

Optimización de los recursos de red de una organización mediante el uso de un servidor dedicado basado en software libre

Memoria

Víctor Martín Goyeneche

UOC -2012-

Tabla de contenido

| | |
|--|-----------|
| 1. Planificación | 5 |
| 1- Introducción..... | 5 |
| 2. Optimización de los recursos de red de una organización..... | 6 |
| 3. Objetivos y alcance del proyecto | 8 |
| 4. Planificación | 8 |
| <i>Entregables</i> | <i>8</i> |
| <i>Calendario de trabajo.....</i> | <i>9</i> |
| <i>Planificación temporal.....</i> | <i>10</i> |
| 5 Material..... | 12 |
| 5.1 Material hardware | 12 |
| 5.2 Material software..... | 12 |
| 6. Plan de contingencia | 12 |
| 6.1 Dificultad a la hora de lograr un entorno de pruebas adecuado..... | 12 |
| 6.2 Contingencias temporales..... | 12 |
| 6.3 Dificultades con la herramienta | 13 |
| Análisis De Requisitos | 14 |
| Estudio de situación inicial..... | 14 |
| 2. Identificación de necesidades | 15 |
| 3. Solución propuesta para la realización de pruebas..... | 16 |
| 4. Desarrollo de las pruebas | 18 |
| 4.1 Configuración del entorno de pruebas..... | 18 |
| 4.2 Balanceo de carga | 29 |
| 4.3 Cache de DNS | 31 |
| 4.4 Filtrado de paquetes..... | 32 |
| 4.6 Cache de contenidos..... | 35 |
| 4.7 Calidad de servicio (QoS)..... | 37 |
| 4.8 Síntesis de resultados | 41 |
| Solución propuesta | 42 |
| 1 Estructura de red..... | 42 |
| 1.1 Tipos de comunicaciones en la organización | 42 |
| 1.2 Comunicaciones con los servicios corporativos | 42 |
| Comunicaciones con otras sedes..... | 43 |
| 1.4 Comunicaciones con el exterior de la organización..... | 44 |
| 1.5 Comunicaciones desde el exterior hacia el interior de la organización..... | 45 |
| 1.6 Diagrama de red de la organización..... | 46 |
| 2 Requisitos de hardware y comunicaciones..... | 47 |
| 2.1 Requisitos de comunicaciones de la sede periférica. | 48 |
| 2.2 Requisitos de comunicaciones de la sede central..... | 48 |
| 2.3 Requisitos de hardware de los servidores Zentyal..... | 48 |
| 3 Configuración propuesta de Zentyal..... | 49 |
| 3.1 Configuración del servidor Zentyal de las sedes..... | 49 |

| | |
|--|-----------|
| <i>3.2 Configuración del servidor Zentyal interno de la sede central</i> | <i>52</i> |
| <i>3.3 Configuración del servidor Zentyal externo de la sede central.....</i> | <i>54</i> |
| Presupuesto estimado | 57 |
| 1 Presupuesto hardware..... | 57 |
| 2 Presupuesto licencias de software y mantenimiento..... | 57 |
| Conclusiones..... | 59 |
| Bibliografía | 60 |
| Índice de figuras | 61 |

Agradecimientos

A Teresa, contigo todo se puede lograr.

1. Planificación

1- Introducción

El presente documento describe la planificación que seguiré a lo largo de la realización del Proyecto Fin de Carrera (en adelante PFC) titulado “Optimización de los recursos de red de una organización mediante el uso de un servidor dedicado basado en software libre”.

Al principio del documento se definirá más detalladamente el contenido del proyecto, los objetivos que se pretenden lograr así como las competencias que se habrán adquirido a su finalización.

A continuación se describirán todas las tareas que se deben llevar a lo largo del PFC, enumerándolas y agrupándolas de forma lógica y se establecerá un calendario de entregas que deberá cumplirse para poder llevarse a cabo el seguimiento del proyecto.

Más tarde se ordenarán las tareas de forma temporal mediante un diagrama de Gantt donde se representarán los hitos importantes así como las dependencias existentes entre ellos. Se reflejarán en él los tiempos que estimados para la realización de cada una de las tareas

2. Optimización de los recursos de red de una organización

En la actualidad el uso de las nuevas tecnologías ha hecho del ancho de banda de las organizaciones un bien muy preciado. Su consumo aumenta considerablemente a lo largo de los años, las organizaciones aprovechan la velocidad de las comunicaciones para establecer sedes en diferentes puntos del planeta manteniendo la gestión del mismo modo que harían si esas personas estuvieran en el mismo edificio. Los contenidos audiovisuales y las redes 2.0 han convertido la Web en algo dinámico y en un recurso imprescindible en todos los ámbitos de actuación, desde las altas finanzas hasta la educación.

Por otra parte el coste de los equipos informáticos ha bajado drásticamente y su potencial ha aumentado del mismo modo. Si antes podía ser impensable que una pequeña organización contara con un servidor dedicado a tareas de optimización de las comunicaciones, actualmente ese coste puede ser asumido fácilmente y rentabilizado en muy poco tiempo bien porque no requieran contratar más ancho de banda al proveedor de servicio o bien porque la diferencia de servicio que son capaces de obtener merece esa inversión.

Por último el software libre ha evolucionado en gran medida en los últimos años principalmente en el ámbito de la usabilidad, que era uno de sus puntos más débiles. La aparición de distribuciones específicas para cada tipo de tarea ha permitido que sea posible encontrar soluciones de software libre que se adapten fácilmente a las necesidades del cliente.

Este hecho se acentúa en el mundo de las redes de comunicaciones donde la cantidad de opciones que ofrece el software libre es inabarcable.

Para la elaboración de este proyecto, con el fin de que éste no sea un planteamiento teórico únicamente basaré la optimización en una empresa ficticia denominada OcupaUOC.

OcupaUOC proporciona servicios de colocación y formación a desempleados, con sedes en diferentes ciudades de España. Cada una de ellas cuenta con usuarios de secretaría y usuarios de formación. Cuentan en cada sede con varias conexiones de banda ancha, generalmente ADSL con accesos diferenciados para los usuarios de secretaría y para los usuarios de formación. Además cada sede tiene una línea de comunicación dedicada para las comunicaciones con la central que proporciona servicios corporativos mediante un servicio contratado de GigaADSL¹.

Basaré mi estudio en la distribución de software libre Zentyal² así como en las herramientas de red más utilizadas en Linux. Zentyal es una distribución Linux³ específica para la administración de políticas de red y gestión de tráfico. Estudiaré su funcionamiento y flexibilidad y realizaré la propuesta sobre su implantación y en su caso los puntos débiles que

¹ Para más información sobre GigaADSL : <http://es.wikipedia.org/wiki/GigADSL>

² Sitio web oficial del proyecto Zentyal: <http://www.zentyal.com>

³ Zentyal es una distribución Linux basada en Ubuntu

he encontrado y propondré una solución que mejore el uso del ancho de banda de la compañía.

3. Objetivos y alcance del proyecto

Con la elaboración de este proyecto se pretenden alcanzar los siguientes objetivos:

- Conocer las herramientas existentes en el software libre para realizar una optimización de recursos de red
- Conocer la herramienta Zentyal y las posibilidades y debilidades que plantea su uso
- Proponer una configuración óptima ante una situación general que podría ser de utilidad a la mayoría de pequeñas empresas españolas.

A lo largo del proyecto se desarrollarán las siguientes competencias:

- Capacidad de definir, planificar y gestionar un proyecto de ingeniería informática
- Capacidad de análisis de la situación así como de las diferentes herramientas de software
- Capacidad de síntesis y de resolución de problemas

Al final del proyecto se obtendrá una memoria final donde se emitirá una recomendación de configuración de red y de configuración del servidor de optimización del tráfico.

4. Planificación

En este apartado se definirán los entregables de los que constará el proyecto, se determinarán todas las tareas necesarias para llevar a cabo cada uno de ellos y se realizará la planificación temporal de cada una de estas tareas.

Entregables

Plan de trabajo – PEC1

Este documento define de forma genérica el proyecto que se va a realizar. Establece el título, una descripción general del proyecto, así como los objetivos y competencias que se van a desarrollar.

También define el plan de trabajo que servirá de base para el desarrollo del proyecto y establece como hitos o puntos de revisión cada uno de los entregables de los que consta el proyecto.

Por último define los medios técnicos que se utilizarán en el desarrollo del mismo, y una evaluación de los principales riesgos que amenazarán el proyecto así como las medidas correctivas que se llevarán a cabo en cada caso si éstos se produjeran.

Análisis y diseño – PEC2

Este documento es el resultado del análisis de los requisitos del cliente así como del estudio detallado de la herramienta Zentyal.

Se documentarán las pruebas y los resultados obtenidos de las utilidades más interesantes que ofrece la herramienta Zentyal.

Además se definirán los puntos débiles de la configuración de red del cliente así como de los cuellos de botella sobre los que se realizará la optimización

Memoria – PEC3

Este documento es la síntesis del trabajo realizado durante el desarrollo del proyecto.

En él se definirá la solución de red que se considera más óptima así como la configuración del servidor Zentyal más apropiada

Memoria Final

En esta entrega se presentará la memoria del proyecto, así como una presentación del mismo

Calendario de trabajo

La planificación de las tareas y actividades se ha realizado a través de un diagrama de Gantt. Se ha tomado como horario de trabajo en el proyecto el siguiente: De lunes a viernes de 20:30 a 23:30 y los sábados y domingos de 08:30 a 13:30

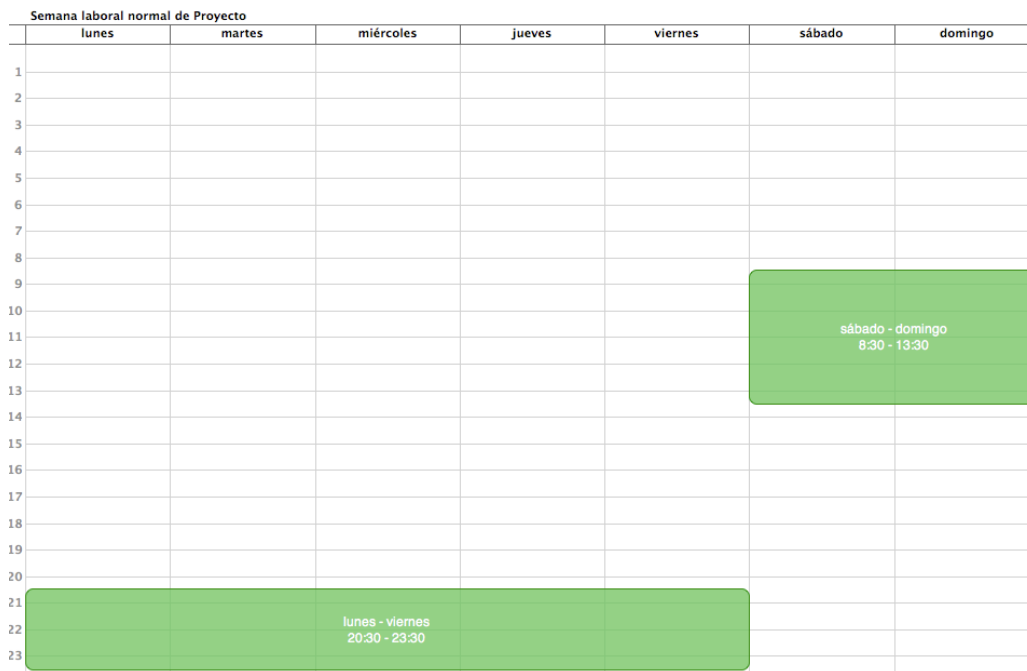


Figura 1. Planificación Temporal - Horario de trabajo-

Planificación temporal

La planificación temporal se ha llevado a cabo a través de un diagrama de Gantt en el que se muestran todas las subactividades que engloban la realización de cada uno de los entregables, el tiempo previsto que se va a dedicar a cada una de ellas así como la fecha prevista de realización.

Optimización de los recursos de red de una organización mediante el uso de un servidor dedicado basado en software libre

Víctor Martín Goyeneche – UOC -2012-

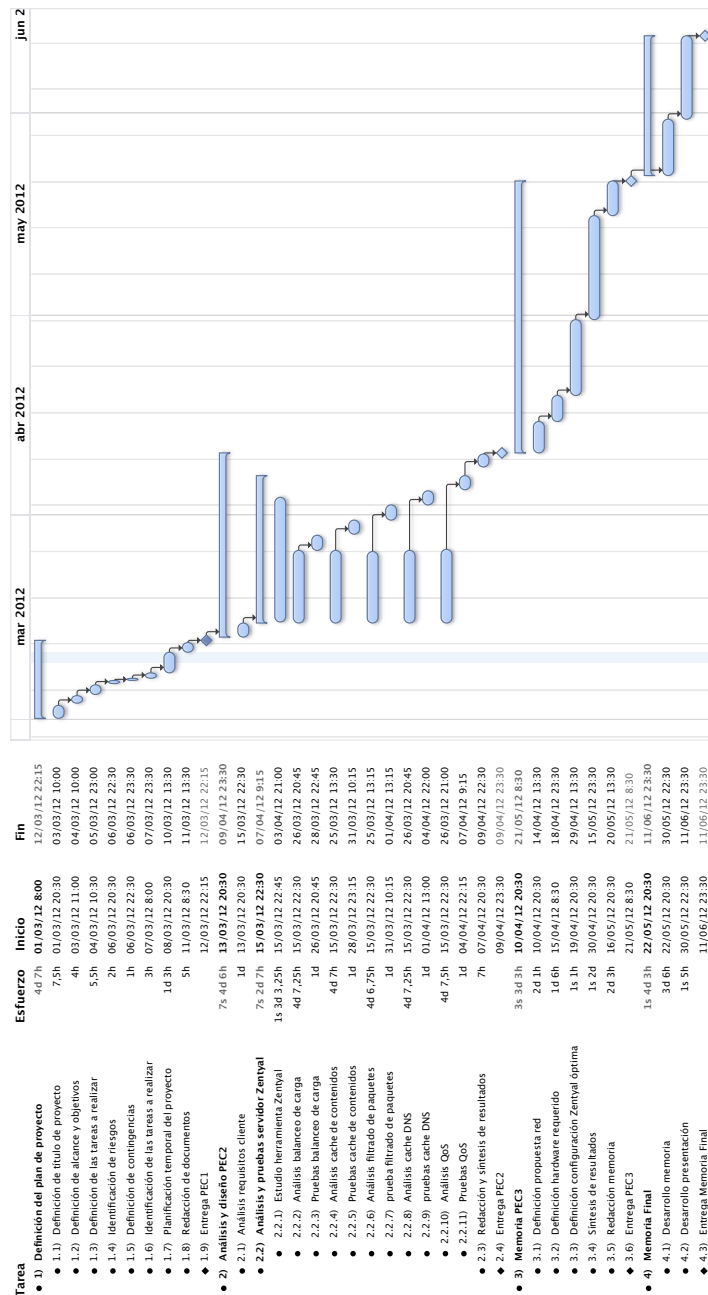


Figura 2. Planificación Temporal - Diagrama de Gantt-

5 Material

En este apartado se detallan los materiales hardware y software utilizados para la realización del proyecto

5.1 Material hardware

El material hardware del que se dispone es el siguiente:

- MacBook 13" Intel Core 2 Duo 2,4 GHz, 2GB de RAM con Mac Os X 10.4
- HP Compaq 7900 Intel Core 2 GHz 4GB de Ram con Windows XP

5.2 Material software

El material software que se utilizará será el siguiente:

- OmniPlan Project Management for osX
- Microsoft Office 2011 para Mac
- Microsoft Office 2003 para PC
- Oracle VirtualBox para Mac y para PC
- Distribución GNU/Linux Zentyal

6. Plan de contingencia

El proyecto contará con un plan de contingencias que será llevado a cabo en el caso de que se produzcan elementos que puedan alterar la planificación prevista.

6.1 Dificultad a la hora de lograr un entorno de pruebas adecuado

En el caso de que no fuera posible simular el comportamiento a través de la virtualización de máquinas se prevé montar un servidor Zentyal en un portátil y utilizar varios equipos que permitan realizar los respectivos análisis.

6.2 Contingencias temporales

Estas contingencias pueden ocurrir por diferentes motivos: Laborales, enfermedad o problemas con alguna entrega de otra asignatura. En estos casos se recuperaría el tiempo ampliando el horario de trabajo del fin de semana utilizando las tardes de 16:00 a 23:30 o hasta corregir la desviación.

6.3 Dificultades con la herramienta

Estas contingencias pueden ocurrir por problemas a la hora de configurar servicios proporcionados por Zentyal. Para tratar de evitar que se produzcan he adquirido el libro Zentyal para administradores de redes preparatorio para el examen de certificación ZeCA.

Además la empresa está ubicada en Zaragoza, lugar donde resido y realiza cursos de formación. Me pondría en contacto con ellos para bien a través de un curso o bien a través de soporte técnico me resolvieran las dudas en caso de necesitarlo.

Análisis De Requisitos

Estudio de situación inicial

La situación de la empresa OcupaUOC viene establecida por la evolución que ésta ha tenido a lo largo del tiempo, ya que las diferentes sedes se encuentran en diferente situación dependiendo de la inversión que se haya efectuado en actualización de las comunicaciones.

En un primer momento las sedes periféricas estaban conectadas directamente a la sede central a través de líneas Giga ADSL, servicio que proporcionaba una red privada a través de ADSL. La sede central tenía contratado una línea de banda ancha con la que daba servicio de Internet a todas las sedes al mismo tiempo que proporcionaba servicios propios como portales internos, correo electrónico o servicio de centralita IP.

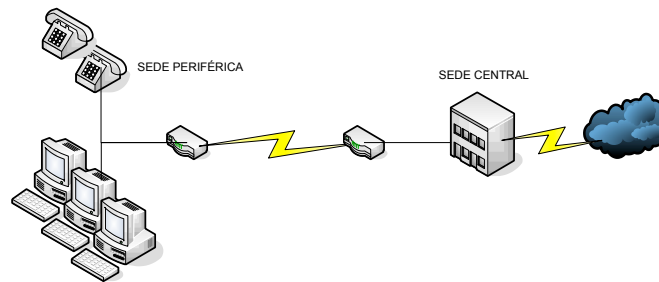


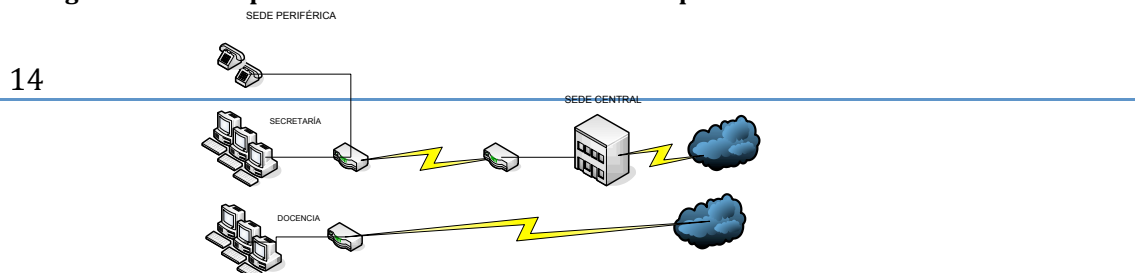
Figura 3. Situación Inicial con sede periférica

A medida que las sedes requirieron más ancho de banda de salida a Internet para la realización de cursos se producía un cuello de botella considerable, no sólo en el ADSL de salida sino también en la salida de banda ancha de la sede central. Las sedes más importantes optaron por contratar una nueva línea ADSL. Esta línea se dedicó al área docente.

Esta solución tenía las siguientes ventajas:

- Los alumnos accedían directamente a Internet sin necesidad de competir por el ancho de banda de salida con los usuarios administrativos
- Los usuarios administrativos notaban una mejora considerable en la conectividad con la sede central

Figura 4 Red OcupaUOC - Situación inicial con sedes periféricas -



Sin embargo tenía las siguientes deficiencias:

- Los alumnos no pueden aprovechar los recursos de la red interna salvo que éstos sean publicados en Internet
- La salida a Internet de los usuarios de secretaría es muy pobre ya que tiene que competir con los usuarios del resto de sedes.

Un grupo de sedes decidió aumentar el ancho de banda de salida a Internet contratando una nueva línea ADSL para su uso en Secretaría

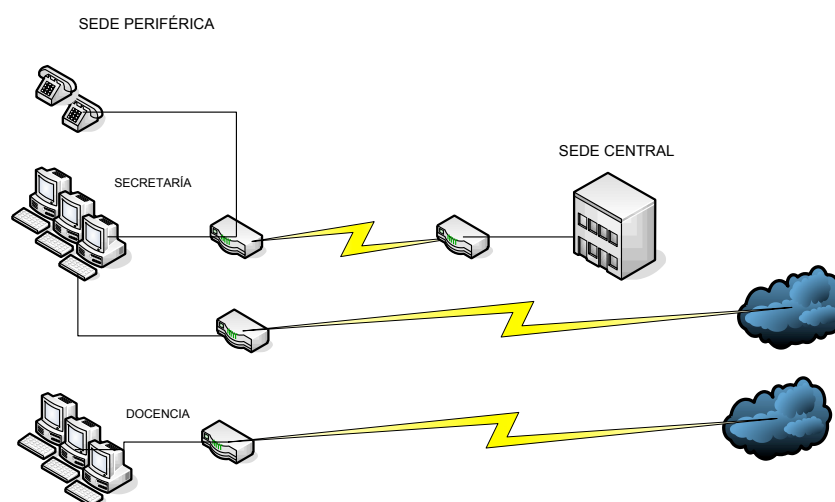


Figura 5. Aumento de conexiones de banda ancha en las sedes periféricas

Una de las consecuencias de la distribución de las líneas ADSL en subredes es que en ocasiones el ancho de banda pico supera el de un ADSL mientras que el resto se encuentran infrautilizados. Esto ocurre cuando en secretaría requieren ancho de banda y no es en horario docente o cuando se realizan cursos fuera del horario de secretaría. La empresa requiere mecanismos para optimizar al máximo sus recursos de comunicaciones.

2. Identificación de necesidades

Para poder optimizar las comunicaciones se requiere un sistema que realice las siguientes funciones:

- Debe establecerse un mecanismo dinámico que gestione el ancho de banda en cada momento.
- Debe ser capaz de gestionar varias conexiones simultáneas y poder escalar el crecimiento de comunicaciones de la sede
- Debe ser capaz de encaminar el tráfico interno por la conexión de intranet
- Debe permitir asignar calidad de servicio a servicios determinados, garantizando así servicios como correo electrónico o voz IP y limitar otros servicios como p2p.
- Debe permitir cache de páginas web, así como filtrado de contenidos

3. Solución propuesta para la realización de pruebas

La solución propuesta consiste en la instalación de un servidor dedicado para la gestión de las comunicaciones. Dicho servidor utilizará en la medida de lo posible herramientas de software libre.

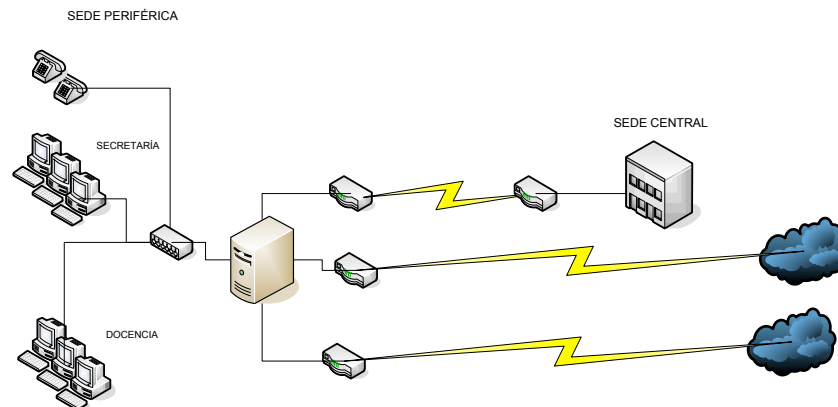


Figura 6. Propuesta inicial de esquema de red

La herramienta elegida para realizar las pruebas de viabilidad es Zentyal.

Zentyal es una herramienta de software libre, basada en Ubuntu especializada en la gestión de redes de comunicaciones. Se utilizará para pruebas una estructura del tipo 3, es decir, dos ADSLs dedicadas a ofrecer servicios de Internet y un ADSL conectado a la red interna para proporcionar servicios internos y servicios de Internet en caso de caídas o fallos de sistema.

La estructura de red en la que basaré el estudio y las pruebas posteriores será la siguiente:

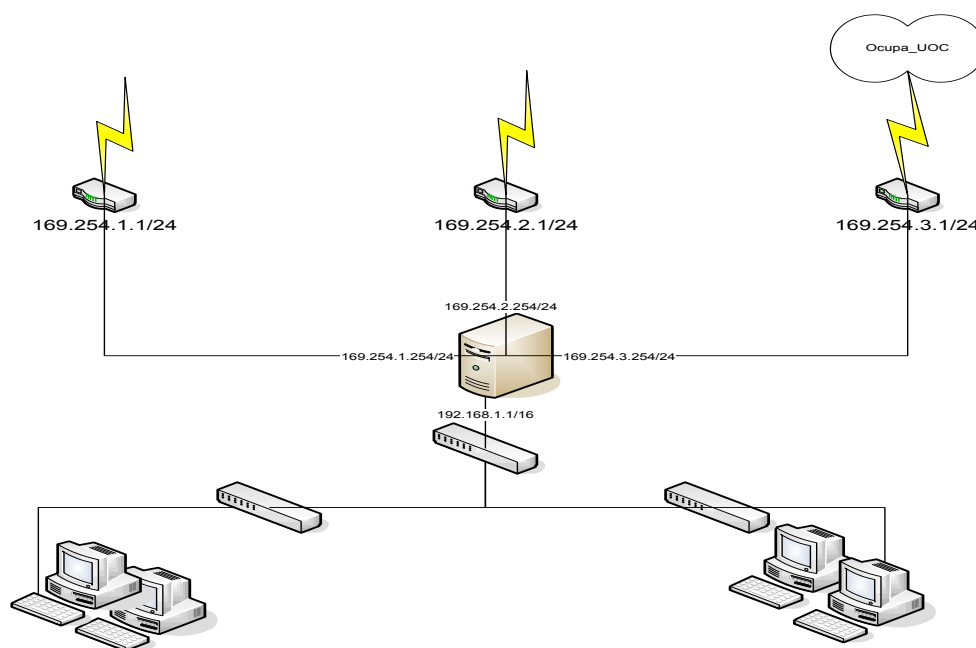


Figura 7. Estructura de red del entorno de pruebas

Esta situación será simulada mediante la herramienta de virtualización de software libre VirtualBox⁴

4. Desarrollo de las pruebas

4.1 Configuración del entorno de pruebas

Para el desarrollo de las pruebas se han utilizado 5 máquinas virtuales con las siguientes funciones

- Una máquina virtual llevará configurado un sistema operativo Ubuntu que se utilizará para realizar pruebas simulando un cliente de la red interna de la sede periférica
- Una máquina virtual será el servidor Zentyal
- Tres máquinas virtuales se comportarán como routers de comunicaciones.

La simulación del esquema de red se realizará aprovechando las diferentes configuraciones que VirtualBox ofrece para la gestión de redes. Se crearán cuatro redes internas que simularán las conexiones físicas entre los routers y la máquina Zentyal así como entre los equipos de la red interna con la interfaz interna del Zentyal.

Las redes creadas serán las siguientes:

⁴ Página Oficial de VirtualBox: <https://www.virtualbox.org/>

- Red interna N° 1 (intnet1): Conecta el router 1 con la interfaz eth0 de la máquina Zentyal
- Red interna N° 2 (intnet2): Conecta el router 2 con la interfaz eth1 de la máquina Zentyal
- Red interna N° 3 (intnet3): Conecta el router 3 con la interfaz eth2 de la máquina Zentyal
- Red interna N° 4(intnetLocal): Conecta los equipos de la red local de la sede con la interfaz eth3 de la máquina Zentyal

A continuación se detallarán las especificaciones de cada una de las máquinas virtualizadas:

4.1.1 Máquina cliente Ubuntu 11.0

La maquina Ubuntu simula cualquier equipo que se encuentre dentro de la red interna de la sede. Podría ser cualquier PC, teléfono de VoIP, tablets, teléfonos móviles a través de un punto de acceso o cualquier tipo de dispositivo IP que requiera comunicación con el exterior bien de Intranet o de Internet.

En este caso la configuración utilizada es la estándar para una instalación de Ubuntu.

Posee 1 GB de memoria RAM, un disco duro con capacidad máxima de almacenamiento de 8GB conectado al puerto SATA, y una tarjeta de red Intel PRO/1000 conectada a la red interna intnetLocal. Si bien en este caso el tipo de adaptador es irrelevante debido al gran número de controladores soportados por esta distribución será de interés elegir un adaptador correcto para las siguientes máquinas.

En el gráfico siguiente se puede ver las características de dicha máquina obtenidas directamente del panel de control de VirtualBox.



Figura 8. Especificaciones VirtualBox de máquina virtual Ubuntu

La instalación y configuración de esta máquina virtual es la predeterminada en una instalación básica de Ubuntu, donde el único punto relevante es la asignación de dirección IP que le he asignado la 192.168.1.254/24

4.1.2 Máquina Zentyal

La máquina Zentyal simula un servidor de comunicaciones Zentyal. Zentyal es una herramienta basada en Ubuntu Server y como tal requiere una configuración de hardware similar a la de la máquina cliente Ubuntu antes definida.

En este caso se ha definido una máquina con 512MB de RAM, un disco duro con una capacidad máxima de 8GB conectado al controlador IDE primario como maestro y un CD-ROM virtualizado mediante el que realicé la instalación con un fichero imagen. Cabe destacar que utilicé IDE en lugar de SATA porque encontré problemas en la instalación que se resolvieron con esta configuración de discos.

Por último se han habilitado los cuatro interfaces que define como máximo VirtualBox para una máquina virtual definiendo el adaptador Intel PRO/1000 MT (Opción por defecto) en todos ellos y definiendo la forma de conexión como de red interna. Se establece que el interfaz 1 estará conectado a la red intnet1, el interfaz 2 a la red intnet 2, el interfaz 3 a la red innet3 y el interfaz 4 a la red intnetLocal.

En el siguiente gráfico se puede apreciar la configuración de la máquina virtual vista desde el panel de control de VirtualBox.



Figura 9. Especificaciones VirtualBox de máquina virtual Zentyal

La instalación de Zentyal es una instalación totalmente guiada donde apenas se establece ninguna configuración, salvo la definición de los usuarios que administrarán la máquina. Toda la configuración queda en manos del panel de control de Zentyal que aparece tras el primer inicio de sesión.

Una vez arrancado por primera vez el servidor virtual, tras acceder al panel se procede a instalar los módulos de Zentyal que se desean configurar.

El asistente ofrece una serie de configuraciones predeterminadas aunque se pueden seleccionar los módulos deseados manualmente. En esta instalación se habilitarán los siguientes módulos:

- Módulo de red: Permite configurar los interfaces de red así como las puertas de enlace de cada uno de ellos. Proporciona mecanismos dinámicos de activación y desactivación de puertas de enlace en caso de caída de un router de salida.
- Módulo DNS: Permite establecer los mecanismos de resolución de DNS. Además permite utilizar el servidor como DNS cache
- Módulo cortafuegos: Permite establecer reglas tanto de acceso desde la red interna al exterior como viceversa, así como las reglas de acceso al servidor Zentyal para su administración.
- Eventos: Mecanismo de alarmas cuando se supera una situación umbral establecida mediante reglas

- Registros: Permite el almacenamiento de los datos del sistema. Imprescindible para algunos módulos como la monitorización
- Monitorización: Muestra gráficos del estado del sistema en todo momento.
- NTP: Permite establecer el servidor Zentyal como un servidor NTP, de modo que pueda sincronizar todos los dispositivos de la red interna.
- Moldeado de tráfico: Permite establecer reglas de nivel 7 de la capa OSI, de este modo se puede establecer mecanismos de Calidad de Servicio.
- Monitor de ancho de banda: Permite monitorizar el consumo de ancho de banda
- En el siguiente gráfico se pueden apreciar los módulos instalados en la instalación Zentyal.

Configuración del estado de los módulos

| Módulo | Depende | Estado |
|---------------------------|--------------------------------|-------------------------------------|
| Red | | <input checked="" type="checkbox"/> |
| Cortafuegos | Red | <input checked="" type="checkbox"/> |
| Antivirus | | <input type="checkbox"/> |
| DNS | | <input checked="" type="checkbox"/> |
| Copia de seguridad | | <input type="checkbox"/> |
| Eventos | | <input checked="" type="checkbox"/> |
| IDS | Red | <input type="checkbox"/> |
| Registros | | <input checked="" type="checkbox"/> |
| Monitorización | | <input checked="" type="checkbox"/> |
| NTP | | <input checked="" type="checkbox"/> |
| VPN | Red | <input type="checkbox"/> |
| Moldeado de tráfico | Red, Cortafuegos | <input checked="" type="checkbox"/> |
| Usuarios y Grupos | | <input type="checkbox"/> |
| Monitor de Ancho de Banda | Red, Registros | <input checked="" type="checkbox"/> |
| Proxy HTTP | Cortafuegos, Usuarios y Grupos | <input type="checkbox"/> |

Figura 10. Módulos Zentyal habilitados en las pruebas

Una vez configurados los módulos que va a utilizar la máquina, y en especial el módulo de red se procede a configurar las interfaces de red de modo que las interfaces eth0, eth1 y eth2 se configuran como WAN mientras que la eth3 se configura como LAN.

Cada una de las interfaces configuradas como WAN se configura con direccionamiento estático y con la dirección de red que corresponde a la red a la que pertenece el router al que están conectados. La nomenclatura utilizada ha sido que todas las redes WAN tengan una dirección del tipo 169.254.x.0/24, que la puerta de enlace de cada una de ellas sea 169.254.x.1/24 y la dirección de Zentyal en esa red 169.254.x.254/24. Siguiendo una nomenclatura similar, la red interna tiene la dirección 192.168.1.x/24 y la puerta de enlace corresponderá al servidor Zentyal y tendrá la dirección 192.168.1.1/24

En el gráfico se pueden apreciar las configuraciones de todos los interfaces obtenidas en el panel de control de Zentyal

The image shows four panels of network configuration for interfaces eth0, eth1, eth2, and eth3. Each panel includes fields for Name, Method, Extern (WAN), IP Address, and Subnet Mask, along with a 'Cambiar' button.

| Interface | Nombre | Método | Externo (WAN) | Dirección IP | Máscara de red |
|-----------|--------|----------|-------------------------------------|---------------|----------------|
| eth0 | eth0 | Estático | <input checked="" type="checkbox"/> | 169.254.1.254 | 255.255.255.0 |
| eth1 | eth1 | Estático | <input checked="" type="checkbox"/> | 169.254.2.254 | 255.255.255.0 |
| eth2 | eth2 | Estático | <input checked="" type="checkbox"/> | 169.254.3.254 | 255.255.255.0 |
| eth3 | eth3 | Estático | <input type="checkbox"/> | 192.168.1.1 | 255.255.255.0 |

Figura 11. Configuración de red del servidor Zentyal

4.1.3 Máquinas emuladoras de router de comunicaciones

Para la simulación de los routers de comunicaciones inicialmente se utilizaron máquinas virtuales Linux que, a través de iptables pudieran encaminar el tráfico hacia Internet.

En estos casos se utilizaron equipos virtualizados con una distribución Ubuntu similar a la del cliente Ubuntu antes definido, con dos tarjetas de red, una destinada a la conexión WAN y otra a la conexión con la máquina Zentyal, sin embargo debido a problemas de recursos en la máquina huésped no se podían lanzar cinco máquinas virtuales de esa potencia. Al final se optó por una distribución Linux denominada Freesco⁵

Freesco es una distribución que simula el comportamiento de un elemento de red como un router, un puente etc.

Funciona directamente desde un disquete y queda cargado en memoria. Requiere 32 MB de memoria RAM.

Las configuraciones de las tres máquinas virtuales desde el panel de control de VirtualBox son las siguientes:

⁵ Freesco: www.freesco.org

| General | General | General |
|---|---|---|
| Nombre: Fresco1 Tipo SO: Linux 2.6 | Nombre: Fresco2 Tipo SO: Linux 2.6 | Nombre: Fresco3 Tipo SO: Linux 2.6 |
| Sistema Memoria base: 64 MB Orden de arranque: Disquete, CD/DVD-ROM, Disco duro Aceleración: VT-x(AMD-V) Paginación anidada | Sistema Memoria base: 64 MB Orden de arranque: Disquete, CD/DVD-ROM, Disco duro Aceleración: VT-x(AMD-V) Paginación anidada | Sistema Memoria base: 64 MB Orden de arranque: Disquete, CD/DVD-ROM, Disco duro Aceleración: VT-x(AMD-V) Paginación anidada |
| Almacenamiento Controlador IDE IDE primario maestro: fresco1.vdi (Normal, 8,00 GB) Controlador SATA Controlador de disquete: fresco1.img (1,41 MB) | Almacenamiento Controlador IDE IDE primario maestro: fresco02.vdi (Normal, 8,00 GB) Controlador SATA Controlador de disquete: fresco02.img (1,41 MB) | Almacenamiento Controlador IDE IDE primario maestro: fresco03.vdi (Normal, 8,00 GB) Controlador SATA Controlador de disquete: fresco03.img (1,41 MB) |
| Red Adaptador 1: PCNet-PCI II (NAT) Adaptador 2: PCNet-FAST III (Red interna, «intnet1») | Red Adaptador 1: PCNet-PCI II (NAT) Adaptador 2: PCNet-FAST III (Red interna, «intnet2») | Red Adaptador 1: PCNet-PCI II (NAT) Adaptador 2: PCNet-FAST III (Red interna, «intnet3») |

12. Especificaciones VirtualBox de las máquinas Fresco

En la instalación de esta distribución se encontraron dos problemas:

En primer lugar, dado que es una distribución tan minimalista no detectó la tarjeta de red predeterminada de VirtualBox, sin embargo sí que fue capaz cuando se definió del tipo PCNet Fast III. De este modo se estableció que cada máquina contaría con dos tarjetas de tipo PCNet Fast III, una configurada mediante NAT para simular la conexión WAN y otra configurada mediante red interna cada una de las máquinas a las redes intnet1, intnet2 e intnet3 respectivamente.

El segundo problema fue la instalación en disco duro, que por motivos desconocidos no lograba arrancar. De todos modos, funcionaba correctamente desde disquete, y permitía guardar los cambios en él sin problema de espacio.

Los disquetes fueron virtualizados a través de tres ficheros imagen, de modo que cada uno de ellos podía tener almacenada su propia configuración.

Una vez arrancada la máquina virtual aparece el siguiente panel de control

```
Welcome to FREESCO v0.4.4 Setup (c) 2011 Lewis Baughman
http://www.freesco.org/
http://www.freesco.net/
http://www.freesco.info/

      F R E E S C O
IP Masquerade Router/Firewall/Server
(Powered by Linux)

Legend: green - required parameters;
        yellow - optional parameters;
        red   - for experts only, 'yeah right' ;-)

Three steps of setup:
  1) choose router type and configure it.
  2) change extended settings.
  3) save configuration, exit and reboot system.

Continue in color or monochrome mode (c/m)? [c]
```

Figura 13. Pantalla de inicio de Fresco

El menú de selección ofrece un gran número de opciones como se puede apreciar en el gráfico siguiente.

```
ADVANCED SETTINGS MENU

[ Users/Passwords ]
-> a) root/admin/ppp
   b) Users menu
   c) Dial-out control

[ Hardware ]
d) COM ports
e) Ethernet cards
f) Modem settings

[ Networks ]
g) Host/Domain
h) Local networks

[ Security/Limitations ]
i) Remote access
j) Access restrictions
k) Internal security
l) NAT helper modules
m) Block extra ports

[ Dial-up router ]
n) Add/Edit/List ISP
o) Diald options

[ Permanent router ]
p) Ethernet ISP
q) Leased line ISP

Advanced settings (x - exit)?
```

Figura 14. Panel de control Freesco

Sin embargo las que se requieren son las siguientes:

- Ethernet cards: En este punto se comprueba si ha detectado las dos tarjetas de red
- Local networks: Se establece la configuración IP de las tarjetas de red

La configuración de red queda del siguiente modo.

- La interfaz de red 0 queda configurada automáticamente mediante DHCP.
- La interfaz 1 queda configurada manualmente con la dirección de red 169.254.x.1

```

                                NETWORK SETTINGS
[ Network # ] 0)                1)                2)
[ Interface ] eth0              eth1
[ IP address ] 10.0.2.15        169.254.1.1

[ Network # ] 3)                4)                5)
[ Interface ]
[ IP address ]

[ Network # ] 6)                7)                8)
[ Interface ]
[ IP address ]

[ Network # ] 9)
[ Interface ]
[ IP address ]

[ ----- Network 1 ----- ]
-> a) Interface Name      = eth1                Ins) Auto Configure Network #1
   b) IP address         = 169.254.1.1          Del) Clear Network #1 Settings
   c) Network mask       = 255.255.255.0
   d) Network address    = 169.254.1.0
   e) Broadcast address  = 169.254.1.255
   f) DHCP server pool   =

Choose network 0-9 or its parameter to change (x - exit)?
```

Figura 15. Configuración de red Freesco

4. 1.4 Estructura de red virtualizada

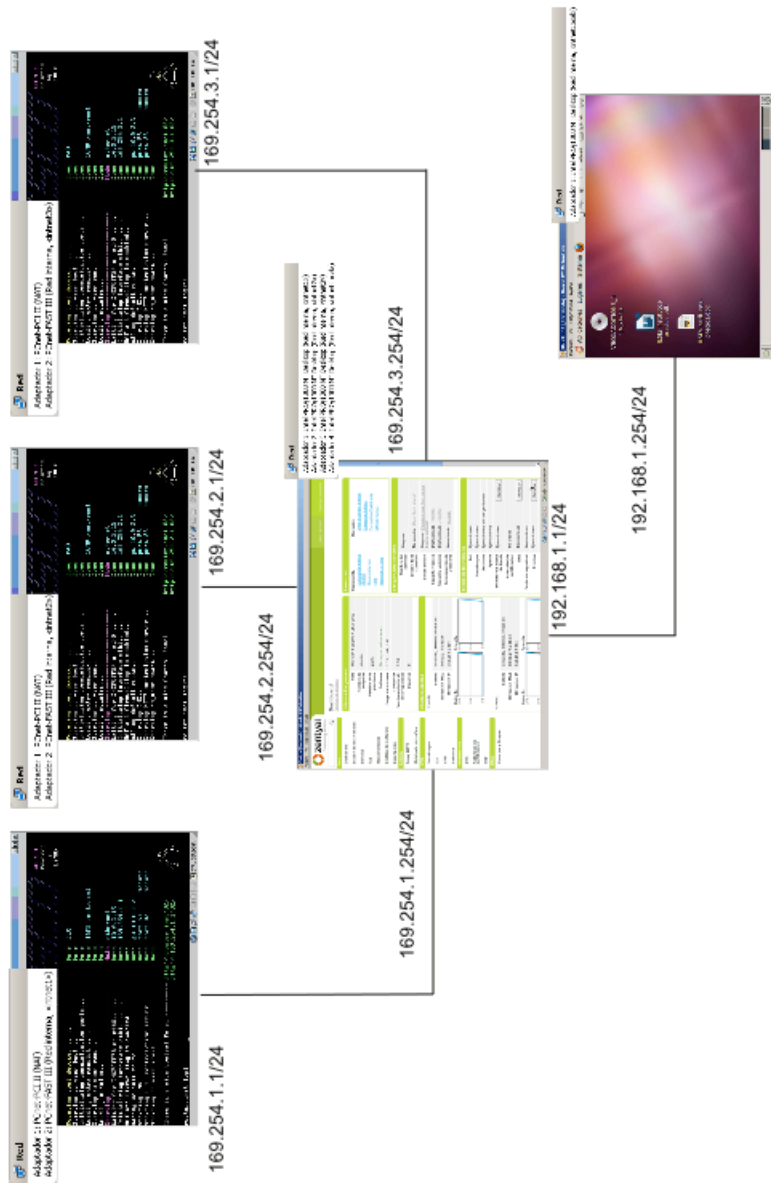


Figura 16. Esquema de red virtualizada

4.2 Balanceo de carga

En Zentyal el balanceo de carga se logra a través del módulo de red. En dicho módulo se establece no sólo los interfaces de red sino también las puertas de enlace. Estas puertas de enlace tienen una característica especial, se habilitan y deshabilitan automáticamente en el momento que detectan que se ha caído una línea o se ha restablecido la conexión.

La configuración de las puertas de enlace permite establecer una puerta de enlace predeterminada, así como establecer pesos a cada una de ellas. Los pesos se utilizarán para balancear el tráfico entre las líneas, bien de forma homogénea (estableciendo el mismo peso a todas ellas) o de cualquier otra forma según las proporciones. Esto requiere habilitar la opción de balanceo de tráfico que se establece más adelante.

La configuración utilizada para realizar las pruebas es tres puertas de enlace con el mismo peso todas ellas. En la imagen se puede ver la configuración utilizada.

| Habilitado | Nombre | Dirección IP | Interfaz | Peso | Predeterminado | Acción |
|-------------------------------------|--------|--------------|----------|------|----------------|--------|
| <input checked="" type="checkbox"/> | ads13 | 169.254.3.1 | eth2 | 1 | ✓ | 🗑️ ✎️ |
| <input checked="" type="checkbox"/> | ads12 | 169.254.2.1 | eth1 | 1 | ✗ | 🗑️ ✎️ |
| <input checked="" type="checkbox"/> | ads11 | 169.254.1.1 | eth0 | 1 | ✗ | 🗑️ ✎️ |

Figura 17. Configuración de puertas de enlace Zentyal

En segundo lugar se ha configurado el balanceo de tráfico así como una regla de múltiples puertas de enlace. Esta opción permite asignar reglas para que se utilice una puerta de enlace independientemente de las opciones de balanceo cuando se cumpla la misma. En este caso se ha establecido que el tráfico que vaya a la red de OcupaUOC se redirijan por la puerta de enlace ads13.



Figura 18. Configuración de balanceo de carga en Zentyal

Por último se establece un modo de detección de caídas de red. La prueba que se ha establecido por es realizar ping a las puertas de enlace. En un entorno de producción sería más aconsejable un ping a un servidor de Internet, como 8.8.8.8, servidor de DNS de Google. En esta entorno virtualizado utilizar uno u otro método no es relevante. Se establece el tiempo entre revisiones en 10 segundos, el número de pruebas a realizar en 6 y el ratio de éxito en un 40%.

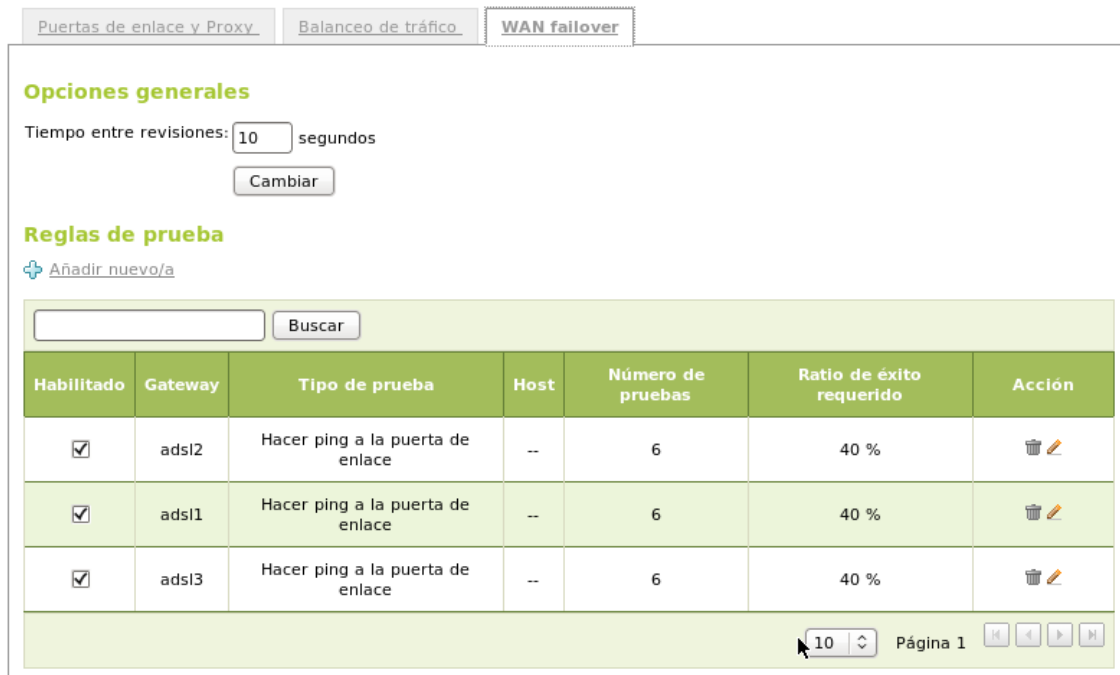


Figura 19. Configuración de reglas de prueba de conectividad

Una vez configurado el entorno se puede comprobar si la configuración funciona correctamente

4.2.1 Prueba de fallo de conexión WAN

Para probar el funcionamiento del Zentyal se apaga de uno en uno cada uno de los routers y se comprueba el estado de la puerta de enlace. Posteriormente se encienden de nuevo y se comprueba cómo se recupera la puerta de enlace que corresponda. El resultado de las pruebas es satisfactorio. Se comprueba que el tiempo de recuperación es aproximadamente de 30 segundos.

4.2.2 Prueba de balanceo de carga

Para probar el balance se descargará una Web a través del comando Linux wget en su modo recursivo.

El resultado de la prueba es que no ha habido balanceo y todo el tráfico ha utilizado la misma puerta de enlace.

Tras realizar varias pruebas se comprueba que cada vez tiende a usar una diferente hasta que iguala los ratios utilizados.

La conclusión que obtengo es que sí que hace balanceo de carga pero que mantiene la conexión establecida hasta que ésta termina. Si hubiera más clientes sí que se hubiera notado ese tráfico pero como no es así se establece la conexión con una puerta de enlace y se mantiene hasta que finaliza dicha conexión.

4.3Cache de DNS

Para establecer el cache de DNS es necesario realizar los siguientes pasos. En primer lugar se deben habilitar los DNS en la máquina, Esta opción se encuentra en el menú red en la opción DNS.

Para poder definir el cache de DNS se debe establecer por un lado un servidor DNS externo y después establecer como servidor de DNS localhost y posicionarlo en primer lugar

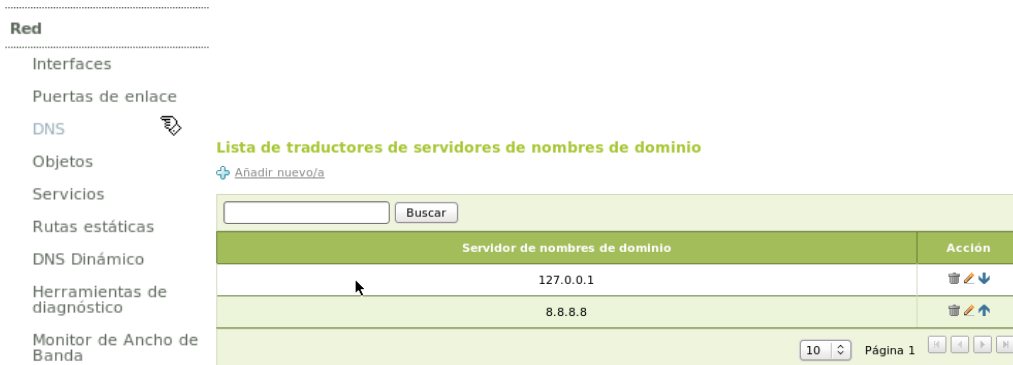


Figura 20. Configuración de DNS

Posteriormente en infraestructura se deben definir redireccionadores que, en caso de fallo redirija a éstos la resolución de nombres, y establezco como redireccionador las tres puertas de enlace, es decir la dirección interna de los routers. Por último habilito DNS cache transparente.



Figura 21. Configuración de redireccionadores de DNS

Los resultados de las pruebas no permiten establecer ninguna conclusión. Debido al poco tráfico de red no se logra ninguna ganancia con el DNS cache, si bien se puede confirmar que funciona correctamente.

4.4 Filtrado de paquetes

En Zentyal se ha cuidado en extremo el filtrado de paquetes. Las herramientas como iptables son poco intuitivas y Zentyal ofrece un asistente muy claro que permite configurar fácilmente cualquier opción de filtrado.


Las reglas se dividen en 4 tipos:

- reglas de filtrado desde las redes internas a Zentyal: Son las reglas que permiten configurar Zentyal o acceder a él desde el interior
- Reglas de filtrado para redes internas: Son las reglas que permiten actuar a Zentyal como un cortafuegos con el exterior

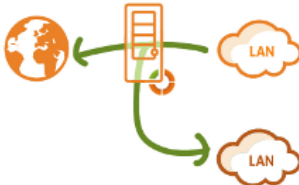
- Reglas de filtrado para redes externas: Son reglas destinadas a permitir el acceso a la máquina Zentyal desde el exterior
- Reglas de filtrado desde las redes externas a las internas: Son reglas destinadas a permitir el acceso a servicios internos desde el exterior como servicios Web, Ftp etc.

En la imagen se pueden apreciar el menú de reglas de filtrado que ofrece Zentyal.


Packet Filter




Reglas de filtrado desde las redes internas a Zentyal
Estas reglas le permiten controlar el acceso desde redes internas a servicios que corren en su máquina Zentyal
[Configurar reglas](#)



Reglas de filtrado para las redes internas
Estas reglas le permiten controlar el acceso desde sus redes internas a Internet, y el tráfico entre sus redes internas. Si desea dar acceso a los servicios de Zentyal, debe usar la sección superior.
[Configurar reglas](#)



Reglas de filtrado desde las redes externas a Zentyal
Estas reglas le permiten controlar el acceso desde redes externas a servicios que corren en su máquina Zentyal.
! Debe saber que añadiendo reglas a esta sección puede estar comprometiendo la seguridad de su red, permitiendo el acceso desde redes no confiables. Por favor, hágalo sólo si sabe lo que está haciendo.
[Configurar reglas](#)



Reglas de filtrado desde las redes externas a las internas
Estas reglas le permiten controlar el acceso desde redes externas a redes internas
! Debe saber que añadiendo reglas a esta sección puede estar comprometiendo la seguridad de su red, permitiendo el acceso desde redes no confiables. Por favor, hágalo sólo si sabe lo que está haciendo.
[Configurar reglas](#)

Figura 22. Panel de control de reglas de filtrado

La configuración por defecto de Zentyal permite acceso desde la intranet a cualquier servicio externo y el acceso al servidor Zentyal desde redes internas para configuración, DNS, servicio de tiempo y servicio de LDAP.

En los gráficos se pueden apreciar las configuraciones de filtrado de paquetes que Zentyal ofrece por defecto.

Filtrado de paquetes ► Redes internas

Configure Rules

+ Añadir nuevo/a

| Decisión | Origen | Destino | Servicio | Descripción | Acción |
|----------|------------|------------|------------|-------------|--------|
| ↑ | Cualquiera | Cualquiera | cualquiera | -- | 🗑️✎️ |

10 | Página 1

Figura 23. Configuración por defecto de filtrado de redes internas
Filtrado de paquetes ► Desde redes internas hacia Zentyal

Configure Rules

+ Añadir nuevo/a

| Decisión | Origen | Servicio | Descripción | Acción |
|----------|------------|---------------------------|-------------|----------|
| ✖ | Cualquiera | Idap | -- | 🗑️✎️⬇️ |
| ✖ | Cualquiera | adsync | -- | 🗑️✎️⬆️⬇️ |
| ↑ | Cualquiera | ntp | -- | 🗑️✎️⬆️⬇️ |
| ↑ | Cualquiera | dns | -- | 🗑️✎️⬆️⬇️ |
| ↑ | Cualquiera | ssh | -- | 🗑️✎️⬆️⬇️ |
| ↑ | Cualquiera | Administración de Zentyal | -- | 🗑️✎️⬆️ |

10 | Página 1

Figura 24. Configuración de filtrado desde redes internas hacia Zentyal

4.5.1 Prueba de filtrado de paquetes

Desde la máquina cliente se realizan las siguientes pruebas:

- Acceso a servicios de Internet: Las pruebas son satisfactorias
- Acceso a la máquina Zentyal: Los protocolos http, Ftp y https no ofrecen conexión. Se permite el acceso por SSH, resuelve nombres a través del DNS de Zentyal y permite la sincronización de hora NTP

- Acceso desde el exterior. Desde las máquinas virtuales de los routers se prueba la conexión a los mismos servicios anteriores. El resultado es que no se puede establecer ninguna conexión.

4.6 Cache de contenidos

La activación del módulo de caché de contenidos consiste básicamente en establecer un Proxy transparente y habilitar que tamaño máximo tendrá la caché de contenidos. Por defecto el tamaño es 100MBytes.

Este módulo proporciona una interfaz amigable de configuración básica del servidor Proxy Squid⁶

⁶ Página oficial del proyecto Squid: <http://www.squid-cache.org/>

Proxy HTTP (mostrar ayuda)

¿Quieres eliminar los anuncios de la navegación de tus usuarios? Obtén la edición [Small Business](#) o [Enterprise](#) que incluyen el servicio de Ad Blocking en las actualizaciones de seguridad automáticas.

Configuración General

Proxy Transparente:
Nótese que no se puede usar proxy HTTPS de forma transparente. Se necesitará añadir una regla de firewall si se habilita este modo.

Bloqueo de Anuncios:
Quitar anuncios de todo el tráfico HTTP

Puerto:

Tamaño de los ficheros de caché (MB):

Política predeterminada: Filter significa que las peticiones HTTP pasan por el filtro de contenidos y que podrían ser rechazados si el contenido no se considera válido.

Figura 25. Configuración de caché de contenidos

En la configuración del Proxy aparecen la opción de bloqueo de anuncios, sin embargo esta opción no está disponible en la versión gratuita y requiere la instalación de la versión Enterprise.

El tamaño de cache por defecto es 100MB. En el caso de las pruebas puede ser un valor correcto. En casos de producción dependerá en gran medida del número de ordenadores cliente que existan así como del tipo de contenido. En un aula es probable que todos requieran acceder a los mismos documentos. Si existen muchos clientes podría ser escaso el tamaño de cache. Por otro lado, una cache más grande requerirá más trabajo de proceso de la información y en el caso de servidores con una carga alta de trabajo podría suponer tiempos de respuesta peores que el acceso a esa información a través de la red.

4.6.1 Pruebas de caché de contenidos

Las pruebas realizadas permiten obtener las siguientes conclusiones. El módulo funciona correctamente. Las imágenes, ficheros y páginas Web se cargan mucho más rápidamente cuando se habilita el Proxy transparente.

En las pruebas realizadas se constató que Zentyal no es capaz de almacenar en la cache contenido de tipo Flash y videos. Si bien Zentyal no es capaz de gestionar este tipo de contenidos, existen webs que relatan cómo se puede conseguir. Cabe destacar la Web <http://wiki.squid-cache.org> que entre su contenido relata cómo conseguir almacenar este contenido.

4.7 Calidad de servicio (QoS)

Zentyal propone un sistema de calidad del servicio basado en reglas de aplicación a protocolos de nivel de aplicación de la pila de protocolos OSI.

Se puede encontrar las opciones de configuración dentro del menú Gateway en las opciones de Moldeado de tráfico.

En moldeado de tráfico se encuentran tres opciones.

- La primera opción, protocolos de aplicación es un mecanismo para agrupar protocolos con la misma funcionalidad al que se pueda aplicar las mismas reglas de calidad del servicio.
- La segunda opción, reglas establece las reglas que se aplicarán.
- La última opción, tasas de interfaz establece velocidades máximas a las que se permite trabajar a la interfaz.

En la imagen posterior se pueden ver los grupos de protocolos establecidos por defecto.

Grupo de servicios basados en aplicación [\(mostrar ayuda\)](#)

Lista de grupos

[+ Añadir nuevo/a](#)

Buscar

| Grupo | protocolos | Acción |
|-----------------|------------|--------|
| chat | | |
| game | | |
| mail | | |
| p2p | | |
| remote_access | | |
| streaming_audio | | |
| streaming_video | | |
| voip | | |
| web | | |

10 Página 1

Gateway

Proxy HTTP

Moldeado de tráfico

Protocolos de Aplicación

Reglas

Tasas de Interfaz

Figura 26. grupos de protocolos para moldeado de tráfico

Los grupos aquí establecidos pueden modificarse, eliminarse o añadirse. Dentro de cada uno están definidos protocolos de nivel 7 agrupados por su funcionalidad.

Como ejemplo los protocolos establecidos como p2p son entre otros skypetoskype, bittorrent, audialogalaxy o applejuice.

En el siguiente gráfico se puede apreciar los protocolos que forman parte del grupo p2p

Grupo de servicios basados en aplicación

Protocolos de nivel 7 agrupados

[Añadir nuevo/a](#)





















| Protocolo | Acción |
|---------------|--|
| xunlei |   |
| skypetoskype |   |
| goboogy |   |
| thecircle |   |
| skypeout |   |
| audialogalaxy |   |
| bittorrent |   |
| freenet |   |
| ares |   |
| applejuice |   |

Figura 27. Servicios incluidos en grupo p2p

Zentyal permite también limitar las velocidades de subida y bajada de cada una de las interfaces. Por defecto las tasas que asigna son las siguientes:





| Interfaz externa | Subida | Descargar | Acción |
|------------------|------------|------------|---|
| eth1 | 16384 Kb/s | 16384 Kb/s |  |
| eth2 | 16384 Kb/s | 16384 Kb/s |  |
| eth1 | 16384 Kb/s | 16384 Kb/s |  |
| eth0 | 16384 Kb/s | 16384 Kb/s |  |

Figura 28. Limitación de tráfico de las interfaces de red

4.7.1 Pruebas de calidad de servicio

Para la ejecución de las pruebas de calidad de servicio se han utilizado la siguiente configuración

En el ordenador huésped se ha ejecutado un programa que convierte al sistema en un servidor de ficheros mediante http. El programa se denomina HFS

En la máquina Ubuntu se ha ejecutado Mozilla Firefox y se ha accedido al servidor de ficheros de la máquina huésped

Se han desactivado dos de las tres máquinas Freesco. El motivo es que las reglas se configuran para interfaces de red y si no se desactivan las reglas no tendrían sentido pues podría encontrar caminos alternativos que no respondiera a las mismas reglas

Se ha configurado una regla de moldeado de tráfico con el fin de limitar el tráfico http a 1Kbps.

Para añadir una regla, en Zentyal se accede al panel de Moldeado de tráfico, y tras seleccionar una interfaz de red se añade una nueva regla.

Las reglas se pueden añadir para servicios basados en puerto, o para servicios basados en objetos (agrupación de servicios), indicando como parámetros si se desea filtrar por origen o destino así como la prioridad de la regla.

Añadiendo un/a nuevo/a regla

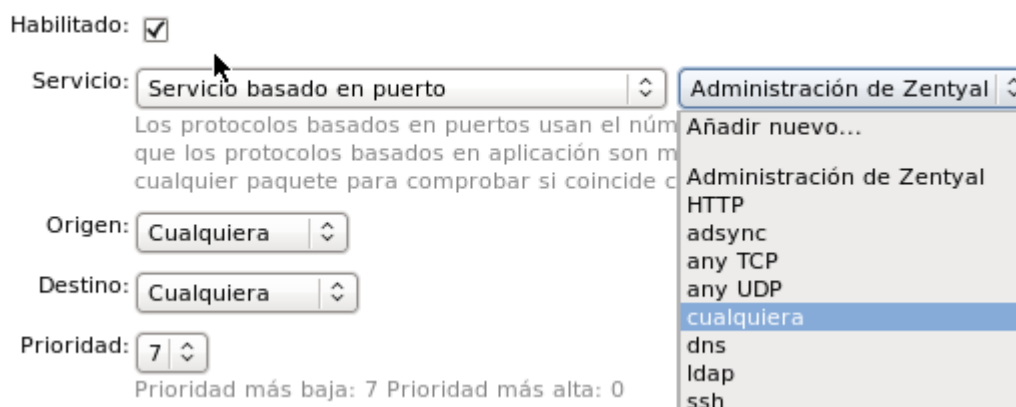


Figura 29. Configuración de reglas de calidad del servicio

Dentro de la selección del servicio se puede configurar diferentes opciones como el puerto o rangos de puertos de origen, el puerto o rangos de puertos de destino así como los protocolos. En la imagen siguiente se ve una configuración para el puerto 20 (FTP).



Figura 30. Configuración de reglas QoS FTP

Para la realización de las pruebas, sin embargo utilizaré la opción http. Una vez grabada la configuración, se procede a la realización de la prueba. En el equipo con Ubuntu se obtiene la siguiente pantalla al acceder al servidor HFS y descargar un fichero de la lista de ficheros que ofrece el servidor.

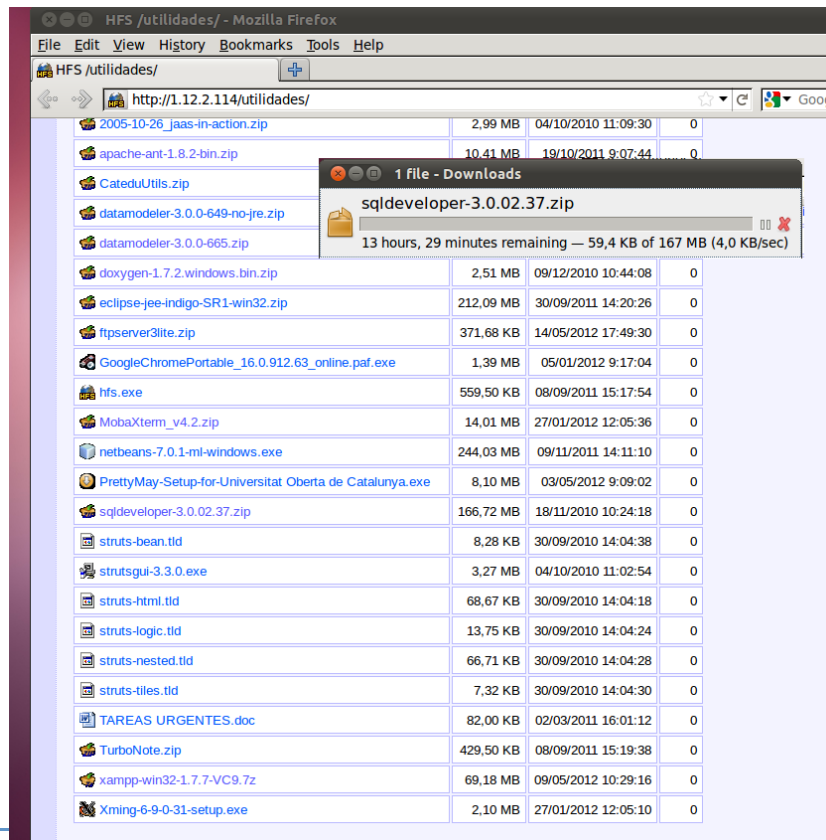


Figura 31. Verificación de bajada de ficheros HTTP

Como se puede apreciar en el gráfico se obtienen las siguientes conclusiones:

- Sí es cierto que la aplicación de la regla limita el ancho de banda en gran medida, sin su aplicación la descarga se producía a más de 100MB/sec.
- La limitación de ancho de banda no llega a ser de 1Kbps como se configuró en el Zentyal sino de 4 KB/s, 32 veces más de lo establecido en el mejor de los casos, es decir, con prioridad 0. En los casos en los que la prioridad era peor la velocidad de descarga aumentaba
- El resultado es un poco decepcionante debido a la granularidad que ofrece el sistema, si bien la posibilidad de limitar el ancho de banda a servicios es interesante y se podría aplicar aún teniendo en cuenta las desviaciones que ofrece.

Tras comentar estas conclusiones en un foro me confirman que cuando Zentyal está trabajando como Proxy transparente las reglas de moldeado de tráfico para tráfico http no se gestionan tal y como realicé las pruebas. Esto sucede porque Zentyal realiza la gestión de moldeado de tráfico a través de reglas de iptables, sin embargo, cuando actúa como Proxy transparente las peticiones no atraviesan el servidor sino que se transforman en peticiones a la máquina Zentyal. Por ello se obtienen diferentes resultados.

4.8 Síntesis de resultados

La herramienta Zentyal ha resultado ser de gran facilidad de uso y eficaz en la función que tiene asignada. Con las pruebas realizadas no se puede medir su eficiencia debido a que el entorno se parece poco a un entorno de producción, sin embargo, dado que está basado en herramientas libres conocidas sobre las que únicamente se ha perfeccionado el entorno de configuración, así como que está siendo utilizado con éxito por empresas líderes y administración pública como aparece en la Web del fabricante proporciona muchas razones para ser optimista.

Solución propuesta

1 Estructura de red

1.1 Tipos de comunicaciones en la organización

Las comunicaciones de la organización se pueden clasificar en cuatro tipos:

El primer tipo de comunicaciones son las **comunicaciones con los servicios corporativos**: En este caso los usuarios de las subsedes requieren consumir servicios corporativos que se encuentran en la sede central. Dentro de estas comunicaciones se encuentran los accesos al servidor Web de Intranet, a los servidores de ficheros, de LDAP, de Groupware y correo electrónico entre otros servicios.

El segundo tipo de comunicaciones son las **comunicaciones con otras subsedes**. En este caso se producen comunicaciones entre las subsedes sin que se requiera que exista para ello comunicación con la central. Este sería el modelo utilizado por las comunicaciones de Voz sobre IP o de mensajería.

El tercer tipo de comunicaciones son las **comunicaciones con el exterior de la organización**. En este caso las comunicaciones se producen desde cada una de las sedes hacia Internet. No existe comunicación con la sede central sino que cada una utiliza su propia infraestructura para acceder a Internet.

Por último el cuarto tipo son las **comunicaciones desde el exterior hacia el interior de la organización**. Estas comunicaciones se producirán hacia el servidor Web público de la organización o el servidor de correo.

1.2 Comunicaciones con los servicios corporativos

Se producen cuando los servicios consumidos se encuentran dentro de la propia red de la organización. Los servidores, que se encuentran en la sede central deben ser accesibles desde los equipos de las subsedes.

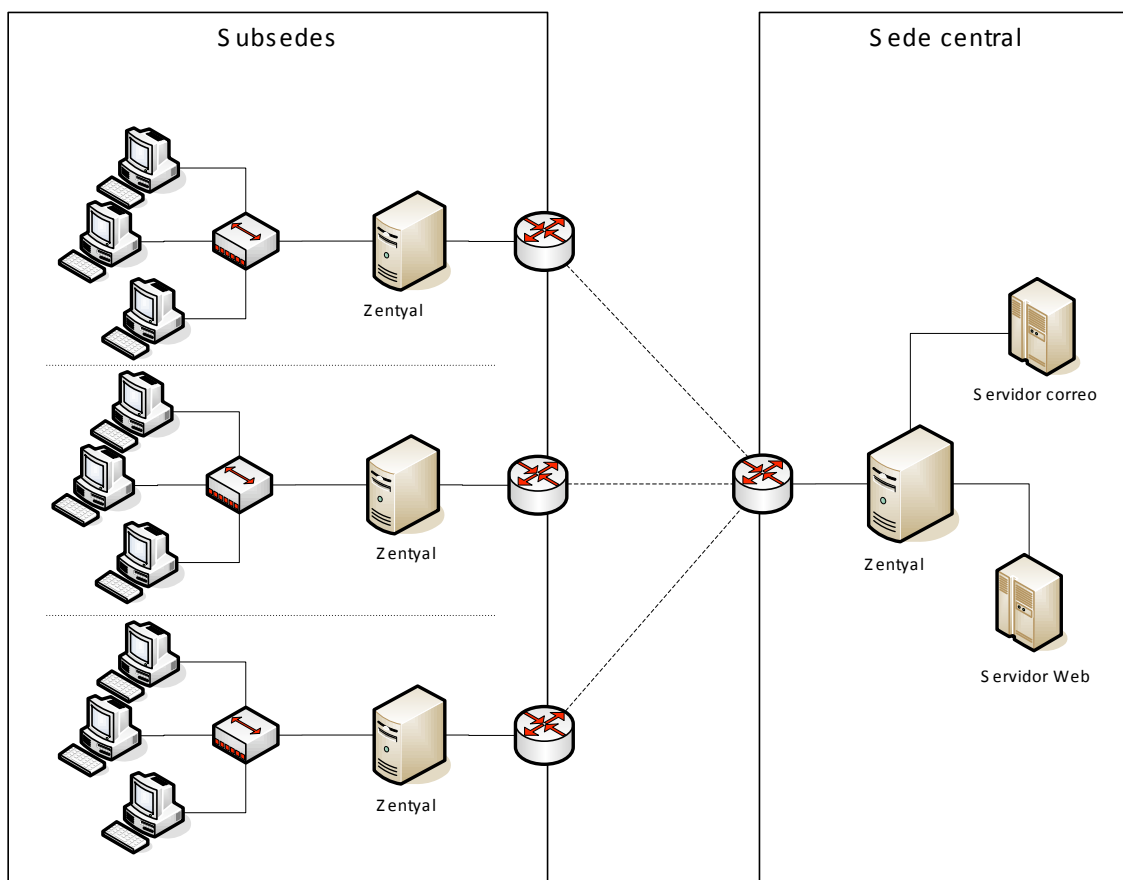


Figura 32. Esquema de red de acceso a servicios corporativos

Comunicaciones con otras subsedes

Cada vez que se produce una comunicación entre diferentes sedes se establece una comunicación directa. En este caso la sede central se comporta como una subsede más

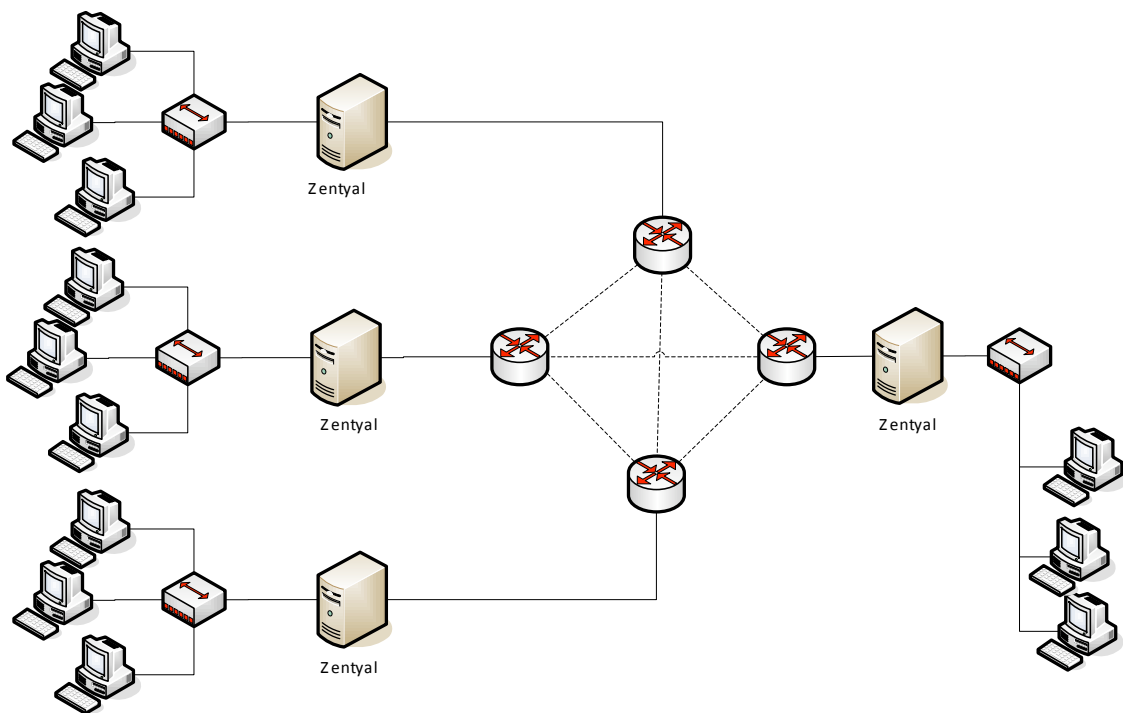


Figura 33. Esquema de red de comunicación entre sedes

1.4 Comunicaciones con el exterior de la organización

Tanto La sede central como las subsedes necesitan disponer de ancho de banda suficiente en sus comunicaciones con Internet. Para ello cada una de ellas contará con una o varias conexiones de banda ancha.

La configuración más favorable sería con al menos dos conexiones de banda ancha contratadas con distintos proveedores de servicios que, a ser posible utilicen diferentes tecnologías, por ejemplo Fibra óptica y ADSL. De este modo no sólo se obtienen redundancia en las líneas sino que ante una incidencia del proveedor de servicio, las comunicaciones se verían afectadas mínimamente.

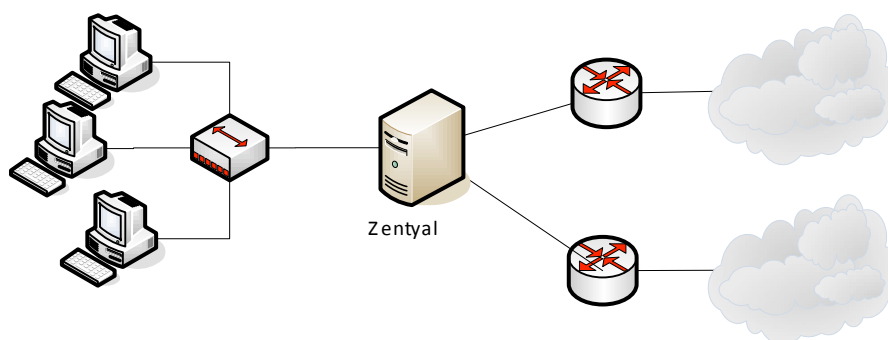


Figura 34. Esquema de red de comunicaciones de una sede con el exterior

1.5 Comunicaciones desde el exterior hacia el interior de la organización

Todas las comunicaciones que se produzcan con el exterior se realizan a través de la sede central.

La sede central ofrece visibilidad a su Web así como a su servidor de correo. Lógicamente si las necesidades de la organización cambiaran se podrían añadir tantos servicios como se requirieran.

Para acceder desde el exterior se debe atravesar un cortafuegos que dará acceso a la zona desmilitarizada. Otro cortafuegos impedirá las conexiones al interior de la organización.

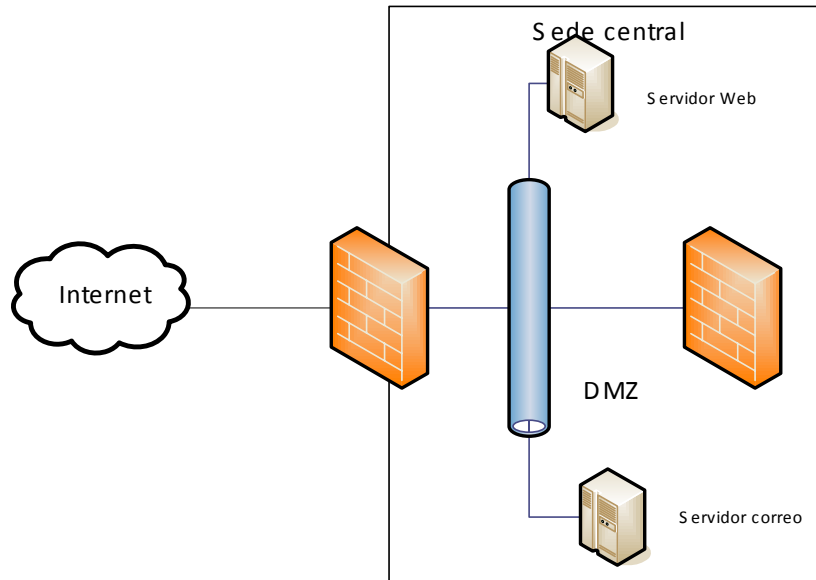


Figura 35. Esquema de red de comunicaciones desde el exterior

1.6 Diagrama de red de la organización

A continuación se detalla la estructura de red propuesta para la organización.

En este diagrama se puede apreciar los siguientes detalles:

Las subsedes poseen al menos dos conexiones de banda ancha que ofrecen servicios de Internet, así como una conexión que ofrece servicio de red privada virtual a través de un proveedor de servicios. Se puede utilizar el servicio GigaADSL que ya poseía la organización inicial para conectar las sedes.

En cada subsede existe un servidor Zentyal que gestiona las comunicaciones de red. De este modo balancea el tráfico de la subsede y encamina las peticiones a la sede central o a otras subsedes.

La sede central cumple la doble función de ofrecer servicios de Internet y de Intranet así como de comunicarse con las subsedes. Las comunicaciones con el exterior se protegen

mediante un servidor Zentyal que proporciona servicios de cortafuegos. Otro servidor Zentyal proporciona la gestión de comunicaciones en ambos sentidos entre la sede central y las periféricas.

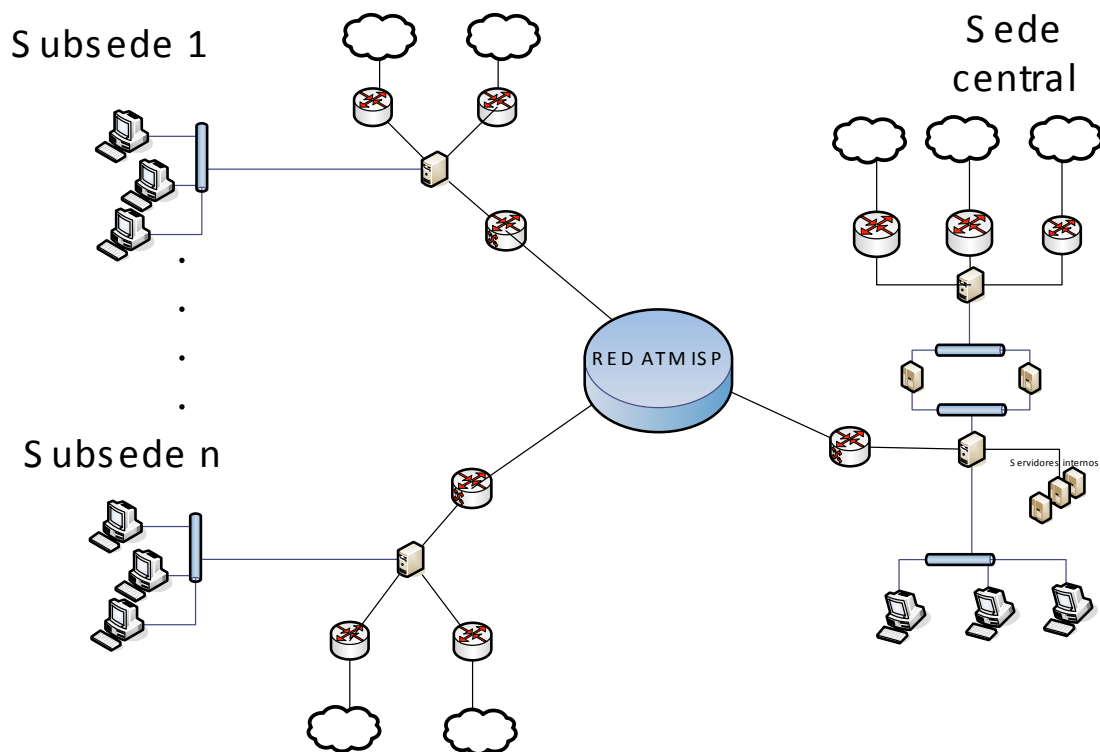


Figura 36. Diagrama de red propuesto

2 Requisitos de hardware y comunicaciones

Antes de definir los componentes y equipos necesarios para la implantación de esta infraestructura de red es necesario conocer la infraestructura inicial con la que cuenta cada sede.

En todas las sedes actualmente existen una conexión de banda ancha de Intranet mediante el servicio Giga ADSL. Además la mayoría de los centros cuentan con al menos una conexión de banda ancha para ofrecer servicios de Internet sin colapsar el servicio GigaADSL.

Cuentan además con los dispositivos de red necesarios, conmutadores 10/100 suficientes para conectar todos los equipos así como encaminadores para ofrecer la comunicación con el exterior.

La sede central posee la misma infraestructura que las sedes periféricas, aunque además cuenta con dos conexiones de banda ancha, una dedicada a los servicios externos y otra dedicada a proporcionar salida a Internet a la sede central y las periféricas que lo requieran. Poseen servidor Web así como servidor de correo corporativo

2.1 Requisitos de comunicaciones de la sede periférica.

Para proporcionar un servicio de calidad, en aquellas sedes de gran tamaño se debe contratar nuevas líneas de banda ancha. Siempre que sea posible se elegirá un proveedor de servicio diferente al que tenga contratado actualmente y que proporcione el servicio por diferente medio. Así si el servicio actual es basado en ADSL se preferirá un servicio basado en fibra óptica, y ADSL en caso contrario. Cada uno de ellos contará con un servidor dedicado para gestionar las comunicaciones.

Los routers reenviarán todo el tráfico entrante al servidor Zentyal correspondiente que lo gestionará.

Los requisitos del servidor se encuentran en el punto 2.3.

2.2 Requisitos de comunicaciones de la sede central

La sede central inicialmente ya cuenta con diferentes conexiones de banda ancha para ofrecer servicios de Internet así como para proporcionar acceso externo a su servidor Web y al correo de la entidad.

Posee además una conexión de banda ancha conectada a la Intranet GigaADSL, con la que se conecta con las sedes periféricas.

Para mejorar el uso de red y aumentar así mismo la seguridad de los servidores requiere de dos servidores dedicados, uno como cortafuegos interno y otro como cortafuegos externo.

2.3 Requisitos de hardware de los servidores Zentyal

Tal y como se ha descrito en los puntos anteriores la organización necesita incluir un servidor Zentyal en cada sede periférica y dos servidores Zentyal en la sede central.

Los requisitos hardware mínimos de estos servidores dependen en gran medida de la carga de trabajo que vaya a soportar. El uso de la red cada vez es más vital en cualquier organización, por lo que se recomienda adquirir servidores que permitan soportar el

incremento de tráfico que pueda surgir a lo largo del tiempo de forma eficaz. Además los precios actuales de los equipos hacen que el desembolso económico no varíe demasiado entre una solución mínima y una solución con mayor perspectiva.

Los puntos críticos de un servidor Zentyal son los siguientes:

- Memoria RAM: Es el punto en el que almacenará los paquetes que debe procesar. Debe ser rápida y suficiente. Se recomienda al menos 4GB
- Disco duro: La capacidad de disco duro permitirá una mayor capacidad de almacenamiento de contenidos, que reducirá drásticamente el consumo de ancho de banda. Se recomienda al menos dos discos S/ATA de 500GB en espejo (RAID 1).
- Procesador: La aplicación de las reglas de tráfico y de calidad de servicio requiere una carga elevada de procesador. Se recomienda procesadores Xeon Dual Core
- Tarjetas de red: Son los puntos de entrada y salida de la información que atraviesa el servidor. Deberán ser de gran calidad y alta capacidad para responder lo más rápidamente posible a la demanda de tráfico que se genere. Requerirán cuatro tarjetas de red Gigabit Ethernet

Esta información se encuentra basada en la documentación técnica ofrecida por Zentyal en su página Web.

3 Configuración propuesta de Zentyal

3.1 Configuración del servidor Zentyal de las subredes

3.1.1 Módulos necesarios

Para la configuración de Zentyal se requerirán los siguientes módulos:

| Configuración del estado de los módulos | | |
|---|--------------------------------|-------------------------------------|
| Módulo | Depende | Estado |
| Red | | <input checked="" type="checkbox"/> |
| Cortafuegos | Red | <input checked="" type="checkbox"/> |
| DNS | | <input checked="" type="checkbox"/> |
| Eventos | | <input checked="" type="checkbox"/> |
| Registros | | <input checked="" type="checkbox"/> |
| Moldeado de tráfico | Red, Cortafuegos | <input checked="" type="checkbox"/> |
| Usuarios y Grupos | | <input checked="" type="checkbox"/> |
| Monitor de Ancho de Banda | Red, Registros | <input checked="" type="checkbox"/> |
| Proxy HTTP | Cortafuegos, Usuarios y Grupos | <input checked="" type="checkbox"/> |

Figura 37. Selección de módulos Zentyal propuesta

3.1.1 Interfaces de red

Las interfaces de red se configurarán de modo similar a la configuración utilizada en las pruebas de la herramienta.

Se utilizarán tres interfaces para las comunicaciones externas, dos de ellas para ofrecer servicios de Internet y otra para conectar con la Intranet de la organización. La cuarta interfaz servirá para como nexo interno con los equipos de la sede.

La propuesta de configuración es la siguiente:

- Eth0: Interfaz externa, con dirección IP 169.254.1.254/24. Se comunica con uno de los routers que proporciona acceso a Internet
- Eth1: Interfaz externa, con dirección IP 169.254.2.254/24. Se comunica con el segundo router que ofrece acceso a Internet.
- Eth2: Interfaz externa, con dirección IP 169.254.3.254/24. se comunica con el router de acceso a la Intranet de la organización
- Eth3: Interfaz interna, con dirección IP 192.168.1.1/24

3.1.2 Puertas de enlace

Se configuran tres puertas de enlace, una para cada interfaz externo de red.

- La interfaz eth0 tendrá definida la puerta de enlace 169.254.1.1, dirección IP interna del primer router de salida a Internet

- La interfaz eth1 tendrá definida la puerta de enlace 169.254.2.1, dirección IP interna del segundo router de salida a Internet
- La interfaz eth2 tendrá definida la puerta de enlace 169.254.3.1, dirección interna del router de acceso a la Intranet corporativa

Las puertas de enlace con salida a Internet tendrán un peso proporcional a su capacidad, de modo que ante velocidades iguales coincidirán. En caso contrario se realizará la proporción. Por ejemplo, ante dos ADSL, uno de 2MBps y otro de 20MBps se establecerá un peso de 1 a la primera puerta de enlace y de 9 a la segunda.

Para estas puertas de enlace se definirá como medida de detección de fallo de red el acceso mediante ping al servidor 8.8.8.8 que corresponde a los servidores públicos de DNS de Google.

La puerta de enlace de Intranet tendrá el peso mínimo, de modo que el tráfico hacia el exterior no se redirija hacia la Intranet salvo en caso de que no exista otro medio de comunicación.

Para esta puerta se definirá como medida de detección de fallo de red el acceso a la puerta de enlace del router.

Se establece además una ruta estática a la red 10.1.0.0/16, donde se encuentran a través del interfaz eth2 para acceder a los servicios corporativos.

Los routers GigaADSL deberán incluir una regla en la que las llamadas dentro de esta subred se redirijan al GigaADSL de la sede central.

3.1.3 Configuración de DNS

La configuración de DNS necesaria será la siguiente:

- Se establecerán tres servidores DNS, uno por cada router con salida a Internet y otro con un DNS público, como 8.8.8.8 o los que proporcione el ISP. Además se añadirá localhost como servidor DNS ya que se activará el módulo de caché de DNS
- Se habilitará la opción de caché de DNS y se definirán como redireccionadores aquellos servidores anteriormente incluidos.

3.1.4 Cortafuegos

La configuración de cortafuegos será la siguiente:

- Se aceptará cualquier paquete de datos que provenga de la red interna
- Si se requiere comunicación entre las subsedes mediante videoconferencia o mensajería instantánea se habilitarán las comunicaciones externas que provengan de la Intranet de los puertos de los servicios requeridos.

3.1.5 Proxy http

Se habilitará la opción de Proxy http en modo transparente.

3.1.6 Moldeado de tráfico

Se habilitarán reglas de moldeado de tráfico del siguiente modo:

- Se establecerá con prioridad 0 el tráfico de y hacia el servidor de correo tanto a sus servicios de pop3, imap y smtp.
- Se establecerá también con prioridad 0 los servicios de Voz sobre IP o de mensajería instantánea que tengan origen y destino direcciones internas de la organización, en el caso de que la organización los requiriera
- A los servicios de sistemas de ficheros, tales como CIFS o NFS se les asignará prioridad 1
- Se establecerá con prioridad 2 el tráfico destinado al servidor Web corporativo, FTP, LDAP así como a los servicios de GroupWare
- Se establecerá con prioridad 3 el tráfico http y https hacia Internet
- Se asignará prioridad 7 (la más baja) a los servicios de mensajería instantánea con el exterior
- Se asignará prioridad 7 a las comunicaciones P2P y se limitará su velocidad a 1Kbps

3.2 Configuración del servidor Zentyal interno de la sede central

La configuración de servidor Zentyal interno de la sede central que se propone es la siguiente

3.2.1 Interfaces de red

Se utilizarán tres interfaces para las comunicaciones externas, dos de ellas para ofrecer servicios de Internet y otra para conectar con la Intranet de la organización. La cuarta interfaz servirá para como nexo interno con los equipos de la sede.

La propuesta de configuración es la siguiente:

- Eth0: Interfaz interna, con dirección IP 10.1.1.254/24 . Gestiona los accesos a los servidores corporativos
- Eth1: Interfaz externa, con dirección IP 10.1.2.254/24. Se comunica con el Zentyal externo para proporcionar acceso a Internet desde el interior. Además permite el acceso al servidor de correo y al servidor Web desde la red interna.
- Eth2: Interfaz interna, con dirección IP 169.254.3.254/24. se comunica con el router de acceso a la Intranet de la organización
- Eth3: Interfaz interna, con dirección IP 192.168.1.1/24

3.2.2 Puertas de enlace

Se configura una puerta de enlace

La interfaz eth1 tendrá definida la puerta de enlace 10.1.1.1 dirección IP interna del servidor Zentyal externo

En este caso no se requiere establecer balanceo de carga ya que el tráfico hacia el exterior se limita a un único interfaz de red.

3.2.3 Configuración de DNS

La configuración de DNS es la misma que la definida en el caso de los Zentyal de las sedes periféricas

3.2.4 Cortafuegos

La configuración de cortafuegos será la siguiente:

- Se aceptará cualquier conexión de datos que provengan de las interfaces de red eth2 y eth3
- Se denegará cualquier establecimiento de conexión desde los interfaces eth0 y eth1

3.2.5 Moldeado de tráfico

En este caso las prioridades de las reglas varían para priorizar aquel tráfico proveniente de las sedes periféricas de sistemas de ficheros o correo.

Las reglas de moldeado de tráfico quedarán del siguiente modo:

- Se establecerá con prioridad 0 el tráfico de y hacia el servidor de correo tanto a sus servicios de pop3, imap y smtp.
- A los servicios de sistemas de ficheros, tales como CIFS o NFS se les asignará prioridad 1
- Se establecerá con prioridad 1 el tráfico destinado al servidor Web corporativo, FTP, LDAP así como a los servicios de GroupWare
- Se establecerá con prioridad 1 los servicios de Voz sobre IP y con prioridad 4 los de mensajería instantánea que tengan origen y destino direcciones internas de la organización, en el caso de que la organización los requiriera
- Se establecerá con prioridad 3 el tráfico http y https hacia Internet
- Se asignará prioridad 7 (la más baja) a los servicios de mensajería instantánea con el exterior
- Se asignará prioridad 7 a las comunicaciones P2P y se limitará su velocidad a 1Kbps

3.2.6 Proxy http

Se habilitará la opción de Proxy http en modo transparente.

3.3 Configuración del servidor Zentyal externo de la sede central

El servidor Zentyal externo tendrá las siguientes funciones:

Proporcionar un acceso seguro a los servidores Web y de correo de la organización
Aprovechar los recursos de banda ancha de la organización de la forma más óptima
Para cumplir estos objetivos se propone la siguiente configuración

3.3.1 Interfaces de red

Se utilizarán tres interfaces para las comunicaciones externas, dos de ellas para ofrecer servicios de Internet y otra para conectar con la Intranet de la organización. La cuarta interfaz servirá para como nexo interno con los equipos de la sede.

La propuesta de configuración es la siguiente:

- Eth0: Interfaz externa, con dirección IP 169.254.1.254/24. Comunica el Zentyal externo con el router externo 1.
- Eth1: Interfaz externa, con dirección IP 169.254.2.254/24. Comunica el Zentyal externo con el router externo 2
- Eth2: Interfaz externa, con dirección IP 169.254.3.254/24. Comunica el Zentyal externo con el router externo 1.
- Eth3: Interfaz interna, con dirección IP 10.1.2.1/24 . Servirá de puerta de enlace del servidor Zentyal interno

3.3.2 Puertas de enlace

Se configuran tres puertas de enlace, una para cada interfaz externo de red.

- La interfaz eth0 tendrá definida la puerta de enlace 169.254.1.1, dirección IP interna del primer router de salida a Internet
- La interfaz eth1 tendrá definida la puerta de enlace 169.254.2.1, dirección IP interna del segundo router de salida a Internet
- La interfaz eth2 tendrá definida la puerta de enlace 169.254.3.1, dirección interna del tercer router de acceso a Internet

Al igual que en la configuración de los Zentyal de las sedes periféricas las puertas de enlace tendrán un peso proporcional a su capacidad.

Las pruebas de detección de fallo seguirán la misma política, tratar de acceder mediante ping al servidor DNS de Google o de los proveedores de servicio de cada una de las líneas contratadas.

3.3.3 Configuración de DNS

La configuración de DNS es la misma que la definida en el caso de los Zentyal de las sedes periféricas

3.3.4 Cortafuegos

La configuración de cortafuegos será la siguiente:

- Se aceptará cualquier establecimiento de conexión de datos que provenga de la red interna, es decir del interfaz eth3

- Se denegará cualquier establecimiento de conexión desde los interfaces eth0, eth1y eth2 que traten de atravesar el Zentyal
- Se aceptarán el establecimiento de conexiones dirigidas al Zentyal a los puertos http, https, POP3, SMTP e IMAP

Además se realizará la siguiente redirección de puertos:

- Las peticiones al puerto 80 y 443 se redirigirán al servidor Web corporativo
- Las peticiones a los puertos 110 , 25 y 143 se redirigirán al servidor de correo corporativo

3.3.5 Moldeado de tráfico

En el servidor externo no se considera necesario establecer reglas de moldeado de tráfico, ya que éste ya se encuentra limitado por la actuación de los Zentyal internos. Además esto permite que el servidor externo esté menos sobrecargado

3.3.6 Proxy http

Del mismo modo que en el moldeado de tráfico no se considera necesario habilitar la opción de Proxy http. Habilitar esta opción no va a proporcionar mejores resultados de navegación y sí que va a sobrecargar al servidor externo

Presupuesto estimado

1 Presupuesto hardware

En los requisitos de hardware se estimaba como solución óptima que cada servidor contaba con al menos 4GB de memoria RAM, dos discos duros de 500GB en espejo, procesador Xeon Dual Core y cuatro tarjetas de red Gigabit Ethernet.

Un servidor que cumpliría los requisitos sobradamente es el siguiente:
DELL™ PowerEdge™ T410

- **Procesador:** Intel Xeon E5603, 4C, 1.60GHz, 4M Cache, 4.80GT/s, 80W TDP, DDR3-1066MHz
- **Memoria:** 8GB Memory for 1CPU, DD3, 1333MHz (2x4GB Dual Ranked LV UDIMMs)
- **Conectividad Raid:** C4 Cabled - RAID 1 for SAS 6/iR, 2 SAS/SATA Cabled HDDs
- **Unidades de disco duro:** 2 HD 500GB, SATA, 3.5-in, 7.2K RPM Hard Drive (Cabled)
- **Tarjetas de red:** Broadcom NetXtreme II 5709 Quad Port 1GbE NIC, PCIe-4

El precio de este servidor es de **1.360,00€** en la tienda online del fabricante.

2 Presupuesto licencias de software y mantenimiento

El proyecto Zentyal es un proyecto de software libre licenciado bajo la licencia GPL de la Free Software Foundation. Zentyal puede desplegarse sin coste adicional, sin embargo en una organización que no cuente con un departamento de sistemas o con expertos en redes y sistemas basados en software libre es altamente recomendable adquirir las licencias de mantenimiento que ofrece la compañía.

La versión de licencia recomendada es la de Small Business Edition (SBE). El coste del servicio SBE es de **495,00€** por servidor y año y proporciona las siguientes ventajas:

- Puesta a punto del servicio
- Soporte técnico
- Actualizaciones periódicas.

- Acceso a funcionalidades que no posee la versión gratuita como eliminación de los anuncios en navegación Web

Conclusiones

Zentyal es una herramienta que proporciona una interfaz amigable a servicios que durante muchos años han estado demostrando su calidad en la mayoría de sistemas de grandes organizaciones, y que no han llegado a las pequeñas organizaciones porque les eran capaces de implantar un entorno que se ajustara a sus necesidades.

Herramientas como iptables o squid no resultaban comprensibles al usuario medio que en muchas ocasiones terminaba usando soluciones comerciales que podían configurar y gestionar con pocos clicks de ratón.

En las pruebas realizadas se ha comprobado su facilidad de uso así como su correcto funcionamiento.

Otra ventaja de Zentyal es que gracias a su licencia GPL existe una importante comunidad de usuarios que lo utiliza y ofrece mejoras que repercuten en el bien común, además Zentyal va añadiendo nuevas funcionalidades que aparecen en el mundo del software libre de una forma rápida ya que en el fondo Zentyal es una versión personalizada de la distribución de Linux Ubuntu.

En la actualidad el coste que puede tener para una organización una solución de gestión de tráfico mediante servidores dedicados no es muy elevado. El precio de los servidores ha caído en los últimos años, y es una inversión que se puede recuperar en poco tiempo.

Las organizaciones ganan en calidad de sus comunicaciones, en seguridad y en uso efectivo de su ancho de banda.

Bibliografía

- Guiomar Corral i Torruella, Jaume Abella i Fuentes (2004)
Diseño de redes de computadores
ISBN- 84-9707-442-4
- Daniel Cortés Fernández (2011-12)
Guía de Puntos de Interés de la Comunidad de Madrid. Ejemplo de plan de trabajo
- Web y documentación de Zentyal- www.zentyal.com
- Proyecto Freesco. www.freesco.org
- Cache de videos de Youtube.
<http://wiki.squid-cache.org/ConfigExamples/DynamicContent/YouTube>
- HFS. <http://www.rejetto.com/hfs/>
- DELL Tienda online <http://www.dell.es>
- Página Oficial del servidor de DNS Bind: <http://www.isc.org/>
- Página oficial de iptables: <http://www.netfilter.org/projects/iptables/index.html>
- Manual de iptables – Proyecto LUCAS
<http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf>
- Configuración de Squid – Proyecto LUCAS
<http://es.tldp.org/LinuxFocus/pub/mirror/LinuxFocus/Castellano/March2002/article235.shtml>

Índice de figuras

| | |
|---|----|
| Figura 1. Planificación Temporal - Horario de trabajo- | 10 |
| Figura 2. Planificación Temporal - Diagrama de Gantt- | 11 |
| Figura 3. Situación Inicial con sede periférica - | 14 |
| Figura 4. Red OcupaUOC - Situación inicial con sedes periféricas | 14 |
| Figura 5. Aumento de conexiones de banda ancha en las sedes periféricas - | 15 |
| Figura 6. Propuesta inicial de esquema de red | 16 |
| Figura 7. Estructura de red del entorno de pruebas | 17 |
| Figura 8. Especificaciones VirtualBox de máquina virtual Ubuntu..... | 20 |
| Figura 9. Especificaciones VirtualBox de máquina virtual Zentyal..... | 21 |
| Figura 10. Módulos Zentyal habilitados en las pruebas..... | 22 |
| Figura 11. Configuración de red del servidor Zentyal | 23 |
| Figura 12. Especificaciones VirtualBox de las máquinas Freesco | 25 |
| Figura 13. Pantalla de inicio de Freesco..... | 25 |
| Figura 14. Panel de control Freesco..... | 26 |
| Figura 15. Configuración de red Freesco..... | 27 |
| Figura 16. Esquema de red virtualizada | 28 |
| Figura 17. Configuración de puertos de enlace Zentyal..... | 29 |
| Figura 18. Configuración de balanceo de carga en Zentyal | 30 |
| Figura 19. Configuración de reglas de prueba de conectividad..... | 30 |
| Figura 20. Configuración de DNS | 32 |
| Figura 21. Configuración de redireccionadores de DNS..... | 32 |
| Figura 22. Panel de control de reglas de filtrado | 33 |
| Figura 23. Configuración por defecto de filtrado de redes internas..... | 34 |
| Figura 24. Configuración de filtrado desde redes internas hacia Zentyal..... | 34 |
| Figura 25. Configuración de caché de contenidos | 36 |
| Figura 26. grupos de protocolos para moldeado de tráfico | 37 |
| Figura 27. Servicios incluidos en grupo p2p..... | 38 |
| Figura 28. Limitación de tráfico de las interfaces de red..... | 38 |
| Figura 29. Configuración de reglas de calidad del servicio | 39 |
| Figura 30. Configuración de reglas QoS FTP | 40 |
| Figura 31 Verificación de bajada de ficheros HTTP | 40 |
| Figura 32. Esquema de red de acceso a servicios corporativos..... | 43 |

| | |
|--|----|
| Figura 33. Esquema de red de comunicación entre sedes | 44 |
| Figura 34. Esquema de red de comunicaciones de una sede con el exterior..... | 45 |
| Figura 35. Esquema de red de comunicaciones desde el exterior..... | 46 |
| Figura 36. Diagrama de red propuesto..... | 47 |
| Figura 37. Selección de módulos Zentyal propuesta | 50 |