

CFGM. Seguridad Informática

Unidad 7

Seguridad de alto nivel en redes: cortafuegos

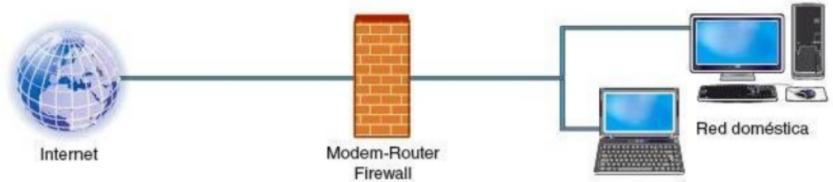
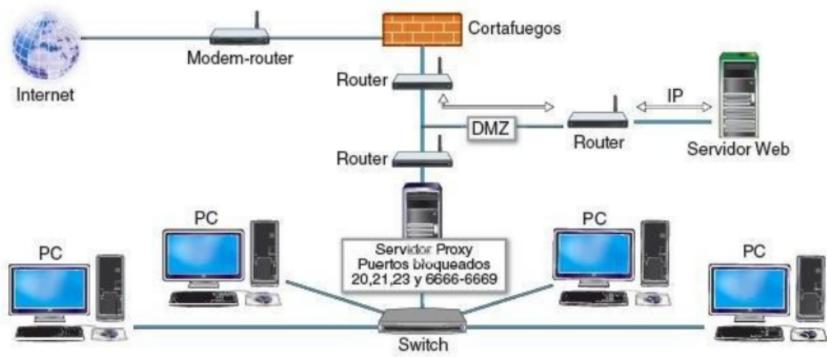
CONTENIDOS

- 1. Seguridad de alto nivel**
- 2. Cortafuegos: qué son y para qué sirven**
- 3. Tipos de cortafuegos**
- 4. Filtrado de Paquetes**
- 5. Uso de cortafuegos**
- 6. Arquitecturas de red con cortafuegos**
- 7. Monitorización y logs**

1. Seguridad de alto nivel

Hay dos elementos imprescindibles que han combinarse, que son los cortafuegos y los proxys. Una estructura típica que mantienen un gran número de empresas es la que ves en la primera Figura, donde se reflejan estos dos mecanismos, que sirven como barrera ante posibles intrusos.

La configuración de una red doméstica, como la que habitualmente tienes en casa, es mucho más simple, como puedes ver en la segunda Figura, donde el router ejerce como cortafuegos.



2. Cortafuegos: qué son y para qué sirven

Un cortafuegos es un sistema que audita y evita los intentos de conexión no deseados tanto desde los equipos hacia la red como desde la red hacia los equipos.

Un cortafuegos puede ser tanto un dispositivo hardware como software, es decir, podemos tener una máquina diseñada específicamente para esta función o utilizar una aplicación que se instala en uno de los equipos conectados a la red.

En la Figura puedes ver la estructura de una red básica donde se ha instalado un equipo que actúa como cortafuegos, ocupándose de filtrar todo aquello que sale y entra a la red de área local.



2. Cortafuegos: qué son y para qué sirven

Además del filtrado de paquetes, el uso del cortafuegos nos ofrece una serie de servicios adicionales muy útiles para proteger el buen uso de nuestra red y nuestros servidores, que tienes en la Tabla.

Servicio	Definición
Bloqueo de tráfico no autorizado	Restringe servicios de Internet, bloqueando páginas Web o el tráfico proveniente de un rango de direcciones IP.
Ocultación de equipos de la LAN	Oculta equipos para que no sean detectados por posibles atacantes.
Registro del tráfico	Dado que el cortafuegos se instala en la frontera entre la red interna y la externa, detecta todo el tráfico que entra y sale de la red, por lo que se puede almacenar su actividad.
Redirección de tráfico entrante	Redirige el tráfico entrante a la organización a la zona DMZ, evitando que llegue a los equipos locales.
Limitación de ancho de banda	Limita el ancho de banda utilizado por un protocolo o un tipo de tráfico
Seguimiento de tráfico y monitorización de ataques	Genera estadísticas con datos sobre el ancho de banda consumido, permitiendo detectar, por ejemplo, si desde un determinado equipo se está descargando un alto volumen de datos procedentes de Internet. Monitoriza los ataques desde el exterior para tomar medidas como el bloqueo del análisis de puertos para evitar los ataques más habituales.

3. Tipos de cortafuegos según su ubicación

La ubicación de los cortafuegos va intrínsecamente relacionada con el sistema que se quiere proteger. Podemos distinguir entre dos tipos de cortafuegos en función de donde se localicen:

- Cortafuegos de sistema o personales.
- Cortafuegos de subredes.



Los cortafuegos de sistema o personales restringen la comunicación no autorizada con un equipo, actuando como un sistema de defensa perimetral, mientras que los cortafuegos de subredes protegen toda una subred en conjunto (actuando como único punto de entrada).

3. Tipos de cortafuegos

Cortafuegos personales

Los cortafuegos personales surgen como respuesta a la necesidad de proteger los equipos pertenecientes a redes privadas particulares, por ejemplo, las que se instalan en nuestros domicilios para permitirnos conectarnos a Internet.

Este tipo de cortafuegos se instala en el equipo del usuario y proporciona cinco funciones principales:

- Permite supervisar todas las conexiones con el exterior, incluyendo los accesos a servicios de Internet.
- Permiten monitorizar los programas locales que tratan de acceder a Internet para que el usuario pueda decidir si permite que lo hagan o no.
- Proporciona mecanismos para bloquear los posibles intentos de intrusión al equipo u otros ataques realizados desde Internet.
- Realiza un registro de todas las conexiones realizadas desde el equipo.
- Algunos de ellos incorporan filtros antispam, así como detección de virus u otros códigos que pueden ser perjudiciales para el equipo.

3. Tipos de cortafuegos

Cortafuegos de subredes

Los cortafuegos de subredes tienen como objetivo aplicar una política de seguridad a un grupo de sistemas desde un único punto. Para ello lo primero que debe hacerse es agrupar los sistemas en zonas de seguridad, de modo que se aplique las mismas reglas a los equipos que forman parte de cada zona, y puedan aplicarse distintas reglas a distintas zonas.

En el caso de los cortafuegos de subredes sus principales funciones son:

- Autorización de servicios (entrantes y salientes).
- Control de acceso a los servicios basándose en la identidad del usuario o equipo.
- Registro y monitorización de accesos a la red.

El uso de los cortafuegos de subred permite establecer una protección global, lo que nos permite relajarnos en la protección individual de cada equipo, estableciendo un único punto de implantación de la política de seguridad. Esto facilita su administración y, dado que los ataques se producen sobre un único sitio, hace más sencilla su vigilancia.

4. Filtrado de Paquetes

Reglas de filtrado

Las reglas de filtrado nos permitirán establecer políticas de seguridad para nuestro sistema, evitando los accesos no autorizados sin crear inconvenientes a los accesos que sí queramos permitir.

Estas reglas se suelen expresar como una tabla de condiciones y acciones que se consulta hasta que se encuentra con la regla que permita tomar una decisión, lo cuál hace especialmente importante que las reglas se establezcan en orden de prioridad de actuación y que los administradores las revisen periódicamente.

Un ejemplo de una tabla teórica es el que puedes ver en la Tabla, donde tienes una serie de reglas definidas en función de las direcciones IP origen y destino y de los puertos origen y destino, donde se indica si se permitirán los paquetes provenientes de esas direcciones.

Nº Regla	IP Origen	Puerto Origen	IP Destino	Puerto Destino	Acción	Observaciones
1	192.168.1.2	1533	192.168.128.2	21	Permitir	
2	192.168.10.3	1400	192.168.128.2	21	Permitir	
3						

4. Filtrado de Paquetes

Reglas de filtrado

Las reglas pueden agruparse en tres tipos:

- Autoprotección del cortafuegos: no se permitirá ningún datagrama dirigido directamente al firewall.
- Reglas de salida, que pueden ser permisivas o restrictivas. Si son permisivas se prohíben las excepciones y el resto se autoriza, si son restrictivas se prohíbe todo excepto las excepciones permitidas.
- Reglas de entrada: está todo prohibido excepto aquellas excepciones que específicamente hayan sido autorizadas.

El ejemplo más claro de reglas de filtrado podemos verlo en el sistema de redes Netfilter de Linux, que se gestiona a través de una utilidad que se denomina iptables, la cual se maneja desde el terminal. La estructura básica de este comando es la siguiente:

```
# iptables –table [COMMAND] chain rule-specification [options]
```

7 Seguridad de alto nivel en redes: cortafuegos

5. Uso de cortafuegos

En todo sistema es conveniente tener instalado y funcionando un cortafuegos, ya sea en un ordenador personal donde utilicemos el cortafuegos integrado en el sistema operativo, o en una red de una empresa, donde necesitaremos herramientas algo más sofisticadas.

5.1. Criterios para elegir un cortafuegos

Criterio	Justificación
Política de seguridad del sistema o la empresa	La configuración según el tráfico o servicios a bloquear.
Nivel de monitorización y control	Hay que decidir cómo se va implementar (que se permitirá y que se denegará).
Económico	En función del valor de lo que vamos a proteger será necesario un desembolso mayor o menor.
Localización	Existen diversas arquitecturas de red que podemos elegir o utilizar cortafuegos personales en los equipos.
Elementos físicos	Equipos necesarios, uso de bastión, routers, etc.
Sistema Operativo	Sistema operativo del bastión o del equipo sobre el que se instala el cortafuegos.

5.2. Instalación y configuración de un cortafuegos comercial

Existen numerosos cortafuegos que podemos elegir para instalar en nuestros sistemas.

6. Arquitecturas de red con cortafuegos

6.1. Screening router

Como frontera entre la red privada y la pública se encuentra un router que puede realizar tareas de filtrado. Es la instalación típica de un hogar o empresa pequeña.

6.2. Dual-Homed Host

La arquitectura dual-homed host se basa en el uso de equipos con dos o más tarjetas de red. Una de estas tarjetas a la red interna que se quiere proteger y la otra externa, normalmente a Internet.

Los equipos de la red interna verán al cortafuegos (bastión) a través de una de las tarjetas de red y los equipos externos a través de la otra, pero el tráfico entre ambas redes estará aislado.

Todo el tráfico debe pasar a través del firewall instalado en el bastión.

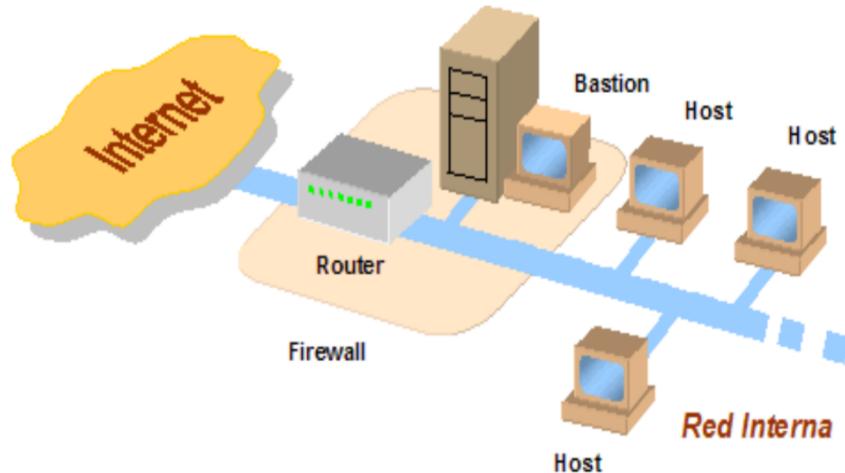
Inconveniente: Si un atacante se hace con el bastión, tendrá acceso a la red interna de la organización.



6. Arquitecturas de red con cortafuegos

6.3. Screened Host

La arquitectura screened-host combina el uso de un router como equipo fronterizo exterior, con un proxy, de modo que el filtrado de paquetes se produce en primer lugar en el router. El proxy permite añadir reglas para las aplicaciones más empleadas, por ejemplo el acceso a Internet a través de los navegadores.



Se combinan ambas opciones, de modo que haya servicios controlados por el router y otros a los que se acceda a través del bastión.

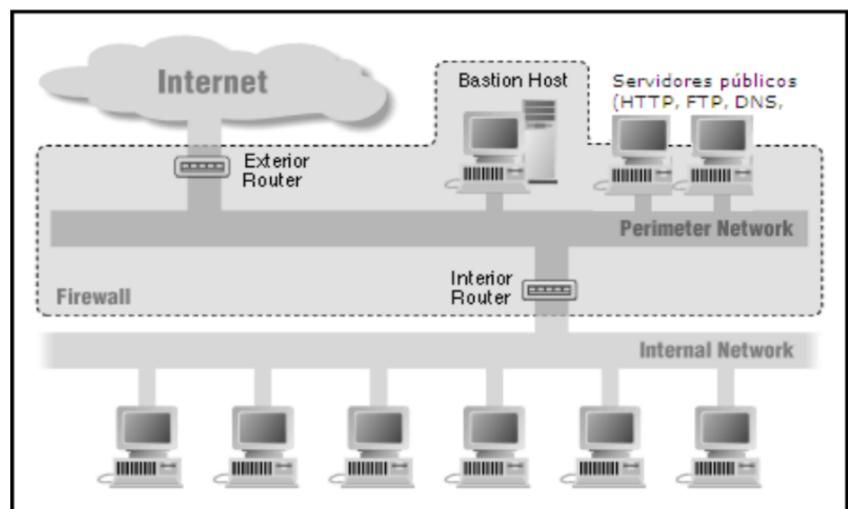
6. Arquitecturas de red con cortafuegos

6.3. Screened Subnet

Mediante la creación de una subred intermedia, denominada DMZ o zona desmilitarizada, entre la red externa y la red privada interna, que permitirá tener dos niveles de seguridad, uno algo menor en el cortafuegos más externo y uno de mayor nivel de seguridad en el cortafuegos de acceso a la red interna.

La DMZ aloja servidores que se deben poder ver desde el exterior, como HTTP, FTP y DNS.

El router externo filtra la entrada de tráfico desde la red externa y la salida hacia la misma, mientras que el router interno se ocupa de filtrar el tráfico generado y dirigido por y hacia los equipos de la red interna.



Es una arquitectura más compleja pero también mucho más segura que las anteriores.

7 Seguridad de alto nivel en redes: cortafuegos

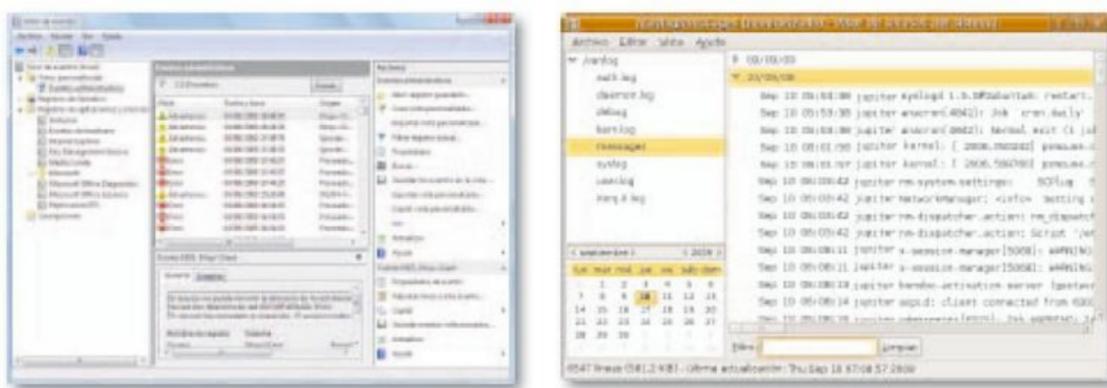
7. Monitorización y logs

Los registros de actividad de un sistema, que habitualmente se conocen como logs, permiten detectar incidentes y comportamientos no habituales.

7.1. Registro de actividad de los sistemas operativos

Los sistemas operativos incorporan logs donde registran información sobre qué usuarios y en qué momento abren o cierran una sesión, qué procesos están en ejecución dentro del sistema, las aplicaciones que son ejecutadas por los usuarios, el uso de los recursos que hacen (impresoras, escaners, etc.) así como los posibles problemas de seguridad.

En los sistemas operativos Windows se utiliza el visor de eventos para analizar los logs del sistema, como ves en las Figura donde tienes el visor correspondiente a Windows Vista y Ubuntu 9.04 respectivamente



7. Monitorización y logs

7.1. Registro de actividad de los sistemas operativos

Los registros sobre los que esta herramienta proporciona información son:

- **Registros de Windows:** muestra información de errores, advertencias o información del sistema operativo y sus aplicaciones, así como información de seguridad, donde muestra los registros de éxito y de fracaso de los servicios auditados, por ejemplo, si un usuario ha podido iniciar la sesión.
- **Registros de aplicaciones y servicios,** cuyo contenido puede variar ya que incluyen registros independientes para los programas que se ejecutan en el equipo, así como registros más detallados relacionados con servicios específicos de Windows.

De igual modo, los sistemas Linux incluyen aplicaciones para poder visualizar los logs, como es la herramienta System Log (Sucesos del Sistema) en Ubuntu, al que puedes acceder a través del menú Sistema, dentro del grupo Administración. Este visor gráfico incluye, entre otras funcionalidades, un calendario y utilidades de filtrado.

7.2. Registros de actividad del cortafuegos

Los cortafuegos incorporan sus propios registros de actividad, especialmente útiles para analizar los bloqueos de accesos no autorizados que se hayan detectado y las actividades anormales que puedan haberse producido en el sistema.

Créditos

Autores del libro del alumno

César Seoane Ruano, Ana Belén Saiz Herrero,

Emilio Fernández Álvarez, Laura Fernández Aranda

Edición

Estudio177.com, Laura García Olaya