SOPHOS
Security made simple.

Mantenga su red bajo control

Por qué los administradores de red necesitan una visibilidad completa de las aplicaciones

La evolución del firewall

A lo largo de los años, el papel del firewall ha evolucionado de froma constante pasando de proteger redes contra alteraciones de código y ataques externos a enfocar su atención más hacia el interior para identificar y eliminar riesgos potenciales y garantizar el cumplimiento de la normativa. Esta evolución se debe en parte a la respuesta ante el cambio que se ha producido en el panorama de amenazas hacia intrusiones y programas de malware diseñados para explotar las vulnerabilidades en las aplicaciones en lugar del propio perímetro de red. Otro factor que ha contribuido a este cambio hacia dentro es la creciente obligación de ofrecer un nivel razonable de cumplimiento normativo, proporcionar protección contra fugas y filtraciones de datos y optimizar el rendimiento de la red.

Básicamente, el firewall de última generación (Next-generation) nació de la necesidad de ofrecer una mayor visibilidad y control de los usuarios y de sus aplicaciones. El firewall de última generación se sitúa literalmente por encima de los puertos y protocolos de los firewalls dinámicos anteriores en los niveles superiores del modelo OSI para proporcionar la identificación de aplicaciones y usuarios.

Los firewalls de última generación usan la inspección detallada de paquetes para identificar aplicaciones y relacionarlas con usuarios o hosts en la red, de modo que los administradores pueden proporcionar los controles apropiados. Por ejemplo, es sumamente útil poder identificar usuarios que ejecutan aplicaciones de intercambio de archivos (peer-to-peer) y bloquearlas, así como controlar el uso excesivo de la reproducción multimedia en streaming, todo ello mientras se priorizan las aplicaciones empresariales importantes como el sistema ERP, el tráfico VoIP y el software CRM.

Cómo funciona el control de aplicaciones de firewalls de última generación (Next-Gen Firewall App Control)

Los firewalls identifican las aplicaciones buscando patrones en el tráfico que coincidan con firmas conocidas. Es similar al reconocimiento facial. Cuando uno ve la cara de una persona que no conoce, la puede comparar con una serie de fotografías. Si hay una imagen que coincide, sabe de quién se trata; si no, realmente no hay manera de saber quién es esa persona.

"Un promedio del 60 % del tráfico de la red no se identifica."

El control de aplicaciones funciona de la misma forma. Mientras algunas aplicaciones llevan el equivalente a una tarjeta con el nombre, facilitando su identificación, la mayoría de aplicaciones no lo hacen y algunas incluso no escatiman esfuerzos para colarse sin ser identificadas. Evidentemente, cuando se detecta una coincidencia y se identifica una aplicación, el firewall la puede controlar (mediante el conformado de tráfico para priorizar o limitar el consumo de ancho de banda) o bloquearla directamente. Pero si no se encuentran coincidencias, el firewall no sabe a qué se enfrenta y no tiene ningún control.

Los problemas del control de aplicaciones de firewalls de última generación

Como cabe imaginar, para muchas aplicaciones no se encontrarán coincidencias. Muchas aplicaciones de riesgo que normalmente se bloquearían en la mayoría de organizaciones, como clientes BitTorrent, usan métodos inteligentes para cambiar constantemente sus patrones de tráfico y la forma en la que se desconectan de la organización para evitar la detección. Esto no difiere mucho de una persona que se cambie el color de pelo o se ponga bigote para eludir el reconocimiento facial.

Otras aplicaciones utilizan el cifrado para evitar la detección, que podría compararse con una persona que llevase pasamontañas. Y otras muchas aplicaciones fingirán ser un navegador para poder burlar el firewall sin ser controladas. Es como una mala persona que se disfraza de una persona famosa. Y luego están las aplicaciones que han cambiado recientemente o que son puntuales, personalizadas o simplemente demasiado crípticas como para tener un patrón que coincida. Estas aplicaciones serían como las personas que no tienen una fotografía reciente en el expediente.

De hecho, a medida que los firewalls son cada vez mejores a la hora de identificar y controlar las aplicaciones no deseadas, estas aplicaciones son cada vez mejores a la hora de evitar la detección.

El resultado final es que la mayor parte del tráfico que pasa hoy en día por un firewall moderno es desconocido, indeterminado o simplemente demasiado genérico como para ser clasificado o controlado.

¿Tiene su informe de control de aplicaciones este aspecto?

Nombre de la aplicación	Porcentaje de aplicaciones
UDP general	25,45 %
Administración de HTTPS general	24,26 %
DNS general	17,8 %
TCP general	14,39 %
Servicios RPC (IANA)	8,86 %
Protocolo BitTorrent - Actividad 1 UDP (Req. SIB 5)-63	1,60 %

Panel de control de firewall convencional que muestra las categorías que no se han podido identificar

¿Es un problema muy serio?

Para comprender mejor lo generalizado que está el problema, Sophos realizó hace poco una encuesta a medianas empresas para determinar el porcentaje de su tráfico de aplicaciones que se quedaba sin identificar o controlar:

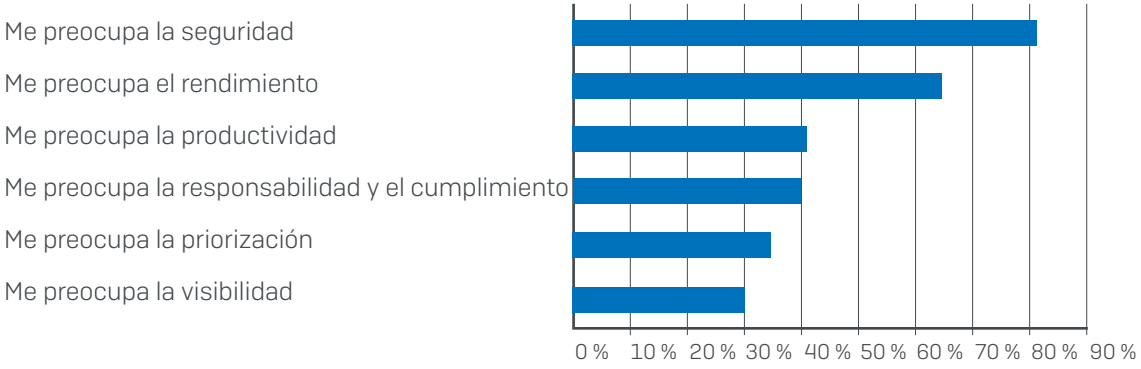
- Casi el 70 % de las organizaciones disponen de un firewall o solución UTM de última generación con detección de aplicaciones
- Un promedio del 60 % del tráfico no se puede identificar... y muchas organizaciones informaron que hasta un 90 % de su tráfico de aplicaciones permanecía sin identificar

Si le preocupa la seguridad, la responsabilidad o el impacto que esta cuestión tiene en el rendimiento de su organización, no es el único...

- El 82 % de los encuestados están preocupados y con razón por los riesgos de seguridad que conlleva esta falta de visibilidad de las aplicaciones
- Al 65 % les preocupa el impacto que esta cuestión puede tener en el rendimiento de su red
- Al 40 % les preocupan los riesgos de cumplimiento y las responsabilidades jurídicas en que pueden incurrir

Mayores preocupaciones por la actual falta de visibilidad de aplicaciones:

¿Qué le preocupa del tráfico de red no identificado? (Selección múltiple)



Principales aplicaciones evasivas y no identificadas

Estas aplicaciones evasivas representan un alto riesgo para la seguridad debido a las vulnerabilidades, un riesgo para el cumplimiento normativo debido a posible contenido inadecuado o ilegal y un riesgo para la productividad y el consumo del ancho de banda.

- Aplicaciones de mensajería instantánea y conferencias (por ej. Skype, TeamViewer)
- BitTorrent y otros clientes P2P (por ej. uTorrent, Vuze, Freenet)
- Clientes proxy y de túnel (por ej. Ultrasurf, Hotspot Shield, Psiphon)
- Juegos (por ej. Valve y Steam)

Desafortunadamente, le será prácticamente imposible saber si alguna de estas aplicaciones se está ejecutando en la red, ya que las firmas de firewall no van a encontrar una coincidencia en la mayoría de los casos.

Además de estas aplicaciones, hay un sinfín de apps tanto benignas como no deseadas que han recurrido al uso de conexiones HTTP y HTTPS genérico para comunicarse con el exterior a través del firewall, contando con el hecho de que casi todas las organizaciones abren su firewall para acceder a Internet en los puertos 80 y 443. En los informes que genere, estas aplicaciones simplemente aparecerán como HTTP, HTTPS, SSL, navegación web y otras categorías generales que no ofrecen ninguna indicación útil.

Y tal vez lo más importante: hay aplicaciones verticales, soluciones ERP, software CRM y otras aplicaciones empresariales cruciales que probablemente sean exclusivas de su organización que no se detecten y que quizá se vean aplastadas bajo el peso de la navegación web y otro tráfico de aplicaciones no deseado simplemente porque no son lo bastante populares como para disponer de una firma.

Por suerte, existe una solución bastante elegante a este problema.

La solución

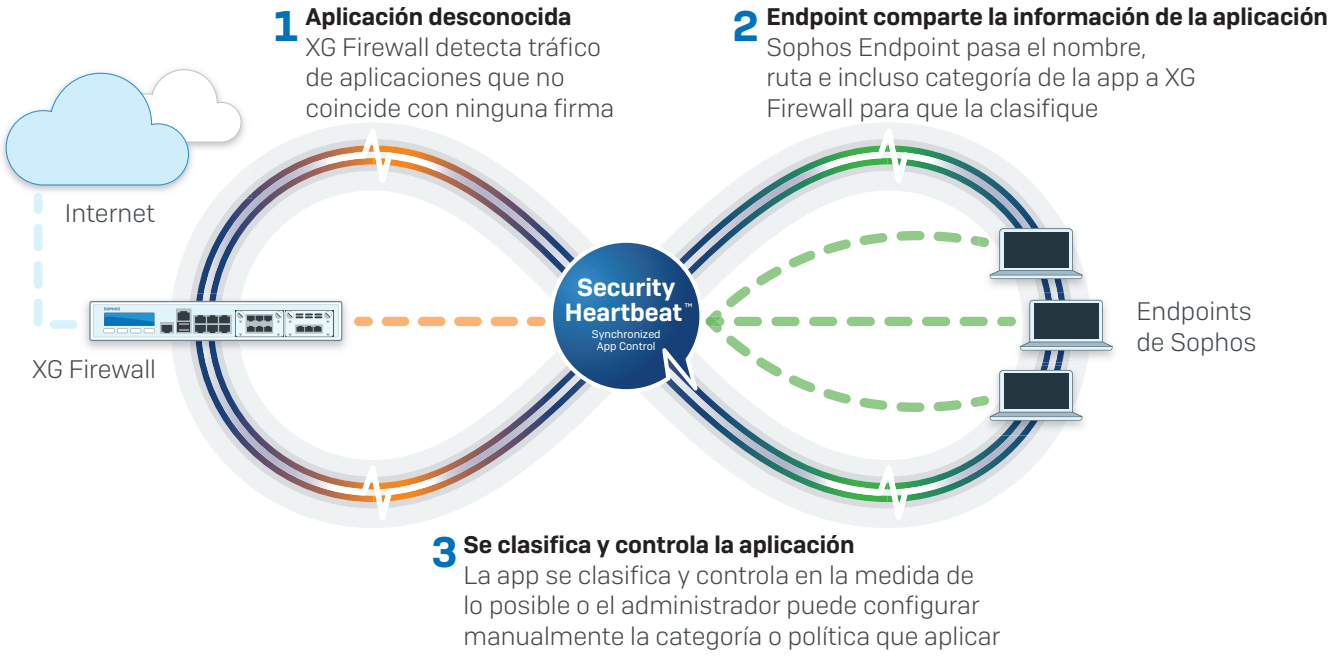
Mientras los firewalls de última generación dependen de la inspección detallada de paquetes, la búsqueda de patrones y las firmas para identificar las aplicaciones que atraviesan la red, el endpoint se halla en una posición única en la que sabe de forma inherente y con absoluta certeza exactamente qué ejecutables generan todo el tráfico de la red. Así pues, la solución parece bastante obvia: conectar el endpoint con el firewall para que compartan esa valiosa información. Afortunadamente, Sophos dispone de la tecnología para permitir esta conexión de forma sencilla y eficaz: La seguridad sincronizada.

La seguridad sincronizada de Sophos es un revolucionario enfoque de la seguridad informática que permite que los productos de seguridad compartan información y funcionen juntos para proporcionar una protección inigualable y una respuesta automatizada ante incidentes, además de visibilidad en tiempo real.

Una de las primeras innovaciones de la seguridad sincronizada, Security Heartbeat™, conecta los endpoints administrados por Sophos Central con Sophos XG Firewall para compartir la información del estado de los mismos, lo que permite la identificación inmediata de los sistemas que corren peligro. Cuando se detecta un riesgo, ya sea a nivel del endpoint o del firewall, se emiten indicadores de tipo semáforo y alertas en tiempo real, permitiendo así identificar al instante el equipo, el usuario y el proceso implicados. Tal vez la ventaja más importante de Security Heartbeat es que el firewall puede incluir la información del estado de los endpoints en las reglas del firewall, lo que permite automatizar la respuesta ya sea limitando el acceso o aislando totalmente el sistema comprometido hasta que se pueda limpiar. Esto ha reducido el tiempo de respuesta de horas a segundos y ayuda a disminuir el riesgo de que las infecciones se propaguen a otras partes de la red.

Otra innovación de la seguridad sincronizada es el control de aplicaciones sincronizado (Synchronized App Control). Como su propio nombre indica, el control de aplicaciones sincronizado aprovecha el ecosistema único de la seguridad sincronizada de Sophos para resolver de forma eficaz y elegante el problema de la identificación del tráfico de aplicaciones desconocidas, evasivas o personalizadas. El control de aplicaciones sincronizado utiliza su capacidad de intercambio de información con el endpoint para determinar el origen del tráfico de aplicaciones no identificado en la red, eliminando así de forma eficaz el grueso velo que oculta las redes hoy en día.

Cómo funciona el control de aplicaciones sincronizado



Es el primer avance revolucionario en la visibilidad y el control de las aplicaciones en la red desde que fue concebido el firewall de última generación.

Cuando un endpoint gestionado mediante Sophos Central se conecta a una red con un dispositivo XG Firewall asociado, establecerá una conexión con Security Heartbeat™ para compartir información de estado, seguridad y telemetría. Además, ahora el endpoint también utilizará esta conexión para compartir con el firewall la identidad de todas las aplicaciones de la red.

Cuando el firewall no pueda confirmar la identidad de la aplicación mediante técnicas de firma tradicionales porque la aplicación es evasiva, personalizada, nueva o utiliza una conexión genérica, la información de la aplicación que proporciona el endpoint se usará para identificarla, clasificarla y controlarla. En la medida de lo posible, las aplicaciones compartidas por el endpoint se clasificarán en una categoría apropiada de forma automática. Así, la aplicación recién identificada y clasificada se someterá automáticamente a las políticas de control de aplicaciones que se estén implementando en el firewall.

Por ejemplo, un cliente BitTorrent evasivo se asignará automáticamente a la categoría de aplicaciones de intercambio de archivos. Y si el firewall tiene implementada una política de control de aplicaciones que bloquea las apps de intercambio de archivos, el nuevo tráfico de BitTorrent se bloqueará de forma automática sin que el administrador de red intervenga.

Las ventajas:

Identifique las aplicaciones desconocidas

El control de aplicaciones sincronizado revela todas las aplicaciones que no están siendo detectadas en la red, incluidas todas las apps nuevas y las aplicaciones de túnel, proxy y VPN que a menudo utilizan el cifrado para eludir el control del firewall, lo que crea un enorme punto ciego además de toda una serie de riesgos para el cumplimiento, el rendimiento y la seguridad. Si ya hay políticas implementadas para bloquear o conformar el tráfico de este tipo de aplicaciones, las apps recién identificadas comprendidas en esta categoría quedarán sujetas a las mismas políticas de forma automática. Además, los usuarios y hosts implicados serán identificados fácilmente, lo que permite intervenir e informar si procede.

Priorice las aplicaciones personalizadas

El control de aplicaciones sincronizado identificará al instante las aplicaciones empresariales personalizadas que son totalmente invisibles para su firewall actual como aplicaciones de finanzas, CRM, ERP, producción y otras aplicaciones en red que son importantes para su organización. Por primera vez, el control de aplicaciones sincronizado proporciona una oportunidad para aplicar reglas de conformado de tráfico(traffic shaping) y QoS para garantizar que esas aplicaciones fundamentales tengan la prioridad adecuada y un rendimiento óptimo.

Controle las aplicaciones esquivas

El control de aplicaciones sincronizado detectará automáticamente todas las aplicaciones evasivas que constantemente cambian la forma en la que se conectan y comunican para eludir la detección y el control. De hecho, el control de aplicaciones sincronizado pone fin a estas tácticas de una vez por todas. Independientemente de lo esquivas que traten de ser estas aplicaciones, no podrán eludir en absoluto el control de aplicaciones sincronizado.

"Es el primer avance revolucionario en la visibilidad y el control de las aplicaciones en la red desde que el firewall de última generación fue concebido."

Qué productos de Sophos se necesitan:

Sophos proporciona un ecosistema completo de productos de seguridad TI que se integran de forma sencilla para ofrecer la seguridad sincronizada. Activar Security Heartbeat™ y el control de aplicaciones sincronizado y la seguridad, visibilidad y control adicionales que ofrecen no podría ser más fácil. Como mínimo, se necesitan Sophos XG Firewall e Intercept X, pero ambos productos pueden desplegarse junto a su infraestructura de seguridad TI existente de forma complementaria para proporcionar la función de seguridad sincronizada sin interrupciones ni tener que eliminar ni reemplazar ninguno de sus productos.

Sophos XG Firewall puede implementarse en paralelo a su firewall existente o bien como la puerta de enlace de firewall principal. También funciona en modo de solo visibilidad y generación de informes cuando XG Firewall está conectado a un switch espejo de conmutador en modo de descubrimiento (también conocido como modo TAP).

En el endpoint, Intercept X puede desplegarse junto a su solución AV actual o bien puede optar por Sophos Central Endpoint Advanced para disfrutar de una protección completa para endpoints de Sophos. Ambos productos admiten la seguridad sincronizada junto a XG Firewall tanto en plataformas Windows como Mac.

Resumen

Los firewalls de última generación no están cumpliendo su promesa de proporcionar la detección de aplicaciones. Existe una limitación inherente en la eficacia de las técnicas de detección de aplicaciones basadas en firmas que significa que la mayoría del tráfico de aplicaciones en las redes actuales no se logra identificar y controlar. Es un problema serio y significativo. Supone grandes riesgos para la seguridad, la productividad, el rendimiento y el cumplimiento normativo.

Por suerte, hay una solución elegante y eficaz: El control de aplicaciones sincronizado utiliza la conexión única de Security Heartbeat™ de Sophos entre los endpoints gestionados mediante Sophos Central y XG Firewall para compartir información de las aplicaciones de la red con toda claridad.

XG Firewall, asistido por el control de aplicaciones sincronizado, puede identificar, clasificar y controlar todo el tráfico de aplicaciones desconocido en la red de forma automática. Es un avance crucial en la visibilidad y control de la red que hace que los demás firewalls de última generación queden obsoletos.

Pruebe Sophos XG Firewall online gratis en es.sophos.com/demo

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

Ventas en Latin America:
Correo electrónico: Latamsales@sophos.com

22-09-17 WPES (NP)

SOPHOS