¿Qué es un firewall de red y cómo funciona?



Si quieres aumentar la seguridad de tu red, un firewall es una de las primeras líneas de defensa que puedes utilizar. Además de limitar los intentos de acceso a +determinadas redes, los firewall modernos han evolucionado para limitar la capacidad de los atacantes malintencionados que buscan robar información sensible a través de una serie de dispositivos.

A pesar de ser una tecnología antigua, los firewall son más importantes que nunca, especialmente a medida que los nuevos dispositivos inteligentes se conectan durante la revolución del Internet de las Cosas [1] (IoT por sus siglas en inglés). A continuación, nos adentraremos en el funcionamiento de los firewalls y en cómo pueden ser utilizados para proteger tu red y reforzar la seguridad.

## ¿Qué es un firewall?

Un firewall es un sistema diseñado para proteger las redes privadas del acceso no autorizado y no verificado en una conexión a Internet. Estos pueden ser de tipo hardware o software, o una combinación de ambos.

Entonces, ¿qué hacen realmente? Los firewall protegen tu computadora, o una serie de computadoras en una red, de los sitios web llenos de malware o de los puertos de red abiertos vulnerables. Ayudan a detener a los posibles atacantes antes de que puedan causar algún daño. Los firewall de red pueden encontrarse en empresas, hogares, escuelas e intranets, las cuales son redes privadas dentro de una organización.

Además, pueden configurarse para impedir el acceso a usuarios [4] de la red a sitios web externos. Por ejemplo, los padres pueden establecer controles parentales sobre los hábitos de navegación de sus hijos o tu lugar de trabajo puede bloquear determinados sitios web para mantenerte concentrado.

## ¿Cuáles son los diferentes tipos de firewall?

### **Filtro de paquetes**

Este es el tipo de firewall más antiguo, pero tiene la ventaja de no afectar al rendimiento general del sistema. Puedes pensar en un firewall de filtrado de paquetes como un punto de control que se emplea en un router o switch de tráfico.

El filtro de paquetes [5] evaluará, valga la redundancia, los paquetes de datos que llegan a través de tu router. Normalmente, este filtro puede evaluar la dirección IP de origen, la dirección IP de destino, el tipo de paquete, el puerto de origen y el puerto de destino.

No inspecciona el contenido real del paquete, solo la información general a nivel superficial. En función de la configuración del firewall, puedes filtrar para permitir o no los paquetes procedentes de direcciones IP específicas o de puertos concretos.

Este tipo de firewall es relativamente simple, por lo que es fácil de evadir si eres un atacante decidido. Es mejor utilizar este tipo de firewall junto con otra arquitectura de firewall más fuerte.

### **Puerta de enlace a nivel-circuito.**

Al igual que el filtro anterior, una puerta de enlace a nivel-circuito [6] tiene un sistema de aprobación o rechazo del tráfico. Funcionan evaluando el protocolo de control de transmisión (TCP por sus siglas en inglés). Esta evaluación determina si el paquete proviene de una sesión legítima.

¿Cómo se ve realmente? En una red con un firewall de puerta de enlace a nivel-circuito configurado, todos los paquetes que salen de la red parecen proceder de esa puerta de enlace, lo que impide las conexiones directas entre una red de confianza y una no confiable.

Los hackers aún pueden burlar este tipo de firewall si se aprovechan de una conexión establecida y envían paquetes con malware u otro contenido malicioso adjunto.

### **Actuando como servidor proxy**

Se cree que este es el tipo de firewall más seguro porque no permite el contacto directo de la red. El servidor de seguridad proxy tiene la capacidad de examinar todo el paquete de red en lugar de detalles a nivel superficial como la dirección IP y el número de puerto. Al verificar la información del paquete, este firewall puede asegurarse que no tenga ningún contenido malicioso.

¿Qué significa esto exactamente? Un encargado de seguridad puede usar un firewall proxy [7] para administrar y tratar mejor los problemas de seguridad, como evaluar diferentes amenazas y otros ataques en la red.

¿Por qué se utiliza este tipo de firewall? Puedes configurar un servidor proxy para bloquear el acceso a diferentes sitios web y filtrar cierto tráfico de puertos para proteger tu red interna.

Un inconveniente de un firewall proxy es que realiza una conexión adicional para cada paquete que entra y sale, lo que puede causar un retraso en el rendimiento del sistema y puede ser un punto débil durante un ataque externo.

### **Firewall de aplicaciones web**

Una puerta de enlace de aplicaciones es similar a un servidor proxy. A continuación, se muestra un ejemplo de cómo funciona:

El usuario de la computadora “A” crea una conexión con la puerta de enlace de la aplicación. Luego, la puerta de enlace de la aplicación decide si el contacto entre los dispositivos debe aprobarse o no. Si se aprueba, se establece una conexión con la computadora externa “B”.

Toda la información pasa por dos conexiones: la computadora del usuario “A” a la puerta de enlace de la aplicación y la puerta de enlace de la aplicación a la computadora externa “B”.

La puerta de enlace de la aplicación verifica todo el tráfico antes de enviarlo. Al igual que un servidor proxy, la dirección IP de la puerta de enlace de la aplicación es la única que se ve desde el exterior, por lo que la red interna permanece oculta.

### **¿Cómo funciona un firewall de red?**

Un firewall es configurado para regular y monitorear constantemente todo el tráfico entrante y saliente. Se diferencia de un simple analizador de tráfico en que un administrador de red o un administrador de seguridad puede controlar dicho tráfico.

Algunos firewall se pueden configurar para bloquear prácticamente todo, excepto personas y acciones que usted permita específicamente.

### **¿Cómo sería la función de un firewall de red en la vida real?**

Digamos que trabajas en una empresa con 100 empleados. Si no tienes un firewall configurado, esas 100 computadoras utilizadas por los empleados son vulnerables y están disponibles para cualquier persona con conexión a Internet. Los hackers pueden aprovechar fácilmente los errores de los empleados e interrumpir la red o propagar malware.

Estas son solo algunas de las formas en que un ataque malicioso a una red podría ocurrir en una red, como la hipotética compañía que no tiene firewall:

* **Inicio de sesión remoto:** los hackers pueden ver u obtener tus archivos en tu dispositivo.
* **Denegación de servicio (DoS por sus siglas en inglés):** ésta es una táctica común que utiliza la fuerza bruta. Un hacker envía una solicitud para abrir una sesión con un servidor que no se puede encontrar. El servidor de destino pronto se ve abrumado por estas solicitudes de sesión incontestables, lo que generalmente resulta en un bloqueo del sistema.
* **Bombardeo de correos electrónicos:** se envía una gran cantidad de correos electrónicos para que tu sistema de correo electrónico no pueda manejar ningún correo nuevo.
* **Macros:** los hackers crean su propia macro (también conocida como una secuencia de comandos de las demandas de la computadora para que se pueda ejecutar una aplicación) que bloquea tu computadora.
* **Virus:** un virus es una forma de malware que se copia a sí mismo de un sistema a otro y puede ser tan inofensivo como un mensaje de broma o puede destruir completamente tus datos.

Si una empresa tiene una configuración de firewall adecuada, cada dispositivo conectado a Internet tendría una línea de defensa que implementa reglas de seguridad particulares.

## En resumen

Los firewall son una tecnología de seguridad antigua, pero siguen siendo increíblemente importantes cuando se trata de proteger tu dispositivo. Ya sea que uses un firewall de red para proteger tu empresa o configures uno para un dispositivo inteligente en tu hogar, son un paso esencial para ayudar a prevenir ataques maliciosos.