¿Qué es un firewall en computación o en redes? ¿Para qué se usa?

¿Qué es un firewall en computación o en redes? ¿Para qué se usa? Firewall en inglés, cortafuegos en castellano. Cada rato en nuestras charlas de seguridad web hablamos del tema de forma tangencial, en nuestros post temáticos también y no faltará quien se rasque la testa y se pregunte en concreto esto qué es.

Lo que significa

Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico o paquete de datos específico en función de un conjunto definido de reglas de seguridad.Su propósito es establecer una barrera entre su red interna y el tráfico entrante de fuentes externas (como Internet) para bloquear el tráfico malicioso como virus y piratas informáticos.

Se puede configurar un firewall de red para que cualquier dato que ingrese o salga de la red tenga que pasar a través de él; esto se logra al examinar cada mensaje entrante y rechazar aquellos que no cumplan con los criterios de seguridad definidos. Cuando se configura correctamente, un firewall permite a los usuarios acceder a cualquiera de los recursos que necesitan, al tiempo que evita la entrada de usuarios no deseados, hackers, virus, gusanos u otros programas maliciosos que intentan acceder a la red protegida.

Los cortafuegos han sido una primera línea de defensa en seguridad de red durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas que

pueden ser confiables y no confiables fuera de las redes, como Internet. Los cortafuegos generalmente están diseñados para proteger el tráfico y las conexiones de la red y, por lo tanto, no intentan autenticar a los usuarios individuales al determinar quién puede acceder a una computadora o red en particular.

Los cortafuegos se pueden usar para separar los nodos de red de las fuentes de tráfico externas, las fuentes de tráfico internas o incluso aplicaciones específicas.
A pesar de ser una tecnología de seguridad más antigua, los firewalls son tan importantes como siempre, especialmente cuando los nuevos dispositivos inteligentes se conectan durante la revolución de Internet de las cosas (IoT).

Un firewall puede ser hardware, software o ambos.

¿Cómo funciona un firewall?

Los cortafuegos analizan cuidadosamente el tráfico entrante en función de reglas preestablecidas y filtran el tráfico proveniente de fuentes no seguras o sospechosas para evitar ataques. Los cortafuegos protegen el tráfico en el punto de entrada de una computadora, llamado puertos, que es donde se intercambia información con dispositivos externos. Por ejemplo, «La dirección de origen 173.18.1.1 puede alcanzar el destino 174.18.2.1 a través del puerto 23.»

Piense en las direcciones IP como casas y los números de puerto como habitaciones dentro de la casa. Solo las personas de confianza (direcciones de origen) pueden ingresar a la casa (dirección de destino), luego se filtra aún más para que las personas dentro de la casa solo tengan acceso a ciertas habitaciones (puertos de destino), dependiendo de si son el propietario , un niño o un invitado. El propietario puede acceder a cualquier habitación (cualquier puerto), mientras que los niños y los invitados pueden ingresar a un determinado conjunto de habitaciones (puertos específicos).

Un firewall actúa como un portero-celador. Supervisa los intentos de obtener acceso a su sistema operativo y bloquea el tráfico no deseado o las fuentes no reconocidas.

Un firewall actúa como una barrera o filtro entre su computadora y otra red, como Internet. Se podría pensar en un firewall como un controlador de tráfico. Ayuda a proteger su red e información administrando el tráfico de su red, bloqueando el tráfico de red entrante no solicitado y validando el acceso evaluando el tráfico de red para detectar cualquier cosa maliciosa como piratas informáticos y malware.

Su sistema operativo y su software de seguridad generalmente vienen con un firewall preinstalado. Es una buena idea asegurarse de que esas funciones estén activadas. Además, asegúrese de que su configuración de seguridad esté configurada para ejecutar actualizaciones automáticamente.

Un cortafuegos aísla absolutamente su computadora o servidor web de Internet mediante un «muro de código» que inspecciona cada «paquete» individual de datos a medida que llega a cada lado del cortafuegos, entrante o saliente de su computadora, para determinar si debe permitirse para pasar o ser bloqueado.

Los firewalls tienen la capacidad de mejorar aún más la seguridad al permitir un control granular sobre qué tipos de funciones y procesos del sistema tienen acceso a los recursos de red. Estos firewalls pueden usar varios tipos de firmas y condiciones de host para permitir o denegar el tráfico. Aunque suenan complejos, los firewalls son relativamente fáciles de instalar, configurar y operar.

Otros recursos valiosos del blog

- Cómo configurar Cloudflare: Dns, Ssl, firewall y Speed
- ¿Cuáles son las ventajas de litespeed web server?
- ¿Puede un Antivirus Proteger Completamente Su Centro De Datos?

- ¿Cómo funciona CPHulk? Cuales son sus usos; cómo configurar

Conclusión

Es muy relevante el tema. Y en el caso de nuestros clientes de HostDime, ¿sabía que puede contratar un firewall físico para su servidor con nosotros? ¿Que esto evitaría muchos problemas e inconvenientes con su información allí alojada? ¿Que es muy profesional tener uno implementado? ¿Que siempre será mejor prevenir que lamentar? Venga llame ya a nuestra empresa, pida una asesoría especializada al respecto. La seguridad no es un juego.