UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA
UNAN-LEÒN

FACULTAD DE CIENCIAS
DEPARTAMENTO DE COMPUTACIÓN

TEMA:

SELECCIÓN Y EVALUACIÓN DE FIREWALLS CON LICENCIA DE SOFTWARE LIBRE

AUTORA: **Br. GUILLÉN ZAMORA MAYELI DONALE**

TUTOR: **Lic. RINA PILAR ARÁUZ ALTAMIRANO.**

LEÓN, 25 DE JULIO DEL 2008.

AGRADECIMIENTO.

Agradezco, a Dios nuestro padre celestial por darme la fuerza, inteligencia y perseverancia para terminar este trabajo.

A mi tutora Licenciada. Rina Aráuz por brindarme su apoyo incondicional y ofrecerme lo mejor de sus conocimientos en todo los momentos que la solicité.

A los profesores: Msc. Martín Ibarra y el Licenciado Aldo Martínez que muy amablemente dedicaron su tiempo a mi trabajo, dándome críticas positivas para el beneficio de esta monografía.

DEDICATORIA.

Dedico la presente monografía de manera muy especial a **Denis Ramón Sevilla Oporta** quien fue mi compañero de vida y estuvo presente siempre en los buenos y malos momentos dándome lo mejor de su persona, su apoyo, ánimo de seguir luchando para superarme y ser mejor en la vida y su ayuda incondicional sin pedir nunca nada a cambio.

DEDICATORIA

A JEHOVA DIOS Padre Celestial por darme la fuerza, sabiduría y la perseverancia para poder terminar el presente trabajo.

A mi madre Lillian Robleto Guillén y mi padre Carlos Zamora Mayorga por darme lo mejor de su persona a través de mi vida, con su amor, cariño, apoyo y ayuda incondicional sin pedir nunca nada a cambio.

A mi hija Fabiola Verónica Sevilla Zamora quien es mi principal motivación para culminar mi trabajo monográfico y así brindarle una mejor educación.

En general a todos mis hermanos que han estado conmigo siempre dándome comprensión, animándome a salir adelante, y apoyándome en todas mis decisiones.

A mi amiga Marjorie Picado Pacheco que de una u otra manera siempre ha estado a mi lado en los buenos y malos momentos brindándome su apoyo, y ayuda incondicional.

A mis amigos: Manuel Sevilla Ruiz, y Juan Carlos Peralta Sirias ya que cada uno de ellos me ayudaron a hacer mi sueño realidad brindándome de manera diferente sus ayudas.

INDICE.

INTRODUCCIÒN.

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada a Internet, sin tomar en cuenta el tipo de negocio, a medida que va aumentando la demanda de usuario en el Internet se van creando menos espacios confidenciales que crean diferentes problemas de seguridad a las organizaciones tales como: Bancos, Paginas privadas en Internet entre otros tipos de sistemas.

Los Firewalls son el dispositivo que funciona como barrera defensiva en las redes permitiendo que los usuarios de redes privadas superen los temores, creando un nivel de protección adecuado para el flujo de la información, protegiendo así la información privada. Aun así que la organización no esta conectada a Internet, esta debería establecer una política de seguridad interna para administrar el acceso al usuario sin afectar la red privada.

Aunque los Cortafuegos son apenas uno de los componentes de un sistema de seguridad, constituyen un componente esencial. Las empresas deben de invertir el tiempo para evaluar el sistema que mejor se ajuste a sus necesidades e implementarlo a la brevedad posible. Las deficiencias de seguridad son un peligro constante y no existe mejor oportunidad para proteger el acceso a la red de su empresa, que implementar un Firewall.

Siendo esto la necesidad de conocer la utilidad de los cortafuegos, su funcionamiento, su importancia y los mecanismos o técnicas para seleccionar el más adecuado dependiendo del sistema que posea o desee implantar el usuario.

Los firewalls libre brindan la seguridad y confianza para proteger información confidencial al igual que lo hacen los software comerciales, siendo estos de vital importancia y con licencia libre en cualquier campo donde se desee brindar protección.

ANTECEDENTES.

Cualquier empresa que contempla conectarse al Internet se ve forzada a lidiar con el tema de la seguridad de la red. La popularización de Internet ha originado múltiples problemas de seguridad hasta el punto en que, hoy por hoy, esta inseguridad inherente a la red es, según todos los expertos, el principal obstáculo para el éxito de las actividades de Comercio electrónico.

En respuestas a estos riesgos se ha ido formando necesidades básicas que requieren tener las distintas empresas conectada a Internet pero que a la vez requieren mantener la confidencialidad, integridad y disponibilidad de su información y recursos de la red.

El Firewall se ha convertido, de esta forma, en un dispositivo indispensable dentro de la arquitectura de cualquier red de ordenadores que tenga acceso a Internet.

Los primeros dispositivos cortafuegos aparecieron en la mitad de la década de los 80, implementaban simples y rudimentarios filtros de paquetes de datos oyéndolos y rechazando aquellos que no cumplían con un formato pre-programado hasta los actuales dispositivos capaces de analizar simultáneamente la actividad en múltiples capas de la red, la tecnología ha evolucionado creando herramientas más sofisticadas y seguras.

Estos software no son seleccionados por el usuario de modo que se escoja el mas conveniente para su sistema, ya que generalmente se selecciona sin ningún criterio técnico basándose en la popularidad de estos; es por ello que se establecerá las diferencias entre estos para demostrar cual es el mas adecuado y que cumple con los requerimientos básicos de seguridad.

En la actualidad no se ha realizado en la Unan-León un tema monográfico que trate sobre este tipo de investigación.

JUSTIFICACIÓN.

El lenguaje que utilizamos y la forma de pensar sobre los códigos maliciosos han cambiado significativamente en los últimos años. Las actuales amenazas de códigos maliciosos son generalmente sinónimos de vulnerabilidades de software y viceversa.

Los investigadores de la seguridad buscan cada vez más vulnerabilidades que se puedan aprovechar de manera remota debido al gran número de blancos a los que pueden acceder las redes interconectadas.

El presente trabajo está dirigido a las diferentes empresas o industrias que deseen implementar una red ya sea esta Doméstica, de área local(LAN) e Inalámbrica, para garantizar una comunicación fluida con la red además de mantener una alta seguridad y por ende privacidad a sus datos, siendo los firewalls la confianza oportuna a los diversos tipos de usuarios brindándoles resguardo en el acceso a la red y sus recursos, de esta manera tanto los usuarios internos como externos se ven beneficiados dándoles mayor comodidad en sus gestiones, las cuales, necesitan de la seguridad que brindan estos tipos de Firewalls.

La tecnología va constantemente evolucionando para lograr beneficios o para causar daños los cortafuegos libres son de gran importancia para contrarrestar la presencia de intrusos en las redes y brindar seguridad, para los cuales están diseñados.

OBJETIVOS.

OBJETIVO GENERAL.

- Realizar selección y evaluación de los Firewalls de software libres más comunes existentes en el mercado.

OBJETIVOS ESPECIFICOS.

- Establecer las diferencias entre algunos tipos de Firewalls con licencia de software libre o gratuito.
- Realizar pruebas de comparación entre los diferentes paquetes de Firewalls con licencia de software libres seleccionados.
- Realizar configuración de un Firewall en Sistema Operativo LINUX.
- Establecer un criterio de selección.

METODOLOGÍA DEL TRABAJO.

El método a utilizar en la investigación es científico general, se basa en la serie ordenada de procedimientos que hace uso de la investigación científica para obtener la extensión de nuestros conocimientos. Este método contribuye a establecer las diferentes estrategias de investigación.

El método científico busca alcanzar la verdad fáctica o basada en hechos mediante la adaptación de las ideas a los hechos, para lo cual utiliza la observación y la experimentación.

RECURSOS DISPONIBLES Y NECESARIOS

- Acceso a INTERNET para la recopilación de la información
- 2 computadoras hp, con 20 Gb de Disco duro, Memoria RAM de 130,544 KB, procesador de 1.60HHz.
- Sistemas Operativos Windows y Linux. Para realizar las pruebas de los diferentes firewalls.
- ip Pc1: 192.168.151.219
- ip Pc2: 192.168.151.235
- Mascara: 255.255.255.0
- Puerta de enlace: 192.168.151.1
- Puerta de enlace: 192.168.151.1
- Tipo de conexión: ADSL
- Topología de red: Estrella
- Una tarjeta de red inalámbrica
- Dos tarjetas de red integradas y dos interfaces de entradas, esto para hacer dos conexiones de Internet, una para exterior y otra para la red LAN.
- El esquema de la red LAN puesta en práctica se elaboro en un Cyber para hacer las pruebas de los diferentes Firewalls.

MÉTODO DE EVALUACIÓN

Los diferentes firewalls seleccionados bajo el sistema operativo Windows fueron puestos en prueba mediante el Tes. **Atelier Web Firewall Tester,** con el fin de establecer las diferencias y rendimientos de cada uno de ellos.

ANÁLISIS Y DISEÑO.

Una de las mayores preocupaciones que tienen hoy en día los administradores de redes es que usuarios ajenos a sus redes logren el acceso y control absoluto de la red local.

Para comprender el nivel de seguridad que una red requiere es necesario considerar como factor principal el valor de los datos. Al evaluar el valor de los datos hay que tomar en cuenta riesgos tales como: perdida de información, alteración del contenido de esta, daños físicos a la red local, como consecuencia de haber comprometido la red. Toda red que esta conectada a Internet necesita un Firewall.

La conectividad total se ha convertido en una necesidad para poder sobrevivir en el ambiente competitivo del nuevo milenio. Esto ha traído, al mismo tiempo, serios problemas de seguridad al facilitar el acceso desde el mundo exterior a través de Internet y así exponer los recursos internos de la red. Para impedir que personas no autorizadas penetren en la red o que accedan a más información de la permitida, se utiliza un sistema de defensa perimetral (cortafuego), el cual se coloca como una barrera de protección entre Internet y la red local.

A la hora de implementar un sistema de red local, surgen preguntas como las siguientes:

¿Qué es un Firewall?
¿Para que sirve?
¿Realmente puede un Firewall protegerme de intrusos?
¿Cuál es el mejor Firewall?
¿Que Firewall elegir a la hora de utilizar uno?
¿Se pueden bajar gratis, o son todos los Firewall pagos?
¿Cual es el más recomendable?

Un sistema basado en Firewalls no es el remedio para la seguridad. Continuamente se descubren fallas en los productos comerciales y aparecen nuevos tipos de ataques. Y lo que es peor, la mayoría de los sistemas se configuran mal y carecen de mantenimiento.

DESCRIPCIÓN DEL PROBLEMA.

La Selección y evaluación del Cortafuego está enfocada en lograr que el cliente elija el mas conveniente y por ende funcione perfectamente brindando la seguridad a su red local. En caso de que el software haya sido adquirido o instalado, la política de seguridad define las reglas que se aplicarán en estos. Las reglas especifican el origen, destino, servicio y acción a realizar para cualquier transacción. También definen que eventos deben guardarse en bitácoras (logs). La primera regla es usualmente no permitir cualquier acción a no ser que esté permitida expresamente, puesto que las posibles brechas de seguridad son más fácilmente identificables de esta manera.

Es imprescindible que la política de seguridad esté diseñada de acuerdo a los activos de información que se quieren proteger y a las condiciones específicas de cada área donde se instale una red local. Es por ello que cada día los Firewalls tienen que ajustarse a las necesidades reales y eventos que suceden al ingresar intrusos a la red local teniendo en cuenta, que cada día surgen nuevas maneras y por ende nuevos intrusos que invaden la seguridad de dichas redes.

El problema principal al momento de conectar una red local a Internet es el acceso de usuarios no autorizados a la red local para acceder a más información de la permitida.

Es por esto que se presenta la selección de los diferentes Cortafuegos más comunes para que el cliente obtenga la información necesaria y de esta manera elija el más conveniente a instalar en su red local o en su PC personal dependiendo de los recursos que posea, limitando el acceso de usuarios indeseados a los recursos de su red.

MARCO TEÓRICO.

Conectar una red a Internet representa un riesgo serio para la seguridad. La red se hace accesible no sólo para los usuarios legítimos, sino también para los hackers. Con el fin de salvaguardar los datos sensibles de una red, se recomienda encarecidamente el uso de un Firewall.

Un cortafuegos, o bien un gateway/router con funciones de Firewall, sirve como protección de seguridad, al evitar entradas no autorizadas a la red.

Debido a la importancia de la seguridad en las redes se ha planteado la utilización de software basados en soluciones denominadas libres u "Open Source".

Antes de entrar en materia debemos conocer ciertos conceptos que se utilizan en este documento y de los cuales debemos estar claros para comprender este tema:

- **Plug-in**: es una aplicación informática que interactúa con otra aplicación para aportarle una función o utilidad específica, generalmente muy específica, como por ejemplo servir como drive (controlador) en una aplicación, para hacer así funcionar un dispositivo en otro programa. Ésta aplicación adicional es ejecutada por la aplicación principal. Los plugins típicos tienen la función de reproducir determinados formatos de gráficos, reproducir datos multimedia, codificar/decodificar emails, filtrar imágenes de programas gráficos.

- **Firewalls o cortafuegos:** un firewall es un sistema que impone una política de seguridad entre la organización de red privada y el Internet.

- **Software libre:** es el software que, una vez obtenido, puede ser usado, copiado, estudiado, modificado y redistribuido libremente.

- **Hacker:** toda persona involucrada en actos que atentan en contra la propiedad intelectual, seguridad en las redes, autores de virus, intrusos de servidores, interceptadores de mensaje de correo, vándalos del ciberespacio, etc.

- **Open source:** es el término con el que se conoce al software distribuido y desarrollado libremente.

- **Red lan:** una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo un edificio.

- **Topología:** la topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio.

En este caso se implemento la topología de estrella que es donde la red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

- **Plataforma:** una plataforma es precisamente el principio, ya sea de hardware o software, sobre el cual un programa puede ejecutarse. ejemplos típicos incluyen: arquitectura de hardware, sistema operativo, lenguajes de programación y sus librerías de tiempo de ejecución.

- **Routers:** dispositivo que permite conectar uno o varios equipos incluso una red de área local (LAN) al Internet a través de una línea telefónica con un servicio adsl, este pertenece al nivel de red de la capa OSI.

- **Ataque:** evento, exitoso o no, que atenta sobre el buen funcionamiento de un sistema.

- **Servidor:** un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

- **Nodo bastión:** es un ordenador en una red que ofrece un único punto de entrada y salida a Internet desde la red interna y viceversa. El nodo bastión se usan para mitigar los riesgos de seguridad en una red, ofreciendo una barrera entre el área pública y privada.

- **Sniffers:** es un programa que rastrea la información que transita en Internet. Desde un correo electrónico, hasta una operación de banca en línea.

- **Servicio:** es un programa que se puede ejecutar utilizando internet. Ejemplos: correo electrónico, chat en línea, world wide web.

- **Ataques syn: es** un ataque de inundación o sobre uso de el bit syn con la finalidad de saturar a la víctima y así dejarlo down, esto es muy usado en las salas de chat o en los servicios de mensajería instantánea (msn, yahoo, etc.)

- **Mecanismos tunneling:** consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de comunicaciones (o red de computadoras).

- **Kernel:** se puede definir como el corazón del sistema operativo. Es el encargado de que el software y el hardware de un ordenador puedan trabajar juntos.

- **Tráfico de entrada:** se denomina tráfico de entrada a la cantidad de datos que ingresan a la red u ordenador. esta circulación se mide en unidades de información por unidad de tiempo: bits/segundo, kb/segundo, o mb/segundo.

- **Tráfico de salida:** se denomina tráfico de entrada a la cantidad de datos que salen a la red u ordenador. esta circulación se mide en unidades de información por unidad de tiempo: bits/segundo, kb/segundo, o mb/segundo.

- **log:** archivo que registra movimientos y actividades de un determinado programa (log file). En un servidor web, se encarga de guardar todos los requerimientos (“requests”) y servicios entregados desde él, por lo que es la base del software de estadísticas de visitas.

- **Paquete:** cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca, también llamado trama.

- **Puerto:** lugar donde la información entra o sale de un ordenador, o ambas cosas.

- **Ftp:** file transfer protocol (protocolo de transferencia de ficheros). Protocolo que permite al usuario de un sistema acceder y transferir ficheros de un ordenador a otro a través de internet.

- **Puerto tcp-udp:** Un puerto es un número de 16 bits, empleado por un protocolo host a host para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos. Existen dos tipos de puertos, los puertosTCP (Transmission Control Protocol) y los puertos UDP (User Datagram Protocol) que son utilizados por el protocolo TCP.

- **Dirección IP:** es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo ip (internet protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia osi.

- **proxy:** el proxy es un servidor conectado normalmente al servidor de acceso a la www de un proveedor de acceso que va almacenando toda la información que los usuarios reciben de la web, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado recibirá la información del servidor proxy en lugar del servidor real.

- **Software de red:** consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí.

- **Gateway:** desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como servidores proxy y la máquina donde se ejecuta recibe el nombre de gateway de aplicación o bastion host.

- **Modelo OSI:** (Open Systems Interconection, Interconexión de sistemas abiertos). El cual es usado para describir el uso de datos entre la conexión física de la red y la aplicación del usuario final. Este modelo es el mejor conocido y el más usado para describir los entornos de red. Las capas del modelo OSI son las siguientes:

1. **Capa física:** se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

2. **Capa de enlace:** asegura con confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de las capacidades que se utilizan en la capa de red.

3. **Capa de red:** proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.

4. **Capa de transporte:** esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario. Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica.

5. **Capa de sesión:** administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión

6. **Capa de presentación:** permite a la capa de aplicación interpretar el significado de la información que se intercambia. esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos

7. **Capa de aplicación:** se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.

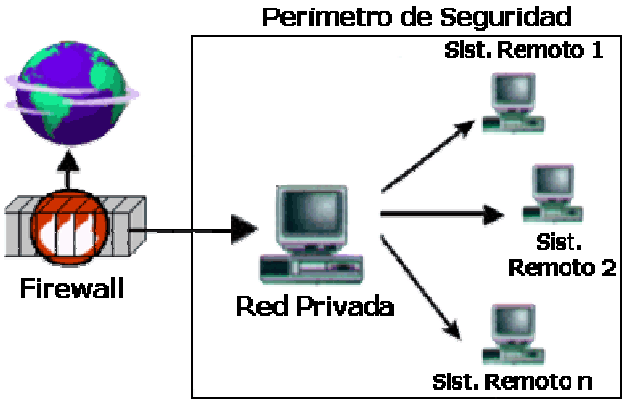
FIREWALL.

Un Firewall es un sistema de seguridad implementado mediante software o hardware que hace de barrera entre una computadora o una red de computadoras y el exterior. Dicho dispositivo analiza todo el tráfico producido entre ambas partes del sistema y se encarga de permitir el paso o no de dicho tráfico dependiendo de la configuración que hayamos realizado para protegerla de intrusos externos que puedan suponer una amenaza a la seguridad. La zona protegida se llama "perímetro de seguridad" y la protección se realiza separándola de una zona externa, no protegida, llamada zona de riesgo.

Puede consistir en distintos dispositivos, sujetos a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

Figura 1



Como puede observarse en la figura 1, el Muro Cortafuegos, sólo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Existen versiones en hardware y software. Los Firewalls hardware ó Firewalls físicos, suelen integrarse en los módem-router de ADSL.

Estos Firewalls son componentes parecidos a los módem externos que se conectan al servidor. Brindan mayor protección al ser una barrera entre el servidor y un intruso. En la mayoría de casos, funcionan como los Firewalls de los sistemas operativos, es decir, no controlan el tráfico saliente para cada aplicación, pero sí que protegen las comunicaciones entrantes en toda la red local; todos los equipos que estén conectados al router estarán protegidos por un Firewall capaz de bloquear el tráfico entrante. Ésta es una buena primera línea de defensa, siempre y cuando no se olvide de instalar un programa de Firewall en todas las estaciones de trabajo.

Los Firewalls software se ponen a la venta o están disponibles de forma gratuita. En ambos casos, el programa controla el tráfico entrante y saliente de forma satisfactoria y es totalmente efectivo. Los Firewalls propietarios suelen estar integrados en paquetes de software de seguridad que son más fáciles de configurar y administrar; además, ofrecen funciones avanzadas, como la detección de ataques mediante denegación de servicio.

Sin embargo, los productos gratuitos normalmente cuentan con funciones menos avanzadas que los productos propietario, como por ejemplo la detección de intrusos (identificación de ataques conocidos con el objetivo de bloquearlos), o bien, la protección de datos personales esta basada en el uso de un filtrado adicional, mediante el cual se bloquean unos datos determinados (como por ejemplo el número de su tarjeta de crédito, etc.), para evitar que salgan del equipo sin su autorización.

Antes de realizar la elección de alguno de estos componentes de software de seguridad para evitar el robo de información, debemos tomar en cuenta algunas decisiones básicas que nos podrán ayudar a escoger el mejor en su campo, las cuales se deben tomar en cuenta al momento de su desarrollo y diseño.

Lo primero que se debe de considerar es: ¿Qué nivel de vigilancia, redundancia y control queremos? y lo segundo es el técnico.

Usualmente un buen firewall debería cumplir con estas condiciones o requerimientos:

- Ser fácilmente configurable
- Presentar información detallada de lo que hace

- Presentar información detallada de las alertas
- Ocupar pocos recursos en memoria
- No ser intrusivo a menos que se lo pidamos
- Ser actualizable

CRITERIOS PARA OPTAR POR UN FIREWALL DETERMINADO.

Tenemos que tener presente que para la elección de un determinado firewall existen varias opciones que nos conlleva a elegir cual se adapta mejor a nuestras necesidades ya que los cortafuegos están implementados para diversas acciones que el usuario requiera, entre estas mencionaremos las siguientes.

- **Integración con la red:** se debe tener presente que los protocolos que se instalen para una determinada red tenga soporte establecido para la misma, Otro aspecto de la integración de red incluye el equipamiento e interfaces requeridos para alta escalabilidad y disponibilidad.
- **Tipos de aplicaciones**: esto se refiere al tipo de uso que le implementemos, ya sea para uso domestico, uso personal o montar una determinada red.
- **Tipos de usuarios:** esto se refiere a la categoría según los privilegios de los usuarios.
- **Cantidad de maquinas:** es un dato muy importante a tener en cuenta ya que la cantidad de maquinas que quieras poner depende del tipo de firewalls que se quiera implementar, por que estos varían.
- **Tipo de información:** son los tipos de filtrado de paquetes que se permite enrutar.
- **Ancho de banda:** es la capacidad de navegación que este tenga en Internet para montar una red.

- **Popularidad de firewall:** este aspecto es muy importante a tomar en cuenta ya que la mayor parte de los usuarios se van por lo mejor que existe en el mercado, y por ende la demanda de un determinado firewall hacen de este el mejor.

- **Eficiencia:** cuando hablamos de este término nos estamos refiriendo que dicho firewall debe cumplir con todas las reglas y normas de bloqueos establecidas para su mejor funcionamiento.

- **Rendimiento:** El rendimiento representa el punto inicial de la evaluación. Al no haber métricas generalmente aceptadas por la industria para medir el rendimiento de los cortafuegos los administradores de redes que quieran saber la velocidad real la que trabajan no tendrán más remedio que instalarlos en la red, activarlos y aplicar las pruebas que considere imprescindibles para su entorno. Los cortafuegos son especialmente atractivos cuando el rendimiento es un factor clave, ya que permiten escalar actualizaciones sencillas, añadiendo mejoras en el sistema en una configuración.

- **Características:** es otro criterio de selección fundamental, ya que estos dispositivos implementan sus características de muy variadas formas, incluso las más simples como las de antivirus, Por ello un paso crítico antes de comprar es averiguar la cobertura exacta del producto y si tal cobertura cumple los requerimientos de nuestro entorno de red y sus perfiles de tráfico entonces estaremos eligiendo el adecuado.

- **Gestión:** La gestión es una de las áreas más difíciles de evaluar, porque no se llega a saber a fondo lo que un cortafuego ofrece al respecto hasta que no se lleva mucho tiempo trabajando con el, una de las características de gestión más importantes es su capacidad para poner en marcha las características UTM de un modo controlado y flexible.

- **Seguridad:** este punto es importante, porque todo aquel que tenga un firewall para proteger su red debe estableserce un usuario y una contraseña para que de esa manera pueda administrarlo.

Todos estos aspectos forman un conjunto muy importante para determinar en si cual cortafuego se asemeja o cumple con tus requisitos a la hora que quieras montar una red.

NECESIDAD DE LOS FIREWALLS.

En general, no lo serian si todos los sistemas de una organización estuviesen adecuadamente configurados, con adecuada protección en la seguridad punto a punto, los usuarios internos fuesen personas de

Confianza, respetuosas de las políticas de seguridad adoptada, escogieran contraseñas correctas, no ofrecieran servicios indebidos en las maquinas de su responsabilidad, si los productos de red ofrecieran solamente los servicios mínimos precisos y estos no vinieran por defecto configurados de manera que permitan realizar de todo a todos.

Los firewalls permiten obviar estas dificultades, las cuales son más difíciles de controlar cuanto mas grande es la red de una organización.

TIPOS DE FIREWALLS.

Antes de profundizar en los tipos de firewalls debemos conocer un poco acerca de la estructura de las capas del Modelo OSI y su relación con los firewalls.

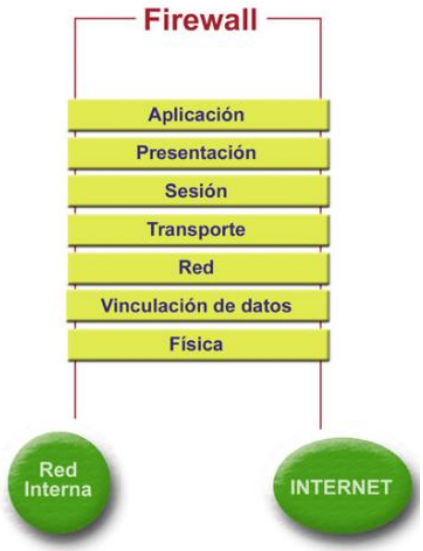
El modelo OSI es conocido porque ofrece una explicación sencilla de la relación entre los complejos componentes de hardware y de protocolo de red. En el modelo OSI, la capa inferior corresponde al hardware y las capas sucesivas al software que usa la red (Software de red)

Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente.

Un Firewall se conecta entre la red interna confiable y la red externa no confiable. Si no contamos con un Firewall, cada uno de los servidores de nuestro sistema se expone al ataque de otros servidores.

El sistema opera en las capas superiores del modelo OSI y tiene información sobre las funciones de la aplicación en la que basan sus decisiones. También opera en las capas de red y transporte, en cuyo caso, examina los encabezados IP y TCP (paquetes entrantes y salientes), y rechaza o acepta paquetes con base en reglas de filtración de paquetes programadas. Así, el Firewall actúa como el punto de cierre que monitorea y rechaza el tráfico en la red en el nivel de la aplicación.

Figura 2.



Existen en el mercado una gran cantidad de firewalls, que van desde los más simples a los más complejos según las características de cada uno, podemos catalogarlos, según su manera de operar, en dos grandes grupos: firewalls de nivel de red, y firewalls de nivel de aplicación.

FIREWALL DE NIVEL DE RED.

También se conocen como Packet-Filtering Gateways. Estos firewalls son los más económicos. Las capacidades de filtro suelen estar presentes en el software del router, y como probablemente vamos a necesitar un router para conectarnos a Internet no hay ningún coste adicional.

Los network firewalls operan despreciando paquetes en base a sus direcciones de origen o destino, o sus puertos. En general se carece de información de contexto, es decir que no posee demasiada información ya que son muy pocos los datos que se analizan y registran, las decisiones son tomadas sólo en base a la información del paquete en cuestión. En función del router, el filtrado se puede hacer a la entrada, a la salida o en ambos lados. El administrador realiza una lista de maquinas aceptables y servicios, y una lista de maquinas y servicios a negar.

El problema es que la mayoría de políticas de seguridad necesitan un control más fino que este. Se pueden definir reglas a este nivel, pero son tediosas, complejas y propensas al error. Aún con una perfecta implementación del filtro, nuestra red interna no estaría totalmente segura.

FIREWALL DE NIVEL DE APLICACIÓN.

Un firewall de nivel de aplicación representa el extremo opuesto en el diseño de un firewall. En vez de usar un mecanismo de propósito general donde para todos los paquetes se realiza la misma acción y así permitir diversos tipos de trafico, el código de propósito especifico puede utilizarse para cada aplicación deseada es decir que para cada paquete realice una operación determinada. Estos firewalls además poseen otra característica apreciada, pueden registrar (log) y controlar todo el trafico de entrada y salida.

Estos firewalls tienen la responsabilidad de tomar los paquetes de una red y llevarlos a otra, previamente abren el paquete, examinan el contenido, y se aseguran que no tiene ningún riesgo potencial. Una vez los paquetes están chequeados, y son seguros, el firewall construye unos nuevos con el mismo contenido.

Así pues solo los paquetes para los cuales hay un código de construcción pueden atravesar el firewall, no se pueden enviar paquetes no autorizados porque no hay código para generarlos.

El Firewall usa uno o más de tres métodos para controlar el tráfico en la red:

PACKET FILTER (FILTRADO DE PAQUETES)

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

1. Protocolos utilizados.
2. Dirección IP de origen y de destino.
3. Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al usuario y por cuales puertos.

Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

1. No protege las capas superiores a nivel OSI.
2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
3. No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
4. Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.

APPLICATION GATEWAY (PROXY-GATEWAYS DE APLICACIONES)

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

Gráficamente:

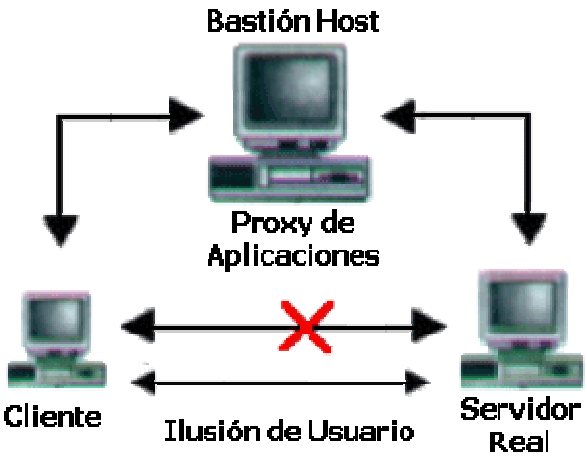


Figura 3.

CIRCUIT LEVEL GATEWAY

Trabajan a nivel de la capa de transporte creando un sistema cliente-servidor de pasarelas (proxies) que actúan filtrando paquetes por protocolos; establecen un control sobre el tráfico de cada protocolo y son específicos para cada uno de ellos, por lo que su eficacia queda disminuida. Comprueban que cada paquete está asociado a una conexión end-to-end

Se basan en el control de las conexiones TCP y actúan como si fuesen un cable de red: por un lado reciben las peticiones de conexión a un puerto TCP, y por otro, establecen la conexión con el destinatario deseado, si se han cumplido las restricciones establecidas, copiando los octetos de un puesto al otro.

Este tipo de firewall suelen trabajar conjuntamente con los servidores proxy, utilizados para la acreditación, es decir, comprobaciones sobre máquina fuente, máquina destino, puerto a utilizar. Una acreditación positiva, significa establecer la conexión.

Este sistema es un avance sobre el filtro de paquetes mencionado, la ventaja es que permite controlar las conexiones por puertos, pero la de gran desventaja de este tipo de sistema es que no verifica el contenido de aplicación de la comunicación.

STATE-FULL INSPECTION

Permite abrir "Puertas" a cierto tipo de tráfico basado en una conexión y volver a cerrar la puerta cuando la conexión termina. Adapta las reglas básicas de firewall para acomodarse a las necesidades específicas de cada protocolo. El Stateful Firewall mantiene un registro de las conexiones, las sesiones y su contexto. Este módulo tiene su asiento entre la capa de Data Link y Network.

Adicionar el seguimiento de estado (Stateful) a las conexiones incrementa la seguridad del filtrado básico pero no tiene nada que ver con el contenido del paquete o la implicación del tráfico.

Esto significa que una vez establecida una conexión válida se puede enviar cualquier tipo de tráfico y el firewall no se dará cuenta. Es decir se da entrada a un visitante, se conoce el visitante pero no se sabe que carga lleva o con que propósito entra.

La ventaja que provee es su alto rendimiento porque como opera solo a nivel de sesión y no de aplicación no tiene que inspeccionar todo el paquete de datos, y por lo tanto con poco hardware maneja un buen ancho de banda. La debilidad que posee es que no provee autenticación por usuario ni revisa toda la trama del paquete, solo los encabezados.

En resumen es la mejor opción de todas las anteriores, se caracteriza por controlar la comunicación desde la capa de red hasta la de aplicación, mantiene una tabla de estado de las conexiones TCP evitando así los ataques SYN y adicionalmente maneja las comunicaciones UDP con una tabla apropiada para este.

POLÌTICAS DEL FIREWALL.

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

- **Política restrictiva**: Se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

- **Política permisiva**: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

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

PROTECCIÒN QUE OFRECE UN FIREWALL.

El nivel de protección que puede darnos un firewall depende en gran medida, de nuestras necesidades. Generalmente, los cortafuegos se configuran para protegernos contra cualquier intento de acceso desautorizado o no correctamente autenticado desde el exterior hacia el interior de nuestra red, o viceversa.

Pero, adicionalmente, uno de los puntos más importantes a tener en cuenta es que un cortafuego nos proporciona un punto único e ineludible de acceso a nuestra red donde podemos centralizar las medidas de seguridad y auditorio sobre la misma.

Los firewall administran los accesos posibles del Internet a nuestro sistema. Sin un firewall, nos exponemos al ataque de otros en el Internet.

Algunas de las ventajas principales de contar con un firewall son:

- **Protege de intrusiones.** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet

- **Protección de información privada.** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios

- **Optimización de acceso.** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

LIMITACIONES DEL FIREWALL.

Son tres las principales amenazas sobre las cuales un Firewall no puede protegernos. Las dos primeras son evidentes.

Un firewall no puede protegernos contra amenazas que no pasan a través de el. Como decíamos anteriormente, el firewall debe de ser el punto único e ineludible de acceso a nuestra red. Si esto no es así su efectividad es sólo parcial.

Tampoco pueden protegernos, generalmente, contra amenazas que proceden del interior de nuestra red. Un empleado malicioso, un troyano o algunos tipos de virus pueden usar mecanismos para realizar acciones perniciosas.

Por último, los firewalls no pueden protegernos contra clientes o servicios que admitimos como válidos pero que son vulnerables. Tampoco puede protegernos contra mecanismos de tunneling sobre HTTP, SMTP u otros protocolos. No son muy efectivos, a pesar de que algunos fabricantes así lo anuncian, contra los virus.

Los firewalls no pueden ni deben sustituir otros mecanismos de seguridad que reconozcan la naturaleza y efectos de los datos y aplicaciones que se estén manejando y actúen en consecuencia.

Además:

Un Firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

No puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El cortafuego no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.

El cortafuego no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

No protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a Internet.

UTILIZACIÓN DEL FIREWALL.

La recomendación de utilizar un firewall hay que extenderla a cualquier tipo de sistema informático que tenga acceso a redes públicas como Internet, desde los que tienen un gran número de usuarios entrelazados por redes internas, hasta los sistemas domésticos compuestos por una sola máquina.

Las prestaciones del cortafuego dependen de las características de la red a proteger.

Las necesidades y recomendaciones relativas a la aplicación de cortafuegos a medianas y pequeñas empresas, dependen en gran medida del tamaño y estructura de su red interna, número de sistemas y componentes y en particular las necesidades de conexión de los usuarios internos a Internet y de usuarios externos a servicios de información de la empresa.

Dentro de esta diversidad, podríamos contemplar el caso de una pequeña empresa que depende en gran medida de su conexión con Internet para el desarrollo de sus actividades de negocio, y que por otra parte

Dispusiese de requisitos de protección muy exigentes relacionados con distintos activos de información.

SERVICIOS ADICIONALES PROPORCIONADOS POR LOS FIREWALLS.

Un valor añadido sobre los cortafuegos actuales son los servicios adicionales de que disponen y que facilitan las labores de protección y administración de la red. Se trata de servicios en algunos casos hechos a medida y en otros habituales de otros dispositivos pero que, en cualquier caso, representan un punto importante a la hora de decidirnos por una u otra implementación.

ALGUNOS DE ESTOS SERVICIOS SON:

Translación de Direcciones de Red (NAT)

Los servicios de NAT (*Network Address Translation*) resuelven dos de los principales problemas de seguridad e infraestructura de las redes actuales. En primer lugar, constituyen una herramienta muy efectiva para esconder las direcciones de red reales de nuestra red interna.

En segundo lugar, y debido a la reducción del espacio de direcciones IP disponibles, muchas organizaciones usan NAT para permitir la salida a Internet de sus equipos de la red interna con un mínimo de direcciones legalmente válidas (ver RFC 1918).

Protocolo de Configuración Dinámica de Hosts (DHCP).

DHCP, *Dynamic Host Configuration Protocol*, es un servicio de asignación automática de direcciones IP con importantes y evidentes ventajas administrativas a la hora de mantener redes de tamaño medio amplio que muchos Firewalls incluyen como valor añadido.

Inspección de Contenidos.

Es uno de los servicios adicionales más interesantes que ofrecen los Firewalls a Nivel de Aplicación: realizar una inspección de contenidos en el tráfico HTTP y SMTP incluyendo los siguientes elementos:

- Applets de Java
- Código ActiveX, JavaScript o CGI.
- Inspección de virus (binarios y de macro).
- Inspección del contenido de ciertos formatos ampliamente introducidos (.zip, .doc, .xls, .ppt, etc.)
- Bloqueo de contenidos en base a URL's, direcciones IP y/o palabras clave.
- Bloqueo de comandos específicos de determinadas aplicaciones.

Autenticación de Usuarios.

Otro servicio básico en los firewalls a nivel de aplicación es la autenticación de usuarios que en los dispositivos a nivel de red debe limitarse a la dirección IP de procedencia de la petición, con el consiguiente riesgo de suplantación, mientras que en estos pueden habilitarse servicios clásicos de combinación login / password.

Disponibilidad y Balanceo de Carga.

Como hemos visto en las descripciones anteriores, uno de los principales Inconvenientes de los firewalls es la disminución del rendimiento que provoca, efecto que se ve agravado en algunos esquemas más que en otros. Los firewalls empresariales de gama alta suelen ofrecer una solución para paliar este problema al mismo tiempo que ofrecen redundancia mediante el balanceo de carga entre dos o más dispositivos cortafuegos. Logramos, de esta forma, mejorar el problema del rendimiento y ofrecer alta disponibilidad y tolerancia a fallos en nuestra política de seguridad.

Integración con Sistemas de Detección de Intrusos (IDS's).

Los sistemas de detección de Intrusos son herramientas o dispositivos que nos permiten inspeccionar nuestro sistema y generar alertas que nos permitan conocer cuando alguien ha tratado de penetrar en nuestro sistema o lo ha conseguido.

Se trata de una tecnología relativamente nueva y en un grado aún bajo de madurez, pero que va ganando cada vez más importancia y mejores resultados. Existen dos tipos de sistemas IDS los de hosts y los de redes. Los de redes se subdividen, a su vez, en distribuidos o no. Los IDS de hosts se basan en el análisis de las estadísticas de uso o el uso indebido de ciertos recursos (comandos, archivos, etc.) del sistema.

Los IDS de red buscan patrones sospechosos en los paquetes TCP, malformaciones en la estructura de los mismos, etc. Se trata, pues, de *sniffers* que poseen tablas (actualizables) con los patrones característicos usados en los intentos de entrar en un sistema.

EL BLOQUEO DE UN PUERTO.

La comunicación que entra y sale de nuestra PC se hace a través de los Puertos. La información necesaria para navegar, efectuar alguna descarga, recibir correo e incluso ordenar a la impresora que realice cualquier impresión entra y sale por dichos puertos.

Las conexiones a nuestro ordenador se hacen a través de los puertos, un firewall cierra los puertos, esto es que ningún programa podrá enviar datos a través de ese puerto, ya que esta cerrado.

Tenemos gran cantidad de puertos, algunos para funciones específicas. Cuando nos conectamos, ignoramos que puertos tenemos abiertos, y cual es el tráfico de información a través de ellos. En esas condiciones, somos perfectos candidatos a sufrir un escaneo exterior, el cual pondría de manifiesto nuestros puertos abiertos, dando opción a que el intruso penetre en nuestro sistema a través de ellos.

Mediante el empleo del firewall podemos cerrar u ocultar nuestros puertos, evitando este tipo de intrusiones. También recibiremos un aviso cuando el firewall detecte algún tipo de escaneo o intento de intrusión, facilitándonos la IP del atacante y el puerto atacado.

SOFTWARE MÁS COMUNES EN EL MERCADO.

- Sygate Personal Firewall
- Private Firewall
- Sunbelt Kerio Personal Firewall
- Norton Personal Firewall
- Freedrom
- BlackIce
- Kerio Personal Firewall
- PERFirewall

- Kaspersky Internet Security
- Deelfield Personal Firewall
- Conseal PC Firewall
- Panda Internet Security
- McAfee Personal Firewall
- Black Ice
- Look 'n' Stop Lite
- McAfee Management Firewall
- eBox Platform (software libre)
- Zone Alarm
- Outpost Firewall
- Kaspersky Anti-Hacker

Sygate Personal Firewall: Pro Sygate Personal Firewall no es solamente un firewall de uso personal de múltiples características y muy fácil de manejar, sino también un completo sistema de seguridad para tu ordenador.

Private Firewall: es un cortafuego que nos ayuda a prevenir accesos no autorizados a nuestro PC, tanto en casa como en el trabajo o en el portátil. Este cortafuego monitoriza constantemente las áreas de nuestro PC donde más probabilidades hayan de sufrir una intrusión (opciones de seguridad del navegador, configuraciones de red, etc) y nos informa de su estado.

Sunbelt Kerio Personal Firewall: es un programa que te ayudará a controlar la seguridad en el intercambio de información mediante redes locales o Internet.

Norton Personal Firewall: es un firewall que incluye las herramientas necesarias para la protección contra virus, hackers y para la protección de los datos e información confidencial, así como el establecimiento de un control paterno de navegación por Internet para evitar que los niños accedan a contenido inadecuados.

Freedrom: Es uno de los mejores firewalls sino el mejor. Por lo único que se le puede achacar es su excesivo consumo de recursos. Es de los mejores que hay para quien desee proteger al máximo su navegación por Internet.

BlackIce: Este firewall de gran calidad tiene a su favor, consume muy pocos recursos es posiblemente el que mas flujo de datos puede controlar sin dejar pasar datos y darle tiempo a analizarlos.

Kerio Personal Firewall: Es un antivirus bueno, potente, no demasiado difícil de configurar, eficiente, y todo lo que se ocurra mas que decir a favor de este firewall. Es indudable su gran calidad y eficiencia. No consume muchos recursos y funciona muy bien.

PERFirewall: Establece una barrera entre la Web y tu PC que sólo podrán atravesar aquellas aplicaciones y servicios que permitas, previene de intrusiones maliciosas y ataques de hackers que intenten colarse vía TCP/UDP, IRC, P2P o cualquier otro medio que abra conexión.

Kaspersky Internet Security: (Antivirus y Firewall) integra otras funcionalidades potentes que complementan en gran medida la seguridad general, utilidades de control paternal, protección ante programas espías, ataques de hackers, robo de identidad y protección de clientes de mensajeria instantánea.

Zone Alarm: Este cortafuego controla cualquier acceso a tu ordenador y los programas que se están ejecutando en él, actualmente podemos decir que es el arma más efectiva para evitar intrusos y virus. Una utilidad imprescindible si utilizas Internet.

Outpost Firewall: Es un cortafuego que esta diseñado para proteger tu red contra los ataques maliciosos, virus, hacker y otros que intenten violar tu privacidad de tu red.

Kaspersky Anti-Hacker: Es un firewall personal diseñado para proteger un equipo con el sistema operativo Windows. Protege el equipo contra el acceso no autorizado a los datos y los intentos de intrusión desde Internet o una red local vecina.

REQUISITOS HARDWARE Y SOFTWARE DEL SISTEMA PARA INSTALAR ZONE ALARM.

Requisitos mínimos:

- Uno de los siguientes sistemas operativos y la memoria RAM mínima necesaria:
- Microsoft® Windows® XP, Home o Professional Edition, 128 MB de RAM.

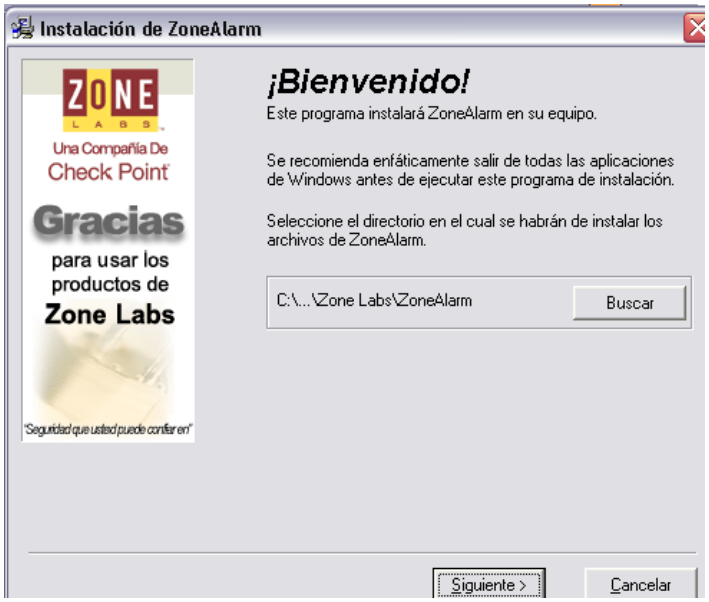
- Microsoft Windows 2000 Professional, 64 MB de RAM
- 50 MB de espacio libre disponible en disco duro
- Pentium® III 450Mhz o superior

INSTALACIÓN DE ZONE ALARM.

Zone alarm es el firewall por excelencia según los usuarios. Ocupa muy poco espacio, unos 3 MBytes y la instalación es rápida y fácil, además de gratuita. Una vez instalado se queda residente en memoria y se encargará de vigilar constantemente mientras estemos conectados a internet.

Los pasos para instalar Zone alarm son los siguientes:

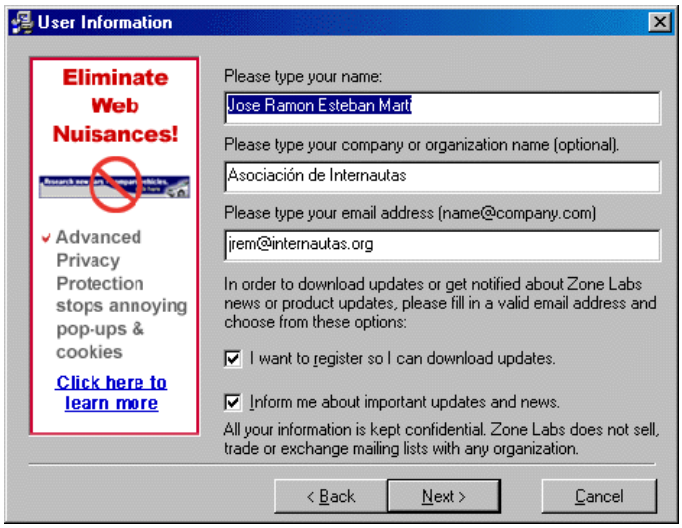
Lo primero es una pantalla de bienvenida y advertirnos que es mejor cerrar cualquier programa que este corriendo mientras hacemos la instalación **siguiente.**



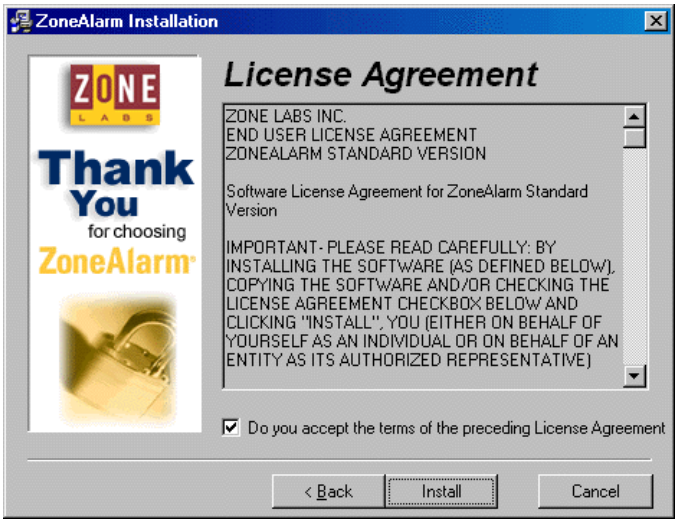
Podemos elegir donde queremos instalarlo pulsando sobre **Browse** y dándole su respectiva direccion, posteriormente Pulsar **Next**

Con este cuadro estamos restableciendo registros de Internet, es decir damos la opción instalación nueva, esto permite una instalación sin complicaciones **siguiente.**

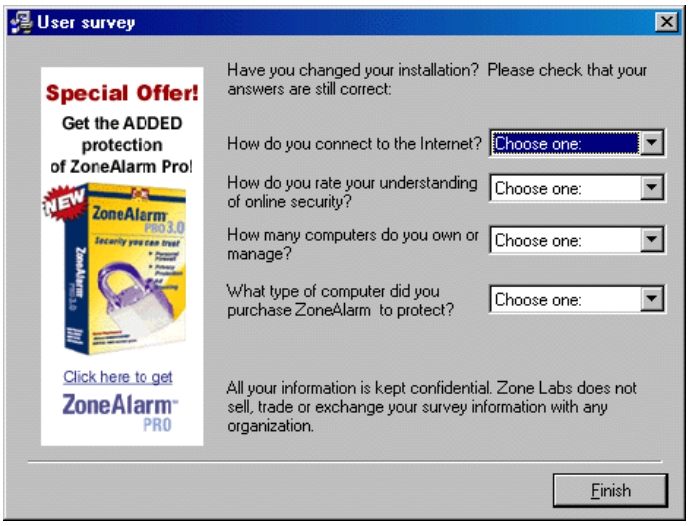
Esta pantalla que viene a continuación nos pide si queremos registrarnos es decir nuestro nombre, empresa y direccion de correo electrónico esto es opcional. Además es recomendable marcar la opción, "**I want to register ZoneAlarm so I can recibe updates**" (Quiero registrar ZoneAlarm ytambién recibir actualizaciones). De esta forma cuando haya nuevas actualizaciones las podremos descargar; esto es importante ya que así tendremos el programa actualizado con las mejoras que se introduzcan y continuamos dando **Next.**



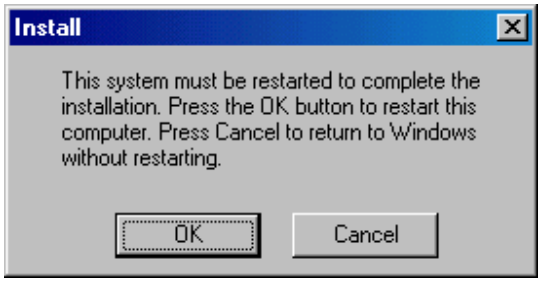
La siguiente pantalla nos habla de las condiciones de la licencia. EL uso personal es gratuito. Pulsar **Install.**



Luego nos pide información sobre como conectarnos a Internet. Respondemos eligiendo una de cada opción y pulsamos **Finish**



Ahora el programa se instalará. Una vez finalizada ésta operación nos pedirá que reiniciemos el sistema Pulsar **OK**



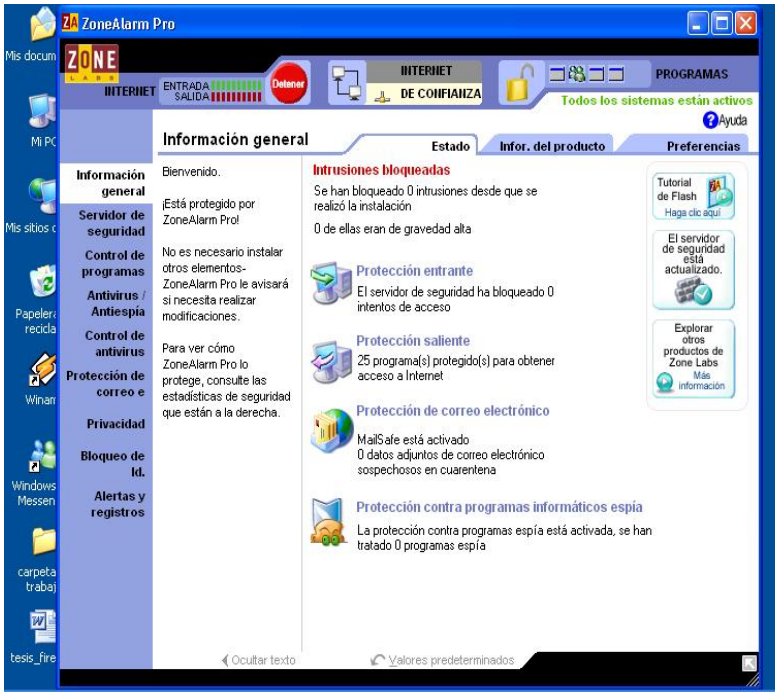
Una vez instalado el firewall y reiniciada nuestra pc, este nos envía un mensaje donde nos indica que ha encontrado una red y nos pide el nivel de seguridad que queremos para dicha red, marcando el nivel: **permitir acceso a zona de confianza.**

Ya que hemos elegido el nivel de seguridad para la red el firewall, ya esta listo para hacer su trabajo.

El diseño de la interfaz es muy agradable y simple a la vez y manejarse en él es muy fácil.

En la pantalla principal se nos muestra las alertas que hemos recibido y la cantidad de información que nos hemos descargado durante nuestra sesión.

Si alguien intenta acceder a nuestro ordenador inmediatamente sale un mensaje explicando que ha sufrido un ataque y ha sido bloqueado, además indica también la dirección IP del atacante.



En el panel de Bloqueo (Locks) podemos bloquear el acceso a internet, para que nadie pueda usarlo sin nuestro permiso.

El siguiente apartado es el de Seguridad (security) y en él elegiremos qué modo de protección queremos: alto, medio y bajo nivel de seguridad, tanto para acceder a internet, como para redes locales. Se recomienda usar el modo de alta seguridad, aunque es un poco molesto a veces, pero más vale prevenir que curar.

Se puede configurar los programas que acceden a Internet (explorer, IRC, antivirus). Si un programa que no esté en la lista intenta acceder a internet se nos comunicará y podemos añadirlo a la lista, para que no de más avisos. Podemos bloquear ciertos programas y desbloquearlo a nuestro antojo y muy fácilmente.

La última pestaña del programa hace referencia a la configuración, tanto del programa como de sus actualizaciones, es recomendable dejar la opción automática ya que de esta manera este mismo se actualiza sin estar pendiente del mismo.

CARACTERÍSTICAS DEL ZONE ALARM.

Es un software cómodo y sencillo, con mucha información en pantalla sobre las distintas opciones y consejos para la configuración.

El diseño de la interfaz es agradable, simple y manejarse en él es muy fácil ocupa poco espacio en memoria, aproximadamente 3 mb y la instalación es rápida y fácil, además de gratuita. Una vez instalado se queda residente en memoria y se encargará de vigilar constantemente mientras estamos conectados a Internet.

Cuando se instala el programa pregunta que como valoramos nuestros conocimientos de internet, y en función a eso, permitiremos que Zone Alarm haga más cosas por su cuenta.

Una característica formidable de este programa es que te hace invisible en internet, si alguien hace una petición a tu pc sea esta de cualquier índole, si tu no has configurado el firewall para responder a esa petición, esa persona o maquina que te solicita la petición no recibirá respuesta, es como si tu pc estuviera apagado.

También si un programa en la pc intenta conectarse a la red, el programa te avisa de la siguiente manera *¿quiere permitir que" nombre del programa" acceda a Internet)* junto con la información técnica de dicho programa, la ip a la que accede, el puerto, el nombre de la aplicación y su versión.

Disponemos de la opción de negar su acceso o permitirlo pulsando **"Yes"** o **"No"**, esto es muy útil ya que cuando estamos navegando y al entrar en algunas paginas estas descargan en nuestra pc programas que se llaman spyware, que una vez instalado intentan conectarse a la red, y envía

Información personal sin ningún control y sin nuestro conocimiento. Esto resulta tedioso ya que las alertas son constantes y debemos de elegir la acción a tomar respecto a dicha alerta y por ende resulta incomodo estar analizando las alertas y la acción a tomar.

Consume recursos, se refiere a la parte del antivirus que incorpora, porque el filtrado de paquetes es inapreciable. La solución para maquinas poco potentes es desactivar el modulo antivirus ya que Cuando la pc está prendida un largo tiempo el proceso vsmon.exe incrementa los recursos de memoria consumidos hasta valores insospechados.

Originalmente consume aproximadamente 1 mb de ram y a medida que pasa el tiempo el mismo llega a consumir 35 mb o más. Obviamente la pc disminuye el rendimiento considerablemente.

El objetivo principal de este proceso es de controlar todo ese tráfico para asegurarse de que no hay ataques ni acciones malas que puedan dañar nuestra red, por eso, cuantas más conexiones se tengan, más trabajo debe realizar y más recursos consumes. Siempre en la información de las alertas veremos el protocolo, la ip y el puerto de la maquina que ha intentado acceder a nuestro sistema.

El servidor de seguridad te protege contra el tráfico peligroso, este tiene dos zonas muy importantes estas son:

Zona de Internet: esta es para protección desde equipos desconocidos contiene a todos los equipos en la Web de forma predeterminada.

Zona de confianza: para compartir con equipos de confianza

Presenta ciertas técnicas empleadas para la seguridad.

- **Alto o modo silencioso:** el equipo esta oculto y protegido contra los piratas informáticos, no se permite compartir recurso, se recomienda esta configuración solo para la zona de Internet.

- **Medio o modo visible:** pero protege equipos; pueden ver el suyo sin compartir sus recursos. NetBIOS entrante esta bloqueado. Es recomendable esta configuración para uso temporal.

- **Bajo:** advertencia el servidor de seguridad esta desactivado.

En esta prueba se empleo la técnica **Medio,** ya que el ordenador forma parte de una red colocándose de esta forma se podrá compartir impresoras u otros ordenadores conectados a Internet.

En caso que el ordenador no estuviese conectado a una red se toma **Alto,** puesto que éste bloquea cualquier intento de acceder a la pc.

Otra opción muy importante que presenta este firewall es la parte de **opciones avanzadas** aquí permite que configuremos los distintos puertos, es decir permite: bloquear servidores de la zona de confianza, de la zona de Internet, archivos host, permitir protocolos pocos frecuente con seguridad alta y los DNS/DHCP salientes.

REQUISITOS HARDWARE Y SOFTWARE DEL SISTEMA PARA INSTALAR OUTPOST FIREWALL.

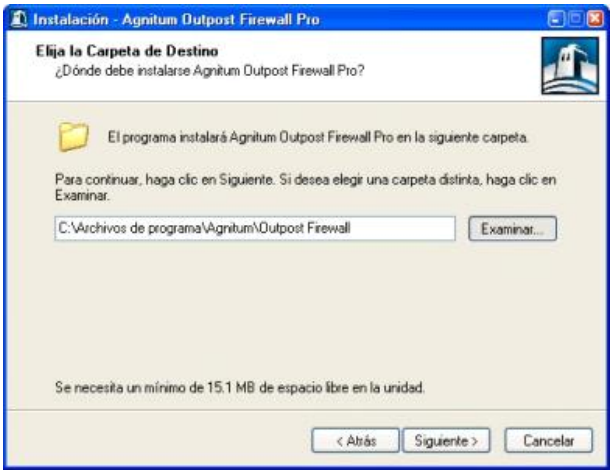
Procesador de 450 MHz o superior (x-86, x-64 o multinúcleo) 256 MB de memoria RAM Bajo un sistema operativo Microsoft Windows Vista, XP, Server 2003 o 2000 SP3 o superior, en sus versiones de 32 bits o de 64 bits.

Instalación de Outpost Firewall.

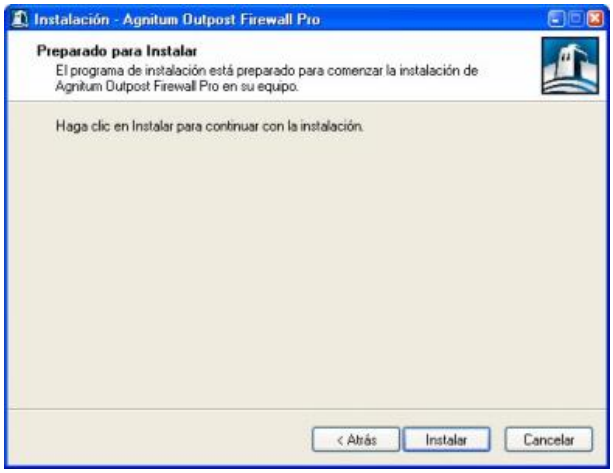
Comenzará el asistente de instalación y deberemos optar entre instalar en el idioma español o inglés luego le damos **Aceptar.**

Luego una ventana de bienvenida nos dará indicaciones de tipo general, es decir que seremos cualquier otro programa que tengamos abierto para no perder dicha información, **Siguiente**

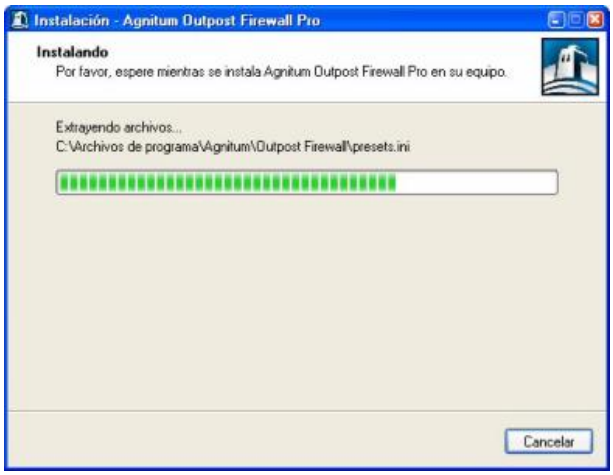
Si está instalando Outpost Firewall por primera vez, le solicitará que confirme la carpeta de instalación esto lo hacemos en Examinar y luego le damos la direccion correspondiente, posteriormente **Siguiente**.



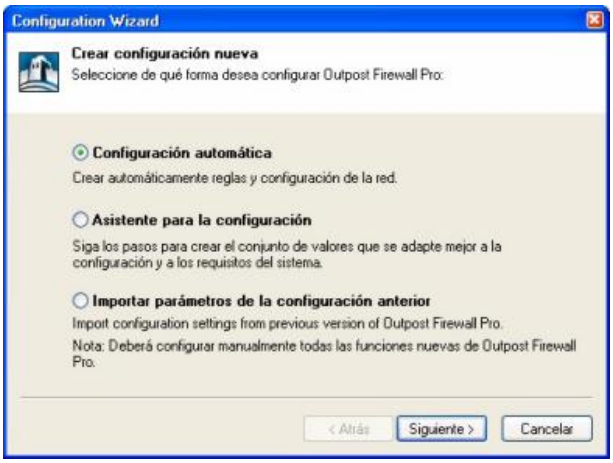
Una vez completada la configuración de parámetros necesarios, Outpost Firewall será instalado en su sistema.



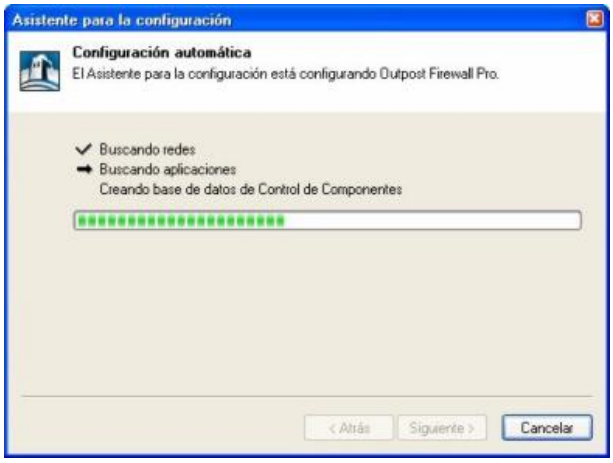
Los archivos necesarios para el funcionamiento de Outpost Firewall son copiados a nuestro disco duro y es modificado el sistema.



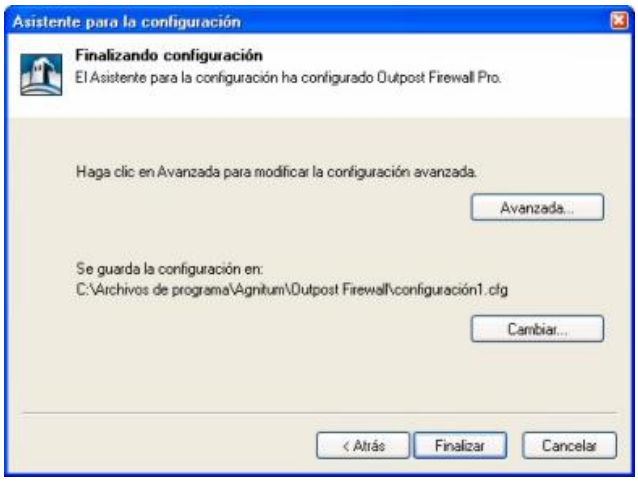
Seleccionamos la opción que mejor se adecue a nuestros conocimientos, preferencias y entorno de trabajo y pulse en el botón **Siguiente** para continuar o en el botón **Cancelar** para abortar esta parte del proceso.



El Asistente para la configuración automática buscará elementos de red instalados.



El siguiente paso es modificar las opciones avanzadas de configuración y la ubicación donde se guardará el archivo que contiene todos los parámetros establecidos para el funcionamiento de Outpost Firewall.



CARACTERÍSTICAS DEL OUTPOST FIREWALL.

Es un firewall por excelencia según los usuarios, diseñado para proteger tu red contra los ataques maliciosos, virus, hacker y otros que intente viola la privacidad de la red.

La instalación de este firewall es muy sencilla siguiente, siguiente, siguiente y configurar un par de normas que fueron explicada en la parte de la instalación.

Al principio se hace un poco complicado, pues el firewall, no viene con unas normas configuradas, a no ser que se la apliques, sino en unos segundos habremos perdido contacto con Internet. ¿Como se arregla?, tiene un sitio en opciones ->aplicación donde nosotros elegimos que programas queremos que accedan a Internet y a cuales no les das permiso, y volvemos a tener Internet.

Este firewall para funcionar tiene 3 modos básicos:

1. **Permisivo**: permite la mayoría del tráfico entrante, desaconsejado a no ser que el usuario sea experto en informática y confíe mucho en la seguridad de Windows.

2. **Aprendizaje**: cuando un programa desea conectar este pregunta y da varias opciones, bloquear, permitir, o usar reglas

predeterminadas,aparte si un mismo programa, quiere conectar por algún otro puerto, que el firewall cree que no es normal en el funcionamiento del programa, te avisa y te pide que quieres hacer bloquear o permitir. Este es el que creemos que se debe usar normalmente.

3. **Restrictivo:** aquí es cuando creemos estar en peligro por un ataque masivo, ponemos este modo, y así aumentamos el nivel de seguridad.

Cuando abrimos el programa, vemos que programas están usando la red, en cuanto a los puertos tenemos una pestaña inmediatamente abajo, que nos dice cuantos programas tienen un puerto abierto, estos pueden ser:

Puerto 80: este es el del servidor Web
Puerto 25: este es el de los correos electrónicos
Puerto 22: ssh protocolo y programa que sirve para acceder a maquinas remotas a través de una red entre otros
Puerto 21: para FTP
Puerto23: telnet
Puerto 3128: servidor intermediario
Puerto 143: para la red de acceso a mensajes electrónicos almacenado en un servidor.

Estos puertos pueden variar, todo depende de los programas que quieran acceder a la red.

Después podremos ver todas las estadísticas de tráfico permitido y tráfico bloqueado.

Además este firewall es el primero en usar una tecnología basada en plug-ins. Incluye plug-ins:

- Examinador de adjuntos, por si los E-mail pueden tener virus.
- Bloqueador de contenido, por si quieres prohibir webs XXX u otro contenido.
- Cache de DNS para no pedir todo el rato la ip de cierto sitio
- Contenido activo, para evitar active-X maliciosos, o sea virus al visitar webs.
- Detección de ataques, escaneos de puertos, intentos de intrusión.

Publicidad, para bloquear pop-ups y anuncios ya que como todos habremos comprobado en innumerables ocasiones los banners y anuncios disminuyen mucho la velocidad de las conexiones. Todas estas opciones guardan logs detallados sobre las intrusiones y ataques.

Otro punto a favor de este programa es que podemos instalarlo en el idioma que más nos convenga, en español por ejemplo, lo cual unido a su sencillo manejo permite que estemos seguros en la red.

REQUISITOS HARDWARE Y SOFTWARE DEL SISTEMA PARA INSTALAR KASPERSKY ANTI-HACKER.

Para poder ejecutar **Kaspersky Anti-Hacker** sin problemas, su sistema debe cumplir con los requisitos hardware y software siguientes

Requisitos generales:

• Equipo con Microsoft Windows 98/ME/NT 4.0/2000/XP instalado

• Para instalar bajo Microsoft Windows NT 4.0/2000/XP, necesita derechos de administrador

• Soporte para el protocolo TCP/IP

• Red local (Ethernet) o conexión por modem (estándar o ADSL)

• Microsoft Internet Explorer 5.0 o superior

• Al menos 50 MB de espacio libre para los archivos de programa y espacio adicional para los informes de actividad.

• Para ejecutar el programa bajo Windows® 98/Me/NT 4.0, necesita:

• Procesador Intel Pentium® de 133MHz o superior bajo Windows 98 o Windows NT 4.0

• Procesador Intel Pentium® de 150MHz o superior bajo Windows Instalación y desinstalación del software 11

• 32 MB RAM

• Servicio Pack v. 6.0 o superior para Windows NT 4.0 Workstation

• Para ejecutar el programa bajo Windows 2000, necesita:

• Procesador Intel Pentium® de 133MHz o superior
• 64 MB RAM

• Para ejecutar el programa bajo Windows XP, necesita:

• Procesador Intel Pentium® de 300MHz o superior
• 128 MB RAM .

Instalación de Kaspersky Anti-Hacker firewall.

Para la instalación del programa ejecutamos setup.exe desde el CD o desde la memoria flash el asistente de instalación funciona de manera interactivo, cada cuadro de dialogo contiene un conjunto de botones que permite controlar la instalación. Estos botones principales son los siguientes: **Aceptar, Cancelar, Siguiente y Anterior**.

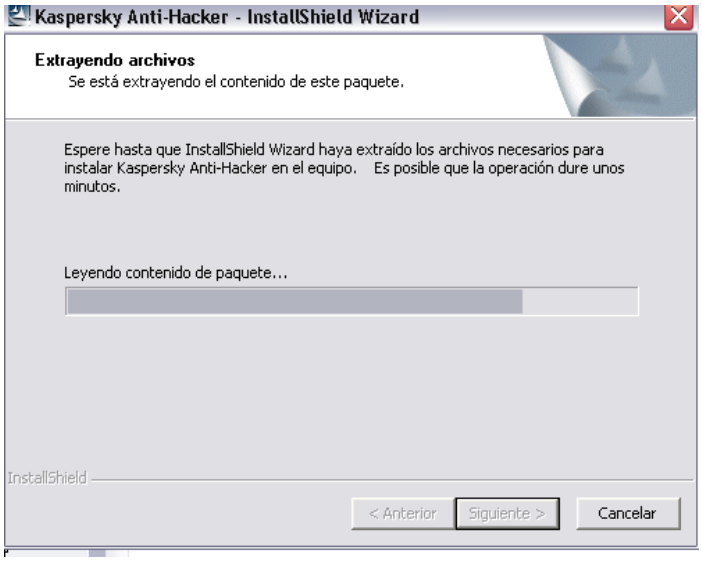
Inmediatamente después de hacer clic en el archivo setup.exe se muestra el primer cuadro de diálogo dando la bienvenida al inicio del asistente de instalación de Kaspersky Anti-Hacker Para continuar con la instalación, haga clic en **Siguiente>**. Haga clic en **Cancelar** si desea cancelar la instalación.

Esta etapa le sirve a Kaspersky Anti-Hacker para determinar en qué carpeta se instalará el programa. La ruta predeterminada es **C:\lab\KasperskyAnti-Hacker\spanish.**

Para modificar la ruta predeterminada, haga clic en **cambiar**, elija una nueva carpeta de instalación en el cuadro de diálogo de selección y haga clic en **Siguiente>**.

A continuación, los archivos de programa de Kaspersky Anti-Hacker se copiarán a su equipo.

El siguiente cuadro de diálogo se encarga de extraer archivos necesarios a su disco duro para instalar dicho firewall.



En este siguiente cuadro nos encontramos con el asistente de instalación de kaspersky este nos guiara durante la instalación del mismo se recomienda cerrar todas las demás aplicaciones antes de la instalación, y posteriormente le damos **siguiente**.

El cuadro de diálogo siguiente del asistente para la instalación contiene el texto del contrato de licencia entre el usuario Kaspersky Léalo con atención y haga clic en **aceptar** si está de acuerdo con sus términos.

Esta etapa de la instalación del programa permite introducir su nombre de usuario y el nombre de su organización.

El asistente para la instalación recupera la información predeterminada en el Registro del sistema operativo. Puede modificar esta información. Haga clic en **Siguiente>** para continuar con el proceso de instalación.

El cuadro de dialogo siguiente nos pide que leamos con mucha atención las características del firewall kaspersky antes de proseguir con su instalación y nuevamente le damos **siguiente.**

Esta etapa permite instalar la llave de licencia de Kaspersky Anti-Hacker. La llave de licencia es su "llave" personal, que almacena información sobre los servicios necesarios para un funcionamiento

Adecuado del programa, el nombre, número y fecha de vencimiento de la licencia.

Especifique el archivo llave en el cuadro de diálogo estándar de Windows Seleccionar archivo y haga clic en **Siguiente >** para continuar con la instalación.

Esta etapa le sirve a Kaspersky Anti-Hacker para determinar en qué carpeta se instalará el programa.

La ruta predeterminada es: **Archivos de programa\Kaspersky Lab\Kaspersky Anti-Hacker**.

Para modificar la ruta predeterminada, haga clic en **Examinar**, elija una nueva carpeta de instalación en el cuadro de diálogo estándar de selección y haga clic en **instalar>**. A continuación, los archivos de programa de Kaspersky Anti-Hacker se copiarán a su equipo.

Instalando kaspersky, es decir se están copiando todos los archivos al disco duro.

Completando el asistente para la instalación contiene explicaciones sobre el fin de la instalación de Kaspersky Anti-Hacker.

Si el sistema necesita registrar algunos servicios antes de terminar la instalación, le invita a reiniciar el equipo. Es una etapa necesaria para poder completar la instalación del producto y finalmente le damos la opción terminar. Con esto hemos concluido la instalación de nuestro firewall.

CARACTERÍSTICAS DEL FIREWALL KASPERSKY ANTI-HACKER.

Es un cortafuego diseñado para proteger un equipo con el sistema operativo Windows. Protege contra el acceso no autorizado a los datos y los intentos de intrusión desde Internet a una red.

Es similar a los otros siempre con algunas diferencias, en cuanto a configuración se refiere, con respecto a la instalación siempre nos guiamos con los botones principales. Aceptar,

Cancelar, siguiente y anterior. También esta en nuestra mano establecer cambios en cuanto a configurar reglas de filtrado de paquetes adecuadas y todo lo que nosotros queremos que salga de nuestra red.

Una de las principales características de este firewall es que Supervisa la actividad de la red TCP/IP de todas las aplicaciones que se ejecutan en su equipo.

Si detecta cualquier acción sospechosa o alguien intenta transmitir cualquier dato de su equipo, Kaspersky Anti-Hacker bloquea el acceso a Internet de este software dañino, y nos manda un mensaje informando de lo sucedido.

Impide los ataques Dos (por denegación de servicio) de todo tipo, Bloquea los ataques de red más comunes mediante un filtro permanente del tráfico entrante y saliente, también informa al usuario de estos ataques.

Mira los intentos de exploración de sus puertos (que suelen anunciar ataques) y prohíbe cualquier intento de comunicación posterior con el quipo atacante.

Permite examinar la lista de todas las conexiones de red establecidas los puertos abiertos así como las aplicaciones de red activas necesario interrumpe las conexiones no deseadas, protege su equipo contra intentos de intrusión, sin otra configuración especial del programa.

Existen dos tipos de operaciones de red que están sujeto con este firewalls:

- **Operaciones a nivel de aplicación** (nivel superior). En este nivel, Kaspersky Anti-Hacker analiza la actividad de las aplicaciones de red, como navegadores Web, programas de correo, de transferencia de archivos y otros.

- **Operaciones a nivel de paquete** (nivel inferior). En este nivel, Kaspersky Anti-Hacker analiza los paquetes de datos enviados o recibidos por la tarjeta de red o el MODEM.

Este firewall tiene cinco niveles de seguridad muy importante esto son:

1. **Autorizar todo**: desactiva el sistema de seguridad en su equipo. Con este nivel de seguridad seleccionado, cualquier actividad de red está autorizada en su equipo.

2. **Autorizar todo**: autoriza la actividad de todas las aplicaciones, salvo aquellas explícitamente prohibidas por reglas de aplicación personalizadas.

3. **Medio**: informa de los eventos de red relacionados con sus Aplicaciones y le permite configurar su sistema de seguridad par un Funcionamiento optimizado.

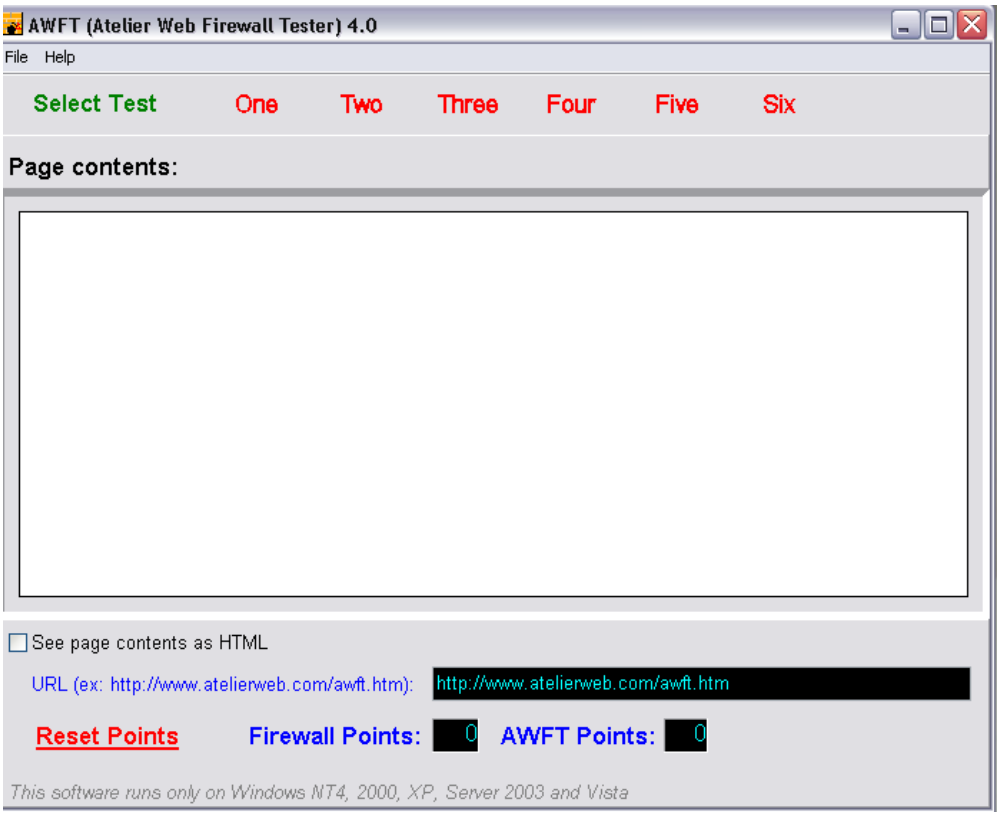
4. **Máximo**: prohíbe la actividad de todas las aplicaciones, acepto aquellas explícitamente autorizadas por reglas de aplicación personalizadas. Cuando activa este nivel de seguridad, no se muestra el cuadro de diálogo de aprendizaje y se bloquea cualquier intento de conexión no previsto en las reglas del usuario.

5. Bloquear todo: prohíbe a su equipo tener acceso a Internet o a la red local. Este nivel crea una situación en la que todos los intentos de Conexión por Internet o por la red local son bloqueados, como si su equipo se encontrara físicamente desconectado.

ATELIER WEB FIREWALL TESTER (TES DE PRUEBA)

La mayoría de los cortafuegos (Firewall) suelen ser bastante fiables, pero no es aconsejable fiarse ciegamente de que funcionan perfectamente. Para ello surge esta aplicación, para verificar y poner a prueba los niveles de seguridad del firewall de los ataques de Internet.

De esta forma se presenta el siguiente Tes que le ayudará a ajustar su Firewall personal para una mayor protección, o para elegir racionalmente un cortafuego entre las alternativas disponibles en el mercado.



Atelier Web Firewall Tester (AWFT) Es una herramienta para probar las fortalezas del programa cortafuegos de uso personal contra intentos de penetración de caballos de troya, programas espía o programas mal intencionado.

El Tes. AWFT se basa en un conjunto de seis pruebas en un solo programa, muy compleja, que combina múltiples técnicas diseñadas para atravesar cortafuegos: inyección directa de procesos en la memoria de una aplicación confiable, ejecución del navegador predeterminado modificación de su bloque de memoria, creación de hilos adicionales en el espacio de memoria de procesos legítimos, entre otras.

A medida que el cortafuego va superando las pruebas, AFWT le otorga un puntaje acumulativo, con un máximo de 10 puntos, estas son:

- **One** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución.

- **Two** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución.

- **Three** Crea una instancia de ejecución en el Explorador de Windows pretendiendo acceder a la red.

- **Four** Intenta cargar el navegador predeterminado utilizando el Explorador de Windows y modificándolo en memoria antes de su posterior ejecución. Esta prueba generalmente derrota a los cortafuegos que requieren la autorización para que una aplicación pueda ejecutar otra ya que el Explorador de Windows es normalmente autorizado.

- **Five** AWFT efectúa una búsqueda heurística de servidores Proxy y otros programas autorizados a acceder a Internet mediante el puerto 80, cargando una copia en memoria y modificándola antes de su ejecución a través de una instancia del Explorador de Windows.

- **Six** AWFT efectúa una búsqueda heurística de servidores Proxy y otros programas autorizados a acceder a Internet mediante el puerto 80, cargando una copia en memoria y modificándola antes de su ejecución a través de una instancia del Explorador de Windows.

IPTABLES.

Iptables es la herramienta que nos permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux, desde su versión 2.4 (en 2.2 era ipchains). Con esta herramienta, podremos crearnos un firewall adaptado a nuestras necesidades.

Su funcionamiento es simple, a iptables se le proporcionan unas reglas, especificando cada una de ellas unas determinadas características que debe cumplir un paquete. Además, se especifica para esa regla una acción o target. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en los que se denominan targets, que indican lo que se debe hacer con el paquete.

Los más usados son bastante explícitos: ACCEPT, DROP y REJECT, pero también hay otros que nos permiten funcionalidades añadidas y algunas veces interesantes: LOG, MIRROR.

En cuanto a los paquetes, el total del sistema de filtrado de paquetes del kernel se divide en tres tablas, cada una con varias chains a las que puede pertenecer un paquete, de la siguiente manera.

- **tabla FILTER:** usado para implementar el firewall. Aquí se produce el filtrado de paquetes.
- **tabla NAT:**(masquerading) para hacer que otros ordenadores se conecten a través del nuestro a una serie de servicios pero con nuestra ip**,** pareciendo que esas conexiones vienen de nuestro equipo.
- **tabla MANGLE**: sirve para alterar el estado de un paquete**.**

Tenemos dentro de la tabla FILTER:

- **INPUT:** todo el tráfico entrante
- **OUTPUT:** todo el tráfico saliente
- **FORWARDING:** para enrutar tráfico a través de nuestro ordenador hacia otro ordenador. Se supone que este tráfico no es para nosotros

Dentro de la tabla NAT tenemos:

- **PREROUTING:** para alterar el tráfico así como llegue a nosotros.

- **POSTROUTING:** para alterar paquetes generados localmente antes de enrutarlos.

- **OUTPUT:** alterar paquetes justo antes de que salgan si

Además tenemos el módulo ipt_conntrack disponible, dispondremos de herramientas para controlar el estado de la conexión**.** Podemos añadir entonces:

- **NEW:** nuevo paquete que viene hacia nosotros
- **RELATED:** paquetes nuevos pero que ya están relacionados con una conexión existente.

Ejemplo**:** cuando usamos un ftp se abren varias conexiones para poder bajar correctamente lo que necesitamos. Si no lo activamos, sólo sería posible la primera conexión y los demás paquetes, aunque

Relacionados con la primera conexión, no se dejarían pasar y la transferencia se interrumpirá.

- **ESTABLISHED:** paquetes asociados a una conexión nueva
- **INVALID**: todos los demás paquetes, que no coincidan con ninguno de los estados descritos

El comando a grandes rasgos quedaría asi:

Iptables <ubicación> <especificación> <acción>

Algunas ordenes básicas:

- **Iptables -F (- - flush):** borra todas las reglas de una cadena.
  Ejemplo: iptables –F INPUT

- **Iptables -L (- -list):** listado de reglas que se están aplicando
  Ejemplo: iptables –L INPUT.

- **Iptables -D(--delete):** borrar una regla
  Ejemplo: iptables –D INPUT –d port 80 –j DROP

- **Iptables –Z(--zero):** pone en cero todos los contadores de una determinada cadena
  Ejemplo: iptables –Z INPUT

- **Iptables –N (-- new-chain):** permite al usuario crear su propia cadena
  Ejemplo: iptables –N allowed

- **Iptables –X (- -delete-chain):** borra la cadena especificada. Si se escribe -X, borrará todas las cadenas creadas en esa tabla.
  Ejemplo: iptables –X allowed

- **Iptables –P (- - policy):** explicita al Kernel que hacer con los paquetes que no coinciden con ninguna regla.
  Ejemplo: iptables –P INPUT DROP

- **Iptables –E(- - rename-chain):** cambia el nombre de una cadena.
  Ejemplo: iptables –E allowed disallowed.

- **-R(--replace) «cadena» «pos»**

  Reemplaza la regla en la posición «pos» de la cadena «cadena», se le pasa como argumento el número de línea dentro de la caneda y la nueva regla.
  Ejemplo: iptables –R INPUT 1 –s 192.168.0.1 –j DROP

Para determinar la ubicación de la regla que se esta agregando se utilizan las siguientes opciones:

- **-t «tabla»**
  Indica en qué tabla se va a ubicar la reglas

- **-A «cadena»**
  Agrega una regla al final de la lista de reglas de la «cadena»
  Ejemplo: iptables –A INPUT.

- **-I «cadena» [pos]**
  Inserta una regla dentro de la cadena «cadena» en la posición [pos]

  Ejemplo: iptables –I INPUT1 –dport 80 –j ACCEPT

Para determinar la especificación del paquete se utilizan estas opciones generalmente:

- **-s «dirección»**
  Indica que el paquete proviene de la dirección «dirección» (se pueden usar prefijos para especificar un rango de IPs o un único número de IP), si se le agrega un! se niega la opción.
  Ej:-A INPUT -s 192.168.1.0/24

- **-d «dirección»**
  Indica que el paquete va destinado a la dirección «dirección».
  Ej: iptables –A INPUT -d 84.56.73.3

- **-i «interfase»**
  Indica la interfase de entrada (en la especificación de interfases se puede utilizar el símbolo ``+'' como metacaracter, por ejemplo ``eth+'' que contempla eth0, eth1, eth2, etc.)
  Ej: iptables –A INPUT –I eth0

- **-o «interfase»**
  Indica la interfase de salida
  Ej: iptables –A FORWARD –o eth0

- **-p «protocolo»**
  Indica el protocolo del paquete (los más comunes son ``tcp'', ``udp'', ``icmp'', pero hay muchos tipos de protocolos soportados).
  Ej: -A INPUT -p TCP

- **-f**
  Permite seleccionar las segundas o terceras partes de paquetes fragmentos. Estos paquetes son peligrosos. Como nuestro interes es determinar la primera parte podemos usar esta opcion asi: iptables –A INPUT! –f.
  Ej: iptables –A INPUT! f.

- **--dport «puerto»**
  Indica el número de puerto destino
  Ej: iptables –A INPUT –p tcp - -dport 22

- **--sport «puerto»**
  Indica el número de puerto origen.
  Ej: iptables –A INPUT –p tcp - - sport 22
  --source-port 22:80
  --source-port: 80 (Puerto 0 a 80)
  --source-port ! 6:1024 (todos los puertos menos el rango de 6 a 1024)

Para determinar la acción de la regla se utiliza una única opción:

- **-j «acción o cadena»**
  Con esta opción le indicamos que cuando un paquete coincida con las características expresadas en la regla, se deberá toma la acción «acción» o saltar a la cadena «cadena».

  Dependiendo la acción el kernel dejará de verificar las subsiguientes reglas o no.
  Ej: iptables –D INPUT –d port 80 –j DROP

  Otras opciones útiles:

- **-nL**
  Lista todas las reglas de la tabla indicada con -t «tabla»

- **--line-numbers**
  Indica que en el listado se agreguen los números de regla (delante de cada una de ellas)

Notas:

- **-i** se usa con reglas INPUT y FORWARD
- **-o** se usa con reglas FORWARD y OUTPUT

Ejemplo de una regla

#Aceptar conexiones al puerto 80 (www) en la tarjeta eth0

- iptables -A INPUT -i eth0 -s 0.0.0.0/0 -p TCP --dport www -j ACCEPT

Dado que el soporte para el firewall está integrado en el kernel de Linux (Netfilter), para poder usar iptables tendremos que asegurarnos de que nuestro núcleo admite el uso de iptables y que añadimos a la configuración del núcleo todos aquellos targets que vayamos a necesitar (aunque siempre es bueno tener los más posibles).

Dado que tenemos multitud de conexiones, más aún si estamos ofreciendo servicios, deberemos introducir una multitud de comandos al iptables cada vez que arranque el núcleo, un trabajo tedioso, de ahí que se opte por la automatización.

Por ello se crea un script, un simple archivo de texto, en el que ponemos todo lo que queramos que ejecute nuestro firewall durante la carga del sistema, y programamos el Linux para que cargue el script durante arranque, olvidándonos de esta tarea tediosa.

ALTERNATIVA DE UN FIREWALL BAJO EL SISTEMA OPERATIVO LINUX

Una alternativa que se encuentra en cuanto a materia de Firewall se refiere es la configuración de un cortafuego bajo la plataforma Linux, lo único que se hace es crear un script de shell en el que se apliquen las reglas de acuerdo a sus necesidades.

El firewall está configurado de la siguiente manera:

```
#!/bin/sh

#firewall para nuestra red LAN....

  ## Limpiamos las reglas

  echo Limpiando reglas...
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

  # Cargamos los modulos...
  echo actualizando y cargando modulos...

/sbin/depmod -a # actualizar los modulos...
```

```
modprobe ip_conntrack
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_mangle
modprobe iptable_nat
modprobe ipt_LOG
modprobe ipt_REJECT
modprobe ipt_MASQUERADE
modprobe ip_conntrack_ftp # para conexión al servidor ftp
modprobe ip_conntrack_irc


  #Establecemos las políticas
  echo estableciendo políticas....

#Entrar y salir lo solicitado
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

  #Activamos el forwading
echo 1>/proc/sys/net/ipv4/ip_forward

  #Configuración de las reglas...
  echo configurando reglas...

   # quitamos los pings
 echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all

# No responde a los broadcast
 echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
## el localhost se deja
  iptables -A INPUT -i lo -j ACCEPT

# Compartimos conexión de internet a la LAN
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Aceptamos el tráfico de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -d 127.0.0.1 -j ACCEPT

# Al firewall tenemos acceso desde la red local
iptables -A INPUT -i eth0 -j ACCEPT
```

```
 # activamos el puerto 80 (web)
iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

# activamos los puertos para http
iptables -A INPUT -i eth0 -p tcp --dport 443 -j ACCEPT

# activamos el puerto ftp
iptables -A INPUT -i eth0 -p tcp --dport 21 -j ACCEPT

# permitimos la conexión con el servidor DNS
iptables -A INPUT -i eth0 -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -i eth0 -p udp --dport 53 -j ACCEPT

# permitimos conexión a SMPT
iptables -A INPUT -i eth0 -p tcp --dport 25 -j ACCEPT
# Permitimos conexiones ssh
iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT

  # admitir paquetes tcp icmp y udp siempre que se hayan  iniciado en esta
maquina
 iptables -A INPUT -p tcp -m state --state ESTABLISHED,RELATED -j ACCEPT

 iptables -A INPUT -p icmp -m state --state ESTABLISHED,RELATED -j
ACCEPT
 iptables -A INPUT -p udp -m state --state ESTABLISHED,RELATED -j
ACCEPT

# impedir que cualquier paquete tcp proveniente del exterior establezca conexión
con el firewall
 iptables -A INPUT -p tcp --syn -j REJECT --reject-with icmp-port-unreachable

# denegamos lo restante
 iptables -A FORWARD -s 0.0.0.0/0 -o eth0 -j DROP

#enmascaramos la red local
iptables -t nat -A POSTROUTING -s 0.0.0.0/0 -o eth0 -j MASQUERADE

   iptables –L

#FIN DEL FIREWALL...
```

Para observar el funcionamiento y que este firewall saliera a Internet desde la red en lenguaje iptable se ejecutó tres pasos fundamentales que se muestra a continuación.

Primeramente desde el shell hay que entrar como root, por defecto en Ubuntu no esta permitido, pero para hacerlo solo basta con teclear:

#>sudo –s –H con este comando tenemos el acceso como root

Hay que tener presente que el quipo debe contar con dos tarjetas de red instaladas, en mi caso cuando se hizo la prueba tenia eth0 la salida a Internet y en la eth1 el acceso a la red donde quiero compartir la conexión, que en este caso es una red.

1. **#> echo 1> /proc/sys/net/ipv4//ip_forward**
   Con esto estamos activando el forwarding, es decir cambiando el bit a true.
   #> iptables -F
   #> iptables -X
   #> iptables -Z
   #> iptables –t nat –F

   Con esto quitamos las reglas que tuviera el iptable, así nos evitamos el ruido que pueda ocasionar.

2. **#> iptables –t nat –A POSTROUTING –s 192.168.25.0/25 –d 0.0.0.0/0 –j MASQUERADE**

Aquí se está enmascarando la red, es decir el servidor identifica que unos de los equipos de la red intenta conectar a una direccion fuera de esta y es el mismo servidor que realiza la petición por si mismo en lugar que el cliente lo haga, así este toma la direccion IP de la maquina que izo la solicitud la enmascara con la direccion IP que le fue asignada, la envía, y cuando llega el paquete de respuesta lo reenvía a la maquina que realizó la petición.

3. **#>iptables –A INPUT –p TCP –m state RELATED –j ACEPT**
   Con esto estamos aceptando todos los paquetes que vengan para que puedan navegar los demás equipos por Internet.

Y por ultimo guardamos los cambios y le damos permiso de ejecucio:

Sudo chmod –v 755 /etc/init.d/iptablesconf

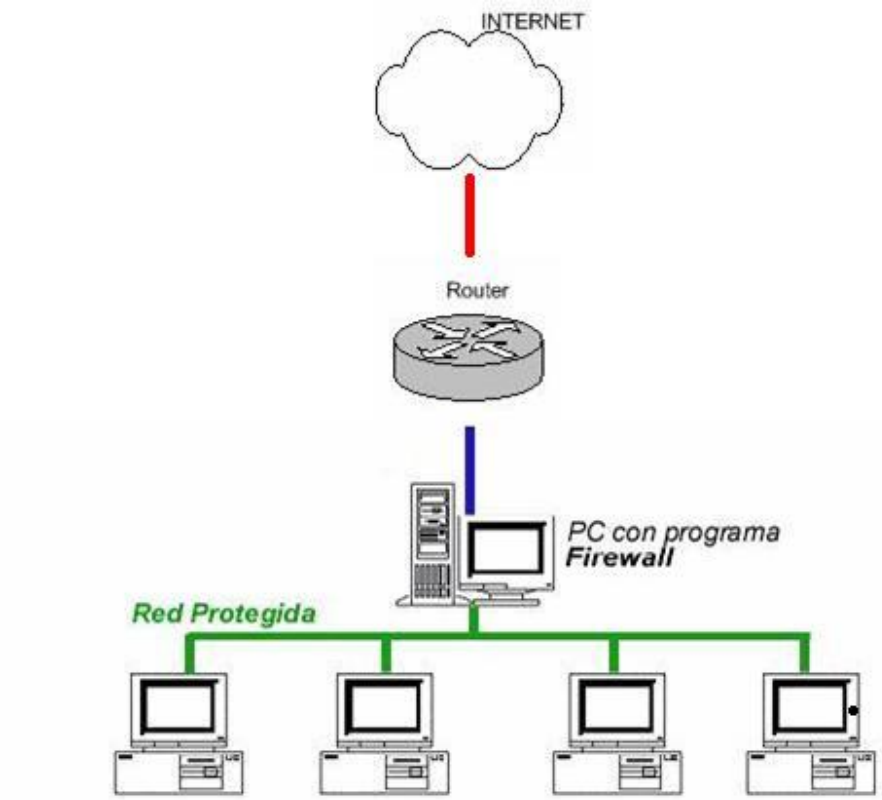
Sudo chmod /etc/init.d/iptablesconf

Si todo esta correcto aparecerá un mensaje como este:

Ejecutando Las Reglas del Firewall… [ok]

La configuración del firewall funciona debidamente, tanto los puertos de salidas como los de entrada hacen sus respectiva función este a diferencia de los firewall en Windows XP es menos tedioso en cuantos a las alertas ya que no son presentados los mensajes a cada momento el análisis lo hace internamente, es decir todos los incidentes y bloqueos se van almacenando en un archivo llamado LOG para tener control del servidor.

ESQUEMA DE LA RED LAN



RESULTADOS DE LOS FIREWALLS

A continuación se muestra el siguiente cuadro comparativo de resultados de los diferentes cortafuegos.

RESULTADOS DE LOS FIREWALLS						
CORTAFUEGOS	**PRUEBAS**					
	One	**Two**	**Three**	**Four**	**Five**	**Six**
Zone Alarm	✓	✓	✖	✖	✓	✖
Outpost Firewall	✓	✓	✓	✓	✓	✓
Kaspersky Anti-Hacker	✖	✖	✖	✖	✖	✖

Zone Alarm

El significado de la prueba que el firewall obtuvo fueron las siguientes:

- **One:** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución.
  El control de procesos ocultos interrumpe impidiendo así este intento.

- **Two:** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución. **El control de componentes indica al usuario y descarta este intento.**

- **Five:** AWFT efectúa una búsqueda heurística de servidores Proxy y otros programas autorizados a acceder a Internet mediante el puerto 80, cargando una copia en memoria y modificándola antes de su ejecución a través de una instancia del Explorador de Windows. **En la totalidad de los casos el bloque de este análisis es bastante difícil para la mayoría de los cortafuegos, pero el Zone Alarm pudo detectarlo por medio del control de procesos ocultos.**

Outpost Firewall

El significado de la prueba que el firewall obtuvo fueron las siguientes:

- **One:** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución.
  El control de procesos ocultos bloquea este intento.

- **Two:** Intenta cargar en memoria una copia del navegador predeterminado y modificar su código antes de su posterior ejecución. **El control de componentes advierte al usuario y bloquea este intento.**

- **Three**: Crea una instancia de ejecución en el Explorador de Windows pretendiendo acceder a la red. **El Asistente de reglas detiene el intento e informa de la situación al usuario.**

- **Four:** Intenta cargar el navegador predeterminado utilizando el Explorador de Windows y modificándolo en memoria antes de su posterior ejecución. Esta prueba generalmente derrota a los cortafuegos que requieren la autorización para que una aplicación pueda ejecutar otra ya que el Explorador de Windows es normalmente autorizado. **En este caso, Outpost Firewall detectó el intento de conexión a través del control de procesos ocultos.**

- **Five:** AWFT efectúa una búsqueda heurística de servidores Proxy y otros programas autorizados a acceder a Internet mediante el puerto 80, cargando una copia en memoria y modificándola antes de su ejecución a través de una instancia del Explorador de Windows.

El bloqueo de este análisis es dificultoso para la mayoría de los cortafuegos pero Outpost Firewall pudo detectar a través del control de procesos ocultos.

- **Six:** AWFT efectúa una búsqueda heurística de servidores Proxy y otros programas autorizados a acceder a Internet mediante el puerto 80, cargando una copia en memoria y modificándola antes de su ejecución a través de una instancia del Explorador de Windows. **En cuanto a este bloqueo en su mayoría no son detectado por los cortafuegos siendo la excepción Outpost Firewall que lo observo por medio del control de componentes.**

Kaspersky Anti-Hacker

El resultado de este firewall fue que no obtuvo puntaje alguno; es decir que de las seis pruebas del test no bloqueó ninguna.

ANÁLISIS DE RESULTADOS DE LOS CORTAFUEGOS

Luego de haber explicado todo lo necesario sobre lo que es un firewall, y para que se utiliza se procedió a realizar las pruebas a los diferentes cortafuegos descargando de Internet el test AWFT (Atelier Web Firewall Tester), luego se instaló y posteriormente se analizó cada una de las reglas.

Al llevar acabo la prueba se observó que el firewall Zone Alarm obtuvo un resultado de cinco puntos de diez que es en total, lo cual significa que el rendimiento fue en menor grado, ya que únicamente obtuvo la mitad de lo establecido.

Esto indica que dicho cortafuego no es el más óptimo para aplicarlo a una red ya que no garantiza la seguridad necesaria para la misma, en cambio con el Outpost Firewall obtuvo la mayor puntuación (10) esto significa que al momento de verificar las seis pruebas del test éste aprobó las reglas concluyendo que es el firewall más recomendado para aplicarlo a una red.

Y por ultimo está el Kaspersky Anti–Hacker no obteniendo puntaje alguno; es decir que de las seis pruebas del test no bloqueó ninguna lo cual significa que no está apto para proteger una red; sin embargo puede ser útil para implementarlo en una computadora personal.

CONCLUSIONES.

Los firewalls distribuidos ofrecen en muchos casos una alternativa eficiente y flexible a las soluciones tradicionales basadas en las limitaciones impuestas por la topología de una red, pero también pueden complementar y aumentar el nivel de seguridad logrado con un firewall.

Existen en el mercado variadas herramientas desarrolladas bajo este nuevo enfoque que implementan en mayor o menor medida las características de los firewalls distribuidos. Para la selección de un determinado firewall que se desee montar se debe tener presente las necesidades básicas tanto del usuario como de la red a instalar.

Se implementó la instalación, configuración y prueba de cuatro firewalls en particular, tres de ellos con el sistema operativo Windows xp éstos son: firewalls Zone alarm, Outpost Firewall y Kaspersky-Anti-hacker. El último se trabajó bajo el sistema operativo Linux utilizando el lenguaje iptable; para establecer las diferencias que brinda cada uno de ellos y posteriormente observar cual se ajustaba más a la red. Cada uno de estos firewall se probó mediante un Test para observar el comportamiento de cada uno.

El Outpost Firewall es el más ampliamente utilizado por los usuarios por tener un alto grado de eficiencia, es decir que cumple con todas las reglas para proteger y mantener bloqueada la red a los distintos tipos de ataques que pueda sufrir. Su manejo y configuración es bastante sencillo, ya que no requiere de un código específico si no que, solamente consiste en seguir las instrucciones para su instalación; además ofrece un alto nivel de protección en varias áreas de trabajo y esto hace de él un buen cortafuego.

En lo que se refiere al Zone Alarm tiene un rendimiento intermedio, es decir, permite proteger parte de la red pero no en gran cantidad ya que sus recursos son limitados y su rendimiento no abarca en gran espacio.

En cuanto al firewall Kaspersky-Anti-hacker está diseñado prácticamente para uso doméstico.

Los sistemas Linux están tomando popularidad por ser gratuitos. IPTABLES es una alternativa flexible en materia de Firewalls, pues no se requiere de muchos recursos para implementarlo, basta con un CPU conectado a la red con un sistema Linux instalado para hacer el filtrado y enrutamiento.

En los firewalls libres para Windows se encuentra un límite en cuanto a modificaciones se refiere, en cambio con IPTABLES se puede crear un firewall propio que contenga los requerimientos que la red necesite.

Es necesario recordar que para elegir un determinado firewall se debe tener presente: el tipo de red a montar es decir integración con la red ya que se debe tomar en cuenta que los protocolos que se instalen tengan soporte establecido para la misma.

Otro aspecto a considerar es los tipos de aplicación a utilizar, esto es el tipo de uso que se desee implementar como: uso doméstico, personal o instalar una determinada red. La cantidad de máquinas es muy importante a tomar en cuenta al momento de elegir un determinado firewall.

Existen otros aspectos que se deben tener presente para elegir el firewall que más se se adapte a las necesidades de la red tales como: tipo de información que se quiere mostrar en la red , ancho de banda, eficiencia, rendimiento, características es decir la cobertura del firewall, gestión y seguridad.

RECOMENDACIONES.

Cuando no se tiene la seguridad adecuada los riesgos en los sistemas de información causan un daño significativo a la red, es por ello que se deben establecer ciertas recomendaciones que permitan proteger la seguridad informática.

En este trabajo se abordó la instalación, configuración y prueba de firewalls, sin embargo es necesario que en futuros trabajos sobre este proyecto se aborde de manera más amplia la prueba de firewalls en redes más grandes ya que se dejan las bases teóricas de cómo instalar y configurar dichos firewalls lo que quedaría por ampliar un poco más es la prueba de más firewall en los distintos sistemas operativos para establecer la diferencia entre ellos ya que se debe tener en cuenta que cada día la tecnología avanza y es necesario actualizar los conocimientos y aún más en cuanto a protección de redes se refiere.

Es necesario tomar en cuenta que para una mejor realización de la prueba de firewalls se debe utilizar una IP pública ya que ésta permite la entrada de todo tipo de información sin restricción alguna, y es ahí cuando se prueba si realmente el firewall está protegiendo la red adecuadamente.

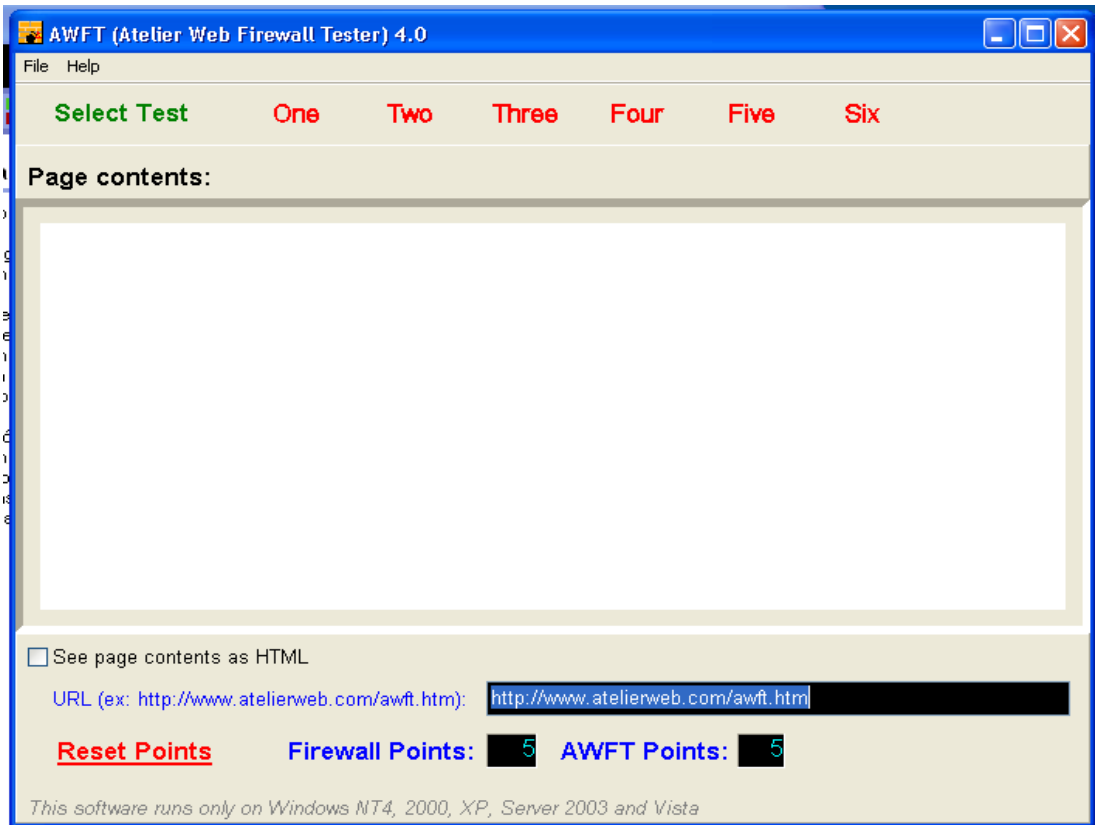
En general es conveniente tener conocimientos previos del trabajo que se va a abordar para buscar la información necesaria, los elementos a utilizar para realizar la prueba y así minimizar el tiempo de investigación y por ende el tiempo de elaboración del trabajo monográfico.

ANEXOS

ANEXOS

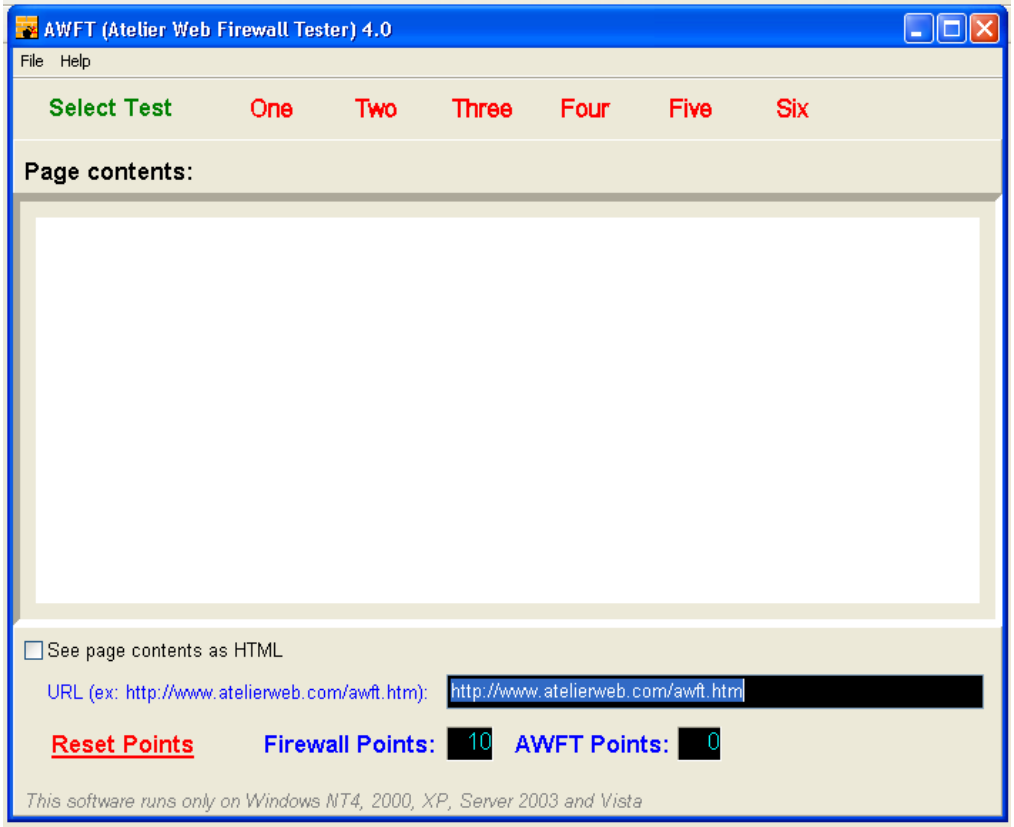
RESULTADO DEL FIREWALL

ZONE ALARM



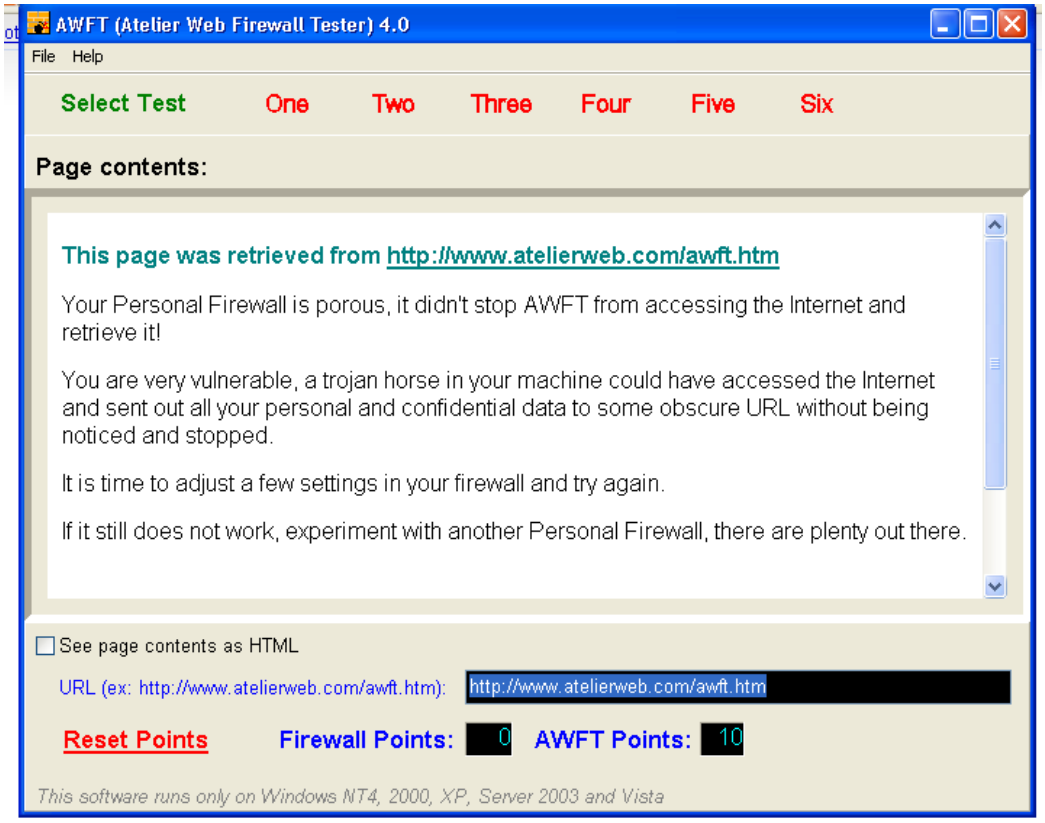
RESULTADO DEL FIREWALL

OUTPOTS FIREWALL



RESULTADO DEL FIREWALL

KASPERKY ANTY-HACKER



BIBLIOGRAFIA.

- www.lawebdelprogramador.com
- www.w3schools.com
- www.3com.com
- www.icsa.net
- www.monografias.com./trabajo3/firewalls/firewalls
- www.infospyware.com/Firewall/Cortafuegos
- www.eswikipedia.org/wiki/Cortafuegos
- www.club.telepolis.com/ramirop/Cortafuegos1
- www.sonicwall.com/es/294.
- www.ciao.es/Opiniones/McAfee_Firewall_199568
- www.atelierweb.com/awft