Instalación y configuración de cortafuegos

# Seguridad y Alta Disponibilidad

**Autor: Miguel Ángel García Felipe**

I.E.S GREGORIO PRIETO

**ÍNDICE:**

# • Cortafuegos:

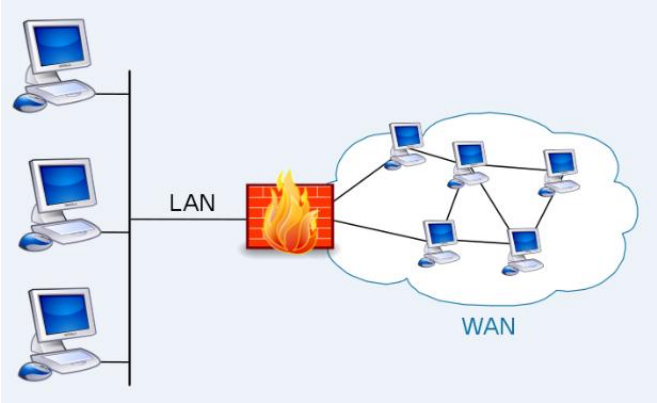
## - Concepto. Utilización de cortafuegos.

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.

**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).

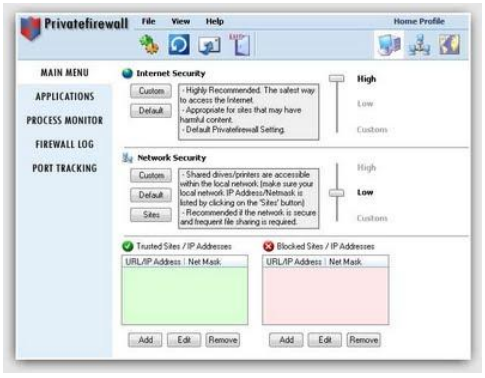
Un cortafuegos de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS). Por ejemplo, si una organización quiere bloquear toda la información relacionada con una palabra en concreto, puede habilitarse el filtrado de contenido para bloquear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

**Acontecimientos posteriores**

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple. En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS).

Actualmente, el Grupo de Trabajo de Comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos.



Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuegos. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como el cortafuegos NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

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

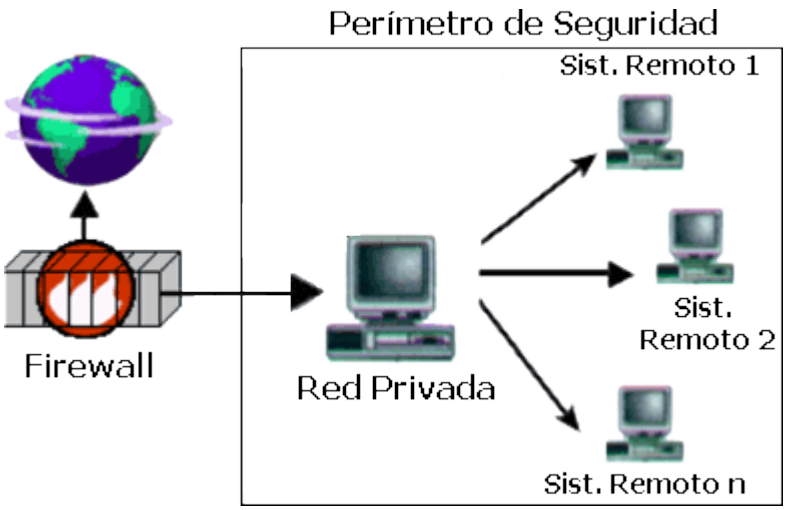
Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes 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.




Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del

interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

**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 auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.

5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

**Filtrado de aplicaciones**

El filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones opera en el nivel 7 (capa de aplicaciones) del modelo OSI, a diferencia del filtrado simple de paquetes (nivel 4). El filtrado de aplicaciones implica el conocimiento de los protocolos utilizados por cada aplicación.

Como su nombre lo indica, el filtrado de aplicaciones permite filtrar las comunicaciones de cada aplicación. El filtrado de aplicaciones implica el conocimiento de las aplicaciones en la red y un gran entendimiento de la forma en que en ésta se estructuran los datos intercambiados (puertos, etc.).

Un firewall que ejecuta un filtrado de aplicaciones se denomina generalmente "pasarela de aplicaciones" o ("proxy"), ya que actúa como relé entre dos redes mediante la intervención y la realización de una evaluación completa del contenido en los paquetes intercambiados. Por lo tanto, el proxy actúa como intermediario entre los ordenadores de la red interna y la red externa, y es el que recibe los ataques. Además, el filtrado de aplicaciones permite la destrucción de los encabezados que preceden los mensajes de aplicaciones, lo cual proporciona una mayor seguridad.

Este tipo de firewall es muy efectivo y, si se ejecuta correctamente, asegura una buena protección de la red. Por otra parte, el análisis detallado de los datos de la aplicación requiere una gran capacidad de procesamiento, lo que a menudo implica la ralentización de las comunicaciones, ya que cada paquete debe analizarse minuciosamente.

Además, el proxy debe interpretar una gran variedad de protocolos y conocer las vulnerabilidades relacionadas para ser efectivo.

Finalmente, un sistema como este podría tener vulnerabilidades debido a que interpreta pedidos que pasan a través de sus brechas. Por lo tanto, el firewall (dinámico o no) debería disociarse del proxy para reducir los riesgos de comprometer al sistema.

**Reglas de filtrado**

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el trafico está basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el

puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado número de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 *y* que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfecionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

## - Listas de control de acceso (ACL).

Las ACL son listas de instrucciones que se aplican a una interfaz del router. Estas listas indican al router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar. La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y número de puerto. Las ACL le permiten administrar el tráfico y examinar paquetes específicos, aplicando la ACL a una interfaz del router. Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL.

Las ACL se pueden crear para todos los protocolos enrutados de red, como el Protocolo Internet (IP) y el Intercambio de paquetes de internetwork (IPX), para filtrar los paquetes a medida que pasan por un router. Las ACL se pueden configurar en el router para controlar el acceso a una red o subred. Por ejemplo, en el Distrito Escolar Washington, las ACL se pueden usar para evitar que el tráfico de los estudiantes pueda entrar a la red administrativa.

Las ACL filtran el tráfico de red controlando si los paquetes enrutados se envían o se bloquean en las interfaces del router. El router examina cada paquete para determinar si se debe enviar o descartar, según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la dirección origen o destino del tráfico, el protocolo de capa superior, u otra información.

Las ACL se deben definir por protocolo. En otras palabras, es necesario definir una ACL para cada protocolo habilitado en una interfaz si desea controlar el flujo de tráfico para esa interfaz. (Observe que algunos protocolos se refieren a

las ACL como filtros.) Por ejemplo, si su interfaz de router estuviera configurada para IP, AppleTalk e IPX, sería necesario definir por lo menos tres ACL. Las ACL se pueden utilizar como herramientas para el control de redes, agregando la flexibilidad necesaria para filtrar los paquetes que fluyen hacia adentro y hacia afuera de las interfaces del router.

## - Ventajas y Limitaciones de los cortafuegos.

**Ventajas**

- **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**

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 cortafuegos 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 y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

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

**Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.
La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

## - Tipos de cortafuegos.

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

- **Cortafuegos de Filtrado de Paquetes:**

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

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

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

**- Cortafuegos del Nivel de Aplicación:**

Utilizan programas servidor (denominados "proxies") que se ejecutan en el cortafuegos. Estos "proxies" toman las peticiones externas, las examinan y reenvían peticiones legítimas al computador interno que proporciona el servicio apropiado. Los cortafuegos del nivel de aplicación pueden soportar funciones como por ejemplo la autentificación de usuario y el registro.

Debido a que un cortafuegos del nivel de aplicación se considera como el tipo más seguro de cortafuegos, esta configuración proporciona un conjunto de ventajas a la organización de riesgo medio-alta:

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

(2) La utilización de "proxies" para diferentes servicios impide el acceso directo a servicios de la red interna, protegiendo a la organización contra computadores internos mal configurados ó no seguros.

(3) La autentificación fuerte de usuario puede ser obligada por los cortafuegos del nivel de aplicación.

(4) Los "proxies" pueden proporcionar registro (ó "logging") detallado en el nivel de aplicación. Los cortafuegos del nivel de aplicación deberían configurarse de modo que el tráfico de red externo (fuera del perímetro de seguridad) aparezca como si el tráfico lo originó el cortafuegos (es decir, sólo el cortafuegos está visible para las redes externas). De esta forma, no está permitido el acceso directo a los servicios de red de la red interna. Todas las peticiones entrantes para los diferentes servicios de red como telnet, ftp, http, rlogin, etc. sin tener en cuenta qué computador de la red interna es el destino final, deben ir a través del "proxy" apropiado del cortafuegos.

Los cortafuegos del nivel de aplicación requieren que se soporte un "proxy" para cada servicio, por ejemplo ftp, http, etc.. Cuando un servicio se requiere que no esté soportado por un "proxy", la organización posee tres alternativas:

(1) Denegar el servicio hasta que el fabricante del cortafuegos desarrolle un "proxy seguro". Esta es la alternativa preferida cuando los nuevos servicios Internet introducidos poseen vulnerabilidades no aceptables.

(2) Desarrollar un "proxy a medida". Esta opción es una tarea bastante difícil y sólo debería emprenderse por organizaciones técnicas sofisticadas.

(3) Pasar el servicio a través del cortafuegos. Utilizando lo que se denomina normalmente "plugs", la mayoría de cortafuegos del nivel de aplicación permiten que los servicios se pasen directamente a través del cortafuegos con sólo un mínimo de filtrado de paquetes.
Esto puede limitar algunas de las vulnerabilidades pero puede comprometer la seguridad de los sistemas detrás del cortafuegos.

Cuando un servicio Internet interno (dentro de la frontera de seguridad) no está soportado por un "proxy" se requiere pasar a través del cortafuegos, el administrador del cortafuegos debe definir la configuración ó "plug" que permita el servicio pedido. Cuando está disponible un "proxy" del fabricante del cortafuegos, el "plug" se inhabilitará y el "proxy" se hará operativo.
Todos los servicios Internet internos (de dentro del perímetro de seguridad) deben ser procesados por software "proxy" del cortafuegos. Si se pide un nuevo servicio, este no se estará disponible hasta que se disponga de un "proxy" del fabricante del cortafuegos y sea verificado por el administrador del cortafuegos. Se puede desarrollar un "proxy a medida" por la propia organización ó por otros fabricantes y sólo se podrá utilizar cuando sea aprobado por el responsable de seguridad de información.

- **Cortafuegos Híbridos:**

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

- Cortafuegos para intranets:

Aunque los cortafuegos normalmente se colocan entre una red corporativa y la red no segura del exterior (ó Internet), en grandes organizaciones, los cortafuegos se utilizan a menudo para crear subredes diferentes dentro de la red interna (denominada también Intranet). Los "cortafuegos para Intranets" se utilizan para aislar una subred particular de la red corporativa total. La razón del aislamiento de un segmento de red puede ser que ciertos empleados sólo pueden acceder a subredes guardadas por estos cortafuegos sólo en base a una necesidad concreta. Un ejemplo puede ser un cortafuegos para el departamento de nóminas ó contabilidad de una organización. La decisión de utilizar un cortafuegos Intranet se basa generalmente en la necesidad de hacer cierta información disponible para algunos pero no para todos los usuarios internos ó para proporcionar un alto grado de responsabilidad para el acceso y utilización de información sensible ó confidencial. Para cualquier sistema que guarde aplicaciones críticas de la organización ó que proporcione acceso a información sensible ó confidencial, deberían utilizarse cortafuegos internos ó

routers de filtrado de paquetes para proporcionar control de acceso fuerte y soportar auditoría y registro. Estos controles deberían utilizarse para dividir la red corporativa interna a la hora de soportar políticas de acceso desarrolladas por los propietarios de información designados.

- **Cortafuegos con capacidad VPN:**

  Las redes privadas virtuales ó VPN (Virtual Private Networks) permiten a las redes seguras comunicarse con otras redes seguras utilizando redes no seguras como Internet. Puesto que algunos cortafuegos proporcionan la "capacidad VPN", es necesario definir una política de seguridad para establecer VPNs. Cualquier conexión entre cortafuegos sobre redes públicas utilizan VPNs cifradas para asegurar la privacidad e integridad de los datos que se pasan a través de la red pública. Todas las conexiones VPN deben ser aprobadas y gestionadas por el administrador de servicios de red. Deben establecerse los medios apropiados para distribuir y mantener claves de cifrado antes del uso operacional de los VPNs.

## - Clasificación por ubicación.

**Cortafuegos personales (para PC)**

La herramienta adecuada para salvaguardar la seguridad del sistema es un firewall personal.
El firewall personal es un programa que funciona en su ordenador de forma permanente.
El programa monitoriza las conexiones que entran y salen de su ordenador y es capaz de distinguir las que son legítimas de las realizadas por atacantes. En este segundo caso, las bloquea y lo notifica al usuario del ordenador.

**Cortafuegos para pequeñas oficinas (SOHO)**

El software de cortafuegos SoHo aísla el ordenador o pequeña red de su conexión a Internet filtrando información, bloqueando puertos abiertos y deteniendo programas maliciosos con controles ActiveX o rutinas en JavaScript.

**Cortafuegos corporativos**

Es un tipo de cortafuego, y como su nombre lo indica, son utilizados mayormente en sistemas interconectados de organizaciones y empresas en donde cierta cantidad de equipos podrían estar conectados en red compartiendo y accediendo a cientos de recursos simultáneamente. Estos sistemas tienen el objetivo de filtrar las comunicaciones en el borde de la organización. Debido a que todo el tráfico que circula desde la red interna hacia fuera y viceversa es elevado, estos sistemas deben ser eficientes en el manejo de todas las conexiones.

Una de las ventajas de la utilización de estos dispositivos es que todos los equipos de la organización estarán protegidos por un único sistema, bloqueando o dejando pasar las comunicaciones que el administrador haya dispuesto para toda la organización.

## - Clasificación por tecnología.

**Filtros de paquetes**

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

**Proxy de aplicación**

Todos los servicios Internet internos (de dentro del perímetro de seguridad) deben ser procesados por software "proxy" del cortafuegos. Si se pide un nuevo servicio, este no se estará disponible hasta que se disponga de un "proxy" del fabricante del cortafuegos y sea verificado por el administrador del cortafuegos. Se puede desarrollar un "proxy a medida" por la propia organización ó por otros fabricantes y sólo se podrá utilizar cuando sea aprobado por el responsable de seguridad de información.

**Inspección de estados (statefullinspection)**

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.

**Hibridos**

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

- Arquitectura de cortafuegos.

### Cortafuegos de filtrado de paquetes

El modelo de cortafuegos más antiguo consiste en un dispositivo capaz de filtrar paquetes, lo que se denomina *choke*. Está basado simplemente en aprovechar la capacidad que tienen algunos *routers* para bloquear o filtrar paquetes en función de su protocolo, su servicio o su dirección IP.

Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el *router* actúa como de *pasarela* de la subred y no hay necesidad de utilizar *proxies*, ya que los accesos desde la red interna al exterior no bloqueados son directos. Resulta recomendable bloquear todos los servicios que no se utilicen desde el exterior, así como el acceso desde máquinas que no sean de confianza hacia la red interna.

Sin embargo, los *chokes* presentan más desventajas que beneficios para la red protegida, puesto que no disponen de un sistema de monitorización sofisticado y el administrador no distingue entre si el router está siendo atacado o si su seguridad se ha visto comprometida. Por otra parte, las reglas de filtrado pueden llegar a ser complejas de establecer y por lo tanto, se hace difícil comprobar su correción.

### Arquitectura Dual-Homed Host

Este modelo se compone de simples máquinas Unix, denominadas *anfitriones de dos bases*, equipadas con dos tarjetas de red: una se conecta a la red interna a proteger y la otra a la red externa. De este modo, los sistemas de la red interna se pueden comunicar con el *dual-homed host*, así como los sistemas del exterior también se pueden comunicar con el *dual-homed host*; es decir, el tráfico entre la red interna y el exterior está completamente bloqueado. En este caso el *choke* y el *bastión* coinciden en el mismo equipo.

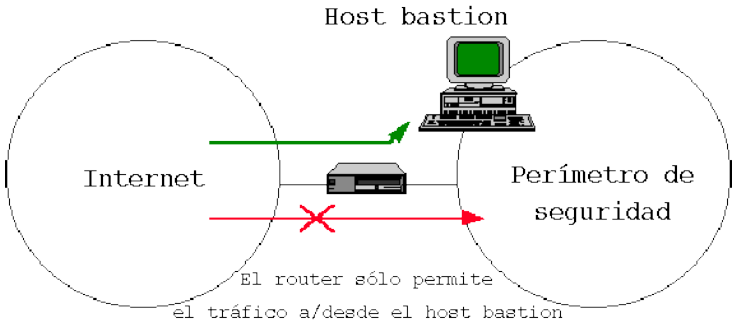
Los *dual-homed hosts* pueden proporcionar un nivel de control muy elevado. Como no se permite el tráfico de paquetes entre la red interna y la externa, un paquete de fuente externa será indicativo de alguna clase de problema de seguridad. Todo el intercambio de datos entre las redes se realiza a través de *servidores proxy* situados en el *host bastión*. Para cada uno de los servicios que se deseen pasar a través del firewall, se ha de ejecutar un *servidor proxy*. También es necesario que esté desabilitado el *IP Forwarding* para que el *choke* no encamine paquetes entre las dos redes.

El uso de *proxies* es mucho menos problemático, pero puede no estar disponible para todos los servicios en los que estemos interesados. La siguiente arquitectura de cortafuegos incorpora opciones extra que permiten proporcionar nuevos servicios.

**Screened Host**

En esta arquitectura se combina un *screening router* con un *host bastión* y el principal nivel de seguridad proviene del filtrado de paquetes. El *screening router* está situado entre el *host bastion* y la red externa, mientras que el *host bastión* está situado dentro de la red interna.

El filtrado de paquetes en el *screening router* está configurado de modo que el *host bastión* es el único sistema de la red interna accesible desde la red externa. Incluso, únicamente se permiten ciertos tipos de conexiones. Cualquier sistema externo que intente acceder a los sistemas internos tendrán que conectar con el *host bastión.* Por otra parte, el filtrado de paquetes permite al *host* establecer las conexiones permitidas, de acuerdo con la política de seguridad, a la red externa.




Screened Host.

La configuración del filtrado de paquetes en el *screening router* se puede hacer de dos formas:

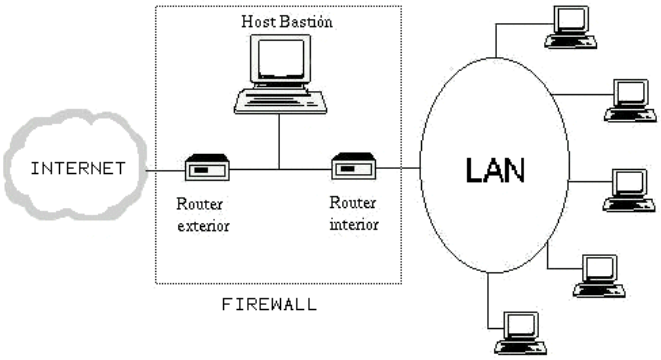
- Permitir a otros hosts internos establecer conexiones a hosts de la red exterior para ciertos servicios.
- Denegar todas las conexiones desde los hosts de la red interna, forzando a los hosts a utilizar los servicos proxy a través del host bastion.

Es decir, los servicios se pueden permitir directamente via filtrado de paquetes o indirectamente via *proxy*, tanto para los usuarios internos como para los usuarios externos.

**Screeened Subnet**

La arquitectura *Screened Subnet* también se conoce con el nombre de red perimétrica o *De-Militarized Zone* (DMZ). En los modelos anteriores, la seguridad se centraba completamente en el *host bastión*, de manera que si la

seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. En cambio, en este modelo se añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consigue reducir los efectos de un ataque exitoso al *host bastión.* La arquitectura DMZ intenta aislar la máquina *bastión* en una red perimétrica, de forma que si un intruso accede a esta máquina no consigue un acceso total a la subred protegida.




*Screened Subnet*.

Se trata de la arquitectura de firewalls más segura, pero también más compleja. En este caso se emplean dos *routers*, exterior e interior, ambos conectados a la red perimétrica como se observa en la figura. En dicha red perimétrica, que constituye el sistema cortafuegos, se incluye el *host bastión*. También se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de la red interna.

La misión del *router* exterior es bloquear el tráfico no deseado en ambos sentidos, es decir, tanto hacia la red perimétrica como hacia la red externa. En cambio, el *router* interior bloquea el tráfico no deseado tanto hacia la red perimétrica como hacia la red interna. De este modo, para atacar la red protegida se tendría que romper la seguridad de ambos *routers*.

En el caso en que se desee obtener un mayor nivel de seguridad, se pueden definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas. Un posible atacante tendría que pasar por todas y cada una de las redes perimétricas para llegar a acceder a los equipos de la red interna. Resulta evidente que cada red perimétrica ha de seguir diferentes reglas de filtrado, ya que en caso contrario los niveles adicionales no proporcionarían una mayor seguridad.

Aunque se trata de la arquitectura más segura, también pueden aparecer problemas. Uno de ellos se puede dar cuando se emplea el cortafuegos para que los servicios fiables pasen directamente sin acceder al *bastión*, lo que puede desencadenar en un

incumplimiento de la política de seguridad. Otro problema, es que la mayor parte de la seguridad reside en los *routers* empleados. Las reglas de filtrado sobre estos elementos pueden ser complicadas de establecer y comprobar, lo que puede desembocar en importantes fallos de seguridad del sistema.

**Otras arquitecturas**

Una manera de incrementar en gran medida el nivel de seguridad de la red interna y al mismo tiempo facilitar la administración de los cortafuegos consiste en emplear un *host bastión* distinto para cada protocolo o servicio en lugar de un único *host bastión*. Muchas organizaciones no pueden adoptar esta arquitectura porque presenta el inconveniente de la cantidad de máquinas necesarias para implementar el cortafuegos. Una alternativa la constituye el hecho de utilizar un único *bastión* pero distintos servidores *proxy* para cada uno de los servicios ofrecidos.

Otra posible arquitectura se da en el caso en que se divide la red intena en diferentes subredes, lo cual es especialmente aplicable en organizaciones que disponen de distintas entidades separadas. En esta situación es recomendable incrementar los niveles de seguridad de las zonas más comprometidas situando cortafuegos internos entre dichas zonas y la red exterior. Aparte de incrementar la seguridad, los *firewalls* internos son especialmente recomendables en zonas de la red desde la que no se permite *a priori* la conexión con Internet.

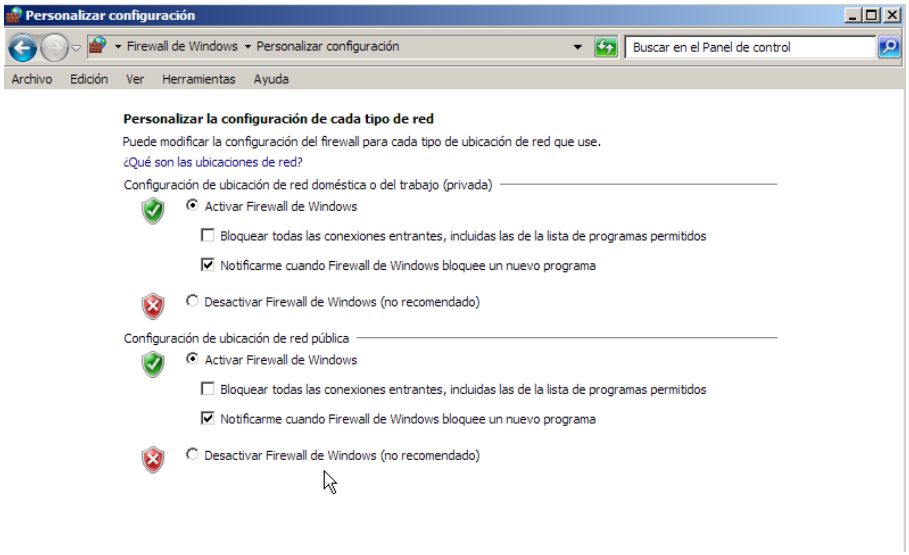
## - Pruebas de funcionamiento. Sondeo.

Un Firewall funciona, en principio, denegando cualquier tráfico que se produzca cerrando todos los puertos de nuestro PC. En el momento que un determinado servicio o programa intente acceder al ordenador nos lo hará saber. Podremos en ese momento aceptar o denegar dicho tráfico, pudiendo asimismo hacer (para no tener que repetir la operación cada vez) "permanente" la respuesta hasta que no cambiemos nuestra política de aceptación. También puedes optar por configurar el Firewall de manera que reciba sin problemas cierto tipo de datos (FTP, chat o correo, por ejemplo) y que filtre el resto de posibilidades. Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Windows XP cuenta con un Firewall, aunque muy sencillo. Sólo te permite filtrar la información que entra en tu ordenador, no la que sale. De esta forma, no te servirá de nada si tienes instalado un programa Adware que recoge datos de tu equipo y se conecta al exterior para enviarlos. Conviene que te instales un Firewall más completo y que te permita configurar políticas de seguridad.

## • Cortafuegos software y hardware:

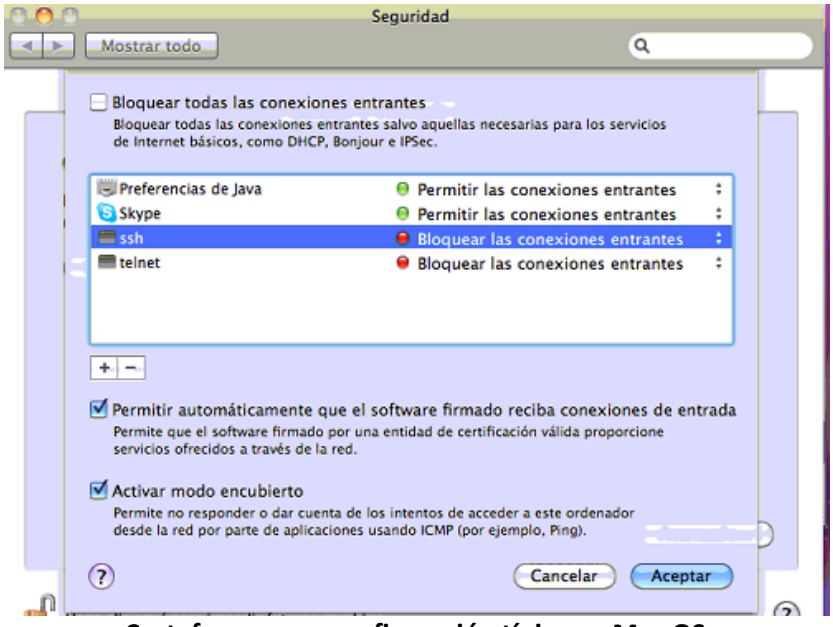
- Cortafuegos software integrados en los sistemas operativos.

Windows cuenta con un cortafuegos integrado, tanto entrante como saliente. Su interfaz básica es muy sencilla.




**Configuración básica del cortafuegos de Windows en Vista y 7**

Mac OS X cuenta con un cortafuegos integrado, sólo para conexiones entrantes.

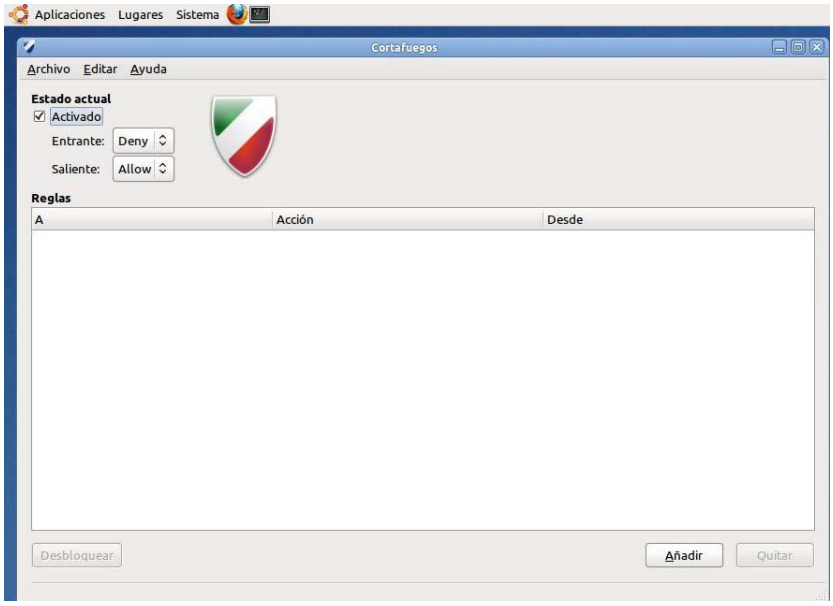



**Cortafuegos con configuración típica en Mac OS**

Para sistemas Linux, es necesario utilizar la línea de comando. Se utilizan reglas llamadas *iptables*, que están implementadas en todos los kernel de todos los Linux.

Son configurables a través de líneas de comando, y permiten total control de puertos y direcciones (tanto entrantes como salientes).

Sin embargo, existen diferentes "interfaces" gráficas que pueden ser instaladas para manejar de forma más cómoda el cortafuegos y sus reglas *iptables.*




**Ejemplo de interfaz gráfica para cortafuegos en Ubuntu**

## - Cortafuegos software libres y propietarios.

### Soluciones Libres

Si se toma la decisión de instalar un Firewall de libre distribución, se recomienda coger todos aquellos que cumplan las necesidades especificas del usuario, y testearlos, usando utilidades especificas para dicha tarea. Después se podrá decidir cuál es el que cumple mejor su "trabajo".

En cuanto a las aplicaciones de Linux, hay que puntualizar que algunas veces es complicado que funcionen, principalmente por incompatibilidades entre versiones, lo que no ocurre con Windows, aunque como ya hemos dicho antes, no se recomienda un Router/Firewall basado en Windows, por ser un Sistema Operativo menos estable que Linux.

Algunos de los firewalls libres podemos encontrar:

ZoneAlarm es, quizá, uno de los firewalls gratuito para uso personalis 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 sólamente en plataformas Windows.

Firestarter es una sencilla herramienta que permite configurar un firewall para Linux, tiene una interficie 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.

**Soluciones Propietarias**

Los cortafuegos propietarios, normalmente suelen ser de tipo hardware y lo podemos incluir en los siguientes 3 tipos:

*La Pequeña Empresa*

Normalmente se instala una maquina dedicada en punta de lanza, con el Firewall corriendo sobre algún sistema operativo preinstalado (normalmente Unix-Linux) y un interfaz grafico para simplificar su administración. Se suelen vender como un equipo completo (Firewall Box), con el servidor, el Sistema Operativo y el Firewall instalado, principalmente para simplificarle el trabajo a aquellas empresas que quieren tener un buen nivel de seguridad sin dedicarle muchos esfuerzos (ningún esfuerzo más allá de la asignación de políticas y reglas).

*La Mediana Empresa*

En estas empresas aparecen las soluciones Hardware y Software, puesto que en esta categoría se encuentran empresas que no desdeñan la comodidad de un Firewall Box y aquellas otras que prefieren la flexibilidad que proporciona un Firewall de Software (sin olvidar que al ser solo el software se invierte en seguridad y no en el equipo sobre el que corre). Dentro de los Firewall de software están aquellos que se instalan sobre un sistema operativo (Windows o Unix) o aquellos que traen una variante de un sistema operativo, en el que se han quitado aquellas funciones vulnerables, o se han reescrito de forma segura.

*Las Grandes Empresas*

En este segmento del mercado incluimos a los ISP's, los grandes centros de datos y las supercorporaciones que tienen un tráfico de red comparable al de muchos proveedores de Internet. Aquí las aplicaciones se centran en

grandes equipos con procesamiento paralelo y las mejores tecnologías de seguridad.

## - Distribuciones libres para implementar cortafuegos en máquinas dedicadas.

Son distribuciones de software libre para implementar cortafuegos en máquinas con pocas prestaciones y suelen ofrecer una interfaz web para administración del router/cortafuegos.

Suelen estar basadas en:

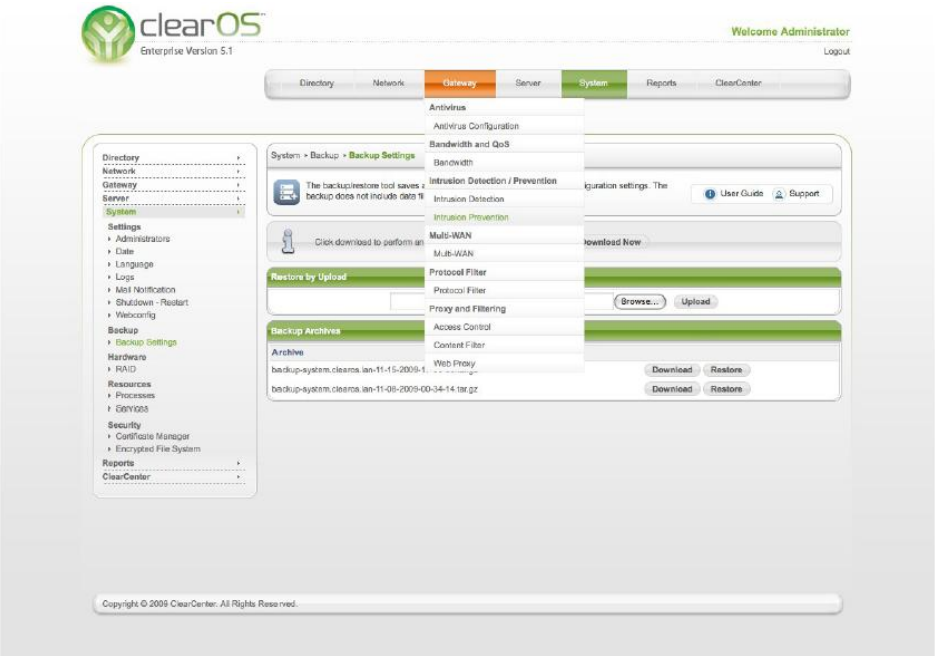
- GNU/Linux: ClearOS, Gibraltar, IPCop, Zentyal, SmoothWall,...
- FreeBSD: m0n0wall, pfSense, etc.

**ClearOS**

Basada en GNU/Linux

*Características:*

- Cortafuegos con estado: iptables
- IDS/IPS: SNORT
- VPN: PPTP, IPSec, OpenVPN
- Proxy Web: Squid
- Filtrado de contenido y antivirus: DansGuardian
- Informes y estadísticas: MRTG




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

Gestión unificada de amenazas (UTM) se refiere a un producto de seguridad integral que incluye la protección contra amenazas múltiples. Un producto UTM normalmente incluye un firewall, software antivirus, filtrado de contenidos y un filtro de spam en un solo paquete integrado. El término fue acuñado originalmente por IDC, un proveedor de datos de mercado, análisis y servicios relacionados. Proveedores de UTM de Fortinet incluyen, LokTek, Secure Computing Corporation y Symantec. Las principales ventajas de la UTM son la sencillez, la instalación y el uso racionalizado, y la capacidad de actualizar todas las funciones de seguridad o programas simultáneamente. Como la naturaleza y la diversidad de las amenazas de Internet evolucionan y se vuelve más complejo, los productos UTM pueden ser adaptados para mantenerse al día con todos ellos. Esto elimina la necesidad de que los administradores de sistemas para mantener múltiples programas de seguridad en el tiempo.

**Las principales ventajas:**

**1.** Reducción de la complejidad: solución de seguridad única. Solo proveedor. Solo AMC
**2.** Simplicidad: Evitar la instalación del software y el mantenimiento de múltiples
**3.** Gestión sencilla: Plug & Play Arquitectura, GUI basada en Web para una fácil gestión
**4.** Reducción de los requisitos de capacitación técnica, un producto de aprender.
**5.** Cumplimiento de la normativa

**Desventajas clave:**

**1.** Punto único de fallo para el tráfico de red
**2.** Único punto de compromiso si la UTM tiene vulnerabilidades
**3.** Impacto potencial sobre la latencia y el ancho de banda cuando la UTM no puede mantenerse al día con el tráfico

- **Bibliografía**

http://es.wikipedia.org/wiki/Cortafuegos_%28inform%C3%A1tica%29
http://www.segu-info.com.ar/firewall/filtradopaquetes.htm
http://es.kioskea.net/contents/**pro**tect/firewall.php3
http://www.monografias.com/trabajos3/firewalls/firewalls.shtml
http://www.elportal.info/etc/sem3/Cap6.txt
http://www.antivirusgratis.com.ar/noticias/display.php?ID=4816
http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cortafuegos/default3.asp
http://www.iit.upcomillas.es/palacios/seguridad/cap10.pdf
http://spi1.nisu.org/recop/al01/rmoreno/arquitecturas.html
www.inteco.es/file/d4f_vt-2kbzM0ex5BxJguQ
http://www.it.uc3m.es/~lmiguel/Firewall_www/SEGURIDAD-to-Web.htm
http://arco.esi.uclm.es/~david.villa/seguridad/cortafuegos.1x3.pdf