Universidad Nacional Autónoma De Nicaragua
Recinto Universitario "Rubén Darío"
Departamento De Tecnología

TEMA:

DISEÑO DE UNA RED QUE PERMITA ACCEDER A LOS SERVICIOS TELEMÁTICOS, APLICANDO ARQUITECTURA DMZ COMO SEGURIDAD, BAJO PLATAFORMA LINUX Y VIRTUALIZACIÓN, EN RADIO FE – NANDAIME

Elaborado por:

Br. Fernando José García Matus
Br. Oscar Danilo Montano López

Tutor:

Edwin Quintero Carballo

TEMA:

SEGURIDAD Y VIRTUALIZACIÓN EN REDES LAN

SUB-TEMA:

DISEÑO DE UNA RED QUE PERMITA ACCEDER A LOS SERVICIOS TELEMÁTICOS, APLICANDO ARQUITECTURA DMZ COMO SEGURIDAD, BAJO PLATAFORMA LINUX Y VIRTUALIZACIÓN, EN LA RADIO FE-NANDAIME

DEDICATORIA

A:

Dios, por brindarme siempre salud y sabiduría para realizar mis proyectos, guiarme por el buen camino y nunca soltarme en esos momentos que envuelven todos los sentimientos en la vida.

Mi Madre, **Marítza del Carmen Matus Lacayo**, quien con arduo esfuerzo y sacrificio siempre sabe guiarme, ayudarme y aconsejarme para ser una persona de bien; a ella que siempre vela para que en nuestra familia exista la paz y el amor, Gracias Mamá.

Mi Padre, **Gregorio Emiliano García Castro**, persona ejemplar que con rectitud y valor me ha enseñado a caminar en esta vida. Cada consejo que me ha dado es un gran regalo que no olvido, digno ejemplo a seguir que agradezco infinitamente por demostrarme confianza y firmeza.

Mis Hermanos, **Elliane, Emiliano, Rodolfo, Cynthia**, por estar conmigo y apoyarme siempre, los quiero mucho.

A mi tío **Medardo García**, al tío mas tuani de todos.

Mi Novia **Michelle Flores y** su **familia**, les agradezco de todo corazón lo bueno que han sido conmigo y los grandes momentos que hemos compartido.

Mis **Amigos**, agradezco a ustedes por estar ahí en todo momento en las buenas y malas, Alejandra, Jade, Emma, Victoria, María, Martha, Jackson “el patrón”, Samuel, Carlos, Juan, Toto, Jorge, Russo, Mijail, Lucho, Ledvi, Fabio, Nacho, Champions, Montano y los q no recuerdo ahorita.

Mis **maestros**, aquellos que marcaron cada etapa de nuestro camino universitario, y que me ayudaron en asesorías y dudas presentadas en la elaboración de mi trabajo.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

Fernando José García Matus

DEDICATORIA

A DIOS

Por haberme permitido llegar hasta este punto y haberme dado salud, ser el manantial de vida y darme lo necesario para seguir adelante día a día para lograr mis objetivos.

A la memoria de mi madre Rosa López

Por confiar en mí, quien cerró sus ojos antes de ver sus sueños realizados, a ella esta tesis por su apoyo, ayuda y sacrificio desde el inicio de mi carrera.

A mi padre Luis Montano

Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante.

A mis hermanos

Isabel, Luis, Lester, Carlos y Bayardo; por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo.

A mis amigos

Que nos apoyamos mutuamente en nuestra formación profesional y que hasta ahora, seguimos siendo amigos: Fer, Fabio, Nacho, Champions, Eveling, Carol, Ana Yeldi, Francela; por haberme ayudado a realizar este trabajo.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto.

Oscar Danilo Montano López

AGRADECIMIENTO

A Dios por ayudarnos y darnos paciencia para no decaer en los momentos difíciles.

A nuestros familiares que nos brindaron su apoyo moral y económico en el transcurso de nuestra carrera.

A los docentes que verdaderamente trabajaron a la par de nosotros, y que nunca trataron de esquivarnos en los momentos de dudas; y que juntos trabajamos arduamente en nuestra formación profesional.

A nuestros colegas: Fabio Baca, Ezequiel Corea y Freddy Orozco (La Champions); que estuvieron al lado nuestro a lo largo de nuestra carrera universitaria; y que con su picardía hicieron más ameno los momentos de cansados trabajos….

A todos aquellos que directa o indirectamente hicieron posible la realización de este trabajo.

A todos ustedes **Muchas Gracias!!!**

INDICE

Contenido

ÍNDICE DE TABLAS

ÍNDICE DE IMÁGENES

INTRODUCCIÓN

La información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales. Por el enorme número de amenazas y riesgos que existen a lo largo del mundo, la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y sobre todo que permita una eficiente administración del riesgo.

Este trabajo consiste en el diseño de una red cuyo escenario es una radio local ubicada en la ciudad de Nandaime que lleva por nombre Radio Fe, con la dificultad que no cuenta con una red segura, capaz de filtrar el acceso desde la red externa.

Esta propuesta se basa en una red que utilice la arquitectura DMZ como seguridad; el propósito es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna. Todo esto se logra mediante la configuración de un firewall, debido a que posee la mayoría de las herramientas de seguridad; además de que se propone la tecnología de virtualización, alojando los servidores en un solo equipo, dando como resultado aprovechamiento de los recursos, ahorro energético y una administración simplificada, permitiendo una considerable reducción de costos al momento de su implementación.

RESUMEN

En el presente trabajo de fin de carrera nos hemos dispuesto a realizar una propuesta de seguridad para la red local de Radio Fe, una emisora joven del municipio de Nandaime, y que puede ser empleada en otras redes de pequeñas empresas. La arquitectura desmilitarizada (DMZ) como base del proyecto, es utilizada para crear un muro perimetral el cual nos salva de posibles ataques que se realicen a nuestra red.

De la mano con UNIX/LINUX utilizamos la potente herramienta Netfilter, que incluye en sus bases a Iptables, el cual utilizamos para crear un verdadero muro perimetral gracias a sus políticas de restricción y acceso dirigida a todo tipo de usuarios.

Uno de los objetivos a alcanzar es la creación de servicios telemáticos (WEB, FTP, DNS, CORREO), para así dar a conocer la radio y tener una base solida en cuanto a el desarrollo tecnológico, esto se hace posible aun mas con la creación de un sitio web por medio del cual la radio podrá hermanarse con radios amigas.

Debido a los altos costos que se tienen a la hora de montar estos nuevos servicios y estructurar bien la topología, se recurrió a la implementación de la virtualización, que nos ayudara a poseer nuestros servidores en una sola maquina física, pero obteniendo un buen desempeño y resultados a la hora de realizar sus funciones, dándonos así una baja en los precios, la cual en el documento reflejamos las comparaciones del uso de la virtualización y cuando no la utilizamos.

JUSTIFICACIÓN

Para la realización de este trabajo se seleccionó la radio local que lleva por nombre “Radio FE”, ubicada en el Centro Cristiano de Restauración Espiritual Nandaime, y que empieza a transmitir en el 2005 por los 98.7 frecuencia modulada, la radio es de carácter cristiano y auspiciada por un organismo extranjero que tiene un plan de sensibilización dirigida a jóvenes canadienses; con la idea de que la transmisiones radiales sea monitoreada por los cooperantes que en algún momento visitaron o visitaran la ciudad (Nandaime), además de llevar el mensaje cristiano mas allá de la localidad y así cumplir con uno de los principios fundamentales de la radio de expandir las enseñanzas cristianas; pretenden transmitir vía internet.

Ante tal la situación, se propuso el diseño de una red que permita acceder a los servicios telemático DHCP, FTP, DNS, CORREO, WEB, utilizando la arquitectura DMZ como seguridad, bajo plataforma Linux y Virtualización; en donde puedan alojar su portal web. Con el uso de las DMZ, la radio tendrá un punto a favor en la seguridad de su información y de sus comunicaciones, creándose una zona de perímetro entre la red interna y la red externa (Internet) lo que permitirá el control todos los individuos que accesen a la red. De esta, además de alcanzar la transmisión por internet, la Integridad, confidencialidad y una buena administración; acompañada de la tecnología de virtualización, lo cual nos ayudara a reducir costos, gestionar de forma más eficiente los recursos, dar un mantenimiento más eficaz y veloz, y sobre todo a simplificar las funciones de administración. De usarse este diseño la radio tendrá una mejor seguridad y tendrá una mayor audiencia. Además podrá hermanarse con otras instituciones cristiana y adquirir recursos de apoyo a beneficio de los proyectos humanitarios mediante publicidad en su página web.

OBJETIVO GENERAL

Diseñar una red que permita acceder a los servicios telemáticos, utilizando arquitectura de seguridad desmilitarizada (DMZ), utilizando Iptables bajo plataforma Linux y Virtualización, en la Radio Fe-NANDAIME

OBJETIVOS ESPECÍFICOS

1. Identificar los aspectos generales de la red de área local de la Radio Fe (topología, estructura, direccionamiento IP)

2. Elaborar un diseño (Topológico y direccionamiento IP) en Radio Fe que incluya servidores de software libre.

3. Instalar un servidor dedicado, en la Radio Fe, para la administración de los servicios (FTP, WEB, DNS, CORREO, DHCP.)

4. Configurar una DMZ bajo una plataforma Linux , para obtener alto nivel de seguridad en la red

5. Proponer una reducción de costo al hacer uso de Virtualización en la red.

1 DESARROLLO

Por lo valiosa que se convierte la información en las empresas, existen personas ajenas a la institución, también conocidas como intrusos informáticos o hackers, que buscan tener acceso a la red empresarial para modificar, sustraer o borrar datos. Tales personajes pueden incluso formar parte del personal administrativo o de sistemas, de cualquier compañía; muchas veces las violaciones e intromisiones a los recursos informáticos se realiza por el personal interno, debido a que éste conoce los procesos, metodologías y tiene acceso a la información sensible de su empresa, es decir, a todos aquellos datos cuya pérdida puede afectar el buen funcionamiento de la organización.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías, porque no existe el conocimiento suficiente relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas.

Para contrarrestar esta problemática y cumplir con los objetivos de este trabajo se elaboró un esquema que nos guiara en la propuesta del diseño de una red que permita acceder a los servicios telemáticos, aplicando arquitectura DMZ como seguridad en Radio Fe – Nandaime.

1.1 Estructura del desarrollo

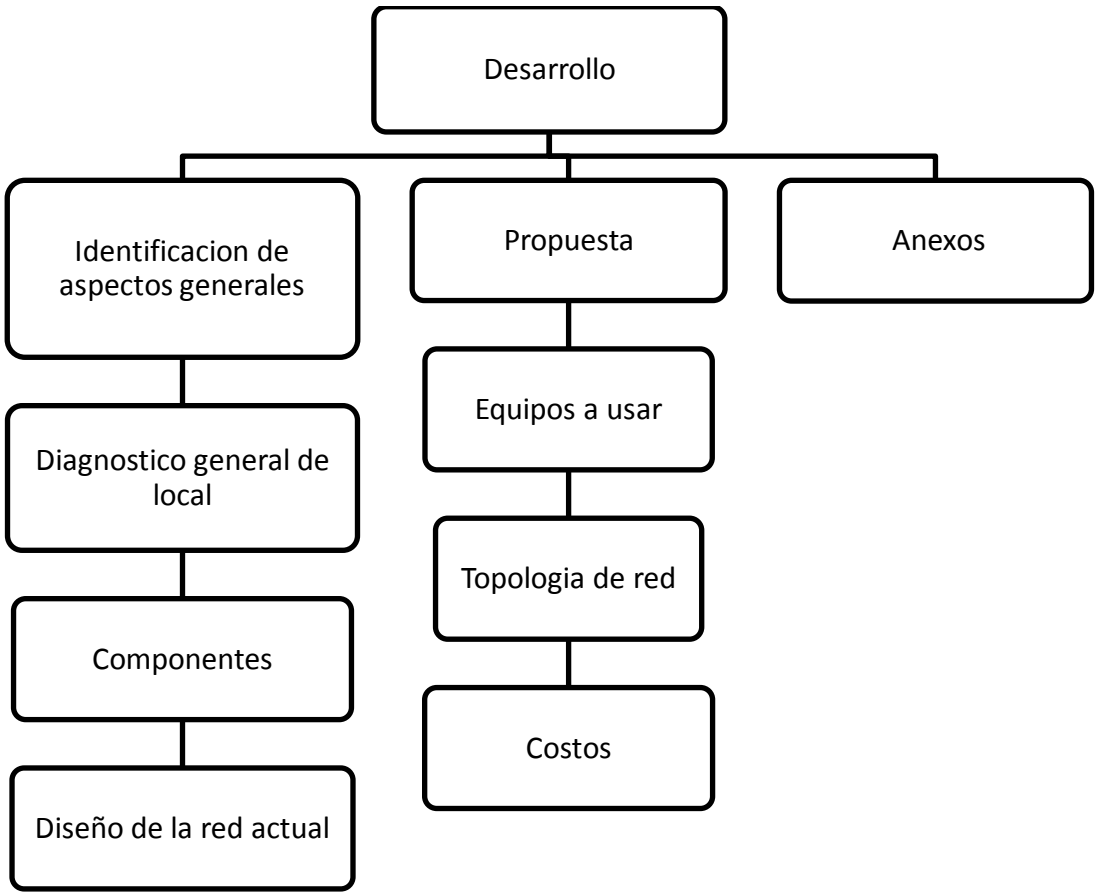

Imagen 1: Esquema del desarrollo

1.2 DIAGNOSTICO

Radio Fe está ubicada a 70 km de la capital en la calle central de la ciudad de Nandaime, municipio del departamento de Granada. Se aloja en el Centro Cristiano de Restauración Espiritual; sale al aire en el 2005 por los 98.7 FM bajo la dirección del Lic. Oscar Alguera, con el fin de fomentar el Cristianismo a la población en general. En la actualidad la radio subsiste de las donaciones que llegan al Centro, proveniente de un organismo extranjero.

Para captar la necesidad de la radio se hizo una visita y entrevista al director quien explico “Radio Fe es una radio que pretende llevar su transmisión vía internet y ampliar nuestra red para brindarle servicio al centro que nos aloja sin poner en riesgo la integridad de la radio…” de igual forma se realizo entrevista a los trabajadores; esto con la intención de identificar un poco más a fondo la debilidad de la red y necesidades de la radio, lo que arrojo resultados satisfactorios.

Se logro percibir que el mayor propósito de la radio es transmitir vía internet, con la dificultad de que no cuentan con una red segura ni de un portal web que además podría ser utilizado para la recaudación de recursos y llevar a ejecución los proyectos sociales en los que el Centro de Restauración espiritual se enfoca. Otro factor que podría limitar las intenciones de la radio es el servicio de internet con el que cuentan, que en la actualidad es de 5M contratado, esto sin descartar que disminuya en dependencia de la cantidad de usuarios conectados al mismo nodo.

En lo que respecta a la red; es una red punto a punto, que carece de seguridad lo que pondría en riesgo la integridad de la radio al momento de alojar en internet su sitio web.

Debido a lo captado mediante las entrevistas se propuso el diseño de una red segura donde puedan alojar su portal web y se podrá transmitir audio y video, permitiéndole una mayor difusión y la posibilidad de hermanamiento con distintos ministerios tanto nacionales como internacionales, que en un futuro les pueden colaborar en materiales, equipos de transmisión, o en donaciones para los proyectos humanitarios que el centro realiza.

Después de las entrevistas se procedió a la inspección del local, donde se identifico cada uno de sus aspectos; esto permitió la elaboración de un plano estructural que luego nos facilitará determinar los puntos donde se ubican los equipos.

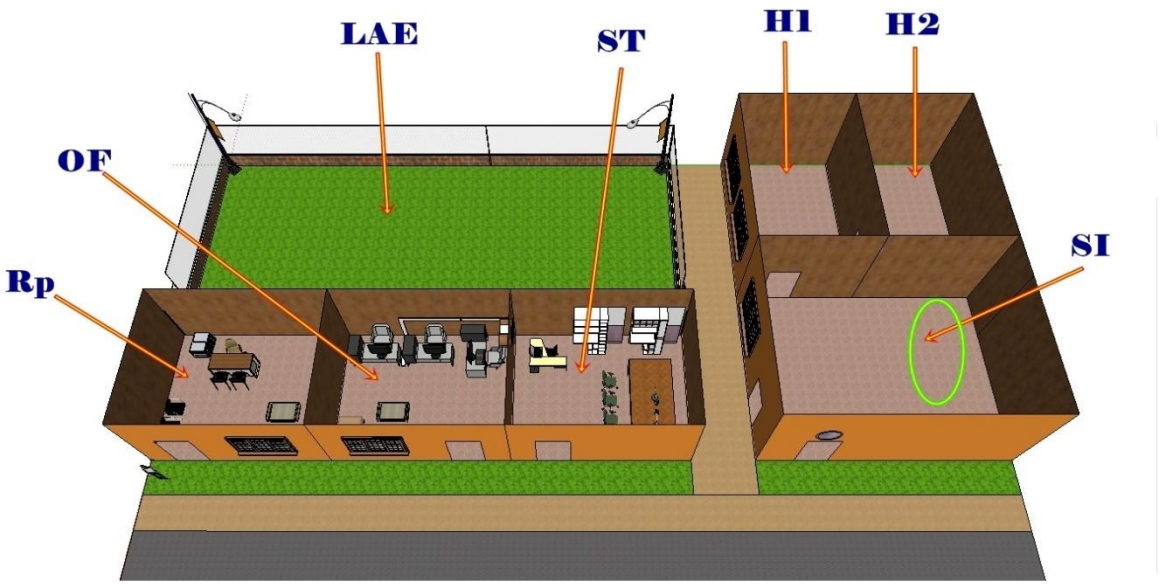

Imagen 2: Plano de las instalaciones de Radio Fe

La figura muestra la estructura física de la radio, en ella se puede contemplar que es una estructura sencilla que cuenta con una recepción, una oficina, la sala de transmisión; estas tres áreas construidas en un mismo edificio de 16m de largo y 4m de ancho el cual está dividido en secciones de 5m de largo por 4m de ancho;

un espacio donde se quiere instalar una pequeña sala de informática que tiene medidas simétricas de 4X4m respectivamente , 2 habitaciones de alojamiento para los cooperantes de 6m de largo y 6m de ancho, un espacio enmallado donde realizan actividades propias del centro. Cada uno de los espacios ha sido caracterizado mediante simbología, la que a continuación se describe en la siguiente tabla.

1.2.1 Descripción de la simbología

Símbolo	Leyenda
RP	Recepción
OF	Oficina
ST	Sala De Transmisión
SI	Sala Destinada Para Informática
H1	Habitación
H2	Habitación
LAE	Local Abierto Para Eventos

Tabla 1: Descripción de Simbología Utilizada en el Plano De Instalaciones

Mediante la inspección ocular de la planta física se observo y reconocieron todos y cada uno de los lugares donde se encuentran los equipos conectados a la red además de los equipos de transmisión constatando así que en la recepción a pesar de ser el punto donde se le brinda información a todos los que visitan el lugar no cuenta con host lo que facilitaría la localización de documentación y le ayudaría a llevar un control de agenda de las actividades que ahí se realizan, en la oficina se localizan un router, tres host donde se tiene información tanto del Centro como de la Radio y en la sala de transmisión dos host y la consola de transmisión.

Para comprender un poco mejor se construyo una rotulación en el plano de la radio en el que se ubican los puntos donde se encuentran los equipos.

A continuación se mencionan los equipos de la red con los que cuenta la radio:

Equipo	Característica
1 ALL IN ONE	ALL IN ONE MSI AE2410 Procesador INTEL DUALCORE 2410M DE 1.7 GHZ DISCO DURO DE 500GB MEMORIA RAM 1GB WINDOWS 7 ULTIMATE
3 DELL	PROCESADOR INTEL CELERON 1.6GZ DISCO DURO DE 500 HZ RAM 1GB WINDOWS XP SERVICE PACK2
MINI LAPTOP HP	PROCESADOR INTEL CELERON 1.6GHZ, 2GB DE RAM 300 GB DE DISCO DURO, WINDOWS 7 ULTIMATE
ROUTER	ROUTER BROADTECH ADSL2+ 8186-V2

Tabla 2: Equipos que Están Conectados en la Red Actual de a Radio

La siguiente grafica muestra la ubicación de los componentes de la red

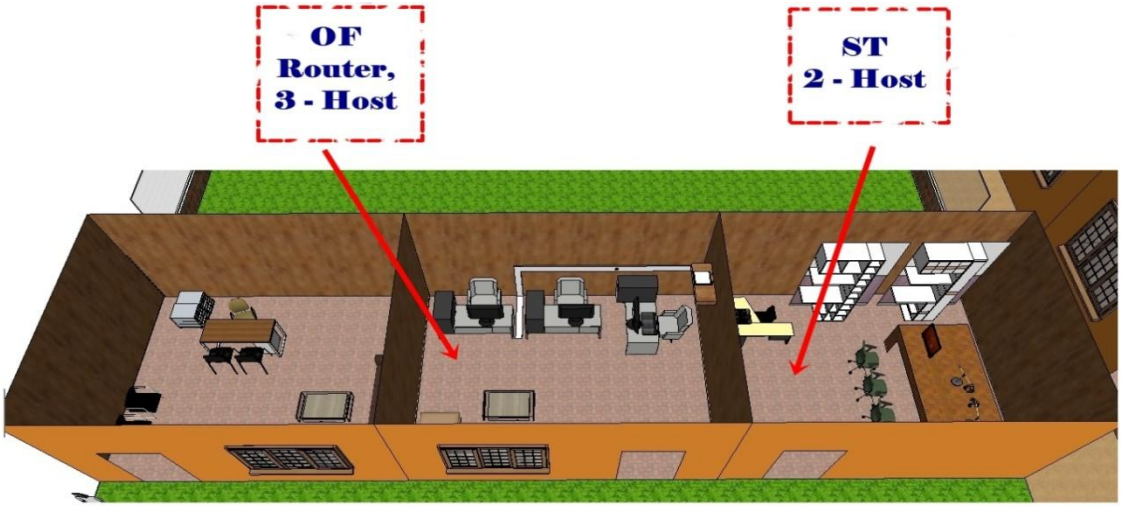

Imagen 3: Red actual de la radio

1.2.1- Aspectos generales de la red de área local de la Radio Fe (topología, estructura, direccionamiento IP)

La red local de Radio Fe, es una red provista por el ISP de Claro, la cual llega hasta Radio Fe desde la línea fija de Teléfono convencional, utilizando línea de abonado digital asimétrica (ADSL), La señal llega a través de un par simétrico de cobre y es separada por un filtro que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL, esto para evitar distorsiones en las señales transmitidas.

Estas señales después de ser separadas llegan hacia el teléfono y hacia el router BROADTECH ADSL2+ 8186-V2. El ancho de banda contratado es de 5 Mb, suministrado por la empresa Claro Nicaragua.

Las características del router son las que se especifican en la siguiente tabla:

Puertos	**4 puertos Ethernet 1 puerto ADSL**
Accesibilidad	Accesibilidad para conexiones wifi
Seguridad	Login y contraseña provista por ISP encriptación de seguridad inalámbrica WEP (muy débil)
Configuraciones	Accesible a configuraciones gracias a su mini pagina web

Tabla 3: Propiedades del router

Suministrada por este router la estructura de la red de la radio es la que se ilustra en la imagen siguiente:

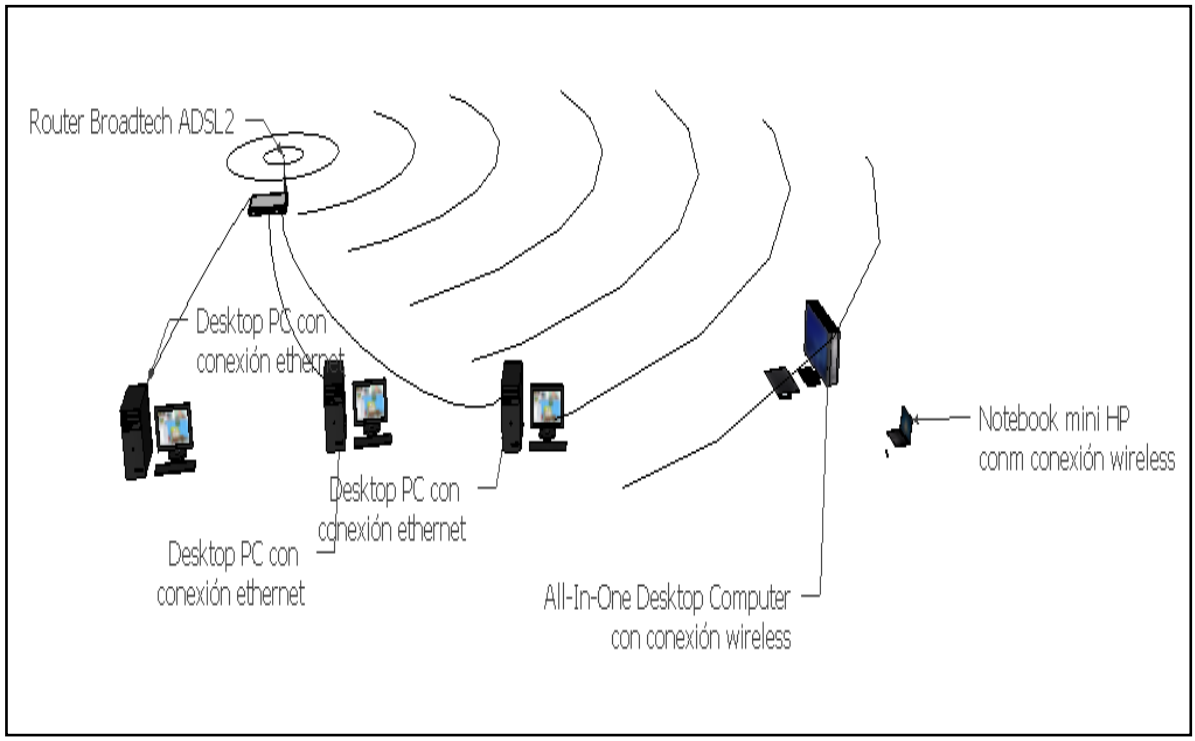

Imagen 4: Estructura de la red actual

Mediante el grafico se puede observar que la red actual presenta una topología en estrella; existe un concentrador central que reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo hacia el nodo central solamente. Esta topología tiene la desventaja de ser vulnerable ante los ataques debido a que por medio del concentrador de nodos se puede tener acceso a cualquier nodo.

A continuación se hace mención de la distribución de los equipos y su medio de conexión:

DISPOSITIVOS	UBICACIÓN
3 PC´S	UBICADOS EN EL ÁREA DE OFICINA (CONECTADOS POR MEDIO DE CABLE ETHERNET)
ROUTER	UBICADO EN EL ÁREA DE OFICINA (ADSL)
2 PC´S	UBICADOS EN LA SALA DE TRANSMISIÓN (CONECTADOS VÍA INALÁMBRICA)

Tabla 4: ubicación y medio de conexión de los equipos

Determinar la ubicación específica de cada uno de los equipos permitió elaborar un plano donde se unifico la estructura de la red y la ubicación de los equipos.

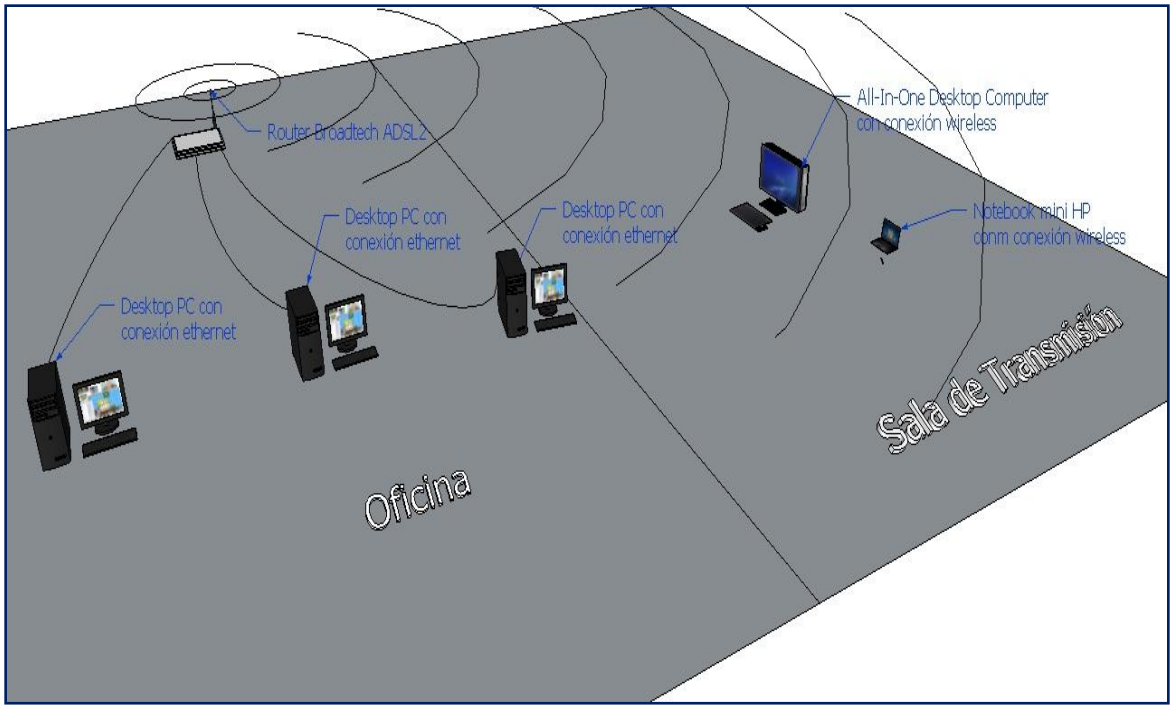

Imagen 6: Distribución de equipos y estructura de la red

1.2.2 Direccionamiento IP

Es provisto por ISP de Claro, al router llegan direcciones IP públicas de salida diversas, esto es, que cada intervalo de tiempo o cada vez que el router sea reiniciado, puede haber cambio en su IP pública, luego desde el router hacia el interior de la red de la radio su direccionamiento es con una IP dinámica, en este caso (192.168.1.0/24), dándose un direccionamiento IP por medio de DHCP (interno en el router) y suministrado de un DNS también en el mismo router. Tenemos también un acceso vía wifi con un área no muy extensa, dotada de una contraseña codificada en WEP.

De acuerdo a estas conexiones, los usuarios tienen acceso sin restricciones a casi todas las páginas web, sin contar con buena seguridad y exponiendo su información a posibles intrusos, también carecen de un sitio web para así darse a conocer además de la vía radial.

Una vez analizada la red de la radio se procedió identificar el sitio hasta donde se ampliara la red, logrando percibir que dicho local posee las dimensiones de 4m x 5m y se encuentra a una distancia 9m con respecto al router. El lugar fue identificado en el plano de las instalaciones.

Imagen 5: Local Hasta donde se Ampliara la Red

Debido a esta distancia del router hacia el lugar donde se requiere ampliar la red, nos dimos cuenta que la señal que llega hasta ahí es muy débil y no se establece una conexión fija en el área, una problemática que debemos resolver, ya que varios de los donantes que llegan a ver el local y se hospedan en las habitaciones llevan con ellos Laptops y necesitan acceso hacia internet.

Con el diagnostico se logro determinar que la radio cuenta con una red plana sin segmentar, que carece de dispositivos de monitorización por lo que no se filtra tráfico de entrada ni salida, quedando expuesta la información interna de la institución la que podría sufrir alteraciones por usuarios remotos, además carece de servidores telemáticos por lo que no tienen una administración de la red, y no cuenta con un portal web. Para que la radio cumpla con su propósito de transmitir vía internet y ampliar sus red para brindarle servicio al centro donde se encuentran ubicados, deberá de reestructurar el diseño de la red con la que cuenta, además será necesario anexar otros equipos en los que se configuraran los servidores telemáticos, en donde se alojará su portal web, debido a esto se elaboro una propuesta del diseño de una red utilizando la arquitectura de una DMZ como seguridad, acompañada de la tecnología de virtualización para reducir costos.

1.3 Diseño de la Propuesta

Después de realizado el diagnostico se procedió a elaborar la propuesta, esta debería de solventar todas las amenazas y vulnerabilidades con los que contaba la radio. Para diseñar la propuesta se partió de cuatro puntos principales.

1- Servidores telemáticos
2- Red segura
3- Portal web
4- Factor económico

Tomando en cuenta los puntos en mención y el propósito de la radio de ampliar la red, se construyo el diseño de la propuesta que se representa a través del

siguiente diagrama. Este dará la pauta a seguir en el cumplimiento con los objetivos del trabajo.

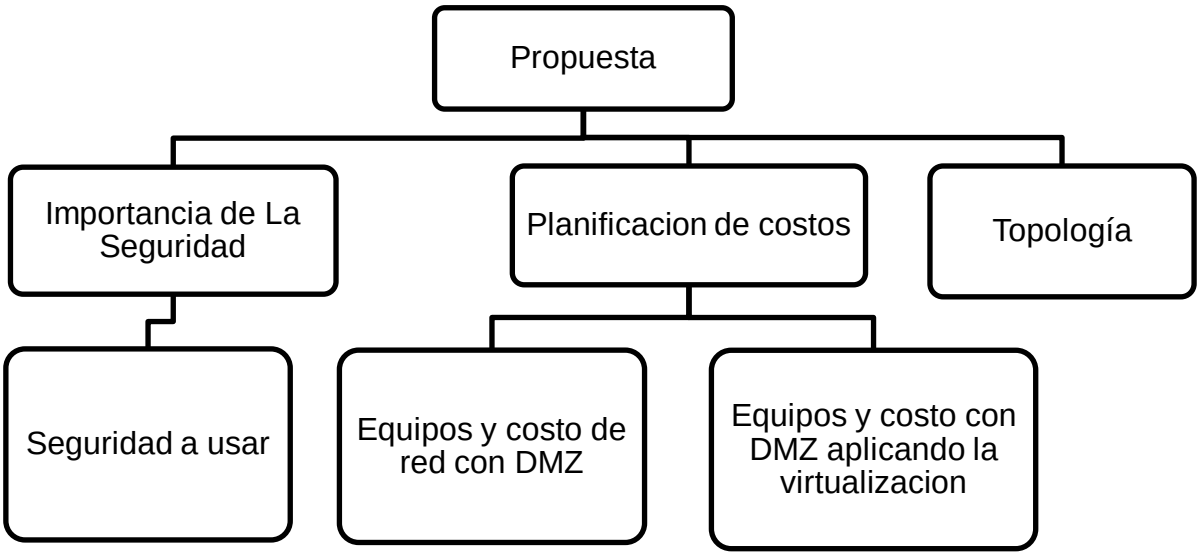

Imagen 6: Esquema de la Propuesta

1.3.1 Importancia de la seguridad en las redes

Continuando, el paso a seguir es explicar el porqué utilizar seguridad en redes, esto para irle dando un poco más de sentido a lo que se pretende con este trabajo.

La seguridad interna de la red es a veces menospreciada por sus administradores. Muy a menudo dicha seguridad incluso no existe, permitiendo a un usuario acceder fácilmente al equipo de otro usuario utilizando debilidades bien conocidas, relaciones de confianza y opciones predeterminadas. La mayor parte de estos ataques necesitan poca o ninguna habilidad, poniendo la integridad de una red en riesgo.

La seguridad de la red es un proceso o acción para prevenir el uso desautorizado de su computadora y no sufrir invasión a la privacidad teniendo en cuenta los peligros que los usuarios pueden tener si no están bien informados. La seguridad de la red es una característica prominente de la red asegurando responsabilidad, confidencialidad, integridad y sobre todo protección contra muchas amenazas externas, etc. La información sobre los diversos tipos de prevención debe de estar actualizados para garantizar su funcionamiento.

Se tiene un concepto erróneo de que la seguridad en redes es solo para las grandes corporaciones donde la integridad y los fondos monetarios están en riesgos, esto porque solo tenemos ideas en grandes hackers y que no le pondrían interés a pequeñas empresas. Se debe tomar muy en cuenta que lo que más motiva a un intruso informático son los retos, ya que trabajan en generar códigos que puedan burlar la seguridad, en su mayoría son jóvenes que quieran probar su nivel de conocimiento en la des-encriptación, sin olvidar a mismos empleados de las pequeñas empresas, y son estos pequeños ataques las amenazas más comunes que podría tener la radio, es por esta razón que este documento se enfoca en el diseño de una red segura.

1.3.2 Tipo de seguridad a usar

Este trabajo se basa en una DMZ (zona desmilitarizada), que es una red local que se ubica entre la red interna de una organización (la radio) y una red externa, generalmente internet, separadas por un Firewall. 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 solo se permitan a la red externa - los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que 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.

Esta zona de 'Buffer' también sirve para brindar servicios al exterior, y asi en el caso de que el intruso logre pasar hasta la DMZ evadiendo el firewall, este quedará atrapado o enjaulado. Los archivos e información importante siempre estarán protegidos con este muro perimetral.

La construcción de esta arquitectura como bien mencionamos se realiza con la obtención de un sistema operativo LINUX con un kernel superior al 2.4.3 y con el agregado de 3 interfaces de red (tarjetas ethernet) al equipo que utilizaremos como firewall.

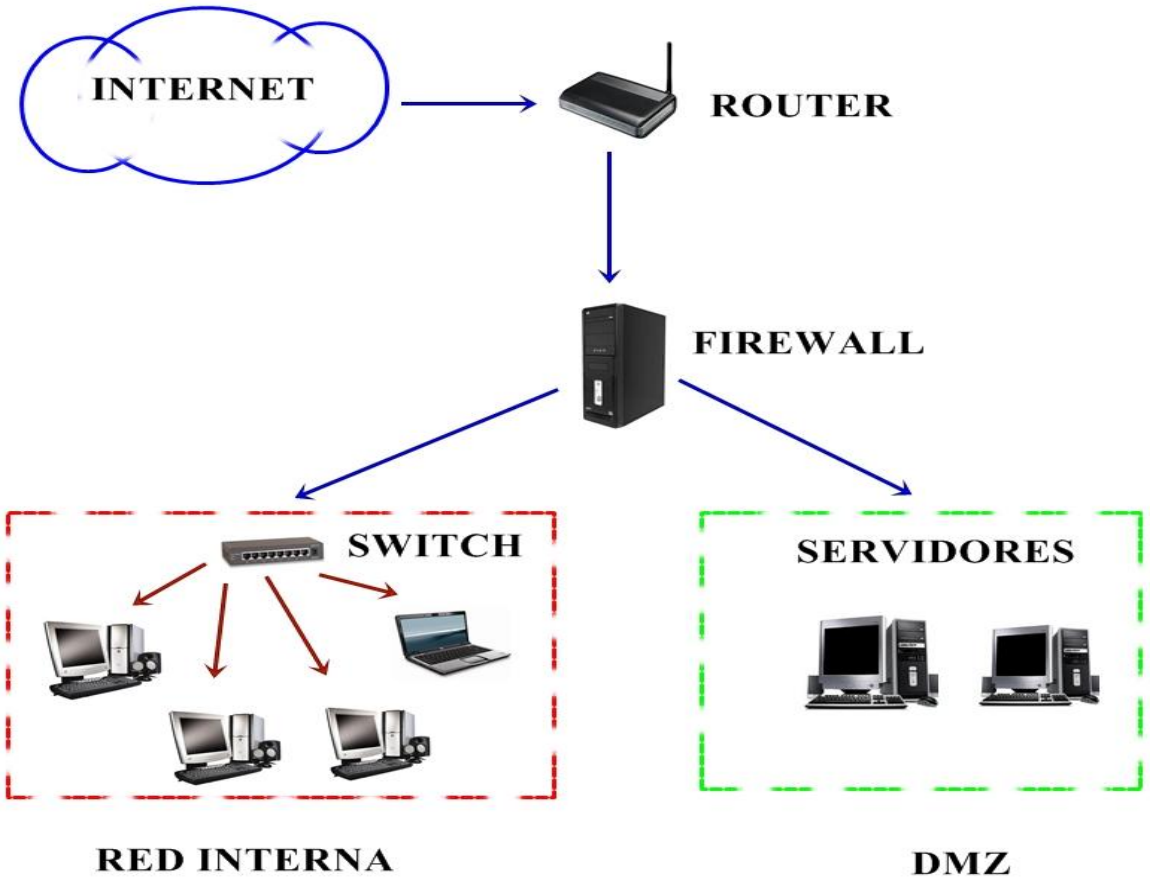

Imagen 7: Estructura de una red que utiliza DMZ

La figura muestra el diagrama de una red típica que usa una dmz con un cortafuego de tres patas que es el que se utilizara en el nuevo diseño de la red. Un cortafuego (Firewall en ingles) es una parte en una red para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas. Esto es lo que se orienta el trabajo, configurar un firewall para crear una DMZ en donde estarán ubicados los servidores de CORREO, FTP, DNS, WEB

Las políticas de accesos en un firewall se deben diseñar poniendo principal atención en sus limitaciones y capacidades, pero también pensando en las amenazas y vulnerabilidades presentes en una red externa. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad, también es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros. El tipo de firewall a usar es de Software, y es utilizado bajo el entorno UNIX/LINUX, con la plataforma Iptables.

1.3.3 Beneficios del firewall con Iptables

Los firewall manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna. También son importantes para llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda.

1.3.4 Políticas de seguridad de Iptables Firewall

Todo Firewall, sea del tipo que sea, se rige por una política de seguridad definida previamente a su configuración. Cuando hablamos de política de seguridad nos referimos a tener una política predeterminada y una colección de acciones a

Realizar en respuesta a tipos de mensajes específicos. Cada paquete se compara, uno a uno, con cada regla de la lista hasta que se encuentra una coincidencia.

Si el paquete no coincide con ninguna regla, fracasa y se aplica la directiva predeterminada al paquete.

Hay dos tipos básicos o políticas de seguridad para un Firewall:

1- Denegar todo de forma predeterminada y permitir que pasen paquetes seleccionados de forma explícita.

2- Aceptar todo de forma predeterminada y denegar que pasen paquetes seleccionados de forma explícita.

La política de denegar todo es la propuesta más segura y por lo tanto con la que vamos a trabajar; pues facilita la configuración de un Firewall seguro pero es necesario habilitar cada servicio sabiendo el protocolo de comunicación para cada servicio que se habilite así como el número de su puerto.

La política de aceptar todo facilita mucho la configuración y la puesta en funcionamiento de un Firewall pero obliga a prever todo tipo de acceso imaginable que se quiera deshabilitar. El peligro es que no se preverá un tipo de acceso peligroso hasta que sea demasiado tarde, o posteriormente habilitará un servicio no seguro sin bloquear primero el acceso externo al mismo. En definitiva, programar un Firewall seguro para aceptar todo, implica más trabajo, mayor dificultad y por tanto es más propenso a errores. Nos disponemos a definir cuál es nuestra política de seguridad y los permisos de entrada o salida de cada una de las subredes de nuestra red.

Se configurara un firewall bajo iptables (de software), estará configurado con la política de denegar todo (DROP), a excepción de aquellos paquetes que tengan una entrada o salida habilitada mediante una o varias reglas.

Es importante que de partida se tenga claro los servicios que van a ser habilitados para cada una de las subredes, de manera que luego creemos las correspondientes reglas y todo lo que no coincida con ello será descartado.

A continuación se muestran la lógica de los servicios y accesos que estarán configurados en el firewall.

El Firewall posee las siguientes interfaces

- Se conecta a Internet mediante una dirección IP estática
- Tiene tres interfaces de red
  - eth0 (IP 192.168.1.4) que da acceso a Internet
  - eth1 (IP 10.10.0.0) que es la puerta de enlace de la red local
  - eth2 (IP 172.16.3.1) que es la puerta de enlace de la DMZ.

1.3.5 ventajas de la DMZ

La DMZ es un método de acuerdo a redes que separa los servidores que a menudo se puede acceder desde el exterior de los equipos que pueden tener almacenado datos confidenciales; debido a esto se puede mencionar como ventas:

- Acceso a los servicios previamente autorizados
- Protege los datos exclusivos de uso interno, al convertirse en un callejón sin salida con los acceso o autorizados.

No olvidemos que la DMZ está acompañada de un firewall que es el que permite el filtrado de el trafico, razón por la cual se pueden mencionar como ventajas de la DMZ.

- Permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados.
- Concentra la seguridad Centraliza los accesos
- Administran los accesos provenientes de Internet hacia la red privada. Sin un firewall , cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Por ello la seguridad en la red privada depende de la "dureza" con que el firewall cuente.
- Administran los accesos provenientes de la red privada hacia el Internet

1.3.6 Desventajas de la DMZ

En este caso debemos de tomar en cuenta que la DMZ en la que se enfoca este trabajo está alojada en un solo equipo esto significa que por estar virtualizado los servidores en un solo host por lo que se podría mencionar como desventajas:

- en dependencia de los requerimientos de la maquinas las Aplicaciones podrían ser más lentas.
- El uso de la virtualización representa conflictos con el licenciamiento que aplican los fabricantes de software. El software de virtualización representa un desafío para los tipos de licencia por usuario existentes actualmente, por lo cual es probable que cambien las reglas respecto al licenciamiento de software. Claro está que su instalación y administración requiere de personal calificado en Tecnologías Informáticas, más su uso puede ser transparente para un usuario promedio corporativo.
- La avería o fallo de un servidor anfitrión de virtualización afecta a todos los servidores virtuales que aloja, por lo que es importante no solo copias de seguridad de las máquinas, sino incluso según lo crítico que sea el proyecto un clusters de servidores anfitriones para evitar te posible fallo.

1.3.7 Servicios accesibles desde la red Externa a la DMZ y viceversa

• Externa → DMZ

Todo cliente podrá ver los servicios que ofrecen la Radio a través de la llamada "zona neutral" en la que se colgarán los servicios WEB, FTP, CORREO Y DNS:

Entonces tenemos que habilitar el tráfico desde cualquiera de las redes externas (0.0.0.0/0) a la red de la DMZ (172.16.3.0/24) para paquetes cuyos protocolos sean HTTP, SMTP, POP3, IMAP, FTP y DNS.

• DMZ → Externa

En sentido inverso se habilitara peticiones y respuesta desde la red externa, esto para que se obtenga una comunicación, y los puertos correspondientes sean accesible desde la red externa.

1.3.8 Servicios accesibles desde la red Interna a la DMZ y viceversa

• Interna → DMZ

En este punto se habilitan los paquetes de la misma manera que en el caso anterior, dando acceso a los servicios que nos ofrece la DMZ (WEB, CORREO, FTP Y DNS).

• DMZ → Interna

Hacemos especial hincapié en que se va a descartar cualquier paquete que vaya en este sentido puesto que no es imprescindible permitir el paso de ningún tipo de tráfico y lo único que provocaría es que existiera un agujero para llegar desde la red externa a la red interna. Además, cabe decir que el sentido de poner en este punto algún servicio es para habilitar única y exclusivamente el acceso a los mismos trabajadores de la radio, de ahí que no tengamos la necesidad de habilitarlos ninguna regla referida al tráfico de entrada de la red interna.

1.3.9 Servicios accesibles desde la red Interna a la Externa y viceversa

• Interna → Externa

Los trabajadores de la red interna podrán tener acceso a los servicios más comunes de (DNS, CORREO, FTP Y WEB), el resto, quedarán cerrados. Con ello nos aseguramos que los programas cuyos protocolos son Peer to Peer, usados muy habitualmente hoy en día, queden deshabilitados; Estas aplicaciones serían un factor añadido de inseguridad que puede ser evitado.

• Externa → Interna

Se va a deshabilitar todo tipo de tráfico porque si no perdería el sentido el colocar una red desmilitarizada que proteja la red interna.

1.4 Diseño de la nueva red

Para el diseño de la nueva red primeramente se tomo en cuenta los equipos con los que cuenta la radio que se reutilizaran, luego con el diagrama que utiliza una red con arquitectura DMZ se identifico los equipos de los que se debe hacer uso para crear la zona de seguridad, y los dispositivos a emplear para que sea posible la ampliación de la red, una vez que se obtuvo toda la información requerida acerca de los equipos con los que se contara, se dará una breve explicación de la función que tendrán los componentes en el nuevo diseño, a elaborar la topología con la que se trabajara en la nueva red, y seguido de los direccionamiento IP que se utilizara.

En vista a los equipos con los que cuenta la radio, el sitio hasta donde se ampliara la red, y considerando la seguridad de la misma se valoro que la topología más recomendable a usar es una topología jerárquica en la que se incluirán nuevos componentes, lo que conlleva a una ampliación de la red.

Los nuevos componentes se describen en la siguiente tabla:

Dispositivos	Características
1PC	PROCESADOR CORE I5 3450 3.1HGz – MEMORIA RAM 8GB DDR3 1333 DISCO DURO 500 GB SATA
1 PC	PROCESADOR PENTIUM 4 – 1GB MEMORIA RAM – 80 GB DISCO DURO IDE
Switch	SWITCH 8 PUERTOS 10/100 SD208 -NA
Cables	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP
Conectores	CONECTORES RJ-45
Linsys	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G - LA

Tabla 5: Dispositivos que se anexaran en la nueva red

En el nuevo diseño se contara con una nueva computadora que nos servirá como Firewall la cual no debe de cumplir con grandes requerimientos en cuanto a procesador, memoria y demás, pero debe de contar con alta fiabilidad en su seguridad. Esta computadora tendrá como sistema operativo Ubuntu Server LTS 10.04 de distribución UNIX/LINUX, contiene un kernel superior al 2.4.3, apto para hacer el uso de IPtables una de las herramientas de cortafuegos populares en lo que respecta a seguridad, permitiendo la creación de la DMZ; la misma herramienta nos permite la utilización de redirecciones utilizando NAT.

Para solventar la necesidad que demanda la radio de incrementar su audiencia y hermanarse con distintos ministerios y/o organizaciones cristianas, se utilizara un computadora que goza de grandes requerimientos en relación a su estructura física, capacidad de memoria, disco duro, procesador; y en todo lo que respecta a alta tecnología; esta computadora posee alto costo pero permite la utilización de la virtualización y de esta forma libraría de la adquisición de otros equipo físicos; ahorrándonos cantidades considerables de dinero. En esta máquina se alojaran los servicios telemáticos DNS, DHCP, FTP, WEB, CORREO; en el que podrán instalar su portal web.

En cuanto a la interconexión de los dispositivos se encuentran los siguientes componentes:

Switch: este elemento es el que permitirá la comunicación entre la red a él se conectaran los host de la red interna y la DMZ, el que su utilizara será uno con capacidad de conexión para 8 equipos, y que puede ser configurable, además a este se conectara la red interna y el Linsys con el cual expandiremos la red.

Cables: es el medio guiado de transmisión que se usara en la red, este será el común par trenzado categoría 5e.

Conectores: estos son las terminales que se ensamblan en la tarjeta de red de cada host, y en los puertos del Switch; serán conectores RJ45, estos también los ensamblaremos en los cables para crear los UTP.

Como anteriormente se menciono la topología a usar es de orden jerárquica como lo muestra la siguiente grafica:

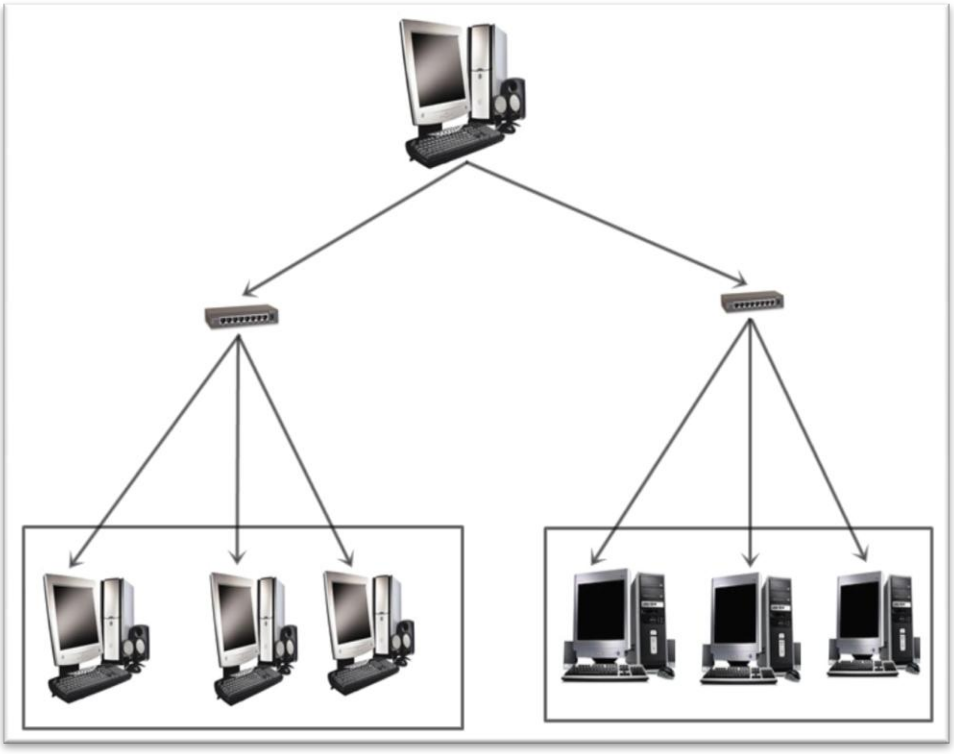

Figura 1: Estructura de La Red de Orden Jerárquica

Como muestra la figura esta topología puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales, que requieren transmitir y recibir de otro nodo sin necesidad de actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

1.4.1 Esquema de direccionamiento.

El esquema de direccionamiento IP y las interfaces de cada una de las maquinas es el siguiente:

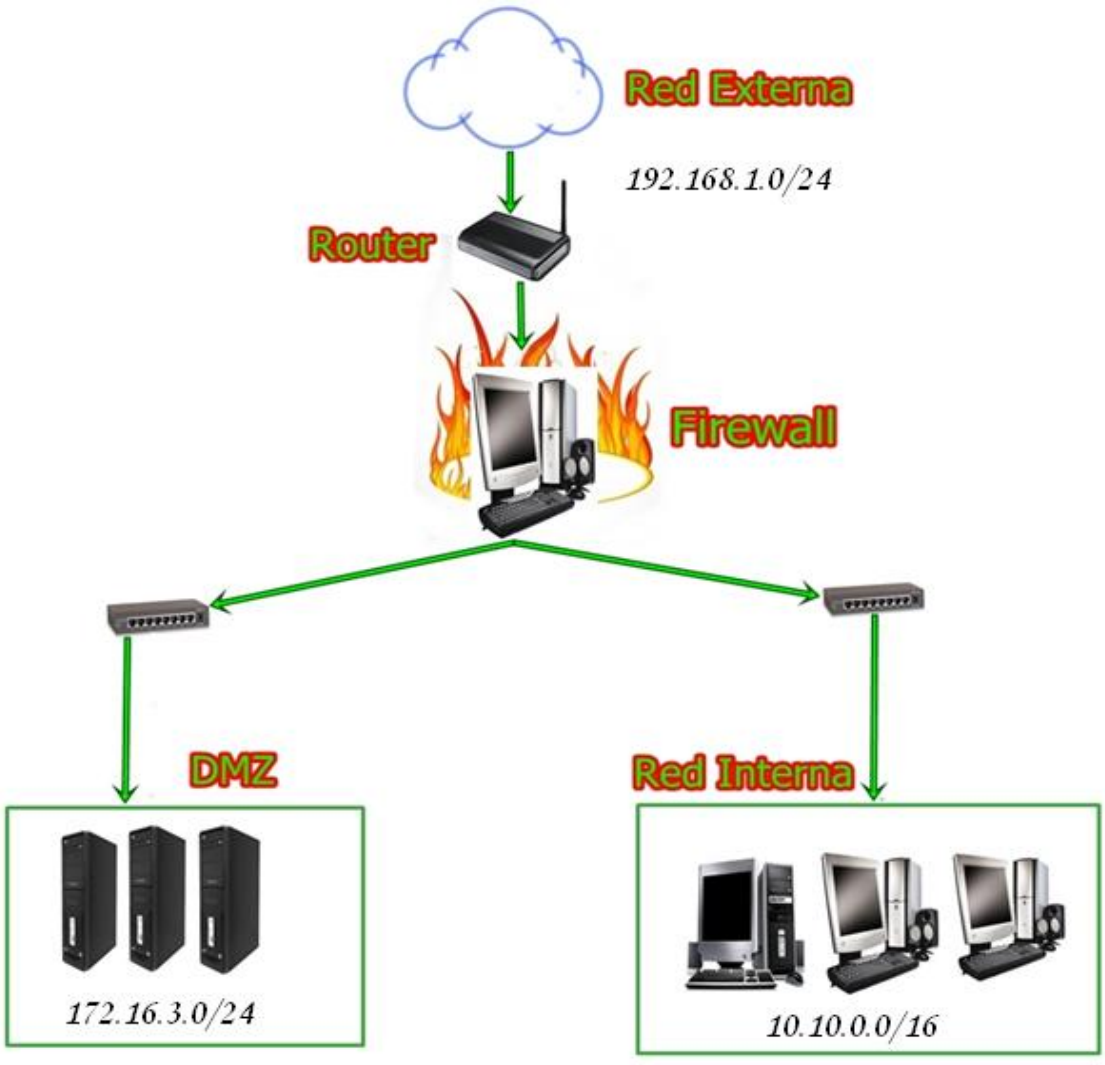

Imagen 8: Esquema de direccionamiento.

1.4.2 Descripción del escenario de trabajo

Como se observa en la ilustración y siguiendo el esquema clásico de una arquitectura perimetral, el escenario está compuesto por direccionamientos IP combinados ya que se utilizan; el direccionamiento que nos otorga el router el cual nos provee una IP publica que variara cada vez que el router sea reiniciado el cual llegara hasta el Firewall luego de pasar por el router nos llegara una ip con numero (192.168.1.0/24), por otra parte es la que nos conectara a la red pública y la misma de donde se conectan los intrusos; a partir de ahí desglosaremos dos subredes, la que va hacia la DMZ (172.16.3.0/24) y la que va hacia la Red interna (10.10.0.0/16) utilizando direcciones IP distintas, creando la DMZ

La red con la que trabajaremos será la 172.16.0.0/24, subneteada en clase C de la siguiente manera:

Ip	Gateway	1ra IP	Ultima IP	Broadcast
172.16.0.0				
172.16.1.0	172.16.1.1	172.16.1.2	172.16.1.254	172.16.1.255
172.16.2.0	172.16.2.1	172.16.2.2	172.16.2.254	172.16.2.255
172.16.3.0	172.16.3.1	172.16.3.2	172.16.3.254	172.16.3.255
. . . .				
172.16.254.0	172.16.254.1	172.16.254.2	172.16.254.254	172.16.254.255

Tabla 6: Tabla de subneteo de la red 172.16.0.0/24

Ip	Gateway	1ra IP	Ultima IP	Broadcast
10.10.0.0	10.10.0.1	10.10.0.2	10.10.0.254	10.10.0.255
10.10.1.0	10.10.1.1	10.10.1.2	10.10.1.254	10.10.1.254
10.10.2.0	10.10.2.1	10.10.2.2	10.10.2.254	10.10.2.255
10.10.3.0	10.10.3.1	10.10.3.2	10.10.3.244	10.10.3.255
....				
10.10.255.0	10.10.255.1	10.10.255.2	10.10.255.254	10.10.255.255

Tabla 7: Tabla de subneteo de la red 10.10.0.0/16

En este diseño se trabajara con las siguientes subredes 10.10.0.0/16 y la 172.16.3.0/24, para la red interna y la DMZ respectivamente.

Red interna (10.10.0.0/16)

Es importante destacar que en esta red se proporciona el servicio DHCP que proviene de la computadora que contiene el FIREWALL. El motivo por el que ubicamos este servidor en este punto es porque lo que se quiere es poder tener un servidor que ofrezca única y exclusivamente IPs a máquinas de la red interna, sin tener la necesidad de que alguien de fuera pueda acceder a este servidor.

Red desmilitarizada o perimetral (172.16.3.0/24)

La DMZ es una zona neutral en la que un cliente podrá acceder a los servicios de la radio sin entrar en la red interna y peligrar su integridad. Además será accesible para los miembros de la radio de la propia red interna; pero en contrapartida desde la red perimetral no se podrá conectar a la red interna ya que podría ser un bug para los atacantes.

En este punto es donde situamos los servicios de la radio que a nosotros en particular nos interesa que sean accesibles desde el exterior, lo que lo diferencia de situarlos en la propia red interna, que únicamente tendrán acceso los trabajadores.

Así pues los servicios que se ofrecen son los siguientes:

La página Web de la Radio, para que cualquier usuario o persona interesada pueda ver las posibilidades que le ofrece la radio.

El servidor de correo. En una institución no todos los trabajadores se ubican siempre en el mismo lugar de trabajo, Por eso, es importante que el trabajador pueda mantenerse al corriente de todo lo sucedido vía mail y así estar en

constante comunicación. Es por eso que el servidor de correo interno se encuentra en esta misma subred, para que pueda ser consultado desde la red externa.

Además, en este punto instalamos el servidor de ficheros FTP para la descarga de ficheros que puedan ser de interés público. Finalmente, otro de los servicios necesarios es el servidor de resolución de nombres DNS, el cual asocia una IP con un nombre de host; Pues es aquí donde le damos un "nombre canónico" al dominio del correo interno y a la página web de la radio.

1.4.2 Servidor Web

La aplicación utilizada para publicar el servidor Web de la radio es el servidor Apache.

El porqué de esta elección se debe a que este servidor es de libre distribución con un uso superior al 50% y ha servido y sigue sirviendo de referencia para muchos de los servidores comerciales que existen actualmente. Siendo un servidor muy completo, no nos hemos dedicado a hacer un estudio profundo sobre sus capacidades, pues tampoco es el objetivo del trabajo, sino que nos hemos limitado a hacer una configuración básica.

Configuración

Para configurar el servicio hemos seguido los siguientes pasos:

Primero nos descargamos el paquete mediante el comando:

sudo apt-get install apache2

A continuación hemos modificado el fichero /var/www/ para escribir lo que queríamos que apareciera en la IP PÚBLICA de nuestro servidor, que se encuentra en la DMZ. Finalmente hemos arrancado el servicio con el comando:

/etc/init.d/apache2 restart

Para comprobar que el proceso se está ejecutando hemos hecho un netstat – ln para ver que el *daemon* de Apache está escuchando por el puerto 80 puerto del servicio Web) para cualquiera de las interfaces.

A continuación hemos accedido al link de nuestra máquina-servidor Web y nos ha aparecido su contenido. Una vez configurado el servidor DNS, la IP para acceder al servidor Web pasa a tener un nombre de host asociado (www.radiofe.com.ni).

1.4.3 Servidor FTP

FTP (File Transfer Protocol) es un protocolo para un servicio de transferencia de ficheros. Se utiliza en modo cliente-servidor: conectados a un ordenador remoto. Según el tipo de conexión que se establezca entre ambos el cliente puede actuar en modo pasivo o modo activo:

Modo Activo

Se establecen dos conexiones distintas. En primer lugar se abre una conexión para la transmisión de comandos (desde cualquier puerto de nuestro ordenador inferior a 1024 hacia el puerto 21 del servidor) y por esa misma conexión, se indica al servidor cual es el puerto (distinto) de nuestro ordenador que está a la escucha de los datos. Entonces, al descargarnos algún archivo es el servidor el que inicia la transmisión de datos, desde su puerto 20 al puerto que le hemos indicado.

Modo Pasivo

La aplicación FTP cliente es la que inicia el modo pasivo, de la misma forma que el modo activo. El cliente FTP indica que desea acceder a los datos en modo pasivo y el servidor proporciona la dirección IP y el puerto aleatorio, sin privilegios (mayor que 1024) en el servidor. Luego, el cliente se conecta al puerto en el servidor y descarga la información requerida.

Firewall en modo activo y pasivo ya que nuestro servidor FTP responderá únicamente a los puertos 20 y 21 y 30000 a 31000, el resto estarán bloqueados.

Configuración

El servidor FTP que vamos a utilizar es vsftpd pues es de los más seguros en cuanto a servidores FTP de GNU/Linux.

El fichero /etc/vsftpd.conf lo hemos configurado como servidor privado, de manera que podrán acceder los usuarios de la red externa y los trabajadores de la empresa con su nombre de usuario.

Para comprobar el funcionamiento del servidor, hacemos un Ftp a 172.16.3.40 (DMZ). Probamos entrando como usuario ya registrado desde una máquina.

Podemos ver que primero debemos autenticarnos con el *login* y *password*. A continuación nos descargamos un archivo. Todo usuario que pueda identificarse podrá descargar cualquier archivo que se le permita en el directorio en el cual está encerrado.

1.4.4 Servidor de Nombres DNS

Todas las máquinas de una red TCP/IP se identifican por una dirección IP de 32 bits. Siendo que es mucho más fácil recordar el nombre de una máquina que recordar una ristra de números configuramos un servidor que asocie una IP con un nombre de máquina. El estándar utilizado en Internet es el DNS (*Domain Name System*).

Tipos de Servidores DNS

Un servidor DNS funciona como una red jerárquica de servidores, dedicados exclusivamente a la traducción de direcciones. Si nos concretamos en la función de un servidor DNS podemos decir que es una base de datos con la lista de nombres e IPs de los *hosts* a los cuales da servicio. Como hemos comentado, la red de servidores DNS es jerárquica, de manera que existen varios tipos de servidores:

• Servidores esclavos: Tienen información de peticiones ya resueltas con lo que son respuestas etiquetadas como “no autorizadas”.

• Servidores master (primarios): Ofrecen respuestas autorizadas porque tienen una copia maestra de los datos de la zona.

• Servidores *forwarding*: Centralizan las peticiones

Configuración

En nuestro caso hemos configurado en la DMZ un servidor master. Para ello nos descargamos el paquete BIND (*Berkeley Internet Name Domain*), que nos proporciona un servidor de nombres llamado *named* y una librería de resolución de DNS.

El fichero de configuración principal del BIND es named.conf. Es aquí donde tenemos que declarar los ficheros de nuestras nuevas zonas.

A continuación creamos los ficheros de zona /var/lib/named/radiofe.zone y 172.16.3.in-addr.arpa.zone que contienen información sobre el espacio de nombre particular. Estos se caracterizan por contener unas directivas y unos registros definidos y explicados en los ficheros correspondientes. Finalmente, una vez configurados los tres ficheros probamos el correcto funcionamiento del servidor. Para ello reiniciamos el *daemon*:

rcnamed restart

Luego, probamos una resolución de nombres con el comando nslookup, de manera que podemos comprobar nuestro servidor DNS asociado a la IP de la máquina y ver que está escuchando por el puerto #53. Por otro lado, como nuestro servidor DNS sólo tiene los dominios del servidor Web, del de correo y del de FTP de la radio, añadimos en el fichero:

/etc/resolv.conf

Una segunda línea con la IP de nuestro servidor DNS (172.16.3.10). Primero se hará la consulta en el servidor DNS local de la DMZ, si el host buscado no consta en éste, se apuntará directamente al puerto #53 del servidor 172.16.3.10 pues dispondrá de más dominios. Éste a su vez apuntará a otros servidores por encima con más información. Pues comprobamos que el servicio DNS es un sistema jerarquizado.

Para comprobar el funcionamiento:

1.4.5 Servidor DHCP

Para que una máquina pueda trabajar en una red TCP/IP necesita como es obvio una dirección IP como mínimo, una máscara y si puede salir de su red, un *Router,* que en nuestro caso será el propio *Firewall*. La asignación manual de estos parámetros puede llegar a ser una tarea pesada y propensa a errores, sobre todo si lo tenemos que hacer para una empresa con un número importante de trabajadores. Además cualquier cambio de direcciones que se tenga que hacer, como por ejemplo pasar de IPs públicas a privadas, o las posibles manipulaciones indeseadas de algunos usuarios provocan una repetición del proceso a grande o pequeña escala. O sea que hacer la asignación de IPs a un número de nodos de manera manual es inviable.

Configuración

Nos lo descargamos mediante la herramienta apt-get. apt-get install dhcp3-server
A continuación modificamos el fichero /etc/dhcp3/dhcpd.conf de configuración desde donde lee el servidor describiendo la dirección de subred (172.16.3.0), la máscara (255.255.255.0), el tiempo máximo (para que el cliente DHCP reciba la IP 7200 s) el rango de IPS a ofrecer (172.16.3.50 – 172.16.3.100) y el servidor DNS

asignado a esta red; el cual será el ubicado en la DMZ de la empresa 172.16.3.10.

Cabe decir, que si tuviésemos más máquinas y fuera de nuestro interés, se podría especificar para una dirección MAC a IP determinada. Una vez escrito el fichero de configuración arrancamos el servicio desde el directorio /etc/init.d en el que se carga de nuevo el sistema.

/etc/init.d/dhcp3-server start

Finalmente para comprobar el buen funcionamiento del servidor, conectamos una máquina a la subred 172.16.3.0 y teniendo la aplicación de dhcp cliente, vemos que dispone de una IP, un *gateway* y un servidor DNS de esa red.

1.4.6 Servidor de Correo

El correo electrónico es un sistema automatizado de entrega de correo convencional, en el que intervienen tres agentes:

• El cliente de correo electrónico (remitente)-MUA (*Mail User Agent*)

• El agente de transporte del correo-MTA (*Mail Transport Agent*)

• El agente de entrega del correo (destinatario)-DA (*Destinator Agent*)

El primero es el que da formato al mensaje, lo dirige y lo entrega al agente del transporte de correo.

El Agente de Transporte o MTA acepta los mensajes de los agentes usuarios (MU) y de otros agentes de transporte. Éste encamina el mensaje por la red adecuada, resuelve los alias y el reenvío.
Finalmente, el Agente DA entrega los mensajes a un destino accesible para el receptor.
Para configurar este servicio utilizamos Postfix como agente de transporte pues es uno de los más utilizado y el que mejor se integra en sistemas UNIX.

Postfixcomo MTA es un daemon del sistema que permite enviar y recibir correo SMTP (*Simple Mail Transfer Protocol*), protocolo de mensajes entre MTA's. Para ello, postfix se queda como proceso residente escuchando el puerto 25, admitiendo y realizando las conexiones SMTP cuando sea necesario.

Configuración

La configuración de postfix es go compleja pero haciéndola funcionar poseeremos un potente agente de transferencia.

Entre los archivos a configurar están
/etc/postfix/main.cf
/etc/postfix/main.cf
/etc/imapd.conf

Por otra parte adjuntaremos un antivirus y un antispam, los archivos de configuración los encontramos en:

/etc/clamd.conf

/etc/amavisd.conf

Por otra parte, en el archivo /etc/aliases definimos el alias para la cuenta de root a donde redireccionar el correo pues no es conveniente estar autenticando la cuenta de root a través de la red para revisar los mensajes originados por el sistema.

1.4.7 Las conexiones a establecerse llevaran el siguiente orden

Proveniente del ISP hacia el router nos llega una dirección IP Publica por medio de la cual tenemos salida hacia Internet, luego el router por medio de NAT nos redirección para lograr la salida, el router nos brinda un direccionamiento IP hacia adentro por medio de DHCP con la red 192.168.1.0/24, haciendo las debidas configuraciones cambiaremos ciertas configuraciones, para mejorar su seguridad y para poner direcciones estáticas por medios guiados (Ethernet).

1.4.8 Conexiones en Router

Por defecto el ROUTER BROADTECH ADSL2+ 8186-V2 proporcionado por la compañía Claro este en su diseño cuenta con cuatro puertos Ethernet de ahí se conectara el firewall, las configuraciones que le aplicamos son las de cambio de seguridad inalámbrica, cambiando la codificación WEP (por defecto de fabrica), por una codificación WPA (un poco mas de seguridad), además cambiaremos el login y contraseña para el acceso al router, esto para dar mas seguridad por si pasan nuestro primer método. Otra cosa que haremos es la apertura de los puertos necesarios para las salidas y respuestas de nuestros debidos servicios.

1.4.9 Conexiones en el Firewall

El firewall estará dotado de 3 interfaces de Red (tarjetas Ethernet) por las cuales se dividirán las subredes.

Eth 0 – aquí se conectara hacia el router para obtener la salida hacia Internet.

Eth1 – Este interfaz se conectara hacia la red interna (172.16.1.1/24).

Eth2 – Este interfaz se conectara hacia la DMZ (172.16.3.1/24).

El Firewall provee servicio DHCP hacia la red Interna.

El Firewall será bajo IPtables.

1.4.10 Switch

Conectada al interface Eth1 del firewall.

1.4.11 Linsys

Conectada al switch para expandirla red hacia la nueva sala de informática, dando acceso a wireless y por medio de cable UTP.

1.4.12 Supercomputadora en DMZ

Conocida como Bastión Host es una PC que estará expuesta, por así decirlo, a ataques provenientes del exterior, pero configurada, testeada y monitoreada para obtener mejor seguridad; conectada al interface Eth2 del firewall, con direccionamiento IP en Clase B.

1.4.13 Ubicación de los equipos en el nuevo diseño de la red.

En el nuevo diseño de la red los equipos se ubicaran de forma similar que en la red original con la salvedad de que los nuevos equipos a utilizar serán colocados en los puntos más óptimos donde se considero que sería más conveniente su administración; lo que si se considero era la localización de los host destinado a servidor, y firewall los que se ubicarían en la única sala climatizada con a que cuenta la radio, conjuntamente a estos equipos se ubicara el router que permite la conexión a internet.

Localización	Equipos
Recepción	1 host para recepcionista
Oficina	3 host para usuarios internos
Sala de transmisión	• 1 Host destinado para servidores • 1 host que funcionara como firewall • 2 host para usuarios internos • Router que permite la conexión a internet • Switch que interconecte a los usuarios internos y a los de la pequeña sala de informática
Sala destinada para informática	• Router Linsys para dar servicio inalámbrico

Tabla 8: Distribución de los Componentes en el nuevo diseño de la red

La tabla anterior describe la ubicación de cada uno de los equipos que componen el diseño de la nueva red, haciendo referencia a los lugares específicos y cantidad de componentes que ahí se ubican.

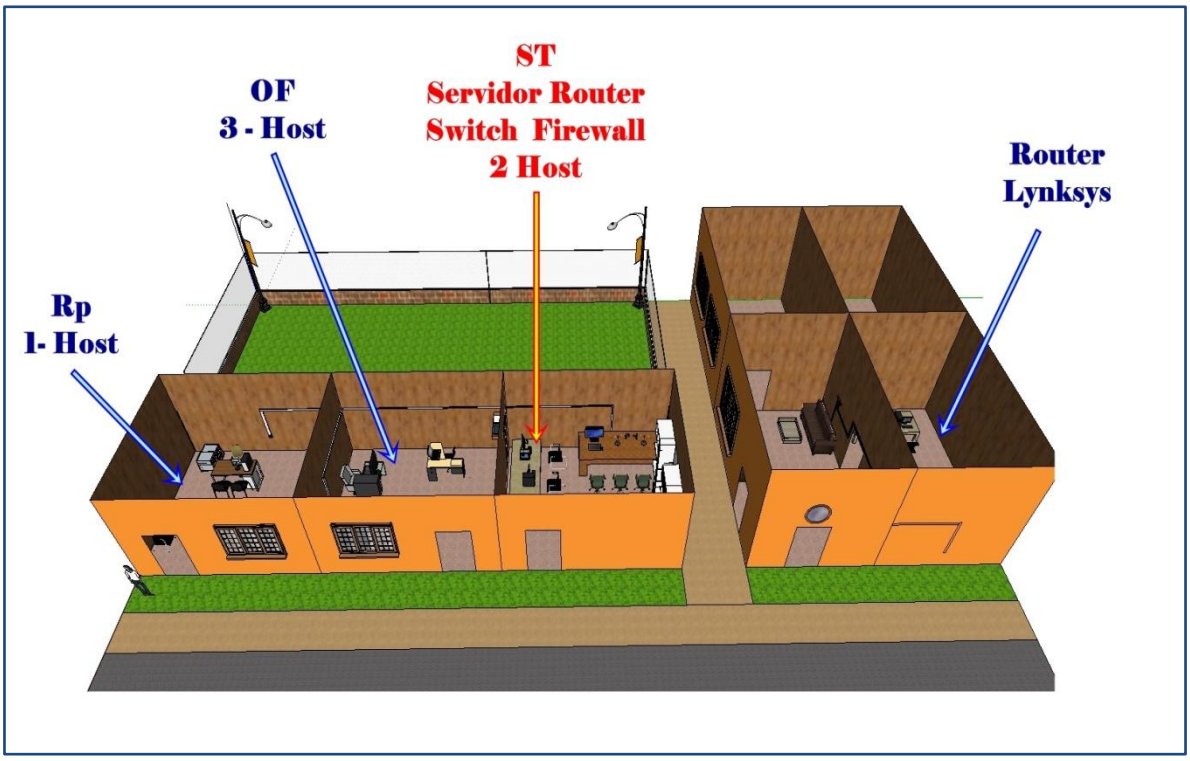

Imagen 9: Caracterización de la ubicación de cada uno de los equipos

Para una mejor comprensión en el plano estructural de la radio se caracterizo las localización de los equipos; los lugares están señalados en azules a excepción de los equipos de mayor importancia que se ubican en la sala de transmisión por ser la sala climatizada; esta identificación en letras rojas flecha amarilla, esto indica que es la sala de mayor importancia; debido a que ahí se encuentra la base fundamental de la red, y se coloco ahí por el simple hecho que es la única sala climatizada; de esta forma se protege el equipo evitando recalentamiento dándole un poco mas de vida útil.

1.5 Diseño del portal web.

Una vez realizado el diseño de la red, y con el objetivo de que la radio tenga la posibilidad de trasmitir en internet; se procedió a la elaboración de un diseño de un portal web; para esto fue necesario reunir toda la información posible sobre creación de sitios web, esto incluye investigación sobre información tanto teórica como técnica, búsqueda de bibliografía y normativa, así como la navegación y los análisis de aquellos sitios referenciales, posibles de ser usados en la elaboración del portal; para llevar se llevar a ejecución este proceso se realizo por etapas.

1- Establecer cuál era la misión y objetivos del sitio

Fue importante establecer cuál era la misión del sitio; por más obvio que pueda parecer es básico establecer cuál es la misión y objetivo del sitio, es muy posible que esto se modifique con el tiempo, pero es importante que se establezca como referencia para el trabajo y las acciones futuras.

2- Determinar la audiencia destinada

Un sitio web debe estar destinado a servir las necesidades del usuario; por lo consiguiente se planteo destinar información compacta, útil, y de interés de la audiencia a la que se dirige y declara el propósito desde un inicio dejando en claro de lo que es el sitio web.

3- Determinar los contenidos.

Se estableció que contenidos presentar en el sitio para cumplir con su misión y satisfacer los requerimientos de la institución y la audiencia. Fue necesario elaborar un pequeño plan de contenidos con información básica a brindar necesariamente en primera instancia lo que se decidió en mutua acuerdo con los miembros de la radio.

4- Determinar la estructura de los contenidos.

Una vez que se determinaron los contenidos se organizo la información, y se dividió en aéreas; se construyo una estructura jerárquica con el fin de establecer niveles y relaciones lo que permitirá al usuario recorrer el sitio haciendo predicciones exitosas de donde encontrar las cosas. Como las páginas web giran en torno a su página principal de acceso, esta debería cumplir funciones claves como plasmar el propósito principal del sitio, puesto a que es la puerta de entrada a toda la estructura desarrollada, de igual forma tendría que prever las necesidades del usuario y velar porque estos encuentren la información que necesiten con el mínimo esfuerzo.

5- Identidad visual.

Se planteo que debería mantener una imagen homogénea para que el sitio tuviera una identidad visual que permitiera asociarlo e identificarlo, con la utilización de logotipos, iconos y links en el mismo lugar

Etapas de evaluación para el sitio web	Planteamientos a cumplir
Misión y Objetivos Del Sitio	Transmisiones radiales de carácter Cristino
Audiencia Destinada	Público en general, niños jóvenes y adultos
Contenidos.	Información de la radio y del centro e restauración general, música y espacio de chat
Estructura De Los Contenidos.	De orden jerárquica
Identidad Visual.	utilización de misma plantilla en la que este insertada el logotipo y los acceso a la información

Tabla 9: Disposiciones por las que debe regirse el portal web

La tabla anterior muestra las disposiciones por el que debe regirse el diseño del portal web. Esta información guiara en la elaboración del esquema de presentación de la plantilla de presentación del sitio web, el debería cumplir con el propósito de la radio.

En primera instancia el esquema debería de tener bien definidas las zonas de navegación, y la de información; además de la identificación del portal que sería la imagen de reconocimiento de la radio. Esta miso esquema es del que regirían todas y cada una de las páginas del sitio la que debería ser estandarizada para facilitar la arte del diseño. Considerando todas estas normativas se elaboro el siguiente esquema que muestra la estructura de las páginas del portal.

<table>
<tr><td colspan="6"></td></tr>
<tr><td colspan="6">TITULO PRINCIPAL</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>LINK</td><td>LINK</td><td>LINK</td><td>LINK</td><td>LINK</td><td>LINK</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td rowspan="2">SLOGAN</td><td colspan="3">TITULO</td><td rowspan="2">IMAGEN</td></tr>
<tr><td colspan="3">INFORMACIÓN</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>IMÁGENES</td><td colspan="2">TRANSMISIÓN</td><td colspan="2">INTERACCIÓN DE LOS USUARIOS</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td>ADICIONAL</td><td>LINK</td><td>LINK</td><td>LINK</td></tr>
</table>

Tabla 10: Estructura de las páginas del sitio web

En el esquema anterior se muestra las estructura caracterizada que tendrán las páginas del portal; mediante el cual se puede observar que es un diseño sencillo pero que cumple con las disposiciones a las que se llegaron en la evaluación de cómo deberían de estar compuesta las páginas de la web. Como se aprecia en el grafico cada página permitirá la fácil navegación hacia las demás páginas todo esto sin perder la identidad de la radio que estar presente en todo momento.

Una vez obtenida la información, después de echa la evaluación previa de los parámetros que se establecerán en el portal y de la elaboración del esquema que tendrán las pagina; se procedió a realizar diagnostico en el que se tomo muy en cuenta el diseño de la red propuesta y el propósito principal de la web que es de transmisiones radiales, y de la posibilidad de interacción de los usuarios cabe destacar que para lograr esto es necesario tener distintos servidores adicionales a los que se encuentran en la DMZ del diseño de la red, como base fundamental para las transmisiones radiales se requiere de un servidor que permita tal trabajo y distintos programas destinados a los fines radiales que se necesitan que trabajen en conjunto; configurarlos y almacenar la información a distribuir demandaría gran espacio de memoria además al momento de transmitir necesitaría un mayor ancho de banda que generaría un poco mas de gastos a la radio.

Considerando que es una radio creciente y que no cuenta con la tecnología necesaria ni con los recursos para la adquisición de distintos servidores; y en vista a la problemática que se enfrentaba (carencia de servidores para la transmisiones radiales), se hizo necesario buscar la forma de solventar esta necesidad, lo que encamino a la investigación de los distintos sitios web que ofrecieran el servicio de forma gratuita encontrándonos con www.ustream.com que es un portal que ofrece la transmisión en vivo de audio y video de forma gratuita; esta es una página en donde se pueden tener canales alternos sin necesidad de tener equipos tan sofisticado y caros que requerirían las estaciones físicas; el único requisito que solicitaba era la afiliación al sitio.

Con la intención de minimizar los gastos en la adquisición de equipos, la optimización de los equipos dentro del diseño de la red, y la elaboración de la pagina web con interacción de los visitantes, lo que se pretendía era minimizar el consumo de memoria y hacer uso de los distintos sitios web que nos brindaran servicios de manera gratuita; debido a esto se abrieron cuentas en distintos portales; el único inconveniente es que se tendría que mantener abierta las cuentas a la misma vez pero eso se puede trabajar en distintas maquinas dentro de la radio lo que reduce el congestionamiento en la memoria al tenerlas abierta en una sola maquina

PORTAL	SERVICIO
USTREAM	Ofreces la opción de transmisión de audio y video, el que puede ser administrado por los afiliados
MIXPOD	Facilita la creación de reproductores de videos el que puede ser anexado al portal web
CBOX	Permite la creación de salas de chat, con monitorización de estadísticas de visitas de la sala.

Tabla 11: Nombre de los portales

La tabla anterior muestra los portales a los que tuvo que afiliar; en la tabla se observa el nombre y los servicios que ofrecen, que son de gran ayuda para la elaboración del sitio web de la radio

Después de realizada las afiliaciones se procedió a la extracción de los códigos fuentes de cada uno de los espacios creados para luego anexarlos al portal web que se diseñara

Puesto que se carecía de conocimientos de programación en código HTML que es el utilizado en el diseño de página web; se recurrió a distintos programas de diseño que facilitaron en gran manera el trabajo. El nombre de los programas y su función se encuentran en la tabla que se muestra a continuación:

Programa	Función
Dreamweaver	Diseño de pagina web
photoscape	Diseño de banner fotográficos
Photoshop	Diseño de banner fotográficos

Tabla 12: Programas Usados En El Diseño Del Sitio Web

Dreamweaver es un programa para diseño y programación web, básicamente para hacer o modificar páginas de Internet. Para utilizarlo necesitas al mínimo conocimiento de lenguaje HTML o PHP, estos son códigos o lenguajes que se utilizan para desarrollar sitios web. El programa es realmente muy completo y sus nuevas versiones son cada vez más sencillas, aunque siempre necesitarás conocer algo del tema para poder utilizarlo.

Se escogió este programa para el diseño del sitio por su facilidad de uso y las distintas aplicaciones con las que trabaja de manera grafica; permitiendo la visualización de la pagina en casi todos los navegadores. Utiliza la tecnología web como CSS y Java Script además de que se puede diseñar y crear sin conocimientos de los códigos HTML permitiendo la extensiones HTML y java Script; los archivos del programa son rutinas de Javascript y hace que sea un programa fluido y está disponible para las MAC, Windows y también puede ser

ejecutado en otras plataformas y lo más interesante es que permite ver los cambios que efectuamos a la vez que se realizan.

Siguiendo las normativas y las disposiciones que se acordaron se elaboro el sitio web que lleva por título Radio Fe. El portal esta creado bajo una plantilla sencilla basada en tablas, con su debida tabulación; contiene los botones tradicionales de un portal en el que figuran:

Inicio, quienes somos, misión, visión, galería, cada uno de estos con su debido link; el cual conlleva a la apertura de nuevas páginas; además cuenta con otras opciones a las que el visitante puede ingresar; tal es el caso de el listado de la programación de la radio, la historia, un espacio donde se reproducen un listado de temas musicales, y el espacio de eventos; de igual forma cuenta con el área de transmisión en línea de la radio; cabe destacar que está dotado para la transmisión de audio y video si hacia lo desease la radio.

La pagina principal es la imagen de la radio; quedo estructurada de forma de que el visitante pueda navegar en el sitio de manera simple, y en el que se dé cuenta o deduzca de la información que encontrara al hacer click en cualquiera de los link para ingresar a las distintas paginas.

En la imagen que se mostrara se puede observa que la plantilla cumple con el esquema en donde se muestra la estructura en cumplimiento con las disposiciones, se observan definidas cada una de las áreas que contiene para una mayor comprensión estas fueron señaladas de modo que se identifique de la mejor manera.

Imagen 10: Pagina Principal del Portal Web de Radio Fe

1.6 Planificación de costos

Por lo que respecta al análisis de costo previsto en esta propuesta adjuntamos tablas en las que se refleja una comparación de equipos y costos al diseñar la red con DMZ utilizando servidores individuales y con DMZ aplicando la virtualización en un solo host. Estos se hizo para una mejor apreciación de porque utilizar la virtualización; se obtendría el mismo funcionamiento a un bajo costo.

1.6.1 Costos al diseñar la red con DMZ utilizando servidores individuales

Para esta valoración hizo una cotización de precios por unidad de los equipos que se deberán comprar, una vez obtenidas las proformas con precios unitarios de distintas casas comerciales; se efectuó balance para sacar los pecios promedios y de esta forma elaborar una tabla donde se plasmara el exacta de equipos con su respectivos costos que arrojaría un promedio del costo total del proyecto. Esto nos permitirá hacer una comparación para demostrar el por qué la utilización de la virtualización.

CANTIDAD	EQUIPOS		PRECIO PROMEDIO
1	SERVIDOR HP PROLIANT ML 150 G6 E5504- 2.0GHZ/2GB/SAS/HOT –SWAP 3.5””/466132-001	$	1,655.33
1	SWITCH CISCO 8 PUERTOS 10/100 SD208 -NA	$	31.44
1	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G - LA	$	89.61
1	UPS TRIPP LITE SMARTOLINE SU2200XLA-110/22OV 7OUT – SU 2200XLA	$	814.45
1	CONECTORES RJ-45	$	0.13
1m	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP	$	0.59

Tabla 13: Precio unitario de los equipos

La tabla anterior muestra los precios promedio de los equipos; estos fueron dejados en dólares para evitar un la variación que tendrían al sufrir un alza el valor del dólar. Obtenido estos precios se procedió a realizar la valoración global de equipos y costos para aproximarnos al valor real de los mismos.

CANTIDAD	EQUIPOS	PRECIÓ UNITARIO	PRECIO TOTAL
4	SERVIDOR HP PROLIANT ML 150 G6 E5504- 2.0GHZ/2GB/SAS/HOT –SWAP 3.5””/466132-001	$ 1,655.33	6621.32
2	SWITCH CISCO 8 PUERTOS 10/100 SD208 - NA	$ 31.44	62.88
1	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G - LA	$ 89.61	89.61
1	UPS TRIPP LITE SMARTOLINE SU2200XLA-110/22OV 7OUT – SU 2200XLA	$ 814.45	814.45
18	CONECTORES RJ-45	$ 0.13	2.394
60	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP	$ 0.59	35.4
1	CABLE RCA CERTIFICADO	$ 7	7
		SUBTOTAL	$ 7633.05
		IVA	$ 1144.581
		TOTAL	$ 8,778.0081

Imagen 11: Tabla de Costo con Servidores Físicos

En la tabla anterior se puntualiza el costo que al que tendría el diseño de la red con servidores físicos; este fue calculado con los precios promedios lo que se acerca al valor real, que podría variar en dependencia de la casa comercial en la que se vallan adquirir los equipos.

1.6.2 Costos al diseñar la red con DMZ utilizando servidores virtualizados.

Con la tecnología de virtualización se disminuyen los costos, debido a que los equipos a usar se disminuirían en gran medida, debido a que los servicios son instalados en un mismo equipo y por ende la cantidad de cable UTP el numero de conectores RJ-45, tendrían una reducción en cuanto a cantidad.

CANTIDAD	EQUIPOS	PRECIO UNITARIO	PRECIO TOTAL
2		$ 641.00	$ 1282
1	SWITCH CISCO 8 PUERTOS 10/100 SD208 – NA	$ 31.44	$ 31.44
1	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G – LA	$ 89.61	$ 89.61
1	UPS TRIPP LITE SMARTOLINE SU2200XLA-110/22OV 7OUT – SU 2200XLA	$ 814.45	$ 814.45
10	CONECTORES RJ-45	$ 0.13	$ 1.3
40	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP	$ 0.59	$ 23.06
1	CABLE RCA CERTIFICADO	$ 7	$ 7
		SUBTOTAL	$ 2284
		IVA	$ 337.27
		TOTAL	$ 2624.24

Imagen 12: tabla de costos con servidores virtualizados

1.6.3 Comparación de costos.

Después de sacar los gastos se procedió a realizar una comparación de costos para obtener asi la diferencia lo que el resultado sería la cantidad que se ahorraría al aplicar la tecnología de virtualización.

SERVIDORES FÍSICOS	SERVIDORES VIRTUALIZADOS	DIFERENCIA
$ 8,778.0081	$ 2624.24	$ 6143.75

Una vez hecha la comparación se evidencia que el consumo se reduce $6143.75 lo que equivale a 69%. Con lo que se puede afirmar que utilizando virtualización se logra un el ismos funcionamiento a bajo precio.

2 CONCLUSIONES

La mayoría de las empresas sufren la problemática de seguridad debido a sus necesidades de acceso y conectividad con:

- Internet.
- Conectividad mundial.
- Red corporativa.

Un alto porcentaje de la información sensible de una empresa se encuentra viajando diariamente sobre su red informática, es por ello que asegurar dichas redes es un tema crítico para el óptimo funcionamiento de una institución.

Es necesario poder garantizar que los recursos informáticos de una empresa, estén disponibles para poder cumplir sus propósitos; esto se logra mediante procedimientos de seguridad que se deben de implementar internamente en cada empresa.

Existen gran cantidad de métodos para asegurar una red informática dentro de una empresa. Uno de los que se usa con más frecuencia, por su alto desempeño y por su factibilidad de acoplarse con la mayoría de las redes, es el aseguramiento mediante redes desmilitarizadas (DMZ).

Radio fe no es la excepción; en la actualidad la radio cuenta con una red punto a punto vulnerable a cualquier tipo ataque y al querer transmitir por internet pondría en riesgo su integridad que la caracteriza como la radio cristiana que hasta el momento ha mantenido.

En vista que la radio carece de una red que se oponga a los accesos no autorizados, y su información puede ser manipulada desde el exterior; se considero la posibilidad de diseñar una red que cumpla con los estándares de una

red desmilitarizada y así se lograría brindar algunos servicios a la red externa; de igual forma actuaria como filtro protector para la red interna protegiéndola de intrusiones maliciosas que puedan comprometer la seguridad de la radio.

El diseño de la red que en este documentos se planteo se basa en una DMZ la que se crea mediante la utilización de un firewall de software debido a que proporcionara la mayoría de las herramientas para complementar la seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red interna y hacia la red externa, es importante establecer que un monitoreo constante de el registro base, nos permitirá detectar un posible intruso y así proteger la información. cabe destacar que este trabajara bajo la plataforma de LINUX, configurado bajo la política de denegar todo.

Además de proponer un nievo diseño de la red se propone la utilización de la virtualización lo que permitirá aprovechar los recursos con los que se cuenta, una administración simplificada y un ahorro energético, dando como resultado una reducción de costo al momento de la implementación de la propuesta. otro aspecto fundamental que se presenta en este documento es el diseño de un portal web el cual se facilita la posibilidad de transmisión de audio y video, siendo este el factor fundamental, puesto que será el punto de partida a futuros hermanamientos con otros ministerios cristianos y el crecimiento del centro donde se encuentra alojada la radio.

3. Bibliografía

1. Dominguez, A., Fuentes, F., Lopez, E. M., & Patrice, H. (1999). *Brandel D. y Napier R., "Linux 6ª Edición.* Madrid.
2. Ferrer Berbegal, M. (2006). *Firewalls software: Estudio, instalación, configuración de esenarios y corporativa.* Catalunya.
3. MORALES RABANALES, H. R. (Mayo de 2009). DISEÑO DE ASEGURAMIENTO DE REDES UTILIZANDO DMZ´S. *SEG ENREDES1* . Guatemala, Guatemala.
4. Robertson, P. D., Matt, C., & Ranum, M. J. (26 de 07 de 2004). *Firewalls de Internet: Preguntas mas Frecuentes.* Recuperado el 4 de 11 de 2012, de http://www.interhack.net/pubs/fwfaq/firewalls-faq.html#SECTION00010000000000000000
5. Sallings, W. (1997). *Comunicaciones y redes de Computadoras 5ª ed.* Prentice - Hall.
6. Wes, S., & Yates, T. (2000). *Building Linux and OpenBSD firewalls.*
7. World, S. (2007). *Server World*. Recuperado el 30 de 10 de 2012, de http://www.server-world.info/en/note?os=SUSE_Linux_Enterprise_Server_11&p=mail

ANEXOS

4.1 Configuración para Servidor DNS (Suse Linux Enterprise Server 11 sp1)

Previo a la instalación del servidor realizamos los debidos ajustes al sistema.

Configuraciones de IP Estática

hostname serverdns address 172.16.3.10

netmask 255.255.255.0
gateway 172.16.3.1
broadcast 172.16.3.255
dns-nameservers 172.16.3.10
dns-search radiofe.com.ni

Luego instalamos Bind, necesario para el servidor.

zypper in bind

Configuración del archivo (resolv.conf), aquí editamos el search, dominio e IP.

vi /etc/resolv.conf

search radiofe.com.ni
domain radiofe.com.ni
nameserver 172.16.3.10

Configuración para las Zonas (named.conf), en este espacio vamos a agregar las zonas que utilizaremos para resolver los nombres, los nombres que se asignan son los de la radio y la ip que utilizara.

vi /etc/named.conf

```
zone "." in {

        type hint;
        file "root.hint";
};
zone "localhost" in {
        type master;
        file "localhost.zone";
};
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};
zone "radiofe.com.ni" in {
        type master;
        file "radiofe.zone";
        allow-transfer { any; };
};
zone "3.16.172.in-addr.arpa" in {
        type master;
        file "172.16.3.zone";
        allow-transfer { any; };
};
```

Configuración de los archivos de zona en el directorio /var/lib/named/

En este apartado configuraremos la resolución de nombres para las zonas directa e inversa, según los servicios que daremos y nuestro dominio quedaran preparados.

Zona Directa

vi /var/lib/named/radiofe.zone

```
$TTL 1w
radiofe.com.ni.     IN SOA          serverdns     root.radiofe.com.ni. (
                                1601201316 ; serial
                                2d         ; refresh
                                4h         ; retry
                                6w         ; expiry
                                1w )       ; minimum

                    IN NS       serverdns
                    IN MX       10 servermail
serverdns           IN A        172.16.3.10
serverweb           IN A        172.16.3.20
servermail          IN A        172.16.3.30
serverftp           IN A        172.16.3.40
www                 IN CNAME    serverweb
ftp                 IN CNAME    serverftp
```

Zona Inversa

vi /var/lib/named/172.16.3.zone

```
$TTL 1w

@       IN SOA      serverdns.  root.radiofe.com.ni. (
                    1601201316 ; serial
                    2d         ; refresh
                    4h         ; retry
                    6w         ; expiry
                    1w )       ; minimum

        IN NS       serverdns.radiofe.com.ni.

10      IN PTR      serverdns.radiofe.com.ni.
20      IN PTR      serverweb.radiofe.com.ni.
30      IN PTR      servermail.radiofe.com.ni.
40      IN PTR      serverftp.radiofe.com.ni.
```

Con los siguientes comandos reiniciamos el servidor y luego lo activamos para que corra desde el inicio.

rcname restart

chkconfig named on

4.2 Configuraciones de un servidor DHCP (Ubuntu server LTS 10.04 LTS)

Previo a la instalación del servidor realizamos los debidos ajustes al sistema. Debido a que el servidor DHCP se encuentra en el firewall tuvimos que configurar 3 interfaces, pero aquí solo tenemos la de la interface eth1 (red Interna) y eth2 (dmz).

gedit /etc/network/interfaces

configuraciones de IP Estática

auto eth1
iface eth1 inet static
address 10.10.0.1
netmask 255.255.0.0

auto eth2
iface eth2 inet static
address 172.16.3.1
netmask 255.255.255.0

Luego realizamos las debidas configuraciones para tener el sistema operando a su mejor seguridad y actualizaciones.

sudo apt-get update
sudo apt-get upgrade

Con el siguiente comando instalamos nuestro servidor DHCP

sudo apt-get install dhcp3-server

Nos dirigimos al archivo /etc/dhcp3/dhcpd.conf donde se encuentra su configuración y lo editamos de la siguiente manera:

gedit /etc/dhcp3/dhcpd.conf

y editamos a nuestra conveniencia:

```
# A slightly different configuration for an internal subnet.
subnet 10.10.0.0 netmask 255.255.0.0 {
range 10.10.0.50 10.10.0.100;
option domain-name-servers 172.16.3.10, 192.168.1.1;
option domain-name "radiofe.com.ni";
option routers 10.10.0.1;
option broadcast-address 10.10.0.255;
default-lease-time 600;
max-lease-time 7200;
interfaces=eth1;
}

subnet 172.16.3.0 netmask 255.255.255.0 {
range 172.16.3.50 172.16.3.100;
option domain-name-servers 172.16.3.10;
option domain-name "radiofe.com.ni";
option routers 172.16.3.1;
option broadcast-address 172.16.3.255;
default-lease-time 600;
max-lease-time 7200;
interfaces=eth2;
}
```

Una vez terminado, solo tenemos que guardar y reiniciar nuestro servidor DHCP, con la siguiente orden:

Service dhcp3-server restart

Y lo activamos desde el arranque del sistema con el comando

Chkconfig dhcp3-server on

3.3 Configuraciones para el servidor FTP (Configuraciones en Ubuntu server 10.04 LTS)

Previo a la instalación del servidor realizamos los debidos ajustes al sistema.

gedit /etc/network/interfaces

hostname serverftp

auto eth0

iface eth0 inet static

address 172.16.3.40

netmask 255.255.255.0

network 172.16.3.0

gateway 172.16.3.1

broadcast 172.16.3.255

dns-nameservers 172.16.3.10

dns-search radiofe.com.ni

Luego realizamos las debidas configuraciones para tener el sistema operando a su mejor seguridad y actualización.

sudo apt-get update

sudo apt-get upgrade

Antes de instalar el servidor ftp vamos a crear los usuarios y asegurarnos que tengan los mínimos permisos y sólo puedan hacer lo que nosotros definamos.

Crearemos un grupo llamado ftp al cual asociaremos los usuarios.

groupadd ftp

Creamos los usuarios con sus correspondientes características.

useradd -g ftp -d /home/987 -c "987 " 987
useradd -g ftp -d /home/radiofe -c " radiofe " radiofe

Les asignamos un password a los usuarios con el comando passwd.

Ahora creamos una shell fantasma en el siguiente directorio

mkdir /bin/ftp

Editamos el fichero /etc/shells y la añadimos en la última línea y continuación editamos el fichero /etc/passwd y buscamos las líneas donde están definidos los usuarios que hemos creado antes y les añadimos el shell falso:

987:x:1005:1005: 987 :/home/987/dominio1:/bin/ftp
radiofe:x:1007:1005: radiofe :/home/radiofe:/bin/ftp

Para instalar el servidor FTP, se paso a su descarga

Sudo apt-get install vsftpd

luego pasamos a su archivo de configuración

gedit /etc/vsftpd.conf

Las configuraciones realizadas fueron las siguientes, agregando o editando ciertas configuraciones para el correcto uso.

```
# Exampleconfig file /etc/vsftpd.conf
listen=YES
#No permitimos usuarios anonimos
anonymous_enable=NO
# Permite que usuarios locales puedan conectarse
local_enable=YES
# Se permite el modo escritura
write_enable=YES
# Agregamos la máscara al FTP
local_umask=003
# Activar mensajes de directorio
dirmessage_enable=YES
#usarreloj Local
use_localtime=YES
#Activar subidas y descargas
xferlog_enable=YES
# Conectar por el puerto  20 (ftp-data).
connect_from_port_20=YES
# Mensaje de Bienvenida
ftpd_banner=Bienvenido a RadioFe transferencia.
#Habilitamos FTP en modo pasivo y establecemos un rango de puertos TCP 30000 - 31000 para las conexiones.
port_enable=YES
pasv_min_port=30000
pasv_max_port=31000
# Enjaula a los usuarios locales dentro de su propio directorio personal, esta opción mejora la seguridad.
chroot_local_user=YES
chroot_list_enable=YES
# Directorio de cada usuario (por defecto)
chroot_list_file=/etc/vsftpd.chroot_list
```

Debiancustomization

#Activamos nuevo directorio para usuarios

userlist_enable=YES

tcp_wrappers=YES

userlist_deny=NO

A continuación creamos el fichero vsftpd.chroot_list el cual tendrá la lista de usuarios que no tendrán acceso al servidor:

touch /etc/vsftpd.chroot_list

Volcamos los datos a este fichero desde etc/password con el comando.

cat /etc/passwd | awk -F: '{ print $1 }' > /etc/vsftpd.chroot_list

Esto nos genera un fichero con los login de usuarios del sistema del cual quitamos los que si queremos que tengan acceso y los ponemos en el fichero /etc/vsftpd.user_list.

Luego pasamos a reiniciar el servidor y a ponerlo activo desde el arranque.

4.4 Configuraciones para un servidor LAMP (Ubuntu server 10.04 LTS)

Previo a la instalación del servidor realizamos los debidos ajustes al sistema.

Creación de un usuario, además del usuario root para realizar las configuraciones.

gedit /etc/network/interfaces

Configuraciones de IP Estática

hostname serverweb

auto eth0

iface eth0 inet static

address 172.16.3.20

netmask 255.255.255.0

network 172.16.3.0

gateway 172.16.3.1

broadcast 172.16.3.255

dns-nameservers 172.16.3.10

dns-search radiofe.com.ni

Luego realizamos las debidas configuraciones para tener el sistema operando a su mejor seguridad.

sudo apt-get update

sudo apt-get upgrade

Instalamos el servidor con el siguiente comando:

sudo apt-get install mysql-server-5.1 apache2 php5 php5-mysql libapache2-mod-auth-mysql

El directorio donde se almacenan los documentos web esta en: /var/www

Reiniciamos los servicios con los siguientes comandos:

Service apache2 restart

Service php5 restart

Service mysql-server restart

Configuramos el archivo apache2.conf, en el cual definimos el nombre del server en el archivo

Sudo gedit /etc/pache2/apache2.conf

Después de la línea donde se define la carpeta root. El archivo queda de la siguiente forma:

49 #

50 ServerRoot "/etc/apache2"

51 ServerName "serverweb"

52 #

Nota: Perso6soft es el nombre del servidor en nuestro caso

Dimos permisos a la carpeta /var/www; para así agregar nuestra página diseñada.

Sudo chmod -R 755 /var/www

Sudo chown -R www-data\: /var/www

Para ver que está funcionando, abrimos en un navegador (Firefox, crome, etc) y ponemos lo siguiente.

http://127.0.0.1

o

http://172.16.3.20 que es la dirección ip que posee nuestro servidor.

Y si ya tenemos montado nuestro servidor DNS, simplemente pondremos el nombre que le hemos asignado, en nuestro caso:

http://www.radiofe.com.ni

Agregamos phpmyadmincon el siguiente comando

Sudo apt-get install phpmyadmin

Con el diseño de la pagina ya acabada, nos dispusimos a pegarla en el directorio, y luego solo permitimos autorización de cambios al usuario root.

Ahora agregamos un archivo en la carpeta /var/www, con el nombre de php.info, y agregamos los siguientes términos

<?

Php.info;

¿>

Con lo antes realizado, veremos las configuraciones de phpmyadmin, introduciendo en un buscador (Firefox, crome, etc) lo siguiente

http://www.radiofe.com.ni/php.info

3.5 Configuraciones del servidor de correo (Suse Linux Enterprise Server 11 sp1)

Previo a la instalación del servidor realizamos los debidos ajustes al sistema.

configuraciones de IP Estática

hostname servermail
address 172.16.3.30
netmask 255.255.255.0
network 172.16.3.0
gateway 172.16.3.1
broadcast 172.16.3.255
dns-nameservers 172.16.3.10
dns-search radiofe.com.ni
Instalaciones de MTA, MDA.

MTA – Agente de transporte de correo

Como agente de transporte se instaló Postfix, por ser uno de los más seguros.

Instalamos Postfix, y luego nos vamos a su archivo de configuración y editamos y agregamos las configuraciones para su correcto uso.

vi /etc/postfix/main.cf

```
# line 91: uncomment and specify domain name
mydomain = radiofe.com.ni
# line 107: uncomment
myorigin = $mydomain
# line 268: uncomment and specify LAN
mynetworks = 127.0.0.0/8, 172.16.3.0/24, 10.10.0.0/16
# line 423: uncomment (use Maildir)
home_mailbox = Maildir/
# line 528: uncomment
header_checks = regexp:/etc/postfix/header_checks
# line 529: add
body_checks = regexp:/etc/postfix/body_checks
# line 671: specify hostname
myhostname = servermail.radiofe.com.ni
# line 675: change
inet_interfaces = all
# line 677: add
mydestination = $myhostname, localhost.$mydomain
, localhost, $mydomain
# line 691: change
smtpd_recipient_restrictions = permit_mynetworks, permit_auth_destination,
permit_sasl_authenticated, reject
# line 693: change
smtpd_sasl_auth_enable = yes
# line 697: change (limit mailbox 100M)
mailbox_size_limit = 102400000
# add at the bottom
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
```

Editamos ahora el archive Header_checks en la carpeta postfix

vi /etc/postfix/header_checks

add at the head

reject if email address is empty
/^From:.*<#.*@.*>/ REJECT
/^Return-Path:.*<#.*@.*>/ REJECT
hide Received line
/^Received:/ IGNORE

También editamos el archive body_checks

vi /etc/postfix/body_checks

/^(|[^>].*)example.com/ REJECT

/^(|[^>].*)example.com/ REJECT
y luego iniciamos el servicio de Postfix y Saslauthd

/etc/init.d/postfixstart

/etc/rc.d/saslauthd start

Agregamos los siguientes servicios para que inicien desde el arranque del sistema

chkconfig boot.clock on

chkconfig postfix on
chkconfig saslauthd on

Ahora configuraremos el MDA (Agente de entrega de correo)
Con Cyrus
Ahora instalamos Cyrus-Imapd

zypperinstall -y cyrus-imapd

Editamos el archivo de configuración agregando y modificandolo

vi /etc/imapd.conf

line 14: add

sasl_mech_list: plain login

line 17: add

allowplaintext: yes

Ahora Iniciamos rpcbind, spld y cyrus

/etc/init.d/rpcbind start

/etc/init.d/slpd start

/etc/init.d/cyrusstart

Ahora los agregamos al inicio del sistema

chkconfig rpcbind on

chkconfig slpd on

chkconfig cyrus on

chgrp mail /etc/sasl*

Le agregamos un password a Cyrus

passwdcyrus

set cyrus's password

Changing password for cyrus.

New Password: -digitamos aqui el pass-

Reenter New Password: -lo volvemos a digitar-

Passwordchanged.

Ahora vamos a agregar un usuario para Cyrus

cyradm --user cyruslocalhost
Password: -introducimos el password de cyrus-
localhost> cm user.servermail
create a mailbox for "admin"
localhost> lm
verify
user.admin (HasNoChildren)
localhost> exit

Con esos pasos se ha agregado un usuario con su respectivo buzón. Ahora editaremos el archivo main.cf de postfix para que pueda utilizar cyrus

vi /etc/postfix/main.cf
# line 683: add
mailbox_transport = cyrus

Reiniciamos Postfix

Ahora agregaremos un certificado para identificarnos y mejorar el correo

Creamos un nuevo directorio para los certificados

mkdir /etc/ssl/CA

Accedemos a el

cd /etc/ssl/CA

Ya dentro de este empezamos a hacer los certificados, en nuestro caso ingresamos lo siguiente y nos pedirá password para el server.key que realizamos:

opensslgenrsa -des3 -out server.key 1024

Generating RSA private key, 1024 bit long modulus

.....++++++

.....++++++

e is 65537 (0x10001)

Enter pass phrase for server.key:

set passphrase

Verifying - Enter pass phrase for server.key:

verify

remove passphrase from private key

Terminado eso ahora ingresamos lo siguiente e igual introducimos el password:

opensslrsa -in server.key -out server.key

Enter pass phrase for server.key:

inputpassphrase

writing RSA key

Le asignamos un periodo de validez al certificado y rellenamos con los datos de nuestra empresa.

opensslreq -new -days 3650 -key server.key -out server.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:NI

State or Province Name (full name) [Some-State]:Nandaime

Locality Name (eg, city) []:Granada
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Radio Fe
Organizational Unit Name (eg, section) []:Radio Fe de los Milagros
Common Name (eg, YOUR name) []:servermail.radiofe.com

Email Address []:admin6@radiofe.com.ni
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

Y ya tenemos realizado nuestro Certificado

Para finalizar solo agregamos los siguientes comandos

openssl x509 -in server.csr -out server.crt -req -signkeyserver.key -days 3650

Y le damos atributos

chmod 400 server.*

Ahora ya con nuestro certificado realizado, nos disponemos a anexarlo a nuestro servidor de correo

Editamos el main.cf de postfix

vi /etc/postfix/main.cf

# line 694: change
smtpd_use_tls = yes

# add at the bottom
smtpd_tls_cert_file = /etc/ssl/CA/server.crt
smtpd_tls_key_file = /etc/ssl/CA/server.key
smtpd_tls_session_cache_database = btree:/etc/postfix/smtpd_scache

Anexamos en el master.cf el smtps, editándolo así:

vi /etc/postfix/master.cf

line 13: uncomment
smtps inet n - n - - smtpd -o smtpd_tls_wrappermode=yes

En el archivo dovecot.conf de la carpeta dovecot, cambiamos los siguientes parametros
Agregamos el Puerto 465 para smtps, mayor seguridad el puerto
vi /etc/services

line 1232: make it comment and add
#urd 465/tcp # URL Rendesvous Directory for SSM

#igmpv3lite 465/udp # IGMP over UDP for SSM

smtps 465/tcp - - - - esta linea es la que agregamos.

Reiniciamos Postfix y Dovecot.

/etc/init.d/postfix restart

Creamos dominios virtuales

vi /etc/postfix/main.cf

# line 664: change
virtual_alias_maps = hash:/etc/postfix/virtual
virtual_alias_domains = hash:/etc/postfix/virtual

Y los agregamos al archivo Virtual

vi /etc/postfix/virtual

add at the head

userA@virtual.host

userB

Hacemos un postmap

postmap /etc/postfix/virtual

y reiniciamos postfix.

Para hacer mejor esto, vamos a agregarle un antivirus y un antispam

Instalamos Clamav (antivirus)

zypperinstall -y clamav

Editamos su archivo de configuracion

vi /etc/freshclam.conf

line 110: makeitcomment

NotifyClamd /etc/clamd.conf

Actualizamos con el siguiente comando

freshclam

updatepettern file

Este proceso puede ser un poco tardado
Luego hacemos un scan

clamscan --infected --remove --recursive /home

---------- SCAN SUMMARY ----------

Known viruses: 554735

Engine version: 0.95.1

Scanned directories: 5

Scanned files: 6

Infected files: 0

Data scanned: 0.01 MB

Data read: 0.00 MB (ratio 2.00:1)

Time: 1.822 sec (0 m 1 s)

Ya tenemos un antivirus para nuestro correo

Ahora instalamos un AntiSpam

zypper install -y amavisd -new spamassassin

Y editamos una línea en su archivo de configuración

vi /etc/clamd.conf

line 170: change

AllowSupplementaryGroups yes

Configuramos Amavis para que funcione con nuestro servidor

vi /etc/amavisd.conf

line 21: specify domain name

$mydomain = 'radiofe.com.ni';

line 152: uncomment and specify FQDN

$myhostname = 'servermail.radiofe.com.ni';

line 154: uncomment

$notify_method = 'smtp:[127.0.0.1]:10025';

$forward_method = 'smtp:[127.0.0.1]:10025';

```
# line 157: uncomment
$final_virus_destiny = D_DISCARD;
$final_banned_destiny = D_BOUNCE;
$final_spam_destiny = D_BOUNCE;
$final_bad_header_destiny = D_PASS;
$bad_header_quarantine_method = undef;
# line 363: uncomment
['ClamAV-clamd',
  &ask_daemon, ["CONTSCAN {}\n", "/var/lib/clamav/clamd-socket"],
  qr/\bOK$/, qr/\bFOUND$/,
  qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

Y luego lo anexamos a postfix

vi /etc/postfix/main.cf

```
# add at the bottom
content_filter=smtp-amavis:[127.0.0.1]:10024
```

Y al master.cf

vi /etc/postfix/master.cf

```
# add at the bottom
smtp-amavisunix -       -       n       -       2 smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
127.0.0.1:10025 inet n  -       n       -       - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
```

-o smtpd_helo_restrictions=

-o smtpd_sender_restrictions=

-o smtpd_recipient_restrictions=permit_mynetworks,reject

-o mynetworks=127.0.0.0/8

-o strict_rfc821_envelopes=yes

-o smtpd_error_sleep_time=0

-o smtpd_soft_error_limit=1001

-o smtpd_hard_error_limit=1000

reniciamos clam, amavis, spamd y postfix

/etc/init.d/clamd restart

/etc/init.d/freshclam restart

/etc/init.d/amavis restart

/etc/init.d/spamd restart

/etc/init.d/postfix restart

Los hacemos arrancar desde el inicio del sistema

chkconfig amavis on

chkconfig spamd on

chkconfig clamd on

chkconfig freshclam on

Y ya tenemos configurado un servidor de correo con antivirus y antispam integrados.

Para la autenticación de usuarios se ultilizo el servidory cliente LDAP, el cual fue configurado para el correcto uso.

Ahora solo hay que conseguir un MUA (agente usuario de correo), tal como lo es mozilla thunderbird, outloock, entre otros, y configurarlos para que utilicen nuestro servidor de correo.

4.6 Configuraciones para el correcto uso de Iptables (Ubuntu server 10.04 LTS)

Primeramente nos dispusimos a actualizarlo a sus más recientes actualizaciones

Sudo apt-get update

Sudo apt-get upgrade

Ahora, el cortafuegos tiene 3 interfaces y he aquí planteamos como se configura.

Cortafuegos

- Se conecta a Internet mediante una dirección IP estática
- Tiene tres interfaces de red
  - eth0 (IP 192.168.1.3), que da acceso a Internet
  - eth1 (IP 10.10.0.1), que es la puerta de enlace de la red local
  - eth2 (IP 172.16.3.1), que es la puerta de enlace de la DMZ.
- Es servidor DHCP de la red local
- No debe ser accesible desde Internet
- Actúa como dispositivo NAT
- Puede hacer consultas DNS al servidor de la red local
- Responde a ping hecho desde la red local o la DMZ

DMZ

- Direccionamiento IP 172.16.3.0/24
- Conectada a la interfaz eth2 del cortafuegos
- Tiene un servidor web (http) IP 172.16.3.20
- servidor de correo (smtp, pop3 e imap) IP 172.16.3.30
- Servidor DNS IP 172.16.3.10
- Servidor FTP IP 172.16.3.40
- Los servidores están virtualizados en una computadora con Windows 7 modificada para mejorar su seguridad.

Red local

- Direccionamiento IP 10.10.0.0/24
- Conectada a la interfaz eth1 del cortafuegos
- Los equipos de la red local deben tener acceso a todos los servicios ofrecidos por los equipos de la DMZ
- Los equipos de la red local pueden utilizar los servicios web (http y https) de cualquier servidor de Internet

Aquí el script para solucionar y garantizar una red segura con IPTABLES

```
#!/bin/bash
# flush de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -t nat -Z
#Denegamos todo en el firewall
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

```
iptables -P FORWARD DROP
#Cargamos los modulos necesarios
modprobe ip_tables
modprobe iptable_nat
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp
#permitimos localhost
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Permitir el trafico de conexiones ya establecidas (el control de tráfico se hace al inicar las conexiones)
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#Reglas NAT necesarias
#SNAT
iptables -t nat -A POSTROUTING -o eth0 -s 10.10.0.0/16 -j MASQUERADE
iptables -t nat -A POSTROUTING -o eth0 -s 172.16.3.0/24 -j MASQUERADE
#DNAT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to
172.16.3.20:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20 -j DNAT --to
172.16.3.40:20
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 21 -j DNAT --to
172.16.3.40:21
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 30000:31000 -j DNAT --to
172.16.3.40
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to
172.16.3.30:25
```

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 110 -j DNAT --to
172.16.3.30:110
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 143 -j DNAT --to
172.16.3.30:143
#activamos ip forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv4/ip_dynaddr
#otro
iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-
pmtu
#Tenemos NAT pero no conexion debido a que el firewall tiene denegado todo
(DROP)
#incluimos reglas para que nuestra DMZ sea visible desde internet
#Aceptamos peticiones al servidor web (http) y su debida respuesta.
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.20 -p tcp --dport 80 -
j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.20 -o eth0 -d 0.0.0.0/0 -p tcp --sport 80 -j
ACCEPT
#Aceptamos peticiones al servidor FTP y su debida respuesta
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.40 -p tcp --dport 20 -
j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.40 -o eth0 -d 0.0.0.0/0 -p tcp --sport 20 -j
ACCEPT
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.40 -p tcp --dport 21 -
j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.40 -o eth0 -d 0.0.0.0/0 -p tcp --sport 21 -j
ACCEPT
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.40 -p tcp --dport
30000:31000 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.40 -o eth0 -d 0.0.0.0/0 -p tcp --sport
30000:31000 -j ACCEPT
```

#Aceptamos peticiones al servidor de correo (SMTP) y sus debidas respuestas

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.30 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth0 -d 0.0.0.0/0 -p tcp --sport 25 -j ACCEPT

#SMTP tambien se comporta como cliente por lo cual tambien envia correos

iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth0 -d 0.0.0.0/0 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.30 -p tcp --sport 25 -j ACCEPT

#Aceptamos peticiones al servidor de correo (POP) y sus debidas respuestas

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.30 -p tcp --dport 110 -j ACCEPT

iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth0 -d 0.0.0.0/0 -p tcp --sport 110 -j ACCEPT

#Aceptamos peticiones al servidor de correo (IMAP) y sus debidas respuestas

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.30 -p tcp --dport 143 -j ACCEPT

iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth0 -d 0.0.0.0/0 -p tcp --sport 143 -j ACCEPT

#Para que los equipos de la DMZ puedan hacer resolucion de nombres (Ejm. envio de correos), le permitimos consultas DNS

iptables -A FORWARD -i eth2 -s 172.16.3.0/24 -o eth0 -d 0.0.0.0/0 -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.0/24 -p udp --sport 53 -j ACCEPT

iptables -A FORWARD -i eth2 -s 172.16.3.0/24 -o eth0 -d 0.0.0.0/0 -p tcp --dport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.0/24 -p tcp --sport 53 -j ACCEPT

#Permitimos las peticiones DNS del equipo 172.16.3.10

iptables -A FORWARD -i eth2 -s 172.16.3.10 -o eth0 -d 0.0.0.0/0 -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.10 -p udp --sport 53 -j ACCEPT

iptables -A FORWARD -i eth2 -s 172.16.3.10 -o eth0 -d 0.0.0.0/0 -p tcp --dport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.10 -p tcp --sport 53 -j ACCEPT

#Con motivos de prueba daremos acceso a internet a la DMZ

#Aceptamos peticiones a los servidores web (http) y su respuesta

iptables -A FORWARD -i eth2 -s 172.16.3.0/24 -o eth0 -d 0.0.0.0/0 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.0/24 -p tcp --sport 80 -j ACCEPT

#Aceptamos peticiones a los servidores web (http) y su respuesta

iptables -A FORWARD -i eth2 -s 172.16.3.0/24 -o eth0 -d 0.0.0.0/0 -p tcp --dport 20:21 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.0/24 -p tcp --sport 20:21 -j ACCEPT

#Aceptamos peticiones a los servidores web (https) y su respuesta

iptables -A FORWARD -i eth2 -s 172.16.3.0/24 -o eth0 -d 0.0.0.0/0 -p tcp --dport 443 -j ACCEPT

iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth2 -d 172.16.3.0/24 -p tcp --sport 443 -j ACCEPT

#Ahora vamos a establecer las reglas necesarias para que los equipos de la red local puedan acceder a los servicios de la DMZ y de los servicios que se permiten de internet

#Local - DMZ

Permitir a todos los equipos de la LAN hacer consultas UDP al servidor DNS de la DMZ.

```
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.10 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.10 -o eth1 -d 10.10.0.0/16 -p udp --sport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones al servidor web (http) y su respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.20 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.20 -o eth1 -d 10.10.0.0/16 -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones al servidor FTP y su debida respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.40 -p tcp --dport 20:21 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.40 -o eth1 -d 10.10.0.0/16 -p tcp --sport 20:21 -m state --state ESTABLISHED,RELATED -j ACCEPT
#FTP pasivo
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.40 -p tcp --dport 30000:31000 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.40 -o eth1 -d 10.10.0.0/16 -p tcp --sport 30000:31000 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones al servidor de correo (SMTP) y su debida respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.30 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth1 -d 10.10.0.0/16 -p tcp --sport 25 -m state --state ESTABLISHED,RELATED -j ACCEPT
#servidor de correo (SMTP) actúa como cliente así que:
iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth1 -d 10.10.0.0/16 -p tcp --dport 25 -j ACCEPT
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.30 -p tcp --sport 25 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones al servidor de correo (POP) y su debida respuesta
```

```
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.30 -p tcp --dport 110 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth1 -d 10.10.0.0/16 -p tcp --sport 110 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones al servidor de correo (IMAP) y su debida respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth2 -d 172.16.3.30 -p tcp --dport 143 -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.16.3.30 -o eth1 -d 10.10.0.0/16 -p tcp --sport 143 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Local - INTERNET
#Aceptamos peticiones a los servidores web (http) y su respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth0 -d 0.0.0.0/0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth1 -d 10.10.0.0/16 -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
#Aceptamos peticiones a los servidores web (https) y su respuesta
iptables -A FORWARD -i eth1 -s 10.10.0.0/16 -o eth0 -d 0.0.0.0/0 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i eth0 -s 0.0.0.0/0 -o eth1 -d 10.10.0.0/16 -p tcp --sport 443 -m state --state ESTABLISHED,RELATED -j ACCEPT
#permitir consultas DNS salientes (sobre TCP y UDP)
iptables -A FORWARD -o eth0 -s 10.10.0.0/16 -p tcp --dport 53 -m state --state NEW -j ACCEPT
iptables -A FORWARD -o eth0 -s 10.10.0.0/16 -p udp --dport 53 -m state --state NEW -j ACCEPT
iptables -A FORWARD -o eth2 -s 10.10.0.0/16 -p tcp --dport 53 -m state --state NEW -j ACCEPT
iptables -A FORWARD -o eth2 -s 10.10.0.0/16 -p udp --dport 53 -m state --state NEW -j ACCEPT
#Incluimos ahora las reglas necesarias para el correcto funcionamiento
#INPUT/OUTPUT
```

iptables -A INPUT -s 10.10.0.0/16 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -s 10.10.0.0/16 -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT

#Se permiten las peticiones y respuestas DHCP

iptables -A INPUT -i eth1 -p udp -s 0.0.0.0/0 -d 255.255.255.255 --dport 67 --sport 68 -j ACCEPT

iptables -A OUTPUT -o eth1 -s 10.10.0.1 -d 255.255.255.255 -p udp --sport 67 --dport 68 -j ACCEPT

iptables -A INPUT -i eth2 -p udp -s 0.0.0.0/0 -d 255.255.255.255 --dport 67 --sport 68 -j ACCEPT

iptables -A OUTPUT -o eth2 -s 172.16.3.1 -d 255.255.255.255 -p udp --sport 67 --dport 68 -j ACCEPT

#Se permiten consultas DNS al servidor de la DMZ

iptables -A OUTPUT -o eth2 -s 172.16.3.1 -d 172.16.3.10 -p udp --dport 53 -j ACCEPT

iptables -A INPUT -i eth2 -d 172.16.3.1 -s 172.16.3.10 -p udp --sport 53 -j ACCEPT

iptables -A OUTPUT -o eth2 -s 172.16.3.1 -d 172.16.3.10 -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -i eth2 -d 172.16.3.1 -s 172.16.3.10 -p tcp --sport 53 -j ACCEPT

#Se permiten consultas DNS al servidor de la DMZ

iptables -A OUTPUT -o eth0 -s 192.168.1.4 -d 192.168.1.1 -p udp --dport 53 -j ACCEPT

iptables -A INPUT -i eth0 -d 192.168.1.4 -s 192.168.1.1 -p udp --sport 53 -j ACCEPT

iptables -A OUTPUT -o eth0 -s 192.168.1.4 -d 192.168.1.1 -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -i eth0 -d 192.168.1.4 -s 192.168.1.1 -p tcp --sport 53 -j ACCEPT

#consultas dns

iptables -A INPUT -s 0.0.0.0/0 -p udp -m udp --sport 53 -j ACCEPT

```
iptables -A OUTPUT -s 0.0.0.0/0 -p udp -m udp --dport 53 -j ACCEPT
#NAVEGAR EN WEB
#iptables -A INPUT -p tcp --dport 80 -j ACCEPT
#iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
#Se permite ping desde la red local y la DMZ
iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -o eth1 -p icmp --icmp-type echo-reply -j ACCEPT
iptables -A INPUT -i eth2 -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -o eth2 -p icmp --icmp-type echo-reply -j ACCEPT
```

4.7 Proformas

MUNDO DIGITAL, S.A.

Calle Principal de Altamira, del BDF 1c al norte
PBX: 2702022 RUC Nº: 120500 - 9015

Cliente : OSCAR MONTANO
Atencion:
Telefono :
Fax :
E-mail:

Fecha: 12-nov-12
Entrega:
Correo: ventas1@syditek.com.ni
Vendedor: Winstong Olivas
T/C: Paralelo al BANPRO

Cantidad	Descripción	Precio/U	Precio/T
1	SERVIDOR HP PROLIANT ML 150 G6 E5504- 2.0GHZ/2GB/SAS/HOT –SWAP 3.5””/466132-001	U$ 1,698.00	U$ 1,698.00
1	SWITCH CISCO 8 PUERTOS 10/100 SD208 -NA	U$ 30.41	U$ 30.41
1	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G - LA	U$ 91.32	U$ 91.32
1	UPS TRIPP LITE SMARTOLINE SU2200XLA-110/22OV 7OUT – SU 2200XLA	U$ 800.58	U$ 800.58
1	CONECTORES RJ-45	U$ 0.13	U$ 0.13
1 m	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP	U$ 0.53	U$0.54

CONDICIONES DE LA OFERTA:

* Tipo de cambio paralelo a BAMPRO
* Emitir pago a nombre de Mundo Digital S.A
* Valides de la oferta: 5 días
* Sujeta a cambio sin previo aviso
* Cheque personalizado

SUBTOTAL	U$ 2620.98
DESCUENTO	0
SUBTOTAL	U$ 2620.98
IVA	U $ 393.147
TOTAL	U$ 3014.127

Winstong Olivas
Ejecutivo De Venta
Cel: 8-8[illegible]61

Calle Principal de Altamira, del BDF 1c al norte / PBX: 2702022 / RUC Nº: 120500 - 9015

Tecnología Computarizada S.A

Calle Principal Altamira D'este No.589 Ferreteria Sinsa 25vrs arriba
Telefono:PBX (505) 2264-8800 - Fax:(505)270-6224 - Email : ventas@comtech.com.ni
RUC No. J0310000000603 - www.comtech.com.ni

Cliente:	**OSCAR MONTANA**	**Nº Prof.**	**68920**
Atención:		fecha	12/11/2012
Teléfono:		Valida hasta	12/11/2012
Email:		Condiciones	CONTADO
		T/cambio	24.1700

Cantidad	Descripción	Precio/U	Precio/T
1	SERVIDOR HP PROLIANT ML 150 G6 E5504- 2.0GHZ/2GB/SAS/HOT –SWAP 3.5””/466132-001	$ 1,598.00	$ 1,598.00
1	SWITCH CISCO 8 PUERTOS 10/100 SD208 -NA	$ 32	$ 32.00
1	ROUTER LINKSYS WIRELESS-G 2.4GHZ WRT54G - LA	$ 89.00	$ 89.00
1	UPS TRIPP LITE SMARTOLINE SU2200XLA-110/22OV 7OUT – SU 2200XLA	$ 816.00	$ 816.00
1	CONECTORES RJ-45	$ 0.14	$ 0.14
1 m	CABLE ETHERNET 10BASE-T PAR TRENSADO UTP	U 0.60	$ 0.60

Subtotal	2535.74
Impuesto	380.361
Total	2916.101

Comentarios:

UN AÑO DE GARANTIA ENTREGA INMEDIATA

Helen Guevara

Nota: Es valida solamente con el sello de la empresa

Nota: Somos Grandes Contribuyentes.
Estamos Exentos del 1% de la Retencion en la Fuente

SEVASA SUCURSAL ALTAMIRA
FERRETERIA ROBERTO MORALES 100 MTS AL SUR
Teléfono No.: 22524204 Fax No.: 22524204
No. RUC 030605-9521

C O T I Z A C I O N

Cliente	Oscar Montano	Nº	00015490
vendedor	Johana Artola	fecha	12/11/20121
Cantidad	Descripción	Precio/U	Precio/T
1	Servidor hp proliant ml 150 g6 E5504- 2.0ghz/2gb/sas/hot –swap 3.5””/466132-001	U$1670.00	U$1670.00
1	Switch cisco 8 puertos 10/100 sd208 -na	U$31.90	U$31.90
1	Router Linksys wireless-g 2.4ghz wrt54g - la	U$88.50	U$88.50
1	Ups tripp lite smartoline su2200xla-110/22ov 7out – su 2200xla	U$812.00	U$812.00
1	Conectores rj-45	U$0.13	U$0.13
1 m	Cable Ethernet 10base-t par trenzado utp	U$0.63	U$0.63
		Subtotal	U$2603.16
		Impuest	U$390.475
		Total	U$2993.63

Concepto: Tasa de cambio 24.17
Valido por dos días
Llamar al 22524204 Ext. 202