

Buy Malwarebytes®

#1 Malware Removal Tool. Get Rid of Viruses & Spyware - Buy Now!



# Tipos de Firewall - Filtrado de Paquetes

[volver](#)

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 autenticación de usuarios y control de accesos con horarios prefijados.

[volver](#)