¿Me conviene un firewall físico o uno lógico? ¿Hardware o software?

¿Me conviene un firewall físico o uno lógico? ¿Hardware o software? La respuesta cortita para el que tiene afán y no quiere ahondar en el tema es, posea ambos, si puede; cada uno hace su oficio y se complementan además muy bien. pero vamos a entrar en detalles.

Bueno, hemos hablado de algunos elementos de seguridad web y hemos introducido algunos conceptos poco a poco en el blog. El camino está lejos de terminar, mucho menos el proceso de aprendizaje continuo que tenemos los webmasters y bloggers (y que no decir de los asesores TI).
Seleccionar un cortafuegos preciso es fundamental para construir un sistema de red seguro.

El Firewall proporciona el aparato de seguridad para permitir y restringir el tráfico, la autenticación, la traducción de direcciones y la seguridad del contenido.

Asegura la protección 365 * 24 * 7 de la red contra piratas informáticos. Es una inversión única para cualquier organización y solo necesita actualizaciones oportunas para funcionar correctamente. Al implementar el firewall no hay necesidad de ningún tipo de pánico en caso de ataques a la red.

Hardware

Un firewall de hardware se parece mucho a un enrutador, pero con muchas más funciones. De hecho, muchos enrutadores tienen un firewall de hardware incorporado, pero la gran mayoría de ellos carece de una gran profundidad de control y

características.

Un firewall de hardware se encuentra entre su red local de computadoras o servidor web e Internet. El firewall inspeccionará todos los datos que ingresan de Internet, pasando los paquetes de datos seguros mientras bloquea los paquetes potencialmente peligrosos. Para proteger adecuadamente una red sin obstaculizar el rendimiento, los cortafuegos de hardware requieren una configuración experta y, por lo tanto, pueden no ser una solución viable para las empresas sin un departamento de TI dedicado. Sin embargo, para las empresas con muchas computadoras o páginas web, poder controlar la seguridad de la red desde un solo dispositivo simplifica el trabajo.

La política y la operación de coincidencia se realizan en hardware dedicado, por ejemplo, utilizando una matriz de compuerta programable en campo (FPGA). Las principales ventajas de un firewall de hardware son un mayor ancho de banda y una menor latencia. Tenga en cuenta que el ancho de banda es la cantidad de paquetes que un firewall puede procesar por unidad de tiempo, y la latencia es la cantidad de tiempo que se requiere para procesar un paquete. No son lo mismo.

Los cortafuegos de hardware pueden funcionar con anchos de banda más rápidos, lo que se traduce en más paquetes por segundo (se logra fácilmente 10 Gbps). Además, los firewalls de hardware pueden operar más rápido ya que el procesamiento se realiza en hardware dedicado. El cortafuegos funciona casi a velocidades fijas; por lo tanto, se agrega muy poco retraso a los paquetes aceptados.

¿Cómo funcionan los firewalls de

hardware?

El firewall de hardware se configura de manera diferente dependiendo de su configuración actual. El firewall se encuentra fuera de su servidor y está conectado directamente a su enlace ascendente. Si se trata de una nueva configuración, el firewall se conecta a su servidor. Si se trata de una nueva configuración para un servidor de producción, se programará una ventana de mantenimiento para manejar la conexión física. Una vez que se establece la conexión con el servidor, todo el tráfico hacia y desde el servidor pasa a través del firewall, lo que lo obliga a pasar la inspección. Esto le permite tener un control granular sobre el tipo de tráfico que está recibiendo, lo cual es increíblemente importante.

Ventajas y desventajas

Como la mayoría de los desarrollos en la industria de TI, los firewalls de hardware más nuevos se centran en funciones «inteligentes» que analizan grandes conjuntos de datos para reconocer malware y ataques cibernéticos basados en actividades irregulares en lugar de depender únicamente de virus catalogados y vectores de ataque.

Otro beneficio de los firewalls de hardware es que siempre están activados. No hay necesidad de preocuparse por si la estación de trabajo que aloja su solución se bloqueará porque estos dispositivos están diseñados para protección 24/7. El único inconveniente de este tipo de solución es el nivel de monitoreo y mantenimiento que requiere. Los firewalls de hardware son extremadamente complejos y administrarlos no es una tarea fácil.

Software

A diferencia del hardware de firewall, el software de firewall son aplicaciones de programa que se ejecutan en una

computadora o servidor web. Funcionan monitoreando todos los puertos abiertos en un webserver y verificando toda la información sobre ellos. Cada puerto monitoreado está específicamente dedicado a un programa que tiene acceso a internet. Debido a esto, el software de firewall contiene una lista de aplicaciones disponibles para acceder a Internet en ciertos puertos. Por lo tanto, si la aplicación permitida está utilizando un puerto específico, el software del firewall verificará el contenido que ingresa en ese puerto y lo pasará a la computadora si es aceptado. Si una aplicación no verificada intenta acceder a la información, el firewall bloqueará toda la información entrante / saliente. Además, notificará al usuario que el programa está intentando acceder a Internet.

Ventajas y desventajas

La ventaja de los firewalls de software es su capacidad para controlar el comportamiento específico de la red de aplicaciones individuales en un sistema. Una desventaja significativa de un firewall de software es que generalmente se encuentra en el mismo sistema que está siendo protegido. Estar ubicado en el mismo sistema puede dificultar la capacidad del firewall para detectar y detener la actividad maliciosa. Otra posible desventaja de los firewalls de software es que, si tiene un firewall para cada servidor web, deberá actualizar y administrar el firewall de uno individualmente.

Por qué necesita un firewall de hardware y software

La diferencia entre el firewall de hardware y software es la siguiente: un firewall de hardware lo protege del mundo exterior, y un firewall de software protege un dispositivo específico de otros sistemas internos.

Más recursos interesantes de HostDime al respecto

- Cómo configurar Cloudflare: Dns, Ssl, firewall y Speed
- ¿Por qué los enrutadores son importantes en los Centros de Datos perimetrales?
- Cómo proteger a su organización de las amenazas de seguridad en medio del aumento de los teletrabajadores