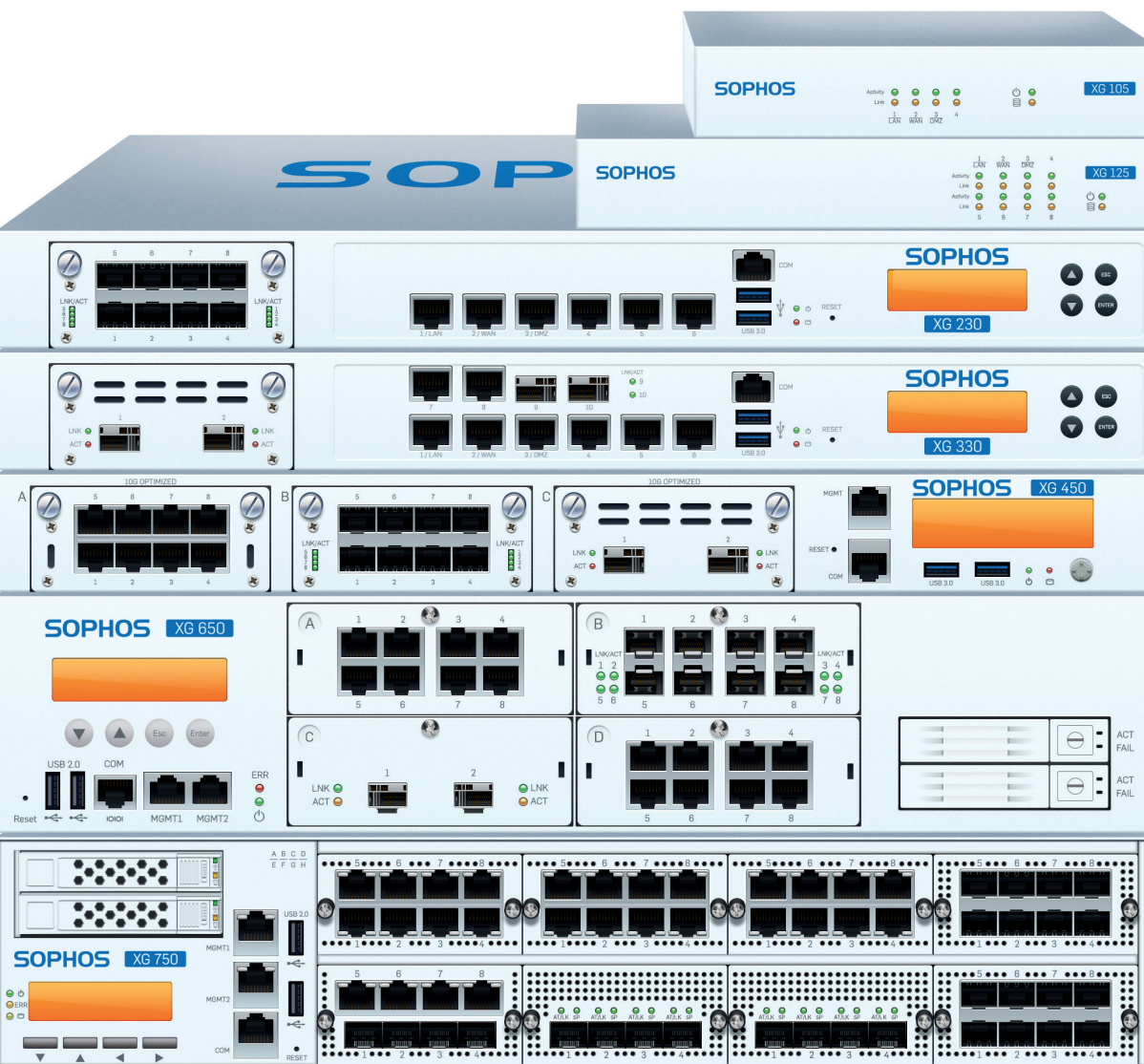# SOPHOS
Security made simple.

v15 Sizing Guidelines

Sophos XG Firewall – XG Series Appliances

Please Note:

This guide is in the process of being updated and replaced with new sizing tools for the latest XG Firewall appliance hardware and firmware. We will announce their availability to all relevant parties as soon as they are available. Thank you for your patience in this matter.

Three steps to specifying the right appliance model

This document provides a guideline for choosing the right Sophos XG Series appliance for your customer. Specifying the right appliance is dependent on a number of factors and involves developing a usage profile for the users and the network environment.

For best results we recommend using the following step-by-step procedure:

1. **Identify the "Total UTM User" Number**
   Understand the customer's environment like browsing behavior, application usage, network and server infrastructure to get an accurate understanding of the actual usage an XG Series appliance will see at peak times.

2. **Make a first estimate**
   Based on the Total weighted User number.

3. **Check specific throughput requirements**
   Understand if any local factors like the maximum available internet uplink capacity will impact performance – check this against Sophos XG Firewall throughput numbers and adjust the recommendation accordingly.

Of course, the best way to understand if an appliance will meet a customer's needs is to test it in the customer environment and with Sophos XG Firewall you can offer a free on-site evaluation of the selected unit.

1. Identify the "Total Weighted User" number

Use the following table to first calculate the Total weighted User number that the appliance will need to handle.

a. Calculate the Weighted User Count number. Identify the user category (Average/ Advanced/Power) that best fits the average user behavior of the users, or estimate how many users fit each category. Use the criteria in table 1.2 to classify the type of users.

- Enter the User Counts in table 1.1, multiply them with the indicated factor, enter the results into the "Weighted User Count" boxes and sum it into the "Total Weighted User Count" box.

b. Identify the System Load Number. Use the criteria using table 1.3 to classify the load.

- Enter the System Load Number in the box "multiplied by System Load" in table 1.1, multiply it with the "Total Weighted User Count" and enter the result into the "Total weighted Users" box.

1.1

Licenses names	User Count	Multiplied by	Weighted User Count
Standard user		1	
Advanced Users		1.2	
Power Users		1.5	
Total User Count		Total Weighted User Count	
		multiplied by System Load	
		Total weighted Users	

1.2 User Category Criteria

Use the criteria described below to classify the type of users.

	Average user	Advanced user (*1.2)	Power user (*1.5)
Email usage (per 10h working day)			
Number of received emails in inbox	< 50	50 to 100	>100
Data volume	Few MBytes	Multiple MBytes	Numerous MBytes
Web usage (per 10h working day)			
Data volume	Few MBytes	Multiple MBytes	Numerous MBytes
Usage pattern	Equally spread throughout the day	Various peaks	Many peaks
Web applications used	Mostly webmail / Google / news	Heavy surfing, moderate media transfer, business applications	Intensive surfing and media transfers (schools, universities)
VPN usage			
VPN remote access usage	Rarely – sporadically connected	Several times per week – connected at regular times	Every day – connected most of the time

1.3 System Load Criteria

Identify any specific requirements that might increase the overall system load and hence the performance requirements for the system.

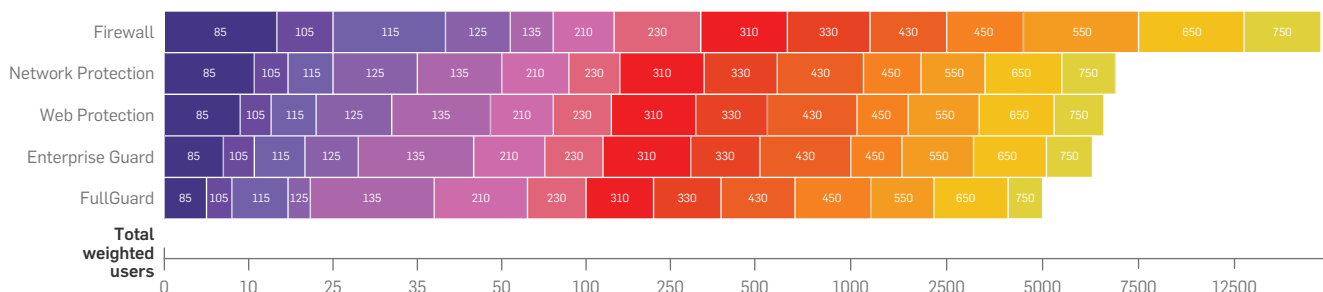|	Average system usage	Advanced system usage (*1.2)	High system usage (*1.5)
Authentication			
Active Directory in use	No	Yes	Yes
FW/IPS/VPN usage			
Variety of systems to be protected by IPS	No IPS protection required	Mostly Windows PCs, 1-2 servers	Various Client Operating systems, browsers and multimedia apps, >2 servers
Email			
Percentage of Spam	<50%	50-90%	>90%
Reporting			
Report storage time and granularity requirement	Up to 1 month web report only (per Domain)	Up to 3 months Up to 5 reports (per Domain)	>3 months (per URL)
Accounting storage time on appliance	No	Up to 1 month	>1 month

2. Make a first estimate — using the calculated "Total weighted User" number

Take the "Total weighted User" and make a first estimate for the required XG Series hardware appliance within the following diagram:

‣ Each line shows the range of users recommended when only using this single subscription.

‣ Please ensure all numbers include users connected via VPN, RED and wireless APs.

Subscription Profile

Rule of thumb:

Firewall	85	105	115	125	135	210	230	310	330	430	450	550		650	750
Network Protection	85	105	115	125	135	210	230	310	330	430	450	550	650	750	
Web Protection	85	105	115	125	135	210	230	310	330	430	450	550	650	750	
Enterprise Guard	85	105	115	125	135	210	230	310	330	430	450	550	650	750	
FullGuard	85	105	115	125	135	210	230	310	330	430	450	550	650	750	

Total weighted users

0	10	25	35	50	100	250	500	1000	2500	5000	7500	12500

‣ Estimate that adding Webserver Protection or Email Protection to any of the subscription profiles mentioned above will decrease range by 5-10% each.

3. Check for specific throughput requirements

Depending on the customer's environment there might be specific throughput requirements driving an adjustment of your first estimate to a higher (or even lower) unit.

These requirements are typically based on the following two factors:

The maximum available internet uplink capacity

The capacity of the customer's internet connection (up- and downlink) should match the average throughput rate that the selected unit is able to forward (depending on the subscriptions in use).

For instance if the download or upload limit is only 20 Mbps then there is no great benefit in using an XG 230 instead of an XG 210, even though the calculated total number of users is around 100. In that case even an XG 210 might be sufficient because it can perfectly fill the complete internet link even with all UTM features enabled.

However, data might not only be filtered on its way to the internet but also between internal network segments. Hence consider internal traffic that traverses the firewall as well in this assessment.

Specific performance requirements based on customer experience or knowledge

If the customer knows their overall throughput requirements among all connected internal and external interfaces (e.g. based on their past experience) then check whether the selected unit is able to meet these numbers.

For instance the customer might have several servers located within a DMZ and want to get all traffic to those servers from all segments to be inspected by the IPS. Or the customer may have many different network segments that should be protected against each other (by using the FW packet filter and/or the Application Control feature). In this case consider that the unit must scan the complete internal traffic between all segments.

v15 Sizing Guidelines

Further questions to ask in order to find out if there are any other performance requirements:

‣ How many site-to-site VPN tunnels are required?

‣ How many emails are being transferred per hour – on average/at peak times?

‣ How much web traffic (Mbps and requests/s) is being generated – on average/at peak times?

‣ How many web servers should be protected and how much traffic is expected – on average/at peak times?

The following section provides detailed performance numbers to help determine whether the selected appliance meets all individual requirements.

Sophos XG Series Hardware performance numbers

The following table provides performance numbers by traffic type measured within Sophos testing labs. "Realworld" numbers represent throughput values achievable with a typical/real life traffic and protocol mix as defined by NSS Labs. Maximum numbers represent best throughput achievable under perfect conditions, e.g. using large packet sizes with UDP traffic only at full CPU load.

Please note that none of these numbers are guaranteed as performance may vary in a real life customer scenario based on user characteristics, application usage, security configurations and other factors. Hence these numbers should only be used as a rough sizing guideline.

Small – Desktop

Model	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
Performance Numbers					
Firewall max.[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 Realworld[2] (Mbps)	360	430	580	750	1,500
Firewall max.[1] (packets per second)	162,500	243,800	284,500	406,000	569,000
IPS max.[3] (Mbps)	510	700	900	1,040	1,750
IPS Realworld[2] (Mbps)	75	86	103	180	232
Web Proxy – AV[5] (Mbps)	330	430	520	590	1,400
Web Proxy – AV Realworld[2] (Mbps)	75	187	234	307	427
IPS + Web Proxy – AV Realworld[2] (Mbps)	31	36	42	58	95
NGFW (IPS + App Ctrl + WebFilter) max.[3] (Mbps)	235	270	310	360	880
NGFW (IPS + App Ctrl + WebFilter) Realworld[2] (Mbps)	25	27	30	75	133
VPN AES max.[3] (Mbps) multiple tunnels/cores	200	300	350	410	950
VPN AES max.[3] (Mbps) single tunnel/core	200	250	290	290	600
VPN AES Realworld[2] (Mbps) multiple tunnels/cores	50	75	90	105	240
WAF Adv. Profile max.[6] (Mbps)	N/A[6]	12	18	22	44
Maximum recommended connections					
New TCP connections/sec	12,000	27,500	27,500	35,000	82,000
Concurrent TCP connections	2,000,000	3,200,000	6,000,000	6,200,000	8,200,000
Concurrent IPsec VPN tunnels	200	300	500	750	1,000
Concurrent SSL VPN tunnels	100	200	240	270	270
Concurrent Access Points	5	10	20	30	40
Concurrent REDs (UTM/FW)[4]	5/10	10/30	15/60	20/80	25/100
WAF Concurrent Virtual Servers	60[7]	60[7]	60[7]	60[7]	60[7]
WAF max. conenctions/sec	700	750	780	950	2,600

1. 1518 byte packet size (UDP)
2. Average of Data Center, Enterprise Perimeter, Higher Education, European Mobile, Financial Network protocol mixes at 50% CPU Usage
3. HTTP traffic
4. UTM=Full content scanning of RED traffic on XG appliance, FW=packet filtering only
5. 512 KByte files
6. AV + all common threats filter active (no AV on XG85)
7. Hard coded limit

Medium – 1U

Model	XG 210 rev.2	XG 230 rev.1	XG 310 rev.1	XG 330 rev.1	XG 430 rev.1	XG 450 rev.1
Performance Numbers						
Firewall max.[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 Realworld[2] (Mbps)	2,060	2,250	3,800	6,100	6,900	7,650
Firewall max.[1] (packets per second)	1,137,800	1,463,000	2,031,860	2,438,200	3,007,200	3,657,400
IPS max.[3] (Mbps)	2,700	4,200	5,500	8,500	9,000	10,000
IPS Realworld[2] (Mbps)	309	361	539	733	893	1,159
Web Proxy – AV[5] (Mbps)	2,300	2,800	3,260	6,000	6,500	7,000
Web Proxy – AV Realworld[2] (Mbps)	538	670	1,140	1,220	1,440	1,690
IPS + Web Proxy – AV Realworld[2] (Mbps)	102	107	207	242	372	463
NGFW (IPS + App Ctrl + WebFilter) max.[3] (Mbps)	1,700	2,420	2,700	4,220	4,800	5,000
NGFW (IPS + App Ctrl + WebFilter) Realworld[2] (Mbps)	176	226	340	425	538	693
VPN AES max.[3] (Mbps) multiple tunnels/cores	1,350	1,500	2,500	3,200	4,800	5,500
VPN AES max.[3] (Mbps) single tunnel/core	760	950	990	920	950	990
VPN AES Realworld[2] (Mbps) multiple tunnels/cores	340	375	625	800	1,200	1,375
WAF Adv. Profile max.[6] (Mbps)	205	240	260	510	560	620
Maximum recommended connections						
New TCP connections/sec	135,000	140,000	200,000	200,000	200,000	200,000
Concurrent TCP connections	8,200,000	8,200,000	17,500,000	17,500,000	20,000,000	20,000,000
Concurrent IPsec VPN tunnels	1,300	1,600	1,800	2,500	3,000	3,500
Concurrent SSL VPN tunnels	300	300	300	300	350	350
Concurrent Access Points	75	100	125	150	230	250
Concurrent REDs (UTM/FW)[4]	30/125	40/150	50/200	60/230	70/250	80/300
WAF Concurrent Virtual Servers	60[7]	60[7]	60[7]	60[7]	60[7]	60[7]
WAF max. conenctions/sec	3,700	4,200	5,000	9,000	14,000	15,500

1. 1518 byte packet size (UDP)
2. Average of Data Center, Enterprise Perimeter, Higher Education, European Mobile, Financial Network protocol mixes at 50% CPU Usage
3. HTTP traffic
4. UTM=Full content scanning of RED traffic on XG appliance, FW=packet filtering only
5. 512 KByte files
6. AV + all common threats filter active (no AV on XG85)
7. Hard coded limit

Large – 2U

Model	XG 550 rev.1	XG 650 rev.1	XG 750 rev.1
Performance Numbers			
Firewall max.[1] (Mbps)	60,000	80,000	120,000
Firewall IMIX (Mbps)	21,500	26,990	33,500
Firewall Realworld[2] (Mbps)	11,700	15,000	19,000
Firewall max.[1] (packets per second)	4,876,500	6,502,000	9,752,900
IPS max.[3] (Mbps)	13,000	20,000	22,000
IPS Realworld[2] (Mbps)	2,160	3,310	3,970
Web Proxy – AV[5] (Mbps)	10,000	13,000	17,000
Web Proxy – AV Realworld[2] (Mbps)	2,480	3,220	3,870
IPS + Web Proxy – AV Realworld[2] (Mbps)	808	1,109	1,330
NGFW (IPS + App Ctrl + WebFilter) max.[3] (Mbps)	8,000	9,000	11,800
NGFW (IPS + App Ctrl + WebFilter) Realworld[2] (Mbps)	1,190	1,730	2,070
VPN AES max.[3] (Mbps) multiple tunnels/cores	8,400	9,000	11,250
VPN AES max.[3] (Mbps) single tunnel/core	640	770	620
VPN AES Realworld[2] (Mbps) multiple tunnels/cores	2,100	2,250	2,800
WAF Adv. Profile max.[6] (Mbps)	1,020	1,700	2,460
Maximum recommended connections			
New TCP connections/sec	200,000	200,000	300,000
Concurrent TCP connections	20,000,000	20,000,000	30,000,000
Concurrent IPsec VPN tunnels	4,000	4,500	5,400
Concurrent SSL VPN tunnels	400	500	500
Concurrent Access Points	300	400	500
Concurrent REDs (UTM/FW)[4]	100/400	150/600	200/600*
WAF Concurrent Virtual Servers	60[7]	60[7]	60[7]
WAF max. conenctions/sec	18,000	21,000	24,000

*Technical limit

1. 1518 byte packet size (UDP)
2. Average of Data Center, Enterprise Perimeter, Higher Education, European Mobile, Financial Network protocol mixes at 50% CPU Usage
3. HTTP traffic
4. UTM=Full content scanning of RED traffic on XG appliance, FW=packet filtering only
5. 512 KByte files
6. AV + all common threats filter active (no AV on XG85)
7. Hard coded limit

Sophos XG Firewall Software/Virtual Appliances

Sophos XG Firewall Software/Virtual Appliances are licenses by numbers of (virtual) cores and (virtual) RAM size. Licenses do not have to match exactly the number of available cores/RAM but will only activate the licensed cores/RAM to be used in the Software.

While the Software/Virtual Appliances might be used on various CPU types with various speeds the performance might vary significantly even if using the same number of cores/RAM size.

The following diagram provides a rough guidance of total weighted user ranges (according to the calculation in chapter 1) recommended for each Software model.

Numbers are based on the following assumptions:

‣ CPU speed = 2.5 GHz (higher speed can significantly increase throughput for most applications)

‣ CPU Type = Core I (up to 6C8), Xeon (8C16 and above)
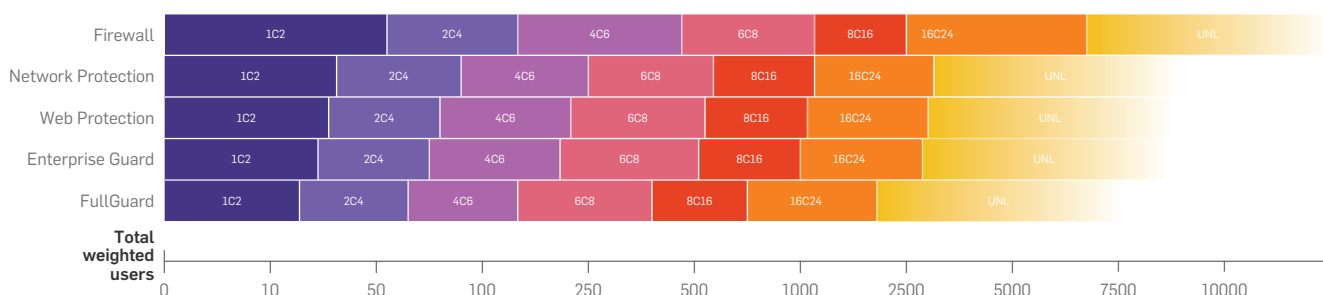
Subscription Profile

Rule of thumb:

‣ Using Sophos XG Firewall in a virtual environment has an estimated ~10% performance/user number decrease caused by the Hypervisor framework.

On-site evaluations

While the procedure explained above is a good foundation for selecting the most appropriate model, it is only based on information received from the customer. There are many factors determining the behavior and performance of an appliance which can only be evaluated in a real life scenario. Therefore, an on-site evaluation within the customer's environment is always the best way to determine whether the selected appliance meets the actual performance requirements of the customer. For further assistance, staff within the Sophos pre-sales teams are ready to assist you with sizing and in selecting the right platform.

Try it now for free

Register for a free 30-day evaluation
at sophos.com/products.