- **manuals.plus** /
- **Sophos** /
- **Sophos XGS 107 Next-Gen Firewall User Manual**

Sophos XGS 107

Sophos XGS 107 Next-Gen Firewall User Manual

Model: XGS 107 (JA1Z1CSUS)

1. Introduction

This manual provides essential information for the installation, operation, maintenance, and troubleshooting of your Sophos XGS 107 Next-Gen Firewall. The Sophos XGS 107 is designed to deliver robust network security with advanced threat protection capabilities for small to medium businesses and branch offices.

2. What's in the Box

Verify that all components are present in your Sophos XGS 107 package:

- Sophos XGS 107 Next-Gen Firewall Appliance
- US Power Cord
- Base License (pre-activated for 1 year)
- Network Protection (1-year subscription)
- Web Protection (1-year subscription)
- Enhanced Support (1-year subscription)
- Xstream TLS and DPI engine
- Security Heartbeat functionality
- SD-RED VPN capabilities
- Reporting features

3. Setup

3.1 Physical Installation

Place the Sophos XGS 107 on a stable, flat surface in a well-ventilated area. Ensure adequate space around the device for proper airflow. Connect the power cord to the appliance and a suitable power outlet.

3.2 Port Identification

Familiarize yourself with the ports on the rear panel of the Sophos XGS 107:

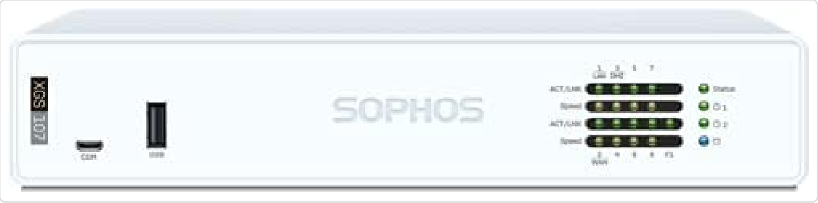


Figure 1: Rear panel of the Sophos XGS 107, featuring dual DC power inputs, a COM port, USB ports, an SFP port, and eight RJ45 LAN/WAN ports. A reset button is also visible.

The front panel includes status LEDs and additional USB ports:

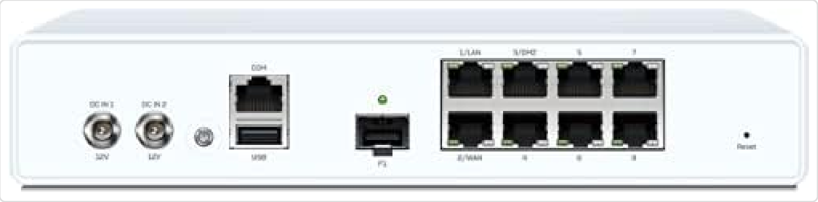


Figure 2: Front panel of the Sophos XGS 107, displaying the Sophos logo, XGS 107 model designation, status LEDs for various functions (Link/Activity, Speed, Status), and USB ports.

3.3 Initial Network Connection

1. Connect your internet service provider's modem or router to the WAN port (typically Port 2) on the Sophos XGS 107.
2. Connect a computer to one of the LAN ports (e.g., Port 1) using an Ethernet cable for initial configuration.
3. Power on the device. Wait for the system status LED to indicate readiness.

3.4 Initial Configuration Access

Access the Sophos Firewall web administration interface by opening a web browser on the connected computer and navigating to the default IP address (e.g., https://172.16.16.16). Follow the on-screen wizard for initial setup, including setting up administrator credentials and basic network parameters.

4. Operating Instructions

The Sophos XGS 107 operates on Sophos proprietary OS, offering a comprehensive suite of security features. The device is designed for ease of management through its web-based interface.

4.1 Xstream Protection Bundle

The XGS 107 comes with the Xstream Protection bundle, providing advanced security features. This bundle includes:

Figure 3: Overview of the Xstream Protection bundle features.

- **Base Firewall Features:** Networking, Wireless, SD-WAN, Application Aware Routing, Traffic Shaping, FastPath, TLS 1.3 Inspection, Deep-Packet Inspection, VPN (IPsec/SSL Site-to-Site and Remote Access VPN), and Reporting.
- **Network Protection:** Xstream TLS Inspection, Xstream DPI engine, IPS (Intrusion Prevention System), Advanced Threat Protection, Synchronized Security Heartbeat, SD-RED VPN.
- **Web Protection:** Xstream TLS Inspection, Web Control, Web Threat Protection, Application Control, Synchronized App Control.
- **Zero-Day Protection:** Xstream TLS Inspection, Xstream DPI engine, Zero-Day Threat Protection, Powered by SophosLabs Intelix, Cloud Sandbox.
- **Sophos Central Management & Orchestration:** Group Firewall Management, backup/firmware updates, SD-WAN Orchestration, Cloud Reporting, XDR and MTR Ready.
- **Enhanced Support:** 24/7 support, feature updates, advanced replacement hardware warranty.

4.2 Detailed Protection Modules

For a comprehensive understanding of each protection module and its capabilities, refer to the detailed descriptions provided:

Figure 4: Detailed breakdown of Sophos Firewall protection modules.

This image provides information on Base Firewall, Network Protection, Web Protection, Zero-Day Protection, Central Orchestration, Email Protection, and Web Server Protection, outlining their respective features and benefits.

5. Maintenance

5.1 Software Updates

Regularly check for and apply firmware updates through the Sophos Firewall web administration interface. Updates provide new features, security patches, and performance improvements. Ensure a stable internet connection during the update process.

5.2 Configuration Backup and Restore

It is recommended to regularly back up your firewall configuration. This allows for quick restoration of settings in case of an issue or during device replacement. Configuration backups can be managed via the web interface.

5.3 Physical Cleaning

Periodically clean the exterior of the appliance with a soft, dry cloth. Ensure ventilation openings are free from dust and obstructions to maintain optimal cooling.

6. Troubleshooting

6.1 Status LED Indicators

Refer to the front panel LEDs (Figure 2) to diagnose basic operational status:

- **System Status LED:** Indicates the overall health and operational state of the device.
- **Link/Activity LEDs:** Show network link status and data activity for each port.
- **Speed LEDs:** Indicate the connection speed of each port.

Consult the Sophos documentation for detailed LED behavior and their corresponding meanings.

6.2 Reset Button

A reset button is located on the rear panel (Figure 1). Pressing this button for a short duration may initiate a soft reboot. Holding it for an extended period (typically 10 seconds or more) may restore the device to factory default settings. Use with caution, as this will erase all configurations.

6.3 Network Connectivity Issues

If you experience network connectivity problems:

- Verify all network cables are securely connected.
- Check the status of your internet service provider's equipment.
- Ensure the Sophos XGS 107 has power and its system status LED is normal.
- Review your firewall rules and network configuration in the web administration interface.

7. Specifications

The following table outlines the technical specifications for the Sophos XGS 107 Next-Gen Firewall:

Protection Modules

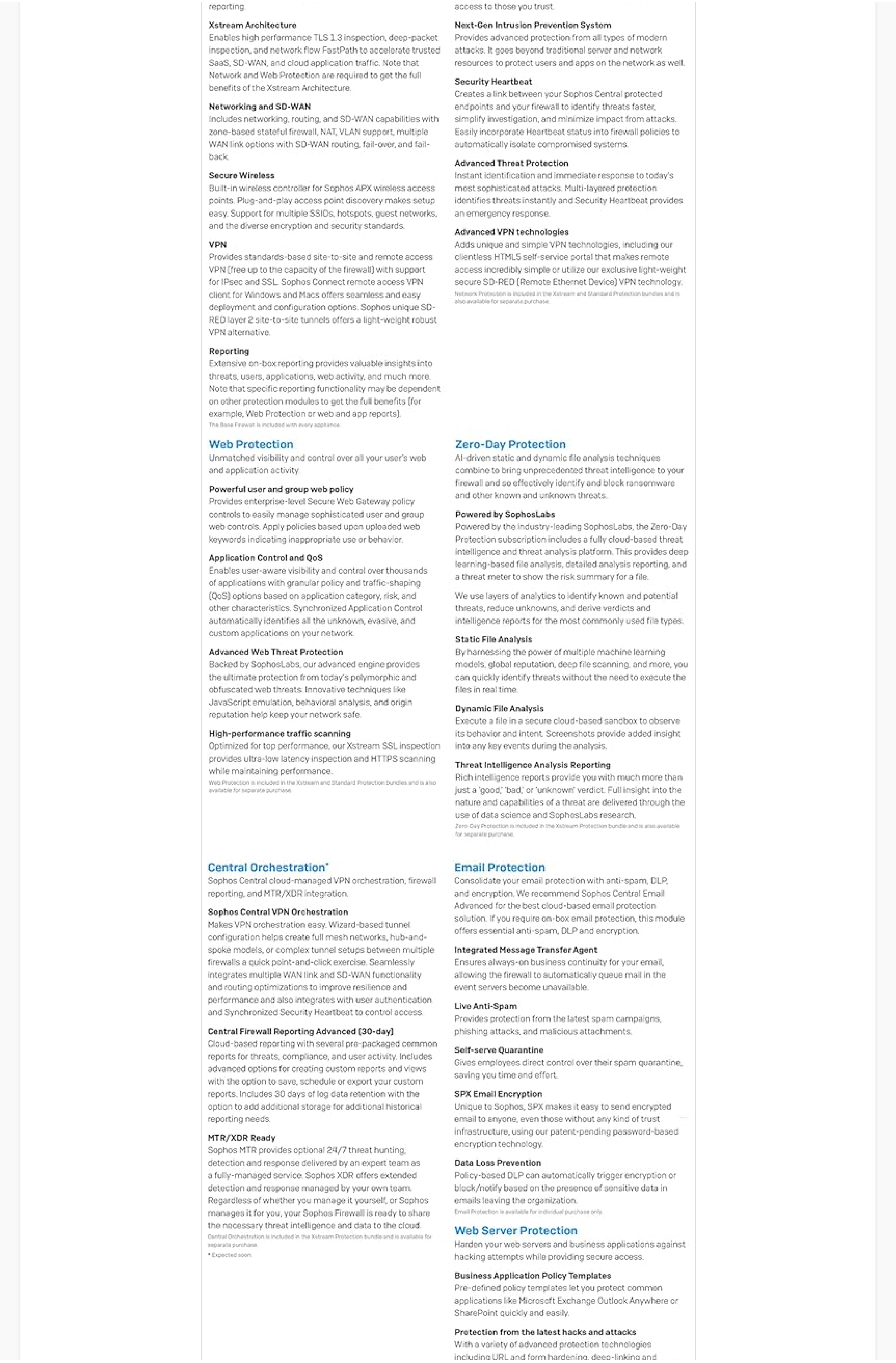
You can choose from a number of modules to customize the protection offered by your firewall to your individual needs and deployment scenario.

Base Firewall

The Sophos Firewall Base license includes the Xstream Architecture, networking, wireless, SD-WAN, VPN, and

Network Protection

All the protection you need to stop sophisticated attacks and advanced threats while providing secure network



reporting.

Xstream Architecture
Enables high performance TLS 1.3 inspection, deep-packet inspection, and network flow FastPath to accelerate trusted SaaS, SD-WAN, and cloud application traffic. Note that Network and Web Protection are required to get the full benefits of the Xstream Architecture.

Networking and SD-WAN
Includes networking, routing, and SD-WAN capabilities with zone-based stateful firewall, NAT, VLAN support, multiple WAN link options with SD-WAN routing, fail-over, and fail-back.

Secure Wireless
Built-in wireless controller for Sophos APX wireless access points. Plug-and-play access point discovery makes setup easy. Support for multiple SSIDs, hotspots, guest networks, and the diverse encryption and security standards.

VPN
Provides standards-based site-to-site and remote access VPN (free up to the capacity of the firewall) with support for IPsec and SSL. Sophos Connect remote access VPN client for Windows and Macs offers seamless and easy deployment and configuration options. Sophos unique SD-RED layer 2 site-to-site tunnels offers a light-weight robust VPN alternative.

Reporting
Extensive on-box reporting provides valuable insights into threats, users, applications, web activity, and much more. Note that specific reporting functionality may be dependent on other protection modules to get the full benefits (for example, Web Protection or web and app reports).

The Base Firewall is included with every appliance.

access to those you trust.

Next-Gen Intrusion Prevention System
Provides advanced protection from all types of modern attacks. It goes beyond traditional server and network resources to protect users and apps on the network as well.

Security Heartbeat
Creates a link between your Sophos Central protected endpoints and your firewall to identify threats faster, simplify investigation, and minimize impact from attacks. Easily incorporate Heartbeat status into firewall policies to automatically isolate compromised systems.

Advanced Threat Protection
Instant identification and immediate response to today's most sophisticated attacks. Multi-layered protection identifies threats instantly and Security Heartbeat provides an emergency response.

Advanced VPN technologies
Adds unique and simple VPN technologies, including our clientless HTML5 self-service portal that makes remote access incredibly simple or utilize our exclusive light-weight secure SD-RED (Remote Ethernet Device) VPN technology.

Network Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

Web Protection

Unmatched visibility and control over all your user's web and application activity.

Powerful user and group web policy
Provides enterprise-level Secure Web Gateway policy controls to easily manage sophisticated user and group web controls. Apply policies based upon uploaded web keywords indicating inappropriate use or behavior.

Application Control and QoS
Enables user-aware visibility and control over thousands of applications with granular policy and traffic-shaping (QoS) options based on application category, risk, and other characteristics. Synchronized Application Control automatically identifies all the unknown, evasive, and custom applications on your network.

Advanced Web Threat Protection
Backed by SophosLabs, our advanced engine provides the ultimate protection from today's polymorphic and obfuscated web threats. Innovative techniques like JavaScript emulation, behavioral analysis, and origin reputation help keep your network safe.

High-performance traffic scanning
Optimized for top performance, our Xstream SSL inspection provides ultra-low latency inspection and HTTPS scanning while maintaining performance.

Web Protection is included in the Xstream and Standard Protection bundles and is also available for separate purchase.

Zero-Day Protection

AI-driven static and dynamic file analysis techniques combine to bring unprecedented threat intelligence to your firewall and so effectively identify and block ransomware and other known and unknown threats.

Powered by SophosLabs
Powered by the industry-leading SophosLabs, the Zero-Day Protection subscription includes a fully cloud-based threat intelligence and threat analysis platform. This provides deep learning-based file analysis, detailed analysis reporting, and a threat meter to show the risk summary for a file.

We use layers of analytics to identify known and potential threats, reduce unknowns, and derive verdicts and intelligence reports for the most commonly used file types.

Static File Analysis
By harnessing the power of multiple machine learning models, global reputation, deep file scanning, and more, you can quickly identify threats without the need to execute the files in real time.

Dynamic File Analysis
Execute a file in a secure cloud-based sandbox to observe its behavior and intent. Screenshots provide added insight into any key events during the analysis.

Threat Intelligence Analysis Reporting
Rich intelligence reports provide you with much more than just a 'good,' 'bad,' or 'unknown' verdict. Full insight into the nature and capabilities of a threat are delivered through the use of data science and SophosLabs research.

Zero-Day Protection is included in the Xstream Protection bundle and is also available for separate purchase.

Central Orchestration*

Sophos Central cloud-managed VPN orchestration, firewall reporting, and MTR/XDR integration.

Sophos Central VPN Orchestration
Makes VPN orchestration easy. Wizard-based tunnel configuration helps create full mesh networks, hub-and-spoke models, or complex tunnel setups between multiple firewalls a quick point-and-click exercise. Seamlessly integrates multiple WAN link and SD-WAN functionality and routing optimizations to improve resilience and performance and also integrates with user authentication and Synchronized Security Heartbeat to control access.

Central Firewall Reporting Advanced (30-day)
Cloud-based reporting with several pre-packaged common reports for threats, compliance, and user activity. Includes advanced options for creating custom reports and views with the option to save, schedule or export your custom reports. Includes 30 days of log data retention with the option to add additional storage for additional historical reporting needs.

MTR/XDR Ready
Sophos MTR provides optional 24/7 threat hunting, detection and response delivered by an expert team as a fully-managed service. Sophos XDR offers extended detection and response managed by your own team. Regardless of whether you manage it yourself, or Sophos manages it for you, your Sophos Firewall is ready to share the necessary threat intelligence and data to the cloud.

Central Orchestration is included in the Xstream Protection bundle and is available for separate purchase.

* Expected soon.

Email Protection

Consolidate your email protection with anti-spam, DLP, and encryption. We recommend Sophos Central Email Advanced for the best cloud-based email protection solution. If you require on-box email protection, this module offers essential anti-spam, DLP and encryption.

Integrated Message Transfer Agent
Ensures always-on business continuity for your email, allowing the firewall to automatically queue mail in the event servers become unavailable.

Live Anti-Spam
Provides protection from the latest spam campaigns, phishing attacks, and malicious attachments.

Self-serve Quarantine
Gives employees direct control over their spam quarantine, saving you time and effort.

SPX Email Encryption
Unique to Sophos, SPX makes it easy to send encrypted email to anyone, even those without any kind of trust infrastructure, using our patent-pending password-based encryption technology.

Data Loss Prevention
Policy-based DLP can automatically trigger encryption or block/notify based on the presence of sensitive data in emails leaving the organization.

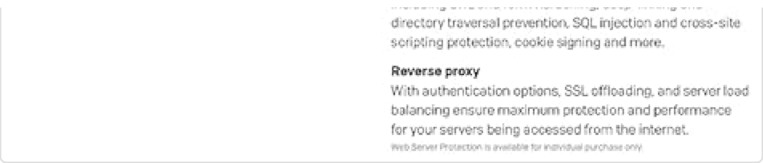
Email Protection is available for individual purchase only.

Web Server Protection

Harden your web servers and business applications against hacking attempts while providing secure access.

Business Application Policy Templates
Pre-defined policy templates let you protect common applications like Microsoft Exchange Outlook Anywhere or SharePoint quickly and easily.

Protection from the latest hacks and attacks
With a variety of advanced protection technologies including URL and form hardening, deep-linking and



directory traversal prevention, SQL injection and cross-site scripting protection, cookie signing and more.

Reverse proxy

With authentication options, SSL offloading, and server load balancing ensure maximum protection and performance for your servers being accessed from the internet.

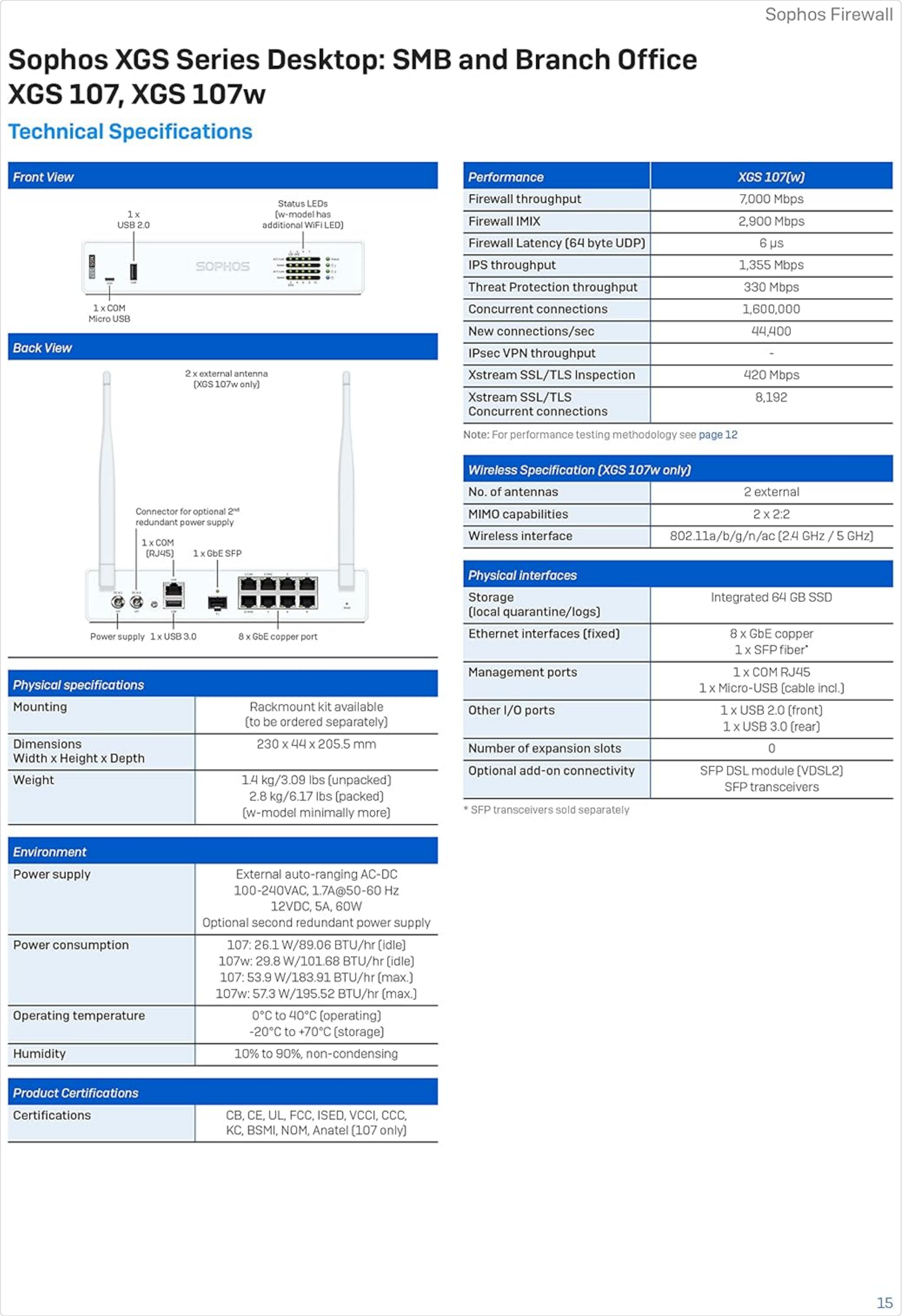
Web Server Protection is available for individual purchase only

Figure 5: Technical Specifications for Sophos XGS 107.

Sophos XGS 107 Key Specifications

Feature	Detail
Brand	Sophos
Model	XGS 107
Firewall Throughput	7,000 Mbps
VPN Throughput	2,030 Mbps
Threat Protection Throughput	330 Mbps
LAN Port Bandwidth	7 Gbps
Number of Ports	13 (including 8x 2.5GE, 1x SFP, 2x USB, 1x COM)
Wireless Communication Standard	802.11n (if applicable for XGS 107w variant)
Operating System	Sophos proprietary OS
Item Weight	8 Pounds
Included Components	1-Year Protection, US Power Cord, Base License, Network Protection, Web Protection, Enhanced Support, Xstream TLS and DPI engine, Security Heartbeat, SD-RED VPN, Reporting

For a comparison of XGS series appliances and their performance metrics, refer to the product matrix:



Sophos Firewall

Sophos XGS Series Desktop: SMB and Branch Office XGS 107, XGS 107w

Technical Specifications

Front View

Back View

Physical specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Height x Depth	230 x 44 x 205.5 mm
Weight	1.4 kg/3.09 lbs (unpacked) 2.8 kg/6.17 lbs (packed) (w-model minimally more)

Environment	
Power supply	External auto-ranging AC-DC 100-240VAC, 1.7A@50-60 Hz 12VDC, 5A, 60W Optional second redundant power supply
Power consumption	107: 26.1 W/89.06 BTU/hr (idle) 107w: 29.8 W/101.68 BTU/hr (idle) 107: 53.9 W/183.91 BTU/hr (max.) 107w: 57.3 W/195.52 BTU/hr (max.)
Operating temperature	0°C to 40°C (operating) -20°C to +70°C (storage)
Humidity	10% to 90%, non-condensing

Product Certifications	
Certifications	CB, CE, UL, FCC, ISED, VCCI, CCC, KC, BSMI, NOM, Anatel (107 only)

Performance	XGS 107(w)
Firewall throughput	7,000 Mbps
Firewall IMIX	2,900 Mbps
Firewall Latency (64 byte UDP)	6 µs
IPS throughput	1,355 Mbps
Threat Protection throughput	330 Mbps
Concurrent connections	1,600,000
New connections/sec	44,400
IPsec VPN throughput	-
Xstream SSL/TLS Inspection	420 Mbps
Xstream SSL/TLS Concurrent connections	8,192

Note: For performance testing methodology see page 12

Wireless Specification (XGS 107w only)	
No. of antennas	2 external
MIMO capabilities	2 x 2:2
Wireless interface	802.11a/b/g/n/ac (2.4 GHz / 5 GHz)

Physical interfaces	
Storage (local quarantine/logs)	Integrated 64 GB SSD
Ethernet interfaces (fixed)	8 x GbE copper 1 x SFP fiber*
Management ports	1 x COM RJ45 1 x Micro-USB (cable incl.)
Other I/O ports	1 x USB 2.0 (front) 1 x USB 3.0 (rear)
Number of expansion slots	0
Optional add-on connectivity	SFP DSL module (VDSL2) SFP transceivers

* SFP transceivers sold separately

15

Figure 6: Sophos XGS Series Product Matrix.

8. Warranty and Support

Your Sophos XGS 107 Next-Gen Firewall includes a 1-year Standard Protection bundle, which provides:

- Base License

- Network Protection
- Web Protection
- Enhanced Support

Enhanced Support includes 24/7 technical assistance and an advanced replacement hardware warranty. For detailed terms and conditions of your warranty and support services, please refer to the official Sophos website or contact your Sophos reseller.

8.1 Contacting Support

For technical assistance, visit the official Sophos support portal or contact Sophos customer service. Ensure you have your product serial number and license information available when seeking support.