¿Cuales son las diferencias entre un firewall y un antivirus?

¿Cuales son las diferencias entre un firewall y un antivirus? Hace rato venimos hablando de seguridad web en distintos post y escenarios. Y no falta quien aun le cueste trabajo distinguir una herramienta como el cortafuegos del anti malware.Tratemos de ayudar con un par de orientaciones útiles.

Antes de entrar en las características diferentes entre los dos digamos que ambas son utilizadas dentro de la estrategia de seguridad de un servidor web, ambas brindan un nivel de seguridad a los sistemas. El firewall evita el acceso no autorizado de redes externas a su sistema, mientras que el antivirus toma lo que está instalado en nuestro equipo de cómputo o nuestro servidor, lo analiza y procede a eliminar la amenaza que haya encontrado. Por decirlo de alguna forma sencilla, el primero es un escudo protector para el perímetro externo mientras que el segundo es la guardia interna, la segunda barrera de seguridad para nuestra información. Para extender la analogía pudiéramos decir que: Un firewall se puede considerar como el ejército, mientras que el antivirus se puede considerar como policía . Un antivirus como la policía combate las amenazas que ya ingresaron a su sistema de cómputo o que se instalarán y que pueden hacer que el sistema se ralentice o falle. En contraste, el firewall es como el ejército en la frontera que bloquea el ataque desde cualquier red externa en primer lugar.

Firewall

- Barrera entrante de la web
- Inspección de datos desde internet hacia el servidor

- Puede proteger no solo el hardware sino también el Software
- Responsabilidad: Autorizar o denegar los datos que pasan al sistema desde un procedencia exterior; monitorea y filtra, de acuerdo a las reglas de seguridad desplegadas.
- Tipo de seguridad: a nivel de red.
- ¿Posibles contraataques? Siempre; si un atacante no encuentra una fisura por un flanco, probará por otro seguramente.
- Los lineamientos de seguridad vienen de fábrica pero se pueden personalizar de acuerdo a la necesidad del servidor específico o sitio web en cuestión.

Antivirus

- Inspecciona, detecta y elimina un programa malicioso.
- Solo protege el software
- Gestiona amenazas internas y externas dependiendo de su potencia y configuración
- Responsabilidad: escanea ficheros corruptos que pudieran ralentizar o lesionar el funcionamiento del servidor y se deshace de ellos.
- Tipo de seguridad: a nivel de aplicación.
- ¿Posibles represalias? Complicado, después que se elimina completamente la amenaza, no hay segunda parte.
- Generalmente sus condiciones de funcionamiento vienen de fábrica.

Como se puede observar la labor de uno complementa el accionar del otro, luego lo más sensato sería tener ambas opciones activas en nuestro servidor web y de esa forma evitarnos dolores de cabeza y ofuscaciones prevenibles.

La protección contra virus del cortafuegos vigila el tráfico en la red, lo que inhibe la entrada de datos maliciosos en la misma y, por lo tanto, frustra los virus. Sin embargo, el

virus puede ingresar a su computadora a través de un enlace de spam, descargas o desde una unidad flash. Además, una vez que pasa por alto la protección del firewall, que lo elude, la función del antivirus resulta útil y conveniente.

El antivirus escanea y detecta el malware para impedir que se siga dispersando, ya sea borrando o segregando el archivo corrupto. Además, a pesar de que el firewall detiene el ingreso de malware y virus al sistema, no puede eliminar la amenaza cibernética que está infectando el sistema.

¿Cómo elegir el mejor software antivirus del servidor?

Si sus datos se almacenan en un servidor físico, debe protegerse con un antivirus de servidor adecuado. Puede instalar la versión de prueba gratuita del software antivirus y ver cómo funciona, o puede comprarlo de inmediato; sin embargo, debe encontrar uno con algunas de las 5 características que se enumeran a

continuación:

1. Detección directa de malware : los antivirus sever deberían proporcionarle una detección rápida de malware y la prevención de las amenazas, incluidos troyanos, gusanos y otros virus.
2. Sandboxing : esta característica autentica todos los procesos que se ejecutan en el servidor y evita que entidades maliciosas penetren en el sistema y dañen su server. Las aplicaciones o procedimientos no reconocidos se guardarán automáticamente y se ejecutarán bajo restricciones especiales.
3. HIPS (Protección contra intrusiones del host) : esta opción supervisa todas las actividades de las aplicaciones y procesos en el servidor y detiene cualquier actividad maliciosa que pueda dañar los datos, el sistema operativo, la memoria del sistema o las claves de registro.
4. Escritorio virtual : este es un entorno de espacio aislado que permite el acceso a Internet y las pruebas de software beta sin alterar la estructura del archivo.
5. Disco de rescate: el disco de rescate realiza análisis antivirus previos al arranque, y puede recuperar contraseñas, detectar y eliminar el rootkit o permitirle transformar los datos del disco dañado a otra unidad.

¿Contra qué ataques protegen los WAF?

Un firewall de aplicación web, o WAF, necesita proteger su servidor web y su contenido de las siguientes categorías de ataques:

1. Cross-Site Scripting (XSS) : código HTML malicioso insertado en un campo de entrada de página web por un hacker
2. Manipulación de campos ocultos : los piratas

informáticos reescriben el código fuente de una página web para alterar los valores contenidos en los campos ocultos y luego publican el código modificado de nuevo en el servidor
Intoxicación por cookies : alterar los valores de los parámetros contenidos en las cookies para corromper los datos pasados entre páginas web

3. Raspado web : extracción automatizada de datos de páginas web
4. Ataques DoS de capa 7 : abrumando un servidor web por la actividad recursiva de la aplicación
5. Manipulación de parámetros : alteración de los valores en los parámetros de una llamada a la página web
6. Desbordamiento de búfer : entrada del usuario que sobrescribe el código en la memoria
7. Opciones de puerta trasera o de depuración : informes de comentarios del desarrollador para pruebas de páginas web que los hackers pueden usar para acceder al procesador
8. Comando sigiloso : un ataque al sistema operativo de un servidor web
9. Navegación forzada : el hacker obtiene acceso a copias de seguridad o carpetas temporales en el servidor web
10. Configuraciones erróneas de terceros : manipulación de inserciones de contenido proporcionadas por otras compañías
11. Vulnerabilidades del sitio / inyecciones SQL : consultas ingresadas en los campos de autenticación de usuario

Aunque un WAF funciona como un front-end para un sitio web, esta tecnología no proporciona una serie de funciones esenciales de control de acceso que su proveedor de alojamiento web necesita. Los WAF se centran en el código HTTP y los procedimientos de solicitud para otras aplicaciones de Internet, como FTP. En estos casos, las versiones seguras de estos protocolos de aplicación, HTTPS y SFTP, también están cubiertas.

Otros recursos valiosos al respecto en HostDime:

- ¿Qué es la seguridad web? Definición, significado, concepto
- ¿Puede un Antivirus Proteger Completamente Su Centro De Datos?
- ¿Qué es un Firewall como servicio, FWaaS? Ventajas