LOS RIESGOS OCULTOS DE LOS FIREWALLS MODERNOS

Descubra cómo puede evitar que su firewall sufra un ataque

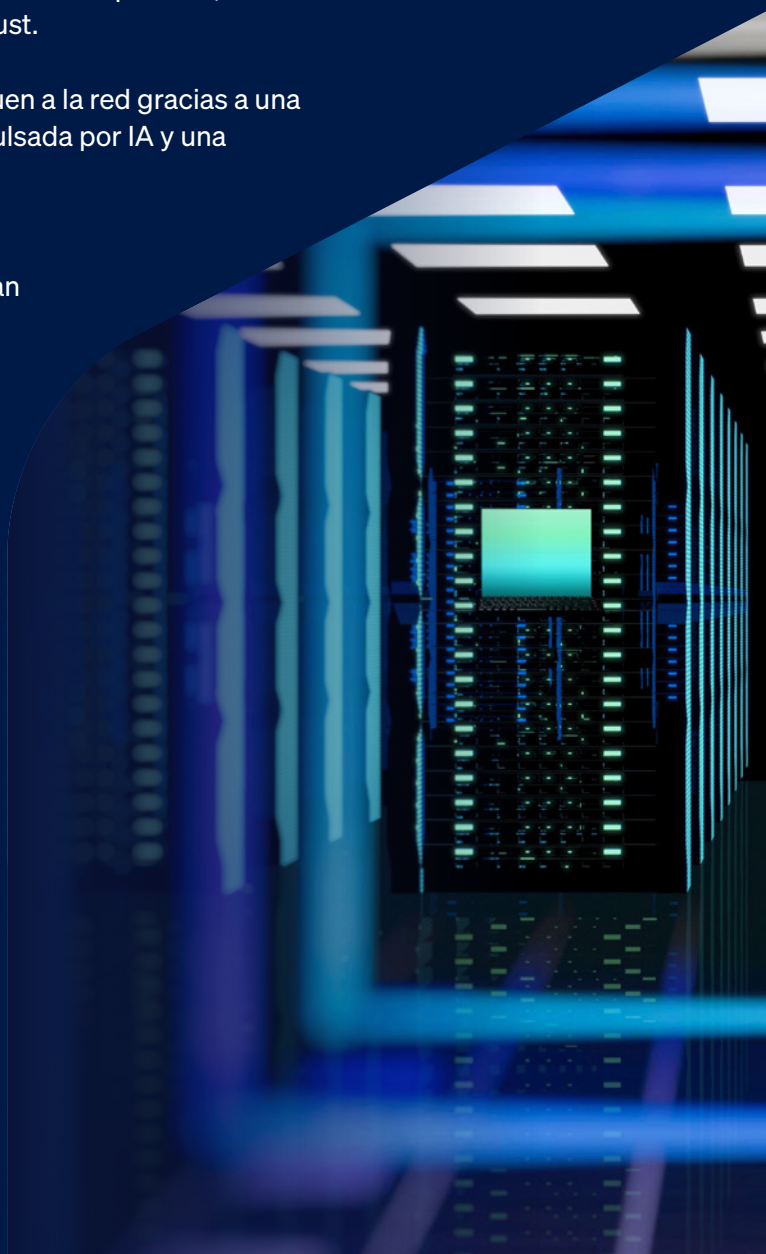
Resumen ejecutivo

Los firewalls de red se enfrentan a un nivel sin precedentes de ataques dirigidos. Casi a diario aparecen titulares relacionados con un nuevo ataque que explota una vulnerabilidad de firewall, lo que pone de manifiesto una realidad preocupante: los firewalls (precisamente los sistemas diseñados para proteger las redes) suponen un riesgo significativo y se han convertido en blancos prioritarios para adversarios sofisticados[1]. Estos ataques no solo aprovechan las vulnerabilidades del propio software del firewall, sino también las deficiencias fundamentales en la forma en que las organizaciones abordan la seguridad de la red.

En este monográfico se presenta un modelo integral de tres pilares para la seguridad de redes moderna, diseñado para combatir las amenazas en todas sus fases: antes, durante y después de su despliegue:

- **Endurecimiento:** reduzca de forma proactiva su superficie de ataque mediante los principios de Secure by Design, la aplicación automatizada de parches, la auditoría de configuraciones y los controles de acceso Zero Trust.
- **Protección:** bloquee las amenazas antes de que lleguen a la red gracias a una inspección avanzada, la detección de amenazas impulsada por IA y una seguridad de alto rendimiento sin concesiones.
- **Detección y respuesta:** identifique y contenga automáticamente a los adversarios activos que operan en la red antes de que logren completar un ataque.

La mayoría de las soluciones de seguridad de red se centran principalmente en la protección, con lo que la infraestructura de red queda expuesta y es incapaz de identificar y responder ante un ataque activo. En este documento ofrecemos a los profesionales de la seguridad de red y a los equipos de TI unas pautas prácticas para implementar estos tres pilares de manera eficaz.



El panorama actual de amenazas

Los firewalls, bajo el punto de mira

Los firewalls de red se sitúan a caballo entre las redes internas de confianza y el mundo exterior hostil. Esta posición privilegiada los convierte en blancos de gran valor. La prensa se ha hecho eco de una sucesión constante de ataques contra los principales proveedores de firewalls: algunos explotan vulnerabilidades ya conocidas que siguen sin parchear en entornos de producción, mientras que otros se centran en configuraciones predeterminadas deficientes o en fallos de diseño que crean puntos débiles explotables[2].

>2000

vulnerabilidades de día cero fueron descubiertas por Mythos en tan solo siete semanas

La IA de vanguardia ha añadido más leña al fuego en lo que respecta a los ciberataques impulsados por la IA agente. En tan solo unas semanas, el modelo Claude Mythos de Anthropic detectó más de 2000 nuevas vulnerabilidades de día cero, lo que augura un cambio radical tanto para los adversarios como para los responsables de la seguridad.

Si bien los titulares sobre las últimas novedades en IA se centran en la capacidad de esta para detectar vulnerabilidades a gran escala, lo más relevante es cómo la IA reduce el tiempo de respuesta, acortando así el intervalo entre la exposición de una vulnerabilidad y el impacto en una empresa. Esto permite a los ciberdelincuentes actuar con mayor rapidez, a mayor escala y con menos obstáculos que antes.

Las consecuencias van mucho más allá de las organizaciones individuales. Cuando los atacantes logran burlar un firewall, no solo obtienen acceso directo a la red, sino que también pueden hacerse con credenciales y acceder a los proveedores y clientes de la organización, lo que les permite, en la práctica, hacerse con el control absoluto de la empresa.

Los tres pilares de la seguridad de red

Una seguridad de red eficaz requiere un enfoque integral que aborde las amenazas a lo largo de todo su ciclo de vida: antes, durante y después del despliegue. Esto da lugar a tres pilares de defensa distintos, pero interconectados:

ENDURECIMIENTO

REDUZCA EL ÁREA DE LA SUPERFICIE DE ATAQUE

Diseñe, desarrolle y mantenga soluciones para minimizar los riesgos, reducir la exposición y reforzar la infraestructura frente a los ataques

PROTECCIÓN

BLOQUEE LOS ATAQUES ANTES DE QUE LLEGUEN A LA RED

Despliegue la mejor protección posible para identificar y evitar que los atacantes y los exploits accedan a la red

DETECCIÓN Y RESPUESTA

DETENGA EN SECO LOS ATAQUES ACTIVOS

Utilice la detección y la respuesta para identificar y aislar automáticamente a un adversario activo

La laguna crítica

La mayoría de los firewalls de red se centran casi exclusivamente en la protección en tiempo real, como el filtrado del tráfico, la prevención de amenazas y los sistemas de prevención de intrusiones. Si bien estas capacidades son esenciales, centrarse únicamente en la inspección del tráfico en tiempo real deja a las organizaciones en una situación de vulnerabilidad.

Los titulares diarios ponen de manifiesto que la mayoría de los firewalls y equipos de TI no logran reforzar eficazmente su entorno, es decir, reducir la superficie de ataque. Los firewalls siguen siendo vulnerables, la saturación por la gestión de parches es generalizada, los productos al fin de vida útil siguen ocupando una posición privilegiada y las VPN de acceso remoto siguen predominando a pesar de sus deficiencias de seguridad. Mientras tanto, en la mayoría de los despliegues de firewalls suelen faltar por completo las funcionalidades de detección y respuesta necesarias para impedir los ataques activos antes de que puedan tener repercusiones.

Para corregir este desequilibrio es necesario prestar especial atención a los pilares que se han descuidado, en particular al refuerzo de la seguridad, que constituye la base de una postura de seguridad resiliente.

Endurecimiento de la infraestructura de red: reducción del riesgo

El endurecimiento consiste en reducir de forma proactiva la superficie de ataque, eliminando las vulnerabilidades antes de que los atacantes puedan descubrirlas y explotarlas.

Estrategias fundamentales de endurecimiento

1. **Minimice la exposición:** revise periódicamente las infraestructuras y los sistemas expuestos a Internet y, a su vez, reduzca el número de posibles puntos de entrada.

2. **Asegúrese de que los sistemas sean «Secure by Design»:** seleccione productos diseñados pensando en la seguridad como principio fundamental.

3. **Audite la configuración y mantenga el software y el firmware actualizados:** mantenga la higiene de seguridad mediante una supervisión continua.

4. **Elimine la identidad vulnerada como vector de ataque:** restrinja el acceso y la autenticación. Implemente la autenticación multifactor (MFA) de forma generalizada y pase de la VPN al Zero Trust Network Access (ZTNA).

Minimice la exposición

Revise periódicamente su infraestructura de red y evalúe en qué fase del ciclo de vida se encuentra cada componente. Si alguna pieza se acerca al fin de vida útil, planifique su sustitución de forma proactiva. El coste de renovar tecnologías obsoletas es mucho menor que el impacto potencial de un ataque de ransomware que explote sistemas que ya no reciben soporte técnico.

Esta es también una oportunidad para simplificar y consolidar su infraestructura de red. Si utiliza dispositivos independientes para firewall, VPN, ZTNA, SD-WAN, DNS y filtrado web, considere la posibilidad de reunir todas estas funciones en una única plataforma. Reducir el número de dispositivos y soluciones en su entorno puede disminuir la complejidad, mejorar la eficiencia y reforzar la resiliencia general.

Mantener su infraestructura actualizada es igualmente importante. Las actualizaciones de firmware y software suelen incluir parches de seguridad críticos para vulnerabilidades que los atacantes podrían explotar. Aunque aplicarlas puede llevar tiempo, el impacto es mucho menor que el de tener que hacer frente a las consecuencias de un ataque de ransomware.

Asegúrese de que los sistemas sean «Secure by Design»

las empresas necesitan productos seguros en la misma medida en que necesitan productos de seguridad.

El sector de la ciberseguridad debe aceptar una verdad fundamental: las empresas necesitan productos seguros en la misma medida en que necesitan productos de seguridad. Cuando los adversarios atacan las herramientas creadas para defender a las organizaciones, estas necesitan productos de seguridad que sean, a su vez, seguros. Las organizaciones deben valorar a los proveedores que demuestren un compromiso sincero con la seguridad y la transparencia, lo que incluye la comunicación clara y oportuna de cualquier incumplimiento: el enfoque adecuado, aunque resulte incómodo.

Entre los principios fundamentales de «Secure by Design» se incluyen:

- La MFA se integra en todos los sistemas de forma predeterminada.
- Se eliminan las contraseñas y credenciales predeterminadas.
- Se implementan parches de seguridad automatizados que minimizan las interrupciones.
- Se aplican procesos de notificación de vulnerabilidades rápidos y transparentes.
- Se realizan auditorías de seguridad y pruebas de penetración periódicas.
- Se incorporan prácticas de ciclo de vida de desarrollo seguro en la ingeniería de productos.

Audite la configuración y mantenga los sistemas actualizados

Los firewalls de red son complejos, lo que los hace propensos a errores de configuración y ajustes poco seguros que pueden crear vulnerabilidades involuntarias para los atacantes. El reto consiste en saber qué está mal configurado y dónde se encuentran esas vulnerabilidades. A veces el problema es evidente, pero lo más habitual es que las lagunas permanezcan ocultas hasta que alguien las aprovecha. La mayoría de los firewalls no ofrecen ningún tipo de información sobre los ajustes de configuración que suponen un riesgo. Elija uno que sí lo haga.

La saturación por la gestión de parches es una realidad, pero no tiene por qué serlo. Los procesos tradicionales de aplicación de parches suponen una carga operativa considerable. Las vulnerabilidades de seguridad pueden detectarse en cualquier momento y ahora, gracias a la IA, a un ritmo alarmante. La frecuencia de las actualizaciones necesarias puede desbordar a los equipos administrativos. La mayoría de los firewalls prometen «actualizaciones automáticas», pero, por lo general, aún requieren que los administradores programen tiempos de inactividad, apliquen el firmware y reinicien los dispositivos.

Las organizaciones deberían plantearse una pregunta sencilla: ¿por qué las actualizaciones de seguridad no pueden ser completamente automáticas? La respuesta es que la mayoría de los proveedores no han diseñado su software para admitir actualizaciones de seguridad automáticas en tiempo real. No obstante, los enfoques arquitectónicos modernos pueden permitir el uso de funciones de actualización automática que:

- Apliquen los parches de seguridad automáticamente, sin la intervención del administrador.
- No requieran tiempo de inactividad del sistema ni reinicios.
- Cubran los periodos entre las principales versiones de firmware.

- Reduzcan el periodo de vulnerabilidad de meses a horas o días.

Los errores de configuración constituyen otro punto de entrada habitual para los atacantes. Los conjuntos de reglas de firewall complejos, los cambios en las políticas mal documentados y las desviaciones en la configuración a lo largo del tiempo pueden dejar abiertos, sin quererlo, puntos de acceso que deberían estar protegidos.

El reto radica en la identificación: ¿cómo pueden saber los administradores qué elementos están mal configurados? Los firewalls tradicionales no ofrecen visibilidad sobre la seguridad de la configuración. Los enfoques modernos incluyen funciones de comprobación automática del estado de seguridad que:

- Auditan continuamente la configuración del firewall en función de las prácticas recomendadas establecidas y los parámetros de referencia del CIS.
- Ofrecen visibilidad de las comprobaciones superadas y fallidas en el panel de control.
- Asignan niveles de gravedad a cada elemento evaluado.
- Permiten profundizar en los datos para ajustar rápidamente la configuración o documentar excepciones intencionadas.

Estas capacidades ofrecen una visibilidad de la que carecen los firewalls tradicionales, lo que garantiza que la postura de seguridad se mantenga óptima aun cuando las configuraciones evolucionen con el tiempo.

67 %

de los incidentes investigados por Sophos en 2025 comenzaron con una identidad vulnerada

Elimine la suplantación de identidad como vector de ataque

El 67 % de los incidentes investigados por Sophos en 2025 se originaron a raíz del robo de credenciales[3], con lo que erradicar los ataques relacionados con la identidad se ha convertido en una prioridad fundamental para el refuerzo de la seguridad. Esto exige adoptar los principios del modelo Zero Trust: no confiar en nada y verificarlo todo.

Las organizaciones que aún dependen de las VPN de acceso remoto deben dar prioridad absoluta a la migración a otras soluciones. ZTNA ofrece una alternativa moderna a las VPN que se ajusta a los principios de Zero Trust. En lugar de conceder un acceso general a la red, ZTNA proporciona un acceso granular a determinadas aplicaciones y recursos. Si un dispositivo se ve comprometido, ZTNA puede limitar o bloquear automáticamente el acceso hasta que se realice la remediación.

Aunque un atacante consiga vulnerar un dispositivo conectado a través de ZTNA, solo obtendrá acceso a las apps específicas a las que ese usuario está autorizado a acceder, y no a toda la red. El perímetro de seguridad se desplaza hasta donde realmente se necesita: en torno a las apps y los datos críticos.

ZTNA ofrece seis ventajas clave con respecto a las VPN:

1. **Autenticación multifactor (MFA) obligatoria:** se exige la MFA para todos los accesos sin excepción, lo que elimina las credenciales vulneradas y los ataques por fuerza bruta como vectores de ataque viables.

2. **El estado de seguridad del dispositivo forma parte de la política de acceso:** el cumplimiento normativo y el estado de seguridad del dispositivo se evalúan continuamente como parte de las decisiones de acceso.

3. **Funciona en cualquier lugar:** ZTNA funciona con la misma eficacia tanto si los usuarios se encuentran en la red corporativa como si trabajan de forma remota, lo que proporciona una seguridad uniforme independientemente de la ubicación.

4. **Conectividad transparente:** las implementaciones modernas de ZTNA proporcionan conexiones transparentes y fiables sin los problemas de conexión que suelen afectar a las VPN.

5. **Mayor visibilidad:** las organizaciones obtienen una visión clara de los recursos a los que acceden los usuarios, lo que mejora la planificación de la capacidad y la gestión de licencias.

6. **Administración más sencilla:** añadir y eliminar usuarios, desplegar nuevas apps y gestionar las políticas de acceso resulta más sencillo con ZTNA que con una VPN tradicional.

Las estrategias de endurecimiento deben incluir la eliminación de las VPN de acceso remoto y el despliegue de una arquitectura Zero Trust con aplicación universal de la autenticación multifactor (MFA).

Protección: bloqueo de amenazas en la puerta de enlace

Despliegue una protección integral para identificar y bloquear las amenazas antes de que lleguen a la red. Esto incluye inspección TLS avanzada, detección de amenazas de día cero basada en IA y análisis inteligente del tráfico que mantiene un alto rendimiento sin comprometer la seguridad.

Requisitos actuales en materia de protección

- **Inspección TLS 1.3 de alto rendimiento:** actualmente, la mayor parte del tráfico web está cifrado, y los atacantes ocultan cada vez más el malware y el tráfico de comando y control dentro de canales cifrados. Los firewalls deben descifrar e inspeccionar el tráfico TLS de forma inteligente, aplicando reglas basadas en políticas que equilibren los requisitos de seguridad con las consideraciones de privacidad y el impacto en el rendimiento.

- **Aceleración por hardware:** las operaciones criptográficas y la inspección del tráfico requieren un gran esfuerzo computacional. Las arquitecturas modernas de firewall deben descargar las apps de confianza y las operaciones criptográficas a vías de aceleración por hardware, con el fin de liberar recursos para la inspección en profundidad del tráfico que no es de confianza.

- **Protección contra amenazas de día cero con IA:** la detección basada en firmas sigue siendo útil, pero resulta insuficiente frente a las nuevas amenazas. El análisis de archivos estáticos basado en IA, combinado con los espacios seguros dinámicos en tiempo de ejecución, permite identificar y bloquear las amenazas de día cero antes de que lleguen a la red —amenazas que los sistemas tradicionales basados en firmas pasarían por alto por completo.

Las capacidades de protección Y el rendimiento deben mejorar con el tiempo, en lugar de disminuir. Los firewalls basados en arquitecturas programables pueden beneficiarse de mejoras tanto en la protección como en el rendimiento mediante actualizaciones de software, lo que prolonga el ciclo de vida útil de las inversiones en hardware. A diferencia de los firewalls tradicionales, que se vuelven más lentos a medida que se añaden nuevas funciones de seguridad, las arquitecturas modernas mantienen o mejoran el rendimiento gracias a una optimización continua.

Detección y respuesta: detener los ataques activos

Cuando los adversarios logran penetrar las defensas, estas detectan rápidamente su presencia y contienen automáticamente la amenaza. La detección y respuesta de red (NDR), combinada con la coordinación entre productos, permite identificar y aislar los sistemas afectados antes de que los atacantes alcancen sus objetivos.

Detección y respuesta de red (NDR)

La detección y respuesta de red utiliza la IA y el análisis de comportamientos para identificar a los adversarios activos que ya se encuentran en la red. A diferencia de las defensas perimetrales, que analizan el tráfico entrante, NDR examina los patrones de tráfico de la red interna en busca de indicadores de peligro:

- Movimiento lateral inusual entre sistemas.
- Comunicaciones de comando y control con hosts externos sospechosos.
- Patrones anómalos de acceso a los datos.
- Intentos de aumento de privilegios.
- Actividades de reconocimiento que analizan los recursos internos.

Tradicionalmente, NDR ha sido una funcionalidad de nivel empresarial que requería productos independientes y una inversión considerable. Ahora, las organizaciones con visión de futuro integran las capacidades de NDR directamente en las plataformas de firewall, lo que hace que esta funcionalidad fundamental sea accesible para las empresas del mercado medio.

Respuesta automatizada

La detección sin respuesta se limita a informar a los administradores de que se han visto comprometidos, a menudo cuando ya es demasiado tarde para evitar daños. Las funciones de respuesta automatizada permiten una contención inmediata.

Cuando se detecta una amenaza en cualquier punto de la infraestructura de seguridad (ya sea mediante el firewall, la protección para endpoints, la seguridad del correo electrónico o un analista de MDR), se necesita una solución de seguridad que coordine una respuesta automatizada en todos los productos de seguridad integrados. Esto puede impedir que un dispositivo vulnerado se comunique con otros sistemas, bloquear su acceso a aplicaciones y datos, y evitar que se mueva lateralmente.

Esta respuesta automatizada resulta especialmente valiosa fuera del horario laboral, momento en el que se concentran el 88 % de los ataques de ransomware[4]. Pensemos en el «escenario del viernes por la noche»: un hacker compromete un dispositivo a última hora del día, cuando el personal de seguridad no está disponible. Sin una respuesta automatizada, el atacante dispone de todo el fin de semana para moverse lateralmente, aumentar sus privilegios y desplegar el ransomware. La organización se percata de la filtración el lunes por la mañana, cuando empiezan a aparecer los archivos cifrados y las demandas de rescate.

Gracias a una respuesta automatizada entre productos, la intrusión inicial desencadena un aislamiento inmediato. El atacante queda atrapado en un segmento en cuarentena, sin poder avanzar ni moverse. El lunes por la mañana, los equipos de seguridad se encuentran con una alerta activa sobre una amenaza contenida, en lugar de un incidente de ransomware a gran escala.

88 %

Porcentaje de ataques de ransomware que se despliegan fuera del horario laboral

Sophos Firewall: una solución integral

Si bien el marco de tres pilares descrito representa las prácticas recomendadas en materia de seguridad, para implementarlo de manera eficaz es necesario elegir una infraestructura que admita los tres pilares.

Sophos Firewall destaca como una de las pocas soluciones que ha invertido de manera significativa en las tres áreas, lo que le permite ofrecer numerosas funciones que los usuarios no encontrarán en ningún otro lugar.

Supervisión de la integridad del sistema

Los equipos de seguridad de Sophos supervisan continuamente todos los sistemas de despliegue en busca de indicios de ataques, lo que permite acelerar la respuesta y la remediación.

Comprobación continua del estado de seguridad

Identifica configuraciones de alto riesgo comparándolas con las prácticas recomendadas y ofrece recomendaciones priorizadas para una mitigación más rápida.

Correcciones automáticas y actualizaciones seguras

Los parches de seguridad se pueden enviar a Sophos Firewall de forma inalámbrica y aplicarse automáticamente sin interrumpir el servicio.

Todas las actualizaciones de firmware están cifradas y firmadas de forma segura para garantizar su integridad y autenticidad.

Endurecimiento de sistemas

Despliegue seguro listo para usar

MFA y puerta de enlace ZTNA integradas

Servicios y portales reforzados y en contenedores

Kernel y plano de control endurecidos para eliminar categorías enteras de vulnerabilidades

Administración remota segura

El acceso cifrado a la gestión a través de Sophos Central elimina la exposición innecesaria del firewall.

Para garantizar la máxima protección, todas las copias de seguridad se almacenan de forma segura y se someten a un doble cifrado en Sophos Central.

Secure by Design

Sophos Firewall responde al pilar del endurecimiento mediante un enfoque integral Secure by Design que elimina la carga que suele conllevar el mantenimiento de una infraestructura segura.

Funcionalidad de actualizaciones automáticas: acabe con la saturación por la gestión de parches

La exclusiva función de actualizaciones automáticas de Sophos Firewall transforma radicalmente el periodo de exposición a las vulnerabilidades:

- Los parches de seguridad se envían de forma inalámbrica y automática tan pronto como Sophos los desarrolla y valida.
- Los parches se aplican sin que tenga que intervenir el administrador.
- No suponen interrupciones ni es necesario reiniciar.
- Las actualizaciones automáticas cubren los periodos entre las principales versiones de firmware, garantizando una protección continua.

Esta ventaja arquitectónica reduce el periodo de vulnerabilidad de meses a horas o días. Cuando Sophos detecta y corrige una vulnerabilidad, todos los clientes de Sophos Firewall reciben protección de forma inmediata, sin necesidad de esperar a que los administradores encuentren un hueco en sus agendas o planifiquen tareas de mantenimiento.

No existe ningún otro principal proveedor de firewalls que ofrezca una automatización verdadera y permita aplicar parches de seguridad sin tiempo de inactividad. Esta funcionalidad por sí sola supone una mejora transformadora en el pilar del endurecimiento.

Comprobación del estado de seguridad: auditoría continua de la configuración

La función «Comprobación del estado de seguridad» de Sophos Firewall ofrece una visibilidad de la configuración sin precedentes:

- Audita continuamente decenas de parámetros de configuración del firewall comparándolos con los estándares del CIS y las prácticas recomendadas del sector.
- Muestra las comprobaciones superadas y fallidas directamente en el panel del centro de control.
- Asigna niveles de gravedad a cada elemento evaluado (crítico, alto, medio, bajo).
- Permite profundizar en los datos para ajustar rápidamente la configuración o documentar excepciones intencionadas.
- Se actualiza automáticamente a medida que evolucionan las prácticas recomendadas.

Esta supervisión proactiva de la configuración garantiza que la postura de seguridad se mantenga óptima aunque las configuraciones cambien con el tiempo. Los administradores reciben alertas inmediatas sobre ajustes potencialmente peligrosos antes de que los atacantes puedan descubrirlos y explotarlos.

Supervisión remota de la integridad

Sophos destaca por supervisar toda nuestra base de dispositivos Sophos Firewall instalados. Gracias a un sensor Linux integrado de Sophos Extended Detection and Response (XDR), podemos supervisar la integridad del sistema, entre otras cosas:

- Cambios de configuración no autorizados.
- Exportaciones de reglas.
- Manipulación de archivos.
- Intentos de ejecución de programas maliciosos.

Este sensor integrado permite a los equipos de seguridad de Sophos supervisar de forma proactiva toda la base de clientes en busca de indicios de ataques, lo que supone una capa de seguridad adicional que ningún otro proveedor de firewall ofrece en la actualidad. Cuando se detectan amenazas, Sophos puede responder de inmediato para ayudar a los clientes a remediarlas, al tiempo que distribuye parches automáticos para proteger al resto de clientes.

Autenticación multifactor y ZTNA integradas

Sophos Firewall integra la autenticación multifactor (MFA) en todos los puntos de acceso administrativos e incluye una puerta de enlace ZTNA integrada, lo que agiliza la adopción y el despliegue de ZTNA, así como la migración desde VPN de acceso remoto vulnerables.

Protección y rendimiento potentes

Aunque muchos proveedores cuentan con potentes funciones de protección, Sophos Firewall ofrece una protección diferente, garantizando una seguridad integral sin sacrificar el rendimiento, algo que a menudo obliga a las organizaciones a desactivar importantes funciones de seguridad.

Arquitectura Xstream FastPath

La arquitectura Xstream programable de Sophos Firewall gestiona el tráfico de forma inteligente para ofrecer la máxima seguridad y el máximo rendimiento**.** Este enfoque garantiza que la activación de funciones de seguridad completas (como la inspección TLS, los espacios seguros y el sistema de prevención de intrusiones) no repercuta negativamente en el rendimiento. Sophos Firewall también integra protección contra amenazas de día cero basada en IA para identificar las amenazas más recientes.

Mejoras continuas en el rendimiento y la protección

A diferencia de los firewalls tradicionales, que se ralentizan a medida que se añaden nuevas funciones de seguridad, la arquitectura programable de Sophos Firewall permite mejorar la protección **y** el rendimiento mediante actualizaciones de software. Los clientes se benefician de mejoras continuas en sus inversiones en hardware sin necesidad de actualizar los equipos: una protección y un rendimiento que mejoran con el tiempo en lugar de disminuir.

Detección y respuesta inigualables

La mayoría de los firewalls de red prácticamente no ofrecen funciones de detección y respuesta de red. Una vez que un atacante logra traspasar las defensas perimetrales, los firewalls tradicionales carecen de mecanismos para identificar la intrusión o responder a ella. Esto supone una brecha crítica que expone a las organizaciones a los ataques más sofisticados.

Sophos Firewall es único en ofrecer funcionalidades de detección y respuesta automatizadas.

Detección y respuesta de red (NDR) integrada

Tradicionalmente, la detección y respuesta de red ha sido una función exclusiva de las grandes empresas que requería productos independientes y una inversión considerable. Sophos Firewall incluye NDR como función estándar dentro de la suscripción de protección convencional:

esto permite a organizaciones de todos los tamaños disponer de una detección de amenazas de nivel empresarial, lo que garantiza que los adversarios que logran penetrar las defensas perimetrales puedan ser identificados antes de que alcancen sus objetivos.

Seguridad Sincronizada: respuesta automatizada entre productos

La detección sin respuesta se limita a informar a los administradores de que se han visto comprometidos, a menudo cuando ya es demasiado tarde para evitar daños. La Seguridad Sincronizada de Sophos Firewall ofrece una respuesta automatizada y coordinada en toda la infraestructura de seguridad.

Cuando un producto de Sophos detecta una amenaza (ya sea el firewall, la protección para endpoints, la seguridad del correo electrónico, Workspace Protection o un analista de MDR), la Seguridad Sincronizada automáticamente:

- Aísla el dispositivo afectado para impedir que se comunique con otros sistemas.
- Bloquea el acceso a las aplicaciones y los datos.
- Impide el movimiento lateral por la red.
- Contiene la amenaza hasta que los equipos de seguridad puedan investigarla y remediarla.

El «escenario del viernes por la noche» ilustra el valor crítico de la respuesta automatizada:

Sin respuesta automática: un hacker compromete un dispositivo a última hora del día, cuando el personal de seguridad no está disponible. El atacante dispone de todo el fin de semana para moverse lateralmente, aumentar sus privilegios y desplegar el ransomware. La organización se percata de la filtración el lunes por la mañana, cuando empiezan a aparecer los archivos cifrados y las demandas de rescate.

Con la Seguridad Sincronizada: la intrusión inicial desencadena un aislamiento automatizado inmediato. El atacante queda atrapado en un segmento en cuarentena, sin poder avanzar. El lunes por la mañana, los equipos de seguridad se encuentran con una alerta activa sobre una amenaza contenida, en lugar de un incidente de ransomware a gran escala.

Esta funcionalidad de respuesta automatizada resulta especialmente valiosa para las organizaciones que no cuentan con una cobertura de operaciones de seguridad 24/7, precisamente aquellas empresas del mercado medio que los proveedores tradicionales de NDR llevan años ignorando.

Conclusión

¿Mi firewall reduce el riesgo o lo aumenta?

Los firewalls de red se enfrentan a una presión de ataques sin precedentes. Los titulares que sacan a la luz vulnerabilidades en muchos de los principales proveedores revelan una verdad incómoda: los sistemas diseñados para proteger las redes se han convertido en blancos prioritarios para los adversarios sofisticados.

El marco de tres pilares presentado en este monográfico (endurecimiento, protección, y detección y respuesta) ofrece un enfoque integral de la seguridad de red que aborda las amenazas antes, durante y después de que se produzcan. Por desgracia, la mayoría de los proveedores de firewalls se centran casi exclusivamente en el pilar de la protección, lo que deja importantes lagunas en las capacidades de endurecimiento y de detección y respuesta.

Para implementar este marco de forma eficaz, es necesario seleccionar una infraestructura que invierta por igual en los tres pilares. Las organizaciones deben valorar a los proveedores de firewalls basándose en los siguientes aspectos:

- **El compromiso con el enfoque Secure by Design**, con pruebas de su implementación, no solo promesas.
- **Capacidades de aplicación automática de parches** que eliminen el tiempo de inactividad y la carga que supone la gestión de parches.
- **Auditorías de configuraciones** que ofrezcan visibilidad sobre la postura de seguridad.
- **Capacidades Zero Trust integradas**, como MFA y ZTNA.
- **Detección y respuesta de red** para identificar amenazas activas.as activas.
- **Funciones de respuesta automatizada** que contengan las amenazas sin intervención humana.

El coste de sustituir una infraestructura obsoleta o inadecuada es considerablemente menor que el de recuperarse de un ataque de ransomware que explota vulnerabilidades conocidas. Es el momento de actuar, antes de que su organización acabe siendo noticia.

La seguridad es una responsabilidad compartida. Los proveedores deben fabricar productos seguros. Las organizaciones deben desplegarlos correctamente, mantenerlos de forma rigurosa y retirarlos cuando alcancen el fin de vida útil. El cumplimiento de sus responsabilidades por ambas partes crea un ecosistema mucho más seguro.

La pregunta clave que debe hacerse es: **¿mi firewall reduce el riesgo o lo aumenta?**

La respuesta depende de si su infraestructura aborda los tres pilares de la seguridad de red moderna, o si deja lagunas críticas que los atacantes no dudarán en aprovechar.

1, 2, 3 ,4 Informe de Sophos sobre adversarios activos 2026.

SOPHOS

Para obtener más información sobre Sophos Firewall, visite **es.sophos.com/firewall**.

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

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