eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
INFORMATIKA FAKULTATEA
FACULTAD DE INFORMÁTICA

Grado en Ingeniería Informática

Ingeniería de Computadores

Trabajo de Fin de Grado

Control de acceso sobre red cableada

Autor

Jose María Caballero

2019

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
INFORMATIKA FAKULTATEA
FACULTAD DE INFORMÁTICA

Grado en Ingeniería Informática

Ingeniería de Computadores

Trabajo de Fin de Grado

Control de acceso sobre red cableada

Autor

Jose María Caballero

Directores

José Miguel Alonso y José Miguel Blanco Arbe

Resumen

El objetivo del proyecto es la implementación de un control de acceso sobre la red cableada local del BCBL. El motivo del proyecto se debe a que, por la naturaleza de los datos que recoge y emplea para su investigación, el BCBL está sujeto al nivel más alto de LOPD *(**L**ey **O**rgánica de **P**rotección de **D**atos)*. Para evitar posibles intrusiones desde dentro de la organización, la política de seguridad recoge medidas como deshabilitar el uso de los puertos USB, navegación limitada a servicios de ficheros en la nube, etc. pero no dispone de ningún control de acceso sobre la red cableada, por lo que cualquier equipo que se conecte a la red tendrá acceso a la misma.

Debido a este motivo, se ha realizado una comparación tecnológica entre dos herramientas de software libre cuyo propósito es el control de acceso sobre una red y se ha seleccionado la más adecuada para la situación del BCBL que ha resultado ser PacketFence.

Una vez seleccionado el software adecuado ha sido instalado en un servidor sobre un entorno de testing donde se han realizado diferentes pruebas en base a diferentes métodos de autenticación, y al comprobar que el control de acceso ha funcionado correctamente se ha realizado el despliegue en una subred concreta de forma exitosa.

Teniendo en cuenta que para realizar un despliegue de este tipo en una red en producción 24 horas al día hay que encontrar el momento oportuno, se ha realizado la planificación para un despliegue global en la red que será implementado cuando el departamento de IT del BCBL lo encuentre oportuno.

Índice general

Índice de figuras

Índice de tablas

Glosario

BCBL: ***B****asque center on* ***C****ognition,* ***B****rain and* ***L****anguage*

IT: ***I****nformation* ***T****echnology*

TFG: ***T****rabajo de* ***F****in de* ***G****rado*

EDT: ***E****structura de* ***D****escomposicón del* ***T****rabajo*

NAC: ***N****etwork* ***A****ccess* ***C****ontrol*

PNAC: ***P****ort-based* ***N****etwork* ***A****ccess* ***C****ontrol*

PKI: ***P****ublic* ***K****ey* ***I****nfraestructure*

CA: ***C****ertification* ***A****uthority*

RA: ***R****egistration* ***A****uthority*

AD: ***A****ctive* ***D****irectory*

AD CS: ***A****ctive* ***D****irectory* ***C****ertificate* ***S****ervices*

LAN: ***L****ocal* ***A****rea* ***N****etwork*

VLAN: ***V****irtual* ***L****ocal* ***A****rea* ***N****etwork*

PPP: ***P****oint to* ***P****oint* ***P****rotocol*

AAA: ***A****uthentication,* ***A****utorization,* ***A****ccounting*

EAP: ***E****xtensible* ***A****uthentication* ***P****rotocol*

SNMP: ***S****imple* ***N****etwork* ***M****anagement* ***P****rotocol*

EAPoL: ***E****xtensible* ***A****uthentication* ***P****rotocol over* ***L****an*

SCEP: ***S****imple* ***C****ertificate* ***E****nrollment* ***P****rotocol*

NDES: ***N**etwork **D**evice **E**nrollment **S**ervice*

SSH: ***S**ecure **SH**ell*

SFTP: ***S**sh **F**ile **T**ransfer **P**rotocol*

TLS: ***T**ransport **L**ayer **S**ecurity*

NAS: ***N**etwork **A**ccess **S**witch*

DMZ: ***D**e**M**ilitarized **Z**one*

CPD: ***C**entro de **P**rocesamiento de **D**atos*

AP: ***A**ccess **P**oint*

DNS: ***D**omain **N**ame **S**ystem*

DHCP: ***D**ynamic **H**ost **C**onfiguration **P**rotocol*

GPO: ***G**roup **P**olicy **O**bject*

LOPD: ***L**ey **O**rgánica de **P**rotección **D**atos*

1. CAPÍTULO

Introducción

No es casualidad que en los tiempos que corren la palabra “ciberseguridad” se escuche con más frecuencia y tenga cada vez más relevancia en el ámbito empresarial. Puede que lo primero que nos venga a la cabeza al escuchar la palabra “ciberseguridad” sea pensar que es algo sobre lo que únicamente los expertos en dicho ámbito tienen que preocuparse, lo cual es un error garrafal. En esta sociedad donde se tiende a informatizar absolutamente todo lo posible, ser conscientes de lo que esto supone es el primer paso hacia la “ciberseguridad” o seguridad informática.

Por ejemplo, puede afirmarse que hoy en día todo el mundo lleva un pequeño ordenador portátil en el bolsillo, y que no todas las personas son conscientes de ello, si no que para muchas de estas personas ese ordenador no es más que un teléfono.

Debido a esto, muchas empresas recurren a instalar Controles de Acceso o *NAC (**N**etwork **A**ccess **C**ontrol)* en sus redes privadas. Esto no significa que los departamentos de seguridad informática de las empresas sospechen de que los mismos empleados o usuarios de la red vayan a realizar acciones delictivas o peligrosas a propósito (aunque también podría darse el caso), significa que el departamento de seguridad informática es consciente sobre la inconsciencia general y social respecto a este tipo de seguridad.

Este TFG ha sido realizado en el BCBL *(**B**asque center on **C**ognition, **B**rain and **L**anguage*), un centro donde se realizan numerosas investigaciones por un grupo de unos 100 investigadores en total. Estos investigadores utilizan equipos propios del BCBL conectados de forma cableada a la LAN *(**L**ocal **A**rea **N**etwork)*.

Estos equipos están configurados mediante políticas GPO *(**G**roup **P**olicy **Object**)* por lo que los usuarios finales no tienen permisos para realizar ciertas acciones, ya sean cambiar configuraciones internas del equipo o instalar software que no esté permitido por los administradores.

El problema comienza cuando cualquiera de estos usuarios puede traer un equipo personal (por ejemplo un ordenador portátil) y conectarlo a la LAN utilizando el mismo cable que, en teoría, únicamente debería utilizarse para conectar los equipos propios del BCBL.

Una vez que un equipo personal ha conseguido acceso a la LAN de la empresa podrían darse multitud de situaciones en las que tanto los servidores como los datos internos del BCBL pudieran quedar comprometidos. Teniendo en cuenta que muchas investigaciones se realizan con sujetos reales, hay una gran cantidad de datos personales sujetos al nivel más estricto de la LOPD que, bajo ningún concepto, pueden salir del centro.

Para evitar este tipo de situaciones se ha implantado un control de acceso sobre la LAN del centro. Este control de acceso está basado en certificados PKI *(**P**ublic **K**ey **I**nfraestructure)*, lo que evitará que ningún equipo que no disponga de un certificado emitido por la CA *(**C**ertification **A**uthority)* local del BCBL pueda tener acceso a la red. En otras palabras, la autenticación se basará en las máquinas y no en los usuarios finales de las mismas, ya que si se impone únicamente una autenticación basada en usuario/contraseña, la situación mencionada anteriormente podría darse igualmente.

En el presente documento se explican todos los pasos realizados para la implementación del NAC en la red del centro desde cero, además de diferentes configuraciones y métodos de autenticación que podrían resultar más eficientes al ser combinados con las autenticaciones de máquinas basadas en certificados.

El presente documento ha sido redactado siguiendo la siguiente estructura:

- **Objetivos y alcance:** En este capítulo se exponen cuales han sido los objetivos principales del proyecto y cómo han sido realizados.
- **Tecnologías y herramientas utilizadas:** Breve explicación sobre las principales tecnologías y herramientas necesarias para la realización del proyecto además de una comparativa tecnológica entre dos potentes herramientas de código libre especializadas en NAC.
- **Desarrollo del proyecto:** En este conjunto de capítulos se explica cómo se ha llevado a cabo el desarrollo del proyecto. Está dividido tres secciones:
  - Implementación en entorno virtual controlado: En esta primera toma de contacto con la herramienta se explica como se ha configurado el sistema para realizar autenticaciones mediante usuarios almacenados en el Directorio Activo del BCBL.
  - Despliegue en subred en producción: En esta fase del desarrollo del proyecto se configura el sistema para realizar autenticaciones basadas en certificados PKI, y una vez testeado, se realiza el despliegue del sistema en una subred en producción.
  - Planificación del despliegue global en la red: En este capítulo se expone como se ha planificado un futuro despliegue global del sistema en la red.
- **Gestión del Proyecto:** En este capítulo se muestra como se ha llevado a cabo la gestión del proyecto sobre diferentes aspectos, tales como el alcance, el tiempo, los riesgos, etc.
- **Conclusiones:** Conclusiones y lecciones aprendidas con la realización del proyecto, además de un apartado de posibles mejoras.
- **Anexos:** Documentos donde se explican diferentes acciones que han tenido que realizarse para poder llevar a cabo el proyecto, pero no se ha visto la necesidad incluir en la documentación.
- **Bibliografía:** Fuentes de información que han sido consultadas durante la realización del proyecto.

2. CAPÍTULO

Antecedentes

En este capítulo se expondrá tanto la motivación de la empresa para implantar un control de acceso a la red, como la caracterización de las tecnologías y herramientas clave que se utilizarán a lo largo del proyecto.

Cabe mencionar que en este capítulo se hará una breve introducción a los diferentes conceptos que serán necesarios conocer mínimamente para poder tener una mayor comprensión sobre el proyecto. Se incluirán tanto herramientas como protocolos y estándares que, o bien son necesarios incluir en la red para la realización del proyecto, o simplemente son elementos que ya forman parte de la misma y por tanto he considerado oportuna su comprensión para poder seguir adelante.

2.1. Motivación

Este proyecto se ha desarrollado en el BCBL (***B**asque center on **C**ognition, **B**rain and **L**anguage*), el centro internacional de investigación interdisciplinar para el estudio de la cognición, el cerebro y el lenguaje que fué fundado conjuntamente por Ikerbasque, Innobasque, la UPV-EHU y la Diputación de Gipuzkoa en 2009.

Este centro utiliza una red local moderadamente grande, con más de un centenar de dispositivos conectados a ella. Esta red tiene como objetivo, entre otras cosas, la comunicación entre los diferentes departamentos del centro, así como el acceso al clúster de cómputo por parte de los investigadores residentes y el acceso a Internet y a los servicios del BCBL.

Teniendo en cuenta que es una red privada en la que se manejan una gran cantidad de datos, incluidos datos personales, tanto de los trabajadores del centro como de los sujetos de investigación que participan en las diversas investigaciones que se realizan en él, es más que razonable pensar que ésta pueda ser víctima de la intrusión de usuarios no deseados.

Es por ello por lo que el objetivo de este proyecto es la implementación de un NAC (***N**etwork **A**ccess **C**ontrol* o *Control de Acceso a la Red*) basado en el protocolo 802.1X sobre la red cableada del centro.

Este control de acceso se basará en evitar que ninguna máquina pueda conectarse a la red sin tener permiso previo para ello. Para ello se realizará una autenticación 802.1X basada certificados emitidos por la propia CA del centro. Los equipos que no tengan soporte para instalar o configurar un cliente para realizar la autenticación mediante el protocolo 802.1X (Impresoras, faxes, escáneres, etc.) serán autenticados mediante sus direcciones físicas o MACs.

2.2. Introducción a tecnologías y herramientas utilizadas

Esta sección constituye una introducción a dichos elementos y no una guía técnica detallada de los mismos, aunque los más importantes se explicarán con más detalle en el capítulo 4 *"Estudio de tecnologías y herramientas"*.

2.2.1. RADIUS

Acrónimo de ***R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice*. Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red. Además de autenticar y autorizar a los usuarios de dichas aplicaciones (ya sean los usuarios finales o las mismas máquinas que están utilizando para realizar la conexión) también es capaz de **contabilizar** las sesiones activas de los mismos. Esto significa que una vez el usuario ha sido autenticado y autorizado, puede iniciarse un registro de conexión con datos sobre inicio/fin de sesión, volumen de datos transferidos,etc. Es por esto por lo que RADIUS está considerado un protocolo AAA (***A**uthentication, **A**utorization, **A**ccounting*). [1]

2.2.2. Estándar IEEE 802.1X

IEEE 802.1X es un estándar IEEE para el control de acceso a la red basado en puertos (***P**ort-based **N**etwork **A**ccess **C**ontrol* o ***PNAC***). Forma parte del grupo de protocolos de red IEEE 802.1y proporciona un mecanismo de autenticación para los dispositivos que desean conectarse a una LAN o WLAN.

IEEE 802.1X define el encapsulamiento del Protocolo de autenticación extensible (***E**xtensible **A**uthentication **P**rotocol* o **EAP**) sobre IEEE 802, que se conoce como *EAP over LAN* (EAP sobre LAN) o **EAPoL**. [2]

[1] https://es.wikipedia.org/wiki/RADIUS
[2] https://es.wikipedia.org/wiki/IEEE_802.1X

2.2.3. Directorio Activo de Windows

Active **D**irectory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Además de esto, también se le puede asignar el servicio de Autoridad Certificadora, lo que significa que desde este mismo servidor se podrán crear y emitir certificados autofirmados, ya sean para ordenadores, usuarios, servicios web, etc. dentro del dominio sobre el que está configurado el Directorio Activo. [3]

2.2.4. Certificados basados en PKI

Una infraestructura de clave pública *(**P**ublic **K**ey **I**nfraestructure)* es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digitalmente información, garantizar el no repudio de un envío, y otros usos.

Todo certificado válido ha de ser emitido por una autoridad de certificación reconocida, que garantiza la validez de la asociación entre el poseedor del certificado y el certificado en sí. [4]

[3] https://es.wikipedia.org/wiki/Active_Directory
[4] https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica

2.2.5. SCEP

El protocolo está diseñado para que la emisión de certificados digitales sea lo más escalable posible. La idea es que cualquier usuario estándar de la red pueda solicitar su certificado digital de forma electrónica y lo más sencilla posible. Por lo general, estos procesos han requerido una intensa aportación de los administradores de red, por lo que no han sido adecuados para despliegues a gran escala. [5]

2.2.6. NDES

El servicio de inscripción de dispositivos de red *(**N**etwork **D**evice **E**nrollment **S**ervice)* es uno de los Servicios de Certificados de Directorio Activo *(***A**ctive **D**irectory **C**ertificate **S**ervices) asignables al Directorio Activo que implementa el Simple Certificate Enrollment Protocol (SCEP) y define la comunicación entre los dispositivos de red y una Autoridad de Registro (RA) para la inscripción de certificados. [6]

[5] https://en.wikipedia.org/wiki/Simple_Certificate_Enrollment_Protocol

[6] https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx

3. CAPÍTULO

Objetivos y alcance

En este capítulo se explicarán cuales son los objetivos más importantes de este proyecto, así como la manera de la que se han conseguido cumplir, mencionando también ciertos inconvenientes o trabas que se han encontrado por el camino y la manera en la que han sido solventados.

3.1. Objetivos

En esta sección se expondrán los objetivos principales de este TFG, los cuales fueron establecidos por el BCBL al comienzo del proyecto. Estos objetivos han sufrido varias modificaciones durante el transcurso y desarrollo del proyecto, por lo que esta sección recogerá únicamente los objetivos que han resultado ser definitivos.

3.1.1. Comparativa de las diferentes herramientas software disponibles

La idea del BCBL es utilizar algún software gratuito y de código libre para realizar el control de acceso a la red. Para ello se han propuesto dos herramientas por el administrador de redes de la empresa: PacketFence y openNAC. La selección de la herramienta no es algo arbitrario por lo que se ha requerido una comparativa de ambas herramientas para seleccionar la más adecuada.

3.1.2. Instalación del software en un servidor en producción

El plan principal del BCBL con este proyecto consiste en implementar un NAC en la red de producción de la empresa. Para ello se requiere preparar un servidor específico situado en esa red en producción donde se instalará el software seleccionado en la Comparativa Tecnológica, desde donde se realizará el control de acceso a la red.

3.1.3. Control de acceso basado en certificados

El objetivo principal del BCBL con este proyecto consiste en realizar una autenticación de los equipos que se conecten a la red. Para ello disponen de un servidor Windows Server 2008 R2 donde tienen instalados los servicios de Directorio Activo (donde se crean y almacenan cuentas de usuario, máquinas, servicios, etc.) y de Autoridad Certificadora (donde se crean y almacenan certificados para las diferentes máquinas, usuarios, servicios etc.).

Utilizando estos servicios se desea realizar una autenticación basada en los certificados que han sido previamente creados por la Autoridad Certificadora y que deberán de estar instalados en los equipos del BCBL. De esta manera se evita que cualquier usuario pueda utilizar el cable ethernet conectado a un equipo corporativo para conectarlo a un equipo personal y tener acceso a la red.

3.1.4. Despliegue automático de los certificados

Teniendo en cuenta el tipo de autenticación sobre la que quieren basar el control de acceso, será necesario un despliegue automático de los certificados para evitar tener que hacerlo manualmente.

3.2. Alcance

En esta sección se explicará cómo se han logrado completar los objetivos del punto anterior durante el desarrollo del proyecto. Para ello se tomará como referencia la EDT mostrada en la siguiente página.

Puede observarse que la EDT está descompuesta en tres ramas principales, dos de las cuales se refieren a la gestión del proyecto y a la parte académica del mismo. Estas dos ramas no se comentarán en esta sección, sino que se centrará en la parte del desarrollo del proyecto bajo la rama principal llamada *Servicio*.

Esta rama es la que recoge el desarrollo del proyecto en su totalidad y ha sido dividida en 4 subramas nombradas *"Estudio de tecnologías y herramientas"*, *"Implementación en entorno virtual controlado"*, *"Despliegue en subred real controlada"* y *"Planificación del despliegue global en la red"*.

En las siguientes páginas se explicará como se ha llevado a cabo el trabajo en dichas subramas para completar los objetivos del proyecto.

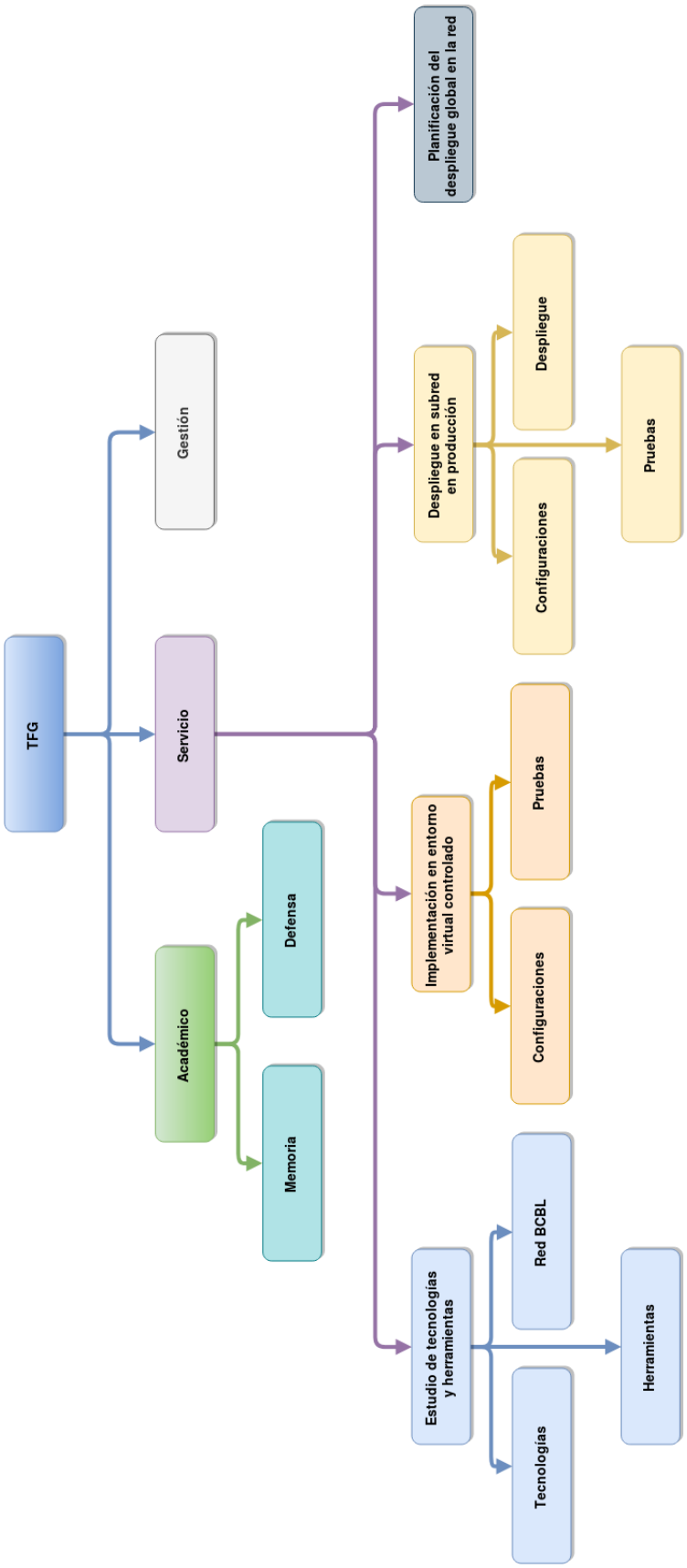


Figura 3.1: EDT del TFG

3.2.1. Estudio de tecnologías y herramientas

Tal y como se ha comentado en la sección de Objetivos, uno de los prerrequisitos para comenzar el desarrollo del proyecto era realizar una comparativa entre las siguientes herramientas de software libre para la realización de controles de acceso a la red: **PacketFence** y **openNAC**. Esta comparativa se realizó buscando información oficial de los desarrolladores de las herramientas y en diversos foros especializados tanto en herramientas de software libre como en controles de acceso a la red.

El documento referente a la mencionada comparativa entre PacketFence y openNAC puede encontrarse al final de este documento, en el Anexo A.

Además de esto, para la realización del proyecto ha sido obligatorio tener que realizar un estudio previo de las tecnologías que se han utilizado en el mismo. Estas tecnologías se refieren a diferentes protocolos, estándares y servicios que se han sido necesarios para el desarrollo del proyecto, tanto de forma activa como de forma pasiva.

El desglose de este estudio tecnológico se encuentra en el capítulo 4 *"Estudio de tecnologías y herramientas"*.

3.2.2. Implementación en entorno virtual controlado

Antes de realizar una instalación en un servidor implantado en una red en producción se creó un pequeño entorno de pruebas en una red de *testing* mediante una máquina virtual. Este entorno de pruebas fue creado con el único motivo de aprendizaje y familiarización con la herramienta para asegurar un mejor comportamiento a la hora de realizar el despliegue en una subred en producción.

Aprovechando este entorno de pruebas también se realizaron diferentes tipos de autenticación que podrían ser útiles para el BCBL en un futuro, como por ejemplo la autenticación basada en usuarios almacenados en el Directorio Activo. Esta es una buena opción para la asignación de VLANs basada en roles. Dicho de otra manera, pueden utilizarse diferentes atributos de las cuentas de usuario para realizar autenticaciones más concretas y añadir un rol específico a cada uno. Una vez que los usuarios están separados en diferentes grupos basados en roles, podrán asignarse diferentes VLANs a cada uno estos grupos.

3.2.3. Despliegue automático de los certificados

Una vez conforme con el manejo y comprensión de PacketFence, se decidió dar paso a la configuración para la autenticación basada en certificados, método elegido por el BCBL para la implementación final.

Para ello es requisito fundamental que cada equipo disponga de un certificado válido[1], y para ello es necesario realizar un despliegue de los certificados. Este despliegue se ha tenido que realizar únicamente para equipos que no dispongan de un Sistema Operativo Windows instalado, ya que al momento de comenzar con el proyecto, el Directorio Activo ya desplegaba dichos certificados a las máquinas incluidas en el dominio con el mencionado Sistema Operativo.

El despliegue automático de los certificados para equipos CentOS fue mucho más costosa y laboriosa de lo esperado, ya que tuvieron que estudiarse nuevas tecnologías y herramientas además de instalar un nuevo servidor Windows Server 2008, dado que la versión del servidor en funcionamiento en la red de producción no era compatible con uno de los protocolos necesarios para el despliegue.

Puede encontrarse un documento más extenso sobre la instalación del Windows Server así como de su configuración para el despliegue de certificados mediante el protocolo SCEP en el Anexo C.

3.2.4. Despliegue en subred en producción

Habiendo desplegado los certificados necesarios a todas las máquinas de prueba se procedieron a realizar autenticaciones basadas en certificados para estos equipos en la maqueta antes de pasarla a producción. Al comprobar que PacketFence se comportaba correctamente, se preparó un nuevo servidor ubicado en una red de producción para realizar una instalación/implementación desde cero.

Una vez que PacketFence estaba instalado y configurado se procedió a desplegar el control de acceso sobre la red del departamento de IT, a la cual hay conectados cinco equipos mediante dos switches. El despliegue fue un éxito y la red del departamento de IT fue reforzada con seguridad basada en el protocolo 802.1X con autenticación mediante certificados emitidos por la CA local del BCBL.

[1] Refiriéndose como válidos únicamente a los certificados emitidos por la CA local del BCBL.

3.2.5. Planificación del despliegue global en la red

Teniendo en cuenta que para realizar un despliegue de este tipo en una red en producción 24 horas al día hay que encontrar el momento oportuno, en el BCBL aún no tenían decidido cuando iba a realizarse dicho despliegue.

Sabiendo que terminaba mi estancia en la empresa, se me pidió realizar un despliegue en la red de IT como guía para que ellos pudieran realizarlo de manera global más adelante.

Además de esto, se realizó una planificación para el despliegue global junto al administrador de redes del BCBL. Esta planificación puede encontrarse en el capítulo 7 *"Planificación del despliegue global en la red"*.

4. CAPÍTULO

Estudio de tecnologías y herramientas

En este capítulo se explicarán con más detalle las tecnologías y herramientas que han sido necesarias utilizar para el desarrollo del proyecto.

4.1. Tecnologías

4.1.1. RADIUS

Antes de entrar en más detalle sobre el protocolo, es conveniente mencionar y conocer los diferentes elementos que toman parte en él:

Solicitante: Elemento hardware desde el que el usuario intenta acceder a la red. *(Ejemplo: un PC de escritorio)*

Servidor de Acceso a la Red o NAS: El solicitante intentará acceder a la red a través de este elemento. *(Ejemplo: un switch de acceso)*

Servidor RADIUS: Servidor con la capacidad de validar solicitudes de acceso.

Funcionamiento

El protocolo utiliza un método de cliente-servidor. Es decir, el servidor RADIUS no realizará ninguna acción hasta que un cliente NAS le haga una petición. El protocolo se basa en los siguientes pasos:

1- El solicitante realiza una petición de acceso a la red al NAS con el cual establece una comunicación punto a punto a nivel de enlace (PPP), enviando sus credenciales de usuario (o máquina).

2- El NAS actuará como cliente del Servidor RADIUS, al que reenviará los datos recibidos por el Solicitante mediante el protocolo RADIUS.

3- El Servidor RADIUS validará la información de autenticación recibida por el solicitante, con lo que obtendrá cierta información relevante acerca del cliente.

4- Si el servidor RADIUS autoriza el acceso a la red (o a una parte concreta de ella) al solicitante, responderá con un mensaje Access Accept, que contiene una serie de parámetros que caracterizan su conexión, como pueden ser la dirección IP o el ancho de banda.

5- El NAS responderá ante el solicitante dependiendo del mensaje que haya recibido del Servidor RADIUS, permitiendo o no el acceso a la red al mismo.

La siguiente imagen[1] representa el flujo de mensajes en un proceso de autenticación/autorización RADIUS con credenciales basadas en usuario y contraseña y mediante una conexión punto a punto entre el solicitante y el NAS.

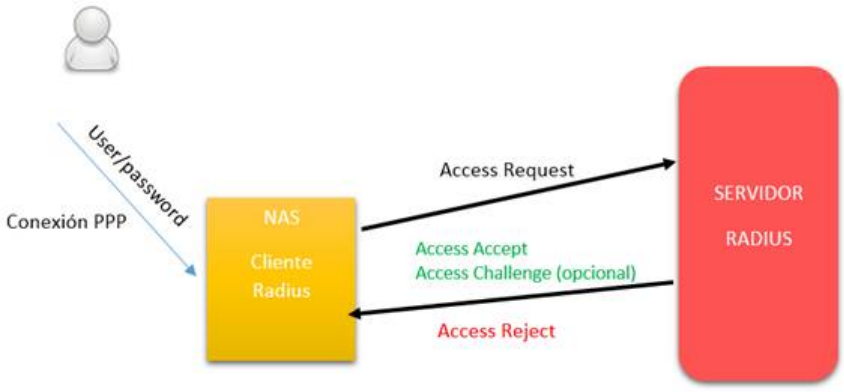


Figura 4.1: Flujo de mensajes en un proceso de autenticación/autorización RADIUS.

[1] https://www.incibe-cert.es/blog/protocolos-aaa-radius

4.1.2. 802.1X

Elementos del protocolo 802.1X

La autenticación 802.1X dispone de tres elementos básicos:

Solicitante: Es el dispositivo cliente (por ejemplo un ordenador portátil) que quiere acceder a la red. Este término puede referirse igualmente al software que está ejecutando el dispositivo y el encargado de enviar las credenciales al Autenticador.

Autenticador: Es el dispositivo en red (normalmente un switch ethernet o un punto de acceso inalámbrico) que se encargará de crear un enlace de datos entre el Solicitante y la misma red, siendo capaz de bloquear el tráfico entre ellos.

Servidor de Autenticación: Es un servidor de confianza capaz de recibir y responder peticiones de acceso a la red. Este servidor proveerá al Autenticador información acerca de si el cliente tiene permitido el acceso a la red o no, y varias configuraciones más que el Autenticador tendrá que aplicar a la hora de permitir el acceso a la red al Solicitante.

Protocolos utilizados y encapsulamiento de los mensajes

Este estándar utiliza los protocolos RADIUS y EAPoL para el flujo de mensajes entre los diferentes elementos del sistema.

El Solicitante y el Autenticador se comunican mediante tramas ethernet (también conocidas como tramas 802.3) que tendrán un *EtherType*[2] que corresponde al protocolo EAPoL *(EtherType=0x888e*). Para ello, el Solicitante necesita un software específico, ya que tiene que ser capaz de modificar la trama ethernet que va a enviar de tal forma que el Autenticador pueda reconocer la trama y saber que no se trata de una trama de ethernet corriente, sino que se trata de una comunicación a través del protocolo EAPoL.

La comunicación entre el Autenticador y el Servidor de Autenticación se realiza a través del protocolo RADIUS. Para ello, el Autenticador encapsula los datos recibidos por el Solicitante en un paquete RADIUS, el cual será encapsulado en un datagrama UDP que a su vez será encapsulado en un paquete IPv4 regular (*EtherType=0x800*) sobre una trama ethernet. Esta conversión se realiza teniendo en cuenta que el Autenticador y el Servidor de Autenticación pueden estar en diferentes localizaciones.

[2]Campo en la cabecera de la trama ethernet cuyo valor representa el protocolo en el que están encapsulados los datos que transporta.

La siguiente imagen[3] representa el encapsulamiento de los mensajes entre el Autenticador y el Servidor de Autenticación en una autenticación 802.1X.

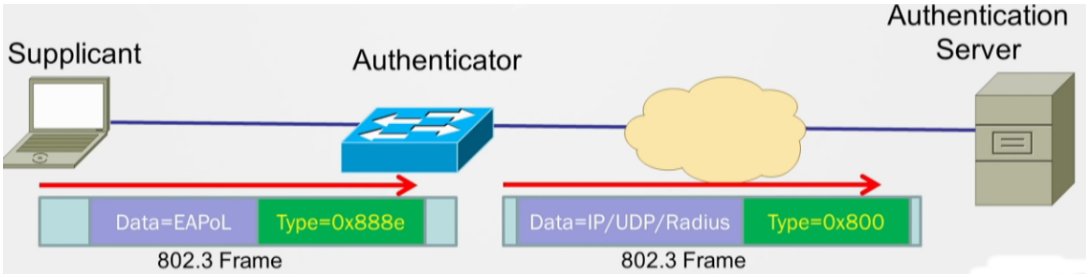


Figura 4.2: Encapsulamiento de los mensajes en una autenticación 802.1X.

Funcionamiento

El funcionamiento de este protocolo podría resumirse brevemente de la siguiente manera:

El Solicitante realiza una petición de acceso al Autenticador, pero no tendrá acceso a la red hasta que el Servidor de Autenticación lo haya verificado y autorizado y dé permiso al Autenticador para concederle el acceso. Para ello, el Solicitante tendrá que proporcionar las credenciales requeridas al Autenticador. Estas credenciales tienen que haber sido especificadas por el administrador de red, y pueden basarse en usuario y contraseña (para autenticar al usuario) o un certificado digital (para autenticar a la propia máquina).

Una vez el Autenticador recibe las credenciales las reenvía al Servidor de Autenticación para que decida qué tipo de acceso tiene permitido el Solicitante. Si el Servidor de Autenticación determina que las credenciales son correctas, informará de ello al Autenticador, quién permitirá el acceso del Solicitante a la red (o subred) a la que el Solicitante esté autorizado a conectarse.

[3] https://www.youtube.com/watch?v=3obzgqslnL8

4.2. Herramientas

4.2.1. PacketFence

En pocas palabras, podría decirse que PacketFence es un software de código libre diseñado para realizar controles de acceso en redes en producción. Cabe mencionar que para este proyecto se barajaba la posibilidad de utilizar openNAC, una herramienta de características similares utilizada para el mismo fin, y que puede encontrarse una comparativa entre ambas en el Anexo A.

Esta herramienta ha sido desarrollada por Inverse en el año 2009 y desde entonces no han dejado de ampliar y mejorar el software hasta convertirlo en una herramienta muy potente que permite centralizar y monitorizar todos los accesos a la red en un solo servidor.

Esta herramienta implementa diferentes servicios de código abierto para su funcionamiento, tales como Apache, MariaDB o FreeRADIUS entre otros, además de tener soporte con los principales fabricantes de switches y routers, tales como Cisco, Aruba, HP, etc.

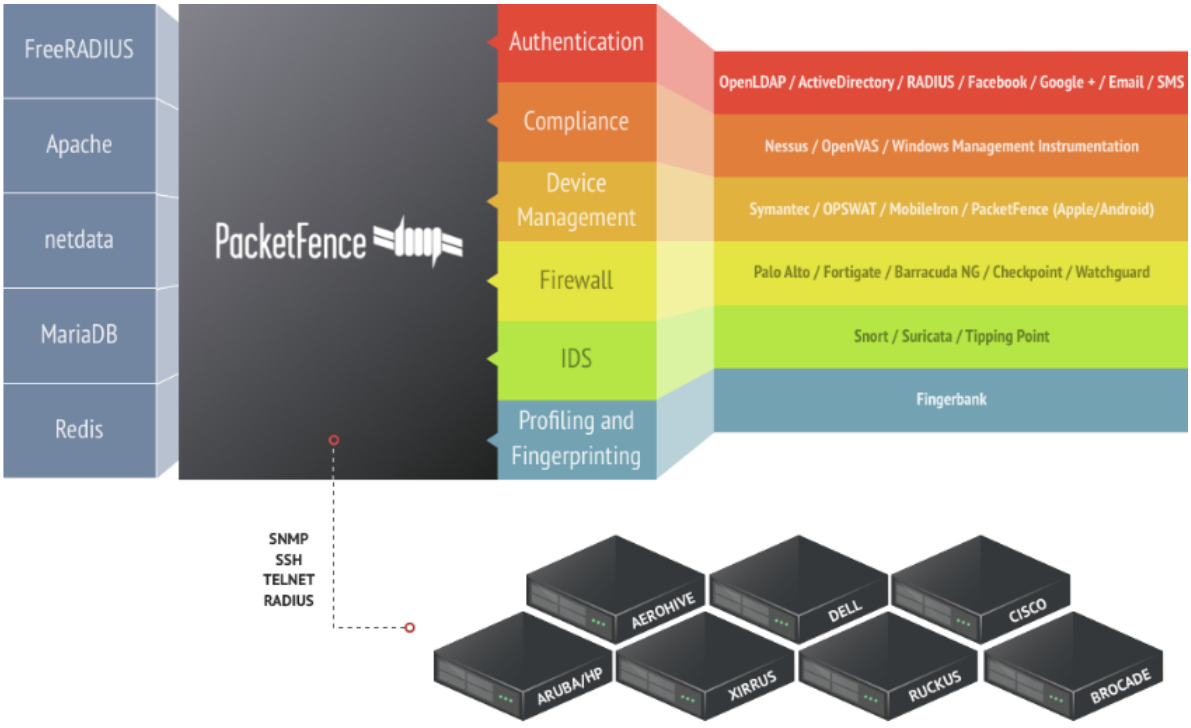


Figura 4.3: Arquitectura de componentes de PacketFence

Además de todo lo mencionado anteriormente, PacketFence también es capaz de trabajar con el Directorio Activo que esté en producción en la red, permitiendo hacer uso de las cuentas o certificados almacenados en él, ya que tiene la capacidad de realizar autenticaciones basadas en el protocolo 802.1X y también tiene soporte EAP-TLS.

El punto fuerte de PacketFence se trata de la asignación de diferentes VLANs mediante SNMP-traps sobre puertos configurados para autenticaciones basadas en 802.1X. Esto significa que PacketFence es capaz de asignar o reasignar en tiempo real diferentes VLANs para un mismo puerto de un punto de acceso.

Para realizar una implementación basada en la asignación de VLANs, el único cambio que tendremos que realizar sobre nuestra red, sera únicamente la de crear dos nuevas VLANs: *Registration* (VLAN que se asignará a los dispositivos mientras realizan la autenticación para acceder a la red) e *Isolation* (VLAN que se asignará a los equipos que no cumplan con ciertos requisitos y no cumplan la política ce acceso establecida).

PacketFence incorporará el servicio de DHCP dentro de estas dos VLANs, mientras que el servicio DHCP en las VLAN en producción de la red seguirá siendo el que se utilizaba hasta ese momento.

En conjunto con la asignación de VLANs pueden establecerse diferentes reglas, por ejemplo basadas en diferentes atributos de las cuentas de usuario almacenadas en el Directorio Activo, que asignarán un *Role* a los usuarios que se accedan a la red, pudiendo establecer una política de asignación de VLANs basada en estos *Roles*, lo que otorga un amplio abanico de posibilidades para el administrador de redes.

4.3. Estudio de la red local del BCBL

4.3.1. Distribución del centro

Este centro cuenta con una red local o LAN de tamaño medio. Esta red, entre otras cosas, comunica los diferentes departamentos del centro y ofrece diversos servicios.

El centro está repartido en 4 plantas dentro del mismo edificio:

- **Planta 0**: Aquí se encuentran tanto el clúster del *Data Center* como las instalaciones de los laboratorios donde se realizan diversos estudios, tales como estudios conductuales, *Eyetracking* (Registro de movimientos oculares), estudio de bebés, magnetoencefalografía, escáneres de resonancia magnética, etc.
- **Planta 1**: En esta planta podemos encontrar un auditorio, un comedor y una pequeña sala de reuniones. Hay instalados un par de Puntos de Acceso (***A**ccess **P**oint* o AC) Wi-Fi provenientes de un switch instalado en la Planta 0.
- **Planta 2**: La segunda planta se trata de la planta más grande del dentro. Aquí es donde están situados los puestos de trabajo de todos los investigadores del centro (la mayoría de los cuales lanzan procesos a ejecutar al *Data Center*), además del Departamento de Administración.
- **Planta 3**: En la tercera planta se encuentra únicamente el departamento de IT del BCBL.

4.3.2. Distribución de la red

El BCBL está distribuido en tres plantas pero parte de su LAN está situada en el edificio de IZFE, ubicado también en el parque tecnológico de Miramón. El *Switch Router* modelo *HP Procurve 5406zl* con el nombre AXON01 es el *core* de la red. Estos switches se conocen como *Core Switches* (switches troncales). Para evitar cortes de conexión en caso de AXON01 sufra algún problema, hay otro switch del mismo modelo llamado AXON02 conectado en el mismo punto para crear redundancia y evitar que toda la red quede incomunicada. Estos switches estan intercomunicados mediante un *trunk* de 2x10Gb en BaseT y tienen conexiones hacia la salida a Internet, a otro CPD que se encuentra en el dificio IZFE y a redes dedicadas a los servicios del BCBL (webservers, bases de datos, zona DMZ, etc.).

Al ser AXON01 y AXON02 *Core Switches*, están conectados a todo resto de componentes que forman la LAN. Para una mejor comprensión de la estructura física de la red, utilizaré las agrupaciones que pueden observarse en la Figura 4.4.

- **Floor 0**: En esta planta hay 3 switches para dar soporte a todos los equipos de laboratorio. Dos de ellos (AXON03 y AXON06) son del modelo *HP ProCurve 2810*. El switch restante (AXON21) es del modelo *HP ProCurve 2910*. Este switch incorpora la característica conocida como PoE (***P**ower **o**ver **E**thernet* o alimentación a través de ethernet), la cual ha permitido conectar los 4 APs Wi-Fi de las plantas 0 y 1 sin necesidad de conectarlos a la corriente, ya que será el mismo switch el que alimente el hardware mediante el cable de conexión ethernet.

  Las conexiones desde los *Core Switches* hasta los switches de esta planta se realizan mediante dos *trunk* de 2x1Gb BaseT, uno por cada *Switch Core*.

- **Floor 2**: De manera similar que en la Planta 0, en esta planta podemos encontrar 4 switches para dar soporte a todos los equipos de los investigadores y a los del departamento de administración. 3 de estos switches (AXON04, AXON05 y AXON09) son del modelo *HP ProCurve 2810*, mientras que el cuarto switch (AXON22) es del modelo *HP ProCurve 2910*, también utilizado para alimentar 8 APs (uno de ellos ubicado en la planta 0 y los 7 restantes ubicados a la planta 2) Wi-Fi vía cable ethernet.

  Igual que en el caso de la Planta 0, las conexiones desde los *Core Switches* hasta los switches de esta planta se realizan mediante dos *trunk* de 2x1Gb BaseT, uno por cada *Switch Core*.

- **IT (Floor 3)**: El departamento de IT está ubicado en la tercera planta del edificio. En esta planta podemos encontrar un único *Switch Router* (AXON18) del modelo *HP ProCurve 3500yl* para dar soporte al departamento. La razón de tener un switch de este tipo instalado en el departamento es porque ha sido reutilizado.

  Al igual que en las Plantas 0 y 2, las conexiones desde los *Core Switches* hasta los switches de esta planta se realizan mediante dos *trunk* de 2x1Gb BaseT, uno por cada *Switch Core*.

- **Clúster - DC BCBL**: Los switches de acceso al *Data Center* (AXON14 y AXON15) son del modelo *Fujitsu Brocade VDX 6730*. Estos switches tienen la opción de utilizar la tecnología *FibreChannel*, pero no está siendo utilizada.

  La conexión entre los *Core Switches* y los switches del clúster son dos *trunks* de 2x10Gb de fibra, uno por cada *Switch Core*.

- **IZFE**: Tal y como se ha comentado en la página anterior, parte de la LAN del BCBL está ubicada en un edificio situado cerca del centro. La parte de la LAN de situada en el edificio IZFE se compone de 4 elementos, dos routers (AXON19 y AXON20) *HP Aruba 3810 16* y dos switches (AXON07 y AXON08) *HP Aruba 2930* que dan soporte a los servidores que el BCBL aloja en este edificio.

  Las conexiones entre los *Core Switches* y los routers del edificio de IZFE, tanto la interconexión entre estos routers, como la conexión con los switches del mismo edificio son mediante enlaces de 10Gb de fibra.

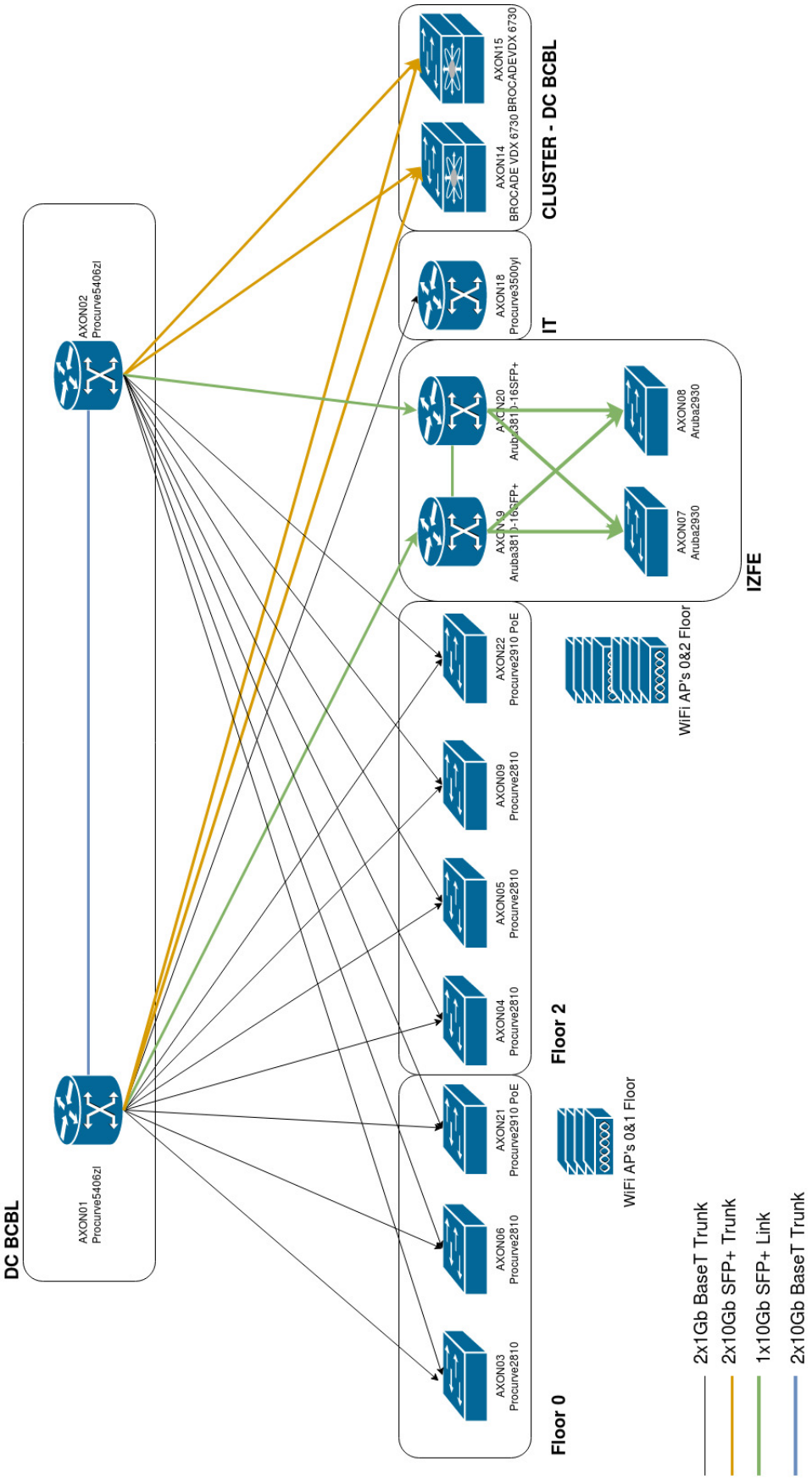


Figura 4.4: Mapa físico de la LAN del BCBL

5. CAPÍTULO

Implementación en entorno virtual controlado

Para llevar a cabo esta implementación en un entorno virtual controlado, se ha utilizado un hipervisor llamado *vSphere*. El BCBL dispone de un servidor de virtualización donde hay una gran cantidad de máquinas virtuales que ofrecen diferentes servicios, como por ejemplo un servidor SFTP, unos cuantos proxys, la Wiki del centro, etc. Este es un entorno perfecto para la instalación de la herramienta y de la realización de las primeras pruebas con ella, sin riesgo a perjudicar para nada a la red del centro y con opciones muy útiles como la de los *snapshot*s, que permiten a la máquina volver a un estado anterior que hayamos guardado, a modo de backup.

La idea es crear una pequeña red virtual utilizando esta herramienta. Se creará una máquina virtual donde se instalará la herramienta seleccionada, y se creará también un *vSwitch* donde se definirán las diferentes VLANs que serán necesarias para el correcto funcionamiento de la herramienta y poder simular un entorno ”real“ aunque sea en pequeña escala.

Una vez conseguido el objetivo de esta fase, el cual únicamente consistirá en la familiarización con la herramienta y sobre todo con el abanico de configuraciones que ofrece, y la implementación de una medida de seguridad basada en puertos mediante el estándar 802.1X. El acceso a la red se realizará mediante una autenticación de usuario y contraseña utilizando credenciales de usuario de BCBL. Aunque el producto final no vaya a consistir en una autenticación de usuario, se ha decidido hacerlo de esta manera para la familiarización con la herramienta, ya que se trata de una configuración más sencilla para la autenticación.

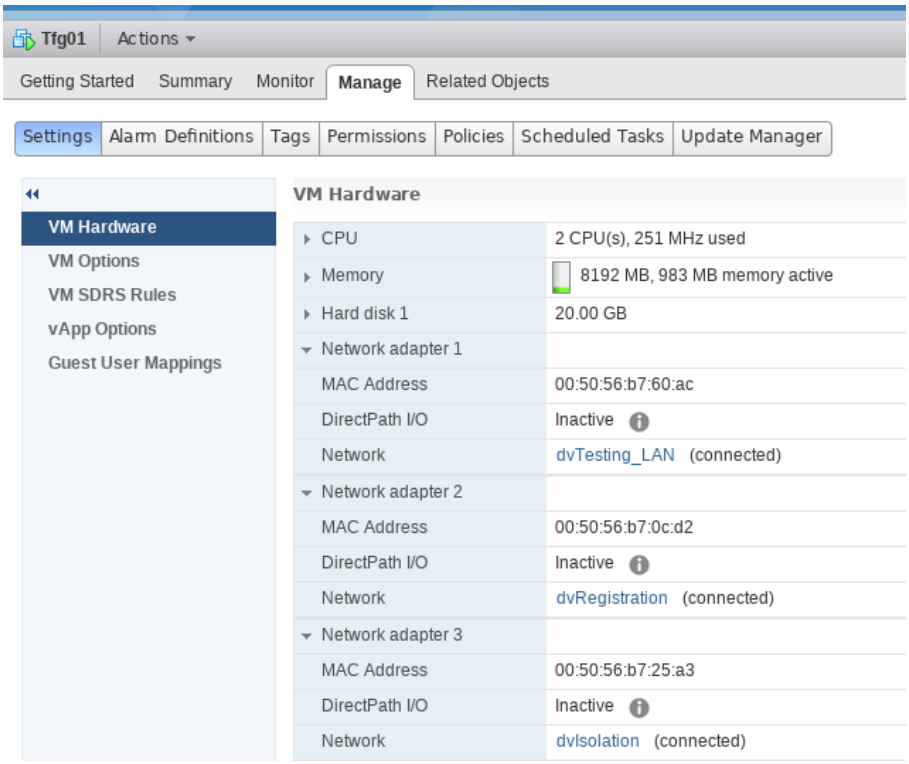


Figura 5.1: Hardware y conexiones de la máquina virtual Tfg01 en *vSphere*.

Como puede observarse en la figura superior (*Figura 5.1*), se ha creado una máquina virtual con el nombre **Tfg01**. Esta máquina está conectada a tres diferentes VLANs mediante tres interfaces de red. Esto se debe a que una de las ideas principales del NAC se basa en la asociación de VLANs a los equipos que tengan acceso a la red, es decir, cada máquina será dirigida a una VLAN dependiendo del rol de la misma, o dicho de otra manera, dependiendo del departamento al que pertenezca.

Este documento no repara en la instalación del software, pero puede encontrarse la guía de instalación y configuración inicial de PacketFence en una máquina CentOS 7 puede encontrarse en el Anexo B.

5.1. Configuración de PacketFence para la autenticación de usuarios

El primer paso para realizar una autenticación de usuarios es el de conectar PacketFence con el Directorio Activo donde están almacenadas todas las cuentas de usuario del BCBL. Este Directorio Activo está instalado en un servidor Windows Server 2008 R2 Standard que también ofrece servicio como Autoridad Certificadora de todos los certificados que se emitirán dentro del BCBL, ya sean de máquinas o de usuarios.

Para conectar PacketFence con el Directorio Activo, lo primero que tendremos que hacer será añadir el *host* donde está instalado el software al dominio del BCBL. Para ello tenemos que acceder a la sección *Configuration –>Policies and Acces Control –>Domains –>Active Directory Domains* y hacer click sobre el botón "ADD DOMAIN". Aparecerá una ventana con un formulario donde tendremos que ingresar los datos acerca del dominio. Estos son los datos que se han ingresado en el formulario:

- Workgroup: *BCBL*
- DNS name of the domain: *bcbl.local*
- Active Directory server: *acc.bcbl.local*
- DNS server(s): *192.168.X.X,192.168.X.X,192.168.X.X*
- OU: *Computers*

Además de estos datos son necesarias las credenciales de un administrador del dominio para poder ingresar en él, y para ello se han utilizado mis credenciales personales del BCBL. Una vez ingresados todos los datos correctamente, tenemos que hacer click sobre el botón "SAVE AND JOIN" y obtendremos un mensaje de confirmación.

Una vez el *host* ya está en el dominio, tenemos que hacer click sobre la pestaña que dice "REALMS", y una vez ahí, hacer click sobre "DEFAULT" y "LOCAL" y asociar a estos el dominio que acabamos de crear.

PacketFence dispone de una característica que se basa en el *Rol* del usuario autenticado, al cual se le podrá asignar una VLAN específica. La creación de los diferentes *Roles* se realiza en *Configuration –>Policies and Acces Control –>Roles*. Haciendo click sobre el botón "ADD ROLE" aparecerá una pequeña ventana donde tendremos que definir un nombre, una descripción y establecer un número máximo de nodos que podrán registrarse con el *Rol* en cuestión asignado.

En este punto se han definido dos *Roles*: Users y IT. Ambos *Roles* se han definido sin número máximo de nodos, ya que estamos en un entorno de pruebas y será irrelevante en esta fase del proyecto.

En este punto podremos añadir el Directorio Activo para poder utilizarlo como fuente de autenticación. Para ello tenemos que navegar hasta *Configuration –>Policies and Acces Control –>Authentication Sources* y hacer click sobre el botón *ADD SOURCE –>Internal –>AD*.

En esta ventana se configuran las reglas que van a utilizarse para la autenticación. Los datos ingresados han sido los siguientes:

- Name: *ACC*
- Description: *Authentication against AD*
- Host: *acc.bcbl.local:389*
- Base DN: *DC=bcbl,DC=local*
- Scope: *Subtree*
- Username Attribute: *sAMAccountName*
- Bind DN: *CN=jcaballero,OU=IT,OU=BCBL,DC=bcbl,DC=local*
- Password: **********

En la parte inferior de la ventana podemos encontrar la sección de definición de reglas, tanto las reglas de autenticación simple, como las reglas de autenticación de administración. Se han definido dos reglas de autenticación para diferenciar a los trabajadores del departamento de IT del resto de usuarios. Esta diferenciación se ha definido para para comprobar que la asignación de VLANs por *Roles* funciona correctamente. Las reglas que se han definido son las siguientes:

Authentication Rules:

1. IT_Staff
   - Name: *IT_Staff*
   - Description: *Authentication for BCBL IT Staff*
   - Matches: *All*
   - Conditions:
     a) *department equals IT*
   - Actions
     a) Role = *IT*
     b) Access duration = *12 hours*
2. BCBL_Users
   - Name: *BCBL_Users*
   - Description: *BCBL User account authentication*
   - Matches: *All*
   - Conditions:
     a) *distinguishedName ends DC=bcbl,DC=local*
   - Actions
     a) Role = *Users*
     b) Access duration = *12 hours*

Administration Rules:

1. BCBL_Admins
    - Name: *PacketFence_Admins*
    - Description: *BCBLian PacketFence Admins*
    - Matches: *All*
    - Conditions:
        a) *cn equals jcaballero*
    - Actions
        a) *Access level = ALL*

Cabe mencionar que en el momento de la autenticación del usuario, éste será contrastado con las reglas en orden ascendente. Siguiendo el ejemplo anterior primero se comprobará si el usuario que está siendo autenticado pertenece al departamento de IT, en cuyo caso se le asignaría el *Role* IT, y en caso de no hacerlo, se comprobará si el usuario pertenece al dominio del BCBL, en cuyo caso se le asignará el *Role* User. Si el usuario ha cumplido alguna de las reglas denominadas *Authentication Rules*, el usuario será contrastado con las reglas incluidas en *Administration Rules* para saber si es un usuario corriente o tiene derechos de administrador en PacketFence.

Antes de hacer click sobre el botón “SAVE” y guardar la configuración, PacketFence tiene que comprobar que la información añadida sobre el dominio y la dirección del Directorio Activo (entre otras cosas) son correctas. Para ello, tendremos que hacer click sobre el botón “TEST” que aparece tras el recuadro de *Password*.

Los datos para poder establecer unas reglas coherentes han sido recogidos directamente de las cuentas existentes en el Directorio Activo del BCBL. Estos son algunos de los atributos que pueden verse sobre mi cuenta personal *jcaballero* del BCBL en el Directorio Activo:

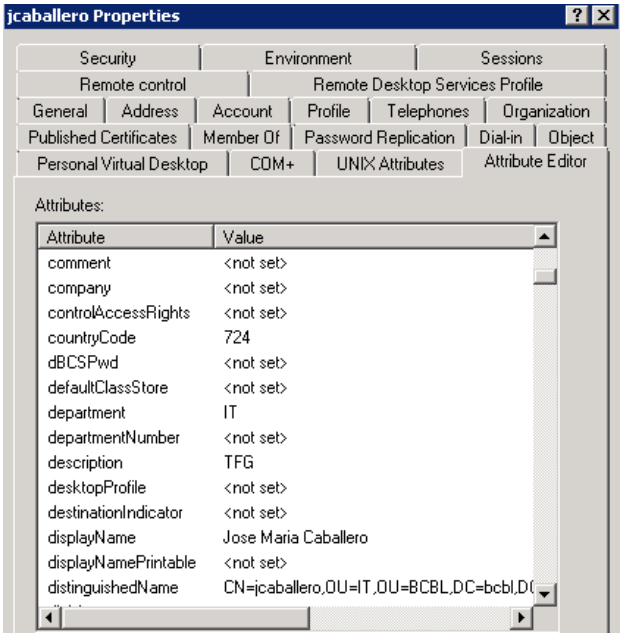


Figura 5.2: Atributos de la cuenta *jcaballero* en el Directorio Activo

Para asegurar la correcta adición del Directorio Activo a PacketFence y la correcta lectura de los atributos de las cuentas, se procederá a comprobar que estas cuentas pueden ser autenticadas correctamente. Para ello PacketFence dispone de un comando para la comprobación de cuentas frente a diferentes fuentes de autenticación. Primero comprobaremos la autenticación de un usuario no perteneciente al departamento de IT. El uso del comando se realiza de la siguiente manera:

```
cd /usr/local/pf/bin/
./pftest authentication [username] [password] [authentication source]
```

Obviamente, no conocemos la contraseña del usuario a autenticar, pero añadiendo el parámetro `[password]` como un string vacío, podemos comprobar que la autenticación funciona aunque aparezca un error de *"Invalid login or password"*.

Autenticación de la cuenta de usuario “ejuaristi” contra la fuente de autenticación “ACC”:

```
[root@TFG01 bin]# ./pftest authentication ejuaristi "" ACC
Testing authentication for "ejuaristi"

Authenticating against 'ACC' in context 'admin'
  Authentication FAILED against ACC (Invalid login or password)
  Matched against ACC for 'authentication' rules
    set_role : Users
    set_access_duration : 12h
  Did not match against ACC for 'administration' rules
```

Figura 5.3: Autenticación de la cuenta de un usuario no perteneciente al departamento de IT y sin derechos de administrador

Podemos comprobar como el usuario ha sido correctamente autenticado contra la fuente de autenticación ACC. Además puede observarse como se le ha asignado el *Role* Users y una duración del acceso de 12 horas, tal y como se había especificado en las reglas de autenticación en ACC.

Para la comprobación de la autenticación de usuarios del departamento de IT con permisos de administración se ha realizado la misma comprobación pero con mi cuenta personal:

```
[root@TFG01 bin]# ./pftest authentication jcaballero "" ACC
Testing authentication for "jcaballero"

Authenticating against 'ACC' in context 'admin'
  Authentication FAILED against ACC (Invalid login or password)
  Matched against ACC for 'authentication' rules
    set_role : IT
    set_access_duration : 12h
  Matched against ACC for 'administration' rules
    set_access_level : ALL
```

Figura 5.4: Autenticación de la cuenta de un usuario perteneciente al departamento de IT y con derechos de administrador

Puede comprobarse como se le ha asignado el *Role* adecuado (IT), además de la duración del acceso establecido anteriormente (12h). También podemos comprobar como ha coincidido con las *“Administration Rules”* y le ha asignado el nivel de acceso ALL tal y como había sido configurado.

Configuración del Switch

En el listado del hardware soportado por PacketFence no aparece el modelo del switch que se utilizará en el BCBL para la autenticación. El switch que se utilizará es el modelo *HP ProCurve 2810-48g*. Aunque este switch no aparece en esta lista, buscando información en diversos foros de PacketFence se ha encontrado una entrada de un usuario que dice haberlo configurado como un *HP ProCurve 2600* con muy buenos resultados, por lo que se ha decidido probar esta solución.

HP Procurve 2500 Series	✔ SNMP	✔ MAC Auth	✔ 802.1X
HP Procurve 2600 Series	✔ SNMP	✔ MAC Auth	✔ 802.1X
HP Procurve 2920 Series		✔ MAC Auth	✔ 802.1X
HP Procurve 3400cl Series	✔ SNMP		
HP Procurve 4100 Series	✔ SNMP		
HP Procurve 5300 Series	✔ SNMP	✔ MAC Auth	✔ 802.1X
HP Procurve 5400 Series	✔ SNMP	✔ MAC Auth	✔ 802.1X

Figura 5.5: Listado de switches HP ProCurve soportado por PacketFence

PacketFence ofrece una guía para configurar diferentes modelos de switches, en la que está incluida la configuración para los switches *HP ProCurve 2600 Series*, por lo que se utilizará dicha guía como referencia para configurar el switch *HP ProCurve 2810-48g*, buscando similaridades entre los comandos que aparecen en la guía de PacketFence y los disponibles en nuestro switch. La configuración que se ha realizado en el switch es la siguiente:

Definir el *host* donde está instalado el servidor RADIUS:

```
radius-server host 192.168.70.25 key "xxxxxxxxx"
```

Definir el *host* y la configuración SNMP:

```
snmp-server host 192.168.70.25 public not-info
```

Configurar autenticación:

```
aaa authentication port-access eap-radius
```

Configurar la seguridad basada en puertos:

```
port-security T1 learn-mode port-access action send-alarm
```

Configuración del puerto:

```
aaa port-access authenticator 1
aaa port-access authenticator 1 client-limit 1
aaa port-access authenticator active
aaa port-access mac-based 1
aaa port-access mac-based 1 addr-moves
aaa port-access mac-based 1 reauth-period 14400
aaa port-access 1 controlled-direction in
```

Notas:

Las keys utilizadas durante la configuración del switch aparecerán como "xxxxxxxxx" para mantener la privacidad del BCBL.

Únicamente se ha configurado el puerto 1 del switch para realizar autenticaciones mediante el protocolo 802.1X.

Un requisito imprescindible para que PacketFence sepa como manejar una conexión entrante ya sea cableada o mediante WiFi, es el de crear un Perfil de Conexión *(Connection Profile)*. En este caso, procederemos a crear un nuevo *Connection Profile* para utilizar la fuente de autenticación basada en el Directorio Activo creada anteriormente, y hacer que PacketFence registre de modo automático cualquier dispositivo que se autentique correctamente mediante el protocolo 802.1X.

Para ello tendremos que navegar a *Configuration –>Policies and Access Control –>Connection Profiles* y hacer click sobre *Add Profile*, donde añadiremos la siguiente información:

- Profile Name: *802.1x*
- Automatically register devices *checked*
- Filters: *If any of the following conditions are met:*
    - Connection Type: *Ethernet-EAP*
- Sources: *ACC (fuente de autenticación creada en pasos anteriores)*

El resto de configuraciones se han dejado con las opciones que PacketFence trae por defecto, ya que no se ha visto necesario cambiar ninguna de ellas.

El último paso para terminar la configuración de PacketFence y autenticar usuarios existentes en el Directorio Activo del dominio, es hacerle saber a PacketFence sobre la existencia del switch que se ha configurado previamente. Para ello tendremos que acceder a *Configuration –>Policies and Acces Control –>Network –>Devices –>Switches* y hacer click sobre el botón *ADD SWITCH –>Default*. Aparecerá una ventana donde tendremos que introducir cierta información acerca del switch:

- En la pestaña *Definition*:
  - IP Address/MAC: *192.168.221.23*
  - Type: *HP ProCurve 2600 Series*
  - Description: *axon23*
  - Mode: *Production*
- En la pestaña *Roles*
  - Role by VLAN ID: *checked*
  - registration: *75*
  - isolation: *76*
  - REJECT: *-1*
  - IT: *70*
  - Users: *77*
- En la pestaña *RADIUS*
  - Secret Passphrase: *xxxxxxxxx*
- En la pestaña *SNMP*
  - Community Read: *Public*
  - Community Write: *Private*

Notas:

La VLAN -1 hace referencia a una VLAN inexistente, por lo que el usuario no será asignado a ninguna VLAN quedando excluido de la red.

Se ha definido la VLAN 77 como la VLAN de usuarios, simulando la VLAN a la que realmente tienen acceso los usuarios del BCBL.

5.2. Configuración del cliente para autenticación de usuarios

La configuración en el cliente varía dependiendo del Sistema Operativo que tenga instalado. Ya que se trata de una implementación de pruebas, se considerará válido si se consiguen los resultados esperados haciendo las pruebas pertinentes en un único Sistema Operativo, que en este caso será Windows 7 ya que es el Sistema Operativo más utilizado por los usuarios en el BCBL.

Para realizar dichas pruebas se ha utilizado un ordenador portátil de la marca *Lenovo*, prestado por el departamento de IT del BCBL.

El primer paso en la configuración del equipo para la autenticación de usuarios mediante el protocolo 802.1X consiste en activar el servicio *WiredAutoConfig*. Para ello tendremos que acceder al panel de control de servicios de Windows, hacer doble click sobre el servicio que se quiere activar, seleccionar *Startup type: Automatic* de la lista desplegable y hacer click sobre el botón *"Start"* para activar el servicio.

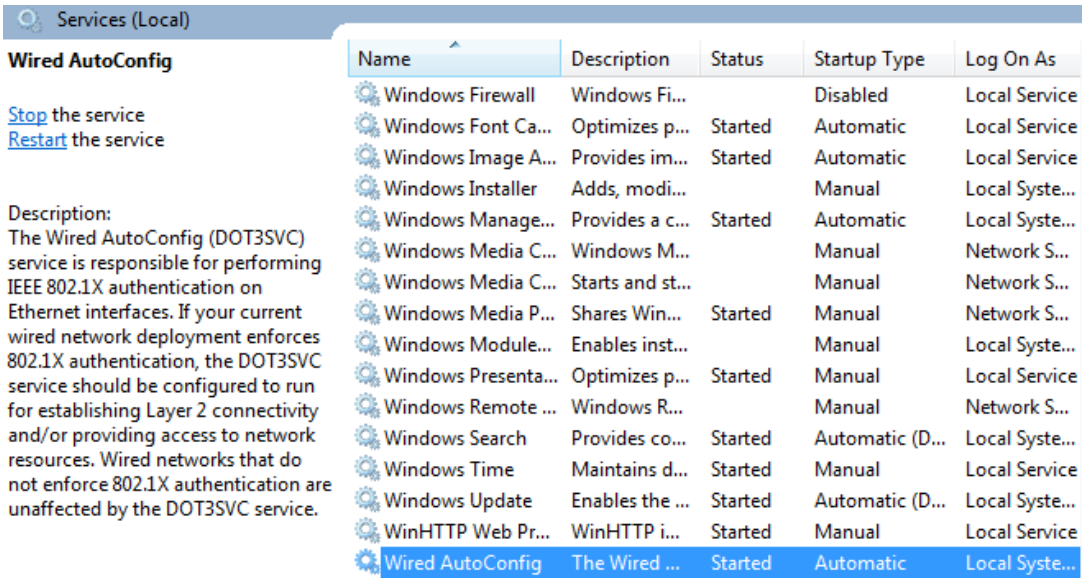


Figura 5.6: Gestor de servicios de Windows

Después de activar el servicio *WiredAutoConfig*, tenemos que abrir la ventana de Propiedades de la interfaz LAN que vamos a utilizar para acceder a la red. En la pestaña de *Authentication* tendremos que activar la opción *"Enable IEEE 802.1x authentication"*. Una vez hecho esto, tendremos que seleccionar *"Choose authentication method: Microsoft Protected EAP (PEAP)"* de la lista y pulsar sobre el botón *Settings*.

En esta ventana tendremos que asegurarnos de que *"Validate server certificate"* está activado, y de que la opción *"Select Authentication Method: Secured password (EAP-MSCHAP v2)"* está seleccionada para después hacer click sobre el botón *Configure* y desmarcar la casilla *"Automatically use my Windows logon name and password (and domain if any)"*.

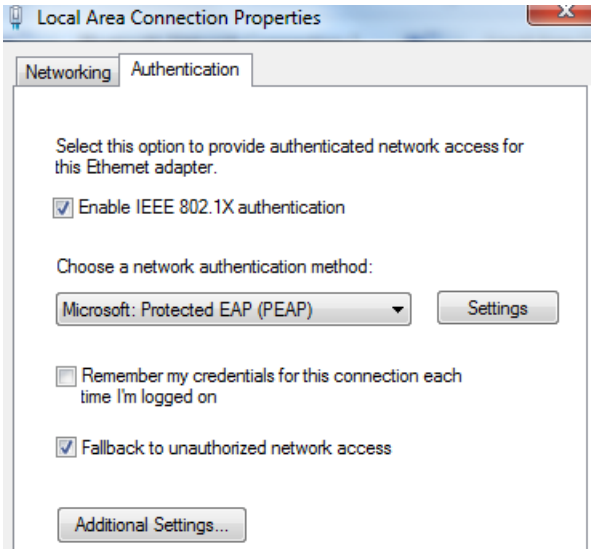


Figura 5.7: Propiedades de la interfaz de para la conexión LAN

Como último paso tendremos que asegurarnos de que dentro de la ventana de configuración que aparece tras pulsar el botón *Additional Settings...* está seleccionada la opción *"Specify authentication mode"* y en la lista desplegable está seleccionada la opción *"User authentication"*.

5.3. Testeo de la autenticación de usuarios

Como primera prueba se va a intentar acceder a la red utilizando un usuario del departamento de IT (más concretamente mi usuario personal). Para ello conectamos vía ethernet la interfaz configurada para la autenticación en el switch (interfaz 1) a la interfaz configurada para conexión LAN en el equipo Windows. En pocos instantes deberá de aparecer un mensaje como el de la siguiente imagen:

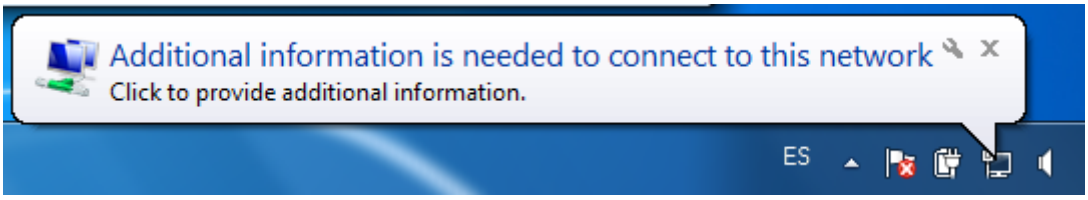


Figura 5.8: Mensaje sobre la necesidad de información adicional para autenticación en la red

Al hacer click sobre dicho mensaje, aparecerá una ventana emergente donde hay que introducir unas credenciales válidas para el dominio.

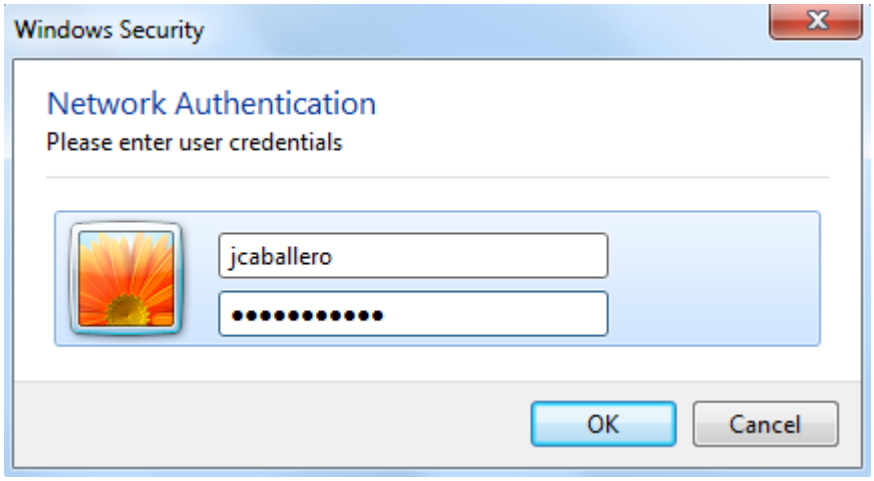


Figura 5.9: Ventana emergente de ingreso de credenciales para autenticación

Si antes de enviar las credenciales hacemos click derecho sobre la interfaz y después sobre *Status –>Details...*. Podrás observarse lo siguiente:

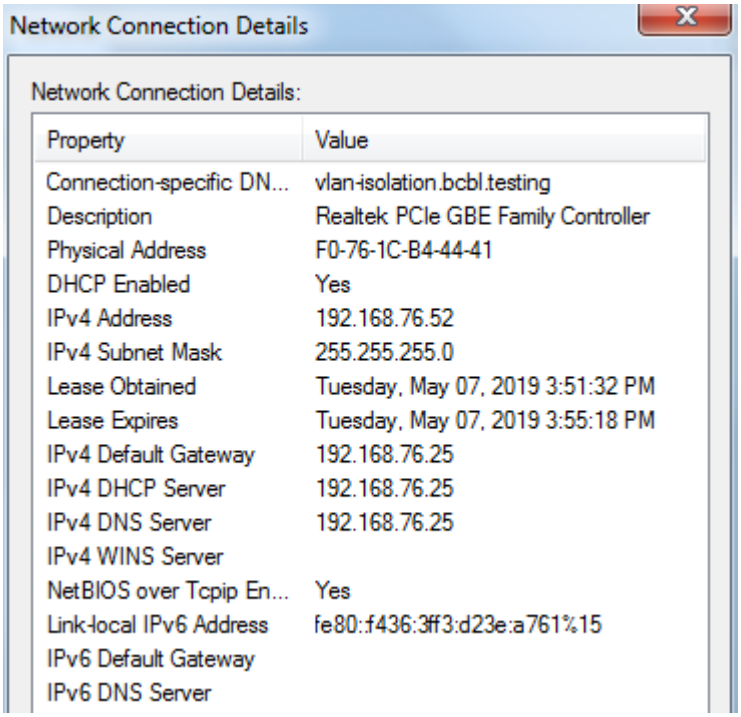


Figura 5.10: Detalles sobre el estado de la interfaz que intenta acceder a la red (pre-auth)

Puede observarse como la IP asignada al equipo es la 192.168.76.52. Esta IP pertenece a la VLAN 76 (Isolation) como puede confirmarse en la primera línea donde dice *"vlan-isolation.bcbl.testing"*. Además, también puede comprobarse que tanto el servidor IPv4 DNS, el servidor IPv4 DHCP y el *Default Gateway* del equipo tienen la misma dirección IP, concretamente la dirección IP de la interfaz **ens192** (Isolation): 192.168.76.25, lo que significa que los servicios de DNS y DHCP proporcionados por PacketFence funcionan correctamente.

Una vez introducidas unas credenciales válidas, puede comprobarse el cambio en la ventana de detalles sobre el estado de la interfaz:

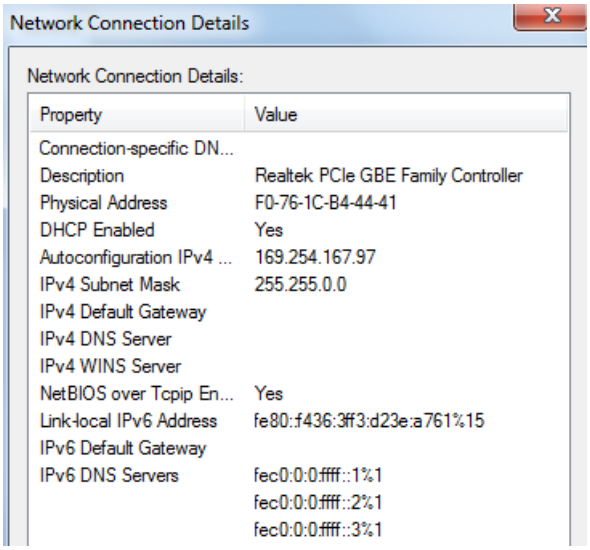


Figura 5.11: Detalles sobre el estado de la interfaz con acceso a la VLAN45

A primera vista puede parecer que no ha funcionado correctamente, ya que falta información acerca de los servidores DNS y DHCP, sobre la VLAN a la que se encuentra conectado el equipo en este momento, etc., pero la verdad es que ha funcionado correctamente. El problema reside en que la VLAN que se ha asignado al equipo es la VLAN 70, tal y como se había configurado en el último paso de la configuración del switch, y esta VLAN es no es más que una VLAN de prueba donde no hay servidores DHCP ni DNS, únicamente unas pocas máquinas virtuales con IPs estáticas. Para comprobar que todo lo comentado es cierto, se realizará una conexión ssh al switch **axon23** y se ejecutará el comando `sh vlan port 1`, con lo que se obtendrá el siguiente resultado por consola:

```
Status and Counters - VLAN Information - for ports 1

 802.1Q VLAN ID Name         Status       Jumbo
 -------------- ------------ ------------ -----
 70             VLAN70       Port-based   No
```

Figura 5.12: Output de la ejecución del comando `sh vlan port 1`

Viendo que el resultado de la ejecución del comando `sh vlan port 1` es precisamente la VLAN 70, se puede concluir con que PacketFence está funcionando correctamente.

Aún así, para asegurar la correcta ejecución de PacketFence, se va a proceder a cambiar la VLAN asignada al *Role* de IT. Concretamente, se le va a asignar la VLAN 45, VLAN correspondiente al departamento de IT. Esta VLAN está en funcionamiento y es una VLAN a la que el switch tiene acceso, por lo que es una buena alternativa para testear.

Para cambiar la VLAN asignada al *Role* de IT, es necesario acceder a la interfaz web de PacketFence y navegar hasta *Configuration –>Policies and Access Control –>Switches*. Una vez aquí, hacer click sobre el identificador del switch que había sido configurado en pasos anteriores y en la pestaña *"Roles"* cambiar el valor de IT por el valor 45. Una vez terminada la configuración hay que hacer click en el botón *"SAVE"* para salvar los cambios realizados.

Una vez cambiada la configuración de PacketFence hay que volver a conectar el ordenador a la red mediante un cable ethernet y volver a introducir unas credenciales válidas. Una vez accedido a la red se pueden volver a observar los detalles del estado de la interfaz de red para ver las diferencias con el caso anterior:

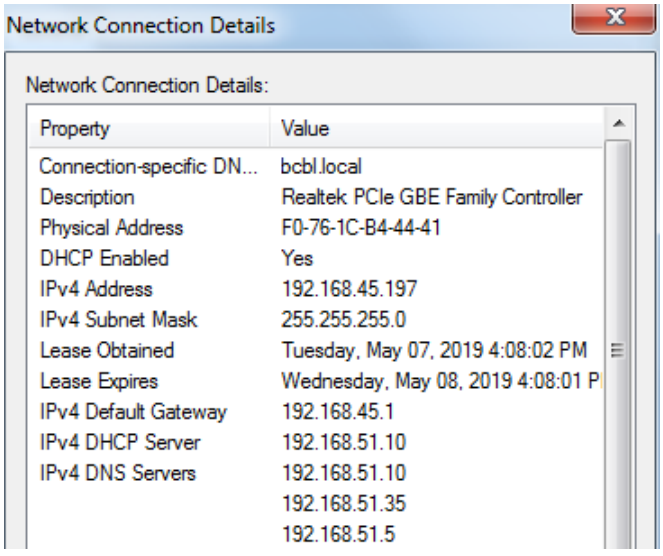


Figura 5.13: Detalles sobre el estado de la interfaz con acceso a la VLAN45

Puede observarse que la IP asignada (192.168.45.197) corresponde a la VLAN 45, y que los servidores DHCP y DNS son los que actúan sobre la red en producción del BCBL, por lo que se puede concluir con que PacketFence está funcionando correctamente.

En la interfaz web de PacketFence también pueden encontrarse datos interesantes acerca de como ha funcionado la autenticación por medio de RADIUS. Navegando a la pestaña *"Auditing"* puede encontrarse un listado con todos los equipos que han intentado acceder a la red y diversos detalles sobre el tipo de conexión y autenticación han realizado, así como detalles sobre el switch (***N**etwork **A**ccess **S**switch* o *NAS*) con el que ha realizado el intercambio de mensajes mediante el protocolo RADIUS.

Se puede acceder a la información acerca de la conexión/autenticación realizada por el nodo en cuestión haciendo click sobre el icono "+" que aparece en la primera columna de cada intento de conexión.

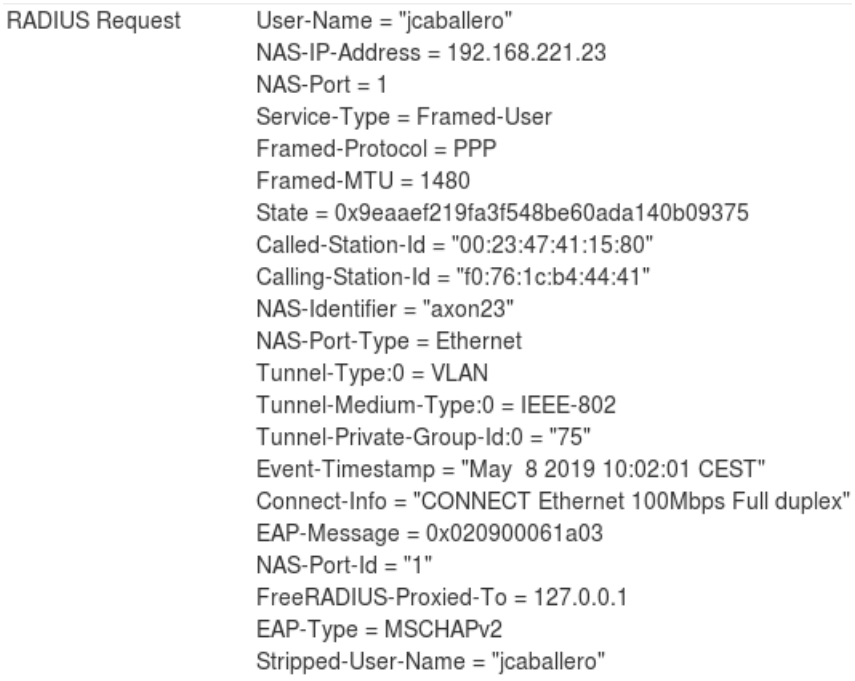


Figura 5.14: Detalles sobre los mensajes RADIUS intercambiados en la autentición de un usuario

Además de la información acerca de la conexión RADIUS también hay una pestaña llamada *Switch Information*, donde aparece información acerca del switch que realizó la autenticación para el nodo sobre el que estamos mirando. Dentro de esta pestaña puede encontrarse la dirección IP del switch, el puerto/interfaz sobre el que se realizó la autenticación, el tipo de conexión que se utilizó, dirección MAC del switch, etc.

Además de esto, en la pestaña *"Nodes"* puede encontrarse la información que PacketFence ha guardado sobre el equipo que ha intentado conectarse.

Status	Online/Offline	MAC Address	Computer Name	Owner	IP Address
unregistered	unknown	00:50:56:b7:0c:ce	TFG02	default	192.168.76.103
unregistered	unknown	00:50:56:b7:71:08	TFG02	default	192.168.75.160
registered	unknown	f0:76:1c:b4:44:41	BCBL-Lenovo03	jcaballero	192.168.76.82

Figura 5.15: Datos sobre los equipos que han intentado acceder a la red (pestaña *Nodes*)

Si se hace click sobre la dirección MAC de uno de los nodos, aparecerá una ventana con todos los datos guardados en el sistema sobre ese nodo.

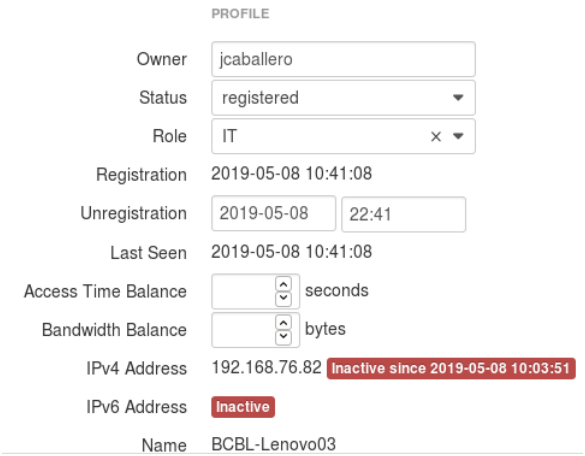
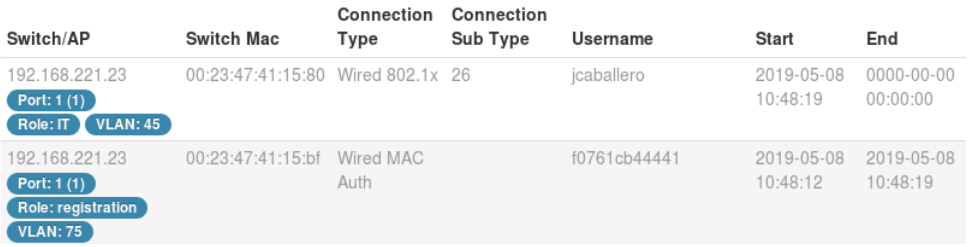


Figura 5.16: Detalles sobre el nodo con dirección MAC F0:76:1C:B4:44:41

Puede observarse como se le ha asignado información acerca del usuario al nodo a la hora de realizar el registro. En este caso, al haber introducido credenciales de un usuario del departamento de IT se le ha asignado el *Role* de IT durante 12 horas (el tiempo de acceso establecido a este *Role* en pasos anteriores).

También se puede apreciar como la IP asignada por PacketFence no ha sido utilizada por el nodo en un tiempo y aparece marcada de color rojo. Esto se debe a que una vez el nodo se ha registrado, durante el periodo de duración del registro (12 horas en este caso) la dirección IP asignada al nodo por PacketFence no será necesaria, ya que al tener acceso a la red, la dirección IP asignada a este nodo será una dirección IP asignada por el servidor DHCP en producción en la red del BCBL.

Dentro de esta ventana hay diferentes pestañas que pueden visitarse, pero la que más información puede proporcionar en base a la autenticación es la pestaña *Location*, donde aparece información acerca de los cambios de VLAN y *Role* del nodo durante el proceso de autenticación.



Switch/AP	Switch Mac	Connection Type	Connection Sub Type	Username	Start	End
192.168.221.23 Port: 1 (1) Role: IT VLAN: 45	00:23:47:41:15:80	Wired 802.1x	26	jcaballero	2019-05-08 10:48:19	0000-00-00 00:00:00
192.168.221.23 Port: 1 (1) Role: registration VLAN: 75	00:23:47:41:15:bf	Wired MAC Auth		f0761cb44441	2019-05-08 10:48:12	2019-05-08 10:48:19

Figura 5.17: Información acerca de un nodo en la pestaña *Location*

Además de la información que PacketFence nos proporciona en su interfaz web, también hay ficheros de *log* que proporcionan información acerca de las autenticaciones que se lleven a cabo. Ejemplos de ello son los archivos *log* `/usr/local/pf/logs/radius.log` y `/usr/local/pf/logs/packetfence.log`, donde puede encontrarse muchísima información acerca de todo lo que está sucediendo en PacketFence.

```
[mac:f0:76:1c:b4:44:41] Accepted user:  and returned VLAN 75
(4741) Login OK: [f0761cb44441] (from client 192.168.221.23 port 1 cli f0:76:1c:b4:44:41)
Need 6 more connections to reach 10 spares
rlm_sql (sql): Opening additional connection (46), 1 of 60 pending slots used
Need 6 more connections to reach 10 spares
rlm_rest (rest): Opening additional connection (42), 1 of 60 pending slots used
(4750)   Login OK: [jcaballero] (from client 192.168.221.23 port 1 cli f0:76:1c:b4:44:41 via TLS tunnel)
[mac:f0:76:1c:b4:44:41] Accepted user: jcaballero and returned VLAN 45
(4751) Login OK: [jcaballero] (from client 192.168.221.23 port 1 cli f0:76:1c:b4:44:41)
```

Figura 5.18: Fragmento del log `packetfence.log` tras una autenticación exitosa

6. CAPÍTULO

Despliegue en subred en producción

Para la realización de este despliegue se trasladará lo realizado hasta el momento a un entorno real controlado, es decir, se realizará un NAC sobre una VLAN específica que está en producción en el BCBL. Además de esto, se cambiará el modo de autenticación, ya que, como se ha comentado en anteriores ocasiones, la idea del BCBL es autenticar las máquinas de los usuarios, y no a los usuarios en sí.

Esta autenticación se realizará en base a los certificados que estén instalados dichas máquinas. Estos certificados tendrán que haber sido emitidos por la *Autoridad Certificadora (CA)* propia del BCBL. Esta CA está instalada en el mismo servidor Windows Server 2008 que el Directorio Activo que se ha utilizado para la autenticación de usuarios en la implementación anterior. Esta CA emite certificados tanto de máquinas como de usuarios, además de certificados para ciertos servicios.

La VLAN en producción que se utilizará para testear el NAC será la VLAN 45, que corresponde a la VLAN del departamento de IT del BCBL.

6.1. Configuración de PacketFence

En esta sección se mostrarán los cambios que se han realizado en la configuración dentro de PacketFence para realizar una autenticación basada en certificados. Han sido necesarias pocas modificaciones en la configuración de PacketFence, ya que va a utilizarse el mismo dominio, mismo punto de acceso (switch), etc. Una de las modificaciones que se han requerido realizar ha sido la de añadir una nueva fuente de autenticación y añadir ciertas reglas en la misma. Para ello hay que acceder a *Configuration –>Policies and Access Control –>Authentication Sources*, y una vez en esta ventana hacer click sobre *ADD SOURCE –>Internal –>EAPTLS*. Para esta fuente de autenticación se han añadido los siguientes datos:

- Name: *Cert_Authentication*
- Description: *Authentication based on certificates issued by bcbl-PFC-CA*

Y al igual que en configuraciones anteriores, hay que elegir ciertas reglas para la autenticar al usuario.

Authentication Rules:

1. BCBL_workstations
    - Name: *BCBL_workstations*
    - Description: *Authentication based on certificates issued by bcbl-PFC-CA*
    - Conditions:
        a) *TLS-Client-Cert-Issuer contains bcbl-PFC-CA*
    - Actions:
        a) Role = *IT*
        b) Access duration = 12 hours

La regla que se ha establecido permitirá el acceso a todos los equipos que dispongan de un certificado que haya sido emitido por la CA del BCBL: **bcbl-PFC-CA**.

Además de esto, hay que asignar esta nueva fuente de autenticación al *Connection Profile* que ya estaba creado (llamado **802.1x**). Para ello hay que navegar a *Configuration –>Policies and Access Control –>Connection Profiles* y hacer click sobre el nombre del perfil para cambiar el valor del parámetro *"Source"* por *"Cert_Authentication"*.

Una vez realizados los cambios explicados en las páginas anteriores, tendremos que crear un certificado para PacketFence y descargar el certificado de la CA en la máquina donde se encuentra instalado (TFG01 en este caso). Estos certificados pueden descargarse directamente desde la interfaz web de la CA `https://acc.bcbl.local/certsrv/mscep`, donde también realizaremos la petición del certificado para PacketFence que tendrá que ser del tipo *Web-Server*.

Una vez hecho esto, tendremos que configurar cierto fichero de configuración de PacketFence para especificarle las rutas donde hemos alojado los certificados. Este fichero se encuentra en `/usr/local/pf/conf/radiusd/eap.conf`. En este fichero tendremos que buscar el bloque de configuración referido a las conexiones TLS con el nombre `tls-config tls-common`. Una vez localizado dicho bloque de configuración tendremos que especificar as rutas para los siguientes ficheros: certificado de PacketFence, clave privada de PacketFence y el certificado de la CA.

En este caso se han especificado las siguientes rutas:

```
certificate_file = [% install_dir %]/conf/ssl/tls_certs/charlie.cer
private_key_file = [% install_dir %]/conf/ssl/tls_certs/charlie.key
ca_file = [% install_dir %]/conf/ssl/tls_certs/ACC.cer
```

La variable `[% install_dir%]` hace referencia a la ruta desde la raíz hasta el directorio de instalación de PacketFence, en este caso: `/usr/local/pf`.

6.2. Despliegue automático de los certificados

Para realizar una autenticación basada en certificados, uno de los requisitos más importantes será el correcto despliegue de los certificados en cuestión. Teniendo en cuenta que en la empresa hay usuarios trabajando con diferentes Sistemas Operativos, habrá que configurar correctamente el despliegue de los certificados para cada uno de estos Sistemas Operativos.

6.2.1. Sistema Operativo Windows 7

Para el despliegue de los certificados en este Sistema Operativo, será suficiente con ingresar la máquina dentro del dominio. Esto se debe a que el controlador de dominio es la máquina *acc.bcbl.local*, que es la misma máquina donde está instalado el Directorio Activo y estaba configurada de antemano para desplegar el certificado *Computers* a todas las máquinas Windows pertenecientes al dominio *bcbl.local*.

Para introducir la máquina con Sistema Operativo Windows 7 en el dominio, tendremos que hacer click sobre el botón de Inicio, click derecho sobre *Computer* y seleccionar *Properties*. Tras ello aparecerá una ventana en la que tendremos que hacer click sobre el botón/link *Change settings* y se abrirá una nueva ventana. En esta ventana haremos click sobre el botón *Change...*, con lo que aparecerá la siguiente ventana emergente:

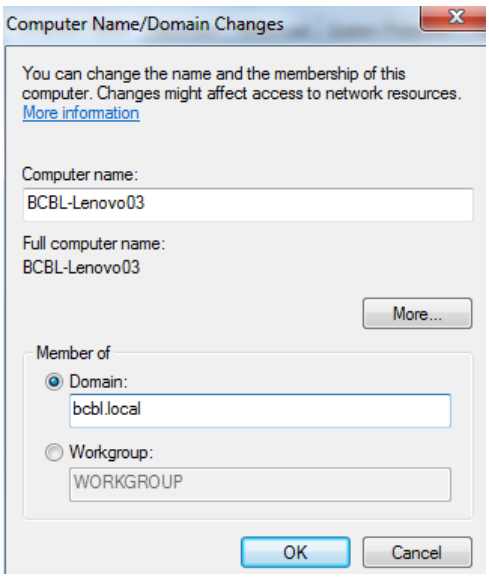


Figura 6.1: Ventana emergente para introducir una máquina en un dominio

En esta ventana seleccionaremos la opción *Domain:* y escribiremos el nombre del dominio en el recuadro de debajo, en este caso **bcbl.local**. Una vez hecho esto haremos sobre el botón *OK* para que aparezca una nueva ventana emergente donde añadiremos las credenciales de una cuenta con privilegios de administrador en el dominio.

Una vez realizados estos cambios se tendrmos que reiniciar el equipo y éste ya pertenecerá al dominio.

6.2.2. Sistema Operativo CentOS 7

Para realizar el despliegue de los certificados en este Sistema Operativo, será necesario el uso del protocolo *SCEP (**S**imple **C**ertificate **E**nrollment **P**rotocol*).

En este punto, se ha topado con un problema inesperado: el Directorio Activo de Microsoft requiere de la instalación del servicio *NDES (**N**etwork **D**evice **E**nrollment **S**ervice*) para realizar despliegues de certificados mediante SCEP, y la versión en funcionamiento del Directorio Activo en el BCBL no soporta la instalación de dicho servicio. La versión instalada en el BCBL es *Microsoft Active Directory 2008 R2* ***Standard***, mientras que la versión que soporta NDES se trata de la versión *Microsoft Active Directory 2008 R2* ***Enterprise***

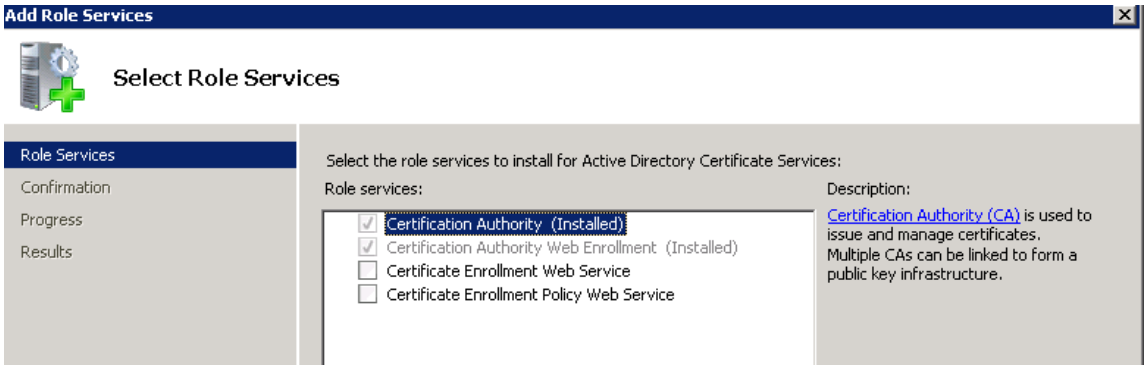


Figura 6.2: La opción NDES no aparece en Windows Active Directory 2008 R2 *Standard*

En este punto, las dos opciones disponibles son las siguientes:

1. Los equipos con Sistema Operativo CentOS 7 tendrán que descargar e instalar los certificados de manera manual
2. Instalar y configurar un servidor Windows Active Directory 2008 R2 *Enterprise* para desplegar los certificados automáticamente a los equipos con CentOS 7.

La opción escogida ha sido la número 2 a petición del BCBL. Puede encontrarse una guía de configuración y testeo de un Windows Server 2008 R2 Enterprise para su utilización como servidor de *autoenrollment* en el Anexo C.

Una vez configurado el servidor Windows Server 2008 R2 Enterprise, se realizará una prueba con la máquina **glia21** con Sistema Operativo CentOS 7. La prueba consistirá en intentar conseguir instalar un certificado a nombre de la máquina mediante la línea de comandos, utilizando *sscep*. Para ello hay que acceder a la terminal de la máquina en modo administrador y realizamos las siguientes acciones:

Como primer paso crearemos el fichero de petición de certificado y para ello puede utilizarse tanto *openssl* como el script `/etc/bin/mkrequest`. Para esta primera prueba se va a utilizar *openssl*:

```
openssl req -new -newkey rsa:2048 -nodes -keyout local.key -out local.csr
-subj '/C=ES/ST=Guipuzcoa/L=Donostia/O=BCBL/OU=IT/CN=glia21.bcbl.local'
```

```
-rw-r--r--  1 root root    1009 May  7 11:56 local.csr
-rw-r--r--  1 root root    1704 May  7 11:56 local.key
```

Figura 6.3: Creación de la petición para un certificado y clave privada para la máquina **glia21**

Una vez creadas la petición de certificado para la máquina y su clave privada asociada, podría hacerse la petición y descarga del certificado de dos maneras, una manual y la otra utilizando SCEP. En esta prueba se utilizará SCEP para la petición del certificado, aunque en las siguientes líneas se explicará de forma breve como podría hacerse de forma manual.

El método manual consiste en acceder directamente a la url `http://TFG03/certsrv/` o a la url `http://acc.bcbl.local/certsrv/`, ya que mediante este método no se hace uso del protocolo SCEP, por lo que puede realizarse la petición directamente a la CA.

Una vez se haya accedido al servidor vía web, hay que hacer click sobre el enlace *"Request a certificate"* seguido de *"Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file."*. En esta ventana tendría que aparecer lo que se ve en la imagen C.12. En este formulario hay que copiar el contenido del fichero *local.csr* y tras hacer click sobre el botón *"Submit"* la CA generará el certificado y podrá se descargado haciendo click sobre el enlace *"Download Certificate"*.

El método mediante SCEP es mucho más sencillo y rápido, ya que consiste en ejecutar dos comandos desde la consola de la máquina. El primero de ellos descargará en la máquina local el certificado de la CA además de dos certificados adicionales que son necesarios para enrolarse mediante SCEP. Estos certificados adicionales se conocen como *"CEP encryption certificate"* y *"Enrollment agent certificate"*. Para ello hay que ejecutar el siguiente comando *sscep*:

```
sscep getca -u http://tfg03/CertSrv/mscep/ -c CA
```

Lo que generará los siguientes ficheros:

```
-rw-r--r--  1 root root    2029 May  7 12:36 CA-0
-rw-r--r--  1 root root    2004 May  7 12:36 CA-1
-rw-r--r--  1 root root    1285 May  7 12:36 CA-2
```

Figura 6.4: Certificados descargados mediante *sscep*

El certificado con terminación en "-0" es el *"Enrollment agent certificate"* mientras que el certificado con terminación "-1" es el *"CEP encryption certificate"*. Para ver el contenido del certificado, por ejemplo, de *CA-0* en modo de texto plano puede utilizarse siguiente comando: `openssl x509 -in CA-0 -text`.

```
X509v3 extensions:
    1.3.6.1.4.1.311.20.2:
        .,.E.n.r.o.l.l.m.e.n.t.A.g.e.n.t.O.f.f.l.i.n.e
    X509v3 Extended Key Usage:
        1.3.6.1.4.1.311.20.2.1
```

Figura 6.5: Parte del contenido del certificado **CA-0** en texto plano

Una vez generados los certificados pertinentes, el último paso consiste en el "enrollmen" en sí. Para ello se requieren los archivos "CA-0", "CA-1", "local.key" y "local.csr".

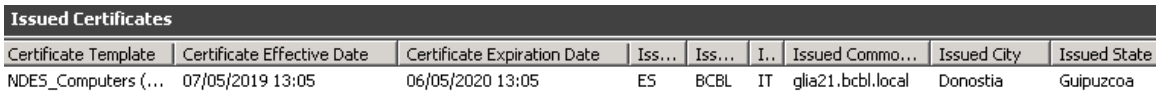
```
sscep enroll -c CA-0 -e CA-1 -k local.key
-r local.csr -l local.crt -S sha1
-u http://tfg03/CertSrv/mscep/mscep.dll
```

El anterior comando generará el archivo "local.crt", que será el certificado para la máquina **glia21**.

```
-rw-r--r-- 1 root root 2029 May  7 12:36 CA-0
-rw-r--r-- 1 root root 2004 May  7 12:36 CA-1
-rw-r--r-- 1 root root 1285 May  7 12:36 CA-2
-rw-r--r-- 1 root root 2171 May  7 13:15 local.crt
-rw-r--r-- 1 root root 1009 May  7 11:56 local.csr
-rw-r--r-- 1 root root 1704 May  7 11:56 local.key
```

Figura 6.6: Certificado creado mediante SCEP para la máquina **glia21**

Se puede comprobar como la CA ha emitido un certificado a para la máquina **glia21**, en la que coinciden la hora de creación del fichero "local.crt" y la publicación del certificado en la CA con un desfase de 10 minutos, debido a la configuración de la CA.



Issued Certificates

Certificate Template	Certificate Effective Date	Certificate Expiration Date	Iss...	Iss...	I..	Issued Commo...	Issued City	Issued State
NDES_Computers (...	07/05/2019 13:05	06/05/2020 13:05	ES	BCBL	IT	glia21.bcbl.local	Donostia	Guipuzcoa

Figura 6.7: Certificado **NDES_Computers** emitido por la CA mediante SCEP.

Para no tener que ejecutar estos comandos a mano por cada máquina CentOS que se añada al dominio, se ha utilizado un script encontrado en la dirección https://blogs.technet.microsoft.com/jeffbutte/2016/12/16/236/. Se han definido las variables en base a la configuración actual además de corregir algún pequeño error que impedía la correcta ejecución del script. Puede encontrarse el código completo del script en el Anexo E.

Una vez comprobado el correcto funcionamiento del script será añadido para que sea ejecutado durante el arranque de las máquinas Linux, ya que este script también renueva el certificado en caso de que ésta haya caducado.

Cabe mencionar que este script (llamado *autoenrollment.sh*) almacena los certificados de la máquina local en el directorio `/etc/pki/tls/private/`, además de crear una copia del certificado *(*.crt)* en el directorio `/etc/pki/tls/certs`, y los certificados provenientes de la CA en `/etc/pki/ca-trust/source/anchors/`.

6.2.3. Sistema Operativo MAC OS X

El despliegue automático de certificados no será necesario para este Sistema Operativo, ya que, tal y como se comenta en la sección *Configuración del cliente para autenticación basada en certificados (6.3)* para configurar una interfaz de red es necesario instalar un servidor *macOS Server* y el BCBL no lo ha visto necesario, por lo que en lugar de ello se realizará una autenticación basada en la dirección MAC de los equipos, al igual que con las impresoras.

6.3. Configuración del cliente para la autenticación basada en certificados

6.3.1. Sistema Operativo Windows 7

Esta sección únicamente recogerá los cambios que hay que realizar sobre una interfaz previamente configurada para la autenticación de usuarios basada en el protocolo 802.1X, tal y como se muestra en la sección 5.2 *Configuración del cliente para autenticación de usuarios*.

Una vez la interfaz está configurada para la autenticación mediante el protocolo 802.1X, los cambios a realizar serán mínimos. Primero tendremos que abrir la ventana de Propiedades de la interfaz LAN que vamos a utilizar para acceder a la red y navegar a la pestaña de *Authentication*, ya que todos los cambios de configuración se harán en ella. En esta ventana sustituiremos *"Microsoft: Protected EAP (PEAP)"* por *"Microsoft: Smart Card or other certificate"*, y después haremos click sobre el botón *Settings* para acceder a una nueva ventana de configuración.

En esta ventana nos aseguraremos de que están marcadas las casillas *"Use a certificate on this computer"* y *"Use simple certificate selection (Recommended)"*, y de que la casilla *"Validate server certificate"* está marcada. Una vez realizados estos cambios clicaremos sobre el botón *OK* para que se guarden los cambios realizados y se cierre la ventana.

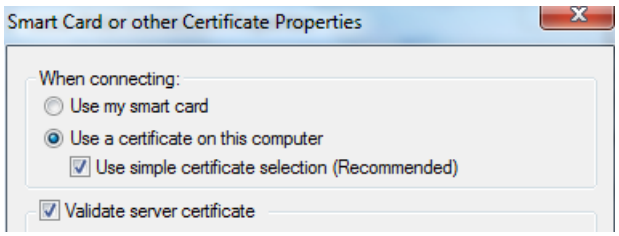


Figura 6.8: Configuración de la ventana *Settings* de una interfaz de red.

Para finalizar con la configuración de la interfaz será necesario hacer click sobre *Additional settings...* y cambiar la selección de la lista desplegable por *"Computer authentication"*.

6.3.2. Sistema Operativo CentOS 7

Esta acción puede realizarse mediante la interfaz gráfica o modificando ficheros de configuración. Se ha decidido hacerlo mediante la interfaz gráfica para facilitar el trabajo. Aún así, la idea es crear un script para no tener que configurar manualmente todos los equipos CentOS, por lo que este apartado también se trabajará más adelante.

Para configurar una interfaz web mediante la interfaz gráfica en CentOS tendremos que pulsar el botón de inicio, escribir *settings* y pulsar Enter. Una vez se abra la ventana de configuración, clicaremos sobre *Network* en la columna de la izquierda para acceder al menú de configuración de interfaces.

A diferencia del Sistema Operativo Windows 7, en CentOS pueden crearse diferentes Perfiles de conexión para una misma interfaz, lo cual puede ser muy cómodo. Para crear un nuevo perfil sobre la interfaz de conexión cableada hay que pulsar el símbolo "+" que aparece en la parte superior derecha el cuadro donde aparecen las interfaces que ya están configuradas dentro de la sección *Wired*.

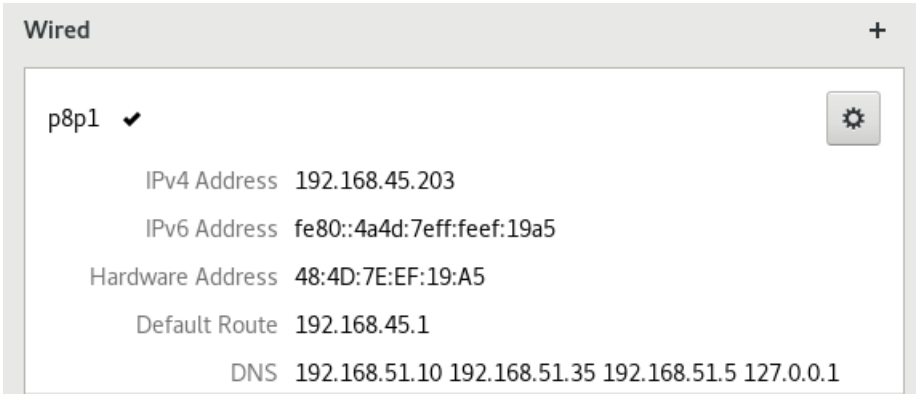


Figura 6.9: Ventana de creación y modificación de perfiles sobre una interfaz de red.

En la pestaña *Identity* únicamente especificaremos el nombre que se le quiera dar al Perfil, para este caso se ha utilizado el nombre **Wired_802.1x**. Después, en la pestaña *Security*:

- 802.1x Security: *ON*
- Authentication: *TLS*
- Identity: *glia21.bcbl.local*
- User certificate: *glia21.crt*
- CA certificate: *tfg03CA.crt-2*
- No CA certificate is required: *unchecked*
- Private key: *glia21.key*
- Private key password: ********

En este punto se ha encontrado un problema, ya que ha aparecido el siguiente mensaje de error al seleccionar la clave privada *glia21.key*:

Figura 6.10: Mensaje de error al seleccionar una clave privada sin contraseña.

Al parecer no se puede establecer una configuración de autenticación mediante certificados si la clave privada asociada al certificado de la máquina no está encriptada mediante el uso de una contraseña. Para encriptar dicha clave privada utilizaremos *openssl* tal y como aparece en el mensaje de error.

```
[root@glia21 ~]# openssl rsa -aes256 -in glia21.key -out glia21.encrypted.key
writing RSA key
Enter PEM pass phrase: ********
Verifying - Enter PEM pass phrase: ********
```

La ejecución del comando anterior generará el fichero `glia21.encrypted.key`, el cual será utilizado para la configuración que se estaba realizando previamente.

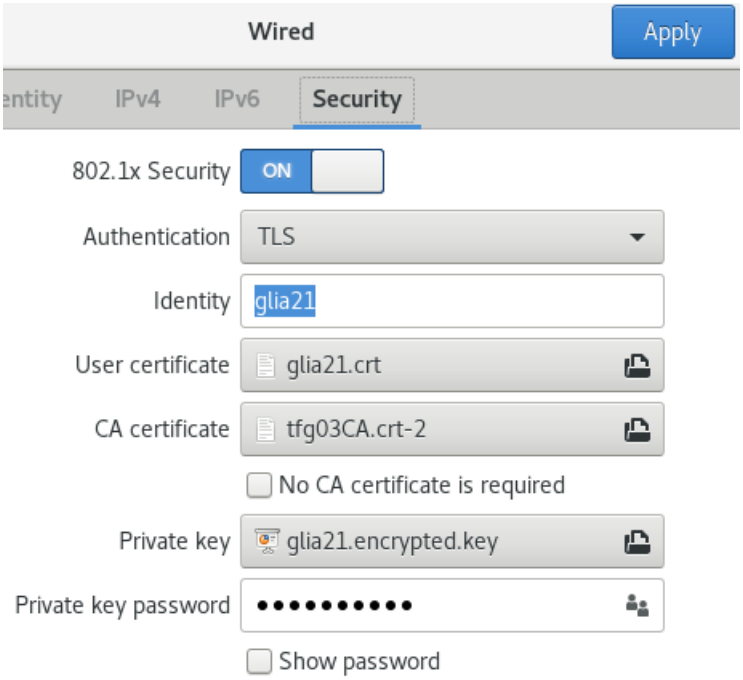


Figura 6.11: Configuración de un perfil de red para la autenticación mediante certificados.

Una vez que el Perfil para la interfaz de red ha sido configurado aparecerá en la lista como opción seleccionable. La primera vez que se haga click sobre él aparecerá una pequeña ventana emergente donde hay que introducir la contraseña con la que se cifró la clave privada. Si la contraseña introducida es correcta, el Perfil podrá empezar a utilizarse como método de conexión.

Script para la configuración automática de interfaces de red

Teniendo en cuenta que esta configuración debería de realizarse automáticamente para cada equipo CentOS con acceso a la red, se va a proceder a realizar un script que cree estas configuraciones. Para ello lo primero será analizar los archivos que esta configuración ha creado en el directorio `/etc/sysconfig/network-scripts`. Listando el contenido del directorio se ha podido observar que el sistema ha creado un fichero de configuración de interfaz llamado `ifcfg-Wired_802.1x` con el siguiente contenido:

```
TYPE=Ethernet
KEY_MGMT=IEEE8021X
IEEE_8021X_EAP_METHODS=TLS
IEEE_8021X_IDENTITY=glia21.bcbl.local
IEEE_8021X_PRIVATE_KEY=/etc/pki/tls/private/glia21.encrypted.key
IEEE_8021X_CLIENT_CERT=/etc/pki/tls/certs/glia21.crt
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME="Wired 802.1x"
UUID=5aca2f64-6369-4ffd-9c14-89f05a6096c6
ONBOOT=yes
```

Tras analizar el fichero de configuración creado por el sistema se puede intuir como podría crearse un script que realice estas configuraciones.

En un principio se ha propuesto crear un nuevo Perfil de red en la interfaz para la autenticación basada en certificados, al igual que se ha realizado mediante la interfaz gráfica al igual que en el paso anterior (6.11). Para ello se ha escrito el siguiente script basado en el comando **nmcli**, cuyo propósito es configurar o crear Perfiles e interfaces de red.

Contenido del script **if_conf_new.sh**:

```
#!/bin/bash
PASS=$(cat /etc/pki/tls/private/.dirinfo/.p)
echo "Creating new 802.1x TLS based Network Profile..."
nmcli connection add type ethernet con-name Wired_802 ifname "*" \
autoconnect true 802-1x.eap tls 802-1x.identity $(hostname) \
802-1x.client-cert /etc/pki/tls/certs/$(hostname).crt \
802-1x.private-key /etc/pki/tls/private/$(hostname).encrypted.key \
802-1x.private-key-password $PASS
if [ $? -eq 0 ]
  then
  echo "Network Profile created successfully!"
  nmcli connection show
  else
  echo "An error ocurred while trying to create the Network Profile"
fi
```

Este script funciona correctamente y crea un nuevo Perfil llamado **Wired_802** sobre que puede ser utilizado sobre cualquier interfaz de red. Cabe mencionar que la contraseña para desencriptar la clave está almacenada en el directorio `/etc/pki/tls/private/.dirinfo/.p`.

```
[jcaballero@glia21 Desktop]$ ./if_conf_new.sh
Creating new 802.1x TLS based Network Profile...
Connection 'Wired_802' (b1251bae-5ce4-4b1b-9637-7f320b69869c) successfully added.
Network Profile created successfully!
NAME       UUID                                  TYPE      DEVICE
p8p1       0037689f-2035-45ec-a15d-13a512be4c03  ethernet  p8p1
Wired_802  b1251bae-5ce4-4b1b-9637-7f320b69869c  ethernet  --
```

Figura 6.12: Perfil de red creado con éxito utilizando el script **if_conf_new.sh**.

Aunque el Perfil se crea correctamente y funciona correctamente, se ha descubierto que al reiniciar el equipo hay algún tipo de conflicto entre los diferentes perfiles y aparece un bug en la interfaz gráfica que puede dar luegar a confusiones. En la siguiente imagen puede observarse cómo se muestra el menú rápido de conexiones tras configurar un nuevo Perfil antes reiniciar el equipo:

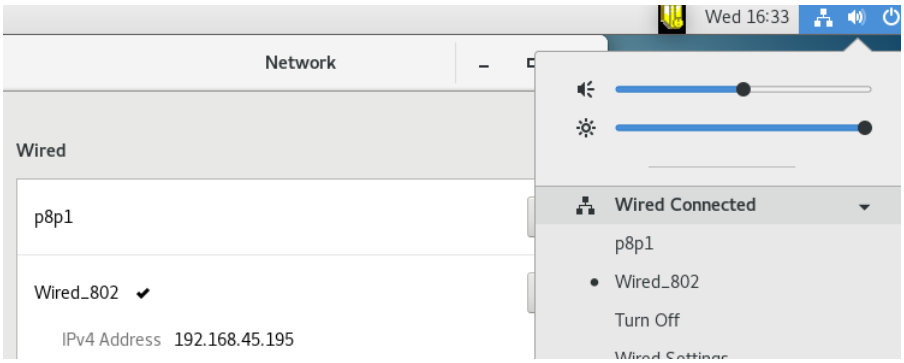


Figura 6.13: Antes de reiniciar el equipo.

La siguiente imagen muestra como, tras reiniciar el equipo, aparece un bug visual en el menú rápido de conexiones:

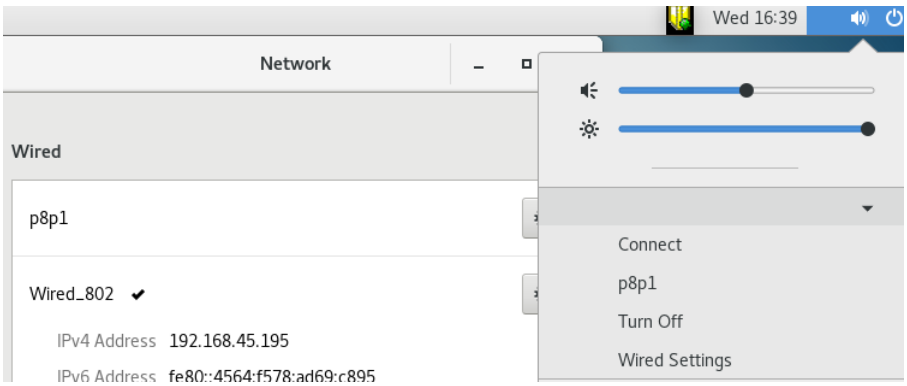


Figura 6.14: Después de reiniciar el equipo.

Se puede observar como además del icono de conexión y el estado de la misma (*Wired Connected* en la imagen 6.13), ni siquiera aparece el Perfil “Wired_802” en la lista de Perfiles del menú de acceso rápido de red, aunque es el que se está utilizando para la conexión y funciona correctamente con una IP de la VLAN 45 asignada.

Por un lado para evitar confusiones entre los usuarios finales de los equipos, y por otro para no tener más Perfiles de red de los necesarios (uno) configurados en el equipo, se ha decidido modificar el script para que no añada un nuevo Perfil de red a la interfaz, sino para que modifique el existente y lo configure de forma que realice la conexión a la red mediante el protocolo 802.1X basado en certificados.

Para ello, el primer paso será conseguir el nombre del Perfil por defecto configurado en el equipo, ya que estos nombres pueden variar dependiendo del equipo (ens, eth, p8p1, Wired Connection, etc.). Para ello se ha utilizado el siguiente comando:

```
nmcli -t | grep connected | grep -v disconnected | awk -F' to ' '{print $NF}'
```

Sin entrar en más detalle sobre este comando, el resultado será un string con el nombre del Perfil de conexión que se esté utilizando (en los equipos recién formateados solamente habrá uno). Gracias a esto se ha podido modificar el script de la siguiente manera para configurar el Perfil una vez encontrado su nombre:

```
IF=$(nmcli -t | grep connected | grep -v disconnected | \
awk -F' to ' '{print $NF}')
PASS=$(cat /etc/pki/tls/private/.dirinfo/.p)
echo "Modifying default $IF Network Profile..."

nmcli connection modify "${IF}" autoconnect true \
802-1x.ca-cert /etc/pki/ca-trust/source/anchors/tfg03CA.crt-2 \
802-1x.eap tls 802-1x.identity $(hostname) \
802-1x.client-cert /etc/pki/tls/certs/$(hostname).crt \
802-1x.private-key /etc/pki/tls/private/$(hostname).encrypted.key\
802-1x.private-key-password $PASS

if [ $? -eq 0 ]
   then
   echo "Network Profile $IF modified successfully!"
   nmcli -p connection show
   else
   echo "An error ocurred while trying to modify the Network Profile"
fi
```

Este script se ha llamado **if_conf_default.sh**, y para comprobar su correcto funcionamiento se ha ejecutado y se ha obtenido el siguiente resultado:

```
[root@glia21 Desktop]# ./if_conf_default.sh
Modifying default p8p1 Network Profile...
Network Profile p8p1 modified successfully!
NAME  UUID                                  TYPE      DEVICE
p8p1  0037689f-2035-45ec-a15d-13a512be4c03  ethernet  p8p1
```

Figura 6.15: Perfil de red por modificado con éxito mediante el script **if_conf_default.sh**.

Además del script anterior, también ha tenido que modificarse el script *autoenrollment.sh*, ya que la clave privada generada por el mismo no es encriptada mediante una contraseña tal y como lo requiere la configuración de interfaces de CentOS para la autenticación mediante el protocolo 802.1X. Las líneas añadidas al script son las siguientes:

```
....... En la comprobación de la instalaciones necesarias .......

if rpm -qa | grep openssl  2>&1 > /dev/null;
        then
        writelog "sscep: openssl is installed."
else
    yum -y install openssl 2>&1 >> $LOGFILE
fi

.............. Una vez creada la clave privada ..............

openssl rsa -aes256 -in /etc/pki/tls/private/$(hostname).key -out \
/etc/pki/tls/private/$(hostname).encrypted.key -passout \
pass:file:/etc/pki/tls/private/.dirinfo/.p
```

El funcionamiento del script será probado más adelante en la sección *Testeo de autenticación basada en certificados (6.4)* para comprobar que tanto las creación de las claves como la encriptación de la clave privada se realiza correctamente.

6.3.3. Sistema Operativo MAC OS X

Para probar la configuración en un equipo con Sistema Operativo Mac OS X, se utilizará un *MacBook Pro* con la versión *El Capitán (versión 10.11.6)* instalada.

Lo primero que se ha realizado ha sido acceder al panel de configuración de las interfaces de red, donde se ha encontrado lo siguiente:

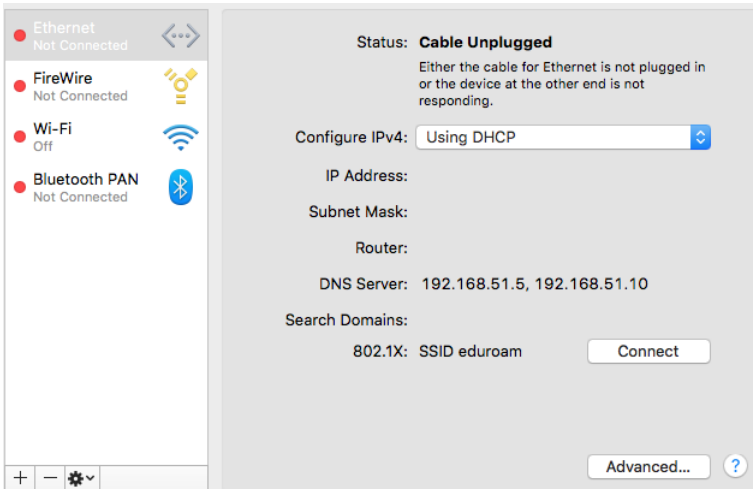


Figura 6.16: Ventana de interfaces disponibles en el equipo

Tal y como puede observarse en la figura superior, la interfaz de Ethernet tiene un perfil para autenticación 802.1X configurado llamado **SSID eduroam**. Este perfil fue creado por eduroam para el BCBL, ya que además de la red WiFi para invitados del BCBL, también disponen de una red eduroam.

Se ha procedido a crear un nuevo perfil de conexión sobre la red Ethernet haciendo click sobre el botón **Advanced...** de esa misma ventana. Una vez aquí, se ha navegado hasta la pestaña *802.1x*, donde se encuentran listados todos los perfiles de configuración sobre la interfaz. En este caso, únicamente aparece el perfil **SSID eduroam** ya que es el único existente hasta el momento.

Lo que se buscaba en esta ventana era una forma de crear un nuevo perfil (en versiones anteriores del Sistema Operativo aparecía un símbolo “+” para ello), pero no se ha encontrado ninguna forma de hacerlo desde esta ventana.

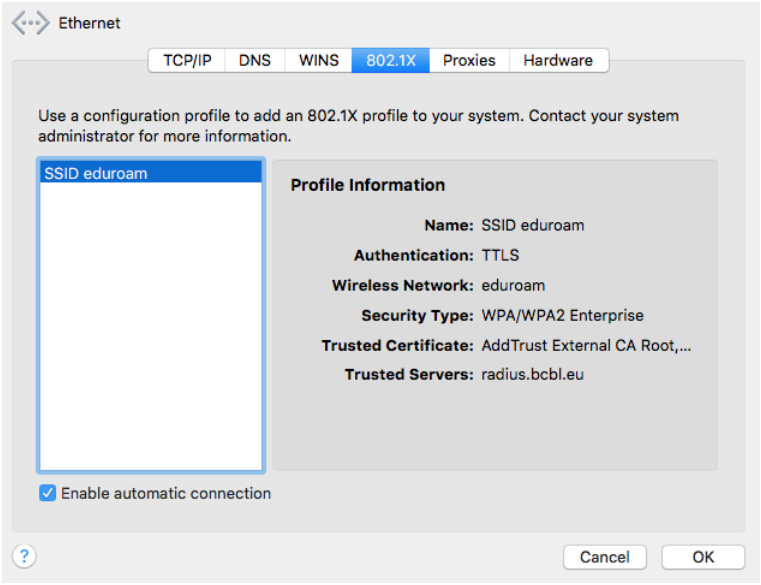


Figura 6.17: Perfiles existentes en el equipo para la interfaz *Ethernet*

Como segunda opción se ha accedido al apartado *Profiles* del menú de configuraciones del sistema, donde aparecen listados todos los perfiles creados para este equipo (únicamente **eduroam** por ahora), y en este caso sí que aparece el símbolo “+” en la parte inferior izquierda para añadir un nuevo perfil.

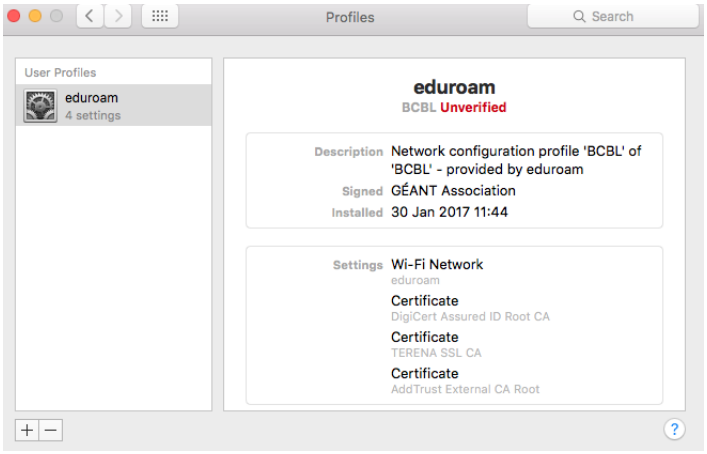


Figura 6.18: Perfiles existentes en el equipo

Una vez hecho click sobre el botón "+" se esperaba que se abriese una ventana de configuración del perfil (al igual que en el caso de la creación de un perfil de configuración para una interfaz en CentOS 7), pero en lugar de eso, se ha abierto una ventana donde hay que seleccionar un archivo de perfil para poder asignarlo a la interfaz de red.

Buscando información en la red acerca de este suceso, se ha encontrado con un problema mayor de lo esperado: a partir de la versión 10.6 de Mac OS, los perfiles de configuración no pueden ser creados localmente como hasta el momento, sino que tienen que ser creados a través de una aplicación llamada *macOS Server* (disponible en la *AppStore* por un precio de 21,99€), de donde podrán ser exportados o descargados vía web una vez hayan sido configurados.

Figura 6.19: Producto *macOS Server* a la venta en la *AppStore*

Se ha comentado todo lo anterior a los superiores del BCBL, quienes han optado por no instalar el servidor ya que hay muy pocos equipos MAC, y además no siempre están en funcionamiento, por lo que se ha decidido ofrecer únicamente conexión mediante WiFi a estos equipos.

Aún así, a petición del BCBL, se procederá a explicar cómo se realizaría la configuración del perfil para la autenticación 802.1X basada en certificados para una interfaz de red cableada. Este documento puede encontrarse en el Anexo D.

6.4. Testeo de autenticación basado en certificados

En esta sección se comprobarán tanto el correcto despliegue de los certificados para todos los Sistemas Operativos configurados, como la autenticación de acceso a la red basada en los mismos.

6.4.1. Sistema Operativo Windows 7

El testeo para este tipo de autenticación es más simple que el anterior, ya que es totalmente transparente para el usuario y el acceso a la red debería de estar garantizado con solamente conectar el cable a la interfaz de red si el equipo dispone de un certificado válido.

Primero comprobaremos que el equipo no dispone de ningún certificado de máquina. Para ello hay que pulsar la tecla de inicio, escribir "mmc" y pulsar Enter para acceder a la Consola de Administración de Windows *(**M**icrosoft **M**anagement **C**onsole)*.

Una vez aquí haremos click sobre *File –>Add/Remove Snap-in...* para abrir una nueva ventana donde seleccionaremos *"Certificates"* del cuadro de la izquierda y pulsaremos el botón *"Add >"*. En la ventana emergente que aparecerá tendremos que seleccionar *"Computer account"* y hacer click sobre *Next*. En el siguiente paso seleccionaremos *"Local computer: (the computer this console is running on)"* y clicaremos sobre *Finish* para cerrar la ventana actual y en el botón *OK* para terminar la importación del *Snap-in*.

Para comprobar que no hay ningún certificado instalado en la máquina, tenemos que recorrer el árbol de directorios de la parte izquierda hasta *Certificates (Local Computer) –>Personal –>Certificates* y una vez aquí podremos comprobar cómo no aparece listado ningún certificado, indicando que no existe ningún certificado asociado a la máquina instalado en ella.

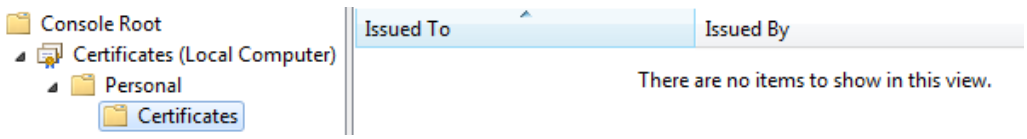


Figura 6.20: Listado de certificados de máquina locales vacío.

Se va a proceder a realizar un intento de conexión a la red con el equipo sin certificado instalado para comprobar que la red es inaccesible.

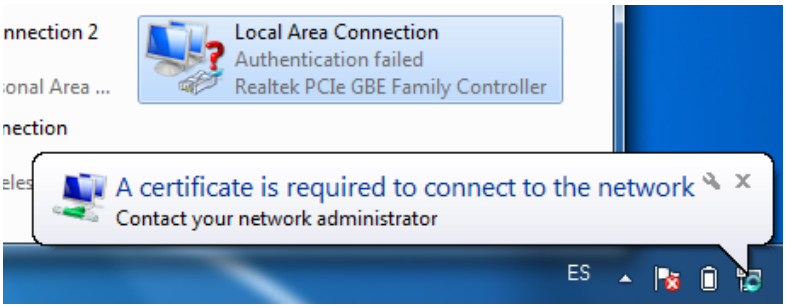


Figura 6.21: Mensaje de alerta al intentar acceder a la red sin un certificado válido.

Para descargar el certificado tendremos que introducir la máquina en el dominio *bcbl.local* tal y como se ha explicado en el apartado *Despliegue automático de los certificados (6.5)*, y una vez hecho podremos observar cómo existe un certificado de máquina donde antes no lo había.

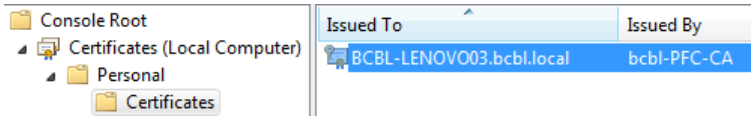


Figura 6.22: Certificado descargado automáticamente al introducir la máquina en el dominio.

Una vez el certificado ha sido descargado en la máquina, procederemos a conectar la máquina a la red para comprobar si realmente tiene acceso a la misma de manera automática.

Figura 6.23: Acceso a la red tras autenticación mediante certificado.

6.4.2. Sistema Operativo CentOS 7

De la misma manera que para el caso anterior, lo primero que realizaremos será comprobar que la descarga automática del certificado de máquina se realiza correctamente. Para ello utilizaremos el script *autoenrollment.sh* generado anteriormente.

Ejecución del script: `./autoenrollment.sh`.

```
[root@glia21 private]# /home/jcaballero/Desktop/autoenrollment.sh
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....................................................+++
e is 65537 (0x10001)
writing RSA key
Subject of the returned certificate: +
Subject of the request: /CN=glia21
[root@glia21 private]# ll
total 20
-rw-r--r-- 1 root root 2078 May 10 11:37 glia21.crt
-rw-r--r-- 1 root root  940 May 10 11:37 glia21.csr
-rw-r--r-- 1 root root 1766 May 10 11:37 glia21.encrypted.key
-rw------- 1 root root 1675 May 10 11:37 glia21.key
```

Figura 6.24: Ejecución exitosa del script *autoenrollment.sh*.

Tal y como puede apreciarse en la figura superior, la ejecución del script ha descargado correctamente el certificado y su clave privada en el directorio `etc/pki/tls/private`, además de que la clave privada ha sido encriptada correctamente mediante las modificaciones realizadas al script en la sección *Configuración del cliente para autenticación basada en certificados (6.3)*. También se crea una copia del certificado *(glia21.crt)* al directorio `/etc/pki/tls/certs`, ya que es, por defecto, el directorio donde se guardan los certificados públicos.

Para comprobar el correcto funcionamiento de PacketFence con equipos CentOS 7, intentaremos acceder a la red a través del equipo en le que se ha configurado la interfaz previamente tal y como se explica en la sección *Configuración del cliente para autenticación basada en certificados (6.3)*.

Teniendo en cuenta que en este punto todos los equipos que forman parte en la autenticación deberían de estar correctamente configurados, la conexión debería de ser inmediata una vez se haya seleccionado el perfil creado anteriormente **(Wired_802.1x)** estando el cable ethernet de la interfaz conectado al switch de acceso que comunica con PacketFence.

Primero intentaremos conectarnos a la red mediante el perfil por defecto *p8p1* para las interfaces de red cableadas y demostrar que no se tiene acceso a la red. Al conectar el cable de red no parece haber ningún problema, ya que el símbolo de conexión que aparece en la parte superior derecha de la pantalla es el mismo que cuando tenemos acceso a la red.

Esto se debe a que en realidad hemos obtenido acceso a la red, concretamente PacketFence ha otorgado una dirección IP válida al ordenador, pero esta IP corresponde a la VLAN 75 *Registration* desde la que no tendremos acceso hacia el exterior, ni tampoco hacia ninguna otra sección privada de la red.

Para comprobar que no se tiene acceso a la red se ha intentado acceder a una página web cualquiera mediante un navegador web y el resultado ha sido el siguiente:

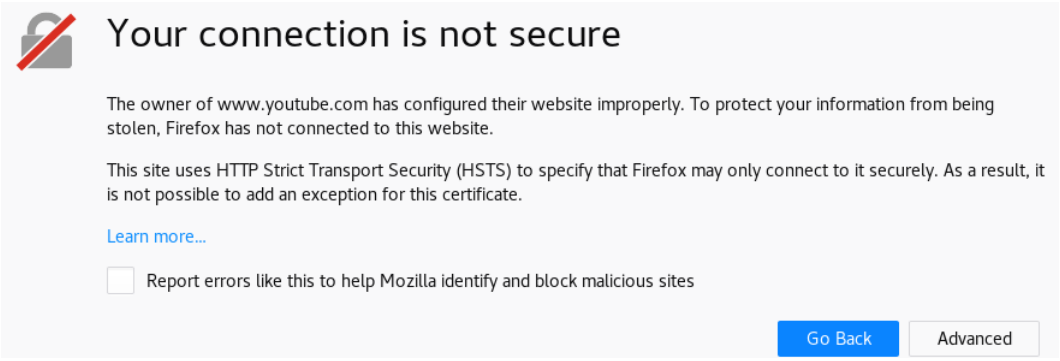


Figura 6.25: Mensaje de error en el navegador al intentar acceder a cualquier sitio web.

Es extraño que en lugar de aparecer un aviso de que no se ha podido alcanzar la dirección web, aparezca un mensaje diciendo que la conexión que estamos intentando realizar no es segura porque el sitio web utiliza un certificado de seguridad no válido. Por ello, se ha decidido investigar un poco más al respecto y se ha descargado el certificado que el navegador web esta obteniendo en nombre de *www.google.com*.

```
https://www.google.com/

Peer's Certificate issuer is not recognized.

HTTP Strict Transport Security: true
HTTP Public Key Pinning: false

Certificate chain:

-----BEGIN CERTIFICATE-----
```

Figura 6.26: Certificado que esta recibiendo el navegador en nombre de *www.google.com*.

Se ha generado un fichero con el contenido del certificado que debería de pertenecer al dominio de Google. Se ha procedido a pasar a texto plano el certificado descargado y se ha obtenido la siguiente información:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            c9:48:ac:e7:37:37:a0:f5
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CA, ST=QC, L=Montreal, O=Inverse, CN=127.0.0.1/emailAddress=support@inverse.ca
```

Figura 6.27: El supuesto certificado de *www.google.com* en texto plano.

Puede observarse que los datos del emisor del certificado no coinciden con los datos de Google. Esto se debe a que el certificado pertenece al servidor de PacketFence, con los datos de *Inverse* de Montreal, la empresa que lo ha diseñado.

Éste es el motivo de que aparezca este mensaje de error tan extraño; PacketFence envía su propio certificado al navegador del equipo que intenta acceder a la red, lo que da lugar a confusiones, ya que el mensaje de error que aparece da a pensar que realmente hay acceso a la red y que ha habido contacto con el otro extremo, aunque no haya sido así.

```
[root@TFG01 ssl]# diff google.crt server.crt
[root@TFG01 ssl]#
```

Figura 6.28: El certificado descargado del navegador y el del servidor PacketFence son iguales.

Mediante el comando `ifconfig` se puede comprobar cómo la dirección IP asignada al equipo corresponde a la VLAN *Registration*, por lo que se deduce que PacketFence ha asignado el *Role: Registration* a la máquina y la ha enviado a la VLAN 75, tal y como está configurado.

```
p8p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.44  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::2159:ecaf:f9a6:4378  prefixlen 64  scopeid 0x20<link>
        ether 48:4d:7e:ef:19:a5  txqueuelen 1000  (Ethernet)
        RX packets 1303141  bytes 976859278 (931.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 901941  bytes 180099796 (171.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 6.29: Al asignarle el *Role: Registration*, la máquina es mandada a la VLAN 75 *(Registration)*.

Se ha cambiado el perfil de conexión de la interfaz de **p8p1** a **Wired_802.1x** y se ha conseguido acceder a la red correctamente. Podemos comprobarlo mediante el comando `ifconfig`:

```
p8p1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.45.195  netmask 255.255.255.0  broadcast 192.168.45.255
        inet6 fe80::28bf:1857:3ee0:cba1  prefixlen 64  scopeid 0x20<link>
        ether 48:4d:7e:ef:19:a5  txqueuelen 1000  (Ethernet)
        RX packets 2864874  bytes 1533282342 (1.4 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2941305  bytes 424656593 (404.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 6.30: Acceso con éxito a la VLAN 45 mediante autenticación basada en certificados.

También podremos comprobar como la VLAN asignada al puerto 1 del punto de acceso es la VLAN 45. Para ello nos conectaremos al switch mediante *ssh* y ejecutaremos el comando `sh vlan port 1`:

```
Status and Counters - VLAN Information - for ports 1

 802.1Q VLAN ID Name         Status       Jumbo
 -------------- ------------ ------------ -----
 45             VLAN45       Port-based   No
```

Figura 6.31: VLAN 45 asignada al puerto 1 del punto de acceso.

6.5. Despliegue

En esta sección se explicará como se ha realizado el despliegue de PacketFence en la subred perteneciente al departamento de IT (VLAN 45) del BCBL.

Para ello, a petición del BCBL se ha creado una nueva máquina virtual (llamada Charlie) en el hipervisor en la que se realizará una instalación y configuración de PacketFence desde cero. La instalación ha sido exactamente igual que en la máquina anterior, aunque la versión de PacketFence haya sido actualizada. Esta guía de instalación puede encontrarse en el capítulo B incluido en los Anexos.

El departamento de IT se compone de un total de 5 equipos conectados a dos switches diferentes. Cuatro de estos equipos están situados en la tercera planta del edificio, conectados a los puertos 1,4,5 y 6 del switch AXON18 (modelo HP ProCurve 3500yl), mientras que el equipo restante está situado en la segunda planta, conectado al puerto 45 del switch AXON05 (modelo HP ProCurve 2810 48G).

El despliegue ha consistido en tres principales tareas:

- Configuración de los switches.
- Configuración de PacketFence.
- Configuración de los equipos.

En las siguientes páginas se procederá a explicar la realización de cada una de estas tareas.

6.5.1. Configuración en PacketFence

La configuración en PacketFence ha sido sencilla teniendo en cuenta que ya se había realizado este tipo de autenticación anteriormente. Por no volver a repetir la configuración desde cero, se procederá a explicar la configuración de la manera más breve posible y haciendo referencias a capítulos anteriores si es necesario.

1 - Creación de Roles:

Configuration –>Policies and Access Control –>Roles

Se ha creado el rol **IT**.

2 - Adición de la máquina en el dominio bcbl.local:

Configuration –>Policies and Access Control –>Domains –>Active Directory Domains

Se ha añadido la máquina al dominio de la misma manera que se ha explicado en el capítulo 5.1.

3 - Crear una fuente de autenticación:

Configuration –>Policies and Access Control –>Authentication Sources

Se ha añadido la misma configuración que se mostró en la sección 6.1.

4 - Crear un perfil de conexión:

Configuration –>Policies and Access Control –>Connection Profiles –>Add Profile

Donde se ha añadido la siguiente información:

- Profile Name: *802.1x*
- Automatically register devices *checked*
- Filters: *If any of the following conditions are met:*
  - Connection Type: *Ethernet-EAP*
- Sources: *Cert_Authentication (fuente de autenticación creada en el paso anterior)*

5 - Añadir los switches a PacketFence:

Configuration –>Policies and Access Control –>Network Devices –>Switches

Se ha añadido la siguiente configuración para cada uno de los switches:

- En la pestaña *Definition*:
  - IP Address/MAC: *192.168.221.X* [1]
  - Type: *HP ProCurve 2600 Series* [2]
  - Description: *AXONXX* [3]
  - Mode: *Production*
- En la pestaña *Roles*
  - Role by VLAN ID: *checked*
  - registration: *75*
  - isolation: *76*
  - REJECT: *-1*
  - IT: *45*
- En la pestaña *RADIUS*
  - Secret Passphrase: *xxxxxxxxx*
- En la pestaña *SNMP*
  - Community Read: *Public*
  - Community Write: *BCBL_Ch@rl13*

[1] X=5 para el AXON05 y X=18 para el AXON18
[2] *Generic* para el AXON18
[3] XX=05 para el AXON05 y XX=18 para el AXON18

6.5.2. Configuración de los switches

Las configuración en ambos switches ha sido idéntica dado que se tratan de switches de la misma familia. Las configuraciones realizadas han sido las siguientes [4]:

```
radius-server host 192.168.241.250 key ‘‘**********’’
snmp-server host 192.168.241.250 community public not-info
snmp-server community BCBL_Ch@rl13 unrestricted
aaa authentication port-access eap-radius
aaa port-access authenticator [PORT-LIST]
aaa port-access authenticator [PORT-LIST] client-limit 1
aaa port-access [PORT-LIST] controlled-direction in
port-security [PORT-LIST] learn-mode port-access action send-alarm
aaa port-access mac-based [PORT-LIST]
aaa port-access mac-based [PORT-LIST] addr-moves
aaa port-access mac-based [PORT-LIST] reauth-period 14400
aaa port-access authenticator active
```

Una vez ejecutado el comando `aaa port-access authenticator active`, los puertos ([PORT-LIST]) configurados mediante los comandos anteriores pasarán a estar securizados mediante el protocolo 802.1X, por lo que se requerirá un método de autenticación para acceder a la red a través de estos puertos.

6.5.3. Configuración de los equipos

La configuración de los equipos se ha realizado de la misma manera que se explica en la sección 6.3. Teniendo en cuenta que son pocos equipos han sido configurados a mano, pero para el despliegue global se añadirán dichas configuraciones mediante GPO (***G**roup **P**olicy **O**bject*) en los equipos Windows y se configurará la ejecución de los scripts creados para la configuración automática de los equipos CentOS mediante *Puppet*.

[4] [PORT-LIST] = 1,4-6 para AXON18 y 45 para AXON05

7. CAPÍTULO

Planificación del despliegue global en la red

7.1. Configuración genérica de los switches

En esta sección se explicará como se procederá a configurar los switches necesarios para el despliegue global del control de acceso a la red. Se han identificado los switches que serán necesarios configurar para realizar dicho despliegue en masa:

1. AXON03 –>192.168.221.3
2. AXON04 –>192.168.221.4
3. AXON05 –>192.168.221.5
4. AXON06 –>192.168.221.6
5. AXON09 –>192.168.221.9
6. AXON18 –>192.168.221.18 (depliegue realizado en el capítulo 6.5)
7. AXON21 –>192.168.221.21
8. AXON22 –>192.168.221.22

Estos 8 switches están distribuídos por todo el BCBL y ofrecen conexión a diferentes departamentos, por lo que podrían agruparse de la siguiente manera:

1. Floor 0: AXON03, AXON06 y AXON22
2. Floor 2: AXON04, AXON05, AXON09 y AXON21

Antes de realizar la configuración definitiva de los switches, pueden ejecutarse los siguientes comandos genéricos a todo ellos, ya que estas configuraciones no serán efectivas hasta ejecutar el comando `aaa port-access authenticator active`. Los comandos a ejecutar en todos los switches identificados en la lista anterior son los siguientes:

```
radius-server host 192.168.241.250 key ‘‘**********’’
snmp-server host 192.168.241.250 community public not-info
snmp-server community BCBL_Ch@rl13 unrestricted
```

Estos comandos definen cuáles serán los servidores RADIUS y SNMP para el switch en cuestión además de definir dos comunidades, una llamada *public* que tendrá permisos de lectura SNMP y otra llamada *BCBL_Ch@rl13* que también tendrá permisos de escritura (estas comunidades fueron definidas también en el switch AXON18 (6.5.2) y configurados en PacketFence (6.5.1) para el despliegue en el departamento de IT). Los servidores RADIUS y SNMP serán el mismo para todos los switches; Charlie (192.168.241.250), el servidor donde está instalado PacketFence.

Una vez realizada esta configuración genérica podrán empezar a configurarse los switches uno a uno, pero primero añadiremos estos switches a PacketFence.

7.2. Configuración de PacketFence

Lo primero será crear tres nuevos Roles: *Users, Printers* y *Mac_OS_X*. Más adelante se explicará como se realizará la autenticación para los dispositivos *Printers* y *MAC_OS_X*.

La adición de estos switches a PacketFence y su configuración se realizará prácticamente de la misma manera que se hizo en el despliegue en el departamento de IT (6.5.1).

Configuration –>Policies and Access Control –>Network Devices –>Switches

Se ha añadido la siguiente configuración para cada uno de los switches:

- En la pestaña *Definition*:
  - IP Address/MAC: *192.168.221.X* [1]
  - Type: *HP ProCurve 2600 Series*
  - Description: *AXONXX* [2]
  - Mode: *Production*
- En la pestaña *Roles*
  - Role by VLAN ID: *checked*
  - registration: *75*
  - isolation: *76*
  - REJECT: *-1*
  - IT: *45*
  - Users: *50*
  - Printers: *50*
  - Mac_OS_X: *50*
- En la pestaña *RADIUS*
  - Secret Passphrase: *xxxxxxxxx*
- En la pestaña *SNMP*
  - Community Read: *Public*
  - Community Write: *BCBL_Ch@rl13*

[1] X = número de AXON
[2] XX = número de AXON

7.3. Configuración individual de los switches

En esta sección se explicará como se debe de realizar la configuración individual de cada switch. Estas configuraciones se realizarán por bloques de switches que forman los grupos mencionados en la lista que puede encontrarse en la sección 7.1. Ha decidido planificarse de esta manera, ya que estas agrupaciones de switches crean sectores dentro de los diferentes departamentos del BCBL y es una manera ordenada y controlada de hacerlo.

Aunque los switches vayan a configurarse en un orden específico para mantener un control, la configuración a realizar en cada uno de ellos es prácticamente idéntica a la del resto, ya que la única diferencia relevante entre ellos será la lista de puertos a configurar en cada uno.

Para realizar una configuración eficiente y no configurar puertos innecesariamente se procederá a identificar cuales de estos puertos conectan con equipos del BCBL y serán éstos los únicos que se configuren.

En los siguientes comandos de configuración habrá que sustituir `[PORT-LIST]` por la lista de puertos utilizados identificados anteriormente. Los comandos a ejecutar en los switches son los siguientes:

```
aaa authentication port-access eap-radius
aaa port-access authenticator [PORT-LIST]
aaa port-access authenticator [PORT-LIST] client-limit 1
aaa port-access [PORT-LIST] controlled-direction in
port-security [PORT-LIST] learn-mode port-access action send-alarm
```

Estos comandos configuran los puertos `[PORT-LIST]` para realizar autenticaciones mediante el protocolo EAP-RADIUS, especificando un número máximo de clientes permitidos en cada uno de ellos. Además de esto también se le especifica que debe de controlar los paquetes de entrada en los puertos no securizados y que debe de enviar una SNMP-trap en caso de no autorizar el acceso a algún dispositivo que intenta conectarse.

Además de estos comandos, en los switches AXON05, AXON03 y AXON09 también habrá que ejecutar los siguientes comandos, ya que hay impresoras o equipos Mac OS X conectados a ellos:

```
aaa port-access mac-based [PORT-LIST]
aaa port-access mac-based [PORT-LIST] addr-moves
aaa port-access mac-based [PORT-LIST] reauth-period 14400
```

Estos comandos configuran los puertos sobre los que se realizará una autenticación basada en direcciones MAC. Estos switches permiten que un mismo puerto pueda realizar tanto autenticaciones 802.1X como autenticaciones basadas en direcciones MAC. El switch intentará primero autenticar el dispositivo mediante el protocolo 802.1X, pero en caso de que el dispositivo cliente no disponga del *"802.1X supplicant"*[3], el switch realizará una autenticación basada en la dirección MAC mediante una conexión NoEAP.

Por último, una vez el switch esté completamente configurado (podremos asegurarnos de su correcta configuración ejecutando el comando `sh run`) tendremos que ejecutar el siguiente comando:

```
aaa port-access authenticator active
```

Este comando pondrá en marcha la configuración que hemos realizado anteriormente en los puertos necesarios, y a partir de este momento, todos estos puertos quedarán securizados mediante autenticaciones 802.1X.

Por último y una vez comprobado que el sistema funciona correctamente podremos ejecutar el comando `write memory` en el switch para guardar la configuración actual y que no se pierda la siguiente vez que se apague.

[3] Software necesario en el cliente para poder realizar una autenticación basada en puertos

7.4. Configuración de los equipos conectados a la red

Los equipos sobre los que habrá que realizar configuraciones son únicamente los equipos con Sistemas Operativos Windows 7 y CentOS (más adelante se explicará como se realizará la autorización para equipos con Sistema Operativo Mac OS X).

7.4.1. Equipos con Sistema Operativo Windows 7

Los equipos que están conectados a la red se configurarán mediante GPO *(**G**roup **P**olicy **O**bject)* desde el Directorio Activo, lo que es muy útil para centralizar todas las configuraciones de los equipos desde un único punto y aplicar dichas configuraciones en masa.

Estas configuraciones se aplicarán a todos los equipos con Sistema Operativo Windows 7 que formen parte del dominio del BCBL. Las configuraciones son exactamente iguales a las que se describieron en el capítulo 6.3.1, por lo que únicamente serán listadas:

- Iniciar el servicio *WiredAutoConfig*
- En la pestaña *Authentication*
  - *"Enable IEEE 802.1x authentication"*
  - *"Choose authentication Method: Microsoft Smart Card or other certificate"*
  - En la ventana *"Settings:"*
    - *"Use a certificate on this computer"*
    - *"Use simple certificate selection (Recommended)"*
    - *"Validate server certificate" –>checked*
  - En la ventana *"Additional Settings..."*
    - *"Computer Authentication"*

Las siguientes imágenes muestran la configuración realizada para todos los equipos con Sistema Operativo Windows 7 del dominio y cómo se ven reflejadas dichas configuraciones en los equipos.

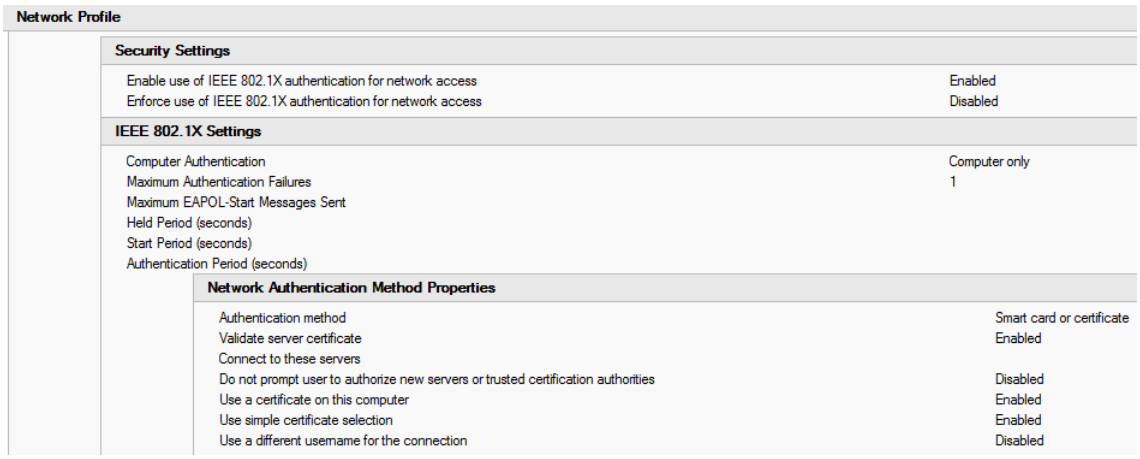


Figura 7.1: Configuraciones establecidas en el Directorio Activo para los equipos Windows 7.

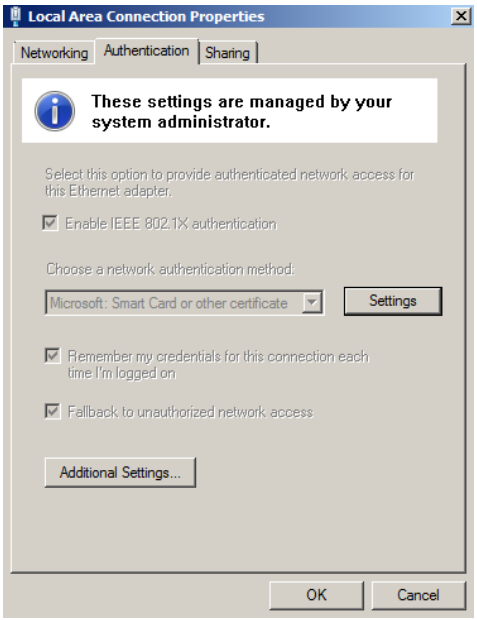


Figura 7.2: Vista de las configuraciones creadas mediante GPO desde los equipos Windows 7.

7.4.2. Equipos con Sistema Operativo CentOS 7

Para los equipos con Sistema Operativo CentOS 7 instalado se ha utilizado *Puppet* para realizar configuraciones en masa. Ya que se habían creado scripts para la configuración de los equipos con estos Sistemas Operativos, únicamente se ha ordenado la ejecución de dichos scripts en caso de cumplir ciertas condiciones. El código para configuración mediante *Puppet* es el siguiente:

```
class portsecurity {

   file { '/etc/pki/tls/private/.dirinfo':
       ensure => directory,
       owner => root,
       group => root,
       mode => 700,
    }
    file { "/etc/pki/tls/private/.dirinfo/.p":
    owner => root,
    group => root,
    mode => 400,
    source => "puppet://medulla01.bcbl.local/extra_files/scripts/p.txt"
    }


    file { "/root/scripts/autoenrollment.sh":
    owner => root,
    group => root,
    mode => 700,
    source => "puppet://medulla01.bcbl.local/extra_files/scripts/autoenrollment.sh"
    }
    file { "/root/scripts/if_conf_default.sh":
    owner => root,
    group => root,
    mode => 700,
    source => "puppet://medulla01.bcbl.local/extra_files/scripts/\
```

```
    if_conf_default.sh"
    }

    exec { 'autoenrollment':
        command => "sh /root/scripts/autoenrollment.sh",
        provider => shell,
        user => root,
        onlyif => 'test  `ls /etc/pki/tls/private/$HOSTNAME.* | wc -l` -ne 4',
        path => '/usr/sbin:/usr/bin:/sbin:/bin',
        require => [ File ['/root/scripts/autoenrollment.sh'], File \
        ['/etc/pki/tls/private/.dirinfo/.p'] ],
    }
    exec { 'ifcfg_802.1x':
        command => "sh /root/scripts/if_conf_default.sh",
        provider => shell,
        user => root,
        onlyif => 'test  `cat /etc/sysconfig/network-scripts/ifcfg-* | \
        grep "IEEE_8021X" | wc -l` -eq 0',
        path => '/usr/sbin:/usr/bin:/sbin:/bin',
        require => [ File ['/root/scripts/if_conf_default.sh'], File \
        ['/etc/pki/tls/private/.dirinfo/.p'] ],
    }

}
```

Los bloques de configuración que comienzan por *file* crean los directorios y ficheros necesarios (scripts y fichero de contraseñas) con los permisos necesarios, mientras que los bloques *exec* realizan ciertas comprobaciones para saber si los scripts tienen que ejecutarse o no.

En el caso del script *autoenrollment.sh* se comprueba que no existan los certificados de la máquina en su directorio correspondiente antes de ejecutarlo, mientras que en el caso del script *if_conf_default.sh* se comprueba que no exista ninguna interfaz configurada para realizar autenticaciones basadas en 802.1X.

7.4.3. Impresoras y equipos con Sistema Operativo Mac OS X

Las impresoras no pueden realizar autenticaciones mediante el protocolo 802.1X, por lo que se realizarán autenticaciones basadas en las direcciones MAC de las mismas. Debido a la imposibilidad para la creación de Perfiles en equipos con Sistema Operativo Mac OS X, se ha decidido autenticar estos equipos también mediante sus direcciones MAC.

Para ello no es necesaria ninguna configuración en estos equipos, sino que la configuración se realizará en PacketFence.

PacketFence dispone de una característica llamada *Security Events* (conocida como *Violations* en versiones anteriores) que recomiendan utilizar para la adición de impresoras a redes securizadas mediante 802.1X.

Estos *Security Events* se componen de los siguientes elementos:

- ID del evento
- *Triggers*
- Acciones a realizar

Cabe mencionar que a la hora de realizar de estas pruebas, PacketFence había publicado una nueva versión (versión 9.01 a fecha del 24 de mayo de 2019) en la que estos *Security Events* no funcionan correctamente. En la versión anterior esta característica tenía el nombre de *Violations* y puede que al realizar ciertos cambios en las configuraciones de estos Eventos hayan creado bugs.

Se han encontrado dos problemas a la hora de configurar estos Eventos:

1. No se configuran correctamente mediante la GUI: Si creamos un Evento mediante la GUI, podremos observar como hay opciones que no se han guardado correctamente si la seleccionamos en la lista para ver sus propiedades. Las opciones seleccionadas no se guardan correctamente en el fichero de configuración `/usr/local/pf/config/security_events.conf`, y los Eventos creados directamente mediante el fichero de configuración no aparecen listados en la GUI.

2. Los Eventos no "saltan" cuando coinciden con las condiciones especificadas como *Triggers*: En este caso se han especificado diferentes direcciones MAC (pertenecientes a impresoras y ordenadores portátiles Mac OS X) y ninguno de estos Eventos ha "saltado" de forma automática, aunque se ha comprobado que la dirección MAC del equipo que ha realizado la petición RADIUS para la autenticación (mirando con detenimiento en el fichero de log `/usr/local/pf/logs/radius.log` los mensajes RADIUS recibidos) coincide con una de las direcciones MAC establecidas como *Trigger*.

El Evento de seguridad creado para una impresora en concreto es el siguiente:

```
priority=1
trigger=mac::3C:D9:2B:A4:7C:80,mac::3c:d9:2b:a4:7c:80,mac::3CD92BA47C80,
mac::3cd92ba47c80,mac::3C-D9-2B-A4-7C-80,mac::3c-d9-2b-a4-7c-80
actions=autoreg,role
desc=Printers
enabled=Y
access_duration=5D
target_category=Printers
```

Puede comprobarse como en la condición *trigger* se ha añadido la misma MAC en múltiples formatos diferentes para realizar diversas pruebas y comprobar si en alguna de ellas el Evento "saltaba" automáticamente con resultados negativos.

En la condición *actions* se ha establecido *autoreg* que debería registrar automáticamente el dispositivo y *role* que debería asignar el Role establecido en la condición *target_category* (Printers en este caso).

Esta configuración ha sido contrastada con ejemplos supuestamente funcionales de la versión anterior de PacketFence por lo que se da por supuesto que la configuración es correcta.

Estos Eventos pueden ser disparados manualmente, la cual ha sido la mejor solución que se ha encontrado para el registro de esos equipos en PacketFence y garantizarles acceso. Para ello hay que Acceder a la pestaña *Nodes* de PacketFence una vez se haya conectado la impresora o equipo Mac OS X a la red. Este dispositivo quedará atrapado en la VLAN 75 (Registration) ya que no tiene forma de autenticarse, y una vez ahí aparecerán en la lista de la pestaña *Nodes* en estado *unregistered*.

Una vez detectado el dispositivo, haremos click sobre él para abrir una ventana donde aparecerá información acerca de ese dispositivo (VLAN y rol asignado, mensajes RADIUS recibidos, etc.) y donde podremos ver una pestaña llamada *Security Events* sobre la que tendremos que hacer click.

Esta ventana trata de una lista de los Eventos relacionados con este dispositivo que hayan sido disparados en algún momento, donde también se podrán disparar manualmente. Para ello no hay más que seleccionar un Evento de la lista y hacer click sobre el botón *"Trigger New Security Event"*. Una vez hecho esto el dispositivo quedará registrado y se le añadirá el Role establecido en la condición *target_category* en la configuración del Evento (Printer o Mac_OS_X) dependiendo del dispositivo y del Evento lanzado.

Para no tener que recurrir a realizar este registro manualmente, la mejor práctica será acceder a la pestaña *Edit* y establecer una duración de acceso de, por ejemplo, 5 años.

Puede encontrarse el registro del log `/usr/local/pf/logs/packetfence.log` al lanzar manualmente el Evento en el Anexo F.

7.5. Adición de nuevos equipos a la red

La adición de nuevos equipos a la red se realizará de la misma manera independientemente del Sistema Operativo que tenga instalado el equipo. Se ha decidido que la forma más sencilla de realizar esta tarea consistirá en dejar algún puerto libre en los switches en los cuales se realizará la autenticación 802.1X, donde se conectará por primera vez el equipo nuevo a añadir.

De este modo, a la hora de incorporar un equipo Windows podrá añadirse al dominio y por tanto descargar su propio certificado y el de la CA, y se realizarán las configuraciones por GPO establecidas por el BCBL. Una vez realizado este paso, el equipo podrá conectarse a la red securizada utilizando uno de los puertos configurados para realizar autenticaciones 802.1X.

A la hora de añadir un equipo CentOS, de la misma manera se utilizara uno de estos puertos “no seguros” para ejecutar mediante *Puppet* los comandos y scripts necesarios. Una vez realizado este paso, el equipo podrá conectarse a la red securizada utilizando uno de los puertos configurados para realizar autenticaciones 802.1X.

8. CAPÍTULO

Gestión del Proyecto

En este capítulo se expone cómo se ha llevado a cabo la gestión de todo el Proyecto de Fin de Grado, incluyendo la gestión del calendario, del alcance, del tiempo y de los riesgos.

8.1. Planificación de la gestión del calendario

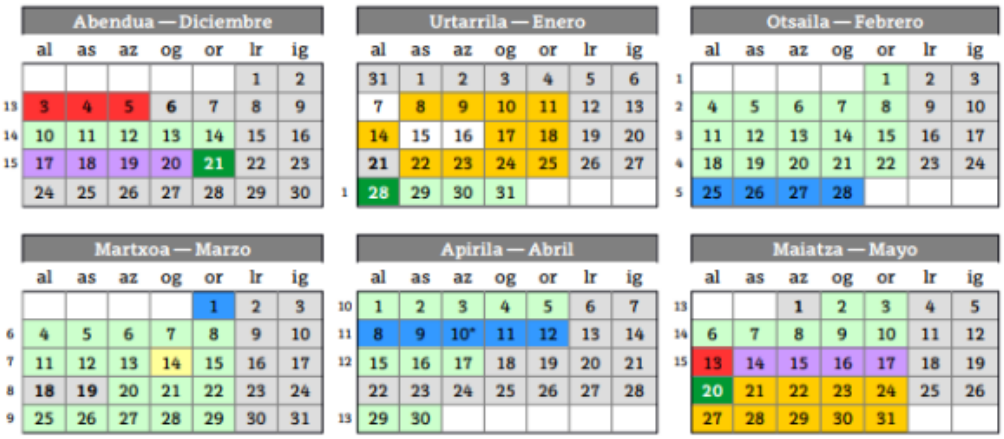


Figura 8.1: Calendario.

El calendario utilizado como referencia es el calendario que puede encontrarse en la página de la facultad de informática de la UPV. He decidido utilizar este calendario ya que los días de fiesta de la facultad coinciden con los días de fiesta del BCBL (18 y 19 de marzo, del 18 al 28 de abril y el día 1 de mayo).

Las semanas están numeradas desde el día 1 de febrero siendo la semana 1 hasta la semana del 13 de mayo siendo la semana 15. A partir de este momento, cada vez que se quiera hacer referencia a una semana en concreto, se utilizará la siguiente nomenclatura: SX. Siendo X el número de semana a la que se está haciendo referencia (ej. semana 3 = S3).

Las jornadas en la empresa serán de 5.5 horas (9:00 - 14:30) excepto martes y jueves que serán 5 horas (9:00 - 14:00) debido a las clases presenciales de la asignatura SRDSI que comienzan a las 15:00. Este horario suma un total de **26.5 horas semanales** en la empresa.

También se ha decidido hacer un seguimiento del TFG por parte de la empresa, por lo que me reuniré con ellos una vez a la semana.

Se ha estipulado que el proyecto tendrá que estar terminado (memoria aparte) para finales de abril o principios de mayo. Suponiendo que el proyecto esté terminado para la S13 y habiendo empezado el 1 de febrero de la S1, sumarían un **total de 302.5 horas** en la empresa, teniendo pendiente la realización de la memoria (que también será supervisada por el BCBL).

8.2. Gestión de los riesgos

En este apartado se intentan listar todos los posibles riesgos que pudiera correr la realización del proyecto. Identificar estos riesgos e intentar proponer soluciones para mitigarlos en la mayor medida posible es una labor que en un futuro podría determinar la correcta finalización del proyecto en el plazo especificado.

1- Problemas personales o de salud:

Problemas relacionados con mi persona, tanto físicos como mentales, tales como podrían ser problemas de salud o sucesos que puedan afectar directamente a mi estado emocional. En este apartado también se incluyen sucesos que puedan ocurrir a familiares o seres queridos y que puedan tener efectos emocionales negativos sobre mí o la necesidad de tener que desplazarme.

Mitigaciones:

Las mitigaciones de este riesgo, podrían ser, a priori, establecer las fechas de los hitos de una manera en la que pueda tener cierta holgura en caso de que suceda algo de lo mencionado. Si la planificación para los hitos no es demasiado justa, y dispongo del tiempo suficiente para terminarlos con cierto tiempo de adelanto, este riesgo no debería de ser demasiado costoso.

En caso de no terminar los hitos a tiempo por culpa alguno de estos motivos, existe otra solución a posteriori, que consiste básicamente en trabajar horas fuera del horario establecido por el BCBL hasta recuperar el tiempo perdido.

2- No realizar una correcta planificacion

Este riesgo podría condicionar la finalización del TFG en el plazo para el que estaba planificado, con sus posteriores repercusiones, como podrían ser no poder realizar la defensa del TFG en la fecha planificada o incluso recibir rechazo por parte del BCBL para continuar con ellos.

Mitigaciones:

Podría evitarse una situación como ésta, siendo "algo pesimista" con los tiempos en la planificación, es decir, haciendo una planificación pensando que seguramente me encontraré con más problemas de lo pensado y añadiendo unas horas de más a las tareas que puedan parecer más abstractas a la hora de hacer la planificación. De esta manera siempre tendré tendré un pequeño margen que podrían evitar la situación mencionada en el punto anterior.

3- Pérdida del trabajo realizado

La pérdida del trabajo realizado podría ser una catástrofe que seguramente se traduciría en la imposibilidad de poder realizar la defensa del proyecto en plazo. Se trata de uno de los mayores riesgos que podría correr el proyecto, aunque tomando las medidas oportunas, es un riesgo con una probabilidad muy baja de suceder.

Mitigaciones:

Esta situación podría evitarse haciendo las suficientes copias de seguridad en diferentes dispositivos. La memoria que ahora mismo estoy escribiendo, está siendo replicada cada día de desarrollo tanto en una nube privada que se encuentra en el BCBL (*NextCloud*), como en el PC de trabajo que estoy utilizando y en un directorio personal montado en dicho PC, pero sobre el que se hacen *backups* todos los días. Además de esto, descargo una copia en mi PC personal todas las semanas.

En el caso del proyecto en sí, también habrá copias de seguridad del mismo, ya que se realizan *backups* tanto del hipervisor como de los servidores que ofrecen servicio al centro.

4- Dificultad en el aprendizaje de las herramientas a utilizar

Las herramientas a utilizar en este proyecto son totalmente desconocidas para mí, lo que significa que tendré que pasar por un proceso de aprendizaje autodidacta en lo que se refiere a las mismas. En el caso de no ser capaz de dominarlas lo necesario como para alcanzar las expectativas que cubren al proyecto significaría no poder ser capaz de realizarlo, o como mínimo, necesitar más tiempo para la realización del mismo. Las consecuencias en el caso de que se diera este riesgo podrían abarcar desde el retraso de los plazos marcados para los hitos hasta la completa cancelación del proyecto, con su posterior realización de otro proyecto diferente desde cero.

Mitigaciones:

La única manera de evitar este riesgo es el de estudiar las herramientas a utilizar hasta un punto en el que tenga un punto de partida para prácticamente cualquier situación, o pedir ayuda en caso de encontrarme con un problema que me requiera demasiado tiempo solucionar.

5- Imposibilidad de realizar alguna actividad obligatoria para el proyecto debido a incompatibilidades o falta de material (hardware o software) por parte del BCBL

Podría darse la situación en la que el proyecto no pueda seguir adelante una vez haya comenzado su desarrollo debido a alguna incompatibilidad o falta de algún software o componente hardware requerido. Esto se debería a una mala planificación, ya que, en caso de encontrarse en una situación como esta debería de haberse detectado antes de comenzar con la fase de desarrollo. Esta situación podría ver comprometida la finalización del proyecto.

Mitigaciones:

Dependiendo del momento en el que se diera esta situación, podría replantearse el proyecto, o en caso de verlo necesario, comenzar uno nuevo. En el caso de que esta situación se diera con el proyecto muy avanzado con poco margen para las fechas de entrega el proyecto no podría terminarse y tendría que ser aplazada su entrega.

8.3. Gestión de las dedicaciones

En esta sección se desglosará la EDT (figura 3.1) en tareas más pequeñas mostrando los tiempos de dedicación para cada una de ellas.

8.3.1. Rama *"Tecnologías y herramientas"*

Esta rama está compuesta por tres sub-bloques: *Tecnologías, Herramientas* y *Red BCBL.*

Bloque *"Tecnologías"*

- Estudio y comprensión del protocolo RADIUS –>4 horas
- Estudio y comprensión del protocolo 802.1X –>4 horas
- Lectura y comprensión del manual del switch HP ProCurve 2810 –>3 horas

Bloque *"Herramientas"*

- Estudio de las características de PacketFence –>5 horas
- Estudio de las características de openNAC –>3.5 horas
- Redacción del documento sobre comparativas tecnológicas –>9 horas
- Estudio del funcionamiento de la herramienta PacketFence –>8 horas
- Familiarización con el Directorio Activo –>2.5 horas

Bloque *"Red BCBL"*

- Charla sobre la estructura de la red –>1 hora
- Estudio y comprensión de la red –>3.5 horas

8.3.2. Rama *"Implementación en entorno virtual controlado"*

Esta rama está compuesta por dos sub-bloques: *Configuraciones* y *Pruebas*.

Bloque *"Configuraciones"*

- Instalación de PacketFence –>4 horas
- Lectura y comprensión de la guía de administración de PacketFence –>15 horas
- Configuración de PacketFence para autenticación de usuarios –>30 horas
- Configuración del switch AXON23 –>1.5 horas
- Configuración del equipo portátil con Sistema Operativo Windows 7 –>1.5 horas

Bloque *"Pruebas"*

- Testeo del correcto funcionamiento del sistema –>25 horas

8.3.3. Rama: *"Despliegue en subred en producción"*

Esta rama está compuesta por tres sub-bloques: *Configuraciones, Pruebas* y *Despliegue*.

Bloque *"Configuraciones"*

- Configuración de PacketFence –>8 horas
- Despliegue de certificados para equipos con Windows 7 –>1 hora
- Despliegue de certificados para equipos con CentOS 7 [1] –>5 horas
    - Estudio sobre la configuración de WS 2008 [2] –>20 horas
    - Configuración de WS 2008 para realizar *autoenrollment* –>55 horas
    - Testeo del correcto funcionamiento del WS 2008 –>5 horas
- Configuración de equipos con Windows 7 –>0.5 horas

[1] En este punto se encontró la necesidad de instalar y configurar una versión concreta de Windows Server
[2] Windows Server 2008

- Configuración de equipos con CentOS 7 –>10 horas
  - Creación de los scripts *autoenrollment.sh* y *if_conf_default.sh* –>5.5 horas
- Configuración de equipos Mac OS X –>4 horas
  - Lectura sobre creación de Perfiles en Mac OS X –>1.5 horas
  - Redacción del documento Anexo D –>0.5 horas

Bloque *"Pruebas"*

- Testeo del correcto funcionamiento del sistema –>12 horas

Bloque *"Despliegue"*

- Instalación y configuración de PacketFence –>30 horas
- Configuración de los switches –>1.5 horas
- Configuración de los equipos –>2.5 horas
- Comprobación del correcto funcionamiento del nuevo sistema –>1 hora

8.3.4. Rama: *"Planificación del despliegue en la red"*

- Planificación y redacción del despliegue –>15 horas

8.3.5. Realización de la memoria

- Realización de la memoria –>87 horas

8.3.6. Total

Las horas invertidas en este TFG suman un TOTAL DE **385.5 horas**.

8.4. Gestión del tiempo

La mejor manera de representar la gestión del tiempo es hacerlo de manera gráfica mediante un diagrama de Gantt:

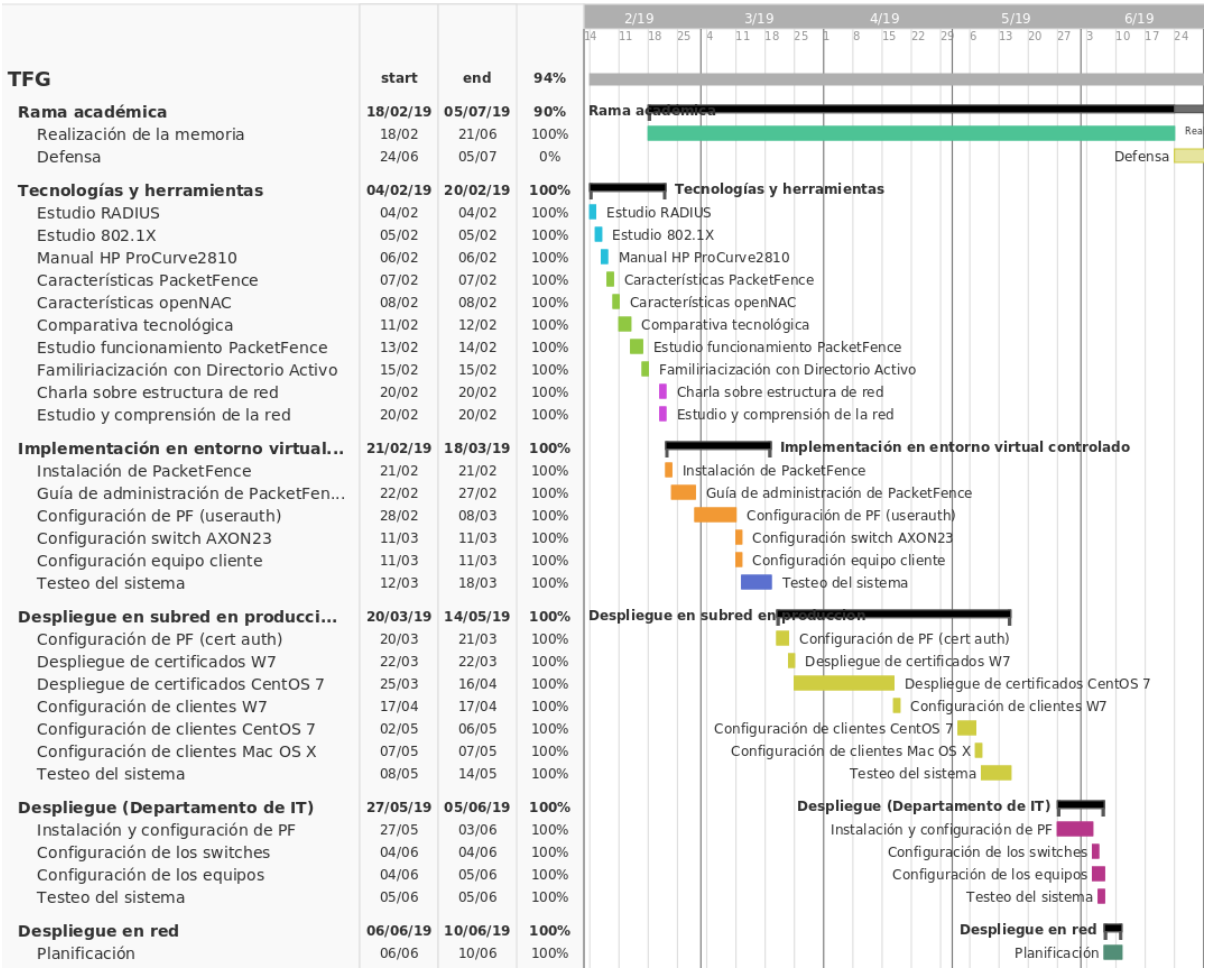


Figura 8.2: Diagrama de Gantt del TFG

8.5. Gestión del alcance

El seguimiento y control del correcto desarrollo del proyecto se ha realizado con frecuencia por parte del BCBL. En un principio se decidió hacer reuniones semanales comenzando en la semana S4, aunque por diversos motivos no ha podido cumplirse a rajatabla, pero se han podido realizar las suficientes reuniones para un correcto seguimiento sobre el proyecto.

Las reuniones realizadas con los superiores del BCBL han sido las siguientes:

- Fecha: 20/02/2019
  - Lugar: Despacho de José Corral
  - Asistentes: José Corral, Javier Gutiérrez y Jose Mª Caballero
  - Duración: 20 minutos
  - Motivo: Seguimiento y control
- Fecha: 27/02/2019
  - Lugar: Despacho de José Corral
  - Asistentes: José Corral, Javier Gutiérrez y Jose Mª Caballero
  - Duración: 15 minutos
  - Motivo: Seguimiento y control
- Fecha: 13/03/2019
  - Lugar: Departamento de IT
  - Asistentes: José Corral, Javier Gutiérrez, Borja Chantre y Jose Mª Caballero
  - Duración: 20 minutos
  - Motivo: Demostración del funcionamiento de una autenticación basada en usuario y contraseña al departamento de IT

- Fecha: 20/03/2019
    - Lugar: Departamento de IT
    - Asistentes: José Corral, Javier Gutiérrez, Borja Chantre y Jose Mª Caballero
    - Duración: 25 minutos
    - Motivo: Demostración del funcionamiento de la asignación de VLANs basada en roles al departamento de IT
- Fecha: 17/04/2019
    - Lugar: Departamento de IT
    - Asistentes: José Corral, Javier Gutiérrez, Borja Chantre y Jose Mª Caballero
    - Duración: 15 minutos
    - Motivo: Seguimiento y control
- Fecha: 09/05/2019
    - Lugar: Departamento de IT
    - Asistentes: José Corral, Javier Gutiérrez, Borja Chantre y Jose Mª Caballero
    - Duración: 20 minutos
    - Motivo: Demostración del funcionamiento de una autenticación basada en certificados al departamento de IT
- Fecha: 22/05/2019
    - Lugar: Despacho de José Corral
    - Asistentes: José Corral, Javier Gutiérrez y Jose Mª Caballero
    - Duración: 10 minutos
    - Motivo: Entrega de la documentación de la fase de desarrollo del proyecto
- Fecha: 12/06/2019
    - Lugar: Departamento de IT
    - Asistentes: José Corral, Javier Gutiérrez, Borja Chantre y Jose Mª Caballero
    - Duración: 45 minutos
    - Motivo: Despliegue de la securización 802.1X en el departamento de IT

9. CAPÍTULO

Conclusiones

En este breve capítulo se exponen las conclusiones obtenidas tras la realización del proyecto. Este capítulo ha sido dividido en dos secciones diferentes; las lecciones aprendidas por una parte, y las posibles mejoras aplicables al proyecto por otra.

9.1. Lecciones aprendidas

Partiendo de la base de que en la carrera únicamente se han visto muchos de estos conceptos de forma teórica, puedo afirmar que he adquirido cierta experiencia en la utilización y/o configuración de ciertas tecnologías y herramientas, como por ejemplo la configuración de un sistema (switches, equipos finales y servidores RADIUS) para realizar una autenticación 802.1X basada en puertos.

Además, también puedo afirmar que he aprendido mucho sobre PacketFence, la herramienta principal del proyecto, además de la instalación, configuración y gestión de un Windows Server para los servicios tanto de Directorio Activo como de Autoridad Certificadora.

Dejando de un lado lo referente a las tecnologías y herramientas que he aprendido a utilizar, también puedo afirmar que la seguridad informática abarca un amplio abanico de metodologías y costumbres, desde las reglas más básicas para todo individuo que haga uso de la tecnología, hasta las reglas más complejas para evitar ataques o intrusiones de características muy concretas, y que es imposible asegurar que un sistema es 100 % seguro y a prueba de cualquier tipo de intrusión o ataque.

9.2. Posibles mejoras

Aunque he quedado satisfecho con el resultado del proyecto, pueden modificarse ciertos aspectos para mejorarlo:

- **Autenticación de máquinas y usuarios:** Además de realizar una autenticación de máquinas basada en certificados emitidos por la CA del BCBL, también podría exprimirse más el potencial de PacketFence realizando, a posteriori, una autenticación del usuario que está utilizando la máquina que ha sido previamente autenticada mediante un portal cautivo. Esto añadiría otra capa de seguridad al sistema, ya que podrían evitarse intrusiones a través de *spoofing* mediante las direcciones físicas de las impresoras para un atacante/intruso externo a la empresa.

  Además, también haría más fácil la asignación de roles y por lo tanto la asignación de VLANs, ya que es difícil realizar dichas asignaciones mediante únicamente los certificados, ya que todos se generan de la misma manera.

- **Detección de elementos en el dispositivo:** PacketFence ofrece compatibilidad con una serie de sistemas para la detección de elementos referentes al equipo conectado que no se quieran admitir en la red. Entre estos sistemas se encuentran por ejemplo FingerBank, Suricata o WMI. Estos sistemas se basan en las "huellas" que deja un dispositivo a la hora de realizar una petición DHCP *(DHCP Fingerprints)*, y son capaces de clasificar cientos de dispositivos diferentes.

  Además del tipo de dispositivo (teléfono móvil, tablet, ordenador portátil, etc.) también son capaces de detectar Sistemas Operativos, versiones y caducidad de los antivirus, software instalado, etc. con lo que se puede crear una lista negra y evitar, por ejemplo, que un equipo con un Sistema Operativo obsoleto o con un antivirus desfasado pueda conectarse a la red.

10. CAPÍTULO

Bibliografía

[1] Wiki interna del BCBL

https://wernicke.bcbl.local/wiki/index.php/

[2] Documentación sobre PacketFence

https://packetfence.org/about.html

[3] Guía de instalación y configuración básica de PacketFence

https://packetfence.org/doc/PacketFence_Installation_Guide.html

[4] Guía de administrador de PacketFence

https://packetfence.org/doc/PacketFence_Administration_Guide

[5] Configuración de switches ProCurve para autenticaciones 802.1X

https://support.hpe.com/hpsc/doc/public/display?docId=mmr_kc-0126241

[6] Documentación de INCIBE sobre RADIUS

https://www.incibe-cert.es/blog/protocolos-aaa-radius

[7] Documentación sobre openNAC

https://redmine-opennac.opencloudfactory.com/projects/opennac/wiki/

[8] Configuración de NDES en un Windows Server 2008

https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx

[9] Documentación sobre OpenSSL

https://wiki.openssl.org/index.php/Command_Line_Utilities#Key_Generation

[10] Configuración de macServer para la creación de Perfiles de red

https://www.afp548.com/2012/11/20/802-1x-eaptls-machine-auth-mtlion-adcerts/

Anexos

A. ANEXO

Comparativa tecnológica: PacketFence vs openNAC

En este documento se estudiarán las herramientas PacketFence y openNAC (ambas herramientas de software de código libre para la implantación de NACs en redes tanto cableadas como inalámbricas) como solución a la implantación de un NAC en el centro BCBL. Para ello se realizará una comparativa entre ellas utilizando documentación oficial disponible en internet de los desarrolladores de cada herramienta. Ambas herramientas son software gratuito y de código abierto.

La elección de la herramienta se basará en los siguientes motivos:

- **Necesidades del centro:** Este será el motivo de más peso para la elección del software. En caso de que una de las dos herramientas no cumpla cualquiera de las necesidades exigidas por el centro *será descartada automáticamente*.
- **Compatibilidad con los equipos que forman parte de la red del centro:** En caso de haber algún tipo de incompatibilidad con algún elemento que forma parte de la red, se estudiarán alternativas que puedan solucionar el problema sin tener repercusión en el funcionamiento actual de la misma . En caso de no encontrar ninguna solución capaz de compatibilizar dicho elemento con la alternativa software en cuestión, ésta *será descartada automáticamente*.

- **Actualizaciones del software:** Se tendrán en cuenta las actualizaciones y la actividad de la comunidad y desarrolladores sobre el software. Al tratarse ambas herramientas de software de código libre, es importante el trabajo de la comunidad sobre ellas, ya que hay muchos usuarios que no son desarrolladores oficiales pero aportan mejoras y correcciones de diferentes tipos de bugs y errores. Además de las aportaciones de la comunidad, también se tendrá en cuenta si el software sigue activo por parte de los desarrolladores, o si en cambio han dejado el proyecto en manos de la comunidad de usuarios desentendiéndose del mismo. Esto podría suponer *un motivo de descarte* de la herramienta.

- **Documentación oficial disponible:** Se tendrá en cuenta la calidad de la documentación oficial que ofrezca la herramienta. En caso de no haber una documentación clara acerca de las especificaciones del software o acerca de la instalación y administración de la misma, la alternativa *podría ser descartada* debido a este hecho.

- **Funcionalidades extra:** También se tendrán en cuenta funcionalidades que puedan ser útiles para futuras implementaciones aunque no formen parte de las necesidades actuales del centro. Este motivo *podría ser decisivo* en caso de que ambas alternativas sean viables en todos los demás aspectos

- **Rendimiento:** Un factor importante a tener en cuenta es el rendimiento de la red y el impacto que pudiera tener el despliegue de una herramienta de este tipo sobre ella. En caso de que se comprobara que la herramienta seleccionada baja considerablemente el rendimiento de la red, *podría desecharse* volviendo a la configuración actual, o en caso de tener tiempo, instalar y desplegar alguna otra alternativa más ligera.

En las siguientes páginas se recopilará toda la información posible acerca de ambas herramientas y sus características utilizando únicamente su *documentación oficial*.

A.1. PacketFence

"PacketFence es una solución de control de acceso a la red (NAC) totalmente respaldada, confiable y de código abierto. Con un impresionante conjunto de características que incluye un portal cautivo para el registro y la remediación, administración centralizada cableada e inalámbrica, compatibilidad con 802.1X, aislamiento de capa 2 para dispositivos problemáticos, integración con el Snort IDS y el escáner de vulnerabilidades de Nessus; PacketFence se puede utilizar para proteger redes de forma efectiva, desde redes pequeñas hasta redes heterogéneas muy grandes." [1]

A.1.1. Características

Modo de implementación (enforcement mode):

- Out-of-band Deployment (despliegue fuera de banda):

  El modo de operación de PacketFence está completamente fuera de banda, lo que permite que la solución pueda escalarse geográficamente y sea más resistente a posibles fallos. Cuando se utiliza la tecnología adecuada (como la seguridad de puertos), un único servidor PacketFence puede ser utilizado para proteger cientos de switches y muchos miles de nodos conectados a ellos.

  A diferencia del modo de despliegue en línea, en el despliegue fuera de banda no todo el tráfico entrante y saliente de la red circulará a través del servidor de PacketFence. Una vez se haya atendido la petición de acceso, el tráfico generado por el nodo autorizado no circulará a través de PacketFence.

[1] https://packetfence.org/about.html#/overview

- Inline Deployment (despliegue en línea):

  Mientras que el despliegue fuera de banda es el método preferido de implementar PacketFence, el despliegue en línea también esta disponible para equipamiento cableado o inalámbrico que no sea manejable.

  A diferencia del despliegue fuera de banda, todo el tráfico que circule por la red circulará a través de PacketFence.

Autenticación y registro:

- Soporte para 802.1X:

  Packetfence incorpora soporte para el estándar de autenticación y autorización 802.1x, ya sea mediante conexión cableada o conexión inalámbrica, gracias al módulo de FreeRADIUS que incluye PacketFence. Para ello pueden utilizarse PEAP-TLS, EAP-PEAP y muchos más mecanismos EAP.

- Registro de dispositivos:

  Packetfence ofrece una solución parecida a la de los portales cautivos, pero con un distintivo importante. A diferencia de la mayoría de soluciones basadas en portales cautivos, los miembros de PacketFence que hayan sido previamente registrados tendrán acceso automático sin requerir ninguna otra autenticación, aunque esta opción es también configurable. Puede especificarse una Política de Uso para que los usuarios no puedan tener acceso a la red hasta que la acepten.

- Integración inalámbrica:

  PacketFence se integra perfectamente en redes inalámbricas gracias al módulo FreeRADIUS que está incluido en el paquete. Esto puede permitir securizar redes cableadas o inalámbricas de la misma manera, utilizando la misma base de datos de usuarios y utilizando el mismo portal cautivo. Además ofrece soporte para diferentes fabricantes de Puntos de Acceso (AP) y controladores inalámbricos.

- Soporte de Voz sobre IP (VoIP):

  También conocido como *Telefonía IP (IPT)*, la VoIP esta totalmente integrada (incluso en entornos heterogéneos) para múltiples fabricantes (Cisco, Edge-Core, HP, LinkSys, Nortel Networks, etc.).

- Detección de actividades anómalas sobre la red:

  Las actividades anormales sobre la red (equipos infectados por virus, gusanos, spyware, tráfico denegado por políticas de establecimiento, etc.) pueden ser detectadas mediante Snort, Suricata u otros sensores comerciales. La inspección de contenido es también posible con Suricata, y puede combinarse con bases de datos de hashes malware como OPSWAT Metadefender. Además de una simple detección, PacketFence ofrece su propio mecanismo de alerta y supresión en cada tipo de alerta. Los administradores tienen la opción de configurar un conjunto de acciones para cada violación.

- Windows Managemente Instrumentation (WMI):

  PacketFence permite al administrador realizar auditorías y ejecutar comandos entre otras opciones sobre ordenadores Windows. Por ejemplo, PacketFence puede verificar si hay algún software no autorizado instalado y/o ejecutándose antes de permitir el acceso a la red.

- Estado de salud:

  A la hora de hacer una autenticación de usuario mediante 802.1x, PacketFence puede realizar una completa evaluación del dispositivo que realiza la petición de conexión utilizando el protocolo de Estado de Salud TNC (Trusted Network Connect Statement of Health protocol). Por ejemplo, PacketFence puede verificar si el dispositivo tiene instalado algún antivirus y si está actualizado, si se han aplicado parches al sistema operativo, etc. Una de las grandes ventajas de esta característica es que no será necesario instalar ningún tipo de software en los dispositivos extremos.

- Agentes de seguridad:

  PacketFence se integra con soluciones de agentes de seguridad como OPSWAT Metadefender Endopoint Management, Symantec SEPM y otros. Puede asegurarse de que el agente está siempre instalado antes de conceder el acceso a la red.También puede comprobar la situación en la que se encuentra un dispositivo extremo y aislarlo.

- Remediación a través de Portal Cautivo:

  Una vez atrapado un usuario, todo el tráfico de red que lo involucre estará determinado por PacketFence. Basándose en el estado actual del nodo (no registrado, violación abierta, etc.), el usuario sera redirigido una URL apropiada. En caso de violación, se mostrarán instrucciones al usuario para la concreta situación en la que se encuentra reduciendo la costosa intervención del servicio de asistencia técnica.

- Aislamiento de dispositivos problemáticos:

  Packetfence cuenta con varias técnicas de aislamiento, incluyendo aislamiento por VLAN con soporte para VoIP para múltiples fabricantes.

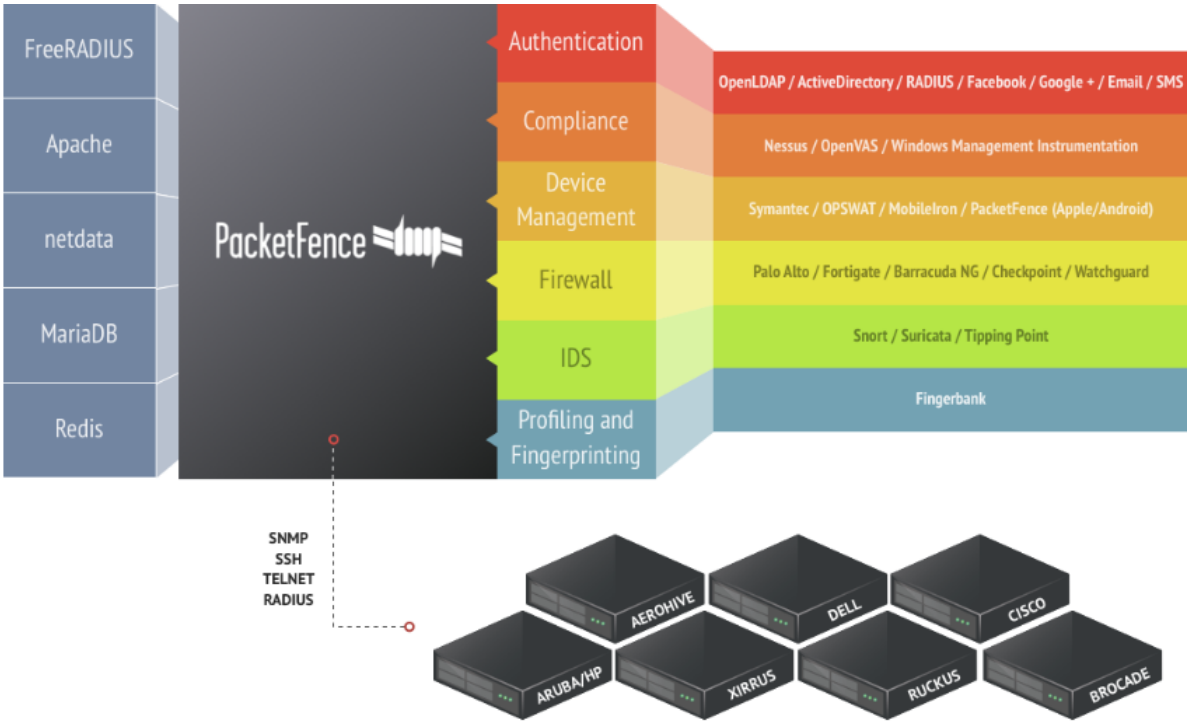


Figura A.1: Arquitectura de componentes de PacketFence

A.1.2. Características avanzadas

- Gestión flexible de VLAN y control de acceso basado en roles:

  La solución está basada sobre el concepto de aislamiento de red mediante asignaciones de VLAN. Para ello no es necesario cambiar la topología de red existente, lo único que será necesario para ello es crear dos VLANs nuevas, una para el registro y otra para el aislamiento. Además, también soporta el método por roles de diferentes fabricantes.

  La VLAN y los roles pueden asignarse utilizando distintos medios:

  1. Por Switch (por defecto para VLAN)
  2. Por categoría del cliente (por defecto para los roles)
  3. Por cliente
  4. Utilizando cualquier decisión arbitraria (si se utilizan extensiones de Perl)

  Además, el método Por Switch puede combinarse con los demás. Por ejemplo, con una configuración por defecto de PacketFence, puede asignarse una VLAN o un rol a impresoras o PCs (en caso de estar categorizadas correctamente) basándose sobre a qué equipo están conectados. Esto implica que pueden conseguirse de forma sencilla VLANs del tipo "por edificio" o "por dispositivo".

- Acceso de invitados - BYOD:

  PacketFence ofrece soporte para un rol o una VLAN especial para invitados. Si se activa una VLAN para invitados, hay que configurar la red de forma en que dicha VLAN de invitados únicamente pueda tener acceso a internet, a la VLAN de registro y al Portal Cautivo para saber como registrarse para conseguir el acceso o cómo funciona el mismo. Hay diferentes métodos para el registro de invitados (en caso de requerirlo):

  - Registro manual de los invitados.
  - Contraseña del día (Password of the day)
  - Autoregistro (con o sin credenciales)
  - Patrocinio de acceso a invitados (un empleado que responde ante un invitado)
  - Acceso de invitados mediante confirmación de email
  - Acceso de invitados mediante confirmación de móvil (vía SMS)
  - Acceso de invitados mediante autenticación de Facebook/Google/GitHub

- Más tipos de violaciones integradas:
  - DHCP Fingerprints (huella DHCP): Puede bloquear dispositivos basados en su huella DHCP. Prácticamente todos los sistemas operativos tienen una huella DHCP única, por lo que se puede bloquear el acceso a la red a diferentes dispositivos basándonos en dicha huella.
  - Direcciones MAC: Se pueden especificar ciertos patrones de direcciones MAC a los que no se quiera conceder acceso. De esta manera podemos evitar que acceda a la red, por ejemplo, un fabricante específico.
- Registro automático:
  - Por dispositivo de red
  - Por huella DHCP
  - Por fabricante en dirección MAC
- Soporte para PKI y EAP-TLS:

  PacketFence soporta EAP-TLS para la autenticación basada en certificados, y también proporciona una pequeña solución PKI que puede ser utilizada para generar un certificado TLS para cada dispositivo o cada usuario. Además también se integra con la solución PKI de Microsoft. PacketFence utilizará el Simple Certificate Exchange Protocol (SCEP) para hablar con el Network Device Enrollment Service (NDES) de Microsoft para crear el certificado apropiado durante un proceso de incorporación de dispositivos finales.
- Contabilidad de ancho de banda
- Integración de Directorio Activo de Microsoft
- Despliegue gradual
- Extensible y personalizable

- Autenticación flexible:

  PacketFence puede autenticar a los usuarios utilizando varios protocolos/estándares. Esto permite integrar PacketFence en la red sin la necesidad de que los usuarios finales tenga que memorizar otra cuenta y contraseña. Las fuentes de autenticación soportadas son las siguientes:

  - LDAP:
    - Directorio Activo de Microsoft
    - Novell eDirectory
    - OpenLDAP
  - RADIUS:
    - Cisco ACS
    - RADIUS (FreeRADIUS, Radiator, etc.)
    - Microsoft NPS
  - Fichero local de usuarios (formato htpasswd de Apache)
  - OAuth2:
    - Facebook
    - Google
    - GitHub
    - LinkedIn
    - Microsoft Live
    - Twitter

- Basado en estándares:

  PacketFence está construido para utilizar estándares abiertos y evitar el bloqueo de proveedores. Entre estos estándares se encuentran:

  - 802.1X
  - Simple Network Management Protocol (SNMP)
  - RADIUS
  - Netflow / PIFIX
  - Wireless ISP Roaming (WISPR)

A.2. openNAC

"openNAC es un control de acceso a la red de código abierto para entornos corporativos LAN / WAN. Permite la autenticación, autorización y auditoría basada en políticas de acceso a la red. Soporta diferentes proveedores de red como Cisco, Alcatel, 3Com o Extreme Networks, y diferentes clientes como PCs con Windows o Linux, Mac y dispositivos como smartphones y tablets.

Basado en componentes de código abierto y autodesarrollo, se basa en estándares de la industria como FreeRadius, 802.1x, AD, LDAP, ... Es muy extensible, se pueden incorporar nuevas funcionalidades debido a su arquitectura en plugins. Fácilmente integrable con los sistemas existentes.

Por último, pero no por ello menos importante, proporciona servicios de valor añadido como la gestión de la configuración, la red, las configuraciones de backup, la detección de redes y la monitorización de redes." [2]

A.2.1. Características

- Control de Acceso a la Red para entornos corporativos LAN / WAN
- Habilita el acceso a la red basado en políticas de autenticación, autorización y auditoría
- Solución compatible con varios proveedores / fabricante
- Basado en componentes Open Source y auto-desarrollo
- Basado en estándares de la industria como RADIUS, 802.1x, LDAP, etc.
- Extensible, se pueden incorporar nuevas características
- Integración fácil con sistemas existentes
- Añade servicios con valor añadido como la administración de la configuración, red, configuraciones de backup, detección de redes (Network Discovery) y monitorización de redes (Network Monitoring)

[2] http://www.opennac.org/opennac/en/about/what-is-opennac.html

A.2.2. Características avanzadas

- Autenticación basada en el estándar 802.1x para dispositivos compatibles
- Soporte de autenticación basado en LDAP o DA (Directorio Activo)
- Soporte para detectar dispositivos corruptos utilizando 802.1x o SNMP traps
- Configuración en masa para dispositivos en línea utilizando el módulo onNetConf
- Bakcups en masa para dispositivos en línea utilizando el módulo onNetBackup
- Detección de sistema operativo, antivirus, firewall y actualizaciones del Sistema Operativo para implementar una política de acceso

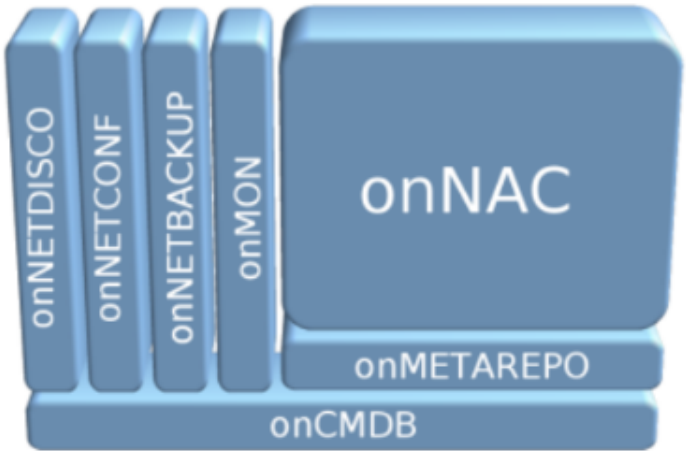


Figura A.2: Estructura modular de openNAC

A.3. Resumen

Teniendo en cuenta la información obtenida a través de las páginas web oficiales de cada una de las herramientas, se puede comprobar como en la web de PacketFence puede encontrarse muchísima más información acerca de su producto, así como una explicación breve de cada una de las características que incluye, mientras que en la página web de openNAC únicamente podemos encontrar un listado de las características que incluye e información acerca de las utilidades del producto en general, y un breve resumen sobre cada uno de los módulos que lo componen. Esta primera impresión decanta la balanza a favor de PacketFence, sin ni siquiera haber entrado en detalle aún.

A continuación se expondrán las diferencias acerca de las características más útiles para este proyecto de cada una de estas herramientas ilustradas mediante una tabla.

Característica	**PacktFence**	**openNAC**
Despliegue híbrido (fuera de banda + en línea)	SI	NO
Soporte para 802.1X	SI	SI
Registro de dispositivos	SI	NO
Detección de actividades anómalas en la red	SI	NO
Remediación mediante Portal Cautivo	SI	NO
Control de acceso basado en Roles	SI	NO
Acceso de invitados (BYOD)	SI	NO
Soporte para PKI y EAP-TLS	SI	NO
Basado en estándares	SI	SI
Detección y monitorización de redes	NO	SI
Soporte basado en LDAP o DA	SI	SI
Políticas de acceso personalizables	SI	SI
Configuración en masa para dispositivo en línea	NO	SI

Tabla A.1: Tabla de comparación de características entre PacketFence y openNAC

A.4. Conclusiones

Puede comprobarse a simple vista cómo PacketFence contiene muchas más características que openNAC. Aunque algunas de ellas no vayan a ser utilizadas en este momento, no está de más que las incluya, ya que pueden ser útiles en un futuro una vez la herramienta esté desplegada en el sistema.

Cierto es que hay utilidades de openNAC que podrían resultar útiles como por ejemplo la detección y monitorización de redes, que no es absolutamente necesaria, o la configuración en masa para dispositivos en línea, que tampoco es necesaria ya que en el BCBL cuentan con herramientas en funcionamiento que cumplen el mismo propósito.

Por si la balanza no estuviese lo suficientemente a favor de PacketFence con lo mencionado hasta ahora, hay una característica por la que openNAC no puede ser la ganadora de esta comparativa y se trata nada menos que el Soporte para PKI y EAP-TLS. Teniendo en cuenta el tipo de control de acceso que quieren implementar en la red del BCBL (autenticación de máquinas basada en certificados) resultará imposible hacerlo mediante openNAC, ya que no tiene soporte para EAP-TLS, por lo que esta opción queda definitivamente descartada y por tanto la *herramienta seleccionada para la realización del proyecto ha sido* ***PacketFence***.

B. ANEXO

Instalación y configuración inicial de PacketFence en CentOS 7

En este documento se explicará como se ha instalado PacketFence en la máquina a modo de guía para usuarios.

Requisitos Hardware mínimos:

- CPU Intel o AMD de 3 GHz
- 8GB de RAM
- 100 GB de espacio en disco (se recomienda RAID-1)
- 1 tarjeta de red (se recomiendan 2)

Sistema Operativo requerido (uno de los tres):

- Red Hat Enterprise Linux 7.x Server
- Community ENTerprise Operating System (CentOS) 7.x
- Debian 8.0 (Jessie)

El primer paso para los Sistemas Operativos basados en Red-Hat será desactivar el *Firewall* y *SELinux*, además de asegurarnos de que la base de datos de *yum* está debidamente actualizada, para ello ejecutaremos los siguientes comandos:

```
[root@TFG01 ~]# echo "SELINUX = disabled" > /etc/selinux/config
[root@TFG01 ~]# systemctl disable firewalld
[root@TFG01 ~]# yum update
```

Además de esto, también debemos decir explícitamente al *Network Manager* que nunca interactúe con nuestra configuración DNS, para ello ejecutamos lo siguiente:

```
[root@TFG01 ~]# echo "[main]
dns=none" > /etc/NetworkManager/conf.d/99-no-dns.conf
[root@TFG01 ~]# systemctl restart NetworkManager
```

Una vez realizados estos pasos, podemos acceder a descargar e instalar PacketFence. Para ello tendremos que añadir el repositorio de PacketFence a *yum* y después descargarlo e instalarlo:

```
[root@TFG01 ~]# yum localinstall http://packetfence.org/downloads/PacketFence/
RHEL7/‘uname -i‘/RPMS/packetfence-release-1.2-6.el7.centos.noarch.rpm
[root@TFG01 ~]# yum install --enablerepo=packetfence packetfence
```

Tras realizar estos pasos, PacketFence ya estará instalado en la máquina. A partir de este punto, la mayoría de configuraciones se realizarán mediante la interfaz web, ya que es una manera más sencilla y visual que la de editar ficheros de configuración, aunque habrá configuraciones que requieran de ello. Para acceder a la interfaz web de PacketFence, tendremos que escribir `https://@ip_packetfence:1443/configurator` en la barra de búsqueda de cualquier navegador web, donde encontraremos el asistente para la cofiguración inicial de PacketFence.

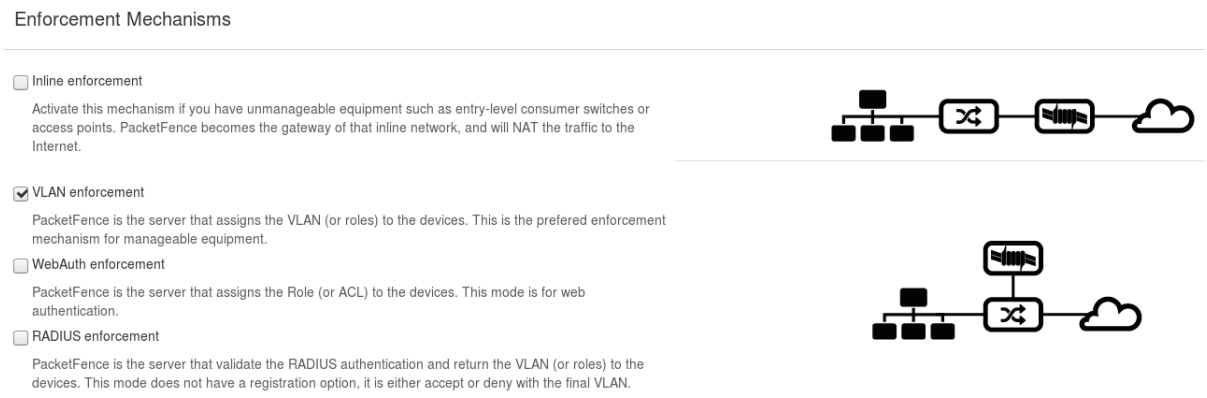


Figura B.1: Paso nº1 en la configuración de PacketFence (Interfaz Web)

En este primer paso tendremos que elegir un tipo de implementación *(enforcement)*, que en este caso será la opción *VLAN enforcement*.

Una vez seleccionado el tipo de implementación, el segundo paso será configurar las interfaces de la máquina virtual. Tal y como se explica en el capítulo 5, esta máquina virtual dispone de tres interfaces de red, cada una conectada a una VLAN:

1. Interfaz ens160: IP = 192.168.70.25 / 24 - VLAN = dvTesting_LAN (VLAN ID 70)
2. Interfaz ens192: IP = 192.168.76.25 / 24 - VLAN = dvIsolation (VLAN ID 76)
3. Interfaz ens224: IP = 192.168.75.25 / 24 - VLAN = dvRegistration (VLAN ID 75)

Estas interfaces tendrán que aparecer listadas en este segundo paso de la configuración. Para configurarlas, haremos click sobre el nombre de cada una de ellas donde tendremos que rellenar un pequeño formulario como el que se muestra en la siguiente imagen:

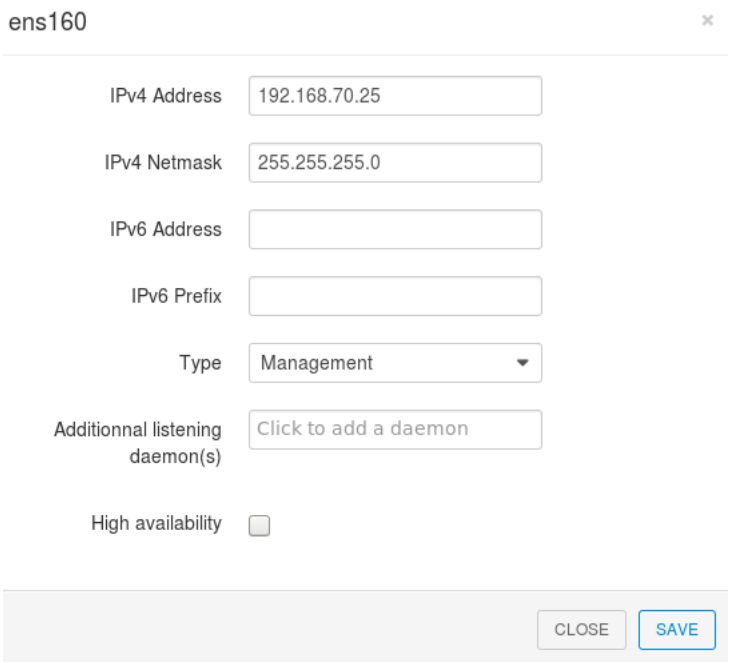


Figura B.2: Paso nº2 en la configuración de PacketFence (Interfaz Web)

En este formulario tendremos que escribir la dirección IP de la interfaz que estamos configurando, la máscara de la red a la que está conectada y el "tipo" de VLAN, es decir, si se trata de una VLAN de registro, de aislamiento o de administración.

Las interfaces se han configurado de la siguiente manera:

- Interfaz ens160: Type = Management (VLAN ID 70)
- Interfaz ens192: Type = Isolation (VLAN ID 76)
- Interfaz ens224: Type = Registration (VLAN ID 75)

Nótese que cuando asignamos el tipo *Isolation* o *Registration* a una de las interfaces aparecerá un pequeño *checkbox* activado que dice "Enable DHCP Server". Esto se debe a que PacketFence asignará direcciones IP a las máquinas que accedan a dichas VLANs mediante DHCP. En el resto de VLANs será el servidor DHCP del dominio quien asigne las direcciones IP.

En el siguiente paso, tendremos que crear un usuario *root* para la base de datos, crear la propia base de datos y crear una cuenta de usuario para el propio PacketFence. En esta base de datos se almacenarán todos los nodos que intenten acceder a la red a través de PacketFence, así como los usuarios autenticados, usuarios administradores, ciertas configuraciones de PacketFence e incluso algún que otro archivo de *log*.

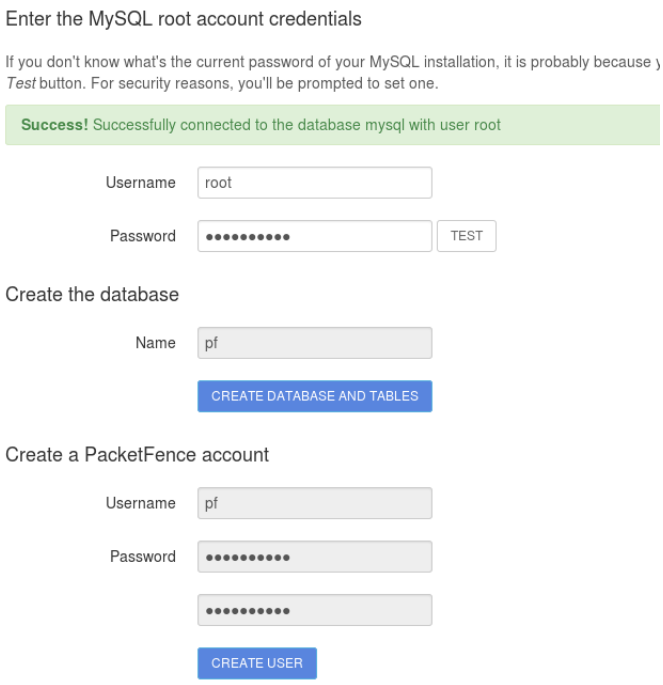


Figura B.3: Paso nº3 en la configuración de PacketFence (Interfaz Web)

Una vez configurados los usuarios y creada la base de datos, en el siguiente paso PacketFence requerirá información acerca del dominio:

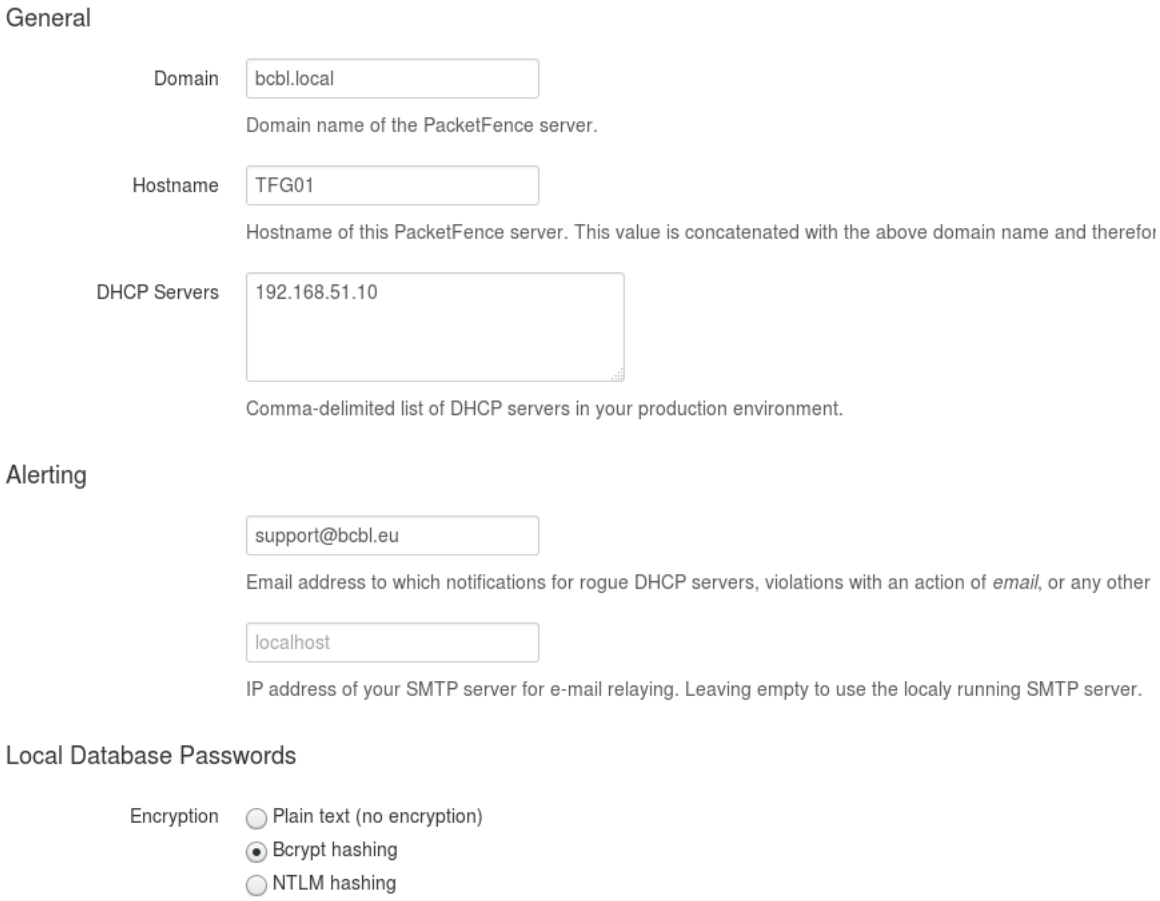


Figura B.4: Paso nº4 en la configuración de PacketFence (Interfaz Web)

En el paso número 5 de este asistente de configuración tendremos que asignar una contraseña a la cuenta de administrador (de nombre “admin”) para PacketFence. Esta cuenta será la cuenta desde la que se realizará toda la configuración, al menos por defecto, ya que más tarde podremos añadir usuarios con privilegios de administración para que, por ejemplo, cualquier empleado del departamento de IT pueda tener acceso a la configuración de PacketFence.

Para cambiar la contraseña, solamente hay que rellenar el formulario que aparece en pantalla escribiendo dos veces la contraseña que queremos asignarle. Una vez hecho esto, hacer click sobre el botón que dice "MODIFY THE PASSWORD". En caso de no haber ningún error, aparecerá una mensaje de confirmación.

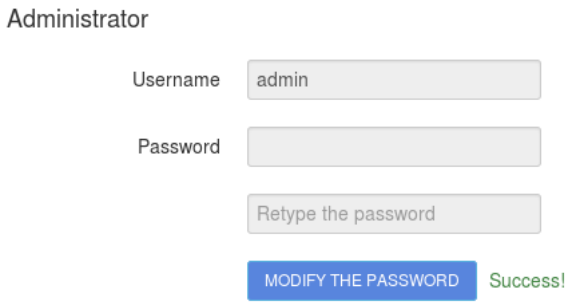


Figura B.5: Paso nº5 en la configuración de PacketFence (Interfaz Web)

Una vez realizados estos 5 pasos de configuración, PacketFence estará listo para empezar a funcionar, aunque obviamente habrá que configurar muchísimas cosas más, ya que esta configuración no es más que una configuración mínima para poder poner en funcionamiento la herramienta.

Antes de la confirmación, nos encontraremos con un paso intermedio (número 6) que servirá para añadir un detector de dispositivos llamado "Fingerbank", que es capaz de detectar todos los dispositivos que estén conectadas a la red, además de detalles más específicos como el Sistema Operativo que utilizan y qué versión de la misma tienen instalada. Este software se basa en la dirección MAC del dispositivo, en los mensajes DHCP que envía, sus firmas en los sockets TCP y en el *User-Agent* del navegador para recopilar toda esta información. Estos dispositivos pueden referirse a relojes inteligentes, teléfonos móviles, tablets, etc. En este caso no se activará, ya que por ahora no va a necesitar detectar ningún dispositivo que no sea un ordenador.

El último paso de este asistente será nada menos que la confirmación de que todas las configuraciones anteriores eran correctas. En esta ventana aparecerán todos los servicios o *demonios* que PacketFence pondrá en marcha en un estado *"Stopped"*. En el momento que pulsemos sobre el botón "START PACKETFENCE" pasarán a un estado *"Starting"* para terminar (si todo ha ido correctamente) en el estado *"Started"*.

Una vez terminada la instalación se podrá acceder a la página de configuración de PacketFence a través del navegador web, al igual que en la fase de instalación (`https://@ip_packetfence:1443`). Para acceder a ella tendremos que hacerlo mediante el usuario "admin" y la contraseña que se le asignó en el paso nº5(B.5) de la instalación.

En la página principal de PacketFence podemos encontrar diversa información acerca del *host* sobre el que está corriendo el software, como por ejemplo el uso del disco, carga media del sistema, RAM del sistema, etc.

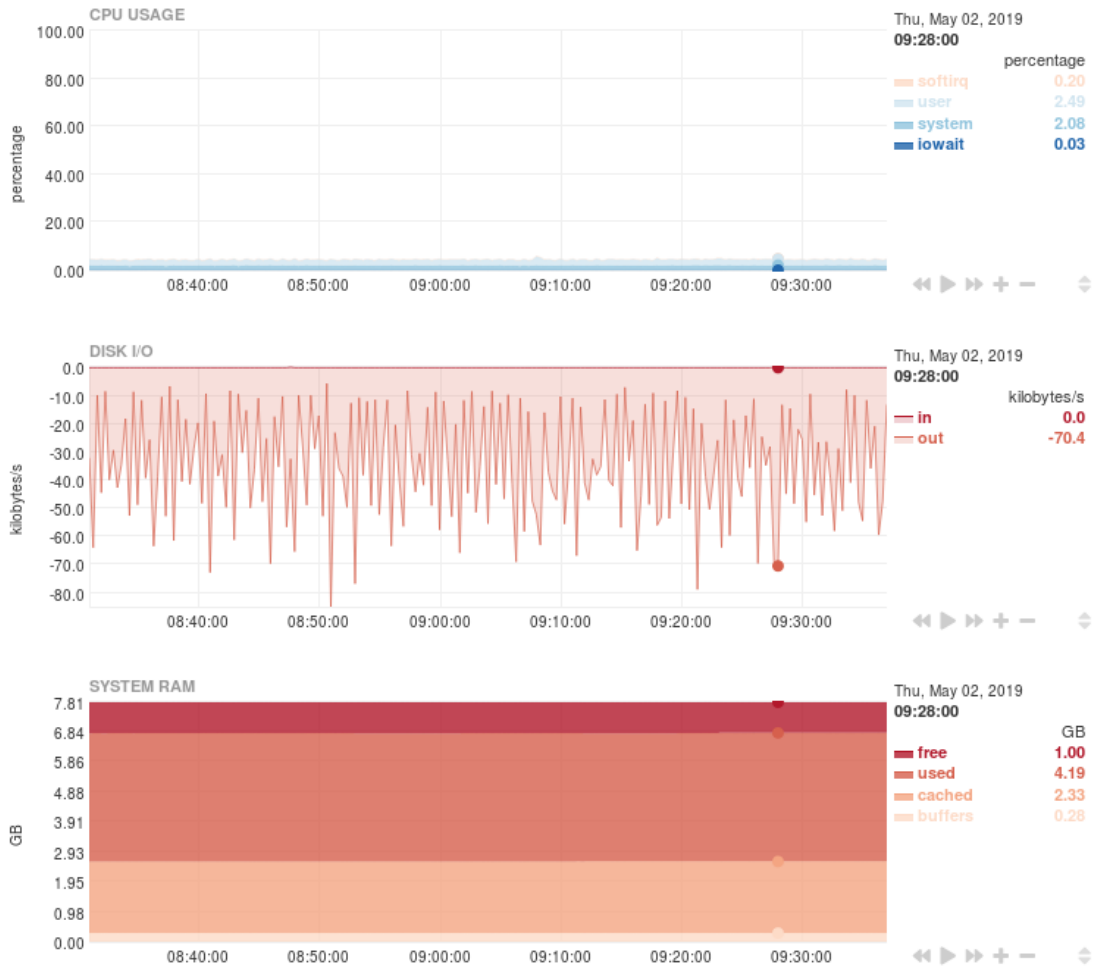


Figura B.6: Página principal de administración de PacketFence

C. ANEXO

Configuración de Microsoft Active Directory 2008 R2 Enterprise

Para la configuración del servidor, el departamento de IT ha instalado un Windows Server 2008 R2 Enterprise en una máquina virtual (se disponía de la licencia anteriormente) a la que se le ha llamado **TFG03**.

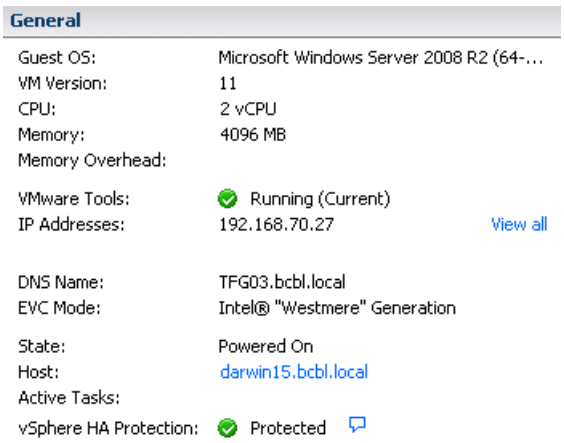


Figura C.1: Parámetros generales de la máquina virtual **TFG03**

El primer paso será crear un usuario administrador del servidor y otro para correr el servicio en sí. Estos usuarios han sido nombrados **SCEPAdmin** y **SCEPSvc** respectivamente. El usuario SCEPAdmin tendrá derechos de administrador sobre el propio servidor, mientras que el usuario SCEPSvc tendrá que ser parte del grupo **IIS_IUSRS**.

Una vez creados los usuarios necesarios, el siguiente paso será instalar un "rol" *ADCS (**A**ctive **D**irectory **C**ertificate **S**ervices)*. Para ello hay que hacer click sobre el enlace "*Add Roles*". Realizado este paso, aparecerá un asistente de instalación de roles, donde hay que seleccionar la casilla *Active Directory Certificate Services* y pulsar sobre el botón *Next* >.

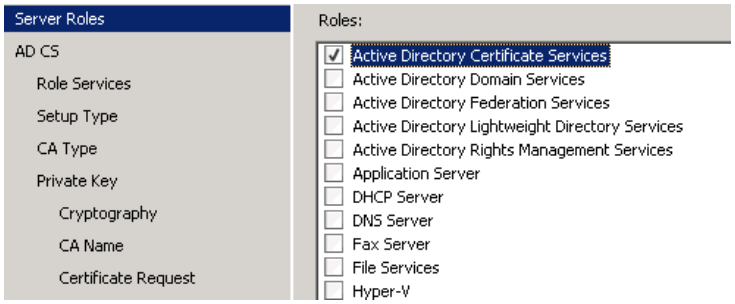


Figura C.2: Ventana de asistente de instalación de roles en *Windows Active Directory*

En este momento se puede comprobar como la opción *Network Device Enrollment Service* sí aparece en la lista, por lo que el siguiente paso consistirá en eleccionar la casilla NDES y pulsar sobre el botón *Next* >:

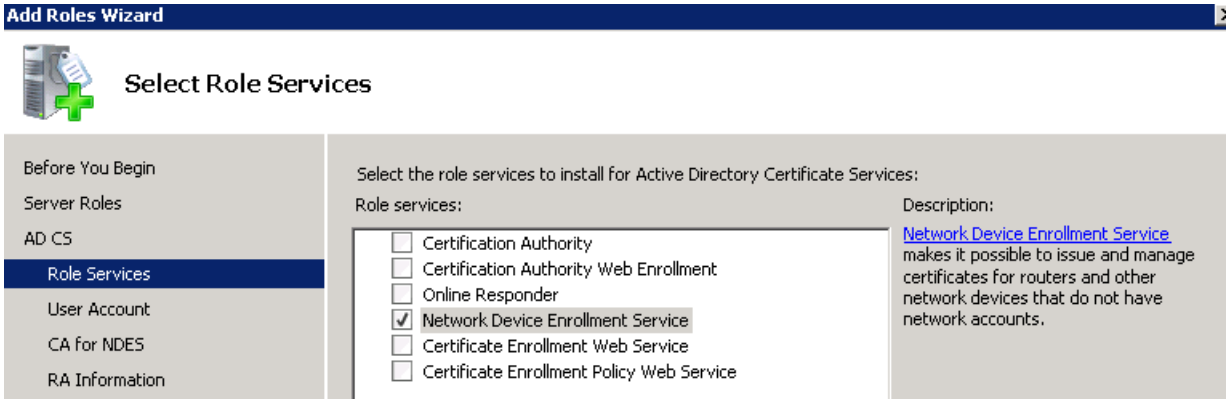


Figura C.3: La opción NDES sí aparece en Windows Active Directory 2008 R2 *Enterprise*

El segundo paso en este asistente *(User Account)* consiste en especificar la cuenta de usuario que el servicio utilizará para ejecutar sus procesos. Esta cuenta debe de estar incluido en el grupo IIS_IUSRS, por lo que se utilizará la cuenta de usuario SCEPSvc que se ha preparado previamente. En caso de especificar un usuario que no esté incluido en el mencionado grupo se obtendrá un mensaje de error.

En el tercer paso dentro de este asistente, hay que especificar la *Certification Authority (CA)* que emitirá los certificados. Podría utilizarse el mismo servidor que está siendo configurado, pero ya que existe una CA activa y en funcionamiento en la red, será la que se utilizará. Para ello se puede añadir el nombre que la CA tiene en el dominio, en este caso *acc.bcbl.local*.

El cuarto paso consiste en introducir información acerca del *Registration Authority (RA)* que estamos configurando. La información introducida en el formulario es la siguiente:

- RA NAME: *TFG03-MSCEP-RA*
- Country/Region: *ES (Spain)*
- E-mail: *support@bcbl.eu*
- Company: *BCBL*
- Department: *IT*
- City: *Donostia*
- State/Province: *Guipúzcoa*

En el siguiente paso hay que especificar la criptografía que se utilizará para la Clave de Firma y la Clave de Encriptado. Ya que no hay requisitos específicos por parte del BCBL, se utilizarán los valores por defecto que aparecen en la ventana.

El último paso de este asistente será la confirmación de los datos introducidos hasta este punto. Para ello comprobamos que los datos que aparecen en la ventana son correctos y hacemos click sobre el botón "Install".

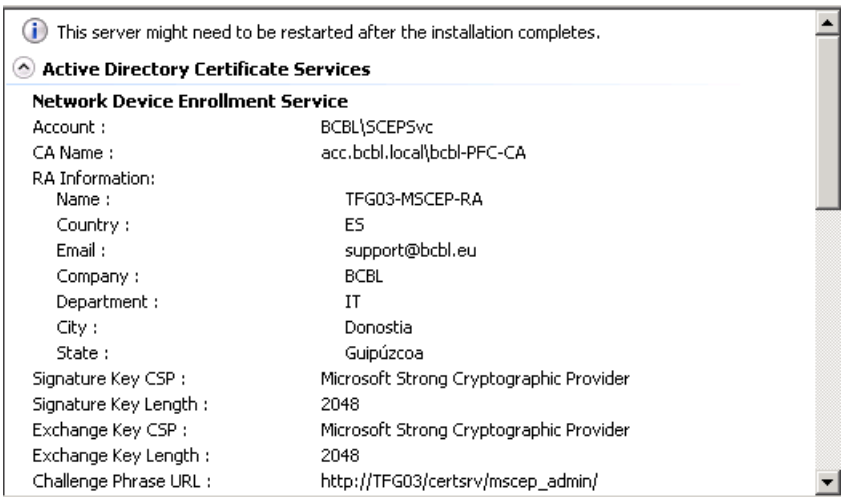


Figura C.4: Resumen de la configuración del RA

Una vez que los servicios se hayan instalado correctamente en el servidor hay que pasar a configurarlos. El protocolo SCEP está configurado de forma en que si un usuario (o máquina) realiza una petición para recibir un certificado, tendrá que saber una contraseña que se encuentra en la dirección `http://TFG03/certsrv/mscep_admin/` y para acceder a dicha dirección se requieren credenciales de administrador del servidor.

Esta opción está bien si se quiere que todos los usuarios que requieran un certificado tengan que pasar este control de seguridad, el cual no podrán traspasar sin ponerse en contacto con el departamento de IT y poder conseguir esa contraseña para poder pedir el certificado, aunque no es el escenario que desean en el BCBL, ya que la idea es que los equipos conectados a la red puedan enrolarse automáticamente *(autoenrollment)* por lo que tendremos que configurar esta característica.

Para ello tendremos que hacer click sobre la tecla de Windows, escribir *regedit* y pulsar Enter. Se abrirá una ventana por la cual iremos navegando en el árbol de directorios que aparece en la columna de la izquierda hasta llegar a *HKEY_LOCAL_MACHINE –>SOFTWARE –>Microsoft –>Cryptography –>MSCEP –>UseSinglePassword* y una vez aquí cambiar el valor del registro *"UseSinglePassword"* a 1. Mediante este cambio forzaremos a que la contraseña necesaria para "autoenrrolarse" sea la misma para todos los equipos, así podrá ser añadida al script *autoenrollment.sh (Anexo E)*. De esta manera, todos los equipos que ejecuten dicho script obtendrán un certificado, pero si un usuario quiere descargarlo manualmente no podrá hacerlo ya que no dispondrá de dicha contraseña para realizar la petición.

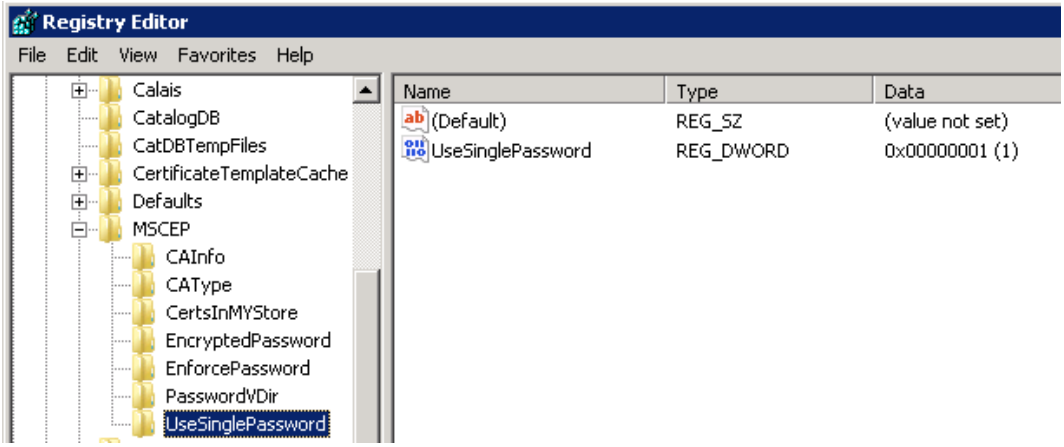


Figura C.5: Ventana para el cambio de valor del registro *UseSinglePassword*

Se recomienda extender la longitud máxima permitida para las URL para evitar problemas, para ello hay que escribir las siguientes líneas en la línea de comandos del servidor:

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.
webserver /security/requestFiltering /requestLimits.maxQueryString:"16384"
/commit:apphost
```

En este punto hay que proceder a crear un duplicado de la plantilla del certificado que se quiere distribuir a través del protocolo SCEP. En este caso se ha decidido duplicar la plantilla llamada *"Computers"* puesto que es el certificado que se emite automáticamente en los equipos con Sistema Operativo Windows. Para ello hay que acceder a la CA del dominio y navegar por el árbol de directorios que aparece en la parte izquierda hasta llegar a *Roles –>Active Directory Certificate Services –>Certificate Templates (acc.bcbl.local)*.

En este directorio aparecerá una lista de todas las plantillas de certificados que hay guardados en la CA. Para crear un duplicado de una plantilla hay que hacer click derecho sobre el nombre de cualquiera de ellas, hacer click sobre *"Duplicate Template"* y en la ventana emergente seleccionar *"Windows Server 2003 Enterprise"*.

Se abrirá una nueva ventana donde se podrán establecer diferentes parámetros asociados al certificado que se emitirá utilizando la actual plantilla. En este caso se ha cambiado el nombre por **NDES_Computers**, y se ha seleccionado la opción *"Supply in the request"* dentro de la pestaña *"Subject Name"*, y los demás parámetros se han dejado con sus valores por defecto.

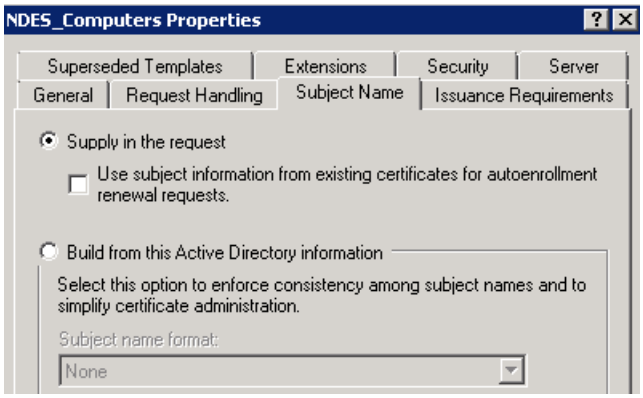


Figura C.6: Ventana de configuración de plantilla NDES_COMPUTERS

Una vez creada la plantilla para los nuevos certificados hay que realizar un último paso para que puedan ser emitidos. Para ello hay que acceder al directorio *Roles –>Active Directory Certificate Services –>bcbl-PFC-CA (nombre de la CA)*, hacer click derecho sobre el directorio *"Certificate Templates –>New –>Certificate Template to Issue"* y en la lista que aparecerá en pantalla seleccionar la plantilla que se acaba de crear y hacer click sobre el botón *"OK"*.

Terminada la configuración acerca de los nuevos certificados a emitir en la CA del dominio, el siguiente paso será cambiar los valores de ciertos registros en la máquina TFG03. Para ello hay que abrir el editor de registros y navegar hasta el directorio *HKEY_LOCAL_MACHINE –>SOFTWARE –>Microsoft –>Cryptography –>MSCEP*. Los registros *"EncryptionTemplate", "GeneralPurposeTemplate"* y *"SignatureTemplate"* tendrán el valor *"IPSECIntermediateOffline"*, el cual habrá que cambiar por el valor **NDES_Computers**.

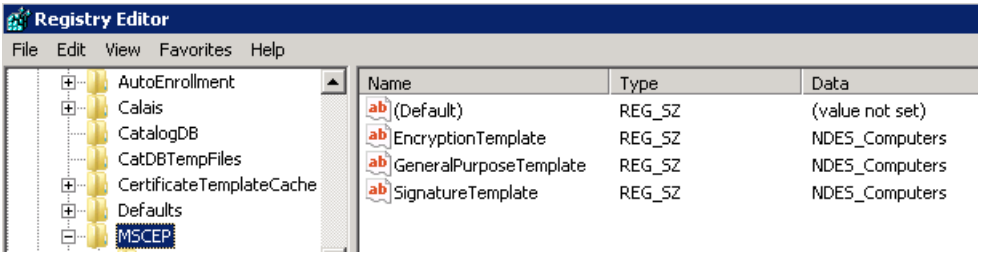


Figura C.7: Registros MSCEP

El último paso para terminar de configurar el Directorio Activo es el de configurar el servidor web para que puedan realizarse peticiones de certificados y la descarga de los mismos vía web. Para ello hay que acceder a *Roles –>Web Server (IIS) –>Internet Information Services (IIS) Manager*. En este punto hay que navegar por el árbol de directorios que aparecerá en la ventana del centro hasta llegar a *TFG03 (BCBL/SCEPAdmin) –>Sites –>Default Web Site –>CertSrv –>mscep* y hacer doble click sobre *"Authentication"*. Click derecho sobre *Anonymous Authentication –>Edit* y seleccionar *"Application pool identity"*.

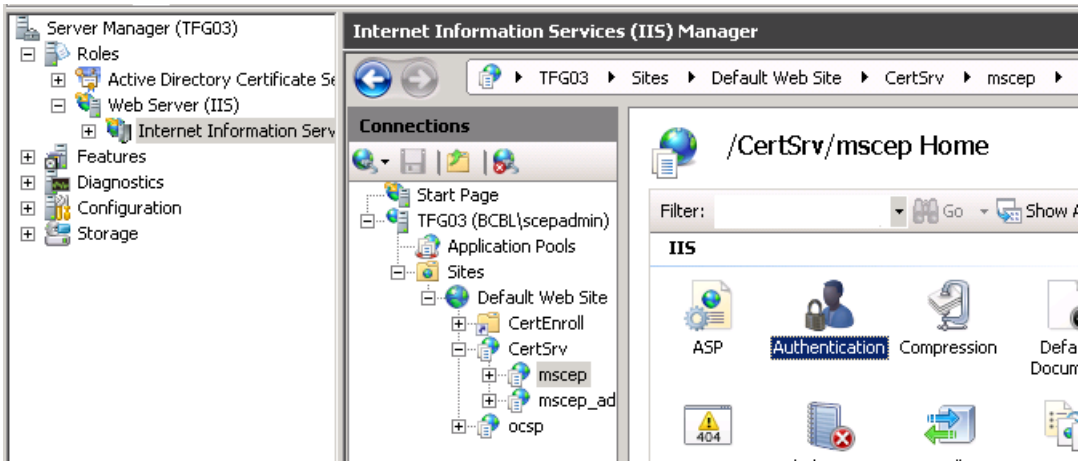


Figura C.8: Ruta hasta la opción *"Authentication"* en IIS

Como último paso para terminar de configurar el servidor web, y por tanto, la configuración del Directorio Activo, hay que navegar hasta *Roles –>Web Server (IIS) –>Internet Information Services (IIS) Manager*. En este punto hay que navegar por el árbol de directorios que aparecerá en la ventana del centro hasta llegar a *TFG03 (BCBL/SCEPAdmin) –>Application Pools*.

En esta ventana hay que configurar dos *"App Pools"*.

La primera será *"DefaultAppPool"*, sobre la que hay que hacer click derecho y seleccionar *"Advanced Settings..."* y una vez ahí, buscar el bloque de opciones *"Process Model"*. Una vez encontrado hay que cambiar dos parámetros dentro del mismo, el primero será *"Identity"*, donde habrá que seleccionar la opción *"Built-in account:"* y elegir **NetworkService** en la lista desplegable. El segundo parámetro a cambiar es el que dice *"Load User Profile"*, al cual habrá que asignar el valor **False**.

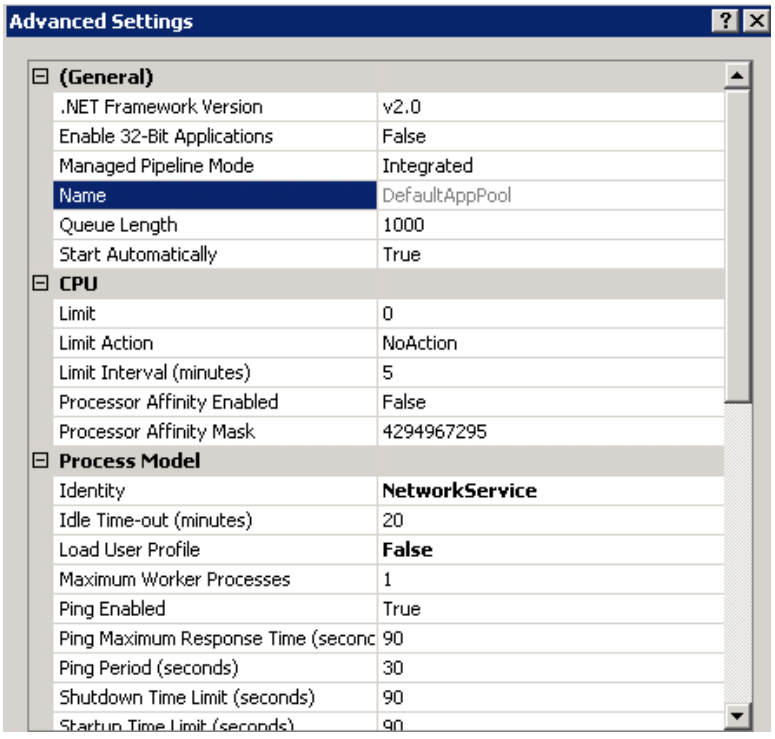


Figura C.9: Configuración de la *App Pool* **DefaultAppPool**

La segunda será *"SCEP"*. De la misma manera, click derecho sobre el nombre y seleccionar *"Advanced Settings..."* y buscar el bloque de opciones *"Process Model"*. El único parámetro a cambiar es el que dice *"Load User Profile"*, al cual habrá que asignar el valor **True**.

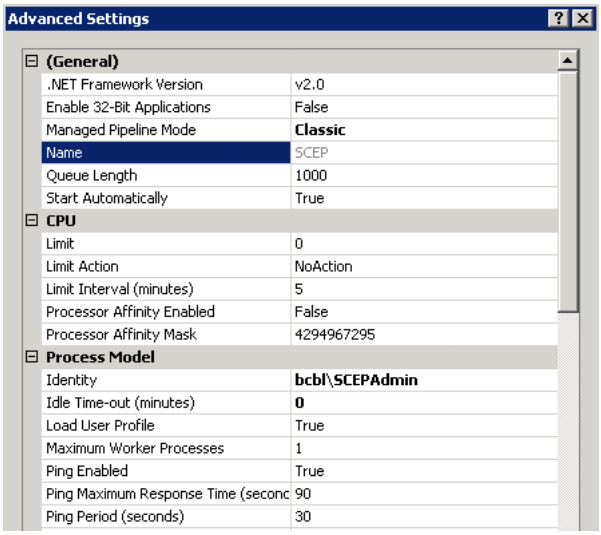


Figura C.10: Configuración de la *App Pool* **SCEP**

Una vez terminado de configurar el servidor web, se puede comprobar el funcionamiento del Directorio Activo accediendo a él mediante un navegdor. Para ello hay que introducir la siguiente url en la barra de navegación: `http://TFG03/certsrv/`

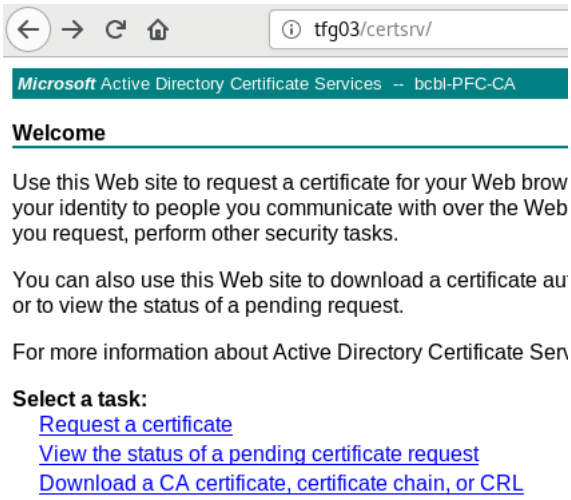


Figura C.11: Acceso vía web al servidor **TFG03**

Tal y como puede observarse en la imágen superior, la Autoridad Certificadora sigue siendo **bcbl-PFC-CA** (acc.bcbl.local en el dominio), lo que significa que seguirá siendo éste servidor el que emita los certificados, pero a través de TFG03 podrán enrolarse automáticamente diferentes tipos de dispositivos, entre ellos los PCs con Sistema Operativo Linux.

Además de esto, también puede hacerse la petición de un certificado directamente desde la web, o descargarse el certificado de la CA para instalarlo en el equipo y que el equipo confíe en los certificados emitidos por ella.

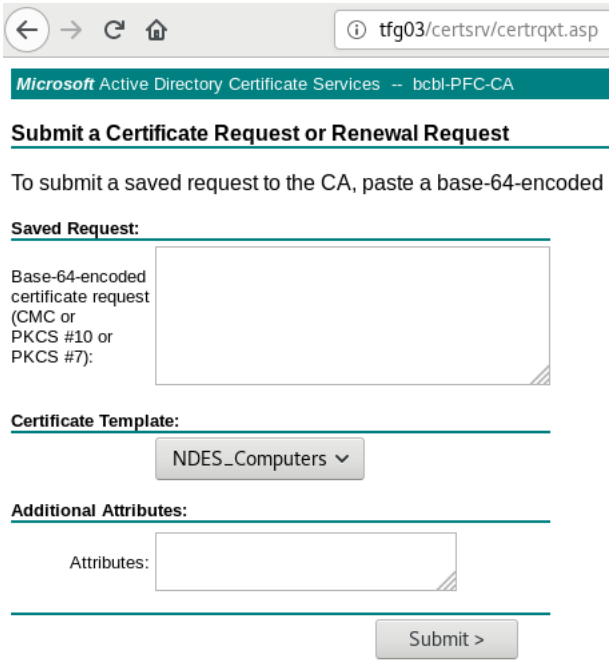


Figura C.12: Formulario de petición de un certificado **NDES_Computers** a la máquina **TFG03**

Con esto concluye la instalación y configuración del servidor *Microsoft Active Directory 2008 R2 Enterprise*, por lo que los equipos con Sistema Operativo Linux deberían de ser capaces de "autoenrrolarse". Para ello se utilizará el comando *sscep*, que se trata de la implementación de un cliente de SCEP que se utiliza mediante línea de comandos.

La única modificación a realizar en la parte del Directorio Activo para permitir el *auto-enrollment* se refiere al certificado en sí. Para ello hay que acceder a la CA y navegar hasta el directorio *Roles –>Active Directory Certificate Services –>Certificate Templates (acc.bcbl.local)*, buscar el nombre del certificado al que queremos otorgar permisos de *autoenrollment*, hacer click derecho sobre él y después hacer click sobre *"Properties"*. En la ventana de propiedades del certificado, navegar a la pestaña *"Security"* y en la lista superior seleccionar el usuario/máquina o grupo de usuarios/máquinas a los que queremos permitir "autoenrrolarse", en este caso *"Domain Computers"*.

En la parte inferior de la ventana se pueden establecer permisos sobre ese certificado para el grupo que haya sido seleccionado en la parte superior. Para conceder permisos de *autoenrollment* solo habrá que hacer click sobre el cuadro de la columna *"Allow"* y fila *"Autoenroll"* y dejarlo marcado con un *check*.

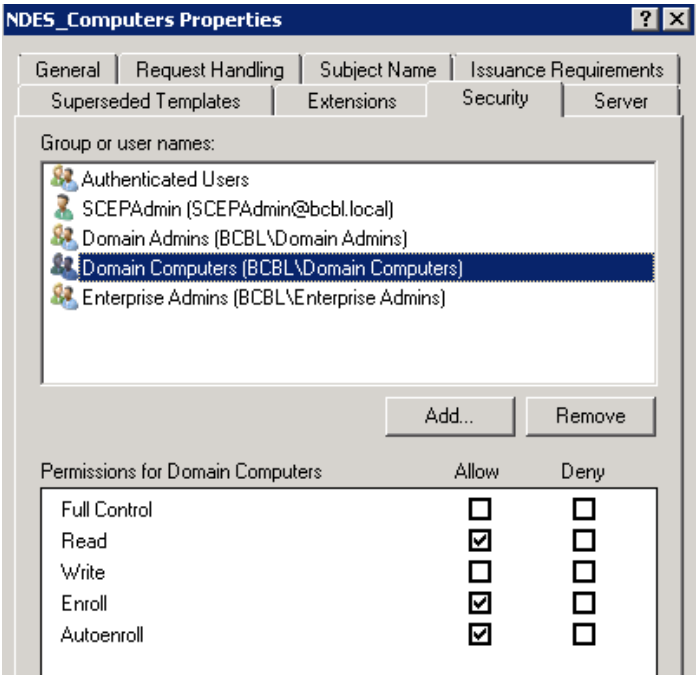


Figura C.13: Ventana de configuración de permisos sobre el certificado **NDES_Computers**

D. ANEXO

Creación de un perfil de configuración en macOS Server

Para crear un nuevo perfil en un servidor *macOS Server* hay que hacer click sobre el botón *"Profile Manager"* que aparece en la columna situada en la parte izquierda de la pantalla principal del servidor. Una vez aparezca la ventana de creación del perfil podrán observarse diversos apartados posibles de configurar para el mismo en la parte izquierda de la ventana. Para crear un perfil que consista en realizar una autenticación basada en certificados para una interfaz específica hay que configurar cuatro apartados:

1. **General:**

   En esta sección hay que añadir información acerca del perfil, así como el nombre, descripción o método de distribución.

2. **AD Certificate:**

   En este apartado hay una línea en la que dice *"Certificate Template"*. El nombre que se añada aquí tiene que coincidir con el nombre del certificado que se utilizará para la autenticación de la máquina, en este caso **NDES_Computers**.

3. **Certificates:**

   En esta sección será imprescindible incluir todos los certificados en los que será necesario confiar para que se pueda confiar en el certificado que generará el Directorio Activo. También habrá que añadir cualquier certificado que vaya a utilizarse en la negociación TLS entre el cliente y el servidor RADIUS.

4. **Network:**

   Aquí es donde se configuran las opciones acerca de los ajustes de red. Si estas configuraciones se han realizado en el orden indicado, en este último apartado debería aparecer cierta información añadida en los apartados anteriores una vez se haya seleccionado TLS como *"EAP type"*. Además de esto, también tendrán que aparecer listados los certificados que se añadieron en el paso número 3, junto a un recuadro que podrá checkearse o no, dependiendo si queremos confiar en ese certificado. Como último paso será necesario añadir el FQDN del servidor RADIUS, que en este caso será la máquina donde está funcionando PacketFence, **tfg01.bcbl.local**.

E. ANEXO

Código del script *Autoenrollment.sh*

```
#!/bin/bash
# Linux Certificate Enrollment Using NDES and SCEP
#####################################################################
# This script is provided as an example for illustration only,
# without warranty either expressed or implied, including, but not
# limited to, the implied warranties of merchantability and/or
# fitness for a particular purpose.
#####################################################################
#
# Insert the NDES Enrollment Password here.
# ndeskey=
# Insert the NDES server FQDN
ndesserver=tfg03.bcbl.local
# CA Filename
cafilename=tfg03
# Number of days ahead of cert expiration to renew
warning_days=45
#############################################################
#EDIT ONLY THE VALUES ABOVE
#############################################################
shopt -s -o nounset
```

```
# Create a log file directory
if [ ! -d /var/log/pki/ndes ]; then
    mkdir -p /var/log/pki/ndes/
fi
DTG=$(date +%Y%m%d%H%M)
LOGFILE=/var/log/pki/ndes/ndes-enrollment$DTG.log
if [ ! -f $LOGFILE ]; then
    touch $LOGFILE
fi
#####################################################################
# LOG FUNCTION TO WRITE LOCAL LOG FILE AND TO /VAR/LOG/MESSAGES
#####################################################################
writelog() {
    echo ${*} 2>&1 >> $LOGFILE
    if [ -f /bin/logger ]
    then
       logger ${*}
    fi
}
#####################################################################
writelog  "sscep: Checking for required packages"
if rpm -qa | grep epel-release  2>&1 > /dev/null;
        then
        writelog "sscep: epel-release is installed."
else
    yum -y install epel-release 2>&1 >> $LOGFILE
fi
if rpm -qa | grep sscep  2>&1 > /dev/null;
        then
        writelog "sscep: sscep is installed."
else
    yum -y install sscep 2>&1 >> $LOGFILE
fi
if rpm -qa | grep openssl  2>&1 > /dev/null;
```

```
        then
        writelog "sscep: openssl is installed."
else
    yum -y install openssl 2>&1 >> $LOGFILE
fi

MKREQUESTSCRIPT=/usr/bin/mkrequest
sed -i 's/KEYBITS=1024/KEYBITS=2048/g' $MKREQUESTSCRIPT
if ! grep -q "string_mask = nombstr" $MKREQUESTSCRIPT ; then
       sed -i '/\[ req \]/a string_mask = nombstr' $MKREQUESTSCRIPT
fi

if [ ! -f /etc/pki/tls/certs/$(hostname).crt ] ; then
        writelog "sscep: $(hostname) does not have an existing certificate. \
        Executing initial enrollment."
        writelog "sscep: Requesting CA certificate chain as x509 .crt files."
        sscep getca -F sha1 -c /etc/pki/ca-trust/source/anchors/\
        ${cafilename}CA.crt -u http://${ndesserver}/certsrv/mscep/mscep.dll/\
        pkiclient.exe? 2>&1 >> $LOGFILE
        writelog "sscep: Adding the CA chain to the host CA trusted chain."
        update-ca-trust enable 2>&1 >> $LOGFILE
        update-ca-trust extract 2>&1 >> $LOGFILE
        writelog "sscep: Generating CSR."
     mkrequest -dns $(hostname) 2>&1 >> $LOGFILE
        writelog "sscep: Moving CSR and new private key."
        mv local.key /etc/pki/tls/private/$(hostname).key
        mv local.csr /etc/pki/tls/private/$(hostname).csr
     openssl rsa -aes256 -in /etc/pki/tls/private/$(hostname).key\
     -out/etc/pki/tls/private/$(hostname).encrypted.key -passout pass:file:\
     /etc/pki/tls/private/.dirinfo/.p
        writelog "sscep: Executing enrollment using NDES key."
        sscep enroll -E 3des -S sha1 -c /etc/pki/ca-trust/source/anchors/\
        ${cafilename}CA.crt-0 -e /etc/pki/ca-trust/source/anchors/\
        ${cafilename}CA.crt-1 -k /etc/pki/tls/private/$(hostname).key -r
```

```
        /etc/pki/tls/private/$(hostname).csr -l /etc/pki/tls/private/\
        $(hostname).crt -u http://${ndesserver}/certsrv/mscep/mscep.dll/\
        pkiclient.exe? -d -v 2>&1 >> $LOGFILE
        writelog "sscep: Checking generated certificate status."
        CERTSTATUS=$(openssl verify /etc/pki/tls/private/$(hostname).crt\
        | cut -d: -f2)
        if [ $CERTSTATUS == "OK" ]; then
                writelog "sscep: Certificate status is: " $CERTSTATUS
                writelog "sscep: Copying new certificate to /etc/pki/tls/\
                certs/$(hostname).crt"
                cp /etc/pki/tls/private/$(hostname).crt /etc/pki/tls/certs/\
                $(hostname).crt 2>&1 >> $LOGFILE
        else
                writelog "sscep: The certificate is not valid per $CERTSTATUS"
        fi
else
        output=$(openssl x509 -in /etc/pki/tls/certs/$(hostname).crt -noout \
        -subject -dates 2>/dev/null)
        cert=$(echo $output | sed 's/.*CN=\(.*\).*not.*/\1/g')
        start_date=$(echo $output | sed 's/.*notBefore=\(.*\).*not.*/\1/g')
        end_date=$(echo $output | sed 's/.*notAfter=\(.*\)$/\1/g')
        start_epoch=$(date +%s -d "$start_date")
        end_epoch=$(date +%s -d "$end_date")
        epoch_now=$(date +%s)
        if [ "$start_epoch" -gt "$epoch_now" ]; then
                writelog "sscep: Certificate for [$cert] is not yet valid"
                writelog $output
        fi
        seconds_to_expire=$(($end_epoch - $epoch_now))
        days_to_expire=$(($seconds_to_expire / 86400))
writelog "existing certificate found"
        writelog "sscep: Days to expiry: ($days_to_expire)"
        warning_seconds=$((86400 * $warning_days))
        if [ "$seconds_to_expire" -lt 0 ]; then
```

```
            writelog "sscep: Certificate [$cert] has expired.  Remove the
            \certificate and rerun to start a new enrollment."
    else
    if [ "$seconds_to_expire" -lt "$warning_seconds" ]; then
        writelog "sscep: Certificate [$cert] is soon to expire \
        ($seconds_to_expire seconds)"
        writelog "sscep: Existing certificate found for $(hostname).\
        Executing re-enrollment."
        writelog "sscep: Backing up current private key."
        mv -f /etc/pki/tls/private/$(hostname).crt
        /etc/pki/tls/private/$(hostname).crt.bak
        mv -f /etc/pki/tls/private/$(hostname).key
        /etc/pki/tls/private/$(hostname).key.bak
        writelog "sscep: Generating CSR."
        mkrequest -dns $(hostname) 2>&1 >> $LOGFILE
        writelog "sscep: Moving CSR and new private key."
        mv -f local.key /etc/pki/tls/private/$(hostname).key
        mv -f local.csr /etc/pki/tls/private/$(hostname).csr
        writelog "sscep: Executing enrollment using existing \
        certificate."
        sscep enroll -E 3des -S sha1 -c /etc/pki/ca-trust/source/
        anchors/${cafilename}CA.crt-0 -e etc/pki/ca-trust/source/
        anchors/${cafilename}CA.crt-1 -k /etc/pki/tls/private/
        $(hostname).key -K /etc/pki/tls/private/\
        $(hostname).key.bak -O /etc/pki/tls/private/$(hostname).crt.bak
        /etc/pki/tls/private/$(hostname).csr -l /etc/pki/tls/private/\
        $(hostname).crt -u http://${ndesserver}/certsrv/mscep/mscep.dll/\
        pkiclient.exe? -d -v  2>&1 >> $LOGFILE
        writelog "sscep: Checking generated certificate status."
        CERTSTATUS=$(openssl verify /etc/pki/tls/private/$(hostname).crt\
        | cut -d: -f2)
           if [ $CERTSTATUS == "OK" ]; then
           writelog "sscep: Certificate status is: " $CERTSTATUS
           writelog "sscep: Copying new certificate to /etc/pki/tls/
```

```
                private/$(hostname).crt"
                cp -f /etc/pki/tls/private/$(hostname).crt /etc/pki/tls/
                certs/$(hostname).crt
                else
                writelog "sscep: The certificate is not valid per \
                $CERTSTATUS"
                writelog "sscep: Restoring the backup existing \
                certificate and keys."
                mv -f /etc/pki/tls/private/$(hostname).crt.bak
                /etc/pki/tls/private/$(hostname).crt
                mv -f /etc/pki/tls/private/$(hostname).key.bak
                /etc/pki/tls/private/$(hostname).key
                         fi
                 fi
        fi
fi
```

F. ANEXO

Registro de packetfence.log al lanzar un *Security Event*

```
INFO pfperl-api(32400): Force security event 3000006 for node 3c:d9:2b:a4:7c:80
even if 595 grace remaining (pf::security_event::security_event_add)
INFO pfperl-api(32400): security event 3000006 added for 3c:d9:2b:a4:7c:80
(pf::security_event::security_event_add)
INFO pfperl-api(32400): executing action 'role' on class 3000006
(pf::action::action_execute)
INFO pfperl-api(32400): executing action 'autoreg' on class 3000006
(pf::action::action_execute)
INFO pfperl-api(32400): security_event 1300003 force-closed for 3c:d9:2b:a4:7c:80
(pf::security_event::security_event_force_close)
INFO pfperl-api(32400): Instantiate profile default
(pf::Connection::ProfileFactory::_from_profile)
INFO pfperl-api(32400): re-evaluating access (manage_register called)
(pf::enforcement::reevaluate_access)
INFO pfperl-api(32400): is currentlog connected at (192.168.221.18)
ifIndex 13 registration (pf::enforcement::_should_we_reassign_vlan)
INFO pfperl-api(32400): Instantiate profile default
(pf::Connection::ProfileFactory::_from_profile)
INFO pfperl-api(32400): Connection type is Ethernet-NoEAP. Getting
role from node_info (pf::role::getRegisteredRole)
INFO pfperl-api(32400): Username was defined "3c:d9:2b:a4:7c:80" -
```

```
returning role 'Printers' (pf::role::getRegisteredRole)
INFO pfperl-api(32400): PID: "default", Status: reg Returned VLAN:
(undefined), Role: Printers (pf::role::fetchRoleForNode)
INFO pfperl-api(32400): VLAN reassignment required (current VLAN = 75 but should
be in VLAN 50) (pf::enforcement::_should_we_reassign_vlan)
INFO pfperl-api(32400): switch port is (192.168.221.18) ifIndex 13 connection
type: Wired MAC Auth (pf::enforcement::_vlan_reevaluation)
INFO pfperl-api(32400): this is a non-reevaluate-access security_event, closing
security_event entry now (pf::action::action_execute)
INFO pfperl-api(32400): security_event 3000006 force-closed for 3c:d9:2b:a4:7c:80
(pf::security_event::security_event_force_close)
INFO pfperl-api(28194): Instantiate profile default
(pf::Connection::ProfileFactory::_from_profile)
t=2019-06-20T13:24:29+0200 lvl=info msg="DHCPOFFER on 192.168.75.213 to
3c:d9:2b:a4:7c:80 (NPIA47C80)" pid=5676 mac=3c:d9:2b:a4:7c:80
t=2019-06-20T13:24:29+0200 lvl=info msg="DHCPREQUEST for 192.168.75.213 from
3c:d9:2b:a4:7c:80 (NPIA47C80)" pid=5676 mac=3c:d9:2b:a4:7c:80
t=2019-06-20T13:24:29+0200 lvl=info msg="DHCPACK on 192.168.75.213 to
3c:d9:2b:a4:7c:80 (NPIA47C80)" pid=5676 mac=3c:d9:2b:a4:7c:80
pfqueue(28745) WARN: [mac:3c:d9:2b:a4:7c:80] Unable to match MAC address to IP
'192.168.75.213' (pf::ip4log::ip2mac)
pfqueue(2904) WARN: [mac:3c:d9:2b:a4:7c:80] Until CoA is implemented we will bounce
the port on VLAN re-assignment traps for MAC-Auth
(pf::Switch::handleReAssignVlanTrapForWiredMacAuth)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] handling radius autz request:
from switch_ip => (192.168.221.18), connection_type =>
Ethernet-NoEAP,switch_mac => (00:23:47:c8:63:73), mac =>
[3c:d9:2b:a4:7c:80], port => 13, username => "3c:d9:2b:a4:7c:80"
(pf::radius::authorize)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] Instantiate profile default
(pf::Connection::ProfileFactory::_from_profile)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] Connection type is Ethernet-NoEAP.
Getting role from node_info (pf::role::getRegisteredRole)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] Username was defined
```

```
"3c:d9:2b:a4:7c:80" - returning role 'Printers' (pf::role::getRegisteredRole)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] PID: "default", Status:
reg Returned VLAN: (undefined), Role: Printers (pf::role::fetchRoleForNode)
httpd.aaa(5789) INFO: [mac:3c:d9:2b:a4:7c:80] (192.168.221.18) Added VLAN 50 to
the returned RADIUS Access-Accept (pf::Switch::returnRadiusAccessAccept)
```