

WHITE PAPER

Ampliación de capacidades para lograr una seguridad de alto rendimiento

Siete criterios para elegir firewalls de nueva generación



Resumen

La transición al trabajo híbrido y la rápida adopción de los servicios en la nube han hecho que, hoy en día, los usuarios puedan conectarse a cualquier recurso desde cualquier lugar y con cualquier dispositivo. Si bien esta flexibilidad es necesaria, lo cierto es que también amplía la superficie de ataque, lo que deja la puerta abierta a amenazas nuevas. Las empresas deben asegurarse de que su seguridad de red les ofrezca visibilidad total de su infraestructura distribuida al completo.

De lo contrario, les resultará imposible poner en marcha y coordinar de manera eficaz un sistema de protección con funciones de detección y corrección de amenazas lo suficientemente rápidas.

Combinar firewalls de nueva generación (NGFW) con los servicios de seguridad basados en la IA de FortiGuard proporciona inteligencia de amenazas en tiempo real, lo que permite ofrecer a los usuarios una seguridad por capas con funciones de prevención de intrusiones, análisis de malware y filtrado web para garantizar la máxima protección. Esta combinación reduce la probabilidad de que se produzcan interrupciones y brechas de datos, lo que, a su vez, minimiza el riesgo de incurrir en costes elevados derivados de las tareas de corrección y de que la reputación de la empresa se vea perjudicada. Los servicios de seguridad que se integran estrechamente con el firewall brindan un modelo eficaz para mejorar la seguridad de red.

Los NGFW deben ofrecer protección contra amenazas en todos los perímetros de las sucursales, el campus y el centro de datos sin que el rendimiento se vea afectado. Para que resulten eficaces en toda la empresa, también deben formar parte de una arquitectura de seguridad más general, integrada y automatizada y abordar las cuestiones relacionadas con la escalabilidad, el coste de propiedad y las consecuencias para el medio ambiente.

Requisitos para evaluar los NGFW

Los NGFW desempeñan un papel fundamental en la protección contra amenazas, ya que ofrecen una seguridad que abarca del perímetro de la red al centro de datos, segmentos internos, la nube y las redes de OT. Los equipos de seguridad recurren a los NGFW para obtener más visibilidad de las amenazas que afectan a los usuarios, los dispositivos, las aplicaciones y la red y aplican la protección contra amenazas siempre que sea necesario. Las empresas deben tener en cuenta siete criterios clave a la hora de evaluar un NGFW:

1. Servicios de seguridad integrados con IA. Los servicios de seguridad basados en la inteligencia artificial (IA) complementan las funciones de los firewalls tradicionales con funciones de detección y protección proactivas frente a las amenazas en evolución, lo que incluye las nuevas amenazas basadas en la IA. Estos servicios ayudan a reducir la carga de trabajo de los equipos de seguridad, mejoran la eficiencia de la protección y la asignación de recursos y optimizan la gestión de la seguridad para que se puedan tomar decisiones más acertadas.

Los NGFW que integran servicios de seguridad basados en la IA ofrecen más protección que los firewalls tradicionales porque incluyen funciones de machine learning capaces de analizar grandes cantidades de datos para detectar patrones anómalos que puedan ser indicio de actividad maliciosa. Gracias a la IA, el firewall puede adaptar las políticas de seguridad de manera dinámica en función de los análisis del tráfico de la red en tiempo real. Así, se garantiza que las medidas de seguridad que se aplican son oportunas y eficaces, lo que reduce el riesgo de sufrir brechas y optimiza la asignación de recursos.

2. Rendimiento de la protección contra amenazas. El rendimiento de la protección contra amenazas mide el desempeño del NGFW cuando ejecuta todas las funciones de protección contra amenazas (firewalls, prevención de intrusiones, antivirus, control de aplicaciones, etc.). Es fundamental que el NGFW siga ofreciendo un alto rendimiento cuando están activas todas estas funciones. Muchos proveedores de NGFW juegan con la ambigüedad a la hora de presentar sus datos relativos al rendimiento de la protección contra amenazas. Por eso, es importante fijarse bien en la información sobre el rendimiento que ofrecen en su documentación, para asegurarse de que reflejen los resultados de las pruebas de carga con todas las funciones de protección contra amenazas activadas.

3. Gestión centralizada. La interfaz de gestión es lo que hace que muchos arquitectos de seguridad decidan descartar la solución que están evaluando. Aunque se haya prestado mucha atención a las funciones y la interfaz de usuario del sistema de gestión, si estas se limitan al NGFW, los equipos de seguridad se verán obligados a pasar de un panel a otro para evaluar las vulnerabilidades y responder a las amenazas. La única manera de lograr una visibilidad y un control integrales es que el NGFW forme parte de una arquitectura de seguridad más general e integrada en la que pueda intercambiar información sobre las amenazas con otros dispositivos de la red y recibir inteligencia de amenazas automáticamente. Desde el punto de vista de la seguridad, lo más eficaz es tener una gestión centralizada. También es lo más eficiente a nivel operativo, ya que reduce tanto el tiempo que hay que dedicar a las tareas administrativas como los costes derivados de las actividades de formación.

**4,45
mills. de \$**

Según un informe reciente, el coste medio global de una brecha de datos alcanzó la cifra récord de 4,45 millones de dólares en 2023, lo que supone un aumento del 2,25 % con respecto al año anterior.¹

4. Garantía de una estrategia de seguridad más amplia. El trabajo híbrido ha cambiado el mundo de la ciberseguridad para siempre. Es muy común que las empresas tengan oficinas en distintos lugares que dependen de conexiones WAN redundantes y, en muchos casos, requieren soluciones de seguridad adicionales como SD-WAN, acceso Zero Trust a la red (ZTNA) y SASE (Secure Access Service Edge).

Numerosos proveedores de NGFW ofrecen funciones SD-WAN, SASE y ZTNA como complementos, lo que ayuda a las empresas con sucursales construir redes de alto rendimiento y alta disponibilidad. Sin embargo, esto no es lo ideal. Es mejor buscar un proveedor que ofrezca funciones SD-WAN, SASE y ZTNA seguras y totalmente integradas en sus NGFW, ya que esto permite consolidar varios productos independientes y aplicar controles centralizados. La consolidación de herramientas contribuye a la reducción de los costes de inversión y a la eliminación de las carencias de seguridad.

5. Relación precio-rendimiento y otros factores operativos que tener en cuenta. Para ampliar el rendimiento, lo que hacen algunos proveedores es aumentar el tamaño y el precio de sus NGFW, una estrategia que puede chocar con el deseo de las empresas de reducir el número de soluciones tecnológicas que utilizan. Busque un NGFW que ofrezca el rendimiento necesario en el formato más compacto posible. Optar por un NGFW de menor tamaño puede reducir el coste total de propiedad (TCO), ahorrar espacio y disminuir el consumo energético, tres aspectos que constituyen objetivos importantes para las empresas que se preocupan por el medio ambiente. Otro factor que hay que tener en cuenta al evaluar el TCO de un NGFW es el coste derivado de su mantenimiento y de la asistencia técnica. Las tecnologías más asentadas juegan con ventaja en este sentido, al igual que los productos de los proveedores que realizan inversiones importantes en investigación y diseño. Los propietarios de NGFW incluidos en esta categoría disfrutarán de implementaciones más fluidas y de un menor volumen de llamadas al servicio de asistencia. A la hora de evaluar NGFW de hardware, fíjese en si ofrecen fuentes de alimentación redundantes y compatibilidad con interfaces de red de 40 GbE y 100 GbE. Estas opciones garantizan la resiliencia y facilitan la migración a redes de mayor capacidad.

6. Tecnología ASIC como factor crítico a la hora de elegir un NGFW. Estos chips especializados se han diseñado para acelerar funciones de seguridad específicas, como el procesamiento de paquetes, el cifrado y el descifrado. Las empresas deben elegir NGFW con ASIC bien diseñados para asegurarse de que son capaces de gestionar grandes volúmenes de tráfico y de ofrecer protección en tiempo real frente a las amenazas avanzadas (latencia baja), todo ello mientras reducen el consumo de energía. Si cuentan con el ASIC adecuado, los NGFW pueden ser una solución de seguridad que ofrezca una mayor eficacia y rentabilidad.

7. Validación externa independiente. A pesar de que la seguridad de red es un sector que cambia a gran velocidad, ninguna empresa puede permitirse correr el riesgo de adoptar una solución que no se haya sometido a las pruebas oportunas. En lugar de confiar ciegamente en lo que diga el proveedor, los arquitectos deberían buscar evaluaciones externas realizadas por organismos de pruebas como [cyberratings.org](https://www.cyberratings.org).

Principales prioridades en materia de NGFW

El NGFW desempeña un papel fundamental en la protección del conjunto de la empresa (tanto en los entornos de IT como en los de OT), lo que incluye los datos corporativos y de los clientes, por lo que los arquitectos de seguridad deberían actuar con diligencia a la hora de estudiar las diferentes opciones. Cuando se evalúen soluciones de NGFW, hay que tener muy presente el riesgo de que prioricen el rendimiento en detrimento de la seguridad, o viceversa. Es imprescindible que sean capaces de ofrecer una protección coherente y consolidada en todos los perímetros distribuidos con el mínimo efecto posible en el rendimiento.

Pero estos no son los únicos aspectos que deben tener en cuenta las empresas. Debido a las limitaciones de espacio y energía, deberían dar preferencia a las soluciones de NGFW compactas que ocupen menos, consuman menos energía y sean lo suficientemente flexibles como para implementarse en el centro de datos o en el perímetro de la red. Los arquitectos de seguridad también deberían asegurarse de que el NGFW se pueda integrar en la arquitectura de seguridad general y de que ofrezca visibilidad integral, además de la capacidad de intercambiar inteligencia de amenazas automáticamente con otros dispositivos.

¹ IBM Security y Ponemon Institute, [The Cost of a Data Breach Report 2023](#) (en inglés).