Capítulo 3

ANALISIS DE PLATAFORMAS PARA EL PROVEEDOR DE SERVICIO DE INTERNET

3.1. Selección de Sistemas Operativos

En este capítulo se conocerán los Sistemas Operativos que podrían ser usados por cualquier Proveedor de Servicio de Internet al final del capítulo se dará la recomendación sobre el Sistema Operativo y el tipo de conexión con el cliente a usarse.

3.1.1. Clases y Análisis Sistemas Operativos

Entre las clases más conocidas de los sistemas operativos se encuentran los siguientes:

- Linux
- OS/2
- Solaris
- Windows

Para su mejor entendimiento a continuación están dos cuadros uno comparativos y el otro de características de los Sistemas Operativos, los mismos que ayudarán para un buen entendimiento y evaluación.

Sistema Operativo	Windows XP	Windows 2000	Mac OS	SUSE Linux	Open BSD	Solaris
Creador	Microsoft	Microsoft	Apple	SUSE	Theo de Raadt	Sun
Año de primera distribución	2001	2000	1984	1994	?	?
Aspectos Generales						
Versión estable	SP2	SP4	9.2	9.1	3.5	10
Licencia	Propietario	Propietario	Propietario	GPL	BSD	Propietario Parcialmente software libre
Tipo de usuario	Equipos para hogar y negocios	Equipos para negocios	Artistas, , Diseñadores, Casa	Hogar	Servidores	Servidores, negocios
Aspectos Técnicos						
Tipo de kernel	Microkernel	Microkernel	Ninguno/Microkernel	Monolítico	Monolítico	Monolítico
Sistema de archivos por defecto	NTFS	NTFS/FAT32	HFS/HFS+	?	Berkeley FFS	Incorporado
Soporte de sistemas de archivo de 16 bits	Si	Si	Si	?	Si	?
Soporte de sistemas de archivo de 32 bits	Si	Si	Si	Si	Si	Si

Herramienta de actualización por defecto	Actualizaciones de Windows	Actualizaciones de Windows	Software de Actualizaciones	?	Fuentes	?
Entorno gráfico[1]	Basado en el kernel	Basado en el kernel	Basado en el kernel	Aplicación: X Window System	Aplicación: X Window System	Aplicación: X Window System
Sistema de ventanas por defecto	Standard Windows	Standard Windows	Macintosh Finder	KDE	N/A	CDE o GNOME
Estilo de **Interfaz gráfica de usuario**	Estilo Luna	Estilo clásico interfase	Platinum	kwin con tema plastik	fvwm	dtwm (con CDE), Metacity con GNOME

Tabla 3.1. Comparación de Sistemas Operativos [1]

[1] www.wikipedia.org

3.1.2. Características de Sistemas Operativos

	Windows 98	Windows NT 4.0	Windows 2000	RedHat Linux 6.2	SuNoS en PC	Linux
Clusterable	No	No	Advanced server y data center: Si	Beowulf Piranha Steeleye	Beowulf	Beowulf
Office Automático?	MS-Office Wordperfect	MS-Office Wordperfect	MS-Office Wordperfect	StarOffice WordPerfect	StarOffice	StarOffice
Fat-16	Si	Si	Si	Si	No	Si
Fat-32	Si	No	Si	Si	No	Si
NTFS	No	Si	Si	Si	No	Si
HPFS	No	Si	Si	Si	No	Si
Sistema Archivo ext2	No	No	No	Si	No	No
Espacio de Dirección	2 Gbytes	2 Gbytes	Advanced Server: 8 GB en el Centro Datos: 64 GB	4 Gbytes en 2.2 y kernel anteriores, pero 64 números enteros del pedacito se apoyan 64 Gbytes en 2.4 kernel	4 Gbytes	Terabytes
SMP	No	Si, 4 CPUs	Si, 8 CPUs en el Centro de Datos, 32 CPUs	Si, 4 CPUs	?	Si, 256 CPUs
Cliente NIS	No	No	?	Si	Si	Si
Servidor NIS	No	No	?	Si	Si	Si
Cliente Kerberos	No	No	No compatible con Unix	Si	Si	Si

Cliente NFS	No	No	Opcional con Servicios para Unix (SFU)	Si	Si	Si
Server NFS	No	No	Opcional con Servicios para Unix (SFU)	Si	Si	Si
Cliente NetBEUI	Si	Si	Si, pero no funciona con version cercana Samba	Si	Si	Si
Server NetBEUI	Si	Si	Si, pero no funciona con version cercana Samba	Si	Si	Si
Seguro	No	No	No	No	No	No
Facil uso con GUI	Si	Si	Si	Si	?	Si
Servidor para la Web	PWS (asosiado con Front Page)	IIS	IIS	Apache	Apache	Apache
Tamaño total de la Instalción				1.7 GBytes		
Lenguaje de encriptación ligado	.bat files	.bat files	.bat files, sh	csh, sh, tcsh, bash, perl, tcl,...	csh, sh, tcsh, perl	csh, sh, tcsh, bash, perl, tcl,...
Escalibidad: Extremo Inferior	Minimo pentium, 32 MBytes RAM	Pentium, 62 MBytes RAM	250 MHz Penitum	Sistemna en Matchbox en Chip del PC. Los libros dicen 4 Mbytes RAM para CPU 80386.		

Escalabilidad: Extremo Superior				2.4 soporta hasta 4 GBytes RAM.SuSE tiene un parche para el 2.2.12 para soportar 4 GBytes. 2.4 talvez soporte 64 GBytes de RAM en ia32!		8 Gbytes RAM
Trabajo del Sistema de Archivo	No	NTFS y HPFS	NTFS y HPFS	Si, ver ReiserFS		

Tabla 3.2. Característica de los Sistemas Operativos[2]

[2] http://www.commercialventvac.com/~jeffs/OS_comparison.html

3.1.3. Sistema Operativo Linux

Para poder entenderlo debemos empezar por conocer su estrecha relación con el sistema operativo UNIX. Esto se debe a que la razón que motivó la creación de Linux fue el deseo de realizar una versión de trabajo UNIX para computadores basados en procesadores Intel o, lo que es lo mismo, para computadores compatibles con IBM PC, que son los que utilizan la mayoría de los usuarios.

Linux puede utilizarse en diferentes plataformas informáticas este fue desarrollado por miles de programadores expertos repartidos por todo el mundo. Con ello se logró que todo ese conocimiento se plasmara en un resultado común para que todos los que desearan utilizarlo, lo hicieran con entera libertad.

3.1.3.1 Fiabilidad / Estabilidad

Linux es un Sistema Operativo robusto y estable, capaz de mantener un funcionamiento correcto y aceptable ante los problemas que pueda provocar una aplicación en concreto.

Permite el arranque, la parada y/o la configuración de todos los servicios sin la necesidad de reiniciar el servidor. Ante la práctica totalidad de los problemas que puedan surgir no será necesario parar el servidor; evitando así que el fallo de una funcionalidad afecte al buen funcionamiento de todas las demás.

3.1.3.2 Rendimiento

El núcleo de Linux puede ser configurado de forma personalizada para cada equipo concreto adaptándose a los componentes hardware específico de cada equipo.

Linux incluye el soporte de protocolos de red a nivel del núcleo del Sistema Operativo.

Estas y otras razones permiten que cada servidor Linux tenga una configuración óptima propia, mejorando considerablemente el rendimiento.

3.1.3.3 Versatilidad

Linux incorpora una larga variedad de aplicaciones que facilitan el completo funcionamiento del servidor de forma eficiente. Por ejemplo:

- Servidor de Correo (entrante y saliente).
- Servidor Web.
- Servidor FTP.
- Servidor para casi la totalidad de las bases de datos (Interbase, Oracle, Informix, DB2, MySQL, ODBC, etc...)

- Sistema para la automatización de tareas (crond)
- Soporte de acceso a sistemas de archivos de: Win95, Win98, WinMe, WinNT, etc...
- Soporte sencillo para la programación de red (sockets)

Otras variedades que tiene Linux es:

- Linux es un Sistema Operativo multiusuario real, permitiendo diferentes usuarios con diferentes permisos y realizando varias sesiones simultáneas en la misma máquina.
- Linux es un Sistema Operativo multipuesto real, permitiendo iniciar sesiones simultáneas desde diferentes máquinas tanto locales como remotas.

Un servidor Linux, por lo tanto, podrá ser administrado remotamente en casi la totalidad de los casos.

3.1.3.4 Comodidad

Permite dar una respuesta cómoda y sencilla a las tareas del día a día, por ejemplo:

- Disponer de un sistema automatizado de copias de seguridad, realizar de forma programada y desasistida, pudiendo ser grabadas directamente a CDROM y/o enviadas automáticamente a diferentes máquinas.
- Acceso a bases de datos a través del Web mediante PHP u otros lenguajes similares.

- Respuesta automática a peticiones realizadas vía e-mail. Pudiendo responder a la propia petición o enviar un correo al responsable que deba tramitarla.

Además, la instalación se la puede realizar ya en modo gráfico y con instalación por defecto que convierte el proceso en algo muy sencillo. Todo ello a través de un entorno gráfico X-Window muy alejado del mito de "UNIX en terminal de texto".

3.1.3.5 Seguridad

Algunos puntos principales para la seguridad son:

- Acceso de usuarios mediante autentificación (nombre de usuario y clave).
- Asignación de diferentes permisos para cada usuario, para cada archivo y para cada proceso en ejecución.
- Soporte de listas de control de acceso (ACL).
- Soporte a nivel del núcleo del Sistema Operativo de filtrado de paquetes (firewall o corta-fuegos), realizándose éste de forma simple e intuitiva.
- Soporte para conexiones de red seguras mediante protocolos de cifrado (SSL).
- Soporte de conexión telnet cifrada (SSH).

- Registro de logs o archivos de bitácora que almacenan información de todas las conexiones y peticiones que se realizan al servidor (/var/log/).
- Disponibilidad de aplicaciones de detección de intrusos (IDS).
- Disponibilidad de aplicaciones para la monitorización del tráfico de red.

Además, hay que tener en cuenta que Linux y la inmensa mayoría de sus aplicaciones se distribuyen con código público, por lo que el descubrimiento y posterior solución de potenciales problemas de seguridad se realiza de forma rápida y continuada.

3.1.3.6 Conclusión

El Sistema Operativo Linux, es muy bueno y sencillo de manejar, todo esto puede ser por el Open Source (Código Abierto), pero a su vez esto puede ser una debilidad, ya que cualquier programador puede revisar y encontrar una falla o puerta de ingreso al sistema. Pero si se usan los parches respectivos será más robusta para ser vulnerada fácilmente.

3.1.4. Sistema Operativo Solaris

3.1.4.1 Características

PORTABILIDAD: El software conformado por una ABI aplicación de interfaces binaria (Application Binary Interface) ejecuta con un Shrink-wrapped (Contracción envuelta) el software en todos los sistemas vendidos con la misma arquitectura del microprocesador. Esto obliga a los desarrolladores de aplicaciones a reducir el costo del desarrollo del software y traer productos al mercado rápidamente, y obliga a los usuarios a actualizar el hardware mientras retienen sus aplicaciones de software y minimizan sus costos de conversión.

ESCALABILIDAD: Las aplicaciones se usan con más frecuencia en el sobre tiempo, y requiere sistemas más poderosos para soportarlos. Para operar en un ambiente creciente, el software debe ser capaz de ejecutar en un rango de ancho poderos y debe ser capaz de tomar ventajas del poder adicional que se está procesando.

INTEROPERATIBIDAD: La estandarización y una clara interface son criterios para un ambiente heterogéneo, permitiendo a los usuarios desarrollar estrategias para comunicarse por medio de su red. El sistema operativo de Solaris puede interoperar con unos sistemas muy populares hoy en el mercado, y aplicaciones que se ejecutan en UNIX se pueden comunicar fácilmente.

COMPATIBILIDAD: La tecnología de la computación continúa avanzando rápidamente, pero necesita permanecer en el ámbito competitivo para minimizar sus costos y maximizar sus ingresos.

3.1.4.2 Herramientas para el Administrador del Sistema

El Sistema Solaris ofrece una variedad de herramientas nuevas para el administrador como lo son:

Dispositivo de Información: para obtener información sobre dispositivos instalados incluyendo nombres, atributos, y accesibilidad.

Sistema de Administración de Archivo: permiten a los administradores crear, copiar, amontonar, depurar, reparar y desmontar sistemas de archivos, crear y remover cadenas de archivos y nombrar tuberías o pipes, y manejar volúmenes.

Manejo del Proceso: esta herramienta ayuda a controlar la agenda de control del sistema. Con esto los administradores pueden generar reportes sobre el desempeño, entrada de identificación, ubicación del acceso a discos, y buscar la manera de afinar el desempeño del sistema.

Usuarios y el manejo del grupo: un administrador puede crear y eliminar entradas en grupos y entradas de identificación del sistema, y asignar grupos e IDs de usuario.

Seguridad: El ASET (Automated Security Enhancement Tool) es una herramienta que incrementa la seguridad, porque permite a los administradores de sistemas revisar archivos del sistema incluyendo permisos, pertenencia, y contenido del archivo. El ASET alerta a los usuarios acerca de problemas de seguridad potencial y donde es apropiado colocar el sistema de archivos automáticamente de acuerdo a los niveles de seguridad especificados.

3.1.4.3 Conclusión

El Sistema Operativo Solaris brinda muchas ayudas, las cuales ayudarán a dar una buena portabilidad, escalabilidad, compatibilidad y seguridad en las aplicaciones para así operar en un ambiente creciente. Solaris tiene buenas herramientas para el administrador de sistemas en donde se puede obtener información rápida sobre dispositivos.

3.1.5. Sistema Operativo Windows Server 2003

3.1.5.1 Características para Implementar, Administrar y Usar

Gracias a su interfaz familiar, Windows Server 2003 es fácil de usar. Los nuevos asistentes simplificados facilitan la configuración de funciones específicas de servidor y de las tareas habituales de administración de servidores, de tal forma que incluso los servidores que no disponen de un administrador dedicado son fáciles de administrar. Además, los administradores disponen de diversas funciones nuevas y mejoradas, diseñadas para facilitar la implementación de Active Directory. Las réplicas de Active Directory de gran tamaño pueden implementarse desde medios de copia de seguridad, y la actualización desde sistemas operativos de servidor anteriores, como Microsoft Windows NT®, es más fácil gracias a la Herramienta de migración de Active Directory (ADMT), que copia contraseñas y permite la creación de secuencias de comandos. El mantenimiento de Active Directory es más fácil con las funciones nuevas, como la posibilidad de cambiar el nombre de los dominios y de volver a definir esquemas.

3.1.5.2 Infraestructura segura

Una informática de red eficiente y segura, ahora es más importante que nunca para que las empresas sigan siendo competitivas. Windows

Server 2003 permite que las organizaciones aprovechen sus inversiones ya existentes en tecnologías de la información, y que amplíen las ventajas de este aprovechamiento a sus asociados, clientes y proveedores, implementando funciones clave como las relaciones de confianza entre bosques del servicio Microsoft Active Directory® y la integración de Microsoft .NET Passport. La administración de identidades en Active Directory abarca la totalidad de la red, ayudando a consolidar la seguridad en toda la empresa. El cifrado de datos confidenciales resulta sencillo, y las directivas de restricción de software pueden usarse para prevenir los daños causados por virus y otro tipo de código malintencionado. Windows Server 2003 es la mejor elección para implementar una infraestructura de claves públicas (PKI), y sus funciones de inscripción automática y de renovación automática facilitan la distribución de tarjetas inteligentes y certificados en la empresa.

3.1.5.3 Confiabilidad y Disponibilidad

Se ha mejorado la confiabilidad mediante una gama de funciones nuevas y mejoradas, como el reflejo de memoria, la Memoria agregada en caliente y la detección de estado en Internet Information Services (IIS) 6.0. Proporciona una mayor escalabilidad, con la posibilidad de escalar desde un único procesador hasta sistemas de 32 direcciones.

Globalmente, Windows Server 2003 es más rápido, con un rendimiento del sistema de archivos hasta un 140 por ciento superior, así como un rendimiento significativamente más rápido para Active Directory, los servicios Web XML, los Servicios de Terminal Server y las redes.

3.1.5.4 Creación de sitios Web de Internet e Intranet

El servidor Web incluido en Windows Server 2003, proporciona una seguridad avanzada y una arquitectura confiable que ofrece aislamiento para las aplicaciones y un rendimiento muy mejorado. El resultado: mayor confiabilidad y rendimiento general. Y los servicios de Microsoft Windows Media® facilitan la creación de soluciones de medios de transmisión por secuencias con programación de contenido dinámico y un rendimiento más rápido y confiable. Las aplicaciones UNIX pueden integrarse o migrarse fácilmente.

Servicios Web XML fáciles de encontrar, compartir y reutilizar

Gracias a su interfaz Windows familiar, Windows Server 2003 es fácil de usar. Los nuevos asistentes simplificados facilitan la configuración de funciones específicas de servidor y de las tareas habituales de administración de servidores, de tal forma que incluso los servidores que no disponen de un administrador dedicado son fáciles de administrar.

3.1.5.5 Windows Server 2003, Web Edition

Diseñado para crear y alojar aplicaciones y páginas Web y servicios Web XML, Windows Server 2003, Web Edition proporciona una única solución para proveedores de servicios Internet (ISP), desarrolladores de aplicaciones y otro tipo de organizaciones que deseen únicamente utilizar o implementar funcionalidad específica de Web. Windows Server 2003, Web Edition aprovecha las mejoras realizadas en los Servicios de Internet Information Server 6.0 (IIS 6.0), Microsoft ASP.NET y Microsoft .NET Framework.

3.1.5.6 Resumen

Una gran ventaja de usar la plataforma Windows es por uso entorno y presentación motivo por el cual se hace fácil de usar y administrar, y como la mayoría de las personas ya conocen de estas bondades habrán muchos candidatos para su manejo, el problema de esta plataforma es que hay que actualizarlo constantemente ya sea por parches que Microsoft publique o por actualización de versiones que esta haga.

3.2. Detección de Intrusos

Un IDS o Sistema de Detección de Intrusiones es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema. Los IDS buscan patrones previamente definidos que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.

Los IDS aportan a nuestra seguridad una capacidad de prevención y de alerta anticipada ante cualquier actividad sospechosa. No están diseñados para detener un ataque, aunque sí pueden generar ciertos tipos de respuesta ante éstos.

Con los IDS, se tienen la capacidad de prevenir y dar una alerta anticipada ante una actividad sospechosa, no previenen ataques, pero generan algunos tipos de alertas sobre los mismos. Con un IDS se puede tener seguridad en el tráfico de la red, analizar paquetes, analizar la red, barrido de puertos, spoffing, etc.

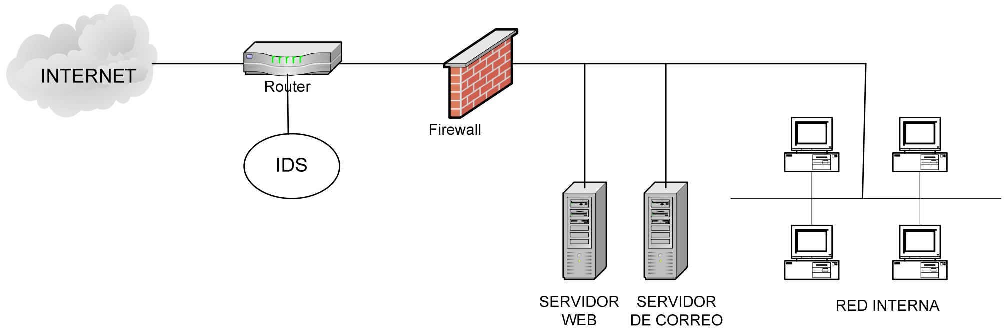

Figura 3.1. Red con IDS

3.2.1. Tipos de IDS

Lo podemos clasificar en tres grupos de la siguiente manera:

- Por Situación
- Según los Modelos de Detecciones
- Tipo de Repuesta

3.2.1.1 Por Situación

Según la función del Software de IDS, estos pueden ser:

- **NIDS:** Sistemas que analizan el Tráfico de la Red Completa.
- **HIDS:** Sistemas que analizan el Tráfico sobre un Servidor o PC.

Los sistemas que analizan la red (NIDS) examinan los paquetes individuales que viajan por ella. A diferencia de las barreras corta fuego, las que, típicamente, solo miran las direcciones IP, los puertos y los tipos de ICMP, los NIDS son capaces de comprender todas las diferentes banderas y opciones que pueden coexistir dentro de un paquete de red. Por lo tanto, un NIDS puede detectar paquetes armados maliciosamente y diseñados para no ser detectados por las relativamente simplistas reglas de filtrado de las barreras corta fuego. Los NIDS miran todo el tráfico que fluye por nuestra red, mientras que los sistemas de detección de intrusiones basados en el tráfico sobre un Servidor específico (HIDS) se preocupan de lo que está ocurriendo en cada computadora individual o "host". Son así capaces de detectar cosas tales como la ocurrencia de repetidos intentos fallidos de acceso o de modificaciones en archivos de sistema considerados críticos.

3.2.1.2 Clasificación según los modelos de detecciones

La siguiente clasificación es por Tipo de detecciones entre los cuales tenemos:

- Detección del mal uso.
- Detección del uso anómalo.

La detección del mal uso involucra la verificación sobre tipos ilegales de tráfico de red, por ejemplo, combinaciones dentro de un paquete que no se podrían dar legítimamente. Este tipo de detección puede incluir los intentos de un usuario por ejecutar programas sin permiso (por ejemplo, “sniffers”). Los modelos de detección basados en el mal uso se implementan observando como se pueden explotar los puntos débiles de los sistemas, describiéndolos mediante unos patrones o una secuencia de eventos o datos (“firma”) que serán interpretados por el IDS.

La detección de actividades anómalas se apoya en estadísticas tras comprender cual es el tráfico “normal” en la red del que no lo es. Un claro ejemplo de actividad anómala sería la detección de tráfico fuera de horario de oficina o el acceso repetitivo desde una máquina remota (rastreo de puertos). Este modelo de detección se realiza detectando cambios en los patrones de utilización o comportamiento del sistema. Esto se consigue realizando un modelo estadístico que contenga una métrica definida y compararlo con los datos reales analizados en busca de desviaciones estadísticas significantes.

3.2.1.3 Por el Tipo de Respuesta

Esta última clasificación hace referencia a la reacción del IDS frente a un posible ataque:

- Pasivos
- Activos o Reactivos

Pasivos

Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. Pero no actúa sobre el ataque o atacante.

Activos o Reactivos

Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.

3.2.2. Arquitectura de IDS

Normalmente la arquitectura de un IDS, a grandes rasgos, está formada:

La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.

Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema. Filtros que comparan los datos snifados de la red o de logs con los patrones almacenados en las reglas.

Detectores de eventos anormales en el tráfico de red. Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía mail, o SMS. Esto es a modo general.

IDS en un Proveedor de Servicios de Internet

Cuando el tráfico de solicitudes de acceso para el ISP es grande, para lo cual es o sería difícil instalar un solo IDS para el control de la misma. Una solución lógica sería colocar o instalar un IDS en cada nodo de conexión, empresa u organización, que se conectan al ISP.

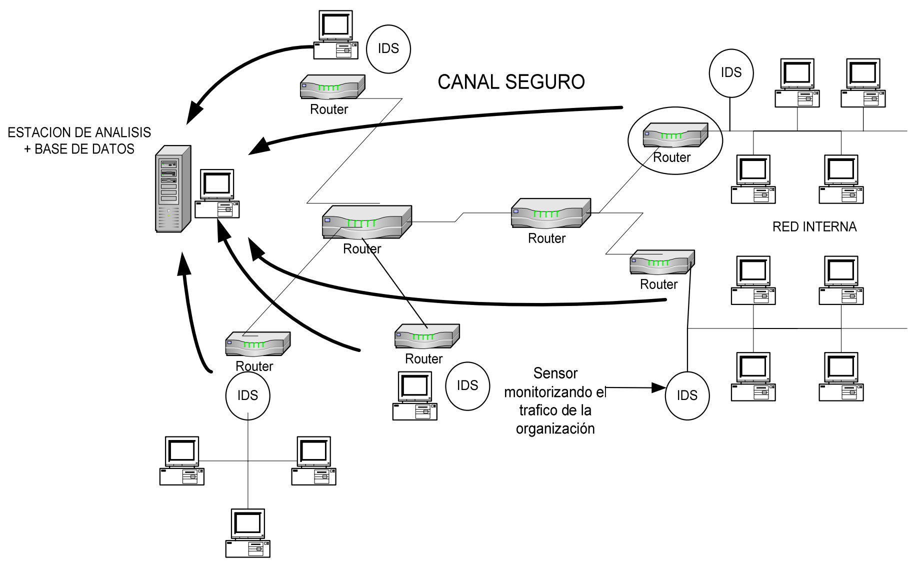

Figura 3.2 Distribución de los censores dentro de un ISP.

Esta transmisión debe realizarse de forma segura (y esto quiere decir “cifrada”) y a intervalos regulares, puesto que si el censor avisa de la alerta nada más, un atacante podría monitorizar el tráfico que genera el censor hacia la estación de análisis y deducir si un ataque ha sido detectado por el censor o no.

Donde es conveniente colocar el IDS

Una actitud paranoica por nuestra parte nos podría llevar a instalar un IDS en cada host ó en cada tramo de red. Esto último sería un tanto lógico cuando se trata de grandes redes. Lo lógico sería instalar el IDS en un dispositivo por donde pase todo el tráfico de red que nos interese.

3.2.3. Conclusiones

Existen muchos IDS en el mercado, desde software con un alto costo económico a ofertas totalmente gratuitas y capaces. Lo que hay que tener en cuenta es quién se encargará del soporte del IDS y si esta lo suficientemente capacitado para actualizar la base de datos del IDS y conocer todos los tipos de ataques y sus variaciones.

Aunque todo esto implique complicaciones, la utilización de IDS en las empresas debería estar integrada en la política de seguridad de las mismas, en completa coordinación con los demás recursos como los Firewall.

Un IDS sería un complemento perfecto para los Firewall, pero debe tomarse en cuenta la ubicación y uso de los mismos. En los ANEXOS de este documento podrán encontrar algunos nombres y características de productos comerciales de IDS.

3.3. Firewall

3.3.1. Característica

Debido a que Internet globalmente no es segura, sus sistemas privados son vulnerables a ataques y uso incorrecto. Un Firewall (o cortafuegos) es un mecanismo de protección que se puede utilizar para controlar el acceso entre una red segura y una menos segura. Un Firewall no es un único componente, es una estrategia diseñada para proteger los recursos de una organización que se pueden alcanzar a través de Internet. Un Firewall sirve de "guardián" entre Internet no segura y las redes internas (ó corporativas, ó Intranet) más seguras. La principal función de un Firewall es la de controlar el acceso centralizado. Si los usuarios exteriores ó remotos pueden acceder a las redes internas sin cruzar el Firewall, su efectividad es mínima. Por ejemplo, si un cierto usuario posee una cuenta Internet por red telefónica conmutada con un Proveedor de Servicios Internet (ó ISP, Internet Service Provider) Comercial y a veces se conecta a Internet desde su PC de la oficina utilizando el modem, está abriendo una conexión no segura con Internet que se salta la protección del Firewall.

Los Firewall también pueden utilizarse para crear segmentos seguros de red de una Intranet corporativa de una organización.

3.3.2. Función

Las principales funciones de un Firewall pueden ser las siguientes:

- Pueden bloquear tráfico no deseado.
- Pueden dirigir tráfico entrante a sistemas internos preparados para tal fin, más confiables.
- Pueden ocultar sistemas vulnerables que no pueden hacerse fácilmente seguros de Internet.
- Pueden registrar el tráfico que sale ó que llega a la red privada.
- Pueden ocultar información como nombres de sistemas, topología de red, tipos de dispositivos de red e identificadores de usuarios internos de Internet.
- Pueden proporcionar autentificación más robusta que la de las aplicaciones estándar. Como con cualquier mecanismo de protección, existen compromisos entre conveniencia y seguridad.

La transparencia es la visibilidad del Firewall tanto para los usuarios de dentro como para los de fuera que atraviesan el Firewall. Un Firewall se dice que es "transparente" para los usuarios si éstos no se dan cuenta, ni se deben detener en el mismo para acceder a la red. Los Firewall normalmente se configuran para ser transparentes a los usuarios de la red interna.

Los Firewall se configuran de forma no transparente para todas las redes externas que deseen atravesarlos. Esto proporciona generalmente el nivel más alto de seguridad sin cargar excesivamente a los usuarios internos.

Un firewall no es sólo un programa, es una combinación de routers, computadores y redes con un software apropiado para implementar políticas de seguridad entre una red protegida y la red externa (Internet).

3.3.3. Tipos

Existen diferentes implementaciones de Firewall que pueden ser organizadas de diferentes formas:

- Filtrado de Paquetes
- Nivel de Aplicación
- Híbridos

3.3.3.1 Filtrado de Paquetes

Utilizan routers con reglas de filtrado de paquetes para conceder ó denegar acceso en base a la dirección fuente, dirección destino y puerto. Ofrecen seguridad mínima pero a muy bajo costo y pueden ser una alternativa apropiada para entornos de bajo riesgo. Son rápidos, flexibles y transparentes. Las reglas de filtrado no suelen ser fácilmente mantenidas en un router, pero existen herramientas disponibles para simplificar las tareas de crear y mantener las reglas.

Los riesgos de los firewall basados en el filtrado de paquetes son:

- Las direcciones origen y destino y los puertos contenidos en la cabecera del paquete IP son la única información disponible para que el router tome la decisión de si permite ó no acceso de tráfico a una red interna.
- No protegen contra "spoofing" (ó engaño) de direcciones DNS ó IP.
- Un atacante tendrá un acceso directo a cualquier computador de la red interna una vez que el acceso haya sido concedido por el Firewall.
- En algunos Firewall de filtrado de paquetes no se soporta la autentificación fuerte de usuarios.
- Proporcionan poca ó ninguna información útil de "logging" (de registro).

3.3.3.2 Nivel de Aplicación

Utilizan programas servidor (denominados "proxies") que se ejecutan en el Firewall. Estos "proxies" toman las peticiones externas, las examinan y reenvían peticiones legítimas al computador interno que proporciona el servicio apropiado. Este tipo de Firewalls pueden soportar funciones como por ejemplo la autentificación de usuario y el registro. Debido a que este tipo de Firewall se considera como el tipo más seguro, esta configuración proporciona un conjunto de ventajas a la organización de riesgo medio-alta.

El Firewall puede configurarse como la única dirección de computador que es visible para la red externa, requiriendo que todas las conexiones hacia ó desde la red interna se realicen a través de los Firewall.

La autentificación fuerte de usuario puede ser obligada por los Firewall del nivel de aplicación.

3.3.3.3 Híbridos

Combinan los tipos de Firewall anteriores y los implementan en serie en vez de en paralelo. Si se conectan en serie, se mejora la seguridad total. Si se conectan en paralelo, entonces el perímetro de seguridad de red sólo será tan seguro como el menos seguro de los métodos utilizados. En entornos de medio a elevado riesgo un firewall híbrido puede ser la elección ideal de Firewall.

3.3.4. Arquitecturas

Se pueden configurar en diferentes arquitecturas, proporcionando diversos niveles de seguridad a diferentes costos de instalación y operación. Las organizaciones deberían hacer corresponder su perfil de riesgo con el tipo de arquitectura de firewall seleccionada. Las principales arquitecturas son:

- Computador Pantalla ó "screened host"
- Subred Pantalla ó "screened subnet"

Computador Pantalla ó "screened host"

Un Firewall con esta arquitectura utiliza un computador denominado "bastión" para que todos los computadores de fuera se conecten, en vez de permitir conexión directa a otros computadores internos menos seguros. Para usar Firewall de filtrado de paquetes, entonces un computador "bastión" debería establecerse para que todas las conexiones desde la red externa vayan a través del computador "bastión" para impedir que la conexión a Internet directa entre la red de la organización y el mundo exterior.

Subred Pantalla ó "screened subnet"

Esta arquitectura es esencialmente similar a la arquitectura del "computador pantalla", pero añade una capa extra de seguridad creando una red en el que reside el computador "bastión" (denominada "red perimetral") que se encuentra separada de la red interna. Una "subred pantalla" se crea añadiendo una red perimetral que separe la red interna de la externa. Esto asegura que si existe un ataque con ,éxito en el computador bastión, el atacante está restringido a la red perimetral por el "router pantalla" que se conecta entre la red interna y la red perimetral.

3.3.5. Para Intranets

Aunque los Firewall normalmente se colocan entre una red corporativa y la red no segura del exterior (ó Internet), en grandes organizaciones, los cortafuegos se utilizan a menudo para crear subredes diferentes dentro de la red interna (denominada también Intranet).

Los " Firewall para Intranets" se utilizan para aislar una subred particular de la red corporativa total. La razón del aislamiento de un segmento de red puede ser que ciertos usuarios sólo pueden acceder a subredes guardadas por estos Firewall sólo en base a una necesidad concreta. El uso de este Firewall se basa generalmente en la necesidad de hacer cierta información disponible para algunos pero no para todos los usuarios internos ó para proporcionar un alto grado de responsabilidad para el acceso y utilización de información sensible ó confidencial.

3.3.6. Administración y Gestión

Un Firewall, como cualquier dispositivo de red debe ser gestionado por alguien. La política de seguridad debe especificar quién es el responsable de la gestión del Firewall. El jefe de seguridad de información debe designar dos administradores de Firewall (uno primario y otro secundario) que serían los responsables de las tareas de conservación y mantenimiento de los Firewall.

El administrador primario debe encargarse de realizar los cambios en el firewall y el secundario sólo deber actuar en ausencia del primario para que no exista acceso simultáneo ó contradictorio en el Firewall.

3.4. Otros Componentes Adicionales

Dispositivos de respaldo en cinta: El respaldo de datos debe ser realizado a intervalos regulares, siguiendo una política establecida. Una máquina de procesador dual puede ser útil para esta tarea, puesto que el sistema operativo puede balancear la carga del proceso de respaldo, con la carga normal de operación, disminuyendo el impacto en el tiempo de respuesta percibido por los usuarios.

Quemadores de CD: Los grabadores de CD ROM son útiles para realizar copias de respaldo de software crítico. Los discos regrabables pueden usarse para guardar copias de datos de operación críticos.
Lamentablemente el uso de estos dispositivos de respaldo, esta limitado por su capacidad de 640 MB. Con el surgimiento de los grabadores para DVD se podrá aumentar la capacidad de almacenamiento a 17 GB en un único disco.
Impresoras: A menos que el ISP provea el servicio de impresión a sus clientes, no hay grandes requerimientos para impresión. Para el ISP basta con tener una impresora de tinta, o una impresora láser de capacidad media.

Unidades de respaldo de energía (UPS): Dentro de las medidas para el aseguramiento de disponibilidad de servicio y de protección eléctrica a los equipos, se tiene la del empleo de Sistemas de Energía Ininterrumpida (UPS).

3.4.1. Equipamiento de Redes CSU/DTU

El CSU/DTU (unidad de servicio al cliente / unidad de servicio de datos) es el dispositivo terminal para el backbone del ISP, y para las líneas de conexión de los abonados. Tanto las conexiones de subida como las de bajada son realizadas a través de compañías de telecomunicaciones (portadora). Este dispositivo puede ser arrendado o comprado a la portadora.

3.4.2. Servidores de Acceso

El servidor de acceso es un dispositivo que viene a reemplazar los antiguos bancos de módems. Ya no se recomienda el uso de bancos de módems debido a que no soportan la norma de módems V.90 (33.6 Kbps en subida y 56 Kbps en bajada) debido a una conversión análogo digital extra.

3.4.3. Aplicaciones según Sistema Operativo

La elección del software a utilizar queda restringida a la elección del sistema operativo. Dentro de las alternativas de sistema operativo se tiene como las más usuales Microsoft Windows Server 2003 y Unix en todos sus sabores: Sunsoft Solaris, SunOS 4, o las distribuciones de Linux.

Las aplicaciones adicionales deben ser configuradas y funcionar correctamente sobre cualquier de plataforma que sea la elegida.

La mayoría escogerán Windows ya que hay más personas con conocimiento en Windows que Linux, pero tenemos que tener en cuenta que los protocolos básicos para Internet fueron diseñados en plataformas Linux.

3.4.4. Servidores Web

Existe una gran variedad de software diseñado para distribuir páginas Web y aplicaciones para mejorar las presentaciones por Web, entre ellas se tiene:

Apache: Apache es el servidor Web más ampliamente utilizado en Internet, más de la mitad de los sitios en el mundo lo utilizan. Puede ser usada por la mayoría de los sistemas operativos.

Dbedit: Una buena característica del Web es la posibilidad de servir como interfaz para las bases de datos. Dbedit permite la interacción entre páginas Web y bases de datos.

Hawkeye: Hawkeye provee un conjunto de aplicaciones TCP/IP integradas que incluyen servidores HTML (Web), SMTP/POP3 (correo), NNTP (noticias), FTP(transferencia de archivos) y chat. Originalmente fue desarrollado para correr en Linux. Requiere MySQL.

3.4.5. Servidores para transferencia de Archivos

Los programas FTP (protocolo de transferencia de archivos) permiten la transferencia de archivos desde /hacia los sitios FTP.

Una ventaja del Sistema Operativo Linux es que tiene una aplicación de FTP. Otros servidores FTP son:

NcFTPd: Es una reimplementación de la versión abierta optimizada para sitios ftp de gran volumen. Tiene licencia comercial.

ProFTPd: Es un servidor FTP para Linux y Unix. Ofrece mejores prestaciones, seguridad y facilidad de administración que la versión estándar abierta del servidor FTP. Las facilidades de configuración y administración son muy similares al Apache.

3.4.6. Servidor de resolución de Nombres

Un servidor de resolución de nombres (DNS), hace la traducción entre nombres de computadores hacia direcciones IP y viceversa. Por ejemplo convierte www.google.com.ec a 189.68.65.36. Utilitarios como nslookup en Unix realizan consultas al servidor DNS para hacer la conversión nombre computador / dirección IP.

BIND: Es la versión estándar de Internet para DNS, viene incluido en la mayoría de las distribuciones de Linux. El paquete incluye el servidor DNS, la librería para resolución de nombres, y herramientas para verificar la buena operación del servidor DNS.

WebDNS: Provee una interfaz CGI para configurar servidores DNS. Su uso primario es hacer más rápido y fácil la adición de nuevas entradas a los archivos de configuración del DNS. Requiere la librería cigc disponible en http://www.boutell.com/cigc.

3.4.7. Software de Servidores de Correo Electrónico

IMAP (protocolo de acceso de mensajes Internet), es un método para una máquina "post office" (oficina de despacho) que acumula el correo de los usuarios y los envía a la máquina local del usuario para que lea sus correos. IMAP provee la misma funcionalidad que POP, y permite a los usuarios leer correos en una máquina remota sin tener que mover su correo local.

Cyrus IMAP server: La universidad Carnegie Mellon tiene una implementación de IMAP. Sólo está la implementación del servidor donde el usuario final no tiene permitido el acceso. Los correos son mantenidos en una base de datos privada. Se diseñó pensando en la eficiencia, desempeño, escalabilidad y seguridad.

Netscape Messaging Server: Es la implementación Netscape de IMAP. Es una implementación escalable y confiable. Toma ventajas del procesamiento paralelo de las tareas. Cuenta con facilidades de cache.

3.4.8. Servidores de Proxy y Cache

Los servidores Proxy son utilizados para proveer un único punto de acceso para los usuarios externos que miran dentro de la red, haciendo más fácil para el administrador la tarea de implementar las políticas de seguridad y las funciones de cache. Los servidores Proxy también funcionan como un embudo para los usuarios dentro de la red, con lo que facilitan el cumplimiento de las funciones de seguridad como el logging y el caching.

Squid: Ofrece un buen desempeño como cache proxy para clientes Web, y soporta requerimientos FTP, Gopher y HTTP. Viene incluido en la distribución Red Hat Linux.

Existen versiones comerciales que realizan funciones de proxy y cache, tales como Traffic Server de Inktomi, Border Manager de Novell.

3.4.9. Software para Bases de Datos

Los servidores de bases de datos pueden ser usados para guardar la información contable (información sobre el número de accesos, volumen del tráfico, etcétera) de los clientes.

Essentia: Es un motor de bases de datos con características tales como chequeo automático de consistencia, respaldos incrementales, administración de replicas de la base de datos, transacciones de dos fases (útiles para consultas remotas), conectividad con bases de dato Java (JDBC) y conexiones a bases de datos abiertas (ODBC).

PostgreSQL: Es un administrador de base de datos relacional (DBMS), que soporta la mayoría de las sentencias SQL, incluyendo subconsultas, transacciones, definición de tipos de usuario y funciones. Viene distribuido con Red Hat Linux.

3.4.10. Paquetes de Contabilidad para ISP

- Los softwares de administración de contabilidad permiten llevar estadísticas del consumo de los usuarios, de manera de poder tarifar dicho consumo.

3.5. Recomendación Final

A continuación damos nuestras sugerencias sobre el Sistema Operativo que el el área operativa de la empresa debé usar para dar los servicios de Internet y el tipo de conexión que brindará los clientes.

3.5.1. Sistema Operativo Área Operativa

Según la investigación realizada, hemos llegado a las siguientes conclusiones:

1. **Windows,** es una plataforma muy usada fácil de manejar y administrar, ya sea por su ambiente amigable o por la cantidad de ayuda que pueda tener.
2. **Linux,** una sistema operativo muy robusto pero no es fácil manejarlo para muchas personas.

Según estos puntos recogidos en base a nuestra investigación y conocimientos decidimos lo siguiente:

- La mejor opción como sistema operativo para el servidor del área de operaciones de la empresa es Linux en cualquiera de sus versiones, debido a su versatilidad, flexibilidad, capacidad de adaptación de código abierto, alto desempeño en ambiente multiusuario, estabilidad, bajo costo y el acelerado desarrollo que ha tenido en los últimos tiempos. Además para esa plataforma vienen diferentes utilitarios de manera gratuita.
- Para el servidor de Administración (para el personal de la empresa) usaremos como plataforma de trabajo el sistema Operativo Window XP y sus aplicaciones correspondientes.

3.5.2. Conexión ISP - Cliente

La conexión entre la empresa y el cliente que se usará es la de la telefonía pública, es decir, será una conexión Dial – Up, se llego a esta conclusión por cuanto aquí en Ecuador no existe una red total de Fibra Óptica y cable toda la ciudad o una gran parte de ella debería hacerse una inversión fuerte, adicionalmente habría que hacer las conexiones de Dial – Up para los lugares que no estén cableados, adicionalmente no se hace referencia por conexión vía Radio por cuanto habría que instalar en cada cliente los equipos de comunicación respectivos y esto representaría para el cliente un costo adicional. Por estos motivos y la economía que a traviesa el país se decidió que la comunicación sería vía telefonía pública.