



## Esta es la apuesta de Sophos ante el incremento de ataques desde la capa de transporte (TLS)

**CIUDAD DE MÉXICO. 21 DE ABRIL DE 2021.-** Sophos, líder mundial en ciberseguridad de última generación, presentó los nuevos dispositivos de firewall de la serie XGS con una protección avanzada contra ciberataques. Los nuevos dispositivos cuentan con la mejor inspección de seguridad de la capa de transporte (TLS) de la industria, incluido el soporte nativo para TLS 1.3, que es hasta cinco veces más rápido que otros modelos disponibles actualmente en el mercado.

*“Los dispositivos de la serie Sophos Firewall XGS representan la actualización de hardware más importante que hayamos lanzado y presentan una detección, protección y velocidad incomparables”, dijo Dan Schiappa, director de productos de Sophos. “Los equipos de seguridad ya no pueden permitirse el lujo de pasar por alto el tráfico encriptado por temor a perjudicar el rendimiento, por eso rediseñamos por completo el hardware de Sophos Firewall para manejar el cifrado moderno existente en internet. Ahora, tienen la capacidad de inspeccionar fácilmente el tráfico encriptado y tener más visibilidad sobre lo que alguna vez fue un agujero negro, con confianza de no comprometer el rendimiento”, añadió.*

- **TLS, una vía cada vez más común para los ciberdelincuentes**

Sophos también publicó hoy una nueva investigación llamada ‘Casi la mitad del malware ahora usa TLS para ocultar las comunicaciones’, que identifica un aumento en la tendencia de los ciberdelincuentes en utilizar la capa de transporte TLS en sus ataques. Esto se debe a que los ciberdelincuentes utilizan esta táctica para cifrar y encapsular el contenido malicioso en esa capa, para evitar ser detectados y llevar a cabo el ataque.

De hecho, el 45% del malware detectado por Sophos desde enero hasta marzo de 2021 utilizó TLS para ocultar el contenido de sus comunicaciones maliciosas. Eso es un aumento asombroso del 23% que la empresa detectó a principios de 2020.

La mayoría del tráfico TLS malicioso que ha detectado Sophos está compuesto por malware de compromiso inicial, como cargadores, cuentagotas e instaladores basados en documentos como BazarLoader, GoDrop y ZLoader.

*“Sin duda, TLS ha mejorado la privacidad de las comunicaciones de internet, pero a pesar de todo lo bueno que ha hecho, también ha facilitado mucho a los atacantes la descarga e instalación de módulos maliciosos y la filtración de datos robados, justo ‘en las narices’ de los equipos de seguridad de TI y la mayoría de las tecnologías de seguridad”, dijo Schiappa.*

# SOPHOS

- **Acelerando la protección contra amenazas**

Con tecnología de la arquitectura Xstream de Sophos Firewall, los dispositivos de la serie XGS brindan la mejor protección contra amenazas de la industria, identificando y deteniendo los ataques conocidos y potenciales más avanzadas, incluido el ransomware. La protección está impulsada por una potente inteligencia ante ciberataques disponible solo a través de SophosLabs Intelix, en donde los archivos sospechosos se detonan de forma segura y se someten a un análisis estático en profundidad, todo para obtener cobertura de detección adicional y recopilación de inteligencia.

Los nuevos procesadores de flujo Xstream dentro de los dispositivos XGS aceleran automáticamente el tráfico confiable, como el software como servicio (SaaS) y las aplicaciones en la nube, proporcionando el máximo margen de protección para el tráfico que requiere TLS. Esto reduce en gran medida la latencia, además de que mejora el rendimiento general de las aplicaciones comerciales y legítimas importantes, en particular las que utilizan datos en tiempo real.

Los procesadores de flujo Xstream son programables por software, lo que permite a Sophos descargar tráfico adicional en el futuro. Esto protege la inversión y la organización de los clientes durante todo su ciclo de vida.

Sophos es el único proveedor que proporciona visibilidad en el panel de control del tráfico TLS. El rendimiento se optimiza desde el primer momento con un amplio conjunto de reglas que SophosLabs actualiza y mantiene para excluir el tráfico seguro de la inspección.

Sophos proporciona una visibilidad del panel de control única e intuitiva para el tráfico de TLS y los problemas de inspección, y los administradores de seguridad pueden agregar excepciones con un solo clic. El rendimiento también se optimiza desde el primer momento con un amplio conjunto de reglas que SophosLabs actualiza y mantiene para excluir el tráfico seguro de la inspección.

Los dispositivos y el firmware de la serie Sophos Firewall XGS ya están disponibles y se administran fácilmente en la plataforma Sophos Central basada en la nube. La integración con Sophos Managed Threat Response (MTR) aumenta aún más la protección con análisis humano para una detección y respuesta de amenazas totalmente administrada 24 horas al día, 7 días a la semana.

- **Disponibilidad**

La serie Sophos Firewall XGS está disponible a través del canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Estos modelos son ideales para organizaciones pequeñas y medianas. Tienen una sólida relación precio/rendimiento y diversas opciones de conectividad adicional. En las próximas semanas estarán disponibles modelos

# SOPHOS

adicionales, diseñados para entornos de borde empresarial que requieren un rendimiento máximo para configuraciones de red más complejas. La licencia simplificada incluye protección combinada con soporte mejorado para la máxima protección y el máximo valor.

- **Testimonios de analistas y socios de canal**

*“Los dispositivos de firewall están evolucionando para asegurar casos de uso más nuevos, incluida la nube y el cambio repentino a una fuerza de trabajo remota en crecimiento”, dijo **Frank Dickson, vicepresidente de IDC.** “La elegancia de la arquitectura de Sophos Firewall está en su capacidad para acelerar el tráfico confiable ante los llamados ‘flujos elefantes’ (grandes flujos de tráfico de VoIP e incluso aplicaciones en la nube) para luego realizar procesos como inspección profunda de paquetes de TLS. El resultado es un dispositivo de red adaptable diseñado para brindar protección mientras satisface y acelera las demandas comerciales cambiantes en una variedad de casos de uso”.*

*“Con los nuevos dispositivos de firewall de la serie XGS detectamos un aumento inmediato en el rendimiento, mismo que se vio duplicado. Sophos Firewall siempre ha sido líder en la industria, pero los dispositivos de la serie XGS son un parteaguas de innovación”, dijo **Sam Heard, presidente de Data Integrity Services.** “Sophos Firewall brinda la protección que nuestros clientes necesitan a medida que mueven cada vez más aplicaciones críticas para el negocio a la nube y adoptan tecnologías de alto nivel de confianza”.*

*“La instalación del dispositivo es increíblemente simple y se administra sin esfuerzo desde Sophos Central, lo que hace que sea exponencialmente más fácil proteger y administrar entornos de clientes diversos y complejos”, dijo **Karen Greer, directora ejecutiva de Secure Content Technologies.** “Saber que Sophos Firewall comparte automáticamente la inteligencia sobre amenazas con otras soluciones en la plataforma a través de su función de sincronización es un cambio que nos brinda total confianza y tranquilidad de que nuestros clientes están protegidos”.*

###

## **Sobre Sophos**

Como líder mundial en seguridad cibernética de última generación, Sophos protege a más de 400,000 organizaciones en más de 150 países de las amenazas cibernéticas más avanzadas de la actualidad. Desarrolladas por SophosLabs, un equipo global de inteligencia contra amenazas cibernética y ciencia de datos, las soluciones basadas en inteligencia artificial y nativas de la nube de Sophos ofrecen seguridad a endpoints (computadoras portátiles, servidores y dispositivos móviles) y redes contra las diversas técnicas de ciberdelincuencia que están en constante evolución, incluidos ransomware, malware, exploits, extracción de datos, incumplimientos de adversarios activos, phishing y más. Sophos Central, una plataforma de administración nativa de la nube, integra toda la cartera de productos de próxima generación de Sophos, incluida la solución de endpoint Intercept X

# SOPHOS

y el Firewall XG, en un único sistema de "seguridad sincronizada" accesible a través de un conjunto de APIs.

Sophos ha impulsado la transición a la ciberseguridad de última generación, aprovechando las capacidades avanzadas en la nube, el aprendizaje automático, las API, la automatización, la respuesta ante amenazas y más, para brindar protección de nivel empresarial a organizaciones de cualquier tamaño. Sophos vende sus productos y servicios exclusivamente a través de un canal global de más de 53,000 socios y proveedores de servicios administrados (MSP). Sophos también pone a disposición de los consumidores sus innovadoras tecnologías comerciales a través de Sophos Home. La compañía tiene su sede en Oxford, Reino Unido. Para obtener más información visita [www.sophos.com](http://www.sophos.com).

**Síguenos en:**

Facebook: <https://www.facebook.com/SophosLatam/>

Twitter: <https://twitter.com/SophosLatAm>

LinkedIn: <https://www.linkedin.com/company/sophos/>