UNIVERSITAT POLITÈCNICA DE VALÈNCIA

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
CAMPUS D'ALCOI

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Politécnica Superior de Alcoy

Análisis e implantación de un sistema de gestión de la seguridad de una red informática en una empresa en producción

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Sanus Ferri, Javier

Tutor/a: Llorca Alcón, Manuel

CURSO ACADÉMICO: 2022/2023

RESUMEN

Este TFG trata sobre la implementación e implantación de un sistema secundario de gestión de la seguridad de la red de una empresa en producción, para reemplazar el sistema principal en caso de avería o en caso de que el sistema principal necesite actualizarse. Para ello, se ha seguido una metodología ágil para cumplir con los objetivos propuestos, marcando distintas fases que se deben llevar a cabo y se pueden modificar en cualquier momento. Además, se han estudiado otros proyectos similares para observar cómo se han desarrollado y cómo mejorarlos. Asimismo, tras haber realizado un estudio de todas las ofertas disponibles en el mercado, se utiliza un software de código libre, Zentyal, que cumple con los requerimientos del cliente. Finalmente, se han instalado los módulos necesarios como el Firewall, el DHCP, las VLANs, conexión vía VPN… Y mediante las distintas pruebas finales se confirma el funcionamiento del sistema desarrollado.

ABSTRACT

This thesis focuses on the implementation and deployment of a secondary network security management system for a company in production, aiming to replace the primary system in case of failure or when an update is required. To achieve this, an agile methodology has been followed to fulfill the proposed objectives, setting different phases that can be modified at any time. Additionally, other similar projects have been studied to observe their development and identify areas of improvement. After conducting a study of all available market offers, an open-source software called Zentyal has been selected, as it meets the client's requirements. Finally, the necessary modules such as the firewall, DHCP, VLANs, VPN connection, etc., have been installed, and through various final tests, the functionality of the developed system has been confirmed.

PALABRAS CLAVES

Firewall, Sistema de seguridad, Código Libre, Gestión de redes, Zentyal.

AGRADECIMIENTOS

Este TFG ha sido posible gracias al apoyo y respaldo de las siguientes personas.

A mis padres y a mi hermano por su paciencia y ayuda siempre que la he necesitado.

A mi familia y amigos por acompañarme en todo momento y su confianza.

A mi tutor, Manolo Llorca, quien ha sido de gran ayuda y ha desempeñado su función de forma clave para completar el trabajo.

A Korott SL, y en especial a mis tres compañeros del Departamento de Sistemas, Gabriel, Gregorio e Iván, quienes me han ayudado, enseñado y acompañado en mis primeros pasos en el mundo laboral.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

1. INTRODUCCIÓN

El presente trabajo, dentro de la asignatura “Trabajo Fin de Grado” del “Grado en Ingeniería Informática” de la Universidad Politécnica de Valencia (UPV) en el campus de la Escuela Politécnica Superior de Alcoy (EPSA), representa la finalización de los estudios y los conocimientos adquiridos durante estos años en el grado mencionado anteriormente.

Con este proyecto, se pretende dar solución a la propuesta de implantación de un sistema secundario de gestión de la seguridad de la red informática en una empresa en producción, conocida a partir de este punto como Korott SL, para poder utilizarse en el momento en el que el sistema principal sufra algún incidente, al tratarse de un sistema crítico.

Por un lado, se utilizarán todos los medios de los que dispone actualmente Korott SL, intentando minimizar los costos, consiguiendo así el menor presupuesto posible.

Por otro lado, no existe una documentación previa dentro de la propia empresa, ni entre el personal, por lo que se deberá realizar un análisis exhaustivo, con el fin de conseguir la solución óptima y que se adapte a los requisitos propuestos.

Asimismo, este proyecto sigue las fases del ciclo de vida propio de un proyecto de administración de redes. Iniciando con un análisis de la situación de partida, se detectan las necesidades y los requisitos funcionales demandados por el cliente, para la posterior elaboración de una propuesta de solución. Tras el visto bueno del cliente, se llevarán a cabo las distintas fases de diseño, desarrollo, implantación, pruebas y mejoras.

Además, es un proyecto que tiene como finalidad el poder seguir mejorando o aumentando su valor para la empresa, ya que, existe un sinfín de posibilidades con el software que se ha decidido utilizar finalmente. Así que, a partir de este punto, se empezará con la descripción de los objetivos del proyecto y su posterior desarrollo.

1.1. Objetivos

El objetivo principal es el de desarrollar y documentar una solución, mediante todos los medios disponibles en Korott SL y utilizando el menor presupuesto posible, implantando así un sistema de red y la gestión de su seguridad, al tratarse de un sistema crítico de una empresa en producción.

En adición al objetivo principal, se derivan los siguientes objetivos que debemos de seguir para acabar cumpliendo el objetivo principal:

- La búsqueda exhaustiva de un software que nos permita cumplir con el objetivo, además de minimizar los costos lo máximo posible.
- Montar las interfaces de red y las distintas VLANs que forman la red de la empresa, manteniendo el diseño actual.
- Diseñar el Firewall y su filtrado de paquetes, mediante reglas de filtrado entre las redes internas y externas, simulando el actual sistema, para controlar el acceso a Internet dando permisos y restringiendo las conexiones.
- Implementar un DHCP en el propio software que asigne de forma automática las distintas direcciones IP, dependiendo de la VLAN o la interfaz a la que se conecte el equipo.
- Crear un Certificado de Autoridad, a partir del cual se podrán crear conexiones con seguridad entre distintos clientes.
- Crear distintas VPNs a partir del Certificado de Autoridad anterior, para poder conseguir que los empleados se puedan conectar de forma remota para trabajar.
- Diseñar un “failover”, para que en el caso de que caiga la red principal, exista una redundancia que permita seguir teniendo conexión.
- Dar la posibilidad de implementar otros servicios de red que mejoren el sistema actual, para mantenerlo actualizado y optimizado.

Para acabar consiguiendo la consecución de estos objetivos, se va a generar una documentación que permitirá:

1. Identificar las necesidades y requisitos del cliente.
2. Comprender el escenario de partida y el análisis sobre este para abordar el problema.
3. Estudiar las alternativas disponibles en el mercado para conseguir una solución.
4. Conocer las razones y los motivos de la solución elegida, entre todas las propuestas.
5. Comprender el diseño de la red de Korott SL.
6. Entender la importancia de la planificación, la instalación y la puesta en marcha de los servicios para asegurar el éxito del proyecto.
7. Analizar e identificar los servicios necesarios que se van a requerir a lo largo del proyecto.
8. Realizar una fase de pruebas que puedan reflejar el correcto funcionamiento de los servicios y herramientas instaladas.
9. Disponer de una documentación completa que permita formar a los empleados para actualizar el sistema y mantenerlo optimizado.

Asimismo, se buscará que este proyecto sea eficaz y eficiente, llevándose a cabo con los recursos disponibles y manteniendo al mínimo el presupuesto utilizado.

1.2. Metodología

La metodología se refiere al conjunto de acciones realizadas para alcanzar el objetivo final, en este caso la implantación de un sistema de red y su gestión de la seguridad, el cual requiere de unos conocimientos previos específicos que nos permitan llevarlo a cabo.

A partir de aquí, se ha elegido por utilizar una metodología ágil, entre las distintas metodologías existentes. En cuanto a gestión de proyectos se refiere, la metodología ágil consiste en que el proyecto sea más flexible a las demandas del cliente y se pueda adaptar a los cambios que surjan durante su realización. Esto es posible al estar

formada por pequeñas etapas, ya que, cada cambio que requiera se puede adaptar para la siguiente etapa, consiguiendo así cumplir con las expectativas del cliente sin perder la calidad con la que se ha de conseguir terminar el proyecto.
Además, al ser una metodología que se basa en pequeñas etapas, se consigue:

- Formar equipos más efectivos y eficientes, mejorando la calidad del producto final.
- Mayor compromiso del equipo encargado de la tarea, mejorando la satisfacción del empleado.
- Mejorar la productividad, asignando de forma más dinámica los recursos y siguiendo las prioridades del cliente.
- Aumentar la rapidez, minimizando el tiempo de producción y la toma de decisiones.

Finalmente, entre las distintas metodologías básicas que se pueden encontrar, se ha elegido utilizar la metodología ágil conocida como “Scrum”, la cual se explica a continuación.

1.2.1. Metodología ágil Scrum

Agregando a lo mencionado anteriormente, en una metodología ágil se trabaja por etapas donde se realizan entregas del proyecto. En este caso, a esas etapas se las conoce como “sprints”, en las que el proyecto va evolucionando desde su versión inicial hasta alcanzar el resultado final.

De la misma manera, esta metodología ágil conocida como Scrum se basa en que todas las tomas de decisiones se llevan a cabo a partir de la información que se conoce y en función de la experiencia de los miembros que realizan el proyecto. Todo esto, provoca un mayor aprendizaje y una mejor organización de los equipos que permite reajustar el proyecto a las exigencias demandadas por parte del cliente.

Además, con la ayuda de diversas herramientas y recursos, como por ejemplo *Microsoft Project*, se puede optimizar la planificación del proyecto, para observar mejor los plazos de entra y el tiempo disponible para cada uno de los “sprints” que se deben llevar a cabo.

Finalmente, para poder ejecutar una planificación óptima, se va a realizar un diagrama de Gantt, cuyo objetivo es mostrar el tiempo empleado en cada una de las distintas tareas a lo largo del tiempo que dure el proyecto, entregando cada “sprint” dentro de los plazos de entrega marcados.

2. ANTEPROYECTO

Antes de comenzar con el desarrollo de los contenidos del proyecto, se va a conocer en qué situación se encuentra la empresa que ha encargado dicho proyecto, teniendo en cuenta los antecedentes de esta y, observando así, como cogen forma los objetivos mencionados con anterioridad.

2.1. Escenario

2.1.1. Situación de la empresa Korott SL

En primer lugar, se conoce que el cliente, la empresa Korott SL, son especialistas en la elaboración de productos para terceros, ofreciendo a sus clientes un servicio completo desde la elección de las materias primas hasta la producción y la logística de los productos finales. Más específicamente, se trata de una empresa farmacéutica que elabora productos dirigidos a la salud y el bienestar de las personas.

Asimismo, desde mediados del 2021, la empresa pasó a formar parte del Grupo EVP, junto a otras empresas que lideran el mercado alemán y el de Reino Unido, ampliando sus mercados a nivel nacional e internacional. Sin embargo, este cambio de propietario también ha traído una serie de cambios continuos en la empresa, para potenciar tanto su marca, como para optimizar los recursos disponibles.

Actualmente, en Korott SL, además de sus oficinas, donde se llevará a cabo el presente proyecto, se encuentran disponibles distintas naves y laboratorios que posibilitan todo su proceso de fabricación de productos farmacéuticos de marca blanca. Todas estas distintas ubicaciones, se encuentran conectadas al mismo sistema de red y este al CPD (Centro de Procesamiento de Datos), para poder almacenar todos los datos que se

tratan en la empresa, y así, tener un registro y una copia de seguridad de todos los procesos que llevan a cabo.

2.1.2. Sistema de gestión de seguridad en la red

Haciendo más hincapié en su sistema de red, se observa que disponen de una red principal, una de backup y una tercera que se utiliza simplemente para realizar pruebas en algunos proyectos. A su vez, se dispone de distintas VLANs como se verá más adelante, para diferenciar entre servidores, PCs, impresoras, pistolas, pantallas de producción… No obstante, nos vamos a centrar en el Firewall Barracuda F400 que se encuentra en el CPD, ya que, es el encargado de la gestión de la seguridad de la red, que tiene como función principal llevar a cabo los siguientes servicios:

- Gestión de reglas que permiten/deniegan el tráfico entre distintas redes, subredes, servicios, IPs, etc.
- Gestión de las distintas VLANs para posteriormente poder manejar el tráfico entre ellas.
- DHCP. Servidor de entrega de direcciones IPs a los distintos equipos ubicados en las distintas VLANs. Cada VLAN dispone de un rango de direcciones IPs asignables distinto.
- VPN. Permite a los usuarios conectarse a sus instalaciones desde posiciones remotas.
- Failover entre la red principal y la de backup para manejar las caídas de conexión o los errores, al tratarse de un sistema crítico.

Todo esto, sumado a los objetivos del proyecto mencionados con anterioridad, se necesitará implementar un sistema de gestión de la seguridad de la red “paralelo” al que ya existe, para duplicar todos estos servicios y que se pueda utilizar, manteniendo todos los servicios ejecutados en funcionamiento, en caso de que el Firewall principal sufra una caída.

Para ello, se va a realizar un análisis exhaustivo para encontrar la solución óptima para el proyecto, y se implementará un equipo con dicha solución. Por lo tanto, se realizarán tantas pruebas como sean necesarias, utilizando la red de backup y la red de pruebas, y finalmente, cuando esté todo el software operativo, se realizará una prueba final en el cual se sustituirá esta solución por el sistema actual para evaluar el impacto en los servicios desplegados y en funcionamiento actualmente. Todo esto, se verá a continuación en el desarrollo de los contenidos.

2.2. Alcance

A partir de aquí, se va a definir la declaración de alcance teniendo en cuenta el escenario de la empresa, la metodología Scrum y los objetivos mencionados con anterioridad. Para ello, se van a marcar una serie de tareas y entregables claves para realizar la entrega del proyecto con éxito.

En primer lugar, se deben de tener en cuenta la necesidad de la empresa para llevar a cabo este proyecto, ya que, de acuerdo con los objetivos mencionados, el sistema de gestión de la seguridad de la red es un sistema crítico y es por ello por lo que debe de existir un sistema de respaldo. Por ello, la empresa encarga un proyecto proponiendo que se utilice el mínimo presupuesto posible, consiguiendo como resultado una réplica simplificada del sistema actual.

En segundo lugar, se incluye una duración del proyecto de dos meses, en los que el responsable debe entregar la solución que será la alternativa al sistema actual. Para ello, el responsable debe planificar la entrega de distintas tareas (separando las entregas por puntos como: configuración de reglas, configuración de la VPN…) cada semana, cumpliendo así los objetivos de los “sprints”, como indica la metodología.

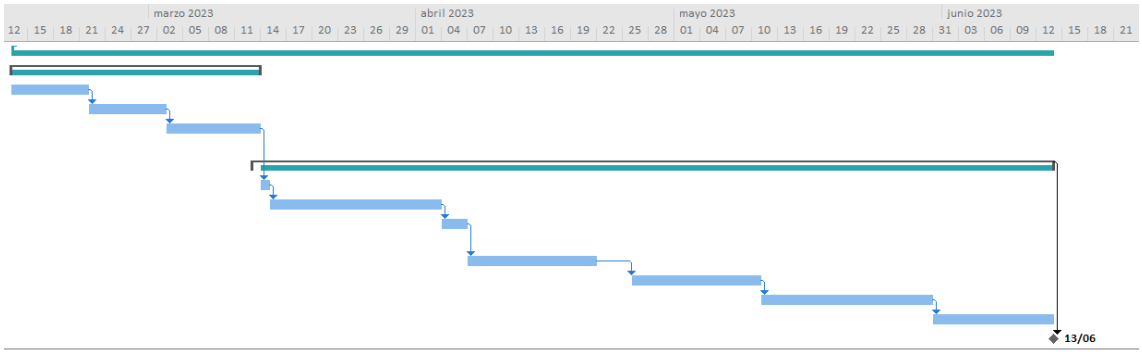


Ilustración 1. Planificación del proyecto.

Una vez realizada esta planificación, se empezará a realizar el proyecto siguiendo los requerimientos del cliente, el cual podrá añadir cualquier cambio o arreglo que observe necesario, tras la entrega de cada “sprint”.

Asimismo, por un lado, se excluirán de la solución propuesta servicios como: controlador del dominio, antivirus… Ya que, la empresa cuenta con unos servicios alternativos y no están incluidos dentro del Firewall principal que se va a replicar. Por otro lado, encontramos limitaciones dentro de la propuesta del propio proyecto, debido a que, al tener un presupuesto fijo y unos recursos limitados disponibles, se podría dar el caso en el que se deba aumentar levemente el presupuesto para poder cumplir con todos los objetivos, aunque en el caso de este supuesto, se comunicará con antelación para realizar un plan de prevención.

Por lo que, finalmente, la estimación de costes se expondrá en el siguiente punto mencionando el presupuesto del que se dispone, y cómo se va a invertir para cumplir con los requerimientos del cliente sin superar el presupuesto inicial. Sin tener que llegar a realizar un plan de prevención.

2.3. Presupuesto

Teniendo claro el alcance del que se dispone dado las tareas, los plazos de entrega, la planificación, las limitaciones, las exclusiones… Se va a analizar los objetivos propuestos por Korott SL y cuál es la mejor forma de llevarlos a cabo con un presupuesto bajo, ya que, el presupuesto es un factor clave para el éxito del proyecto.

2.3.1. Miembros del equipo

Para empezar, por un lado, los recursos humanos son mínimos, al tener en dicho proyecto como responsable a un alumno en prácticas, aunque lo supervisa el jefe del departamento de sistemas de la empresa.

Por lo tanto, en este caso, el capital necesario será de 4,3€ por hora trabajada, como estipula la normativa de la universidad, la UPV, en la cual estudia dicho alumno. Es decir, un salario de 1376€ durante los dos meses que va a estar el proyecto en marcha, desde su inicio hasta la entrega final.

2.3.2. Capacitación e investigación

Además, sabiendo de antemano que el encargado de realizar el proyecto será un alumno en prácticas, este necesitará tiempo y recursos para ponerse al día, y conocer a fondo el sistema que necesita replicar.

Para ello, se analizará el sistema de gestión de seguridad de la empresa, junto al responsable del departamento y teniendo los datos almacenados en las copias de

seguridad, para saber cómo funciona dicho sistema. Por lo que, no supone un aumento del presupuesto, al estar incluido en el salario del estudiante.

2.3.3. Equipamiento

Por otro lado, los recursos que se encuentran disponibles en el departamento son muy útiles, ya que, se encuentran muchos dispositivos sin uso actualmente. Por eso, se utilizarán dos PCs, como clientes para realizar pruebas de acceso y comunicación entre ellos, y otro PC, para replicar el sistema crítico vía una solución "OpenSource", a través de un software conocido como "Zentyal", que nos permite la aplicación de todos los servicios con los que cumple el Firewall actual.

Asimismo, se utilizarán unas copias del controlador de dominio y del sistema "SISLOG", encargado de gestionar todos los almacenes, en otros dos PCs, para poder realizar cuantas pruebas sean necesarias sin causar daños en los sistemas principales.

En resumen, se implantará la solución con los recursos ya disponibles que ofrece la empresa y una solución software sin coste alguno, por lo que en este aspecto no será necesario aumentar el presupuesto.

2.3.4. Espacio de trabajo

En cuanto al espacio de trabajo, todo el proyecto se va a llevar a cabo en el Departamento de Sistemas, ubicado en la planta baja dentro de las Oficinas de Korott SL, donde se dispondrá de todos los recursos mencionados anteriormente. Por lo que, en este caso, tampoco será necesario aumentar el presupuesto del proyecto.

2.3.5. Fondo para contingencias

Asimismo, se tendrá en cuenta un margen en el presupuesto de 150€, en el caso de que sea necesario conseguir un nuevo dispositivo o cambiar piezas de alguno de los utilizados, ya que, los que se van a utilizar pueden tener un pequeño deterioro al no estar en constante funcionamiento.

2.3.6. Costes totales

Finalmente, teniendo en cuenta todos los puntos mencionados anteriormente, el presupuesto final para dar comienzo el proyecto es de 1526€, el cual vamos a desglosar en una tabla para conocer más detalladamente en que se van a utilizar.

Al final de la memoria, se realizará una comparación para verificar que el presupuesto calculado en el anteproyecto concuerde con el presupuesto final tras la entrega del proyecto.

2.4. Estado del arte

Para empezar, una vez identificado el problema que tiene la empresa al no poder actualizar sus sistemas, sin tener un sistema secundario que gestione la seguridad de la red, y el aumento de implementaciones de estos tipos de sistemas de gestión de la seguridad de la red en todo el mundo, provocan que se vaya a indagar más sobre esta problemática.

Es muy importante actualmente, dado que cada vez se utilizan más dispositivos con acceso a la red. Esto implica, que hay que tener más en cuenta la seguridad con el paso

de los años, ya que, cualquiera tiene acceso a la red, y se deben de proteger los datos de cada uno y toda la información que puede ser crítica para cada persona.

Viendo estos problemas, en Korott SL, se observó que el sistema que gestiona actualmente la red de la empresa, el Firewall Barracuda F400, se encontraba desactualizado. Esto implica, que se pueda seguir trabajando con normalidad dentro de la empresa, pero es mucho más vulnerable por factores externos.

Por lo tanto, al tratarse de un sistema crítico de la empresa, se decidió por implantar un sistema secundario que pueda suplir este Firewall en caso de emergencia mientras se realiza una actualización, para aplicar parches o corregir posibles errores que se evitan en las siguientes actualizaciones del software utilizado.

A continuación, al tener que desarrollar un proyecto alrededor de dicho sistema de gestión, se van a estudiar distintos casos con anterioridad al nuestro, analizando los resultados obtenidos para compararlos con nuestro objetivo y ver si cumplen las expectativas propuestas.

2.4.1. Investigación de proyectos antecedentes

Se han encontrado dos investigaciones que servirán como referencia a la hora de replicar el sistema del Firewall de la empresa.

Ambas investigaciones se han llevado a cabo en el año 2016, utilizando un software libre, el cual nos va a interesar conocer, ya que, nuestro presupuesto está muy ajustado y si se conoce una herramienta “OpenSource” de antemano, va a permitir desarrollar el proyecto de una forma óptima.

En primer lugar, se encuentra la investigación que lleva por título "*Alternativa de software libre como solución única de los servicios de gestión de red entre barco y sede*" (Jiménez, 2016), escrita por Alberto Hernández Jiménez.

Esta investigación viene impulsada por la necesidad de actualizar los sistemas de comunicaciones del *Barco Oceanográfico García del Cid*, para que la comunidad científica desarrolle sus actividades en las condiciones más favorables, incluyendo la adquisición de un sistema de comunicaciones VSAT mediante antena de banda Ku, gracias al concurso público del proyecto de cofinanciación FEDER. Asimismo, tiene como propuesta la búsqueda de una solución que utilice software libre para gestionar los servicios de red y recopilar información de todos los equipos que componen la red, manteniendo las mismas características de las que se dispone en ese momento o superiores, y que su administración sea sencilla.

Tras su debido análisis del sistema, se pasa de un escenario con un enrutador CISCO que solo se puede administrar a través de comandos y que no cubre todas las necesidades del cliente como proporcionar DNS y DHCP, a la implantación de la solución elegida, en este caso Zentyal, que cubría todas las necesidades requeridas por el cliente para gestionar la red, recopilar información y redireccionar las IPs para homogeneizar todas las plataformas que gestiona la UTM-CSIC.

En segundo lugar, se encuentra la investigación que lleva por título "*Análisis e implantación de un sistema integrado de gestión, para la red de datos de la Universidad Estatal de Bolívar matriz, en software libre*" (Gaibor, 2016), escrita por Jairo Lizandro Ramos Gaibor.

Este trabajo de investigación presenta un estudio comparativo e implementación de un Sistema Integrado de Gestión para la red de datos de la Universidad Estatal de Bolívar matriz en software libre.

Tras realizar un análisis exhaustivo de la configuración de los distintos sistemas integrados de gestión disponibles, se implementa la opción OSSIM por sus beneficios y costos. Esta solución, recolecta la información de los dispositivos conectados a la red de la universidad, configurando además al mismo tiempo servicios web, mail, plataforma virtual… Por otro lado, con la información conseguida a través de la monitorización de los dispositivos, suministra eventos y alarmas reportando la información a los equipos y a sus distintos servicios para facilitar la respuesta en el caso de la aparición de fallos en estos. Es decir, acaba mejorando la toma de decisiones para la UEB a nivel directivo.

2.4.2. Conclusión de proyectos antecedentes

Como ya se ha mencionado anteriormente, se necesita que la solución a implantar dentro de la empresa sea capaz de suplantar el sistema principal, llevando a cabo sus funciones principales.

Por ello, se ha realizado una búsqueda de antecedentes donde se busca un objetivo similar que utilice software libre y defina una serie de servicios implantados que cumplan con las necesidades del cliente. Así que se ha definido una búsqueda donde se ha dado importancia a términos como “OpenSource”, “Firewall”, “Sistema de gestión”, “Seguridad en la red”, etc. Dando como resultado muchos proyectos, entre los que se han elegido los más parecidos a las necesidades de Korott SL.
Tras las investigaciones realizadas, se observa en ambos proyectos que el resultado obtenido es el esperado, ya que, se quería comprobar la eficacia de soluciones de software libre que se puedan instalar en distintas empresas o centros, cumpliendo estas implementaciones con las expectativas que se mantienen en el proyecto. Por ello, es posible ver cómo se consigue realizar la instalación de distintos servicios que facilitan la gestión de la red y su seguridad.

Sin embargo, se deberían de implementar en ambos proyectos unas políticas de seguridad siguiendo las normas ISO, más específicamente la norma ISO 27001, para tener un manual estandarizado que siga una metodología específica, como prevención ante cualquier fallo del propio sistema.

En conclusión, ambos proyectos son de gran utilidad para conocer distintas soluciones libres que se encuentran en el mercado, que pueden cumplir perfectamente con las necesidades y requerimientos de la empresa. Simplemente, se necesitaría implementar las políticas de seguridad siguiendo la norma ISO 27001 como se menciona previamente.

3. DESARROLLO DE LOS CONTENIDOS

A continuación, una vez conocido el anteproyecto realizado tras un análisis de Korott SL, se va a proceder al desarrollo de todos los pasos que se han llevado a cabo para la realización de este proyecto. Para ello, se seguirán las exigencias del cliente definidas en los objetivos.

3.1. Alternativas de soluciones "OpenSource"

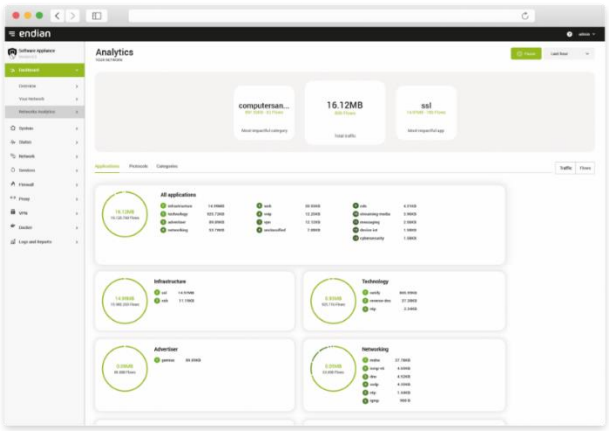
Para empezar, se van a buscar las distintas alternativas que se puedan encontrar en el mercado para replicar nuestro sistema principal. En adición, se buscará una solución "OpenSource", entre todas las opciones posibles, para mantener el presupuesto del proyecto ajustado y no incrementarlo. Por consiguiente, se van a presentar las distintas soluciones del mercado que se han encontrado, que cumplen con los requisitos y que se podrían implementar.

3.1.1. EndianOS

Endian (Endian, 2023) proporciona una plataforma de ciberseguridad que conecta personas y dispositivos. Su objetivo es desarrollar las plataformas de código abierto más potentes y fáciles de usar del mundo. Por lo tanto, esta solución conecta, controla, analiza y administra todos los dispositivos que se encuentren en su red. Como principales características tiene:

- Acceso de desarrollo. Ofrece una API segura que se puede utilizar para crear aplicaciones que interactúen o utilicen datos desde dentro de "Switchboard".

- Gestión de puerta de enlace. Crea puertas de enlace de forma remota para poder establecer conexión.
- Gestión de aplicaciones. Define las aplicaciones que son accesibles por los usuarios.
- Implementación sin contacto. Se incluyen varios métodos de implementación sin contacto, que permiten a los administradores aprovisionar de forma centralizada configuraciones de dispositivos que se aplican automáticamente a los dispositivos.
- Visualización y análisis de datos. Crea tablas personalizadas para visualizar datos, de forma que permite lograr un mantenimiento predictivo.
- Gestión de usuarios. Crea y administra usuarios para asignarlos a distintos grupos creando accesos según los roles de los usuarios.
- Gestión de terminales. Proporciona un fácil acceso a sus dispositivos finales a través de su propia dirección IP virtual.
- Acceso móvil. Compatibilidad con prácticamente todas las plataformas (PCs, tabletas y dispositivos móviles).
- Recopilación de datos. Recopila datos de los dispositivos utilizando el hardware Endian 4i. Se puede agregar los protocolos propios utilizando el sencillo SDK de recopilador.



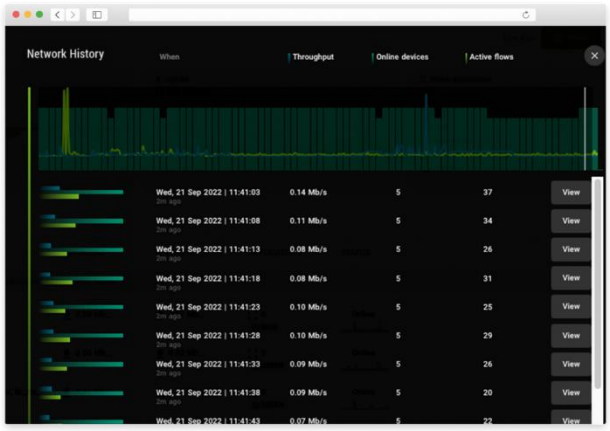


Ilustración 2. Gráficas de análisis en EndianOS.

3.1.2. OPNsense

OPNsense (OPNsense, 2023) es un software de código libre basado en FreeBSD, que se utiliza como herramienta de enrutamiento y firewall. Incluye la mayoría de herramientas disponibles en otros softwares de pago, como el Dashboard, una interfaz de usuario moderna, conocer el estado del firewall, un controlador del tráfico, analizador de flujo de red integrado, autenticación de dos factores, VPN, alta disponibilidad o conmutación por error de hardware, proxy de almacenamiento en caché, detección y prevención de intrusos, copias de seguridad, informes… Además de muchas otras funcionalidades, que cumplen con los requisitos del cliente.

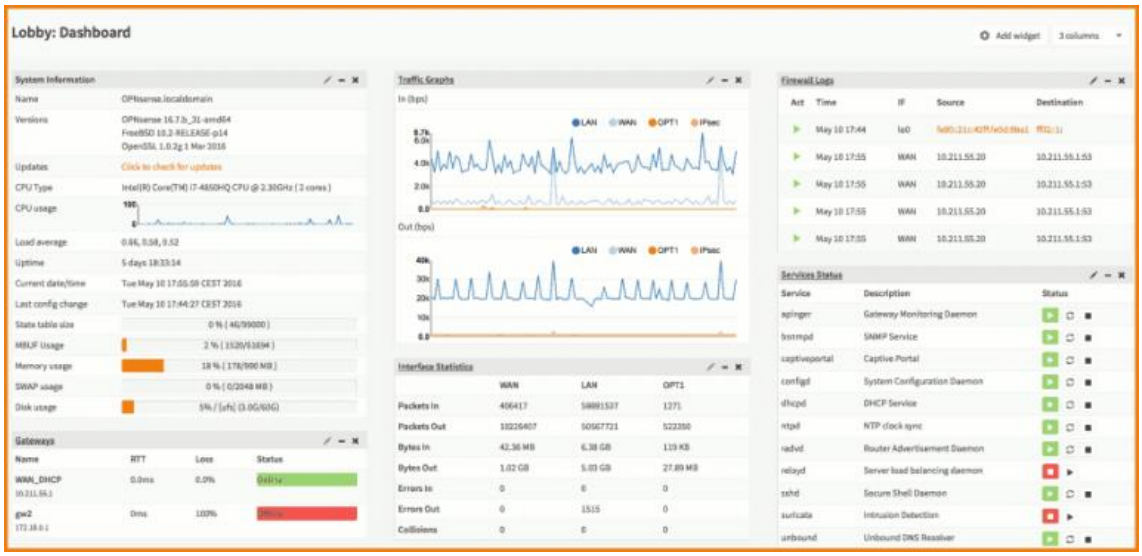


Ilustración 3. Dashboard OPNsense.

3.1.3. ClearOS

ClearOS (ClearOS, 2023) es una distribución GNU/Linux basada en CentOS y Red Hat que implementa un sistema de gestión de red. De las distintas versiones, hay

una versión “Community” que se instala en su propio hardware con licencia GPL GNU, que contiene las siguientes características:

- Interfaz simple. Proporciona una amplia variedad de funciones de TI para la nube, la puerta de enlace, la red, el servidor y más; todo integrado en una plataforma.
- Configuración web limpia y sencilla. Ofrece una interfaz basada en navegador simple. Deje atrás el mundo negro de las interfaces de línea de comandos.
- Características robustas de VPN. Utiliza IPsec VPN para administrar direcciones IP dinámicas, proporciona acceso remoto seguro mediante OpenVPN y se puede configurar también una conexión PPTP.
- Mercado de ClearOS. Está equipado con ClearOS Marketplace que incluye más de 75 funciones TI integradas que se presentan como aplicaciones, que le permite escalar la funcionalidad del servidor.
- Seguridad de nivel empresarial. Ofrece antivirus, antiphising, detección de intrusos, análisis inteligente basado en el contenido de la web, filtro de protocolo L7 analizando paquetes y control de acceso aplicando restricciones a usuarios y grupos.
- Recuperación de datos. Da soluciones escalables de almacenamiento remoto, de 5GB a 500TB de respaldo de datos. También permite guardar una copia de seguridad de la configuración que permita replicar el sistema.

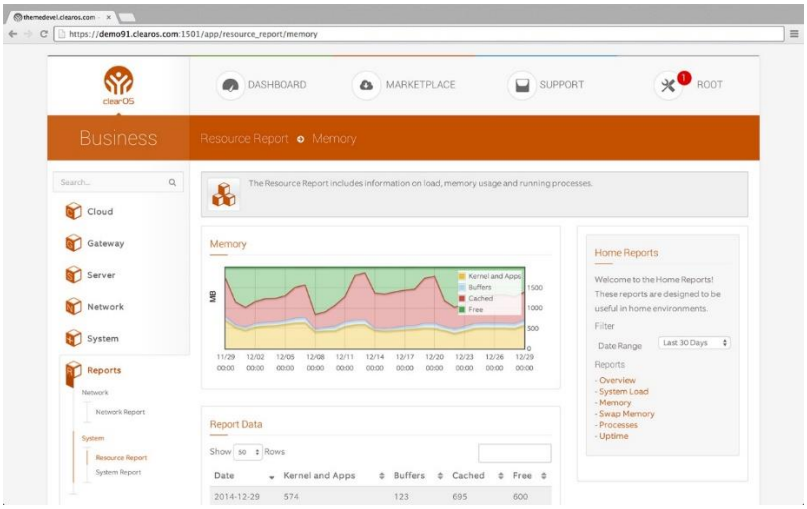


Ilustración 4. Vista principal ClearOS.

3.1.4. NethServer

NethServer (NethServer, 2023) es un sistema operativo para amantes de Linux, diseñado para ser implantado en PYMES. Este SO se define por las siguientes características:

- Se puede modular al gusto del cliente y contiene diversas funciones como MailServer, WebServer, Firewall, VPN, etc.
- Simplifica las tareas de administración a través de una potente interfaz y una fácil configuración.
- Está basado en CentOS/RHEL, una distribución de servidor generalizada y popular, en la que confían las actualizaciones de seguridad de rutina y una estabilidad sólida.
- Software 100% de código abierto, impulsado por colaboradores e impulsado por la comunidad. Mantiene canales de comunicación abiertos y bien documentados.
- Es escalable y personalizable, además de tener una extensibilidad incorporada y una gran cantidad de módulos.
- NethServer en cuanto a su seguridad: cumple con las normas de cumplimiento, protege su infraestructura informática y proporciona un entorno seguro.
- Gracias al uso eficiente de los recursos, es rápido en hardware moderno y responde en máquinas menos potentes.

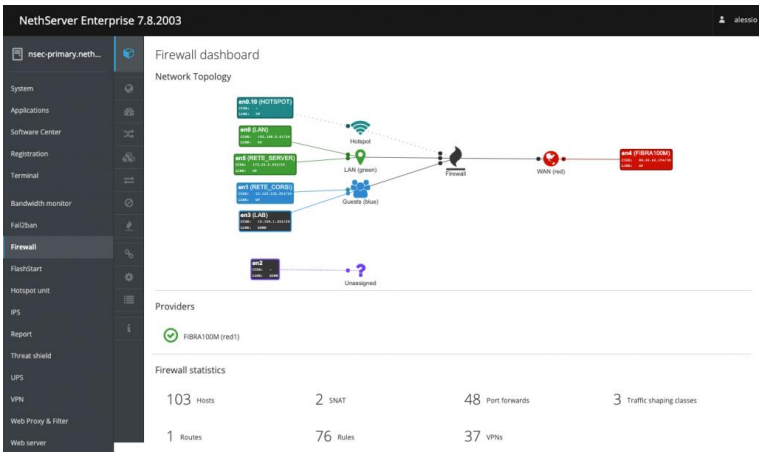


Ilustración 5. Dashboard del Firewall de NethServer.

3.1.5. Artica

Artica (Artica, 2023) se basa en Debian10 y SQUID4x, y proporciona una poderosa interfaz web que permite a cualquier persona instalar y administrar servicios Linux, como Firewall, SMTP, VPN, DNS, DHCP… Además de incluir las siguientes características:

- Filtro URL. La base de datos se adapta a la implementación de reglas de acceso para controlar las actividades de los usuarios y dispositivos.
- FTP con antivirus. El antivirus se integra en el Proxy a través del protocolo ICAP para obtener el mejor rendimiento para la verificación de contenidos.
- Motor de estadísticas. Permite mostrar distintos gráficos para saber cuándo, dónde y cómo usan el ancho de banda los usuarios.
- Arquitectura y disponibilidad. Puede usarse como Proxy estándar o transparente, evita el tiempo de inactividad y aumenta la productividad manteniendo un acceso constante a Internet, y proporciona servicios de distribución y balanceo en tiempo real para crear un clúster de proxy HTTP.
- Otras muchas características mencionadas anteriormente como Firewall, DNS, VPN, DHCP…

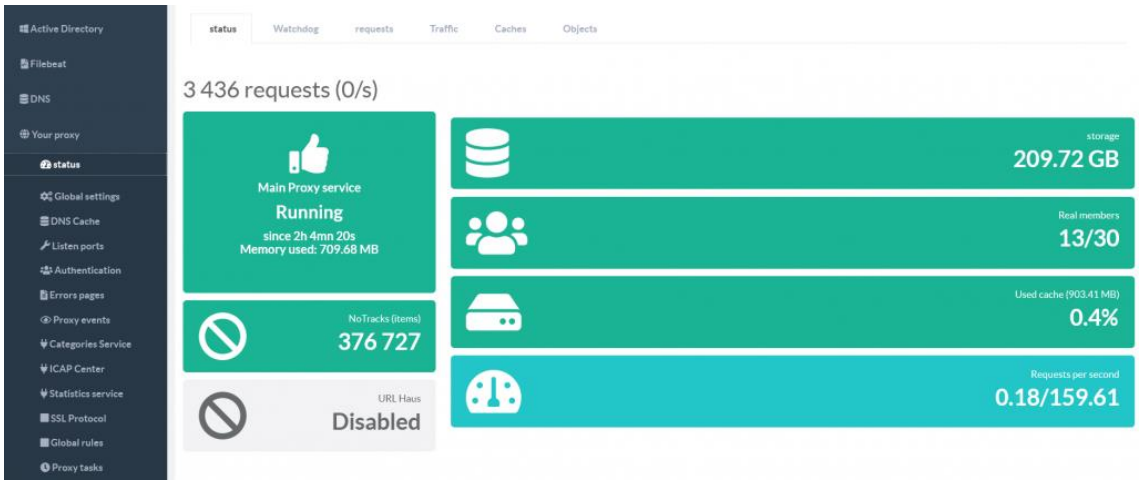


Ilustración 6. Status Artica.

3.1.6. Zentyal

Zentyal (Zentyal, 2023) está dirigido a empresas con experiencia y herramientas internas para instalar, configurar y mantener el despliegue, por sí mismas, de los distintos módulos que proporciona este software. Asimismo, implementa protocolos Microsoft Exchange sobre componentes estándares de código abierto para asegurar su compatibilidad con clientes Microsoft Outlook. Algunos de los módulos o características que se pueden implementar son:

- Directorio y dominio. Administración central de los dominios y directorios, usuarios y grupos, autenticación de inicio de sesión, compatible con SO Windows XP/Vista/7/8/10, uso compartido de archivos, permiso de acceso a usuarios y grupos…
- Correo. Soporta protocolos como SMTP, POP3, IMAP, etc. Proporciona correo web, sincroniza con dispositivos móviles a través de ActiveSync, posee múltiples dominios de correo virtual, antivirus y filtro de correo…
- Red. Permite modificar todo lo relacionado con la configuración de la red y el enrutamiento como la puerta de enlace, servicio de autenticación de red, Proxy HTTP, IDS/IPS y contiene software integrado como Netfilter o IProute2.
- Firewall. Filtra los paquetes, permite o deniega accesos, redirecciona los puertos disponibles y puede utilizar traducciones SNAT de las direcciones de red de origen.
- Infraestructura. Proporciona servidores DHCP, DNS, NTP y FTP. Permite crear certificados de autoridad, administrar el servicio vía web, creación de redes VPN…
- Mantenimiento. Permite mantener todos los módulos dando alertas en tiempo real y reportes diarios.
- Soporte y actualizaciones. Se dan actualizaciones de software y seguridad de forma constante. Además, la comunidad y los miembros del equipo de desarrollo dan asesoramiento y soporte.

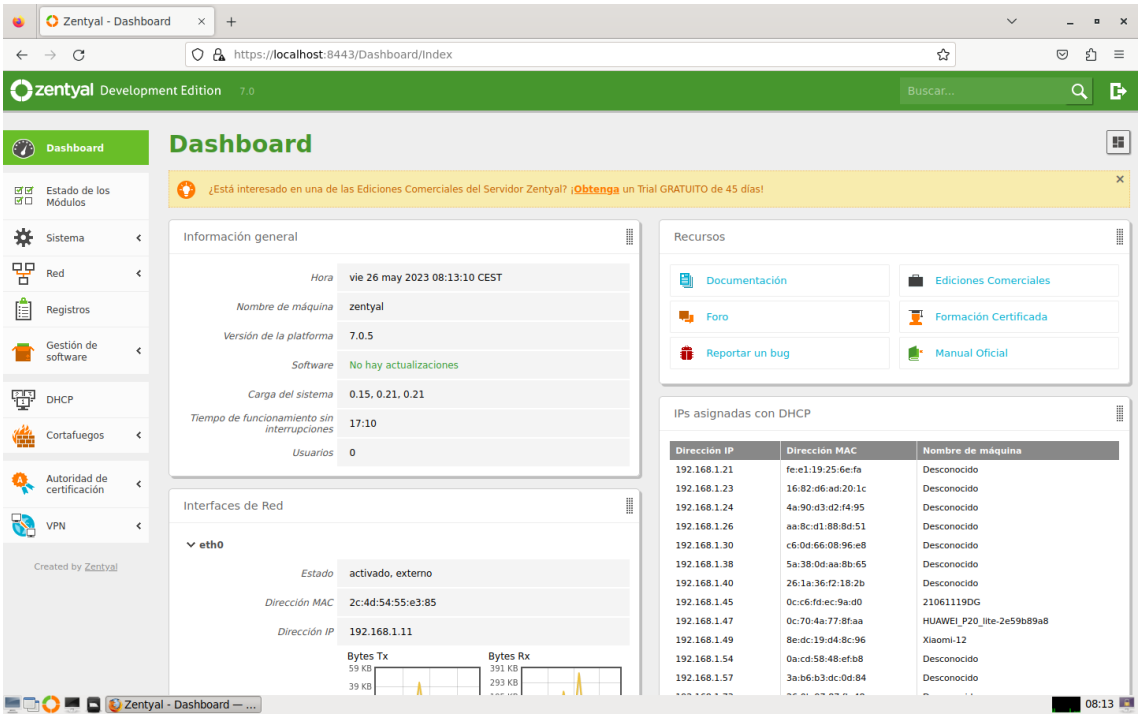


Ilustración 7. Dashboard de Zentyal.

3.2. Análisis y selección de alternativas

Tras conocer las distintas alternativas de código abierto disponibles en el mercado, se observa que muchas de ellas pueden implementar los requerimientos que pide el cliente para el proyecto, pero en especial nos vamos a centrar en la solución “OpenSource” de Zentyal.

Por un lado, se ha elegido esta solución, ya que, con los módulos y herramientas que se pueden instalar se pueden llevar a cabo las exigencias del cliente, cumpliendo así con los objetivos planteados desde un principio. Es decir, se va a poder configurar la red y el enrutamiento de esta, se va a modificar la infraestructura al gusto del cliente creando VPN, servidores DHCP, DNS… Y lo más importante, se van a poder configurar las reglas

del firewall para poder gestionar la seguridad de la red, configurada previamente. Además, es compatible con Microsoft Outlook, que se utiliza en la empresa cliente, al implementar protocolos Microsoft Exchange sobre componentes estándares de código abierto que hacen posible esta compatibilidad, y facilitará la gestión de la seguridad de la red.

Por otro lado, dentro de la propia empresa ya se ha utilizado en alguna ocasión dicha solución de código libre, por lo que se conoce cómo funciona y existe un manual para la correcta utilización de este software. Esto aumenta el valor de esta solución, dado que el conocimiento que tenemos de su funcionamiento es mayor que el de resto de soluciones.

Asimismo, ofrece muchos otros servicios que se pueden implementar en un futuro, si se necesitan mejoras en este sistema de "réplica", además de un mantenimiento constante al ofrecer reportes diarios, actualizaciones de software y de seguridad, y asesoramiento y soporte en el momento que se necesite.

Por lo tanto, la solución elegida finalmente entre todas las disponibles del mercado será Zentyal.

3.3. Diseño de la solución a implementar

A continuación, se va a diseñar la solución que se va a implementar para cumplir con las demandas del cliente, de forma eficiente y eficaz, para aprovechar los recursos de los que ya disponemos y evitar aumentar el presupuesto final y que así se ajuste al presupuesto inicial.

En primer lugar, se cuenta con un manual con los datos necesarios para poder implementar todos los servicios necesarios como el firewall, el servidor DHCP, el

servidor DNS, la configuración de las VPNs… A partir de este manual, se configurarán todos los servicios en la solución “OpenSource” escogida previamente.

Por ello, se va a instalar la solución Zentyal de código abierto en un PC, desde el que vamos a tener el acceso de administración para el resto de los módulos que se instalarán.

A partir de ese punto, se seguirá el siguiente esquema como diseño de implementación de la instalación que se va a llevar a cabo.

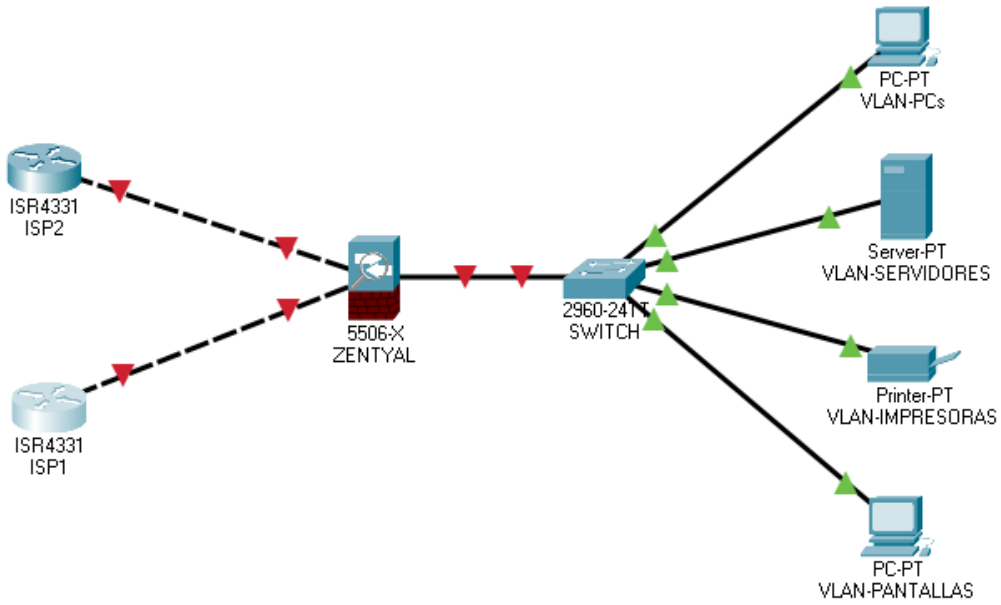


Ilustración 8. Diseño de la solución a implantar sin representar todas las VLANs.

Como se observa en la imagen anterior, el firewall será el servicio principal para ‘replicar’ el sistema actual de la empresa. A partir de este, se filtrarán los paquetes y se permitirá o se denegará la comunicación por parte de los distintos dispositivos conectados a las distintas VLANs existentes. A este servicio, se sumarán el servidor DHCP y DNS, que permitirán tener una IP dentro del rango de la VLAN a los distintos dispositivos y conexión a Internet. Por último, el firewall se encuentra conectado a la red secundaria

para realizar pruebas, y en el caso de que esta red fallase, a través de un “failover” el firewall se conectará a una tercera red que se utiliza específicamente para caídas de red dentro de la empresa.

Con todo esto detallado, se va a realizar la implantación de la solución final, y se van a realizar las distintas pruebas para observar su funcionamiento.

3.4. Implantación de la solución final

Para empezar con la implantación de la solución final, se llevará a cabo la instalación de Zentyal (Documentación Zentyal, 2023) en el PC que se utilizará para administrarlo.

En primer lugar, se descargará el software mencionado anteriormente, y se ubicará el archivo .iso descargado en un USB para realizar dicha instalación, en la que se utilizará la documentación oficial del equipo de desarrollo de Zentyal, en la cual encontramos detalladamente todos los pasos que se han de seguir para realizar una buena instalación de este software.

En segundo lugar, una vez realizada la instalación, se necesita introducir toda la información sobre la configuración de red, indicando si las interfaces de red son externas, para conectarse a Internet, o internas, para conectarse a la red local. Más tarde, se podrán establecer diversos parámetros de configuración, que veremos más adelante en el módulo de red.

Tras configurar toda la red, se va a empezar con la instalación de los módulos que se necesitarán más adelante para cumplir con los requerimientos de Korott SL. Asimismo, dependiendo de los módulos escogidos, es posible que pida más datos a rellenar de estos módulos tras configurar las interfaces de red.

Una vez finalice el proceso de instalación de los módulos instalados, el instalador avisará y ya se podrá acceder al Dashboard y a la configuración específica de cada uno de los módulos instalados.

Para acceder al Dashboard, será necesario acceder a su interfaz web a través del propio entorno gráfico de la máquina donde se encuentre instalado el Zentyal. Para poder acceder a su interfaz web se debe acceder a “https://localhost:8443”, o a través de la dirección “https://direccionIP:8443” desde cualquier máquina conectada a una red interna, siendo ‘direccionIP’ la IP de dicha máquina. Al acceder a la interfaz, en la primera pantalla se solicitan el nombre de usuario y la contraseña que se han establecido durante la instalación.

Ilustración 9. Credenciales de acceso a Zentyal.

Una vez conseguido el acceso, aparece la interfaz de administración, donde se observa cómo se divide la pantalla en tres partes principales: el contenido principal, un menú lateral y otro menú superior.

El contenido principal es aquel que ocupa la gran parte de la pantalla, en este caso el Dashboard y las distintas tablas con la información resumida que proporcionan de todos los módulos. En cuanto a los menús, el menú lateral izquierdo sirve para observar y poder acceder a todos los módulos instalados, mientras que el menú superior se utiliza para realizar búsquedas, guardar los cambios realizados o cerrar la sesión.

A continuación, se van a conocer las distintas herramientas implementadas para cumplir con los objetivos propuestos por el cliente.

3.4.1. Dashboard

El Dashboard es la pantalla inicial de la interfaz, donde se muestran una serie de herramientas que resumen la información del resto de módulos instalados. Estas herramientas se pueden reordenar, eliminar o crear nuevas.

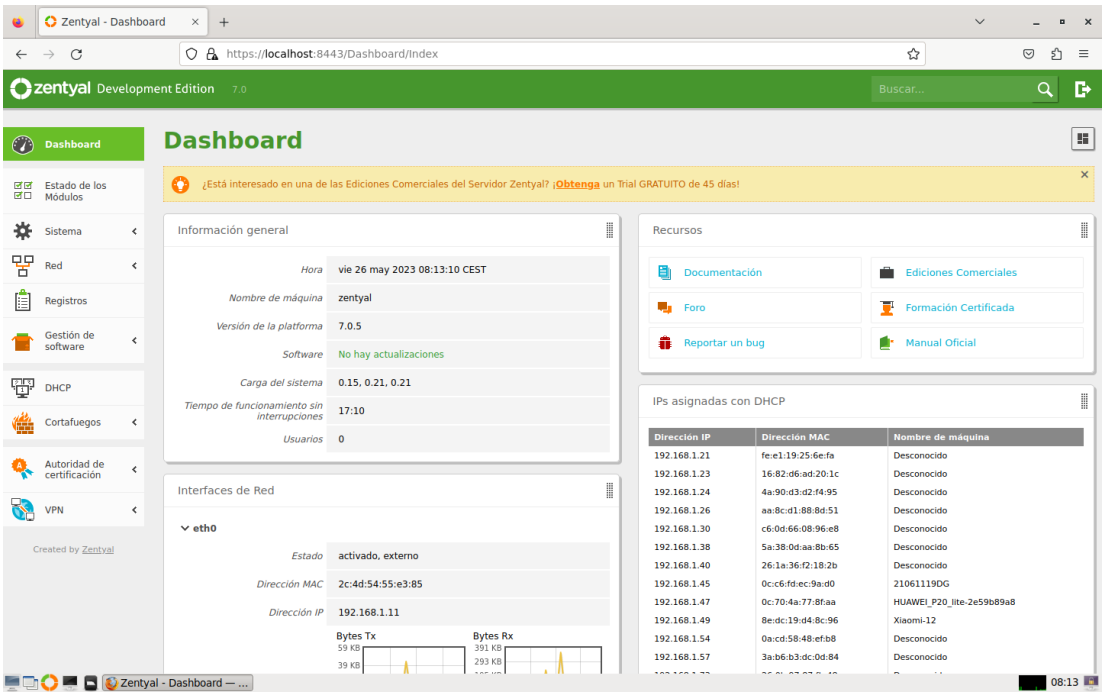


Ilustración 10. Dashboard con el resumen de los módulos configurados.

En primer lugar, para reordenarlas se pulsa en los títulos y se arrastra al lugar que se desee. Luego, para añadir una nueva, se busca en el menú superior y se arrastra al contenido principal junto al resto de herramientas. Y, por último, para eliminarlas, se usa la cruz situada en la esquina superior derecha de cada una de las herramientas.

3.4.2. Estado de los módulos

La siguiente opción en el menú de la izquierda es el estado de los módulos, que se encarga de habilitar o deshabilitar los distintos módulos para que estos puedan ser configurados. Estos módulos, pueden depender de otros servicios para su funcionamiento. En la siguiente imagen se muestra como dichas dependencias aparecen en la columna 'Depende' y si no son habilitadas, no se podrá habilitar el módulo deseado.

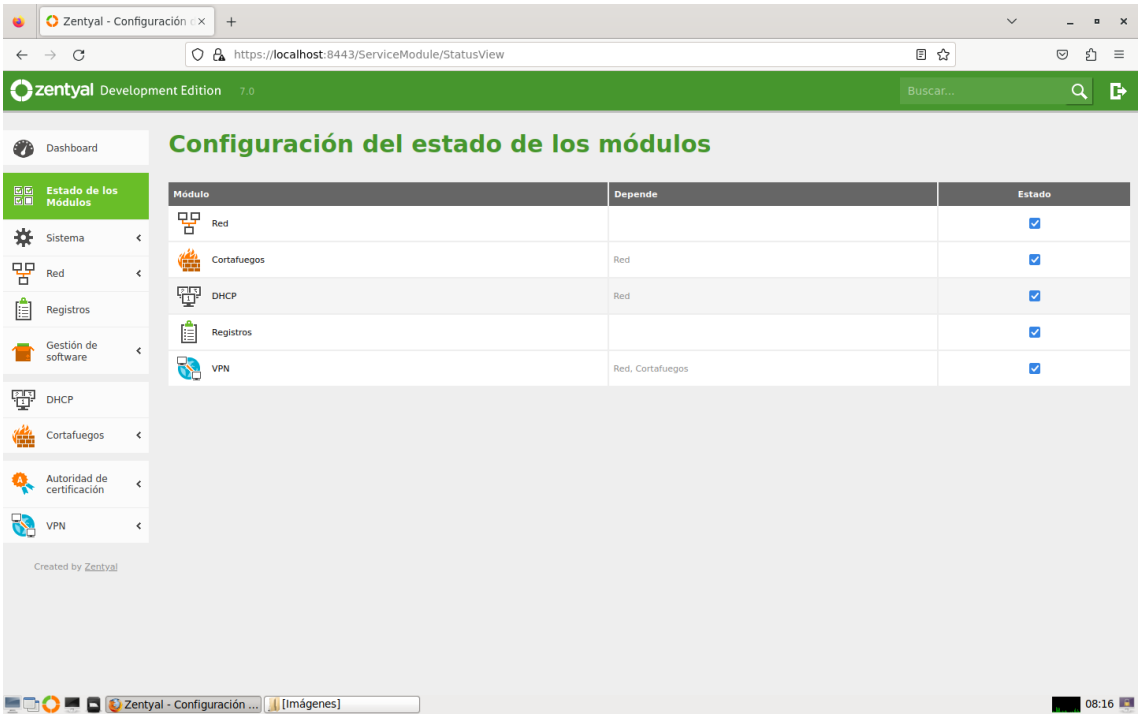


Ilustración 11. Configuración de los estados de los módulos.

Asimismo, de todos los “Widgets” que se muestran en el Dashboard, hay uno que destaca por encima del resto. Esta herramienta muestra el resumen del estado de los módulos instalados previamente. Puede encontrarse con los siguientes estados:

- Ejecutándose. Se ejecuta aceptando conexiones de los clientes. Aparece la opción para reiniciar el servicio.
- Disponible. El módulo está disponible para ser utilizado en cualquier momento.
- Detenido. El servicio de dicho módulo se encuentra sin funcionamiento, ya que, ha sido detenido por el administrador o porque ha surgido algún problema. Se da la opción de volver a arrancar el servicio.
- Deshabilitado. En este caso, muestra que el módulo ha sido deshabilitado explícitamente por el administrador.

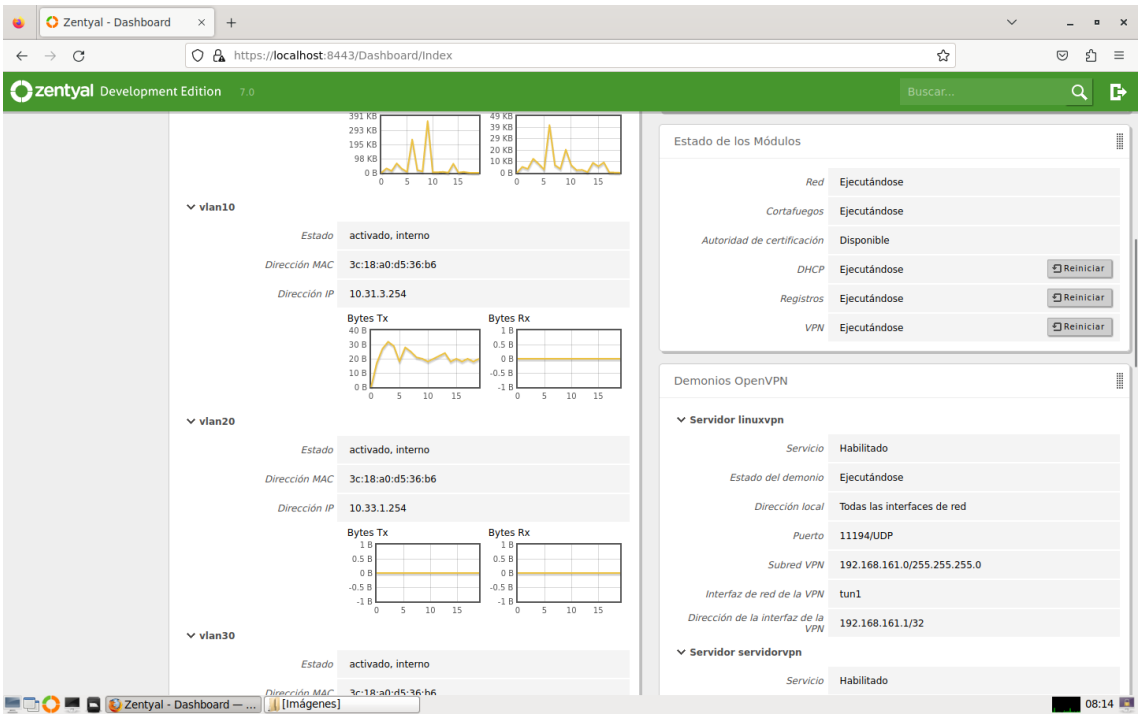


Ilustración 12. Estado de los módulos en el Dashboard.

Cabe añadir que la primera vez que un servicio ha sido habilitado, se pide una confirmación para realizar cambios en el sistema y sobrescribe algunos ficheros de

configuración. Tras aceptar dicha confirmación, se deben de guardar los cambios para que se establezca la nueva configuración.

3.4.3. Sistema

A continuación, si se elige la opción sistema en el menú de la izquierda, se pueden modificar varios parámetros generales de Zentyal.

Como se observa en las imágenes posteriores, los parámetros generales que se pueden modificar son:

- Cuentas de administrador. Se pueden configurar las cuentas que mantengan el poder administrativo de Zentyal. En este caso, simplemente necesitamos la cuenta de administrador para gestionar todo el sistema.
- Idioma. Sirve para seleccionar el idioma de la interfaz que se desee. Por defecto, selecciona el idioma de la ubicación y del teclado detectado en la instalación.
- Puerto TCP de administración. Por defecto este puerto se encuentra en el puerto 8443 utilizando el protocolo TCP mediante HTTPS, pero se puede cambiar por cualquier puerto. Este puerto será el utilizado para administrar Zentyal.
- Nombre de máquina y dominio. Tanto el nombre de la máquina como el dominio se pueden modificar, aunque los actuales hacen referencia a los que se han configurado durante la instalación. Si estos se modifican, se ha de reiniciar la máquina para que todos los servicios se actualicen y utilicen el dominio correcto.

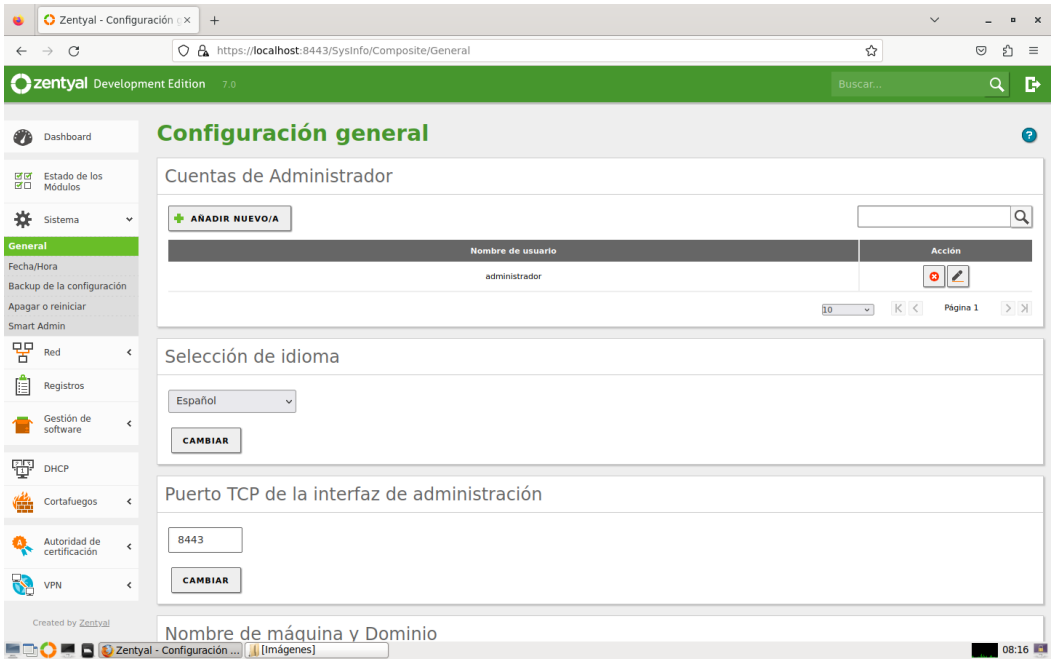


Ilustración 13. Configuración general del servidor.

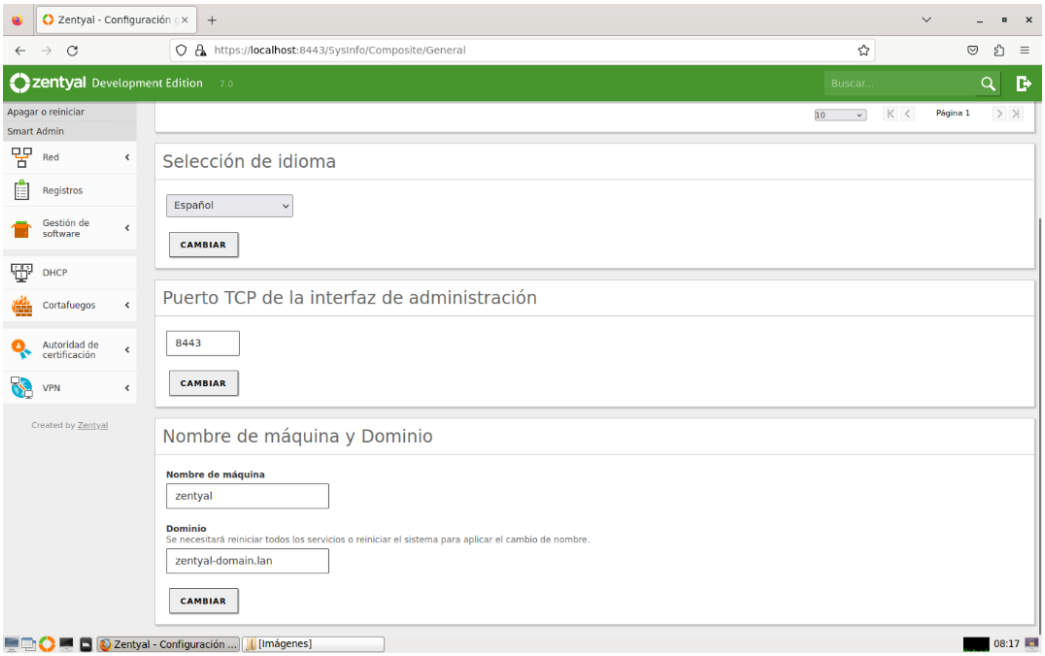


Ilustración 14. Más configuraciones generales del servidor.

Por otro lado, se encuentra el servicio de sincronización de fecha y hora. Este utiliza el servidor NTP, que utiliza el puerto 123 del protocolo UDP. Para ponerlo en funcionamiento es necesario seleccionar correctamente la zona horaria en la que se encuentra la máquina, en este caso Europa/Madrid. Una vez seleccionada la zona horaria, se puede comprobar que el servicio sincroniza automáticamente la hora y que se deshabilita la opción de modificar la fecha y la hora manualmente.

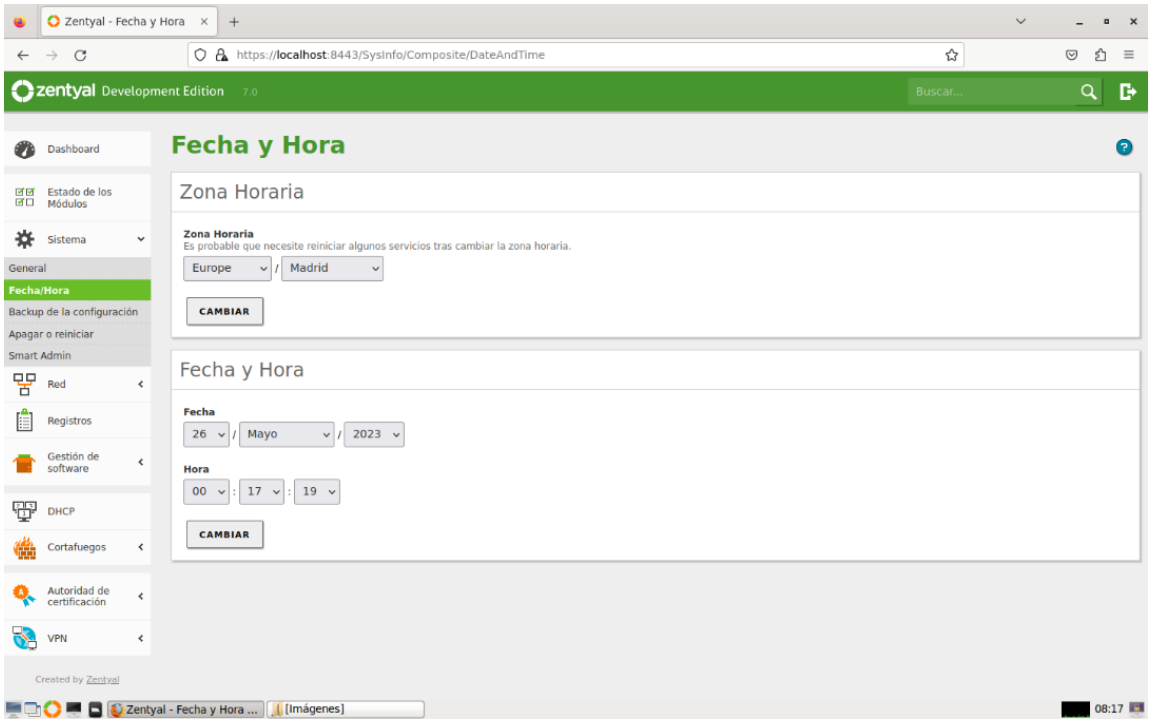


Ilustración 15. Fecha y hora del servidor.

Por último, cabe destacar que la configuración general de este software permite crear o restaurar copias de seguridad de la configuración para poder recuperar el servidor ante un desastre. Estas “backups” se guardan en local, es decir, en el disco duro de la propia máquina, por lo que, se deberá de copiar además en otro soporte físico externo, por si la máquina sufre algún daño.

En este caso, se han realizado distintas copias de seguridad. La primera, utilizando un clonador de disco, para tener la copia directamente en otro disco. Y, la segunda,

utilizando esta herramienta se ha creado una “backup” de la configuración, de la que se muestra la fecha en la que se ha realizado y el tamaño de esta. Si existen cambios de la configuración por guardar, Zentyal prohibirá realizar copias de seguridad.

En el caso de querer restaurar una de estas copias, simplemente se deberá de escoger el archivo que contiene la configuración deseada y restaurarlo. Es importante que el servidor donde se restaure la copia tenga la misma versión del software, el mismo número de interfaces y los mismos módulos instalados que la copia de seguridad.

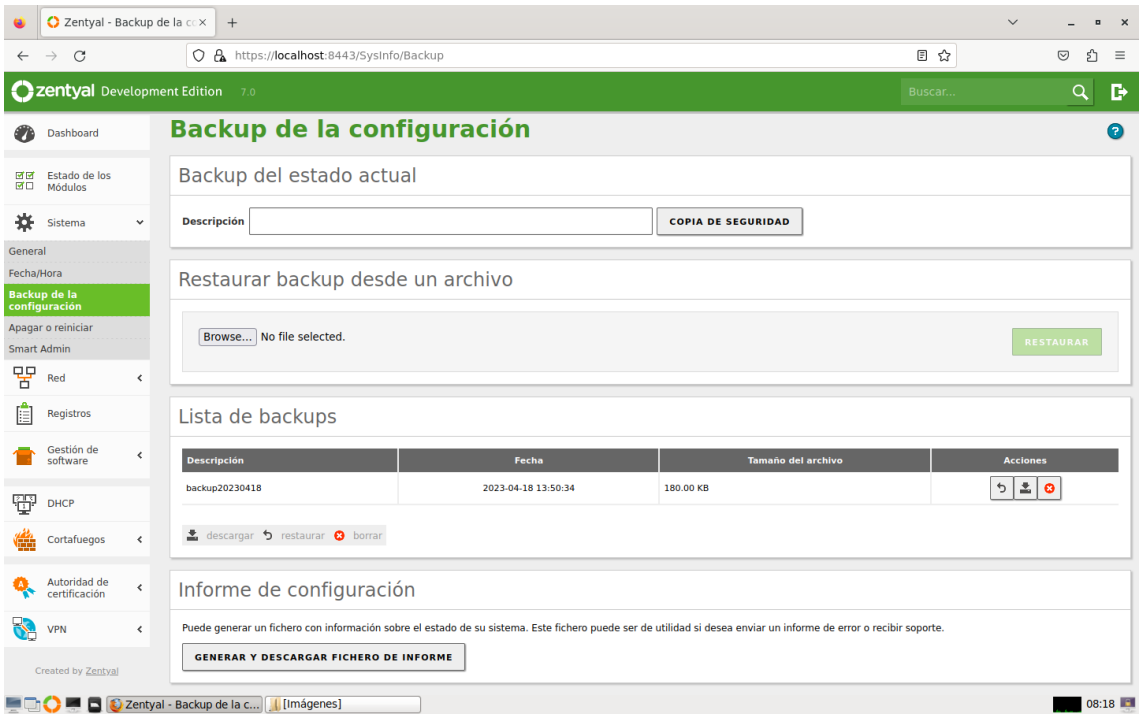


Ilustración 16. Backup de la configuración de Zentyal.

3.4.4. Gestión de software

En cuanto a la gestión del software, como cualquier sistema, el servidor de Zentyal necesitará actualizaciones constantes, o la mejora de sus servicios instalando

los nuevos módulos que se necesiten. Por un lado, Zentyal permite instalar, actualizar y eliminar módulos mediante la gestión de componentes. Para ello, se debe de acceder desde gestión de software y luego a gestión de componentes. Al entrar en dicha sección, se observan tres pestañas dependiendo de la acción que se quiera llevar a cabo:

- Instalar. Se muestran el nombre del módulo, la versión y la opción de seleccionarlo para instalarlo o no. Una vez seleccionados los módulos que se deseen, hay que apretar en el botón 'Instalar' que aparece debajo de la lista. También se puede actualizar la lista de los módulos que aparecen.

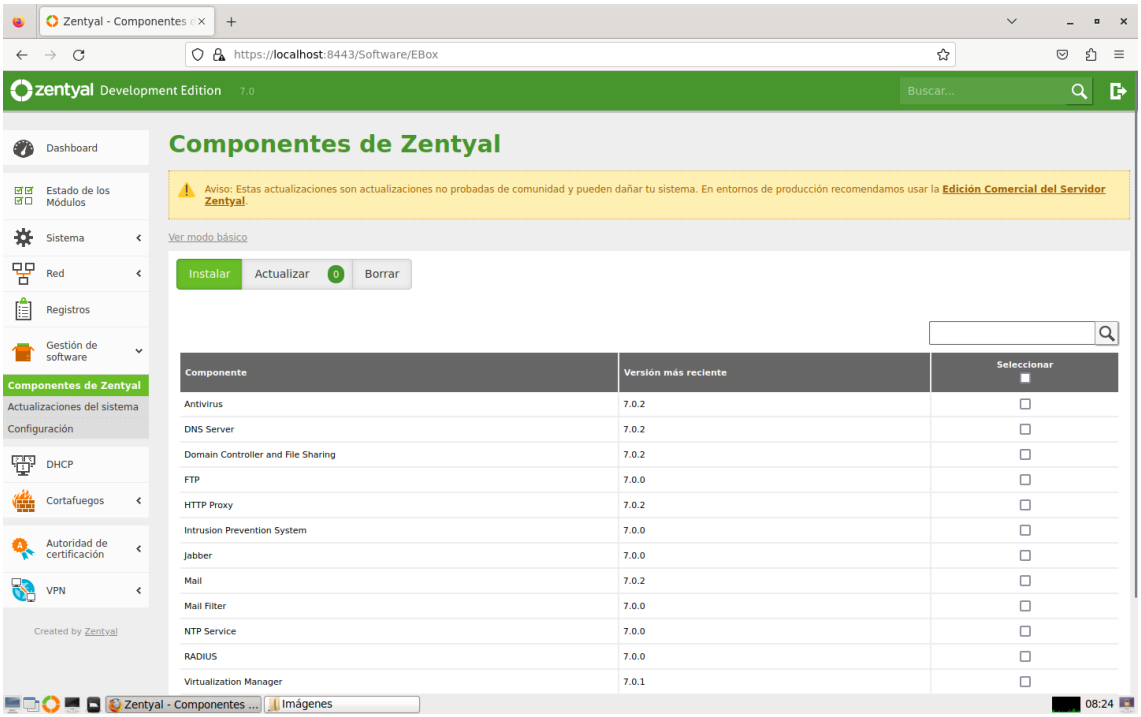


Ilustración 17. Instalación de nuevos módulos.

- Actualizar. En esta pestaña se muestran el número de actualizaciones disponibles, si no hay ninguna aparece un 0. En el caso de que aparezcan actualizaciones, se seleccionan los paquetes que se deseen actualizar y luego se pulsa en el botón 'Actualizar'.
- Borrar. En esta sección, se observa la misma tabla que en la opción de instalar con tres columnas, donde se debe de seleccionar los paquetes que se deseen

eliminar. Por último, se tiene que pulsar el botón ‘Borrar’ que se encuentra debajo de la tabla para finalizar el proceso. Antes de realizar dicha acción, se pide una confirmación para eliminar definitivamente los paquetes seleccionados.

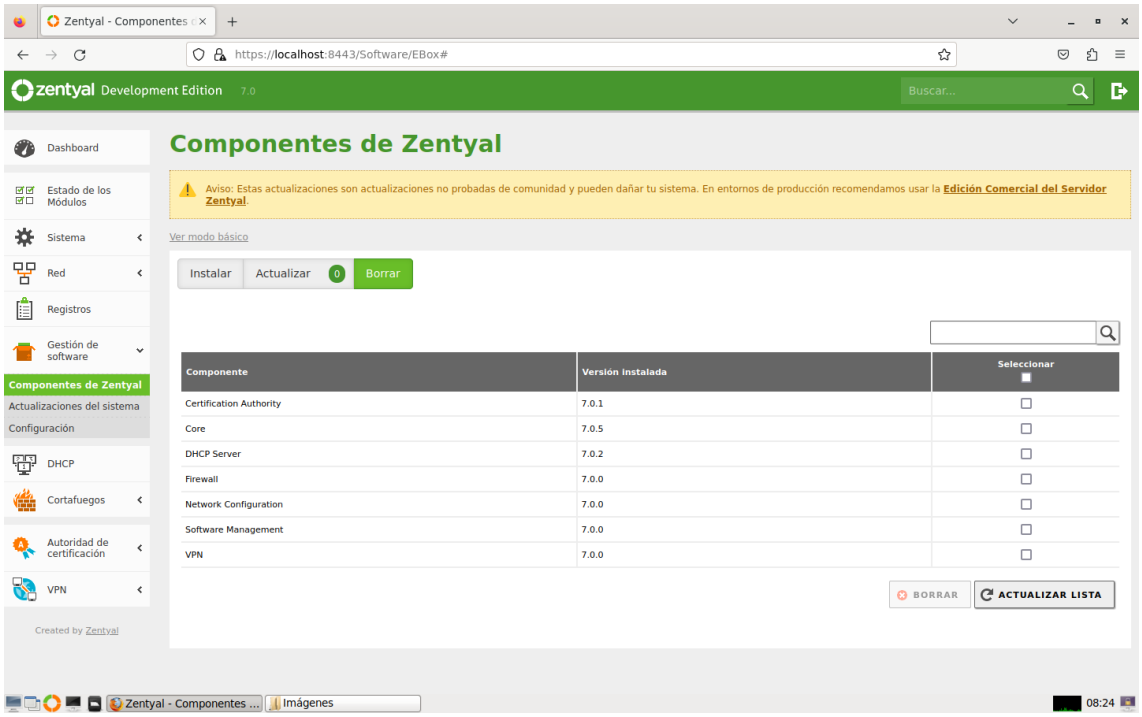


Ilustración 18. Eliminación de módulos ya instalados.

Además de los componentes de Zentyal, en este apartado del menú también se encuentran las actualizaciones del sistema que mantienen en constante funcionamiento los módulos que se utilizan. Al entrar en actualizaciones del sistema en el submenú d la izquierda, aparece una lista de los paquetes que se pueden actualizar, siempre que el sistema no esté actualizado. Si aparecen actualizaciones, simplemente se deben de seleccionar aquellas que se deseen implementar y luego pulsar en el botón ‘Actualizar’, y si no aparecen, se puede forzar la búsqueda de nuevas actualizaciones mediante el botón de ‘Actualizar lista’.

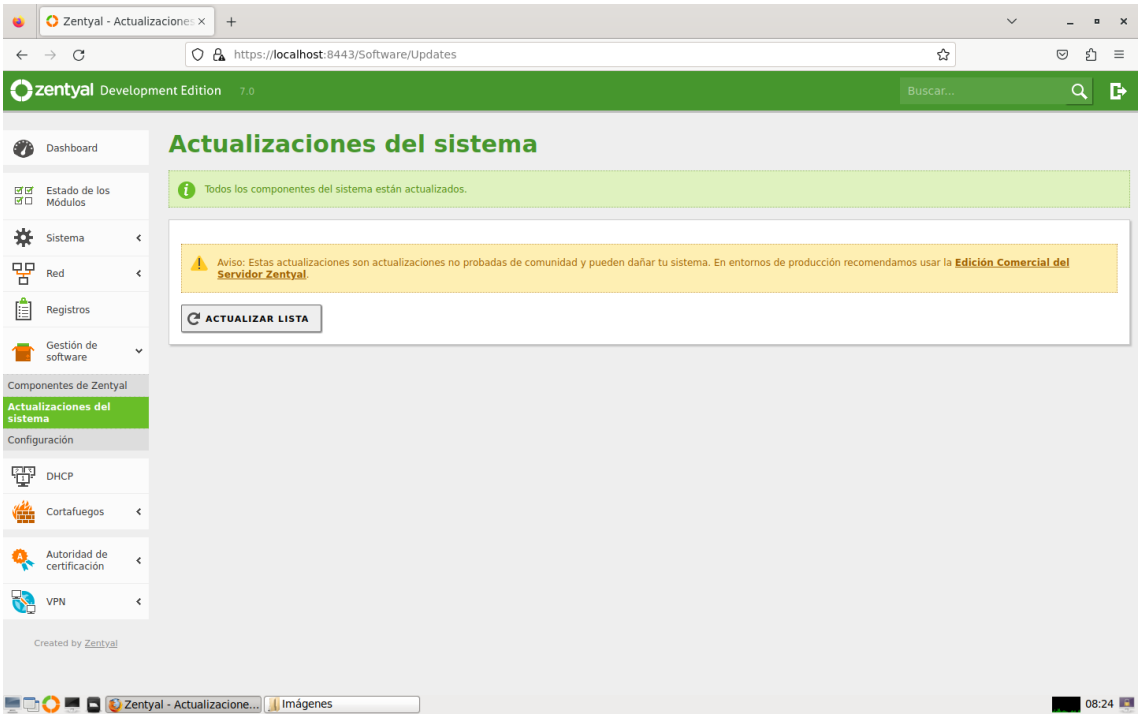


Ilustración 19. Actualizaciones disponibles del sistema.

De todas las actualizaciones, las de seguridad son las más importantes y el sistema las remarca con un icono de especial de un escudo, aunque se actualizan igual que el resto de las actualizaciones.

Finalmente, también se permite que las actualizaciones se instalen de forma automática activándolas desde el submenú de configuración dentro de la gestión del software. Solo es necesario indicar la hora del día en la que se van a realizar las actualizaciones y el sistema automatizará el proceso.

3.4.5. Registros

Al mismo tiempo, Zentyal permite guardar información de todos los módulos a través de los registros. Estos registros se almacenan en una base de datos de MySQL

que permite realizar consultas, actualizaciones e informes de forma eficaz y eficiente, y que se pueden consultar a través de la interfaz del propio servidor, pero para poder utilizarlo primero se debe de habilitar desde la opción ‘estado de los módulos’ que se ha mencionado con anterioridad.

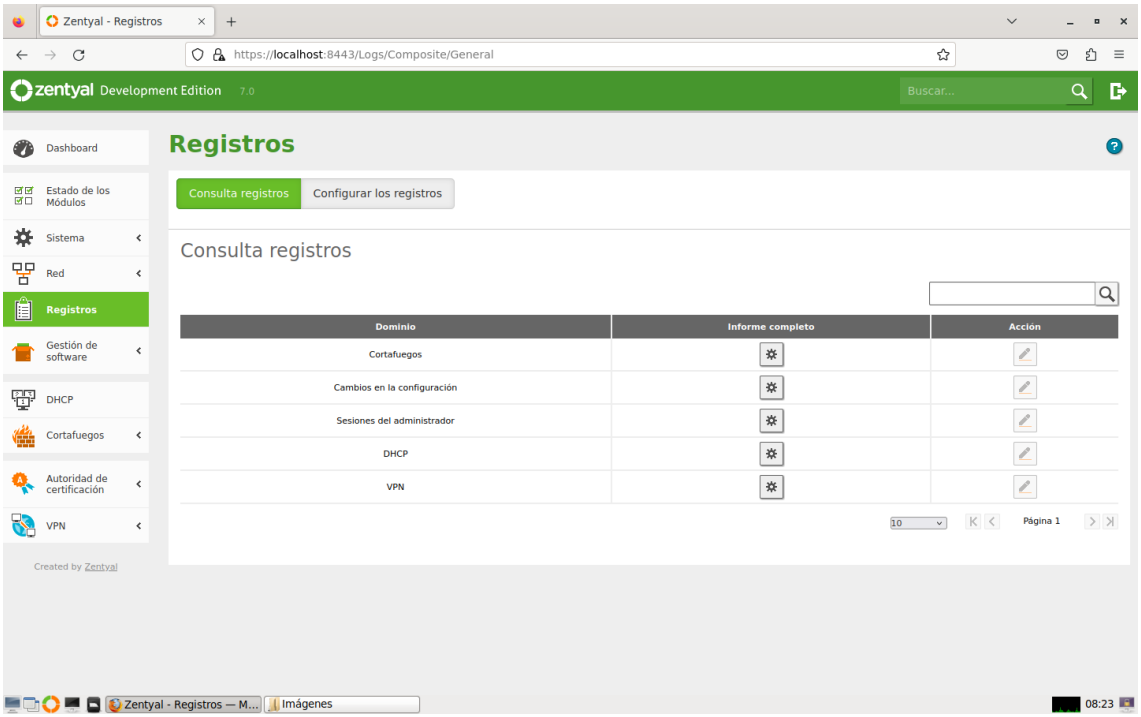


Ilustración 20. Consulta de registros del servidor.

Una vez seleccionada la opción de informe dentro de registros, esta nos ofrece un informe detallado para todas las acciones y datos registrados del servicio seleccionado, aunque dependiendo del módulo la información y los filtros que se muestran son distintos.

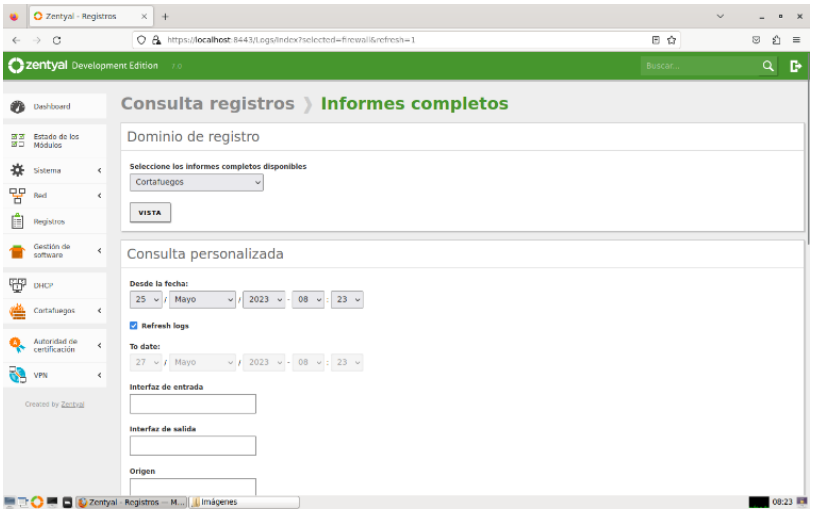


Ilustración 21. Informes completos sobre los registros.

Todas estas consultas, se pueden almacenar y etiquetarlas como eventos para que salte una notificación en el caso de que se produzca una coincidencia con algún registro ya guardado.

Asimismo, si la consulta realizada no tiene límite de tiempo, los resultados se actualizan automáticamente con los nuevos datos registrados.

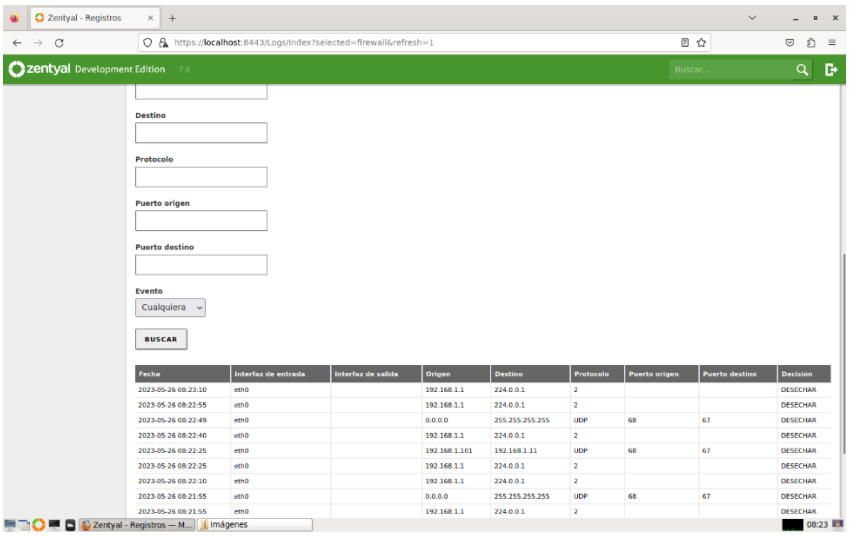


Ilustración 22. Registros almacenados en el servidor.

Por otro lado, también es importante saber que se puede modificar la configuración de los registros de los servicios instalados. Para cada servicio se puede marcar como habilitado o deshabilitado, dependiendo de si se quiere almacenar los registros de ese dominio, y se pueden purgar los registros anteriores indicando el tiempo máximo que se almacenarán estos, eliminando aquellos que superen la fecha marcada, en este caso una semana. Aunque esta segunda opción se puede forzar y se pueden eliminar todos los registros almacenados entre una hora y noventa días, seleccionando la opción que se desea y apretando encima del botón 'Purgar'.

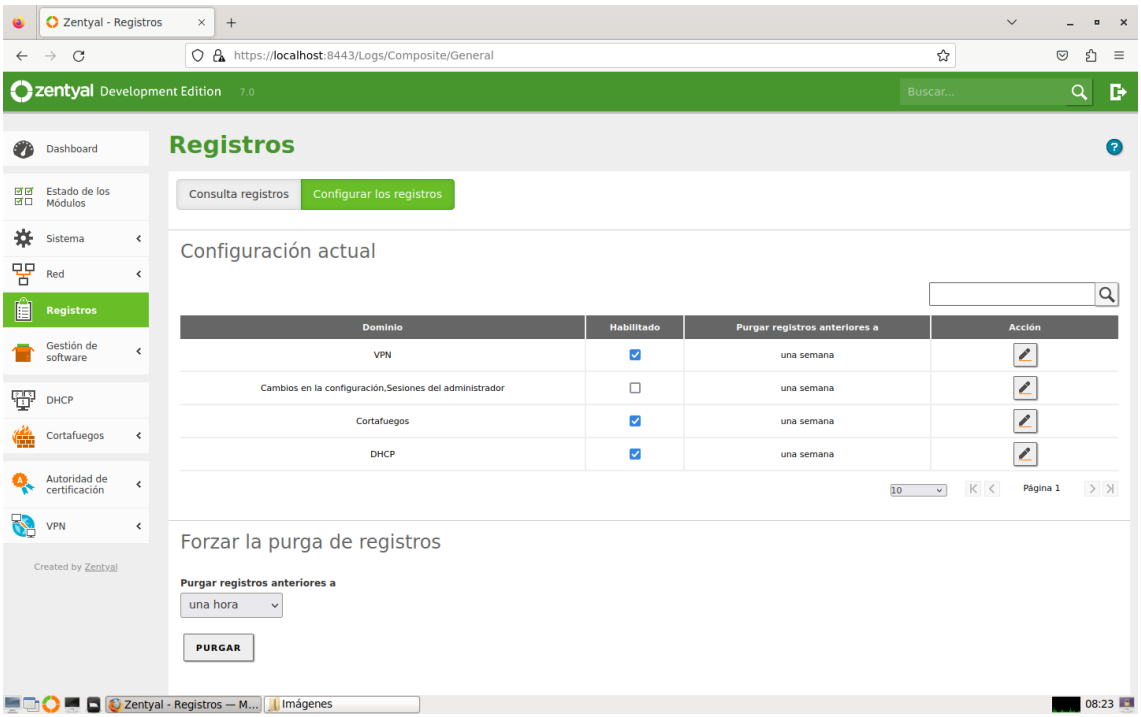


Ilustración 23. Configuración de los registros.

Además, es importante saber que Zentyal trata de forma distinta a las acciones que surten efecto de forma instantánea, quedando registradas permanentemente, y a las acciones que no se aplican hasta guardar los cambios, que se muestran en la ventana emergente de 'Guardar cambios' hasta que estos se aplican.

Una vez instalados todos los módulos básicos para manejar y configurar el servidor de Zentyal, se van a instalar todos los módulos que se necesitan para cumplir con el objetivo principal del proyecto, es decir, con las demandas y requerimientos impuestos por el cliente.

3.4.6. Red

En este servicio, lo que se va a conseguir es conectar el servidor a la máquina para que tenga conexión para poder realizar cualquier cambio o actualización que se desee, o para establecer comunicación con otros equipos.

Interfaces de red

En primer lugar, se conectarán dos tarjetas de red al servidor y se van a configurar cada una de ellas con los parámetros establecidos por la empresa. Una de ellas definida como externa que dará la conexión a Internet, y la otra como interna conectada a la red interna.

A cada una de las tarjetas de red se le puede establecer la dirección de red por varios métodos, como:

- Estática. Método mediante el que se especifica la dirección IP, la máscara de red y, además, se pueden asociar distintas interfaces virtuales para ofrecer un servicio en más de una dirección IP o subred.
- Dinámica. Método que especifica la dirección IP y la máscara de red de forma automática, tanto para una red interna como para una externa.
- PPPoE. Si se dispone de un router ADSL PPPoE y sólo hay que introducir el nombre de usuario y la contraseña dada por el proveedor.
- Trunk (802.1Q). En el caso de tener que conectar el servidor a una o más redes VLAN. Con este método, se pueden crear todas las interfaces necesarias para segmentar la red local, mejorar el rendimiento y aumentar la seguridad de la red.

- Bridged. Más conocido como modo puente de red, que consiste en conectar dos interfaces de red conectadas a dos redes diferentes y que se comuniquen de modo transparente.
- Bonding. Método que se utiliza en el caso de querer unir dos o más interfaces físicas para crear una interfaz virtual con la suma del ancho de banda de ambas interfaces. Este método se debe realizar solo sobre las interfaces de red internas del servidor.

La primera de estas tarjetas de red, que lleva por nombre 'eth0', se define mediante el método estático, en el que se han definido la dirección IP '192.168.1.11' y la máscara de red '255.255.255.0', como se observa en la siguiente imagen. En cuanto a interfaces virtuales, no se ha añadido ninguna.

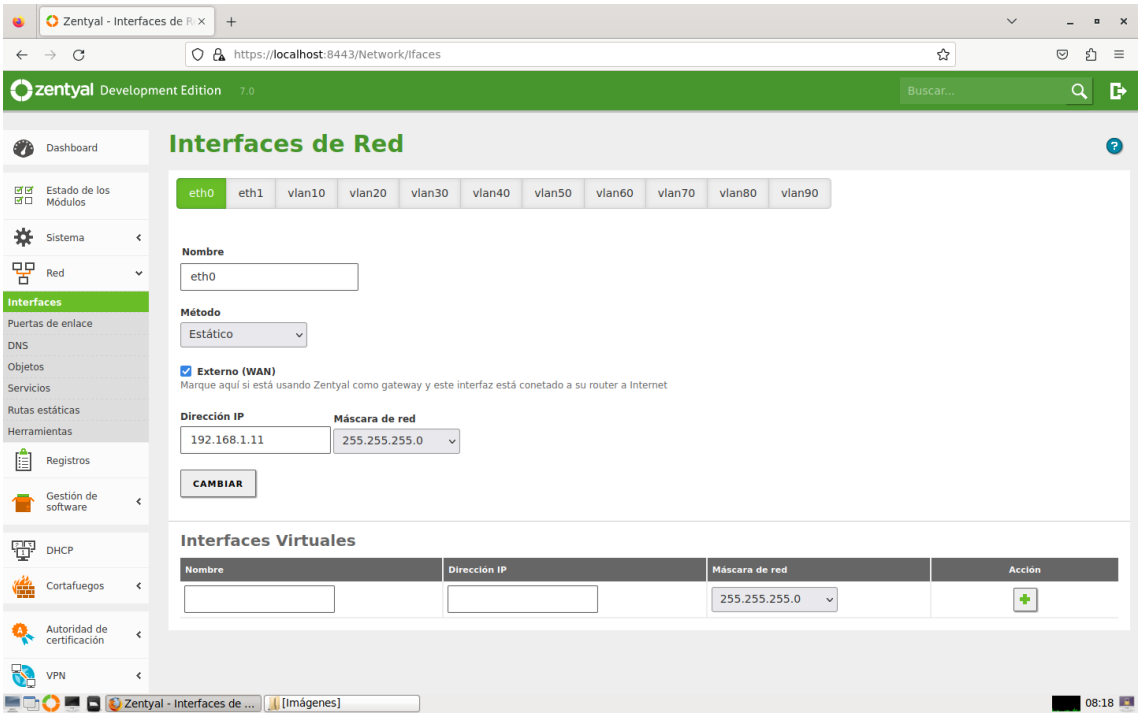


Ilustración 24. Configuración de las Interfaces de red.

La segunda de estas tarjetas de red, que lleva por nombre 'eth1', se ha definido mediante el trunk (802.1Q), en el que se han definido nueve VLANs distintas, para

recrear el sistema de la empresa, donde cada VLAN se utiliza para un tipo de dispositivos, diferenciando entre PCs, impresoras, pistolas, pantallas…

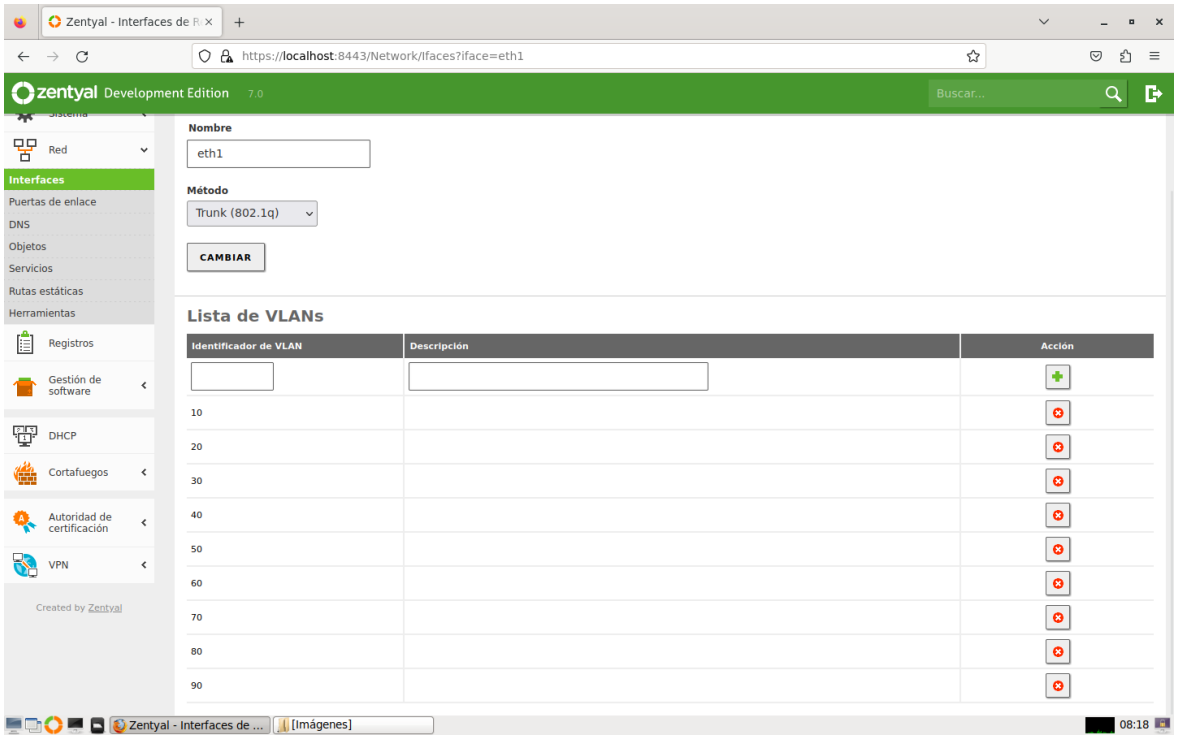


Ilustración 25. Lista de VLANs creadas.

De todas las VLANs, a continuación, se muestran la VLAN10 y la VLAN60, donde la máscara de red sigue siendo de tipo C, como en la 'eth0', sin embargo, en este caso las direcciones IP de ambas VLANs, '10.31.3.254' y '10.31.5.254' respectivamente, nos indican las puertas de enlace que utilizarán todos los dispositivos de estas dos subredes.

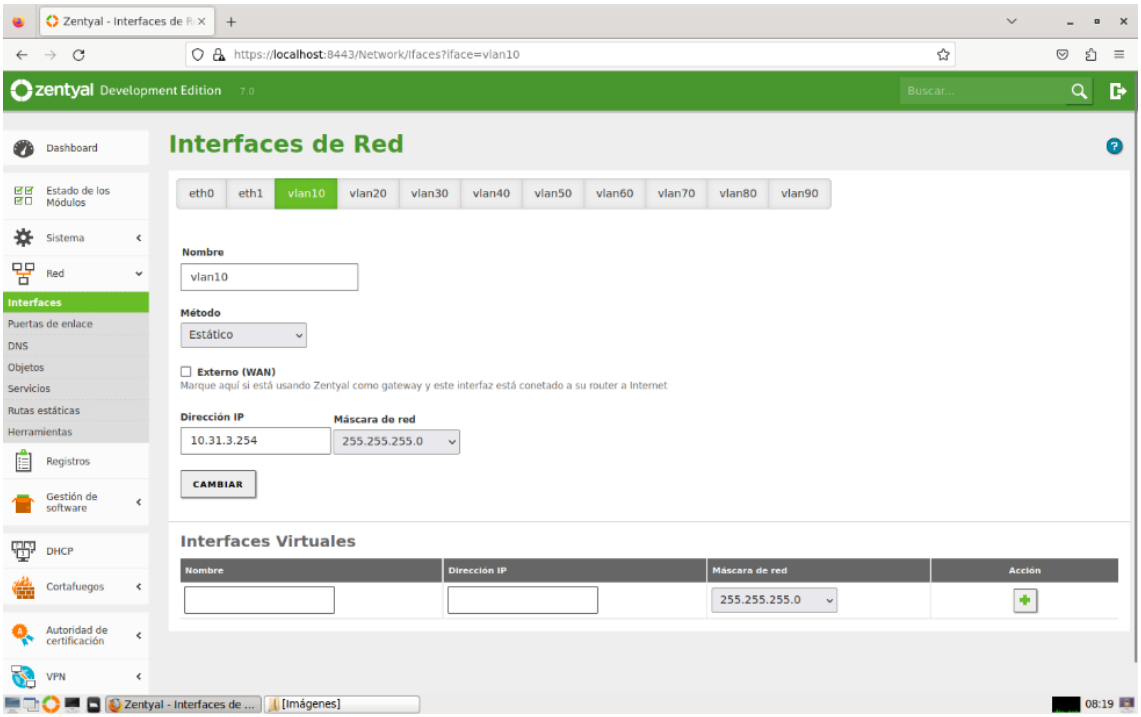


Ilustración 26. Ejemplo de configuración de la VLAN10.

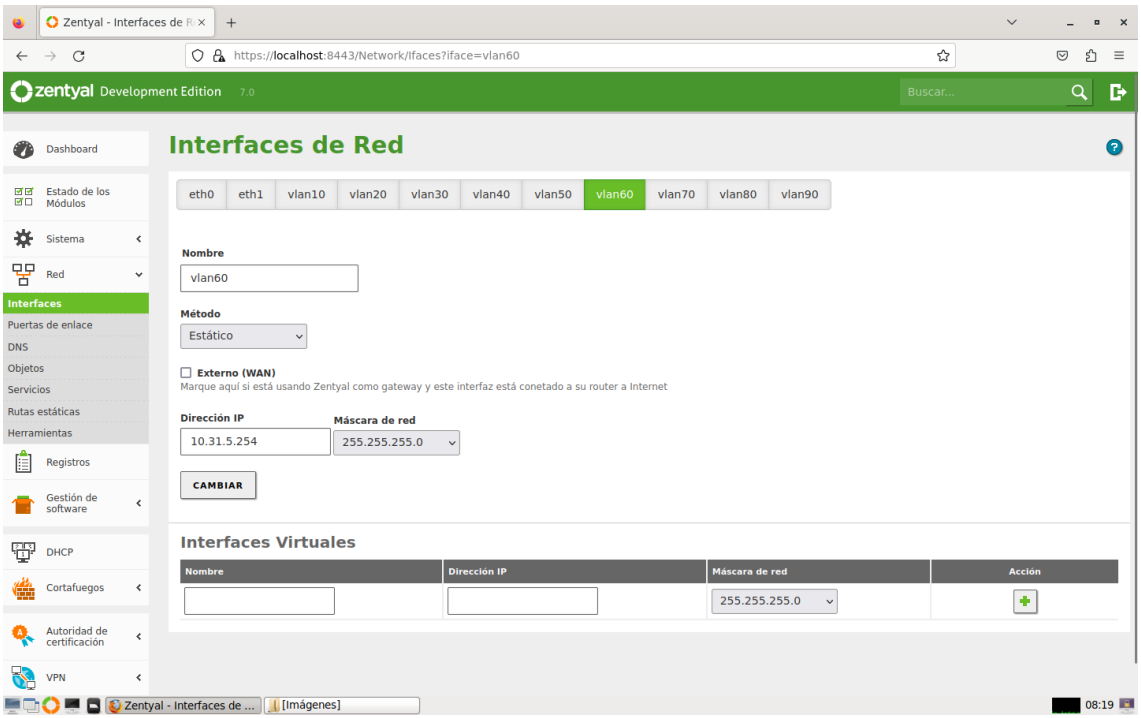


Ilustración 27. Ejemplo de configuración de la VLAN60.

Puerta de enlace y DNS

Lo siguiente para tener conexión a Internet, va a ser definir la puerta de enlace y los DNS que se van a utilizar.

La puerta de enlace es la ruta por defecto que siguen las conexiones para salir a la red externa, es decir, para salir a Internet. Para establecer una puerta de enlace se debe indicar un nombre, una dirección IP que debe ser accesible directamente desde el servidor sin intermediarios, un peso para conocer la preferencia entre las distintas puertas de enlace que pueden existir y marcar si será la puerta de enlace predeterminada o no. Como se observa en la siguiente imagen la puerta de enlace que se utilizará como predeterminada, lleva por nombre 'gw1' con la dirección IP '192.168.1.1' y se encuentra habilitada para su uso.

Una vez establecida la puerta de enlace se puede habilitar o deshabilitar, editar o eliminar dicha puerta de enlace.

Además, se puede configurar un proxy, aunque en este caso no será necesario.

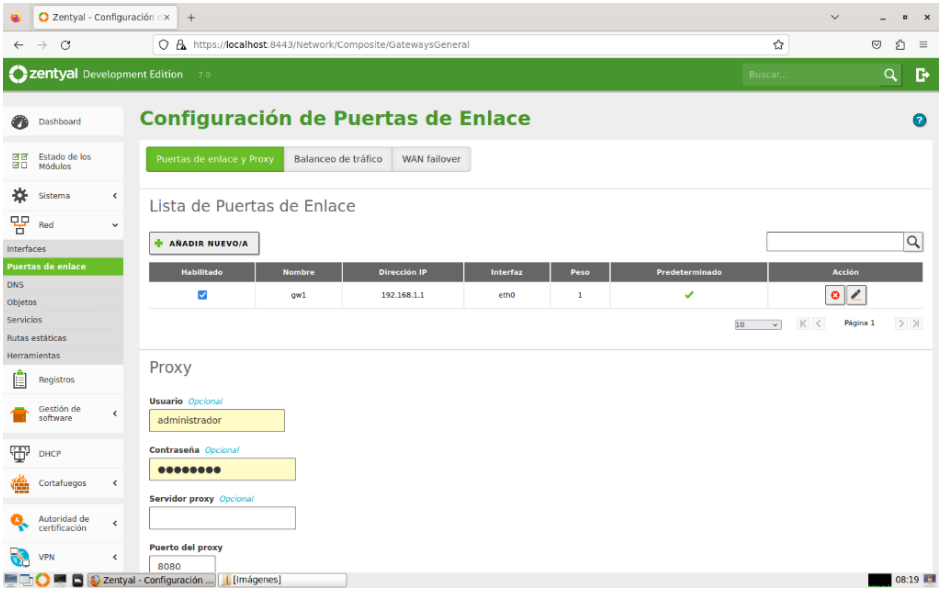


Ilustración 28. Configuración de la puerta de enlace.

En cuanto al DNS, para que el sistema sea capaz de resolver distintos nombres de dominio, hay que indicarle los DNS que sean necesarios. En este caso se definen el DNS primario y el secundario del router, siendo las direcciones de dichos DNS las siguientes ‘80.58.61.250’ y ‘80.58.61.254’, respectivamente.

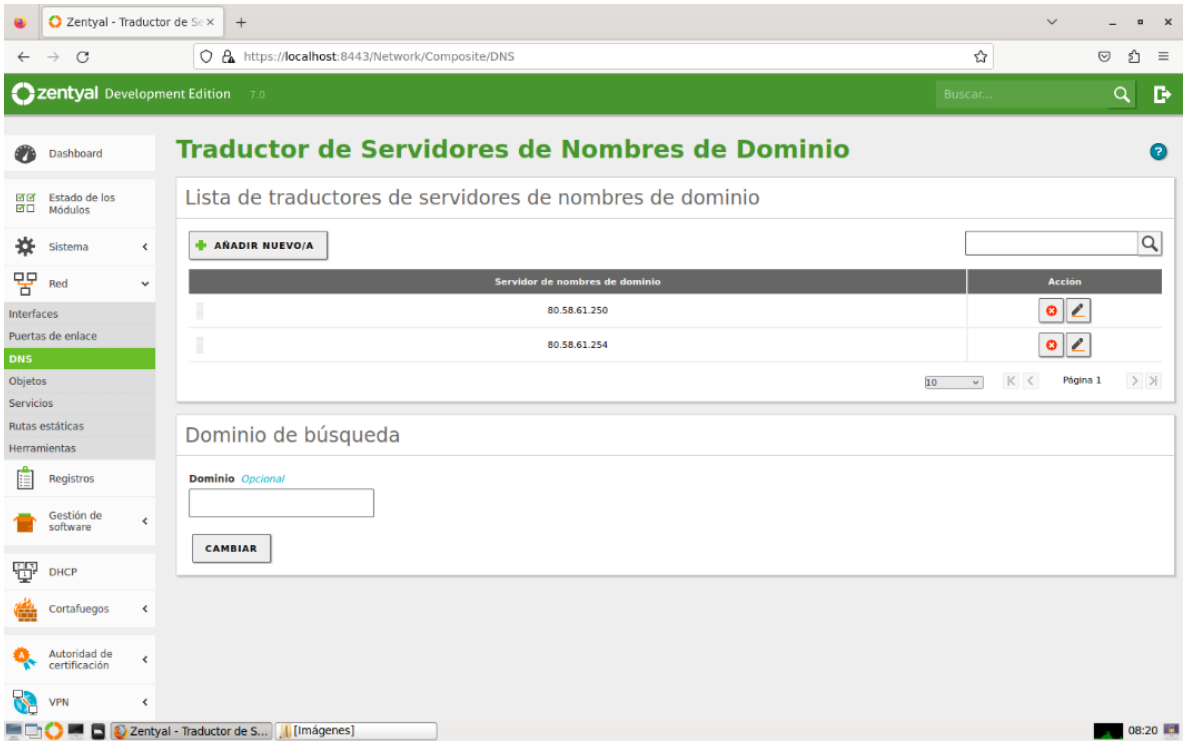


Ilustración 29. Configuración DNS primario y secundario.

Objetos y Servicios de red

A continuación, se van a definir los objetos y los servicios de red que se utilizarán más adelante para establecer las reglas que se van a introducir en el Firewall, ya que, muchos de estos utilizan las mismas reglas, y al definirlos como objetos o servicios simplemente se definen dichas reglas una vez.

Por un lado, se encuentran los objetos de red que son aquellos elementos o conjunto de elementos que se encuentran dentro de la red.

En primer lugar se observa una lista vacía, pero al ir creando objetos estos se van añadiendo a la lista. En dicha lista, se observan los nombres dados a los objetos, así como las distintas acciones que se pueden realizar con ellos como crear, editar, eliminar o clonar.

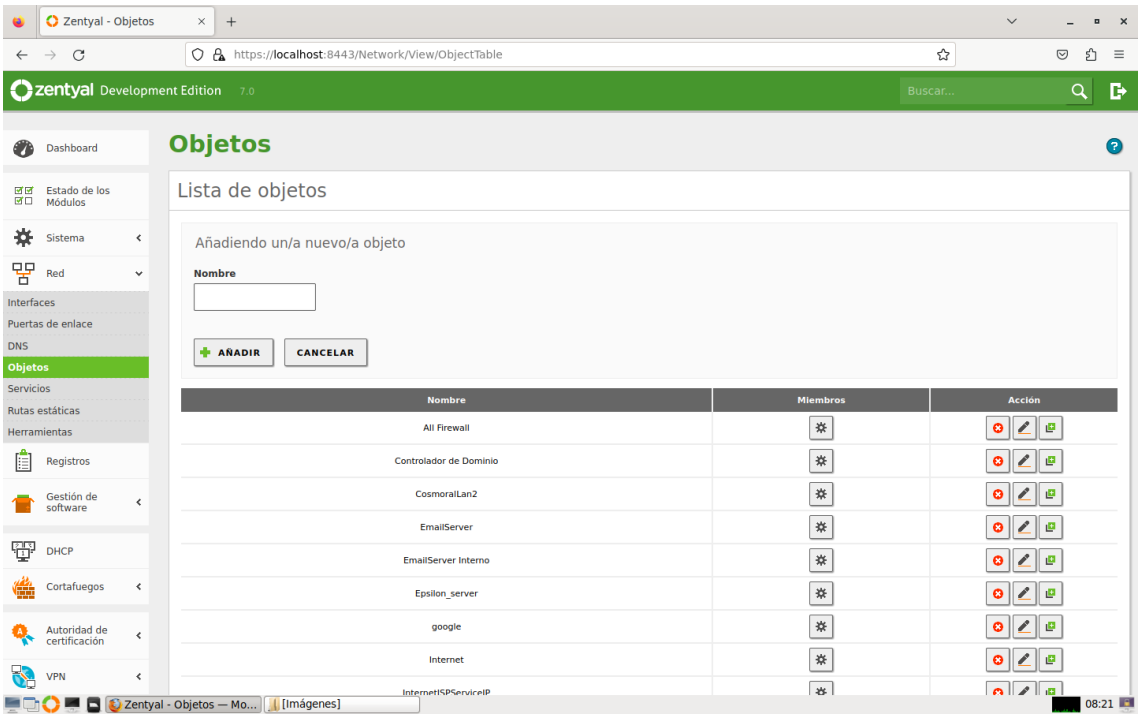


Ilustración 30. Lista de los objetos de red creados.

Para crear un nuevo objeto, simplemente se añade el nombre que va a llevar dicho objeto y se añade a la lista. Una vez añadido, se le da a editar y como en la imagen siguiente, se pedirá el nombre de cada dispositivo vinculado a este objeto y su dirección IP.

Además, cabe destacar que un miembro o dispositivo puede estar vinculado a más de un objeto, aunque hay que tenerlo en cuenta al configurar las reglas del firewall para no obtener configuraciones no deseadas.

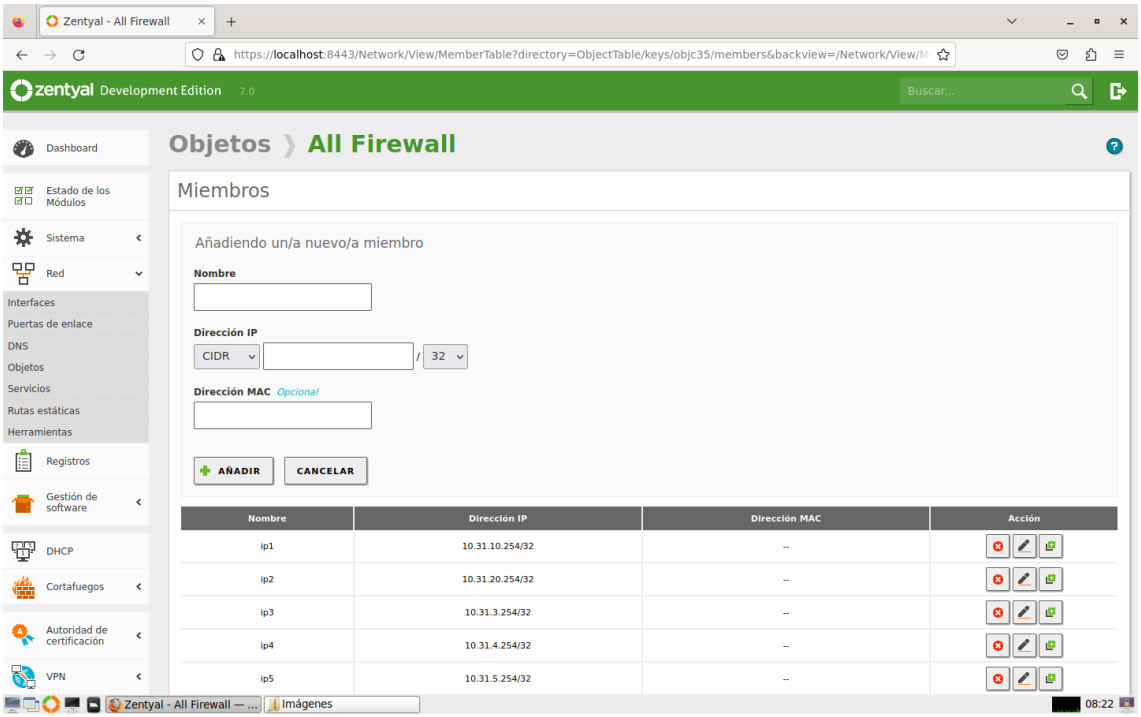


Ilustración 31. Creación de un nuevo objeto de red.

Por el otro lado, se encuentran los servicios de red que son la manera de representar los protocolos y puertos que se van a utilizar por cada aplicación o módulo.

Se utilizan de forma similar a los objetos, pero en este caso hace referencia a un conjunto de puertos, en vez de a un conjunto de direcciones IP.

En este caso, al igual que con los objetos, aparece en primer lugar una lista vacía de los servicios disponibles, en la cual se pueden añadir los servicios deseados dando un nombre al servicio y una descripción.

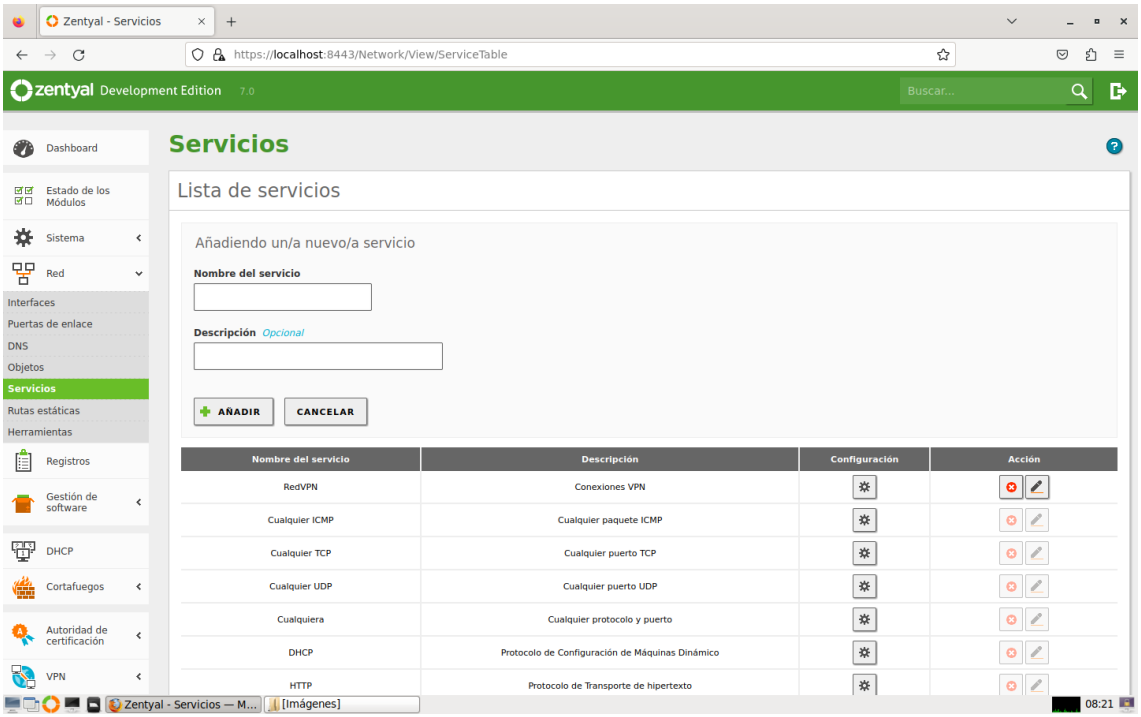


Ilustración 32. Lista de los servicios de red creados.

Una vez dado el nombre de servicio y una pequeña descripción de este, dentro de la configuración se puede elegir el tipo de protocolo a elegir y los puertos origen y destino que van a utilizar.

Como se observa en el siguiente ejemplo, el servicio que se ha configurado para la VPN utiliza el protocolo UDP, desde un puerto origen cualquiera a dos puertos destino distintos, el ’1194’ y el ‘11194’, que se utilizarán más adelante para configurar la VPN para los distintos empleados que requieran de esta.

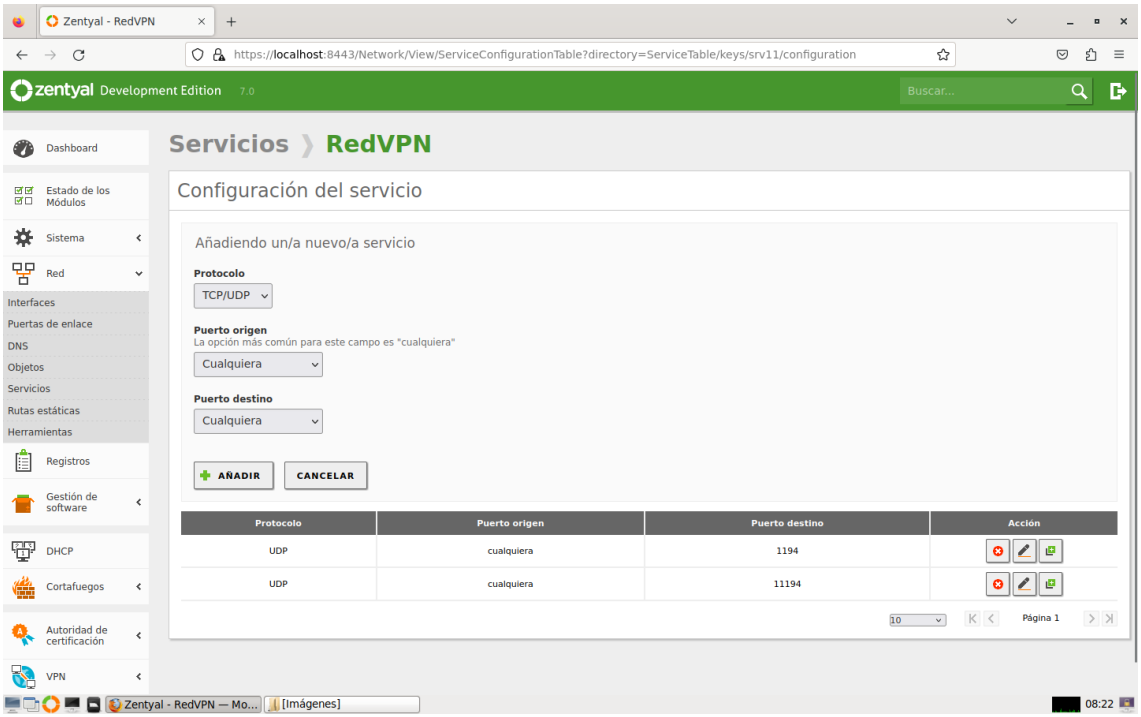


Ilustración 33. Creación de un nuevo servicio de red.

Failover

Por último, para configurar el “failover”, para que la empresa siga funcionando por si la red principal cae, se debe de configurar la tolerancia a fallos en la que se requiere que existan habilitadas dos o más puertas de enlace. Una vez estén habilitadas dichas puertas, se deben de establecer unas reglas de prueba a la puerta de enlace principal, estableciendo el número de pings que se van a lanzar a una IP determinada y cumpliendo un ratio de éxito definido, que en este caso las reglas serán de 6 pings a la dirección IP 8.8.8.8 de Google, con un ratio mínimo del 40%. Si estas reglas no se cumplen, se establecerá automáticamente la conexión a través de la segunda puerta de enlace que tenemos definida en el servidor.

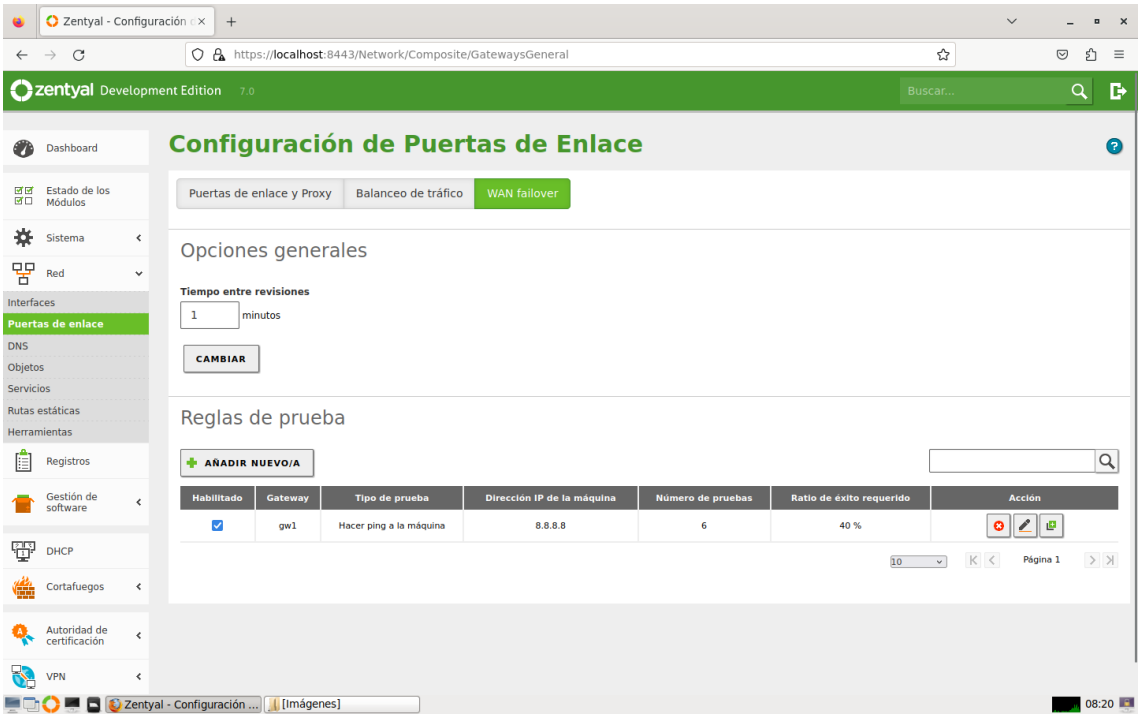


Ilustración 34. Configuración del 'Failover'.

3.4.7. Firewall

Para este módulo, Zentyal utiliza el subsistema del kernel de Linux llamado 'Netfilter', que proporciona servicios de filtrado, de tráfico y redirección de conexiones. Además, proporciona una configuración predeterminada segura, diferenciando entre las conexiones internas y las externas para realizar un filtrado más estricto. Esto se puede modificar al gusto del cliente, para adaptarse a las necesidades requeridas.

Una vez, se selecciona el módulo del cortafuegos se diferencian cuatro secciones donde cada una controla diferentes flujos de tráfico, dependiendo del origen y del destino. Son:

- Reglas de filtrado de redes internas a Zentyal.
- Reglas de filtrado para las redes internas.

- Reglas de filtrado desde la redes externas a Zentyal.
- Reglas de filtrado para el tráfico saliente de Zentyal.

A partir del esquema dado por el cliente, se va a determinar en qué sección se debe situar las reglas de filtrado del tráfico que deseamos controlar.

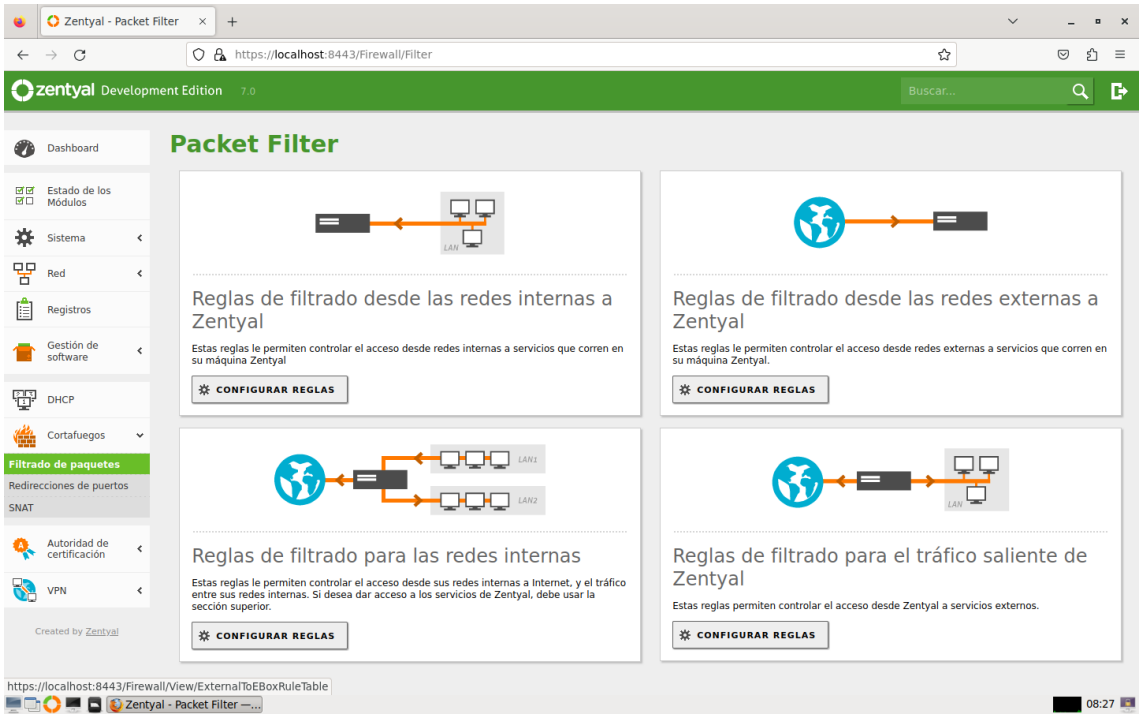


Ilustración 35. Secciones disponibles para configurar las reglas del Firewall.

A la hora de definir las reglas del firewall, Zentyal provee una forma sencilla de definirlas utilizando los servicios y objetos de red, introducidos anteriormente, para especificar que protocolos y puertos se aplican, y sobre que direcciones de origen o destino.

El parámetro de mayor relevancia será la decisión a tomar con las nuevas conexiones creadas. En cualquiera de las cuatro secciones se permite tomar tres tipos distintos de decisiones:

- Aceptar la conexión.

- Denegar la conexión.
- Registrar la conexión como un evento y seguir evaluando el resto de reglas.

A partir de este momento, todas las reglas configuradas aparecen en una tabla y son aplicadas ordenadamente “de arriba a abajo”. Es decir, cuando más arriba se coloque una regla más prioridad se le da, por eso el orden de las reglas en las tablas es muy importante. Asimismo, se le puede añadir un campo de descripción para conocer el funcionamiento de cada una de las reglas.

A continuación, observamos cuatro imágenes, mostrando las cuatro secciones y algunas de las reglas creadas en cada sección. Como se observa, todas las secciones contienen tablas distintas, por lo que al crear las reglas se piden distintos datos a rellenar. Una vez rellenados los datos de cada una de las reglas se pueden modificar, y al mismo tiempo, cualquier regla puede ser eliminada, clonada o cambiada de lugar en la tabla para aumentar o disminuir su prioridad.

Para definir todas las reglas, se ha seguido un documento dado por el cliente, Korott SL, el cual permite replicar el sistema principal tal y como se encuentra actualmente. Cualquier modificación posterior se debe de añadir y dejarla documentada para tener una copia de seguridad.

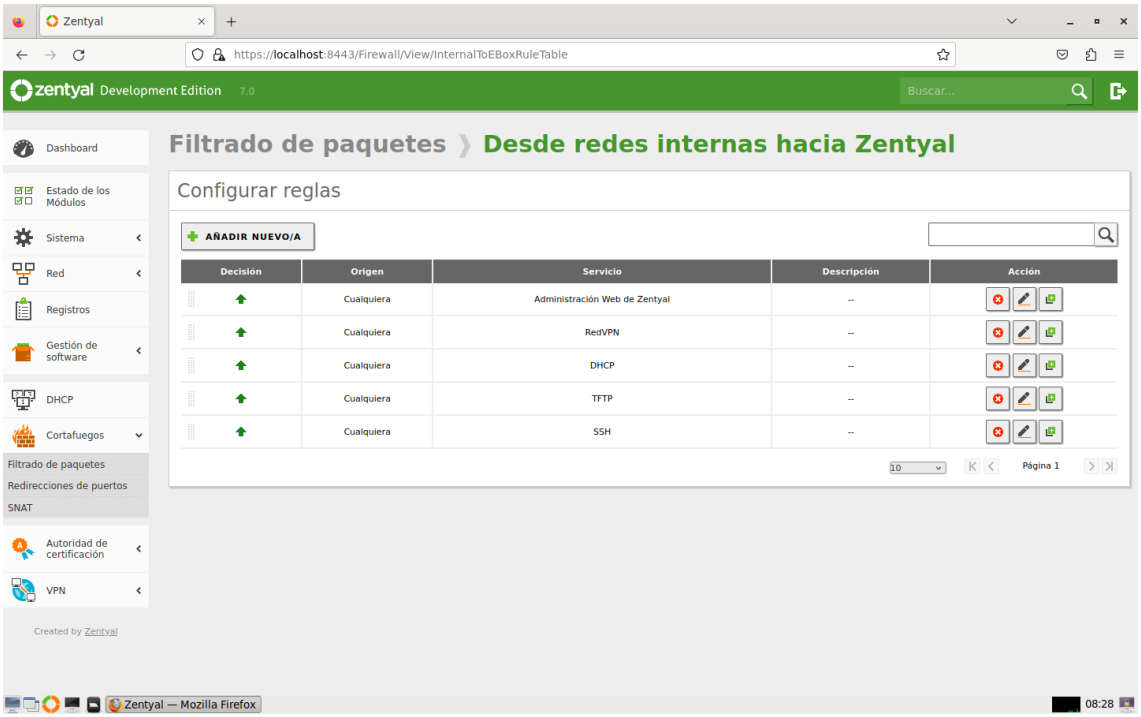


Ilustración 36. Reglas desde redes internas hacia el servidor.

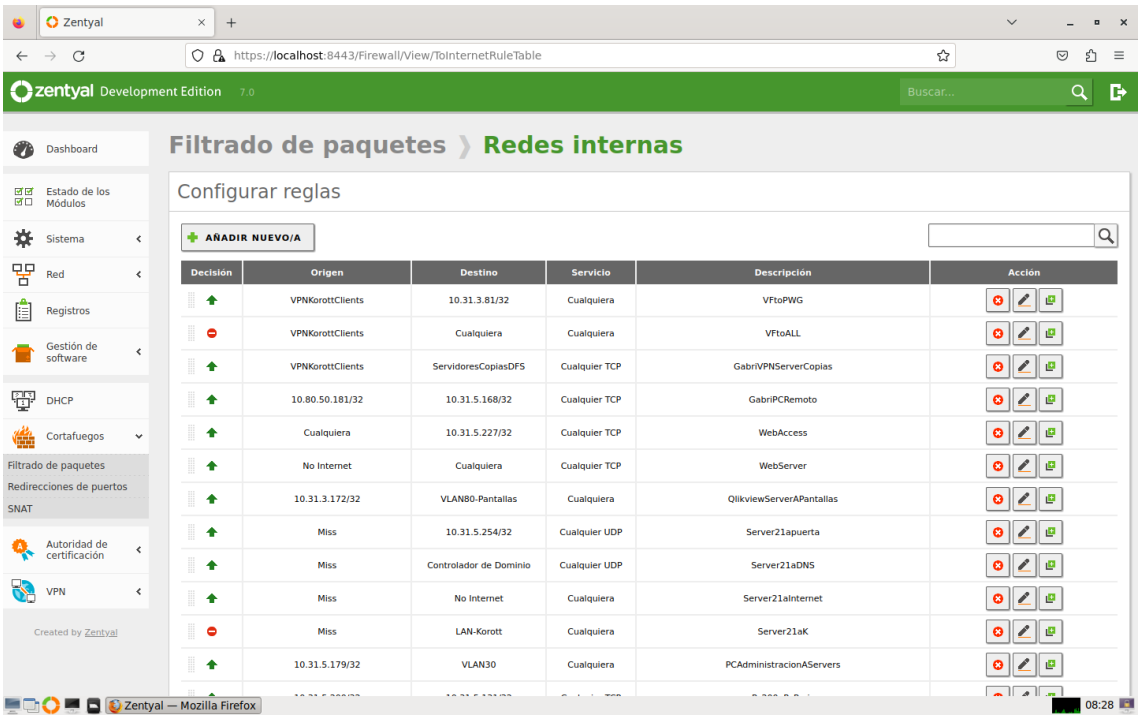


Ilustración 37. Reglas dentro de las redes internas.

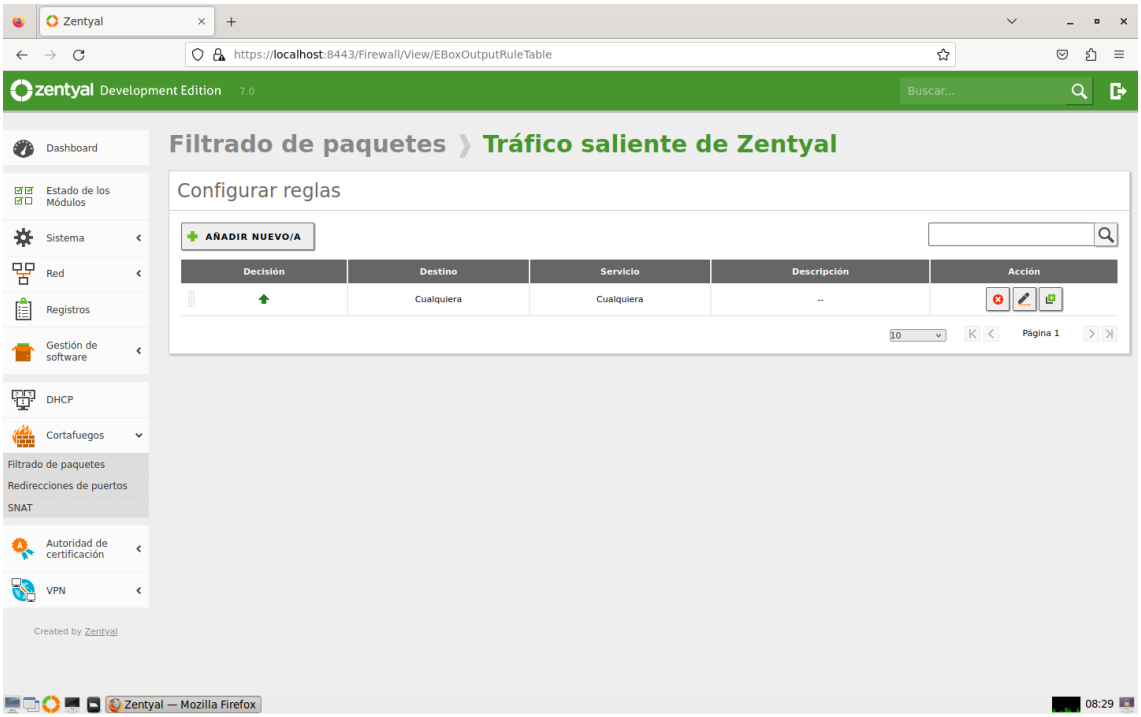


Ilustración 38. Reglas del tráfico saliente desde el servidor.

Ilustración 39. Reglas desde las redes externas hacia el servidor.

Finalmente, como se observa el mayor número de reglas se encuentran en las redes internas, ya que, lo que más interesa es controlar todo el tráfico interno de la empresa, mientras que el externo está directamente denegado.

3.4.8. DHCP

A la hora de configurar el servicio de DHCP se necesita una interfaz interna configurada sobre la que se despliega el servicio. Una vez dentro del menú, se encuentra una lista de todas las interfaces disponibles sobre las que se puede ofrecer el servicio. Además, para que no salten errores ni se den IP duplicadas, se debe de eliminar el servicio DHCP del router como se explicará en las pruebas finales.

En este caso, se observan como interfaces disponibles todas aquellas que han sido creadas con anterioridad, tanto la interfaz principal para realizar las conexiones como las distintas VLANs creadas.

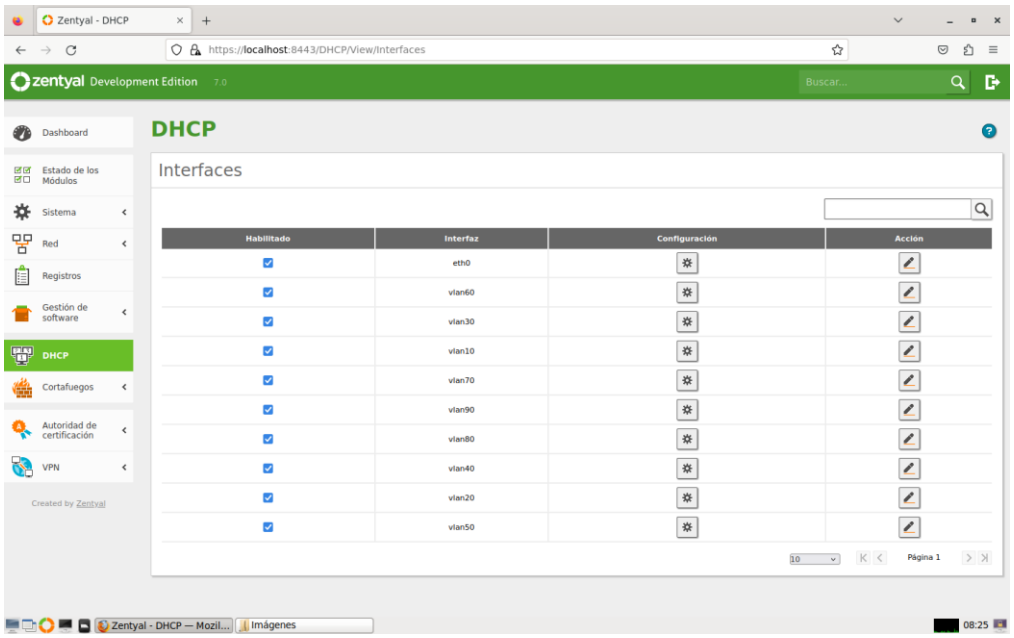


Ilustración 40. Servicio DHCP.

Entre todas estas interfaces disponibles, se va a utilizar la primera, la ‘eth0’, como ejemplo para conocer más a fondo como se configura este módulo. Una vez dentro de la configuración de una interfaz, aparecen distintos parámetros para configurar:

- Puerta de enlace. Es la puerta de enlace que va a emplear el cliente para comunicarse con destinos que no están en su red local. En este caso, siempre se utiliza la puerta de enlace configurada con anterioridad.
- Dominio de búsqueda. Se puede añadir un dominio de búsqueda para poder realizar un nuevo intento de resolver un nombre de dominio, cuando no ha tenido éxito en un principio.
- Servidor de nombres primario y secundario. Son los nombres de dominio que usará el cliente cuando tiene que resolver un nombre de dominio. Si el primario no tiene éxito, utilizará el secundario. En este caso el nombre primario y el secundario son ‘80.58.61.250’ y ‘80.58.61.254’, respectivamente.
- Servidor NTP. Es opcional para sincronizar el reloj del cliente, sino el cliente usará el suyo propio.
- Servidor WINS. Es opcional para resolver nombres en una red NetBIOS, aunque en este caso no es necesario.
-

Una vez rellenados todos los parámetros se da a cambiar, para guardar los cambios.

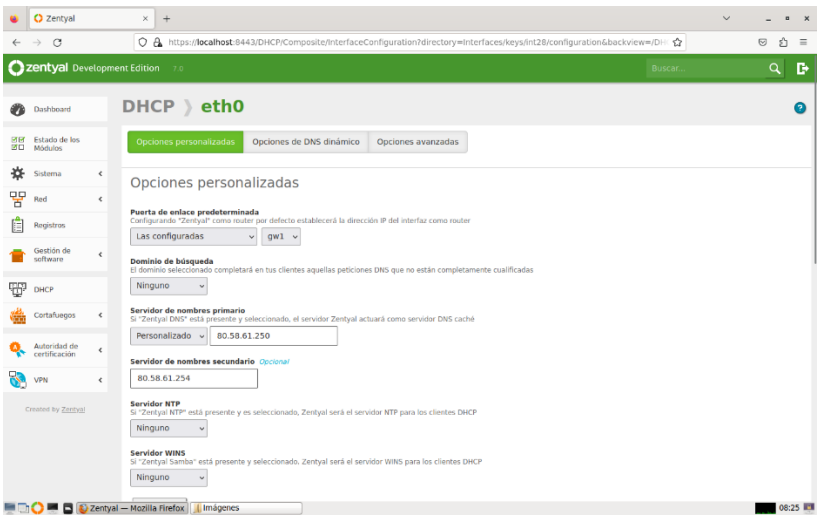


Ilustración 41. Configuración del DHCP para la interfaz 'eth0'.

Más tarde, debajo de estas opciones se pueden ver los rangos dinámicos de direcciones y las asignaciones estáticas. Para que funcione, se debe de dar como mínimo un rango de direcciones para que este servicio pueda distribuir las distintas IPs.

Como se observa en la siguiente imagen, aunque el rango disponible es desde '192.168.1.1' a '192.168.1.254', se ha creado el rango de direcciones que se pueden administrar por DHCP desde la IP '192.168.1.21' a '192.168.1.253', ya que, las primeras 20 direcciones y la última están reservadas por si en algún momento se desea implementar algún servicio especial. En este caso no hay asignaciones estáticas de direcciones, solo la última que está definida como puerta de enlace. Al igual que en el ejemplo, el resto de interfaces mantienen la misma configuración.

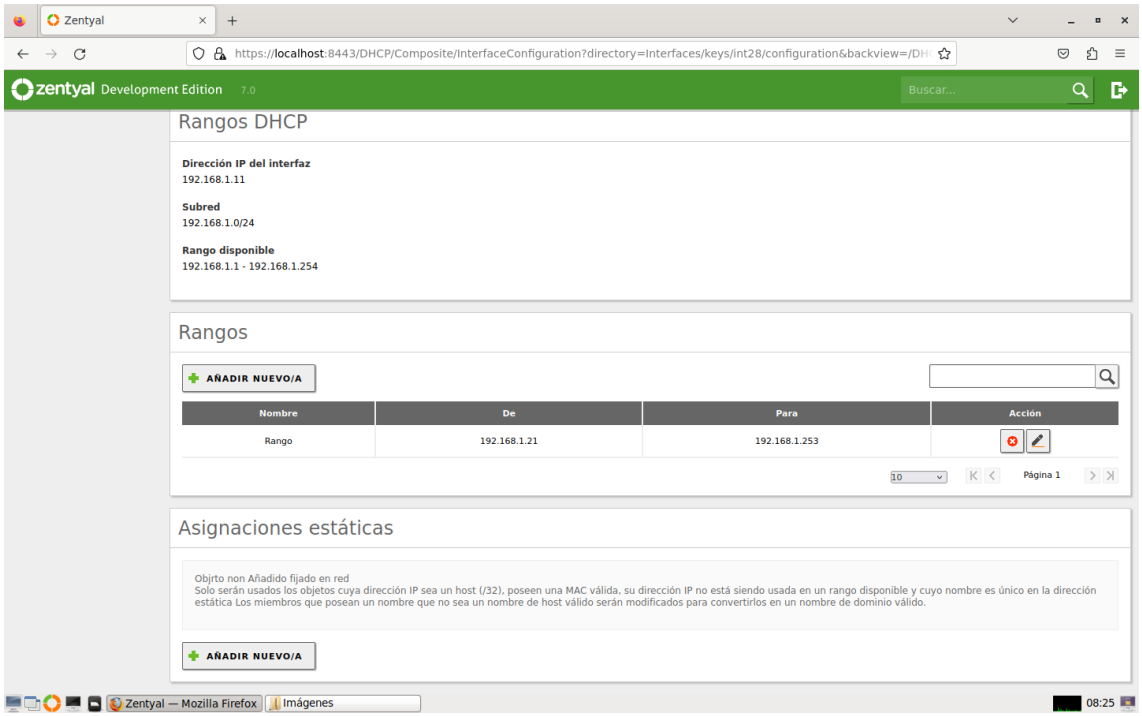


Ilustración 42. Rango disponible para el DHCP implementado.

Asimismo, se puede añadir un DNS dinámico, aunque en este caso no interesaba por lo que no se ha añadido dicha opción.

Finalmente, dentro de las opciones avanzadas se añaden los tiempos de asignación, los cuales se han dejado con los valores predeterminados que van desde 1800 segundos a 7200. Una vez expirado este tiempo se tiene que pedir la renovación para que el servicio proporcione otra dirección IP.

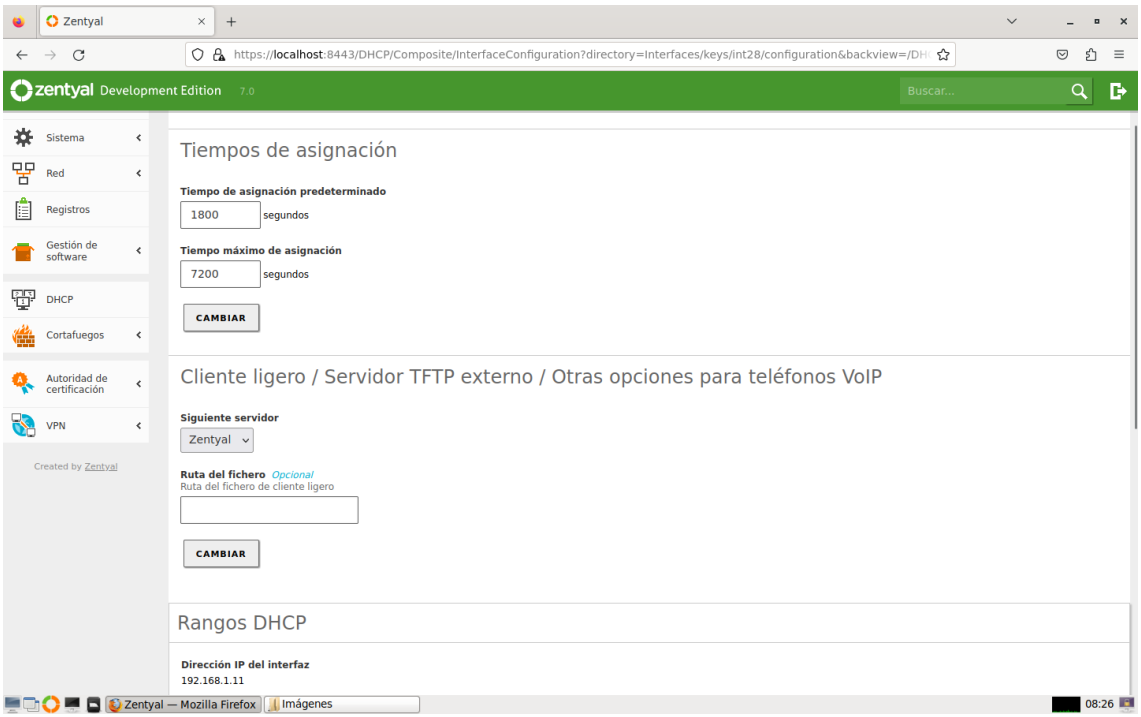


Ilustración 43. Tiempos de asignación del DCHP.

3.4.9. VPN y Autoridad de certificación

Por último, los dos últimos servicios que se han configurado son el certificado de autoridad y la VPN. El primero es necesario para que el segundo funcione correctamente.

Lo primero es habilitar el servicio de autoridad de certificado, el cual crea automáticamente el primer certificado, que es el certificado que da permiso como

autoridad para poder crear otros que ya sean utilizados por distintos servicios. Para ello, se deben de introducir un nombre de certificado y una fecha de expiración. Tras esto, el resto de certificados deberán de tener la misma fecha límite.

Una vez el certificado haya sido creado, aparecerá en la lista de certificados, estando disponible para el administrador y el resto de módulos. A través de la lista de certificados podemos realizar distintas acciones con ellos como descargar las claves, revocar el certificado o renovarlo. Si se revoca se debe de especificar el motivo por el que se ha eliminado desde un desplegable con las distintas opciones.

A continuación, el resto de certificados que se observan en la siguiente imagen se crearán automáticamente al crear las diferentes VPN.

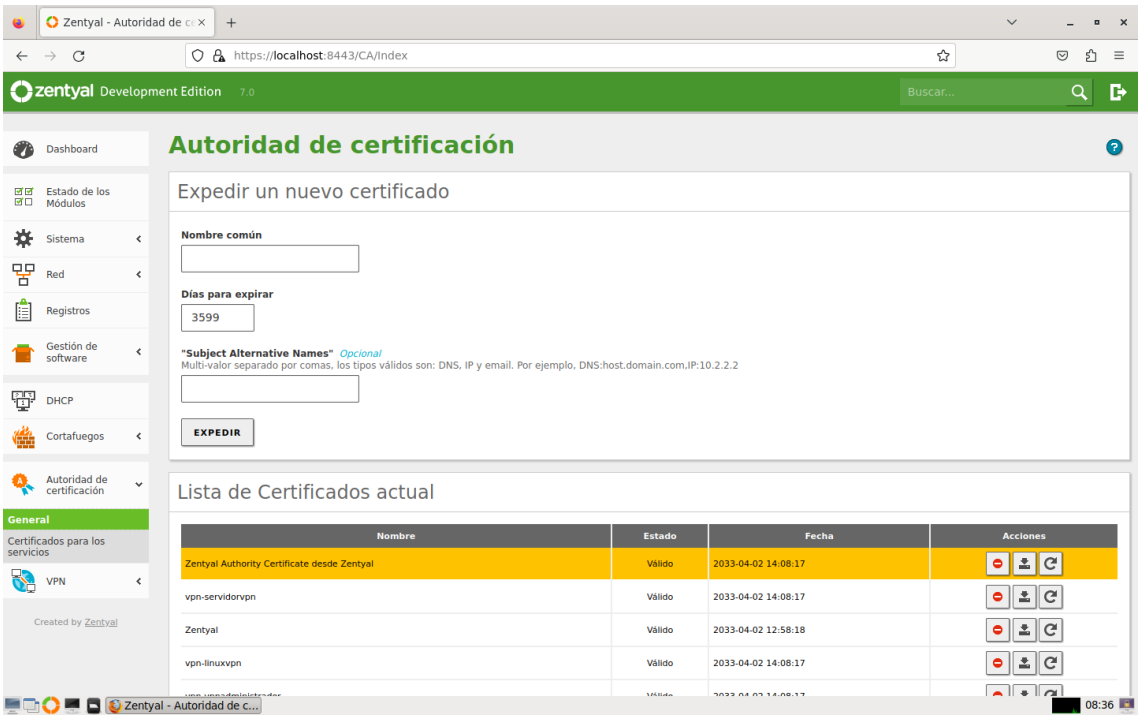


Ilustración 44. Lista de los Certificados de Autoridad creados.

En otros casos, también es necesario activar los certificados para los servicios, como en el caso de la administración web de Zentyal. En este caso, se debe de crear un

certificado especial para el servicio de administración web como se observa a continuación, y se debe dejar habilitado o no se podrá utilizar correctamente.

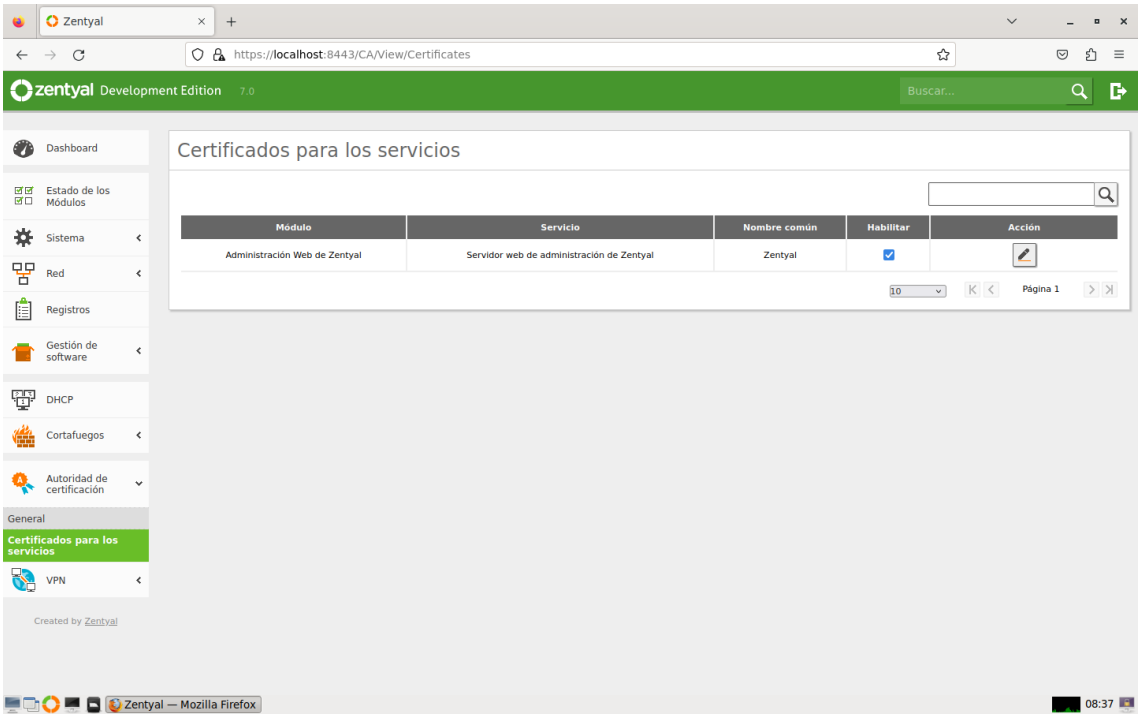


Ilustración 45. Lista de los Certificados necesarios para los servicios.

Una vez habilitado el servicio de autoridad de certificación, se pasa a configurar las distintas VPN que se utilizarán para poder satisfacer las necesidades del cliente. En este caso, se utiliza OpenVPN para configurar y gestionar las redes privadas virtuales. Se pueden añadir tantas VPN como se deseen, pero para explicar cómo funciona se va a hacer hincapié en el ejemplo de la VPN para clientes Windows de la empresa.

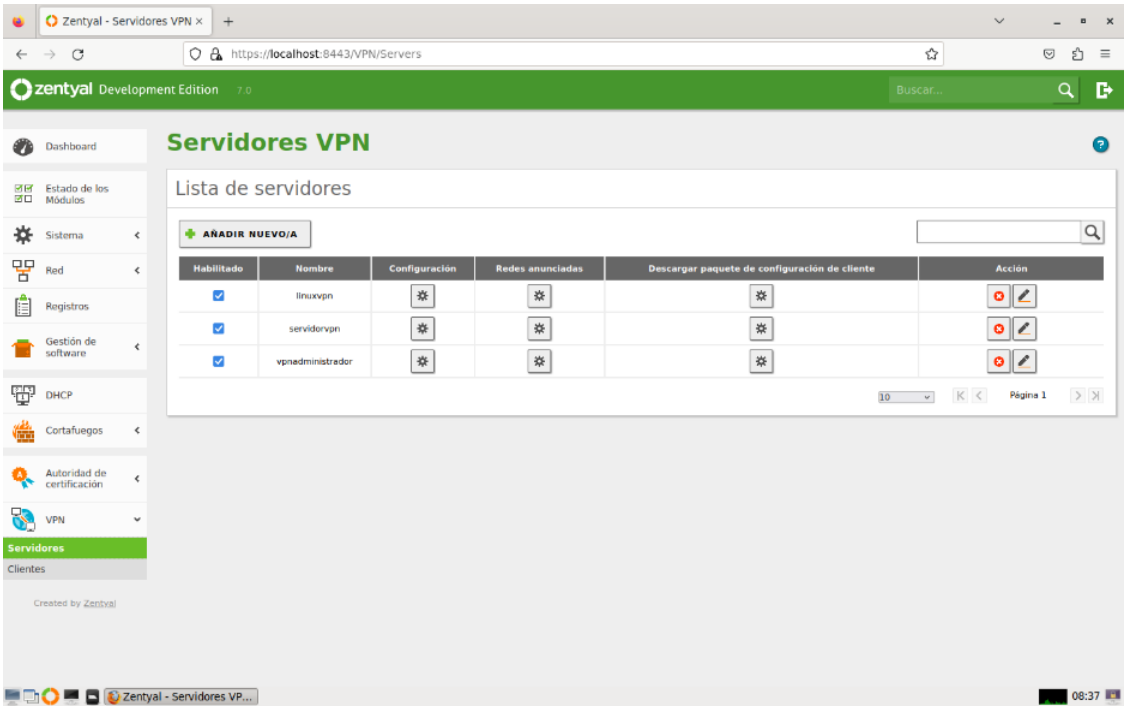


Ilustración 46. Lista de servidores VPN habilitados.

Para crear una VPN, lo primero es darle el nombre. Tras esto ya se puede entrar a configurar los distintos parámetros necesarios.

Lo primero será definir el tipo de protocolo y el puerto, que en nuestro caso serán protocolo UDP y puerto 1194 para esta VPN. Hay que tener claro que no se puede utilizar el mismo puerto para distintas VPN. Más adelante, se ha de definir la dirección IP que van a tener los dispositivos al conectarse a la VPN, que en este caso serán IPs que pertenecen a la red '192.168.160.0'. Además, se añade el certificado de autoridad que se acaba de crear, al crear la VPN. Por último, existen varias casillas para poder marcar, pero en este caso solo interesa activar la interfaz TUN (más semejante a un nodo de IP capa 3, y si no se activa se utiliza una de tipo TAP más semejante a un bridge de capa 2), la traducción de dirección de red NAT y redirigir la puerta de enlace para que todo el tráfico del cliente viaje a través de la VPN.

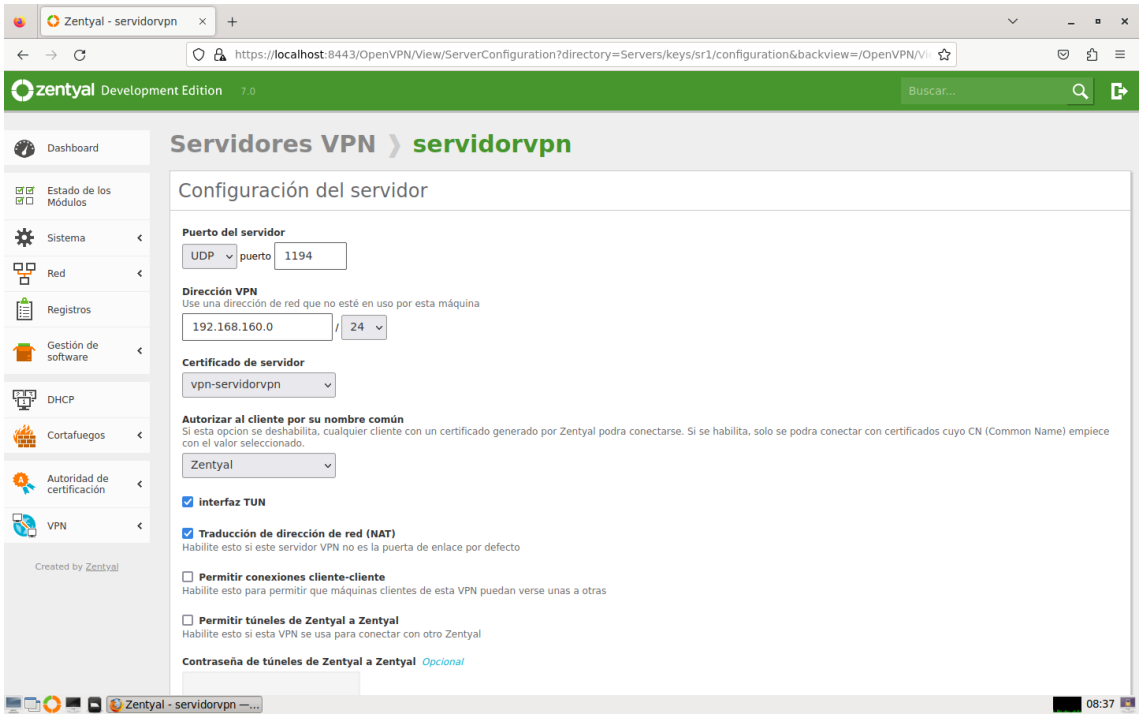


Ilustración 47. Configuración de un servidor VPN.

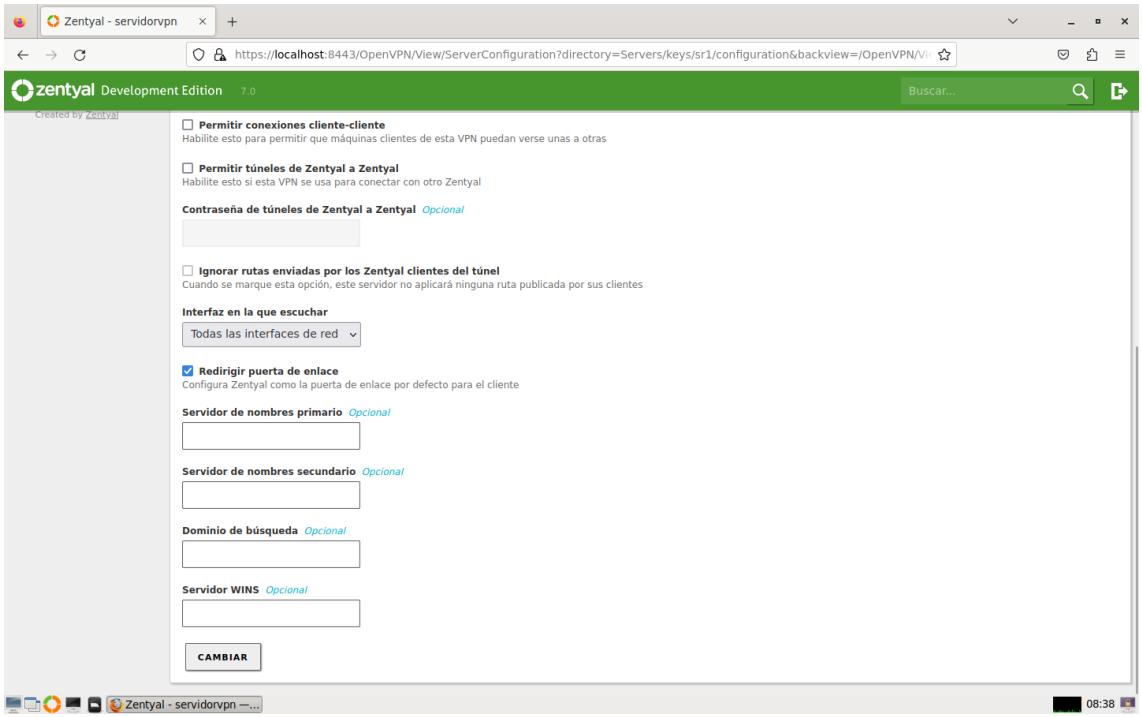


Ilustración 48. Más configuración del servidor VPN anterior.

A continuación, se deben de configurar las redes a las que se tiene acceso desde la VPN. En este caso, como es una VPN de administrador se le da acceso a todas las interfaces conocidas.

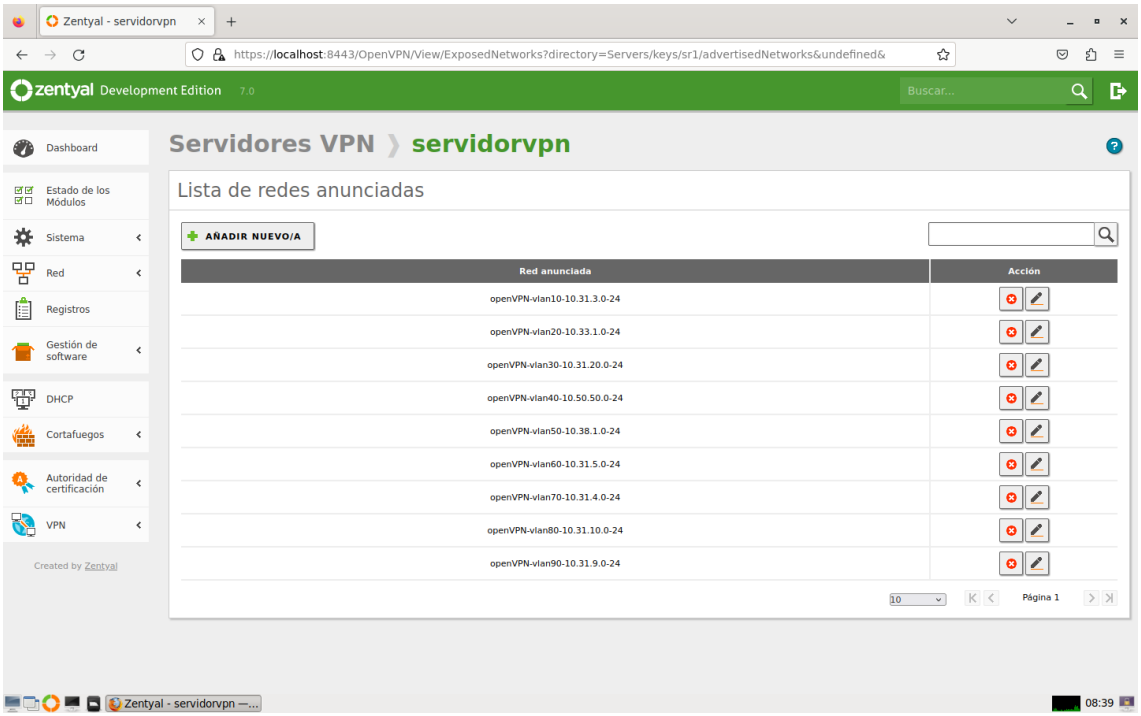


Ilustración 49. Lista de redes a las que se puede conectar mediante la VPN.

Finalmente, para poder establecer una conexión se debe de descargar la configuración del cliente para poder instalarla en el cliente. Para ello, se pide el tipo de cliente, que en este caso es Windows. A continuación se pide el certificado de la autoridad de certificación creado en primera instancia, y también la dirección IP del servidor, que es la IP pública. Con todo esto, ya se puede descargar la configuración e instalarla en el cliente para conectarse a través de una VPN.

La única diferencia que tiene un cliente Windows con un Linux al descargar la configuración, es que al cliente Windows se le puede incluir el instalador de OpenVPN y al Linux no.

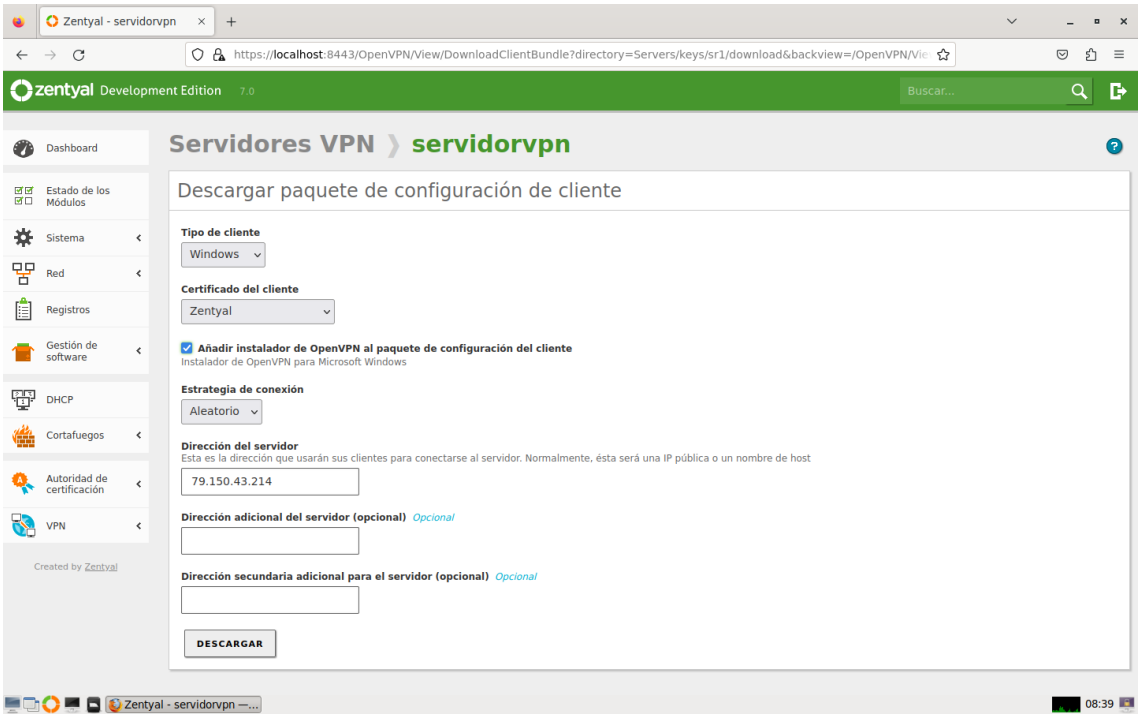


Ilustración 50. Descarga de la configuración del cliente de la VPN.

3.5. Diseño del entorno de prueba

Tras la configuración de todos los módulos que se encuentran en el software de Zentyal, se va a llevar a cabo el diseño del entorno que se va a utilizar finalmente para realizar las pruebas.

Para poder llevar a cabo dichas pruebas se van a necesitar distintos dispositivos, uno para el servidor y otros dos para comprobar la comunicación entre dos clientes distintos, además de un switch para administrar las VLANs.

Con todo esto, se van a realizar las pruebas para comprobar que se han configurado bien todos los módulos y que funcionan correctamente, cumpliendo con las expectativas propuestas por el cliente.

3.6. Resultados obtenidos

En primer lugar, para poder a empezar a obtener resultados, lo primero que se debe hacer es configurar el switch para administrar las distintas VLANs. Para ello, se reseteará el switch para dejarlo de fábrica, y una vez reseteado se accederá con las credenciales predeterminadas para poder configurarlo como se desee.

En este caso, los primeros cuatro puertos se dejarán para acceder como administrador al switch y poder cambiar la configuración en cualquier momento, y el resto se utilizan para definir las VLANs. Como todas las VLANs se han configurado igual, solo se van a realizar pruebas con aquellas que son más utilizadas como la VLAN de equipos, la de impresoras, la de servidores…

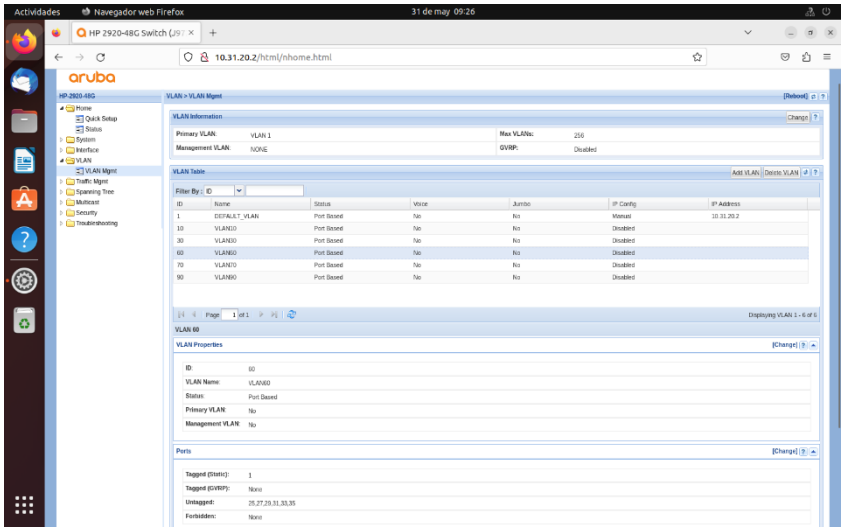


Ilustración 51. Configuración del Switch para administrar las VLANs creadas.

A continuación, se configuran los puertos del router para poder establecer las conexiones VPN. Por lo tanto, se accede al router con las credenciales del cliente y se modifican los puertos necesarios para aceptar las conexiones virtuales.

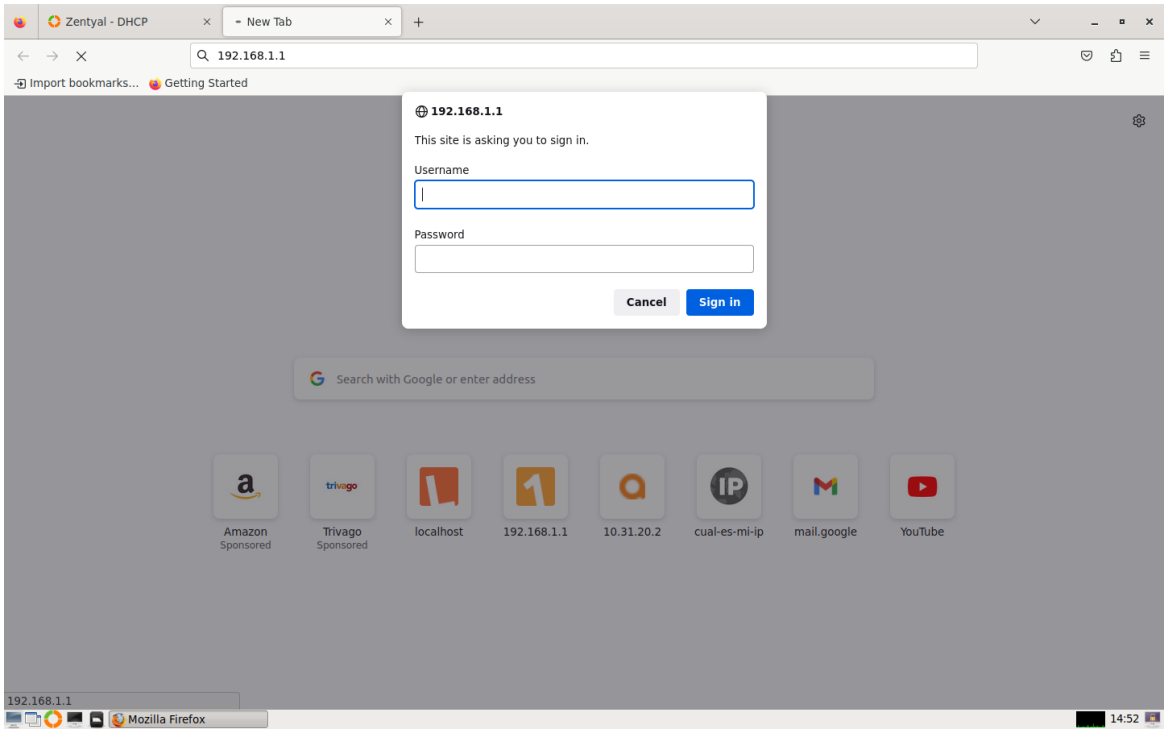


Ilustración 52. Credenciales de acceso al router.

Una vez introducidas las credenciales, se van a dejar abiertos los mismos puertos que se han configurado previamente en el módulo VPN del servidor de Zentyal. En este caso, se dejan abiertos los puertos ‘1194’ y ‘11194’ que se utilizan para establecer las conexiones VPN, y el puerto ‘8443’ para poder administrar el servidor vía web.

Además, se ha deshabilitado la función de asignar IPs dinámicamente a través del DHCP, para que este servicio sea proporcionado por el propio servidor.

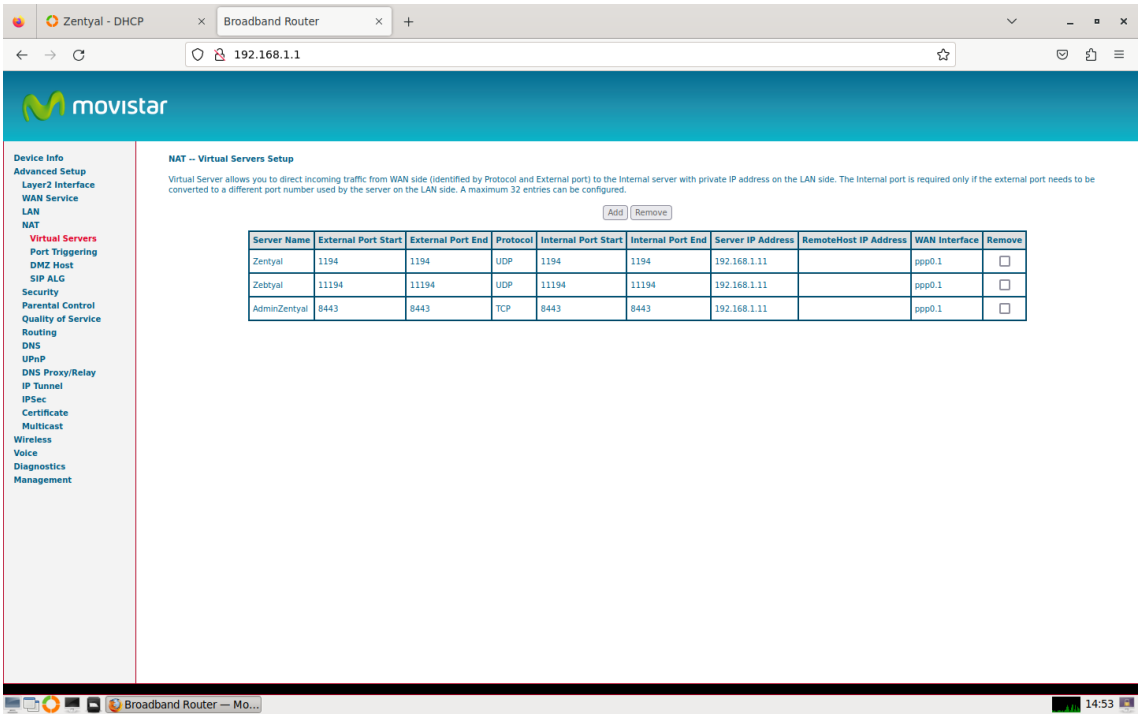


Ilustración 53. Puertos habilitados en el router para establecer las conexiones vía VPN.

Una vez realizadas estas configuraciones, se va a llevar a cabo la realización de distintas pruebas para comprobar que todo el sistema funciona correctamente.

En primer lugar, desde el propio servidor, se van a lanzar pings a las distintas interfaces y VLANs, para comprobar que todo el tráfico pasa por el servidor, ya que, este se va a utilizar como firewall y debe de aceptar o denegar el tráfico.

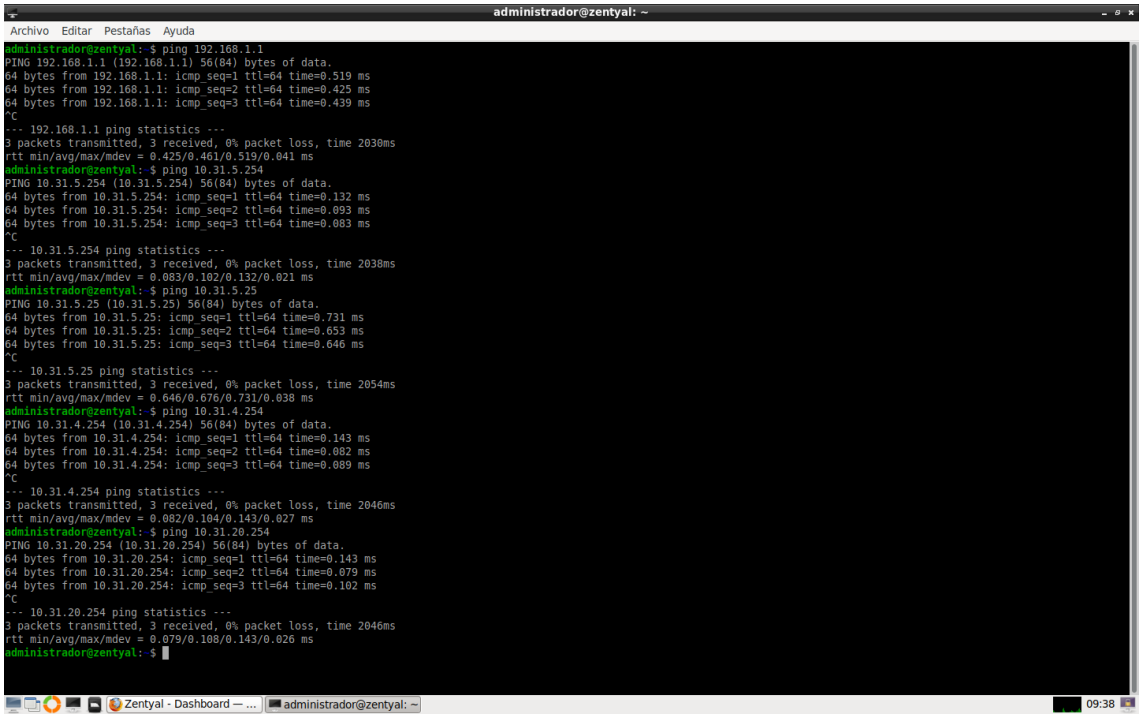


Ilustración 54. Pruebas de comunicación desde el propio servidor.

Más adelante, tras comprobar que el servidor puede establecer conexión en cualquier interfaz, se va a comprobar que los dos clientes solo puedan establecer conexiones dentro de las VLANs en las que se encuentren y no puedan detectar dispositivos de otras interfaces.

Para ello, desde un cliente Linux, con una IP ’10.31.5.25’, se comprueba que tenga acceso tanto a su propia puerta de enlace ‘10.31.5.254’, como a la puerta de enlace del servidor ‘192.168.1.1’ y también al router ‘192.168.1.11’. Tras estas comprobaciones, se hace ping a un servidor y a una impresora, con IPs ’10.31.20.2’ y ’10.31.4.221’ respectivamente, y se observa que no se puede acceder a dichas direcciones desde el cliente Linux. Con esto, se comprueba que tanto las VLANs definidas, como el funcionamiento del firewall, es correcto y deniega el tráfico entre distintas VLANs.

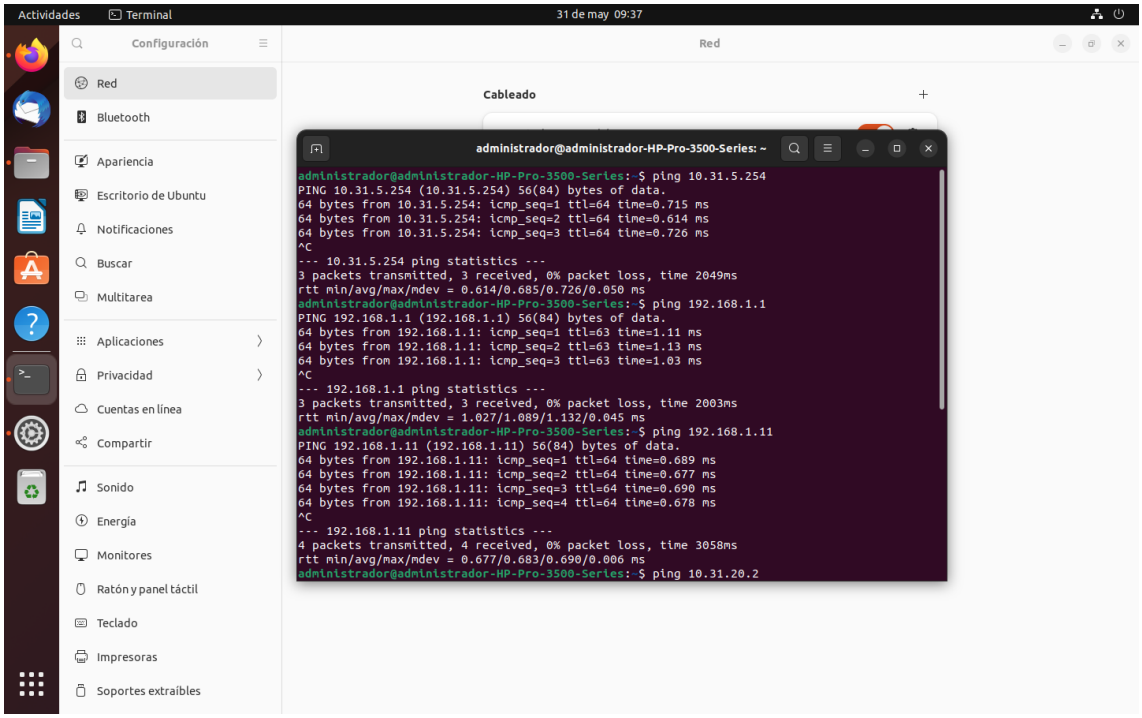


Ilustración 55. Prueba 1 de comunicación desde el cliente Linux.

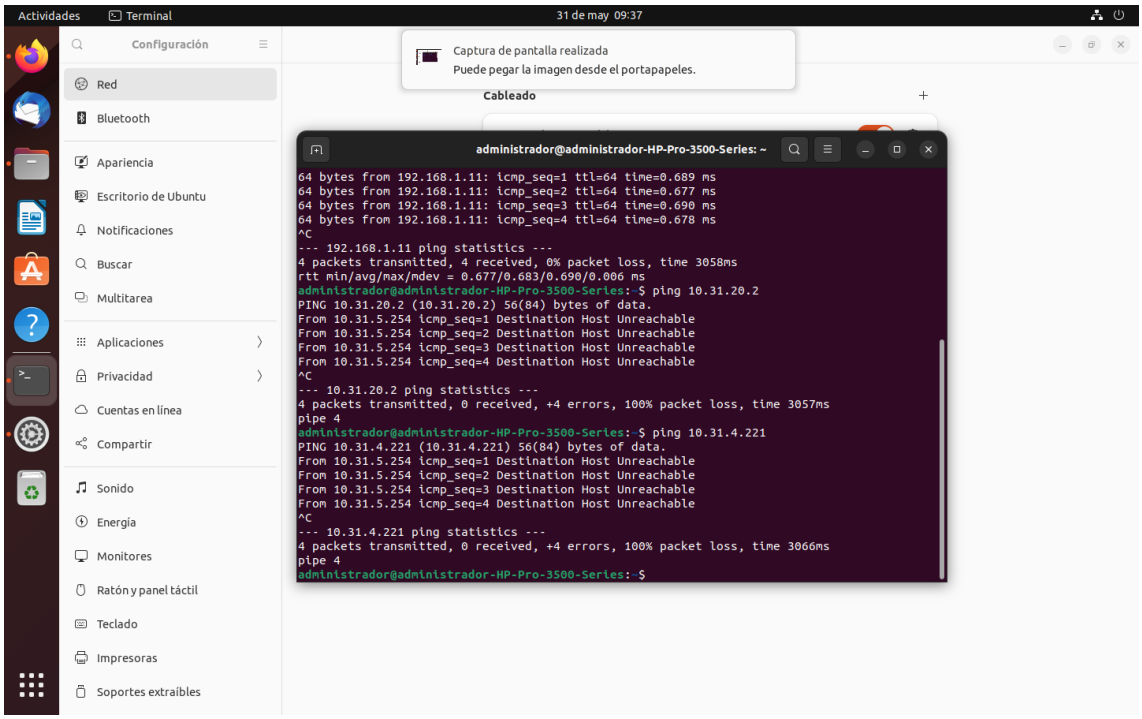


Ilustración 56. Prueba 2 de comunicación desde el cliente Linux.

Y para observar que entre dispositivos dentro de la misma VLAN sí que hay respuesta, se ha cogido el otro cliente, en este caso Windows, y se ha definido una dirección IP dentro del mismo rango ’10.31.5.22’ y se ha lanzado un ping contra el cliente Linux, observando que en este caso al pertenecer a la misma VLAN sí que se obtiene una respuesta.

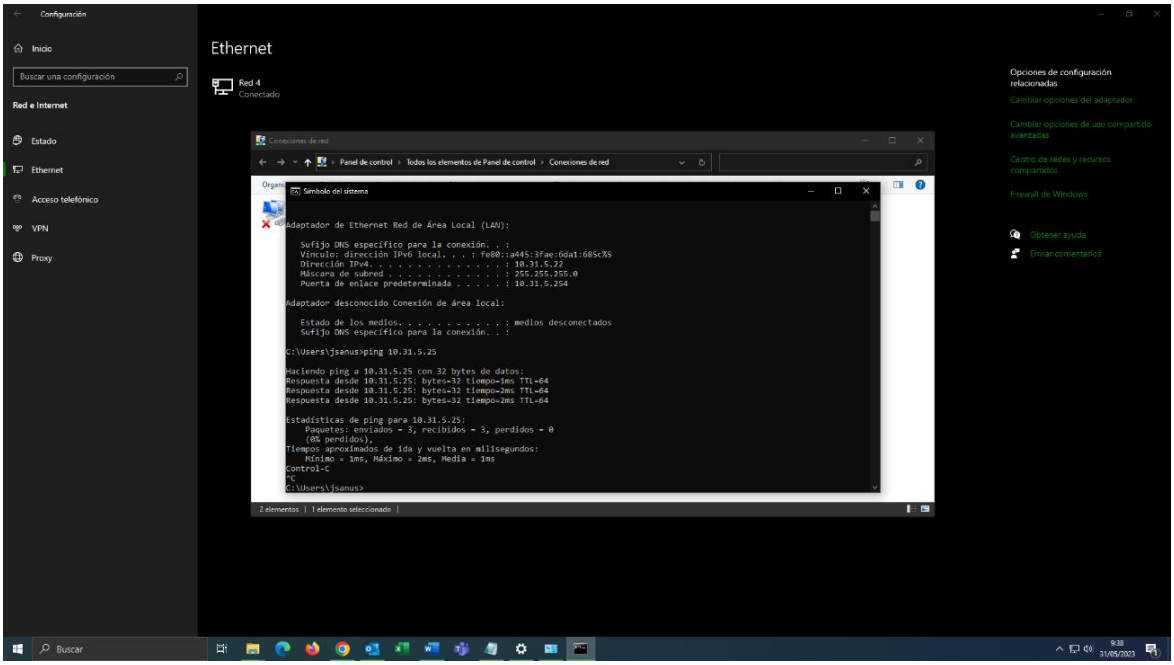


Ilustración 57. Prueba de comunicación desde el cliente Windows.

Tras comprobar que todas las VLANs funcionan correctamente, se ha colocado el cliente Windows en una red diferente al del servidor para comprobar que el módulo de la VPN funciona correctamente.

Para ello se ha tenido que instalar OpenVPN (en Linux no hace falta instalarlo), y tras la instalación, se deben de colocar los certificados y las claves descargadas previamente en la configuración de la VPN, en el directorio correspondiente. Una vez incluidos estos archivos, ya se puede arrancar OpenVPN, y se observa como el cliente establece una conexión con el servidor y le proporciona una IP dentro del rango ‘192.160.1.x’.

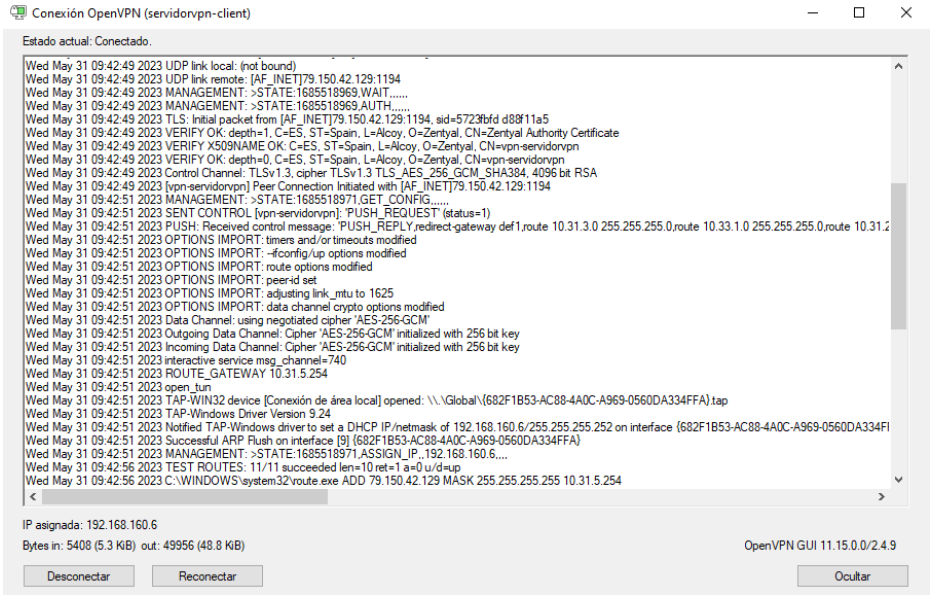


Ilustración 58. Establecer conexión VPN a través de OpenVPN.

Tras establecer la conexión, se puede acceder al Dashboard del servidor para observar que el servidor VPN se está ejecutando. Asimismo, también muestra la dirección IP que se le ha proporcionado y el momento desde el cual lleva conectado. Esto se utiliza por si hay una conexión no deseada para poder bloquearla y que no se vuelva a conectar.

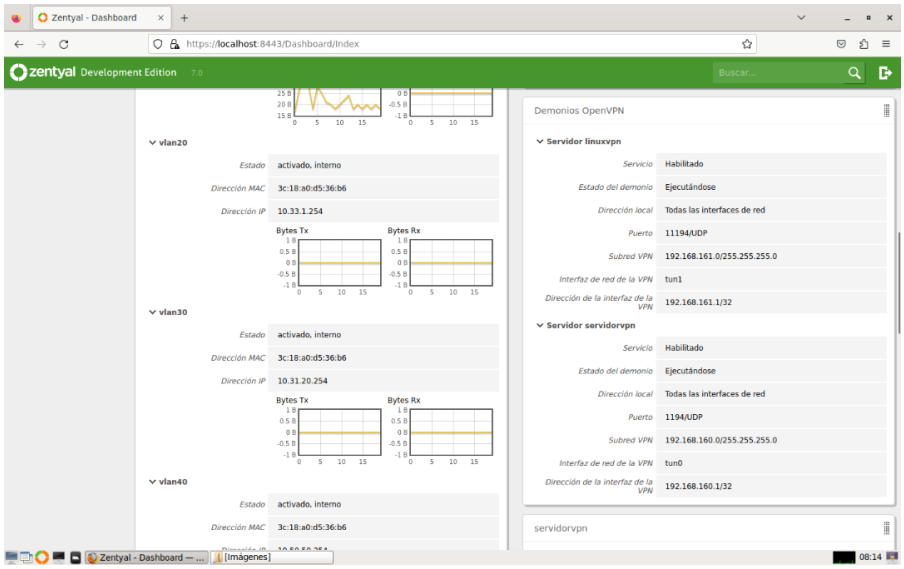


Ilustración 59. Vista desde el Dashboard del servidor de la VPN desplegada.

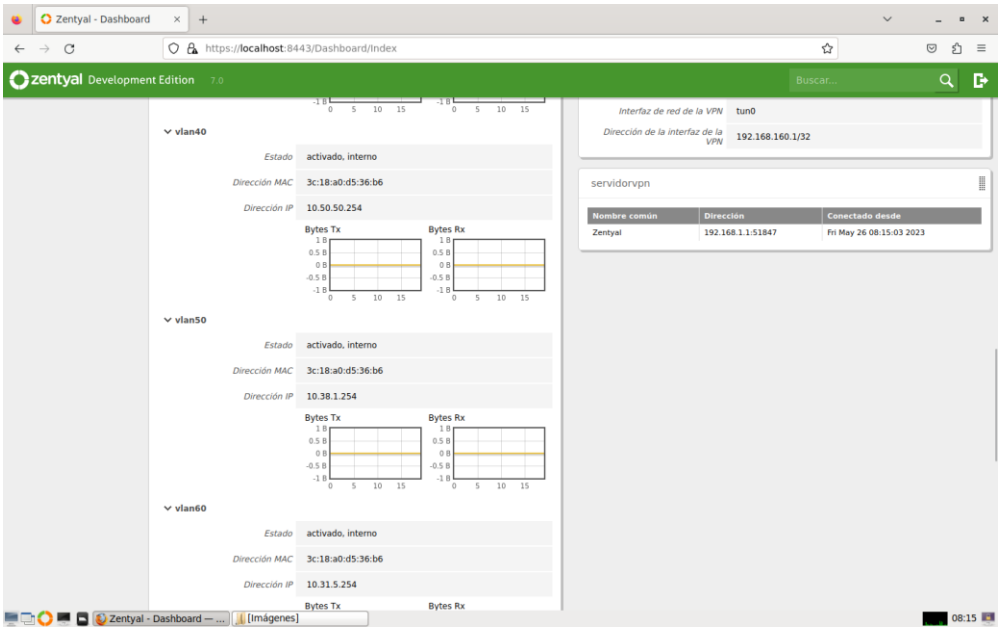


Ilustración 60. Vista del Dashboard del cliente conectado a través de la VPN.

Una vez conectado vía VPN, se puede acceder a la administración web desde el cliente definiendo el puerto que hemos habilitado previamente, donde se piden las credenciales para poder entrar y poder configurar los módulos desde fuera del servidor.

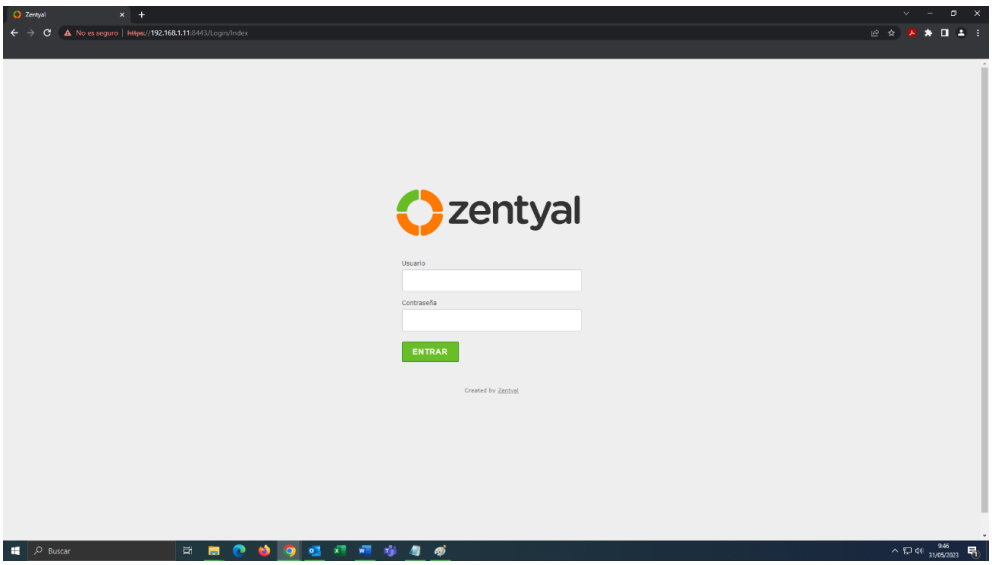


Ilustración 61. Acceso administración vía web desde el cliente conectado a través de la VPN.

Finalmente, una vez introducidas las credenciales, se observan las mismas funciones que en el servidor principal. Se puede observar como gestiona direcciones IP a través del módulo DHCP, el tráfico que manejan las distintas interfaces de red…

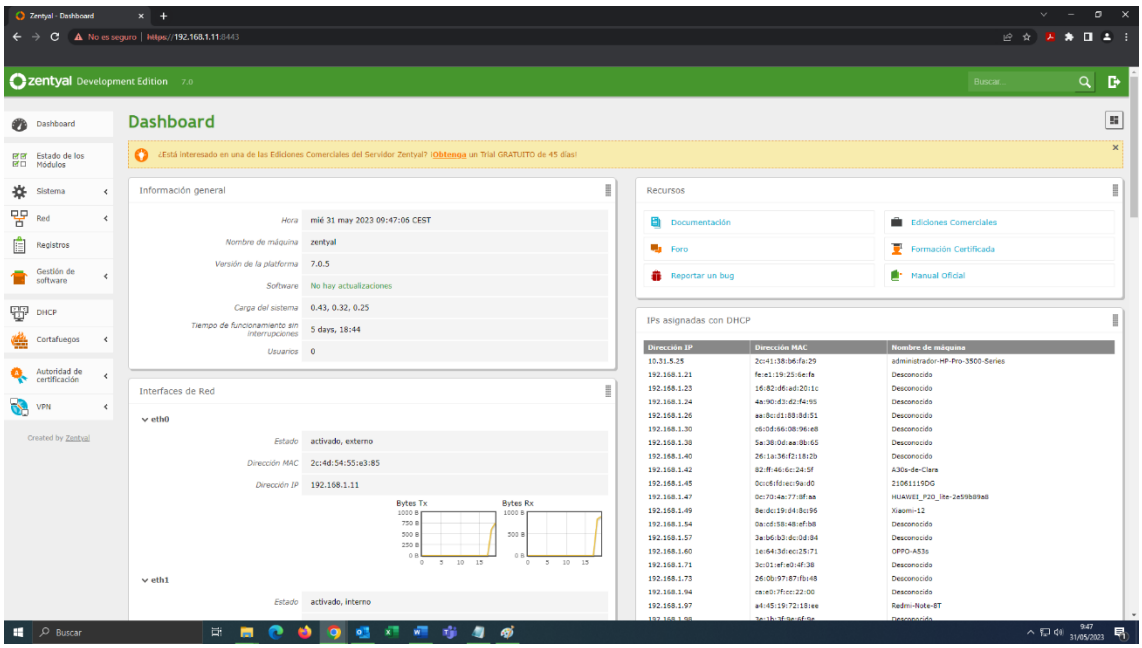


Ilustración 62. Vista del Dashboard desde el cliente conectado vía VPN.

Ambas VPN siguen el mismo proceso para conectarse, la única diferencia es que en la VPN del cliente Linux, el rango de direcciones IP es '192.161.1.X'.

Por último, todas las reglas aplicadas en el firewall funcionan correctamente como se ha observado al permitir o denegar los paquetes que se transfieren, por lo que, definitivamente, este sistema de réplica está capacitado para sustituir al sistema crítico principal en caso de avería.

4. CONCLUSIONES

Para finalizar el proyecto, se ha visto como se ha desarrollado y documentado una solución, mediante todos los medios disponibles en Korott SL y utilizando el menor presupuesto posible, implantando así un sistema de la gestión de la seguridad de la red, que pueda reemplazar al sistema principal en cualquier momento.

Para llegar a cumplir con el objetivo principal y cumplir con las expectativas del cliente, se han seguido una serie de pasos, empezando por la búsqueda exhaustiva de un software que nos permita cumplir con el objetivo, que en este caso ha sido Zentyal, que además, ha permitido reducir los costes, al tratarse de un software de código abierto.

Una vez encontrado dicho software, a continuación, se ha dado a conocer como se configuran sus distintos módulos que permiten llevar a cabo el objetivo final.

Teniendo claro cuál era el objetivo, se ha llevado a cabo con la implantación de los distintos módulos que se han explicado con anterioridad, ya que, son aquellos que han permitido replicar el sistema principal de forma óptima, para que en el momento de reemplazarlo funcione sin problemas.

Para finalizar, tras las pruebas, se observa que el funcionamiento del sistema es el deseado por lo que ha sido un éxito tanto su configuración como la puesta en marcha del servidor Zentyal en el sistema principal.

Además, al utilizar una aplicación 'OpenSource' ha permitido que el proyecto se ajuste al presupuesto principal, sin tener que ampliarlo como ocurre en muchos otros proyectos ya que es uno de los principales motivos por los que no se cumplen muchos proyectos.

En resumen, la implantación del sistema de gestión de la seguridad de la red ha sido un éxito al replicar el sistema crítico principal de forma óptima, y no provocar errores en las pruebas de implantación del servidor.

5. BIBLIOGRAFÍA

Artica. (Marzo de 2023). Obtenido de https://artica-proxy.es/caracteristicas/

ClearOS. (Marzo de 2023). Obtenido de https://www.clearos.com/products/clearos-editions/clearos-7-business#descripci%C3%B3n-general

Documentación Zentyal. (Abril de 2023). Obtenido de https://doc.zentyal.org/es/

Endian. (Marzo de 2023). Obtenido de https://www.endian.com/

Gaibor, J. L. (2016). *Pontifica Universidad Católica del Ecuador.* Obtenido de Repositorio de Grado y Posgrado: http://repositorio.puce.edu.ec/handle/22000/13689

Jiménez, A. H. (Diciembre de 2016). *Universitat Oberta de Catalunya.* Obtenido de https://openaccess.uoc.edu/handle/10609/58645

NethServer. (Marzo de 2023). Obtenido de https://www.nethserver.org/learn-more/

OPNsense. (Marzo de 2023). Obtenido de https://opnsense.org/about/features/

Zentyal. (Marzo de 2023). Obtenido de https://zentyal.com/features/

6. ANEXO I: GLOSARIO

A continuación, se van a definir una serie de términos que aparecen a lo largo del proyecto, siendo de gran importancia que se entiendan con claridad. Los términos son los siguientes:

- Firewall. También conocido como cortafuegos, es el encargado de permitir o denegar el tráfico de la red entrante, saliente o dentro de una red privada, es decir, es el encargado de la seguridad del sistema. Funciona a través de reglas que se encargan de tomar las decisiones de los paquetes de datos de forma selectiva. Se pueden implementar en hardware, software o combinando ambos.
- VLANs. Conocido por sus siglas como "Virtual Local Area Network", es el conjunto de equipos y periféricos agrupados en un solo dominio de difusión, sin importar su ubicación física, permitiendo así que los dispositivos se agrupen por los servicios que realiza en lugar de por proximidad. Resumiendo, es un método para crear redes lógicas independientes en la misma red física.
- Enrutamiento. Más conocido como "Routing", tiene la finalidad de mover paquetes entre dispositivos a través de la red, es decir, trata de buscar el mejor camino entre las distintas posibilidades dentro de una red entre distintos dispositivos que mantienen una gran conectividad.
- DNS. El "Domain Name System" es un sistema de nomenclatura, utilizado por dispositivos conectados a una red privada o a Internet, que se encarga de traducir los nombres de dominio a direcciones IP ("Internet Protocol") para que los navegadores sean capaces de enrutar los distintos paquetes en Internet.
- DHCP. También conocido como "Dynamic Host Configuration Protocol", es un protocolo que se encarga de asignar automática y dinámicamente una dirección IP a un dispositivo, tanto para una red privada, desde el router hacia los equipos de la red local, como para asignar una IP pública para poder establecer una conexión a través de Internet. Utiliza una arquitectura cliente-servidor, siendo el DHCP el servidor encargado de proveer un servicio, y los clientes, los dispositivos, que son los que encargan dicho servicio, en este caso una IP, tanto privada como pública, para poder comunicarse en la red.

- VPN. Son las siglas de “Virtual Private Network”. Esta red virtual, permite crear una red local sin la necesidad de que sus miembros se encuentren físicamente conectados, sino que se conectan a través de Internet. Además, proporciona algunas ventajas como una mayor flexibilidad y la utilización de túneles de datos, que redirige todo el tráfico de red desde el dispositivo y el proveedor de Internet hacia el servidor VPN, desde donde se enviará a su destino.
- Failover. Se encarga de comprobar la integridad de la conexión de la red principal, y en caso de que la calidad de conexión sea baja o se produzca algún error, redirige todo el tráfico por la conexión secundaria, evitando así la inestabilidad de la red principal y permitiendo que se siga trabajando con normalidad. Es decir, se trata de un respaldo de seguridad que permite la redundancia en la red, asegurando la supervivencia de la conexión al proporcionar una ruta alternativa. Puede tratarse de una redundancia activa, si ambas redes están disponibles al mismo tiempo, o pasiva, si una red está activa y la otra se encuentra en “modo de espera”.
- ISP. Por sus siglas “Internet Service Provider”, se trata del proveedor que suministra conexión a Internet a los clientes, conectando a estos a través de distintas tecnologías ADSL, fibra óptica, satélite…