

Lista de funciones de Sophos Firewall

Sophos Firewall

Aspectos destacados

- ▶ La arquitectura Xstream proporciona niveles increíbles de visibilidad, protección y rendimiento a través del procesamiento de paquetes basado en el flujo
- ▶ La inspección TLS de Xstream ofrece un alto rendimiento, compatibilidad con TLS 1.3 sin repercutir en el rendimiento, no depende de ningún puerto, políticas de nivel empresarial con excepciones predefinidas, visibilidad única del panel de control y solución de problemas de compatibilidad
- ▶ El motor DPI de Xstream proporciona protección del escaneo de transmisiones para IPS, AV, web, control de apps e inspección TLS en un único motor de alto rendimiento
- ▶ FastPath del flujo de red de Xstream ofrece automáticamente aceleración inteligente y basada en políticas del tráfico de confianza
- ▶ SD-WAN de Xstream ofrece selección de enlaces basada en el rendimiento con un reenrutamiento sin impacto, monitorización de SD-WAN, herramientas de orquestación SD-WAN multisitio y aceleración FastPath del tráfico de túnel VPN IPsec
- ▶ La interfaz de usuario diseñada específicamente con centro de control interactivo utiliza indicadores tipo semáforo (rojo, amarillo, verde) para identificar al instante y rápidamente qué necesita atención
- ▶ El Centro de control ofrece información instantánea sobre el estado de seguridad de los endpoints, aplicaciones de Mac y Windows no identificadas, aplicaciones en la nube y TI en la sombra, cargas sospechosas, usuarios de riesgo, amenazas avanzadas, ataques de red, sitios web objetables y mucho más
- ▶ Navegación optimizada en dos clics a cualquier lugar con búsqueda inteligente
- ▶ El widget del Centro de control de políticas supervisa la actividad política de las políticas empresariales, de usuario y de red y realiza un seguimiento de las políticas no utilizadas, desactivadas, modificadas y nuevas
- ▶ El modelo de políticas unificadas combina todas las reglas de inspección de firewall, NAT y TLS en una sola pantalla con opciones de agrupación, filtrado y búsqueda
- ▶ Administración de reglas de firewall optimizada para grandes conjuntos de reglas con agrupación automática y manual personalizada, además de una función que proporciona información al pasar por encima el ratón e indicadores de aplicación
- ▶ Todas las reglas de firewall proporcionan un resumen rápido de la seguridad y el control aplicados para AV, espacios seguros, IPS, web, app, conformado de tráfico (QoS) y Heartbeat
- ▶ Las políticas de IPS, web, app, TLS y conformado de tráfico (QoS) predefinidas permiten una configuración rápida y una personalización sencilla para escenarios de despliegue comunes (por ejemplo, la CIPA, políticas típicas del lugar de trabajo y más)
- ▶ Sophos Security Heartbeat™ conecta los endpoints de Sophos con el firewall para compartir el estado de la seguridad y la telemetría, permitiendo la identificación instantánea de endpoints poco seguros o en peligro
- ▶ La respuesta a amenazas activas identifica, bloquea y responde automáticamente a los adversarios activos de feeds de amenazas proporcionadas por SophosLabs, analistas de MDR o terceros
- ▶ El Control de aplicaciones sincronizado identifica, clasifica y activa automáticamente el control de todas las aplicaciones de Mac/Windows desconocidas en la red
- ▶ La visibilidad de aplicaciones en la nube permite la detección instantánea de TI en la sombra y ofrece conformado de tráfico con un solo clic
- ▶ La herramienta del simulador de pruebas de políticas permite simular y probar reglas de firewall y políticas web por usuario, IP y hora del día
- ▶ Los principios de la iniciativa "Diseñado para la máxima seguridad" garantizan que se refuerce el firewall contra ataques

- API de configuración para todas las funciones de integración de RMM/PSA
- La integración de NDR basada en la nube mejora la detección de adversarios activos
- La puerta de enlace ZTNA integrada en cada firewall asegura un acceso sencillo a las aplicaciones desde cualquier lugar
- La gestión y generación de informes basada en la nube de Sophos Central permite la administración de políticas de grupo y una consola para todos sus productos de seguridad de TI de Sophos
- El asistente de configuración optimizado y fácil de usar permite un despliegue rápido listo para usar en tan solo unos minutos
- Despliegue Zero Touch y configuración en Sophos Central para nuevos firewalls
- Integración perfecta con Sophos MDR y XDR
- Portal de autoservicio de usuarios
- Seguimiento de cambios de configuraciones
- Control flexible de acceso de dispositivos para servicios por zonas
- Opciones de notificación de capturas SNMP o correo electrónico
- SNMP v3 (incluida supervisión de hardware) y monitorización de Netflow/sFlow
- Soporte de administración centralizada a través de Sophos Central (disponible solo para clientes con soporte válido)
- Configuraciones de copia de seguridad y restauración: localmente, a través de FTP o correo electrónico; bajo demanda, diariamente, semanalmente o mensualmente, con la opción de volver a asignar puertos al actualizar los dispositivos de hardware
- Compatibilidad con los certificados de Let's Encrypt para WAF, SMTP, configuración TLS, inicio de sesión de zonas Wi-Fi, la consola de administración web, portal de usuario, portal cautivo, portal VPN y portal SPX
- API para la integración de terceros
- Cambio de nombre de interfaz
- Opción de acceso remoto para el soporte de Sophos
- Administración de licencias basada en la nube desde MySophos

Base Firewall

Administración general

- Gestión de reglas de firewall e interfaz de usuario optimizada y diseñada específicamente para grandes conjuntos de reglas con agrupación con una función que ofrece una vista rápida de las reglas e indicadores de aplicación
- Autenticación de doble factor (contraseña de un solo uso) para acceso del administrador, portal de usuario, IPsec, VPN SSL y WAF
- Herramientas avanzadas de registro y solución de problemas en la de usuario (por ejemplo, captura de paquetes)
- Soporte para alta disponibilidad (HA) para agrupar dos dispositivos en modo activo-activo o activo-pasivo con configuración rápida de HA plug-and-play compatible con múltiples enlaces de sincronización redundantes
- Interfaz de línea de comandos (CLI) completa accesible desde la interfaz de usuario
- Administración basada en roles con integración de Azure AD para inicio de sesión único
- Actualizaciones de firmware a través de SSL con anclaje de certificados para máxima seguridad
- Definiciones reutilizables de objetos del sistema que admiten búsquedas para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores

Firewall, conexión en red y enrutamiento

- Firewall de inspección dinámica y detallada de paquetes
- La arquitectura de procesamiento de paquetes Xstream proporciona niveles increíbles de visibilidad, protección y rendimiento a través del procesamiento de paquetes basado en el flujo
- Inspección TLS de Xstream de alto rendimiento, compatibilidad con TLS 1.3 sin repercutir en el rendimiento, no depende de ningún puerto, políticas de nivel empresarial, visibilidad única del panel de control y solución de problemas de compatibilidad
- El motor DPI de Xstream proporciona protección del escaneado de transmisiones para IPS, AV, web, control de apps e inspección TLS en un único motor de alto rendimiento
- FastPath del flujo de red de Xstream ofrece automáticamente aceleración inteligente y basada en políticas del tráfico de confianza, tráfico VPN IPsec y tráfico cifrado por TLS

- › Políticas basadas en usuarios, grupos, horas o redes
- › Políticas de tiempo de acceso por usuario/grupo
- › Aplicación de política entre zonas, redes o por tipo de servicio
- › Soporte para políticas de aislamiento de zonas y basadas en zonas
- › Zonas predeterminadas para LAN, WAN, DMZ, LOCAL, VPN y Wi-Fi
- › Zonas personalizadas en LAN o DMZ
- › Políticas NAT personalizables con enmascaramiento de IP y compatibilidad completa de objetos para redirigir o reenviar múltiples servicios en una sola regla con un práctico asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas en solo unos clics
- › Definiciones de objetos de red reutilizables para todas las reglas con búsqueda inteligente y global de texto libre
- › Protección contra floodings: Bloqueo de ataques de denegación de servicio y denegación de servicio distribuido, y exploración de puertos
- › Bloqueo de países por IP geográficas
- › Enrutamiento: estático, multidifusión (PIM-SM) y dinámico: RIP, BGP, OSPFv3 (IPv6) BGPv6
- › Clonación, activación o desactivación de rutas estáticas, redistribución de rutas BGP dinámicas en OSPFv3, uso de opciones de Blackhole route (ruta Blackhole) y uso de enrutamiento multirruta de igual coste (ECMP) para equilibrio de carga
- › Compatibilidad de proxy de subida
- › Enrutamiento de multidifusión independiente del protocolo con inspección IGMP
- › Puentes compatibles con STP y reenvío de emisiones de ARP
- › Compatibilidad y etiquetado de DHCP para VLAN
- › Compatibilidad de puente VLAN
- › Compatibilidad de trama gigante
- › Activación/desactivación de interfaces físicas
- › Compatibilidad de WAN inalámbrica (n/a en despliegues virtuales)
- › Agregación de enlaces de interfaces 802.3ad
- › Configuración total de DNS, DHCP y NTP

- › DNS dinámico (DDNS)
- › Certificación de aprobación del programa con logotipo "IPv6 Ready"
- › Delegación de prefijo DHCP de IPv6
- › Compatibilidad con túneles IPv6 incluido despliegue rápido de 6in4, 6to4, 4in6 e IPv6 (6rd) a través de IPsec

SD-WAN de Xstream

- › Los perfiles SD-WAN de Xstream admiten múltiples opciones de enlaces WAN, como VDSL, DSL, cable, LTE/móvil y MPLS
- › Los SLA basados en el rendimiento seleccionan automáticamente el mejor enlace WAN en función de la fluctuación, la latencia o la pérdida de paquetes
- › Equilibrio de carga de SD-WAN en múltiples enlaces SD-WAN usando estrategias de ponderación o persistencia de la sesión de Round Robin
- › El reenrutamiento sin impacto mantiene las sesiones de las aplicaciones cuando el rendimiento del enlace cae por debajo de los umbrales y se realiza una transición a un enlace WAN que ofrezca un mejor rendimiento
- › Los gráficos de monitorización de SD-WAN proporcionan información en tiempo real sobre latencia, fluctuación y pérdida de paquetes para todos los enlaces WAN
- › Aceleración FastPath de Xstream del tráfico de túnel Ipsec en SD- WAN
- › La SD-WAN sincronizada, una función de Seguridad 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.
- › Enrutamiento de aplicaciones sobre enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas
- › Soporte VPN robusto, incluidos IPsec y VPN SSL
- › Túnel RED de capa 2 único con enrutamiento

Conformado de tráfico base y cuotas

- › Conformado de tráfico (QoS) flexible basado en red o usuario (opciones mejoradas de conformado de tráfico web y de aplicaciones incluidas con la suscripción a Protección web)
- › Establecimiento de cuotas de tráfico basadas en usuario en la carga/descarga o tráfico total y cíclico o no cíclico

- › Optimización VoIP en tiempo real

- › Marcado DSCP

Conexión inalámbrica segura

- › Sencillo despliegue plug-and-play de puntos de acceso inalámbricos de Sophos (solo serie APX); se muestran automáticamente en el centro de control del firewall
- › Supervisión y administración centralizada de todos los puntos de acceso y clientes inalámbricos a través del controlador inalámbrico integrado
- › Creación de puentes entre los puntos de acceso y LAN, VLAN o una zona separada, con opciones de aislamiento de cliente
- › Soporte para múltiples SSID por radio, incluidos SSID ocultos
- › Soporte para diversos estándares de seguridad y cifrado incluidos WPA2 Personal y Enterprise
- › Opción de selección de ancho de canal
- › Compatible con IEEE 802.1X (autenticación RADIUS) con soporte para servidor primario y secundario
- › Soporte para 802.11r (transición rápida)
- › Soporte para puntos de acceso para cupones (personalizados), contraseña del día o aceptación de términos y condiciones
- › Acceso inalámbrico a Internet para invitados con opciones de jardín vallado
- › Acceso por tiempo a la red inalámbrica
- › Modo de red en malla de puentes y repetidores inalámbricos con puntos de acceso compatibles
- › Optimización en segundo plano de selección automática de canales
- › Compatibilidad con inicio de sesión HTTPS

Autenticación

- › El ID de usuario sincronizado utiliza la Seguridad Sincronizada para compartir el ID de usuario de Active Directory con sesión iniciada actualmente entre los endpoints de Sophos y el firewall sin un agente en el servidor o cliente de AD
- › Autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS+
- › Agentes de autenticación de servidores para Active Directory SSO, STAS, SATC

- › Inicio de sesión único: Active Directory, eDirectory, auditoría de RADIUS

- › Inicio de sesión único de Azure AD para acceso del administrador a la consola de Webadmin

- › Inicio de sesión único de Azure AD para que los usuarios se autenticuen para acceder a la web a través del portal cautivo

- › SSO de AD transparente con aplicación de HSTS, lo que permite enlaces de Kerberos y NTLM a través de HTTP o HTTPS

- › Importación de grupos de Azure AD y compatibilidad con RBAC

- › Agentes de autenticación de clientes para Windows, Mac OS X, Linux 32/64

- › Autenticación SSO del navegador: Autenticación proxy transparente (NTLM) y Kerberos

- › Portal cautivo de navegador

- › Certificados de autenticación para iOS y Android

- › Servicios de autenticación para IPsec, SSL, L2TP, PPTP

- › Soporte para autenticación de Chromebooks de Google para entornos con Active Directory y G Suite de Google

- › Integración de Google Workspace a través del cliente LDAP con SSO de Chromebooks de Google

- › Autenticación basada en API

Portales de autoservicio para usuarios y VPN

- › SNMP v3 (incluida supervisión de hardware) y monitorización de Netflow/sFlow

- › Descarga de cliente de autenticación de Sophos

- › Descarga de cliente de acceso remoto SSL (Windows) y archivos de configuración (otros sistemas operativos)

- › Información de acceso a puntos inalámbricos

- › Cambio de nombre de usuario y contraseña

- › Visualización de uso de personal de Internet

- › Acceso a mensajes en cuarentena y administración de listas blancas/negras de remitentes basadas en el usuario (requiere Protección del correo electrónico)

Opciones de VPN base

- › VPN de sitio a sitio: SSL, IPsec, AES/3DES de 256 bits, PFS, RSA, certificados X.509, clave compartida previamente

- Túnel de VPN de sitio a sitio RED de Sophos (robusto y ligero)
- Aceleración FastPath de Xstream para tráfico de túnel IPsec (tanto para el de sitio a sitio como para el de acceso remoto)
- Herramientas de importación, supervisión y administración de AWS VPC
- L2TP y PPTP
- VPN basada en enrutamiento con selectores de tráfico
- Acceso remoto: Compatible con clientes VPN de SSL, IPsec, iPhone/iPad/Cisco/Android
- Compatible con IKEv2
- Conexión IPsec dinámica con conmutación por error HA para RBVPN, PBVPN y VPN de acceso remoto sin pérdida de sesión en escenarios de conmutación por error HA
- Monitorización de estado de túnel VPN de IPsec a través de SNMP
- Soporte IPsec avanzado para PSK y grupos DH 27-30 / RFC6954 únicos
- Cliente SSL para Windows y descarga de configuración a través del portal de usuario

Cliente de Sophos Connect

- Autenticación: Clave previamente compartida (PSK), PKI (X.509), token y XAUTH
- Admite inicio de sesión único de Entra ID (Azure AD)
- Permite Seguridad sincronizada y Security Heartbeat para usuarios remotos conectados
- Túneles divididos inteligentes para conseguir un enrutamiento óptimo del tráfico
- Compatibilidad de cruce NAT
- Resumen gráfico del estado de las conexiones gracias al monitor de clientes
- Soporte para clientes Mac (IPsec) y Windows (SSL/IPsec)

Protección de redes

Prevención de intrusiones (IPS)

- Motor de inspección detallada de paquetes IPS Next-Gen de alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre una base de reglas de firewall para conseguir el máximo rendimiento y protección
- Miles de firmas

- Selección de categorías granular
- Soporte para firmas IPS personalizadas
- Filtros inteligentes de políticas IPS que permiten políticas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones

Respuesta a amenazas activas y Security Heartbeat™

- La respuesta a amenazas activas supervisa/bloquea automáticamente APT y otras amenazas identificadas a través de los feeds de amenazas de Sophos X-Ops para protección contra amenazas avanzadas de bots y adversarios activos que intentan contactar con destinos maliciosos mediante detecciones de DNS, AFC y firewall multicapa
- La respuesta a amenazas activas supervisa/bloquea automáticamente las amenazas identificadas por los feeds de amenazas de MDR/XDR publicados por un analista del SOC de Sophos o del cliente/Partner al combinar Sophos Firewall con Xstream Protection con Sophos MDR/XDR
- La respuesta a amenazas activas supervisa/bloquea automáticamente feeds de amenazas de terceros de fuentes de información de amenazas industriales, verticales o regionales con Xstream Protection
- La Seguridad Sincronizada con Security Heartbeat de Sophos marca instantáneamente con un estado de Heartbeat rojo los dispositivos comprometidos que intentan contactar con cualquier indicador de amenaza identificado por la respuesta a amenazas activas y sus feeds de amenazas relacionados. El estado de Heartbeat también lo supervisan los endpoints gestionados por Sophos y se comparte con el firewall, incluyendo detalles tales como host, usuario, proceso, recuento de incidentes y momento del incidente
- Las condiciones de Sophos Security Heartbeat se pueden adjuntar a cualquier regla de firewall, limitando automáticamente el acceso a los recursos y segmentos de red de un dispositivo que se haya visto comprometido hasta que se limpie
- Sophos Firewall también inicia automáticamente la protección contra el movimiento lateral en caso de que un endpoint gestionado se vea comprometido informando a todos los endpoints en buen estado gestionados por Sophos para que rechacen el tráfico desde el dispositivo comprometido bloqueando efectivamente el dispositivo, incluso en el mismo segmento de la LAN

Gestión de dispositivos SD-RED

- Administración centralizada de todos los dispositivos SD-RED

- ▶ Sin configuraciones: Se conecta de forma automática mediante un servicio de aprovisionamiento basado en la nube
- ▶ Túnel cifrado protegido con certificados X.509 digitales cifrado AES de 256 bits
- ▶ Ethernet virtual para transferencias fiables de todo el tráfico entre ubicaciones
- ▶ Administración de direcciones IP con configuración de servidores DNS y DHCP definida de forma central
- ▶ Desautorización remota de dispositivos SD-WAN tras el período elegido de inactividad
- ▶ Compresión del tráfico de túneles
- ▶ Opciones de configuración de puertos de VLAN

VPN sin cliente

- ▶ Portal de autoservicio HTML5 cifrado único de Sophos compatible con RDP, SSH, Telnet y VNC

Protección web

Control y protección web

- ▶ Protección web de DPI de transmisión o inspección en modo proxy explícito
- ▶ El modo proxy explícito admite autenticación por conexión para múltiples usuarios en la misma IP de origen
- ▶ Protección mejorada contra amenazas avanzadas
- ▶ Base de datos de filtros de URL con millones de sitios en 92 categorías con el respaldo de SophosLabs
- ▶ Políticas de cuotas de navegación basadas en el tiempo por usuario/grupo
- ▶ Políticas de tiempo de acceso por usuario/grupo
- ▶ Escaneado de malware: bloquea todas las formas de virus, malware de Internet, troyanos y spyware en HTTP/S, FTP y correo electrónico basado en web
- ▶ Protección contra malware de Internet avanzado con simulación de JavaScript
- ▶ Búsquedas de Live Protection en tiempo real en la nube con la información más reciente sobre amenazas
- ▶ Segundo motor de detección independiente de malware (Avira) para escaneado dual
- ▶ Escaneado en tiempo real o en modo de lotes
- ▶ Protección contra pharming

- ▶ Aplicación de restricciones de inquilino para O365
- ▶ Detección y aplicación de túnel de protocolo SSL
- ▶ Validación del certificado
- ▶ Copia en caché de contenido web de alto rendimiento
- ▶ Forzar caché para actualizaciones de Sophos Endpoint
- ▶ Filtrado de tipos de archivo por tipo MIME, extensión y tipos de contenido activo (por ejemplo, ActiveX, applets, cookies, etc.)
- ▶ Aplicación de YouTube for Schools por política (usuario/grupo)
- ▶ Aplicación de SafeSearch (basado en DNS) para los principales motores de búsqueda por política (usuario/grupo)
- ▶ Supervisión y aplicación de palabras clave web para registrar, notificar o bloquear contenido web que coincida con listas de palabras clave con la opción de cargar listas personalizadas
- ▶ Bloqueo de aplicaciones no deseadas (PUA)
- ▶ Opción de anulación de políticas web para que profesores o personal permitan temporalmente el acceso a sitios o categorías bloqueadas que usuarios seleccionados puedan personalizar o gestionar en su totalidad
- ▶ Alertas instantáneas para cualquier usuario que navegue por una categoría web restringida (con una frecuencia de hasta cada 5 minutos)

Visibilidad de aplicaciones en la nube

- ▶ El widget del Centro de control muestra la cantidad de datos cargados y descargados en aplicaciones de la nube clasificadas como nuevas, autorizadas, no autorizadas o toleradas
- ▶ Detección rápida de IT en la sombra
- ▶ Desglose de información para obtener detalles sobre usuarios, tráfico y datos
- ▶ Acceso con un solo clic a las políticas de conformado de tráfico
- ▶ Filtrado de uso de aplicaciones en la nube por categoría o volumen
- ▶ Informe detallado y personalizable sobre el uso de aplicaciones en la nube para obtener informes completos históricos

Protección y control de aplicaciones

- Control de aplicaciones sincronizado para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas de Windows y Mac en la red mediante el intercambio de información entre endpoints gestionados por Sophos y el firewall
- Control de aplicaciones basado en firmas con patrones para miles de aplicaciones
- Visibilidad y control de aplicaciones en la nube para descubrir IT en la sombra
- Filtros inteligentes de control de aplicaciones que permiten políticas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones
- Descubrimiento y control de microaplicaciones
- Control de aplicaciones basado en categoría, características (por ejemplo, consumo de ancho de banda y productividad), tecnología (por ejemplo, P2P) y nivel de riesgo
- Aplicación de políticas de control de aplicaciones por usuario o por regla de red

Conformado de tráfico web y de aplicaciones (Web and App Traffic Shaping)

- Opciones de conformado de tráfico avanzado (QoS) por categoría web o aplicaciones para limitar o garantizar la prioridad de las cargas/descargas o del tráfico total y la velocidad de forma individual o compartida.

DNS Protection

Servicio DNS basado en la nube

- Servicio de resolución del nombre de dominio
- Servicio DNS basado en la nube de alto rendimiento
- Con el respaldo de SophosLabs y tecnología de IA
- Bloqueo de URL maliciosas en la búsqueda DNS
- Controles granulares de cumplimiento para bloquear sitios web no deseados por categoría
- Administrado desde Sophos Central

NDR Essentials

Network Detection and Response

- NDR basada en la nube
- Con la tecnología de IA
- Detecta comunicaciones cifradas de amenazas sin

descifrado TLS

- Detecta algoritmos de generación de dominios
- Asigna puntuaciones a las amenazas potenciales y alerta sobre cualquier amenaza que supere el umbral establecido
- Compatibilidad completa con generación de informes y registro

Protección de día cero

Análisis dinámico de espacio seguro

- Integración completa en el panel de control de su solución de seguridad de Sophos
- Inspección de ejecutables y documentos que contienen contenido ejecutable (incluidos archivos con las extensiones .exe, .com y .dll, .doc, .docx, .docm, .rtf y PDF) y archivos comprimidos que contengan cualquiera de los tipos de archivo anteriores (incluidos ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z y Microsoft Cabinet)
- Análisis agresivo de comportamiento, red y memoria
- Detecta comportamientos de evasión del espacio seguro
- Tecnología de Machine Learning con Deep Learning que escanea todos los archivos ejecutables soltados
- Incluye tecnología de prevención de exploits y CryptoGuard de Sophos Intercept X
- Informes detallados de archivos maliciosos con capturas de pantalla y capacidad de liberar archivos desde el panel de control
- Selección opcional del centro de datos y opciones de políticas de grupos y usuarios flexibles para el tipo de archivo, exclusiones y acciones sobre el análisis
- Admite enlaces de descarga de un solo uso

Análisis estático de información sobre amenazas

- Todos los archivos que contienen código activo descargados a través de la web o que llegan al firewall como archivos adjuntos de correo electrónico como, por ejemplo, archivos ejecutables y documentos con contenido ejecutable (incluidos archivos con la extensión .exe, .com y .dll, .doc, .docx, .docm, .rtf y PDF), así como los archivos comprimidos que contengan cualquiera de los tipos anteriores (incluidos ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z y Microsoft Cabinet), se envían automáticamente para análisis de información sobre amenazas

- ▶ Los archivos se comprueban en relación con la amplia base de datos de información sobre amenazas de SophosLabs y se someten a múltiples modelos de Machine Learning para identificar malware nuevo y desconocido
- ▶ Los informes exhaustivos incluyen un widget del panel de control para los archivos analizados, una lista detallada de los archivos que se han analizado y los resultados, y un informe detallado en el que se describe el resultado de cada modelo de Machine Learning

Orquestación en Central

Orquestación de SD-WAN

- ▶ Orquestación de SD-WAN y VPN con creación sencilla y automatizada mediante asistente de túneles de VPN de sitio a sitio entre ubicaciones de red utilizando una arquitectura óptima (concentrador, malla completa o una combinación)
- ▶ Compatible con túneles de VPN IPsec, SSL o RED Se integra a la perfección con funciones de SD-WAN para la priorización de aplicaciones, la optimización del enrutamiento y el aprovechamiento de múltiples enlaces WAN para garantizar resiliencia y rendimiento

Central Firewall Reporting Advanced

- ▶ Almacenamiento de datos en la nube durante 30 días para informes históricos del firewall con funciones avanzadas para guardar, programar y exportar informes personalizados

Integración con XDR y MDR

- ▶ Integración con Sophos XDR y MDR para proporcionar telemetría e información sobre amenazas con el fin de realizar búsquedas y análisis de amenazas
- ▶ La respuesta a amenazas activas de Sophos utiliza feeds de amenazas de los analistas de MDR y XDR para identificar, bloquear y aislar automáticamente las amenazas activas en la red
- ▶ La telemetría de indicadores de peligro (IoC) de Seguridad Sincronizada recopila información importante sobre cualquier amenaza, usuario, proceso y dispositivo que se haya visto comprometido

Protección del correo electrónico

Protección y control del correo electrónico

- ▶ Escaneado del correo electrónico con compatibilidad para SMTP, POP3 e IMAP.
- ▶ Servicio de reputación con supervisión de brechas de spam basada en tecnología patentada de detección de patrones recurrentes
- ▶ Bloqueo de spam y malware durante la transacción SMTP

- ▶ Protección antispam mediante DKIM y BATV
- ▶ Protección basada en listas de rechazo de spam y Sender Policy Framework (SPF).
- ▶ Verificación de destinatarios para direcciones de correo mal escritas
- ▶ Segundo motor de detección independiente de malware (Avira) para escaneado dual
- ▶ Búsquedas de Live Protection en tiempo real en la nube con la información más reciente sobre amenazas
- ▶ Actualizaciones automáticas de patrones y firmas
- ▶ Compatibilidad con host inteligente para retransmisión saliente
- ▶ Detección, bloqueo y escaneado de tipos de archivo en los archivos adjuntos
- ▶ Aceptación, rechazo o descarte de mensajes de gran tamaño
- ▶ Detecta direcciones web de suplantación de identidades en mensajes de correo electrónico
- ▶ Uso de reglas de escaneado de contenido predefinidas o creación de sus propias reglas personalizadas basadas en diversos criterios con opciones granulares de políticas y excepciones
- ▶ Compatibilidad con cifrado TLS para SMTP, POP e IMAP
- ▶ Adición automática de firma en todos los mensajes salientes
- ▶ Archivador de correo electrónico
- ▶ Listas negras y blancas de remitentes basadas en usuarios, individuales y gestionadas a través del portal del usuario

Gestión de cuarentena de Sophos Email

- ▶ Resumen de cuarentena de spam y opciones de notificaciones
- ▶ Cuarentenas de malware y spam con opciones de búsqueda y filtrado por fecha, remitente, destinatario, asunto y motivo, con posibilidad de liberar y eliminar mensajes
- ▶ Portal de autoservicio para que el usuario pueda ver y liberar mensajes en cuarentena

Cifrado del correo electrónico y DLP

- ▶ Cifrado de SPX (pendiente de patente) de mensajes de sentido único
- ▶ Autoregistro de destinatarios para la gestión de contraseñas de SPX
- ▶ Adición de archivos adjuntos a respuestas seguras de SPX
- ▶ Totalmente transparente, sin necesidad de software ni clientes adicionales

- › Motor de DLP con escaneo automático de mensajes de correo electrónico y adjuntos para detectar datos delicados
- › Listas de control del contenido (CCL) con tipos de datos delicados predefinidos para PII, PCI, HIPAA, entre otros, actualizadas por SophosLabs

Protección de servidores web

Protección firewall de aplicación web

- › Servidor proxy inverso
- › Motor de refuerzo de URL con enlaces profundos y prevención de cruces de directorios
- › Motor de form hardening
- › Protección contra inyección SQL
- › Protección anti cross-site scripting
- › Motores antivirus duales (Sophos y Avira)
- › Descarga de cifrado de HTTPS (TLS/SSL)
- › Firma digital de cookies
- › Enrutamiento basado en rutas
- › Aplicación de la política de rangos IP geográficos
- › Configuración personalizada de cifrado y aplicación de la versión TLS
- › Aplicación de HSTS y X-Content-Type-Options
- › Compatible con el protocolo Outlook en cualquier lugar
- › Autenticación inversa (descarga) básica y basada en formularios para acceder a servidores
- › Abstracción de servidor virtual y servidor físico
- › El equilibrio de carga integrado distribuye todos los visitantes entre los distintos servidores
- › Anulación granular de comprobaciones individuales según las necesidades
- › Cumplimiento de solicitudes de redes de origen o direcciones web de destino especificadas
- › Compatibilidad con operadores y lógica
- › Contribuye a la compatibilidad con diferentes configuraciones y despliegues no estándar
- › Opciones para modificar los parámetros de rendimiento del firewall de aplicaciones web
- › Opción de límite de tamaño de análisis
- › Permiso/bloqueo de rangos de direcciones IP
- › Compatibilidad con comodines para rutas y dominios de servidores
- › Adición automática de un prefijo/sufijo para autenticación

Informes y registros

Central Firewall Reporting

- › Opciones de informes predefinidos con personalización flexible
- › Informes para dispositivos de Sophos Firewall: hardware, software, virtuales y en la nube
- › Interfaz de usuario intuitiva que ofrece una representación gráfica de los datos
- › El panel de control de informes proporciona una vista rápida de los eventos de las últimas 24 horas
- › Identificación sencilla de actividades de red, tendencias y posibles ataques
- › Copia de seguridad de registros fácil con una rápida recuperación para necesidades de auditoría
- › Despliegue simplificado sin necesidad de conocimientos técnicos

Central Firewall Reporting Advanced

- › Informes agregados multifirewall
- › Guardar plantillas de informes personalizados
- › Informes programados
- › Exportación de informes en formato PDF, CSV o HTML
- › Almacenamiento de datos durante un año como máximo por firewall
- › Conector para MDR/XDR Data Lake para la búsqueda de amenazas

Presentación de informes integrada

- › NOTA: La generación de informes de Sophos Firewall está incluida sin coste adicional, pero la disponibilidad de registros individuales, informes y widgets puede depender de las licencias de los módulos de protección correspondientes
- › Cientos de informes integrados con opciones personalizadas: Paneles de control (tráfico, seguridad y cociente de amenazas por usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), red y amenazas (respuesta a amenazas activas y feeds de amenazas, Security Heartbeat, IPS, inalámbrico, protección contra amenazas de día cero), VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- › Supervisión de la actividad actual: estado de seguridad del sistema, usuarios activos, conexiones IPsec, usuarios remotos, conexiones activas, clientes inalámbricos, cuarentena y ataques DoS

- Supervisión del rendimiento de enlaces SD-WAN en cuanto a latencia, fluctuación y pérdida de paquetes
- Anonimización de informes
- Programación de informes para múltiples destinatarios por grupo, con opciones de frecuencia flexibles
- Exportación de informes en formato HTML, PDF y Excel (XLS)
- Marcadores de informes
- Personalización de la retención de registros por categoría
- Visor de registros completo con vista por columnas y vista detallada, potentes opciones de filtrado y búsqueda, ID de regla con hipervínculo y personalización de la vista de datos

Administración centralizada

Sophos Central

- La administración y la generación de informes en la nube para múltiples firewalls de Sophos Central facilita la administración de políticas de grupo y una consola única para todos los productos de seguridad de TI de Sophos
- La administración de políticas de grupo permite modificar objetos, configuraciones y políticas una sola vez y sincronizarlas automáticamente en todos los firewalls del grupo
- El Administrador de tareas proporciona un registro de auditoría histórico completo y supervisión de los cambios en las políticas de grupo
- La gestión de copias de seguridad y firmware en Sophos Central almacena los últimos cinco archivos de copia de seguridad de configuración para cada firewall, con la opción de anclar uno para almacenamiento permanente y facilitar el acceso
- La programación de actualizaciones de firmware desde Sophos Central permite aplicar actualizaciones automatizadas de forma sencilla en cualquier momento
- El despliegue Zero Touch permite realizar la configuración inicial en Sophos Central y exportarla después para su carga en el dispositivo desde una unidad flash durante el inicio, lo que vuelve a conectar automáticamente el dispositivo con Sophos Central

Zero Trust Network Access

- Puerta de enlace ZTNA de Sophos integrada para un acceso seguro a las aplicaciones alojadas detrás del firewall
- Administrado desde Sophos Central

Secure by Design

- La comprobación del estado de seguridad de Sophos Firewall compara docenas de configuraciones con las mejores prácticas para identificar posibles riesgos con opción de profundizar fácilmente para solucionar cualquier problema
- Capacidad automatizada de aplicación de parches Zero Touch para corregir vulnerabilidades sin tiempo de inactividad
- Kernel reforzado para mejorar la seguridad, el rendimiento y la escalabilidad, con aislamiento estricto de procesos y mitigación frente a ataques de canal lateral
- Supervisión remota de la integridad por Sophos mediante un XDR Sensor integrado que permite la supervisión en tiempo real de la integridad del sistema, incluidas configuraciones no autorizadas, ejecución de código malicioso, manipulación de archivos y más, para identificar y responder rápidamente a los ataques
- Arquitectura Xstream Next-Gen con un nuevo plano de control para máxima seguridad y escalabilidad
- Creación de contenedores de límites de confianza clave y portales de usuario/VPN
- Administración centralizada cifrada y segura a través de Sophos Central, eliminando la necesidad de acceso remoto para administración
- Autenticación multifactor en todos los sistemas como protección contra el robo de credenciales y ataques de fuerza bruta
- Puerta de enlace ZTNA integrada para un acceso remoto más seguro y protección de la aplicaciones
- Despliegues seguros listos para usar que garantizan la aplicación de las mejores prácticas de seguridad con controles de acceso estrictos

Resumen de características de Sophos Firewall por suscripción

	Paquete de protección Xstream					Disponible por separado				
	Paquete de protección estándar					Disponible por separado				
	Firewall base	Protección de redes	Protección web	DNS Protection	Funciones exclusivas del paquete	Protección de día cero	Orquestación en Central	Central Firewall Reporting Advanced	Protección de correo electrónico	Protección de servidores web
Administración general (incl. HA)	✓									
Arquitectura de Xstream	✓									
Firewall, conexión en red y enrutamiento	✓									
SD-WAN de Xstream	✓									
Conformado de tráfico base y cuotas	✓									
Conexión inalámbrica segura	✓									
Autenticación	✓									
Portal de autoservicio de usuarios	✓									
VPN (IPsec, SSL, etc)	✓									
VPN de sitio a sitio RED	✓									
Cliente VPN Sophos Connect	✓									
Prevención de intrusiones (IPS)		✓								
Respuesta a amenazas activas										
Feeds de amenazas de Sophos X-Ops		✓								
Feed de amenazas de MDR/XDR					✓					
Feeds de amenazas de terceros					✓					
Seguridad Sincronizada con Security Heartbeat		✓								
Gestión de dispositivos SD-RED		✓								
VPN sin cliente		✓								
Control de aplicaciones sincronizado			✓							
Control y protección web			✓							
Protección y control de aplicaciones			✓							
Visibilidad de aplicaciones en la nube			✓							
Conformado de tráfico web y de aplicaciones (Web and App Traffic Shaping)			✓							
Seguridad DNS y cumplimiento				✓						
NDR Essentials					✓					
Análisis dinámico de espacio seguro						✓				
Análisis de información sobre amenazas						✓				
Orquestación de SD-WAN							✓			
Datos de Central Firewall Reporting*		7 días	7 días	7 días	7 días	7 días	30 días	Hasta 1 año	7 días	7 días
Funciones de CFR Advanced							✓	✓		
Protección y control del correo electrónico									✓	
Gestión de cuarentena de Sophos Email									✓	
Cifrado del correo electrónico y DLP									✓	
Protección firewall de aplicación web										✓
Generación de informes/ registro integrado	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Administración a través de Sophos Central*		✓	✓	✓	✓	✓	✓	✓	✓	✓
Puerta de enlace ZTNA**		✓	✓	✓	✓	✓	✓	✓	✓	✓
Diseñado para la seguridad	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Importante: Algunas funciones no son compatibles con los modelos XGS 87 y XGS 88 (generación de informes integrada, escaneado antivirus dual, escaneado antivirus WAF y funcionalidad del agente de transferencia de mensajes (MTA) de correo)

Las opciones de licencia para MSP difieren ligeramente respecto a lo anterior

* El tiempo de retención del almacenamiento de datos es una estimación basada en el uso medio de la red y variará en función del volumen real de datos de registro. [Herramienta de estimación de almacenamiento.](#)

** Incluido en cualquier paquete, soporte o suscripción de protección. Los clientes con una licencia Base deben añadir soporte para poder acceder a estas funciones.

Resumen de características de Sophos Firewall por suscripción

	Soporte Superior (incluido en paquete de protección Standard y Xstream)	Soporte Enhanced Plus (Disponible como actualización del soporte Enhanced)
Soporte multicanal 24/7 (teléfono, portal web, chat), incluida asistencia remota y acceso de autoservicio a la base de conocimientos y foros de soporte.	✓	✓
Versiones de descargas, actualizaciones y mantenimiento de firmware **	✓	✓
Administración de Sophos Central, generación de información y puerta de enlace ZTNA	✓	✓
Sustitución avanzada de hardware para dispositivos activos	✓	✓
Sustitución avanzada de hardware para un dispositivo HA pasivo*		✓
Sustitución avanzada de hardware para dispositivos SD- RED/APX		✓
Acceso VIP (llamadas dirigidas a ingenieros sénior)		✓
Consultoría remota (de 2 a 8 horas al año)		✓

* Para activar la cobertura avanzada RMA en un dispositivo HA pasivo, el dispositivo activo debe tener una licencia de soporte Enhanced Plus

Si desea información detallada, consulte [Guía de servicios de soporte de Sophos](#).

** Nota: debe añadirse el soporte a todo módulo individual adquirido para poder recibir actualizaciones del firmware

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

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