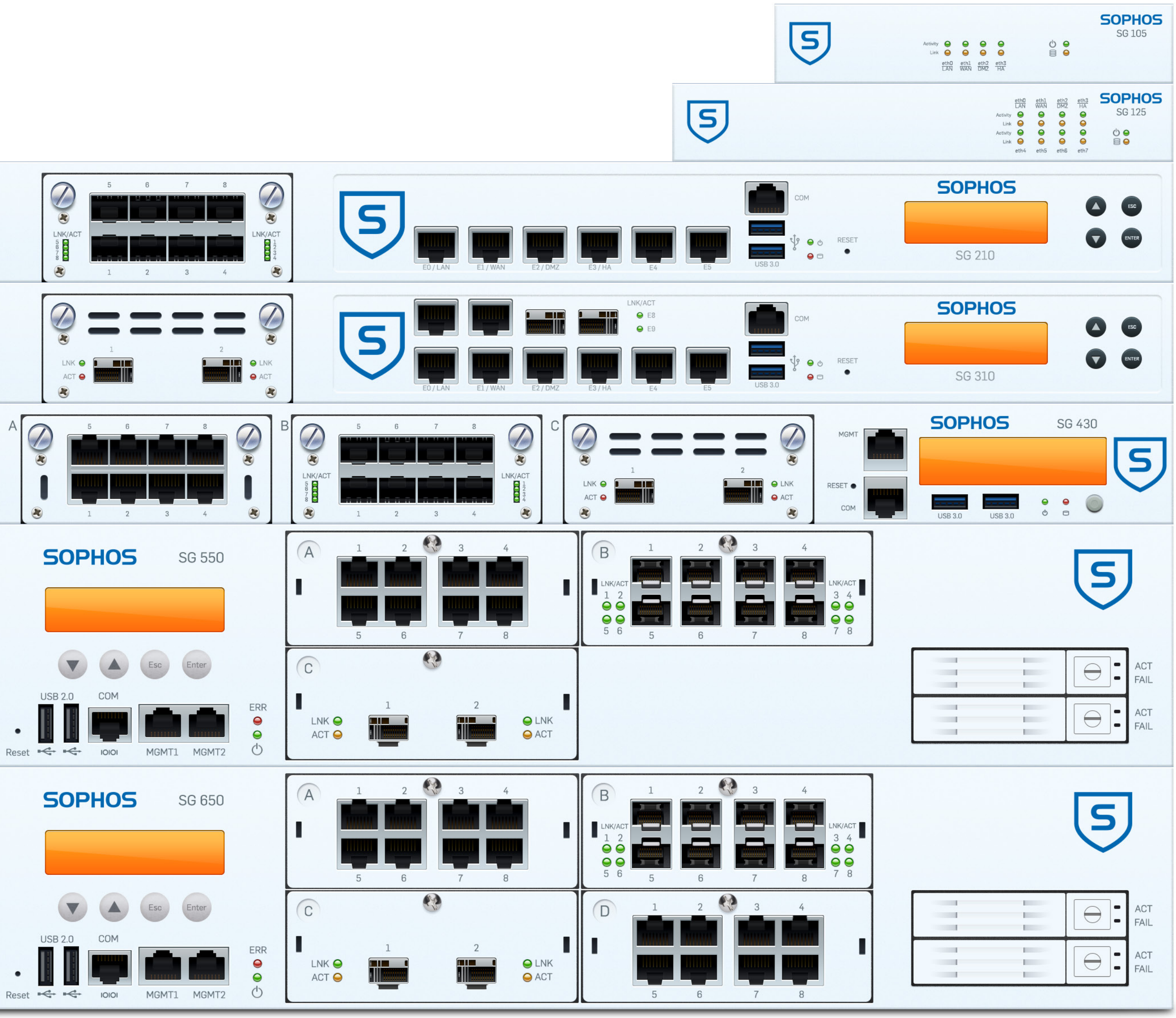
SOPHOS
Security made simple.

Sizing Guideline

Sophos UTM 9.2 - SG Series Appliances



Sophos UTM 9.2 Sizing Guide for SG Series appliances

Three steps to specifying the right appliance model

This document provides a guideline for choosing the right Sophos SG 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 SG Series appliance will see at peak times.
2. **Make a first estimate**
   Based on the Total UTM 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 UTM 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 SG Series appliance you can offer a free on-site evaluation of the selected unit.

1. Identify the "Total UTM User" number

Use the following table to first calculate the Total UTM 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 UTM Users" box.

Table 1.1

	User Count	Multiplied by	Weighted User Count
Standard user		1	
Advanced Users		1.5	
Power Users		2	
Total User Count		Total Weighted User Count	
		multiplied by System Load	
		Total UTM Users	

1.2 User Category Criteria

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

	Average user	Advanced user (*1.5)	Power user (*2)
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.

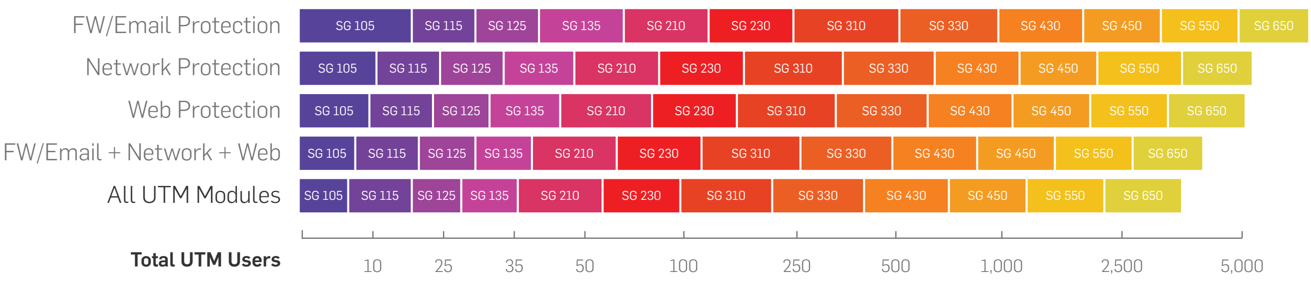
	Average system usage	Advanced system usage (*1.2)	High system usage (*1.5)
Authentication			
Active Directory in use	No	Yes	Yes
FW/IPS/VPN usage			
Variety of systems to be protected by IPS	No IPS protection required	Mostly Windows PCs, 1-2 servers	Various Client Operating systems, browsers and multimedia 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 first estimate — using the calculated “Total UTM User” number

Take the “Total UTM User” and make a first estimate for the required SG 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:

- Estimate that adding Wireless Protection, Webserver Protection or Endpoint 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 SG 230 instead of an SG 210, even though the calculated total number of users is around 100. In that case even an SG 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 wants 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 require that the unit must scan the complete internal traffic between all segments.

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 SG 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 mix, maximum numbers represent best throughput achievable under perfect conditions, e.g. using large packet sizes.

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. For detailed information please refer to the "Sophos UTM - Performance Test Methodology" document.

Small - Desktop

Model	SG 105/w rev.1	SG 115/w rev.1	SG 125/w rev.1	SG 135/w rev.1
Performance Numbers				
Firewall max.[1] (Mbps)	1,500	2,300	3,100	6,000
Firewall Realworld[2] (Mbps)	1,420	1,630	2,100	3,650
ATP Realworld[2] (Mbps)	1,260	1,470	1,490	3,200
IPS max.[1] (Mbps)	350	500	750	1,500
IPS all rules (Mbps)	165	200	320	540
FW + ATP + IPS max.[1] (Mbps)	810	950	1,140	1,750
FW + ATP + IPS Realworld[2] (Mbps)	120	135	165	370
App Ctrl Realworld[2] (Mbps)	1,320	1,430	1,790	3,120
VPN AES max.[3] (Mbps)	325	425	500	1,000
VPN AES Realworld[4] (Mbps)	95	130	155	280
Web Proxy plain[5] (Mbps)	215	380	475	850
Web Proxy – AV[5] (Mbps)	90	120	200	350
Web requests/sec[5] – AV	360	500	900	1,650
Maximum recommended connections				
New TCP connections/sec	15,000	20,000	24,000	36,000
Concurrent TCP connections	1,000,000	1,000,000	2,000,000	2,000,000
Concurrent IPsec VPN tunnels	80	145	175	250
Concurrent SSL VPN tunnels	35	55	75	120
Concurrent Endpoints	10	20	30	40
Concurrent Access Points	10	20	30	40
Concurrent REDs (UTM/FW)	10/30	15/60	20/80	25/100

[1] 1518 byte packet size (UDP), default rule set

[2] NSS Perimeter Mix (TCP/UCP)

[3] AES-NI with AES GCM where possible (UDP)

[4] NSS Core Mix (TCP/UCP)

[5] Throughput: 100kByte files, requests/sec: 1Kbyte files (numbers are for single scan, throughput will decrease by 15-20% when dual scan is activated)

[6] Technical limit

Medium - 1U

Model	SG 210 rev.1	SG 230 rev.1	SG 310 rev.1	SG 330 rev.1	SG 430 rev.1	SG 450 rev.1
Performance Numbers						
Firewall max.[1] (Mbps)	11,000	13,000	17,000	20,000	25,000	27,000
Firewall Realworld[2] (Mbps)	6,270	6,350	6,560	8,850	11,450	12,750
ATP Realworld[2] (Mbps)	3,724	3,748	5,230	8,550	11,310	12,180
IPS max.[1] (Mbps)	2,000	3,000	5,000	6,000	7,000	8,000
IPS all rules (Mbps)	608	714	1,390	1,420	1,650	1,970
FW + ATP + IPS max.[1] (Mbps)	1,910	2,850	4,790	5,890	6,650	7,570
FW + ATP + IPS Realworld[2] (Mbps)	432	572	875	880	950	1,690
App Ctrl Realworld[2] (Mbps)	3,658	3,801	5,150	8,570	11,350	12,230
VPN AES max.[3] (Mbps)	1,000	2,000	3,000	4,000	4,000	5,000
VPN AES Realworld[4] (Mbps)	300	400	850	1,200	1,550	1,800
Web Proxy plain[5] (Mbps)	1,350	1,650	2,100	2,950	3,510	4,100
Web Proxy – AV[5] (Mbps)	500	800	1,200	1,500	2,000	2,500
Web requests/sec[5] – AV	2,100	2,300	3,100	4,200	5,400	6,500
Maximum recommended connections						
New TCP connections/sec	60,000	70,000	100,000	120,000	130,000	140,000
Concurrent TCP connections	4,000,000	4,000,000	6,000,000	6,000,000	8,000,000	8,000,000
Concurrent IPsec VPN tunnels	350	500	800	1,200	1,600	2,000
Concurrent SSL VPN tunnels	180	200	230	250	280	300
Concurrent Endpoints	75	150	300	500	750	1,000
Concurrent Access Points	75	100	125	150	222[6]	222[6]
Concurrent REDs (UTM/FW)	30/125	40/150	50/200	60/230	70/250	80/300

Large - 2U

Model	SG 550 rev.1	SG 650 rev.1
Performance Numbers		
Firewall max.[1] (Mbps)	40,000	60,000
Firewall Realworld[2] (Mbps)	14,070	18,950
ATP Realworld[2] (Mbps)	13,230	17,845
IPS max.[1] (Mbps)	12,000	16,000
IPS all rules (Mbps)	3,895	5,710
FW + ATP + IPS max.[1] (Mbps)	15,980	25,600
FW + ATP + IPS Realworld[2] (Mbps)	3,280	6,130
App Ctrl Realworld[2] (Mbps)	13,350	13,990
VPN AES max.[3] (Mbps)	8,000	10,000
VPN AES Realworld[4] (Mbps)	2,110	2,380
Web Proxy plain[5] (Mbps)	4,700	6,800
Web Proxy – AV[5] (Mbps)	3,500	5,000
Web requests/sec[5] – AV	15,000	23,500
Maximum recommended connections		
New TCP connections/sec	200,000	220,000
Concurrent TCP connections	12,000,000	20,000,000
Concurrent IPsec VPN tunnels	2,200	2,800
Concurrent SSL VPN tunnels	340	420
Concurrent Endpoints	1,000[6]	1,000[6]
Concurrent Access Points	222[6]	222[6]
Concurrent REDs (UTM/FW)	100/400	150/600

1. 1518 byte packet size (UDP), default rule set
2. NSS Perimeter Mix (TCP/UCP)
3. AES-NI with AES GCM where possible (UDP)
4. NSS Core Mix (TCP/UCP)
5. Throughput: 100kByte files, requests/sec: 1Kbyte files (numbers are for single scan, throughput will decrease by 15-20% when dual scan is activated)
6. Technical limit

Sophos UTM Software/Virtual Appliances

For choosing a typical system configuration when installing Sophos UTM software on Intel-compatible PCs/ servers Sophos recommends selecting a Sophos SG Series Hardware appliance that fits the needs first (based on the guidance shown above) and then choose a suitable hardware configuration from the table below.

Model	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 Rangeley Dual Core (1.7 GHz)	Atom Rangeley Quad Core (2.4 GHz)	Celeron Dual Core (2.70GHz)	Pentium Dual Core (3.20GHz)	Dual Core i3 (3.50GHz)	Quad Core i5 (2.9GHz)	Quad Core Xeon E3- (3.20GHz)	Quad Core Xeon E3- (3.50GHz)	2* 6 Core Xeon E5- (2.6 GHz)	2* 10 Core Xeon E5- (2.8 GHz)
Memory (GB)	2	4	4	6	8	8	12	12	16	16	24	48

Using Sophos UTM in a virtual environment has a estimated ~10% performance decrease caused by the Hypervisor framework.

How is “user” defined in licenses for software/virtual installations?

“User”, in the sense of Sophos software licensing, are workstations, clients servers, and other devices that have an IP-address and are protected by or recieve service from the Sophos gateway.

As soon as a “user” communicates with or through the gateway, their IP-address is added to the list of licensed devices in the gateway’s local databasae. No distinction is made if the “user” communicates with the Internet or with a device in another LAN-segment. DNS- or DHCP-queries to the gateway are also counted. If several users communicate through a single device with only one IP-address (e.g. mail-server or web-proxy), every user is counted as a separate user.

The license mechanism only uses data from the last seven days. If an IP-address has not been used in the last seven days, it is removed from the database.

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. Hence 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 sizing and in selecting the right platform.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

© Copyright 2014. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

SOPHOS