Universidad del Azuay

Facultad de Administración de Empresas

Escuela de Ingeniería de Sistemas

Implementación de un sistema proxy con seguridad para la navegación de médicos y pacientes en el Hospital Santa Inés"

Monografía previa a la obtención del título de

Ingeniero de sistemas

Autores: María Salomé Narváez Montoya

RomelLeuvísTenesaca Gómez

Director: Ingeniero Esteban Crespo Martínez

Cuenca,Ecuador

2012

***Dedicatoria*:**

Esta monografía está dedicada a Mis Padres quienes han sido el mi apoyo incondicional durante toda mi vida brindándome cariño, amor y comprensión, a mi hermano Joffre quien ha sido el más grande ejemplo de perseverancia para alcanzar mis metas y objetivos y a mi Dios principalmente que me ha dado la sabiduría para poder encaminarme en esta difícil etapa de la vida.

Salomé Narváez M.

***Dedicatoria*:**

Esta monografía va dedicada a toda mi familia, quienes creyeron en mí hasta el final, y siempre seguirán haciéndolo, a mi madre por el amor y sacrificio que ha hecho, y por el gran apoyo y confianza depositada.

De manera especial a Salome Narváez, por su apoyo en momentos difíciles, por sus palabras de aliento y amor que me ayudaron a alcanzar esta meta, sin ella todo esto hubiese sido mucho más difícil.

Rommel Tenesaca G.

***Agradecimiento*:**

Mi gratitud especialmente está dirigida a Rommel quien con su amor y confianza me ha demostrado que juntos se puede superar los altos y bajos que conlleva esta ardua tarea, a mis Padres y hermanos que siempre están cuando los necesito; y a nuestro Director de Tesis Ing. Esteban Crespo que más que director se ha portado como un amigo de manera ética y profesional durante la elaboración de esta monografía.

Salomé Narváez M.

***Agradecimiento*:**

Quiero empezar agradeciendo a Dios, por poner en este camino, brindarme la luz y la fuerza necesaria para seguir adelante con dedicación.

Expresar mis sinceros agradamientos al Ing. Esteban Crespo por su apoyo durante todo este tiempo, sus conocimientos fueron fundamentales para lograr nuestro objetivo.

A mis compañeros y amigos de clase, gracias por el apoyo los conocimientos y la ayuda que me brindaron, todo este tiempo, esperando que sigamos siendo amigos durante toda la vida.

Rommel Tenesaca G.

INDICE

Resumen

En el Hospital Santa Inés, se implementó la herramienta Zentyal para resolver irregularidades referentes a la seguridad, administración, control y tráfico dentro de la red pública que esta maneja. En esta herramienta que se ha implementado, se configuró el servidor proxy para establecer políticas de seguridad, segmentación de usuarios, autentificación, limitación de ancho de banda según perfiles; permitiéndonos adquirir conocimientos avanzados en cuanto a la utilización y administración de una red mediante la investigación realizada.

ABSTRACT

Zentyal tool was implemented in Santa Ines Hospital in order to solve different irregularities within the public network that is employed in this institution, in the following areas: security, administration, control, and traffic. A proxy server was enabled so as to establish security policies, as well as user segmentation, authenticity, and limitation of broadband according to each profile. This research will allow us to obtain advanced information regarding the network use and management.

UNIVERSIDAD DEL AZUAY
DPTO. IDIOMAS

Translated by,

Diana Lee Rodas

Introducción

A medida que el tiempo pasa las comunicaciones se han vuelto el punto clave para fraudes dentro de las empresa e instituciones las cuales manejan grandes cantidades de información, la seguridad junto con la tecnología tienen que ir de la mano para que las instituciones puedan crecer de manera libre sin el temor de que sus datos sean alcanzados por redes intrusas con objetivos ajenos a los de la empresa; por otro lado especificando mejor nuestro campo se pude decir que las redes a nivel de salud son una rama potencial para la mala utilización de la información, debido a la información sensible que posee el historial de cada paciente, datos que almacenan los médicos de manera confidencial, que al estar dentro de una red puede caer en manos de usuarios mal intencionados que la utilicen de manera inapropiada, otra brecha de inseguridad es la forma con la que está configurada la red pública en el Hospital, carece de herramientas que proporcione un nivel más alto de seguridad.

Por lo que esta monografía está enfocada en la seguridad de una red pública que requiere de ciertos parámetros para mejorar su eficiencia y eficacia para el uso de pacientes y personal, diferenciando esas dos categorías de manera adecuada para el mejor aprovechamiento de los recursos en el Hospital Santa Inés .

Objetivos

Objetivo General

- Implementar un sistema de control de navegación para internet en una red pública segmentado en categorías.

Objetivos Específicos

- Implementar políticas de seguridad a los usuarios (médicos, pacientes, visitas) en la red pública en el Hospital Santa Inés a través de la implementación de un proxy
- Analizar Zentyal como herramienta para conseguir seguridad, estabilidad, administrabilidad, usabilidad y ahorro en costos.
- Mejorar la calidad de servicio aprovechando los recursos existentes
- Segmentación de usuarios para acceso a la red

Objetivos Personal

- Utilizar los conocimientos adquiridos en seguridad de la información y en el curso de graduación en general, a la vez que nos preparamos para los retos y exigencias que existen actualmente en nuestra sociedad.
- Adquirir conocimientos acerca de soluciones reales en problemas de seguridad que se presentan en la actualidad mediante la implementación de herramientas de gestión de redes y seguridad en el Hospital Santa Inés.

CAPÍTULO 1: MARCO TEÓRICO

1.1 Introducción a la Seguridad

Con el desarrollo tecnológico que se ha venido dando en los últimos años. Las posibilidades de interconexión a través de las redes, han abierto a las organizaciones y empresas nuevas maneras de interactuar con sus empleados y clientes, lo que conlleva también nuevas amenazas respecto a la estructura de un sistema y a la información. Estas nuevas amenazas han provocado que las organizaciones tomen medidas de seguridad para proteger la información y la infraestructura de sus sistemas. Estas medidas son documentos que constan de directrices que orienten en cuanto al uso y acceso adecuado de los sistemas tecnológicos.

1.2 Políticas de seguridad

Una política de seguridad consiste en establecer un conjunto parámetros o requisitos para proteger un sistema de accesos no autorizados, generalmente esta políticas son establecidas por la alta gerencia y estipulada lo que se puede hacer (política permisiva) y lo que no se puede hacer (política prohibitiva).

En muchas ocasiones las políticas de seguridad no son correctamente establecidas por lo que las personas que están sujetas a estas no pueden entender y no puedan cumplir, para que una política tenga éxito debe ser expresada de manera clara, buscando la facilidad de entendimiento y el interés por parte del personal.

1.2.1 Estructuración de una Política de seguridad

Para lograr que una política sea correctamente estructurada y definida, debemos seguir ciertos criterios y fundamentos lo cuales nos garantizan una mejor elaboración de una política de seguridad.

1.2.2 La Gestión de la Seguridad

Para que los procesos de seguridad sean llevados a cabo debe haber un compromiso por parte de todos los miembros de la organización.

Gestionar la seguridad implica también tener procesos de control interno como auditorías internas de los procesos, capacitación al personal, tener una evaluación de los riesgos.

1.2.3 Las Personas responsables de la Seguridad

En una organización debe haber una persona encargada del control procesos de seguridad implementados, esta persona debe tener conocimiento de la funcionalidad de cada procedimiento y de las actividades que se llevan a cabo en la empresa, con el fin de establecer parámetros de seguridad en cada proceso.

1.2.4 El Sistema de Seguridad

El sistema de seguridad hace referencia al conjunto de estructura de la organización, procesos, funciones y recursos que se establecen para gestionar la seguridad.

Es importante que al elaborar de una política de seguridad estén contempladas todas las eventualidades que se puedan presentar, por ello al elaborar una medida de seguridad hay que tomar en cuenta cada aspecto de la misma.

En una organización los recursos y capacidad muchas veces pueden ser limitados por lo tanto un sistema de seguridad debe estar acorde con las necesidades y recursos de la empresa.

1.2.5 Control de los Procesos

Este control tiene por objetivo minimizar las causas de riesgo en un proceso determinado, en este punto es conveniente analizar proceso a proceso todas las actividades que interfieren en cada uno de ellos, con el fin de prevenir cualquier eventualidad que puedan presentarse.

1.2.6 Proceso de Seguridad

Son acciones llevadas a cabo para cumplir con una política de seguridad implementada previamente. Para ello implica tener un control de todos los

procesos de seguridad que se deben cumplir en la realización de una actividad u operación.

1.2.7 Aplicación de una Política de Seguridad

A pesar de los esfuerzos que hacen las organizaciones junto con el personal de seguridad informática definiendo parámetros y requisitos de seguridad, muchas de estas políticas no llegan a tener el éxito en una empresa, no causan el impacto que se esperaba, existen barreras que impiden que estas políticas de seguridad alcancen sus objetivos.

La alta gerencia muchas veces, desconoce de los beneficios que puede proporcionar las políticas de seguridad en la empresa, la falta de percepción de posibles focos de inseguridad en la empresa ya se con la información o con la infraestructura hace que los ejecutivos piense en medidas de seguridad como algo extra e innecesario.

La falta de estrategias de seguridad, la carencia de conocimiento e investigación por parte del personal de seguridad informática, hacen que los recursos y gastos informáticos para implementar una política de seguridad sean elevados. Para que una medida de seguridad tenga éxito el gerente debe adecuarse a los recursos con lo que se disponen en una empresa y aprovecharlos al máximo.

La capacitación y concientización del personal de la organización puede resultar complicado, ya que tendrán que cumplir ciertos parámetros y ciertas normas que no estaban acostumbrados a realizar. Todo el personal de la organización incluido usuarios, deberá tomar conciencia de la importancia que puede llegar a tener una medida de seguridad y deberán estar dispuestos a trabajar en conjunto con el personal de seguridad.

Para que las medidas de seguridad surtan efecto, tienen que estar alineadas a los objetivos de la empresa, responder a sus intereses, comprometer a los actores a que intervengan activamente de estas medidas, y tomar conciencia de la importancia que tiene la seguridad en una organización.

1.2.8 Ventajas y Desventajas de Usar Políticas de Seguridad

Diariamente nos encontramos con ciertos riesgos dentro de nuestra vida cotidiana, en la cual siempre prestamos atención a lo que hemos conseguido con tal esfuerzo, por lo que hemos luchado para que funcione correctamente y nos aseguramos que siempre este protegido ya que no sabemos las intenciones de las personas externas a nuestros objetivos, pasa lo mismo con las empresas que tienen su información como algo preciado ya que es como un repositorio de datos donde los clientes confían a través del tiempo demostrando con ética, profesionalismo y compromiso que al establecer políticas de seguridad en su empresa la información puede estar resguardada para un uso positivo, de igual manera para el correcto funcionamiento de la empresa misma, por lo que establecer políticas de seguridad en una empresa sea cual sea su objetivo de servicio, siempre será como mantener su información dentro de una caja fuerte.

1.2.9 Ventajas de Usar Políticas de Seguridad

- Se establece para proteger el acceso de personas externas a la que la entidad ofrece el servicio
- Ayuda a proteger la información en cuanto a fraudes y mala utilización de la misma
- Ayuda a restringir el paso a virus o enlaces dañinos que pueden perjudicar el funcionamiento de la red
- Permiten el control de configuraciones correctas en los equipos necesarios para la seguridad de la información.
- Permite establecer nuevos métodos de seguridad implementando las últimas Tecnologías.
- Permite educar a los administradores de red y usuarios el uso correcto de las redes y a su vez a proteger la información que utilizan diariamente
- Ayuda en el análisis de los posibles riesgos desconocidos

1.2.9 Desventajas de las políticas de seguridad en redes inalámbricas

- Altos costos de equipos para la protección de la información
- Demora en el tiempo de cumplimiento de tareas debido al proceso que requiere cumplir una política de seguridad.
- Representa costos en cuanto a capacitación al personal al implementar nuevas políticas.
- Discordias entre personal en cuanto a la adaptación de dichas políticas.
- Falta de asignación de funciones ya que nadie se quiere responsabilizar por información delicada que pueda traer consigo consecuencias de perdida.

1.3 Herramientas que Intervienen en la Seguridad

En el mercado hay cientos de herramientas que nos ayudan a mejorar la seguridad de una infraestructura de un sistema o de datos, sin embargo hay que tomar en cuenta los recursos tanto humanos como económicos con que dispone una empresa, lo más conveniente a la hora de analizar cuál de todas las herramientas utilizar será el objetivo que percibe alcanzar una organización o empresa con respecto a la seguridad y los recursos con los que se cuenta, una vez elegida una herramienta tratar de explotar todo su potencial para bien del departamento de seguridad y de la empresa.

1.3.1Certificados digitales

Para una organización que utiliza internet como el medio de comunicación dentro y fuera de sus instalaciones surge un problema, que es la identificación de personas y entidades. Por ejemplo en la web nos pide ingresar datos personales para realizar transacciones, como saber si en la página en la que queremos realizar dicha transacción, es la página de la entidad o empresa que dice ser.

Una solución a asta interrogante es la utilización de un certificado o firma digital, el cual es un fichero no modificable, con esta tecnología se garantiza que el autor de una transferencia o mensaje es quien realmente dice ser,

garantiza también la posibilidad de que receptor pueda comprobar la autoría de una transferencia o un mensaje sin que este pueda alterar el mensaje.

Los certificados digitales o firmas digitales emplean una técnica de encriptación de dos claves Pública y Privada relacionadas entre sí. La Clave Publica es utilizada para verificar un mensaje o una transferencia a través de la clave privada, la des-encriptación de mensajes solo puede realizarse a través de la clave privada por ello la importancia de la misma.

En un certificado digital, la clave pública y privada es asociada con datos referentes la información de un usuario o entidad, este certificado se instala en el navegador, la cual funciona como una credencial de acceso.

Un certificado digital lo pueden emitir cualquiera pero por lo general hay entidades Certificadoras como Verising o Banco Central del Ecuador, que son entidades que proporcionan información detallada de las políticas necesarias para emitir y administrar un certificado digital, lo que hace que estos sean confiables para los usuarios.

1.3.1.1 Estructura de los Certificados Digitales

La estructura de un certificado digital tiene que ser comprensible y confiable a la vez, ya que la información tiene que ser recuperable y entendible. Los certificados digitales tienen que seguir un estándar ya que se tienen que poder leer y entender independientemente de quien emita el certificado.

El estándar S/MIME especifica que los certificados digitales utilizados para S/MIME se atienen al estándar X.509 de la Unión internacional de telecomunicaciones (ITU).

El estándar X.509 especifica que los certificados digitales contienen información normalizada. En concreto, los certificados de la versión 3 de X.509 contienen los campos siguientes:

- **Versión.-** contiene el número de versión del certificado.

- **Número de serie del certificado.-** Un número que identifica de manera única al certificado y que está emitido por la entidad emisora de certificados.
- **Identificador del algoritmo de firmado.-** Los nombres de los algoritmos de claves públicas que la entidad emisora ha utilizado para firmar el certificado digital.
- **Nombre del emisor.-** La identidad de la entidad emisora de certificados que emitió realmente el certificado.
- **Periodo de Validez.-** El período de tiempo durante el cual un certificado digital es válido; contiene una fecha de inicio y una fecha de caducidad.
- **Nombre del Sujeto.-** El nombre del propietario del certificado digital.
- **Información de clave pública del sujeto.-** La clave pública asociada al propietario del certificado digital y los algoritmos de claves públicas asociados a la clave pública.
- **Identificador único del emisor.-** Información que puede utilizarse para identificar de manera única al emisor del certificado digital.
- **Identificador único del sujeto.-** Información que puede utilizarse para identificar de manera única al propietario del certificado digital.
- **Extensiones.-** Información adicional relacionada con el uso y el tratamiento del certificado.
- **Firma digital de la autoridad certificadora.-** La firma digital real realizada con la clave privada de la entidad emisora utilizando el algoritmo especificado en el campo.

1.3.1.2 El cifrado

La criptografía es parte de la computación ya que estudia la trasformación de la información que es fácil de leer para el ser humano en información que no se puede leer directamente, sino que debe descifrarse antes de ser leída. Si alguien se hace con un mensaje cifrado, es incomprensible para todo el que no tenga capacidad de descifrarlo.

En los mensajes digitales se convierte en una herramienta ideal para solucionar los problemas de confidencialidad y autenticidad. Su principal funcionalidad es la ocultación de ficheros y mensajes a ojos no autorizados y en la firma de documentos, impidiendo que estos se modifiquen sin que los cambios sean detectados.

El funcionamiento seria que el emisor manda un mensaje y este pasa por un cifrado, con la ayuda de una clave, para crear un texto cifrado. El texto cifrado llega al destinatario que, convierte el texto cifrado apoyándose en otra clave; en el texto ya descifrado. Las dos claves implicadas en el proceso de cifrado /descifrado pueden ser o no iguales, dependiendo del sistema de cifrado utilizado.

1.3.1.3 Criptografía Simétrica

Este tipo de criptografía utiliza para cifrar una clave igual a la usada para descifrar, define un conjunto de métodos que permiten efectuar una comunicación segura entre Emisor y un receptor una vez que se ha consensuado una clave secreta, con la cual se cifrará el mensaje en el origen y se descifrará en el destino; este tipo de criptografía tiene gran velocidad de cifrado y descifrado pero también tiene como punto negativo el hecho que el emisor debe enviar la clave secreta por algún medio seguro al receptor lo cual es riesgoso.

1.3.1.4 Criptografía Asimétrica

A diferencia que la criptografía Simétrica este tipo usa para cifrar una clave diferente a la usada para descifrar; provee métodos que permiten efectuar una comunicación segura entre un emisor y un receptor utilizando dos claves diferentes por cada uno, una para cifrar como ya se ha mencionado se llama clave pública y otra para descifrar que es la clave privada.

Siempre una clave pública se corresponde con una clave privada; en la práctica no puede hallarse una clave privada utilizando la clave pública, pues se requiere un de demasiado esfuerzo lo cual es un gran obstáculo para los interesados en descifrar dichas claves.

Aunque posee mayor potencia de cómputo para cifrar y descifrar en el método anterior; es más seguro al no tener la necesidad de ningún intercambio de clave de descifrado.

1.3.1.5 Clases de Certificado Digital

La clasificación de los certificados digitales depende de en qué medios hayan sido utilizados para verificar la veracidad de la información.

- Existen certificados que se utilizan para probar el procedimiento de firma digital, no tienen costo y se pueden descargar de la siguiente página : www.certificadodigital.com
- Por otro lado existen otros que certifican que la persona que posee el certificado es quien dice ser, y que la dirección de correo está bajo su control; para corroborar la identidad de la persona la Autoridad de registro solicita un documento que acredite, con la documentación de identificación oficial en el ámbito nacional.

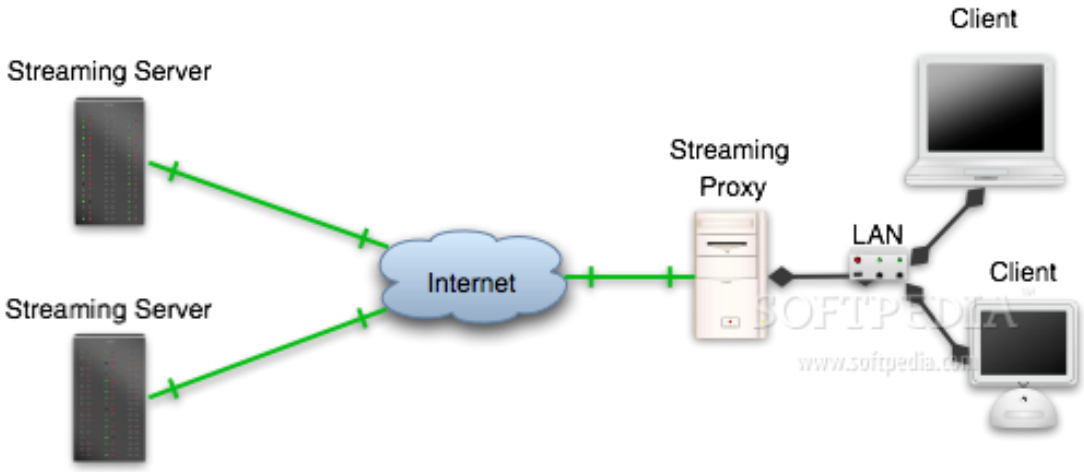
1.3.1.6 Autoridad de Certificación

Existe una autoridad de certificación que es responsable de brindar las herramientas para poder emitir, con calidad técnica de manera segura, el par de claves, público y privada, que constituye el eje de del certificado, así como también de:

- Asegurar su propia clave privada, que es la que se utiliza para aprobar las solicitudes.
- Garantizar la calidad técnica del sistema informático

1.3.2 Servidores Proxy

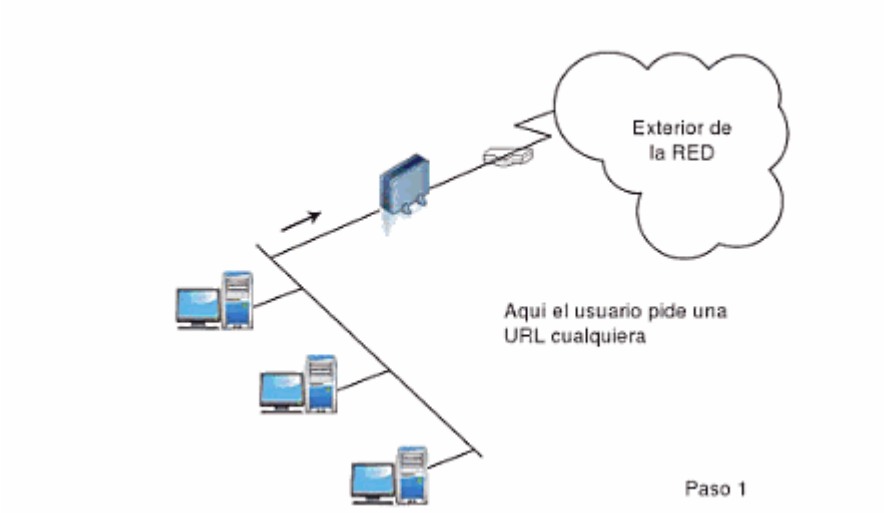
Un servidor proxy es un equipo o programa situado entre el sistema del usuario e internet para realizar una acción en representación de otro. Un servidor proxy intercepta conexión de red que un cliente hace a un servidor destino, los motivos pueden ser varios como seguridad, rendimiento y navegación anónima.



Fuente: Servidores Proxy * http://linux.softpedia.com/progScreenshots/RTSP-Caching-Proxy-Screenshot-6530.html

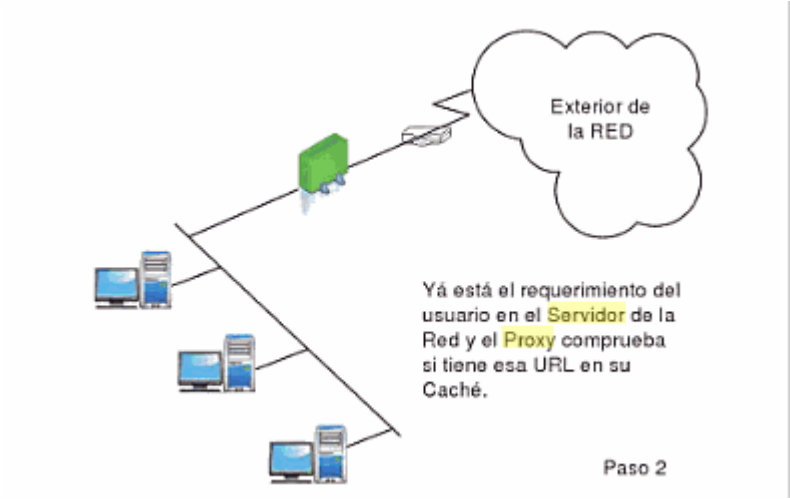
1.3.2.1Como funciona un servidor proxy

- El cliente realiza un petición cualquiera, pudiendo ser estar un petición http al puerto 80 a través de un navegador hacia un servidor web



Fuente: Funcionamiento de un servidor proxy Paso1 (Castillo, Sánchez, & Rodríguez, 2010)

- Cuando el servidor proxy recibe la petición busca en su memoria chache la página solicitada, si la encuentra verifica la fecha y la hora de la versión de la página con el servidor remoto. Si esta página no ha sido actualizada devuelve inmediatamente la página al solicitante, ahorrándose tiempo, y tráfico en la red. Si la página ya ha sido actualizada lo captura del servidor web y lo devuelve al solicitante, actualizando su cache para futuras peticiones.



Fuente: Funcionamiento de un servidor proxy Paso2 (Castillo, Sánchez, & Rodríguez, 2010)

Un servidor proxy también puede actuar como filtro, existen ciertas aplicación que están configuradas como proxies para que filtren el contenido de una página web.

Existen servidores proxy que cambian el formato de las páginas para acoplarse a ciertos requerimientos por parte de los usuarios, un claro ejemplo es el formato que un servidor proxy puede dar a una página para que esta se cargue en un Smartphone.

Otros servidores interceptan el contenido de la página para proteger a los usuarios de posibles amenazas por código malicioso como virus troyanos, etc.

1.3.2.2 Ventajas de utilizar un servidor proxy

Como se ha visto utilizar un servidor proxy como medidas de seguridad nos proporciona algunas ventajas:

- **Filtrado de contenido:** Un servidor tiene la calidad de hacer restricciones con respecto al tráfico o a los servicios, puede hacer un filtrado para que el tráfico generado por el cliente sea solo tráfico HTTP o solo SMTP, mejorando potencialmente la seguridad de una red.
- **Velocidad de respuesta:** Si un cliente realiza una petición de una página al servidor web, el servidor proxy intercepta esta petición busca en su cache si la encuentra lo enviar al cliente con una velocidad de respuesta superior
- **Modificación de contenido:** Un servidor proxy puede llegar a modificar el contenido de una página para un requerimiento especial por parte de un cliente
- **Ahorro de tráfico**: un servidor web disminuye el tráfico en una red, ya que si el contenido está alojando en la cache del servidor proxy, este solo hace una consulta para ver si ha existido alguna modificación, si no es así el servidor se encargar de enviar la información al cliente directamente desde su cache, y no desde un servidor destino.

1.3.2.3 Desventajas de utilizar un servidor proxy

- **Caducidad de la información:** la información que puede estar almacenada en la cache de un servidor proxy no siempre está actualizada, sobre todo si no se ha realizado ninguna consulta del cliente sobre una página ya consultada anteriormente, generalmente el contenido de una página es modificada con frecuencia, y si no se ha consultado esta información recientemente puede estar desactualizada.
- **Restricciones técnicas:** para cierto tipo de usuarios, sobre todo si no tiene una política de seguridad establecida en cuanto al tipo de tráfico que debe generar en la red puede resultar molestoso la restricciones

que un servidor proxy proporcionar, el cliente puede requerir navegar libremente en la red, realizar cualquier tipo de peticiones al servidor destino.

1.3.2.4 Tipos de Proxies

- **Proxies Transparentes**

Son utilizados por muchas empresas y usuarios comunes para reforzar la seguridad en la red, normalmente un servidor proxy no es transparente al cliente, mientras que un servidor de este tipo transparente puede ser configurado manualmente por el usuario, por lo que puede decidir navegar o no en una red bajo la protección de un proxy.

- **Proxies inverso**

Es un servidor alojando en un servidor web destino, todo el tráfico pasa por este servidor proxy, existen varias razones para instalar un servidor de este tipo

- **Proxies de Seguridad**

Actúa como protectores de un servidor web ya que todo el tráfico pasa por este servidor

Cuando se crea un servidor web generalmente el cifrado SSL es realizado por el proxy y no por el servidor web, el servidor proxy es equipado con hardware de aceleración SSL (Secure Socket Layer).

Balanceo de carga: muchas veces un servidor proxy inverso puede estar destinado al balanceo de carga entre los diferentes servidores web, para mejorar el rendimiento, en este caso este servidor puede llegar a reescribir las URLs (traducción de la URL externa a la URL interna según el servidor en que se encuentre la información).

- **Proxies NAT (Network Address Translations)**

NAT se utiliza para hacer traducciones de IPs, necesario cuando varios equipos acceden a internet bajo una misma conexión. Un dispositivo es encargado de

realizar la traducción de una dirección ip privada a una ip pública, en este caso el servidor proxy será el encargado de realizar esta traducción de direcciones y de distribuir las páginas a los clientes que hicieron la petición.

Gran parte de empresas utilizan un servidor proxy NAT para que realice esta tarea, la razón principal es la seguridad que proporcionar, al tener múltiples usuarios y una sola conexión a internet es posibles que todos los equipos estén expuesto a ataques directos desde el internet.

1.4 Redes VLAN

Supongamos que en el campus universitario existe un edificio con una red LAN para los estudiantes y otra red LAN para el personal docente, después de un tiempo la universidad cuenta con otro edificio con estudiantes y docentes, sin embargo el departamento de seguridad quiere que todas las computadoras de los estudiantes en los dos edificios compartan las mismas características de control y seguridad , ¿ cómo hacer para cumplir con este requerimiento si los departamentos están separados geográficamente? Realizar una conexión física para todas las computadoras, el objetivo del departamento de seguridad es ahorrar recursos y facilitar la administración de la seguridad y la red.

Una solución a esta interrogante, es la utilización de VLAN, esta es una tecnología LAN virtual, permite al administrador de red crear un grupos virtuales de dispositivos de manera lógica, estos dispositivos se comportara como si estuvieran en una red independiente, así comparta una infraestructura común con otras VLAN.

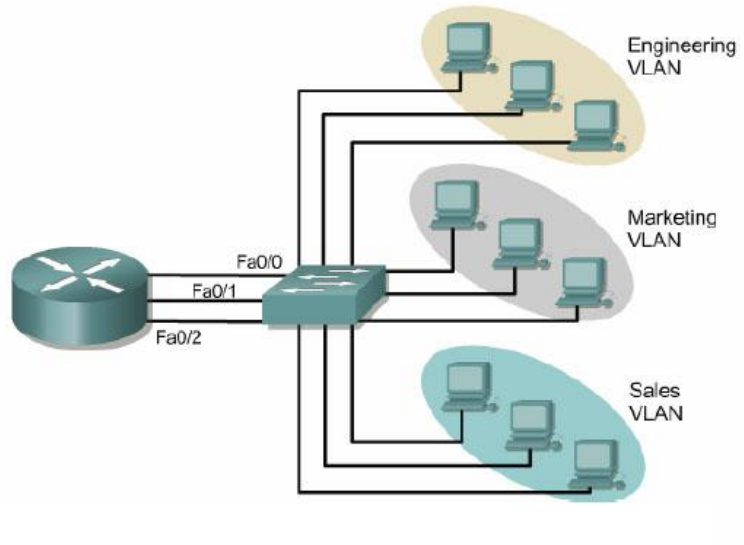
1.4.1 Definición

Una VLAN (red de área local virtual) es una manera de crear redes lógicamente independientes dentro de una misma red física. Nos ayudan a reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.

Los administradores de red configuran las VLANS mediante software en lugar de hardware, lo que las hace flexibles. Una de las mayores utilidades de las VLANS surge cuando se traslada físicamente un equipo de un lugar a otros: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

1.4.2 Detalles de las VLAN

- Una VLAN es una red LAN independiente no de manera física sino lógica
- Un VLAN permite segmentar varias pc's independientemente de si comparten una misma conexión física
- Se puede asignar un nombre a cada VLAN para identificar su función
- El uso de VLANS no ayuda también a reducir la contención por el uso de la red.
- También permite balancear la carga de la red
- Facilita agregar y cambiar de lugar los equipos reduciendo costos de administración
- Nos ayuda a implantar políticas de seguridad



Red segmentada en 3 redes VLAN

Fuente: CCNA3 (LAN switching and wireless)

1.4.3 Ventajas de la VLAN

- **Seguridad:** la segmentación de la red, hace que los usuarios no tengan acceso a toda la red de una empresa, por lo tanto no tienen acceso a todos los datos por lo que disminuye la posibilidad de que existan violaciones de información confidencial.
- **Rendimiento**: la división logia de una red en grupos de trabajo más pequeños, reduce el tráfico innecesario que puede darse y potencia el rendimiento.
- **Reducción de costos**: si segmentamos una red por capa 2 y de forma logia reducimos costos de enlaces, ancho de banda y conexiones físicas ya que no será necesario.
- **Facilidad de administración:** con la implementación de VLAN mejoramos de manera significativa la administración de la red, podemos tener usuarios agrupados por requerimientos similares compartiendo una misma VLAN, se podrá identificar al función de una VLAN de acuerdo a su nombre, si queremos adicionar un cliente a un grupo se deberá asignar un puerto en un rango que pertenezca a cierta VLAN, lo que hace que sea un proceso sencillo.

1.4.4 Administración de VLAN

Planificación de las capacidades:

- Tamaño de las VLANs
- Numero de VLANs
- Número de usuarios de cada VLAN
- Perfiles de tráfico
- Tamaño del dominio de ejecución del algoritmo STP (spanningtreeProtocol)

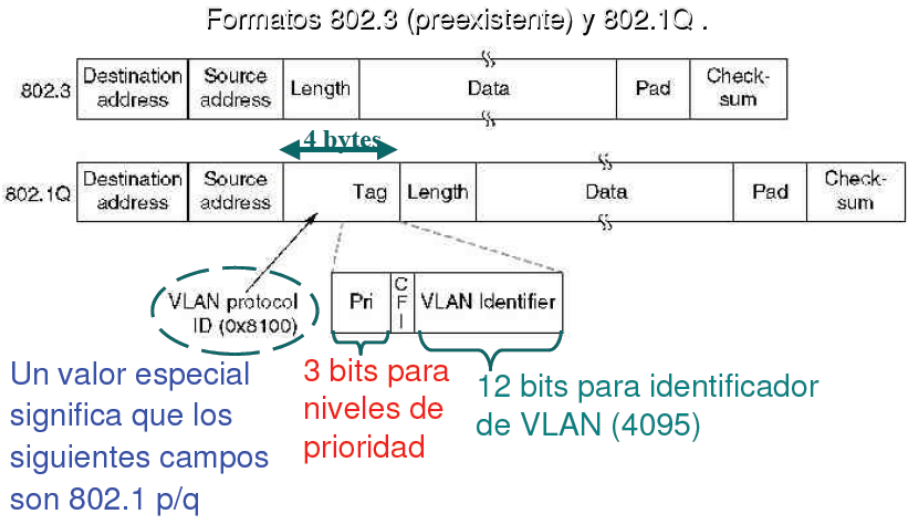
Seguridad:

- Aislar subredes de acuerdo a la privacidad
- Ubicación de servidores en sitios seguros

1.4.5 Estándares relacionados

IEEE para VLANs (802.1q) y Calidad de Servicio a nivel de capa MAC o 2 de OSIesta incluye la posibilidad de especificar prioridades en "flujos", que es utilizado por 802.1p el cual puede ser utilizado para QoS en capas superiores (RSVP).

Trama IEEE 802.1 P/Q



Fuente: Redes locales Virtuales Emilio Hernández, Carlos Figueira

En la actualidad la implementación de las VLAN está basada en los puertos, la VLAN es asociada a un puerto denominado puerto de acceso.

1.4.6 Tipos de VLAN más comunes son:

- **VLAN de Datos:** Llamada también VLAN de usuario, esta VLAN está configurada para enviar solo tráfico de datos generado por usuarios, es muy conveniente separa el trafico que se genera en la red, en una VLAN de datos no es conveniente generar tráfico de voz de administración
- **VLAN Nativa:** Esta VLAN está asociada a un puerto troncal 802.1 Q que permite tráfico etiquetado y no etiquetado. EL puerto de enlace 802.1 Q coloca el tráfico que llega de otras VLAN así como el tráfico que no llega de otras VLAN en una VLAN nativa.

- **VLAN predeterminada:** Cuando se inicia un switch todos los puertos pertenecen a una VLAN predeterminada, por lo general cuando no se ha realizado ninguna configuración de VLAN todos los puertos pertenecen a esta VLAN haciendo que todos sean parte de un mismo dominio broadcast generalmente esta vlan es la VLAN1.
- **VLAN de administración:** esta es una VLAN que el usuario configura para configurar las capacidades de un switch y poder administrarlas de mejor manera, generalmente esta VLAN es la predeterminada es decir la VLAN1. Por seguridad no es recomendable dejar a la VLAN1 como VLAN de administración, a una VLAN de administración se le debe asignar una dirección IP y una máscara para poder acceder y manejar un switch.
- **VLAN de Voz**: por cuestiones de rendimiento es aconsejable tener una VLAN de voz, si una organización maneja este tipo de tráfico ya que este tipo de tráfico requería un ancho de banda garantizado y prioridad de transmisión.

CAPÍTULO 2: ANÁLISIS DEL ENTORNO ACTUAL

2.1 Descripción actual Del objeto de Estudio

La red el Hospital Santa Inés esta segmentada en dos grupos que son: red pública y red privada, esto con el fin de mejorar el rendimiento y facilitar la administración de la red. Esta segmentación resulta muy útil a la hora de asignar un usuario a la red, la segmentación ayuda a tener un mayor control sobre los usuarios y podemos hacer una distinción entre usuarios de una u otra red mejorando ciento por ciento la administración. Como mencionamos la red del Hospital esta segmentada en dos subredes, las cuales se detallan a continuación:

Red privada está comprendida por:

- Personal Administrativo
- Enfermería
- Tomografía
- Rayos X
- Contabilidad
- Gerencia
- Informática
- Mantenimiento
- Ingeniería Clínica
- Emergencia
- Cuidados Intensivos
- Farmacia
- Quirófanos

La red pública está comprendida por:

- Consultorios
- Hotelería
- Red Inalámbrica

2.2 Análisis de Seguridad

De acuerdo a un análisis de la red segmentada podemos identificar los siguientes focos de inseguridad en la red pública la cual será objeto de nuestro estudio.

La red pública del Hospital Santa Inés necesita mejorar y organizar las políticas de seguridad de acuerdo a los siguientes parámetros:

- el acceso a la red
- los horarios disponibles para acceder a la red
- los usuarios que accederán a la red

2.2.1 El acceso a la red

Los usuarios que acceden a la red pública del Hospital Santa Inés, puede realizar cualquier acción, no tiene ningún filtro a la hora de navegar a través de la red, pueden realizar descargas, subir contenido a la web, ver videos en línea, lo cual consume un excesivo ancho de banda, dejando fuera a usuarios que realmente necesitan el servicio. Por otro lado cuando se establece una conexión a la red el usuario no tiene ningún servidor proxy u otro tipo de mecanismo que controle y mejore el rendimiento de esta red.

Para mejorar en este sentido y estructurar mejor la seguridad se realizara la configuración de un servidor proxy, que permitirá establecer filtros de navegación, limitación de descargas en línea, mejorar la velocidad de acceso.

2.2.2 Horarios de acceso a la red

Los horarios de acceso a un red puede resultar muy convenientes sobre todo para mejorar significativamente el control de la red, los usuarios fijos deberán tener un horario de acceso para mejorar la calidad de acceso, los usuarios deberán tener acceso a la red los en los horarios que previamente serán establecidos.

Para establecer horarios a los usuarios fijos, se les categorizara por grupos, estos grupos tendrán un horario común. Por ejemplo una asignación de horario para

el personal de Recepción de consultorios el horario será de 8h00 a 18h30 de lunes a sábado.

2.2.3 Usuarios que accederán a la red

Es necesario conocer quiénes son los usuarios que acceden a la red para monitorear sus actividades si así fuera el caso. Se puede categorizar a los usuarios por grupos para establecer reglas de navegación y controlar mejor las actividades que estos realicen esto aplica a usuarios fijos como son personal administrativo y médico.

Una vez que se tenga categorizados los usuarios por grupos, estos deberán sujetarse a una regla y horarios de navegación.

2.3 Delimitar el Campo de Estudio

El campo de concentración será la red pública del Hospital Santa Inés, en esta red se identificara cada foco de inseguridad para reestructurar las política existentes o implementar nuevas políticas de seguridad, todo el análisis a realizarse se lo hará en esta red (red pública del Hospital Santa Inés) la cual necesita un control, mejorar la administración, la seguridad y el rendimiento en general. En un futuro cercano esta red contara con la ampliación para lo que es red dedicada de consultorios, el análisis realizado servirá también para esta red, como lo muestra el siguiente diagrama de red.

Diagrama de red del Hospital Santa Inés

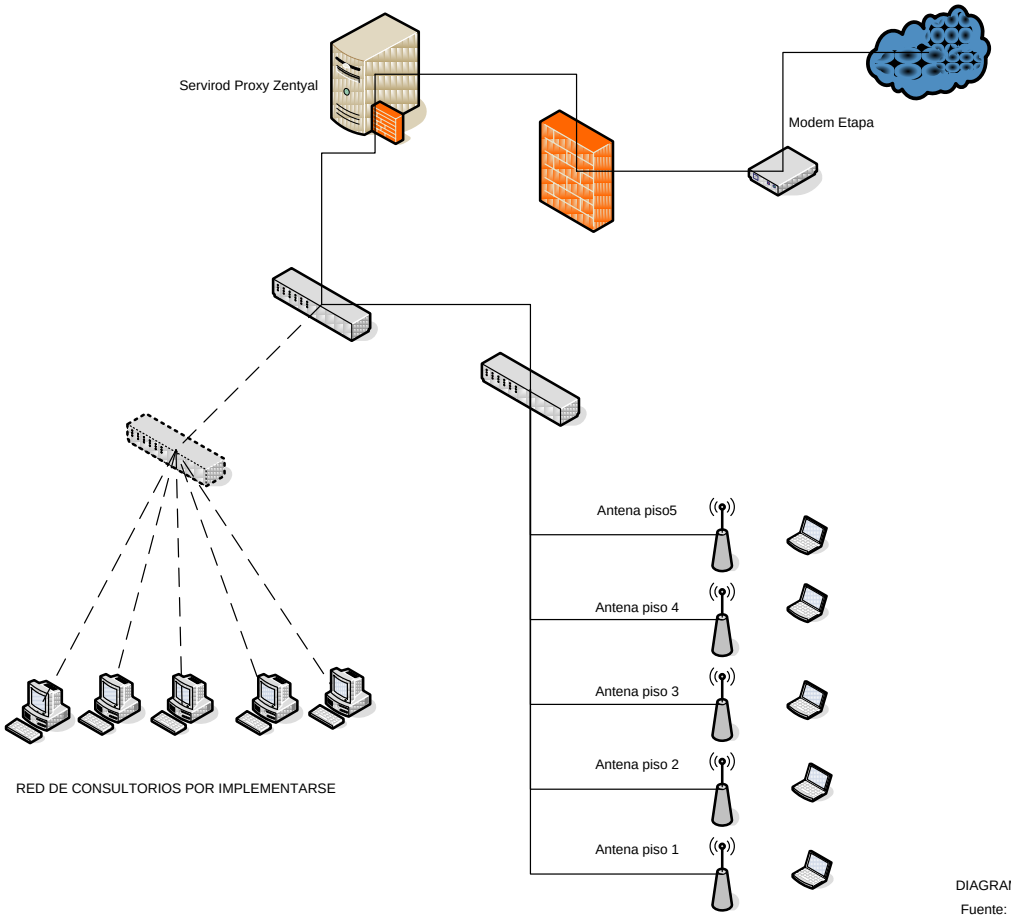


DIAGRAMA DE RED HOSPITAL SANTA INES
Fuente: Desarrollado por el Autor

CAPÍTULO 3: PROPUESTA TÉCNICA

3.1 Análisis y administración de la herramienta Zentyal para manejo de políticas de seguridad

Esta herramienta conocida en épocas anteriores como eBoxPlatform, es un servidor de código abierto para las PYMEs, puede actuar en diferentes ámbitos tales como la infraestructura de red, como puerta de enlace a Internet(Gateway), gestionando la seguridad (UTM), así como también como servidor de comunicaciones y servidor de oficina al mismo tiempo; dentro de esta herramienta también se encuentra un framework para hacer fácil la implementación de nuevos servicios basados en Unix.

3.1.1 Zentyal Gateway

Nos permite configurar un cortafuegos de alta seguridad, también reglas de enrutamiento avanzadas para múltiples conexiones de internet, esto incluye balanceo de carga y tolerancia a fallos. Ofrece proxy HTTP cachea las páginas web mejorando la velocidad de navegación, filtrando contenidos y descartando las amenazas web con distintos perfiles de usuario. El módulo Radius proporciona seguridad para redes WIFI con autenticación centralizada.

3.1.2 Balanceo de Carga y Disponibilidad

Esta característica tiene como objetivo estar siempre conectado, con múltiples conexiones a internet, puedes distribuir el tráfico de forma trasparente y seguir conectado aunque las conexiones sufran algún fallo. Se puede definir conexiones para VozIP o entre sedes.

3.1.3 Moldeado de Tráfico y QoS

Este módulo se encarga de priorizar el tráfico o usuarios y garantiza que el tráfico crítico se sirve siempre con calidad, de manera independiente de la carga de red. Se puede evitar P2P o descargas que consumen el ancho de banda.

3.1.4 Caché Transparente

Para una conexión de internet más rápida los datos se descargan una sola vez si es que los usuarios han visitado las mismas páginas web, de esta manera la velocidad de navegación se incrementa y reduce el consumo de ancho de banda en el tráfico.

3.1.5 Filtro de Contenido Web

Como política de seguridad Zentyal bloquea el contenido peligroso, controla el acceso a sitios inapropiados o se puede filtrar el acceso a sitios específicos. Monitorea la navegación de usuarios y ayuda a cumplir las políticas de uso de internet ofreciéndonos un entorno de trabajo seguro.

3.1.6 Instalación

Zentyal puede ser instalado en una máquina real o virtual. Esto no impide que se puedan instalar otros servicios adicionales, no gestionados a través de la interfaz de Zentyal, que deberán ser instalado y configurados manualmente.

La versión para servidores funciona perfectamente sobre Ubuntu.

La instalación la hemos realizado mediante el instalador la cual se recomienda, así como también seguir los siguientes pasos:

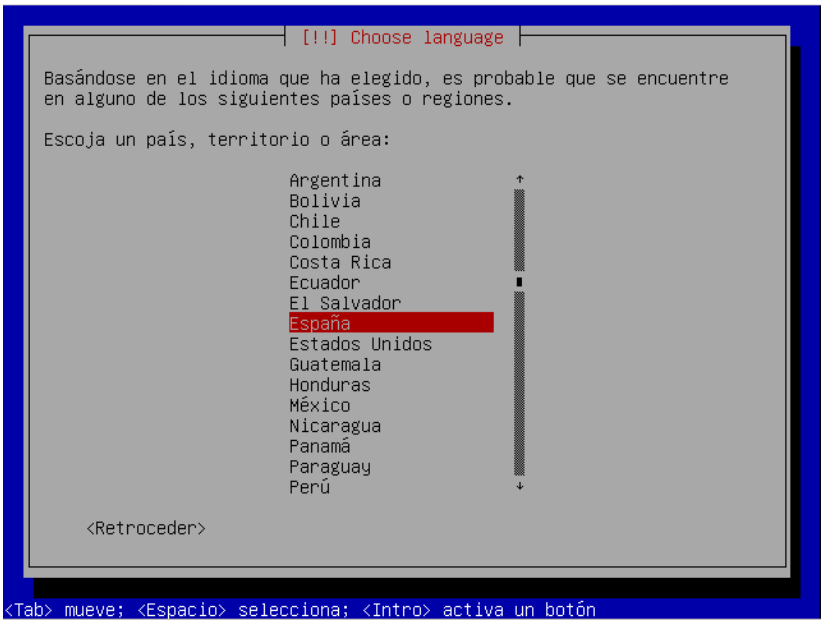
- Para empezar seleccionaremos el lenguaje de la instalación, lo cual en nuestro caso es español.

Fuente: Selección del idioma *http://doc.zentyal.org/es/installation.html

- Los usuarios debemos elegir la opción por omisión a no ser que estén instalando en un servidor con RAID por software o quieran hacer un particionado más específico a sus necesidades concretas.

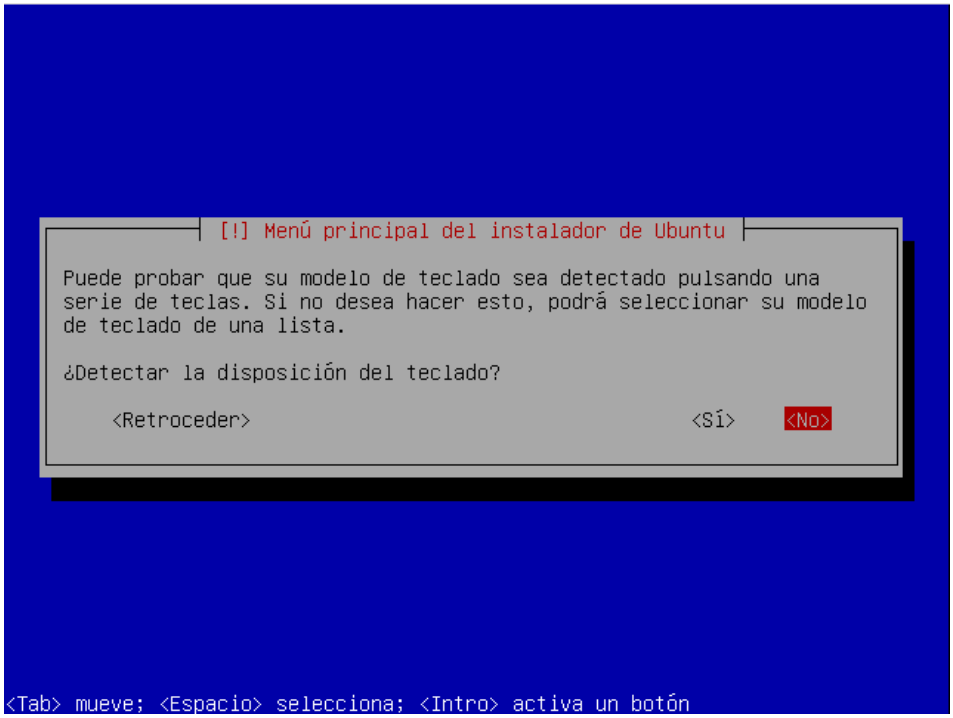
Fuente: Inicio del instalador * http://doc.zentyal.org/es/installation.html

- En el siguiente paso elegiremos el lenguaje que usará la interfaz de nuestro sistema una vez instalado, para ello nos pregunta por el país donde nos localizamos, en este caso España.



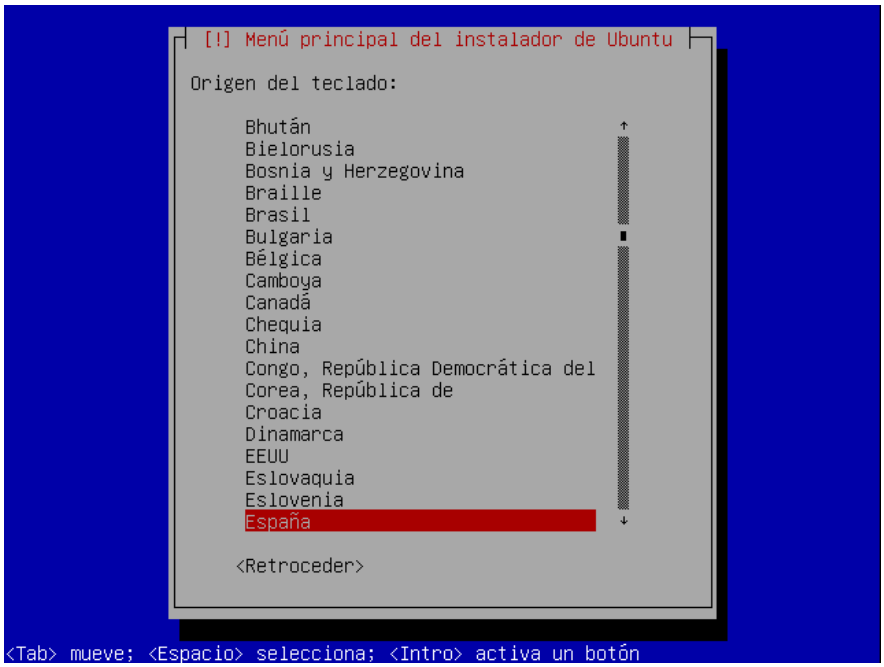
Fuente: Localización geográfica * http://doc.zentyal.org/es/installation.html

- Podemos usar la detección de automática de la distribución del teclado, que hará unas cuantas preguntas para asegurarse del modelo que estamos usando o podemos seleccionarlo manualmente escogiendo No.



Fuente: Auto detección del teclado *

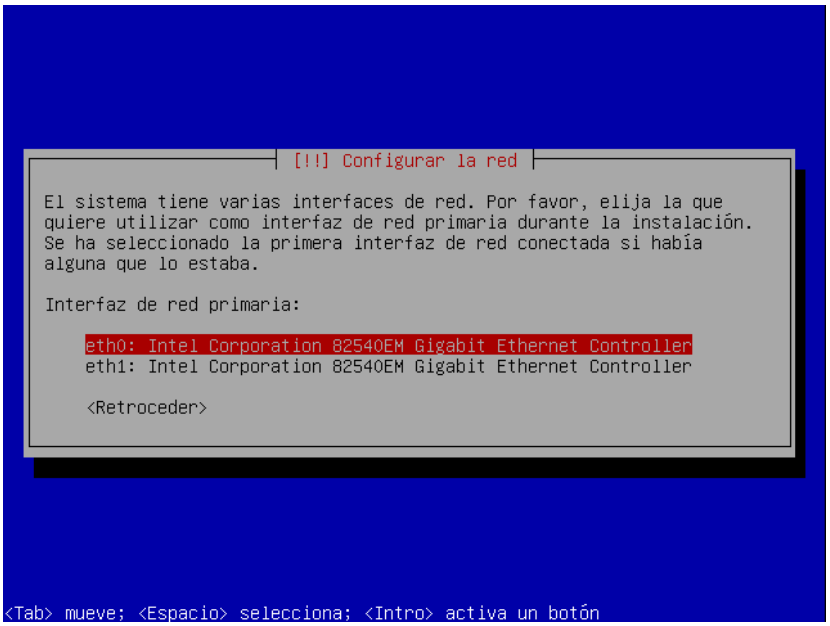
http://doc.zentyal.org/es/installation.html



Fuente: Selección del teclado *

http://doc.zentyal.org/es/installation.html

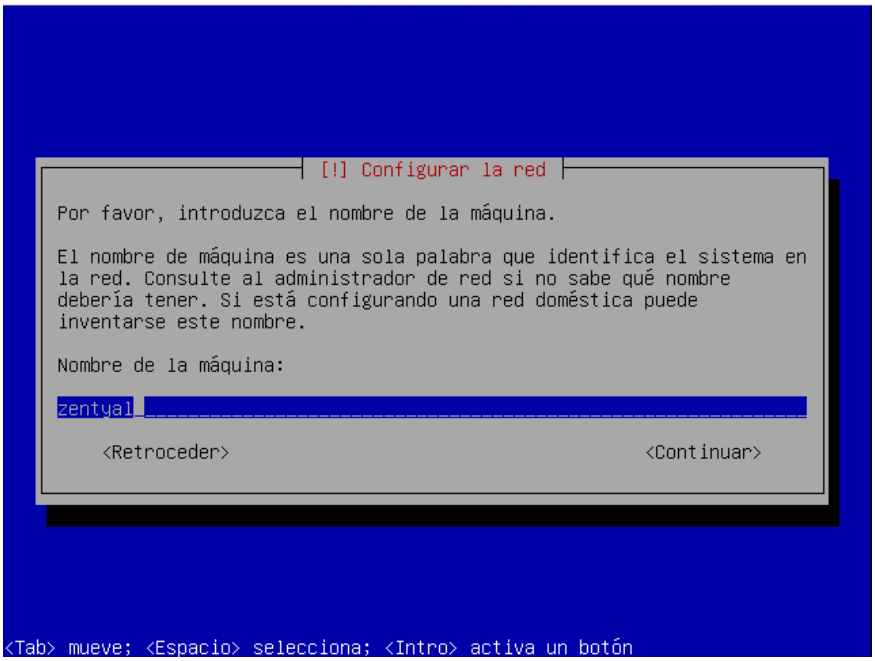
- En caso de que dispongamos de más de una interfaz de red, el sistema nos preguntará cuál usar durante la instalación (por ejemplo para descargar actualizaciones). Si tan solo tenemos una, no habrá pregunta.



Fuente: Selección de interfaz de red *

http://doc.zentyal.org/es/installation.html

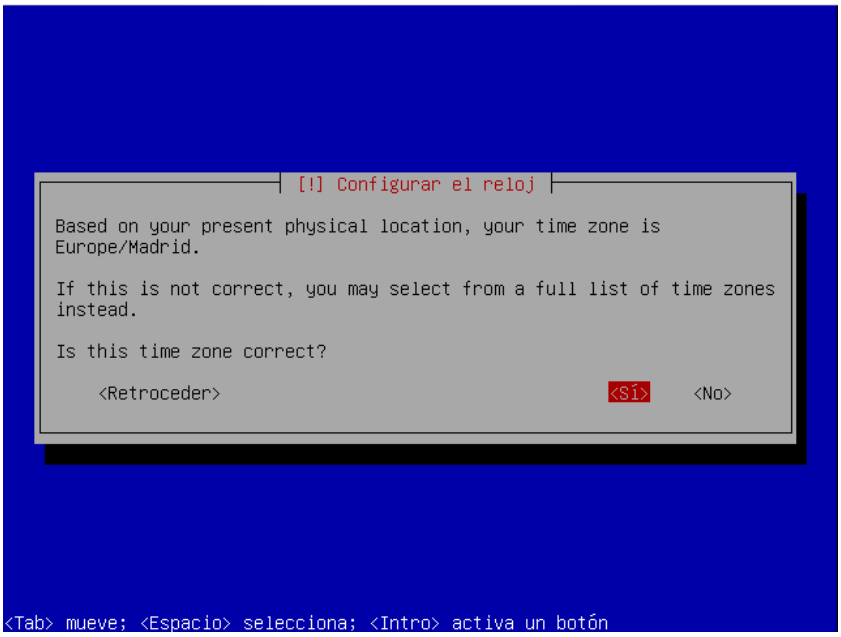
- Después elegiremos un nombre para nuestro servidor; este nombre es importante para la identificación de la máquina dentro de la red.



Fuente: Nombre de la máquina *

http://doc.zentyal.org/es/installation.html

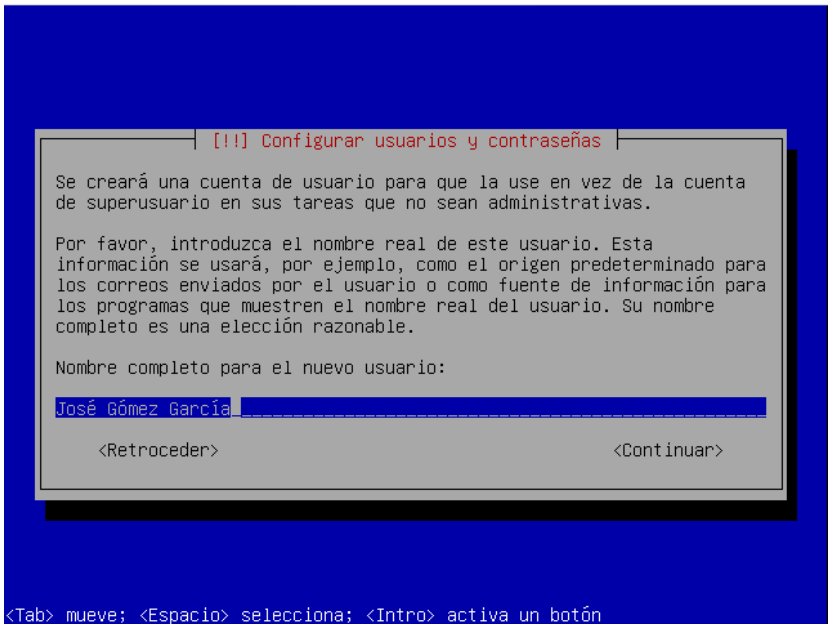
- En el siguiente paso, se nos pregunta por nuestra zona horaria, que se auto configurará dependiendo del país de origen que hayamos seleccionado anteriormente, pero se puede modificar en caso de que sea errónea.



Fuente: Zona horaria * http://doc.zentyal.org/es/installation.html

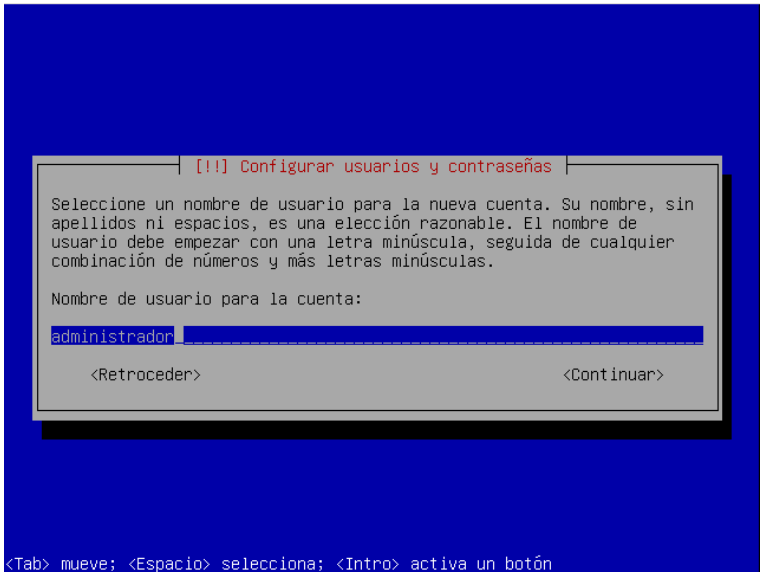
- Una vez terminados estos pasos, comenzará la instalación que irá informando de su estado mediante el avance de la barra de progreso.

- A continuación se nos pregunta por el nombre real del administrador.



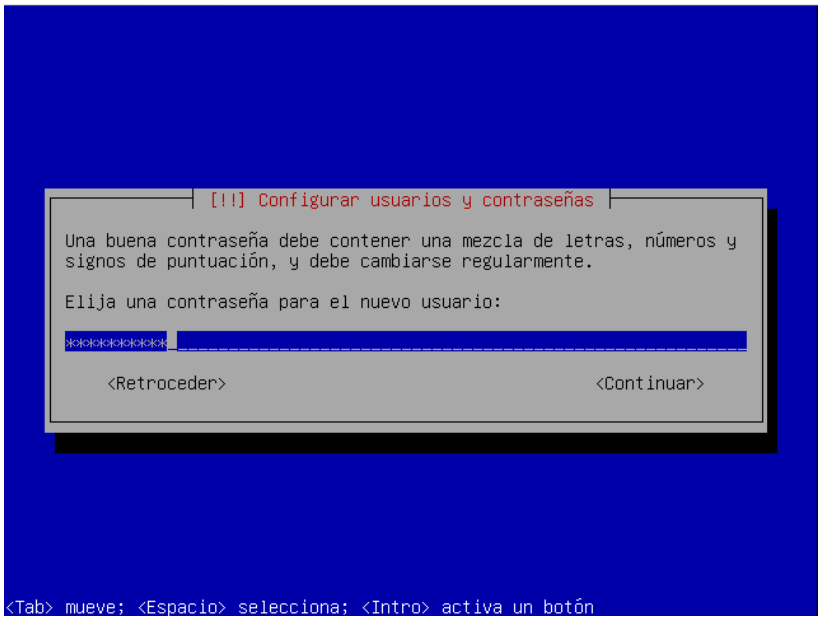
Fuente: Nombre del usuario * http://doc.zentyal.org/es/installation.html

- Después, habrá que indicar el nombre de usuario o login usado para identificarse ante el sistema. Este usuario tendrá privilegios de administración y además será el utilizado para acceder a la interfaz de Zentyal.



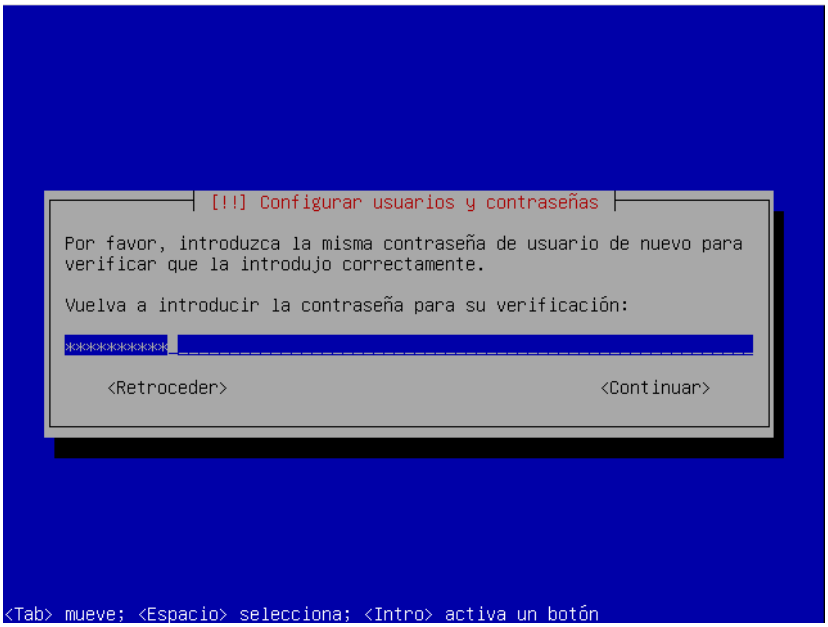
Fuente: Nombre de usuario en el sistema * http://doc.zentyal.org/es/installation.html

- En el siguiente paso nos pedirá la contraseña para el usuario. Cabe destacar que el anterior usuario con esta contraseña podrá acceder tanto al sistema (mediante SSH o login local) como a la interfaz web de Zentyal, por lo que seremos especialmente cuidadosos en elegir una contraseña segura (más de 12 caracteres incluyendo letras, cifras y símbolos de puntuación).



Fuente: Contraseña * http://doc.zentyal.org/es/installation.html

- E introduciremos de nuevo la contraseña para su verificación.



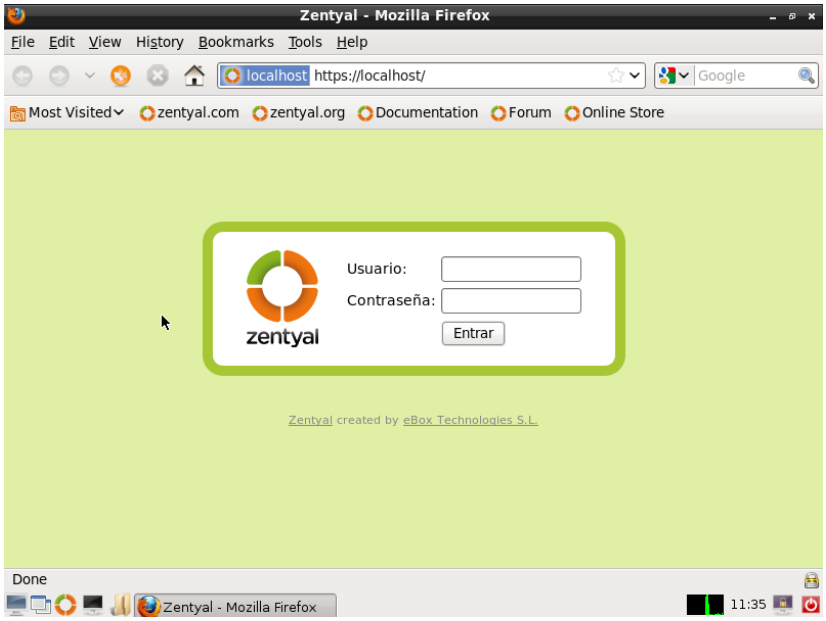
Fuente: Confirmar contraseña *

http://doc.zentyal.org/es/installation.html

- La instalación del sistema base está completada; ahora podremos extraer el disco de instalación y reiniciar.

Fuente: Terminar * http://doc.zentyal.org/es/installation.html

- El sistema arrancará un interfaz gráfico con un navegador que permite acceder a la interfaz de administración, y, aunque tras este primer reinicio el sistema haya iniciado el entorno gráfico automáticamente, de aquí en adelante, necesitará autenticarse antes de que éste arranque.



Fuente: Entorno gráfico con la interfaz de administración *
http://doc.zentyal.org/es/installation.html

- Para la configuración de los módulos se usa el usuario y contraseña indicados durante la instalación, para otro usuario añadido luego al grupo admin podrá acceder a la interfaz de igual manera tendrá privilegios de sudo en el sistema.
- Para poder comenzar con la configuración para poder utilizar esta herramienta podemos seleccionar los paquetes que requerimos según nuestras necesidades.

Fuente: Perfiles de paquetes instalables *
http://doc.zentyal.org/es/installation.html

Los perfiles con los que cuenta Zentyal son:

- **Gateway**

Actúa como puerta de enlace de la red local ofreciendo un acceso a internet seguro y controlado.

Administrador de Amenazas

Protege la red local contra ataques, intrusiones, amenazas a la seguridad interna y posibilita la interconexión entre redes locales a través de internet.

- **Infraestructura**

Gestiona la infraestructura de la red local con los servicios básicos: DHCP,DNS,NTP, servidor HTTP.

- **Office**:

Se puede utilizar como servidor de recursos compartidos de la red local como: ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos.

- **Comunicaciones Unificadas:**

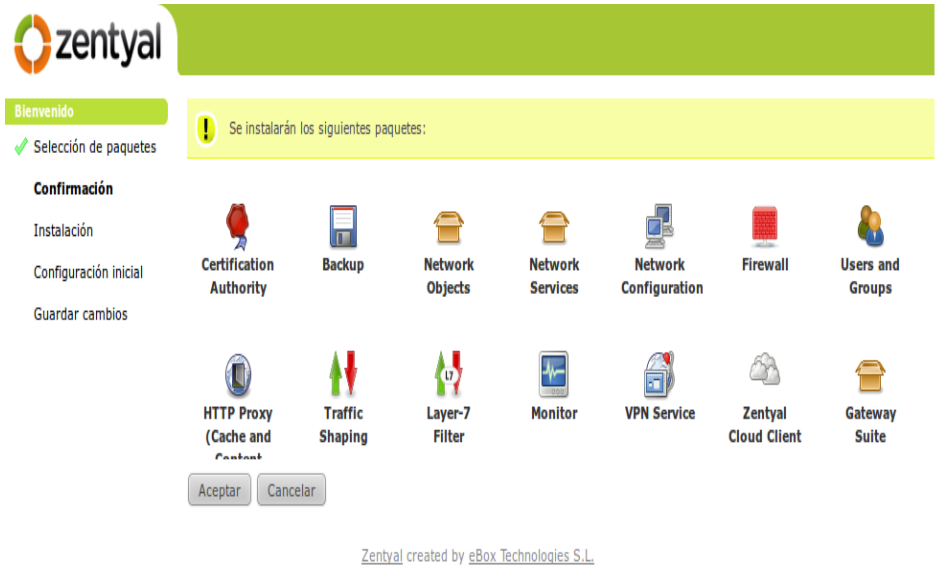
Es un centro de comunicaciones para las empresas, incluye correo, mensajería instantánea y Voz IP.

Podemos seleccionar varios perfiles para hacer que Zentyal tenga, de forma simultánea, diferentes roles en la red.

También podemos instalar un conjunto manual de servicios simplemente dando un clic sobre sus respectivos iconos sin necesidad de amoldarnos a los perfiles, o bien, instalar un perfil más unos determinados paquetes que también nos interesen.

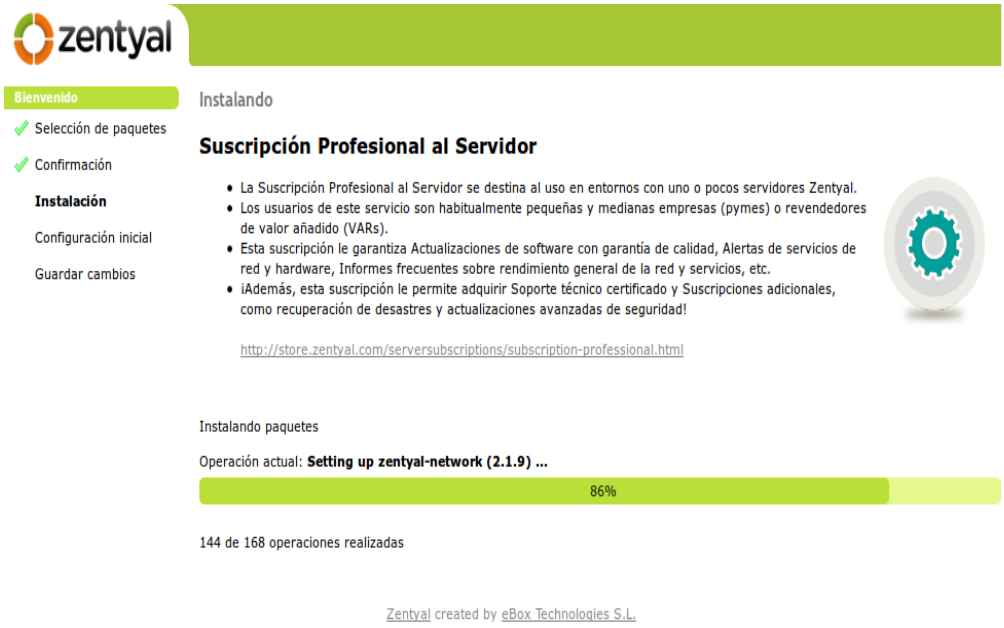
Vamos a usar la instalación del perfil de Gateway que es uno de nuestros perfiles necesarios.

Al terminar la selección, se instalarán también los paquetes adicionales necesarios y además si hay algún complemento recomendado se preguntará si lo queremos instalar. Esta selección no es definitiva, ya que posteriormente podremos instalar y desinstalar el resto de módulos de Zentyal a través de la gestión de software.



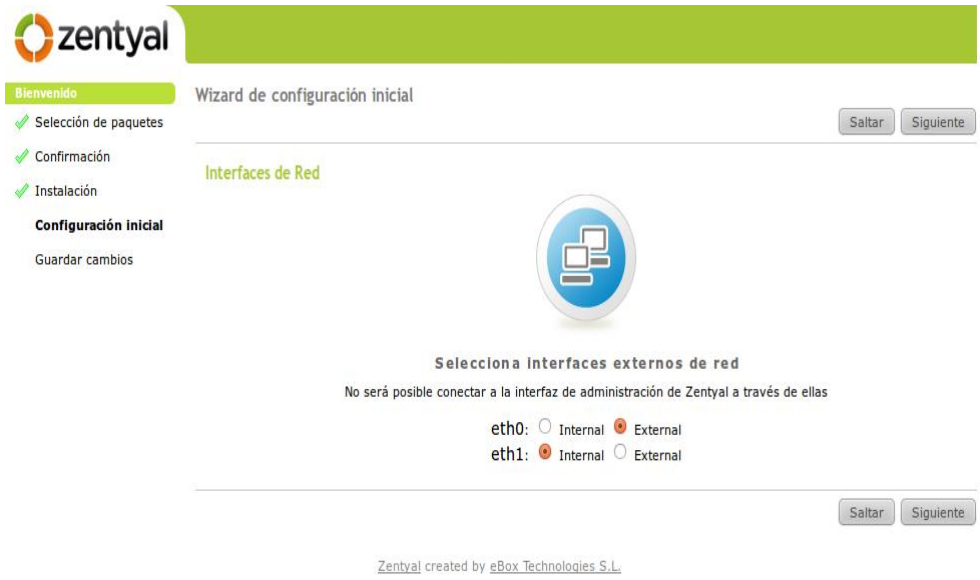
Fuente: Paquetes adicionales * http://doc.zentyal.org/es/installation.html

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso.



Fuente: Instalación e información adicional *
http://doc.zentyal.org/es/installation.html

En primer lugar se solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es interna o externa, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Se aplicarán políticas estrictas en el cortafuegos para todo el tráfico entrante a través de interfaces de red externas.



Fuente: Seleccionar el modo de interfaces de red *
http://doc.zentyal.org/es/installation.html

A continuación tendremos que seleccionar el tipo de servidor para el modo de operación del módulo Usuarios y Grupos. Si sólo vamos a tener un servidor elegiremos Servidor stand-alone. Si por el contrario estamos desplegando una infraestructura maestro-esclavo con varios servidores Zentyal y gestión de usuarios y grupos centralizada o si queremos sincronizar los usuarios con un Microsoft Active Directory, elegiremos Configuración avanzada. Este paso aparecerá solamente si el módulo Usuarios y Grupos están instalados. Configurar el modo de Usuarios y Grupos puede tomar unos minutos.

Fuente: Modo de operación de usuarios y grupos *
http://doc.zentyal.org/es/installation.html

El último asistente permite suscribir el servidor a Zentyal Cloud. En caso de tener una suscripción registrada tan sólo es necesario introducir los credenciales. Si todavía no se tiene un usuario en Zentyal Cloud es posible registrar automáticamente una cuenta con suscripción básica gratuita.

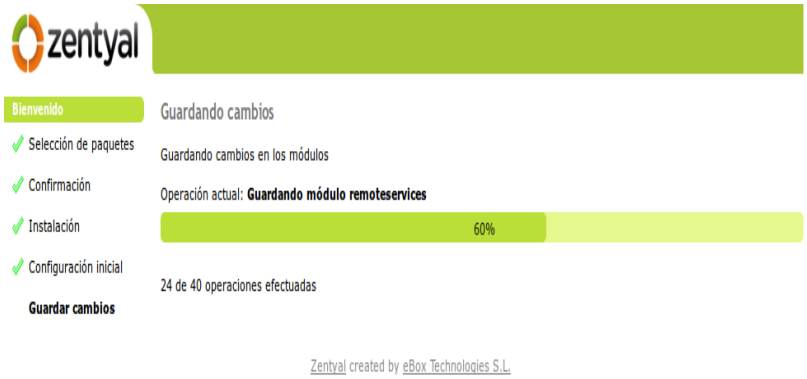
En ambos casos el formulario solicita un nombre para el servidor. Éste es el nombre que lo identificará dentro de la interfaz de Zentyal Cloud.

Asistente de suscripción a ZentyalClo

Fuente: Asistente de configuración de zentyal Cloud *
http://doc.zentyal.org/es/installation.html

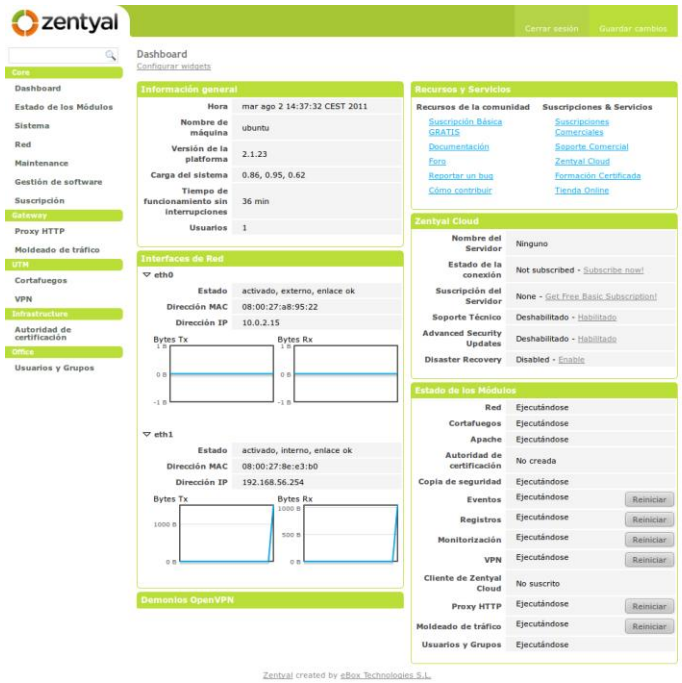
Una vez hayan sido respondidas estas preguntas, se procederá a la configuración de cada uno de los módulos instalados.

Fuente: Configuración inicial finalizada * http://doc.zentyal.org/es/installation.html



Fuente: Guardando cambios * http://doc.zentyal.org/es/installation.html

Cuando finalice el proceso de guardar cambios ya podremos acceder al Dashboard.



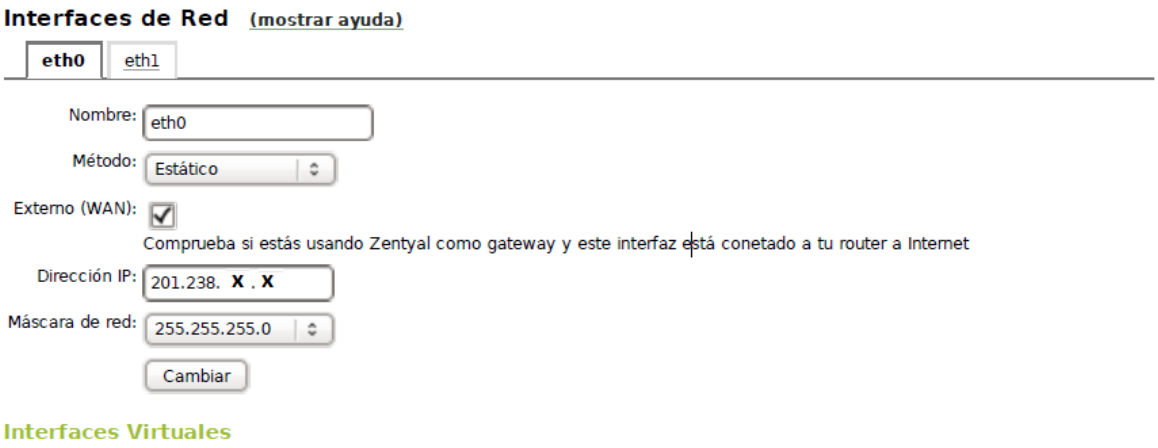
Fuente:Dashboard * http://doc.zentyal.org/es/installation.html

3.2 Implementación de un Servidor Proxy

Para comenzar con la implementación de políticas y reglas de seguridad en el Hospital Santa Inés, empezaremos con la configuración de las interfaces del Equipo Zentyal destinado a ser el proxy de la red.

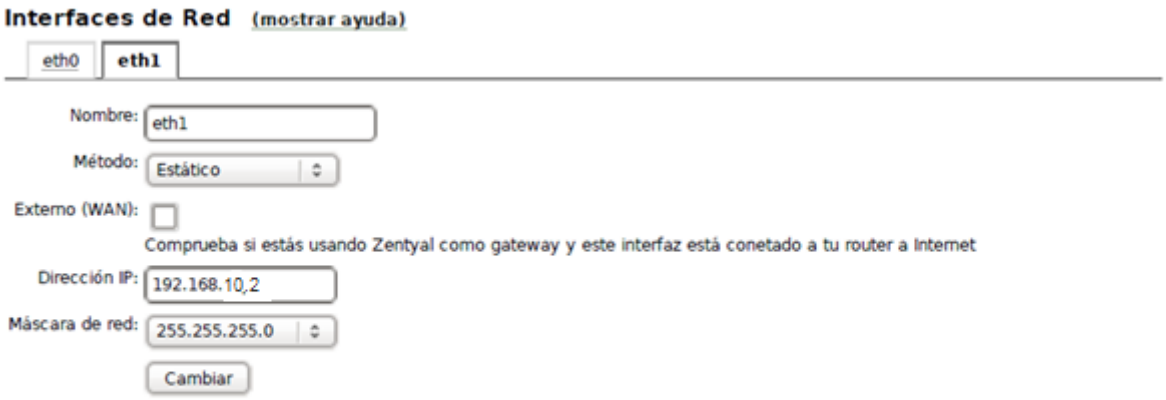
En el Equipo Zentyal, el cual vamos a configurar, tendremos dos tarjetas de red (eth0 y eth1) como se indican en las figuras siguientes. Para ello iremos a Red-> Interfaces y nos mostrara todas las interfaces que tengamos en el equipo, en este caso nos mostrara las dos interfaces.

Interface Eth0: esta interfaz va a estar conectada directamente al modem Etapa con la dirección IP: 201.238.X.X (Oculto por Confidencialidad), para que actué como filtro entre la red interna y la nube.



Fuente: Desarrollado por el Autor

Interface Eth1: esta interface es la que va a conectarse a la red interna del Hospital con la IP: 192.168.10.2

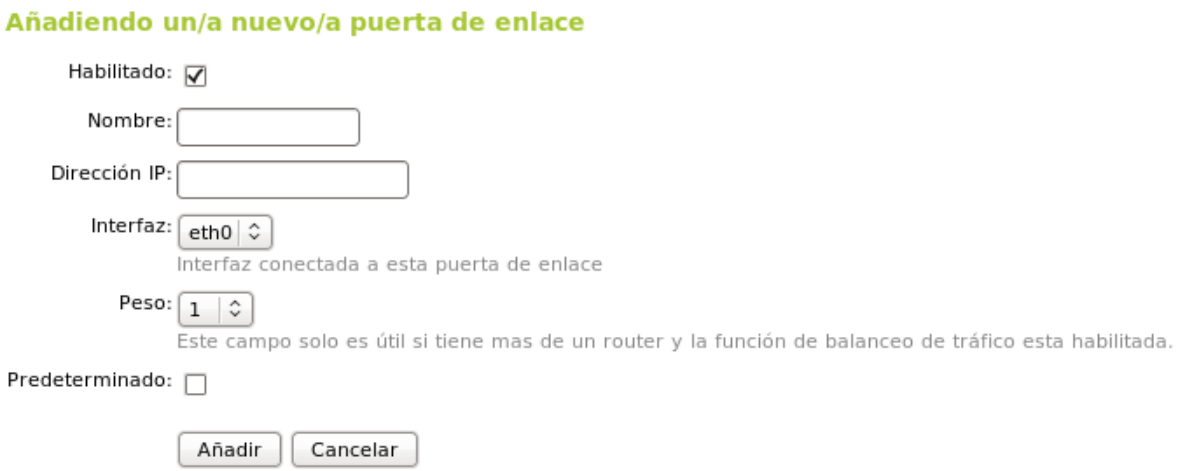


Fuente: Desarrollado por el Autor

3.2.1 Puertas de enlace Proxy

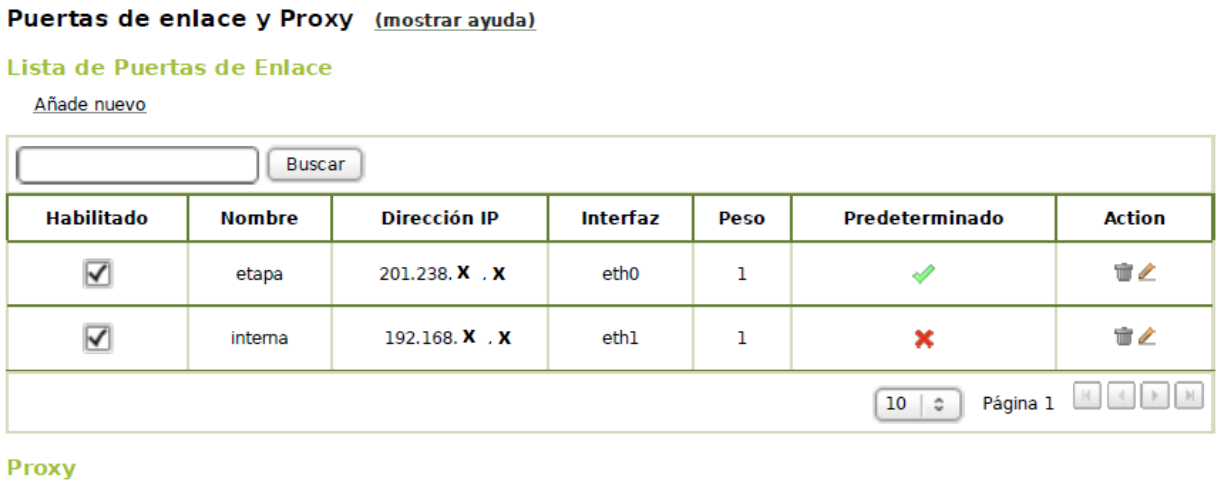
Si un equipo en la red interna conectada a la interface eth1 realiza una petición http, el equipo Zentyal que actúa como servidor proxy deberá re-direccionar para que esta petición salga por la interface eth0, por ello es necesario que configuremos dos puertas de enlace en este equipo. Una para la salida de la red interna del Hospital, y una segunda para la nube (Internet).

Para configurar iremos a la opción Red-> a continuación ingresamos a Puertas de Enlace, damos clic en Añade nuevo e ingresamos la información (Nombre, Dirección IP, Interfaz, Peso).



Fuente: Desarrollado por el Autor

Nota: es importante que la puerta de enlace de salida a la nube (Internet) sea configurada como predeterminada para que los equipos conectados a la red interna tengan salida a internet.



Fuente: Desarrollado por el Autor

3.2.2 Configurando el Proxy

Una vez que configurada, conectadas y realizada las pruebas necesarias de las interfaces y las puertas de enlace, iremos al modulo Gateway donde se encuentra la opción Proxy.

Para la configuración inicial iremos a la opción Servidor Proxy -> a continuación seleccionamos configuración general, aquí se mostrara una pantalla de configuración con el tipo de Proxy, numero de puerto, tamaño de fichero en cache y la política inicial de seguridad.

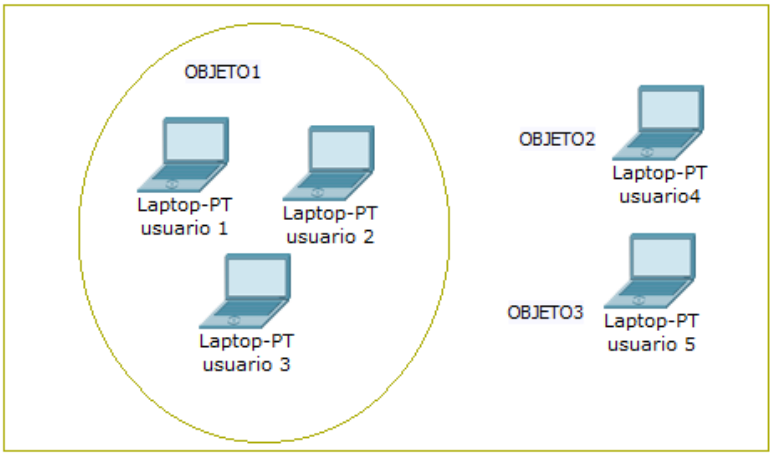
Nota: si queremos que el servidor proxy sea transparente es decir el equipo que actúe como servidor proxy configure automáticamente la dirección Ip en cada uno de los equipos como es el caso del Hospital Santa Inés, la opción proxy transparente debe estar marcada. Adicional tendremos que aplicar políticas y reglas que se detallan más adelante para que el proxy transparente funcione.

Fuente: Desarrollado por el Autor

3.2.3 Creación de Objetos de red

Siguiendo con la configuración proxy, se necesita definir los objetos de red para que el cliente pueda acceder a la red a través de un servidor proxy y a su vez que la seguridad implementada en este servidor funcione correctamente.

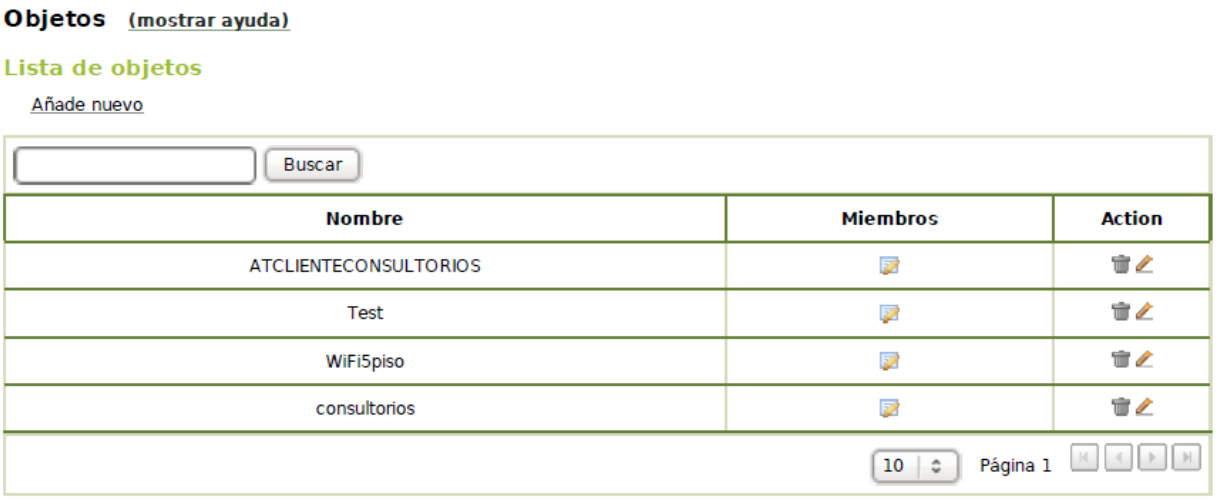
- **Objeto de red:** es una forma de representar a un usuario o grupo de usuarios mediante un nombre, esta opción permite nombrar a una IP o conjunto de IPs que representa a los usuarios para facilitar la administración de una red y de las políticas de seguridad.



Fuente: Desarrollado por el Autor

Para crear un objeto de red se deberá ingresa al módulo Core-> opción Objetos de red, y se muestra la opción Añadir nuevo/a para ingresar el nombre del objeto. En la figura se muestra los objetos creados en la red del Hospital Santa Inés.

Nota: los objetos se puede ir creando de acuerdo a los requerimientos por parte de los usuarios



Fuente: Desarrollado por el Autor

3.2.4 Políticas de Objeto Proxy

En la configuración de un servidor proxy, es necesario implementar políticas de objeto proxy a cada objeto de red creado anteriormente, para agrupar a los usuarios por características de requerimientos generales y establecer las bases de acceso mediante el servidor proxy. Para configurar una política de objeto nos dirigimos al módulos de Gateway-> dentro de la opción Proxy-> entramos en políticas de objeto y nos presenta la opción Anadir nuevo/a.

En el caso del Hospital Santa Inés se han configurado las siguientes políticas de objeto

Política de Objeto (mostrar ayuda)

Lista de objetos

Añade nuevo

Buscar

Objeto	Política	Periodo de tiempo permitido	Política de grupo	Perfil de filtrado	Action
consultorios	Filter	All time		ABIERTO-CONSULTORIOS	
ATCLIENTECONSULTORIOS	Filter	All time		Prohibidos	
Test	Always allow	MTWHFA		default	

10 Página 1

Fuente: Desarrollado por el Autor

3.2.5 Funcionamiento Proxy

En el funcionamiento de una red sin seguridad los usuarios acceden al internet directamente sin ningún tipo de restricciones. Si se realiza un trazado de ruta hacia los servidores Google el resultado es una conexión sin ninguna seguridad y un acceso directo a la nube (Internet)

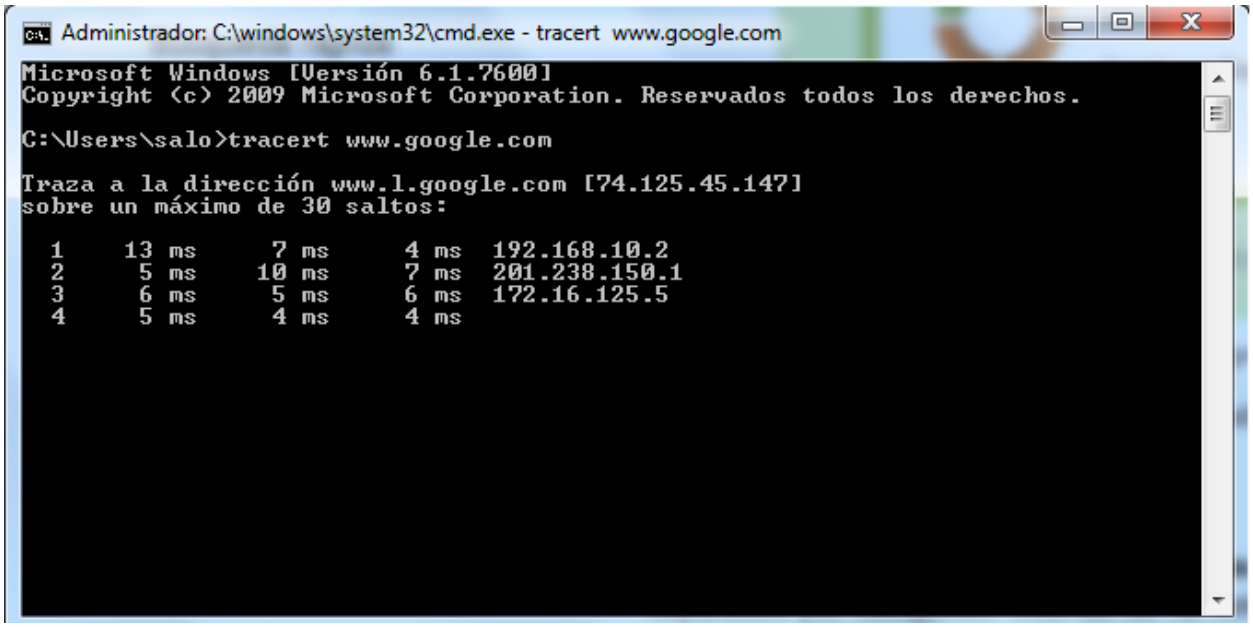
```
  1     3 ms     1 ms     1 ms  192.168.1.1
  2    21 ms    19 ms    17 ms  201.238.160.1
  3    14 ms    14 ms    13 ms  172.16.125.5
  4    15 ms    16 ms    13 ms  172.16.125.253
  5    24 ms    22 ms    22 ms  190.90.146.121
  6    47 ms    34 ms    35 ms  190.90.209.146
  7    80 ms    78 ms    83 ms  sl-st30-mia-0-4-2-1.sprintlink.net [144.223.67.5
]
  8    78 ms    77 ms    77 ms  144.232.6.126
  9   187 ms    96 ms    79 ms  209.85.253.116
 10    97 ms    97 ms    96 ms  209.85.254.252
 11    98 ms    95 ms    98 ms  72.14.232.215
 12   107 ms   107 ms   107 ms  209.85.253.141
 13    96 ms    96 ms    95 ms  yx-in-f147.1e100.net [74.125.45.147]

Trace complete.
```

Fuente: Desarrollado por el Autor

Si los usuarios acceden a la nube a través de un servidor proxy, lo que hacen es conectarse primero al Proxy y luego este re-direcciona la salida al internet con la seguridad y los beneficios antes mencionados que implica un servidor proxy.

Haciendo un trazado de ruta a los servidores Google se tendrá el siguiente resultado.



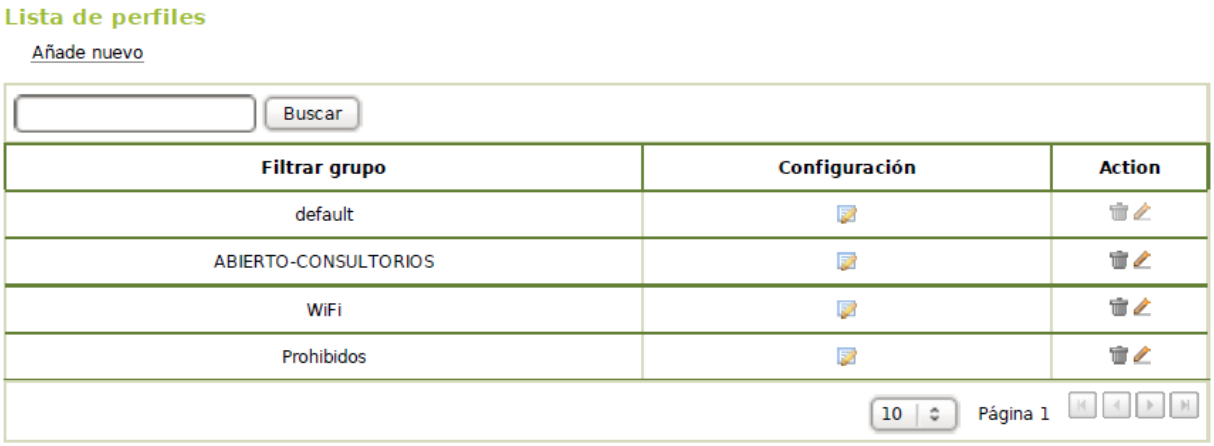
Fuente: Desarrollado por el autor.

3.3 Implementación de Políticas de seguridad

Para mejorar la seguridad en el servidor proxy, se pueden establecer políticas de seguridad y filtrado, esto se logra a través de las configuraciones de perfiles de filtrado que se puede aplicar a cada objeto de red creado anteriormente.

Para configurar un perfil de filtrado nos ubicaremos en el módulo Gateway-> ingresamos en la opción Proxy-> y en la opción Perfiles de Filtrado, creamos perfiles de acuerdo a las seguridades requeridas.

En el Hospital Santa Inés se configuro inicialmente los siguiente perfiles de filtrado.

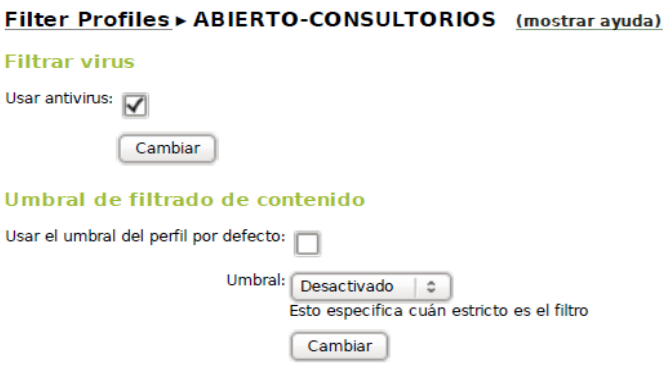


Fuente: Desarrollado por el Autor

Cada uno de estos perfiles tiene una política de acceso establecida, de acuerdo a los requerimientos por parte del usuario y de acuerdo a un análisis de seguridad.

3.3.1 Política Abierto-Consultorios

Esta política agrupa a usuarios que tiene la necesidad de un acceso sin mayor control en cuanto a contenido en la web, es decir navegación libre a sitios web, accediendo a través de un proxy (de hecho todos las políticas y objetos de red accederán mediante el Servidor Proxy Zentyal).

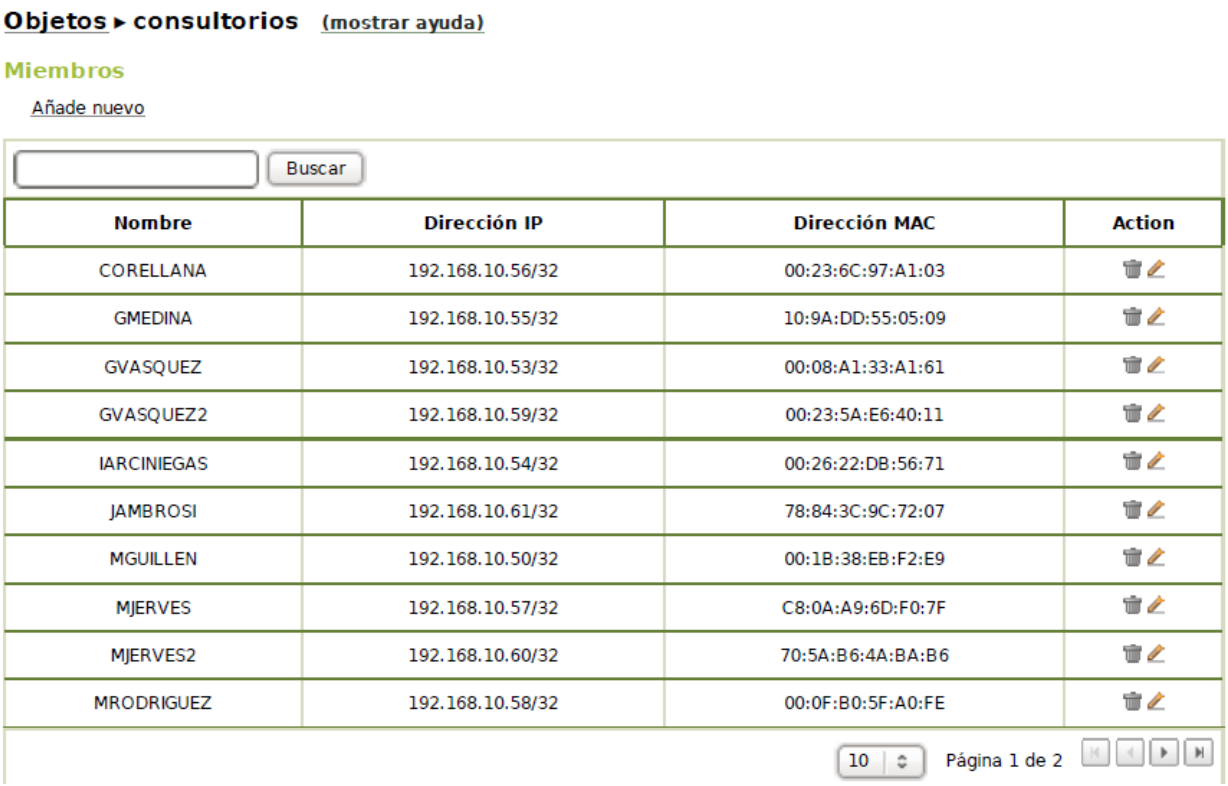


Fuente: Desarrollado por el Autor

3.3.1.1 Miembros del Perfil Abierto-Consultorios

Este perfil de acceso (política de seguridad) esta aplicado al objeto de red denominado CONSULTORIOS, lo miembros que pertenecen a este objeto son los equipos de cada uno de los doctores de este Hospital, para controlar que efectivamente sea este equipo, se adiciona la dirección MAC de la tarjeta de red de estos usuarios.

La imagen muestra algunos de los miembros del Objeto de Red consultorios



Objetos ▸ consultorios (mostrar ayuda)

Miembros

Añade nuevo

Buscar

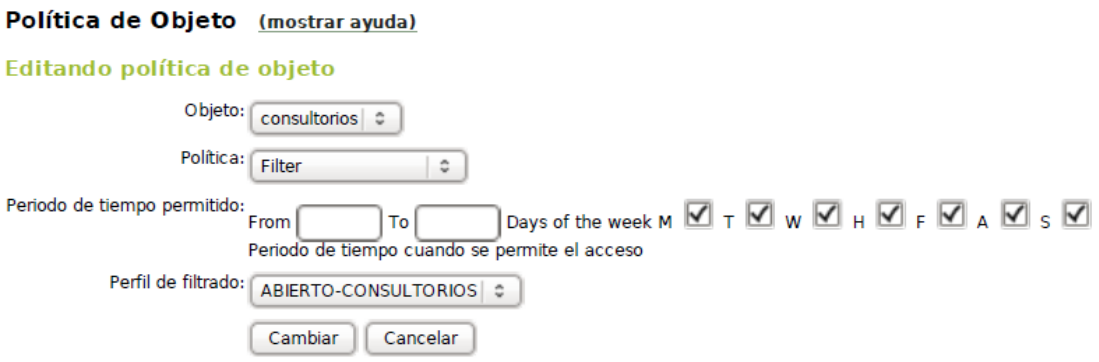
Nombre	Dirección IP	Dirección MAC	Action
CORELLANA	192.168.10.56/32	00:23:6C:97:A1:03	
GMEDINA	192.168.10.55/32	10:9A:DD:55:05:09	
GVASQUEZ	192.168.10.53/32	00:08:A1:33:A1:61	
GVASQUEZ2	192.168.10.59/32	00:23:5A:E6:40:11	
IARCINIEGAS	192.168.10.54/32	00:26:22:DB:56:71	
JAMBROSI	192.168.10.61/32	78:84:3C:9C:72:07	
MGUILLEN	192.168.10.50/32	00:1B:38:EB:F2:E9	
MJERVES	192.168.10.57/32	C8:0A:A9:6D:F0:7F	
MJERVES2	192.168.10.60/32	70:5A:B6:4A:BA:B6	
MRODRIGUEZ	192.168.10.58/32	00:0F:B0:5F:A0:FE	

10 Página 1 de 2

Fuente: Desarrollado por el Autor

3.3.1.2 Acceso a la Política Abierto-Consultorios

El tipo de acceso es un acceso filtrado, lo que indica que posteriormente se puede incrementar restricciones, inicialmente no hay filtraciones por contenido en esta política. El horario es totalmente abierto, el usuarios puede acceder cualquier día a cualquier hora.



Fuente: Desarrollado por el Autor

3.3.2 Política Prohibidos

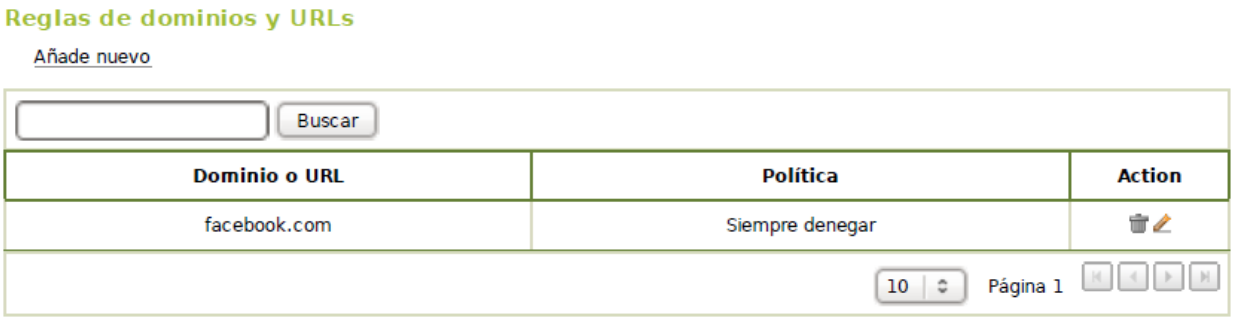
Este perfil restringe al máximo la seguridad de acceso, el tipo de contenido y los dominios a los cuales acceden los usuarios. Utilizan acceso filtrado por un antivirus del servidor proxy, tiene un umbral de perfil activado como muy estricto, este umbral analiza los contenidos texto, imágenes de una página web decidiendo si dicha página es apropiada a no de acuerdo a una puntuación que da a la página. Las opciones para el umbral de perfil son: deshabilitado, muy permisivo, pasivo, medio, estricto y muy estricto.

Fuente: Desarrollado por el Autor

A esta política se adiciona bloqueo de páginas tales como facebook.com, youtube.com, twetter.com restringido para el personal de atención al cliente.

Fuente: Desarrollado por el autor

Nota: podemos ir añadiendo dominios de acuerdo a requerimientos de seguridad del Hospital.



Fuente: Desarrollado por el autor

3.3.2.1 Miembros del perfil Prohibidos

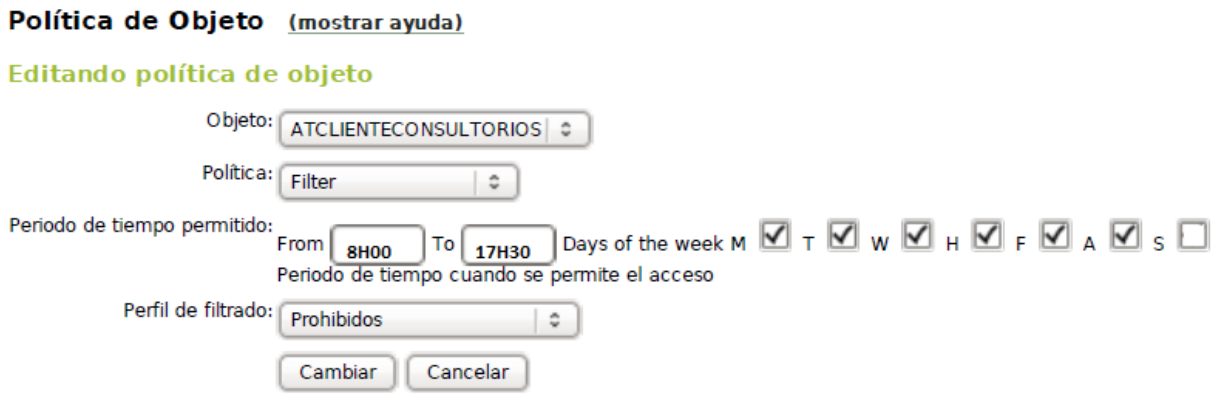
Este perfil o política de seguridad está asignada a todos los usuarios de atención al cliente como puede ser las secretarias de cada piso, personal informativo, etc. Para tener mayor control de los equipos asignados a tipo de usuarios, se utilizara la dirección MAC de la tarjeta de red.

En la figura muestra algunos miembros de este perfil.

Fuente: Desarrollada por el Autor

3.3.2.2 Acceso a la Política Prohibidos

En cuanto al acceso del personal a la web, está limitado a los días lunes, martes, miércoles jueves, viernes y sábado en el horario de 8H00 a 17H30, es decir solo tendrán acceso a internet en esos días y en ese horario con las políticas de seguridad establecidas previamente.



Fuente: Desarrollado por el Autor

3.3.3 Política WiFi

El Perfil Wifi esta aplicado para los usuarios que quieran tener acceso inalámbrico a la red pública del Hospital, tendrá restricciones de dominio y

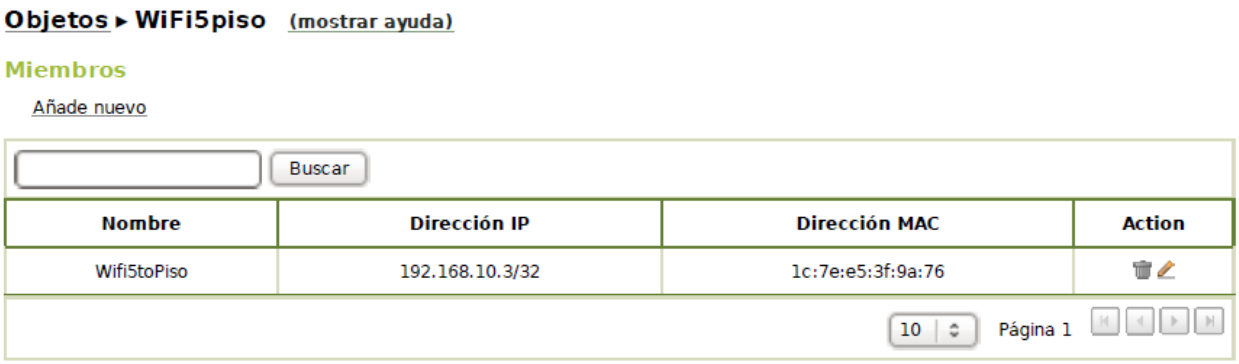
contenido, no tendrán acceso a páginas que estén dentro de las políticas de restricción de dominios.

Fuente: Desarrollado por el Autor

3.3.3.1 Miembros del perfil Wifi

Para este tipo de usuarios se darán un rango de direcciones para tener un control y aplicar el perfil Wifi configurado, el rango de direcciones IP estarán dadas mediante configuración adicional de un servidor DHCP que funciona en el mismo equipo Proxy Zentyal.

Adicional a esta configuración existirá también un objeto creado denominada Wifi5Piso el cual será miembro de este perfil.

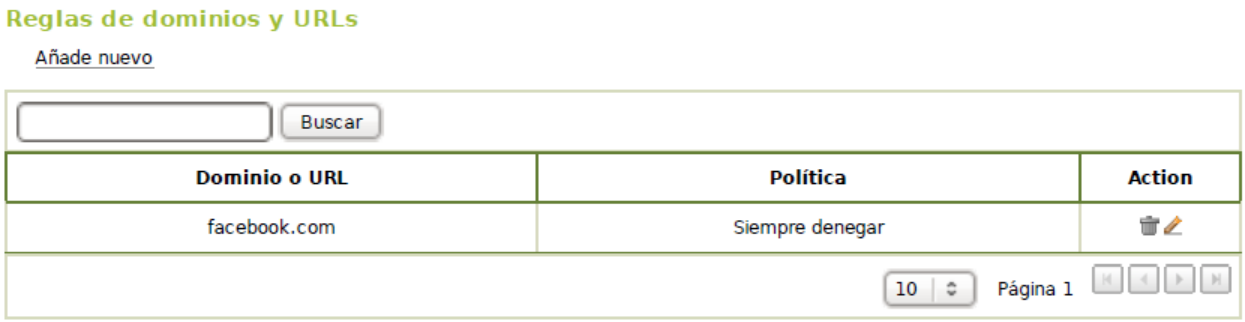


Fuente: Desarrollado por el Autor

3.3.3.2 Acceso a la Política WiFi

Se tendrá un acceso abierto a esta política en cuanto a días y horarios para poder acceder, las restricciones serán únicamente en cuanto al perfil Wifi mencionado anteriormente.

Adicionalmente existirá bloqueo de dominios, páginas que no puedan acceder desde una conexión inalámbrica como facebook, youtube, etc



Fuente: Desarrollado por el Autor

3.4 Implementación de certificados digitales

Dentro de los temas a tratar se encuentra Certificados Digitales el cual según el análisis de requerimientos realizado y tomando en cuenta la implementación de otro módulo más completo se ha concluido que se dará a conocer como información adicional la creación de Certificados digitales ya que en el módulo de creación de "Portal Cautivo" automáticamente nos permite descargarnos un certificado digital.

Dentro del módulo de infraestructura se cuenta con la integración con **OpenSSL** para gestionar como Autoridad de Certificación, y además configurar el ciclo de vida de los certificados expedidos por dicha entidad.

El proyecto OpenSSL es un refuerzo de colaboración para desarrollar un sistema robusto, de grado comercial, con todas las funciones y de código abierto de herramientas la aplicación de la capa de sockets seguros (SSL v2/v3) y TransportLayer Security (TLS v1), así como un servicio completo, la

fuerza de propósito general biblioteca de criptografía. El proyecto está gestionado por una comunidad mundial de usuarios que usan Internet para comunicarse, planear y desarrollar el kit de herramientas OpenSSL y su documentación relacionada.

OpenSSL se basa en la biblioteca OpenSSL excelente desarrollada por Eric A. Young y Tim J. Hudson. El kit de herramientas OpenSSL está licenciado bajo una licencia estilo Apache, que básicamente significa que usted es libre de obtener y utilizar para fines comerciales y no comerciales, sujetas a algunas condiciones de la licencia simples. *http://www.openssl.org/

3.4.1 Creación de certificados de autoridad de certificación

Este módulo no tiene que ser activado como se lo ha hecho con los demás, para la utilización de esta bondad de Zentyal se requiere estar registrado en la llamada CA(Autoridad de Certificación), la cual nos solicita que ingresemos los siguientes datos:

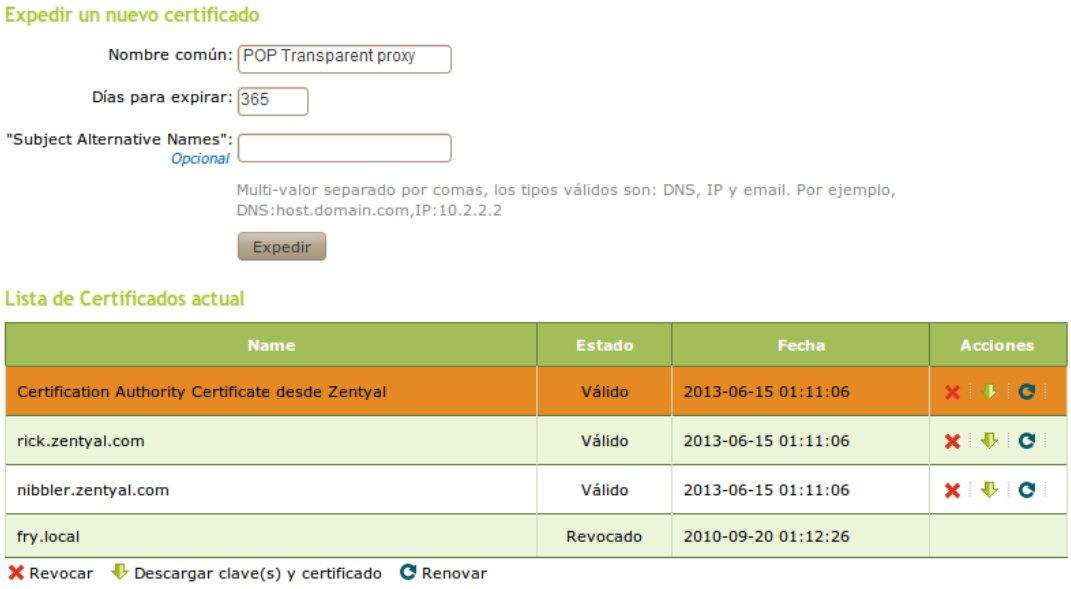
Fuente: Desarrollado por el Autor

- Nombre de la Organización: Se describe el nombre de la Empresa o entidad que está autorizada para expedir los certificados en este caso el Hospital Santa Inés.

- Código de País: El cual es opcional se refiere un acrónimo de dos letras el cual sigue el estándar de la ISO-3166-1.
- Ciudad: El nombre de la ciudad en este caso Cuenca
- Estado: Que es un campo opcional al igual que los dos anteriores.
- Días para expirar: Para establecer la fecha de expiración se debe saber que si algunos servicios dependen de esta CA, se revocaran los certificados expedidos.

3.4.2 Crear un certificado Digital

Para crear un certificado Digital dentro de Zentyal tenemos que llenar los siguientes campos dependiendo para el uso que se requiera:



Fuente: Desarrollado por el Autor

- Nombre Común: En este caso tenemos que utilizar el mismo nombre del servicio en el cual se va a utilizar, para este caso el servicio es POP TransparentProxy.
- Días a Expirar: se ha puesto 365 días, se debe tomar en cuenta que el tiempo a expirar el certificado debe ser menor al tiempo para el que fue creado el CA.

3.4.3 Configuración de Certificados de Servicio

Para cada servicio podemos crear un Nombre el cual se identificará con cada servicio para asignar un certificado digital, lo activaremos para después reiniciar el módulo al cual se está aplicando ese servicio para poder utilizarlo.

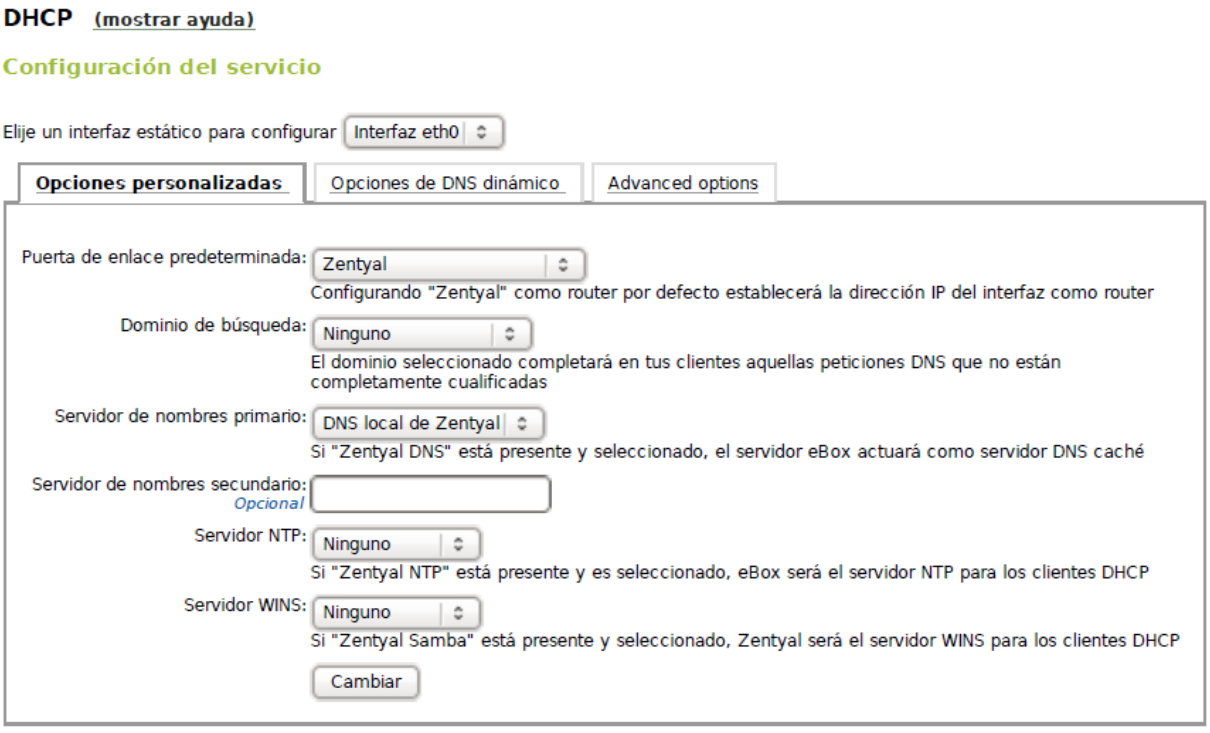
3.5 Configuración de servidor DHCP

Con la nueva configuración y esquema de la red del Hospital Santa Inés, es necesario que se implemente un servidor DHCP, para aprovechar recursos y a su vez mejorar tiempos de respuesta se implementa en el mismo equipo de Servidor Proxy Zentyal una configuración para que actúe como Servidor DHCP, que asignará de acuerdo a la interfaz las direcciones IP a cada usuario conectado a la red.

Existirá dos tipos de asignaciones DHCP, una para la interface conectada entre el Servidor y el Modem ETAPA.

3.5.1 Configuración de interfaces

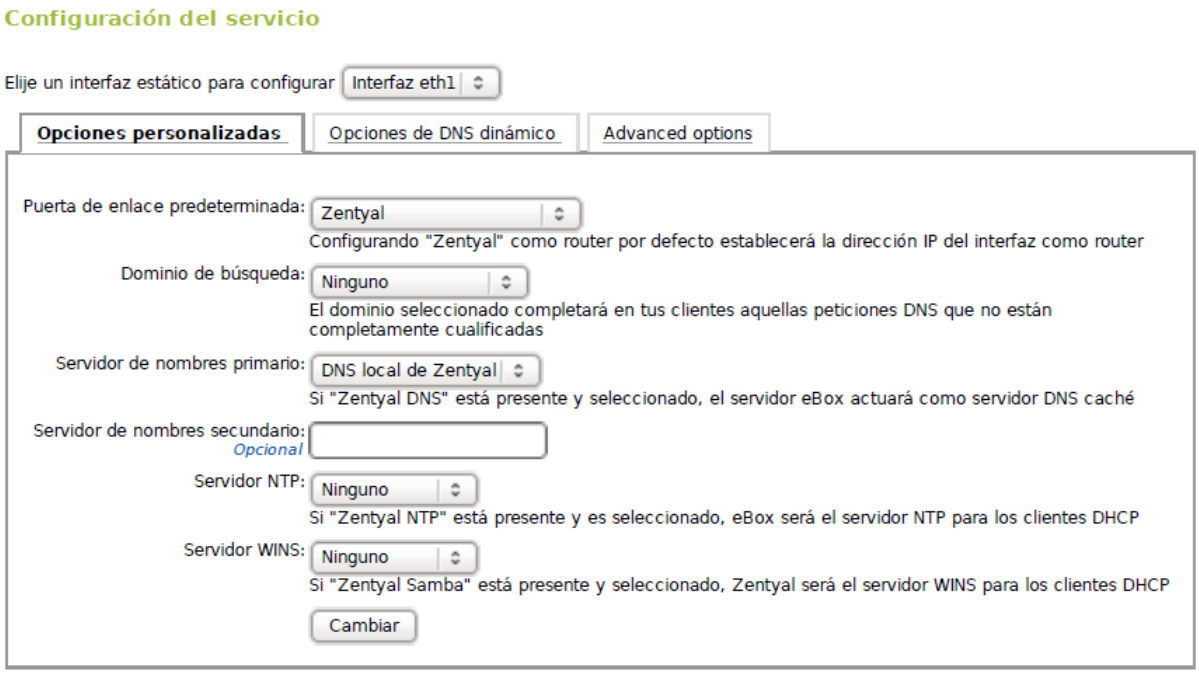
- Configuración DCHP interfaz eth0: esta interface está conectada al modem ETAPA el cual provee acceso a internet.



Fuente: Desarrollado por el Autor

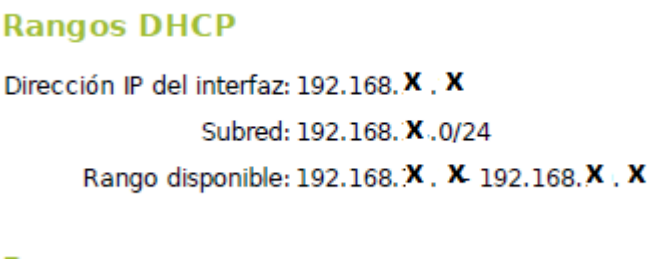
Rango de direcciones (Oculto por Confidencialidad): en esta opción podemos configurar los rangos en los cuales se quiere que asigne una dirección IP al usuario.

- **Configuración DCHP interfaz eth1:** Esta interface está conectada a la red interna del Hospital Santa Inés, es necesario que el Servidor Proxy Zentyal actué también como Servidor DHCP para la red interna, sobre todo por las políticas de seguridad implementas en el servidor proxy. A cada usuario de la red interna del Hospital se le asignará una IP automáticamente.



Fuente: Desarrollado por el Autor

Rango de direcciones (Oculto por Confidencialidad): en la interface eth1 está configurado el rango de direcciones IP para que se asignado mediante DHCP a los usuarios, como se muestran en la figura.

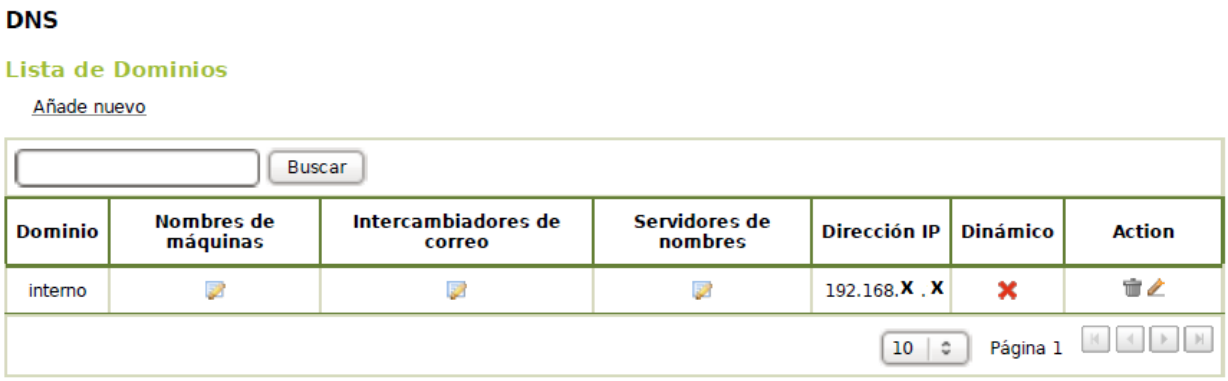


Fuente: Desarrollado por Autor

3.6 Configuración de servidor DNS

Para resolución de nombre de dominios se implementó un Servidor DNS, este funciona como un servidor de dominios para las redes internas de Zentyal * www.Zentyal.org , en ocasiones las redes internas de Zentyal requerirá hacer una consulta al servidor DNS cache.

Para realizar esta configuración se ingresara en el módulo Infraestructura-> opción DNS en este opción nos presenta la opción añadir nuevo/o dominio. La configuración realizada muestra el siguiente resultado.



Fuente: Desarrollado por el Autor

3.7 Configuración del Portal Cautivo

Lo que permite una configuración de portal cautivo es, limitar el acceso a la red a la interface interna que se aplique la configuración. La limitación del

acceso se basa en pedir usuario y contraseña a cada cliente que este registrado en la Ficha Usuarios de Zentyal.

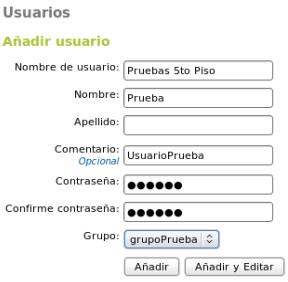
- En el usuario se muestra la siguiente imagen pidiendo usuario y contraseña

Fuente: Desarrollado por el Autor

- Una vez, que el usuario ingresa los datos, el servidor verifica y autentifica la conexión mostrando un mensaje de acceso en una pantalla minimizada.

Fuente: Desarrollado por el Autor

- Los usuarios son gestionados a través de Grupos de Usuario Zentyal, un grupo puede contener a varios usuarios



Fuente: Desarrollado Por el Autor

Para configurar el portal cautivo, ubicarse en el módulo Gateway-> Portal Cautivo y nos presentara la opción para ingresar los datos. El grupo creado anteriormente con los usuarios respectivos y el puerto por el cual Zentyal re-direccionara las peticiones HTTP al puerto de identificación HTTPS. En la pestaña Usuarios Actuales se mostraran todos los usuarios autentificados y que este conectados actualmente.

Fuente: Desarrollado por el Autor

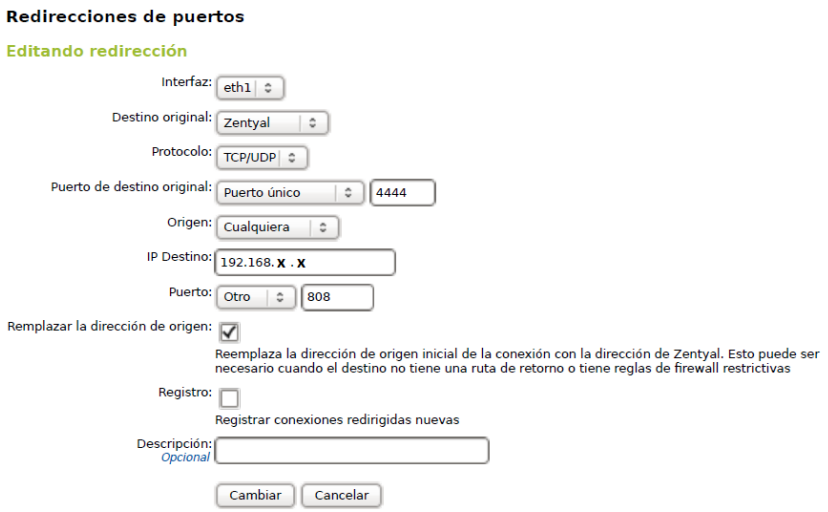
Nota: En el caso de tener configurado un servidor proxy con un puerto diferente (808) como es el caso del Hospital Santa Inés, se tendrá que hacer una redirección de puertos, para que la autentificación mediante el Portal Cautivo se exitosa.

3.7.1 Redirección de Puertos

Módulo UTM-> Cortafuegos-> Redirección de Puertos

Para realizar la re-dirección de un puerto, primero se identifica y se define la interface por la cual Zentyal recibe tráfico entrante. Destino Original que puede ser el propio Zentyal, una dirección IP o un Objeto. Puerto Destino Original que puede ser un solo puerto o un grupo de puertos. Finalmente se establecerá la IP de destino por donde el servidor recibirá las peticiones y el puerto al cual se realizará la traducción.

- Traducción de puerto del Hospital Santa Inés



Fuente: Desarrollado por el Autor

- Listado de las traducciones de puertos Hospital Santa Inés

Fuente: Desarrollada por el Autor

CAPÍTULO 4: ANÁLISIS FINANCIERO

4.1 Análisis de costos de equipos

Para la implementación dentro del Hospital Santa Inés se ha requerido los siguientes equipos:

Cantidad	Descripción	Costo
1	Pc con 2 tarjetas de red	1000
1	Switch	200
2	Patchcord	10
	Costo de mano de obra	2000
	Total	3210

El costo total en cuanto a equipos dentro de la implementación es de 3210$ lo cual representa una inversión dentro del Hospital Santa Inés para mejorar el servicio que ofrece.

4.2 Análisis de costos de capacitación de usuarios

Para la capacitación para la persona que utilizará el módulo de usuarios y grupos dentro del hospital, en el cual se instruirá para agregar un grupo y usuario para la conexión de internet dentro del portal Cautivo.

Cantidad	Descripción	Costo
1	Administrador Zentyal	50$
1	Manual Usuario	20$
	Total Costo Capacitación	70$

Para obtener el costo total de la capacitación del usuario que emitirá las credenciales de conexión para internet dentro del Hospital se requiere de la ayuda del Administrador Zentyal quien será la persona que realice la

capacitación la cual durara 2 horas aproximadamente el costo por hora es de 25$ lo cual nos da un total de 50$, de igual manera se requiere un manual de usuario que servirá de guía para las siguientes personas que ocupen el cargo de la persona que emite dichas credenciales sin tener que necesitar nuevamente dicha capacitación , el costo del manual tendrá un valor de 20$, dándonos un total de costo de capacitación de 70$.

Nota: Ver en anexos "Manual de Usuario"

4.3 Análisis de costo beneficio

Tomando en cuenta el costo que representa esta implementación podemos concluir que los beneficios obtenidos son en mayor cantidad:

- Segmentación de usuarios
- Mejor redistribución del ancho de banda
- Mejor calidad del servicio de internet
- Implementación de políticas de seguridad
- Control total de la red pública del Hospital

Por lo tanto la implementación resulto un beneficio para el Hospital Santa Inés y una inversión en cuanto a equipos para su funcionamiento, por lo que se puede seguir aumentando usuarios que utilicen este servicio con la seguridad y control adecuado sin temor a que colapse la red o se caiga el servicio.

Además si se desea implementar nuevas políticas de seguridad el administrador de la herramienta utilizada (Zentyal), puede hacerlo sin tener que retomar todo desde cero sino simplemente con una previa capacitación en cuanto a la utilización de la misma.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al término de nuestro trabajo investigativo acerca de la "Implementación de un Proxy con seguridad para la navegación de médicos y pacientes en el Hospital Santa Inés" hemos llegado a las siguientes conclusiones:

- Los objetivos planteados fueron alcanzados totalmente, ya que al implementar un servidor proxy se ha mejorado el rendimiento, calidad y seguridad de la red dentro del Hospital.
- Se estableció a Zentyal como herramienta base para poder realizar la administración y control total de la red pública analizando su funcionalidad, calidad y costo invertido en la misma.
- Dentro de la funcionalidad de la herramienta Zentyal como una de sus bondades se realizó la segmentación de usuarios dentro del Hospital para mayor control acerca de tipos de usuarios y sus restricciones.
- Para un mejor control de la red pública nos pudimos dar cuenta que al establecer la funcionalidad de un Portal Cautivo donde los usuarios tengan que loguearse para la conexión a internet ayudara a los administradores de red a tener una mejor organización de los usuarios y aprovechamiento de los recursos existentes.
- Para la realización de esta investigación se puede decir que el tiempo invertido fue aprovechado en su totalidad dentro del Hospital Santa Inés realizando las configuraciones necesarias en horarios factibles sin afectar mayormente a los usuarios.
- De acuerdo a nuestro análisis realizado de Costo Beneficio se puede concluir que las ventajas obtenidas, resultan mayores al costo de inversión de equipos y recursos humanos utilizados para la implementación de esta solución.
- Dentro de la parte humana en representación al Hospital Santa Inés se puede destacar el apoyo incondicional por parte de nuestro director Ing. Esteban Crespo que como Administrador del Departamento de

Sistemas nos proporcionó la información y herramientas necesarias para poder realizar esta investigación e implementación.

- Para poder aprovechar de manera adecuada los recursos que poseen las pequeñas y grandes empresas se requiere de una administración y un análisis de los requerimientos para poder establecer control de navegación y políticas de seguridad.

Recomendaciones

Luego de llegar a las conclusiones anteriormente descritas establecemos las siguientes recomendaciones:

- Para implementar políticas y herramientas de seguridad es necesario que exista un departamento de seguridad de la información el cual se encargue de establecer los niveles de seguridad por los que están clasificados los usuarios.
- En cuanto a la creación de usuarios y permisos debe existir una persona debidamente capacitada para realizar esta tarea.
- Para la administración de red de las pequeñas y grandes empresas se recomienda la herramienta "Zentyal " .
- Hacer conocer las políticas de seguridad y navegación a los usuarios para su comprensión al momento de utilizar el servicio.

Bibliografía

Alfonso Garcia-Cerevignon Hurtado, M. d. (s.f.). Seguridad Informática.

Andreu, J. (2010). Servicios de Red. EDITEX.

Castillo, F. S., Sánchez, G., & Rodríguez, J. R. (2010). Redes Locales. Madrid: Ediciones Paraninfo, SA.

Mathon, P. (Diciembre 2002). Proxy y Firewall. Amadeu Brugués: ENI.

Stallings, W. (2004). Fundamentos de Seguridad Aplicaciones y Estándares. Madrid: Pearson Educación S.A.

Fuentes en internet:

- http://es.tldp.org/COMO-INSFLUG/es/pdf/Cortafuegos-COMO.pdf
- http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.pdf
- http://www.galpon.org/wiki/images/6/69/200710_ciclo_conferencias_firma-digital.
- http://www.taringa.net/posts/linux/8450763/Manual-completo-Instalacion-de-Zentyal-Firewall-de-Linux.html
- http://cerowarnings.blogspot.com/2012/04/zentyal-configuracion-de-proxy.html
- http://www.openssl.org/
- http://doc.zentyal.org/es/installation.html

Anexos

Manual de usuario

1. Dentro del servidor Zentyal se encontrara un icono llamado Panel de Control donde accederá a al usuario y contraseña para entrar como administrador.
2. Una vez logueado como administrador se puede crear un grupo de la siguiente manera:
    - Ingresar al a "Grupos" dentro del módulo Office

Fuente: Desarrollo del autor

Dentro de esta pantalla nos pide ingresar el nombre del grupo y de manera opcional un comentario acerca del grupo creado, pulsamos en añadir donde pasara el nombre creado a la lista de grupos existentes.

3. Una vez creado el grupo se crea un usuario dentro del módulo office pulsamos en usuarios.

Fuente: Desarrollo del autor

Dentro de esta pantalla se ingresa el nombre de usuario el cual servirá para loguearse para acceder a internet dentro de la red pública, Nombre y Apellido para tener un registro de quien es el solicitante del servicio, Contraseña para poder acceder la cual se debe hacer saber al usuario y se selecciona el grupo al que pertenece el usuario en este caso se puede elegir entre los grupos Wifi, Atención al cliente y Consultorios.

4. Finalmente de esta manera el usuario se podrá conectar a la red pública y podrá conectarse con su usuario y contraseña.

Fuente: Desarrollo del autor