Instalación y configuración de cortafuegos (Seguridad y alta disponibilidad)

Utilización de cortafuegos

Cuando un programa de nuestro ordenador necesita acceder a Internet, establece una conexión en la que enviará o recibirá la información que le sea necesaria, desde nuestro ordenador hacia Internet o desde Internet hacia nuestro ordenador, dando lugar a conexiones entrantes o salientes.

El cortafuegos, más conocido como firewall, es una herramienta que permite gestionar qué programas pueden establecerlas y qué programas no, y qué tipo de conexiones serán permitidas.

El firewall funciona como una puerta de enlace de la red con filtro y sólo es eficaz en aquellos paquetes que deben pasar a través de ella. Por lo tanto, sólo puede ser eficaz cuando la única ruta para estos paquetes es a través del firewall.

Filtrado de paquetes de datos

Cualquier router utiliza reglas de filtrado para reducir la carga de la red; por ejemplo, se descartan paquetes cuyo TTL ha llegado a cero, paquetes con un control de errores erróneos, o simplemente tramas de broadcast.

Además de estas aplicaciones, el filtrado de paquetes se puede utilizar para implementar diferentes políticas de seguridad en una red; el objetivo principal de todas ellas suele ser evitar el acceso no autorizado entre dos redes, pero manteniendo intactos los accesos autorizados.

Su funcionamiento es habitualmente muy simple: se analiza la cabecera de cada paquete, y en función de una serie de reglas establecidas de antemano la trama es bloqueada o se le permite seguir su camino; estas reglas suelen contemplar campos como el protocolo utilizado (TCP, UDP, ICMP, …), las direcciones fuente y destino, y el puerto destino, lo cual ya nos dice que el firewall ha de ser capaz de trabajar en los niveles de red (para discriminar en función de las direcciones origen y destino) y de transporte (para hacerlo en función de los puertos usados).

Tipos de cortafuegos. Características. Funciones principales

Tipos de cortafuegos:

- Cortafuegos de filtrado de paquetes.
- Puerta de enlace a nivel de circuito.
- Firewall de inspección con estado.
- Puerta de enlace de nivel de aplicación (también conocido como firewall proxy).
- Firewall de próxima generación.

Algunas características generales:

- Diferentes niveles de protección.
- Protección de distintas redes.
- Accesos a la red y accesos a Internet.
- Protección contra intrusos.
- Bloqueos.
- Definición de Reglas.

Funciones principales:

- Administrar los accesos de los usuarios a los servicios privados de la red.

- Registrar todos los intentos de entrada y salida de una red.
- Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.
- Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como filtrado de protocolo.
- Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite.
- Controlar las aplicaciones que pueden acceder a Internet.
- Detección de puertos que están en escucha y en principio no deberían estarlo.

Instalación de cortafuegos. Ubicación

En GNU/Linux podemos instalar NFTables, una arquitectura de filtrado de paquetes que se integra con el núcleo de Linux y reemplaza al anterior IPTables .

En Windows viene instalado por defecto en todas las versiones.

Reglas de filtrado de cortafuegos

En los firewalls suele haber cuatro tablas distintas que almacenan las reglas que regulan operaciones sobre paquetes:

- **filter** se refiere a las reglas de filtrado (aceptar, rechazar o ignorar un paquete);
- **nat** se refiere a la traducción de las direcciones de origen o destino y puertos de los paquetes;
- **mangle** se refiere a otros cambios en los paquetes IP;
- **raw** permite otras modificaciones manuales en los paquetes antes de que lleguen al sistema de seguimiento

de conexiones.

Cada una de las tablas contienen listas de reglas llamadas cadenas.

La tabla filter tiene tres cadenas estándar:

- **INPUT:** se refiere a paquetes cuyo destino es el propio firewall;
- **OUTPUT:** se refiere a los paquetes que emite el firewall;
- **FORWARD:** se refiere a los paquetes que transitan a través del firewall (que no es ni su origen ni su destino).

La tabla nat también tiene tres cadenas estándar:

- **PREROUTING:** para modificar los paquetes tan pronto como llegan;
- **POSTROUTING:** para modificar los paquetes cuando están listos para seguir su camino;
- **OUTPUT:** para modificar los paquetes generados por el propio firewall.

Pruebas de funcionamiento. Sondeo

El sondeo de un firewall va dirigido a testear el estado de los puertos (cerrado, abierto o filtrado).

Registros de sucesos de un cortafuegos

Los registros de sucesos graban en un fichero todas las entradas y salidas del cortafuegos.