Universitat Oberta de Catalunya

uoc.edu

Autenticación y autorización basado en localización en red en entornos corporativos.

Carolina Rueda
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Víctor Méndez Muñoz
Víctor García Font

02/06/2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Autenticación y autorización basado en localización en red en entornos corporativos*
Nombre del autor:	*Carolina Rueda Ventura*
Nombre del consultor/a:	*Víctor Méndez Muñoz*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	06/2020
Titulación:	*MISTIC*
Área del Trabajo Final:	*Identidad Digital*
Idioma del trabajo:	Castellano
Palabras clave	*Autenticación; Autorización; Suscripción a redes privadas*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

Actualmente todas la empresas están empezando a buscar soluciones que mejoren la seguridad desde el punto de vista de la informática. Hay diferentes ámbitos en los que se puede mejorar, ya sea autenticación, entorno de trabajo, auditorias, autorización, entre otros. En el caso de la autenticación hay diferentes maneras de abordarla, la que hemos escogido para este caso es la autenticación en la red privada de una empresa. Ya que es importante restringir el uso de esta red a personal autorizado.

Para ello se utilizará el método *case study*, que consiste en investigar un caso de uso en concreto en profundidad, para explorar causas de los principios subyacentes. Se quiere buscar una solución que ayude a mejorar la autenticación de una red privada, como por ejemplo con la utilización de certificados, dando un grado más de seguridad.

Abstract (in English, 250 words or less):

Nowadays all companies are starting to search for solutions that improve security from the point of view of computing. There are different areas in which can be improved, authentication, work environment, auditories, authorization, etc. In the case of authentication there are different ways of approaching it. The one chosen to analyze in this case is authentication in a company's private network. Since it is important for a company to restrict the use of this network only to authorised persons.

To study this case the method used is *case study*. This method consists of involving an up-close, in-depth, and detailed examination of a particular case. We want to find a solution that helps improve the authentication of a private network, such as the use of certificates, giving a higher degree of security

Índice

Lista de Figuras

Lista de Tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

Cada vez más las empresas apuestan por mejorar la seguridad en la redes que utilizan cada día. La información que un atacante puede sustraer de un posible ataque fructífero puede ser perjudicial para la empresa, también teniendo en cuenta que puede ser información confidencial con la que alguien puede extraer beneficio de ella.

Por ello es importante tener correctamente configurada la red privada de las empresas. Teniendo en cuenta que algunos usuarios de estas redes pueden ser vulnerables a ataques de ingeniería social y se podría extraer información.

Actualmente en la empresa en la que estoy trabajando se está gestionando de la siguiente manera. Para que un empleado pueda autenticarse y poder entrar en la red el dispositivo que utilice para conectarse a de estar registrada su MAC. Así cualquier dispositivo externo a la empresa no puede conectarse a la red privada.

Aunque tengamos un sistema de autenticación tiene algunas carencias y se puede mejorar si hablamos de la parte de seguridad. Porque el problema que podemos tener es que si una persona externa consigue la MAC de algún dispositivo que esté autorizado, puede impersonar y conseguir entrar en la red sin la necesidad de disponer de un dispositivo autorizado.

Lo que se quiere hacer en este TFM es mejorar esta parte de la red privada. Se quiere hacer una prueba de concepto para la mejora de este sistema de autenticación. Se estudiarán los posibles protocolos de autenticación, los posibles programas candidatos para gestionarlo y la tecnología que se necesite para probar si es adecuada la solución.

Como este proyecto se basa en la red privada que tiene actualmente la empresa en la que trabajo. Cuando se decidan algunas opciones, como por ejemplo qué versión de servidor se utilizará. Se tendrá en cuenta el estado actual en la que la red privada está configurada. Porque si en un futuro se quiere hacer la implementación real, las modificaciones pertinentes que se hayan de hacer serán más sencillas si la tecnología utilizada es similar.

1.2 Objetivos del Trabajo

El objetivo de este TFM es mejorar la seguridad en base a la autenticación en la red privada de la empresa. Para ello se estudiará las posibles opciones que se utilizan en la actualidad, decidiendo por la mejor resultados nos pueda dar en un futuro.

Primero se explicarán los conceptos básicos que se utilizarán en todo el proyecto. Después se analizarán las posibles opciones, definiendo los pros y contras que tengan cada solución. Una vez escogido que se utilizará se diseñará el sistema que configuraremos. Los objetivos de este proyecto los podemos separar en los siguientes:

Objetivos de investigación

- Analizar y evaluar qué opciones hay para mejorar la autenticación en una red privada.
- Hacer una valoración del estado de arte en la autenticación en redes privadas.
- Investigar que tipo de protocolos hay actualmente.
- investigar qué programas nos pueden ser útiles para esta implementación.
- Seleccionar la mejor opción para nuestro caso de uso.

Objetivos de implementación:

- Configurar un prototipo para poder analizar y evaluar las posibles ventajas e inconvenientes que nos puede aportar la solución escogida.
- Tener en cuenta que el prototipo ha de ser lo más cercano al estado actual de la red privada.
- Configurar los diferentes dispositivos para el prototipo
- Configurar las diferentes tecnologías que se han seleccionado para hacer este prototipo.
- Comprobar que todo funciona correctamente y que la autorización en la red es correcta.
- Tener un testbed para poder hacer las pruebas necesarias de configuración y funcionalidad.
- Considerar como se puede implementar en un sistema real.

1.3 Enfoque y método seguido

Este TFM entraría en el tipo de case study, como explica P.Cristina en su artículo "*El método de estudio de caso*" [5], es un método de investigación que estudia casos concretos. Se quiere evaluar la posibilidad de utilizar nuevas herramientas, técnicas y métodos existentes para resolver en nuestro caso el problema de seguridad que puede tener una red privada. En nuestro caso se quiere mejorar el sistema de autenticación que se está utilizando en la red privada de la empresa que trabajo actualmente.

El proyecto se separará en tres partes. La primera donde se hará un estudio del arte de qué sistemas y tecnología se utiliza actualmente. En esta se seleccionará la que mejor vaya para nuestro caso de uso.

En la segunda se empezará a configurar los diferentes actores. Lo primero será crear un escenario en el que hacer el prototipo.

Una vez esté todo configurado y funcione correctamente pasamos a la tercera parte. Esta última consistirá en comprobar que todo esté funcionando como debería comprobando que los diferentes componentes se pueden autenticar correctamente.

Por último si se considera que este prototipo es lo que se necesita se pasará a un entorno real. Para ello se hará un pequeño planing de cómo se podría hacer este proceso para que fuera ágil y los usuarios del sistema no tuvieran problemas en la etapa de esta mejora.

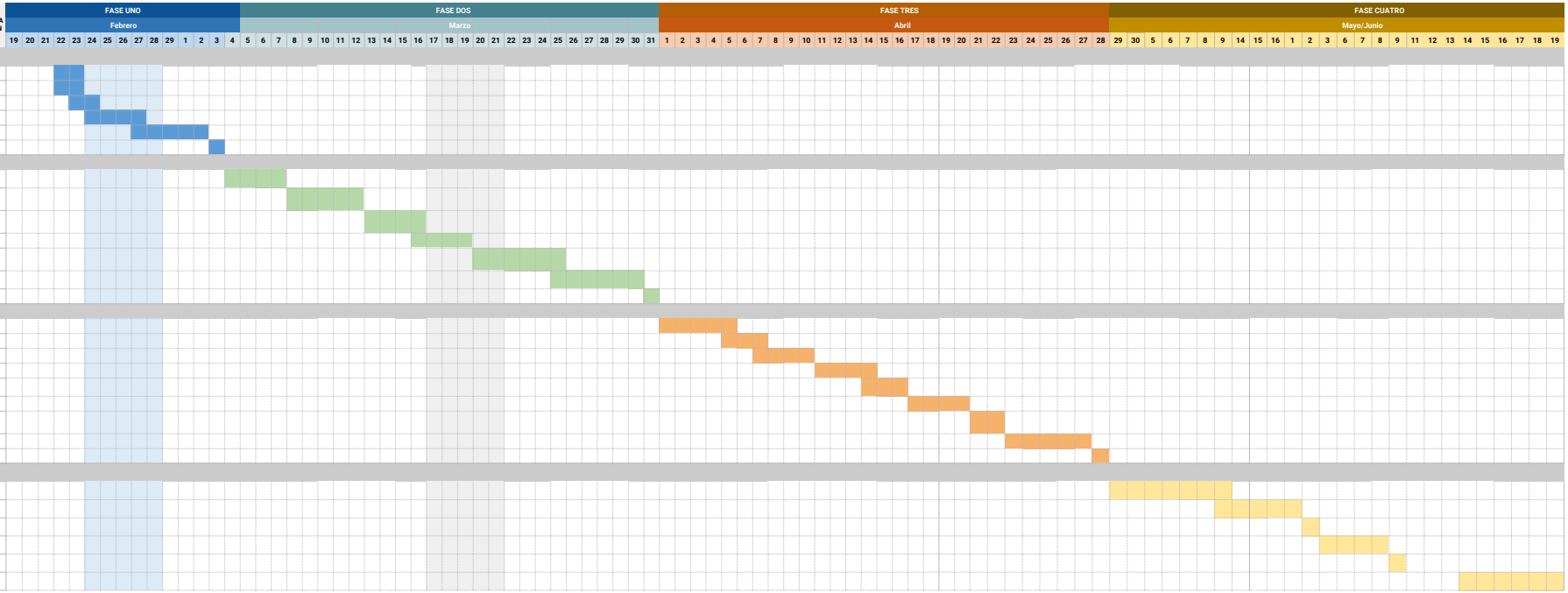
Con esto ya tendríamos que enfoque y método seguiremos. En el siguiente apartado se hará la planificación que se seguirá. Se utilizará el método agile junto con un gráfico de Gantt para planificar mejor el proceso. El método agile consiste en separar los objetivos del proyecto en partes diferentes que se entregan en plazos cortos, dando una mayor representación de cómo va el proceso. En el caso que no se cumplan los plazos descritos, se debe buscar otra estrategia que ayude a mejorar la productividad. En nuestro caso se han separado los hitos en las entregas que hay que realizar. En el supuesto que este método no sea el adecuado se buscará una solución que nos ayude a superar los objetivos del proyecto.

1.4 Planificación del Trabajo

Cod	Tarea	Inicio	Fin	Duración
1	**Plan de trabajo**			
1.1	Definir problema	22/02/2020	23/02/2020	2
1.2	Definir objetivos	22/02/2020	23/02/2020	2
1.3	Definir metodología	23/02/2020	24/02/2020	2
1.4	Planificación del trabajo	24/02/2020	27/02/2020	3
1.5	Estado del arte	27/02/2020	01/03/2020	4
1.6	**Entrega del plan de trabajo**	**03/03/2020**	**03/03/2020**	**Hito**
2	**Análisis y diseño del proyecto**			
2.1	Definición de conceptos	04/03/2020	07/03/2020	4
2.2	Investigación sobre protocolos de autenticación	08/03/2020	12/03/2020	5
2.3	Investigación de posibles programas de gestión de usuarios	13/03/2020	16/03/2020	4
2.4	Diseño del prototipo	16/03/2020	19/03/2020	4
2.5	Recopilación de la información obtenida	21/03/2020	25/03/2020	5
2.6	Redacción de la PEC	25/03/2020	30/03/2020	5
2.7	**Entrega de la PEC**	**31/03/2020**	**31/03/2020**	**Hito**
3	**Implementación**			
3.1	Instalación de sistemas operativos	01/04/2020	05/04/2020	5
3.2	Configuración del switch	05/04/2020	07/04/2020	3
3.3	Instalación de packetFence	07/04/2020	10/04/2020	3
3.4	Configuración de PacketFence	11/04/2020	14/04/2020	4
3.5	Instalación de Windows Server	14/04/2020	16/04/2020	3

3.6	Configuración Windows server	17/04/2020	20/04/2020	4
3.7	Recopilación de la información obtenida	21/04/2020	22/04/2020	2
3.8	Redacción de la PEC	23/04/2020	27/04/2020	5
3.9	**Entrega de la PEC**	**28/04/2020**	**28/04/2020**	**Hito**
4	**Presentación y defensa del TFM**			
4.1	Revisión de la información redactada	29/04/2020	09/05/2020	11
4.2	Redacción de las partes finales	09/05/2020	16/05/2020	8
4.3	**Entrega Memoria Final**	**02/06/2020**	**02/06/2020**	**1**
4.4	Preparación video	03/06/2020	08/06/2020	6
4.5	**Entrega Video**	**09/06/2020**	**09/06/2020**	**1**
4.6	**Defensa del TFM**	**15/06/2020**	**19/06/2020**	**5**

NÚMERO EDT	TÍTULO DE LA TAREA	FECHA DE INICIO	FECHA DE ENTREGA	DURACIÓN
1	**Plan de proyecto**			
1.1	Definir problema	22/02/20	23/02/20	1
1.2	Definir objetivos	22/02/20	23/02/20	1
1.3	Definir metodología	23/02/20	24/02/20	1
1.4	Planificación del trabajo	24/02/20	27/02/20	3
1.5	Estado del arte	27/02/20	01/03/20	4
1.6	Entrega del plan de trabajo	03/03/20	03/03/20	0
2	**Análisis y diseño del proyecto**			
2.1	Definición de conceptos	04/03/20	07/03/20	4
2.2	Investigación sobre protocolos de autenticación	08/03/20	12/03/20	3
2.3	Investigación de posibles programas de gestión de usuarios	13/03/20	16/03/20	4
2.4	Diseño del prototipo	16/03/20	19/03/20	3
2.5	Recopilación de la información obtenida	21/03/20	25/03/20	4
2.6	Redacción de la PEC	25/03/20	30/03/20	5
2.7	Entrega de la PEC	31/03/20	31/03/20	0
3	**Implementación**			
3.1	Instalación de sistemas operativos	01/04/20	05/04/20	4
3.2	Configuración del switch	05/04/20	07/04/20	2
3.3	Instalación de packetFence	07/04/20	10/04/20	3
3.4	Configuración de PacketFence	11/04/20	14/04/20	3
3.5	Instalación de Windows Server	14/04/20	16/04/20	2
3.6	Configuración Windows server	17/04/20	20/04/20	3
3.7	Recopilación de la información obtenida	21/04/20	22/04/20	1
3.8	Redacción de la PEC	23/04/20	27/04/20	4
3.9	Entrega de la PEC	28/04/20	28/04/20	0
4	**Presentación y defensa del TFM**			
4.1	Revisión de la información redactada	29/04/20	09/05/20	10
4.2	Redacción de las partes finales	09/05/20	30/05/20	21
4.3	Entrega Memoria Final	02/06/20	02/06/20	0
4.4	Preparación video	03/06/20	08/06/20	5
4.5	Entrega Video	09/06/20	09/06/20	0
4.6	Defensa del TFM	15/06/20	19/06/20	4



1.5 Estado del arte

Primero de todo se hará un estudio del estado del arte en sistemas de autenticación en redes privadas. Se analizará qué sistemas son los más adecuados para el caso que se a planteado estudiar en este proyecto. En segundo lugar se llevará a cabo un prototipo para este caso de estudio.

El paper de José R. Arana, Leandro A. Villa y Oscar Polanco[6] hace un estudio de cómo implementar un sistema de control de acceso a una red. En este artículo se analizan diferentes protocolos que juntos crean una solución que nos podrías servir. Las diferentes herramientas utilizadas son:

- *RADIUS* [4] es un protocolo de autenticación y autorización para aplicaciones de acceso a red. Se encarga de dar respuesta a los clientes que intentan acceder a una red.

- *IEEE 802.1X* [8] es una norma del IEEE que define el acceso de control por puertos. Nos da la capacidad de configurar los puertos de una red LAN para que solo se puedan autenticar si coincide con unas determinados condiciones.

- *EAP-TLS Authentication Protocol* [9] Es un protocolo de autenticación que proporciona autenticación mutua, negociación de cifrado protegido e intercambio de claves entre dos puntos.

- *PEAP* [10] Es un protocolo de autenticación que mejora EAP utilizando un canal TLS. Esto nos permite tener comunicaciones cifradas, autenticadas, integridad con autenticación mutua de punto a punto.

- *EAP-TTLS* [11] Utiliza el protocolo EAP que encapsula una sesión TLS, que consiste en una fase de reconocimiento y otra fase de envío de datos.

Junto con la descripción de estos términos [6], el artículo nos presenta que dependiendo de qué grado de seguridad o que objetivos tenemos debemos escoger una u otra opción.

En el artículo de H.Nunoo-Mensah, E.Kofi Akowuah i K.Boateng [7] hacen una revisión de las técnicas de control de acceso a redes educativas comparando los diferentes programas para hacer control de acceso de redes que son de código abierto. Entre ellos;

- *OpenNac* [12] es un programa de código abierto de acceso de control de red LAN/WAN. Nos permite autenticar, autorizar y basado en políticas para acceder a la red. También nos da monitorización en tiempo real de los usuarios y dispositivos que hay en la red.

- *PacketFence* [3] es una solución de control de acceso de red (NAC) de código abierto. Con un portal para la gestión de usuarios y configuración, centralizado en la gestión por cable o Wireless. Soporta 802.1X, aislamiento de capa 2 de posibles dispositivos problemáticos. Sirve tanto para grandes o pequeñas redes.

- *FreeNac* [13] nos proporciona un control de acceso para LAN. También nos da la opción de tener control de puertos y del estado de los cables. Los usuarios se pueden identificar en la red vía MAC o con certificados y MAC (802.1X). En la capa de comunicación se utiliza FreeRadius.

Estos serían los principales programas que se comparan en el artículo. Las diferencias características que comparan son análisis de datos, autenticación de dispositivos, control de ancho de banda, soporte con diferentes vendedores, soporte con redes LAN o WAN, integración del programa con la infraestructura, interfaz del administrador, reporte de incidencias y si hay soporte con el equipo que desarrolla estas soluciones. Con esto podemos tener una idea de cuales serían opciones ideales para nuestro caso de uso. Este documento llega a la conclusión que las tres opciones tienen buenas características que tener en cuenta. Pero que PacketFence es el más completo de los tres ya que tiene análisis de dispositivos y monitorización de ancho de banda.

Con esto tenemos un resumen de el estado en la que están las tecnologías que se utilizarán en este proyecto. Qué protocolos tenemos la opción de utilizar, que beneficios nos aportan unos u otros. Como en el segundo que nos analiza los diferentes programas que se pueden implementar para nuestro caso de uso, en el caso que se quiera utilizar programas *open-source*. En las siguientes fases del proyecto se llevará un análisis mayor de las posibles soluciones.

2. Análisis y diseño del proyecto

En este capítulo nos centraremos en la definición de algunos conceptos básicos con los que se trabajarán en este proyecto. También, partiendo del estado del arte actual, se estudiarán las diferentes soluciones para este caso de estudio de autenticación en redes privadas. Elegir qué solución es la más adecuada para nuestro caso y diseñar una estructura para poner en práctica esta solución

2.1 Definiciones de conceptos

2.1.1 Redes

Lo primero que vamos a definir es el concepto de red. Según la rae la definición basada en informática es "*Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información.*" [14] Como vemos no especifica cuántas computadoras han de ser las que conforman esta red. Por ello dependiendo de en qué nos basamos tienen diferentes clasificaciones.

La primera separación es entre si una red es pública o privada. Se dice que es pública cuando es la que nos proporciona un servicio a cambio del pago de una cuota. Sería el caso de las redes que tenemos en casa y que contratamos a alguna compañía de telefonía para que nos de conexión a internet.

Por otro lado tenemos la red privada que es aquella que es administrada por una organización en particular. A esta red solo tiene acceso los usuarios que el administrador les a autorizado. Estas son el tipo de redes que se configuran en las empresas para que los empleados de esta puedan comunicarse entre ellos y compartir información sin que salga al exterior. Cuando este tipo de redes está correctamente configurada da un grado más de seguridad para salvaguardar información de la empresa administrada. El administrador suele ser el departamento de *IT (Information Technology)* que son los encargados del servicio técnico. En algunos casos es posible contratar a una empresa externa para que la administre, pero es más común encontrar a alguien de dentro que sea encargue de esta tarea.

Otra división que es común es dependiendo del tamaño de la red. Este tipo se separan en estos principalmente[15]:

- *Personal Area Network (PAN)*, este tipo de redes conocidas como redes domésticas o personales tienen un alcance pequeño. Son las que cualquier persona tiene en su casa particular configuradas, y no tienen una gran complejidad.

- *Local Area Network (LAN),* Estas redes son las más comunes en empresas y son más complejas de configurar. Su alcance puede llegar a 1Km de distancia. Por ello son comunes que se utilice para administrar una sede de una empresa.

- *Metropolitan Area Network (MAN)* Son redes más extensas, a veces son conjuntos de LANs de una empresa que tiene varias sedes en una misma ciudad o cercanas entre sí.

- *Wide Area Network (WAN)* Son las más extensas siendo un conjunto de las dos anteriores. Pueden llegar a miles de kilómetros. La más conocida es la red pública de Internet, cuyo nombre procede de Inter Networking, o interconexión de redes.

También podríamos considerar la *VLAN* como otro tipo de red. Este tipo es normalmente una separación virtual de una LAN o MAN. Se crean para poder separar las redes privadas por ejemplo dependiendo del departamento. Así es más fácil organizar los servicios que puede ofrecer la red. En nuestro caso simularemos una red LAN separadas en VLAN que irán por departamentos. Así nuestro caso de uso se podrá basar en un caso real de una red privada separada por VLAN.

2.1.2 Autenticación y Autorización

Otro concepto que es importante tener claro es la diferencia entre autenticación y autorización. La definición de cada concepto es:

- Autenticación[16]: “Procedimiento de comprobación de la identidad de un usuario de un recurso informático”

- Autorización[17]: “Acto de una autoridad por el cual se permite a alguien una actuación en otro caso prohibida.”

Como vemos hay una diferencia entre un concepto y otro. El primero se produce cuando vamos a hacer entrar en un servicio web y tenemos que autenticarnos para demostrar que somos quien decimos ser. Para ello normalmente tenemos un usuario y contraseña que nos identifican como usuarios. En cambio autorización es aquello que cuando entramos en esa web, dependendiendo de qué rol nos hayan asignado tendremos permisos para llevar a cabo acciones determinadas. Es importante tener claros estos conceptos para poder buscar mejor que soluciones son las que necesitamos para el caso de uso que se va a estudiar en este proyecto.

Para poder demostrar que el usuario es quien dice ser cuando se autentica, se utiliza el término verificación de la identidad. En el cual hay muchas técnicas y formas de probarlo. Pero no todas tienen el mismo nivel de seguridad y

verificabilidad [19]. Los cinco factores que se utilizan para identificar la seguridad de esta autenticación son los siguientes [18]:

- Factor del conocimiento (¿Que sabes?): esta categoría es lo que el usuario utiliza para identificarse basándose en algo que sabe. Por ejemplo, su nombre de usuario, una contraseña, un PIN o la respuesta a una pregunta en concreto.

- Factor de posesión (¿Que tienes?): Este se basa en materiales que el usuario posee para identificarte, como por ejemplo un dispositivo móvil.

- Factores de inherencia (¿Que eres?): Consiste en elementos que son integrados en el usuario que se identifica. El ejemplo más claro es una autenticación biométrica porque es algo que todos tenemos.

- Factores de Lugar (¿Donde estás?): Dependiendo de en qué lugar te detecte el servicio puede dar un dato más para saber si eres tú. Por ejemplo en el caso de lo bancos, a veces, si no comunicas que vas hacer un viaje a otro país y utilizas la tarjeta de credito te la pueden llevar a cancelar por seguridad de que no te hayan robado la cuenta.

- Factor de tiempo (¿Cuando te autorizas?) La hora en la que intentas acceder al servicio puede dar datos si eres tú quien está intentando autenticarse. Por ejemplo si un empleado intenta acceder un sábado noche a un servicio de la empresa, sin necesidad de que haya una alerta es posible que sea un intento de suplantación.

Dependiendo del grado de seguridad que queramos en nuestro servicio podemos poner más de un factor de autenticación. Por ejemplo podemos poner el usuario y contraseña del empleado que sería algo que sabes. Como segundo factor un certificado instalado en su máquina que sería algo que tiene. Así tendríamos una autenticación de doble factor. También se podría considerar el factor de lugar, porque al ser una red privada con cable se necesita estar conectada a ella. Teniendo en cuenta que si alguien accede vía VPN a de justificar el lugar donde la está utilizando para que no de un falso negativo. Como se ha explicado en el ejemplo de el factor de tiempo también se podría tener en cuenta, pero daría mayor dificultad a la hora de configurar el sistema.

En el campo de la informática hay muchas herramientas que nos ayudan a gestionar la autenticación y la autorización en sistemas. Podemos contar con estándares, protocolos, programas entre otras cosas.

2.1.3 IEEE 802.1x

Estándar IEEE [20] para redes locales y metropolitanas basado en control de acceso por puertos. Regulan el acceso a la red protegiendo contra la transmisión y recepción por partes no autenticadas o no autorizadas, así evita que interrumpan en la conexión, se robe información o pérdida de datos. Se creó para redes cableadas pero actualmente es más utilizado en redes inalámbricas. Crea una capa entre la capa de acceso y los procesos de autenticación, donde se traduce los paquetes a un formato que pueda entender el sistema de autenticación que utilice la red. Para la autenticación se utiliza el protocolo EAP y para el proceso de autenticación en la red PAE (port access entity). Este proceso tiene tres componentes básicos

- *Supplicant*: El cliente que solicita el acceso a la red.
- Autenticador: Dispositivo entre el suplicante y el servidor de autenticación.
- Servidor de autenticación: El servidor que realiza la autenticación.

Como vemos en la figura 1 el *supplicant* se comunica con el autenticador con un protocolo EAPOL. En cambio el autenticador se comunica con el servidor de autenticación con un mensaje encapsulado EAP, normalmente se utiliza RADIUS como servidor y protocolo. Este sería el esquema principal de las comunicaciones que se producen en este estándar. Al utilizar protocolos EAP tenemos una variedad para que se escoja el que mejor aplique al sistema que se va a administrar.

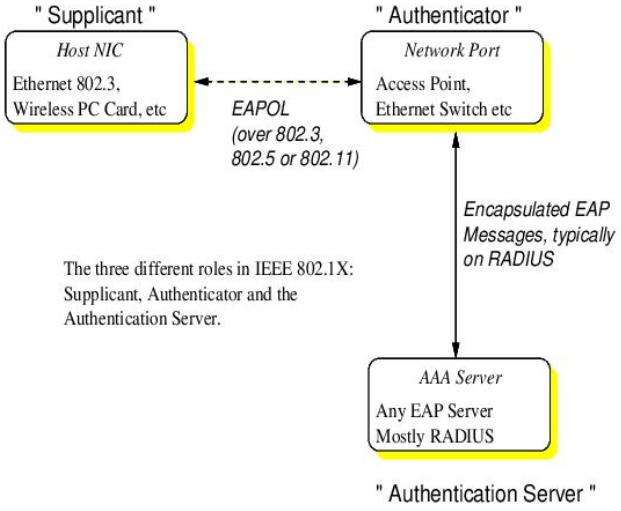


Figura 1. Esquema IEEE 802.1X [21]

2.1.4 EAP

Extensible Authentication Protocol (EAP) [22] es un protocolo de autenticación que soporta diferentes métodos. Normalmente corre directamente por la capa de enlace como PPP o IEEE 802, sin la necesidad de IP. Una de las ventajas de EAP es su flexibilidad. Se utiliza para escoger un mecanismo de autenticación, normalmente se selecciona después de que haya llegado la petición de autenticación, así tiene detalles de que puede soportar el cliente y seleccionar la mejor opción.

Los pasos que sigue este protocolo son los siguientes. Primero el autenticador envía una petición con un campo tipo específico al usuario para autenticarlo. Este le responde con el mismo campo si es el correcto. Cuando se decide qué protocolo se va a utilizar acaba la transmisión. En el caso que la transmisión sea exitosa se envía un paquete de "*EAP Success"*, pero en caso contrario ha de enviar un "*EAP Failure"* para que el cliente sepa que no se ha podido autenticar.

Dependiendo de las necesidades de la red que se está configurando se puede escoger un protocolo u otro. Las posibles opcione son EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST, EAP-LEAP.

2.1.4.1 EAP-MD5 [23]

El servidor hace una autenticación con usuario y contraseña cifrado con el algoritmo MD5. Solo se comprueba si estos son correctos sin comprobar nada más y solo se autentica el cliente no el servidor así que es unidireccional. Tampoco permite la administración y generación dinámica de claves. Como vemos este método no es recomendado, ya que solo sirve para autenticar al usuario y MD5 es posible derivar la contraseña.

2.1.4.2 EAP-TLS[9]

EAP-Transport Layer Security incluye soporte para autenticación basada en certificados y derivación de claves, utilizando la negociación de cifrado protegido, autenticación mutua y capacidades de gestión de claves del protocolo TLS. Servidor y cliente deben de instalar un certificado común para poder hacer la autenticación entre ellos. En este intercambio se negocia la clave de sesión de cifrado. Con la gestión de certificados le da a EAP-TLS mayor seguridad, pero tiene mayor coste de administración. Ya que al tener que gestionar los certificados en una red privada con muchos usuarios conlleva a una mayor gestión.

2.1.4.3 EAP-TTLS [11]

Encapsula en una sesión TLS (*Transport Layer Security)* que consiste en una fase de *handshake* y una fase de transmisión de datos. En la primera fase el servidor se autentica ante el usuario utilizando TLS, creando un túnel seguro para la segunda fase. Una vez es seguro, el usuario es autenticado ante el servidor con un mecanismo aleatorio de autenticación que va encapsulado en el túnel seguro. Esto hace que solo el servidor necesite un certificado, haciendo que la gestión de estos sea más fácil de utilizar. La autenticación se hace vía constraseña pero esta es cifrada por el túnel establecido en la primera fase con el certificado del servidor.

2.1.4.4 EAP-FAST [24]

Flexible Authentication via Secure Tunneling Extensible Authentication Protocol utiliza PAC (*Protected Access Credential)* para establecer un túnel TLS en vez de utilizar certificados digitales. Utilizando PACs con gran entropía que pueden ser generadas manualmente o dinámicamente. No es obligatorio que el servidor utilice certificados, pero es posible su configuración. Las PACs son entregadas de manera manual o automáticamente.

2.1.4.5 EAP-PEAP [10]

Protected Extensible Authentication Protocol tiene dos fases como EAP-TTLS. Pero dentro del túnel puede hacer otros métodos como enlace criptográfico de métodos externos e internos. Solo soporta protocolos de EAP dentro del túnel esta podría ser una de las diferencias entre PEAP y EAP-TTLS. También solo el servidor es necesario que tenga un certificado instalado.

2.1.4.6 EAP-LEAP [25]

Es un tipo de autenticación EAP que se utiliza en redes WLAN. Los datos se cifran con claves WEP generadas dinámicamente y admite autenticación mutua del cliente y servidor. Se ha probado que es posible atacar a las claves WEP y saltarse esa parte de la seguridad. Así que hay otros métodos que son más seguros que este. También al ser utilizados en redes WLAN y nuestro caso de uso solo se hará con redes LAN no será una opción.

2.1.4.7 MAB [26]

Este protocolo no pertenece a EAP. Se utiliza cuando tienes una red configurada con el estándar 802.1X pero algún dispositivo como puede ser una impresora o un teléfono de voz ip, que no soportan protocolos complicados, se han de configurar que MAB. Este autentica a los usuarios con la MAC que tienen asignada. Normalmente estos dispositivos tienen una VLAN dedicada a ellos por si alguien es capaz de hacer una suplantación, que no puedan acceder a gran parte de la información al ser una red aislada.

2.1.4.8 Comparación

Después de haber presentado todas las variables que nos ofrece EAP vamos a hacer una comparación y escoger el protocolo que se utilizará en este caso de uso. Para ello vamos a hacer una tabla donde se recojan las principales e importantes características que tienen que tener.

Tipos de EAP en ---------- Ventajas/funciones	MD5	TLS	TTLS	PEAP	FAST	LEAP
Se necesita certificado de cliente	No	Sí	No	No	No (PAC)	No
Se necesita un certificado de servidor	No	Sí	Sí	Sí	No (PAC)	No
Atributos de autenticación	Unidireccional	Mutua	Mutua	Mutua	Mutua	Mutua
En que se especializa	MD5	Seguridad de nivel de transporte	Seguridad de nivel de transporte por túneles	Seguridad de nivel de transporte protegido	Autenticación flexible mediante tunelización segura	Protocolo ligero de autenticación ampliable

Tabla 1. Tabla comparativa tipos EAP

Con esto podemos descartar a MD5 y LEAP por ser unos protocolo que no son lo suficientemente seguros y no utilizan certificados para mejorar la seguridad. Por otro lado tenemos FAST que tampoco utiliza certificados y utiliza PAC que también se han de gestionar.

Entonces nos quedarían TLS, TTLS y PEAP. Como hemos comprobado anteriormente TTLS y PEAP son muy parecidos, la única diferencia destacable es que PEAP solo soporta protocolos EAP en sus transmisiones. Por ello este quedaría descartado ya que queremos utilizar también el protocolo MAB para dispositivos que no pueden utilizar EAP.

Por último tenemos TTLS y TLS. La gran diferencia es que TLS el usuario necesita igual que el servidor un certificado y esto puede complicar la administración de ellos, pero dan un extra de seguridad que si solo nos autenticamos vía usuario y contraseña como es el caso de TTLS. Como este caso de uso se basa en una empresa pequeña con pocos usuarios que gestionar, se ha decidido utilizar el protocolo TLS para la prueba que se hará. En el caso que en un futuro se vea que es más complicado de gestionar de lo que se ha previsto, es posible que se haga otro caso de estudio para pasar a otras posibles soluciones.

2.1.5 RADIUS

RADIUS (Remote Authentication Dial-In User Server) es un protocolo de autenticación y autorización basado en cliente/servidor. Cuando el cliente quiere autenticarse en una red, envía su usuario y contraseña que llega a un NAS (*Network Access Server)* sobre el protocolo PPP, quien envía esta petición al servidor RADIUS con el protocolo RADIUS. Este comprueba la información y mediante el esquema del protocolo EAP le asigna una IP.

El NAS que opera como cliente de RADIUS suele ser el switch al que se conecta el usuario que quiere ingresar en la red privada. Este se encarga de pasar la información al servidor RADIUS, y actuar dependiendo de la respuesta que le haya llegado.

Los servidores RADIUS se encarga de recibir petición del usuario, autenticar al usuario y retornar la información de la configuración que sea necesaria para que el cliente RADIUS se lo pueda entregar al usuario. Otro de los roles del servidor RADIUS es que puede actuar como un proxy del cliente para otros servidores RADIUS o otros servidores de autenticación.

2.1.6 NAC

Network Access Control ofrece poder administrar dispositivos con gestión de identidad aplicando políticas de gestión. Es el encargado de cómo utilizar la red, dando visibilidad y herramientas para facilitar la gestión de esta para reducir el impacto de las intrusiones. Al tener la capacidad de gestionar el acceso del usuario, puede decidir dependiendo de qué tipo de usuario seas a qué recursos puedes acceder. Por ejemplo en las empresas se puede separar dependiendo de a qué departamento pertenezcas tener unos permisos y otros.

Ahora se definirán algunas opciones de opensource que podemos utilizar. Se ha decidido utilizar este tipo de programas para abaratar posibles costes. Los casos que se han estudiado no hay que comprarlos para su uso. Las tres opciones que se analizarán son OpenNac, PacketFence y FreeNac. Se han escogido estas tres porque son las más utilizadas y tienen suficiente documentación para llevar a cabo la instalación si fuera necesario.

2.1.6.1 OpenNac

Es un controlador de acceso de red de *open source* que da acceso a redes. El programa se basa en conocidos estándares como FreeRadius, 802.1x, AD, ldap,. Funciona con diferentes sistemas como Windows, Linux, etc. Tiene varias funcionalidades como gestión de dispositivos, detección de intrusos y sistema de autenticación. Permite la autenticación, la autorización y el acceso a la red basado en políticas. La arquitectura de este programa está basado en plugins esto nos permite que si hay una nueva funcionalidad es fácil de instalarla y configurarla. Por último nos permite tener un *backup* de la configuración y monitorizar la red entre otras cosas.

2.1.5.2 PacketFence

Es una solución NAC que es compatible con muchas soluciones, confiable y de código abierto. Una de sus características es que incluye un portal fácil de usar para la administración de dispositivos en una red por cable o inalámbrica. Soporta 802.1X, MAB y aislamiento de capa 2. Es compatible tanto para redes pequeñas como de gran tamaño. Se puede configurar el sistema en modo online o offline, dependiendo de las necesidades del cliente. Podemos monitorizar los dispositivos que hay en la red y mirar cuanto gastan de ancho de banda. Esto nos permite tener una mejor imagen de si está bien configurada o se podría mejorar su calidad. Es posible gestionar las VLAN dependiendo qué rol tenga el usuario que se está autenticando. Esto nos permite que si un usuario sin rol entra puede ser enviado a una red de cuarentena o con solo acceso a internet.

2.1.6.3 FreeNac

Es una solución con GPL *OpenSource* para control de acceso de LAN y administración dinámica de VLAN. Nos ayuda con la asignación de VLAN, control de acceso a toda clase de dispositivos como servidores, ordenadores, impresoras, teléfonos de voz IP entre otros. Tiene compatibilidad con autenticación con certificados o MAC. También es compatible con FreeRadius, 802.1x y OpenVMPS para modos VMPS. FreeNAC tiene redundancia y carga compartida para alta disponibilidad como características adicionales, proporciona informes flexibles, inventario en vivo de dispositivos de extremo a extremo en la red.

2.1.6.4 Comparación

Con una tabla se pondrán las características más importantes de cada uno para poder elegir cual es el que nos conviene más para nuestro caso de uso.

Carácteristicas	OpenNac	PacketFence	FreeNac
Análisis de la red	Sí	Sí	Sí
Autenticación de dispositivos	Sí	Sí	Sí
Administrador de ancho de banda	No	Sí	No
Compatible con otras soluciones	Sí	Sí	Sí
Soporte para redes con cable e inalámbricas	Sí	Sí	Sí
Soporte técnico	Activo	Activo	No muy activo
Interfaz de Administrador	Interfaz Web	Interfaz Web	Interfaz Gráfica
Informes	Sí	Sí	Sí

Tabla 2. Tabla comparativa NAC

Como vemos los tres casos nos ofrecen muchas cualidades que son básicas a la hora de gestionar una red. Si que hay algunas características como por ejemplo si el soporte técnico está activo o no. En el caso de tener algún problema con la solución necesitamos que tengan respuesta lo más rápido posible. Por ello descartamos la solución FreeNac porque el soporte no está muy activo y esto puede perjudicarnos en un futuro.

En el caso de elegir OpenNac o FreeRadius no hay mucha diferencia. En la tabla podemos ver que la única diferencia que tienen es que OpenNac no soporta la administración de ancho de banda. Esta característica nos puede ser útil a la hora de administrar la red. Por ejemplo en el caso de la red para invitados, podemos bajar la capacidad y así poder dar más capacidad a nuestros empleados. Por otra parte investigando sobre manuales de instalación, PacketFence tiene mayor calidad de documentación. Dando un punto más para elegir esta solución.

En conclusión escogeremos PacketFence porque es la solución más completa de las tres, estando actualizada al día. Teniendo mayor capacidad para la administración de servicios y usuarios de una red privada.

2.2 Comparación sistemas de autenticación

Después de explicar en los conceptos principales que tipo de protocolos, programas o estándares que se van a utilizar. En este apartado se creará una tabla donde se resumirá que nos aporta cada uno de los componentes. Que en el conjunto con cada una de sus características podemos crear una solución que nos ayude a resolver este caso de uso.

EAP	**RADIUS**	**NAC**	**802.1x**
Protocolo de autenticación	Protocolo de autenticación y autorización	Programa de control de acceso	Estándar IEEE basado en control de acceso por puertos
LAN or WLAN	LAN or WLAN	LAN or WLAN	LAN or WLAN
Se comunica con RADIUS	Es comunica con EAP, NAC y 802.1x	Se comunica con RADIUS, MAB y EAP	Utiliza NAC, RADIUS y EAP
Diferentes métodos de autenticación	Diferentes métodos de autenticación	Diferentes tipos de NAC	Depende de cómo se configuren sus
-	Asignamiento de roles automáticamente	Asignamiento de roles automáticamente	Asignamiento de roles automáticamente
Configuración con certificados o sin	Configuración con certificados o sin	Configuración con certificados o sin	Configuración Con certificados o sin

Tabla 3. Comparación de componentes

Con esta tabla podemos ver que cada actor nos da una solución diferente y que juntas crea una solución estable. Por ejemplo EAP es un protocolo autenticación, pero no controla la autorización a los servicios. Esto puede ser controlado por RADIUS o NAC, que tienen la características para hacerlo. Una de las mejores características es que pueden hablar entre sí, esto nos permite configurar una red que tenga varias capas de control. En el caso de 802.1x hace un control de puertos, esto nos permite que dependiendo de cómo esté configurada la red, aunque un usuario que no esté autorizado quiera entrar por un puerto específico, si no está configurado no podrá. También contando con el apoyo de RADIUS y NAC que hacen esto sea más seguro. Por último destacar que en los cuatro casos se puede configurar un certificado para la autenticación y autorización del usuario que es el objetivo que queremos llegar con este caso de uso.

3. Prueba de concepto

En este apartado se explicará los pasos importantes que se han llevado a cabo para poder hacer una prueba de concepto con las conclusiones que se han presentado en el apartado anterior. Primero se presentará qué arquitectura se ha propuesto y el por qué. En segundo lugar una pequeña muestra de los pasos más importantes a la hora de la instalación o algunos aspectos determinantes. Por último se presentará un análisis de la prueba de concepto, los pros y contras que nos proporciona esta solución planteada.

3.1 Componentes

A continuación se hará un breve resumen del material que se utilizará para la prueba de concepto. Se separarán en dos subapartados dependiendo si son hardware o software. Con una breve explicación de sus características, el porque se a escogido.

3.1.1 Hardware

3.1.1.1 Switch

El switch escogido es un Cisco IOS C2960S con la versión 12.2(55)SE7 del software instalado para la configuración. Este switch nos permitirá hacer las conexiones físicas entre los servidores. Así se puede simular la red privada de la empresa con mayor precisión. Se ha escogido este tipo de switch porque soporta los sistemas que se quieren configurar.

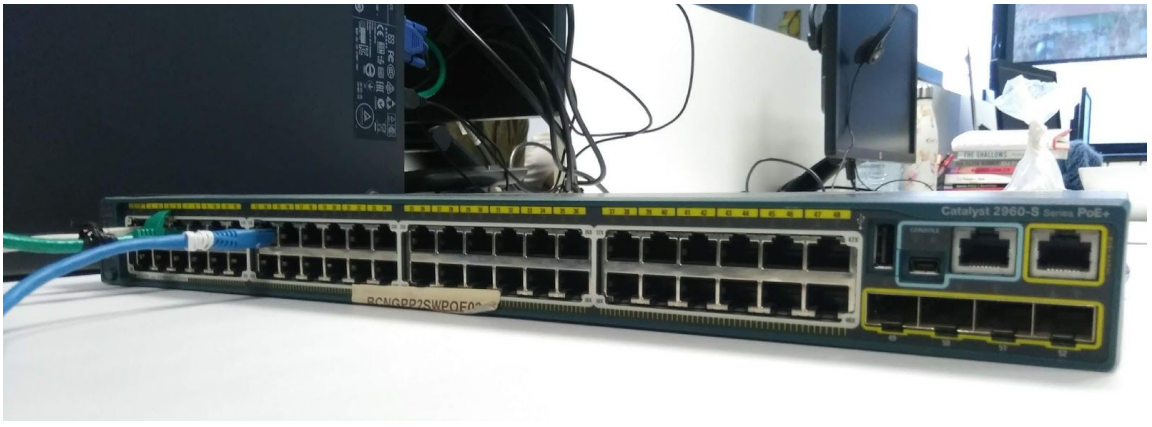


Figura 2. Switch Cisco IOS C2960S

3.1.1.2 Servidores

Los servidores que se han utilizado son dos. El primer servidor Lenovo ThinkCentre E73 tiene instalado de sistema operativo un Debian 9.9.0. Este es el que se ha escogido para hacer la instalación del PacketFence. El segundo servidor que tenemos es Lenovo ThinkCentre E73, instalado un “windows server 2012 R2”. Aquí es donde se ha configurado el Active Directory (AD).

Figura 3. Servidores Lenovo ThinkCentre E73

3.1.1.3 Ordenadores

Se han utilizado dos portátiles uno con Windows 10 y el otro con Ubuntu 18 como usuarios que quieren autenticarse en el sistema de prueba que hemos creado. El portátil de Windows 10 es un HP Probook 5330m con un i-core 3. El Ubuntu 18 es un Lenovo ThinkPad E530c con una memoria RAM de 16GiB y un i-core 5.

3.1.2 Software

3.1.2.1 Debian [27]

La distribución que se ha escogido es Debian. Entre las distribuciones de Linux es una de las más estabilidad y segura. Es ligero y rápido comparado con otras distribuciones haciendo que sea una opción usarlo. También es un sistema con mucha documentación dándonos más facilidad a la hora de configurarlo. La versión que se ha utilizada será la Strech que es la LTS actual.

3.1.2.2 Windows Server

Windows server es una distribución de windows específica para el uso de servidores. Se utiliza para la administración del sistema de autenticación y autorización de la red. Tiene algunas ventajas como que es fácil de administrar entre otras. Se ha escogido este tipo de servidor porque es el que actualmente se utiliza en la empresa, dando así una imagen más real si en un futuro se quiere hacer la implementación.

3.1.2.3 Active Directory

Como se ha descrito en el subapartado anterior la versión instalada es “windows server 2012 R2”, se escogió esta versión porque es la que actualmente está instalada en nuestra empresa. Así la prueba de concepto es más cercana a la realidad que tenemos actualmente. Una vez se pase a producción se actualizará la versión a una más actual.

3.1.2.4 PacketFence

La versión que se instala en el servidor Debian de PacketFence es 9.0.1. Para poder acceder al portal de packetfence y configurarlo, solo se necesita acceder vía un explorador que esté en la misma red a la que pertenece este servicio. Se configurarán como pueden acceder los dispositivos a la red. Dependiendo si tienen capacidad para soportar 802.1x o no. En el caso que no lo tengan como las impresoras, se registrará la MAC de estos dispositivos para que tengan la posibilidad de autenticarse vía MAB.

3.1.2.5 Protocolos de autenticación

El protocolo de autenticación que se ha escogido es EAP-TLS dentro de los posibles 802.1x que se han expuesto anteriormente. Este protocolo te da la posibilidad de utilizar certificados digitales para el proceso de autenticación, dando un grado más de protección a la red interna de la empresa. Este protocolo también da la posibilidad de utilizarlo en un escenario con redes WLAN, esto nos permitiría que si en un futuro se quiere poner este tipo de protocolos en este tipo de redes sería viable. Se generará un certificado por cada usuario que pueda autenticarse vía 802.1x. Así sólo los usuarios a los que se les haya proporcionado estos certificados podrán autenticarse en la red.

Los certificados se generarán por usuario. Así cada usuario tendrá su propio certificado para poder autenticarse en la red privada. En el caso que nuevos usuarios sean creados se tendrá que generar un certificado nuevo. Instalarlo en la máquina que vaya a utilizar el usuario, para que en el momento que vaya a autenticarse contra el servidor pueda utilizarlo.

Por otra parte a los dispositivos que no soporta 802.1x como por ejemplo los teléfonos con Voz IP o las impresoras. En estos se configurará MAB, un protocolo de autenticación que utiliza las direcciones MAC de los dispositivos. Estos dispositivos se encontrarán en una VLAN restringida solo para los servicios que puedan necesitar. En el caso que alguien pueda conseguir acceso mediante spoofing de la MAC de estos dispositivos que no afecte a la seguridad de la red. También se ha de comentar que el protocolo RADIUS encargado de la gestión del switch también tiene la capacidad de ser un protocolo de autenticación y autorización.

3.2 Arquitectura

Para esta prueba de concepto se ha diseñado un sistema simple compuesto por dos servidores(PacketFence y Active Directory), un switch y un portátil que actúa de usuario que quiere autenticarse en esta red.

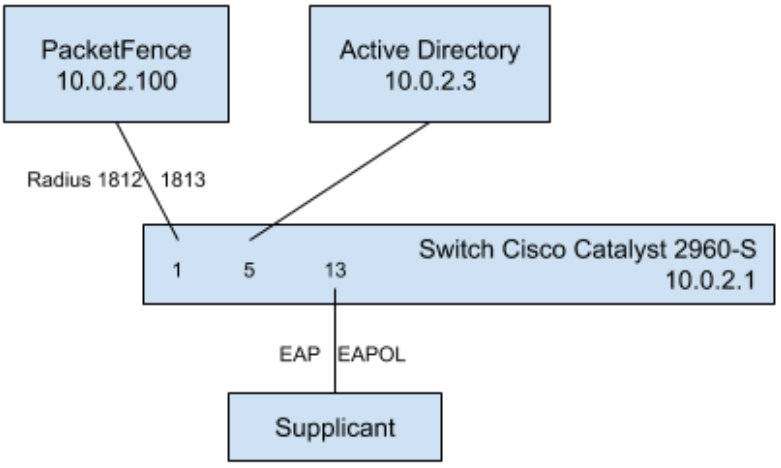


Figura 4. Simulación red privada

Como vemos en la figura 4 la red que se ha configurado es 10.0.2.0. Al switch se le a asignado la ip 10.0.2.1. Al AD la 10.0.2.3 con el puerto 5 y por último al PacketFence en la ip 10.0.2.100 con el puerto 1.

Para el caso de los usuarios se ha configurado solo el puerto 13 para hacer la pruebas. Este puerto está configurado con los dos protocolos explicados anteriormente EAP-TLS y MAB. Lo que se consigue es que cualquier dispositivo que se conecte a este puerto, packetfence primero pedirá que se autentique vía EAP-TLS, en el caso que no sea posible porque no lo soporte pasará a MAB. Por ello notaremos que la autenticación por MAC es un poco más lenta que por certificados. Ya que Packetfence primero lo intenta con la que hemos configurado como primera opción.

Entre la conexión PacketFence y el switch se utiliza el protocolo de autenticación RADIUS. Que hace de enlace entre los dos puntos, para poder llevar la petición del usuario que quiere autenticarse. Por otro lado tenemos el protocolo EAP encapsulado en EAPOL, que es el encargado de llevar la petición del usuario entre este y el switch. Todo este conjunto de herramientas permite que en una red privada los usuarios puedan autenticarse y ser autorizados de forma segura.

3.3 Configuración

Para que se pueda entender un poco mejor como se ha llevado a cabo esta prueba de concepto, se explicarán los pasos más importantes en la configuración de los actores de este sistema. En el anexo se incluirá con más detalle algunas partes de estas configuraciones.

3.3.1 Switch

Primero de todo hacemos un telnet a la ip de configuración del switch para poder entrar y hacer los cambios necesarios. Comprobamos que la configuración de 802.1x está activa. En el caso contrario la activamos, para que los posibles cambios sean efectivos. Dentro del fichero escribimos “dot1x system-auth-control”, así activamos globalmente la autenticación basada en puertos 802.1X. Los siguiente pasos que se han de hacer son:

- Crear un nuevo modelo para que la autenticación local sea aplicada en todas las líneas y interfaces.
- Crear un grupo de servidor nuevo con el nombre packetfence y lo configuramos con la ip que se utilizará para la configuración de este.
- Configurar la autenticación y autorización para que pertenezcan al grupo definido anteriormente.
- Determinar qué protocolos de autenticación y autorización de aplicaciones de acceso serán utilizados,
- Configurar las VLANs que habrá en la red. En este caso tendremos tres, una para autenticaciones vía EAP-TLS, otra para MAB y otra para usuarios que no pertenezcan a ningún grupo. Este último grupo es para aislar a usuarios o solo dar acceso a internet y que no puedan entrar en la red privada.
- Asignar el rango de IPs para cada VLAN
- Configurar interfaces de las VLAN.
- Configurar los puertos para cada conexión.

- Ordenar con qué protocolo se utilizará. Primero pondremos a 802.1x, en el caso que no sea posible se utilizará MAB

Después podemos configurar el tiempo en el que un usuario debe volver a autenticarse o si ha de ser periódico o no. Determinamos qué pasa cuando más de un dispositivo se conecta al mismo puerto. Lo configuramos que cuando un nuevo dispositivo se conecta en un puerto donde ya había alguien, este nuevo dispositivo reemplace al viejo. Así cualquier persona que quiera conectarse no necesita tener un puerto en concreto al que acceder. En nuestro caso, solo se configurará un puerto, en un caso real se debería configurar cada puerto con las necesidades necesarias. El puerto que se ha escogido es el 13. Activamos que se pueda utilizar MAB y habilitar 802.1X en el puerto 13 con los parámetros por defecto. Estos serían los parámetros que se deberían configurar más importantes.

3.3.2 PacketFence

Como ya se ha explicado anteriormente PacketFence es el que se encargará del control de acceso de la red. Explicaremos los detalles más importantes para configurar correctamente PacketFence con los diferentes actores del sistema. Las configuraciones básicas que se han de hacer son:

- Definiremos que PacketFence actúe como un servidor RADIUS.
- Configurarán las interfaces por las que se podrán configurar el switch y definir la interfaz del administrador que debería de estar en la misma red.
- Base de datos. Se dará la información necesaria para crear la base de datos donde se almacenarán las configuraciones que hagamos.
- Proveeremos el nombre de dominio, la lista de servidores DHCP entre otros.
- Crearemos un nombre y usuario para el administrador de PacketFence.
- Cuando se confirme que todo es correcto se iniciarán los servicios configurados y nos redirigirá a la página de administrador.
- Conectarse al Active Directory, para utilizar los usuarios configurados en este.
- Añadir la configuración del switch.
- Configurar perfiles para cada tipo de conexión. Por ejemplo una para 802.1x y otra para MAB.
- Configurar la PKI con la que se generarán los certificados.

3.3.3 Active Directory

En el caso del active directory sólo se explicará qué roles específicos se necesitan instalar para esta prueba de concepto. Las otras instalaciones más específicas estarán en el anexo. Los roles que se necesitarán instalar son:

- DNS, para poder configurar la red en la que estamos y servidor de dominio
- Servicio de administración de certificados, para que los usuarios se puedan autenticar con certificados
- Servidor web, para poder crear una web que nos ayude a crear y gestionar certificados.

Con esto ya tendríamos los roles más importante de la configuración del active directory. Una de las ventajas del AD es que su interfaz gráfica es intuitiva y nos ayuda a que sea fácil la configuración de este.

3.3.4 Usuarios

Una vez todos los servicios estén configurados solo quedaría explicar cómo han de hacer los usuarios que quieren acceder a esta red privada. Este apartado se explicará más detalladamente en el anexo separando los dos casos. El primero en el caso que el usuario utilice Windows y el segundo que utilice Linux. Lo único que hay que hacer en los dos casos es instalar el certificado del usuario su dispositivo. Se configura qué tipo de conexión se utilizará y se conecta el cable en el puerto escogido que es el 13. Una vez esto si el usuario tiene un certificado correcto y escribe correctamente la contraseña del certificado, tendrá acceso a la red privada con una IP perteneciente a la VLAN configurada.

3.4 Análisi de la prueba de concepto

A continuación se hará un resumen de los pros y contras que nos puede aportar esta solución en un entorno real, como es una red privada de una empresa.

Lo primero que analizaremos es si nos está proporcionando el extra de seguridad que queríamos y si los costes de trabajo y dinero son asumibles. Como se ha comentado al principio solo se utilizaba la MAC de cada ordenador para identificar si el usuario podía acceder a la red privada de la empresa. Esto podría dar el caso que si alguien descubre la MAC de una usuario que tenga autorización, pueda hacer un suplantamiento de identidad y entrar. Lo que sugerimos en este caso de uso es mediante el estándar 802.1x, específicamente el protocolo EAP-TLS que nos permite utilizar certificados,

mejorar la seguridad de la red privada. Si un usuario que está autorizado en la red, a parte de su usuario necesita su certificado y contraseña. Un atacante tendrá más dificultades para poder acceder que de la forma que se hace actualmente. Aún quedaría expuesto la parte de la red que dispositivos que no tienen la capacidad de soportar certificados, como por ejemplo impresoras o teléfonos de voz ip. Pero estos casos se aíslan en un VLAN que solo tenga acceso a las necesidades de estas y nada más.

También podría dar el caso que gente externa quiera conectarse a la red privada vía cable para tener una mejor conexión. En este caso se podría configurar una VLAN que solo tenga acceso a internet, así se cubriría esta necesidad.

Por otro lado tenemos los costes de administración y mantenimiento de esta prueba de red a gran escala. En este caso sí que tendríamos un mayor coste de administración y mantenimiento al principio de la transición. Para reducir este coste, podríamos empezar a pasar a los usuarios a esta nueva forma de autenticarse por grupos de usuario, por ejemplo por cada VLAN que haya o departamento. Una vez estos ya estén configurados y todos funcionen correctamente durante un tiempo sin dar problemas, pasar al siguiente grupo. Al principio cuando se tenga que pasar toda la empresa a este tipo de red, si que habrá un coste de trabajo mayor, pero en el momento que toda la empresa se haya traspasado a esta nueva forma de autenticación, el coste de administración bajará considerablemente a solo las nuevas altas o bajas de personal. El mantenimiento de la red solo aumentará por la complejidad mayor que tiene este tipo de soluciones. Pero al darle un mayor nivel de seguridad es compensable.

Para la administración y mantenimiento de certificados que dará más trabajo al departamento que gestiona este tipo de problemas, se podría configurar el sistema para cuando un certificado esté a punto de caducar que notifique al administrador o al propio usuario y que haga una petición de renovación. Así no habrá problemas de conexión cuando el usuario quiera conectarse. Además como la creación de estos certificados ser harán de forma escalonada, no todos los certificados caducarán al mismo tiempo y esto dará un margen para que se pueda trabajar en ello.

Por otro lado tenemos los costes que puede costar este tipo de cambio. Por la parte de material de hardware, podríamos empezar por los switches que se utilizarían los mismos que hay actualmente, así que por esta parte no habría problema. En el caso de los programas como active directory se debería de actualizar a una versión más actual, para prevenir que cualquier vulnerabilidad nos pueda afectar. Esto podría nos costaría un coste extra de dinero porque habría que comprar una nueva licencia, pero mejoraría la seguridad. Por otro lado tenemos Packetfence, que al ser un programa de código abierto, no se ha de pagar licencias, así que tendríamos el coste de configuración de este solo. Aunque esto puede repercutir indirectamente a la contratación de otra persona si está aumentando el trabajo del departamento que se tendrá que hacer cargo de esto.

En el caso de la administración de los usuarios al ser compatible con el LDAP de active directory que es actualmente el que se utiliza en la empresa, no nos daría un extra de trabajo, porque no se tendrían configurar los usuarios duplicados para PacketFence y AD. Esto nos rebaja la posible carga de trabajo que nos podría dar en el aspecto de la administración de usuarios de la red privada de la empresa en la que se quiere aplicar esta solución.

Al ser programas que son conocidos hay una gran documentación tanto de instalación como para solucionar problemas. Al estar cada día mejorando y actualizándose en las nuevas tecnologías, tienen habilitados servicios de atención al usuario, vía foros, por email entre otros. Esto nos permite que si tenemos algún problema tengamos alguna manera con la que encontrar una solución fácil y rápidamente. En el caso que hayamos encontrado una vulnerabilidad o un fallo podemos comentarlo y que busquen una posible solución y así ayudar a la comunidad.

Por último tenemos que tener en cuenta que esta solución no es perfecta y podría haber algún atacante que pudiera encontrar alguna vulnerabilidad en algún punto de la arquitectura. Utilizarla para poder entrar en la red privada y sustraer información. Pero cada día salen nuevas vulnerabilidades y ataques, se trata de ponérselo lo más difícil posible. Con esta solución lo que queremos conseguir es poner unas capas más de seguridad, haciendo que un atacante lo tenga más complejidad a la hora de intentar entrar en la red privada.

A continuación se presenta una tabla con un resumen de las características que juegan a nuestro favor y en contra de la esta posible solución.

Ventajas	**Desventajas**
Más seguridad	Más coste de administración y mantenimiento de la red
Fácil de configurar	Administración de certificados
No gran coste de dinero	Nueva licencia de Windows
Compatible con el sistema actual	Posibles nuevas vulnerabilidades
Reusabilidad de componentes	Contratación de personal extra
PacketFence código abierto su licencia es gratis.	
Gran documentación de los programas escogidos.	

Tabla 4. Tabla ventajas y desventajas prueba de concepto

Como vemos tenemos algunas ventajas y desventajas en esta solución, pero podríamos considerar que las ventajas son mayores en este caso que las desventajas. Si que es cierto que la mayor desventaja es la administración y mantenimiento de la red. Pero es un coste, como ya se ha comentado previamente, que al principio tendrá mucho trabajo pero en el momento que toda la empresa ya se haya adaptado a esta nueva solución el coste bajará considerablemente. Así que se podría asumir por la mejora de la seguridad de la red privada. Es importante que desde fuera no puedan acceder, pero no nos tenemos que descuidar que alguien de dentro pueda tener acceso a información que sea privada y pueda interferir en los fines de la empresa.

4. Conclusiones

El objetivo de este caso de estudio era buscar un refuerzo en la seguridad de las redes privadas de las empresas. Se ha buscado diferentes tecnologías para poder escoger la que más beneficios aporta a nuestro caso.

Unos de los objetivos planteados era buscar el estado del arte para la mejora de la seguridad en redes privadas. Que tipo de protocolos existen actualmente, qué programas nos ayudan asumir este objetivo, entre ellos cual se asemeja a nuestras necesidades. Este objetivo se ha completado escogiendo las tecnologías que más se acercaban a nuestro caso de uso planteado.

Como se ha visto a lo largo del trabajo de final de máster, hay muchas opciones en las que escoger y entre ellas diferentes variables que probar. En nuestro caso solo se ha hecho la implementación de una solución por tiempo y recursos, pero una posible mejora sería probar las diferentes soluciones planteadas, y estudiar de forma práctica si hay mejoras o no respecto a la solución escogida.

Las herramientas escogidas están basadas en las que se utilizan actualmente en la empresa que se basa este caso de uso. Esto ayuda que si en un futuro se quiere implementar esta solución, sea más fácil porque algunas ya están siendo usadas.

Para planear el trabajo que se ha ido haciendo durante todo el curso se ha utilizado Agile. Que nos ha ayudado a seleccionar pequeños objetivos para ir cumpliendo con las fechas establecidas de las entregas planificadas para este cuatrimestre. Agile al ser una herramienta que plantea pequeños hitos, nos da la opción que en el caso que no se haya organizado bien, se puede corregir al momento para que en el próximo hito se pueda ajustar correctamente.

Por último en este proyecto me he puesto al día y aprendido qué tipo de soluciones se aplican hoy en día para la autenticación y autorización de redes privadas. Encontrando muchas opciones con sus ventajas y desventajas. Me ha ayudado a tener una vista de que cada día las soluciones van evolucionando y que hay que estar al día de las nuevas posibles mejoras.

4.1 Pasos en el futuro

Algunas mejoras que se podrían hacer en un futuro, sería actualizar todos los componentes que tenemos a la última versión. Así si alguna herramienta tiene una posible vulnerabilidad no se podría utilizar para poder entrar en el sistema.

Por otro lado, se podrían hacer otros prototipos con otras herramientas para poder comprobar si tienen otras ventajas que no nos da la escogida. Así podríamos conocer con más información qué solución sería la mejor.

Otra mejora a plantear, sería la solución escogida pero con redes Wifi. Así los usuarios de la red privada no deberían de conectarse vía cable y tendrían acceso a la red privada en cualquier punto donde llegará la conexión. Esto también plantea algunos problemas de seguridad que se deberían de estudiar, ya que al no necesitar una conexión vía cable, cualquier persona que llegará a la red wifi podría probar de buscar una manera de entrar.

Como conclusión siempre hay que estar buscando nuevas soluciones y estar actualizados a las posibles vulnerabilidades que puedan surgir y sus soluciones.

5. Glosario

AD: Active Directory
EAP: Extensible Authentication Protocol
EAPOL: Extensible Authentication Protocol over LAN
EAP-FAST: Flexible Authentication via Secure Tunneling Extensible Authentication Protocol
EAP-TLS: Extensible Authentication Protocol - Transport Layer Security
EAP-TTLS: Extensible Authentication Protocol - Tunneled Transport Layer Security
IEEE: Institute of Electrical and Electronics Engineers
LAN: Local Area Network
MAB: MAC Authentication Bypass
MAC: Media Access Control
MAN: Metropolitan Area Network
MD5: Message-Digest Algorithm 5
NAC: Network Acess Control
PAC: Protected Access Credential
PAN: Personal Area Network
PAE: Port Access Entity
PEAP: Protected Extensible Authentication Protocol
PIN: Personal Identification Number.
RADIUS: Remote Authentication Dial-In User Service
VLAN: Virtual Local Area Network
VPN: Virtual Private Network
WAN: Wide Area Network

6. Bibliografía

[1] Descripción general de 802.1X y tipos de EAP [Fecha de consulta: 29 de febrero del 2020]
<https://www.intel.es/content/www/es/es/support/articles/000006999/network-and-i-o/wireless-networking.html>

[2] Control de acceso a red basada en puertos [Fecha de consulta: 29 de febrero del 2020]
<https://www.perlesystems.es/supportfiles/port-based-network-access.shtml>

[3] PacketFence [Fecha de consulta: 29 de febrero del 2020] <https://packetfence.org/>

[4] *Remote Authentication Dial In User Service (RADIUS)* [Fecha de consulta: 29 de febrero del 2020]
<https://www.hjp.at/doc/rfc/rfc2865.html>

[5] Piedad Cristina Martínez, [Fecha consulta: 02 de marzo del 2020] *El método de estudio de caso*

[6] Arana, José R.; Villa, Leandro A.; Polanco, Oscar, [Fecha consulta: 02 de marzo del 2020] *Implementación del control de acceso a la red mediante los protocolos de autenticación, autorización y auditoría*
<https://www.redalyc.org/pdf/2913/291329165011.pdf>

[7] Henry Nunoo-Mensah, Emmanuel Kofi Akowuah, Kwame Osei Boateng [Fecha consulta: 02 de marzo del 2020] *A Review of Opensource Network Access Control (NAC) Tools for Enterprise Educational Networks*
<https://www.researchgate.net/publication/277012927_A_Review_of_Opensource_Network_Access_Control_NAC_Tools_for_Enterprise_Educational_Networks>

[8] *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines* [Fecha de consulta: 29 de febrero del 2020]
<https://www.hjp.at/doc/rfc/rfc3580.html>

[9] *The EAP-TLS Authentication Protocol* [Fecha de consulta: 29 de febrero del 2020] <https://www.hjp.at/doc/rfc/rfc5216.html>

[10] *Protected EAP Protocol (PEAP)* [Fecha de consulta: 29 de febrero del 2020] <https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-06>

[11] *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version* [Fecha de consulta: 29 de febrero del 2020] <https://www.hjp.at/doc/rfc/rfc5281.html>

[12] *OpenNac*, [Fecha de consulta: 29 de febrero del 2020] <http://sourceforge.net/projects/opennac>

[13] “FreeNAC”, [Fecha de consulta: 29 de febrero del 2020] <http://www.freenac.net/phpBB2>

[14] “Definición de red”, [Fecha de consulta: 26 de marzo del 2020] <https://dle.rae.es/?w=red>

[15] José Dordoigne, [Fecha consulta: 26 de marzo del 2020] *Redes Informáticas*

[16] “Definición de autenticación” [Fecha consulta: 27 de marzo del 2020] <https://dej.rae.es/lema/autenticaci%C3%B3n>

[17] “Definición de autorización”, [Fecha consulta: 27 de marzo del 2020] <https://dle.rae.es/?w=autorizaci%C3%B3n>

[18] Authentication, [Fecha de consulta: 27 de marzo del 2020] <https://searchsecurity.techtarget.com/definition/authentication>

[19] The Economic Times, Authentication, [Fecha de consulta: 27 de marzo del 2020] <https://economictimes.indiatimes.com/definition/authentication>

[20] 802.1X: Port-Based Network Access Control, [Fecha de consulta: 27 de marzo del 2020] <https://1.ieee802.org/security/802-1x/>

[21] Arunesh Mishra, William A. Arbaugh, [Fecha consulta: 27 de marzo del 2020] *An initial Security Analysis of the IEEE 802.1x Standard*

[22] Extensible Authentication Protocol (EAP), [Fecha consulta: 27 de marzo del 2020]<https://tools.ietf.org/html/rfc3748>

[23] Yogesh Singare, Manish Tembhurkar, [Fecha consulta: 27 de marzo del 2020] A Comparitive Analysis of EAP Authentication Mechanism for WLAN

[24] *The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)* [Fecha consulta: 27 de marzo del 2020]<https://tools.ietf.org/html/rfc4851>

[25] *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs* [Fecha consulta: 27 de marzo del 2020] <https://www.hjp.at/doc/rfc/rfc4017.html>

[26] *MAC Authentication Bypass Deployment Guide,* [Fecha consulta: 27 de marzo del 2020] <https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.html>

[27] *¿Qué es Debian?,* [Fecha consulta: 21 de Abril del 2020] <https://www.debian.org/releases/jessie/armel/ch01s01.html.es>

7. Anexo

7.1 Switch

Para poder activar 802.1x en el switch primero comprobamos si está activo o no, en caso negativo lo activamos. Para ello en el terminal escribimos:

→ show dot1x
    Sysauthcontrol Disabled
    Dot1x Protocol Version 3
→ enable
→ configuration terminal

Dentro del fichero escribimos “dot1x system-auth-control”, así activamos globalmente la autenticación basada en puertos 802.1X. Creamos un nuevo modelo para que la autenticación local sea aplicada en todas las líneas y interfaces.

→ aaa new-model

Creamos un grupo de servidor nuevo con el nombre packetfence y lo configuramos con la ip que se utilizará para la configuración de este.

→ aaa group server radius packetfence
    server 10.0.2.100 auth-port 1812 acct-port 1813

Configuramos la autenticación y autorización para que pertenezcan al grupo definido anteriormente como packetfence.

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

El siguiente paso es determinar qué protocolo de autenticación y autorización de aplicaciones de acceso a la red tendremos. En este caso es RADIUS (Remote Authentication Dial In User Service). La ip que se utilizará para que el switch y packetfence se puedan comunicar es 10.0.2.100, con puerto 1813 y con la opción que la clave se utilice para esta conexión sea fuerte.

→ aaa server radius dynamic-author
    client 10.0.2.100
    server-key useStrongerSecret
    port 3799

A continuación configuramos las VLAN que habrá en este sistema de pruebas. Estas serán 3, una en la que se conectarán los usuarios que se autentique vía EAP-TLS, otra para los teléfonos o impresoras que se autentiquen con MAB y

por último una para los que intenten conectarse pero no tengan un grupo asignado. Para ello primero excluimos de estas VLANs las IP que no se pueden asignar a los usuarios.

→ ip dhcp excluded-address 10.0.50.1 10.0.50.10
→ ip dhcp excluded-address 10.0.48.1 10.0.48.10

Una vez ya están excluidas pasamos a definir qué ip formarán las VLANs comentadas anteriormente. Las separaremos en 10.0.48.0, 10.0.50.0 y 10.0.102.0. Ponemos lease 3 que determina el tiempo que puede estar conectado a la red

→ ip dhcp pool vlan14
    network 10.0.48.0 255.255.255.0
    lease 3
→ ip dhcp pool vlan5
    network 10.0.50.0 255.255.255.0
    lease 3
→ ip dhcp pool vlan102
    network 10.0.102.0 255.255.255.0
    lease 3

Para acabar con la configuración de las VLANs, definimos la interfaz de cada una

→ interface Vlan5
    ip address 10.0.50.1 255.255.255.0
→ interface Vlan14
    ip address 10.0.48.1 255.255.255.0
→ interface Vlan102
    ip address 10.0.102.1 255.255.255.0

En esta prueba solo se configura un puerto para que los ordenadores que hacen de cliente puedan autenticarse. En un entorno real se tendría que configurar cada puerto por separado dependiendo de las necesidades en ese momento. Para ello lo haremos de la siguiente manera. En la interfaz 13 que es la escogida para ser configurada. Las partes más importantes son

→ interface GigabitEthernet1/0/13
    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

Con la orden “authentication order” podemos definir el orden que utilizará el switch para utilizar un protocolo o no. En nuestro caso el primero que ha de probar es el 802.1x y después vía MAC. La “priority” es parecida al orden, da prioridad al primer protocolo que esté en la lista. “authentication port-control auto” nos permite que sea automático que pase de autorizado a no autorizado sin la necesidad que manualmente tengamos que hacer algún cambio. Activamos que se pueda utilizar MAB con “mab”. “dot1x pae authenticator” habilita 802.1X en el puerto 13 con los parámetros por defecto.

7.2 PacketFence

Como ya se ha explicado anteriormente PacketFence es el que se encargará del control de acceso de la red. Explicaremos los detalles más importantes para configurar correctamente PacketFence con los diferentes actores del sistema.

Primero de todo vamos a “https://10.0.2.100:1443/configurator” aquí se configurarán las opciones básicas para configurar el switch con PacketFence.

Una vez ya estamos en la página de administrador es cuando podemos hacer cambios mayores. Por ejemplo el primer paso será conectarnos con el Active Directory que se ha configurado. Para ello configuramos el dominio que tiene el AD en PacketFence. Vamos a “Configuration→Policies and Access Control→Domains→Active Directory Domain” y creamos un nuevo dominio.

Nos pedirá la ip del servidor de active directory, usuario y contraseña del administrador del sistema del AD, entre otras cosas. Como vemos en la figura 3 así es como quedaría la configuración del dominio.

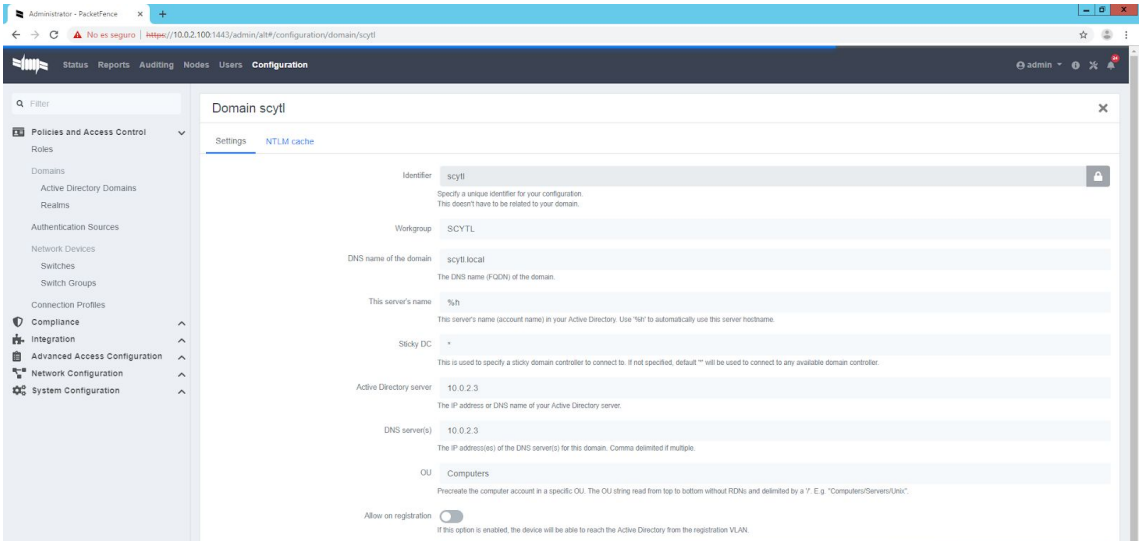


Figura 5. Configuración dominio PacketFence

Una vez ya tenemos conexión con el AD vamos a hacer que se autentiquen contra él. Así se utilizará directamente la base de datos de los usuarios que tiene Active Directory. En Authentication Sources" creamos una nueva fuente de autenticación. Con la configuración necesaria del AD. Como vemos en la figura 6 nos muestra los diferentes campos que necesitamos. La mayoría son de la configuración hecha de LDAP del Active Directory. Cuando tengamos todo le podemos dar a test para comprobar que la conexión se hace correctamente. Si al darle a test sale "'Success! LDAP connect, bind and search successful" es que se ha podido vincular al servidor de LDAP. Así nos aseguramos que podemos seguir sin tener problemas en este punto.

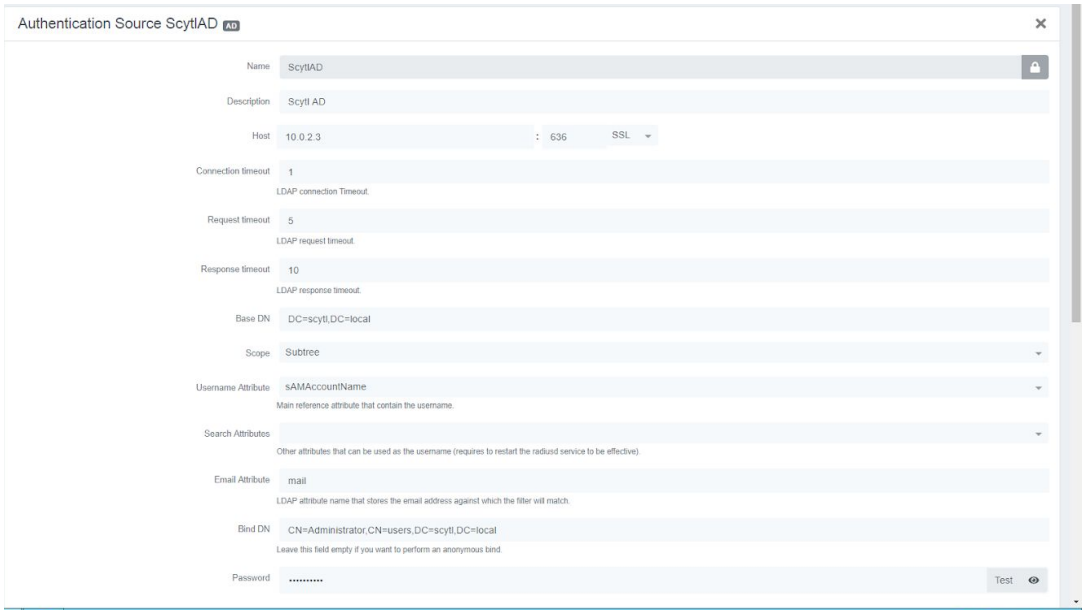


Figura 6. Configuración fuente active directory

Con la seguridad que ya tenemos conexión, vamos a añadir el switch al PacketFence. En la figura 7 vemos los diferentes datos que hay que introducir:

- IP: 10.0.2.1.
- Tipo: Cisco Catalyst 2960
- Modo: producción.

También en la pestaña de Roles se han de configurar que VLAN serán las que se asignen a los usuarios que tienen se puedan autenticar ante el servidor. La siguiente pestaña que se ha de revisar es RADIUS, aquí determinaremos la "secret Passphrase" que se utilizará. Por último en la pestaña SNMP proveer los valores de Community Read y Community Write. Con esto ya tendremos la parte del switch configurada.

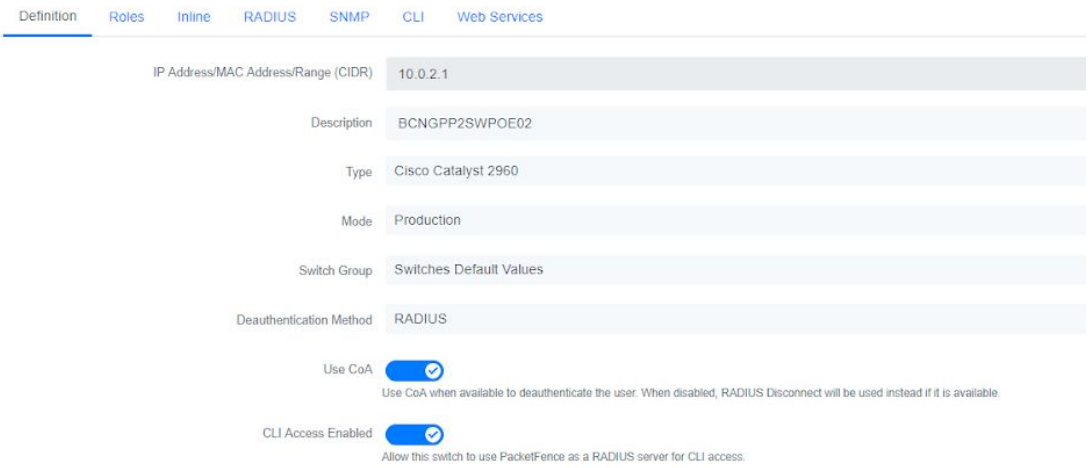


Figura 7. Configuración Switch

Lo siguiente será el perfil de conexión, que configura a PacketFence que hacer cuando una conexión viene vía 802.1x o MAB. Para ello configuraremos dos perfiles uno para cada protocolo. El primero que configuraremos será a 802.1x, activamos Enable profile y Automatically register devices. Después se define un filtro que es el que se encargará de decidir qué tipo de protocolo es el que se utilizará. Como vemos en la figura 8 hay que poner en el tipo de conexión dentro del filtro Ethernet EAP, junto con la fuente definida anteriormente.

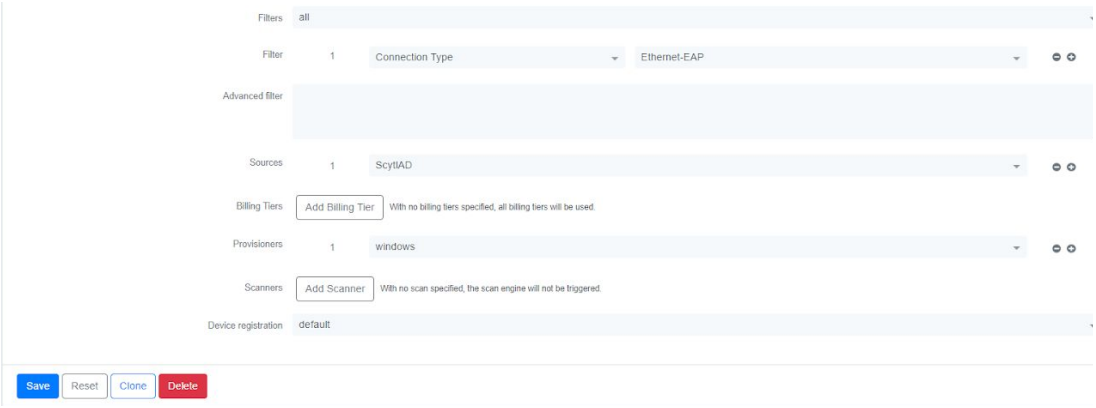


Figura 8. Configuración filtro 802.1X

Ahora configuramos la segunda regla que es para la autenticación por MAC. Se trata de hacer lo mismo que la anterior pero el Connection-Type será del tipo Ethernet-NoEAP, así este filtro no utilizará la versión EAP.

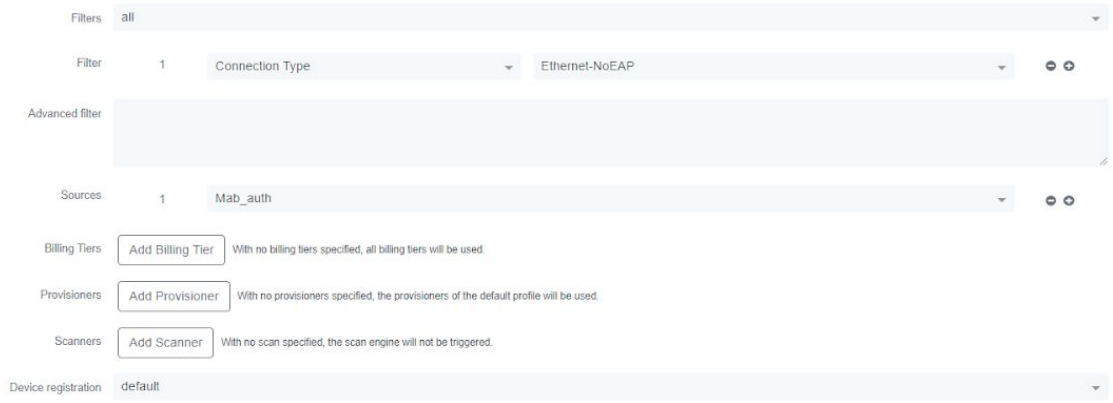


Figura 9. Configuración filtro MAB

Ahora que ya hemos configurado los dos perfiles que vamos a utilizar en las conexiones ya podemos pasar a ver la configuración que necesitamos para el active directory. Por parte de PacketFence faltaría configurar la PKI que se ha de crear con el Active Directory que será el encargado de crear certificados. Esto se explicará junto a la creación de esta.

7.3 Active Directory

En el caso del active directory sólo se explicará qué roles específicos se necesitan instalar para esta prueba de concepto. Como vemos en la figura 10 necesitaremos el rol de DNS para poder configurar la red en la que estamos y servidor de dominio. Después el servicio de administración de certificados, para que los usuarios se puedan autenticar con certificados.

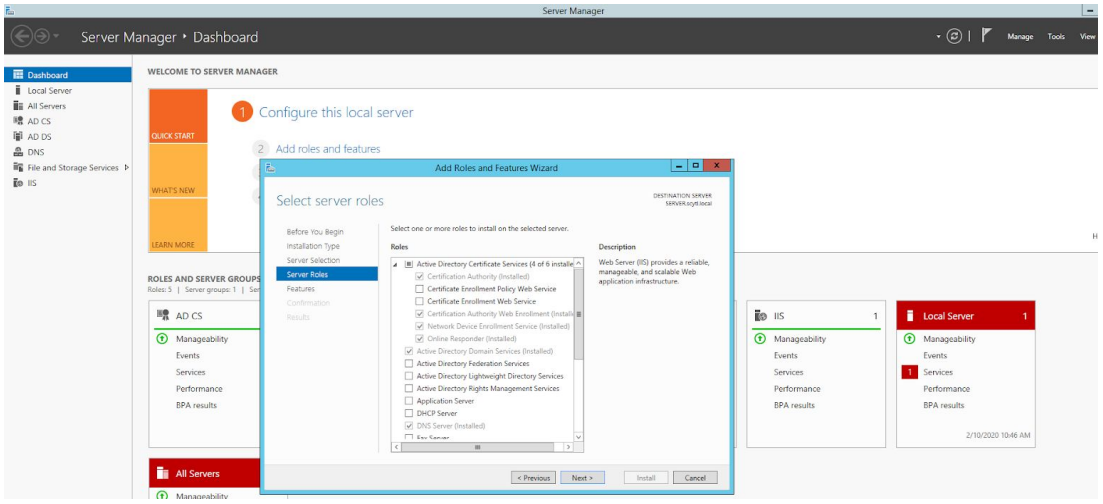


Figura 10. Configuración de roles AD

En segundo lugar también se ha de instalar el servidor web para poder crear una web que nos ayude a crear y gestionar certificados. Como vemos en la figura 11 esos serían los roles que se han de instalar.

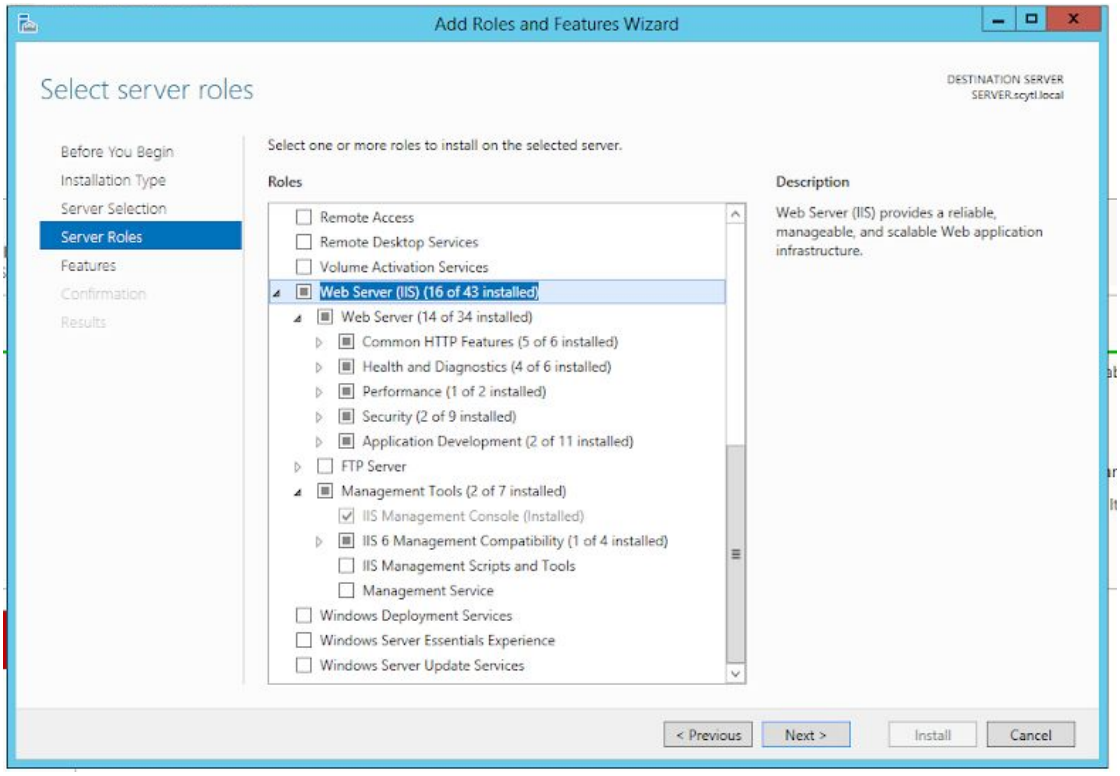


Figura 11. Configuración de roles AD 2

Con esto ya tendríamos los más importante de la configuración del active directory. Una de las ventajas del AD es que su interfaz gráfica es intuitiva y nos ayuda a que sea fácil la configuración de este.

7.4 Usuarios

Una vez todos los servicios estén configurados solo quedaría explicar cómo han de hacer los usuarios que quieren acceder a esta red privada. Este apartado se separará en dos casos el primero en el caso que el usuario utilice Windows y el segundo que utilice Linux. Pero en los dos casos solo se explicará cómo conectarse.

7.4.1 Windows

Primero de todo vamos a configurar la conexión del ordenador para que utilice EAP-TLS. Vamos al panel de “Network connections” y modificaremos Ethernet 2, para ello entraremos en la properties de esta.

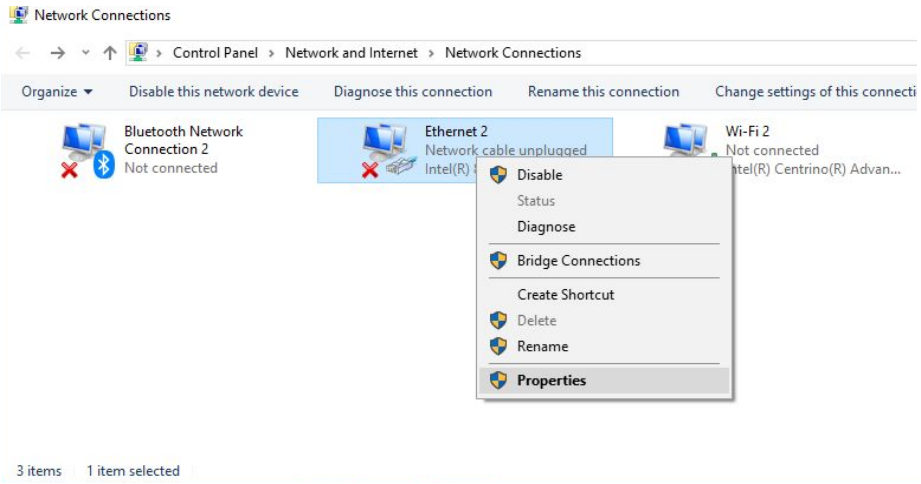


Figura 12. Configuración ethernet.

Dentro de este menú vamos a Authentication y habilitamos el "IEEE 802.1.X authentication". Seleccionamos el EAP-TTLS en el método. Le damos a settings para configurar el método que hemos escogido.

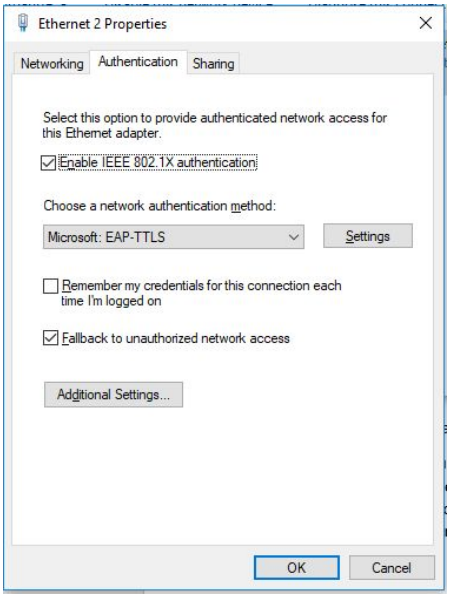


Figura 13. Propiedades ethernet.

Los cambios que se han de hacer en este menú son:

- Seleccionar la CA del active directory que se instaló en su momento de la misma manera que hemos instalado nuestro certificado.
- Quitar que sea posible la identidad privada para que el server pueda saber quien es el que se conecta y no sea anónimo.
- En la opción de "client authentication" seleccionamos la opción "select an EAP method for authentication", dentro del desplegable de esta opción escogemos la "Microsoft: Smart card or other certificate"

Una vez esté todo correcto de este menú pasamos a configurar el método de autenticación que hemos escogido dándole al botón "*Configure*" que hay abajo a la derecha de este menú.

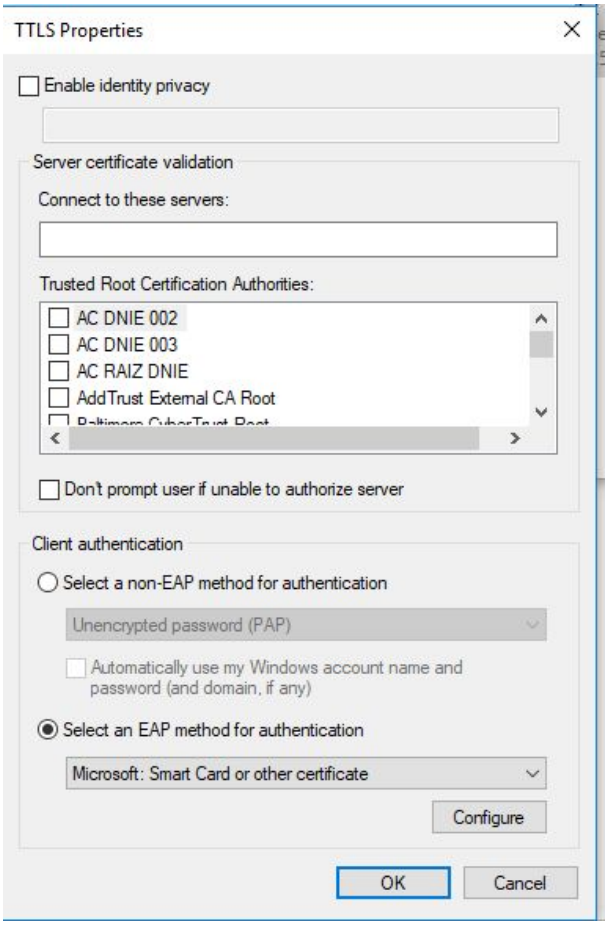


Figura 14. TTLS properties

En este último menú se configura las propiedades del certificado que se utilizará:

- Seleccionamos que queremos autenticarnos con un certificado de este ordenador.
- Validar la identidad del servidor con la CA que hemos instalado antes.
- Marcar la casilla de “Use different user name for the connection” para que nos deje escoger con que usuario nos queremos conectar.
- En el caso que el ordenador tuviera el mismo nombre que el usuario no haría falta marcar esta opción.

Guardamos los cambios y ya podemos conectarnos con el certificado.

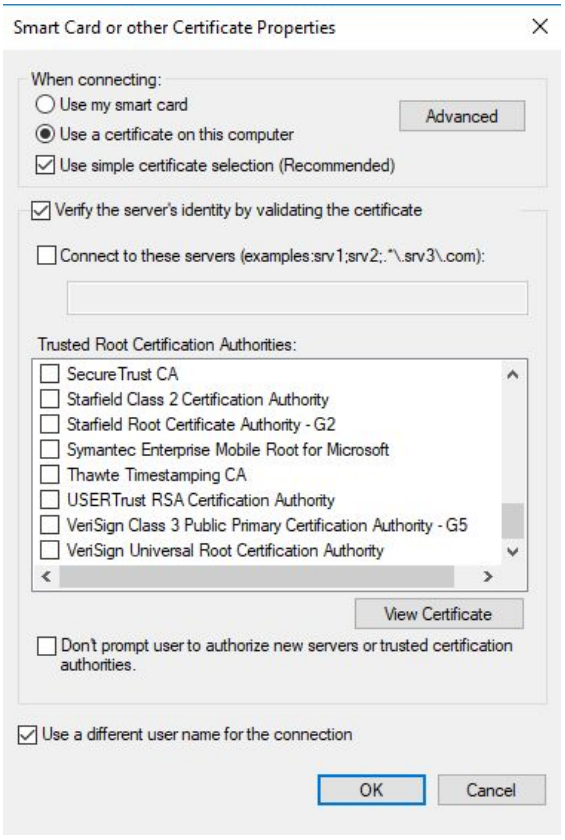


Figura 15. Certificate properties

Para ello conectamos el cable ethernet a nuestro pc y nos saldrá una ventana para que escojamos el certificado del usuario con el que nos queremos conectar. Le damos a aceptar y si todo está configurado correctamente nos debería dar una IP en el rango correcto del rol que nos ha asignado el Switch, que en este caso sería Research&Security del rango 10.0.48.0/24.

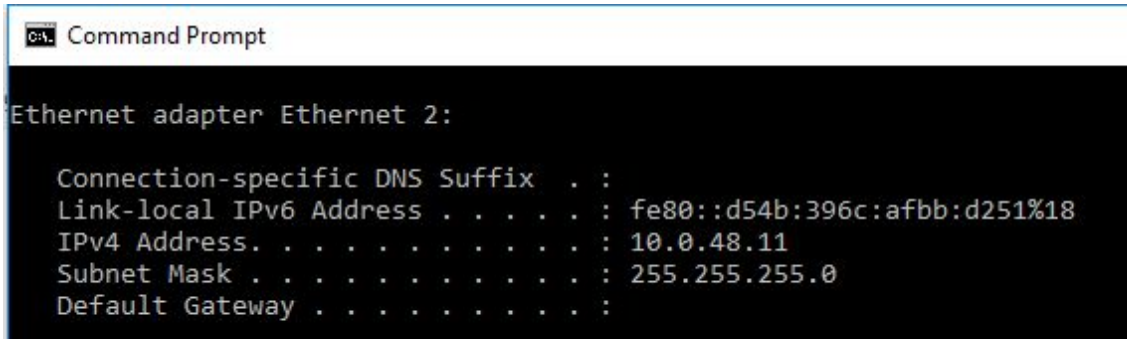


Figura 16. Ip Rol Asignado.

Con esto ya tendríamos toda la configuración de una máquina Windows se conecte al active directory via packetfence. En el caso que fuera vía MAB porque fuera un dispositivo que no soporta certificados, solo se tendría que conectar y si la MAC está configurada correctamente en PacketFence se auto gestionaria y se asignará una ip con el rol de voice. Estos solo tendrían acceso a la parte de la red privada dedicada a este tipo de gestiones.

7.4.2 Ubuntu

En el caso de ubuntu es más sencillo de configurar. Solo hay que ir a las opciones de red, la pestaña *Security* y configurar los siguiente:

- 802.1X Security: ON
- Autentication: TLS,
- Identity: nombre de usuario con el que queremos autenticarnos.
- User Certificate: El certificado del usuario con el que queremos autenticarnos.
- Private Key: La clave privada del usuario
- Private Key Password: La contraseña de la clave privada.

Figura 17. Configuración de red por cable

Con estos datos ya podemos autenticarnos y que nos den una ip correspondiente a esta configuración. Como en el caso anterior la ip ha de ser del rango de 10.0.48.0/24. Como vemos en la figura 18, se nos ha asignado la ip 10.0.48.146.

```
enp12s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.48.146  netmask 255.255.255.0  broadcast 10.0.48.255
        inet6 fe80::6416:afad:6460:7d2  prefixlen 64  scopeid 0x20<link>
        ether 20:89:84:d2:c9:8f  txqueuelen 1000  (Ethernet)
        RX packets 1863024  bytes 1807931632 (1.8 GB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 808514  bytes 144686627 (144.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 18. Ip en la nueva red privada

Con todos estos pasos, tendríamos la configuración básica de los elementos que conforman esta prueba de concepto.