

Firewalls de red integrados: una solución esencial para la empresa distribuida actual

¿Qué es una solución de firewall de red integrado?

La mayoría de las organizaciones carecen de seguridad y visibilidad coherentes en los distintos segmentos de sus redes distribuidas, y los ciberdelincuentes están aprovechando esta circunstancia a su favor. La interconexión del centro de datos, el campus, la nube y las oficinas, ha incrementado el tráfico de un extremo a otro, lo que permite que una brecha abierta en una parte de la red se propague rápidamente a otras. La forma más eficaz de abordar este desafío es implementar la misma seguridad en todas las partes de la red, permitiendo así la correlación centralizada de amenazas y la protección coordinada para múltiples áreas de la empresa de manera simultánea. Sin embargo, las complejidades y diferencias entre los diversos ecosistemas de red pueden dificultar esta tarea.

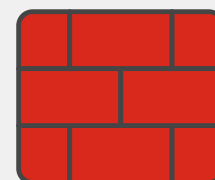
Los firewalls de red se pueden implementar para proporcionar funciones críticas de NGFW en cualquier lugar de la red (campus, centro de datos, nube FWaaS y entornos SASE) con la gestión unificada remota. Usando el mismo sistema operativo, se crea una plataforma única e integrada que puede abarcar, escalar y adaptarse a las redes dinámicas y distribuidas actuales. Una consola de gestión unificada puede coordinar la protección en todos los dominios de TI, incluidos sitios corporativos, nubes públicas y privadas, y trabajadores remotos. Este enfoque integrado permite a los equipos de TI automatizar la detección y respuesta a amenazas, orquestar configuraciones y aplicar políticas sin invertir horas en operaciones manuales innecesarias, una circunstancia especialmente relevante teniendo en cuenta la limitación en recursos debida a la brecha de competencias en ciberseguridad.

La necesidad de firewalls de red integrados

Los firewalls de red son esenciales para proteger las redes de accesos no autorizados y ataques malintencionados. Actúan como guardianes digitales, supervisando y controlando el tráfico de la red para evitar accesos no autorizados, fugas de datos y otras amenazas a la seguridad. Estas soluciones están diseñadas para abordar cuatro desafíos críticos a los que se enfrentan las organizaciones de TI en la actualidad:

1. Complejidad de TI

Muchos de los NGFW actuales no pueden admitir las capacidades clave, lo que obliga a los departamentos de TI de las empresas a adquirir soluciones de seguridad independientes para las sedes corporativas, los entornos de nube pública y privada, y los trabajadores remotos, lo cual genera incoherencias operativas, como errores de configuración que pueden provocar brechas en la red.



Fortinet ha sido reconocida como líder en el Magic Quadrant™ de Gartner® para firewalls de red durante 13 años consecutivos y ocupa la posición más alta en capacidad de ejecución en el último informe.¹

2. Déficit de competencias en ciberseguridad

Además de la complejidad, los productos específicos de ciberseguridad aumentan el riesgo para las organizaciones debido a sus largos periodos de adaptación. La existencia de varios productos de este tipo obliga al personal de TI encargado de la ciberseguridad a dedicar más tiempo a aprender nuevas funciones y cuadros de mando, lo que supone un riesgo aún mayor para las empresas, ya que muchos puestos del área de ciberseguridad siguen sin cubrirse debido a la gran escasez mundial de talento.

3. El auge de las amenazas avanzadas

La complejidad y la escasez de habilidades en ciberseguridad no son los únicos factores que impulsan la necesidad de firewalls de red integrados. Las amenazas avanzadas y sofisticadas aumentan con rapidez, en muchos casos gracias a la inteligencia artificial. Estas amenazas avanzadas son cada vez más difíciles de detectar y resultan más devastadoras para las empresas. Sus vectores de ataque abarcan la web, las aplicaciones, los contenidos y los dispositivos. El ransomware, por ejemplo, sigue causando trastornos en sectores verticales, como la tecnología operativa (OT), las administraciones central, regional y local, el sector industrial y las organizaciones sanitarias.

4. El rol de la IA/ML y la inteligencia sobre amenazas

La complejidad, la supervisión manual y un panorama de amenazas en expansión exigen una protección coordinada. No basta con que el firewall pueda abarcar las diferentes áreas de la red. También deben contener las capacidades de inteligencia artificial y aprendizaje automático (IA/ML) necesarias para proteger frente a amenazas conocidas y desconocidas. Al incorporar a los firewalls de red seguridad impulsada por IA/ML, estos pueden identificar y clasificar aplicaciones, direcciones URL web, usuarios, dispositivos, malware, etc., todo ello mientras automatizan la aplicación de políticas en todos los dominios. IA/ML se encuentra en el corazón de la automatización del firewall de red y puede reducir considerablemente la cantidad de trabajo manual que implica la protección de TI empresarial.

Qué buscar en una solución de firewall de red para entornos híbridos

Gestión centralizada y unificada

Las ventajas más importantes de los firewalls de red son la detección de amenazas, la gestión de políticas y la orquestación automática de respuestas a las amenazas en cualquier punto de la red utilizando todas las herramientas a su disposición.

La gestión centralizada coordina y unifica sus dominios en una única solución de seguridad de TI empresarial, lo que permite una protección sencilla y automatizada que se extiende desde las sedes corporativas hasta la nube y los trabajadores remotos. Dado que las distintas organizaciones tienen requisitos diferentes para gestionar los firewalls de red dispares, debe darse soporte a todos los modelos posibles, incluidos dispositivos, máquinas virtuales, SaaS y servicios de firewall gestionados.

Su firewall de red también debe reunir a los equipos del centro de operaciones de red (NOC) y del centro de operaciones de seguridad (SOC) a través de un único cuadro de mando para gestionar y supervisar toda la superficie de ataque.

Dispositivos basados en ASIC

Cada entorno de su red presenta desafíos de seguridad únicos. Los sitios corporativos requieren de dispositivos que puedan escalar las funciones de seguridad, lo que garantiza una protección coherente sin afectar a la experiencia del usuario.

Las organizaciones de hoy en día, ávidas de rendimiento, necesitan dispositivos que incluyan circuitos integrados de aplicación específica mejorados, o ASIC, para aumentar la velocidad de los servicios de seguridad críticos. Un appliance de seguridad diseñado con un ASIC personalizado puede descargar numerosas funciones que consumen muchos recursos, como firewalls, VPN, IPS e incluso SSL/TLS o inspección profunda de paquetes (DPI). Los ASIC pueden mejorar considerablemente el rendimiento de las funciones de seguridad en comparación con los procesadores generales.

Firewall nativo en la nube

Los firewalls nativos cloud protegen las cargas de trabajo de las aplicaciones de nube pública implementadas en entornos de IaaS en modalidad de infraestructura como código. La incorporación de un firewall de red nativo en la nube a su entorno de nube también reduce la carga de trabajo de las operaciones de seguridad de la red al ampliar la visibilidad y eliminar la necesidad de configurar, aprovisionar y mantener una infraestructura de software de firewall, lo cual permite a los equipos de seguridad centrarse en la gestión de políticas.



Firewall virtual

Los firewalls virtuales se utilizan habitualmente para proteger entornos virtualizados en centros de datos definidos por software y entornos multi-cloud. Al ser la solución menos costosa y más fácil de transportar, el personal de TI puede trasladar rápidamente un firewall virtual de una nube a otra. Los firewalls virtuales dentro de una solución de firewall de red permiten además un ecosistema de seguridad integral para su centro de datos definido por software, lo que ayuda a su proceso de consolidación a la vez que protege su entorno de las amenazas utilizando una variedad de servicios de ciberseguridad más allá del firewall stateful.

Firewall como servicio

Firewall como servicio (FWaaS) es una solución de firewall que se ofrece como servicio basado en la nube, lo que permite a las empresas simplificar y escalar su infraestructura de TI. En muchos aspectos, el FWaaS es muy parecido al firewall físico que se implementa en las instalaciones, ya que ofrece toda la gama de funciones de NGFW, como filtrado web, protección avanzada frente a amenazas, IPS y seguridad DNS. Un firewall de red implementado como solución FWaaS amplía sus exclusivas funciones a usuarios y dispositivos distribuidos, combinando una escalabilidad casi instantánea con un control centralizado.

Un único sistema operativo

La rápida expansión de los perímetros de la red ha agravado los desafíos que plantea la proliferación de proveedores y soluciones específicas. Las distintas soluciones especializadas no pueden trabajar juntas ni compartir información, lo que imposibilita la aplicación de políticas de seguridad coherentes, la visibilidad de extremo a extremo y la automatización. Intentar mantener y supervisar numerosas soluciones híbridas, de hardware, software y XaaS también sobrecarga a los equipos de seguridad.

Un único sistema operativo consolida numerosas tecnologías y casos de uso en un marco de gestión y políticas único y simplificado. Mientras que la consola de gestión unificada aúna sus operaciones de front-end, un sistema operativo único garantiza que diversas implantaciones, como dispositivos, firewalls virtuales y nativos de la nube, y agentes FWaaS, puedan interoperar en el back-end.

El valor de los firewalls de red integrados

Los firewalls de red integrados aportan enormes beneficios a las TI empresariales, entre los que se incluyen el aumento de la eficiencia operativa de las TI, la simplificación de las operaciones de ciberseguridad, la reducción del riesgo organizativo, el alivio del déficit de competencias en ciberseguridad, la protección resistente frente a ciberamenazas conocidas y desconocidas, la automatización y coordinación mediante IA/ML y un menor coste total de propiedad.

¹ [A Leader Positioned Highest in Ability to Execute](#), Fortinet, acceso del 13 de septiembre de 2024.