UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Diseño, desarrollo e implementación de una red de área local (LAN) en GA-AUTOTRIM

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Rubén Vivas Alegre

Tutor: Carlos Tavares Calafate

Cotutor: Borja Mantecón Fernández

Curso 2018-2019

A mis padres, por darme la vida.

A mi tío, por descubrirme la informática.

A mi abuela, por enseñarme el significado de luchar.

A mi abuelo, por haber luchado.

A mi familia.

Y al amor de mi vida, por serlo.

La redacción de estas palabras sella el final del presente trabajo. Un trabajo que ha servido para aprender y para experimentar y que, sin duda alguna, ha contribuido a hacer de mí un alumno mejor, tanto a nivel personal como a nivel profesional.

Este trabajo tiene un gran impacto en mí, pues gracias a él he podido tener la oportunidad de desarrollar una idea y trabajar en algo que ha sido realmente ilusionante.

Quiero agradecer este trabajo en primer lugar a la Universitat Politècnica de València y a la Escuela Técnica Superior de Ingeniería Informática por darme la oportunidad de formarme como persona y como profesional. A los diferentes docentes que, a través de mi paso por el grado, han conseguido impregnarme de conocimiento y de sentimiento hacia la informática.

Quiero dar las gracias a la empresa Grupo Antolín-Autotrim S.A.U las facilidades que me han brindado para la realización del proyecto, así como a mis tutores en la empresa: Santi y Borja, que no solo me han ayudado, sino que también me han hecho aprender. Sin esta estrecha colaboración esto no hubiera sido posible.

Hago una especial mención a mi compañero de piso Guille que nos hemos ayudado en todo momento y nos hemos empujado mutuamente para lograr finalizar nuestros respectivos trabajos. También a Carles, Ferran y Juan Ignacio que han hecho que el paso por las aulas haya sido mucho más ameno.

Me gustaría agradecer a Lourdes Peñalver que de forma totalmente desinteresada ha atendido en todo momento mis dudas y me ha ayudado a entender mejor los diferentes aspectos trabajados. ¡Muchas gracias por tu ayuda!

Hay una persona que ha soportado todos mis nervios, mis dudas, mis cambios de opinión y mis prisas, y ella es el amor de mi vida, Lydia, que con toda la paciencia del mundo ha soportado mis noches de insomnio y mi estrés sin dejar de hacerme sentir apoyado.

También quiero agradecer a mi tío, Vicente, que desde bien pequeño siempre me ha transmitido su pasión por este mundo y ha logrado siempre despertar en mí el interés. También a mis padres que siempre me han transmitido los valores por el buen hacer.

Finalmente, debo hacer un enorme agradecimiento a mi tutor, Carlos. No solo me ha ayudado en todo momento a resolver todo tipo de dudas, sino que lo ha hecho con una rapidez y una agilidad que han contribuido en gran parte a que esto hoy sea realidad. ¡Muchas gracias Carlos!

¡Muchas gracias a todos vosotros!

Rubén Vivas

Valencia, 29 de Junio de 2019.

Resumen

En el ámbito de las redes presentes en multitud de Pequeñas Y Medianas Empresas, existen comúnmente multitud de vulnerabilidades en su arquitectura que las vuelve sumamente propensas a recibir ataques. El objetivo principal de este trabajo pretende aprovechar parte de la arquitectura de red presente en la empresa Grupo Antolín-Autotrim S.A.U para transformarla y ampliarla, haciendo uso de diferentes elementos, técnicas y tecnologías en pos de incrementar notablemente la seguridad de la red y proteger los activos de la empresa.

Para poder llevar a cabo el proyecto, se ha realizado primeramente un análisis de riesgos de los activos presentes en la red actual de la empresa para determinar cuáles son las vulnerabilidades principales y los riesgos más propensos a los que están expuestos. Los resultados de este análisis han servido para poder establecer una arquitectura que solvente las vulnerabilidades y proteja los activos de los riesgos destacados mediante el uso de una serie de elementos de seguridad debidamente configurados y de una arquitectura adecuada.

La arquitectura de la red propuesta, junto con la configuración de los diferentes elementos incluidos, ha sido probada en un entorno virtual donde se han realizado una serie de pruebas que demuestran la mejora que se consigue en el ámbito de la seguridad en comparación con la arquitectura actual.

Los resultados de las pruebas realizadas sobre la arquitectura propuesta permiten concluir que es posible mejorar de forma notable la seguridad de la red de la empresa G.A-Autotrim en función de los riesgos a los que está expuesta haciendo uso de una arquitectura segura y de un conjunto de elementos y técnicas que aprovechan en parte la arquitectura actual con una inversión asumible por parte de la empresa.

Palabras clave: arquitectura, red, seguridad, firewall, perímetro.

Abstract

In the scope of the networks present in most Small and Medium Enterprises, there is commonly a multitude of vulnerabilities in their architecture which makes them extremely prone to suffer from attacks. The main objective of this work is to take advantage of part of the network architecture present in the company Grupo Antolín-Autotrim S.A.U to transform and expand it, making use of different elements, techniques and technologies in pursuit of a significant increase in the security of the network, and to protect the assets of the company.

In order to be able to carry out the project, a risk analysis of the assets present in the company's current network was first carried out to determine which are the main vulnerabilities and the most common risks to which they are exposed. The results of this analysis have served to define an architecture that solves the vulnerabilities and protects the assets from the outstanding risks through the use of a series of properly configured security elements and an adequate architecture.

The proposed network architecture, together with the configuration of the different elements included, has been tested in a virtual environment where a series of tests have been carried out to evidence the security improvements achieved in comparison with the current architecture.

The results of the tests carried out on the proposed architecture allow us to conclude that it is possible to significantly improve the security of the G.A-Autotrim company's network depending on the risks to which it is exposed, making use of a secure architecture and a set of elements and techniques that take advantage in part of the current architecture with an investment that can be assumed by the company.

Keywords : architecture, network, security, firewall, perimeter.

Resum

En l'àmbit de les xarxes presents en multitud de Petites i mitjanes empreses, existeixen comunament multitud de vulnerabilitats en la seua arquitectura que les torna summament propenses a rebre atacs. L'objectiu principal d'aquest treball pretén aprofitar part de l'arquitectura de la xarxa present en l'empresa Grupo Antolín-Autotrim S.A.U per a transformar-la i ampliar-la, fent ús de diferents elements, tècniques i tecnologies per tal d'incrementar notablement la seguretat de la xarxa i protegir els actius de l'empresa.

Per a poder dur a terme el projecte, s'ha realitzat primerament una anàlisi de riscos dels actius presents en la xarxa actual de l'empresa per a determinar quines són les vulnerabilitats principals i els riscos més propensos als quals estan exposats. Els resultats d'aquest anàlisi han servit per a poder establir una arquitectura que solvent les vulnerabilitats i protegisca els actius dels riscos destacats mitjançant l'ús d'una sèrie d'elements de seguretat degudament configurats i d'una arquitectura adequada.

L'arquitectura de la xarxa proposada, juntament amb la configuració dels diferents elements inclosos, ha sigut provada en un entorn virtual on s'han realitzat una sèrie de proves que demostren la millora que s'aconsegueix en l'àmbit de la seguretat en comparació amb l'arquitectura actual.

Els resultats de les proves realitzades sobre l'arquitectura proposada permeten concloure que és possible millorar de forma notable la seguretat de la xarxa de l'empresa G.A-Autotrim en funció dels riscos als quals està exposada fent ús d'una arquitectura segura i d'un conjunt d'elements i tècniques que aprofiten en part l'arquitectura actual amb una inversió assumible per part de l'empresa.

Paraules clau: arquitectura, xarxa, seguretat, firewall, perímetre.

Tabla de contenidos

Índice de figuras

Índice de tablas

1. Introducción

1.1. Contexto

El presente proyecto parte la red de área local existente en la empresa GA-Autotrim. Esta empresa cuenta con una red que en su momento no se ideó para las dimensiones que ha adquirido hoy en día. Es por ello, que poco a poco, se ha ido mejorando y añadiendo funcionalidades sin que llegue a poder considerarse una red segura y protegida contra las amenazas existentes en los tiempos que corren.

La red actualmente consta de dos *routers* de entrada, de dos operadores distintos. Por una parte se tiene la red de fibra óptica proporcionada por Movistar, y por otra parte la red 4G proporcionada por la compañía Orange. Estos dos *routers* están conectados a un mismo *switch*. Este *switch* se podría decir que es el núcleo de la red, pues a él se conectan los dos cortafuegos y el resto de diferentes dispositivos. Lo más destacado conectado a este *switch*, son los tres *racks* de *switches* distribuidos a lo largo de la planta, uno de ellos en el almacén, otro en la planta, y otro en las oficinas. La función de estos *racks* es la de albergar varios *switches* estacados y un *patch panel* que va enlazado a las diferentes tomas, por lo que solo se da red a aquellas tomas necesarias.

Adicionalmente, existe un radioenlace creado entre esta planta y otra del mismo grupo (Valplas) situada a 3 kilómetros de distancia, para abastecer de red a dicha planta.

Como se puede comprobar, es una red con una cierta extensión, que carece completamente de zonas diferenciadas, y cuya seguridad se podría ver comprometida en un momento determinado.

1.2. Motivación

Por todos estos motivos, se hace indispensable un buen diseño y una buena arquitectura de la red de área local para, entre otros, poder garantizar una determinada disponibilidad e integridad de la información, así como la seguridad de la red ante posibles ataques.

Personalmente, había diferentes alternativas sobre la temática del presente trabajo, pero en un mundo donde cada vez se almacena más y más información, y donde cada vez estamos más conectados, se hace muy interesante estudiar la forma de diseñar una red de extensión media para proteger dicha información, más aún cuando su arquitectura es menos segura de lo que debiera ser.

En este caso, me atrae especialmente el tema elegido, en primer lugar, por la forma en la que, dependiendo únicamente de la arquitectura de una red, se puede mejorar no solo la seguridad, sino también la disponibilidad y la estabilidad de la misma, y, en segundo lugar, tras haber cursado la asignatura de Seguridad en Redes, donde hicimos un proyecto de asignatura diseñando el perímetro y la seguridad de una red.

Creo que este aspecto de vital importancia para la mayoría de Pequeñas Y Medianas Empresas, en este caso Autotrim, ya que puede ayudarles a proteger los datos de sus clientes, los cuales son muy delicados, y por supuesto los suyos propios, además de mejorar la experiencia del usuario.

Se puede consultar más información acerca del estado actual de la red en el Anexo 1 del presente trabajo.

1.3. Objetivos

Los objetivos que se van a perseguir en el presente trabajo parten de un único propósito: Diseñar, desarrollar e implementar una red de la misma extensión, aprovechando la infraestructura existente, de forma que se garantice un cierto nivel de seguridad e integridad.

En este caso, el Grupo Antolin-Autotrim se va a beneficiar de una mejora en la seguridad de la información que manejan, y los trabajadores disfrutarán de una mejor experiencia de usuario.

Los objetivos que se desean alcanzar en el presente trabajo se pueden resumir de la siguiente forma:

I. En primer lugar, conocer los riesgos mediante un análisis para averiguar en qué puntos de la solución se debe invertir mayor tiempo en función de los activos actuales de la empresa que se desean proteger.
II. En segundo lugar, se busca establecer el diseño y el desarrollo de la solución propuesta, y para ello se espera desarrollar una arquitectura de red por zonas teniendo en cuenta los riesgos reales obtenidos en el análisis de riesgos.
III. En tercer lugar, se espera realizar una posible implementación de la configuración de los *firewall*s y *routers*, en un entorno virtual, para cumplir con los objetivos anteriores.
IV. El último objetivo es, gracias a la consecución de los anteriores, conseguir diseñar una red segura, mejorando la existente, para la empresa Grupo Antolín-Autotrim.

1.4. Impacto esperado

En el presente trabajo se pueden identificar diversos usuarios. El usuario principal, en este caso, son los trabajadores y la dirección de la empresa, pero también existen diferentes usuarios secundarios que se ven afectados por el presente trabajo, como los diferentes operarios que la componen, y el grupo internacional al que pertenece Autotrim.

El impacto que se espera obtener en el usuario principal se ve reflejado en la mejora de su experiencia y en la seguridad de los datos que maneja debido al incremento de la

seguridad en la red, la disponibilidad, y rendimiento de la misma. Se espera una red más rápida, más segura, y más estable, para de esta forma mejorar el rendimiento de la planta y, además, protegerla de posibles amenazas, dado que se trata de un sector de riesgo.

Se verán beneficiados también los trabajadores de planta, que trabajan día a día con los diferentes equipos de producción. Además, los trabajadores de oficina, que verán mejorados los servicios como la telefonía, o el sistema de impresiones.

Indirectamente, también se ve implicada la empresa a nivel de grupo, dado que se va a proteger la información y mejorar el rendimiento de la red entre diferentes plantas.

1.5. Metodología

Comenzando por el objetivo número uno, el primer paso se centra en el análisis de la red. Para ello se va a realizar un análisis de riesgos donde se van a identificar los diferentes activos de la red actual que contienen debilidades, para poder proponer una solución que mejore la seguridad y las prestaciones de la red.

Para cumplir con el segundo objetivo, se va a diseñar y desarrollar la solución, donde se identifican los diferentes nodos que integran la red (*routers*, *switches*, *firewall*s, puntos de acceso, servidores), y también se va a diseñar la arquitectura por zonas que va a adoptar la red, y que viene decidida por la solución que se adopta. Es decir, en este punto se va a establecer una arquitectura de la red y se procede a desarrollarla.

El tercer objetivo, se centrará en la implementación y pruebas de la red diseñada anteriormente. Dado que no es posible llevarlo a cabo en un entorno real, se implementará de manera virtual. Para ello se realizará la configuración de los *firewall*s y *routers* ubicados en la zona más externa, y los *firewall*s de la zona perimetral de la red, junto con las reglas de entrada y salida que proporcionan seguridad a esta zona.

El objetivo final del presente trabajo es conseguir diseñar una red de área local segura, a la altura de las necesidades actuales de la empresa Grupo-Antolín Autotrim, aprovechando la red existente.

1.6. Estructura

El presente proyecto, establece una estructura claramente definida, formada por diversos bloques principales compuestos, a su vez, por diferentes sub-bloques que los completan.

A partir del presente punto, se encuentran las convenciones que se van a adoptar en el proyecto, es decir, diferentes normativas de marcado que se van a llevar a cabo para distinguir citas, palabras extranjeras etc.

Capítulo II: Estado del arte

El capítulo dos trata del estado del arte, donde se va a explicar la situación actual en cuanto a la mejora en la seguridad en redes y que técnicas se suelen emplear. Para completar este punto, se realizará una propuesta, donde se espera detallar brevemente qué se espera mejorar con el presente proyecto, y cuáles son las similitudes con la red que está en funcionamiento actualmente.

Capítulo III: Análisis del problema

El siguiente capítulo es el análisis del problema, donde se espera analizar de forma exhaustiva los riesgos que presenta la red actual, y la seguridad que se emplea, para poder plantear una solución de la forma más apropiada que solvente los riesgos existentes.

Capítulo IV: Diseño y desarrollo de la red

El capítulo cuatro, se centra exclusivamente en el diseño y el desarrollo de la red, de forma teórica, que se obtiene de la solución, es decir, en diseñar un perímetro sólido y las diferentes zonas de la arquitectura. Una arquitectura detallada y explicada desde lo general, hasta lo particular.

Capítulo V: Implementación y pruebas

Este capítulo se enmarca en la parte práctica del trabajo, y se detalla la implementación de la solución; puesto que no se puede realizar en el entorno real, se realizará una simulación de cómo quedarían implementados los *firewall* y los *routers* de forma virtual, entrando en detalle en la configuración de ciertos aspectos como las reglas de los cortafuegos y configuraciones más generales.

Capítulos finales: Presupuesto, conclusión, referencias, anexos y glosario

En los capítulos posteriores se puede encontrar el presupuesto detallado del proyecto, la conclusión del presente trabajo, junto a las referencias, diferentes anexos y el glosario.

1.7. Convenciones

Se van a definir una serie de convenciones que serán utilizadas durante todo el trabajo, para de esta forma facilitar la lectura y la búsqueda de recursos.

En primer lugar, las palabras extranjeras se van a remarcar en cursiva, como por ejemplo, *network*.

Para definir citas de menos de cuarenta palabras en el trabajo, se van a entrecomillar, haciendo énfasis en la cita. Para ello, al final de la cita, se va a indicar el autor, el año, y la página del libro del que se extrae el texto citado.

Para definir citas de más de cuarenta palabras, se insertará la cita separada del resto del texto, y al final se va a indicar el autor, el año y la página del libro citado.

Para aquellas citas parafraseadas, se indicará al principio del texto el autor y el año. En el caso de ser una corporación, también se indicarán las siglas.

Para nombres de dispositivos se hará uso de las mayúsculas y la negrita, como por ejemplo, **AUTSW08010.**

2. Estado del arte

Existen actualmente diferentes propuestas acerca de cómo proteger una red o hacerla más segura para protegerla frente a ataques.

Convery, S. (2004) considera que la seguridad de la red es un sistema. No es únicamente un *firewall*, no es una detección de intrusiones, y no es una red privada virtual. La seguridad no es nada que los sistemas de Cisco o cualquiera de sus socios o competidores puedan vender, ya que si bien estos productos y tecnologías juegan un papel importante, la seguridad de la red es más compleja. Todo comienza, con una política de seguridad.

Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005) aseguran que los sistemas con acceso a Internet (computadoras con direcciones IP a las que se puede acceder desde Internet) reciben entre varios cientos o incluso miles de intentos de ataque cada día, y lanzan la siguiente pregunta: ¿Tiene su organización acceso a experiencia en todos los aspectos de la seguridad perimetral, incluidas redes, *firewall*s, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), redes privadas virtuales (VPN), seguridad de UNIX, y seguridad de Windows?

Alonso, C. G. M., Gabriel, D. O., Ignacio, A. A., & Elio, S. R. (2014) mencionan que, contra los ataques a redes informáticas, se han desarrollado tecnologías informáticas que, como los cortafuegos o la criptografía de comunicaciones, parecen impecables. Dicen que son necesarios, pero hacen hincapié en la prevención, la detección y la respuesta.

Estos autores centran sus textos en diversas políticas de seguridad, en sistemas de detección de intrusos, en *firewall*s, o en la seguridad de los propios equipos que componen la red. Para complementar todas estas técnicas, en las próximas secciones del presente trabajo se diseña una propuesta, la cual se detalla a continuación.

2.1. Propuesta

El marco tecnológico en el que se enmarca el proyecto que se desea llevar a cabo es el de las tecnologías de la información, en concreto, el ámbito de las redes y la seguridad en ellas. Viene justificado por la necesidad de mejorar este ámbito en la empresa para adaptarse a las nuevas necesidades y a los nuevos tiempos.

No se pretende presentar una idea que haga cambiar la totalidad de la red con la que se cuenta actualmente, ya que se pretende aprovechar los elementos disponibles, y añadir otros nuevos cuando sea realmente necesario. Además, se desea llevar a cabo una modificación de la arquitectura general de la red, sin llegar a eliminar completamente la actual. En resumen, es una mejora sustancial de la red existente, pero sin perder su esencia y aprovechando múltiples elementos.

Se va a diferenciar en el número de zonas que integran la red, y se va a mejorar la arquitectura para lograr un mayor aislamiento del exterior, permitiendo lograr una mayor seguridad y disponibilidad de la red.

3. Análisis del problema

3.1. Análisis de riesgos

El siguiente proceso de análisis de riesgos se realiza basándose en la metodología de análisis y gestión de riesgos de los Sistemas de la Información (Magerit 3.0), definido por el Ministerio de Hacienda y Administraciones Públicas (2012), que describe el procedimiento para definir los activos, y una relación de amenazas y vulnerabilidades.

El proceso de análisis de riesgos llevado a cabo se puede dividir en seis fases:

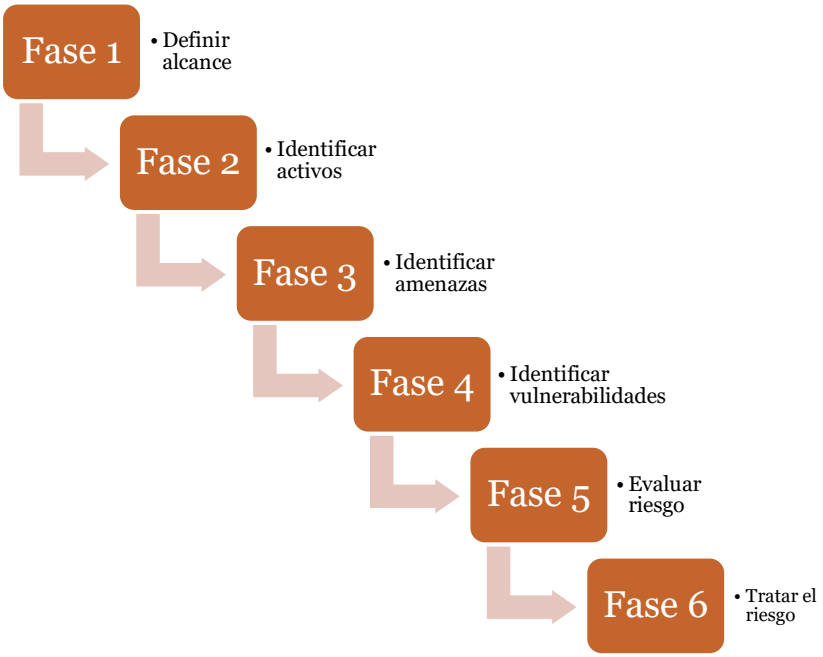

Figura 1. Proceso del análisis de riesgos.

La fase seis del proceso se llevará a cabo en la propuesta de la solución, donde se tendrán en cuenta todos los riesgos a tratar para diseñar la solución.

3.1.1. Conceptos previos

En primer lugar, para poder llegar a evaluar los diversos riesgos, es necesario introducir algunos conceptos previos que se ven a continuación.

En este sentido, se define como activo de la empresa cualquier objeto, bien sea material o inmaterial, a proteger por Autotrim, es decir, cualquier elemento importante para la operatividad y el correcto funcionamiento de la empresa. Teniendo en cuenta que

Autotrim se encuentra ante un entorno industrial, se pueden clasificar los activos de la siguiente forma:

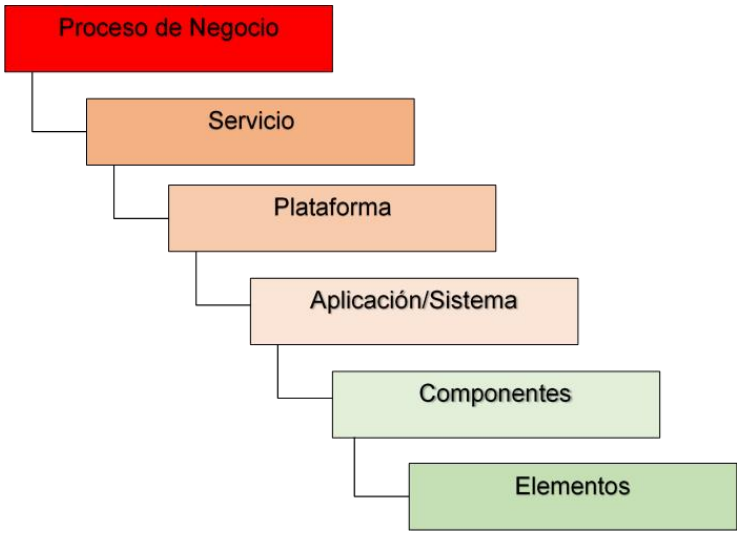

Figura 2. Clasificación de activos.

Cada uno de estos activos posee unos atributos que sirven para calcular el impacto que se produce sobre los mismos. Este impacto es conocido como el porcentaje de pérdida sobre el activo. Los atributos no son más que diferentes propiedades que definen al activo. Los atributos que se pueden encontrar en los diferentes activos de los que dispone la empresa son los siguientes:

Figura 3. Atributos de los activos.

La **integridad** se define como el atributo consistente en que el activo de información no ha sido alterado de manera no autorizada, según norma ISO/IEC 13335-1:2004. Es decir, es muy importante que los datos no sean modificados fuera de control. Estos datos reciben una alta importancia cuando su alteración, bien sea intencionada, o bien sea de forma voluntaria, causa graves daños a la organización. Por el contrario, se considera que son de poca importancia o relevancia cuando su alteración, sea de la manera que sea, no supone ninguna preocupación a la empresa. (MHAP, 2012).

La **disponibilidad** es el atributo de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren, siguiendo la norma UNE 71504:2008. Si un activo deja de estar disponible y tiene una gran repercusión en la empresa, se dice que este activo tiene una gran importancia desde el punto de vista de la disponibilidad; si, por el contrario, no tiene gran importancia si está o no disponible, se dice que carece de valor apreciable. Este atributo afecta a todo tipo de activos. Es frecuente que este atributo requiera de un tratamiento por escalones, pues el coste de la indisponibilidad va aumentando de forma no lineal con la duración de la interrupción, desde una breve interrupción sin importancia, hasta una interrupción prolongada que puede derivar en el cese de la actividad en la empresa. (MHAP, 2012).

La **autenticidad** de los datos es el atributo de los activos consistente en que una entidad es quien dice ser, o bien que garantiza la fuente de la que proceden los datos, según la norma UNE 71504:2008. La autenticidad de los usuarios es lo contrario de la oportunidad de fraude o uso autorizado de un servicio. Si la prestación de un servicio a falsos usuarios supone un grave perjuicio para la empresa, se dice que dice que la autenticidad de los usuarios es de gran importancia. Si, por el contrario, no supone un grave perjuicio, se dice que la autenticidad no posee una elevada valoración desde el punto de vista de la autenticidad. (MHAP, 2012).

El atributo **trazabilidad** es el consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad, siguiendo la norma UNE 71504:2008. Si no quedara una constancia fehaciente del uso del servicio, se abriría las puertas al fraude, incapacitaría a la empresa para perseguir delitos, y podría suponer el incumplimiento de obligaciones legales. (MHAP, 2012).

En un análisis previo se pueden identificar a simple vista diversos activos que posee la empresa, y que posteriormente se tratarán debidamente:

Planos y diseños de los techos que se fabrican
Información sobre empleados (RRHH)
Facturas y cuentas (Administración)
Información de procesos de ingeniería y calidad
Servicios web (Web de inventario, control de racks)
Servicio de control de accesos y fichajes
Servicio de impresiones por cola única
Aplicación de trazabilidad de la pieza en WaterJet y rebordeadoras
Aplicaciones dedicadas a la producción
Paneles-PC
Equipos portátiles
Discos duros
Teléfonos
SAI y sistemas de generación eléctricas

Figura 4. Identificación preliminar de activos.

Otro activo a destacar son los servidores ubicados en el CPD, protegidos mediante control de accesos y sistema anti-incendio, que contienen todos los servidores virtuales sobre los que se ejecutan los diferentes servicios. Estos servidores se pueden definir como uno de los activos principales de Autotrim. Su atributo disponibilidad puede afectar gravemente a los atributos de los diferentes activos de la empresa.

Dado que el objeto de estudio del presente trabajo se basa en la red de área local de la empresa, se van a tomar como activos todos aquellos que estén directamente relacionados con la propia red, puesto que estos activos son los que podrán comprometer, al verse deteriorados por un impacto, la integridad y la seguridad de la red, quedando de esta forma excluidos aquellos activos que se encuentran en la red, pero no participan de forma activa en ella, como equipos portátiles, teléfonos, impresoras y todos aquellos dispositivos que se conecten a la red pero no formen parte de la misma.

Entre todos estos activos se producen numerosas dependencias. Es decir, por ejemplo, la pérdida de un servidor conlleva la pérdida de los atributos disponibilidad de las diversas aplicaciones que dependen de él, pero no afectan a los atributos confidencialidad e integridad.

Estas dependencias, son difíciles de evaluar, y se deben conocer para calcular el impacto que se produce sobre el activo en cuestión.

3.1.2. Actores

Sobre los propios activos aparecen una serie de actores que interactúan de forma directa sobre los mismos, y cada uno de ellos lo hace de una forma diferente, por lo que se procura siempre que estos actores protejan los activos de la empresa. Se distinguen tres actores principales, como se observa a continuación:

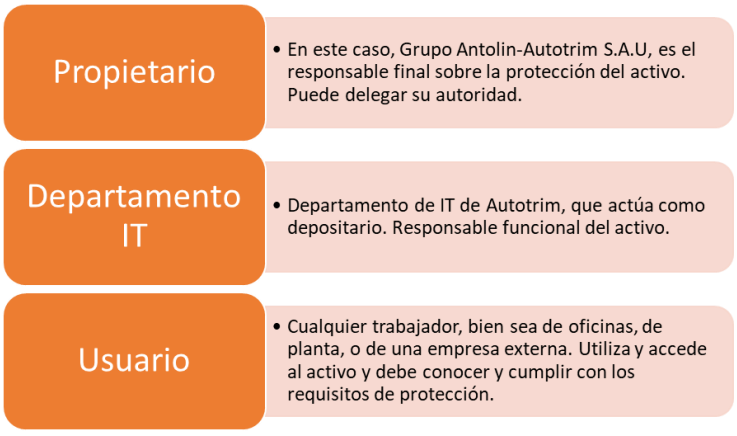

Figura 5. Actores sobre un activo.

Estos actores desarrollan una actividad conjunta de una forma preestablecida. Se establecen una serie de relaciones entre ellos, que en ocasiones resulta tediosa, para evitar comprometer el activo. Esta interacción se detalla en la siguiente figura:

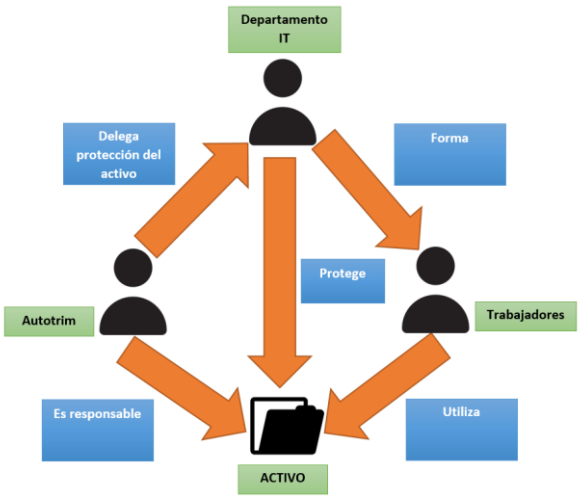

Figura 6. Interacción de los actores.

Sobre un activo se pueden producir diversas amenazas, que son un elemento externo al entorno, normalmente asociado a un evento, que en caso de ocurrir puede desembocar en un deterioro parcial o total del activo. Al tratarse de elementos externos, como bien pueda ser un terremoto, o un desastre natural, no suele ser factible actuar sobre ellas puesto que no se tiene el control sobre ellas.

Es muy probable que los activos posean vulnerabilidades, que no son más que debilidades, en este caso internas al entorno de la información, cuya presencia debilita la seguridad de todos o de alguno de los activos.

Se pretende reducir todo lo posible el número de vulnerabilidades que puedan existir, en este caso, debido a la arquitectura de la red, y de los dispositivos que la componen.

Partiendo de la base de que un riesgo es la contingencia o proximidad de un daño, queda claro que la presencia de una vulnerabilidad va a desembocar siempre en un riesgo sobre alguno de los activos, como se puede comprobar en la siguiente figura:

Figura 7. Proceso de un riesgo sobre un activo.

Dado que tanto si se produce una amenaza, que no es posible controlar, o si existe una vulnerabilidad, se produce un riesgo. Por tanto, se concluye que el riesgo no se reduce, erradica o minimiza, es algo que siempre está ahí, lo que se debe buscar es reducir el impacto, y en ocasiones la probabilidad de ocurrencia. Es decir, nunca se puede eliminar o reducir de forma completa.

3.1.3. Alcance y activos

Para poder realizar un correcto análisis de riesgos, antes de nada, es necesario conocer el alcance de este análisis. En este caso, dado el área sobre el que se basa el presente proyecto, se define el alcance como "Los componentes que forman la red de área local en Autotrim". Se va a analizar cuáles son los posibles riesgos que pueden afectar a la integridad de la red, y por tanto, de los componentes que dependen de ella.

Una vez es conocido el alcance, se identifica de forma concreta y detallada cuales son los activos más importantes de la empresa que guardan relación con el alcance definido. Para ello, se identifican de forma ordenada los diferentes activos, como se observa en la siguiente tabla:

Tabla 1. Activos de la red de Autotrim.

ID	NOMBRE	DESCRIPCIÓN	RESPONSABLE	TIPO	UBICACIÓN	CRÍTICO
AC_1	Servidores	Servidores de inicio de sesión aplicaciones, DHCP, ficheros e impresoras	Departamento IT	Redes (Físico)	CPD	SÍ
AC_2	*Firewalls*	Fortigate Fortinet cortafuegos	Departamento IT	Redes (Físico)	CPD	SÍ

AC_3	*Router main*	Puerta de enlace. Acceso a red externa	Departamento IT	Redes (Físico)	CPD	SÍ
AC_4	*Router backup*	Puerta de enlace. Acceso a red externa. Repuesto	Departamento IT	Redes (Físico)	CPD	SÍ
AC_5	*Rack* oficinas	Cajón de *switches* PoE y no PoE	Departamento IT	Redes (Físico)	CPD	SÍ
AC_6	*Rack* almacén	Cajón de *switches* PoE y no PoE	Departamento IT	Redes (Físico)	Almacén	SÍ
AC_7	*Rack* planta	Cajón de *switches* PoE y no PoE	Departamento IT	Redes (Físico)	Planta	SÍ
AC_8	Puntos de acceso inalámbricos	Diferentes APs por la planta	Departamento IT	Redes (Físico)	Planta	NO
AC_9	Medios de impresión	Cola de impresión única	Departamento IT	Redes (No físico)	Servidor	NO
AC_10	Red telefónica	Red de telefonía IP	Departamento IT	Redes (No físico)	Puntos de acceso	NO
AC_11	Cableado fibra óptica	Cableado entre *racks* de planta	Departamento IT	Redes (Físico)	Planta	SÍ

3.1.4. Amenazas

Estos activos están expuestos de forma permanente a diferentes amenazas, por lo que es importante identificarlas. El conjunto de amenazas es amplio y diverso, por lo que se realiza un enfoque práctico y aplicado.

Para identificar correctamente estas amenazas, se dividen según el origen de las mismas, y se evalúa qué atributos de los activos se pueden ver afectados por estas amenazas.

Se seleccionan todas aquellas amenazas que puedan tener un impacto sobre la seguridad de la red de Autotrim, y se excluyen todas aquellas debidas a desastres naturales como incendios o inundaciones, así como todas aquellas relacionadas con fallos de los diferentes componentes o fallos de suministro, dado que, a pesar de que sí influyen en la disponibilidad de la red, no influyen en su integridad y confidencialidad, que es el área que se espera mejorar en el presente objeto de estudio. Aquellas amenazas que puedan generar un impacto sobre los equipos que conforman la red, y que afectan únicamente a su disponibilidad, están detalladas en el Anexo 3.

3.1.4.1. Errores y fallos no intencionados

Fallos no intencionados causados por las personas:

Tabla 2. Errores y fallos no intencionados.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
FNI_2	Errores del administrador	Integridad/Confidencialidad/Disponibilidad	Datos/Servicios/Software/Equipos/Redes
FNI_4	Errores de (re)encaminamiento	Confidencialidad	Servicios/Redes/Software
FNI_5	Errores de secuencia	Integridad	Servicios/Redes/Software
FNI_7	Alteración accidental de la información	Integridad	Datos/Servicios/Software/Redes
FNI_8	Destrucción de la información	Disponibilidad	Datos/Servicios/Software/Redes

3.1.4.2. Ataques intencionados

Fallos deliberados causados por las personas:

Tabla 3. Ataques intencionados.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
AI_1	Abuso de privilegios de acceso	Integridad/Confidencialidad/Disponibilidad	Datos/Servicios/Software/Equipos/Redes
AI_2	Uso no previsto	Integridad/Confidencialidad/Disponibilidad	Servicios/Software/Equipos/Redes
AI_4	Reencaminamiento de mensajes	Confidencialidad	Servicios/Software/Redes
AI_5	Alteración de secuencia	Integridad	Servicios/Software/Redes
AI_6	Análisis de tráfico	Confidencialidad	Redes
AI_7	Intercepción de información	Confidencialidad	Redes
AI_8	Modificación deliberada de información	Integridad	Datos/Servicios/Software/Redes
AI_9	Denegación de servicio	Disponibilidad	Servicios/Equipos/Redes

Se va a prestar especial atención a todas aquellas amenazas que estén directamente relacionadas con la red de área local de Autotrim, es decir, todas aquellas que incluyan el término “redes” en su columna de activos afectados.

3.1.5. Vulnerabilidades

Este punto se encuentra enmarcado en la cuarta fase del análisis de riesgos, y se van a estudiar las características de los activos que componen la estructura de la red de Autotrim, para de esta forma identificar los diferentes puntos débiles. Todas estas vulnerabilidades, puesto que ya están orientadas a los activos que son objeto de estudio, se tendrán en cuenta para plantear una posible solución posteriormente, puesto que a través de dichas vulnerabilidades se podrá materializar una posible amenaza, y, por tanto, producirse un riesgo.

Para estudiar las diferentes vulnerabilidades que están presentes en los activos de la empresa, se muestran en una tabla las ID de los activos, junto a las vulnerabilidades presentes en dichos activos:

Tabla 4. Vulnerabilidades.

ACTIVO	VULNERABILIDAD(ES)
AC_01	Servidores internos conectados directamente al *router* que da a Internet mediante un *switch*.
AC_02	*Firewall*s colgando del *switch* principal, sin diferenciar varias zonas con redes distintas en la arquitectura.
AC_03	*Router* sin IDS/*firewall* activo analizando el tráfico conectado directamente a Internet.
AC_04	*Router* sin IDS/*firewall* activo analizando el tráfico conectado directamente a Internet.
AC_05	*Rack* conectado directamente a la única red existente, que da a Internet.
AC_06	*Rack* conectado directamente a la única red existente, que da a Internet.
AC_07	*Rack* conectado directamente a la única red existente, que da a Internet.
AC_08	Los puntos de acceso se conectan directamente a un conmutador que se encuentra conectado al *router* externo. Fácil intercepción de paquetes que viajan por los APs.
AC_09	Cola de impresión instalada en activo AC_1, lo que puede derivar en una intercepción de los archivos enviados.
AC_10	Red de telefonía enlazada a una puerta de enlace situada en la misma red donde se sitúan los *router* puerta de enlace. Peligro de desviación de datagramas y secuencias.

AC_11	Solo se conectan por fibra dos *racks* al *switch* principal, el resto por cobre. Se pierde en disponibilidad y en velocidad de transmisión.

3.1.6. Evaluación de riesgos

Para cada par activo-amenaza que se pueda producir, se va a estimar la probabilidad de que ocurra, y el daño estimado, según la escala proporcionada en el anexo 2. Para dicha evaluación, solo se seleccionan los activos de tipo red, para de esta forma evaluar únicamente los riesgos que afectan a la red actual.

En este tipo de evaluación, dado que es cuantitativa, el riesgo real de que se produzca una amenaza sobre cierto activo es el resultado de multiplicar la probabilidad de que ocurra con el impacto esperado.

Como se ha comentado anteriormente, para cada par activo-amenaza se va a calcular la probabilidad de que ocurra, el impacto sobre el activo, y, finalmente, la concatenación de ambos determinará el riesgo real.

Para poder establecer un umbral determinado que resuma cuán importante es el riesgo, se debe tener en consideración que el máximo valor de un riesgo posible es 9, y el mínimo es 1. Por esta razón, se establece como umbral el valor 4, es decir, todo aquel riesgo que sea mayor o igual a 4, se deberá tratar. A la hora de tratar el riesgo, se pueden definir diversas estrategias que se resumen en las siguientes cuatro medidas:

- **Transferir** el riesgo→ Derivar el riesgo a un tercero que pueda asumirlo. Por ejemplo, contratar una empresa especializada en el riesgo a tratar.
- **Eliminar** el riesgo→ Eliminar cualquier elemento que no sea de gran relevancia que derive en un riesgo real. Por ejemplo, eliminar el uso de memorias USB a no ser que sea estrictamente necesario.
- **Asumir** el riesgo→ Siempre se debe justificar, pero si en ocasiones el coste de tratar el riesgo es superior a los daños que puede ocasionar, se puede asumir este riesgo.
- **Implantar** medidas→ Es la opción que vamos a tomar en el presente caso de estudio. Se trata de plantear una serie de soluciones y medidas a tomar, en este caso en la red de Autotrim, para prevenir los posibles riesgos.

3.1.6.1. Activo 1

Tabla 5. Riesgos sobre el activo 1.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_1	FNI_2	1	3	3
AC_1	FNI_4	1	3	3
AC_1	FNI_5	1	3	3
AC_1	FNI_7	2	3	**6**
AC_1	FNI_8	2	3	**6**
AC_1	AI_1	1	2	2
AC_1	AI_2	1	2	2
AC_1	AI_4	1	3	3
AC_1	AI_5	1	3	3
AC_1	AI_6	1	3	3
AC_1	AI_7	1	3	3
AC_1	AI_8	1	3	3
AC_1	AI_9	2	2	**4**

El resultado del análisis de riesgos en el activo 1 (AC_1), señala que hay 3 amenazas con un riesgo importante sobre el activo, que en este caso se trata de los servidores centrales ubicados en el CPD de Autotrim. Concretamente se trata de las amenazas que tienen que ver principalmente con la información, es decir, su alteración y/o eliminación, además de la denegación del servicio, es decir, que dejen de estar disponibles.

Esta información, y estos riesgos de importancia, se tendrán en cuenta posteriormente para plantear una posible solución, y elegir la solución final que implante las medidas necesarias para mitigar este tipo de riesgos.

3.1.6.2. Activo 2

Tabla 6. Riesgos sobre el activo 2.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_2	FNI_2	1	3	3
AC_2	FNI_4	1	3	3
AC_2	FNI_5	1	3	3
AC_2	FNI_7	1	3	3
AC_2	FNI_8	1	3	3
AC_2	AI_1	1	3	3
AC_2	AI_2	1	3	3
AC_2	AI_4	1	3	3
AC_2	AI_5	1	3	3
AC_2	AI_6	1	3	3
AC_2	AI_7	1	3	3
AC_2	AI_8	1	3	3
AC_2	AI_9	2	3	**6**

En el presente activo, AC_2, se trata de los *firewall*s de la empresa, otra pieza clave en la red actual de Autotrim, aunque en este caso solo hay una amenaza que produzca un riesgo a tener en cuenta sobre los mismos, y se trata de la denegación del servicio, es decir, que alguien intencionadamente provoque la denegación del servicio, no solo desde dentro de la empresa si no desde fuera de la misma, por lo que será necesario implantar alguna solución que satisfaga el presente riesgo. Este resultado también se tendrá en cuenta en las diferentes propuestas de solución.

3.1.6.3. Activo 3

Tabla 7. Riesgos sobre el activo 3.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_3	FNI_2	1	3	3
AC_3	FNI_4	2	3	**6**
AC_3	FNI_5	1	3	3
AC_3	FNI_7	1	3	3
AC_3	FNI_8	1	3	3
AC_3	AI_1	1	3	3
AC_3	AI_2	1	3	3
AC_3	AI_4	2	3	**6**
AC_3	AI_5	1	3	3
AC_3	AI_6	1	3	3
AC_3	AI_7	1	3	3
AC_3	AI_8	1	3	3
AC_3	AI_9	1	3	3

El activo actual (AC_3), se trata del *router* principal, es decir, de la puerta de enlace que está directamente conectado a la red externa, y que por tanto se va a tratar de un activo realmente crítico e importante. A pesar de solo haber 2 amenazas a tratar, que son la del re-encaminamiento de mensajes hacia una dirección incorrecta, de forma intencionada, los *routers* son un elemento clave en las estructura de la red, y, por tanto, son un elemento muy importante en la solución que se plantee, ya que aporta la ventaja de poder interconectar dos redes, es decir, actuar como nexo entre ambas, cosa que resulta muy interesante para crear distintas zonas.

3.1.6.4. Activo 4

Tabla 8. Riesgos sobre el activo 4.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_4	FNI_2	1	3	3
AC_4	FNI_4	2	3	**6**
AC_4	FNI_5	1	3	3
AC_4	FNI_7	1	3	3
AC_4	FNI_8	1	3	3

AC_4	AI_1	1	3	3
AC_4	AI_2	1	3	3
AC_4	AI_4	2	3	**6**
AC_4	AI_5	1	3	3
AC_4	AI_6	1	3	3
AC_4	AI_7	1	3	3
AC_4	AI_8	1	3	3
AC_4	AI_9	1	3	3

Dado que se trata exactamente del mismo elemento que el anterior, se obtiene el mismo resultado. Se trata de un *router* de repuesto que se activa en caso de fallo del *router* principal.

3.1.6.5. Activo 5

Tabla 9. Riesgos sobre el activo 5.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_5	FNI_2	2	2	**4**
AC_5	FNI_4	1	3	3
AC_5	FNI_5	1	3	3
AC_5	FNI_7	1	3	3
AC_5	FNI_8	1	3	3
AC_5	AI_1	2	2	**4**
AC_5	AI_2	1	2	2
AC_5	AI_4	1	3	3
AC_5	AI_5	1	3	3
AC_5	AI_6	1	3	3
AC_5	AI_7	1	3	3
AC_5	AI_8	1	3	3
AC_5	AI_9	2	2	**4**

Respecto al activo 5 (AC_5), se trata de un *rack* de *switches* localizado en el CPD, que sirve a las oficinas, por lo que a partir de la información que se maneja a través de él, puede llegar a ser algo más crítico que los otros dos *racks*. Es por ello por lo que se encuentran tres posibles amenazas que se deben tratar en la posible solución. La primera de ellas se trata de errores del administrador, en este caso dependen a partes iguales del departamento IT de la empresa y del equipo CGP de la central. Las otras dos amenazas se deben al abuso de privilegios de acceso, es decir, dependiendo de en qué parte de la red se encuentren estos *racks*, se pueda acceder a ellos desde fuera de la red de forma intencionada, lo que conduce a una previsible denegación de servicio. La ubicación de estos *racks* en la propuesta de la solución se tendrá muy en cuenta.

3.1.6.6. Activo 6

Tabla 10. Riesgos sobre el activo 6.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_6	FNI_2	1	2	2
AC_6	FNI_4	1	2	2
AC_6	FNI_5	1	2	2
AC_6	FNI_7	1	2	2
AC_6	FNI_8	1	3	3
AC_6	AI_1	1	2	2
AC_6	AI_2	1	2	2
AC_6	AI_4	1	2	2
AC_6	AI_5	1	2	2
AC_6	AI_6	1	2	2
AC_6	AI_7	1	2	2
AC_6	AI_8	1	2	2
AC_6	AI_9	1	3	3

Como se puede ver el activo actual (AC_6), se trata de un *rack* ubicado en el almacén de materia prima, por donde no circula información excesivamente sensible, por lo que el impacto de alguna amenaza en este *rack* tendría una cierta relevancia, pero en ningún caso se comprometería la información. A pesar de ello, en la red, a este *rack* se le puede llegar a ubicar a la misma altura que el de oficinas, puesto que así se previene de posibles amenazas, aspecto que se verá en la solución.

3.1.6.7. Activo 7

Tabla 11. Riesgos sobre el activo 7.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_7	FNI_2	1	2	2
AC_7	FNI_4	1	2	2
AC_7	FNI_5	1	2	2
AC_7	FNI_7	1	2	2
AC_7	FNI_8	1	3	3
AC_7	AI_1	1	2	2
AC_7	AI_2	1	2	2
AC_7	AI_4	1	2	2
AC_7	AI_5	1	2	2
AC_7	AI_6	1	2	2
AC_7	AI_7	1	2	2
AC_7	AI_8	1	2	2
AC_7	AI_9	2	3	**6**

En este caso, se trata de un caso muy similar al anterior, pues es un *rack* de producción donde la única información que podría tener una mayor trascendencia sería la de la trazabilidad de la producción, con la única excepción de que aquí la

disponibilidad sí tiene una importancia mayor, ya que una denegación de servicio en este *rack* implica la parada del stock de la producción que causaría un paro temporal de las líneas, algo que puede llegar a ralentizar el proceso y a generar ligeros percances. Es por ello que este *rack* se tratará con mayor importancia que el anterior, a pesar de que ambos son similares.

3.1.6.8. Activo 8

Tabla 12. Riesgos sobre el activo 8.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_8	FNI_2	1	2	2
AC_8	FNI_4	2	3	**6**
AC_8	FNI_5	1	3	3
AC_8	FNI_7	1	3	3
AC_8	FNI_8	1	3	3
AC_8	AI_1	1	2	2
AC_8	AI_2	1	2	2
AC_8	AI_4	2	3	**6**
AC_8	AI_5	1	3	3
AC_8	AI_6	2	3	**6**
AC_8	AI_7	2	3	**6**
AC_8	AI_8	1	3	3
AC_8	AI_9	2	3	**6**

El activo con el que se trata ahora (AC_8) se trata de otro de los elementos más críticos de la red, dado que maneja un grueso importante de información. Se extraen numerosas amenazas con un riesgo que supera el umbral establecido. La primera de ellas está relacionada con el reencaminamiento de datos, el cual es muy peligroso en un AP dado que puede significar una pérdida importante de información sensible. El siguiente punto trata del mismo caso, pero intencionado por una persona externa o interna. Las dos siguientes tienen que ver con el análisis del tráfico que circula por ellos, y el último con la disponibilidad de los AP. Para mitigar estos aspectos, se planteará una solución que tenga en cuenta dichas amenazas.

3.1.6.9. Activo 9

Tabla 13. Riesgos sobre el activo 9.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_9	FNI_2	2	2	**4**
AC_9	FNI_4	2	2	**4**
AC_9	FNI_5	1	2	2
AC_9	FNI_7	1	2	2
AC_9	FNI_8	1	3	3
AC_9	AI_1	1	3	3
AC_9	AI_2	2	2	**4**

AC_9	AI_4	1	2	2
AC_9	AI_5	1	2	2
AC_9	AI_6	1	2	2
AC_9	AI_7	1	3	3
AC_9	AI_8	1	3	3
AC_9	AI_9	1	2	2

El activo AC_9 se trata de la cola virtual única de impresión segurizada donde todos los usuarios mandan las impresiones deseadas para posteriormente imprimir desde la impresora conveniente. Es por ello que los errores de encaminamiento y los errores del administrador no intencionados se convierten en un riesgo importante a la hora evitar desviar las impresiones a una fuente desconocida, dado que se puede tratar de información confidencial. Un uso no previsto intencionado puede derivar en un riesgo importante para la información contenida en las impresiones. Por estos motivos, se deberá proponer una solución para evitar al máximo estos riesgos.

3.1.6.10. Activo 10

Tabla 14. Riesgos sobre el activo 10.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_10	FNI_2	1	2	2
AC_10	FNI_4	1	3	3
AC_10	FNI_5	1	3	3
AC_10	FNI_7	1	3	3
AC_10	FNI_8	1	3	3
AC_10	AI_1	1	2	2
AC_10	AI_2	1	2	2
AC_10	AI_4	1	3	3
AC_10	AI_5	1	2	2
AC_10	AI_6	1	3	3
AC_10	AI_7	1	3	3
AC_10	AI_8	1	2	2
AC_10	AI_9	2	2	**4**

El activo AC_10 resume la actividad relacionada con la red de telefonía de VoIP, dado que se trata de una red de telefonía independiente del resto, y cualquier amenaza solo afectará a la voz sobre IP, por lo que no tendrá un impacto elevado salvo en el caso de que afecte de forma intencionada a la disponibilidad, en cuyo caso podrá ocasionar daños importantes al funcionamiento de la empresa. Por eso se estudiará de qué forma se puede integrar esta red de telefonía en la red general de Autotrim para solucionar el riesgo de la denegación del servicio.

3.1.6.11. Activo 11

Tabla 15. Riesgos sobre el activo 11.

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
AC_11	FNI_2	1	3	3
AC_11	FNI_4	1	2	2
AC_11	FNI_5	1	2	2
AC_11	FNI_7	1	2	2
AC_11	FNI_8	2	3	**6**
AC_11	AI_1	1	3	3
AC_11	AI_2	2	3	**6**
AC_11	AI_4	1	3	3
AC_11	AI_5	1	3	3
AC_11	AI_6	1	3	3
AC_11	AI_7	1	3	3
AC_11	AI_8	1	3	3
AC_11	AI_9	2	3	**6**

La conexión por fibra óptica entre los diferentes *racks* (AC_11) conforma otro de los activos más importantes, dado que sin ella los *racks* de producción y almacén quedarían incomunicados de forma rápida y segura. Por lo que los riesgos a tener en cuenta, es decir, aquellos que superan el umbral establecido en 4, son aquellos relacionados con la destrucción de la información que viaja a través de este canal, debido a un uso no intencionado, y un uso no previsto junto a la denegación del servicio por un uso malintencionado, es decir, gastar ese canal para enviar cierta información no deseada, o bien detener este flujo de información, en cuyo caso, se produciría un riesgo de dimensiones importantes a tener en cuenta por la empresa.

3.1.7. Tratamiento

Sobre estos activos se ha analizado cuales son las amenazas posibles a las que están expuestos, las cuales serán de gran utilidad para la decisión de qué arquitectura se tomará como solución. El análisis de las amenazas también ha servido para poder calcular, a partir del impacto y la probabilidad que tienen, el riesgo, el cual se ha evaluado de forma cuantitativa fijando un umbral a partir del cual merece un tratamiento. En este caso, dado que se pretende diseñar una arquitectura de red adaptada a la empresa, el tratamiento que se pretende dar a estos riesgos es el de implantar medidas para contenerlo.

Se elige este tratamiento puesto que tratar de eliminar estos riesgos, en el entorno automovilístico en el que se trabaja, conectado de forma constante a la red externa, se toma como un suceso imposible.

Dado que el presupuesto en todo lo que respecta a la seguridad se asume por parte de la empresa, se considera que es estrictamente necesario no asumir los riesgos que

pueden llevar a exponer la información de la red, y comprometer de esta forma su disponibilidad e integridad.

De esta solo queda la opción de, o bien trasferir los riesgos a terceros, o implantar mejoras. Por parte de la empresa y del propio Grupo Antolin, los riesgos que afecten a la red de la empresa, y las mejoras que se deban implantar para mejorarlos, se decide que se solucionan desde la propia empresa, evitando de esta forma trasferir a terceros todo lo relacionado con la propia red de área local.

3.1.8. Conclusión

Para concluir, aquellas amenazas que presenten un riesgo real, y afecten a la integridad de algún activo que compone la red, se definen como críticas, pues esos activos tratan con información y datos de carácter personal, bien sea de la empresa o del usuario, y por tanto son de una elevada sensibilidad.

Aprovechando el análisis de riesgos de la red actual de Autotrim que se ha llevado a cabo con anterioridad, se va a prestar especial atención a aquellas tuplas cuyo riesgo es igual o mayor a 4, y que afectan a la integridad, pues es de vital importancia mitigar estos riesgos con garantías para no comprometer información confidencial.

Por todo esto, en la solución propuesta, se va a mantener como un pilar fundamental la protección de los datos, evitando comprometer cualquier tipo de información sensible.

4. Diseño y desarrollo de la solución

El presente capítulo va a definir, desde un punto de vista teórico, cuáles son las características que debe incorporar la arquitectura propuesta. También se va a explicar cuál va a ser el funcionamiento de la arquitectura, y qué se espera de los diversos componentes que la van a conformar, así como del hardware que se va a emplear.

4.1. Solución propuesta

4.1.1. Riesgos

Para diseñar una solución que mitigue aquellos riesgos destacados que se han obtenido previamente en el análisis de riesgos, es necesario conocerlos más a fondo. Para ello, se resume en la siguiente tabla cuales son aquellos riesgos para los que hay que implantar medidas, y por tanto a tener en cuenta en el diseño de la red:

Tabla 16. Riesgos destacados.

ACTIVO	AMENAZA	RIESGO
AC_1	FNI_7	6
AC_1	FNI_8	6
AC_1	AI_9	4
AC_2	AI_9	6
AC_3	FNI_4	6
AC_3	AI_4	6
AC_4	FNI_4	6
AC_4	AI_4	6
AC_5	FNI_2	4
AC_5	AI_1	4
AC_5	AI_9	4
AC_7	AI_9	6
AC_8	FNI_4	6
AC_8	AI_4	6
AC_8	AI_6	6
AC_8	AI_7	6
AC_8	AI_9	6
AC_9	FNI_2	4
AC_9	FNI_4	4
AC_9	AI_2	4
AC_10	AI_9	4
AC_11	FNI_8	6
AC_11	AI_2	6
AC_11	AI_9	6

En esta tabla se muestra un resumen de todos los riesgos que requieren tratamiento surgidos tras el análisis de riesgos llevado a cabo anteriormente. Es por ello que van a ser de vital importancia en el diseño de la solución y en la arquitectura de la red que se va a proponer a continuación.

4.1.2. Solución

Para aquellas amenazas que tengan que ver con los privilegios administrativos de los diferentes dispositivos que componen la arquitectura, se debe tomar la decisión de crear un único usuario administrador para cada dispositivo, para evitar un uso no previsto y un abuso de privilegios. Por esta razón se va a establecer una política de renovación de contraseña mensual, pudiendo incluso ser semanal, para reducir el riesgo en el caso de que la contraseña sea compartida con personal no autorizado. Lo que se pretende es que una única persona posea la clave de administrador, y que además se deba renovar con cierta periodicidad.

Las amenazas que tienen que ver con la alteración de secuencias, intercepción de las mismas o análisis del tráfico, requieren una arquitectura en la que haya mínimo cuatro equipos con un IDS/IPS en función del dispositivo. En este caso, como estarán basados en la red serán NIDS (Network IDS) en el caso de optar por el sistema IDS, cuya función es la de, mediante el uso de unos sensores virtuales, analizar, comparar y registrar la totalidad del tráfico que circula por el dispositivo en el que se haya configurado. De este análisis se puede comparar el resultado con firmas de ataques bajo sospecha, así como comportamientos anómalos incluyendo exploración de puertos o paquetes malformados. Donde más importancia cobran los IDS/IPS es en los *firewall*s que actúan como puerta de enlace, dado que todo el tráfico debe pasar obligatoriamente por ellos. De esta manera, combinan el poder de la inteligencia para detectar anomalías en paquetes con el poder del *firewall* para bloquearlos antes de que accedan a la red.

Para todas aquellas amenazas relacionadas con el (re)encaminamiento de paquetes e información, se toma la decisión de desarrollar una arquitectura en tres zonas, es decir, una zona roja, próxima a Internet, que presenta mayor riesgo, una zona amarilla, intermedia, que presenta un riesgo medio, y una zona verde, compuesta por la red interna de la empresa, que se espera que sea muy segura, donde cualquier actividad sospechosa debe ser neutralizada al instante. Para conseguir esto, cada zona contará como mínimo con una red distinta, por la que habrá que encaminar correctamente el tráfico deseado entre ellas, evitando así un desvío de paquetes anómalo dado que, para desviarlo, habrá que atravesar diferentes redes, lo que complica la labor del atacante.

En lugar de utilizar un *router* como nexo entre las tres zonas, se pretende utilizar dos *firewall*s Next Generation de capa tres, que poseen todas las funcionalidades de un enrutador común, y además añaden un sistema IPS, más allá de las propias funcionalidades de un cortafuegos en sí. El cortafuegos ***front-end*** poseerá además una red desmilitarizada en unas de sus interfaces, donde irá conectado un servidor DNS, para que pueda ser accedido desde cualquier extremo de la red.

Se va a contar con un equipo dedicado únicamente a la monitorización de la red comprendida entre los dos *firewall*s, funcionando como un HIDS (Host IDS) y NIDS, buscando anomalías en los diferentes hosts de la red además de en la propia red.

De esta forma, se espera que todo el tráfico que circule de forma entrante pueda ser completamente analizado, comparado, registrado, y posteriormente bloqueado, en caso de ser sospechoso. Primero con los *firewall*s software y los sensores IDS de los *routers*, posteriormente con los *firewall*s hardware y los sensores IPS, y finalmente por el equipo de monitorización con el HIDS y el NIDS, asegurando de esta forma que no existe tráfico sospechoso entrante a la red interna, y tampoco en los equipos de la misma.

4.2. Arquitectura de la red propuesta

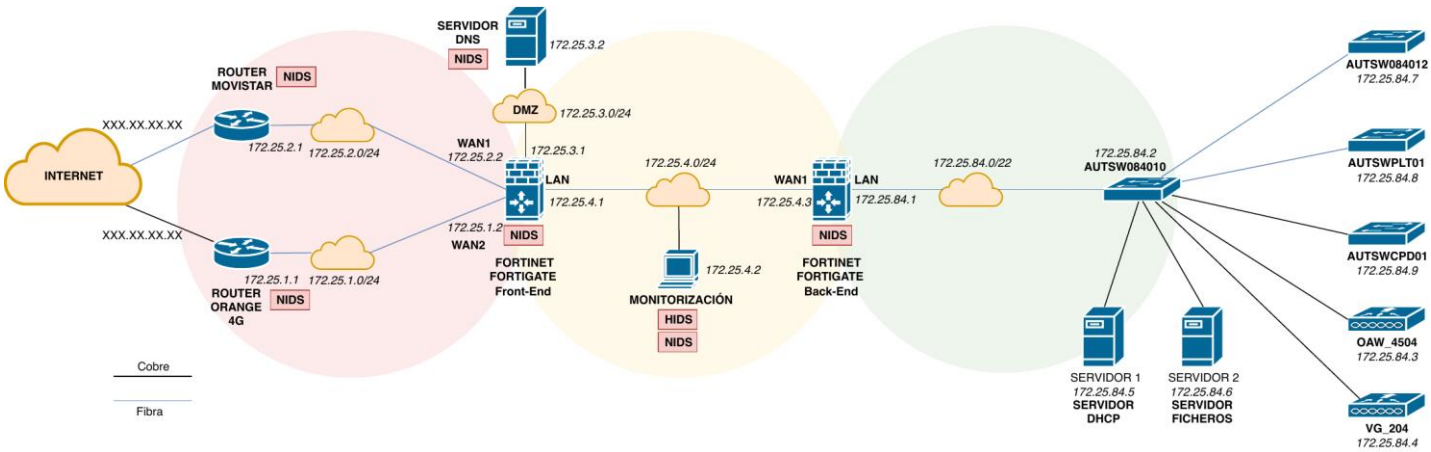

Figura 8. Arquitectura de red propuesta por zonas.

La anterior figura describe la arquitectura obtenida como solución, que se presenta con mayor detalle en el anexo 4.

Se proponen hasta cinco redes distintas, en tres zonas que se verán posteriormente, para aislar cada vez más los dispositivos a proteger.

La primera zona está directamente expuesta a Internet, y por tanto va a ser la más peligrosa. La segunda zona es una zona intermedia que estará expuesta a amenazas, aunque en menor medida. La última zona es la red interna, y es la más segura. Se espera que esta zona mitigue todos aquellos riesgos a los que estaba expuesta anteriormente.

Se puede observar que conserva una parte de la arquitectura anterior, pues a partir del *switch* **AUTSW084010**, se conserva la misma estructura de la red actual de Autotrim.

El objetivo de la arquitectura no se centra en la parte interna de la red, la zona verde, pero sí en todo lo que hay hasta alcanzar dicha red interna. Concretamente, en todas

aquellas zonas que hay que atravesar para lograr mitigar aquellos riesgos extraídos del análisis realizado con anterioridad.

En este proyecto, se pretende trabajar en profundidad en la zona roja, y sobre todo en la amarilla, porque son las que van a determinar el nivel de seguridad de la red resultante, y son las que se van a encargar de soportar todos los posibles ataques, ya que se espera que en la zona verde no se produzca ningún tipo de anomalía. Esta organización por zonas se estudiará con detenimiento más adelante.

4.3. Diseño detallado

4.3.1. Hardware

Después de conocer la arquitectura de la red, queda saber qué es cada uno de los componentes de la misma, y cuáles son sus funciones. Para ello se va a realizar un estudio para decidir qué dispositivos son idóneos para las necesidades detectadas.

Para detallar el hardware empleado en la arquitectura propuesta, se va a comparar, para cada tipo de dispositivo, dos o tres opciones diferentes en función de sus puntos fuertes, sus puntos débiles, y el precio, empezando por la zona roja, y acabando por la zona verde.

4.3.1.1. Router

Tabla 17. Tabla comparativa para el elemento router.

MARCA	MODELO	PROS	CONTRAS	PRECIO
Mikrotik	CCR1036-8G-2S+EM	Puertos SFP+, interfaz de configuración visual, simulación virtual gratis. 8GB de ram. Toma de corriente redundante.	Menor compatibilidad con otros dispositivos de otras marcas.	**1.115,72 €**
Cisco	4331	Puertos PoE.	4GB de ram, sin forma de virtualizarlo, sin toma de corriente redundante.	1695,57€

Para los *routers* de ambas redes, se decide gastar la marca Mikrotik por varias razones, entre las que figuran las siguientes ventajas: Dispone de imágenes para

máquinas virtuales de forma gratuita con el sistema operativo *Router*OS propietario de la marca, y que viene en el núcleo de la familia de enrutadores que ofertan. Esto supone una ventaja a la hora de poder realizar pruebas de forma virtual sin poner en riesgo la red, pudiendo realizar mejoras directamente cuando ya han sido probadas de forma simulada. La segunda ventaja también viene relacionada con el sistema operativo *Router*OS que utilizan, y es su gran sencillez, a la par de completo y útil, permitiendo trabajar con los IDS (logging) de forma profesional. A estos hechos se suma que poseen una toma de corriente redundante. El modelo es el CCR1036-8G-2S+EM, y gracias a los puertos SFP+, permite alcanzar grandes velocidades de trasmisión mediante fibra óptica. Además incorpora 8GB de memoria RAM, por lo que se convierte en una opción ideal para que siempre estén disponibles y resolver con solvencia cualquier tipo de sobrecarga. Además de estos factores que le dan ventaja sobre su competidor Cisco, existe la diferencia de precio, puesto que la opción del fabricante Mikrotik es más barata.

4.3.1.2. Firewall front-end

Tabla 18. Tabla comparativa para el elemento front-end.

MARCA	MODELO	PROS	CONTRAS	PRECIO
Fortinet	Fortigate 600E	Protección contra amenazas de 7Gbps, Puertos SFP+ y SFP.	Una sola fuente de alimentación.	**6240,00€**
Cisco	FirePower 2120	Capacidad multiservicio.	Protección contra amenazas de 3Gbps. Una sola fuente de alimentación.	13346,16€
Fortinet	FortiGate 500E	Puertos SFP+ y SFP.	Protección contra amenazas de 4.7Gbps. Una sola fuente de alimentación.	5166,68€

El primer *firewall*, que hace de nexo entre la zona roja y amarilla, llamado ***front-end***, va a suponer una mejora sustancial respecto a los que se gastan actualmente, y va a ser de mayores prestaciones que el segundo. El motivo radica en las mejoras que ofrece en la velocidad de protección y de inspección, y es por ello que, tras explorar diversas alternativas dentro de la marca Fortinet y Cisco, se elige el modelo Fortigate 600E, dado que también dispone de puertos SFP+, lo que será perfecto para poder conectar los *routers* mediante fibra óptica a máxima velocidad, lo que se traduce en disponibilidad. También incluye una mejora en cuanto a la velocidad de procesamiento, alcanzando velocidades de protección de amenazas de hasta 7Gbps, y velocidades de inspección de paquetes de hasta 8Gbps.

Como aspecto negativo, solo posee una única fuente de alimentación, aunque es expansible a dos de forma modular. Dado que posee un precio intermedio entre los tres propuestos, y que para la zona en la que se encuentra se requiere una velocidad de protección algo superior al ***back-end***, se considera ideal para la función que va a desempeñar.

Destacar que el modelo de Cisco dobla el precio para ofrecer unas características similares o incluso inferiores, y es por ello por lo que se descarta desde un principio.

4.3.1.3. Firewall back-end

Tabla 19. Tabla comparativa para el elemento back-end.

MARCA	MODELO	PROS	CONTRAS	PRECIO
Fortinet	FortiGate 500E	Puertos SFP+ y SFP.	Protección contra amenazas de 4.7Gbps, Una sola fuente de alimentación.	**5166,68€**
Fortinet	FortiGate 400E	Protección contra amenazas de 5Gbps	Una sola fuente de alimentación, sin puertos SFP+.	4666,33€
Cisco	FirePower 2110	Capacidad multiservicio.	Protección contra amenazas de 1.9Gbps, Una sola fuente de alimentación.	4704,54€

En el segundo de los *firewall*s, el ***back-end***, se va a emplear un modelo inferior, el 500E, que reduce ligeramente las velocidades de amenazas e inspección respecto al ***front-end***, pero sigue conservando las interfaces SFP+ para conectar los dos *firewall*s mediante fibra óptica. Se elige esta reducción en el modelo pensando en que el *firewall* del ***front-end*** es el que va a tener más carga de trabajo analizando posibles amenazas, ya que es el que va a absorber todo el tráfico sin filtrar. Sin embargo, el ***back-end*** va a recibir un tráfico que ya ha sido filtrado, por lo que va a tener una carga de trabajo menor, únicamente absorbiendo grandes cargas en el caso de que el primero deje de estar operativo, en cuyo caso seguiría pudiendo responder a las necesidades aunque con menor fiabilidad, hasta que volviera a estar operativo el ***front-end***.

El modelo de Cisco equivalente, a pesar de tener un precio medio, vuelve a quedarse muy atrás en cuanto a velocidad de protección, por lo que las diferencias de prestaciones no compensan la diferencia de precio.

El modelo Fortigate 400E sería el modelo ideal en prestaciones y precio, pero no lleva interfaz SFP+, únicamente SFP. Dado que conlleva una diferencia notable en la velocidad de transmisión, se opta por el 500E, que sí incluye este tipo de interfaz.

Tanto para el ***front-end*** como para el ***back-end***, se decide gastar esta marca en concreto, dado que se trata de unos cortafuegos denominados *Next Generation Firewall* (NGFW), cuyas ventajas radican en que, además de poseer las características tradicionales de un cortafuegos, dan soporte a redes VPN, incorporan IPS, control de aplicaciones, antivirus, o protección contra la denegación de servicios. Por esto, se convierte en la opción ideal dado que se espera realizar el análisis del tráfico mediante los sensores IPS que incorpora.

4.3.1.4. Equipo de monitorización

Tabla 20. Tabla comparativa para el equipo de monitorización.

MARCA	MODELO	PROS	CONTRAS	PRECIO
HP	WorkStation Z4 G4	16GB de ram, SDD	Intel Xeon W Procesador Intel	**2680,99€**
Lenovo	ThinkStation P330	16gb de ram	HDD magnético, Intel i7-8700	2379€
Dell	Precision 7820	Intel Xeon Bronze 3104, Gráfica Radeon Pro WX 2100	8GB de ram, HDD magnético	3008,88€

Para el equipo de monitorización se necesita una alta disponibilidad y una solvencia en el tiempo de respuesta, por lo que se opta por una estación de trabajo de la marca HP, modelo Z4 G4, con procesador Intel Xeon y 16Gb de RAM, preparado para estar siempre en marcha ejecutando los servicios HIDS y NIDS. A pesar de tener un procesador inferior a la opción ofrecida por Dell, tiene el doble de memoria principal y un disco duro de estado sólido que, junto a la memoria principal que incluye, lo hace mucho más solvente, incluso igualando la merma de procesador, a un precio bastante inferior. La opción de Lenovo, a pesar de ser 300€ más barata, dispone de disco duro magnético y un procesador de la familia I7 de Intel, lo que lo hace inferior a las opciones de HP y Dell.

Todo el hardware relacionado con la zona verde de la red se mantiene con el actual hardware, primero porque se ha renovado recientemente mediante un hardware que cumple holgadamente con los requisitos esperados, y, en segundo lugar, porque la seguridad en los dispositivos que conforman esta parte de la red pasa a un segundo plano, siendo el principal objetivo la funcionalidad y estabilidad de la red.

La siguiente tabla resume el hardware de nueva adquisición extraído del análisis comparativo realizado en el presente apartado:

Tabla 21. Resumen dispositivos nueva adquisición.

MARCA	MODELO	TIPO DISPOSITIVO
Mikrotik	CCR1036-8G-2S+EM	*Router* entrada
Fortinet	Fortigate 600E	*Firewall* ***front-end***
Fortinet	Fortigate 500E	*Firewall* ***back-end***
HP	WorkStation Z4 G4	Equipo HIDS.

En el Anexo 1 están disponibles las definiciones de cada componente de la red actual para conocer en detalle cada dispositivo que conforma la red que se va a conservar.

4.3.2. Arquitectura por zonas

¿Por qué se elige una arquitectura por zonas? Pues bien, el principal objetivo es aislar el tráfico en diferentes redes únicamente conectadas entre ellas por dispositivos, en este caso *firewall*s, encargados de detectar y neutralizar posibles ataques. A mayor aislamiento, más complicado se hace que se pueda producir satisfactoriamente un ataque.

De esta forma se puede segmentar el tráfico y analizar los paquetes con mayor precisión. La idea es que, mediante la configuración correcta de los *firewall*s y sus reglas, que se verá en el punto 5.2, el tráfico solo consiga salir de la zona verde hacia Internet, pero no pueda acceder de la zona roja a la red interna. Aquí es donde cobra sentido el uso de la zona desmilitarizada disponible en el ***front-end***. Esta zona DMZ se utiliza normalmente para establecer distintos servicios que deben ser accedidos desde Internet, y además desde la red interna, lo cual conlleva un riesgo considerable; en este caso, esa zona albergará el servidor DNS.

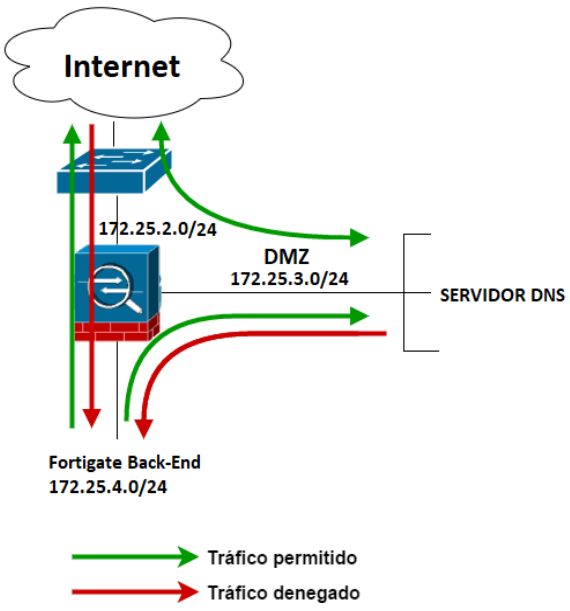

Figura 9. Tráfico con la DMZ.

En la figura 9 se puede ver cómo se van a implementar las reglas en el *firewall*, permitiendo el tráfico al servidor DNS desde la red externa y desde la interna, pero únicamente permitiendo el tráfico de la zona verde hacia afuera.

La arquitectura propuesta incluye diferentes componentes ejecutando un sensor IDS/IPS; estos sensores están estratégicamente situados, en un primer lugar en los *routers* (logging) previos al cortafuegos ***front-end***, dado que en este punto podrán analizar todo el tráfico que circula entre internet y la totalidad de la red, ya que es el único punto por el que se puede entrar un ataque desde el exterior. Este punto también contiene un contra, y es que tanto tráfico sin filtrar generará un ruido que puede afectar al funcionamiento del IDS (logging) e inundará el sistema de falsas alertas, por lo que se debe configurar de forma poco sensible.

El segundo punto donde se propone la ubicación de estos sensores es en el servidor DNS situado en la zona desmilitarizada, que soluciona el problema del ruido, dado que ya recibe un tráfico previamente filtrado por el *firewall*, aunque posee un contra, y es que solo analizará aquel tráfico que el cortafuegos no haya filtrado, por lo que todo el tráfico bloqueado se quedará sin ser analizado por este sensor.

El último punto donde se propone la presencia del IDS es en el equipo de monitorización en forma de HIDS, un sensor de características similares que se encarga de examinar los equipos que componen la red en busca de alteraciones sospechosas, y también en forma de NIDS. Esta ubicación presenta unas características similares a la zona DMZ, y otorga redundancia en el análisis del tráfico para aumentar la protección.

4.3.2.1. Zona roja

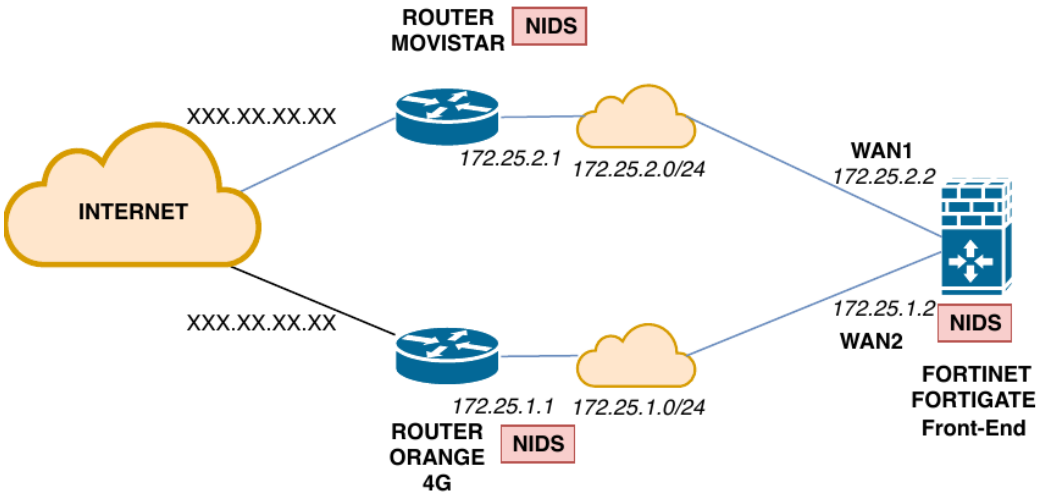

Figura 10. Zona roja.

La zona roja, como se ha mencionado anteriormente, al ser la más próxima a Internet, va a estar expuesta a un mayor número de amenazas. Tal y como se observa en la figura 10, existen dos ISP, es decir, dos proveedores de internet. La explicación de esto radica en la redundancia del acceso a Internet, dado que es posible que en algún momento alguno de los dos proveedores presente algún defecto en la línea. En esos casos siempre se dispondrá de otro proveedor proporcionando el servicio a Internet. Por este motivo, el proveedor principal abastece el servicio mediante fibra óptica, y el segundo de ellos lo hace mediante red de telefonía 4G, pensando en que si la avería es de un tipo, quizás pueda funcionar de otra forma. Esto se explica más adelante.

Para el presente estudio se desconoce las direcciones que proporcionan los ISP, pero sí se da por hecho que son direcciones estáticas. Por esta razón en el apartado 5 de la implementación se supondrán unas direcciones aleatorias para poder realizar pruebas, las cuales se rellenan con los caracteres 'X' en la figura 10.

En esta zona de la red se va a hacer un análisis previo de la totalidad del tráfico con los NIDS incorporados en los *routers*, ya que a través de estos *routers* va a circular todo el tráfico entrante o saliente de la red. Estos *routers*, a su vez, tendrán una reserva hecha con la dirección a asignar a cada interfaz WAN del Fortigate ***front-end***. Es decir, el *router* Mikrotik de Movistar en la dirección 172.25.2.1 tendrá definido en su servidor DHCP un lease estático con la dirección física de la interfaz WAN1 del ***front-end***, y de igual forma se configurará el *router* Mikrotik de Orange en la dirección 172.25.1.1, con una reserva en la dirección 172.25.1.2 para la interfaz WAN2 del ***front-end***.

Estos *routers* van a llevar integrados un mecanismo con unas reglas básicas, es decir, dado que el tráfico saliente ya vendrá filtrado por ambos *firewall*s, se permitirá todo. Sin embargo, para tráfico entrante, se va a restringir para que únicamente se pueda acceder a los servicios del servidor DNS; para ello se establecerán unas reglas que solo permitan conexiones UDP cuyo destino sea el servidor DNS. Esto se hace dado que los *routers* son el primer elemento con el que se va a encontrar un posible atacante, por lo que ha de ser un impedimento desde el primer momento. Se va a configurar una serie de reglas para proteger el *router* desde el exterior, es decir, para que sea imposible acceder al *router* desde la parte WAN, y solo sea accesible desde la LAN, dado que si el atacante consigue acceder al *router*, podría peligrar el resto de la red puesto que podría apagarlo y producir una denegación de servicios entre otros. Estas reglas van a proteger al *router* de los principales ataques conocidos, por lo que solo se debe permitir el tráfico y las conexiones desde la red LAN hacia la WAN y/o el *router*, pero no del propio *router* a la WAN.

Se va a crear una interfaz específica en el ***front-end*** llamada SD-WAN, que no es más que una interfaz virtual que engloba a las dos interfaces de entrada WAN1 y WAN2, y equilibra el tráfico que circula por cada una de ellas, para de esta forma, en caso de que se pierda conectividad hacia Internet en una de ellas, automáticamente el 100% del tráfico circule por la opuesta. Así se consigue redundancia en la conectividad a Internet, sin que la red interna apenas llegue a apreciar cambio alguno cuando se produce el fallo en el abastecimiento de alguno de los dos proveedores de Internet.

Aunque el cortafuegos ***front-end*** sirve de nexo entre la zona roja, la zona desmilitarizada, y la zona amarilla, se va tratar junto al cortafuegos ***back-end*** en la zona amarilla.

4.3.2.2. Zona DMZ

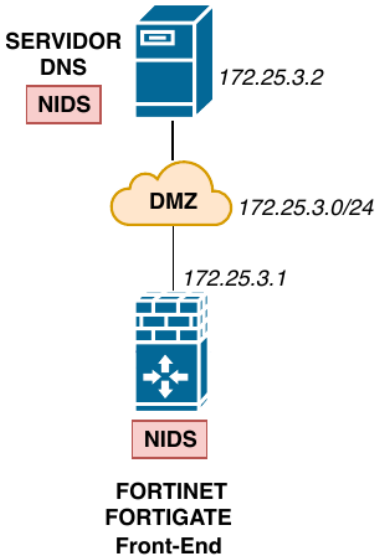

Figura 11. Zona desmilitarizada.

Esta zona, aunque aparente tener un tamaño inferior al resto de las zonas, se considera una zona muy importante, ya que es la única que podrá ser accedida desde la zona verde de la red y desde el exterior. Es por estas características por las que se hace muy interesante situar en esta zona desmilitarizada aquellos servidores que necesiten ser accedidos desde ambos extremos, como en este caso el servidor de DNS.

Para esta zona desmilitarizada se va a emplear una máscara de red 255.255.255.0 (/24); se piensa en una máscara de éstas características pensando siempre en el crecimiento de la red, y las necesidades que puedan aparecer en un futuro.

Para el correcto funcionamiento de esta red, se deben aplicar una serie de reglas en el cortafuegos que permitan el tráfico del exterior al servidor DNS, de la zona amarilla también al servidor DNS. Sin embargo, ningún tráfico debe salir de esta red, para no comprometer la seguridad de la zona amarilla y verde.

El servidor DNS incorpora un NIDS que va a analizar la totalidad del tráfico que circula por esta zona. Este tráfico ya vendrá filtrado desde el *firewall*, por lo que no se captará aquellas amenazas que ya hayan sido bloqueadas.

Nos gustaría pensar que este servidor es un host bastión, una zona bien fortificada, pero cuando se aplica a un host en una red, esto implica fortalecer el sistema operativo y las aplicaciones de acuerdo con las mejores prácticas. (Zeltser, L. et al, 2005, capítulo 1). Por esta razón, este servidor deberá protegerse también de forma autónoma haciendo uso de un cortafuegos propio, y de aquellas técnicas que se consideren necesarias en las aplicaciones que ejecute.

4.3.2.3. Zona amarilla

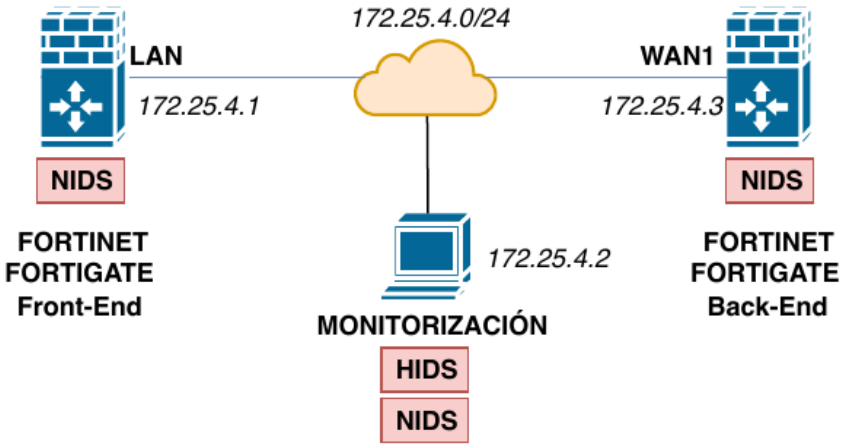

Figura 12. Zona amarilla.

En la figura 12 se muestra la zona amarilla de la red; esta zona, debido a su ubicación entre dos cortafuegos, se define como una zona de riesgo medio, donde es menos probable que la seguridad pueda ser comprometida. La red que conforma esta zona usa la máscara 255.255.255.0 (/24), ya que en este caso el cortafuegos no va a tener el servidor DHCP activado en su interfaz LAN (Internal). Además, la dirección WAN1 del cortafuegos ***back-end*** irá fijada de forma estática en el mismo, y de igual forma para el host de monitorización.

El equipo de monitorización ejecutará un HIDS (Host IDS) y un NIDS para analizar sospechas en los diferentes equipos de la red, además de en la red en sí. Dado que, como se ha mencionado anteriormente, en un principio el tráfico solo va a estar permitido desde la zona verde hacia la zona roja (exterior), se deberá configurar una regla especial en el cortafuegos ***back-end*** que permita a este host acceder a la zona verde para analizar los diferentes hosts que integran dicha zona.

El primer cortafuegos, el ***front-end***, deberá integrar unas reglas menos restrictivas y menos sensibles para evitar falsos positivos, dado que va a absorber la totalidad del tráfico entrante sin filtrar. Por defecto, estos cortafuegos llevan la política de bloquear todo el tráfico, y éste se va permitiendo mediante reglas, según sea necesario. Es decir, una política es una regla que se aplica automáticamente en caso de que no se encuentre ninguna regla para el caso en cuestión. Por esta razón, este cortafuegos llevará establecidas unas reglas menos sensibles. También se deberá tener en cuenta una serie de rutas y políticas de ruta que deriven por defecto el tráfico que circule por la interfaz WAN1 hacia la red 172.25.2.0/24, y el que circule por la WAN2 hacia la red 172.25.1.0/24, con las correspondientes puertas de enlace, que en este caso serán las direcciones IP de sendos *routers*, para que de esta forma el tráfico que circule por la red 172.25.4.0/24 pueda alcanzar otras redes sin problemas.

El segundo cortafuegos, el ***back-end***, al encontrarse en una situación clave como nexo entre la zona amarilla y la zona verde, debe llevar unas políticas más estrictas, dado que aquí el tráfico ya va a llegar filtrado por el primer cortafuegos, y cualquier tipo de tráfico sospechoso debe ser neutralizado en este punto para impedir que acceda a la zona verde, lo cual sería intolerable. Además, este segundo cortafuegos deberá incorporar todas aquellas reglas que posee el primero, así como las exclusivas del ***back-end***. Esta decisión se toma puesto que puede darse el caso de que el ***front-end*** sufra una caída, o sea superado, en cuyo caso el ***back-end*** deberá de hacer funciones de ambos cortafuegos, por lo que es necesario que posea también las reglas del primero. Adicionalmente, habrá que establecer una serie de rutas y políticas de ruta para encaminar el tráfico saliente de la interfaz LAN (internal) a la WAN1, y que, por tanto, la red 172.25.4.0/24 sea alcanzable desde la zona verde, y ese tráfico sea enrutado a través de la puerta de enlace 172.25.4.1, perteneciente a la interfaz LAN (internal) del cortafuegos ***front-end***

4.3.2.4. Zona verde

En la figura 13 se observa la zona más protegida de la arquitectura propuesta, que define lo que se denomina la red interna. Esta zona de la red se mantiene prácticamente igual a la original, y el *switch* **AUTSW084010**, tendrá asignada la IP 172.25.84.2 de forma estática, ya que la interfaz LAN (internal) del cortafuegos ***back-end*** no llevará servidor DHCP asociado que asigne direcciones de forma automática. De este proceso se encargará el servidor DHCP dedicado denominado servidor 1, que estará conectado directamente al *switch* mencionado anteriormente.

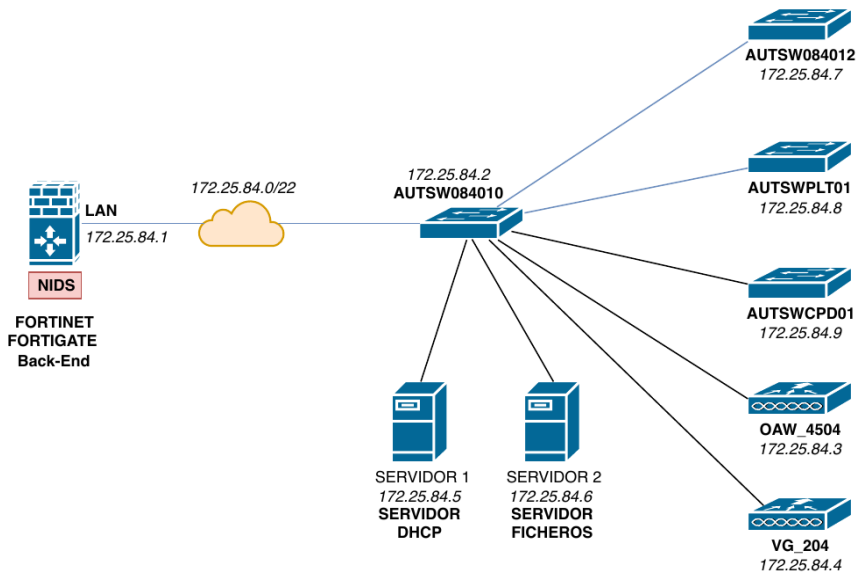

Figura 13. Zona verde.

Además, este *switch* irá conectado los diferentes *racks* de la misma forma que están actualmente, además del conmutador de puntos de acceso y de la puerta de enlace de la voz sobre IP.

El servidor DHCP se mantendrá configurado de la misma forma que hasta ahora: se crearán tres *pools (*grupo de direcciones IP), una en la subred 172.25.84.0/22, otra en la 172.25.85.0/22, y finalmente otra en la subred 172.25.86.0/22. En las dos primeras se asignarán IPs estáticas, pudiendo hacer las correspondientes reservas por direcciones físicas, mientras que la *pool* predefinida para el DHCP será la última, para todos aquellos dispositivos que soliciten una dirección.

En esta zona se debe dar por hecho que no existe ningún tipo de riesgo producido por una amenaza debida a un ataque deliberado contra la integridad de la red. Cualquier amenaza que se produzca sobre un activo en esta zona supondrá un fracaso en la seguridad de la red.

Cabe destacar que el *switch* **AUTSW084010** se enlazará con el ISP prioritario de Movistar directamente por fibra óptica en su totalidad, por lo que se espera que se obtenga mayor agilidad del tráfico, además de una mejor estabilidad. Sin embargo, el tráfico que por necesidad deba salir a Internet por el ISP de Orange dispondrá de conectividad mediante fibra hasta el propio *router*, a partir del cual el tráfico comenzará a viajar mediante la red celular de datos, de menor agilidad y estabilidad. Por todo esto, se va a implementar la arquitectura de forma que la interfaz WAN1 del ***front-end*** tenga mayor peso que la de la interfaz WAN2, siendo esta únicamente utilizada en caso de avería del proveedor principal, Movistar. Gracias al hardware escogido, se van a utilizar puertos SFP+ para la fibra óptica, que mejora considerablemente las prestaciones del antecesor SFP, pasando de una velocidad de hasta 4.25Gbps a una velocidad de hasta 16Gbps.

5. Implementación y pruebas

En este apartado se procede a poner en práctica el diseño de la arquitectura presentado en el capítulo anterior. Para ello se va a representar la zona roja y la zona amarilla de forma virtual, mediante el software de virtualización VMware.

La implementación de la arquitectura, se va a centrar en las capas tres, cuatro y siete del modelo ISO/OSI.

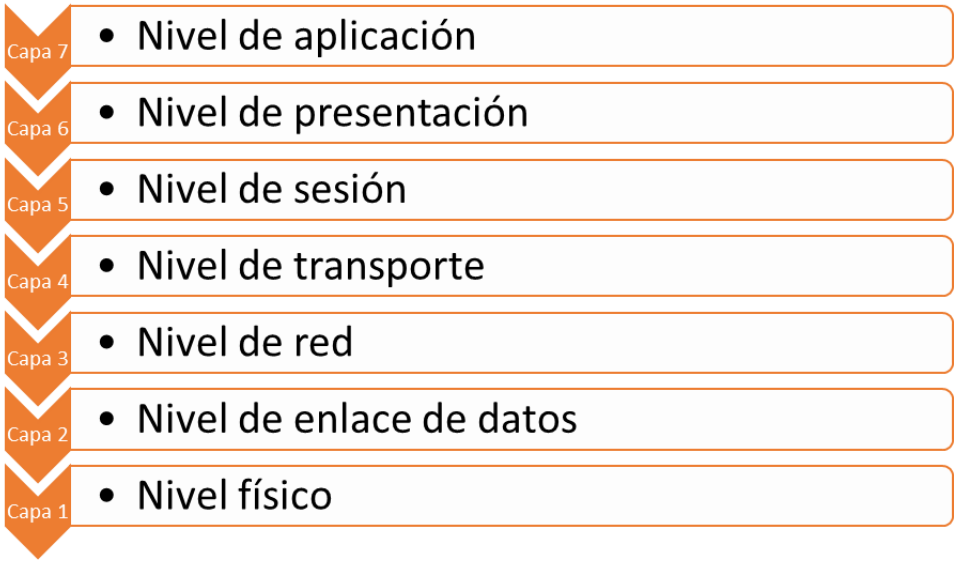

Figura 14. Capas del modelo ISO/OSI.

La capa de red se encarga de identificar el enrutamiento entre redes, es decir, el objetivo de la capa es conseguir que los datos lleguen satisfactoriamente desde el origen hasta el destino. Los dispositivos que se encargan de que esto se produzca, se conocen comúnmente como encaminadores o *routers*.

Los *routers* incorporados en la arquitectura trabajan de forma exclusiva en esta capa, es decir, se encargan únicamente de encaminar el tráfico por el camino correcto, permitiendo el tráfico de datos entre varias redes distintas.

Los dos *firewalls* Fortigate trabajan con la capa tres e incorporan la función routing de encaminar datos, como si de un *router* se tratara, de ahí que se empleen como nexos entre zonas, ya que permiten encaminar correctamente el tráfico de una red a otra. Gracias a esta capa, el dispositivo puede tomar decisiones con la información que obtenga de dicha capa, como filtrado de paquetes por origen, destino, y protocolo, o descarte de paquetes malformados. Adicionalmente, trabaja con la capa cuatro, (nivel de transporte), y funciona con *stateful inspection,* es decir, controla o filtra el estado de las conexiones. Por ejemplo, puede aceptar o rechazar todas las conexiones REPLY, o cualquier información contenida en la cabecera de un datagrama IP.

Además, estos cortafuegos trabajan sobre la capa siete del modelo OSI (Application gateways), lo que significa que, inspeccionan de forma inteligente el contenido de los paquetes, es decir, realizan funciones a nivel de aplicación. Entre otros pueden inspeccionar los protocolos http y https para, por ejemplo bloquear las conexiones HTTP de Rusia. Permiten filtrar por URL y por aplicación, y permiten proteger la red de ataques de denegación de servicio o de inyecciones de código.

Por lo tanto, los *firewall*s usados trabajan con las capas tres, cuatro y siete del modelo OSI, lo que resulta muy interesante para poder detener cualquier tipo de amenaza.

5.1. VMware

Para la implementación de la arquitectura se hace uso de VMware, un potente software de virtualización que permite manejar diversas máquinas virtuales y conectarlas entre ellas mediante el uso de redes virtuales.

En el anexo 5 se puede ver la configuración de las distintas máquinas virtuales en VMware. El objetivo es que, mediante el uso de redes virtuales, se comuniquen correctamente las máquinas emulando de forma virtual la red propuesta. Para ello se configuran las siguientes redes virtuales:

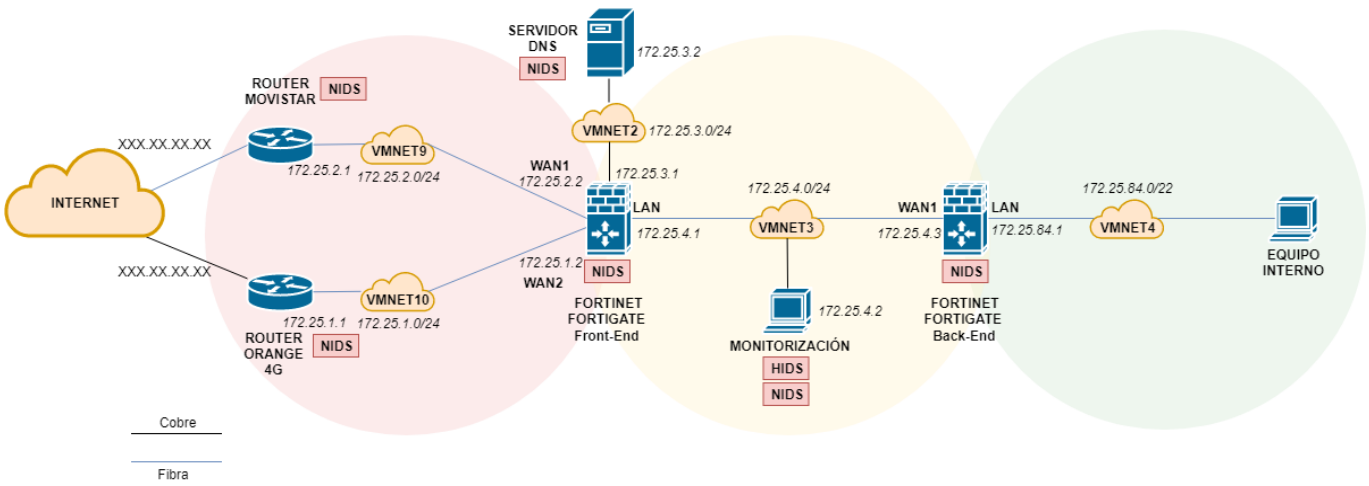

Figura 15. Arquitectura implementada mediante redes virtuales.

Como se observa, la red que conforma la zona verde ha sido reemplazada por un único equipo a fin de realizar pruebas desde esa zona. Esto se realiza debido a que la red interna se conserva en su totalidad respecto al despliegue que está operativo actualmente, por lo que las reglas que se apliquen al equipo interno serán las mismas que se esperan aplicar al resto de la red, sin ningún tipo de distinción.

5.1.1. Routers

A partir de este momento, el *router* que representa la línea de Movistar se va a llamar *router* 2.1, haciendo referencia a su dirección IP. De igual forma, el *router* que representa la línea de Orange, pasará a llamarse *router* 1.1.

Para la configuración general de ambos *routers* cabe destacar algunas consideraciones a tener en cuenta. Primero de todo, dado que se prueba en un entorno virtual, la dirección WAN de cada uno de ellos no se conoce, puesto que no están conectados físicamente a la dirección proporcionada por el correspondiente ISP. Por esta razón, la interfaz WAN de cada *router* se configura desde VMware como NAT, es decir, toman la dirección IP del host anfitrión sobre el que se ejecutan las máquinas, y la traducen a una dirección IP propia.

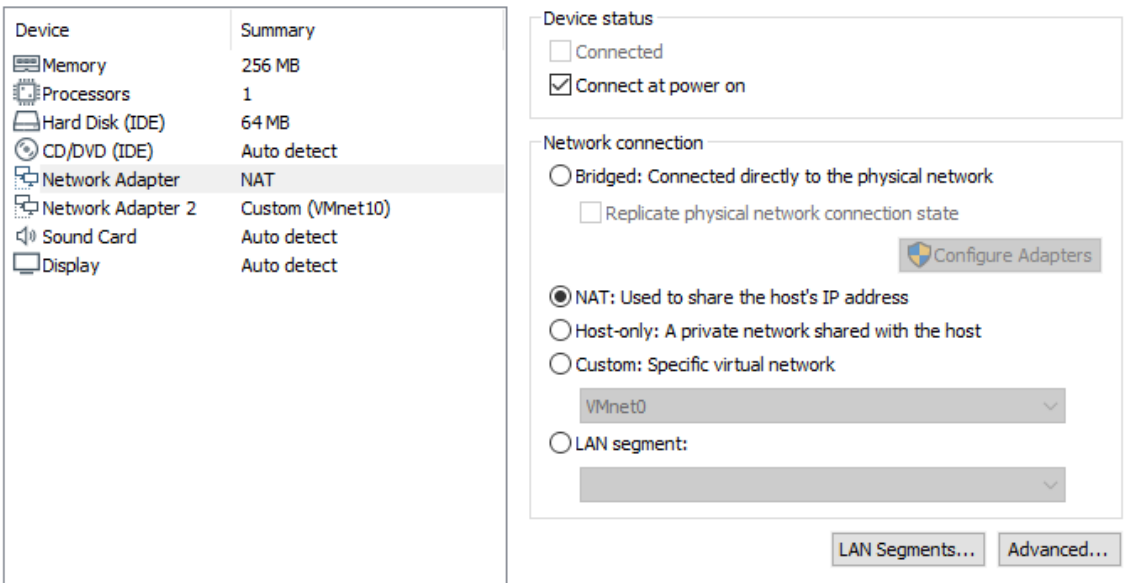

Figura 16. Configuración de interfaz WAN por NAT.

Como se observa en la figura anterior, cada *router* tiene dos adaptadores de red: el primero hace referencia a la interfaz ether1, la WAN, y el segundo hace referencia a la ether2, la LAN. Ambos deben tener la opción "Connect at power on" para que, por defecto, estén encendidos al poner en marcha la máquina virtual.

5.1.2. Front-end

La configuración de la máquina virtual del cortafuegos ***front-end*** difiere de la del ***back-end*** en un aspecto que se va a comentar. Esta máquina va a llevar cuatro adaptadores de red. Cada uno de estos adaptadores representa un puerto físico del *firewall* emulado, por lo que en este caso el primer adaptador representa la interfaz WAN1, el segundo representa la interfaz DMZ a la que se conecta el servidor DNS perteneciente a la zona desmilitarizada, el tercero de ellos enlaza con el equipo de monitorización y el ***back-end***, y por último, el cuarto adaptador representa la interfaz WAN2, donde se conecta el *router* de la línea de Orange 4G.

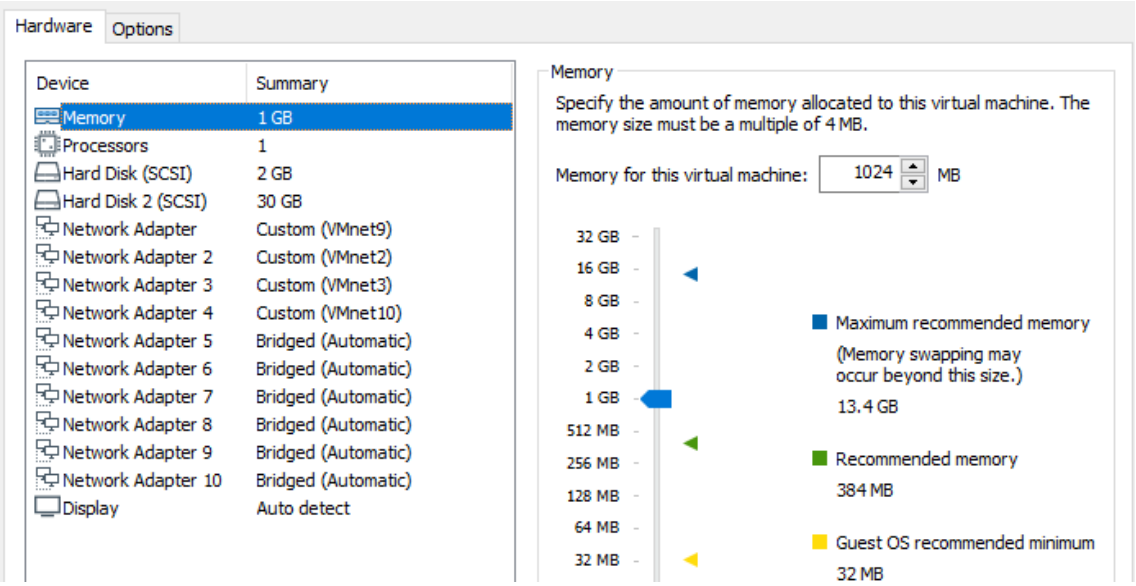

Figura 17. Adaptadores de red en el front-end.

5.1.3. Back-end

Como se ha mencionado anteriormente, este cortafuegos solo va a disponer de dos adaptadores de red, a diferencia del ***front-end***. El primero de ellos va a representar la interfaz WAN1, que recibe el tráfico del primer *firewall*. Por otra parte, el tercero de ellos, representa la interfaz LAN, donde irá conectada la máquina virtual del equipo interno cuya función es la de simular la red interna de la zona verde. El segundo adaptador y el resto de los disponibles se dejan sin encender dado que no se va a hacer uso de ellos.

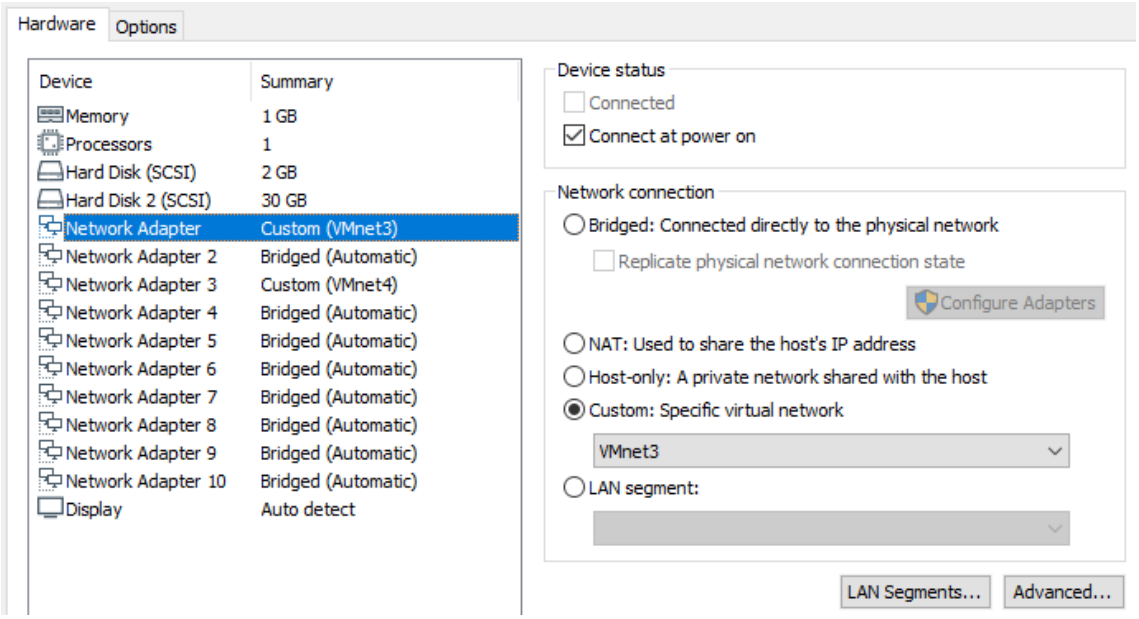

Figura 18. Adaptadores de red en el back-end.

5.1.4. Equipos monitorización e interno

Tanto el equipo empleado para la monitorización de la red, como el equipo interno que se emplea para simular una representación de la red de la zona verde, disponen de una configuración idéntica en los adaptadores de red del software VMware, como se observa a continuación:

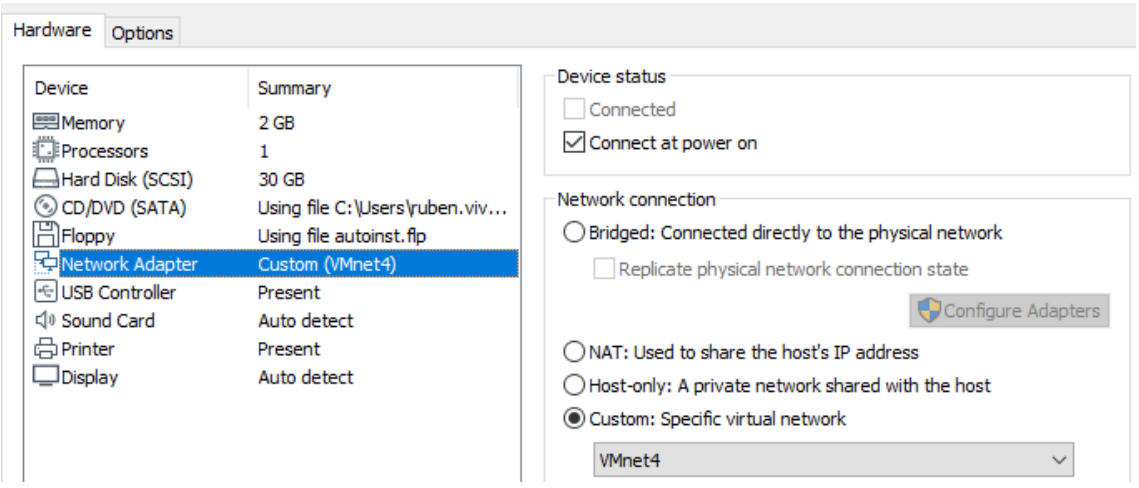

Figura 19. Adaptador de red en los dos equipos.

Únicamente llevan activo un adaptador de red que lo conecta a sus respectivas redes.

5.2. Equipo de monitorización

Este equipo va a ejercer también de NIDS, es decir, se va a emplear un software capaz de analizar el tráfico que circula por la red. Además, se va a ejecutar un HIDS que se va a encargar de analizar los diferentes equipos de la red.

A la hora de elegir un software NIDS, se disponen de dos opciones de código libre. Por una parte está Suricata, cuyo principal atractivo es que es multihilo, y la segunda opción, que es la elegida, es Snort. Se elige Snort dado que posee una característica muy atractiva: el uso de preprocesadores. Por este motivo se prioriza el uso de Snort sobre Suricata.

Para el software HIDS, después de buscar entre varias alternativas de pago como SolarWinds o PaperTrail, se elige el uso de un software de código libre también, por lo que se opta por OSSEC. La detección de intrusos la realiza buscando anomalías, y se implementa a partir del uso de políticas. La herramienta es multiplataforma, por lo que se hace ideal para equipos Windows y Linux.

5.3. Routers

Los *routers* trabajan sobre la capa tres del modelo OSI representado en la figura 14. Es decir, definen el enrutamiento y el envío de paquetes entre las redes. Para realizar este transporte, utilizan cuatro procesos básicos:

I. Direccionamiento
II. Encapsulamiento
III. Enrutamiento
IV. Desencapsulamiento

La función básica de estos *routers* es la de almacenar las tablas de enrutamiento para determinar por donde deben viajar los paquetes. El *router* decide por donde debe reenviar el paquete para cada uno de ellos cuando llega a la interfaz de la puerta de enlace, en este caso bien sea a la dirección 172.25.1.1 o la dirección 172.25.2.1, dependiendo de dónde venga encaminado el tráfico desde el ***front-end***.

El *router* podrá decidir qué hacer con este tráfico, si bien lo envía al *router* o dispositivo de capa tres del próximo salto (next-hop), si bien lo envía directamente al host de destino si se encuentra en la misma red, o si bien lo descarta si se trata de un paquete malformado.

Dado que el funcionamiento que se espera de ambos *routers* es exactamente el mismo, las pruebas se van a realizar sobre uno de ellos en todo momento. Una vez se compruebe el correcto funcionamiento, se clonará dicha configuración en el otro *router*.

5.3.1. Configuración general

Para el presente caso de estudio, la configuración de estos *routers* se basa en una configuración principal que se explica a continuación. Se debe configurar correctamente que la obtención de la dirección IP en la interfaz ether1 (WAN) sea automática, es decir, que gaste mediante NAT la misma que el host anfitrión. Además, se debe configurar de forma estática la dirección IP de la interfaz ether2 (LAN), junto con la máscara de red. Esta interfaz es la que conecta directamente con el *firewall* ***front-end***, por lo que deberá llevar activada la función NAT. El motivo de esto es que cada paquete que salga de la zona roja al exterior debe hacerlo encapsulado bajo la dirección IP origen WAN del *router*.

Por ejemplo, suponiendo que el host anfitrión tiene la dirección IP 192.168.0.48 en la red de área local en la que se encuentra, cualquier paquete cuya dirección IP origen sea la del equipo anfitrión, cuando atraviese el *router* físico de dicha área local, tomará la dirección origen igual a la dirección WAN de dicho *router*.

Ahora bien, el *router* virtual que representa al de Orange, posee la dirección 192.168.232.130, que VMware traduce automáticamente en la dirección 192.168.0.48 del host anfitrión, por lo que cada paquete que provenga de la red 172.25.1.0/24 deberá ser trasformado en el *router* 1.1 en un paquete cuya dirección origen sea 192.168.232.130 (WAN del *router* 1.1) para poder seguir la ruta lógica hacia Internet.

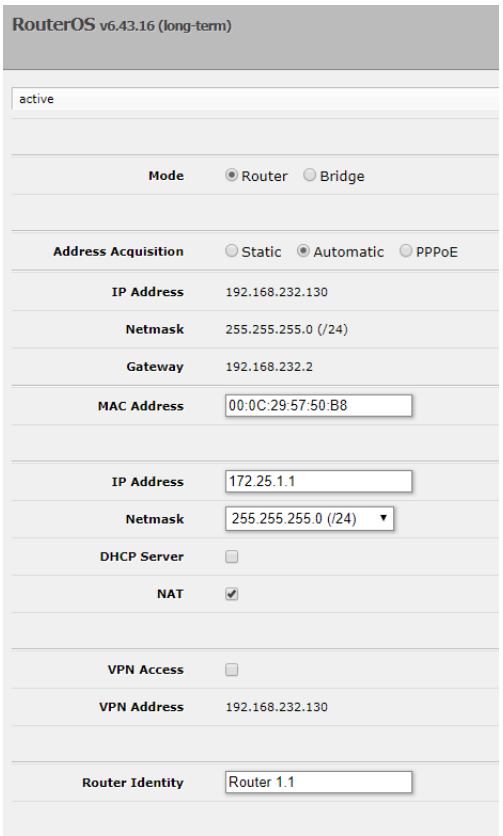

Figura 20. Configuración general router 1.1.

En esta figura se pueden observar diversos campos que se van a comentar a continuación. En primer lugar, el modo de ambos *routers* debe ser "*router*", dado que no van a ser un mero puente entre interfaces como si fueran un hub. Es decir, estos *routers* deben adoptar las funciones de *router,* y actuar como un dispositivo de capa tres según el modelo OSI para realizar funciones de enrutador del tráfico.

La adquisición de dirección IP, como se ha mencionado anteriormente, debe ser automática, puesto que de la traducción se encarga VMware. La configuración a destacar es el campo "IP Address", donde hay que imputar la dirección IP de la interfaz LAN que deseamos que tome el *router*. En este caso, dado que se trata del *router* 1.1, esta dirección será la 172.25.1.1. Junto a la dirección IP, se debe indicar la máscara de red con la que contará la red 172.25.1.0; en este caso, pensando en un posible crecimiento en el futuro, será la 255.255.255.0, capaz de albergar 254 hosts.

Por último se selecciona la opción NAT, como se ha explicado anteriormente.

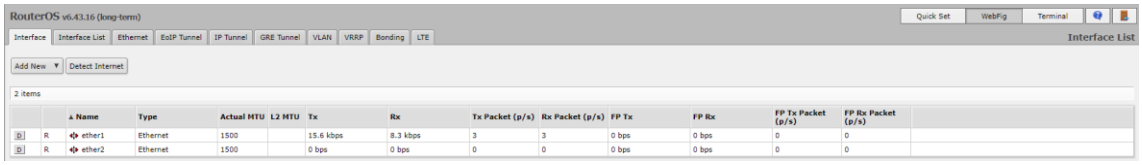

Figura 21. Interfaces de los router.

5.3.2. Firewall

Como se ha explicado en el diseño de la solución, estos *routers* van a poseer un mecanismo integrado que va a realizar un primer filtrado del tráfico. Mediante este mecanismo se debe permitir todo el tráfico del interior de la red hacia el exterior, ya que el tráfico saliente del ***front-end*** ya estará doblemente filtrado según las reglas establecidas. Sin embargo, solo se deberán permitir en exclusiva aquellas conexiones UDP entrantes que vayan dirigidas al servidor DNS.

También se quiere evitar el uso de "*IP Spoofing*", es decir, tráfico con direcciones IP falsas. Lo que se busca es establecer un filtro que compruebe si los paquetes recibidos en las interfaces ether2 (LAN) pertenecen a esa red. De manera análoga, se pretende comprobar que ningún paquete llega a la interfaz ether1 (WAN) con IP origen de la red LAN.

El objetivo principal de las reglas que se esperan definir, es aislar el *router* de la WAN, o lo que es lo mismo, que desde la WAN hacia el *router* no se pueda acceder a no ser que se trate de una conexión establecida por el *router*, ni usando la dirección WAN, ni usando diferentes ataques, ni realizar un ping. Esto se hace para que el atacante en ningún momento consiga tener acceso de ningún tipo al *router*. Desde la WAN hacia la LAN, solo se deben permitir contestaciones a conexiones establecidas desde dentro, y conexiones hacia el servidor DNS.

5.3.2.1. Servicios

Los *routers* Mikrotik, vienen con una serie de servicios habilitados por defecto:

- Api
- Api-ssl
- ftp
- ssh
- winbox
- www

Dadas las características de la red, se requiere dejar únicamente activos los servicios ssh, www, y una variante para webs con certificado ssl, www-ssl, quedando configurado como en la siguiente figura:

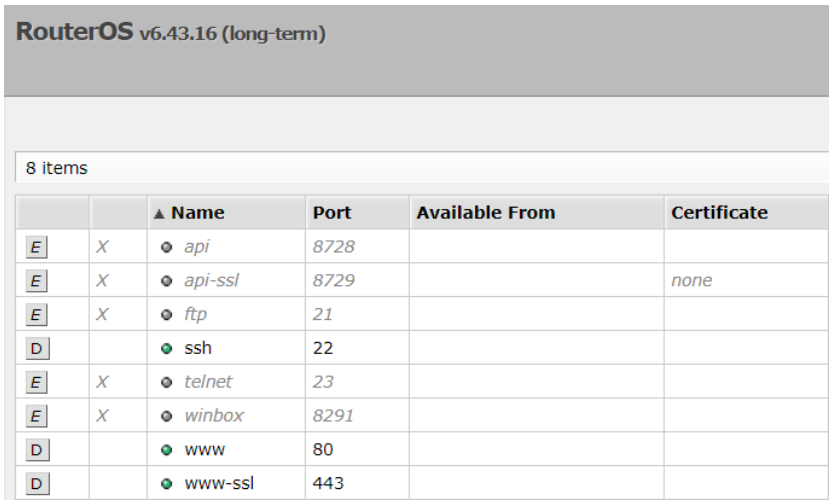

Figura 22. Servicios permitidos en los routers.

5.3.2.2. Listados de red

Para simplificar el trabajo, se van a añadir unos listados de red, cuyo propósito es simplificar el trabajo agrupando dispositivos de la red en diferentes listados. Esto va a ayudar en la definición de las reglas del *firewall*. En este caso se van a generar los siguientes listados:

Tabla 22. Listados definidos en los routers.

DIRECCIÓN DE LA RED	NOMBRE DEL LISTADO
172.25.1.0/24	Red_roja_movistar
172.25.2.0/24	Red_roja_orange
172.25.4.0/24	Red_amarilla

172.25.84.0/22	Red_verde

Se definen mediante el uso de los siguientes comandos los listados contenidos en la tabla anterior:

```
[admin@Router 2.1] > /ip firewall address-list add address=172.25.1.0/24 list="R
ed_roja_movistar"
[admin@Router 2.1] > /ip firewall address-list add address=172.25.2.0/24 list="R
ed_roja_orange"
[admin@Router 2.1] > /ip firewall address-list add address=172.25.4.0/24 list="R
ed_amarilla"
[admin@Router 2.1] > /ip firewall address-list add address=172.25.84.0/22 list="
Red_verde"
[admin@Router 2.1] > _
```

Figura 23: Definición de listados en el router.

También se definen aquellos dispositivos que ofrecen servicios en la red, en este caso el servidor de DNS, el equipo de monitorización, y, por último, los servidores DHCP y de ficheros. Además, para realizar las diferentes pruebas, se añade el equipo de la red interna cuya dirección es 172.25.84.2. El resultado es el siguiente:

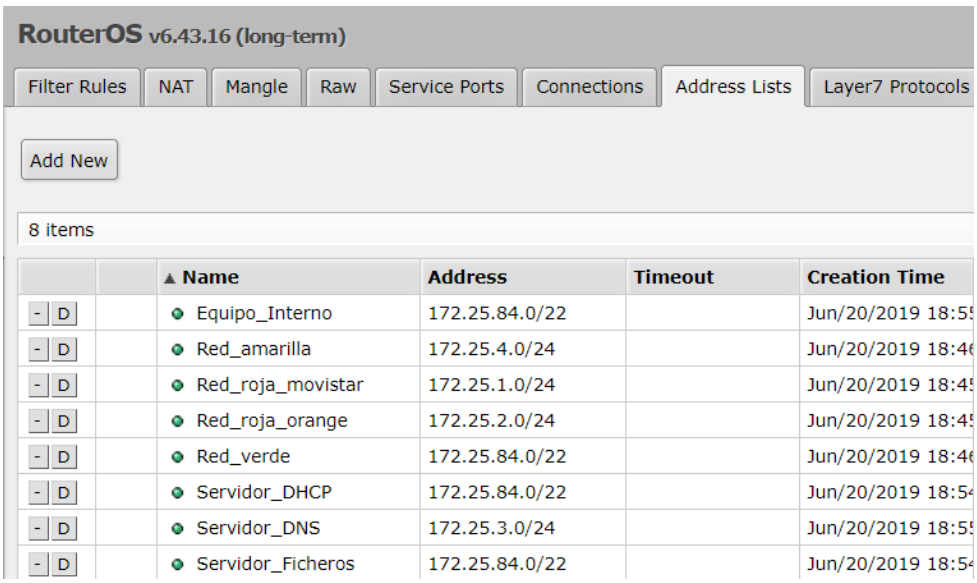

Figura 24. Listados declarados en los routers.

5.3.2.3. Reglas del firewall

Tabla 23. Tipo de reglas del firewall.

TIPO DE REGLA	DEFINICIÓN
FORWARD	Tráfico que atraviesa el *router*.
INPUT	Tráfico que tiene como destino el propio *router*.
OUTPUT	Tráfico que sale del propio *router*.

En la anterior tabla se puede observar las diferentes reglas que existen para configurar el cortafuegos del *router* en función de cual sea el destino del tráfico que lo atraviesa.

Para las conexiones cuyo destino sea el propio *router* (INPUT) se definen las reglas detalladas en la tabla 24 pensando en el tráfico que se desea permitir hacia él. Se van a aceptar únicamente aquellas conexiones que sean relacionadas y establecidas, por tanto se van a denegar todas las conexiones inválidas.

Respecto al tráfico, se va a permitir todo el que provenga desde el interior de la red, es decir, desde la interfaz LAN, y se denegará todo el tráfico restante, excepto el que se defina en el DST-NAT. También se crean unas reglas para prevenir ataques SynFlood y de escaneo de puertos en el *router*.

Tabla 24. Reglas del firewall INPUT.

REGLA	MODO	TIPO DE REGLA
Conexiones relacionadas y establecidas al *router*	ACEPTAR	INPUT
Conexiones inválidas al *router*	DENEGAR	INPUT
Tráfico desde interfaz LAN al *router*	ACEPTAR	INPUT
Tráfico restante excepto DST-NAT al *router*	DENEGAR	INPUT
Ataques SynFlood	DENEGAR	INPUT
Ataques Port Scan	DENEGAR	INPUT

Para aquel tráfico cuyo propósito sea cruzar el *router* (FORWARD) se va a definir una serie de reglas, incluyendo una que solo permita las conexiones relacionadas y establecidas en ambos sentidos, es decir, solo se van a permitir aquellas conexiones que tengan que ver con una que se haya generado previamente en sentido inverso.

Además se van a crear reglas para evitar los principales ataques conocidos, tal como se muestra en la siguiente tabla:

Tabla 25. Reglas del firewall FORWARD.

REGLA	MODO	TIPO DE REGLA
Conexiones relacionadas y establecidas	ACEPTAR	FORWARD
Ataques spammers	DENEGAR	FORWARD
Ataques disable tracert	DENEGAR	FORWARD
Tráfico y conexiones hacia servidor DNS	ACEPTAR	FORWARD

Respecto a las reglas tipo OUTPUT, es decir, el tráfico del propio *router* al exterior, no se configura ninguna, por lo tanto, no estarán permitidas. Con esto se busca aislar completamente el *router* del exterior, y que, por lo tanto, no sea alcanzado.

Finalmente se añade una regla de tipo INPUT, para que cualquier tráfico o conexión que no haya sido permitido mediante una regla específica, se rechace. Esto lo hace la regla: "*Drop anything else!*".

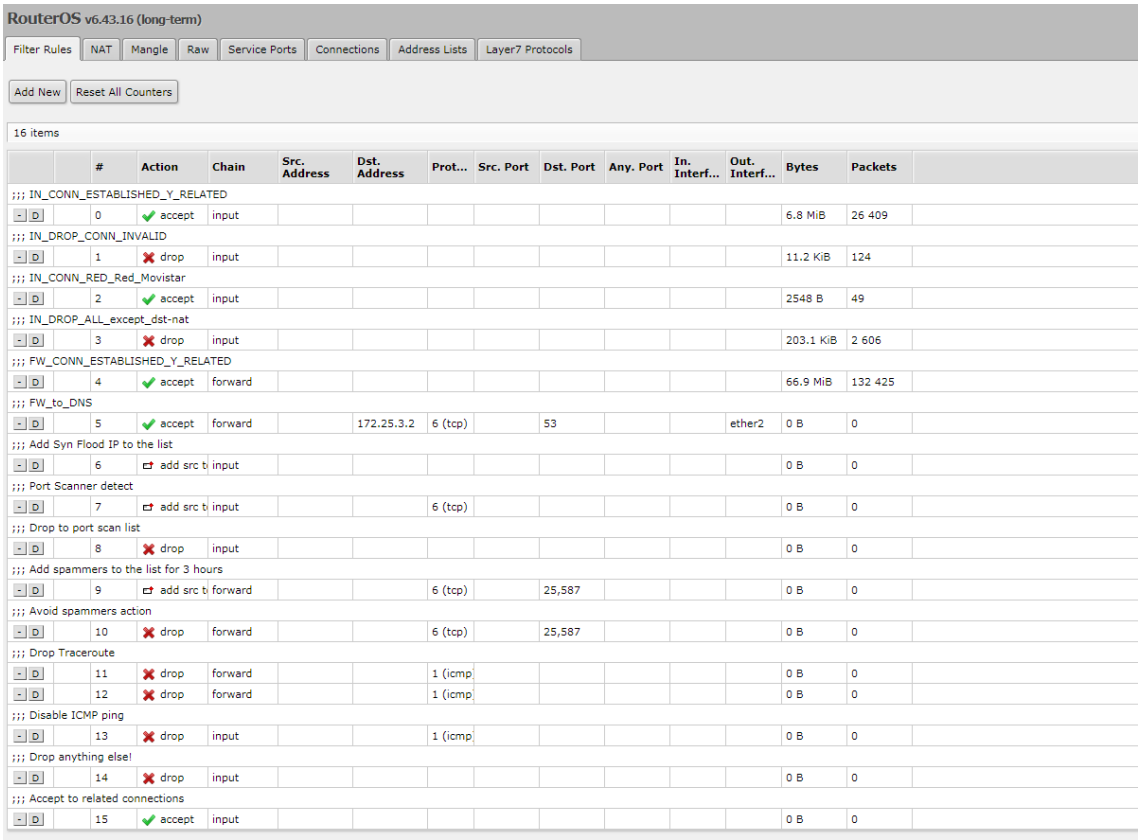

Figura 25. Reglas del firewall definidas en los routers.

En la figura 25 se observa cómo quedan configuradas las reglas en el *firewall* de los *routers*.

Con esta serie de reglas se va solventar aquellos riesgos que afectaban a los *routers* y al tráfico que circulaba por ellos, es decir, se va a solventar aquellas amenazas que tienen que ver con la denegación de servicios y con el re-encaminamiento de datos.

Se realizan una serie de pruebas para comprobar que efectivamente está funcionando correctamente. Para ello, se comprueba que ya no se tiene acceso al *router* desde el host anfitrión, puesto que se encuentra en la red WAN del *router*, pero sí que se tiene acceso desde el interior de la red, tanto desde el equipo interno como desde el equipo de monitorización.

5.3.3. NIDS

Desde el punto de vista de la monitorización resulta interesante el uso de un software especializado en detección y prevención de intrusos, como es el caso del equipo de monitorización que va a implementar el software Snort de código libre, especializado en analizar la totalidad del tráfico de la red. Sin embargo, desde el punto de vista del perímetro resulta mucho más interesante aprovechar la tecnología que ofrece Mikrotik en materia de *logs*.

*Router*OS, el sistema operativo que implementan los *routers,* dispone de una herramienta llamada *logging*. Esta herramienta es capaz de capturar diversos tipos de eventos e información de estado en base a unas reglas.

Cada entrada que se registra en el log incluye la fecha de cuando ha ocurrido el evento, a qué tipo de amenaza pertenece (*topic*), la severidad, y el propio mensaje. Dicha severidad, se define como el nivel de alerta en el que se puede clasificar un evento dado en el *router* cuando coincide con alguna de las reglas configuradas. *Router*OS utiliza el estándar RFC3164 para conseguir clasificar el tráfico existente en el *router* en base a los siguientes niveles de seguridad:

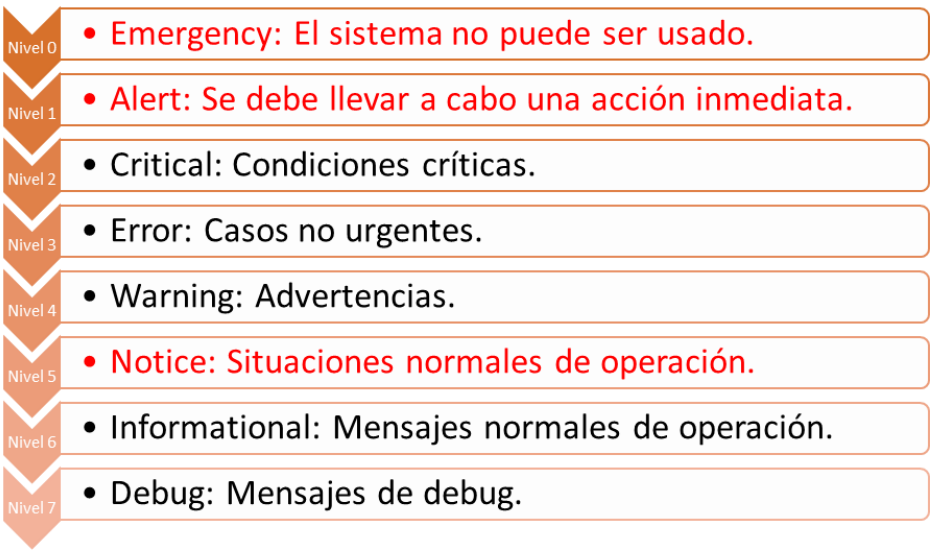

Figura 26. Niveles de severidad de los eventos.

Los niveles cero, uno y cinco, no se pueden implementar en *Router*OS, aunque sí se detallan dado que son igualmente relevantes. Estos niveles de severidad se aplican a un tipo de amenaza (*topic*). Entre las opciones de *Router*OS figuran más de cincuenta *topics*, pero dada la arquitectura presentada, y dada la función de puerta de enlace con Internet de estos *routers,* se destacan los siguientes *topics*:

Tabla 26. Topics de los eventos.

TOPIC	DESCRIPCIÓN
DDNS	Mensajes de log generados por la herramienta manual: Tools →Dynamic DNS.
Web-Proxy	Mensajes de log generados por Web-Proxy.
PPTP	Mensajes de PPTP relacionados con el cliente y servidor.
SSH	Mensajes de log generados por conexión SSH.
Firewall	Mensajes de log generados cuando se produce la acción de una de las reglas del *firewall*.

Las reglas se relacionan con eventos que se desean controlar de forma que, cuando ocurre dicho evento, se va a generar una entrada en el log. Es posible disponer de una regla conformada por un *topic* sin una severidad asociada, y viceversa.

Dado que los *routers* forman parte de la red más externa (zona roja), y que sirven de frontera entre Internet y el resto de la red, se deben definir unas reglas con una severidad más baja, es decir, menos sensibles. La razón de esto es que, a mayor severidad en esta zona, mayores falsos positivos se van a producir dado que reciben la totalidad del tráfico, por lo que, a medida que se vaya profundizando en la red, se va a aplicar reglas más severas, tanto en los IDS/IPS como en los cortafuegos, siendo el ***back-end*** el que posea las reglas más estrictas dado que toda alerta o sospecha en esa zona se debe contemplar como una amenaza directa. Por todo esto, se definen las siguientes reglas para los *routers*:

Tabla 27. Reglas en el log de los routers.

ID REGLA	SEVERIDAD	TOPIC
RL_1	2	-
RL_2	3	-
RL_3	2	*Firewall*
RL_4	3	*Firewall*
RL_5	4	*Firewall*
RL_6	2	DDNS
RL_7	3	DDNS
RL_8	4	DDNS
RL_9	2	Web-Proxy
RL_10	3	Web-Proxy
RL_11	4	Web-Proxy

Con esta serie de reglas definidas se va a generar un log cada vez que se produzca un evento de severidad dos o tres, independientemente de cual sea el *topic*. Estos niveles de severidad se corresponden con el nivel "critical" y el nivel "error" según la figura 26. Es decir, cada vez que se produzca un evento crítico o un error no urgente, se va a escribir en una entrada del log sin importar cuál sea el *topic*.

Además, para los *topics* que se corresponden con *firewall*, DDNS y Web-Proxy, se establece que se registre una entrada cada vez que la severidad de uno de estos sea de nivel dos, tres, o cuatro, o, lo que es lo mismo, cada evento crítico, error no urgente, o advertencia. De esta forma se va a establecer un registro de aquellos eventos que requieren atención.

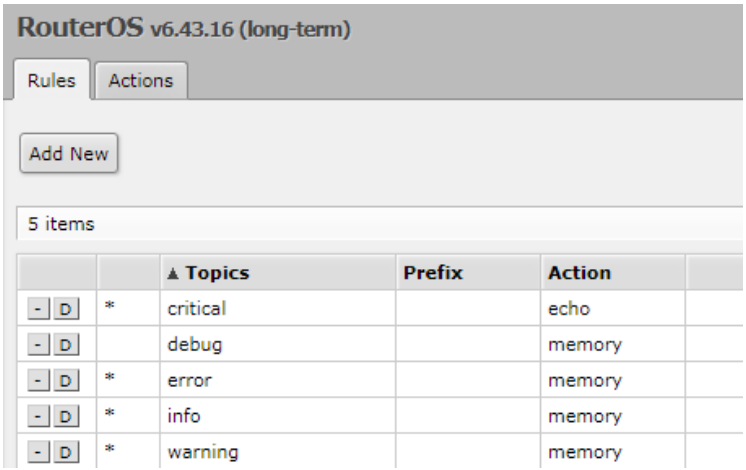

Figura 27. Topics establecidos en los routers.

En la figura 27 se muestra los diferentes niveles de severidad que llevan preestablecidos *Router*OS para los eventos. Con estos niveles, junto con los *topics*, se va a configurar las diferentes reglas.

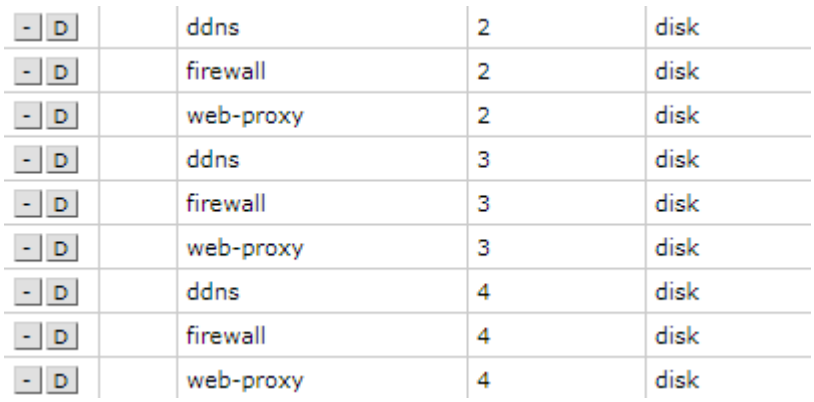

Figura 28. Reglas creadas sobre los tópicos.

Después de declarar aquellas reglas que se han estimado, conforme a la tabla 27, se puede comprobar en la figura 29 que se crean los dos ficheros log donde se van a registrar todos los eventos que se recojan siguiendo las directrices establecidas en la figura 28.

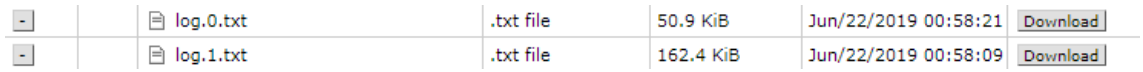

Figura 29. Ficheros log dónde se recogen los eventos.

Para realizar una prueba, se accede desde el host anfitrión al *router* a través de la interfaz WAN que los une. Dado que mediante el uso de una regla del *firewall* se ha deshabilitado el acceso al *router* (INPUT) desde la red WAN, en la figura 30 se puede observar cómo se genera un registro en el log dónde se identifica un equipo cuya dirección física e IP es la del host anfitrión que envía un mensaje a la dirección de difusión intentando contactar el *router* sin éxito.

```
firewall, info 4: input: in:ether1 out:(unknown 0), src-mac: 00:50:56:c0:00:08, proto UDP, 192.168.232.1:57621->192.168.232.255:57621,
firewall, info 3: input: in:ether1 out:(unknown 0), src-mac: 00:50:56:c0:00:08, proto UDP, 192.168.232.1:57621->192.168.232.255:57621,
firewall, info 2: input: in:ether1 out:(unknown 0), src-mac: 00:50:56:c0:00:08, proto UDP, 192.168.232.1:57621->192.168.232.255:57621,
```

Figura 30. Entrada del log asociada al evento.

5.4. Firewalls

Olaf Kirch (2000) define *firewall* como una máquina segura y confiable que se ubica entre una red privada y una red pública. El *firewall* está configurado con un conjunto de reglas que determinan qué tráfico de red se permitirá pasar, y cuál será bloqueado o rechazado.

Los *firewall*s elegidos, de ambos modelos, trabajan sobre la capa siete del modelo ISO/OSI definida en la figura 14 al ser *firewall*s NGFW. Esto no quiere decir que únicamente trabajen sobre esa capa; trabajar sobre esa capa implica trabajar sobre las capas tres y cuatro.

Gracias a la capa tres, se puede trabajar sobre los datagramas IP que circulan por el *firewall*. Es decir, se aplican diferentes tipos de criterios para determinar que datagramas se desean filtrar, en función de, por ejemplo: el tipo de protocolo (TCP, UDP, ICMP, etc), el tipo de datagrama (SYN/ACK, datos, ICMP, etc.), y también en función de la dirección IP origen y destino.

Sobre esta capa se va a definir la mayoría del conjunto de las reglas que se van a incorporar inicialmente en los *firewall*s, y el motivo es que las reglas que se definen en esta capa son de gran utilidad para mitigar aquellos ataques relacionados con accesos no autorizados, denegación de servicios y suplantación IP (*IP spoofing*). Sin embargo, no es apropiada para evitar la explotación de las debilidades en los servicios de red o las

escuchas ilegales. Dado que el principal riesgo que se debe evitar, extraído del análisis de riesgos, es el de la denegación de servicios, se va a trabajar principalmente sobre la capa tres.

Adicionalmente, estos cortafuegos trabajan sobre la capa cuatro del modelo ISO/OSI (*stateful inspection*), por lo que son capaces de filtrar por conexiones, es decir, por la información que contiene las cabeceras IP y TCP/UDP.

La capa siete sobre la que trabajan estos *firewall*s les permite inspeccionar los protocolos HTTP o HTTPS, filtrar por URL, filtrar por usuarios, y realizar control de aplicaciones (WEB,FTP, P2P…). Esta capa se hace idónea para filtrar el tráfico en función de los departamentos o los usuarios que acceden desde la zona verde hacia Internet.

5.4.1. Front-end

El ***front-end*** se encuentra en el nexo entre la zona roja y la zona amarilla de la red. A pesar de que el tráfico que le va a llegar ya va a estar previamente filtrado por los *routers*, el tráfico que llega a este cortafuegos va a ser el total que circula entre el exterior y el interior de la red, y es por ello que las reglas que se van a definir en este *firewall* deben ser menos restrictivas, para evitar el continuo bloqueo de tráfico debido a falsos positivos. Además, se debe permitir el tráfico interno hacia el servidor DNS ubicado en la zona desmilitarizada.

Este cortafuegos va a disponer de cuatro interfaces activas que se detallan a continuación:

Tabla 28. Interfaces en el cortafuegos front-end.

INTERFAZ	RED
Puerto 1 (WAN1)	172.25.2.0/24
Puerto 2 (DMZ)	172.25.3.0/24
Puerto 3 (LAN)	172.25.4.0/24
Puerto 4 (WAN2)	172.25.1.0/24

5.4.1.1. Configuración general

Tal como se muestra en la tabla 28, se configuran las cuatro interfaces con las redes correspondientes, de forma que ninguna de estas interfaces tiene el servidor DHCP activo, es decir, todos aquellos dispositivos que se conectan a una de estas interfaces, llevan una dirección IP asignada de forma estática.

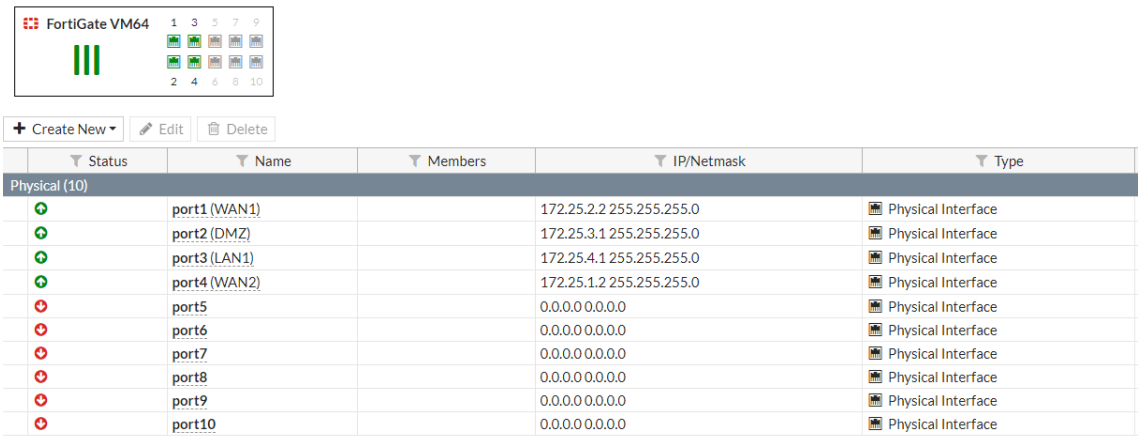

Figura 31. Interfaces declaradas en el cortafuegos front-end.

En la figura 31 se observa como cada una de las cuatro interfaces definidas lleva asignada la dirección IP dentro de la red a la que se conectan. La interfaz WAN1 conecta directamente con el *router* 2.1 (Movistar), mientras que la WAN2 lo hace con el *router* 1.1 (Orange). La interfaz DMZ, se corresponde a la zona desmilitarizada donde se halla el servidor DNS, y, finalmente, la interfaz LAN es aquella que conecta el *firewall* ***front-end*** con el ***back-end***, es decir, la zona amarilla. En el sexto anexo se puede encontrar la configuración de las interfaces más detallada.

Esta configuración se define como la configuración básica, dado que sin definir correctamente las interfaces no se va a lograr comunicación alguna entre los extremos. En el mismo sentido, también se debe configurar correctamente el encaminamiento del tráfico. Esta configuración se va a realizar en el apartado 5.4.1.3.

5.4.1.2. Redundancia a la entrada

Como se ha comentado en el diseño de la solución, la empresa consta de dos proveedores de servicio de Internet (ISP). Esto es debido a que se desea un alta disponibilidad en la conexión a Internet, y que, por lo tanto, si deja de estar operativo uno de los dos proveedores, se pueda utilizar el otro.

Para conseguir de manera efectiva este planteamiento, es necesario llevar a cabo una serie de configuraciones en el cortafuegos ***front-end***. Es decir, se debe indicar al propio cortafuegos, que es el que se encarga de encaminar el tráfico hacia el exterior, que debe hacerlo de forma predeterminada por ambos *routers*, y que de forma automática cuando deje de estar disponible uno de los dos proveedores, derive la totalidad del tráfico hacia el otro proveedor.

Para llevar a cabo esta tarea, FortiOS (Sistema operativo de los Fortigate) en su versión 6.0 incorpora una herramienta destinada a ello llamada SD-WAN, de sus siglas en inglés significa red WAN definida por software. Gracias a esta herramienta se va a crear una interfaz WAN virtual en la que se va incluir las dos interfaces WAN físicas, tanto la del *router* 2.1 del proveedor Movistar como la del *router* 1.1 del proveedor

Orange. Una vez creada la interfaz WAN virtual, se va a proceder a indicar el volumen que se desea que circule de forma predeterminada por cada interfaz WAN física, es decir, un balanceo entre ambas interfaces. Gracias a este balanceo, se va a conseguir que una vez se detecte que una de las dos interfaces no consigue alcanzar Internet, se desviará de forma automáticamente, y en cuestión de segundos, la totalidad del tráfico a la interfaz disponible hasta que la otra vuelva a estar operativa.

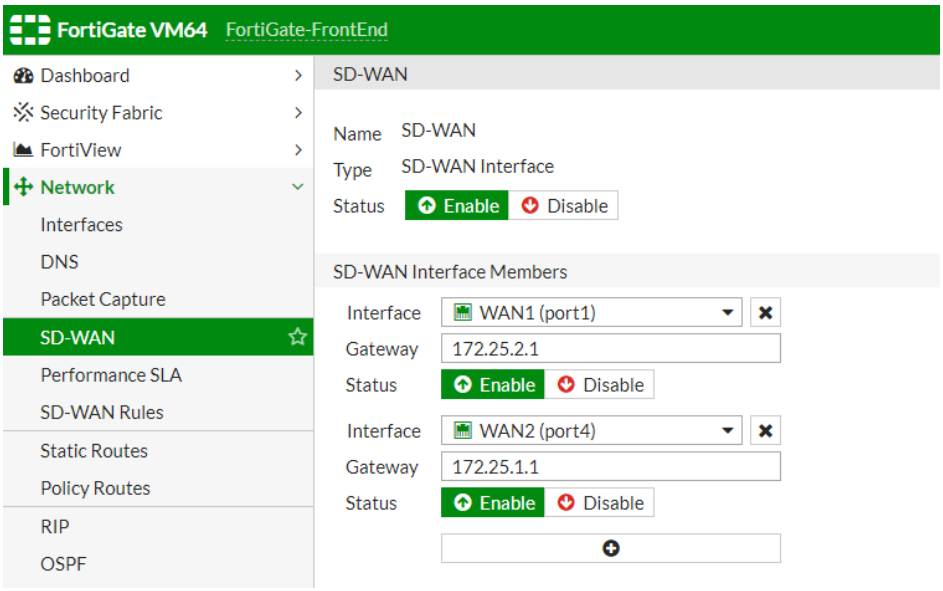

Figura 32. Configuración de la interfaz virtual SD-WAN.

Como se puede observar en la anterior figura, se habilita la interfaz SD-WAN y se añade como miembros a las dos interfaces WAN físicas, indicando, para cada caso, la puerta de enlace que corresponde a la dirección de los correspondientes *routers*.

Finalmente, se configura el balanceo de la interfaz para determinar qué porcentaje de tráfico debe circular por cada una de las interfaces físicas. Para ello, en las reglas de la interfaz SD-WAN se indica el porcentaje del volumen de tráfico que se desea que circule por cada interfaz. En este caso se elige que un 75% del tráfico circule por la interfaz WAN1, dado que se trata de fibra óptica de Movistar de altas prestaciones capaz de absorber con normalidad dicha cantidad de tráfico, mientras que el 25% restante se desviará por la interfaz WAN2 de Orange, dado que se trata de una red celular de datos que no aporta la misma estabilidad y capacidad que su competidora. En caso de que el cortafuegos detecte que no encuentra conexión a Internet en alguna de las dos interfaces físicas, en cuestión de segundos cambiará la dirección del tráfico para que el 100% circule por la interfaz opuesta.

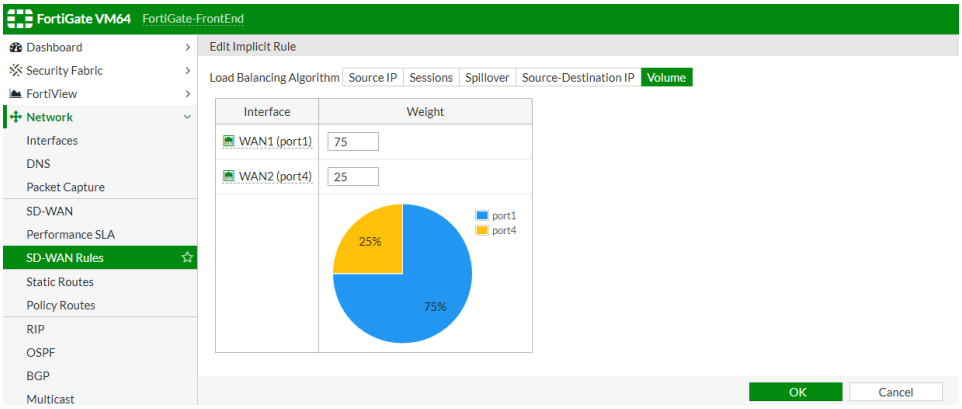

Figura 33. Configuración del balanceo en la interfaz SD-WAN.

5.4.1.3. Encaminamiento del tráfico

Malhotra, R. (2002) menciona que aquellas redes conectadas directamente al dispositivo son de acceso inmediato, es decir, no requieren de ningún mecanismo específico para descubrir esas redes. En el momento en el que las redes a las que pertenecen las diferentes interfaces del ***front-end*** se activan, éstas aparecen en la tabla de enrutamiento del cortafuegos.

La única red cuya distancia es mayor a las directas que se desea alcanzar es la red WAN de los *routers* (Internet) de forma predeterminada. Para ello se va a establecer como ruta por defecto la interfaz SD-WAN, que se va a encargar de enrutar el tráfico por cada una de las interfaces, dependiendo de cuál sea el estado de éstas.

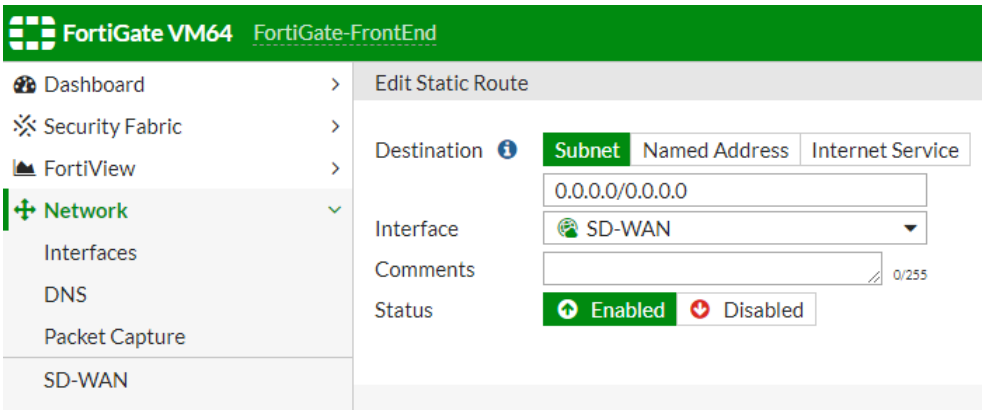

Figura 34. Configuración de la ruta estática por defecto.

Malhotra, R. (2002) dice que la solución de las rutas estáticas es poco escalable, y que a medida que la red en cuestión sufre un crecimiento se hace mucho más interesante el uso de rutas dinámicas haciendo uso de diferentes protocolos de enrutamiento (RIP, EIGRP u OSPF). Es por esto que se va a tener dicho aspecto en cuenta como trabajos futuros derivados de la presente solución.

5.4.1.4. IPS

Se ha de establecer una diferencia clara entre IDS e IPS. A pesar de que parte del funcionamiento de ambos es parecido, poseen una diferencia importante: en el *router* se ha visto que se ha hecho uso de unos logs a modo de IDS, cuya única función es la de analizar, comparar y registrar en un fichero todos aquellos eventos sospechosos. Es decir, un IDS no altera de ninguna forma los paquetes que viajan por la red. Lo que hacen es comparar la actividad de la red con bases de datos de amenazas conocidas para detectar diversos eventos que comprometen la seguridad, bien sea un escaneo de puertos o bien una violación de las políticas de seguridad. En cambio, un IPS sí altera los paquetes que viajan por la red en función de unas reglas establecidas. Evita que el paquete se entregue dependiendo del contenido del mismo, de forma similar a como el propio cortafuegos evita el tráfico por dirección IP. Este sistema funciona en el mismo área que el cortafuegos, entre la red externa y la interna a modo de nexo. Por esta razón, FortiOS integra este sistema en su cortafuegos, dado que la combinación de ambos se convierte en una herramienta de extremada utilidad para frenar ataques.

FortiOS trae configurados una serie de perfiles con diferentes firmas en su apartado IPS. En este caso, como se ha comentado con anterioridad, este primer *firewall* debe llevar unas reglas menos restrictivas que el ***back-end***, y, además, se ha de tener en cuenta que existe un servidor DNS en la zona desmilitarizada, por lo que se va a crear un perfil nuevo con unas firmas personalizadas para este caso.

Este perfil debe contemplar qué equipos se tratan de proteger por tal de incorporar aquellas firmas que más se adecuen. Para ello, a continuación se analizan los diferentes dispositivos que se van a proteger.

En un primer caso, se va a proteger el servidor DNS, situado en la interfaz DMZ de este cortafuegos. Los servidores DNS utilizan las conexiones UDP en el puerto 53 para respuestas de tamaño inferior a 512 bytes, y conexiones TCP en el mismo puerto para respuestas de tamaño igual o superior a 512 bytes. Además va a ejecutar un sistema operativo Windows. Para proteger dicho activo, se van a configurar todas aquellas firmas que cumplan con dichas condiciones.

También se debe configurar incluyendo aquellas firmas que protejan los clientes Linux (***back-end***) y clientes Windows (Equipo de monitorización y resto de equipos), principalmente en aquellas conexiones TCP/UDP, contemplando también el mayor número de ellas.

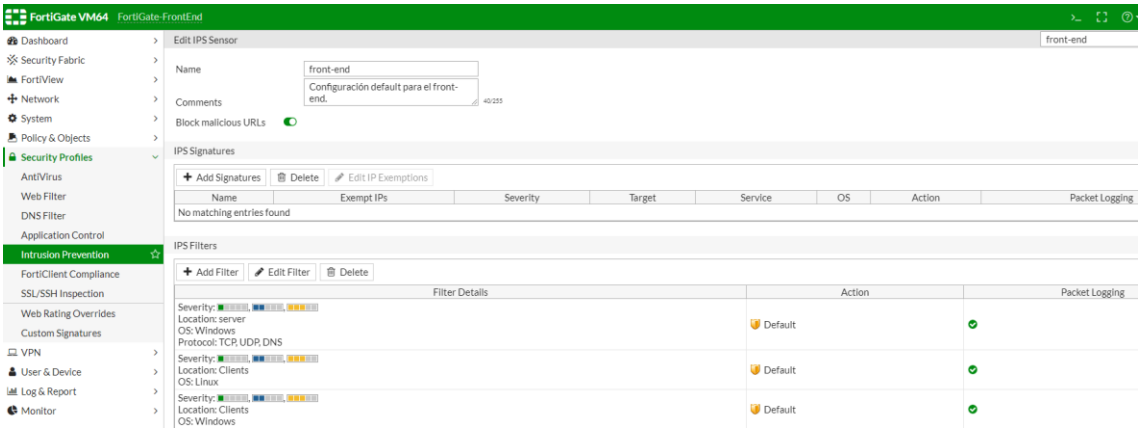

Figura 35. Filtros IPS configurados en cortafuegos front-end.

En la figura 35 se observa los tres filtros que se han aplicado en el IPS: el primero de ellos hace referencia a la protección del servidor DNS, el segundo de ellos al cortafuegos ***back-end***, y el último de ellos al resto de equipos Windows. Como se ha mencionado anteriormente, este cortafuegos debe ser configurado con menor severidad que su sucesor, por lo que se configura con los niveles de seguridad que van comprendidos desde el nivel informacional hasta el nivel medio.

5.4.1.5. Reglas del firewall

El *firewall* ***front-end*** se define como un punto clave en el perímetro de la red, pues es el primer gran impedimento que se va a encontrar el atacante si consigue atravesar los *routers*. Además, sirve de nexo entre cuatro redes y dos zonas, por una parte la red WAN que conecta con el *router* 2.1, la red WAN que conecta con el *router* 1.1, la zona desmilitarizada donde se encuentra el servidor DNS, y, por último, la red LAN que comunica con la zona amarilla de la red. Por lo tanto, se deben tener en cuenta aquellas reglas contra ataques que también se han configurado en el *router*, y en este sentido se debe tener en cuenta el ataque conocido como *IP spoofing* (Suplantación de IP).

La principal diferencia en este cortafuegos es la existencia de la zona desmilitarizada, ya que dicha zona debe ser accesible tanto desde Internet como desde la red Interna, pero no debe tener acceso a la zona amarilla ni a la red interna.

FortiOS lleva de forma implícita una política que bloquea todo el tráfico, por lo que se hace necesario permitir el tráfico mediante las reglas necesarias. Es decir, todo aquel tráfico que no esté permitido mediante una regla explícita para ello, será bloqueado de forma automática por dicha política.

Fortigate ofrece en sus *firewall*s una herramienta muy interesante llamada RPF (*Reverse Path Filter*). Se trata de una aplicación de seguridad que permite eliminar un paquete entrante en función de su dirección IP de origen. La dirección IP origen del paquete se verifica en la tabla de enrutamiento para verificar la ruta inversa, es decir, la ruta hacia la dirección IP origen del paquete. En función de cómo esté configurado el

filtro, el paquete se puede reenviar o eliminar. Esta herramienta se hace muy útil para solucionar aquellos ataques de suplantación de dirección IP (*IP spoofing*) dado que se puede comprobar si los paquetes cuya dirección IP origen sea de dentro de la red, realmente procede de allí. Para realizar este proceso se dispone de dos modos; el primero de ellos se define como modo estricto dónde se realiza una búsqueda de enrutamiento (con la mejor coincidencia) para el campo de dirección IP origen del paquete, y en ese caso el paquete se descarta si su interfaz de origen no coincide con la interfaz de origen en la búsqueda del enrutamiento. El segundo modo, definido como ruta factible, no solo tiene en cuenta la mejor ruta de coincidencia, sino que también se verifican otras rutas que apuntan a interfaces de origen de paquetes; si alguna de ellas acepta la dirección origen del paquete, se da el paquete como válido.

Actualmente esta herramienta viene incorporada de forma predefinida en el nivel de las interfaces, por lo que asegura una clara protección contra este tipo de ataques.

Se ha comentado con anterioridad que este primer *firewall* (***front-end***) va a ser menos restrictivo que el segundo (***back-end***). Sin embargo, en cuanto a tráfico exterior, aquel tráfico que proviene de la zona amarilla y desea viajar hacia Internet, va a ser tratado exactamente de la misma manera que el mismo tráfico que se va a permitir en el segundo cortafuegos. El motivo de esta decisión es simple, si el *firewall* ***back-end*** sufre cualquier tipo de impedimento que le impida operar con normalidad, debe ser entonces este *firewall* el que adopte aquellas reglas, por lo que van a estar replicadas de igual forma para garantizar el uso de las mismas.

Adicionalmente, se va a permitir todo el tráfico externo que provenga de la dirección 172.25.3.2 (Servidor DNS), y que previamente ya ha sido habilitado en el *firewall* del *router*.

Respecto al tráfico interno, aquel que proviene de Internet e intenta acceder al resto de la red, solo se va a permitir tráfico cuya dirección de destino sea la 172.25.3.2, es decir, el servidor DNS. De igual forma, este tráfico, con este destino, ya ha sido habilitado en el *firewall* de los *routers*. El resto de tráfico entrante va a estar bloqueado de forma implícita, excepto aquel relacionado con conexiones previamente establecidas desde el interior, es decir, las respuestas a peticiones realizadas desde el interior de la red. Este tráfico por defecto viene habilitado en FortiOS.

Se puede establecer un resumen del tráfico que se desea permitir mediante el uso de reglas en este *firewall* que se muestra en la siguiente tabla. Todo el tráfico no incluido en dicha tabla será bloqueado de forma implícita, excepto aquel tráfico relacionado con respuestas a peticiones originadas en sentido inverso.

Tabla 29. Reglas del firewall front-end.

ORIGEN	DESTINO	REGLA
Zona roja	DMZ	Permitido
DMZ	Zona roja	Permitido
Zona amarilla (con condiciones)	Zona roja	Permitido
Zona amarilla	DMZ	Permitido

En la figura 9 se pude observar de forma gráfica cual es el objetivo que se logra haciendo uso de estas reglas.

El tráfico externo que se desea permitir es exactamente el mismo que se permite actualmente por orden de la empresa. Se puede observar en la siguiente tabla qué tráfico se desea por parte de la empresa:

Tabla 30. Tráfico externo permitido en el front-end.

TIPO DE ACCESO	ACCIÓN
Acceso web (http, https)	Permitido
Conexiones TCP y UDP	Permitido
Conexiones a DNS	Permitido
Acceso remoto (VNC, RDP, SSH, Telnet)	Permitido
Acceso a servidor Microsoft Exchange	Permitido
Windows active directory	Permitido

El resto de tráfico se deniega de forma predeterminada, entre el que se incluye el correo electrónico común debido a medidas de seguridad. Dado que la empresa trabaja junto a Microsoft, se utiliza el correo mediante los servidores Exchange, y éste será el único correo permitido.

Para empezar a configurar esta serie de reglas se hace necesario definir unas direcciones predeterminadas que engloben todas las direcciones de cada una de las cuatro redes que se conectan a este *firewall* como se muestra a continuación:

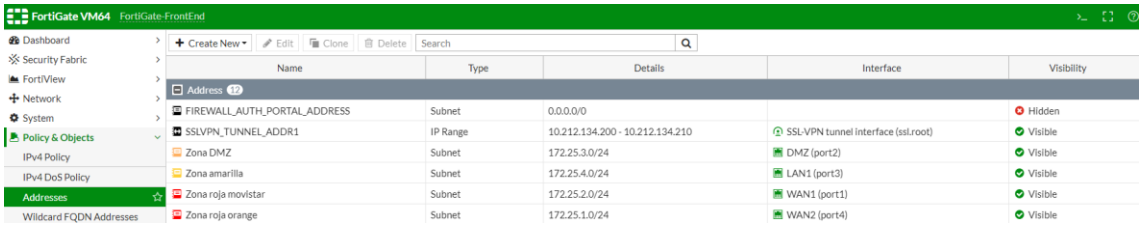

Figura 36. Direcciones correspondientes a cada zona.

Esta tarea simplifica bastante la creación de las diferentes reglas que se va a llevar a cabo. La primera de ellas va a ser una de tráfico entrante de la interfaz SD-WAN hacia la interfaz DMZ, y viceversa. La segunda, una que permita el tráfico externo hacia la interfaz DMZ, y, finalmente, una regla que permita el tráfico externo desde la zona amarilla en función de las restricciones mencionadas en la tabla 30.

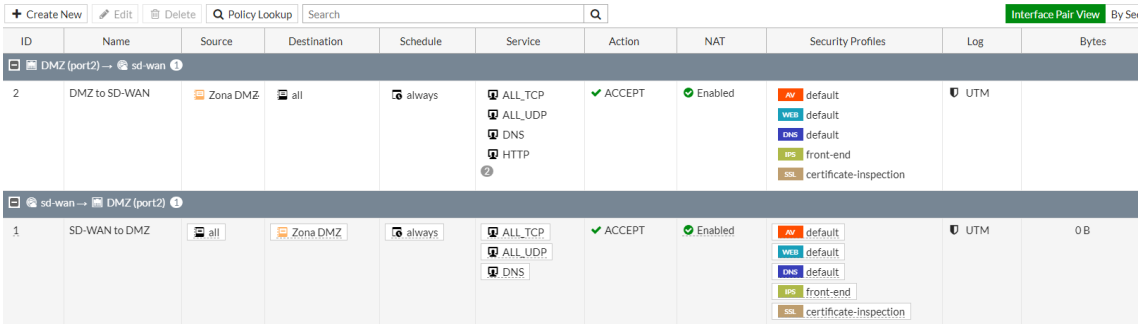

Figura 37. Reglas zona DMZ.

En la figura 37 se observa las dos reglas relacionadas con la zona DMZ, en primer lugar la regla que permite el tráfico de salida con más servicios que el de entrada y se hace uso en ambos casos del perfil de IPS creado con anterioridad. De entrada, únicamente se permite conexiones TCP, UDP, y DNS, las únicas necesarias para establecer comunicación con el servidor.

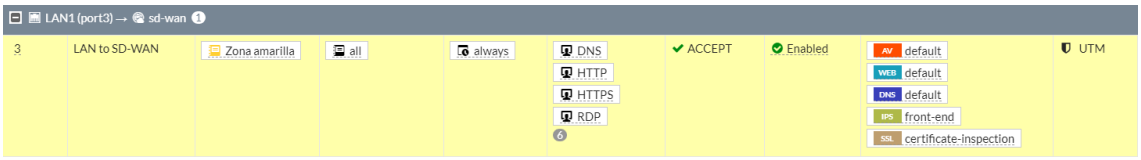

Figura 38. Regla externa para la zona amarilla.

En la figura 38 se crea la regla que permite el tráfico externo desde la zona amarilla a la zona roja en base a los criterios de la tabla 30 establecidos por la empresa. En todas las reglas se hace uso del perfil IPS creado anteriormente.

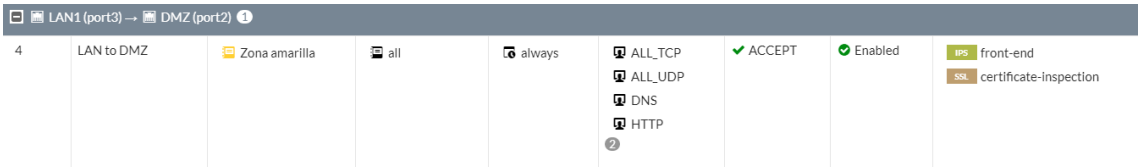

Figura 39. Regla externa hacia la zona DMZ.

Finalmente, se crea la regla que permite el tráfico desde la zona amarilla de la red hacia la zona DMZ. Para este caso se habilitan las conexiones TCP/UDP necesarias para el servidor DNS, además de acceso WEB para la configuración del mismo.

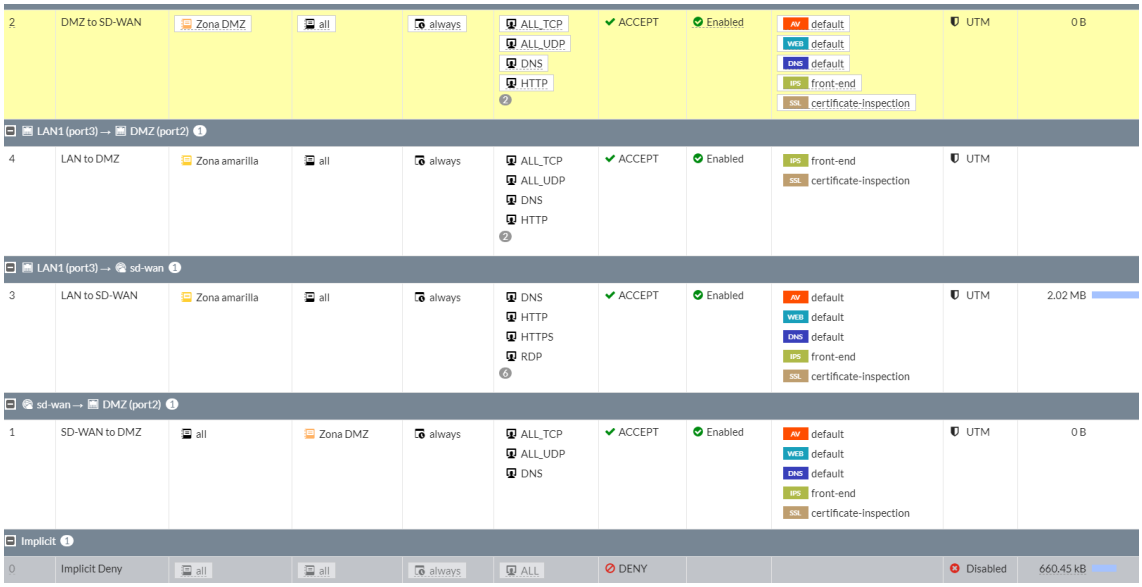

Figura 40. Resumen de las reglas en el front-end.

En la figura 40 se aprecia el resumen de las reglas configuradas en el *firewall*, incluyendo la política implícita de rechazar todo lo que no esté permitido.

5.4.2. Back-end

El ***back-end*** es el cortafuegos que se encuentra en el nexo entre la zona amarilla y la zona roja. La zona en la que se encuentra se denomina zona crítica, y esto es debido a que, en este punto, el tráfico ya viene filtrado previamente por dos cortafuegos, por lo que cualquier anomalía aquí debe ser neutralizada. Para esto, se va a configurar el cortafuegos con unas reglas lo más restrictivas posibles, a diferencia del ***front-end***.

La interfaz LAN del ***back-end*** es la que enlaza directamente con la red interna, aunque tampoco tiene habilitada la función de servidor DHCP dado que existe un servidor dedicado exclusivamente para dicha función actualmente. Este *firewall* va a disponer de dos interfaces tal como se muestra a continuación:

Tabla 31. Interfaces del cortafuegos back-end.

INTERFAZ	RED
Puerto 1 (WAN)	172.25.4.0/24
Puerto 3 (LAN)	172.25.84.0/22

5.4.2.1. Configuración general

La configuración general de este *firewall* se basa en la correcta configuración de las interfaces de las que hace uso. Dado que su principal función es la de la comunicación entre la zona amarilla y la zona verde, estas interfaces deben encontrarse configuradas de forma y manera que logren comunicarse en sus respectivas redes.

Cada una de las interfaces que se declaran en la tabla 30 llevan asignada dicha dirección de forma estática; a su vez, cada dispositivo que se conecte a dicha interfaz llevará asignada de forma estática su dirección IP.

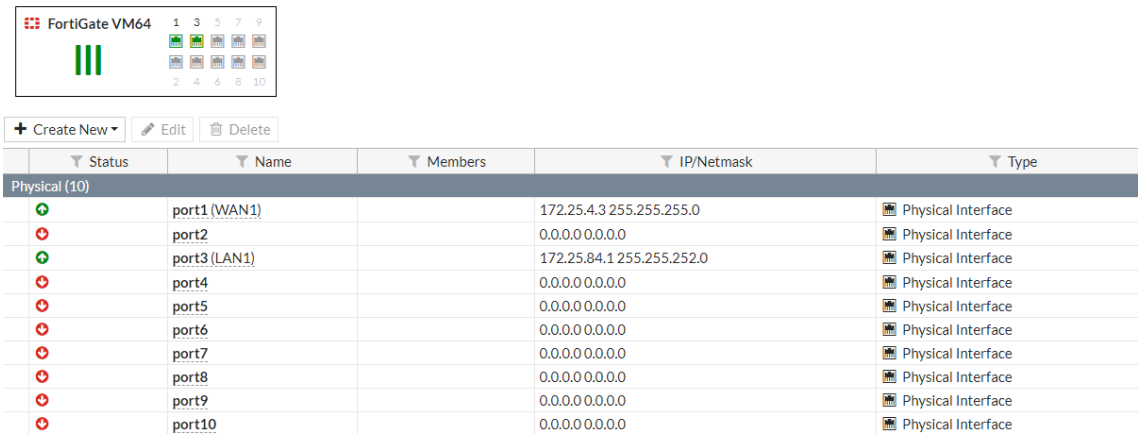

Figura 41. Interfaces declaradas en el cortafuegos back-end.

La primera interfaz (WAN1) es la que se encarga de conectar con el primer *firewall* (***front-end***) a través de la red VMnet3. En cambio, la tercera interfaz se trata de la interfaz LAN, y es a través de ella que se va dar servicio a la red de la zona verde. A modo de pruebas, en este extremo hay conectado una máquina virtual (equipo interno) para realizar aquellas comprobaciones pertinentes desde la zona verde.

Esta debe ser la primera configuración que se lleva a cabo, pues sin tener las interfaces correctamente configuradas se hace imposible operar con el cortafuegos.

En el séptimo anexo se puede encontrar la configuración de ambas interfaces detalladas para su consulta.

5.4.2.2. Encaminamiento del tráfico

Anteriormente se ha comentado que aquellas redes que estén directamente conectadas al cortafuegos van a ser alcanzables directamente dado que se declaran de forma automática en su tabla de enrutamiento. Por este motivo, la única red que se desea alcanzar desde este *firewall* es la red externa, es decir, Internet. Esta ruta debe definirse como la ruta por defecto. Todo el tráfico interno que llegue al ***back-end*** debe desviarse

por la interfaz WAN mediante la puerta de enlace 172.25.4.1, es decir, el *firewall* ***front-end***, que ya decidirá por donde desvía el tráfico en función del estado de los enlaces con Internet de los dos proveedores gracias a la interfaz SD-WAN.

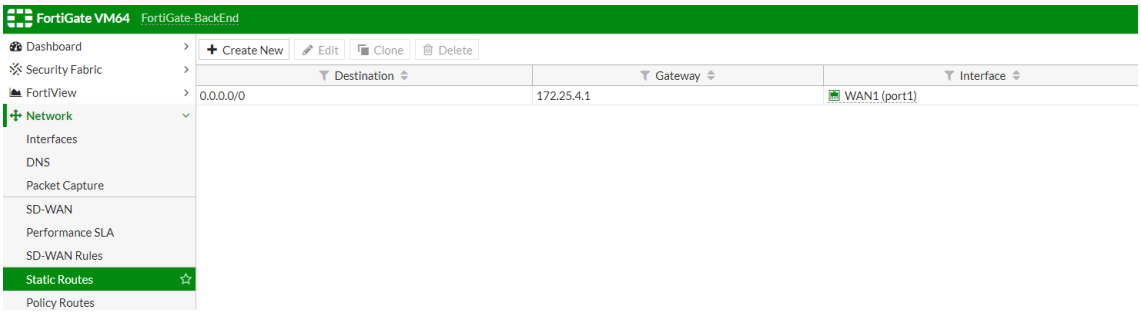

Figura 42. Ruta estática en el cortafuegos back-end.

Malhotra, R. (2002) dice que el uso de encaminamientos estáticos es poco escalable, pues a medida que crecen las necesidades y el tamaño de la red se hace más complicado encaminar todo el tráfico de manera correcta. Por este motivo, habla de que, en ese caso, deberá emplearse el direccionamiento dinámico usando diversos protocolos (OSPF, EIGRP o RIP). Dado que en la arquitectura presentada en el presente trabajo únicamente requiere de un encaminamiento hacia el *firewall* ***front-end***, éste se realizará de forma estática.

5.4.2.3. IPS

El sistema de prevención de intrusos (IPS) constituye una importante herramienta para lograr neutralizar ataques a la red que protege. A diferencia del IDS que únicamente analiza, compara y registra los eventos sin controlar el tráfico, este sistema es capaz de tener control sobre el tráfico y bloquear ciertos paquetes en función de su contenido, tras analizarse y compararse con una serie de firmas extraídas de los ataques más conocidos.

Tal como se ha comentado, tanto las reglas del *firewall* como del IPS del ***back-end*** deben tener en cuenta las del ***front-end***, es decir, deben ser un conjunto donde se incluyan las reglas del primer *firewall* y, además, aquellas más estrictas para proteger la zona verde. Esto se hace debido a que es posible que, en un momento determinado, el ***front-end*** deje de estar operativo, y este cortafuegos deba adoptar el rol de ambos por lo que debe estar configurado con aquellas reglas menos severas que se configuraban en el ***front-end***, además de aquellas más severas y estrictas que se implantan por primera vez en este *firewall*.

La zona verde está compuesta por dos servidores Windows que utilizan el protocolo DHCP para las conexiones, multitud de equipos cliente con sistema operativo Windows, y los *switches* y puertas de enlace basados en sistemas Linux. También se va a prevenir ataques a través de conexiones TCP/UDP, SSH y Telnet gracias a la configuración de unos filtros cuyas firmas satisfagan dicho criterio.

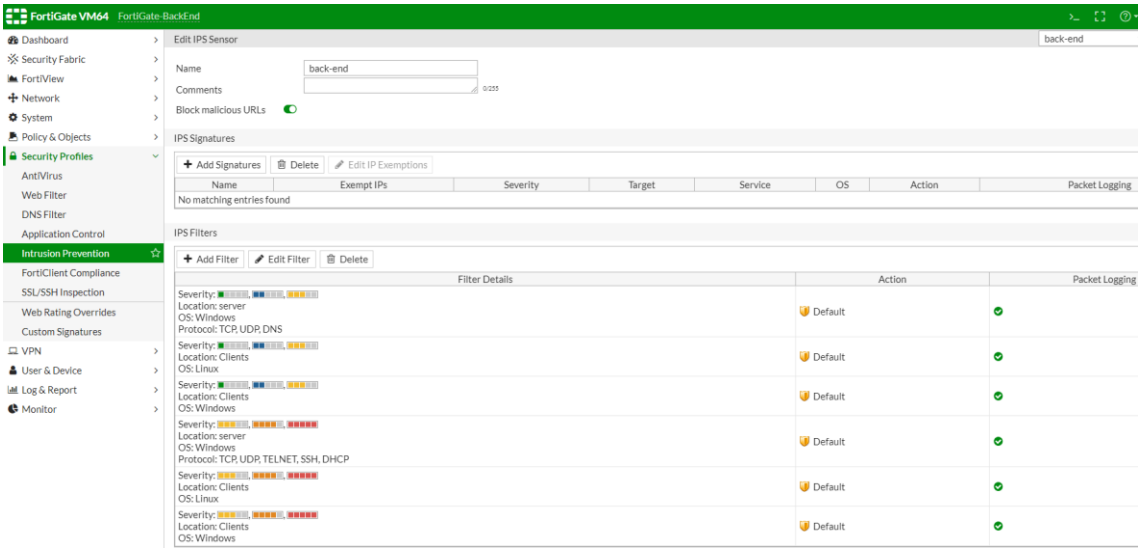

Figura 43. Filtros IPS configurados en el cortafuegos back-end.

Como se observa en la figura 43, los tres primeros filtros configurados se corresponden con los configurados en el ***front-end*** con una severidad inferior, mientras que los tres últimos filtros hacen referencia a los configurados de forma exclusiva en este cortafuegos, y que van a constituir, en combinación con las reglas del *firewall*, una importante herramienta para proteger todos aquellos activos que se encuentran en la zona verde de la red. La acción que deben llevar a cabo se establece como "*default*", lo que quiere decir que se aplica la que lleva predeterminada cada firma que compone dicho filtro. Además se activa el "*packet logging*", que realizaría además la función de un IDS: analizar, comparar y registrar.

Tal como se ha comentado con anterioridad, todas estas funciones se corresponden con aquellas de la capa tres del modelo ISO/OSI, es decir, aquellas relacionadas con los paquetes IP (Origen, destino, protocolo y puerto).

5.4.2.4. Reglas del firewall

Como se ha mencionado, este *firewall* va a poseer exactamente las mismas reglas en cuanto a tráfico externo se refiere. Esto se emplea para crear una cierta redundancia en caso de que se produzca una parada del presente cortafuegos. Por este motivo, solo va a disponer de una única regla declarada en el *firewall*. El motivo es que el sistema IPS ya está analizando amenazas en los diferentes paquetes de la red, y además por defecto se tiene activo un sistema que evita la suplantación de identidad, por lo que lo único que queda es hacer uso de esta regla para filtrar el tráfico IP (capa tres del modelo ISO/OSI) en función de las necesidades de la empresa. De igual forma, el tráfico interno va a estar bloqueado de forma implícita, excepto para aquellas conexiones establecidas y/o relacionadas que de forma predeterminada sí se permite.

Los servicios que se van a implementar en dicha regla son aquellos que satisfacen los tipos de acceso mencionados en la tabla 30, y que son los que están actualmente en funcionamiento, por lo que se define la regla como se observa a continuación:

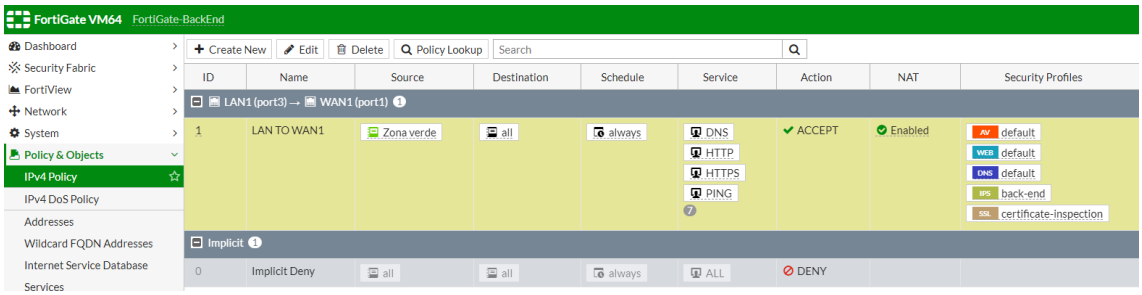

Figura 44. Resumen de las reglas en el back-end.

En la figura 44 se observa la regla mencionada, la cual permite todo el tráfico externo que cumpla únicamente con los servicios establecidos por Autotrim.

El IPS continua activo en dicha regla, analizando el tráfico y descartando aquellos paquetes que supongan una amenaza con cualquier severidad.

6. Presupuesto

El presente trabajo parte de una red existente, por ese mismo motivo se aprovecha gran parte de la infraestructura disponible. A pesar de ello, se hace necesario la compra de nuevo hardware y material para poder desarrollar e implementar la arquitectura de red diseñada a lo largo del presente proyecto.

Para realizar un análisis del coste de los elementos, se va a dividir éstos según la naturaleza de los mismos. Todos los precios indicados son PVP, por lo que es necesario realizar un descuento de entre un 20% y un 30% para obtener el precio PVD.

Cabe destacar que este presupuesto trabaja sobre unos importes orientativos, y que podrá variar en base a la variación del coste de los dispositivos seleccionados.

6.1. Hardware

Tabla 32. Importe total del hardware.

PRODUCTO	PROVEEDOR	PRECIO €	UNIDADES	IMPORTE €
Router Mikrotik CCR1036-8G-2S+EM	Amazon	**1.115,72 €**	2	**2.231,44 €**
Fortinet Fortigate 600E	Amazon	**6.240,00 €**	1	**6.240,00€**
Fortinet Fortigate 500E	Amazon	**5.166,68 €**	1	**5.166,68 €**
HP Workstation Z4 G4	HP	**2.680,99€**	2	**5.361,98 €**
			TOTAL HARDWARE (€)	**19.000,01€**

En la tabla 32 se observa el importe detallado de cada uno de los componentes hardware de los que se debe realizar una compra para llevar a cabo el proyecto.

En cuanto a software no se detalla una tabla de importe dado que se ha optado por emplear software de código libre, y por tanto gratuito (Snort y Ossec).

6.2. Accesorios

El resto del importe que se debe invertir va a derivar en accesorios para interconectar los diferentes dispositivos, así como en dispositivos que se hacen necesarios para el correcto funcionamiento de los mismos. Hacen falta cuatro cables de fibra óptica para conectar los dos *routers* al ***front-end,*** otro cable para conectar el front-end con el back-end, y, finalmente otro para conectar el primer *firewall* con el segundo, y finalmente otro cable para conectar el ***back-end*** con el *switch* **AUTSW084010.** Para poder conectar correctamente estos cables de fibra óptica a los diferentes dispositivos hace falta transceptores SFP para conectarlos a los puertos habilitados para ello. Estos dispositivos deben ser de la marca del fabricante de los dispositivos para conservar la garantía. En total, dos de Cisco y cuatro de Fortinet.

Finalmente se prevé la compra de un cable RJ-45 de cinco metros de categoría seis para conectar el servidor DNS al *firewall* ***front-end***.

No se estima la compra extra de cables RJ-45 dado que los dispositivos propuestos sustituirían a los actuales que ya poseen cables de este tipo de categoría, y que resultan totalmente solventes para el caso actual.

Tabla 33. Importe total accesorios.

PRODUCTO	PROVEEDOR	PRECIO €	UNIDADES	IMPORTE €
Cable fibra óptica 5 mts dúplex monomodo PVC(OFNR)	FS	**3,40 €**	4	**13,6 €**
Transceptor Mikrotik S+RJ10 10000Mbit/s SFP+	Amazon	**45 €**	2	**90 €**
Transceptor QSFP+ MTP/MPO 40GBASE-SR4	FS	**35 €**	4	**140 €**
Cable de Red Ethernet LAN RJ45 UTP Cat 6 4.6m 10/100/1000 Mbps hasta 10 Gbps	FS	**2,90 €**	1	**2,90 €**
			TOTAL ACCESORIOS (€)	**246,5 €**

Se estima solo la compra de aquellos elementos que, o bien sustituyen a los actuales, o bien significan un nuevo elemento en la arquitectura. Sin embargo, dado que se

mantiene la mayor parte de la red en lo relacionado con el hardware, no se debe renovar gran parte de la misma. Esto es gracias también a que el hardware actual que se decide mantener acaba de ser recientemente actualizado a un hardware a la altura de la nueva arquitectura de la red, capaz de dar soporte a toda la empresa con total solvencia.

Relación de proveedores:

Tabla 34. Relación de proveedores.

Proveedor	Contacto
Amazon	http://www.amazon.es
FS	http://www.fs.com
HP	http://www.hp.es

7. Conclusiones

El presente trabajo ha estudiado la red actual de la empresa Grupo Antolín-Autotrim S.A.U en busca de posibles vulnerabilidades. Este estudio ha dejado en evidencia que algunos de los activos que componen la red están expuestos a ciertos riesgos.

Los resultados obtenidos en base al objetivo principal del trabajo – "conseguir diseñar una red segura para la empresa GA-Autotrim" – permiten concluir que es posible alcanzar un nivel de seguridad mucho mayor al actual empleando diversas técnicas relacionadas con la arquitectura de la red.

El análisis de los riesgos y el estudio de las vulnerabilidades que se ha llevado a cabo se han establecido como piezas clave en el desarrollo de la solución, pues han ayudado a entender en qué puntos se debían focalizar las diferentes técnicas empleadas.

El resultado del este análisis de riesgos ha ayudado a dilucidar la arquitectura de red propuesta como solución, y ha permitido desarrollarla en base a unos riesgos que mitigar. El uso de una arquitectura ordenada por diferentes zonas ha conseguido aislar completamente el tráfico de Internet a la red interna proporcionando una seguridad elevada. Gracias al uso de cortafuegos como puntos de nexo entre las diferentes zonas se ha comprobado que resulta mucho más complicado completar satisfactoriamente un ataque dado que se limita el tráfico interno.

La implementación de la red en un entorno virtual ha permitido comprobar la mejora sustancial lograda en cuanto a seguridad de la red, al quedar más protegida del exterior, así como mejorar los supuestos que no se habían tenido en cuenta en el desarrollo.

Los resultados obtenidos en el presente trabajo pueden servir como reflexión para diversas Pequeñas Y Medianas Empresas (PYMEs) que desconocen el uso de las técnicas y elementos de los que se han hecho uso en el trabajo. Es posible mejorar la seguridad de forma importante únicamente haciendo uso de software de código libre y mejorando la arquitectura de la red, es decir, con una inversión relativamente baja se puede mejorar de forma drástica la seguridad. Por tanto, como síntesis, las propuestas de mejora se pueden articular sobre dos ejes: el análisis de riesgos, y el desarrollo de una arquitectura organizada en base a ellos.

No obstante, este estudio presenta algunas limitaciones que sirven de base para futuros proyectos que se pueden llevar a cabo en la red de Grupo Antolín-Autotrim S.A.U que se presentan en el apartado 7.2.

7.1. Relación del trabajo con los estudios cursados

El desarrollo del trabajo realizado hace uso de diversas técnicas y tecnologías que se enmarcan dentro de la especialización de la informática conocida como "Tecnologías de la Información" y, por tanto, guardan una estrecha relación entre sí.

El análisis y desarrollo de una arquitectura de red segura viene directamente relacionado con diversas asignaturas de la especialización mencionada, como por ejemplo: "Diseño y Configuración de Redes de Área Local", "Redes Corporativas", "Seguridad en Redes", o "Administración de Sistemas". Estas asignaturas han aportado la amplia base de conocimientos en los que se basa el proyecto, los cuales han sido ampliados para definir el problema y poder desarrollar la solución.

Por una parte, el hecho de haber cursado dichas asignaturas ha permitido hacer un uso correcto de las diferentes técnicas y tecnologías estudiadas para llevar a cabo el proceso de mejora de la arquitectura de la red de la empresa Autotrim. Por otra parte, ha servido para despertar el interés por la mejora constante de la seguridad.

La realización del proyecto ha requerido del uso de diferentes competencias transversales y destrezas adquiridas a lo largo de los estudios. En concreto, se ha hecho uso de las competencias basadas en el diseño y proyecto, instrumental específica, y análisis y resolución de problemas.

Gracias a las destrezas adquiridas mediante la competencia "diseño y proyecto" se ha logrado en mayor grado el diseño del proyecto de manera ordenada. La competencia "instrumental específica" ha contribuido en gran medida a que se haga un buen uso del diferente software empleado para realizar las pruebas pertinentes, mientras que la competencia "análisis y resolución de problemas" ha ayudado a realizar un correcto análisis del problema actual para encontrar la solución más adecuada.

En definitiva, los estudios cursados han establecido una serie de técnicas, tecnologías y buenas prácticas que han servido como base, y que, habiendo sido ampliadas mediante la búsqueda de información, han dado lugar al desarrollo efectivo del presente proyecto.

7.2. Trabajos futuros

El presente proyecto define una arquitectura segura básica para Autotrim, es decir, determina una arquitectura segura a partir de la existente para reducir las vulnerabilidades y proteger mejor los actuales activos frente amenazas externas. Sin embargo, este proyecto supone un punto de partida a una enorme ventana de mejoras y trabajos futuros que de él pueden derivar.

Se van a presentar tres posibles ampliaciones basadas en el presente trabajo que se han planteado durante la realización del mismo.

7.2.1. Uso de VLANS

En primer lugar, resulta interesante el uso de diferentes VLANS en la zona verde de la red. A pesar de que no aportan seguridad extra desde el punto de vista de una amenaza externa, sí resultan de gran utilidad para ordenar el tráfico y de esta forma poder distinguir con facilidad el origen del mismo.

Los *switches* con los que cuenta actualmente la zona verde de la red soportan los estándares de etiquetado 802.1Q necesarios para el uso de VLANS.

Se establecería una VLAN por cada uno de los *racks* pertenecientes a un departamento. Sin embargo, según las políticas actuales de la empresa, se requiere de comunicación entre dispositivos pertenecientes a estas diferentes VLANS. Para ello sería necesario adquirir un *switch* de capa tres del modelo ISO/OSI que reemplace al switch **AUTSW084010**, es decir, que posea las funciones de enrutamiento características de un *router*. Esto es necesario porque se requiere de un encaminador que sea capaz de reenviar el tráfico de una VLAN a otra, dado que cada VLAN es un dominio de *broadcast* único y, por tanto, de manera predeterminada no pueden comunicarse entre ellas.

También sería posible realizar la comunicación entre VLANS manteniendo el switch mencionado anteriormente, y realizar el reenvío del tráfico a través del *firewall* ***back-end*** con la diferencia de que, en este caso, se trabajaría con todas las VLANS sobre la misma interfaz física, por lo que sería necesario realizar el reenvío del tráfico mediante un enlace troncal (*trunk*). Gracias a estos enlaces troncales se permite el reenvío de tráfico de diferentes VLANS mediante el mismo enlace físico.

7.2.2. Uso de una VPN

Se puede llegar a hacer necesario la conexión de diferentes sedes junto con la central del Grupo Antolín para compartir recursos y servicios. Por este motivo se hace necesario el uso de VPNs. Por definición, una red privada virtual (VPN) es una tecnología empleada para transportar tráfico de una red privada a otra a través de una pública, en este caso

Internet, garantizando la integridad y la privacidad. Generalmente se consigue mediante la creación de un túnel que atraviesa la red pública.

En este caso, la conexión se trataría de una VPN *firewall* a *firewall*, es decir, entre el *firewall* de Autotrim y el *firewall* de la central o de otras sedes. Para este caso, Fortigate proporciona comunicación segura a través de una red pública (Internet) entre múltiples cortafuegos, haciendo uso de diferentes tecnologías como IPsec y sockets seguros (SSL). Gracias a ello se crearía un túnel directo entre ambos cortafuegos, donde se protegería la integridad y la privacidad de la información como si de la misma red de área local se tratara.

7.2.3. Uso de enrutamiento dinámico

Durante la implementación del proyecto se ha mencionado las limitaciones que supone el encaminamiento estático del tráfico en los diferentes dispositivos con capacidad de enrutamiento. Este tipo de enrutamiento es útil atendiendo al tamaño de la red estudiada, es decir, en un entorno local donde solo se debe encaminar el tráfico en uno o en dos sentidos. A medida que la red va creciendo, y el tráfico debe fluir hacia más destinos, comienza a hacerse necesario la declaración de más y más rutas a través de las cuales debe viajar el tráfico, lo que se convierte en una ardua tarea además de poco eficiente, por lo que se concluye que es poco escalable.

Por este motivo, nace el enrutamiento dinámico soportado por los cortafuegos y los *routers* presentados en el proyecto. Este tipo de enrutamiento se basa en tres grandes protocolos: OSPF, BGP y RIP. OSPF es utilizado generalmente en redes privadas, mientras que BGP se usa más en redes públicas. Mientras tanto, RIP está prácticamente en desuso y rara vez se utiliza actualmente.

Estos protocolos se basan en dos métodos: vector distancia y algoritmo de estado de enlace. Las diferencias entre estos dos métodos están básicamente en el momento del intercambio de la información de enrutamiento, en qué tipo de información se envía durante el intercambio, y cómo gestionar cambios de topología.

Gracias al uso del enrutamiento dinámico se podría obtener una gran escalabilidad de la red, y un encaminamiento del tráfico con un mantenimiento muy bajo, ya que el enrutamiento dinámico se encargaría de determinar cuál es el camino óptimo para alcanzar el destino.

8. Referencias

Alonso, C. G. I. L. M., Gabriel, D. O., Ignacio, A. A., & Elio, S. R. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES*. Madrid, España: UNED.

Análisis de riesgos. (2017, 16 enero). Recuperado 8 junio, 2019, de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Bautts, T., Kirch, O., Dawson, T., & Purdy, G. (2005). *Linux Network Administrator's Guide*. NY, EEUU: O'Reilly Media.

Convery, S. (2004). *Network Security Architectures*. Indianapolis, EEUU: Cisco Press.

Creating a Strong Firewall Security Policy. (s.f.). Recuperado 29 junio, 2019, de https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

Colaboradores de Wikipedia. (2019, 30 abril). *Zona desmilitarizada (informática)*. Recuperado 28 junio, 2019, de https://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica)

Delfirosales, D. R. (s.f.). *Configuración de DHCP Server en FortiGate*. Recuperado 29 junio, 2019, de https://delfirosales.blogspot.com/2015/12/configuracon-de-dhcp-server-en-fortigate.html

Fortinet Documentation Library. (s.f.). Recuperado 29 junio, 2019, de https://docs.fortinet.com/

Fortinet Knowledge Base - View Document. (s.f.). Recuperado 29 junio, 2019, de https://kb.fortinet.com/kb/documentLink.do?externalID=FD35222

Deal, R. A. (2004). *Cisco Router Firewall Security*. Indianapolis: Cisco Press.

Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). *Inside Network Perimeter Security*. EEUU: Sams Pub.

Magerit 3.0. (s.f.). Recuperado 8 junio, 2019, de https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar/metodologia.html

Malhotra, R. (2002). *IP Routing*. London: O'Reilly Media, Incorporated.

Paulo Colomés, P. C. (2015, 5 diciembre). *¿Qué es la DMZ?* Recuperado 28 junio, 2019, de http://www.redescisco.net/sitio/2015/12/05/que-es-la-dmz/

RedIRIS - Cortafuegos: Conceptos teóricos. (s.f.). Recuperado 22 junio, 2019, de https://www.rediris.es/cert/doc/unixsec/node23.html

Redundant Internet with SD-WAN. (s.f.). Recuperado 29 junio, 2019, de https://docs.fortinet.com/document/fortigate/6.0.0/cookbook/990932/redundant-internet-with-sd-wan

9. Anexos

9.1. Anexo 1. Red actual de Autotrim

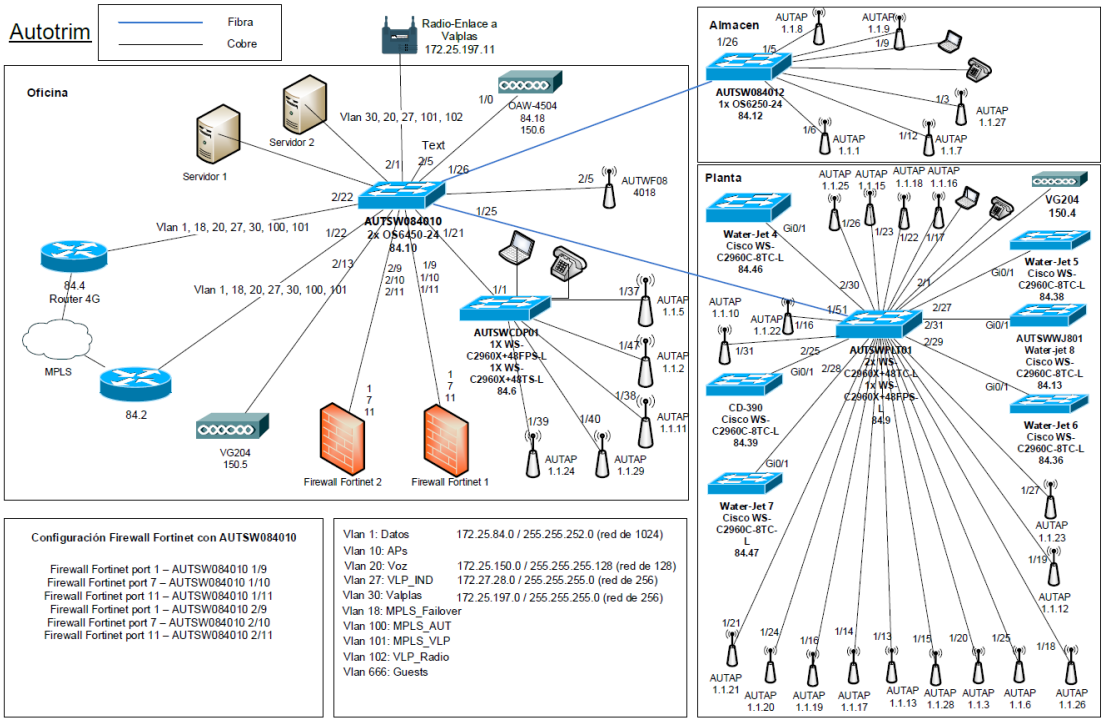

Figura 45. Diagrama de red actual

En la anterior figura se muestra el diagrama de red actual de Autotrim. La parte de la oficina, que es la principal, se encuentra ubicada en el CPD, junto a los servidores. Adicionalmente aparece el *rack* de planta, que es un *stack* de tres *switches* Cisco, todos con 48 puertos, que va conectado mediante fibra óptica al CPD. A este *rack* se le conectan diversos *switches* de menor tamaño que hacen la función de *hub* en cada una de las líneas para concentrar todos los dispositivos que acceden a la red en una línea en un único punto. Además, se conectan multitud de puntos de acceso que están repartidos a lo largo de la planta, y que comparten cuatro redes wifi principales que se detallarán a continuación.

El siguiente *rack* es el de almacén, de menores dimensiones, y es únicamente un *switch* de 24 puertos que concentra un reducido número de puntos de acceso repartidos por el almacén. Cabe destacar que este *rack* también va enlazado mediante fibra óptica al CPD.

A pesar de que los dos *racks* que se encuentran ubicados fuera del CPD y están enlazados a él mediante fibra óptica, también lo están mediante cobre, para de esta forma garantizar una cierta disponibilidad.

El punto clave de la red es el *switch* **AUTSW084010**, un stack compuesto de dos *switches* de 24 puertos cada uno. A este *switch* se conecta el *router* principal y los de backup, además de los dos *firewalls* y los enlaces de fibra óptica a los *racks* de planta.

También dispone de un radioenlace a otra planta del grupo Antolín que se encuentra en las proximidades para proporcionar red a la otra planta.

A continuación se detalla cada uno de los elementos que componen la red:

Tabla 35. Listado de elementos actuales en la red de Autotrim.

NOMBRE	TIPO	DESCRIPCIÓN	MARCA	MODELO
***Router* 84.2**	*Router*	*Router* principal	Cisco	892FSP
***Router* 4G 84.4**	*Router*	*Router* backup por red 4G	Cisco	800 Series
***Firewall* 1**	*Firewall*	Puerta de enlace de la red y *firewall* principal.	Fortinet	Fortigate 100E
***Firewall* 2**	*Firewall*	*Firewall* de backup.	Fortinet	Fortigate 100E
AUTSW084010	*Switch*	*Switch* general en CPD	Alcatel	2x OS6450-24
AUTSWCPD01	*Switch*	*Switch* de *rack* de oficinas en CPD para ordenadores y teléfonos	Cisco	WS-C2960X+48FPS-L WS-C2960X+48TS-L
AUTSWPLT01	*Switch*	*Switch* de *rack* de planta para ordenadores y teléfonos, además de maquinaria industrial	Cisco	2x WS-C2960X+48TC-L 1x WS-C2960X+48FPS-L
AUTSW084012	*Switch*	*Switch* de *rack* de almacén para ordenadores y teléfonos	Alcatel	OS6250-24
AUTSWWJ801	*Switch*	Mini *switch* Water-Jet 8	Cisco	WS-C2960C-8TC-L
Water-jet 4	*Switch*	Mini *switch* Water-Jet 4	Cisco	WS-C2960C-8TC-L
CD-390	*Switch*	Mini *switch* rebordeadoras	Cisco	WS-C2960C-8TC-L
Water-jet 7	*Switch*	Mini *switch* Water-Jet 7	Cisco	WS-C2960C-8TC-L
Water-jet 5	*Switch*	Mini *switch* Water-Jet 5	Cisco	WS-C2960C-8TC-L
Water-jet 6	*Switch*	Mini *switch* Water-Jet 6	Cisco	WS-C2960C-8TC-L
AUTAPX.X.XX	Punto de acceso	Antenas puntos de acceso	Toshiba	Alcatel OAW-AP61
OAW-4504	Conmutador WLAN	Concentrador de los diferentes puntos de acceso	Alcatel	OmniAccess OAW-4504

VG-204	Puerta enlace VoIP	Puertas de enlace para los teléfonos que funcionan con voz sobre IP	Cisco	VG 204
Radio-Enlace	Enlace con otra planta	Enlace físico mediante vía dedicada con la planta de Valplas	Cisco	Aironet 1240AG

Al *switch* **AUTSW084010** van conectados los dos servidores de la empresa, que contienen todas las máquinas virtuales con todos los servidores que están en uso, entre ellos el servidor DHCP, encargado de asignar direcciones IP a los dispositivos de la red, el servidor de ficheros, que contiene todas las carpetas de acceso público y las unidades de red personal de cada usuario, etc.

Los ordenadores de la empresa y los teléfonos VoIP van conectados en exclusiva a uno de los tres *racks*, bien sea el de oficinas, el de planta, o el de almacén.

9.2. Anexo 2. Evaluación de riesgos cuantitativa

9.2.1. Tabla para el cálculo de la probabilidad de una amenaza

Tabla 36. Cálculo de la probabilidad de una amenaza.

CUANTITATIVO	DESCRIPCIÓN
1	La amenaza se materializa como mucho una vez al año.
2	La amenaza se materializa como mucho una vez al mes.
3	La amenaza se materializa como mucho una vez a la semana.

9.2.2. Tabla para el cálculo del impacto

Tabla 37. Cálculo del impacto.

CUANTITATIVO	DESCRIPCIÓN
1	El daño derivado de la amenaza no tiene consecuencias relevantes.
2	El daño derivado de la amenaza tiene consecuencias importantes.
3	El daño derivado de la amenaza tiene consecuencias muy graves.

9.3. Anexo 3. Amenazas fuera del caso de estudio

9.3.1. Desastres naturales

Sucesos que pueden ocurrir sin intervención de ningún ser humano como causa directa o indirecta:

Tabla 38. Amenazas asociadas a desastres naturales.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
DN_1	Fuego	Disponibilidad	Equipos
DN_2	Daños por agua	Disponibilidad	Equipos

9.3.2. De origen industrial

Sucesos que pueden ocurrir de forma accidental, se dan a partir de la actividad humana en un entorno industrial como Autotrim. Estas amenazas se pueden dar de forma accidental o deliberada:

Tabla 39. Amenazas asociadas a origen industrial.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
OI_1	Fuego	Disponibilidad	Equipos
OI_2	Daños por agua	Disponibilidad	Equipos
OI_3	Avería de origen físico o lógico	Disponibilidad	Equipos/Software
OI_4	Corte del suministro eléctrico	Disponibilidad	Equipos
OI_5	Condiciones inadecuadas de temperatura	Disponibilidad	Equipos

9.3.3. Errores y fallos no intencionados

Fallos no intencionados causados por las personas:

Tabla 40. Amenazas asociadas a fallos no intencionados.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
FNI_1	Errores de los usuarios	Integridad/Confidencialidad/Disponibilidad	Datos/Servicios/Software
FNI_3	Difusión de software dañino	Integridad/Confidencialidad/Disponibilidad	Software
FNI_6	Escapes de información	Confidencialidad	-

9.3.4. Ataques intencionados

Fallos deliberados causados por las personas:

Tabla 41. Amenazas asociadas a ataques intencionados.

ID	TIPO DE AMENAZA	ATRIBUTOS AFECTADOS	ACTIVOS AFECTADOS
AI_10	Destrucción de información	Disponibilidad	Datos/Servicios/Software
AI_3	Difusión de software dañino	Integridad/Confidencialidad/Disponibilidad	Software

9.4. Anexo 4. Red propuesta

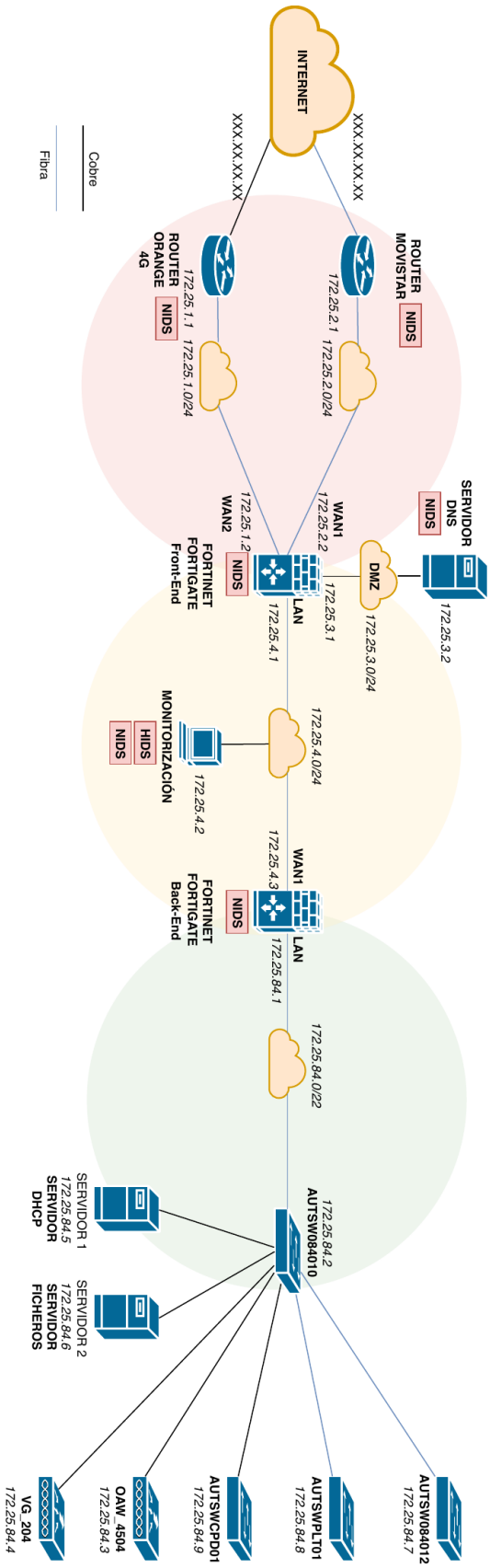

Figura 46. Arquitectura de red ampliada.

9.5. Anexo 5. Configuración VMware

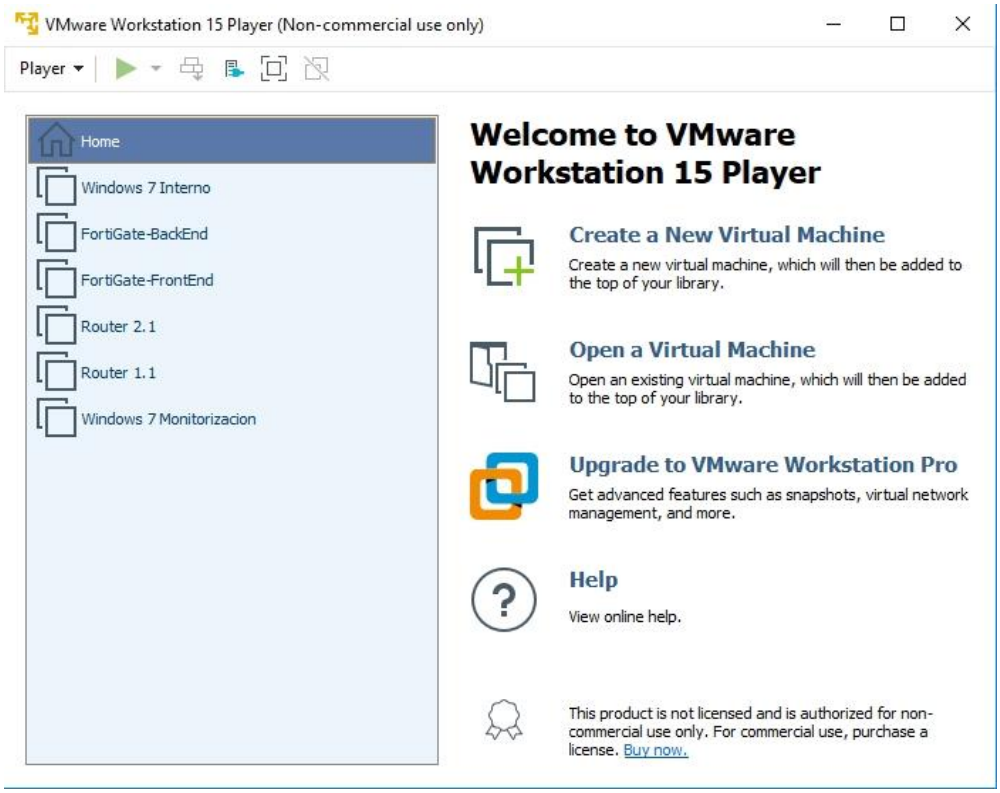

Figura 47. Pantalla principal VMware.

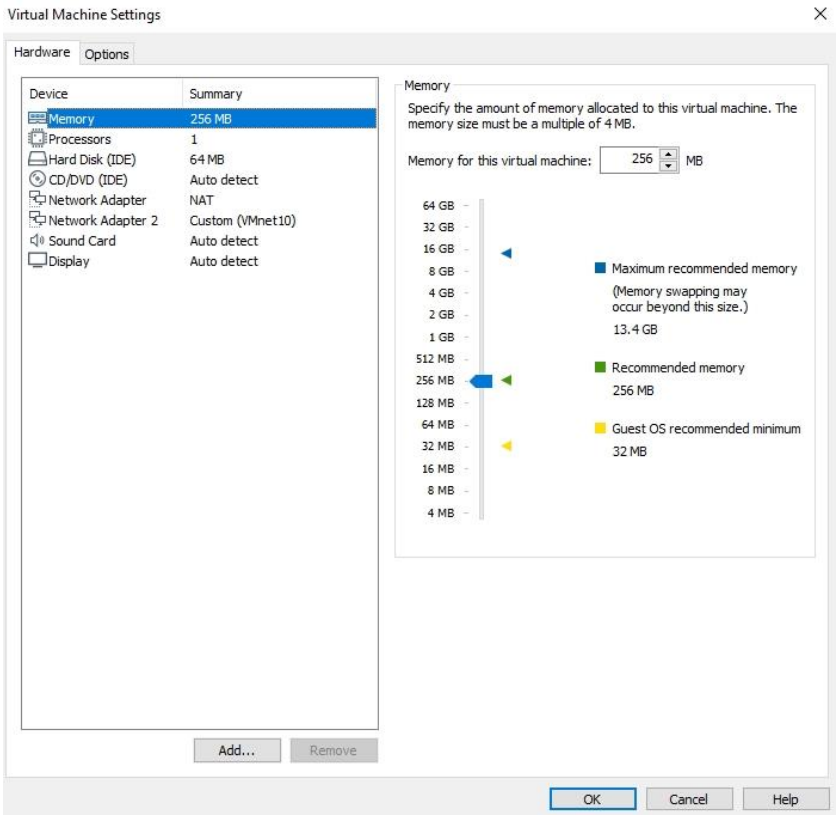

Figura 48. Configuración router 1.1.

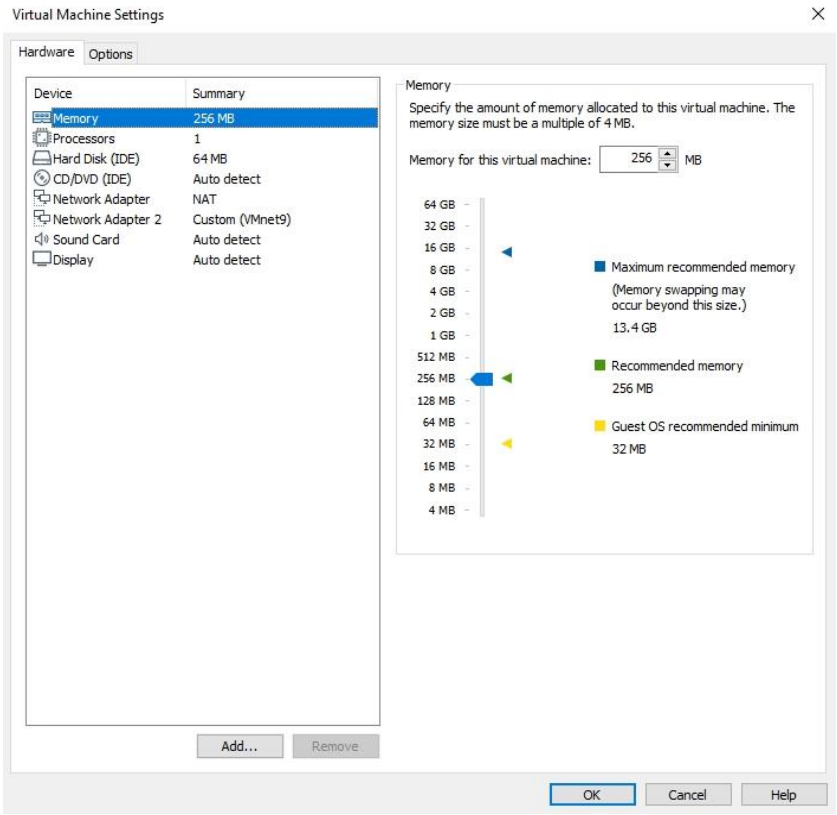

Figura 49. Configuración router 2.1.

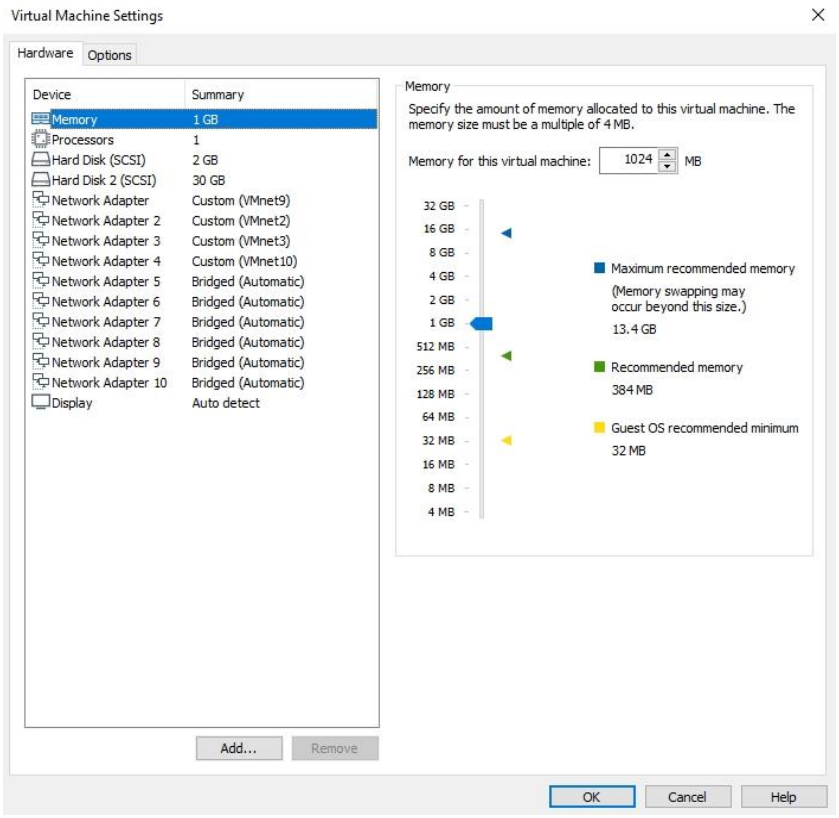

Figura 50. Configuración firewall front-end.

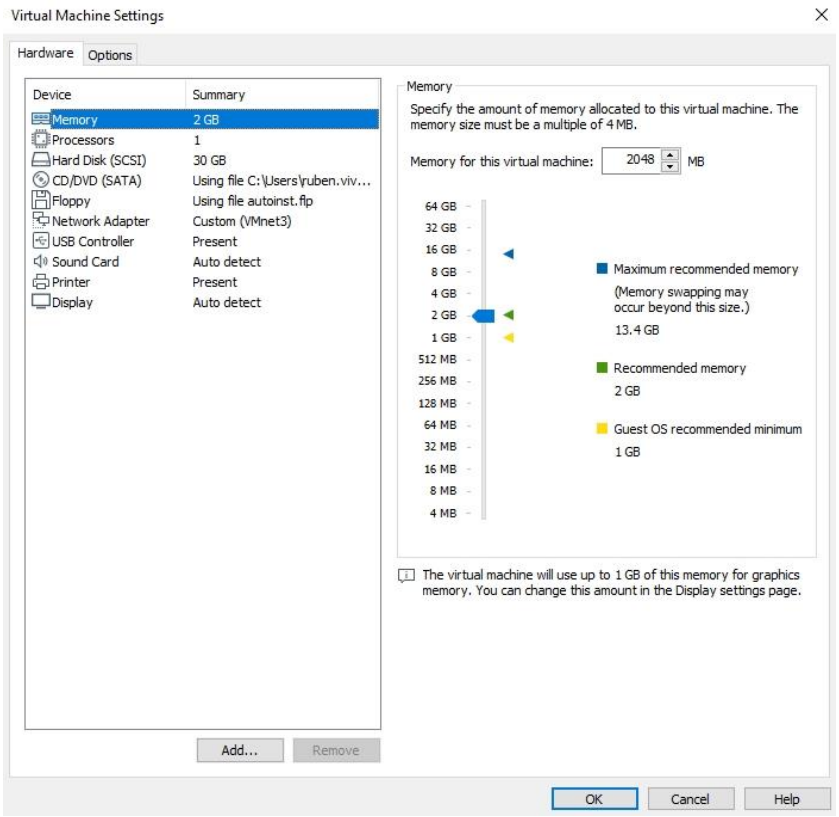

Figura 51. Configuración equipo monitorización.

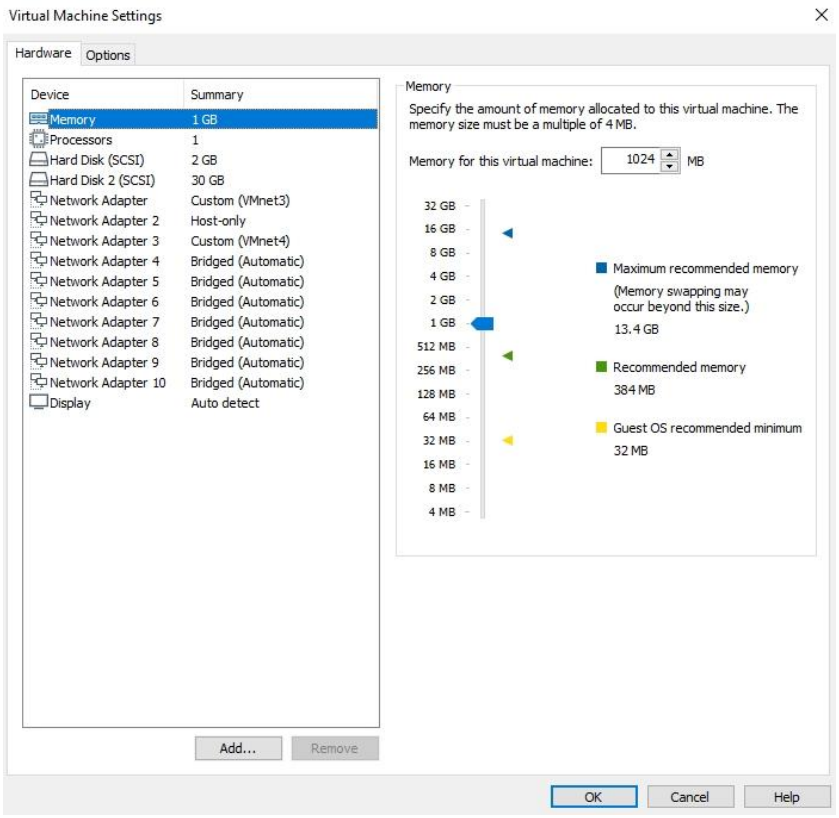

Figura 52. Configuración firewall back-end.

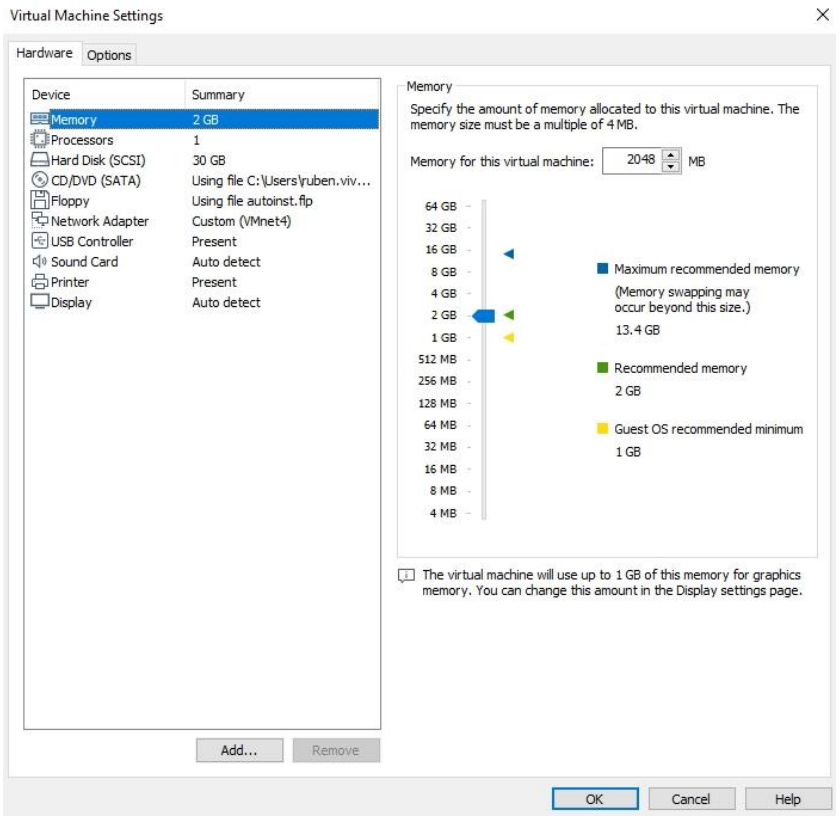

Figura 53. Configuración equipo interno.

9.6. Anexo 6. Interfaces cortafuegos front-end

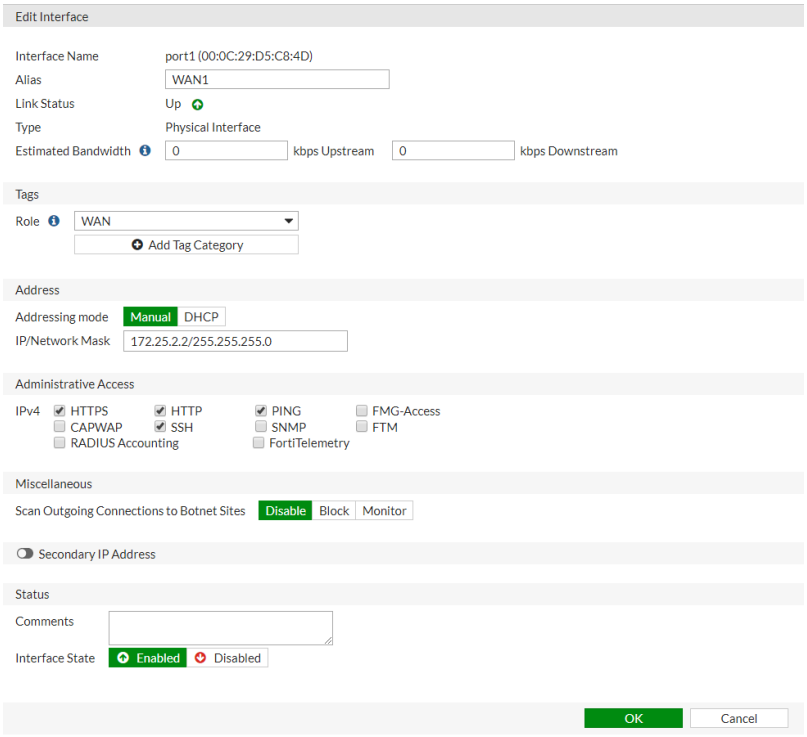

Figura 54. Interfaz WAN1 del front-end.

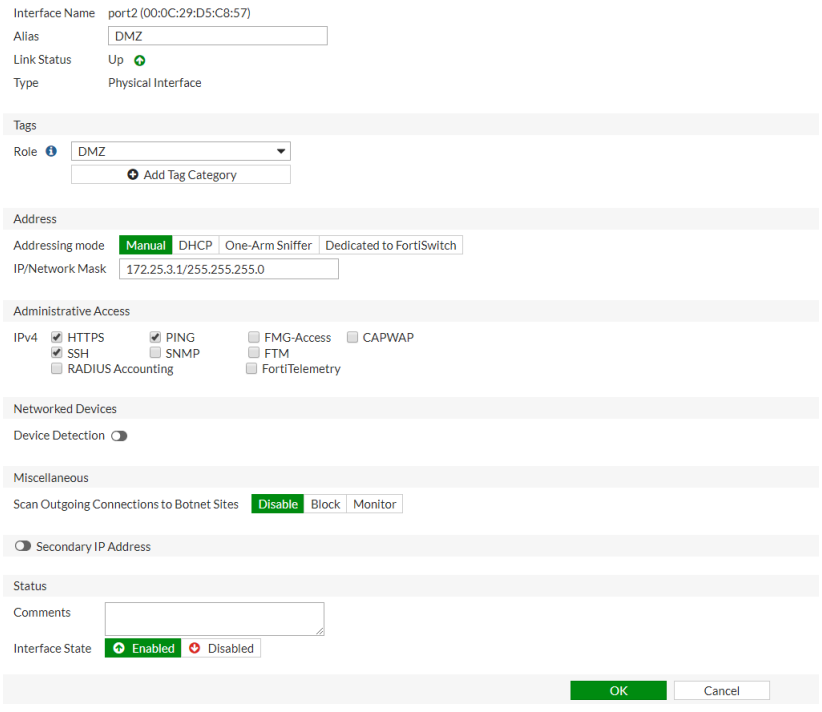

Figura 55. Interfaz DMZ en el front-end.

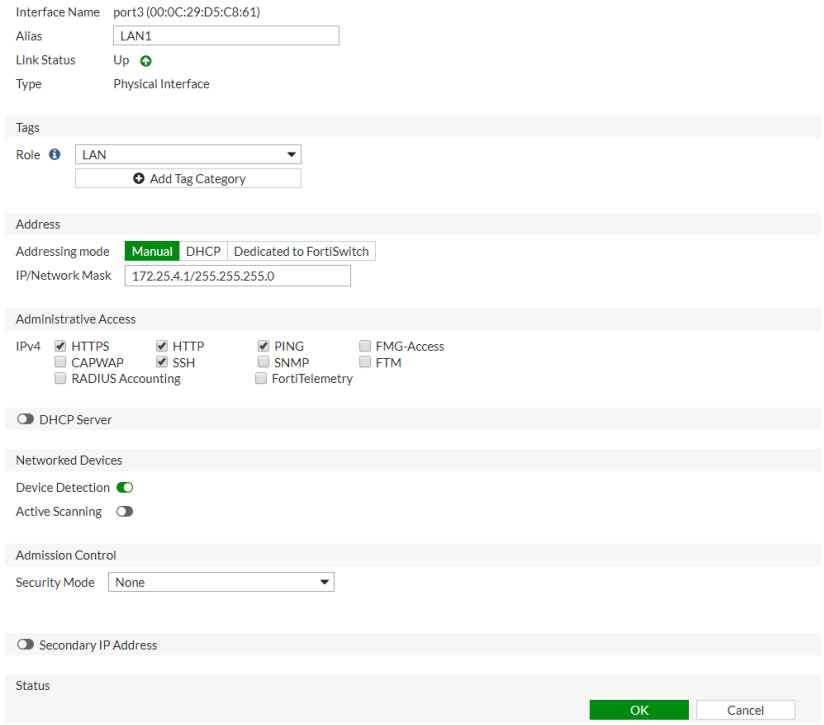

Figura 56. Interfaz LAN en el front-end.

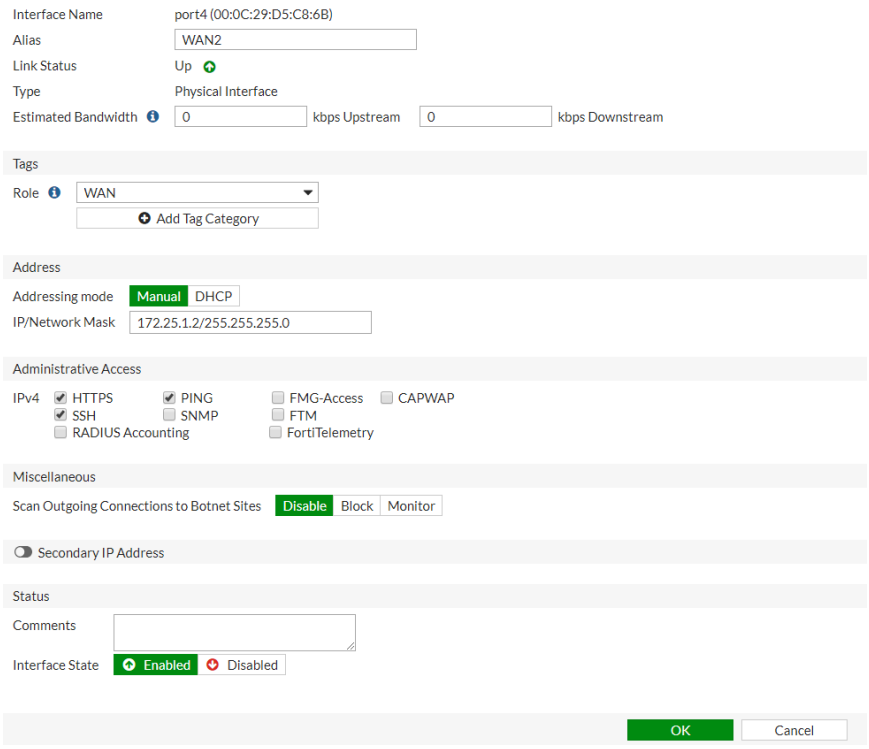

Figura 57. Interfaz WAN2 en el front-end.

9.7. Anexo 7. Interfaces cortafuegos back-end

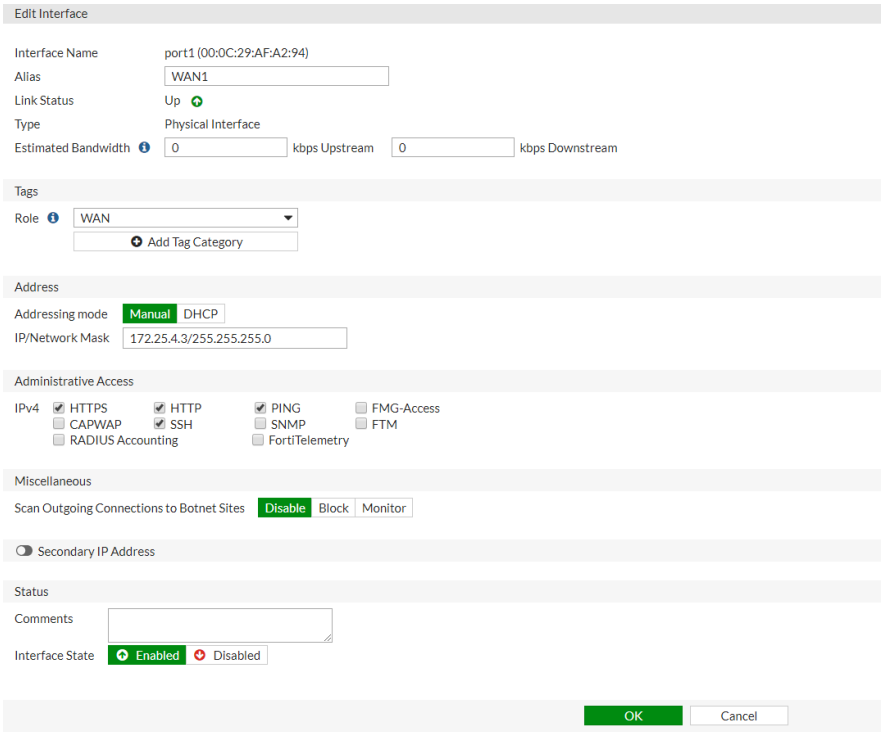

Figura 58. Configuración interfaz WAN en el back-end.

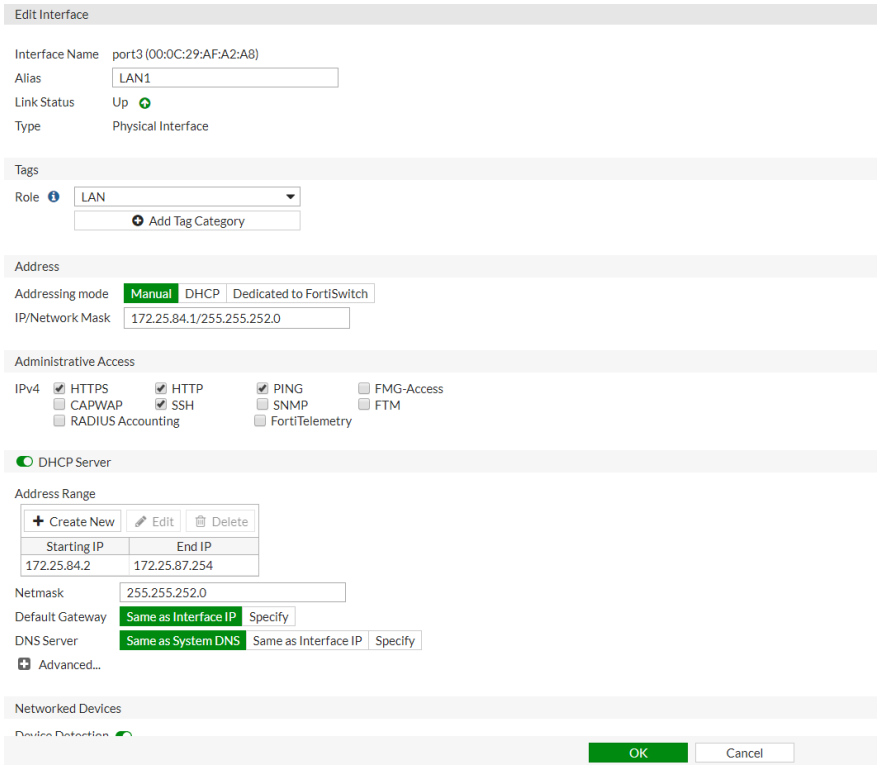

Figura 59. Configuración interfaz LAN en el back-end.

10. Glosario

Tabla 42. Glosario.

TÉRMINO	SIGNIFICADO
DMZ	Zona desmilitarizada
AP	Punto de acceso
CPD	Centro de procesamiento de datos
PoE	Power over Ethernet
DNS	Domain Name System
ISP	Internet Service Provider
NAT	Network Adress Translation
DHCP	Dynamic Host Configuration Protocol
VLAN	Virtual Lan
LAN	Local area network
NIDS	Network IDS
IDS	Intrusion detection system
HIDS	Host IDS
VPN	Virtual Private Network
HUB	Concentrador
NGFW	Next Generation Firewall
URL	Localizador de recursos uniforme
WWW	World Wide Web
FTP	File Transfer Protocol
P2P	Peer to Peer
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SD-WAN	Software defined wan
RIP	Routing Information Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
OSPF	Open Shortest Path First
PVP	Precio Venta al Público
PVD	Precio Venta al distribuidor
SFP	Small form-factor pluggable
SSL	Secure Sockets Layer
PYME	Pequeña Y Mediana Empresa
CGP	Centro de Gestión Personalizado
VoIP	Voice Over IP