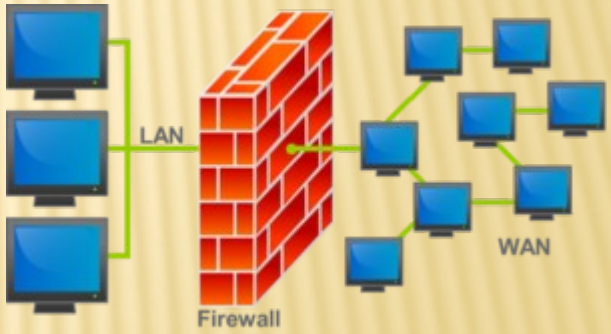
CORTAFUEGOS

QUE ES CORTAFUEGOS?

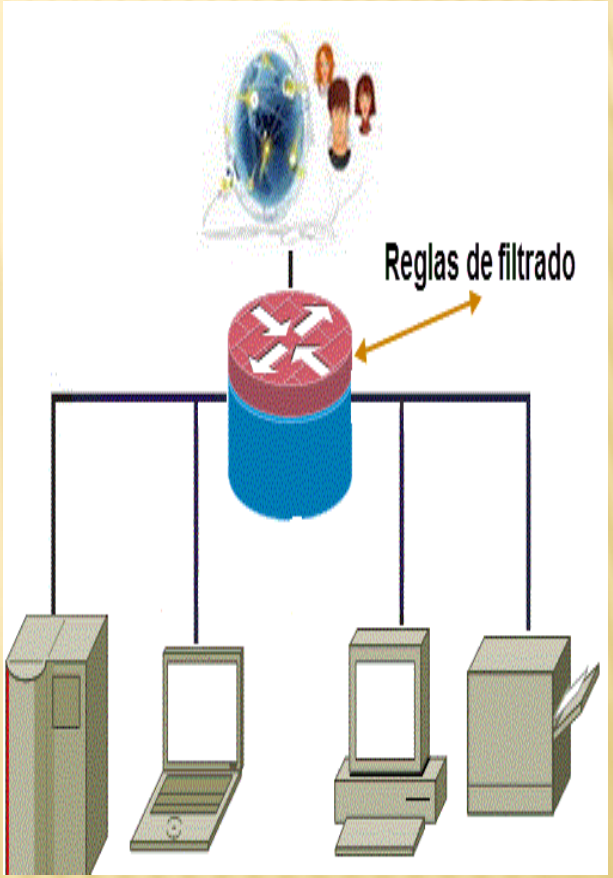
- Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- Los cortafuegos pueden ser implementados en hardware o software,
- Examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados



HISTORIA CORTAFUEGOS

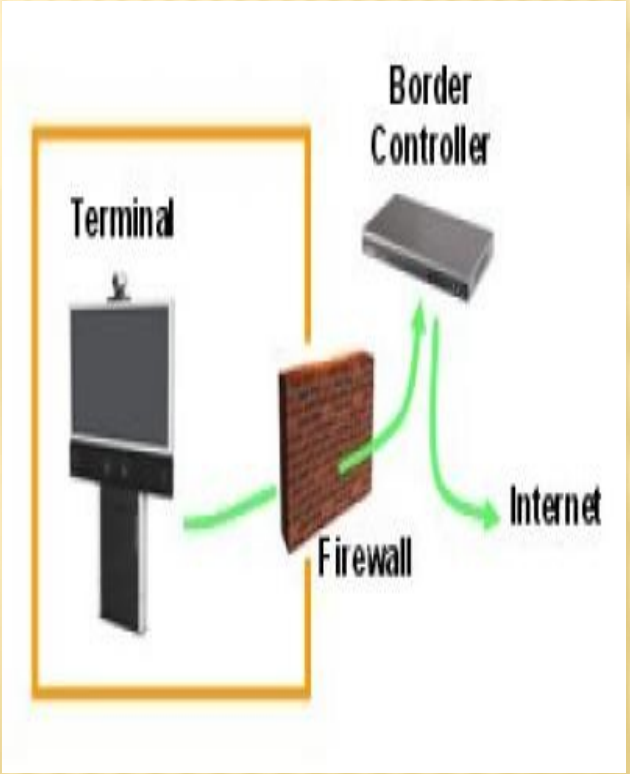
CORTAFUEGO DE RED: FILTRADO DE PAQUETES

- 1988: Fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet.
- El filtrado de paquetes actúa mediante la inspección de los paquetes, Si un paquete coincide con el conjunto de reglas del filtro, el paquete se reducirá o será rechazado.
- Se filtra cada paquete basándose únicamente en la información contenida en el paquete en sí.



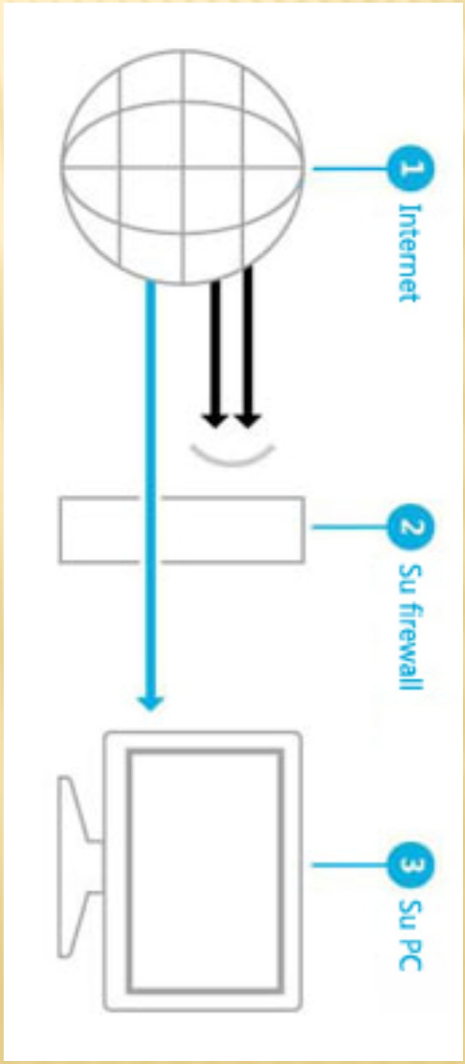
CORTAFUEGOS DE ESTADO

- 1989 y 1990: 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



CORTAFUEGOS DE APLICACIÓN

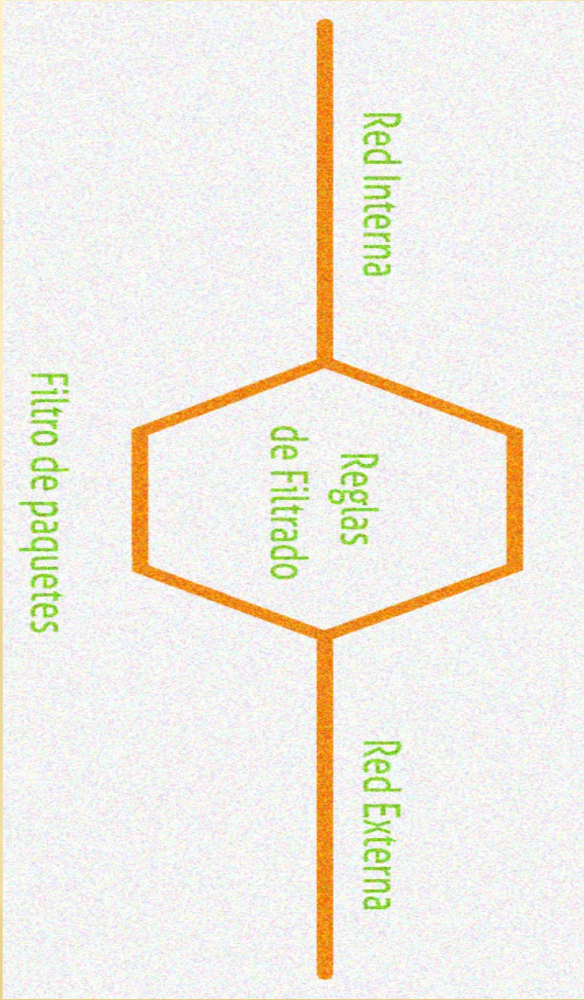
- Son aquellos que actúan sobre la capa de aplicación.
- Permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.
- Es mucho mas seguro que el cortafuego de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI.
- Puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP



TIPOS DE CORTAFUEGO

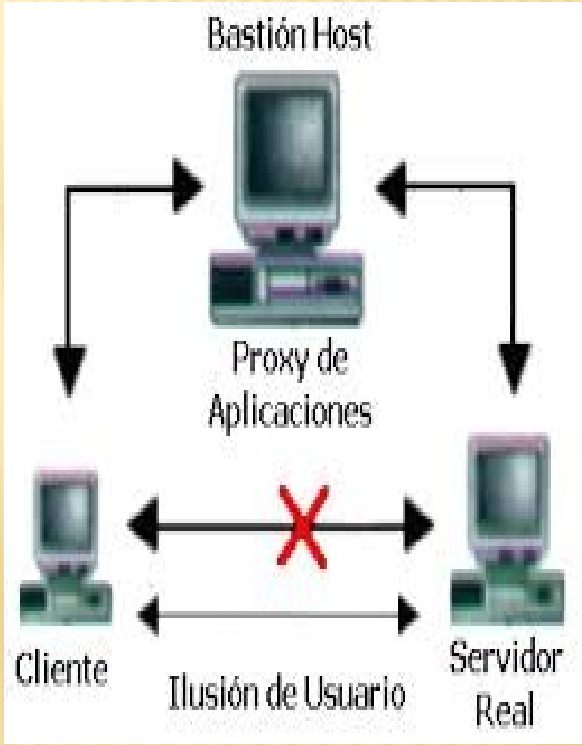
FILTRADO DE PAQUETES

- El Router es el encargado de filtrar los paquetes:
  - Protocolos utilizados
  - Dirección IP de origen y de destino
  - Puerto TCP/UDP de origen y de destino
- 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.
- Trabaja en los niveles de Transporte.



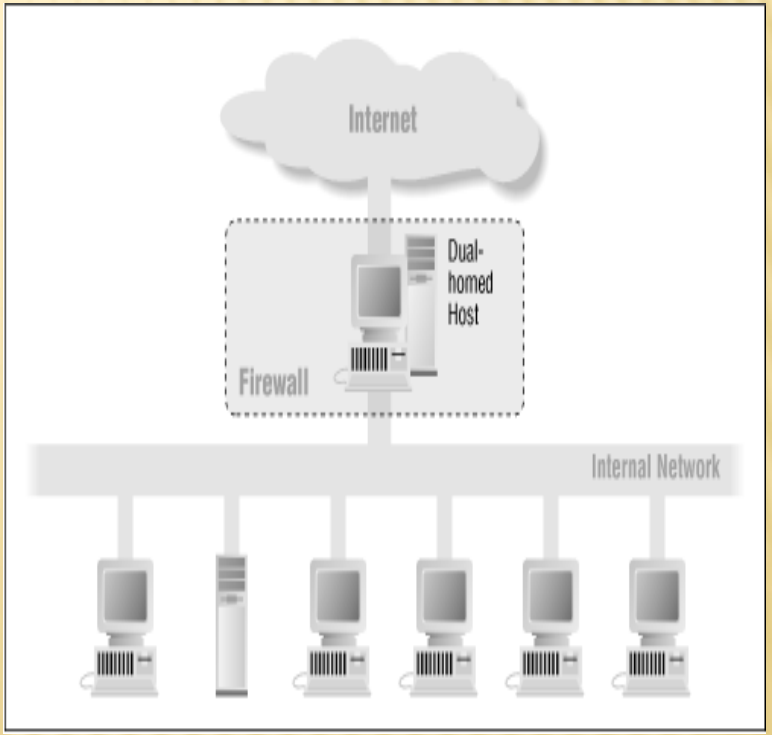
PROXY Y GATEWAYS DE APLICACIONES

- Actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.
- Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente.
- Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.



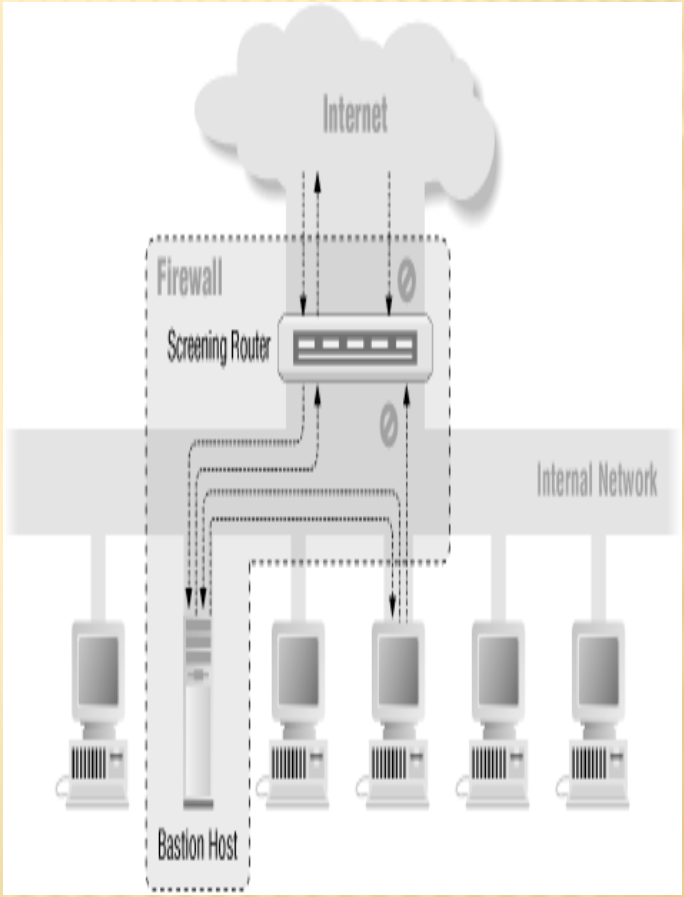
DUAL HOMED HOST

- Son dispositivos que están conectados a ambos perímetros y no dejan pasar paquetes IP.
- Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre este y el usuario interior.



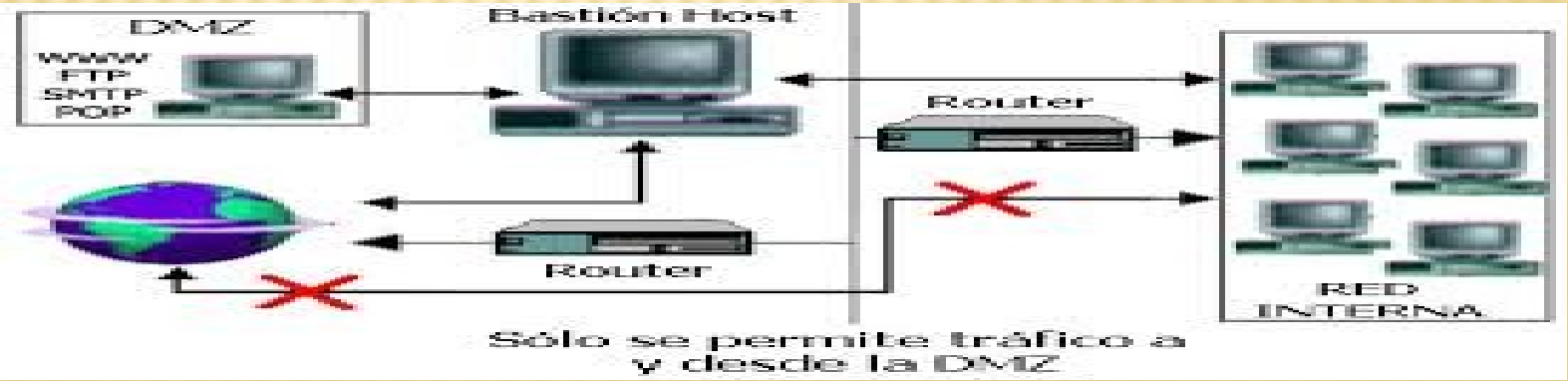
SCREENED HOST

- Se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes
- En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.



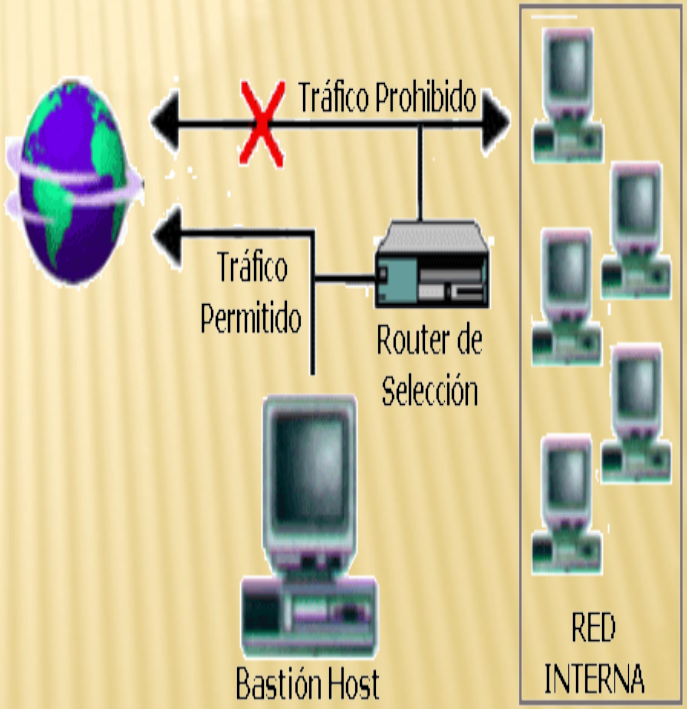
SCREENED SUBNET

- Aisla la máquina más atacada y vulnerable del Firewall.
- Si un intruso accede a esta máquina no consiga el acceso total a la subred protegida.
- Se utilizan dos Routers, uno exterior y otro interior.
- El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa.
- El Router interior hace lo mismo con la red interna y la DMZ



RESTRICCIONES EN EL FIREWALL

- Usuarios internos con permiso de salida para servicios restringidos, estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
- Usuarios externos con permiso de entrada desde el exterior, usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.



BENEFICIOS DE UN FIREWALL

- Los Firewalls manejan el acceso entre dos redes, y si no existiera, todos las computadoras de la red estarían expuestos a ataques desde el exterior.
- El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.
- Llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido más en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

LIMITACIONES DE UN FIREWALL

- El hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso.
- No son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar.
- "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.
- NO protege de la gente que está dentro de la red interna.