SOPHOS

Novedades de

Sophos Firewall

Nuevas funciones destacadas de Sophos Firewall OS v21.5

Mayor protección y rendimiento

Integración de Sophos NDR Essentials con Sophos Firewall

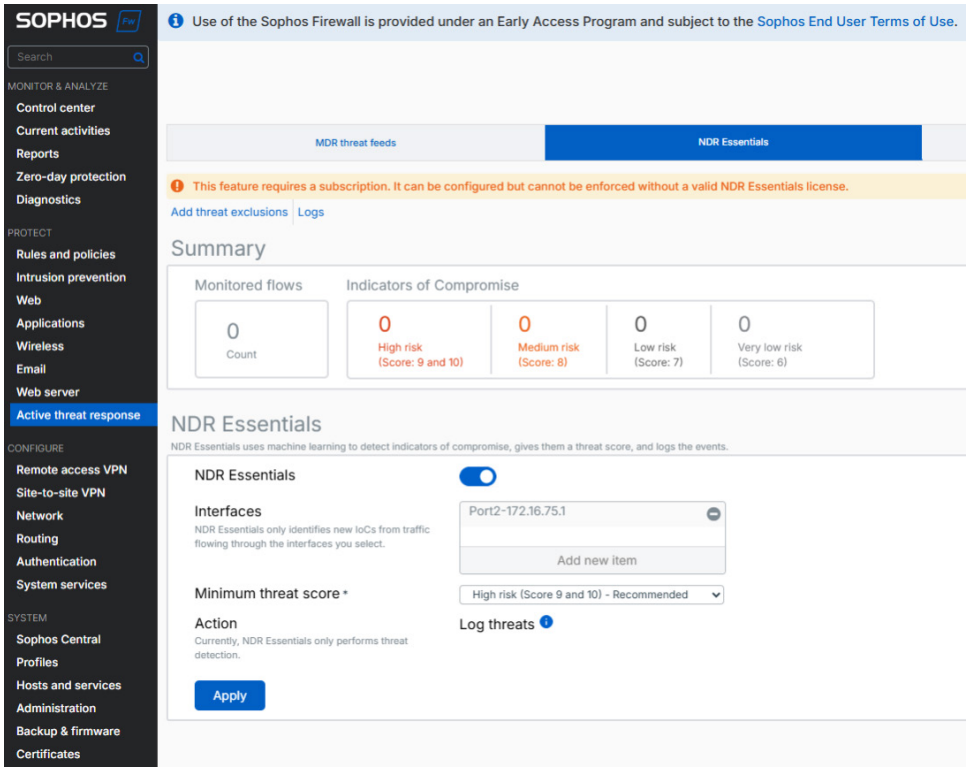
Network Detection and Response (NDR) es una categoría de productos de seguridad de la red que ha sido concebida para detectar comportamientos anómalos del tráfico con el fin de ayudar a identificar a los adversarios activos que operan en la red. Los atacantes expertos son muy eficaces a la hora de eludir la detección, pero en algún momento deben desplazarse o comunicarse fuera de la red para llevar a cabo un ataque. Normalmente, NDR se integra en la red utilizando sensores que supervisan y analizan el tráfico de la red para identificar este tipo de actividad sospechosa.

Los productos NDR existen desde hace muchos años, y Sophos NDR forma parte de nuestra cartera de productos MDR/XDR desde principios de 2023. Sin embargo, con SFOS v21.5, integramos NDR con Sophos Firewall, una novedad en el sector, sin coste adicional para los clientes de Sophos Firewall con la protección Xstream.

Integrar NDR con un firewall next-gen puede parecer algo obvio, pero el reto es hacerlo de forma que no afecte al rendimiento del firewall. El análisis del tráfico de NDR requiere una capacidad de procesamiento considerable. Por lo tanto, hemos adoptado un enfoque innovador que consiste en desplegar una solución NDR en la nube de Sophos para liberar al firewall de esta pesada tarea.

Sophos Firewall v21.5 presenta NDR Essentials, nuestra nueva plataforma de Network Detection and Response. Utiliza las últimas detecciones basadas en IA para ayudar a identificar adversarios activos y comparte esa información a través de la API de feeds de amenazas de Sophos Firewall como parte de la respuesta a amenazas activas para mantenerle informado de todas las detecciones y su riesgo relativo.

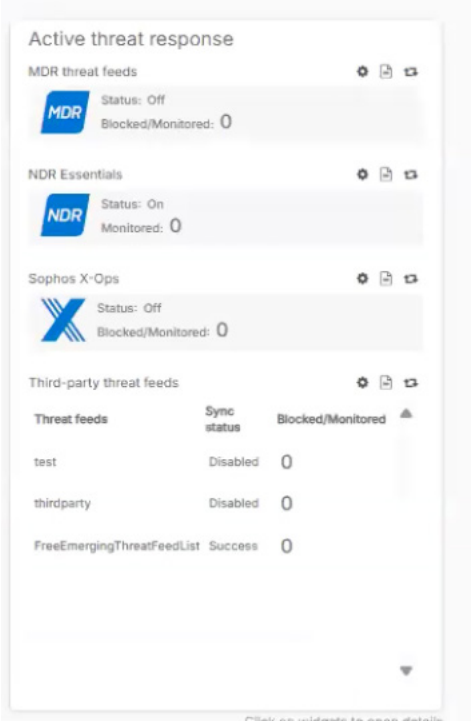
Cómo funciona: Sophos Firewall captura los metadatos del tráfico cifrado por TLS y las consultas DNS y envía esa información a NDR Essentials en la nube de Sophos, donde se analizan los datos utilizando varios motores de IA. Puede detectar cargas cifradas maliciosas sin necesidad de descifrado TLS, así como dominios nuevos e inusuales generados mediante algoritmos que suelen ser un indicador importante de compromiso. La extracción de metadatos la lleva a cabo un nuevo motor ligero que se ejecuta en la ruta rápida FastPath de Xstream, por lo que solo está disponible en los firewalls de hardware de la serie XGS. Es posible que los firewalls de software, virtuales y en la nube obtengan esta capacidad de integración con NDR en el futuro, pero no en la v21.5.



Configure y supervise su feed de NDR Essentials en "Respuesta a amenazas activas", junto a sus otros feeds de amenazas.

El nuevo feed de amenazas de NDR Essentials se gestiona junto con los otros feeds de amenazas (Sophos X-Ops, MDR y feeds de terceros) en el área Respuesta a amenazas activas del firewall, como se muestra en la captura de pantalla anterior. La configuración es sencilla: accione el switch correspondiente para activarlo, seleccione las interfaces internas que desea supervisar, defina un umbral mínimo de riesgo de detección y ¡listo!

Las detecciones de NDR Essentials se clasifican en una escala del 1 (riesgo bajo) al 10 (riesgo más alto). Usted decide la puntuación de riesgo que define el umbral de una alerta en función de su entorno. El valor predeterminado recomendado es riesgo alto (9-10). Todas las detecciones con una puntuación igual o superior a 6 se registrarán, pero solo aquellas que alcancen o superen su umbral activarán notificaciones y se mostrarán como alertas en el nuevo widget del panel de control de su Centro de control. Las detecciones con una puntuación inferior a 6 pueden ser falsos positivos y, en consecuencia, no se registran. Actualmente no se bloquean las detecciones de NDR Essentials, pero quizá sea una opción en el futuro. Se puede acceder a las detecciones a través del informe de respuesta a amenazas activas disponible tanto con la opción de generación de informes integrada como a través de Sophos Central Firewall Reporting.



Cualquier detección de NDR Essentials que alcance o supere el valor del umbral de riesgo especificado se muestra en el widget mejorado del Centro de control.

Si desea obtener información más detallada sobre la detección y las capacidades adicionales de búsqueda de amenazas, le recomendamos encarecidamente que eche un vistazo a Sophos Extended Detection and Response (XDR) con la implementación completa de Sophos NDR y la nueva consola de investigación de NDR. Quizá también le interese considerar nuestro servicio completo de detección y respuesta gestionadas. 24/7. Todos estos productos y servicios funcionan mejor junto con sus dispositivos Sophos Firewall.

SSO para VPN de acceso remoto

Inicio de sesión único de Entra ID (Azure AD) para el cliente de Sophos Connect y el portal VPN

Una de las funciones más solicitadas facilita el acceso remoto a través de VPN para los usuarios finales, al permitirles utilizar las credenciales de red de su empresa con el cliente de Sophos Connect y el portal VPN del firewall. Ahora, SFOS v21.5 integra el inicio de sesión único de Entra ID (Azure AD) con Sophos Connect y el portal VPN. Ofrece integración nativa en la nube con los protocolos estándar del sector OAuth 2.0 y OpenID Connect para una experiencia fluida. Compatible con el cliente de Sophos Connect 2.4 y posteriores en Microsoft Windows.

Otras mejoras en materia de VPN y escalabilidad

Mejoras en la interfaz de usuario y en la usabilidad: los tipos de conexión han pasado de llamarse "sitio a sitio" a "basados en políticas", y las interfaces de túnel ahora se llaman "basadas en ruta" para hacerlas más intuitivas.

Validación mejorada del grupo de asignación de direcciones IP: VPN de acceso remoto a través de SSLVPN, IPsec, L2TP y PPTP para eliminar posibles conflictos de IP.

Aplicación estricta de perfiles: en los perfiles IPsec que excluyen los valores predeterminados para garantizar un establecimiento de comunicación satisfactorio, eliminando así la posible fragmentación de paquetes y que los túneles no se establezcan correctamente.

Escalabilidad de VPN basada en enrutamiento: la capacidad de VPN basada en enrutamiento se duplica con soporte para hasta 3000 túneles.

Escalabilidad SD-RED: ahora, los dispositivos Sophos Firewall admiten hasta 1000 túneles RED de sitio a sitio y hasta 650 dispositivos SD-RED.

Sophos DNS Protection

Simplificación del servicio Sophos DNS Protection

El año pasado pusimos en marcha nuestro servicio DNS Protection y lo ofrecimos de forma gratuita a todos los clientes de firewall con licencia de protección Xstream. Con esta versión, Sophos DNS Protection se beneficia de una integración mejorada con Sophos Firewall: un nuevo widget del centro de control para indicar el estado del servicio, nuevos datos en materia de resolución de problemas mediante registros y notificaciones, y un nuevo tutorial guiado sobre cómo configurar Sophos DNS Protection fácilmente.

Mejoras en la optimización de la gestión y la usabilidad

Como en cada lanzamiento de Sophos Firewall, esta versión incluye varias mejoras de usabilidad que facilitan la gestión diaria.

Columnas de tabla ajustables: esta función, solicitada desde hace tiempo, permite ajustar el ancho de las columnas de muchas pantallas de estado y configuración del firewall, que se conservan en la memoria del navegador para visitas posteriores. Muchas pantallas se benefician de esta nueva función, como las de SD-WAN, NAT, SSL, Hosts y servicios, y VPN de sitio a sitio.

Búsqueda ampliada de texto libre: ahora, las rutas SD-WAN permiten la búsqueda por nombre de ruta, ID, objetos y valores de objeto como direcciones IP, dominios u otros criterios. Las reglas ACL locales también admiten la búsqueda por nombre y valor de objeto, incluida la búsqueda basada en el contenido.

Configuración predeterminada: por demanda popular, se han eliminado las reglas de firewall y el grupo de reglas por defecto al configurar un nuevo firewall, y durante la configuración inicial solo se proporcionan la regla de red por defecto y las reglas MTA. El grupo de reglas de firewall por defecto y el sondeo de puerta de enlace por defecto para las puertas de enlace personalizadas están configurados en "Ninguno" de forma predeterminada.

Nuevo tipo de letra: la interfaz de usuario de Sophos Firewall tiene un nuevo tipo de letra más claro y definido para aumentar la legibilidad y mejorar el rendimiento.

Otras mejoras

Licencias virtuales, de software y en la nube: las licencias virtuales, de software y en la nube (BYOL) de Sophos Firewall ya no tienen límite de RAM. Ahora, las licencias están estrictamente limitadas por el número de núcleos y no tienen restricciones en cuanto a la RAM.

Mayor límite de tamaño de archivo en WAF: admite un límite configurable de tamaño de archivo de solicitud (carga) para el firewall de aplicaciones web (WAF), que ahora puede escanear archivos de hasta 1 GB.

Diseñado para la seguridad: mejoramos continuamente la seguridad de Sophos Firewall y, en esta versión, añadimos la recopilación de telemetría en tiempo real para señalar los cambios inesperados en los archivos principales del sistema operativo mediante una validación de hash segura. Así, nuestros equipos de supervisión podrán identificar de forma proactiva posibles incidentes de seguridad antes de que se conviertan en un verdadero problema.

Relajación de la delegación de prefijos DHCP: ahora se admiten prefijos de /48 a /64, lo que mejora la interoperabilidad con los ISP. Además, los anuncios de enrutador (RA) y el servidor DHCPv6 están activados por defecto.

Descubrimiento de MTU de rutas de acceso: esta función resolverá los errores de descifrado TLS debidos a la última compatibilidad con el intercambio de claves ML-KEM (Kyber) en los navegadores. El motor de inspección detallada de paquetes de Sophos Firewall detectará y ajustará automáticamente la MTU de cada flujo, lo que garantizará un rendimiento óptimo en función de las condiciones específicas de la red.

NAT64 (tráfico IPv6 a IPv4): NAT64 es compatible con el tráfico IPv6 a IPv4 en modo proxy explícito. En este modo, los clientes que solo tienen IPv6 pueden acceder a sitios web IPv4. El firewall también admite el proxy ascendente IPv4 para clientes con IPv6 solamente.

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

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

31-03-2025 ES (DD)