UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

ADMINISTRACION DE REDES: MEDICION Y OPTIMIZACION DEL ACCESO A INTERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

LUIS ENRIQUE FLOREZ MAMANI

PROMOCION
2002 - I

LIMA – PERU
2008

ADMINISTRACION DE REDES: MEDICION Y OPTIMIZACION DEL ACCESO A INTERNET

Este informe lo dedico a las personas que me apoyaron durante mi vida universitaria y profesional, a mi padre y hermanos, pero en especial a mi madre quién dio su vida para que esto fuera posible.

SUMARIO

El presente informe pretende dar un enfoque del acceso a Internet que se realiza desde una empresa o institución, las medidas que se deben tener en cuenta, el análisis que se debe manejar para optimizar este recurso, así como también pretende explicar los equipos que se pueden utilizar para la medición del uso de Internet y los equipos que se pueden utilizar para el control y optimización del mismo.

El propósito del presente informe es brindar las herramientas necesarias a los alumnos o ingenieros que deseen implementar el acceso a Internet de una red de una forma segura y optima utilizando los recursos existentes tanto libres como los de venta en el mercado.

En el presente informe se ha conseguido cubrir la información relacionada a los diferentes tipos de ataques a los que estamos expuestos en Internet y las medidas y equipos que podemos utilizar para defendernos de los mismos, así como los detalles de configuración de los equipos que gestionaran nuestro acceso a Internet.

INDICE

PROLOGO

El presente informe se propone como objetivo desarrollar una metodología o modelo de guía para realizar las diferentes implementaciones del acceso a Internet, así como también llevar una administración optima de dicho acceso evitando todo tipo de ataque a la red y optimizando el uso de Internet.

El desarrollo de este informe consta de 4 capitulos estructurados de la siguiente manera:

El capitulo I ofrece un panorama general del problema a analizar, la importancia de un adecuado control del acceso a Internet así como la forma en que se evaluara y trabajara dicho análisis.

El capitulo II nos da una visión conceptual del tema, mostrando un resumen del acceso a Internet, las ventajas y desventajas de este servicio, así como un detalle de los ataques a los que los usuarios están expuestos al navegar en Internet y las recomendaciones de defensa para estos ataques.

El capitulo III describe los equipos y sistemas usados en la medición y control del acceso a Internet, se dará una breve explicación de equipos tales como Routers, Firewalls, Proxies, analizadores de ancho de banda y servidores generadores de reportes, todos ellos en conjunto nos darán una optima administración de nuestra salida a Internet

El capitulo IV nos mostrara el análisis realizado en una red corporativa usando los equipos anteriormente mencionados, los resultados obtenidos y las prevenciones del caso, así como las medidas que se deben realizar a fin de mantener un acceso a Internet optimo, seguro y productivo en temas laborales.

CAPITULO I
PLANTEAMIENTO DE INGENERIA DEL PROBLEMA

El problema planteado en el presente caso hace referencia al acceso que una empresa maneja hacia Internet. La diversidad de sistemas que maneja una empresa hace necesaria la investigación, análisis y optimización de este recurso primero como medida de seguridad y segundo con el fin de mantener una administración óptima del uso de este recurso que proveerá un valor agregado a la empresa.

En el presente capitulo veremos la descripción del problema *planteado, los objetivos del* trabajo, la evaluación del problema así como las limitaciones del trabajo y una síntesis del mismo.

1.1 Descripción del problema

La mayor parte de las empresas a nivel mundial tienen la necesidad debido al avance tecnológico de realizar sus operaciones diarias a través de conexiones hacia Internet o usando enlaces WAN hacia sus otras sedes. En este marco es cuando entra a tallar el análisis y la ingeniería a fin de estudiar, analizar y proponer mejoras para estas comunicaciones, las mejoras no solo son a nivel de optimización del uso del ancho de banda que se maneja, si no también en la seguridad de la red que se administra. Actualmente tanto para las grandes empresas como para las pequeñas la necesidad de conectarse a Internet ya sea para enviar información correspondiente al rubro de la empresa como información de Oracle, SAP, Base de datos, de correo o de navegación es ineludible, en este informe se analizarán los métodos de mejoras y optimización para este recurso que por si maneja un alto costo.

El problema de las conexiones radica básicamente en que algunas empresas no llevan un control de la utilización de su salida a Internet, ni un control de las páginas que los usuarios pueden acceder, este control es básico dado que determinara que paginas de contenido no laboral se están utilizando para luego ser bloqueadas en los equipos de

seguridad, adicionalmente con el análisis del uso del ancho de banda de podrán conocer que protocolos utilizan mayor nacho de banda del enlace a fin de poder disminuir su uso de ser el caso.

1.2 Objetivos del trabajo

Los objetivos de este informe apuntan a poder reconocer los distintos protocolos de comunicación que viajan en un enlace hacia Internet, identificar las distintas modalidades de ataques que se tienen en Internet así como las técnicas para poder evitar y contrarrestar dichos ataques, así también como conocer que información es la predominante en una red y analizar la forma de optimizar su uso, adicionalmente este informe pretende dar una visión más amplia sobre los diversos productos que se tienen actualmente en el mercado tales como el servidor Proxy basado en Linux, que es un sistema Linux que permite configurar reglas de bloqueo y aceptación de acceso a ciertas paginas webs que el administrador de la red configura, el cortafuegos o Firewall que es el dispositivo principal en la seguridad de una red, es la puerta de nuestra red hacia Internet donde podemos bloquear o permitir el acceso a redes, direcciones y protocolos, el Packetshaper de Packeteer que es un analizador de ancho de banda y el servidor SARG que es un sistema que elabora reportes del uso de Internet que realiza cada usuario y reportes de los sitios webs más visitados en una red, todos estos equipos sirven para optimizar el uso del ancho de banda hacia Internet o hacia una sede remota de una empresa o institución.

1.3 Evaluación del problema

El problema a evaluar se analizará sobre una red corporativa la cual maneja a su vez varias sedes con enlaces WANs nacionales como internacionales, adicionalmente se cuenta con cerca de 2000 usuarios conectados, por lo que la diversidad de protocolos y sistemas usados es amplia. En dicha red de maneja un amplio enlace hacia Internet, el cual a su vez es controlado por un equipo analizador de ancho de banda, el Packetshaper que se conecta a su vez a un Firewall de la marca Checkpoint y que luego pasa por el servidor de navegación o Proxy. Las mediciones se realizaran sobre las estadísticas del uso del recurso de Internet en el periodo de una semana, dicha información será recogida de los logs navegación del servidor Proxy, de los logs del Trucking del firewall, de los reportes del uso del ancho de banda del Packetshaper y de los reportes de navegación del servidor Sarg.

Dicho acceso a Internet será medido y analizado en el periodo de prueba con el fin de sacar conclusiones que nos permitan depurar páginas no laborales y optimizar el uso del ancho de banda hacia Internet.

1.4 Limitaciones del trabajo

Las limitaciones del presente trabajo básicamente son la no disponibilidad física de los equipos a fin de realizar alguna demostración del uso de los mismos, aún así se dará una amplia explicación de las funciones de dichos equipos, así como la explicación de las configuraciones que se deben realizar sobre cada uno de ellos a fin de poder administrar y optimizar el servicio de Internet en una organización.

1.5 Síntesis del trabajo

En síntesis este trabajo cubrirá el análisis diario que realiza un administrador de red de los recursos de su empresa en un periodo promedio de una semana, donde se podrá apreciar el uso del ancho de banda hacia Internet, así como el uso de los sistemas críticos que utiliza una empresa o institución como son el correo, los sistemas de base de datos como SAP, Oracle, SQL, los sistemas de transferencia de información como el FTP, el SSH, entre otros.

Este análisis nos dará una mejor visión para proponer mejoras o cambios en nuestras configuraciones de los equipos de red que administramos y así asegurar la estabilidad y el buen funcionamiento de nuestra red, libre de ataques y libre del uso de navegación hacia paginas webs que no son productivas para la empresa.

CAPITULO II
MARCO TEORICO CONCEPTUAL

En el presente capitulo resumiremos los antecedentes que se tienen sobre el acceso a Internet, revisaremos los problemas genéricos que se presentan al acceder a Internet, los tipos de acceso y las ventajas y las desventajas del acceso a dicho recurso, adicionalmente veremos los distintos tipos de ataques que tenemos actualmente, tales como el ataque tipo Spoofing, el caballo de Troya, los programas espías o Spywares el Phishing, el cual es uno de los mas conocidos en la actualidad por suplantar las cuentas bancarias vía Web, los ataques de fuerza bruta y el ataque de tipo denegación de servicios, veremos también algunas técnicas de defensa antes estos ataques y las medidas que debemos tomar para mantener la seguridad en nuestra red en lo concerniente al acceso a Internet.

2.1 Antecedentes del problema

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de computadoras diseñada para permitir la comunicación general entre usuarios de varias computadoras se ha desarrollado en un gran número de pasos. La unión de todos estos desarrollos culminó con la red de redes que conocemos como Internet. Esto incluía tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones.

Las más antiguas versiones de estas ideas aparecieron a finales de los años 50. Implementaciones prácticas de estos conceptos empezaron a finales de los 60 y a lo largo de los 70. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los 90 se introdujo la World Wide Web, que se hizo común.

La infraestructura de Internet se esparció por el mundo, para crear la moderna red mundial de computadoras que hoy conocemos. Atravesó los países occidentales e intentó una penetración en los países en desarrollo, creando un acceso mundial a

información y comunicación sin precedentes, pero también una brecha digital en el acceso a esta nueva infraestructura.

Un método de conectar computadoras, prevalente sobre los demás, se basaba en el método de la computadora central o unidad principal, que simplemente consistía en permitir a sus terminales conectarse a través de largas líneas alquiladas. Este método se usaba en los años 50 por el Proyecto RAND para apoyar a investigadores como Herbert Simon, en Pittsburgh (Pensilvania), cuando colaboraba a través de todo el continente con otros investigadores de Santa Mónica (California) trabajando en demostraciones de teoremas automatizadas e inteligencia artificial.

Un pionero fundamental en lo que se refiere a una red mundial, J.C.R. Licklider, comprendió la necesidad de una red mundial, según consta en su documento de enero, 1960, Man-Computer Symbiosis (Simbiosis Hombre-Computadora): "Una red de muchos [ordenadores], conectados mediante líneas de comunicación de banda ancha" las cuales proporcionan "las funciones hoy existentes de las bibliotecas junto con anticipados avances en el guardado y adquisición de información y [otras] funciones simbióticas"

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzados. Como parte del papel de la oficina de procesado de información, se instalaron tres terminales de redes: una para la System Development Corporation (S.D.C.) en Santa Mónica, otra para el Proyecto Genie en la Universidad de California (Berkeley) y otra para el proyecto Multics en el Instituto Tecnológico (M.I.T.) de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.

"Para cada una de estas tres terminales, tenía tres diferentes juegos de comandos de usuario. Por tanto, si estaba hablando en red con alguien en la S.D.C. y quería hablar con alguien que conocía en Berkeley o en el M.I.T. sobre esto, tenía que irme de la terminal de la S.D.C., pasar y registrarme en la otra terminal para contactar con él.

Dije, es obvio lo que hay que hacer: si tienes esas tres terminales, debería haber una terminal que fuese a donde sea que quisieras ir y en donde tengas interactividad. Esa idea es el ARPANet."

La seguridad es un tema que debe inquietar a cualquier organización que hoy día decida conectar su red a otras sobre Internet. Basta echar un vistazo a las estadísticas para tomar conciencia del riesgo que se corre: el número de incidentes contra sistemas

conectados casi se duplica cada año, según el Computer Emergency Response Team Coordination Center (CERT-CC). Y no debe extrañarnos, si tenemos en cuenta el vertiginoso crecimiento de Internet en los últimos años, que implica, por una parte, nuevas redes susceptibles de ser atacadas, y por otros, nuevos atacantes en potencia.

Lo cierto es que tal y como están las cosas, atacar una red conectada a Internet que no haya sido protegida de un modo "especial" es relativamente fácil, y mucho más aún si se utilizan sistemas operativos antiguos que no han sido actualizados ni debidamente "parcheados". En la red es posible encontrar, sin mucho esfuerzo, listas de debilidades tanto de protocolos como de sistemas operativos, así como guías que señalan los pasos a seguir para explotar dichas debilidades. Incluso existen servidores de ftp anónimo con todo tipo de herramientas orientadas a tomar el control de cualquier máquina.

Todas las líneas actuales de investigación en seguridad de redes comparten una idea: la concentración de la seguridad en un punto. Se obliga a que todo el tráfico entre la red que se pretende proteger y las redes externas pase por un mismo punto. Este punto se conoce con el nombre de firewall, y físicamente puede ser desde un simple Host hasta un complejo conjunto de redes separadas por routers. El empleo de un firewall (figura 1.1) presenta enormes ventajas sobre los enfoques de seguridad en redes tradicionales (que requieren la seguridad individual de cada Host conectado, y por tanto sólo pueden justificarse en entornos con un reducido número de máquinas), permitiendo concentrar todos los esfuerzos en el control de tráfico a su paso por el firewall.

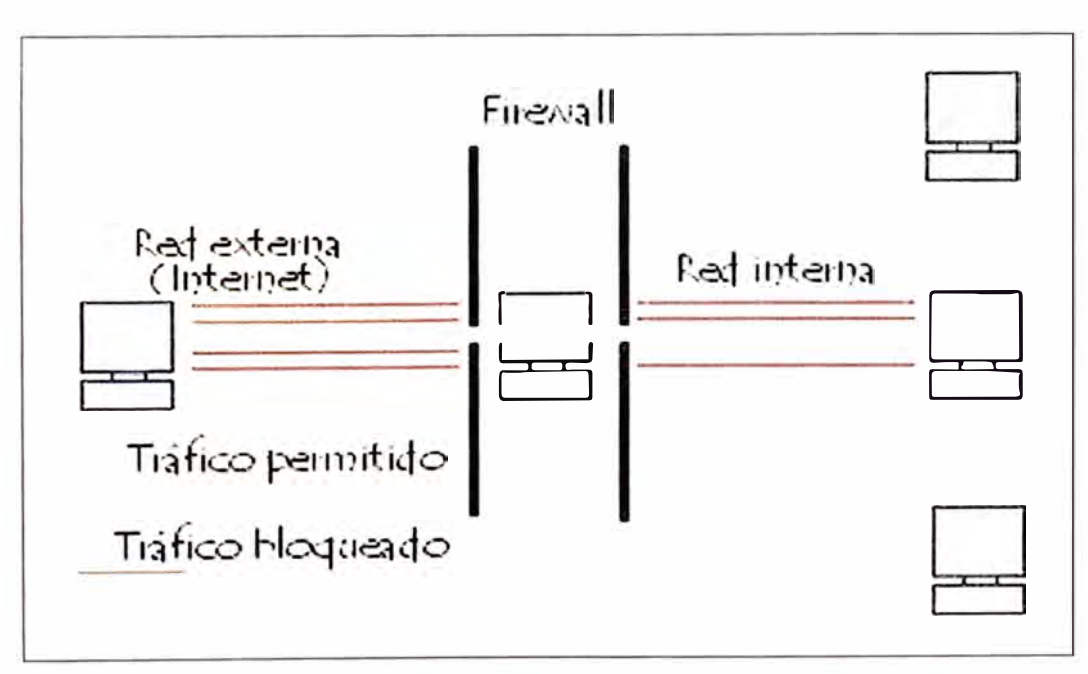


Fig 1.1 Firewall Perimetral

El firewall permite a su vez el acceso o el bloqueo de las direcciones IPs y los puertos que podamos definir para nuestra red como el ejemplo de la tabla 1.1

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.6.3	tcp	cualquiera	80
3	Aceptar	192.168.10.0	cualquiera	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Tabla 1.1 Reglas a configurar en el Firewall

2.2 Acceso a Internet: Generalidades

Muchas personas definen Internet como "La red de redes", y otros tantos como "La Autopista de la Información".

Efectivamente, Internet es una red de redes porque está hecha en base a unir muchas redes locales de computadoras y servidores, o sea de unos pocos ordenadores en un mismo edificio o empresa. Además, ésta es "La red de redes" porque es la más grande.

Prácticamente todos los países del mundo tienen acceso a Internet. En algunos, como los del Tercer Mundo, sólo acceden los millonarios y en otros como USA o los países más desarrollados de Europa, no es difícil conectarse.

Por la Red de Internet circulan constantemente cantidades increíbles de información. Por este motivo se le llama también La Autopista de la Información. Se estiman cerca de 200 millones de "Internautas" a nivel mundial, es decir, de personas que "navegan" por Internet en todo el Mundo. Se dice "navegar" porque es normal el ver información que proviene de muchas partes distintas del Mundo en una sola sesión.

Una de las ventajas de Internet es que posibilita la conexión con todo tipo de computadoras, desde las personales, hasta las más grandes que ocupan habitaciones enteras. Incluso podemos ver conectadas a la Red cámaras de vídeo, robots, y máquinas de refrescos, etc.

Una página de Internet contiene información de un tema en particular. Estas páginas contienen texto, gráficas, fotos e incluso videos y música.

La mayor parte de las empresas importantes tienen sitios en Internet, en donde se muestra información de la empresa, se describen los productos y servicios que ofrecen, y se realiza una mejor comunicación entre la empresa y sus clientes.

Algunos de los servicios disponibles en Internet, aparte de la Web, su versión evolucionada Web 2.0 y los sistemas operativos Web (WebOS, EyeOS), son el acceso remoto a otras máquinas (SSH, Telnet y Remote Desktop), la transferencia de archivos (FTP), el correo electrónico (SMTP y POP), los boletines electrónicos (news o grupos de noticias), las conversaciones en línea (IRC y chats), la mensajería instantánea, compartir archivos (P2P, P2M, Descarga Directa), la radio a la carta (Podcast), el visionado de vídeo a la carta (P2PTV, Miro, Joost, Videocast) y los juegos en línea.

2.3 Tipos de acceso a Internet

Internet incluye aproximadamente 5000 redes en todo el mundo y más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red. Los servicios disponibles en la red mundial de PC, han avanzado mucho gracias a las nuevas tecnologías de transmisión de alta velocidad, como DSL y Wireless, se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite (ver tu casa desde el cielo), observar el mundo por Webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego multijugador en 3D, un buen libro PDF, o álbumes y películas para descargar.

El método de acceso a Internet vigente hace algunos años, la telefonía básica, ha venido siendo sustituida gradualmente por conexiones más veloces y estables, entre ellas el ADSL, Cable Módems, o el RDSI. También han aparecido formas de acceso a través de la red eléctrica, e incluso por satélite (generalmente, sólo para descarga, aunque existe la posibilidad de doble vía, utilizando el protocolo DVB-RS).

Algunas de los medios por los que se puede acceder a Internet son:

ADSL

ADSL Este sistema permite transmitir información en formato digital a través de las líneas normales de teléfono. Utiliza frecuencias que no utiliza el teléfono normal, por lo que es posible conectar con Internet y hablar por teléfono a la vez mediante la instalación de un splitter o filtro separador. El ADSL es un tipo de conexión a través de banda ancha. Las velocidades que se pueden alcanzar son de hasta 8 Mbps de recepción y de hasta 1 Mbps de envío de datos. No obstante, la velocidad de transmisión también depende de la distancia del módem a la centralita, de forma que si la distancia es mayor de 3 Kilómetros

se pierde parte de la calidad y la tasa de transferencia empieza a bajar. Este es uno de los servicios de conexión que aumenta más rápidamente.

Fibra óptica

Los usuarios de este tipo de conexión, además de la conexión a Internet, tienen la posibilidad de recibir servicios como televisión de pago, video bajo demanda, telefonía, etc. Mediante este tipo de conexión se pueden alcanzar velocidades teóricas de hasta 30 Mbps, pero lo normal es disponer de alrededor de 300 Kbps. Es una forma de conexión a la Red que utiliza la señal de televisión a través de cableado de fibra óptica. Este servicio toma uno de los canales de la señal de televisión y lo utiliza para acceder a la Red. La ventaja del uso de la línea de TV es que el ancho de banda es mucho mayor. Se trata de una tecnología totalmente distinta donde en lugar de establecer una conexión directa, o punto a punto, con el proveedor de acceso, se utilizan conexiones multipunto, en las cuales muchos usuarios comparten el mismo cable. Cada punto de conexión a la Red o nodo puede dar servicio a entre 500 y 2000 usuarios y la distancia de éste al usuario no puede superar los 500 metros. La velocidad de subida puede rozar la cifra de 1 Mbps; por otra parte hay que saber que es un sólo cable el que transmite los datos de abonado en abonado, repartiendo el ancho de banda entre cientos de ellos, además de las interferencias que recibe del entorno

Dial Up

Una conexión Dial-Up es un servicio de acceso a Internet que establece una conexión a Internet mediante una línea telefónica y un MODEM, permitiéndole acceder a todas las herramientas disponibles en Internet como son el E-Mail (Electronic Mail), WWW (World Wide Web), FTP (File Transfer Protocol), IRC, etc. Características del servicio Dial Up: Acceso Dial Up con tarifa reducid, conexión sin límites 24 Horas al día, sin restricciones de horario, 1 Cuenta de Email POP3, con Webmail, sistema AntiSpam y AntiVirus para tu Email entre otros.

Cable

Normalmente se utiliza el cable coaxial que también es capaz de conseguir tasas elevadas de transmisión pero utilizando una tecnología completamente distinta. En lugar de establecer una conexión directa, o punto a punto, con el proveedor de acceso, se utilizan conexiones multipunto, en las cuales muchos usuarios comparten el mismo cable.

Las principales consecuencias del uso de esta tecnología son:

Cada nodo (punto de conexión a la Red) puede dar servicio a entre 500 y 2000 usuarios.

Para conseguir una calidad óptima de conexión la distancia entre el nodo y el usuario no puede superar los 500 metros.

No se pueden utilizar los cables de las líneas telefónicas tradicionales para realizar la conexión, siendo necesario que el cable coaxial alcance físicamente el lugar desde el que se conecta el usuario.

La conexión es compartida, por lo que a medida que aumenta el número de usuarios conectados al mismo nodo, se reduce la tasa de transferencia de cada uno de ellos.

Esta tecnología puede proporcionar una tasa de 30 Mbps de bajada como máximo, pero los módems normalmente están fabricados con una capacidad de bajada de 10 Mbps y 2 Mbps de subida. De cualquier forma, los operadores de cable normalmente limitan las tasas máximas para cada usuario a niveles muy inferiores a estos, sobre todo en la dirección de subida

Redes Inalámbricas

Las redes inalámbricas o Wireless son una tecnología normalizada por el IEEE que permite montar redes locales sin emplear ningún tipo de cableado, utilizando infrarrojos u ondas de radio a frecuencias desnormalizadas (de libre utilización).

Están compuestas por dos elementos:

- Punto de acceso (AP) o "transceiver": es la estación base que crea un área de cobertura donde los usuarios se pueden conectar. El AP cuenta con una o dos antenas y con una o varias puertas Ethernet.

- Dispositivos clientes: son elementos que cuentan con tarjeta de red inalámbrica. Estos proporcionan un interfaz entre el sistema operativo de red del cliente y las ondas, a través de una antena.

El usuario puede configurar el canal (se suelen utilizar las bandas de 2,4 Ghz y 5Ghz) con el que se comunica con el punto de acceso por lo que podría cambiarlo en caso de interferencias. En España se nos impide transmitir en la totalidad de la banda 2,4 Ghz debido a que parte de esta banda está destinada a usos militares.

La velocidad con el punto de acceso disminuye con la distancia.

Los sistemas inalámbricos de banda ancha se conocen cómo BWS (Broadband Wireless Systems) y uno de los más atractivos, son los sistemas LMDS (Local Multipoint Distribution Service) que es un sistema inalámbrico de banda ancha punto-a-multipunto que utiliza la especificación de comunicación de microondas.

2.4 Ventajas del acceso a Internet

La evolución y el acceso al Internet en estos últimos tiempos ha crecido enormemente y hoy hay mucha gente inmersa en este mundo, especialmente las nuevas generaciones ya nacieron con esto, por lo que dentro de un tiempo ya el Internet será algo intrínseco en nuestras vidas, y su crecimiento no lo podremos detener.

Internet tiene un impacto bastante pronunciado en el trabajo, el ocio, el entretenimiento, el conocimiento y otras áreas a nivel mundial. Gracias a la superautopista de la información, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y las bibliotecas tradicionales, la Web o la Internet han permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los Weblog, que se utilizan en gran parte como diarios que normalmente están siendo actualizados. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes o cibernautas con conocimiento de expertos e información libre.

He aquí algunas de las ventajas del acceso a Internet:

- Hace la comunicación mucho más sencilla.
- Fácil acceso y bajo costo.
- Es posible conocer e interactuar con muchas personas de todas partes del mundo.
- Es posible intercambiar correos con contactos de trabajo o familiares en tiempo real.
- La búsqueda de información se vuelve mucho más sencilla, sin tener que ir forzadamente a las bibliotecas tradicionales.
- Es posible encontrar muchos puntos de vista diferentes sobre alguna noticia.
- Es posible la creación y descarga de software libre, por sus herramientas colaborativas, tal es el caso de Linux.
- La computadora se actualiza periódicamente más fácil que si no tuviéramos Internet.
- Es posible encontrar soporte técnico de toda clase sobre alguna herramienta o proceso.

Es posible realizar pagos de agua, luz, teléfono o educación de una forma segura y con ahorro de tiempos considerables comparando con el pago del servicio en persona.

- El seguimiento de la información a tiempo real es posible a través del Internet.
- Es posible comprar fácilmente a otras tiendas de otros países
- Y es posible compartir muchas cosas personales o conocimientos que a otro le puede servir, y de esa manera, se vuelve bien provechoso.

2.5 Desventajas del acceso a Internet

Internet es una valiosa fuente de información, pero es también una poderosa fuente de riesgos. Por ejemplo una posible entrada de un programa espía o Spyware, la generación de brechas para intrusiones, la paralización de actividades en caso de denegación de servicios, la posibilidad de que los empleados deshonestos evadan información, la revelación no intencionada de información sensible y los secretos industriales, los ataques basados en correo electrónico, accesos remotos no controlados, contaminación vía P2P y por mensajería instantánea, la lista es larga y por lo tanto, merece un exhaustivo conocimiento del tema y un análisis de las probabilidades de que estos sucesos puedan ocurrir en nuestra red.

Es importante resaltar que la Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales el ingreso de Internet y las nuevas tecnologías de información es muy limitada para las personas; esta brecha ha permitido que estas limitaciones varíen.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas, las cuales van a permitir la comunicación cada vez más amplia alrededor del mundo.

El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas. Conociendo este hecho y relacionándolo con la felicidad originada por las relaciones personales, podemos concluir que cuando una persona tenga una necesidad de conocimiento popular o de conocimiento no escrito en libros, puede recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet dicha persona preferirá prescindir del obligado protocolo que hay que cumplir a la hora de acercarse a alguien personalmente para obtener dicha información y por ello no establecerá una relación personal sino virtual. Este hecho, implica la existencia de un medio capaz de albergar soluciones para diversidad de problemas.

He aquí algunas de las desventajas que representa el acceso a Internet:

- Así como es de fácil encontrar información buena, es posible encontrar de la misma forma información mala, desagradable (pornografía, violencia explícita, terrorismo) que puede afectar especialmente a los menores.
- Genera una gran dependencia o vicio del Internet, descuidando al usuario de muchas actividades personales o laborales.
- El principal puente de la piratería es el Internet (Existen programas que realizan la compartición de libros o CDs a los demás cibernautas sin pago alguno al autor)
- Distrae a los empleados en su trabajo.
- Dominio de computadora, para poder utilizar el Internet.
- Dependencia de procesos. Si hay un corte de Internet, hay muchos procesos que se quedan varados por esa dependencia.
- Dependencia de energía eléctrica. Si hay un corte de energía en la empresa o en la casa, nos quedamos sin el servicio de Internet (no es el caso de la telefonía convencional).
- Hace que nazcan otros males tales como el spam, el malware, la proliferación de los virus, el phising, etc.

2.6 Tipos de ataques en Internet

Durante los primeros años de Internet, los ataques a sistemas informáticos requerían pocos conocimientos técnicos. Por un lado, los ataques realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Por el contrario, los ataques externos se producían gracias al conocimiento de las contraseñas necesarias para acceder a los equipos de la red.

Con el paso de los años se han ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a Internet. Estos nuevos métodos de ataque se han ido automatizando, por lo que en muchos casos sólo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a Internet tiene acceso hoy en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

En la mayor parte de la bibliografía relacionada con la seguridad en redes informáticas podemos encontrar clasificadas las tres generaciones de ataques siguientes:

- Primera generación: ataques físicos. Encontramos aquí ataques que se centran en componentes electrónicos, como podrían ser los propios ordenadores, los cables o los dispositivos de red. Actualmente se conocen soluciones para estos ataques, utilizando protocolos distribuidos y de redundancia para conseguir una tolerancia a fallos aceptable.

- Segunda generación: ataques sintácticos. Se trata de ataques contra la lógica operativa de los ordenadores y las redes, que quieren explotar vulnerabilidades existentes en el software, algoritmos de cifrado y en protocolos. Aunque no existen soluciones globales para contrarrestar de forma eficiente estos ataques, podemos encontrar soluciones cada vez más eficaces.

- Tercera generación: ataques semánticos. Finalmente, podemos hablar de aquellos ataques que se aprovechan de la confianza de los usuarios en la información. Este tipo de ataques pueden ir desde la colocación de información falsa en boletines informativos y correos electrónicos hasta la modificación del contenido de los datos en servicios de confianza, como, por ejemplo, la manipulación de bases de datos con información pública, sistemas de información bursátil, sistemas de control de tráfico aéreo, etc.

A continuación analizaremos algunos de los ataques más conocidos que se producen en Internet.

2.6.1 Spoofing

Es una técnica más o menos sofisticada de autenticar una máquina en otra máquina con una dirección fuente de "confianza". En otras palabras, consiste en modificar en los mensajes que salen de una máquina la dirección fuente haciendo creer a los destinatarios de esos mensajes que es otra dirección quien le envía el mensaje y además esa es una dirección de "confianza". Por una dirección de "confianza" se entiende que esa dirección esta autorizada a mantener una relación con la máquina destino. Autenticación es el proceso mediante el cual las maquinas se identifican una con la otra. Normalmente confianza y autenticación mantienen una relación de inversa proporcionalidad, es decir a mayor confianza menos autenticación es requerida, y a mayor autenticación, menor confianza hay. A pesar de que no nos damos cuenta nosotros estamos autenticándonos constantemente, por ejemplo tenemos que utilizar nombre usuario y contraseña para utilizar alguno de los siguientes servicios:

• La Conexión a Internet

• FTP Sites

• Servicios de Telnet y cuentas de usuario

El significado de que todas estas autenticaciones y muchas más sean requeridas es la poca confianza que existe en Internet con los usuarios que se conectan. Las máquinas se pueden autenticar de muchas maneras, dependiendo de su relación de confianza. Por ejemplo una máquina puede ser autenticada por su nombre de Host o por su dirección IP.

La mecánica de un ataque Spoofing

El hecho de que la autenticación de direcciones fuente falle, no supone que sea posible el Spoofing. Esto es porque el mecanismo de conexión requiere mucho más que simplemente una dirección IP correcta, requiere un dialogo entre las dos máquinas. Este dialogo puede explicarse por pasos:

• El protocolo IP es responsable del transporte de los paquetes, pero este transporte es inseguro, no hay garantía alguna de que los paquetes lleguen intactos. IP a veces no consigue que lleguen los paquetes, así que el primer paso para iniciar una conexión es que lleguen los paquetes intactos al host apropiado.

• Después de que los paquetes hayan llegado, actúa TCP. TCP es un servicio más seguro y tiene herramientas para comprobar si los paquetes llegan y si lo hacen intactos. Cada paquete es verificado individualmente. TCP procesa si los paquetes tienen error secuencialmente, si 5 paquetes son enviados (1,2,3,4,5), estos son procesados en orden de llegada. Cuando se inicia una conexión TCP el primer paquete del cliente se identifica con un número de secuencia aleatorio, los siguientes paquetes están numerados con respecto a este número. El servidor responde a este mensaje con el reconocimiento de este número de secuencia y con un número de secuencia propio que debe ser reconocido por el cliente. Este procedimiento de inicio de una conexión TCP se llama protocolo a tres bandas. El problema para quien quiere generar un ataque de spoofing se puede caracterizar como sigue.

Primero debe "trucar" la dirección fuente y segundo debe mantener un diálogo con la máquina objetivo. Es esta segunda parte de este proceso la que hace complejo el ataque, y el porqué es debido a que la secuencia de dialogo no es arbitraria, es la máquina objetivo quien genera el número de secuencia al cual debe responder el atacante con el reconocimiento pertinente. Además el atacante debe adivinar este número de secuencia

ya que no recibe los paquetes que envía el objetivo puesto que la dirección IP fuente que el atacante ha enviado estaba "trucada".

Pongamos un ejemplo:

• El cracker conoce que 200.48.4.5 y 63.45.12.8 mantienen una relación de confianza, es decir tienen una conexión establecida y quiere entrar en 200.48.4.5. Para entrar debe hacerse pasar por 63.45.12.8 y lo consigue "trucando" la dirección de su máquina. • El problema reside en que las respuestas de 200.48.4.5 son enrutadas hacia 63.45.12.8 y no a la máquina del cracker. Es por esto que el cracker nc puede ver el tráfico de paquetes, y es por esta incapacidad de ver el tráfico de estos paquetes por lo que a esta técnica de spoofing se le llama "blind spoofing". Si por el contrario el trafico de estos paquetes puede ser visto por el cracker entonces la técnica se llama "Non blind spoofing".

El caso de los ataques "blind spoofing" presenta una mayor problemática. Mirando el ejemplo que hemos puesto si la maquina 63.45.12.8 responde a la maquina objetivo mientras se está produciendo el ataque entonces fallará todo el proceso. Debido a esto el atacante deberá además realizar un paso antes de realizar el ataque. Deberá realizar el spoofing cuando la máquina 63.45.12.8 no esté en marcha o implementar un mecanismo para que 63.45.12.8 se ponga a "dormir" y deje de enviar tramas a la máquina objetivo. La máquina 63.45.12.8 puede ser "matada" mediante un ataque SYN flood, de esta manera el sistema será incapaz de tener más conexiones "medio abiertas" y no puede utilizar la red.

Los principales pasos que se deben llevar a cabo en un ataque spoofing son:

• El cracker debe identificar su objetivo.

• Debe "dormir" el host por el que el se quiere hacer pasar.

• Debe "trucar" su dirección IP con la del host por el que se quiere hacer pasar.

• Se debe conectar al objetivo como si fuera el host dormido.

• Debe adivinar el número de secuencia correcto que espera el objetivo.

Los primeros cuatro pasos son sencillos, pero adivinar el número de secuencia resulta muy complicado. Para realizar esta tarea el cracker debe ejecutar una conexión de prueba solicitando al objetivo una petición de conexión. El objetivo responde a esta petición con una ráfaga de números de secuencia. El cracker entonces registra esos números de secuencia y cierra la conexión. El cracker examina los números de secuencia que ha obtenido del objetivo, en este análisis el intenta descubrir un patrón ya que el conoce que esos números de secuencia son incrementados uniformemente por un

algoritmo especialmente diseñado para ese propósito. Su tarea es descubrir ese algoritmo con el fin de averiguar los valores numéricos con los que los números de secuencia son incrementados. Cuando él conoce esto puede predecir que numero de secuencia es solicitado en la conexión para la autenticación y está listo para generar el ataque. Spoofing es una difícil y extraordinaria técnica, pero lo más sorprendente de todo es que en ambientes de seguridad relativa a redes desde 1985 se sabia que spoofing era posible. Cuando el proceso de conexión y autenticación han concluido, el cracker debe crear un agujero más apropiado a través del cual "colarse" en el sistema y no tener que utilizar spoofing cada vez que quiere conectarse con el objetivo. El agujero más fácil es rescribir el fichero .rhosts de manera que el objetivo aceptara conexiones sin necesidad de pedir autenticación adicional. De esta manera el cracker puede cerrar la conexión y reconectarse cuantas veces quiera sin necesidad de contraseña y tiene control sobre el sistema.

Aunque parecen pocos los servicios que se conoce que son vulnerables, tengamos en cuenta que la mayoría de servicios de red que conocemos utilizan autenticación basada en direcciones IP y aunque los otros servicios son propios de sistema UNIX, el resto de sistemas NO-UNIX no son inmunes. Windows NT por ejemplo es vulnerable a ataques de números de secuencia. Las sesiones pueden ser "secuestradas" a través de adivinar el número de secuencia TCP. En el fondo es un problema de spoofing, que incluso afecta a conexiones NetBIOS y SMB. Los ataques de Spoofing solian ser raros, debido a la complejidad del proceso, pero después de Enero de 1995 se volvieron más comunes. Esto es asi porque antes de 1995 quien generaba un ataque de este tipo debia tener un amplio conocimiento acerca de TCP/IP, sockets y programación de red, pero ahora eso ya no es preciso, ya que empezaron a aparecer programas que realizaban Spoofing. Hoy en día aplicaciones que implementan Spoofing están ampliamente difundidas y pueden ser descargadas incluso desde Internet.

2.6.2 Caballo de Troya

El Caballo de Troya es un programa que se enmascara como algo que no es, normalmente con el propósito de conseguir acceso a una cuenta o ejecutar comandos con los privilegios de otro usuario.

El caballo de Troya también es conocido como Troyano, se denomina troyano (o caballo de Troya, traducción fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a

través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona.

Un troyano no es en sí un virus, aún cuando teóricamente pueda ser distribuido y funcionar como tal. La diferencia fundamental entre un troyano y un virus consiste en su finalidad. Para que un programa sea un "troyano" sólo tiene que acceder y controlar la máquina anfitriona sin ser advertido, normalmente bajo una apariencia inocua. Al contrario que un virus, que es un huésped destructivo, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa alojado dentro de una aplicación, una imagen, un archivo de música u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene. Una vez instalado parece realizar una función útil (aunque cierto tipo de troyanos permanecen ocultos y por tal motivo los antivirus o anti troyanos no los eliminan) pero internamente realiza otras tareas de las que el usuario no es consciente, de igual forma que el Caballo de Troya que los griegos regalaron a los troyanos.

Habitualmente se utiliza para espiar, usando la técnica para instalar un software de acceso remoto que permite monitorizar lo que el usuario legítimo de la computadora hace (en este caso el troyano es un spyware o programa espía) y, por ejemplo, capturar las pulsaciones del teclado con el fin de obtener contraseñas (cuando un troyano hace esto se le cataloga de keylogger) u otra información sensible.

2.6.3 Spywares o programas espías

Los programas espías o spywares son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a Internet.

Pueden tener acceso a información personal del usuario como por ejemplo al correo electrónico y al password; la dirección y la dirección de los DNSs; teléfono, país; páginas

que se visitan, qué tiempos se está en ellas y con qué frecuencia se regresa; qué software está instalado en el equipo y cuál se descarga; qué compras se hacen por internet; tarjeta de crédito y cuentas de banco.

Los programas espías pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo. Bajar programas desde sitios "NO OFICIALES" también puede ser de alto riesgo, muchos sitios Web ofrecen programas que crean instaladores con spyware a fin de darte lo que buscabas pero a su vez vigilarte y bombardearte con publicidad que ellos venden.

Los programas de recolección de datos instalados con el conocimiento del usuario no son realmente programas espías si el usuario comprende plenamente qué datos están siendo recopilados y a quién se distribuyen.

El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

Las consecuencias de una infección de spyware moderada o severa (a parte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50% en casos extremos), y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet.

2.6.4 Ingeniería social

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados,

criminales, o delincuentes computacionales (mejor conocidos como hackers, aunque el termino correcto es cracker) para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, pretendiendo, por ejemplo, ser un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía la Internet o la Web se usa, adicionalmente, el envío de solicitudes de renovar permisos de acceso a páginas Web o memos falsos que solicitan respuestas e incluso las famosas "cadenas". Llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema esta solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (pesca). Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores. En realidad, los administradores de sistemas informáticos raramente (o nunca) necesitan saber la contraseña de los usuarios para llevar a cabo sus tareas. Sin embargo incluso este tipo de ataque podría no ser necesario — en una encuesta realizada por la empresa Boixnet, el 90% de los empleados de oficina de la estación Waterloo de Londres reveló sus contraseñas a cambio de un bolígrafo barato.

Otro ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en e-mails, ofreciendo, por ejemplo, fotos "intimas" de alguna persona famosa o algún programa "gratis" (a menudo aparentemente provenientes de alguna persona conocida) pero que ejecutan código malicioso (por ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam). Ahora, luego de que los primeros e-mails maliciosos llevaron a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar esos archivos de forma explícita para

que ocurra una acción maliciosa. Muchos usuarios, sin embargo, abren casi ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.

2.6.5 Phishing

El "phishing" es una modalidad de estafa diseñada con la finalidad de robar la identidad de un usuario. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

En esta modalidad de fraude, el usuario malintencionado envía millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Dada la confianza que los usuarios tienen depositada en las entidades de las que son clientes, y por desconocimiento o simplemente ante la incertidumbre y temor creados, acceden a dichas páginas Web piratas, donde el defraudador o delincuente informático, obtiene los datos personales o claves de acceso personales.

Es a partir de este momento donde empieza el fraude:

- Utilización del número de tarjeta y fecha de caducidad para compras por Internet (comercio electrónico).
- Realización de transferencias bancarias no consentidas ni autorizadas.
- Retiro de efectivo en cajeros con duplicados de las tarjetas, entre otros.

2.6.6 Sniffing

Es la técnica por la cual utilizando un programa se escucha la conversación entre 2 PCs y de acuerdo a la seguridad que tuvieran estos equipos se podría obtener datos personales como usuarios, password, números de tarjetas de crédito, etc.

Uno de los ataques más peligrosos usando el método de Sniffing consiste en la intercepción de datos de pagos realizados online con tarjetas de crédito, utilizando después estos datos para hacer compras sin que el titular de la tarjeta se entere.

Una pequeña nota cultural: "Sniffing" deriva de "sniff", que en inglés significa Olfatear.

¿Como funciona?

En realidad, la placa de red de una computadora siempre recibe todos los paquetes que circulan por la red (al igual que cualquier máquina conectada). Cada paquete es analizado, pero solo son aceptados aquellos que están dirigidos hacia ella. Esto forma parte del funcionamiento normal de cualquier red Ethernet.

Al activar un sniffer, estamos haciendo que nuestra placa de red acepte cualquier paquete de datos, sin importar si está dirigido hacia nosotros. Técnicamente, es setear la placa en "modo promiscuo".

De esta manera es posible robar passwords, e-mail, y cualquier tipo de información, ya sea de carácter público o privado.

Cabe aclarar, que se puede utilizar un sniffer, sólo para saber si una máquina determinada está transmitiendo información, o si lo está haciendo correctamente. Es decir que también existe el sniffing "usado para hacer el bien".

El sniffing es un peligro real, que no necesita de grandes medios y, lo que es peor, indetectable en la mayor parte de casos; a pesar de que existen métodos para tratar de detectar sistemas con un interfaz en modo promiscuo, no suelen ser todo lo efectivos que uno podría esperar, ya que detectar una máquina en este estado no es inmediato. Es el fraude más difícil de realizar y solo es posible si el estafador es un experto hacker.

2.6.7 Denegación de servicios

Un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca

la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivos.

El llamado DDoS (siglas en inglés de Distributed Denial of Service, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del flood o saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigidas a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido sofisticándose hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

Un ejemplo actual: el domingo 3 de febrero de 2008, la Web Genbeta dejó de funcionar debido a un DDoS de gran magnitud que afectó no solo a éste, sino a todo Weblog SSL.

2.6.8 Ataque de fuerza bruta

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permita el acceso.

Dicho de otro modo, define al procedimiento por el cual a partir del conocimiento del algoritmo de cifrado empleado y de un par texto claro/texto cifrado, se realiza el cifrado (respectivamente, descifrado) de uno de los miembros del par con cada una de las posibles combinaciones de clave, hasta obtener el otro miembro del par. El esfuerzo requerido para que la búsqueda sea exitosa con probabilidad mejor que la par será 2

elevado a (n − 1) operaciones, donde n es la longitud de la clave (también conocido como el espacio de claves).

Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Contraseñas que sólo utilicen dígitos numéricos serán más fáciles de descifrar que aquellas que incluyen otros caracteres como letras, así como las que están compuestas por menos caracteres serán también más fáciles de descifrar, la complejidad impuesta por la cantidad de caracteres en una contraseña es logarítmica.

Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, son muy costosos en tiempo computacional. La fuerza bruta suele combinarse con un ataque de diccionario.

Un software Free que realiza ejecuta esta técnica es el Brutus, el cual intenta conexiones de forma continua a un host o dirección IP.

2.7 Técnicas de defensa

En una sociedad cada vez más dependiente de las tecnologías de la información, debemos estar preparados para ataques informáticos", justificaba James Mattis, jefe del Mando de la OTAN para la Transformación, la puesta en marcha de un centro de ciberdefensa dentro de la organización militar. En mayo se anunció la creación del Centro de Excelencia en Ciberdefensa (CEC), que se ha instalado en Tallin (Estonia) y estará operativo en breve. España, Italia, Alemania, Eslovaquia, Estonia y Letonia forman parte de él, y se espera que otros países de la OTAN se unan a la iniciativa este año. El objetivo es, según dice el memorándum fundacional del centro, proteger los estados de los ciberataques, entrenar a militares, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad.

No sólo las empresas o los particulares son víctimas de la delincuencia a través de Internet. Como explica Madis Tüür, portavoz del CEC, en un mundo que se sustenta en las infraestructuras de la información y la comunicación, estas se convierten en objetivos prioritarios de los "enemigos" de un Estado. "A menudo se cree que el ciberataque es algo adicional al ataque físico, pero ya no es así (...), no se puede subestimar", afirma Tüür.

La información clasificada almacenada en redes internas podría ser interceptada y usada con fines oscuros; los ordenadores que controlan centrales nucleares, eléctricas,

etcétera, bloqueados, paralizando así su actividad o interviniendo en ella; las bases de datos de hospitales y otras instituciones públicas, alteradas; los servicios Web de la Administración, colapsados. En definitiva, todo lo que sea susceptible de estar conectado a una red podría manipularse con diferentes herramientas informáticas. Las consecuencias serían muy diversas, "desde el robo de secretos de Estado al caos general de un país o la utilización de centros energéticos clave para causar atentados", explican fuentes de la OTAN.

En Redes también se aplica el dicho de que "La mejor defensa es la prevención", es por esto que se cuenta actualmente con una gama de marcas y equipos que se encargan de mantener la seguridad de nuestra red, en nuestro caso se tiene una gran cantidad de equipos que se encargan de analizar el trafico desde Internet hacia nuestra red para que no lleve virus, correos Spam, Troyanos, programas espías, entre otros.

La información que viaja de una red a otra de preferencia debe ser protegida ya se por protocolos de encriptación como IPSEC o usando una conexión VPN.

Otra forma de proteger la información transmitida por la red desde la capa de aplicación a través de túneles extremo a extremo a nivel de aplicación, son las aplicaciones SSH, Secure Shell (SSH). La interfaz de usuario es una línea de comandos segura de la capa de aplicación, inicialmente pensado para evitar el paso de contraseñas en las conexiones de telnet. Se considera el sustituto de los protocolos "r" (rsh, rcp, rlogin, ...) SSH es una aplicación especificada en drafts del IETF e implementa la parte de control a través del puerto 22.

Las funciones de SSH son, autenticación de equipos y usuarios (utilizando diferentes métodos de autenticación: RSA, Kerberos, ...), envío de contraseñas cifrados, permite generar canales X11 seguros para exportar pantalla por el uso de conexión cifrada, permite incorporar servidores externos de autenticación como Radius y Tacacs+, realiza el intercambio de claves públicas RSA, además que puede utilizar servidores de gestión de claves tanto con enfoque distribuido (claves en los equipos) como con enfoque centralizado (claves en una CA): certificados X.509.

¿Cómo defenderse de estos Ataques?

La mayoría de los ataques mencionados se basan en fallos de diseño inherentes a Internet (y sus protocolos) y a los sistemas operativos utilizados, por lo que no son "solucionables" en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes:

1. Mantener las máquinas actualizadas y seguras físicamente
2. Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
3. Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
4. No permitir el tráfico "broadcast" desde fuera de nuestra red. De esta forma evitamos ser empleados como "multiplicadores" durante un ataque Smurf.
5. Filtrar el tráfico IP Spoof.
6. Auditorias de seguridad y sistemas de detección.
7. Mantenerse informado constantemente sobre cada unas de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
8. Por último, pero quizás lo más importante, la capacitación continúa del usuario.

En este capitulo se han revisado las diversas técnicas de ataques que existen actualmente en Internet, así como las recomendaciones a fin de evitar que nuestra red sea victima de estos ataques, con esta información en el siguiente capitulo conoceremos los equipos que hacen posible mantener la seguridad y el control de nuestra red en lo concerniente al acceso a Internet, así como la configuración que se debe manejar en cada uno de ellos.

CAPITULO III
SISTEMAS DE MEDICIÓN Y CONTROL DE ACCESO A INTERNET

Después de analizar los distintos tipos de ataque a los que una red esta expuesta al conectarla hacia Internet revisaremos la diversidad de equipos y productos que se tienen actualmente en el mercado con la intención de protegernos de dichos ataques.

En este capitulo revisaremos las funciones de los equipos de seguridad en el acceso a Internet tales como el router, donde revisaremos la forma de configurar las reglas que realizan el bloqueo de una IP o URL, revisaremos el servidor Proxy y el Firewall, que en conjunto son la base de la seguridad de una red, así como los equipos gestores del ancho de banda de Internet entre otros.

3.1 Administración del acceso a Internet

La administración del acceso de una red a Internet se basa en aplicar los conocimientos de prevención de ataques adquiridos durante nuestra formación académica, si bien es cierto existe una serie de equipos que realizan las funciones de detección, análisis y eliminación de información no relevante al trabajo diario, también es necesario tener un equipo de personas que puedan administrar dichos dispositivos, monitorearlos, realizar estadísticas y proponer mejoras, así como estar a la vanguardia de los equipos usados en actualidad y hacerle un seguimiento a las nuevas versiones, los parches liberados y los upgrades necesario a fin de mantener un sistema de protección actualizado en nuestra red.

A continuación se detallaran algunos de los equipos más importantes en la medición y control del acceso a Internet donde se usan equipos tales como routers, equipos de seguridad perimetral como los Firewalls, servidores Proxies, Analizadores de ancho de banda de un enlace hacia Internet, servidores de reportes del consumo de recursos de Internet.

3.2 Routers

Es un dispositivo enrutador o encaminador que nos sirve para interconectar redes de ordenadores y que actualmente implementan puertas de acceso a Internet como son los router para ADSL, los de Cable o 3G.

Son ya hoy por hoy en su mayoría dispositivos de Hardware desarrollados por fabricantes como Cisco o Juniper y cuyo software esta desarrollado por esas mismas empresas, aunque también pueden ser ordenadores implementados con los protocolos de red (RIP, OSPF, IGRP, EIGRP y BGP) para los cuales existen ya paquetes (normalmente de software libre) con los distintos Drivers como pueden ser: Quagga, Vyatta, Zebra o ZebOs.

Es decir, si una persona tiene solo un ordenador lo normal sería que tuviera un modem que serviría para conectarse a Internet a través de la red de un proveedor en el caso que nos ocupa, pero si se tiene más de un ordenador lo habitual es que se tenga un router para que la red pueda conectarse a la red del proveedor y este se conecte a Internet compartiendo el ancho de banda que se haya contratado entre los distintos ordenadores de la red. De esta manera el router se convierte en el intermediario entre la red local e Internet.

Para ello el router posee dos direcciones IPS, una la IP pública que nos otorga nuestro proveedor que pueden ser tanto estática (que es siempre la misma) como dinámica (que cambia aleatoriamente en función de las necesidades de nuestro proveedor) que suelen ser la mayoría; y otra IP privada que es la que tiene o le damos para nuestra red interna o local y que nos servirá para centralizar las comunicaciones entre nuestras distintas máquinas u ordenadores.

Partiendo de aquí lo que cobra especial importancia es el software con el cual controlaremos nuestra red. Debe de tener sistemas de seguridad para evitar los ataques extemos procedentes de Internet, permitirnos el control del ancho de banda que tenemos para repartir ya sea entre distintas aplicaciones u ordenadores, y regular el tráfico de nuestra red de la manera más sencilla.

Lógicamente los Routers hechos por fabricantes ganan esta carrera, y como es normal hay fabricantes, y fabricantes como ocurre en el mundo de los ordenadores personales. El que mayor fama y reputación tiene hoy por hoy es Cisco sobre todo a raíz de la adquisición de Linksys (marca aun existente pero que en breve será sustituida oficialmente por Cisco) que viene a ser como la marca Apple para el mundo de la informática personal, es decir, que marca la diferencia.

Linksys (ahora Cisco) fue una empresa pionera en añadir determinadas opciones o funciones a sus Routers no profesionales como es la tecnología QoS, DMZ, entre otros.

Modos del router

La mayoría de los cambios de configuración, tanto en routers como en switches de Cisco, se hacen en el modo de configuración global. Para este fin, primero se debe dar la orden:

Router> enable

con lo cual se entra al modo privilegiado, y el prompt cambia a Router#. Luego, se da la orden:

Router# configure terminal

con lo cual se entra al modo de configuración global, y el prompt cambia a Router(config)#.

De aquí, se cambia a modos de configuración específicos, por ejemplo, al modo de interface, de sub-interface,

En los ejemplos anteriores, no se ha incluido el prompt del router, suponiendo que éste se llama "Router". El prompt aparece en pantalla; no se le debe escribir como parte del comando. Sin embargo, es importante saber en qué modo se dan determinados comandos.

Manejo de la configuración

Para fines de prácticas, es conveniente borrar la configuración previa del router. (Esto no se recomienda para un router usado en una red de uso real.)

En el modo privilegiado:

Router# erase startup-config

Router# reload

Después de hacer cambios, se puede guardar la configuración, para que no se pierda al reiniciar el router:

Router# copy running-config startup-config

Es recomendable también realizar copias de seguridad de la configuración actual antes de realizar cambios o modificaciones de las reglas que actualmente maneja el router o el switch a configurar.

Comandos comunes de configuración

Nombre del router.- Cuando se tienen varios routers, es conveniente que cada router tenga un nombre distintivo; esto ayuda a evitar confusiones.

Router# hostname Router_X

Configuración básica de interfaces

Las interfaces tienen nombres que se pueden abreviar como F0 (o F0/0) para FastEthernet, S0 para seriales, etc.

Para cada interfaz, se debe hacer lo siguiente:

! Seleccionar la interfaz

Router(config)# interface S0

! Habilitar la interfaz

Router(config-if)# no shutdown

! Asignar una dirección IP

Router(config-if)# ip address 10.0.1.2 255.255.255.0

! Sólo para el extremo DCE de interfaces seriales, fijar la velocidad:

Router(config-if)# clock rate 64000

Para asignar las direcciones IP, se debe recordar que diferentes interfaces de un router están en diferentes subredes; mientras que dos extremos de una comunicación (por ejemplo, dos interfaces seriales de dos routers, conectados entre sí), están en la misma subred.

Habilitar el enrutamiento

Los routers tienen que aprender las rutas de redes que no están directamente conectadas a dichos dispositivos. La manera más fácil de lograr esto es habilitando un protocolo de enrutamiento en cada router involucrado. Ejemplo para RIP:

! Habilitar enrutamiento IP; debería estar habilitado por default, pero no siempre lo está

Router(config)# ip routing

! Seleccionar un protocolo de enrutamiento

Router(config)# router rip

! Especificar redes directamente conectadas

Router(config-router)# network 10.0.0.0

Se indica, con una o más órdenes network, las redes directamente conectadas al router. En el caso de RIP, se usan redes de las clases A, B y C.

3.2.1 Listas de acceso IP

Las listas de acceso se utilizan para controlar y gestionar el acceso de tráfico de interés para la red y de tráfico no deseado. Las listas de acceso son herramientas poderosas usadas para controlar el acceso hacia y desde segmentos de red. Se pueden filtrar los paquetes poco interesantes y ser usados para aplicar las políticas de seguridad. Utilizando la combinación adecuada de listas de acceso, los administradores de la red tendrán las herramientas necesarias para hacer cumplir casi cualquier política de acceso que se pueda inventar. Después que las listas son construidas, se pueden aplicar a cualquiera interfaz de tráfico entrante o saliente. Mediante la aplicación de listas de acceso al router se puede activar el análisis de cada paquete que cruza una interface específica y también se pueden tomar las medidas de seguridad necesarias.

Tipos de listas de acceso IP

Existen dos tipos de listas de acceso, las listas de acceso Standard y las listas de acceso extendidas:

Listas de acceso estándar:

Las listas de acceso IP estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

Listas de acceso extendidas:

Las listas de acceso extendidas comprueban tanto la dirección de origen como la de destino de cada paquete. También pueden verificar protocolos especificados, números de puerto y otros parámetros.

Una vez creada, una ACL debe asociarse a una interfaz de la siguiente manera:

Lista de acceso entrante:

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento

Lista de acceso saliente:

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión.

Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido para los paquetes que entran en interfaces de entrada, paquetes que se trasmiten por el router, y paquetes que salen de las interfaces de salida del router.

Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones Telnet salien es o los protocolos de enrutamiento propios de los routers.

3.3 Firewalls

Un firewall es un sistema que está configurado para controlar el flujo de tráfico entre dos redes. Los cortafuegos son comúnmente configurados de manera especial en sistemas Unix, pero los cortafuegos también se han construido fuera de muchos otros sistemas, incluidos los sistemas diseñados específicamente para su uso como cortafuegos. Uno de los equipos que realiza todas las funciones de un firewall y de gran rendimiento es el Firewall de la marca CheckPoint, pero competidores como Cisco PIX están ganando terreno rápidamente en este rubro de seguridad.

También es frecuente conectar a los cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior como se indica en la Fig. 3.1.

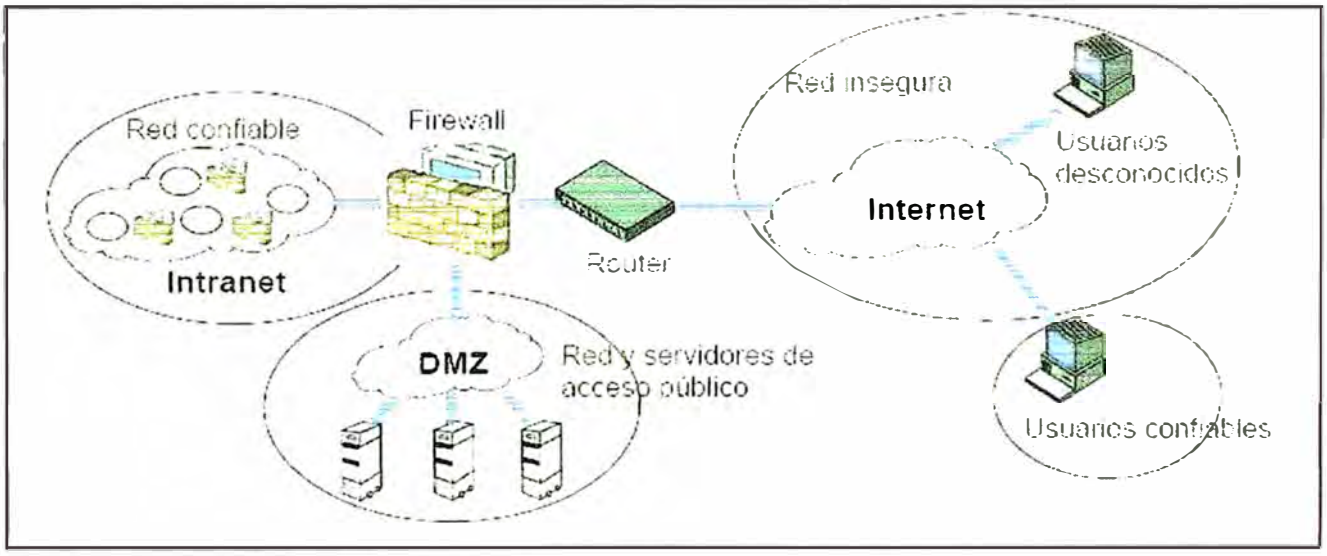


Fig. 3.1 Ubicación del Firewall en una red

Ventajas de un cortafuegos

- Protege de intrusiones El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
- Protección de información privada. Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
- Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Limitaciones de un cortafuegos

- Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (diskettes, memorias, etc) y sustraigan éstas del edificio.
- El cortafuegos no puede proteger contra los ataques de Ingeniería social
- El cortafuegos no puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por cualquier medio de almacenamiento u otra fuente.
- El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

Tipos de cortafuegos

Hay dos tipos según la arquitectura: A nivel de hardrware. A nivel de software.

A nivel de Hardware se refiere a las cajas de las distintas marcas que ya vienen configuradas para cumplir las funciones de filtros en la red, administradas por una consola en su mayoría de tipo Web.

A nivel de Software se refiere a un sistema operativo que puede ser editado a fin de configurar nuestras propias políticas de acceso y restricción en la red, un ejemplo de este

tipo de Firewall es el Firewall de Linux que además de poder ser un equipo Proxy puede ser un firewall basándose en el uso de listas de acceso de seguridad similares a las de un router.

Políticas de los cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- Política *restrictiva*: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- Política *permisiva*: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

El Firewall usado en este informe corresponde a un Firewall de la Marca Checkpoint, equipo conocido por su uso práctico y potencia en el análisis de tráfico. El Firewall Checkpoint utiliza las siguientes consolas de monitoreo:

Check Point

Check Point Software Technologies Ltd. (Nasdaq: CHKP) es líder mundial asegurando Internet con sus soluciones Firewall/VPN. La arquitectura de redes virtuales seguras (SVN) de la compañía proporciona la infraestructura necesaria para realizar comunicaciones seguras y fiables en Internet. Esta arquitectura, involucrada en la familia de productos "Next Generation", asegura las comunicaciones y los recursos en las redes corporativas y sus relaciones con empleados remotos, sucursales y socios de negocios.

La administración del Firewall en mención es llevada a cabo desde las consolas de administración que posee el producto las cuales se indican en la figura Fig. 3.2, en dicha figura podemos observar el SmartView Tracker que es la herramienta principal de monitoreo mediante la cual se puede realizar un seguimiento a una determinada dirección IP ya sea de entrada o de salida y se puede observar a que direcciones se ha conectado en las últimas horas y por que puertos, con este análisis el administrador puede tomar medidas sobre esta dirección IP consultada a fin de optimizar la regla que maneja en el firewall ya sea cerrando puertos o restringiendo direcciones que no son necesarias para su funcionamiento.

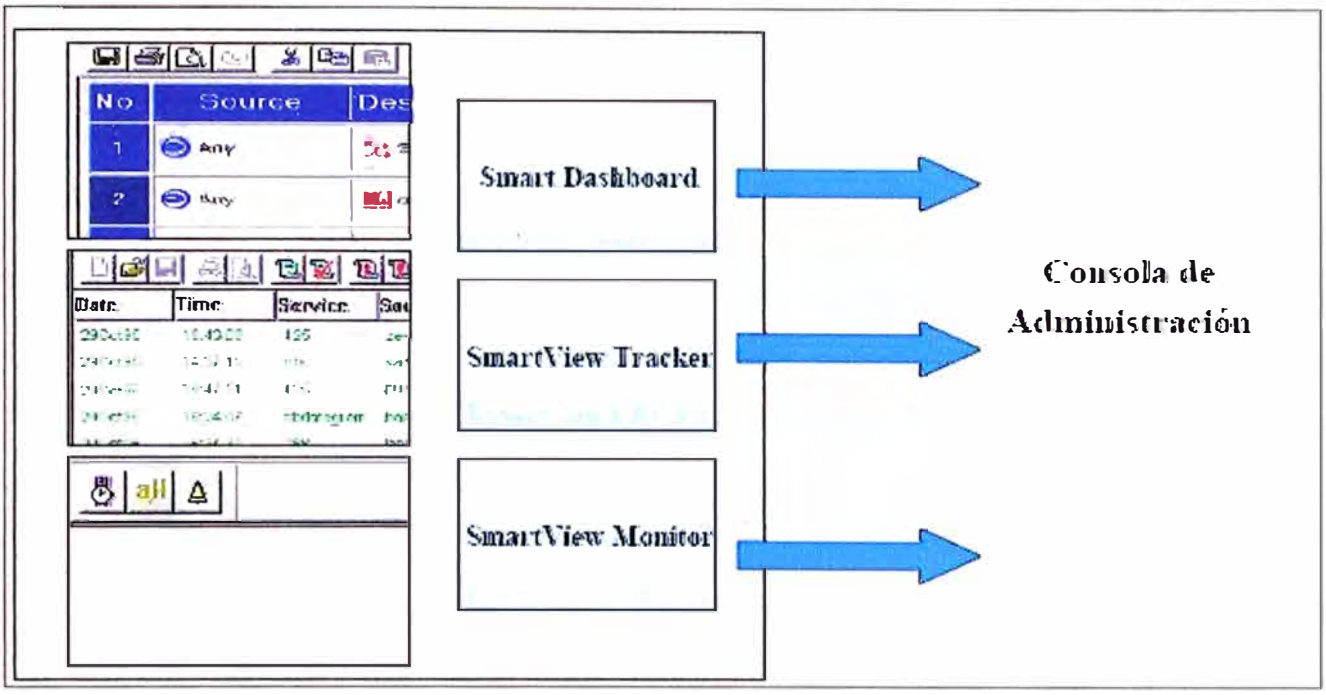


Fig. 3.2 Consolas de administración del Checkpoint

Check Point NGX Application Intelligence R60

Última generación en sistemas Firewall del líder mundial Check Point Technologies que es, hasta la fecha, el mayor pasó que ha dado el fabricante en su evolución como proveedor líder de seguridad en Internet.

NGX es la plataforma de seguridad unificada para las soluciones de Check Point de seguridad interna, perimetral y Web, cuya misión es reducir el costo y la complejidad de la seguridad de las empresas de todos los tipos y garantizar que dichos sistemas de seguridad se puedan ampliar para hacer frente a cualquier amenaza.

La principal aportación de la plataforma NGX, es cambiar la forma en que las empresas conciben sus despliegues de seguridad al conjugar una mayor, más amplia e inteligente protección a todo nivel (End –to– End) a través de una arquitectura de seguridad unificada.

Al mismo tiempo, con NGX, Check Point aúna seguridad y conectividad pues la nueva plataforma incorpora el 100% de las funcionalidades de un router (SecurerPlatform Pro) con objeto de permitir a las empresas gestionar las redes más sofisticadas de forma mucho más efectiva y con menos recursos.

NGX provee gestión unificada de la seguridad perimetral, interna y Web, reduciendo los costos de la gestión de seguridad al permitir al administrador definir y gestionar

centralmente las políticas desde una única consola. La incorporación de nuevas capacidades en el módulo Intelligent Inspection protegen más aplicaciones y redes de amenazas con el fin de asegurar la confidencialidad, disponibilidad y la integridad de la información crítica empresarial.

NGX incluye avanzadas capacidades VPN entre las que destaca un router dinámico (SecurePlatform Pro) que permite a las empresas gestionar grandes y complejos entornos de red. Check Point es el único fabricante que proporciona una plataforma unificada para toda su línea de productos y en todos los niveles de red.

3.4 Servidor Proxy

¿Qué es un servidor Proxy? Un servidor Proxy es un dispositivo de red que gestiona el tráfico entre su red local y los servidores en Internet, y determina si los paquetes de información se les permiten pasar a través de la red. Cuando un equipo cliente hace una petición, el Proxy traduce la petición y la transmite a Internet previa autenticación y validación de permisos. Cuando un ordenador en Internet responde, el servidor Proxy pasa la respuesta al ordenador cliente.

Restringir Conexiones

Puede configurar un servidor Proxy para bloquear las conexiones entrantes a fin de permitir que los clientes LAN a iniciar las conexiones a servidores de Internet, sino también evitar que los clientes de Internet de iniciar las conexiones a servidores de la LAN. También se puede configurar un servidor Proxy para limitar las conexiones salientes a fin de que los clientes LAN sean autenticados mediante el uso de sus credenciales de seguridad estándar.

Puede restringir las conexiones salientes de varias maneras-por el usuario, programa, protocolo, TCP / UDP número de puerto, la hora del día, el nombre de dominio o dirección IP.

Caché de Información

Los servidores Proxy caché de información general de la Internet. Por ejemplo, si varios usuarios ver la misma página Web en Internet, un servidor Proxy que puede recuperar solamente una vez la página de Internet, conservar una copia de la página en su caché y, a continuación, remitir la copia a todos los usuarios. Esto reduce el tráfico entre su intranet y la Internet debido a que el Proxy no tiene que recuperar la página Web de la Internet por separado para cada usuario.

Squid.

Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes. Al iniciar Squid da origen a un número configurable de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS.

3.5 Gestor de ancho de banda: Packetshaper

PacketShaper es una solución de gestión de ancho de banda con la que poder administrar y controlar las aplicaciones utilizadas en las redes WAN (Wide Area Network). Este producto de Packeteer transmite los datos más relevantes a una velocidad constante, mientras que aquellos datos que no son tan indispensables circulan por una parte más pequeña del ancho de banda disponible. Estas características de PacketShaper hacen que ningún tipo de tráfico monopolice el enlace. Entre las aplicaciones en las que esta herramienta de gestión se puede emplear están ERP, streaming media, VoIP y bases de datos, entre otras.

La línea de productos PacketShaper está compuesta por cuatro modelos que son PS 1500 para líneas de hasta 128 y 515 Kbps ó 2Mbps; PS 2500 para líneas de hasta 2 ó 10 Mbps; PS 4500 hasta 45 Mbps; y PS 6500 para aquellas líneas que alcancen los 100 Mbps. En la figura Fig. 3.3 observamos las características físicas de un equipo analizador de ancho de banda modelo 7500.

Fig. 3.3: Packetshaper modelo 7500

El Packetshaper puede realizar las funciones de Monitoring, Shaping, Compression y Aceleration, siendo estas 3 funciones los pilares de su administración y optimización del uso del ancho de banda un enlace, ya sea hacia Internet o hacia otra sede.

Monitoring

La monitorización es el software básico que viene en cada uno de los equipos. Se encarga de la visualización de la cantidad y del tipo de tráfico que está pasando por la red. Con el monitoring podemos tener la información del consumo de ancho de banda del que se hace uso, y sobre todo con qué tipo de tráfico se está consumiendo el ancho de banda.

El PacketSeeker nos da información en tiempo real no sólo del tipo de tráfico que está pasando por la red, si no además de la aplicación que se está ejecutando.

Shaping

La parte de shaping es el software que permite controlar el tráfico descubierto por la parte de monitorización y establecer prioridades para el uso de las aplicaciones.

Permite definir prioridades en la utilización de nuestra red.

Con el Shaping seremos capaces de organizar el tráfico existente en nuestra red y dar un alto rendimiento a las aplicaciones que lo necesiten. El Shaping es capaz de bloquear tráfico en nuestra red para que aplicaciones de uso no comercial como Kazaa, Gnutella o mensajerías instantáneas no sean utilizadas y perjudiquen el ancho de banda de las aplicaciones de producción.

El Shapping es la característica más usada del Packetshaper debido a que con esta opción podemos reservar amplios anchos de banda para aplicaciones útiles a la empresa y limitar los anchos de banda para las aplicaciones que no tienen un fin productivo sobre la misma, identificando también los distintos protocolos que atraviesan nuestro enlace y aplicando reglas de optimización sobre los mismos.

Compression

El módulo de compresión hace que los datos pasados a través del packetshaper sean de menor tamaño y como consecuencia el uso del ancho de banda sea menor.

El módulo de compresión hace que el tráfico susceptible de recibir esta característica se comprima y ocupe menos acho de banda al ser enviado.No comprimirá tráficos que por sus características no deban ser comprimidos ya que las funciones de compresión-descompresión decelerarían el rendimiento. Un ejemplo de este tipo de tráfico sería VoIP. La compresión se hace siempre entre dos appliances de packeteer

Con la compresión aceleramos el tráfico Wan.

Aceleration

La aceleración se encargará de optimizar las conexiones tcp entre los dos sitios interponiéndose entre los servidores y los clientes y haciendo que las latencias existentes en la red se mitiguen y se pueda llegar a trabajar en la Wan casi como en la Lan.

Existen diversos modelos de Packeshapers, entre ellos tenemos los equipos descritos en el siguiente cuadro Fig. 3.4, el equipo usado en el presente análisis corresponde a un Packetshaper modelo 3500, el cual soporta un análisis de ancho de banda para enlaces menores a 45Mbps manejando un máximo de 512 clases configurables a fin de limitar el uso de cada protocolo identificado por el dispositivo.

PACKETSHAPER MODELS SPECIFICATIONS

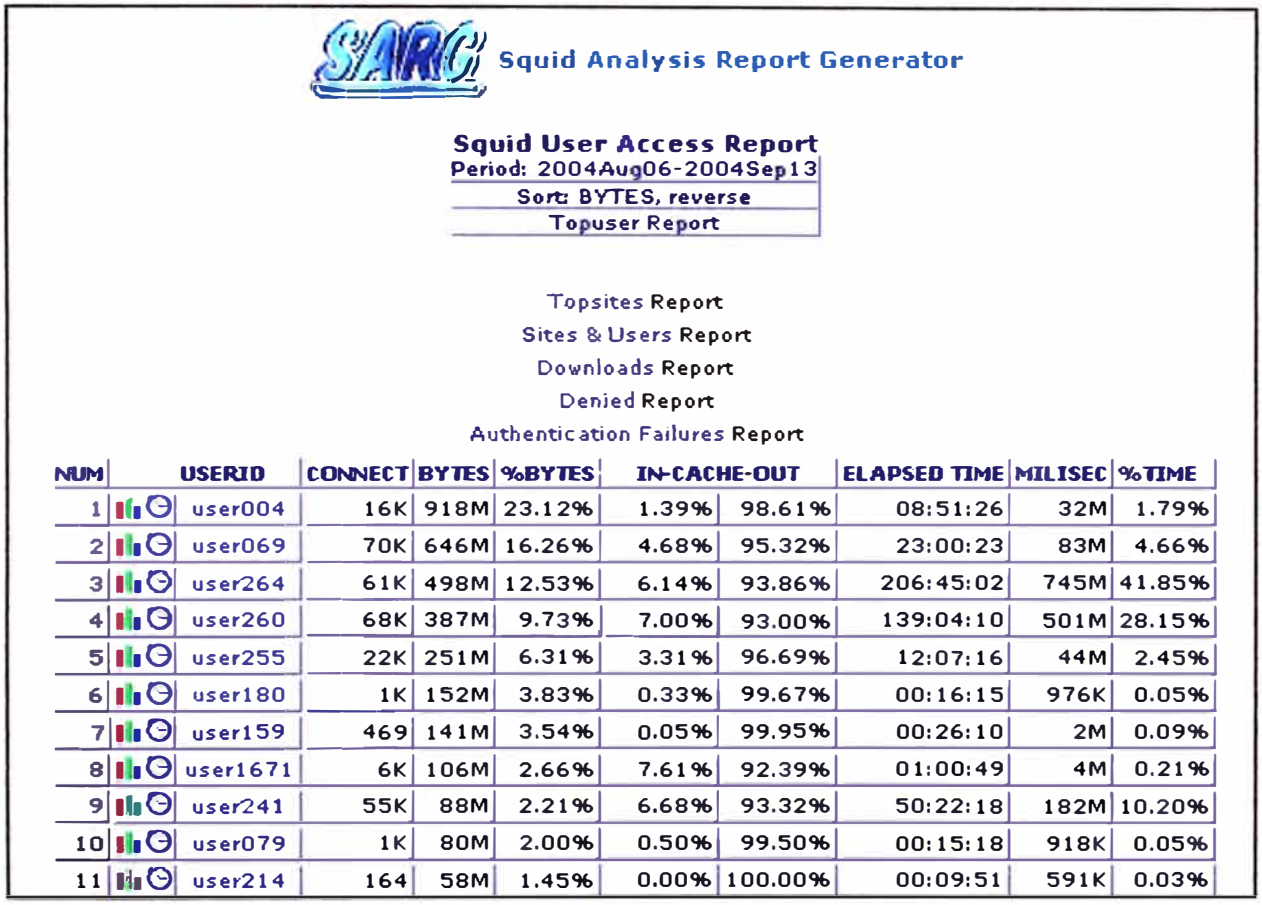
PacketShaper	900	1400	1700	3500	7500	10000
Maximum Classes	256	256	512	512	1024	2048
Maximum Concurrent Flows	5K	5K	30K/15K	40K/20K	200K/100K	400K/200K
Maximum Throughput	2 Mbps	2 Mbps	45 Mbps	45 Mbps	200 Mbps	1 Gbps
Maximum Compression Tunnels	10	10	15	30	100	1000

Fig. 3.4 Especificaciones técnicas del Packetshaper

3.6 Servidor de reportes de navegación: SARG

Sarg es un programa para ver los informes de uso del Squid de una red. En palabras de su programador: Sarg es un Squid Analysis Report Generator que nos permite ver a "dónde" están navegando los usuarios dentro de Internet. Sarg genera informes en html, con muchos campos, como: usuarios, Direcciones IP, bytes transmitidos, sitios Web and tiempos.

La información procesada por SARG es obtenida de los logs de navegación del servidor Proxy o Squid, se pueden programar con la ejecución de dichos reportes en lapsos de una semana o un mes y se obtienen cuadros que pueden ser analizados a fin de observar a los usuarios tops o las paginas de contenido no laboral accedidas.



Squid Analysis Report Generator

Squid User Access Report
Period: 2004Aug06-2004Sep13
Sort: BYTES, reverse
Topuser Report

Topsites Report
Sites & Users Report
Downloads Report
Denied Report
Authentication Failures Report

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	user004	16K	918M	23.12%	1.39%	98.61%	08:51:26	32M	1.79%
2	user069	70K	646M	16.26%	4.68%	95.32%	23:00:23	83M	4.66%
3	user264	61K	498M	12.53%	6.14%	93.86%	206:45:02	745M	41.85%
4	user260	68K	387M	9.73%	7.00%	93.00%	139:04:10	501M	28.15%
5	user255	22K	251M	6.31%	3.31%	96.69%	12:07:16	44M	2.45%
6	user180	1K	152M	3.83%	0.33%	99.67%	00:16:15	976K	0.05%
7	user159	469	141M	3.54%	0.05%	99.95%	00:26:10	2M	0.09%
8	user1671	6K	106M	2.66%	7.61%	92.39%	01:00:49	4M	0.21%
9	user241	55K	88M	2.21%	6.68%	93.32%	50:22:18	182M	10.20%
10	user079	1K	80M	2.00%	0.50%	99.50%	00:15:18	918K	0.05%
11	user214	164	58M	1.45%	0.00%	100.00%	00:09:51	591K	0.03%

Fig. 3.5 Reporte obtenidos por SARG

Sarg es un generador de reportes de análisis de Proxy Squid, el cual permite ver “a donde” los usuarios han navegado a través de su acceso a Internet.

Sarg genera reportes en formato HTML, con cualquier campo, así como: usuario, *dirección IP, bytes, sitios y horas, etc.*

Requisitos.

Se asume *que los paquetes requeridos ya han* sido instalados y configurados

adecuadamente y que están funcionando correctamente.

- Squid-2.5.STABLE1-2.rpm o superior
- Httpd-2.0.40-21.rpm o superior
- Sarg-1.4.1-5.0.rpm o superior

Para instalar los programas ejecutamos el siguiente comando:

rpm -ivh [paquete rpm]

ej.:

rpm -ivh httpd-2.0.40-21.rpm

rpm -ivh squid-2.5.STABLE1.2.rpm

rpm -ivh sarg-1.4.1-5.0.rh9.dag.rpm

Ubicación de los archivos:

ejecutable sarg /usr/bin/sarg

configuración /etc/sarg/sarg.conf

cd sarg

Archivos a modificar:

/etc/sarg/sarg.conf

Este es el archivo de configuración del programa Sarg, aquí se le define la ubicación de los archivos logs de Squid donde pondrá la salida y como será la presentación. A continuación se presenta el archivo modificado que se esta utilizando en el servidor: Archivo Sarg.conf sugerido para generar reportes semanales:

#

language English

access_log /var/log/squid/access.log

title "Reporte Acceso Internet por Usuario"

output_dir /var/www/html/squid

date_format u

lastlog 5

overwrite_report yes

topsites_num 100

max_elapsed 28800000

report_type topsites sites_users users_sites date_time denied auth_failures

site_user_time_date

show_successful_message no

topuser_fields NUM DATE_TIME USERID CONNECT BYTES %BYTES IN-CACHE-OUT USED_TIME MILISEC %

TIME TOTAL AVERAGE

user_report_fields CONNECT BYTES %BYTES IN-CACHE-OUT USED_TIME MILISEC %TIME TOTAL AVERAGE

site_user_time_date_type table

3.7 Antivirus

Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

Un antivirus tiene tres principales funciones y componentes:

- VACUNA es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en tiempo real.
- DETECTOR, es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de control y reconocimiento exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.

- ELIMINADOR es el programa que una vez desactivada la estructura del virus procede a *eliminarlo* e *inmediatamente* después a *reparar* o *reconstruir* los *archivos* y *áreas* afectadas.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los *códigos* (*también* conocidos como *firmas* o vacunas) de los virus conocidos, *por* lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

Actualmente a los antivirus se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como Heurística) o la verificación contra virus en redes de computadoras.

Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador Web (ActiveX, Java, JavaScript).

Los *virus*, *gusanos*, *spyware*, *troyanos*, entre otros, son *programas* informáticos que se ejecutan normalmente sin el consentimiento del legítimo propietario y que tienen la característica de ejecutar recursos, consumir memoria e incluso eliminar o destrozar la *información*.

Una característica adicional es la capacidad que tienen de propagarse. Otras características son el robo de información, la pérdida de esta, la capacidad de suplantación, que hacen que reviertan en pérdidas económicas y de imagen.

Existen diversidad de marcas para los antivirus, entre ellas tenemos:

- Avast

- Nod32

- Panda Antivirus

- McAfee Virus Scan

- Norton antivirus

- AdWare

- Symanstec Antivirus

- Etc

En el presente capitulo hemos revisado los distintos tipos de equipos que en conjunto brindan la seguridad del acceso hacia Internet de una empresa, con esta configuración trabajaremos en el análisis y presentación de los resultados de las mediciones realizadas en el transcurso de una semana en una red corporativa de una empresa con cerca de 2000 usuarios.

En el siguiente capitulo observaremos los resultados de dichas mediciones y las mejoras que se pueden aplicar con el fin de optimizar el uso del acceso a Internet de dicha red.

CAPITULO IV
ANALISIS Y PRESENTACION DE RESULTADOS

Después de conocer los distintos equipos que en conjunto otorgan al seguridad al acceso a Internet pasaremos a revisar las configuraciones realizadas en las pruebas de medición realizadas sobre la empresa corporativa que maneja sistemas como el correo, el SAP, Oracle, SQL, Internet, entere otros, las configuraciones son realizadas en el Firewall, en el servidor Proxy, así como los equipos de administración del ancho de banda y de ejecución de reportes de navegación.

En este capitulo observaremos las configuraciones realizadas, así como los valores encontrados y las sugerencias de mejoras de optimización que se dan para estos casos.

4.1 Análisis descriptivo de la información relativa a las variables de estudio

Para el análisis del acceso a Internet a medir se configuraron los siguientes parámetros en los equipos de comunicación que forman parte de la red de datos:

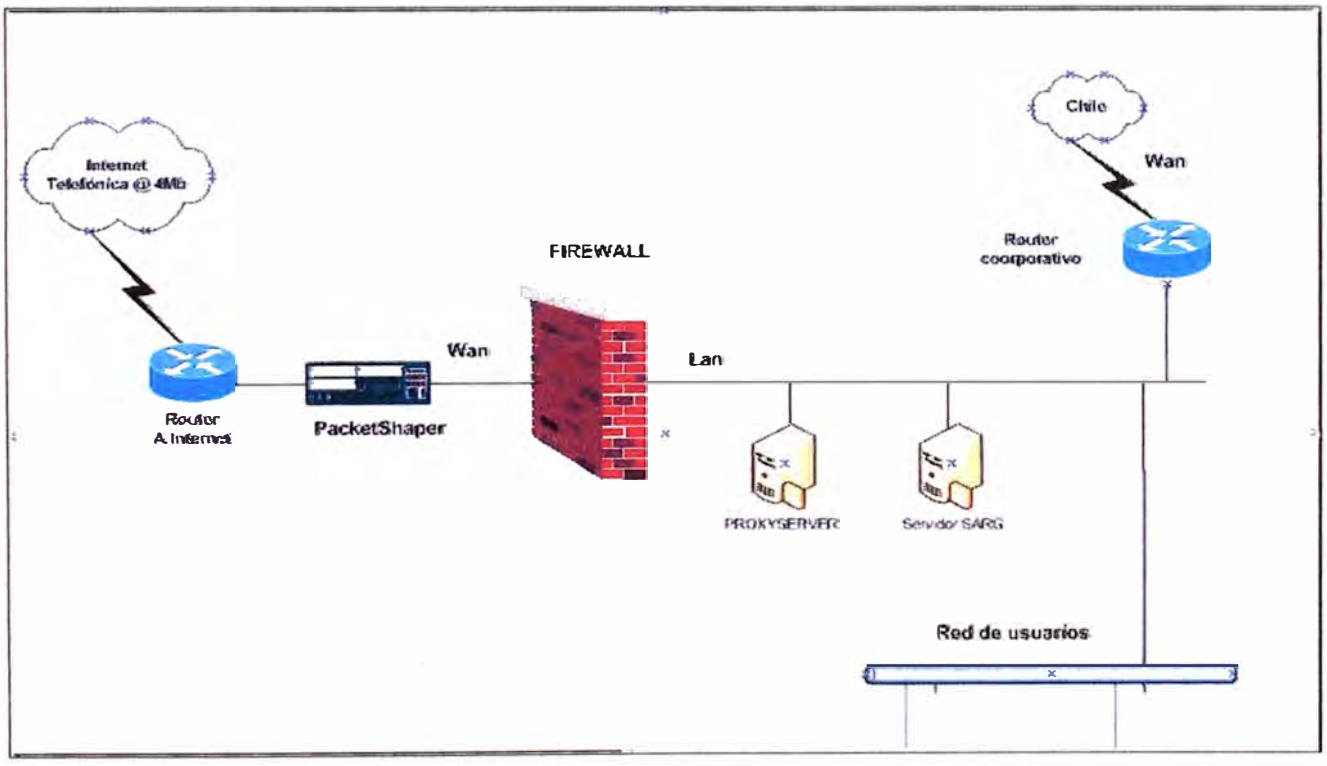


Fig. 4.1: Diagrama de red de la empresa a analizar

4.1.1 Configuración realizada en el Packetshaper

Básicamente el análisis inicial indica que el mayor consumo del enlace hacia Internet es utilizado por la navegación a nivel del puerto 80 (HTTP), seguido por el correo y el Firewall:

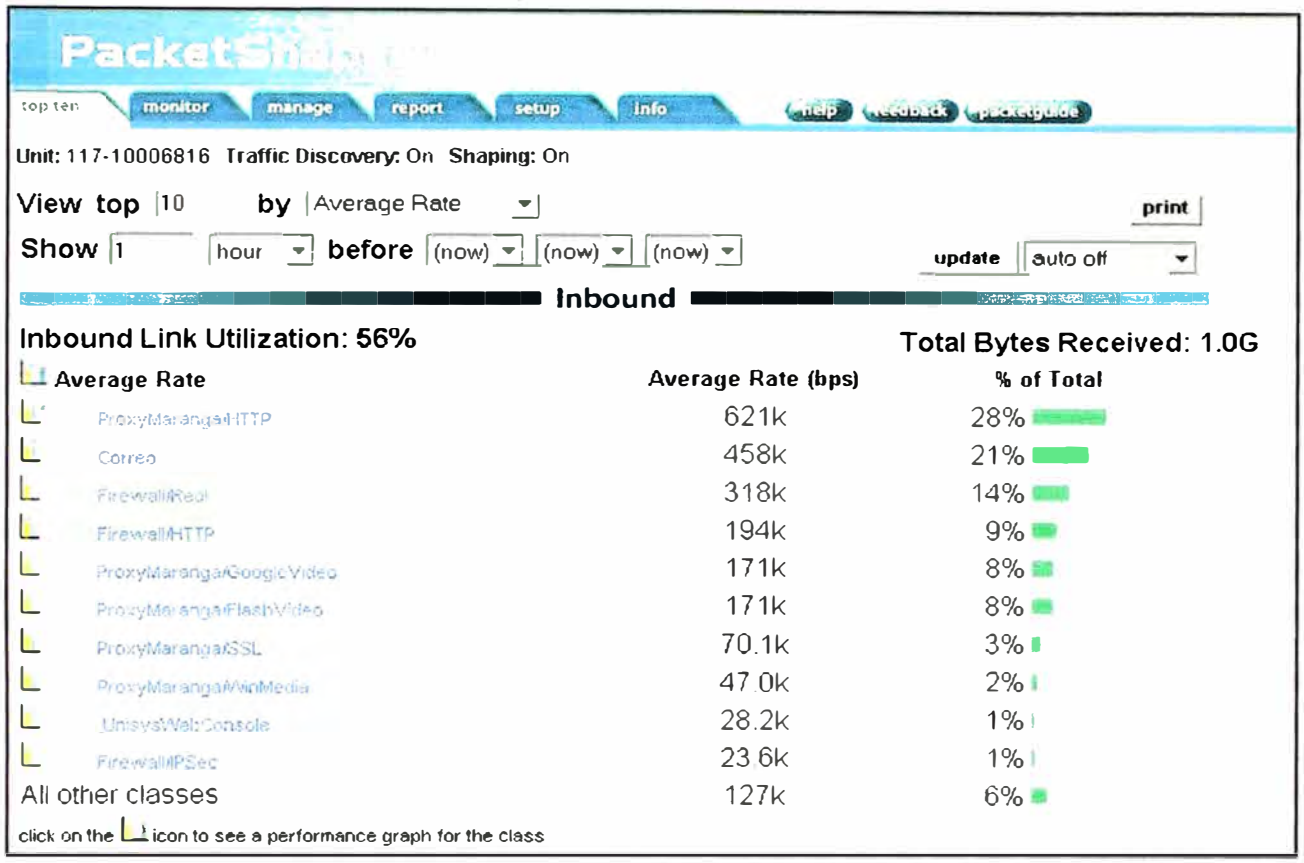


Fig. 4.2 Uso de las aplicaciones a nivel local

Bajo esta premisa inicialmente descubierta se puede configurar una clase a fin de limitar el uso de la navegación entre un valor aminito y un máximo, para este caso se configura como valor mínimo 0Mb y como valor máximo 1.6Mb, si en un punto de trabajo la red necesita crecer más allá de este valor el acceso a Internet sufrirá una lentitud por formarse un cuello de botella en este punto.

En la siguiente figura, Fig.4.3, se observa los formatos que viajan a través del puerto 80 y son detectados por el servidor Proxy, así como los valores de 0Mb y 1.6Mb seteados para esta clase: Las clases no solo pueden ser configuradas para el acceso Internet, puerto 80, si no también para protocolos o sistemas que se desean administrar y hayan sido detectados por el Packetshaper, de ser así se configura la clase y se configuran a su vez los limites para cada una de las aplicaciones identificadas.

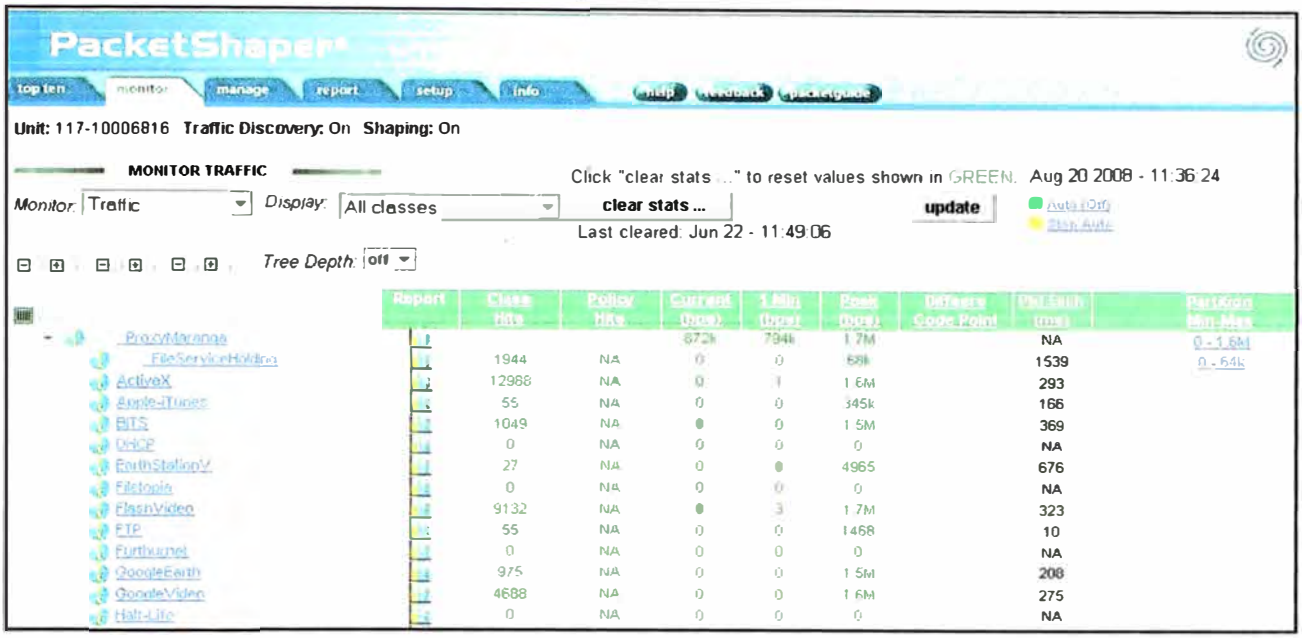


Fig. 4.3 Clase del Proxy configurada en el Packetshaper

4.1.2 Configuración realizada en el Firewall

Básicamente en el Firewall se define una regla que indique que el servidor Proxy tiene salida a Internet a través de los puertos 80 y 443, que son los puertos de navegación y navegación segura usada por algunas paginas webs, adicionalmente a estos 2 puertos se podría habilita algún otro puerto debido alguna situación especial que lo acredite.

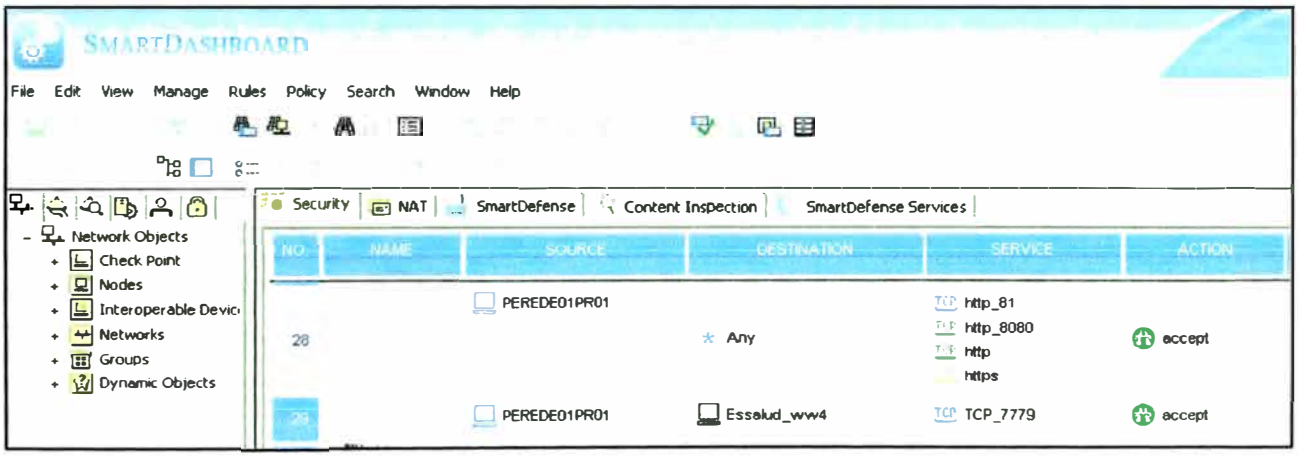


Fig. 4.4 Configuración del servidor Proxy en el Firewall de la red

4.1.3 Configuración realizada en el servidor Proxy

Después de instalar el Squid sobre el servidor se tienen que configurar los grupos a permitir y a bloquear dentro de la red, para ello se genera una estructura de archivos que

son accedidos por el demonio del programa Squid instalado en el servidor con sistema operativo Linux.

Básicamente el archivo que maneja las operaciones de aceptación o denegación de acceso a las URLs de Internet es el archivo squid.conf el cual se ubica en la ruta /usr/local/squid/etc/squid.conf.

Los archivos que se configuraron para este caso tienen la siguiente forma:

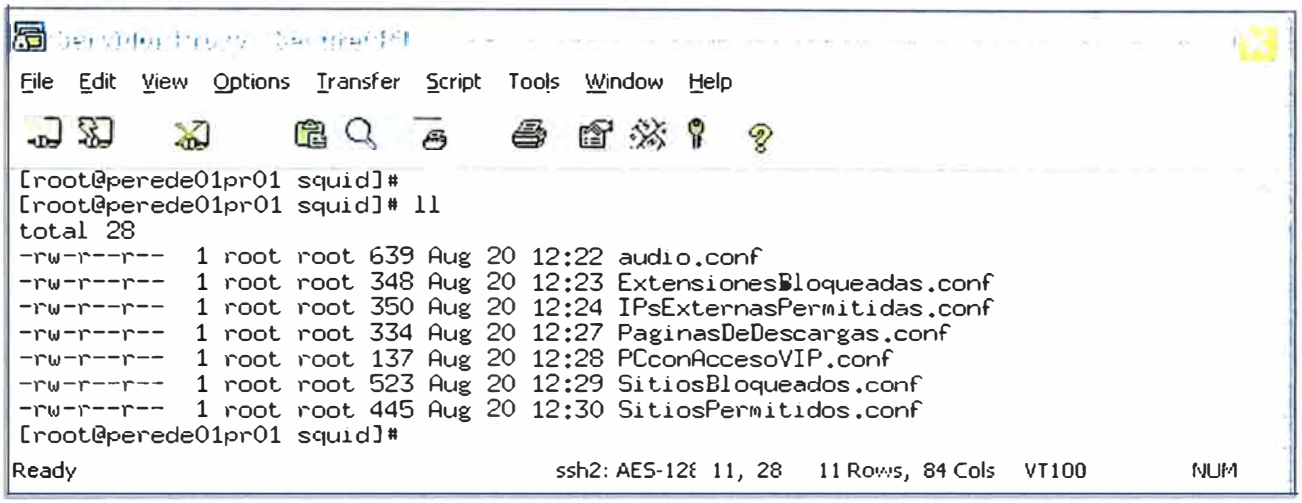


Fig. 4.5 Archivos configurados en el servidor Proxy

Donde audio.conf corresponde a las direcciones públicas que son repositorios de música en Internet:

Fig. 4.6 Direcciones públicas que son repositorios de música en Internet

Adicionalmente el archivo ExtensionesBloqueadas.conf corresponde a la serie de extensiones que deben ser filtradas en nuestra red debido a lo potencialmente peligrosas que son, tal es el caso de extensiones de tipo *.exe, *.vbs, *.dll, o extensiones de índole no laboral como *.mp3, *.avi. *.wav

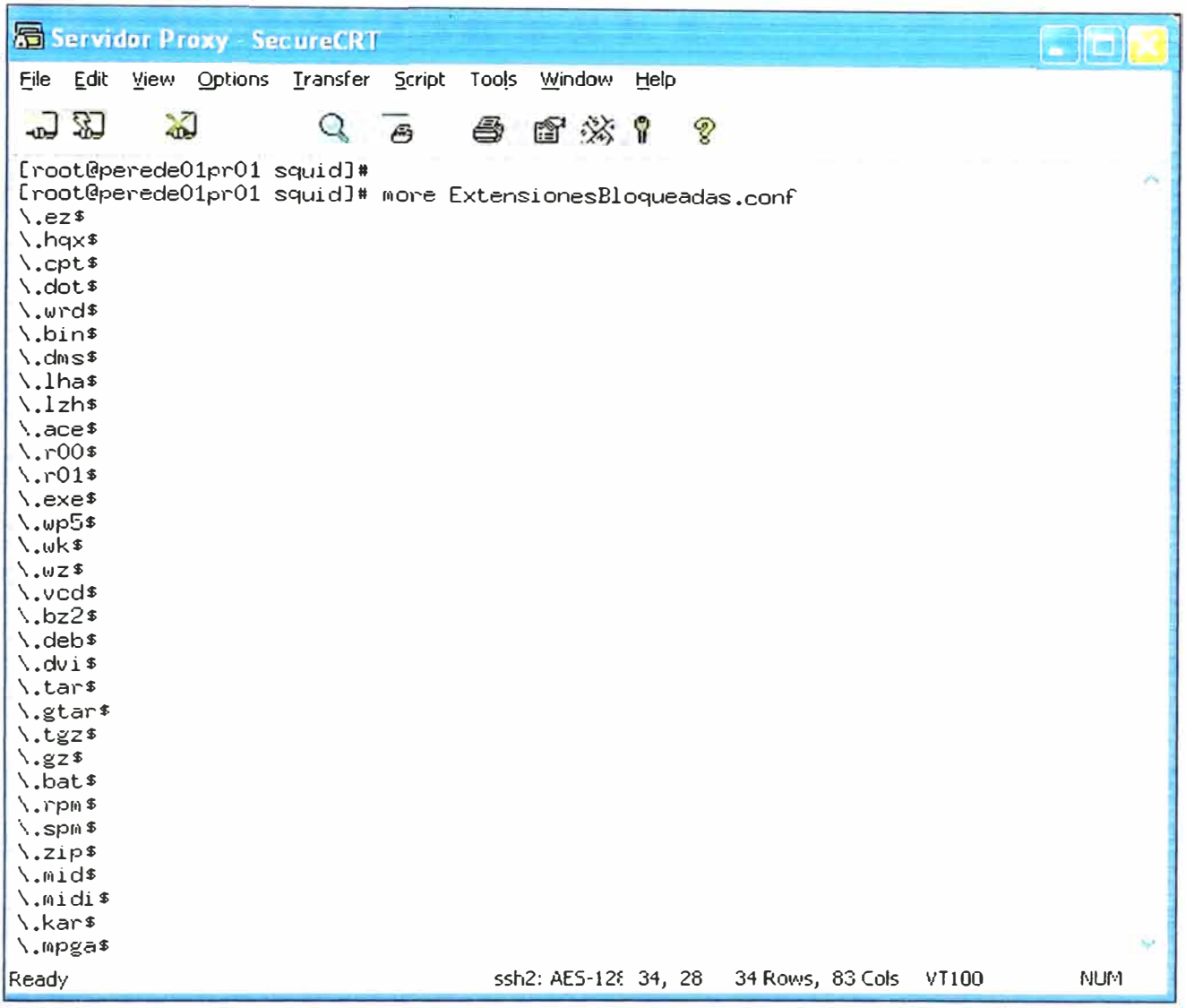


Fig. 4.7 Archivos de extensiones a filtrar en la red

Así mismo existe un archivo con las páginas webs o dominios que deben ser filtrados en nuestra red a fin de que no se instalen programas espías, Spyware, virus o simplemente información de tipo no laboral. Este archivo es uno de los más importantes en la configuración del Squid dado que en el indicamos las paginas de contenido no laboral a bloquear, dichas paginas pueden obtenidas por la revisión de los reportes periódicos o por la actualización con listas negras obtenidas desde Internet, cualquier página Web

que se publique en este archivo será bloqueada automáticamente de nuestra red y un registro del intento de acceso quedara grabado en los logs del sistema operativo.

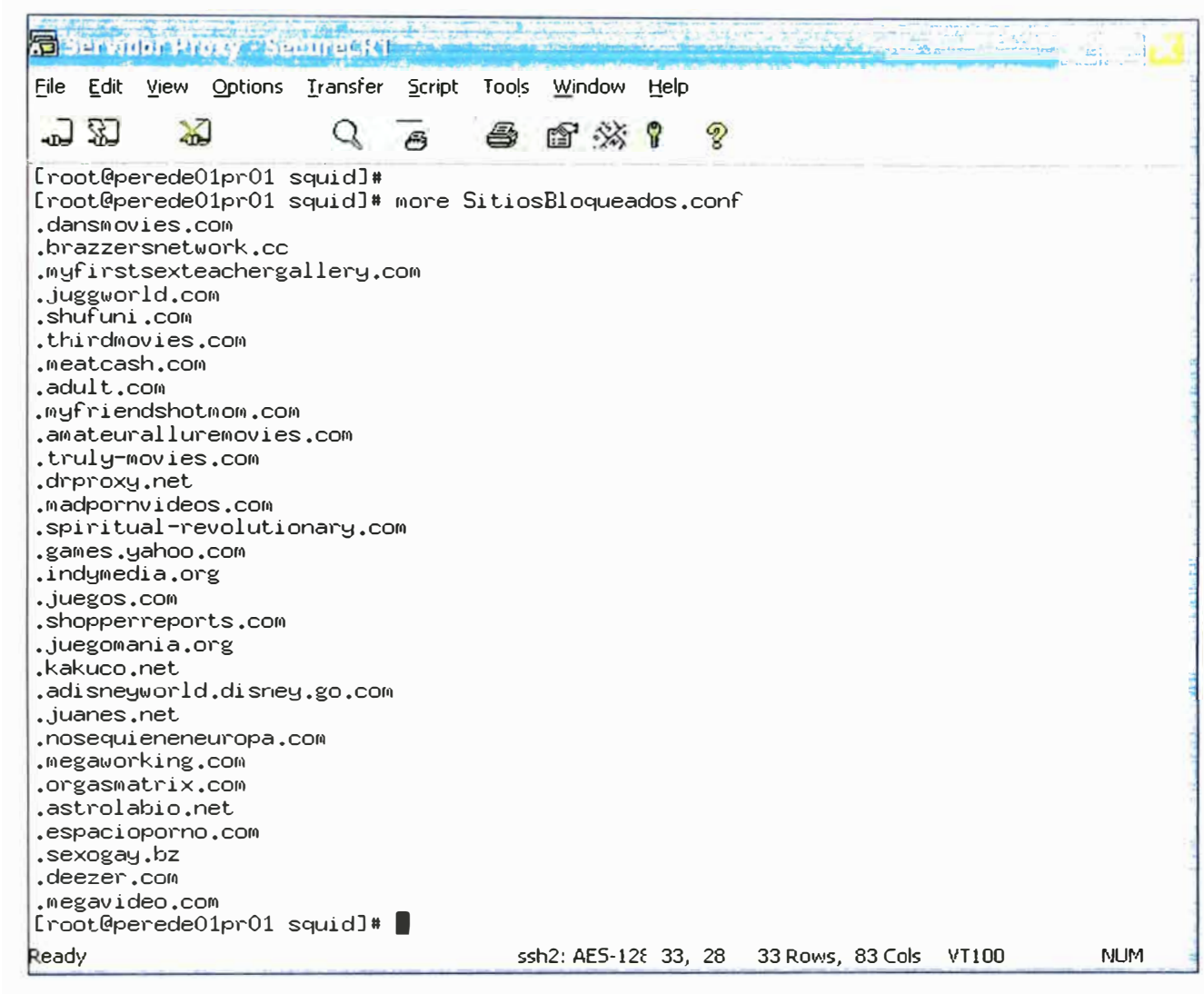


Fig. 4.8 Archivo que contiene los sitios bloqueados para la red

4.1.4 Configuración realizada en el servidor SARG

El servidor SARG una vez instalado es configurado a fin de que pueda procesar los logs semanales del servidor SQUID y pueda a su vez generar los reportes donde indique el uso del ancho de banda por cada usuario, las paginas webs a las que accede, así como los usuarios Tops y las páginas más visitadas en la empresa.

La configuración sugerida es la realizada en el punto 3.6 del presente informe, donde se indican también los programas que el sistema operativo debe tener instalados a fin de que los reportes puedan ejecutarse usando el servicio Apache, en todo caso de no tener dicho programa instalado se puede descargar desde la pagina Web de Red Hat.

4.2 Análisis de los datos y resultados obtenidos

A continuación realizaremos la generación del reporte de navegación hacia Internet en el servidor SARG:

4.2.1 Generación del reporte en el SARG

El análisis de los resultados se inician en el servidor Squid con la revisión del log semanal generado, esta tarea se puede programar para realizarla todos los lunes, básicamente se programa la generación del log para que se ejecute a las 00:00 horas y maneje un correlativo semanal:

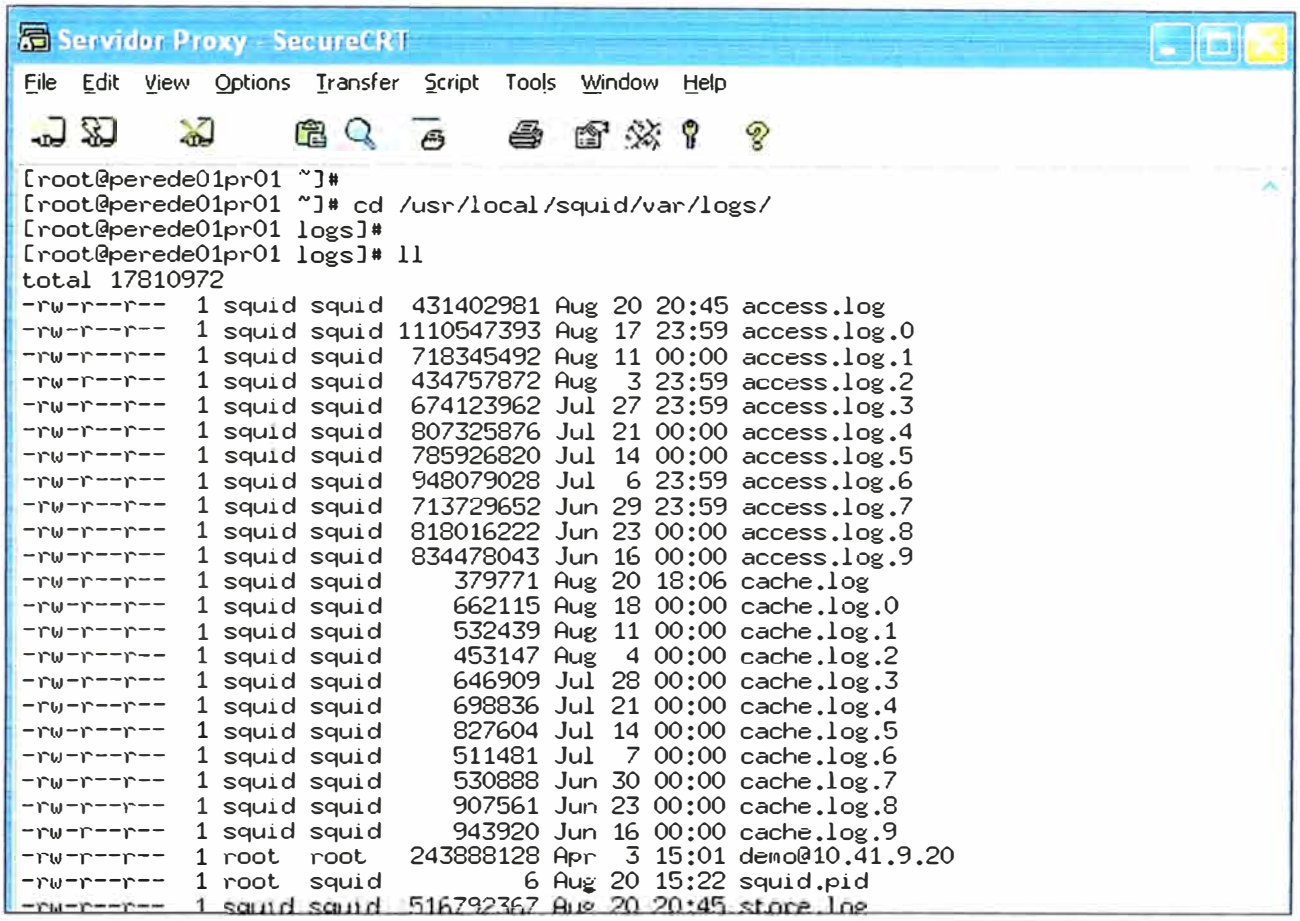


Fig. 4.9 Logs generados por el servidor Proxy

Luego de observar el log generado se procede a realizar la transferencia vía FTP hacia el servidor encargado de realizar el reporte, el servidor SARG. Para esta transferencia de archivos se puede utilizar algún cliente FTP como el Filezilla o se puede manejar a través de línea de comandos, colocando siempre la transferencia en modo binario y habilitando el modo hash a fin de observar el avance de los paquetes transferidos.

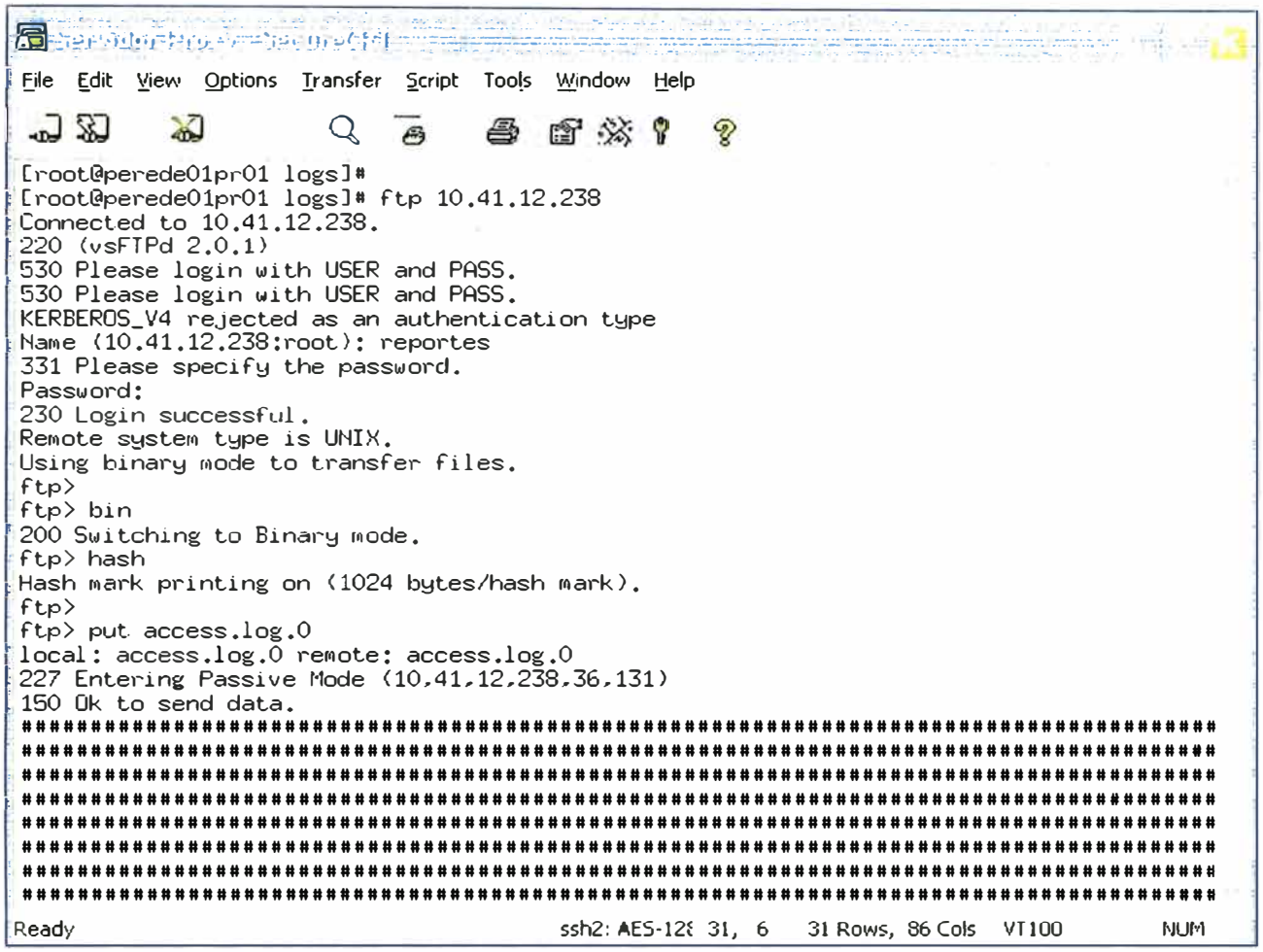


Fig. 4.10 Transferencia de archivos vía FTP

Luego ingresamos al servidor SARG y ejecutamos la tarea que producirá el reporte de navegación de la semana seleccionada:

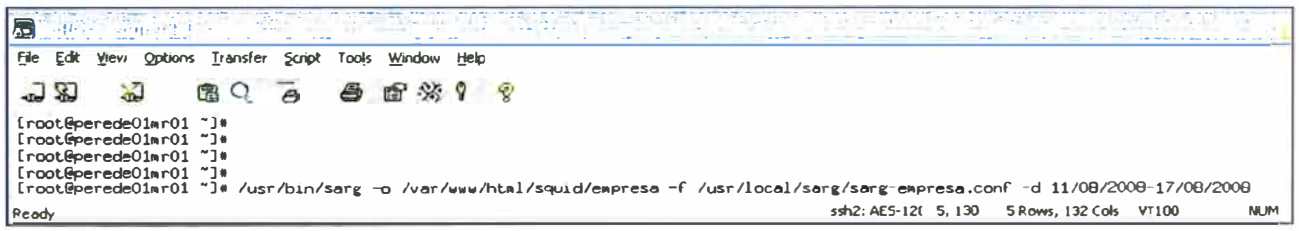
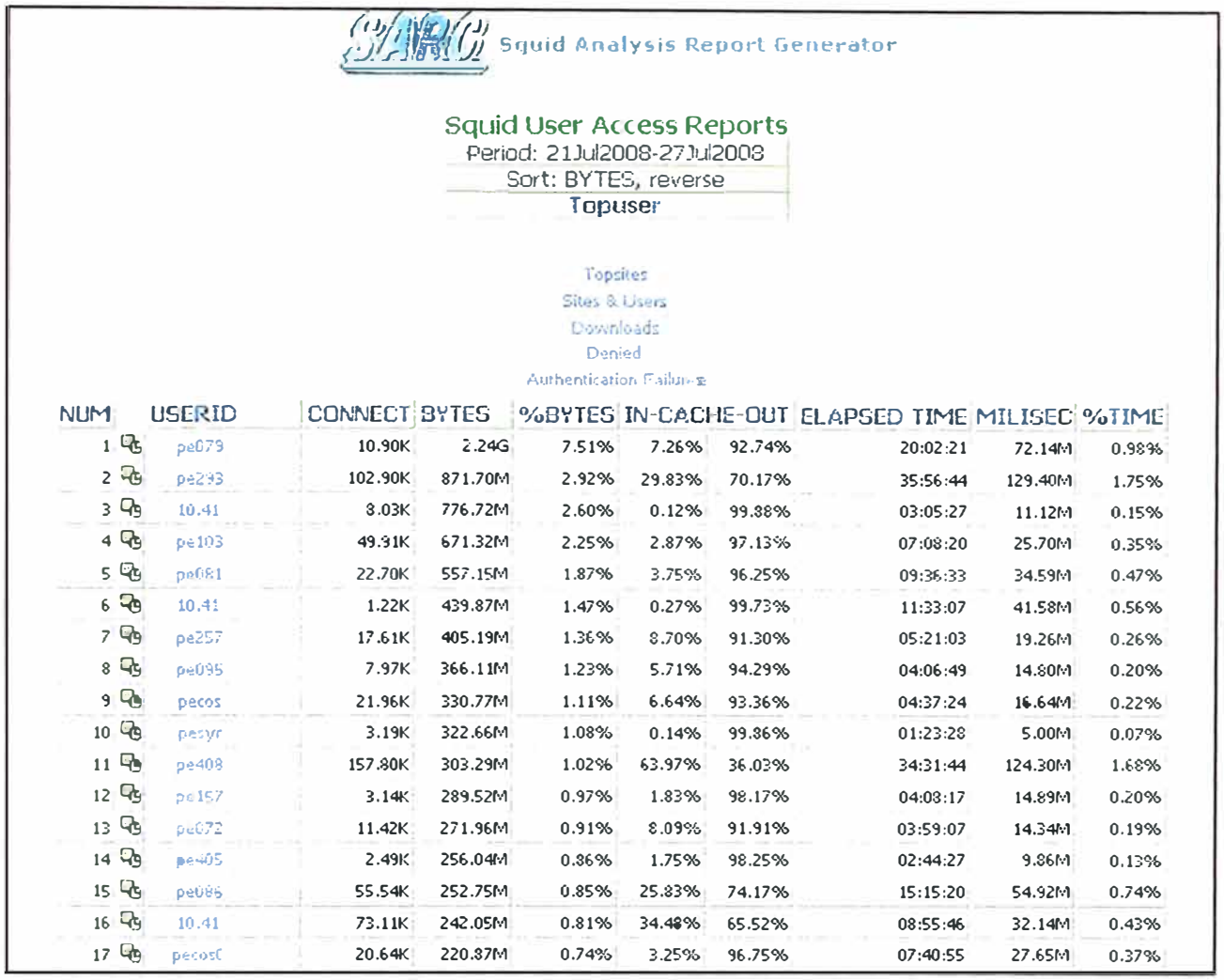


Fig. 4.11 Comando que ejecuta el reporte semanal en el servidor SARG

4.2.2 Análisis obtenido en el servidor SARG

Los reportes del servidor SARG son obtenidos en HTML ingresando a la dirección IP del servidor, allí observamos los usuarios que acceden a Internet desde la empresa, esto usuarios se encuentran ordenados de forma descendente en base al uso del ancho de

banda total de Internet, en este reporte podemos apreciar las conexiones realizadas por el usuario hacia Internet, la cantidad de Bytes transferidos, el porcentaje del ancho de banda total utilizado por el usuario y el tiempo total que estuvo conectado a Internet.



Squid Analysis Report Generator

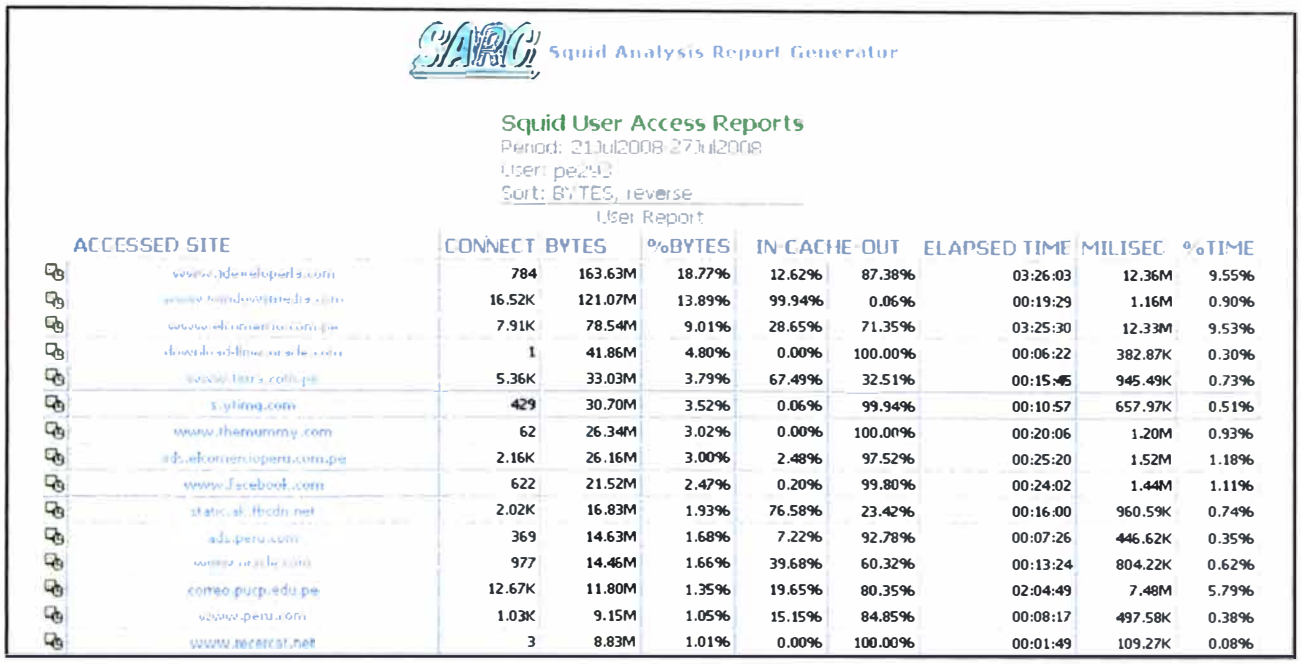
Squid User Access Reports
Period: 21Jul2008-27Jul2008
Sort: BYTES, reverse
Topuser

Topsites
Sites & Users
Downloads
Denied
Authentication Failures

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
1	pe079	10.90K	2.24G	7.51%	7.26%	92.74%	20:02:21	72.14M	0.98%
2	pe293	102.90K	871.70M	2.92%	29.83%	70.17%	35:56:44	129.40M	1.75%
3	10.41	8.03K	776.72M	2.60%	0.12%	99.88%	03:05:27	11.12M	0.15%
4	pe103	49.31K	671.32M	2.25%	2.87%	97.13%	07:08:20	25.70M	0.35%
5	pe081	22.70K	557.15M	1.87%	3.75%	96.25%	09:36:33	34.59M	0.47%
6	10.41	1.22K	439.87M	1.47%	0.27%	99.73%	11:33:07	41.58M	0.56%
7	pe257	17.61K	405.19M	1.36%	8.70%	91.30%	05:21:03	19.26M	0.26%
8	pe095	7.97K	366.11M	1.23%	5.71%	94.29%	04:06:49	14.80M	0.20%
9	pecos	21.96K	330.77M	1.11%	6.64%	93.36%	04:37:24	16.64M	0.22%
10	pesyr	3.19K	322.66M	1.08%	0.14%	99.86%	01:23:28	5.00M	0.07%
11	pe408	157.80K	303.29M	1.02%	63.97%	36.03%	34:31:44	124.30M	1.68%
12	pe157	3.14K	289.52M	0.97%	1.83%	98.17%	04:08:17	14.89M	0.20%
13	pe072	11.42K	271.96M	0.91%	8.09%	91.91%	03:59:07	14.34M	0.19%
14	pe405	2.49K	256.04M	0.86%	1.75%	98.25%	02:44:27	9.86M	0.13%
15	pe086	55.54K	252.75M	0.85%	25.83%	74.17%	15:15:20	54.92M	0.74%
16	10.41	73.11K	242.05M	0.81%	34.48%	65.52%	08:55:46	32.14M	0.43%
17	pecos0	20.64K	220.87M	0.74%	3.25%	96.75%	07:40:55	27.65M	0.37%

Fig. 4.12 Reporte inicial del servidor SARG con los usuarios tops

Adicionalmente si se desea tener un detalle de cada uno de los usuarios, se puede ingresar a su informe personal con solo dar un click en el usuario de red, en este punto se pueden observar al detalle ordenadas por uso de nacho banda consumido las paginas webs a las que ha accedido el usuario durante el periodo de una semana, así como los bytes transferidos entre la URL y su PC, también podemos apreciar el porcentaje de bytes de todo el uso que tuvo el usuario y el tiempo que estuvo activa dicha conexión, con este detalle se puede apreciar si la navegación del usuario corresponde a temas de índole laboral o no y con esta información tomar las medidas correspondientes y de ser necesario bloquear los links de tipo no laboral en el archivo SitiosBloqueados.conf del servidor Proxy.



Squid Analysis Report Generator

Squid User Access Reports

Period: 21Jul2008-27Jul2008
User: pe290
Sort: BYTES, reverse

User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILISEC	%TIME
www.[illegible].com	784	163.63M	18.77%	12.62%	87.38%	03:26:03	12.36M	9.55%
www.[illegible].com	16.52K	121.07M	13.89%	99.94%	0.06%	00:19:29	1.16M	0.90%
www.[illegible].com.pe	7.91K	78.54M	9.01%	28.65%	71.35%	03:25:30	12.33M	9.53%
download.[illegible].com	1	41.86M	4.80%	0.00%	100.00%	00:06:22	382.87K	0.30%
www.[illegible].com.pe	5.36K	33.03M	3.79%	67.49%	32.51%	00:15:45	945.49K	0.73%
s.ytimg.com	429	30.70M	3.52%	0.06%	99.94%	00:10:57	657.97K	0.51%
www.themummy.com	62	26.34M	3.02%	0.00%	100.00%	00:20:06	1.20M	0.93%
ads.elcomercioperu.com.pe	2.16K	26.16M	3.00%	2.48%	97.52%	00:25:20	1.52M	1.18%
www.facebook.com	622	21.52M	2.47%	0.20%	99.80%	00:24:02	1.44M	1.11%
static.ak.fbcdn.net	2.02K	16.83M	1.93%	76.58%	23.42%	00:16:00	960.59K	0.74%
ads.peru.com	369	14.63M	1.68%	7.22%	92.78%	00:07:26	446.62K	0.35%
www.[illegible].com	977	14.46M	1.66%	39.68%	60.32%	00:13:24	804.22K	0.62%
correo.pucp.edu.pe	12.67K	11.80M	1.35%	19.65%	80.35%	02:04:49	7.48M	5.79%
www.peru.com	1.03K	9.15M	1.05%	15.15%	84.85%	00:08:17	497.58K	0.38%
www.accercar.net	3	8.83M	1.01%	0.00%	100.00%	00:01:49	109.27K	0.08%

Fig. 4.13 Reporte de acceso a Internet detallado por usuario.

4.2.3 Análisis obtenido en el Firewall

El Firewall registra el acceso del servidor Proxy a cualquier página Web de Internet, este acceso por ser solicitado por el Proxy es permitido debido a la regla configurada inicialmente, usando la herramienta del Firewall Checkpoint "Tracking" podemos observa las salidas del Proxy las distintas direcciones IP públicas de Internet:

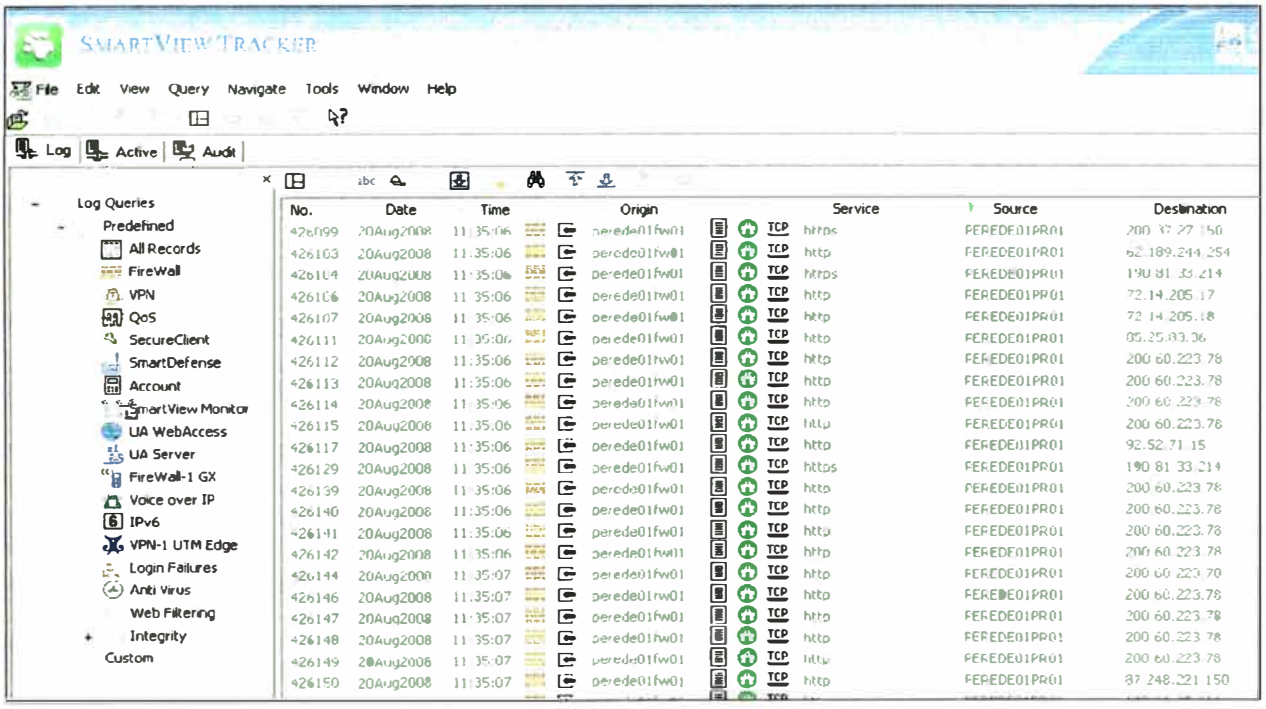


Fig. 4.14 Navegación del servidor Proxy a través del Firewall

4.3 Optimización del recurso de Internet en la red

La optimización del acceso a Internet es la parte final de este informe, luego de analizar los accesos de los usuarios Tops, las páginas webs de tipo no laboral a las que acceden los usuarios se pueden agregar dichas paginas en el archivo **SitiosBloqueados.conf** del servidor Proxy:

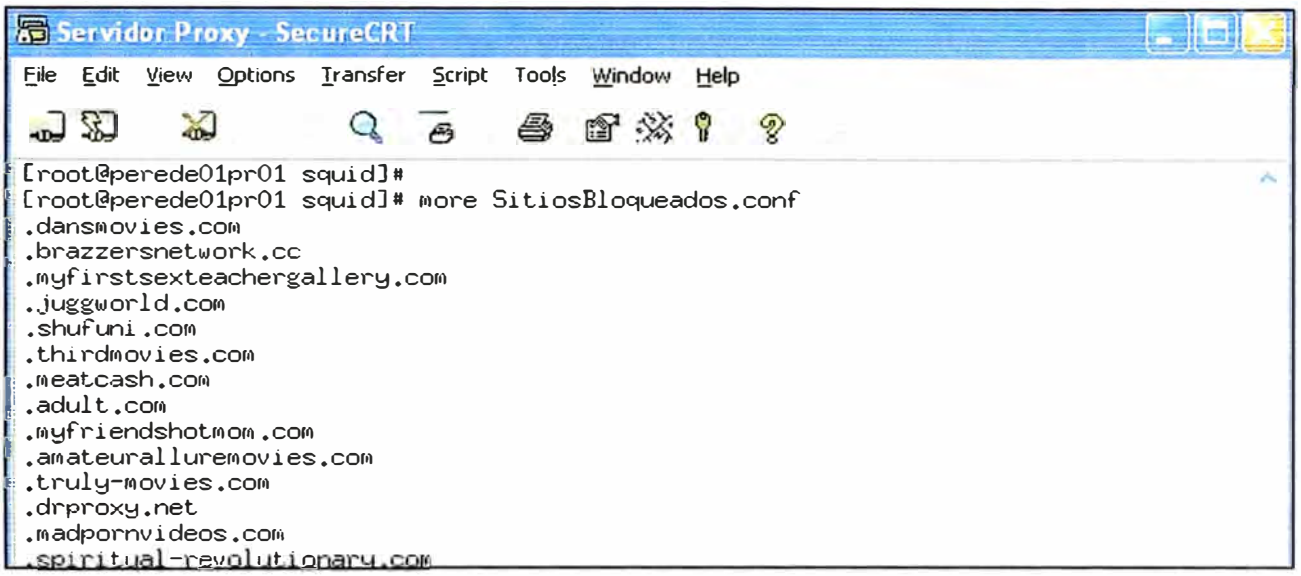


Fig. 4.15 Archivos que manejan los dominios bloqueados en el servidor Proxy

Otro punto con el que se puede optimizar el uso del ancho de banda hacia Internet es configurando la partición inicial del Packetshaper a un valor más óptimo de acuerdo al reporte del equipo. Por ejemplo en la figura Fig. 4.16 observamos el uso del ancho de banda de la partición de Internet de la empresa, en esta partición se configuro un limite de 1.6Mb, por lo que si el consumo de todos los usuarios llegara a este valor las conexiones serian cortadas y los usuarios sentirían una lentitud en el servicio, ante esto solo quedaría ampliar de forma temporal el valor máximo de la partición y proceder a analizar las paginas webs visitadas y las extensiones de los archivos descargados.

Estos gráficos nos dan los reportes efectivos del uso del ancho banda así como la salud de la red tomando en cuenta los paquetes dropeados y nos brinda también reportes de las conexiones exitosas o rechazadas en un periodo de tiempo, los reportes pueden ser ejecutados en periodos de una semana, un mes o en un intervalo de tiempo seleccionado.

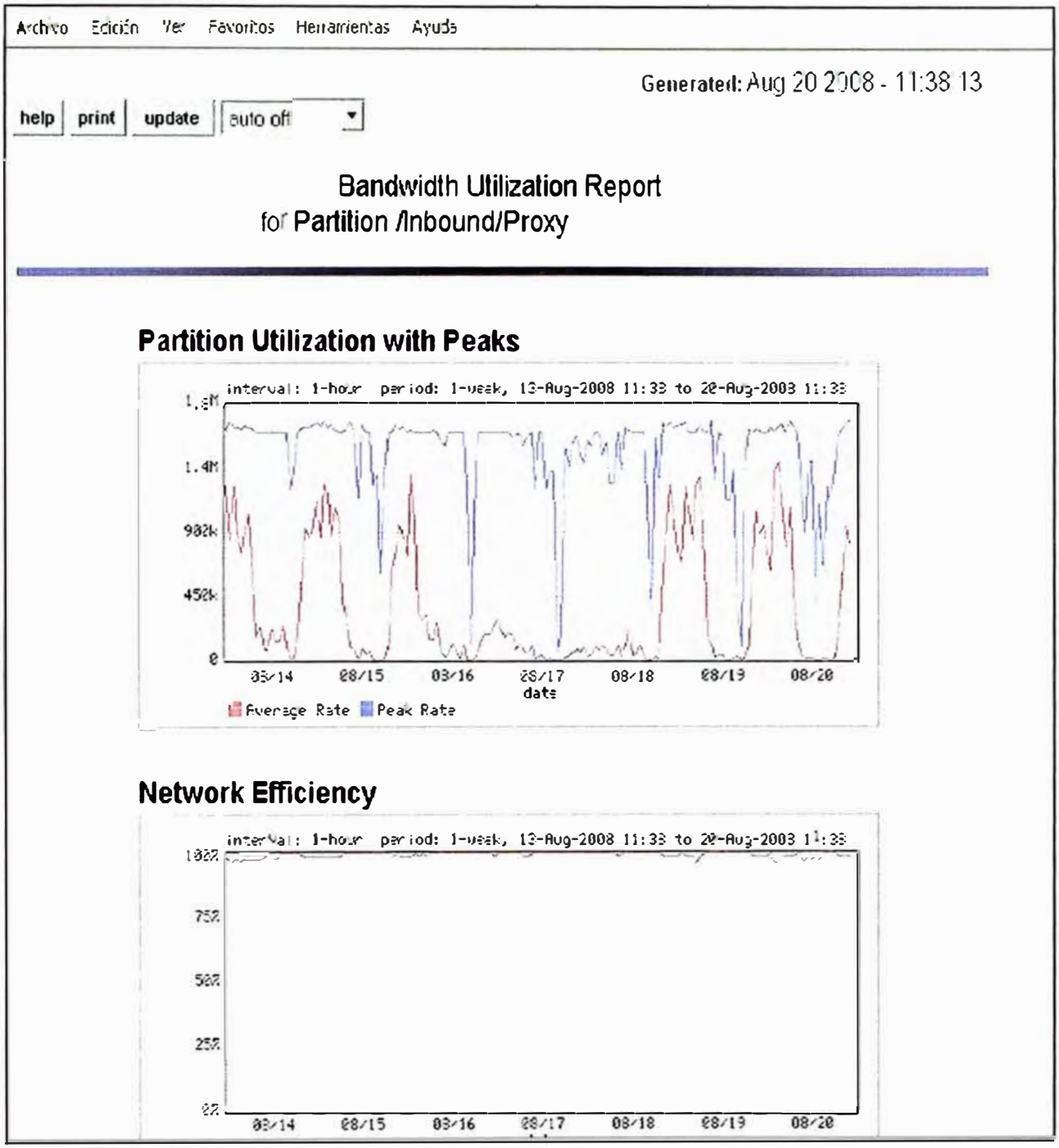


Fig. 4.16 Reporte del uso actual de Internet a través del Packetshaper

Un punto adicional que se puede observar de los reportes del servidor SARG es que debido a cantidad de programas espías y troyanos que se infiltran desde Internet el acceso a paginas Web de índole no laboral y la publicidad de productos aumenta debido a la instalación no deseada de barras de acceso o Hotbars:

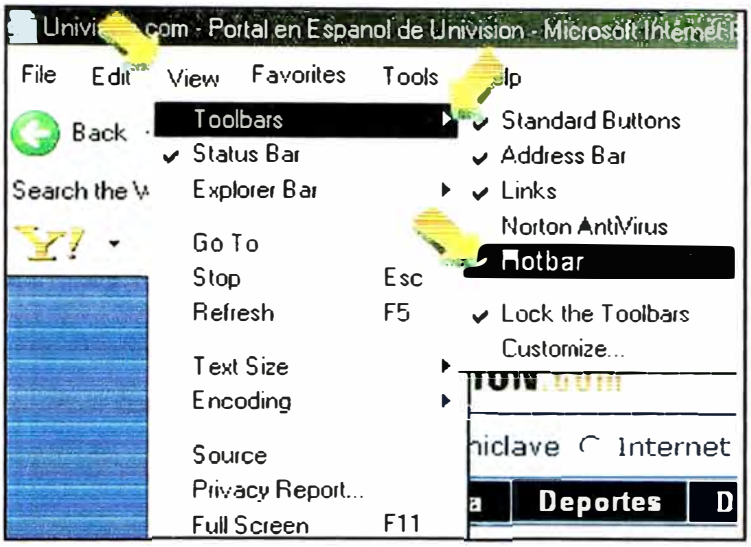


Fig. 4.17 Barras Hotbar

El acceso a estas paginas también es detectado por el servidor SARG y después de su análisis podemos determinar que equipos tienen esta conexión activa, mucho de los usuarios no tienen conocimiento de que sus maquinas tienen esta barra activa, pero con esta información se puede coordinar con el soporte local la desinstalación de la misma.

8862	skins.gmodules.com	pe09989535
8863	skins.hotbar.com	10.41.10.82 10.41.10.85 10.41.53.160 10.41.53.164 10.41.53.169 10.41.53.181 10.41.53.20 10.41.53.208 10.41.53.78
8864	skins.hotbar.com	10.41.10.113 10.41.10.133 10.41.10.82 10.41.10.85 10.41.45.125 10.41.45.132 10.41.45.85 10.41.45.96 10.41.46.145 10.41.53.102 10.41.53.160 10.41.53.164 10.41.53.169 10.41.53.181 10.41.53.189 10.41.53.20 10.41.53.208 10.41.53.78 10.41.9.237 10.41.9.240
8865	skins.hotbar.com	10.41.10.82 10.41.10.85 10.41.53.160 10.41.53.164 10.41.53.169 10.41.53.181 10.41.53.20 10.41.53.208 10.41.53.78
8866		pe15590347

Fig. 4.18 Equipos detectados con acceso a Hotbar.

Todos estos puntos analizados ayudaran a tener un óptimo control y uso del acceso a Internet desde nuestra red.

4.4 Presupuesto y tiempo de ejecución

El presupuesto depende de la cantidad y calidad de los equipos que se usaran en esta red, en el mercado se tienen diversidad de Routers y Firewalls que pueden cumplir los requisitos mínimos para la seguridad de una red, la ventaja de esta implementación es que el acceso de los usuarios a Internet es controlado por un servidor Proxy bajo Linux y el servidor de reportes maneja el servicio SARG también sobre un servidor Linux, como

es conocido Linux es una distribución libre por lo que los costos por adquirir el programa es nulo, la inversión básicamente esta en el Hardware.

Por ejemplo una red empresarial con cerca de 1000 usuarios debería invertir en un Firewall de tipo Hardware cuyo precio puede llegar a los $10 000, a esto se le puede sumar un router Cisco 2600 para el control del trafico externo cuyo precio se encuentra cercano a los $5000, un buen servidor para que soporte el servidor Proxy y el servidor de reportes de acceso a Internet puede bordear los $5 000, por lo que una solución seria solo en Hardware puede acercarse a los $20 000, esto fuera de las horas hombres que se invertirían en configurar dichos equipos y en mantener su optima administración.

Por otro lado podemos contar con una pequeña red con cerca de 20 usuarios, donde el acceso a Internet actualmente es provisto con un pequeño router, por lo que la necesidad de un router ya se encontraría cubierta, la configuración del Firewall se puede dar también sobre Linux, existen versiones que manejan este sistema, como el Linux Fedora, la implementación del Proxy y del servidor de reportes puede darse sobre el mismo equipo, que en caso de ser para el uso de una red pequeña se podría implementar todo en una sola PC Dual Core que puede bordear los $1000, esto fuera del costo de las horas hombres que implique la configuración de dicha solución.

En resumen dependiendo de la cantidad de usuarios y de la importancia de la información a controlar será necesario el uso o no de equipos de cierto costo.

Con este análisis observamos que las medidas de control y administración del acceso a Internet son variadas en cuanto a equipos a configurar y administrar, así como a criterios de filtros a aplicar, la información expuesta será de apoyo para la implementación de un sistema de seguridad de acceso a Internet que deseemos configurar a futuro en donde tendremos en cuenta la variedad de ataques existentes en Internet y la variedad de equipos y técnicas con las que podemos contrarrestar dichos ataques.

CONCLUSIONES

1 El acceso a Internet es un recurso crítico en cualquier organización, este servicio posee una gran cantidad de ventajas en temas de productividad y comunicación, pero también presenta una exposición a una gran variedad de peligros en la red como ataques de virus, infección de programas espías o troyanos entre otros.

2 Evidentemente la seguridad en Internet afecta sobremanera a las empresas que operan con sistemas críticos, ya que la información personal y confidencial de sus trabajadores esta expuesta a través de Internet. En definitiva, la seguridad afecta a todos: a las grandes compañías por ser una tentación y por las consecuencias de una posible filtración, y a los usuarios individuales por su vulnerabilidad.

3 La seguridad en Internet consiste en implementar mecanismos para que cuando se reciba un mensaje o se realice una transacción por medios electrónicos, se asegure la integridad del contenido y la identidad del remitente y del receptor. Las contraseñas y palabras claves ya no son un mecanismo suficientemente fiable y seguro, ya que éstas pueden ser interceptadas durante su transmisión, de lo que desgraciadamente nos damos cuenta muy tarde o cuando ya se ha perdido información valiosa de la compañía.

4 Ante todos estos ataques y problemas que rodean a Internet es importante mantener un acceso a Internet controlado por los equipos estudiados en el presente informe, así como también mantenerse a la vanguardia de las tecnologías aprendiendo las nuevas técnicas de ataques y los nuevos equipos que nos protegerán de ellas, solo así podremos asegurar la confiabilidad y la seguridad de nuestra red.

ANEXO A

INSTALACION DEL SERVICIO SQUID

INSTALACION DEL SERVICIO SQUID

Para poder llevar al cabo los procedimientos descritos es necesario tener instalado al menos lo siguiente en un servidor con sistema operativo Linux:

- Al menos squid-2.5.STABLE6
- httpd-2.0.x (Apache), como auxiliar de caché con aceleración.
- Instalación a través de yum.

Si cuenta con un sistema con CentOS o White Box Enterprise Linux 3 o versiones posteriores, utilice lo siguiente y se instalará todo lo necesario junto con sus dependencias:

yum -y install squid httpd

yum -y update kernel iptables

- Instalación a través de up2date.

Si cuenta con un sistema con Red Hat™ Enterprise Linux 3 o versiones posteriores, utilice lo siguiente y se instalará todo lo necesario junto con sus dependencias:

up2date -i squid httpd

up2date -u kernel iptables

Configuración básica.

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf, y podrá trabajar sobre este utilizando su editor de texto simple preferido. Existen un gran número de parámetros, de los cuales recomendamos configurar los siguientes:

- http_port
- cache_mem
- cache dir
- Al menos una Lista de Control de Acceso

- Al menos una Regla de Control de Acceso
- Iniciando, reiniciando y añadiendo el servicio al arranque del sistema.

- **http_port**

Default: http_port 3128

http_port 192.168.1.254:3128

http_port 192.168.1.254:8080

- **cache_mem**

De modo predefinido se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

Si se posee un servidor con al menos 128 MB de RAM, establezca 16 MB como valor para este parámetro:

cache_mem 16 MB

- **cache_dir**

Este parámetro se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? De modo predefinido Squid utilizará un caché de 100 MB, de modo tal que encontrará la siguiente línea:

cache_dir ufs /var/spool/squid 100 16 256

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un caché de 700 MB:

cache_dir ufs /var/spool/squid 700 16 256

Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. No modifique esto números, no hay necesidad de hacerlo.

- **Al menos una Lista de Control de Acceso**

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.1.n con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

acl miredlocal src 192.168.1.0/255.255.255.0

También puede definirse una Lista de Control de Acceso especificando un fichero localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP. Ejemplo:

acl permitidos src "/etc/squid/permitidos"

- **Reglas de Control de Acceso.**

Estas definen si se permite o no el acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

La sintaxis básica es la siguiente:

http_access [deny o allow] [lista de control de acceso]

En el siguiente ejemplo consideramos una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

http_access allow permitidos

- **Aplicando Listas y Reglas de control de acceso.**

Una vez comprendido el funcionamiento de la Listas y las Reglas de Control de Acceso, *procederemos a determinar cuales utilizar para nuestra configuración*.

Caso 1.

Considerando como ejemplo que se dispone de una red 192.168.1.0/255.255.255.0, si se desea definir toda la red local, utilizaremos la siguiente línea en la sección de Listas de Control de Acceso:

acl todalared src 192.168.1.0/255.255.255.0

Habiendo hecho lo anterior, la sección de listas de control de acceso debe quedar más o menos del siguiente modo:

Listas de Control de Acceso: definición de una red local completa

Recommended minimum configuration:

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 todalared src 192.168.1.0/255.255.255.0

A continuación procedemos a aplicar la regla de control de acceso:

http_access allow todalared

- **Iniciando, reiniciando y añadiendo el servicio al arranque del sistema.**

Una vez terminada la configuración, ejecute el siguiente mandato para iniciar por primera vez Squid:

service squid start

Si necesita reiniciar para probar cambios hechos en la configuración, utilice lo siguiente:

service squid restart

Si desea que Squid inicie de manera automática la próxima vez que inicie el sistema, utilice lo siguiente:

chkconfig squid on

Lo anterior habilitará a Squid en todos los niveles de ejecución.

ANEXO B

ESPECIFICACIONES TECNICAS DE LOS DISPOSITIVOS DE OPTIMIZACION DEL USO DEL ANCHO DE BANDA DE INTERNET

ANEXO B

ESPECIFICACIONES TECNICAS DE LOS DISPOSITIVOS DE OPTIMIZACION DEL USO DEL ANCHO DE BANDA DE INTERNET

ESPECIFICACIONES TECNICAS DEL ROUTER CISCO 2800

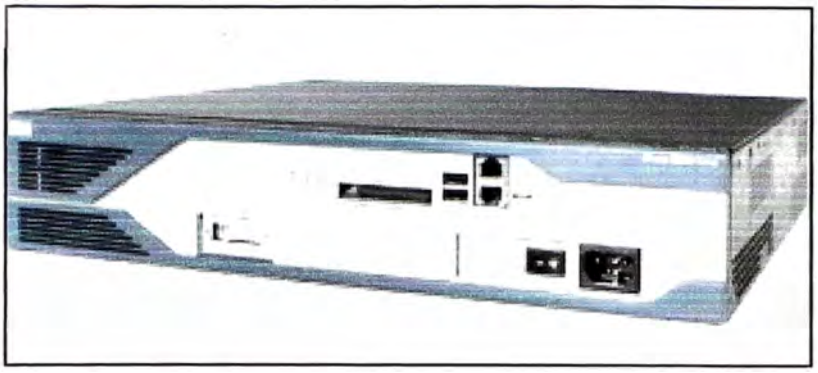


Fig. B. 1 Router Cisco 2800

Características principales Router CISCO 2821 Integrated Services Router	
Descripción del producto	Cisco 2821 Integrated Services Router - encaminador
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 2U
Dimensiones (Ancho x Profundidad x Altura)	43.8 cm x 41.7 cm x 8.9 cm
Peso	11.4 kg
Memoria RAM	256 MB (instalados) / 1 GB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Características	Cisco IOS , protección firewall, cifrado del hardware, asistencia técnica VPN, soporte de MPLS, filtrado de URL
Cumplimiento de normas	IEEE 802.3af
Alimentación	CA 120/230 V (50/60 Hz)

Tabla B.1 Especificaciones técnicas del router Cisco 2800

ESPECIFICACIONES TECNICAS DEL PACKETSHAPER 3500

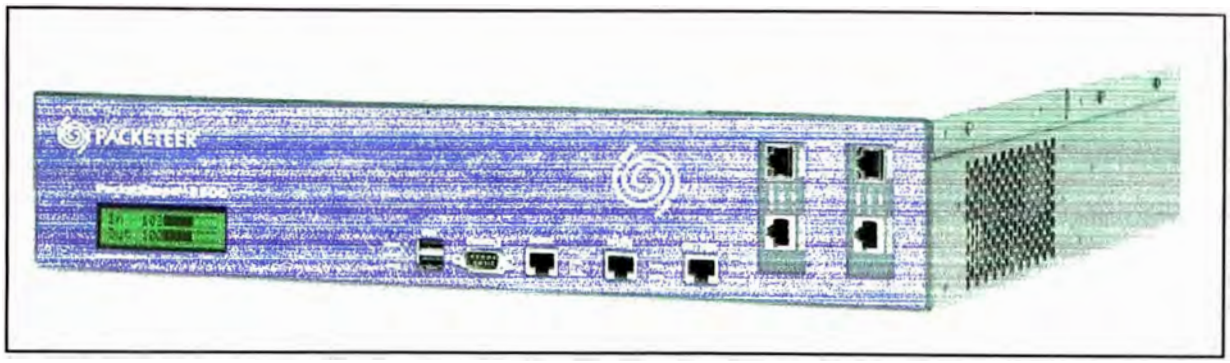


Fig. B. 2 Packetshaper modelo 3500

Características principales Packetshaper modelo 3500

Dimensiones	Estándar montaje de estante de 19 pulgadas Altura: 3.50 adentro. (8.89 cm) Anchura: 17.35 adentro. (44.07 cm) Profundidad: 16 adentro. (40.64 cm)
Peso	18.04 libras. (8.18 kilogramos)
Puertos de red por el NIC	Dos puertos de Ethernet del gigabit: 1000Base-T, 100Base-T, o 10BaseT
Ranuras de extensión	Dos (cada ranura puede acomodar un módulo de la extensión del LAN)
Puerto de administración	Un puerto de Ethernet del gigabit
Puerto serial	Puerto serial (En-compatible) RS-232 con el varón DB-9 conectador
El panel del LCD	Sí. Vea el LCD artesonar mensajes de error de los mensajes y del panel del LCD
Puertos del USB	Dos *(reservado para el uso futuro)*
Estado LED	Si *todas las* condiciones siguientes son verdades, el LED es verde, si no es ambarino: • todos los acoplamientos están para arriba • el formar está prendido • la dirección configurada del ranurador del sitio es detectada por el PacketShaper o la dirección del ranurador del sitio se fija a *ningunos*

Avería LED	Iluminado cuando en caja fuerte o modo corrompido
Energía LED	Iluminado cuando la unidad se tapa en un enchufe de energía activa y la unidad se gira
Acoplamiento LED	Iluminado cuando el cable de la red está conectado correctamente en ambos extremos
Tx/Rx LED	Oscila cuando la unidad es que transmite y de recepción de datos
Velocidad LED	Indica velocidad del acoplamiento: • ámbar = Gbps 1 • verde = 100 Mbps • de = 10 Mbps
Data* eléctrico	Grado de la fuente de alimentación: 100/240 VAC, 50/60 hertzio, 2.5A C.C. de potencia de salida: 56 vatios Energía de entrada de la CA: 69 vatios Corriente de entrada: • 0.80 A en 90 VAC/60 hertzio • 0.61 A en 120 VAC/60 hertzio • 0.42 A en 180 VAC/60 hertzio • 0.33 A en 240 VAC/60 hertzio *Measured con 2 1 de alimentación fuente de LEMs y. Para las unidades configuradas con dos fuentes de alimentación, vea PacketShaper 7500 especificaciones de producto para los datos eléctricos aplicables.
Disipación de calor	236 BTU/hour
Ambiental (Funcionamiento)	Temperatura: 32° F a 104° F (0° C a 40° C) Higrometría: el 0% a el 95% non-condensing Altitud: 0 a 10.000 funcionamientos del pie
Ambiental (Almacenaje)	Temperatura: -13 ° F al °F 131 (- 25° C a 55° C) Humedad: el 5% a el 95% Presión de aire: kPa 70 a 106
Velocidad manejada del acoplamiento	Se ofrecen las configuraciones múltiples; acoplamientos de ayudas hasta el duplex de 45 Mbps por completo -. La configuración de los programas determina el máximo que forma capacidad.

Tabla B.2 Especificaciones técnicas del Packetshaper 3500

BIBLIOGRAFIA

1 Gonzalo Asensio, "Seguridad en Internet", Nowtilus – España, 2006.

2 Joel Scambray, Stuart McClure y George Kurtz, "Hackers 2 Secretos y soluciones para la seguridad de redes", Osborne McGraw-Hill – Madrid, 2001.

3 http://www.segu-info.com.ar/ataques/ataques.htm

4 http://damr.net/

5 http://www.cisco.com/en/US/products/ps5882/index.html

6 http://support.packeteer.com/documentation/packetguide/8.1/products/specifications-3500.htmhttp://www.checkpoint.com/products/

7 http://www.checkpoint.com/products/network_security/index.html

8 http://www.linux.org.py

9 http://www.linuxparatodos.net/

10 http://www.tech-faq.com/lang/es/ip-access-lists.shtml

11 http://www.perantivirus.com/sosvirus