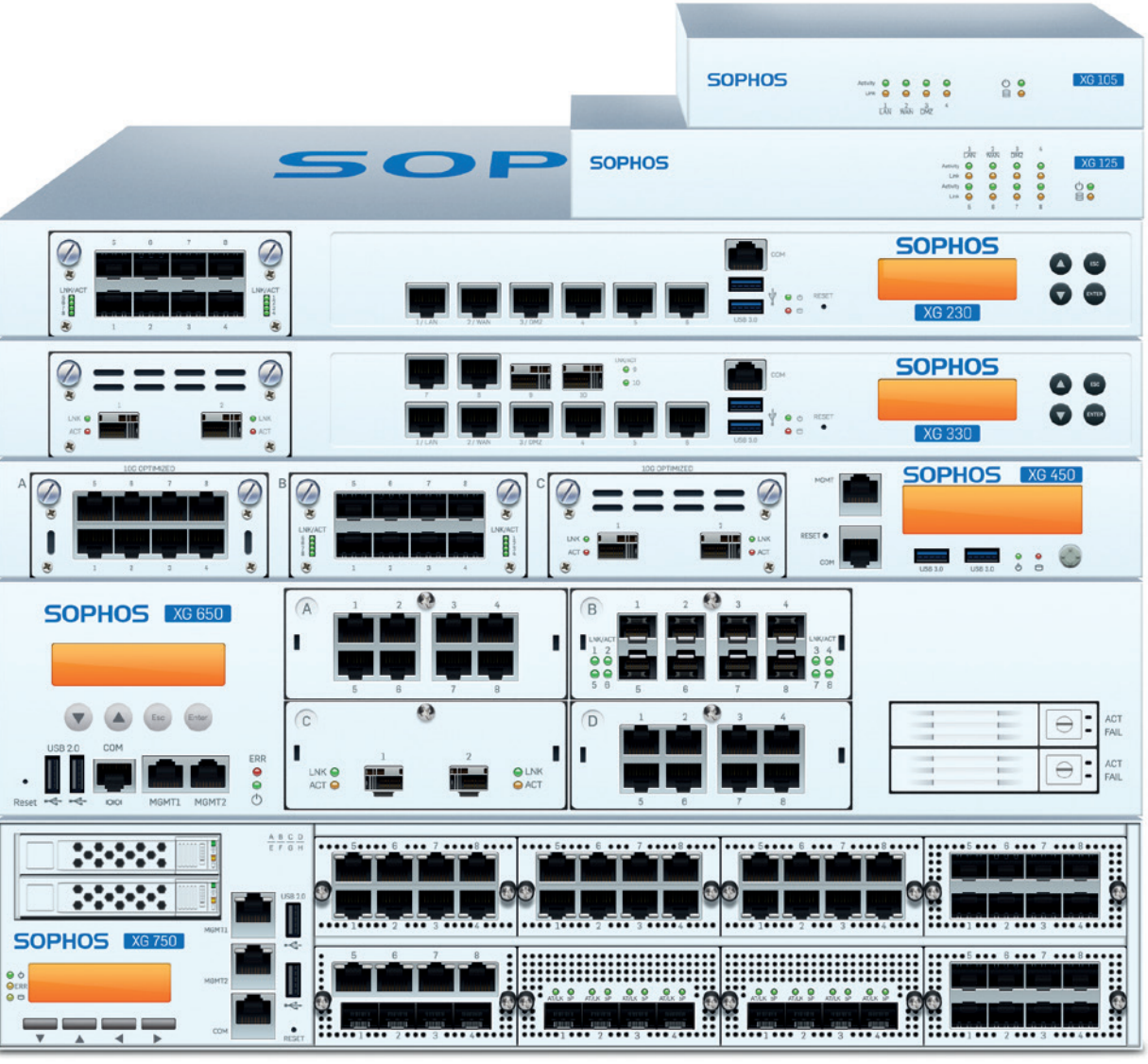
SOPHOS
Security made simple.

Sizing Guide

Sophos XG Firewall – XG Series Appliances



In drei Schritten zum richtigen Appliance-Modell

Mit diesem Leitfaden können Sie bestimmen, welches Appliance-Modell der Sophos XG Serie das richtige für Ihren Kunden ist. Um entscheiden zu können, welches Appliance-Modell am besten geeignet ist, müssen verschiedene Faktoren bedacht werden. Daher sollten Sie ein Nutzungsprofil der Benutzer und der Netzwerkumgebung erstellen.

Für optimale Ergebnisse empfehlen wir Ihnen, nach den folgenden Schritten vorzugehen:

1. **Ermitteln Sie die „gewichtete Gesamtzahl der Benutzer“**
   Hierbei handelt es sich nicht um die tatsächliche Anzahl der Benutzer, sondern um einen speziell errechneten Wert, der die gewichtete Benutzerzahl sowie die Systembelastung berücksichtigt.
2. **Bestimmen Sie, welche Appliance voraussichtlich die richtige ist**
   Hierbei handelt es sich um eine vorläufige Entscheidung, die auf der errechneten „gewichteten Gesamtzahl der Benutzer“ basiert.
3. **Prüfen Sie, ob es besondere Durchsatzanforderungen gibt**
   Ermitteln Sie, ob bestimmte Vorort-Faktoren (z. B. maximal verfügbare Internet-Uplink-Kapazität) die Performance beeinflussen werden. Vergleichen Sie das Ergebnis mit den Durchsatzwerten unserer Appliances und passen Sie Ihre Entscheidung ggf. entsprechend an.

Um festzustellen, ob eine Appliance die Bedürfnisse des jeweiligen Kunden erfüllt, ist es natürlich immer am besten, direkt in der Kundenumgebung zu testen. Mit der Sophos XG Firewall können Sie einen solchen Vorort-Test für das ausgewählte Modell kostenlos anbieten.

1. „Gewichtete Gesamtzahl der Benutzer“ ermitteln

Errechnen Sie in Tabelle 1.1 die von der Appliance zu verarbeitende „gewichtete Gesamtzahl der Benutzer“.

a. Errechnen Sie die gewichtete Benutzerzahl: Ermitteln Sie die Benutzerkategorie (durchschnittlich/stärker/intensiv), die dem üblichen Verhalten der Benutzer am ehesten entspricht, oder schätzen Sie, wie viele Benutzer den einzelnen Kategorien jeweils zuzuordnen sind. Nutzen Sie für die Zuordnung die Kriterien in Tabelle 1.2.

- Tragen Sie die ermittelten Benutzerzahlen der einzelnen Kategorien in Tabelle 1.1 ein. Multiplizieren Sie die Benutzerzahlen mit dem jeweils angeführten Faktor und tragen Sie die Ergebnisse in die Felder der Spalte „Gewichtete Benutzerzahl“ ein. Anschließend addieren Sie alle Werte und notieren das Ergebnis hinter dem Feld „Summe gewichtete Benutzerzahl“.

b. Ermitteln Sie die Systembelastung: Verwenden Sie dazu die Kriterien in Tabelle 1.3.

- Tragen Sie den Faktor der Systembelastung (durchschnittlich *1, stärker *1,2, intensiv *1,5) in Tabelle 1.1 in das Feld hinter „multipliziert mit Systembelastung“ ein. Multiplizieren Sie diesen Faktor mit der „Summe gewichtete Benutzerzahl“ und tragen Sie das Ergebnis in das Feld „Gewichtete Gesamtzahl der Benutzer“ ein.

Tabelle 1.1

Lizenznamen	Benutzerzahl	Multipliziert mit	Gewichtete Benutzerzahl
Durchschnittliche Nutzung		1	
Stärkere Nutzung		1,2	
Intensive Nutzung		1,5	
Benutzerzahl gesamt		Summe gewichtete Benutzerzahl	
		multipliziert mit Systembelastung	
		Gewichtete Gesamtzahl der Benutzer	

Tabelle 1.2 Kriterien Benutzerkategorie

Verwenden Sie zur Klassifizierung der Benutzertypen die unten aufgeführten Kriterien.

	Durchschnittliche Nutzung	Stärkere Nutzung (*1,2)	Intensive Nutzung (*1,5)
E-Mail-Nutzung (an einem 10-Stunden-Arbeitstag)			
Anzahl E-Mails im Posteingang	Weniger als 50	50 bis 100	Mehr als 100
Datenvolumen	Wenige Megabytes	Mehrere Megabytes	Viele Megabytes
Internetnutzung (an einem 10-Stunden-Arbeitstag)			
Datenvolumen	Wenige Megabytes	Mehrere Megabytes	Viele Megabytes
Verwendungsmuster	Gleichmäßig über den Tag verteilt	Mehrere Spitzen	Viele Spitzen
Verwendete Webanwendungen	Hauptsächlich webbasierte E-Mails/ Google/News	Hohes Surfaufkommen, moderate Medienübertragungen, Geschäftsanwendungen	Intensives Surfen und intensive Medienübertragungen (Schulen, Universitäten)
VPN-Nutzung			
Nutzung von VPN-Remotezugriff	Selten – sporadisch verbunden	Mehrmals wöchentlich – regelmäßig verbunden	Täglich – meistens verbunden

Tabelle 1.3 Kriterien Systembelastung

Ermitteln Sie, ob bestimmte Faktoren die Systembelastung möglicherweise erhöhen und demzufolge auch die Leistungsanforderungen an das System beeinflussen können.

	Durchschnittliche Systemnutzung	Stärkere Systemnutzung (*1,2)	Intensive Systemnutzung (*1,5)
Authentifizierung			
Active Directory-Nutzung	Nein	Ja	Ja
FW-/IPS-/VPN-Nutzung			
Diverse Systeme über IPS zu schützen	Kein IPS-Schutz erforderlich	Größtenteils Windows-PCs, 1–2 Server	Diverse Client-Betriebssysteme, Browser und Multimedia-Apps, mehr als 2 Server
E-Mail			
Spamanteil	< 50 %	50–90 %	Mehr als 90%
Reporting			
Vorhaltezeit und Detailliertheit der Reports	Bis zu 1 Monat nur Webreports (pro Domäne)	Bis zu 3 Monate Bis zu 5 Reports (pro Domäne)	Mehr als 3 Monate (je URL)
Vorhaltezeit der Nutzungsdaten	Nein	Bis zu 1 Monat	Mehr als 1 Monat

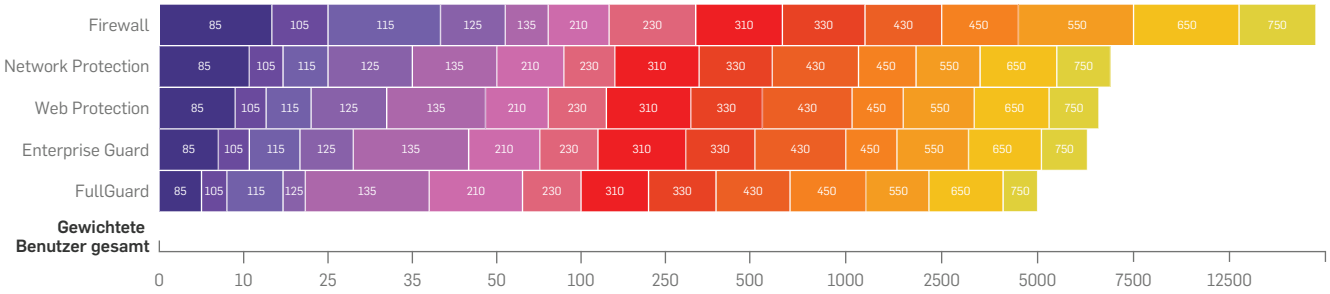
2. Die richtige Appliance bestimmen – basierend auf der errechneten „gewichteten Gesamtzahl der Benutzer“

Mit Hilfe des unten stehenden Diagramms können Sie bestimmen, welche Hardware Appliance für Ihren Kunden voraussichtlich die richtige ist:

- Die einzelnen Zeilen zeigen die empfohlene Appliance für die jeweilige Subscription.
- Wichtig: Achten Sie darauf, dass Sie bei allen Werten auch die Benutzer berücksichtigen, die sich über VPN, RED und Wireless Access Points verbinden.

Subscription-Profil

Faustregel:



- Durch das Hinzufügen von Webserver Protection oder Email Protection zu den oben genannten Subscription-Profilen verringert sich die empfohlene „gewichtete Gesamtzahl der Benutzer“ um jeweils 5–10 %.

3. Prüfen, ob es besondere Durchsatzanforderungen gibt

Je nach Kundenumgebung können sich besondere Durchsatzanforderungen ergeben, aufgrund derer Sie Ihre in Schritt 2 getroffene Entscheidung anpassen müssen. Je nach den Anforderungen kann ein Modell mit höherer (oder geringerer) Leistung benötigt werden als anfänglich gedacht.

Diese Durchsatzanforderungen ergeben sich meist aus den folgenden zwei Faktoren:

Maximal verfügbare Internet-Uplink-Kapazität

Die Kapazität der kundenseitigen Internetverbindung (Up- und Downlink) sollte der durchschnittlichen Durchsatzrate entsprechen, die das gewählte Modell weiterleiten kann (abhängig von den verwendeten Subscriptions).

Beträgt beispielsweise das Download- oder Uploadlimit nur 20 MBit/s, bietet der Einsatz einer XG 230 anstelle einer XG 210 nur wenige Vorteile – obwohl die errechnete Gesamtzahl der Benutzer bei etwa 100 liegt. In diesem Fall ist möglicherweise sogar eine XG 210 ausreichend, da sie selbst bei Aktivierung aller UTM-Funktionen die gesamte Internetverbindung optimal ausfüllen kann.

Allerdings werden Daten unter Umständen nicht nur auf ihrem Weg ins Internet gefiltert, sondern auch zwischen internen Netzwerksegmenten. Berücksichtigen Sie daher auch internen Datenverkehr, der die Firewall durchläuft.

Besondere Leistungsanforderungen basierend auf Erfahrungen oder Kenntnissen des Kunden

Kennt der Kunde seine gesamten Durchsatzanforderungen für alle verbundenen internen und externen Schnittstellen (z. B. durch in der Vergangenheit gesammelte Erfahrungswerte), sollten Sie prüfen, ob das von Ihnen gewählte Modell über die entsprechende Leistung verfügt.

So betreibt der Kunde vielleicht mehrere Server innerhalb einer DMZ und möchte den gesamten Datenverkehr von allen Segmenten zu diesen Servern von der IPS prüfen lassen. Oder der Kunde besitzt viele unterschiedliche Netzwerksegmente, die voreinander geschützt werden sollten (durch die Verwendung der FW-Paketfilter und/oder der Application Control-Funktion). In diesem Fall müssen Sie sicherstellen, dass die gewählte Appliance den gesamten internen Datenverkehr zwischen allen Segmenten scannen kann.

Weitere Fragen, mit denen Sie herauszufinden können, ob es noch mehr besondere Leistungsanforderungen gibt:

- Wie viele Site-to-Site-VPN-Tunnel sind erforderlich?
- Wie viele E-Mails werden pro Stunde übertragen – im Durchschnitt/zu Spitzenzeiten?
- Wie viel Internet-Datenverkehr (MBit/s und Anfragen/s) wird generiert – im Durchschnitt/zu Spitzenzeiten?
- Wie viele Webserver sollen geschützt werden und mit wie viel Datenverkehr ist zu rechnen – im Durchschnitt/zu Spitzenzeiten?

Im nächsten Abschnitt finden Sie genaue Leistungskennzahlen, mit denen Sie prüfen können, ob die gewählte Appliance alle individuellen Anforderungen erfüllt.

Sophos XG Serie – Leistungskennzahlen Hardware

Die folgende Tabelle enthält Leistungskennzahlen nach Datenverkehrstyp, die auf Messungen der Sophos Testlabs basieren. Die Realwerte zeigen den Durchsatz, der bei einem gewöhnlichen Datenverkehr- und Protokoll-Mix (definiert von den NSS Labs) erzielt werden kann. Die Höchstwerte zeigen den besten Durchsatz, der unter optimalen Bedingungen (z. B. mit großen Paketgrößen mit reinem UDP-Verkehr) bei voller CPU-Last erzielt werden kann.

Keiner dieser Werte lässt sich garantieren, da die Leistung in einer realen Kundenumgebung variieren kann, je nach Benutzereigenschaften, Anwendungsnutzung, Sicherheitskonfigurationen und sonstigen Faktoren. Diese Werte sollten daher lediglich als grobe Richtwerte verstanden werden.

Kleine Modelle – Desktop

Modell	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
Leistungskennzahlen					
Firewall, Höchstwert[1] (MBit/s)	2.000	3.000	3.500	5.000	7.000
Firewall-IMIX (MBit/s)	780	1.040	1.330	1.750	2.750
Firewall, Realwert[2] (MBit/s)	360	430	580	750	1.500
Firewall, Höchstwert[1] (Pakete pro Sekunde)	162.500	243.800	284.500	406.000	569.000
IPS, Höchstwert[3] (MBit/s)	510	700	900	1.040	1.750
IPS, Realwert[2] (MBit/s)	75	86	103	180	232
Webproxy – AV[5] (MBit/s)	330	430	520	590	1.400
Webproxy – AV, Realwert[2] (MBit/s)	75	187	234	307	427
IPS + Web Proxy – AV, Realwert[2] (MBit/s)	31	36	42	58	95
NGFW (IPS + App Ctrl + WebFilter), Höchstwert[3] (MBit/s)	235	270	310	360	880
NGFW (IPS + App Ctrl + WebFilter) Realwert[2] (MBit/s)	25	27	30	75	133
VPN AES, Höchstwert[3] (MBit/s), mehrere Tunnel/Cores	200	300	350	410	950
VPN AES, Höchstwert[3] (MBit/s), ein Tunnel/Core	200	250	290	290	600
VPN AES, Realwert[2] (MBit/s), mehrere Tunnel/Cores	50	75	90	105	240
WAF Adv. Profile, Höchstwert[6] (MBit/s)	--[6]	12	18	22	44
Maximal empfohlene Anzahl an Verbindungen					
Neue TCP-Verbindungen (pro Sek.)	12.000	27.500	27.500	35.000	82.000
Gleichzeitige TCP-Verbindungen	2.000.000	3.200.000	6.000.000	6.200.000	8.200.000
Gleichzeitige IPsec-VPN-Tunnel	200	300	500	750	1.000
Gleichzeitige SSL-VPN-Tunnel	100	200	240	270	270
Gleichzeitige betriebene Access Points	5	10	20	30	40
Gleichzeitig betriebene REDs (UTM/FW)[4]	5/10	10/30	15/60	20/80	25/100
WAF, gleichzeitig betriebene virtuelle Server	60[7]	60[7]	60[7]	60[7]	60[7]
WAF, Verbindungen pro Sekunde, Höchstwert	700	750	780	950	2.600

1. Paketgröße 1518 Byte (UDP)
2. Durchschnittswert verschiedener Protokolle (Rechenzentrum, Unternehmensperimeter, Hochschulen/Universitäten, europäische Mobil-Services, Finanznetzwerke) bei einer CPU-Auslastung von 50 %
3. HTTP-Verkehr
4. UTM = vollständige Inhalts-Scans von RED-Datenverkehr auf XG Appliance, FW = nur Paketfilterung
5. 512 KB-Dateien
6. Antivirus + Filter für alle gängigen Bedrohungen aktiv (kein Antivirus auf XG 85)
7. Hardcodiertes Limit

Mittlere Modelle – 1U

Modell	XG 210 Rev. 2	XG 230 Rev. 1	XG 310 Rev. 1	XG 330 Rev. 1	XG 430 Rev. 1	XG 450 Rev. 1
Leistungskennzahlen						
Firewall, Höchstwert[1] (MBit/s)	14.000	18.000	25.000	30.000	37.000	45.000
Firewall-IMIX (MBit/s)	4.900	6.110	8.530	11.230	12.950	15.650
Firewall, Realwert[2] (MBit/s)	2.060	2.250	3.800	6.100	6.900	7.650
Firewall, Höchstwert[1] (Pakete pro Sekunde)	1.137.800	1.463.000	2.031.860	2.438.200	3.007.200	3.657.400
IPS, Höchstwert[3] (MBit/s)	2.700	4.200	5.500	8.500	9.000	10.000
IPS, Realwert[2] (MBit/s)	309	361	539	733	893	1.159
Webproxy – AV[5] (MBit/s)	2.300	2.800	3.260	6.000	6.500	7.000
Webproxy – AV, Realwert[2] (MBit/s)	538	670	1.140	1.220	1.440	1.690
IPS + Webproxy – AV, Realwert[2] (MBit/s)	102	107	207	242	372	463
NGFW (IPS + App Ctrl + WebFilter), Höchstwert[3] (MBit/s)	1.700	2.420	2.700	4.220	4.800	5.000
NGFW (IPS + App Ctrl + WebFilter), Realwert[2] (MBit/s)	176	226	340	425	538	693
VPN AES, Höchstwert[3] (MBit/s), mehrere Tunnel/ Cores	1.350	1.500	2.500	3.200	4.800	5.500
VPN AES, Höchstwert[3] (MBit/s), ein Tunnel/Core	760	950	990	920	950	990
VPN AES, Realwert[2] (MBit/s), mehrere Tunnel/Cores	340	375	625	800	1.200	1.375
WAF Adv. Profil, Höchstwert[6] (MBit/s)	205	240	260	510	560	620
Maximal empfohlene Anzahl an Verbindungen						
Neue TCP-Verbindungen (pro Sek.)	135.000	140.000	200.000	200.000	200.000	200.000
Gleichzeitige TCP-Verbindungen	8.200.000	8.200.000	17.500.000	17.500.000	20.000.000	20.000.000
Gleichzeitige IPsec-VPN-Tunnel	1.300	1.600	1.800	2.500	3.000	3.500
Gleichzeitige SSL-VPN-Tunnel	300	300	300	300	350	350
Gleichzeitige betriebene Access Points	75	100	125	150	230	250
Gleichzeitig betriebene REDs (UTM/FW)[4]	30/125	40/150	50/200	60/230	70/250	80/300
WAF, gleichzeitig betriebene virtuelle Server	60[7]	60[7]	60[7]	60[7]	60[7]	60[7]
WAF, Verbindungen pro Sekunde, Höchstwert	3.700	4.200	5.000	9.000	14.000	15.500

1. Paketgröße 1518 Byte (UDP)
2. Durchschnittswert verschiedener Protokolle (Rechenzentrum, Unternehmensperimeter, Hochschulen/Universitäten, europäische Mobil-Services, Finanznetzwerke) bei einer CPU-Auslastung von 50 %
3. HTTP-Verkehr
4. UTM = vollständige Inhalts-Scans von RED-Datenverkehr auf XG Appliance, FW = nur Paketfilterung
5. 512 KB-Dateien
6. Antivirus + Filter für alle gängigen Bedrohungen aktiv (kein Antivirus auf XG 85)
7. Hardcodiertes Limit

Große Modelle – 2U

Modell	XG 550 Rev. 1	XG 650 Rev. 1	XG 750 Rev. 1
Leistungskennzahlen			
Firewall, Höchstwert[1] (MBit/s)	60.000	80.000	120.000
Firewall-IMIX (MBit/s)	21.500	26.990	33.500
Firewall, Realwert[2] (MBit/s)	11.700	15.000	19.000
Firewall, Höchstwert[1] (Pakete pro Sekunde)	4.876.500	6.502.000	9.752.900
IPS, Höchstwert[3] (MBit/s)	13.000	20.000	22.000
IPS, Realwert[2] (MBit/s)	2.160	3.310	3.970
Webproxy – AV[5] (MBit/s)	10.000	13.000	17.000
Webproxy – AV, Realwert[2] (MBit/s)	2.480	3.220	3.870
IPS + Web Proxy – AV, Realwert[2] (MBit/s)	808	1.109	1.330
NGFW (IPS + App Ctrl + WebFilter), Höchstwert[3] (MBit/s)	8.000	9.000	11.800
NGFW (IPS + App Ctrl + WebFilter) Realwert[2] (MBit/s)	1.190	1.730	2.070
VPN AES, Höchstwert[3] (MBit/s), mehrere Tunnel/Cores	8.400	9.000	11.250
VPN AES, Höchstwert[3] (MBit/s), ein Tunnel/Core	640	770	620
VPN AES, Realwert[2] (MBit/s) mehrere Tunnel/Cores	2.100	2.250	2.800
WAF Adv. Profile, Höchstwert[6] (MBit/s)	1.020	1.700	2.460
Maximal empfohlene Anzahl an Verbindungen			
Neue TCP-Verbindungen (pro Sek.)	200.000	200.000	300.000
Gleichzeitige TCP-Verbindungen	20.000.000	20.000.000	30.000.000
Gleichzeitige IPsec-VPN-Tunnel	4.000	4.500	5.400
Gleichzeitige SSL-VPN-Tunnel	400	500	500
Gleichzeitige betriebene Access Points	300	400	500
Gleichzeitig betriebene REDs (UTM/FW)[4]	100/400	150/600	200/600*
WAF, gleichzeitig betriebene virtuelle Server	60[7]	60[7]	60[7]
WAF, Verbindungen pro Sekunde, Höchstwert	18.000	21.000	24.000

*Technisches Limit

1. Paketgröße 1518 Byte (UDP)
2. Durchschnittswert verschiedener Protokolle (Rechenzentrum, Unternehmensperimeter, Hochschulen/Universitäten, europäische Mobil-Services, Finanznetzwerke) bei einer CPU-Auslastung von 50 %
3. HTTP-Verkehr
4. UTM = vollständige Inhalts-Scans von RED-Datenverkehr auf XG Appliance, FW = nur Paketfilterung
5. 512 KB-Dateien
6. Antivirus + Filter für alle gängigen Bedrohungen aktiv (kein Antivirus auf XG 85)
7. Hardcodiertes Limit

Sophos XG Firewall Software-/virtuelle Appliances

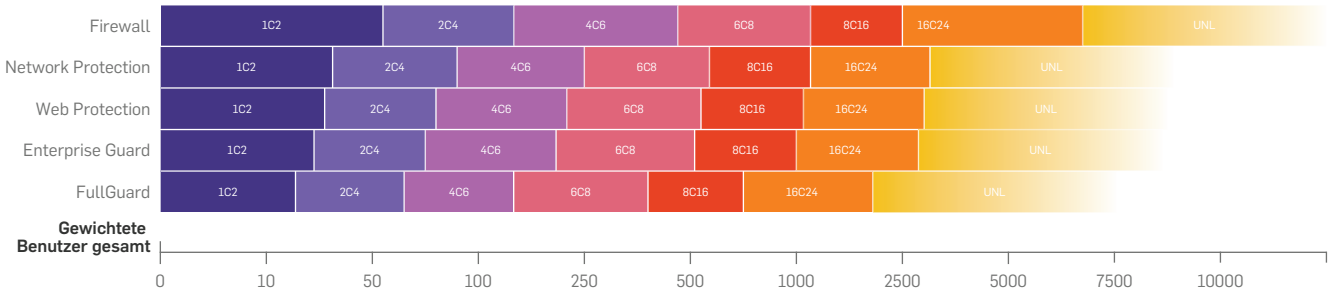
Sophos XG Firewall Software-/virtuelle Appliances werden nach Anzahl der (virtuellen) Cores und (virtueller) RAM-Größe lizenziert. Lizenzen müssen nicht exakt mit der Anzahl der verfügbaren Cores/RAM-Größe übereinstimmen, aktivieren jedoch nur die lizenzierten Cores/lizenzierte RAM-Größe zur Verwendung in der Software.

Software-/virtuelle Appliances können auf verschiedenen CPU-Typen mit unterschiedlichen Geschwindigkeiten eingesetzt werden. Die Performance kann jedoch stark variieren – selbst wenn die gleiche Core-Anzahl/RAM-Größe genutzt wird.

Die folgende Abbildung gibt Ihnen einen groben Überblick über die für jedes Software-Modell empfohlenen gewichteten Benutzergesamtzahlen (gemäß der Berechnung in Kapitel 1).

Die Zahlen basieren auf den folgenden Annahmen:

- CPU-Geschwindigkeit = 2,5 GHz (höhere Geschwindigkeit kann den Durchsatz für die meisten Anwendungen deutlich erhöhen)
- CPU-Typ = Core I (bis zu 6C8), Xeon (8C16 und höher)



Subscription-Profil

Faustregel:

- Beim Einsatz der Sophos XG Firewall in virtuellen Umgebungen ist mit einem Leistungsverlust/einer Verringerung der Benutzerzahl von schätzungsweise 10 % zu rechnen. Dies wird durch das Hypervisor-Framework verursacht.

Vorort-Tests

Die oben beschriebene Vorgehensweise dient als Grundlage zur Wahl eines geeigneten Modells, basiert jedoch ausschließlich auf Kundenangaben. Tatsächlich werden das Verhalten und die Performance einer Appliance von vielen Faktoren beeinflusst, die sich nur unter realen Bedingungen beurteilen lassen. Daher ist ein Vorort-Test immer die beste Methode, um zu ermitteln, ob die gewählte Appliance die Leistungsanforderungen des Kunden erfüllt. Das Sophos Pre-Sales-Team hilft Ihnen gerne bei der Bestimmung des geeigneten Modells.

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter
www.sophos.de/produkte

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2016-09-21 SG-DE (DD)

SOPHOS