Que es

Un firewall o cortafuegos es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes.

Es cualquier sistema (desde un simple Router hasta varias redes en serie) utilizado para separar una maquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.

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

Características

Los cortafuegos pueden ser usados a través de una solución de hardware, es decir un dispositivo físico, o a través de un programa informático instalado en el sistema operativo del ordenador que se desea proteger.

En entornos empresariales suele ser común la utilización de cortafuegos basados en hardware, que protegen y separan la red interna del exterior. Se sitúan en un punto determinado de la conexión entre la red interna y la red exterior.

Sin embargo, en ambientes domésticos la utilización más extendida son las soluciones por software, bien mediante programas informáticos existentes para tal fin o configurando los que incorporan los sistemas operativos. Se sitúan entre el ordenador del usuario y el resto de la red a la que pertenece.

Este se encarga de comprobar los intentos de conexión entrantes y salientes del ordenador o red de ordenadores, controlando el puerto, protocolo IP, etc.

Ventajas de los cortafuegos

Bloquea el acceso a personas no autorizadas a redes privadas

Administra los accesos provenientes de internet hacia la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el internet. Por ello la seguridad en la red privada depende de la “dureza” con que el firewall cuente.

Administra los accesos provenientes de la red privada hacia internet.

Permite al administrador de la red mantener fuera de la red privada a los usuarios no autorizados (tal como hackers, crackers y espías), prohibiendo potencialmente la entrada o salida de datos.

El firewall crea una bitácora en donde se registra el trafico mas significativo que pasa a través de él.

Concentra la seguridad ya que centraliza los accesos.

Inconvenientes y limitaciones

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, (una conexión PPP).

El firewall no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, pues el firewall no es un antivirus. Es preciso instalar software antivirus en cada máquina.

El firewall no puede ofrecer protección alguna una vez que el agresor lo traspasa.

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 protege de los fallos de seguridad de los servicios y protocolos cuyo trafico este permitido.

Clasificación de los cortafuegos

Según su ubicación:

- Cortafuegos personales
- Cortafuegos para pequeñas redes SOHO (Small Office Home Office)
- Cortafuegos corporativos

Tipos según su tecnología:

- Filtrado de paquetes de datos
- Pasarelas de nivel de aplicación (proxys)
- Inspección de estados
- Pasarelas a nivel de circuitos (híbridos)

Cortafuegos personales

- **Cortafuegos personales:** es un caso particular de cortafuegos que se instala como software en un ordenador filtrando las comunicaciones entre el y el resto de la red. Se usa, por tanto, a nivel personal.
- Se instalan de forma residente en nuestro ordenador y permiten filtrar y controlar la conexión a la red.
- **Entrante:** el que controla las conexiones que “entran” en el sistema. Por ejemplo, desde el punto de vista de un servidor que muestra paginas web, un cliente que desee visualizar esta página, será una conexión entrante que debería verificar en su tabla de reglas. Este tipo de cortafuegos es muy usado tanto en servidores como en sistemas que habitualmente actúan como clientes. Por ejemplo, todos los sistemas windows cuentan con un cortafuegos entrante activado por defecto y la inmensa mayoría de los

routers usados para establecer una conexión ADSL tienen un firewall entrante activado por defecto, que protege al ordenador interno.

- **Saliente:** controla las conexiones que "salen" del sistema. Está pensado en mayor medida para clientes, para comprobar hacía que direcciones IP o que puertos se conecta nuestro ordenador. Este tipo de cortafuegos es mucho menos usado que el entrante, aunque es más seguro, puesto que nos permite tener control total de hacia donde intentan conectarse los programas y, por tanto, nuestros datos.

Cortafuegos para pequeñas redes SOHO

SOHO es el acrónimo de Small Office-Home Office (pequeña Oficina-Oficina en casa)

Es un termino que se aplica para determinar a los aparados destinados a un uso profesional o semiprofesional pero que, a diferencia de otros modelos, no están pensados para asumir un gran volumen de trabajo.

El entorno SOHO propiamente dicho se refiere a toda la tecnología informática, a muebles funcionales, productos y servicios destinados al armado de una oficina en un ámbito doméstico.

Cortafuegos de filtrado de paquetes

Cortafuegos de filtrado de paquetes de datos (packet filter firewalls):

Se analiza el trafico de la red fundamentalmente en la capa 3, teniendo en cuenta a veces algunas características físicas propias de la capa 1. Los elementos de decisión con que cuentan a la hora de decidir si un paquete es valido o no son los siguientes:

- La dirección de origen desde donde, supuestamente, viene el paquete (capa 3)
- La dirección del host de destino del paquete (capa 3)
- El protocolo especifico que esta siendo usado para la comunicación, frecuentemente ethernet o IP, aunque existen cortafuegos capaces de desenvolverse con otros protocolos como IPx, NetBIOS, etc. (capas 2 y 3).
- El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
- Los puertos de origen y destino de la sesión (capas 3 y 4).
- Los puertos de origen y destino de la sesión (capa 4).
- El interfaz físico del cortafuegos a través del que el paquete llega y por el que habría que darle salida (capa 1), en dispositivos con 3 o más interfaces.

Ejemplos: iptables en linux y ACL´s en cisco

Ventajas:

- Rapidez, transparencia y flexibilidad.
- Proporcionan un alto rendimiento y escalabilidad y muy bajo coste, y son muy útiles para bloquear la mayoría de los ataques de denegación de servicio, por ello se siguen

implementando como servicios integrados en algunos routers y dispositivos hardware de balanceo de carga de gama media-alta.

Inconvenientes:

- Limita funcionalidad y su dificultad a la hora de configurarlos y mantenerlos
- Son fácilmente vulnerables mediante técnicas de spoofing
- No pueden prevenir contra ataques que exploten vulnerabilidades especificas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI
- No son, pues, efectivos como medida única de seguridad, pero si muy prácticos como primera barrera, en la que se bloquean ciertos ataques, se filtran protocolos no deseados y se pasan los paquetes restantes a otro cortafuegos que examine las capas mas altas del producto.

Cortafuegos por filtrado de aplicación

Cortafuegos de filtrado por aplicación

La practica totalidad de los cortafuegos de este tipo, suelen prestar servicios de proxy.

Un proxy es un servicio especifico que control a el trafico de un determinado protocolo (como HTTP, FTP, DNS, etc.) proporcionando un control de acceso adicional y un detallado registro de sucesos respecto al mismo.

Los servicios o agentes típicos con que cuentan este tipo de dispositivos son: DNS, Finger, FTP, HTTP, HTTPS, LDAP, NMTP, SMTP y Telnet.

Los agentes o servicios proxy están formados por dos componentes: un servidor y un cliente. Ambos suelen implementarse como dos procesos diferentes lanzados por un único ejecutable. El servidor actúa como destino de las conexiones solicitadas por un cliente de la red interna. El cliente del servicio proxy es el que realmente encamina la petición hacia el servidor externo y recibe la respuesta de este. Posteriormente, el servidor proxy remite dicha respuesta al cliente de la red interna.

De esta forma estamos creando un aislamiento absoluto, creando comunicación directa entre la red interna y la red externa. En el dialogo entre cliente y servidor proxy se evalúan las peticiones de los clientes de la red interna y se decide aceptarlas o rechazarlas en base a un conjunto de reglas, examinando meticulosamente que los paquetes de datos sean en todo momento correctos.

Ventajas:

- Detallados registros de trafico (ya que pueden examinar la totalidad del paquete de datos).
- Servicio de autenticación
- Nula vulnerabilidad que presentan ante ataques de suplantación (spoofing)
- Servicios añadidos: como cache y filtro de URL´s.

Inconvenientes:

- Menor velocidad de inspección
- Necesidad de contar con servicios específicos para cada tipo distinto de trafico
- Imposibilidad de ejecutar muchos otros servicios en él (puesto que escucha en los mismos puertos)

Reglas de filtrado

Los cortafuegos funcionan filtrando las comunicaciones en ambos sentidos entre su interfaz interna (la que lo conecta a su red) y la externa.

El mecanismo de funcionamiento para realizar este filtrado es a través de una lista de reglas.

Las reglas, pueden ser de dos tipos: de **aceptación** y de **rechazo**. Y el rechazo se descompone en **rechazo** y **denegación**. (en iptables se corresponde con los argumentos **ACCEPT**, **REJECT** y **DROP**).

La lista de reglas de entrada (del exterior hacia la red) es totalmente independiente de la lista de reglas de filtrado de salida (de la red hacia el exterior). Las distintas listas de reglas se llaman cadenas (**chains**).

Cuando un cortafuegos **rechaza** una petición externa, envía una respuesta negativa diciendo que no acepta la comunicación, por el contrario, si **descarta** una petición, no envía ningún tipo de respuesta, es decir, que el agente externo que intento establecer contacto, no sabrá siquiera si la maquina existe o esta apagada.

Políticas de cortafuegos

Hay dos políticas básicas en la configuración de un cortafuegos:

- Política restrictiva: se deniega todo el trafico excepto el que esta explícitamente permitido. El cortafuegos obstruye todo el trafico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suele utilizar las empresas y organismos gubernamentales.
- Política permisiva: se permite todo el trafico excepto el que esta 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 mas segura, ya que es más difícil permitir por error trafico potencialmente peligroso, mientras que en la política permisiva es posible que no haya contemplado algún caso de trafico peligroso y sea permitido por omisión.

Cortafuegos de filtrado de paquetes

El modelo de cortafuegos mas antiguo consiste en un dispositivo capaz de filtrar paquetes, lo que denomina **choke**.

Esta 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.

Los cortafuegos de filtrado de paquetes utilizar una técnica de filtrado, que consiste en una lista de ordenes ejecutadas secuencialmente a la entrada/salida de cada paquete en las interfaces de un Router, con las opciones de permitir o bloquear, por ejemplo: iptables en linux y ACL en Cisco.

Esta arquitectura es la mas simple de implementar y la mas 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.

Ventajas:

- Disponible en casi cualquier Router y en muchos sistemas operativos
- Ofrece un alto rendimiento para redes con una carga de tráfico elevada
- Necesita pocos recursos
- Es fácil añadir nuevos protocolos o aplicaciones

Inconvenientes:

- Las reglas de filtrado pueden llegar a ser complejas de establecer y, por lo tanto, se hace difícil comprobar su corrección
- Al procesar los paquetes de forma independiente, no se guarda ninguna información de contexto (no se almacenan históricos de cada paquete), ni se puede analizar a nivel de capa de aplicación, dado que esta implementado en los routers
- No disponen de un sistema de monitorización sofisticado
- No disponen de un sistema de monitorización sofisticado
- Es difícil de manejar la autenticación y autorización

Cortafuegos DUAL-HOMED host

Una dual-homed host architecture esta construida un ordenador con dos tarjetas de red.

Este host es capaz de enrutar paquetes IP desde una red a otra. Pero los paquetes IP de una red a la otra no son enrutados directamente. El sistema interno al firewall puede comunicarse con el dual-homed host, y los sistemas fuera de firewall también pueden comunicarse con él, pero los sistemas no pueden comunicarse directamente entre ellos

También es necesario que el IP forwarding este deshabilitado en el equipo: aunque una maquina con dos tarjetas puede actuar como un Router, para aislar el tráfico entre la red interna y la externa es necesario que no se enruten paquetes entre ellas.

Así, los sistemas externos ´verán´ al host a través de una de las tarjetas y los internos a través de la otra, pero entre las dos partes no puede existir ningún tipo de trafico que no pase por el cortafuegos.

Cortafuegos screened subnet (DMZ)

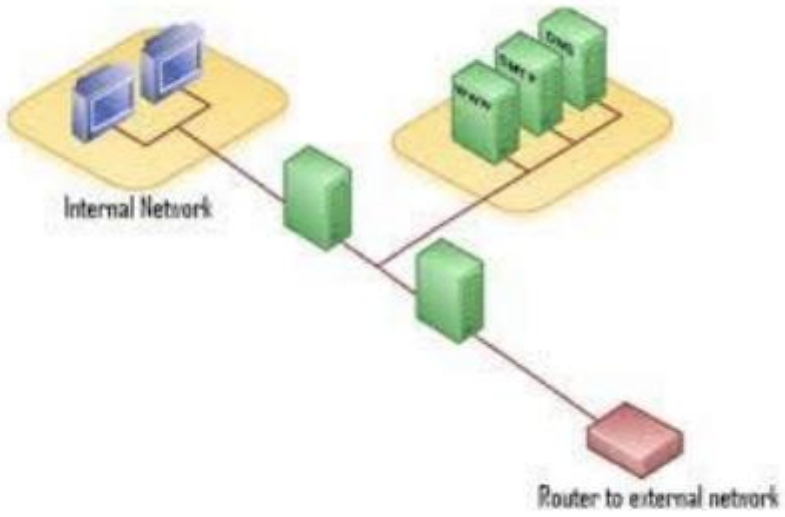
La arquitectura screened subnet también se conoce con el nombre de red perimetral o de-militarized zone (dmz)

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.

Se crea una red aislada utilizando dos routers. Todos los hosts pueden acceder a la red intermediaria pero no la pueden atravesar directamente.

La arquitectura DMZ intenta aislar la maquina bastión en una red perimétrica, de forma que si un intruso accede a esta maquina no consigue un acceso total a la subred protegida.



Se emplean dos Routers, exterior e interior, ambos conectados a la red perimetral donde se incluye el host bastión. También se podrían incluir sistemas que requieran el 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 trafico no deseado en ambos sentidos, es decir, tanto hacia la red perimetral como hacia la red externa.

El Router interior bloquea el trafico no deseado tanto hacia la red perimetral como hacia la red interna. De este modo, para atacar la red protegida se tendría que romper la seguridad de ambos routers.

Para obtener un mayor nivel de seguridad, se pueden definir varias redes perimetrales en serie, cada una con diferentes reglas e filtrado. Situando los servicios que requieran de menor fiabilidad en las redes mas 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.

Cortafuegos. Otras arquitecturas

Alternativa 1: emplear un host bastión distinto para cada protocolo o servicio en lugar de un único host bastión. Como inconveniente se tiene la cantidad de máquinas necesarias para implementar el cortafuegos

Alternativa 2: un único bastión, per distintos servidores proxy para cada uno de los servicios ofrecidos

Alternativa 3: división de la red interna en diferentes subredes, situando cortafuegos internos entre dichas zonas y la red exterior. Aparte de incrementar la seguridad, los firewalls internos son específicamente recomendables en zonas de la red desde la que no se permite a priori la conexión con internet.