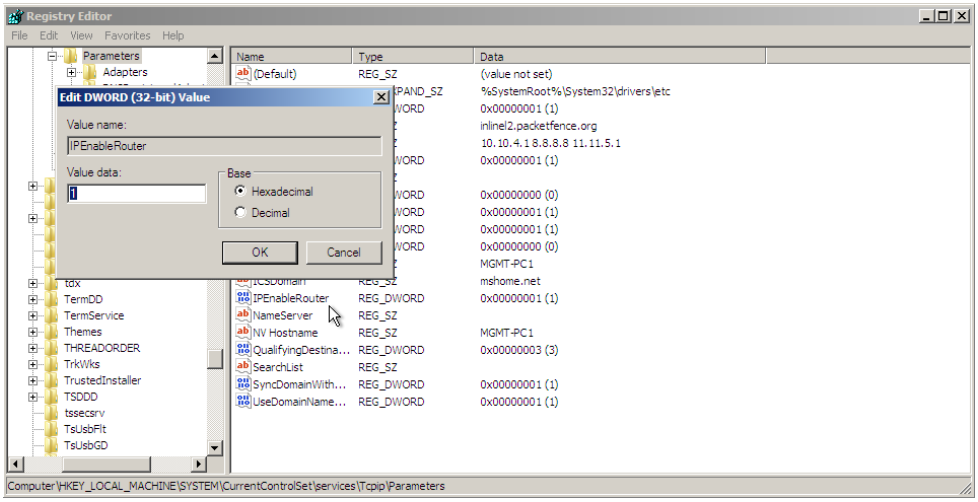

Figura 32. Habilitación de IP_forwading en el usuario estándar

Cuando ya se tiene esta función activada, conectamos la computadora al puerto del switch, y si se ha configurado de manera adecuada nos estaría asignado una dirección IP en el rango correcto del rol que se ha configurado. Para comprobar esto, accedemos al terminal de comandos de la computadora. En la figura 33 podemos observar que Packetfence ha asignado correctamente la dirección IP de acuerdo a la subred en el rango 11.11.5.0 y el tipo de rol y conexión configurado en packetfence.

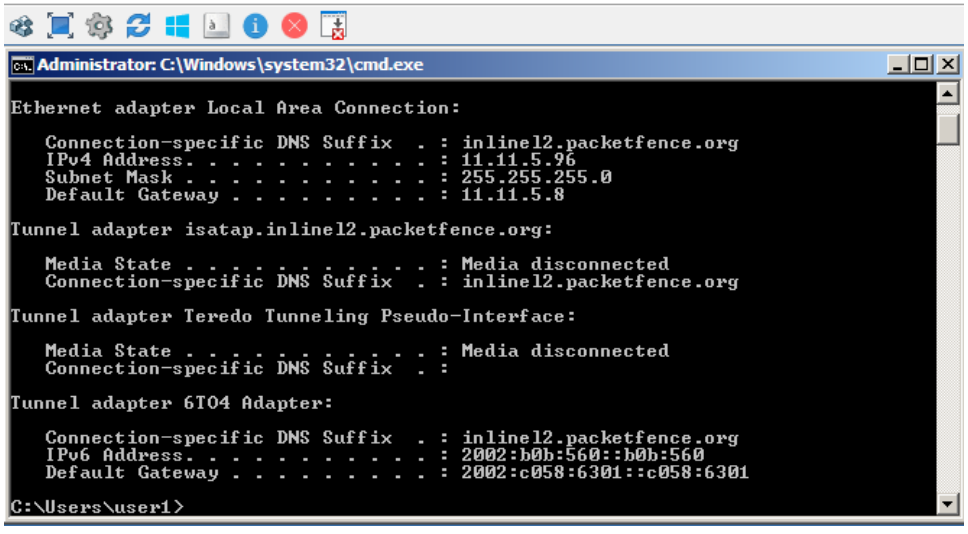

Figura 33. Rol IP asignado al usuario estándar

Para saber los detalles de esta conexión, accedemos al portal de administración de packetfence y en la pestaña *status* → *Dashboard* podemos ver el estado de la conexión. En la figura “” en el círculo rojo vemos que el sistema ha registrado un dispositivo, y en el círculo verde se detecta el tipo de conexión.

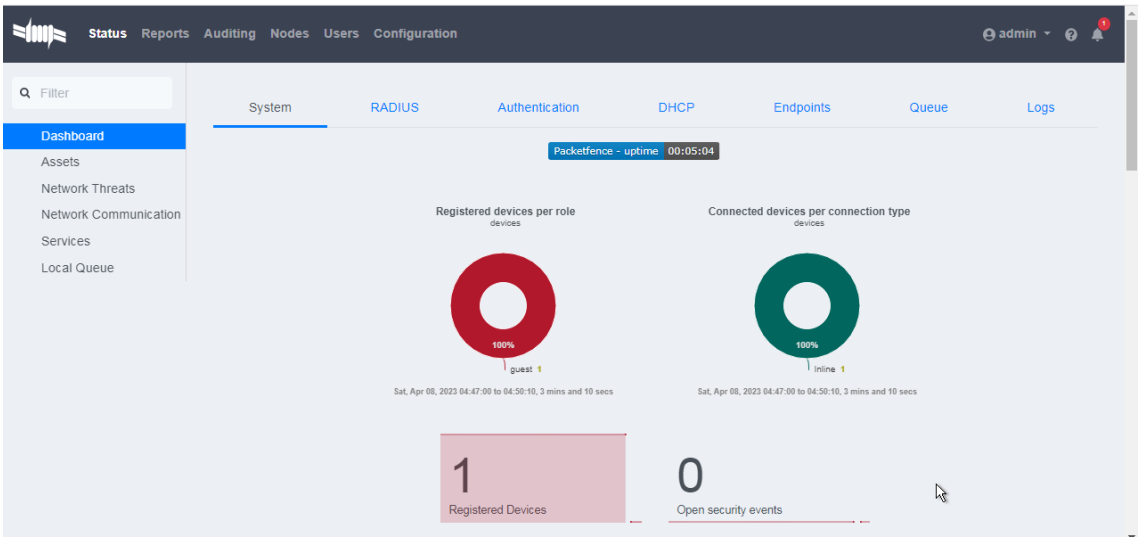

Figura 34. Usuario estándar registrado

En la pestaña “nodes” se ha obtenemos más información como el estado conexión del dispositivo, la detección de la dirección MAC, la fecha en la que se ha detectado por primera vez la conexión del dispositivo, el nombre del dispositivo, la dirección IP, el rol asignado y el tipo de conexión.

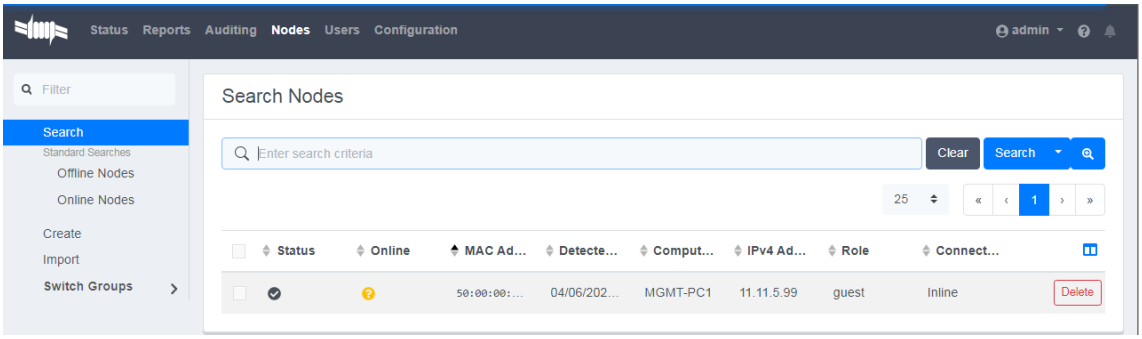

Figura 35. información de la conexión del usuario estándar

Si hacemos clic en la dirección MAC nos aparece más información del rol configurado como, por ejemplo, el tiempo de conexión que dispone el dispositivo, la última vez de conexión entre otros. En este caso le he asignado a los usuarios estándares que se conecten a esta red un tiempo máximo de 24 días, cuando exceda tendrán que registrarse de nuevo.

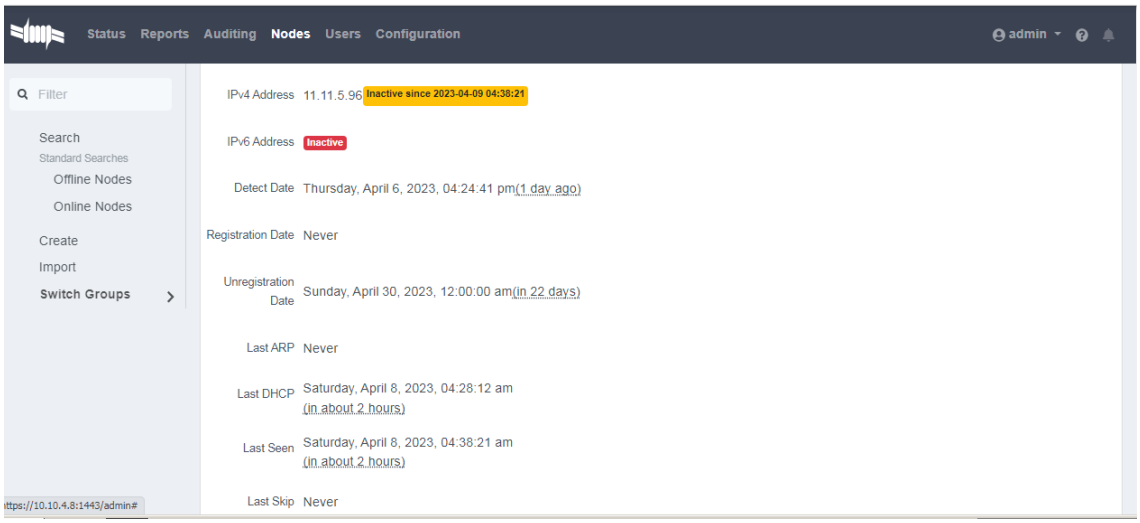

Figura 36. Información adicional de la conexión

9. Conclusiones y trabajo futuro

Este trabajo fin de master se ha centrado en el estudio y planteamiento de una posible solución de seguridad con el NAC de packetfence para una red corporativa que pueda garantizar el acceso seguro de los usuarios a la red. En primer lugar, se ha presentado un estudio de viabilidad para plantearse de manera estratégica que es lo necesario que se deberá hacer para poder alcanzar los objetivos, se ha hecho una investigación sobre teorías, conceptos, y estudios previos que guardan relación con el trabajo fin del master.

Uno de los objetivos principales ha sido implementar el NAC en una máquina virtual e integrarlo en una red estándar para crear políticas de control de acceso. También se integrado el controlador de dominio AD a la red para crear usuarios y grupos que serán filtrados por packetfence para autenticarlos. He realizado una comparativa de los distintos métodos de autenticación y se ha comprobado que cada uno de ellos ofrece una solución de seguridad y que todos juntos el sistema de red se hace más seguro.

A lo largo de este trabajo, packetfence ha demostrado ser una herramienta de seguridad potente ya que permite la creación de políticas personalizadas y detectar amenazas de manera eficiente. Hay muchas cosas que se pueden conseguir implementar con este NAC, pero por cuestiones de tiempo y recursos no se ha podido profundizar en el tema. Por ejemplo, una posible mejora que se puede implementar en la red configurada puede ser la autenticación de los usuarios mediante certificados.

Para la organización de este trabajo he utilizado la herramienta trello, y he ido creando tarjetas y estableciendo fechas límites para finalizar con cada objetivo. Aunque haya habido retrasos, esto me ha ayudado a trabajar de manera eficaz y organizada.

Finalmente, con este trabajo he podido actualizar mis conocimientos sobre las distintas técnicas, protocolos y soluciones que se aplican hoy en día para garantizar el acceso seguro a las redes. Por otro lado, algunos de los pasos que se pueden realizar en el futuro seria la experimentación en un entorno real, la configuración de certificados para la autenticación de los usuarios.

10. Referencias

1. https://www.packetfence.org
2. David Romera. (2021, 9 de diciembre) ejemplos de análisis DAFO. Disponible en: Ejemplos de análisis DAFO: Qué es y cómo se hace (holded.com)
3. Canva. Disponible en: https://www.canva.com
4. José Vicente Berná Martínez (versión del documento, 2023.02.06) Guía para el Desarrollo de los Trabajos Fin de Grado y Fin de Máster.
5. Trello. https://www.trello.com
6. Benjie. (2022, March 15). MAC Authentication Bypass (MAB) authentication explained. Disponible en: https://study-ccnp.com/mac-authentication-bypass-mab-authentication-explained/
7. Wikipedia contributors. (n.d.). *Extensible Authentication Protocol*. Disponible en: https://es.wikipedia.org/wiki/Extensible_Authentication_Protocol
8. De Luz, S. (2021, September 20). Descubre para qué sirve un servidor RADIUS y su funcionamiento. RedesZone. Disponible en: https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/
9. Wikipedia. (2018, 4 de febrero). Disponible en: IEEE 802.1X. https://en.wikipedia.org/wiki/IEEE_802.1x
10. Wikipedia. (16 de septiembre de 2008). Control de acceso a la red. Disponible en: https://es.wikipedia.org/wiki/Control_de_acceso_a_red
11. INCIBE. (2019, agosto 6). Sistemas de control de acceso a la red. Disponible en: https://www.incibe.es/protege-tu-empresa/catalogo-deciberseguridad/listado-soluciones/sistemas-control-acceso-red
12. Rueda, C. (n.d.). Autenticación y autorización basado en localización en red en entornos corporativos. Uoc.edu. Disponible en: https://openaccess.uoc.edu/bitstream/10609/120606/8/cruedavTFM0620memoria.pdf
13. VMware Workstation Pro documentation. (n.d.). Vmware.com. Disponible en: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html

14. Wikipedia contributors. (n.d.). Google Cloud.The Free Encyclopedia. Disponible en: https://es.wikipedia.org/w/index.php?title=Google_Cloud&oldid=136022803
15. No title. (n.d.). Eve-ng.net. Disponible en: https://www.eve-ng.net/
16. PuTTY: a free SSH and Telnet client. (n.d.). Org.uk. Disponible en: https://www.chiark.greenend.org.uk/~sgtatham/putty/
17. Last modified by Martin. (2014, septiembre 12) Introducción WinScp. Disponible en: https://winscp.net/eng/docs/lang:es
18. Fernández, Y. (2018, April 10). Archivos ISO: qué son y cómo montarlos en Windows y macOS. Disponible en: https://www.xataka.com/basics/archivos-iso-que-son-y-como-montarlos-en-windows-y-macos
19. ZeroTier. (n.d.). Disponible en: https://www.zerotier.com/
20. Hernandez, E. [@life4cisco]. (2022, July 22). Instalación de EVE-NG en Google Cloud Gratis, te mostramos como. Youtube. Disponible en: https://www.youtube.com/watch?v=k6GjmipANIk
21. How to load images. (2019, November 6). Eve-ng.net; EVE-NG Ltd. Disponible en: https://www.eve-ng.net/index.php/documentation/howtos/
22. How to load images. (2019, November 6). Eve-ng.net; EVE-NG Ltd. Disponible en: https://www.eve-ng.net/index.php/documentation/howtos/
23. Network Collective [@NetworkCollective]. (2021, February 28). Part #2: Give your EVE-NG lab internet access. Youtube. Disponible en: https://www.youtube.com/watch?v=7CJR2l8VXM0
24. Imanol Gómez miranda (septiembre 2021) Implementación y creación de escenarios de pruebas en cisco ISE.
25. Rueda, C. (n.d.). Autenticación y autorización basado en localización en red en entornos corporativos. Uoc.edu. disponible en: https://openaccess.uoc.edu/bitstream/10609/120606/8/cruedavTFM0620memoria.pdf

Anexos

1. Alojamiento de las máquinas virtuales en VMware Workstation

En VMware Worktation, con la imagen de PacketFence ya se podía acceder al portal web de configuración del NAC, pero era necesario un dispositivo que los enlace como un switch para realizar las configuraciones, este es el motivo por el cual se ha integrado el NAC directamente en el emulador.

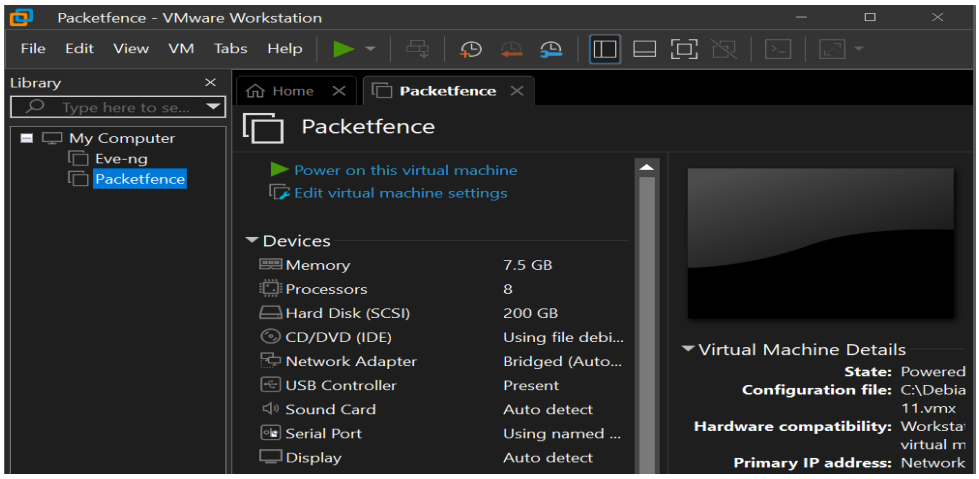

Figura 37. Alojamiento inicial del NAC y EVE-NG

2. Facturación en google cloud

Decidí migrar el proyecto a cloud porque no disponía de recursos necesarios en materia de capacidad de almacenamiento.

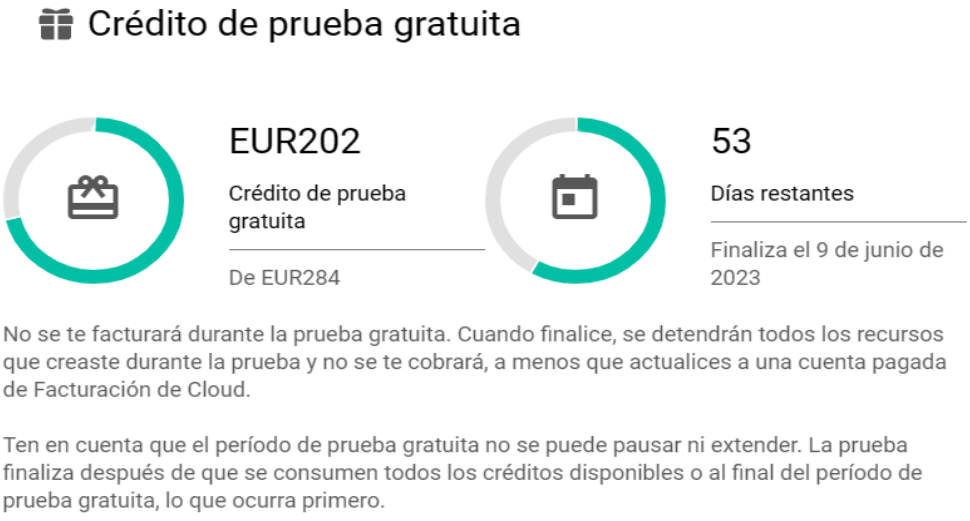

Figura 38. Créditos de prueba gratuita en google cloud

3. Reglas de firewall creadas en google cloud

Estas configuraciones normalmente se deben crear para bloquear todo el tráfico que viene del exterior de mi red, pero como esto es una prueba he creado la regla *"permitall"* para permitir el tráfico y que no me cree complicaciones más a delante cuando esté con las configuraciones e implementaciones.

Figura 39. Reglas de cortafuegos creada en google cloud

4. Visualización Inicial de eve-ng

Una vez accedido a EVE-NG con la IP externa que nos ofrece la instancia e introducido las credenciales por defecto, esta es la visualización inicial del entorno de trabajo en donde he creado la carpeta TFM2022 para la implementación.

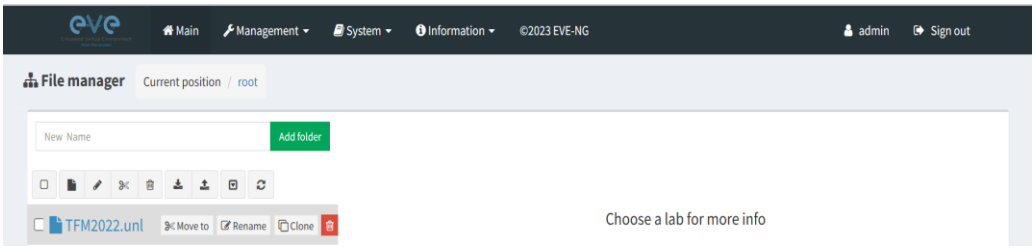

Figura 40. Vista previa EVE-NG

5. Transferencia de archivos a eve-ng

Para transferir los archivos de del equipo físico a EVE-NG, es importante subir los archivos como recomienda la página oficial de EVE-NG, es decir, a la hora de subir un archivo creamos la carpeta con el nombre seguido de la versión y guardar el archivo dentro de esa carpeta; estas carpetas se hospedan en la ruta "/opt/unetlab/addons/qemu/".

En el lado izquierdo de la figura 41 se encuentran las imágenes en el equipo físico, en el lado derecho las imágenes ya subidas a EVE-NG.

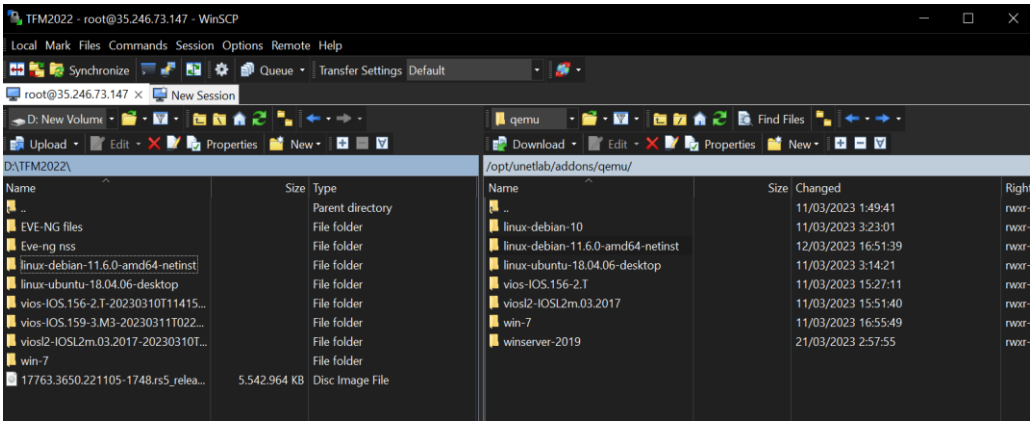

Figura 41. Transferencia de archivos en WinScp

6. Asignación de IP

En el archivo: /etc/network/interfaces configuraré una IP estática y mascara de red a la pnet9, y reiniciaré la red para que la IP se actualice correctamente en la interface. Para que surta efecto esta configuración y que los cambios se realicen correctamente se ejecuta el comando: systemctl restart networking

Figura 42. Asignación de IP a la instancia

7. Habilitación de IP forwading

Esta función permite que EVE-NG pueda reenviar el trafico IP a los destinos que no conoce. En el archivo /etc/sysctl.conf basta con dejar sin comentar la línea para que para activarlo.

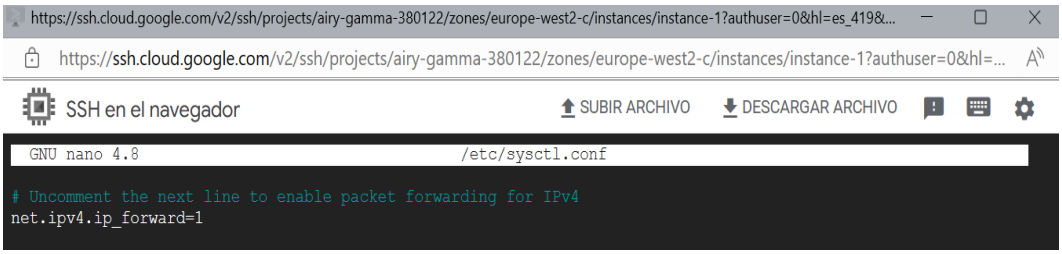

Figura 43. Configuración de IP forwading en la instancia

8. Regla de IpTables para NAT saliente

En esta configuración el comando "`iptables -t -A POSTROUTING -o pnet0 -s 198.18.18.0/24 -j MASQUERADE`" modifica las reglas de firewall netfilter, determina la tabla NAT que es la que se va a modificar, determina la secuencia de la tabla NAT. donde deberán ser añadidas las reglas. procesa los paquetes cuando van saliendo del sistema, determina la interfaz que deben enviarse los paquetes, la conducta de destino a realizar en los paquetes que guardan coincidencia con la regla establecida.

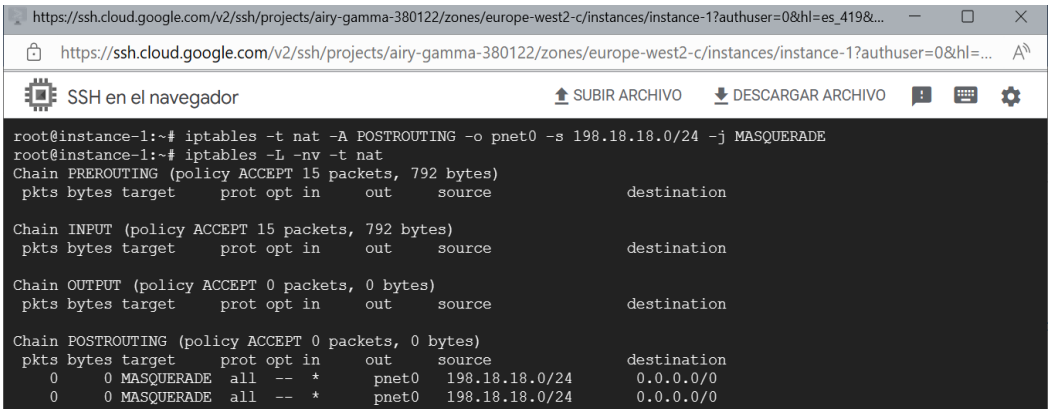

Figura 44. Regla iptables del trafico saliente de EVE-NG

9. Triangulación de la red con Zerotier

Esta configuración de VPN es una adición al trabajo, para establecer una conexión de red triangulada con Zerotier para poder acceder a los dispositivos con aplicaciones locales en mi pc en lugar de cli vía navegador.

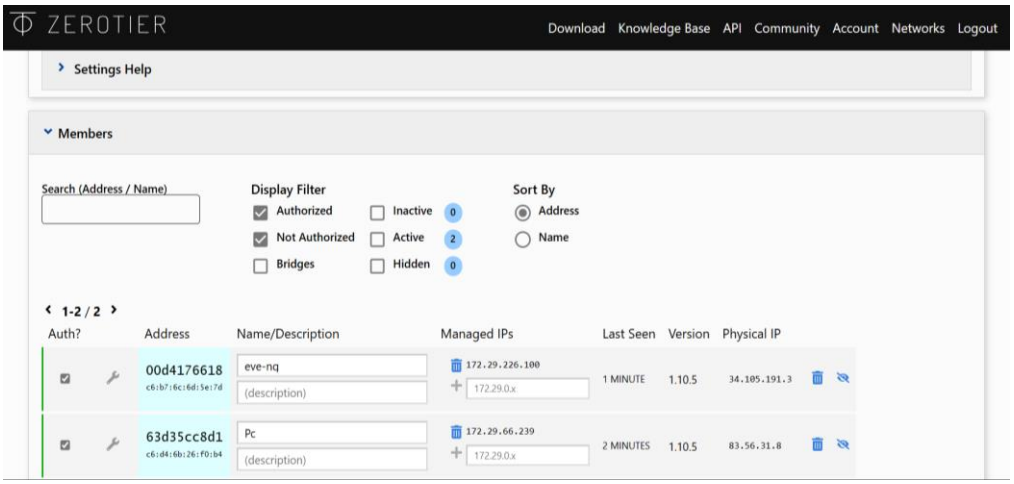

Figura 45. VPN Zerotier

10. Configurador de packetfence, Paso1.

Para definir la interfaz de red que será la que se comunicará con el switch de acceso, esta interfaz será de tipo ‘management”.

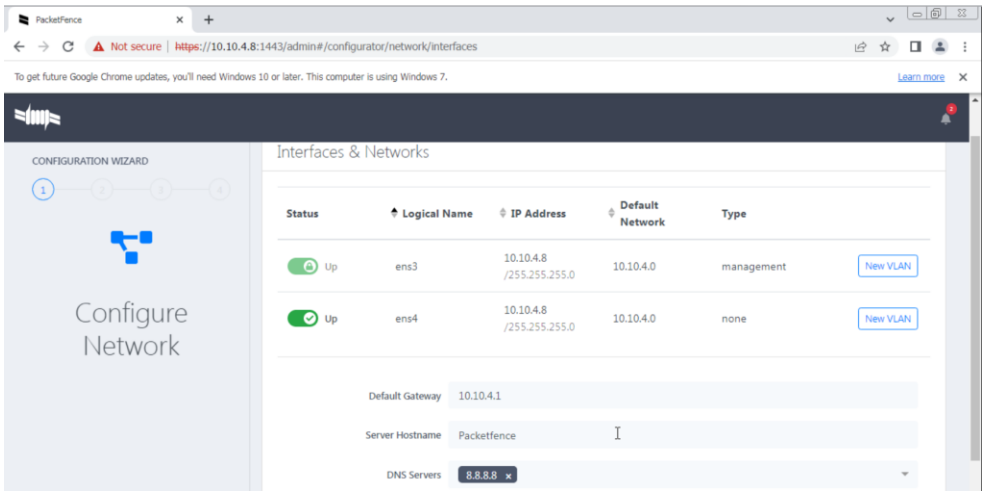

Figura 46. Configuracion inicial de red para Packetfence

11. Configurador de packetfence, paso 2.

En este paso, se define toda la información que se requiere para generar la base de datos. Igualmente, el host, el nombre de dominio y las credenciales de gestión del administrador.

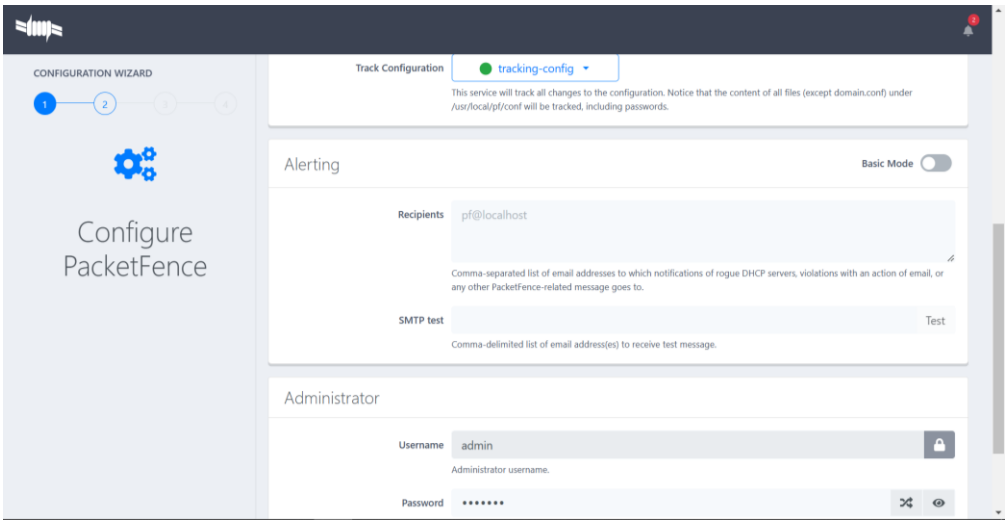

Figura 47. Configuracion de las credenciales admin en packetfence

12. Configuración del Router

```
R1#sh run

Building configuration...

Current configuration : 1312 bytes

!

version 12.4

service config

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!
```

hostname R1

!

boot-start-marker

boot-end-marker

!

enable secret 5 1R9Cb$KA5L7RwesFz/d2M1IWzvV/

!

no aaa new-model

memory-size iomem 5

ip cef

--More--

*Mar 1 00:15:35.727: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from(tftp://255.255.255.255/network-conip name-server 8.8.8.8

!

multilink bundle-name authenticated

!

archive

log config

hidekeys

!

interface FastEthernet0/1

description coneccion con internet

```
 ip address 198.18.18.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/0
 description coneccion con Sw1
 ip address 10.10.4.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet1/0
 --More--
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
*Mar  1 00:16:16.743: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from(tftp://255.255.255.255/cisconet.c description uplink with
!
router eigrp 1
 network 10.0.0.0
```

```
 auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.18.18.1
!
ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/0 overload
access-list 1 permit 10.10.4.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

13. Configuración del Switch 1

- Primero que todo, en caso de que no esté habilitado el control de autenticación habrá que hacerlo en el switch con el comando:

```
dot1x system-auth-control
```

- El siguiente paso es la configuración global de AAA:

```
aaa new-model
```

- A continuación, habrá que crear un grupo de servidor de nombre packetfence y utilizando su dirección IP:

```
aaa group server radius packetfence
    server 10.10.4.8 auth-port 1812 acct-port 1813
```

- Lo siguiente es configurar la autenticación y autorización de tal forma que estos formen parte del grupo de que se acaba de crear:

```
aaa authentication login local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
```

- Un paso muy importante es establecer el protocolo de autenticación y autorización dispondremos para poder acceder a la red. Como se ha mencionado se usa el protocolo de RADIUS entre el switch y packetfence.

```
radius-server host 10.10.4.8 auth-port 1812 acct-port
1813 timeout 2 key useStrongerSecret
    radius-server vsa send authentication
```

También se debe configurar la VLAN, una para los usuarios que se autentican por 802.1X, otra para los que soporten MAB y otra para usuarios que no tengan grupos asignados a

los puertos en los que se conectaran los dispositivos o usuarios, pero como en este escenario de prueba, en el switch 1 solo se ha configurado un puerto para la conexión, entonces se ha creado una sola VLAN.

Aparte de la configuración basica del puerto e/1, la configuración especifica que se ha realizado en el puerto e/1 para la autenticación en el del switch es la siguiente:

```
switchport mode Access
switchport Access Vlan20
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
dot1x timeout quiet-period 2
dot1x time tx-period 3
```

A continuación, la configuración completa de switch 1:

```
User Access Verification


Username: admin
Password:


Sw1>en
Password:
Sw1#show run
Building configuration...
Current configuration : 2755 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Sw1
!
boot-start-marker
```

```
boot-end-marker
!
enable secret 4 0dNf2ldHgFNSUdBfp7wD01BSh0xua3joT5tvmc7uLzs
!
username admin privilege 15 secret 4 0dNf2ldHgFNSUdBfp7wD01BSh0xua3joT5tvmc7uLzs
aaa new-model
!
aaa group server radius packetfence
 server 10.10.4.8 auth-port 1812 acct-port 1813
!
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
!
aaa server radius dynamic-author
 client 10.10.4.8
 server-key useStrongerSecret
 port 3799
!
aaa session-id common
!
```

```
ip cef
ip dhcp excluded-address 10.10.4.1 10.10.4.30
ip dhcp excluded-address 10.10.4.1 10.10.4.25
!
ip dhcp snooping vlan 20
no ipv6 cef
ipv6 multicast rpf use-bgp
!
dot1x system-auth-control
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Ethernet0/0
 description coneccion con el R1
 switchport access vlan 20
 switchport mode access
 duplex auto
 ip dhcp snooping limit rate 10
!
```

```
interface Ethernet0/1
 description coneccion con el usuario corporatvo
 switchport access vlan 20
 switchport mode access
 duplex auto
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 10800
 authentication timer reauthenticate 10800
authentication violation replace
 mab
 no snmp trap link-status
 dot1x pae authenticator
 dot1x timeout quiet-period 2
 dot1x timeout tx-period 3
 ip dhcp snooping limit rate 10
!
interface Ethernet0/2
 description coneccion con el NAC de Packetfence
 switchport access vlan 20
```

```
 switchport mode access
 duplex auto
 ip dhcp snooping limit rate 10
!
interface Ethernet0/3
 description coneccion con el controlador de dominio AD
 switchport access vlan 20
 switchport mode access
 duplex auto
 ip dhcp snooping limit rate 10
!
interface Ethernet1/0
 description coneccion con la pc Admin
 switchport access vlan 20
 duplex auto
 ip dhcp snooping limit rate 10
!
interface Ethernet1/1
 duplex auto
!
interface Ethernet1/3
 duplex auto
```

```
!
interface Vlan20
 ip address 10.10.4.2 255.255.255.0
 shutdown
!
router eigrp 1
 network 10.0.0.0
!
ip default-gateway 10.10.4.1
!
no ip http server
!
snmp-server community public RO
snmp-server community private RW
!
radius-server host 10.10.4.8 auth-port 1812 acct-port 1813 timeout 2 key
useStrongerSecret
radius-server vsa send authentication
!
control-plane
!
line con 0
```

```
 logging synchronous
line aux 0
line vty 0 4
!
end
```

14. Configuración del Switch 2

```
User Access Verification


Username: admin
Password:


Sw2>en
Password:


Sw2#sh run
Building configuration...


Current configuration : 1087 bytes
!
version 15.1
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Sw2
!
boot-start-marker
boot-end-marker
!
!
!
username admin privilege 15 secret 4 0dNf2ldHgFNSUdBfp7wD01BSh0xua3joT5tvmc7uLzs
no aaa new-model
!
ip cef
!
!
ip dhcp snooping vlan 30
no ipv6 cef
ipv6 multicast rpf use-bgp
```

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface Ethernet0/0
 description connecion con el NAC de Packetfence
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet0/1
 description connecion con el usuario estandar
 switchport access vlan 30
 switchport mode access
 duplex auto
 ip dhcp snooping limit rate 10
!
interface Ethernet0/2
 duplex auto
!
```

```
interface Ethernet0/3
 duplex auto
!
interface Vlan30
 ip address 11.11.5.2 255.255.255.0
 shutdown
!
no ip http server
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```