Universidad de Valladolid

ESCUELA DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA
MENCIÓN EN INGENIERÍA DE SOFTWARE

Estudio, diseño e implantación de un cortafuegos UTM libre para pequeñas organizaciones

Alumno: Patricia Sanz Marcos

Universidad de Valladolid

ESCUELA DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA
MENCIÓN EN INGENIERÍA DE SOFTWARE

Estudio, diseño e implantación de un cortafuegos UTM libre para pequeñas organizaciones

Alumno: Patricia Sanz Marcos
Tutor: Jesús M. Vegas Hernández

A todos con los que he compartido esta etapa, pero en especial a Fran y a David.

Agradecimientos

En primer lugar, a ISEND por haberme ofrecido esta oportunidad y por las facilidades aportadas, y a mi tutor Jesús M. por toda la ayuda y consejos que me ha dado durante esta etapa.

En segundo lugar, a mi familia, que me ha estado apoyando durante todo momento, en especial a mi hermano.

También me gustaría expresar a mi agradecimiento a mi pareja, Fran, y mis amigos que no ha dejado que me desmotive en ningún momento.

A todos ellos, mil gracias.

Resumen

Este documento describe el proceso de análisis e implantación de seguridad en una infraestructura real, en la cual, después del router de entrada, todo el tráfico es gestionado a través de un firewall. Este documento se centrará en las carencias de la infraestructura, siendo la mayor de estas un firewall propiamente configurado y actualizado. Se realizará un estudio con el objeto de aportar una solución de bajo coste al problema. Para ello se estudiarán diferentes firewalls open source y gratuitos que hay en el mercado, y se instalará y realizará la configuración adecuada para disponer de todos los servicios necesarios de una red, donde los usuarios puedan trabajar de forma cómoda, segura, y controlada.

Abstract

This document describes the process of auditing and implementing cybersecurity for a real infrastructure. Infrastructure in which, after an entry router, all traffic is managed through a firewall. Putting the focus on infrastructure deficiencies, the largest of them being a properly configured and updated firewall. Venturing to the study of low cost solutions to solve this problem. To do this, a study about comparing different free and open source firewalls on the market will be made. Afterwards, one of them will be installed and configured with all the necessary services to create a network where users can work in a comfortable, safe, and controlled manner.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1. Contexto

Hoy en día la ciberseguridad es muy importante, especialmente en estos tiempos en los que trabajar en remoto puede ser vital. Actualmente, los ciberataques crecen a un ritmo vertiginoso. En 2017 se registraron más de 120.000 incidentes, según los datos recogidos por el INCIBE, siendo siete de cada diez ciberataques registrados en España contra PYMES[1]. Estos ataques son cada vez más numerosos y sofisticados. Pueden tener como consecuencias desde saltarse las primeras líneas de defensa de la red, hasta dejar sistemas inoperativos. Debido a esto hoy en día aplicar ciberseguridad a las empresas es esencial. Para ello uno de los puntos clave es disponer de un firewall resiliente que permita gestionar los movimientos dentro la red de la infraestructura. En este proyecto se dará una solución eficiente y de bajo coste a estas necesidades, de tal forma que asumir los costes de su implementación no supongo un gran reto para la entidad que instale el sistema.

Este proyecto se realiza en el contexto de los estudios de Ingeniería Informática, concretamente como Trabajo de Fin de Grado. Como cualquier proyecto, se deben seguir una serie de fases para llegar a obtener el producto deseado. Primero se deberá realizar una parte de planificación y análisis del proyecto. Después, se desarrollará la fase de diseño e integración, y, por último, la fase de análisis de los resultados. Cada una de estas fases con su correspondiente seguimiento.

En este documento, bajo la sección Estructura de la Memoria, se detalla la estructura del mismo de forma detallada.

1.2. Motivación

El motivo del desarrollo de este proyecto es la implantación de un sistema de bajo coste que mejore la seguridad de la infraestructura de red en una pequeña empresa. La infraestructura de la empresa consta de un de router de frontera que redirige todo el tráfico de la red a un firewall, dicho firewall, en concreto el sistema IMTv2[2], desarrollado por la empresa IMTCLOUD[3], tiene una antigüedad superior a 10 años y se le considera obsoleto. Se pretende sustituir el sistema firewall actual de la empresa por otro que cubra las necesidades que han emergido a lo largo de estos años. Todo ello sin que ello sin que esto suponga un gran desembolso para la entidad.

1.3. Objetivos

El principal objetivo de este TFG es la implantación de un firewall UTM open source en la infraestructura de red de una empresa, con el fin de mejorar la seguridad y servicios prestados. Para ello se deberán realizar las siguientes tareas:

- Analizar el paradigma actual de ciberseguridad en la industria. Se realizará un estudio que permita comprender las necesidades básicas en ciberseguridad para PYMEs en los tiempos actuales para que, una vez contextualizada la situación, se pueda implantar la mejor opción.
- Analizar la estructura actual de la red. Para saber qué requisitos debe cumplir el firewall a implantar, y si verdaderamente es necesario sustituir el equipo actual, se deberá conocer la red a gestionar: qué equipos la conforman, cuál es su disposición, qué servicios se han de prestar, cuáles son las necesidades de estos, y cuántas de estas necesidades cubre el firewall actual.
- Realizar un estudio de las capacidades de diferentes alternativas que provee la comunidad open source por las que se podría sustituir el firewall actual, siempre y cuando esto cubra las necesidades de la entidad en cuanto a seguridad y servicios, para aportar así mejoras a la infraestructura actual. Para ello se analizarán teóricamente varios de las soluciones más populares a fecha de hoy, y se decidirá cuál de ellas cubre mejor las necesidades de la entidad. Sabemos que los requisitos impuestos previamente por la entidad son:
  - Redireccionar el tráfico de los servicios de la entidad.
  - Gestionar el acceso a los diferentes recursos por parte de los usuarios.
  - Acceso y denegación de acceso a los diferentes recursos.
  - Gestionar el ancho de banda para un uso óptimo de los recursos.
  - Proveer acceso seguro desde el exterior mediante VPN (teletrabajo).
- Puesta a prueba e integración de la solución elegida. Una vez elegido el firewall que gestionará la red empresarial, se testearán las capacidades de este en un entorno de

pruebas, con el objeto de comprender, gestionar y analizar dicho firewall para así, cuando se implante en la red empresarial se conozca la configuración más idónea de este. Se puede dividir esto en las siguientes subtareas:

  - Elección y configuración del hardware.
  - Instalación del sistema.
  - Análisis, instalación y configuración de los diferentes paquetes (funcionalidades)
  - Configuración del sistema.
  - Pruebas de los servicios implantados.

- Integración del sistema en el entorno real. El proceso será similar al punto anterior pero con las restricciones que supone trabajar en un entorno no de pruebas.
- Para concluir el proyecto, a partir de los resultados obtenidos de la integración del sistema, se realizará la prospectiva de las capacidades y posibles ampliaciones futuras.

1.4. Alcance

El producto final de este proyecto constará de la integración de un sistema que realizará las siguientes tareas:

- Gestionar qué tipo de trafico se permite o bloquea en función del puerto, dirección de origen y dirección de destino. Los usuarios de la red local dispondrán de acceso a los servicios de la empresa.
- Acceso seguro mediante VPN: Ciertos empleados dispondrán de acceso a la red de área local a través de una conexión externa mediante VPN.
- Establecer el ancho de banda máximo para el acceso a internet en función al usuario para proveer un acceso equitativo y dimensionado a la capacidad de la red.
- Filtrado de contenido web: Restringir el acceso a redes sociales y contenido ilícito en la red.
- Filtrado de contenido en función de la aplicación: monitorizar el tráfico desde LAN en función de la aplicación utilizada por el usuario.

Además de la implantación de este sistema, se realizará un manual de usuario que permita al administrador de la red reconfigurar los parámetros con facilidad.

1.5. Estructura de la Memoria

El contenido de la memoria se organiza de la siguiente forma:

Capítulo 1: Introducción. En este capítulo se presenta el proyecto. Se ofrece una visión general sobre el proyecto realizado, incluyendo el contexto, los objetivos, alcance del proyecto, estructura de la memoria y contenido de la memoria.

Capítulo 2: Estado del arte. En este capítulo se realiza el análisis del paradigma actual en ciberseguridad con respecto a las pymes. También se introduce el contexto teórico de las tecnologías principales usadas en este proyecto.

Capítulo 3: Plan de Proyecto. En este capítulo se incluye el documento de planificación del proyecto. Se describen las tareas a realizar, la metodología utilizada en el proceso de desarrollo, la gestión de tiempo, riesgos y el presupuesto.

Capítulo 4: Análisis de la infraestructura y elicitación de requisitos. En este capítulo se realiza el análisis de infraestructura. Incluye la elicitación de requisitos, definición de roles, especificación de casos de uso, y diagramas físico-lógicos de la infraestructura.

Capítulo 5: Diseño de la solución. En este capítulo se estudian y comparan diferentes los firewalls de código abierto frente a las necesidades de la entidad, se elige la solución a implementar y se desarrollan los casos de uso.

Capítulo 6: Implantación en entorno de pruebas. En este capítulo se construye una maqueta de red, se describen los detalles la configuración y pruebas realizadas de los diferentes módulos del sistema, junto con sus resultados, para comprobar que el sistema funciona correctamente.

Capítulo 7: Integración, Pruebas y Evaluación. Se incluye la descripción de las fases de integración, los test realizados y una evaluación comparativa del sistema.

Capítulo 8: Conclusiones y Trabajo Futuro. Se incluye una descripción con los resultados obtenidos, una valoración personal y posibles líneas de trabajo futuras.

Capítulo 9: Bibliografía. Contiene las referencias bibliográficas consultadas a lo largo del desarrollo del proyecto.

Anexos. En esta sección se encuentra una descripción de los archivos adjuntados junto con este documento.

Capítulo 2

Estado del arte

2.1. Introducción

Hoy en día, los sistemas de información con base tecnológica están presentes en todos los procesos de cualquier empres. Las empresas han de adaptarse a cambios tecnológicos continuos rápidamente, así como enfrentarse a ciberataques cada vez más sofisticados y frecuentes a los que se ven sometidas. Por estos motivos la ciberseguridad se ha convertido en un punto esencial para proteger los activos de una empresa.

Para abordar la seguridad se debe tener una visión integral del entorno, interno y externo, teniendo en cuenta no solo aspectos técnicos si no también físicos, organizativos y legales. Esta perspectiva panorámica se plasmará en un Plan Director de Seguridad que facilitará la gestión global de los proyectos e iniciativas tomadas en la empresa con respecto a seguridad de la información [4]

En este capítulo se dará una visión global del protocolo llevado a cabo a la hora de implantar medidas de ciberseguridad en una empresa, haciendo incapié en aspectos a tener para el análisis de riesgos y posibles soluciones a implantar con respecto seguridad perimetral, ya que ese es el alcance del proyecto.

2.2. Plan Director de Seguridad

El Plan Director de Seguridad consiste en la definición y priorización de un conjunto de proyectos que tienen como objetivo reducir los riesgos relacionados con los sistemas de información a los que está sometida la empresa[5]. Básicamente en un Plan Director de seguridad se analiza la situación actual de la empresa y se definen mediadas a aplicar por prioridad para cubrir los riesgos.

El Plan Director de Seguridad consta de 6 fases que se repetirán ciclicamente hasta disponer de una versión final satisfactoria del plan. Las fases son:

1. **Análisis de la situación actual de la empresa**: Se ha de conocer cuál es la situación actual de la empresa. En esta fase se define el alcance del plan, por ejemplo en el caso de este proyecto sería el departamento TIC, concretamente el sistema de seguridad perimetral para la intranet. Tras fijar el alcance se hace un análisis en el que se evaluarán aspectos normativos con respecto al marco legal, regulatorios con respecto a estándares de ciberseguridad, una inspección de instalaciones y un análisis de riesgos.

2. **Análisis de la estrategia de la organización**: Se han de conocer los planes de desarrollo de la empresa para poder alinear la estrategia de seguridad tanto con la estrategia TIC como con la general de negocio.

3. **Definición de proyectos e iniciativas**: Una vez obtenido un análisis de riesgos y alineadas las estrategias se definen y ponen en marcha iniciativas para cubrir las debilidades detectadas en la fase 1.

4. **Clasificación y priorización de los proyectos a realizar**: Tras obtener todas las medidas y proyectos a desarrollar se deben clasificar y priorizar en función del riesgo y el coste de desarrollo.

5. **Aprobacion por la dirección**: Completas las fases 1-4 ya se dispone de una versión preliminar del Plan Director de Seguridad que deberá ser revisado y aprobado por la Dirección.

6. **Implantación**: Una vez aprobado el plan se ponen en marcha los proyectos e iniciativas estipulados.

Figura 2.1: Fases de un Plan Director de Seguridad

2.3. Estándares en ciberseguridad

Los estándares en ciberseguridad son una colección de conceptos, políticas, guías y colecciones de herramientas que tienen como objeto la protección de una organización y sus activos. Se usan como referencia a la hora de realizar el Plan Director de Seguridad, especialmente para el análisis de la Fase 1 y para el análisis de riesgos. En esta sección se definiran los estándares más utilizados.

2.3.1. Familia ISO/IEC 27000

Los familia de estándares ISO/IEC 27000 esta dedicada a la gestión de la seguridad de la información. Contiene las mejores prácticas recomendadas sobre cómo desarrollar, impementar y mantener las especificaciones para los sistemas de gestión de la seguridad de la infomarción. Son los estándares de referencia internacional y la base de otros estándares como del ENS o NIST. Cada estándar de esta familia está diseñado para poner el foco en un punto determinado. Dentro de los estánderes más reconocidos estan:

- ISO/IEC 27001: Define las bases de la seguridad de la información dentro de la empresa. Proporciona un modelo y orientación detallada para la implmentación de un sistema que permita la reducción de la exposición de la información a riesgos.[6]
- ISO/IEC 27002: Define en detalle los controles del ISO 27001 para llevar a cabo su correcta implementación.
- ISO/IEC 27005: Es un código de mejores prácticas para desarrollar una metodología de gestión de riesgos. En el se definen y categorizan los riesgos para su posterior evaluación y tratamiento.

2.4. Marco legal

A la hora de establecer un plan de seguridad dentro de la empresa se han de conocer y acatar las leyes actualmente vigentes tanto para país en el que esta establecida la empresa como para el que ofrece servicios y productos. España cuenta con un código de Derecho de Ciberseguridad[7] que facilita esta tarea. Se trata de una recompilación actualizada de toda legislación española relacionada con la seguridad de la información y la ciberseguridad en general.

En esta sección hablaremos de algunas de las leyes más importantes a tener en cuenta a la hora de implantar soluciones de ciberseguridad en una pequeña empresa del sector privado.

En la Figura 2.2 podemos observar la evolución de las leyes con respecto a la materia en ciberseguridad para pymes. En función del sector de negocio al que pertenezca la empresa a

tratar se han de cumplir ciertos aspectos regulatorios, pero toda empresa española ha cumplir con la LOPDGDD y la LPI.

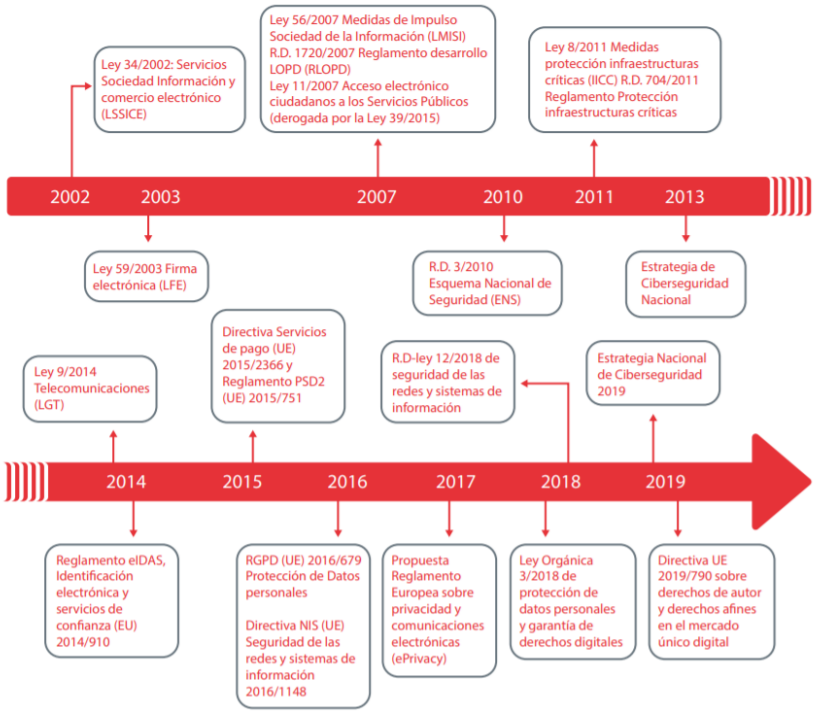


Figura 2.2: Desarrollo legal de ciberseguridad en pymes. España.[8]

LOPDGDD que adapta al contexto español el **RGPD** de la UE que entró en vigor el 25/05/2018. Son las normas que regulan el tratamiento de los datos sensibles pertenecientes a personas físicas. Toda empresa con ámbito de actuación en la UE ha de acatar el RPGD. Es importante tenerlo en cuenta para la seguridad perimetral de la empresa, puesto que este reglamento dictamina que la empresa ha de proteger proactívamente la confidencialidad de los datos de los usuarios. Los principios en los que se basa este reglamento son:

1. Licitud, lealtad y trasparencia: Los datos personales han de ser adquiridos de forma lícita. El interesado debe ser informado de los datos que cede, para qué se van a usar y cuánto tiempo se verán recogidos dentro del organismo de forma que se pueda identificar.

2. Limitación de la finalidad: La finalidad para la que se recogen los datos personales ha de ser desarrollada e informada de forma clara y concisa al interesado. También implica la prohibición de que estos datos sean tratados posteriormente de forma incompatible a estos fines.

3. Minimización de datos: Los datos recogidos deben ser adecuados y limitados a lo necesario en relación al fin con el que se recogen.

4. Exactitud de datos: Los datos han de ser correctos, completos y actualizados. El interesado tiene derecho a reactificar el tratamiento de sus datos.
5. Limitación del plazo de conservación de datos: Se limita el tiempo de conservación de los datos al logro del fin que persigue su tratamiento.
6. Integridad y confidencialidad: Se impone a la entidad que trata los datos a actuar proactivamente en cuanto a la protección de los datos que tratan ante cualquier riesgo que pueda violar la confidencialidad e integridad de estos. En caso de la violación de este principio el tratador tendra 72 horas para informar a las autoridades.

LPI (Ley de Protección Intelectual): Con el objeto de proteger la propiedad intelectual se establece un marco por el cual se puede registrar obras por parte de empresas o personas físicas. Una vez registradas se perseguirá y castigará su uso ilícito. Esta ley también es importante para la realización de este TFG, puesto que se deberán tomar medidas para evitar su incumplimento en la intranet empresarial, como puede ser la monitorización del tráfico y restricción de acceso a webs de descargas.

Ley 34/2002: Regula los aspectos jurídicos de las actividades como el comercio electrónico, la contratación en línea, la inforación y los servicios de intermediación. Se aplica para empresas que realizan comunicaciones comerciales a través de la red y refleja los datos a mostrar obligaoriamente en la web de la empresa que realiza esas actividades comerciales.

Ley 8/2011[9]: Dentro del marco normativo asoaciado la la ciberseguridad en empresas tiene especial importancia la Ley de Protección de Intraestructuras Críticas que es complementado por el Real Decreto 704/2011[10]. Esta ley la han de acatar todos los organismos considerados críticos para el país que se definen en ella misma y se basa en el plan clásico de auditar, reducir las ciberamenazas y crear planes de contingencia que toda empresa debería seguir para su correcto funcionamiento. Los objetivos de esta norma se pueden resumir en:

- Catalogar el conjunto de infraestructuras que presentan servicios esenciales, como pueden ser salud, TIC, transporte o alimentación entre otras.
- Diseñar un planteamento de medidas de prevención y protección contra las posibles amenazas a las que se enfrentan estas infraestructuras. Este planteamento se dividide en dos:
  - PSO: define una política general del operado. Aquí se define la metodología de analisis de riesgo y los criterios de aplicación de medidas de ciberseguridad entre otros.
  - PPE: define los Planes de Protección Específicos, es decir, las medidas concretas a aplicar para garantizar la seguridad lógica y física.

2.5. Riesgos

Para saber a que riesgos se exponen los activos de una empresa se deben conocer las amenazas a las que esta expuesta. Las amenazas se basan en las vulnerabilidades de la

infraestructura para atentar contra el sistema. Si existe una vulnerabilidad en el sistema, siempre existirá alguien que intentará explotarla, y por lo tanto un riesgo de que esta sea explotada. Para conocer más sobre vulnerabilidades vaya a la sección 4.6.4.

Figura 2.3: Relación entre amenaza, vulnerabilidad y riesgo dentro de un sistema[11]

Dentro del contexto de la ciberseguridad se define como activo la información contenida en el entorno empresarial. Las propiedades principales a proteger son:

- Confidencialidad: La información solo debe ser accesible únicamente a las personas autorizadas.
- Integridad: La información solo debe modificarse tras su autorización.
- Disponibilidad: La información debe ser siempre accesible para las personas autorizadas a ella.

Hay muchos tipos de amenzas pero generalmennte se clasifican del siguiente modo[12]:

- Dependiendo del lugar donde está situado el agente atacante:
  - Interna: Procede del interior del sistema atacado. Por ejemplo un empleado que utiliza su puesto de trabajo para llevar realizar el ataque.
  - Externa: Procede del exterior del sistema atacado. Por ejemplo una inundación.
- Dependiendo de la vía de ataque:
  - Física o ambiental: Afectan al hardware o a las instalacionesen donde se ubica este. Por ejemplo un fuego o un robo.
  - Lógica: Afectan al software del sistema.

2.5.1. Ataques al sistema

El mecanismo por el cual un agente de amenazas explota las vulnerabilidades del sistema es el ataque. En esta sección se van a clasificar los ataques lógicos deliberados.

Un ataque informático a un sistema normalmente se compone de varios pasos ordenados[12]:

1. Descubrimiento de los sistemas que componen la red en la que se haya el objetivo.
2. Exploración de las vulnerabilidades de los sistemas de la red.
3. Explotación de las vulnerabilidades detectadas.
4. Compromiso del sistema.
5. Ocultamiento o eliminación de los rastros que prueban el ataque.

Cuando el atacante lleva a cabo estos pasos usa varias técnicas de ataque. Los más conocidas y comunes en la actualidad según INCIBE[13] son:

- **Ataques a las contraseñas**: Ataque a las credeciales de acceso al sistema mediante técnicas como fuerza bruta o diccionario.
- **Ataques por ingeniería social**: El atacante usa técnicas psicológicas de manipulación dirigidas al usuario con el objetivo de que este realice una acción que beneficie al propio atacante. Los ataques más comunes de este tipo son los tipo phising, usando como medio aplicaciones de mensajería, pero puede usar otros medios como llamadas telefónicas o sms.
- **Ataques a conexiones**: El atacante intercepta transición de información entre dos partes, generalmente usuario y servidor, con el objetivo de monitorizar y extraer datos sensibles del usuario. Entre los ataques a conexiones destacan:
  - **Redes trampa**: Suele darse en sitios con redes wifi públicas. El atacante crea una red wifi con las mismas o similares características externas de la red pública. Tiene como objetivo el robo de información sensible de los usuarios.
  - **Spoofing**: El atacante suplanta la identidad de entidades o personas en la red. Dentro de este tipo de ataques los más comunes son suplantación de IP, falsificación web, suplantación de email y suplantación de DNS.
  - **Ataque a las cookies**: El atacante captura peticiones HTTP con la intención de robar y/o modificar el contenido de las cookies ya que este puede traer información sensible de la víctima, como credenciales.
  - **DDos**: El atacante realiza una cantidad de peticiones masiva al servidor desde varios dispotivos pudiendo llegar a dejarlo inoperativo.
  - **Inyección SQL**: ataque a una aplicación web que compromete su base de datos mediante sentencias SQL maliciosas.
  - **Escaneo de puertos**: se analizan los puertos de una maquina para ver qué puertos estan abiertos, cerrados, protocolos de seguridad aplicados. Todo ello para encontrar vulnerabilidades a explotar en el sistema.
  - **Man in The Middle**: El atacante intercepta la comunicación entre dos partes que, insertándose en el medio, bien capturando la información del intercambio o impersonando una de las partes. Tiene como objetivo el robo de información sensible.

  - **Sniffing**: El atacante interfiere el tráfico de la red através de programas de captura de paquetes. Tiene como objetivo el robo de información sensible.

- **Ataques por malware**: Introducción en el sistema de software que está diseñado específicamente para interrumpir, dañar u obtener acceso no autorizado a un sistema informático. Existen muchos tipos de malware como el Ram

  - **Virus**: software malicioso que usa como modo de transmisión otro archivo o programa y una vez en el host, si es ejecutado por el usuario se atureplicará y causará daños dentro del equipo.
  - **Adware**: malware que muestra anuncios a la víctima con el objetivo de generar ingresos al atacante. Normalmente se instala camuflado junto a programas descargados de repositorios no oficiales.
  - **Troyano**: Se camuflan como sotfware legitimo para infectar el software de la victima con diversos objetivos como crear puertas traseras, robar información sensible o monitorizar los movimientos del equipo infectado.
  - **Gusano**: Variante de virus que se autoreplica e infecta a otros equipos con capacidad de realizar cambios en la configuración del sistema.
  - **Criptojacking**: El atacante usa los recursos del dispositivo de la víctima para minar criptomonedas.

2.5.2. Ciberamenazas dentro del entorno empresarial

En la sección anterior se han listado los ciberataques más comunes, pero como el entorno del estudio es una PYME es importante clasificar las amenazas y ataques de los son presa las PYMEs con más frecuencia. A continuación se listan las ciberamenazas más comunes dentro de un entorno empresarial, y por lo tanto las que debe conocer en mayor profundidad según el INCIBE[14]:

- **Fugas de información**: Se produce cuando infomación relativa a la empresa es puesta en poder de una persona no autorizada rompiendo así la confidencialidad de dicha información. Las formas más comunes de perdida de la confidencialidad dentro de una organización son:

  - **Extracción de dispositivos físicos** con información sensible en su interior, bien por robo o por extravío.
  - **Uso del correo electrónico**. Ya sea de forma involuntaría o a raíz de ataques basados en ingeniría social.
  - **Uso de redes inalámbricas no confiables** o con medidas de seguridad insuficientes.
  - **Uso de inadecuado de redes sociales**, como la publicación de datos sensibles relativos a la empresa en ellas.
  - **Uso inadecuado de las herramientas empresariales**, como dar acceso a un sistema externo a la nube de la empresa.

  - **Malware** como troyanos, adware o spyware.
  - **Uso de credenciales inseguras**, poco robustas o de defecto.

- **Ataques tipo phishing**:Usa la ingeniería social para manipular psicológicamente al propio usuario del sistema con el objetivo de que este realice una acción que beneficie al atacante. Su principal mendio de propagación es el correo electrónico.

- **Fraude del CEO**: Con el objetivo de robar fondos de la empresa, el atacante se hace pasar por un alto directivo de la empresa. Tras recompilar información de la persona a suplantar la identidad, el atacante trata de, usualmente mediante intercambio de emails, convencer a un empleado con capacidad de realizar transferencias financieras de que le haga urgentemente una trasferencia de dinero de los fondos de la empresa a otra cuenta bajo el control del atacante.

- **Fraude de RR.HH.**: Parecido al fruade del CEO. Se suplanta la identidad de un empleado cualquiera y se trata de convencer a un empleado de RR.HH., usualmente por intercambio de emails, de que la nómina del empleado se ingrese a una nueva cuenta que estará bajo control del atacante.

- **Suplantación de proveedores**: Parecido al fruade del CEO. Se suplanta la identidad de un proveedor y se trata de convencer a un empleado, usualmente realizando eail spoofing, de que realice una transferencia bancaria a una cuenta que estará bajo control del atacante.

- **Sextorsión**: La victima recibe un email en el que se le extorsiona para realizar un pago amenazandola con revelar contenido visual comprometido de esta a sus conocidos y por las redes sociales bajo la premisa de haber hackeado sus dispositivos.

- **Ataques contra la página web corporativa**. Estos ataques en general están basados en el aprovechamiento de vulnerabilidades del sistema como software no parcheado, malas configuraciones o errores de diseño en la web. Este tipo de ataques se puede clasificar en:

  - **Fuga de información**: El atacante extrae información confidencial de la empresa.
  - **DoS y DDoS**: El atacante realiza una cantidad de peticiones masiva al servidor de tal manera que lo deja inoperativo.
  - **Defacement**: El atacante cambia la apariencia de la web corporativa, pudiendo usarla como trampolín para tralizar otro tipo de fraudes como phishing o distribución de malware.

- **Ransomware**: Por medio de malware se restringe el acceso a la información de los dispositivos afectados, generalmente cifrándola. El atacante generalmente pide un rescate económico a cambio de la recuperación de su acceso.

- **Fraude de falso soporte de Microsoft**: La victima se comunica telefonicamente con el estafador, que se hace pasar por tecnico de Microsoft y, pretendiendo solucionar varios problemas, roba información a la victima, instala software de acceso remoto o solicita dinero a cambio de solucionar problemas inexistentes.

- **Campañas de emails con malware**: Envio de email que instan a la victima a descargar y ejecutar programas que comprometerán su sistema camuflandolos como otro tipo de archivos adjuntos con los que la víctima está familiarizada, por ejemplo un excel, o como un enlace de descarga de dicho archivo.

2.5.3. Análisis de riesgos

En el análisis de riesgos se detecta y calcula la probabilidad y coste de que se materialicen ciertas amenazas. En función a estos parámetros y del marco legal, se decide si el riesgo se debe evitar, mitigar, trasferir su gestión a terceros o coexistir con él. Las pautas a seguir para realizar el análisis se reflejan en la Figura 2.4

Figura 2.4: Fases del análisis de riesgos[11]

2.6. Medidas de Defensa

En esta sección se va a hablar de las medidas que se pueden aportar para la mitigación de los riesgos posibles encontrandros tras en análisis del entorno empresarial. Se profundizará en la seguridad perimetral y los sistemas UTM ya que el objetivo de este proyecto es la implantación de uno de estos sistemas.

Para una defensa completa se debe aplicar defensa en profundidad. La defensa en profundidad consiste en la introducción de múltiples capas de seguridad que reducen la probabilidad de compromiso introduciendo medidas varias de seguridad a todos los niveles (seguridad perimetral, seguridad interna y factor humano)[12]. En la Figura 2.5 se observan las posibles capas de seguridad.

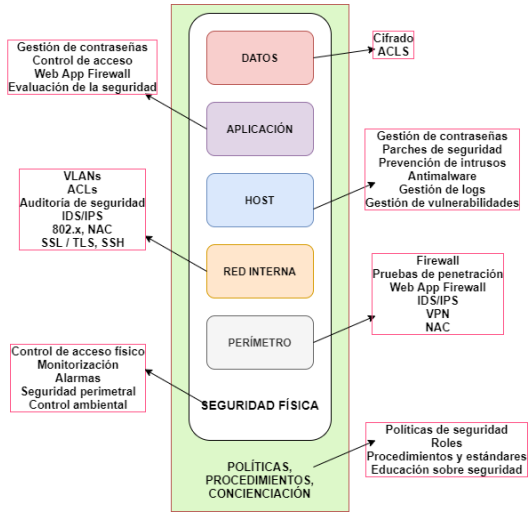


Figura 2.5: Niveles de defensa en profundidad[11]

La medidas para aplicar seguridad en la red interna se pueden resumir en: cortafuegos personales, actualizaciones del sistema y aplicaciones, antivirus y gestión de la configuración del sistema.

Las medidas para acotar los riesgos humanos se basan en políticas de seguridad corporativas, gestión de incidencias y concienciación de los usuarios.

Las medidas a tomar para aplicar seguridad perimetral son: filtrado de tráfico mediante cortafuegos, sistema de detección de intrusos que monitorice el tráfico de la red, controles de acceso a la red, defensa contra malware y cifrado de datos.

2.6.1. Seguridad perimetral

En una red se describe el perimetro como el conjunto de sistemas que ofrecen servicios a una red externa. El hecho de estar abiertos hacia el exterior aumenta la probabilidad de exposición de vulnerabilidades que podrían ser explotadas.

Las funciones que debe cumplir una red perimetral son:

- Rechazar las conexiones de clientes externos a servicios que sólo deban ser accedido desde la red interna.
- Distinguir y establecer políticas de tratamiento para los diferentes tipos de tráfico en función a su red de procedencia.
- Seleccionar el tráfico procedente o dirigido hacia determinados nodos de la red con el objeto de impedir el tráfico que no provenga de donde debería provenir.

- Proporcionar un punto único de conexión con el exterior. Este punto debe ser controlable.
- Redireccionar el tráfico de entrada permitido hacia los sistemas alojados en la red interna o perimetral y rechazarlo cuando el tráfico no cumpla con las políticas de seguridad establecidas.
- Ocultar los servicios vulnerables a la red externa.
- Ocultar información referente a las características de la red interna.

Para la aplicación de estas medidas se pueden usar varios dispositivos como pueden ser un sistema firewall, sistema IDS/IPS, servidor VPN, servidores proxy... o un sistema UTM que centralice estos servicios.

2.7. Firewall UTM

Un sistema UTM integra en un único dispositivo un conjunto de soluciones de seguridad perimetral. Esto permite un gran ahorro económico y simplificación de la red frente a la incorporación de estos servicios mediante varios dispositivos. Una UTM se puede definir como un cortafuegos a nivel de aplicación al se le incoporan otros servicios, llamados areas de gestión. Algunos ejemplos de areas de gestión son: servidor VPN, gestión de antivirus, antispam, filtrado de contenidos y Deteccion/Prevención de intrusos.

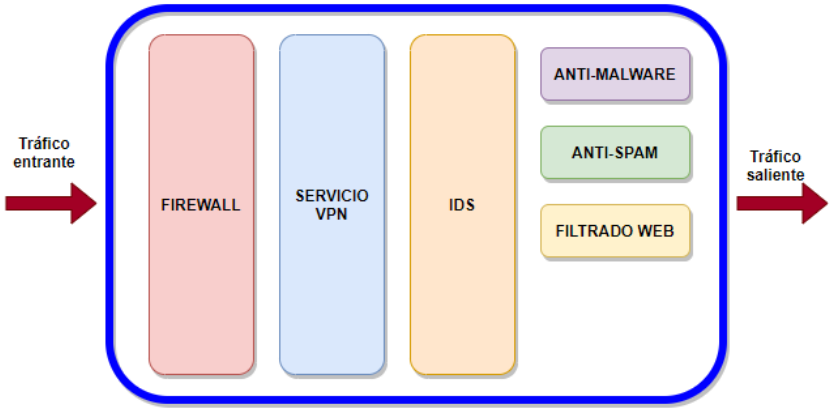


Figura 2.6: Esquema orgánico de una UTM

En cuanto al procesamiento de datos, tal y como se observa en la Figura 2.7, la UTM analiza los datos con diferentes criterios desdes la capa de red, escalando hasta las capa de aplicación. Primero los paquetes son analizados por el firewall, después por el filtrado de

contenido, luego por el IDS (a no ser que este configurado en modo promiscuo, en cuyo caso analizará paquetes a la vez que el firewal) y por último servicios como el antivirus.

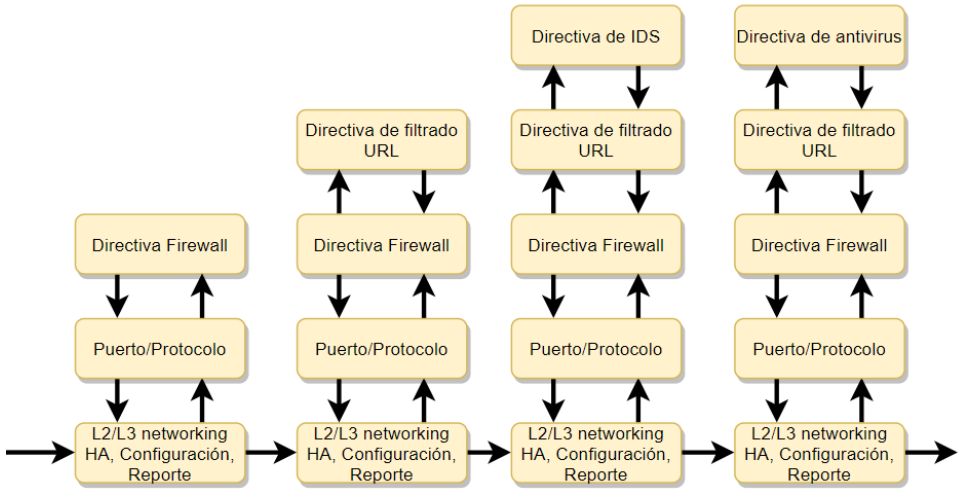


Figura 2.7: Flujo de datos y operación en una UTM

2.7.1. Arquitectura de una red con UTM

La UTM se debe instalar en la red perimetral, concretamente entre la red externa e interna. La UTM debe generar una red en estrella hacia los diferentes segmentos de la red. De esta manera cualquier flujo de datos entre dos redes tendrá que pasar por el sistema UTM. Esto permite al UTM analizar todas las conexiones pasar saber si son permitidas y el contenido de los mensajes para detectar posibles amenazas.

2.7.2. Areas de gestión en una UTM

Cada área de gestión se corresponde con una funcionalidad de UTM. Estas áreas generalmente son implementadas mediante servicios proxy de alto nivel, es decir pasarelas de aplicación. En las siguientes secciones de este capítulo se resumen la teoria de las áreas de gestión mas importates usadas para este proyecto TFG.

2.7.3. Firewall: Filtrado de conexiones

Para filtrar las conexiones el elemento principal es el núcleo de funcionalidades de la UTM, el firewall clásico. Hay 3 tipos de configuración clásica. La UTM usa los 3:

1. **Filtrado de paquetes estático, sin estado:** Es el más básico. Acepta paquetes en función de si los campos que componen el paquete IP (Puerto, dirección IP, protocolo...) coinciden para una de las reglas de aceptación del cortafuegos.

2. **Filtrado de paquetes dinámico:** Las reglas del filtrado de paquetes se crean y destruyen dinámicamente en función a la aparición y cierre de conexiones. A partir de paquetes de salida permitidos se crean automáticamente reglas para aceptar el tráfico de respuesta al de salida. Normalmente se combina el filtrado dinámico con el estático.

3. **Con inspección de estado:** Además de usar las técnicas de filtrado de 1 y 2, mantiene una tabla en la que se registra el estado de las conexiones activas en cada momento. Las entradas de la tabla se eliminan automáticamente cuando se cierra la conexión o tras un tiempo sin registro de actividad. Procesa los datos en la capa de aplicación.

2.7.4. IDS

Los Sistemas de Detección y Prevención de Intrusos tienen como objetivo la detección y prevención de ataques contra el sistema. Constan de las siguintes características generales:

1. **Función de monitorización mediante sensores:** Estos sensores son elementos pasivos y configurables que examinan el flujo de tráfico en el segmento en el que están desplegados. Si encuentran alguna anomalía generarán un evento. En el caso práctico de este TFG estará desplegado en el propio UTM, por lo que monitorizará el tráfico entre la LAN, DMZ y extranet.

2. **Función de detección de patrones:** Detectección patrones de intrusión en los registros de los servicios o comportamiento del sistema y producción de alertas para reportar el incidente a partir de los eventos recibidos por los sensores.

3. **Consola:** Interfaz por la cual se muestran los eventos y alertas al administrador. A través de la consola se pueden configurar los sensores y realizar acciones en función de los eventos recibidos.

4. **Gestor de alertas:** Parte del sistema que administra las alertas que se hayan generado.

Los IDS se puede clasificar según varios factores:

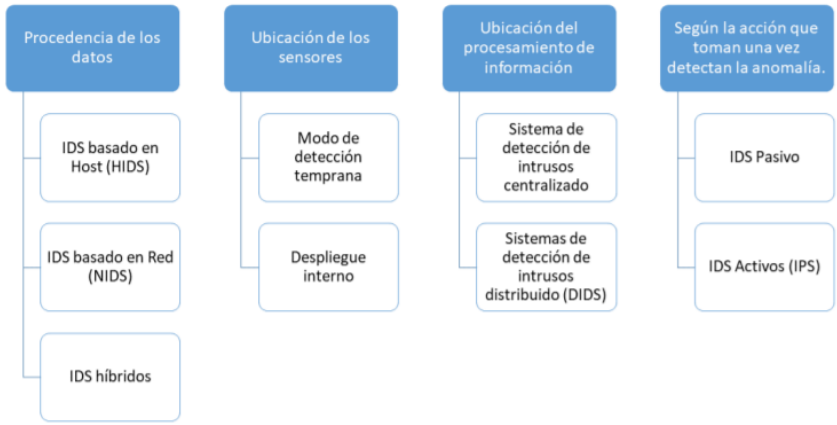


Figura 2.8: Clasificación de los IDS[12]

En el caso de los IDS integrados en un dispositivo UTM mantienen la siguiente clasificación:

- **NIDS:** Controla el tráfico de la red. Analiza todos los paquetes entrantes en busca de patrones extraños. A su vez los sistemas NIDS pueden funcionar:
  - Mediante un sistema de firmas: Se mantiene una base de datos de firmas. Estas firmas son reglas configurables por el administrador. Si el tráfico activa una de estas reglas se se producirá un evento.
  - Mediante deteccion de comportamientos anómalos: busca variaciones en el comportamiento del flujo de paquetes que indiquen anomalias en el comportamiento del usuario. Para ello hay que establecer una línea base de comportamiento para la red. Es dificil de afinar.
  - Modo híbrido: Los sistemas NIDS que usan el modo híbrido combinan el sistema de firmas, que funciona mejor con ataques conocidos, junto con la detección de anomalias, que funciona mejor para la detección de ataques aún no registrados.
- **Despliegue:** El desplique depende de la interfaz en la que se configure el sensor dentro la UTM:
  - En la WAN: es de detección temprana ya que analiza todo el tráfico entrante a la red sin ningún tipo de filtro.
  - En LAN/DMZ: es de despliegue interno ya que monitoriza las conexiones realizadas por los dispositivos internos de la interfaz. Las reglas firewall se procesarán antes del analisis de los paquetes. Los paquetes ya están filtrados por el firewall. Esto generará menos falsos positivos que en la detección temprana sin embargo también se darán más falsos negativos.
- **Centralizado:** Todos los datos procedentes de 1 o más sensores son enviados a un dispotivo central para su análisis.

- En un dispositivo UTM se pueden configurar ambos acciones a tomar:
  - **IDS Pasivo:** Sólo notifican generando alertas. No actúan contra un ataque. Procesan la información (paquetes y registros) en intrusiones y se generan alertas.
  - **IDS Activo:** Actúa contra el atacante, no se limita a la monitorización. Es similar a un firewall, con la diferencia de que el IPS actúa según los encabezados y el contenido del paquete. El firewall actúa en base al encabezado. Los IDS activos detectan la amenaza que genera la alerta y luego realizar acciones en base a ella.

Filtrado de contenido

En la Figura 2.9 se observa el flujo de funcionamiento que normalmente implementa un NIDS:

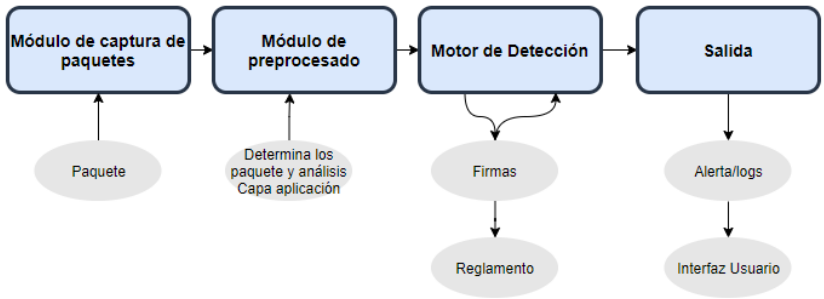


Figura 2.9: Flujo de funcionamiento en NIDS [15]

El flujo de la Figura 2.9 se resumen en:

1. Se realiza el sniffing, es decir analiza el paquete y lo manda el preprocesador.
2. En el preprocesado se buscan anomalias en las cabeceras de los paquetes y se envia la información al motor de detección para su análisis.
3. En el motor de detección se compara la información procesada del paquete con el conjunto de reglas.
4. En el plugin de salida se realiza la acción a tomar en función de si se disparó o no alguna de las reglas.

2.7.5. Control de tráfico web y caché

Squid

El firewall por su cuenta no puede realizar acciones en función del contenido de los paquetes HTTP/HTTPS. A nivel de firewall todo lo que se puede ver será la dirección IP de

destino, el puerto, los metadatos (No se puede hacer mediante hostnames a nivel de firewall porque no ve el hostname debido a que esto pasa en una petición diferente, además la DNS estará en el cuerpo de la petición). Para un mayor control sobre el tráfico web, se usa Squid, proxy que puede ver la transacción HTTP completa, incluyendo el nombre del sitio web de la petición, y puede capturar de forma transparente el contenido de esa petición HTTP, pero para HTTPS no.

Esta herramienta se usa principalmente para:

- Acelerar el acceso a recursos en línea que se usen de forma regular mediante su almacenamiento en la caché local.
- Ahorrar ancho de banda reduciendo la duplicación de descargas. Guarda en la caché y disco de la UTM de servicios como actualizaciones de windows y otros elementos a los que los clientes de la red vayan a acceder con frecuencia.
- Otras acciones de tráfico de red como control de acceso y reportes(SquidGuard y LightSquid).

Modos de Squid

Existen dos modos de configuración de Squid principales:

- **Proxy Directo:** El cliente sabe que está hablando con un proxy. Tal y como muestra la Figura 2.10, con este modo para HTTPS solo se puede capturar el hostname de destino.
- **Proxy Transparente:** las conexiones son interceptadas y desviadas hacia Squid sin necesidad de configuración alguna en la parte del cliente. El cliente no sabe de la existencia del proxy. Tal y como se muestra en la Figura 2.10, con este modo, si no se usa ningún tipo de configuración adicional, el proxy no podrá ver nada respecto al tráfico HTTPS.

Para la correcta intercepción de tráfico HTTPS se necesitará una configuración adicional del proxy, que se divide en los siguientes modos según su nivel de intrusión:

- **Bumb:** Permite a Squid realizar MITM entre el cliente y el servidor, pudiendo así desencriptar el contenido de la conexión. El certificado de autoridad del sitio web no llega al cliente, sino que el proxy presenta a éste uno falso, auto-firmado. Para hacer esto posible el cliente deberá confiar en dicho certificado, por lo que habría que instalarlo todos los navegadores del cliente. Tal y como se muestra en la Figura 2.10, es el único modo que permite ver el contenido de las páginas HTTPS y la URL completa. Se puede configurar tanto para el modo transparente como para el directo.
- **Peek:** Sólo se puede ver el hostname, no la URL completa. Observa la negociación SSL para ver el hostname al que el cliente trató de contactarse, cual es su petición. Después de hacer el Peek se podría realizar Splice.

- **Stare:** Como peek, pero pudiendo hacer bump después en lugar de Splice.
- **Splice:** Permite conectar 2 clientes, el cliente y el servidor de forma más directa, como si no hubiera proxy.
- **Peek Splice (Splice all):** Combinación de los modos peek con splice, también llamado Splice all. Sólo puede ver el hostname, pero en la mayoría de los casos será suficiente para determinar si un sitio deberá o no ser bloqueado por SquidGuard. Normalmente es la opción más viable porque no se rompe la cadena de confianza. Se puede configurar tanto para el modo transparente como para el directo.

Squid Mode	HTTPS Destination Host	HTTPS Request URL	HTTPS Page Contents	Self-Signed CA on Clients	Error Page Redirect
Direct	✓				HTTP Only
Transparent					HTTP Only
D+Peek&Splice	✓				HTTP Only
T+Peek&Splice	✓				HTTP Only
D+MITM/Bump	✓	✓	✓	✓	✓
T+MITM/Bump	✓	✓	✓	✓	✓

Figura 2.10: Alcance de los modos de Squid [16]

SquidGuard

Squidguard es un plug-in de Squid que se usa para el control de acceso basado en el dominio, la URL completa, o palabras contenidas en esta, solicitado por el cliente, pero no por contenido del cuerpo de la página web. Sus funciones principales son:

- Permitir o denegar el acceso en función al cliente y/o destino.
- Redirigir a una página de error las solicitudes a accesos a páginas bloqueadas.
- Listas personalizadas de sitios o listas negras preestablecidas de otras fuentes divididas por categorías establecidas en función al tipo de sitios (ej: apuestas, juegos...).

LightSquid

Plug-in de Squid que se usa para crear reportes del historial de accesos web a partir de los logs de Squid. Los reportes pueden incluir qué clientes se conectan a qué web, cuando ancho de banda consumieron. Puede crear reportes mensuales, diarios, etc.

2.7.6. AntiMalware

También existen plugins que permiten bloquear rangos de direcciones IP de Spammers, botnets, malware, spyware y/o bloques de direcciones IP en función del país. Están gestiona-

dos con mediantes listas ditables por el usuarios o preexistentes que se actulizan cada cierto tiempo. En ejemplo es pfBlockerNG de pfSense. Básicamente hace dos cosas:

- Bloqueo de IPs basado en reglas de firewall
- DNS sinkhole. Bloqueo de URL maliciosa mediante su redireccionamiento a una falsa IP.

2.7.7. VPN

Las VPNs se usa para establecer conexiones seguras sobre redes de transporte inseguras. Por ejemplo para que un empleado se conecte desde su casa por escritorio remoto a un ordenador conectado a la intranet empresarial. Para ello se establece un tunel VPN. La técnica de tunelización consiste en encapsular un protocolo de red sobre otro, creando un tunel entre dos puntos de una red por el cual se puede transmitir de forma segura cualquier tipo de datos. De esta forma los valores del protocolo encapsulado serán desapercibidos por los elementos intermedios de la conexión.

Dentro del contexto de las UTM, estas hacen de servidor VPN para gestionar conexiones VPN, aumentando así la confidencialidad e integridad de los datos. A cambio necesitan una mayor potencia de cálculo para realizar las operaciones de cifrado y descifrado y no generar cuellos de botella.

Existen 2 arquitecturas básicas de configuración para el acceso remoto

- **De acceso remoto o roadWarrior:** Con el objeto de que un usuario se conecte a una red local remota se establece un tunel entre dicho usuario y el servidor VPN remoto que le dará acceso a la red local. Para la creación del tunel el usuario debe autenticase frente al servidor de acceso remoto, y el servidor, ante el cliente. Una vez autenticados ambos se establece el tunel y el usuario podrá relacionarse con los nodos de la red como si fuera un usuario local.
- **VPN punto a punto o site-to-site:** En este caso el tunel se establece entre dos redes locales en lugar de un cliente y un servidor VPN. Cada red local tendrá su propio servidor VPN. Cualquiera de los clientes de una red local podrá establecer conexión clientes de la otra red como si estuvieran en la misma y viceversa.

Tecnologias utilizadas con VPN:

- PPTP (Point-to-Point Tunneling Protocol): protocolo de Microsoft diseñado específicamente para implementar VPN. PPTP corre sobre el protocolo de enlace de datos PPP (Poin-to-Point-Protocol). PPTP utiliza túneles GRE para implementar el túnel de una VPN, encapsulando tramas PPP y cifrado RC4. Permite una conexión por túnel. La autentificación de usuarios se realiza a través de los protocolos PAP (Password Authentication Protocol) y MSCHAP (versión de Microsoft de CHAP). Se debe tratar de evitar su uso ya que se han encontrado diversas vulnerabilidades referentes a su uso.

- L2TP (Layer 2 Tunneling Protocol): utiliza el protocolo PPP para proporcionar una envoltura inicial de los datos y luego incluir los encabezados adicionales. L2TP se debe usar siempre junto con IPSec debido a que L2TP solo realiza la autenticación entre los puntos finales del túnel a la hora de establecer la conexión, pero no para cada uno de los paquetes que viajan a través de el.

- IPSEC: Protocolo a nivel del red. Permite definir un túnel entre dos pasarelas. Una pasarela IPSec normalmente consiste en un router de acceso o firewall en el que esté implementado el protocolo IPSec. Las pasarelas IPSec están situadas entre la red privada del usuario y la red compartida del operador.

- SSL/TLS: Protocolo a nivel de transporte. Permite la autenticación tanto de cliente como servidor, usando claves públicas y certificados digitales. Proporciona comunicación segura mediante el cifrado de la información entre emisor y receptor.

2.7.8. Accesos al sistema

HTTPS

Para el acceso al configurador web del sistema se usa el protocolo HTTPS. Al protocolo de aplicación HTTP se añade el protocolo SSL en la capa intermedia entre este y TCP. SSL es el encargado de cifrar la comunicación.

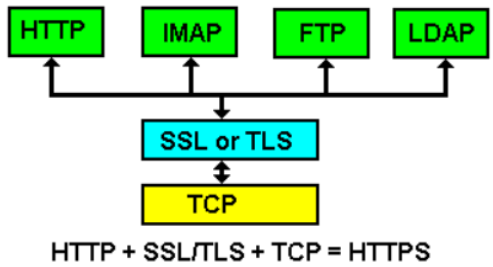


Figura 2.11: Arquitectura HTTPS[53]

SSL logra establecer una conexion segura mediente la creación de la clave de sesión. La clave de sesión es simétrica. Sin embargo el protocolo SSL dicta que para establecer la conexión de cifrado simétrico se ha de enviar del cliente al servidor mediante el uso de cifrado asimétrico. El uso de este cifrado asimétrico se apoya en la infraestructura PKI (Infraestructura de Clave Pública) que define conjunto de elementos necesarios para crear el sistema de certificación usado. Las fases de SSL para establecer una comunicación cifrada vienen dadas por la Figura 2.12.

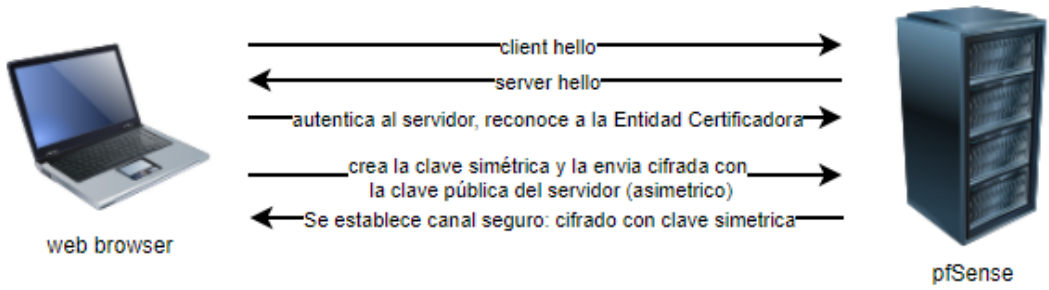


Figura 2.12: Flujo de operaciones SSL

SSH y SSH-Agent

Con el túnel ssh, al igual que con SSL, se cifra la sesión. En una conexión ssh una vez encriptada de forma simétrica para la creación del tunel, el usuario debe autenticarse. Para ello tradicionalmente este debe introduce sus credenciales, usuario y contraseña.

Para reforzar la seguridad de las conexiones ssh, se puede añadir una capa extra de seguridad, gestionada mediante algún ssh-agent, autenticando la conexión además de con las credenciales de usuario y la contraseña, mediante un par de claves asimétricas. En la Figura 2.13 se muestra cómo se autentifican el cliente y servidor mediante el paso extra de par de clave.

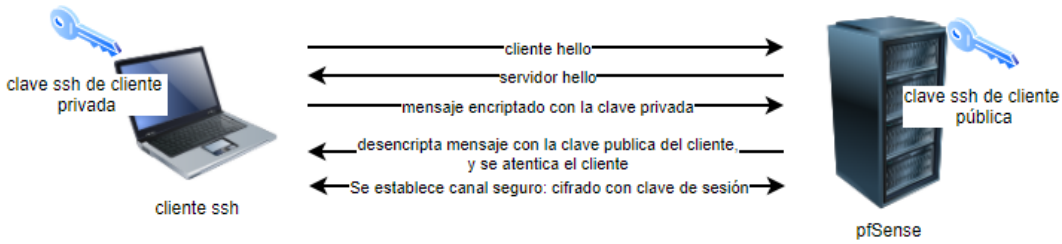


Figura 2.13: Flujo operaciones SSH con autenticación de usuario por clave

2.8. Estudio Comparativo

En esta sección se realizará una comparativa entre los UTMs tipo software más populares. Estos han de ser de software libre pues el cliente quiere reducir costes. Elegir un firewall UTM open source no reduce los niveles de seguridad si se compara con uno comercial por lo que analizamos las siguientes opciones.

En la Tabla 2.1 se observa una pequeña comparativa de las caracteristicas de algunos de los firewalls UTM más populares [39] que se están considerando para implantar como solución. Todos tienen las funciones requeridas por el cliente, por lo que habrá que comparar un poco más alla de las funcionalidades para elegir el firewall a instalar. A lo largo de las siguientes subsecciones se analizaran las diferentes caracteristicas que puede tener el firewall UTM.

Caraterística\UTM	PfSense	OPNSense	IPFire	ZeroShell
Licencia	Apache 2.0	Simplified BSD	GPL	GPL
SO	FreeBSD	FreeBSD	Linux	Linux
Firewall core	Packet Filter	Packet Filter	NetFilter	NetFilter
IDS	Snort/Suricata	Snort/Suricata	Suricata	Snort
Acceso	SSH, Web (HTTP/HTTPS), RS232	SSH, Web (HTTP/HTTPS), RS232	SSH, Web (HTTPS), RS232	SSH, Web (HTTPS), RS232
QoS	Si	Si	Si	Si
DMZ	Si	Si	Si	Si
Configuración	texto\GUI	texto\GUI	texto\GUI	GUI
NAT	Si	Si	Si	Si
VPN	OpenVPN, IPsec, L2TP, IKEv2, Tinc, PPTP	OpenVPN, IPsec, L2TP, IKEv2, Tinc, PPTP	OpenVPN, IPsec, IKEv2	OpenVPN, IPsec, IKEv2
Módulos de terceros	Si	No	Si	No
Filtrado Web y caché	Squid	Squid	Squid	Squid
Antivirus	Clamav con Squid	Clamav con Squid	Clamav con Squid	Clamav con Squid
Actualizaciones	Frecuentes	Frecuentes	Frecuentes	Frecuentes
Comunidad	Muy activa	Activa	Poco activa	Poco activa
Documentación	Muy alta	Alta	Media	Media
Hardware recomendado	CPU >1 Ghz RAM >1 GB	CPU >1 Ghz RAM >2 GB	CPU >1 Ghz RAM >1 GB	CPU >233 Mhz RAM >96 MB

Tabla 2.1: Comparativa de UTMs libres [38, 40, 41, 42]

2.8.1. SO: Linux vs FreeBSD

FreeBSD es más seguro y robusto. Prueba de ello es que el número de vulnerabilidades encontrado es significativamente menor, tal y como se observa en las gráficas de la Figura 2.14

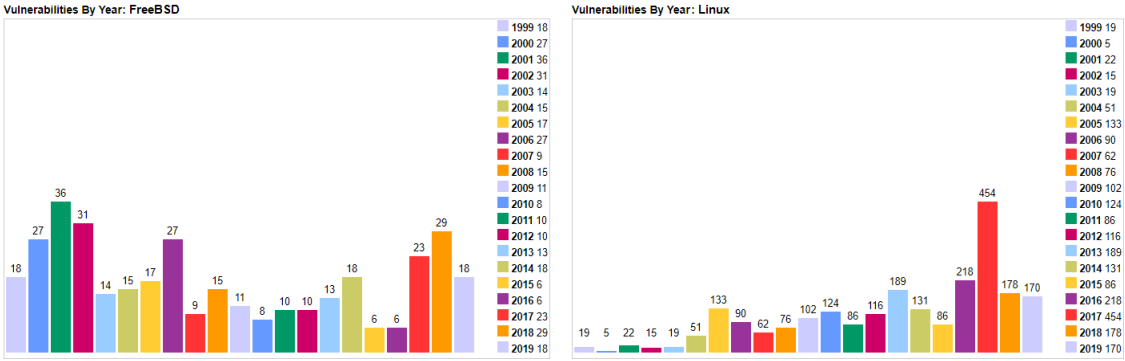


Figura 2.14: Vulnerabilidades por año FreeBSD[43], Linux[44] según el CVE

2.8.2. Filtrado de conexiones: Packet Filter vs Netfiler(Iptables)

Ambos permiten realizar operaciones de operaciones de manipulación de paquetes. Representan la parte central y más importante del firewall. Sus características principales son:

- Filtrado de paquetes con control de estado.
- Filtrado de paquetes sin control de estado.
- Traducción de direcciones y puertos NAT/PAT.
- Extensión del framework por terceros. En el caso de los UTM es muy importante porque parte de los módulos que se estudiarán a continuación basan su funcionalidad en estos mecanismos:
  - Control de tráfico. Es la base en los mecanismo de QoS.
  - Control de número de veces que se activa una regla. Importate para los sistemas de monitorización de tráfico.
  - Implementación de proxies transparentes a partir del subsistema NAT/PAT.

Packet filter y Netfiler extienden la misma funcionalidad, en sus diferencias cabe destacar:

- Packet filter esta implementado en sistemas FreeBSD y Netfiler en sistemas Linux.
- Síntaxis: Packet Filtering usa una sintaxis más sencilla que iptables.

2.8.3. IDS: Snort vs Suricata

Como Sistema de Detección y Prevención de Intrusos se ha de elegir entre Snort y Suricata.

Ambos son herramientas NIDS basadas en un motor que funciona con una base de datos de reglas o firmas. Son las alternativa de bajo coste a NIDS comerciales en entidades pequeñas y medianas. Snort tiene una ligera mayor popularidad que Suricata.

Tienen tres modos de acción:

- **Modo sniffer**: se monitoriza por pantalla toca actividad de las redes configuradas en Snort.
- **Modo NIDS**: Se generan alarmas en función a una comparación del flujo de datos y la base de firmas instaladas y activas en el NIDS. Estas firmas son reglas que se actualizan periodicamente en función al a base de datos de donde se descarguen. También el usuario puede crear sus propias reglas para limitar el uso de determinadas aplicaciones.
- **Modo packet logger**: se almacenan logs de toda la actividad de la red para realizar un análisis de posterior de esta.

A continuación se muestra una pequeña comparativa entre Snort y Suricata para ayudar a distinguir el NIDS a instalar idealmente. La Tabla 2.2 muestra más favorable el uso de Snort frente a Suricata debido que la documentación disponible y la actividad de la comunidad es

mayor. La Figura 2.15 muestra la justificación de esta decisión. El número de vulnerabilidades registradas en el CVE es menor para Snort.

Característica\IDS	Snort	Suricata
Licencia	GNU GPL v2	GNU GPL v2
Modo detección	Reglas	Reglas
Detección automática de protocolos	Si	Si
Multihilo	Si	Si
Personalización CPU	Si (a partir de la versión 3.0)	Si
Calidad Documentación	Alta	Media
Comunidad	Muy activa	Activa

Tabla 2.2: Comparativa de características principales

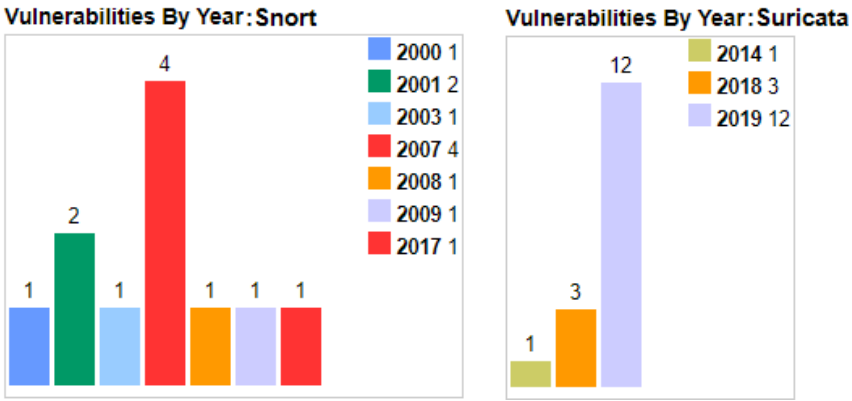


Figura 2.15: Vulnerabilidades por año Snort[45], Suricata[46] según CVE

2.8.4. Filtrado web, caché y antivirus

Para todos los firewall estudiados se usa servidor proxy Squid, por lo que no se realizará comparativa de este punto. Vaya a la sección 2.7.5 para más información sobre el funcionamiento y funcionalidades de Squid.

2.8.5. Protocolos VPN

Para seleccionar el protocolo VPN se ha creado una pequeña tabla comparativa con las características principales de las opciones disponibles más atractivas, Tabla 2.3.

	OpenVPN	IKEv2/IPSec	L2TP/IPSec	PPTP
Introducción	Muy popular. No estandarizado bajo RFC. Usa SSL/TLS para el intercambio de llaves.	Estandarizado en RFC 7296. Estándar de defecto en internet.	Estandarizado en RFC 3193.	Basado en tuneliazar PPP de capa 2
Encriptación	Usa la libreria OpenSSL que implementa algoritmos 3DEs, AES, RC5... Con IKEv2 máximo de 256 bit keys	Implementa algoritmos 3DEs, AES, Blowfish, Camellia. Con IKEv2 máximo de 256 bit keys	Encapsulación doble via procolo estándar IPSec	Microsoft Point-to-Point que implementa algoritmos RSA y RC4. Máximo de 128 bit keys
Vulnerabilidad	No conocido para el uso de algoritmo + certificado de autentificación	No conocido para el uso de algoritmo + certificado de autentificación. Conocidas si se usa IKE.	No conocido para el uso de algoritmo + certificado de autentificación	Sistema de autentificación es vulnerable a ataques por diccionario. RC4 es vulnerable a ataques como bit-flipping.
Velocidad	Similar a IKEv2	Similar a OpenVPN	Similar a OpenVPN	Más rápido que OpenVPN, IPSec
Puertos	Cualquiera con UDP o TCP	Fijos: UDP 500, 50 y 4500	Fijos: UDP 500, 1701 y 4500	Fijos: TCP 1723, 47
Plataformas compatibles	Windows, macOS, Linux, Apple iOS, Android, DD-WRT	Windows, macOS, Linux, Apple iOS, Android	Windows, macOS, Linux, Apple iOS, Android	Windows, macOS, Linux, Apple iOS, Android, DD-WRT
Rendimiento	Estable y rápido sobre todo tipo de conexiones	Estable y rápido sobre todo tipo de conexiones. Configuración puede ser más compleja que OpenVPN.	Estable sobre todo tipo de conexiones. El más lento de la comparativa. Configuración puede ser más compleja que OpenVPN.	Existen problemas de compatibilidad con protocolo GRE y algunos routers. No es confiable en conexiones inestables.

Tabla 2.3: Comparativa de características principales de protocolos VPN[47]

Observando la tabla comparativa resulta como mejor opción el uso de OpenVPN ya que no cuenta con vulnerabilidades notables, su configuración es sencilla frente al resto de protocolos sin vulnerabilidades y el hecho de que pueda usar cualquier puerto facilita la configuración del firewall.

Capítulo 3

Plan de proyecto

3.1. Resumen del proyecto

En este capítulo se definirá la planificación del proyecto en detalle. Se documentarán las fases del proyecto y por cada fase se definirán sus tareas junto con la calendarización de las mismas. También se hará una exploración de los posibles riesgos además de un seguimiento de los mismos.

3.1.1. Propósito, Alcance y Objetivos

El objetivo de este proyecto es la integración de un sistema firewall UTM de bajo coste que permita cubrir las necesidades actuales de seguridad en la infraestructura de red de una pequeña empresa. Para una mayor detalle de los objetivos lea el capítulo 1. Los requisitos de la integración están definidos en el capítulo 4

3.1.2. Definiciones y Acrónimos

En la Tabla 3.1, se presentan los acrónimos y definiciones que aparecen a lo largo de este documento.

Acrónimo	Significado
INCIBE	Instituto Nacional de Ciberseguridad de España
TFG	Trabajo de Fin de Grado
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
RPGD	Reglamento General de Protección de Datos
UP	Unified Process
UTM	Unified Threat Management
ENS	Esquema Nacional de Seguridad
NIST	National Institute of Standards and Technology
PSO	Plan de Seguridad del Operador
PPE	Planes de Protección Específicos
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol
NAT	Network Address Traslation
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
DNS	Domain Name System
WAN	Wide Area Network
LAN	Local Area Network
DMZ	Demilitarized Zone
VLAN	Virtual Local Area Network
QoD	Quality of Detection
NVT	Network Vulnerability Test

Tabla 3.1: Acrónimos

3.2. Metodología

Para la realización de este proyecto se ha optado por la adaptación de una metodología iterativa e incremental como UP[17] a las características del mismo. El motivo de esta elección se basa en la facilidad de aplicación a un trabajo individual con un enfoque en la investigación para un fin.

Cada iteración está compuesta por 4 fases que conforman el ciclo del vida del proyecto: Inicio, elaboración, construcción y transición. Sobre cada fase se aplica una serie de iteraciones que obtienen como resultado el refinamiento de los artefactos. Por cada una de las iteraciones se sigue un desarrollo en cascada donde, para la tarea del proyecto a realizar, primeramente se planificará, se desarrollarán los requisitos, después se realizará un análisis, y a partir de estos se diseñará una solución, que después de eso se implementará y testará. Si todo funciona correctamente se desplegará dicha solución.

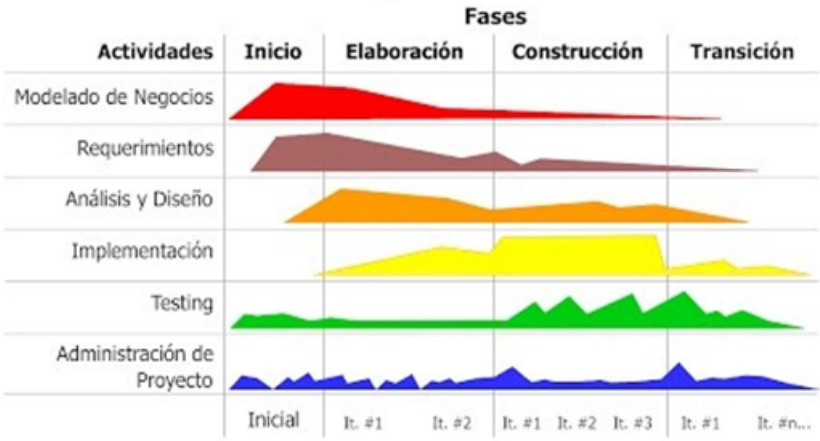


Figura 3.1: Ciclo de vida UP

3.2.1. Artefactos del Proyecto

En este este proyecto los artefactos a desarrollar son los siguientes:

- Plan de Desarrollo
- Requisitos
- Análisis y diseño
- Implementación
- Test

3.2.2. Definición de las fases del proyecto

- **Inicio**: En esta fase se realiza el análisis del proyecto en sí para poder determinar el alcance general del proyecto. En esta fase las actividades a realizar son las siguientes:
  - Alcance del proyecto: análisis del contexto, estado del arte, requisitos y restricciones más importantes.
  - Planificación y preparación del caso de negocio: Análisis y gestión de riesgos, plan de proyecto y costes.
  - Análisis de la viabilidad del proyecto: Estudio de las posibles soluciones y costes.
  - Preparación del entorno: Herramientas.
- **Elaboración**: En esta fase se diseña una solución preliminar a partir de un análisis obtenido de la síntesis del alcance del proyecto y su viabilidad. Se realizarán las siguientes tareas:

- Análisis de la infraestructura.
- Análisis de diferentes alternativas para el diseño de una la solución preliminar.
- Refinamiento de los requisitos.
- Refinamiento de la solución seleccionada, definición de componentes a usar.
- Desarrollo planes de iteración de la siguiente fase.

Construcción: En esta fase se desarrolla el producto. Se clarifican los requisitos pendientes y se implanta el sistema en un entorno de pruebas de forma iterativa e incremental, obteniendo versiones del mismo para así minimizar los riesgos. Para ello habrá que:

- Desarrollar la solución en el entorno de pruebas, proceso y herramientas.
- Testear de los diferentes componentes del sistema para comprobar que cumplen con la funcionalidad deseada.
- Desarrollo planes de iteración de la siguiente fase.

- **Transición**: En esta fase marca el fin de proyecto. Se integrará el sistema en el entorno de producción, se cubrirán los casos de uso que no se hayan podido en la infraestructura maqueta si se da el caso, se completará, integrará y testeará el producto. En ella se analizarán los resultados obtenidos, se ajustarán errores y defectos encontrados, se capacitará a los usuarios y se proveerá de parte del soporte necesario. Las tareas principales de esta fase son:

  - Integración del sistema
  - Testeo en el entorno real
  - Afinación de las configuraciones en función del feedback proporcionado por el cliente.
  - Manual de usuario
  - Análisis de la mejora en el sistema.

3.3. Gestión del Proceso

En la estimación de las tareas a desarrollar, se tendrá como referencia otros proyectos realizados antes de características similares.

3.3.1. Gestión de tiempo

En esta sección se incluye un resumen de las figuras temporales relevantes, y se detalla el seguimiento de las tareas del proyecto previamente establecidas.

Se incluye un diagrama Gantt con los intervalos y fechas de desarrollo de cada fase del proyecto:

Resumen temporal del proyecto	
Fecha de inicio	2/2020
Fecha de fin	6/2021
Carga de trabajo semanal	7 horas
Horas totales previstas	288 horas
Horas finales	336 horas

Tabla 3.2: Tabla de resumen temporal del proyecto

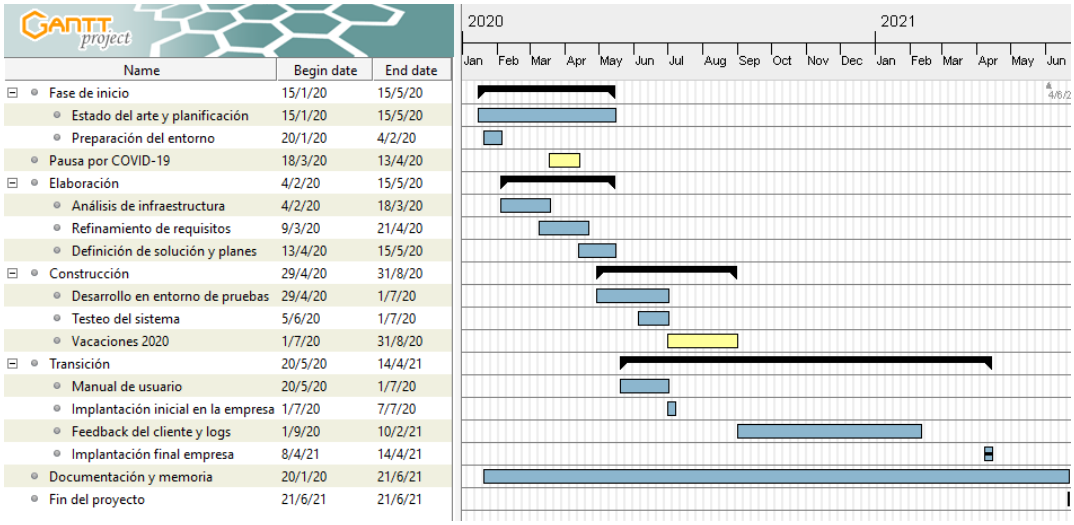


Figura 3.2: Diagrama Gantt de las fases del proyecto

Aunque la estimación de horas de trabajo aproximadamente se cumplió, durante la realización de este proyecto han tenido efecto varios de los riesgos contemplados en 3.3.2 Plan de gestión de riesgos:

Con la llegada de la pandemia COVID-19 el proyecto tuvo un parón no planificado de aproximadamente 1 mes porque se dieron los riesgos de enfermedad del trabajador y pérdida de comunicación con cliente. Así mismo la comunicación con cliente se deterioró considerablemente hasta junio de 2020.

La pandemia también ocasionó el cambio de requisitos y artefactos de proyecto. Se realizó una primera integración del sistema donde no se activaron todos los plugins testeados en el entorno de pruebas con el objeto de reducir el nivel de refinamiento a aplicar y a la vez dotar al cliente de un sistema seguro y de capacidad para realizar conexiones VPN que permitieran a parte de sus empleados trabajar desde casa usando conexiones más seguras de las que estaban usando en aquel instante.

También se han dado problemas de integración del sistema, sobretodo durante la segunda fase de instalación, en la que se introdujeron las aplicaciones que necesitan un refinamiento

constante por parte del administrador.

3.3.2. Plan de gestión de riesgos

En esta sección se identifican riesgos a los que esta expuesto el desarrollo del proyecto, soluciones de mitigación y contingencia y el seguimiento de los riesgos durante las fases del proyecto.

En se describen los riesgos de forma descendente, es decir, de más crítico a menos crítico.

Identificador	**R01- Error en la planificación**
Descripción	Se realiza una mala planificación de los tiempos de elaboración del proyecto.
Impacto	Crítico
Probabilidad	80 %
Exposición	Alto
Plan de mitigación	Analizar las tareas adecuadamente y desarrollarlas dentro de los tiempos establecidos.
Plan de contingencia	Priorizar el desarrollo de las tareas por criticidad, replanificar la calendarización de las tareas y reevaluar los riesgos.

Tabla 3.3: R01 - Error en la planificación

Identificador	**R02 - Pérdida de datos y/o documentos**
Descripción	Se realiza una mala planificación de los tiempos de elaboración del proyecto.
Impacto	Carastrófico
Probabilidad	1 %
Exposición	Bajo
Plan de mitigación	Usar un sistema de versiones en la nube además de guardar en local.
Plan de contingencia	Evaluar el impacto, replanificar la calendarización de tareas y reevaluar los riesgos.

Tabla 3.4: R02 - Pérdida de datos y/o documentos

Identificador	**R03 - Conocimiento insuficiente sobre las tecnologías**
Descripción	El tiempo establecido para el aprendizaje de las tecnologías es insuficiente para el desarrollo del proyecto.
Impacto	Crítico
Probabilidad	50 %
Exposición	Medio
Plan de mitigación	Realizar una labor de investigación para ver que tecnologias y nivel de conocimiento se necesita para la configuración e integración correcta del equipo.
Plan de contingencia	Evaluar el impacto y replanificar la calendarización de tareas para una mayor investigación en las tecnologías a aplicar.

Tabla 3.5: R03 - Conocimiento insuficiente sobre las tecnologías

Identificador	**R04 - Problemas de integración del nuevo sistema**
Descripción	Se dan problemas a la hora de integrar el equipo en el entorno real.
Impacto	Crítico
Probabilidad	90 %
Exposición	Alto
Plan de mitigación	Investigar sobre el equipo a implantar y realizar pruebas de las configuraciones implantadas.
Plan de contingencia	Replanificar las tareas y afinar las configuraciones del equipo hasta su correcta integración.

Tabla 3.6: R04 - Problemas de integración del nuevo sistema

Identificador	**R05 - Indisponibilidad del trabajador**
Descripción	El trabajador no puede cumplir con los plazos establecidos por priorización de otros trabajos ya que se encuentra trabajando en otra empresa.
Impacto	Crítico
Probabilidad	70 %
Exposición	Alto
Plan de mitigación	Dedicar los días no laborales en la otra empresa a desarrollar el proyecto.
Plan de contingencia	Replanificar la planificación de las tareas y reevaluar los riesgos.

Tabla 3.7: R05 - Indisponibilidad del trabajador

Identificador	**R06 - Enfermedad del trabajador**
Descripción	El trabajador enferma y no puede cumplir con los plazos establecidos.
Impacto	Crítico
Probabilidad	80 %
Exposición	Alto
Plan de mitigación	Cuidar la salud del trabajador y dedicar los días no laborables a la realización del proyecto.
Plan de contingencia	Priorizar el desarrollo de las tareas por criticidad, replanificar la calendarización de las tareas y reevaluar los riesgos.

Tabla 3.8: R06 - enfermedad del trabajador

Identificador	**R07 - Pérdida de comunicación con cliente**
Descripción	No se consigue la comunicación entre el cliente y el trabajador influyendo en la continuidad del proyecto.
Impacto	Crítico
Probabilidad	60 %
Exposición	Alto
Plan de mitigación	Fijar fechas de reuniones con antelación.
Plan de contingencia	Replanificar la planificación de las tareas y reevaluar los riesgos.

Tabla 3.9: R07 - Pérdida de comunicación con cliente

Identificador	**R08 - Cambio de requisitos**
Descripción	Durante la realización del proyecto se encuentran requisitos que no se tuvieron en cuenta durante las primeras fases.
Impacto	Crítico
Probabilidad	80 %
Exposición	Alta
Plan de mitigación	Analizar los objetivos del proyecto adecuadamente para fijar correctamente los requisitos.
Plan de contingencia	Priorizar el desarrollo de las tareas por criticidad, replanificar la calendarización de las tareas y reevaluar los riesgos.

Tabla 3.10: R08 - Cambio de requisitos

3.3.3. Estimación de costes

En esta sección se describen los recursos necesarios para el desarrollo del proyecto. Los recursos se dividirán en 4 categorías: personal, equipos y herramientas, material de oficina y espacio. Para cada uno de ellos se adjunta una descripción, la disponibilidad y las fechas de necesidad.

Personal

El proyecto consta de una única persona para gestionarlo y llevarlo a cabo. Esta persona realizará funciones de auditor IT. Siendo el único recurso en personal de proyecto, se necesitará durante la duración completa del proyecto.

Seguridad / Ciber Seguridad y Auditoría

CATALUÑA	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	50 - 60K	60 - 80K	80 - 100K	100 - 130K	↑
Cybersecurity Engineer	35 - 40K	40 - 50K	50 - 60K	60 - 80K	↑
IT Auditor/a	30 - 40K	40 - 50K	50 - 60K	60 - 80K	↑

C. DE MADRID	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	50 - 60K	60 - 70K	70 - 90K	90 - 120K	↑
Cybersecurity Engineer	40 - 50K	50 - 60K	60 - 80K	80 - 95K	↑
IT Auditor/a	30 - 40K	40 - 55K	55 - 65K	65 - 85K	↑

ANDALUCÍA	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	40 - 50K	50 - 60K	60 - 70K	70 - 90K	↑
Cybersecurity Engineer	25 - 28K	28 - 32K	32 - 40K	40 - 55K	↑
IT Auditor/a	25 - 30K	30 - 40K	40 - 50K	50 - 65K	↑

C. VALENCIANA	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	40 - 50K	50 - 60K	60 - 70K	70 - 90K	↑
Cybersecurity Engineer	25 - 28K	28 - 32K	32 - 40K	40 - 60K	↑
IT Auditor/a	25 - 30K	30 - 40K	40 - 50K	50 - 70K	↑

PAÍS VASCO	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	40 - 50K	50 - 60K	60 - 70K	70 - 90K	↑
Cybersecurity Engineer	25 - 28K	28 - 32K	32 - 40K	40 - 60K	↑
IT Auditor/a	25 - 30K	30 - 40K	40 - 50K	50 - 70K	↑

ARAGÓN	≤ 2 años	2 - 6 años	6 - 10 años	>10 años	Tendencia
CISO	40 - 50K	50 - 60K	60 - 70K	70 - 90K	↑
Cybersecurity Engineer	20 - 25K	25 - 30K	30 - 40K	40 - 60K	↑
IT Auditor/a	20 - 25K	25 - 30K	30 - 40K	40 - 60K	↑

Figura 3.3: Remuneraciones medias en ciberseguridad, España 2021[19]

Para establecer el coste de este recurso, tendremos en cuenta la Figura 3.3. En esta Figura podemos observar que los salario de auditor IT con menos de 2 años de experiencia oscilan entre los 20-40 K en España. Valladolid no es una ciudad con salarios a la alta por lo que se establecerá un salario de 25.000€/año, lo que equivale a unos 13.5€/hora.

Equipos y herramientas

Durante este proyecto se ha usado software gratuito para la disminución de los costes del mismo. Para el desarrollo del proyecto se necesitarán las siguientes herramientas:

- **Ordenador portátil:** se usará para la realización completa del proyecto. Tabla 3.11
- **Servidor (2):** Un servidor de pruebas, para el entorno de pruebas, Tabla 3.12, y otro para el entorno real, Tabla 3.13.
- **Google Drive:** Para guardar las copias de seguridad del trabajo.

- **Teams Microsoft:** Como método de comunicación con los tutores.
- **OpenVAS:** Para el análisis de vulnerabilidades.
- **PfSense:** UTM software que se configura e implanta.
- **PuTTy:** Para el acceso a la UTM mediante SSH.
- **PuTTyGen:** Para fortalecer la confidencialidad del acceso a la UTM.
- **Draw.io:** Para la realización de diagramas.
- **Escritorio remoto:** Para el acceso al entorno real.
- **Navegador Chrome:** Para la configuración de la UTM.
- **WakeOnLanGui:** Para encender los PC del entorno real mediante Wake On LAN.
- **OpenVPN Client:** Para el acceso al entorno real.
- **TightVNC:** Para el acceso a escritorio remoto.
- **Latex:** Para la realización de la memoria.
- Durante la realización de los test es posible que se usen otros equipos como ordenadores o routers cedidos temporalmente por la empresa.

Ordenador portátil		
Descripción:	Ordenador portátil MSI, año 2015.	
Componentes	Procesador:	Core i7-4712HQ CPU @ 2.3GHz 3.3GHz.
	Memoria RAM:	8 GB DDR3.
	Tarjeta gráfica:	NVIDIA GeForce® 920M.
	Disco Duro:	SATA 1 TB.
	Resolución de la pantalla:	1920x1080 ppp.
Precio de compra:	700€	
Precio amortización proyecto:	0*€ (Ya amortizado)	

Tabla 3.11: Ordenador portátil: características.

Servidor pruebas		
Descripción:	Servidor del año 2011	
Componentes	Procesador:	i7-2700K CPU @ 3.50GHz.
	Disco Duro:	SATA 500 GB.
	Memoria RAM:	4 GB DDR3.
Precio de compra:	1200€	
Precio amortización proyecto:	0*€ (Ya amortizado)	

Tabla 3.12: Servidor para el entorno de test:características

Servidor		
Descripción:	Servidor para entorno real	
Componentes	Procesador:	Xenon 2.2GHz—10MB—4C—80W
	Memoria RAM:	16 GB DDR3.
	Tarjeta gráfica:	NVIDIA GeForce® 920M.
	Disco Duro:	SATA 2x500 GB.
	Puertos NIC:	4.
Precio de compra:	211.77€	

Tabla 3.13: Servidor entorno real: características.

Espacio:

- **Hogar del trabajador**: La mayor parte del proyecto se desarrollará desde la casa del propio desarrollador del proyecto.
- **Conexión a internet**: Será necesario en todas las fases del proyecto. Se contabilizará como gastos al proyecto al realizarse en su mayoría el proyecto desde el hogar del trabajador.
- **Electricidad**: Será necesario en todas las fases del proyecto. Se contabilizará como gastos al proyecto al realizarse en su mayoría el proyecto desde el hogar del trabajador.
- **CPD**: Será necesario acudir al entorno en el que se implatará el UTM como mínimo en la fase de implantación.

En base a todos los recursos necesarios mencionados anteriormente se calcula el coste de los activos y pasivos usados para el desarrollo del proyecto. Se ve reflejado en la Tabla 3.14 :

Recurso	Precio dentro del proyecto	Cantidad	Subtotal
1. Ordenador portátil	0€	1	0€
2. Servidor pruebas	0€	1	0€
3. Servidor	211.77€	1	211.77€
4. Coste trabajador	13.5€/hora	336 horas	4536.00€
5. Internet	30.00€/mes	336 horas	14.00€
6. Electricidad	0.15€/kwh	336 horas	50.4€
		Total:	4812.17€

Tabla 3.14: Presupuesto

Capítulo 4

Análisis de la infraestructura y fijación de objetivos

En este capítulo se realiza el análisis de infraestructura. Incluye una primera elicitación de requisitos en función a las necesidades del cliente, definición de roles, diagramas físico-lógicos de la infraestructura y estimación de debilidades de esta.

Tanto para determinar si las metas impuestas por el cliente son asequibles, como para comunicar los requisitos de este proyecto adecuadamente, se debe caracterizar la red de la empresa. A lo largo de este capítulo, con la intención de dar una visión más completa de la infraestructura de la empresa, de cara a poder definir sus necesidades con certeza, se realizarán varios mapas de red con diferente nivel de detalle, para realizar estos diagramas se seguirán las indicaciones impartidas por el método descendente[20] en la medida de lo posible, también se tendrán en cuenta las preferencias del cliente a la hora de definir las necesidades de la infraestructura.

4.1. Caracterización de la arquitectura lógica

La red de la empresa que vamos a estudiar cuenta con un edificio de 4 plantas, donde se encuentran varias salas a las que se deberá proveer de servicios de red. En la Figura 4.1 se caracteriza la arquitectura lógica de la red en dicho edificio, con el propósito de dar una percepción general de la estructura de la red antes de entrar en detalles físico-lógicos. Como se puede observar en la Figura 4.1, la red troncal tiene un claro diseño de *collapsed backbone*[21], donde todos los elementos se conectan al switch central, formando así una topología de estrella. También se observa que se dispone en una jerarquía de dos capas[22], la de núcleo contraído y la de acceso. La capa de núcleo contraído esta formado por el switch central, (switch gestionable de capa 2), junto con el *UTM firewall* y el router, mientras que la capa de acceso la conforman el resto equipos conectados al switch central.

Este tipo de diseño es clásico en infraestructura pequeñas como la que se va a estudiar, pues es fácilmente configurable y escalable, pero hay gran riesgo si alguno de los equipos troncales falla. Al no haber redundancia de estos, si un equipo troncal falla no habrá conexión de red.

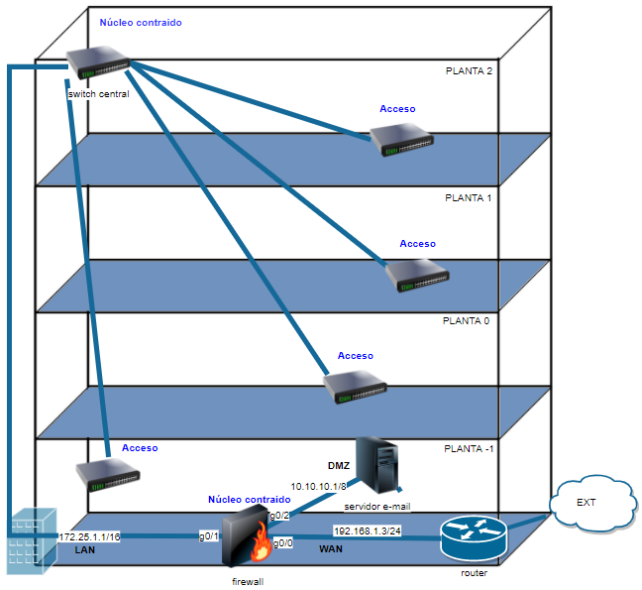


Figura 4.1: arquitectura lógica

En la Figura 4.1 también se puede observar las subredes desde el punto de vista del firewall. El firewall cuenta con 3 interfaces de red activas, que conectan con 3 subredes que son:

- WAN: Conecta al puerto 0 del firewall cuya dirección es 192.168.1.3. Está conectado al router que da acceso a internet. En esta subred el firewall obtiene una dirección IP estática a partir del router que está conectado a internet. Todo el tráfico del router está redireccionado al firewall. El firewall está configurado para que actúe como servidor DHCP de esta subred.

- LAN: usa el puerto 1 del firewall cuya dirección es 172.25.1.1. Está conectado al switch central que gestionará todas las conexiones entre los equipos de la LAN. El firewall está configurado para que actúe como servidor DHCP de esta subred.

- DMZ: usa el puerto 2 del firewall con la dirección de red 10.10.10.1/8. Está directamente conectado al servidor de correo electrónico, puesto que único servidor que requiere ser accedido por usuarios no pertenecientes a la empresa. El firewall está configurado para que actúe como servidor DHCP de esta subred.

Subred	Dirección IP/Máscara	Router por Defecto	Servidor DHCP	Rango de Asignaciones
WAN	192.168.3.0/24	192.168.1.1	192.168.3.1	192.168.3.2-254
LAN	172.25.0.0/16	172.25.1.1	172.25.1.1	172.25.1.2-254
DMZ	10.0.0.0/8	10.10.10.1	10.10.10.1	10.10.10.2-254

Tabla 4.1: Direccionamiento

4.2. Caracterización de nombres

Para permitir la identificación de todos los elementos de la red se ha usado un esquema de nombres con las siguientes partes:

- Elemento: identifica el tipo de elemento.
- Numero identificativo del tipo de elemento: identifica el número dentro del tipo de elemento.
- Puerto: identifica al número puerto dentro del elemento principal de conexión (switch gestionable de capa 2). Si el elemento no está conectado a algún puerto se usará 00 en la identificación del puerto.
- Lugar: identifica la ubicación del elemento.
- Función: protocolo de transmisión.

Si el elemento se trata de un equipo:

"elemento" "Numero identificativo del tipo de elemento"- "puerto" "lugar"

Si es un elemento de conexión de red:

"elemento" "identificación numérica del elemento" "función"- "puerto" "lugar "

Las referencias de cada uno de los tipos definidos anteriormente pueden ser las siguientes:

ELEMENTO	**ETIQUETA**
Servidor	SV
Switch	SW
Router	RT
Firewall	FW
Telefono	TL
Ordenador	PC
Rack	RK
NAS	NS
LUGAR	**ETIQUETA**
Oficinas	OFI
Comercial	COM
Desarrollo	DES
Centro Datos	CPD
Común	CMN
Piso 2	P2
Piso 1	P1
Piso 0	P0
Piso -1	PS
FUNCIÓN	**ETIQUETA**
Transmisión voz	V
Transmisión datos	D
Transmisión mixta (voz y datos)	M

Tabla 4.2: Referencias

Como ejemplo de caracterización de nombre tenemos “S17V-03COM” que define al switch 17 que transmite voz, conectado a la boca 3 del switch central, y que se sitúa en el departamento comercial.

4.3. Caracterización del cableado del edificio y disposición de los elementos

Para caracterizar el cableado debemos localizar los elementos principales de conexión estos están definidos en Figura 4.2 y Figura 4.3:

- RK02M-00P2: Armario rack situado en Piso 2 dispone del switch central y bocas patch con alcance de toda su planta
- RK01M-00CPD: Armario rack situado en Piso -1, en la sala CPD, contiene todos los equipos del CPD.

- RK03M-00CPD: Armario rack situado en Piso -1, en la sala CPD, contiene el patch con alcance a los pisos -1, 0 y 1 y un switch de la capa de acceso

Una vez localizados los elementos principales, estudiamos el cableado entre plantas y salas. Viene dispuesto como el esquema de Figura 4.2 y Figura 4.3. Todas las conexiones, tanto para el cableado vertical, como el horizontal, como el de área de trabajo, se realizan mediante cable Ethernet de categoría 5e, que soporta Gigabit Ethernet, 1000 Mbps, y hasta 100 metros de distancia del cableado entre repetidores, sin que resulte en una caída significativa de la velocidad de transmisión de datos.

4.3.1. Cableado vertical

El cableado vertical lo conforman los cables troncales del edificio, en este caso serán los que conectan los 3 armarios rack entre sí.

RK02M-00P2 se conecta con RK03M-00CPD mediante cables de longitud inferior a 40 metros que van del switch central, S00M-00P2, a un switch localizado en el segundo armario, S16T-03CPD, también a las bocas patch de dicho armario.

RK02M-00P2 se conecta con RK01M-00CPD a través de cables de longitud inferior a 40 metros que parten de diferentes bocas del switch central a una serie de elementos agrupados en este armario, tal como el firewall, y diversos servidores.

4.3.2. Cableado horizontal

El cableado horizontal está formado por los cables que conectan el área de trabajo, a la red troncal. En este caso está conformado por los cables que, por el interior de las paredes, van desde los paneles patch de los armarios rack a las rosetas de las salas del edificio.

RK02M-00P2 contiene el patch que conectará al switch central los equipos que se conecten a cualquier habitación perteneciente a la planta 2.

RK03M-00CPD contiene el patch que conectará al switch central los equipos que se conecten a cualquier habitación perteneciente a la plantas -1, 0 y 1.

4.3.3. Cableado de área de trabajo

El cableado de área de trabajo está formado por el cableado, o tecnología de conexión inalámbrica, que conecta los equipos de trabajo de cada sala al cableado horizontal. En este caso por todas las conexiones de cada equipo desde las tomas de datos a los terminales.

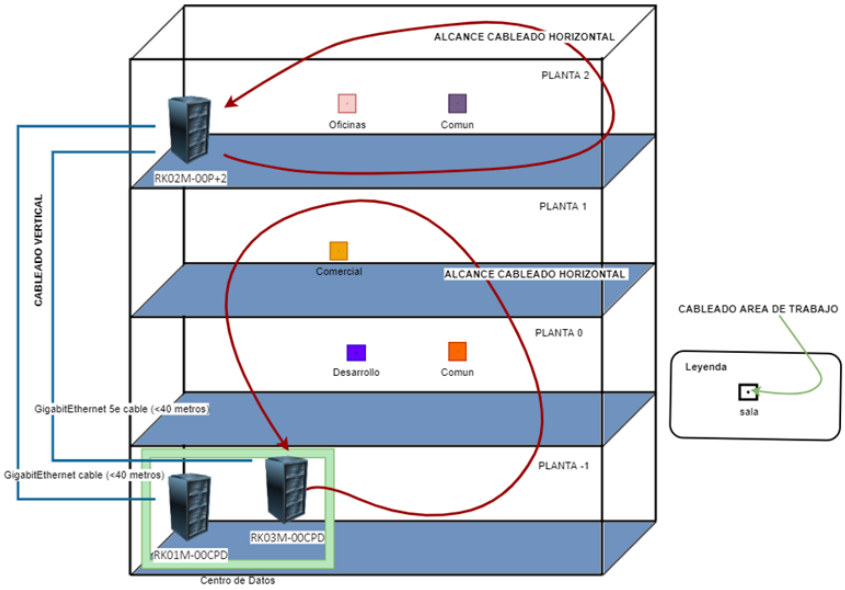


Figura 4.2: arquitectura de la red

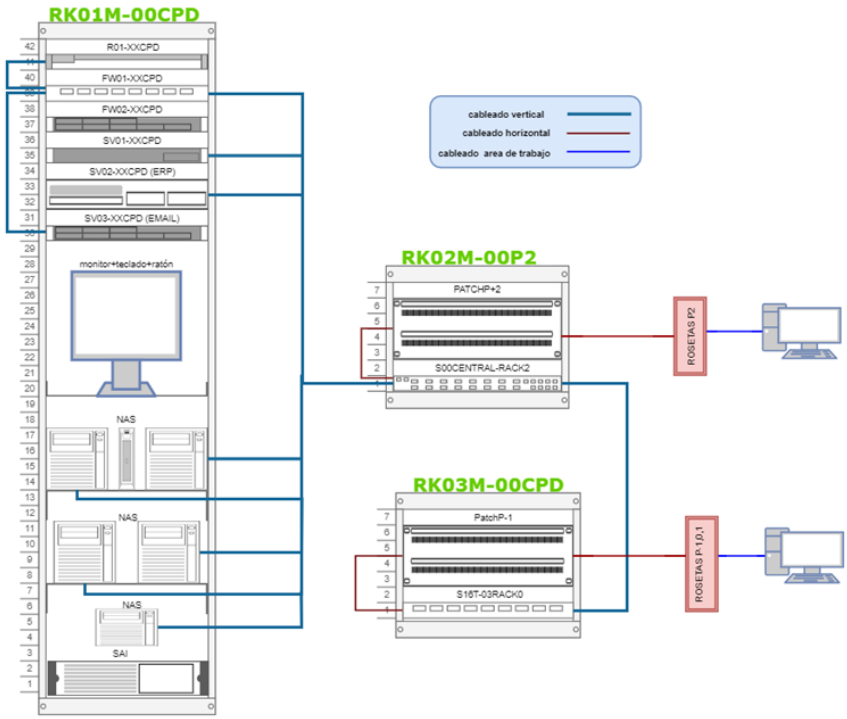


Figura 4.3: Conexiones entre racks

No se prevén problemas de velocidad de conexión por parte del cableado del edificio, dado que se usan cables ethernet de categoría 5e para todas las conexiones en una red con cables de longitud significativamente menor a 100 metros, y no se usa tecnología WIFI.

4.4. Seguridad Física dentro del edificio

Se dispone de control de acceso al edificio mediante alarmas, cámaras, cerraduras tradicionales y magnéticas.

El acceso al Centro de Datos esta cubierto de la misma manera, además se dispone de un potente sistema de seguridad antincendios automático, y de un sistema de enfriamiento de las instalaciones.

Por estos motivos se considera que no es necesaria la mejora ante riesgos físicos ya que la empresa sigue los estándares de seguridad en cuanto al acceso y protección física de la infraestructura.

4.5. Elementos de la red

La red de la empresa consta de aproximadamente 100 equipos conectados a la capa de acceso, en su mayoría teléfonos y ordenadores personales. También se dispone de varios servidores de almacenamiento de datos, PBX y servidor email.

4.5.1. Tablas de elementos principales

Identificación	Tipo	Modelo
S00M-00P2	Switch Central	Netgear GS748T-500EUS
R01M-XXCPD	Router	Arcadyan PRV3399B-B-LT
FW01M-XXCPD	Firewal UTM	HP ProLiant DL120
SV03D-XXCPD	Servidor Email	HP DL140 G3

Tabla 4.3: equipos principales

Componente físico x 1
Producto: Switch Netgear GS748T-500EUS[23, 24]

Fabricante: NEATGEAR
Modelo: GS748T-500EUS
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3az, IEEE 802.3x
Frecuencia: 50/60 Hz
SRAM: 16 MB DDR
Memoria Flash: 2MB
Nº Puertos Gigabit Ethernet: 48
Nº Puertos SFP: 4G
Máximo consumo energético: 41.1 W
Gestión: L2 managed
Métodos de gestión: HTTP, SNMTP

Tabla 4.4: switch GS748T-500EUS

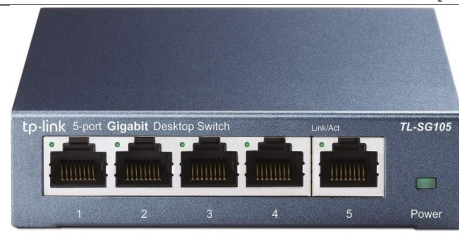
Componente físico x 8
Producto: Switch TP-Link TL-SG105[25]

Fabricante: TP-Link
Modelo: TL-SG105
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1p
Frecuencia 50/60 Hz
Memoria Flash: 1 Mb
Nº Puertos gigabitEthernet: 5
Máximo consumo energético: 3.2 W
Gestión: L2 unmanaged

Tabla 4.5: Switch TP-Link TL-SG105

Componente físico x 2
Producto: TP-Link TL-SG108[25]

Fabricante: TP-Link
Modelo: TL-SG108
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1p
Frecuencia 50/60 Hz
Memoria Flash: 1.5 Mb
Nº Puertos gigabitEthernet: 8
Máximo consumo energético: 3.97 W
Gestión: L2 unmanaged

Tabla 4.6: Switch TP-Link TL-SG108

Componente físico x 2
Producto: Switch YuanLey YS082G-P[26, 27]

Fabricante: YuanLey
Modelo: YS082G-P
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.3x, IEEE 802.3at
Frecuencia: 50 Hz
Nº Puertos UpLink Gigabit Ethernet: 2
Nº Puertos POE Fast Ethernet: 8
Máximo consumo energético: 120 W
Protocolos de gestion: L2 unmanaged

Tabla 4.7: Switch YS082G-P

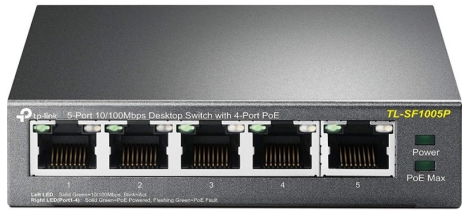
Componente físico x 5
Producto: TP-Link TL-SF1005P[28]

Fabricante: TP-Link
Modelo: TL-SF1005P
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.3x
Frecuencia: 50/60 Hz
Nº Puertos POE Fast Ethernet: 4
Nº Puertos Fast Ethernet: 1
Máximo consumo energético: 63.51W
Protocolos de gestion: L2 unmanaged

Tabla 4.8: Switch TL-SF1005P

Componente físico x 1 (Propiedad del ISP)
Producto: Arcadyan PRV3399B-B-LT[29]

Fabricante: Arcadyan
Modelo: PRV3399B-B-LT
Memoria DDRAM: 256 MB
Memoria FLASH: 128 MB
Frecuencia:50/60 Hz
Nº Puertos SPF: 1
Nº Puertos FXS: 2
Puertos Gigabit Ethernet: 4
Consumo energético: 12.9W
Métodos de gestión: HTTP

Tabla 4.9: Router PRV3399B-B-LT

Componente físico x 1
Producto: HP DL140 G3[30]

Fabricante: HP
Modelo: ProLiant DL140G3
CPU: Quad-Core Intel Xeon processor E5310
RAM: 4 GB
CACHE: 8 MB
HDD: 80 GB
Nº Puertos Gigabit Ethernet: 2

Tabla 4.10: Servidor DL140G3

Componente físico x 1
Producto: I.M.T. integrated, Infodesain (2007)

Fabricante: Infodesain
Modelo: I.M.T. integrated
CPU: VIA C7 Processor 1000MHz
RAM: 1 GB
Cache: 8 MB
SDD: 30 GB
Tarjeta de red:Realtek RTL8119[31]
Nº Puertos Fast Ethernet: 4
Kernel: Linux 2.6.18 i686

Tabla 4.11: IMT infodesain

4.6. Configuración de los elementos principales de la red

4.6.1. Servicios activos del switch central

S00M-00P2 es el elemento central de distribución del trafico dentro de la LAN. Este elemento no solo distribuye el tráfico, sino que aporta una capa de seguridad extra con las siguientes configuraciones:

VLANs del tipo IEEE 802.Q

Permite o deniega el paso del tráfico asignando y desasignando etiquetas VLAN ID. Se dispone de las VLANs de Tabla 4.12:

- VLAN 1: Es la de defecto. Está afiliada a todos los puertos, todos ellos configurados como *Untagged* para esta VLAN, es decir, configurados para ser desprovistos de etiqueta VLAN al abandonar el switch. Se usa como control de tráfico.

- VLAN 2: Están afiliados todos los puertos cuya transmisión sea de VOIP (Teléfonos VoIP y PBX). Todos de tipo Untagged.

- VLAN 10-40: Cada VLAN está afiliada exclusivamente a los puertos que conectan con la sala de su departamento y sus servidores asociados. Todos están afiliados al puerto de conexión con el firewall UTM, NET, así como al ERP. Todos los puertos son Untagged.

- VLAN 50-100: VLANs de servicios internos. Los puertos afiliados serán exclusivamente sus clientes. Todos los puertos son Untagged.

- VLAN 120: Conecta al firewall UTM, ofrece conexión con el servidor de correo e internet.

VLAN ID	VLAN NOMBRE	Puertos (Untagged todos)	
		Etiqueta interna	Afiliados
1	Default	35-48	Todos
2	VOZ	1-9	1-9, 110
10	OFI	10-15	10-15, 27, 28, 34
20	COM	16, 17	16, 17, 27, 29, 34
30	DES	18-20	18-20, 27, 30, 34
40	CMN	21-26	21-27, 31, 32, 34
50	ERP	27	10-27
60	NS1	28	10-15, 28
70	NS2	29	16, 17, 28
80	NS3	30	18-20, 30
90	NS4	31	21-27, 31
100	NS5	32	21-27, 32
110	SV1	33	1-9, 33, 34
120	NET	34	10-34

Tabla 4.12: Vlans en switch central

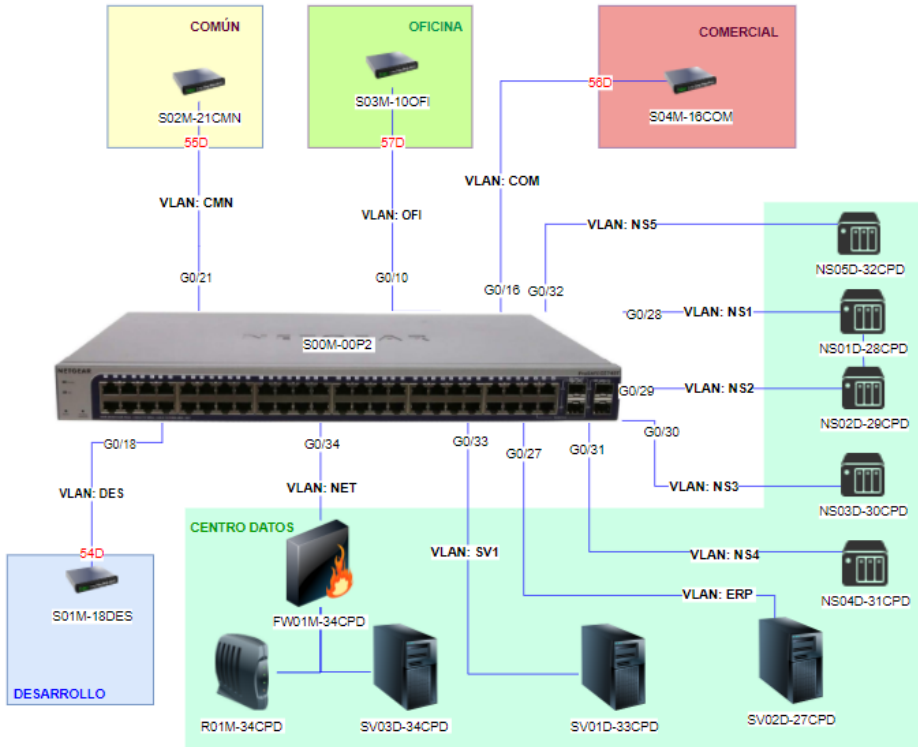


Figura 4.4: Conexiones al switch central

Rate Limits

Configuración de límites de ancho de banda según el puerto, tanto para el tráfico saliente como para el entrante.

Trusted MAC address

Tabla con de direcciones MAC. Sólo redirigirá el tráfico de aquellos equipos cuya MAC esté inscrita en la tabla. Si no hay elementos en la lista redirigirá el trafico de forma independiente a cuál sea la MAC de origen.

IP Access List

Contiene la lista de direcciones IP que pueden acceder a la parte de configuración del switch. Si no hay elementos en la lista permitirá acceder a todas las direcciones IP

4.6.2. Servicios en DMZ

En la DMZ únicamente de dispone de un servidor de correo puesto que será el único servicio que requiere ser accedido por usuarios externos. Los protocolos por los que tendría que ofrecer servicio son: POP3, SMTP, IMAP.

4.6.3. Firewall

El firewall instalado es un I.M.T versión 2.6.18[32]. Es un cortafuegos UTM bajo el SO Linux 2.6.18, que combina e integra múltiples servicios orientados a la seguridad. Todos los servicios integrados son configurables a través de una interfaz web.

A continuación, dividimos los servicios que otorga el sistema firewall en 3 bloques: Servicios que usa el cliente actualmente. Servicios en los que se ha detectado un problema con su funcionamiento. Servicios disponibles en desuso.

Servicios usados

Actualmente los únicos servicios que están siendo usados activamente por el cliente son:

- **IPTables**: Reglas de filtrado y redirección de tráfico en la capa 3. Es el firewall perimetral. Se usan las siguientes tablas dentro de esta:
  - **NAT**: El firewall esta desplegado en Modo Pasarela, es decir, realiza función de IP Forwarding. Se conecta recibiendo todas las peticiones de los equipos de la red, las procesa y las envía por la interfaz interna, externa o DMZ.

- **Filtrado**: Lista de control de acceso a la red por IP, puerto y protocolo. La lista esta configurada en modo secuencial, es de decir, la prioridad de las reglas esta regulado por su orden de aparición en sentido descendiente.

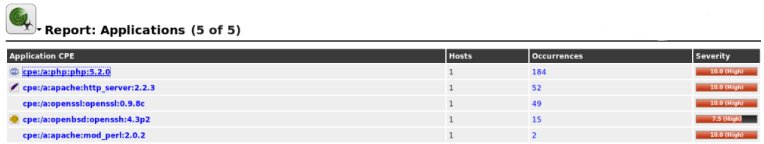


Figura 4.5: Filtrado mediante ACL

- **Servidor DHCP**: asigna direcciones IP, así como la puerta de enlace y los servidores DNS automáticamente a las máquinas en la red local.
- **Servidor DNS**: proporciona la posibilidad de definir dominios internos con sus correspondientes subdominios según las necesidades de la red. Dominio de email definido.
- **Protocolo de enrutamiento RIP**.

El equipo además de los servicios de firewall mencionados en la seccion anterior consta de los siguientes servicios modulares que fueron contratados por la empresa:

Servicio	Funcionalidad	Funcional
Chivato web	Recopilar y mostrar información de los sitios web accedidos por usuarios de la red interna	NO
ntop	Recopilar y mostrar información referente al uso de la red interna	SI
IDS	Detección de intrusos	NO
Gestor PKI	Generar certificados	SI
Cacti RRDTool	Generar gráficos referentes al tráfico de red	NO
Control Web	Controlar el acceso web de los usuarios	NO
WOL	Encender equipo en remoto	NO
Auditor Seguridad	Escaneo de vulnerabilidades de seguridad	NO

4.6.4. Vulnerabilidades en el sistema

Para analizar que riesgos ocasiona el sistema UTM firewall actualmente instalado, se realiza un escaneo de vulnerabilidades desde la red interna contra este, con el objeto de conocer a que fallos de seguridad está expuesta la red. La herramienta utilizada para realizar este escaneo es OpenVAS. A partir de una configuración dada devolverá como resultado un informe con las vulnerabilidades, cómo se detectaron, su severidad, etc.

Las métricas a utilizar en este análisis son:

- Severidad: Valor entre 0.0 y 10.0 que viene dado por el *CVSS Base Score Calculator*[36]. Siendo 10.0 la máxima severidad, este valor viene definido por:

- Vector de Acceso (AV): Cómo es explotada la vulnerabilidad. A más remoto pueda estar un atacante del host, mayor será la puntuación de la vulnerabilidad para este aspecto. Puede ser:
  - Local (L): Requiere acceso físico al sistema o desde una cuenta local por parte del atacante.
  - Adyacente a la red (A): Requiere acceso a la red local.
  - Red externa(N): Se puede realizar desde una red externa.
- Complejidad de Acceso (AC): complejidad del ataque para explotar la vulnerabilidad una vez que el atacante ha ganada acceso al sistema. A menor complejidad mayor será la puntuación. Se clasifican en:
  - Alto (H): Existencia de condiciones muy específicas.
  - Medio (M): Existencia de condiciones comunes pero especificas.
  - Bajo (L): No se necesitan condiciones especificas para llevar a cabo el ataque, por ejemplo en sistema con configuración por defecto.
- Autenticación (Au): Veces que el atacante debe autenticarse para explotar la vulnerabilidad. A menores veces mayor será la puntuación. Se clasifican en:
  - Múltiple (M): Requiere 2 o mas autenticaciones
  - Única (S): Requiere 1 autenticación.
  - No Requerida (N): No requiere autenticación.
- Impacto en la Confidencialidad (C): Cantidad de información no autorizada a la que tiene acceso el atacante tras explotar la vulnerabilidad. A mayor acceso mayor será la puntuación. Se clasifica en:
  - Ninguna (N): No tiene acceso a información.
  - Parcial (P): Tiene acceso a información parcial.
  - Completa (C): Tiene acceso a toda la información del sistema.
- Integridad (I): Cantidad de información que puede ser modificada por el atacante. A mayor cantidad mayor será la puntuación. Se clasifica en:
  - Ninguna (N): No afecta a la integridad de la información.
  - Parcial (P): Parte del sistema es susceptible a modificación de información.
  - Completa (C): Toda la información del sistema está comprometida.
- Disponibilidad (A): Impacto en la disponibilidad del sistema si la vulnerabilidad es explotada. A menor disponibilidad mayor será la puntuación. Se clasifica en:
  - Ninguna (N): No impacta a la disponibilidad del sistema.
  - Parcial (P): Puede haber interrupciones en la disponibilidad de los recursos del sistema.
  - Completa (C): Puede hacer que el sistema no este disponible por completo.

- QoD (Calidad de Detección): valor entre 0 % y 100 % que indica la fiabilidad de la detección de la vulnerabilidad. Siendo 100 % detectada vía exploit y por lo tanto completamente verificada.[37] Para los escáneres realizados se recogerán vulnerabilidades del rango estándar de QoD, entre 100 %-70 %.

Se han realizado 2 tipos de escáneo con OpenVas:

- CVE[35]: permite pronosticar posibles riesgos de seguridad basados en información publicada por proveedores e investigadores de seguridad en la base de datos de CVE. Este tipo de escáner no debe usarse para evaluar si existe o no una vulnerabilidad real, sino que debe usarse para brindar al usuario final una idea de las vulnerabilidades potenciales debido a que los resultados corresponden a las vulnerabilidades individuales del sistema. No toma el conjunto del sistema en consideración, simplemente devuelve todas las coincidencias con la base de datos CVE. Por ello se devolverán muchos falsos positivos.

- OpenVAS Default: Hace un escaneo del sistema en su conjunto para obtener las vulnerabilidades del sistema. Para extraer las vulnerabilidades aplica test de NVT. En los resultados se mostrará el test NVT aplicado, el QoD, y la severidad de cada vulnerabilidad.

Resultados escaneo CVE

Para las vulnerabilidades unitarias, se puede observar que se han detectado 303 vulnerabilidades en el sistema, siendo un 27 % de ellos vulneralidades con una severidad alta, que ponen el sistema gran riesgo.

Las puntuaciones las vulnerabilidades vienen dadas por:

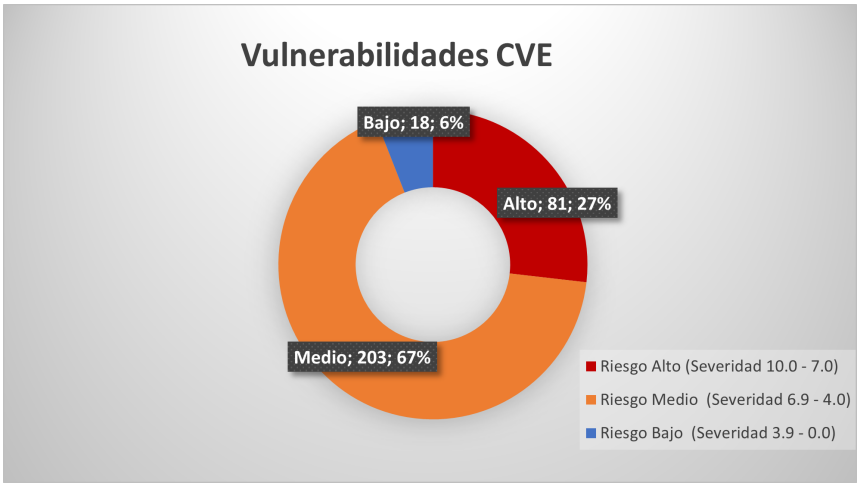


Figura 4.6: Vulnerabilidades CVE - infodesain

En la clasificación por tipo observada en la Figura 4.7 se puede ver que de las 5 aplicaciones detectadas por OpenVAS 4 tienen posibles puntos de explotación de vulnerabilidades con severidad 10.0, que indica la posibilidad de completa toma de control del sistema por parte de un atacante.

Report: Applications (5 of 5)

Application CPE	Hosts	Occurrences	Severity
cpe:/a:php:php:5.2.0	1	184	10.0 (High)
cpe:/a:apache:http_server:2.2.3	1	52	10.0 (High)
cpe:/a:openssl:openssl:0.9.8c	1	49	10.0 (High)
cpe:/a:openbsd:openssh:4.3p2	1	15	7.5 (High)
cpe:/a:apache:mod_perl:2.0.2	1	2	10.0 (High)

Figura 4.7: Vulnerabilidades CVE por tipo - infodesain

Resultados escaneo OpenVAS Default

El número de vulnerabilidades detectadas en función al sistema completo es significativamente menor que el de las unitarias. Se ha reducido considerablemente las vulnerabilidades que aportan un gran riesgo. 2 frente a 83, tal y como se puede observar en las figuras 4.8 y 4.6 respectivamente.

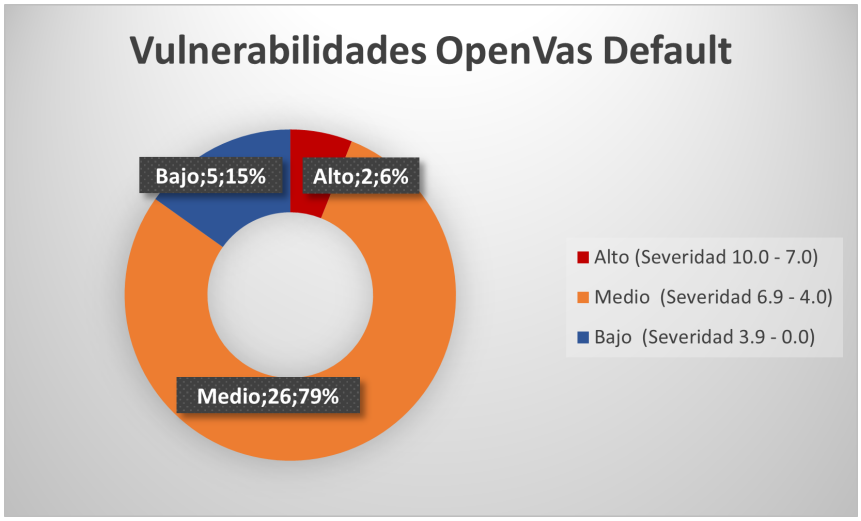


Figura 4.8: Vulnerabilidades test OpenVas Default - infodesain

La Tabla 4.13 compone un resumen de las diferentes vulnerabilidades detectadas durante el análisis:

Vulnerabilidad	Severidad	QoD	Localización
Apache httpd Web Server Range Header Denial of Service Vulnerability	7.8	100 %	8000/tcp 443/tcp
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8	70 %	443/tcp
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8	99 %	8000/tcp 443/tcp 3128/tcp
Tildeslash Monit <5.25.3 Multiple Vulnerabilities	5.5	80 %	2812/tcp
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0	98 %	443/tcp
SSL/TLS: Certificate Expired	5.0	99 %	443/tcp 1241/tcp
Cleartext Transmission of Sensitive Information via HTTP	4.8	80 %	2812/tcp
FTP Unencrypted Cleartext Login	4.8	70 %	21/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	98 %	443/tcp
SSL/TLS: Report Weak Cipher Suites	4.3	98 %	1241/tcp 443/tcp
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3	80 %	443/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3	80 %	443/tcp
Apache Web Server ETag Header Information Disclosure Weakness	4.3	80 %	443/tcp 8000/tcp
SSH Weak Encryption Algorithms Supported	4.3	95 %	22/tcp
Mod_Perl Path_Info Remote Denial Of Service Vulnerability	4.3	80 %	443/tcp 8000/tcp
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	4.3	80 %	443/tcp
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3	99 %	443/tcp 8000/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.3	80 %	443/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0	80 %	1241/tcp 443/tcp
TCP timestamps	2.6	80 %	general/tcp
Apache mod_perl 'Apache::Status' and 'Apache2::Status' Cross Site Scripting Vulnerability	2.6	80 %	443/tcp 8000/tcp
SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)	2.6	98 %	443/tcp
SSH Weak MAC Algorithms Supported	2.6	90 %	22/tcp

Tabla 4.13: Lista de vulnerabilidades encontradas

Observando la Tabla 4.13 destacan las 2 vulnerabilidades de severidad alta se corresponden con vulnerabilidad de denegación de servicio para los puertos 443 y 8000. El riesgo de que se explote esta vulnerabilidad es alto debido que tiene un QoD de 100 %. Además como tiene una puntuación de severidad alta es fácil de explotar. Como se puede observar en la Figura 4.9, tiene una severidad de 7.8. Esta nota vienen dada por las condiciones para su explotación. Se indica que la vulnerabilidad se puede explotar desde una red externa, tiene una complejidad de acceso baja, no requiere autenticación, no impacta a la confidencialidad ni a la integridad de la información pero si a la disponibilidad ya que puede hacer que el sistema no esté disponible por completo.

La causa de estas vulnerabilidades viene dada por el hecho de usar una versión de Apache obsoleta.

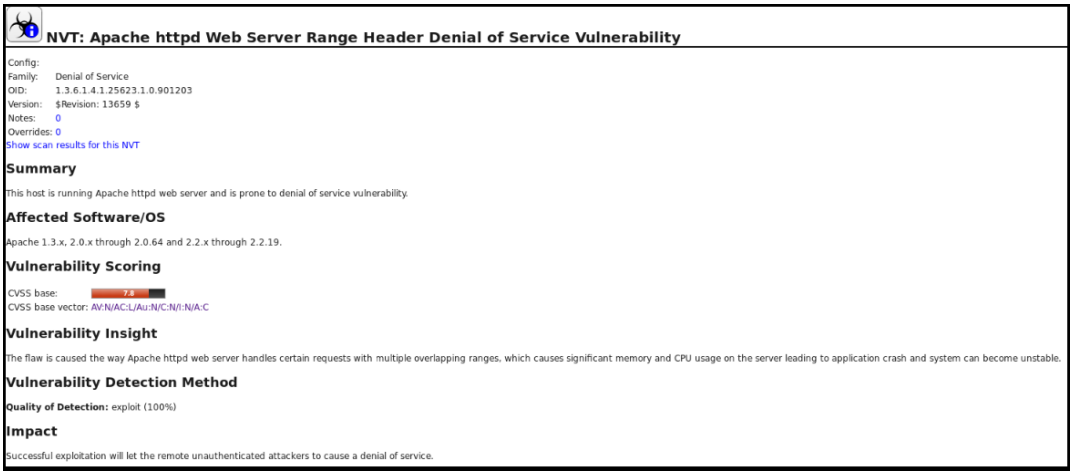


Figura 4.9: Vulnerabilidades en puerto 443 y 8000 - infodesain

En cuanto a las vulnerabilidades de severidad media, que se corresponden, en la Tabla 4.13, a las vulnerabilidades con severidad dentro del rango 6.8-4.0, se observa que la gran mayoría corresponde a encriptaciones débiles y servicios obsoletos. Estas vulnerabilidades también vienen dadas por el uso de servicios y hardware obsoleto.

En el caso de las vulnerabilidades de severidad baja ocurre exactamente lo mismo que para las de severidad alto y medio, existen por el hecho de usar hardware y servicios obsoletos.

Los informes obtenidos dejan claro que este equipo es muy vulnerable y se ha de reemplazar de inmediato.

Confidencialidad

Antes de realizar ningún análisis, se hizo un escaneo de puertos, donde se detectó que el puerto 3000, un puerto que no se está usando por parte de los empleados de la empresa, esta abierto.

Accediendo desde el exterior se observa que a lo que se accede es a la interfaz web del programa ntop. Todos los datos de la red de la empresa se encuentran disponibles desde ese puerto.

Se ha podido acceder a esos datos desde una red externa, y sin ningún tipo de autenticación, simplemente escribiendo en el navegador la dirección de acceso.

Se considera que esta configuración causa una gran brecha en la confidencialidad de la red de la empresa.

4.7. Características de la red actual

A continuación, se resume la funcionalidad que cumple la red con la configuración actual:

Nº	Descripción
1	La red permite conexión entre usuarios afiliados a una misma VLAN.
2	Se permite todo tipo de conexiones de la red interna a la externa.
3	La red dispone de DMZ con un servidor email.
4	La red permite conexión de usuarios internos al servidor de email disponible en la DMZ.
5	La red permite conexión de usuarios externos al servidor de email disponible en la DMZ.
6	La red permite escalabilidad de equipos.
7	El MTBF de disponibilidad de la red es de 3000 horas aproximadamente, es decir, cada 4 meses se produce un fallo en la infraestructura de red que no permite realizar las funciones habituales a alguno de los equipos.
8	El ancho de banda esta limitado a 100 MBPS para la totalidad de la red.

Tabla 4.14: funciones actuales de la red

4.7.1. Grupos de usuarios actuales

Se distinguen 3 tipos de usuarios en el uso de la red:

- Usuario externo: usuario con acceso restringido al servidor de email ubicado en la DMZ. Se conectan a la red mediante IP pública.
- Usuario interno limitado: usuario de la red interna con acceso a todos los servicios de su departamento.
- Usuario Administrador: Usuario interno con acceso a toda la red, puede monitorizar la red y cambiar las configuraciones de esta.

4.8. Evaluación del análisis de la red

En esta sección se va a resumir las conclusiones a las que se ha llegado a partir de los resultados obtenidos por el estudio de la red.

Para ajustarse a los requerimientos de seguridad actuales se debe cambiar el sistema firewall instalado actualmente por uno que funcione adecuadamente, aumente la seguridad actual de la infraestructura, cumpla los estándares de seguridad, y ofrezca los servicios que el cliente quiere explotar.

A continuación se resume en una lista los motivos por los cuales se ha llegado a esta conclusión a partir del estudio del equipo:

- Hardware anticuado: Dispositivo cuello de botella no solo por su localización sino también debido a que las tarjetas de red no soportan más de 100 MBps, impidiendo aprovechar todo el ancho de banda proporcionado por el ISP.
- Servicios obsoletos: El equipo lleva sin actualizarse mas de 10 años. Todos los módulos de seguridad y servicios son versiones pertenecientes a los años 2005-2007, lo que suponen un gran riesgo para la seguridad de la red debido a las vulnerabilidades de estos encontradas a lo largo de los años.
- Configuración no óptima: Se han detectado módulos que directamente comprometen la información de la red empresarial entre otras.
- Falta de servicios: Algunos de los servicios requeridos por el cliente no funcionan adecuadamente.
- Producto descontinuado: El fabricante dejo de dar soporte al producto hace años, no se dispone de mantenimiento, la empresa cambio de nombre, también se abandonó el soporte de la página web del producto, apenas hay documentación e información sobre el sistema.

Se recomienda duplicar los elementos troncales de la red para aportar redundancia eliminando así puntos únicos de falla.

4.9. Requisitos

A partir del estudio de la red podemos desglosar los objetivos del cliente en los siguientes requisitos que debe cumplir la red al rediseñarla introduciendo el nuevo sistema:

Nº	Descripción del requisito
1	Los requisitos deben ser gestionados por un único sistema firewall.
2	Se permitirá todo tipo de conexiones de la red interna a la externa para los usuarios no limitados
3	La red dispondrá de DMZ con un servidor email.
4	La red permitirá conexión de usuarios internos al servidor de email disponible en la DMZ.
5	La red permitirá conexión de usuarios externos al servidor de email disponible en la DMZ.
6	Se limitarán los servicios de la red externa a los que pueden acceder los usuarios internos limitados
7	Se limitará el ancho de banda usado por determinados usuarios
8	Se permitirá el acceso a algunos recursos de la red interna de forma segura, desde una red externa, a través de VPN.
9	Los datos de los usuarios internos deberán estar protegidos ante intrusos.
10	La red permitirá conexión entre usuarios afiliados a una misma VLAN.
11	La red permitirá escalabilidad de equipos.
10	El MTBF de disponibilidad de la red deberá ser superior a 4000 horas.
11	Se dispondrá de herramientas de monitorización de la red accesibles por los administradores de forma segura.
12	El administrador de la red podrá realizar cambios sobre las configuraciones de la red, y por lo tanto del sistema.
13	Los accesos del administrador al sistema firewall deberán realizarse mediante protocolos que garanticen el acceso seguro.

Tabla 4.15: Requisitos

4.10. Grupos de usuarios

Se distinguen los siguientes tipos de usuarios en la configuración que se debe implantar:

- Usuario externo: usuario con acceso restringido al servidor de email ubicado en la DMZ. Pertenecen a la red externa, se conectan a la red mediante ip pública.
- Usuario interno limitado: usuario de la red interna con acceso a todos los servicios de su departamento, pero con acceso limitado a servicios proporcionados por la red.
- Usuario interno: usuario de la red interna con acceso a todos los servicios de su departamento.
- Usuario invitado: usuario de la red interna que no forma parte de la estructura de red habitual de la empresa. Tiene acceso limitado a servicios proporcionados por la red
- Usuario VPN: usuario que se conecta desde el exterior mediante VPN y tendrá los permisos de su usuario interno homólogo. Se conectan a la red mediante IP pública.
- Usuario Administrador: Usuario interno con acceso a toda la red, puede monitorizar la red y cambiar las configuraciones de esta.

4.11. Casos de Uso

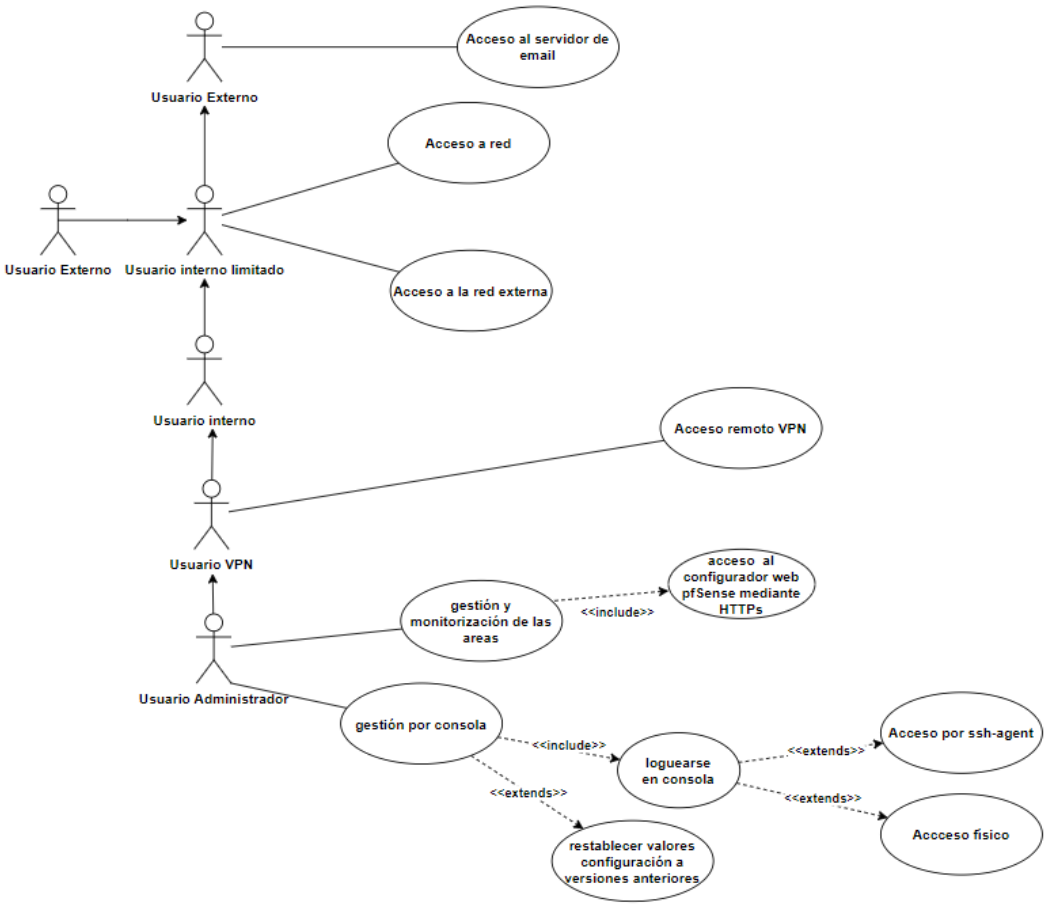


Figura 4.10: Diagrama de casos de uso

Figura 4.11: Diagrama de casos de uso, detalle gestión y monitorización de las áreas

UC1	Acceso a la red
Req Asociado	2,4
Actores	usuario interno limitado, interno, administrador, invitado, VPN.
Descripción	El usuario se conecta a la intranet
Precondición	El usuario se conecta físicamente a la LAN o tiene una conexión VPN
Secuencia	1- El usuario solicita una dirección IP 2- El sistema le manda una dirección IP a asignar. 3- El usuario tiene acceso a intranet
Postcondición	El usuario dispone de dirección IP de subred LAN
Excepciones	3a - El sistema deniega la petición, el caso de uso queda sin efecto.

Tabla 4.16: Descripción del caso de uso: Acceso a la red

UC2	Acceso a la red externa
Req Asociado	2, 6
Actores	usuario interno limitado, interno, administrador, invitado
Descripción	El usuario se conecta a la externa
Precondición	Se ha realizado el CU acceso de red
Secuencia	1- El usuario solicita acceso a un servicio de la red externa. 2- El sistema comprueba que el usuario tienen permisos para realizar esa petición. 3- El sistema envía la respuesta del sistema externo al usuario.
Postcondición	El usuario ha recibido el recurso
Excepciones	2a - El sistema comprueba que el usuario no tiene permisos para realizar esa petición y le manda un mensaje de aviso, el caso de uso queda sin efecto.

Tabla 4.17: Descripción del caso de uso: Acceso a la red externa

UC3	Acceso al servidor de email
Req Asociado	4,5
Actores	Todos
Descripción	El usuario establece conexión el servidor email
Precondición	Que no tenga ningún bloqueo para el acceso
Secuencia	1- El usuario solicita acceso al servidor email de la DMZ. 2- El sistema comprueba que el usuario tienen permisos para realizar esa petición. 3- El sistema envia la respuesta del servidor al usuario.
Postcondición	El usuario ha recibido el recurso.
Excepciones	3a - El sistema no recibe respuesta antes del timeout, el caso de uso queda sin efecto.

Tabla 4.18: Descripción del caso de uso: Acceso al servidor de email

UC4	Acceso remoto VPN
Req Asociado	8
Actores	usuario VPN
Descripción	El usuario accede desde el exterior a recursos de la red interna.
Precondición	El usuario esta la red externa. Se ha realizado el CU Registrar conexiones VPN para el usuario.
Secuencia	1- El usuario solicita conexión VPN al sistema. 2- El sistema comprueba la identidad del usuario y acepta. 3- El usuario accede a los recursos internos como si estuviera conectado desde la LAN.
Postcondición	El usuario ha accedido al recurso de la red interna.
Excepciones	2a - El sistema no reconoce al usuario y deniega la petición, el caso de uso queda sin efecto.

Tabla 4.19: Descripción del caso de uso: Acceso remoto VPN

UC5	Acceso por ssh-agent
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario accede al sistema por consola.
Precondición	Se ha realizado el CU crear usuarios y acceso de red.
Secuencia	1- El usuario solicita conexión SSH. 2- El sistema autentifica al usuario, cifra la conexión y solicita la contraseña 3- El usuario introduce la contraseña. 4- El sistema provee acceso al usuario.
Postcondición	El usuario dispone de permisos para modificar la configuración del sistema.
Excepciones	1a - El usuario no reconoce al sistema, el caso de uso queda sin efecto. 2a - El sistema no reconoce al usuario y deniega la petición, el caso de uso queda sin efecto. 3a - El usuario cancela, el caso de queda sin efecto. 3b - El usuario ha introducido la contraseña incorrecta demasiadas veces, el sistema bloquea el intento de conexiones para el usuario durante un tiempo que aumenta exponencialmente en función del número de intentos. El caso de uso queda sin efecto.

Tabla 4.20: Descripción del caso de uso: Acceso por ssh-agent

UC6	Acceso físico
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario accede a la configuración por consola del sistema.
Precondición	El usuario se conecta físicamente al sistema.
Secuencia	1- El usuario conecta su equipo con el sistema. 2- El sistema pide credenciales de acceso. 3- El usuario introduce las credenciales de usuario. 4- El sistema muestra las opciones de configuración al usuario.
Postcondición	El usuario dispone de permisos para modificar la configuración del sistema.
Excepciones	3a- El sistema no reconoce al usuario y deniega la petición, el caso de uso queda sin efecto.

Tabla 4.21: Descripción del caso de uso: Acceso físico

UC7	Loguearse en consola
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario accede a la configuración por consola del sistema.
Precondición	El usuario dispone de rol de administrador.
Secuencia	1- El usuario establece conexión con el sistema. 2- El sistema pide credenciales de acceso. 3- El usuario introduce las credenciales de usuario. (Extensión CU5 o Extensión CU6) 4- El sistema muestra las opciones de configuración al usuario.
Postcondición	El usuario dispone de permisos para modificar la configuración del sistema.
Excepciones	3a- El sistema no reconoce al usuario y deniega la petición, el caso de uso queda sin efecto.

Tabla 4.22: Descripción del caso de uso: Loguearse en consola

UC8	Gestión por consola
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario realiza cambios de configuración desde la terminal.
Precondición	El usuario ha realizado el login CU en consola
Secuencia	1- El usuario accede a una de las opciones de configuración (Extensión CU9) 2- El sistema concede el permiso de acceso 3- El usuario realiza los cambios. 4- El sistema comprueba, guarda y aplica los cambios realizados.
Postcondición	El usuario ha cambiado la configuración del sistema.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.23: Descripción del caso de uso: Loguearse en consola

UC9	Restablecer valores configuración a versiones anteriores
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario restablece la configuración a una versión anterior
Precondición	El usuario ha realizado el CU loguearse en consola
Secuencia	1- El usuario selecciona la opción de restablecer configuración anterior. 2- El sistema muestras las configuraciones anteriores 3- El usuario selecciona la versión a restablecer 4- El sistema comprueba, guarda y aplica los cambios realizados.
Postcondición	El usuario ha cambiado la configuración del sistema.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto.

Tabla 4.24: Descripción del caso de uso: Restablecer valores configuración a versiones anteriores

UC10	Acceso al configurador web mediante HTTPs
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario accede al sistema por interfaz gráfica.
Precondición	Se ha realizado el CU crear usuarios y acceso a red
Secuencia	1- El usuario solicita conexión HTTPs 2- El sistema autentifica al usuario, cifra la conexion y solicita credenciales 3- El usuario introduce las credenciales. 4- El sistema muestra la página principal del configurador.
Postcondición	El usuario se ha logueado en el configurador web del sistema.
Excepciones	1a- El usuario no reconoce al sistema, el caso de uso queda sin efecto. 2a- El sistema no reconoce al usuario y deniega la petición, el caso de uso queda sin efecto. 3a- El usuario cancela, el caso de queda sin efecto. 3b- El usuario ha introducido las credenciales incorrectas demasiadas veces, el sistema bloquea el intento de conexiones para el usuario durante un tiempo que aumenta exponencialmente en función del número de intentos. El caso de uso queda sin efecto.

Tabla 4.25: Descripción del caso de uso: Acceso al configurador web mediante HTTPs

UC11	Gestión/monitorización de las áreas
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario gestiona/monitoriza el sistema.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs y acceso a red
Secuencia	1- El usuario accede a una de las áreas de configuración. (Extensión 12-24) 2- El sistema muestra el área 3- El usuario gestiona/monitoriza el sistema. 4- El sistema lleva a cabo la acción realizada.
Postcondición	El usuario obtiene postcondición de alguno de los casos extensión 12-24
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce la acción como incorrecta. Continúa en paso 3.

Tabla 4.26: Descripción del caso de uso: Gestión/monitorización de las áreas

UC12	Crear backup de configuración
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario obtiene el archivo de la configuración actual
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs y acceso de red
Secuencia	1- El usuario accede al área de backup. 2- El sistema muestra el área. 3- El usuario solicita la descarga del archivo de configuración del sistema. 4- El sistema genera el archivo de configuración.
Postcondición	El usuario dispone del archivo de configuración del sistema.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto.

Tabla 4.27: Descripción del caso de uso: Crear backup de configuración

UC13	Gestionar permisos de conexión entre interfaces
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario modifica los permisos de acceso entre usuarios de las interfaces.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs y acceso de red
Secuencia	1- El usuario accede al área de firewall. 2- El sistema muestra el área. 3- El usuario modifica las reglas de firewall para la interfaz. 4- El sistema comprueba, guarda y aplica los cambios realizados
Postcondición	Los permisos de acceso entre interfaces han cambiado.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.28: Descripción del caso de uso: Gestionar permisos de conexión entre interfaces

UC14	Wake on Lan
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario enciende uno de los equipos conectados a la LAN.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, Registrar conexiones de equipos y acceso de red.
Secuencia	1- El usuario accede al área de WOL. 2- El sistema muestra el área. 3- El usuario selecciona el equipo a despertar. 4- El sistema enciende el equipo.
Postcondición	El equipo ha sido encendido.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.29: Descripción del caso de uso: Wake on Lan

UC15	Registrar conexiones de equipo
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario configura DHCP estático para un equipo.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, Registrar conexiones de equipos y acceso de red.
Secuencia	1- El usuario accede al área de DHCP de la interfaz 2- El sistema muestra el área. 3- El usuario rellena los datos de direccion IP, mac, host... 4- El sistema registra el mapeo estático DHCP.
Postcondición	El equipo recibe la dirección IP configurada.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.30: Descripción del caso de uso: Registrar conexiones de equipo

UC16	Registrar conexiones VPN
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario configura un nuevo cliente VPN
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, Registrar conexiones de equipos, acceso de red y crear usuarios
Secuencia	1- El usuario accede al área de configuración VPN 2- El sistema muestra el área. 3- El usuario rellena los datos de conexión del cliente. 4- El sistema registra al nuevo acceso VPN
Postcondición	Hay un nuevo cliente VPN con privilegios de acceso a la red mediante VPN
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.31: Descripción del caso de uso: Registrar conexiones VPN

UC17	Monitorizar el tráfico de red
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario monitoriza el tráfico de red
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, el acceso de red
Secuencia	1- El usuario accede al area del log de tráfico de red 2- El sistema muestra el área. 3- El usuario visualiza los logs de tráfico de red
Postcondición	El usuario visualiza los datos
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto.

Tabla 4.32: Descripción del caso de uso: Crear usuarios

UC18	Crear usuarios
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario monitoriza el tráfico de red
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, y acceso de red
Secuencia	1- El usuario accede al área de gestión de usuarios. 2- El sistema muestra el área. 3- El usuario crea un nuevo usuario, asignandole los permisos correspondientes. 4- El sistema guarda los cambios de usuario.
Postcondición	El usuario visualiza los datos
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.
Alternativas	Si el usuario ya existe en el sistema: 1- El usuario accede al area de gestión de usuarios. 2- El sistema muestra el área. 3- El usuario selecciona el usuario del sistema a modificar. 4- El sistema muestras las opciones a editar. 5- El usuario edita la configuración del usuario de sistema. 6- El sistema guarda los cambios de usuario.
Excepciones	3b, 5b- El usuario cancela la operación, el caso de uso queda sin efecto. 6b- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 4.

Tabla 4.33: Descripción del caso de uso: Crear usuarios

UC19	Gestionar permisos de los usuarios de la intranet a recursos web
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario cambia los permisos de acceso a determinados recursos web de la red externa
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, acceso de red, y crear usuarios
Secuencia	1- El usuario accede al área de gestión del proxy web 2- El sistema muestra el área. 3- El usuario modifica las listas de acceso para el usuario. 4- El sistema guarda las nuevas normas de acceso para el usuario.
Postcondición	Los permisos de acceso cambiaron para el usuario configurado.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.34: Descripción del caso de uso: Gestionar permisos de los usuarios de la intranet a recursos web

UC20	Cambiar el ancho de banda percibido por usuario
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario cambia el ancho de banda percibido por un usuario del sistema
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, acceso de red, y crear usuario
Secuencia	1- El usuario accede al área de gestión de gestión de ancho de banda 2- El sistema muestra el área. 3- El usuario modifica el ancho de banda percibido por el usuario del sistema 4- El sistema guarda la nueva configuración de repartición de ancho de banda.
Postcondición	El ancho de banda cambió para el usuario configurado.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.35: Descripción del caso de uso: Cambiar el ancho de banda percibido por usuario

UC21	Bloquear tráfico en función listas IP, pais
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario cambia los permisos de comunicación con sistemas externos.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, y acceso de red
Secuencia	1- El usuario accede al área de gestión de listas de bloqueo. 2- El sistema muestra el área. 3- El usuario activa las listas negras que desea aplicar 4- El sistema guarda los cambios de configuración
Postcondición	Los permisos de acceso a recursos de terceros o desde terceros han cambiado
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.36: Descripción del caso de uso: Bloquear tráfico en función listas IP, país

UC22	Cambiar elementos a almacenar en caché por el sistema
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario cambia la configuración de los elementos que guarda en disco el sistema para su posterior acceso por parte de los usuarios.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, y acceso de red
Secuencia	1- El usuario accede al área de gestión del proxy web 2- El sistema muestra el área. 3- El usuario cambia las reglas de almacenamiento de elementos. 4- El sistema guarda los cambios de configuración
Postcondición	Los usuarios descargarán recursos nuevos desde el sistema o desde un sistema externo en función a la nueva configuración.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema reconoce los cambios como incorrectos, vuelve a pedir un nuevo valor de configuración. Continúa en paso 3.

Tabla 4.37: Descripción del caso de uso: Cambiar elementos a almacenar en caché por el sistema

UC23	Monitorización por capa de aplicación
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario monitoriza el tráfico de capa de aplicación y realiza cambios pertinentes en función a este.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, y acceso de red
Secuencia	1- El usuario accede al área de gestión del IDS 2- El sistema muestra el área. 3- El usuario monitoriza la actividad de los usuarios.
Postcondición	El usuario visualiza los datos de actividad de los usuarios.
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto.

Tabla 4.38: Descripción del caso de uso: Monitorización por capa de aplicación

UC24	Actualizar áreas del sistema
Req Asociado	12
Actores	usuario administrador
Descripción	El usuario actualiza las áreas de configuración del sistema.
Precondición	Se ha realizado el CU acceso al configurador web mediante HTTPs, y acceso de red
Secuencia	1- El usuario accede al área de gestión de paquetes del sistema. 2- El sistema muestra el área. 3- El usuario seleciona las areas que desea actualizar. 4- El sistema actualiza las áreas.
Postcondición	El sistema se ha actualizado
Excepciones	3a- El usuario cancela la operación, el caso de uso queda sin efecto. 4a- El sistema no puede actulizar correctamente el área, el caso de uso queda sim efecto.

Tabla 4.39: Descripción del caso de uso: Actualizar áreas del sistema

Capítulo 5

Diseño de la Solución

5.1. Introducción

En este capítulo se va a diseñar la solución que permita cumplir con los requisitos del proyecto. El diseño de la solución a diseñar depende fuertemente del sistema a instalar y configurar, por ello, tras haber realizado el análisis es imperativo elegir el sistema a instalar. Una vez dotados del sistema a configurar que permita el acoplamiento de todas los requisitos que conformen la red segura se diseña la solución por cara requerimiento.

5.2. Elección de la UTM

En la sección 2.8 se realizó una comparativa entre los diferentes candidatos a implantar como sistema solución. Se ha elegido pfSense. Los motivos de la decisión son los siguientes:

- **Actualizaciones frecuentes**: Tiene actualizaciones frecuentes del sistema y sus componentes. Semanales o mensuales. Únicamente OPNsense esta a la par con pfSense en este sentido. El resto de firewalls estudiados no hay tenido actualizaciones en meses. Este punto es crucial para el mantenimiento del sistema.
- **Soporta software de terceros** por lo que el abanico de opciones se amplia extensamente.
- **Comunidad**: De los sistemas estudiados el que consta de una comunidad mayor y más activa puesto que pfSense lleva años afianzado en el sector y su popularidad no decae debido a sus estabilidad, frecuentes actualizaciones y soporte de software de terceros.
- **Documentación**: pfSense dispone de documentación oficial muy cuidada, extensa y actualizada además de la ya proporcionada por su comunidad.

- **SO FreeBSD**: Se considera la instalación de un sistema basado en FreeBSD una mejor opción frente a uno basado en Linux. FreeBSD es más seguro y robusto.
- **Filtrado mediante Packet Filter**:Debido a su dependencia con SO FreeBSD.
- Se puede usar como IDS tanto **Snort** como Suricata.
- **OpenVPN**: además de ser la mejor opción del mercado actualmente, pfSense cuenta con un wizard de configuración de OpenVPN.
- Su **interfaz** de configuración y gestión es *friendly*.
- Integra todos los componentes necesarios y preferibles para la configuración del equipo en el entorno del cliente.

5.3. Elección del Hardware

Para la implantación de un pfSense que cumpla todos los requisitos del cliente en el entorno empresarial el hardware ha de cumplir las siguientes características[48]:

- Para el IDS Snort se necesitarán +2 GB de RAM.
- Para Squid se ha de tener en cuenta que consume 14 MB de RAM por cada GB de caché en disco, más los requerimientos del propio Squid.
- Para la NIC (network interface card) : Se recomienda Intel PRO/1000 1Gb o PRO/10GbE 10Gb NICs porque tienen un soporte sólido de controladores en FreeBSD y tienen gran rendimiento con el sistema.
- CPU que incluya AES-NI para usar el equipo como servidor VPN.
- Un disco mayor de 4 GB. Con todos los componentes a instalar y servicios de cache se ha optado por un disco de 500 GB.
- Se ha de comprobar la compatibilidad de los elementos con FreeBSD en las guías de freeBSD. [49]

Tras tener en cuenta los requisitos mínimos requeridos por el software pfSense se ha decidido comprar un un DL360e de segunda mano. Las características se pueden observar en la Tabla 5.1.

Se ha decidido comprar un hardware que sobrepase ampliamente los requisitos mínimos pensando en su uso a largo plazo. También se podrá ampliar sus capacidades en un futuro si fuera necesario.

Componente físico x 1
Producto: HP Proliant DL360e Gen8 1U 8x2.5"[50]

Fabricante: HP
Modelo: ProLiant DL360e Gen8
CPU: Quad-Core Intel Xeon E5-2407V1 2.20Ghz(10MB Cache, 6.40Gts, 80W)
RAM: 16 GB
CACHE: 10 MB
HDD: 2x500 GB
Nº Puertos Gigabit Ethernet: 4

Tabla 5.1: Servidor DL360e

5.4. Arquitectura

Para el router se asociará la MAC del equipo que contiene el pfSense instalado como dirección la dirección IP estática 193.168.1.3. Este equipo se asigna como DMZ en el router para que todo el tráfico que inicie conexión desde la red externa sea redirigido al pfSense.

Una vez instalado pfSense se deben configurar las diferentes interfaces de red. La configuración de las interfaces seguirá el esquema de la Figura 5.1. El firewall cuenta con 3 interfaces de red activas. Cada una corresponde a una subred:

- WAN: Conecta al puerto em0 del firewall cuya dirección es 192.168.1.3. Está conectado al router que da acceso a internet. No se configura DHCP para esta interfaz. No debe crear conexiones desde esta interfaz.
- LAN: usa el puerto em1 del firewall cuya dirección es 172.25.1.1. Los usuarios de la red interna se conectan desde esta interfaz. El firewall está configurado para que actúe como servidor DHCP de esta subred.
- DMZ: usa el puerto r10 del firewall con la dirección de red 10.10.10.1. Hay un equipo que simulará el servidor de correo de la red original. No se configura servidor DHCP para esta interfaz. La dirección IP de equipo se configura como estática.
- VPN: usa una dirección de red dentro de RFC1918 pero fuera de cualquiera otra red interna del sistema.

Subred	Dirección IP/Máscara	Router por Defecto	Servidor DHCP	Rango de Asignaciones
WAN	192.168.3.0/24	192.168.1.1	–	–
LAN	172.25.0.0/16	172.25.1.1	172.25.1.1	172.25.1.2-100
DMZ	10.0.0.0/24	10.10.10.1	–	–
VPN	172.16.0.0/16	172.16.0.1	172.16.255.254	–

Tabla 5.2: Direccionamiento red

Para el entorno de pruebas se diseña una pequeña red donde se colocará un pfSense entre el router y la red interna con el objeto de testear y configurar cada una de las áreas del pfSense para su posterior implantación en la empresa, cuya arquitectura física no cambia con respecto a la analizada en el capítulo 4 Esta red tendrá interfaces homólogas a la de la empresa para facilitar la posterior implantación del equipo pfSense.

La red tendrá un aspecto similar al de la Figura 5.1. Su construcción se verá sujeta a cambios a medida que se realicen las pruebas unitarias para cada una de las áreas de la UTM.

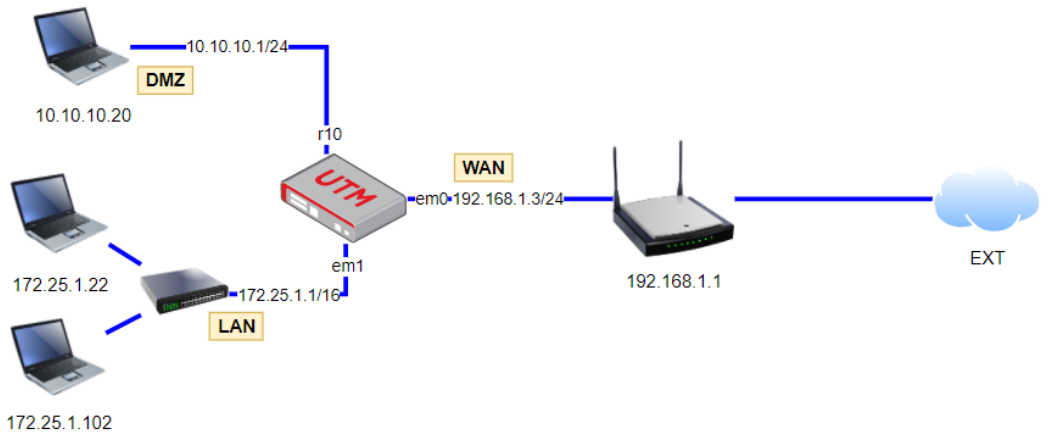


Figura 5.1: Red interna para pruebas

5.5. Elementos de la red

El hardware donde se instala pfSense ha sido cedido por el cliente y cumple con los requisitos mínimos para la ejecución de todas las áreas a instalar. Ver la Tabla 5.3. Los nodos estaciones terminales de trabajo de la red 5.2 serán portátiles varios, como el propio PC de trabajo para este proyecto.

Componente físico x 1
Producto: Servidor para el entorno simulado

CPU: i7-2700K CPU @ 3.50GHz
RAM: 4 GB DDR3
HDD: SATA 500 GB
Nº Puertos Gigabit Ethernet: 3

Tabla 5.3: Servidor para el entorno simulado

Componente físico x 1 (Propiedad del ISP)
Producto: Arcadyan PRV3399B-B-LT[29]

Fabricante: Arcadyan
Modelo: PRV3399B-B-LT
Memoria DDRAM: 256 MB
Memoria FLASH: 128 MB
Frecuencia:50/60 Hz
Nº Puertos SPF: 1
Nº Puertos FXS: 2
Puertos Gigabit Ethernet: 4
Consumo energético: 12.9W
Métodos de gestión: HTTP

Tabla 5.4: Router PRV3399B-B-LT- entorno simulado

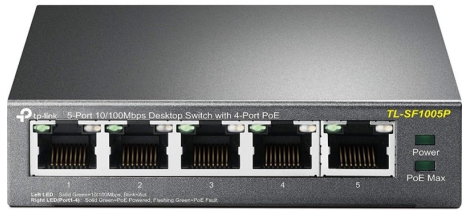
Componente físico x 5
Producto: TP-Link TL-SF1005P[28]

Fabricante: TP-Link
Modelo: TL-SF1005P
Protocolos: IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.3x
Frecuencia: 50/60 Hz
Nº Puertos POE Fast Ethernet: 4
Nº Puertos Fast Ethernet: 1
Máximo consumo energético: 63.51W
Protocolos de gestión: L2 unmanaged

Tabla 5.5: Switch TL-SF1005P

5.6. Configuración de los elementos principales

Sistema de ficheros: Se ha elegido ZFS frente a UFS debido a que ZFS es un sistema atómico. Cada vez que ocurre una escritura, esta contiene todo lo necesario para mantener un estado estable. Esto reduce drásticamente la probabilidad de que el sistema quede corrupto ante situaciones inesperadas como cortes de energía.[52]

5.7. Accesos al equipo pfSense

5.7.1. Acceso seguro al configurador web de pfSense

Para que el administrador acceda al pfSense forma segura se han de cambiar varias configuraciones para que acceda de forma segura se realizan varias acciones:

1. Añadir una contraseña segura que dificulte los ataques por fuerza bruta o diccionario.
2. Habilitar el acceso mediante el protocolo HTTPS

Características contraseña

Las contraseñas para el acceso al sistema pfSense deben cumplir con los estándares del de ciberseguridad. Sus características deben ser:

- 8 o más caracteres.
- Generada aleatoriamente.
- Evitar patrones o secuencias en la contraseña.
- Evitar usar como contraseña información asociada al usuario, conocidos de este, o la empresa, que puedan ser de carácter público.
- Evitar usar cualquier combinación de los elementos mencionados a evitar.

Habilitar el acceso mediante el protocolo HTTPS

Para proteger la integridad, privacidad y autenticidad de las conexiones del actor administrador con el configurador web pfSense se habilita el protocolo HTTPS que encriptará la comunicación. Para ello se diseña la infraestructura PKI de la que hace uso SSL. Se crea el certificado de servidor y los de entidad certificadora que se instalan en cliente. Una vez realizada esta acción se habilita el protocolo HTTPS asignado al certificado de servidor creado.

Se ha decidido crear una estructura jerárquica de certificados para que, si en un futuro se crean más certificados intermedios, en caso de verse comprometido alguno de los certificados se podrá solucionar el problema simplemente revocando el acceso a dicho certificado en lugar de tener que desactivar el certificado raíz. Desactivar el certificado raíz invalidaría todos los certificados.

La infraestructura PKI que se crea dispone de:

- Una Autoridad Certificadora raiz creada en pfSense.
- Una Autoridad Certificadora intermedia en pfSense firmado por el certificado raíz.
- El certificado de servidor de pfSense firmado por el certificado intermedio.

Todos los elementos de la PKI son configurados con SHA256 y RSA-2048 o superior, pues se consideran los suficientemente seguros.

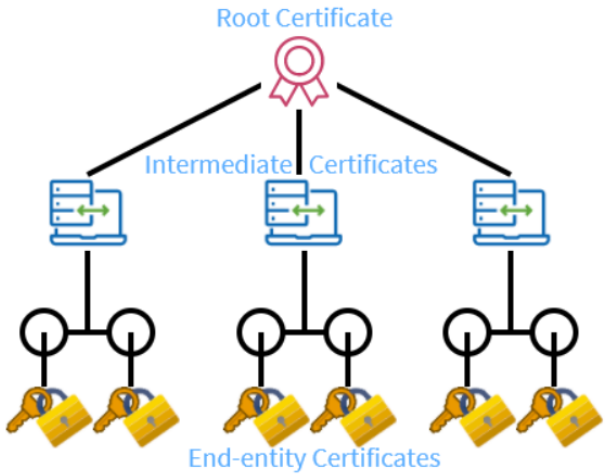


Figura 5.2: Cadena de confianza de certificados[54]

Una vez creada la estructura PKI en el pfSense y activado HTTPS se instala en el ordenador del administrador los certificados de raíz e intermedios. Una vez realizada esta acción el actor administrador, y sólo este actor, podrá acceder al configurador web de pfSense de forma segura. Para obtener más información sobre el funcionamiento de este protocolo vaya a la sección 2.7.8

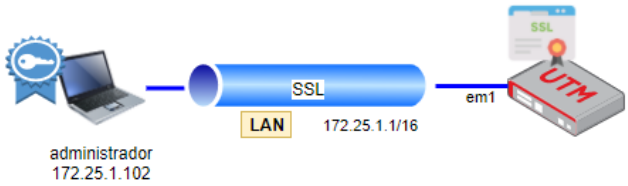


Figura 5.3: Acceso al webconfigurator mediante HTTPS

5.8. Acceso a pfSense mediante ssh y ssh-agent

Para que el actor administrador pueda conectarse a la consola de pfSense en remoto se configura un túnel SSH. Con el túnel SSH, al igual que con SSL, se cifra la sesión. En una conexión SSH una vez encriptada de forma simétrica para la creación del túnel, el usuario debe autenticarse. Para ello tradicionalmente este debe introduce sus credenciales, usuario y contraseña.

Para reforzar la seguridad de las conexiones SSH, se ha añadido una capa extra de seguridad autenticando la conexión además de con las credenciales de usuario y la contraseña, mediante un par de claves asimétricas.

Para generar el par de claves asimétricas se ha decidido usar el SSH-Agent PuttyGen ya que el administrador se conectará mediante Windows. Para obtener más información sobre el funcionamiento de este protocolo vaya a la sección2.7.8

5.9. Reglas de firewall

Para controlar el flujo de conexiones entre las diferentes interfaces se usan las reglas de firewall. Se dividen por interfaz: WAN, LAN, DMZ

Reglas de la interfaz LAN

Para la interfaz LAN se configuran las reglas de firewall LAN outbound, que son los servicios a usar por esta interfaz, en el siguiente orden:

1. Regla para permitir el acceso a la interfaz web a los administradores de red. Los puertos del alias antilockoutports son: 443, 22 y 80. El alias TI se corresponde con las direcciones IP de los administradores.
2. Regla para bloquear el acceso remoto al configurador web. Los puertos del alias antilockoutports son: 443, 22 y 80.
3. Regla para permitir el acceso a DNS de pfsense.
4. Regla para permitir el acceso a páginas web. Los puertos del alias WEBPORTS son: 443 y 80.
5. Regla para permitir conectar al servidor de email en DMZ.
6. Regla para rechazar el acceso a la subred DMZ.
7. Regla para permitir el acceso general a internet.

Reglas LAN
1-pass in quick on em1 inet proto tcp from <TI>to 172.25.1.1 port = ssh flags S/SA keep state 1-pass in quick on em1 inet proto tcp from <TI>to 172.25.1.1 port = https flags S/SA keep state 1-pass in quick on em1 inet proto udp from <TI>to 172.25.1.1 port = ssh keep state 1- pass in quick on em1 inet proto udp from <TI>to 172.25.1.1 port = https keep state
2- block drop in quick on em1 inet proto tcp from any to 172.25.1.1 port = ssh flags S/SA 2- block drop in quick on em1 inet proto tcp from any to 172.25.1.1 port = https flags S/SA 2- block drop in quick on em1 inet proto tcp from any to 172.25.1.1 port = http flags S/SA
3- pass in quick on em1 inet proto tcp from 172.25.0.0/16 to 172.25.1.1 port = domain flags S/SA keep state 3- pass in quick on em1 inet proto udp from 172.25.0.0/16 to 172.25.1.1 port = domain keep state
4- pass in quick on em1 inet proto tcp from 172.25.0.0/16 to any port = http flags S/SA keep state 4- pass in quick on em1 inet proto tcp from 172.25.0.0/16 to any port = https flags S/SA keep state
5- pass in quick on em1 inet from 172.25.0.0/16 to <SV_EMAIL>flags S/SA keep state
6- block return in quick on em1 inet from 172.25.0.0/16 to 10.10.10.0/24
7- pass in quick on em1 inet from 172.25.0.0/16 to any flags S/SA keep state

Tabla 5.6: Definición de las reglas de acceso desde la interfaz LAN

Reglas de la interfaz DMZ

1. Regla para permitir al servidor de email el acceso a todo en general. El alias svemail contiene la dirección IP del servidor de email.
2. Regla para rechazar a elementos conectados a la DMZ el acceso a redes privadas. Si otro equipo distinto del servidor de email se conectase a la DMZ solo podría comunicarse con la red externa.

Reglas DMZ
1- pass in quick on rl0 inet from <SV_EMAIL>to any flags S/SA keep state
2- block return in log quick on rl0 inet from 10.10.10.0/24 to <RFC1918>

Tabla 5.7: Definicion de las reglas de acceso desde la interfaz DMZ

Reglas de la interfaz WAN

1. Regla para bloquear las conexiones desde cualquier IP privada.
2. Regla para bloquear las conexiones desde IPs no registradas por IANA.
3. Reglas para permitir la conexión desde cualquier dirección al servidor de email de la DMZ mediante los protocolos: IMAPS, SMTP, IMAP, SMTP/S y SMTP/TLS.
4. Reglas para la creación de túneles VPN que permitan a usuarios conectarse de forma remota a su departamento en la LAN. De estas reglas se hablara en apartado VPN.

Reglas WAN
1- block drop in log quick on em0 reply-to (em0 192.168.1.1) inet from <pfB_PRI1_v4>to any label ÜSER_RULE: pfB_PRI1_v4 auto rule"
2- block drop in log quick on em0 from <bogons>to any label "block bogon IPv4 networks from WAN" 2- block drop in log quick on em0 from <bogonsv6>to any label "block bogon IPv6 networks from WAN"
3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto tcp from any to <SV_EMAIL>port = imap flags S/SA keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to <SV_EMAIL>port = imap keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto tcp from any to <SV_EMAIL>port = imaps flags S/SA keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to <SV_EMAIL>port = imaps keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto tcp from any to <SV_EMAIL>port = smtp flags S/SA keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to <SV_EMAIL>port = smtp keep state label 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto tcp from any to <SV_EMAIL>port = submission flags S/SA keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to <SV_EMAIL>port = submission keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto tcp from any to <SV_EMAIL>port = smtps flags S/SA keep state 3- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to <SV_EMAIL>port = smtps keep state
4- pass in quick on em0 reply-to (em0 192.168.1.1) inet proto udp from any to any port = openvpn keep state

Tabla 5.8: Definición de las reglas de acceso desde la interfaz WAN

5.10. Reglas de redirección NAT

Para que los usuarios externos puedan conectarse con el servidor de email que se encuentra en la DMZ hay que configurar las redirecciones de tráfico hacia la DMZ.

Para ello se ha usado Port Forward, que permite el acceso a un dispositivo de red interna a través de un puerto específico. Las reglas de Port Forward para el acceso al servidor email en la DMZ son:

1. Regla que redirige el tráfico procedente de la WAN a través del puerto 143 al servidor de email.
2. Regla que redirige el tráfico procedente de la WAN a través del puerto 993 al servidor de email.
3. Regla que redirige el tráfico procedente de la WAN a través del puerto 25 al servidor de email.
4. Regla que redirige el tráfico procedente de la WAN a través del puerto 456 al servidor de email.
5. Regla que redirige el tráfico procedente de la WAN a través del puerto 587 al servidor de email.

PortFoward
1- rdr on em0 inet proto tcp from any to 192.168.1.3 port = imap -><SV_EMAIL>round-robin 1- rdr on em0 inet proto udp from any to 192.168.1.3 port = imap -><SV_EMAIL>round-robin
2- rdr on em0 inet proto tcp from any to 192.168.1.3 port = imaps -><SV_EMAIL>round-robin 2- rdr on em0 inet proto udp from any to 192.168.1.3 port = imaps -><SV_EMAIL>round-robin
3- rdr on em0 inet proto tcp from any to 192.168.1.3 port = smtp -><SV_EMAIL>round-robin 3- rdr on em0 inet proto udp from any to 192.168.1.3 port = smtp -><SV_EMAIL>round-robin
4- rdr on em0 inet proto tcp from any to 192.168.1.3 port = smtps -><SV_EMAIL>round-robin 4- rdr on em0 inet proto udp from any to 192.168.1.3 port = smtps -><SV_EMAIL>round-robin
5- rdr on em0 inet proto tcp from any to 192.168.1.3 port = submission -><SV_EMAIL>round-robin 5- rdr on em0 inet proto udp from any to 192.168.1.3 port = submission -><SV_EMAIL>round-robin

Tabla 5.9: Definición de las reglas de redirección

5.11. Acceso a la red por parte de los usuarios: Asignación de direcciones

Para que un usuario se le permita el acceso a la red LAN pfSense debe asignarle una dirección IP.

Los usuarios no invitados dispondrán de una dirección IP fija. Los usuarios invitados tendrán una dirección IP asignada por el servidor DHCP de pfSense. El rango de direccionamiento viene descrito en la Tabla 5.2

5.11.1. Conexión remota: OpenVPN

Para que los empleados puedan conectar en remoto a la red interna de la empresa se crean túneles VPN. Cada empleado tendrá un túnel VPN exclusivo que le permita conectarse desde su casa a un determinado equipo perteneciente a la red LAN.

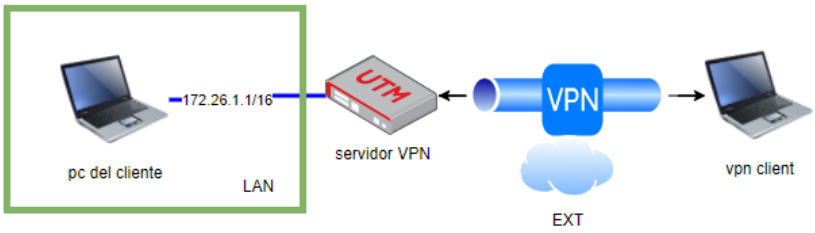


Figura 5.4: conexión VPN empleado con escritorio remoto

Para la creación de los túneles VPN se ha usado OpenVPN por los motivos dados en la sección 2.8.5. Para ello se deberá:

1. Crear la infraestructura de certificados (PKI): La estructura de certificados para la VPN cuenta con una entidad certificadora, un certificado de servidor y certificados de usuario.
2. Configurar OpenVPN: En OpenVPN se configuran las características del servidor VPN, junto con las reglas que concedan el paso a la conexión del cliente OpenVPN.
3. Configurar el acceso del cliente.

En la Tabla 5.10 se muestran las características de los tuneles VPN a crear por el servidor.

OpenVPN Server				
Interfaz	Protocolo/Puerto	Túnel	Crypto	Descripcion
WAN	UDP4/1194	172.16.0.0/16	AES-128-CBC/SHA256 4096 bits	Túnel Admin
WAN	UDP4/1198	172.17.7.0/24	AES-128-CBC/SHA256 4096 bits	Túnel Comercial

Tabla 5.10: Servidor VPN túneles

5.12. Limitadores de ancho de banda

Para garantizar la calidad de servicio se han configurados límites de descarga y de subida para los usuarios de la red interna. 5 Para los usuarios de la red LAN en la Figura 5.1 se

asigna un ancho de banda de 5 MBs de subida y de bajada mediante la herramienta Traffic Shaper, que esta ya integrada en pfSense.

Grupo_1		
IP address	Subida Máximo	Bajada Máximo
172.25.1.22	5 MB	5 MB
172.25.1.102	5 MB	5 MB

Tabla 5.11: Ancho de banda para los nodos de la LAN en la red de la Figura5.1

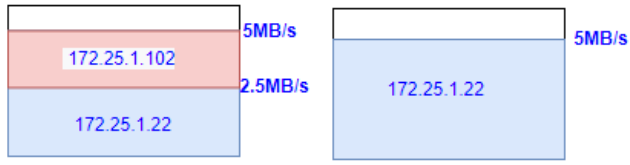


Figura 5.5: Repartición del ancho de banda para usuarios de la red 5.1

5.13. Control de tráfico web: Squid, SquidGuard

El cliente quiere poder observar a qué sitios web se conectan sus empleados y, a su vez, restringir el acceso a determinadas páginas web. Para ello se ha decido usar como control de tráfico Squid debido a que encaja a la perfección los requisitos del cliente. Esta herramienta se usará tanto para el filtrado y control web de las peticiones de los clientes dentro de la red privada, como para el guardado en la caché y disco de nuestra UTM de actualizaciones de Windows y otros elementos a los que los clientes de la red vayan a acceder con frecuencia, para así acelerar el acceso a los recursos en línea y reducir el ancho de banda utilizado.

Para conocer más sobre el funcionamiento de Squid y sus plugins vaya a la sección 2.7.5

Se ha decido guardar reservar un espacio en disco de 50 GB para guardar con la caché de Squid las actualizaciones de Windows.

Se ha decidido configurar Squid en modo Transparente en modo peeksplice. Esta configuración evita tener que realizar configuraciones en cliente y su vez permite tomar decisiones de acceso o no al servicio web en función de su hostname.

La configuración de lista negra de accesos viene dada por la Tabla 5.12

Lista Negra	
Tipología/Hostname	Usuarios
Apuestas	172.25.1.102
Agresivo	172.25.1.102
www.meneame.net	172.25.1.102

Tabla 5.12: servicios denegados por usuario

5.13.1. Control del tráfico por capa de aplicación: IDS

Con el objeto de monitorizar el tráfico a nivel de aplicación y poder detectar posibles ataques se ha decidido instalar Snort frente a Suricata por los motivos dados en la comparativa de la sección 2.8.3

Se han tomado las siguientes decisiones con respecto a su configuración:

Snort			
Despliegue	Acción	Firmas/Patrón	Sensores
WAN	IDS Pasivo	Híbrido	Centralizado (pfSense)
LAN	IDS Pasivo	Híbrido	Centralizado (pfSense)

Tabla 5.13: Modo de despliegue Snort en la red

5.13.2. Bloqueador de malware: pfBloquerNG

Se ha decidido integrar pfBloquerNG para:

- Bloquear tráfico proveniente de direcciones negras DNSBL[55] para bloquear páginas de malware. Se ha decidido filtrar por las 3 listas aportadas.
- Bloquear tráfico por pais. Se ha decidido bloquear tráfico proveniente de Singapur, el país del que provienen más ciberataques del mundo en la actualidad.[56]
- Las conexiones a bloquear serán peticiones desde la interfaz LAN que coincidan con algún elemento de la lista negra y tráfico proveniente de la WAN que cumpla el mismo criterio.
- Como DNS SinkHole se usa una dirección que no vaya a estar en uno por ningún otro servicio.

pfBlockerNG					
Rastreo	DNS SinkHole	DNSBL_EASY	DNSBL_ADDS	DNSBL_Malicious	País
Entrantes:WAN y Hacia: LAN	172.20.10.1	SI	SI	SI	Singapur

Tabla 5.14: Diseño configuración pfBloquerNG

Capítulo 6

Implantación en el Entorno de Pruebas

Es este capítulo se explican las configuraciones realizadas para la implantación de un UTM pfSense que cubra todos los requisitos de cliente. Los detalles de la red y las directrices establecidas se encuentran en el capítulo de 5.

Los detalles paso a paso de cada una de las configuraciones se encuentran el documento adjunto *Manual de configuración y uso*.

6.1. Preparación del entorno de pruebas

El software a instalar en el equipo, pfSense 2.4.5, se descarga desde la página oficial de pfSense[51]. Se instalará en el equipo de la Tabla 5.4. Las opciones a aplicar de descarga son:

- Arquitectura: AMD64
- Instalador: Memstick installer
- Consola: VGA

La instalación de pfSense en el equipo se realiza desde una memoria USB donde se ha grabado la imagen. Se seleccionará particionamiento ZFS por los motivos dados en la sección 5.6

6.2. Configuración de las interfaces

Para crear las interfaces del mostradas en la Figura 5.1 y la Tabla 5.2. Primero se ha de configurar el router frontera para que redirija el tráfico a pfSense. Para ello:

- En el router frontera se asociará la MAC del equipo que contiene el pfSense instalado como dirección la dirección IP estática 193.168.1.3. Este equipo se asigna como DMZ en el router para que todo el tráfico que inicie conexión desde la red externa sea redirigido al pfSense.

En el firewall se configuran las 3 interfaces de red activas mencionadas en la Tabla 5.2 . Cada una corresponde a una subred:

- WAN: Conecta al puerto em0 del firewall cuya dirección es 192.168.1.3. Está conectado al router que da acceso a internet. No se configura DHCP para esta interfaz. No debe crear conexiones desde esta interfaz.
- LAN: usa el puerto em1 del firewall cuya dirección es 172.25.1.1. Los usuarios de la red interna se conectan desde esta interfaz. El firewall está configurado para que actúe como servidor DHCP de esta subred.
- DMZ: usa el puerto r10 del firewall con la dirección de red 10.10.10.1. Hay un equipo que simulará el servidor de correo de la red original. No se configura servidor DHCP para esta interfaz. La dirección IP de equipo se configura como estática.

La interfaz WAN y LAN se deberán configurar mediante consola por acceso físico a pfSense.

```
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on firewall ***

 WAN (wan)       -> em0        -> v4: 192.168.1.3/24
 LAN (lan)       -> em1        -> v4:
 DMZ (opt1)      -> r10        -> v4:

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 1
```

Figura 6.1: Configuración de interfaces mediante consola

Mediante la opción 1 de la Figura 6.1 se asigna la correspondencia entre interfaz y mediante la opción 2 los rangos en caso de haber servidor DHCP y direccionamientos. La configuración específica viene dada por la Tabla 6.1

Configuración	Option 1	Option 2	Option 2	Option 2	Option 2
Interfaz	**Asignación física**	**DHCP**	**IPv4**	**Máscara**	**Gateway**
WAN	em0	no	192.168.1.3	255.255.255.0	192.168.1.1
LAN	em1	start range:172.25.1.2 end range: 172.25.1.100	172.25.1.1/16	255.255.0.0	–
DMZ	rl0	no	10.10.10.1/24	255.255.255.0	

Tabla 6.1: configuración interfaces

6.2.1. Acceso seguro al configurador web de pfSense

El actor administrador accede al configurador web de pfSense a través de la dirección 172.25.1.1 mediante el protocolo http. Por defecto las credenciales de pfSense son usuario: admin, password: pfsense. Tal y como se ha comentado en la sección 5.7.1, para que el usuario administrador pueda acceder al configurador web de forma segura se ha de:

1. Configurar los parámetros de pfSense tal como hostname, DNS server, nueva contraseña...
2. Añadir una contraseña segura que dificulte los ataques por fuerza bruta o diccionario. Se seguirán los estándares indicados en la sección 5.7.1
3. Habilitar el acceso mediante el protocolo https.

Para la primera conexión a través del configurador web se mostrará un wizard de configuración donde se configurará la información general del equipo. Las configuraciones aplicadas son las de la Tabla 6.2

Wizard	
Domain	miempresa.es
Hostname	firewall
Primary DNS Server	172.25.1.1
Secondary DNS Server	8.8.8.8
NTP Server	hora.roa.es
Password	Exma9pel?0Fpsas*

Tabla 6.2: configuración aplicada en wizard

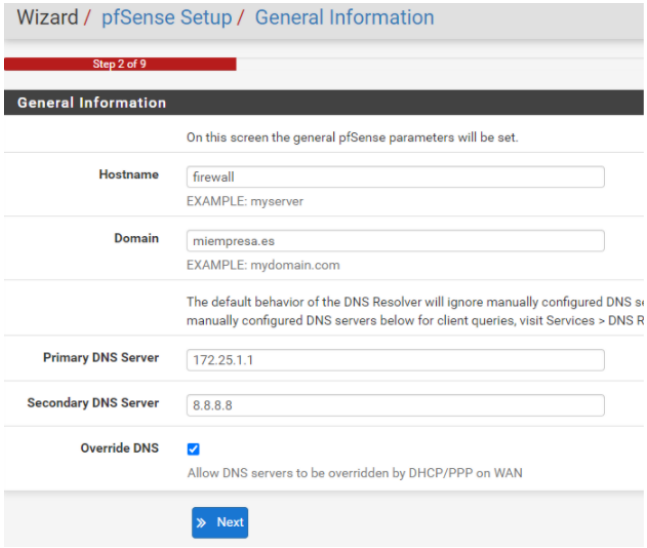


Figura 6.2: wizard configuración

Habilitar el acceso mediante el protocolo HTTPS

Para habilitar HTTPS como protocolo de acceso al configurador web:

1. Se crea la autoridad certificadora raíz. Sus características vienen dados por la Figura 6.3.
2. Se crea el autoridad certificadora intermedio. Sus características vienen dados por la Figura 6.4.
3. Se crea el certificado de servidor. Sus características vienen dados por la Figura 6.5.
4. Se habilita HTTPS en pfSense
5. Se instalan las entidades certificadoras en el PC del administrador

Desde System>Certificate Manager se crean los certificados.

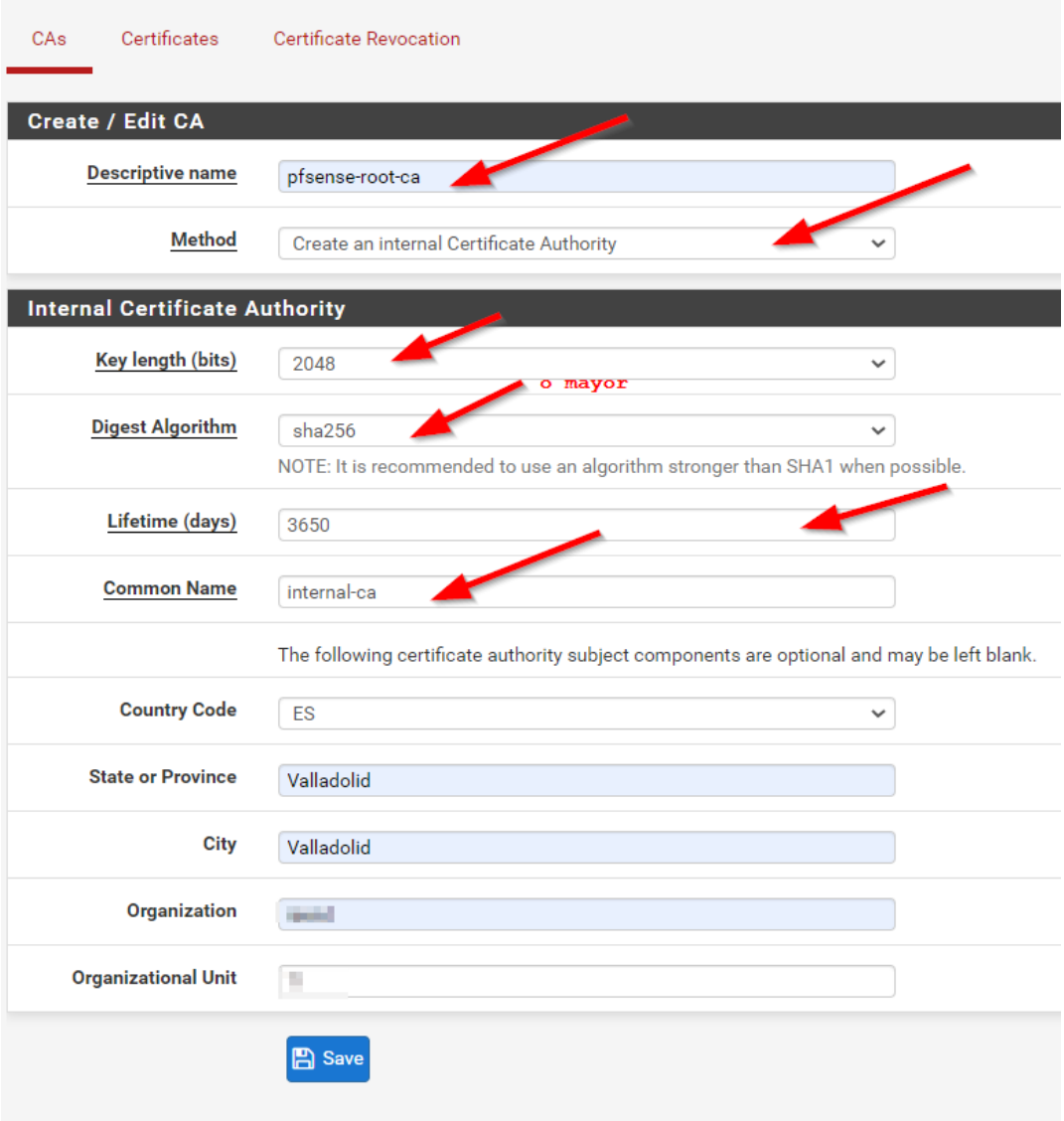


Figura 6.3: Configuración CA raíz para HTTPS

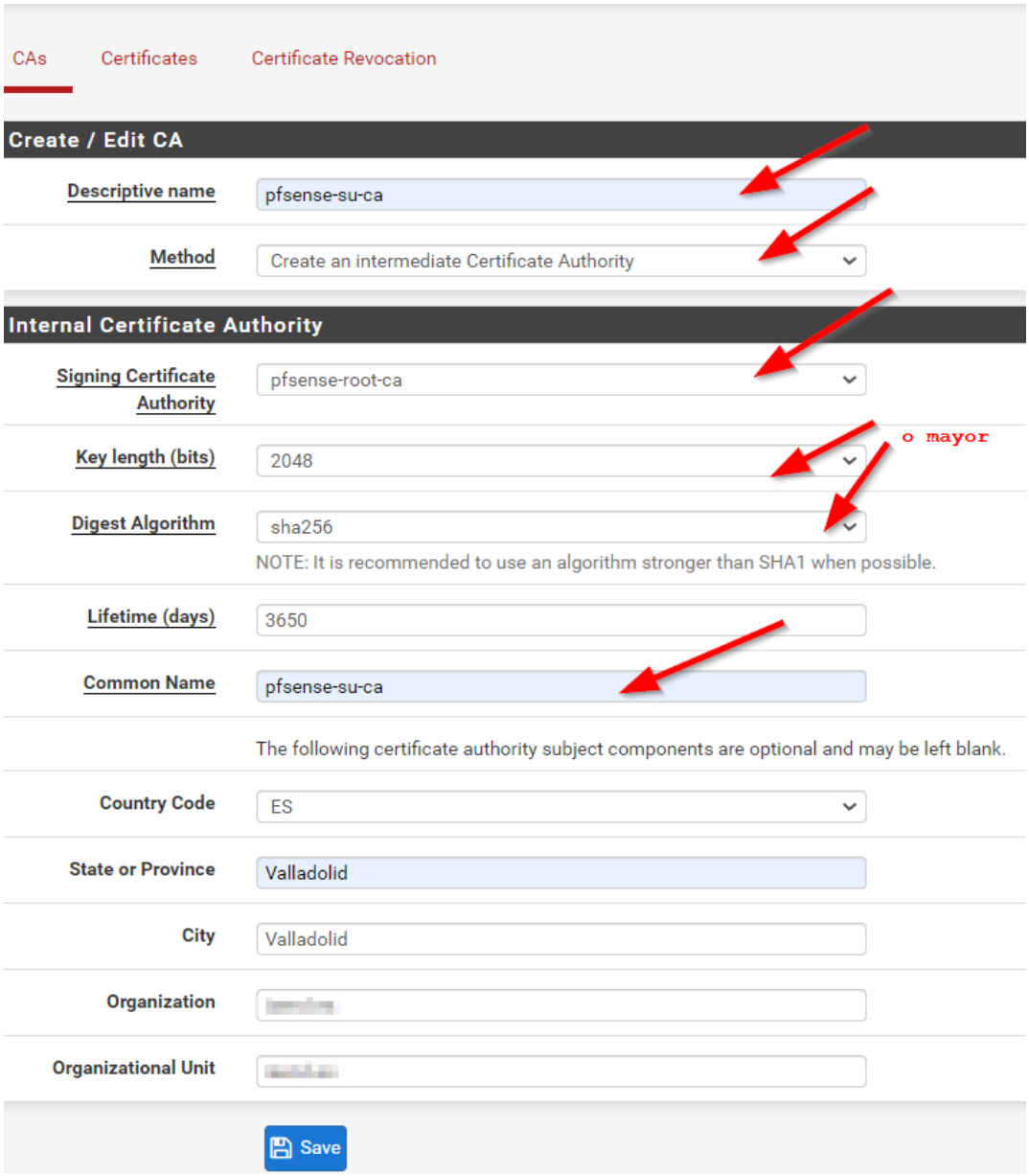


Figura 6.4: Configuración CA intermedia raíz para HTTPS

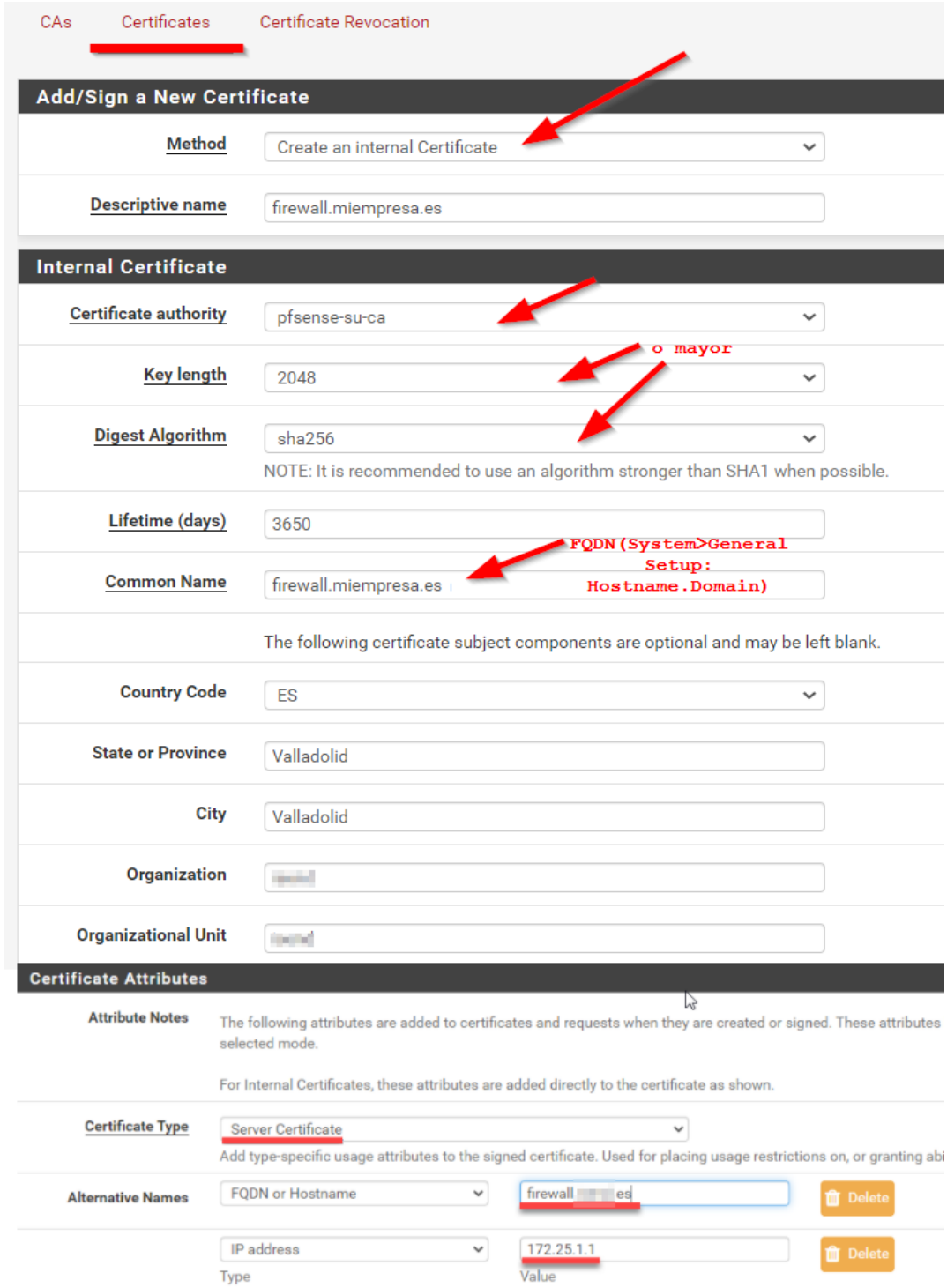


Figura 6.5: Configuración certificado de servidor para HTTPS

Una vez creada la estructura PKI en el pfSense y activado HTTPS se instala en el ordenador del administrador los certificados de raíz e intermedios. Una vez realizada esta acción el actor administrador, y sólo este actor, podrá acceder al configurador web de pfSense de forma segura.

Después se activa el protocolo HTTPS asignándole el certificado de servidor que se creó previamente.

Una vez realizados estos pasos se podrá acceder al configurador web de pfSense por protocolo https a través de las direcciones dadas en el certificado: firewall.miempresa.es ó 172.25.1.1

6.3. Acceso a pfSense mediante ssh y ssh-agent

Para que el actor administrador pueda conectarse a la consola de pfSense en remoto se configura un túnel SSH.

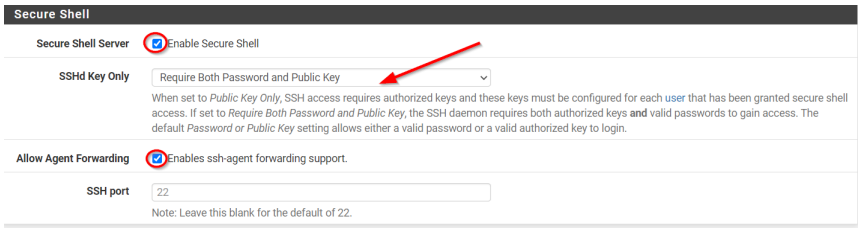


Figura 6.6: Configuración acceso túnel SSH + par-clave

El puerto se dejará el de defecto, 22, los ataques por fuerza bruta exitosos son improbables gracias al sshguard, configurable bajo la sección de *Login protection*.

Para la gestión de acceso mediante clave pública se usa PuttyGen. La clave creada mediante PuttyGen se asigna en pfSense al usuario admin para que sólo mediante ese usuario se puedan establecer conexiones SSH y solo para el cliente que disponga de la clave privada.

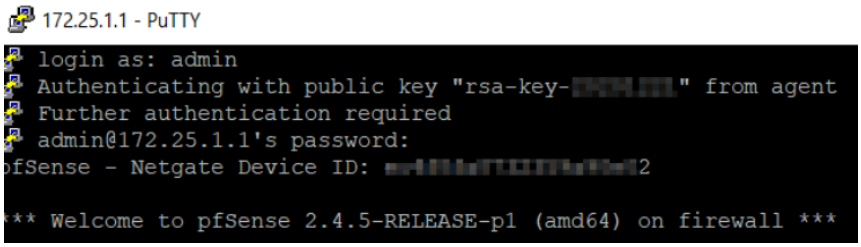


Figura 6.7: Acceso mediante SSH + par-clave

6.4. Reglas de firewall

Para controlar el flujo de conexiones entre las diferentes interfaces usamos las reglas de firewall. Se dividen en 3 tipos.

Reglas de la interfaz LAN

Para la interfaz LAN se configuran las reglas de firewall LAN outbound, que son los servicios a usar por esta interfaz, en el siguiente orden:

1. Regla para permitir el acceso a la interfaz web a los administradores de red. Los puertos del alias antilockoutports son: 443, 22 y 80. El alias TI se corresponde con las direcciones IP de los administradores.
2. Regla para bloquear el acceso remoto al configurador web. Los puertos del alias antilockoutports son: 443, 22 y 80.
3. Regla para permitir el acceso a DNS de pfsense.
4. Regla para permitir el acceso a páginas web. Los puertos del alias WEBPORTS son: 443 y 80.
5. Regla para permitir conectar al servidor de email en DMZ.
6. Regla para rechazar el acceso a la subred DMZ.
7. Regla para permitir el acceso general a internet.

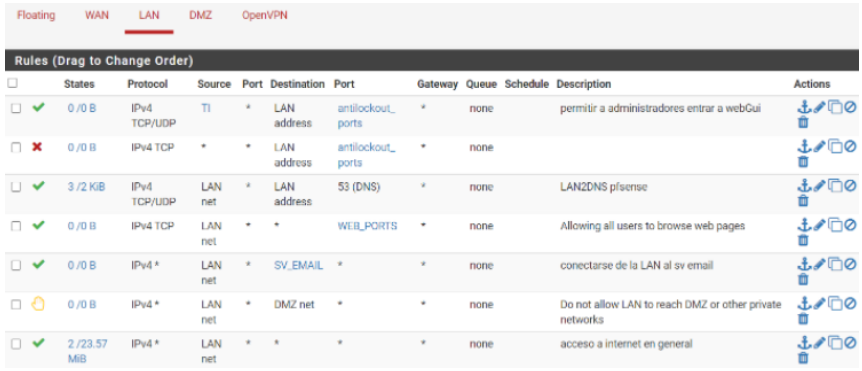


Figura 6.8: Reglas de firewall en la interfaz LAN

Reglas de la interfaz DMZ

1. Regla para permitir al servidor de email el acceso a todo en general. El alias svemail contiene la dirección IP del servidor de email.
2. Regla para rechazar a elementos conectados a la DMZ el acceso a redes privadas. Si otro equipo distinto del servidor de email se conectase a la DMZ solo podría comunicarse con la red externa.

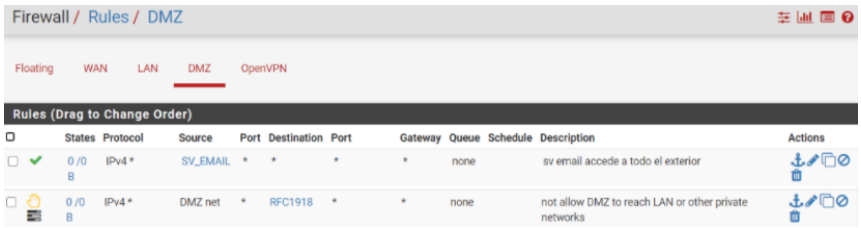


Figura 6.9: Reglas de firewall en la interfaz DMZ

Reglas de la interfaz WAN

1. Regla para bloquear las conexiones desde cualquier IP privada.
2. Regla para bloquear las conexiones desde IPs no registradas por IANA.
3. Reglas para permitir la conexión desde cualquier dirección al servidor de email de la DMZ mediante los protocolos: IMAPS, SMTP, IMAP, SMTP/S y SMTP/TLS.
4. Reglas para la creación de túneles VPN que permitan a usuarios conectarse de forma remota a su departamento en la LAN. De estas reglas se hablara en apartado VPN.

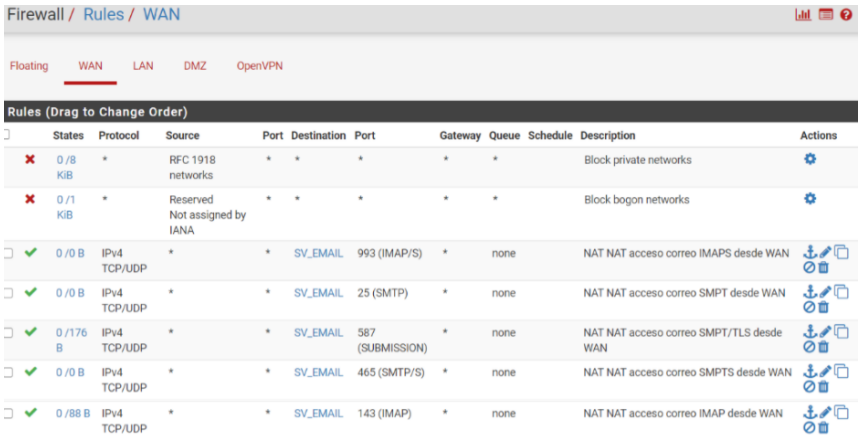


Figura 6.10: Reglas de firewall en la interfaz WAN

6.5. Reglas de redirección NAT

Para que los usuarios externos puedan conectarse con el servidor de email que se encuentra en la DMZ hay que configurar las redirecciones de tráfico hacia la DMZ.

Para ello se ha usado Port Forward, que permite el acceso a un dispositivo de red interna a través de un puerto específico. Las reglas de Port Forward para el acceso al servidor email en la DMZ son:

1. Regla que redirige el tráfico procedente de la WAN a través del puerto 143 al servidor de email.
2. Regla que redirige el tráfico procedente de la WAN a través del puerto 993 al servidor de email.
3. Regla que redirige el tráfico procedente de la WAN a través del puerto 25 al servidor de email.
4. Regla que redirige el tráfico procedente de la WAN a través del puerto 456 al servidor de email.
5. Regla que redirige el tráfico procedente de la WAN a través del puerto 587 al servidor de email.

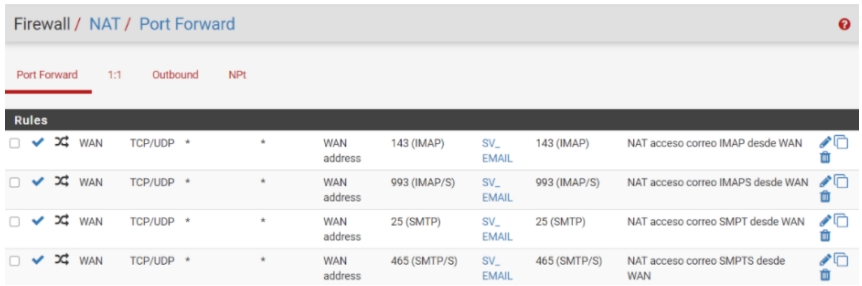


Figura 6.11: Reglas de Port Forward

La creación de reglas de port fowarding desencadena la creación automática de las reglas de firewall necesarias para poder realizar las redirecciones. Las reglas creadas para el acceso al servidor de email han desencadenado la creación de las reglas de firewall de la firewall de la Figura 6.12

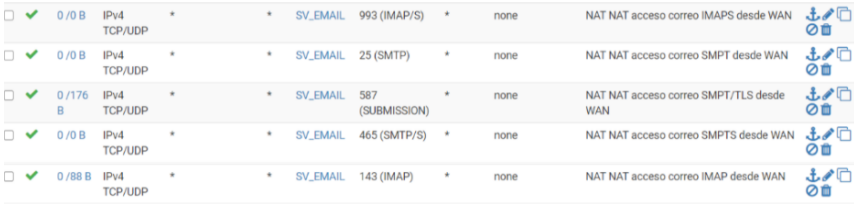


Figura 6.12: Reglas de firewall para poder realizar port forward

6.6. Asignación de direcciones a usuarios y WoL

Para que a un usuario invitado se le permita el acceso a la red LAN pfSense debe asignarle una dirección IP. Para ello se ha activado el servidor DHCP en LAN que asignará direcciones dinámicamente a los usuarios que le pidan conexión. El rango de direccionamiento dinámico viene dado en la Tabla 6.1

Los equipos con dirección estática reciben la misma dirección que les sera asignada por el equipo firewall anterior. Para estos usuarios hay que configurar previamente su dirección haciendo un mapeo en la interfaz LAN desde *Services*>*DHCP Server*>LAN>*DHCP Static Mapping*

- **MAC Address:** d8:cb:8a:84:eefc
- **IP Address:** 172.25.1.22
- **Hostname:** patri
- **Description:** mapeo estático para patri-pc

Para configurar el WoL simplemente hay que hacer click a la opción desde la tabla de *DHCP Leases*.

6.6.1. Conexión remota: OpenVPN

Para que los empleados puedan conectar en remoto a la red interna de la empresa se han creado túneles VPN. Cada empleado tendrá un túnel VPN exclusivo que le permita conectarse desde su casa a un determinado equipo perteneciente a la red LAN.

Para la creación de los túneles VPN se ha usado OpenVPN por los motivos dados en la sección 2.8.5. Para ello se han seguido los siguientes pasos:

1. **Crear la infraestructura de certificados (PKI)**: La estructura de certificados para la VPN cuenta con una entidad certificadora, un certificado de servidor y certificados de usuario. La creación y el uso de estos certificados está explicado en la sección 6.2.1.

2. **Configurar OpenVPN**: En OpenVPN se configuran las características del servidor VPN, junto con las reglas que concedan el paso a la conexión del cliente OpenVPN. Esta configuración se realiza mediante un wizard que ayuda a no saltarse ningún paso a la hora de realizar la configuración. Una vez elegidas todas las propiedades del túnel de conexión se creará automáticamente una regla de firewall en la interfaz WAN que permita la entrada de conexiones al servidor VPN y otra regla de OpenVPN que permita al tráfico de un nodo OpenVPN remoto conectarse a los recursos de la red interna.

3. **Configurar el acceso del cliente**: Se crea una entidad cliente cuyas propiedades de *Configuración de autenticación de usuario*, *Configuración de túnel* y *Configuración criptográfica* coinciden con las del servidor. Es decir con las de la Figura 6.13.

4. **Autenticar al usuario**: Para autenticar al usuario este debe disponer de un certificado de usuario firmado por la entidad autenticadora de de VPNs creada anteriormente. Para ello se crea un usuario por cliente que vaya a usar la VPN. Las certificados de usuario se crean desde el propio usuario. Una vez creado el certificado, se exporta con OpenVPN Client Export. El usuario debe instalar el archivo descargado en el cliente de OpenVPN de su casa para poder conectarse a la dirección IP señalada en el certificado de servidor.

En la Figura 6.13 se observan las características elegidas para OpenVPN junto con una pequeña explicación.

1. **Type of Server**: Local User Access
2. **Certificate Authority**: <<nombre de certificado de autoridad para OpenVPN>>
3. **Server Certificate**: <<nombre de certificado de servidor OpenVPN>>
4. **General OpenVPN Server information**:
   - Interface: WAN
   - Protocol: UDP on IPv4 only
   - Local Port: 1194
   - Description:Tunel VPN - <<grupo>>
5. **Cryptographic Settings:**
   - TLS authentication: chequeado
   - Generate TLS Key: chequeado
   - D-H Params: 4096 bit
   - Encryption Algorithm: AES-128-CBC/SHA256
   - Auth Digest Algorithm: SHA256
   - Hardware Crypto: bsd cryptodev engine - RSA...AES-256-CBC
6. **Tunnel Settings:**
   - Tunel network: 172.17.1.0/24 u otro rango de direcciones que pertenezcan a direcciones privadas pero no se encuentren dentro de las direcciones dentro de la LAN. Es decir de 172.16.0.0 - 17.24.255.255 y 172.26.0.0-172.31.255.255
   - Redirect gateway: chequeado
   - Local network:172.25.7.0/24,172.25.x.x/32(IP del equipo al que se conecta)
7. **Client Settings:**
   - Dynamic IP: chequeado.
   - Topology: Subnet - one IP address per client in a common subnet
8. **Firewall Rule Configuration:**
   - Firewall Rule: chequeado.
   - OpenVPN Rule: chequeado.

Figura 6.13: configuración de OpenVPN.

En la Figura 6.14 se observa la asignación del certificado para un usuario administrador.

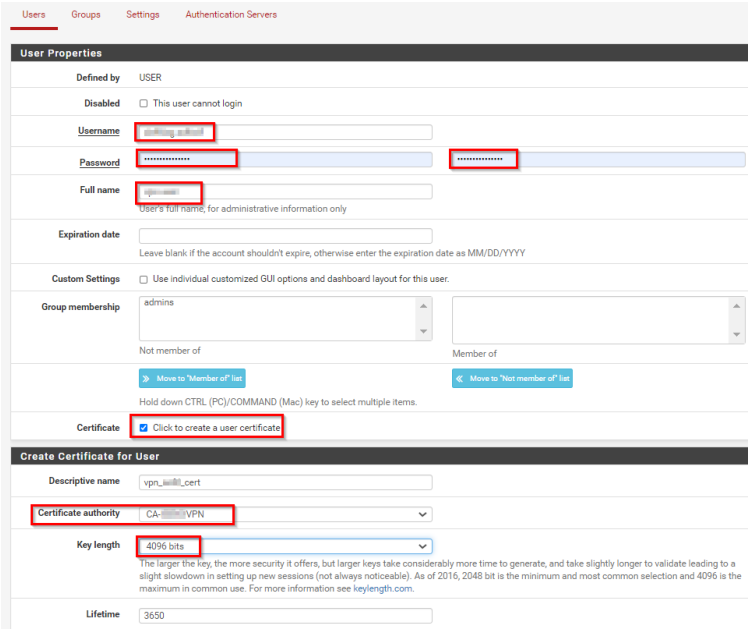


Figura 6.14: asignación de certificado a usuario.

6.7. Limitadores de ancho de banda

Para el grupo de usuarios Grupo_1 se ha definido un ancho de banda a repartir de 5 MB y 5 MB de bajada.

Grupo_1		
IP address	Subida Máximo	Bajada Máximo
172.25.1.22	5 MB	5 MB
172.25.1.102	5 MB	5 MB

Tabla 6.3: Ancho de banda para los nodos de la LAN en la red de la Figura 5.1

Para ello:

1. Se ha definido el límite de subida y el de bajada con la herramienta Traffic Shaper. Con las siguientes características:
   - **Enable**: marcada la opción para habilitar el limitador.
   - **Name**: Bajada o Subida, en función del limitador

- **Mask**: Destination address
- **Bandwidth**: 5 Mbps

2. Se ha definido un alias con el grupo de direcciones IP de usuario al que se va a asignar la restricción de ancho de banda.

3. Se ha creado una regla de firewall que asigna los limites de ancho de banda al grupo de usuarios.Se puede observar en la Figura 6.15. Las características de la regla son:

   - **Action:Pass.**
   - **Interface: LAN.**
   - **Source:** Single host o valor del alias creado, en nuestro caso **Grupo_1.**
   - **Destination: any.**
   - **Destination Port Range: WEB_PORTS** (alias para los puertos 80 y 443).
   - **In /Out pipe:** Para In (tráfico que entra a pfSense por el puerto de la interfaz LAN): **Subida** y para Out (tráfico que sale de pfSense por el puerto de la interfaz LAN): **Bajada**.

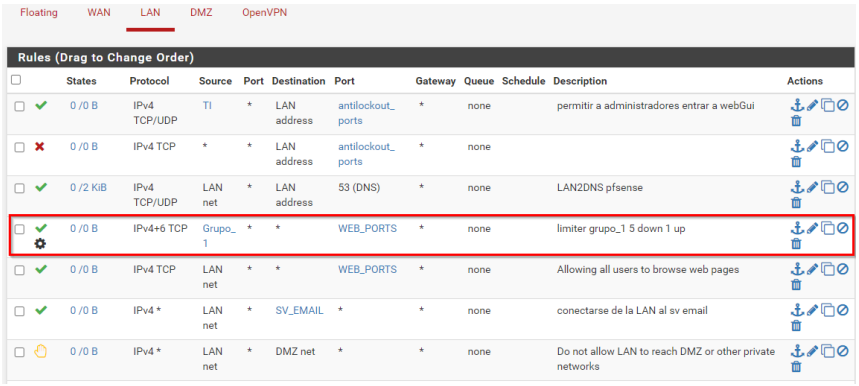


Figura 6.15: Alias para las direcciones del limiter

6.8. Control de tráfico web: Squid, SquidGuard

6.8.1. Configuración de Squid cache

Services>*Squid Proxy Server*>Caché Para guardar caché se realiza la siguiente configuración:

- **Hard Disk Caché size: 5000**. Es lo recomendado por los expertos en pfSense. Para guardar en disco las actualizaciones de Windows.

- **aufs**. Para evitar bloquear las operaciones I/O de otros procesos de Squid.
- **Maximum object Size: 512. (MB)**. Se ha tomado en consideración que se quieren cachear en disco las actualizaciones de Windows. Se puede elevar en caso de observar paquetes de actualización mayores que el tamaño seleccionado.
- **Memory Caché Size: 2000**. Se recomienda usar siempre menos del 50 % de la RAM física. Se tiene que tener en cuenta que Squid usa 14 MBytes de RAM por GB de caché. Se marca la opción de Caché dynamic content para guardar contenido dinámico de las páginas web cuando sea posible.
- **Custom refresh_patterns**: se añade el patrón para guardar en caché las actualizaciones de Windows. Ver Figura 6.16
- **Habilitar Transparent HTTP Proxy** y dejar el resto de opciones con los datos por defecto.
- **Habilitar Bypass Proxy for Private Address Destination** para no interferir con las conexiones VPN.

```
refresh_pattern -i microsoft.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip)
4320 80% 43200 reload-into-ims
refresh_pattern -i windowsupdate.com/.*\.(cab|exe|ms[i|u|f]|
[ap]sf|wm[v|a]|dat|zip) 4320 80% 43200 reload-into-ims
refresh_pattern -i windows.com/.*\.(cab|exe|ms[i|u|f]|[ap]sf|wm[v|a]|dat|zip)
4320 80% 43200 reload-into-ims
refresh_pattern -i avg.com/.*\.(bin) 4320 100% 43200 reload-into-ims
refresh_pattern -i symantecliveupdate.com/.*\.(zip|exe) 43200 100%
43200 reload-into-ims
refresh_pattern -i avast.com/.*\.(vpu|vpaa) 4320 100% 43200 reload-into-ims
refresh_pattern -i avira-update.com/.*\.* 720 100% 10800 reload-into-ims
refresh_pattern -i (download|adcdownload).apple.com/.*\.(pkg|dmg) 4320 100%
43200 reload-into-ims
```

Figura 6.16: Patrón para cachear actualizaciones de Windows

6.8.2. Configuración del modo transparente en Squid

La configuración general de Squid será:

- Habilitar Squid habilitando: **enable squid proxy**.
- Se mantiene habilitado: **keep setting** para mantener entre versiones la configuración y todos los datos referentes a Squid.
- En **proxy interface** se selecciona: LAN y loopback. Son las interfaces de las que el tráfico será interferido por Squid. Loopback es necesario seleccionarlo para usar LightSquid.
- Se habilita **Allow Users on Interface** Para permitir usar el proxy a todos los usuarios de la interfaz seleccionada.

- Se habilita **Resolve DNS IPv4 First**. Para agilizar consultas, es posible que el proveedor no trabaje con IPv6 aún.

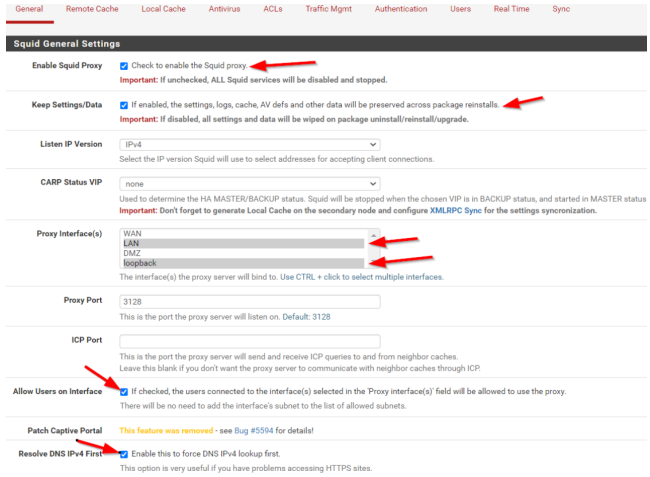


Figura 6.17: Configuración General de Squid 1

En la sección del modo de intercepción se selecciona:

- Habilitar **HTTPS/SSL Interception**.
- Marcar el **modo** de intrusión SSL/MITM Mode como **Splice all**.
- Añadir como Certificado de autoridad CA una nueva entidad certificadora creada desde pfSense para Squid.

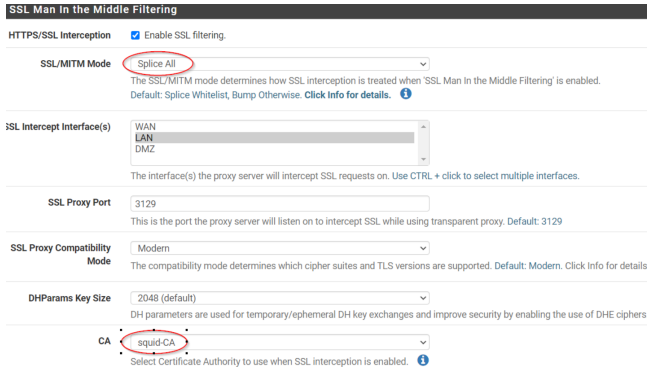


Figura 6.18: Configuración General de Squid 2

Por último se añade una regla de firewall que obligue a los usuarios de la LAN a usar el servidor DNS de pfSense para así tener que pasar por el proxy Squid.

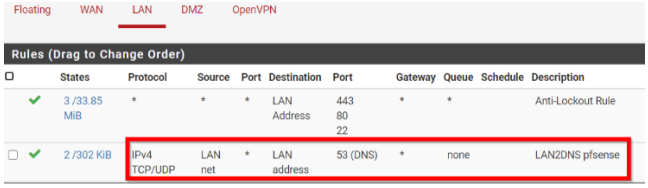


Figura 6.19: Regla para forzar el paso por DNS de pfSense

6.8.3. Configuración de SquidGuard

Se configura SquidGuard para permitir o denegar el acceso a páginas web en función del cliente que realiza la petición y la URL de ésta, bien sea el dominio, la URL completa o palabras contenidas en dicha URL. Para realizar su configuración realizaremos los siguientes pasos:

1. **Añadir una lista negra a SquidGuard:** *Services>Squid Proxy Server*>General settings, en apartado Blacklist options.Se habilita el uso de listas negras. La lista a instalar y usar es shallalist.
2. Se configura el **grupo de usuarios** al que se deshabilitara. Únicamente contiene al usuario de la dirección IP 172.25.1.102.
3. Se configura el **grupo de ACLs** al que se deshabilitara los servicios de categorías de apuestas, agresivo y la página web meneame.net. Ver imagen 6.20. En el caso de la página web se añade una nueva categoría al grupo que se ha descargado de la shallalist. Se crea desde pfSense.

Figura 6.20: Grupo restringido

6.8.4. Configuración de LightSquid

Para crear reportes del historial de accesos web a partir de los logs de Squid configuramos LightSquid. Se configura desde *Status>Squid Proxy Reports*. Opciones seleccionadas de configuración:

- **Lightsquid Web Port: 7445**. Puerto a través del cual se accede a la interfaz web de LightSquid para ver los reportes.
- **LightSquid Web SLL: chequeado**. Para ver el reporte a través de https.
- **User y Password: Los mismos que para pfsense**. Credenciales de acceso a los reportes generados por LightSquid.
- **Report Template Settings:** opciones de configuración de la vista.
- **IP Resolve Method: DNS.**
- **LSkip URL(s):** Aquí se introducen los dominios y direcciones IP que no queremos que se muestren el reporte. Deberán separarse mediante —.
- **Refresh Scheduler: 2 horas**. Periodo de tiempo que tardará en actualizar los reportes de forma automática. Ponemos un valor alto para evitar el consumo de CPU, dado que se puede refrescar manualmente.

6.9. Control del tráfico por capa de aplicación: IDS

Como IDS pasivo se usa Snort. Como reglas para generar alertas se usarán las reglas de la comunidad de Snort. Para ello hay que registrarte en Snort y conseguir un Oinkcode. También se hace uso de OpenAppID para detectar la aplicación a la que pertenece el tráfico rastreado. La configuración general de Snort será la siguiente:

- **Enable Snort VRT:** Se chequea para activar las reglas de Snort VRT o Vulnerability Research Team
- **Snort Oinkmaster Code:** Se pega el Oinkcode para poder realizar la descarga de las reglas.
- **Enable Snort GPLv2:** Se chequea para activar las reglas de la comunidad de Snort
- **Enable ET Open:** Se chequea para activar las reglas de Snort de Amenazas emergentes.
- **Enable OpenAppID:** Se chequea para descargar los detectores de OpenAppID.
- **Enable RULES OpenAppID:** Se chequea para descargar las reglas de OpenAppID.
- **Update Interval:** 1 DAY
- **Hide Deprecated Rules Categories:** chequeado para eliminar reglas obsoletas.

Se activa Snort en la WAN y en la LAN con la política menos restrictiva: Uso de política IPS, Modo conectividad y alerta.

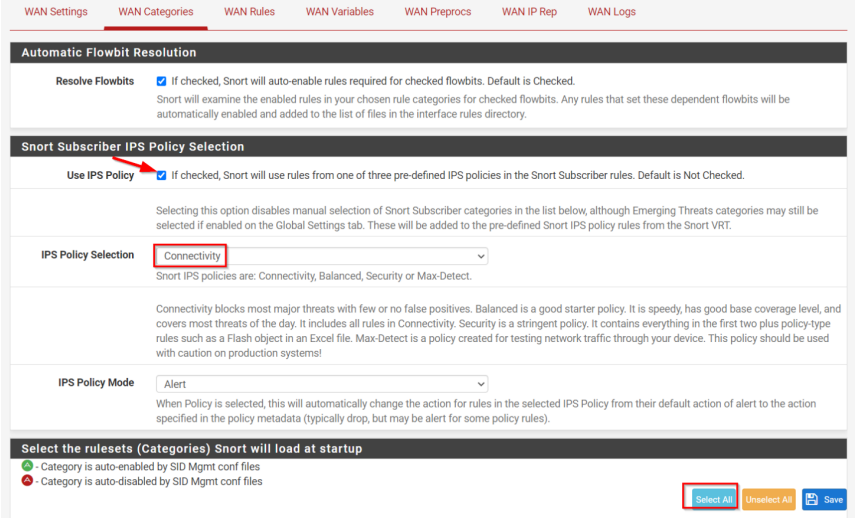


Figura 6.21: WAN configuración Snort

6.10. Bloqueador de malware: pfBlockerNG

La configuración del área pfBlockerNG para el bloqueo en función de listas DNS e IPs es el siguiente:

- **Inbound en WAN** y **Outbound en LAN**.
- **SinkHole** en 172.20.10.1.
- Descarga de las listas: DNSBL_EasyList, DNSBL_ADs, DNSBL_Malicious y pfB_PRI1_v4
- Bajo Firewall>pfBlockerNG>General se cambia la configuración de **CRON** para que actualice las listas **una vez al día**, a las 00 horas, para minizar impacto.
- Bajo Firewall>pfBlockerNG>IP **Enable kill states**: para matar estados de los que se han encontrado conexiones para IPs añadidas a las listas de bloqueo.
- Para pfB_PRI1_v4 se cambia las actualizaciones a 1 vez al día y se configura para que deniegue el tráfico a esas IPs tanto de entrada como de salida.

Para realizar el bloqueo por país hay que configurar Firewall>pfBlockerNG>GeoIP:

Se introduce la licencia **MaxMind GeoIP configuration**:

Figura 6.22: Licencia GeoIP

Para configurar el bloqueo por países se crea una regla usa Deny Inbound, para el listado de Direcciones IP en la lista del país seleccionado. Deny Inbound es la mejor opción ya que los servicios en la DMZ están expuestos, pero un usuario podría querer acceder a algún servicio dentro del rango de IPs del país al que se ha decidido bloquear el tráfico entrante.

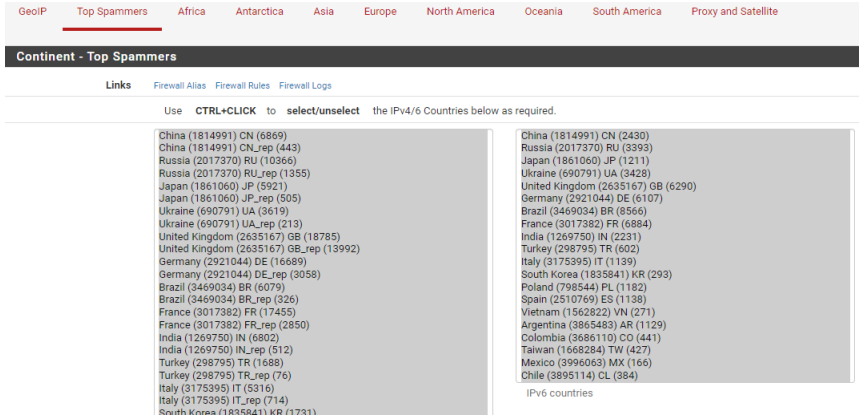


Figura 6.23: Selección de países a bloquear con GeoIP

Capítulo 7

Integración, Pruebas y Evaluación

En este capítulo se hablará de la integración del sistema en el entorno real, los test realizados tanto en el entorno de pruebas como en el real y se realizará una evaluación comparativa del estado de la segura antes de la introducción del nuevo equipo y ahora.

7.1. Integración

La integración del sistema se ha llevado acabo en dos etapas.

7.1.1. Integración: Fase 1

En la primera fase de integración se cubrieron para la empresa todos Casos de Uso a excepción de del UC5, UC21 y U23. Durante esta fase se extrajo la configuración del entorno de pruebas y se importó en el entorno empresarial. Se configuraron parte de las direcciones estáticas necesarias y túneles VPN. En esta fase se dejaron configuradas y activadas las siguientes áreas:

- Interfaces
- Firewall
- NAT
- DHCP
- Conexiones a pfSense HTTPS y SSH.

- Squid
- OpenVPN
- WOL

Durante esta fase Squid se tuvo que afinar el sistema de caché de Squid dado que dificultaba la cargar de contenidos web. Para la integración se ha desactivado el sistema caché de Squid dado que estaba dando problemas a algunos empleados.

7.1.2. Integración: Fase 2

En la segunda fase de integración se cubrieron los Casos de Uso UC5, UC21 y U23. Durante esta fase se reconfiguró manualmente:

- SSH-Agent
- PFBlockerNG
- Snort

Durante esta fase se tuvo que reconfigurar PFBlockerNG porque una de las listas negras no se actualizó correctamente generando el bloqueo de Linkedin. También se tomo la decisión de desactivar las listas de bloqueo por país.

7.2. Test

Las pruebas realizadas para la verificación de correcto funcionamiento del equipo son las siguientes:

TEST 01	
Descripción	DHCP static mapping
Resultado esperado	El usuario obtiene dirección IP estática 172.25.1.102
Resultado obtenido	El usuario obtiene dirección IP estática 172.25.1.102
Validación	OK

Tabla 7.1: TEST 01

TEST 02	
Descripción	Servidor DHCP en LAN da dirección IP
Resultado esperado	El usuario obtiene dirección IP dentro del rango 172.25.1.02-100
Resultado obtenido	El usuario obtiene dirección IP estática 172.25.1.22
Validación	OK

Tabla 7.2: TEST 02

TEST 03	
Descripción	Usuario de la interfaz LAN hace ping al equipo en DMZ (10.10.10.20)
Resultado esperado	El usuario recibe respuesta
Resultado obtenido	El usuario recibe respuesta
Validación	OK

Tabla 7.3: TEST 03

TEST 04	
Descripción	Usuario de la interfaz DMZ hace ping al equipo en LAN
Resultado esperado	El usuario recibe respuesta
Resultado obtenido	El usuario recibe respuesta
Validación	OK

Tabla 7.4: TEST 04

TEST 05	
Descripción	Usuario de la red externa hace ping al equipo en DMZ
Resultado esperado	El usuario recibe respuesta
Resultado obtenido	El usuario recibe respuesta
Validación	OK

Tabla 7.5: TEST 05

TEST 06	
Descripción	Escaner de puertos desde la red externa
Resultado esperado	Puertos abiertos: 25,143,465,587,993
Resultado obtenido	Puertos abiertos: 25,143,465,587,993
Validación	OK

Tabla 7.6: TEST 06

TEST 07	
Descripción	Protocolo HTTPS para el configurador web
Resultado esperado	El usuario se conecta a pfSense mediante HTTPS
Resultado obtenido	El usuario se conecta a pfSense mediante HTTPS
Validación	OK

Tabla 7.7: TEST 07

TEST 08	
Descripción	Conexión a pfSense mediante túnel ssh a través de puttyGen
Resultado esperado	El usuario se conecta
Resultado obtenido	El usuario se conecta
Validación	OK

Tabla 7.8: TEST 08

TEST 09	
Descripción	Despertar equipo mediante WoL
Resultado esperado	El equipo se enciende
Resultado obtenido	El equipo se enciende
Validación	OK

Tabla 7.9: TEST 09

TEST 10	
Descripción	Reducir el ancho de banda de un usuario a 1 MB
Resultado esperado	El usuario recibe un máximo de ancho de banda de 1 MB
Resultado obtenido	El usuario recibe un máximo de ancho de banda de 1 MB
Validación	OK

Tabla 7.10: TEST 10

TEST 11	
Descripción	Conexión mediante openvpn al equipo de la red interna 172.25.1.22
Resultado esperado	El usuario se conecta
Resultado obtenido	El usuario se conecta
Validación	OK

Tabla 7.11: TEST 11

TEST 12	
Descripción	Creación de usuario en pfSense
Resultado esperado	El usuario se crea
Resultado obtenido	El usuario se crea
Validación	OK

Tabla 7.12: TEST 12

TEST 13	
Descripción	Bloqueo de domonio .meneame.net para un usuario de la subred LAN
Resultado esperado	El usuario no puede acceder a la página web
Resultado obtenido	El usuario no puede acceder a la página web
Validación	OK

Tabla 7.13: TEST 13

TEST 14	
Descripción	Sistema caché de elementos web
Resultado esperado	Se han almacendo elementos en /var/squid/cache/
Resultado obtenido	Se han almacendo elementos en /var/squid/cache/
Validación	OK

Tabla 7.14: TEST 14

TEST 15	
Descripción	bloqueo de domonio .meneame.net para un usuario de la subred LAN
Resultado esperado	el usuario no puede acceder a la página web
Resultado obtenido	el usuario no puede acceder a la página web
Validación	OK

Tabla 7.15: TEST 15

TEST 16	
Descripción	Importación de una configuración de pfSense
Resultado esperado	La configuración se ha integrado en el equipo exitosamente
Resultado obtenido	La configuración se ha integrado en el equipo exitosamente
Validación	OK

Tabla 7.16: TEST 16

TEST 17	
Descripción	Se ha bloqueado contenido de las listas pfBlockerNG
Resultado esperado	El usuario no ha podido acceder al contenido de la web bloqueada
Resultado obtenido	El usuario no ha podido acceder al contenido de la web bloqueada
Validación	OK

Tabla 7.17: TEST 17

TEST 18	
Descripción	El usuario monitoriza el tráfico mediante los logs de Snort
Resultado esperado	El usuario observa en la lista de logs las apps que generan tráfico
Resultado obtenido	El usuario observa en la lista de logs las apps que generan tráfico
Validación	OK

Tabla 7.18: TEST 18

TEST 19	
Descripción	El usuario externo envia un email a un empleado de la empresa
Resultado esperado	El empleado recibe el email al buzón de su correo de empresa
Resultado obtenido	El empleado recibe el email al buzón de su correo de empresa
Validación	OK

Tabla 7.19: TEST 19

TEST 20	
Descripción	*Hard shutdown* del equipo
Resultado esperado	El equipo se reinicia sin errores
Resultado obtenido	El equipo se reinicia sin errores
Validación	OK

Tabla 7.20: TEST 20

7.3. Evaluación comparativa

Se realiza un escaneo de vulnerabilidades desde la red interna contra pfSense para conocer si se debe cubrir alguna vulnerabilidad del sistema y la mejora frente al antiguo sistema instalado en la red empresarial. La herramienta utilizada para realizar este escaneo es OpenVAS. A partir de una configuración dada devolverá como resultado un informe con las vulnerabilidades, cómo se detectaron, su severidad, etc.

Vulnerabilidad	**Severidad**	**QoD**	**Localización**
TCP timestamps	2.6	70 %	general/tcp

Tabla 7.21: Lista de vulnerabilidades encontradas pfSense

La única vulnerabilidad encontrada ha sido la de la tabla 7.21. Esta vulnerabilidad permitiría, potencialmente, a un atacante conocer el tiempo de funcionamiento o *uptime* del equipo.

Se ha decidido no mitigar esta debilidad por los siguientes motivos:

- TCP timestamps es necesario para el sistema: Desactivar TCP timestamps reducirá el tamaño de las ventanas TCP, afectando al rendimiento del equipo del equipo, especialmente para las conexiones VPN. [57]
- La vulnerabilidad tiene un riesgo muy bajo.

Además de esto se ha realizado un escaneo de puertos desde la red externa, en el que se ha comprobado que únicamente los puertos que se deseaban estaban abiertos hacia el exterior.

Si se comparan las vulnerabilidades del sistema pfSense integrado frente a las mencionadas del antiguo sistema que se disponía en la red empresarial (ver sección 4.6.4), se puede observar que se ha producido una mejora significativa en cuanto a la seguridad de la red.

Capítulo 8

Conclusiones y Trabajo Futuro

En este proyecto se ha mejorado la infraestructura de red de una pequeña empresa, ajustándola a los requerimientos de seguridad actuales. A su vez se ha aportado la funcionalidad necesaria para que los empleados desempeñen su trabajo adecuadamente.

Para realizar esta mejora se ha desarrollado un análisis de la red empresarial con el objeto de encontrar las debilidades y puntos de mejora. En este análisis se llegó a la conclusión de que se debía sustituir el equipo firewall de la red por otro que mitigase las vulnerabilidades de red encontradas y que a su vez cubriese las nuevas necesidades funcionales de la empresa que han ido surgiendo a lo largo de los años.

Con la realización de este proyecto se ha implantado una solución que ha mitigado una serie de riesgos desencadenados por la mala configuración y antigüedad del equipo de la red sustituido:

- **Vulneración de la confidencialidad**:
  - **Problema**: El equipo firewall UTM daba servicios de monitorización de la red interna a usuarios de la red externa sin necesidad de verificación de usuario empleado de la empresa.
  - **Solución**: Con la configuración que se ha realizado en este proyecto sólo los usuarios que se autentifiquen como administrador del sistema tienen autorización para acceder a estos servicios. La comunicación de estos servicios siempre se realiza mediante canales de comunicación seguros.
- **Cuellos de botella**:
  - **Problema**: El equipo sustituido ocasionaba cuellos de botella en la red no solo por su localización sino también debido a que las tarjetas de red no soportan más de 100 MBps, impidiendo aprovechar todo el ancho de banda proporcionado por el ISP.

- **Solución**: El equipo instalado consta de tarjetas de red que soportan hasta 1000 MBps, permitiendo aprovechar el ancho de banda contratado y mejorando las conexiones de red.

- **Vulnerabilidades por software obsoleto**:
  - **Problema**: Se detectaron múltiples vulnerabilidades como consecuencia del uso de software descontinuado.
  - **Solución**: El equipo instalado está en constante desarrollo y permite la fácil actualización del sistema y sus áreas de gestión.

Además de estudiar las vulnerabilidades del antiguo sistema se han realizado los mismo test para el nuevo sistema implantando dando resultados positivos. Tal y como se menciona en la sección 7.3, al contrario que con el antiguo sistema, no se han encontrado vulnerabilidades para la configuración realizada en pfSense que se deban mitigar.

Como ya se ha mencionado previamente también se han cubierto necesidades del cliente, siempre orientadas a la mejora en la seguridad como son: la configuración de OpenVPN para la conexión mediante túneles VPN de usuarios en la red externa que desean acceder a algún servicio en la LAN, además de otras herramientas como son pfBlockerNG o Squid que permiten monitorizar y gestionar el tráfico de la red de forma controlada.

En conclusión, el sistema implantado en este proyecto es robusto, y cubre las necesidades requeridas por el cliente, sin embargo, hay pie a mejoras:

Como mejoras de cara al futuro se propone cambiar la estructura de la red a una que duplique los elementos troncales de la misma para crear redundancia y eliminar así los puntos únicos de falla. Una solución sería crear una arquitectura maestro-esclavo en la que participen 2 equipos pfSense. En caso de quedar fuera de servicio uno de ellos, tomaría el control de la red el otro.

Apéndice A

Adjuntos

Los elementos que se han adjuntado junto con este documento son:

- **Manual_administrador.pdf**: Manual del admistrador.
- **configuracion_firewall.xml**: Configuración de pfSense.
- **CVE_infodesain_Report.pdf**: Reporte de vulnerabilidades infodesain CVE.
- **infodesain_rapido.pdf**: Reporte de vulnerabilidades infodesain Openvas Default.
- **pfsense-report.pdf**: Reporte de vulnerabilidades de pfSense.

Bibliografía

[1] Anton Cabian Muñoz, *se registraron más de 120.000 incidentes, según los datos recogidos por el Instituto Nacional de Ciberseguridad (INCIBE), siendo siete de cada diez ciberataques registrados en España son contra PYMES,* [En linea]. Disponible en: https://fundacioninade.org/sites/inade.org/files/tribuna_rh_acm_01-12-2018.pdf. [Accedido: 10-mayo-2020]

[2] IMT technology version 2.3 http://mirror1.infodesain.com/en/imt.php [Accedido: 10-mayo-2020]

[3] Empresa IMTCloud https://www.imtcloud.com [Accedido: 10-mayo-2020]

[4] *Decálogo ciberseguridad empresas. Una guía de aproximacion para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf [Accedido: 12-marzo-2020]

[5] *Plan Director de Seguridad. INCIBE.* https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf [Accedido: 12-marzo-2020]

[6] *Frameworks for IT management* https://www.academia.edu/3905111/ISO_27001_Information_Security_Management_Systems [Accedido: 12-marzo-2020]

[7] *Código de Derecho de la Ciberseguridad. BOE.* https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173 [Accedido: 12-marzo-2021]

[8] *Cumplimiento Legal - Colección Protege tu emplesa. INCIBE* https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_cumplimientolegal.pdf [Accedido: 12-marzo-2020]

[9] *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas* https://www.boe.es/eli/es/l/2011/04/28/8/con [Accedido: 12-marzo-2020]

[10] *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas* https://www.boe.es/eli/es/rd/2011/05/20/704/con [Accedido: 12-marzo-2020]

[11] *Decálogo ciberseguridad empresas. Amenaza vs vulnerabilidad.* https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian [Accedido: 20-enero-2020]

[12] *Seguridad y Alta Disponibilidad. 1ª Edicion. Alfredo Abad Domingo* [Accedido: 20-enero-2020]

[13] *Guía de ciberataques* https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf [Accedido: 20-enero-2020]

[14] *Ciberamenazas contra entornos empresariales. INCIBE.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberamenazas_contra_entornos_empresariales.pdf [Accedido: 11-febrero-2020]

[15] *Understanding Intrusion Detection* https://iratoon.medium.com/intrusion-detection-part-2-f20052c0b3f0 [Accedido: 20-abril-2020]

[16] *Squid, SquidGuard and Lightsquid on pfSense* https://www.slideshare.net/NetgateUSA/squid-squidguard-and-lightsquid-on-pfsense-23-24-pfsense-hango [Accedido: 15-febrero-2020]

[17] Unified Process http://www.bawiki.com/wiki/Unified-Process.html [Accedido: 17-febrero-2020]

[18] Eclipse Process Composer, OpenUP. https://www.eclipse.org/epf/general/OpenUP.pdf [Accedido: 17-febrero-2020]

[19] *Estudio de remuneración en el sector tecnológico* https://www.michaelpage.es/sites/michaelpage.es/files/estudio_remuneracion_tecnologia_2021.pdf [Accedido: 17-febrero-2020]

[20] Priscilla Oppenheime, *Top-Down Networking Design Third Edition.* Characterizing Large Internetwork [pag. 60]

[21] *Backbone in Networking* https://networkencyclopedia.com/backbone-in-networking/ [Accedido: 3-marzo-2020]

[22] Gary A. Donahue, *Network Warrior, O'Reilly.* Collapsed core [pag. 474]

[23] *GS748Tv5* https://www.downloads.netgear.com/files/GDC/datasheet/en/GS716Tv3-GS724Tv4-GS748Tv5.pdf [Accedido: 3-marzo-2020]

[24] *GS748T* https://www.downloads.netgear.com/files/GS748T_UM_30Oct07.pdf [Accedido: 10-may-2020]

[25] *TL-SG105-108* https://static.tp-link.com/res/down/doc/TL-SG105-108.pdf [Accedido: 3-marzo-2020]

[26] *77* http://www.yuanley.com/index.php?route=product/product&path=306&product_id=110 [Accedido: 20-abril-2020]

[27] *YuanLey switch PoE* http://www.yuanley.com/support/YuanLey%20PoE%20Switch%20User%20Manual.pdf [Accedido: 20-abril-2020]

[28] *TPLINK tlsf1005p* https://www.useip.co.uk/datasheets/6877/tplink_tlsf1005p_5_port_desktop_switch_with_4port_poe.pdf [Accedido: 20-abril-2020]

[29] *Router orange* https://ayuda.orange.es/particulares/adsl-y-fibra/configuracion-e-instalacion/2148-todo-lo-que-debes-saber-sobre-tu-rout [Accedido: 22-abril-2020]

[30] *HP ProLiant DL140* https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=c04282505 [Accedido: 22-abril-2020]

[31] *RTL8139* https://en.wikipedia.org/wiki/RTL8139 [Accedido: 22-abril-2020]

[32] *IMT manual de usuario*, infodesain https://documentos.tech/document/manual-imt-v21.html [Accedido: 25-abril-2020]

[33] *infodesain web* http://mirror1.infodesain.com/es/imt.php [Accedido: 10-mayo-2020]

[34] *CVE Linux* https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/version_id-37054/opec-1/Linux-Linux-Kernel-2.6.18.html [Accedido: 10-may-2020]

[35] *CVE* https://cve.mitre.org/about/index.html [Accedido: 10-mayo-2020]

[36] *CVSS métricas* https://www.first.org/cvss/v2/guide [Accedido: 13-mayo-2020]

[37] *OpenVas terminología* https://securityorb.com/general-security/openvas-term-to-know/ [Accedido: 13-mayo-2020]

[38] *Comparativa de firewalls* https://en.wikipedia.org/wiki/Comparison_of_firewalls [Accedido: 13-mayo-2020]

[39] *Top 10 firewalls* https://cybersecuritynews.com/best-open-source-firewall/ [Accedido: 16-junio-2020]

[40] *Comparativa técnica de pfSense contra OPNsense* https://www.firewallhardware.it/en/ipfire[Accedido: 20-may-2020]

[41] *Zeroshell* https://en.wikipedia.org/wiki/Zeroshell [Accedido: 21-may-2020]

[42] *Comparativa técnica de pfSense contra OPNsense* https://www.firewallhardware.it/en/pfsense-vs-opnsense-technical-comparison/ [Accedido: 21-may-2020]

[43] *CVE-FReeBSD Vulnerabilidades* https://www.cvedetails.com/vendor/6/Freebsd.html [Accedido: 1-junio-2020]

[44] *CVE-Linux Vulnerabilidades* https://www.cvedetails.com/vendor/6/Freebsd.html [Accedido: 1-junio-2020]

https://www.cvedetails.com/vendor/17948/Suricata-ids.html [Accedido: 1-junio-2020]

[45] *CVE-Snort Vulnerabilidades* https://www.cvedetails.com/vendor/621/Snort.html [Accedido: 3-junio-2020]

[46] *CVE-Suricata Vulnerabilidades* https://www.cvedetails.com/vendor/17948/Suricata-ids.html [Accedido: 3-junio-2020]

[47] *Comparacion de protocolos VPN* https://restoreprivacy.com/vpn/openvpn-ipsec-wireguard-l2tp-ikev2-protocols/[Accedido: 3-junio-2020]

[48] *Requisitos de Hardware para pfSense* https://docs.netgate.com/pfsense/en/latest/hardware/size.html [Accedido: 4-junio-2020]

[49] *Compatibilidad de harware con freeBSD* https://www.freebsd.org/releases/10.3R/hardware/ [Accedido: 4-junio-2020]

[50] *Datasheet HP ProLiant DL360e Generation 8 (Gen8)* https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=c04128167 [Accedido: 4-junio-2020]

[51] *Descargar pfSense* https://www.pfsense.org/download [Accedido: 10-junio-2020]

[52] *Entendiendo ZFS* https://arstechnica.com/information-technology/2020/05/zfs-101-understanding-zfs-storage-and-performance/ [Accedido: 10-junio-2020]

[53] *TLS/SSL survival guide* http://www.zytrax.com/tech/survival/ssl.html [Accedido: 10-junio-2020]

[54] *Chain of Trust* https://blog.keyfactor.com/certificate-chain-of-trusts [Accedido: 16-junio-2020]

[55] *DNSBL* https://www.dnsbl.info/ [Accedido: 16-junio-2020]

[56] *País orifen más ciberataques* https://as.com/meristation/2017/09/22/betech/1506102670_087509.html [Accedido: 16-junio-2020]

[57] *TCP window* https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/description-tcp-features [Accedido: 21-mayo-2020]