

Buy Malwarebytes®

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



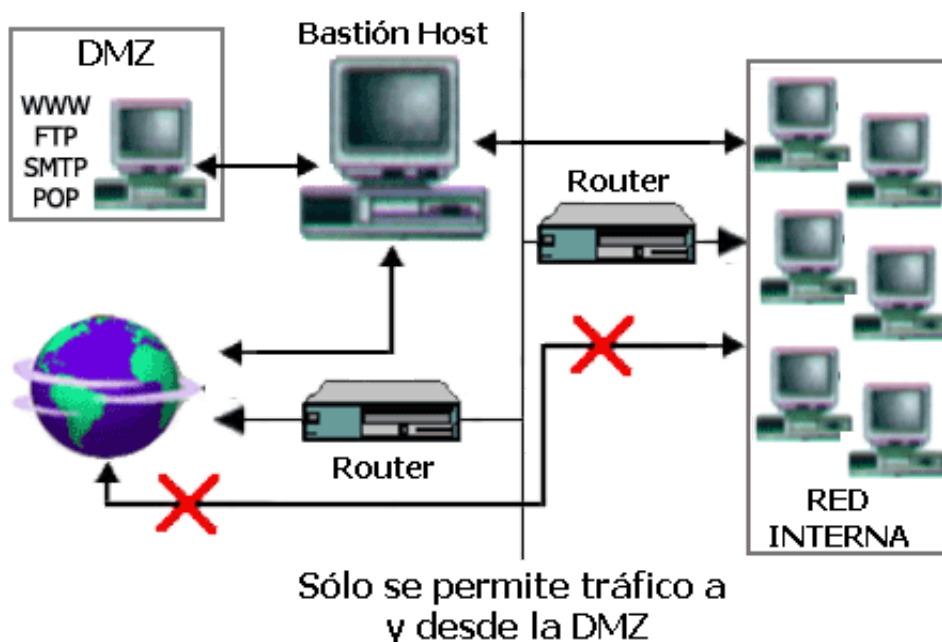
Tipos de Firewall - Screened Subnet

[volver](#)

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema 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 (zona entre el Router externo y el interno).

Es posible definir varias niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.



Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separados de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa.

Los sistemas Dual-Homed Host y Screened pueden ser complicados de configurar y comprobar, lo que

puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

[volver](#)