ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD DE LA RED LAN DE LA EMPRESA INSURCOL LTDA

MANUEL EDUARDO CARREÑO SANDOVAL

UNIVERSIDAD INDUSTRIAL DE SANTANDER

ESPECIALIZACIÓN EN TELECOMUNICACIONES

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES

BUCARAMANGA

2.010

ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD DE LA RED LAN DE LA EMPRESA INSURCOL LTDA

MANUEL EDUARDO CARREÑO SANDOVAL

Monografía presentada como requisito para optar al título de

Especialista en Telecomunicaciones

Director

Ing. Raúl Bareño Gutierrez

UNIVERSIDAD INDUSTRIAL DE SANTANDER

ESPECIALIZACIÓN EN TELECOMUNICACIONES

ESCUELA DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA Y DE TELECOMUNICACIONES

BUCARAMANGA

2.010

DEDICATORIA

A Dios por darme la iluminación y sensatez para afrontar este reto académico.

A mi señora madre y hermano menor, quienes son mi eje de fuerza y mi empuje para todas las acciones que tomo, desarrollo y concluyo.

A mis amigos y familiares que me apoyaron para seguir avanzando en mis estudios académicos para ser un mejor profesional.

AGRADECIMIENTOS

A la empresa Insurcol Ltda, quienes me brindaron el espacio para retomar mis estudios y llevarlos a una feliz culminación, unido a esto la confianza otorgada para el desarrollo de las diferentes labores dentro de la organización.

A todos mis compañeros de especialización, por haber sido un grupo abierto a nuevas vivencias, amistades y experiencias académicas.

Al director de proyecto Raúl Bareño Gutierrez por su ayuda desinteresada y orientación para la elaboración de esta monografía.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pàg.

LISTA DE TABLAS

Pàg.

GLOSARIO

AMENAZA: Del ingles Threat, es una situación donde humanos u ocurrencias naturales pueden causar un resultado indeseable.

ATAQUE: Es literalmente un asalto a la seguridad de un sistema y es derivada de una amenaza (Threat) inteligente. Los ataques producen una acción que viola la seguridad. Los ataques están divididos en 2 tipos: Activos y Pasivos y se pueden categorizar como externos o internos dependiendo del origen del ataque.

DATAGRAMA: Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ETD destino.

DHCP: (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor), es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

EXPLOIT: Significa Explotación, es una manera o vía definida para “romper” la seguridad de una computadora o sistema a través de las vulnerabilidades.

HUB: También llamado concentrador, es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs presentan un gran nivel de colisiones y propician o generan al alto margen de tráfico de red.

MODO PROMISCUO: Es aquel en el que una computadora conectada a una red compartida, tanto la basada en cable de cobre como la basada en tecnología inalámbrica, captura todo el tráfico que circula por ella.

MTU: La unidad máxima de transferencia (Maximum Transfer Unit - MTU), es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet.

PROXY: Programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

ROUTER: En español enrutador, direccionador, ruteador o encaminador, es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un router es

un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica la dirección IP del equipo deseado.

SWITCH: Un conmutador es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network- Red de Área Local).

TRAMA: En redes una trama es una unidad de envío de datos. Viene a ser sinónimo de paquete de datos o Paquete de red, aunque se aplica principalmente en los niveles OSI más bajos, especialmente en el Nivel de enlace de datos.

Normalmente una trama constará de cabecera, datos y cola. En la cola suele estar algún chequeo de errores. En la cabecera habrá campos de control de protocolo. La parte de datos es la que quiera transmitir en nivel de comunicación superior, típicamente el Nivel de red.

VULNERABILIDAD: Es la presencia de una falla, en cualquier fase de diseño o implementación de un sistema, programa (software), producto o componente, que puede llevar a comprometer la seguridad de un sistema. Tales vulnerabilidades pueden ser explotadas para producir perdida de información y/o penetrar en el sistema o producto vulnerable.

RESUMEN

TITULO: ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD DE LA RED LAN DE LA EMPRESA INSURCOL LTDA*.

AUTOR: MANUEL EDUARDO CARREÑO SANDOVAL **.

PALABRAS CLAVES: Seguridad Informática, política de seguridad informática, Firewall, ataques informáticos, vulnerabilidades

DESCRIPCION:

A medida que las tecnologías de la información y la comunicación siguen en continúa evolución, en asocio con la globalización de la Internet, estas han permitido el aumento del conocimiento de usuarios comunes en el manejo de herramientas informáticas, generando espacios de aprendizaje y de crecimiento de la curiosidad por parte de estos, incluyendo usuarios internos de una red empresarial que en ocasiones buscan conocer o romper la seguridad presente en la misma. Estos ataques afectan las actividades de las estructuras administrativas y comerciales de una organización, propiciando el robo o divulgación de información confidencial, afectando el Good Will de la empresa. En el mundo de hoy, la información tiene un valor elevado y debe ser protegida, significándole a un administrador de red de datos protegerla tanto de virus, troyanos y otros similares, sino también cuidarla de ataques de intrusos externos o filtraciones de usuarios internos por realizar ataques con el fin de detectar vulnerabilidades al interior de la red y obtener algún provecho.

La presente monografía no pretende analizar los diferentes ataques informáticos actuales o los mas frecuentes, como estos se podrían presentar, o que consecuencias traerían, sino mostrar un esquema de seguridad utilizado en una empresa, realizar algunos ataques al interior de esta, describir las fallas detectadas y presentar algunas opciones para su corrección, las cuales sirvan de soporte para el mantenimiento de la misma y a su vez sirva como caso de experiencia a otros administradores de red en su necesidad para determinar o fortalecer sus políticas de seguridad o refuerce los ya existentes.

---

* Trabajo de grado

** Facultad de Especialización en Telecomunicaciones. Escuela de Ingenierías Eléctrica, Electrónica y de Telecomunicaciones. Director: Raúl Bareño Gutierrez.

SUMMARY

TITLE: ANALYSIS OF THE POLITICIANS OF SECURITY OF THE NET LAN OF THE COMPANY INSURCOL LTDA*.

AUTHOR: MANUEL EDUARDO CARREÑO SANDOVAL**.

KEY WORDS: Computer security, politics of computer security, Firewall, computer attacks, vulnerabilities

DESCRIPTION:

As the technologies of the information and the communication continue in evolution it continues, in I associate with the globalization of the Internet, these they have allowed the increase of the knowledge of common users in the handling of computer tools, generating learning spaces and of growth of the curiosity on the part of these, internal users of a managerial net that look for to know or to break the present security in the same one in occasions including. These attacks affect the activities of the administrative and commercial structures of an organization, propitiating the robbery or popularization of confidential information, affecting the Good Will of the company. In today's world, the information has a high value and it should be protected, meaning an administrator of net of data to protect it so much of virus, troyanos and other similar ones, but also to take care of it of external intruders' attacks or internal users' filtrations to carry out attacks with the purpose of to detect vulnerabilities to the interior of the net and to obtain some profit.

The present monograph doesn't seek to analyze the different current computer attacks or those but you frequent, as these they could be presented, or that consequences would bring, but showing an outline of security used in a company, to carry out some attacks to the interior of this, to describe the detected flaws and to present some options for its correction, which serve as support for the maintenance of the same one and in turn serve like case of experience to other net administrators in its necessity to determine or to strengthen their politicians of security or already reinforce those existent.

*Grade project.

** Ability of Specialization in Telecommunications. Electric, Electronic school of Engineerings and of Telecommunications. Director: Raúl Bareño Gutierrez.

INTRODUCCIÓN

Con el crecimiento de Internet, su fácil manejo y manipulación, ha facilitado el conocimiento en sistemas ha diversas personas, debido a la gran cantidad de documentos y software que se puede descargar de manera libre, lo que ha hecho que los usuarios hayan incrementado sus conocimientos en diversas áreas, volviéndose mas curiosos, más adeptos y hasta más expertos respecto al conocimiento de los sistemas; en ciertas ocasiones, en algunos de estos usuarios se ha despertado, incrementado o generado la curiosidad por adentrarse en las redes de ciertas organizaciones o incluso en conocer falencias de la propia red de datos en donde laboran con el fin de aplicar lo aprendido, visto y/o escuchado para así utilizar el software o aplicativos descargados; esta facilidad tecnológica también le ha abierto la brecha a ciertos individuos que han aprendido y mejorado sus conocimientos informáticos o se han imaginado alguna manera para generar delitos informáticos en diversas categorías.

La presencia de virus informáticos ha sido el dolor de cabeza siempre presente para los administradores de redes de datos, sin embargo con el pasar de los años y avances tecnológicos este ha pasado a convertirse en un dolor controlable, a través de los antivirus los antispyware, entre otras diversas utilidades presentes ene. mercado, fortaleciendo la seguridad en la estación de trabajo, pero la existencia del comercio electrónico para la compra y venta de productos, entre diversos servicios ofrecidos y utilizados a través de la Web, generan espacios para que la seguridad informática se de cabida como un ítem importante para la protección de los activos informáticos de la

compañía, debido a la posibilidad de verse afectados por una consulta, acceso o malversación en el momento del envío o recepción de información.

Este trabajo de grado elaborará una pequeña evaluación a la seguridad informática de una empresa, mostrando el esquema de seguridad actual de la red informática de la empresa Insurcol Ltda, basado en algunos esquemas básicos de prevención, luego se mostrarán y explicarán algunos ataques controlados realizados a la red, para luego cerrar con algunas recomendaciones u observaciones sobre como mejorar este esquema de red y brindar o mejorar la calidad de la seguridad de la red.

Este trabajo busca ser un modelo de apoyo para otros administradores de red sobre falencias de seguridad generalmente presentes en las redes de datos y se muestran algunos consejos de cómo se podrían solucionar con unos pequeños tips que se mencionarán, sin que esto implique unja gran inversión en tecnología tanto en hardware como en software para una organización.

1. MARCO TEORICO

En este espacio se tratarán conceptos básicos referentes al estado actual y componentes de la red de la organización, tales como red de transmisión de datos, red de área local, protocolos, dispositivos de red, entre otros, además de mencionar conceptos sobre seguridad informática, ataques frecuentes y vulnerabilidades en las redes de tipo TCP/IP.

1.1 TERMINOLOGIA DE RED

1.1.1 Red de transmisión de datos.

Una red de transmisión de datos es un conjunto de elementos físicos y lógicos que permiten la interconexión de equipos y satisfacen todas las necesidades de comunicación de datos entre los mismos.

1.1.2 Red de área local

También llamada LAN (del inglés Local Area Network), Con estas se pretende cubrir espacios de transmisión internos o privados para la organización, a la cual se pueden conectar gran cantidad de dispositivos y compartir los recursos que estén allí disponibles, apta para la empresa ya que por lo general son elaboradas para edificios, para el caso de la monografía son dos casas contiguas, siendo un espacio de cobertura reducido a solo metros, la velocidad de

transmisión es de 1 a 100 Mbps (Megabits o millones de bits por segundo).

1.1.3 Medio de transmisión

La organización se encuentra básicamente conectada en cableado categoría 5 para la transmisión de datos en los equipos de la compañía.

Este cable es del tipo par trenzado, el cual se encuentra compuesto por conductores de cobre aislados en plástico y trenzado en pares, se cuenta con este tipo de cable debido a su bajo y costo y fácil adaptación para su conexión, este tipo de cable permite la conexión a 100 Mbps.

Este tipo de cable contiene 4 pares en su interior:

- Blanco/azul – azul … contactos: 5 * 4
- Blanco/ naranja – naranja … contactos: 3 * 6
- Blanco/ verde – verde … contactos: 1 * 2
- Blanco/ marrón … contactos: 7 * 8

El ponchado de este cable bajo permite que el equipo al cual se le conecte aproveche de mejor manera el ancho de banda existente en la red o el asignado por el esquema de red al cual pertenezca.

1.1.4 Topología de red

Es la forma física o aquella estructura de interconexión establecida para el establecimiento de comunicación y transmisión de datos entre los diferentes dispositivos de red pertenecientes a una red.

La compañía se encuentra bajo un esquema de red en estrella, donde las diferentes estaciones de trabajo se conectan a un nodo principal, este nodo principal distribuye las peticiones solicitadas por alguna terminal hacia otras estaciones, este equipo se conecta a un conmutador o switch, donde las demás estaciones se conectan a este para la recepción de datos. Una de las ventajas de este esquema, es en caso de falla de una estación, las otras pueden seguir funcionando normalmente sin verse afectadas por fallas individuales.

Los principales criterios para tener este tipo de topología es debido a su fiabilidad por garantizar la entrega y/o recepción de los datos solicitados, costo y tiempos de respuesta cortos en las peticiones solicitadas.

1.1.5 Firewall

Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

1.1.6 Protocolo TCP/IP

TCP (Transmission-Control-Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn.

Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

1.2 SEGURIDAD INFORMATICA

Seguridad Informática es el proceso de prevenir y detectar el uso no autorizado de las computadoras o de los recursos de red, estas medidas preventivas ayudan a los administradores de red a detener a los usuarios no autorizados (intrusos o Hackers) de acceder a cualquier parte del sistema de computadoras. La detección permite determinar quién o que está intentando penetrar al sistema, y si tuvieron éxito en la penetración al sistema, ¿que pudieron haber hecho o a que información tuvieron acceso en tu sistema?, la seguridad informática busca proteger aquellos bienes tangibles y no palpables de la organización como el software, los sistemas de información o las bases de datos, siendo solo utilizados y manipulados por el personal autorizado para tal fin.

1.2.1 Conceptos básicos[1]

Confidencialidad (Confidentiality)

Evita la divulgación intencional o accidental del contenido de un mensaje o cualquier otro tipo de información, es decir, sólo las personas o procesos autorizados pueden acceder a la información.

Integridad (Integrity)

El concepto de integridad garantiza que la información es exacta y completa, esto incluye los siguientes tópicos:

[1] MEDINA VILLALOBOS, Jorge Alberto. Introducción a la seguridad informática, Bucaramanga, 2009, 88p.

- Personas o procesos no autorizados no pueden modificar los datos.
- Personas o procesos autorizados no realizan modifican no autorizadas a los datos.
- Los datos son consistentes interna y externamente.

Disponibilidad (Availability)
Asegura que los usuarios autorizados podrán tener un acceso confiable y oportuno a la información o a los recursos computacionales en el momento que ellos lo requieran.

1.2.2 Otros Conceptos Importantes

Identificación (Identification)
Es el medio por el cual un usuario proclama su identidad ante un sistema. La identificación es usada comúnmente en Control de Acceso pues, es necesaria para la autenticación y la autorización.

Autenticación (Authentication)
Cuando se puede garantizar la identidad de un usuario y se comprueba que el usuario es quien dice ser.

Autorización (Authorization)
Son los derechos y permisos concedidos a un individuo o un proceso al que se le ha permitido acceder a un recurso computacional.

Observancia (Accountability)
Es la capacidad del sistema para registrar las acciones y el comportamiento de un individuo dentro del sistema, y su capacidad para determinar la identidad del usuario.

No Repudio (Don't Disavowal)
Es cuando la información involucrada en un evento corresponde a quien participa. Las personas que intervienen un evento no pueden evadir o negar su intervención.

1.3 VULNERABILIDADES DE UNA RED TCP/IP[2]

Vulnerabilidades de la capa de red. Las vulnerabilidades de la capa de red están estrechamente ligadas al medio sobre el que se realiza la conexión. Esta capa presenta problemas de control de acceso y de confidencialidad.

Vulnerabilidades de la capa internet. En esta capa se puede realizar cualquier ataque que afecte un datagrama IP. Se incluyen como ataques contra esta capa las técnicas de sniffing, la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes.

Cualquier atacante puede suplantar un paquete si indica que proviene de otro sistema. La suplantación de un mensaje se puede realizar, por

[2] ALFARO JOAQUÍN, García. Aspectos avanzados de seguridad en redes, Barcelona, 2004.

ejemplo, dando una respuesta a otro mensaje antes de que lo haga el suplantado.

En esta capa, la autenticación de los paquetes se realiza a nivel de máquina (por dirección IP) y no a nivel de usuario. Si un sistema suministra una dirección de máquina errónea, el receptor no detectaría la suplantación. Para conseguir su objetivo, este tipo de ataques suele utilizar otras técnicas, como la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc.

Por otro lado, los paquetes se pueden manipular si se modifican sus datos y se reconstruyen de forma adecuada los controles de las cabeceras. Si esto es posible, el receptor sería incapaz de detectar el cambio.

Vulnerabilidades de la capa de transporte. La capa de transporte transmite información TCP o UDP sobre datagramas IP. En esta capa podemos encontrar problemas de autenticación, de integridad y de confidencialidad. Algunos de los ataques más conocidos en esta capa son las denegaciones de servicio debidas a protocolos de transporte.

En cuanto a los mecanismos de seguridad incorporados en el diseño del protocolo de TCP (como las negociaciones involucradas en el establecimiento de una sesión TCP), existe una serie de ataques que aprovechan ciertas deficiencias en su diseño. Una de las vulnerabilidades más graves contra estos mecanismos de control puede comportar la posibilidad de interceptación de sesiones TCP establecidas, con el objetivo de secuestrarlas y dirigirlas a otros equipos con fines deshonestos.

Estos ataques de secuestro se aprovechan de la poca exigencia en el protocolo de intercambio de TCP respecto a la autenticación de los equipos involucrados en una sesión.

Así, si un usuario hostil puede observar los intercambios de información utilizados durante el inicio de la sesión y es capaz de interceptar con éxito una conexión en marcha con todos los parámetros de autenticación configurados adecuadamente, podrá secuestrar la sesión.

Vulnerabilidades de la capa de aplicación. Como en el resto de niveles, la capa de aplicación presenta varias deficiencias de seguridad asociadas a sus protocolos. Debido al gran numero de protocolos definidos en esta capa, la cantidad de deficiencias presentes también sería superior al resto de capas.

1.4 ATAQUES FRECUENTES*

1.4.1 Escuchas de red

Son aplicaciones que se encargan de capturar e interpretar tramas y datagramas en entornos de red basados en difusión, conocidos como escuchas de red o sniffers, es posible realizar el análisis de la información contenida en los paquetes TCP/IP que interceptan para

* Por el gran número de ataques existentes y el grado de definiciones presentes para este apartado, se realiza una conjugación de los conceptos encontrados en dos escritos, Introducción a la Seguridad Informática y Aspectos avanzados de seguridad en redes, recopilando puntos exactos sobre ataques frecuentes, pero sin afectar su sentido real de explicación

poder extraer todo tipo de información, siendo un Snnifer, un programa que intercepta toda la información que pase por la interfaz de red a la que esté asociado. Una vez capturada, se podrá almacenar para su análisis posterior.

De esta forma, sin necesidad de un acceso directo algún sistema de la red, un atacante podría obtener información sobre cuentas de usuario, claves de acceso o incluso mensajes de correo electrónico en el que se envían estas claves. Este tipo de técnica se conoce como sniffing.

Las técnicas de sniffing también se conocen como técnicas de eavesdropping y técnicas de snooping.

La primera, eavesdropping, es una variante del sniffing, caracterizada por realizar la adquisición o intercepción del tráfico que circula por la red de forma pasiva, es decir, sin modificar el contenido de la información.

Por otra parte, las técnicas de snooping se caracterizan por el almacenamiento de la información capturada en el ordenador del atacante, mediante una conexión remota establecida durante toda la sesión de captura. En este caso, tampoco se modifica la información incluida en la transmisión.

La forma mas habitual de realizar técnicas de sniffing en una red, probablemente porque está al alcance de todo el mundo, es la que podríamos denominar sniffing software, utilizando las aplicaciones que ya mencionadas.

1.4.2 Desactivación de filtro MAC

Es la posibilidad de configurar la interfaz de red para que desactive su filtro MAC (poniendo la tarjeta de red en modo promiscuo).

Las redes basadas en dispositivos Ethernet fueron concebidas en torno a una idea principal: todas las máquinas de una misma red local comparten el mismo medio, de manera que todos los equipos son capaces de ver el tráfico de la red de forma global.

Cuando se envían datos es necesario especificar claramente a quien van dirigidos, indicando la dirección MAC. De los 48 bits que componen la dirección MAC, los 24 primeros bits identifican al fabricante del hardware, y los 24 bits restantes corresponden al número de serie asignado por el fabricante. Esto garantiza que dos tarjetas no puedan tener la misma dirección MAC.

Para evitar que cualquier máquina se pueda apropiar de información fraudulenta, las tarjetas Ethernet incorporan un filtro que ignora todo el tráfico que no les pertenece, descartando aquellos paquetes con una dirección MAC que no coincide con la suya. La desactivación de este filtro se conoce con el nombre de modo promiscuo.

Con el uso adecuado de expresiones regulares y otros filtros de texto, se podría visualizar o almacenar únicamente la información que mas interese; en especial, aquella información sensible, como nombres de usuario y contraseñas.

El entorno en el que suele ser mas efectivo este tipo de escuchas son las redes de área local configuradas con una topología en bus. En este tipo de redes, todos los equipos están conectado a un mismo cable. Esto implica que todo el tráfico transmitido y recibido por los equipos de la red pasa por este medio común.

1.4.3 Suplantación de ARP

El protocolo ARP es el encargado de traducir direcciones IP de 32 bits, a las correspondientes direcciones hardware, generalmente de 48 bits en dispositivos Ethernet. Cuando un ordenador necesita resolver una dirección IP en una dirección MAC, lo que hace es efectuar una petición ARP (ARP-request) a la dirección de difusión de dicho segmento de red, FF:FF:FF:FF:FF:FF, solicitando que el equipo que tiene esta IP responda con su dirección MAC.

Es decir, una maquina A, con IP 192.168.0.10 con una MAC 0A:0A:0A:0A:0A:0A solicita por difusión qué dirección MAC está asociada a la IP 192.168.0.2. La máquina B, con IP 192.168.0.2 y MAC 0B:0B:0B:0B:0B:0B debería ser la única que respondiera a la petición.

Con el objetivo de reducir el tráfico en la red, cada respuesta de ARP (ARP-reply) que llega a la tarjeta de red es almacenada en una tabla caché, aunque la máquina no haya realizado la correspondiente petición. Así pues, toda respuesta de ARP que llega a la máquina es almacenada en la tabla de ARP de esta máquina. Este factor es el que se utilizaría para realizar el ataque de suplantación de ARP, este engaño se conoce con el nombre de envenenamiento de ARP”.

El objetivo de un ataque de suplantación de ARP es poder capturar tráfico ajeno sin necesidad de poner en modo promiscuo la interfaz de red, envenenando la tabla de ARP de los equipos involucrados en la comunicación que se quiere capturar se puede conseguir que el conmutador les haga llegar los paquetes. Si el engaño es posible, cuando las dos máquinas empiecen la comunicación enviarán sus paquetes hacia la máquina donde está el sniffer y este, para evitar descubrir el engaño, se encargará de encaminar el tráfico que ha interceptado.

Una posible solución para evitar ataques de suplantación de ARP es la utilización de direcciones MAC estáticas, de manera que no puedan ser actualizadas. En este caso, los ARP-Reply enviados por el atacante serían ignorados. El principal inconveniente de esta solución es que el encargado de administrar la red debe almacenar en la tabla ARP la asociación entre la dirección IP con sus correspondientes direcciones MAC de cada equipo de la red y actualizar de forma manual en el caso de cambios de tarjetas Ethernet en los equipos involucrados.

1.4.4 Fragmentación IP

.

El protocolo IP es el encargado de seleccionar la trayectoria que deben seguir los datagramas IP. No es un protocolo fiable ni orientado a conexión, es decir, no garantiza el control de flujo, la recuperación de errores ni que los datos lleguen a su destino.

La fragmentación divide los datagramas IP en fragmentos de menor longitud y se realiza en el nivel inferior de la arquitectura para que sea

posible recomponer los datagramas IP de forma transparente en el resto de niveles. El reensamblado realiza la operación contraria.

El proceso de fragmentación y reensamblado se irá repitiendo a medida que los datagramas vayan viajando por diferentes redes.

Aunque la fragmentación es, por lo general, una consecuencia natural del tráfico que viaja a través de redes con MTU de distintos tamaños, es posible que un atacante pueda realizar un mal uso de esta propiedad del protocolo IP para provocar ataques de denegación de servicio (a causa de una mala implementación de la pila TCP/IP), así como para esconder y facilitar la fase de recogida de información o incluso para hacer pasar desapercibidos e introducir en la red paquetes para la explotación de servicios.

1.4.5 Ataques de denegación de servicio

.

Un ataque de denegación de servicio, es un incidente en el cual un usuario o una organización es privada de los servicios de un recurso que esperaba obtener. Normalmente, la pérdida de servicio se corresponde con la imposibilidad de obtener o acceder a un determinado servicio o recurso de red por parte de un usuario legítimo como, por ejemplo, el acceso a una página web.

.

Los ataques de denegación de servicio pueden ser provocados tanto por usuarios internos en el sistema como por usuarios externos. Dentro del primer grupo podríamos pensar en usuarios con pocos

conocimientos que pueden colapsar el sistema o servicio inconscientemente.

Por ejemplo, usuarios que abusan de los recursos del sistema, ocupando mucho ancho de banda en la búsqueda de archivos de música o de películas, usuarios malintencionados que aprovechan su acceso al sistema para causar problemas de forma premeditada, etc.

En el segundo grupo se encuentran aquellos usuarios que han conseguido un acceso al sistema de forma ilegitima, falseando además la dirección de origen con el propósito de evitar la detección del origen real del ataque (mediante ataques de suplantación).

El peligro de los ataques de denegación de servicio viene dado por su independencia de plataforma. El protocolo IP permite una comunicación homogénea (independiente del tipo de ordenador o fabricante) a través de espacios heterogéneos (redes Ethernet, ATM, entre otras). De esta forma, un ataque exitoso contra el protocolo IP se convierte inmediatamente en una amenaza real para todos los equipos conectados a la red, independientemente de la plataforma que utilicen.

1.4.6 IP Flooding

El ataque de IP Flooding se basa en una inundación masiva de la red mediante datagramas IP.

Este ataque se realiza habitualmente en redes locales o en conexiones con un gran ancho de banda. Consiste en la generación de tráfico

basura con el objetivo de conseguir la degradación del servicio. De esta forma, se resume el ancho de banda disponible, ralentizando las comunicaciones existentes de toda la red.

1.4.7 Smurf DoS

El atacante selecciona una victima y un intermediario, el cual debe tener un ancho de banda mucho mayor que el de la victima; una vez seleccionados los objetivos, el atacante envía un paquete ICMP echo request (ping) a la dirección de broadcast de la red que está usando como intermediario (10.255.255.255), con esto las 224 – 2 hosts de la red enviaran simultáneamente un paquete ICMP reply a la dirección que originó el ICMP echo request, la cual en este caso será la IP spoofeada de la victima.

Si el atacante envía este ping de forma ininterrumpida a intervalos muy pequeños, la red con un gran ancho de banda inundará a la victima con paquetes ICMP replies, impidiendo que la victima pueda utilizar su ancho de banda para realizar sus tareas cotidianas.

Este tipo de ataque puede evitarse modificando los dispositivos de red para que no respondan a paquetes tipo broadcast, y adicionalmente, los host de la red no deberían responder a paquetes ICMP enviados a la dirección de broadcast

1.4.8 Man-in-the-middle (MITM)

En este tipo de ataques, el intruso se sitúa en el medio de una comunicación entre dos personas, sin que ninguna de las partes se entere que el canal de comunicaciones ha sido comprometido. Cuando este tipo de ataques se presenta, el atacante obtiene la posibilidad de leer, insertar o modificar el tráfico entre las victimas. Para realizar este tipo de ataques, el intruso debe hacer uso de otros ataques como lo son el ARP spoofing e IP Spoofing.

1.4.9 TCP/SYN Flooding

Cada vez que se procesa una conexión, deben crearse datagramas IP para almacenar la información necesaria para el funcionamiento del protocolo. Esto puede llegar a ocupar mucha memoria. Como la memoria del equipo es finita, es necesario imponer restricciones sobre el número de conexiones que un equipo podrá aceptar antes de quedarse sin recursos.

El ataque de TCP/SYN Flooding se aprovecha del número de conexiones que están esperando para establecer un servicio en particular para conseguir la denegación del servicio.

Cuando un atacante configura una inundación de paquetes SYN de TCP, no tiene ninguna intención de complementar el protocolo de intercambio, ni de establecer la conexión. Su objetivo es exceder los límites establecidos para el número de conexiones que están a la espera de establecerse para un servicio dado.

Esto puede hacer que el sistema que es víctima del ataque sea incapaz de establecer cualquier conexión adicional para este servicio hasta que las conexiones que estén a la espera bajen el umbral.

Hasta que se llegue a este límite, cada paquete SYN genera un SYN/ACK que permanecerá en la cola a la espera de establecerse, debido a que cada conexión tiene un temporizador, es decir, un límite de tiempo para que el sistema espere el establecimiento de la conexión, cuando se excede el límite de tiempo, se libera la memoria que mantiene el estado de esta conexión y la cuenta de la cola de servicios disminuye en una unidad. Después de alcanzar el límite, puede mantenerse completa la cola de servicios, evitando que el sistema establezca nuevas conexiones en este puerto con nuevos paquetes SYN.

El único propósito de la técnica es inundar la cola de servicios, el atacante normalmente falsea la dirección de origen del paquete, modificando la cabecera IP de los paquetes que intervendrán en el ataque de una inundación SYN.

1.4.10 Back Door

Los ataques tipo back door pretenden obtener acceso a una red mediante un bypass a todas las políticas de seguridad de la organización Estos ataques están ligados al uso de conexiones tipo dial-up o redes telefónicas.

1.4.11 Troyanos (Trojan Horses)

Los troyanos son aplicaciones que esconden en su interior código malicioso bajo la apariencia de ser herramientas útiles. Una vez que se ejecutan estos programas, el código malicioso (virus, gusano) inicia su ataque a la red. En la mayoría de los casos, los troyanos pretenden permitir acceso no autorizado a los dispositivos atacados (estación de trabajo, servidor). Un troyano puede verse como una aplicación que abre back doors que serán posteriormente explotadas por un intruso; generalmente, esta puerta trasera es un puerto abierto.

1.4.12 Exploids

El termino exploid hace referencia a una pieza de software que se aprovecha de errores o vulnerabilidades de un código. Generalmente se utilizan para realizar escaladas de privilegios o negaciones de servicio.

Los exploits se pueden clasificar dependiendo del tipo de vulnerabilidad que atacan. Entre los más comunes están:

- Buffer overflow: Es un error de software en el cual se copia una cantidad de datos de gran tamaño sobre un área de memoria más pequeña. Si la operación no se interrumpe se sobrescribirán otras zonas de memoria. En algunos casos esto supone la posibilidad de alterar el flujo del programa, permitiendo que realice operaciones no previstas.

- Format String: Estas vulnerabilidades aparecen comúnmente cuando el programador desea imprimir una cadena de caracteres que contienen datos suministrados por el usuario. Esto sucede debido a que, por lo general, los programadores no definen correctamente las dimensiones de las variables de entrada y salida.

1.4.13 SMTP Spoofing

El atacante falsea los encabezados de SMTP para enviar correos electrónicos a nombre de terceras personas. Este tipo de ataque se presenta debido a que el protocolo SMTP no posee mecanismos de autenticación propios.

1.4.14 Phishing

Estos ataques pretenden obtener información sensible de forma fraudulenta, tal como lo son los passwords y los números de tarjetas de crédito. El ataque se basa en la suplantación de una persona o un dominio confiable por medio de un mensaje (e-mail spoofing) aparentemente real dentro del cual existe un hipervínculo con el nombre de un dominio real, pero que internamente redireccionará al usuario a un sitio falso. El phishing es una combinación de SMTP spoofing y URL Spoofing

1.4.15 Virus

Los virus son códigos maliciosos que se adhieren a un programa y se ejecutan cuando el programa anfitrión es ejecutado. Los virus suelen infectar los sistemas operativos de dos formas diferentes: reemplazando uno o más programas del SO; o adjuntándose a sí mismos en un programa del SO, alterando su funcionalidad. Una vez que un virus cambia la funcionalidad del SO, queda habilitado para controlar varios de los procesos que se están ejecutando.

Para evitar ser detectados, los virus usualmente crean varios archivos ocultos dentro del código fuente del SO o en sectores que no se encuentran actualmente en uso. Cuando un virus logra infectar un SO puede provocar graves consecuencias sobre los sistemas que dependen este para desempeñar funciones básicas.

El ciclo de vida de un virus está compuesto por dos fases: reproducción y activación. En la fase de reproducción el virus permanece oculto y no interfiere con el funcionamiento normal del sistema infectado, sin embargo, durante este periodo el virus busca activamente nuevos anfitriones en los que pueda replicarse. En la fase de activación, el virus inicia un proceso gradual o repentino de destrucción sobre el sistema infectado; por lo general el virus puede activarse basándose en una fecha o una hora determinada. A continuación se describen los tipos más comunes de virus:

- Virus tipo Macro: Son el tipo de virus más comunes y suelen afectar muchos tipos de aplicaciones, generalmente Microsoft

Excel y Microsoft Word. Se esparcen principalmente por medio del correo electrónico, adhiriéndose a los archivos adjuntos. Entre los más conocidos están el virus Melisa y el virus I Love You.

- Virus polimórficos: Este tipo de virus son difíciles de detectar debido a se ocultan del antivirus cambiando su apariencia después de cada infección. Un virus polimórfico podría adoptar más de 2x109 formas diferentes. Por ejemplo: Beagle, Doser.

- Virus Stealth: Pueden ocultar su presencia interceptando los servicios de interrupción y retornando información falsa al software antivirus y a los usuarios finales, el programa recibe los datos que espera aunque no correspondan con el estado real del archivo o zona del disco interrogados. Ocultan las variaciones de tamaño y los cambios de fechas de los archivos infectados. Por ejemplo: Dark Avenger, Brain.

- Works: Este tipo de virus no se adhiere a los archivos sino que reside en la memoria del sistema, desde allí se autoreplica y se transporta a través de la red, infectando rápidamente otras máquinas. Debido a la forma en que se replican, los recursos del sistema infectado se consumen hasta el punto de provocar que las tareas ordinarias se hagan excesivamente lentas o simplemente no puedan ejecutarse. Por ejemplo: Netsky, Nimda.

1.4.16 Spam

Se define como Spam el hecho de enviar correos electrónicos no solicitados y en cantidades masivas. La publicidad y el mercadeo de cosas ilegales o restringidos (material pornográfico, drogas, títulos profesionales) generan la mayor parte del spam en el mundo, no obstante, se considera como spam otro tipo de correos como lo son aquellos que pretenden engañar a los usuarios (fraudes, hoaxes, bromas, etc.).

1.4.17 Adware

Son agentes de software que se instalan en el sistema operativo. Tiene como función desplegar avisos publicitarios a través de ventanas emergentes del navegador. Por lo general, este tipo de código se instala por medio de controles ActiveX cuando el usuario está navegando, o cuando el usuario instala en su máquina aplicaciones tipo freeware o shareware.

1.4.18 Spyware

Este tipo de código resulta potencialmente peligroso cuando se instala en un equipo pues tiene la capacidad de recopilar información sobre los usuarios que trabajan sobre la máquina infectada. La información recopilada por el spyware es, generalmente, enviada a un tercero a través de Internet.

1.5 Beneficios de la Seguridad Informática

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Se evitan pérdidas de datos por causa de virus o gusanos.
- Prevenir la propagación de virus en su red.
- Minimizar el riesgo de ser espiado o controlado desde Internet.
- Prevenir robos de información.
- Uso de la navegación de Internet de forma segura.
- Bloquear las incursiones por 'puertas traseras' en las estaciones de trabajo.

2. DIAGNÓSTICO DEL ESTADO ACTUAL DE LA RED DE DATOS

2.1 Descripción de componentes y convenciones de los equipos de red.

En la actualidad la empresa Insurcol Ltda. Cuenta con 56 equipos de computo y un servidor Proxy, el cual a su vez funciona como Firewall o cortafuegos y un MODEM DSL proporcionado por el ISP (Proveedor de servicios de Internet), el cual esta conectado a este Proxy/firewall para dar la salida a Internet.

Este Proxy/Firewall, cuenta con un sistema operativo llamado PF/SENSE, el cual es de versión libre, su navegación puede ser a través de una interfaz WEB o de consola, este sistema operativo permite el acceso a los usuarios a Internet a través de una de sus características que es el portal cautivo, el cual permite acceder a los servicios de Internet ya sea a través de la solicitud de un login y password o de paso libre, este paso libre es determinado en una sección del PFsense, donde se determina cual o cuales direcciones IP se pueden asignar sin acceso restringido, lo que le brinda un nivel de seguridad para aquellas personas que se conecten a la red interna, a su vez este permite hacer seguimiento de la navegación de los usuarios, determinar IP usadas en el momento de hacer la consulta a través de la tabla ARP, limitar acceso a páginas o dar acceso libre, a través de cerrar puertos o la sección de reglas para permitir paso a ciertas páginas o todas en general dependiendo de la dirección que se le asigne al usuario, ya que este sistema operativo da permiso libre es a IP’s fijas mas no a un usuario o usuarios determinados.

La empresa cuenta básicamente con:

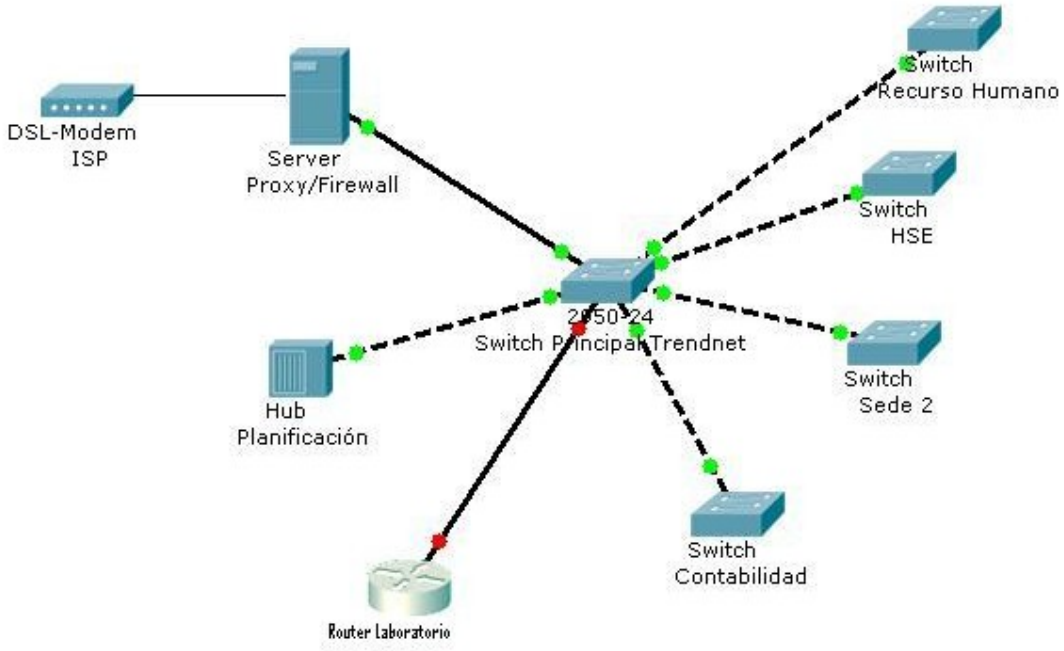
- Un servidor principal, el cual es el PFsense, quien hace las veces de servidor Proxy, servidor DHCP y de Firewall.

- Un Switch principal de 24 puertos al cual se conectan los demás switches de las secciones del área administrativa junto con algunas estaciones de la compañía.

- Un MODEM ADSL, por el cual se obtiene el servicio de Internet por medio del proveedor de servicios, este MODEM esta conectado al PFsense, quien es el encargado de dar la salida y la entrada de Internet para los diferentes usuarios conectados a la red.

- Un router, ubicado en la zona de laboratorio, donde básicamente se conectan aquellos usuarios flotantes que llegan con equipos portátiles y se les genera una dirección de conexión automática por DHCP, esta dirección es generada por el PFsense, junto con un login y un password para que puedan establecer conexión.

Figura 1. Diagrama Lógico de Red



Fuente: Insurcol Ltda.

2.2 Elaboración de Esquemas de red actual por áreas administrativas.

Actualmente la empresa Insurcol LTDA cuenta con un esquema de red bajo la topología en estrella operando así:

Switch Principal:

Se denomina como principal debido a que a este equipo es donde esta conectado el servidor PFsense (Proxy/Firewall,), quien se encarga de compartir el Internet hacia las demás estaciones, a su vez a este

conmutador se conectan los switches de las áreas de HSE, Recurso Humano, Contabilidad, Switch Sede 2 y algunas estaciones como las de Gerencia, Subgerencia, Asistentes Administrativos, sistemas y el Hub de planificación.

Es un conmutador que trabaja bajo capa dos, no es configurable.

Tabla 1. switch TE100-S24

Equipo	 Conmutador de 24 puertos a 10/100Mbps TE100-S24
Marca	Trendnet
Características	• 24 puertos Auto MDI-II/MDI-X NWay a 10/100Mbps • Integra un motor de búsqueda de dirección y soporta hasta una dirección MAC de 8k. • RAM interno de 1,5Mb para un registro de estructura (frame buffering). • Modo de transferencia Full/half dúplex para cada puerto.

	• Velocidad por cable de filtrado y reenvío. • Control de flujo IEEE 802.3x para modo full-dúplex . • Control de flujo de contrapresión para modo half-dúplex. • Método de conmutación de almacenamiento y reenvío. • LEDs de diagnóstico de gran alcance en el panel frontal. • Sin ventilador de refrigeración para una buena operación.

Switch Recurso humano:

En esta área se encuentran ubicadas 8 estaciones de trabajo de las cuales 6 se conectan al switch y 2 directamente al switch principal.

Tabla 2. switch DES-1008D

Equipo	 DES-1008D
Marca	Dlink

Características	8 Puertas 10/100Mbps. Las puertas tienen la capacidad de negociar las velocidades de red entre 10BASE-T y 100BASE-TX, como también el modo de operación en Half o Full Duplex.

Switch Hse:

En esta área se encuentran ubicadas 4 estaciones de trabajo las cuales se conectan al switch Trendnet.

Tabla 3. Switch TE100-S8

Equipo	 Switch TE100-S8
Marca	Trendnet
Características	¦ 8 puertos RJ-45 Fast Ethernet Auto-MDIX y de Auto-Negociación a 10/100Mbps ¦ Compatible con los estándares IEEE 802.3 y IEEE 802.3µ ¦Compatible con control de flujo IEEE 802.3x ¦Ofrece entradas de dirección MAC de 1K ¦ Compatible con Windows, Linux, y los sistemas

	operativos de Mac. ¦ Método de conmutación de almacenamiento y reenvío ¦Arquitectura sin bloqueos. ¦LEDs de diagnóstico. ¦Plug & Play.

Switch Contabilidad:

En esta área se encuentran ubicadas 8 estaciones de trabajo de las cuales 6 se conectan al switch 3com y las otras 2 van directamente al switch principal.

Tabla 4. Switch 3Com OfficeConnect

Equipo	 3Com OfficeConnect Fast Ethernet Switch 8
Marca	3Com
Características	Conmutación 10/100 Ethernet. Instalación plug-and-play y sin necesitar ninguna configuración, se adapta fácilmente en su red no administrada. La función de full-duplex admite la transferencia de datos bidireccional, duplicando el ancho de banda eficaz de la red.

HUB Planificación:

En esta área se encuentran ubicadas 7 estaciones de trabajo, de las cuales 2 se conectan directamente al switch principal y las restantes 5 a un HUB de 8 puertos.

Tabla 5. HUB Genius 8 Puertos

Equipo	Marca	Características
 HUB	Genius	Standard: IEEE802.3, 10Base-T,10Base-2 & Repeater Specification Interface: 8 x RJ-45 connectors, 1 x BNC connectors Data Rate: 10 Mbps Dimensiones: 19cm x 12.5cm x 2.6cm

Switch Sede 2:

Tabla 6. Switch TE100-S24

Equipo	
	 Conmutador de 24 puertos a 10/100Mbps TE100-S24

Marca	Trendnet
Características	• 24 puertos Auto MDI-II/MDI-X NWay a 10/100Mbps. • Integra un motor de búsqueda de dirección y soporta hasta una dirección MAC de 8k. • RAM interno de 1,5Mb para un registro de estructura (frame buffering). • Modo de transferencia Full/half dúplex para cada puerto. • Velocidad por cable de filtrado y reenvío. • Control de flujo IEEE 802.3x para modo full-dúplex. • Control de flujo de contrapresión para modo half-dúplex. • Método de conmutación de almacenamiento y reenvío. • LEDs de diagnóstico de gran alcance en el panel frontal. • Sin ventilador de refrigeración para una buena operación.

Este equipo es un concentrador, al cual se conectan los equipos de las áreas de Calidad, Importaciones, Departamento Técnico, donde:

Dpto Técnico cuenta con 13 computadores.
Importaciones cuenta con 4 computadores.
Calidad cuenta con 6 computadores.

Para las áreas de Dpto técnico y de calidad se encuentran ubicados otros 3 switch de 8 puertos para dar cobertura a las estaciones de trabajo restantes allí ubicadas.

3. DEFINICIÓN DE POLÍTICA DE SEGURIDAD INFORMÁTICA

3.1 Descripción de controles actuales

Acceso a Internet.

En la actualidad el control existente es a través del Proxy/Firewall, el cual permite la navegación o salida a Internet, esta navegación se activa cuando el usuario abre su navegador por primera vez luego de encender el equipo, donde se le solicita un login y password (esta solicitud de loggeo se realiza todos los días, en caso de reinicio del servidor, por inactividad de la cuenta durante dos horas o luego de 12 horas de estar activa la sesión volverá a pedir loggeo), de estar correctos los datos diligenciados podrá navegar e incluso descargar correos o enviarlos a través de Microsoft Outlook o el Outlook Express. aplicativo donde se encuentran instaladas las cuentas de correo de la empresa asignadas para cada usuario o área.

Copias de seguridad.

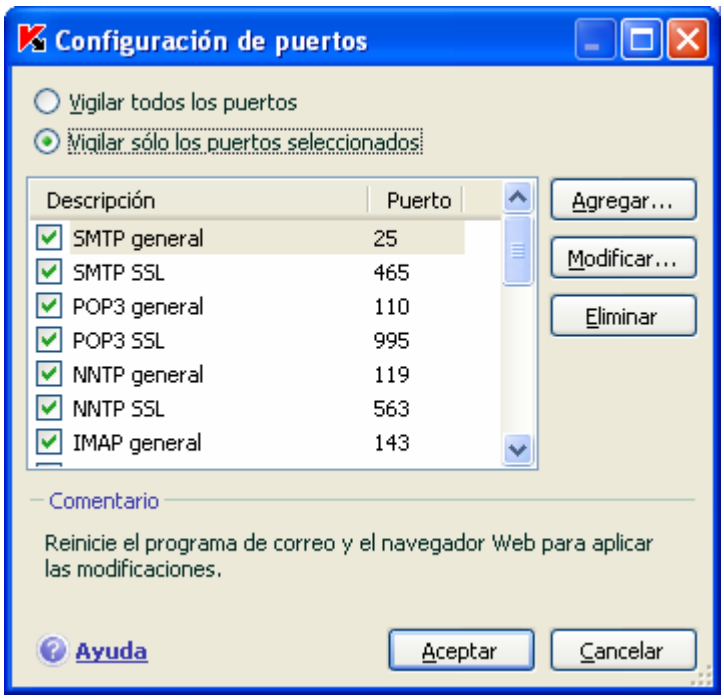
Para salvaguardar la información, la organización adapto un cuarto, el cual es restringido para todos los empleados de la organización excepto para aquella persona encargada de almacenar , buscar y retirar estas copias en caso de ser solicitadas para consulta, revisión o recuperación de información, este cuarto es para el almacenamiento de los CD's y los DVD's generados por las diferentes dependencias de la empresa, estas copias son generadas mensualmente por los usuarios de computadores de escritorio y de computadores portátiles de los

diferentes departamentos, sin embargo ciertas áreas debido a la importancia de su información, realizan un back up diario.

Control sobre software malicioso

En la actualidad la compañía ha delegado un presupuesto para la adquisición de antivirus para todos y cada uno de los equipos, licencias que se han renovado en este segundo año luego de su adquisición y licencias nuevas para los equipos comprados recientemente, para esta adquisición se probo con varias versiones betas y de licenciamiento libre, donde una de estas fue la que brindo mas respaldo y seguridad para la protección del equipo, dándose el voto de confianza sobre el Kaspersky Internet Security, este es un programa que unifica en un solo aplicativo todo un esquema de protección, ya que no solo es antivirus, sino que ofrece brinda otros módulos como la protección contra el correo no deseado, las intrusiones de piratas, protección contra amenazas desconocidas y ciertos tipos de fraude por Internet, así como la posibilidad de controlar el acceso del usuario a Internet, ya que cuenta con la posibilidad de ejercer un pequeño de control de trafico del equipo por medio del bloqueo de puertos (Ver figura Configuración de Puertos Kaspersky).

Figura 2. Configuración de Puertos Kaspersky



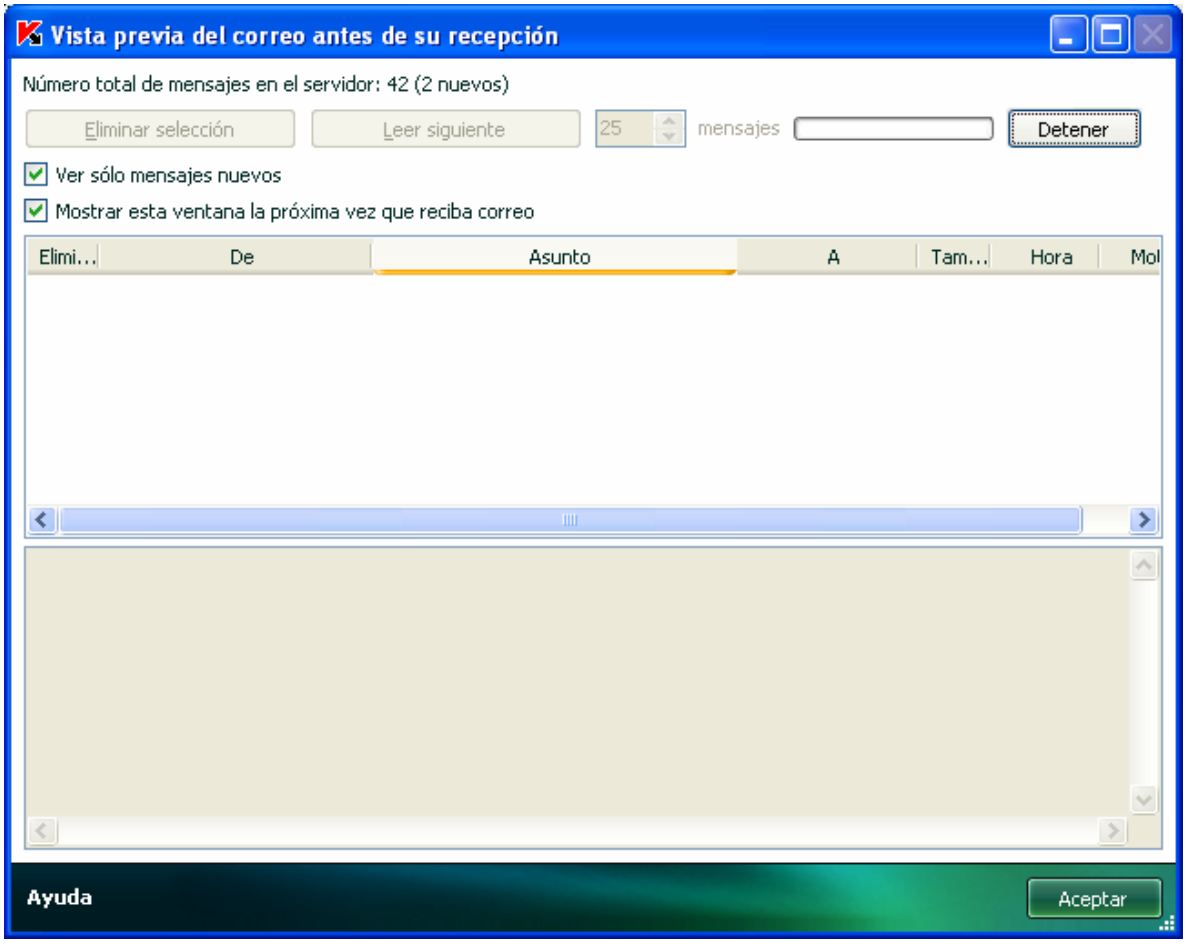
Fuente: Kaspersky Internet Security

Además de esto posee un componente llamado Defensa proactiva diseñado para analizar el comportamiento de las aplicaciones instaladas en su equipo, supervisar los cambios en el Registro del sistema, rastrear las macros y luchar contra amenazas ocultas. El componente utiliza un analizador heurístico capaz de detectar varios tipos de programas malintencionados. Para ello, mantiene un histórico de la actividad maligna, aplicando el principio de que es posible deshacer las acciones de un programa malintencionado y restaurar el sistema al estado anterior a los daños.

El programa protege a los usuarios contra procesos ocultos (rootkits) y marcadores telefónicos; bloquea pancartas publicitarias (banners) ventanas emergentes y secuencias de comandos malévolas descargadas de sitios Web; detecta sitios con anzuelos (phishing) y protege a los usuarios contra la transmisión no autorizada de datos confidenciales (contraseñas para conexiones Internet, correo o servidores ftp).

Otra buena característica es debido a que en la empresa se utiliza como cliente de correo el Microsoft Office Outlook y el Microsoft Outlook Express para el envío y recepción de correos, ofreciéndole este aplicativo una protección sobre el correo no deseado, debido a su componente antispam, el cual presenta una pantalla (Ver figura AntiSpam Kaspersky) antes de descargar los correos a la bandeja de entrada para que el usuario seleccione aquellos de usuarios desconocidos y los elimine. El programa analiza los mensajes enviados con estos protocolos en busca de virus, brindando una posibilidad de configurar el antivirus directamente en el cliente de correo.

Figura 3. Figura AntiSpam Kaspersky



Fuente: Kaspersky Internet Security

3.2 Alcance de política de seguridad

En el momento la organización no cuenta con una clara o implementada política de seguridad informática, básicamente se limita a control de acceso a Internet, y la asignación de una clave para cada usuario para que este pueda navegar en Internet, recibir y enviar correos; lo que se pretende es establecer una política de seguridad clara, estable, racional y acorde a los requerimientos de la empresa, la cual sea ecuánime para

las diferentes secciones del área administrativa de la empresa Insurcol para la sede de Bucaramanga.

Para esto, se debe determinar por parte de la organización la lista de servicios que serán ofrecidos por la red, las áreas de la organización proveerán tales servicios, quien o quienes tendrán acceso a esos servicios, Quién administrará esos servicios, entre otros.

Sin embargo para el caso de esta monografía lo que se pretende es establecer la política para el Firewall, siendo esta una política de bajo nivel que describe cómo el firewall controlará el acceso a los servicios restringidos.

Esta tarea se puede realizar bajo dos esquemas, permitir todos los servicios, e ir restringiendo a medida que se detectan las falencias o denegar todos los servicios, e ir permitiendo a medida que se requieran.

Finalmente anexar unos acuerdos internos a través de direcciones IP o de listas de control de acceso unos ítems específicos del sistema, donde se determine de acuerdo a las funciones del usuario el control de acceso o el permiso de acceso a ciertos recursos para ciertos individuos de la organización.

Para que esta política sea efectiva, una política requiere viabilidad, para favorecer su implementación, asegurarse de que sea comunicada a través de la toda la organización. Además, debe ser integrada y consistente con otras directivas existentes, leyes, guías, procedimientos, y la misión global de la empresa.

3.3 Establecimiento de plan de seguridad

La generación de un buen plan de seguridad, ofrece un marco o una pauta de guía general para el forjamiento de una política de seguridad, de esta forma la política o las diferentes políticas que se creen o se implementen serán consistentes con toda la arquitectura de seguridad, para esto se debe:

Determinar objetivos. Estos objetivos dependen de las necesidades a cubrir por parte de la empresa y se relacionan básicamente con:

Servicios ofrecidos frente a la seguridad provista: cada servicio ofrecido a un usuario tiene su propio riesgo de seguridad.

Facilidad de uso frente a la Seguridad: Un sistema muy fácil de usar permitirá el acceso a casi todos los usuarios y por lo tanto serán menos seguro.

Costo de la seguridad frente al Riesgo de pérdida: existen muchos costos de seguridad: monetarios, de desempeño y facilidad de uso. Los riesgos de pérdida pueden ser de privacidad, de datos, y servicios. Cada tipo de costo debe ser balanceado con respecto a cada tipo de perdida.

3.3.1 Definición de la política de seguridad

“Una política de seguridad es un enunciado formal de las reglas que los usuarios que acceden a los recursos de la red de una organización deben cumplir” [RFC-2196].

Lo que se busca básicamente con la política de seguridad es:

- Informar a los usuarios de la red sus obligaciones o deberes para proteger a los recursos de la red.

- Especificar los mecanismos a través de los cuales estos requerimientos pueden ser logrados.

- Proveer una guía que permitirá implementar, configurar y controlar los sistemas de la red para determinar su conformidad con la política.

3.3.2 Elaboración de la política de seguridad

Al permitir el acceso de los servicios de la red de la organización al personal, se generan o se pueden presentar ciertos peligros, donde algún usuario podría explotar o detectar vulnerabilidades potenciales, aumentándose la dificultad y complejidad para la protección de la red de datos, sin embargo, al enfrentar los riesgos, se pueden minimizar estos mismos. Para esto, se debe tener un conocimiento detallado de los riesgos que pueden ocurrir en el manejo y uso de los protocolos de red, de los sistemas operativos y de las aplicaciones que son accesadas, así

como las medidas que pueden ser tomadas para protegerlos. El plan es el primer paso y es la base para asegurar que todas las bases sean cubiertas.

Aun cuando la empresa en la actualidad cuenta con un cortafuego, asegurar los datos involucra algo más que solo conectarse a un firewall con una interface atractiva. Lo que se requiere es de un plan comprensivo de defensa. El cual debe ser comunicado para que pueda ser significativo para la gerencia y usuarios finales. Esto conlleva capacitación, unido a la explicación de las consecuencias de las violaciones. La política puede llevar inmersa la instalación de un firewall (el cual ya existe actualmente), pero no necesariamente la política de seguridad gira en torno al montaje, las restricciones o reglas que se puedan establecer a través del firewall.

Al elaborar la política de seguridad esta debe atender a los 3 conceptos básicos referenciados en el marco teórico de esta monografía, confidencialidad, integridad, disponibilidad,

Para diseñar la política de seguridad de una red se deben generar y responder algunas cuestiones de índole general para los asuntos internos de seguridad para la organización y sean claves para poder llevar a cabo una sólida definición.

Las preguntas podrían ser:

- ¿Que recursos se deben proteger?

- ¿De quién se debe proteger los recursos?
- ¿Cuáles y cómo son las amenazas que afectan a tales recursos?
- ¿Qué tan valioso es para la organización este recurso?
- ¿Qué medidas pueden ser implementadas para proteger el recurso o los recursos?
- ¿Cuál es el costo de aplicar alguna medida de control y/o prevención?
- ¿En cuanto tiempo puede ser implementada estas medidas?
- ¿Quién autoriza a los usuarios?

Al responder estas incógnitas o tal vez otras más, se deriva algunas de las siguientes políticas:

Política de privacidad: Define funciones de monitoreo, registro de actividades y acceso a recursos de la red.

- Política de acceso: Define derechos de acceso y privilegios para los usuarios con respecto a conexiones externas, comunicación de datos, conexión de dispositivos a la red, incorporación de nuevo software a la red, etc.

- Política de autenticación: Establece un servicio de confiabilidad mediante alguna política de contraseñas o de mecanismos de firmas digitales, estableciendo guías para la autenticación remota y el uso de dispositivos de autenticación.

- Política de administración de la red: Describe como se puede a través de algún tipo de tecnología manipular la administración interna y externa de la red por parte de los encargados o usuarios autorizados. De aquí surge la consideración de si se puede o de si se debe permitir una administración remota, para algún usuario tipo administrador u otro autorizado, el cual brinde soporte de red, control, monitoree o haga seguimiento a la red interna de la organización, de las estaciones de trabajo desde alguna terminal externa o incluso desde la casa de este superusuario.

3.3.3 Divulgación de la política de seguridad

Una vez generada la política de seguridad se debe abrir un espacio para la implementación de la política, esto con el fin de hacer participe a los diferentes usuarios de la red, de sus deberes y de sus obligaciones frente al buen uso de los recursos, para conseguir un mejor aprovechamiento de la misma y evitar desgastes en el consumo de recursos, aumentar o propiciar un mayor seguimiento, control y monitoreo personalizado de navegaciones por y para cada usuario, generando un tráfico innecesario y consumo de ancho de banda requerido para otras aplicaciones.

El divulgar la política de seguridad de la información brinda una participación al empleado sobre el uso de los activos informáticos de la compañía, creando una responsabilidad y conciencia en el manejo o manipulación de estos elementos, lo cual conlleve a un mejor desarrollo y cumplimiento de las actividades laborales diarias dentro de la compañía.

4. REALIZACIÓN DE ATAQUES INTERNOS A LA SEGURIDAD DE LA RED DE DATOS.

4.1 Selección de ataques de seguridad en la red.

Previamente a la realización del ataque a uno o varios equipos de la red de la organización se selecciona los objetivos generales a atacar, basándose en herramientas para la obtención y recolección de la información.

Para determinar algunas de las vulnerabilidades de la red de la organización se utilizo la modalidad de **Password Sniffig,** basándose en el uso de un sniffer, el cual es el encargado de capturar el tráfico de la red que se está enviando desde la máquina de la víctima, y obtener toda la información que viaje en claro por la red, como lo pueden ser los nombres de usuarios y sus contraseñas. Para esta prueba se utilizo el aplicativo wireshark, el cual es un software de versión libre y se utilizo para determinar si era posible capturar el login y password de algún usuario, para obtener acceso para la navegación de Internet, dentro de la LAN, igualmente determinar el usuario y la clave para acceder al Proxy/firewall a través de la consola WEB, por último detectar la clave y nombre de usuario de alguna cuenta de correo electrónico de la empresa configurada en los equipos en el aplicativo de correo, esta prueba se realizo desde el equipo del Ing. De Sistemas.

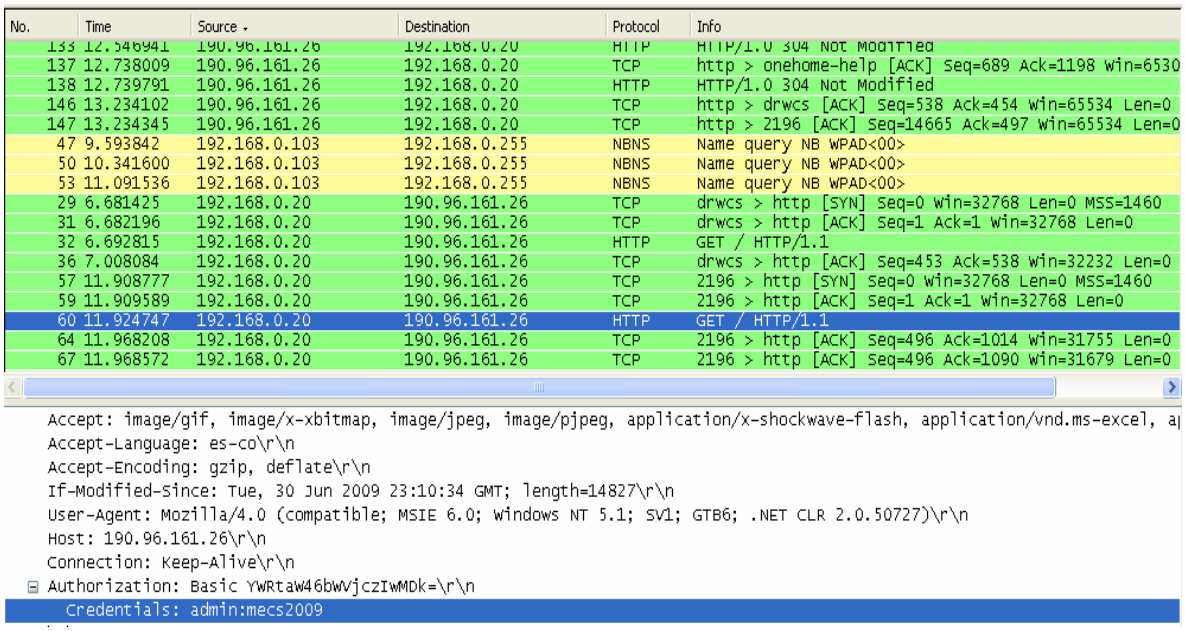
Una segunda prueba que se realizo fue el escaneo de red mediante un aplicativo de versión libre SoftPerfect Network Scanner, el cual permite observar todos los equipos pertenecientes a la red, con su dirección IP asignada al momento del escaneo y los recursos que tiene compartidos, con esta prueba lo que se pretende es determinar que equipos tienen carpetas o recursos compartidos que a la final no los este usando o no deban ser visto para toda la red y a que a su vez están generando trafico en la red al indicar que estas recursos están libres y a disposición para su uso.

4.2 Descripción de resultados de los ataques de red.

Luego de escoger un equipo de la red de la organización para hacer la prueba se instalo este aplicativo, el wireshark en el equipo del Ing. de sistemas, luego de dejarlo cargar y obtener tramas de red por algunas horas y al hacer la revisión de algunos segmentos de la captura, se detecto lo siguiente.

Al acceder desde este equipo a la consola WEB del Proxy/Firewall, se capturo login y password, tal como se ve en la siguiente imagen.

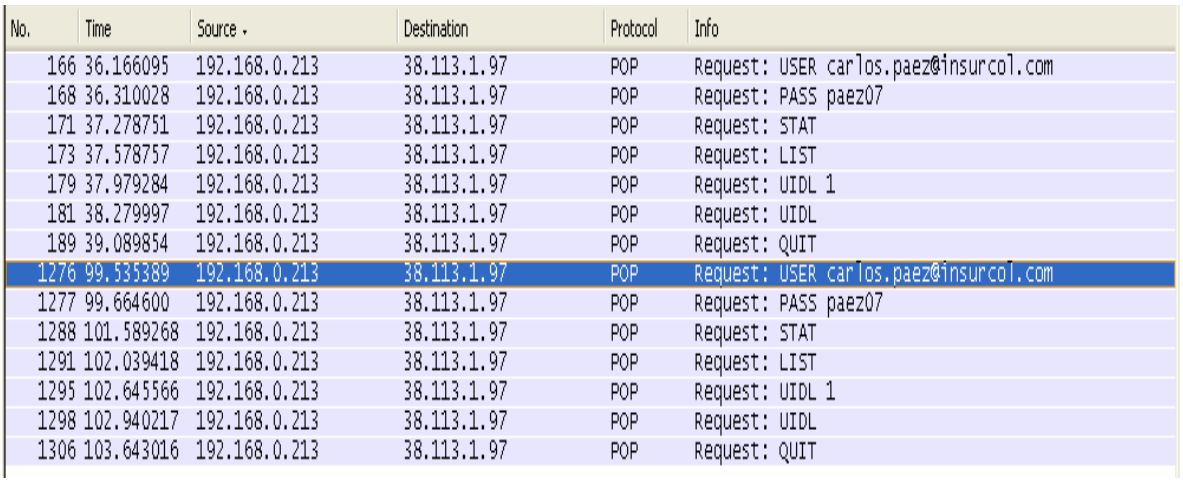
Figura 4. Captura con Wireshark



Fuente: Red LAN Insurcol LTDA

A su vez, se detecto el acceso de un usuario de la empresa a la consulta del correo personal, a través del protocolo POP3, por medio del Outlook Express, en la siguiente figura se encuentra una trama subrayada en color azul con el nombre de usuario y en la siguiente línea aparece la contraseña.

Figura 5. Captura con Wireshark – trafico POP



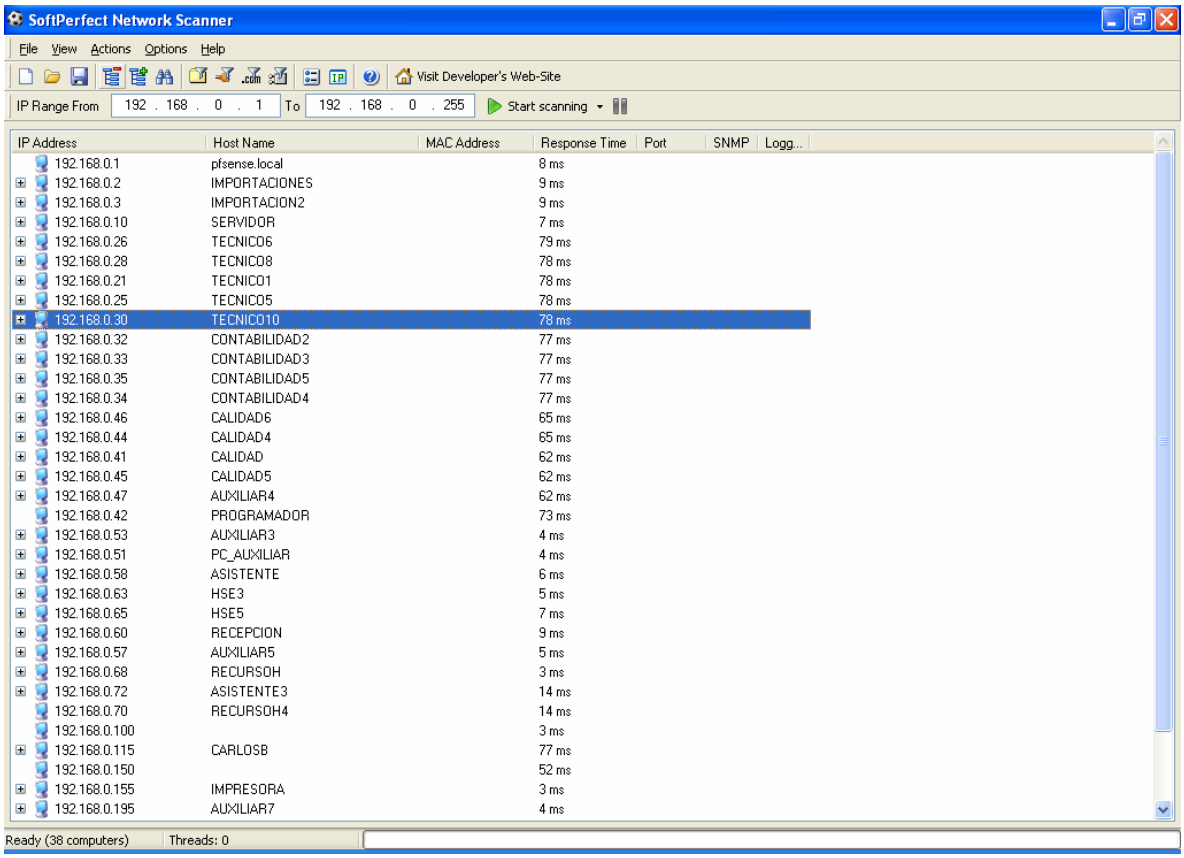
No.	Time	Source	Destination	Protocol	Info
166	36.166095	192.168.0.213	38.113.1.97	POP	Request: USER carlos.paez@insurcol.com
168	36.310028	192.168.0.213	38.113.1.97	POP	Request: PASS paez07
171	37.278751	192.168.0.213	38.113.1.97	POP	Request: STAT
173	37.578757	192.168.0.213	38.113.1.97	POP	Request: LIST
179	37.979284	192.168.0.213	38.113.1.97	POP	Request: UIDL 1
181	38.279997	192.168.0.213	38.113.1.97	POP	Request: UIDL
189	39.089854	192.168.0.213	38.113.1.97	POP	Request: QUIT
1276	99.535389	192.168.0.213	38.113.1.97	POP	Request: USER carlos.paez@insurcol.com
1277	99.664600	192.168.0.213	38.113.1.97	POP	Request: PASS paez07
1288	101.589268	192.168.0.213	38.113.1.97	POP	Request: STAT
1291	102.039418	192.168.0.213	38.113.1.97	POP	Request: LIST
1295	102.645566	192.168.0.213	38.113.1.97	POP	Request: UIDL 1
1298	102.940217	192.168.0.213	38.113.1.97	POP	Request: UIDL
1306	103.643016	192.168.0.213	38.113.1.97	POP	Request: QUIT

Fuente: Red LAN Insurcol LTDA

La segunda prueba se realizo mediante el uso de un aplicativo para el escaneo de red, el SoftPerfect Network Scanner, el cual es un software de versión libre.

En esta primera imagen se muestran los diferentes equipos que pertenecen a la red de la empresa (columna Host name) con su correspondiente dirección IP (columna IP Adress).

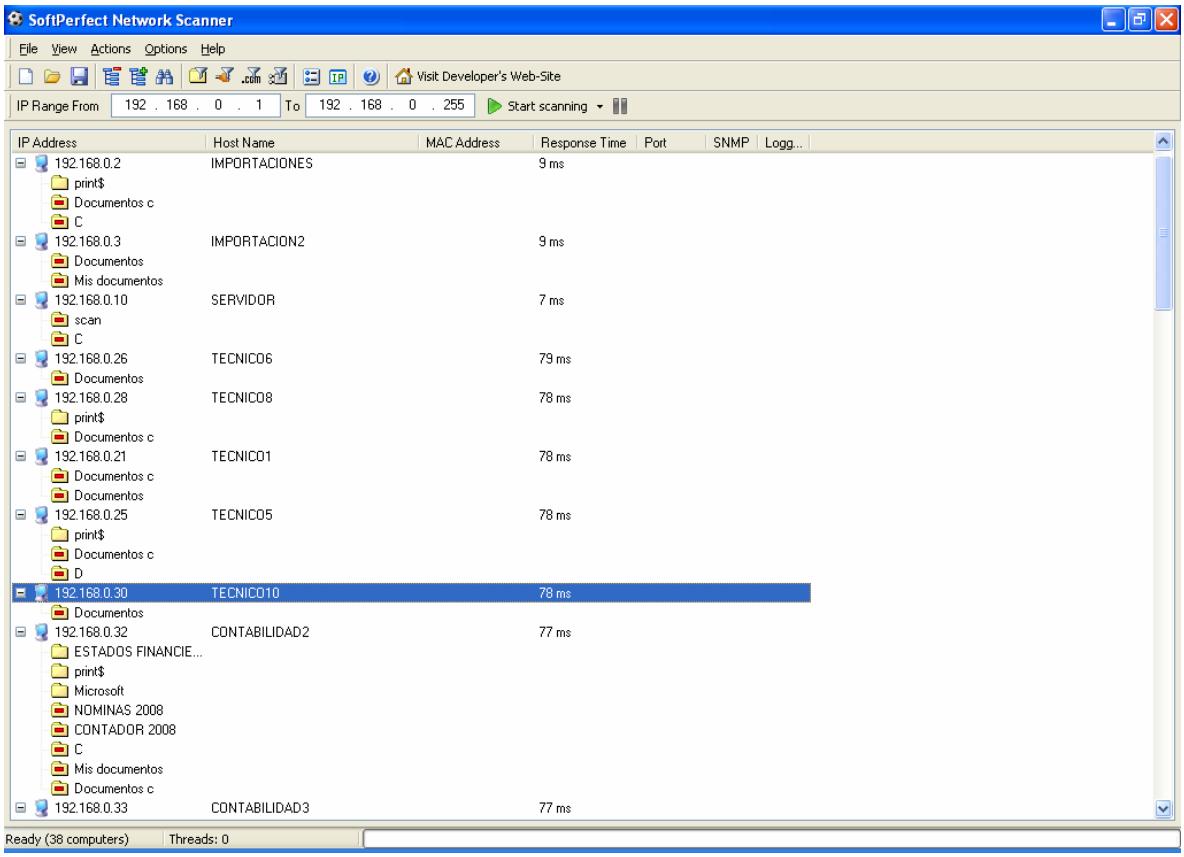
Figura 6. Network Scanner



Fuente: Red LAN Insurcol LTDA

En esta siguiente imagen se despliegan los recursos compartidos por parte de algunos de los equipos seleccionados.

Figura 7 Network Scanner – Recursos Compartidos



Fuente: Red LAN Insurcol LTDA

4.3. Descripción de métodos para contrarrestar las vulnerabilidades detectadas.

Firewall

En la actualidad la compañía cuenta con un Proxy/firewall, pero es usado básicamente para generar cuentas de usuario para el acceso a

Internet, con estas cuentas de usuario se podrá navegar en Internet y proceder a la descarga y envío de correos, negar el acceso a ciertas páginas web a través del uso de listas negras para filtrar por categorías y/o registrando una a una las páginas Web betadas.

El propósito principal de un firewall es controlar el acceso a, desde o hacia una red protegida. Implementa políticas de acceso a la red forzando que todas las conexiones pasen a través de el, en dónde pueden se examinadas, evaluadas y registradas[3].

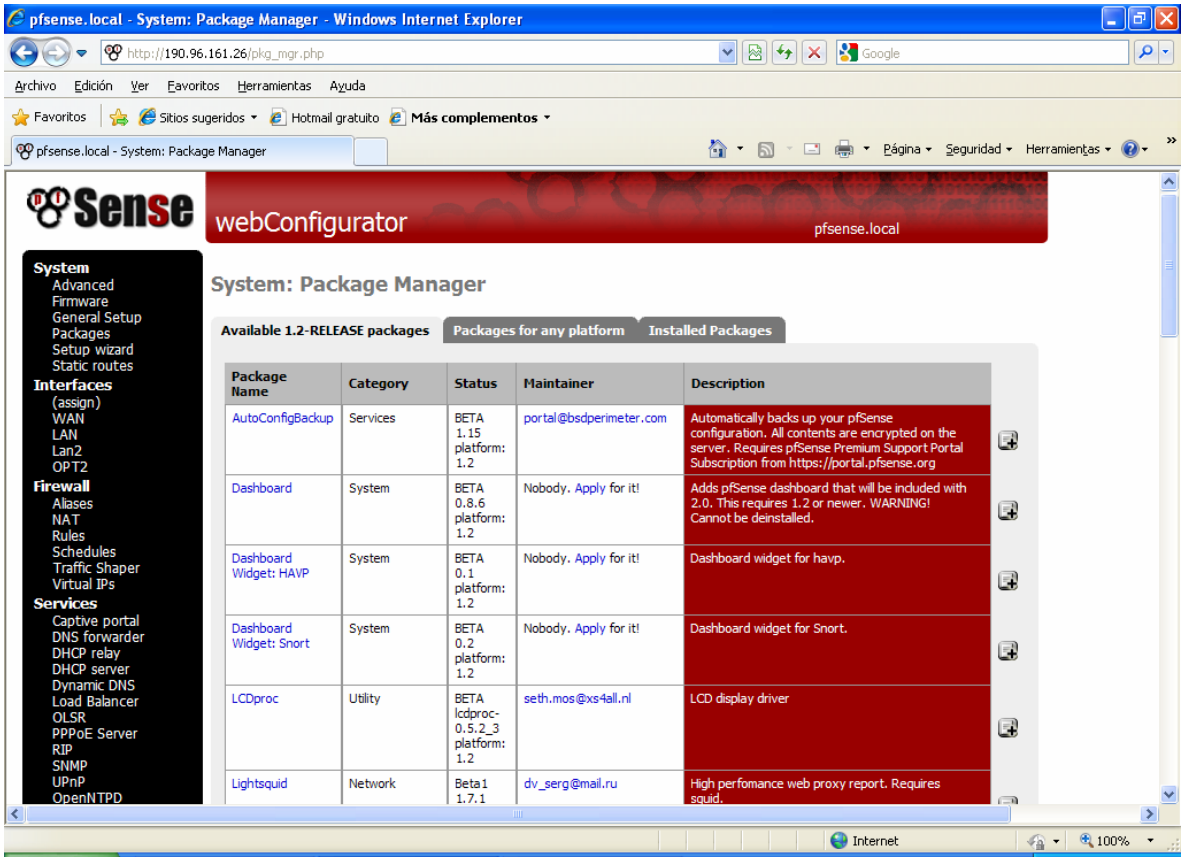
En la organización el firewall existente es el cortafuegos PFsense, el cual se encuentra instalado en un PC, marca HP, modelo Proliant ML110, es un equipo del año 2.005, lo que hace de este sistema operativo muy económico para la organización, en términos de licenciamiento, ya que es una versión FreeBSD, lo que significa que es un sistema operativo libre para computadoras basado en las CPU de arquitectura Intel, incluyendo procesadores 386, 486 (versiones SX y DX), y Pentium[4], este aplicativo no consume grandes cantidades de recurso de máquina, es decir, no requiere grandes cantidades de espacio en disco duro para la instalación o para el almacenamiento de los archivo de seguimiento (log) o de varios slot's de memoria, por el consumo de recursos que el Firewall para la carga del sistema operativo o para el análisis y seguimiento de la red, todo lo contrario,

[3] MEDINA VILLALOBOS, Jorge Alberto. Introducción a la seguridad informática, Bucaramanga, 2009, 88p.

[4] Disponible in Internet: http://es.wikipedia.org/wiki/FreeBSD

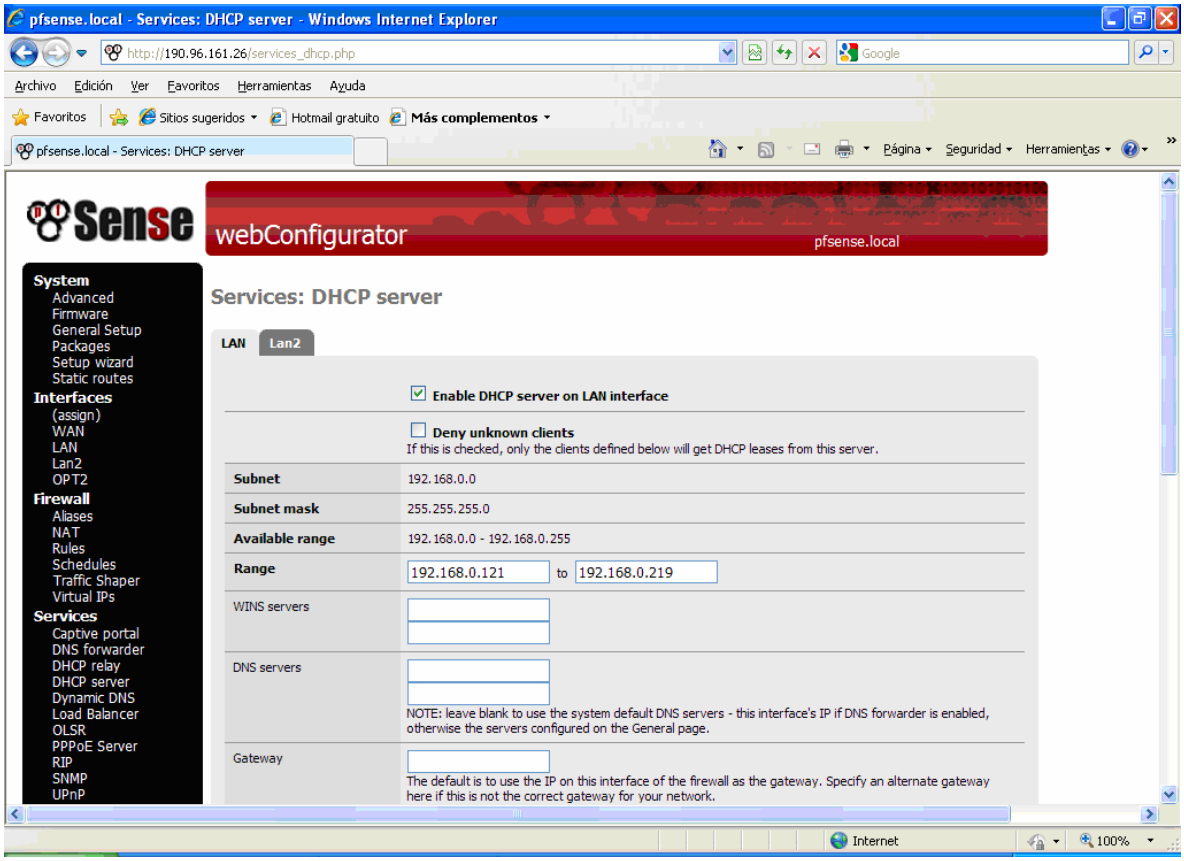
este sistema operativo es capaz de administrar y generar cuentas de usuario, comportarse como router y ser un servidor DHCP (Ver figura 9), además de al instalarse algunos plugin (ver figura 8) puede hacer seguimiento a la navegación de usuarios, mantener la tabla ARP para conocer equipos conectados a la red, donde muestra dirección IP con su dirección MAC, así como la interface por la cual esta conectada es decir WAN o LAN.

Figura 8. Package Manager – Pfsense



Fuente: Firewall Insurcol LTDA

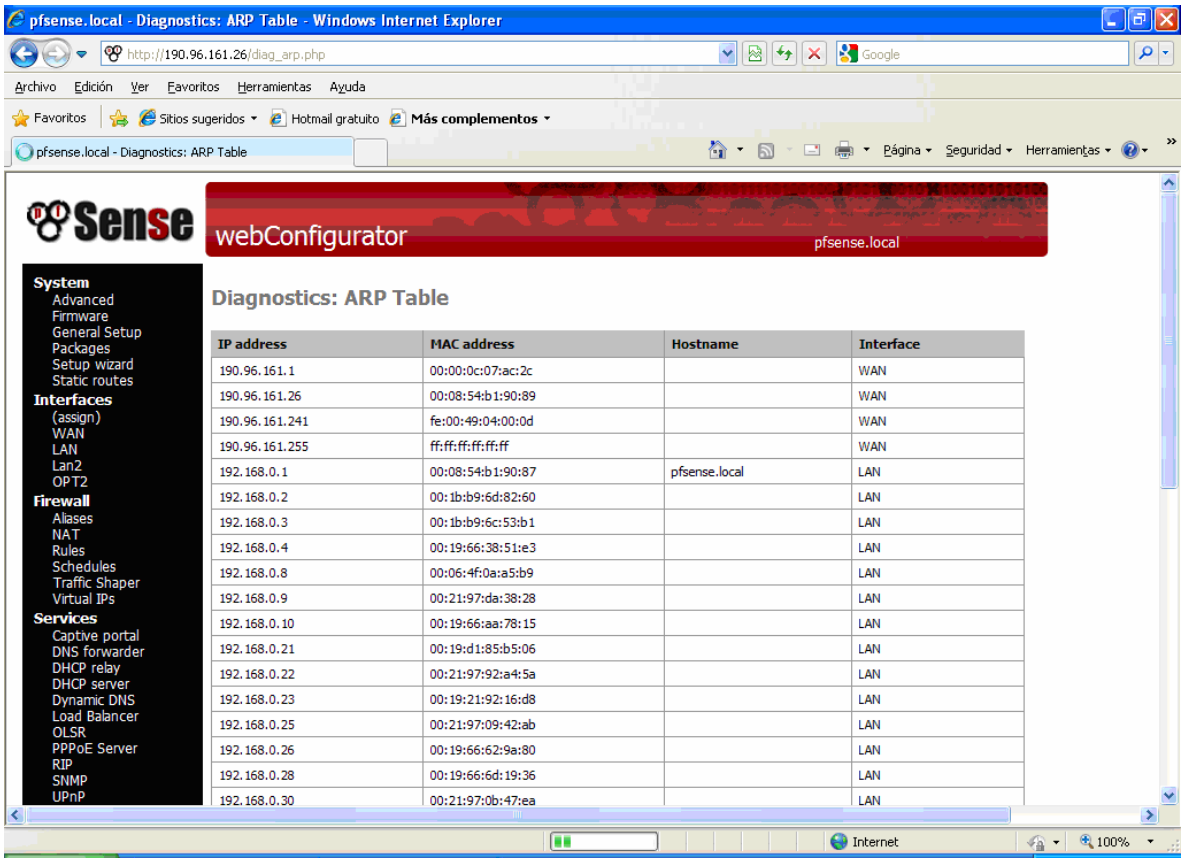
Figura 9. Servidor DHCP



Fuente: Firewall Insurcol LTDA

Al tener una tabla ARP **(Ver figura 10)** definida por el PFsense, obliga al administrador de red a conocer la cantidad de equipos instalados en su organización, tener un archivo con la tabla de direcciones IP asignadas a los equipos y así pueda determinar si tiene algún intruso conectado a la red, ya sea por conocimiento de las direcciones MAC o por las direcciones IP asignadas.

Figura 10. TABLA ARP



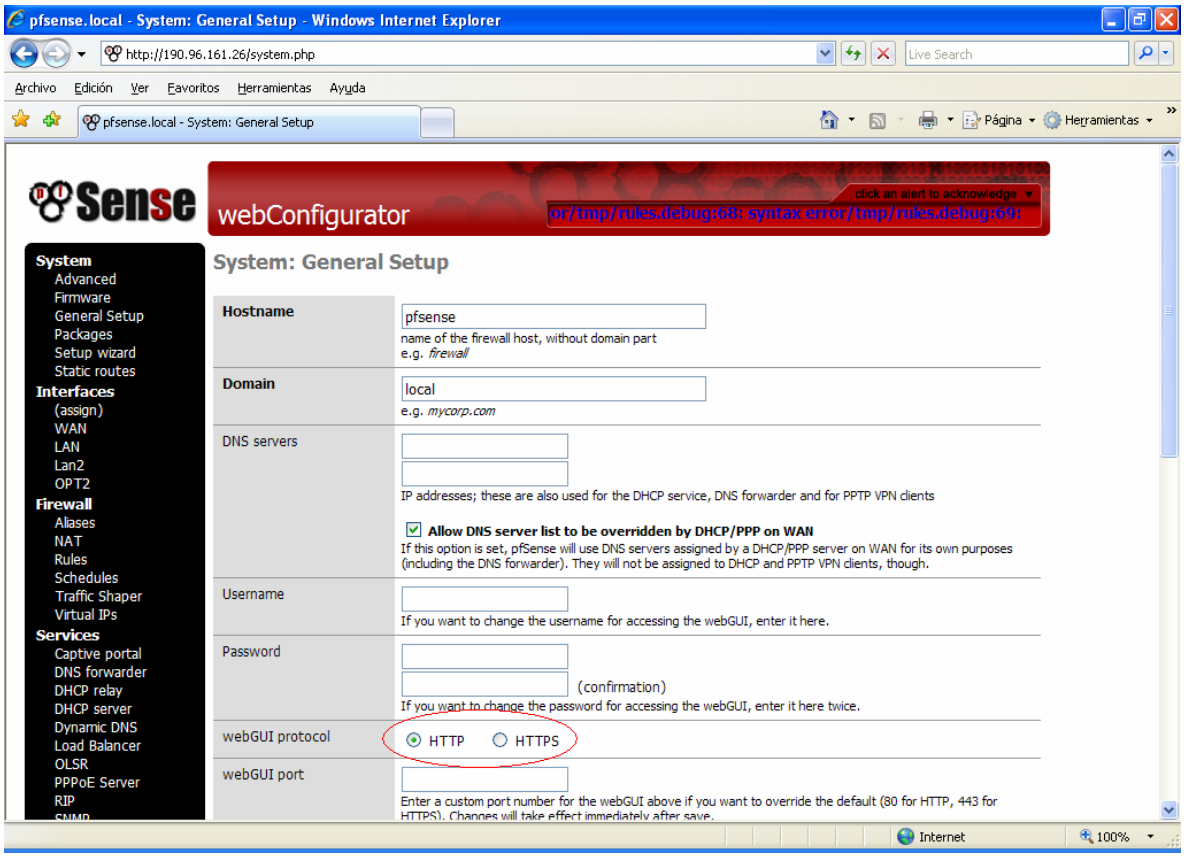
Fuente: Firewall Insurcol LTDA

4.4 Indicación de métodos de seguridad aplicables al interior de la red LAN.

Partiendo del Firewall actual de la compañía, el cual funciona bajo el sistema operativo Pfsense, este brinda la posibilidad de pasar de un loggeo vía HTTP a HTTPS, de acuerdo con la figura de la parte inferior, a su vez se deben revisar las reglas establecidas en este firewall y activar la posibilidad de que una dirección IP pueda tener acceso vía

consola WEB a través del puerto 443 concerniente al HTTPS, y así pueda acceder el usuario administrador y seguir haciendo los cambios de configuración ha futuro que sean pertinentes.

Figura 11. Webconfigurator PFsense



Fuente: Firewall Insurcol LTDA

Un segundo ítem es documentar, mejorar o robustecer el manejo del PFsense para obtener un mayor grado de seguridad para el interior de la organización, ya que un Firewall tiene varias aplicaciones, no solo dar salida a Internet, para efectos de la empresa también podría:

- Bloquear de tráfico no permitido
- Ocultar vulnerabilidades de los sistemas.
- Almacenar o registrar una bitácora (log) del tráfico entrante y saliente.
- Ocultar información como los nombres de los sistemas, la topología de red, los dispositivos de red y la identificación de los usuarios.
- Brindar autenticación más segura.
- Hacer seguimiento sobre la navegación de los usuarios.

4.5 Política de seguridad

La compañía en la actualidad no cuenta con una política de seguridad documentada, sin embargo, básicamente con lo que si cuenta es con una serie de reglas establecidas aplicables a una política de seguridad, al interior de la organización se han dictaminado ciertas premisas sobre uso y manipulación de los equipos y recursos de la empresa, además ha sido comentada al personal a través de una charla en general.

Una política de seguridad es un compendio de normas, procedimientos e instrucciones que describen la forma adecuada para usar los recursos de un sistema de computo, las responsabilidades y el que hacer en caso de un incidente de seguridad.[5]

[5] BARON GONZALEZ, Henry Javier. Política de seguridad informática y aplicabilidad en la red de datos de la empresa CELTEL LTDA. Bucaramanga, 2007, 79p.

Para lo cual se debe establecer dos tipos de políticas. Una primera política de acceso a la red, en la cual se definan los servicios permitidos, los servicios a negarse, el uso o manejo que se le debe dar a los servicios permitidos y las condiciones o excepciones que pueda tener esta política.

Una segunda política para el Firewall, la cual describa la forma en que actuara el cortafuego ante las restricciones de acceso y el filtrado de servicios que se definió en la política de acceso a la red.

La empresa en sus diferentes áreas de trabajo no tiene una diferencia entre los diferentes usuarios que acceden a la red pertenecientes a las áreas administrativas, ya que todos manejan una aplicación principal para el desarrollo de sus labores Microsoft office y el correo, luego la restricción o acceso de un usuario es aplicable para todos los demás, simplemente se han creado unas direcciones libres para algunos usuarios:

- Dos direcciones libres para alta dirección, debido a que ellos generan pagos en línea y consulta a ciertas páginas de soporte y subasta pública en línea, donde entra la posibilidad de que el firewall restrinja o bloquee algún acceso algún sitio web por los puertos cerrados.
- Dos direcciones libres más para el departamento técnico, básicamente por el acceso a páginas de subasta pública, videoconferencias, Chat de soporte técnico en línea con ciertas

firmas a la cual la empresa representa, esto debido a que el firewall ha bloqueado en ciertas ocasiones algunos sitios web.

- Los demás usuarios cuentan para el acceso a Internet con un nombre de usuario y contraseña y así puedan acceder a este servicio, además de descargar y enviar correos.

4.5.1 Política de servicio de acceso a la red

Esta política de servicio de acceso se debería enfocar en asuntos de uso específico de Internet y otras redes externas. Esta política debe ser realista, lógica y previamente probada antes de ser puesta en marcha, es decir, debe ser una política que permita reducir los riesgos informáticos de la organización, pero que le permita a los usuarios de la misma el acceso a los recursos de la red, para ello se debe tener en cuenta dos puntos:

Aspecto tecnológico.

Este punto se refiere al aporte económico brindado por la empresa para mejorar la seguridad de la información en términos de adquisición de equipos (servidores, firewall o router), adecuaciones de la planta física (centro de computo, extintores, zonas de acceso restringido), sistemas operativos, manejo correcto de la información (copias de seguridad). En el momento la empresa cuenta con:

Un Firewall, un Servidor marca HP, modelo Proliant ML110 de segunda generación, el cual tiene conectado el MODEM del ISP y este servidor es el encargado de limitar o permitir el acceso a Internet.

Un router inalámbrico, marca Linksys, el cual es controlado por el firewall, para permitir la conexión de los computadores portátiles de algunos usuarios que de manera no regular llegan a la empresa y tienen este tipo de equipos.

Aspecto Humano.

Capacitación o divulgación de la información al personal sobre la política de seguridad, indicando responsabilidades, derechos, deberes, privilegios y niveles de riesgo entre los usuarios, reporte de incidentes o detecciones de fallas, entre otros.

Bajo este aspecto mas del 70% del personal es profesional o tecnólogo, con conocimientos básicos en herramientas informáticas o las utilizadas en la empresa, al cual ya se les ha informado sobre limitantes en la navegación, prohibiciones a sitios y los correctivos que se generan una vez son descubiertos intentando a sitios no autorizados

4.5.2 Política en el firewall

Este tipo de política es propia para cada firewall, pero se debe basar en la creación de reglas para el acceso o uso de servicios. Existen dos implementaciones básicas en el diseño de las políticas de acceso:

- Permitir cualquier servicio a menos que esté expresamente negado.
- Negar cualquier servicio a menos que esté expresamente permitido.

La primera implementación es la menos aconsejable, ofrece una mayor cantidad de opciones para esquivar las restricciones del firewall, donde solo se restringen servicios a medida que se detecten las fallas o hasta que estas se reflejen.

La segunda es mucho más fuerte y seguro pero, a su vez, es más difícil de implementar y puede crear mayor impacto en los usuarios, debido a que todo los servicios están cerrados y se van otorgando a medida que se vayan requiriendo.

Para el caso de la organización se debe tener presente que una política de Firewall no es equivalente a la política de seguridad de la información, aun cuando ambas buscan salva guardar la integridad de la empresa, los objetivos de cada una apunta a horizontes diferentes.

Antes de elaborarse o crearse una política de cortafuego o de Firewall, debe existir algún método de análisis de riesgo sobre las aplicaciones necesarias o utilizadas en las labores diarias que conduzcan al logro de la misión de la empresa. Los resultados de este análisis incluirán una lista de las aplicaciones y cómo esas aplicaciones se afianzarán. El proceso para crear esta lista no se relaciona en esta monografía, es un ítem que se debe abordar al interior de la organización, sin embargo, requerirá el conocimiento de las vulnerabilidades asociada a cada aplicación y el costo – beneficio relacionado a cada una de estas. Este análisis de riesgo debe sustentarse en las amenazas, vulnerabilidades, y contramedidas en el lugar para mitigar las vulnerabilidades, y el impacto en caso de fallas o ataques. La meta es entender y evaluarlos para establecer una política del cortafuego

Los pasos involucrados para crear una política del cortafuego son como sigue[6]:

- La identificación de aplicaciones de red necesarias a proteger.
- La identificación de vulnerabilidades asociadas a las aplicaciones,
- El análisis del costo - beneficio de los métodos de aseguramiento de las aplicaciones,
- La creación de una matriz de tráfico de aplicaciones que muestra el método de protección.

[6] WACK, John. Guidelines on firewalls and firewall policy, Gaithersburg, 2002. 74 p.

- La creación de regla del cortafuego, basado en las aplicaciones de la matriz de tráfico.

El termino aplicaciones no necesariamente hace referencia a un software en especial utilizado al interior de la organización, sino a puertos de conexión o por el cual se hace el intercambio de información a través de la red interna o la salidas a Internet, como también los servicios de comunicación existentes o cargados por defecto en las diferentes estaciones de trabajo como el telnet. En el Firewall instalado actualmente se cumple con los siguientes puntos:

A) Bloquear de tráfico no permitido

En este ítem el sistema operativo PFsense del Firewall de la compañía cuenta con una sección de reglas el cual permite cerrar y abrir puertos como lo son:

- El POP (Protocolo de la oficina de correo) y el SMTP (Protocolo Simple de Transferencia de Correo), los cuales están abiertos debido a que las diferentes estaciones de trabajo o los clientes de la LAN usan aplicativos de correo como lo es el microsoft Outlook o el Outlook Express para obtener los mensajes de correo electrónico almacenados en el servidor.
- Puerto 80 para http.
- Puerto 443 para HTTPS - HTTPS/SSL usado para la transferencia segura de páginas web.

- Puerto 22 SSH - Secure Shell, protocolo informático que sirve para acceder a máquinas remotas.
- Puerto 21 FTP - Protocolo de Transferencia de Ficheros.
- Los otros no se han habilitado por seguridad para los equipos.

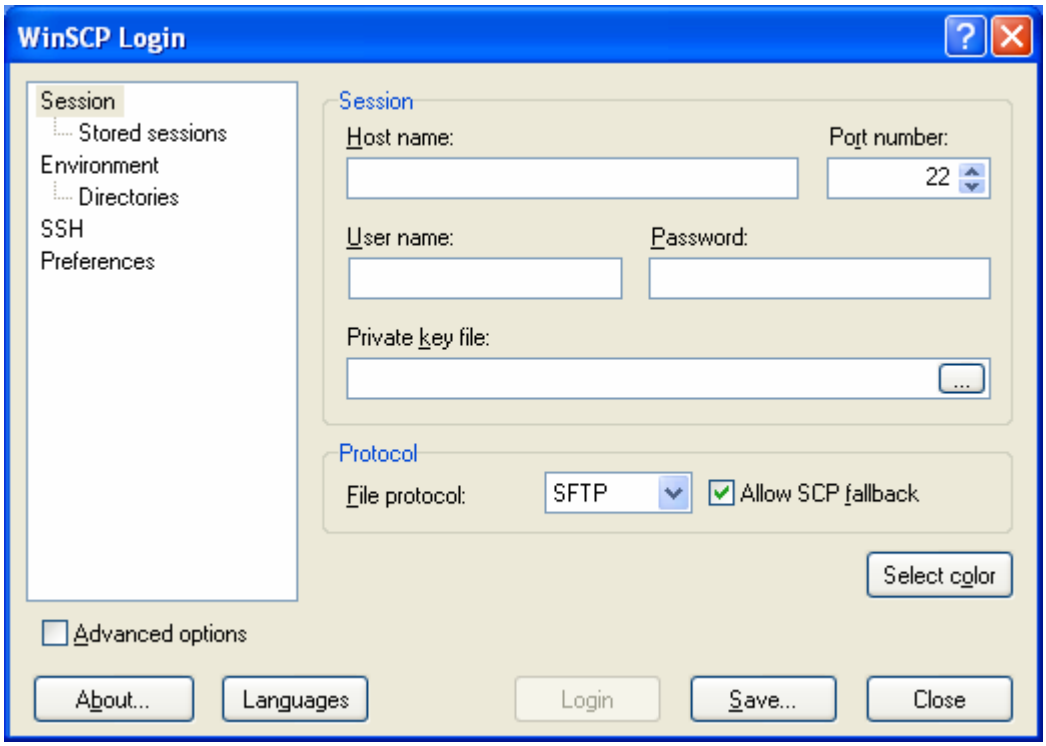
Figura 12. Aperturas de puertos (PFSense)

Fuente: Firewall Insurcol Ltda

B) Hacer seguimiento sobre la navegación de los usuarios.

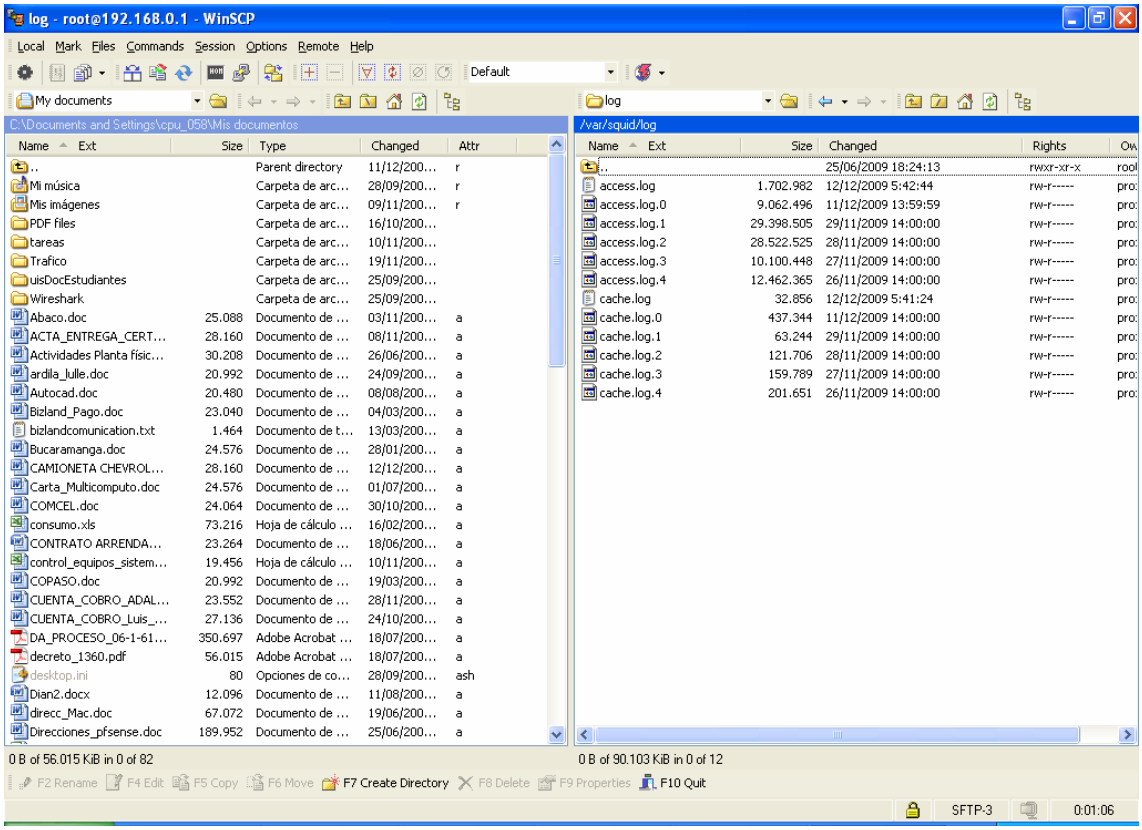
En este punto se utilizo la combinación de dos aplicativos el WinSCP, el cual permite al administrador de red conectarse aun equipo de la red local o de manera remota, para este caso el acceso es hacia el firewall, conociendo de antemano su IP, nombre de usuario y contraseña, donde a través de una ventana tipo Windows puede acceder al árbol de directorios del equipo y descargar el log diario de navegación de las estaciones, a un equipo Windows, con este registro se puede monitorear la navegación por usuario, sin embargo este archivo debe ser activado en el firewall para que se genere.

Figura 13. WinSCP Login



Fuente: Aplicativo WinSCP

Figura 14. WinSCP Conexión



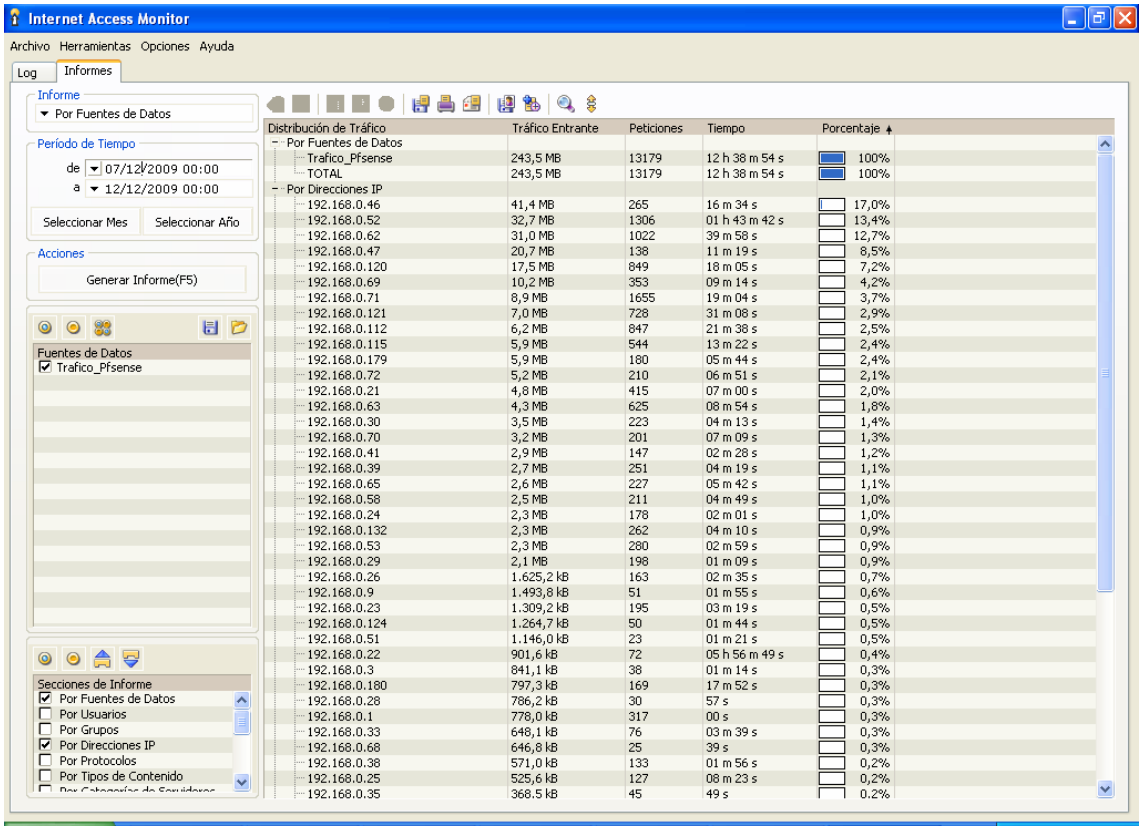
Fuente: Aplicativo WinSCP

Una vez descargado en una máquina Windows, para el caso de esta monografía el archivo se abre con un software llamado i am - Internet acces monitor, este es un programa para controlar la eficacia de la utilización del ancho de banda de Internet por los empleados de una compañía, este aplicativo puede determinar con facilidad qué empleados utilizan más el ancho de banda, cuándo y qué exactamente descargan, cuánto tiempo pasan en línea y qué volumen de transferencia de datos generan por su actividad en línea[7]. Se utilizo la

[7] Disponible en Internet: http://www.redline-software.com/spa/products/iam/

versión Beta para efecto de las pruebas, este aplicativo puede filtrar por usuario, sitios visitados y direcciones IP, para el caso de la organización se ha seleccionado las direcciones IP's, debido a que se tiene registrada la dirección IP para cada estación, el informe refleja las diferentes páginas WEB que haya accesado un usuario determinado dependiendo de la dirección IP escogida. En este punto es donde la organización centra su atención en la política de seguridad, para evitar que los usuarios pierdan horas hombre de trabajo en accesos o navegaciones a sitios Web innecesarias o no autorizados.

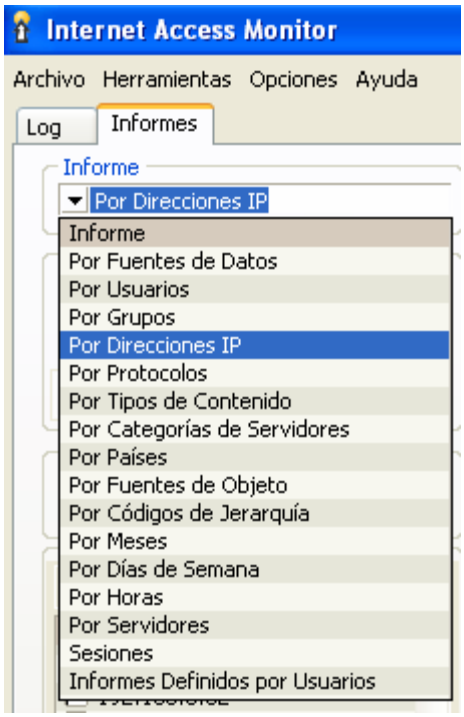
Figura 15. Trafico Internet Acces Monitor



Fuente: Aplicativo Internet Acces Monitor

Con este software, el administrador de red como ya conoce previamente la dirección IP, asignada a cada equipo, puede generar informes, por cada estación u otros ítems que este aplicativo también le permite.

Figura 16. Filtro de Informes



Fuente: Aplicativo Internet Acces Monitor

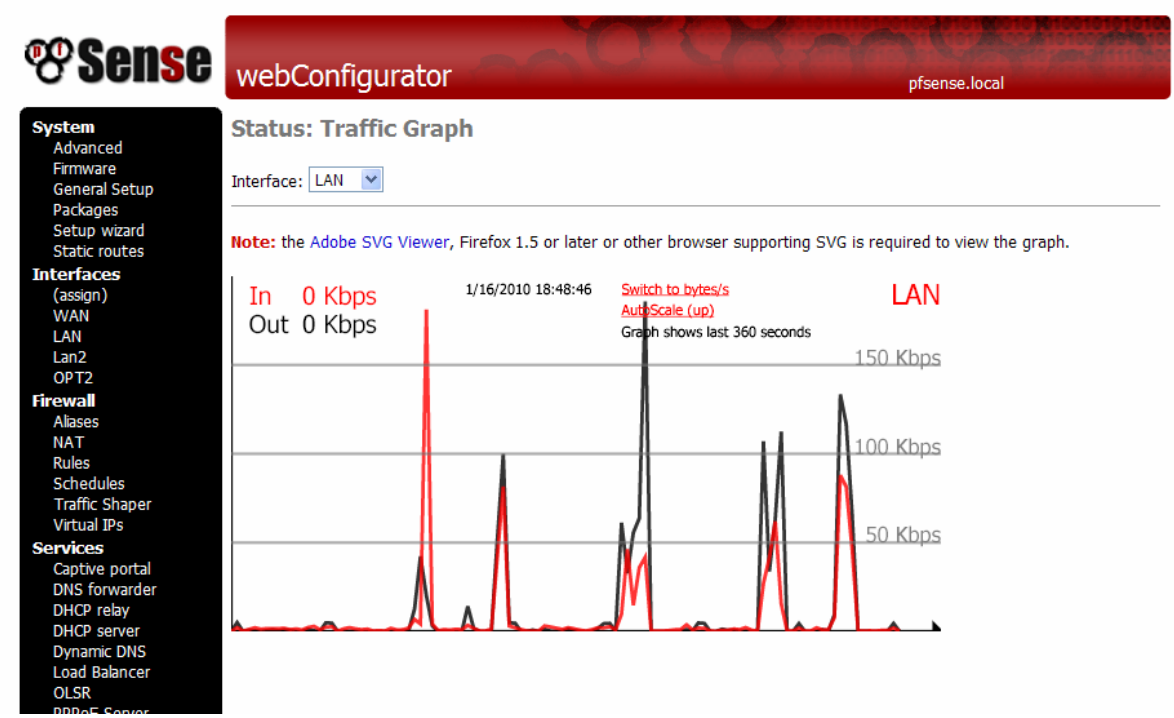
Así, el administrador de red conoce a que páginas entro cierta estación en un día determinado y realizar seguimiento diario de ser necesario al usuario o usuarios, por este hecho, para así determinar su bloqueo o no a través del firewall a estas páginas visitadas.

C) Almacenar o registrar una bitácora (log) del tráfico entrante y saliente.

En este punto el PFsense permite realizar dos actividades:

Generar graficas de tráfico en la red LAN, mostrando picos de velocidad de entrada y salida, grafica que se muestra automáticamente una vez se entra en el link de Graph Traffic y la muestra mientras este la pantalla activa.

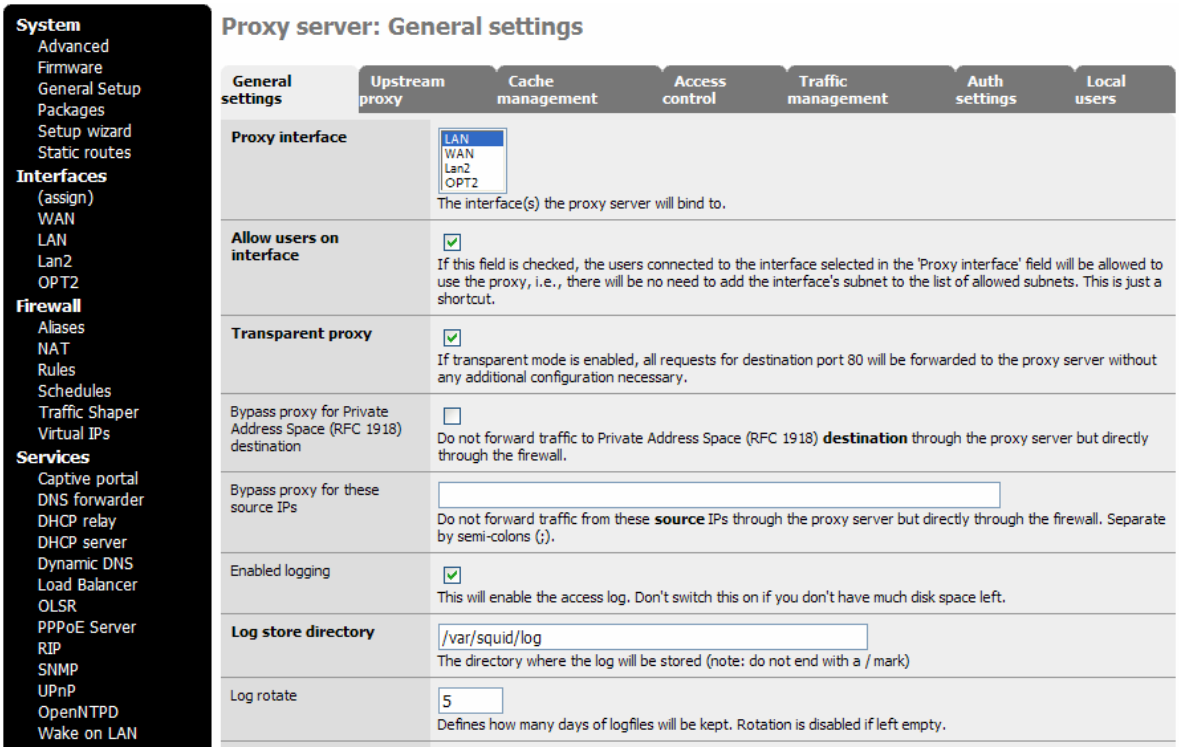
Figura 17. Tráfico LAN PFSense



Fuente: Firewall Insurcol Ltda

La segunda opción, es activar en la zona de Proxy Server el enabled logging, el cual va a permitir generar los log de navegación de usuarios y así a través de algún aplicativo como el Internet access monitor mencionado anteriormente, el administrador pueda imprimir la estadística de navegación, acceso, peticiones y consumo de ancho de banda en porcentajes por equipos, grupos, usuarios, entre otros.

Figura 18. Proxy Server – Pfsense



Fuente: Firewall Insurcol Ltda

Luego de activar esta casilla, se comienzan a generar los log de acceso y navegación dentro de la LAN, con estos archivos se debe buscar una interfaz capaz de interpretar este tipo de archivo y los pueda cargar

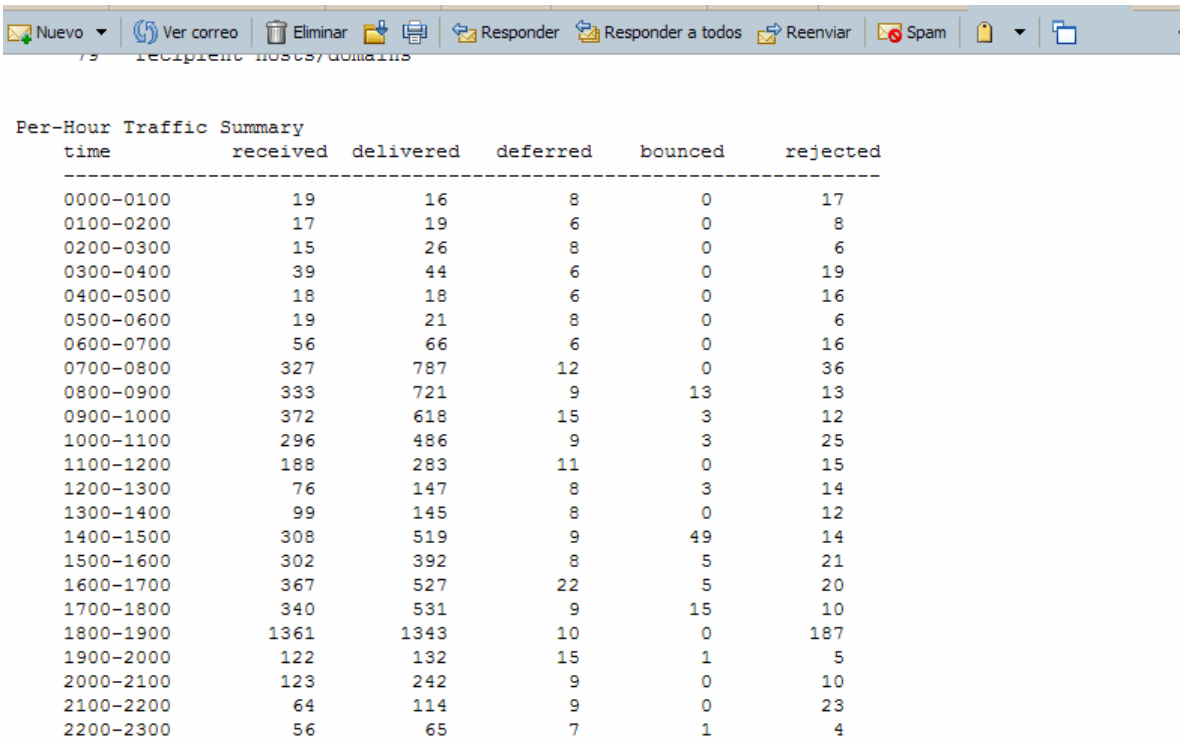
para su revisión y seguimiento, un ejemplo de estos es el mostrado en la figura siguiente:

Figura 19. Reporte de mensajes de correo

Fuente: Firewall Insurcol Ltda

Este tipo de informe generado, se muestra en varios segmentos, comenzando con un registro de tráfico por hora, donde se expone en una hora específica, la cantidad de correos enviados, recibidos, rechazados, luego muestra los dominios a los cuales se envío correos o en los que se recibieron, siguiendo con un top de las cincuenta (50) cuentas de correo donde se muestra en pantalla la cantidad de correos enviados y recibidos por cada una de estas cuentas de correo y el tamaño total en KB de los mensajes enviados por estas.

Figura 20. Reporte de tráfico por Hora



Per-Hour Traffic Summary

time	received	delivered	deferred	bounced	rejected
0000-0100	19	16	8	0	17
0100-0200	17	19	6	0	8
0200-0300	15	26	8	0	6
0300-0400	39	44	6	0	19
0400-0500	18	18	6	0	16
0500-0600	19	21	8	0	6
0600-0700	56	66	6	0	16
0700-0800	327	787	12	0	36
0800-0900	333	721	9	13	13
0900-1000	372	618	15	3	12
1000-1100	296	486	9	3	25
1100-1200	188	283	11	0	15
1200-1300	76	147	8	3	14
1300-1400	99	145	8	0	12
1400-1500	308	519	9	49	14
1500-1600	302	392	8	5	21
1600-1700	367	527	22	5	20
1700-1800	340	531	9	15	10
1800-1900	1361	1343	10	0	187
1900-2000	122	132	15	1	5
2000-2100	123	242	9	0	10
2100-2200	64	114	9	0	23
2200-2300	56	65	7	1	4

Fuente: Firewall Insurcol Ltda.

D) Brindar autenticación más segura.

Actualmente la compañía con la instalación del firewall limita la conexión de Internet a través del PFsense, lo cual restringe sitios a través de sus listas negras.

Al interior de la organización cada usuario para navegar en la Web y recibir o enviar correos a través del Microsoft Outlook o el Outlook Express, debe cargar el navegador de Internet donde al inicio de cada jornada laboral o transcurrido cierta cantidad de tiempo donde el firewall

detecte o determina inactividad por navegación o no uso de los aplicativos de correo, el Firewall solicita un nombre de usuario y contraseña, para tener acceso a estos servicios.

Para el acceso al firewall, se debe habilitar el loggeo con el protocolo HTTPS para evitar la captura del login y pasword, así como definir un puerto en especial para que pueda ser este accesado vía consola WEB y minimizar aun mas intentos de conexión por cualquier usuario, ya que así quien intente conectarse deberá conocer la dirección IP, el puerto, login y password, incluso si es de manera interna se puede asignar solo a una IP en especial para que pueda ser vista por esta..

CONCLUSIONES

- La compañía aun cuando no tiene implementada una política de seguridad informática dentro de su esquema organizacional, se ha ido acercando a esta poco a poco, debido a los riesgos informáticos que se han venido sucediendo con base a experiencias de fallas presentadas en otros sectores o competidores.

- La organización cuenta con un Proxy/firewall, el cual presenta una lista de reglas o restricciones para la navegación y establecimiento de límites de accesos a través de claves para la conexión a Internet, recepción y envío de correos.

- La empresa cuenta con una propuesta integral respecto de la seguridad de los equipos de la red de datos con la adquisición del Kaspersky Internet Security como apoyo a la protección de datos en el equipo.

- La compañía con la configuración y mantenimiento al Firewall PFSense mitiga el ataque de entes externos, debido al cierre de puertos, el tipo de sistema operativo y seguimiento al tráfico de red.

RECOMENDACIONES

- Crear una conciencia en los usuarios de la organización, respecto de la realización de copias de seguridad, actualización de antivirus, escaneo del equipo con cierta periodicidad.

- Determinar una metodología para el establecimiento de la seguridad de la red de datos.

- Generar una política de seguridad acorde con los objetivos de la empresa, donde se empalme el costo – beneficio, donde se brinde una buena seguridad para el interior y exterior de la red en términos de navegación y uso o manipulación de los datos y equipos sin que represente restricciones o condiciones caóticas en la operatividad de los mismos.

BIBLIOGRAFÍA

BARON GONZALEZ, Henry Javier. Política de seguridad informática y aplicabilidad en la red de datos de la empresa CELTEL LTDA. Bucaramanga, 2007, 79p.

MEDINA VILLALOBOS, Jorge Alberto. Introducción a la seguridad informática, Bucaramanga, 2009, 88p

GARCIA ALFARO, JOAQUÍN. Aspectos avanzados de seguridad en redes, Barcelona, 2004. 292p

WACK, John. Guidelines on firewalls and firewall policy, Gaithersburg, 2002. 74 p.

Documentación disponible en Internet:

http://es.wikipedia.org/wiki/FreeBSD. FreBSD

http://www.wisedatasecurity.com/definiciones-seguridad.html. ¿Que es seguridad informatica?

http://www.faqs.org/rfcs/rfc2196.html. RFC2196 - Site Security Handbook

http://www.redline-software.com/spa/products/iam/. Internet Access Monitor

http://www.monografias.com/trabajos12/fichagr/fichagr.shtml#SEGUR. Auditoría de Sistema y políticas de Seguridad Informática

http://www.indigo.com.mx/temas-de-interes-informatico/12-conceptos-basicos-de-seguridad-informatica.html#ventajas. Conceptos básicos de seguridad informatica