DISEÑO DE UNA INFRAESTRUCTURA DE RED MEDIANTE UNA SOLUCIÓN OPEN SOURCE FAVORABLE A LA EMPRESA ANPRA LTDA.

AUTORES:
Carlos Hernán González Rincón
Diego Manuel Blanco Montes

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN
FACULTAD DE INGENIERÍA ELECTRÓNICA
BUCARAMANGA
2008

DISEÑO DE UNA INFRAESTRUCTURA DE RED MEDIANTE UNA SOLUCIÓN OPEN SOURCE FAVORABLE A LA EMPRESA ANPRA LTDA.

Autores:

Carlos Hernán González Rincón 69523

Diego Manuel Blanco Montes 73711

PROYECTO DE GRADO PARA OPTAR POR AL TÍTULO DE INGENIERO ELECTRÓNICO

Directora:

Ing. Angélica Flórez Abril, MSc.

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA DE INGENIERÍA Y ADMINISTRACIÓN

FACULTAD DE INGENIERÍA ELECTRÓNICA

BUCARAMANGA

2008

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Ciudad y Fecha:

AGRADECIMIENTOS

El éxito de este proyecto ha sido posible gracias a los conocimientos adquiridos que hemos recibido de parte de la Universidad Pontificia Bolivariana y a la dedicación y apoyo de nuestros maestros a lo largo de toda nuestra carrera.

Agradecemos especialmente a nuestros padres por su apoyo y confianza incondicional para que todos nuestros proyectos se estén haciendo realidad.

Al gerente de la empresa ANPRA Ltda., Ingeniero José Luis Angarita Vergel y todos sus empleados sin los cuales no habría sido posible la realización de este proyecto.

A la ingeniera Laura Marcela Chacón Rueda, a nuestra directora Angélica Flórez y a todas las personas que de una u otra manera nos guiaron y nos brindaron la colaboración necesaria durante estos meses para el desarrollo de nuestro proyecto.

Finalmente infinitas gracias a Dios quien nos ha prestado la vida, ha sido nuestro guía y fuente de inspiración permitiéndonos avanzar y lograr la culminación exitosa de todos nuestros propósitos

A nuestros padres, hermanos y demás familiares, quienes con su amor y sacrificio se convirtieron una vez más en el mejor apoyo para alcanzar nuestros objetivos.

TABLA DE CONTENIDO

Lista de Figuras

Lista de Planos

Lista de Tablas

Pág.

RESUMEN

En éste proyecto se diseñó e implementó una infraestructura de red que permitió unir la sede de la empresa ubicada en la ciudad de Bucaramanga con la sede ubicada en Bogotá con una relación costo/beneficio favorable a la empresa ANPRA LTDA. Para la realización de este proyecto se utilizó Router Open Source Vyatta, la cual es una tecnología abierta al usuario que le brinda herramientas similares a las ofrecidas por los Router comerciales con una diferencia de costos considerable. Con esta tecnología se pudo implementar una Red Privada Virtual que permitió a la empresa ANPRA compartir información con niveles de seguridad aceptables entre las bases de datos creadas en cada uno de los puntos. La metodología que se llevó a cabo para la realización de este proyecto fue la siguiente: primero se hizo un estudio de la infraestructura de red con la que contaba ANPRA para conocer su topología y cómo se encontraba conectada la red en su totalidad, posteriormente se realizó un análisis del nivel de seguridad que tenía la información dentro de la empresa para encontrar vulnerabilidades que hicieran débiles su red de datos, después se hizo un análisis comparativo entre las soluciones open source y comerciales para definir la opción que proporcionara la relación costo/beneficio necesaria para el proyecto, y finalmente se elaboró el diseño de la infraestructura de red que uniera a las dos sedes junto con la implementación. Este proyecto se encuentra en funcionamiento desde mayo del 2008.

PALABRAS CLAVES: Infraestructura, tecnología libre, Red Privada Virtual, Red Informática.

ABSTRACT

In this project was designed and implemented a network infrastructure that allowed to join the head office of the company located in the city of Bucaramanga with the office located in Bogota with a cost/benefit relation in pro of the ANPRA LTD Company. For the achievement of this project there was used Router Open Source Vyatta, which is an open technology that offers the user similar tools to the ones offered by the commercial Router with a considerable difference of costs. With this technology it was possible to implement a Virtual Private Network that allowed the company to share information at acceptable safety levels between the databases created in each one of the points. The methodology used for the achievement of this project was the following one: first a study of the network infrastructure with which ANPRA was provided was made to meet its topology and how was the network connected in its totality, later there was realized an analysis of the safety level that the information had inside the company to find vulnerabilities that were doing weak its computer network, later on, a comparative analysis between the open source and commercial solutions was made to define an option that was able to provide the cost/benefit relationship necessary for the project, and finally there was arranged the design of the network infrastructure that joined the two head offices along with the implementation. This project is working since May, 2008.

KEYWORDS: Infrastructure, Open Source, Virtual Private Network, Computer Network

INTRODUCCIÓN

ANPRA Ltda es una empresa fundada en el año 1994 con el propósito de vender auto-partes de marcas de automóviles comerciales. Desde el momento de su creación esta empresa ha ido en constante crecimiento, trabajando para mejorar continuamente sus procesos y servicios, razón por la cual nace el proyecto de ampliación a nivel nacional por medio de sedes distribuidas en lugares estratégicos del país, de tal manera que la entrega de sus productos se pueda hacer en el menor tiempo posible a sus clientes.

Las necesidades de ampliación, junto a los requerimientos que demandan la implementación de tecnologías que permitan la conectividad entre las sedes, se constituyen en los primeros obstáculos al iniciar el proyecto de ampliación, puesto que no se cuenta con el capital suficiente para la inversión en dispositivos de enrutamiento que suplan con las necesidades de conexión y seguridad en el intercambio de información entre las sedes, factor que afecta directamente hoy en día a varias de las empresas pequeñas, debido a que por falta de recursos la seguridad de su información se encuentra en un nivel bajo.

El objetivo de este proyecto está centrado en la reducción de costos tanto de adquisición como de implementación de una tecnología que supla con las necesidades de conexión de la empresa, y al mismo tiempo que brinde el tipo de seguridad que requiere el intercambio de información entre las sedes de Bucaramanga y Bogotá. La metodología que se utilizará para la realización de este proyecto va ligada al desarrollo que han tenido las soluciones Open Source en el ambiente de networking, demostrando la eficiencia y funcionalidad que tiene esta tecnología frente a las soluciones comerciales.

OBJETIVOS

OBJETIVO GENERAL

Diseñar y construir un prototipo de la infraestructura de red de la empresa ANPRA Ltda. de manera que permita obtener una relación costo/beneficio favorable a la empresa. Esta red empleara Routers Open Source VYATTA.

OBJETIVOS ESPECÍFICOS

- Analizar la red actual estudiando los requerimientos de la empresa para mejorar la relación costo/beneficio.

- Analizar las soluciones Open Source y comerciales comparando sus características para encontrar los beneficios que se pueden tener a partir de la implementación del software libre.

- Diseñar una infraestructura de red que garantice niveles de seguridad y confiabilidad aceptable para la transmisión de datos entre las dos sedes.

- Implementar un prototipo de la arquitectura de comunicación, que demuestre una correcta transmisión supliendo los inconvenientes y necesidades de la empresa ANPRA.

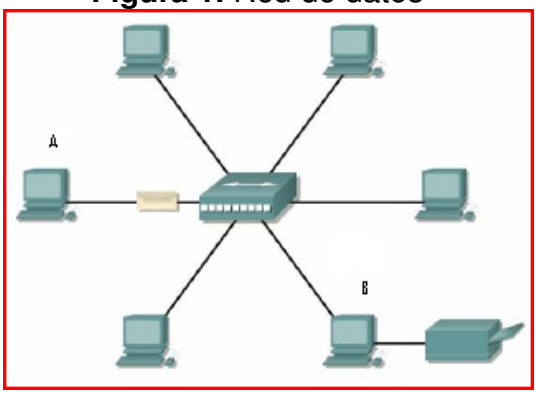
1. MARCO TEÓRICO

La finalidad de este proyecto es diseñar una red que supla las necesidades tanto de comunicación como de seguridad teniendo en cuenta la reducción en la inversión de dinero. Antes de profundizar en cada una de las etapas del proyecto, es necesario contextualizar al lector acerca del papel que cumple cada elemento utilizado o factor estudiado. En este capítulo se estudiarán los tipos de red con sus diferentes topologías y arquitecturas, para tener una visión de cómo la red en la empresa se encuentra operando. Se estudiarán los elementos utilizados para la seguridad implementada y los dispositivos necesarios para el montaje de la infraestructura propuesta.

1.1 RED DE DATOS

Es un conjunto de equipos (computadores o dispositivos) conectados a través de un sistema de telecomunicación con el fin de comunicarse y compartir información (archivos), recursos (fax, unidades de disco, impresoras, etc.) y servicios (correo electrónico, Internet, chat, etc.). El objetivo fundamental es permitir que las máquinas conectadas a una red de datos, puedan hacer uso tanto de los dispositivos adyacentes en el sistema como de su procesamiento, permitiendo crear un medio por el que se puedan comunicar los usuarios, obtener recursos comunes y compartir servicios que ayuden a la elaboración de tareas de manera grupal. En la figura 1, el dispositivo A envía a imprimir un archivo al dispositivo B dentro de una red.
Una red puede tomar distintas formas las cuales definen su topología, y distintas características especiales que definen su clase [1].

Figura 1. Red de datos

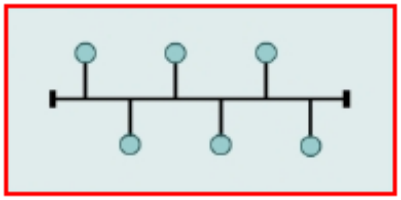


Tomado de Cisco/CCNA-1

1.1.1 Topología de la red

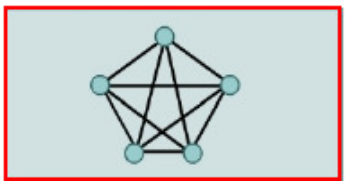
Es la configuración adoptada por las estaciones de trabajo que conforman una red para conectarse entre sí, esta es determinada únicamente por la configuración de las conexiones entre nodos. El tipo de topología de una red es el que define su estructura y la manera como se ha dispuesto el cable al igual que la forma en que los computadores se encuentran conectados para realizar el envío de datos. Las topologías físicas más usadas son las siguientes:

- **Topología de bus:**



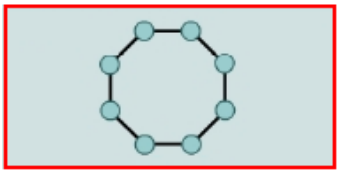
En este tipo de topología los dispositivos se encuentran conectados en forma lineal a un único canal de comunicaciones o backbone.

- **Topología en malla:**



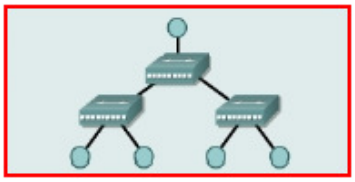
En este tipo de topología todos los nodos se encuentran comunicados entre sí, permitiendo el envío de información por el camino más corto o menos congestionado, lo cual evita que se presenten problemas de interrupción en la comunicación.

- **Topología en anillo:**



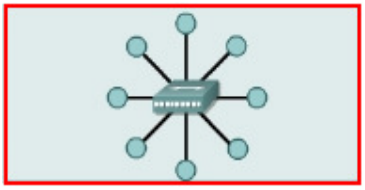
En este tipo de topología toda la información de la red pasa a través de cada uno de los nodos, hasta que la información llega a su destino final. Se le llama topología de anillo debido a que su forma es el de una estructura circular en el que cada computador se une al siguiente por medio de enlaces punto a punto.

- **Topología jerárquica:**



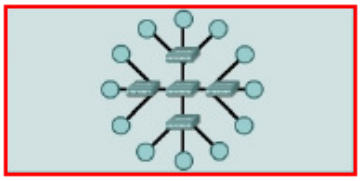
En este tipo de topología los dispositivos de conexión se encuentran ubicados en forma de cascada formando una red jerárquica conectada a un dispositivo central el cual se encarga de controlar todo el tráfico de la red.

- **Topología en estrella:**



En este tipo de topología los dispositivos se encuentran conectados a un punto central el cual actúa como un intercambiador, si un dispositivo quiere enviar datos a otro, envía los datos al dispositivo central y el los retransmite al dispositivo final.

- **Topología en estrella extendida:**



Este tipo de topología es una variante de la topología de estrella debido a que resulta de la unión de varias de ellas; esta se utiliza cuando se tienen una gran cantidad de dispositivos dentro de la red [2].

1.1.2 Clases de Redes

Existen tres clases de redes las cuales se convierten en las principales hoy en día. Las clases de redes más utilizadas son Red LAN (Red de Área Local) ideal para una empresa, Red WAN (Red de Área Extensa) utilizada para conectar redes LAN entre países y ciudades, y las Redes MAN (Redes de Área Metropolitana) utilizada para conectar varias redes LAN dentro de una misma ciudad.

Para determinar el tipo de red que se desea implementar es necesario tener en cuenta las siguientes variables:

- Propietario: es necesario determinar si la red es privada o pública (Internet).
- Distancia de cobertura: es necesario observar el lugar en donde se desea implementar la red y se deben tener en cuenta las distancias entre las conexiones de los dispositivos.
- Arquitectura física: se debe tener en cuenta el diseño de la red y la manera en que se deben interconectar los dispositivos de red, qué infraestructura se va a utilizar y qué topología de red se implementará.
- Tamaño: hace referencia a la distancia y el número de dispositivos que la red tendrá [3, p. 17].

- **Red LAN**

Local Area Network o Red de Área Local, es una red conectada en un área relativamente pequeña, conformadas por oficinas, departamentos de trabajo o un conjunto de dispositivos en un edificio o conjunto de edificios.

Este tipo de tecnología permite a las empresas compartir localmente archivos y periféricos de manera eficiente, posibilitando la comunicación interna de toda la red. Usualmente el cable utilizado para conectar todas las máquinas dentro de una red LAN es de tipo coaxial o UTP a velocidades de transmisión entre 10 y 100 Mbps (Ethernet y Fast Ethernet), mientras que dentro de las redes LAN de alta velocidad pueden encontrarse velocidades que alcanzan los 10 Gbps (Gigabit Ethernet); por lo general la tecnología más utilizada en las redes LAN es Ethernet [3, p. 18].

Según Soul Cast Beta en su clasificación de las redes de comunicación expone varias características que definen a una red LAN [4]:

- Los canales de transmisión son propios de los usuarios o empresas.
- Los enlaces son líneas con transmisión de alta velocidad.
- Incrementan la eficiencia y productividad de los trabajos al poder compartir recursos e información entre oficinas.
- Las tasas de error son menores que en las redes WAN.
- Se convierte en un sistema seguro.

- **Red WAN**

Wide Area Network o Red de Área Extensa, es una red punto a punto utilizada para interconectar redes LAN entre países y continentes. El diseño de una red

WAN es mucho más complejo que el de una red LAN debido a que tiene que enrutar correctamente todos los paquetes de video, voz, datos e imágenes provenientes de todas las redes conectadas a ella; de igual manera la velocidad de transmisión es menor en la primera debido a que la distancia de recorrido es mayor [5].

Características:

- Cubren una región, país o continente siendo capaz de conectar varias redes LAN.
- Dividen subredes intercomunicadas entre sí.
- Conectan múltiples LAN.
- Utilizan usualmente Routers en los extremos de las redes.

- **Red MAN**

Metropolitan Area Network o Red de Área Metropolitana, es una red que abarca un área metropolitana como: ciudad o municipio. Debido a que una MAN consta de una o mas redes LAN dentro de un área geográficamente común, se puede decir que una red MAN es una red LAN de gran extensión, cubriendo de esta manera varios puntos de trabajo en una misma ciudad o región específica [6].

1.1.3 Dispositivos de Red

Los dispositivos de red son los encargados de transportar los datos que deben transferirse entre los dispositivos de usuario final, su función es la de la concentración, administración y comunicación de las conexiones. En el proyecto se trabajarán con los siguientes dispositivos de red [2, p. 28]:

- **Switch o Conmutador**

Es un hardware también llamado puente multi-puerto situado en la capa de enlace de datos (se encarga de la topología de la red, la notificación de errores, el acceso a la red, entrega ordenada de tramas y el control de flujo) cuyo objetivo es concentrar la conectividad de dos o más dispositivos a un punto de la red, encargado de crear tablas de envío que determinan el destino de los datos basándose en las direcciones MAC de destino además de funcionar como un filtro en la red que mejora el rendimiento y seguridad de la LAN. El Switch conmuta tramas desde los puertos de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total [7].

- **Router o Enrutador**

Es un dispositivo que además de concentrar múltiples conexiones, es capaz de regenerar señales otorgando características específicas. Los tres tipos de conexiones básicos de un router son las interfaces LAN, las interfaces WAN y los puertos de administración. Además es el responsable de hacer que el paquete de datos llegue a su destino final, para ello analiza la información dentro de un paquete, lee su dirección de red y busca el camino más corto a seguir por dicho paquete entre una interconexión de redes de nivel de capa tres (Nivel de red que establece, conmuta, mantiene, controla y termina el envío de paquetes entre redes).

Cuenta con los componentes básicos de un computador estándar (CPU, Memoria, Bus de datos, Interfaces, etc.), sin embargo está diseñado para ejecutar funciones específicas que lo caracterizan, estas son algunas de sus funciones [2 p.250-254]:

- Enrutamiento.
- Punto de enlace entre diversos tipos de red:
  - LAN – LAN
  - LAN – MAN
  - LAN – WAN – LAN
  - WAN – WAN
  - LAN – Internet

Nota: No funciona si no es configurada cada interface [3 p.148].

- **AP (Access Point o punto de acceso)**

Es un hardware encargado de recibir, almacenar y transmitir información dentro de una red creada a través de la conexión de dispositivos de comunicación inalámbrica. El AP es un intermediario entre unos PCs y una red externa, el cual cuenta con una dirección IP asignada para poder ingresar a su modo de configuración; hay que tener en cuenta que este soporta un grupo limitado de usuarios y su velocidad de transmisión es directamente proporcional a la distancia a la que ellos se encuentren del mismo [8].

- **Firewall (Corta-fuegos)**

Es un dispositivo de seguridad ya sea de tipo hardware o software que se utiliza como filtro para permitir o denegar la transmisión de datos de una red a otra, examinando toda la comunicación entrante o saliente y dando paso sólo al tráfico autorizado según las reglas implementadas, en las que generalmente lo que no se admite se prohíbe por defecto. Normalmente se sitúa entre una red privada y una

red pública actuando como un agente de seguridad que controla la información y protege la red interna de una compañía. Para permitir o denegar una comunicación, el Firewall examina el tipo de servicio al que corresponde, por ejemplo: Web o correo, dependiendo del servicio, el Firewall decide si lo permite o no. De igual forma el Firewall verifica si la conexión es entrante o saliente y dependiendo de su dirección efectúa una acción sobre la transmisión existente [2 p. 411].

- **Servidor Proxy**

Un servidor proxy es un equipo situado entre el usuario e Internet con el fin de registrar copias locales de los sitios web que el usuario visita y bloquear el acceso a una Web. Dentro del servidor proxy se encuentra algo que se conoce como el servidor de seguridad, y es el encargado de bloquear algunas páginas Web por distintas razones. El principio operativo básico de un servidor proxy se basa en lo siguiente:
Cuando el usuario se conecta a Internet con una aplicación del cliente configurada para utilizar un proxy, la aplicación primero se conecta con el servidor para entregarle la solicitud que posteriormente enviará al servidor en Internet (al que la aplicación del cliente desea conectarse). Finalmente, el servidor le envía la respuesta al proxy el cual a su vez la envía a la aplicación del cliente.

Las características más importantes del servidor proxy son [9]:

- Funciona como un filtro de contenidos y como un servidor de seguridad, son un mecanismo de seguridad implementado por los proveedores de Internet o por los administradores de la red en un entorno de Intranet para desactivar el acceso y filtrar el acceso a ciertas páginas Web que son consideradas malignas.
- Mejora el rendimiento, el servidor proxy guarda en la memoria caché las páginas a las que han accedido los computadores de una red determinada durante un cierto tiempo. Cuando el dispositivo solicita una página web ya consultada, el servidor proxy utiliza la información guardada en la caché y de esta forma accede con mayor velocidad al sitio web solicitado.

- **VPN (Red Privada Virtual)**

Es un túnel encriptado entre dos puntos, es decir, una estructura de red virtual (confidencial y exclusiva) creada dentro de una red (pública o privada) que utiliza el mismo proceso y las mismas políticas de acceso de las redes privadas para permitir a los usuarios trabajar remotamente con la red local. Una VPN permite que una red LAN pueda comunicarse con una o más redes LAN para crear un

canal seguro que mantenga la integridad y confidencialidad de los datos, por medio de mecanismos de autenticación y cifrado dentro de una red pública como Internet.

Se podría decir que existen dos tipos de conexiones en las redes privadas virtuales (VPN): El primer tipo se llama client-to-site, un usuario remoto establece conexión con la oficina principal, este caso hace referencia a aquellos clientes o usuarios que obtienen permiso para conectarse a una red específica. El segundo tipo site-to-site, una sede remota u oficina con varios computadores se une a una red central, el caso de un almacén con sucursales en otras partes [2 p. 34-36].

Entre algunas de sus características importantes se pueden encontrar las siguientes:

- Autenticación de Usuarios: La VPN controla quién y cuándo puede acceder a los recursos remotos.
- Manejo de direcciones: Asigna direcciones privadas manteniendo en secreto la dirección real del origen, hace uso de NAT.
- Encripción de datos: Todos los datos son encriptados con el fin de ser transportados con seguridad en redes públicas.
- Manejo de claves: Se generan llaves de encripción en los extremos de la VPN.

- **NAT (Network Address Translation o Traducción de Dirección de Red)**

NAT fue originalmente diseñada para ayudar a conservar el número de direcciones IP agotadas debido al crecimiento de dispositivos que tienen acceso a Internet. Hoy en día se ha convertido en una aplicación muy importante en el manejo de seguridad de las redes.

Un dispositivo capaz de habilitar NAT en su configuración, puede utilizar direcciones IP privadas y aún así tener conectividad con el resto de Internet, reemplazando la dirección IP privada por la dirección IP pública (proceso de enmascaramiento o masquerade) en su salida a Internet. Esta nueva dirección con la que sale el paquete es la única que queda expuesta durante el viaje a través de Internet. La anterior, es una de muchas funciones que puede tener NAT en el proceso de enrutamiento de paquetes, todas las características y tipos no se estudiarán debido a que solo se utilizaron algunas específicas durante el proyecto que se explicarán a continuación[10]:

SNAT (Source NAT o NAT de origen): es la más común de los tipos de NAT, es usada cuando un computador interno necesita iniciar una sesión con un computador externo. SNAT cambia el direccionamiento origen de los paquetes que viajan de la red interna a la red externa. Utiliza la opción “masquerade” para reemplazar la dirección origen por la de la interface de salida del paquete.

DNAT (Destination NAT o NAT de destino): es utilizada cuando un computador externo necesita iniciar sesión con un computador interno. DNAT cambia la dirección de destino de los paquetes que viajan de la red externa a la red interna.

Inside-address y Outside-address: especifican la conversión de dirección que toma el paquete en la regla de NAT. Ellos definen la información que es sustituida dentro del paquete por la dirección original. Inside-address es usada en DNAT, especifica la dirección por la que es sustituida la dirección IP destino del paquete de entrada. Outside-address es usada con SNAT, especifica la dirección por la que es sustituida la dirección origen del paquete de salida.

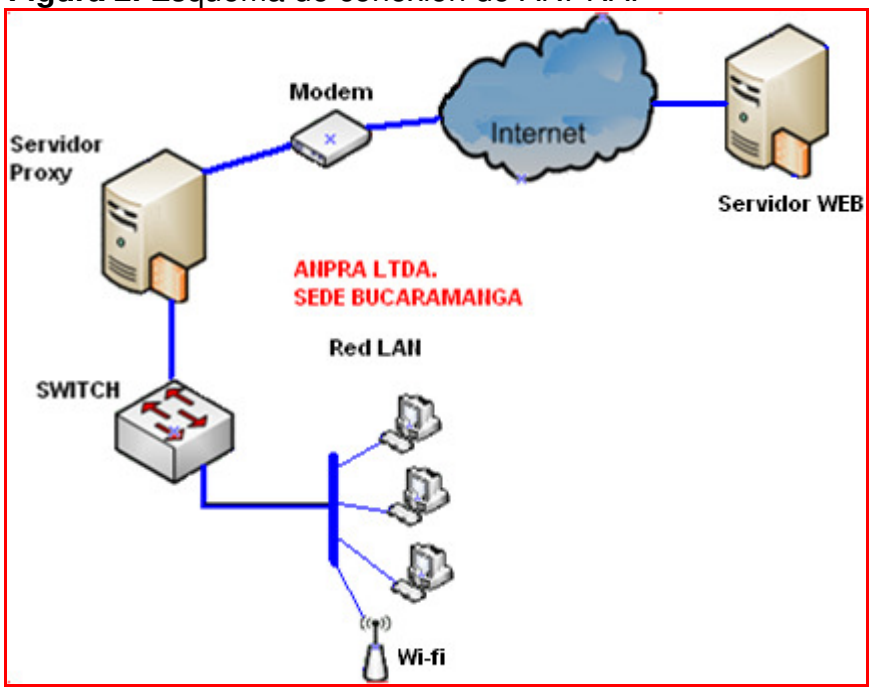
Inbound y Outbound: especifica si la interface es de salida o de entrada. Cuando se utiliza la opción destino (DNAT) se debe especificar la interface de entrada (Inbound-interface), cuando se utiliza la opción Origen (SNAT) se debe especificar la interface de salida (Outbound-interface).

2. ESTADO ACTUAL DE LA INFRAESTRUCTURA DE RED DE ANPRA Ltda.

En este capítulo se estudiará el estado actual de la infraestructura de red de la empresa ANPRA, los dispositivos que la conforman, la forma en que está conectada, el direccionamiento IP de sus equipos y los departamentos que la conforman.

2.1 ESQUEMA DE CONEXIÓN DE LA RED DE ANPRA Ltda.

Figura 2. Esquema de conexión de ANPRA.



El acceso a Internet de la empresa se encuentra custodiado por el servidor que está conectado al Modem con dirección IP pública 201.21.138.18 y máscara de red 255.255.255.0; la velocidad del canal de Internet es de 512 Kbps, suministrado por el Proveedor de Servicios de Internet Telebucaramanga. La empresa CAMINOWEB presta sus servicios de hosting donde se encuentra el servidor Web de ANPRA.

En el servidor se tiene activo el servicio de DHCP que suministra el direccionamiento IP a los computadores distribuidos en cada uno de los

departamentos de la empresa conectados al Switch (ver Figura 2), Además, se encuentra configurado como servidor proxy, tiene almacenada toda la información vital de la empresa, la base de datos, los precios, clientes, entre otros. El rango de direcciones IP va desde la 192.168.254.2 hasta 192.138.254.254 con máscara 255.255.255.0.

2.1.1 Cableado de red

La topología de la infraestructura de red de la empresa ANPRA, se define como una Estrella la cual se encuentra dividida en dos pisos:

- **Primer piso**

- El primer piso de aproximadamente 340 metros cuadrados lo conforman los departamentos de Logística, venta al Público, Caja, Bodegas, Sala de Ventas y Distribución (ver Plano No. 1).

- En este piso se encuentran ubicados siete computadores los cuales están conectados por medio de cable UTP categoría 5e, norma TIA-EIA 568-A al Switch ubicado en el segundo piso; el cableado del primer piso es dirigido al segundo por medio de un tubo PVC de 2" (ver Plano No. 2).

- El Access Point se encuentra ubicado en el departamento de bodegas del primer piso junto a las bodegas 1 y 2 donde se encuentra la mercancía (ver Plano No. 2).

- **Segundo piso**

- El segundo piso de aproximadamente 340 metros cuadrados lo conforman los departamentos de Gerencia, el Centro de Telecomunicaciones, la Sala Administrativa y la Sala de Conferencias (ver Plano No. 3).

- En este piso se encuentran ubicados siete computadores los cuales están conectados por medio de cable UTP categoría 5e norma TIA-EIA 568-A al Switch ubicado en el Centro de Telecomunicaciones (ver Plano No. 4).

- En el cuarto de telecomunicaciones se encuentran los dispositivos de conectividad para la red local, también se encuentra el servidor Proxy (ver Plano No. 4).

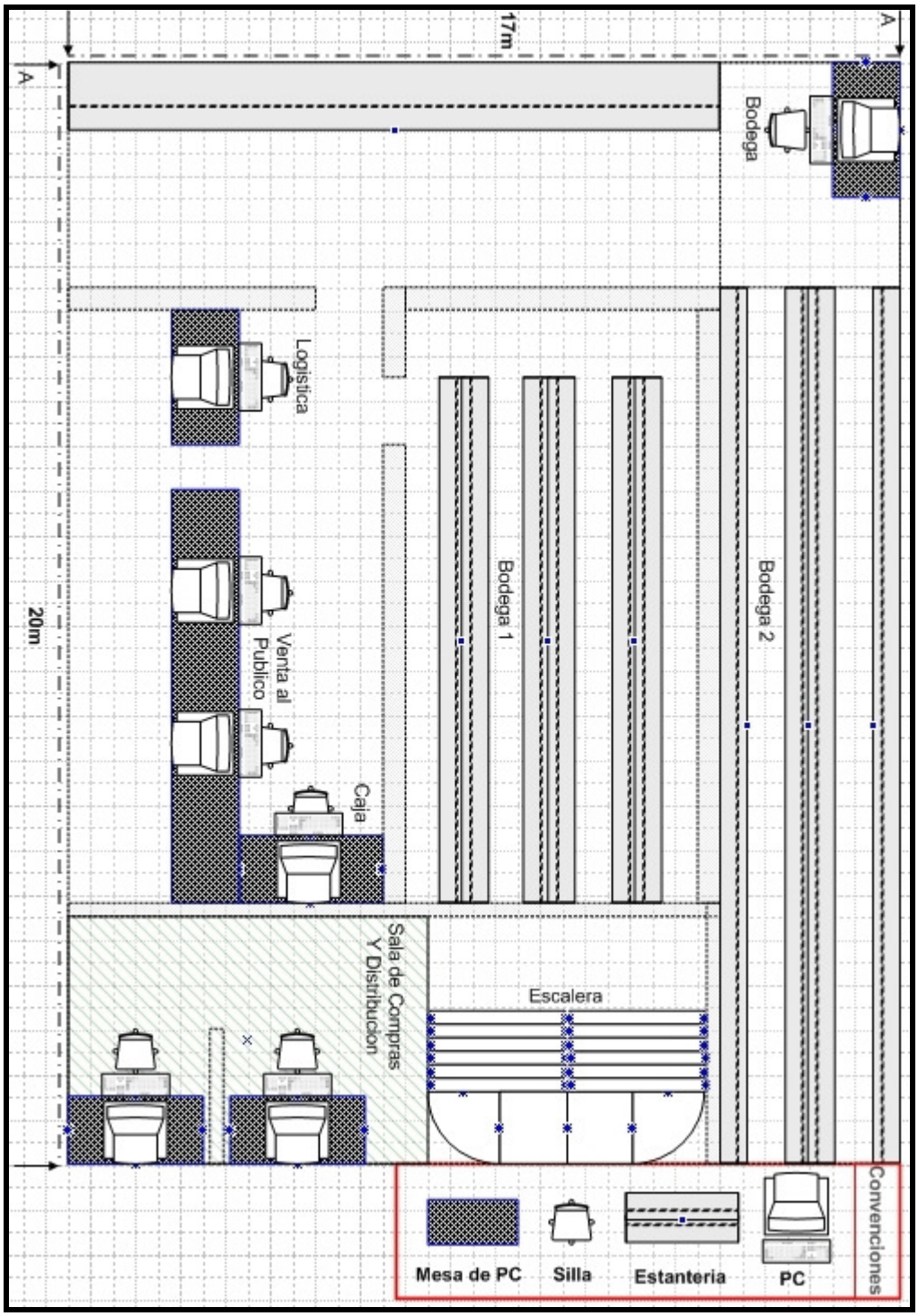
2.1.2 Direccionamiento IP

La empresa ANPRA, cuenta con el siguiente direccionamiento IP para todos sus departamentos distribuidos de la siguiente manera:

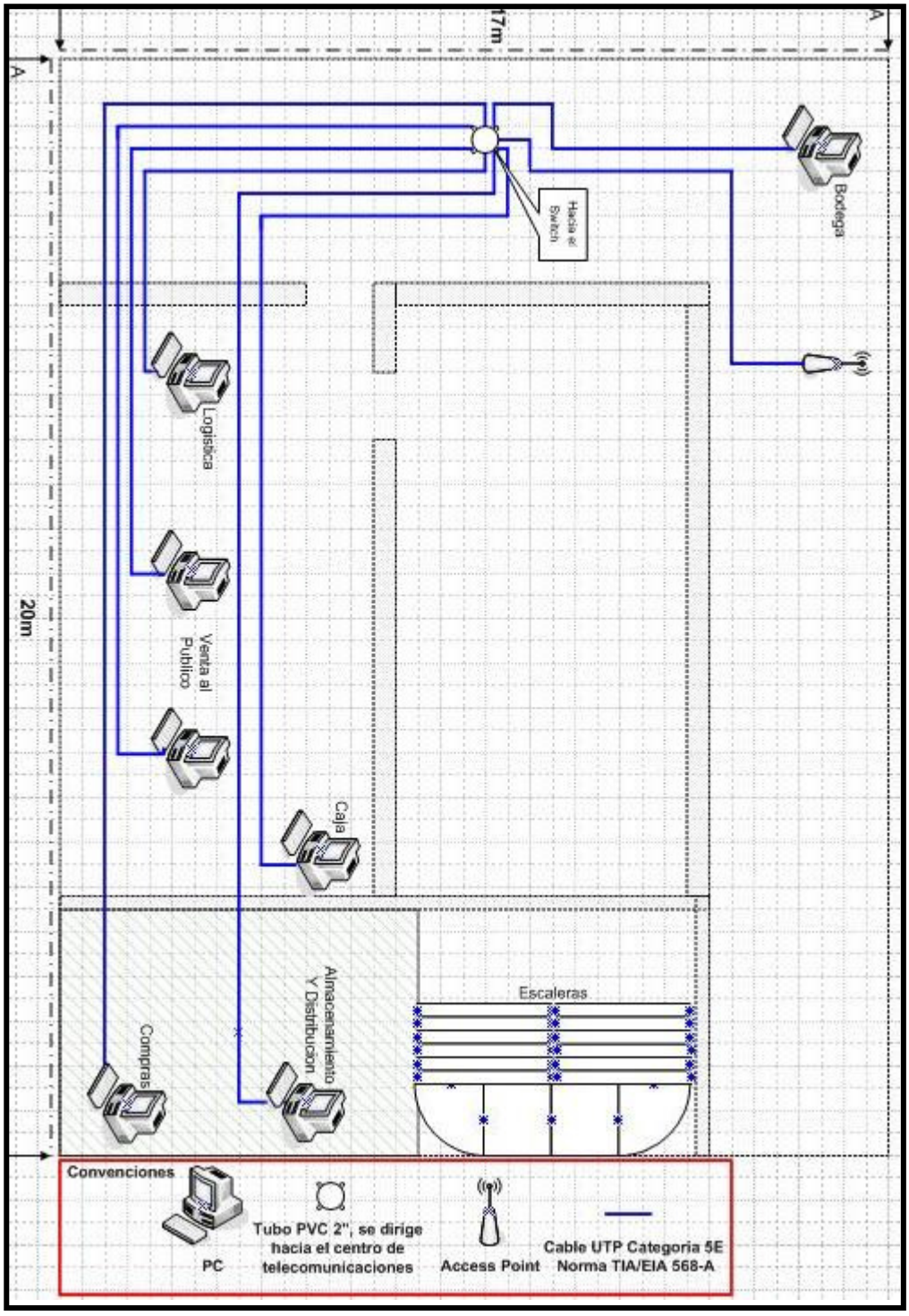
Tabla 1. Direccionamiento IP de la Empresa ANPRA.

DEPARTAMENTOS O DEPENDENCIAS	DIRECCIONAMIENTO IP
Bodega	192.168.254.12 , 192.168.254.65
Logística	192.168.254.15
Venta al público	192.168.254.17 , 192.168.254.19
Caja	192.168.254.9
Sala de Compras y distribución	192.168.254.56 , 192.168.254.35
Gerencia	192.168.254.13
Sala de conferencias	192.168.254.18 , 192.168.254.21
Sala administrativa	192.168.254.100 , 192.168.254.98 , 192.168.254.75

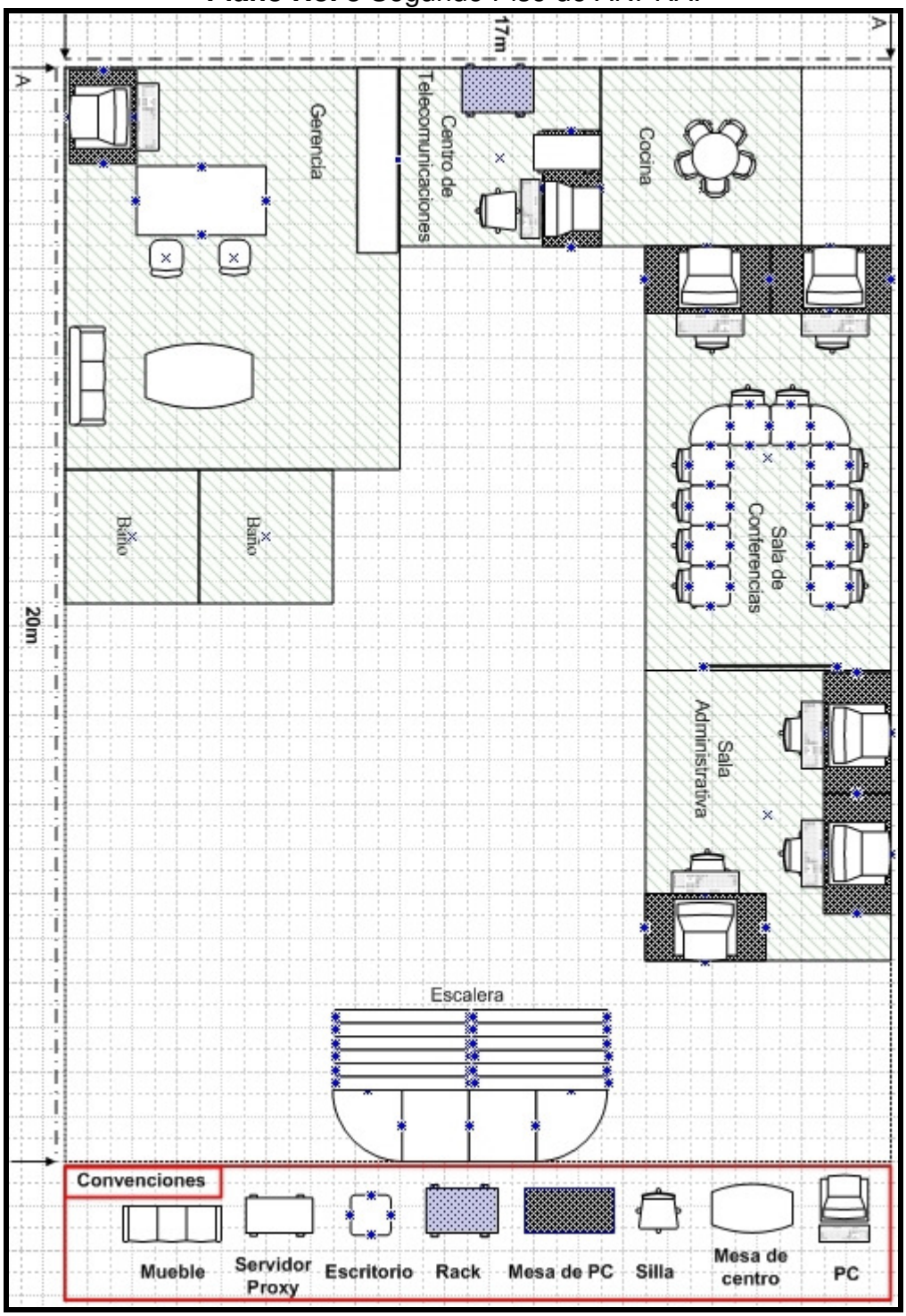
Plano No. 1 Primer Piso de ANPRA.



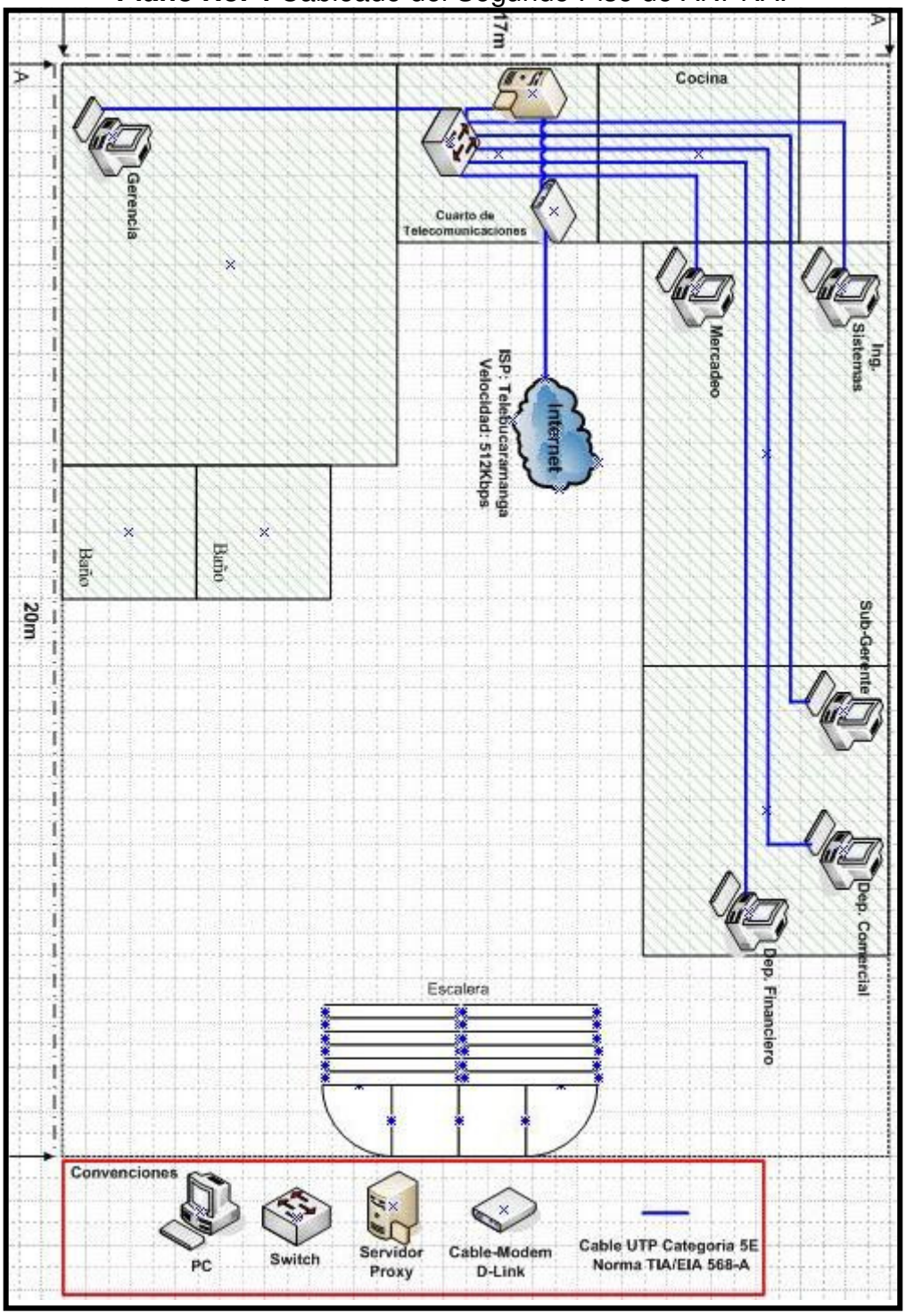
Plano No. 2 Cableado del Primer Piso de ANPRA.



Plano No. 3 Segundo Piso de ANPRA.



Plano No. 4 Cableado del Segundo Piso de ANPRA.



3. ANÁLISIS DEL NIVEL DE SEGURIDAD DE LA INFORMACIÓN EN LA RED DE ANPRA Ltda.

La seguridad de la información es de gran importancia actualmente y es un concepto que muchas empresas no han tenido en cuenta, ya sea porque desconocen las amenazas a las que se encuentran expuestas día a día o las utilidades que traería este nuevo gasto. Debido a la ignorancia que se tiene referente a estos temas, la inversión que hacen muchas compañías para ayudar a minimizar el grado de vulnerabilidad dentro de una red es muy baja, quedando insegura la información.

Usualmente las empresas toman conciencia de la seguridad informática tras recibir un ataque que se ve reflejado en la pérdida, robo, alteración o secuestro de la información.

Teniendo en cuenta lo anterior, la empresa se vió obligada a buscar medidas que ayudaran a mitigar cualquier amenaza que pudiese afectar la integridad de la información manejada por parte de ésta.

La empresa ANPRA, inició sus labores a mediados del año 1994 con sólo cuatro computadores, sin contar con una arquitectura de red apropiada. Con el pasar de los años se han ido agregando los dispositivos necesarios para su operatividad dentro de una red local y salida a Internet, todo esto sin tener en cuenta aspectos y políticas de seguridad que protejan la información que la empresa maneja y almacena.

En este capítulo se hará un estudio de las vulnerabilidades presentes en la infraestructura de red con la que cuenta actualmente ANPRA, mencionando sus posibles soluciones. El estudio se divide en tres fases, en primer lugar se hará un estudio de manera interna, mencionando las debilidades que tiene la red LAN de la empresa, posteriormente, se hará un análisis del servidor de la empresa y los servicios con los que cuenta ANPRA, y finalmente se hará un estudio de manera externa al tráfico que genera y recibe la red para encontrar sí existe o no anomalías que afecten la integridad de la información.

3.1 DEBILIDADES INTERNAS EN LA RED DE ANPRA Ltda.

El proyecto de proteger una red no garantiza un 100% de defensa frente a los diversos ataques que puedan ser realizados hacia la compañía, por esta razón, ni la cantidad de dinero que se invierta en seguridad, ni el tiempo que los ingenieros

gasten en supervisar la red podrán asegurarle a los administradores que la empresa se encuentre totalmente protegida.

Actualmente se espera que las personas vinculadas a una empresa conozcan o tengan conocimientos mínimos acerca de la seguridad informática, teniendo en cuenta que uno de los activos importante de una compañía es la información. El hecho de no tener claro el valor que tiene la información dentro de la organización, es un factor que puede influir en la ocurrencia de los siguientes inconvenientes:

- Alteración de los datos manejados dentro de la compañía.
- Pérdida de información.
- Divulgación de información personal.
- Documentación de diseños y productos propios de la fábrica haciendo que lleguen a manos equivocadas tanto de personas internas como de personas externas a la compañía.

Todo lo anterior, sin tener en cuenta los problemas de seguridad a los que se enfrenta la información que viaje a través de Internet. El desarrollo del estudio del nivel de seguridad interno de la infraestructura de ANPRA, se hará mediante un análisis de las distintas vulnerabilidades dentro de la red, entrevistas con el personal que labora en la compañía y desarrollo de actividades junto al ingeniero de sistemas. Todo esto permitirá crear estrategias para concienciar a los empleados y al mismo tiempo buscar soluciones a los diferentes inconvenientes que se puedan encontrar.

3.1.1 Amenazas Internas

Es importante tener en cuenta que el éxito de una red segura empieza desde los empleados de la misma compañía, por esta razón se hace de vital importancia estudiar varios aspectos dentro de la empresa que podrían convertirla en vulnerable. Se encontraron deficiencias en:

a. Hardening a base de datos.
b. Servidor, ISA Server 2004.
c. Manejo de los Backups.
d. Acceso dentro de la red LAN (libre acceso dentro de la red).
e. Sesiones de usuario (se encuentran sin clave).
f. Entrenamiento del personal (no existe concienciación).
g. Archivos y directorios (no hay restricción de uso).
h. Seguridad física.
i. Passwords (claves débiles).

j. Red Interna (el Internet inalámbrico permite que los visitantes utilicen la misma subred de la empresa).
k. Access Point (seguridad con WEP).

a. Hardening a Base de Datos

Hardening es una acción que se compone de varias actividades o un conjunto de buenas prácticas y procedimientos tanto físicos como lógicos, que son llevados a cabo por el administrador de un sistema operativo para reforzar y aumentar el nivel de seguridad de los equipos y aplicaciones de una compañía, con el propósito de hacerle más difícil la materialización de un ataque a una persona con malas intenciones. Es importante recordar que esta es una de las operaciones que se deben tener en cuenta para llegar a un buen punto de seguridad dentro de la empresa; hacer Hardening no quiere decir, que el sistema podrá ser invulnerable a ataques, pero si ayudará a minimizar los ataques a los que quedan expuestas día a día las bases de datos [11].

- **Procedimientos Físicos**

La seguridad de los datos comienza desde la protección de los dispositivos que contienen la información vital de la empresa. Se podrá crear una excelente seguridad lógica para proteger los datos sensibles de la compañía, pero si no se tiene en cuenta un buen mecanismo o procedimiento de seguridad física, la información estará vulnerable dentro de las mismas instalaciones, debido a que personal no autorizado tendrá acceso a aquellos equipos de almacenamiento de bases de datos donde podrá modificar, extraer y destruir información almacenada, y así como también por los daños que este personal podría hacer de manera física como: desconexión, robo, destrucción o manipulación de los servidores [12].

Actualmente ANPRA, no cuenta con un procedimiento o mecanismo de protección física de los dispositivos de almacenamiento de información, dejando a la empresa expuesta a cualquier manipulación por parte de personal no autorizado dentro y fuera de la compañía.

Para una buena práctica de Hardening de seguridad física es recomendable que se tomen las siguientes medidas:

- Ubicar los servidores en salas cerradas donde sea de carácter obligatorio registrar la entrada y salida de cualquier persona.

- Desconectar de Internet la red de ANPRA mientras se esté instalando el sistema operativo al servidor de la empresa debido a que toda la red queda expuesta sin ninguna protección alguna.

- No dejar las llaves puestas en las carcasas de los servidores.

- Definir contraseñas del sistema operativo.

- Definir el orden de inicio de la BIOS para que el servidor no pueda ser iniciado desde un Diskette o CD.

- Eliminar unidades que no se necesiten en el servidor (unidad de diskette, unidad de CD, etc.).

- **Procedimientos Lógicos**

La seguridad lógica consiste en establecer medidas o procedimientos que protejan el acceso a la información, de tal manera que solo sea manipulada por personal autorizado. Después de descubrir las deficiencias con las que cuenta la seguridad física dentro de ANPRA, es importante tener en cuenta que en general los daños sufridos en el interior de la empresa a nivel de software o datos, son los determinantes en cuanto a la dinámica de la empresa, debido a que afectan directamente la operación y el desempeño en cuanto a productividad dentro de la organización.

Estos son algunos de los aspectos en los que se encontraron deficiencias y las posibles soluciones que se plantean para las diversas vulnerabilidades:

1) **Seguridad en la instalación del Sistema Operativo:** Las carpetas que manejen información vital para la empresa deben estar en un disco diferente al disco donde se encuentre el sistema operativo instalado, debido a que si existe alguna falla en el sistema la integridad de los datos no se verá comprometida.

2) **Contraseñas Fuertes:** La contraseña establecida en el servidor de la empresa, debe tener un alto grado de complejidad ya que en muchas ocasiones es utilizado el ataque por fuerza bruta, el cual a pesar de ser un mecanismo lento que deja rastros, es muy efectivo frente a contraseñas débiles. Es necesario establecer políticas de bloqueo de sesión por intentos fallidos y al mismo tiempo crear periodos de caducidad permitiendo así, una renovación en la clave cada cierto tiempo.
   Nota: Se pudo tener acceso a la cuenta del servidor utilizando como usuario: Administrador, y como contraseña: admin.

3) **Instalación, Configuración y Actualización de Software de seguridad:** antivirus, anti-spyware, anti-spam, Firewall, entre otros. ANPRA., en su servidor cuenta con un Firewall llamado ISA Server 2004, el cual se encuentra configurado con los parámetros por defecto. Esto podría acarrear mal funcionamiento en la red debido a que las opciones que vienen con el programa podrían no ajustarse a las necesidades y requerimientos de la

empresa, afectando el nivel de seguridad junto al enrutamiento de paquetes desde la organización hacia Internet.

4) **Permisos para utilización de ciertos programas:** La única restricción que existe por medio de una contraseña en ANPRA es el ingreso a la base de datos, por lo tanto es necesaria la creación de perfiles de usuario dentro de la empresa para permitir o restringir la utilización de ciertos programas o aplicaciones, limitando el libre acceso a los recursos e información del sistema.

5) **Controles de acceso externos e internos:** Se debe crear un control de permisos y puertos para prevenir la instalación de tecnologías tanto software como hardware, que puedan comprometer la seguridad y el rendimiento de la red [13].

b. Acceso dentro de la red LAN

La empresa ANPRA cuenta con una red LAN que trabaja en una única red para todas sus dependencias (Gerencia, Subgerencia, Logística, Punto de venta, Mercadeo, Caja, Compras, Departamento de Bodega, Financiero, Comercial, Distribución y Sistemas) y clientes que llegan a la compañía, sin ningún tipo de control, generando así varios problemas y amenazas hacia la red interna de la compañía como:

- Tráfico indeseado en el canal de Internet utilizado por la empresa debido a que ninguna estación de trabajo tiene limitación para hacer uso del ancho de banda.

- Acceso por parte de usuarios malintencionados a información que no corresponde a su dependencia (nómina, base de datos, lista de precios, lista de clientes, información sensible de la empresa, etc.).

- Manipulación de la información con un propósito específico para propio beneficio (desvío de Fondos, alteración en la nómina etc.).

- Comprometer toda la red al introducir un virus de forma accidental o de manera premeditada por parte de los usuarios.

- Captura y monitoreo de todo el tráfico de la red utilizando programas de sniffer (Ethereal, Wireshark, TCP-dump, Snort, etc.) para encontrar deficiencias en la red que puedan ser aprovechadas en un ataque.

Es importante no subestimar las capacidades de los empleados que tengan acceso a la red, pues se desconoce el grado de conocimiento que ellos pueden tener y del que pueden valerse para realizar un ataque contra la empresa. Dada esta situación, es difícil para un administrador de red pensar que los empleados

traicionarían la compañía donde laboran; sin embargo, es necesario tener en cuenta este tipo de aspectos para realizar un buen trabajo de seguridad que ayude en caso de sufrir cualquier problema de esta índole.

La creación de listas de control de acceso en el Router VYATTA, ayudaría a reducir en gran porcentaje los inconvenientes que se podrían generar debido a la ausencia de algún control interno y a respaldar el tema de la confidencialidad y protección de la información. Este método además de mejorar el aprovechamiento del ancho de banda haciendo la conectividad más eficiente, permitirá o prohibirá el tráfico según las condiciones establecidas dentro de la red de ANPRA [2 p. 399-403].

Una lista de control de acceso permitirá establecer:

- ✓ Permisos sobre el modo en que los usuarios y empleados acceden o salen de la red de ANPRA.

- ✓ Los servicios a los que determinada estación de trabajo puede acceder.

- ✓ Rechazo al tráfico dependiendo de: Origen del tráfico
  Destino del tráfico
  Protocolo utilizado

c. Manejo del Backup

Actualmente en la empresa se realiza el backup de los datos de la siguiente manera:

- Diariamente se hace un backup en la máquina del Ingeniero de Sistemas de todos los datos suministrados por el servidor, como lo son el listado de clientes, listado de almacenes, nómina, compras, etc.

- Semanalmente se recopila toda la información guardada en la máquina del Ingeniero de Sistemas y se graba en DVDs etiquetados con la fecha a la cual corresponde esa información.

- La Subgerente hace la custodia de los discos de backup de ANPRA, y los almacena en su residencia (no se tienen detalles si las condiciones son óptimas para poder proteger la integridad de la información almacenada). La confidencialidad de los datos almacenados en los discos se basa en la confianza obtenida a través de los años entre la Subgerente y el Gerente de la empresa.

- Debido a que no se realiza ningún tipo de revisión periódica de los datos almacenados en los discos, se desconoce si aún conservan la información contenida.

Nota: Es importante mencionar que en caso de que suceda algún tipo de percance donde se vean afectadas las instalaciones de ANPRA, es probable que ocurra una pérdida de datos en la información que no haya recibido un procedimiento de backups, debido a que el servidor de la empresa no cuenta con un mecanismo de replicación de datos en un lugar fuera de la empresa o con el servicio de una entidad que guarde las copias de seguridad de los elementos de software necesarios para asegurar el funcionamiento del sistema en la compañía.

Se propone una solución que podría ayudar en caso de ocurrir algún tipo de percance con las instalaciones de la empresa. La solución consiste en la contratación de los servicios de una empresa que custodie y almacene los datos de ANPRA de manera eficiente y segura, todo esto teniendo en cuenta que la importancia o el valor de la información debe justificar la inversión, debido a que esta propuesta puede resultar costosa. Estas empresas ofrecen una gran cantidad de servicios garantizando:

- Calidad: Instalaciones altamente equipadas con equipos de última generación, basados en los más altos estándares de calidad.

- Seguridad: El lugar donde se almacenan los datos están construidos con toda la seguridad necesaria contra temblores, incendios y cortocircuitos, muchas de estas empresas cuentan con un suministro eléctrico permanente.

Algunas de las razones por las cuales es necesario el uso de estos servicios son:

- La cantidad de datos almacenados en el servidor de la empresa va en aumento y por tanto su capacidad de almacenamiento se ha ido agotando.

- Inadecuadas condiciones de los lugares en los que se almacenan las copias de seguridad, ya que al momento de requerir los datos se podría provocar un mal funcionamiento de los discos afectando la integridad de la información.

- La necesidad de realizar copias continuas para que pueda garantizarse una recuperación completa de los datos en caso de sufrir alguna pérdida total de la información en el servidor de la empresa [14].

Esta propuesta va acompañada de la realización de replicas de la información de manera distribuida en los servidores que se encuentren en cada una de las sedes de la empresa, mediante la utilización de soluciones Open Source. Esta solución permite manejar un esquema de contingencia y continuidad del negocio en el caso de perdida o daño de información en alguna de las sedes. La metodología

propuesta para el procedimiento del almacenamiento y respaldo de los backups en cada una de las sedes, es la siguiente:

- Copia de cada sistema operativo utilizado dentro de la organización.
- Copia de cada uno de los programas utilizados en el negocio de la compañía.
- Copia de la base de datos del servidor (clientes, ventas, precios, personal laboral, etc.)
- Cada dato almacenado debe contar con un documento donde se registre: Identificación del archivo, aplicación que lo usa y longitud del archivo. Además deberá contener especificaciones como: Fecha, hora, persona que realiza el backup y por cual persona fue ordenado, este es un procedimiento tanto para los backups de software como de los datos.
- En el caso de software se registrará medio de almacenamiento, la versión, número de licencia y número de medios de almacenamiento que ocupa.
- Los medios magnéticos deberán ir etiquetados con la información pertinente de registro.
- El administrador de red debe hacer diariamente un respaldo de la información contenida en la base de datos de la empresa.
- Semanalmente se debe hacer un respaldo de toda la información útil para la empresa no contenida en la base de datos.
- El acceso a esta información debe estar restringido a personal no autorizado.
- Se debe establecer un periodo de revisión de toda la información guardada.
- El lugar donde estén guardadas todas las copias de seguridad, deben garantizar: confiabilidad, autenticidad, integridad y privacidad de la información[15].

d. Seguridad en sesiones de usuario

Se refiere al proceso de administrar en forma eficiente todas las cuentas de usuario que existan o que se encuentren habilitadas dentro de la empresa.

Actualmente dentro de ANPRA, no existe una persona que realice auditoria a las características, contraseñas y privilegios de las cuentas de usuario para el acceso a los datos e información sensible de la empresa. Para incrementar la seguridad

de las cuentas de usuario se deben tomar ciertas medidas y modificar algunos aspectos como:

- Las cuentas de "invitado" deben ser eliminadas de todos los computadores, así como también todas aquellas cuentas que fueron creadas para propósitos especiales o que pertenecían a empleados que ya no laboran en la empresa. Además, la cuenta Administrador debe ser renombrada para evitar ataques directos a ella.

- Las cuentas administrativas deben tener una copia de seguridad para evitar la pérdida de información en caso de que exista algún problema inesperado con la cuenta real.

- Se debe crear un conjunto de procedimientos referentes a la administración de archivos, correos y acceso de personal que ya no labora en la empresa.

- Se deben asignar permisos de manera obligatoria a los nuevos empleados que operen dentro de la red ANPRA, que sean supervisados por el respectivo personal encargado para evitar la asignación de recursos a personas que no deben tener acceso a ella.

- Dar carácter obligatorio al uso de una contraseña en cada una de las sesiones y establecer políticas que estén relacionadas con la seguridad en el manejo de las contraseñas de las sesiones, estableciendo el periodo de caducidad, tamaño de la contraseña, posibilidad para que esta no sea repetida [16].

e. Acceso Inalámbrico para los visitantes

La empresa ANPRA cuenta con un Access point marca D-Link ubicado en el departamento de bodega, el cual ofrece un servicio de conectividad inalámbrica a los visitantes y empleados de la empresa. Las redes inalámbricas cada día son más utilizadas, pero en muchas ocasiones no se tiene en cuenta los cuidados mínimos de configuración para evitar intrusiones sobre estas redes.

El problema de inseguridad inalámbrica que se presenta en ANPRA, radica en 2 situaciones:

- El Access point se encuentra conectado al Switch de la empresa el cual maneja una sola subred para darle direccionamiento IP a todos los departamentos, de esta manera permite la conectividad a Internet de todas las personas, tanto visitantes como empleados de la empresa. El problema radica en tener una conexión inalámbrica para los dos grupos debido a que personas ajenas tienen acceso a la misma red dejando en peligro el servidor y demás computadores que contienen información vital de la empresa. La solución a este problema es la ubicación de dos Access Point situados en distintas redes

creadas por el Router VYATTA. La primera red brindaría Internet inalámbrico de manera interna a los empleados de ANPRA y la segunda a los visitantes o compradores que lleguen a la empresa.

- El tipo de seguridad que tiene el Access Point para evitar el ingreso a la red de personas no deseadas es WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado), el problema es que actualmente éste ha sido roto en muchas ocasiones. Fácilmente se puede llegar a encontrar información y videos en páginas Web como "Youtube" y en motores de búsqueda con las instrucciones paso a paso para poder descubrir la contraseña de acceso. Por lo tanto, es recomendable utilizar el sistema de cifrado WPA (*Wi-Fi Protected Access* - 1995 - Acceso Protegido Wi-Fi), y restringir el acceso inalámbrico ya sea por identificación de MAC o IP de cada visitante.

f. Concienciación y entrenamiento del personal

La parte más insegura de cualquier red interna son las personas, por lo cual es necesario adoptar procedimientos y prácticas para educar al usuario teniendo en cuenta aspectos como:

- Establecer buenos hábitos y prácticas de seguridad para disminuir el riesgo de ser vulnerables ya sea contra ataques a la red, virus, códigos maliciosos, spam, etc., debido a que no es suficiente diseñar un esquema de seguridad si no se administra correctamente día a día.

- Realizar un esquema sencillo, viable y efectivo que supla las necesidades principales de la compañía, donde se establezcan buenas prácticas y se documenten los procedimientos relacionados con seguridad adoptando mecanismos para comprobar que los empleados los sigan, ya que si se tiene un esquema de seguridad robusto y complejo que sobredimensione las necesidades principales de la empresa, podría evitar que los empleados lo sigan de forma prudente.

- Se debe entrenar a todo el personal de la empresa enfocándose en las nuevas técnicas de seguridad adoptadas, para facilitar la unión entre los trabajadores y el intercambio de sus destrezas, conocimientos y experiencias de modo que se fomente un ambiente de continua formación, apoyo y responsabilidad, que mejore la calidad de trabajo maximizando de esta manera la utilización de las capacidades de los recursos humanos de ANPRA.

- Se deben acondicionar los puestos de trabajo en el que se le proporciona a los empleados la información, el conocimiento y los recursos requeridos, para desempeñarse óptimamente en sus labores e inculcarle a cada uno la idea de que es dueño de su propio trabajo [17].

3.2 ANÁLISÍS DE LA SEGURIDAD IMPLEMENTADA POR PARTE DEL SERVIDOR Y SERVICIOS CON LOS QUE CUENTA ANPRA Ltda.

Uno de los aspectos importantes en este proyecto, abarca el estudio del nivel de seguridad de los servicios ofrecidos por el servidor de ANPRA, para que de esta manera se encuentren los aspectos que hacen vulnerable a la empresa a partir de la seguridad que ella implementa en sus servicios a la infraestructura de red vista en el capitulo anterior. El análisis se hizo estudiando las características y mecanismos que la empresa utiliza para manejar toda la información sensible de la organización.

La empresa ANPRA cuenta con una infraestructura de red sencilla debido al número reducido de computadores distribuidos para cada una de las dependencias. Actualmente su seguridad se encuentra basada en la protección que brinda su servidor dentro de la empresa mediante el software ISA server 2004 y el hosting suministrado por CAMINOWEB que le brinda el servicio Web. Las políticas que se manejan en el servidor son las siguientes:

- ISA Server 2004

La empresa ANPRA, como mecanismo de "protección" cuenta con el firewall ISA Server 2004 con su configuración por defecto, es decir no se ha hecho ninguna modificación a las 30 políticas que vienen predefinidas llamadas Reglas de Directiva del Sistema. La modificación arbitraria de estas políticas, puede causar el mal funcionamiento en algunos servicios, por tanto es necesario tener un conocimiento previo para poder manipularlas.

REGLAS DE DIRECTIVA DEL SISTEMA

ORDEN	**NOMBRE**	**ACCION**
1	Permitir acceso a servicios de directorio para propósitos de autenticación.	Permitir

PROTOCOLOS	**DE/ESCUCHA**	**A**
-Catálogo global de LDAP -Catálogo global de LDAPS -LDAP -LDAP (UDP) -LDAPS	Host Local	Interna Controladores de dominio

- La habilitación de este grupo de configuración permite que el servidor ISA tenga acceso a los servicios de directorio, para propósitos de autenticación.

ORDEN	NOMBRE	ACCION
2	Permitir la administración remota desde equipos seleccionados que usan MMC	Permitir

PROTOCOLOS	DE/ESCUCHA	A
- Control de Firewall de Microsoft - Datagrama de NetBios - RPC - Servicio de nombres NetBios - Sesión NetBios	Equipos de admón. remota	Host Local

- Permite la administración remota del servidor ISA desde computadores seleccionados que usan Microsoft Management Console (MMC).

ORDEN	NOMBRE	ACCION
3	Permitir la administración remota desde equipos seleccionados por medio de terminal server	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-RDP (Servicios de Terminal Server)	Equipos de admón. Remota	Host Local

ORDEN	NOMBRE	ACCION
4	Permitir el registro remoto a servidores de confianza que usan NetBios	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Datagrama NetBios -Servicio de nombres NetBios -Sesión NetBios	Host Local	Interna

ORDEN	NOMBRE	ACCION
5	Permitir la autenticación RADIUS del servidor ISA a servidores RADIUS de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Contabilidad RADIUS	Host Local	Interna

ORDEN	NOMBRE	ACCION
6	Permitir la autenticación Kerberos del servidor ISA a servidores de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Kerberos-Sec (TCP) -Kerberos-Sec (UDP)	Host Local	Interna Controladores de dominio

- Permite que el servidor ISA tenga acceso a los servicios de directorio, para propósitos de autenticación.

ORDEN	NOMBRE	ACCION
7	Permitir DNS del servidor ISA hacia servidores seleccionados	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-DNS	Host Local	Todas las redes (y Host Local)

ORDEN	NOMBRE	ACCION
8	Permitir peticiones DHCP del servidor ISA a todas las redes	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-DHCP (petición)	Host Local	En cualquier lugar

ORDEN	NOMBRE	ACCION
9	Permitir peticiones DHCP del servidor ISA a todas las redes	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-DHCP (respuesta)	Host Local	Host Local

ORDEN	NOMBRE	ACCION
10	Permitir peticiones ICMP de equipos seleccionados al servidor ISA	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Ping	Equipos de admón. remota	Host Local

ORDEN	NOMBRE	ACCION
11	Permitir peticiones ICMP del servidor ISA a servidores seleccionados	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Marca de hora de ICMP -Petición de información de ICMP -Ping	Host Local	Todas las redes (y Host Local)

ORDEN	NOMBRE	ACCION
12	Permitir el trafico de cliente VPN al servidor ISA	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-PPTP	Externa	Host Local

ORDEN	NOMBRE	ACCION
13	Permitir el trafico VPN de sitio a sitio hacia el servidor ISA	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
	Externa Puerta de enlaces remotas IPSec	Host Local

ORDEN	NOMBRE	ACCION
14	Permitir el trafico VPN de sitio a sitio desde el servidor ISA	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
	Host Local	Externa Puertas de enlace remotas

ORDEN	NOMBRE	ACCION
15	Permitir CIFS de Microsoft del servidor ISA a servidores de confianza	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
-CIFS de Microsoft (TCP) -CIFS de Microsoft (UDP)	Host Local	Interna Controladores de dominio

ORDEN	NOMBRE	ACCION
16	Permitir el registro SQL remoto del servidor ISA a servidores seleccionados	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
-SQL de Microsoft (TCP) -SQL de Microsoft (UDP)	Host Local	Interna

ORDEN	NOMBRE	ACCION
17	Permitir HTTP/HTTPS del servidor ISA a sitios especificados	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
-HTTP -HTTPS	Host Local	Sitios permitidos de directiva del sistema

ORDEN	NOMBRE	ACCION
18	Permitir peticiones HTTP/HTTPS del servidor ISA a servidores seleccionados, para los comprobadores de conectividad	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
-HTTP -HTTPS	Host Local	Todas las redes (y Host Local)

ORDEN	NOMBRE	ACCION
19	Permitir el acceso de equipos de confianza al recurso compartido de instalación de cliente firewall en el servidor ISA	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-CIFS de Microsoft (TCP) -CIFS de Microsoft (UDP) -Datagrama NetBios -Servicio de nombre NetBios -Sesión NetBios	Interna	Host Local

ORDEN	NOMBRE	ACCION
20	Permitir la supervisión remota de rendimiento del servidor ISA desde servidores de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Datagrama NetBios -Servicio de nombre NetBios -Sesión NetBios	Equipos de admón. Remota	Host Local

ORDEN	NOMBRE	ACCION
21	Permitir NetBios del servidor ISA a servidores de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Datagrama NetBios -Servicio de nombre NetBios -sesión NetBios	Host Local	Interna

- Permite NetBios del servidor ISA a equipos de confianza, para propósitos de diagnóstico.

ORDEN	NOMBRE	ACCION
22	Permitir RPC del servidor ISA a servidores de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-RPC (todas las interfaces)	Host Local	Interna Controladores de dominio

- Permite que el servidor ISA tenga acceso a los servicios de directorio, para propósitos de autenticación.

ORDEN	NOMBRE	ACCION
23	Permitir HTTP/HTTPS del servidor ISA a sitios de informes de error de Microsoft especificados	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-HTTP Y HTTPS	Host Local	Sitios de informa de error de Microsoft

ORDEN	NOMBRE	ACCION
24	Permitir la autenticación SecurID del servidor ISA a servidores de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-SecurID	Host Local	Interna

- Permite que el servidor ISA tenga acceso a los RSA ACE/Server de confianza para la autenticación de SecurID.

ORDEN	NOMBRE	ACCION
25	Permitir la supervisión remota del servidor ISA a servidores de confianza, por medio del agente MOM	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-Agente de Microsoft Operation Manager	Host Local	Interna

- Permite la supervisión remota del servidor ISA por medio de Microsoft Operations Manager (MOM).

ORDEN	NOMBRE	ACCION
26	Permitir todo el trafico HTTP desde el servidor ISA hacia todas las redes (para las descargas de CRL)	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-HTTP	Host Local	Todas las redes (y Host Local)

- Permite descargar la versión mas reciente de la lista de revocación de certificados (CRL) por medio de protocolo HTTP. La CRL se descarga automáticamente cuando llega un nuevo certificado.

ORDEN	NOMBRE	ACCION
27	Permitir NTP del servidor ISA a servidores NTP de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-NTP (UDP)	Host Local	Interna

- Permite el protocolo de tiempo de red (NTP) del servidor ISA a servidores de confianza.

ORDEN	NOMBRE	ACCION
28	Permitir SMTP del servidor ISA a servidores NTP de confianza	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-SMTP	Host Local	Interna

ORDEN	NOMBRE	ACCION
29	Permitir HTTP del servidor ISA a equipos seleccionados, para trabajos de descarga de contenidos	Permitir

PROTOCOLOS	DE/ESCUCHA	A
-HTTP	Host Local	Todas las redes (y Host Local)

ORDEN	NOMBRE	ACCION
30	Permitir la comunicación de Control de Firewall de Microsoft a equipos seleccionados	Permitir
PROTOCOLOS	**DE/ESCUCHA**	**A**
Todo el tráfico saliente	Host Local	Equipos de admón. remota

ORDEN	NOMBRE	ACCION
31	Regla predeterminada	Denegar
PROTOCOLOS	**DE/ESCUCHA**	**A**
Todo el tráfico	Todas las redes (y Host Local)	Todas las redes (y Host Local)

- Regla de acceso predefinido que protege las redes al bloquear todo tráfico que no este permitido explícitamente por otras reglas de acceso definidas por usuarios. Esta regla siempre se procesa al final de todas.

El servidor de la empresa contiene la base de datos donde almacena toda la información correspondiente a empleados, clientes, facturación, cartera y características de los productos que comercializa. Brinda también, el servicio de correo (usuario@anpra.com) y servidor proxy. El Hecho de habilitar o instalar gran cantidad de servicios o protocolos da lugar a tener mayor cuidado en la configuración de cada uno de ellos, esto sucede porque se aumentan las posibilidades para que una persona pueda ingresar a la red de manera no autorizada. ANPRA con el fin de reducir la posibilidad de ataques al servidor Web, optó por adquirir los servicios de una empresa especializada en hosting y venta de nombres de dominios llamada Caminoweb, la cual se encarga de brindar la seguridad necesaria del hosting, dejándole a la empresa ANPRA, una total administración de la página web. El servidor Web es un servicio que puede ser atacado debido a que se debe programar adecuadamente teniendo en cuenta bloquear, restringir y deshabilitar ciertas funciones que están por defecto y sirven como una puerta de entrada para los atacantes.

La Empresa, hace uso del plan *Extra de Windows*, (ver Figura 3), y su nombre de dominio es www.anpra.com suministrado por Caminoweb, para brindar el servicio [18].

Figura 3. Plan de servicios ofrecido por Caminoweb.

Qué plan debo comprar?	PLANES LINUX			PLANES WINDOWS		
	Micro	Básico	Extra	Micro	Básico	Extra
	Comprar	Comprar	Comprar	Comprar	Comprar	Comprar
Valor Anual Pesos	$84,000	$126,000	$168,000	$105,000	$147,000	$210,000
Espacio en Disco (MB)	50	400	800	50	400	800
Trafico Mensual (GB)	2	5	10	2	5	10
Dominio Incluido	1	1	1	1	1	1
Subdominios	5	10	20	5	10	20
Cuentas de E-Mail POP3	5	20	200	5	20	200

Tomado de caminoweb.com

3.2.1 Análisis del servidor de la empresa ANPRA Ltda. por medio del uso de herramientas de detección de vulnerabilidades

El uso de herramientas especializadas en el estudio y análisis de vulnerabilidades presentes en una red, ayudan en la ardua tarea de reconocer las deficiencias con las que cuenta la seguridad actual implementada en ANPRA. A continuación se hará un análisis al servidor de la empresa, utilizando las siguientes herramientas para encontrar qué deficiencias podrían afectar su funcionamiento:

Tabla 2. Herramientas de Análisis de Vulnerabilidades utilizadas.

Tipo de Herramienta	Versión	Fecha de inicio	Fecha de Finalización
Shadow Security Scanner	Version 7.131	02-04-08	04-04-08
Nessus	Versión 3.2.0	03-04-08	03-04-08
NMap	Versión 4.60	03-04-08	03-04-08

Nessus es un software libre que se utiliza para escanear redes, la selección de este programa se hace debido a la facilidad de manejo y al informe detallado que muestra de las vulnerabilidades del sitio y los posibles ataques que se pueden hacer a esa vulnerabilidad para aprovecharla. Nmap al igual que Nessus es un software libre que sirve para hacer un rastreo más detallado de los puertos TCP y UDP abiertos de una máquina, además muestra servicios que corren en dicha maquina y deficiencias que la hacen vulnerable. Estos dos programas aparecen

en el top 15 security/hacking Tools & utilities en el puesto uno y dos de la página www.darknet.org.uk. Shadow Security Scanner es considerado uno de los mejores analizadores en entornos Windows debido a su base de datos actualizada en cuanto a vulnerabilidades se refiere. Se escogió este programa debido a las características y opciones de ataques que vienen con el programa junto a los tipos de escáner separados que hacen un análisis detallado de servicios de manera individual.

1) Nessus

Es una herramienta que realiza un análisis de los puertos del computador objetivo, contiene una gran lista de plugins los cuales se actualizan periódicamente para realizar las pruebas de vulnerabilidad y buscar cuales puertos se encuentran abiertos y cuáles de ellos pueden ser explotados [19].

Se realizó un análisis con la herramienta Nessus al servidor de la empresa ANPRA, fueron analizados todos los puertos y se obtuvieron los siguientes resultados:

- **Reporte del analizador (Scan)**

Tabla 3. Resultado del análisis de Nessus al servidor de la empresa.

Escaneo	Computador	200.21.238.18
	Hora de inicio	17:33:27
	Hora de finalización	17:51:25
	Tiempo total de ejecución	00:18:58
Descripción	El servicio SMTP está activo en el puerto 25. Este servicio es blanco de SPAM, como recomendación se debe desactivar si no se utiliza	
Solución	Deshabilitar el servicio si no se utiliza o filtrar el tráfico entrante a este puerto	

El análisis realizado con la herramienta Nessus no encontró ninguna vulnerabilidad para ser explotada en el servidor que corresponde a la empresa ANPRA.

2) Nmap

Además de obtener la lista de puertos abiertos al ejecutar Nmap, con este software se puede obtener información adicional como: el nombre de DNS, listado de sistemas operativos posibles y direcciones MAC.

Hora de ejecución del escaneo:

Hora de inicio: 15:53
Hora de finalización: 16:20
Tiempo total de ejecución de la herramienta: 00:27

Mediante la herramienta Nmap se realizaron 2 tipos de análisis:

a. Análisis Intensivo (Intense Scan):

Para realizar un análisis intensivo se utiliza el siguiente comando con las variables –T, Aggresive, -A y –V.

Nmap –T Aggressive –A –v 200.21.238.18

- **-T:** Comando para elegir la plantilla de tiempo que se desea, se puede especificar cualquiera de estas opciones: paranoid, sneaky, polite, normal, aggressive and insane (sigiloso, amable, normal, agresivo y loco) respectivamente.

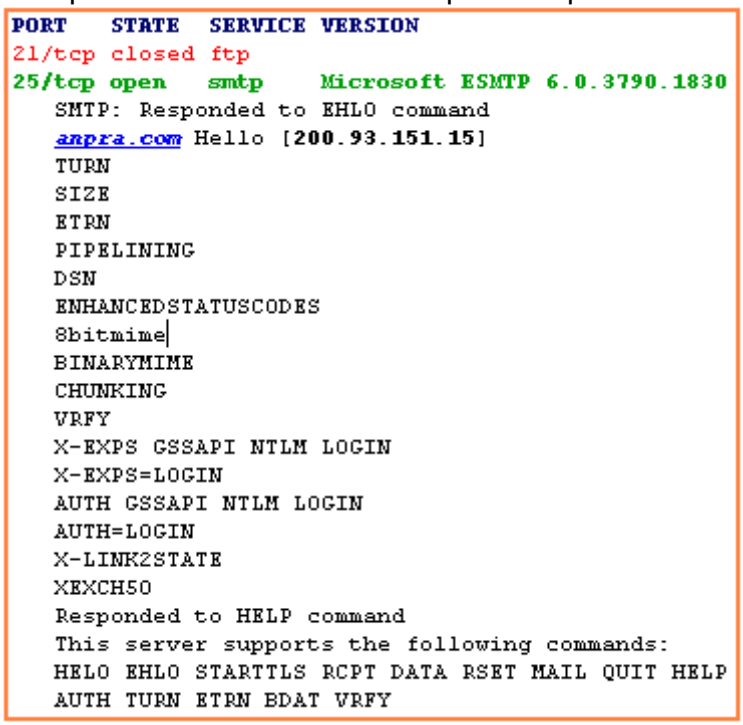
- **Aggressive:** Esta plantilla de tiempo hace que los sondeos no sean demorados, se utiliza cuando la red es rápida y fiable, mientras que con el uso de plantillas como paranoid se consume menos recursos del sistema y ancho de banda, aumentando el tiempo de los sondeos, por otra parte si se utiliza la plantilla insane se realiza un sondeo muy rápido, consumiendo gran recurso del sistema y al mismo tiempo sacrificando fiabilidad por velocidad.

- **-A:** Habilita la detección de SO (Sistema Operativo) y de versión del mismo.

- **-v:** Muestra el número de la versión del sistema operativo.

✓ **Función Salida Nmap (Nmap Output)**

Figura 4. Reporte del análisis con Nmap de los puertos del servidor.

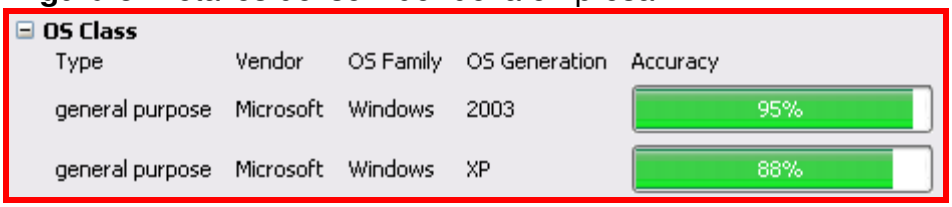


La herramienta detecta dos puertos TCP (ver Figura 4), el puerto 21 correspondiente al servicio FTP se encuentra cerrado y el puerto 25 correspondiente al servicio SMTP se encuentra abierto, con la versión Microsoft ESMTP 6.0.3790.1830. La estructura mostrada (turn, size, pipeling, etc.) corresponde a las extensiones utilizadas en la identificación entre el servidor SMTP y los clientes. En Tech-FAQ, una página encargada del estudio de todo el tema de comunicaciones expone tres métodos que pueden ser configurados para una comunicación SMTP segura: *Autenticación Básica, Autenticación Anónima y la Autenticación Integrada de Windows.* En la autenticación básica se establece un nivel no complicado de seguridad, para acceder el cliente establece el nombre de usuario, nombre de dominio y password. La Autenticación Anónima es típica para la comunicación de Internet y soportada por todos los clientes. Esta autenticación se utiliza para limitar el acceso a carpetas públicas y directorios. Y por último la Autenticación Integrada de Windows; este tipo de autenticación soporta seguridad y eficiencia en la comunicación debido a que los passwords son transmitidos en una forma encriptada. En este caso donde la versión es superior a la Windows 2000, se utiliza kerberos.

✓ **Función Detalles de los Equipos (Host Details)**

Muestra la información correspondiente a los sistemas operativos y las versiones con las que cuenta el servidor de la red de ANPRA.

Figura 5. Detalles del servidor de la empresa



Claramente se puede observar en la figura anterior que la herramienta Nmap es efectiva ya que pudo establecer los sistemas operativos y versiones presentes en la red de ANPRA, con altos los porcentajes de exactitud. En general con este tipo de escáner no se encontró ninguna vulnerabilidad presente en el equipo.

b. Escaneo rápido y detallado (Quick and verbose scan)

Para realizar un escaneo rápido y detallado se utiliza el siguiente comando con las variables –d, -T, Aggresive, -packect_trace, -v y –n.

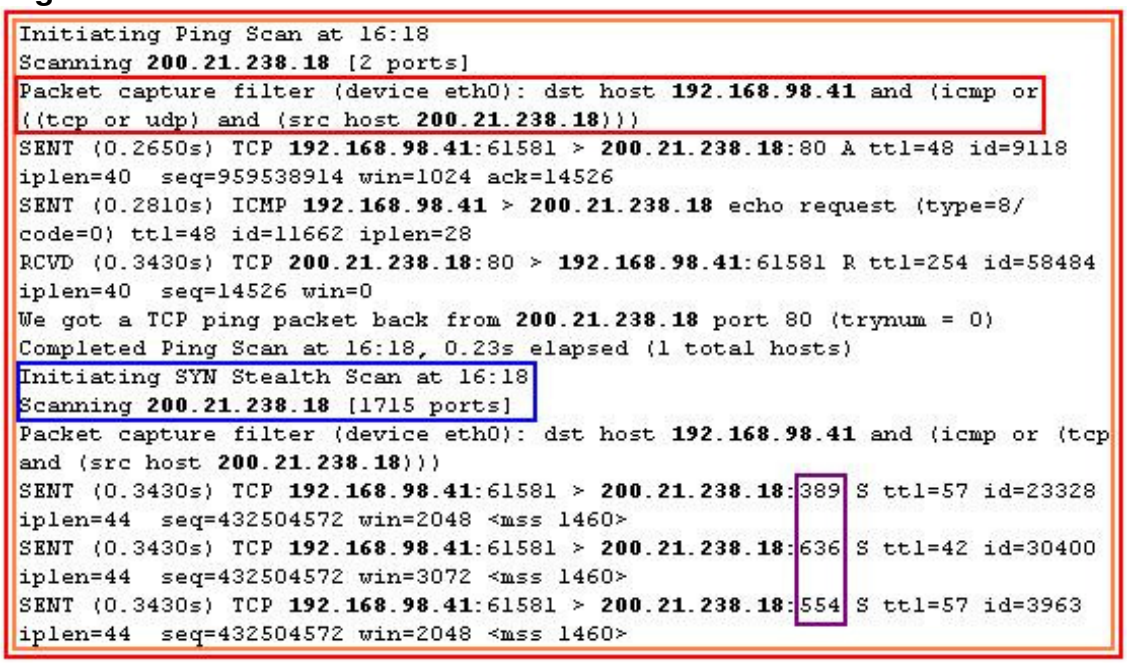
Namp –d –T Aggressive –packet_trace –v –n 200.21.238.18

- **-d:** Fija o incrementa el nivel de depuración (Proceso de identificar y corregir errores de programación).
- **--packet-trace:** Muestra todos los paquetes enviados y recibidos.
- **-n:** No resuelve el DNS, es decir, no traduce la dirección IP en un nombre de dominio.

✓ **Función Salida Nmap (Nmap Output)**

Después de realizar el escáner con la función anterior, los resultados obtenidos de la herramienta se muestran en el siguiente grafico.

Figura 6. Resultados del escáner al servidor de ANPRA.



Puerto donde se envían los SYN “invisibles” a la dirección IP: 200.21.238.18.

Indica el filtrado de paquetes ICMP, TCP o UDP en la dirección IP: 200.21.238.18.

Por medio de SYN “invisibles” se realiza una petición de conexión en 1775 puertos de la dirección IP: 200.21.238.18.

La herramienta envía SYN “invisibles” a 1715 puertos correspondientes al servidor de ANPRA, se realiza de esta manera para que el firewall no se alerte y bloquee este tipo de escaneo.

Al finalizar el escáner realizado en 1715 puertos al servidor de la empresa, se observa que 1713 puertos no respondieron a los SYN fantasmas, solo 2 puertos fueron identificados, el puerto 21 correspondiente a FTP el cual se encuentra cerrado y el puerto 25 correspondiente a SMTP el cual se encuentra abierto e indica la confirmación de la conexión, pero no indica ningún establecimiento de conexión de 3 fases (3 way handshake). No se encontraron vulnerabilidades.

3) Shadow Security Scanner (SSS)

Esta herramienta detecta por medio del escáner de puertos vulnerabilidades presentes es servicios como: FTP, SSH, Telnet, SMTP, DNS, HTTP, POP3, Windows Media Service, NetBIOS, SSL, TCP/IP y UDP. Realiza un análisis muy detallado descubriendo las vulnerabilidades presentes y sus posibles soluciones [20].

Se realizó un análisis de vulnerabilidades al servidor de la empresa ANPRA, mediante los diferentes tipos de escáner con los que cuenta la herramienta: Full Scan, Only NetBIOS Scan, Only FTP Scan, Only HTTP Scan, SANS/FBI TOP 20 Scan y DoS Checker.

a. Análisis Total (Full Scan)

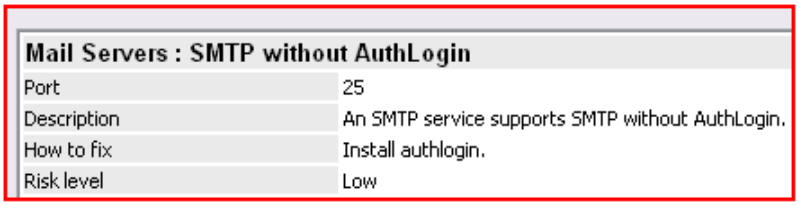
Por medio de esta opción se escanean todos los puertos (1 – 65355) y posibles vulnerabilidades del servidor de la empresa ANPRA.

Tabla 4. Información general del análisis total al servidor.

General	Dirección IP	201.21.238.18
	Nombre del Equipo	mail.sistelec.com.co
	Inicio del escaneo	02/04/2008 02:01:24 p.m.
	Finalización del escaneo	03/04/2008 01.33.27 a.m.

Reporte:

Figura 7. Resultados del análisis total mediante SSS al servidor.



El riesgo mostrado en la Figura 7, hace referencia al Protocolo Simple de Transferencia de Correo. La Empresa ANPRA, al momento de instalar su nuevo servidor, habilitó SMTP con su configuración por defecto, por tal razón la opción de AuthLogin no utiliza ningún modo de autenticación de los explicados en el reporte anterior de *Intense Scan* (ver Figura 4), las contraseñas de los usuarios son enviadas con la configuración que el protocolo *kerberos* utiliza. Estas características de seguridad se pueden cambiar en la configuración del servidor especificando el tipo de autenticación que se va a utilizar para que las contraseñas viajen seguras al momento de utilizar este tipo de servicio.

b. Análisis de sólo NetBIOS (Only NetBIOS Scan)

Se realiza el escaneo de las posibles vulnerabilidades presentes en la NetBIOS del servidor de la empresa ANPRA.

Tabla 5. Resultados de Only NetBIOS Scan al servidor.

General	Dirección IP	200.21.238.18
	Nombre del Equipo	mail.sistelec.com.co
	Inicio del escaneo	04/04/2008 11:15:33 a.m.
	Finalización del escaneo	04/04/2008 11:16:05 a.m.
Vulnerabilidades	Ninguna	
Estadísticas	Máquina	200.21.238.18
	Estado	Escaneo completo. (100%)
	Puertos auditados	0
	Puertos TCP	0

No se encontró ninguna vulnerabilidad presente en la ejecución del escáner NetBIOS al servidor de la empresa.

c. Análisis de solo FTP (Only FTP Scan)

Se realiza el escaneo de las posibles vulnerabilidades presentes en el Protocolo de Transferencia de Archivos (FTP) del servidor de la empresa.

Reporte:

Tabla 6. Resultados del análisis Only FTP Scan al servidor.

General	Dirección IP	200.21.238.18
	Nombre del Equipo	mail.sistelec.com.co
	Inicio del escaneo	04/04/2008 11:34:35 a.m.
	Finalización del escaneo	04/04/2008 11:35:01 a.m.
Puertos TCP	Puerto 21	FTP
Vulnerabilidades	Ninguna	
Estadísticas	Máquina	200.21.238.18
	Estado	Escaneo completo. (100%)
	Puertos auditados	0
	Puertos TCP	0
	Puertos UDP	0

No se encontró vulnerabilidad presente en la ejecución del escáner Only FTP.

d. Análisis de solo HTTP (Only HTTP Scan)

Se realiza el análisis de las posibles vulnerabilidades presentes en el Protocolo de Transferencia de Hipertexto (HTTP) del servidor de la empresa ANPRA.

Tabla 7. Resultados de Only HTTP Scan al servidor.

General	Inicio del escaneo	04/04/2008 11:41:13 a.m.
	Finalización del escaneo	04/04/2008 11:41:44 a.m.
Vulnerabilidades	Ninguna	
Estadísticas	Estado	Escaneo completo. (100%)
	Puertos auditados	0
	Puertos TCP	0
	Puertos UDP	0

El análisis realizado con la herramienta Only http Scan no encontró ninguna vulnerabilidad para ser explotada en el servidor que corresponde a la empresa ANPRA.

e. Análisis del Top 20 de SANS/FBI (SANS/FBI Top 20 Scan)

Se realiza el escaneo de las posibles vulnerabilidades presentes en el Top 20 de la SANS/FBI del computador 200.21.238.18 correspondiente al servidor de la empresa ANPRA.

Reporte:

Tabla 8. Resultado de SANS/FBI Top 20 Scan al servidor.

Escaneo	Computador	200.21.238.18
General	Dirección IP	200.21.238.18
	Nombre del Equipo	mail.sistelec.com.co
	Inicio del escaneo	04/04/2008 11:43:09 a.m.
	Finalización del escaneo	04/04/2008 11:44:07 a.m.
Puertos TCP	Puerto 21	FTP- Protocolo de Transferencia de Archivos
	Puerto 25	SMTP – Protocolo Simple de Transferencia de Correo
Vulnerabilidades	Ninguna	
Estadísticas	Máquina	200.21.238.18
	Estado	Escaneo completo. (100%)
	Puertos auditados	0
	Puertos TCP	2
	Puertos UDP	0

El análisis realizado con la herramienta SANS/FBI Top 20 Scan encontró dos puertos abiertos sin ninguna vulnerabilidad para ser explotada en el servidor que corresponde a la empresa ANPRA.

f. DoS Checker

Shadow Security Scanner cuenta con un modulo de pruebas de resistencia ante ataques de denegación de servicios (DoS), solo es necesario ingresar a la función **DoS Checker** para poder visualizar los iconos correspondientes a los servicios disponibles que pueden ser atacados desde esta herramienta [21].

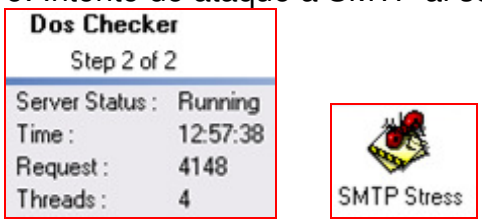
1. HTTP (Hypertext Transfer Protocol)
2. SMTP (Simple Mail Transfer Protocol)
3. FTP (File Transfer Protocol)
4. POP3 (Post Office Protocol)
5. IMAP (Internet Message Access Protocol)

Al momento de elegir uno de estos servicios es necesario ingresar la dirección IP del computador a atacar, además de los datos como puerto, retardo y tamaño de los paquetes, (ver Figura 8). El programa comienza a atacar el servicio, indicando en la ventana el estado del ataque (Running) demostrando que el servicio aún está corriendo sobre el computador, si llegado el caso ocurre una denegación de servicios, en el estado del ataque cambia a (Down) indicando que el servicio está abajo.

Figura 8. Opción de denegación de servicios

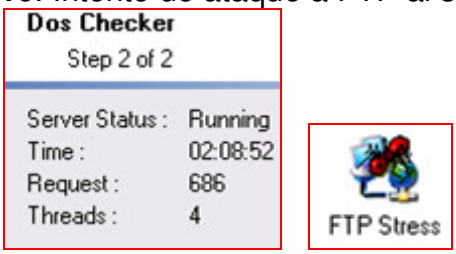
Al realizarse el análisis Total (Full Scan) fueron detectados 2 puertos TCP disponibles en el servidor de la empresa ANPRA, el puerto 21 correspondiente a FTP (Protocolo de Transferencia de archivos) y el puerto 25 correspondiente a SMTP (Protocolo Simple de Transferencia de Correo), por tanto se realizaron pruebas con DoS Checker a los puertos 21 y 25 durante un tiempo considerable obteniendo los siguientes resultados:

Figura 9. Intento de ataque a SMTP al servidor.



Se ejecutó el DoS Checker tratando de crear una denegación de servicios al servicio SMTP, pero luego de casi 13 horas de envío de paquetes el estado del servidor está funcionando, indicando que no hubo éxito en el intento de denegación de servicios.

Figura 10. Intento de ataque a FTP al servidor.



Se ejecutó el DoS Checker tratando de crear una denegación de servicios al servicio FTP, pero luego de 2 horas de envío de paquetes el estado del servidor está funcionando, indicando que no hubo éxito en el intento de denegación de servicios.

Nota: En los resultados obtenidos del estudio realizado anteriormente por cada una de las herramientas y el análisis que se hace a partir de ellas, aportan como conclusión que la red aparenta una seguridad aceptable. Se puede observar claramente que cada una de ellas califica las deficiencias encontradas en (Alto, Medio, Bajo o Ninguno), en el caso de la red correspondiente a la empresa ANPRA, solo fue encontrado un problema con riesgo bajo mediante la herramienta Shadow Security Scanner, mientras que con las demás herramientas no se detectó ningún tipo de vulnerabilidad.

3.3 ANÁLISIS DEL TRÁFICO DE RED ANPRA Ltda.

Para una buena comunicación entre las dos sedes es necesario que exista un ancho de banda adecuado que permita el envío y recepción de paquetes sin ninguna dificultad. Se estudiará el tráfico de red que tiene la empresa ANPRA, analizando el comportamiento de los paquetes, para establecer un informe que demuestre la manera en que es aprovechado el ancho de banda y definir si cumple con las necesidades que requiere la interconexión entre las dos sedes.

3.3.1 Análisis del tráfico

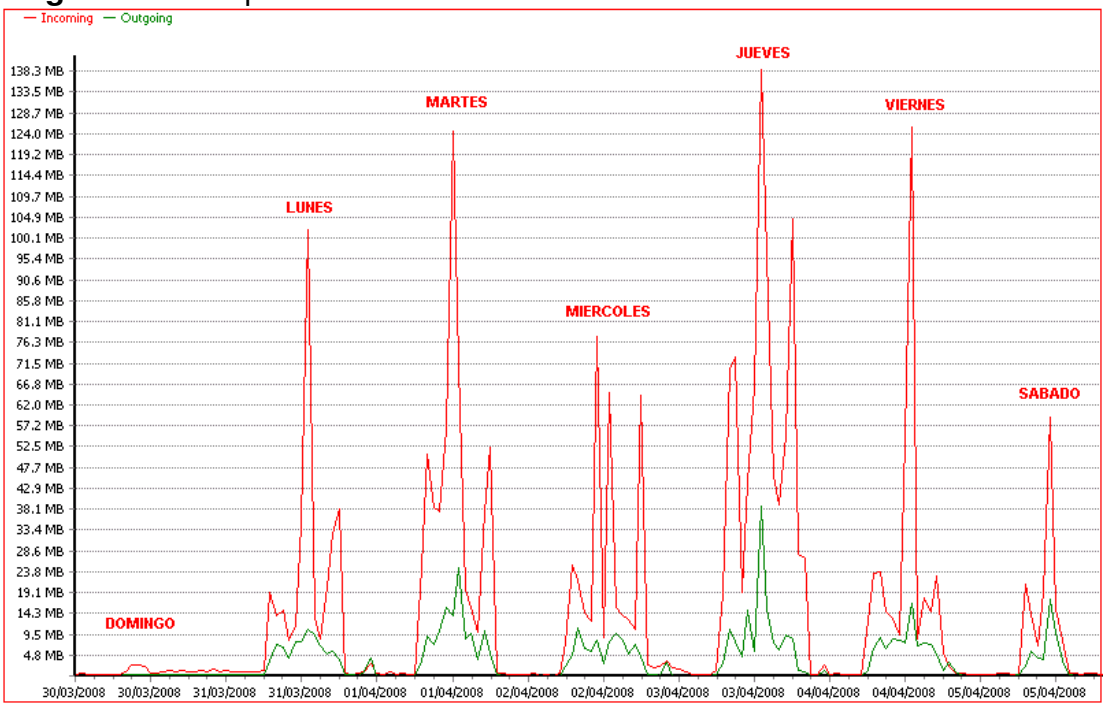
El análisis que se presenta en este proyecto, corresponde al tráfico generado entre la semana del 28 de marzo y 5 de abril por parte de la red de ANPRA, se utilizaron varias herramientas confiables para observar la desviación de valores que podría haber una de otra y obtener resultados aceptables. Se utilizaron tres herramientas para el estudio del tráfico en la red: AnalogX Netstat Live por su supervisión y muestra del tamaño en tiempo real de los datos que se transfieren por la red, BW meter por las gráficas que se obtienen fáciles de analizar de todo el tráfico y finalmente wireshark por la información detallada que suministra de cada uno de los datos que son transmitidos.

Tabla 9. Herramientas de estudio del tráfico de red.

Tipo de Herramienta	Versión	Fecha de inicio	Fecha de Finalización
AnalogX Netstat Live	2.11	28-03-08	05-04-08
BW meter	2.5	28-03-08	05-04-08
Wireshark	0.99.7	28-03-08	25-04-08

La Figura 11 se obtuvo del programa BW meter, muestra la cantidad de archivos que se enviaron (Outgoing) de color verde y la cantidad de archivos que se recibieron (Incoming) de color rojo, durante toda la semana correspondiente al 30 de marzo hasta el 5 de abril.

Figura 11. Comportamiento del tráfico de red.



En esta figura se puede apreciar lo siguiente:

- La mayor transferencia se hizo el día jueves 3 de abril, con 833.4 MB descargados y 136.3 MB enviados para un total de 969.6 MB de datos transferidos durante ese día.

- La hora con mayor transferencia de datos fue la 1:00 PM del día jueves 3 de abril con un total de 138.7 MB descargados y 38.7 MB enviados, para un total de 177.3 MB de datos transferidos durante esa hora.

- La menor transferencia se hizo el día lunes 31 de Marzo, con 329.6 MB descargados y 85.6 MB enviados para un total de 415.2 MB de datos transferidos durante ese día, ver Figura 12.(Datos obtenidos de BW meter)

- Según el reporte del trafico semanal, la cantidad total de archivos enviados durante la semana fue 580.7 MB y recibidos 2.5GB para un total de 3.1GB de datos transferidos entre el domingo 30 de Marzo al sábado 5 de Abril. (Datos obtenidos con BW meter)

Figura 12. Cantidad de datos transferidos por la red..

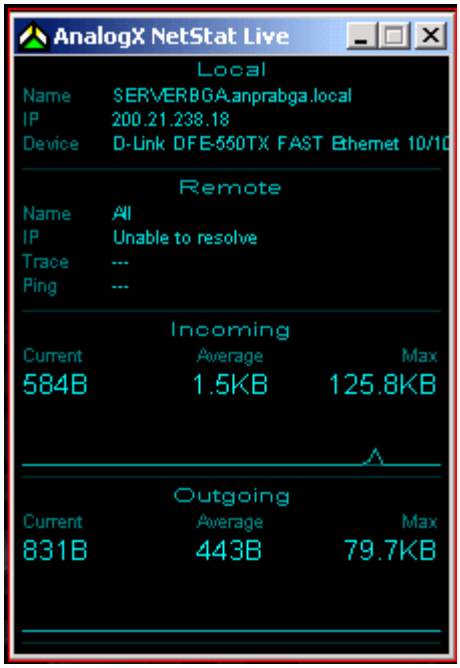
Daily Report

Time span: 31 days

Date	Recv.	Sent	Total
05/04/2008	151.0 MB	48.5 MB	199.5 MB
04/04/2008	352.1 MB	95.8 MB	447.9 MB
03/04/2008	833.4 MB	136.3 MB	969.6 MB
02/04/2008	362.9 MB	87.0 MB	450.0 MB
01/04/2008	543.8 MB	122.5 MB	666.2 MB
31/03/2008	329.6 MB	85.6 MB	415.2 MB
30/03/2008	22.9 MB	5.0 MB	27.9 MB

- La mayor velocidad de transferencia de descarga fue de 125.8 KB/s y de envío 79.7KB/s, ver Figura 13. Teniendo en cuenta que la capacidad del canal es de 512 KB/s, si estas velocidades se presentaran en un mismo instante se estaría ocupando casi el 50% de la capacidad del canal.

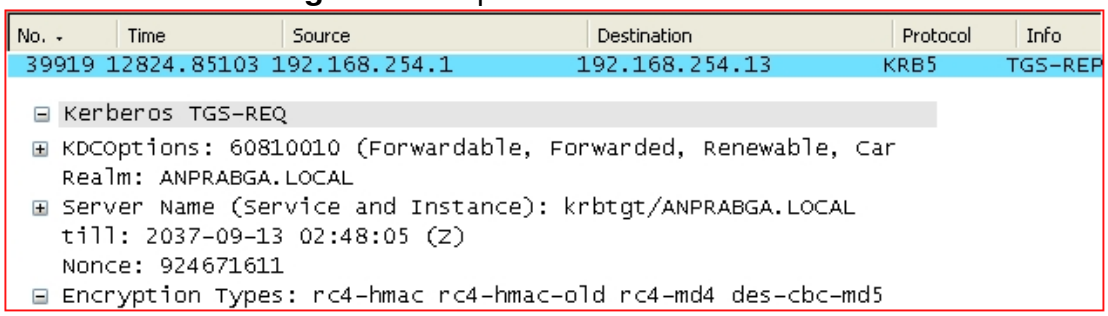
Figura 13. Velocidades de transferencia de la red.



- Se hizo un registro de 781 procesos en la red de ANPRA sin encontrar en alguno de ellos una amenaza para la red interna de la empresa.

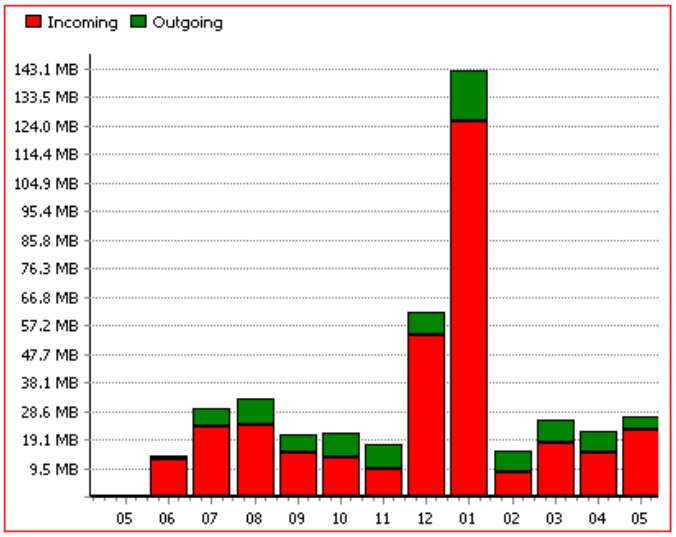
- Las sesiones de usuario y contraseñas, son manejadas por medio de un programa de autenticación llamado KERBEROS, instalado en el Windows Server 2003 de la empresa. El cliente se autentica por medio del servidor en solicitud de un ticket, que permitirá posteriormente utilizar el servicio. De esta manera todas las contraseñas que viajen dentro de la red de la empresa se encontrarán cifradas bajo el sistema de autenticación rc4 (*sistema de cifrado de flujo*) utilizado por el protocolo de autenticación de KERBEROS. En la Figura 14. se muestra un instante de tiempo en el que una de las máquina de la empresa con nombre de cliente ANPRABGA.LOCAL trata de establecer sesión con el servidor haciendo uso del servicio KERBEROS (datos tomados de Wireshark) [22].

Figura 14. Captura de tráfico de la red.



- Según el reporte del tráfico diario, el comportamiento por día del tráfico de red es similar al mostrado en la figura 15, la máxima transferencia de datos se presenta diariamente a la una de la tarde. Esto se debe a que en ese instante (hora de almuerzo) la mayoría de personas que permanecen en la empresa se dedican a bajar archivos totalmente ajenos a la información manejada y enviada por parte de ANPRA (datos tomados de BWMeter).

Figura 15. Tráfico de red en un día aleatorio de la red.



4. ANÁLISIS DE LAS SOLUCIONES COMERCIALES Y OPEN SOURCE PARA IMPLEMENTACIÓN DE ROUTERS

En este capítulo se analizarán las soluciones comerciales y Open Source de manera separada, estudiando las características y funciones más importantes de cada una de ellas, Además se hará una comparación entre las herramientas Open Source y las licenciadas para que finalmente se pueda establecer la herramienta que posea las características indicadas para el desarrollo del proyecto.

4.1 ANÁLISIS DE LAS SOLUCIONES COMERCIALES

El análisis que se hará a continuación está enfocado al aspecto económico y a las características más importantes de los dispositivos de enrutamiento de 3 empresas reconocidas como CISCO, 3COM y NORTEL.

- **CISCO Systems, Inc[1].**

Cisco es una empresa creada en el año de 1984 por un grupo de científicos de la Universidad de Stamford, California (USA). Dentro de su amplia gama de productos se seleccionó un Router que puede suplir con las necesidades de ANPRA.

Figura 16. Router CISCO2811

Tomado de Hardware.com

Este Router es la nueva serie que reemplaza a la serie Cisco2600, con mejoras en la disponibilidad, fiabilidad y desempeño. Estas son algunas de sus características:

[1] Los precios fueron tomados de la página web: http://us.hardware.com en el mes de marzo de 2008.

- Dos puertos 10/100 Fast Ethernet integrados.
- Hardware de encriptación.
- QoS (calidad de servicio).
- Protocolos de interconexión de datos Ethernet y FastEthernet.

El costo de este dispositivo es de 2.495.oo dólares.

Nota: El precio de este artículo no incluye tarjetas de red, DRAM memory y compact flash memory.

- Si se desea agregar una tarjeta con 4 conexiones 10/100 Ethernet, tiene un costo adicional de: 425.oo dólares.
- La memoria DRAM de 256 MB tiene un costo adicional de 660.oo dólares.
- La Compact Flash Memory de 64 MB tiene un costo adicional de 140.oo dólares.

El costo total de un Router Cisco con todas las características anteriormente mencionadas es de 3.720.oo dólares [23].

- **Router 3COM**

3COM es una compañía de gran trayectoria que provee soluciones de networking a nivel mundial, está enfocada en brindar una excelente calidad a bajo costo. En su variedad de dispositivos se encontró un Router que se ajusta a las necesidades de ANPRA, ver la Figura 18.

Figura 17. Router 3Com, Ref. 3033

Tomado de Hardware.com

Este Router cuenta con las siguientes características:

- 4 puertos de Switching 10/100
- Seguridad y control avanzado, VPN, Firewall y Encriptación
- Integración de voz y datos: QoS, Routing Multicast
- Memoria DRAM de 64 MB
- Memoria flash de 8 MB

El costo total de este dispositivo es de 1.059.oo dólares[2].

Tabla 10. Descripción técnica del Router 3-Com® Router 3033[3].

Descripción del producto	3-Com Router 3033
Tipo de dispositivo	Encaminador + conmutador de 4 puertos (integrado)
Factor de forma	Externo
Dimensiones (Ancho x Profundidad x Altura)	30 cm. x 18 cm. x 4.5 cm.
Peso	1 Kg.
Localización	Europa
Memoria RAM	64 MB SDRAM
Memoria Flash	8 MB
Protocolo de direccionamiento	OSPF, BGP-4, RIP-1, RIP-2, IGMP, VRRP, PIM-SM, PIM-DM, GRE
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	L2TP, IPSec, PPPoE, PPPoA
Protocolo de gestión remota	SNMP 1, SNMP 2, Telnet, SNMP 3
Características	Protección Firewall, Encaminamiento IP, soporte de NAT, asistencia técnica VPN, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), Stateful Packet Inspection (SPI), prevención contra ataque de DoS (denegación de servicio), activable.

[2] El precio fue tomado de la página web: http://www.3com.com, en el mes de marzo de 2008.
[3] Tomado de http://www.ciao.es/3Com_Router_3033 en el mes de marzo de 2008.

- **Router NORTEL**

NORTEL es una compañía encargada de diseñar e innovar tecnología referente a computación, redes, aplicaciones y usuarios finales. Muchas de sus soluciones tales como tecnologías de voz, inalámbrica, óptica y manejo de paquetes impulsan día a día el comercio entre zonas distantes ofreciendo seguridad en su comunicación. En su gama de dispositivos se encontró un Router interesante que ayudaría a suplir las necesidades de conexión de ANPRA.

Figura 18. Router NORTEL, Ref. Secure Router 4134

Tomado de NORTEL.COM

El Router Nortel Secure 4134 es el nuevo miembro de la familia Secure Router, su diseño modular soporta una variedad de servicios de red avanzados, incluyendo enrutamiento entre los protocolos IPv4 e IPv6, tecnología WAN de alto rendimiento, alta densidad de conmutación Ethernet, Voz sobre IP (VoIP) y seguridad en una sola plataforma integrada. Con sus capacidades y alto rendimiento, dirige las necesidades de Routing y conectividad que requiere la empresa y necesidades de conectividad para cada uno de los departamentos internos. La versión que cuenta con las siguientes características tiene un precio de 8.345.oo dólares[4] [24].

[4] El precio fue tomado de la página web: http://products.nortel.com/, en el mes de marzo de 2008.

Tabla 11. Características técnicas del Secure Router 4134

Peso Actual	22 libras
Contenido	Chasis, documentación
Memoria	128 MB
Puertos	Chassis Slots: 3 medium module slots 4 small module slots 1 large module slot (combining 2 medium slots) 2 x 10 / 100/1000 Ethernet copper / 2 x GigE SFP Fiber ports Management ports: Compact Flash USB Fast Ethernet Auxiliary and Console ports RJ-45

Tomado de http://pc.pcconnection.com

4.2 ANÁLISIS DE SOLUCIONES OPEN SOURCE

- **VYATTA**

Es un Router Open Source que provee amplias funcionalidades que combinan las características, el funcionamiento, la confiabilidad, la flexibilidad y la seguridad que puede ofrecer un Router comercial, pero su ventaja se basa en una buena relación costo/beneficio para la empresa que implemente este tipo de solución.

VYATTA Corporate fue creada en el año 2005 por un grupo de personas con amplio conocimiento en el área de Networking. Esta empresa es relativamente nueva pero su fortaleza se basa en la calidad de servicio que ofrecen las personas que trabajan en ella; su fundador Allan Leinwand (quien trabajó con Cisco System) junto a 100 empleados, forman parte de este grupo selecto de profesionales con gran experiencia en networking y desarrollo Open Source, haciendo de esta empresa una gran competencia para otras de mayor trayectoria.

La palabra VYATTA viene del idioma Sanskrit que es un lenguaje mántrico y tiene como significado “abierto”. Este nombre fue pensado con el propósito de mostrar que VYATTA, siendo una compañía nueva, tiene una ideología con fundamentos centrados en ofrecer productos Open Source (código abierto) al mercado [25].

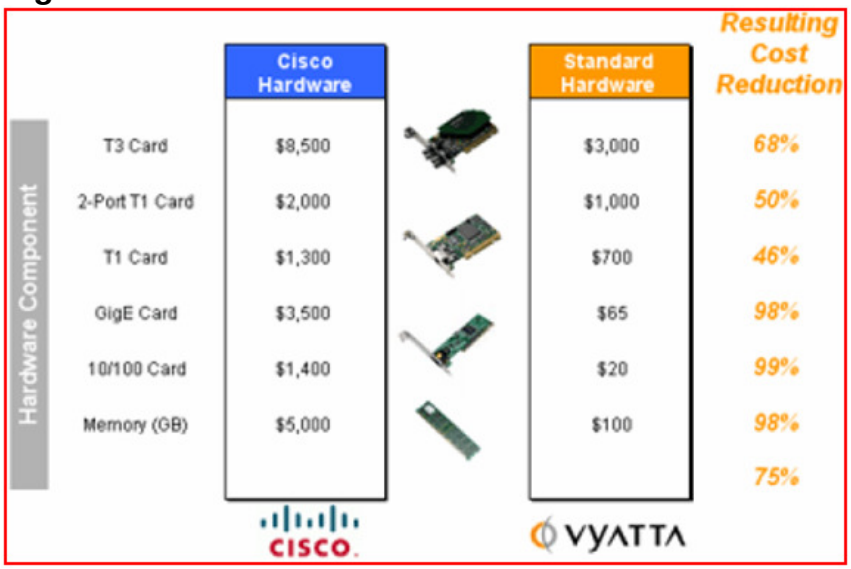
VYATTA dispone de una versión gratuita de 122 MB llamada VYATTA Community Edition que puede ser descargada desde su sitio Web oficial:

http://www.vyatta.com/download/sw_registration.php, permitiendo al usuario trabajar con ella desde un CD Live o desde el disco duro del PC donde sea instalado. Este tipo de versión no ofrece soporte y su actualización es semestral, por tanto esta versión es una muy buena opción para pequeñas y medianas empresas que desean un servicio básico y eficiente. VYATTA ofrece dos versiones comerciales, la versión profesional por USD$647 anuales que incluye actualización de software ilimitada y acceso online/e-mail al equipo de soporte técnico de VYATTA, también cuenta con una versión enterprise por USD$897 anuales que ofrece soporte online y telefónico además de actualizaciones ilimitadas. [5]

Este Router soporta interfaces Ethernet 10/100/1000 e interfaces T1/E1 (para enlaces WAN), soporta los protocolos de enrutamiento más comunes (OSPF, BGP-4, RIPV2 y rutas estáticas), incluye un Firewall y Software para VPNs y NAT; en resumen, VYATTA es un Router Open Source muy confiable y completo. La compañía VYATTA trabaja con socios como Sangoma, que fabrica tarjetas de interface WAN T-1 y T-3 para sistemas PC x86 y se espera que pronto anuncie una ampliación de empresas que puedan desarrollar dispositivos compatibles con VYATTA [26].

VYATTA por medio de un documento llamado White Paper presenta un estimado de precios de componentes de hardware donde muestra una gran diferencia entre el hardware propietario para Cisco y el hardware Standard que funcionan con VYATTA, (ver Figura 19).

Figura 19. Precios CISCO vs. VYATTA



Tomado de VYATTA.com

[5] La recopilación de precios fueron tomadas el día 10 de marzo del 2008 de la pagina de vyatta.org

VYATTA presenta interesantes características dentro de las cuales cabe resaltar las siguientes:

- Es capaz de mantener la red segura por medio de su Firewall.
- Ofrece conexión segura punto a punto por medio de VPNs.
- Ofrece actualización gratuita cada seis meses en la versión Community Edition.
- Ofrece herramientas que proporcionan una administración completa de la red.

VYATTA corre desde un PC x86 y según las pruebas a las que fue sometido, el procesamiento de este es directamente proporcional a la velocidad de la máquina que se utiliza para ejecutar el LiveCD. La empresa fabricante de VYATTA menciona que no es necesario tener un computador de última tecnología, ya que con un computador de mediana capacidad el Router Open Source funciona muy bien y es capaz de competir contra el procesamiento de un Router comercial [27].

- **XORP (eXtensible Open Router Plataform)**

XORP es una plataforma Open Source desarrollada bajo el lenguaje de programación C++, creada por Mark Handley y un grupo de la universidad de Berkeley, California, en un intento por diseñar una herramienta que fuese flexible a futuras investigaciones, así como también al desarrollo de nuevos protocolos de enrutamiento que suplieran las necesidades de networking.

Dave Roberts, vicepresidente de estrategia y marketing de WEBSENSE Inc. afirma que XORP necesita ser compilado desde una máquina Linux para su instalación e integración de las librerías. Igualmente Roberts añade que XORP no cuenta con los protocolos Virtual Router Redundancy Protocol (VRRP) y SNMP los cuales son ofrecidos en las otras herramientas de enrutamiento [28].

XORP es actualmente utilizado por pequeñas y medianas empresas así como también por instituciones educativas en todo el mundo, presenta una plataforma que implementa protocolos de enrutamiento para IPv4 e IPv6 y una función para configurarlo de manera que pueda interactuar con los dos protocolos. XORP puede ser descargado de manera gratuita desde su Home Site: http://www.xorp.org/livecd.html junto con su hash en MD5, utilizado para verificar la integridad de la descarga; posterior a esta se crea una imagen que funciona como un LiveCD para computadores x86 con un tamaño de 109 MB.

XORP presenta sus características de una manera muy interesante, pero señala que su uso más común es para prácticas de laboratorio en entidades educativas; a futuro se habla de un gran fortalecimiento y fuerte competencia frente a las demás herramientas de enrutamiento [29].

- **LINUX LiveCD Router**

Es un Router de distribución libre diseñado para proteger y compartir la conexión a Internet, este LiveCD puede ser descargado desde la página web: http://www.wifi.com.ar/english/cdRouter/ y tiene un tamaño de 90 MB. Los requisitos mínimos para su funcionamiento son:

- PC 486
- 16 MB de RAM
- Lector de CD 2X
- Puertos PCI
- Lector Floppy

No es necesario el uso de disco duro, ya que utiliza la memoria RAM creando un disco virtual en la memoria que emula el disco duro del computador; incluye herramientas como Firewall, Administración por SSH (Secure Shell), monitoreo de SNMP (Simple Network Management Protocol), entre otros.

Una de las grandes ventajas que tiene esta plataforma es que se puede incluir un Access Point para suministrar y recibir las peticiones de diversos dispositivos inalámbricos sin importar su marca o nivel de seguridad debido a que Linux LiveCD Router/Firewall sería el encargado de brindar las funciones de seguridad, acceso y enrutamiento.

Este tipo de herramienta ofrece dos versiones comerciales: Linux LiveCD Firewall PRO y Hotspot Wi-Fi, los cuales incluyen aplicaciones específicas que brindan la opción de administrar todas las funcionalidades por medio de una interfaz gráfica más sencilla y vistosa.

Linux LiveCD Firewall PRO incluye:

- Firewall con una interfaz web sencilla.
- Herramientas que optimizan el ancho de banda.
- Administración de OpenVPN con la interfaz web.
- Soporte vía E-mail durante 1 año.

Linux LiveCD Firewall PRO es una herramienta de excelente calidad que ofrece servicios de alto nivel pero es necesario pagar la versión comercial de Linux LiveCD de 99.oo dólares[6] para obtener la WEBGUI. La ventaja de tener una interfaz gráfica conlleva a tener una herramienta más amigable con el usuario y más sencilla para su configuración, este tipo de servicio solo es adquirido con la versión comercial de Linux LiveCD [30].

[6] Precio tomado de la página web: http://www.easylivecd.com/english/cdrouter/ , en el mes de Marzo de 2008.

- **FREESCO (FREE ciSCO)**

Es un Router desarrollado bajo el sistema operativo Linux en código abierto como una alternativa de enrutamiento; diseñado con características similares a algunas soluciones comerciales de Cisco, 3com, Nortel y otros. La visión de FREESCO se basa en encontrar diferentes alternativas para hacer un producto cada día más eficiente teniendo en cuenta la minimización de los costos al momento de implementar esta tecnología. Su ventaja es que muchas de las herramientas que se necesitan para operar y administrar el Router pueden ser almacenadas en un disco de 1.44 MB.

Estas son algunas de las opciones que FREESCO ofrece:

- Se puede utilizar como un puente o bridge para máximo tres conexiones Ethernet.
- Conexión máxima para tres interfaces Ethernet y hasta dos módems.
- Servidor DHCP.
- Servidor HTTP.
- Capaz de funcionar desde un único disquete con tan solo 6 MB de RAM y desde i386 en adelante.

FREESCO es una solución eficaz para pequeñas empresas con un bajo número de computadores, debido a que sólo tiene capacidad para soportar un número limitado de NICs (Network Interface Card), esto quiere decir que la empresa que tenga implementado este tipo de solución deberá limitarse al número reducido de interfaces para trabajar óptimamente [31].

4.3 CUADRO COMPARATIVO DE LAS DIFERENTES SOLUCIONES OPEN SOURCE

Mediante la siguiente tabla comparativa se pueden observar las características más importantes de las soluciones Open Source y de esta manera encontrar la herramienta que supla con las necesidades de la empresa ANPRA, teniendo en cuenta los siguientes aspectos:

- Expansión: La empresa siempre ha estado en constante crecimiento, por tanto es necesario que su infraestructura cambie de acuerdo a las necesidades existentes por medio de dispositivos de red que brinden un óptimo rendimiento a un costo accesible.

- Comunicación entre las 2 sedes: ANPRA-Bucaramanga requiere de una comunicación con la nueva sede que se ubicará en la ciudad de Bogotá, por esta razón requiere de una tecnología que brinde herramientas para crear una

red privada virtual, que supla con las necesidades de seguridad que requiere la comunicación entre las dos sedes teniendo en cuenta que la inversión debe ser baja. Existen varios tipos de tecnología para suplir las necesidades de comunicación de las dos sedes como líneas alquiladas, Routers comerciales pero su costo de inversión es muy alto.

Tabla 12. Cuadro comparativo de las diferentes soluciones Open Source

	XORP	Linux LiveCD Router	FREESCO	VYATTA
Diseñado para grandes y medianas empresas		■		■
LiveCD	■	■	■	■
Almacenamiento en Floppy	■		■	
Interfaz Gráfica		■		■
Firewall		■		■
Balanceo de 2 conexiones de Internet (Multi ISP)		■		■
VPN		■		■
Solución más reconocida a nivel mundial, confiable y compatible con otros dispositivos				■
Pago de servicios adicionales necesarios para el proyecto		■		

Convenciones	Si: ■	No: □

VYATTA y Linux LiveCD Router son las soluciones más completas según las características mostradas en el cuadro comparativo; del análisis se concluye que se trabajará con VYATTA debido al reconocimiento y trayectoria que tiene esta empresa, además de sus diversas funciones brindando confiabilidad, compatibilidad y versatilidad en el diseño de su estructura, de igual manera por las diferentes herramientas que VYATTA ofrece de manera gratuita frente a las ofrecidas por Linux LiveCD Router.

4.4 ANÁLISIS GENERAL ENTRE LAS SOLUCIONES OPEN SOURCE Y COMERCIALES

Los productos ofrecidos por Cisco, 3Com, Nortel, entre otras compañías, son muy funcionales y eficientes pero su alto costo de adquisición puede ser un problema para las PYMES, debido al elevado costo de implementación para suplir las necesidades. En algunas ocasiones la inversión es innecesaria pues no se utiliza toda la capacidad que ofrece un Router, y en otras no se puede modificar la programación para satisfacer las necesidades del usuario por el hecho de utilizar una herramienta patentada y comercial, por esta razón está creciendo día a día el planteamiento de nuevas tecnologías de Software Libre que brindan la seguridad y conexión que el usuario requiere [32].

Microsoft, Oracle, Sun Microsystems, Cisco, Juniper, entre otros, adquieren un gran margen de ganancia en cada uno de sus productos, es por esta razón que las soluciones de código abierto han creado nuevas alternativas que brinden servicios como Web Server (Apache) y bases de datos (MySQL). Los altos precios de implementación en tecnología de networking, hacen de los Router Open Source una opción para la solución de inconvenientes que muchas compañías por falta de dinero no podrían implementar en sus empresas.

La razón por la cual se escogió VYATTA para llevar a cabo este proyecto es que cuenta con todas las características que la empresa ANPRA necesita para obtener una conexión segura entre dos o más sedes ubicadas dentro del país. A diferencia de las soluciones estudiadas, VYATTA brinda en su versión Community Edition todas las herramientas que las demás opciones Open Source ofrecen pero de manera gratuita la cual puede ser descargada desde su sitio Web[7].

El dispositivo más costoso es el Cisco, aunque existen herramientas comerciales más económicas como es el caso del Router 3Com, el cual ofrece todas las funciones que ANPRA necesita, pero aún sigue siendo costosa la implementación de esta herramienta dentro de la infraestructura de red de la empresa.

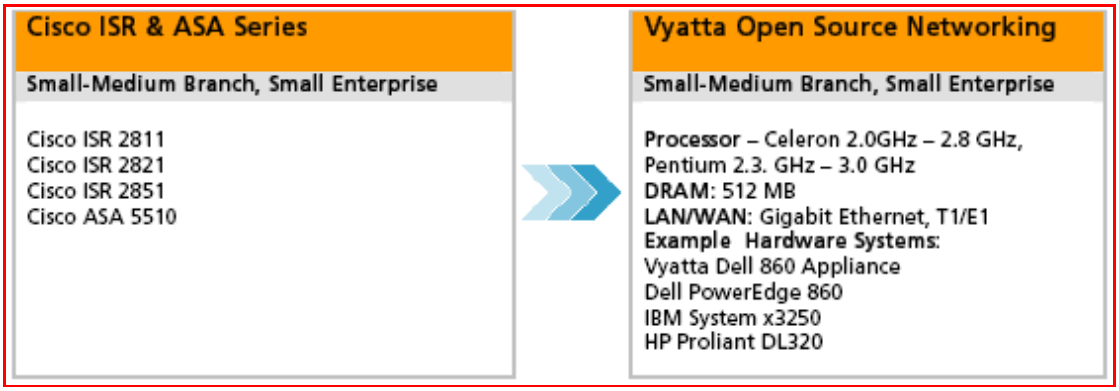
[7] http://www.vyatta.com/download/index.php

Aunque las soluciones comerciales muestran una gran variedad de herramientas que podrían brindarle a las compañías seguridad y confiabilidad en su infraestructura de red, se observa según las opciones estudiadas anteriormente que el factor económico es un impedimento para que las pequeñas y medianas empresas adquieran estos tipos de dispositivos; motivo que se convierte en factor importante en la selección de la solucion a implementar, por lo cual se decidió utilizar el Router Open Source VYATTA en el desarrollo de este proyecto.

4.5 COMPARATIVO DE REQUERIMIENTOS ENTRE UN ROUTER CISCO Y UN COMPUTADOR DONDE SE INSTALA UN ROUTER OPEN SOURCE VYATTA

Los frameworks suministrados por www.vyatta.org califican y proporcionan una idea del rendimiento que tendrá el Router VYATTA a partir de las especificaciones de los componentes que conformen el computador que se utilice en el montaje del Router Open Source y al mismo tiempo lo comparan con el dispositivo de enrutamiento de cisco al cual se estaría reemplazando. El computador que se utilizará en el montaje del proyecto tiene características similares al mostrado en la siguiente figura.

Figura 20. Cuadro comparativo de requerimientos entre un Router Cisco Vs un PC con VYATTA



Tomado de Vaytta Open-Source Networking Replacement Guide

5. DISEÑO DE LA INFRAESTRUCTURA DE RED QUE GARANTICE NIVELES DE SEGURIDAD Y CONFIABILIDAD ACEPTABLES PARA LA TRANSMISION DE DATOS ENTRE LAS DOS SEDES

Después de haber finalizado con el estudio de las características de la red de ANPRA, se inicia la etapa del diseño de la infraestructura que comunique las dos sedes ubicadas en la ciudad de Bucaramanga y Bogotá. En este capítulo se diseñará una estructura de red que supla con las necesidades de comunicación existentes en la compañía, se darán a conocer algunas características del sistema financiero y el proceso que utiliza la empresa para efectuar los pedidos, para que de esta manera se tenga en cuenta este proceso en todo el diseño.

5.1 SISTEMA CONTABLE-FINANCIERO MERLÍN

ANPRA cuenta con un sistema contable-financiero llamado Merlín, el cual se encarga de manejar contabilidad, cartera, facturación, compras e inventario de la empresa. Este programa guarda todas sus listas en archivos SQL ubicados en el servidor de su sede principal. Los pedidos de autopartes se hacen mediante Internet o dispositivos móviles (Qtek) de los vendedores externos.
La operación para realizar los pedidos mediante un dispositivo móvil es la siguiente:

- Periódicamente se descarga un correo con archivos en SQL en texto plano de las listas de clientes, precios y artículos nuevos.

- Diariamente desde la empresa se crea un correo para ser descargado por las Qtek con un archivo en SQL en texto plano con la lista de los artículos agotados.

- Se realiza el pedido en el dispositivo móvil eligiendo el cliente, los artículos y el precio es adicionado automáticamente dependiendo de la cantidad de artículos seleccionados.

- Al finalizar el pedido se envía un archivo en SQL en texto plano al hosting donde son guardados en una base de datos ACCESS.

- Cada 5 minutos el servidor de la empresa ANPRA verifica si se han realizado nuevos pedidos, si los hay, descarga los pedidos almacenados en el hosting.

- En la bodega por medio de una PDA se descargan los pedidos almacenados en el servidor de la empresa y se realiza el proceso de selección de productos para su posterior envío al cliente.

Es necesario destacar que la transferencia de archivos que maneja ANPRA, donde contienen las listas nuevas de clientes, artículos y precios que son descargados por los dispositivos móviles (Qtek) tienen un tamaño máximo de 1MB, mientras que los archivos descargados con el listado de autopartes agotadas diariamente son menores a 100KB, esto refleja que el ancho de banda necesario para este tipo de transacciones es mínimo.

Nota: Los datos de los pedidos enviados al hosting son almacenados en ACCESS debido a que CAMINOWEB no brinda el servicio de almacenamiento de archivos SQL en su plan de Windows Extra [33].

5.2 NECESIDADES PARA LA INTERCONEXIÓN DE LAS DOS SEDES

Todos los repuestos importados al país llegan a Zona Franca en la ciudad de Bogotá (*zona donde se almacenan las importaciones sin necesidad de pagar impuestos),* al salir de allí, se envían directamente a ANPRA en la ciudad de Bucaramanga y desde allí se manejan todas las ventas al país. Los mayores compradores se encuentran en Bogotá, es decir, los repuestos tienen que mandarse nuevamente a la ciudad de origen, o en otros casos, la mayoría de los pedidos deben pasar por Bogotá. En otras palabras, el hecho de tener la sede principal ubicada en Bucaramanga implica el aumento del valor en cada uno de los productos de la empresa y tiempo de envío, haciendo este factor una debilidad en la competitividad con las demás empresas.

Debido a las razones anteriores la sede principal de la empresa se ubicará en la ciudad de Bogotá, de esta manera, surge la necesidad de crear una conexión punto a punto que supla con todas las necesidades de seguridad requeridas para las actualizaciones de base de datos que se creen con toda la información proveniente de la sede principal o viceversa.

Se crea una propuesta basada en lo siguiente:

- Establecer un dispositivo de enrutamiento en cada una de las sedes de tal manera que la información pueda ser compartida por ambas. Cada dispositivo de enrutamiento se creará a partir de la utilización de Routers Open Source VYATTA, que minimicen los gastos de inversión en dispositivos comerciales.

- Crear mediante los Routers Open Source una Red Privada Virtual (VPN) entre Bogotá-Bucaramanga con todos los requerimientos de seguridad, que

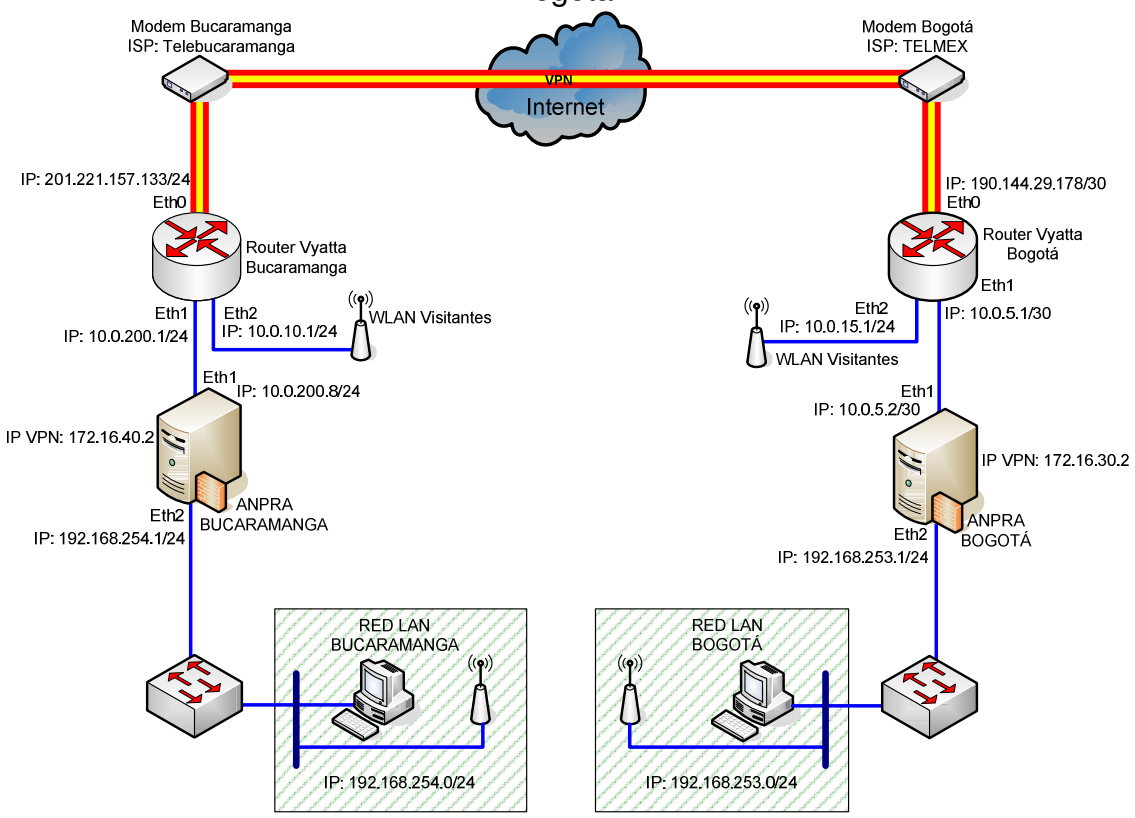
sustituyan el uso de una conexión punto a punto debido a los altos costos de implementación de estos servicios.

- Crear una subred distinta a la utilizada por la red LAN de la empresa para el acceso a Internet por parte de los visitantes y compradores que lleguen a ANPRA para que la red de los clientes sea independiente de la red la compañía.

5.3 DISEÑO DE LA INFRAESTRUCTURA DE RED MEDIANTE LA SOLUCION OPEN SOURCE VYATTA ENTRE LAS SEDES BUCARAMANGA Y BOGOTÁ

La figura 21 muestra la conexión que se hará a partir de la implementación de los Routers VYATTA en cada una de las sedes que tendrá la empresa ANPRA en la ciudad de Bucaramanga y Bogotá. Se creará cada una de las subredes requeridas (visitantes y red local privada) en las dos sedes junto a las características de conexión y seguridad de cada subred.

Figura 21. Esquema de conexión de la sede ANPRA Bucaramanga – ANPRA Bogotá



5.3.1 Infraestructura de red en oficinas de Bucaramanga y Bogotá

- **Direcciones IP publicas**

La dirección IP pública de la empresa en la ciudad de Bucaramanga es 201.221.157.133/24, aunque el valor de la máscara permite un total de 254 direcciones posibles solo se le permite a la empresa tomar dos direcciones IPs 201.221.157.133/24 y 201.221.157.134/24 de las cuales solo se trabajará con la dirección 201.221.157.133.

La dirección IP pública de la empresa en la ciudad de Bogotá es 190.144.29.178/30, el valor de la máscara permite un total de 2 direcciones posibles 190.144.29.177 y 190.144.29.178, pero en este proyecto se trabajará únicamente con la dirección IP 170.144.29.178. El proveedor del servicio de Internet en Bogotá se llama TELMEX.

- **Distribución de las interfaces del Router**

El Router VYATTA-Bucaramanga se ubicará entre el servidor de la empresa y el Modem de Telebucaramanga. La interface de salida Ethernet 0 del Router estará conectada al Modem, la interface de salida Ethernet 1 estará conectada al servidor, y por último la interface Ethernet 2 estará conectada a la nueva subred creada, en esta subred se ubicará un Access Point marca D-Link para que brinde acceso inalámbrico a los visitantes de ANPRA – Bucaramanga (ver Figura 21).

El Router VYATTA-Bogotá se ubicará entre el servidor de la empresa y el Modem de TELMEX. La interface de salida Ethernet 0 del Router estará conectada al Modem, la interface de salida Ethernet 1 estará conectada al servidor, y por último la interface Ethernet 2 estará conectada a la nueva subred creada, en esta subred se ubicará un Access Point marca D-Link para que brinde acceso inalámbrico a los visitantes de ANPRA-Bogotá.

- **Direccionamiento de las interfaces del Router**

BUCARAMANGA:

Interface Ethernet 0: 201.221.157.133/24
Interface Ethernet 1: 10.0.200.1/24
Interface Ethernet 2: 10.0.10.1/24

BOGOTÁ:

Interface Ethernet 0: 190.144.29.178/30
Interface Ethernet 1: 10.0.5.1/30
Interface Ethernet 2: 10.0.15.1/24

- **Direccionamiento Interno de la compañía**

BUCARAMANGA:

Interface Ethernet 1 del servidor-Bucaramanga: 10.0.200.8/24
Interface Ethernet 2 del servidor-Bucaramanga: 192.168.254.1/24

El direccionamiento interno de la red LAN Bucaramanga (ver figura 21) no se modificará, la única dirección que cambia es la dirección del servidor que antes era la dirección pública 201.221.157.133 y ahora se convierte en la dirección 10.0.200.8/24. Quedará configurado con las mismas características de servicios (Proxy y DHCP) y el direccionamiento IP interno 192.168.254.0/24 que le da a ANPRA-Bucaramanga por medio del Switch conectado a la interface Ethernet 2.

El direccionamiento de la red Wi-Fi de los visitantes estará custodiado por el servidor de ANPRA-Bucaramanga. La dirección IP de la interface a la que está conectado el Access Point es la 10.0.10.1/24.

BOGOTÁ:

Interface Ethernet 1 del servidor-Bogotá: 10.0.5.2/30
Interface Ethernet 2 del servidor-Bogotá: 192.168.253.1/24

El direccionamiento interno de la red LAN Bogotá (ver Figura 21) quedará a cargo del servidor ANPRA-Bogotá, se configurará como servidor Proxy y DHCP con dirección 192.168.253.1/24 para que se encargue de darle el direccionamiento IP de la red LAN de la compañía por medio del Switch marca de D-link que se conectará a la interface Ethernet 2 del servidor de ANPRA-Bogotá.

El direccionamiento de la red Wi-Fi de los visitantes estará custodiado por el servidor de ANPRA-Bogotá. La dirección IP de la interface a la que está conectado el Access Point es la 10.0.15.1/24.

- **VPN**

La seguridad que se implementará en la conexión de las dos sedes dependerá de la estructura de la VPN debido a que será el medio por donde se comuniquen ANPRA-Bucaramanga con ANPRA-Bogotá y viceversa.

La arquitectura de protocolos que manejará la seguridad en la VPN será IPsec, junto a protocolos de encripción de llaves Internet Key Exchange (IKE) y encapsulamiento de paquetes Encapsulating Security Payload (ESP), además de esquemas de cifrados como AES y 3DES, funciones hash MD5 y SHA-1, y finalmente el protocolo criptográfico Diffie-Hellman.

BUCARAMANGA:

- Proceso de NAT: cuando el servidor de la empresa ANPRA-Bucaramanga se quiera comunicar con el servidor de la empresa ANPRA-Bogotá, el paquete que sale del servidor de Bucaramanga será direccionado por la VPN. Este paquete tomará la dirección 172.16.40.2 reemplazando la dirección original del servidor 10.0.200.8/24, ver Figura 21. Solo se permitirá ingresar a la VPN todo lo que venga de la red LAN interna de la empresa. No se permitirá ingreso a la VPN la red de los visitantes de ANPRA-Bucaramanga.

- Cuando la Empresa ANPRA-Bucaramanga hace uso de Internet, los paquetes viajan con la dirección 201.221.157.133; correspondiente a su dirección Pública. Si se desea utilizar la Red Privada Virtual para establecer la comunicación con la sede ubicada en Bogotá, los paquetes viajan con la dirección 172.16.40.2.

BOGOTÁ

- Proceso de NAT: cuando el servidor de la empresa ANPRA-Bogotá se quiera comunicar con el servidor de la empresa ANPRA-Bucaramanga, el paquete que sale del servidor de Bogotá será direccionado por la VPN. Este paquete tomará la dirección 172.16.30.2 reemplazando la dirección original del servidor 10.0.5.2/30, ver Figura 21. Solo se permitirá ingresar a la VPN todo lo que venga de la red LAN interna de la empresa. No se permitirá ingreso a la VPN la red de los visitantes de ANPRA-Bogotá.

- Cuando la Empresa ANPRA-Bogotá hace uso de Internet, los paquetes viajan con la dirección 190.144.29.178; correspondiente a su dirección Pública. Si se desea utilizar la Red Privada Virtual para establecer la comunicación con la sede ubicada en Bucaramanga, los paquetes viajan con la dirección 172.16.30.2.

- **Cableado**

Se utilizará cables directos UTP categoría 5e entre la conexión de servidor-Router, Router-Modem, y finalmente Router-Access Point. La longitud de cada uno de los cables será de aproximadamente 1.5 metros y todos estos dispositivos se ubicarán en el centro de Telecomunicaciones (ver planos del cableado de ANPRA).

5.3.2 Dispositivos de la infraestructura

Para el diseño de la infraestructura se comprarán unos dispositivos, otros ya se encontraban dentro de la empresa.

Tabla 13. Dispositivos adquiridos en la creación de la Infraestructura de red de Bucaramanga – Bogotá

DISPOSITIVO	CANTIDAD	PRECIO($) c/u	CONDICION
Computador-Bogotá	1	500.000	Nuevo*
Computador-B/manga	1	500.000	Nuevo*
Cableado	6	30.000	Nuevo
Access Point[8]	3	180.000	Nuevo
Switch[9]	1	260.000	Nuevo

*Nuevo: Todos los componentes del computador son totalmente nuevos, excepto la unidad de diskette y dos memorias RAM de 512MB que pertenecían a otros computadores de la empresa que no estaban en funcionamiento. Todo lo anterior se hizo para optimizar el desempeño y de esta manera utilizar los computadores para instalar el Router Open Source Vyatta.

Características principales:

- **Switch**

Soporta Full/half duplex por puerto
Control de flujo para transmisión segura
Auto-negociación MDI/MDIX
Tamaño desktop
Plug&Play (permite utilizarlo sin necesidad de instalarlo en los equipos)

- **Acces Point**

Operación DualBand
Velocidad hasta 108 Mbps
Seguridad WPA
Firewall Avanzado, SPI y filtrado de URL

[8] DI -784, Corporate Indoor Internet Server 802.11a/11g, 54/108 Mbps3.
[9] DES -1016D Unmanaged SOHO/Workgroup 16-port 10/100 Mbps Switch.

6. IMPLEMENTACIÒN DEL DISEÑO DE RED

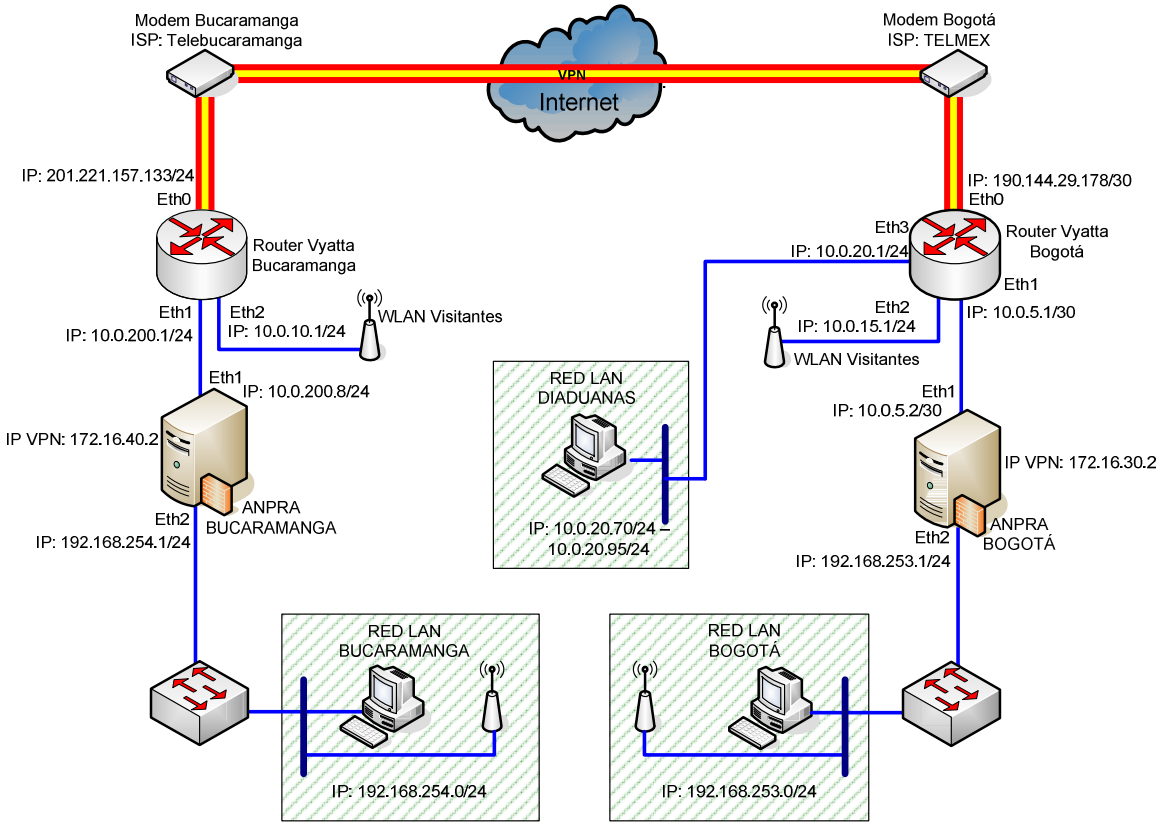
En este capítulo se mostrará la infraestructura de red montada entre las dos sedes, además se dará a conocer todas las etapas que se realizaron para la ejecución del proyecto, desde los dispositivos que se utilizaron hasta las características de configuración y las distintas actividades que se llevaron a cabo para la implementación del diseño propuesto a la empresa ANPRA. La implementación del proyecto se divide en tres etapas, la primera etapa hace referencia a la planeación y compra de los dispositivos necesarios para la implementación del proyecto junto a la descarga del Router Open Source, la etapa intermedia abarca las pruebas que se realizaron durante la configuración de los dispositivos, y finalmente la ultima etapa que comprende la implementación de los dispositivos y la puesta en marcha de la infreaestructa entre las dos sedes.

Se tuvo que realizar un cambio al final del proyecto el cual consistió en la adecuación de una interface Ethernet nueva al Router Vyatta de Bogotá debido a que la empresa decidió montar una red adicional en la sede de Bogotá que recibió el nombre de Diaduanas.

De acuerdo al diseño realizado y a los cambios que se dieron durante la implementación del proyecto, la infraestructura final que se implementó entre las dos sedes de ANPRA es la mostrada en la figura 22, donde se brinda seguridad en la conexión entre las 2 sedes por medio de una Red Privada Virtual (VPN) establecida entre los dos Router Open Source Vyatta y las características en su configuración que le brindan integridad y autenticación a la información que viaja a través de ella.

La nueva interface creada en la ciudad de Bogotá donde está ubicada la red de Diaduanas no tendrá acceso a la red privada virtual. Finalmente la única información que podrá acceder a la VPN será la que tenga como salida la interface Ethernet 1 en cada uno de los Router Vyatta (ver Figura 22), que corresponde a la interface a la que se encuentran conectados el servidor ANPRA-Bucaramanga y el servidor ANPRA-Bogotá en cada sede.

Figura 22. Infraestructura de red implementada en ANPRA



6.1 ETAPA DE INICIACIÓN

En esta etapa del proyecto se realiza la adquisición y adecuación de los dispositivos necesarios para la implementación del diseño propuesto en el capitulo anterior, la descarga e instalación del Router Open Source en los computadores.

6.1.1 Compra de computadores

Inicialmente se pensó en utilizar dos computadores de la empresa, pero la Gerencia decidió mejorar las características de hardware e invirtió dinero para la compra de dos equipos nuevos que estuvieran dentro de las especificaciones de las comparativas de requerimientos entre un Router Cisco Vs un PC con VYATTA, descritas en el capítulo 4 (ver figura 20), estas son las características de los dos computadores utilizados para la instalación del Router Vyatta en cada una de las sedes:

- Procesador: AMD Sempron 2.6 GHz
- DRAM: 1024 MB
- LAN/WAN: 10/100 Fast Ethernet
- Hard Drive: 80 GB

Nota: las características de los equipos adquiridos cumplen los requerimientos para emular un router cisco de la serie 2800.

6.1.2 Descarga e Instalación de VYATTA

Fue necesario descargar Vyatta Community Edition totalmente gratis desde su sitio web: http://www.vyatta.com/download/index.php y su integridad fue verificada mediante un hash en md5.

Cada equipo adquirido por ANPRA tiene como única y exclusiva función operar como un Router basado en Debian GNU/Linux, no se encuentra instalado otro sistema operativo en los computadores utilizados para la implementación. Vyatta puede ser utilizado como un Live CD o puede ser instalado en el disco duro mediante el comando:

```
vyatta:~# install-system
```

Nota: solo se utilizaron 5 GB del disco duro de cada computador, es importante tener en cuenta que si se desea utilizar Vyatta en el computador con el sistema operativo Windows, este afectará el sistema operativo previamente instalado. El disco duro de los computadores no tenía ningún sistema operativo instalado previamente, quedando únicamente con Vyatta, el cual instala por defecto DEBIAN (distribución libre del sistema operativo Linux) en su instalación inicial.

6.1.3 Nueva Dirección de Internet

Fueron necesarios algunos cambios para iniciar con la implementación del proyecto ya que ANPRA es una empresa que necesita tener en funcionamiento su servidor e Internet las 24 horas del día, por esta razón se solicitó una segunda dirección IP fija para realizar las pruebas iníciales con los Router ya que no se podía desconectar la red de ANPRA debido al envió de archivos que tiene periódicamente vía Internet.

Al iniciar el proyecto, la empresa tenía la dirección IP 201.21.238.18/24, al momento de la solicitud de una dirección IP adicional, el Proveedor de Servicios de Internet informo a ANPRA que se encontraban reorganizando el direccionamiento IP, por tal motivo reemplazó la dirección con la que se conectaba a Internet la empresa y asigno las direcciones IP 201.221.157.133/24 (dirección IP actual de ANPRA Ltda.) y 201.221.157.133.134/24 (dirección IP utilizada para las pruebas realizadas durante el proyecto).

Nota: es necesario el direccionamiento IP fijo debido a que en la programación de la VPN se establecen direcciones IP que no pueden ser modificadas.

6.2 ETAPA INTERMEDIA

Al tener instalado el Router Open Source Vyatta en cada uno de los equipos, se comenzaron las pruebas para la configuración del Router de Bucaramanga, la dirección IP utilizada para realizar dichas pruebas fue: 201.221.157.134 con el fin de no afectar el normal funcionamiento de la empresa ANPRA.

6.2.1 Cuadro de Configuraciones Básicas

Inicialmente se realizó la configuración básica para cada una de las interfaces de red por medio de los siguientes comandos:

Tabla 14. Comandos básicos de la configuración del Router Vyatta[10].

Comandos de Configuración	Descripción del Comando
vyatta@vyatta> configure	Comando para entrar al modo de configuración del Router
vyatta@vyatta# set interfaces ethernet eth0 address 10.0.0.1 prefix-length 24	Comando para configurar las interfaces de red, en este caso la interface eth0, el 24 corresponde a la máscara 255.255.255.0
vyatta@vyatta# set interfaces ethernet eth0 description "Office LAN"	Comando para configurar la descripción de la interface, en este caso la interface eth0 correspondiente a la LAN, esta configuración es opcional
vyatta@vyatta# set protocols static route 0.0.0.0/0 next-hop 201.221.157.1	Comando para usar una ruta estática, indicando que todos salen por el next-hop correspondiente al Gateway
vyatta@vyatta# set service nat rule 1	Comando para configurar las reglas del NAT para las interfaces del Router
vyatta@vyatta# set service nat rule 1 type masquerade	Comando donde la dirección IP origen del paquete de salida es reemplazado por la dirección IP de la interface de salida
vyatta@vyatta# set service nat rule 1 outbound-interface eth1	Comando que indica la interface eth1 sale por la interface eth0
vyatta@vyatta# set service nat rule 1 protocols all	Comando que permite todos los protocolos
vyatta@vyatta# set service nat rule 1 source network 10.0.200.0/24	Comando que indica la dirección origen de la interface, en este caso la eth1
vyatta@vyatta# set service nat rule 1 destination network X.X.X.X/X	Comando utilizado para definir el destino de los paquetes en la red
vyatta@vyatta# commit	Comando para hacer permanente lo cambios en la configuración
vyatta@vyatta# save	Comando para guardar toda la configuración en el disco duro (/opt/vyatta/etc/config)

[10] Tomado del frameworks Vyatta_evalguide disponible en formato PDF en www.vyatta.com

Nota: es importante saber que la interfaz de configuración del Router Open Source Vyatta es similar a la interfaz del IOS de Cisco.

6.2.2 Adquisición de nuevos dispositivos de red

De acuerdo al diseño que se planteó para el proyecto fue necesaria la compra de los siguientes dispositivos:

- **3 Access Point D-Link:** uno de los Access Point se utilizó para la WLAN de visitantes de la empresa ANPRA-Bucaramanga, los dos restantes corresponden a la WLAN de empleados y WLAN de visitantes de ANPRA-Bogotá.

- **1 Switch de 24 puertos D-Link:** empleado para la LAN de ANPRA-Bogotá.

- **Otros:** Tarjetas de red, cables directos, cables cruzados.

6.3 ETAPA FINAL

Al concluir con todas las pruebas realizadas en ANPRA-Bucaramanga con ambos Router Open Source Vyatta funcionando óptimamente, cada uno con una dirección IP pública diferente. Posteriormente se incluyeron dentro de la infraestructura de red de ambas sedes para que entrara en funcionamiento la VPN y brindara una seguridad adicional a la empresa.

6.3.1 Implementación en ANPRA Ltda. Bogotá

Luego de tener en completo funcionamiento los dos Router Vyatta, fue necesario el desplazamiento hacia la cuidad de Bogotá para la implementación del Router Open Source que posteriormente se configuró con la dirección IP pública 190.29.144.178/30, suministrada por TELMEX en Bogotá y una velocidad de transmisión de 1MB. A diferencia de Telebucaramanga esta conexión llega hasta la empresa con fibra óptica y en el rack por medio de un transceiver lo convierte a RJ-45.

En la Cuidad de Bogotá al tener una dirección IP diferente a la que se tenía en las pruebas realizadas en Bucaramanga fue necesario volver a configurar el Router Vyatta de ANPRA-Bogotá, debido a que las pruebas en bucaramanga se hacían con las dos direcciones IP 201.221.157.133/24 y 201.221.157.134/24.

6.3.2 Diaduanas

Diaduanas es una SIA (Sociedad Intermediaria Aduanera) que se encuentra dentro de las instalaciones de la sede de ANPRA-Bogotá y se encarga de nacionalizar toda la mercancía de autopartes importadas por ANPRA y demás clientes, por tanto fue necesario instalar una interface de red adicional para suministrar Internet a una Red de Área Local exclusivamente para la SIA, por tal motivo se configuro el servicio de DHCP para que por medio de la interface eth3 el Router Vyatta suministre el direccionamiento a esa subred, el rango de direcciones IP va desde la dirección IP 10.0.20.70/24 hasta la dirección IP 10.0.20.95/24, es decir, está configurado para 25 posibles direcciones IP. Este tipo de configuración se hizo de esa manera ya que no se tenía conocimiento de la infraestructura de red correspondiente a Diaduanas.

6.3.3 Configuración del Router Vyatta-Bucaramanga

La siguiente configuración corresponde al Router de Bucaramanga.

Se adaptaron y configuraron tres interfaces Ethernet al Router VYATTA-BUCARAMANGA:

La Ethernet 0 corresponde a la dirección IP: 201.221.157.133 máscara 255.255.255.0 y es la encargada de darle salida a Internet a la empresa.

ethernet eth0 {
hw-id: 00:08:a1:a9:01:79
address 201.221.157.133 {
prefix-length: 24

La Ethernet 1 corresponde a la dirección IP: 10.0.200.1 máscara 255.255.255.0 y es la que se encuentra conectada al servidor de ANPRA.

ethernet eth1 {
hw-id: 00:08:54:df:a0:d9
address 10.0.200.1 {
prefix-length: 24

La Ethernet 2 corresponde a la dirección IP: 10.0.10.1 máscara 255.255.255.0 y es la que se encuentra conectada al Access Point de los visitantes. A esta interface se le activó el servicio de DHCP para que suministre dirección IP a los visitantes asignándoles desde la dirección 10.0.10.20/24 hasta 10.0.10.50/24.

ethernet eth2 {
hw-id: 00:19:db:e9:3e:f9

address 10.0.10.1 {
prefix-length: 24
service {
dhcp-server {
shared-network-name inalambrica {
subnet 10.0.10.0/24 {
start 10.0.10.20 {
stop: 10.0.10.50
dns-server 201.221.151.31
dns-server 201.221.151.32
default-router: 10.0.10.1
domain-name: "inalambrica.bucaramanga"

Los passwords de los usuarios están cifrados y se activó el servicio de SSH el cual utiliza el puerto 22 para poder tener control del dispositivo desde otros lugares fuera de la empresa.

ssh {
login {
user root {
authentication {
encrypted-password: "1WQ2tyL7m$gtYPSxd5TS0urUwHe4wSN/"
plaintext-password: ""

user vyatta {
authentication {
encrypted-password: "1CUR.hUu.$PIW.N1nMl0JP2iY8jN9lm1"
plaintext-password: ""

Configuraciones de las reglas NAT:

Las configuraciones de las reglas NAT 10 y 15 son necesarias para que pueda operar la VPN entre las dos sedes.

Los paquetes salientes desde la dirección IP origen 10.0.200.8 (dirección del servidor de ANPRA-Bucaramanga) con dirección IP destino 172.16.30.2 (dirección enmascarada del servidor en Bogotá) viaja a través de la VPN con la dirección 172.16.40.2.

nat rule 10
type: "source"
outbound-interface: "eth0"
source address: "10.0.200.8"
destination address: "172.16.30.2"
outside-address address: 172.16.40.2

Esto quiere decir que toda la información que venga del servidor de Bucaramanga hacia el servidor de Bogotá la direccionará el ROUTER-VYATTA por la VPN con una IP diferente enmascarando la IP origen 10.0.200.8 con la dirección IP 172.16.40.2.

Así mismo, cuando llegan paquetes con dirección IP origen 172.16.30.2 (dirección enmascarada del servidor en Bogotá) con dirección IP destino 172.16.40.2 (dirección enmascarada del servidor en Bucaramanga) el Router-Vyatta Bucaramanga lo direccionará hacia el servidor de la empresa que se encuentra con la dirección IP 10.0.200.8.

nat rule 15 {
type: "destination"
inbound-interface: "eth0"
source address: "172.16.30.2"
destination address: "172.16.40.2"
inside-address address: 10.0.200.8

Las Nat-rules 102 y 103 le establecen a la red por cuál interface tienen salida a Internet con una forma de Nat-rule llamada “masquerade”. En la opción masquerade, la dirección IP origen del paquete de salida es reemplazado por la dirección IP de la interface de salida.

rule 102 {
type: "masquerade"
outbound-interface: "eth0"
source network: "10.0.200.0/30"

rule 103 {
type: "masquerade"
outbound-interface: "eth0"
source network: "10.0.10.0/24"

6.3.4 Configuración del Router Vyatta-Bogotá

La siguiente configuración corresponde al Router de Bogotá.

Se adaptaron y configuraron cuatro interfaces Ethernet al Router VYATTA-BOGOTÁ:

La Ethernet 0 corresponde a la dirección IP: 190.144.29.178 máscara 255.255.255.252 y es la encargada de darle salida a Internet a la empresa.

ethernet eth0 {
description: "internet.trelsa"
hw-id: 00:03:ce:8a:2c:61
address 190.144.29.178 {
prefix-length: 30

La Ethernet 1 corresponde a la dirección IP: 10.0.5.1 máscara 255.255.255.252 y es la que se encuentra conectada al servidor de ANPRA sede Bogotá.

ethernet eth1 {
description: "lan.trelsa"
hw-id: 00:08:54:48:2d:e2
address 10.0.5.1 {
prefix-length: 30

La Ethernet 2 corresponde a la dirección IP: 10.0.15.1 máscara 255.255.255.0 y es la que se encuentra conectada al Access Point de los visitantes. A esta interface se le activó el servicio de DHCP para que suministre dirección IP a los visitantes asignándoles desde la dirección 10.0.15.80/24 hasta 10.0.15.90/24.

ethernet eth2 {
description: "inalambrica.trelsa"
hw-id: 00:08:54:48:2d:a8
address 10.0.15.1 {
prefix-length: 24

service {
dhcp-server {
shared-network-name wtrelsa {
subnet 10.0.15.0/24 {
start 10.0.15.80 {
stop: 10.0.15.90
dns-server 200.26.137.135
dns-server 200.14.207.210
default-router: 10.0.15.1
domain-name: "trelsa.zona.franca"

La Ethernet 3 corresponde a la dirección IP: 10.0.20.1 máscara 255.255.255.0 y se encuentra conectada a una subred llamada "*diaduanas*" dentro de la empresa ANPRA. sede Bogotá. A esta interface se le activó el servicio de DHCP para asignándoles desde la dirección 10.0.15.70/24 hasta 10.0.15.95/24.

ethernet eth3 {
description: "diaduanas"
hw-id: 00:19:db:e5:56:53

address 10.0.20.1 {
prefix-length: 24
shared-network-name diaduanas {
subnet 10.0.20.0/24 {
start 10.0.20.70 {
stop: 10.0.20.95
dns-server 200.26.137.135
dns-server 200.14.207.210
default-router: 10.0.20.1
domain-name: "diaduanas.local"

Los passwords de los usuarios están cifrados y se activó el servicio de SSH el cual utiliza el puerto 22 para poder tener control del dispositivo desde otros lugares fuera de la empresa.

ssh {
login {
user root {
authentication {
encrypted-password: "1WG2Zds78$pUp9CCofUESpP5n5fsUyC/"
plaintext-password: ""

user vyatta {
authentication {
encrypted-password: "1wotdoenH$YUUICrz.LRj/uQhll0Wdd1"
plaintext-password: ""

Configuraciones de las reglas NAT:

Las configuraciones de las reglas NAT 10 y 15 son necesarias para que pueda operar la VPN entre las dos sedes.

Los paquetes salientes desde la dirección IP origen 10.0.5.2 (dirección del servidor de ANPRA-Bogotá) con dirección IP destino 172.16.40.2 (dirección enmáscarada del servidor en Bucaramanga) viaja a través de la VPN con la dirección 172.16.30.2.

nat {
rule 10 {
type: "source"
outbound-interface: "eth0"
source address: "10.0.5.2"
destination address: "172.16.40.2"
outside-address address: 172.16.30.2

Esto quiere decir que toda la información que se dirija del servidor de Bogotá hacia el servidor de Bucaramanga la direccionará el Router-Vyatta por la VPN con una IP diferente enmascarando la IP origen 10.0.5.2 con la dirección IP 172.16.30.2.

Así mismo, cuando llegan paquetes con dirección IP origen 172.16.40.2 (dirección enmascarada del servidor en Bucaramanga) con dirección IP destino 172.16.30.2 (dirección enmascarada del servidor en Bogotá) el ROUTER-VYATTA lo direccionará hacia el servidor de la empresa que se encuentra con la dirección IP 10.0.5.2.

rule 15 {
type: "destination"
inbound-interface: "eth0"
source address: "172.16.40.2"
destination address: "172.16.30.2"
inside-address address: 10.0.5.2

Las Nat-rules 102, 103 y 104 le establecen a la red por cual interface tienen salida a Internet con una forma de Nat-rule llamada “masquerade”. En la opción masquerade, la dirección IP origen del paquete de salida es reemplazado por la dirección IP de la interface de salida.

rule 102 {
type: "masquerade"
outbound-interface: "eth0"
source network: "10.0.5.0/24"

rule 103 {
type: "masquerade"
outbound-interceace: "eth0"
source network: "10.0.15.0/24"

rule 104 {
type: "masquerade"
outbound-interface: "eth0"
source {
network: "10.0.20.0/24"

6.4 CARACTERÍSTICAS DE LA VPN

La configuración de la VPN se hace con la dirección de los dos servidores funcionando en cada una de las sedes ubicadas en la ciudad de Bogotá y Bucaramanga, estableciendo medidas que proporcionan seguridad en la comunicación y acceso a los recursos ofrecidos en cada uno de los servidores de la compañía ubicados a distancia.

La arquitectura de protocolos que manejan la seguridad en la VPN se llama IPsec, la cual proporciona la seguridad de la comunicación mediante técnicas de encriptación, autenticación y llaves de administración que brindan a la conexión integridad en su comunicación.

La arquitectura IPsec utiliza dos componentes los cuales son soportados por VYATTA:

- El protocolo de Encapsulating Security Payload (ESP)
- El protocolo de Internet Key Exchange (IKE), referido como ISAKMP/oakley.

ESP se encarga de encriptar los datos de los paquetes previniéndolos de ser monitoreados e IKE les proporciona seguridad en su viaje dentro de la VPN mediante el intercambio de llaves criptográficas, métodos de autenticación y encripción entre los puntos finales, cada protocolo se ejecuta por medio de dos procesos de negociación llamados *proposal*. Para la encriptación del intercambio de llaves (IKE) y el encapsulamiento de datos (ESP) se utilizaron los esquemas de cifrados AES256 y 3DES; para la autenticación de los datos se utilizaron las funciones Hash MD5 y SHA-1 utilizando el método de autenticación *Pre-Shared Secret*. Para la seguridad en el intercambio de llaves encriptadas se utilizó el protocolo criptográfico Diffie-Hellman[11].

[11] El protocolo Diffie-Hellman (debido a Whitfield Diffie y Martin Hellman) permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Tomado de https://upcommons.upc.edu

Grupo IKE-Bucaramanga
ike-group "IKE-1E"
proposal 1
encryption: "aes256"
dh-group: 5
proposal 2
lifetime: 3600

Grupo ESP-Bucaramanga
esp-group "ESP-1E"
proposal 1
encryption: "aes256"
proposal 2
encryption: "3des"
hash: "md5"
lifetime: 1800

Tipo de Autenticación
site-to-site {
peer 190.144.29.178 {
authentication {
pre-shared-secret: "test_key_1"

ike-group: "IKE-1E"
local-ip: 201.221.157.133
tunnel 1 {
local-subnet: 172.16.40.2/32
remote-subnet: 172.16.30.2/32
esp-group: "ESP-1E"

Grupo IKE-Bogotá
ike-group "IKE-1W" {
proposal 1 {
encryption: "aes256"
dh-group: 5
proposal 2 {
lifetime: 3600

Grupo ESP-Bogotá
esp-group "ESP-1W" {
proposal 1 {
encryption: "aes256"
proposal 2 {
encryption: "3des"
hash: "md5"
lifetime: 1800

Tipo de Autenticación
site-to-site {
peer 201.221.157.133 {
authentication {
pre-shared-secret: "test_key_1"

ike-group: "IKE-1W"
local-ip: 190.144.29.178
tunnel 1 {
local-subnet: 172.16.30.2/32
remote-subnet: 172.16.40.2/32
esp-group: "ESP-1W"

Con las configuraciones realizadas en los Routers, queda en completo funcionamiento el enrutamiento de los paquetes en cada una de las sedes brindando salida a Internet y al mismo tiempo la comunicación segura entre Bucaramanga-Bogotá por medio de la VPN.

CONCLUSIONES

Se diseñó e implementó una infraestructura de red en la empresa ANPRA Ltda que cumple con las características de seguridad necesarias para el intercambio de información entre las dos sedes. Estas sedes se unieron por medio de la VPN creada mediante los Routers Open Source Vyatta lo cual permitió obtener una relación costo/beneficio favorable a la compañía.

Se seleccionó la tecnología Open Source para no tener que recurrir a inversiones mayores en dispositivos comerciales que brindaban las mismas funciones pero incrementaban los costos.

Dentro de las opciones open source se eligió el sistema Vyatta debido al óptimo desempeño que podía brindar en la infraestructura de red y a la variedad de herramientas útiles que podía ofrecer en comparación a las otras Soluciones Open Source.

Se obtuvieron resultados óptimos en la comunicación de las dos sedes ubicadas en las ciudades de Bucaramanga y Bogotá, evidenciando la facilidad de manejo del sistema en general y la flexibilidad de configuración del Router Vyatta.

Con la selección de mecanismos y la implementación de protocolos de seguridad se logró garantizar la confiabilidad del sistema diseñado e implementado, reduciendo el riesgo de fallas mayores a causa de posibles ataques hacia los servidores de la empresa.

Se propusieron estrategias que minimizaran los riesgos de fallas internas que pudieran afectar el correcto funcionamiento de la red de ANPRA, identificando las vulnerabilidades existentes en la infraestructura de red con la que contaba la compañía, además del diseño e implementación de soluciones para fortalecer la seguridad de los datos almacenados en el sistema de información de la empresa.

Inicialmente se propuso realizar un prototipo donde se demostrara la funcionalidad del diseño, pero gracias a la colaboración por parte de la empresa se pudo implementar y actualmente, las sedes ubicadas en Bucaramanga y Bogotá, se encuentran utilizando la Red Privada Virtual creada por los Router Open Source Vyatta, intercambiando información entre sus servidores (listado de productos, clientes, almacenes, nómina, cartera, inventario de productos, etc.).

RECOMENDACIONES

Se recomienda a la empresa realizar los siguientes cambios en pro de su seguridad:

Diseñar y establecer políticas de seguridad de la información de la empresa que contribuyan a la escalabilidad de la compañía sin que estas afecten el core del negocio ni el desempeño de los empleados. Estas políticas deben tener como objetivo y deben estar enmarcadas en el mejoramiento de la calidad de producción de la empresa y concienciación del personal que labora en ANPRA.

Mejorar la seguridad física de los dispositivos de la empresa y el acceso a ellos, debido a que es un punto crítico dentro de la seguridad de la información de la empresa, ya que al estar expuestos los dispositivos de la compañía a personal no autorizado que pueda ocasionar algún tipo de daño, puede ser causa de cualquier acto malicioso que pueda afectar uno de sus activos más importantes (datos e Información).

Mantener actualizados todos los dispositivos de la empresa especialmente los Router Open Source Vyatta los cuales son la puerta de entrada a la infraestructura de red de la empresa.

Se recomienda hacer un análisis del tráfico de red generado y recibido por la sede ubicada en la ciudad de Bogotá, para que de esta manera se encuentren aspectos que puedan afectar el óptimo rendimiento de la red privada virtual. De igual manera se sugiere como prueba, crear la VPN entre los dos puntos utilizando un mismo proveedor de servicios de internet para ver si los tiempos de respuesta entre las dos sedes mejoran.

REFERENCIAS:

[1] Cosistec. “Que es una red de datos?”. La Paz, Bolivia. Mayo de 2008. Disponible en: http://www.cosistec.com/index.php?id=quienes

[2] MicroCisco-Staky. “Cisco Networking Academy Program, CCNA 1 y 2”. Version 3.1, curriculum en formato pdf. Abril 2006.

[3] Flórez, Angélica. “Redes de Datos”. Primera edición. Bucaramanga, Santander. 2007.

[4] Soul Cast Beta. “Curso de redes, Clasificación de las redes de comunicación. Lima, Perú. Octubre de 2006. Disponible en: http://www.soulcast.com/post/show/29431/redes

[5] Shvoong. “Topologías de red, Las redes WAN”. Herzliya, Israel. Septiembre de 2007. Disponible en: http://es.shvoong.com/internet-and-technologies/computers/1676349-topolog%C3%ADas-red/

[6] Revista RED, La comunidad de expertos en redes. “Fundamentos de Redes”. Ciudad de Mexico. Noviembre de 2002. Disponible en: http://www.ciberhabitat.gob.mx/museo/cerquita/redes/fundamentos/02.htm

[7] Soto, Lauro. “Conmutadores, Switch”. Tijuana, México. Abril de 2008. Disponible en: http://www.mitecnologico.com/Main/ConmutadoresSwitch

[8] Viklund, Andreas. “Soporte Hardware, Que es un Access Point”. Lima, Perú. Abril de 2007. Disponible en: http://mashard.perublogs.com/2007/04/Que-es-un-Access-Point.html

[9] Dnet Comunicaciones S.A. “Modulo servidor proxy”. Lima, Perú. 2007. Disponible en: http://www.dnet.com.pe/expansionibsd.htm

[10] Gómez Atuesta, Edwin. Velandía Enciso, Andrés. “Aspectos de seguridad en implementaciones de NAT & PAT”. Formato pdf. Bucaramanga, Colombia. Marzo de 2007.

[11] Molina L. Guillermo. “Seguridad en Aplicaciones y Bases de Datos”. Bucaramanga, Colombia. Septiembre de 2007. Disponible en: Especialización en Seguridad Informática, Universidad Pontificia Bolivariana.

[12] SEGU-INFO. “Seguridad de la Información, Seguridad Física”. Argentina. 2008. Disponible en: http://www.segu-info.com.ar/fisica/seguridadfisica.htm

[13] SEGU-INFO. “Seguridad de la Información, Seguridad Lógica”. Argentina. 2008. Disponible en: http://www.segu-info.com.ar/logica/seguridadlogica.htm

[14] Normadat. “Custodia y manejo de BackUp”. España. 2008. Disponible en: https://www.normadat.es/

[15] Red IRIS. “ Copias de seguridad”. Espanna. Julio 15 de 2002. Disponible en: http://www.rediris.es/cert/doc/unixsec/node13.html

[16] Hallberg, Bruce A. “Fundamentos de Redes, Seguridad de las cuentas”. Primera Edición. Traducido de la Tercera Edición de Networking a Beginner’s Guide. México, D.F. McGraw Hill. 2004; p 149-150

[17] Coll, Michael Henric. “Coaching Empresarial”. España. 2007. Disponible en: http://www.gestiopolis.com/canales/derrhh/articulos/63/coach.htm

[18] Caminoweb. “Hosting y Dominios, Planes Windows”. Bogotá, Colombia. 2008. Disponible en: http://www.caminoweb.com/products/pw.html

[19] Tenable. “Nessus, The Network Vulnerability Scanner”. Estados Unidos de América. 2008. Disponible en: http://www.nessus.org/nessus/

[20] Safety-Lab. “Shadow Security Scanner”. Estados Unidos de América. 2008. Disponible en: http://www.safety-lab.com/en/products/securityscanner.htm

[21] WikiLearning. “Manual sobre Shadow Security Scanner – Utilización del S.S.S. 2007. Disponible en: http://www.wikilearning.com/tutorial/manual_sobre_shadow_security_scanner-utilizacion_del_s_s_s/4363-2

[22] Red Hat, Inc. “Manual de referencia (Kerberos)”. 2008. Disponible en: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-kerberos.html

[23] Hardware.com. “Precio y características de Router Cisco”. Estados Unidos de América. 2008. Disponible en: http://us.hardware.com/product.asp?id=CISCO2811

[24] NORTEL. “Características de Secure Router 4134 de Nortel”. Estados Unidos de América. 2008. Disponible en: http://products.nortel.com/go/product_content.jsp?segId=0&parId=0&prod_id=62360

[25] VYATTA home page. *“Welcome to the dawn of Open Sourcenetworking, Corporate Overview and Vyatta name”.* 2007. Disponible en: http://www.vyatta.com/about/index.php

[26] Munguia, Leonel. “Vyatta, el fin de los Router Cisco”. Guatemala, Guatemala. Marzo de 2007. Disponible en: http://www.soportederedes.com/2007/03/vyatta-el-fin-de-los-routers-cisco.html

[27] VYATTA, INC. “White Paper, Why Vyatta is Better tan Cisco”. 2007. Formato pdf. Disponible en: http://www.vyatta.com/download/whitepapers/Vyatta_Better_than_Cisco.pdf

[28] Telecommunity. “Juniper y Cisco, amenazados por una compañía de enrutamiento de código abierto”. Febrero de 2006. Disponible en: http://www.telcommunity.com/visor.php?id_noticia=16441

[29] XORP. “XORP is the eXtensible Open Router Plataform”. Estados Unidos de América. 2008. Disponible en: http://www.xorp.org/

[30] EasyLiveCD. “Linux LiveCD Router – Free”. Estados Unidos de América. 2007. Disponible en: http://www.easylivecd.com/english/cdrouter/

[31] Freesco. “Free – Cisco”. Estados Unidos de América. 2006. Disponible en: http://www.freesco.org/index.php?id=o

[32] Rojo, Iñaki I. “Baquía, Open Source II”. España. Octubre de 1999. Disponible en: http://www.baquia.com/com/legacy/8513.html

[33] Caminoweb. “Hosting y Dominios, Planes Windows”. Bogotá, Colombia. 2008. Disponible en: http://www.caminoweb.com/products/pw.html