¿Qué es un Firewall como servicio, FWaaS? Ventajas

¿Qué es un Firewall como servicio, FWaaS?¿Para qué sirve? ¿Vale la pena? Seguimos reflexionando en la seguridad de los servidores web, como una necesidad recurrente en nuestro diario acontecer.
Firewall as a Service es un firewall entregado como un servicio basado en la nube que permite a los clientes mover parcial o totalmente la inspección de seguridad a una infraestructura en la nube.

No solo oculta los dispositivos de cortafuegos físicos detrás de una nube de humo y espejos, sino que en realidad elimina el dispositivo por completo. Con esta tecnología, los sitios de una organización se conectan a un firewall único, lógico y global con una política de seguridad unificada compatible con las aplicaciones.

FWaaS aprovecha los avances en software y tecnologías en la nube para ofrecer una amplia gama de capacidades de seguridad de red a pedido donde sea que las empresas lo necesiten, incluido el filtrado de URL, análisis forense de red y prevención de infecciones. Todo el tráfico empresarial de centros de datos, sucursales, usuarios móviles e infraestructura en la nube se agrega a la nube. Esto permite que se aplique una política de seguridad integral en el tráfico de WAN e Internet, para usuarios de ubicaciones fijas y móviles.

Ventajas

Arquitectura más simple

Todo el tráfico de red se agrega a la nube, ya sea desde usuarios remotos, centros de datos u sucursales. Por lo tanto,

hay un solo punto para DPI que elimina la tediosa tarea de mantener sincronizadas las políticas de firewall distribuido. También se eliminan los dispositivos de cortafuegos. Todas las ubicaciones de una empresa son atendidas por un único firewall basado en la nube con una política de seguridad compatible con las aplicaciones.

Escalabilidad

La escalabilidad de FWaaS es un subproducto de su arquitectura simple. El uso de un único firewall para procesar todo el tráfico simplifica la planificación de la capacidad. Agregar nuevos sitios y cambios en el ancho de banda también se vuelve más fácil.

Política de seguridad unificada

Esto también es un subproducto de la arquitectura simple de FWaaS. La arquitectura de cortafuegos heredada requería dispositivos de firewall de transporte específicos para sucursales que no usan MPLS. Y, una organización puede obtener dispositivos de firewall de diferentes proveedores, o incluso diferentes modelos del mismo proveedor. Tener dispositivos diferentes hace que sea difícil mantener una política de seguridad uniforme en todos ellos.

Visibilidad total del tráfico de red

Las soluciones de seguridad web protegen a los usuarios contra amenazas de Internet como malware y phishing. Las redes dinámicas actuales necesitan un enfoque diferente. Numerosas empresas dependen de costosas MPLS basadas en redes WAN para vincular sucursales remotas. El backhauling del tráfico a través de una ubicación primaria conduce al efecto trombón después de que los usuarios remotos intenten acceder a aplicaciones empresariales basadas en la nube y SaaS. Esta configuración conduce a una falta de visibilidad y control en la red. Al migrar el firewall a la nube, las empresas pueden beneficiarse de una administración centralizada, así como de una seguridad única impulsada por una visibilidad completa de toda la red.

Mantenimiento más fácil

Los dispositivos de firewall heredados requerían actualizaciones y parches de software frecuentes. La falta o la demora de actualizaciones crearon riesgos de seguridad. Los firewalls de FWaaS siempre están actualizados, por lo que no hay riesgos de actualizaciones de software tardías o perdidas.

Esto libera al personal de TI para dedicar su tiempo a planificar las necesidades futuras de la infraestructura en lugar de las tareas de mantenimiento.

Mejor recuperación ante desastres

La mayoría de las empresas dependen en gran medida de la continuidad y el tiempo de actividad para mantener una ventaja competitiva en el mercado actual. El tiempo de actividad también es crítico para la satisfacción y retención del cliente. Con las amenazas de seguridad que surgen diariamente, una violación de la red de seguridad podría indicar un desastre que resulte en altos costos con respecto a la reputación y los recursos. Cuando utiliza el servicio de firewall administrado , obtiene expertos en seguridad de TI que son proactivos en la detección de nuevas amenazas y su mitigación. Además, el riesgo de amenazas a la seguridad de la red como resultado de la configuración incorrecta del firewall se minimiza y, en caso de falla, también hay una recuperación rápida.

Servicios de protección integral

Los proveedores de FWaaS ayudan a administrar y monitorear cada dispositivo de seguridad utilizado por su red. Esto generalmente incluye firewalls administrados, protección antimalware y antivirus, servicios de seguridad personalizados, redes privadas virtuales (VPN), escaneo de vulnerabilidades y detección de intrusos que ayudan a cumplir con los estándares de cumplimiento de la industria. Todos estos servicios se ofrecen desde un centro de datos de alta disponibilidad que posee sus salvaguardas de seguridad. Además, cada centro consta de tecnologías de redundancia integradas que garantizan la seguridad de su red en caso de falla.

Otros recursos indispensables

- ¿Por qué es importante la seguridad del sitio web?
- Protocolo http/2 tanto en litespeed web server como en Cloudflare
- ¿Cómo está mejorando la inteligencia artificial la industria del alojamiento web?