Auditoria en seguridad informática

IFCT0109 – Seguridad informática

MF0487_3 (90 horas)

Descripción de los aspectos sobre cortafuegos en auditorías de sistemas informáticos

- Introducción
- Principios generales de cortafuegos
- Componentes de un cortafuegos de red
- Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
- Arquitecturas de cortafuegos de red
- Otras arquitecturas de cortafuegos de red
- Resumen

Introducción

Uno de los aspectos fundamentales de las auditorías de los sistemas de información es la evaluación de su nivel de seguridad. Este grado de seguridad no solo debe considerar las vulnerabilidades de las aplicaciones instaladas en los equipos, sino que también debe abarcar una serie de medidas que intenten bloquear la entrada de ataques que puedan afectar a la información.

Tanto si los ataques afectan levemente a la información como si tienen efectos devastadores sobre el sistema, es necesario implantar un sistema de protección que detecte los posibles atacantes y que evite y prevenga su entrada. Una de las medidas más eficientes y utilizadas para esto es la implantación de cortafuegos de red.

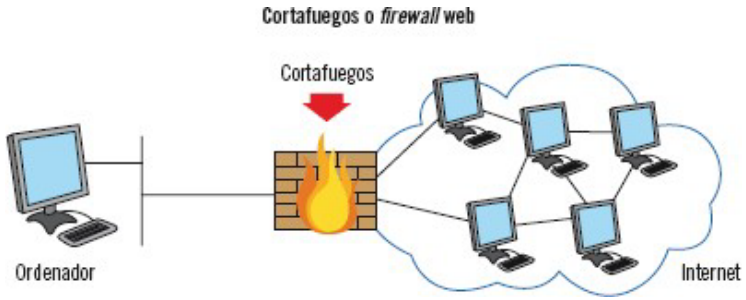
En este capítulo, se describen los distintos tipos de cortafuegos junto con sus componentes, utilidades y arquitecturas principales.

Principios generales de cortafuegos

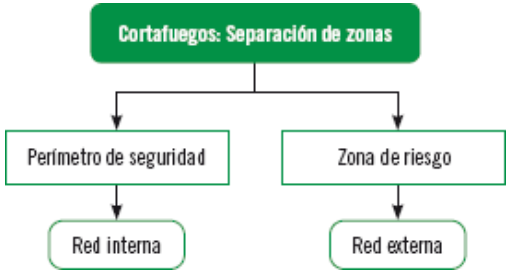
Principios fundamentales de los cortafuegos

Cortafuegos: Un cortafuegos es un sistema de seguridad que se utiliza para proteger las redes de información. Su función principal es establecer una barrera entre la red local (la red interna de una organización) y la red exterior (generalmente Internet) para prevenir ataques y mejorar la seguridad de la organización.

Perímetro de seguridad: El perímetro de seguridad es el espacio que está protegido por el cortafuegos. Este espacio generalmente es propiedad de la organización y corresponde a su red interna. Es decir, es la red que la organización quiere proteger de posibles amenazas externas.



Zona de riesgo: La zona de riesgo es la red contra la cual se protege el perímetro de seguridad. En la mayoría de los casos, esta red es Internet, ya que es la principal fuente de amenazas y ataques a la seguridad de la información.



Principios generales de cortafuegos

Principios fundamentales de los cortafuegos

Objetivos del cortafuegos:

- Establecer un enlace controlado: El cortafuegos establece un enlace controlado entre la red interna y la red externa. Esto significa que todo el tráfico que pasa entre estas dos redes debe pasar a través del cortafuegos, lo que permite al cortafuegos inspeccionar y controlar este tráfico.
- Proteger la red interna: El cortafuegos protege la red interna de posibles ataques e intrusiones procedentes de la red externa. Esto se logra mediante una variedad de técnicas de seguridad, como la inspección de paquetes, la filtración de IP, la prevención de intrusiones, entre otras.
- Establecer un punto único de defensa: El cortafuegos actúa como un punto único de defensa contra las amenazas de seguridad. Al concentrar la seguridad en un solo punto, la organización puede maximizar tanto la conectividad como la seguridad del sistema. Esto también facilita la gestión de la seguridad, ya que todas las decisiones de seguridad y todas las actividades de registro y monitoreo se centralizan en un solo lugar.

Principios generales de cortafuegos

Principios fundamentales de los cortafuegos

Características de diseño de un cortafuegos

Para maximizar la confiabilidad y eficiencia de un cortafuegos, su diseño e implementación deben ser cuidadosamente considerados, tomando en cuenta todos los aspectos relevantes de la organización.

El diseño de la estructura de un cortafuegos debe perseguir tres objetivos fundamentales:

- Todo el tráfico de datos desde la red interna hacia el exterior debe pasar por el cortafuegos.
- Solo se permitirá pasar a la red local el tráfico autorizado específicamente por la política de seguridad de la organización.
- El cortafuegos debe ser inmune a posibles intrusiones, mediante la utilización de sistemas confiables y de sistemas operativos seguros.

Aparte de los objetivos, el diseño del cortafuegos debe contemplar los siguientes servicios de control de accesos:

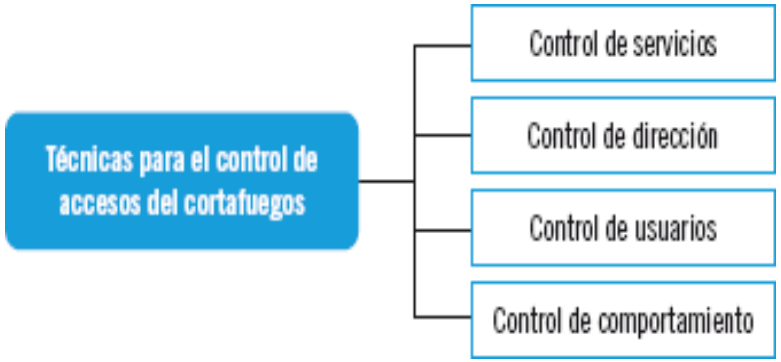
- Control de servicios: establece qué tipo de servicios de la organización son accesibles desde las redes internas y externas
- Control de dirección: establece las direcciones de entrada y salida en las que se permitirá el tráfico de datos desde/hacia la red externa.
- Control de usuarios: establece controles de acceso para determinar a qué servicios puede acceder cada usuario.
- Control de comportamiento: establece el uso concreto de ciertos servicios particulares.

Principios generales de cortafuegos

Principios fundamentales de los cortafuegos

Características de diseño de un cortafuegos

Servicios de control de accesos:



Los cortafuegos no protegen de los ataques originados desde dentro la red interna, por lo que es necesario implantar medidas de seguridad adicionales que impidan la expansión de intrusiones internas.

Principios generales de cortafuegos

Principios fundamentales de los cortafuegos

Características de configuración de un cortafuegos:

Política de seguridad:

- Nivel de protección: La organización debe establecer el nivel de protección deseado, que dependerá de la utilización de la red y las características de los usuarios.
- Tipo de política: Se puede elegir entre una política restrictiva (denegar todo lo que no se permite) o una política permisiva (permitir todo lo que no se deniega).

Monitorización:

- Grado de control: La organización debe definir el grado de monitorización y control que desea establecer sobre el tráfico de red.
- Herramientas de monitorización: Existen diferentes herramientas disponibles para monitorizar el cortafuegos, como registros, alertas y análisis de tráfico.

Economía:

- Valor de los activos: El coste del cortafuegos dependerá del valor de los activos que se desea proteger.
- Costes de implantación y mantenimiento: Se deben considerar tanto los costes de instalación como los costes de mantenimiento a lo largo de la vida útil del cortafuegos.

La decisión sobre qué tipo de cortafuegos implantar debe basarse en un equilibrio entre la seguridad, la monitorización y la economía. Es importante tener en cuenta que una inversión en un cortafuegos de alta calidad puede ayudar a proteger la organización de ataques costosos.

Componentes de un cortafuegos

Mecanismos de protección en un cortafuegos

Una vez definidas las características principales del cortafuegos, es necesario seleccionar los mecanismos de protección que se van a incorporar para cumplir con las políticas de seguridad de la organización.

Los cortafuegos se basan en tres componentes principales sobre los que se implementan estos mecanismos:

- Filtrado de paquetes: Se utiliza para controlar el flujo de datos entrante y saliente, permitiendo solo el tráfico legítimo.
- Proxy de aplicación: Actúa como intermediario entre las aplicaciones de la red interna y las externas, controlando el acceso y protegiendo la privacidad.
- Monitorización de la actividad: Registra y analiza el tráfico de red para detectar y prevenir intrusiones o actividades maliciosas.

Componentes de un cortafuegos

Mecanismos de protección en un cortafuegos

Filtrado de paquetes:

El filtrado de paquetes es una técnica fundamental para controlar el acceso a la red. Se basa en reglas predefinidas que analizan la información de la cabecera de cada paquete, como el protocolo utilizado, la dirección IP de origen y destino, y el puerto de destino.

Tipos de reglas de filtrado:

- Permisivas: Permiten el acceso a la red si se cumplen ciertas condiciones.
- Restrictivas: Deniegan el acceso a la red a menos que se cumplan ciertas condiciones.

Ejemplo de tabla de reglas de filtrado:

IP origen	IP destino	Acción
158.34.0.0	*	Denegar
158.35.0.0	*	Denegar
*	193.23.32.9	Denegar
*	195.45.15.0	Permitir (excepto 158.34.0.0)

En este ejemplo, se deniega el acceso a la red desde las IP 158.34.0.0 y 158.35.0.0, así como a la IP de destino 193.23.32.9.

Se permite el acceso a la IP 195.45.15.0 desde cualquier IP excepto 158.34.0.0.

Componentes de un cortafuegos

Mecanismos de protección en un cortafuegos

Filtrado de paquetes:

Ventajas del filtrado de paquetes:

- Mejora la seguridad de la red.
- Reduce la carga de la red.
- Es fácil de configurar y administrar.

Desventajas del filtrado de paquetes:

- No es infalible. Los atacantes pueden encontrar formas de eludir las reglas de filtrado.
- Puede ser complejo de configurar para redes complejas.

La correcta definición de las reglas de filtrado de tramas es fundamental. Si se definen reglas incorrectamente, se puede incurrir en graves fallos de seguridad por permitir accesos potencialmente peligrosos.

Componentes de un cortafuegos

Mecanismos de protección en un cortafuegos

Proxy de aplicación

Un proxy de aplicación es un tipo de software que actúa como intermediario entre los clientes de una red interna y los servidores externos. El proxy recibe las solicitudes de los clientes, las reenvía al servidor correspondiente y devuelve la respuesta al cliente.

Ventajas:

- Permiso exclusivo de servicios con proxy: El proxy solo permite usar los servicios para los que existe un proxy. Si la pasarela de aplicación solo tiene proxies para protocolos HTTP y FTP, el servicio proxy solo permitirá el uso de los servicios con estos protocolos, denegando el resto de servicios.
- Filtrado de protocolos: El proxy ofrece opciones de filtrado de datos más allá del filtrado por las características de la cabecera del paquete.
- Simplificación de reglas de filtrado: El proxy facilita la tarea de establecer y definir las reglas de filtrado.

Desventajas:

- Necesidad de proxy propio para cada servicio: Cada servicio requiere un proxy específico.
- Mayor coste: Los proxies son más costosos que los filtros de paquetes simples.
- Menor rendimiento: Los proxies tienen menor rendimiento que los filtros de paquetes.
- Cuellos de botella: Los proxies pueden convertirse en cuellos de botella de redes.

Componentes de un cortafuegos

Mecanismos de protección en un cortafuegos

Monitorización de la actividad

La monitorización de la actividad del cortafuegos es crucial para la seguridad de la red, ya que permite:

- Identificar ataques: Detecta intrusiones o intentos de ataque a la red.
- Analizar comportamientos: Observa patrones de tráfico sospechosos para prevenir futuros ataques.
- Obtener información: Ofrece datos sobre el uso de la red y las conexiones realizadas.

Se recomienda registrar información como:

- Estadísticas generales: Tipos de paquetes, direcciones IP, etc.
- Conexiones al sistema: Origen, destino, nombre del usuario, etc.
- Intentos denegados: Protocolos y direcciones IP involucradas.
- Falsificaciones de direcciones: Paquetes externos con direcciones IP internas.

<u>Beneficios:</u>

- Mejora la seguridad: Permite detectar y prevenir intrusiones.
- Ayuda a la resolución de problemas: Facilita la identificación de la causa de problemas de red.
- Proporciona información para auditorías: Permite demostrar el cumplimiento de las normas de seguridad.

Tipos de cortafuegos (por ubicación y funcionalidad)

Existen tres tipos principales de cortafuegos, clasificados según su ubicación y funcionalidad:

- Router con filtrado de paquetes
- Gateway a nivel de aplicación
- Gateway a nivel de circuitos

Routers con filtrado de paquetes

Los routers con filtrado de paquetes son un tipo de cortafuegos que filtran los paquetes IP entrantes basándose en una serie de reglas predefinidas. Según la definición de estas reglas, estos routers pueden descartar el paquete o reenviarlo.

Las ventajas de los routers de filtrado de paquetes incluyen su simplicidad, su invisibilidad para los usuarios y su alta velocidad. Sin embargo, presentan desventajas como la dificultad para definir correctamente las reglas de acceso y la falta de autenticación de los usuarios.

Ventajas	Desventajas
Simple	Dificultad para definir correctamente las reglas de acceso
No visibles para los usuarios	Bajo rendimiento si se pretenden filtrar muchos paquetes
Alta velocidad	No protege contra ataques a nivel aplicación, no requieren autenticación de usuarios

Tipos de cortafuegos (por ubicación y funcionalidad)

Routers con filtrado de paquetes

Son especialmente susceptibles a ciertos tipos de ataques:

- La suplantación de direcciones IP por direcciones internas.

  En este ataque, el atacante falsifica su dirección IP para hacerse pasar por un dispositivo de confianza dentro de la red, como tu ordenador o una impresora. De esta forma, puede acceder a recursos a los que normalmente no tendría acceso. IP-Spoofing

- Los ataques de encaminamiento de fuente.

  Es un tipo de ataque en el que un atacante se sitúa entre dos dispositivos, a menudo un dispositivo de usuario y un servidor, e intercepta o modifica las comunicaciones entre ambos.

  En el contexto de los cortafuegos, este tipo de ataques pueden ser particularmente problemáticos para los routers de filtrado de paquetes. Estos routers, al bloquear ciertas direcciones IP, no pueden impedir los ataques de encaminamiento de fuente. Para solucionar este problema, se aconseja eliminar los paquetes de datos que utilizan esta opción.

- Fragmentos de reducido tamaño.

  Un ataque de fragmentos de reducido tamaño, también conocido en inglés como "Small Fragment Attack", es un tipo de ataque que explota la forma en que los cortafuegos procesan los paquetes de datos.

  En este tipo de ataque, el atacante divide los paquetes de datos en fragmentos muy pequeños. Debido a su tamaño reducido, estos fragmentos pueden pasar desapercibidos por el cortafuegos o pueden consumir una gran cantidad de recursos del cortafuegos al tener que procesar un gran número de pequeños paquetes, lo que puede llevar a una disminución del rendimiento del sistema.

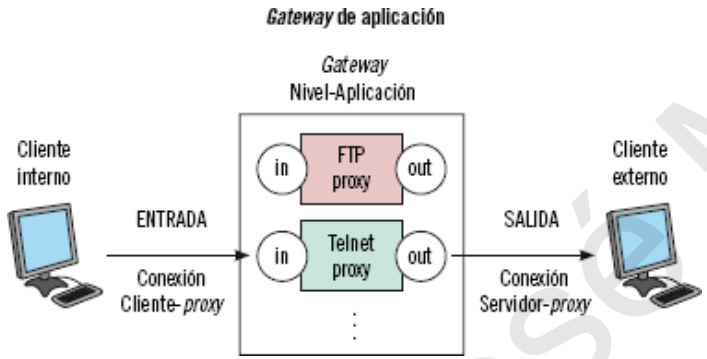
Tipos de cortafuegos (por ubicación y funcionalidad)

Gateways a nivel de aplicación

Los gateways a nivel de aplicación, también conocidos como servidores proxy, son repetidores de tráfico a nivel de aplicación. Cuando un usuario solicita un servicio, lo hace a través del proxy. Este recibe la petición, realiza el pedido al servidor real y devuelve la información solicitada al usuario.

Estos gateways ofrecen una mayor seguridad que los routers de filtrado de paquetes, ya que revisan solo las aplicaciones permitidas y todo el tráfico de red entrante. Sin embargo, pueden provocar cuellos de botella debido al exceso de procesamiento en cada conexión. Esto se debe a que el proxy debe actuar como intermediario entre tu dispositivo y la aplicación, lo que añade una capa adicional de procesamiento que puede ralentizar la comunicación.

A diferencia de los servidores proxy tradicionales que funcionan a nivel de red y manejan el tráfico de manera más eficiente, los proxies de aplicación necesitan procesar individualmente cada solicitud realizada a través de la aplicación específica



Ventajas	Desventajas
Mayor seguridad que routers de filtrado de paquetes	Cuellos de botella por sobrecarga de procesamiento en cada conexión
Sólo revisa las aplicaciones, servicios, permitidos. Aumento de eficacia.	
Revisa todo el tráfico de red entrante y evita el tráfico directo entre redes	

Tipos de cortafuegos (por ubicación y funcionalidad)

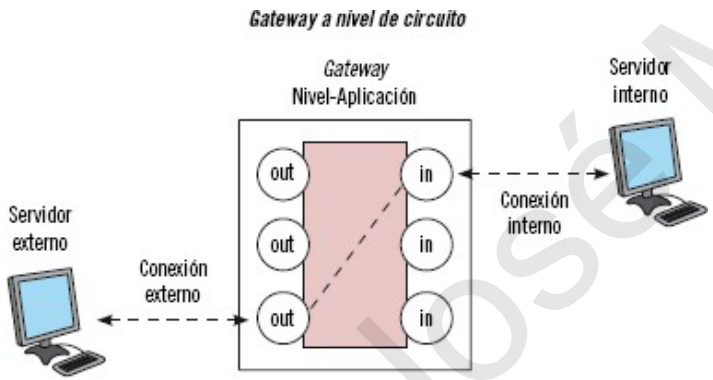
Gateways a nivel de circuito

Los gateways a nivel de circuito son sistemas que redirigen los paquetes de datos una vez que se ha establecido y validado la conexión. Estos gateways permiten determinar una política restrictiva que permite cerrar y abrir puertos solo cuando sea estrictamente necesario.

A diferencia de un firewall tradicional que analiza paquetes de datos individuales, un gateway a nivel de circuito analiza las sesiones de comunicación establecidas entre dispositivos y verifica los puertos de origen y destino utilizados, los protocolos de comunicación empleados y La validez de la sesión

En base a las reglas de seguridad predefinidas, el gateway permite o deniega el establecimiento o continuación de la sesión.

En resumen, los gateways a nivel de circuito ofrecen una capa adicional de seguridad al controlar las conexiones establecidas entre dispositivos en lugar de analizar paquetes de datos individuales.



Ventajas	Desventajas
Mayor seguridad al analizar sesiones en lugar de paquetes individuales.	No analiza el contenido individual de los paquetes.
Facil gestión. Se definen políticas a nivel de sesión y no en base a paquetes.	Mayor latencia, por inspección de las sesiones, por el procesamiento
Alta velocidad	Poco flexible en la adaptación a aplicaciones y protocolos nuevos.

Tipos de cortafuegos (por ubicación y funcionalidad)

Host bastion

El host bastion es un punto crítico del sistema en la seguridad de la red identificado por el administrador del cortafuegos. Aunque **no es un tipo de cortafuegos en sí**, es importante mencionarlo debido a su relevancia en la estrategia de seguridad de la red.

Se trata de un servidor altamente fortificado ubicado en un punto crítico de la red, configurado para:

- Atraer y resistir intentos de ataques informáticos
- Actuar como plataforma para ejecutar servicios seguros como gateways a nivel de aplicación o a nivel de circuito.

En resumen, un host bastión funciona como una capa adicional de defensa, centralizando los servicios vulnerables en un sistema fuertemente protegido para minimizar el riesgo de ataques exitosos a la red interna de una organización

Arquitecturas de cortafuegos de red

Introducción

Las arquitecturas de cortafuegos de red van más allá de los simples routers con filtrado de datos o gateways. Ofrecen mayor seguridad al combinar estos elementos con bastiones para un bloqueo más eficaz de datos potencialmente peligrosos.

Las arquitecturas complejas más comunes son:

- Dual-homed host
- Screened host
- Screened Subnet (DMZ)

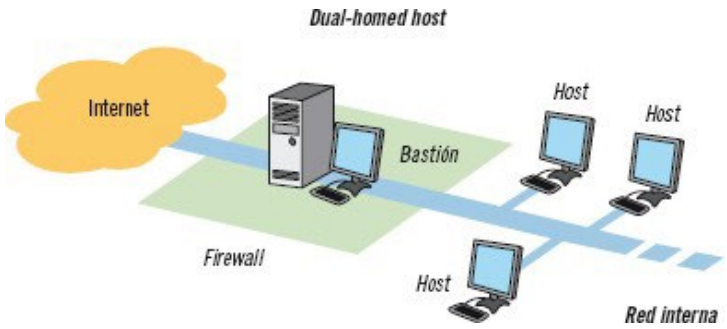
Arquitecturas de cortafuegos dual-homed host

Las arquitecturas dual-homed host ofrecen mayor protección que los cortafuegos simples. Y se caracterizan por:

- Dos tarjetas de red: una para la red interna y otra para la externa.
- Mayor seguridad: el tráfico entre Internet y la red interna debe pasar por el host bastion.
- Servidor proxy: necesario para cada servicio que se desee pasar por el firewall.

Existen dos formas de ofrecer los servicios del host bastión:

- Cuentas de usuario: los usuarios de la red interna acceden al host bastión con sus credenciales. Menos seguro porque depende de la fortaleza de las contraseñas de los usuarios
- Servicios proxy: se ejecuta un servidor proxy para cada servicio permitido. Más seguro porque la seguridad de la red interna no depende de las contraseñas de los usuarios



Arquitecturas de cortafuegos de red

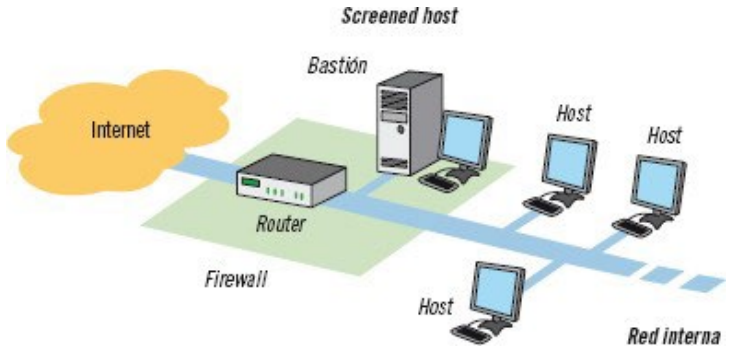
Arquitecturas de cortafuegos con host con pantalla (single-homed host)

Los cortafuegos de host único están formados por dos sistemas de protección que filtran las conexiones a nivel de circuito y aplicación:

- Router con filtrado de paquetes: configurado para que todos los paquetes de la red externa pasen por el host bastión.
- Host bastión: ubicado entre la red interna y el router, es el único que puede establecer conexiones entre ambas redes, permitiendo solo tipos específicos de conexiones y protocolos.

Configuración del router:

- Permisos para hosts específicos: solo hosts determinados pueden abrir conexiones a la red externa para servicios concretos.
- Deshabilitar conexiones externas: solo el host bastión puede establecer conexiones externas.
- Redirección de paquetes: ciertos paquetes de datos del exterior se dirigen directamente a los hosts internos a través del router.



Arquitecturas de cortafuegos de red

Arquitecturas de cortafuegos con host con pantalla (single-homed host)

Ventajas:

- Más flexibles que las arquitecturas simples: permiten redirigir ciertos servicios a la red interna a través del router.
- Mayor seguridad: la red local permanece oculta al exterior gracias al bloqueo del tráfico del host bastión.

Desventajas:

- Complejidad: la configuración y administración son más complejas que las arquitecturas simples.
- Punto único de fallo: si se vulnera el host bastión, el intruso tendrá acceso completo a la red interna.

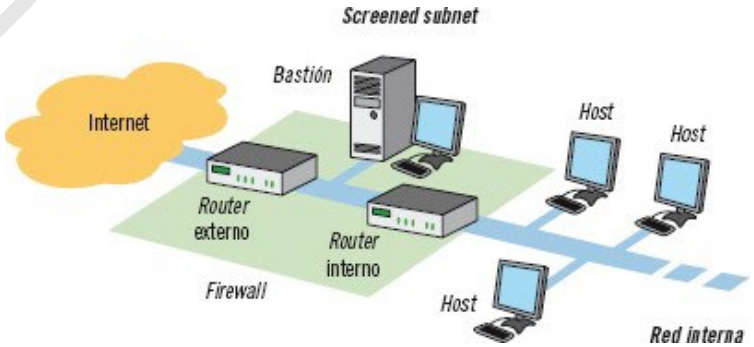
En comparación con las arquitecturas de host dual:

- Las screened host son más seguras: añaden una capa de seguridad al filtrar la información por el host bastión y el router.
- Las dual-homed host son menos complejas: solo filtran la información por el host bastión.

Arquitecturas de cortafuegos de red

Arquitecturas de cortafuegos screened subnet (DMZ)

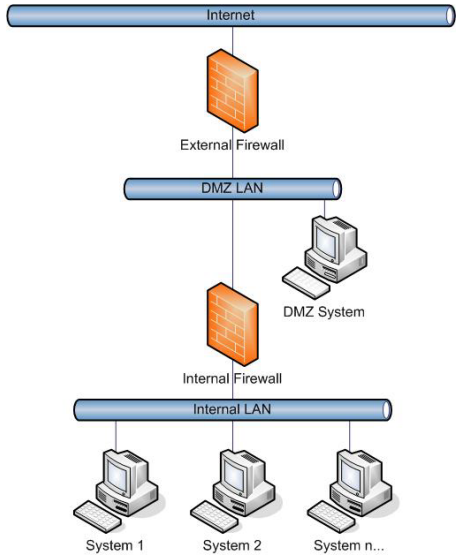
Las arquitecturas screened subnet resuelven el problema de seguridad del host bastion: si un atacante accede al host, también podría acceder a toda la red interna.



Solución: añadir una red de perímetro (DMZ) donde se conecta el host bastion.

Configuración:

- Router interno: entre la red interna y la DMZ.
- Router externo: entre la DMZ y la red externa.
- Host bastion: entre los dos routers.



Funciones de los elementos:

- Router externo: protege a la red interna y la DMZ de ataques externos.
- Router interno: protege a la red interna de la DMZ y la red externa.
- Host bastion: punto de contacto para las conexiones de la red externa.

Arquitecturas de cortafuegos de red

Arquitecturas de cortafuegos screened subnet (DMZ)

Ventajas:

- Mayor seguridad: aísla la red interna de la externa.
- Disminuye el impacto de ataques al host bastion.
- Oculta el tráfico de la red local.

Desventajas:

- Más compleja que otras arquitecturas y mayor coste.

Arquitecturas de cortafuegos de red

Característica	Dual-Homed Host	Screened Host	Screened Subnet (DMZ)
Número de dispositivos Firewall	1	2 (router y host bastión)	2 o más (router externo, router interno y opcionalmente host bastión)
Ubicación del host bastión	Directamente conectado a la red interna y externa	Detrás del router, en la red interna	En una red separada (DMZ)
Nivel de seguridad	Medio	Alto	Alto
Flexibilidad	Alta	Media	Baja
Complejidad	Baja	Media	Alta
Punto único de fallo	El host bastión	El host bastión o el router	El router externo, el router interno o el host bastión (opcional)

Otras arquitecturas de cortafuegos de red

Utilización de varios host bastiones

Objetivos:

- Aumentar el rendimiento de los servicios de red.
- Obtener servicios de apoyo con la introducción de redundancia.
- Separar servicios determinados por necesitar niveles distintos de seguridad.

Red perimetral con un solo router

Implantación de la red perimetral con un solo router, que haría las funciones de router interno y externo a la vez.

- Requisito: El router debe ser capaz de procesar todo el tráfico de datos que reciba.
- Peligro: Si el ataque consigue vulnerar el router, tendrá acceso a toda la red interna.

Utilización del host bastion como router externo

- Ventajas:

  Permite conectar dos redes con interfaces de red distintas. El host bastion ejecuta a la vez el filtrado de paquetes de datos y los servicios proxy.

- Desventajas:

  Elevado coste para el desempeño de los servicios proxy. El host bastion está más expuesto a posibles ataques.

Resumen

Un cortafuegos es un sistema que protege una red local de ataques externos. El perímetro de seguridad es el área protegida por el cortafuegos.

Al elegir un cortafuegos, se deben considerar:

- Política de seguridad de la organización
- Monitorización del cortafuegos
- Presupuesto

Tipos de cortafuegos:

- Routers con filtrado de paquetes: Filtran los datos según reglas predefinidas.
- Gateways a nivel de aplicación: Permiten el acceso solo a determinadas aplicaciones.
- Gateways a nivel de circuito: Redirigen los datos después de validar la conexión.

Arquitecturas de cortafuegos más complejas:

- Dual-homed host
- Screened host
- Screened subnet (DMZ)

La elección del tipo de cortafuegos depende de las necesidades de seguridad de la organización, del valor de los activos y la información a proteger.