INSTALACIÓN

Y

CONFIGURACIÓN

DE

CORTAFUEGOS

María Ángeles Peñasco Sánchez- Tema 5- SAD –SRI

Cortafuegos:

- Concepto. Utilización de cortafuegos.
- Historia de los cortafuegos.
- Funciones principales de un cortafuegos: Filtrado de paquetes de datos, filtrado por aplicación, Reglas de filtrado y registros de sucesos de un cortafuegos.
- Listas de control de acceso (ACL).
- Ventajas y Limitaciones de los cortafuegos.
- Políticas de cortafuegos.
- Tipos de cortafuegos.
- Clasificación por ubicación.
- Clasificación por tecnología.
- Arquitectura de cortafuegos.
- Pruebas de funcionamiento. Sondeo.

•Cortafuegos software y hardware:

- Cortafuegos software integrados en los sistemas operativos.
- Cortafuegos software libres y propietarios.
- Distribuciones libres para implementar cortafuegos en máquinas dedicadas.
- Cortafuegos hardware. Gestión Unificada de Amenazas “Firewall UTM” (Unified Threat Management).

Cortafuegos:

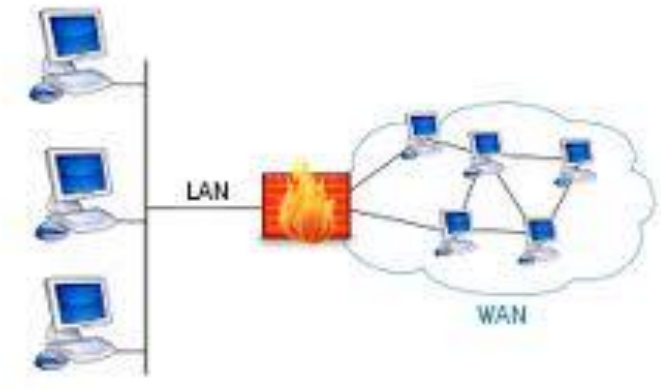
Concepto. Utilización de cortafuegos.

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



Historia de los cortafuegos.

El término "firewall / fireblock" significaba originalmente una pared para confinar un incendio o riesgo potencial de incendio en un edificio. Más adelante se usa para referirse a las estructuras similares, como la hoja de metal que separa el compartimiento del motor de un vehículo o una aeronave de la cabina. La tecnología de los cortafuegos surgió a finales de 1980, cuando Internet era una tecnología bastante nueva en cuanto a su uso global y la conectividad. Los predecesores de los cortafuegos para la seguridad de la red fueron los routers utilizados a finales de 1980, que mantenían a las redes separadas unas de otras. La visión de Internet como una comunidad relativamente pequeña de usuarios con máquinas compatibles, que valoraba la predisposición para el intercambio y la colaboración, terminó con una serie de importantes violaciones de seguridad de Internet que se produjo a finales de los 80:

- Clifford Stoll, que descubrió la forma de manipular el sistema de espionaje alemán.
- Bill Cheswick, cuando en 1992 instaló una cárcel simple electrónica para observar a un atacante.
- En 1988, un empleado del Centro de Investigación Ames de la NASA, en California, envió una nota por correo electrónico a sus colegas que decía:

  "Estamos bajo el ataque de un virus de Internet! Ha llegado a Berkeley, UC San Diego, Lawrence Livermore, Stanford y la NASA Ames."

- El Gusano Morris, que se extendió a través de múltiples vulnerabilidades en las máquinas de la época. Aunque no era malicioso, el gusano Morris fue el primer ataque a gran escala sobre la seguridad en Internet; la red no esperaba ni estaba preparada para hacer frente a su ataque.

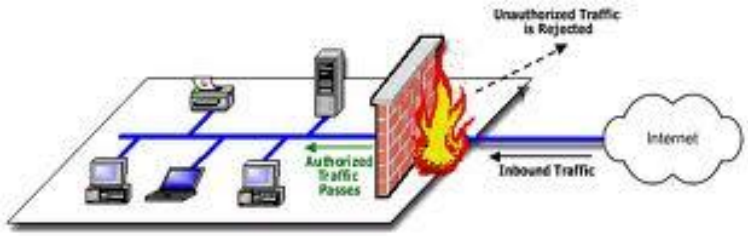
Funciones principales de un cortafuegos: Filtrado de paquetes de datos, filtrado por aplicación, Reglas de filtrado y registros de sucesos de un cortafuegos.

Primera generación – cortafuegos de red: filtrado de paquetes

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

El filtrado de paquetes actúa mediante la inspección de los paquetes (que representan la unidad básica de transferencia de datos entre ordenadores en Internet). Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá (descarte silencioso) o será rechazado (desprendiéndose de él y enviando una respuesta de error al emisor). Este tipo de filtrado de paquetes no presta atención a si el paquete es parte de una secuencia existente de tráfico. En su lugar, se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí (por lo general utiliza una combinación del emisor del paquete y la dirección de destino, su protocolo, y, en el tráfico TCP y UDP, el número de puerto). Los protocolos TCP y UDP comprenden la mayor parte de comunicación a través de Internet, utilizando por convención puertos bien conocidos para determinados tipos de tráfico, por lo que un filtro de paquetes puede distinguir entre ambos tipos de tráfico (ya sean navegación web, impresión remota, envío y recepción de correo electrónico, transferencia de archivos…); a menos que las máquinas a cada lado del filtro de paquetes son a la vez utilizando los mismos puertos no estándar.

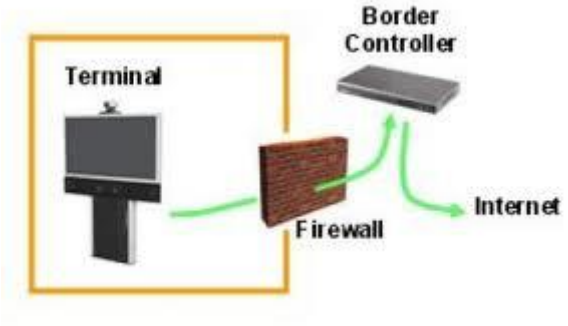
El filtrado de paquetes llevado a cabo por un cortafuegos actúa en las tres primeras capas del modelo de referencia OSI, lo que significa que todo el trabajo lo realiza entre la red y las capas físicas. Cuando el emisor origina un paquete y es filtrado por el cortafuegos, éste último comprueba las reglas de filtrado de paquetes que lleva configuradas, aceptando o rechazando el paquete en consecuencia. Cuando el paquete pasa a través de cortafuegos, éste filtra el paquete mediante un protocolo y un número de puerto base (GSS). Por ejemplo, si existe una norma en el cortafuegos para bloquear el acceso telnet, bloqueará el protocolo IP para el número de puerto 23.



Segunda generación – cortafuegos de estado

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la tercera generación de servidores de seguridad. Esta tercera generación cortafuegos tiene en cuenta además la colocación de cada paquete individual dentro de una serie de paquetes.

Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

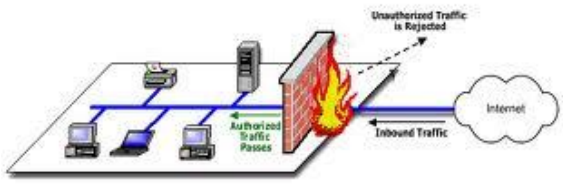


Tercera generación - cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos de aplicación es ISA (Internet Security and Acceleration).

Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear esa palabra en particular. No obstante, los cortafuegos de aplicación resultan más lentos que los de estado.



Listas de control de acceso (ACL).

Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI.

En redes informáticas, ACL se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio. Tanto servidores individuales, como enrutadores pueden tener ACL de redes. Las listas de control de acceso pueden configurarse generalmente para controlar tráfico entrante y saliente y en este contexto son similares a un cortafuegos.

Existen dos tipos de listas de control de acceso:

- Listas estándar, donde solo tenemos que especificar una dirección de origen;
- Listas extendidas, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino

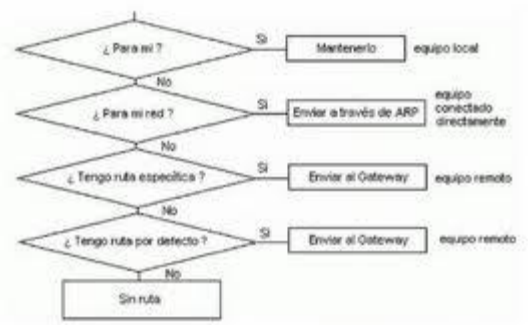


Figura 1. Encaminamiento de paquetes en arquitectura TCP/IP.

Ventajas y Limitaciones de los cortafuegos.

Ventajas de un cortafuegos

Bloquea el acceso a personas y/o aplicaciones no autorizadas a redes privadas.

Limitaciones de un cortafuegos

Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

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

Políticas de cortafuegos.

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

- Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.
- 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. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

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 omisión.

Tipos de cortafuegos.

Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Cortafuegos personal

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por tanto, a nivel personal.

Clasificación por ubicación.

Cortafuegos de capa de red o de filtrado de paquetes

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

Cortafuegos de capa de aplicación

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

Clasificación por tecnología.

Nivel de aplicación de pasarela

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

Arquitectura de cortafuegos.

Existen muchas maneras de estructurar su red para proteger su sistema mediante el uso de un cortafuegos.

Si tiene una conexión exclusiva para Internet a través de un encaminador, podría conectarlo directamente a su sistema cortafuegos o podría pasar por un concentrador de red (hub) para proporcionar a los servidores que se encuentran fuera del cortafuegos un acceso completo.

Arquitectura conmutada

Si usa un servicio conmutado como una línea ISDN, se podría usar una tercera tarjeta de red que permita disponer de una red perimétrica (DMZ). Esto proporciona un control absoluto sobre los servicios de Internet, manteniéndolos separados de la red regular.

Arquitectura de encaminador único

En el encaminador existe la posibilidad de establecer algunas reglas estrictas para el filtro, siempre y cuando haya un encaminador o un módem de cable entre usted e Internet y usted sea el propietario del encaminador. Si el propietario del encaminador es su ISP y, en este caso, no tiene los controles que necesita, puede pedir a su ISP que agregue los filtros.

Cortafuegos con servidor proxy

Si tiene que controlar por dónde se mueven los usuarios de su red, la cual es pequeña, puede integrar un servidor proxy en su cortafuegos. Algunas veces, los ISP lo hacen para confeccionar una lista de interés de sus usuarios con el fin de revenderlas a agencias de marketing.

Si lo prefiere, puede integrar el servidor proxy en su LAN, en cuyo caso, el cortafuegos debe poseer unas órdenes que hagan posible que el servidor proxy sólo se conecte a Internet para aquellos servicios que ofrece. De esta manera, los usuarios sólo podrán acceder a Internet a través del proxy.

Configuración redundante de Internet

Si va a ejecutar un servicio como YAHOO o, tal vez, SlashDot, puede que desee compilar un programa multimódulo en su sistema empleando encaminadores redundantes y cortafuegos.

Mediante la utilización de técnicas de circuito cíclico DNS para dar acceso a varios servidores web desde una URL y varios ISP, es posible crear un servicio de funcionamiento óptimo del 100% con encaminadores y cortafuegos que usan técnicas de alta disponibilidad.

Es muy fácil que la red se le vaya de las manos. Verifique cada conexión. Todo lo que necesita es un usuario con su módem para comprometer su LAN.

Pruebas de funcionamiento. Sondeo.

Son relativamente habituales en nuestros días. No conviene ser extremista, es decir, no ser excesivamente paranoico ni pasar absolutamente del tema.

En realidad la mayoría de ataques y/o escaneos no los realizan hackers o crackers, suelen llevarlos a cabo los que en esta terminología se denominan lamers, es decir, gente con pocos o nulos conocimientos, que utiliza herramientas de otro para intentar acceder o averiguar datos de un sistema. Si el firewall lo permite, la mejor opción es auditarlos (registrar cuando y desde donde ocurren en un fichero histórico) para poder estudiar sus características (frecuencia, origen, puertos afectados, etc...). Con todos esos datos en la mano es más sencillo determinar si se trata de alguien inexperto, o si realmente se avecina un ataque serio.

- Cortafuegos software y hardware:

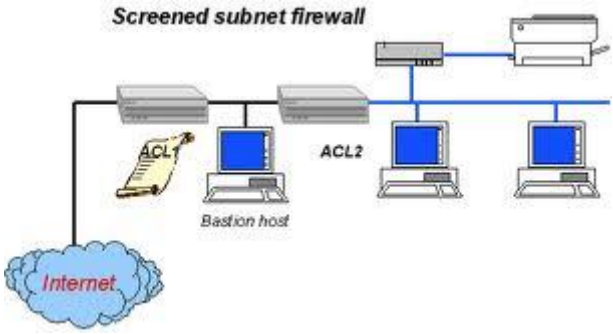
Cortafuegos software integrados en los sistemas operativos.

Para usuarios particulares, el cortafuegos más utilizado es un cortafuego de software. Un buen cortafuegos de software protegerá tu ordenador contra intentos de controlar o acceder a tu ordenador desde el exterior, y generalmente proporciona protección adicional contra los troyanos o gusanos de E-mail más comunes.

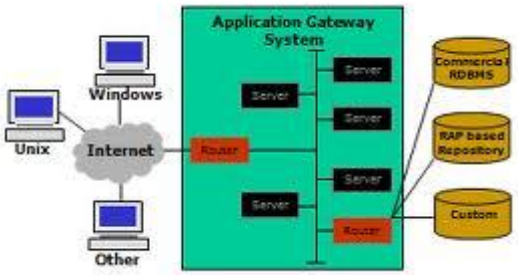
La desventaja de los cortafuegos de software es que protegen solamente al ordenador en el que están instalados y no protegen una red.

Hay varios tipos de técnicas cortafuegos

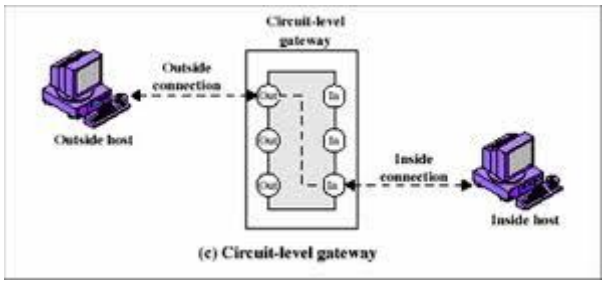
- Packet filter: mira cada paquete que entra o sale de la red y lo acepta o rechaza basándose en reglas definidas por el usuario. La filtración del paquete es bastante eficaz y transparente a los usuarios, pero es difícil de configurar. Además, es susceptible al IP Spoofing.



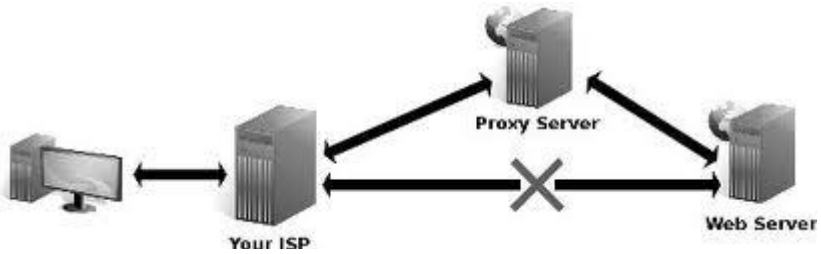
- Application gateway: Aplica mecanismos de seguridad a ciertas aplicaciones, tales como servidores ftp y servidores telnet. Esto es muy eficaz, pero puede producir una disminución de las prestaciones.



- Circuit-level gateway: Aplica mecanismos de seguridad cuando se establece una conexión TCP o UDP. Una vez que se haya hecho la conexión, los paquetes pueden fluir entre los anfitriones sin más comprobaciones.



- Proxy server: Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta con eficacia las direcciones de red verdaderas.



Cortafuegos software libres y propietarios.

Existen muchos cortafuegos pero se pueden dividir básicamente en dos tipos:

- De pago
- Gratuitos

Muchas casas comerciales que tienen firewalls de pago también distribuyen alguno gratuito, sobre todo pensando en el usuario casero que normalmente no se gasta mucho dinero en programas.

La diferencia entre un firewall gratuito y uno de pago viene en la cantidad de funciones que tienen estos últimos; suelen ser más y con más opciones. Aun así, para un usuario casero con poca experiencia, basta un firewall gratuito. Una vez que se tenga experiencia con él, se puede uno plantear instalar uno de pago.

Los Firewall (cortafuegos) te avisan cuando algún programa trata de conectarse a internet desde tu PC, intentando de esta forma proteger tu computadora de posibles intrusiones de Internet. Últimamente debido a la gran cantidad de programas espía que existen, el uso de un firewall se ha vuelto indispensable. Algunos de los cortafuegos más conocidos son gratis para uso personal.

Ghost Wall es un cortafuegos que filtra los paquetes y utiliza poca cantidad de recursos con una latencia menor que otros firewalls. Hay versiones disponibles para Windows de 32 y 64 bits.

Guarddog es una utilidad para la configuración de un cortafuegos para las iptables de Linux. El software es GNU GPL.

PC Tools Firewall Plus es un cortafuegos gratuito para Windows que filtra paquetes de entrada y salida de nuestro sistema. El software permite crear reglas para las aplicaciones que se conectan a la red y reglas para el filtro de paquetes. El registro es gratuito, pero es necesario registrarse con el email para activar el software pasado el período de evaluación.

SoftPerfect Personal Firewall es un firewall para el sistema operativo Windows que filtra paquetes por IP, y viene con un gran conjunto de reglas predefinidas para permitir o denegar el acceso de ciertas aplicaciones a Internet.

ZoneAlarm es, quizás, uno de los firewalls gratuito para uso personal más conocido que hay. Es muy sencillo y fácil de usar. La versión gratuita te permite decidir que aplicaciones tendrán acceso a internet, pero no te permite bloquear IP's específicas. Funciona solamente en plataformas Windows.

Firestarter es una sencilla herramienta que permite configurar un firewall para Linux, tiene una interface gráfica para KDE y GNOME y soporta el kernel de Linux 2.6. Firestarter se encarga eficientemente de detener el paso a las intrusiones hacia nuestro sistema.

WIPFW es un proyecto de software libre alojado en sourceforge que filtra paquetes en plataformas Windows.

Distribuciones libres para implementar cortafuegos en máquinas dedicadas.

Existen equipos diseñados específicamente para trabajar como cortafuegos. La ventaja fundamental de estos aparatos es que todos sus componentes han sido diseñados con los mismos requisitos de seguridad, al contrario de lo que ocurre con otras soluciones.

Algunos cortafuegos dedicados (o "cajas negras") disponen de circuitos que realizan algunas funciones que de otra forma se harían por software, acelerando enormemente las prestaciones. El cifrado en las redes privadas virtuales es lo que más se beneficia de esto; un router solamente puede hacerlo a velocidades moderadas, mientras algunos cortafuegos dedicados son capes de cifrar un flujo de datos a velocidades de hasta 100 Mbps

La ventaja fundamental de algunos de ellos, de cualquier manera, es la sencillez de configuración. Muchos problemas de seguridad se deben a errores provocados por equipos complicados o tediosos de configurar. Cuanto más sencillo resulte, más improbable es cometer errores.

Algunos modelos recientes, además, pueden incorporar un antivirus dentro de la misma unidad, ofreciendo una primera línea de defensa cuyo funcionamiento no se ve afectada por los propios virus; algunos de ellos desactivan el software antivirus de los equipos afectados.

Cortafuegos hardware. Gestión Unificada de Amenazas “Firewall UTM” (Unified Threat Management).

Los firewall de hardware se utilizan más en empresas y grandes corporaciones. Normalmente son dispositivos que se colocan entre el router y la conexión telefónica. Como ventajas, podemos destacar, que al ser independientes del PC, no es necesario configurarlos cada vez que reinstalamos el sistema operativo, y no consumen recursos del sistema. Un ejemplo de ellos es el Panda GateDefender Integra, una UTM - unidad para la Gestión unificada de amenazas) que protege la red de la compañía de cualquier tipo de riesgo que pueda llegar a través de Internet, dado que incluye todas las protecciones necesarias en un único dispositivo: Firewall, IPS, VPN, Anti-malware, Content Filter, Anti-spam y Filtrado web

TM (en inglés: Unified Threat Management) o Gestión Unificada de Amenazas. El término fue utilizado por primera vez por Charles Kolodgy, de International Data Corporation (IDC), en 2004.

Se utiliza para describir los cortafuegos de red que engloban múltiples funcionalidades en una misma máquina. Algunas de las funcionalidades que puede incluir son las siguientes:

UDP - VPN - Antispam - Antiphishing - Antispyware - Filtro de contenidos - Antivirus - Detección/Prevención de Intrusos (IDS/IPS)

Se trata de cortafuegos a nivel de capa de aplicación que pueden trabajar de dos modos:

Desventajas:

- Se crea un punto único de fallo y un cuello de botella, es decir si falla este sistema la organización queda desprotegida totalmente.
- Tiene un coste fijo periódico.

Ventajas: Se pueden sustituir varios sistemas independientes por uno solo facilitando su gestión.

UTM es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo.

Pueden tener varios modos: - Modo proxy: hacen uso de proxies para procesar y redirigir todo el tráfico interno. - Modo Transparente: no redirigen ningún paquete que pase por la línea, simplemente lo procesan y son capaces de analizar en tiempo real los paquetes. Este modo, como es de suponer, requiere de unas altas prestaciones hardware