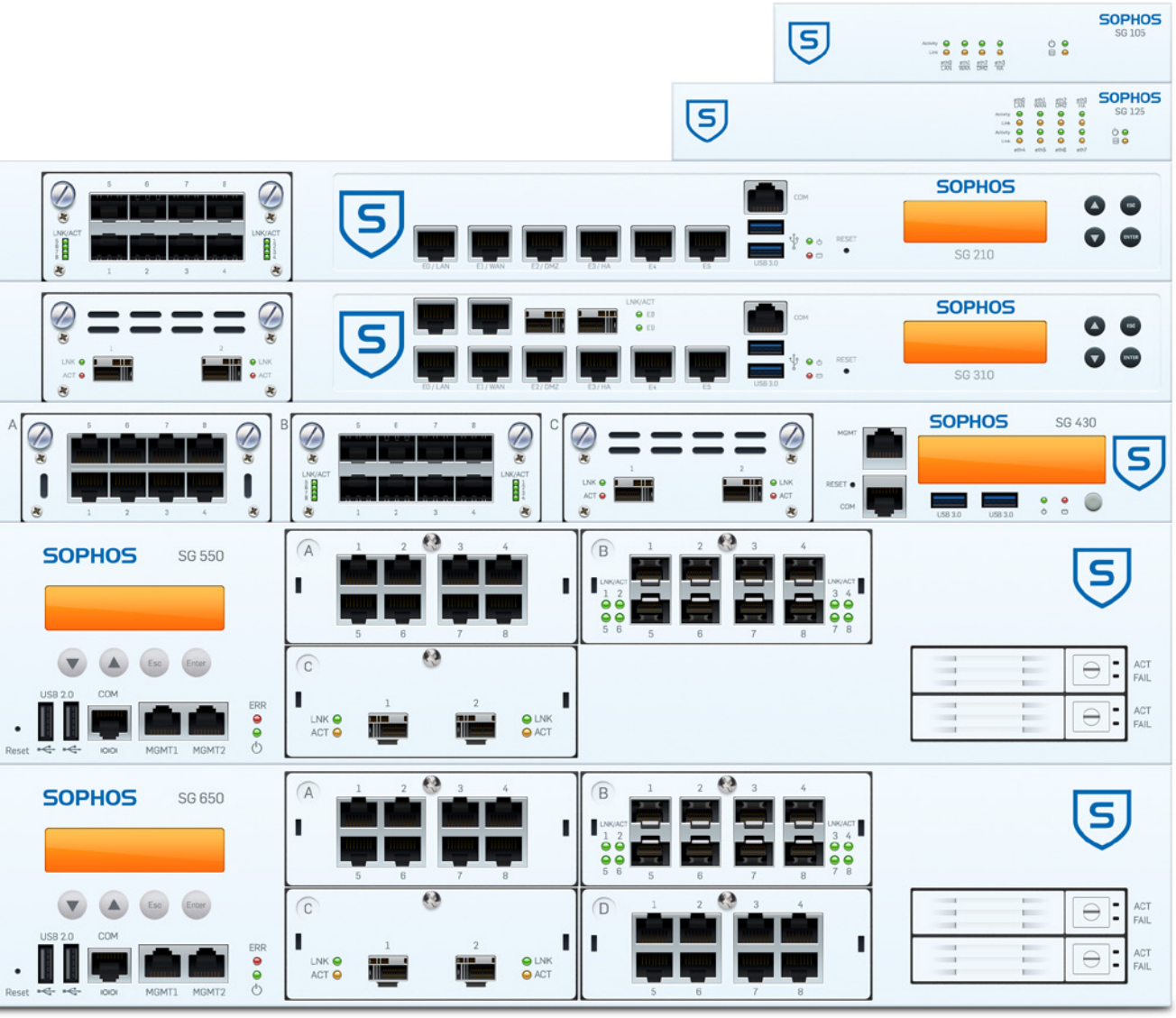
SOPHOS

Security made simple.

Sizing Guide

Sophos UTM 9.2 – SG Series Appliances



In drei Schritten zum richtigen Appliance-Modell

Mit diesem Leitfaden können Sie bestimmen, welches Appliance-Modell der Sophos SG 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 „Gesamtzahl der UTM-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 „Gesamtzahl der UTM-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 den Sophos SG Series Appliances können Sie einen solchen Vorort-Test für das ausgewählte Modell kostenlos anbieten.

1. „Gesamtzahl der UTM-Benutzer“ ermitteln

Errechnen Sie in Tabelle 1.1 die von der Appliance zu verarbeitende „Gesamtzahl der UTM-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 „Gewichtete Benutzerzahl gesamt“.

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 „Gewichtete Benutzerzahl gesamt“ und tragen Sie das Ergebnis in das Feld „Gesamtzahl der UTM-Benutzer“ ein.

Tabelle 1.1 Berechnung: „Gesamtzahl der UTM-Benutzer“

	Benutzerzahl	Multipliziert mit	Gewichtete Benutzerzahl
Durchschnittliche Nutzung		1	
Stärkere Nutzung		1,5	
Intensive Nutzung		2	
Benutzerzahl gesamt		Gewichtete Benutzerzahl gesamt	
		multipliziert mit Systembelastung	
		Gesamtzahl der UTM-Benutzer	

Tabelle 1.2 Kriterien Benutzerkategorie

Verwenden Sie zur Klassifizierung der Benutzertypen die unten aufgeführten Kriterien.

	Durchschnittliche Nutzung	Stärkere Nutzung (*1,5)	Intensive Nutzung (*2)
E-Mail-Nutzung (an einem 10-Stunden-Arbeitstag)			
Anzahl der 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

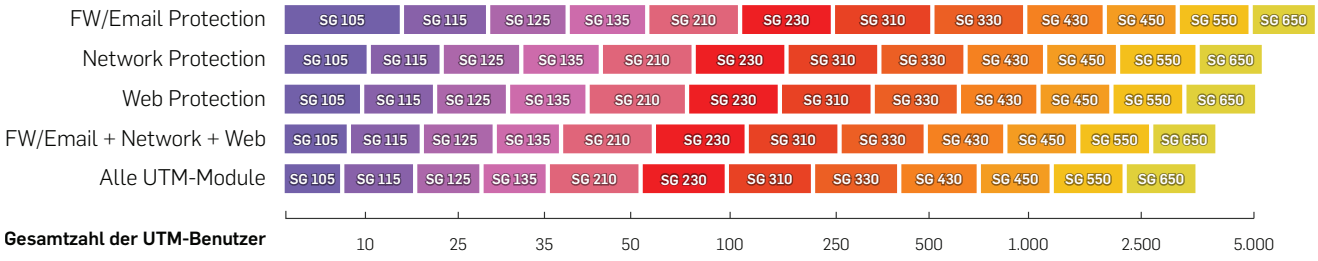
Ermitteln Sie, ob bestimmte Faktoren die Systembelastung möglicherweise erhöhen und demzufolge auch die Leistungsanforderungen an das System beeinflussen können.

	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-Mails			
Spamanteil	weniger als 50 %	50–90 %	Mehr als 90 %
Reporterstellung			
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 „Gesamtzahl der UTM-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 Wireless Protection, Webserver Protection oder Endpoint Protection zu den oben genannten Subscription-Profilen verringert sich die empfohlene „Gesamtzahl der UTM-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 SG 230 anstelle einer SG 210 nur wenige Vorteile – obwohl die errechnete Gesamtzahl der Benutzer bei etwa 100 liegt. In diesem Fall ist möglicherweise sogar eine SG 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 SG 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-Mix erzielt werden kann. Die Höchstwerte zeigen den besten Durchsatz, der unter optimalen Bedingungen (z. B. mit großen Paketgrößen) 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. Details entnehmen Sie bitte dem Dokument „Sophos UTM - Performance Test Methodology“.

Kleine Modelle – Desktop

Modell	SG 105/w Rev. 1	SG 115/w Rev. 1	SG 125/w Rev. 1	SG 135/w Rev. 1
Leistungskennzahlen				
Firewall, Höchstwert[1] (MBit/s)	1.500	2.300	3.100	6.000
Firewall, Realwert[2] (MBit/s)	1.420	1.630	2.100	3.650
APT, Realwert[2] (MBit/s)	1.260	1.470	1.490	3.200
IPS, Höchstwert[1] (MBit/s)	350	500	750	1.500
IPS, alle Regeln (MBit/s)	165	200	320	540
FW + ATP + IPS, Höchstwert[1] (MBit/s)	810	950	1.140	1.750
FW + ATP + IPS, Realwert[2] (MBit/s)	120	135	165	370
App Control, Realwert[2] (MBit/s)	1.320	1.430	1.790	3.120
VPN AES, Höchstwert[3] (MBit/s)	325	425	500	1.000
VPN AES, Realwert[4] (MBit/s)	95	130	155	280
Webproxy, Standard[5] (MBit/s)	215	380	475	850
Webproxy – AV[5] (MBit/s)	90	120	200	350
Webanfragen/Sekunde[5] – AV	360	500	900	1.650
Maximal empfohlene Verbindungsanzahl				
Neue TCP-Verbindungen (pro Sek.)	15.000	20.000	24.000	36.000
Gleichzeitige TCP-Verbindungen	1.000.000	1.000.000	2.000.000	2.000.000
Gleichzeitige IPsec-VPN-Tunnel	80	145	175	250
Gleichzeitige SSL-VPN-Tunnel	35	55	75	120
Gleichzeitig betriebene Endpoints	10	20	30	40
Gleichzeitige betriebene Access Points	10	20	30	40
Gleichzeitig betriebene REDs (UTM/FW)	10/30	15/60	20/80	25/100

1. Paketgröße 1518 Byte (UDP), Standardregelsatz
2. NSS Perimeter Mix (TCP/UCP)
3. AES-NI mit AES GCM, falls möglich (UDP)
4. NSS Core Mix (TCP/UCP)
5. Durchsatz: 100 Kilobyte-Dateien, Anfragen (pro Sek.): 1 Kilobyte-Dateien (die Werte beziehen sich auf Einzelscanning und können bei der Aktivierung von Dualscanning um 15–20 % niedriger ausfallen)
6. Technisches Limit

Mittlere Modelle – 1U

Modell	SG 210 Rev. 1	SG 230 Rev. 1	SG 310 Rev. 1	SG 330 Rev. 1	SG 430 Rev. 1	SG 450 Rev. 1
Leistungskennzahlen						
Firewall, Höchstwert[1] (MBit/s)	11.000	13.000	17.000	20.000	25.000	27.000
Firewall, Realwert[2] (MBit/s)	6.270	6.350	6.560	8.850	11.450	12.750
APT, Realwert[2] (MBit/s)	3.724	3.748	5.230	8.550	11.310	12.180
IPS, Höchstwert[1] (MBit/s)	2.000	3.000	5.000	6.000	7.000	8.000
IPS, alle Regeln (MBit/s)	608	714	1.390	1.420	1.650	1.970
FW + ATP + IPS, Höchstwert[1] (MBit/s)	1.910	2.850	4.790	5.890	6.650	7.570
FW + ATP + IPS, Realwert[2] (MBit/s)	432	572	875	880	950	1.690
App Control, Realwert[2] (MBit/s)	3.658	3.801	5.150	8.570	11.350	12.230
VPN AES, Höchstwert[3] (MBit/s)	1.000	2.000	3.000	4.000	4.000	5.000
VPN AES, Realwert[4] (MBit/s)	300	400	850	1.200	1.550	1.800
Webproxy, Standard[5] (MBit/s)	1.350	1.650	2.100	2.950	3.510	4.100
Webproxy – AV[5] (MBit/s)	500	800	1.200	1.500	2.000	2.500
Webanfragen/Sekunde[5] – AV	2.100	2.300	3.100	4.200	5.400	6.500
Maximal empfohlene Verbindungsanzahl						
Neue TCP-Verbindungen (pro Sek.)	60.000	70.000	100.000	120.000	130.000	140.000
Gleichzeitige TCP-Verbindungen	4.000.000	4.000.000	6.000.000	6.000.000	8.000.000	8.000.000
Gleichzeitige IPsec-VPN-Tunnel	350	500	800	1.200	1.600	2.000
Gleichzeitige SSL-VPN-Tunnel	180	200	230	250	280	300
Gleichzeitig betriebene Endpoints	75	150	300	500	750	1.000
Gleichzeitige betriebene Access Points	75	100	125	150	222[6]	222[6]
Gleichzeitig betriebene REDs (UTM/FW)	30/125	40/150	50/200	60/230	70/250	80/300

Große Modelle – 2U

Modell	SG 550 Rev. 1	SG 650 Rev. 1
Leistungskennzahlen		
Firewall, Höchstwert[1] (MBit/s)	40.000	60.000
Firewall, Realwert[2] (MBit/s)	14.070	18.950
APT, Realwert[2] (MBit/s)	13.230	17.845
IPS, Höchstwert[1] (MBit/s)	12.000	16.000
IPS, alle Regeln (MBit/s)	3.895	5.710
FW + ATP + IPS, Höchstwert[1] (MBit/s)	15.980	25.600
FW + ATP + IPS, Realwert[2] (MBit/s)	3.280	6.130
App Control, Realwert[2] (Mbps)	13.350	13.990
VPN AES, Höchstwert[3] (MBit/s)	8.000	10.000
VPN AES, Realwert[4] (MBit/s)	2.110	2.380
Webproxy, Standard[5] (MBit/s)	4.700	6.800
Webproxy – AV[5] (MBit/s)	3.500	5.000
Webanfragen/Sekunde[5] – AV	15.000	23.500
Maximal empfohlene Anzahl an Verbindungen		
Neue TCP-Verbindungen (pro Sek.)	200.000	220.000
Gleichzeitige TCP-Verbindungen	12.000.000	20.000.000
Gleichzeitige IPsec-VPN-Tunnel	2.200	2.800
Gleichzeitige SSL-VPN-Tunnel	340	420
Gleichzeitig betriebene Endpoints	1.000[6]	1.000[6]
Gleichzeitige betriebene Access Points	222[6]	222[6]
Gleichzeitig betriebene REDs (UTM/FW)	100/400	150/600

1. Paketgröße 1518 Byte (UDP), Standardregelsatz
2. NSS Perimeter Mix (TCP/UCP)
3. AES-NI mit AES GCM, falls möglich (UDP)
4. NSS Core Mix (TCP/UCP)
5. Durchsatz: 100 Kilobyte-Dateien, Anfragen (pro Sek.): 1 Kilobyte-Dateien (die Werte beziehen sich auf Einzelscans und können bei der Aktivierung von Dualscans um 20–25 % niedriger ausfallen)
6. Technisches Limit

Sophos UTM-Software-/virtuelle Appliances

Zur Wahl einer typischen Systemkonfiguration bei der Installation von Sophos UTM-Software auf Intel-kompatiblen PCs/Servern empfehlen wir die folgende Vorgehensweise: 1) Wahl einer den Anforderungen entsprechenden Sophos SG Series Hardware Appliance (mit Hilfe der Anleitung oben); 2) Wahl einer geeigneten Hardware-Konfiguration aus der Tabelle unten.

Modell	SG 105/w Rev. 1	SG 115/w Rev. 1	SG 125/w Rev. 1	SG 135/w Rev. 1	SG 210 Rev. 1	SG 230 Rev. 1	SG 310 Rev. 1	SG 330 Rev. 1	SG 430 Rev. 1	SG 450 Rev. 1	SG 550 Rev. 1	SG 650 Rev. 1
CPU	Atom Baytrail Dual Core (1,46 GHz)	Atom Baytrail Dual Core (1,75 GHz)	Atom Baytrail Dual Core (1,7 GHz)	Atom Rangeley Quad Core (2,4 GHz)	Celeron Dual Core (2,70 GHz)	Pentium Dual Core (3,20 GHz)	Dual Core i3 (3,50 GHz)	Quad Core i5 (2,9 GHz)	Quad Core Xeon E3- (3,20 GHz)	Quad Core Xeon E3- (3,50GHz)	2* 6 Core Xeon E5- (2,6 GHz)	2* 10 Core Xeon E5- (2,8 GHz)
Arbeitsspeicher (GB)	2	4	4	6	8	8	12	12	16	16	24	48

Beim Einsatz von Sophos UTM in virtuellen Umgebungen ist mit einem Leistungsverlust von schätzungsweise 10 % zu rechnen. Dieser wird durch das Hypervisor-Framework verursacht.

Anzahl der Benutzer ermitteln

Was bedeutet „Benutzer“ im Zusammenhang mit Software-Lizenzen?

Mit „Benutzer“ sind im Rahmen der Sophos Software-Lizenzierung Workstations, Clientserver und sonstige Geräte gemeint, die über eine IP-Adresse verfügen und vom Sophos Gateway geschützt werden oder einen Service von diesem in Anspruch nehmen.

Sobald ein „Benutzer“ mit dem oder durch das Gateway kommuniziert, wird seine IP-Adresse zur Liste lizenzierter Geräte in der lokalen Datenbank des Gateways hinzugefügt. Ob der „Benutzer“ mit dem Internet oder mit einem Gerät in einem anderen LAN-Segment kommuniziert, macht dabei keinen Unterschied. DNS- oder DHCP-Anfragen an das Gateway werden ebenfalls mitgezählt. Wenn mehrere Benutzer durch ein einziges Gerät mit nur einer IP-Adresse kommunizieren (z. B. E-Mail-Server oder Webproxy), wird jeder Benutzer separat gezählt.

Für den Lizenzmechanismus werden lediglich Daten der letzten sieben Tage verwendet. Ungenutzte IP-Adressen werden nach sieben Tagen aus der Datenbank gelöscht.

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.

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

Oxford, GB | Boston, USA

09.14RP.sgde.simple