UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN

"FIREWALL CON MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2000"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A:

JUAN ALBERTO GUERRERO NAVA

DIRECTOR DE TESIS:
ING. RODOLFO VÁZQUEZ MORALES

SAN JUAN DE ARAGÓN, ESTADO DE MÉXICO **2004**

Agradecimientos

En especial a mi prometida, Susana Jurado; quien tuvo la perseverancia y la insistencia para que no me diera por vencido en realizar esta tesis.

A mi familia empezando por mis papás Cristina y Miguel, por darme la mejor herramienta para salir adelante en esta vida; la educación. A mis hermanas Christian y Jessica, por el apoyo y la paciencia que me concedieron durante toda la carrera. También a mis abuelos, tíos y primos; por creer en mí.

A mi asesor, el Ingeniero Rodolfo Vázquez por sus siempre atinados comentarios y observaciones; y también los revisores Ing. Gladis Fuentes, Ing. Mirna Ramírez, M.T.I. Omar Mendoza y Lic. Israel Juárez por compartir sus notas y opiniones acerca de este trabajo para ampliarlo y mejorarlo.

A todos los profesores de la carrera de Ingeniería en Computación quienes tuvieron la inquebrantable fe de compartir sus conocimientos para impartir cátedra a toda la generación 1997-2001.

A mis mejores amigos Mario Christopher (Manolo), Xavier Omar (Xavi-Men), Eduardo (Lalo Loco), Marco Antonio (Chaparrito), Alberto (Willy) e Ivonne (Mike); por el mutuo apoyo para salir siempre adelante y llegar al final.

Por último pero no menos importante, a nuestra ***alma mater*** quien nos concediera una oportunidad y un espacio para realizar nuestros estudios.

A todos ustedes... GRACIAS.

Juan Alberto Guerrero Nava

Frank

AGRADECIMIENTOS DEL ASESOR

Universidad Nacional Autónoma de México:
Gracias por darme la oportunidad de contribuir con la grandeza de nuestra máxima casa de estudios, apoyando a quienes como yo, en un momento de nuestra vida académica lo necesitábamos.

Alberto:
Gracias por hacerme parte de tu proyecto de tesis, se que tus principios, capacidad y tenacidad te llevarán a grandes empresas, nunca lo olvides.

A nuestros revisores:

Lic. Israel Juárez Ortega:
Gracias por seguir siendo mi maestro y marcar con su plática la pauta de mi desarrollo profesional, con mucho cariño y respeto.

MTI. Omar Mendoza González:
En ocasiones la vida nos lleva a conocer personas con las que es placentero trabajar, tú eres una de ellas.

Ing. Mirna Miriam Ramírez Guerra:
Gracias por compartir tu entusiasmo hacia la cátedra y por las aportaciones a este trabajo.

Ing. Gladis Fuentes Chávez:
Pocas personas como tú tienen tan firme el compromiso universitario, gracias por trasmitírmelo y recordarme en todo momento que "Por mi raza hablará el espíritu".

Ing. Rodolfo Vázquez Morales.

Firewall con Microsoft Internet Security and Acceleration Server 2000

Índice General

Firewall con Microsoft Internet Security and Acceleration Server 2000

Índice de Figuras

Firewall con Microsoft Internet Security and Acceleration Server 2000

Índice de Tablas

CAPÍTULO 1

SEGURIDAD INFORMÁTICA

1.1 ¿QUÉ ES SEGURIDAD Y SEGURIDAD COMPUTACIONAL?

Trataremos puntos esenciales acerca de la seguridad en el área de la informática; dando pie a un preámbulo de ideas donde podremos usar estos conocimientos teóricos para desarrollar una buena política de seguridad a implementar en la empresa o industria, de tal manera que sean entendibles y accesibles a toda persona.

Existen herramientas de apoyo como las criptográficas para establecer un buen perímetro de seguridad; recordándonos de igual manera, que ningún método es 100% seguro sino que la combinación de varios es lo que nos proporciona una fiabilidad del 99.5%.

SEGURIDAD

Por seguridad se entiende como la característica de cualquier sistema (sea informático o no) que nos señala que está libre de cualquier peligro, riesgo o daño[1]. Entendiendo de igual manera que se destinarán y crearán ciertos dispositivos o reglas para evitar accidentes.

Según la opinión de varios expertos, esta definición es difícil de conseguir; por lo tanto se puede definir dicho sistema como fiable, es decir, la probabilidad de que un sistema se comporte tal y como se espera. Se entenderá por sistema como el conjunto de computadoras, servidores, impresoras, cableados de red, dispositivos de almacenamiento, sistemas operativos, otros programas, etc.; que nos sirven para ejecutar diversos procesos tales como la creación o modificación de datos. Implican también, los diversos problemas y riesgos que estos puedan traer, como la perdida o el robo de información.

Para poder mantener un sistema seguro (o fiable) se deben considerar y garantizar tres aspectos:

1. Confidencialidad
2. Integridad
3. Disponibilidad.

[1] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pag. 3

Confidencialidad	Nos expresa que los objetos de un sistema sólo pueden ser accedidos únicamente por personas autorizadas a ellos; la seguridad se integra en esta propiedad en general, que queda entendida como el nivel de calidad del servicio ofrecido.
Integridad	Nos dice que los objetos sólo pueden ser modificados por elementos autorizados y de manera controlada.
Disponibilidad	Indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

Tabla 1 Aspectos a considerar de un sistema fiable

SEGURIDAD COMPUTACIONAL

Anteriormente, el concepto de seguridad computacional no era tomado en serio, ya que implementar dicha seguridad era costoso; aquella empresa que lo hiciera contaba con un cuarto, un piso o tal vez un edificio completo para la instalación de las computadoras destinadas a ofrecer protección. Algunas personas sabían como usar las computadoras y se consideraban privilegiadas por saber los "secretos de la máquina".

La seguridad computacional o informática son técnicas desarrolladas para la protección tanto de los equipos informáticos como de la información contenida en ellos, ya sea que estos equipos sean individuales, o bien conectados a una red.

En la actualidad, considerar la seguridad de la información y los equipos de cómputo es de gran importancia debido al incrementado uso de los mismos; en cierta forma, aquella empresa que no use equipos de cómputo corre el riesgo de no prosperar y quien haga uso de las computadoras debe considerar como proteger sus datos y PC's.

1.1.1 ¿QUÉ SE DESEA PROTEGER?

Dentro de la seguridad en equipos computacionales tenemos cuatro elementos que deseamos proteger y éstos son el software, el hardware, servicios externos y la información siendo este último el más importante.

HARDWARE

Por hardware entendemos que son todos los elementos físicos que constituyen a la computadora como el CPU, los dispositivos periféricos, los medios de almacenamiento, tarjetas de red, etc.

Es decir, el equipo donde se ejecutan todos los procesos.

SOFTWARE

El software es el conjunto de programas que hacen que el hardware realice diversas funciones, y dentro de estos programas tenemos a los Sistemas Operativos y los programas de aplicación.

SERVICIOS EXTERNOS

Los servicios externos se refieren a aquellos proporcionados desde la red mundial, tales como los servicios de correo electrónico, el acceso mismo a Internet, las redes privadas virtuales (VPN), entre otros. Estos representan grandes riesgos, ya que la mayor parte de la propagación de virus se realiza por estos medios y no olvidemos la penetración ilegal de un extraño en una red local o en la misma VPN.

INFORMACIÓN

La información es el conjunto de datos lógicos que son manejados por el software y el hardware y también por el usuario a través de procesos, dichos datos pueden viajar por una red o tal vez tener acceso a una base de datos. Los datos constituyen el principal elemento a proteger, ya que es el más amenazado y difícil de recuperar; en caso de una pérdida de base de datos o de un proyecto de algún usuario, no existe un medio original de donde poderlo restaurar.

El concepto de seguridad en la información es más amplio que una simple protección de datos a nivel lógico. Si queremos proporcionar seguridad real habrá que tener en cuenta factores internos y externos; así como caracterizar el sistema que albergará la información de tal manera que podamos identificar las amenazas.

Este tipo de situaciones nos lleva a realizar copias de seguridad, pero si la política que existe para dicha copia es muy estricta, entonces será muy difícil poder recobrar la información antes de la pérdida.

Los cuatro elementos descritos anteriormente están expuestos a una multitud de amenazas y ataques. Generalmente las formas de ataque se dividen en cuatro grupos:

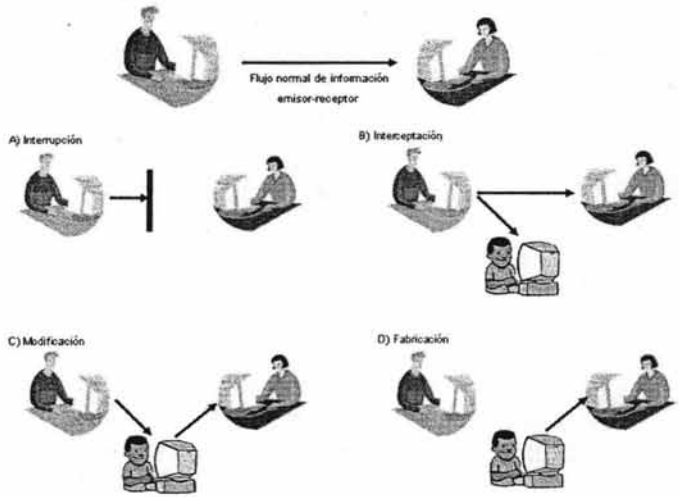


Figura 1 Amenazas a las que está expuesta el flujo de información

A) Interrupción

Se clasifica como interrupción si un objeto del sistema se pierde, ya no sirve o no está disponible.

B) Interceptación

Se dice que es interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema.

C) Modificación

Se tratará de modificación cuando el elemento no autorizado, además de conseguir el acceso, modifica dicho objeto.

D) Fabricación

Se trata de una amenaza o ataque fabricado si la modificación es destinada a conseguir un objeto similar, de tal forma que sea difícil diferenciar entre el objeto original y el modificado.

1.1.2 ¿DE QUIÉN Y DE QUÉ NOS PROTEGEMOS?

En varias publicaciones que tratan sobre la seguridad informática, nos encontramos que los autores intentan de alguna manera clasificar en grupos a los diversos elementos que puedan atacar a nuestro sistema. Sabemos que la mayoría de los ataques son provocados por personas que, con intención o sin ella, pueden generarnos enormes pérdidas. Pero, ¿qué hacen estas personas que debemos protegernos? Sencillamente se debe a la falta de conocimiento acerca de las herramientas computacionales que posee, originando una situación desesperante al momento que llegan a borrar de manera accidental la información.

Además de las personas existen las amenazas lógicas, los cuales son programas que pueden causar daño a nuestro sistema[2]. Y por último las catástrofes sean naturales o artificiales, los cuales son los factores menos probables de pérdidas de información, que si bien es cierto, nadie se encuentra a salvo de algún siniestro tal como un terremoto, un incendio o tal vez una inundación.

Personas

Como se mencionó antes, la mayoría de los ataques provendrán de personas, que en últimas instancias nos causaran daños eliminando o modificando nuestra información.

[2] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pag. 5

Generalmente se tratarán de hackers (piratas informáticos) que tratarán de conseguir un máximo nivel de privilegios aprovechando riesgos lógicos, tales como los agujeros (bugs) del software.

De igual manera, no olvidemos que los hackers no son los únicos interesados en penetrar el sistema y atacarnos, encontramos también a diversos grupos los cuales se pueden considerar como amenaza.

Personal

Las amenazas a la seguridad de un sistema provenientes del personal de la propia empresa se toman en cuenta rara vez, ya que se supone existe un ambiente de confianza; lo que sugiere pasar por alto el hecho de que cualquier persona pueda comprometer la seguridad de los equipos.

Sin embargo nadie mejor que ese personal, son quienes realizan esos ataques mayor y normalmente accidentales, ya que no conocen las políticas de seguridad que rodean al sistema. Pero también hay que recordar que el mismo personal conoce a la perfección el sistema y sus puntos débiles.

Desempleados

Este grupo de personas son los potencialmente interesados en atacar de una manera u otra al sistema, sobre todo si estos no abandonaron el entorno laboral por voluntad propia o pasaron a otra empresa que es la competencia.

Esto sucede, ya que aún se mantienen vigentes las cuentas dentro del sistema; estas personas ingresan (como si aún estuvieran trabajando para la organización) ya que conocen a la perfección dicho programa y pueden conseguir privilegios necesarios para causar daños.

Curiosos

Las personas suelen ser curiosas por naturaleza, y más si trabajan en un ambiente donde se forman profesionales interesados en el campo tecnológico de las comunicaciones y la teleinformática; si existe una combinación, entonces se produce una serie de cadenas de gente intentando acceder a sistemas donde no tienen acceso oficialmente.

En ocasiones, esto lo hacen para leer información íntima de algún colega o tan solo para romper la seguridad del sistema y probarse a sí mismos para saber hasta dónde pueden llegar. Hay que tener en cuenta que la mayoría de estos ataques no se realizan con la intención de hacer daño, pero si hay un porcentaje pequeño que la haría y esto es por falta de ética.

Terroristas

Son personas simplemente dedicadas a penetrar un sistema y causar algún daño en él.

Intrusos Remunerados

Este grupo de atacantes es el más peligroso, pero solo se dedican a sistemas muy grandes, tales como la Defensa Nacional o la Agencia de Seguridad Nacional. Por lo general, se trata de gente experta en problemas de seguridad con un amplio conocimiento de los sistemas empleados para la protección.

Amenazas Lógicas

Dentro de las amenazas lógicas encontramos un gran tipo de programas que de una forma u otra dañan nuestro sistema; son creados intencionalmente el software malicioso (conocido también como malware) que pueden penetrar por los agujeros del sistema.

Herramientas de Seguridad

Cualquier herramienta de seguridad es considerada actualmente una peligrosa arma de doble filo, ya que los administradores del sistema las utilizan para detectar fallos y darles solución. Sin embargo, esos mismos programas detectores de fallos y vulnerabilidades, son utilizados por los invasores para conocer las mismas debilidades y aprovecharlas para atacar los equipos.

Puertas Traseras

En los sistemas operativos de aplicaciones grandes, es habitual el de insertar "atajos" para la autentificación del programa o núcleo que se diseñe. A estos atajos se les conoce como puertas traseras. Con esto se consigue una velocidad mayor para su depuración y la detección de fallos.

Si un atacante descubre una de estas puertas traseras, corremos el peligro de que tengan un acceso global a datos que no deberían ver y pone en existencia la debilidad y aparte la integridad del sistema.

Bombas Lógicas

Son parte de códigos de programa que normalmente permanecen sin hacer nada, hasta que son activadas por el usuario a través de una función específica. Cuando son activados, estos programas suelen ser perjudiciales.

Canales Cubiertos

Son canales de comunicación que permiten la transferencia de información, de tal manera que violan las reglas establecidas en el servidor donde se encuentra la información. Sin embargo, este tipo de amenaza no es muy habitual, ya que los atacantes prefieren otro tipo de ataques lógicos más fáciles.

Virus

Los virus, al igual que las bombas lógicas, son una secuencia de líneas de programa que se inserta en un archivo ejecutable (se le denomina huésped) oculto a la vista del usuario; de forma que cuando el archivo se ejecute, también lo haga el virus.

Gusanos

Son programas capaces de ejecutarse y propagarse a sí mismos a través de las redes. Aprovechan los bugs para conectarse y dañarlos, llevando consigo en ocasiones algún tipo de virus.

Caballos de Troya

Son líneas de instrucciones escondidas en un programa de forma que parezca que realiza las funciones que desea el usuario, de tal manera que ejecuta funciones ocultas sin el conocimiento de la persona.

Programas Bacteria

Con este nombre se le conoce a los programas que no realizan alguna función útil, sino que solamente se reproducen hasta acabar con los recursos del sistema produciendo un conflicto y una negación del sistema.

Catástrofes

Esta categoría es la amenaza menos probable de causar daño a nuestro entorno, pero como se mencionó antes, no estamos a salvo de algún siniestro. Es por esto que se toman algunas medidas básicas de prevención y políticas de seguridad para el respaldo de la información.

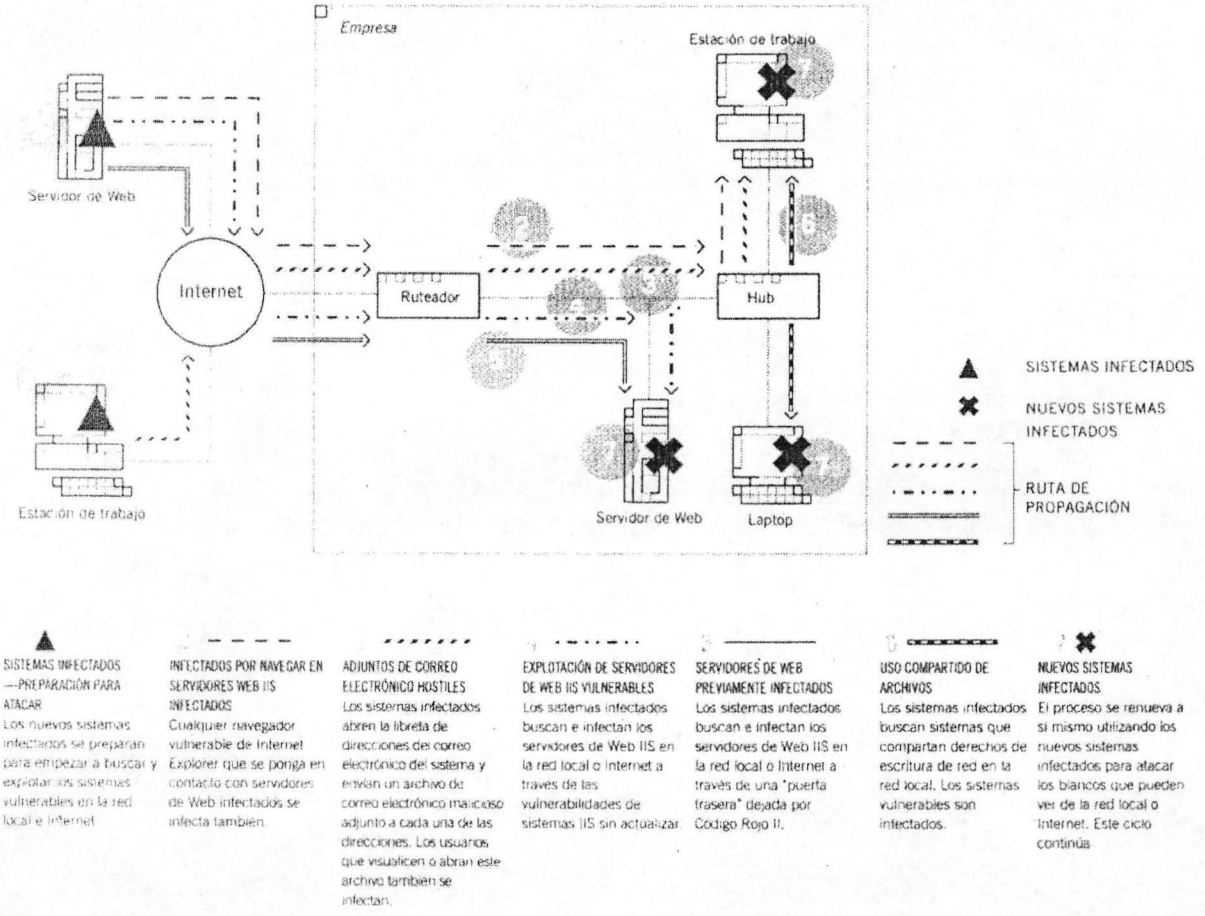


Figura 2 Método de Ataque del Virus Nimda

Los métodos de propagación del gusano Nimda. Cada ruta numerada representa una de las distintas formas en que Nimda se propaga. Múltiples métodos de propagación es una de las características de las amenazas combinadas.

1.1.3 ¿CÓMO NOS PODEMOS PROTEGER?

En los puntos anteriores se ha hablado de aspectos que pueden incluirse en la política de seguridad y que crearán responsabilidades para que dichos eventos mencionados anteriormente, no ocurran. A todo lo anterior se le denomina mecanismos de seguridad y se vuelven la parte más visible del sistema, además de que se convierte en la herramienta básica para poder garantizar la protección del sistema o red[3].

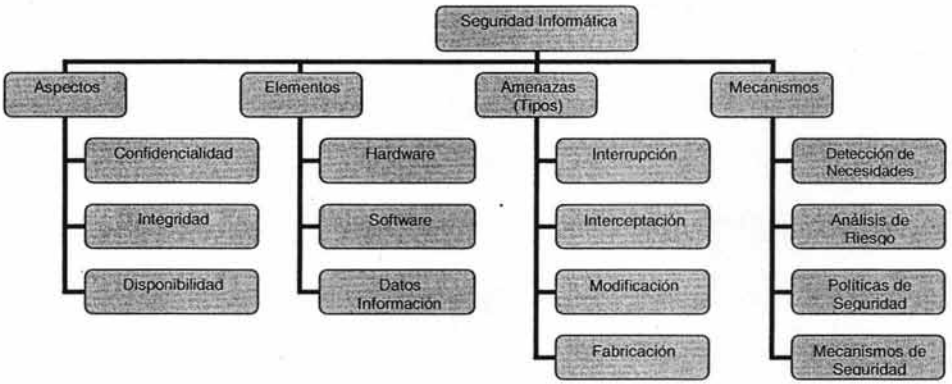


Figura 3 Esquema global de la seguridad informática

Para poder establecer los mecanismos o estrategias de seguridad podemos partir de hechos que hayan ocurrido anteriormente en la empresa o industria, considerando los siguientes puntos:

- Detección de Necesidades
- Análisis de Riesgos
- Políticas de Seguridad.

[3] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pag. 11

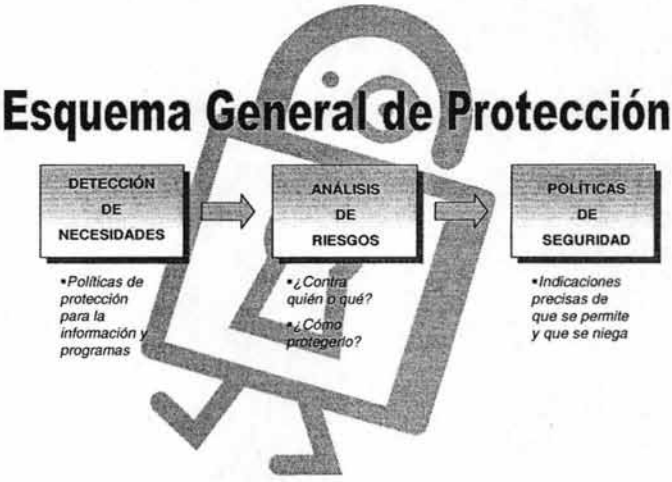


Figura 4 Esquema General de Protección

DETECCIÓN DE NECESIDADES

Este punto es el que nos permitirá establecer más adelante nuestras políticas de seguridad cuestionándonos ¿Quién soy? y ¿Qué información manejo? Esto lo podemos hacer desde dos puntos de vista; tanto como administrador como al mismo tiempo usuario final.

La primera pregunta es más comúnmente que la hagamos como administradores y no tanto como usuarios, ya que un usuario que utiliza la computadora y no es administrador no se preocupará por querer crear una política de seguridad para un centro de cómputo. Entonces, si soy administrador, tenemos un panorama mejor definido de las necesidades que queremos proteger.

En cuanto a la segunda pregunta ¿Qué información manejo?; es definitivo que haremos una política de protección general para todos los archivos de información y también para todos los programas que utilizamos incluyendo los sistemas operativos y software indispensable para la organización.

GRUPO MASSAT es un despacho contable que se compone de 4 áreas fundamentales que son Contabilidad, Nómina, Auditoria y Sistemas (Soporte Técnico); dentro de las necesidades de la empresa GRUPO MASSAT, S. DE R.L. DE C.V. (y en específico para las áreas contables) se encuentran los siguientes:

- **PROCESOS**, en el cual reconocemos el almacenamiento y modificación de las bases de datos y toda información que sea generada por los usuarios, como aquella que sea obtenida de Internet.
- **EQUIPOS**, en este rubro entran todos aquellos que forman parte de la empresa para permitir el uso diario de los datos almacenados. Computadoras para usuarios finales, servidores para almacenar información, cableado de red para la comunicación entre computadoras (LAN), servicio de Internet mediante un gateway proporcionado por un proveedor especializado (MAXCOM, S.A. DE C.V.), dispositivos portátiles de almacenamiento de datos, reguladores para energía eléctrica, entre otros.
- **SERVICIOS**, los que son necesarios para esta empresa es el acceso a Internet contando con acceso al sitio web y al correo electrónico, acceso permanente al servidor local donde se encuentra la información, esta se almacena y modifica en la aplicación "Conta2000 para Windows" recientemente migrado de su predecesor que funcionaba en MS-DOS; protección antivirus que deberá estar actualizado constantemente (la única manera de actualizarlo es vía Internet) y actualizaciones de sistemas operativos disponibles por Internet.
- **USUARIOS**, para la empresa GRUPO MASSAT, el número de usuarios total actual es de 16 a 20 comprendido en cuatro áreas que son contabilidad, nómina, impuestos y sistemas. Sin embargo se tiene una estimación de crecimiento a lo largo del año de hasta aproximadamente 30 o tal vez 40 usuarios; todos con diferentes IP's para hacer posible la comunicación a través de la LAN.

Una de las prioridades más importante es el acceso constante a bases de datos contables seguida de la disponibilidad de la información que llega por correo electrónico y la disponible en Internet y por último sus herramientas de trabajo, que en este caso son los equipos de cómputo.

El siguiente esquema muestra la distribución geográfica de los usuarios.

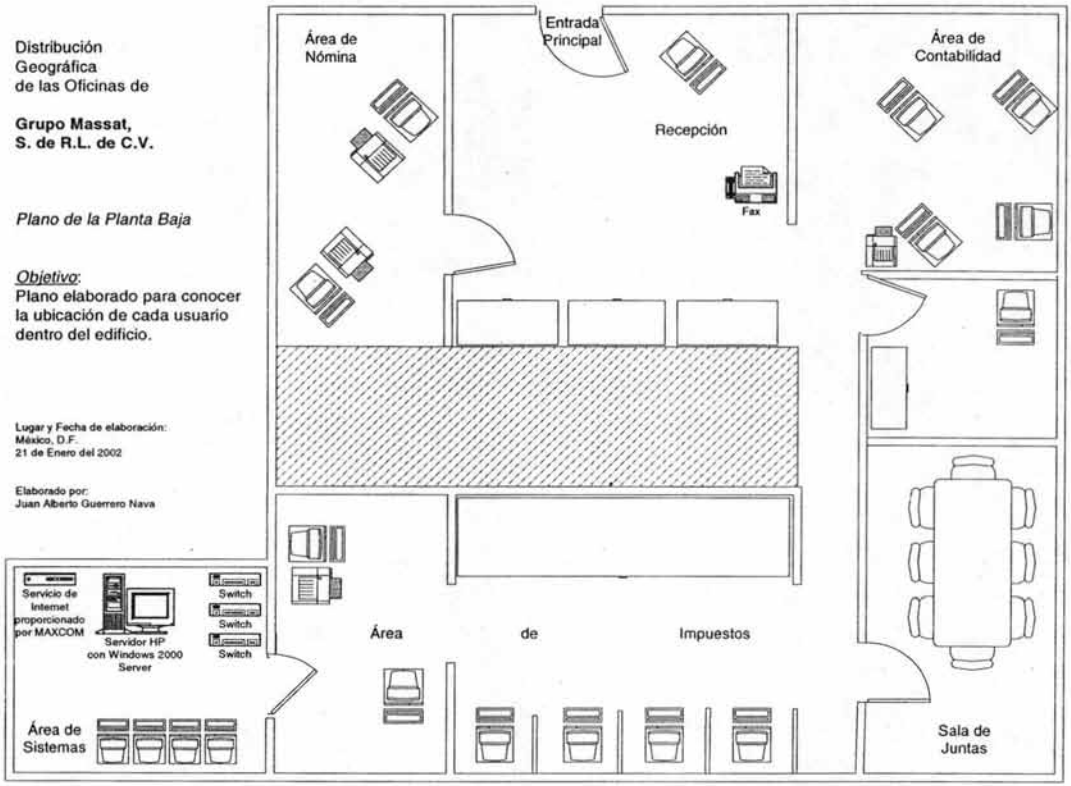


Figura 5 Distribución de los usuarios en Grupo Massat

Para esta empresa no existe un orden específico de prioridades, así que la prioridad uno será la accesibilidad a las bases de datos; después tomaremos como prioridad dos el acceso al servicio de correo electrónico, ya que es uno de los métodos de comunicación existente con los clientes y que sirve como técnica de intercambio de archivos e información.

Como tercera prioridad se encuentra los equipos de cómputo y de oficina, que deben recibir mantenimiento por lo menos una vez cada dos meses; el mantenimiento se realiza debido a que se ha notado que en ciertas ocasiones el polvo es un factor que provoca el mal funcionamiento de la PC, pero no solamente se hace un mantenimiento a nivel hardware sino que también se debe realizar a nivel software mediante una auditoria de programas para saber que está permitido instalarse y que no.

ANÁLISIS DE RIESGOS

Este término hace referencia al necesario proceso de responder a preguntas frecuentes como son ¿Qué queremos proteger? ¿Contra quién o qué? y ¿Cómo queremos protegerlo? Conociendo y evaluando los riesgos que enfrentaremos, se podrán implementar soluciones prácticas para minimizar efectos.

Siendo esta una empresa de giro contable, su mayor riesgo es el de la pérdida de información seguida de posibles fallas ya sea en la base de datos o en el acceso al servidor. Existen otras fallas de orden natural que escapan de nuestras posibilidades de hacer algo, una de estas son la falla de energía eléctrica, tal vez un incendio o siendo dramáticos un sismo que pudiera ocasionar alguna grieta en el edificio de tal manera que este se derrumbe.

Siguiendo el punto anterior acerca de las prioridades en la detección de necesidades, estableceremos ejemplos acerca de causas posibles que generen problemas y de posibles medidas de implementación para su corrección.

Causa	Se puede deber a	Posible corrección
No hay acceso al servidor donde se encuentra la base de datos	El sistema operativo no reconoce al usuario o su contraseña.	Asignar una nueva identidad al usuario o cambiar solamente la contraseña.
	La tarjeta de red de la estación de trabajo tiene fallas.	Si el problema es físico (previo pruebas realizadas en otra PC), habrá que cambiar la tarjeta de red. Si el problema es del tipo software (previo pruebas realizadas en la PC o en otra PC), habrá que instalar la correcta versión del controlador del dispositivo.
	Problemas con el cable de red, el conector o el puerto terminal del Hub o Switch donde se encuentra conectada la PC.	Para determinar el origen del problema deberá usarse un probador de cables de 8 hilos. Suponiendo que el problema se encuentre en el Hub o Switch, se deberá asignar un nuevo puerto a la estación de trabajo, en caso de que exista alguno libre.
No se puede acceder a la base de datos	El número permitido de usuarios para acceder la base de datos.	Contactar al proveedor de la base de datos par ampliar el acceso a un mayor número de usuarios.
	Problemas con la tarjeta de red y/o el cableado de red.	Cambio físico de la tarjeta de red y/o instalación correcta del controlador del dispositivo. Para determinar el origen del problema deberá usarse un probador de cables de 8 hilos.
No hay servicio de Internet y/o correo electrónico	Problemas con el proveedor de Internet.	Contactar al proveedor del servicio y reportar el problema.
	Problemas con el administrador del sitio web y correo electrónico.	Contactar al proveedor del servicio y reportar el problema.
La computadora se congela repentinamente	Falla en el microprocesador, memoria, disco duro u otro dispositivo.	Realizar una extensa prueba de cada dispositivo y después realizar combinaciones para hallar la causa posible.
La computadora se apaga sin razón alguna	Problemas en el regulador de voltaje interno de la computadora o no está indicado el voltaje correcto.	Habrá que cerciorarse de que esté indicado el voltaje correcto en las PC's a 115v. Si el problema es mayor, como una pieza dañada, habrá que llevar el equipo a reparación con personal especializado en el tema.

Tabla 2 Diferentes Medidas de Implementación a diversos problemas

Como parte del análisis de riesgo se elabora una identificación de recursos y una identificación de amenazas (ver 1.3.1 donde se ejemplifica).

POLÍTICA DE SEGURIDAD

Se trata de un "término general" que se aplica a situaciones o recursos diversos; donde es necesario clarificar los requisitos de la política para transformarlos en indicaciones precisas de lo que se permite y se niega en la operación de un sistema (ver el apartado 1.3.3).

1.2 MECANISMOS DE SEGURIDAD

Los mecanismos de seguridad se hallan divididos en tres grupos que son:

1) De prevención
2) De detección
3) De recuperación

Los ***mecanismos de prevención*** aumentan la seguridad del sistema durante su funcionamiento normal, disminuyendo el riesgo de que ocurran violaciones a la seguridad; un ejemplo puede ser un programa criptográfico para la protección de los datos o el antivirus quienes tienen ciertas propiedades para evitar la entrada a algunos virus que circulan por Internet.

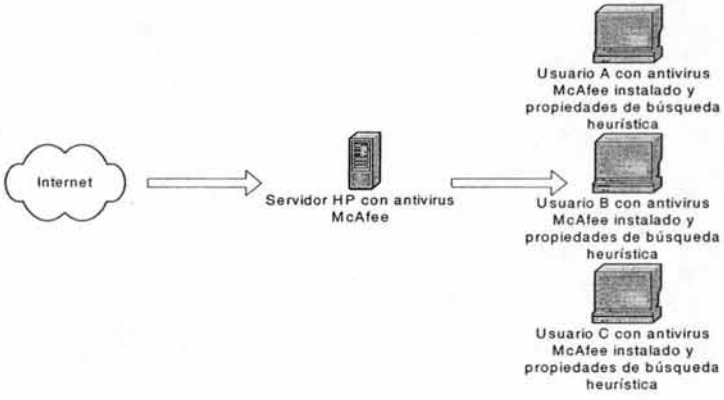


Figura 6 Ejemplo de Mecanismo de Prevención

Los ***mecanismos de detecciones*** se conocen por ser aquellos que detectan los intentos de violaciones o la violación de la seguridad; consideremos como ejemplo los programas de auditoria y los de monitoreo de la red local en cuanto a actividades irregulares como peticiones excesivas a Internet sin razón alguna, lo que podría dar pie a sospechas de que exista algún programa tipo caballo de troya.

Figura 7 Ejemplo de Mecanismo de Detección

Los ***mecanismos de recuperación*** se aplican para retornar el funcionamiento adecuado del sistema cuando se ha detectado una violación del mismo; como ejemplo se encuentran los programas de copias de seguridad, también existen otros programas de recuperación que ayudan cuando se ha borrado información de un disquete o un disco duro.

Figura 8 Ejemplo de Mecanismo de Recuperación

Puede parecer claro que estos tres tipos de mecanismos son importantes, sin embargo, se hará un énfasis en el uso tanto de los mecanismos de prevención como de detección; ya que éstos nos proporcionarán una buena seguridad al sistema que estemos usando.

1.3 POLÍTICAS DE SEGURIDAD

La palabra política hace que mucha gente sienta temor, ya que hace referencia a un documento que ha sido creado por algún tipo de junta o comité organizador. Sin embargo en este tema se hablará de la política que cuyo propósito básico es la de establecer una dirección teórica de lo que se intenta lograr.

Hay que tener en cuenta que será un proceso largo y difícil, ya que es exactamente el tipo de trabajo o tarea opuesta de la que disfrutan los técnicos.

Política de Seguridad es un término que se define como un conjunto de requisitos definidos por los responsables directos o indirectos de un sistema que indican en términos generales que es lo que está permitido y que no en el área de seguridad[4].

Sin embargo, la mayoría de los problemas que surgen los ocasiona la misma gente que quiere establecer una política de seguridad utilizando de tal manera un lenguaje y palabras técnicas que la mayoría de los usuarios no entiende, ocasionando que en determinado momento se sientan incómodos.

Consideremos de igual manera que intentar escribir una política de seguridad puede resultar difícil, ya que tenemos una idea firme de cómo debe ser dicho manuscrito y que posiblemente no siga el estándar que deseamos que tenga al estar finalizado.

Podemos pensar en una política absoluta donde habrá un solo sitio que nadie pueda penetrar, donde las contraseñas sean buenas y únicas y que nadie utilizará la contraseña de otro para algún fin. Por otro lado, si se tiene muy poca seguridad, la organización o empresa puede caer en manos de atacantes.

[4] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pag. 253

1.3.1 TIPOS DE POLÍTICAS DE SEGURIDAD

Dentro de los tipos de políticas de seguridad[5] podemos encontrar clasificaciones como las que se mencionan a continuación y que son las más comunes:

- Políticas de Seguridad para la protección del hardware.
- Políticas de Seguridad para la protección de información y software.

POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DE HARDWARE

El hardware es el elemento más caro de un sistema de cómputo pero no es el más difícil de recuperar.

La aplicación de barreras físicas y procedimientos de control así como las medidas de prevención y contramedidas contra las amenazas de los recursos y la información confidencial, es en lo que consiste la seguridad física de un sistema informático. Sin embargo, este aspecto es olvidado con demasiada frecuencia al momento de hablar de la seguridad o políticas de seguridad de uno o varios equipos informáticos.

Tomemos en cuenta lo siguiente, si queremos establecer una política de seguridad para este punto podemos realizar una ***identificación de recursos*** dentro de los cuales podemos obtener los siguientes: procesadores, impresoras, teclados, tarjetas de red, monitores, servidores, unidades floppy y CD, etc.

Acto seguido haríamos una ***identificación de amenaza*** que en el aspecto hardware sería una sobrecarga eléctrica, un sismo, un incendio, una inundación o simplemente daño del equipo ya sea por uso inadecuado o agotamiento del tiempo de vida.

[5] Una introducción al mundo de los firewalls, Damián Ferrer, 16 de Marzo 2003; http://www.kriptopolis.com

A partir de que se identificaron los recursos y sus posibles amenazas y que ya se establecieron las políticas de seguridad; el siguiente paso podría ser el de establecer ***estrategias de solución*** siempre haciéndonos la siguiente pregunta:

¿Qué podemos hacer cuando la política de seguridad ha sido violada?

POLÍTICA DE SEGURIDAD PARA LA PROTECCIÓN DE INFORMACIÓN Y SOFTWARE

Existen diferentes aspectos que debemos tomar en cuenta al momento de realizar una política de seguridad para el hardware, uno de estos aspectos será si nuestra información y datos no se ven afectados o dañados.

Si queremos establecer una política de seguridad para información y software debemos identificar los recursos como se hizo anteriormente. La identificación de recurso para software es el sistema operativo, programas de diagnóstico, programas de comunicación (Internet, Netscape, etc.), programas de herramientas de oficina, etc. La identificación de recurso para información es los almacenados en discos, cintas magnéticas, los que están en línea, bases de datos, etc.

Hacemos una identificación de amenaza como pérdida de información, datos irrecuperables, fallos en el sistema operativo, modificación por personas no autorizadas, etc.

A partir de que se identificaron los recursos y sus posibles amenazas y que ya se establecieron las políticas de seguridad; el siguiente paso podría ser el de establecer ***estrategias de solución*** siempre haciéndonos la siguiente pregunta:

¿Qué podemos hacer cuando la política de seguridad ha sido violada?

1.3.2 ELEMENTOS CLAVE DE LA POLÍTICA DE SEGURIDAD

Antes que nada, la política de seguridad es una forma de comunicación entre usuarios y administradores del sistema. Podemos considerar los siguientes nueve elementos como clave para la elaboración de nuestra de política de seguridad[6].

1. Explicaciones.
2. Leguaje común.
3. Autoridad para aplicar.
4. Disponibilidad.
5. Utilidad.
6. Integridad.
7. Autenticidad.
8. Confidencialidad.
9. Posesión.

Explicación	Es muy importante que la política de seguridad sea explícita, clara y comprensible desde un principio para saber el porqué deben tomarse ciertas decisiones.
Lenguaje Común	La mayoría de las personas no son expertas en temas como la seguridad y la computación. Es por eso que la política debe ser agradable a los usuarios, considerando que al momento que la están leyendo comprendan como si se les estuviera explicando.
Autoridad para aplicar	Este apartado hace referencia al de tener que vivir bajo la política de seguridad; si no se siguen las reglas alguien debe hacer algo para solucionarlo. De tal manera que existe alguien responsable de llevar a cabo las soluciones y la política especificará quién será esa persona.
Disponibilidad	Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten.

[6] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pág. 253

Utilidad	Los recursos y la información del sistema que se maneja debe ser útil.
Integridad	La información del sistema estará disponible exactamente como lo almacenó el administrador del sistema.
Autenticidad	El sistema verificará la identidad de los usuarios así como los usuarios identificarán al sistema.
Confidencialidad	La información estará disponible para su propietario y para el administrador del sistema.
Posesión	El administrador del sistema tendrá el control absoluto todo el momento.

Tabla 3 Elementos Clave de la Política de Seguridad

1.3.3 COMO CONFORMAR LA POLÍTICA DE SEGURIDAD

Para conformar una política de seguridad que funcione bien, es esencial el decidir cuál es nuestra opinión personal. De tal manera que si hemos administrado o tomado decisiones acerca de seguridad, de alguna forma se ha fortalecido una teoría o teorías internas acerca de seguridad.

Debemos tener claro y conciso lo que es una política interna, para así poder discutir con los demás, asuntos relacionados acerca de cómo establecer dicha política. Este sería un primer paso.

El segundo paso consiste en establecer qué significa la política de seguridad para los demás. Es decir, si yo soy usuario ¿qué esperaría de la seguridad? De igual manera, si yo soy administrador ¿qué esperaría de la seguridad?

Para poder contemplar una buena política de seguridad, habría que tomar muy en cuenta las necesidades de los usuarios. Si nos encontramos en una empresa con conexión a Internet; consideraríamos las necesidades del flujo de información. Veamos como ejemplo una política de seguridad con esta necesidad (se puede aplicar también para el apartado 1.1.3 en la sección DETECCIÓN DE NECESIDADES).

Política de Seguridad Informática para GRUPO MASSAT en su ramo informático Massat Computer Systems, S. de R.L. de C.V.
Necesidad del Flujo de Información. Control de la Navegación en Internet.
• Sólo los servidores de correo electrónico, deben ser los únicos autorizados para el envío y recepción de los mismos. • Todo lo que llega por SMTP debe ser filtrado por contenido, anexos, virus, encabezados. • Todo lo que llega por SMTP de archivos anexos, no rebasará la capacidad de 1.5 MB. • Todo lo que llega por SMTP de archivos anexos que tengan terminación ".exe", ".dll", ".pif" o ".scr"; se rechazará de inmediato. • Se restringirán todos los puertos y sólo se permitirán los más utilizados (http, ftp, SMTP, POP3) • Estará restringido el acceso a sitios Web como los pornográficos y los de ocio.

Tabla 4 Ejemplo de Reglas para el Flujo de Información

1.3.4 POSIBLES FACTORES EXTERNOS QUE INFLUYEN EN LA POLÍTICA DE SEGURIDAD

Existen elementos que se encuentran fuera del sitio donde está nuestra red local (empresa u organización). Tales elementos como la ubicación geográfica, formatos legales u obligación legal de cualquier tipo pueden ser factores externos que influyen en la elaboración de la política de seguridad.

De igual manera podríamos considerar ciertas leyes que en algún momento nos pueden frenar por considerar que los actos que realiza el administrador de la red en cuanto al monitoreo de la actividad del usuario, sea determinado como una invasión de su privacidad.

Si se tratase del lugar donde se ubica la empresa (rentan un piso o más en un edificio corporativo), se consideraría una política de revisión en cuanto el empleado dejara las oficinas o tal vez siendo menos estrictos, a su hora de salida. Un ejemplo podría ser el aseguramiento de la información, tratándose de información importante como una base de datos del gobierno.

Debemos abarcar a las personas afectadas por la política de seguridad, de tal manera que también tomen decisiones en cuanto a políticas y estrategias de seguridad; ya que son quienes más trabajan, y además, laboran en equipo.

Incluso una manera de asegurar la información y que puede ser tomada como una política de seguridad es el uso de herramientas de encriptación de datos y base de datos, que sólo se conecten a un servidor de la red local para su funcionamiento y no pueda ser usado en el exterior desde cualquier punto geográfico; de tal manera que la información siempre será resguardada por una contraseña que sólo será valida en la LAN. ¿Pero qué es la encriptación y todo lo que deriva de aquí?

1.4 CONCEPTOS DE BÁSICOS DE CRIPTOGRAFÍA

La criptología es la ciencia que se ocupa de los problemas teóricos relacionados con la seguridad en el intercambio de mensajes entre un emisor y un receptor. Esta ciencia se divide en dos ramas: **criptografía** y **criptoanálisis**. La criptografía se ocupa del cifrado de mensajes en clave y del diseño de criptosistemas. El criptoanálisis trata de descifrar los mensajes en clave rompiendo el criptosistema.

1.4.1 CRIPTOGRAFÍA

La criptografía es una de las ciencias más antiguas, ya que sus orígenes se encuentran en el nacimiento de la civilización; sin embargo hay quienes todavía la consideran un arte, como en el caso de la Real Academia de la Lengua Española.

El uso original de la criptografía era el de proteger la confidencialidad de la información tanto política como militar, sin embargo ya no se aplica exclusivamente a esas dos áreas, sino que ahora se encuentra disponible para todo aquel que quiera la confidencialidad y seguridad de determinados datos[7].

Aunque originalmente la criptografía mantenía en secreto un mensaje (lo que proporcionaba confidencialidad); en la actualidad también se busca garantizar la autentificación y la integridad de los mensajes.

1.4.2 CRIPTOSISTEMA

Un criptosistema es el diseño, como su nombre lo indica, de un nuevo sistema criptográfico. Matemáticamente se definiría {M, K, E, D} donde:

- **M** representa el conjunto finito de todos los datos del mensaje sin cifrar (llamado también *alfabeto*), a partir del cual se utilizan normas sintácticas y semánticas, pudiendo emitir un mensaje en claro (lo que se denomina texto plano o *plain text*).

- **C** representa el conjunto de todos los mensajes cifrados posibles.

- **K** representa el conjunto finito denominado *espacio de claves*, formado por todos las posibles claves empleadas, tanto en el cifrado como en el descifrado.

- **E** es el conjunto de transformaciones de cifrado (familia de funciones) del alfabeto en sí mismo. El proceso de cifrado se suele representar como: $E(k,m)=C$ donde $k \in K$, $m \in M$ y $C \in M$.

- **D** es el análogo de E, es decir, es el proceso de transformación de descifrado que se representaría como: $D(k',m)=M$ donde $k' \in K$, $C \in M$ y $M \in M$.

[7] Criptografía y Números Primos, Manuel Lucena, 22 de Julio 2003; http://www.kriptopolis.com

El emisor envía un texto claro, que es tratado por un cifrador con ayuda de una clave *k*, creando un texto cifrado o criptograma. Este criptograma llega a un descifrador a través de un canal de comunicaciones, el cual convierte el criptograma de nuevo en texto claro con ayuda de una clave *k'*; de esta manera, el texto claro debe coincidir con el texto originalmente enviado.

1.4.3 CRIPTOANÁLISIS

El criptoanálisis es la ciencia complementaria de la criptografía, ya que la criptografía trata de crear y analizar criptosistemas seguros; mientras que el criptoanálisis se encarga de romper esos sistemas demostrando así su vulnerabilidad.

Para establecer las debilidades de un sistema de cifrado, se analizan y asumen las peores condiciones del caso, como son:

I. La persona encargada del criptoanálisis tiene acceso completo al algoritmo de encriptación.

II. El criptoanalista tiene una considerable cantidad de texto cifrado.

III. Esta persona conoce parte del texto cifrado.

También nos encontramos con ataques específicos en donde posiblemente no se cumplan las condiciones antes mencionadas. Un método de ataque consistiría en probar todas y/o cada una de las claves posibles del espacio de claves denominando a este ataque como *ataque de fuerza bruta* o *exhaustivo*.

Cualquier algoritmo de cifrado se considerará seguro siempre y cuando soporte todos los ataques conocidos hasta ahora.

1.4.4 PGP (PRETTY GOOD PRIVACY)

Phil Zimmermann desarrolló este programa criptográfico para la firma digital de correos electrónicos basado en criptografía simétrica. PGP también permite el cifrado de archivos de una forma convencional mediante criptografía asimétrica; por lo tanto, esta parte de PGP lo convierte en una excelente herramienta de cifrado para nuestros requerimientos de sistema. No es el mismo mecanismo que se emplea para cifrar un archivo que el que se emplea para cifrar un correo.

Actualmente PGP se ha convertido en un estándar internacional, lo que da lugar a la aparición de varios productos de PGP que van desde el cifrado de correos y archivos hasta la encriptación de particiones de disco duro mediante el software PGPDisk. Así como también permite la codificación de TCP/IP por medio de PGPnet.

ESTRUCTURA DE PGP

Los algoritmos simétricos son considerablemente más rápidos que los asimétricos[8]; es por esta razón que PGP encripta primero el mensaje generando una clave de sesión aleatoriamente y enseguida codifica esta clave usando la llave pública del destinatario o lo que es lo mismo una contraseña (suponemos que existe un emisor y un receptor que utilizan PGP).

Cuando decodificamos un mensaje, PGP busca la cabecera de claves públicas con las que se codificó y nos pide la contraseña; si la contraseña es correcta PGP descifrará el mensaje.

La seguridad de PGP (o gran parte de éste) reside en la calidad del generador aleatorio de claves de sesión ya que si alguien obtiene la secuencia de claves que se usa en ese momento, podrá descifrar nuestros mensajes no importando a quien vayan dirigidos. PGP utiliza un método que genera números pseudo aleatorios muy seguro.

[8] Criptografía y Seguridad en Computadores, Manuel José Lucena López, Septiembre 1999, pág. 126

Figura 9 Funcionamiento de PGP

MEJOR RENDIMIENTO DE PGP

PGP podrá proporcionar gran rendimiento si se emplea de manera correcta, pero si se usa de manera inadecuada se convertirá en una protección inútil. Es por ello que mencionaremos tres puntos que harán de PGP nuestra mejor herramienta:

1. Escoger contraseñas adecuadas.
2. Proteger adecuadamente los archivos.
3. Firmar sólo las claves de cuya autenticidad estemos seguros.

VENTAJAS DE PGP

- Es un programa gratuito para usos no comerciales
- Está disponible para múltiples tipos de ordenadores y sistemas operativos
- Es un programa de manejo sencillo, especialmente si se usa a través de MS-DOS con una interfaz, o en otros sistemas operativos (Windows, Mac, Linux)
- Resulta virtualmente indescifrable si la longitud de la clave es lo bastante larga

DESVENTAJAS DE PGP

- Muchas veces sucede que el mensaje es auténtico pero la firma digital no puede ser comprobada por problemas técnicos
- PGP no hace salvaguarda alguna de ninguno de los datos de cabecera

1.4.5 FUNCIÓN HASH

Una de las herramientas de la criptografía son las funciones Hash, que sirven para comprimir un texto en un bloque de longitud fija y se utilizan en autentificación y firma digital. Es necesario recalcar que esta función ***NO ENCRIPTA***, solo comprime el texto. Los documentos a firmar son generalmente grandes; la función hash asocia una cadena de longitud de 160 bits lo que lo hace manejable para el propósito de firma digital. Una vez obtenidas estas cadenas de longitud fija se les denomina comúnmente ***resumen***.

Los algoritmos de funciones hash más utilizados son:

- MD5
- SHA

MD5

Su nombre proviene de Resumen de Mensaje (Message Digest), desarrollado por Ron Rivest; donde se procesan entradas de bloques de 512 bits generando una salida de 128 bits. El mensaje se rellena de manera que sea 64 bits más corto que un múltiplo de 512 bits, pudiendo procesar mensajes largos.

SHA

El nombre significa Algoritmo de Seguridad Hash (Secure Hash Algorithm). Es un algoritmo desarrollado por los Estados Unidos originalmente para la alta seguridad de los sistemas informáticos pretendiendo ser un estándar en protección de documentos. Este algoritmo funciona tomando una cadena de longitud menor a la de 2^{64} bits para producir un mensaje de 160 bits llamado resumen (mencionado anteriormente).

El resumen entonces puede ser usado en un Algoritmo de Firma Digital (Digital Signature Algorithm, DSA); el cual genera o verifica una firma para el mensaje. Comúnmente estos resúmenes son muchos mejores que los mismos mensajes pues es de menor tamaño que su original.

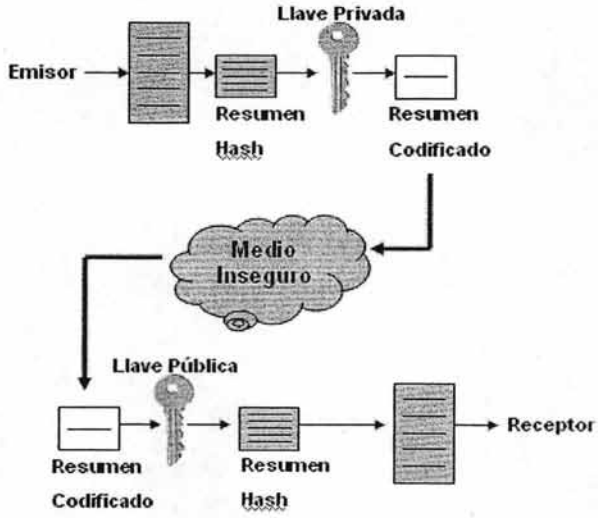


Figura 10 Funcionamiento de Hash

Los conceptos de seguridad informática; son parte de un proceso de creación, selección, implementación y ejecución de los firewalls en el que participan directa o indirectamente aquellos que manejan datos. Por supuesto, estos conceptos nos habrán de guiar hacia la toma de la decisión de qué firewall usar; ya que existen dos categorías diferentes dentro de los cuales hay diversas herramientas con diferentes características y capacidades.

Haber conocido acerca del funcionamiento de ciertas herramientas de encriptación, nos puede dar una idea acerca de los elementos que podríamos usar para aumentar el nivel de seguridad de una Red Local para evitar ataques que deriven en la pérdida de información o tal vez al daño físico del equipo.

Incluso en firewalls como los de CISCO, incluyen la herramienta 3DES (y otras más) como parte de su sistema que protege la transmisión de datos a través del Internet. Esto es, debido a que CISCO es líder en firewalls y por lo tanto como parte de su estrategia de mercado, debe estar al día con los avances tecnológicos.

CAPÍTULO 2

CONCEPTOS BÁSICOS DE FIREWALL

Los diversos conceptos fundamentales acerca de los firewall nos introducirán a sus elementos básicos y de ahí nos llevarán a conocer las diferentes arquitecturas que se pueden crear para una red local.

De igual manera, conoceremos los tipos de firewall como lo son los de software y los de hardware. Una vez que conozcamos estos conceptos, los encargados de administrar la red local podrán decidir que sistema es el mejor para implementar teniendo en cuenta ciertos puntos como podrían ser el costo y el uso e implementación del mismo.

Pero de manera general ¿qué hace un firewall? Simplemente es una herramienta más de protección cuya finalidad la define el usuario; el firewall es como una alarma que se activa cuando ha detectado cierta irregularidad en el lugar donde fue instalada. Supongamos un auto al que le acaban de instalar dicha herramienta, si el auto lo tratan de abrir la alarma se activará avisando al propietario; entonces, si hay un intento de ataque desde Internet hacia nuestra LAN, el firewall lo detectará dando aviso al administrador de la red.

2.1 INTRODUCCIÓN AL FIREWALL

La palabra firewall, desde la década de los ochentas, la han utilizado para describir a un dispositivo que bloquea el tráfico a una red de elementos no deseados. La primera descripción se hizo en el libro "***PRACTICAL UNIX SECURITY***" publicado en el año de 1990 escrito por Garfinkel y Spafford[9].

Los firewalls aparecen con mucha frecuencia cuando se trata de seguridad, comunicaciones, vulnerabilidades, etc. La simplicidad de esta palabra es lo que lo hace tan poderoso; ya que aplicando reglas adecuadas en un solo lugar, podemos controlar el tráfico existente entre una red externa y una interna.

[9] El ABC de la Seguridad Informática, Ulises Castillo, Agosto 1998.

2.2 DEFINICIÓN DE FIREWALL

No existe una terminología exacta acerca de lo que es un firewall, tanto en componentes como arquitecturas, ya que la gente puede interpretar los cortafuegos a su manera. Sin embargo la siguiente definición sirve de una manera clara para lo que se trata de explicar.

Un firewall (cortafuegos) es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre conjuntos de redes privadas, o una red privada e Internet. Podemos definir un firewall como un sistema (desde un simple *router* hasta varias redes en serie) utilizado para separar una máquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.

Daniel Ortiz[10], Coordinador de Tecnología de Trend Micro destaca con la siguiente opinión:

> *"un firewall es capaz de denegar los accesos no autorizados, pero no tiene la suficiente capacidad para detectar que en un intercambio de información haya una infección que ponga en riesgo a la máquina usuaria y por lo tanto, la integridad de toda la red".*

El espacio protegido, denominado ***perímetro de seguridad***, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa no confiable llamada ***zona de riesgo***.

Para entender lo que es un firewall, es necesario conocer sus componentes de funcionamiento.

[10] Revista RED, Octubre 2003

BREVES ESTADÍSTICAS

- El 50% de las compañías a nivel mundial ha sufrido un gran ataque.
- El 90% de las compañías atacadas tenían un antivirus y un firewall.
- En el 2003, el mercado de firewalls creció de un 30% hasta 34%.
- Para 2004, se espera que este mercado crezca hasta un 50%.

2.2.1 COMPONENTES DE UN FIREWALL

Uno de los componentes es el ***host*** o ***host bastión***, que se conoce como un sistema de cómputo conectado a una red y que además está asegurado, y que en principio estará inerme a ataques por estar abierto a Internet[11]. Su función es ser el punto de contacto entre los usuarios de la red interna con el exterior (otras redes o Intenet).

Figura 11 Host Bastión Simple

[11] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pág. 191

Dependiendo de la complejidad y la configuración de la red, un **host bastión simple** puede estar en guardia por sí mismo, o puede ser parte de un largo sistema de seguridad con diferentes reglas de protección. Los requerimientos pueden variar conforme al producto y necesidades de la empresa.

El ***filtrado de paquete***[12] es la acción de desaprobar el flujo de información entre dos redes, de acuerdo a ciertas normas o reglas ya preestablecidas. El filtrado lo puede realizar basándose en los siguientes campos:

- Dirección IP origen
- Dirección IP destino
- Puerto de origen
- Puerto de destino

Los ***servicios proxys***[13] son programas que permiten o niegan el acceso a una aplicación determinada entre redes. El proxy se divide en servidor y cliente; un ***servidor proxy*** es un programa que autoriza o devuelve las peticiones de los ***clientes proxy*** (un explorador web haciendo peticiones para conectarse a otro explorador web), comunicándose con algún servidor externo real.

Figura 12 Esquema Global de Firewall

[12] Servicio que se integra con el servicio proxy, el firewall y el caché para evitar que el contenido no autorizado de Internet sea accesado por los usuarios.
[13] Servicio para compartir una conexión simple de Internet a una oficina completa.

2.3 ARQUITECTURAS DE FIREWALL

Los firewalls tienen diferentes arquitecturas según las necesidades de seguridad de la empresa u organización que quiera implantarlo[14]. Aquí se listan algunos ejemplos de firewalls, que son las que se usan comúnmente:

- Arquitectura de Filtrado de Paquetes
- Arquitectura Dual Homed Host o Host con Doble Acceso
- Arquitectura de Host Protegido o Screened Host
- Arquitectura de Subred Protegida o Screened Subnet (DMZ)

2.3.1 ARQUITECTURA DE FILTRADO DE PAQUETES

Se trata de un modelo de firewall antiguo, el cual se basa en aprovechar algunos ruteadores para filtrar o bloquear paquetes según su protocolo, servicio o dirección IP. Sin embargo es el más común y fácil de emplear por ser pequeño en sitios sin ninguna complicación.

Esta arquitectura es la más usada en organizaciones o empresas que no requieren grandes niveles de seguridad, permitiendo que los accesos de la red interna hacia el exterior no bloqueados sean de manera directa.

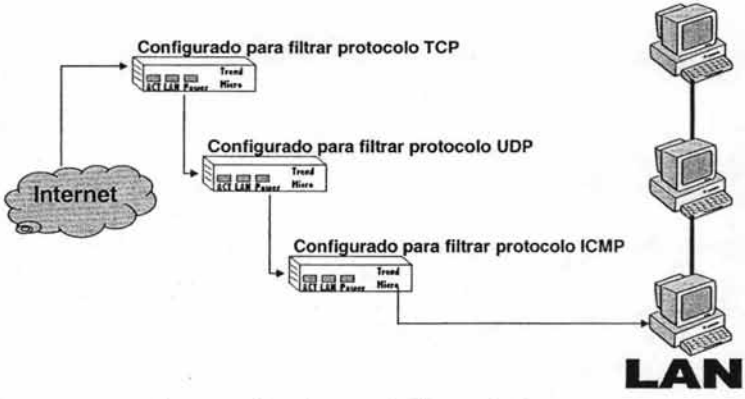


Figura 13 Arquitectura de Filtrado de Paquetes

[14] Seguridad en Unix y Redes, Antonio Villalón Huerta, Julio 2000, pág. 198

Puesto que esta arquitectura aprovecha los ruteadores que hay disponibles, es fácil usar cualquier sistema operativo como plataforma y su configuración y administración pueden ser relativamente sencillos, lo que representaría una clara ventaja al hacer uso de esta opción.

Sin embargo, si la empresa se encuentra en constante crecimiento; los ruteadores tendrían que ser de mayor capacidad para dar soporte a diversos usuarios y entre más usuarios más ruteadores y de mayor tamaño lo que sería una desventaja al requerir de más espacio físico y de más inversión.

2.3.2 ARQUITECTURA DUAL HOMED HOST O HOST CON DOBLE ACCESO

Otro modelo de firewall es el de *Host con Doble Acceso* que se construye alrededor de una computadora que tiene por lo menos dos tarjetas de red y que se denominan anfitrionas o interfaces de dos bases.

Una de las tarjetas de red se conecta con el exterior (Internet u otra red privada) mientras que la otra tarjeta se conecta a la red interna funcionando como enrutadores de paquetes IP. Sin embargo, los paquetes no se enrutan de forma correcta lo que ocasiona conflictos de comunicación bloqueada.

Si esto llegase a ocurrir, se detendrían las actividades laborales de los usuarios para poder solucionar el problema; siendo esta una desventaja que crearía pérdidas económicas a la empresa.

Realmente no existen ventajas con esta arquitectura, ya que para funcionar necesitaría de servicios proxys lo que presentaría un cuadro de inseguridad muy alto para la empresa.

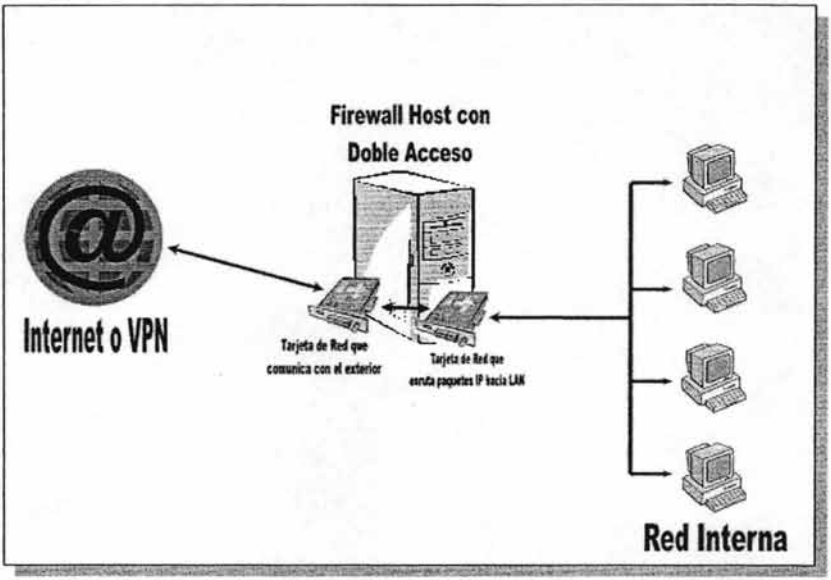


Figura 14 Esquema de Dual Homed Host

2.3.3 ARQUITECTURA DE HOST PROTEGIDO O SCREENED HOST

Por medio de esta arquitectura, se proporciona seguridad a través del filtrado de paquetes. El firewall de host protegido está combinado por un ruteador de filtrado de paquetes y un host bastión (o gateway) que se localizan en una subred protegida del sitio del ruteador.

El filtrado de paquetes en el ruteador está configurado de tal manera que el host bastión es el único sistema de la red interna con el cual los servidores externos se comunicarán, estableciendo cierto tipo de conexiones autorizadas, lo cual indica que el filtrado de paquetes también permite que el host bastión abra conexiones permitidas hacia el exterior.

Considerando este firewall, la configuración del filtrado de paquetes en el ruteador protegido podría negar o aceptar el tráfico de ciertas aplicaciones de acuerdo con los siguientes procedimientos:

- Se permite que otros servidores internos establezcan conexiones con servidores de redes externas.
- No se permitirán todas las conexiones de los servidores internos.
- Los ruteadores rechazarán el tráfico de alguna aplicación originada desde el exterior, a excepción de que provenga del host bastión.

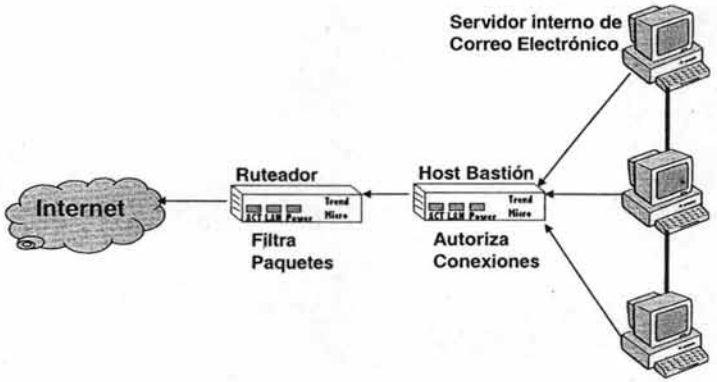


Figura 15 Esquema de Host Protegido

La ventaja que presenta esta arquitectura, es la posible combinación y el aprovechamiento de diferentes servicios; por ejemplo el uso del filtrado de paquetes para ciertas comunicaciones y el uso del servicio proxy para otros. Pero esto, dependerá de las políticas establecidas en la empresa para la seguridad de la red.

Sin embargo, la desventaja que presenta esta arquitectura es que si el Host Bastión es atacado, se permitirá crear una brecha de seguridad entre éste y el ruteador; comprometiendo así la integridad y la seguridad completa de la red.

2.3.4 ARQUITECTURA DE SUBRED PROTEGIDA O SCREENED SUBNET (DMZ)

Esta arquitectura también se conoce como *red perimétrica* o *De-Militarized Zone* (DMZ); se puede usar para localizar cada componente de los cortafuegos sobre un sistema separado añadiendo una capa o nivel de seguridad, es decir, colocando una subred entre la red externa y la red interna.

Los host bastión son máquinas vulnerables de la red a pesar de que se protegen. Este tipo de firewall es flexible, permitiendo servicios confiables entre Internet y la red interna; dependiendo de los niveles de seguridad establecidos en la subred. La creación de subredes en esta arquitectura permite crear hasta cierto punto, crear cierta sensación de seguridad (desde el punto de vista de administrador y usuario) es una ventaja.

Sin embargo, esta flexibilidad crea excepciones en la política de seguridad que a su vez origina un posible firewall débil; lo que sería una desventaja para la empresa y los administradores de la red local.

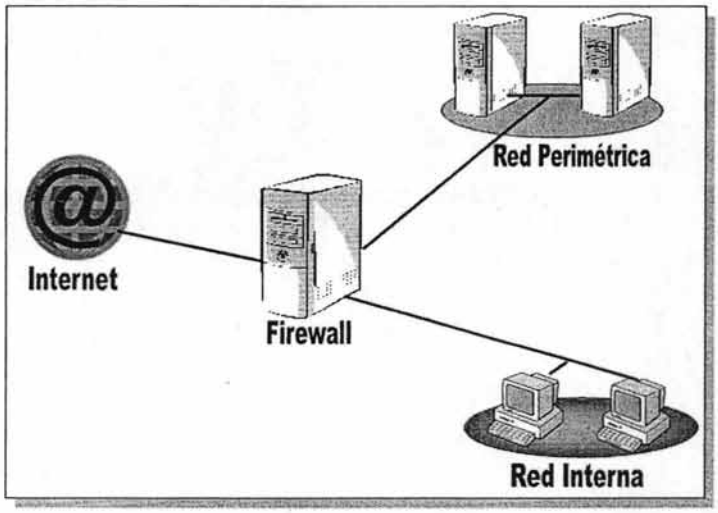


Figura 16 Esquema de Arquitectura de DMZ

2.4 TIPOS DE FIREWALL

Los firewalls son cada vez más necesarios en nuestras redes, pero esto no significa que se use exclusivamente como la herramienta perfecta de seguridad; al contrario es una de tantas herramientas que combinadas nos pueden dar la sensación de un sistema totalmente fiable casi llegando al concepto ideal de seguridad.

Desde que aparecieron los cortafuegos, estos han tenido varias formas de implementarse de tal manera que en la actualidad podemos identificar dos grupos:

- Firewall de Hardware
- Firewall de Software

Existe otra categoría que es los Firewall Personales; que básicamente surge de las necesidades de usuarios de computadora que se conectan a Internet por medio del módem y que se les conoce como usuarios para entornos de banda ancha. Los firewall para esta clase de usuarios vienen integrados normalmente en los antivirus como podría ser ***Norton Personal Firewall*** o ***McAfee Personal Firewall***.

Están diseñados para brindar la máxima seguridad posible al usuario, proporcionándole cierto nivel de protección, facilidad de uso y mantenimiento. Estos firewall contienen un asistente de configuración, así como varias configuraciones predeterminadas y no pierden su funcionalidad[15].

2.4.1 FIREWALL DE HARDWARE

Son equipos físicos que incluyen su propio software para operar, este programa generalmente no se instala en la computadora y se utilizan en las empresas, industrias, corporativos, etc.; para lograr rendimientos mejores. Sin embargo estos equipos tienen que ser administrados y operados por personal técnico altamente especializado.

[15] Firewalls: La Primera Línea de Defensa, Damián Ferrer, 16 de Marzo 2003; http://www.kriptopolis.com

FIREWALL DE CISCO

Cisco Pix, líder en esta rama de tecnología de seguridad, que tienen actualmente en el mercado diferentes series de estos firewall tipo hardware; ofrece diseños que proporcionarán un enriquecido servicio de seguridad y de alto nivel.

Los productos Cisco Pix Security Appliances (Aplicaciones de la Seguridad con Cisco Pix) proveen un buen rango de seguridad así como de servicios de red tales como son VLAN (Virtual Local Area Network, Red de Área Local Virtual); NAT (Network Address Translation, Conversiones de Direcciones de Red); PAT (Port Address Translation, Conversión de Direcciones de Puerto); filtros de contención para JAVA/ActiveX, filtros URL, soporte para PPPoE y mucho más. Incluye estándares de servicios avanzados de seguridad para datos de voz y multimedia.

Cisco Pix Security Appliances soporta clientes de acceso remoto para VPN (disponible para plataformas Microsoft Windows 2000 y 2003, Linux, Solaris y Mac OS X); proporciona tecnología de encriptado de datos utilizando Encriptación de Datos Estándar (Data Encryption Standar, DES); Triple DES (3DES) y el método Estándar Avanzado de Encriptación (Advanced Encryption Standar, AES).

A continuación se listarán algunos ejemplos de los productos Cisco de la serie 500, cada uno tiene su respectiva manera de instalación y configuración (se sugiere visitar la página web www.cisco.com), ejemplos sugerentes que pueden usarse en conjunto con otros firewalls y reforzar la seguridad de una red local:

1. Cisco Pix 501 Firewall
2. Cisco Pix 506E Firewall
3. Cisco Pix 151E Firewall
4. Cisco Pix 525 Firewall
5. Cisco Pix 535 Firewall

FIREWALL DE SYMANTEC

Symantec ofrece un producto similar que denomina con el nombre de **Symantec Gateway Security** siendo un dispositivo de seguridad de gateway que integra cinco funciones básicas que previene brechas de seguridad en el perímetro de la red.

Este dispositivo combina funciones como firewall, antivirus, detección de intrusos, filtrado de contenido y VPN. Symantec Gateway Security reduce costos y los posibles problemas que se presenten al adquirir, instalar y administrar los elementos individualmente; todas las funciones mencionadas antes pueden ser configurados y administrados de forma local o remota a través de una interfaz gráfica de usuario en la consola de administración llamada Symantec Raptor.

Symantec Gateway Security ofrece tres modelos para las necesidades de las empresas con 50 hasta 1000 nodos. Todos los modelos ofrecen máxima velocidad de transferencia, tiempo de actividad y escalabilidad, preconfigurados con mecanismo de alta disponibilidad y balanceo de cargas.

A continuación mostraremos en la siguiente tabla una comparación de los 3 modelos que Symantec ofrece:

	MODELOS		
	5110	5200	5300
Velocidad de Transferencia Máxima	Hasta 40Mbps	Hasta 90 Mbps	Hasta 90 Mbps
Velocidad de Transferencia Sostenida	12 Mbps	40 Mbps	40 Mbps
Fácil de utilizar y administrar	Sí	Sí	Sí
Incluye información de soporte	1 año de Soporte Gold	1 año de Soporte Gold	1 año de Soporte Gold
Tamaño de red recomendado	Hasta 50 nodos	Hasta 250 nodos	Hasta 1000 nodos
VPN remoto a sitio	Opcional	Opcional	Opcional
VPN sitio a sitio	Estándar	Estándar	Estándar

Alta Disponibilidad y Balanceo de Carga	Opcional	Opcional	Opcional
Firewall	Inspección completa	Inspección completa	Inspección completa
Antivirus	Tipo Carrier	Tipo Carrier	Tipo Carrier
Detección de Intrusos	Activada	Activada	Activada
Filtrado de Contenido	URL	URL	URL
ESPECIFICACIONES DE HARDWARE			
Puertos Ethernet	4 interfaces de red 10/100 BaseT independientes	4 interfaces de red 10/100 BaseT independientes	4 interfaces de red 10/100 BaseT independientes
Puertos Seriales	2 puertos	2 puertos	2 puertos
UPS (Sistema de Alimentación Ininterrumpida)	Admite UPS	Admite UPS	Admite UPS
LCD	Panel LCD para garantizar una instalación y administración útiles	Panel LCD para garantizar una instalación y administración útiles	Panel LCD para garantizar una instalación y administración útiles
Tensión de entrada	100/40 V, 50/60HZ	100/40 V, 50/60HZ	100/40 V, 50/60HZ
Consumo típico de potencia de operación	50 Vatios	100 Vatios	100 Vatios
Consumo de potencia máximo	60 Vatios	130 Vatios	130 Vatios
DIMENSIONES FÍSICAS			
Peso	4.2 Kg	10.7 Kg	10.7 Kg
Dimensiones (cm)	43.2 ancho x 31.8 profundo x 4.5 alto	44.5 ancho x 57.8 profundo x 4.5 alto	44.5 ancho x 57.8 profundo x 4.5 alto

Tabla 5 Diferentes Modelos del producto Symantec Gateway Security

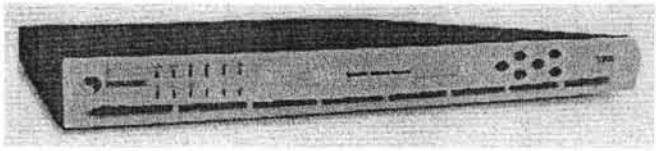


Figura 17 Firewall Tipo Hardware de Symantec

Para obtener más información acerca de estos productos se recomienda visitar el sitio web www.symantec.com.mx. En cuanto a los requisitos de sistema para el funcionamiento de la consola se requiere Windows 2000 o NT, 128MB de RAM mínimo y Procesador Pentium III de 300MHz o superior.

FIREWALL DE TREND MICRO

Trend Micro es otra de las marcas que tiene gran influencia en el mercado de la seguridad informática. En el listado de productos existentes en el mercado, se encuentran aquellos que se dedican a la protección de los servicios provenientes de Internet u otras redes locales; esta categoría se denomina **INTERNET GATEWAY**.

Dentro de esta categoría se encuentran subcategorías de productos a elegir, según los más convenientes para la empresa.

Aquí localizamos un producto en específico que puede ser combinado con firewall de software; **InterScan WebProtect para ISA** tiene compatibilidad con el programa de Microsoft y tiene las siguientes características:

1. Rastrea infecciones a través de los registros detallados de la actividad en cada archivo infectado o los intentos frustrados de violación de seguridad.
2. Provee una forma automática de actualizaciones en el web que están programadas en intervalos específicos a la vez que tiene la forma manual de hacer la actualización.
3. Provee un escaneo óptimo del tráfico http a través de la estrecha integración con Microsoft ISA Server.
4. Implementación rápida y fácil sin necesidad de algún cambio de cliente o usuario final.
5. Reduce costos y tiempo por no requerir la compra de hardware o software adicional.
6. Protege contra gusanos de Internet, como el famoso **CodeRed**.

Figura 18 Firewall Tipo Software de Symantec

VENTAJA DEL FIREWALL TIPO HARDWARE

La ventaja que presenta este tipo de firewall es la individualidad e independencia con respecto a la computadora, es decir; no necesita a la computadora al 100% para realizar sus funciones a excepción de la carga del software de configuración y administración (si es que tuviera, ya que algunos pueden ser configurados y administrados desde telnet).

DESVENTAJA DE FIREWALL TIPO HARDWARE

Este tipo de firewall presenta ciertas desventajas tales como el costo, administración y mantenimiento (se requiere de un especialista), en ciertas ocasiones las dimensiones físicas y en otras ocasiones no existen actualizaciones vía Internet para el producto. Estas desventajas pueden influir de manera fácil en una decisión de alguna persona que requiera comprar el equipo e instalarlo.

2.4.2 FIREWALL DE SOFTWARE

Aquí encontramos aplicaciones que corren sobre los sistemas operativos más populares como los son Windows NT, 2000 Server, 2003 Server y Advance Server y también UNIX y Linux. Estos a su vez su subdividen en modelos que defienden redes enteras como los específicos para defender servidores.

Desgraciadamente poseen una pequeña desventaja la cual es, que deben coexistir con el sistema operativo y por lo tanto su instalación es algo complicada igual que su mantenimiento; por esta simple razón se requiere de personal que sepa manejar el producto y además conozca bastante bien el sistema operativo.

Como ventaja ofrecen flexibilidad, ya que permiten adaptarse al software y hardware disponible. Este tipo de firewall, es conocido también como *Firewall de software corporativo.*

FIREWALL DE UNIX Y LINUX

Los cortafuegos para Unix y Linux vienen integrados en los sistemas operativos y su configuración se determina mediante el acceso al firewall para implementar políticas de seguridad mediante archivos de configuración como daemons (demonios), ipchains e iptables.

Para la configuración de un firewall en Linux, es común utilizar los ipchains ya que proporcionan las siguientes funcionalidades:

1. Bloqueo/Acceso del paso de datos basado en IP/Puerto/Interface de Origen/Interface Destino
2. Enmascaramiento de conexiones, basado en IP/Puerto/Interface de Origen/Interface Destino
3. Redireccionamiento de puertos
4. Creación de Cadenas para reglas y condiciones más complejas, y más fácil de mantener
5. Routing de calidad de servicio (Quality Of Service); útil en conexiones de baja velocidad o saturadas
6. Especificación de IP/Puerto/Interface

Veamos un ejemplo de configuración de ipchains en una máquina con Linux en donde queremos denegar el tráfico ICMP[16] que nos llega; para ello deberíamos ejecutar la sentencia siguiente:

alberto : ~ # ipchains –A input –p icmp –j DENY

[16] Internet Control Message Protocol, forma parte de los Protocolos de Internet integrado en los datagramas para el envío y recepción de información, asegurando que dicho fragmento de información no se pierda.

Con la opción "-A" se indica que se añade la regla especificada a la *chain*; "input" es una regla que afecta a los paquetes entrantes; "-p" especifica el protocolo deseado; "-j" indica el objetivo que en este ejemplo es DENY.

Como mencionamos anteriormente, se necesita de personal que conozca muy bien el sistema operativo para poder configurar correctamente el firewall. La configuración del cortafuegos en Unix o Linux puede ser bastante complicado y/o tedioso, lo que originaría el establecer mal una regla provocando que la comunicación con otras redes (incluyendo Internet) no se establezcan; haciendo del firewall un sistema de defensa débil. A continuación, veamos un ejemplo completo de comandos de Linux para la configuración de las ipchains de tal manera que sea una puerta de enlace ejecutándose en 2 interfaces. En la configuración de este script se utilizarán algunas variables que definiremos:

1. **ETH0IP** ES LA DIRECCIÓN IP DE LA INTERFAZ EXTERNA
2. **ETH0NET** ES LA RED
3. **ETH0NETMASK** ES LA MÁSCARA DE LA RED
4. **HOSTFIABLE1, HOSTFIABLE2** SON ANFITRIONES FIABLES PARA ADMINISTRACIÓN DE WEB/SSH
5. **ETH1IP** ES LA DIRECCIÓN IP DE **ETH1** (LA INTERFAZ INTERNA)
6. **ETH1NET** ES LA RED
7. **ETH1NETMASK** ES LA MÁSCARA DE LA RED

```
ETH0IP=1.1.1.1
ETH0NET=1.1.1.0
ETH0NETMASK=24
HOSTFIABLE1=1.5.1.1
HOSTFIABLE2=1.5.1.2
ETH1IP=10.0.0.1
ETH1NET=10.0.0.0
ETH1NETMASK=24

PATH=/sbin

ipchains –F input
ipchains –F output
ipchains –F forward

#Anti spoofing
ipchains –A input –p all –j DENY –s 10.0.0.0/8 –i eth0 –d 0.0.0.0/0
ipchains –A input –p all –j DENY –s 127.0.0.0/8 –i eth0 –d 0.0.0.0/0
ipchains –A input –p all –j DENY –s 192.168.0.0/16 –i eth0 –d 0.0.0.0/0
ipchains –A input –p all –j DENY –s 172.16.0.0/16 –i eth0 –d 0.0.0.0/0
ipchains –A input –p all –j DENY –s $ETH0IP –i eth0 –d 0.0.0.0/0

#ICMP
ipchains –A input –p icmp –j ACCEPT –s $ETH0NET/$ETH0NETMASK –i eth0 –d 0.0.0.0/0
ipchains –A input –p icmp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0

#SSH
ipchains –A input –p tcp –j ACCEPT –s $HOSTFIABLE1 –i eth0 –d 0.0.0.0/0 22
ipchains –A input –p tcp –j ACCEPT –s $HOSTFIABLE2 –i eth0 –d 0.0.0.0/0 22

#BLOQUEO 1:1023
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1:1023
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1:1023

#BLOQUEAR OTRAS COSAS
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1109
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1524
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 1600
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 2003
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 2049
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 2105
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3001
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3001
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3128:3130
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3128:3130
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3306
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 3306
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 4444
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 6000:6100
ipchains –A input –p udp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 6000:6100
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 6667
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 7000

#ADMINISTRACION DE WEB
ipchains –A input –p tcp –j ACCEPT –s $HOSTFIABLE1 –i eth0 –d 0.0.0.0/0 10000
ipchains –A input –p tcp –j ACCEPT –s $HOSTFIABLE2 –i eth0 –d 0.0.0.0/0 10000
ipchains –A input –p tcp –j DENY –s 0.0.0.0/0 –i eth0 –d 0.0.0.0/0 10000

#REGLAS REDIRECCIONAMIENTO
ipchains –P forward DENY
ipchains –A forward –p all –j MASQ –s $ETH1NET/$ETH1NETMASK –d 0.0.0.0/0
```

Tabla 6 Ejemplo de IPChains

Sin embargo, los firewall para sistemas operativos como Unix o Linux no son los únicos que existen; también encontramos los diseñados para plataformas Microsoft, entre ellos los que están integrados en los antivirus como McAfee y Norton y el diseñado por Microsoft ISA Server (tema central de este trabajo).

FIREWALL DE SYMANTEC

Symantec ofrece un producto llamado Enterprise Security Firewall (Symantec Client Security) ofreciendo un servicio de 3 en uno; antivirus, firewall y detección de intrusos. Ofrece una ***administración integrada*** donde se puede instalar, configurar, administrar y actualizar las funciones antivirus, firewall y detección de intrusos de las estaciones de trabajo desde una sola consola.

Symantec Client Security garantiza una protección efectiva en el cumplimiento de la política de seguridad en las estaciones de trabajo analizando el tráfico de entrada y salida; a través de su integración de tecnología (firewall y detección de intrusos) realiza un análisis y comparación de tráfico entrante y saliente con los juegos de firma conocidos de tal manera que permite el bloqueo de una dirección IP hasta por 30 minutos cuando detecta un intento de intrusión. Para mayor información de este producto se recomienda visitar el sitio web www.symantec.com.mx

VENTAJA DEL FIREWALL TIPO SOFTWARE

Estos firewall tienen grandes cualidades a su favor, entre estas se encuentran la instalación, configuración y mantenimiento (sí se tratara de alguno compatible con los Sistemas Operativos Windows); el bajo costo (gratuito en el caso de Linux) y la principal es que no ocupa espacio físico.

En el mantenimiento, para ciertos firewalls existen actualizaciones y para otros se publican sugerencias de cómo mejorarlos vía programación.

DESVENTAJA DEL FIREWALL TIPO SOFTWARE

La desventaja de estos firewalls, al igual que los de hardware, es la necesidad de personal especializado en el producto. Otra desventaja es que no deja de ser un programa y como tal ocupa cierto espacio en la memoria de la computadora, en el disco duro y es un proceso que continuamente se ejecuta, lo que provocaría que la computadora o el servidor donde esté instalado se vuelva lento. Como es un programa, existen actualizaciones y herramientas de apoyo lo que genera más espacio y se ejecutan más procesos.

Las arquitecturas mostradas pueden dar ideas de cómo realizar una muralla de resguardo frente a la red mundial; orientándonos a tomar la mejor decisión acerca de que tipo de firewall es el mejor para implementar.

La decisión de usar un firewall de software; es en muchas ocasiones, la mejor opción dado que se tiene un mejor conocimiento de la herramienta gracias a la diversa información que existe en la web; y no presenta los riesgos que pueden existir en uno de tipo hardware, como una sobrecarga eléctrica o la falta de espacio para su instalación.

Sin embargo habría que considerar las ventajas y desventajas que este tipo de firewall presenta; no obstante, al final la decisión la tomarán los administradores encargados de la red local considerando el nivel de importancia de lo que deseen proteger.

CAPÍTULO 3

SELECCIÓN E IMPLEMENTACIÓN DEL FIREWALL CON MICROSOFT ISA SERVER 2000

Los productos Microsoft son conocidos a escala mundial hoy en día. Su popularidad es tal, que vemos su uso desde el hogar hasta en la empresa; la elección de qué programas usar depende de las necesidades del usuario, generalmente hablando.

En México, las Pequeñas y Medianas Empresas (PyME) han adoptado esta tecnología por su ambiente amigable y de fácil manejo. Por lo menos, nueve de cada diez PyMES basan todas sus operaciones y manejo de información con la tecnología Microsoft. Dentro de este 90% de PyMES, hay quienes utilizan servidores para el almacenamiento y administración de la información contando con acceso a Internet rápido.

Sin embargo, del 90% solo un 10% conoce o ha escuchado acerca de los firewalls pero no lo implementaron por falta de conocimiento acerca del tema. Quienes lo hayan intentado, no supieron como escogerlo o configurarlo si es que ya contaban con uno.

De estos datos, estamos entendiendo que las empresas se encuentran desprotegidas ante ataques de hackers y la mayoría han sufrido ataques continuos de virus.

Para GRUPO MASSAT, S. de R.L. de C.V.; el manejo de información de clientes es la operación normal de todos los días; sin embargo se encuentran desprotegidos y constantemente han tenido ataques de virus. Como es un despacho recién formado (inició sus operaciones en el año 2001), no ha tenido hasta el momento gran renombre a nivel nacional o internacional (aún cuando cuenta con oficinas en Cuba y New York), por lo cual no ha sido objeto de ataques de hackers.

Massat Computer Systems (ramo informático de Grupo Massat) conoce la posible problemática de tener información sin protección, se ha sufrido de severos ataques virales que ponen en riesgo la integridad de los datos. El ataque más severo lo tuvieron en el mes de Diciembre del 2002 dejando los sistemas operativos de las computadoras sin operabilidad y con pérdida de información de hasta un 70%. Otro ataque menos severo tuvo lugar en el mes de Noviembre del 2003, con consecuencias menos graves.

Dada la importancia de los datos que se manejan, se ha propuesto al dueño implementar una herramienta que permita restringir el uso del Internet a lo necesario y de "localizar" en los correos entrantes alguna indicación de virus. Esta herramienta propuesta es Microsoft Internet Security and Acceleration Server 2000; el cual se le explicó el motivo de su implementación en esta organización. A continuación se explica porqué se elige este software y no otro.

3.1 ¿CÓMO ELEGIR ESTE PRODUCTO?

ELECCIÓN DE UN FIREWALL DE MANERA GENERAL

El establecimiento de una protección a través del firewall, dependerá en gran medida de aspectos tales como la plataforma y sistema operativo que se usan en la empresa; y de otros factores tales como el rendimiento, su costo y el soporte que llegara a necesitar. Sería un acto ilógico seleccionar un firewall por las cualidades novedosas que pudiera tener sin estar seguros de que se adaptará adecuadamente a toda la infraestructura implementada en la empresa.

Además de considerar funcionalidad y compatibilidad, será necesario realizar una consulta con un especialista en seguridad informática para garantizar ciertas características adicionales tales como el soporte técnico del producto y la manera en que se otorga; pero sobre todo, los costos implicados en la elección del sistema de seguridad.

En resumen, se deben considerar los siguientes puntos para la correcta elección del firewall:

1. *Sistema Operativo.* En la elección del firewall se considerará el sistema operativo por medio del cual se desee configurar y administrar.
2. *Compatibilidad.* Siguiendo esta línea de decisiones, la compatibilidad juega un papel importante para que el firewall pueda ser implementado; si no hay compatibilidad con toda la plataforma de la empresa (dígase computadoras, red, sistemas operativos, etc.) el cortafuegos no se implementará con éxito.

3. *Rendimiento.* Con rendimiento se hace referencia al buen funcionamiento del firewall, y se puede comprobar con las características proporcionadas por el diseñador del firewall y siempre y cuando cumplan con los requisitos que exige la empresa.
4. *Costo.* Uno de los factores importantes es el costo al momento de la compra, el costo involucrado al momento de instalarlo y finalmente el costo por mantenimiento y soporte; estas tres características deberán ser evaluadas por aquellas personas que autoricen la compra del firewall.
5. *Soporte.* Todo producto (hardware y/o software) cuenta con personal altamente capacitado en soporte del producto. Se evaluará esta característica junto con el de costo para determinar la conveniencia de tener un firewall independientemente del tipo que se escoja.
6. *Requerimientos.* Los requerimientos se refieren a las necesidades del propio firewall como por ejemplo espacio en disco y buena capacidad de memoria (si se trata de firewall tipo software) ó de un sistema operativo compatible (en ambos tipos de firewall) para la administración, configuración y mantenimiento del firewall.

ELECCIÓN DE ISA SERVER

La elección se basa principalmente en la plataforma y compatibilidad de Internet Security and Acceleration Server 2000 con el sistema operativo usado en la empresa donde se desea instalar, en este caso Microsoft Windows 2000 Server o Microsoft Windows 2003 Server (se recomienda leer el apartado ***3.2 Requerimientos de Hardware y Software***).

Grupo Massat, S. de R.L. de C.V.; cuenta con un servidor marca HP con ciertas características físicas que hacen posible el uso del sistema operativo Microsoft Windows 2000 Server (y que posiblemente pueda actualizarse a la nueva versión que es 2003 Server). Dado que requieren de alguna manera proteger sus datos de ataques externos y de virus, y considerando lo tardado y muy costosa migración de productos Windows a Linux; la decisión de instalar este programa se consideró principalmente en la compatibilidad con el sistema operativo del servidor y además, con las terminales de los usuarios.

La compatibilidad de este software, es casi general para cualquier sistema operativo Windows; a través de su Microsoft Client Firewall (Cliente de Firewall Microsoft), es posible la instalación del firewall en cualquier computadora que tenga un sistema Windows 98, Windows 2000 Professional, etc.

Con la elección hecha, el siguiente esquema nos muestra como debería quedar el sistema informático de la empresa una vez que se añada el firewall.

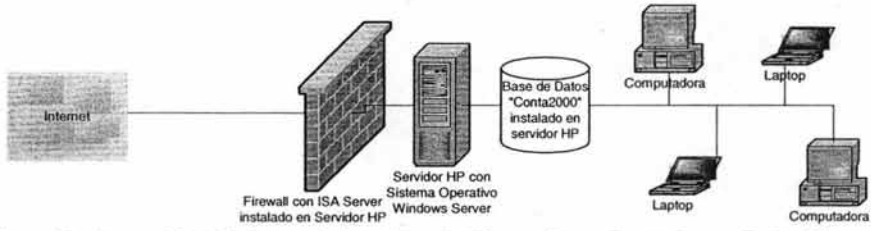


Figura 19 Proyección del sistema informático de "Grupo Massat" cuando se añada el firewall

Entre otras características para elegirlo, podemos hacer mención de la facilidad de configuración (ya que se basa en un ambiente gráfico agradable al usuario); la disponibilidad del proveedor en soporte técnico (vía Internet o telefónica); la fácil actualización vía Internet, lo que permite la compatibilidad de agregar módulos alternos (si los hubiera).

Y otro punto de elección, no menos importante pero sí el de mayor influencia; el costo en el momento de compra y el costo de mantenimiento a largo plazo. Si bien es cierto que este producto pertenece a la Corporación Microsoft, el costo de inversión no se debe ver a través de la compra de la marca, sino de la funcionalidad del sistema.

Este producto de la Corporación Microsoft se ha elegido específicamente para esta empresa, ya que todas sus operaciones se basan en tecnología Microsoft. Las necesidades que se mencionaron en el capítulo uno como la accesibilidad a la información, al correo electrónico y al Internet; han sido consideradas y este software cuenta con la flexibilidad de proporcionar dichos servicios y de administrarlos de manera segura como se haría con cualquier programa basado en esta plataforma.

En cuanto al costo de mantenimiento a largo plazo, no habría mucha preocupación ya que existen actualizaciones y ayuda gratuita en el sitio web de Microsoft.

3.2 ¿PORQUÉ UTILIZAR INTERNET SECURITY AND ACCELERATION SERVER 2000?

Microsoft Internet Security and Acceleration Server 2000 es un software empresarial de tipo servidor que ofrece servicios de reserva de espacio (cache) y firewall; maniobra en el sistema operativo Microsoft Windows Server. Está diseñado para ofrecer políticas de acceso basados en el control, aceleración y administración del trabajo vía Internet. Diseño que sirve para las concretas necesidades de Grupo Massat.

ISA Server (como se le conoce) proporciona ciertos beneficios como lo son:

- Aceleración
- Seguridad
- Dirección

ACELERACIÓN

Proporciona aumento de velocidad en el acceso a páginas Web mediante una reserva de espacio altamente funcional. Reduce nuestra conexión de ancho de banda y al mismo tiempo reduce el tráfico en nuestra red.

SEGURIDAD

Ofrece protección de accesos no autorizados por medio de la inspección del tráfico de información en la red; protegiendo también sitios Web (si disponemos de uno), correos electrónicos y otras aplicaciones de severos ataques externos. Para mayor seguridad, filtra paquetes de datos tanto de entrada como de salida. Establece accesos seguros para usuarios autorizados desde Internet hacia una red interna mediante redes privadas virtuales.

DIRECCIÓN

ISA Server provee control de acceso centralizado para asegurar y reforzar políticas corporativas de seguridad. Mejora la productividad de la organización limitando el uso aprobado de Internet hacia ciertas aplicaciones; también proporciona herramientas para monitoreo y produce reportes que muestran como es usada la conexión a Internet.

3.3 REQUERIMIENTOS DE HARDWARE Y SOFTWARE

Para poder realizar la instalación correcta de ISA Server es necesario cumplir con requisitos de hardware y software como los que se lista a continuación con sus respectivas características:

Componente	Requerimiento
Procesador	Superior a Pentium II o compatible que trabaje a 300MHz o más. Cabe mencionar que ISA Server soporta hasta 4 procesadores en su edición estándar para las pequeñas y medianas empresas. ISA Server en su edición empresarial no tiene límite para soportar procesadores y se usa en corporativos grandes.
Memoria	Se requiere de Memoria de Acceso Aleatorio (RAM) de una capacidad mínima de 256 megabytes (MB).
Espacio en Disco Duro	El espacio debe ser mínimo de 40 MB y aparte tener espacio para la realización de las reservaciones (cache). Se sugiere un mínimo de 2GB en adelante.
Formato del Disco y del Sistema de Archivos	Se recomienda una partición local de disco duro formateado con el sistema de archivo NTFS (New Technology File System).
Sistema Operativo	Microsoft Windows 2000 Server, Microsoft Windows 2003 Server o Microsoft Windows Advance Server. Se requiere instalar el Service Pack 1 para Windows 2000 Server (disponible actualmente la versión Service Pack 4 en el sito web de Microsoft). Es requerido que estos sistemas operativos tengan instalados el servicio de directorio llamado *Active Directory*.
Ambiente de Red	Se necesita una tarjeta de red que sea compatible con el sistema operativo Windows Server para realizar comunicación con la red interna y además tener un módem o un Servicio Digital de Red Integrado (ISDN) compatible con el sistema operativo Windows Server para la comunicación con Internet.

Tabla 7 Requerimientos para la instalación de ISA Server

Estos requerimientos los proporciona el mismo fabricante del producto y en ciertos momentos hacen concordancia con los requerimientos del sistema operativo Microsoft Windows Server.

Supongamos que el espacio en disco duro no es suficiente, el programa mismo detectará esta falta de espacio indicándonos que no puede proseguir la instalación. Si la computadora donde se instaló ISA Server no está en un ambiente de red, la funcionalidad del programa estará limitada a funciones locales en vez de administrar a una LAN (para lo que se diseñó originalmente).

En otros aspectos, el sistema operativo Microsoft Windows Server por sí solo presenta una estabilidad inicial del 50%; lo que indica que el otro 50% presenta fallas donde puede ser atacado por hackers y virus (el virus MSBLASTER ocasionaba que los sistemas operativos de Microsoft con tecnología NT se reiniciaran por sí mismos).

Estas fallas suelen ser corregidas por el fabricante a través de sus actualizaciones de seguridad o Services Packs (un conjunto de actualizaciones).

La instalación de ISA Server y su respectiva configuración, pueden ayudar a que estas vulnerabilidades no sean tan fáciles de atacar; aunque es aconsejable que se realicen dichas actualizaciones.

3.4 LUGAR DE IMPLEMENTACIÓN

La empresa decidirá qué tipo de firewall es el que le conviene más, considerando si mantendrá o no su plataforma basada en Microsoft (como se mencionó al principio). Pare el despacho contable Grupo Massat, la decisión de implementar ISA Server 2000 se debe principalmente al uso de tecnología Microsoft; se realizó una propuesta al dueño de la empresa, de añadir un servidor con sistema operativo Linux y configurar el firewall. Sin embargo, los costos de instalación, configuración y mantenimiento resultaron ser elevados por la sencilla razón de contratar servicios de un especialista en Linux para dicha tarea.

Este software puede ser implementado en empresas pequeñas y medianas que vayan de un mínimo de 5 computadoras (incluso puede ser 1 sola PC) hasta el máximo permitido por el programa según las especificaciones de Microsoft. Para Grupo Massat, este software cumple satisfactoriamente con las especificaciones requeridas (tomando en cuenta lo citado en el párrafo anterior); además se puede identificar una *topología estrella* de red, en donde las terminales se concentran en un punto terminal que es un switch o ruteador. En cuanto al número de usuarios, Grupo Massat actualmente tiene 20 empleados; lo que significa que son 20 usuarios de red con 20 terminales, y cada usuario en su computadora tiene un sistema operativo Windows de Microsoft Corporation.

Esquema General de Grupo Massat

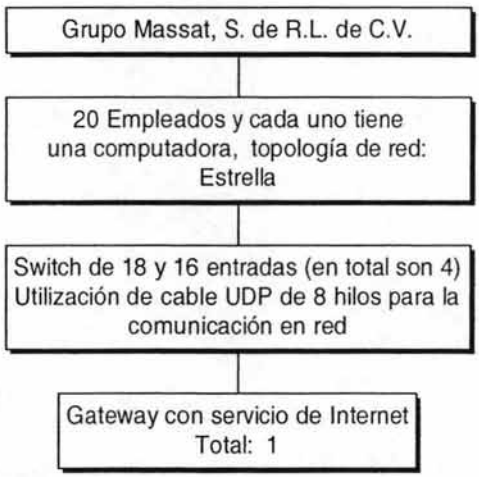
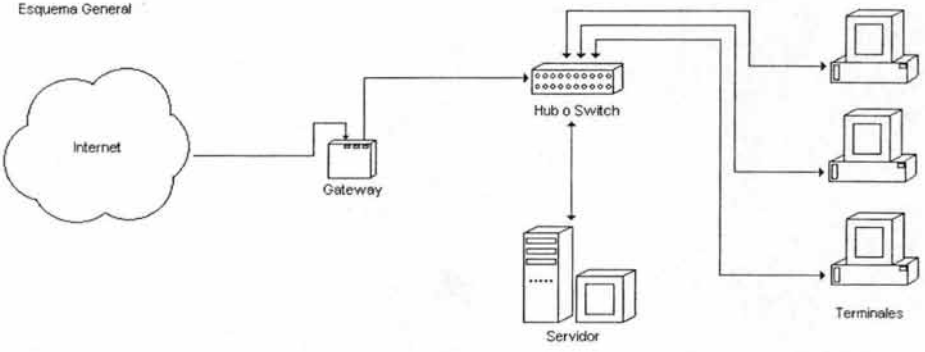


Figura 20 Componentes de la Empresa "Grupo Massat"

Proyecto de Cambio de Cableado Estructurado de Red para Grupo Massat

Objetivo: Renovar el cableado de red de Grupo Massat ya que el existente está muy deteriorado.
Aumentar el número de nodos por el posible crecimiento de esta pequeña empresa.

Esquema General



Esquema General de Grupo Massat (Procesos y Servicios)

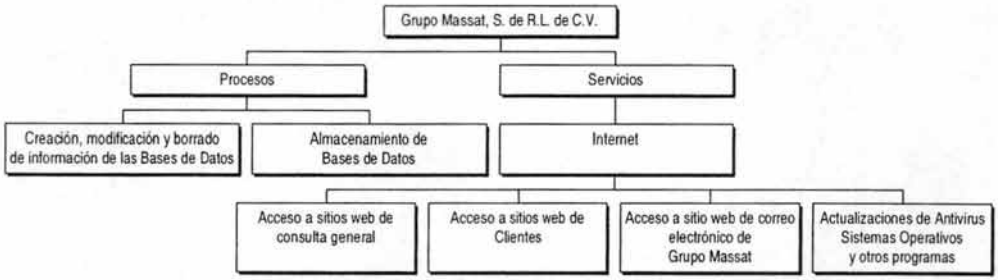


Figura 21 Procesos y Servicios de la Empresa "Grupo Massat"

Para poder justificar más claramente la implementación de Microsoft Internet Security and Acceleration Server 2000, mencionaremos una de las problemáticas más constantes para Grupo Massat (y para otras empresas). Dentro de los servicios que Grupo Massat necesita para desarrollar sus labores de manera normal, es el constante uso del Internet tanto para el envío y recepción de correos electrónicos como la consulta de diversas páginas web.

El servicio de Internet no está limitado de ninguna forma, lo que da acceso libre a cualquier sitio; generando así una necesidad de navegar en la red mundial causando distracción al empleado de sus labores. Un problema real es el uso del programa MSN Messenger que cada día adquiere un importante reconocimiento, motivo por el cual el dueño de esta firma ha solicitado se controle este problema. Una de las sugerencias fue el de implementar ISA Server.

Usar ISA Server representa la ventaja de tener que usar Windows 2000 Server o Windows 2003 Server, ya que de esta manera; ambos programas en su combinación representan una buena herramienta para poder delimitar funciones a los usuarios. Las limitaciones pueden llegar a ser un tema delicado; ya que si llegamos a limitar un servicio necesario por error, a la empresa le costaría por el retraso que generaríamos a sus empleados.

Para poder saber qué limitar y qué no, es necesario retomar la detección de necesidades de Grupo Massat. Necesidades que ya se mencionaron de forma general en el Capítulo 1.

Supongamos un ejemplo de empresa; una oficina con aproximadamente 100 contadores y auditores para quienes la información que generan como la que obtienen de clientes es importante y vital. Tienen acceso a Internet y tienen cada uno instalado un buen antivirus; es posible que logren evitar la entrada de varios virus, sin embargo la entrada no autorizada de algún intruso que cause daños a la información o la pérdida de los mismos sería fatal para esta oficina.

La implementación del ISA Server y en particular el firewall, ayudarían a parar estos ataques. Hago hincapié en que el firewall es tan sólo la primera línea de defensa. La buena implementación quedará a cargo tanto del administrador (establecimiento del nivel del firewall) como la elaboración de las políticas de seguridad.

Es recomendable el usar un buen antivirus que cuente con características como la búsqueda de cadena, búsqueda algorítmica y búsqueda heurística.

ISA Server, es una buena herramienta para implementar; teniendo buena flexibilidad y permitiéndonos crear las configuraciones y políticas correctas para evitar desastres como la pérdida de información.

La creación de filtros de paquetes sabemos que queda a cargo del administrador, por lo tanto tendrá la responsabilidad de determinar bien las reglas que deberán seguir los usuarios de la red de área local.

Estas reglas también pueden ser creadas en la medida que el administrador observe los reportes que proporciona ISA Server, estos reportes serán de gran ayuda para establecer nuevas reglas o mejorar las existentes.

3.5 INSTALACIÓN Y CONFIGURACIÓN DE ISA SERVER

Antes de empezar a instalar ISA Server, debemos verificar la conectividad de nuestra red para minimizar problemas de conexión después de que la instalación del software haya quedado completada. De igual manera, debemos prever la siguiente información:

- *El CD-Key.* Que se compone de 10 dígitos numéricos.
- *Las opciones de instalación.* Se refiere al modo de instalación y los diversos componentes que vienen incluidos en el software.
- *Selección de formación (Array Selection).* Referido al esquema de Active Directory modificado para iniciar en un entorno de red. Si este esquema no se ha iniciado, ISA Server será instalado como un servidor solitario en una PC.
- *Modo de Instalación.* La selección de instalación de ISA Server en el modo que más nos convenga; Modo Firewall, Modo de Espacio Reservado (Cache) o Modo Integrado.

Una vez identificados los requerimientos necesarios y la información que debemos considerar; podemos proceder a instalar ISA Server en nuestra computadora. Cabe recordar, que como es un producto de plataforma Microsoft, el proceso de instalación es sencillo ya que cuenta con ayuda incorporada para su instalación.

Insertamos el disco compacto en donde viene el programa de Microsoft Internet Security and Acceleration Server 2000; automáticamente iniciará una pantalla con diferentes opciones en donde elegiremos la opción de ***Install ISA Server***. Iniciará el procedimiento de instalación del producto como todo software de Windows; una pantalla de bienvenida y botones de comandos para seguir o salir de la instalación.

El proceso de instalación nos guiará hasta un punto en donde encontraremos la siguiente pantalla. Un cuadro de diálogo que nos ofrece opciones de instalación.

1. ***Instalación Típica***. Donde el producto se instalará con las opciones que comúnmente se usarían.

2. ***Escoger Instalación.*** Seleccionamos los componentes que se instalarán y que creemos nos ayudarán en nuestra labor de obtener seguridad para la empresa. En este punto, nos encontramos con los siguientes componentes de ISA Server como son *Servicios ISA*, *Servicios Incluidos* y *Herramientas de Administración.*

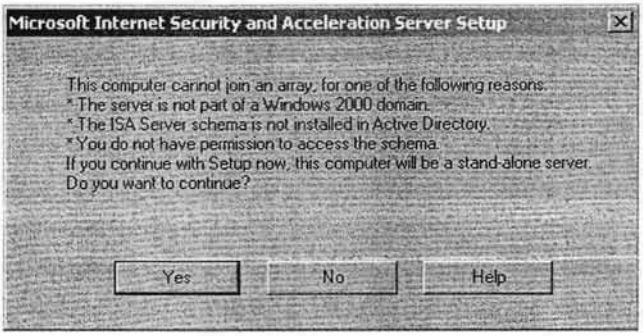
   - ***Servicios ISA.*** Este servicio es requerido, ya que contiene servicios para el tráfico y control de acceso entre varias redes.
   - ***Servicios Incluidos.*** Incluye el servicio Microsoft H.323 Gatekeeper y el servicio Message Screener. El protocolo H.323 es un estándar el cual permite las conferencias multimedia en tiempo real y las comunicaciones de las redes. El servicio Message Screener contiene filtro para el tráfico de entrada del protocolo SMTP.
   - ***Herramientas de Administración.*** Incluye herramientas de administración para ISA Server, el cual es requerido para la instalación; también incluye herramientas de administración para el servicio H.323 Gatekeeper el cual su instalación es opcional.

3. ***Instalación Completa.*** El programa de instalación copiará a nuestra computadora todos los elementos que ofrece ISA Server para poder utilizarlos.

Nos muestra además, la ubicación estándar donde se instalará Microsoft ISA Server; dándonos la opción de cambiar la ubicación de la carpeta del software.

Siguiendo con la instalación hallaremos el siguiente cuadro de diálogo que veremos a continuación, y que aparece por las siguientes razones:

- No pertenecemos a un dominio de Windows Server.
- No se encuentra instalado el servicio *Active Directory* de Windows Server o no se ha iniciado.
- No tenemos permisos de accesos al dominio.



Recordemos el *Array Selection*, si no se ha iniciado, el software por lo tanto, se instalará en el modo de servidor *stand-alone* (servidor solitario). Realmente, esta advertencia no tiene gran importancia; ya que, aunque exista un dominio podemos crear nuestro propio dominio, sin afectar el existente.

Lo importante es que nuestra computadora cuente con una dirección IP, para posteriormente, direccionar los demás equipos hacia nuestra IP de la PC donde se está instalando ISA Server.

SELECCIONANDO EL MODO DE INSTALACIÓN

En esta parte del proceso de instalación, habremos de elegir el modo que más nos convenga siguiendo los requerimientos y las políticas de seguridad del lugar donde se instalará ISA Server.

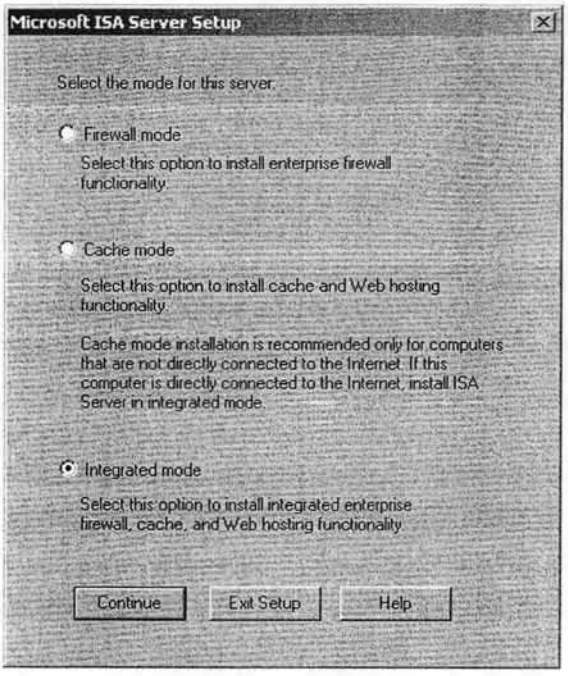


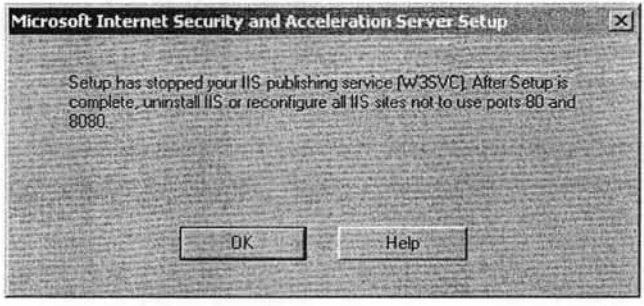
Figura 22 Opciones de instalación de ISA Server

En el cuadro de diálogo que se muestra arriba, nos pregunta el modo servidor para el software permitiéndonos escoger entre los siguientes:

- ***Servidor Modo de Firewall***. El cual instalará únicamente los servicios que pueda proporcionar un firewall.
- ***Servidor Modo de Reservación de Espacio (Caché)***. Hará la instalación únicamente de los servicios que proporciona el caché para el acceso inmediato a páginas web. Para este modo se recomienda, que la computadora no esté conectada de manera directa al Internet. Si el servicio de Internet entra directo por nuestra computadora, se recomienda instalar el modo *Servidor Integrado*.
- ***Servidor Modo Integrado***. Hará la instalación de los dos modos anteriores, proporcionando funcionalidad de servidor anfitrión en el acceso hacia Internet y servicios de Firewall.

Para ver la funcionalidad del software ISA Server, escogeremos el modo integrado no importando si nuestra PC tiene conexión directa con el Internet o no.

Cuando hemos presionado el botón "Continuar", aparece el siguiente recuadro diciéndonos que nuestro servicio de Internet Information Services conviene ser detenido para poder proseguir con la instalación. De hecho, se nos recomienda remover este servicio o reconfigurarlo no usando los puertos 80 u 8080.



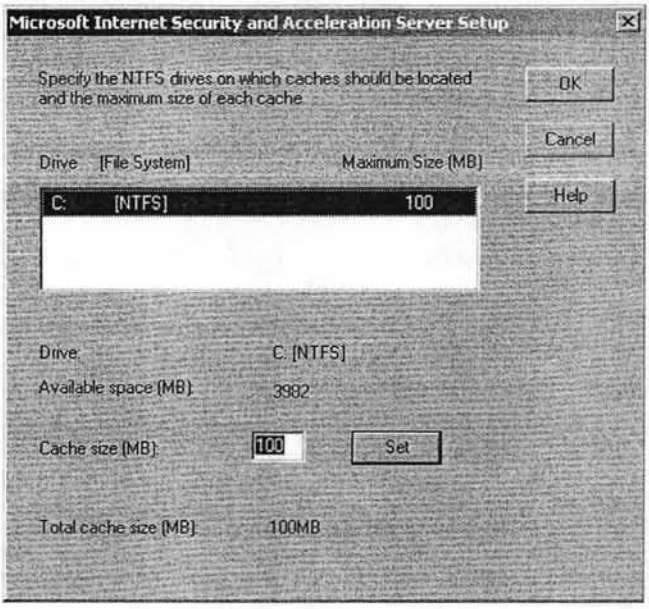
La causa de que se nos pide reconfigurar IIS, es debido a que ISA Server utiliza el puerto 80 para servicios Web, o en su caso el puerto 8080; y dos servicios no pueden usar el mismo puerto para la misma función.

INDICANDO EL TAMAÑO DE ESPACIO RESERVADO (CACHÉ)

Como hemos seleccionado la opción de modo integrado, el servicio caché nos solicita un espacio de reserva para el acceso a páginas web.

Por default, nos muestra la unidad C ya que no existe ninguna otra partición en nuestro disco duro; si existiese nos la mostraría listada. El sistema de archivos es NTFS que es el utilizado por los sistemas Windows Server. El tamaño mínimo estándar que muestra es de 100MB, modificable según las necesidades de los usuarios de nuestra red; es decir, que tanto se conecten a Internet y que tantas páginas consulten.

El espacio disponible puede variar conforme al tamaño del disco duro.



Se hace la recomendación de aumentar 0.5MB por cada proxy de cliente web, del que se quiera hacer uso.

CONFIGURANDO LA TABLA DE DIRECCIONES LOCALES

El programa de instalación de ISA Server 2000 nos pide definir una dirección IP o un grupo de direcciones de IP para las cuales el programa estará proporcionando servicio. Hay que notar que aparece un botón *Construir Tabla* que si lo presionamos tomará directamente las direcciones IP de la lista del programa Active Directory sin la necesidad de que el Administrador de la LAN tenga que definirlas manualmente.

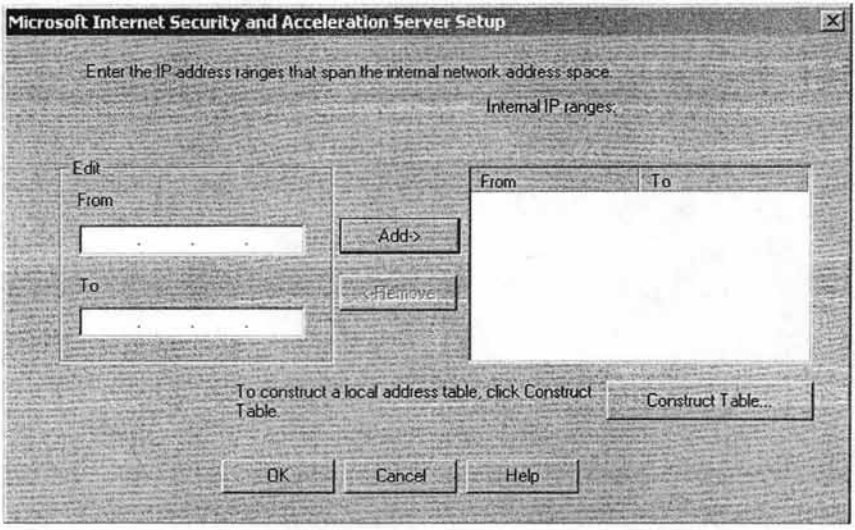


Figura 23 Tabla de Direcciones Locales en ISA Server

La construcción de las tablas se hace de manera general sin excluir alguna IP. El programa de ISA Server puede soportar direcciones IP reservadas para uso interno proporcionados por IANA (Internet Assigned Numbers Authority). Estas direcciones son las siguientes:

- De **10.0.0.0** hasta **10.255.255.255**
- De **192.168.0.0** hasta **192.168.255.255**
- De **172.16.0.0** hasta **172.31.255.255**

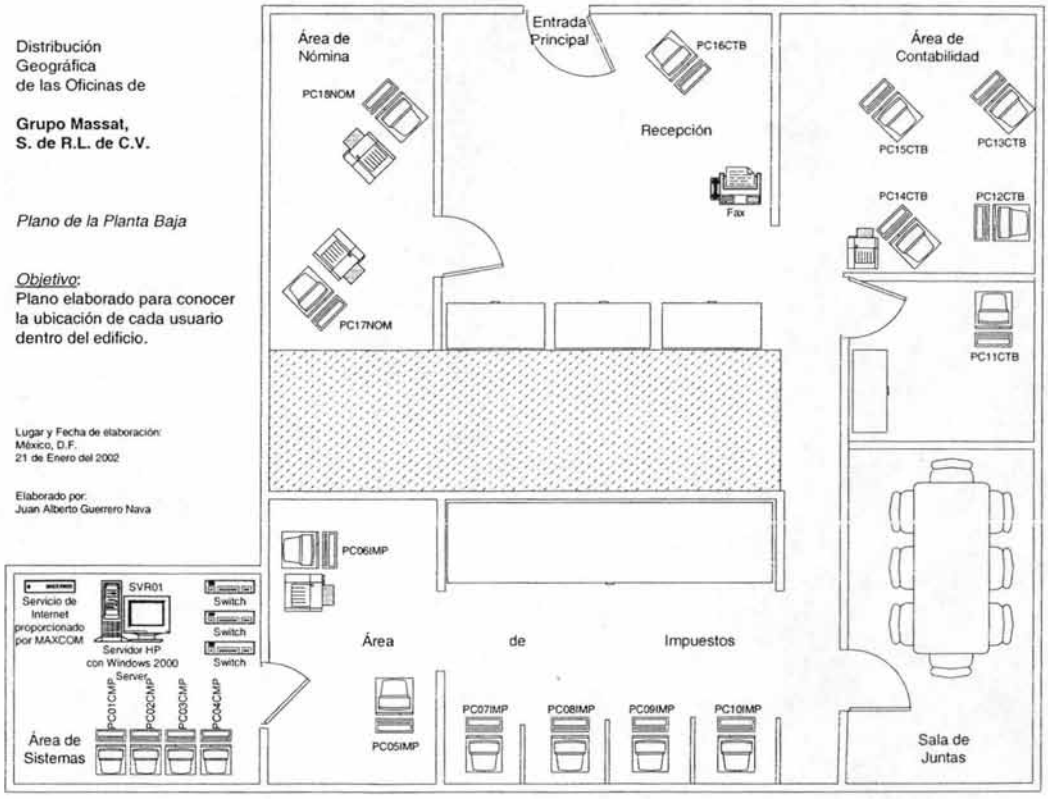
Si deseamos construir nuestra propia tabla de direcciones locales, podemos hacer uso del editor para incluir las direcciones que deseamos; es decir, si queremos el rango de direcciones IP de *10.60.1.1* hasta *10.60.1.30* y otro rango de direcciones IP que sea desde *172.18.0.55* hasta *172.19.0.10.* En el cuadro nos indica desde donde comienza la IP y en que IP terminará.

Una vez concluido todo el proceso de instalación de Microsoft Internet Acceleration and Security Server 2000, el programa comenzará inmediatamente a funcionar; dándonos opciones más adelante para poder modificar los parámetros necesarios para configurar este software.

3.6 CONFIGURACIÓN DEL FIREWALL

En este apartado del capítulo tercero, trataremos directamente con el tema central de este trabajo de investigación que es la configuración y el uso del firewall.

Considerando que el firewall es la primera línea de defensa entre una LAN e Internet, debemos de planear bien las políticas de configuración del cortafuego que harán de nuestra LAN un sitio seguro; por lo tanto, definiremos el escenario en donde se implementará dicho firewall de la siguiente manera: retomaremos el plano geográfico de la distribución de los usuarios (Capítulo 1 página 15) para diseñar una tabla con las aplicaciones que más comúnmente se usan.



Clave PC	Aplicación	Cliente	Servidor	Soft. Local
SVR01	S.O. Windows 2000 Server		✓	✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft ISA Server 2000 (incluye Firewall)		✓	✓
	Acceso a Internet sin restricción			
	Conta2000 para Windows		✓	✓
	Iomega Backup			✓
PC01CMP	S.O. Windows 2000 Profesional			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
PC02CMP	S.O. Windows XP Professional			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
	MSN Messenger	✓		✓
PC03CMP	S.O. Windows 98 Segunda Edición			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
PC04CMP	S.O. Windows 2000 Profesional			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
PC05IMP PC06IMP PC07IMP PC08IMP PC09IMP PC10IMP	S.O. Windows XP Professional o Windows 98 Segunda Edición			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
	MSN Messenger	✓		✓
	Sipred y Validador Sipred			✓
	DEM			✓
	DIM			✓
PC11CTB PC12CTB PC13CTB PC14CTB PC15CTB PC16CTB	S.O. Windows XP Professional o Windows 98 Segunda Edición			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción			
	MSN Messenger	✓		✓
	Conta2000 para Windows	✓		✓

Clave PC	Aplicación	Cliente	Servidor	Soft. Local
PC17NOM PC18NOM	S.O. Windows 98 Segunda Edición			✓
	Office 2000 Profesional			✓
	Antivirus McAfee On Line	✓		✓
	Microsoft Client Firewall	✓		✓
	Acceso a Internet sin restricción	✓		✓
	MSN Messenger			✓
	SUA			✓
	RAMSAL			

La tabla anterior muestra un escenario de los programas que tienen los equipos informáticos definiendo si son del tipo cliente o servidor. Usando esta información será posible poder contemplar reglas o políticas para configurar el firewall; en la tabla anterior observamos que en todas las computadoras tienen instalado el popular programa de MSN Messenger y que también tienen en común el acceso libre a Internet.

3.6.1 POLÍTICAS PARA LA CONFIGURACIÓN DEL FIREWALL

La primera decisión se trata de la política de seguridad de la organización propietaria de dicho firewall; la configuración y la potencia del nivel de seguridad serán distintas en una empresa que utilice el cortafuegos para el bloqueo de tráfico externo hacia el dominio de su propiedad frente a otra empresa u organización en dónde sólo se intente evitar el ocio de los empleados o usuarios internos en la red, un ejemplo sería bloqueado servicios externos tales como los *chats*, basándonos en la información obtenida anteriormente.

A continuación se añadirán algunos ejemplos de servicios tanto externos como internos que pueden considerarse para crear reglas de control en el firewall; de hecho algunas reglas están ejemplificadas en la tabla 4 del Capítulo 1.

1. Acceso a Internet por el puerto 80 u 8080.
2. Restringir el acceso a sitios web cuyo contenido sea inapropiado para las horas laborales, dentro de estos se consideran los pornográficos, casinos y juegos virtuales, deportivos, de los tipos religiosos, aquellos que ofrezcan información acerca de invasión de computadoras de manera ilegal (hackers), etc.

3. Determinar reglas para permitir descargas de archivos vía Internet, restringiendo específicamente aquellos que tengan extensión ".mp3" o alguno similar.
4. Minorizar o restringir por completo el uso de programas de mensajería instantánea (messengers).
5. Autentificar a usuarios que deseen ingresar a la red local desde el exterior, si se tratara de un intento ilegal se debe notificar al administrador o encargado de red.

La segunda decisión a considerar en el diseño, es el nivel de monitorización, redundancia y nivel deseado en la organización; una vez que la política se haya definido, habrá que examinar la forma en que se implementará el firewall indicando de manera básica que se permite y que se niega (el listado anterior nos puede otorgar ideas de esos permisos).

La tercera decisión es concerniente a lo económico, esto se da en valor de lo que deseamos proteger, es decir, considerar si debemos gastar más, gastar menos o simplemente no gastar nada.

CONFIGURANDO EL FIREWALL MEDIANTE EL ASISTENTE

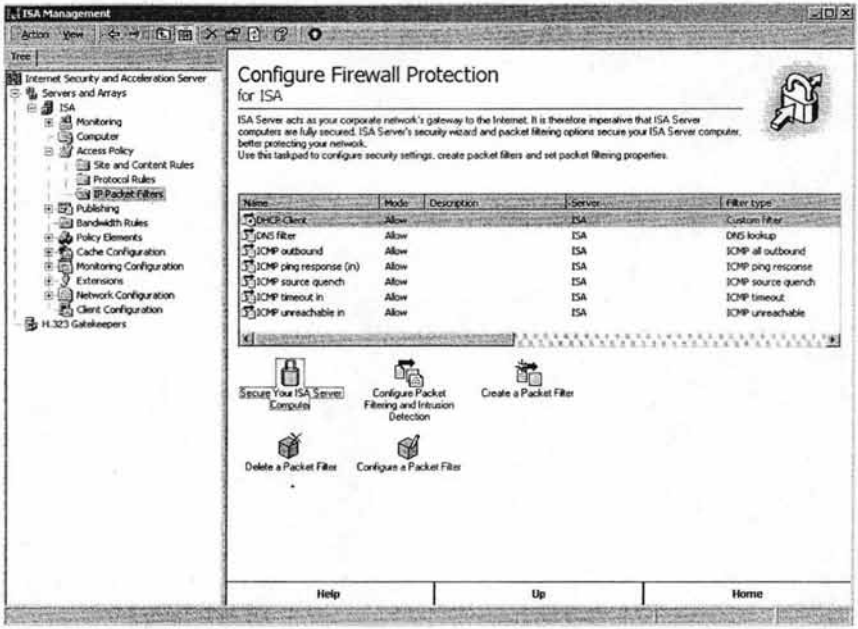


Figura 24 Asistente para la configuración del Firewall en ISA Server

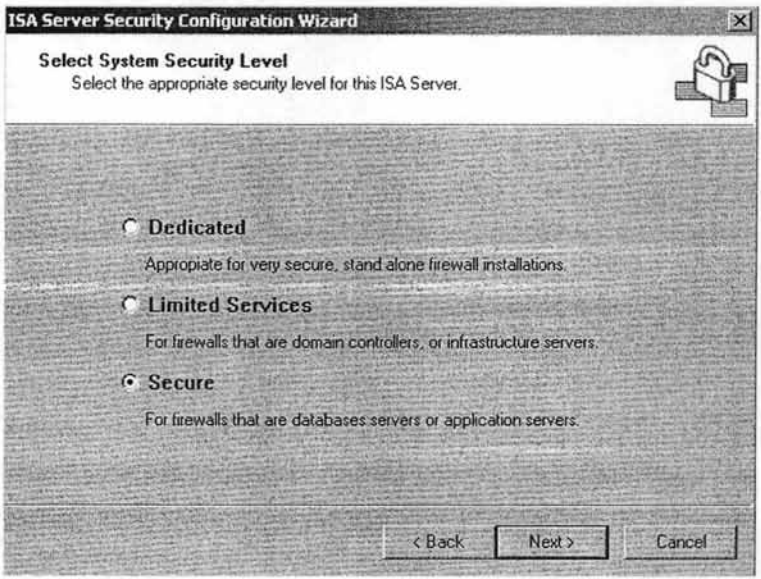
Usando el asistente para la configuración del firewall, en solo cuatro pasos se logra la configuración para un sistema seguro.

Lo primero que hay que hacer es desplegar desde nuestra consola de ISA Server la opción de *Políticas de Acceso*, para luego seleccionar *Filtro de Paquetes IP*. Presionamos en la opción *Asegurar Computadora con ISA Server*, y seguimos los pasos que nos muestra el Asistente de Configuración.

El nivel de seguridad seleccionado para el sistema, será determinado según haya sido el modo de instalación de ISA Server; en consideración con las políticas de seguridad que la empresa o nosotros hayamos establecido.

Estos niveles de seguridad se componen de tres opciones las cuales son:

- *Dedicado.* Usado normalmente cuando ISA Server se ha instalado en modo firewall y que no requiere de otras aplicaciones.
- *Servicios Limitados.* Esta configuración se usa cuando en la computadora donde se ubicó ISA Server, se instaló el modo integrado; es decir, las funciones integradas y combinadas de firewall y reservación de espacio (caché).
- *Seguro.* Se usa esta configuración, cuando en la computadora con ISA Server se proporciona un servicio en particular; como puede ser un servidor Web, un servidor de base de datos, un servidor de correo electrónico, etc.



Presionamos siguiente y hemos finalizado el proceso de *Configurar el Firewall mediante el Asistente.*

Esta es la manera rápida y fácil de establecer un firewall con esta tecnología, pero sin embargo; podemos establecer otras reglas para que el cortafuego sea más seguro y esta es, la de establecer *Propiedades para el Filtrado de Paquetes IP.*

FILTRO DE PAQUETES IP

Permitir el filtrado de paquetes es tener control entre la comunicación de una red externa hacia nuestra PC con ISA Server y de ahí a la LAN. Por lo tanto, debemos entender los encabezados de estos paquetes para poder crear filtros correctos que permitan una comunicación bidireccional.

La información de un encabezado de paquete IP, se compone de:

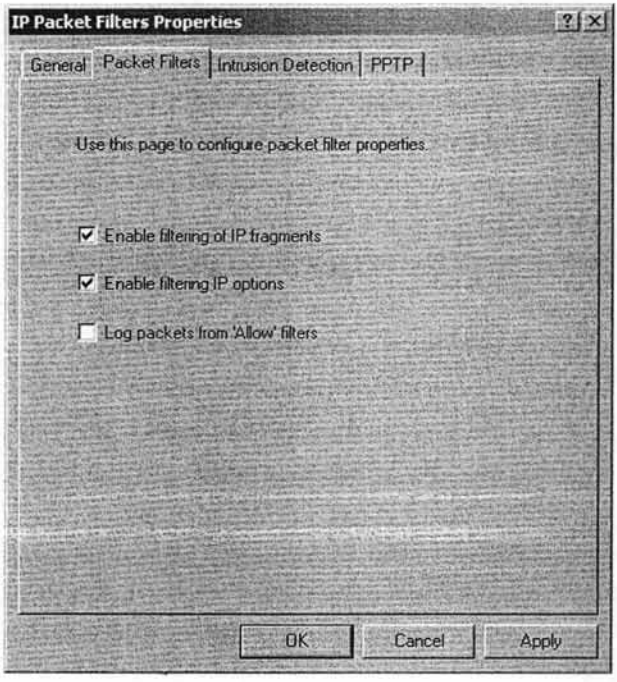
- Fuente de la dirección IP y su respectivo puerto
- Destino de la dirección IP y el respectivo puerto
- Información del protocolo IP

Como lo mencionamos arriba, se establece una comunicación o tráfico bidireccional; pero ISA Server también abre los puertos apropiados dinámicamente que permiten la devolución de la dirección IP y su puerto del paquete original. Es importante mencionar que; el filtrado de paquetes dinámico, permite que los paquetes devuelvan el puerto y la dirección IP del paquete original solamente durante el tiempo que dure la sesión.

Existen dos tipos de filtrado de paquetes que son *Permitir Filtro* y *Denegar Filtro.* El primero es usado para definir cuales paquetes de redes externas serán aceptados. El segundo se usa para crear excepciones a los paquetes permitidos; por ejemplo, podemos permitir la entrada del tráfico SMTP a un servidor de correo, para después entonces crear un filtro de bloqueo para denegar acceso al servidor de correo para una dirección IP que fue el origen de un intento previo de ataque externo.

Antes de crear filtros IP, debemos identificar bien los puertos y protocolos asociados para especificar paquetes correctos. También debemos identificar los rangos direcciones IP de las computadoras para la fuente y el destino.

Desde nuestra consola de ISA Server desplegamos la opción de *Políticas de Acceso*, para luego seleccionar *Filtro de Paquetes IP*. Presionamos en la opción *Configurar Filtrado de Paquetes y Detección de Intrusos*. En la pestaña *Filtro de Paquetes*, habilitamos las dos primeras opciones que nos aparecen; *Habilitar Filtros de Fragmentos IP* y *Filtros de Opciones de IP*.



CREACIÓN DE UNA REGLA DE FILTRADO DE PAQUETES IP

Para realizar una configuración exitosa debemos conocer los componentes que deberemos configurar y que a continuación se listan:

1. **Protocolo IP**. Proporciona opciones como los protocolos ICMP, TCP y UDP; y también las opciones Any (cualquiera) y Protocolos de Costumbre (Custom Protocol).
2. **Número de Protocolo**. Tipo de número del protocolo IP; para los protocolos ICMP, TCP, UDP y Any, esta casilla está desactivada. Para la opción Custom Protocol la casilla se activa para especificar el número del protocolo que deseamos configurar.
3. **Dirección**. Aquí se especifica la dirección para la comunicación del protocolo. Para la mayoría de los protocolos podemos especificar los siguientes modos como son *Inbound*, *Outbound* y *Both*. Pero para el Protocolo UDP sus opciones son diferentes y tenemos las siguientes direcciones:
   - *Send Only*. Solamente envía paquetes.
   - *Send/Receive*. Envía paquetes y puede recibir respuestas.
   - *Receive Only*. Solamente recibe paquetes.
   - *Receive/Send*. Recibe paquetes y puede enviar respuestas.
   - *Both*. Es la combinación de las cuatro anteriores, lo que establece una comunicación bidireccional.
4. **Puerto Local y Número de Puerto**. Se especifica el puerto donde se aplicará la regla. Existen opciones como son:
   - *All Ports*. La regla se aplica a todos los puertos sin excepción.
   - *Dynamic*. La regla se aplica para puertos que los usuarios típicamente usan para establecer conexiones con servidores; los puertos son desde 1025 hasta 5000.
   - *Fixed Port*. Seleccionamos un puerto en específico en donde debemos seleccionar el tipo de número del puerto. Para las opciones anteriores, este cuadro de diálogo no se habilita.

5. **Puerto Remoto y Número de Puerto.** Se especifica el puerto donde se aplicará la regla. Existen dos opciones que son:
   - *All Ports.* La regla se aplica para todos los puertos remotos.
   - *Fixed Port.* Se selecciona un puerto en específico donde debemos definir el tipo de número para el puerto.

Los siguientes dos puntos, sólo son aplicables para el protocolo ICMP.

6. **Tipo.** La regla se aplica al protocolo ICMP. Existen dos opciones que son los siguientes:
   - *All Types.* La regla se aplica a todos los tipos del protocolo ICMP.
   - *Fixed Type.* Se aplica la regla a un tipo de ICMP en específico, definiendo también el número del tipo.
7. **Código.** La regla se aplica al protocolo ICMP. Existen dos opciones que son los siguientes:
   - *All Codes.* Se aplica la regla a todos los códigos del protocolo ICMP.
   - *Fixed Code.* Se aplica la regla a un tipo de código de ICMP en específico, definiendo también el número del tipo del código.

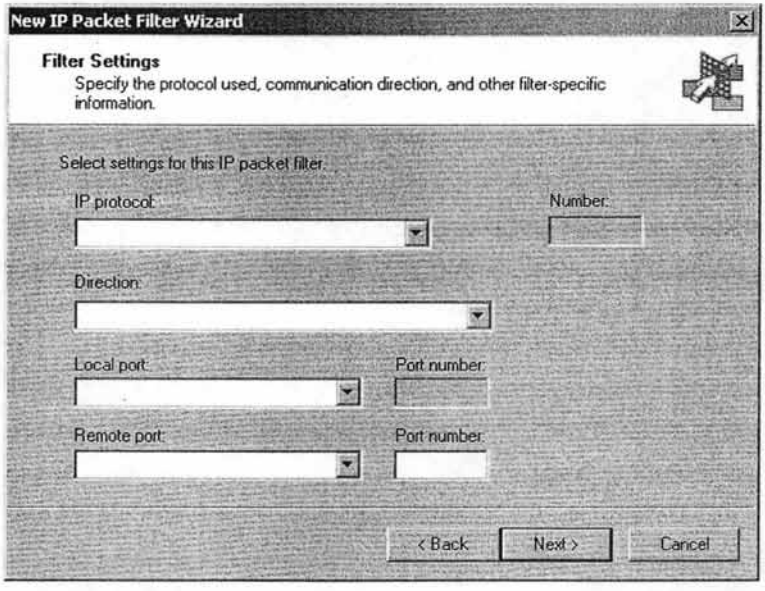
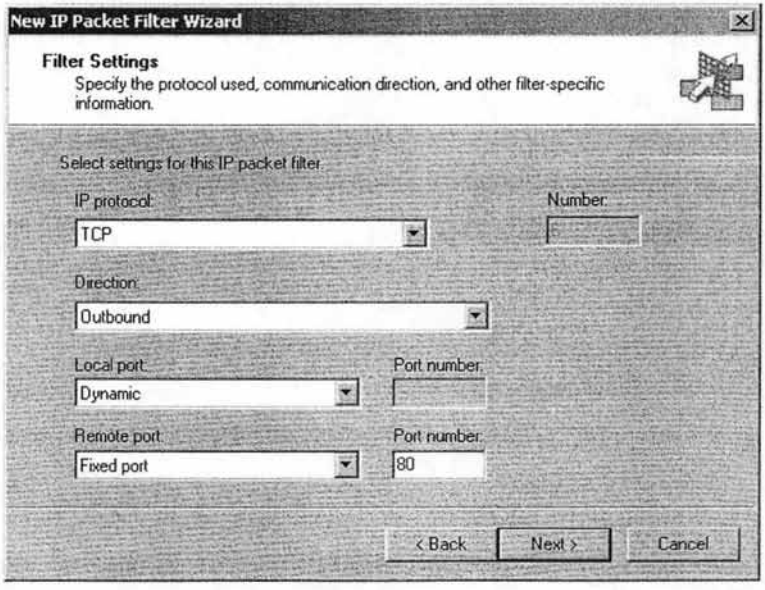


Figura 25 Asistente para la creación de nuevas reglas de filtrado de paquetes

Definidos los componentes para la configuración del filtrado de paquetes, procederemos a crear un filtro que permite la transmisión de bloques por el puerto 80, es decir; permitiremos la salida a Internet para que los usuarios de la red interna se conecten a nuestra computadora servidor (ISA Server), y tener un control acerca del tiempo que pasen navegando y saber que páginas son las que visitan; de esta manera se cumpliría la primera política de seguridad que sugiero puede establecerse en una empresa, industria o un gran corporativo.

Dado que ISA Server nos proporciona guías de ayuda para la configuración, no es necesario programar manualmente las reglas como tendría que ser el caso de UNIX o Linux. Desde la consola de ISA Server, seleccionamos la opción *Crear Filtros de Paquetes IP*.

Para que los usuarios de la LAN tengan acceso a Internet, seleccionamos *Permitir Transmisión de Paquetes*; de este modo, podrán acceder a cualquier página web que deseen. Sin embargo, debemos recordar que siguiendo los mismos pasos podemos bloquear sitios web donde los usuarios; lejos de trabajar, perderían tiempo en otras cosas.



En la ilustración anterior, ya hemos definido el tipo de protocolo IP que en este caso será **TCP**; la dirección de la comunicación es del tipo salida (**Outbound**); los puertos locales del tipo dinámico (**Dynamic**) y el puerto remoto es del tipo compuesto (**Fixed port**) con el número de puerto definido (**80**).

Este filtro de paquetes será aplicado para todas las computadoras dentro de nuestra red local. También tenemos opciones para seleccionar solo una computadora o determinadas computadoras.

Siguiendo este ejemplo podemos crear diferentes filtros para diferentes aplicaciones, según la política de seguridad que se haya establecido en la empresa y, del nivel de importancia de la información de los usuarios de la red de área local.

3.6.2 CONFIGURACIÓN DE ACCESO SEGURO A INTERNET

Ya hemos visto que la política de configuración del firewall puede ser aplicable para cualquier empresa. Para que veamos que nuestros filtros que creamos funcionan correctamente, debemos habilitar la conexión a Internet de una manera segura.

Internet Security and Acceleration Server 2000, ofrece políticas de acceso basadas en el control. El administrador de red puede configurar políticas de acceso específicas para permitir la accesibilidad de ciertos sitios web y ciertos contenidos en sitios web; también puede configurar disponibilidad de protocolos particulares para la salida a Internet.

Una política de acceso de ISA Server consiste de los siguientes elementos:

1. **Protocol Rules**. Define los protocolos que ISA Server utiliza para establecer comunicación entre una red interna e Internet.
2. **Site and Content Rules**. Define el tipo de contenido y los sitios los cuales el Proxy permite o niega el acceso.
3. **Policy Elements**. Define la configuración del uso de las reglas.

PLANEAR UNA ESTRATEGIA DE POLÍTICA DE ACCESO

Para planear una buena política de acceso podemos tener en cuenta los siguientes puntos, considerando que son aplicables en la empresa y no tendrán ninguna derivación negativa en las labores de los empleados.

1. **Determinar los requerimientos de la empresa basados en la propia necesidad del negocio**. Una política de acceso podría ser consistente con las necesidades de la organización, si esta es identificada como importante; es necesario realizar este paso y tener bien identificados los recursos de los que dispondría el negocio como la accesibilidad a Internet y el uso del correo electrónico, que podrían ser primordiales y de hecho son necesarios en esta era de la informática.
2. **Definir las reglas que son necesarias**. La política de acceso para la organización, pueden ser implementadas si definimos las reglas correctas. Un ejemplo sería, definir una regla que permita el acceso en horas de trabajo a la dirección web www.fiscalia.com.mx.
3. **Crear los elementos de la política**. Las reglas se construyen en bloques los cuales se usarán para que funcionen las políticas de acceso.
4. **Probar las reglas**. En este punto, nos aseguraremos que las reglas permitidas para el acceso a los usuarios proveen solamente lo necesario para la empresa.

El establecer acceso a Internet, puede contraer ciertos riesgos tanto externos (como virus o ataques de hackers) como internos (ocio por parte de los empleados). Es por esta razón, que hemos enfatizado en que el o los administradores deben de diseñar correctamente las reglas que permitan el acceso a la red mundial.

Para establecer este acceso, se deben de crear los protocolos correctos. Para establecer conexión con Internet, el protocolo que debe habilitarse es TCP con el puerto 80 con dirección de salida y también deben habilitarse en ISA Server los servicios que son *FTP*, *FTP Download Only*, *HTTP* y *HTTPS*.

En la siguiente figura se muestra como deben estar habilitados los protocolos para el acceso a Internet.

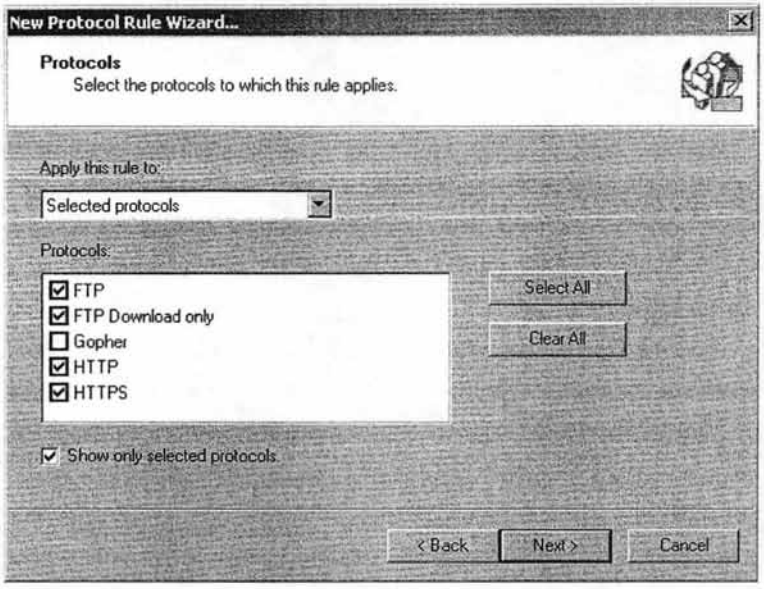


Figura 26 Protocolos de acceso a Internet

El administrador de la red local, puede crear o definir protocolos como el TCP o el UDP. Pero para controlar el tráfico de la red interna; se debe usar otro tipo de protocolo, como el Protocolo de Control de Mensajes por Internet (ICMP) el cual habría que crear filtros de paquetes como ya se expuso en la sección anterior.

La configuración del acceso a Internet como la creación de su protocolo por el puerto 80, dan como resultado que los usuarios de la red local obtengan servicio a la red mundial.

3.6.3 CREACIÓN DE GRUPOS DE CONTENIDO

Los *contenidos de grupo* definen el contenido de los sitios web. Es decir, permite crear las reglas que autoriza o niega el acceso a sitios web por medio del tipo del contenido en dicho sitio.

Cuando se crean estos *grupos*, podemos especificar el tipo de contenido por medio del MIME (Extensiones Multipropósito de Correo por Internet, Multipurpose Internet Mail Extensions) y de la extensión del archivo. Microsoft ISA Server utiliza estas definiciones de MIME cuando se aplican reglas de tráfico HTTP; y usa las extensiones de archivo cuando se aplican las reglas de tráfico para FTP.

Para crear un grupo de contenido seguiremos los siguientes pasos:

1. En ISA Management, desplegamos la consola raíz y presionamos con el botón derecho sobre ***Content Groups***, presionamos en ***New*** y luego en ***Content Group***.
2. En la caja de diálogo, en el apartado ***Name***, tecleamos el nombre con el cual se identificará al nuevo grupo de contenido.
3. En el apartado ***Description***, se tecleará el nombre con el cual conoceremos las características del grupo de contenido.
4. En ***Availabe Types***, se seleccionará cualquiera de las opciones *Seleccionar un tipo de contenido existente* o *Añadir nuevo tipo de contenido.*
5. Clic en ***Add***, y repetir los pasos del uno al cuatro tantos tipos se quieran crear.

Es importante recordar que Microsoft ISA Server, usará solamente los grupos de contenido cuando se apliquen las reglas para el tráfico de HTTP (en las peticiones de todas las computadoras terminales que deseen usar el Internet). En el caso del FTP, estas reglas se aplicarán cuando existan peticiones de clientes Web Proxy.

3.6.4 CREACIÓN DE REGLAS PARA EL ANCHO DE BANDA

Antes de empezar la creación de las reglas, es necesario determinar la efectividad del ancho de banda. Por ejemplo, si la red interna opera a 100 megabits por segundos (Mbps), la efectividad del ancho de banda será de 100Mbps; si opera a través de una conexión telefónica (dial-up connection) a 56 kilobits por segundo (Kbps), la efectividad del ancho de banda será de 56Kbps.

Grupo Massat utiliza un servicio DSL (Digital Subscriber Line) a través de un ruteador, cuyo ancho de banda de operación es de 512Mbps. Para determinar la operación efectiva del ancho de banda en ISA Server, se realizará lo siguiente:

1. En ISA Management, desplegamos la raíz y con el botón derecho seleccionamos ***Bandwidth Rules***.
2. Seguido, seleccionaremos ***Properties***.
3. En la caja de diálogo que aparece, seleccionamos ***Enable Bandwidth Control*** de manera que quede habilitado.
4. En el apartado ***Effective bandwidth (Kbit/Sec)***, escribimos 5120 y aceptamos los cambios.

Cuando se haya determinado la funcionalidad del servicio de acceso a Internet, se puede proceder a determinar las reglas que controlarán el ancho de banda y por medio de las cuales podemos decidir que porcentaje se usa en determinados procesos y en que horarios. A través de los siguientes pasos podremos crear reglas para el control del ancho de banda.

1. En ISA Management, desplegamos la raíz y con el botón derecho seleccionamos ***Bandwidth Rules***. Seleccionamos ***New*** y enseguida ***Rule***.
2. En el asistente, en el apartado ***Bandwidth Rule Name***, escribimos el nombre de la nueva regla y presionamos en ***Next***.

3. En la página de protocolos, se seleccionará una de las opciones que aparecen (***All IP Traffic; Selected Protocols; All IP Traffic Except Selected***). Suponiendo un ejemplo, pensaremos que se necesita darle prioridad al programa Windows Media; en este caso se seleccionaría la opción ***Selected Protocols***.
4. Para la página ***Schedule***, se seleccionará un horario de aplicación.
5. En ***Client Type***, se seleccionará una de las opciones que aparecen (***Any Request; Specific Computers; Specifics Users and Groups***) que mejor se acomode a la configuración de la regla que se está creando.
6. Para ***Destination Sets***, se seleccionará cualquiera de las opciones: ***All destinations; All internal destinations; All external destinations; Specified destinations; All destinations except selected set***.
7. Para la página ***Content Groups***, se seleccionarán uno o más grupos.
8. En el cuadro ***Bandwidth Priority***, se selecciona cualquiera de las dos opciones siguientes: ***Use default scheduling priority***; ***Custom***. La primer opción aplica cuando se le desea dar prioridad al horario establecido en el sistema operativo Windows 2000; la segunda opción aplica cuando ya hay una configuración previa de las prioridades del ancho de banda.
9. Para acabar, presionamos en el botón ***Finish***.

3.7 CASO PRÁTICO: CONTROL DE ACCESO A MSN MESSENGER

En este caso práctico, mostraremos la manera de instalar el Microsoft Client Firewall de ISA Server y una de muchas posibilidades de crear una política de restricción de uso del MSN Messenger para evitar el ocio entre los empleados de la firma Grupo Massat.

Microsoft Internet Security and Acceleration Server 2000 al momento de su instalación genera una carpeta en donde se encuentra localizado el cliente del firewall que será utilizado para instalarlo en otras computadoras; de esta manera existirá una computadora local con el programa ISA Server instalado y terminales con el cliente instalado.

ISA Server en su herramienta firewall, no funciona inmediatamente como lo hace con las solicitudes de Internet; para que el firewall funcione correctamente en una red local necesita de ser instalado en cada computadora terminal.

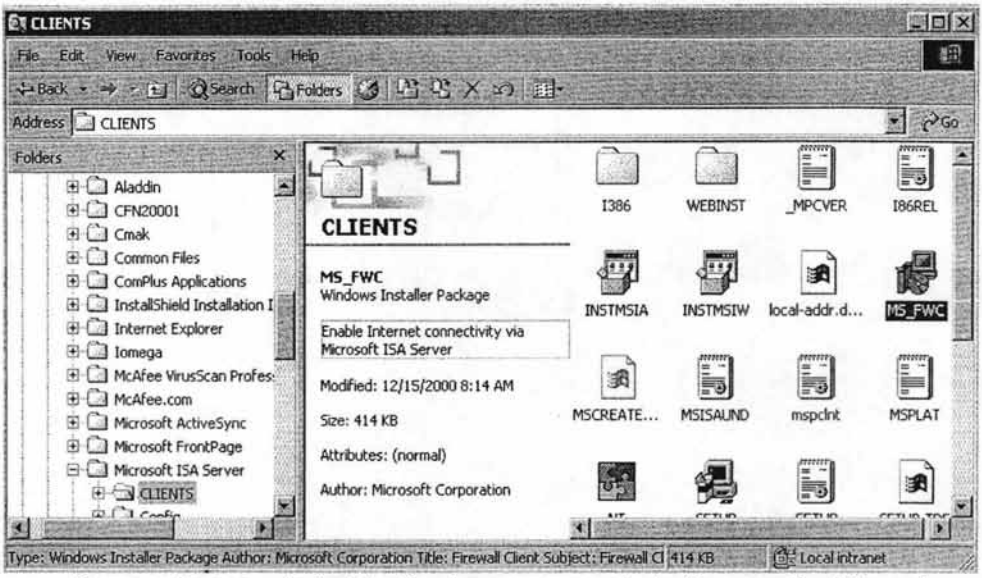
El método de instalación es relativamente sencillo, solo necesitamos que la computadora terminal donde se instalará el firewall tenga acceso a la red y que pertenezca al dominio (es decir que esté dentro de la red local); el administrador de la red deberá compartir la unidad donde se instaló ISA Server en el servidor para accesarla y poder instalar el cliente.

La dirección de acceso sería la siguiente:

\\ *unidad del servidor* \ *Program Files* \ *Microsoft ISA Server* \ *Clients*

Una vez que se tiene acceso hasta este punto, encontraremos el ejecutable del cliente firewall que nos ayudará a ejecutar las reglas que se hayan establecido y controlar de una manera más eficientemente todas aquellas peticiones y procesos que los usuarios necesiten; así como controlar el acceso a sitios de Internet poco apropiados a los intereses de la empresa, que en este caso sería Grupo Massat, S. de R.L. de C.V.

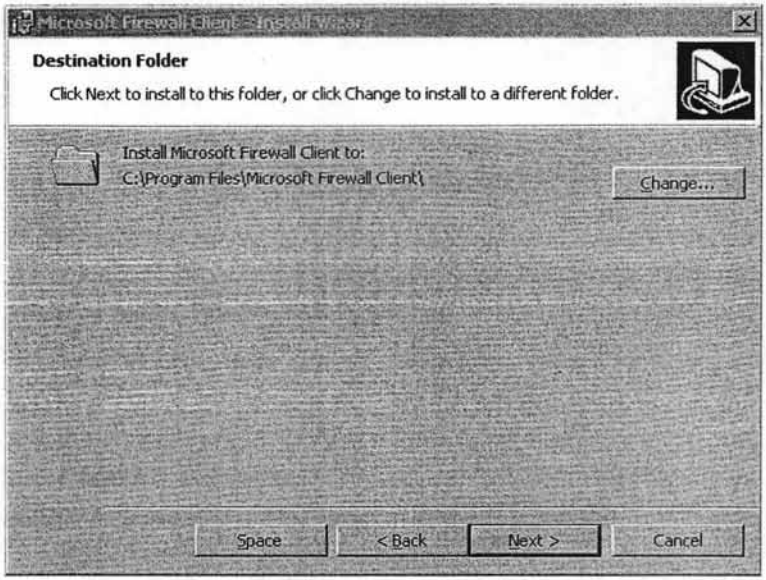
En la figura siguiente se muestra la carpeta CLIENTS el cual contiene el archivo ejecutable del cliente firewall.



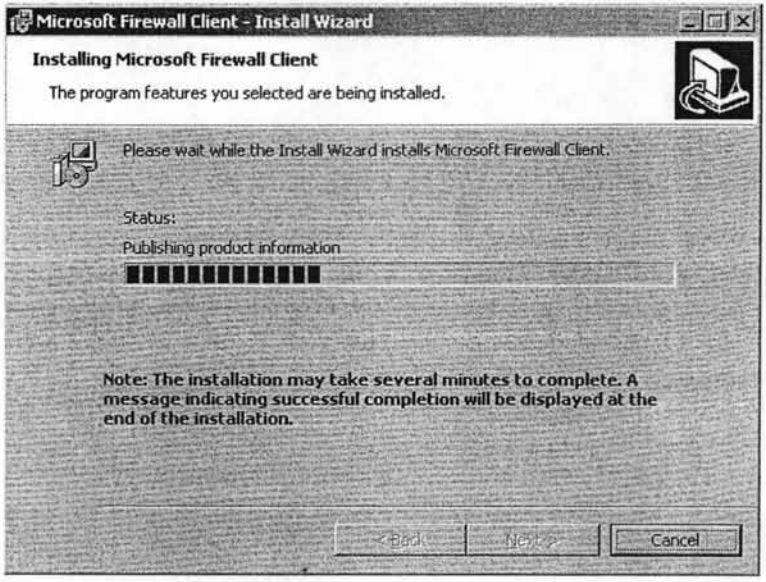
Como sabemos, la instalación de programas de la Corporación Microsoft es sencilla y se inicia presionando la tecla Intro o dando doble clic sobre el icono representativo del programa.

Recordando nuevamente, al iniciar la instalación del Cliente del Firewall; éste se instalará localmente en la computadora terminal, más específicamente en el disco duro local (C:\). El Cliente buscará automáticamente la carpeta **Program Files** (si el Sistema Operativo es en inglés) o la carpeta **Archivo de Programas** (si el Sistema Operativo es en español).

La figura siguiente representa el momento en que el Cliente Firewall busca una ubicación y nos la muestra; aún así, tenemos la opción de cambiar esa ubicación si acaso no queremos que se instale en la carpeta *Program Files*.

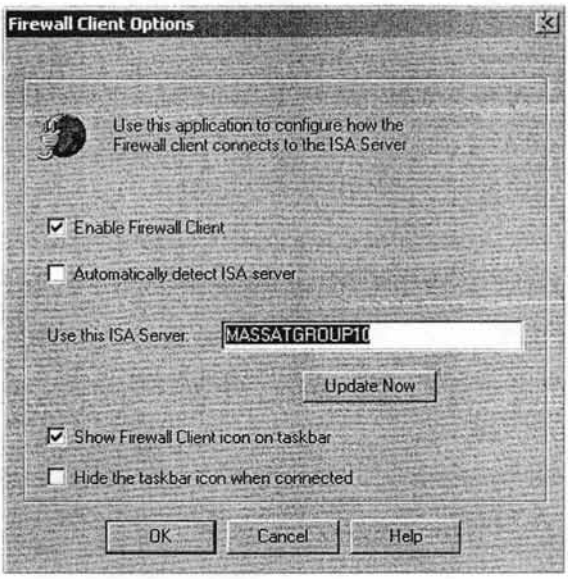


El proceso de instalación sólo toma unos minutos. Este cliente es compatible con computadoras que tengan instalados sistemas operativos desde Microsoft Windows 98 en adelante. Para aquellas computadoras que tengan Microsoft Windows XP, será necesario apagar y encender la computadora de nuevo. Sin embargo se sugiere que toda PC donde se instale el Microsoft Client Firewall, se reinicie.



Cuando la instalación del Cliente del Firewall haya finalizado, veremos un icono en la parte inferior derecha de la pantalla (junto al reloj del sistema) que indica que el cliente ha sido instalado satisfactoriamente y está en funcionamiento.

El Cliente del Firewall detecta automáticamente la configuración vía red del servidor y de las reglas creadas en Microsoft ISA Server. El Firewall funcionará correctamente si el administrador de la red, ha creado reglas correctas que permitan al usuario trabajar de manera adecuada y dentro del horario establecido, sin contratiempos de algún tipo.



Supongamos el siguiente ejemplo, se sabe que una de las formas de pérdidas de tiempo laboral para varias empresas es el ocio de sus empleados en horas de trabajo a través de los chats y en particular con el popular MSN Messenger de hotmail. Sería falso decir que por medio de este firewall podemos negar o prohibir el servicio de messenger.

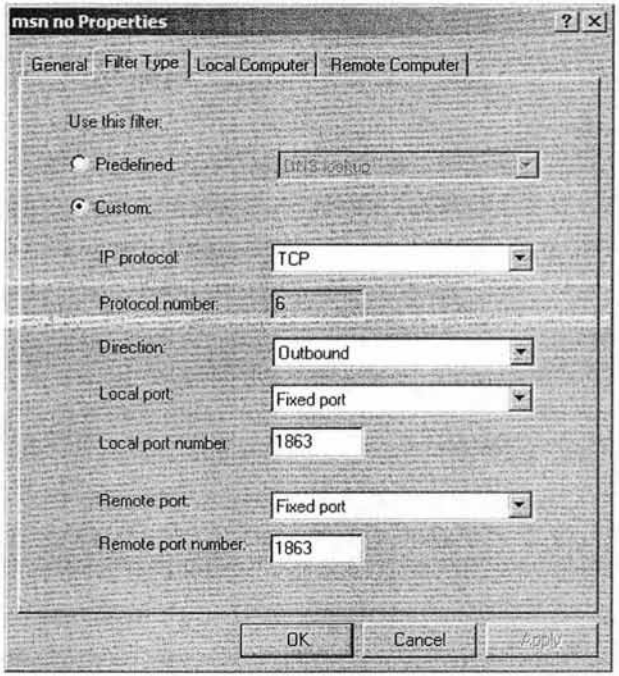
MSN Messenger funciona de la siguiente manera:

1. Cuando se conecta, utiliza por default el puerto 80 y así poder confirmar nombres de usuarios y contraseñas en la base de datos del sitio web Hotmail.
2. Si llegara a existir problemas con el puerto 80, buscará un puerto disponible al azar para conectarse a Internet y confirmar las credenciales de los usuarios.

Cuando se ha conectado, los usuarios pueden hacer uso de las diversas herramientas que proporciona tales como uso de *webcam*, *audio*, *envío y recepción de archivos*, *invitación a otros usuarios para hablar*, etc.

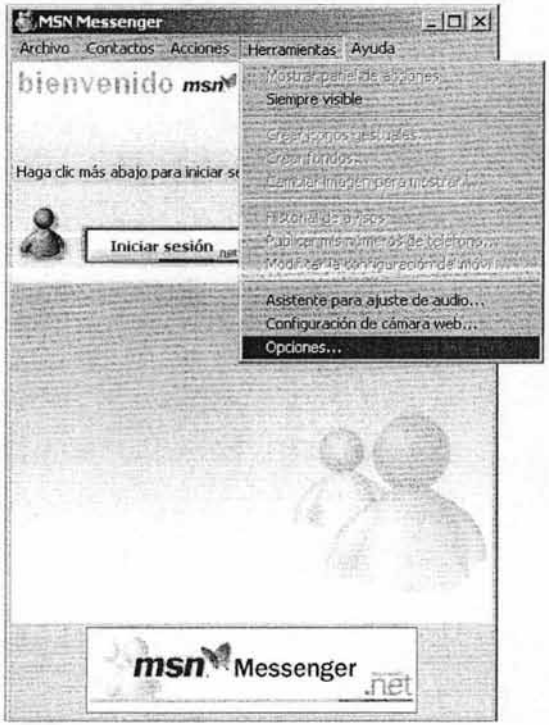
Por cada servicio que la persona use, se abrirán diferentes puertos y de ésta manera la computadora estará expuesta a peligros tales como infección de virus o entrada a la PC de manera ilegal por otra persona (hacker). Es por ésta razón que es falso decir que se puede prohibir; lo que sí se puede lograr es controlar el servicio.

Una manera de controlarlo sería creando un bloqueo de servicio del messenger por medio del puerto 1863; tomamos esta configuración en particular puesto que en ISA Server 2000 existe una política similar. Sin embargo esta configuración que crearemos no funcionará a menos que modifiquemos el programa messenger; en las siguientes figuras se explica lo que se trata de hacer.



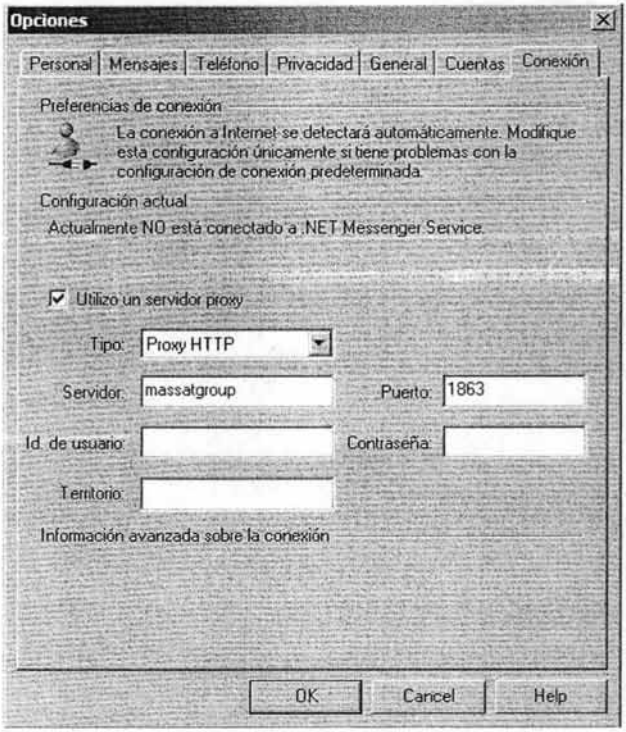
Al momento de crear el filtro que nos permitirá hasta cierto punto controlar el MSN Messenger, deberemos especificar que se trata de un protocolo tipo TCP con dirección de salida (está en la red local y buscará la base de datos en Internet para conectarse).

Los puertos local y remoto, deberán estar especificados en *puerto combinado* y el número de puerto lo especificaremos en el *1863*. En la creación del filtro para controlar messenger, existen dos pestañas más que se refiere a computadora local y remota; aquí deberemos señalar que esta regla se aplicará a todas las computadoras de la red local (que en la actualidad son un total de 20). Para Grupo Massat, S. de R.L. de C.V. por ser una pequeña empresa es posible aplicar un control por computadora realizando la siguiente configuración en el messenger. En el Menú *Herramientas* seleccionamos el submenú *Opciones*.

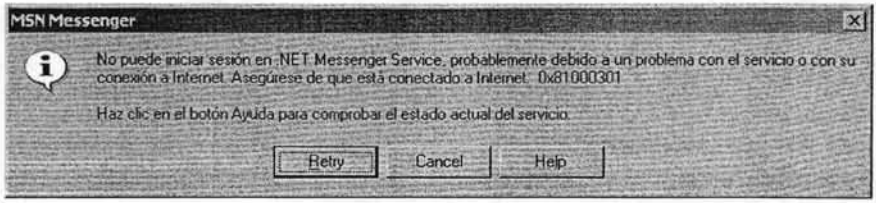


Al tener el cuadro de diálogo en pantalla de las Opciones, buscaremos la sección que nos permita configurar la conexión de MSN Messenger; en sus preferencias habilitaremos la sección que permite utilizar un servidor proxy. En la sección *Tipo* escogemos la opción *Proxy http* y en el puerto escribiremos el *1863*. No es necesario establecer algún nombre de servidor.

Realizar este tipo de configuración en cada computadora nos permitirá la sensación de control del messenger; sin embargo el usuario podría instalar nuevamente el programa y este lograría conectarse aún cuando el firewall está instalado. Para evitar que esto suceda, se puede establecer una configuración en el sistema operativo de tal manera que el usuario no tenga permiso alguno de hacer instalación de programas sin la previa consulta del administrador de la red local.



Una vez realizada esta breve operación, hacemos el intento de conectarnos y tendremos como resultado el siguiente cuadro de error.



Debido a que podemos manipular las restricciones desde el Microsoft ISA Server, no estaría mal el crear una política que penalice el uso de este tipo de programas. En realidad, podíamos haber escogido cualquier número de puerto a excepción del 80 u 8080; ya que estos puertos son los requeridos por Microsoft ISA Server para el acceso a Internet.

Con las configuraciones sugeridas anteriormente, no puede haber manera de que los empleados usen el MSN Messenger en las horas de trabajo; a excepción de que hagan una nueva instalación de dicho programa de mensajería popular.

Microsoft Internet Security and Acceleration Server 2000, es una herramienta capaz de proveer soluciones satisfactorias para las pequeñas y medianas empresas (en general para cualquier empresa) por su fácil manejo y configuración. De igual manera, es una herramienta relativamente económica y de la cual existen actualizaciones a través de Internet.

Para ejemplificar de manera general el funcionamiento de ISA Server, hablando más propiamente sobre el caso práctico anterior, veremos un esquema general de sencilla apreciación.

OPERACIÓN GENERAL DE MICROSOFT INTERNET SECURITY AND ACCELARATION SERVER 2000

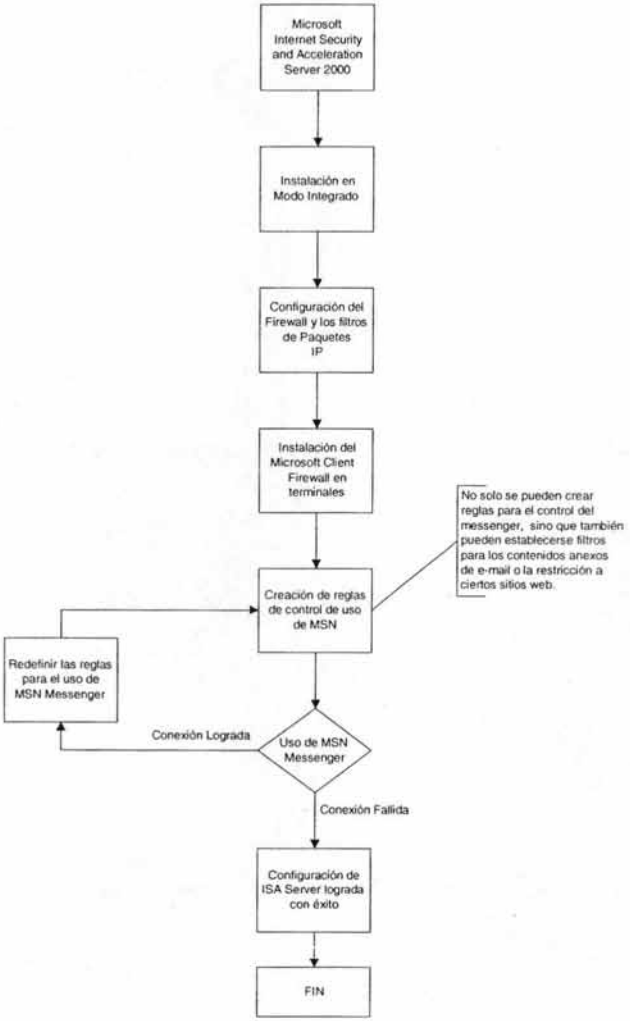


Figura 27 Operación de ISA Server después de su configuración

Pero no solamente es una herramienta que sirve como firewall o de espacios reservados para el acceso rápido a sitios web, otra de sus ventajas es la realización de reportes que proporcionan información acerca de la actividad de los usuarios en la red local. Reportes de los cuales se hablarán en el capítulo 4.

La operación de ISA Server no sólo se limita a controlar el MSN Messenger, también puede realizar funciones como las que se listan a continuación (ya mencionadas anteriormente):

a) Filtros de contenido de correos electrónicos.
b) Restricción de acceso a sitios web.
c) Descargas de programas (sin previa autorización del administrador de red).
d) Restricción completa hacia Internet, por días específicos u horas específicas según las políticas de seguridad.
e) Intento de instalación de programas sin autorización del administrador de red.
f) Conexión de una red local o otra, creando una VPN con ISA Server.
g) Configuración de Servidores Web Públicos.
h) Configuración de Servidores de Correos Públicos
i) Envío de Mensajes en Pantalla
j) Configuración del protocolo H.323 (para servicios de comunicaciones multimedia)

Todas las operaciones mencionadas, pueden ser aplicables a las PyMES dependiendo del uso que se le otorgue y de la necesidad de implementarlo. Los recursos o módulos de los cuales dependerá para su constante actualización deberán ser proporcionados por el mismo creador del producto; esto debido a la firma digital que se ha implementado en los productos. Si dicha firma no llega a ser similar con ISA Server, este no se instalará correctamente provocando un mal funcionamiento del programa instalado e incluso de ISA Server 2000.

CAPÍTULO 4

MONITOREO Y REPORTE DE ACTIVIDADES

El determinar las futuras reglas de configuración del ISA Server, tiene mucho que ver con los reportes que los administradores de redes generen.

Estos reportes servirán de apoyo para determinar los puntos débiles de una red local, así como determinar que herramientas de apoyo pueden usarse para fortalecer dichos puntos. Pero ¿Cada cuándo se deben generar los reportes? ¿Qué información deben contener? La respuesta es sencilla, los reportes serán generados conforme los usuarios tengan acceso a Internet, ya que de ahí se decidirá en cierta forma, el futuro de la empresa en cuanto a actividades reales laborales o actividades de ocio dentro de las horas de trabajo.

Un procedimiento sencillo para generar un reporte sería considerar la periodicidad que puede ser de una semana, evaluando las problemáticas que el reporte presente en entorno a los usuarios. Tales problemáticas pueden ser el uso excesivo de Internet cuando se precisaría de dos o tres horas para realizar las investigaciones que requieran.

4.1 ESTRATEGIAS DE MONITOREO

Entenderemos por estrategia de monitoreo el de detectar ataques a la red local en donde se ha instalado el software ISA Server. Sin una estrategia de monitoreo y reportes, el administrador de la red no se daría cuenta acerca de los eventos importantes que están ocurriendo en la red local.

Si no cuentan con un buen monitoreo de actividades, no podrán confrontar los intentos de intrusión o configurar de manera adecuada los reportes y eventos que ofrece ISA Server.

PLANEAR UNA ESTRATEGIA DE MONITOREO

Para poder planear una estrategia de monitoreo (y en dado caso, también de reportes), podemos considerar las siguientes líneas:

- Categorizar la información que se necesita recolectar.
- Determinar la información que es crítica.
- Documentar la estrategia.
- Crear estrategias para saber como responder a eventos críticos.
- Diseñar un plan para archivar la bitácora.

4.2.1 DETECCIÓN DE INTRUSOS

Internet Security and Acceleration Server 2000 tiene integrado un sistema que permite la detección de intrusos. ISA Server puede implementar la detección de intrusos para el nivel de paquetes (protocolo IP de Internet) y el nivel de aplicación; de tal manera que, podemos disparar una alerta cuando el sistema detecta una intrusión o ataque específico al sistema.

Es posible determinar acciones que el sistema puede llevar a cabo cuando detecta un ataque o intrusión. Estas acciones pueden ser la de enviar un mensaje por correo electrónico o una página de reporte al administrador, documentarlo en la bitácora de eventos o ejecutar un programa o script.

ISA Server también ofrece la posibilidad de configurar alertas de notificación, esto es; cuando el sistema deja de dar servicio de manera inesperada.

ATAQUES A NIVEL PAQUETES (IP)

La detección de intrusos, es una herramienta que ISA Server posee. Como parte de su funcionamiento, puede detectar ataques a nivel paquetes IP, como los siguientes:

- **Buscar ataques en todos los puertos**. Esto ocurre cuando un intruso intenta obtener acceso a más números de puertos que los preconfigurados por el sistema. El administrador de la red, especifica los números de puertos que estarán disponibles para el acceso al exterior. Los intrusos realizan una búsqueda de puertos abiertos en la computadora para acceder a ella; lo que representa como un punto de entrada para atacar y consecuentemente realizar más ataques mediante uno o varios de estos puertos abiertos.
- **Buscar ataques a IP**. El intruso realiza repetidamente un intento de conexión a la computadora destino; los paquetes TCP con los que se comunica contienen determinadas banderas que permiten su conexión. Esta acción indica que el atacante prueba puerto abiertos mientras que evade el registro de la bitácora del sistema.
- **Ataque por partes**. Ocurre cuando el intruso establece conexión *engañosa (spoofed)* por medio del protocolo TCP mediante una dirección fuente IP y su respectivo número de puerto para que coincida con la dirección destino IP y su número de puerto. El engaño (spoofing) se refiere a un truco de computadora que provee información para acceder de manera no autorizada usando direcciones IP falsas.
- **Ataque Ping de la Muerte**. Cuando un intruso añade una cuenta de datos al protocolo ICMP (Internet Control Message Protocol) como paquete de respuestas. Este ataque puede causar que las computadoras que ejecutan ciertas implementaciones basados en TCP dejen de responder de manera inesperada, el cual les niega el servicio a usuarios legítimos.
- **Ataque Bomba UDP**. Este ataque ocurre cuando el intruso envía un paquete ilegal UDP (User Datagram Protocol). Este paquete es construido con valores ilegales en determinados campos lo que causa que las computadoras que usan un sistema operativo antiguo, se pasmen cuando este paquete es recibido.

ATAQUES A NIVEL APLICACIÓN

ISA Server también tiene la capacidad de realizar rastreos de ataques a nivel aplicación, como los siguientes:

- **Transferencia de Zona para puertos privilegiados (1-1024).** La información de zona de DNS usualmente no se transfiere a computadoras externas porque, esta puede contener información muy importante acerca de nuestra red. Por lo tanto, el ataque ocurre cuando la computadora usa una aplicación cliente de DNS para transferir zonas a un servidor interno DNS. Los puertos que se encuentran entre 1 y 1024 son considerados puertos privilegiados, porque se reservan para aplicaciones de servidor. Lo que comúnmente se usa para transferir zonas de respuestas entre aplicaciones de servidor.
- **Transferencia de Zona para puertos altos (después de 1024).** Tiene una función similar al anterior, la diferencia radica que después del puerto 1024; los puertos se usan para aplicaciones clientes. Sin embargo, no tenemos la garantía de que la transferencia de información provenga de una aplicación cliente.
- **Desbordamiento del Estado del POP.** El ataque tiene lugar cuando el intruso intenta ganar privilegios de acceso a las computadoras por medio de la ejecución de versiones del POP (Post Office Postal) para generar un desbordamiento del buffer (estado) de este servicio.

Cuando configuremos la detección de intrusos, notaremos que ISA Server 2000 puede identificar cuando ocurre un ataque en nuestra red y entonces determinar que acción realizar de las que están preconfiguradas. En la siguiente figura vemos como habilitar la detección de ataques para nivel paquetes IP.

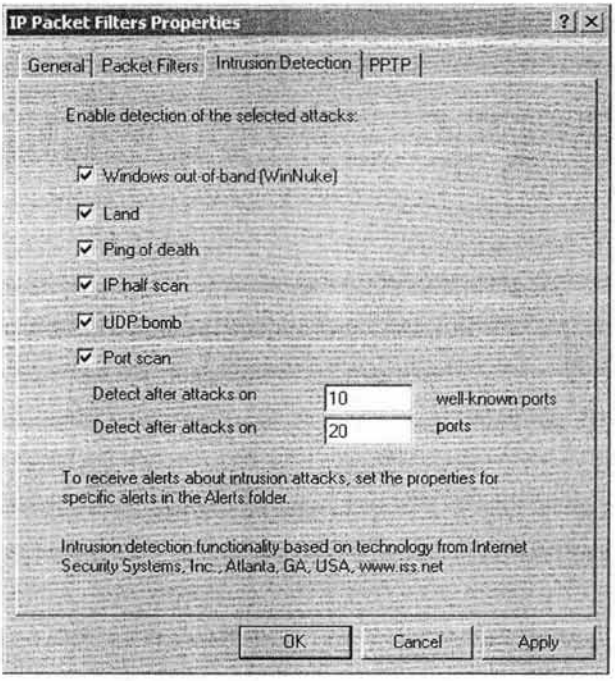


Figura 28 Propiedades de los filtros de paquetes

En esta otra figura, veremos que las opciones se encuentran habilitadas para la detección de ataques a nivel aplicación.

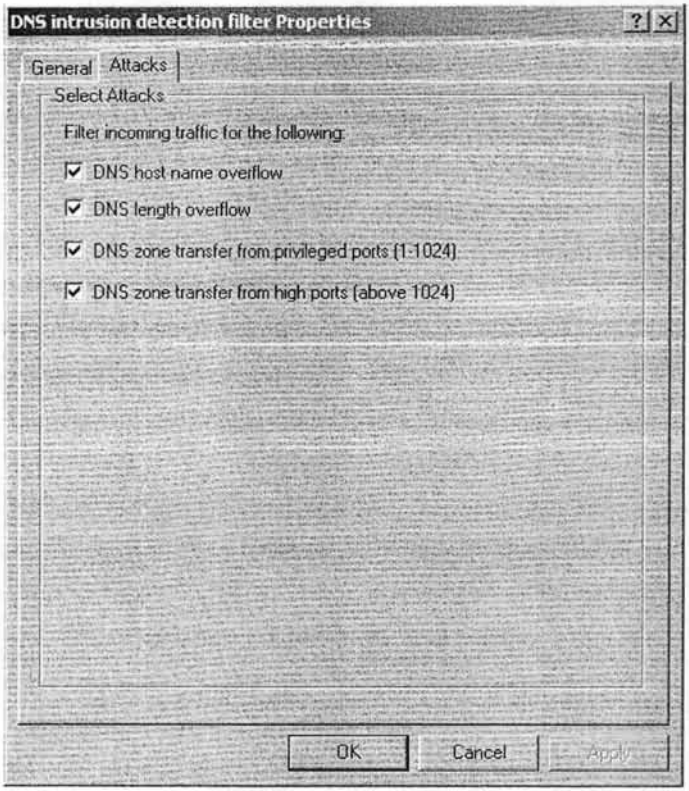


Figura 29 Detección de intrusos en ISA Server

EVENTOS EN ISA SERVER

Los *eventos* en ISA Server; no son mas que condiciones que utiliza el programa para poder detectar durante su operación, anomalías tales como intentos de intrusión, problemas con los servicios establecidos o fallas en la comunicación.

Usando estos eventos podemos realizar configuraciones de alertas. La *alerta* es definida como la acción que ISA Server realiza cuando ha detectado un evento. A continuación se listan algunos eventos con su definición que puede detectar ISA Server.

Evento	Descripción
Intrusión en el DNS	Indica que ha ocurrido un desbordamiento en el nombre del anfitrión (host), un ataque a la zona de puertos altos o un ataque a la zona de transferencia.
Detección de Intrusión	Un usuario externo intenta un ataque por medio de la visita no autorizada.
Tirar los paquetes IP	Indica que los paquetes IP que no están permitidos en la política de acceso, se desechan (caen o tiran).
Violación al Protocolo IP	Indica que ISA Server ha detectado y desechado un paquete con opciones IP inválidas.
Engaña al IP (IP spoofing)	ISA Server lo detecta cuando la dirección fuente del paquete IP no es válida.
Intrusión en el POP	Detecta el ataque hacia el POP cuando se produce un desbordamiento del buffer.
Solicitud de SOCKS rechazada	ISA Server rechazó una petición del SOCKS debido a una violación en la política de acceso.

Tabla 8 Eventos detectables en ISA Server

ALERTAS EN ISA SERVER

Internet Security and Acceleration Server 2000, supervisa acontecimientos (eventos) a través del servicio de alerta que viene integrado al software. Este servicio de alerta puede dar inicio a la realización de una acción en específico dependiendo del ataque detectado.

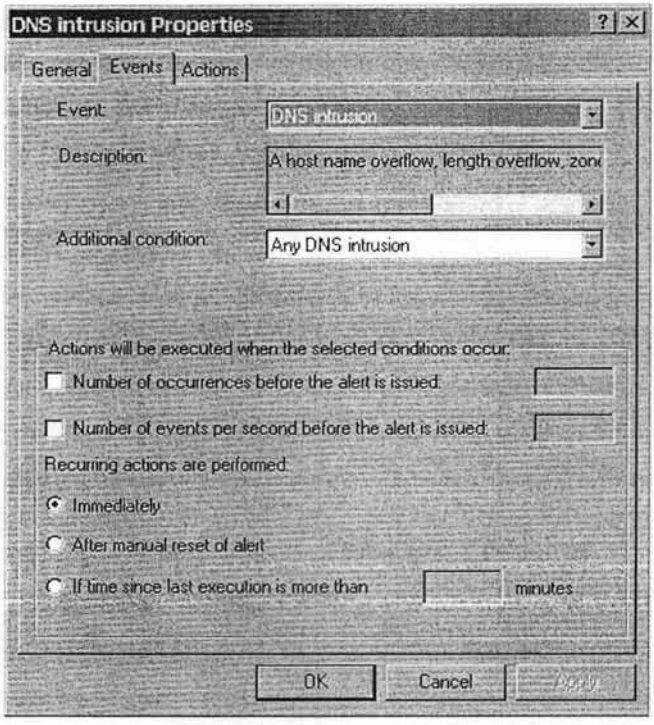
Por medio de ISA Server, podemos configurar alarmas para enviar notificaciones vía correo electrónico, ejecutar una aplicación en especial o detener los servicios e iniciar otros. Si es necesario, y si la política de seguridad así lo permite; el envío de correo electrónico puede suceder cuando un determinado número de veces de intentos intrusión ocurre.

Al momento de configurar una alerta, ISA Server nos ofrece opciones como las que se listan a continuación.

Opción seleccionada	Definición
Envía mensaje por correo electrónico	Se debe proporcionar el nombre o la dirección IP del servidor SMTP, un destinatario, una dirección de regreso y cualquier destinatario que se pueda incluir en la lista de ***Cc:***.
Empezar un programa	Se provee la ubicación o trayectoria del programa que se desea ejecutar en el servidor ISA.
Detener el servicio seleccionado de ISA Serverr	Se selecciona el servicio o servicios a detener. Las opciones válidas son el Servicio de Firewall, el Servicio Web Proxy y el Servicio de Programación de Horarios para Descargas de Contenido Cache.
Iniciar el servicio seleccionado de ISA Server	Se selecciona el servicio o servicios a iniciar.

Tabla 9 Opciones para configurar Alertas en ISA Server

Una vez configurado las alertas en ISA Server, podemos acceder a sus propiedades de tal manera que podemos decidir como funciona la alerta. En la siguiente imagen se muestra dichas propiedades y a continuación se explicarán cada una en una tabla.



Propiedad	Realiza la acción
Número de ocurrencias antes de publicar la alarma	Aquí permitimos un cierto número de anomalías antes de que se ejecute la alerta.
Número de eventos por segundo antes de que la alerta se publique	Se puede permitir un cierto número de anomalías por segundo que se registran en la bitácora de eventos.

Acciones que se realizan cuando se repiten eventos

Propiedad	Realiza la acción
Inmediatamente	Seleccionar esta opción puede dar lugar a que se ejecuten una gran cantidad de acciones debido a las constantes alertas de acontecimientos específicos.
Después de ajustar manualmente la alarma	Seleccionar esta opción da como resultado una sola acción de alerta incluso cuando existen múltiples acontecimientos.
Último periodo de ejecución desde ... minutos	Esta opción da lugar a múltiples acciones de un acontecimiento solamente cuando ocurre el evento un número especificado de minutos.

4.2.2 ACTIVIDAD DE ISA SERVER

El servidor ISA Server, registra las peticiones tanto de entrada como de salida; de tal manera que ISA Server actúa conforme responde a estas peticiones. Cuando se configura el registro de eventos de ISA Server, este genera los registros del servidor en el array.

De igual manera, genera los registros para los accesos a la LAN y los registros de actividad de la seguridad que proporciona ISA Server.

La ventaja que ofrece ISA Server, es que podemos generar los registros en varios formatos; para después poder analizarlos, aprovechar su funcionamiento y revisar los parámetros de seguridad del software.

FORMATOS DE LOS REGISTROS

Cuando configuramos los registros de actividad de ISA Server, este crea archivos de registro por cada computadora que se encuentre conectada hacia ISA Server; además podemos elegir el o los tipos de registro que deseemos.

Los archivos de registro que ISA Server genera son los siguientes:

1. Archivo de Registro del Filtrado de Paquetes
2. Archivo de Registro del Servicio del Firewall
3. Archivo de Registro del Servicio Proxy del Web

Por defecto, ISA Server guarda todos los archivos de registro en el fólder ISALogs debajo del fólder de instalación de ISA Server. Podemos guardar los archivos de registro en los siguientes formatos:

- **Formato W3C**. Este formato se usa para que las aplicaciones de reporte tengan compatibilidad y puedan ser reconocidos por el World Wide Web. En el formato W3C contiene los datos y la información que describe detalles como la versión, fecha y campos registrados. Los campos no seleccionados no son registrados en ISA Server.
- **Formato ISA.** Utilizamos este formato cuando se usa un medio de divulgación que pueda interpretar registros del servidor ISA. Este formato solo contiene datos y no la información sobre el formato de datos; además, ISA Server registra los campos no seleccionados y los identifica como campos vacíos.
- **Formato ODBC.** Se usa este formato para guardar los registros en una base de datos tipo ODBC (Conectividad Abierta para Bases de Datos, Open DataBase Connectivity).

ARCHIVOS DE REGISTRO DE LA ACTIVIDAD DEL FILTRADO DE PAQUETES

ISA Server puede registrar todos los paquetes que pasan a través de él hacia el archivo de registro del filtro de paquetes. Por defecto, el servidor ISA registra únicamente los paquetes que se encuentren dañados. Sin embargo, esta configuración puede ser modificable para reducir la carga del servidor en cuanto al registro de los paquetes dañados.

Estos registros, también puede contener información acerca de paquetes permitidos por la política del filtrado de paquetes IP. ISA Server puede registrar los paquetes permitidos o bloqueados siempre y cuando la política del filtro lo permita.

4.2 ESTRATEGIAS DE REPORTES

Los reportes del tipo informático juegan un papel importante para cualquier empresa, ya que estos permiten advertir las posibles fallas de seguridad y la manera en que podemos prevenirlas.

El uso de la herramienta reportes de ISA Server; contribuye a que los administradores de la red cuenten con un informe acerca de la actividad de la red local.

ISA Server, puede generar diferentes tipos de informes. Reportes que se muestran como páginas web de modo que, pueden ser vistas en cualquier navegador. Podemos guardar estos reportes de formato web, para después añadirle formato especial. ISA Server puede generar los siguientes tipos de reportes:

- **Reporte Breve**. Los reportes breves incluyen un sistema de estadísticas acerca del uso de ISA Server. Combina datos del servicio de bitácora del web proxy y servicio de registro del firewall.

- **Reporte de uso del Web.** Este tipo de reporte incluye un sistema que despliega a los usuarios de la web, respuestas comunes y los navegadores que usan. Este informe muestra como una organización hace uso del Internet y se basa en el archivo de registro del servicio web proxy.

- **Reporte del uso de aplicaciones.** El uso de reportes de aplicaciones exhiben la manera en que se usa Internet, el tráfico de entrada y salida y las aplicaciones cliente. Este tipo de reporte puede ayudarnos a planear la capacidad de la red y determinar políticas acerca del ancho de banda. El reporte se basa en los registros de servicio del firewall.

- **Reporte del uso de tráfico de la red.** La utilización de este tipo de reporte despliega el uso total de Internet ya sea por aplicación, protocolo y dirección; así como el uso de conexiones simultáneas y algunas otras estadísticas. Este reporte hace uso de la combinación de los registros del servicio Web Proxy y del Firewall; ayudan a la planeación de una mejor política para el uso de Internet y del ancho de banda del mismo.

- **Reportes de Seguridad.** Ayudan a la identificación de violaciones de seguridad o intentos de ataque después de que hayan ocurrido. Estos informes se generan por la combinación de los registros de servicios del Web Proxy, del Firewall y del Filtro de Paquetes.

4.2.1 REPORTE DE ACTIVIDADES DE ISA SERVER

Puesto que el tema de investigación es acerca del firewall, nos enfocaremos en tipos de reportes que usan el servicio de registros del mismo.

A través de este trabajo, hemos revisado temas que tratan acerca de la seguridad de una red de computadoras (es decir, Red de Área Local); por lo tanto, sería bueno determinar el uso de por lo menos tres tipos diferentes de reportes proporcionados por ISA Server que nos pueden ser de gran ayuda para establecer buenas políticas de seguridad (si ya existen, entonces sería corregir y aumentar).

De esta manera estaremos logrando como buenos administradores de red, proporcionar un nivel de seguridad "CONFIABLE" (no confundir con excelente ó 100% seguridad).

CINCO ERRORES EN LO QUE SE TIENE QUE EVITAR CAER
1. No contar con especialistas en seguridad informática que se mantengan actualizados y realicen funciones alrededor de la seguridad informática al 100%.
2. Considerar que la instalación de un firewall es suficiente en lo que a seguridad informática se refiere.
3. Olvidar la protección al interior, ya que las estadísticas indican que el mayor peligro está justamente dentro de la empresa.
4. No tomar en cuenta debidamente las políticas de seguridad; o bien, contar con ellas pero no ejecutarlas.
5. No proteger los datos que fluyen por la red a través de recursos corporativos que se proporcionan a usuarios remotos.

Tabla 10 Errores comunes en el entorno de seguridad informática[17]

[17] Revista Red, Octubre 2003, Claudia Martínez Salcedo, pág. 28

La manera de crear reportes en ISA Server es, definiéndolos desde la consola del software en la pestaña *Monitoring Configuration.* Siguiendo el asistente de creación tendremos los reportes de la forma periódica que deseemos.

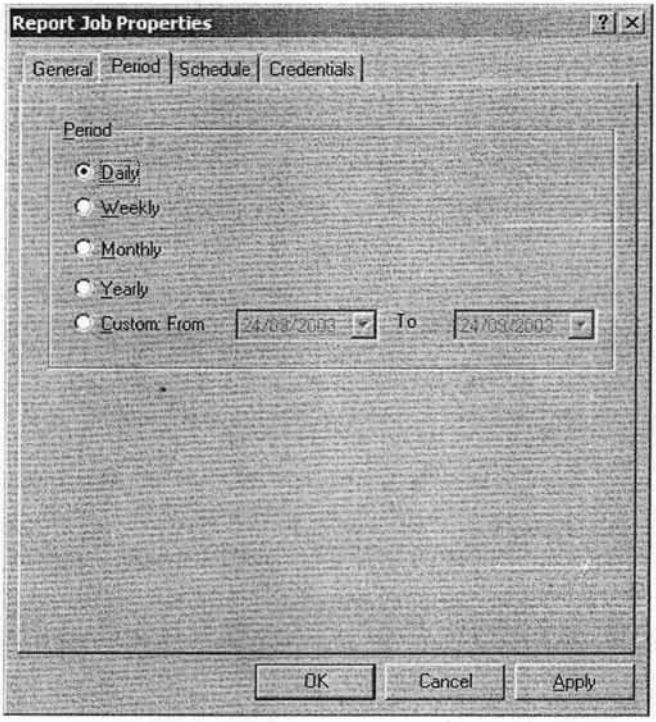
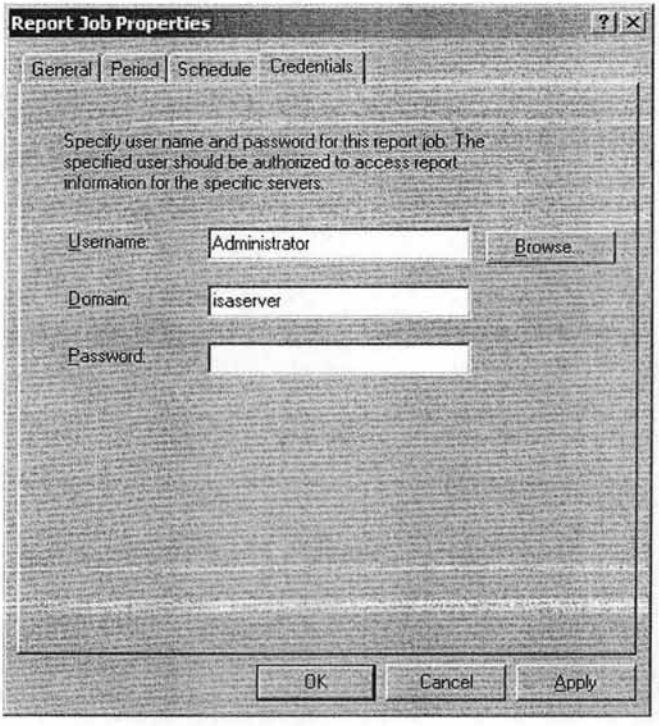


Figura 30 Propiedades de los reportes

Observemos que en la pestaña *Credentials* nos pedirá un nombre de usuario, un dominio y una contraseña; obviamente serán datos de nosotros como los administradores de la red.



Cuando hayamos finalizado de dar de altas tantos reportes queramos, podremos verlos en los formatos que escogimos, obteniendo de estos todos los datos necesarios para seguir mejorando el nivel de seguridad de la red local.

A la vez, de crear o mejorar las políticas de seguridad informática y de datos y evitar, cuantiosas pérdidas en la empresa.

A continuación, veremos un ejemplo gráfico de un reporte en formato HTML.

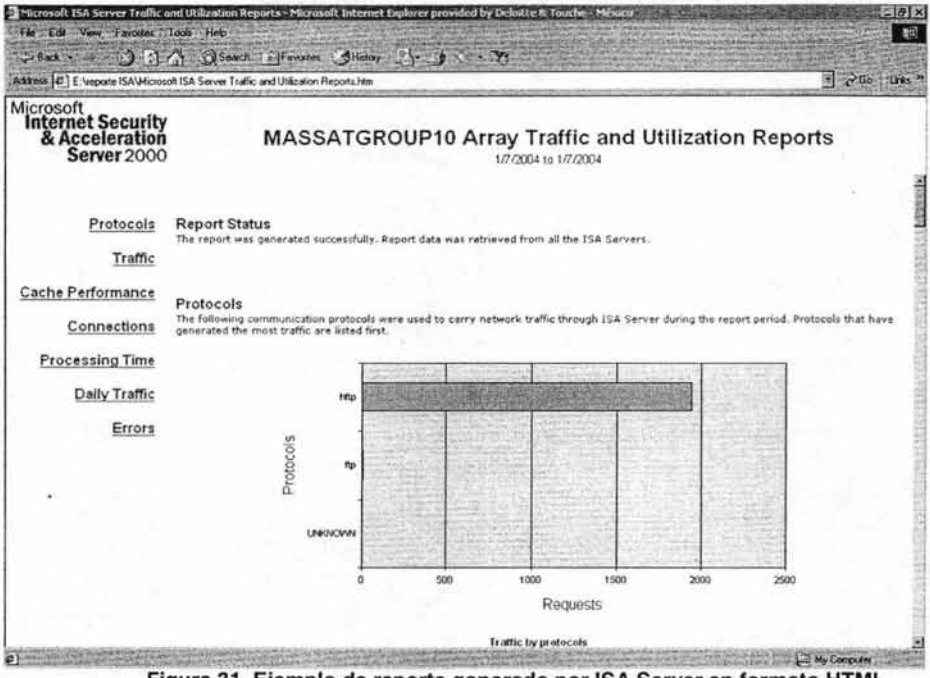
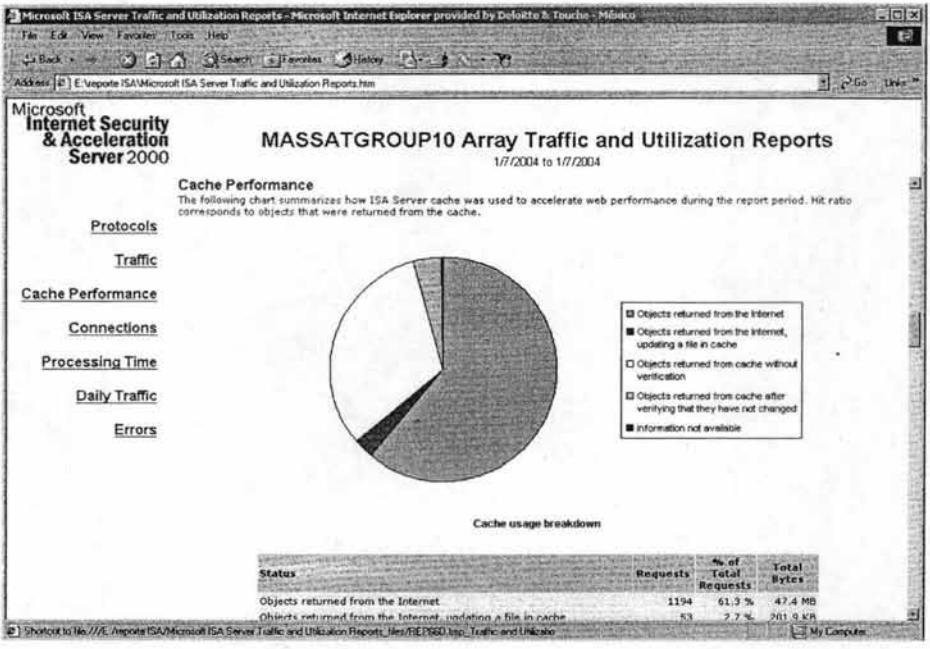


Figura 31 Ejemplo de reporte generado por ISA Server en formato HTML

En este se muestra la actividad de los protocolos FTP y HTTP. La actividad en el protocolo HTTP es de uso constante para esta firma contable y con justa razón, ya que deben estar en constante contacto con la Secretaría de Hacienda y Crédito Público en el envío de informes contables y de auditoria así como también con los reportes de nómina.

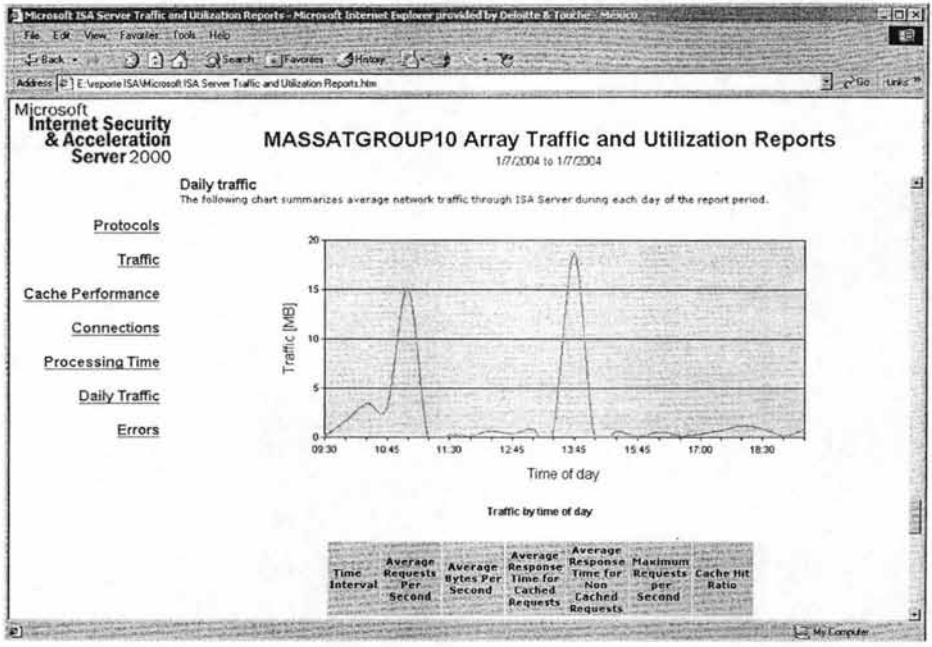
Como se ha mencionado anteriormente, el diseño de los reportes y el monitoreo de la red estará a cargo de o los administradores, quienes deberán tomar en cuenta a los usuarios al momento del diseño de los reportes. La razón es la siguiente: si en algún momento alguien (un usuario final, un socio de la empresa, incluso otro administrador) desea saber el comportamiento de la red informática; la información deberá estar disponible y además entendible.

Cuando se hace mención acerca del entendimiento de los reportes, nos referimos a la ayuda visual y gráfica que pueda existir en estos resúmenes. Para ejemplificar más claramente veamos la siguiente figura.



Microsoft ISA Server, no solamente nos puede proporcionar reportes técnicos que los administradores de redes puedan entender; sino que también hay una parte entendible para cualquier usuario en donde se detalla gráficamente las horas en donde existe un uso incrementado de la red interna en el intercambio de información y el uso del protocolo HTTP (Internet).

La siguiente figura demuestra lo que se acaba de definir en las líneas anteriores.



Sin embargo, el formato HTML no es el único con el cual se pueden manejar los reportes. Microsoft ISA Server nos permite exportar y guardar esta información en el formato ".xls"; es decir, en archivos de Excel.

Desgraciadamente, ISA Server solo se limita a estas dos opciones de formatos de reportes. Por lo cual, deberemos escoger la opción más adecuada para manejar la información; o en su debido caso utilizar ambas opciones según nos convenga como administradores de la red local.

La mejor defensa es la combinación de herramientas de monitoreo con el firewall o los conjuntos de firewall, así como también el realizar una campaña de concientización hacia los usuarios para que de alguna manera implementen ciertas medidas de seguridad y minimizar posibles riesgos de ataques externos o infecciones de virus de computadoras.

Cabe recordar que para una empresa, el manejo de la información es más importante que el mismo equipo de cómputo. Los procedimientos de respaldo de información (si los hubiera) deberán ser evaluados y aprobados por los administradores de la infraestructura tecnológica sin hacer a un lado las políticas de seguridad; tomando en cuenta la periodicidad de ataques remotos o la frecuencia con la que se infectan con virus y si tienen alguna pérdida de datos debido a dichos factores.

Para quienes piensan en tomar la decisión de implementar firewall, deberán considerar variables tales como costo, compatibilidad, método de implementación, método de configuración, costo del mantenimiento, especialización en el producto entre otros. A su vez, asumirán responsabilidades acerca del monitoreo de las actividades de los usuarios finales dentro y fuera de la red local.

Como sabemos, los productos de la Corporación Microsoft son propensos a diversos ataques debido a que es considerada una copia de Linux. Sin embargo, aquí en México, un cierto porcentaje de las empresas (grandes, pequeñas y medianas) usan esta tecnología debido a los convenios establecidos entre las marcas de computadoras (por ejemplo Dell, IBM, HP, Sony, etc.) y Microsoft; que puede traer como consecuencia el uso del programa que se ha estado mencionando en esta tesis que es Microsoft Internet Security and Acceleration Server 2000.

ISA Server ha demostrado poseer total flexibilidad y bajo costo de mantenimiento, característica y ventaja a favor del programa para su uso. Para las PyMES, sería una buena solución para reducir su nivel de vulnerabilidad ante Internet. Al final, la decisión le corresponde tomarla a aquella persona que busca aumentar la seguridad de la red local.

CONCLUSIONES

En el presente trabajo se plantean las problemáticas más frecuentes de seguridad informática que pueden existir en las diversas organizaciones e instituciones, las cuales nos obligan a definir estrategias y tomar medidas adecuadas para hacer frente a este tipo de situaciones, todas ellas enfocadas a disminuir los riesgos de nuestra operación diaria.

Esta necesidad de implementación ha tomado el carácter de obligatorio, sin importar tamaño, rubro o infraestructura de las empresas; para lo cual existen una enorme cantidad de elementos y esquemas, los cuales se pueden adaptar a las necesidades especificas, por ejemplo, las PyMES, donde la gran mayoría de ellas basan su operación en productos Microsoft.

Ante tal escenario resulta de suma importancia la implementación de un Firewall (como una alternativa de solución) adecuado a la infraestructura de las PyMES, siendo indispensable hacer un análisis considerando una serie de criterios que nos ayuden a justificar su selección. Existe una gran variedad de productos con firewall, siendo una excelente opción Microsoft Internet Security and Acceleration Server 2000.

Las conclusiones a las que se llegaron son:

- La operación de todas las empresas lleva implícitamente un riesgo, el cual no se puede eliminar, pero si disminuir con estrategias y herramientas adecuadas que no entorpezcan la operación diaria.
- Para diseñar y elegir las estrategias y herramientas adecuadas que nos ayuden a disminuir los riesgos de operación, es necesario un análisis formal que nos oriente y de certidumbre, ya que no podemos experimentar en la operación.
- Existen muchas herramientas para seguridad informática, algunas han alcanzado el carácter de indispensable, siendo una de ellas los firewall.

- Se debe recordar en todo momento que los firewall (como otros elementos de seguridad informática) necesitan configuración, actualización y administración para asegurar su correcto uso y desempeño, no son elementos que se instalan y se olvidan; al contrario, cada situación que cambia en la infraestructura que protegen obligan que se revise su configuración para asegurar que cumplan con su objetivo.
- Los firewall no son mágicos, tienen gran capacidad, pero también tienen sus limitantes; por lo tanto en el cotidiano monitoreo que se realiza, se debe tener cuidado de tomar en cuenta cualquier detalle o riesgo encontrado para poder corregirlo. Existen muchos dispositivos y herramientas que nos permiten complementar o subsanar las limitantes de un firewall, la clave esta en hacer una correcta selección con un análisis previo.
- Microsoft Internet Security and Acceleration Server 2000 es un firewall que cumple con las expectativas de los administradores y usuarios, sobre todo para las PyMES que utilizan las herramientas de Microsoft, recordando en todo momento que hay herramientas que lo pueden complementar.

GLOSARIO

Palabra(s)	Descripción
3DES	Triple Data Encryption Estándar
Active Directory	Un servicio de directorios es un servivio de red que identifica todos los recursos en ella y los vuelve accesibles a los usuarios y a las aplicaciones. El elemento principal de AD es el directorio, que almacena informacion sobre los recursos de la red y los servicios que hacen disponible la informacion. Los recursos almacenados en el directorio, como los datos del usuario, impresoras, servidores, bases de datos, grupos, computadoras y politicas de sistema, se denominan objetos.
AES	Advance Encryption Standar
Bugs	Puntos débiles de los programas, generalmente aprovechados por hackers para demostrar los bajos niveles de seguridad existentes o lo mal diseñados que puedan estar los softwares.
DES	Data Encryption Standar
DNS	(Domain Name System). Sistema de Nombres de Dominio. El DNS un servicio de búsqueda de datos de uso general, distribuido y multiplicado. Su utilidad principal es la búsqueda de direcciones IP de sistemas centrales ("hosts") basándose en los nombres de estos. El estilo de los nombres de "hosts" utilizado actualmente en Internet es llamado "nombre de dominio". Algunos de los dominios mas importantes, que sin embargo son muy escasamente utilizados fuera de los Estados Unidos de América, son: .COM (comercial- empresas), .EDU (educacion, centros docentes), .ORG (organización sin ánimo de lucro), . NET (operación de la red), .GOV (Gobierno USA) y .MIL (ejercito USA). La mayoría de los países tienen un dominio propio. Por ejemplo, .US (Estados Unidos de América), .ES (España), .AU (Australia).
FTP	FTP son las siglas de File Transfer Protocol, el nombre del protocolo estándar de transferencia de ficheros. Su misión es permitir a los usuarios recibir y enviar ficheros de todas las máquinas que sean servidores FTP. El usuario debe disponer del software que permita hacer la transferencia (actualmente todos los navegadores, ya disponen de ese software para recibir ficheros). Los ficheros pueden ser documentos, textos, imágenes, sonidos, programas, etc., es decir, cualquier cosa que se pueda almacenar en un fichero o archivo. En Internet hay miles de ordenadores con centenares de ficheros de todas las clases a los que el público tiene acceso. Para conectar con un servidor FTP, debemos conocer su dirección al igual que para conectar con una página Web: Ej. ftp://ftp._____ Hay muchos servidores FTP y por lo tanto, muchos ficheros. Para buscar estos ficheros se puede utilizar el sevicio Archie. Archie reúne todos los ficheros FTP y los indexa regularmente por título y palabra clave.

Palabra(s)	Descripción
Gateway	Computador que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, una puerta de acceso podría conectar una LAN de computador personal a una red de mainframe. Una puerta de acceso de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.
H.323	El protocolo H.323 es un estándar aprobado por ITU (International Telecommunication Union) que define como se *empaquetan* los datos multimedia transmitidos a través de la red.
H.323 Gatekeeper	Servicio de ISA Server 2000 que permite configurar y dirigir conexiones entrantes que utilicen el protocolo H.323
Hacker(s)	Tradicionamente se considera Hacker al aficionado a la informática cuya afición es buscar defectos y puertas traseras para entrar en los sistemas. Para los especialistas, la definición correta sería: experto que puede conseguir da un sistema informático cosas que sus creadores no imaginan.
HTML	(HyperText Markup Language). Lenguaje de marcado de Hipertexto. Es el lenguaje estándar para describir el contenido y la apariencia de las páginas en el WWW.
HTTP	(Hiper Text Transfer Protocol). Protocola de transferencia de HiperTexto. Es el protocolo de Internet que permite que los exploradores del WWW recuperen información de los servidores. Es un protocolo de aplicación con la sencillez y velocidad necesaria para sistemas de información distribuidos, colaborativos y de diferentes medios. Es un protocolo general, independiente y orientado a objetos usado para diferentes tareas, como sistemas de nombres de servidores y de administración de objetos distribuidos, a través de la extensión de sus métodos (comandos). Una característica de HTTP es la forma de representar los datos, permitiendo a los sistemas funcionar independientemente de los datos siendo transferidos. HTTP ha sido usado por el WWW desde 1990.
HTTPS	HyperText Transfer Protocol Secure
IANA	(Internet Assigned Number Authority). Autoridad de Números Asignados en Internet. Organización responsable de asignar los números usados por los protocolos TCP/IP. Por ejemplo, la IANA asigna direcciones IP.
ICMP	(Internet Control Message Protocol). Protocolo de control de mensajes de interred. Protocolo usado por el IP para informar de errores y excepciones. El ICMP también incluye mensajes informativos usados por algunos programas como ping.
IIS	Internet Information Services
IP	Internet Protocol. El IP es utilizado por los protocolos del nivel de transporte como TCP para encaminar los datos hacia su destino. Tiene únicamente la misión de encaminar el datagrama, sin comprobar la integridad de la información que contiene.

Palabra(s)	Descripción
ISDN	(Integrated Services Digital Network). Siglas inglesas de la RDSI, Red Digital de Servicios Integrados. Red digital de servicios integrados. Estándar internacional de telecomunicaciones para la transmisión de voz, video y datos a través de líneas digitales que corren a 64 Kbits/seg.
LAN	(Local Area Network). Red de área local. El término LAN define la conexión física y lógica de ordenadores en un entorno generalmente de oficina. Su objetivo es compartir recursos (como acceder a una misma impresora o base de datos) y permite el intercambio de ficheros entre los ordenadores que componen la red. Los servidores son máquinas de alta velocidad que contienen programas y datos que comparten todos los usuarios de redes. Las estaciones de trabajo, o clientes, son los computadores personales de los usuarios, que realizan procesamiento autónomo y tienen acceso a los servidores de la red según se requiera. El software de control en una LAN es el sistema operativo de la red como NetWare, UNIX y Appletalk que reside en el servidor. En cada cliente reside una parte componente del software y permite que la aplicación lea y escriba datos del servidor como si estuviera en la máquina local. La transferencia de mensajes es administrada por un protocolo de transporte como IPX, SPX y TCP/IP. La transmisión física de datos es realizada por el método de acceso (Ethernet, Token Ring, etc.) que se implementa en los adaptadores de la red y que conectan a las máquinas. La vía de acceso real de las comunicaciones es el cable (par trenzado, cable coaxial, fibra óptica) que interconecta cada adaptador de red.
Malware	Programa creado con intenciones maliciosas para, posiblemente, causar algún tipo de daño ya sea en el sistema operativo o más concretamente en algún tipo de datos.
MIME	(Multipurpose Internet Mail Extension) Extensión multipropósito de correo Internet. Extensiones para el formato SMTP que permite llevar múltiples tipos de datos (binario, audio, video, etc.).
MS-DOS	Microsoft System - Disk Operating Systems
NAT	Network Address Translation
Nodo	Es el punto en donde se producen dos o más conexiones en una red de comunicaciones. No se trata de un elemento estrictamente físico, sino de una unidad funcional que exige hardware y software. Un nodo puede incluir controladores de comunicaciones, clusters, servidores, repetidores, etc,
NTFS	New Technology File System
ODBC	Open Data Base Connection (Conección abierta a base de datos) . Es una forma de conección a veces de datos, independientemente del lenguaje o programa que estemos utilizando. Cada fabricante provee su propia libreria(DLL) con las caracteristicas de conección a las bases de datos.
PAT	Port Address Translation

Palabra(s)	Descripción
Path	Camino que toma el software para acceder a los datos contenidos en una unidad de almacenamiento.
POP3	(Post Office Protocol). Protocolo de Oficina de Correos. Protocolo diseñado para permitir a sistemas de usuario individual leer correo electrónico almacenado en un servidor.
PPPoE	(Point to Point Protocol). Protocolo de punto a punto. Se utiliza para la transmisión de información entre ordenadores por vía telefónica.
Proxy	Es un programa que realiza la tarea de encaminador, utilizado en redes locales, su función es similar a la de un router, pero es injustificable el gasto en redes locales
Puerto	Es un elemento hardware, una especie de enchufe que permite la salida y entrada del ordenador mediante la conexión a distintos tipos de periféricos.
PyME	Pequeña y Mediana Empresa
Router	Originalmente, se identificaba con el término gateway, sobre todo en referencia a la red Internet. En general, debe considerarse como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.
SMTP	(Simple Mail Transfer Protocol). Protocolo Simple de Trasferencia de Correo. Protocolo que se usa para trasmitir correo electrónico entre servidores.
Socket	Número de identificación compuesto por dos números: La dirección IP y el número de puerto TCP. En la misma red, el nº IP es el mismo, mientras el nº de puerto es el que varia.
Switch	Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI. Término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.
TCP	(Transmision Control Protocol/Internet Protocol). Se trata de un estándar de comunicaciones muy extendido y de uso muy frecuente para software de red basado en Unix con protocolos Token-Ring y Ethernet, entre otros. Es compatible con productos de muchas marcas: IBM, DEC, Sun, AT&T, Data General, etc. TCP/IP es conforme a los niveles 3 y 4 de los modelos OSI. Este conjunto de protocolos fue desarrollado originalmente para el Departamento de Defensa de Estados Unidos.

Palabra(s)	Descripción
UDP	User datagram protocol. Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya esta blecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Se utiliza cuando se necesita tran smitir voz o vídeo y resulta más importante transmitir con v elocidad que garantizar el hecho de que lleguen absolutament e todos los bytes.
UPS	(Uninterrumpible Power Supply). Fuente de alimentación ininterrumpible. Energía de seguridad que se emplea cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de voltaje inaceptable. Los pequeños sistemas UPS proveen energía de baterías durante sólo unos pocos minutos; los necesarios para apagar el computador de manera ordenada. Los sistemas complejos están conectados a generadores eléctricos que pueden proveer energía durante días. Una UPS en línea provee una fuente constante de energía eléctrica a partir de una batería, mientras ésta es recargada a partir de la energía de corriente alterna. Una UPS fuera de línea, también conocida como standby power system (SPS - sistema de alimentación auxiliar), conmuta a energía de batería en unos pocos milisegundos después de detectar una falla en el suministro de energía.
URL	(Universal Resource Locator). Localizador Universal de Recursos. Sistema unificado de identificación de recursos en la red. Las direcciones se componen de protocolo, FQDN y dirección local del documento dentro del servidor. Permite identificar objetos WWW, Gopher, FTP, News, etc. Una cadena que suminstra la dirección Internet de un sitio Web o de un recurso World Wide Web, junto con el protocolo por el que se tiene acceso a ese sitio o a ese recurso. El tipo más común de dirección URL es http://, que proporciona la dirección Internet de una página Web.
VLAN	Virtual Local Area Network
VPN	(Virtual Private Network) Red privada virtual. Red de comunicaciones de área ancha provista por una portadora común que suministra aquello que asemeja líneas dedicadas cuando se utilizan, pero las troncales de base se comparten entre todos los clientes como en una red pública. Permite configurar una red privada dentro de una red pública.

BIBLIOGRAFÍA Y REFERENCIAS URL

- **DEPLOYING AND MANAGING MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2000**,
  Microsoft Training and Certification,
  Curso 2159A

- **CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES**,
  Manuel José Lucena López,
  Segunda edición, Septiembre de 1999,
  167 páginas.

- **SEGURIDAD EN UNIX Y REDES**,
  Antonio Villalón Huerta,
  Julio del 2000,
  325 páginas.

- **LINUX: INTALACIÓN Y PRIMEROS PASOS**,
  Matt Welsh,
  Noviembre de 1996,
  242 páginas.

- **EL ABC DE LA SEGURIDAD INFORMÁTICA**,
  Ulises Castillo,
  Agosto de 1998,
  140 páginas.

- **Revista RED**,
  Sección "De Portada",
  Publicada en el mes de Octubre 2003

Referencias URL

- http://www.networking.com/netdesing/wall2.html
- http://caissa.odn.state.us/sa/htmfiles/0506/x0038_do.htm
- http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html
- http://jjnet.prohosting.com/linux/como-firewall.html
- http://www.deepzone.org/editions/others/gestion.htm
- http://www.vicomsoft.com/knowledge/reference/firewalls1.html
- http://www.eurologic.es/cifrado/hash.htm
- http://www-mat.upc.es/~jforne/ce_tema2.pdf
- http://lssd.esimecu.ipn.mx/ssi/memorias/4.pdf
- http://www.inf.utfsm.cl/~rmonge/seguridad/cripto-04.pdf
- http://www.secure-hash-algorithm-md5-sha-1.co.uk
- http://www.itl.nist.gov/fipspubs/fip180-1.htm
- http://www.symantec.com/region/mx/product/integrated/clientsecurity
- http://www.cisco.com/en/Us/products/hw/vpndevc/ps2030
- http://segurinet.com/gsal/cortafuegos.htm
- http://www.trendmicro.com/la/products/gateway/iswp-isa/evaluate/overview.htm
- http://www.urg.es/~aquiran/cripto/pgp01.htm

- http://perux.iespana.es/defecpgp.html
- http://www.busan.edu/~nic/networking/firewall
- http://www.windowssecurity.com
- http://www.iana.org
- http://www.unam-cert.unam.mx
- http://www.glosarium.com
- http://www.isaserver.org
- http://www.microsoft.com/mexico