SOPHOS
Cybersecurity made simple.

Los secretos más oscuros de los firewalls de red

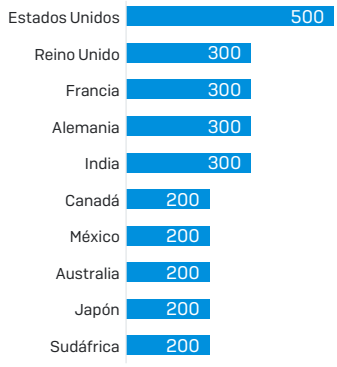
Resultados de una encuesta independiente patrocinada por Sophos a 2700 directores de TI de medianas empresas.

Introducción

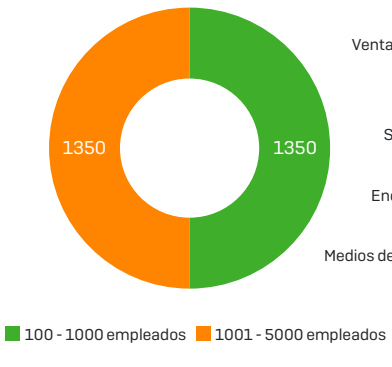
A finales de 2017, Sophos patrocinó un estudio de investigación independiente sobre el estado de la seguridad de las redes en medianas empresas de todo el mundo. Este programa de investigación analizó las experiencias, preocupaciones y necesidades futuras de directores de TI, con especial hincapié en los firewalls y las defensas de la red.

El estudio, realizado por la firma líder de investigación británica Vanson Bourne, preguntó a 2.700 directores de TI de empresas de 100 a 5000 usuarios en 10 países de cinco continentes.

País del encuestado



Tamaño de la empresa



Sector de la empresa

Este monográfico revela los secretos más oscuros de los firewalls actuales, exponiendo cómo están dejando en la estacada a las empresas en áreas clave de protección, visibilidad y respuesta ante amenazas, y el impacto que tienen estas carencias en los directores informáticos de todo el mundo.

SECRETO OSCURO 1

LOS FIREWALLS NO PROPORCIONAN LA PROTECCIÓN QUE NECESITAN LAS EMPRESAS

Resumen ejecutivo

- Las empresas se ven afectadas por una media de 16 ordenadores infectados al mes.
  - Una media de 13 al mes en empresas de 100 - 1000 usuarios.
  - Una media de 20 al mes en empresas de 1001 - 5000 usuarios.
- El 79 % de los directores informáticos desean una mejor protección de su firewall.
- Una protección más eficaz es la mejora en el firewall más deseada por casi la mitad de los directores de TI (48 %).

Actualmente, sufrir múltiples infecciones al mes es la norma

El firewall es la puerta de enlace entre su red e Internet. A menudo también es la puerta de enlace entre distintas partes del entorno informático, por ejemplo, la DMZ y los servidores, varios segmentos LAN, redes inalámbricas y zonas de confianza y de no confianza. Junto con la protección para endpoints, es un pilar integral de la infraestructura de seguridad.

Como consecuencia de esta posición clave, el firewall también constituye la primera línea de defensa fundamental contra las amenazas de malware: las detiene antes de que accedan a la red y evita que se propaguen lateralmente o se extiendan por el entorno, por ejemplo, si entran a través de un dispositivo USB infectado.

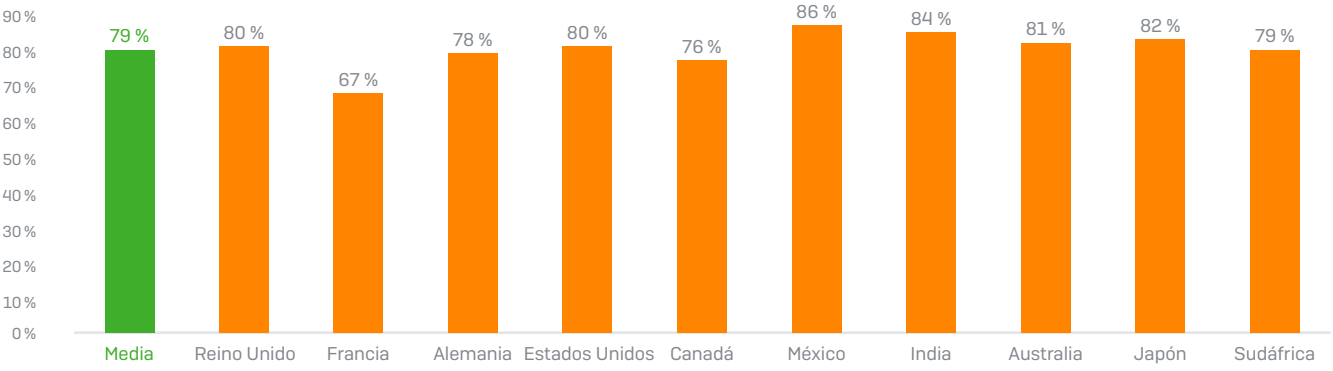
A pesar de la importancia de su papel en la defensa contra las amenazas, la encuesta reveló que los firewalls están dejando en la estacada a las empresas a la hora de proporcionar la protección que necesitan. Cada mes, las empresas se ven afectadas por una media de 16 ordenadores infectados. Las pequeñas empresas (100 - 1000 usuarios) se enfrentan a 13 ordenadores infectados cada mes, mientras que las grandes empresas (1001 - 5000 usuarios) experimentan infecciones en 20 equipos.

> **16** equipos infectados al mes

En vista de estas continuas infecciones, no es de extrañar que casi cuatro de cada cinco directores informáticos (79 %) deseen una mejor protección de su firewall. De hecho, una protección más eficaz es la mejora más deseada por casi la mitad de los directores de TI (48 %). Este deseo de una mayor protección comprende tanto la seguridad del perímetro, para impedir que las amenazas entren, como la protección interna, para evitar que se propaguen si logran entrar.

La protección insuficiente es, por desgracia, un problema de ámbito mundial: al menos dos tercios de los directores de TI desean una mejor protección en cada país encuestado.

% DE ENCUESTADOS QUE DESEAN QUE SU FIREWALL LES PROPORCIONE UNA MAYOR PROTECCIÓN



SECRETO OSCURO 2

LOS DIRECTORES DE TI NO SABRÍAN DECIR CÓMO SE CONSUME EL 45 % DE SU ANCHO DE BANDA

Resumen ejecutivo

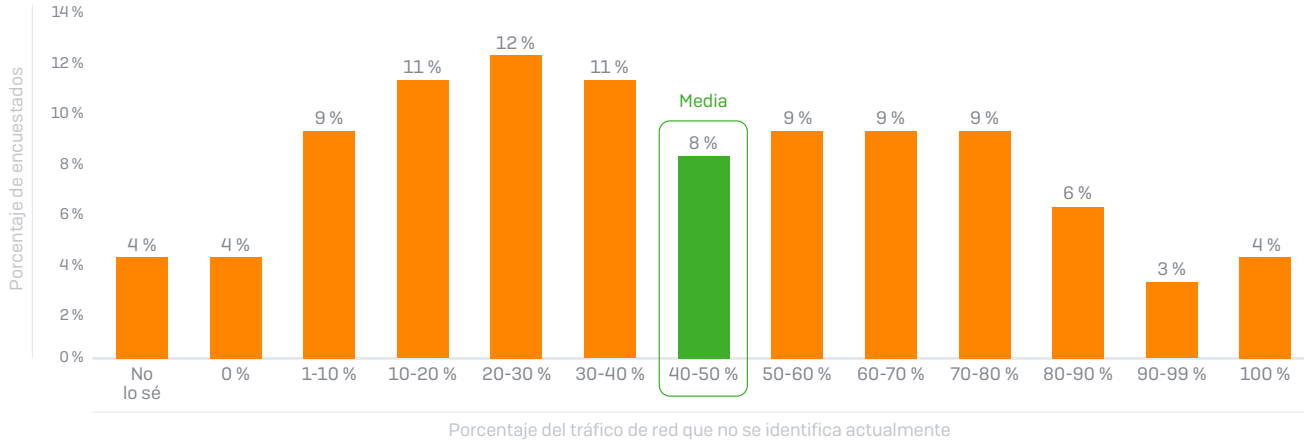
- Un promedio del 45 % del tráfico de red no se identifica. En consecuencia, no puede controlarse.
- Aproximadamente uno de cada cuatro directores informáticos (23 %) no pueden identificar el 70 % del tráfico de sus redes.
- La falta de visibilidad del tráfico de red conlleva preocupaciones en distintos ámbitos:
  - Al 84 % les preocupa la seguridad.
  - Al 52 % les preocupa la productividad.
  - A 4 de cada 10 les preocupa no poder justificar cómo se consume su ancho de banda.
  - Al 42 % les preocupa la responsabilidad legal o el cumplimento normativo debido a contenido potencialmente ilegal o inapropiado.
  - El 50 % han invertido en aplicaciones personalizadas que no pueden priorizar.
- El sector sanitario es el que tiene más problemas con las aplicaciones personalizadas: dos tercios (67 %) tienen aplicaciones personalizadas que su firewall no puede identificar.
- El 85 % de los directores de TI quieren que sus firewalls les proporcionen una mayor visibilidad.

No se puede controlar lo que no se puede ver

Controlar el tráfico de red es un papel fundamental de todo firewall. Hay que ser capaz de priorizar las aplicaciones esenciales, limitar las aplicaciones que no están relacionadas con el trabajo y bloquear las aplicaciones maliciosas como los clientes BitTorrent. El problema es que, si no se ve lo que se ejecuta en la red, no se puede controlar.

La encuesta reveló que el 45 % del tráfico de red actual no se puede identificar, por lo que no se puede controlar. El llamado «control de aplicaciones» sencillamente no es posible en casi la mitad del tráfico. Y para casi uno de cada cuatro directores de TI (23 %) la problemática es todavía mucho mayor, al no poder identificar el 70 % o más del tráfico de su red.

¿QUÉ PORCENTAJE DE SU TRÁFICO DE RED NO SE PUEDE IDENTIFICAR ACTUALMENTE?



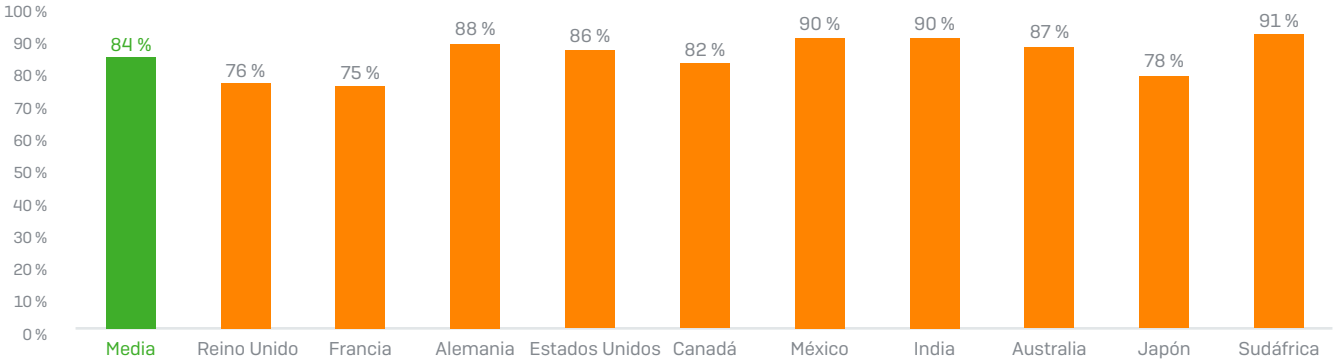
Esto se debe a que la gran mayoría de firewalls convencionales identifica las aplicaciones mediante una detección basada en firmas, de la misma manera en que funciona un software antivirus tradicional. Esto conlleva los mismos problemas que los antivirus tradicionales. En el caso que nos ocupa, las aplicaciones que no se hayan detectado y catalogado anteriormente simplemente no pueden verse y, aunque tengan una firma, muchas aplicaciones no escatiman esfuerzos para modificar sus patrones de red para evitar la detección. Además, muchas aplicaciones han recurrido a camuflarse como navegadores web para evitar su control, ya que casi todos los firewalls habilitan el acceso a Internet para navegar por la red.

Con la falta de protección, la visibilidad también es una cuestión global, aunque el país más afectado es la India, donde el 57 % del tráfico de red no se identifica. En el extremo contrario se encuentra Japón, el país menos afectado, con un tercio de su tráfico de red sin identificar. Probablemente esto se deba a un control con políticas más estrictas, una menor propensión a usar aplicaciones SaaS/en la nube frecuentemente cifradas y una menor tendencia a utilizar aplicaciones no autorizadas.

La falta de visibilidad conlleva preocupaciones en distintos ámbitos:

Seguridad. Si no vemos lo que hay en la red, ¿cómo sabemos si es malicioso, sospechoso o de alto riesgo? ¿Y cómo saber si tenemos usuarios deshonestos cuyo comportamiento expone a la empresa a amenazas de malware o filtraciones? Esa es la razón por la que la seguridad es una preocupación para el 84 % de los encuestados.

% DE ENCUESTADOS QUE OPINAN QUE LA FALTA DE UNA VISIBILIDAD EFICAZ DE LAS APLICACIONES ES MOTIVO DE GRAN PREOCUPACIÓN EN MATERIA DE SEGURIDAD



Productividad. Si uno no ve qué consume su ancho de banda, no puede priorizar las aplicaciones de productividad vitales y reducir el nivel de prioridad de las aplicaciones no relacionadas con el trabajo. Además, uno tampoco obtiene información sobre lo que los usuarios están usando; la pérdida de productividad debido a aplicaciones no deseadas o innecesarias es motivo de preocupación para algo más de la mitad (52 %) de las empresas encuestadas.

Transparencia. En la era actual de «Internet en cualquier lugar» y la prevalencia de las aplicaciones basadas en la nube, el ancho de banda se ha convertido en un activo empresarial fundamental pero también en un gasto económico considerable. Las empresas acuden a sus equipos de TI para que den cuenta de cómo se utiliza este valioso recurso, pero la falta de visibilidad sobre el tráfico de red hace que esto sea prácticamente imposible. Como consecuencia, por término medio, a cuatro de cada diez directores informáticos les preocupa no poder justificar cómo se consume su ancho de banda.

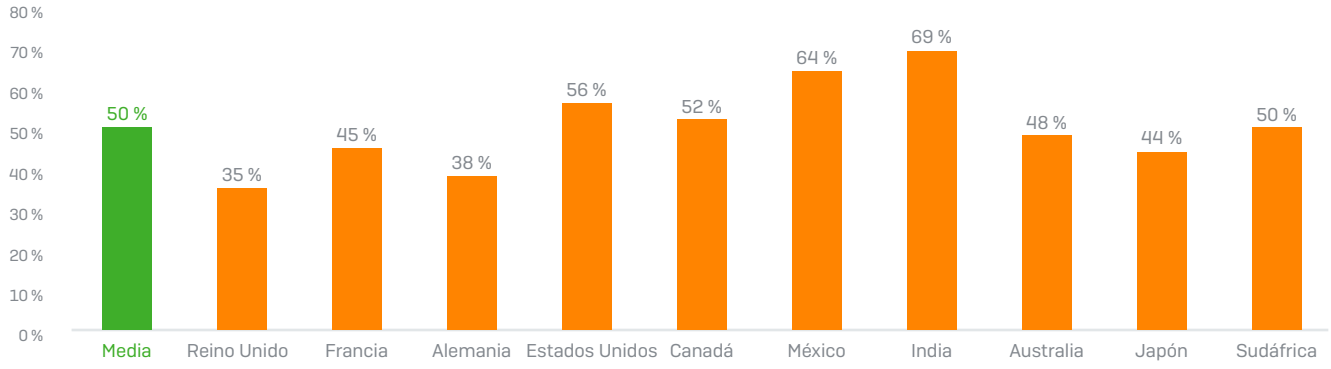
La encuesta reveló diferencias regionales importantes en cuanto a la transparencia. A los que más les preocupa este aspecto es a los directores de TI de la India (61 %) y Sudáfrica (55 %) y, a los que menos, a los de Japón (28 %) y Alemania (30 %). Estas cifras probablemente reflejen las distintas prácticas empresariales existentes en todo el mundo, así como expectativas diferentes en cuanto al cumplimiento de las políticas empresariales.

Cumplimiento y responsabilidad jurídica. Aunque los directores informáticos de los países encuestados se enfrentan a distintas obligaciones legales y de cumplimiento, a todos les preocupa descargar, alojar o distribuir contenido ilegal o inapropiado. De media, el 42 % comparten esta preocupación, con la India (52 %) y el Reino Unido (47 %) a la cabeza de la lista. Sin la capacidad de ver lo que se ejecuta en la red, los directores de TI no pueden garantizar que todo sea legítimo, con lo que sus empresas corren el riesgo de no cumplir las normativas.

Retorno de la inversión (ROI). Las aplicaciones empresariales o verticales personalizadas son cada vez más habituales y suponen una inversión significativa para cualquier empresa. Van desde programas que se han modificado para adaptarse a necesidades concretas de una compañía hasta aplicaciones personalizadas al 100 % creadas a medida para una empresa. La encuesta reveló que el 50 % de las empresas cuentan con aplicaciones en red personalizadas que su firewall no puede identificar. Por consiguiente, no pueden priorizarlas, algo que limita su capacidad de maximizar el ROI derivado de la aplicación y permitir que sus usuarios trabajen con la máxima eficiencia.

El ROI es otro ámbito en el que observamos grandes diferencias entre las regiones. La India, México y EE. UU. tienen un número de aplicaciones personalizadas que no pueden identificar superior a la media, mientras que el Reino Unido es el último de la lista, con un 35 %. Esta variación probablemente refleje las distintas tendencias a la hora de invertir en aplicaciones personalizadas en lugar de aplicaciones listas para usar, además de cuestiones de visibilidad.

% DE ENCUESTADOS CON APLICACIONES PERSONALIZADAS QUE EL FIREWALL NO PUEDE IDENTIFICAR



Todas las industrias tienen problemas con aplicaciones empresariales personalizadas que no pueden identificar, pero el sector sanitario es el que tiene más dificultades. Dos tercios de las entidades sanitarias tienen aplicaciones personalizadas que su firewall no puede identificar y, por lo tanto, no pueden controlar. Es probable que esto se deba a que las entidades sanitarias presentan una mayor tendencia a tener aplicaciones en red personalizadas para atender necesidades específicas, así como una infraestructura anticuada.

El 85 % está de acuerdo: la visibilidad es una prioridad fundamental

Como ya hemos mencionado, uno no puede controlar lo que no puede ver. Es por eso que el 85 % de los directores de TI desean que sus firewalls ofrezcan una mayor visibilidad. Esto les permitiría:

- **Reducir las amenazas de seguridad** al identificar los usuarios y las aplicaciones que suponen un riesgo.
- **Incrementar la productividad** al controlar el tráfico de aplicaciones no relacionadas con el trabajo.
- **Optimizar el ancho de banda** para uso profesional.
- **Minimizar las preocupaciones sobre la responsabilidad legal o el cumplimento normativo** al bloquear el contenido ilegal o inapropiado.
- **Maximizar el ROI** de las aplicaciones empresariales personalizadas.
- **Justificar** el tráfico de red.

> El **85 %** quieren que sus firewalls les proporcionen una mayor visibilidad

SECRETO OSCURO 3

LOS FIREWALLS INEFICACES CUESTAN A LAS EMPRESAS TIEMPO Y DINERO

Resumen ejecutivo

- De media, se tardan 3,3 h en identificar, aislar y reparar los equipos infectados.
- Por término medio, las empresas invierten siete días laborables al mes en reparar los ordenadores infectados.
  - De media, las empresas pequeñas (100 - 1000 usuarios) dedican cinco días laborables al mes a la remediación.
  - De media, las grandes empresas (1001 - 5000 usuarios) dedican diez días laborables al mes a la remediación.
- El 99 % reconocen que sería útil si el firewall pudiera aislar los ordenadores infectados de forma automática.
- El 97 % probablemente comprarían la protección de firewall y de endpoints del mismo fabricante si mejorase las tasas de detección y la respuesta automatizada ante incidentes.

Se pierde más de una semana al mes en reparar los equipos infectados

Como ya hemos visto, los firewalls no proporcionan la protección que necesitan las empresas.
En consecuencia, los equipos de TI dedican mucho tiempo y esfuerzo a arreglar los ordenadores infectados.
Para determinar la magnitud del problema, la encuesta formuló dos preguntas clave:

1. ¿**Cuánto** se tarda, de media, en identificar, aislar y reparar los equipos infectados?
2. Por término medio, ¿de **cuántos** ordenadores infectados se hace cargo su empresa cada mes?

Los resultados fueron sorprendentes.

De media, se tardan 3,3 h (o casi medio día laborable) en identificar, aislar y reparar un equipo infectado.
Es significativo observar que las empresas pequeñas tardan menos tiempo que las grandes, con una media de 2,9 h en las empresas de 100 - 1000 usuarios, hasta 3,9 h en las de 1001 - 5000 usuarios.

> **7 días** se invierten en reparar ordenadores infectados cada mes (sobre la base de una jornada de 7,5 h)

Las empresas se ven afectadas por una media de 16 ordenadores infectados al mes. Basándonos en una jornada de 7,5 h, esto significa que cada mes dedican 7 días laborables a resolver infecciones.

Tamaño de la empresa	Núm. de equipos infectados al mes	Horas para limpiar un ordenador	Número total de horas de limpieza al mes	Núm. de días al mes (7,5 horas = jornada)
100 – 1000	13	2,8	36,4	4,9
1001 – 5000	20	3,9	78	10,4
Media	16	3,3	52,8	7,04

Al tener en cuenta las implicaciones de este tiempo de limpieza, tenemos que considerar el tiempo inmediato y el coste de recursos, pero también el coste de oportunidad: ¿qué podría estar haciendo el equipo de TI si no tuviera que limpiar? Los equipos de TI tienen cada vez más presión, tanto por una mayor demanda de su tiempo como por una notable escasez de conocimientos sobre seguridad informática. El 70 % de los profesionales de la ciberseguridad afirma que su empresa se ha visto afectada por la falta de conocimientos en esta materia[i]. La mayoría no puede permitirse el lujo de invertir siete días al mes en limpiar los ordenadores infectados.

Teniendo en cuenta las consecuencias de tiempo y costes de reparar los equipos infectados de forma manual, no es de extrañar que el 99 % de los directores de TI quieran que su firewall aísle los sistemas comprometidos automáticamente y que el 90 % opine que sería «sumamente» o «muy» útil. Un porcentaje similar (97 %) probablemente compraría la protección de firewall y de endpoints del mismo fabricante para beneficiarse de una mejora en las tasas de detección y en la respuesta automatizada ante incidentes.

Conclusión

Hemos destapado los secretos más oscuros de los firewalls de red de hoy día: no consiguen proporcionar las funciones clave que necesitan las empresas. Desde la protección de red hasta la visibilidad y la respuesta, las experiencias actuales de los directores de TI quedan muy por debajo de lo que desean y necesitan para proteger sus empresas. En vista de ello, es hora de que las empresas analicen nuevamente su seguridad de red e implementen soluciones que se ajusten mejor a sus necesidades.

[i] *The Life and Times of Cybersecurity Professionals. The Enterprise Strategy Group, 2017*

Lecturas recomendadas

- Monográfico Prácticas recomendadas con firewalls para bloquear el ransomware: se explica cómo tuvieron lugar ataques de ransomware recientes como WannaCry y Petya y las funciones que necesitan los firewalls para detener estos tipos de ataque.
- Monográfico Por qué los administradores de red necesitan una visibilidad completa de las aplicaciones: análisis exhaustivo de las dificultades de la visibilidad del tráfico de red y qué se puede hacer para solucionarlas.
- Guía para la adquisición de firewalls: tecnologías y funciones clave que hay que tener en cuenta al seleccionar un firewall, así como las preguntas que formular a los proveedores.

Sophos XG Firewall: soluciona los problemas de los firewalls de red

Sophos XG Firewall está diseñado para satisfacer las necesidades cambiantes de los directores de TI y aborda los desafíos clave a los que se enfrentan los firewalls de hoy día.

- **Protección.** XG Firewall detiene las amenazas desconocidas con una completa suite de protección avanzada que incluye Deep Learning, IPS, ATP, espacios seguros y AV dual.
- **Visibilidad.** XG Firewall expone riesgos ocultos con la visibilidad de todas las aplicaciones, usuarios de mayor riesgo, amenazas avanzadas, cargas sospechosas y mucho más.
- **Respuesta.** XG Firewall responde automáticamente ante incidentes identificando y aislando al instante los sistemas infectados hasta que puedan limpiarse.

Eche un vistazo a estos enlaces para ver el reconocimiento que ha recibido XG Firewall:

- NSS Labs – «Entre los mejores»
- SC Media – «Una convergencia muy creativa de numerosas y sólidas funciones»
- PC Pro – «Un dispositivo UTM muy versátil que combina máximo rendimiento con una increíble relación calidad-precio»

Para obtener más información y empezar a probarlo gratis, vaya a es.sophos.com/xgfirewall.

Ventas en España:
Tel.: (+34) 91 375 67 56
Email: comercialES@sophos.com

Ventas en Latin America:
Email: Latamsales@sophos.com

4-4-18 NA-ES [TN]

SOPHOS