SOPHOS
Cybersecurity delivered.

Guía para la adquisición de firewalls next-gen

Según encuestas recientes, estos son los principales problemas que tienen los administradores de redes y responsables de TI con sus firewalls:

- Escasa visibilidad sobre las aplicaciones, los riesgos y las amenazas de la red
- Dudas sobre la protección contra el ransomware y los ataques más recientes
- Falta de respuesta o asistencia cuando hay una amenaza en la red
- Desafíos a la hora de alcanzar los objetivos de red SD-WAN

Si alguno de estos problemas le resulta familiar, no es usted el único. El caso es que la mayoría de firewalls next-gen de hoy día no están cumpliendo con su trabajo. No son capaces de ofrecer una visibilidad adecuada ni una protección o respuesta a amenazas apropiada, y carecen de funciones de red SD-WAN sencillas y flexibles.

A la hora de preseleccionar su próximo firewall, puede resultar difícil saber por dónde empezar. En primer lugar, conviene que identifique sus requisitos clave. Una vez hecho esto, no tendrá más remedio que enfrentarse a la ardua tarea de leer todos los sitios web y las hojas de datos de los proveedores para determinar qué firewall puede no solo cubrir sus necesidades, sino también hacer el trabajo que se dice que hace.

Cómo utilizar esta guía

Esta guía de compra está diseñada para ayudarle a tomar la decisión más acertada para su empresa y evitar acabar lamentándose como otros compradores de firewalls. Detalla todas las características y funciones que debe tener en cuenta a la hora de evaluar un firewall y decidir su adquisición. También hemos incluido preguntas importantes para su partner o proveedor de TI a fin de garantizar que el producto satisfaga sus necesidades. Y, en las últimas páginas, encontrará una práctica tabla que le ayudará a preseleccionar los proveedores de firewalls más adecuados y así ahorrar tiempo.

La tormenta perfecta en la seguridad de redes: el cifrado

El incesante incremento de los flujos de tráfico cifrado ha creado una tormenta perfecta, con consecuencias nefastas. Veamos estos importantes datos:

- El 90 % del tráfico de Internet ahora está cifrado por TLS
- El 50 % de los servidores de malware, PUA y hackers utilizan el cifrado para evitar la detección
- La gran mayoría de las empresas no inspeccionan el tráfico cifrado

Cuando preguntamos a las empresas por qué no inspeccionan el tráfico cifrado, mencionan el rendimiento como la razón principal. La inspección de TLS simplemente consume demasiados recursos para que la mayoría de firewalls puedan hacer frente al enorme volumen de tráfico cifrado. La segunda razón más importante para no inspeccionar el tráfico cifrado es que suele causar problemas de usabilidad, puesto que degrada Internet.

Este reto fundamental que plantea el cifrado y la incapacidad de la mayoría de firewalls para abordarlo está generando otra serie de problemas: la visibilidad sobre los comportamientos y contenidos de riesgo, el cumplimiento de la normativa y la protección contra el ransomware, los ataques y las filtraciones. En efecto, el cifrado es la causa raíz de muchos de los principales problemas de seguridad de las redes de hoy en día. Por desgracia, la mayoría de las redes se limitan a hacer la vista gorda ante la gran mayoría del tráfico que pasa por ellas. Esto ya no es necesario. Hay una forma muy eficaz de afrontar este reto.

Para obtener más información, consulte nuestro monográfico: ¿El cifrado ha hecho irrelevante su firewall actual?

Principales funciones fundamentales

Para resolver sus mayores desafíos en cuanto a la visibilidad de la red, la protección y la respuesta a las amenazas, he aquí cuatro funciones críticas imprescindibles que necesita en su próximo firewall y que probablemente no tenga en la actualidad:

Inspección TLS 1.3: el 90 % del tráfico de Internet ahora está cifrado y esa cifra va en aumento, por lo que es absolutamente crítico que su próximo firewall incluya la inspección TLS 1.3. Y lo que quizás es más importante, debe proporcionar la información y el rendimiento necesarios para hacerlo de forma eficiente, sin convertirse en un cuello de botella ni obligarle a comprar un firewall mucho más caro de lo que realmente necesita. No todo el tráfico cifrado requiere inspección, y no todo el tráfico cifrado la admite. Su próximo firewall tiene que permitir todos los estándares y suites de cifrado más recientes. También debe contar con excepciones inteligentes integradas para ser más selectivo con respecto al tráfico que debe inspeccionar, y al mismo tiempo proporcionar herramientas para identificar fácilmente los posibles problemas y añadir excepciones sobre la marcha para evitarlos. También debe ofrecer un rendimiento adecuado para hacer frente a un volumen de cifrado cada vez mayor, tanto en el presente como en el futuro.

Protección contra amenazas de día cero: las amenazas evolucionan constantemente. La variante de ransomware utilizada para atacar a una empresa mañana será, casi con toda seguridad, diferente de la utilizada ayer. Esta es la realidad del panorama actual de las amenazas. Su próximo firewall debe contar con inteligencia artificial basada en múltiples modelos de Machine Learning, además de espacios seguros con detección avanzada de exploits y detección de ransomware de CryptoGuard para identificar las últimas amenazas de día cero y detenerlas antes de que entren en la red.

Aceleración de aplicaciones FastPath: es probable que alrededor del 80 % del tráfico de su red provenga de aproximadamente el 20 % de sus aplicaciones. Estos flujos de elefante son típicos de las herramientas de reunión y colaboración, streaming de contenido y VoIP. Consumen muchos recursos para ser inspeccionados y requieren un rendimiento óptimo para ofrecer una gran experiencia de usuario, lo que supone un enorme desafío. Su próximo firewall debe ser capaz de gestionar adecuadamente estos flujos de tráfico de confianza y descargarlos para proporcionar un rendimiento óptimo y crear un margen de rendimiento adicional para el tráfico que realmente necesita una inspección de paquetes más detallada.

Redes y orquestación de SD-WAN: la mayoría de organizaciones han pasado a depender de conexiones a Internet WAN redundantes y tienen múltiples emplazamientos que requieren soluciones SD-WAN sencillas, asequibles y resilientes que se adapten a su red. Cualquiera que haya intentado configurar túneles VPN entre varios firewalls, gestionar la redundancia automática y los escenarios de conmutación por error, y optimizar el enrutamiento de aplicaciones a través de múltiples enlaces WAN sabe que esto supone un gran reto. Su próximo firewall debe ofrecer capacidades SD-WAN integradas que incluyan un enrutamiento SD-WAN automatizado y resiliente, opciones SD-Branch asequibles y una orquestación de red SD-WAN sencilla.

Integración con otros productos de ciberseguridad: ya no basta con que los productos de seguridad informática funcionen de forma aislada. Los sofisticados ataques actuales requieren múltiples capas de protección que funcionen de manera coordinada y compartan información para dar una respuesta sincronizada. Su próximo firewall debe integrarse con otros sistemas, como su protección antivirus para endpoints, a fin de compartir información importante sobre amenazas y telemetría. Esto permitirá que ambos sistemas funcionen mejor de forma conjunta para coordinar una defensa cuando sufra un ataque. Estos sistemas también deben compartir una interfaz de gestión común para facilitar el despliegue, la gestión diaria, la búsqueda de amenazas entre productos y la generación de informes.

Estas cuatro funcionalidades garantizarán que los principales problemas de sus firewalls actuales pasen a ser historia, y reforzarán su protección de redes de cara al futuro.

Funciones críticas	Preguntas para los proveedores
Inspección TLS 1.3 Proporciona visibilidad del creciente volumen de tráfico cifrado que atraviesa las redes	‣ ¿Su inspección TLS es compatible con el último estándar 1.3? ‣ ¿Funciona en todos los puertos y protocolos? ‣ ¿Se basa en streaming o en proxy? ‣ ¿Cuál es el impacto sobre el rendimiento? ‣ ¿El panel de control ofrece visibilidad de los flujos de tráfico cifrados? ‣ ¿El panel de control ofrece visibilidad de los sitios que no admiten el descifrado? ‣ ¿Ofrece herramientas sencillas que permitan añadir excepciones para sitios problemáticos? ‣ ¿Viene con una lista de exclusión completa? ‣ ¿Quién mantiene la lista? ¿Se actualiza periódicamente?
Protección contra amenazas de día cero Protección contra las amenazas desconocidas más recientes mediante Machine Learning y espacios seguros	‣ ¿Incluye su firewall tecnología para detectar amenazas nunca vistas anteriormente? ‣ ¿Utiliza Machine Learning para analizar los archivos? ‣ ¿Cuántos modelos de Machine Learning se aplican? ‣ ¿Incluye su solución el aislamiento en espacios seguros? ‣ ¿El aislamiento en espacios seguros permite el paso del archivo mientras se analiza? ‣ ¿La solución de espacio seguro se ejecuta localmente o en la nube? ‣ ¿Incluye la solución de espacio seguro tecnología líder de protección de endpoints para identificar amenazas como el ransomware en el entorno de espacio seguro? ‣ ¿Qué tecnología para endpoints se utiliza para asistir en el aislamiento en espacios seguros? ‣ ¿Qué tipo de generación de informes se proporciona de forma integrada (en lugar de un producto de generación de informes aparte)? ‣ ¿Qué tipo de visibilidad ofrece el panel de control?
Aceleración de aplicaciones FastPath Descarga del tráfico de aplicaciones de confianza a una ruta rápida FastPath para mejorar el rendimiento y reducir la carga de trabajo	‣ ¿Admite su firewall la aceleración de FastPath del tráfico de confianza y de flujos de elefante? ‣ ¿Se realiza por software o por hardware? ‣ ¿Cómo se identifican las aplicaciones para la aceleración de FastPath? ‣ ¿Qué herramientas de políticas se ofrecen a los administradores para controlar qué aplicaciones se descargan? ‣ ¿Se proporcionan firmas de manera predefinida para acelerar algunas aplicaciones y colocarlas en la ruta rápida FastPath? ‣ ¿Son sus procesadores de flujo de paquetes FastPath programables, actualizables y adaptables al futuro?
Redes y orquestación de SD-WAN Herramientas potentes y fáciles de usar para administrar múltiples enlaces WAN y redes de superposición de sucursales	‣ ¿Integra su firewall capacidades sofisticadas de SD-WAN? ‣ ¿Permite el enrutamiento del tráfico de aplicaciones a través de enlaces WAN por aplicación, usuario o tipo de servicio? ‣ ¿Permite identificar y enrutar el tráfico de aplicaciones oscuras o personalizadas? ‣ ¿Ofrece transiciones de impacto cero que mantienen las conexiones de las aplicaciones cuando se produce una interrupción del ISP o espera a que la aplicación solicite una nueva conexión? ‣ ¿Ofrece una orquestación centralizada de redes de superposición VPN SD-WAN de apuntar y hacer clic entre varios firewalls y emplazamientos? ‣ ¿Su firewall descarga y acelera el tráfico de túnel VPN de SD-WAN por hardware? ‣ ¿Ofrece opciones de hardware asequibles y sin necesidad de intervención para conectar de forma segura emplazamientos o dispositivos remotos?
Integración con otros productos de seguridad La integración es esencial para ofrecer una protección por capas adecuada y compartir información entre los productos para responder a las amenazas o para las investigaciones forenses y la búsqueda de amenazas	‣ ¿Su firewall se integra con una tecnología para endpoints? ‣ ¿Qué información se comparte entre los dos productos? ‣ ¿Una amenaza identificada por un producto se comparte con el otro? ‣ ¿Cuál es la respuesta cuando se detecta una amenaza? ¿Puede aislar las amenazas automáticamente? ¿Cómo? ‣ ¿Facilita el endpoint alguna información sobre los usuarios o el uso de las aplicaciones al firewall? ‣ ¿Se pueden gestionar el firewall y el endpoint desde la misma consola? ¿Está basada en la nube? ‣ ¿Se puede hacer una búsqueda de amenazas entre productos (XDR)? ‣ ¿Ofrece el proveedor un servicio de supervisión de la red y respuesta a las amenazas totalmente administrado? ‣ ¿Se integra el firewall con otros productos como Wi-Fi, ZTNA, dispositivos perimetrales o switches de red?

Funciones básicas de firewall

Las tecnologías siguientes también son componentes esenciales de cualquier solución de firewall. La mayoría de estas funciones son elementos básicos consolidados de cualquier firewall, por lo que los proveedores suelen diferenciarse en función de la facilidad de gestión y el nivel de visibilidad procesable que ofrecen.

Asegúrese de que su próximo firewall no solo incluya estas funciones, sino que también ofrezca una gestión sencilla y, lo que es más importante, una mayor visibilidad de los riesgos y problemas en cada una de estas áreas.

Funciones básicas	Preguntas para los proveedores
Inspección detallada de paquetes y prevención de intrusiones Ofrece descifrado e inspección de amenazas y exploits	‣ ¿Su inspección TLS es compatible con el último estándar 1.3? ‣ ¿Funciona en todos los puertos y protocolos? ‣ ¿Se basa en streaming o en proxy? ‣ ¿Cuál es el impacto sobre el rendimiento? ‣ ¿El panel de control ofrece visibilidad de los flujos de tráfico cifrados? ‣ ¿El panel de control ofrece visibilidad de los sitios que no admiten el descifrado? ‣ ¿Ofrece herramientas sencillas que permitan añadir excepciones para sitios problemáticos? ‣ ¿Viene con una lista de exclusión completa? ‣ ¿Quién mantiene la lista? ¿Se actualiza periódicamente?
Protección contra amenazas avanzadas Identifica bots y otras amenazas avanzadas y malware que intentan realizar llamadas a casa o comunicarse con servidores de comando y control	‣ ¿Incluye su firewall tecnología para detectar amenazas nunca vistas anteriormente? ‣ ¿Utiliza Machine Learning para analizar los archivos? ‣ ¿Cuántos modelos de Machine Learning se aplican? ‣ ¿Incluye su solución el aislamiento en espacios seguros? ‣ ¿El aislamiento en espacios seguros permite el paso del archivo mientras se analiza? ‣ ¿La solución de espacio seguro se ejecuta localmente o en la nube? ‣ ¿Incluye la solución de espacio seguro tecnología líder de protección de endpoints para identificar amenazas como el ransomware en el entorno de espacio seguro? ‣ ¿Qué tecnología para endpoints se utiliza para asistir en el aislamiento en espacios seguros? ‣ ¿Qué tipo de generación de informes se proporciona de forma integrada (en lugar de un producto de generación de informes aparte)? ‣ ¿Qué tipo de visibilidad ofrece el panel de control?
Protección web y filtrado de URL Proporciona protección contra malware basado en la web, sitios web comprometidos y descargas web	‣ ¿Admite su firewall la aceleración de FastPath del tráfico de confianza y de flujos de elefante? ‣ ¿Se realiza por software o por hardware? ‣ ¿Cómo se identifican las aplicaciones para la aceleración de FastPath? ‣ ¿Qué herramientas de políticas se ofrecen a los administradores para controlar qué aplicaciones se descargan? ‣ ¿Se proporcionan firmas de manera predefinida para acelerar algunas aplicaciones y colocarlas en la ruta rápida FastPath? ‣ ¿Son sus procesadores de flujo de paquetes FastPath programables, actualizables y adaptables al futuro?
Control de aplicaciones Visibilidad y control del tráfico de aplicaciones para conformar o bloquear el tráfico no deseado y acelerar y priorizar el tráfico de aplicaciones esenciales	‣ ¿Qué fuentes de información se utilizan para identificar las aplicaciones? ‣ ¿Puede el motor de aplicaciones utilizar la información obtenida del endpoint para mejorar considerablemente la identificación de las aplicaciones, o se limita solo a lo que el firewall puede recopilar del paquete? ‣ ¿Se pueden asignar aplicaciones a FastPath y enrutarlas por enlaces WAN preferidos mediante reglas de políticas? ‣ ¿Dispone el sistema de un panel de control que ofrezca información sobre las aplicaciones en la nube y la TI en la sombra?

Productos de firewall complementarios

Los siguientes productos complementarios pueden ser importantes para ampliar la red y la protección donde se necesite. Asegúrese de que el proveedor de su elección ofrece estos productos adicionales y permite integrarlos fácilmente con su firewall, ya sea gestionados directamente desde él o a través de la misma consola de administración central que el firewall.

Productos complementarios	Preguntas para los proveedores
Dispositivos perimetrales SD-WAN para sucursales Dispositivos asequibles y fáciles de instalar para conectar pequeñas sucursales remotas	‣ ¿Ofrece un dispositivo para conectar emplazamientos remotos al firewall principal a través de una VPN dedicada? ‣ ¿Se puede desplegar sin necesidad de intervención? ‣ ¿Cuánto cuesta? ‣ ¿Admite tanto un túnel dedicado como uno dividido? ‣ ¿Qué opciones de conectividad modular admite, como Wi-Fi o LTE?
Puntos de acceso inalámbricos Amplíe la red para incluir conexiones inalámbricas	‣ ¿Incluye el firewall un controlador inalámbrico integrado? ‣ ¿Cuánto cuesta? ‣ ¿Sus puntos de acceso inalámbricos son Plug and Play? ‣ ¿Son compatibles con múltiples radios y SSID? ‣ ¿Admiten las redes en malla?
ZTNA Acceso a la red Zero Trust para conectar a los usuarios remotos a las aplicaciones y los datos de forma segura	‣ ¿Dispone de una solución ZTNA? ‣ ¿Se integra de alguna manera con su firewall o endpoints? ‣ ¿Se gestiona desde la misma consola de administración central que el firewall? ‣ ¿El agente ZTNA se despliega junto a su agente para endpoints? ‣ ¿Cómo se integra el estado de seguridad de los dispositivos en su solución ZTNA?
Protección del correo electrónico Protección del correo electrónico contra el spam, el phishing y el correo no deseado	‣ ¿Ofrece una solución integrada de protección del correo electrónico? ‣ ¿Ofrece protección del correo electrónico gestionada en la nube? ‣ ¿Incluye el aislamiento de archivos adjuntos sospechosos en espacios seguros? ‣ ¿Admite el cifrado del correo electrónico y la DLP? ‣ ¿Ofrece enrutamiento basado en dominios y un modo de MTA completo? ‣ ¿Ofrece un portal de usuarios para la administración de cuarentenas?
WAF Firewall de aplicaciones web para la protección del proxy inverso de los servidores locales expuestos a Internet	‣ ¿Ofrece funciones WAF integradas? ‣ ¿Facilita la configuración con plantillas predefinidas para aplicaciones comunes alojadas en servidores? ‣ ¿Ofrece endurecimiento, protección contra secuencias de comandos entre sitios y protección contra manipulaciones de cookies? ‣ ¿Proporciona descarga de autenticación de proxy inverso?

Funciones de gestión

Los productos de firewall suelen diferenciarse por su facilidad de gestión. Muchos firewalls que llevan décadas en el mercado se ven afectados por la incorporación de nuevas funciones al producto con el tiempo que utilizan diferentes conceptos de interfaz de usuario y que hacen que cada sección del producto parezca un producto completamente diferente. Las siguientes funciones pueden suponer una enorme diferencia en el despliegue y la gestión diaria.

Funciones de gestión	Preguntas para los proveedores
Administración centralizada Gestión de varios firewalls o productos de seguridad TI	‣ ¿Ofrece una solución de administración en la nube? ‣ ¿Cómo se gestionan varios firewalls a través de esta solución? ‣ ¿Qué otros productos se gestionan desde la misma consola en la nube? ‣ ¿La información sobre amenazas se comparte entre productos y es posible la búsqueda de amenazas entre productos?
Generación de informes Funciones de generación de informes que se ofrecen	‣ ¿El firewall incluye almacenamiento integrado para los datos de registro? ¿Cuánta capacidad? ‣ ¿Se incluye la generación de informes integrada? ¿Cuánto cuesta? ‣ ¿Admite la generación de informes en la nube? ¿Cuánto cuesta? ‣ ¿Se pueden crear, guardar, exportar y programar informes personalizados? ‣ ¿Se admite la exportación de datos de syslog? ‣ ¿Se admiten la generación de informes y la búsqueda de amenazas entre productos?
Experiencia de gestión En qué medida el firewall simplifica la gestión diaria y resalta lo que es importante	‣ ¿Ofrece su producto un panel de control detallado con opciones de análisis desglosados? ‣ ¿Las políticas para el control web, el control de aplicaciones, el IPS y el conformado de tráfico se encuentran todas en un solo lugar, o tengo que configurar estos componentes en diferentes áreas del producto? ‣ ¿Se ofrece una experiencia de usuario uniforme en las distintas partes del producto? ‣ ¿Existe una amplia ayuda contextual, documentación, vídeos y otros contenidos integrados para quien adquiera un firewall nuevo?
Portal para usuarios Portal de autoayuda para los usuarios	‣ ¿Ofrece su firewall un portal para usuarios que les permita descargar clientes o configuraciones de VPN y gestionar los correos electrónicos en cuarentena?

Opciones de despliegue

Otra consideración importante a la hora de elegir su próximo firewall es la facilidad con la que se integrará en su red, tanto en la actualidad como en el futuro. Lo conveniente es un firewall que se adapte a la red, no uno que exija que la red se adapte al firewall. Asegúrese de que su proveedor ofrece diversas opciones de despliegue, incluido el soporte de plataformas en la nube pública como AWS y Azure, así como las plataformas de virtualización más utilizadas, y opciones de dispositivos de hardware flexibles y modulares.

Opciones de despliegue	Preguntas para los proveedores
Dispositivos de hardware Asegúrese de que su próximo firewall esté lo más preparado posible para el futuro	‣ ¿Cuántos modelos de dispositivos ofrece que se adapten a mis necesidades? ‣ ¿Qué opciones de conectividad se incluyen? ‣ ¿Qué opciones de conectividad modular se incluyen? ‣ ¿Hay fuentes de alimentación redundantes? ‣ ¿Qué opciones de alta disponibilidad ofrece? ‣ ¿Las actualizaciones de firmware están incluidas en la licencia? ‣ ¿Cuál es la garantía del hardware?
En la nube, virtual y software Nube pública y soporte virtual para redes híbridas que pueden ser importantes en la actualidad o en el futuro	‣ ¿Su firewall está disponible en Marketplace para plataformas en la nube pública como AWS y Azure? ‣ ¿Admite todas las plataformas de virtualización habituales? ‣ ¿Su dispositivo está disponible como solución de software para ejecutarse en hardware X86?

Lista de comprobación de funciones del firewall

	Sophos	Meraki	Fortinet	PAN	SW	WG
Funciones básicas de firewall						
Simulador de pruebas de políticas web y reglas de firewall	✓		✓	✓		✓
Optimización de paquetes FastPath	✓		✓	✓		
Sistema de prevención de intrusiones	✓	✓	✓	✓	✓	✓
Control de aplicaciones	✓	Limitado	✓	✓	✓	✓
Motores AV duales	✓					✓
Visibilidad de aplicaciones en la nube de TI en la sombra	✓		✓	✓	✓	✓ - OEM
Bloqueo de aplicaciones no deseadas (PUA)	✓		✓	✓	✓	
Control y protección web	✓	✓	✓	✓	✓	✓
Monitorización e imposición de palabras clave web	✓		✓	✓	✓	✓
Motor DPI: ¿streaming, proxy o ambos?	✓	Flujo	✓	Flujo	Streaming	Proxy
Visibilidad del riesgo de usuarios y apps (cociente de amenazas por usuario)	✓		Limitado			
Protección contra amenazas avanzadas	✓	✓	✓	✓	✓	✓
Registros e informes históricos integrados	✓		Limitado	Limitado		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Protección de servidores y correo electrónico						
WAF completo integrado	✓		Adicional*			
Protección integrada del correo electrónico: antivirus, antispam, cifrado, DLP	✓					

	Sophos	Meraki	Fortinet	PAN	SW	WG
SD-WAN y VPN						
Acceso remoto por VPN completo, ilimitado y gratuito	✓	Adicional*	✓	Adicional*	Adicional*	Adicional*
VPN IPSEC y SSL de sitio a sitio	✓	✓	✓	✓	✓	✓
VPN de sitio a sitio con túnel SD-RED de capa 2	✓					
Orquestación de SD-WAN administrada en la nube	✓	✓	Adicional*		✓	
Administración de enlaces y enrutamiento de SD-WAN	✓	✓	✓	✓	✓	✓
Transiciones de conmutación por error de SD-WAN con cero impacto	✓		✓	✓		
Identificación y enrutamiento SD-WAN del tráfico de aplicaciones desconocidas o personalizadas	✓			✓		
Aceleración y descarga del tráfico VPN por hardware	✓		✓			
Dispositivos de túnel VPN asequibles y sin intervención	✓					

	Sophos	Meraki	Fortinet	PAN	SW	WG
Inspección TLS						
Inspección TLS 1.3	✓		✓	✓	✓	✓
Visibilidad de los problemas de tráfico cifrado en el panel de control	✓					
Creación de excepciones de TLS desde el panel de control	✓					

* Estas funciones están disponibles con un coste adicional.

	Sophos	Meraki	Fortinet	PAN	SW	WG
Protección contra amenazas de día cero						
Análisis de múltiples modelos de ML de archivos sospechosos	✓	✓	✓	✓	✓	
Aislamiento dinámico en espacios seguros de archivos sospechosos	✓	✓	✓	✓	✓	✓
Análisis de archivos en la nube	✓	✓	✓	✓	✓	✓
Generación de informes integrada de análisis de amenazas completos	✓	✓			✓	

	Sophos	Meraki	Fortinet	PAN	SW	WG
Optimización de paquetes FastPath						
Descarga de tráfico SaaS, en la nube y SD-WAN a FastPath	✓		✓	✓		
Herramientas de políticas y descarga automática a FastPath	✓		✓	✓		
Descarga y aceleración por hardware	✓		✓	✓		
Procesadores de flujo de paquetes programables	✓			✓		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Funciones de integración de protección para endpoints						
Identificar los hosts comprometidos	✓	✓	Adicional*	✓	✓	✓
Aislar automáticamente los hosts en el firewall de otras partes de la red	✓		Adicional*			✓
Aislar automáticamente los hosts a nivel del endpoint para evitar la propagación lateral	✓			Adicional*		✓
Identificar aplicaciones de red desconocidas (Control de aplicaciones sincronizado)	✓			✓		
Activar la búsqueda de amenazas entre productos (XDR)	✓			✓		
Habilitar un servicio de respuesta a amenazas totalmente gestionado	✓			✓		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Integración con la cartera de soluciones de acceso a la red						
Solución con controlador inalámbrico integrado y puntos de acceso	✓	✓	✓		✓	✓
Se integra con una solución ZTNA	✓	✓	✓	✓	✓	
Se integra con switches de red	✓	✓	✓		✓	
Se integra con dispositivos perimetrales (SD-RED) de acceso a servicios remotos	✓					

* Estas funciones están disponibles con un coste adicional.

	Sophos	Meraki	Fortinet	PAN	SW	WG
Administración en la nube						
Gestión completa del firewall desde la nube, sin costes adicionales	✔	✔	Adicional*		Adicional*	✔
Una única consola en la nube para endpoints, servidores, dispositivos móviles, firewalls, correo electrónico y cifrado	✔					✔
Gestión de grupos de firewalls desde la nube	✔	✔	Adicional*		✔	
Programar actualizaciones del firmware desde la nube	✔	✔	✔		✔	✔
Desplegar nuevos firewalls desde la nube (sin intervención)	✔	✔	Adicional*		✔	✔
Generación de informes de firewall en la nube	✔	✔	✔		✔	✔
Búsqueda de amenazas entre productos (XDR) gestionada en la nube	Adicional*			Adicional*		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Opciones de despliegue virtual y en la nube						
AWS	✔	✔	✔	✔	✔	✔
Azure	✔	✔	✔	✔	✔	✔
Google	Futuro	✔	✔	✔		
Nutanix	✔		✔	✔	✔	
FWaaS	Futuro		✔	✔		
Plataformas de virtualización	✔	✔	✔	✔	✔	✔
Dispositivo de software (x86)	✔					

* Estas funciones están disponibles con un coste adicional.

Sophos Firewall

Si quiere conocer las funciones y características de Sophos Firewall, no se pierda estos recursos:

- Informe de la solución de Sophos Firewall
- Lista de funciones de Sophos Firewall
- Folleto de Sophos Firewall

Pruébelo gratis hoy mismo

Pruebe Sophos Firewall online gratis
es.sophos.com/demo

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

22-03-31 ES (PC)