SOPHOS
Cybersecurity delivered.

Sophos Firewall

Informe de solución

Contenido

Sophos Firewall

Sophos Firewall ha sido diseñado desde cero para abordar los principales problemas actuales con los firewalls, al tiempo que proporciona una verdadera plataforma next-gen para afrontar el panorama de amenazas en constante evolución y la Internet cifrada moderna. Sophos Firewall le permite adoptar un nuevo enfoque a la forma en que identifica riesgos ocultos, se protege frente a amenazas y responde a incidentes, a la vez que ofrece un rendimiento óptimo. Nuestra arquitectura de Xstream para Sophos Firewall constituye una arquitectura de procesamiento de paquetes que ofrece unos niveles extraordinarios de visibilidad, protección y rendimiento.

Sophos Firewall proporciona una visibilidad inigualable de los usuarios de riesgo, las aplicaciones no deseadas, las cargas sospechosas y las amenazas persistentes. Se integra perfectamente en un completo paquete de tecnologías de protección que resulta fácil de configurar y mantener. A diferencia de los firewalls antiguos, Sophos Firewall se comunica con otros sistemas de seguridad de la red para convertirse en su punto de imposición de confianza para contener amenazas y evitar que el malware se propague o filtre datos fuera de la red, automáticamente y en tiempo real.

Sophos Firewall cuenta con cuatro ventajas clave con respecto a otros firewalls de red:

1. **Expone los riesgos ocultos**: Sophos Firewall hace un trabajo mucho mejor que otras soluciones a la hora de exponer los riesgos ocultos a través de un panel de control visual, la generación integrada y en la nube de informes detallados y datos de riesgos únicos.
2. **Bloquea amenazas desconocidas**: Sophos Firewall hace que el bloqueo de las amenazas desconocidas sea más fácil, rápido y efectivo que con otros firewalls, gracias a un completo paquete de funciones de protección avanzada que es muy fácil de configurar y gestionar.
3. **Responde automáticamente a incidentes**: Sophos Firewall con Seguridad Sincronizada responde automáticamente a los incidentes de la red gracias a Sophos Security Heartbeat™, que comparte información en tiempo real entre los endpoints y el firewall.
4. **Optimiza su red SD-WAN**: las capacidades SD-WAN de Xstream en Sophos Firewall permiten configurar redes de superposición SD-WAN complejas con solo apuntar y hacer clic. También puede aprovechar la selección automática de enlaces WAN basada en el rendimiento con transiciones instantáneas de cero impacto entre enlaces para optimizar el rendimiento de las aplicaciones, la resiliencia de la red y la continuidad de la actividad, al tiempo que se reducen los costes de conectividad.

Exponer riesgos ocultos

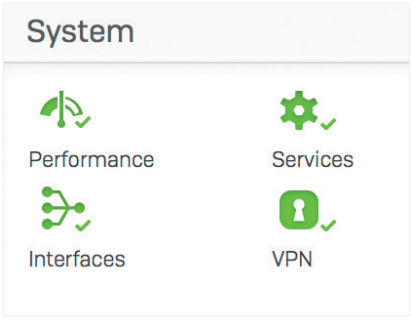
Reviste una importancia clave que un firewall moderno analice la gran cantidad de información que recopila, correlacione datos si es posible y destaque solamente la información más importante que requiere la adopción de medidas, idealmente antes de que sea demasiado tarde.

Centro de control

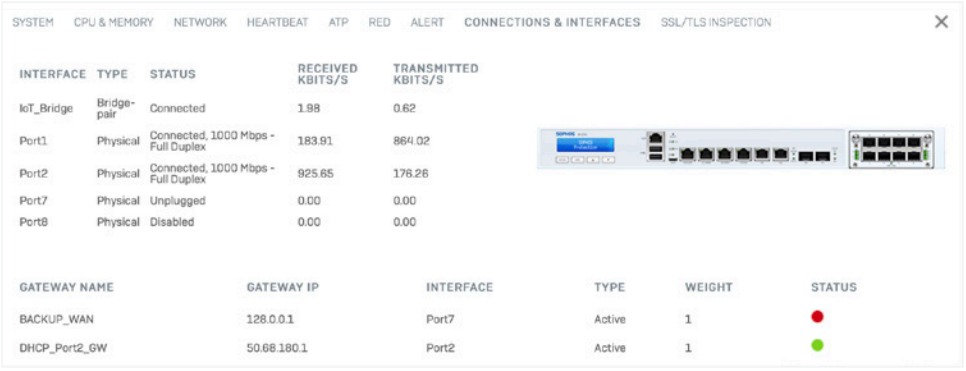
El Centro de control de Sophos Firewall ofrece un nivel de visibilidad sin precedentes de la actividad, los riesgos y las amenazas de la red.

Utiliza indicadores de tipo semáforo para concentrarse en lo que es más importante para usted.

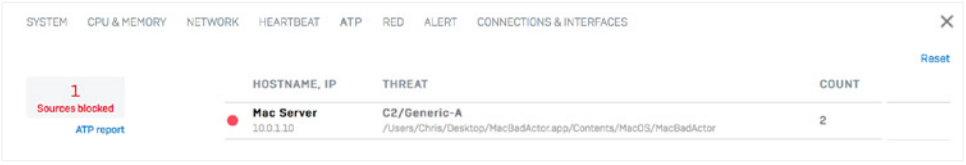
Si algún elemento aparece de color rojo, requiere atención inmediata. El amarillo indica un posible problema. Y si todos los elementos están en verde, no es necesario realizar ninguna acción.



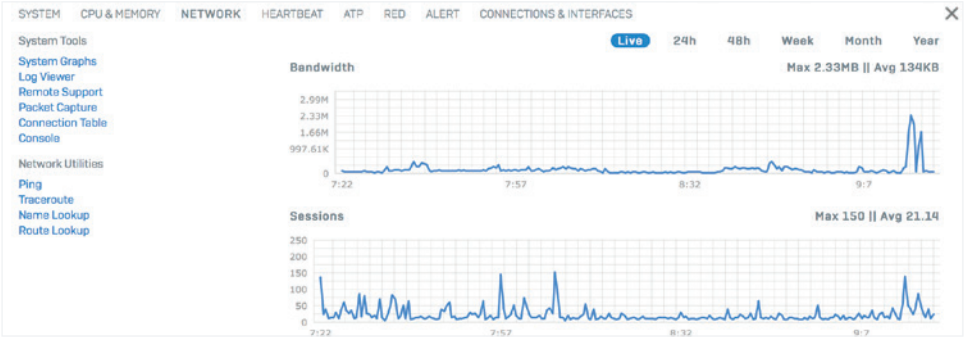
Cada widget del Centro de control ofrece información adicional que se muestra fácilmente al hacer clic en el widget en cuestión. Por ejemplo, para consultar el estado de las interfaces del dispositivo, basta con hacer clic en el widget "Interfaces" del Centro de control.



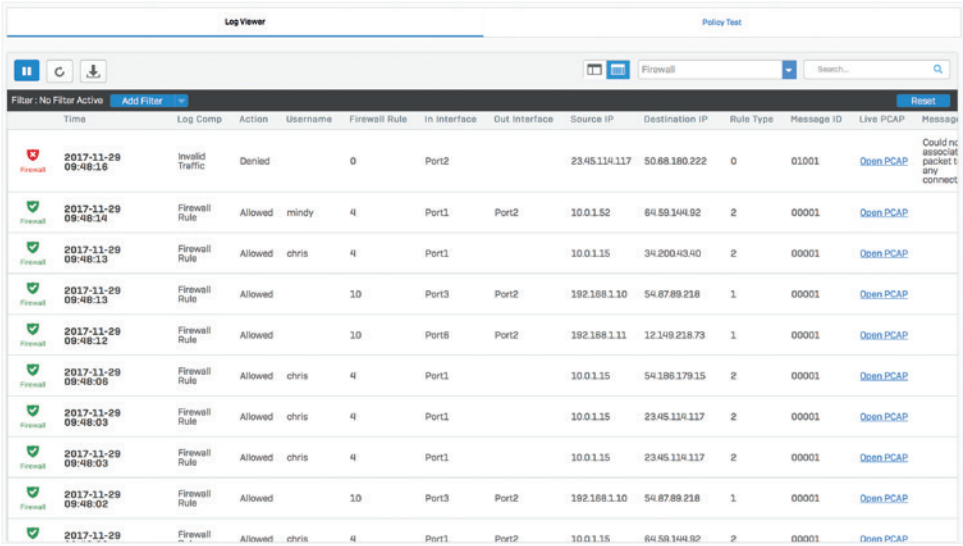
Para determinar el host, el usuario y el origen de una amenaza avanzada, solo hay que hacer clic en el widget "ATP" (protección contra amenazas avanzadas) en el panel de control.



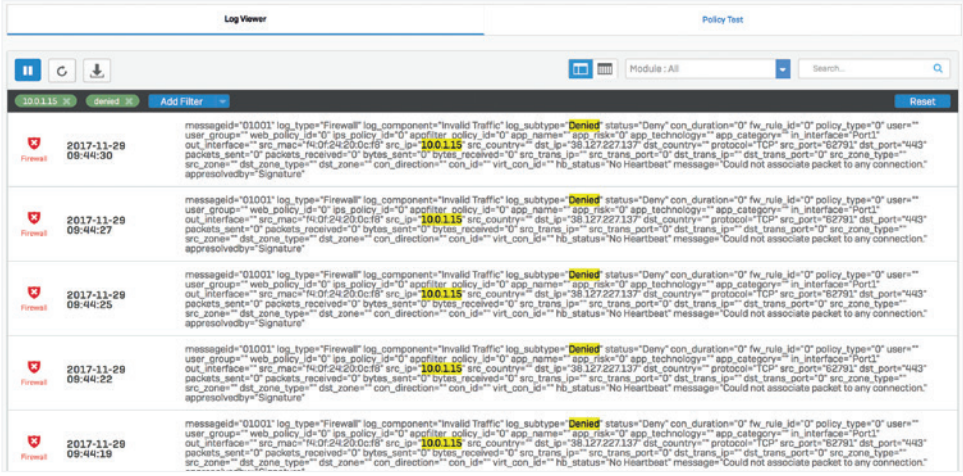
Los gráficos de sistema también muestran el rendimiento en el tiempo con periodos seleccionables, tanto si desea consultar las últimas dos horas como el último mes o año. Y proporcionan acceso rápido a herramientas de resolución de problemas utilizadas habitualmente para solucionar posibles problemas.



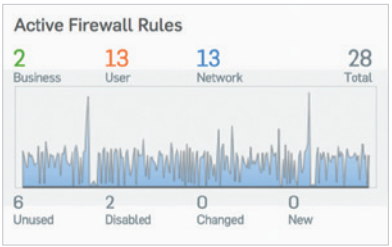
El visor del registro en directo está disponible desde cada pantalla con un solo clic. Puede abrirlo en una ventana nueva para supervisar el registro pertinente mientras trabaja en la consola. Muestra dos vistas: un formato más simple basado en columnas del módulo del firewall y una vista unificada más detallada con potentes opciones de filtrado y ordenación que agrupa los registros de todo el sistema en una única vista en tiempo real.



La mayoría de los administradores de redes probablemente se pregunten si tienen demasiadas reglas de firewall, cuáles son realmente necesarias y cuáles en realidad no se están utilizando. Con Sophos Firewall, esa duda se despeja.



El widget "Reglas del firewall activas" muestra un gráfico en tiempo real del tráfico que está procesando el firewall según el tipo de regla: reglas de aplicaciones empresariales, usuarios y redes. También muestra un número activo de reglas por estado, incluidas las reglas sin usar, lo que le da la oportunidad de reorganizarlas. Como con otras áreas del Centro de control, al hacer clic en cualquiera de ellas se desglosarán y, en este caso, se abrirá la tabla de reglas de firewall ordenada por el tipo o estado de regla.

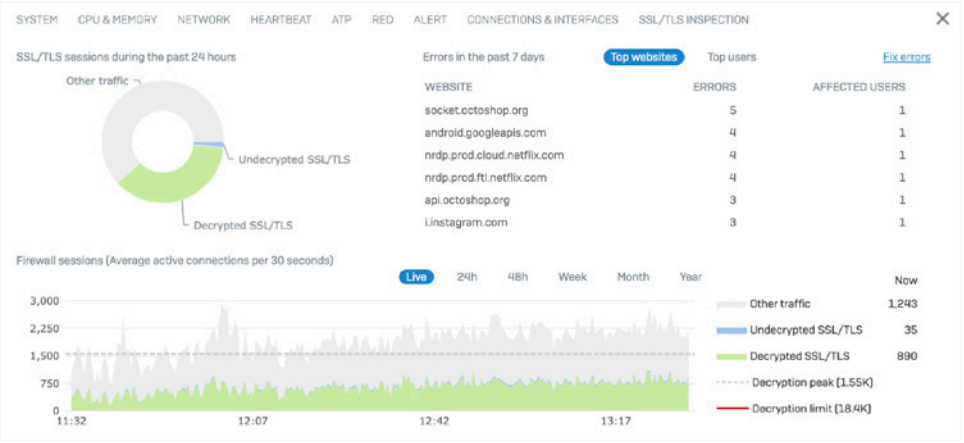


Inspección TLS de Xstream

Se está gestando la tormenta perfecta en torno al tráfico cifrado. Según Google, el volumen del tráfico cifrado en redes ha crecido a más de un 90 %. Este aumento representa una oportunidad para los ciberdelincuentes para lanzar ataques que están ocultos y, por tanto, son difíciles de detectar. Al fin y al cabo, no se puede detener lo que no se puede ver. Por desgracia, la mayoría de organizaciones no pueden hacer nada al respecto porque sus firewalls carecen de la potencia necesaria para utilizar la inspección TLS/SSL sin ralentizarse drásticamente.

Sophos Firewall, con su nuevo motor de inspección SSL de Xstream, tiene una capacidad mucho mayor para conexiones simultáneas y ofrece herramientas de políticas flexibles para tomar decisiones inteligentes sobre qué se debe escanear, con descarga en caso necesario. Usando las herramientas de políticas SSL, las organizaciones pueden crear políticas TLS/SSL de nivel empresarial relacionadas con el tráfico no descifrable, certificados, protocolos, opciones de imposición de cifrado y más. Sophos Firewall es compatible con TLS 1.3 y todos los paquetes de cifrado modernos en todos los puertos y aplicaciones del sistema.

Las herramientas adicionales disponibles directamente en el panel de control permiten a los administradores ver exactamente cuánto tráfico de red está cifrado y cómo se está gestionando. Sophos Firewall es mucho más efectivo a la hora de mostrar esta información que otras soluciones, especialmente en cómo destaca los errores detectados debido a la validación de certificados o sitios web que no admiten los estándares de cifrado más recientes.



Sophos Firewall ofrece información sobre los flujos de tráfico cifrado y cualquier problema que surja de la inspección TLS directamente desde el Centro de control

Los administradores también pueden abrir ventanas emergentes detalladas para ver exactamente qué sitios tienen problemas y por qué, además de los usuarios que están experimentando dificultades. A partir de ahí, pueden tomar medidas directamente para excluir una aplicación o un sitio del cifrado a fin de evitar problemas. Ninguna otra solución de inspección SSL ofrece la misma accesibilidad a esta información.

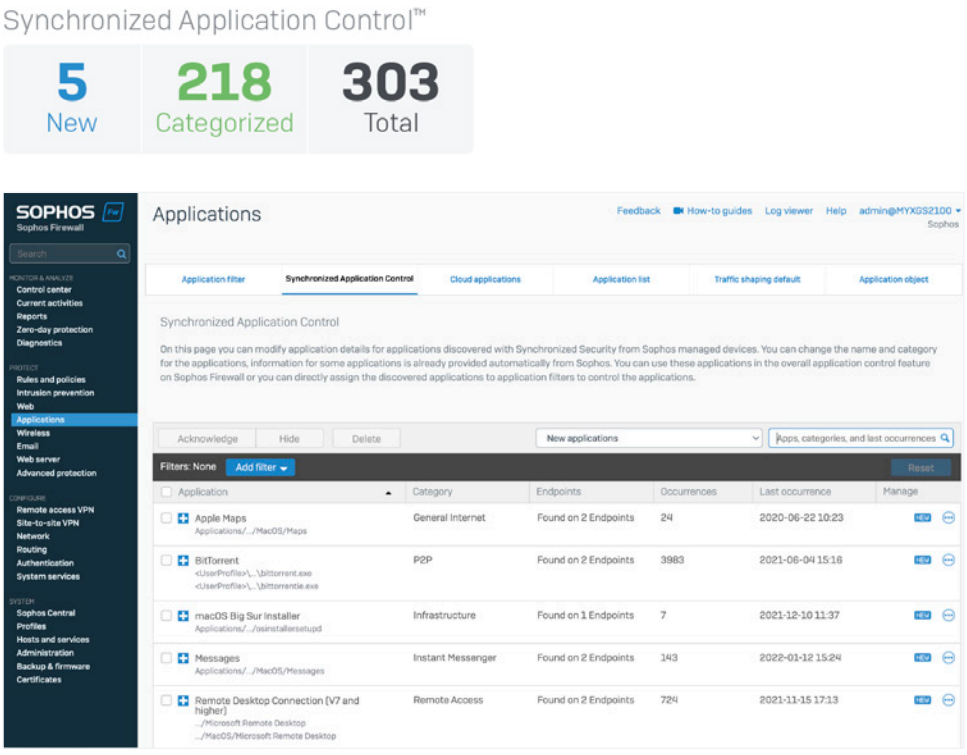
Control de aplicaciones sincronizado

El problema del control de aplicaciones de los firewalls next-gen actuales es que la mayoría del tráfico de aplicaciones no se identifica: se muestra como sin clasificar, desconocido, HTTP genérico o HTTPS genérico.

La razón de esto es sencilla, y es que los motores de control de aplicaciones de todos los firewalls dependen de firmas y patrones para identificar las aplicaciones. Como es de esperar, las aplicaciones de mercado verticales personalizadas, como aplicaciones médicas y financieras, no tendrán nunca firmas. Otras aplicaciones esquivas como los clientes BitTorrent y VoIP y aplicaciones de mensajería cambian constantemente su comportamiento y firma para eludir la detección y el control. Ahora muchas de ellas utilizan el cifrado para evadir la detección, mientras que otras simplemente recurren al uso de conexiones genéricas de tipo navegador web para comunicarse con el exterior a través del firewall porque los puertos 80 y 443 suelen estar desbloqueados en la mayoría de firewalls.

El resultado es una falta total de visibilidad de las aplicaciones de la red, y no se puede controlar lo que no se ve. La solución a este problema es muy elegante a la vez que efectiva: el Control de aplicaciones sincronizado de Sophos, que utiliza nuestra conexión exclusiva Seguridad Sincronizada con endpoints administrados por Sophos.

Funciona del siguiente modo. Cuando Sophos Firewall ve tráfico de aplicaciones que no puede identificar con firmas, pregunta al endpoint qué aplicación está generando ese tráfico.



Las aplicaciones desconocidas que han sido detectadas por el Control de aplicaciones sincronizado pueden clasificarse de forma automática o manual.

Entonces el endpoint puede compartir el ejecutable, la ruta y a menudo su categoría, y devolver esta información al firewall. Luego el firewall puede utilizar la información para clasificar y controlar la aplicación automáticamente en la mayoría de situaciones.

Si Sophos Firewall no puede determinar la categoría correcta de la aplicación automáticamente, el administrador puede establecer la categoría deseada o asignar la aplicación a una política existente.

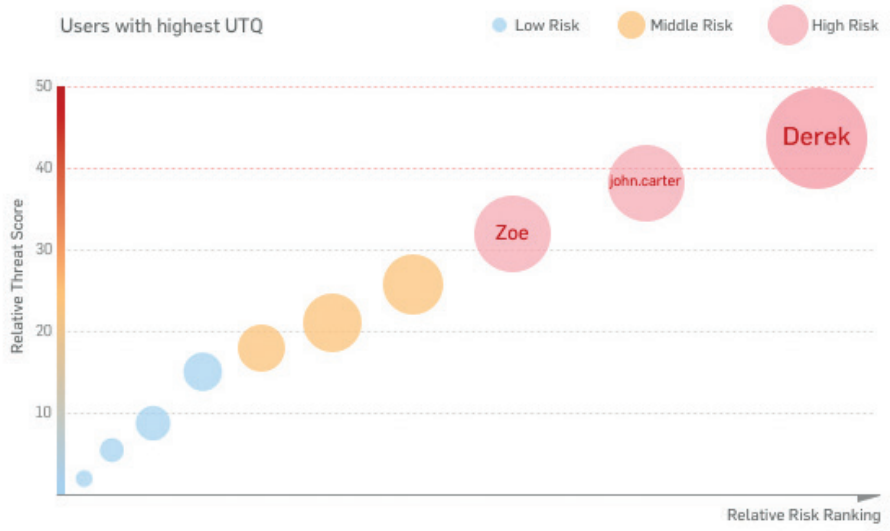
Una vez clasificada una aplicación, ya sea automáticamente o por parte del administrador de red, queda sujeta a los mismos controles de políticas que todas las demás aplicaciones de esa categoría, con lo que resulta muy fácil bloquear todas las aplicaciones no identificadas que no desee y priorizar aquellas que sí quiera.

El Control de aplicaciones sincronizado es un avance revolucionario en visibilidad y control de aplicaciones, puesto que ofrece una absoluta claridad sobre todas las aplicaciones en uso en la red, incluidas las que anteriormente no se identificaban ni controlaban.

Principales usuarios de riesgo

Diversos estudios han demostrado que los usuarios son el eslabón más débil en la cadena de seguridad. La buena noticia es que los patrones de conducta de los seres humanos pueden utilizarse para predecir y evitar ataques. Además, los patrones de uso pueden ayudar a ilustrar la eficiencia con que se utilizan los recursos corporativos y si las políticas de usuario deben ajustarse.

El cociente de amenazas por usuario (UTQ) de Sophos ayuda al administrador de seguridad a señalar a los usuarios que suponen un riesgo en función de su comportamiento web sospechoso y el historial de amenazas e infecciones. Una puntuación de riesgo UTQ alta de un usuario puede indicar acciones no intencionadas debido a una falta de concienciación sobre seguridad, una infección de malware o acciones malintencionadas.

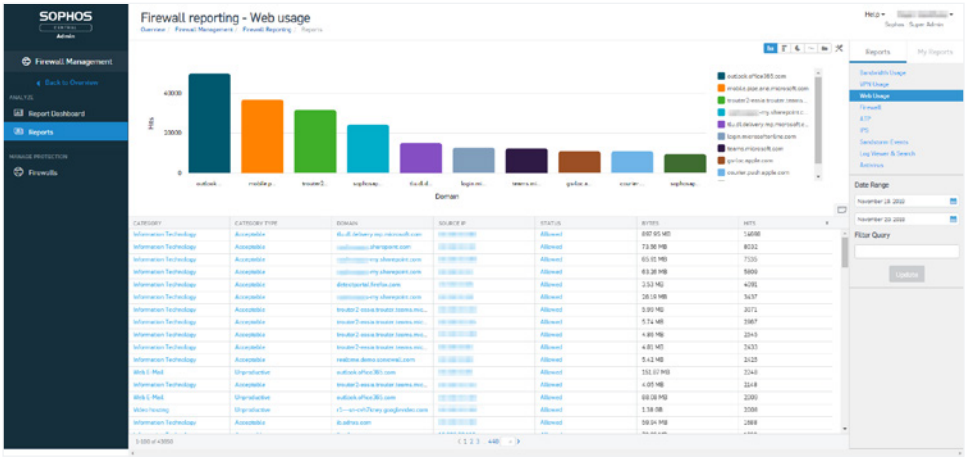


Sophos Firewall destaca los usuarios de mayor riesgo de un vistazo.

Conocer al usuario y las actividades que han provocado el riesgo ayuda al administrador de seguridad de la red a tomar las medidas necesarias, así como a educar a sus usuarios de mayor riesgo o a aplicar unas políticas más estrictas o más apropiadas para controlar su comportamiento.

Opciones de informes flexibles

Sophos Firewall es único entre los productos de firewall nex-gen y UTM, puesto que ofrece opciones de generación de informes integradas y en la nube con un alto grado de personalización sin costes adicionales. Sophos Central Firewall Reporting (CFR) permite a las organizaciones obtener una visión más completa de la actividad de la red a través del análisis. Gracias a su completo paquete de informes integrados y herramientas para crear cientos de variaciones, CFR proporciona información procesable sobre el comportamiento de los usuarios, el uso de las aplicaciones, los eventos de seguridad y mucho más. Los informes interactivos y el panel de control de informes permiten a los administradores profundizar en los datos de syslog almacenados en su cuenta de Sophos Central para obtener una vista granular que se presenta en un formato visual para facilitar su comprensión. Después se pueden analizar los datos para detectar tendencias que podrían identificar brechas en la posición de seguridad y poner de relieve la necesidad de posibles cambios de políticas.



Sophos Firewall ofrece numerosas opciones de generación de informes integrada y en la nube.

Sophos Firewall ofrece generación de informes integrada. Elija entre una amplia variedad de informes, organizados convenientemente por tipo, con varios paneles de control integrados. Se incluyen cientos de informes con parámetros personalizables en todas las áreas del firewall, como la actividad de tráfico, seguridad, usuarios, aplicaciones, web, redes, amenazas, VPN, correo electrónico y cumplimiento. Es sencillo programar el envío de informes periódicos por correo electrónico a su dirección o a los destinatarios que designe, así como guardar los informes como HTML, PDF o CSV.

Bloquear amenazas desconocidas

La protección contra las últimas amenazas de red requiere una sinfonía de tecnologías que funcionen al unísono y que tengan un maestro director al frente, el administrador de red. Desafortunadamente, la mayoría de firewalls funcionan más bien como un hombre orquesta tocando al tiempo que practica malabarismos con cuchillos, con reglas de firewalls definidas en un área, políticas web en otra, inspección TLS/ SSL por otro lado y control de aplicaciones en otra parte totalmente distinta del producto.

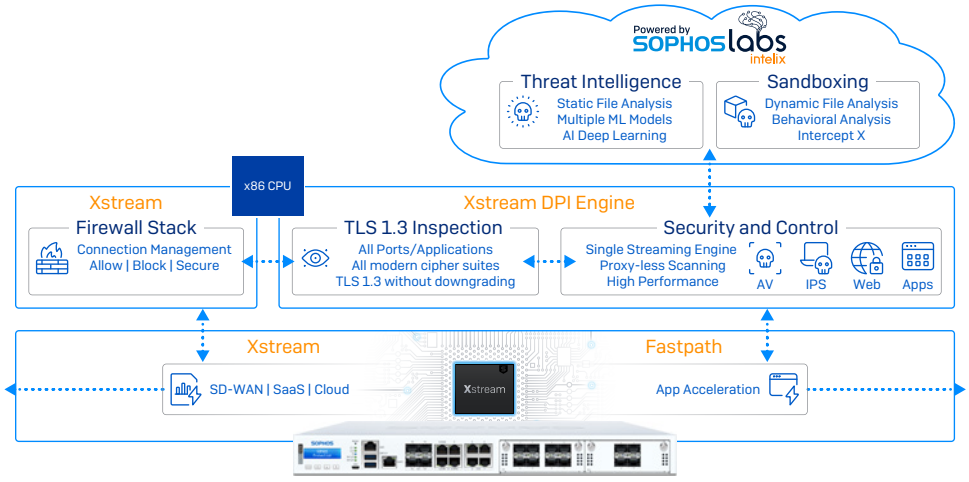
En Sophos, no solo pensamos que necesita la tecnología de protección más avanzada disponible, sino que también entendemos que debe ser fácil de configurar, desplegar y gestionar en el día a día, porque una protección mal configurada suele ser peor que no contar con ninguna protección en absoluto.

Una parte fundamental del ADN de Sophos siempre ha sido el compromiso con la simplicidad. Sin embargo, y quizá más importante aún, Sophos tiene una excepcional predisposición a adoptar cambios y tomar las medidas necesarias para hacer las cosas de un modo distinto a fin de ofrecer una mayor protección y una mejor experiencia del usuario.

Sophos Firewall hace cosas de forma distinta que suponen una gran diferencia.

Protección y rendimiento de Xstream

El rendimiento del firewall no debe ralentizarse cuando se activa la seguridad necesaria para mantener las redes protegidas de amenazas. Uno de los componentes principales de la arquitectura de procesamiento de paquetes de Xstream de Sophos Firewall es un motor de inspección detallada de paquetes (DPI) de alta velocidad. El motor DPI ofrece un escaneado de seguridad en un solo paso y sin proxy para el control de aplicaciones, antivirus, web e IPS además de nuestra inspección SSL de Xstream.



La arquitectura Xstream de Sophos Firewall con procesadores de flujo Xstream programables ofrece una protección y un rendimiento potentes.

Cuando se establece una nueva conexión, es procesada por la pila del firewall, que toma decisiones sobre si permitir, bloquear o escanear el tráfico para detectar amenazas. Si el tráfico requiere escaneado de seguridad, reenvía los paquetes al motor DPI de transmisión de alto rendimiento sin proxy que escanea los paquetes incluso si están cifrados. Esto solo se utiliza para algunos paquetes iniciales. Después, la pila del firewall se hace a un lado y descarga el procesamiento al motor DPI por completo. Esto mejora notablemente la latencia y el rendimiento.

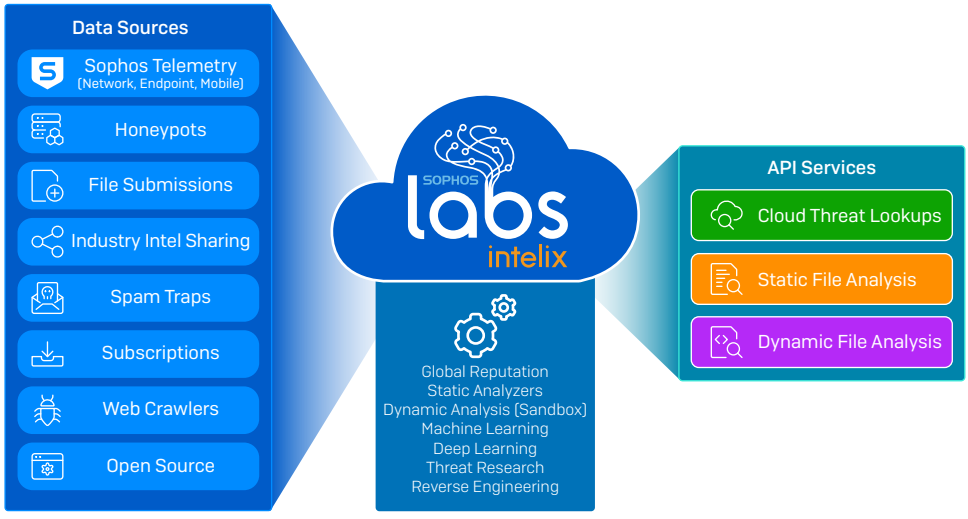
A continuación, si la transmisión se considera segura y ya no requiere más inspección, el motor DPI puede descargar el flujo por completo a la ruta rápida FastPath del flujo de red de Sophos, que proporciona una ruta acelerada para el tráfico de confianza. Esto mejora el rendimiento de forma espectacular al liberar otros recursos de la inspección del tráfico que no lo necesita.

Protección contra amenazas de día cero

Dado que las amenazas avanzadas como el ransomware son cada vez más dirigidas y esquivas, existe la necesidad crítica de disponer de identificación y protección predictivas contra las amenazas de día cero. La solución definitiva para esto tiene dos vertientes:

1. **Análisis de Machine Learning estático**: proporciona análisis predictivo y detección a través de múltiples modelos de Machine Learning con redes neuronales artificiales, combinado con la reputación global y el escaneado profundo de archivos, todo ello sin necesidad de ejecutar el archivo en tiempo real.
2. **Análisis de espacio seguro en tiempo de ejecución dinámico**: detona el malware en tiempo real en un entorno de espacio seguro en la nube para obtener información clave exclusiva sobre la actividad del archivo a fin de revelar la verdadera naturaleza y las capacidades de una amenaza desconocida.

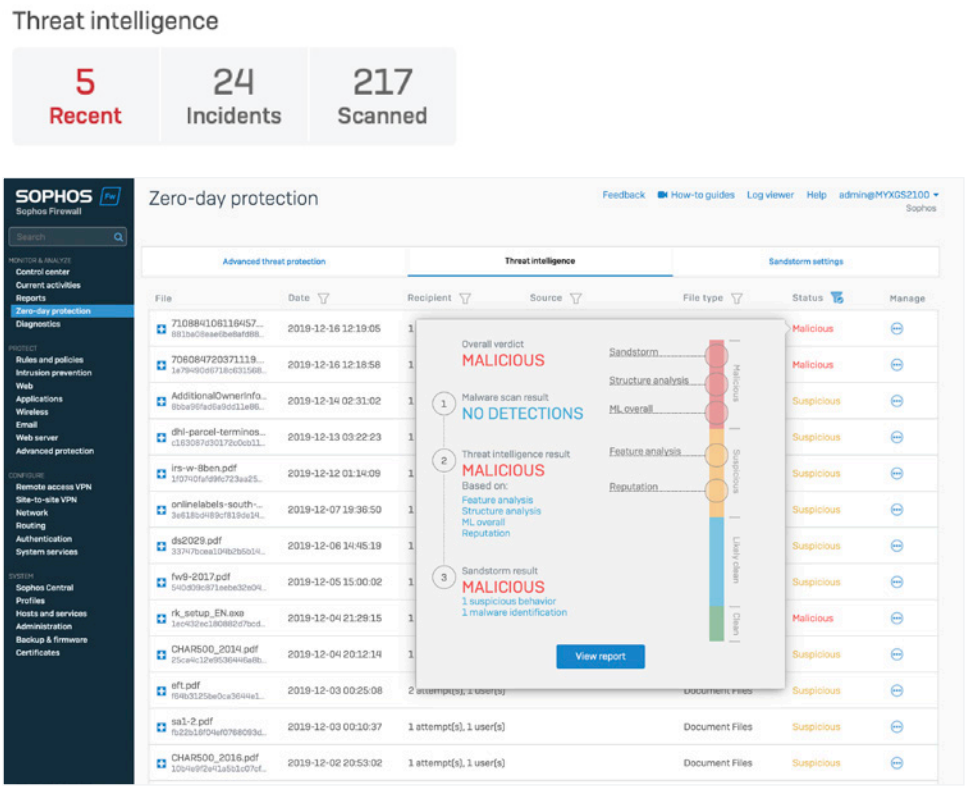
Sophos Firewall incluye estas dos importantes tecnologías de protección, impulsadas por SophosLabs Intelix. SophosLabs, nuestro reconocido laboratorio de investigación de amenazas de ciberseguridad de primer nivel, ha desarrollado la plataforma definitiva de información y análisis de amenazas en SophosLabs Intelix. Utiliza la última tecnología de Machine Learning, décadas de investigación sobre amenazas y petabytes de información para ofrecer una protección inigualable contra las amenazas desconocidas más recientes.



La protección de día cero de Sophos Firewall se basa en el análisis de Machine Learning de SophosLabs Intelix.

Cuando el motor DPI de Xstream de Sophos Firewall realiza un análisis antivirus de un archivo que entra en la red y determina que hay código activo, retiene el archivo temporalmente y lo envía al servicio SophosLabs Intelix en la nube para realizar un análisis del archivo tanto estático como dinámico. A continuación proporciona un resumen de los resultados en el Centro de control de Sophos Firewall a través del widget Información sobre amenazas y este informe navegable (abajo), y solo libera el archivo para la aplicación de descarga o el destinatario de correo electrónico si el archivo está limpio.

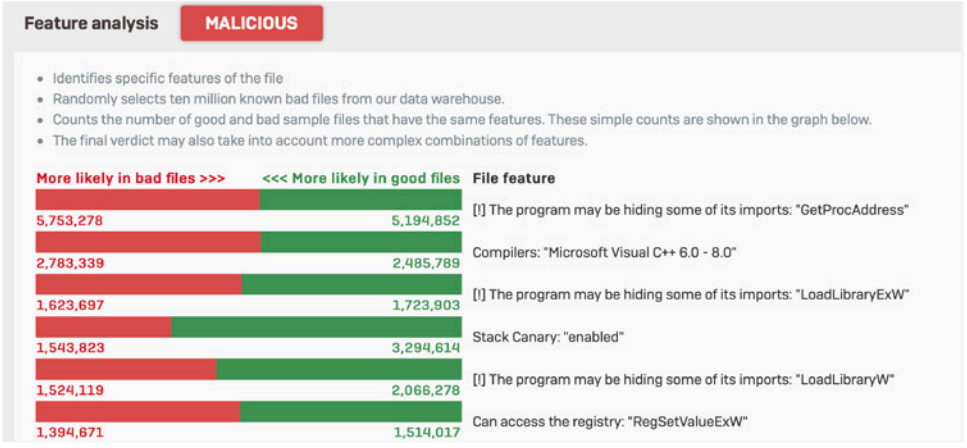
Este último paso es importante, ya que muchas soluciones antimalware avanzadas para firewalls suelen liberar el archivo al usuario final antes de que el análisis se haya completado, lo que puede tener como resultado una limpieza compleja y costosa si el archivo acaba clasificándose como una amenaza.



La protección de día cero de Sophos Firewall identifica amenazas nuevas y desconocidas antes de que entren en su red.

Análisis de Machine Learning estático

El análisis estático de archivos utiliza múltiples modelos de Machine Learning para analizar varias características, funciones y elementos de genética y reputación del archivo, comparándolo con millones de archivos benignos y maliciosos de la base de datos de SophosLabs para emitir un veredicto en segundos sobre cualquier archivo nuevo y desconocido. Es notablemente rápido y eficaz a la hora de identificar nuevas amenazas y nuevas variantes de amenazas existentes, en particular amenazas que no son fáciles de aislar en un espacio seguro, como los documentos protegidos por contraseña que contienen malware.



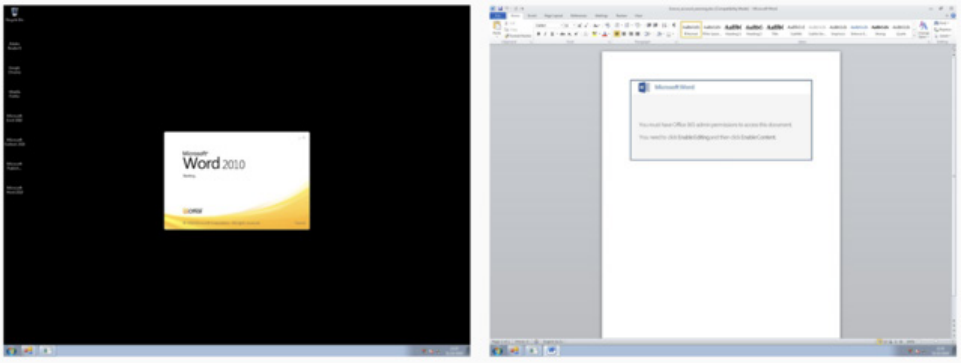
Se utilizan múltiples modelos de Machine Learning para analizar los archivos sospechosos en busca de amenazas de día cero.

Análisis de espacio seguro en tiempo de ejecución dinámico

Cuando apareció la tecnología de espacios seguros, solo era asequible para las grandes corporaciones. Pero ahora, gracias a las soluciones de espacio seguro basadas en la nube como Sophos Sandstorm, el precio es increíblemente asequible incluso para las empresas más pequeñas. Por primera vez, las pequeñas y medianas empresas tienen acceso a espacios seguros con tecnología de Deep Learning que va mucho más allá de las funciones de las soluciones de espacios seguros locales dedicadas que implementaban las empresas por millones de dólares hace apenas unos años.

Como está basado en la nube, no se necesita ningún software ni hardware adicional, y el rendimiento del firewall no se ve afectado. Cualquier archivo que el motor DPI de Xstream determina que contiene código activo, como un archivo adjunto de correo electrónico o una descarga web, se carga y detona automáticamente en un espacio seguro en la nube de SophosLabs Intelix, al tiempo que se realiza un análisis estático (explicado arriba) para determinar su comportamiento en tiempo de ejecución antes de que se permita su entrada en la red.

Para identificar amenazas, SophosLabs ha integrado las últimas tecnologías de protección de Intercept X, nuestro producto para endpoints next-gen líder del sector, en Sophos Sandstorm, que incluye Deep Learning, detección de exploits y CryptoGuard (para detectar el ransomware activo que cifra los archivos en tiempo real). También supervisa toda la actividad de la red, el registro, la memoria y los archivos en busca de características de tipo malicioso para emitir un veredicto. Ningún otro firewall ofrece este tipo de análisis en tiempo de ejecución con la mejor protección contra amenazas del mundo, Intercept X. Y ningún otro firewall ofrece el nivel de visibilidad e información que ofrece Sophos Firewall, incluida una serie completa de capturas de pantalla con lo ocurrido al ejecutar el archivo.

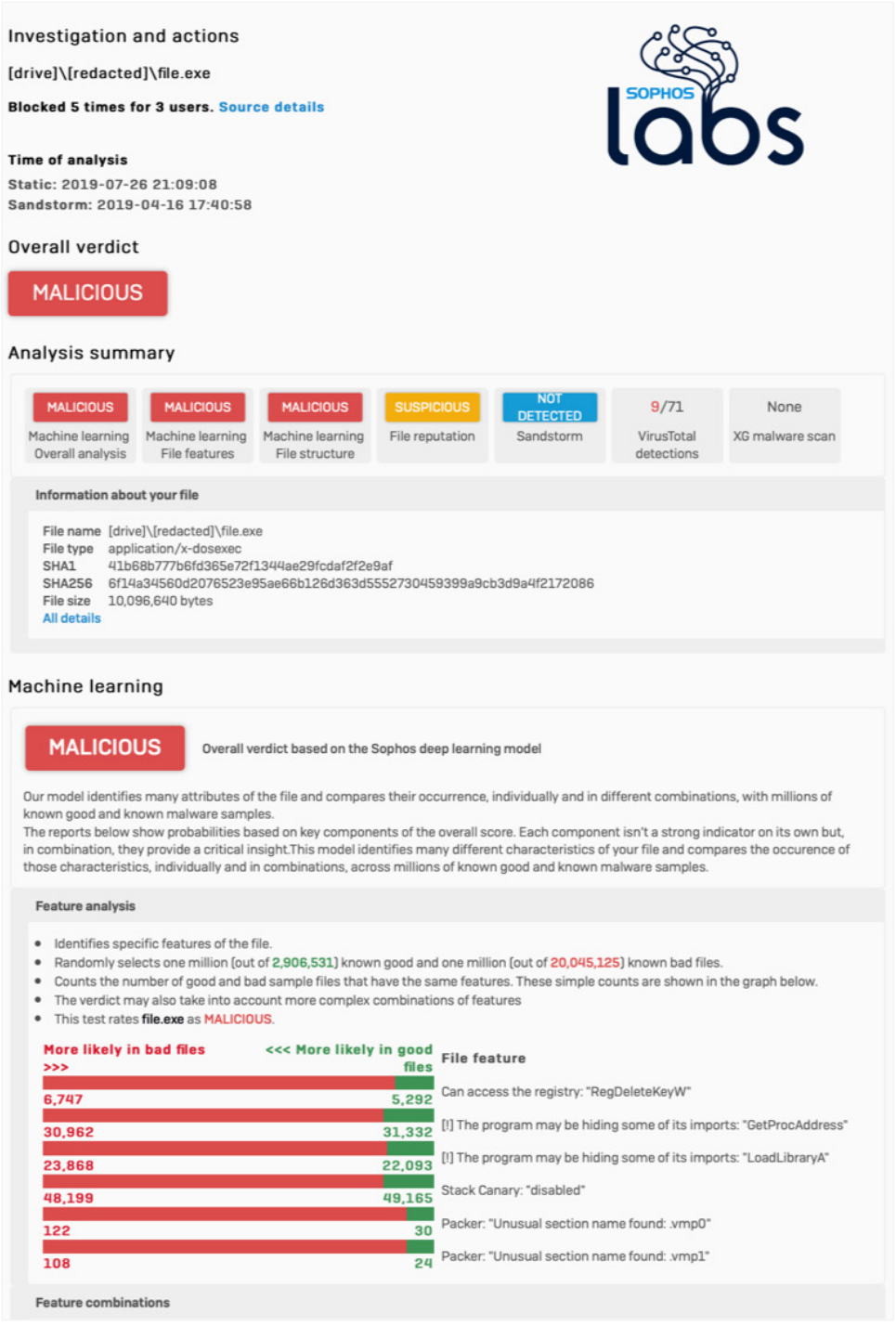


El análisis de espacio seguro en tiempo de ejecución detona los archivos en un entorno seguro para determinar el comportamiento y proporciona capturas de pantalla para que las revise.

El uso de espacios seguros es particularmente eficaz para detectar amenazas que acechan en archivos normalmente benignos que pueden no tener ninguna característica maliciosa evidente, como archivos de Office con macros, o actualizaciones de aplicaciones o ejecutables benignos que han sido alterados.

Informes de protección contra amenazas

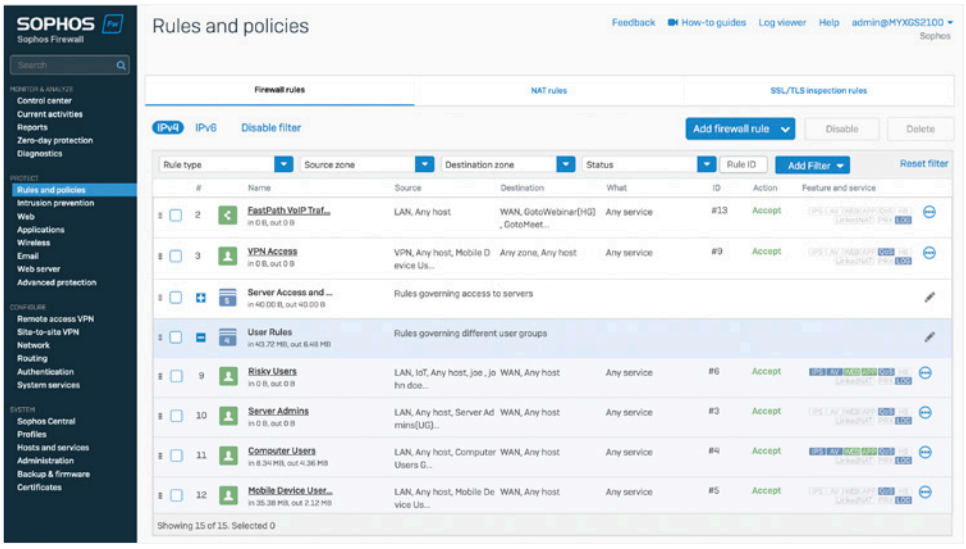
Cada archivo analizado por Sophos Firewall viene acompañado por un informe que proporciona todos los detalles de los resultados de los distintos análisis y los veredictos. El informe cubre seis aspectos diferentes, entre ellos, los distintos análisis de Machine Learning, la reputación del archivo, el espacio seguro e incluso datos de VirusTotal de terceros.



Administración de reglas unificada

Administrar un firewall puede ser increíblemente complejo. Con numerosas reglas, políticas y configuraciones de seguridad distribuidas en diferentes áreas funcionales, a menudo siendo precisas varias reglas distintas para ofrecer la protección necesaria, son muchas las cosas que hay que hacer.

Con Sophos Firewall, aprovechamos la oportunidad para replantearnos la forma en que se organizan las reglas y el modo en que se gestiona su posición en materia de seguridad. En vez de tener que rebuscar las políticas adecuadas en la consola de administración, reunimos toda la gestión de imposiciones y reglas del firewall en una sola pantalla unificada. Ahora puede ver, filtrar, buscar, editar, añadir, modificar y organizar todas las reglas de firewall desde un mismo lugar.



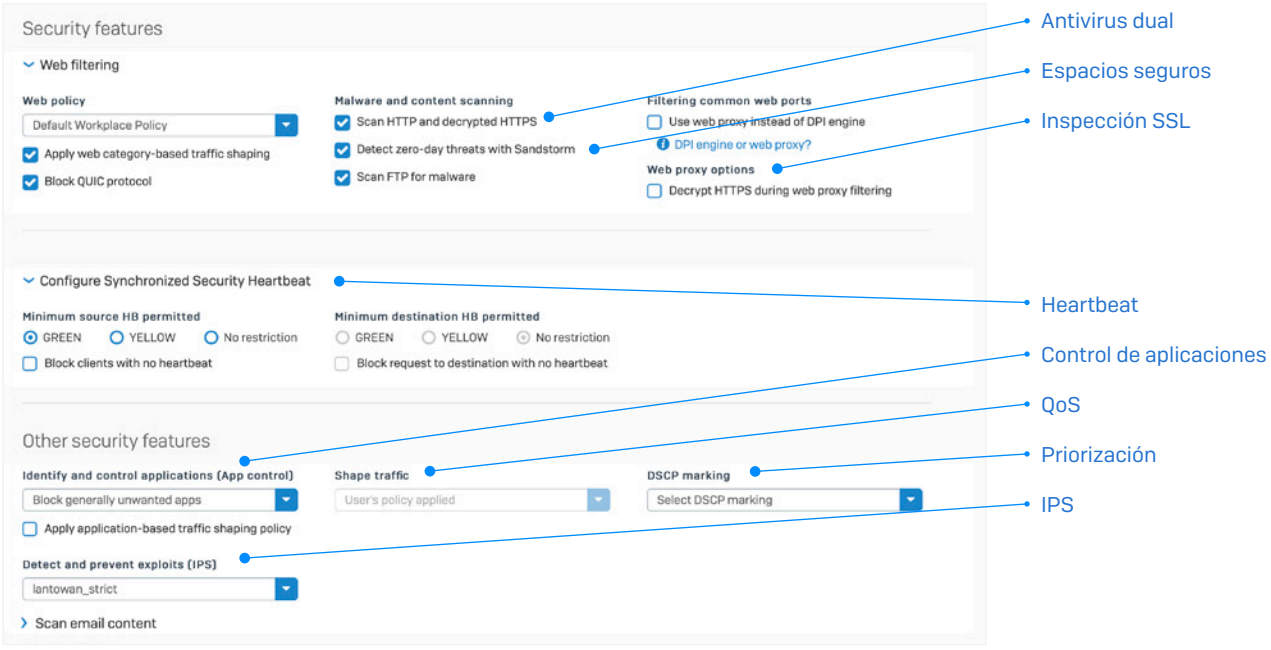
Sophos Firewall reúne todas sus reglas de políticas de acceso, NAT e inspección TLS en un solo lugar, lo que facilita su gestión.

Con las reglas para usuarios, aplicaciones empresariales, NAT, inspección TLS/SSL y redes resulta fácil ver solo las políticas que se necesitan, al tiempo que se dispone de una única y cómoda pantalla para la gestión.

Los iconos de los indicadores ofrecen información importante de las políticas, como su tipo, estado, imposición y mucho más.

Gestionar el estado de seguridad de un vistazo

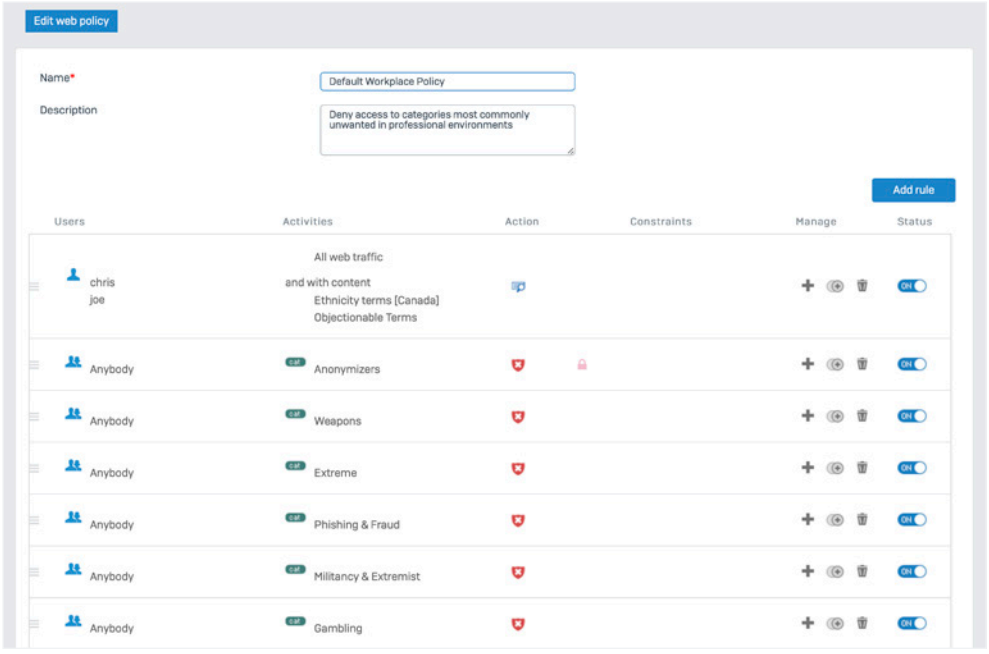
Ya sea a través de su cuenta de Sophos Central en la nube o la interfaz de usuario de Sophos Firewall, con Sophos resulta increíblemente sencillo configurar y gestionar todo lo necesario para una protección moderna y hacerlo todo desde una única pantalla.



Configure su postura de seguridad completa en una pantalla utilizando políticas predefinidas o personalizadas.

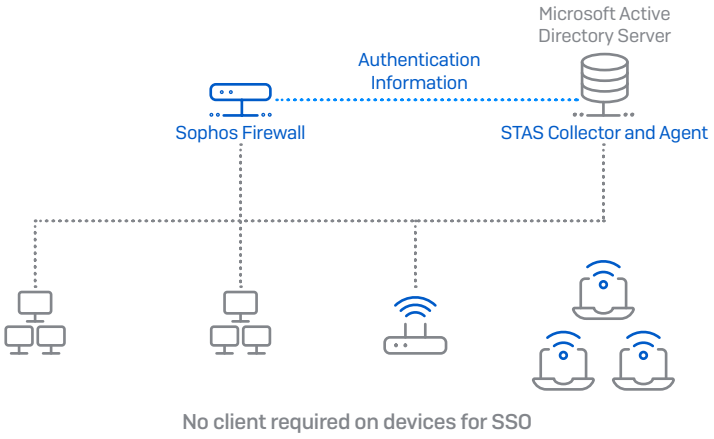
Puede configurar y ajustar la seguridad y el control para el antivirus, la inspección TLS/SSL, los espacios seguros, IPS, el conformado de tráfico, el control web y de aplicaciones, Security Heartbeat, NAT, el enrutamiento y la priorización en un único lugar, y todo ello regla por regla, usuario por usuario o grupo por grupo.

Y si quiere ver exactamente qué está haciendo cualquiera de sus políticas ajustables, o incluso realizar cambios, puede editarlas ahí mismo, sin tener que dejar la regla del firewall y acceder a otra parte del producto.



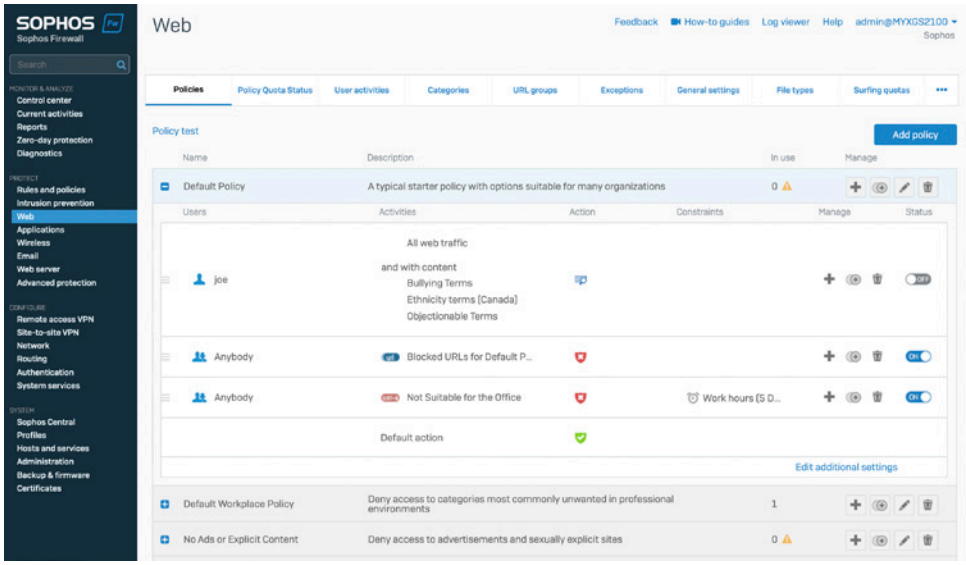
Vea los detalles de las políticas de un vistazo y haga cambios sin salir de la pantalla de reglas del firewall.

Las opciones de autenticación flexibles le permiten saber fácilmente quién es quién e incluyen servicios de directorio como Active Directory, eDirectory y LDAP, así como NTLM, Kerberos, RADIUS, TACACS+, RSA, agentes de cliente o un portal cautivo. Además, Sophos Transparent Authentication Suite (STAS) se integra con servicios de directorio como Microsoft Active Directory para una autenticación del inicio de sesión único sencilla, transparente y fiable.



Puerta segura de enlace a Internet de nivel empresarial

El control y la protección web son un elemento fundamental en cualquier firewall pero, por desgracia, en la mayoría de implementaciones de firewalls parecen algo secundario. Nuestra experiencia en la creación de soluciones de protección web de nivel empresarial nos ha proporcionado los conocimientos para desplegar el tipo de control de políticas web que solo suele encontrarse en soluciones de puerta segura de enlace a Internet (SWG) empresariales que cuestan diez veces más. Hemos implementado un modelo de políticas jerárquico basado en la herencia que hace que crear políticas sofisticadas sea sencillo e intuitivo. Se incluyen plantillas de políticas predefinidas listas para usar para la mayoría de implementaciones más comunes, como entornos laborales típicos, cumplimiento de la CIPA para la educación y mucho más. Significa que puede tenerlo todo en funcionamiento y cumplir con las normativas de forma inmediata, con sencillas opciones de ajuste y personalización a su alcance.



Las potentes políticas web de nivel empresarial ofrecen controles granulares.

De hecho, sabemos que las políticas web son uno de los elementos que se cambian más a menudo a diario en un firewall, motivo por el cual nos hemos esforzado mucho en facilitarle la gestión y el ajuste de las políticas en función de sus necesidades empresariales y de usuario. Puede personalizar fácilmente usuarios y grupos, actividades (compuestas por URL, categorías, filtros de contenido y tipos de archivo), acciones (bloquear, permitir o avisar) y añadir o ajustar restricciones según la hora del día y el día de la semana.

Funciones para el sector educativo

Sophos Firewall ofrece varias funciones ideales para entornos educativos en que las políticas web y el cumplimiento son requisitos fundamentales. Entre las funciones específicas para la educación se incluyen:

- Políticas web preestablecidas para el cumplimiento de la CIPA
- Filtrado de contenido y generación de informes por palabras clave
- Opciones para la restricción de SafeSearch y YouTube por políticas de grupos/usuarios
- Invalidaciones de páginas de bloqueo que pueden gestionar los profesores
- Completa generación de informes integrada para identificar los posibles problemas con prontitud

Ahora las políticas web incluyen la opción de registrar, supervisar e incluso imponer una política relacionada con contenido dinámico basado en listas de palabras clave. Esta función es especialmente importante en entornos educativos para garantizar la seguridad online de los menores y proporcionar información sobre estudiantes que utilizan palabras clave relacionadas con la autolesión, el acoso escolar, la radicalización y otro contenido inadecuado. Las bibliotecas de palabras clave pueden cargarse en el firewall y aplicarse a cualquier política de filtrado web como criterio adicional, con acciones para registrar, supervisar o bloquear resultados de búsqueda o sitios web que contengan las palabras clave de interés.

Se proporcionan informes completos para identificar las coincidencias de palabras clave y los usuarios que buscan o consumen contenido de palabras clave de interés, lo que permite una intervención proactiva antes de que un usuario en riesgo se convierta en un problema real.

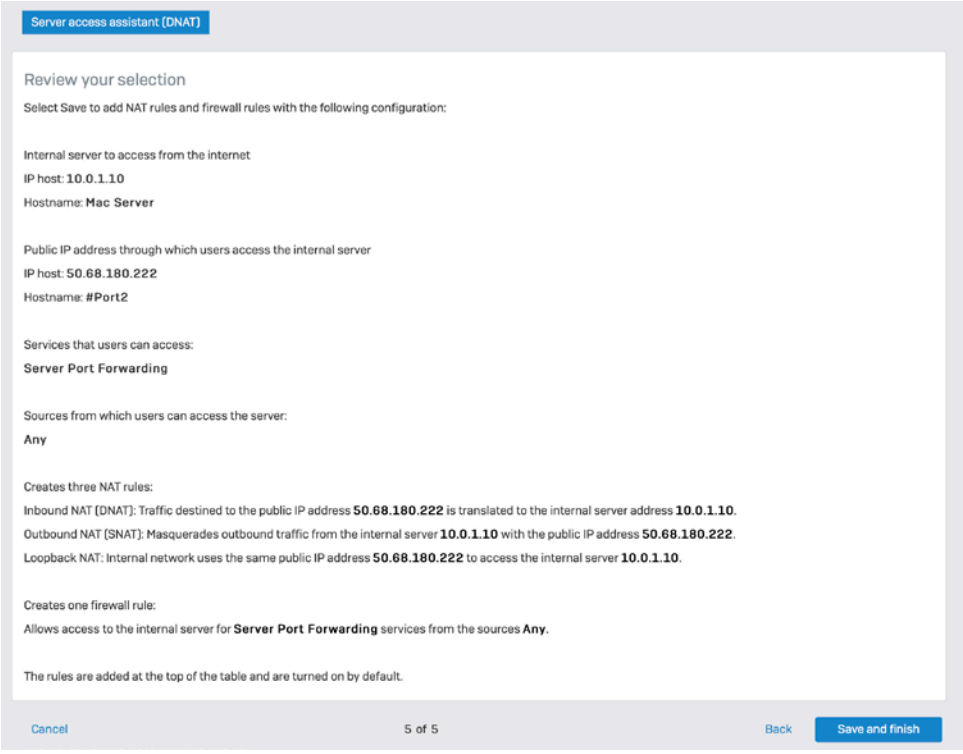
Sophos Firewall ayuda con el cumplimiento de políticas de la CIPA de forma inmediata, lo que permite un rápido cumplimiento. También ofrece controles potentes y flexibles de las restricciones de SafeSearch y YouTube por políticas de usuarios/grupos. Y se puede dar a los profesores la opción de configurar y gestionar sus propias invalidaciones de políticas para permitir que sus clases puedan acceder a sitios web que normalmente estarían bloqueados como parte del plan de estudios.

Son políticas web potentes sin complicaciones.

Configuración NAT simplificada

Cualquiera que haya intentado configurar reglas de NAT (traducción de direcciones de red) sabe lo complicado que puede llegar a ser. Pero no tiene por qué serlo. Sophos Firewall incluye una completa funcionalidad NAT para empresas que permite configuraciones NAT potentes y flexibles como NAT de origen (SNAT) y NAT de destino (DNAT) en una única regla con criterios de selección granulares. Para simplificar una DNAT compleja, un asistente fácil de usar le guía durante el proceso de creación de una configuración NAT completa en solo unos clics.

Los administradores también pueden sacar partido de una cómoda opción de NAT vinculada al crear una regla de firewall. La NAT vinculada crea automáticamente una regla de configuración NAT correspondiente, lo que reduce todavía más el tiempo necesario para crear y configurar reglas NAT.

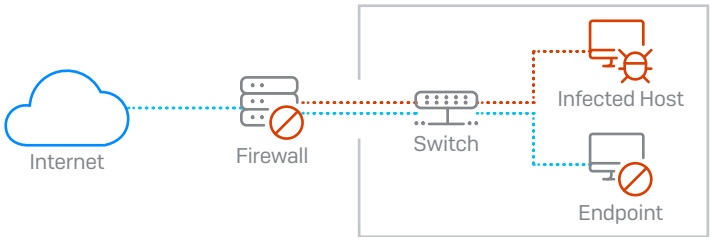


Saque partido al potente a la vez que intuitivo asistente de reglas NAT para crear controles de acceso complejos con solo unos pocos clics.

Respuesta automática a incidentes

Una de las funciones de firewall más solicitadas por los administradores de red es la capacidad de responder automáticamente a los incidentes de seguridad en la red.

Sophos Firewall es la única solución de seguridad para redes que identifica totalmente el origen de una infección en la red y responde limitando el acceso del dispositivo infectado a los otros recursos de red de forma automática. Esto es posible gracias a nuestra tecnología única de Sophos Security Heartbeat, que comparte el estado de seguridad y datos de telemetría entre los endpoints administrados por Sophos y su firewall.



Sophos Firewall y Security Heartbeat pueden aislar automáticamente los hosts infectados en su red.

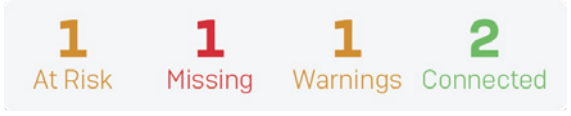
Sophos Firewall integra el estado de los hosts conectados de forma única en las reglas del firewall, lo que permite limitar automáticamente el acceso a recursos delicados de la red por parte de cualquier sistema afectado hasta que se descontamine.

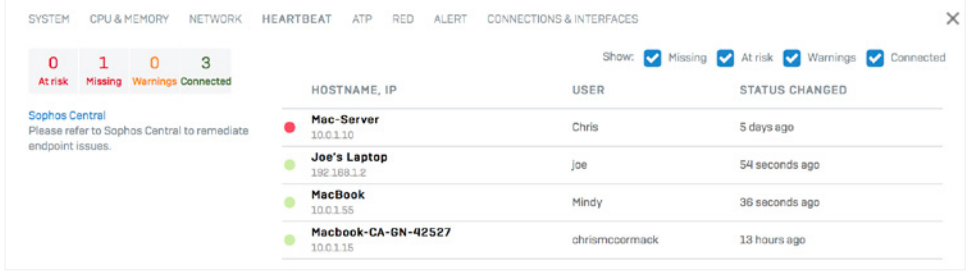
Sophos Firewall no solo puede aislar los endpoints para evitar que accedan a otras partes de la red en el firewall, sino que también puede obtener ayuda de todos los endpoints con buen estado de seguridad de la red para aislar aún más un host comprometido a nivel del endpoint.

Esta protección contra la propagación lateral, que así se denomina, aísla e impide que las amenazas o los atacantes se propaguen lateralmente por la red hasta otros sistemas, incluso aunque estén en el mismo segmento de red o dominio de difusión en que normalmente no puede intervenir el firewall. Se trata de una solución sumamente simple y efectiva ante el desafío de los adversarios activos que operan en su red. Y solo es posible si su endpoint y firewall funcionan de forma conjunta en una defensa coordenada o sincronizada.

Security Heartbeat

Sophos Security Heartbeat comparte información en tiempo real utilizando un enlace seguro entre sus endpoints administrados por Sophos y Sophos Firewall. Simplemente sincronizando los productos de seguridad que antes funcionaban de manera independiente, le permite crear una protección más eficaz frente a aplicaciones maliciosas avanzadas y ataques dirigidos.





El estado de Security Heartbeat™ de la red es visible en el Centro de control.

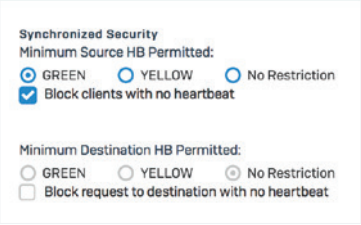
Security Heartbeat no solo identifica la presencia de amenazas avanzadas al instante, sino que también puede utilizarse para comunicar información importante acerca de la naturaleza de la amenaza, el sistema host y el usuario. Y, quizás más importante aún, Security Heartbeat también puede actuar automáticamente para aislar o limitar el acceso a los sistemas comprometidos hasta que estén libres de malware. Es una tecnología fascinante que ha revolucionado la forma en que las soluciones de seguridad TI identifican y responden a las amenazas avanzadas.

Security Heartbeat para los endpoints administrados detrás del firewall puede hallarse en uno de estos tres estados:

El estado de **Heartbeat verde** indica que el dispositivo endpoint se encuentra en buen estado y tiene permiso para acceder a todos los recursos de red apropiados.

El estado de **Heartbeat amarillo** avisa de que un dispositivo puede tener una aplicación no deseada (PUA), no cumple la normativa o está experimentando otro tipo de problema. Puede elegir a qué recursos de red puede acceder un Heartbeat amarillo hasta que el problema en cuestión se resuelva.

El estado de **Heartbeat rojo** indica que hay un dispositivo que corre el riesgo de ser infectado por una amenaza avanzada y puede estar intentando contactar con una red de bots o un servidor de comando y control. Usando la configuración de políticas de Security Heartbeat en su firewall, puede aislar fácilmente los sistemas cuyo estado de Heartbeat sea de color rojo hasta que se hayan limpiado para reducir los riesgos de fugas de datos o evitar que se propague la infección.



Configure los requisitos de Security Heartbeat como parte de cualquier regla de firewall.

Solo Sophos puede ofrecer una solución como Security Heartbeat, porque solo Sophos es líder en soluciones de seguridad tanto para endpoints como para redes. Mientras que otros fabricantes se están empezando a dar cuenta de que este es el futuro de la seguridad TI y desesperados intentan implementar algo parecido, todos se encuentran en clara desventaja: no poseen una solución para endpoints líder en el mercado ni una solución para firewalls líder en el mercado que poder integrar.

Un mundo Zero Trust

La confianza se ha convertido en una palabra peligrosa en el sector de TI, especialmente cuando esa confianza es implícita. Se ha demostrado que crear un gran perímetro corporativo precintado y confiar en todo lo que se encuentra en su interior es una estrategia condenada al fracaso.

Zero Trust es un enfoque holístico a la seguridad que gestiona estos cambios y cómo las organizaciones trabajan y responden a las amenazas. Se trata de un modelo y una filosofía para saber cómo pensar sobre la seguridad y cómo ejecutarla.

Nada ni nadie es digno de una confianza automática, ni dentro ni fuera de la red corporativa. Sin embargo, llegados a cierto punto será necesario confiar en algo. Con Zero Trust, esta confianza es temporal y se establece desde múltiples fuentes de datos, además de reevaluarse constantemente.

Zero Trust nos permite controlar toda nuestra infraestructura, desde dentro de la oficina hasta las plataformas en la nube que utilizamos. Se acabaron la falta de control fuera del perímetro corporativo y las dificultades con los usuarios remotos.

¿Cómo pasamos a Zero Trust y sacamos partido de todas las ventajas que ofrece? Si bien nadie puede ofrecer Zero Trust en una única solución, Sophos ofrece un amplio catálogo de tecnologías y controles de seguridad que aceleran y simplifican su camino hacia Zero Trust.

Sophos Central: la plataforma de ciberseguridad en la que más confía el mundo aúna estas tecnologías dispares y complementarias en una única consola de administración en la nube para ayudarle a organizar y supervisar su red Zero Trust.

Seguridad Sincronizada: ciberseguridad que comparte información entre endpoints, ZTNA, firewalls y otros sistemas de forma continuada para ofrecer información y visibilidad entre sí.

Sophos ZTNA: constituye una verdadera solución Zero Trust Network Access para conectar a los usuarios de forma segura a las aplicaciones y los datos.

Sophos Firewall: cree segmentos y microperímetros alrededor de usuarios, dispositivos, aplicaciones, redes y más.

Server Protection e Intercept X: asigne un estado de seguridad del dispositivo a cada dispositivo para que, en el caso de que uno se vea comprometido, los dispositivos puedan aislarse e impedir que se conecten a otros dispositivos automáticamente.

Servicio Managed Threat Response (MTR): supervisa toda la actividad de los usuarios en toda la red e identifica credenciales de usuario potencialmente comprometidas.

Optimice su red SD-WAN

Hay pocos términos relacionados con las redes que hayan levantado tanto revuelo como SD-WAN (red de área extensa definida por software). Y todo este revuelo ha ido acompañado de información útil y teoría confusa a partes iguales. Como resultado, SD-WAN ha acabado significando cosas diferentes para distintas personas, mientras que otras aún intentan descifrar su significado.

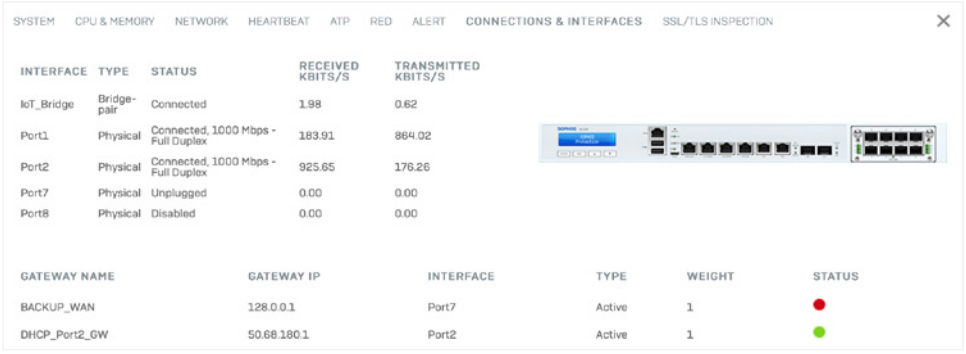
Fundamentalmente, el concepto de SD-WAN tiene que ver a menudo con lograr uno o más de estos cuatro objetivos en el contexto de las redes:

- **Reducción de los costes de conectividad:** las conexiones MPLS (conmutación de etiquetas multiprotocolo) tradicionales son caras, por lo que las organizaciones están pasándose a opciones WAN de banda ancha más asequibles como cable, DSL y 3G/4G/LTE.
- **Continuidad de la actividad:** las organizaciones requieren soluciones que proporcionen redundancia, enrutamiento, conmutación por error y conservación de las sesiones en caso de posibles fallos o interrupciones de la WAN.
- **Calidad de las aplicaciones críticas:** las organizaciones buscan visibilidad en tiempo real del tráfico y del rendimiento de las aplicaciones para mantener la calidad de las sesiones de las aplicaciones empresariales importantes.
- **Orquestación de VPN entre sucursales más sencilla:** la orquestación de VPN entre emplazamientos es a menudo compleja y lleva mucho tiempo, por lo que es imprescindible contar con herramientas que simplifiquen y automaticen la implementación y la configuración.

Sophos Firewall con SD-WAN de Xstream le permite alcanzar incluso sus objetivos de SD-WAN más ambiciosos de forma sencilla y asequible con un conjunto completo de opciones de orquestación, administración y optimización del rendimiento y la fiabilidad de SD-WAN.

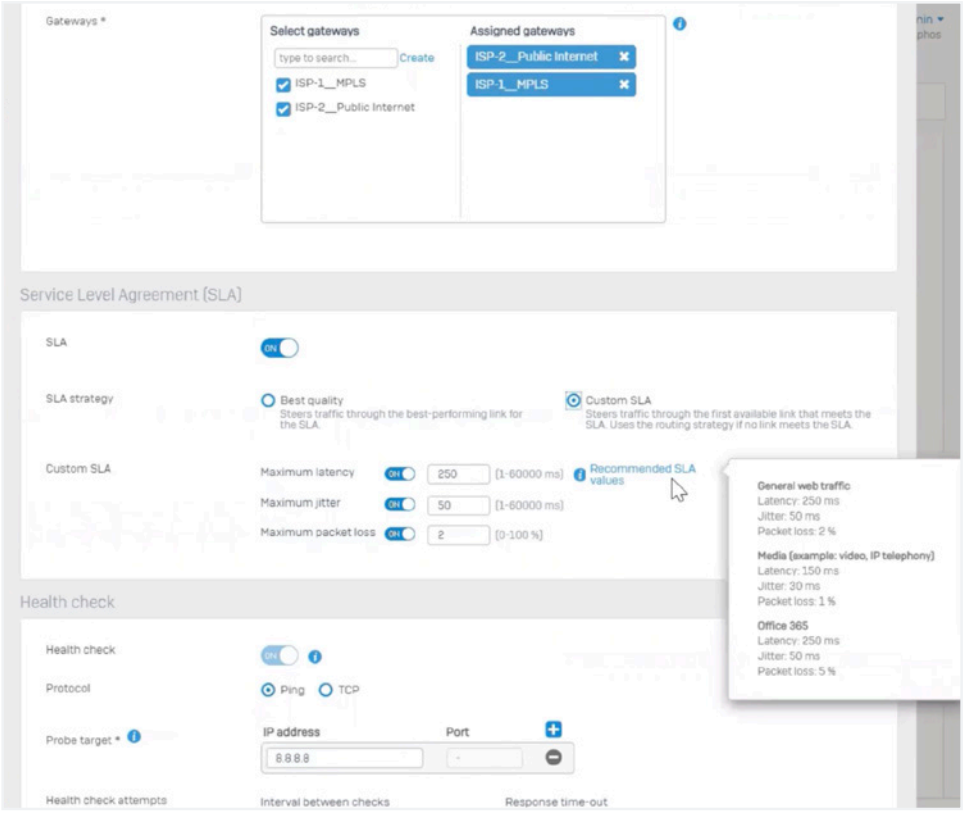
SD-WAN de Xstream

Gestionar el enrutamiento del tráfico de aplicaciones a través de varios enlaces WAN es un principio clave de SD-WAN, y Sophos Firewall con SD-WAN de Xstream ofrece una solución de administración de enlaces potente y flexible, independientemente de si utiliza varias conexiones MPLS, DSL, cable o móvil.



El estado de enlaces WAN se muestra en la parte inferior del widget de estado de la interfaz disponible a través del panel de control.

Los perfiles de SD-WAN definen una estrategia de enrutamiento a través de múltiples puertas de enlace WAN que permiten un reenrutamiento fluido y eficiente de las conexiones de las aplicaciones en función del rendimiento de enlaces WAN. Las transiciones entre enlaces se producen de forma instantánea con impacto nulo en las sesiones de las aplicaciones y sin interrupciones, lo que proporciona una continuidad y un rendimiento perfectos de las aplicaciones, y la mejor experiencia para el usuario final incluso en los entornos de ISP más problemáticos o inestables.



La configuración de perfiles de SD-WAN basados en el rendimiento es intuitiva y sencilla.

Las estrategias de enrutamiento de perfiles de SD-WAN pueden basarse en criterios de primer enlace disponible o de rendimiento. Los criterios de monitorización del rendimiento incluyen la latencia, fluctuación y pérdida de paquetes, y pueden utilizar múltiples destinos de sondeo para sondeos PING y TCP.

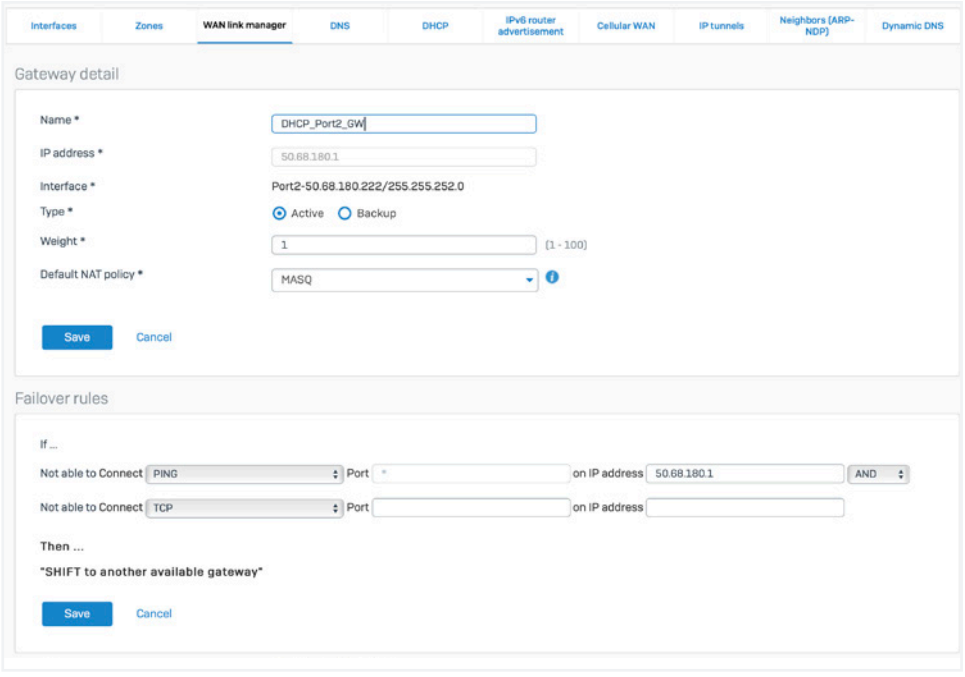
Los perfiles de SD-WAN pueden seleccionar automáticamente el mejor enlace en función del rendimiento o de acuerdo con sus políticas de SLA personalizadas que definen valores específicos para la fluctuación, latencia o pérdida de paquetes máximas aceptables antes de redirigir el tráfico a un enlace de mejor rendimiento sin afectar en absoluto a las conexiones activas.

Supervisar el rendimiento de su red SD-WAN es sencillo gracias a los gráficos históricos y en tiempo real de latencia, fluctuación y pérdida de paquetes. Los marcos temporales que pueden seleccionarse son tiempo real, las últimas 24 o 48 horas, o también la última semana o mes. También se incluye el registro avanzado del rendimiento y el enrutamiento de SD-WAN.

Monitorice el rendimiento de sus distintos enlaces WAN en tiempo real.

Aceleración FastPath de Xstream del tráfico VPN de SD-WAN

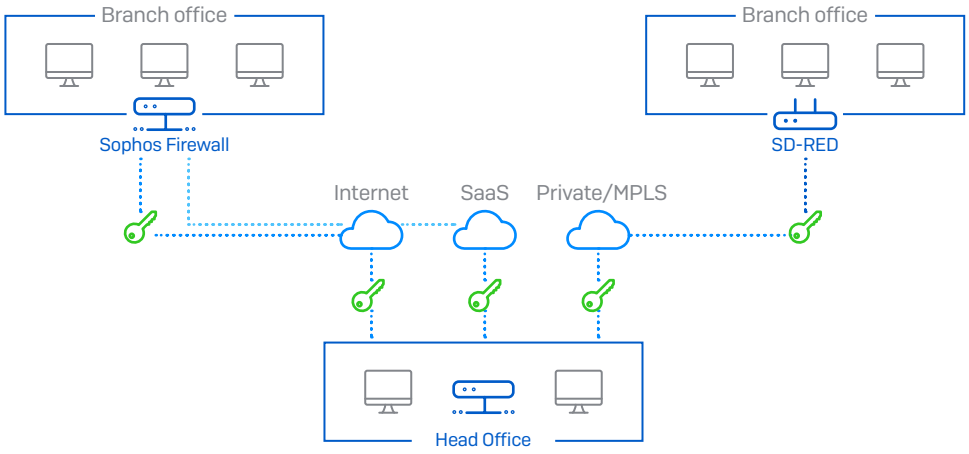
Sophos Firewall utiliza los procesadores de flujo Xstream integrados en los dispositivos de la serie XGS para ofrecer aceleración por hardware del tráfico de túnel VPN IPsec. Esto mejora drásticamente el rendimiento, ya que traslada al procesador de flujo Xstream algunos de los procesos intensivos de la CPU necesarios para los túneles IPsec, como la encapsulación o el cifrado y la desencapsulación o el descifrado por ESP (carga de seguridad de encapsulación). Esta nueva función aprovecha al máximo las capacidades criptográficas del hardware del procesador de flujo Xstream y tiene la ventaja añadida de liberar recursos de la CPU para otras tareas como la inspección detallada de paquetes del tráfico que lo necesite.
La aceleración FastPath de Xstream para el tráfico IPsec funciona tanto para el tráfico VPN de sitio a sitio como para el de acceso remoto.



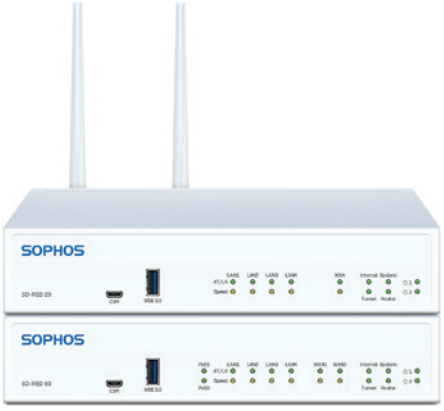
Administración de enlaces WAN de Sophos Firewall, incluyendo equilibrio y reglas de conmutación por error.

Conectividad de sucursales SD-Branch

En Sophos hemos sido pioneros en el área de la conectividad e implementación de sucursales sin necesidad de intervención con nuestros exclusivos dispositivos SD-RED. Estos dispositivos asequibles son sumamente fáciles de implementar para una persona sin conocimientos técnicos y proporcionan un túnel seguro y robusto de capa 2 entre el dispositivo y un firewall central.

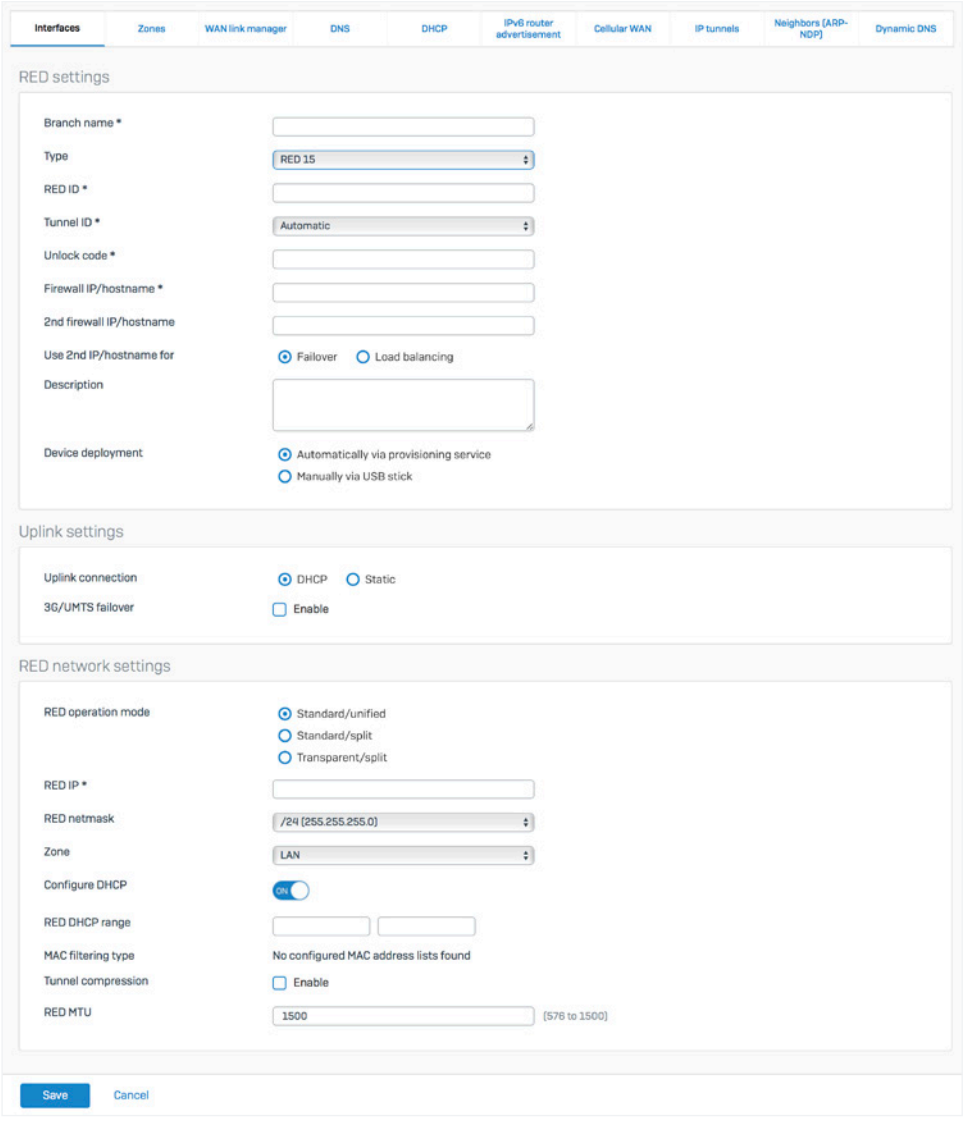


Sophos Firewall y los dispositivos SD-RED ofrecen opciones de túnel para conectar sucursales de forma sencilla y asequible a través de SD-WAN.



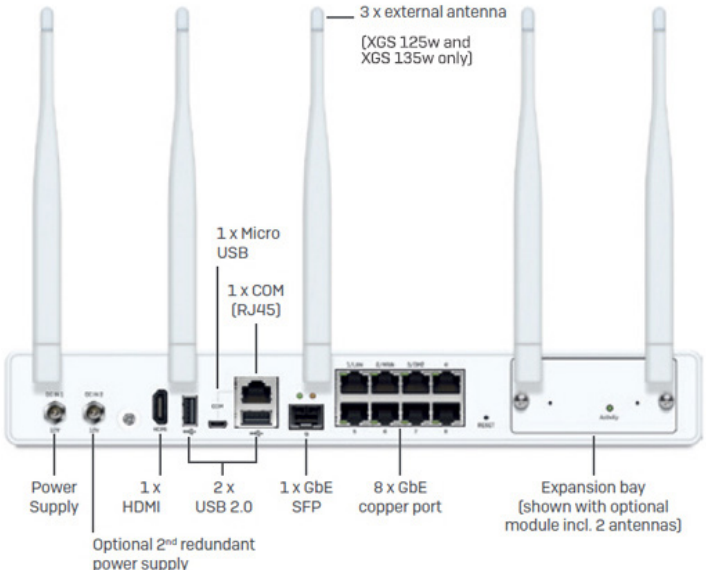
Los dispositivos SD-RED de Sophos ofrecen una solución asequible y sin necesidad de intervención para la conectividad SD-WAN de las sucursales.

Desplegar dispositivos SD-RED no podría ser más sencillo: basta con anotar el número de serie del dispositivo en el firewall y enviarlo a la ubicación remota. Cualquier persona sin conocimientos técnicos en la ubicación remota solo tiene que conectar el dispositivo y se pondrá en contacto con nuestro servicio de aprovisionamiento en la nube automáticamente para establecer una conexión segura de túnel con su dispositivo Sophos Firewall.



SD-RED de Sophos ofrece una solución de conectividad SD-WAN para sucursales flexible, segura y asequible.

Nuestros dispositivos de escritorio de la serie XGS también ofrecen excelentes soluciones de conectividad SD-WAN para sucursales con opciones flexibles de conectividad como VDSL y móvil, además de interfaces de cobre y fibra, y soporte para nuestros sólidos túneles SD-RED.

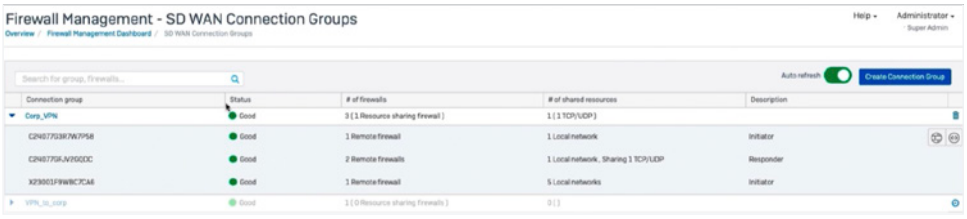


Algunos modelos de escritorio como el XGS 135w que se muestra aquí vienen con opciones de conectividad WAN LTE/móvil, VDSL, cobre o fibra.

Soporte y orquestación de VPN

Si alguna vez ha configurado varios túneles VPN entre diferentes firewalls, sabrá lo largo y tedioso que puede ser el proceso. Sophos Firewall admite la orquestación de SD-WAN en Sophos Central, lo que convierte la interconexión de múltiples túneles entre varios firewalls en una tarea rápida y sencilla.

Solo tiene que seleccionar los firewalls administrados que desea que participen en el grupo de conexión SD-WAN y, a continuación, seleccionar los recursos de red a los que desea que tenga acceso cada emplazamiento. Con solo pulsar un botón, verá cómo su red de superposición VPN SD-WAN cobra vida al crearse automáticamente todos los túneles y reglas de acceso de firewall necesarios, incluida la redundancia.



Desde Sophos Central, puede configurar rápidamente redes de superposición SD-WAN complejas y monitorizarlas.

Tanto si necesita una topología de red en malla completa como de concentrador y radio o de cualquier otro tipo, Sophos Central se encargará automáticamente de todas las configuraciones de túneles y firewall necesarias en el back-end para habilitar su red de superposición SD-WAN.

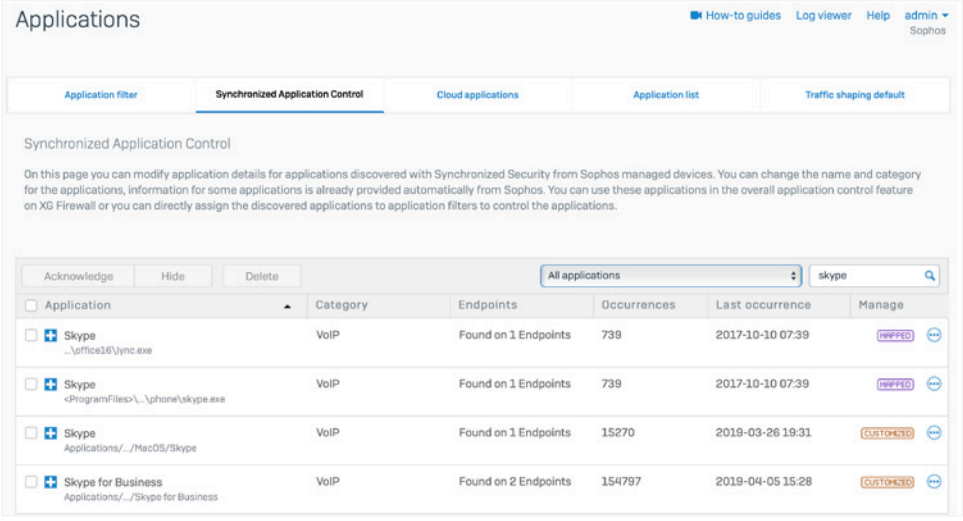
Por supuesto, Sophos Firewall admite todas las opciones estándar de VPN de sitio a sitio que cabe esperar, incluidas IPsec y SSL. Incluso ofrecemos nuestro propio y exclusivo túnel SD-RED de capa 2 con enrutamiento que es muy robusto y ha demostrado funcionar de manera fiable en situaciones de alta latencia tales como enlaces por satélite.

Visibilidad y enrutamiento de aplicaciones

Otra función importante para lograr objetivos de SD-WAN es la selección de rutas de aplicaciones y el enrutamiento para garantizar la calidad y minimizar la latencia para aplicaciones vitales como VoIP.

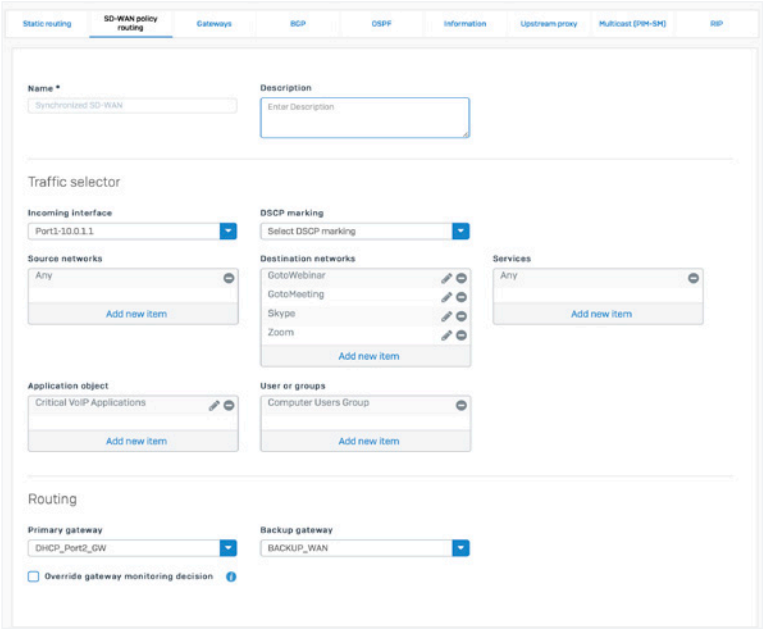
Por supuesto, no se puede enrutar lo que no se puede identificar, por lo que la identificación y visibilidad precisas y fiables de las aplicaciones son de vital importancia. Esta es un área en la que Sophos Firewall y la Seguridad Sincronizada de Sophos ofrecen una ventaja increíble. El Control de aplicaciones sincronizado ofrece un 100 % de claridad y visibilidad de todas las aplicaciones en red, lo que proporciona una ventaja significativa a la hora de identificar aplicaciones decisivas, especialmente aplicaciones oscuras o personalizadas.

La SD-WAN sincronizada, una función de Seguridad Sincronizada, ofrece ventajas adicionales con enrutamiento de aplicaciones de SD-WAN. La SD-WAN sincronizada se sirve de la claridad y fiabilidad adicionales de la identificación de aplicaciones que implica el uso compartido de la información del Control de aplicaciones sincronizado entre los endpoints administrados por Sophos y Sophos Firewall. Ahora, las aplicaciones anteriormente no identificadas también se pueden añadir a las políticas de enrutamiento de SD-WAN, lo que proporciona un nivel de control y fiabilidad del enrutamiento de aplicaciones que otros firewalls no pueden igualar.



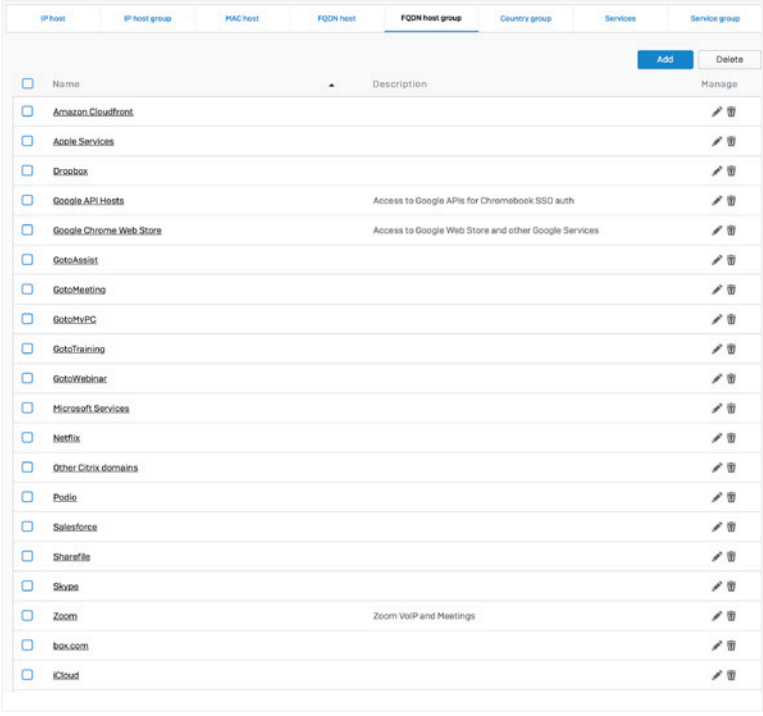
El Control de aplicaciones sincronizado identifica el 100 % de todas las aplicaciones en red, lo que facilita la priorización y enrutamiento de las aplicaciones importantes.

Sophos Firewall también permite el enrutamiento basado en aplicaciones y la selección de rutas en todas las reglas del firewall, incluido por usuario y grupo. Los controles granulares de enrutamiento basado en políticas (PBR) permiten definir el enrutamiento a través de la conexión WAN de puerta de enlace principal o de reserva y configurarse para la dirección de reproducción. Juntas, estas funciones permiten dirigir fácilmente el tráfico de aplicaciones importantes hacia la interfaz WAN óptima.



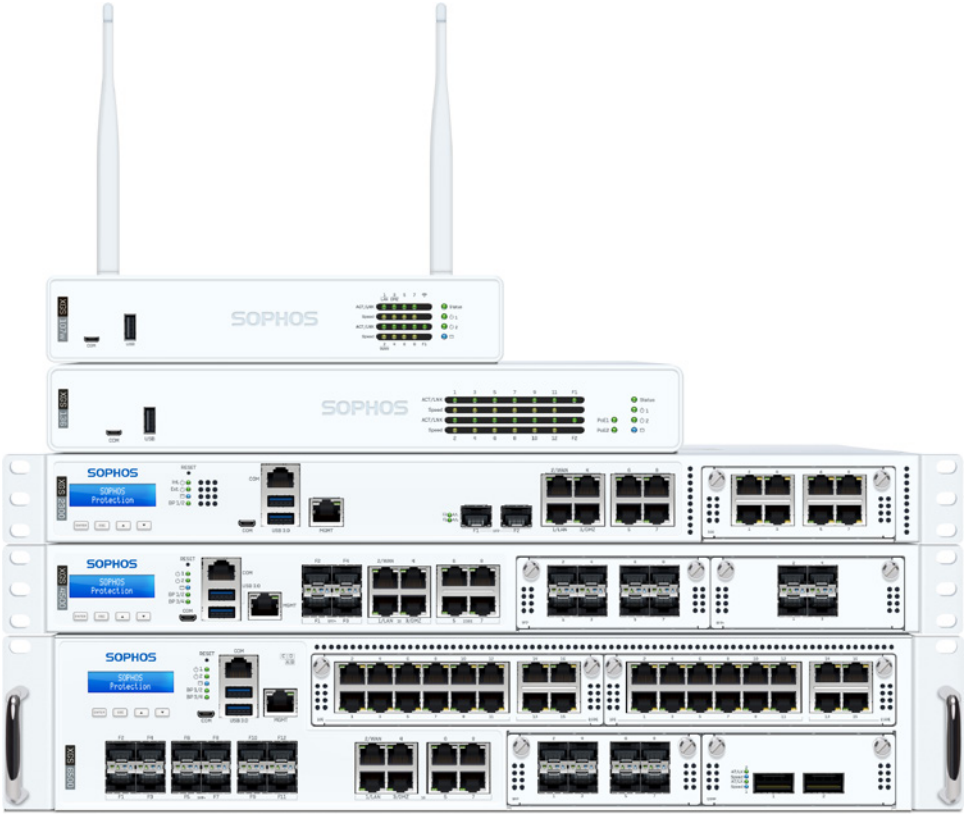
El enrutamiento basado en políticas de SD-WAN ofrece herramientas flexibles para enrutar el tráfico de aplicaciones críticas.

Sophos Firewall también incluye objetos de nombre de dominio completo (FQDN) predefinidos para servicios SaaS en la nube populares, con miles de definiciones de hosts FQDN incluidas para utilizar de inmediato y la opción de añadir más de forma sencilla.



Los objetos de host FQDN predefinidos que facilitan la selección de rutas y el enrutamiento basado en aplicaciones.

Añadir Sophos Firewall a cualquier red fácilmente



Los dispositivos de hardware de la serie Sophos Firewall ofrecen opciones de despliegue flexibles con puertos con derivación fail-open incluidos en todos los modelos 1U y disponibles en módulos FleXi Port para activar esta función también en nuestros dispositivos 2U. Los puertos con derivación permiten instalar Sophos Firewall en modo puente con los firewalls existentes. Si Sophos Firewall necesita apagarse o reiniciarse para actualizar el firmware, los puertos con derivación permiten la continuidad de la actividad al permitir que el tráfico siga fluyendo, lo que evita cualquier interrupción en la red. Esta función posibilita nuevas opciones de despliegue totalmente exentas de riesgos sin reemplazar ninguna infraestructura de red existente. Además, nuestra protección next-gen para endpoints, Intercept X, se ejecuta junto a cualquier producto antivirus para escritorio existente, lo que permite desplegar una solución completa de Seguridad Sincronizada de Sophos en cualquier red sin reemplazar nada.

Sophos Firewall: es ciberseguridad sin complicaciones.

Solicitud de precio

Solicite un presupuesto sin compromiso adaptado a sus necesidades en es.sophos.com/firewall-quote

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

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

30-03-22 ES (DD)