Cortafuegos (Firewall)

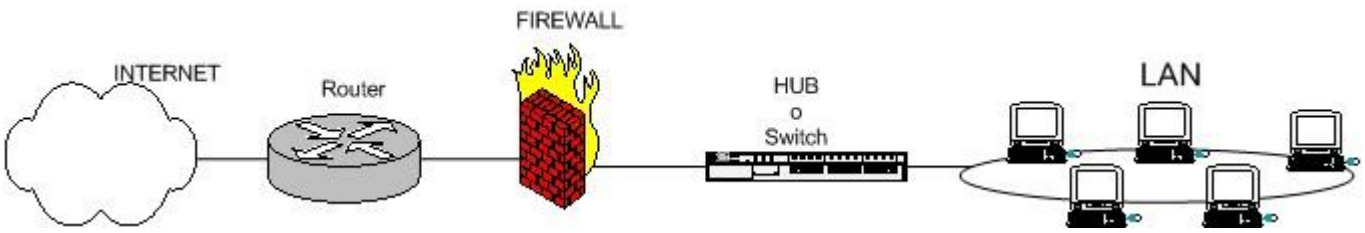
Arquitecturas de cortafuegos

Juan Nieto González
– IES A Carballeira -

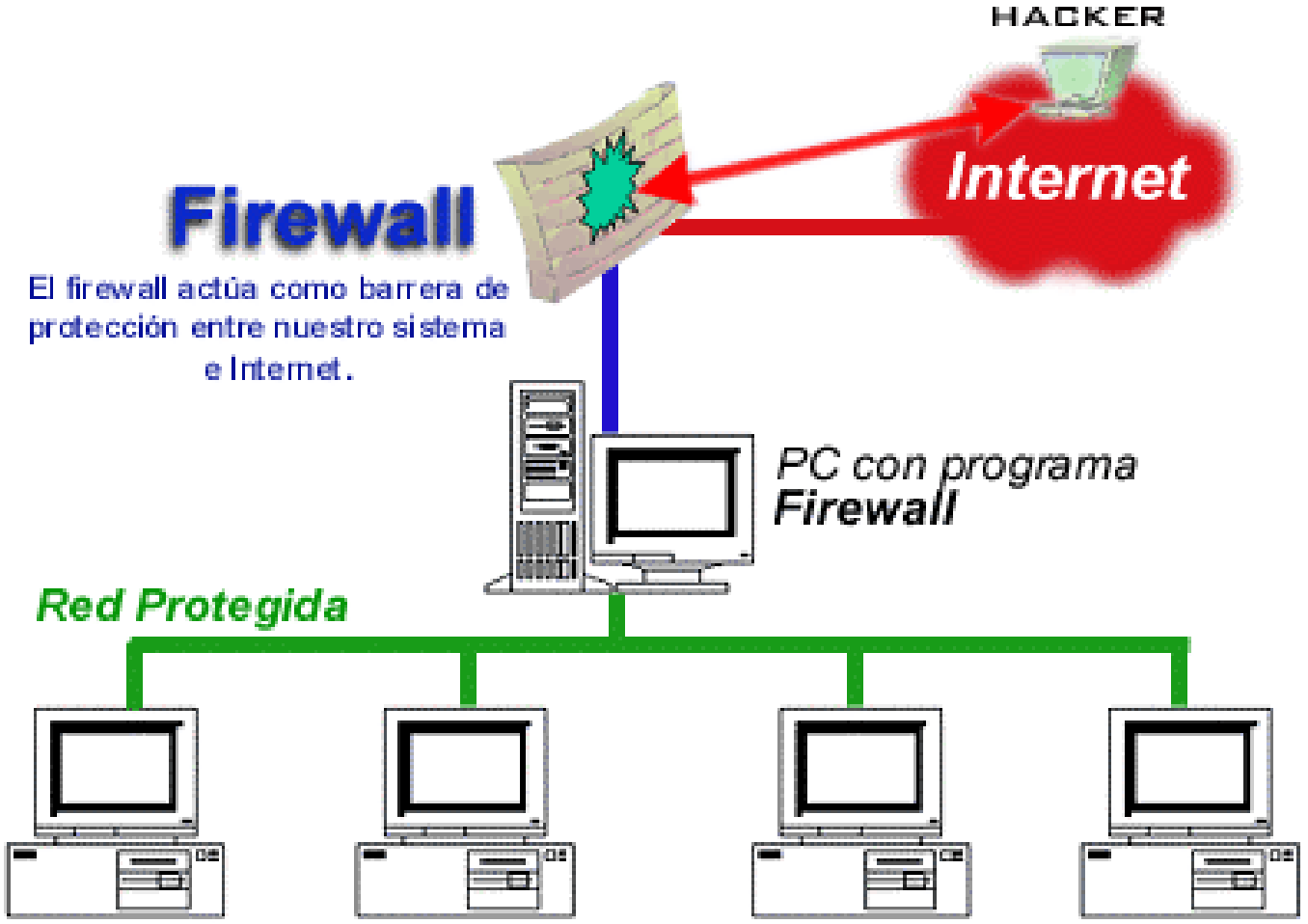
ÍNDICE

1.a- ¿Qué es un firewall ?

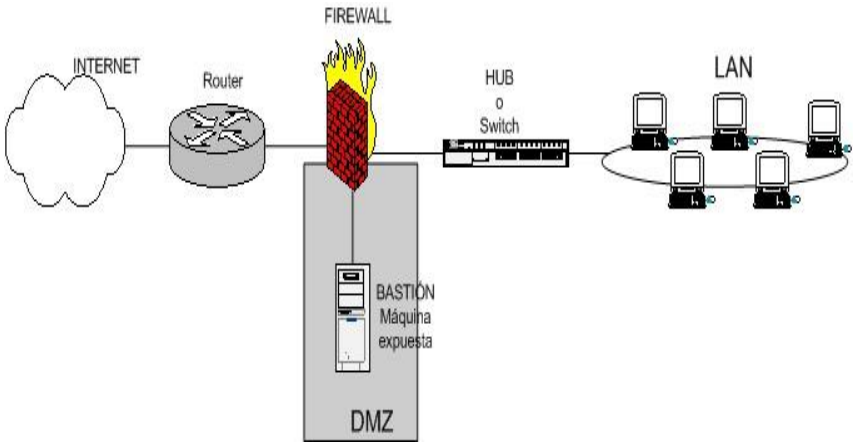
- Un firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos.
- El firewall puede ser un **dispositivo físico** o un **software** sobre un sistema operativo.
- En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no.
- Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT.

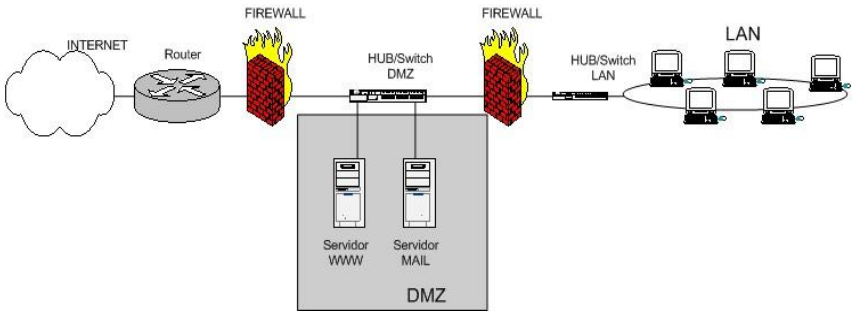


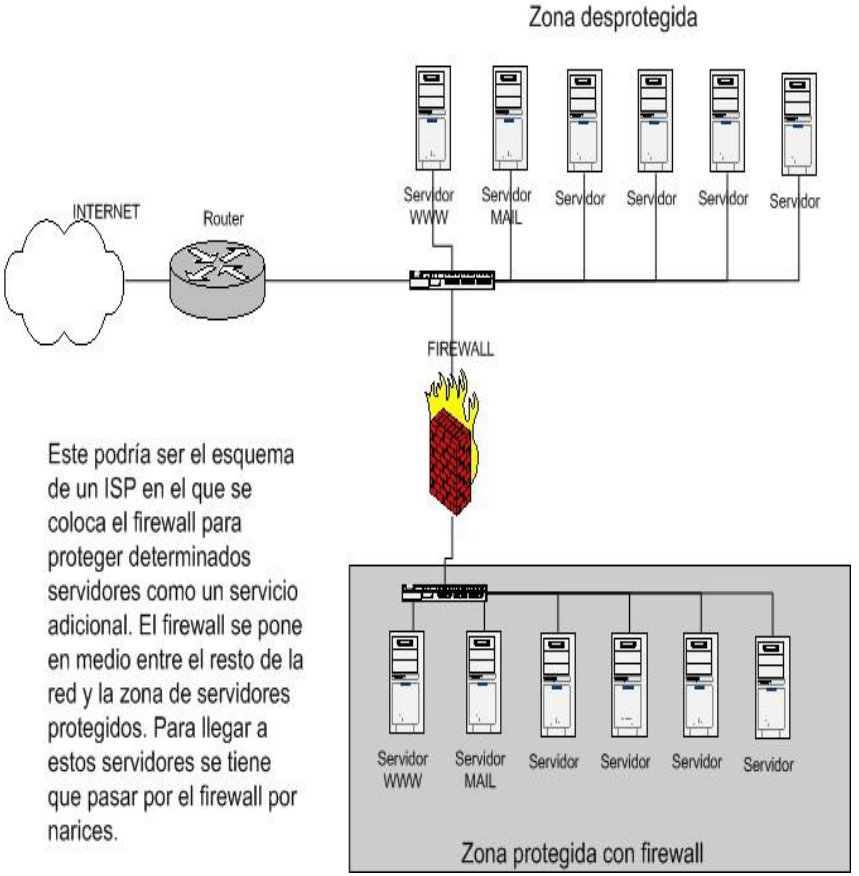
1.B ¿Para qué quiero un cortafuegos?



1.c No todos los sistemas requiren la misma configuración







Este podría ser el esquema de un ISP en el que se coloca el firewall para proteger determinados servidores como un servicio adicional. El firewall se pone en medio entre el resto de la red y la zona de servidores protegidos. Para llegar a estos servidores se tiene que pasar por el firewall por narices.

1.D Funcionamiento de los cortafuegos I

- TODOS funcionan empleando reglas
- Existen dos tipos de políticas “por defecto”
  - Aceptar todo tráfico – tendremos que eliminar el tráfico que no interese
  - Rechazar todo el tráfico – aceptaremos lo que queramos
- En una red “seria” debemos emplear siempre el segundo método.Por defecto bloqueamos todo el tráfico, tanto entrante como saliente, y sólo permitiremos aquél que nos interese.

1.D Funcionamiento de los cortafuegos II

Un caso práctico en pseudolenguaje:

- Politica por defecto ACEPTAR.
- Todo lo que venga de la red local al firewall ACEPTAR
- Todo lo que venga de la ip de mi casa al puerto tcp 22 ACEPTAR
- Todo lo que venga de la ip de casa del jefe al puerto tcp 1723 ACEPTAR
- Todo lo que venga de hora.rediris.es al puerto udo 123 ACEPTAR
- Todo lo que venga de la red local y vaya al exterior ENMASCARAR
- Todo lo que venga del exterior al puerto tcp 1 al 1024 DENEGAR
- Todo lo que venga del exterior al puerto tcp 3389 DENEGAR
- Todo lo que venga del exterior al puerto udp 1 al 1024 DENEGAR

- Habilita el acceso a puertos de administración a determinadas IPs privilegiadas.

- Enmascara el trafico de la red local hacia el exterior (NAT, una petición de un pc de la LAN sale al exterior con la ip pública), para poder salir a Internet
- Deniega el acceso desde el exterior a puertos de administración y a todo lo que este entre 1 y 1024.

2.- Tecnologías de Firewall

- 2.1 Filtros de paquetes
- 2.2 Puertas de enlace de aplicación
- 2.3 Puertas de enlace del nivel de circuito
- 2.4 Inspección de paquetes con estado

2.1 Filtros de paquetes

- Se basan en establecer reglas para permitir/denegar IP, puertos de E/S.

- Realizan un enrutamiento rápido, pero muy simple, se puede colar por los puertos abiertos “cualquier” tráfico. (por ejemplo un emule por un puerto 80)

2.2 Puertas de enlace de aplicación (I)

- Trabajan en el nivel de aplicación del modelo TCP/IP, por esto son capaces no sólo de trabajar con determinados protocolos, sino que son capaces de analizar el tráfico para ver:
  - si dicho tráfico se corresponde con el servicio (lo que pasa por el puerto 80, p.e. se corresponde con el protocolo http)
  - permitir/denegar determinadas instrucciones o servicios de dicho protocolo (rechazar un put del protocolo FTp)

2.2 Puertas de enlace de aplicación (II)

- Funcionamiento: establecen un punto intermedio, haciéndose pasar por el cliente para el servidor y por un servidor para el cliente, de manera totalmente transparente.
- ***Es el más exhaustivo de todos***, requiere mucha máquina y puede tener problemas con inundación SYN y PING, además para aplicaciones no estándar (desarrolladas o por, o para nosotros) puede ser mucho más difícil de configurar

2.3 Puertas de enlace de nivel de circuito

- Serían el equivalente a un Proxy

2.4 Inspección de paquetes con estado

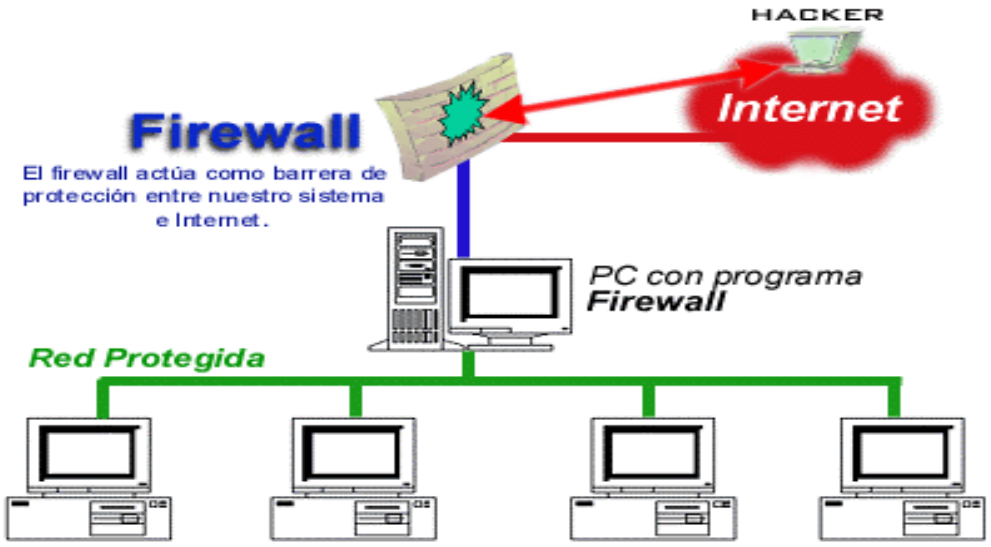
- Su acrónimo procede del inglés SPI (Stateful Packet Inspection).
- Son una mezcla de los dos primeros.
- Funcionamiento:
  - **Por un lado, filtran los paquetes en función de protocolos**
  - **Controlan el estado de las conversaciones**, (p.e. si alquien desde fuera intenta simular una trama perteneciente a una conversación previamente establecida, consultaría en su BD si los números de secuencia se corresponden con alguna Existente, sino es así lo rechazaría, a diferencia de los filtros de paquetes que tan sólo comprobaría la existencia o no del bit SYN.
- Sistema muy empleado ya que es rápido y permite bastantes comprobaciones

3. Métodos de implementación del Cortafuegos

- 3.1 De Red basados en Host
- 3.2 Basados en enrutadores
- 3.3 Basados en Host
- 3.4 Firewall de equipos

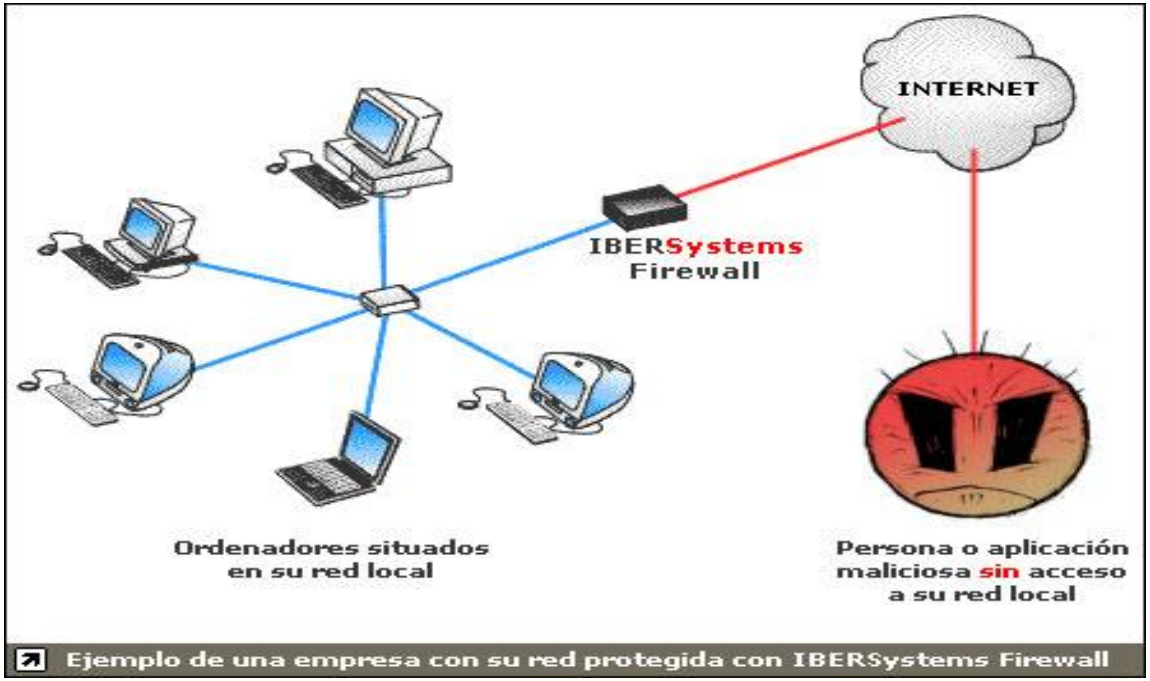
3.1 De Red basados en host

- Existen dos métodos para implementar este sistema:
  - **Una aplicación** que corre sobre un SO existente, Win Nt/2000/2003, Sun Solaris y HPUX generalmente. Para una instalación se suele "asegurar" previamente el SO eliminando servicios/demonios innecesarios, esta tarea a veces la hace la propia aplicación y otras aplicaciones de terceros
  - **Integrado en el propio SO** generalmente basadas en UNIX, construyen un SO que integra todas las capacidades, lo que lo suele hacer más seguro pero requiere un aprendizaje adicional



3.2 Basados en enrutadores

- En redes pequeñas que no pueden costearse otros sistemas, realizan un filtrado de paquetes.
- En otras redes constituyen el primer filtro realizando parte del trabajo que debería realizar el firewall al eliminar las primeras tramas.



Ejemplo de una empresa con su red protegida con IBERSystems Firewall

3.3 Basados en Host

- Para asegurar entre 1 y 5 host.
- En redes pequeñas, son únicamente una aplicación.
- En redes mayores al no ofrecer control centralizado no suelen emplearse.
- Otro uso es asegurar los ordenadores que se conectan desde nuestra casa al centro de trabajo.
- En cualquier caso, todos los host de una empresa deberían tener implementado un cortafuegos individual.

3.4 Firewall de equipos

- Son dispositivos que integran software y hardware propio para realizar esta función.
- Los hay desde muy económicos para entornos SOHO (oficina pequeña o doméstica) hasta para trabajar en entornos con múltiples Gigabit Ethernet.

Bibliografía

- “Firewalls” Manual de referencia Mc Graw-Hill
- Imágenes presentación:
  - www.infospyware.com
  - www.eitd.net
  - www.ibersystems.es
  - www.javiersanchez.es
- Imágenes y texto:
  - www.pello.info