CAPITULO I

ESTUDIO DE LA INFRAESTRUCTURA ACTUAL

INTRODUCCION

Ecuasanitas S. A es una empresa dedicada a dar servicio de Medicina prepagada 28 años de experiencia, atiende a sus clientes en clínicas, centros médicos y 9 ciudades del Ecuador, que forman parte de la red. El compromiso de la empresa es de otorgar un servicio de calidad, con el mejor trato que merecen sus clientes. Por lo que el acceso oportuno de los usuarios a la información del sistema de la empresa se obtiene las grandes ventajas obtenidas por los clientes satisfechos.

Ecuasanitas S.A cuenta con más de 200 equipos en su red local en la ciudad de Quito, divididos en 4 agencias, por lo que una de las principales preocupaciones en el Área de Sistemas es la seguridad que fluyen en la red. Debido a esto este proyecto esta dedicado a buscar las mejores soluciones para asegurar de la mejor forma la red de la empresa.

La Misión de Ecuasanitas es otorgar y garantizar atención médica de calidad a nuestros clientes.
La Visión de Ecuasanitas es mantener el liderazgo de la atención médica a través del compromiso de su Gente y la excelencia en el servicio.

1.1. PLATAFORMAS, HARDWARE Y SOFTWARE DE SERVICIOS

Los servidores actuales son una conformación mixta de plataformas de hardware y software. Entre los más utilizados se tiene Unix, Windows, Linux este tipo de arquitectura sirve para la finalidad que se desea obtener en este estudio.

1.1.1. AMBIENTES UNIX/LINUX/WINDOWS.

1.1.1.1 Ambientes Unix.

Los programas del sistema Unix están funcionalmente clasificados en el núcleo que es el cual planifica tareas y gestiona el mantenimiento de datos, el shell es el que relaciona e interpreta las órdenes ingresadas por el usuario.

Entre los servicios principales de Unix tenemos:

- Servicios de correo electrónico.
- Servicios generales de red.
- Servicios de representación y administración del sistema.

A continuación se recalcan las principales ventajas del sistema Unix:

El sistema está escrito en un lenguaje de alto nivel, haciéndolo fácil de leer, comprender, cambiar, y mover a otras máquinas.

- Posee una simple interfase de usuario con el poder de dar los servicios que los usuarios quieren.
- Usa un sistema de archivos jerárquico que permite un mantenimiento fácil y una implementación eficiente.
- Usa un formato consistente para los archivos, el flujo de bytes, haciendo a los programas de aplicación más fáciles de escribir.
- Provee una simple y consistente interfase a los dispositivos periféricos.
- Es un sistema multiusuario y multitarea; cada usuario puede ejecutar varios procesos simultáneamente.
- Oculta la arquitectura de la máquina al usuario, haciendo fácil de escribir programas que se ejecutan en diferentes implementaciones hardware.

Las principales desventajas son:

- Comandos poco claros y con demasiadas opciones.
- Escasa protección entre usuarios.
- Sistema de archivo lento.
- El costo de las licencias y soporte técnico para la instalación y configuración del sistema operativo en servidores es alto.

1.1.1.2 Ambientes Linux.

Linux es un sistema operativo, compatible con el Unix, posee características muy significativas que lo diferencian del resto de sistemas operativos existentes en el

mercado, una de ellas es que es un software libre, lo que significa que no se tiene que pagar ningún tipo de licencia a ninguna casa desarrolladora por su utilización, otra de las diferencias es que viene acompañado del código fuente.

Linux es un conjunto de instrucciones que permite hacer cualquier tipo de tarea en el ordenador.

Entre algunas características de Linux se tiene:

- Es potente, seguro y estable, puede realizar infinidad de programas para cualquier tarea.
- Tiene la función de conectar varios usuarios a la misma máquina al mismo tiempo. Otra finalidad es que varios procesos pueden usar la misma zona de memoria para ejecutarse, es decir que si alguno intenta escribir en esa memoria, la página se escribe en otro lugar. Esto nos brinda dos beneficios como son: Aumento de velocidad y reducción de uso de memoria. [1]

1.1.1.3 Ambientes Windows

Las estaciones de trabajo tienen instalados indistintamente los sistemas operativos Windows 95/98/2000/XP, las características de hardware van desde una Pentium I hasta las Pentium IV, con procesadores desde 166MHZ hasta 3.0 GHZ, discos duros desde 3.0GB hasta 80 GB, y memoria Ram desde 16MB hasta 1GB, todos los usuarios tienen conexión al sistema principal de la empresa que se encuentra en el servidor de producción, los usuarios de Windows se conectan a este servidor por medio de 2 emuladores los cuales son:

EMULADOR	FABRICANTE	COMPATIBILIDAD	CONEXIÓN	SERVICIO DE IMPRESIÓN
Tiny Plus Versión 4.0	Century Software	Windows 95 / 98	Telnet	Century Internet
Winsock, Windows, TCP/IP	Network Instruments	Windows 2000 / XP	Telnet	Nprint

TABLA1. 1 Comparativo de emuladores

[1] www.hospedajesydominios.com, Enero 2005

Existen también usuarios que leen datos desde el servidor de Oracle los cuales se conectan por medio del Internet al servidor de aplicaciones, por el cual se conectan a la base de datos Oracle.
Todos los usuarios conectados a la red tienen la posibilidad de compartir los recursos de la red como son compartición de archivos, impresoras, la utilización de mail interno y externo y algunos usuarios la utilización de Internet.

El servicio de mail interno se lo provee por medio de un producto de Microsoft llamado Office mail de Windows 95, los clientes ingresan al servicio por medio del Microsoft Outlook.

El servicio de mail externo se lo provee por medio de la creación de las cuentas en un servidor que no maneja Ecuasanitas, sino que solo administra las cuentas de usuario ya que este servicio es contratado a una empresa la cual configura y administra el servidor, los clientes se conectan por medio de Outlook Express.
Los usuarios que utilizan Internet se conectan al servidor Proxy (ecuasanitas.server) , la configuración se realiza en TCP/IP y se añade los DNS y la puerta de enlace que es la dirección IP del servidor de Internet, la dirección del usuario con acceso al Internet debe ser añadida en el archivo squid.conf del servicio Squid del servidor Proxy

1.2. DESCRIPCION DE FUNCIONALIDAD DE LOS SERVIDORES.

Básicamente en el edificio matriz se cuentan con 5 servidores, como se indicará en el diagrama de Distribución, en donde cada uno de ellos cuenta con funciones importantes como son:

El Servidor Proxy, sirve como un servidor Web y Proxy las características del equipo cumple con las necesidades de los usuarios dentro la red ya que no se tiene inconvenientes de lentitud al ingreso de los usuarios para la salida al Internet.

El servidor de Desarrollo en el cual se realizan los respaldos de archivos diarios del servidor de Producción y de la Base de Datos Oracle, además es en donde se encuentran almacenados todos los programas fuentes que se utilizan en el sistema de la empresa.

El servidor de Aplicaciones en donde se encuentran toda la programación realizada en java y es el servidor por el cual se conectan los usuarios de Guayaquil y de Quito a la Base de Datos Oracle.

El servidor de Base de Datos Oracle es en el cual se almacena la Base de datos de todos los clientes de la Empresa que poseen la cobertura de Reembolso de Medicamentos,

El servidor de Producción, es al cual todos los usuarios se conectan al sistema de Ecuasanitas, es en donde se encuentra almacenada la Base de datos de todos los Clientes a nivel nacional de la Empresa, este servidor es muy importante ya que es el servidor central de la Empresa y contiene todos los datos de los usuarios.

Como se indica en las especificaciones de los servidores cada uno de ellos es muy importante ya que cumplen funciones diferentes dentro de la red, las principales ventajas de cada uno de ellos son las características técnicas que poseen por lo tanto son equipos de rápido acceso dentro de la red. Una de las desventajas es la del servidor de aplicaciones ya que posee el sistema operativo Red Hat 8.0, debido a que es un sistema que ya no tiene soporte técnico ni parches dentro del Internet, pero existe la posibilidad de que mas adelante se actualice el sistema operativo.

1.2.1 DIAGRAMA DE DISTRIBUCION DE SERVIDORES.

Hoy en día la Empresa Ecuasanitas S.A cuenta con 5 servidores los cuales se distribuyen cómo se indica en el siguiente diagrama:

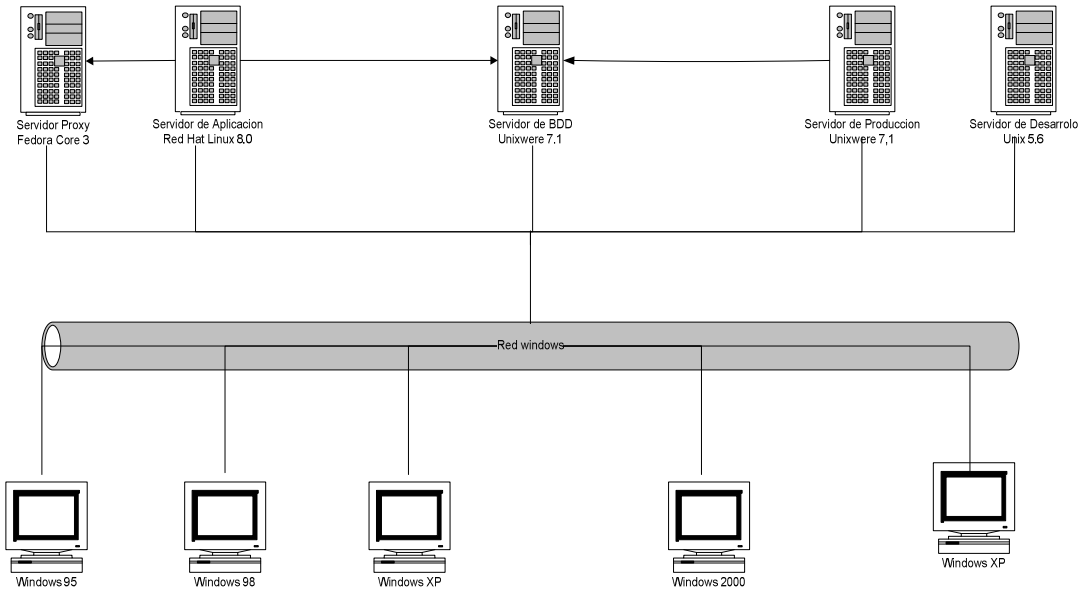

DIAGRAMA ECUASANITAS

GRAFICO 1. 1 Diagrama de Servidores de la Matriz de Ecuasanitas S.A

SERVIDOR	FUNCION	PROCESADOR	MEMORIA	DISCO	MARCA
Internet	Proxy	Pentium IV 3.0 ghz	1GB	80 GB.	HP
Aplicación	J2ee	Pentium IV 1.8 ghz	512 MB	40 GB.	IBM
Base de Datos	Oracle Versión 9i	2 Procesadores Intel Xeon 2.8 ghz	1 GB	5 Discos 36 GB C/U hot swap	CLON
Producción	Rm/Cobol	2 Procesadores Intel Xeon 3.0 ghz	1 GB	3 discos de 36 GB C/U Hot Swap	CLON
Desarrollo	Sco Unix 5.0.6	2 Procesadores Intel Xeon 3.0 ghz	1 GB	3 discos de 72 GB C/U Hot Swap	HP

TABLA1. 2 Características de Servidores.

1.2.1.1 Software de Control de Reglas en Servidor Proxy.

Existe una variedad de paquetes de software de Proxy para Linux, tal es el caso Squid que es un Proxy a nivel de de aplicaciones para HTTP, HTTPS y FTP. También puede ejecutar peticiones DNS bastante rápido de lo que puede hacerlo la mayoría de software cliente. Squid es ideal para acelerar el acceso a WWW, y para controlar el acceso a sitios Web (utilizando paquetes como SquidGuard).

Squid es un servidor Proxy muy confiable, robusto y versátil. Al ser Software libre, además de estar disponible el código fuente, esta libre de pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

Entre otras cosas, Squid puede hacer Proxy y caché con los protocolos http, FTP, GOPHER, Proxy de SSL, caché transparente, aceleración http, caché de consultas DNS y más. [2]

Las ventajas de utilizar el Squid son:

- Soporta protocolos de aplicación como (HTTP, FTP, etc.)
- Tiene un avanzado mecanismo de autentificación como (a quien y cuando se permite utilizar el Proxy).
- Permite actuar como 'caché' de Internet, copiando contenido en forma local para poder acceder más rápido (por ejemplo, animaciones flash).
- Es un software Libre.

Las desventajas de utilizar, un Proxy:

- La máquina donde funcionara el Proxy debe tener capacidad de almacenamiento acorde a la caché que se necesita.

[2] http://www.icmm.csic.es/pomt/SQUID.htm, Marzo 2005

- Debe tener un buen poder de procesamiento, ya que no es solo un 'reenvio' de paquetes TCP/IP.
- En la mayoría de ocasiones es más rápido hacer NAT que utilizar un Proxy.

1.3. TIPOS DE FIREWALL EXISTENTES

En la actualidad se debe tener muy en cuenta que se necesita de todo el apoyo en lo referente a las seguridades de los equipos de computo por lo que a continuación se explicará las funciones de los firewalls vía software que se pretende configurar en este proyecto.

1.3.1 FIREWALLS VIA SOFTWARE.

Un Firewall es un dispositivo de seguridad que no solo se compone de software sino que puede requerir de varios componentes de hardware de acuerdo con la política de seguridad establecida. De acuerdo a la investigación realizada en el mercado en la actualidad casi todas las empresas poseen un Firewall para la seguridad de las redes, pero a pesar de esto no se puede afirmar que una red tenga una seguridad al cien por ciento.

Existen adicionalmente diferentes tipos de Firewalls que van desde Filtradores de Paquetes (Packet Filters) hasta Aplicaciones Gateways con Proxys. [3]

El establecimiento de un Firewall definitivamente requiere de mucho conocimiento técnico y de buena disposición administrativa. Se requiere de mucho conocimiento técnico porque generalmente los ataques se realizan a través de malas configuraciones de los dispositivos de una red o los archivos de configuración que presentan los diferentes sistemas operativos y productos de base como servidores Web, Mail, etc.

---

[3] www.deltaasesores.com, Enero 2005

Para la empresa Ecuasanitas la seguridad es una de las principales tareas a tomar en cuenta, la organización decide conectar su red privada al Internet. Ya que los principales accesos que se tiene son los servicios de World Wide Web (WWW), Internet Mail (e-mail), Telnet, Chat y File Transfer Protocol (FTP).

Para superar los temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Aun si la organización no esta conectada al Internet, se debería establecer una política de seguridad interna para administrar el acceso de usuarios a los recursos de la red y proteger sensitivamente la información importante.

El firewall instalado en el servidor de Proxy determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este, ya que no se cuenta con un firewall instalado para los clientes Windows, pero también se puede activar una protección mínima que se encuentra en el TCP/IP de la configuración de red a partir de Windows 2000 y XP.

En la actualidad se cuenta con un Proxy que realiza las funciones de firewall pero con configuraciones básicas de seguridad.

1.4. ENLACES DE COMUNICACIÓN EXISTENTES.

Los enlaces de comunicación existentes en la empresa son: Enlaces LAN y Enlaces Radio MODEM, que a continuación se detallan:

1.4.1 ENLACES LAN

El tipo de red instalada en la Empresa Ecuasanitas es una LAN que es una red de datos de alta velocidad y tolerante a fallas, que cubre áreas geográficas relativamente pequeñas. Las cuales conectan wokstations, PC's impresoras y otros dispositivos.

La LAN ofrece a los usuarios de la red muchas ventajas entre las que se incluyen un acceso compartido a dispositivos y aplicaciones, intercambio de archivos entre usuarios conectados y comunicación entre usuarios vía correo electrónico, Internet y otras aplicaciones.

La red LAN se compone de computadores, tarjetas de interfaz de red 10/100, medios networking, dispositivos de control de tráfico de red y dispositivos periféricos. La LAN instalada hace posible que la empresa comparta de forma eficiente elementos tales como archivos e impresoras y permiten la comunicación vía mail e Internet.

La empresa posee una red LAN con los siguientes componentes:

- 5 servidores los cuales proveen de servicios a los usuarios.
- 160 estaciones de trabajo con el sistema operativo Windows que comparten la red y sus recursos.
- Un sistema de cableado estructurado el cual esta constituido de cable UTP categoría 5e tanto el backbone como la red horizontal.
- Entre los equipos de conectividad se cuenta con 5 switch marca 3COM los cuales están conectados en forma apilada (up link), para la conectividad de los usuarios dentro de la oficina matriz. Se posee 4 Radio Modems marca Orinoco para la conectividad de las agencias con la matriz, y un router cisco 800 para el ingreso al Internet.
- El protocolo utilizado es el TCP/IP, no se posee un servidor de dominio sino un grupo de trabajo.
- La red es privada de clase B

Diagrama Físico de la Red LAN

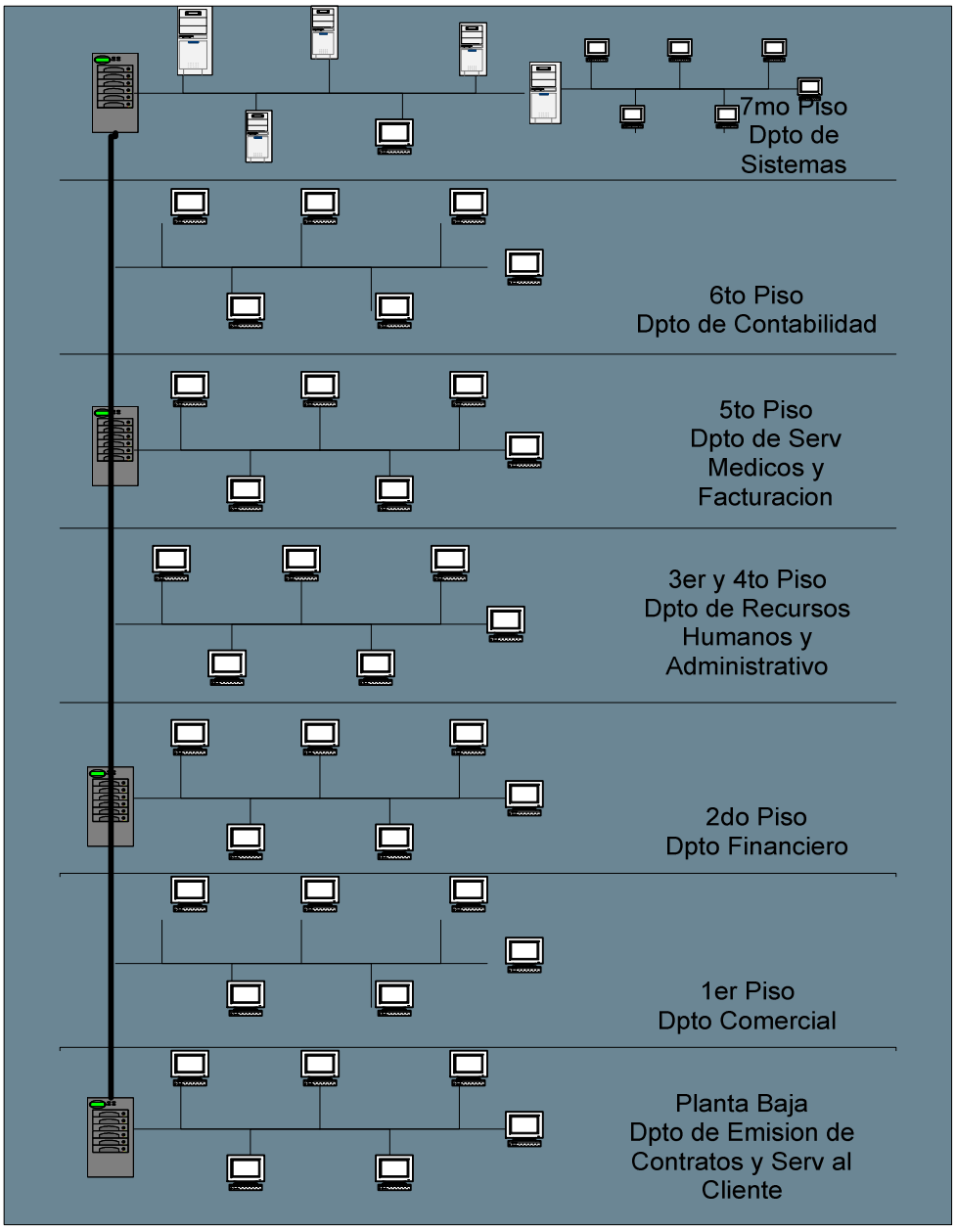

GRAFICO 1. 2 Diagrama Físico de la Red LAN

(Edificio Principal)

1.4.1.1 Características de los equipos de enlace

Switch 3 Com Baseline

Los 5 equipos existentes en la red son de 48 puertos 10/100/1000 capa 2 conectados en up link, tienen una configuración fija. Idóneos para trabajar con cableado estructurado con montajes en racks, sin necesidad de administración o configuración.

Router Airspan

Este equipo es utilizado para la conexión de última milla, con un ancho de banda de 128Kb, específicamente es utilizado para la conexión de Internet.

1.5. ENLACES SPREAD SPECTRUM.

Ecuasanitas para conectar las redes LAN de las agencias con la red de la matriz, realizó la conexión con la técnica denominada Spread Spectrum, esta técnica permite conseguir una conexión segura dentro de un ambiente hostil que implica la posibilidad de interferir la señal trasmitida por oyentes y receptores no autorizados. Sin embargo se sacrifica ancho de banda, es decir se trasmite con un ancho de banda mucho mayor que el mínimo necesario a cambio de obtener otros beneficios como es la seguridad de los datos trasmitidos.

Básicamente, Spread Spectrum es una técnica mediante la cual una señal modulada es nuevamente modulada, de manera tal de producir una señal que interfiera muy poco con otra señal que este ocupando la misma banda de frecuencia, Por lo tanto un señal de banda AM (Amplitud Modulada) comercial, podría no notar la presencia de una señal spread spectrum que este operando en la misma banda. De manera recíproca, una señal de spread spectrum podría no detectar la presencia de una señal AM broadcasting, por que se

puede decir que las señales son transparentes ya no interfieren la una con la otra.

La principal ventaja de tener una conexión mediante Spread Spectrum es su capacidad de rechazar las interferencias, ya sean de origen no intencional.

Spread Spectrum debe cumplir con dos características:
1.- Spread Spectrum es un modo de transmisión por el cual los datos de interés a trasmitir ocupan un ancho de banda mayor que el mínimo necesario.
2.- La expansión del espectro se lleva a cabo antes de la transmisión a través de un código que es independiente de la secuencia de datos. Este mismo código es usado en el receptor (en forma sincronizada) para comprimir de nuevo el espectro y así recuperar la secuencia de datos original.

Uno de los atributos importantes de la modulación spread spectrum es que se puede proveer protección contra señales interferentes (jamming) de potencia finita. La señal jamming puede ser ruido de banda ancha bastante potente o una señal multitono que es dirigida al receptor en forma intencional para interferir la comunicación. La protección contra jamming se logra haciendo que la señal de información ocupe un ancho de banda mayor que mínimo necesario. Esto hace la señal transmitida adopte la apariencia de una señal de ruido. De esa manera, se puede propagar por el canal sin que sea detectada por otros usuarios ajena a la empresa.
La frecuencia utilizada por al empresa Ecuasanitas es de 2.4GHZ, y la velocidad de los datos con la cual son trasmitidos es de 11Mbps, con el estándar 802.11b. [4]

1.5.1 EQUIPOS UTILIZADOS EN EL ENLACE

Routers Orinoco COR1100

[4] http://nernet.unex.es/~miguel/pdfs/teoria_comunicaciones/Tema4.pdf , Julio 2005

Existen dos routers instalados en la matriz de la empresa los cuales permiten el enlace con las agencias que Ecuasanitas posee.

Estos equipos trasmiten los datos a 11 Mbits. son compatible con el estándar 802.11b (Wi-Fi). Los equipos extienden el alcance de su red Ethernet cableada, proporcionan un fácil acceso a la red a los usuarios. Cuentan con características únicas de arquitectura, como su doble ranura para tarjetas PC, agregan capacidad Ethernet a 10/100 Mbps.

Las principales ventajas son:

Arquitectura de ranuras para tarjeta PC inalámbrica.

Su doble ranura para Tarjetas PC le da flexibilidad en el uso de radios Orinoco y protege su inversión. Puede cambiar de tecnología con tan solo cambiar su tarjeta PC Orinoco.[5]

El sistema consiste en:

- COR-1100 Ruteador Central Externo (Central Outdoor Router, COR)
- ROR-1000 Ruteador Remoto Externo (Remote Outdoor Router, ROR)
- Cliente de Ruteador Externo (Outdoor Router Client, ORC)

Antenas

Las características principales de las antenas utilizadas en el enlace son:

- Antena unidireccional Tipo Grid
- Trabaja sobre 2.4GHz a 2.5GHz para IEEE802.11b WLAN
- Alta ganancia de 24dBI para mayor cobertura
- Tamaño pequeño [6]

---

[5] Orinoco Or manager User´s Guide for Outdoor Router 1000/1100

[6] Orinoco Or manager User´s Guide for Outdoor Router 1000/1100

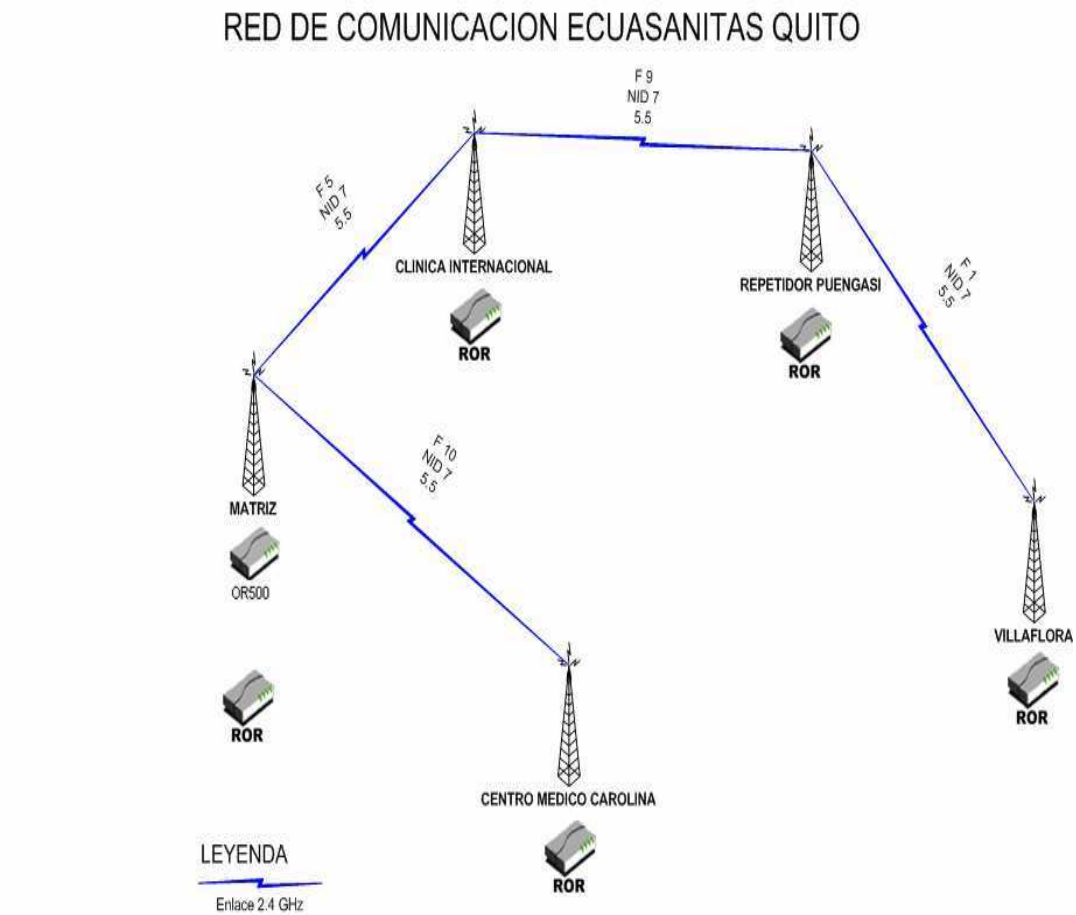

GRAFICO 1. 3 Gráfico de enlace de Radios.

1.6. SERVICIOS QUE PRESTARA A FUTURO

Los usuarios conectados a la red LAN de la empresa han crecido notablemente a medida que pasa el tiempo, por lo que se analiza la posibilidad de crear nuevos servicios para una mejor comunicación

1.6.1 PLANES PARA AMBIENTES INTRANET /EXTRANET.

1.6.1.1 Ambiente Intranet

Debido a que las intranets actualmente se han convertido en la herramienta más efectiva e importante para la comunicación y gestión al interior de los negocios. Se piensa en la posibilidad de implementar una intranet en la

empresa la cual permiten integrar una gran cantidad de servicios para el usuario interno con una interfase común como es el navegador (Browser).

Las principales ventajas que se ofrecerá, con la creación de la Intranet será:

El adecuado tratamiento de la información dentro de la organización es un aspecto estratégico de máxima importancia que define la calidad de la gestión y servicio.

Debido a que la intranet utiliza tecnologías de Internet, permite compartir, de un modo efectivo, rápido y económico, información y recursos entre los usuarios de la Red, accediendo a todos los servicios desde un mismo, sencillo y amigable interfaz gráfico

La Intranet hace que esta sea una solución eficaz, al estar basada en estándares abiertos y universales, arquitecturas escalables y multiplataforma, permitiendo el acceso tanto a los sistemas corporativos como a los recursos de Internet.

La flexibilidad y potencia de los desarrollos de la intranet permiten crear un amplio banco de aplicaciones entre las que se pueden citar:

- Comunicaciones internas.
- Normativas, procedimientos y manuales.
- Publicación de noticias y novedades.
- Agendas de actividades y actos programados.
- Distribución y transferencia de información.
- Enlaces con distintas bases de datos y aplicaciones remotas.
- Directorios de acceso común y/o restringido.
- Cuadro informativo.
- Encuestas y sugerencias.

1.6.1.2 Ambientes Extranet

Debido a que Ecuasanitas es una empresa que brinda un servicio y trabaja con prestadores médicos de varias clínicas y hospitales del país se tendría en un futuro la necesidad de implementar una extranet, ya que es una herramienta que se utiliza para llevar a cabo tareas complejas por lo regular la relación que establece una extranet es de proveeduría o atención a clientes, pero llega incluso a mantener relaciones entre empresas que desarrollado B2B. En la mayoría de los casos, no importa que una extranet exista fuera del firewall de una empresa (herramienta que bloquea el acceso a visitantes no autorizados) o a través de otras compañías, para accesarla siempre será necesario contar con claves específicas.

Los principales beneficios serian permitir al cliente y prestadores médicos accedan a los sistemas de información de forma directa pero controlada y segura con el objetivo de lograr grandes beneficios en ahorro de tiempos, oportunidades de negocios, mejoramiento en el servicio al cliente, costos en llamadas telefónicas, optimización de procesos, entre otros.

CAPITULO II

ANALISIS DE LOS MEDIOS DE ACCESOS SEGUROS APLICABLES A LA EMPRESA

INTRODUCCION

En el capitulo anterior se hizo un estudio de la infraestructura que actualmente se tiene en la empresa, por lo que se ha visto la necesidad de realizar un análisis profundo de la seguridad de la red en el ambiente general de las plataformas con las cuales se trabajan por lo que se realizó el análisis de accesos seguros los cuales se podría aplicar a la empresa.

2.1 ACCESO VIA WEB

Dentro de los accesos Web las posibilidades de aplicar seguridades son los certificados digitales, el protocolo SSL, entre otros que pueden realizar estas tareas.

2.1.1. CERTIFICADOS DIGITALES

Un certificado digital es el equivalente electrónico a un Documento de Identidad que permite la identificación, firma y ciframiento electrónico de documentos y mensajes.

Uno de los principales problemas que surgen cuando se realiza el ingreso al Internet es el de la identificación de las personas o entidades. Por ejemplo, ¿Cómo se asegura de que una clave pública que se ha encontrado en Internet pertenece realmente a quien dice pertenecer?[7]

Una posible solución a este problema es la utilización de un Certificado digital que es fichero digital intransferible y no modificable, emitido por una tercera parte de confianza (AC), que asocia a una persona o entidad una clave publica.

[7] www.certificadodigital.com.ar/frameset_serv.htm, Septiembre 2005

Los certificados digitales que siguen el estándar X509v3, utilizado por los navegadores contienen la siguiente información:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado
- Fecha de validez
- Número de serie
- Identificación del emisor del certificado.

Con el certificado digital se permitirá a la empresa realizar gestiones empresariales, y cualquier proceso que suponga la actualización o consulta de datos por parte del usuario en las distintas administraciones públicas.
Uno de los principales componentes de la realización de un certificado digital es la firma digital que es el equivalente de la firma convencional, es decir de que es un añadido al final del mensaje conforme se está de acuerdo con lo que allí se dice. La firma digital es una transformación de un mensaje en forma de cualquier persona con conocimiento del mensaje y de la clave pública del firmante pueda comprobar que dicha transformación ha sido realizada realmente por el firmante.[8]

En conclusión al análisis se puede decir que los certificados digitales permiten intercambiar información de forma confidencial con el intercambio de una clave pública y su poseedor una clave privada con la que se puede firmar cualquier documento. Ya que en la vida diaria es necesario el intercambio de información la cual se puede rechazar o aceptar la identidad de una persona.

Por consiguiente si la empresa requiriera en un futuro que los usuarios realicen los pagos de cuotas vía Web se podría implementar una pagina Web segura con un certificado digital de una entidad que emita el mismo, a nombre de Ecuasanitas S.A, complementado con el protocolo SSL para establecer una comunicación segura.

---

[8] www.certificadodigital.com.ar/frameset_serv.htm, Septiembre 2005

2.1.2 PROTOCOLO SECURE SOCKET LAYER (SSL)

Para establecer una comunicación segura vía Web se puede utilizar el protocolo SSL en donde previamente el cliente y el servidor realicen un proceso de reconocimiento mutuo y de petición de conexión. El SSL soporta solicitudes de conexión por puertos diferentes al utilizado normalmente para este servicio. El protocolo SSL tiene un saludo inicial, en donde el cliente envía al servidor información del SSL implementado, de los algoritmos de encriptación que soporta, las longitudes de claves máximas que admiten para cada uno de ellos y las funciones hash que pueden utilizar. También se le solicita al servidor el envió de su certificado digital X2509v3, con objeto de verificar el cliente la identidad del mismo y recoger su clave pública. Existen medidas adicionales, en donde el cliente envía asimismo una clave numérica aleatoria, para que se pueda establecer una comunicación segura mediante otros protocolos o algoritmos en el caso de que el servidor Web no posea certificado digital.

A continuación, el servidor SSL responde al cliente, enviándole su Certificado Digital con una llave pública e informándole de su versión de SSL, de los algoritmos y longitudes de clave que soporta.
Entre las principales ventajas que se puede conseguir con la implementación del protocolo SSL son los avances en la implementación de sistemas de comunicación seguros, que hacen posible un crecimiento importante en las transacciones por Internet. En conclusión la seguridad que proporciona SSL es Autenticidad, Confidencialidad, Integridad y No Repudio.

Las desventajas de utilizar SSL es que carece de muchos de los elementos necesarios para construir un sistema de transacciones seguras usando Internet. Debido a que el SSL garantiza la confidencialidad e integridad de los datos en tránsito. Por lo tanto, si se envían datos personales al servidor, entre ellos el ya citado número de tarjeta de crédito, el número de la seguridad social, el DNI, SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Por lo que los datos

podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito. [9]

En conclusión el SSL provee una capa para asegurar los protocolos de Internet (como HTTP, SMTP, FTP, etc) y prevenir que la información transmitida por ellos sea falsificada, modificada o interceptada por terceras personas mientras se encuentra en tránsito por la red. Además con SSL se asegura la información, la autenticidad e integridad de los datos.

2.2 ACCESO VIA RADIUS

Radius es un protocolo usado en ambientes de la red, normalmente se usa para los dispositivos de la red como los Routers, Modems de Servidores, pero también se lo puede configurar vía software, se lo usa por las siguientes razones:

- Generalmente no pueden administrarse un gran número de usuarios con la información de autenticación distinta. Por lo que se requiere más almacenamiento de los muchos sistemas que lo poseen.
- Con la implementación del servidor Radius que es un Acceso remoto Dial up se facilitara la administración de los servidores desde cualquier parte en forma centralizada y se brindara un nivel de seguridad
- Radius proporciona un nivel de protección contra un Sniffing y ataque de hackers. Es un protocolo de autenticación remota que provee de protección intermitente.
- El servicio de Radius se apoya uniformemente en los vendedores de hardware ya que la plataforma en la que los servidores Radius se llevan a cabo son sistemas incluidos, por lo tanto cualquier cambio en el protocolo Radius tendría que ser por lo menos minimamente compatible con las ya existentes de los clientes de Radius y Servidores.

[9] http://www.iec.csic.es/criptonomicon/comercio/ssl.html, Septiembre 2005

Aplicabilidad

En este análisis se tratara de algunas de las características principales de Radius y razones por las cuales se podría implementar un servidor Radius, para la autenticación de usuarios y contraseñas. Ya que dependiendo del modo de autenticación que se use las debilidades del usuario-contraseña descritas pueden o no pueden componer la seguridad del esquema de autenticación.

Por otro lado cuando un sistema de Challenge/Response esta en uso, es un compromiso completo de los atributos del Usuario-Contraseña lo que expondría solo la información no permitida a los ataques que pueden darse al sistema de autenticación. Este análisis no cubre la funcionalidad de las cuentas del protocolo de Radius ya que normalmente no transporta la información que debe guardarse como confidencial.

PAQUETE QUE TRANSPORTA RADIUS.

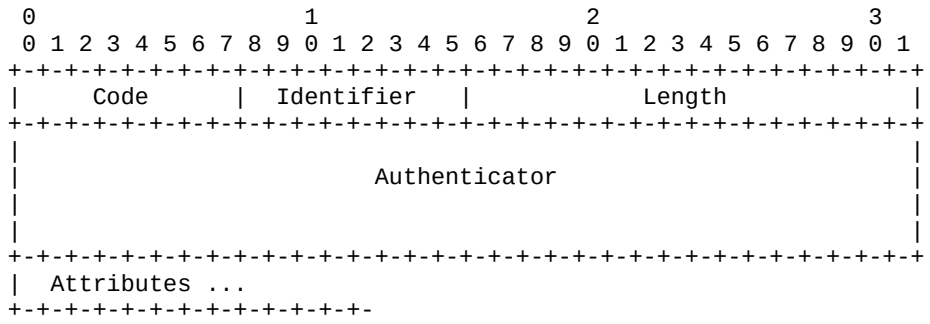

GRAFICO2. 1 Paquete de transporte Radius [10]

El código establecido por el paquete Radius es el siguiente:

VALOR	DESCRIPCION
1	ACCESO-PETICION
2	ACCESO-ACCEPTACION
3	ACCESO-RECHAZO
4	CONTADOR-PETICIONES
5	CONTADOR-RESPUESTAS
11	ACCESO-NO PERMITIDO
12	ESTATUS DEL SERVIDOR
13	ESTATUS DEL CLIENTE
255	RESERVADO.

TABLA2. 1 Paquete que trasporta Radius.

[10] www.untruth.org/~josh/security/radius/radius-auth.html, Septiembre 2005

El identificador es un valor de octeto que le permite al cliente del Radius enviar una contestación como correcta.

La sección de atributos es donde un número arbitrario de campos del atributo se guarda. Los únicos atributos pertinentes son el Usuario-Nombre y atributos del Usuario-Contraseña.[11]

Para la autenticación de Radius se utilizará Acceso-Petición que involucra el nombre del usuario y contraseña del usuario, seguido por el Acceso-Aceptación, Acceso-Rechazo o un fracaso. Para lo cual se requiere del Cliente y del Servidor, en donde el cliente es el que tiene la información de la autenticación que desea validar, y el servidor es el que tiene el acceso a una base de datos de información de la autenticación que puede usar para validar la demanda de la autenticidad del cliente.

Los siguientes pasos describen el planteamiento genérico que se utilizaría para autenticar el equipo de un usuario de modo que obtenga un acceso.

- Sin una clave de autenticación válida, el punto de acceso prohíbe el paso de todo el flujo de tráfico.
- Cuando la estación recibe el desafió, responde con su identidad. El punto de acceso reenvié la identidad de la estación a un servidor Radius que realiza los servicios de autenticación.
- Posteriormente, el servidor Radius solicita las credenciales de la estación, especificando el tipo de credenciales necesarios para confirmar su identidad. La estación envía sus credenciales al servidor Radius (a través del “puerto no controlado” del punto de acceso.
- El servidor Radius válida las credenciales de la estación y transmite una clave de autenticación al punto de acceso. La clave de autenticación se cifra de modo que solo el punto de acceso pueda interpretarla.

[11] www.untruth.org/~josh/security/radius/radius-auth.html, Agosto 2005

- El punto de acceso utiliza la clave de autenticación para trasmitir de manera segura las claves correctas a la estación, incluida una clave de sesión de unídifusión para esa sesión y una clave de sesión global para las multidifusiones.
- Para mantener un nivel de seguridad, se puede pedir a la estación que vuelva a autenticarse periódicamente.

2.3 ACCESO VIA TACACS

La preocupación de los administradores de red son los accesos remotos a los servidores, routers, etc, en fin a los dispositivos de ínterconectividad por personas ajenas a la empresa o sin autorización por lo que se analizará un servicio que permite la conexión remota con autenticación.

TACACS (Sistema de Control de Acceso al Controlador de Acceso a la Terminal), es un protocolo de autenticación, que suministra autenticación de acceso remoto y servicios relacionados, como por ejemplo, se puede realizar registro de eventos, las contraseñas de usuario se administran en una base de datos central en lugar de administrarse en routers individuales, suministrando una solución de seguridad de red fácilmente escalable.[12]

El servidor de TACACS permite que un host LINUX de la red haga la validación de passwords, lo cual permitiría un acceso mas controlado a los routers de la empresa, dejando atrás la limitación de que exista un par de passwords para acceder al router. En la máquina LINUX que ejecuta el servidor TACACS para validar las peticiones enviadas a los Router. El fichero Standard /etc/passwd es el que se usa para la validación de usuarios. Con el manejo de comandos se controlará lo que ocurre, si el servidor TACACS esta o no esta respondiendo, si se da este caso podría quedarse Sin acceso al router, por lo que se configura el servidor para que indique si le dejaría loguearse sin password (SUCCEED) o si permite al router autentificar de modo Standard (PASSWORD).

[12] www.ciscoredaccionvirtual.com/redaccion, Agosto 2005

También se analizará un método para mantener una lista de usuarios y sus Passwords directamente en el router. El comando "USERNAME user PASSWORD.

2.4 REDES VIRTUALES ENTRE LOCALIDADES

Una de las preocupaciones de los administradores de la red de la empresa Ecuasanitas, es la seguridad en la comunicación de sus agencias, por lo que se desea configurar una VPN entre la agencia de Quito y Guayaquil ya que es de suma importancia la conexión entre ambas localidades debido a que es necesario trabajar con los recursos compartidos de una manera segura y no que sean dos redes que operen aisladamente. Por lo que surgió la necesidad de proveer el acceso a los usuarios de ambas redes. La VPN es una gran alternativa a la conexión WAN lo que reducirá costos y se brindara un servicio en línea mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

2.4.1 ¿QUE ES UNA VPN?

Es un sistema de comunicación de túnel seguro que procede de un computador de un usuario remoto, a través de Internet, y va directamente a la red privada de la empresa (un punto de conexión en el extremo de la red pública existente). Una red VPN permite que los usuarios accedan de forma segura a una red privada a través de varios tipos de conexión a Internet.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública, como se muestra en la siguiente figura:

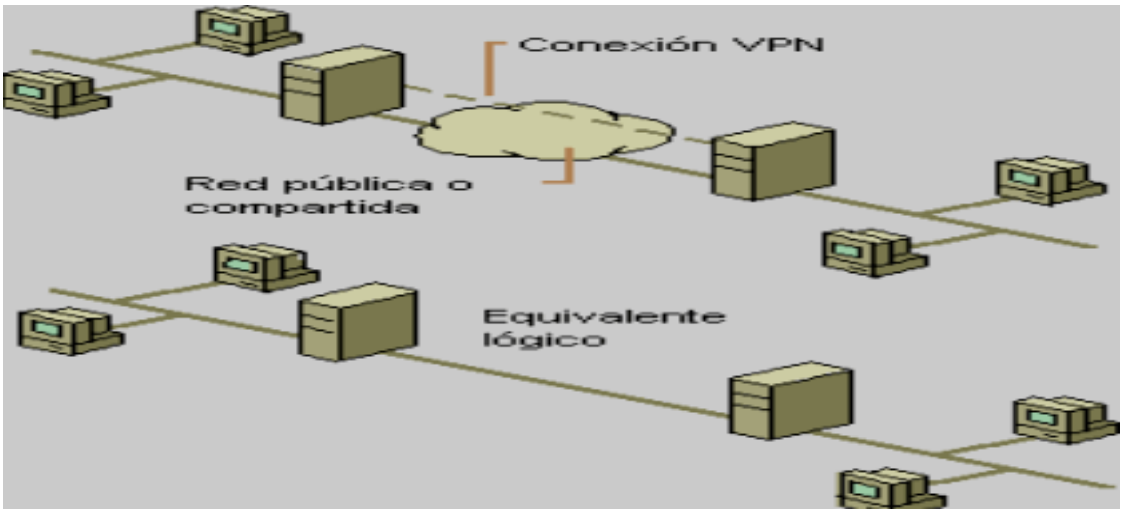

GRAFICO2. 2 Esquema general de una conexión VPN[13]

2.4.1.1 Tecnología de túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

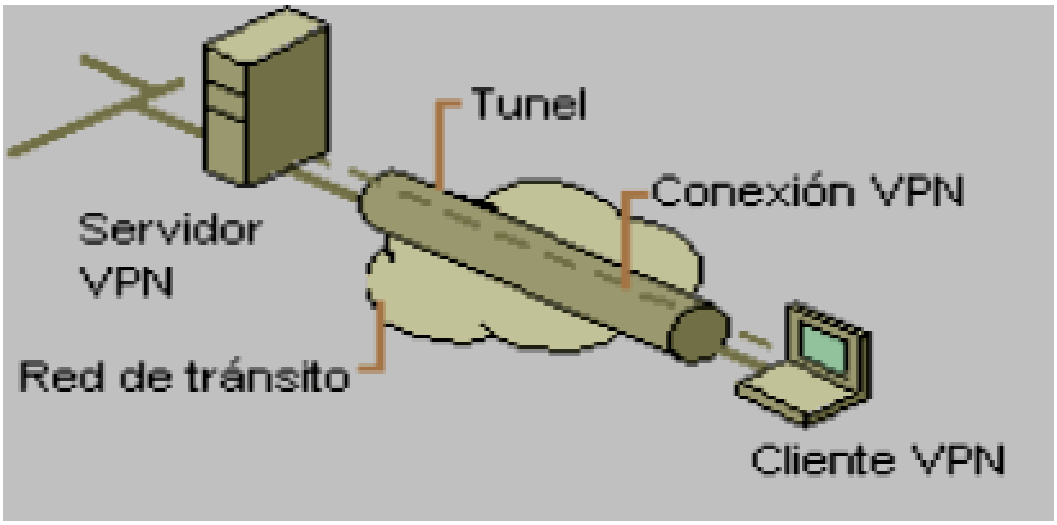

GRAFICO2. 3 Tipo de Tecnología [13]

[13] www.monografias .com, Agosto 2005

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de transito se envían los datos sin problemas.

2.4.1.2 Requerimientos básicos de una VPN

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario.
- Administración de direcciones.
- Codificación de datos.
- Administración de claves.
- Soporte a protocolos múltiples.

Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accedió, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

Herramientas de una VPN

- VPN Gateway
- Software
- Firewall
- Router

Donde se puede implantar:

Los VPN son ideales para centros de datos, centros de almacenamiento u oficinas centrales regionales que necesitan conexiones muy rápidas con muchos desplazamientos. El servicio ofrece Ethernet en el área extensa para aumentar al máximo la simplicidad y la economía.

Una razón para la implantación de los VPN´s es la financiera: los enlaces dedicados son demasiados caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo. Las conexiones con Internet tienen un coste más bajo que los enlaces dedicados, principalmente cuando las distancias son largas.

Internet es una red pública, donde los datos en tránsito pueden ser "leídos por cualquier equipo". La seguridad en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión, no puedan ser descifrados. Los datos transitan codificados por Internet en " Túneles Virtuales" creados por dispositivos VPN´s que utilizan criptografía; y esos dispositivos que son capaces de " entender" los datos codificados forman, una " red virtual" sobre la red pública. Es esa red virtual la que es conocida como VPN.

2.4.1.3 Ventajas de una VPN

Dentro de las ventajas más significativas se recalcan las siguientes:

- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costes.

- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

Conclusión.-

Los VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro apoyado en el internet, el único inconveniente que pudieran tener los VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

2.4.1.4 Protocolos de la VPN

Los protocolos mas utilizados en las VPN son: PPTP (Point to Point Tunneling Protocol o Protocolo de túnel punto a punto) y L2TP (Layer 2 Tunneling Protocol o Protocolo de túnel de capa 2). Para seleccionar el protocolo que se desea utilizar para configurar el servidor, se debe comprender el funcionamiento de ambos protocolos y tener en cuenta sus funciones de autenticación y encriptación.

Si se compararan y decoficarán los datos de los protocolos PPTP y L2TP en el modelo de referencia OSI, se encontrará que el principal punto en común es que ambos descansan en PPP (Point to Point Protocol o Protocolo punto a punto). PPP es la base para los dos protocolos VPN y el protocolo que encapsula los datos de transferencia (esto es, la carga) a través de una red

privada. PPTP y L2TP añaden otra capa de encapsulación para transferir la carga a través de un túnel en una red pública.

PPTP.- Sirve para proveer entre usuarios de acceso remoto y servidores de una red privada Virtual, como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP como Internet.[14]

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos Call ID y velocidad de conexión.

En el PPTP el encapsulado de tramas PPP en datagramas IP, utilizando una versión extendida del GREE. La conexión de control se realiza sobre TCP puerto 1723.

L2TP.- Facilita el entunelamiento de paquetes PP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que corran.

El escenario típico L2TP, cuyo objeto es la creación de entunelar marcos PPP entre e sistema remoto o cliente LAC y un LNS ubicado en una LAN local. [1]

2.5 ESTUDIO DE VIABILIDAD ECONOMICO, TECNICO, LOGISTICO

2.5.1 VIABILIDAD ECONOMICA

- Además se puede complementar esta fundamentación con la investigación de campo, ya que esta ayudará al desarrollo de herramientas que se necesitan en el lugar mismo de los hechos, la empresa ECUASANITAS, también ayudará a

[14] www.monografias.com/trabajos12/monvpn/monvpn.shtml, Agosto 2005

la observación de como deberían estar estructurados las seguridades requeridas por el personal de la empresa.

- El desarrollo de este proyecto esta encaminado sobre la base de la investigación demostrativa ya que gracias a ella, se obtiene bases lógicas para el desarrollo de las ideas a defender, para llegar a alcanzar los objetivos antes fijados y la correcta aplicación de los conocimientos adquiridos en base a investigación documental.

- Se utilizará algunos métodos para esto como es la utilización de RADIUS, VPN`s, TACAS, obteniendo así una herramienta capaz de solventar las necesidades que un administrador de redes en general necesita para la correcta administración y mantener la información con mejores seguridades, para la gestión y monitoreo de la red que administra.

- Se obtendrá una base teórica muy rica, gracias a la aplicación de la investigación documental, ya que mediante esta se recopilarán datos informativos que ayuden al crecimiento sostenido de dicha base para así asegurar que los objetivos van a estar correctamente desarrollados y las metas propuestas serán alcanzadas por parte de del autor del proyecto

- El desarrollo de este proyecto se lo puede realizar con herramientas basadas en los sistemas operativos Linux, o Windows, pero todas las configuraciones se las ha realizado bajo el sistema operativo Linux ya que es un desarrollo con código libre, licenciamiento gratuito pero el asesoramiento técnico tiene un costo, en este caso existe un apoyo por parte de la Empresa Ecuasanitas con el autor para la generación de este proyecto, y es un ahorro para la empresa que el costo en el mercado para la configuración de los servicios a implementarse son de 1.650 dólares.

EQUIPOS, SOFTWARE Y COSTOS.-

ITEM	*DESCRIPCION*	*CANTIDAD*	*P/UNITARIO*	*P/UNITARIO*
1	COMPUTADOR (SERVIDOR)	1	700	700
2	ROUTERS	1	500	500
3	MANO DE OBRA DE VPN	1	100	100
4	MANO DE OBRA DE RADIUS	1	200	200
5	MANO DE OBRA DE TACACS	1	150	150
	TOTAL			1.650

TABLA2. 2 COSTOS

CONCLUSIONES DE FACTIBILIDADA DE COSTOS

Se concluye que existe la factibilidad para la realización del proyecto, ya que antes de iniciar con el mismo se pidió una autorización al Gerente General de la empresa para la realización de mismo.

2.5.2 VIABILIDAD TECNOLÓGICA.

- El desarrollo de este proyecto esta garantizado; ya que existe las herramientas necesarias en el mercado que ha aplicado estas ideas, pero es demasiado costoso para la implantación del mismo dentro de la empresa ECUASANITAS, por lo que al autor se le ha asignado la tarea de implementarlo en una forma más económica y personalizada para las necesidades de la misma, y la implementación eficiente de la misma según las necesidades a futuro.
- Además del beneficio que representa la posesión de estas herramientas, los cuales pueden servir en un futuro próximo para la realización de planes mucho más ambiciosos tomando como base a este proyecto.
- Los conocimientos que el autor tiene acerca redes, sistema operativo LINUX y de seguridades en redes, y el fuerte estímulo que la empresa ECUASANITAS ofrece hacia el área de investigación, y el gran asesoramiento que el autor recibirá de los Tutores miembros de la Escuela

de Ingeniería en Sistemas aseguran que el desarrollo de esta herramienta se llevará a cabo dentro de los límites y necesidades establecidas.

- La base física disponible como es: licencias de la plataforma LINUX no existe ningún inconveniente ya que es una plataforma de libre adquisición y junto a la capacidad instalada de computadores de la misma, garantizan que la base física no será un problema para el desarrollo de esta aplicación.

Con la implantación de estas herramientas, la información de la empresa va ha tener la fiabilidad y esto ayuda a que usuarios no autorizado, no puedan acceder a la misma.

Se puede plantear que esto ayudará siempre que este dentro de las políticas de la empresa. Existen pocas herramientas en el mercado para la generación de las seguridades en Intranet, también es porque el costo es demasiado alto para poder a acceder a las mismas.

Justificación

- Para empezar a realizar el diseño de las seguridades de la red se debe tener la infraestructura lista.
- Para este proyecto no se necesita adicionar más personal, ya que este proyecto solo necesita equipos y software.
- La seguridad de la red sirve para que no ingresen a la información de otros usuarios, y solo tener acceso a la suya.

Conclusiones

- La estrategia competitiva de la empresa se enfoca en la calidad que debe tener las seguridades, se ve localizada mediante en la configuración de los servidores para el manejo de una información segura y confiable, por lo que mediante esto se obtiene conocimiento técnico y esto genera una ventaja técnica competitiva.
- De acuerdo a los estudios realizados de las necesidades existentes se puede asumir que con la implementacion de este proyecto los usuarios se beneficiaran de herramientas confiables en el momento de querer acceder a los recursos tecnologicos de la empresa.

- El éxito del proyecto recae en cumplir los objetivos propuesto en el análisis realizado, ya que si no se implementa las estrategias previstas, no se tendría una visión favorable en el proyecto, por lo que se recomienda un presupuesto anual desde el primer año para asegurar los objetivos, esto es investigación y desarrollo.
- El proyecto es financiado en un su totalidad por la empresa, lo que permite que el proyecto se pueda ejecutar y esto será una inversión para la misma ya que se reflejará fiabilidad de la información que necesite los usuarios.

2.5.3 VIABILIDAD LOGISTICA.

- Uno de los puntos más importantes que se esperan del desarrollo de este proyecto, es la mayor facilidad que los administradores de redes obtendrán para el mejoramiento de las seguridades entre redes, a las cuales accedan los usuarios, el fácil aprendizaje de la herramienta y la integración total de la misma de utilitarios que se necesitan para realizar la hasta ahora, ardua tarea de administrar, monitorear y gestionar una red.
- Basándose en los acceso que realizan los usuarios a la red y la utilización de aplicaciones por parte de los mismos, se puede concluir si a un determinado servidor accede gran cantidad de usuarios a la vez y así tomar las respectivas medidas ya sea redistribuyendo las aplicaciones dentro de los servidores.
- Garantizar la correcta ejecución de la herramienta dentro del sistema Operativo LINUX, además garantizando la velocidad del mismo gracias a la utilización de las herramientas anteriormente mencionadas (TACACS, RADIUS, VPN`s), mejorando de una manera eficiente el acceso a las redes de la empresa.

En conclusión el análisis realizado hasta el momento es lo que se ha encontrado factible realizarlo en las instalaciones de Ecuasanitas, en lo cual se encuentran en potestad de que sea implementado o no en su totalidad.

CAPITULO III

DISEÑO E IMPLEMENTACION DE LOS ACCESOS SEGUROS A LA EMPRESA

INTRODUCCION

Se analizará la factibilidad de realizar un diseño y la configuración de los medios seguros aplicables a la empresa para el ingreso a la red, de acuerdo a la infraestructura que se tiene actualmente.

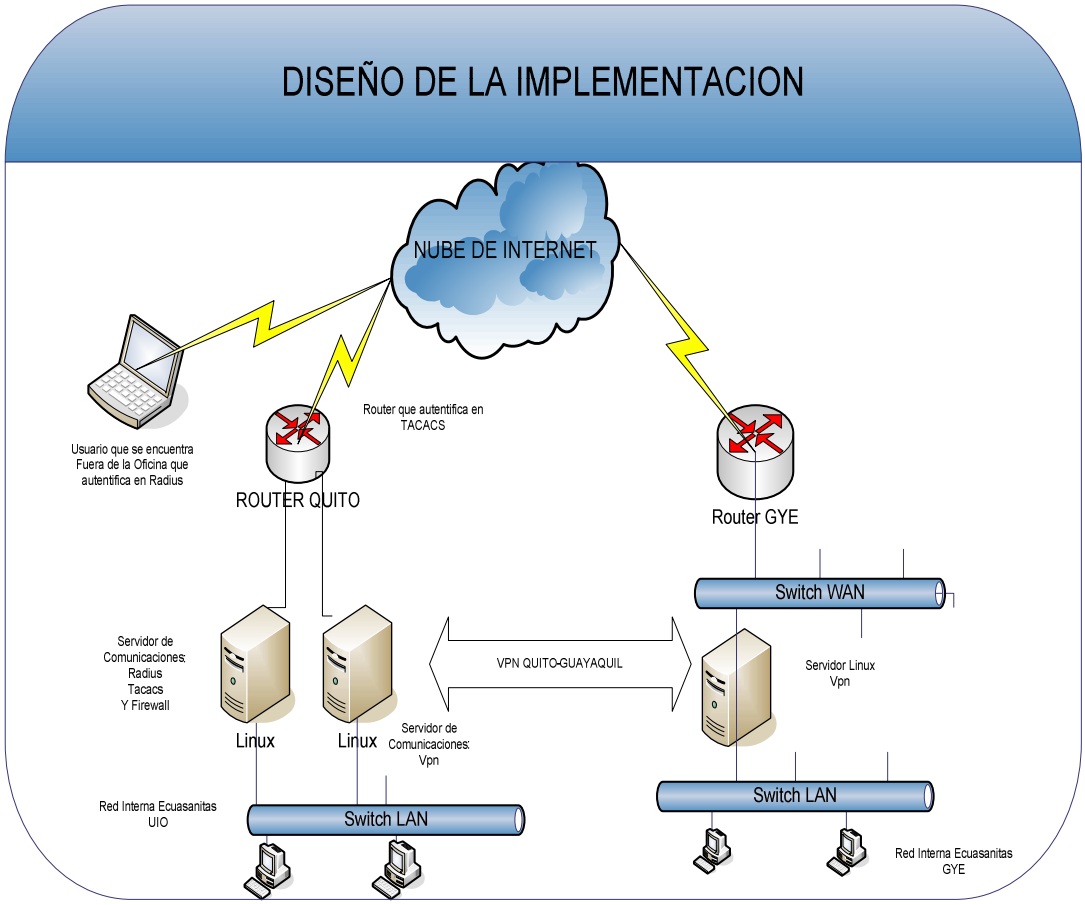

GRAFICO3. 1 DISEÑO DE LA IMPLEMENTACION

3.1 ESQUEMA Y DEFINICION DE POLITICAS DE SEGURIDAD A DESARROLLARSE

En vista de que el presente proyecto esta enfocado en realizar un diseño de medios seguros para el ingreso a la red de datos de la organización, es conveniente establecer reglas de seguridad, las cuales serán diseñadas específicamente para verificar y controlar el acceso a Internet para todos los usuarios internos de la red de Ecuasanitas.
Las reglas a definirse son:

- Control de Acceso a páginas Web (Navegación)
- Control de Búsqueda en el Internet
- Bloqueo de Redes Peer to Peer, tales como Kassa, Morfeo, etc.

Los controles se los realizará con la herramienta Squid, la cual será instalada en el servidor con sistema operativo Fedora Core 3.

3.1.1 RECOMENDACIONES BASICAS PARA LOS USUARIOS DE LA RED

- Los Administradores de Red, deben actualizar en forma permanente los últimos parches de los sistemas operativos a todas las estaciones de trabajo de los usuarios internos de la red en tareas programadas en cada computador.

- Se debe actualizar todas las semanas los registros de definiciones de los antivirus y si es posible diariamente.

- Las claves de los accesos no deben estar asociadas a datos comunes del usuario como la fecha de nacimiento, el nombre, apelativos, etc.
- Cambiar la clave de acceso por lo menos cada 60 días. Aunque lo recomendable es hacerlo mensualmente.

- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos.

- El administrador de la red, deben verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.

- No instalar software pirata. Además de transgredir con la ley, pueden contener virus, Spyware o archivos de sistemas incompatibles con el del usuario.

En conclusión, las reglas a desarrollarse en el proyecto están enfocadas estrictamente al uso y acceso al Internet, por parte de los usuarios autorizados internamente al ingreso a este medio, se ha enfocado el diseño de reglas para el acceso a Internet, debido a que es un medio vulnerable y no confiable.

POLITICA	OBJETIVO	NORMAS A CUBRIR	PROCEDIMIENTO
Control de acceso a las Páginas Web	Monitorear y permitir el acceso al Internet para el uso de páginas que sean relacionadas con el negocio de la empresa por ejemplo: Entidades Bancarias, búsqueda de información relativa a Empresas de medicina prepagada, y todo lo relacionado con Sistemas de informática.	El usuario debe usar el Internet y paginas Web exclusivamente para el uso de trabajos relacionados con la empresa.	Controlar el acceso en el servidor Proxy determinando las reglas y accesos para cada departamento y/o usuario.
Control de búsqueda en el Internet.	Controlar la búsqueda al personal que tenga el acceso al Internet y sea usado para fines de la empresa	El administrador de la red debe determinar por departamento y usuario las necesidades de acceso y búsqueda de información en el Internet.	El administrador de la red clasificará por departamento y/o usuario. Determinará por cada departamento el tipo de búsqueda permitida. Controlará por usuario el tiempo y uso de la información en el Internet.
Control de de tráfico de entrada y salida al Internet.	Controlar el tráfico tanto de entrada y de salida desde el servidor de Ecuasanitas hacia el Internet, para de esta manera optimizar el uso de banda ancha y evitar el uso de trafico P2P.	El administrador de la red debe determinar las aplicaciones del uso de Internet tanto de entrada como de salida.	Generar las reglas respectivas y necesarias tanto de entrada como de salida al Internet con el uso de reglas en el firewall.
Generar reportes de uso de las páginas Web.	Visualizar por cada usuario el uso y tiempo de utilización de las páginas Web	El administrador de la red debe generar un reporte del uso de páginas Web	Generar reportes semanales por cada usuario del acceso a programas e informaron del Internet.

TABLA3. 1 Descripción de Políticas de Seguridad en el Internet.

3.1.2 CONFIGURACION DE POLITICAS

Las políticas especificadas en el esquema se configuraran con el servicio Squid Versión 2.0 del sistema operativo Linux Fedora Core 2,

3.1.2.1 Configuración de Accesos y Reglas

Instalación y Configuración del Squid.

El squid no se instala de manera predeterminada a menos que se especifique durante la instalación del sistema operativo Linux, pero viene incluido en los cd's de instalación de casi todas las distribuciones actuales. El procedimiento de instalación es exactamente el mismo que con cualquier otro software.

Mount /mnt/cdrom/

rpm –SUV /mnt/cdrom/RPMS/squid-*.i386.rpm

eject

Por diversas cuestiones de seguridad no es recomendable utilizar versiones del kernel anteriores al 2.4.9.

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf.

Parámetros a configurar

- http_port
- cache_mem
- cache_dir
- Listas de control de acceso
- Reglas de control de acceso
- httpd_accel_host
- httpd_accel_port
- httpd_accel_with_proxy

Squid por defecto utiliza el puerto 3128 para atender peticiones.

Default: http_port 3128

http_port 3128

El parámetro cache _mem establece la cantidad ideal de memoria para especificar:

- Objetos en transito
- Objetos Hot
- Objetos negativamente almacenados en el caché

Los datos de estos objetos se almacenan en bloques de 4 kb. El parámetro cache_mem especifica un limite máximo en el tamaño total de bloques acomodados, donde los objetos en transito tienen mayor prioridad. Sin embargo los objetos Hot y aquellos negativamente almacenados en el caché podrán utilizar la memoria no utilizada hasta que sea requerida.

Por defecto se establecen 8MB, pero en este caso se establecerá 64MB por las necesidades requeridas de la configuración.

cache_mem 64 MB

El parámetro cache_dir, se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. Esto significa cuanto se desea almacenar de Internet en el disco duro, por tanto la configuración requerida es la siguiente:

cache_dir ufs /cache 4000 16 256

Se ha especificado 4000 MB en el caché de esta manera se almacenarán en este ya que entre mas grande sea el caché se utiliza menos ancho de banda.

Los números 16 y 256 significan que el directorio del caché contendrá 16 subdirectorios con 256 niveles cada uno.

auth_param basic children 5

auth_param basic realm Squid proxy-caching web server

auth_param basic credentialsttl 2 hours

refresh_pattern ^ftp:	1440	20%	10080
refresh_pattern ^gopher:	1440	0%	1440
refresh_pattern.	0	20%	4320

Listas de control de Acceso: definición de la red completa

Configuración recomendada

acl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT

Reglas de control de acceso: Acceso a una lista de Control de Acceso.

Estas definen si se permite ó no el acceso al Squid. Se aplican a las listas de Control de Acceso.

http_access allow localhost

Definición de la lista de páginas a las cuales los usuarios no podrán acceder.

acl paginas_deny url_regex "/etc/squid/blacklists"
http_access deny paginas_deny

Definición de la lista de usuarios permitidos a la navegación.

acl permitidos src "/etc/squid/permitidos"
http_access allow permitidos

Definición de la lista de páginas a las cuales los usuarios podrán acceder

acl paginas_allow url_regex "/etc/squid/whitelists"
http_access allow paginas_allow
http_access deny all !paginas_allow

El parámetro http_reply_access permite hacer una replica de las peticiones de los clientes.

http_reply_access allow all

El parámetro icp_access , permite o deniega acceso al Puerto ICP que se basa en al lista de acceso.

#Default:

icp_access allow all

Cache con Aceleración

Cuando un usuario hace una petición hacia un objeto en Internet, este es almacenado en el cache del Squid. Por lo tanto si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificaciones alguna desde que accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en vez de volver a descargarlo desde Internet lo que permite navegar más rápido y optimiza la utilización de ancho de banda.

HTTPD-ACCELERATOR OPTIONS

httpd_accel_host 192.168.0.200

httpd_accel_port 80

httpd_accel_with_proxy on

httpd_accel_uses_host_header on

3.1.3 CONFIGURACION DE REPORTEADOR.

Los reportes son muy importantes ya que se puede hacer un seguimiento de lo que realizan los usuarios dentro de los accesos permitidos al Internet.

Los reportes serán generados con el software sarg.

Instalación del Software

rpm –ivh sarg-2.0.7-1.fc2.mack.i386.rpm

Sarg utiliza el fichero de configuración localizado en /etc/sarg/sarg.conf.

Parámetro access_log file, indica en donde se guarda los log del los accesos de los usuarios.

TAG: access_log file

Where is the access.log file

sarg -l file

#access_log /usr/local/squid/var/logs/access.log

access_log /var/log/squid/access.log

Parámetro output_dir, indica en el directorio en donde se guardan los reportes.

TAG: output_dir

The reports will be saved in that directory

sarg -o dir

#

#output_dir /var/www/html/squid-reports

output_dir /var/www/sarg/ONE-SHOT

Parámetro resolve_ip yes/no, convierte la dirección ip en un nombre de dirección www.

TAG: resolve_ip yes/no

Convert ip address to dns name

sarg -n

#resolve_ip no

resolve_ip yes

Parámetro mail_utility mail|mailx, se usa para enviar un mail de los reporte vía SMTP.

TAG: mail_utility mail|mailx

Mail command to use to send reports via SMTP

#

#mail_utility mailx

mail_utility mail

Parámetro max_elapsed milliseconds, indica el tiempo de uso

TAG: max_elapsed milliseconds

If elapsed time is recorded in log is greater than max_elapsed use 0 for #elapsed time.

Use 0 for no checking

#max_elapsed 0

8 Hours

max_elapsed 28800000

Parámetro show_successful_message yes|no, indica si el reporte generado fue procesado satisfactoriamente.

TAG: show_successful_message yes|no

Shows "Successful report generated on dir" at end of process.

#show_successful_message yes

show_successful_message no

3.2 CONFIGURACION DEL FIREWALL

Se realizó la configuración del firewall a nivel de software, en la instalación del sistema operativo se define si se desea o no activar este servicio o caso contrario se lo puede realizar manualmente.

service iptables start

El firewall utiliza el fichero de configuración localizado en /etc/sysconfig/firewall

Inicializando configuración de Firewall

#IPTABLES='/sbin/iptables'

 # Definiciones de Red

ALL='0.0.0.0/0'

DHCPTARGET='255.255.255.255/24'

ETH0='10.0.0.243/32'

ETH0_NET='10.0.0240/255.255.255.248'

GATEWAY='10.0.0.241/32'

ETH1='192.168.250.225/32'

ETH1_NET='192.168.250.0/255.255.0.0'

LO='127.0.0.1/32'

LO_NET='127.0.0.1/255.0.0.0'

#--

Permitiendo FORWARDING para direcciones dinámicas.

#--

```
# Modulo que se activa para que funciona el forwardeo de paquetes
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv4/ip_dynaddr
#------------------------
# Control  anti-spoofing.
#------------------------
# Elimina el spoffing
for file in /proc/sys/net/ipv4/conf/*/rp_filter; do
  echo 1 > $file
done
#-----------------------------------------------------
# REGLA DE REDIRECT PARA HABILITAR PROXY Y FTP TRANSPARENTE.
#-----------------------------------------------------

$IPTABLES -t nat -A PREROUTING -p tcp --dport 80 -s $ETH1_NET -d $ALL -j
REDIRECT --to-port 3128

# Input/Forward/Output REGLAS DE FIREWALL

$IPTABLES -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
$IPTABLES -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
$IPTABLES -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# REGLA 100 [ ALL ALL tcp backorifice DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport backorifice -j DROP
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport backorifice -j DROP
#
# REGLA 200 [ ALL ALL udp backorifice DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport backorifice -j DROP
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport backorifice -j DROP
```

```
#
# REGLA 300 [ ALL ALL tcp netbus DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport netbus -j DROP
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport netbus -j DROP
#
# REGLA 400 [ ALL ALL udp netbus DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport netbus -j DROP
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport netbus -j DROP
#
# REGLA 500 [ ALL ALL tcp netbus2 DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport netbus2 -j DROP
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport netbus2 -j DROP
#
# REGLA 600 [ ALL ALL udp netbus2 DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport netbus2 -j DROP
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport netbus2 -j DROP
#
# REGLA 700 [ ALL ALL tcp netbus3 DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport netbus3 -j DROP
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport netbus3 -j DROP
#
# REGLA 800 [ ALL ALL udp netbus3 DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport netbus3 -j DROP
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport netbus3 -j DROP
#
# REGLA 900 DNS UDP -TCP [ ALL ALL tcp-udp domain ACCEPT NO IN/FWD
]
#
```

```
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport domain -j ACCEPT
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport domain -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport domain -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport domain -j ACCEPT
#
# REGLA 910 SMTP UDP -TCP [ ALL ALL tcp-udp smtp ACCEPT NO IN/FWD
]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport smtp -j ACCEPT
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport smtp -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport smtp -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport smtp -j ACCEPT
#
# REGLA 920 POP3 UDP -TCP [ ALL ALL tcp-udp pop3 ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport pop3 -j ACCEPT
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport pop3 -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport pop3 -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport pop3 -j ACCEPT
#
# REGLA 930 PPTP UDP -TCP [ ALL ALL tcp-udp pptp ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $ALL --dport 1723 -j ACCEPT
$IPTABLES -A FORWARD  -p udp -s $ALL -d $ALL --dport 1723 -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport 1723 -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport 1723 -j ACCEPT
#
# REGLA 930 HTTP  UDP -TCP [ ALL ALL tcp-udp http ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ALL --dport http -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ALL --dport http -j ACCEPT
#
# REGLA 940 SQUID  UDP -TCP [ ALL ALL tcp-udp squid ACCEPT NO
IN/FWD ]
```

```
#
$IPTABLES -A INPUT  -p tcp -s $ACCESSRAM -d $ETH0 --dport squid -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ETH1_NET -d $ETH0 --dport squid -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ETH1_NET -d $ETH0 --dport squid -j ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ETH1_NET -d $ETH1 --dport squid -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ETH1_NET -d $ETH1 --dport squid -j ACCEPT
#
# REGLA 950 TELNET-FTP  tcp-udp  [ ALL ALL tcp-udp ACCEPT NO IN/FWD ]
#
# REGLA 3200: NIEGA COMPLETAMENTE EL PING CON DETERMINADOS REQUERIMIENTOS NO ESPECIFICADOS [ ALL ALL icmp ALL DENY YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL -d $ALL -j DROP
$IPTABLES -A FORWARD  -p icmp -s $ALL -d $ALL -j DROP
```

 # Default Rules

```
# Default FORWARD policy: log and drop.
$IPTABLES -A FORWARD -j LOG --log-prefix 'FORWARD Policy [DROP]:'
$IPTABLES -P FORWARD DROP
#
# Default OUTPUT policy: accept.
#
$IPTABLES -P OUTPUT ACCEPT
#
# Default INPUT policy: log and drop.
#
$IPTABLES -A INPUT -j LOG --log-prefix 'INPUT Policy [DROP]:'
```

$IPTABLES -P INPUT DROP

3.3 CONFIGURACION DE VPN

Se realiza la configuración de la VPN con túneles ip_gree y se utilaza como protocolo de conexión el PPTP.
Los archivos de configuración tanto en el servidor de Guayaquil como en Quito se ubican en el /etc/rc/rc.local
Básicamente se trata de unir las dos redes locales usando una interfaz de red virtual que se va a crear.

En cada extremo se cera un interfaz de túnel. Este interfaz es punto a punto, debe especificarse la IP publica remota a la que se va a conectar y la IP privadas de cada punto una vez direccionadas las interfaces se pueden ingresar rutas par hacer que las distintas redes se vean a través de estos túneles.

En Quito se tendría el túnel de la siguiente manera:
La red local es la 192.168.250.0 y se desea llegar a la 192.168.0.0 a través del túnel.
modprobe ip_gre
/sbin/iptunnel add gre1 mode gre remote 10.0.10.14 local 10.0.10.70 dev eth0
/sbin/ifconfig gre1 10.0.0.1 netmask 255.255.255.252 up
/sbin/route add -net 192.168.0.0 netmask 255.255.255.0 gw 10.0.0.2
En donde la dirección 10.0.0.14 es la dirección pública del servidor de Guayaquil y la dirección pública de Quito es la 10.0.0.70 creadas en la interfaz eth0
Se debe añadir una ruta con la dirección privada del servidor remoto.
En el lado de Guayaquil la red local es la 192.168.0.0 y se desea llegar a la 192.168.250.0
/sbin/depmod -a
/sbin/modprobe ipt_REDIRECT
/sbin/modprobe ipt_MASQUERADE
/sbin/modprobe ipt_multiport

```
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_nat_irc
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -d  ! 192.168.250.0/24 -j MASQUERADE
iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 80  -j REDIRECT --to-port 8080

############### TUNEL A GUAYAQUIL

modprobe ip_gre
ip tunnel add TUNA mode gre remote 10.0.236.70 local 10.0.245.14
ip link set TUNA up
ip addr add 10.0.0.2/30 dev TUNA
ip route add 192.168.250.0/24 dev TUNA
```

El protocolo GRE utliza el puerto 47 el cual se debe abrir en el Router y en el firewall que se tiene configurado en ambos lados.

```
Iptables –A INPUT  –p 47 –j ACCEPT
Iptables –A OUTPUT  -p 47 –j ACCEPT
```

3.4 CONFIGURACION DEL TACACS.

Se realiza la configuración del tacacs para realizar la administración de routers
El archivo de configuración se ubica en el /etc/tacacs/tac_plus.conf
Definición de la clave del router
key = XXXX

Autentificación del usuario administrador en el servidor tacacs

```
# Use /etc/shadow file to do authentication
default authentication = file /etc/shadow
# Where is the accounting records to go
```

```
accounting file = /var/log/tac_acc.log
#All services are alowed..
user = DEFAULT {
   default service = permit
}
user = poli {
   default service = permit
   login = cleartext "XXX"
   name = "poli-tes"
   service = exec {
        default attribute = permit
}
}
```

3.4.1 CONFIGURACION DE ROUTER

El router que se configura es el Cisco series 800

El nivel de privilegio del usuario se le asignó un nivel 15 es un nivel con los privilegios de configuración.

Inicialización del Tacacs+ en el router

```
Starting TACACS+ :                              [  OK  ]
#########################
```

Autentificación vía telnet desde el equipo

```
#########################

[root@xserver tacacs]# telnet 192.168.250.253
Trying 192.38.250.253...
Connected to 192.168.250.253.
Escape character is '^]'.
User Access Verification
Username: poli
Password:
Ecuasanitas>ena
Password:
```

Ecuasanitas#sh conf
Using 1440 out of 131072 bytes
!
version 12.2 (Version del Route)
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Ecuasanitas
!
logging rate-limit console 10 except errors
##
Activación de autentificación con tacacs+
##
aaa new-model
!
!
###
Activación del grupo default que sea con tacacs+ #
 # caso contrario se activa el backup del equipo #
###
aaa authentication login default group tacacs+ local
###
Activacion de password de administrador del router
###
enable secret 5 1VEi6$yPW2bZ1orO4N8fv7ohXqs/
enable password cisco
!
###
##
Usuario de respaldo del router si el tacas+ esta dado de baja

```
##################################################################
##
username backup privilege 15 password 0 backup
ip subnet-zero
!
no ip dhcp-client network-discovery
lcp max-session-starts 0
!
interface Ethernet0
ip address 192.68.250.253 255.255.255.0
hold-queue 32 in
!
interface ATM0
no ip address
no atm ilmi-keepalive
 dsl equipment-type CPE
 dsl operating-mode GSHDSL symmetric annex A
 dsl linerate AUTO
!
interface ATM0.1 point-to-point
description ACCESS
ip address 172.16.82.10 255.255.255.252
pvc 0/32
vbr-nrt 79 79
encapsulation aal5snap
 !
interface ATM0.11 multipoint
description ADMINISTRACION
ip address 172.17.1.32 255.255.255.0
pvc 11/1
ubr 64
encapsulation aal5snap
 !
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.82.9
ip http server
!
tacacs-server host 192.168.250.225  Direcion ip del servidor de Tacacs+
tacacs-server key xxxx
snmp-server community sangatsu RO
snmp-server location Office EcuaSanitas, Quito
snmp-server contact Teleholding Quito, hmitsch@teleholding.com
#########################################################################
###
# Configuración de autenticación vía consola del router          #
#########################################################################
###
line con 0
password xxxxx
transport input none
stopbits 1
#########################################################################
###
# Configuración de autenticación para telnet del router          #
#########################################################################
###
line vty 0 4
login authentication default
password xxxxx
!
scheduler max-task-time 5000
end
```

3.5 CONFIGURACION DE RADIUS.

Se configuró el Freeradius un software desarrollado para la autenticación de usuarios vía dial up.

Instalación del FreeRadius

Tar -zxvf freeradius.tar.gz

Los archivos de configuración se ubican en /etc/raddb

Los archivos configurados son:

USER

/etc/raddb/user

En este archivo se define el usuario y el grupo que van a tener acceso desde un equipo conectado a una línea dial up, y se especifica el tipo de conexión, este caso es con el protocolo PPP que requiere conexión tipo CHAP

```
##############################################3
# configuracion radius pptp
##############################################
DEFAULT       Group == "tesis", Auth-Type := Accept
DEFAULT Framed-Protocol == PPP
                Framed-Protocol = PPP,
        Framed-Compression = Van-Jacobson-TCP-IP
```

RADIUSCLIENT

/etc/radiusclient

Es requerido para la conexión con el pppd.

```
auth_order      radius,local
login_tries          4
login_timeout  60
nologin /etc/nologin
issue              /etc/radiusclient/issue
authserver      localhost
acctserver      localhost
servers /etc/radiusclient/servers
dictionary  /etc/radiusclient/dictionary
login_radius    /usr/sbin/login.radius
seqfile             /var/run/radius.seq
mapfile /etc/radiusclient/port-id-map
default_realm
```

radius_timeout 10
radius_retries 3
login_local /bin/login

DICCIONARIO

/etc/radiusclient/dictionary

Este archivo contiene las traducciones del diccionario que analiza las demandas y contestaciones generadas por el cliente y el servidor.

ATTRIBUTE	User-Name	1	string	
ATTRIBUTE	Password		2	string
ATTRIBUTE	CHAP-Password		3	string
ATTRIBUTE	NAS-IP-Address		4	ipaddr
ATTRIBUTE	NAS-Port-Id		5	integer
ATTRIBUTE	Service-Type		6	integer
ATTRIBUTE	Framed-Protocol		7	integer
ATTRIBUTE	Framed-IP-Address		8	ipaddr
ATTRIBUTE	Framed-IP-Netmask		9	ipaddr
ATTRIBUTE	Framed-Routing		10	integer
ATTRIBUTE	Filter-Id		11	string
ATTRIBUTE	Framed-MTU		12	integer
ATTRIBUTE	Framed-Compression		13	integer
ATTRIBUTE	Login-IP-Host		14	ipaddr
ATTRIBUTE	Login-Service		15	integer
ATTRIBUTE	Login-TCP-Port		16	integer
ATTRIBUTE	Reply-Message		18	string
ATTRIBUTE	Callback-Number	19	string	
ATTRIBUTE	Callback-Id		20	string
ATTRIBUTE	Framed-Route		22	string
ATTRIBUTE	Framed-IPX-Network		23	ipaddr
ATTRIBUTE	State		24	string
ATTRIBUTE	Session-Timeout		27	integer
ATTRIBUTE	Idle-Timeout		28	integer
ATTRIBUTE	Termination-Action		29	integer
ATTRIBUTE	Called-Station-Id		30	string

ATTRIBUTE Calling-Station-Id 31 string
ATTRIBUTE Acct-Status-Type 40 integer
ATTRIBUTE Acct-Delay-Time 41 integer
ATTRIBUTE Acct-Input-Octets 42 integer
ATTRIBUTE Acct-Output-Octets 43 integer
ATTRIBUTE Acct-Session-Id 44 string
ATTRIBUTE Acct-Authentic 45 integer
ATTRIBUTE Acct-Session-Time 46 integer
ATTRIBUTE Acct-Terminate-Cause 49 integer
ATTRIBUTE NAS-Port-Type 61 integer
ATTRIBUTE Port-Limit 62 integer
ATTRIBUTE Connect-Info 77 string

/etc/radiusclient/servers

Este archivo contiene la clave del servidor radius

localhost xxxxxxxx
xserver.ecuasanitas.com.ec xxxxxxxx

/etc/raddb/client.conf

Contiene las entradas correspondientes para le servidor de radius (/etc/radiusclient/servers para los clientes NAS.

localhost xxxxxxxx
xserver.ecuasanitas.com.ec xxxxxxxx

3.5.1 CONFIGURACION DEL PPP

Se configura el chap para la autenticación del usuario y el password

/etc/ppp/chap-secret

Archivo en donde se guardan los usuarios y las claves.

Los asteriscos significan que permita el ingreso de todos.

* * * *
#sojeda pptpd sojeda*

/etc/ppp/options

El cliente recibe las direcciones ip remotas asignadas en el radius

Nombre del sistema local para autentificar los usuarios del chap-secrets
name pptpd
Se define el tipo de encriptación que se va usar
ppp_mppe.o
require-chap
Especificación de los DNS internos de la red
ms-dns 192.168.200.1
ms-dns 10.0.0.2

Habilitación para revisar los log cuando se envía una petición el pppd
debug
Configuración del seteo del cliente de radius.
plugin radius.so

/etc/ppp/pppoe-server-options

Configuración del servidor PPP
require-chap
login
lcp-echo-interval 10
lcp-echo-failure 2
ms-dns 192.168.200.1
ms-dns 10.0.0.2
plugin radius.so
plugin radattr.so

/etc/ppp/pptpd

Se configura las direcciones IP local del servidor y las direcciones remotas que se asignan a los clientes radius.
option /etc/ppp/options.pptpd
debug
logwtmp
proxyarp
localip 192.168.250.225
remoteip 192.168.250.249,192.168.250.250

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

- Las estaciones de Windows 95 y 98 son de alto riesgo ya que no tienen las propiedades para la configuración de las seguridades pertinentes, para la compartición de archivos dentro de la red.

- El hecho de utilizar código libre como Linux es que se puede modificar el código de acuerdo a nuestra conveniencia y necesidad, la desventaja es el mantenimiento y soporte técnico ya que es costoso, por otra parte la inestabilidad de algunas versiones por ende siempre hay que estar actualizando las versiones y buscar constantemente los parches de seguridad para los servicios que se goza de este sistema operativo.

- Es más óptima la encriptación a nivel de antenas de los enlaces de radios ya que influye en un 15% en overhead de 10k bajo el enlace.

- Las definiciones acertadas en la configuración del Squid ayuda a optimizar la utilización del disco del equipo y el ancho de banda de la red.

- La creación del Servidor Tacacs+, permitirá en un futuro la administración de los Routers a nivel nacional, y de esta forma el administrador de la red tendría un mejor manejo de los routers.

- La creación del Servidor Radius, permitirá el acceso vía modem desde cualquier parte del país a los usuarios de la red.

- Para una mejor administración de los servidores sería recomendable la colocación de los mismos en pisos intermedios ya que así se podría mejorar la seguridad de los mismos.

- Es recomendable la actualización de los sistemas operativos Windows 95 y 98 al sistema operativo XP para un mejor control de seguridades a nivel de comparticion de recursos en la red.

- Se recomienda la actualización del sistema operativo Red hat a otros como fedora que en la actualidad tienen en el mercado un buen soporte y existen en el Internet constantemente actualizaciones de parches para varios productos que se corren bajo este sistema operativo.

- El Squid es servidor Proxy muy confiable, robusto y con las facilidades necesarias para realizar las configuraciones que se requieren.

- Se recomienda realizar un chequeo constante del uso de Internet, uso de ancho de banda para mejorar el rendimiento de la red.

- Con el uso de la VPN se tendrá un acceso seguro y se funden dos redes diferentes como que parezcan una sola.

- Los costos de implementación de los servicios que se han estudiado en este proyecto dentro del mercado son altos.

BIBLIOGRAFIA

Orinoco Or manager User´s Guide for Outdoor Router 1000/1100

www.hospedajesydominios.com

www.deltaasesores.com

www.tiservinet.es/Recursos/CertificadosDigitales

www. Htmlweb.net

www.cyberpirata.org

www.adslayuda.com/Zyxel650+file-21.html

www.untruth.org/~josh/security/radius/radius-auth.html

www.ciscoredaccionvirtual.com/redaccion

www.blacksheepnetworks.com

http://linuca.org/body.phtml?nIdNoticia=281

www.arsenet.com

www.terra.es

http://nernet.unex.es/~miguel/pdfs/teoria_comunicaciones/Tema4.pdf

www.monografias.com/trabajos12/monvpn/monvpn.shtml

www.cisco.com/warp/public/44/solutions/network/vpn.shtml

www.iec.csic.es/criptonomicon/comercio/ssl.html

www.buanzo.com.ar/sec/rincon_squid.html

http://es.tldp.org/Tutoriales/doc-servir-web-escuela

www.certificadodigital.com.ar/frameset_serv.htm

http://web.uservers.net/soporte/docview.php

www.monografias .com

ANEXOS

ANEXO 1

PROCESO DE AUTENTICACION DEL RADIUS.

PROCESO INICIAL DEL CLIENTE.-

El cliente crea un paquete de Radius de Acceso-Petición, que incluye el usuario-nombre y atributos del Usuario-contraseña, en donde el campo del identificador del paquete del Acceso-Petición es generado por el cliente, el proceso de la generación para el campo del identificador no es especificado por el Protocolo Radius, pero se lleva a cabo como un contador que se incrementa en cada demanda.

El paquete del Acceso-Petición contiene 16 octetos en el campo del autentificador. El autenticador de la Petición se escoge al azar un string de 16 octetos.
Este paquete es completamente desprotegido, excepto por los atributos del Usuario-Password, los cuales son protegidos de la siguiente forma:

El cliente y el servidor comparten un secreto. El secreto compartido es seguido por la petición que se autentica a través del MD5 el cual crea un valor de 16 octetos que es XORed con la contraseña que ingresa el usuario. Si la contraseña del usuario es mayor que 16 octetos, se realizan los cálculos de MD5 adicionales usando el ciphertex anterior en lugar del Autenticador de la petición

ANEXO 2

PROTOCOLO DE LA VPN L2TP

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre el LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es un conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extreme de la conexión L2TP y es el otro para el LAC. El LNS es la terminación lógica de una sesión PPP que esta siendo puesta en un túnel desde el sistema remoto por el LAC.

Un Cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

En el L2TP el encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701.

ANEXO 3

REGLAS DE CONFIGURACION DEL FIREWALL

```
#--------------------
# Flush all rulesets.
#--------------------
# Elimina toda clase de configuracio de iptables Ej: firewall por default de linux
$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD
$IPTABLES -X

#---------------------------------
# Permitir a al interface loopback
#---------------------------------
# Permite conexion de la red 127.0.0.0/0 que es una ip interna propio del
equipo
$IPTABLES -A INPUT -i lo -s $ALL -d $ALL -j ACCEPT
$IPTABLES -A OUTPUT -o lo -s $ALL -d $ALL -j ACCEPT

#########################################################################
###############
# INGRESO DE REGLAS
#########################################################################
###############
# bloquea todo el trafico
$IPTABLES -t filter -P FORWARD DROP

#---------------------------------------
# REGLAS DE FORWARDING RED 192.168.0.0/16
#---------------------------------------
$IPTABLES -t filter -A FORWARD -d $ALL -s $ETH1_NET -j ACCEPT
$IPTABLES -t filter -A FORWARD -d $ETH1_NET -j ACCEPT

#---------------------------------------
```

```
# ENMASCARAMIENTO RED 192.168.0.0/16
#----------------------------------------
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 80 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 443 -s $ETH1_NET -d
$ALL -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 20 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 21 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 53 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p udp --dport 53 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 25 -s $ETH1_NET -d $ALL
-j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 1863 -s $ETH1_NET -d
$ALL -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 110 -s $ETH1_NET -d
$ALL -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 5190 -s $ETH1_NET -d
$ALL -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p tcp --dport 1900 -s $ETH1_NET -d
$ALL -j MASQUERADE
$IPTABLES -t nat -A POSTROUTING -p icmp -s $ETH1_NET -d $ALL -j
MASQUERADE
$IPTABLES -A INPUT  -p tcp -s $ACCESSRAM -d $ETH0 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p udp -s $ACCESSRAM -d $ETH0 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ETH0_NET -d $ETH0 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p udp -s $ETH0_NET -d $ETH0 --dport 21:23 -j
ACCEPT
```

```
$IPTABLES -A INPUT  -p tcp -s $ETH1_NET -d $ETH0 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p udp -s $ETH1_NET -d $ETH0 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ETH1_NET -d $ETH1 --dport 21:23 -j
ACCEPT
$IPTABLES -A INPUT  -p udp -s $ETH1_NET -d $ETH1 --dport 21:23 -j
ACCEPT
# REGLA 960 WEBMIN  TCP [ ALL ALL tcp-udp webmin ACCEPT NO IN/FWD
]
#
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ETH0 --dport webmin -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ETH0 --dport webmin -j
ACCEPT
$IPTABLES -A INPUT  -p tcp -s $ALL -d $ETH1 --dport webmin -j ACCEPT
$IPTABLES -A FORWARD  -p tcp -s $ALL -d $ETH1 --dport webmin -j
ACCEPT
#
# REGLA 100O BROADCAST [ ALL DHCPTARGET udp bootps ACCEPT NO
IN ]
#
$IPTABLES -A INPUT  -p udp -s $ALL -d $DHCPTARGET --dport bootps -j
ACCEPT
#
# REGLA 1100 [ ALL ALL icmp echo-reply ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type echo-reply -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type echo-reply -d $ALL -j
ACCEPT
#
# REGLA 1200 [ ALL ALL icmp destination-unreachable ACCEPT NO IN/FWD ]
#
```

```
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type destination-unreachable -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type destination-
unreachable -d $ALL -j ACCEPT
#
# REGLA 1300 [ ALL ALL icmp network-unreachable ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type network-unreachable -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type network-unreachable -
d $ALL -j ACCEPT
#
# REGLA 1400 [ ALL ALL icmp host-unreachable ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type host-unreachable -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type host-unreachable -d
$ALL -j ACCEPT
#
# REGLA 1500 [ ALL ALL icmp protocol-unreachable ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type protocol-unreachable -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type protocol-unreachable -
d $ALL -j ACCEPT
#
# REGLA 1600 [ ALL ALL icmp port-unreachable ACCEPT NO IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type port-unreachable -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type port-unreachable -d
$ALL -j ACCEPT
#
# REGLA 1700 [ ALL ALL icmp source-route-failed ACCEPT YES  IN/FWD ]
```

```
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type source-route-failed -d $ALL
-j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type source-route-failed -d
$ALL -j ACCEPT
#
# REGLA 1800 [ ALL ALL icmp network-unknown ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type network-unknown -d $ALL -
j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type network-unknown -d
$ALL -j ACCEPT
#
# REGLA 1900 [ ALL ALL icmp host-unknown ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type host-unknown -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type host-unknown -d $ALL
-j ACCEPT
#
# REGLA 2000 [ ALL ALL icmp network-prohibited ACCEPT YES  IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type network-prohibited -d $ALL
-j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type network-prohibited -d
$ALL -j ACCEPT
#
# REGLA 2100 [ ALL ALL icmp host-prohibited ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type host-prohibited -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type host-prohibited -d
$ALL -j ACCEPT
#
```

```
# REGLA 2200 [ ALL ALL icmp TOS-network-unreachable ACCEPT YES
IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type TOS-network-unreachable -
d $ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type TOS-network-
unreachable -d $ALL -j ACCEPT
#
# REGLA 2300 [ ALL ALL icmp TOS-host-unreachable ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type TOS-host-unreachable -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type TOS-host-unreachable
-d $ALL -j ACCEPT
#
# REGLA 2400 [ ALL ALL icmp communication-prohibited ACCEPT YES
IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type communication-prohibited -
d $ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type communication-
prohibited -d $ALL -j ACCEPT
#
# REGLA 2500 [ ALL ALL icmp echo-request ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type echo-request -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type echo-request -d $ALL -
j ACCEPT
#
# REGLA 2600 [ ALL ALL icmp time-exceeded ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type time-exceeded -d $ALL -j
ACCEPT
```

```
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type time-exceeded -d
$ALL -j ACCEPT
#
# REGLA 2700 [ ALL ALL icmp ttl-zero-during-transit ACCEPT YES IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type ttl-zero-during-transit -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type ttl-zero-during-transit -
d $ALL -j ACCEPT
#
# REGLA 2800 [ ALL ALL icmp ttl-zero-during-reassembly ACCEPT YES
IN/FWD ]
#
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type ttl-zero-during-reassembly -
d $ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type ttl-zero-during-
reassembly -d $ALL -j ACCEPT
# REGLA 2900 [ ALL ALL icmp parameter-problem ACCEPT YES IN/FWD ]
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type parameter-problem -d $ALL
-j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type parameter-problem -d
$ALL -j ACCEPT
# REGLA 3000 [ ALL ALL icmp ip-header-bad ACCEPT YES IN/FWD ]
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type ip-header-bad -d $ALL -j
ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type ip-header-bad -d $ALL
-j ACCEPT
# REGLA 3100 [ ALL ALL icmp required-option-missing ACCEPT YES IN/FWD
$IPTABLES -A INPUT  -p icmp -s $ALL --icmp-type required-option-missing -d
$ALL -j ACCEPT
$IPTABLES -A FORWARD  -p icmp -s $ALL --icmp-type required-option-
missing -d $ALL -j ACCEPT
```