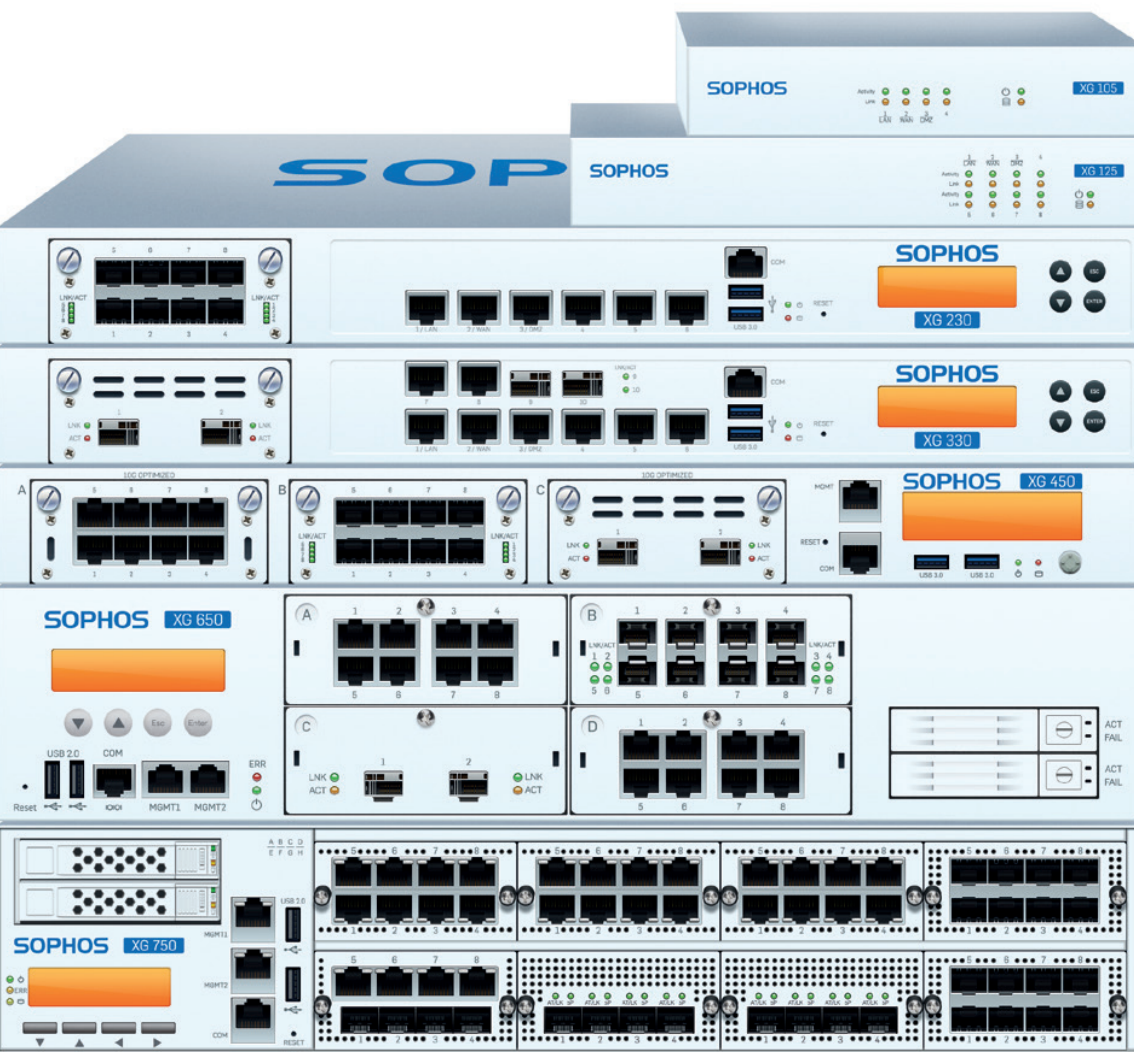


Guía de tamaños

Sophos XG Firewall – Dispositivos de la serie XG



Guía de dimensionamiento de Sophos Firewall OS 15.01.1 para dispositivos de la serie XG

Especificar el modelo de dispositivo adecuado en tres pasos

Este documento ofrece orientación para elegir el dispositivo Sophos de la serie XG más adecuado para su cliente. Para especificar el dispositivo adecuado, es necesario tener en cuenta una serie de factores y crear un perfil de uso de los usuarios y el entorno de red.

Para obtener los mejores resultados, recomendamos utilizar el procedimiento siguiente:

1. **Determine el número "Total de usuarios de UTM"**Estudie el entorno del cliente, por ejemplo, las costumbres de navegación por Internet, las aplicaciones utilizadas y la infraestructura de redes y servidores, para conseguir una idea precisa del uso que se hará de un dispositivo de la serie XG en horas punta.
2. **Realice un cálculo inicial aproximado**Basado en el número "Total de usuarios ponderados".
3. **Revise los requisitos de rendimiento específicos**Analice si algún factor local (por ejemplo, la capacidad máxima disponible de enlace ascendente a Internet) puede afectar al rendimiento. Compare los resultados con las tasas de rendimiento de Sophos XG Firewall y ajuste la recomendación según corresponda.

Evidentemente, la mejor forma de averiguar si un dispositivo se ajusta a las necesidades de un cliente es probarlo en el entorno y, con Sophos XG Firewall, puede ofrecer una evaluación gratuita en las instalaciones de la unidad elegida.

1. Determine el número "Total de usuarios ponderados"

Utilice la tabla siguiente para calcular en primer lugar el número "Total de usuarios ponderados" que deberá soportar el dispositivo.

- a. Calcule el número "Suma ponderada de usuarios". Determine la categoría de usuarios [Normal/Avanzado/Extremo] que mejor se ajuste al comportamiento medio de los usuarios o calcule cuántos usuarios se corresponden con cada categoría. Utilice los criterios de la tabla 1.2 para clasificar los tipos de usuarios.
 - Introduzca los totales de usuarios en la tabla 1.1, multiplíquelos por el factor indicado, introduzca los resultados en las casillas "Suma ponderada de usuarios" e indique el total en la casilla "Suma ponderada total de usuarios".
- b. Determine el número de carga del sistema. Utilice los criterios de la tabla 1.3 para clasificar la carga.
 - Introduzca el número de carga del sistema en la casilla "multiplicado por carga del sistema" de la tabla 1.1, multiplíquelo por la "Suma ponderada total de usuarios" e indique el resultado en la casilla "Total de usuarios ponderados".

1.1

Nombres de licencias	Total de usuarios	Multiplicado por	Suma ponderada de usuarios
Usuario estándar		1	
Usuarios avanzados		1,2	
Usuarios avanzados		1,5	
Suma total de usuarios		Suma ponderada total de usuarios	
		multiplicado por carga del sistema	
		Total de usuarios ponderados	

1.2 Criterios de las categorías de usuarios

Utilice los criterios que se describen a continuación para clasificar los tipos de usuarios.

	Usuario medio	Usuario avanzado (x 1,2)	Usuario extremo (x 1,5)
Uso del correo electrónico (por jornada laboral de 10 horas)			
Número de mensajes recibidos en el buzón	< 50	De 50 a 100	>100
Volumen de datos	Pocos Mbytes	Múltiples MBytes	Gran cantidad de MBytes
Uso de Internet (por jornada laboral de 10 horas)			
Volumen de datos	Pocos Mbytes	Múltiples MBytes	Gran cantidad de MBytes
Patrón de uso	Repartido de forma equitativa a lo largo del día	Varios picos	Muchos picos
Aplicaciones web utilizadas	Principalmente correo web, Google, noticias	Navegación por Internet cuantiosa, transferencia multimedia moderada, aplicaciones empresariales	Navegación por Internet y transferencias multimedia intensas (colegios, universidades)
Uso de VPN			
Acceso remoto a VPN	Poco habitual, conexiones esporádicas	Varias veces a la semana, conexiones a las mismas horas	Todos los días, conexión casi constante

1.3 Criterios de la carga del sistema

Identifique todos los requisitos específicos que puedan aumentar la carga general del sistema y, por consiguiente, los requisitos de rendimiento.

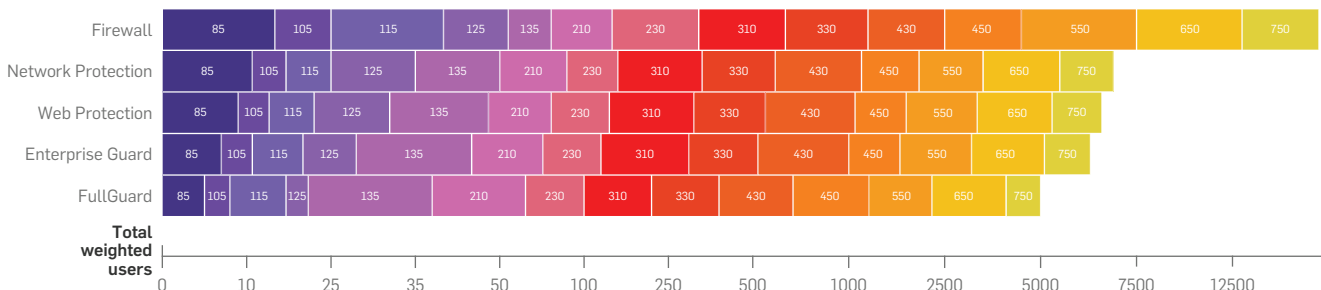
	Uso normal del sistema	Uso avanzado del sistema (x 1,2)	Uso intensivo del sistema (*1,5)
Autenticación			
Active Directory en uso	No	Sí	Sí
Uso del cortafuegos/IPS/VPN			
El IPS debe proteger sistemas diversos	No es necesaria protección con IPS	Principalmente ordenadores personales de Windows, 1-2 servidores	Varios sistemas operativos cliente, navegadores y aplicaciones multimedia, más de 2 servidores
Correo electrónico			
Porcentaje de correo no deseado	<50%	50-90%	>90%
Informes			
Requisitos de precisión y tiempo de almacenamiento de informes	Informe web de hasta 1 mes solamente (por dominio)	Hasta 3 meses Hasta 5 informes (por dominio)	> 3 meses (por dirección web)
Tiempo de almacenamiento contable en el dispositivo	No	Hasta 1 mes	> 1 mes

2. Realice un cálculo inicial aproximado utilizando la suma ponderada total de usuarios obtenida

Utilice la suma ponderada total de usuarios y realice un primer cálculo aproximado del dispositivo de hardware de la serie SG necesario en el diagrama siguiente:

- Cada línea indica el rango de usuarios recomendado al utilizar solamente esa suscripción.
- Asegúrese de que todas las cantidades incluyen los usuarios conectados a través de VPN, RED y puntos de acceso inalámbricos.

Perfil de suscripción



Regla general

- Tenga en cuenta que, al añadir protección de servidores web o correo electrónico a cualquiera de los perfiles de suscripción mencionados anteriormente, el rango disminuirá en un 5-10% por módulo.

3. Revise los requisitos de rendimiento específicos

Según el entorno de cada cliente, pueden existir requisitos de rendimiento específicos que exijan un ajuste del cálculo inicial con una unidad superior (o incluso inferior).

Dichos requisitos suelen basarse en los dos factores siguientes:

La capacidad máxima disponible de enlace ascendente a Internet

La capacidad de la conexión a Internet del cliente (enlace ascendente y descendente) debería coincidir con la tasa media de rendimiento que puede ofrecer la unidad elegida (dependiendo de las suscripciones utilizadas).

Por ejemplo, si el límite de carga o descarga es 20 Mbps, usar un dispositivo XG 230 en lugar de un XG 210 no aportaría grandes ventajas, a pesar de que el número total de usuarios calculado sea aproximadamente 100. En ese caso, podría ser suficiente un dispositivo XG 210, ya que puede cubrir perfectamente el enlace a Internet completo incluso con todas las funciones de UTM activadas.

Sin embargo, es posible que los datos no se filtren solamente al salir a Internet, sino también entre los segmentos de red internos. Por lo tanto, durante la evaluación, es importante tener en cuenta el tráfico interno que atraviesa el firewall.

Requisitos de rendimiento específicos basados en la experiencia y los conocimientos del cliente

Si el cliente conoce los requisitos generales de rendimiento de todas las interfaces internas y externas conectadas (por ejemplo, basándose en experiencias anteriores), compruebe si la unidad elegida puede cumplirlos.

Por ejemplo, el cliente puede contar con varios servidores ubicados en un DMZ y querer que el IPS inspeccione todo el tráfico que llegue a ellos desde cualquier segmento de la red. O puede que el cliente tenga muchos segmentos de red diferentes que deban protegerse entre sí (utilizando el filtrado de paquetes del FW o la función de restricción de aplicaciones). En este caso, tenga en cuenta que la unidad debe escanear todo el tráfico interno entre todos los segmentos.

Guía de tamaños

Estas son otras preguntas que puede hacer al cliente para averiguar si existen otros requisitos de rendimiento:

- ¿Cuántos túneles VPN sitio-a-sitio son necesarios?
- ¿Cuántos mensajes de correo electrónico se transfieren por hora, por término medio, en horas punta?
- ¿Qué cantidad de tráfico web [Mbps y solicitudes por segundo] se genera, por término medio, en horas punta?
- ¿Cuántos servidores web deben protegerse y qué cantidades de tráfico se prevén, por término medio, en horas punta?

La sección siguiente ofrece cantidades de rendimiento detalladas para ayudarle a determinar si los dispositivos elegidos cumplen los requisitos individuales.

Rendimiento del hardware Sophos de la serie XG

La tabla siguiente refleja las cifras de rendimiento por tipo de tráfico según las mediciones realizadas en los laboratorios de pruebas de Sophos. Las cantidades del mundo real representan valores de rendimiento que se pueden alcanzar con una combinación de tráfico normal y real, según lo definido por NSS Labs. Las cantidades máximas representan el mejor rendimiento que se puede alcanzar en condiciones perfectas, por ejemplo, utilizando paquetes de gran tamaño solo con tráfico UDP y con plena carga de CPU.

Recuerde que no garantizamos ninguna de estas cantidades, ya que el rendimiento puede variar en situaciones reales según las características de los usuarios, el uso de aplicaciones, la configuración de la seguridad y otros factores. Por lo tanto, estas cantidades solo deben utilizarse como una guía aproximada para el dimensionamiento.

Pequeño - Escritorio

Modelo	XG 85/w rev.1	XG 105/w rev.2	XG 115/w rev.2	XG 125/w rev.2	XG 135/w rev.2
Rendimiento					
Firewall, máx.¹ (Mbps)	2.000	3.000	3.500	5.000	7.000
Firewall, IMIX (Mbps)	780	1.040	1.330	1.750	2.750
Firewall, mundo real² (Mbps)	360	430	580	750	1.500
Firewall, máx.¹ (paquetes por segundo)	162.500	243.800	284.500	406.000	569.000
IPS, máx.³ (Mbps)	510	700	900	1.040	1.750
IPS, mundo real² (Mbps)	75	86	103	180	232
Proxy web, AV⁵ (Mbps)	330	430	520	590	1.400
Proxy web, AV mundo real² (Mbps)	75	187	234	307	427
IPS + proxy web, AV mundo real² (Mbps)	31	36	42	58	95
NGFW (IPS + App Ctrl + WebFilter), máx.³ (Mbps)	235	270	310	360	880
NGFW (IPS + App Ctrl + WebFilter), mundo real² (Mbps)	25	27	30	75	133
VPN AES, máx.³ (Mbps) varios túneles/núcleos	200	300	350	410	950
VPN AES, máx.³ (Mbps) un túnel/núcleo	200	250	290	290	600
VPN AES, mundo real² (Mbps) varios túneles/núcleos	50	75	90	105	240
WAF Adv. Profile, máx.⁶ (Mbps)	N/A ⁶	12	18	22	44
Conexiones máximas recomendadas					
Conexiones TCP nuevas/seg.	12.000	27.500	27.500	35.000	82.000
Conexiones TCP simultáneas	2.000.000	3.200.000	6.000.000	6.200.000	8.200.000
Túneles VPN IPSec simultáneos	200	300	500	750	1.000
Túneles VPN SSL simultáneos	100	200	240	270	270
Puntos de acceso concurrentes	5	10	20	30	40
RED concurrentes (UTM/FW)⁴	5/10	10/30	15/60	20/80	25/100
Servidores virtuales concurrentes WAF	60 ⁷	60 ⁷	60 ⁷	60 ⁷	60 ⁷
WAF máx., conexiones/s	700	750	780	950	2.600

1. Tamaño de paquete 1518 bytes (UDP).

2. Promedio de combinaciones de protocolos de centros de datos, perímetros empresariales, educación superior, dispositivos móviles europeos y redes financieras a un 50% de uso de CPU

3. Tráfico HTTP

4. UTM=Escaneo completo de contenido de tráfico RED en dispositivo XG, FW=solo filtrado de paquetes

5. Archivos de 512 KBytes

6. AV + todos los filtros de amenazas comunes activados (sin AV en XG85)

7. Límite de codificación fija

Medio - 1U

Modelo	XG 210 rev.2	XG 230 Rev.1	XG 310 Rev.1	XG 330 Rev.1	XG 430 Rev.1	XG 450 Rev.1
Rendimiento						
Firewall , máx.¹ (Mbps)	14.000	18.000	25.000	30.000	37.000	45.000
Firewall, IMIX (Mbps)	4.900	6.110	8.530	11.230	12.950	15.650
Firewall, mundo real² (Mbps)	2.060	2.250	3.800	6.100	6.900	7.650
Firewall , máx.¹ (paquetes por segundo)	1.137.800	1.463.000	2.031.860	2.438.200	3.007.200	3.657.400
IPS, máx.³ (Mbps)	2.700	4.200	5.500	8.500	9.000	10.000
IPS, mundo real² (Mbps)	309	361	539	733	893	1.159
Proxy web, AV⁵ (Mbps)	2.300	2.800	3.260	6.000	6.500	7.000
Proxy web, AV mundo real² (Mbps)	538	670	1.140	1.220	1.440	1.690
IPS + proxy web, AV mundo real² (Mbps)	102	107	207	242	372	463
NGFW (IPS + App Ctrl + WebFilter), máx.³ (Mbps)	1.700	2.420	2.700	4.220	4.800	5.000
NGFW (IPS + App Ctrl + WebFilter), mundo real² (Mbps)	176	226	340	425	538	693
VPN AES, máx.³ (Mbps) varios túneles/núcleos	1.350	1.500	2.500	3.200	4.800	5.500
VPN AES, máx.³ (Mbps) un túnel/núcleo	760	950	990	920	950	990
VPN AES, mundo real² (Mbps) varios túneles/núcleos	340	375	625	800	1.200	1.375
WAF Adv. Profile, máx.⁶ (Mbps)	205	240	260	510	560	620
Conexiones máximas recomendadas						
Conexiones TCP nuevas/seg.	135.000	140.000	200.000	200.000	200.000	200.000
Conexiones TCP simultáneas	8.200.000	8.200.000	17.500.000	17.500.000	20.000.000	20.000.000
Túneles VPN IPSec simultáneos	1.300	1.600	1.800	2.500	3.000	3.500
Túneles VPN SSL simultáneos	300	300	300	300	350	350
Puntos de acceso concurrentes	75	100	125	150	230	250
RED concurrentes (UTM/FW)⁴	30/125	40/150	50/200	60/230	70/250	80/300
Servidores virtuales concurrentes WAF	60 ⁷	60 ⁷	60 ⁷	60 ⁷	60 ⁷	60 ⁷
WAF máx., conexiones/s	3.700	4.200	5.000	9.000	14.000	15.500

1. Tamaño de paquete 1518 bytes (UDP).

2. Promedio de combinaciones de protocolos de centros de datos, perímetros empresariales, educación superior, dispositivos móviles europeos y redes financieras a un 50% de uso de CPU

3. Tráfico HTTP

4. UTM=Escaneo completo de contenido de tráfico RED en dispositivo XG, FW=solo filtrado de paquetes

5. Archivos de 512 KBytes

6. AV + todos los filtros de amenazas comunes activados (sin AV en XG85)

7. Límite de codificación fija

Grande - 2U

Modelo	XG 550 Rev.1	XG 650 Rev.1	XG 750 Rev.1
Rendimiento			
Firewall , máx.¹ (Mbps)	60.000	80.000	120.000
Firewall, IMIX (Mbps)	21.500	26.990	33.500
Firewall, mundo real² (Mbps)	11.700	15.000	19.000
Firewall , máx.¹ (paquetes por segundo)	4.876.500	6.502.000	9.752.900
IPS, máx.³ (Mbps)	13.000	20.000	22.000
IPS, mundo real² (Mbps)	2.160	3.310	3.970
Proxy web, AV⁵ (Mbps)	10.000	13.000	17.000
Proxy web, AV mundo real² (Mbps)	2.480	3.220	3.870
IPS + proxy web, AV mundo real² (Mbps)	808	1.109	1.330
NGFW (IPS + App Ctrl + WebFilter), máx.³ (Mbps)	8.000	9.000	11.800
NGFW (IPS + App Ctrl + WebFilter), mundo real² (Mbps)	1.190	1.730	2.070
VPN AES, máx.³ (Mbps) varios túneles/núcleos	8.400	9.000	11.250
VPN AES, máx.³ (Mbps) un túnel/núcleo	640	770	620
VPN AES, mundo real² (Mbps) varios túneles/núcleos	2.100	2.250	2.800
WAF Adv. Profile, máx.⁶ (Mbps)	1.020	1.700	2.460
Conexiones máximas recomendadas			
Conexiones TCP nuevas/seg.	200.000	200.000	300.000
Conexiones TCP simultáneas	20.000.000	20.000.000	30.000.000
Túneles VPN IPSec simultáneos	4.000	4.500	5.400
Túneles VPN SSL simultáneos	400	500	500
Puntos de acceso concurrentes	300	400	500
RED concurrentes (UTM/FW)⁴	100/400	150/600	200/600*
Servidores virtuales concurrentes WAF	60 ⁷	60 ⁷	60 ⁷
WAF máx., conexiones/s	18.000	21.000	24.000

*Límite técnico

1. Tamaño de paquete 1518 bytes (UDP).

2. Promedio de combinaciones de protocolos de centros de datos, perímetros empresariales, educación superior, dispositivos móviles europeos y redes financieras a un 50% de uso de CPU

3. Tráfico HTTP

4. UTM=Escaneo completo de contenido de tráfico RED en dispositivo XG, FW=solo filtrado de paquetes

5. Archivos de 512 KBytes

6. AV + todos los filtros de amenazas comunes activados (sin AV en XG85)

7. Límite de codificación fija

Dispositivos de software/virtuales de Sophos XG Firewall

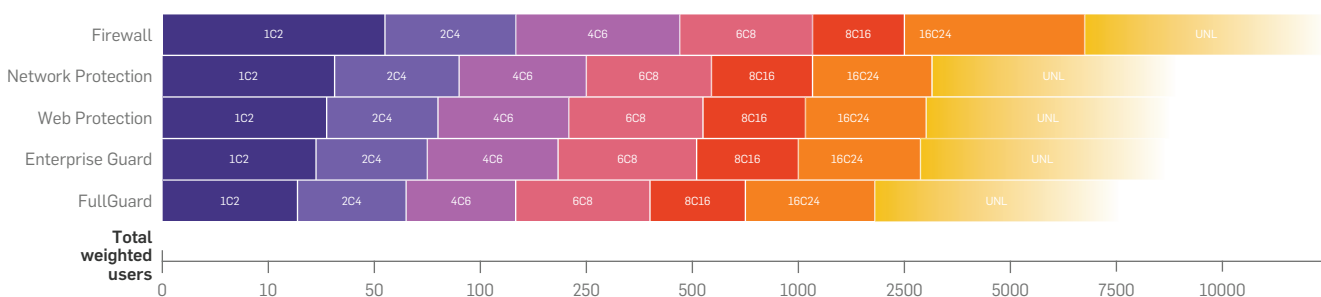
Los dispositivos de software/virtuales de Sophos XG Firewall son licencias por número de núcleos (virtuales) y tamaño de RAM (virtual). Las licencias no tienen que coincidir con el número de núcleos/RAM disponibles, pero solo activarán los núcleos/RAM con licencia que se utilizarán en el software.

Si bien los dispositivos de software/virtuales pueden utilizarse en varios tipos de CPU con distintas velocidades, el rendimiento puede variar de forma significativa si se utiliza el mismo número de núcleos/tamaño de RAM.

El siguiente diagrama ofrece una orientación básica de los rangos del total de usuarios ponderados (según el cálculo del capítulo 1) recomendados para cada modelo de software.

Las cantidades se basan en las siguientes suposiciones:

- Velocidad de CPU = 2,5 GHz (una mayor velocidad puede aumentar notablemente el rendimiento para la mayoría de aplicaciones)
- Tipo de CPU = Core I (hasta 6C8), Xeon (8C16 y superior)



Perfil de suscripción

Regla general

- A causa del marco de hipervisor, se calcula que el uso de Sophos XG Firewall en entornos virtuales disminuye el rendimiento/número de usuarios en alrededor del 10%.

Evaluaciones en las instalaciones

A pesar de que el procedimiento descrito anteriormente es una buena base para seleccionar el modelo más adecuado, está basado solamente en la información proporcionada por el cliente. Existen muchos factores que afectan al comportamiento y al rendimiento de un dispositivo y que solo pueden evaluarse en una situación real. Por lo tanto, las evaluaciones locales en el entorno del cliente son siempre la mejor forma de determinar si el dispositivo elegido cumple realmente los requisitos de rendimiento. Para obtener más ayuda con los tamaños y elegir la plataforma adecuada, los equipos de ventas de Sophos están siempre a su disposición.

Pruébalo gratis hoy mismo

Regístrese en sophos.com/es-es/products para probarlo gratis durante 30 días.

