SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

2.5.0.MF0487_3. Capítulo 5

Aspectos sobre cortafuegos en auditorías de sistemas informáticos

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Aspecto fundamental de auditoría: Evaluación de medidas de seguridad.

Nivel de vulnerabilidades.

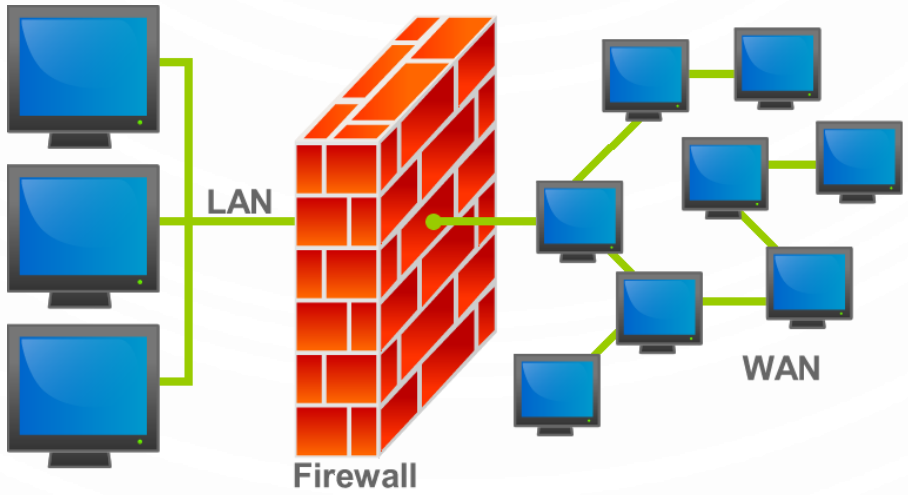
Medidas que intenten bloquear la entrada de ataques que puedan afectar a la información.

El cortafuegos como medida más eficiente.

2. PRINCIPIOS GENERALES DE CORTAFUEGOS

A mayor conectividad, mayor número de amenazas.

Un cortafuegos o firewall es un sistema compuesto por uno o varios dispositivos cuya función principal es la separación entre la red local de un sistema de información y la red exterior para impedir la entrada de ataques y aumentar el nivel de seguridad de la organización.



2. PRINCIPIOS GENERALES DE CORTAFUEGOS

El cortafuegos utiliza los conceptos de perímetro de seguridad y zona de riesgo para determinar las redes interna y externa de un sistema de información:

Perímetro de seguridad: espacio protegido por el cortafuegos, suele ser propiedad de la organización y se corresponde con su red interna.

Zona de riesgo: es la red frente a la que se protege el perímetro de seguridad con el cortafuegos.

2. PRINCIPIOS GENERALES DE CORTAFUEGOS

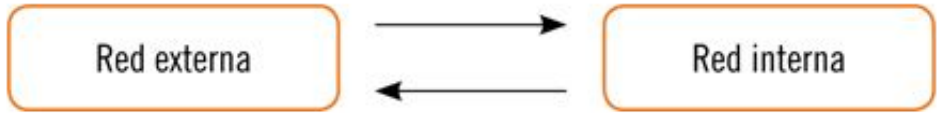
Los cortafuegos son la medida más efectiva de seguridad si se pretende tener conectado el sistema de información de la organización.

Está claro que la protección completa y más efectiva sería el aislamiento total de la red interna de la red externa con la no conexión de los dispositivos a Internet.

Este formato de protección es muy eficaz, ya que impide que entre cualquier intruso no autorizado a la red interna, pero conlleva pérdidas de conectividad importantes debidas al aislamiento total.

2. PRINCIPIOS GENERALES DE CORTAFUEGOS

Otra opción es mantener el sistema de información de la organización conectado con la red externa sin protección.



Esta configuración ya evita el problema de la falta de conectividad, pero deja al sistema completamente vulnerable ante posibles incidentes de seguridad e intrusiones.

2. PRINCIPIOS GENERALES DE CORTAFUEGOS

La mejor alternativa, después de ver las ventajas e inconvenientes de los formatos anteriores, es la utilización de un cortafuegos.

Con esta configuración se mantiene la conectividad del sistema con el exterior, pero se resuelven problemas de seguridad con la implantación del cortafuegos, que impide accesos no autorizados.

2. PRINCIPIOS GENERALES DE CORTAFUEGOS

La protección que ofrece un cortafuegos se define en tres objetivos básicos:

- **Establecer un enlace controlado entre la red interna y la red externa de un sistema de información.**
- **Proteger a la red interna de posibles ataques e intrusiones procedentes de la red externa (Internet).**
- **Establecer un punto único de defensa con una ubicación estratégica (aumentando lo máximo posible tanto la conectividad como la seguridad del sistema).**

2.1. CARACTERÍSTICAS DE DISEÑO DE UN CORTAFUEGOS

El diseño de la estructura de un cortafuegos debe realizarse teniendo en cuenta 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 penetraciones de intrusos, mediante la utilización de sistemas confiables acordes y de sistemas operativos seguros.

2.2 CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

Cuando se va a implantar y configurar un cortafuegos en un sistema de información, hay que tomar tres decisiones fundamentales:

- **Política de seguridad**
- **Monitorización**
- **Economía**

2.2 CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

Política de seguridad

La primera decisión trata sobre la política de seguridad del cortafuegos y del nivel de protección que se pretende implantar.

Cada organización debe establecer la protección del cortafuegos, atendiendo a la utilización de la red y a las características de los usuarios.

No es lo mismo que la empresa desee bloquear todo el tráfico de una red que pretenda bloquear solo sitios web potencialmente peligrosos.

2.2 CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

Monitorización

La segunda decisión hace referencia al grado de monitorización y control que pretende establecer la organización.

En el momento de definir la política de seguridad a establecer, la empresa tendrá que definir el grado de seguridad del cortafuegos, decidiendo qué tipo de información se va a permitir y cuál se va a denegar.

Se distinguen dos posturas opuestas para decidir la monitorización del firewall:

Política restrictiva: en la que se deniega todo lo que no se permite.

Política permisiva: en la que se permite todo lo que no se deniega.

Una política restrictiva siempre es más aconsejable en materia de seguridad, pero con su aplicación es posible que las limitaciones de acceso a ciertos sitios sean excesivas e impidan el desarrollo de las tareas habituales de la organización.

2.2 CARACTERÍSTICAS DE CONFIGURACIÓN DE UN CORTAFUEGOS

Economía

El último punto a tener en cuenta para tomar la decisión de qué cortafuegos implantar en la organización es puramente económico. Según la valoración de los activos y de la información objetivo que se desee proteger, los costes a asumir por la implantación serán menores o superiores.

Es evidente que, cuanto mayor sea el valor de los activos a proteger, mayor será el gasto que deberá soportar la organización para la implantación del cortafuegos y mayor calidad deberá tener el sistema a implantar.

Sin embargo, si el valor de los activos que se pretenden proteger es limitado, no merecerá la pena realizar una alta inversión: es posible que la inversión supere los costes que podría ocasionar algún tipo de ataque.

3. COMPONENTES DE UN CORTAFUEGOS DE RED

Cuando ya se han decidido las características principales del cortafuegos a implantar, el siguiente paso es decidir qué mecanismos se van a incorporar a dicho cortafuegos para cumplir con las políticas de seguridad definidas por la organización.

Todos los cortafuegos están compuestos por tres componentes sobre los que se deberán implantar los mecanismos de protección:

- **Filtrado de paquetes.**
- **Proxy de aplicación.**
- **Monitorización de la actividad.**

3.1. FILTRADO DE PAQUETES

El funcionamiento del componente de filtrado de paquetes es bastante sencillo:

Se analiza la cabecera de cada paquete de datos que pretende entrar en la red local de la organización.

Según las reglas preestablecidas por la organización y atendiendo al análisis del paquete, se le permitirá el acceso o será bloqueada.

Los aspectos más habituales por analizar son:

- **Protocolo utilizado.**
- **Dirección de origen y dirección de destino.**
- **Puerto de destino.**

3.2. PROXY DE APLICACIÓN

Aplicaciones software que reenvíen o bloqueen conexiones a unos servicios concretos.

- **Permisión exclusiva de servicios con proxy:** los servicios proxy solo permiten usar aquellos 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:** los servicios proxy ofrecen opciones de filtrado de datos yendo más allá del filtrado por las características de la cabecera del paquete (como es el caso del componente filtrado de paquetes).
- **Simplificación de reglas de filtrado:** los servicios proxy facilitan la tarea de establecer y definir las reglas de filtrado por su mayor simplicidad ante el componente de filtrado de paquetes. Simplemente hay que permitir el tráfico de datos hacia la pasarela y bloquear el resto de datos.

3.3. MONITORIZACIÓN DE LA ACTIVIDAD

La monitorización de la actividad del cortafuegos es imprescindible para la seguridad de los elementos que protege, ya que permite obtener información sobre:

- **Todos los ataques que se han producido (o se están produciendo).**
- **La presencia de paquetes de datos sospechosos (independientemente de si finalmente son ataques reales o no).**

4. TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD

Se destacan tres tipos de cortafuegos atendiendo a su ubicación y funcionalidad:

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

4.1. ROUTERS CON FILTRADO DE PAQUETES

Los routers con filtrado de paquetes son un tipo de cortafuegos que filtran los paquetes IP entrantes, atendiendo a una serie de reglas predefinidas: según la definición de estas reglas, estos routers descartan el paquete o lo reenvían.

4.1. ROUTERS CON FILTRADO DE PAQUETES

Los routers con filtrado de paquetes son un tipo de cortafuegos que filtran los paquetes IP entrantes, atendiendo a una serie de reglas predefinidas: según la definición de estas reglas, estos routers descartan el paquete o lo reenvían.

Ventajas

- Simplicidad.
- No son visibles para los usuarios.
- Destacan por su elevada velocidad.

Desventajas

- Dificultad para la correcta definición de las reglas de acceso a los paquetes de información.
- No requieren autentificación de los usuarios.

4.2. GATEWAYS A NIVEL DE APLICACIÓN

Los gateways a nivel de aplicación se asocian al componente de servidores proxy de los cortafuegos.

Son repetidores de tráfico a nivel de aplicación: cuando un usuario solicita un servicio, lo realiza a través del proxy. Una vez recibida la petición, el proxy realiza el pedido al servidor real y devuelve la información solicitada al usuario.

Su finalidad principal es el análisis de los paquetes de datos para detectar contenidos que puedan violar la seguridad de la red.

4.2. GATEWAYS A NIVEL DE APLICACIÓN

Ventajas

Ofrece mayor seguridad que los routers de filtrado de paquetes.

Revisa solo las aplicaciones permitidas, aumentando su eficacia.

Revisa todo el tráfico de red entrante.

Evita el tráfico directo entre redes.

Desventajas

Puede provocar cuellos de botella por sobrecarga de procesamiento en cada conexión.

4.3. GATEWAYS A NIVEL DE CIRCUITO

Los gateways o pasarelas a nivel de circuito son sistemas que redirigen los paquetes de datos cuando se ha comprobado que se ha establecido la conexión.

Para establecer la conexión, estos gateways validan el inicio de la comunicación para verificar si se realiza correctamente según el protocolo de trasportes.

Cuando ya se ha validado la comunicación, todos los paquetes que se reenvíen a continuación no son verificados (solo se revisan las cabeceras de los paquetes).

En términos generales, los gateways a nivel de circuito establecen funciones que determinan qué conexiones serán permitidas para la transmisión de datos.

Este tipo de firewall ofrece la posibilidad de determinar una política restrictiva que permita cerrar y abrir puertos solo cuando sea estrictamente necesario.

4.4. HOST BASTION

Host bastion es un punto crítico del sistema en la seguridad de la red identificado por el administrador del cortafuegos. No es un tipo de cortafuegos en sí, pero es interesado mencionarlo porque sirve como plataformas para:

Gateways a nivel de aplicación.

Gateways a nivel de circuito.

Se trata de una aplicación ubicada en un punto crítico de un servidor para proteger a la red interna de la organización. Este punto crítico ha sido configurado previamente para que atraiga los posibles ataques que intenten acceder al sistema.

5. ARQUITECTURAS DE CORTAFUEGOS DE RED

Además de la utilización de los cortafuegos simples como los routers con filtrado de datos o los sistemas de pasarela única, hay varias posibilidades de firewalls más complejos que permiten el aumento de la seguridad del perímetro de seguridad.

Las arquitecturas complejas más comunes son las siguientes:

Dual-homed host.

Screened host.

Screened Subnet (DMZ).

Estas tres arquitecturas, además de utilizar un sistema como el router de filtrado o el gateway, combinan estos elementos con bastiones para un bloqueo de datos potencialmente peligroso más eficaz que permita una mayor protección del sistema de información.

5.1. ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST

Las arquitecturas de cortafuegos dual-homed host ofrecen una mayor protección que los cortafuegos simples y están compuestas por dos placas de red:

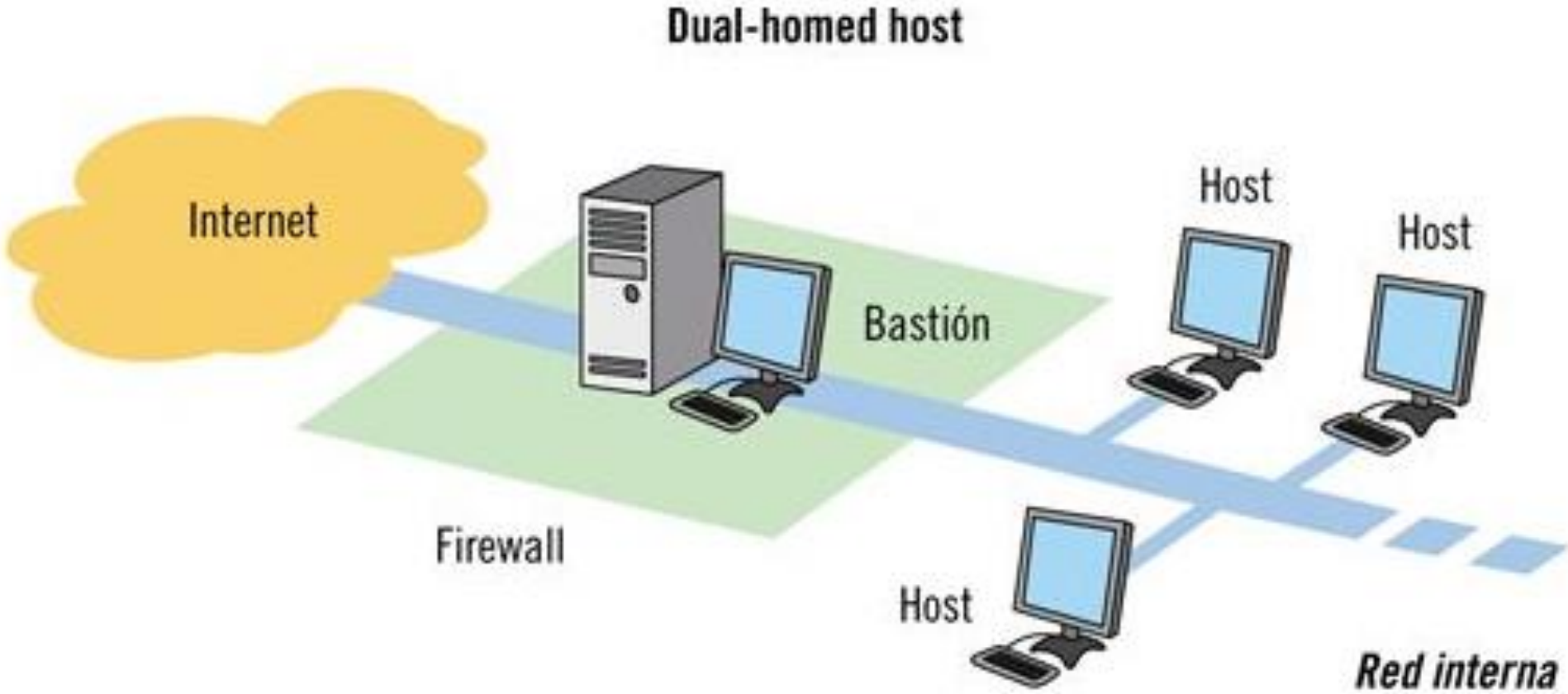
Una de las tarjetas suele conectarse a la red interna.

La otra tarjeta se conecta a la red externa de la organización.

Con esta arquitectura se evita que, si el router con filtrado de tramas se ve comprometido, se permita el acceso del tráfico de red a la red interna, ya que toda la información entre Internet y la red interna debe pasar previamente por el host bastion.

Estos sistemas deben ejecutar por lo menos un servidor proxy para cada servicio que se desee pasar por el firewall.

5.1. ARQUITECTURAS DE CORTAFUEGOS DUAL-HOMED HOST



5.2. ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)

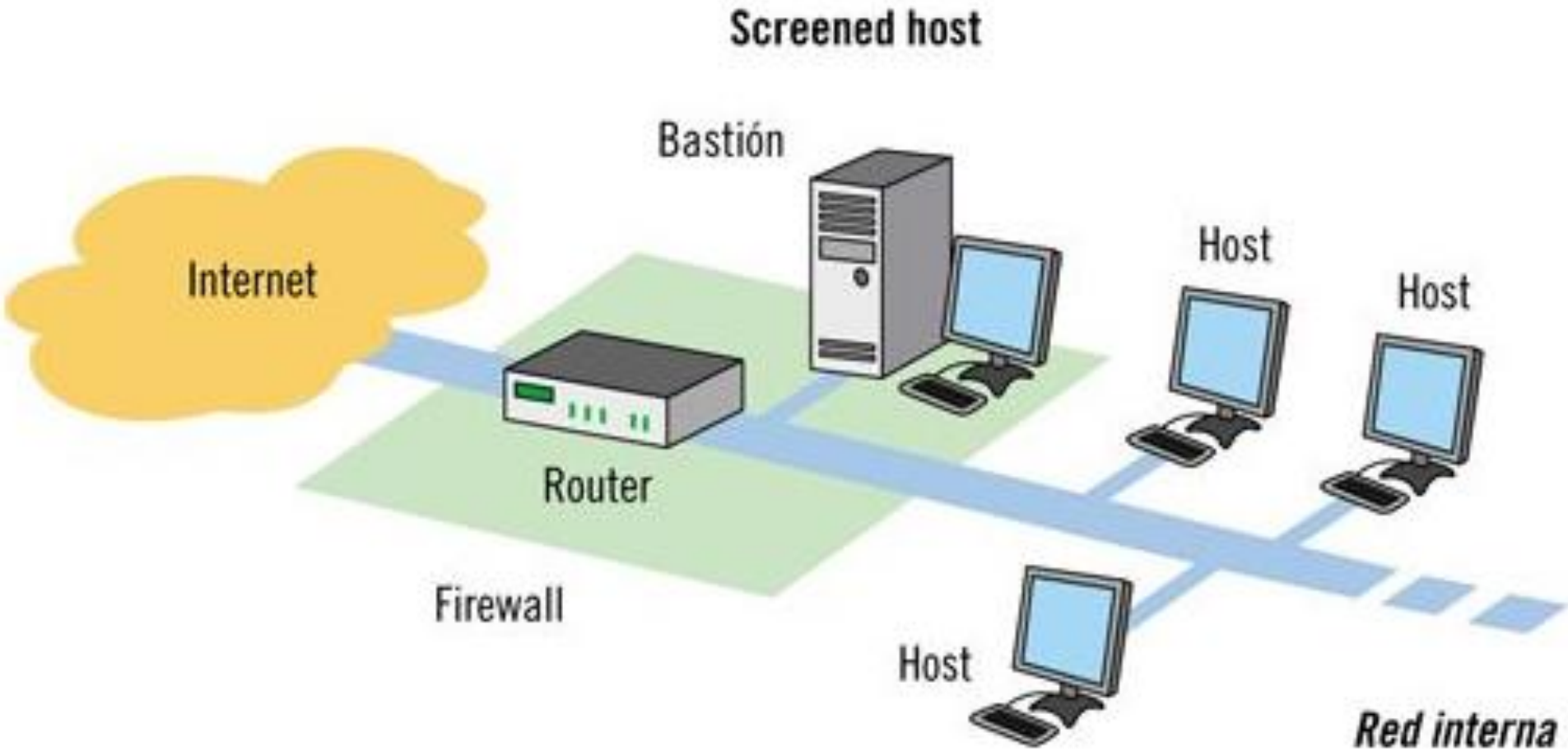
Los cortafuegos single-homed host están formados por dos sistemas de protección que filtran conexiones a nivel de circuito y a nivel de aplicación:

Un router con filtrado de paquetes.

Un host bastion.

En estas arquitecturas, el router se configura específicamente para que todos los paquetes de datos que provienen de la red externa deban pasar obligatoriamente por el host bastion, lo que obliga a la organización al establecimiento de elevados sistemas de protección a dicho bastión.

5.2. ARQUITECTURAS DE CORTAFUEGOS CON SCREENED HOST (SINGLE-HOMED HOST)



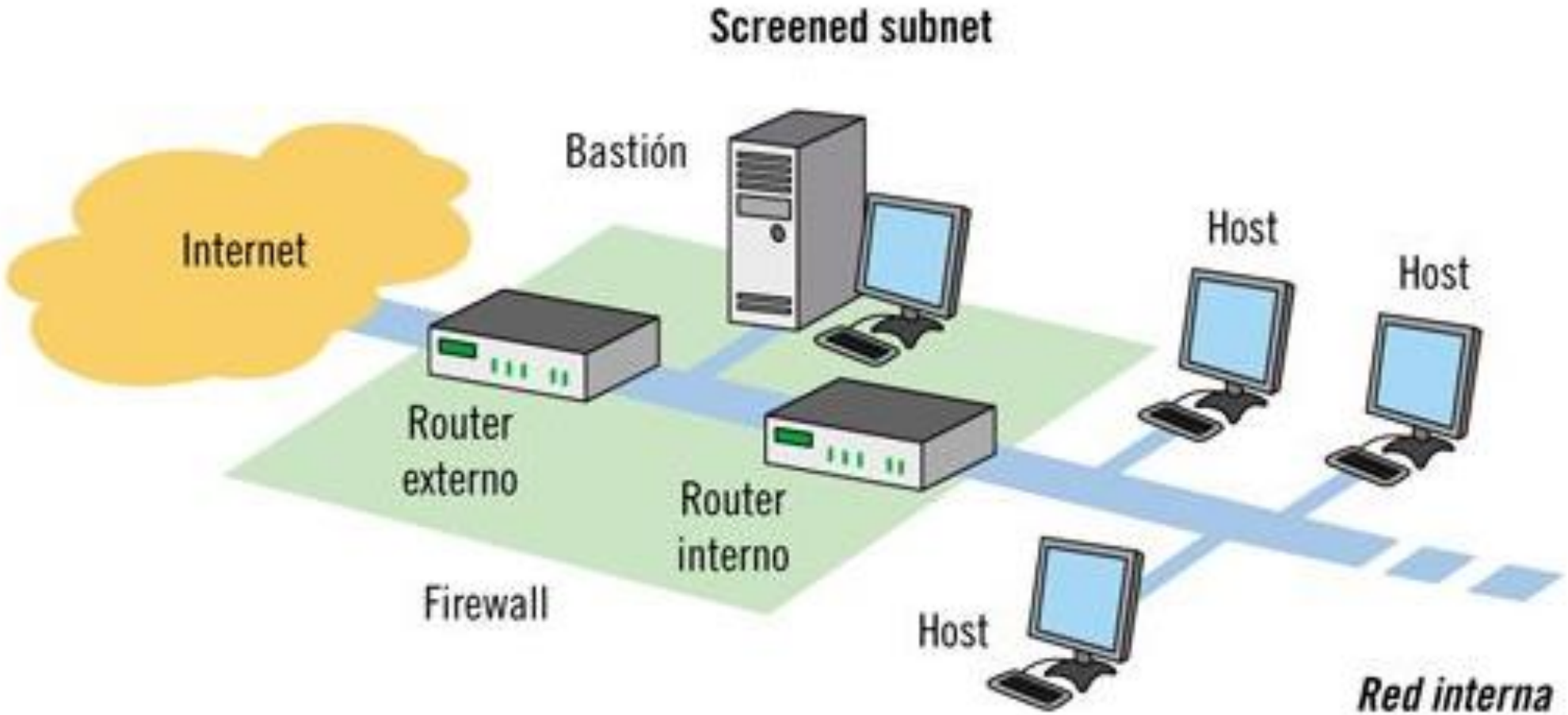
5.3. ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)

Estas arquitecturas se ofrecen como solución al problema de seguridad del establecimiento de host bastion: en las arquitecturas anteriores, si un atacante puede acceder al host bastion, podrá también acceder a toda la red interna.

Las arquitecturas de cortafuegos screened subnet añaden un elemento más de seguridad que evite el acceso a la red por vulneración del host bastion.

Este elemento de seguridad se establece con una red de perímetro en la que se conecta el host bastion, la red llamada "zona desmilitarizada-DMZ".

5.3. ARQUITECTURAS DE CORTAFUEGOS SCREENED SUBNET (DMZ)



6. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

A partir de las arquitecturas vistas anteriormente, se pueden establecer distintas configuraciones según las necesidades de protección de cada organización.

Utilización de varios host bastions

Red perimetral con un solo router

Utilización del host bastion como router externo

6.1. UTILIZACIÓN DE VARIOS HOST BASTIONS

Una de las posibles configuraciones alternativas es la utilización de varios host bastions con algunos de los siguientes 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.

6.2. RED PERIMETRAL CON UN SOLO ROUTER

Utilización de un solo router para la implantación de una red perimetral: este router haría las funciones de router interno y externo a la vez.

El requisito fundamental para el establecimiento de esta arquitectura es que el router sea capaz de procesar todo el tráfico de datos que reciba, ya que debe filtrar tanto los datos de la red interna como los de la red externa.

6.3. UTILIZACIÓN DEL HOST BASTION COMO ROUTER EXTERNO

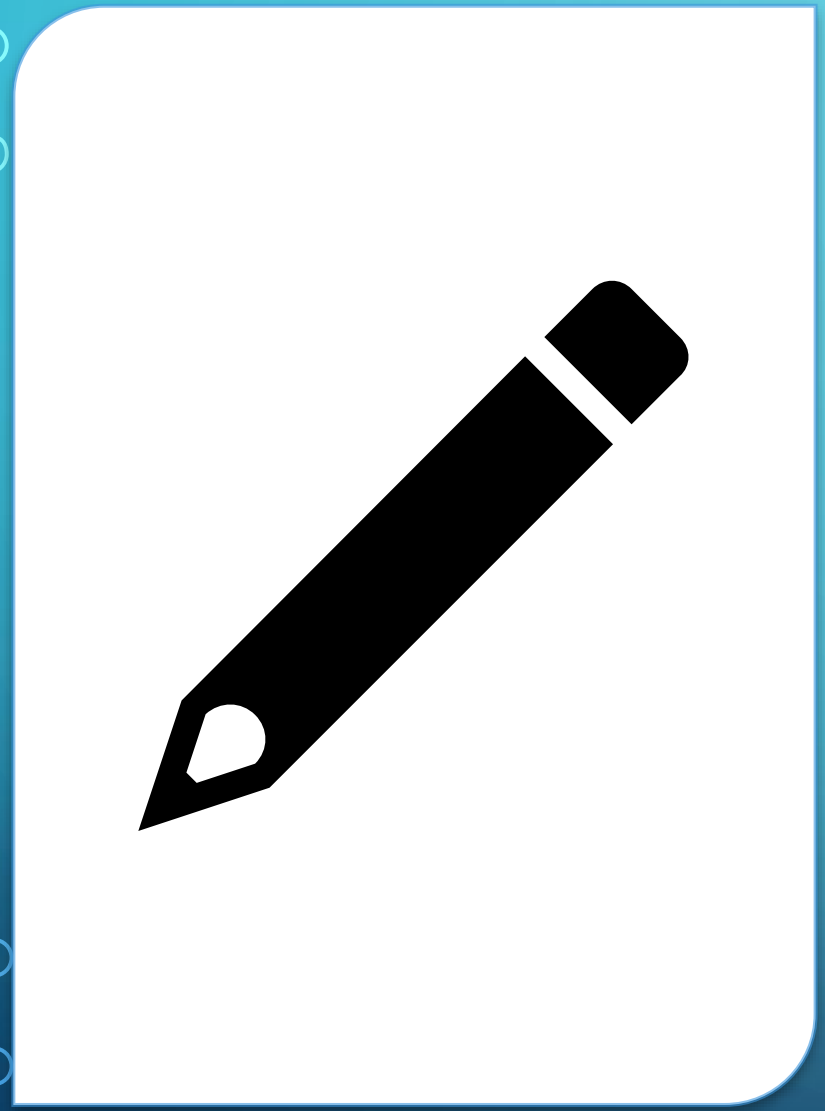
Cuando se quieren conectar dos redes con interfaces de red distintas, se puede utilizar el host bastion como router externo.

Con esta arquitectura, el host bastion ejecuta a la vez el filtrado de paquetes de datos y los servicios proxy.

El principal inconveniente de esta configuración es su elevado coste para el desempeño de los servicios proxy. Además, aunque no se expone a vulnerabilidades, sí es cierto que el host bastion está más expuesto a posibles ataques, al no haber ninguna barrera entre la red local y este.

Por ello, se recomienda el establecimiento de medidas adicionales de seguridad que añadan protección extra al host bastion y minoren su vulnerabilidad ante intrusiones y ataques.

Ejercicios



2.5.100.1.MF0487_3. EJERCICIOSCAPITULO_5.DOCX