UNIVERSIDAD DE SANTIAGO DE CHILE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELECTRICA

ANTEPROYECTO DE INSTALACIÓN DE RED LAN PARA PEQUEÑA EMPRESA CON SEGURIDAD OPEN-SOURCE

FRANCISCO JAVIER RAU ANDRADE

Profesor guía: Hugo Eduardo Zamora Farías
Ingeniero Civil Electricista
Magíster en Telecomunicaciones

Para optar al Título de Ingeniero de Ejecución en Electricidad

Santiago – Chile
2009

Dedicatoria

A todas las personas que me hicieron posible llegar al final de esta etapa de mi vida. Mis sinceros agradecimientos.

Francisco

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

TÍTULO: Anteproyecto de instalación de red LAN para pequeña empresa con seguridad open-source.
CLASIFICACIÓN TEMATICA: Redes de área local; Servidores; Cortafuegos: seguridad de computadores; Linux: seguridad.
AUTOR: Rau Andrade, Francisco Javier
CARRERA: Ingeniería de Ejecución en Electricidad
PROFESOR GUÍA: Zamora Farías, Hugo Eduardo
AÑO: 2009
CODIGO UBICACIÓN BIBLIOTECA: **2009 / E / 39**

RESUMEN

La necesidad de expansión de las empresas se ven reflejadas en las tecnologías que las incorporan. Es por ello que al tener una red LAN rápida, eficiente y confiable contribuye al desarrollo de ésta. Además si se lograr reunir estas características con herramientas libres y open-sources se tiene menor impacto a los recursos de una pequeña empresa.

En este documento se ve reflejado el diseño de una red LAN que contempla servidores para soportes de distintos servicios, entre los destacados, archivos, Web y correo, protegiéndola con herramientas y técnicas de seguridad tanto a nivel de servidores como de red.

CAPTITULO 1: INTRODUCCIÓN

1.1 ORIGEN

PLANTEAMIENTO DEL PROBLEMA

Este proyecto nació por la necesidad de un requerimiento de la Empresa TELECTRICA LTDA., ya que desea trasladarse de ubicación (cambio de domicilio) por ampliación de infraestructura a la comuna de Pudahuel, Santiago de Chile y a su vez ampliar sus servicios de telecomunicaciones ya que en este ámbito no cuenta con una red de calidad.

El requerimiento solicitado es desarrollar una red de área local (LAN), de alta capacidad. Además de este requerimiento se sitúa otros puntos importantes como el desarrollo de servidores para soportes de distintos servicios, entre los más destacados, DHCP, archivos, Web y correo.

Uno de los requerimientos más importantes de esta empresa es la seguridad, que contemple características de una red fiable y confiable.

Conforme a esto se aplicará herramientas de seguridad en redes y en servidores, ya que es fundamental y primordial contar con redes confiables y seguras para respetar la confidencialidad de la empresa.

1.2. OBJETIVOS DEL PROYECTO

1.2.1 Objetivo General

El objetivo general es diseñar una red de área local de alto nivel con acceso a Internet banda ancha, que permita administrar o manejar toda la información necesaria para aumentar la productividad de la Empresa, contemplando una red que se centre principalmente en su protección, y que posea herramientas de seguridad en la red, para garantizar su privacidad y confidencialidad.

1.2.2 Objetivos Específicos

- Realizar un estudio de las distintas tecnologías de redes de telecomunicaciones para diseñar una red de área local (LAN) e Intranet.
- Estudiar las distintas alternativas de solución para la nueva infraestructura de la Empresa, y señalar las distintas opciones de administración de la red LAN.
- Analizar distintas alternativas de solución basándose en la factibilidad técnica y financiera.
- Plantear configuración a servidores de red aplicando los distintos servicios que poseerán, ya siendo servidor firewall, correo, Web, DHCP y archivos.
- Diseñar Red WLAN *(Wireless Local Area Network).*
- Aplicar herramientas de seguridad a la red local diseñada.

1.3 ESTUDIO DE NECESIDADES

Actualmente la Empresa cuenta con una red local que carece de seguridad, conectividad, no posee servicios de correo, ni una red con distintas jerarquías. Esto conlleva a la no satisfacción de todas las necesidades del personal ya que tampoco cuenta con una red WLAN, que posibilita la movilidad en el acceso de Internet.

Debido a la expansión que desea realizar la Empresa en su infraestructura y al aumento de contrato de personal, se desea cambiar de ubicación (domicilio) a la comuna de Pudahuel, Santiago de Chile a una nueva infraestructura. Por ende se tendrá que realizar un diseño de una nueva red que satisfaga las siguientes necesidades a la Empresa:

Red de área local con servidor de archivos de alta velocidad centrando características de fluidez y rapidez.

Soporte WIFI, por la gran masificación de la red Wireless (WLAN) que ha tenido en el país, la movilidad, versatilidad y conectividad que permite otorgar al personal que posean equipo portátil.

Poseer un servidor de correo que le permita enviar y recibir e-mail de Internet.

Para garantizar una seguridad máxima y de alta confiabilidad, se estudiarán las herramientas, aplicaciones y/o equipos más actuales de una red local, basado en software open-source.

1.4 DESARROLLO Y ALCANCES

Se estudiarán herramientas y/o aplicaciones de seguridad en la red disponible, ya que es de vital importancia actualizar en este ámbito, ya que con los constantes ataques a la red Internet que se han producido en nuestro país, se tiene que contar con una red robusta y sólida, sobretodo si ésta es aplicada a una Empresa. Si además comprendemos los mecanismos que se siguen en las conexiones en red, y nos mantenemos actualizados, podemos tener un nivel de seguridad y una funcionalidad aceptables.
El desarrollo de este proyecto se limitará a solo su estudio, prueba y diseño, es decir, no se realizará implementación, pero se dejará todas las herramientas para un futuro posterior.

1.5 APORTE PERSONAL

Conocer las últimas tecnologías en conectividad de redes de área local y entregar un esquema de alternativas de desarrollo de instalación de redes locales, que son importantes procesos a la hora de construir una Empresa.
Conocer métodos, herramientas, soluciones de seguridad basada en software open-source.

Además proveer una solución que acomode todas las necesidades que la Empresa requiera, en otorgar una red de área local que garantice su fluidez, rapidez y por sobre todas las cosas, seguridad.

1.6 ESTADO DEL ARTE

Existen memorias o libros relacionados con el diseño de redes LAN, debido a que esta área es de gran implementación en el mercado, siempre hay nuevas tecnologías de acceso a la red, es por ello que es necesario actualizar en este ámbito las distintas soluciones aplicables en una Empresa.

1.7 ORGANIZACIÓN DEL DOCUMENTO

El presente trabajo está divido en 6 capítulos: el capitulo 1 es la introducción al problema, donde se mencionan la descripción del problema a tratar, junto con los objetivos del proyecto y las necesidades a considerar.

En el capitulo 2 se presenta los fundamentos teóricos relacionados con el desarrollo de redes LAN, necesarios para realizar este trabajo y una introducción a la seguridad tanto en red como a servidores, dando a conocer los ataques que se ven expuestos y su prevención.

En el capitulo 3 se presenta los requerimientos y necesidades que posee la Empresa para plantear alternativas de solución que las satisfagan.

En el capitulo 4 se presenta las alternativas de solución analizándolas tanto en ámbito técnico como económico, estableciendo la elección de una de ellas.

En el capitulo 5 se presenta el desarrollo de la solución, conformado por el diseño de la red LAN, dando a conocer su análisis, pruebas, implantación y uso. Además se detalla la configuración de los equipos a implementar con sus respectivos servicios.

En el capitulo 6 se presentan las conclusiones con respecto a la solución realizada y a los resultados obtenidos.

CAPITULO 2: FUNDAMENTOS TEÓRICOS DE REDES LAN Y SEGURIDAD DE LA INFORMACIÓN

2.1 INTRODUCCIÓN

Para poder entender los temas que se tratan en este trabajo, a continuación se entregan varios fundamentos teóricos los que se verán durante este capitulo.

2.2 REDES LAN

Redes LAN son las siglas de Local Area Network [1], red de área local.
Estas redes son usadas para la interconexión de computadores personales y estaciones de trabajo en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios). Se caracterizan por: tamaño restringido, tecnología de transmisión (por lo general broadcast), alta velocidad y topología.
Son redes con velocidades entre 1 Mbps y 1 Gbps, tiene baja latencia y baja tasa de errores. Cuando se utiliza un medio compartido es necesario un mecanismo de arbitraje para resolver conflictos.

Características importantes

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Cableado específico instalado normalmente a propósito.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km (una FDDI puede llegar a 200 km)
- Uso de un medio de comunicación privado

- La facilidad con que se pueden efectuar cambios en el hardware y el software
- Posibilidad de conexión con otras redes
- limitante de 100 m

2.2.1 Consideración de Topología de red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.
En cuanto a este diseño de red LAN se contemplará la topología de red estrella, siendo la más usada en el mercado actualmente.

2.2.1.1 Topología en estrella

La topología en estrella tiene un nodo central desde el que se irradian todos los enlaces hacia los demás nodos. Por el nodo central, generalmente ocupado por un hub, pasa toda la información que circula por la red. La ventaja principal es que permite que todos los nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red se desconecta.

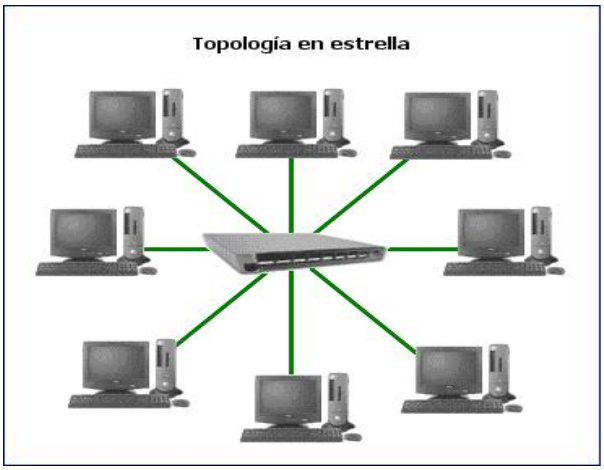


Figura 2 – 1: Topología en estrella

Las redes en estrella tienen una dependencia total de su nodo central, así se reducen características como potencia, precio y demás prestaciones.

2.2.2 Componentes de una red LAN

Una red LAN esta conectada y organizada por componentes de red que cumplen funciones especificas para el funcionamiento de ella.
A continuación se muestra un diagrama y se listan los componentes:

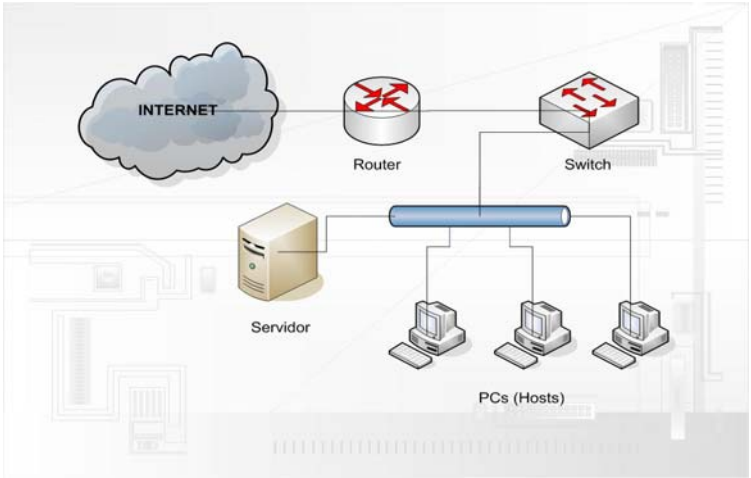


Figura 2 – 2: Diagrama de red LAN típica.

2.2.2.1 Servidor

Un servidor [2] es una computadora que formando parte de una red, provee servicios a otros denominados clientes.
El servidor, entonces, no hace más que poner sus recursos a disposición de las demás computadoras, para cuando estas los requieran.
Entre estos servicios que puede poseer un servidor están el respaldo de información, acceso al Internet, seguridad en una red, acceso a medios de información, entre otros muchos servicios que se pueden establecer. Cuando una red consta de un servidor y varios clientes, se dice que posee una arquitectura cliente/servidor. Internet puede ser vista como un gran conjunto de servidores preparados para satisfacer las necesidades de las máquinas clientes, en última instancia manejadas por los usuarios.

2.2.2.2 Router

Un router [2] es un dispositivo de hardware o software, de interconexión de redes de computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.
El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos, a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete, otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

2.2.2.3 Switch

Un switch llamado también conmutador, es el dispositivo analógico que permite interconectar redes operando en la capa 2 (enlace de datos) del modelo OSI. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro. Su empleo es muy común cuando existe el propósito de conectar múltiples redes entre sí para que funcionen como una sola. Un conmutador suele mejorar el rendimiento y seguridad de una red de área local.

El funcionamiento de un conmutador o switch, tiene lugar porque el mismo tiene la capacidad de aprender y almacenar direcciones de red de dispositivos alcanzables a través de sus puertos. A diferencia de lo que ocurre con un hub o concentrador, el switch hace que la información dirigida a un dispositivo vaya desde un puerto origen a otro puerto destino.

2.2.2.4 Terminal NIC

(NIC, Network Interface Card, placa de red) [1]. Una tarjeta de red es un tipo de tarjeta de expansión que se inserta en la placa madre o a un puerto como el USB, y que permite conectar una computadora a una red y así poder compartir recursos (impresoras, archivos e Internet).

Una tarjeta de red inalámbrica permite lo mismo, sólo que sin emplear cables de red, sino que se utilizan ondas radio para transmitir la información.

Pertenece a la capa 2 del modelo de referencia OSI, se identifica a través de una dirección MAC única, que solo pertenecerá a esa tarjeta de red.

2.3 MODELO OSI

El modelo OSI [1] es un modelo que comprende 7 capas. Las capas del modelo OSI son las siguientes:

Figura 2 – 3: Modelo OSI

- **La capa física** define la manera en la que los datos se convierten físicamente en señales digitales en los medios de comunicación (pulsos eléctricos, modulación de luz, etc.).
- **La capa de enlace de datos** define la interfaz con la tarjeta de de red y cómo se comparte el medio de transmisión.
- **La capa de red** permite administrar las direcciones y el enrutamiento de datos, es decir, su ruta a través de la red.
- **La capa de transporte** se encarga del transporte de datos, su división en paquetes y la administración de potenciales errores de transmisión.
- **La capa de sesión** define el inicio y la finalización de las sesiones de comunicación entre los equipos de la red.

- **La capa de presentación** define el formato de los datos que maneja la capa de aplicación (su representación y, potencialmente, su compresión y cifrado) independientemente del sistema.
- **La capa de aplicación** le brinda aplicaciones a la interfaz. Por lo tanto, es el nivel más cercano a los usuarios, administrado directamente por el software.

2.4 MODELO TCP/IP

En el modelo TCP/IP o Internet se divide en 4 niveles:

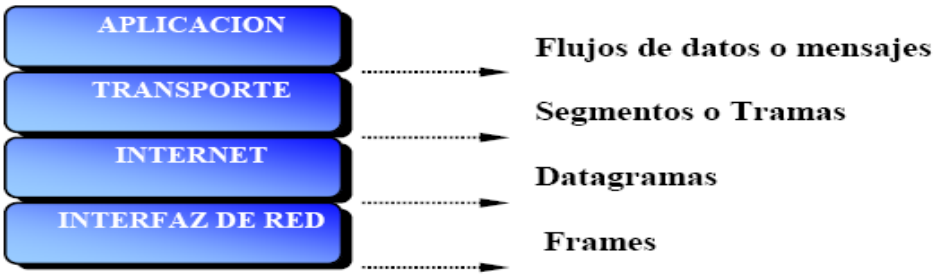


Figura 2 – 4: Modelo TCP/IP

- **Nivel de Aplicación**. Proporciona una comunicación entre procesos o aplicaciones en sistemas distintos. Además se ocupa de las necesidades de presentación y sesión. En realidad es un conjunto de protocolos como TELNET, FTP, HTTP, y SNMP.
- **Nivel de transporte.** Se establece una comunicación extremo-a-extremo en la que se realiza un control del flujo de información. Los protocolos son el TCP y el UDP.
- **Nivel de Internet**. Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP).

- **Nivel de acceso a la red**. Es el nivel más bajo y la que se relaciona más directamente con el hardware. Este nivel es el responsable del intercambio de datos entre dos sistemas conectados a una misma red.

2.5 CABLEADO ESTRUCTURADO

Los sistemas de cableado estructurado constituyen una plataforma universal por donde se transmiten tanto voz como datos e imágenes y constituyen una herramienta imprescindible para la construcción de edificios modernos o la modernización de los ya construidos. Ofrece soluciones integrales a las necesidades en lo que respecta a la transmisión confiable de la información, por medios sólidos; de voz, datos e imagen.

La instalación de cableado estructurado debe respetar las normas de construcción internacionales más exigentes para datos, voz y eléctricas tanto polarizadas como de servicios generales, para obtener así el mejor desempeño del sistema.

2.5.1 Especificaciones y tipos de cable de red

Cable de Categoría 5e

La categoría 5e, puede soportar transmitir datos a velocidades de hasta 100 Mbps. (Esta autorizado para escalar a 1 Gb.)

Está diseñado para señales de alta integridad. Estos cables pueden ser blindados o sin blindar.

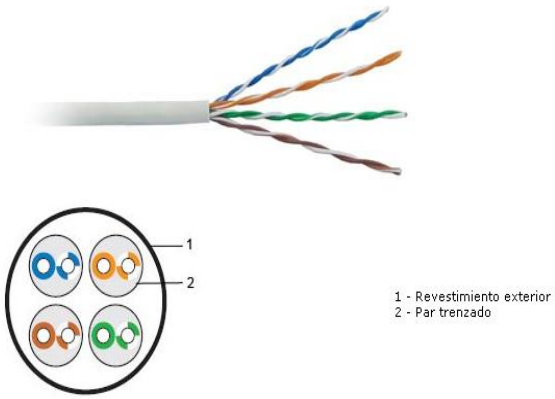


Figura 2 – 5: Esquema de cableado cat 5e

Características Técnicas:

- Conductor: alambre de cobre 24 AWG
- Aislamiento: polietileno de consistencia incrementada, grosor mínimo 0,18 mm
- Diámetro del cable 0,9±0,02 mm.
- Diámetro exterior del cable 5,1±0,2 mm.
- Temperatura máxima admisible:

Cable de Categoría 6

Es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que son compatibles con versiones anteriores de estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para *crosstalk* y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 300 MHz en cada par.

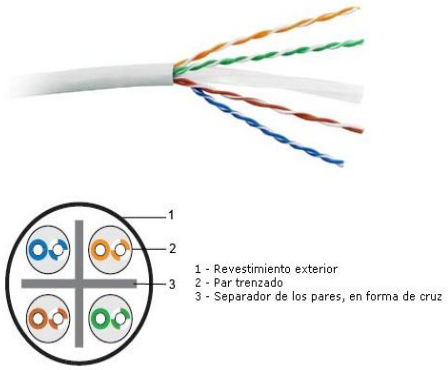


Figura 2 – 6: Esquema de cableado cat 6

Características Técnicas:

- Conductor: alambre de cobre 24 AWG.
- Aislamiento: polietileno de consistencia incrementada, grosor mínimo 0.18 mm.
- Diámetro del cable 0.99±0.02 mm.
- 4 pares trenzados con separación de polietileno.
- PVC (grosor mínimo del forro 0.4 mm).
- Diámetro exterior del cable 6.2±0.2mm.
- Temperatura máxima admisible: 75°C

Cable de Categoría 7

Es un estándar de cable para Ethernet [10] y otras tecnologías de interconexión, que puede hacerse compatible hacia atrás con los tradicionales de Ethernet (actuales cable de categoría 5/5e y cable de categoría 6). El cat 7 posee especificaciones aún más estrictas para *crosstalk* y ruido en el sistema que cat 6. Para lograr esto, se ha agregado blindaje a cada par de cable individualmente y para el cable entero. Con una toma de tierra correcta, el revestimiento trenzado y las pantallas individuales de lámina de aluminio, aumentan significativamente el parámetro electromagnético de compatibilidad del cable.

El estándar cat 7 fue creado para permitir 10 Gigabit Ethernet sobre 100 metros de cableado de cobre.

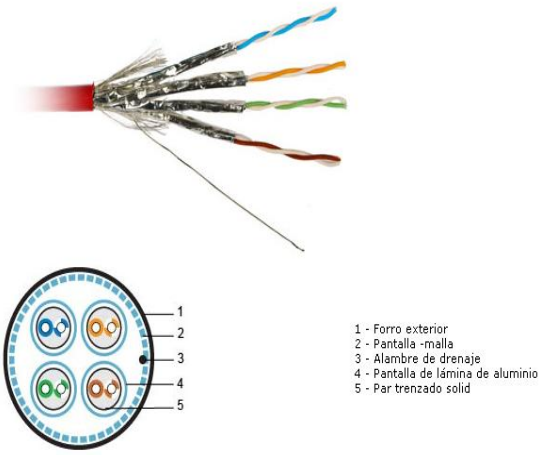


Figura 2 – 7: Esquema de cableado cat 7

Características Técnicas:

- Conductor: hilo de cobre desnudo, 23 AWG
- Aislamiento: SFS PO, 1.43 mm
- Cantidad de hilos: 8
- Cantidad de pares: 4
- Pantalla exterior: revestimiento trenzado de cobre estañado, que cubre el 55% del revestimiento del cable.
- Diámetro exterior del cable: 8.4 mm.
- Peso del cable: 61 kg/km.
- Esfuerzo durante el tendido del cable: 130 N máximo durante la instalación.

El cable tiene un valor nominal de resistencia ondulatoria de 100 Ohms en frecuencia de hasta 600 MHz.

2.5.1 Componentes del cableado estructurado

Se compone de los siguientes componentes:

- Sistema de cableado vertical (backbone).
- Sistema de cableado horizontal.
- Acometida de entrada (AI).
- Cuarto de telecomunicaciones (TC).
- Área de trabajo (WA).
- Cruzada horizontal (HC).

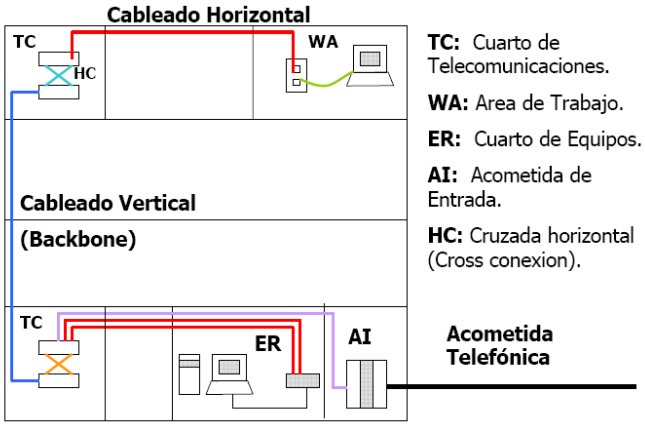


Figura 2 – 8: Componentes del cableado estructurado

Área de Trabajo (WA)

Los componentes del área de trabajo se extienden desde la terminación del cableado horizontal en la salida de información, hasta el equipo en el cual se está corriendo una aplicación sea de voz, datos, video o control.

Cableado Horizontal

Se extiende desde el área de trabajo hasta el armario del cuarto de telecomunicaciones (TC).

Incluye el conector de salida de telecomunicaciones en el área de trabajo, el medio de transmisión empleado para cubrir la distancia hasta el armario, las terminaciones mecánicas y la conexión cruzada horizontal.

Conexión cruzada: elemento usado para terminar y administrar circuitos de comunicación. Se emplean cables de puente (*jumper*) o de interconexión (patch cord).

No se permiten puentes, derivaciones y empalmes a lo largo de todo el trayecto del cableado. Se debe considerar su proximidad con el cableado eléctrico que genera altos niveles de interferencia electromagnética (motores, elevadores, transformadores, etc.) y cuyas limitaciones se encuentran en el estándar ANSI/EIA/TIA 569.

La máxima longitud permitida entre rosetas para una línea independientemente del tipo de medio de Tx utilizado es 90 m.

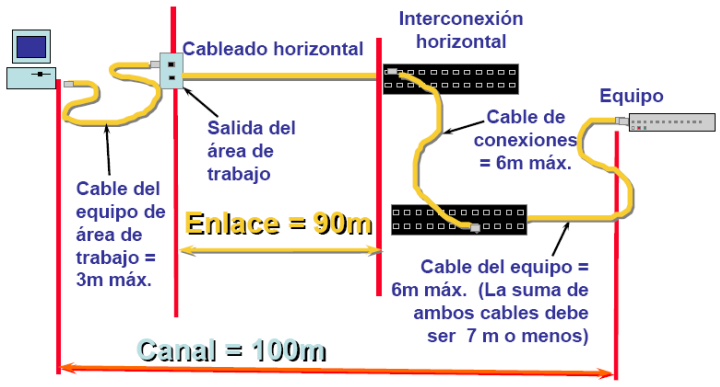


Figura 2 – 9: Esquema de conexión de cableado horizontal

Cableado vertical, troncal o backbone (dorsal)

El cableado vertical, permite la interconexión entre los gabinetes de telecomunicaciones, cuartos de telecomunicaciones y los servicios de la entrada. Consiste de cables de dorsal *cross-connects* principales y secundarios, terminaciones mecánicas y regletas o *jumpers* usados conexión dorsal-a-dorsal. Esto incluye:

- Conexión vertical entre pisos (*risers*).
- Cables entre un cuarto de equipos y cable de entrada a los servicios del edificio.
- Cables entre edificios.

La diferencia principal de un cableado horizontal y vertical, radica en su importancia, ya que en el cableado vertical, es el “tronco” de una red, por este pasan todos los servicios que queremos implementar, ya que se comunica con los otros cuartos de telecomunicaciones, estableciendo una red vertebral, estos tipos de cables deben ser robustos en cuanto a fabricación, velocidad y deben contemplar un respaldo en caso de falla.

Cuarto de Telecomunicaciones

Un cuarto de telecomunicaciones, es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. Todo edificio debe contar con al menos un cuarto de

telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

Acometida de entrada

La entrada a los servicios del edificio, es el punto en el cual el cableado externo hace interfaz con el cableado de la dorsal dentro del edificio. Este punto consiste en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto o espacio de entrada. Los requerimientos de la interface de red están definidos en el estándar TIA/EIA-569A.

2.5.2 Sistema Eléctrico

La norma ANSI/TIA/EIA-607, discute el esquema básico y los componentes necesarios para proporcionar protección eléctrica a los usuarios e infraestructura de las telecomunicaciones mediante el empleo de un sistema de puesta a tierra adecuadamente configurado e instalado.

Componentes de aterramientos:

TBB: (Telecommunications bonding backbone): Es un conductor de cobre usado para conectar la barra principal de tierra de telecomunicaciones (TMGB), con las barras de tierra de los armarios de telecomunicaciones y salas de equipos (TGB). Su función principal es la de reducir o igualar diferencias de potenciales entre los equipos de los armarios de telecomunicaciones, se deben diseñar de manera de minimizar las distancias, el diámetro mínimo es de 6 AWG, no se admiten empalmes, no se admite utilizar cañerías de agua como "TBB".

TGB (Telecommunications Grounding Busbar): Es la barra de tierra ubicada en el armario de telecomunicaciones o en la sala de equipos.
TMGB (Telecommunications main ground Busbar): Es la barra principal de tierra, ubicada en las "facilidades de entrada". Es la que se conecta a la tierra del edificio. Actúa como punto central de conexión de los TGB. Además la tierra de telecomunicaciones debe ser distinta de la de energía.

Características eléctricas

- Resistencia: No puede exceder 9.38 ohm / 100 m, no puede haber diferencias de más de 5% entre cables del mismo par.
- Capacitancia: No puede exceder 6.6 nF a frecuencia de 1 kHz.
- Impedancia característica 100 ohm +/- 15% en el rango de frecuencias de la categoría del cable.

2.6 SEGURIDAD DE LA INFORMACIÓN

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas (cada día) en sistemas operativos, aplicaciones de software, protocolos de red, *browsers* de Internet, correo electrónico y todas clase de servicios informático disponible.
Los sistemas operativos abiertos (como Unix y Linux) tienen agujeros mas conocidos y controlados, que aquellos que existen en sistemas operativos cerrados (como Windows). La importancia y ventaja del código abierto, radica en miles de usuarios analizan dicho código en busca de posibles *bugs* y ayudan a obtener soluciones en forma inmediata.
Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad y herramientas de *hacking* que los explotan, por lo que

hoy también se hace indispensable contar con productos que conocen esas debilidades, puedan diagnosticarlas y actualizar el programa afectado con el parche adecuado.

La seguridad de la información se define como “Las medidas adoptadas para prevenir el uso no autorizado, mal uso, modificación, por negación de uso de conocimiento de hechos, datos o capacidades [6].
La seguridad de la información surge debido a la necesidad de contrarrestar las amenazas que existen en el medio.
La seguridad de la información se entiende como la preservación de las siguientes características: confidencialidad, integridad y disponibilidad.

2.6.1 Confidencialidad

Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos, se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje.

2.6.2 Integridad

Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera.

2.6.3 Disponibilidad

Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten [6].

2.7 ATAQUES Y VULNERABILIDADES

Para poder planear e implementar una buena estrategia de seguridad, primero debe tener en cuenta algunos de los problemas que un atacante motivado y determinado explota para comprometer los sistemas.

2.7.1 Amenazas a la Seguridad de la red

Los malos hábitos cuando se configuran los siguientes aspectos de una red pueden incrementar los riesgos de ataques.

2.7.1.1 Arquitecturas inseguras

Una red mal configurada, es un punto de entrada principal para usuarios no autorizados. Al dejar una red local abierta, vulnerable a la Internet que es altamente insegura, es casi como que dejar una puerta abierta en un vecindario con alta criminalidad.
Puede que no ocurra nada durante un cierto tiempo, pero eventualmente alguien intentará aprovecharse de la oportunidad.

2.7.1.2 Redes de difusión

Los administradores de sistemas a menudo fallan al darse cuenta de la importancia del hardware de la red en sus esquemas de seguridad. El hardware

simple, tal como switches y routers a menudo se basan en *broadcast* (difusión) o en el principio de sin-interruptores; esto es, cada vez que un nodo transmite datos a través de la red a un nodo recipiente, los switches o routers hace una difusión de los paquetes de datos hasta que el nodo recipiente recibe y procesa los datos.

2.7.2 Ataques en redes y servidores

1.- TCP Connect (Scanning)

Esta es la forma básica del escaneo de puertos TCP. Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con a él.
Su principal desventaja es que este método es fácilmente detectable por el administrador del sistema.

2.- TCP SYN Scanning

La técnica TCP SYN Scanning, se implementa un escaneo de "media-apertura", dado que nunca se abre una sesión TCP completa. Se envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.
La principal ventaja de esta técnica de escaneo es que pocos sitios están preparados para registrarlos. La desventaja es que en algunos sistemas Unix, se necesitan privilegios de administrador para construir estos paquetes SYN.

3.- ICMP Flooding

Parecido al SYN Flood, el *flood* de echo del ICMP o mejor conocidos como Ping Floods, trabaja sobrecargando a una máquina host con información en demasía, así logrando que la velocidad de la red se reduzca a niveles inaceptables. Estos ataques utilizan el comando ping, el cual usa el protocolo ICMP. El comando que por lo normal es usado para enviar mensajes de prueba a una dirección IP de una máquina en Internet para ver si está disponible. Si el host está disponible responderá.

4.- "IP Spoofing" (ataque de suplantación)

Involucra cambiar el encabezado de un paquete en un mensaje, para indicar que él viene desde otra IP en vez de la verdadera. Las direcciones suplantadas son usualmente las de sistemas de confianza, por lo que permite a un atacante pasar a través de un firewall o router sin ser filtrado. La mayoría de los firewalls modernos protegen en contra de *"IP spoofing".*

5.- Ataque Smurf

Un ataque *Smurf* es un ataque DoS que utiliza IP *spoofing*. El ataque *Smurf* funciona dirigiendo ping *floods* (inundación de ping) con IP spoofed a una dirección IP de *broadcast.* Las direcciones IP de *broadcast* son las que contienen todos unos o todos ceros en la porción del host de la dirección.
Las direcciones de *broadcast* son usadas para transmitirle la misma información a muchas máquinas. Si la información es enviada a la dirección *broadcast,* entonces sólo tendrá que ser enviada una sola vez para que le llegue a todas las máquina con esa dirección de *broadcast*.

6.- Utilización de *exploits*

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrado un error en los programas utilizados.
Los programas para explotar estos "agujeros" reciben el nombre de *exploits* y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos *exploits* (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

7.- Buffer *overflows*

Ocurre cuando el número de caracteres de una entrada de texto, excede el máximo número permitido por el programador que escribió cierto *software*, con lo cual puede provocar comportamientos inesperados, como ganar acceso a ciertos espacios de memoria, bloquear o “botar” un sistema, o ganar acceso a sistemas o redes. Muchos hoyos de seguridad están basados en problemas del tipo buffer *overflow.*

8.- Obtención de Passwords

Este método comprende la obtención por "Fuerza Bruta", de aquellas claves que permiten ingresar a los sistemas, aplicaciones, cuentas, etc. Muchas *passwords* de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En este caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras

a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la *password* correcta.

2.8 ELEMENTOS Y HERRAMIENTAS DE PROTECCIÓN (REDES Y SERVIDORES)

2.8.1 Firewall

Un firewall de la red es una barrera contra el potencial de actividades maliciosas y que permite que los usuarios de la red puedan pasar por una puerta para llevar a cabo sus tareas de comunicación, entre la red asegurada interna y la red insegura externa. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

A continuación se describen los tipos de firewall*:*

Existen distintos tipos de firewalls, dependiendo de como estos funcionan o en que capa del modelo TCP (Transmission Control Protocol)/IP (Internet Protocol) ellos trabajan. Los principales son los siguientes:

2.8.1.1 Filtrado de paquetes

El filtrado de paquetes se basa en la decisión de reenviar un paquete basado en la información encontrada en la capa de transporte TCP/UDP (User Datagram Protocol), es decir, a través de la IP o en el Protocolo de Control de Transmisión (TCP) o Paquete de Datagrama de Usuario (UDP). En este modo se actúa

como un router con algo de “inteligencia”, pero este filtrado es realizado sobre paquetes individuales, es decir, no sigue las sesiones TCP. Esto trae como problema que es difícil detectar paquetes suplantados (*spoofing*). El filtrado de paquetes está configurado para permitir o bloquear tráfico dependiendo de la dirección de IP de origen o destino, puertos de origen y destino y el tipo de protocolo: TCP, UDP, ICMP (Internet Control Message Protocol), etc. También existe el filtrado de paquetes usando inspección *stateful* permite mantener rastro de las sesiones de red, así cuando este recibe un paquete ACK, este puede determinar su legitimidad haciendo match del paquete en una tabla de conexiones.

2.8.1.2 Firewall de aplicaciones

Este firewall actúa como un intermediario en las sesiones de red. Una conexión termina en el firewall y una sesión separada es iniciada desde el firewall hasta el host de destino. Las conexiones son analizadas completamente en todas las capas hasta la capa de aplicación para determinar si estas son permitidas.
Esto implica un mayor nivel de seguridad en comparación con el filtrado de paquetes y el filtrado de paquetes con inspección *stateful,* pero también afecta el *performance*, dado el trabajo que ello conlleva.

2.8.2 IDS (Sistema de Detección de Intrusos)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés, *Intrusion Detection System*), es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a los recursos.

Un IDS protege a un sistema contra ataques, malos usos y compromisos. Puede también monitorear la actividad de la red, auditar las configuraciones de la red y sistemas por vulnerabilidades, así como analizar la integridad de los datos. Dependiendo de los métodos de detección que se selecciona a utilizar, existen numerosos beneficios directos e incidentales de usar un IDS.
Los tipos más importantes de IDSes mencionados en el campo de seguridad son conocidos como IDSes *basados en host* y *basados en red*.

2.8.2.1 IDS basado en host

Un IDS basado en host, analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera). Consultan diferentes tipos de registros de archivos (kernel, sistema, servidores, red, cortafuegos) y comparan los registros contra una base de datos interna de peculiaridades comúnes sobre ataques conocidos. Los IDSes basados en host de Linux y Unix hacen uso extensivo de syslog y de su habilidad para separar los eventos registrados por severidad (por ejemplo, mensajes menores de impresión versus advertencias importantes del kernel). Además filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados posteriormente.

2.8.2.2 IDS basados en la red

Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDS basados en host. La filosofía de diseño de un IDS basado en la red, es escanear los paquetes de red al nivel del enrutador o host,

auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, puede escanear su propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete.

Los IDSes que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escaners, husmeadores y otras herramientas de auditoria y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como:

- Engaño de direcciones IP (IP Spoofing).
- Ataques de rechazo de servicio (DoS).
- Envenenamiento de caché ARP.
- Corrupción de nombres DNS.

La mayoría de los IDSes basados en la red requieren que el dispositivo de red del sistema host sea configurado a modo *promiscuo*, lo cual permite al dispositivo capturar *todos* los paquetes que pasan por la red.

2.8.2.2.1 Snort

Snort es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión) [7].

Está diseñado para ser completo y preciso en el registro de actividades maliciosas de la red y en notificar a los administradores cuando existe una potencial violación o abertura.

Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un Sistema Detector y Preventor de Intrusos.

Puede funcionar como sniffer (se ve en consola y en tiempo real qué ocurre en la red, todo el tráfico disponible), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se “autentifica”. Así se sabe cuando, de donde y cómo se produjo el ataque.

La característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques. Snort tiene una base de datos de ataques que se está actualizando constantemente y a la cual se puede añadir o actualizar a través de la Internet. Los usuarios pueden crear firmas basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort (localizada en *http://www.snort.org/lists.html*), para que así todos los usuarios de Snort se puedan beneficiar. Esta ética de comunidad y compartir ha convertido a Snort en uno de los IDSes basados en red más populares, actualizados y robustos.

2.8.3 Hardening a servidores

El Hardening es una técnica compuesta por un conjunto de actividades llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de este [8].

Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad.

Una de las primeras cosas que hay que dejar en claro del hardening de sistemas operativos, es que no necesariamente logrará forjar equipos invulnerables. En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender globalmente un sistema.

CAPITULO 3: REQUERIMIENTOS DE LA SOLUCIÓN

3.1 INTRODUCCIÓN

Se analizarán los requerimientos y necesidades de la Empresa para su posterior desarrollo de alternativas de solución que satisfagan todas las problemáticas que esta presenta.

3.2 DOCUMENTACIÓN

TELECTRICA LTDA. Es una empresa que cuenta con profesionales de una alta calificación, ampliamente capacitados para evaluar, asesorar y ejecutar proyectos relacionados con las áreas de ingeniería, diseño y construcción y proyectos de montajes eléctricos, cuyo principal objetivo es otorgar soluciones integrales a los requerimientos de clientes y satisfacer la demanda por medio de un servicio integral de ejecución de obras bajo esquemas previsibles de plazos, costos y calidad de producción de las mismas.

Misión: Soluciones integrales a los requerimientos de obras de construcción, proyectos eléctricos y tecnológicos de nuestros clientes, otorgando un servicio de primer nivel y asegurando la calidad de nuestras intervenciones mediante el aporte de personal altamente calificado, tanto en la planificación profesional de los proyectos, en su calidad de equipo humano, como en su implementación técnica.

Además, se proyecta la relación con nuestros clientes como verdaderos socios estratégicos, apoyándolos en el logro de sus metas corporativas a través del mejoramiento continuo de sus plataformas tecnológicas.

Visión: Proyectar nuestra empresa como líder en soluciones de construcción, eléctricas, apoyando permanentemente el desarrollo y eficiencia de nuestros clientes.

3.2.1 Personal actual y futuro de la Empresa

La nueva infraestructura se divide en 2 pisos, en el primer piso del edificio a trasladarse se encuentra personal administrativo mientras que en el segundo piso se encuentra por lo general personal gerencial.

Actualmente en la infraestructura actual, se encuentran 10 personas teniendo distintas responsabilidades y cargos correspondientes, se espera una expansión futura a 22 personas más adelante en el nuevo edificio.

En las siguientes tablas, se dará a conocer la expansión del personal que se tiene pensada a futuro y los puntos de red requeridos que deberá tener la red local.

Oficinas 1° Piso

Tabla 3 – 1: Personal ubicado en el 1º piso.

Of. Recepción	
1 Punto de Red.	Recepcionista
Of. Administración (1)	
2 Puntos de Red.	Jefe Personal Administrativo
Of. Administración (2)	
2 Puntos de Red.	Jefe Adquisiciones Administrativo
Of. Contabilidad	

3 Puntos de Red.	Jefe de Contabilidad. Administrativo Administrador de Redes.
Of. Bodega	
1 Punto de Red.	Bodeguero

Total 1° piso: 9 puntos de red.

Oficinas 2° Piso

Tabla 3 – 2: Personal ubicado en el 2º piso.

Of. Gerencia General	
1 Punto de Red.	Gerente Gral.
Of. Proyectos	
4 Puntos de Red.	Jefe de Proyectos Arquitecto Dibujante 1 Dibujante 2
Administración Gral.	
3 Puntos de Red.	Jefe de Operaciones Director de Obra Jefe de Finanzas
Recursos Humanos	
2 Puntos de Red.	Jefe de R.R.H.H. Administrativo R.R.H.H.
Sala de Reuniones	
3 Puntos de Red.	Vacantes

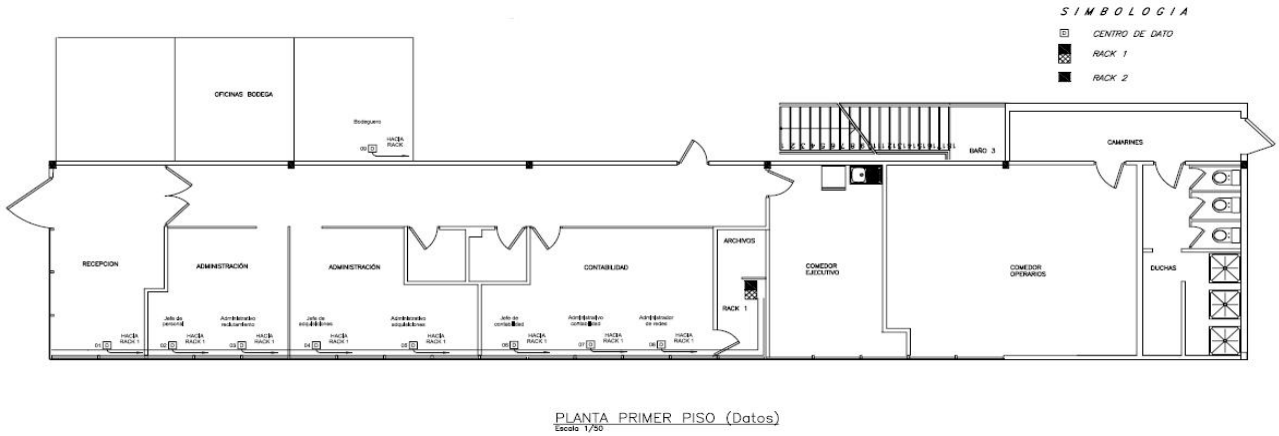
Total 2° piso: 13 puntos de red.

Total Edificio: 22 puntos de red

3.2.2 Planos de puntos de red Edificio

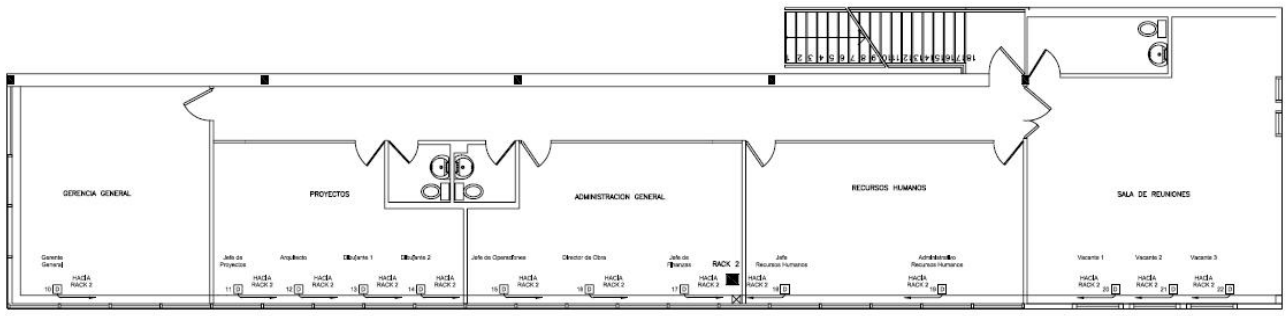
A continuación se da a conocer los planos del edificio, con sus respectivos puntos de red de la nueva infraestructura. Para una mejor visualización de los planos, revisar ANEXO 6.

1° Piso



PLANTA PRIMER PISO (Datos)
Escala 1/50

2° Piso



PLANTA SEGUNDO PISO (Datos)
Escala 1/50

Figura 3 – 1: Plano de red edificio.

Teniendo en cuenta 22 puntos de red como petición de la Empresa se requiere sectorizar en 2 grupos cada puesto de trabajo, para eventual acceso al servidor de archivos. Esta sectorización se tendrá en cuenta para la creación de carpetas para su compartición teniendo 2 niveles de acceso. (Gerencia y administrativo)

3.2.3 Equipos y hardware actual de la Empresa

Como se mencionó anteriormente se cuenta con 10 computadores entre ellos notebooks y Pcs más el servidor.

Las características de los equipos son relativas. Lo importante es que se realizó una revisión a los que posean mejores condiciones de servidor.

Se obtiene la conclusión que 3 equipos de los 10 computadores, son aptos para ser considerados usados como servidores, dejando las siguientes características.

Tabla 3 – 3: Equipos y hardware de la Empresa.

Computador Nº 1

Procesador	Intel Pentium 4 – 2 Ghz
RAM	1 GB
Disco Duro	80 GB IDE

Computador Nº 2

Procesador	AMD Athlon 64 – 2.2 Ghz
RAM	2 GB
Disco Duro	160 GB SATA

Computador Nº 3

Procesador	Intel Pentium 4 – 1.6 Ghz
RAM	1GB
Disco Duro	120 GB IDE

Los demás computadores cuentan con características como procesadores Pentium III con 512 Ram y 40 Gb, dejándolos para uso para el personal de la Empresa.

3.3 PROBLEMÁTICAS Y SITUACIÓN ACTUAL

La red local que cuenta actualmente la Empresa carece de seguridad, no presenta un servidor de correo, servidor de archivos con jerarquía, ni una red inalámbrica.

Esta presenta un servidor central con S.O Windows 2000, que a su vez da acceso a Internet a 10 computadores, por medio de un plan de acceso a Internet de una compañía ISP ubicada en la infraestructura actual.

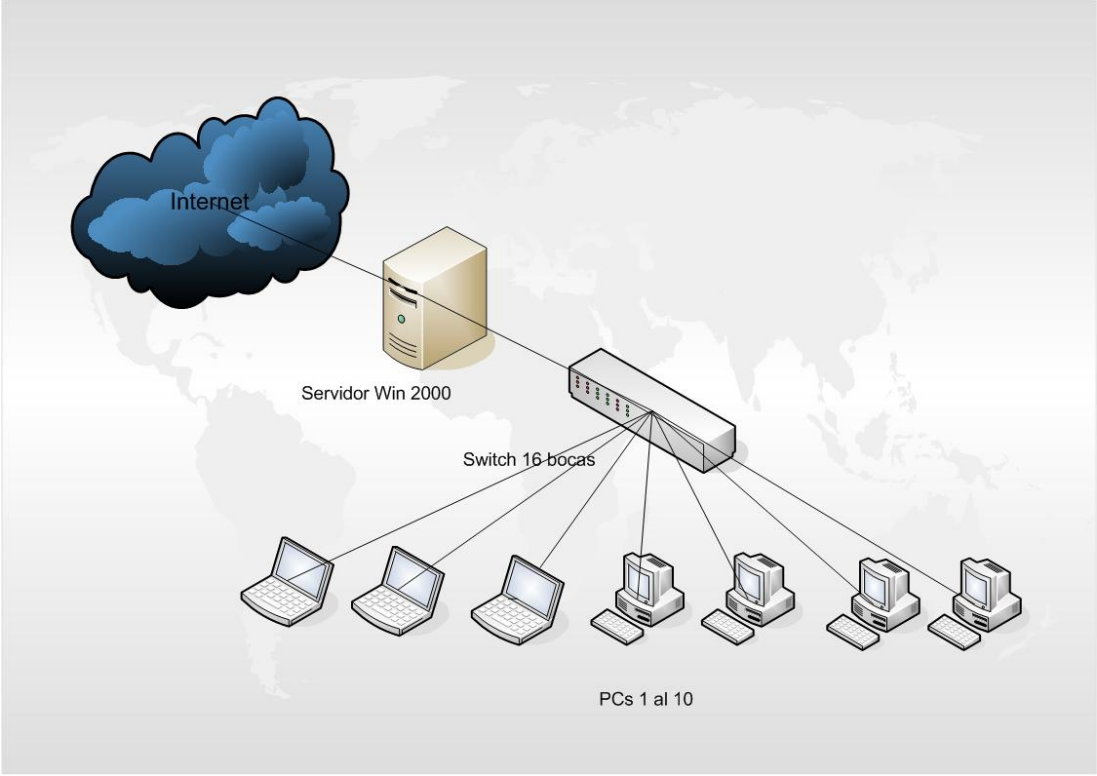


Figura 3 – 2: Esquema situación actual de la Empresa.

Por el motivo a la expansión que desea realizar la Empresa en su infraestructura y al aumento de contrato de personal, se desea cambiar de ubicación (domicilio) a la comuna de Pudahuel, Santiago de Chile a una nueva infraestructura. Por ende surgen nuevas necesidades a satisfacer a la Empresa, esto conlleva a diseñar una red tal que cumpla con todos los requisitos que se detallarán a continuación.

- Red de área local de alta velocidad, incluyendo servidores de alta calidad que puedan ser administrados por una interfaz amigable, cómoda y eficiente y teniendo presente una futura expansión.

- Que cuente con un servidor de archivos para la compartición de datos a nivel de red, accediendo a él con autentificación dependiendo de la jerarquía del usuario.

- Poseer un servidor de correo que permita enviar y recibir e-mail vía Internet e Intranet y de fácil administración.

- Soporte WIFI, por la gran masificación de la red Wireless (WLAN) que ha tenido en el país, la movilidad, versatilidad y conectividad que permite otorgar al personal que posean equipo portátil.

Además que tenga los siguientes requerimientos de seguridad:

- Bloqueo de correos *spam* a la empresa, lo cual provoca un problema de seguridad, si alguno llegase a tener virus.

- Bloqueos a páginas Web, con lo que bajan programas (muchos de ellos ilegales), virus, mp3, o acceden a material pornográfico, en donde se podría dar el caso que la empresa tenga problemas legales si alguien accediera a ella.

- Limitar el ancho de banda a usuarios, dejando a los servicios más importantes para su uso.

- Protección ante ataques externos ya que se podrían tener los consiguientes riesgos, pérdida de información, robo de información, tiempo fuera de línea, pérdida de tiempo, etc.

- Bloqueo y filtrado de puertos para denegación de programas computacionales, que no sean uso de la Empresa.

- Detección de accesos no autorizados a la red o a un computador.

Todos los requerimientos anteriores pueden ser solventados por un dispositivo UTM[1] (*Unified Threat Management*) o Gestión Unificada de Amenazas, este término se utiliza para describir un firewall de red que engloban múltiples funcionalidades en una misma máquina. Las funcionalidades que debe incluir son las siguientes:

- Antispam.
- Antiphishing.
- Filtro de contenidos.
- Antivirus.

[1] UTM es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.
El término fue utilizado por primera vez por Charles Kolodgy en 2004.

- Detección/prevención de Intrusos (IDS/IPS)

Este además se encargará de dar acceso a Internet a la red interna.

La solución de la red local y seguridad debe cumplir las siguientes necesidades:

TELECTRICA LTDA. necesita de una solución de bajo costo relativo, dado que es una empresa pequeña de presupuesto limitado, pero esta demanda no debe ser un impedimento para que sus necesidades no puedan ser satisfechas o sea insegura o limitada en funciones o características.

La solución a desarrollar debe ser fácil de administrar, es decir, que posea una interfaz gráfica (sin comandos del tipo Unix), fácil de acceder (vía Web de preferencia), en definitiva que tenga una curva de aprendizaje que permita al personal que administre el firewall, no poseer profundos conocimientos informáticos o de programación para usarlo rápidamente y que al mismo tiempo cometa menos errores posibles al cargar reglas.

Además de intentar de realizar la solución ocupando recursos (hardware, equipos) ya disponibles en la Empresa.

Las características técnicas del dispositivo UTM que se requieren son:

- Soporte de más de 25 usuarios como mínimo.
- Soporte de DMZ (Zona Desmilitarizada).
- Gestión del Trafico/QoS.
- Antivirus, IDS/IPS (Instrusion Prevention System).
- Soporte de NAT (Network Address Translation).

En el capitulo siguiente se detallará 3 alternativas de solución con respecto al firewall a ocupar, ya que el será el encargado de proveer de acceso a Internet a la red interna, además de establecer políticas de control de acceso, protección IDS, entre otras opciones de configuración.

CAPITULO 4: ANÁLISIS TÉCNICO Y ECONÓMICO DE LAS ALTERNATIVAS DE SOLUCIÓN

4.1 INTRODUCCIÓN

En el siguiente capitulo se dará a conocer las posibles alternativas de solución, conociendo sus detalles técnicos y económicos, dando a elegir una solución y desarrollándola a lo largo del trabajo de titulación, planteándola con ilustraciones la instalación de toda la red corporativa de la Empresa.

4.2 ALTERNATIVAS DE SOLUCIÓN

En el mercado existen soluciones de seguridad que difieren de características, dependiendo de las necesidades de las empresas. Existen las soluciones de hardware y software. Las soluciones de seguridad se pueden dividir en las soluciones en los del tipo software libre y software del tipo propietario.
Se analizaran 3 soluciones en el ámbito técnico y económico.

4.2.1 Análisis técnico de alternativas de solución

Antes de entrar al análisis técnico se explicará algunas mediciones que efectúan los fabricantes a los equipos firewall, para dar las características técnicas del equipo.

Existen dos grandes grupos de tipos de medidas, de conformidad (conformance) y de rendimiento (performance). La conformidad permite comprobar si un dispositivo cumple con las recomendaciones, el rendimiento, nos dice que tan bien se comporta el equipo bajo diferentes condiciones. Por

ejemplo eligiendo un grupo de dispositivos todos ellos pueden “pasar” las pruebas de conformidad, pero con las pruebas de rendimiento se puede comparar los dispositivos.

Tabla 4– 1: Pruebas de conformidad y rendimiento

Pruebas de Conformidad	Pruebas de Rendimiento
¿Envía y recibe los mensajes en el formato correcto?	¿Realiza correctamente la priorización de mensajes?
¿El dispositivo se apaga al recibir un mensaje inapropiado?	¿Con alta carga de tráfico continúa funcionando?
¿Realiza la tarea deseada?	¿Bloquea comunicaciones no deseadas?

Las que interesan son las pruebas de rendimiento con el enfoque del estándar IETF[2] (BMWG), grupo de Benchmarking Methodology Working Group que se consideran mas apropiado para medidas de performance.

La principal meta del BMWG es de realizar una serie de recomendaciones en lo concerniente a medidas de performance en tecnologías de interredes (internetworking technologies), más aún estas recomendaciones se pueden enfocar en los sistemas o servicios que son construidos por estas tecnologías.

Cada recomendación describirá:

- La clase de equipo, sistema, o servicio brindado.
- Discutirá las características de performance correspondiente a cada clase.
- Deberá identificar claramente el tipo de medida.
- Deberá brindar los requerimientos para la presentación de los resultados obtenidos, en un formato común y no ambiguo.

[2] El **IETF** (**I**nternet **E**ngineering **T**ask **F**orce, Grupo de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986.

El alcance del BMWG está limitado a la caracterización de la tecnología utilizada mediante estímulos simulados en ambientes de laboratorio. En otras palabras el BMWG no pretende producir benchmarks para redes operacionales.
La terminología y metodología de pruebas se desarrollan según la La RFC[3] 2544, que discute y define un número de pruebas que pueden ser utilizadas para describir y comparar las características de performance de dispositivos de interconexión de redes. Asimismo describe los formatos para el reporte de los resultados de las pruebas.
Una de las medidas importantes en los dispositivos firewall es el throughput que es la máxima tasa a la cual ninguna de las tramas ofrecidas es descartada por el dispositivo, el procedimiento a medir según RFC 1242, es enviar un número específico de tramas a una tasa específica a través del DUT (Device Under Test, en este caso el equipo firewall), luego contar las tramas correctamente recibidas desde el DUT. Si la cantidad de tramas ofrecidas es menor a la cantidad de tramas correctamente recibidas desde el DUT, la tasa del flujo ofrecido se reduce y el ensayo se vuelve a correr.
El throughput es la máxima tasa a la cual la cantidad de tramas transmitidas por el DUT es la misma que la transmitida por el equipo de prueba. El ensayo debe realizarse con los formatos y tamaños de tramas especificados.

4.2.1.1 Cisco ASA 5505 SEC PLUS

Cisco ASA 5505 es una solución de nueva generación, diseñada para mejorar la defensa de las redes en pymes, oficinas remotas y pequeñas empresas. El dispositivo Cisco ASA 5505 es un componente central de la estrategia Self-Defending Network de Cisco Systems. Forma parte de una familia de

[3] Las RFC (Peticiones de comentarios) son un conjunto de documentos que sirven de referencia para la comunidad de Internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, los estándares, las tecnologías y los protocolos relacionados con Internet y las redes en general.

dispositivos de seguridad de red multifunción que ofrece la amplitud y profundidad necesarias para proteger empresas de cualquier tamaño. Su defensa proactiva frente a amenazas evita que los ataques se extiendan por toda la red de la empresa, permitiendo a las empresas proteger varios segmentos de una red al mismo tiempo, lo que consolida la inversión en seguridad y minimiza la complejidad de las instalaciones y reduce los costes operativos. Posee un hardware de 256 de Memoria y una memoria flash de 64 MB.

Detalles Técnicos

Tabla 4 – 2: Detalles técnicos equipo Cisco Asa 5505

Rendimiento de Firewall (throughput)	150 Mbps
Rendimiento de VPN (throughput)	100 Mbps
Usuarios	50
Túneles VPN	25
Interfaces (10/100)	8 puertas 10/100 Mbps c/ 2 Power over Ethernet. 1: DB-9 Serial
NAT/NAT dinámico	SI
VLAN	SI
Enrutamiento dinámico	SI
VoIP	SI
Prevención de intrusos	SI
DMZ	SI
Balanceo de Carga	NO
Gestión del tráfico / QoS	SI

Administrable vía http	SI
Aplicación Proxies	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323, TFTP

4.2.1.2 Watchguard Firebox Edge X20e

Firebox Edge X20e, se conecta fácilmente a la red ubicándose entre la conexión a Internet y la red interna. Esta configuración define una conexión para Internet y otra para la red corporativa protegida. Incorpora 6 puertas 10/100 para la red LAN. Firebox X Edge e-Series es ideal para pequeñas empresas que requieran un excelente nivel de protección y prestaciones.

Detalles Técnicos

Tabla 4 – 3: Detalles técnicos equipo Watchguard Firebox Edge X20e

Rendimiento de Firewall (throughput)	100 Mbps
Rendimiento de VPN (throughput)	35 Mbps
Usuarios	30
Túneles VPN	15
Interfaces (10/100)	6: 10/100 1: DB-9 Serial
NAT/NAT dinámico	SI
VLAN	SI (con actualización)
Enrutamiento dinámico	NO
VoIP	SI
Prevención de intrusos	SI
DMZ	SI

Balanceo de Carga	SI
Gestión del tráfico / QoS	SI
Administrable vía http	SI
Aplicación Proxies	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323, TFTP

4.2.1.3 Smoothwall Firewall

Smoothwall Firewall es una solución de Seguridad Integral que protege la red y mejora la conectividad, ofreciendo todos los servicios que se necesitan y fácil de configurar.

Smoothwall Firewall es un appliance basado en tecnología de inspección de estados que identifica cada paquete entrante, reconociendo la fuente y el contenido de cada paquete Smoothwall Firewall puede proteger contra intrusiones no deseadas o ataques externos de hackers.

Smoothwall Firewall es 100% open-source e incluye, entre sus funciones principales, una variedad de características:

- Firewall con inspección de estados.
- Antivirus HTTP/FTP.
- Filtro de Contenido Web.
- Antivirus POP3/SMTP, Anti-Phishing y Antispam.
- VPN SSL/TLS.
- IDS y variadas utilidades más.

Firewall con inspección de estados

Smoothwall Firewall es un appliance basado en tecnología de inspección de estados que identifica cada paquete entrante, reconociendo la fuente y el

contenido de cada paquete, Smoothwall puede proteger contra intrusiones no deseadas o ataques externos de hackers.

Seguridad Web

El filtro de contenidos de Smoothwall Firewall mantiene una experiencia de navegación Web de forma segura, protegiendo contra virus y contenidos no deseados como violencia, pornografía o software pirata. Permite monitorizar accesos, mejorando así la productividad. También es útil en compañías que buscan que sus empleados naveguen solo por sitios bien definidos, asegurando así la integridad de los negocios y un uso adecuado de los recursos.

VPNs fáciles y rápidas

Con OpenVPN, se puede levantar un túnel seguro encriptado con SSL entre sucursales de tu compañía o entre agentes remotos hacia la red corporativa de la Empresa. Los clientes soportados abarcan una gran cantidad de Sistemas Operativos como lo son Linux, Mac OSX o Windows.

Detalles Técnicos

Las algunas características técnicas correspondientes a este software dependen del equipamiento hardware que tenga el equipo en donde se va a instalar.
El siguiente detalle será dado ocupando un servidor de acuerdo a las siguientes características:

Procesador: Intel Pentium 4 – 2.2 Ghz
Memoria Ram: 1 GB
Disco Duro: 80 GB

Tabla 4 – 4: Detalles técnicos equipo software Smoothwall Firewall

Rendimiento de Firewall (throughput)	500Mbps
Rendimiento de VPN (throughput)	150 Mbps
Usuarios	100
Túneles VPN	25
Interfaces (10/100)	3: 10/100/1000 (depende del hardware)
NAT/NAT dinámico	SI
VLAN	SI (con actualización)
Enrutamiento estático	SI
VoIP	SI
Deteccion de intrusos (IDS)	SI
DMZ	SI
Balanceo de Carga	NO
Gestión del tráfico / QoS	SI
Administrable vía http	SI
Aplicación Proxies	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323.

4.2.2 Cuadro técnico comparativo de alternativas de solución

A continuación se muestra una tabla técnica comparativa de las 3 soluciones.

Tabla 4 – 5: Cuadro técnico comparativo de alternativas de solución

Equipos / Características	Cisco ASA 5505 SEC PLUS	Watchguard Firebox Edge X20e	Smoothwall Firewall
Rendimiento de Firewall	150 Mbps	100 Mbps	500Mbps
Rendimiento de VPN	100 Mbps	35 Mbps	150 Mbps
Usuarios	50	30	100
Túneles VPN	25	15	25
Interfaces (10/100)	8 puertas 10/100 Mbps c/ 2 Power over Ethernet. 1: DB-9 Serial	6: 10/100 Mbps 1: DB-9 Serial	3: 10/100/1000 Mbps (depende del hardware)
Detección de intrusos	SI	SI	SI
Prevención de intrusos	SI	SI	SI (requiere instalación)
DMZ	SI	SI	SI
Gestión del tráfico / QoS	SI	SI	SI
Administrable vía http	SI	SI	SI
Aplicación Proxies	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323, TFTP	HTTP, HTTPS, SMTP, FTP, POP3, SIP, H.323.

El rendimiento real de las soluciones puede variar dependiendo de las condiciones de la red y los servicios activados.

Se visualiza en la tabla comparativa que Smoothwall Firewall es superior en rendimiento (performance) frente a las otras soluciones, ya que no esta limitado por el hardware como la solución de Cisco y de Watchguard. Esto además involucra un soporte mayor de usuarios en la red LAN, ya que un usuario ocupa recursos del firewall, ya sea cuando, se conecta a Internet, envía un mail, realiza conferencias, descarga archivos, etc. Esto se traduce en que si el firewall no posee capacidad de procesar altos paquetes por segundo, se ralentizará la red y a su vez crea congestión y no permite el correcto funcionamiento de la empresa.

En cuanto al número de interfaces de red se tiene que las soluciones propietarias posee una mayor cantidad. Esto beneficia a las redes que necesiten establecer un mayor control de política de seguridad a interfaces, es decir, conectar en una puerta de red, servidores públicos, en otra puerta de red conexión Wifi estableciendo que paquetes se conectan o envían de una interfaz a otra.

Watchguard ofrece balanceo de carga en dos interfaces permitiendo conectar dos ISP (Internet Service Provider; proveedor de servicios de Internet), con capacidad failover, haciendo ininterrumpida la conexión de Internet.
Cisco además de sus 8 interfaces posee dos con POE (Power over Ethernet), permitiendo conectar teléfonos IPs, o dispositivos compatibles.
Smoothwall Firewall en cuanto al rendimiento solo lo limita el hardware, donde se encuentra instalado, es decir a mayor hardware, mayor procesamiento de paquetes. Por ende mayor rendimiento en general y a conexiones VPN (Virtual Private Network). En cambio una solución como Cisco o Watchguard se encuentran limitados por el procesador que usan y las memorias internas que poseen, no pudiéndose realizar ninguna actualización en cuanto a hardware.

Por ejemplo, si se llegase a requerir un hardware con mayor procesamiento por parte de la empresa para aplicaciones que requieran más tráfico, como podría ser video conferencia, se tendría que comprar un nuevo equipo y por ende una nueva licencia.

En resumen, las características técnicas de las 3 soluciones cumplen con los requerimientos antes mencionados en el capitulo anterior, pero Smoothwall sobresale en cuanto al rendimiento.

Algunas características técnicas que se mencionaron anteriormente de las soluciones de Cisco y de Watchguard no presenta Smoothwall. Pero estas no están siendo requeridas por parte de la empresa.

4.2.3 Análisis económico de alternativas de solución

A continuación se describen las soluciones indicando precios y garantías y/o servicios de actualización.

4.2.3.1 Cisco ASA 5505 SEC PLUS

Tabla 4 – 6: Detalles económico Cisco Asa 5505

Ítem	**Costo**
Cisco ASA 5505 SEC PLUS	US$ 1.420
SMARTnet (incluye 1 año)	US$ 0
Actualizaciones (AV, IPS, AS)	Sin considerar
TOTAL (Precios sin IVA)	**US$ 1.420**

Cotización Proveedor I-Technology Ltda. *www.i-technology.cl*

SMARTnet™ de Cisco:

1. Renovación de tecnología (Cisco IOS®): mantenimiento, *releases* menores y mayores del software Cisco IOS vía Web o a través del envío de medios le permiten maximizar su inversión en tecnología Cisco.

2. Herramientas en línea y recursos de transferencia de conocimiento (Cisco.com): acceso registrado al soporte en línea de Cisco, líder en la industria, con avanzadas herramientas técnicas en línea, tales como el Bug Toolkit y el Troubleshooting Engine.

3. Centros de soporte telefónico (TAC): Acceso directo a nivel mundial, 24x7x365, a la experiencia y conocimiento técnico de Cisco.

4. Reemplazo rápido de partes: Una parte de reemplazo se enviará a la localidad del cliente, de acuerdo con la opción de entrega que se seleccione.

4.2.3.2 Watchguard Firebox Edge X20e

Tabla 4 – 7: Detalles económico Watchguard Firebox Edge X20e

Ítem	**Costo**
Firebox Edge X20e	US$ 650
Servicio LiveSecurity (1 año gratis)	US$ 0
Actualizaciones AV	US$ 240 (1 año)
Actualizaciones filtro contenidos	US$ 110 (1 año)
Actualizaciones IDS/IPS	US$ 120 (1 año)
TOTAL (Precios sin IVA)	**US$ 1120**

Cotización Proveedor Viared Computación Ltda. *www.viared.cl*

LiveSecurity incluye:

- Garantía de hardware con sustitución anticipada de hardware.
- Actualizaciones de software.
- Soporte Técnico.
- Recursos de Auto-Ayuda.

Garantía de reemplazo de hardware adelantado

Suscripción activa LiveSecurity se extiende de un año de garantía de hardware que se incluye con el equipo.

El servicio de suscripción da acceso a las actualizaciones tanto de software actual y funcional equipamiento.

Soporte Técnico

Equipos de expertos dispuestos a solucionar problemas.

La suscripción incluye el servicio de clase mundial de apoyo técnico.

Representantes disponibles 12 horas al día, 5 días a la semana en la zona horaria local.

4.2.3.3 Smoothwall Firewall

Tabla 4 – 8: Detalles económico software Smoothwall Firewall.

Ítem	**Costo**
Software Smoothwall Firewall	US$ 0
Soporte	-
Hardware (3 NIC 1000 Mbps)	US$ 54
Actualizaciones IDS/IPS	US$ 0
TOTAL (Precios sin IVA)	**US$ 54**

Software Open-source Smoothwall Firewall *www.smoothwall.org*
Cotización T/Red PCI GigaLan DGE-530T 10/100/1000 Mbps. en *www.pcfactory.cl*
Cabe señalar que el hardware a utilizar es uno de los 3 servidores mencionados anteriormente.
Smoothwall Firewall por ser un software open-source no tiene soporte de pago, solo el que da la comunidad de desarrolladores.

4.2.4 Cuadro económico comparativo de alternativas de solución

A continuación se muestra una tabla económica comparativa de las 3 soluciones.

Tabla 4 – 9: Cuadro económico comparativo de alternativas de solución.

Equipos / Item	**Cisco ASA 5505 SEC PLUS**	**Watchguard Firebox Edge X20e**	**Smoothwall Firewall**
Costo de Equipo	US$ 1.420	US$ 650	US$ 54 (3 NIC 1Gbps)
Servicio o Soporte (hasta 1 año)	US$ 0	US$ 0	No tiene soporte
Actualizaciones de servicios	No Contemplado	US$ 470	US$ 0
TOTAL (Sin IVA)	**US$ 1.420**	**US$ 1120**	**US$ 54**

La tabla comparativa de soluciones muestra el valor de los equipos y licencias que están incluidas en el mismo costo, pero solo hasta un año. Las soluciones propietarias están sujetas a renovación de licencia para años posteriores, además algunas aplicaciones o servicios no están incluidas en el valor base, estas son como antivirus, antispam, protección a IDS, etc. es decir, solo por requerir algunas de ellas, se cobrará una licencia asociada al servicio. El valor dependerá de la cantidad de usuarios y del tipo de servicio.

En cambio la solución open-source Smoothwall Firewall no tiene costo alguno por más aplicaciones o servicios que estén disponibles, el problema se efectúa cuando se necesite instalar algún servicio, tendrá que el mismo administrador de la red poseer conocimientos necesarios para realizarlo.
Es decir, se requiere de algún conocimiento previo de S.O Linux por parte del operador. No siendo así, si se tiene alguna solución implementada con Cisco o con Watchguard.
Las ventajas económicas de Smoothwall frente a las otras soluciones propietarias son las siguientes:

- Costo monetario $0 por el software.
- Costo monetario $0 por updates y upgrades.
- Software sin limites artificiales en cuanto a numero de usuarios y características o funcionalidades, sólo el limite impuesto por el hardware.
- Costo monetario $0 por definiciones de antivirus, IDS, antispam.

Las desventajas de las soluciones de pago frente a Smoothwall se muestran a continuación:

- Desarrolladores son empresas con trayectoria, las que ofrecen los productos y servicios lo que otorga una seguridad al implementar sus productos.
- Ofrecen soporte oficial y presentan planes de soporte 24x7x365.
- Ofrecen capacitaciones oficiales con personal preparado para tal función.

En resumen hay una balanza a la hora de elegir entre las soluciones propietarias y open-source, ya que si se requiere de una solución que la instale y configure el proveedor, que presente soporte en línea y telefónico de 24x7x365 que se cuente con los recursos para pagar licencias por servicios asociados adicionales y que en definitiva la empresa contemple todos los gastos requeridos, es una excelente solución. Pero por otra parte si se requiere de una solución que posea el costo mínimo de instalación, configuración y puesta en marcha, que el soporte lo realice el propio administrador de red, que no posea gastos futuros como actualizaciones de software, licencias, etc, y se cuente con gente capacitada para implementar soluciones open-source, Smoothwall Firewall es la solución.

4.3 ELECCIÓN DE LA SOLUCIÓN

Una de las ventajas de las soluciones propietarias como se dijo anteriormente, es que los desarrolladores son empresas consolidadas las que ofrecen los productos y servicios, lo que da cierta seguridad. Además ofrecen soporte y se puede a optar a planes de 24x7x365.

Una de las grandes desventajas en comparación con software open-source es el costo alto de equipamiento, licencias e implementación por parte de empresas como Cisco y Watchguard. Además se debe cancelar por las actualizaciones de antivirus, definiciones de patrones del IDS/IPS y estas tienen

licencias por tiempo limitado. Siendo de gran alto costo para la Empresa TELECTRICA.

Dada las especificaciones técnicas requeridas por la Empresa que se mencionaron en el capitulo anterior, como por ejemplo: soporte a mas de 25 usuarios, sistema de antivirus, antispam, protecciones IDS/IPS, bloqueo de contenido, protección a ataques externos, limitación de ancho de banda a aplicaciones, entre otras.
Las 3 soluciones cumplen con los requisititos y/o necesidades, pero Smoothwall Firewall es la que presenta mayor rendimiento y capacidad de conexiones, esto es importante dado que en un escenario donde estén puestas las soluciones propietarias como la de Cisco o de Watchguard, en una alta de demanda de tráfico, se ralentizará toda la red LAN en comparación con Smoothwall, esto se debe por la performance, que es superior aproximadamente 5 veces en comparación de las soluciones propietarias, dado que Smoothwall no se encuentra limitado por hardware. También si se ralentizase se podrá cambiar fácilmente el hardware de Smoothwall, por un superior.
Además Smoothwall trabaja en un hardware con interfaces de red (NIC) de alta capacidad, siendo velocidades de 1Gpbs.

Con respecto a las características económicas, también mencionadas en el capitulo anterior que necesita o requiere la Empresa, como por ejemplo: necesidades de adquirir equipamiento a bajo costo ya que ella presenta presupuesto limitado, solución fácil de administrar e intentar de realizar o diseñar una solución ocupando los recursos ya disponibles.
Solo una alternativa de solución cumple con todos los requerimientos, y ella es Smoothwall Firewall.

Las soluciones como Cisco y Watchguard al ser soluciones cerradas y de pago, estas se ven limitadas por el licenciamiento, esto es, número máximo de clientes simultáneos o concurrentes, tipos de módulos y/o funcionalidades habilitadas, esto dado que al ser empresas con fines de lucro, su fin ultimo es obtener el mayor provecho en las ventas. Pero a su vez, estas empresas ofrecen soporte, actualizaciones, capacitación a sus clientes, elementos que tienen un gran peso al momento de evaluar una solución, ya que para empresas con mayores presupuestos, la evaluación de una solución no siempre se basa solamente en cual es la del menor costo monetario.

Las soluciones open-source son de acceso libre, esto quiere decir que no se paga por usarlas, se puede ver el código fuente, se puede copiar, usar y modificar si así se requiriese, lo cual las convierten en una excelente alternativa a las empresas con poco presupuesto.

Las soluciones open-source tienen a la comunidad desarrolladora de aplicaciones como soporte, los cuales están constantemente mejorando las aplicaciones y desarrollado parches en caso de encontrar un problema. En el software open-source no se tienen límites del tipo cantidad de usuarios por licencia, y sólo se limita a la potencia del hardware que soporta el software instalado.

El software open-source también permite integraciones de varias soluciones en un mismo “paquete”, lo que permite tener una “caja negra” que efectúe múltiples tareas, complejas en muchos casos y todo por el mismo costo monetario por el software: $0. Si se necesita soporte se puede solicitar a una empresa (la que provee el software o una empresa dedicada a dar soporte) o a una persona que domine el tema y los costos dependerán si se elige uno u otro.

En definitiva la solución que más se acerca a los requerimientos y/o necesidades tanto en aspectos económicos como técnicos es una solución open-source, es decir, Smoothwall Firewall.

4.4 PRESUPUESTO MATERIALES Y ELEMENTOS DE RED LAN

A continuación se detalla las cotizaciones contempladas para la realización de la instalación de la red LAN en la nueva infraestructura.
Se mencionan las medidas tanto del cableado horizontal y vertical.

Cableado Horizontal 1º piso = 120 Mts.
Cableado Horizontal 2º piso = 150 Mts.
Cableado Vertical = 10 Mts. (se considera el de respaldo)

Total Cableado = 180 Mts.

La siguiente cotización contempla elementos de red, realizada en Pcfactory, *www.pcfactory.cl*.

Tabla 4 – 10: Cotización de elementos de red.

ITEM	CANTIDAD	COSTO UNIT.	COSTO TOTAL
DLink T/Red PCI GigaLan DGE-530T Giga 10/100/1000	2	$14.839	$29.678
Advantek Switch 24b ANS-2402G 19" +2Port GigaLan	2	$92.581	$185.162
Linksys Access Point WAP54G	2	$55.699	$111.398
Air802 Cable UTP cat6 Rollo 305m	1	$43.656	$43.656
UPS APC 1500 VA 865w Back RS BR1500i	3	$154.200	$462.600
TOTAL (INCLUYE IVA)			$832.494.-

A continuación cotización que contempla materiales para instalación de red, realizada en Comdiel Ltda. *www.comdiel.cl*

Tabla 4 – 11: Cotización de materiales de instalación de red.

ITEM	CANTIDAD	COSTO UNIT.	COSTO TOTAL
ORGANIZADOR HORIZONTAL 19" 1U SATRA	2	$9.800	$19.600
GABINETE DE PISO 19" - 1,50 x 0,63 x 0,81 M - SATRA	1	$239.580	$239.580
GABINETE DE PARED 19" 6U SATRA	1	$66.825	$66.825
ZAPATILLA ELÉCTRICA 6 POSICIONES	2	$19.157	$38.314
PATCH PANEL 24 PUERTOS RJ-45 CAT6 UNIVERSAL LINE	2	$44.900	$89.800
CONECTOR MODULAR MACHO RJ-45 CAT 6 MULTIFILAR	40	$90	$3.600
ORGANIZADOR VERTICAL DOBLE CON TAPA SATRA	2	$63.250	$126.500
CABLE PATCH CAT 6 INTERIOR, 4 PARES, 26 AWG, LEONI-KERPEN	100	$180	$18.000
KIT 2 VENTILADORES PARA GABINETE DE PARED SATRA	2	$15.741	$31.482
AMARRA PLÁSTICA 96MM X 2.4MM	100	$3,43	$343
CODO	30	$1.568	$47.040
PROLONGADOR	30	$770	$23.100
PLAQUETAS DE IDENTIFICACIÓN MP	80	$120	$1.600
ROSETA MODULAR MURAL RJ-45 CAT6	30	$980	$29.400
CANALETA DE PISO 75x17	80	$1.480	$118.400
SUBTOTAL			**$853.584.-**
19%IVA			**$162.181.-**
TOTAL			**$1.015.765.-**

Para dar acceso a Internet a la red LAN en la nueva infraestructura, se realizan presupuestos en distintas empresas que proveen servicios de Internet (ISP).
Las características del servicio de Internet deben ser las siguientes.

- Disponer de IP Fija, por uso del servidor de correo.
- Tener control de la configuración del Proveedor de Internet, para habilitar puertos ya sea del servicio de correo, control de *spam*, etc.
- Alta velocidad de conexión por la jerarquía de la red Lan.

Primeramente se contactó a VTR Empresas y se solicito un presupuesto con las características ya mencionadas, pero no poseen ningún servicio de IP fija, solo dinámica, tampoco dan servicio de control de puertos.

En Telefónica Empresas, para las características ya mencionadas presenta un plan que cumple esas condiciones llamado Speedy Negocios Multiusuario, que es un servicio ADSL e incluye línea telefónica.

Tabla 4 – 12: Cotización de acceso de Internet banda ancha.

Velocidad	Renta Mensual	Cantidad Pc
2 Mega	UF 1,55	Hasta 10 a 15
4 Mega	UF 1,80	Hasta 15 a 20
6 Mega	UF 2,00	Hasta 20 a 30

Luego se realiza un presupuesto en Grupo GTD Internet S.A.
Ellos presentan un plan ADSL Multiusuario de 2 Mbps, para la solicitud requerida, a 5 UF Mensuales.

La necesidad de la empresa es requerir un plan que cumpla todas las características ya mencionadas, y que sea al menor costo. El único plan que reúne estos requisitos es el de Telefónica Empresas.

Este ISP recomienda una cantidad de PCs para cada plan, como la red LAN está contemplada a 22 puntos de red, se recomienda el plan de 6 Mbps.

CAPITULO 5: DISEÑO Y CONFIGURACIÓN DE LA RED LAN

5.1 INTRODUCCIÓN

En el siguiente capítulo, se dará a conocer el diseño de la red de área local más la configuración de los distintos servidores. Primeramente el que estará al frente de la red; servidor firewall *(*UTM*),* luego el servidor de correo y finalmente el servidor de archivos.

5.2 DISEÑO DE LA RED DE ÁREA LOCAL

Efectuado los requerimientos de red y seguridad se establece el nuevo diseño de la red local.

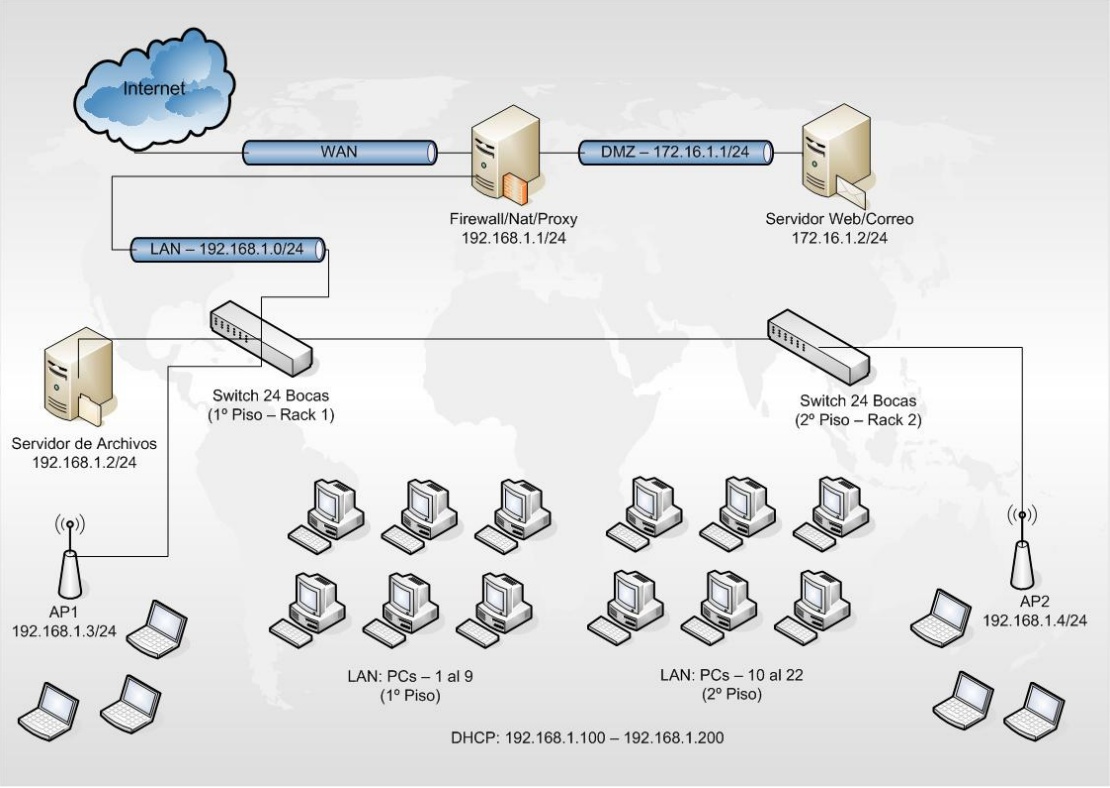


Figura 5 – 1: Diseño de la red de área local.

Se establecerá una zona DMZ, Demilitarized Zone (zona desmilitarizada), que se ubica entre la red interna y la red externa de la Empresa.

El objetivo de una DMZ, es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ's puedan dar servicios a la red externa, a la vez protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un "callejón" sin salida.

El diseño de la política del firewall será del siguiente modo:

Tabla 5 – 1: Política del Firewall.

	Internet	DMZ	Interna
Internet (eth0)		**ws: http** **ws: https** **ms: smtp**	**NO PERMITDO**
DMZ (eth1) **172.16.1.1/24**	**- dns** **-smtp**		**NO PERMITIDO**
Interna (eth2) **192.168.1.1/24**	**-http** **-https**	**ms: smtp** **ms: dns** **ms: pop3** **ms: pop3s** **Ws: http**	

En la tabla 5 – 1, se define la política del firewall como “denegar todo con excepciones”, solo permitiendo lo establecido, es decir, solo se dejara los puertos de los servicios principales que se ocuparán.

WS corresponde a las siglas de Web Server y MS, corresponden a las siglas de Mail Server.

La configuración de las direcciones IPs quedará del siguiente modo, la red interna usa el rango de IP privado 192.168.1.X, otorgando IP a los usuarios internos mediante un servicio DHCP desde el rango 192.168.1.100 a 192.168.1.200. Esta tarea la efectuará el servidor firewall, es decir, Smoothwall Firewall.

El rango 192.168.1.1 a 192.168.1.10 es un rango reservado para servidores y en este rango se instalará el firewall, el servidor de correo, servidor web y los Access Points Inalámbricos, quedando de la siguiente manera:

Tabla 5 – 2: Configuración de direcciones IP.

Servidor / Elemento de red	**Dirección IP/Mascara de subred**
Servidor Smoothwall Firewall	192.168.1.1/24
Servidor (correo, Web)	192.168.1.2/24
Access Point Inalámbrico 1° Piso	192.168.1.3/24
Access Point Inalámbrico 2° Piso	192.168.1.4/24

El firewall al constar de tres zonas, necesita usar una IP por zona. Para la zona externa se utiliza una IP fija que la otorgará el ISP, para la zona DMZ será 172.16.1.1/24 y para la zona interna 192.168.1.1/24.

5.3 CONFIGURACIÓN DEL 1° SERVIDOR (FIREWALL/PROXY/DHCP)

5.3.1 Primera Parte: Instalación de Smoothwall Firewall

La instalación de Smoothwall Firewall consta de 2 partes, la primera que es en modo texto define el idioma, dirección IP de las zonas; GREEN (red interna), ORANGE (DMZ), RED (acceso a Internet) y la instalación básica del firewall. La segunda parte que es en modo gráfico, se accede a ella mediante un Web *Browser* donde se configura el resto de las preferencias y reglas.

Al ingresar el cd al servidor, se llegará a la siguiente imagen (ver figura 5 – 2), en cual se elige el modo de instalación. Para la normal instalación se presiona *enter.* En la figura 5 – 3, se hace advertencia de que si se continúa con la instalación, los datos contenidos en el disco duro, serán destruidos. Como se está seguro que el disco duro esta vacío y es especialmente utilizado para la instalación de Smoothwall Firewall, se procede seleccionando Ok.

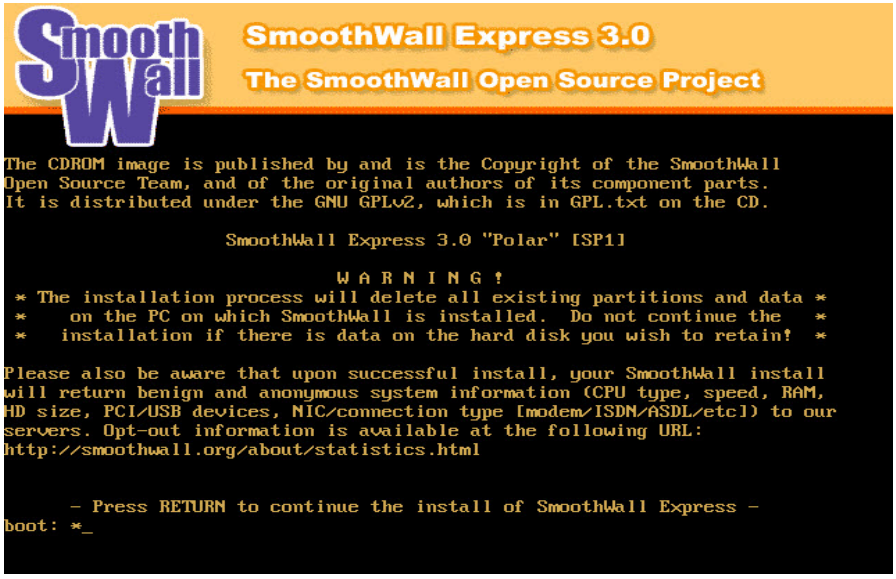


Figura 5 – 2: Pantalla de inicio de Smoothwall Firewall

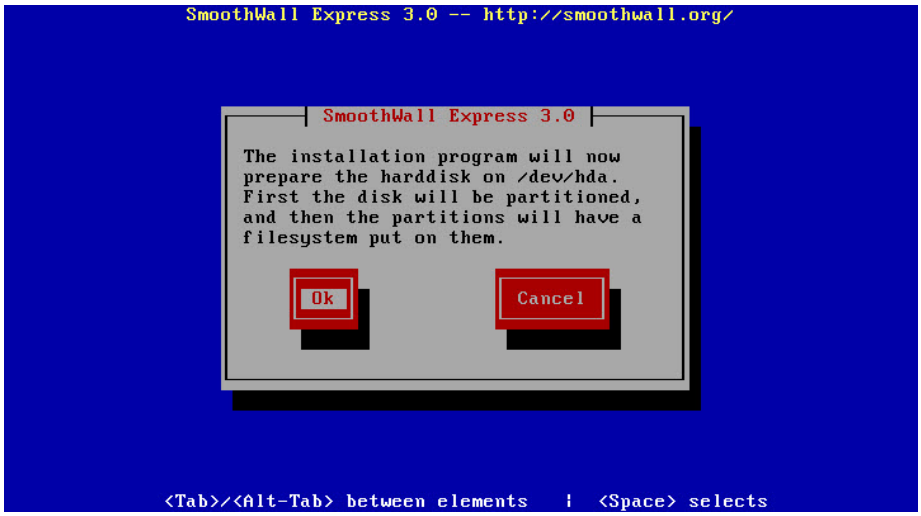


Figura 5 – 3: Advertencia de instalación (partición de disco).

Luego preguntará si se posee un archivo de backup (figura 5 – 4) para poder ser restaurado el sistema firewall, conservando los valores de configuración que se tenían previos, si es una nueva instalación se niega esta opción.

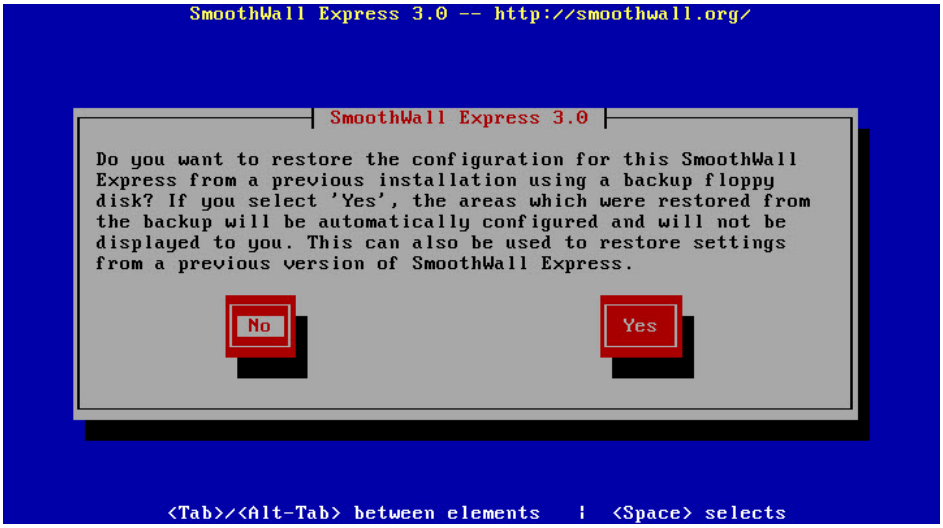


Figura 5 – 4: Advertencia de restauración de Smoothwall Firewall.

Después de instalado Smoothwall Firewall, se procede a elegir la configuración de la red. Se elegirá la configuración RED + GREEN + ORANGE, por las características de la red a configurar.

Cuando se indique configurar las interfaces de red, Smoothwall Firewall las identifica como Interface Roja (RED), la que será conectada al ISP (Proveedor de servicios de Internet), Interface Verde (GREEN), la que será conectada a la red interna e Interface Naranja (ORANGE), la zona DMZ.

En la configuración de la interface verde (GREEN) (figura 5 – 5), se asigna la dirección IP y mascara de red.

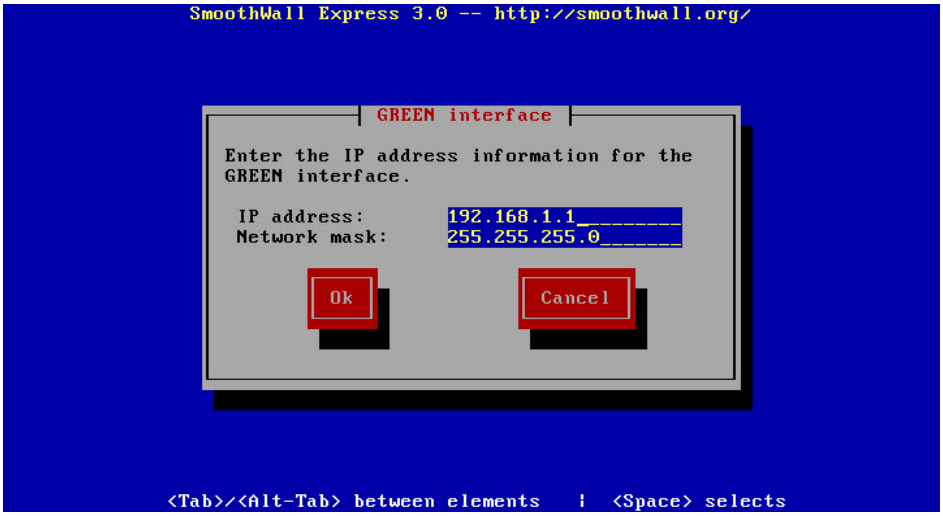


Figura 5 – 5: Configuración de interface de red LAN *(Green).*

En la configuración de la interface roja (RED), permite conexión de tipo estática, dinámica, PPPoE, MODEM Analógico, etc. Dependiendo de la conexión a elegir se tendrá que configurar las opciones referente a la elección.

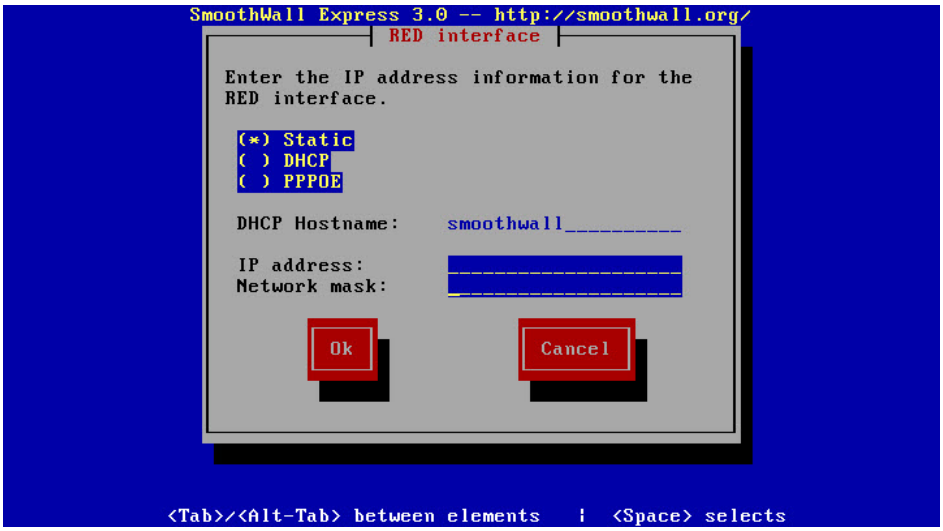


Figura 5 – 6: Configuración de interface WAN *(Red).*

En la configuración de la interface naranja (ORANGE) (figura 5 - 7), se asigna la dirección IP, máscara de red de la zona DMZ, que estarán los servicios de correo, DNS y Web.

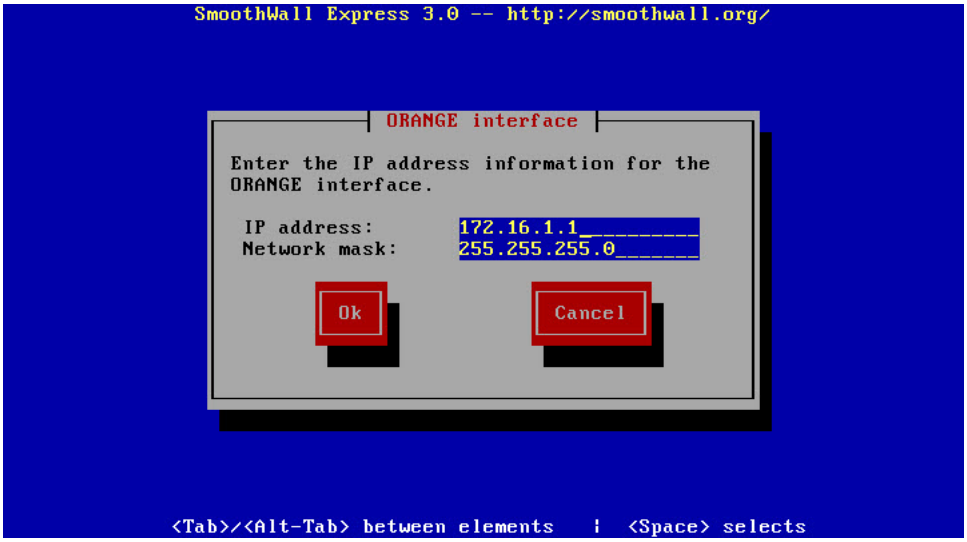


Figura 5 – 7: Configuración de interface de zona DMZ *(Orange).*

Después de la determinación de las interfaces de red, se configura el servidor DHCP.

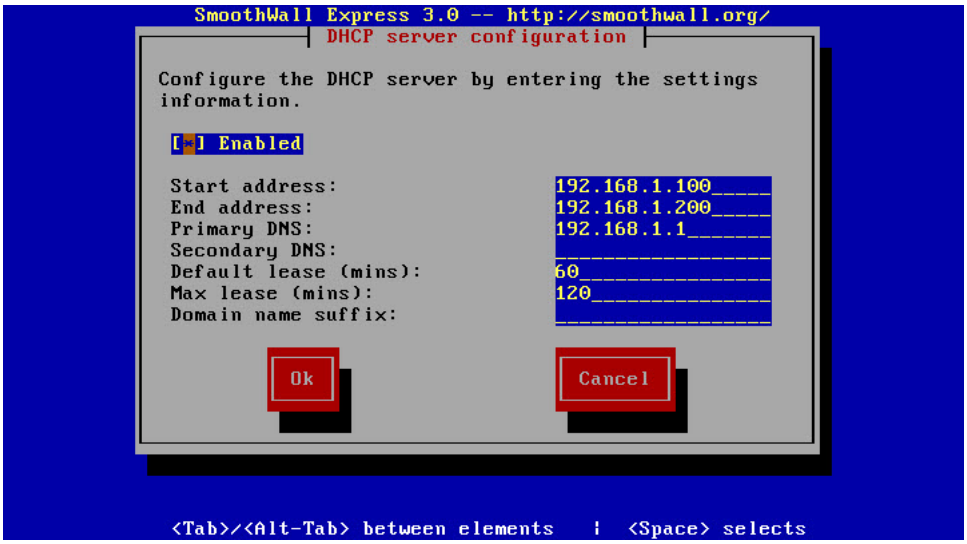


Figura 5 – 8: Configuración de servicio DHCP.

Una vez que se realiza la configuración, se presiona OK, y se da por terminado la instalación de Smoothwall Firewall. Se reinicia el servidor y se espera a que se complete la carga de servicios.

Al final de la carga se puede acceder al menú *shell*, con opción de restaurar los valores por defecto, como reiniciar el servidor por alguna razón o motivo, o simplemente manejar el entorno como cualquier distribución LINUX.

5.3.2 Segunda Parte: Configuración de Smoothwall Firewall

Para la configuración de Smoothwall Firewall es necesario utilizar un Web *Browser* desde algún PC de la red interna. Para entrar a la consola Web se debe ingresar mediante la dirección IP del servidor, que es la que se configuró, es decir, *https://192.168.1.1:441*, la que luego automáticamente se redireccionará a una pagina segura https.

En esta página aparecerá una alerta de certificado digital SSL, es normal ya que se esta usando un certificado autofirmado y este al no ser emitido por una entidad certificadora, el navegador muestra una advertencia.

En la figura 5 – 9 se muestra la pantalla de bienvenida al proceso de configuración.

Figura 5 – 9: Pantalla de bienvenida de Smoothwall Firewall.

Ahora se entrará a configurar los servicios que ofrece Smoothwall Firewall además de las opciones de antivirus, Traffic shaping, filtro *spam*, IDS, monitoreo de trafico, reglas de salida hacia Internet desde la red interna y *proxy* transparente para trafico HTTP, POP3, FTP, SMTP, entre otros.

5.3.2.1 Configuración de *traffic shaping*

Con respecto a la configuración de traffic shaping o priorización de trafico, se priorizó el tráfico en los protocolos STMP, POP3 e IMAP, ya que el sistema de

correo debe ser enviado y entregado oportunamente frente a navegación por la Web y Multimedia.

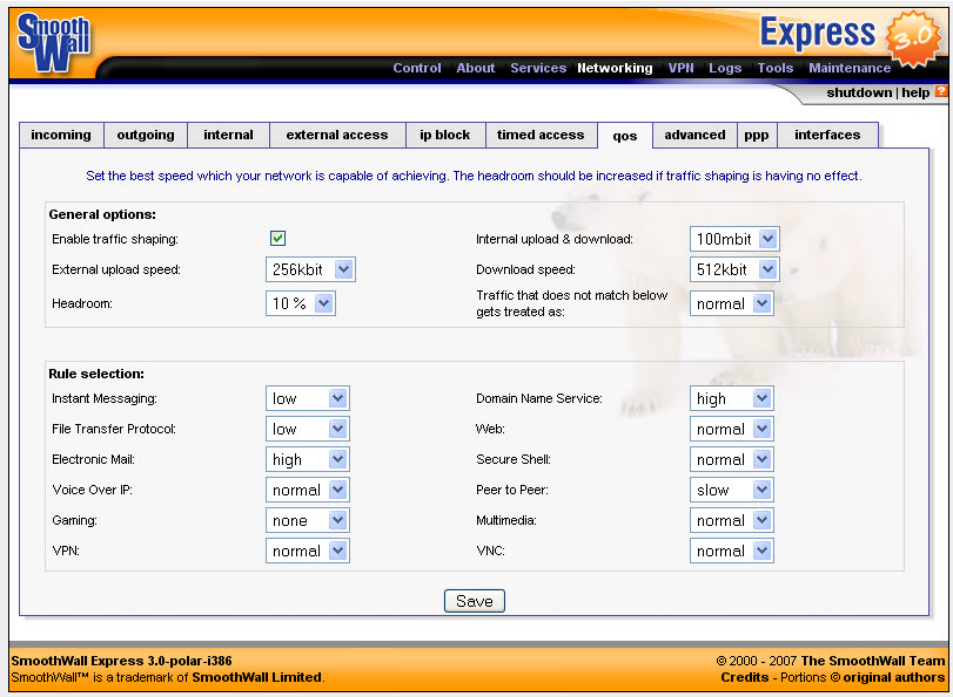


Figura 5 – 10: Configuración de *traffic shaping*.

5.3.2.2 Configuración del firewall

En la configuración del firewall de Smoothwall Firewall como se puede apreciar en la figura 5 – 11, se bloquea todo el trafico con excepciones que se detallan a continuación. Cabe destacar que aquí se pueden denegar servicios que utilicen algún puerto sea este TCP o UDP, como por ej. Programas Peer to Peer.

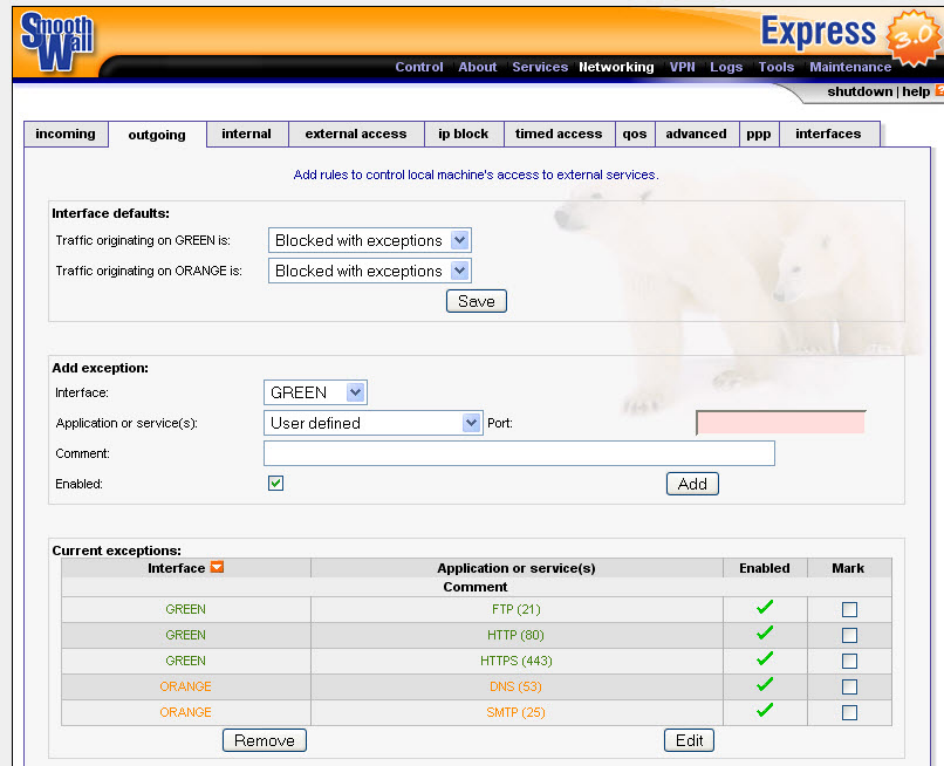


Figura 5 – 11: Configuración del firewall.

5.3.2.3 Firewall de Inter-Zona

En la figura 5 – 12, se muestra la configuración del tráfico de Inter-Zona, siendo la zona DMZ; 172.16.1.1. Como se puede apreciar, la política de esta configuración es que la zona DMZ no tenga acceso a la red interna, pero si viceversa.

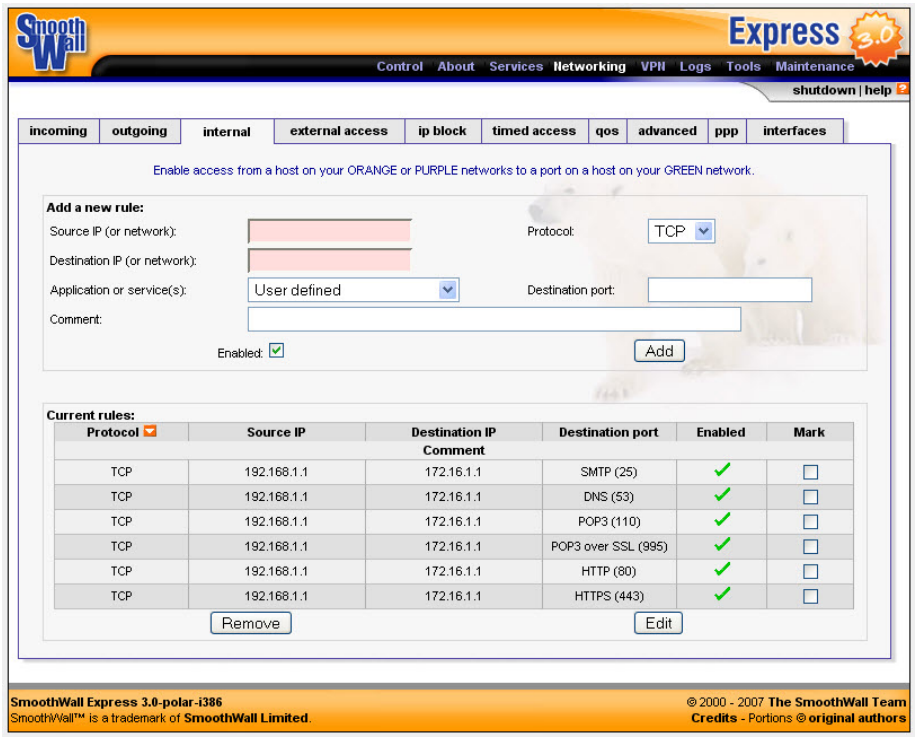


Figura 5 – 12: Configuración del tráfico de Inter-Zona.

5.3.2.4 Configuración de Proxy

Referente a la configuración del servidor *proxy*, se activó en modo transparente, los logs para informes de errores, espacio en memoria y caché en disco duro para las paginas Web visitadas y así poder ser entregadas lo mas rápido posible al usuario, de esta manera se ahorra ancho de banda usado.

A la zona DMZ no se habilita el *proxy*, por razones de no presentar problemas de configuración con el servidor de correo.

Una característica de restricción al ancho de banda utilizado del *proxy,* es que se puede configurar el límite de transferencia que un usuario puede alcanzar en un día, ya sea, en subida o bajada de datos. Luego de este límite se negará la conexión.

Además de la activación del antivirus para correos, navegación Web, transferencias de archivos vía FTP, se restringió las páginas con contenido explícito y no apropiado para el ambiente de trabajo, como páginas con contenido pornográfico, sitios Web de entretención, etc.

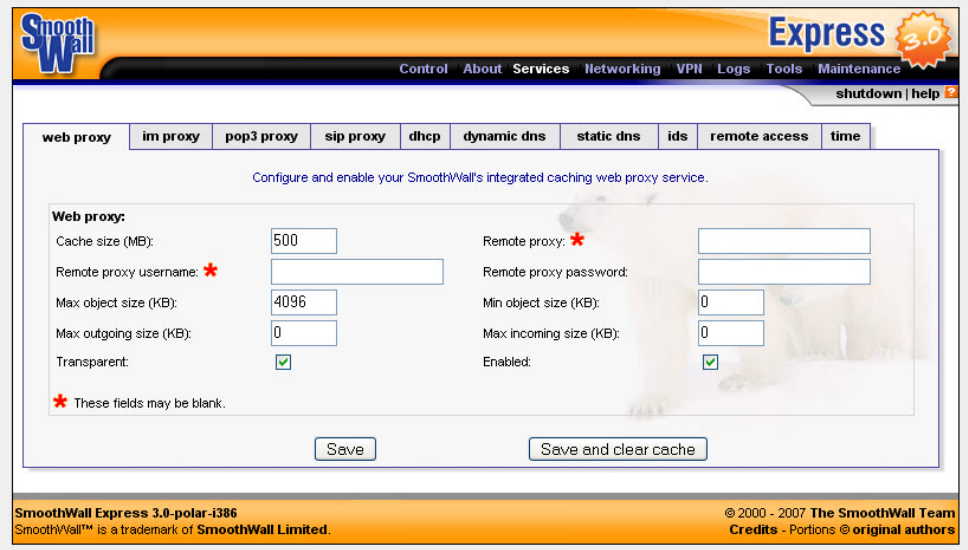


Figura 5 – 13: Configuración del servidor *proxy*.

5.3.2.5 Configuración de IDS (sistema de detector de intrusos)

En la configuración del detector de intrusos o IDS, se activa la opción a modo *enable.*

Al igual que un antivirus, el IDS trabaja en función de definiciones o reglas, por lo que es importante tener las últimas actualizaciones instaladas. Esto se puede hacer mediante una suscripción al sitio de SNORT [7], en el se obtiene las reglas certificadas "Sourcefire VRT" (previo registro en el sitio de SNORT) para obtener el oink code y este pueda ser ingresado dentro de Smoothwall Firewall.

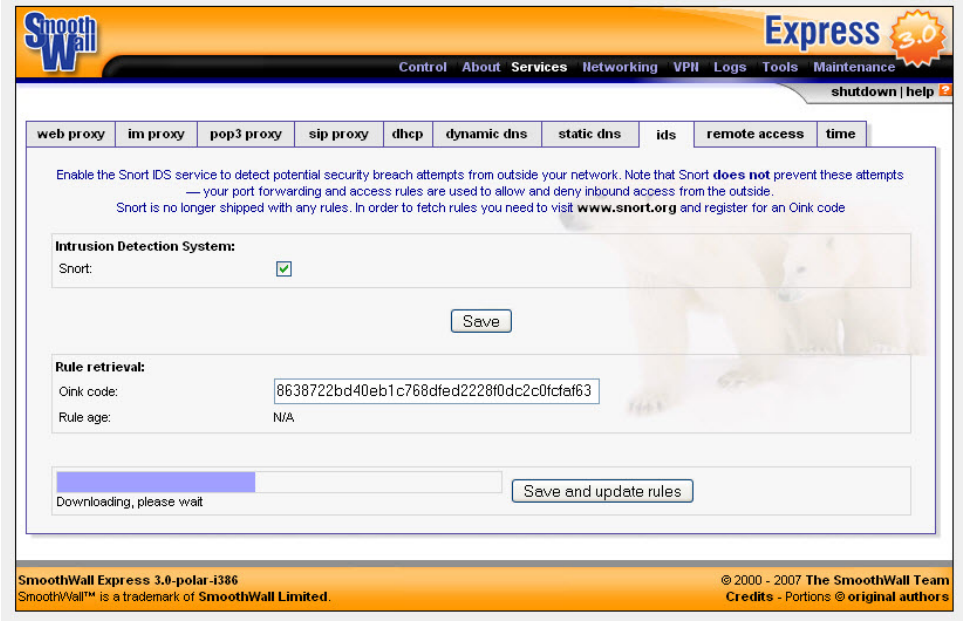


Figura 5 – 14: Configuración de IDS.

5.4 ALTERNATIVAS DE SOLUCIÓN DE CORREO PARA EL 2° SERVIDOR (CORREO/WEB).

Para elegir la solución de correo se realizará una pequeña comparativa entre aplicaciones solo open-source, ya que por las necesidades y requerimientos de la empresa de poseer un presupuesto limitado.
Es por esto que una opción como Microsoft Exchange queda descartada por su alto costo de licencia, actualización, etc.

Las tres soluciones más importantes que se tienen en el modelo open-source son:

- Zimbra Collaboration Suite.
- Open-Xchange.
- Scalix.

Para realizar la comparativa, se ha tenido en cuenta 3 factores:

- Características del conector para Microsoft Outlook.
- Conectores para clientes de correo (Thunderbird, Novell Evolution, Kontact).
- Sistemas operativos soportados.

Es difícil comparar en cierto modo el modo de instalación de las aplicaciones, el diseño ya que son muy similares.
Las 3 soluciones son para uso profesional.
Además las 3 soluciones son de un único instalador que integra todos los servicios y/o softwares en una única suite de aplicación. Están diseñados sobre una arquitectura modular usando tecnologías de código abierto. Incluyen soporte para multitud de protocolos estándares que le permiten interactuar con los clientes de software.

Para poder definir que solución de correo elegir, se debe identificar en primer lugar las necesidades, tanto en funcionalidad como en capacidad de integración en el entorno actual. La Empresa actualmente no posee ningún servidor de correo interno. Pero para remediarlo ocupan Gmail como correo electrónico, usando el dominio de Gmail.
Estas cuentas están configuradas a Microsoft Outlook. Debido a esto, están muy familiarizados con este cliente de correo.
Es por ello, que uno de los puntos principales a comparar será la integración y compatibilidad que tiene con Microsoft Outlook.

5.4.1 Zimbra Collaboration Suite

Zimbra es una solución completa de correo electrónico corporativo y colaboración con Antivirus y Antispam, que se integra con Microsoft Outlook 2003/2007 , iSync de Mac y Novell Evolution.

Zimbra fue adquirida en el año 2007 por Yahoo. Hoy en día, puede considerarse el servicio de correo electrónico profesional para empresa de Yahoo.

Además de emplear los típicos módulos de calendario, contactos y tareas, Zimbra aporta módulos nuevos para almacenar documentos, “chatear” con compañeros de oficina o crear contenido dentro de un Bloc de Notas.

Es posible, desarrollar los llamados “Zimlets”[4] para expandir el potencial de la solución integrándolo con sistemas de telefonía IP.

La integración con móviles tipo BlackBerry, iPhone, Windows Mobile, etc. se puede realizar con Zimbra Mobile.

Con Zimbra, es posible realizar una migración desde un entorno IMAP4, Microsoft Exchange, Lotus y también ficheros “*.pst”[5] de Microsoft Outlook.´

El producto, está compuesto por un conjunto de servicios Linux (Openldap[6], Mysql[7] (, Postfix (MTU, Mail Transfer Unit)) integrados entre sí, para hacer una solución muy robusta y probada.

[4] Un Zimlet es una miniapliación que se ejecuta sobre la Interfaz de Zimbra y permite acceder a información disponible en otros sistemas a través de tecnologías web services

[5] Los archivos PST de Outlook contienen los correos electrónicos de una cuenta de usuario específica.

[6] *OpenLDAP* es una implementación open source y gratuita del protocolo LDAP.

[7] MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario.

5.4.2 Open-Xchange

Open-Xchange es una solución robusta que se integra con Microsoft Outlook, iSync de Mac, mediante un conector que debe ser instalado en el PC del usuario.

Además de los módulos típicos como Calendarios, Tareas y Contactos, Open-Xchange nos aporta un repositorio de documentos, que nos permite utilizarlo además como bloc de notas o almacén de favoritos. Cabe destacar la opción para importar contactos de Facebook y Linked In directamente en una carpeta de contactos.

Como valor añadido, se pueden desarrollar módulos (en Java) para expandir el potencial de la solución integrándolo con sistemas de telefonía VoIP, agregando nuevas funcionalidades sin necesidad de modificar el núcleo.

Se puede migrar un Microsoft Exchange, hacia un servidor Open-Xchange. También es posible migrar buzones IMAP4 y la información de calendarios, contactos, tareas de nuestro Microsoft Outlook / iSync de Mac.

Open-Xchange, se compone de un conjunto servicios que podemos añadir a una infraestructura de correo ya consolidada (Servidores SMTP/IMAP, Bases de datos de usuarios Openldap), aportándonos toda un área funcional de colaboración.

5.4.3 Scalix

Scalix, es una solución robusta de correo electrónico y colaboración que se integra con Microsoft Outlook 2003 / 2007 y Novell Evolution, mediante un conector que debe ser instalado en el PC del usuario.

Scalix está heredado de una tecnología muy probada que inicialmente empezó a desarrollar Hewlett Packard.

El producto, está diseñado para sustituir entornos Microsoft Exchange y no aporta ninguna funcionalidad extra, ciñéndose sólo a los módulos de calendarios, contactos y carpetas de correo compartidas. En lo que a la integración con dispositivos móviles se refiere, actualmente no tiene desarrollado ningún sistema de sincronización sin cables, aunque siempre se pueden ir a soluciones de terceros como Notify Link[8].

Es posible realizar una migración completa desde entornos Exchange, manteniendo ambos en producción (Co-existencia). También se puede emplear la migración de ficheros "*.pst" de Microsoft Outlook o mediante IMAP4

El sistema está compuesto por un conjunto de aplicaciones para Linux, unas como Sendmail o PostgreSQL[9] y otras basadas en un sistema heredado de HP.

5.4.4 Cuadros comparativos de alternativas de solución de correo

A continuación se presentan cuadros comparativos de las 3 soluciones, que definirán la elección. Como se mencionó anteriormente, se compararán características de servicio para definir elección, ya que son soluciones muy similares entre si.

Tabla 5 – 3: Conectores soportados, para clientes de correo electrónico.

Conectores para clientes	**ZIMBRA**	**OPEN-XCHANGE**	**SCALIX**
Outlook	Completa	Sólo PIM[10]	Completa

[8] NotifyLink permite a los usuarios la sincronización inalámbrica de las características de sistemas de colaboración de correo electrónico. ofrece a los clientes un conjunto de características de sincronización inalámbrica para agendas de eventos, programar reuniones, aceptar o rechazar las solicitudes de reuniones.

[9] PostgreSQL es un sistema de gestión de base de datos relacional orientada a objetos de software libre, publicado bajo la licencia BSD.

[10] El PIM (Personal information management) se basa en la información de contactos y la agenda.

2003 / 2007			
iSync Mac	Completa	Completa	No disponible
Thunderbird	IMAP	IMAP	IMAP
KDE Kontact / Kmail	Sólo IMAP	Completa	Sólo IMAP

Tabla 5 – 4: Características del conector Microsoft Outlook.

	ZIMBRA	**OPEN-XCHANGE**	**SCALIX**
Sincronización Correo	Nativo	IMAP	Nativo
Sincronización PIM	Nativo	Nativo	Nativo
Modo Offline / Online	SI	SI	SI
Abrir buzón de otro usuario	SI	IMAP	SI
Autoinstalable	SI	SI	SI
Autenticación	User-pass	User-pass	User-pass

Tabla 5 – 5: Sistemas operativos soportados.

	ZIMBRA	OPEN-XCHANGE	SCALIX
RED HAT	SI	SI	SI
SUSE NOVEL	SI	SI	SI
DEBIAN	NO	SI	NO
UBUNTU	SI	NO	NO

Difícil la elección de una solución de manera absoluta. Todas estas soluciones open-source están diseñadas para un uso profesional.

Entre los puntos que pueden marcar la diferencia es el apoyo de un grueso de clientes como Outlook, si sus usuarios no quieren gastar más y si la usan a veces en “offline”. Se tiene que poseer un plugin o un protocolo IMAP apoyo fiable.

Como se visualizó que la integración del cliente de correo Microsoft Outlook con Zimbra es de forma innata y presenta un completo soporte, se recomienda elegir esta solución como cliente de correo.

OpenX-change presenta solamente una interactuación con Microsoft Outlook de información de contactos y agenda, y Scalix también es compatible con Outlook pero no con sistemas Macintosh, precisamente, iSync de Mac, para no presentar problemas de compatibilidad con Microsoft Outlook.

La aplicación de servidor de correo recomendada utilizar es Zimbra Collaboration Suite (ZCS), que es una suite de mensajería y colaboración de código abierto. Algunas características más detalladas se muestran a continuación:

- Flexibilidad: fácil personalización según las necesidades de la organización.
- Libertad: uso de cualquier navegador Web y de aplicaciones de escritorio tradicionales.

- Durabilidad: servidor de correo electrónico y calendario extraordinariamente fiable y ampliable.
- Baja dificultad de mantenimiento: gestión muy sencilla, tanto mediante una interfaz gráfica como desde la consola.
- Se ofrece bajo la licencia Yahoo! PublicLicense (YPL), versión 1.1, en forma de una versión de código abierto, sin coste de licencias alguno.
- Está disponible para diversas plataformas y distribuciones de Linux y para MacOS X.

A continuación se describirá la arquitectura de Zimbra Collaboration Suite.

5.4.5 Componentes de la arquitectura de Zimbra Suite

Zimbra Collaboration Suite [13] está formada por un conjunto de componentes que trabajan juntos para formar una solución completa. El núcleo del servidor está escrito en Java, utilizándose Jetty[11] como servidor de aplicaciones. El servidor se integra con otros sistemas como el MTA (Mail Transfer Agent), la base de datos y los paquetes de seguridad.
El agente de transferencia de correos (MTA), enruta los mensajes de correo al servidor de Zimbra.
Este servicio está integrado a través de Postfix, Zimbra incorpora varios filtros de seguridad, como antivirus y antispam, entre otros.

Asimismo, el MTA puede integrarse con otras tecnologías, como Spamhaus, u otras soluciones de seguridad comerciales. Asimismo, soporta por defecto los protocolos principales de cifrado de canal, SSL (Secure Sockets Layer*)* y TLS (Transport Layer Security)

[11] Servidor HTTP y contenedor de Servlets escrito en Java. Jetty se publica como un proyecto de software libre bajo la licencia Apache 2.0.

La arquitectura del sistema está formada por los siguientes componentes:

Zimbra Server

Zimbra Server es el núcleo de Zimbra Collaboration Suite. Está diseñado sobre una arquitectura estable y modular usando tecnologías de código abierto contrastadas.
El servidor de Zimbra empaqueta todos los componentes principales en un instalador y utiliza, entre otras, tecnologías como Linux, Jetty, Postfix, MySQL y OpenLDAP.
Zimbra soporta múltiples dominios y también perfiles de usuarios, que denomina COS (Class Of Service). En estas clases de servicio se pueden definir las cuotas de almacenamiento y las características a las cuales tendrán acceso los usuarios. La siguiente lista presenta las más destacadas en su versión actual:

- Correo electrónico.
- Libreta de direcciones.
- Calendario de citas.
- Mensajería instantánea.
- Redacción de correos en formato HTML.
- Acceso externo por IMAP4/POP3.
- Creación de una dirección de reenvío automático del correo.
- Creación de una respuesta automática a la recepción de correos.
- Filtros de correo.

Zimbra MTA

El servidor de correo electrónico de Zimbra está formado, de diversas partes:

- Un MTA
- Un almacén de buzones de correo accesible por IMAP4 y POP3, con soporte para cifrado del canal mediante (SSL).
- Unos filtros de contenidos (antivirus y antispam).

Zimbra utiliza Amavis como filtro de contenidos y SpamAssassin y ClamAV como filtros antispam y antivirus, respectivamente. También, es posible configurarlo para que utilice cualquier otro filtro antispam.
El correo se recibe mediante SMTP, se enruta mediante una tabla de transportes y se entrega al almacén de correo haciendo uso del protocolo LMTP (Local Mail Transfer Protocol, Protocolo de transporte local de correo).

Zimbra Store

Zimbra Store, utilizando Jetty como contenedor de servlets, almacena el correo electrónico. Cada cuenta se configura en un servidor, y esta cuenta está asociada con un buzón de correo que contiene todos los mensajes y ficheros adjuntos. El servidor de buzones está formado por:

- El almacén de datos.
- El almacén de mensajes.
- El almacén de índices.
- Las utilidades de conversión de adjuntos a HTML.

Zimbra tiene su propio almacén de datos, almacén de mensajes y almacén de índices para los buzones de ese servidor. En cuanto llega un correo, el servidor de Zimbra crea un nuevo proceso para indexar el mensaje.

El almacén de datos es una base de datos MySQL, en la cual los identificadores de mensajes son enlazados con las cuentas de usuario. El almacén de datos relaciona el identificador del buzón con la cuenta de usuario a la que pertenece en el directorio LDAP. Esta base de datos contiene el conjunto de etiquetas definido por el usuario, las carpetas, las citas del calendario y los contactos de los usuarios, así como el estado de cada mensaje de correo (leídos, no leídos, etiquetas asociadas a cada mensaje y la carpeta en la cual reside el mensaje).
El almacén de mensajes guarda todos los mensajes y sus adjuntos en formato MIME[12] (Multipart Internet Mail Extension). Los mensajes enviados a múltiples destinatarios dentro del mismo servidor sólo son almacenados una vez.
La tecnología necesaria para indexar y buscar la proporciona Lucene.

Zimbra LDAP

Dada la gran diversidad de servicios y aplicaciones que suele disponerse hoy en día, es necesario disponer de un directorio de usuarios basado en LDAP.

Zimbra Collaboration Suite utiliza por defecto OpenLDAP para almacenar y gestionar el almacén de usuarios, integrando de serie el soporte para la replicación. Además, permite fácilmente su configuración para el uso de directorios LDAP externos, incluyendo Active Directory de Microsoft.

[12] MIME (Multipurpose Internet Mail Extensions), (Extensiones de Correo de Internet Multipropósito), son una serie de convenciones o especificaciones dirigidas a que se puedan intercambiar a través de Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario

El esquema LDAP de Zimbra está disponible por si se desea utilizar en una instalación LDAP ya existente, facilitando de esta manera la gestión centralizada de las cuentas de usuario de nuestra instalación. Cada cuenta tiene un identificador único de buzón de correo, que representa el punto principal de identificación en todo el sistema.

Zimbra SNMP y Zimbra Logger

La instalación de ambos paquetes es opcional. En cada servidor donde esté instalado, Zimbra SNMP (Simple Network Management Protocol), recoge información periódica del estado del sistema.

Por su parte, Zimbra Logger instala herramientas de agregación de logs, informes y seguimiento de mensajes. Sin este paquete no se podrán utilizar las funcionalidades de seguimiento de mensajes y estadísticas del servidor de la consola gráfica de administración.
La publicación y compartición de contenidos es homogénea en todo el sistema tanto para contactos, como para el calendario o los documentos. Esta compartición puede realizarse con usuarios internos y externos del sistema. El cliente de correo permite la gestión de varias identidades y de varias cuentas de correo, incluyendo la agregación de cuentas externas mediante POP3.

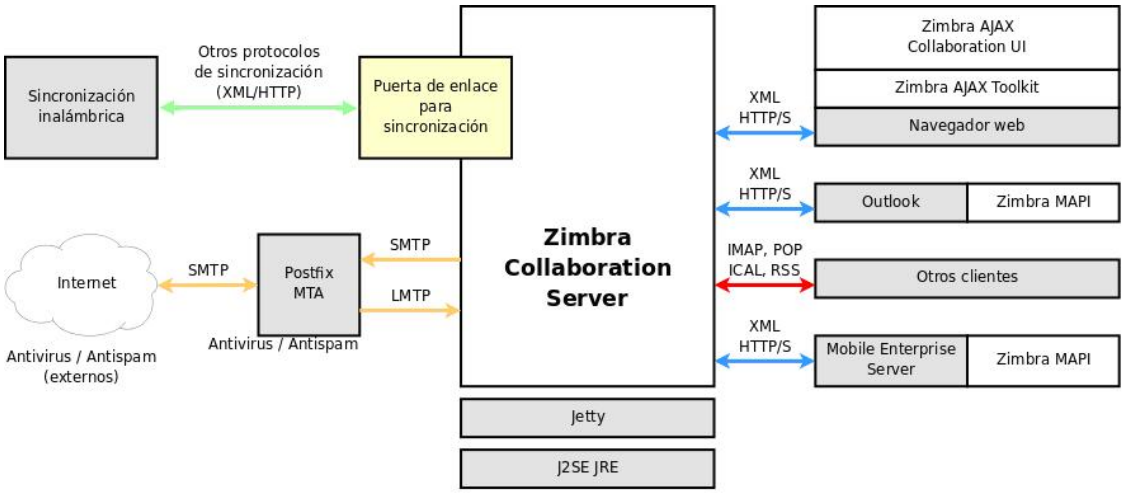


Figura 5 – 15: Diagrama de funcionamiento de software Zimbra Suite.

Zimbra permite personalizar el entorno, incluyendo soporte para temas y una versión sólo HTML para aquellos PCs antiguos o entornos que no puedan hacer uso de Javascript. Además permite la personalización de logos, textos y mensajes.

5.4.6 Requerimientos, instalación y configuración de Zimbra

Los requerimientos de Zimbra Collaboration Suite son, en comparación con otros productos similares, bastante bajos. Para entornos de hasta 50 cuentas la siguiente configuración debería ser suficiente:

- CPU Intel/AMD de 32bits a 1.5 GHz o superior.
- 1 GB de RAM.
- 5 GB de espacio libre en disco para el software y los logs
- Espacio adicional para el almacenamiento del correo y las bases de datos (depende del número de cuentas y de la cuota de disco asignada a cada una).

Para instalaciones de más de 2000 cuentas de usuario, se recomienda CPU de 64 bits, lo que lleva a la necesidad de duplicar la RAM (mínimo 4 GB). El uso de discos SCSI es siempre recomendado frente a SATA por su fiabilidad y rendimiento. En general, y Zimbra no es una excepción, a mayor cantidad de RAM, mayor rendimiento general debido a la caché del kernel, y mayor fiabilidad.

Por supuesto, todos estos valores son orientativos y únicamente útiles en un caso estándar. Es muy posible que sea preciso aumentarlos en función de los picos de carga que se prevean (por ejemplo si un cierto número, muy elevado, de usuarios acceden a la misma hora a comprobar el correo).

Para ver una serie de utilidades que son de frecuente uso, ver ANEXO 3.

Para comenzar a instalar Zimbra Edition, se procede a elegir una distribución de Linux, esta será Ubuntu Server.

En el proceso de instalación para que el servidor trabaje adecuadamente se debe elegir los paquetes que se usaran solamente y así no se sobrecargará el sistema, para ello, se elegirá:

- OpenSSH[13] Server, para controlar el servidor a distancia.
- DNS Server, para configurar Zimbra para tener la resolución del dominio.

Para que el servidor de correo Zimbra, funcione correctamente, se debe configurar el servidor DNS a nivel local. Este es un requisito a la hora de instalar Zimbra Edition, ya que cuando se esté en la instalación misma, se pedirá resolver el dominio.

Cabe decir que si se quiere tener un servidor de correo a nivel externo, es decir, no solo local, sino que se reciban mails desde Internet, se debe decir al

[13] SSH (Secure SHell,: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

proveedor de servicios (ISP) contratado, que configuren los registros DNS inversos (reverse DNS o rDNS). El tema de la autenticación, se puede ver en el ANEXO 2. Para conocer como se encuentra el estado de resolución para el dominio configurado, en este caso “telectrica.cl”, hay diferentes páginas Web que hacen un test al dominio, como por ej. *http://www.intodns.com/*, *http://www.mxtoolbox.com/*.

Un punto importante no mencionado es que para tener un servidor de correo, se debe tener una IP pública fija, ya que si es dinámica se debe tener en cuenta que esta va ir cambiando en Internet, y no va ser ubicada por el dominio correspondiente. Si ya se tiene una IP pública fija, dada por el ISP contratado, debe ser revisada para que no se encuentre en la lista de SPAMs, para ello, se debe consultar a la siguiente dirección: *http://www.spamhaus.org*, esta pagina Web es un proyecto de Steve Linford comenzado en 1998, para evitar el *spam* en los servidores y correos de Internet. Cada servidor de correo consulta esta lista, al recibir un correo desde Internet, el correo que se encuentre en ella, será bloqueado y mandado devuelta al servidor que envió dicho correo, con una notificación que no pudo ser entregado.

Figura 5 – 16: Sitio Web Spamhaus Proyect.

Para conocer la instalación y configuración de Zimbra collaboration suite 5.0 open-source en Ubuntu Linux Server 64 Bits. (Ver ANEXO 1)

Una vez ya instalado, se entrará a la configuración de administrador de Zimbra.

Para esto se debe ingresar a la siguiente *URL: https://mail.telectrica.cl:7071*

Aquí se ingresa con usuario: admin y la contraseña que se seleccionó anteriormente.

En la consola de administración se puede ver todas las herramientas con las que trabaja, como por ejemplo:

- Crear usuarios, alias, listas de distribución, recursos.
- Poder configurar servicios, dominios, servidores, zimlets, extensiones administrativas.
- Monitorear estados de los servicios, estadísticas de los servidores.
- Ofrece herramientas tales como colas de correo, certificado entre otros.

En la figura 5 – 17, se ven cargados los procesos que conllevan al funcionamiento general de Zimbra Edition.

Para crear un usuario, por ejemplo, francisco.rau@telectrica.cl; se debe ir a la siguiente pestaña, menú direcciones, cuentas, con esto se abrirá la siguiente pantalla (ver figura 5 – 18):

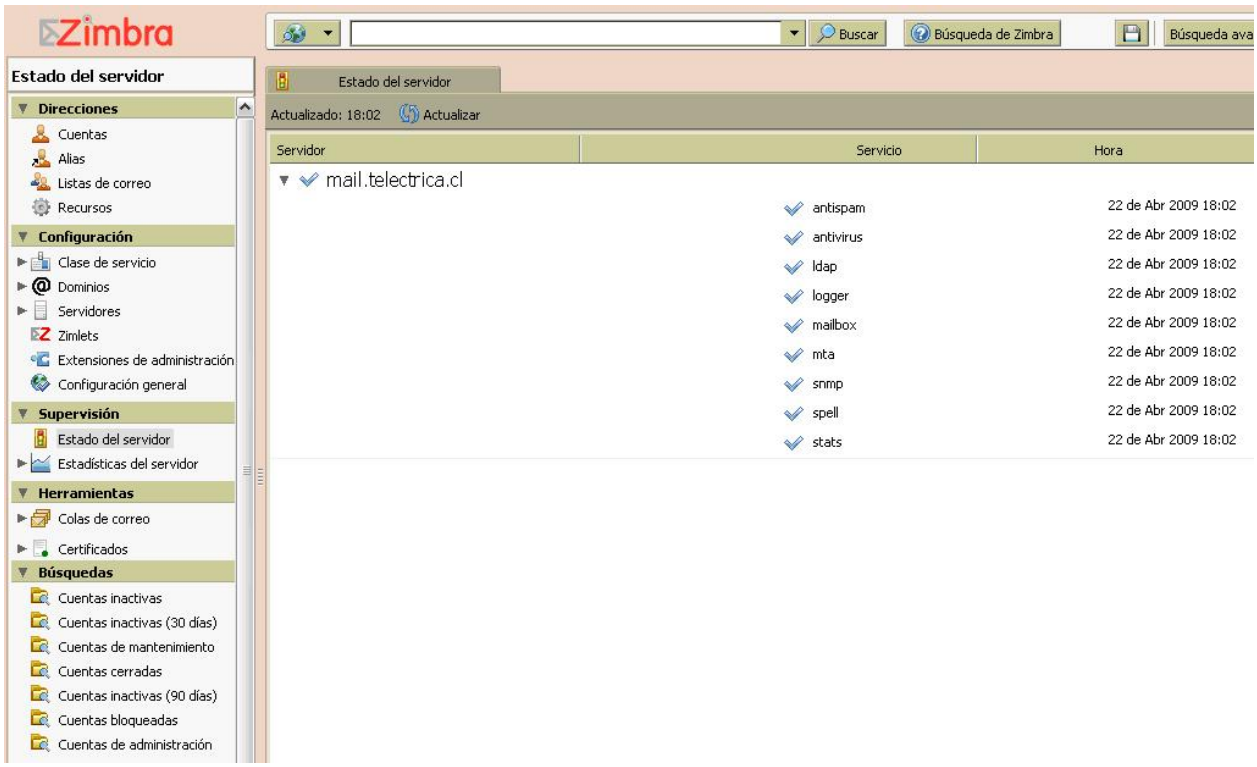


Figura 5 – 17: Consola de administración de Zimbra.

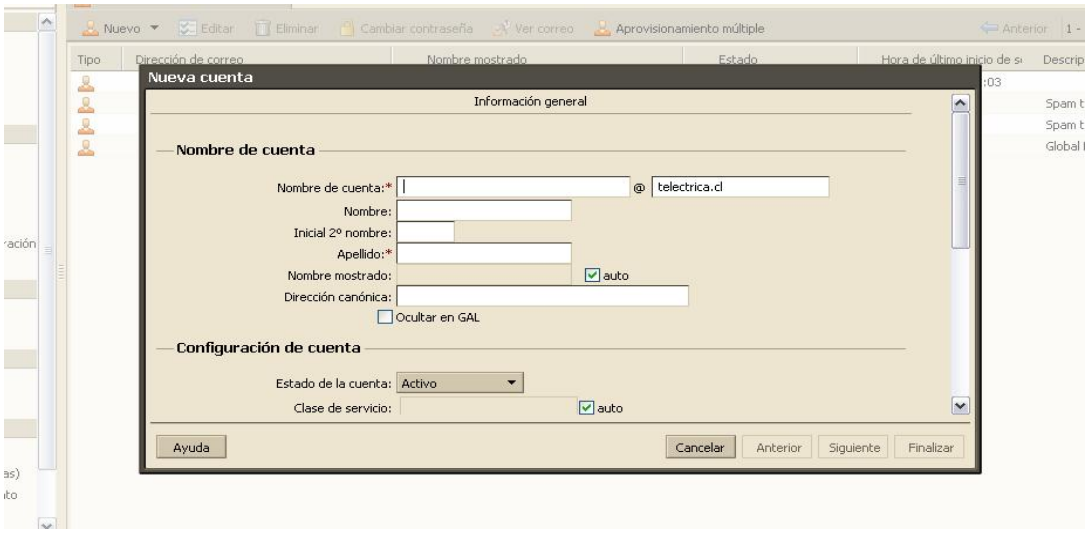


Figura 5 – 18: Formulario de creación de usuario.

Llenando el formulario de cuenta, nombre, apellido, información general, tipo de interface a usar, servicios que obtendrá el usuario y entre otras opciones de configuración.

Se accederá al menú de configuración de administración de las cuentas, y se verifica la cuenta creada.

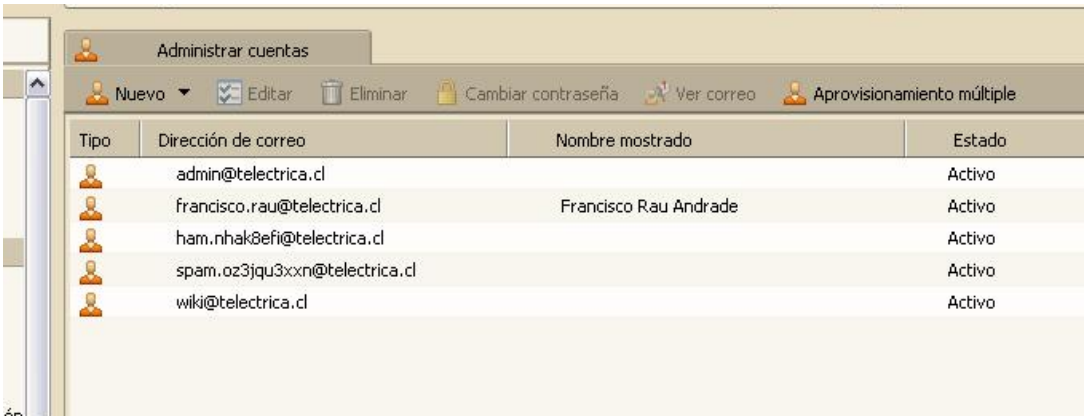


Figura 5 – 19: Administración de cuentas de usuario.

Una vez ya creado las cuentas para cada usuario, estos podrán acceder a la interfaz grafica de usuario de Zimbra, notar que no es la misma para acceder al menú de administración de Zimbra.

Para acceder a ella, se ingresa a la siguiente url: http://mail.telectrica.cl/

Una vez ya accedido al webmail de Zimbra, se tiene una interfaz fácil de usar y potente a la vez.

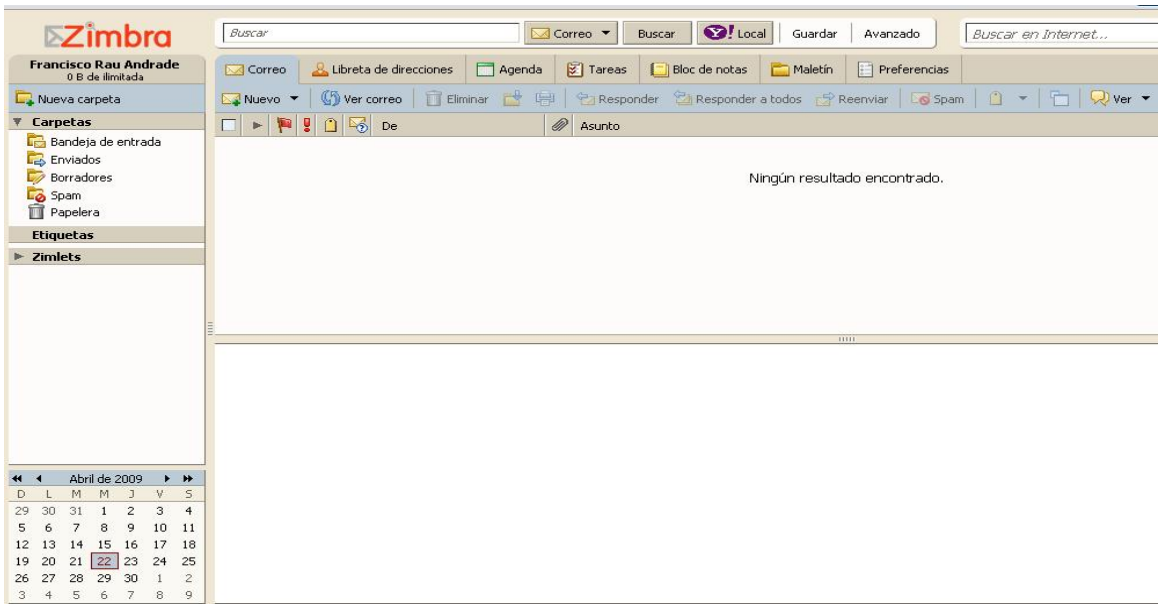


Figura 5 – 20: Entorno Web de e-mail de usuario.

5.4.7 Instalación y configuración de Apache

Para alojar páginas Webs se debe tener instalado un servidor Web, para ello se recomienda Apache, ya que es gratuito y el más usado para este propósito.
Para poder ocupar el servidor Web Apache, se debe habilitar (desocupar) el puerto 80, ya que esta siendo usado por Tomcat (servidor Web) de Zimbra. Cuando se tiene libre el puerto 80, se puede instalar sin problemas el servidor Apache. Una vez ya instalado, se recomienda activar los modulos “mod_proxy”, “mod_rewrite”, mod_proxy_html, mod_ssl y mod_proxy_http, para redireccionar el webmail de zimbra (que esta instalado con Tomcat), al servidor Web Apache.

Cabe señalar que el modulo Proxy se encuentra por defecto denegando todo, es por esto, que se debe configurar al igual que el modulo rewrite, para que acepte nuestras peticiones de la red.
Después de instalar apache, en la configuración de virtual hosts, se crea un nuevo archivo, para responder las peticiones a webmail de Zimbra.
Lo que se realiza es colocar la ubicación del sitio Web principal, llamado *www.telectrica.cl* y también la redirección del Webmail de Zimbra a webmail.telectrica.cl a *https. (Pagina segura).*

5.5 CONFIGURACIÓN DEL 3° SERVIDOR (ARCHIVOS)

5.5.1 Aplicación de Samba

Para configurar el servidor de archivos se utilizará Samba[14] (servidor de archivos) en un servidor con S.O Linux (Ubuntu Server 8.04 de 32 Bits).
Para tener un fácil manejo de creación de usuarios, carpetas y otorgamiento de permisos se instaló la herramienta Webmin, que es una herramienta de configuración de sistemas accesible vía web para OpenSolaris, GNU/Linux y otros sistemas Unix. Esto hace que sea más fácil la configuración de Samba.

5.5.2 Configuración de Samba a través de Webmin.

Se crearán dos usuarios y/o carpetas con distinto nivel de acceso una llamada “Gerencia” y la otra “Personal”, ya siendo la primera para el ingreso de usuarios que corresponda al nivel gerencia con su respectiva autenticación.
Lo mismo para la carpeta “Personal”.

A continuación se muestra un ejemplo de configuración de edición de usuario, crear comparticiones y configurar seguridad en Samba.

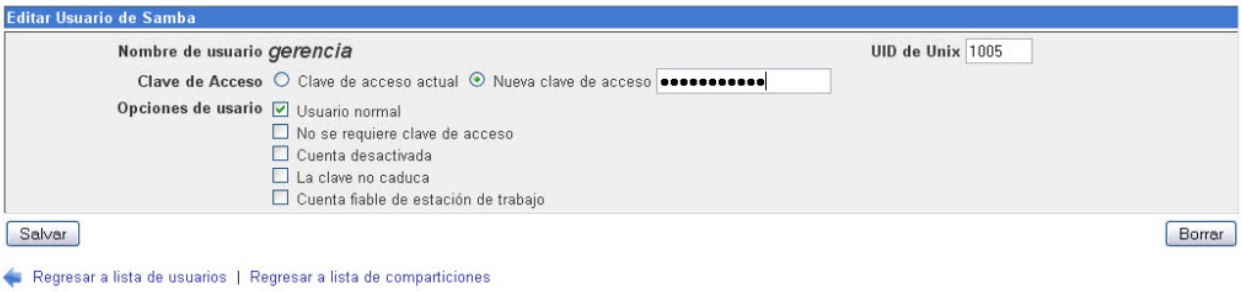


Figura 5 – 21: Edición de usuario en Samba.

[14] **Samba** es una implementación libre del protocolo de archivos compartidos de Microsoft Windows. De esta forma, es posible que ordenadores con GNU/Linux o Unix en general se vean como servidores o actúen como clientes en redes de Windows

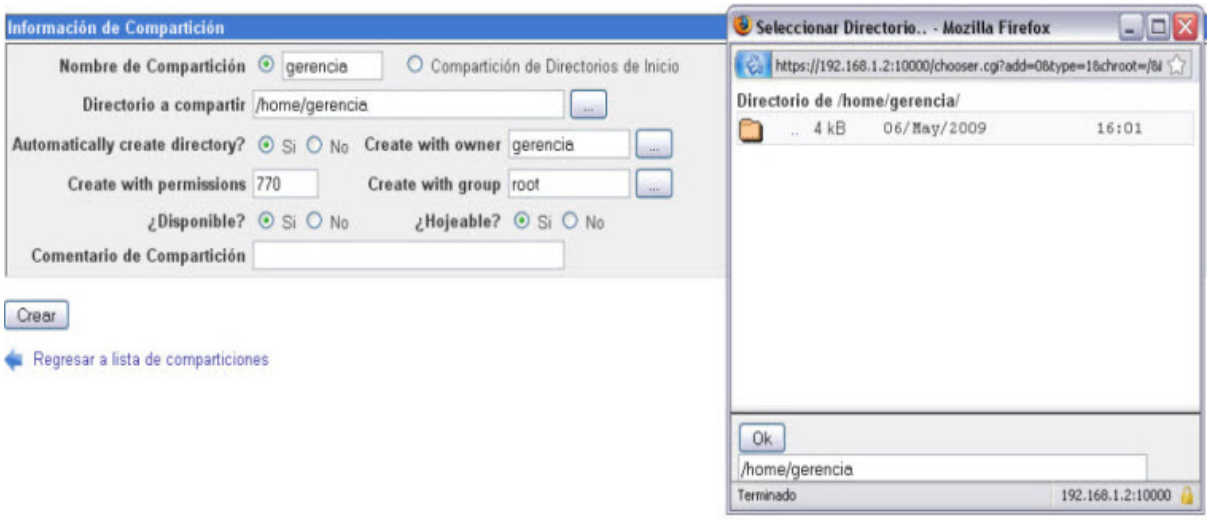


Figura 5 – 22: Creación de compartición de un archivo.

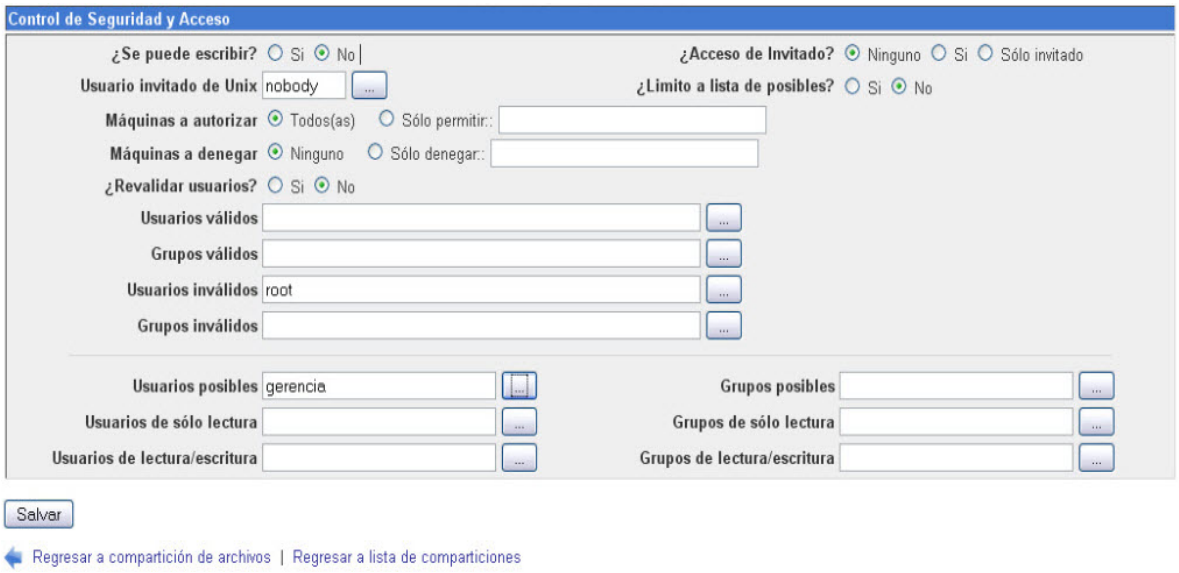


Figura 5 – 23: Configuración de seguridad de directorio Gerencia.

5.6 APLICACIÓN DE SEGURIDAD AL SERVIDOR DE ARCHIVOS

Al aplicar hardening al servidor de archivos se fortalecen los accesos a este, se asegura y se refuerza la información contenida y por ende la red local.
Hay variadas aplicaciones de hardening en S.O Linux como por ej. SELinux, Apparmor, Lids y Grsecurity que se diferencian en el modo de control de acceso.

Aplicación de hardening Linux con herramienta Grsecurity.

GRSecurity [5] es una solución de seguridad a modo de parche de kernel *(núcleo de Linux),* que permite establecer múltiples comprobaciones, verificaciones y controles de una forma activa del sistema. Estos mecanismos van desde la protección a nivel de funcionamiento del kernel, control de ejecución de las tareas en la pila TCP/IP, control de las actividades de los usuarios, permisos de ejecución en determinadas áreas del sistema, controles adicionales a la seguridad impuesta por chroot[15].
GRSecurity se basa en la siguiente filosofía:

- La seguridad no puede ser resuelta en una sola capa.
- Complicar el uso del sistema por aumentar la seguridad es inconcebible.
- Tiene que haber una forma de proteger todo el software que tengamos instalado, no sólo el que venga con nuestra distribución.
- Los humanos, en muchos casos, son el eslabón más débil en la seguridad.

[15] CHROOT es una llamada al sistema en Linux que permite configurar un directorio como "raíz" del sistema de ficheros para sus procesos. Es decir, permite configurar el sistema de forma tal que se puedan lanzar procesos confinados dentro de un determinado directorio. Cualquier fichero o directorio que esté fuera del CHROOT les quedará inaccesible.

La razón de elección de la aplicación Grsecurity radica en el hecho que es una herramienta poderosa frente a las otras mencionadas anteriormente. La herramienta que le podría igualar sería SELinux [9], pero aplicar las políticas de esta configuración es más complicado, ya que SElinux tiene una fuerte implementación de MAC (ver ANEXO 5), mientras que Grsecurity es más simple para usar y ofrece otras características exclusivas, como protección a espacios dirigidos y limitar recursos, esto es porque utiliza RBAC (Role Based Access Control).

RSBAC asocia roles a cada usuario. Cada rol define qué operaciones pueden ser llevadas a cabo sobre ciertos objetos. Dada una colección bien escrita de roles y operaciones, los usuarios estarán restringidos a hacer solamente aquellas tareas que se le configura. La restricción por defecto "deny-all" (negar todo), asegura que un usuario no pueda realizar una acción de la cual no haya pensado.

El sistema RBAC viene con una excelente característica denominada "modo de aprendizaje". Dicho modo puede generar una política previsora de mínimos privilegios para su sistema. Esto permite ahorros de tiempo y dinero para poder instalar múltiples servidores seguros.

Para usar el modo de aprendizaje se activa utilizando la herramienta llamada gradm de Grsecurity.

Gradm es una herramienta que le permite administrar y mantener una política para su sistema. Con ella puede activar o desactivar el sistema RBAC, recargar los roles RBAC, cambiar su rol, configurar un contraseña para el modo de administración, etcétera.

Protección de la red

La pila TCP/IP de Linux es vulnerable a ataques basados en predicciones. Grsecurity incluye parches de aleatorización para contrarrestar esos ataques. Aparte de esos parches, también puede activar restricciones a los sockets, con lo que se prohíbe completamente el acceso a la red a ciertos grupos.

Grsecurity permite a los administradores controlar IPs y puertos que se pueden activar en el servidor, también que IPs y puertos pueden conectarse los usuarios remotamente, que tipo de sockets y procesos pueden ser usados, y también que protocolos para sockets están disponibles.

Para instalar Grsecurity se recomienda hacer un respaldo de archivos ya que se instalará un nuevo *kernel* y ello conlleva a compilar el sistema operativo.
No olvidar que Grsecurity se instala parchando la distribución de Linux instalada, en este caso, se parchará a Ubuntu Server.
La instalación y configuración de Grsecurity queda referida al ANEXO 4

5.7 CONFIGURACIÓN DE RED INALÁMBRICA (ACCESS POINTS)

5.7.1 Configuración de Red Inalámbrica (AP1)

Para la red Lan se colocaran 2 access point Linksys WAP54G, tanto en el 1º piso como en el 2º piso, ambos en el pasillo para tener una excelente señal en el edificio.

Para el primer access point llamado “AP1”, tendrá la siguiente configuración:

IP: 192.168.1.3/24

GATEWAY: 192.168.1.1

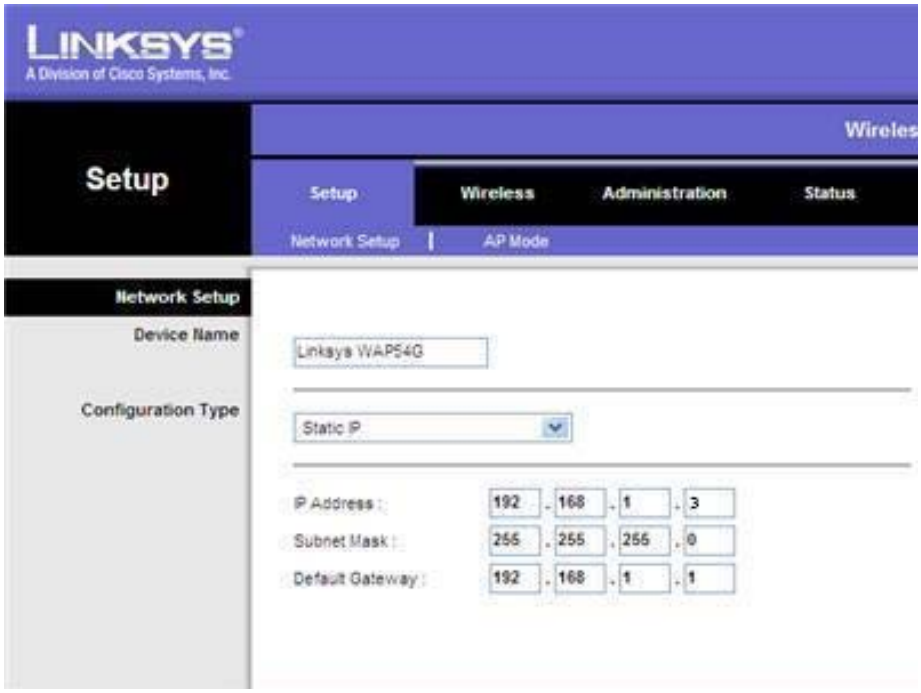


Figura 5 – 24: Configuración de *access point (AP1).*

5.7.2 Configuración de Red Inalámbrica (AP2)

Para el segundo access point llamado “AP2”, tendrá la siguiente configuración:
IP: 192.168.1.4/24
GATEWAY: 192.168.1.1

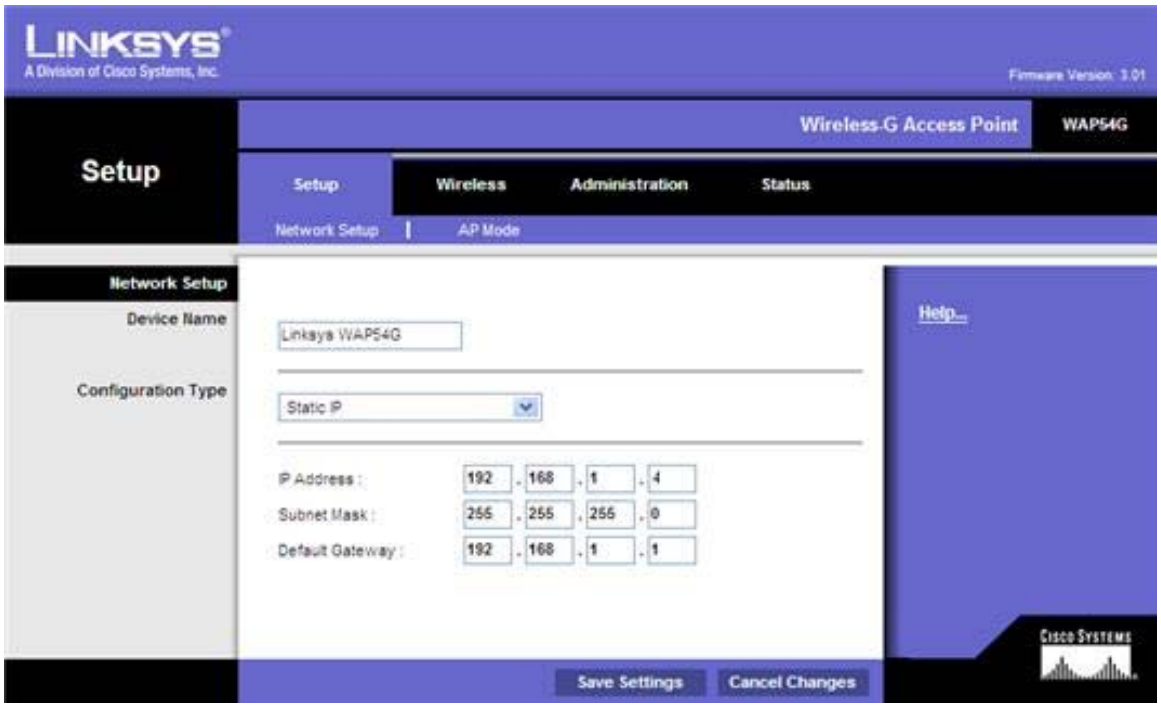


Figura 5 – 25: Configuración de *access point (AP2).*

En ambos casos la configuración de seguridad se realizó con el modo de seguridad WPA, con encriptación TKIP. Se quería realizar con WPA2 con encriptación AES, pero no es soportada por computadores portátiles antiguos.

CAPITULO 6: CONCLUSIONES

1.- Primeramente en este trabajo de titulación se describe las distintas tecnologías involucradas, dando información en el cableado de categorías 5e, 6 y 7, entre otras.
Cabe destacar que para el uso actual, se debe instalar categoría 6 para soportar a futuro velocidades de 1Gbps. Con respecto a la arquitectura de la red LAN, se decide por trabajar a velocidades entre servidores y switches de 1Gbps, dejando el cableado cat 6 disponibles a clientes (host), para ser utilizado a dicha velocidad en un futuro posterior. Esto beneficia a la red LAN, ya que no se deberá cablear el edificio nuevamente cuando se necesite una actualización.

2.- Las soluciones desarrolladas en redes LAN dependen de las condiciones y problemáticas que posea cada institución. Cuando se habla de pequeña empresa, se requiere que los gastos para implementar una red de área local que presente distintos servicios y además que contemple alta seguridad sean mínimos, no por ello la solución será de mala calidad o de baja eficacia.
La elección de Smoothwall Firewall como solución desarrollada en este trabajo, cumple con todos las necesidades que requiere la Empresa siendo estable, dando seguridad en la red interna, priorizando tráfico y dándole un costo mínimo tanto en software y hardware, este último por la reutilización del servidor con que la entidad contaba. Además se usará como administración de la red LAN.

En cuanto a las características técnicas de la solución Smoothwall Firewall frente a las soluciones de pago, esta es superior por el hecho de que el hardware utilizado es de mejor rendimiento y puede actualizarse en cuanto a la velocidad de las tarjetas de red, en la velocidad de procesamiento y en la

memoria, tanto de instrucción (ram), como de almacenamiento. Lo ultimo es recomendado si se requiere almacenar una buena cantidad de logs de registro, en cuanto al firewall o del sistema de protección contra intrusos (IDS).
Además se utilizó la zona DMZ (desmilitarizada), ya que unas de las necesidades es contar con servicios de correo y Web, y en base a que el software open-source Smoothwall Firewall posee esa característica se establecen tres zonas, llamadas WAN (área publica), DMZ (zona servidores) y LAN (interfaces a usuarios). Dando una seguridad mayor y evitando intrusiones a la red interna.

3.- En cuanto a la instalación y configuración del servidor de correo, se basa en la misma decisión de elección que el software Smoothwall Firewall. Siendo estas, software open-source, por su costo cero, gran rendimiento y accesible interfaz al usuario, siendo esta última de gran importancia para el personal de la empresa. El software open-source como es el caso de Smoothwall Firewall y Zimbra Suite, es una solución real y al alcance de las empresas pequeñas, las cuales comúnmente presentan poco presupuesto para invertir en servidores de seguridad informática y de servicios de correo. El aspecto “negativo” de esta solución open-source es que se debe tener base técnica previa o buscar la información necesaria para poder realizar una solución de buena calidad, que se adapte a las necesidades de la empresa y a veces, el encontrar esta información, no es tan fácil como se podría pensar.

Al contrario de las soluciones pagadas como Cisco y Watchguard que ofrecen gente capacitada para soporte 24x7x365, respaldo, actualizaciones, licencias para mayores usuarios e instalación total del sistema (“llave en mano”), siendo esto último una mala instrucción por parte de los administradores que manejarán el sistema, ya que no van a ser posibles o les tomará mas tiempo de

realizar medidas necesarias cuando tengan que actualizar políticas de seguridad o ante una eventual peligro.

4.- Se recomienda realizar actualizaciones periódicas al servidor firewall, en el sistema antivirus y al sistema IDS, revisiones a *logs* del firewall.
Con respecto al servidor de (correo, Web) y archivos siempre hay nuevas actualizaciones y parches a problemas de seguridad y de funcionalidad que hay que revisar.

5.- Con respecto a la Instalación de la red Wireless, se utilizaron 2 Access Point (AP), uno en cada piso, esto es para tener mas cobertura en toda la infraestructura. Fueron utilizados access point y no routers Wireless, para aprovechar las opciones de configuración de políticas de seguridad que ofrece Smoothwall Firewall. La configuración de seguridad utilizada en la red Wireless fue de WPA con encriptación TKIP, ya que es soportada en computadores portátiles antiguos. Se recomienda una vez que se tengan dispositivos o computadoras inalámbricas más actualizadas se haga un cambio en la seguridad y encriptación.

6.- Con respecto a la instalación del servidor de archivos se efectuó dos niveles jerárquicos de acceso. En él se ubicará toda la información de la empresa, es por ese motivo que se aplica *“hardening”* con la herramienta de seguridad llamada Grsecurity, fortaleciendo los accesos de intrusos con distintas opciones de configuración, el problema de esto, es que una incorrecta configuración puede bloquear ciertos procesos del sistema, dejando a veces inutilizable el servidor. Si se le agrega a esto, lo dificultoso de la instalación ya que es mediante de una compilación al sistema Linux, puede que sea un exceso de seguridad al equipo. Pero si se piensa que en cuanto a seguridad, siempre es bueno reforzar al máximo los servicios y/o aplicaciones, es una excelente

herramienta, si se realiza una correcta instalación al servidor que se quiere proteger.

7.- Se invitan a los alumnos o al lector, a realizar mejoras en cuanto a las soluciones planteadas en este trabajo de titulación.
Unas de las mejoras de la solución open-source Smoothwall Firewall a realizar a futuro, es la creación de una zona para la red inalámbrica obteniendo así un mejor control del tráfico pudiendo establecer políticas de seguridad.
Para el software open-source Zimbra Collaboration Suite, a través de Zimbra Admin GUI poder manejar cuentas de Samba, grupos y dominios.

Una mejora importante pero complicada a la solución de *hardening,* sería aplicar la herramienta Grsecurity a los servidores Web y correo, pero respetando la funcionalidad de este, es decir, no entorpecer los procesos de las aplicaciones, así cuida el correcto funcionamiento del sistema.

El aporte entregado en este trabajo de titulación fue desarrollar una solución que fuese del alcance de una pequeña empresa, que necesite de una red LAN de alta velocidad con herramientas de seguridad robustas y eficientes a bajo costo, dejando en el documento el desarrollo económico y técnico de la solución.
Se demuestra también que es posible desarrollar redes LAN usando solo software libre y open-source, sin estar sometidos a costos y licencias.

GLOSARIO

100Base-T: También conocido como Fast Ethernet o Ethernet de alta velocidad, se trata de un estándar de conexión Ethernet con una velocidad de transferencia de datos de hasta 100 Mbps.

802.3: Especificación del IEEE (Institute of Electrical and Electronics Engineers) que describe las características de las conexiones Ethernet en redes de cableado.

Access point (Punto de acceso): Dispositivo que intercambia los datos entre los diferentes ordenadores de la red. Los puntos de acceso no suelen tener cortafuegos ni funciones de traducción de direcciones (NAT).

Conector RJ-45: Clavija que se encuentra en los extremos de los cables Ethernet que realiza la conexión entre los ordenadores u otros dispositivos y el cable Ethernet.

DHCP: Sigla de Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de hosts). Es un protocolo TCP/IP que asigna automáticamente direcciones IP temporales a los ordenadores de la red local (LAN). El USR8200 Firewall/VPN/NAS es compatible con el uso de DHCP, lo que le permite compartir la conexión a Internet con varios ordenadores de la red.

DMZ: Sigla de Demilitarized Zone (Zona desmilitarizada). Se trata de un conjunto de dispositivos y subredes ubicadas entre la red privada y la conexión a Internet que protegen a dicha red de accesos no autorizados.

DNS: Sigla de Domain Name System (sistema de nombres de dominio). Servicio de consulta de datos utilizado principalmente en la Red para traducir

los nombres de los hosts en direcciones de Internet. La base de datos DNS traduce los nombres de dominios DNS a direcciones IP, de forma que los usuarios puedan localizar los ordenadores y servicios a través de nombres más sencillos.

Ethernet: Estándar de red que se sirve del cableado para proporcionar acceso a la red. Es la tecnología que más se utiliza para conectar ordenadores entre sí.

Firewall (Cortafuegos): Sistema de seguridad que protege la red de amenazas externas, como ataques de piratas informáticos. Un hardware de cortafuegos es un dispositivo de encaminamiento de conexión que dispone de una configuración de comprobación de datos específica con la que protege los dispositivos a los que está conectado.

IMAP

Internet Message Access Protocol. Los servidores que trabajan con IMAP reciben y almacenan los mensajes.

LDAP

Protocolo ligero de acceso al directorio (LDAP, del inglés Lightweight Directory Access Protocol). Un protocolo que permite a los usuarios acceder a información de contacto a través de una red.

Modelo de referencia ISO/OSI: Abreviatura del modelo de referencia de interconexión de sistemas abierto del Organismo Internacional de Estandarización (ISO).

Postfix

Es un Agente de Transporte de Correo (MTA) de software libre.

Sendmail

Es un popular "agente de transporte de correo" (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en "encaminar" los mensajes correos de forma que estos lleguen a su destino, se ejectuta sobre LINUX.

SMTP

Simple Mail Transfer Protocol. Normalmente, una aplicación de correo electrónico usa SMTP para enviar un mensaje a un servidor de correo. Después éste reenvía el mensaje al servidor adecuado.

SSL

Nivel de socket seguro (SSL, del inglés Secure Sockets Layer). Un protocolo seguro de transferencia de información a través de una red.

TLS

Seguridad de nivel de transporte (Transport Layer Security). Un protocolo seguro de transferencia de información a través de una red.

UTP: Sigla de Unshielded Twisted Pair (Par trenzado sin blindar) Cable con más de un par de hebras de alambre trenzadas sin ninguna cubierta protectora. Es más flexible y ocupa menos espacio que los cables de par trenzado blindados (STP) pero ofrecen un ancho de banda menor.

BIBLIOGRAFíA

[1]. GORMAZ RÍOS, VÍCTOR JAVIER, Diseño de red LAN en Instituto Profesional IPLACEX, administrada por servidor de red.
2007 - TUS-ELEC 2007 G671d.

[2]. ASENJO CASTRUCCIO, ESTEBAN ANDRÉS, Optimización e implementación de la red Lan del instituto de electricidad y electrónica UACH. 2006 UACH.

[3]. QUEZADA CANDIA, LUIS ANDRÉS, Incorporando seguridad en servidores Linux con herramientas de software libre.
2005 - TUS-MAT 2005 Q5i.

[4]. The Perfect Linux Firewall Part I - IPCop | HowtoForge - Linux Howtos and Tutorials.
URL: *http://www.howtoforge.com/perfect_linux_firewall_ipcop*
Última fecha de acceso a URL: Enero 2009.

[5]. GRSECURITY - Seguridad en sistemas Linux mediante Detección, Prevención y Contención.
URL:http://www.hacktimes.com/files/GRSECURITYHackTimes.com.V1.0.pdf
Última fecha de acceso a URL: Abril 2009.

[6]. ANTONIO PERPINAN, **Seguridad de sistemas GNU/Linux.**
Código Libre Dominicano
URL: http://www.codigolibre.org
Última fecha de acceso a URL: Mayo 2009.

[7]. SNORT.

URL: http://en.wikipedia.org/wiki/Snort_(software)

Última fecha de acceso a URL: Abril 2009

[8]. HARDENING.

URL: http://technet.microsoft.com/es-ar/library/dd574128.aspx

Última fecha de acceso a URL: Febrero 2009

[9]. SELINUX

URL: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-selinux.html

Última fecha de acceso a URL: Junio 2009

[10]. HYPERLINE SYSTEMS, Cableado cat. 7

URL:http://esp.hyperlinesystems.com/catalog/cable/sstp4_c7_solid_indoor.shtml

Última fecha de acceso a URL: Marzo 2009

[11]. SECURITY FOCUS

URL: http://www.securityfocus.com

Última fecha de acceso a URL: Mayo 2009

[12]. CERT (Equipo de Respuestas a Emergencias de Computación)

URL: http://www.cert.org

Última fecha de acceso a URL: Abril 2009

[13]. ZIMBRA COLLABORATION SUITE

URL: http://www.zimbra.com

Última fecha de acceso a URL: Febrero 2009

ANEXOS

ANEXO 1: Instalación de Zimbra Edition

Se procederá a desinstalar exim ya que zimbra viene con su propio servidor de correo, se desinstalará sus principales archivos.

```
#apt-get remove --purge exim4 exim4-base
```

Se procede a instalar algunos paquetes necesarios. Algunos de estos paquetes ya están instalados en el sistema.

```
#apt-get install sudo libidn11 curl fetchmail libgmp3c2 libexpat1
```

Ahora se procederá a descargar Zimbra la cual es una aplicación muy completa ya que ella viene con todo lo que se necesita para configurar un servidor de correo sin necesidad de descargar otras aplicaciones.
Al descargar Zimbra se descarga por defecto, zimbra apache, zimbra snmp, zimbra schema, entre otros paquetes.
Primero se irá al directorio de los archivos temporales ya que allí es donde se alojaran todos los archivos a descargar.

```
#cd /tmp
```

Se conectará al servidor para descargar Zimbra suite, para versión Ubuntu Server 64 bits.

```
#wget
http://h.yimg.com/lo/downloads/5.0.14_GA/zcs5.0.14_GA_2850.UBUNTU8_64.20090303215740.tgz
```

Ahora se descomprimirán el archivo zcs*.tgz

tar -xzf zc*

Ya cuando todos los paquetes se hayan descargado en temporales se ingresa al archivo:

#cd /temp/zcs*

Una vez ya ingresado al directorio, para ejecutar la instalación se escribe el siguiente comando.

#./install.sh

Zimbra ahora va a comprobar si los prerrequisitos están instalados en el sistema. Debe aparecer algo similar a lo siguiente:

```
Checking for prerequisites...
    NPTL...FOUND
    sudo...FOUND sudo-1.6.8p12-4
    libidn11...FOUND libidn11-0.6.5-1
    fetchmail...FOUND fetchmail-6.3.6-1etch1
    libpcre3...FOUND libpcre3-6.7+7.4-4
    libgmp3c2...FOUND libgmp3c2-2:4.2.1+dfsg-4
    libxml2...FOUND libxml2-2.6.27.dfsg-6
    libstdc++6...FOUND libstdc++6-4.1.1-21
    openssl...FOUND openssl-0.9.8c-4etch3
    libltdl3...FOUND libltdl3-1.5.22-4
Prerequisite check complete.
Checking for standard system perl...
    perl-5.8.8...FOUND standard system perl-5.8.8
```

Ahora se selecciona los paquetes a instalar menos el de zimbra –Proxy.

Debe de quedar similar a esto.

```
Found zimbra-mta
Found zimbra-snmp
Found zimbra-store
Found zimbra-apache
Found zimbra-spell
Found zimbra-proxy


Select the packages to install

Install zimbra-ldap [Y] Y

Install zimbra-logger [Y] Y

Install zimbra-mta [Y] Y

Install zimbra-snmp [Y] Y

Install zimbra-store [Y] Y

Install zimbra-apache [Y] Y

Install zimbra-spell [Y] Y

Install zimbra-proxy [N] N
Checking required space for zimbra-core
checking space for zimbra-store
```

Después de la instalación, aparecerá el menú de configuración de Zimbra.

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                             Enabled
   3) zimbra-store:                            Enabled
        +Create Admin User:                    yes
        +Admin user to create:                 admin@telectrica.cl
******** +Admin Password                       UNSET
        +Enable automated spam training:       yes
        +Spam training user:                   spam.oz3jqu3xxn@telectrica.cl
        +Non-spam(Ham) training user:          ham.nhak8efi@telectrica.cl
        +Global Documents Account:             wiki@telectrica.cl
        +SMTP host:                            mail.telectrica.cl
        +Web server HTTP port:                 80
        +Web server HTTPS port:                443
        +Web server mode:                      http
        +IMAP server port:                     143
        +IMAP server SSL port:                 993
        +POP server port:                      110
        +POP server SSL port:                  995
        +Use spell check server:               yes
        +Spell server URL:                     http://mail.telectrica.cl:7780/aspell.php
        +Configure store for use with reverse mail proxy: FALSE
        +Configure store for use with reverse web proxy: FALSE

   4) zimbra-mta:                              Enabled
   5) zimbra-snmp:                             Enabled
   6) zimbra-logger:                           Enabled
   7) zimbra-spell:                            Enabled
   8) Default Class of Service Configuration:
   r) Start servers after configuration        yes
   s) Save config to file
   x) Expand menu
   q) Quit
```

Se deberá ingresar una contraseña al acceso de administrador.

Como política de empresa todo el mundo que se conecte al Webmail deberá ser redirigido por página segura, es por esto, que se cambio el modo del Web Server a https.

Una vez ya hecho los cambios, se aplica la configuración escribiendo “a”, como se muestra en la siguiente figura:

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                          Enabled
   3) zimbra-store:                         Enabled
   4) zimbra-mta:                           Enabled
   5) zimbra-snmp:                          Enabled
   6) zimbra-logger:                        Enabled
   7) zimbra-spell:                         Enabled
   8) Default Class of Service Configuration:
   r) Start servers after configuration     yes
   s) Save config to file
   x) Expand menu
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes] y
Save config in file: [/opt/zimbra/config.8600] y
Saving config in y...done.
The system will be modified - continue? [No] y
Operations logged to /tmp/zmsetup.04222009-154557.log
Setting local config values...
```

Ya completada la instalación, se comprobará si lo servicios de zimbra se están ejecutando correctamente. Para ello se debe cambiar la cuenta para ingresar como administrador zimbra. Con el comando.

su – zimbra

Y con el siguiente comando podremos ver el estado de los servicios.

```
zimbra@mail:~$ zmcontrol status
Host mail.telectrica.cl
        antispam                Running
        antivirus               Running
        ldap                    Running
        logger                  Running
        mailbox                 Running
        mta                     Running
        snmp                    Running
        spell                   Running
        stats                   Running
zimbra@mail:~$
```

Todos los servicios que trae esta suite, están corriendo satisfactoriamente.

ANEXO 2: Configuración de Autentificación en Zimbra

Si se requiere por parte del ISP (Proveedor de Servicios en Internet) autentificarse para mandar lo correos de Zimbra, se debe realizar la siguiente configuración.

Se entra a la consola de administración de Zimbra, como administrador, en la pestaña Configuración, se entra a la configuración general.
En el recuadro de “MTA de retransmisión para entrega externa” (ver Figura A3 – 1), se debe colocar el servidor SMTP, que entrego el ISP al que se le contrata el servicio de Internet. Además se debe colocar el puerto al cual esta dirigido.

Si este requiere colocar un usuario y contraseña se debe ir a la consola del servidor, es decir, en *Shell* se debe ingresar en modo usuario zimbra.
Con el siguiente comando:

```
#sudo – zimbra
```

Con el siguiente comando se creará un archivo de texto en el cual tendrá el nombre y contraseña de la autentificación del servidor STMP.

```
$echo mailrelay.example.com username:password > /opt/zimbra/conf/relay_password
```

Con el siguiente comando se creará una tabla de loopback en postfix de Zimbra.

```
$postmap hash:/opt/zimbra/conf/relay_password
```

$postmap -q mailrelay.example.com /opt/zimbra/conf/relay_password

Después del último comando ingresado se debe volver el nombre de usuario y contraseña que se colocó anteriormente.
Para que postfix use la contraseña señalada anteriormente se debe escribir en el archivo de configuración del mismo. Esto se hace con el siguiente comando:

$postconf -e smtp_sasl_password_maps=hash:/opt/zimbra/conf/relay_password
$postconf -e smtp_sasl_auth_enable=yes
$postconf -e smtp_cname_overrides_servername=no

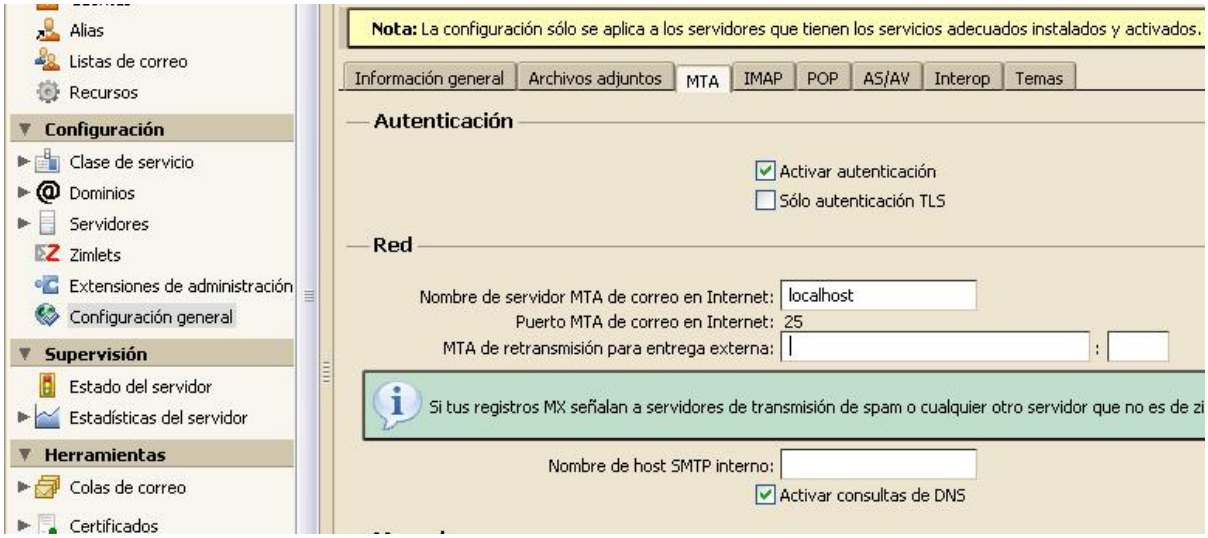


Figura A2 – 1: Configuración de autentificación en Zimbra

Una vez hecho lo anterior, se debe reiniciar postfix, con el siguiente comando:

$ postfix reload

Cabe mencionar que todos los comandos ingresados se realizaron con el usuario zimbra.

El siguiente comando, a2ensite (available2enablesite) crea un enlace en sites-enable al sitio que se indique (es decir, activa el virtualhost que se acaba de crear). Este comando se ingresa en el directorio /etc/apache2.

```
# a2ensite zimbra
```

Se recarga apache2:

```
# /etc/init.d/apache2 force-reload
```

ANEXO 3: Utilidades y comandos en Zimbra Collaboration Suite

Todos los comandos deberán ejecutarse como usuario zimbra, normalmente accedido mediante *sudo su – zimbra* al hacer login:

- zmcontrol status: obtener el estado de los diversos daemons que forman el sistema Zimbra.
- zmcontrol start/stop: arrancar/parar el sistema Zimbra.
- zmcontrol -v: mostrar la versión
- zmtlsctl [mixed|both|http|https|redirect]: cambiar el tipo de acceso permitido al webmail.
    - mixed realizará la validación sobre HTTPS y luego volverá al modo HTTP.
    - both permitirá indistintamente uno y otro.
    - redirect cambiará al usuario al modo https y lo mantendrá en ese modo (recomendado).
    - http forzará que se trabaje sólo sobre HTTP.
    - https forzará que se trabaje únicamente sobre HTTPS (recomendado).
- El fichero de configuración principal de Zimbra es /opt/zimbra/conf/localconfig.xml. Cualquier cambio que se quiera hacer

sobre el sistema para que sobrevivan a las actualizaciones deberán realizarse en éste fichero y en los demás dentro del directorio /opt/zimbra/conf.

- zmzimletctl listZimlets: mostrará un listado de los Zimlets instalados.
- zmzimletctl deploy zimlet.zip: instalrá el Zimlet zimlet.zip, que deberá encontrarse dentro del subdirectorio /opt/zimbra/zimlets-extra/.
- zmlocalconfig: permite realizar cambios sobre la configuración local guardada en el fichero /opt/zimbra/conf/localconfig.xml.
- zmprov: aprovisionamiento de cuentas. zmprov es un comando que permite interactuar con casi cualquier parte del sistema desde la consola de comandos, por ejemplo para crear o borrar cuentas desde un script. Puede actuar sobre los siguientes sistemas:
    - Cuentas.
    - Calendario.
    - Configuración.
    - COS (Class Of Service).
    - Dominios.
    - Listas de distribución.
    - Buzones de correo.
    - Wiki.
    - Búsquedas.
    - Servidores.
    - Otros (misceláneos).

Los comandos de consola disponibles se encuentran en /opt/zimbra/bin. Además un gran conjunto de utilidades del sistema en forma de scripts de Perl están disponibles en /opt/zimbra/libexec.

ANEXO 4: Instalación de Grsecurity

Para tener una optima instalación, se sugiere actualizar el servidor, con el siguiente comando.

#apt-get upgrade

#apt-get update

Se descargan algunas dependencias para instalar Grsecurity.

#apt-get install build-essential bin86 kernel-package ncurses-dev

Se ingresa al directorio /usr/src, para descargar el kernel que soporta Grsecurity, además del parche y la utilidad de administración Gradm.

Descarga del Kernel:

#wget http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.27.10.tar.bz2

Descarga de Grsecurity:

#wget http://www.grsecurity.net/grsecurity-2.1.12-2.6.27.10-200812271347.patch.gz

Nótese que la versión del Kernel y la versión del parche Grsecurity debe ser la misma, en este caso es la versión 2.6.27.10, para que sean compatibles.
Cuando se baja el Gradm, la herramienta de administración de GRSecurity para el sistema RBAC, tenemos que bajar la versión que corresponda a la del GRSecurity que se elige.
(Se encuentra en la misma página donde se baja su parche).

Descarga de Gradm:

#wget http://www.grsecurity.net/gradm-2.1.12-200812271437.tar.gz

Ahora se comienza a parchear con Grsecurity las fuentes del Kernel, para ello se necesita descomprimir el kernel descargado.

#tar -xjvf linux-2.6.27.10.tar.bz2

Se aplica el parche a las fuentes con el comando **patch.**

#gunzip < grsecurity-2.1.12-2.6.27.10-200812271347.patch.gz | patch -p0

Se cambia el nombre del directorio para diferenciar el nuevo Kernel a los demás, y se crea un enlace para trabajar más cómodamente.

#mv linux-2.6.27.10 linux-2.6.27.10-grsec

#ln -s linux-2.6.27.10-grsec linux

Se entra al directorio /usr/src/Linux, y se ingresa el comando,

#make menuconfig

Se desarrolla la compilación como cualquier otra versión en Linux.

Grsecurity se instala en la configuración del Kernel de Linux, dentro de **Security Options** (ver figura 5 – 30).

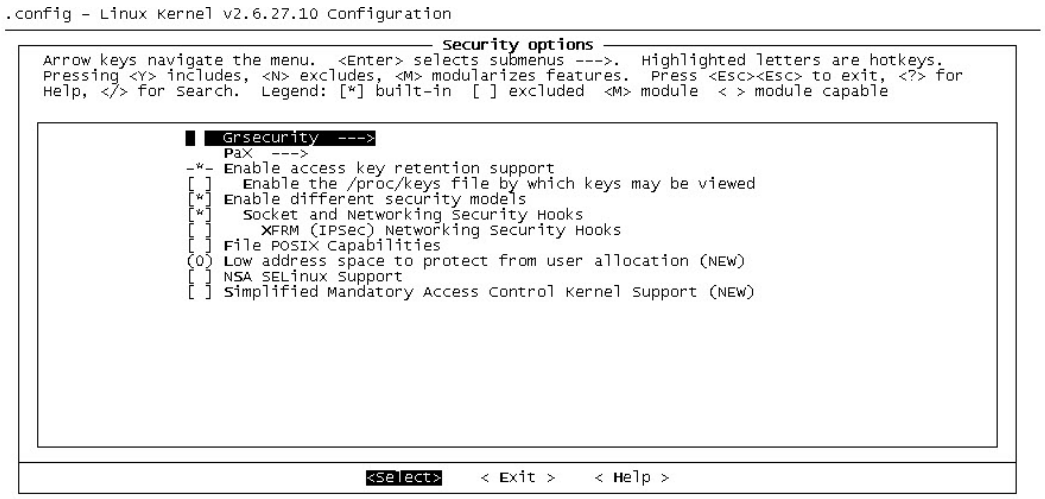


Figura A4– 1: Instalación Grsecurity

Ingresando en él se tiene la opción de definir distintos niveles de seguridad por defecto: low, medium y high que configuran todas las opciones al nivel correspondiente de seguridad.

Para la configuración de seguridad al servidor de archivos se elegirá la opción low.

Para saber qué abarca cada uno, se puede ingresar a la ayuda que se tiene en la parte inferior derecha de la pantalla.

Descripción de opciones de configuración de Grsecurity

Debido a tener variadas opciones de configuración se describirá las más importantes a continuación, y en ella estará activa la opciones de la configuración low, previamente elegida.

Address Space Protection

(Deny writing to /dev/kmem, /dev/mem, and /dev/port)

Suele ser una medida de seguridad no tener soporte para módulos y, de esta forma, evitar que se pueda cargar código malicioso en el *kernel*. Esta opción, además, deniega el acceso de escritura a los dispositivos mencionados, lo que aumenta el nivel de seguridad bloqueando los métodos disponibles para cargar código al *kernel* activo.

Concretamente, esta opción no trabaja bien con el modo gráfico o con aplicaciones como el vmware.

Disable privileged I/O

Otra opción que permite proteger al servidor de que se hagan modificaciones en el kernel activo. No es compatible con el uso del modo gráfico.

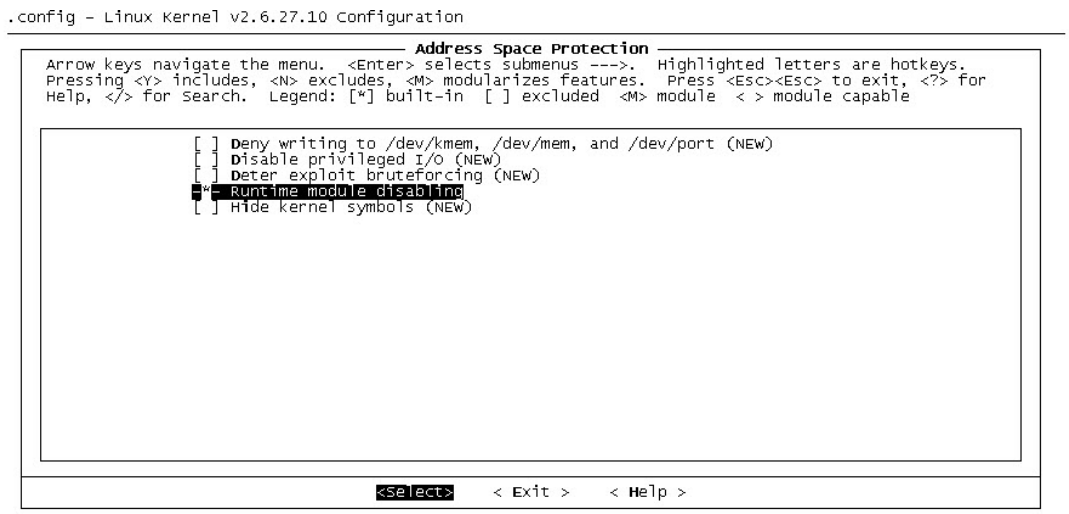


Figura A4 – 2: Configuración *address space protection*

Role Based Access Control Options

Hide kernel processes

Si se activa esta opción, se va a poder esconder los procesos relacionados con el kernel. Para ver, se tendrá que autenticar con la aplicación Gradm.

(3) Maximum tries before password lockout

La cantidad de veces que el usuario se puede validar en el entorno Linux.

(30) Time to wait after max password tries, in seconds

El tiempo que se tiene entre los intentos de validación.

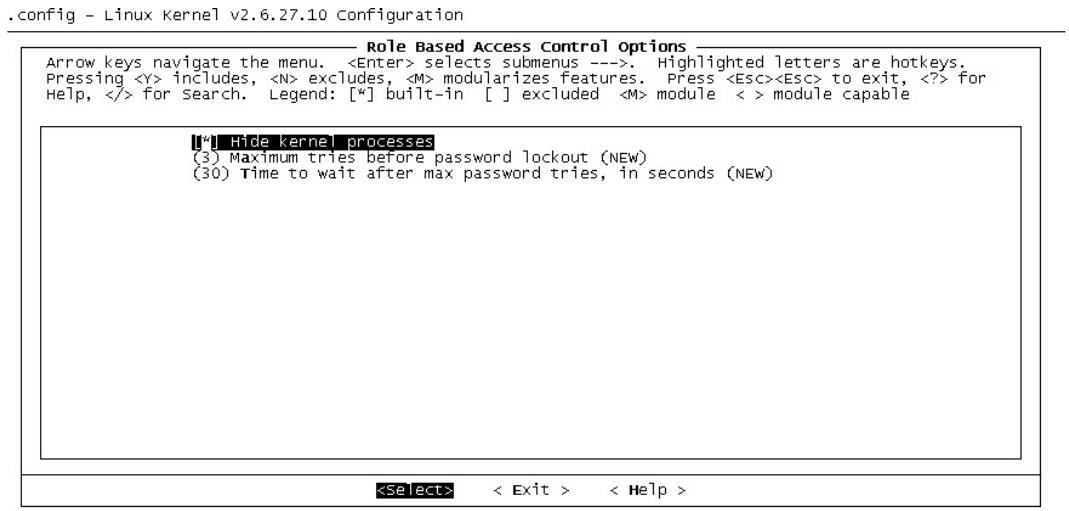


Figura A4 – 3: Configuración *role based access control options*

Filesystem Protections

- **Proc restrictions**

Algo muy inseguro es que los usuarios puedan ver los procesos del sistema o los de otros usuarios. Habilitando esta opción, se aumenta la seguridad del directorio /proc[16] y, a partir de ese momento, los usuarios van a poder ver únicamente sus procesos.

[16] *Llamado sistema de archivos, contiene una jerarquía de archivos especiales que representan el estado actual del kernel, permitiendo a las aplicaciones y usuarios mirar detenidamente en la vista del kernel del sistema.*

- **Linking restrictions**

Luego de elegir esta opción, los usuarios no van a poder seguir links simbólicos para los cuales no son dueños en directorios con permisos sticky bit[17], como el /tmp, a menos que el dueño del enlace sea el dueño del directorio.

- **Chroot jail restrictions**

De activar esta opción, se tendrá disponibles más restricciones que aumentan la seguridad en entornos chroot.

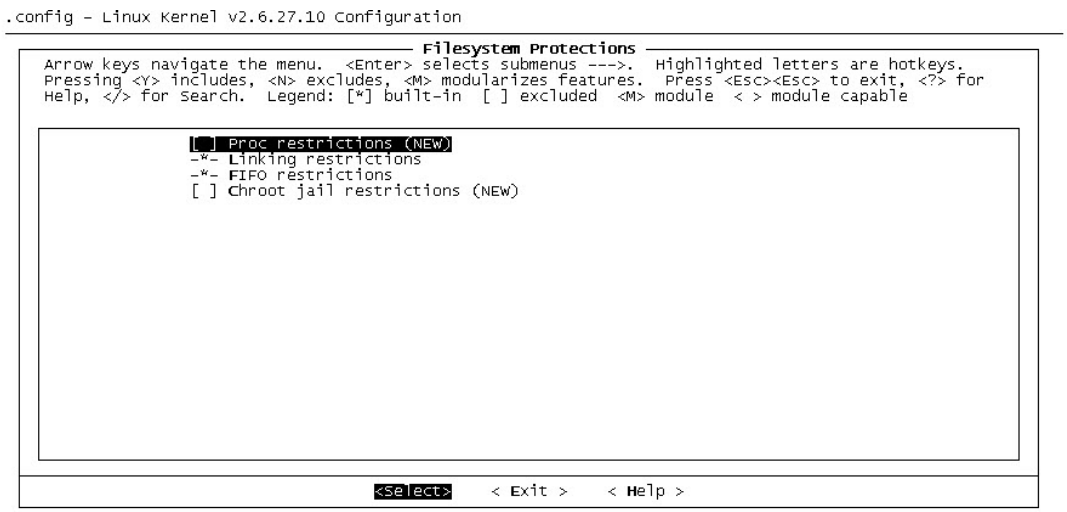


Figura A4 – 4: Configuración *filesystem protections*

Kernel Auditing

Single group for auditing

Con esta opción, Grsecurity va a auditar qué aplicaciones ejecuta cada usuario, aplicaciones, etc. Si se tiene muchos usuarios, los logs crecen demasiado. Con esta opción se puede limitar los logs a un grupo de usuarios concreto.

[17] *Es un permiso de acceso que puede ser asignado a ficheros y directorios.*

Las siguientes opciones sirven para registrar o no ciertas acciones de los usuarios. Es posible registrar ejecuciones, cambios de directorio, recursos, dispositivos montados y desmontados, señales enviadas a los procesos, entre otras opciones.

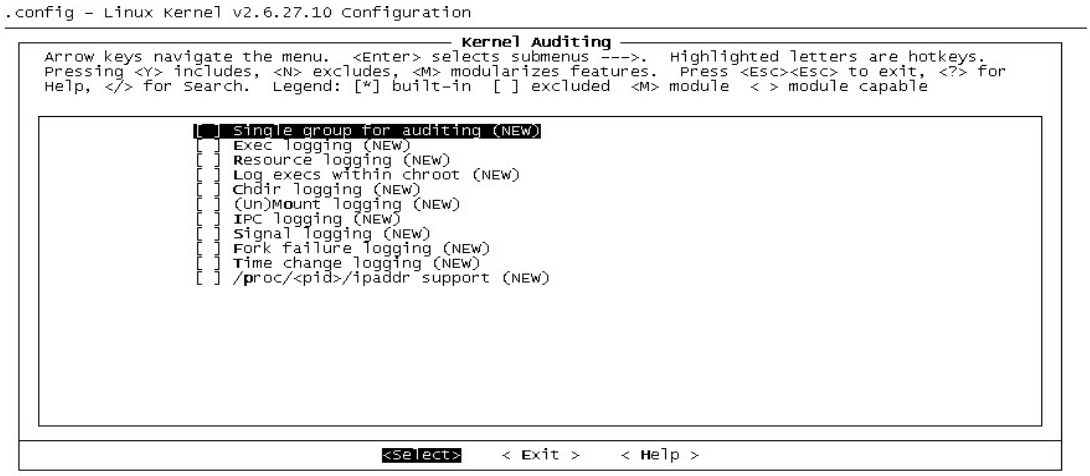


Figura A4 – 5: Configuración *kernel auditing*

Sysctl[18] support

Con esto se habilita la posibilidad de modificar opciones de Grsecurity de inmediato activando o desactivándolas en el directorio “/proc/sys-/kernel/grsecurity”.

[18] *El comando sysctl es usado para visualizar, configurar y automatizar configuraciones del kernel en el directorio /proc/sys/. Para tener una vista rápida de todas las variables configurables en el directorio /proc/sys/, se escribe el comando /sbin/sysctl -a como root.*

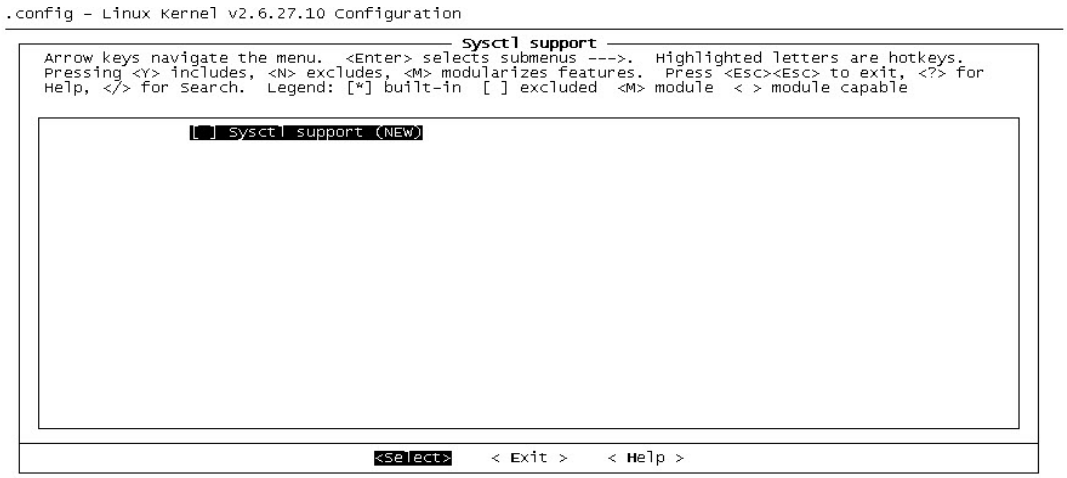


Figura A4 – 6: Configuración *sysctl support*

Logging Options

(10) Seconds in between log messages (minimum)

Se fija el tiempo mínimo entre mensajes del GRSecurity al syslog[19].

(4) Number of messages in a burst (maximum)

Idem al anterior, pero con la cantidad máxima de mensajes consecutivos.

[19] *syslog es un estándar para el envío de mensajes de registro en una red, su función es registrar un intento de acceso con contraseña equivocada, variaciones en el funcionamiento normal del sistema, alertas cuando ocurre alguna condición especial, errores del hardware o el software, entre otras opciones.*

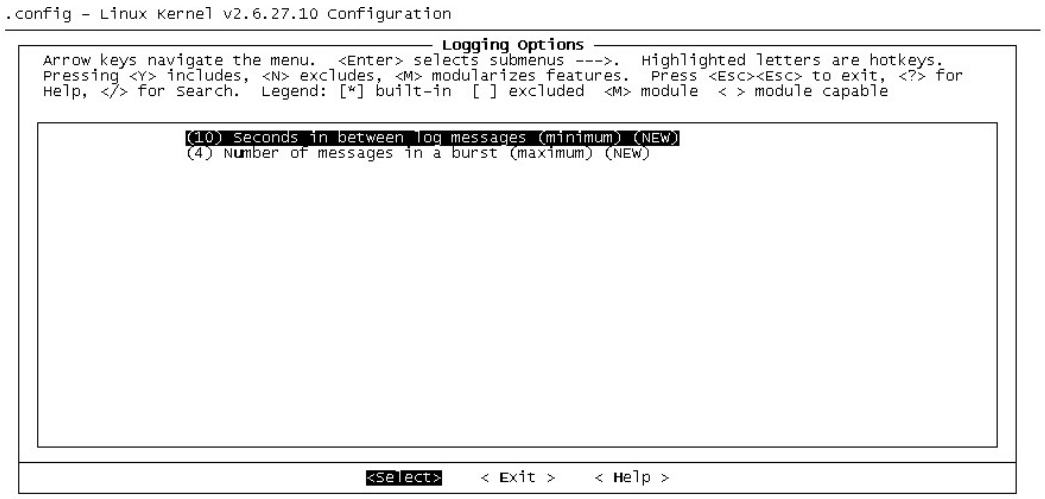


Figura A4 – 7: Configuración *logging options*

Generar ACLs usando modo *learning*

Existe una forma de autogenerar las ACLs[20] usando la herramienta de Grsecurity llamada gradm.

En Linux en modo *shell,* se ejecuta el siguiente comando para iniciar la herramienta.

#gradm –D

[20] es un concepto usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Se pedirá el password que se define con anterioridad. Luego se puede ejecutar gradm para que “aprenda” los servicios, aplicaciones que ejecuta el servidor, de esta forma, genera las ACLs de forma automática en el sistema. El proceso tarda tiempo que se defina, dado que durante el aprendizaje de gradm, se tendrá que usar todos los servicios que se puedan de la manera que corresponda.

En otras palabras, se forzará la rotación de logs, se ejecutara las tareas programadas, todo lo que usualmente se hace con el equipo. Así, gradm aprenderá lo que tiene que permitir y puede generar reglas lo más completas posible.

```
linux:/var/log# gradm -F -L /etc/grsec/learning.log
```

Luego, se tiene un archivo en /etc/grsec llamado learning.log, se va a crear reglas en base a él de la siguiente forma:

```
linux:/etc/grsec# gradm -F -L /etc/grsec/
learning.log -O /etc/grsec/acl
```

Ya teniendo listo el archivo de ACLs, se examinará un extracto de él:

```
subject / {
        /
        /dev                            h
        /dev/initctl
        /lib                            rx
        /proc                           h
        /proc/sys/kernel/version        r
        /var                            h
        /var/mail/root
        /var/spool/cron/crontabs
        /bin
        /bin/ls                         x
        /bin/ps                         x
        /etc                            r
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/grsec                      h
        /sbin
        /sbin/gradm                     x
        /usr
        /usr/local
        /usr/share/zoneinfo/America/Bs_As    r
        -CAP_ALL
        bind    disabled
        connect disabled
}
```

Siendo:

```
x = ejecutar
r = leer
h = oculto
```

Figura A4 – 8: Registro de archivo ACLs

También se pueden personalizar estos valores por proceso para tener un sistema lo más ajustado posible. Se pueden crear políticas para aplicaciones, como bind, apache, vsftpd y todos los servicios que están disponibles en el entorno Linux,

Ahora se comenzará a usar el nuevo esquema de seguridad. Para hacerlo, se activará Grsecurity, pero antes se renombra el archivo acl al esperado.

```
# mv acl policy
```

Se activa grsecurity:

```
# gradm -E
```

Cuando se ejecute un comando como “ls all” al directorio /etc/grsec este no se podrá mostrar ya que se configuró como “invisible”, por lo que luego de activar Grsecurity, no se podrá ver más el directorio.

ANEXO 5: Modelos de control de acceso

Tradicionalmente los sistemas Unix han utilizado el modelo de control de acceso discrecional (Discretionary Access Control, DAC) en el que un usuario tiene un completo control sobre los objetos que le pertenecen y los programas que ejecuta. Así mismo, el programa ejecutado por un usuario tendrá los mismos permisos de ese usuario que lo está ejecutando.

Esto implica que la seguridad del sistema depende de las aplicaciones que se están ejecutando y, por tanto, cuando se produce una vulnerabilidad de seguridad en una aplicación, ésta afecta a todos los objetos a los que el usuario tiene acceso. Así, si la aplicación es ejecutada por root, el atacante puede obtener los máximos privilegios en la máquina, comprometiendo la seguridad global del sistema.

Otro modelo de control de acceso es el denominado control de acceso obligatorio (Mandatory Access Control, MAC), donde existe una política de seguridad definida por el administrador y que los usuarios no pueden modificar. Esta política va más allá de establecer propietarios de archivos sino que fija "contextos", en donde se indica cuando un objeto puede acceder a otro objeto.

Este modelo de control de acceso puede aumentar el nivel de seguridad, especialmente cuando se establece como base de la política definida que no se permite cualquier operación no expresamente autorizada. La implementación de este modelo de seguridad para todo un sistema puede ser una tarea muy tediosa.

En teoría deben definirse reglas para cualquier usuario que utiliza cualquier programa que accede a cualquier objeto del sistema. Para evitar tener que llegar a este detalle de definición, algo que fácilmente se convertiría en un monstruo inmanejable, se utiliza el concepto de control de acceso basado en roles (Role-Based Access Control, RBAC). Bajo este modelo, el administrador define una serie de roles y asigna a los usuarios en los diferentes roles que corresponden a su perfil. Como ejemplo, el usuario de un programa únicamente necesita disponer de permisos para leer y escribir los archivos utilizados por esa aplicación concreta, pero nada más.
Otros usuarios es posible que necesiten permisos para poder leer archivos, pero no modificarlos. Cada uno de estos usuarios se asignará a diferentes roles.

Las listas de control de acceso (ACLs, *Access Control Lists*) proveen de un nivel adicional de seguridad a los ficheros extendiendo el clásico esquema de permisos en Unix: mientras que con estos últimos sólo podemos especificar permisos para los tres grupos de usuarios habituales (propietario, grupo y resto), las ACLs van a permitir asignar permisos a usuarios o grupos concretos; por ejemplo, se pueden otorgar ciertos permisos a dos usuarios sobre unos ficheros sin necesidad de incluirlos en el mismo grupo. Este mecanismo está disponible en la mayoría de sistemas Unix (Solaris, AIX, HP-UX), mientras que en otros que no lo proporcionan por defecto, como Linux, puede instalarse como un *software* adicional.