Sophos XGS 136

Sophos XGS 136 Next-Gen Firewall User Manual

Model: XGS 136

1. Introduction

This manual provides essential information for the installation, operation, and maintenance of your Sophos XGS 136 Next-Gen Firewall. The Sophos XGS 136 is designed to deliver advanced network security with high performance, utilizing a dual-processor architecture and a dedicated Xstream Flow Processor for accelerated threat processing.

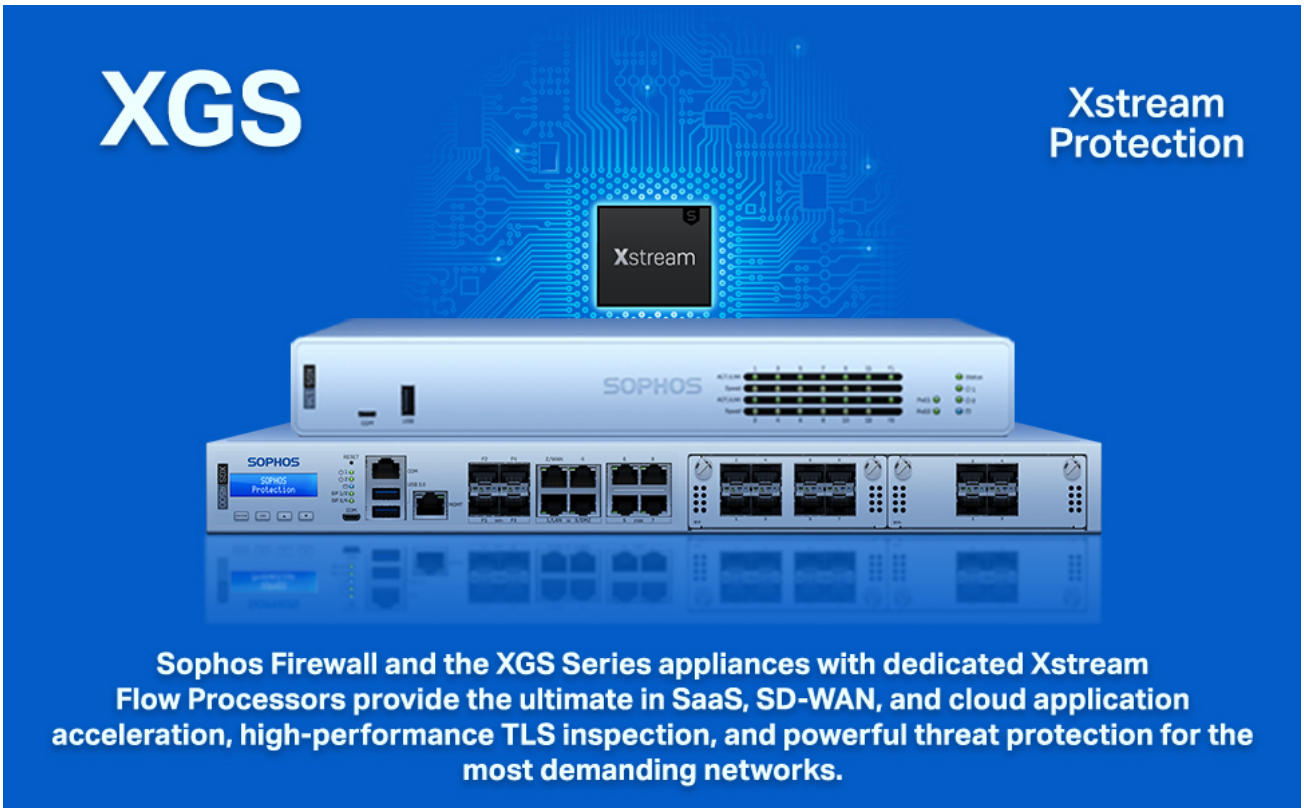


Image 1.1: Sophos XGS Series with Xstream Protection overview. This image illustrates the core components and the protective capabilities of the Sophos XGS firewall.

2. Product Overview

The Sophos XGS 136 is a desktop-form factor next-generation firewall suitable for small to medium businesses and branch

offices. It integrates multiple security functions into a single appliance, providing comprehensive protection against various cyber threats. The device features multiple network ports for flexible deployment and connectivity.

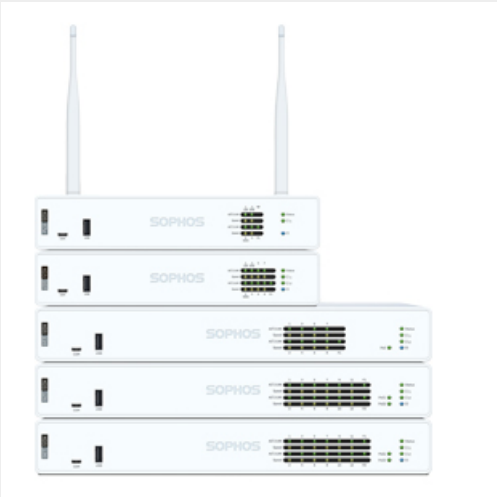


Image 2.1: Sophos XGS Series Appliances. This image displays a stack of various Sophos XGS series firewall models, highlighting their compact design.

2.1 Front Panel

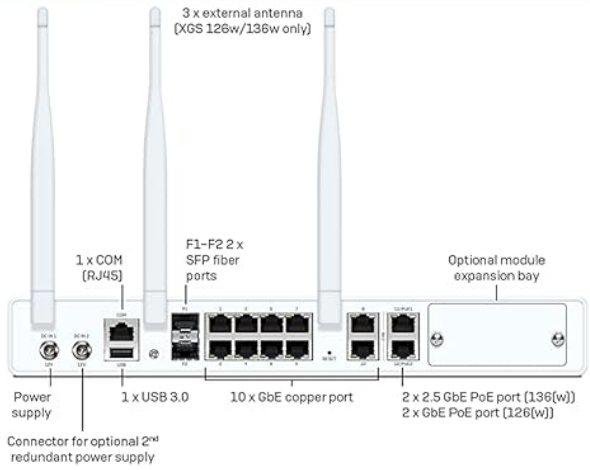
The front panel of the Sophos XGS 136 features status indicators and a USB port for management or external storage.

Sophos XGS Series Desktop: SMB and Branch Office
XGS 126, XGS 126w, XGS 136, XGS 136w

Technical Specifications

Front View

Back View



Physical specifications	
Mounting	Rackmount kit available (to be ordered separately)
Dimensions Width x Height x Depth	320 x 44 x 213 mm
Weight	2.4 kg/5.29 lbs (unpacked) 4.4 kg/9.70 lbs (packed) (w-model minimally higher)

Environment	
Power supply	External auto-ranging AC-DC 100-240VAC, 2.5A@50-60 Hz 12VDC, 12.5A, 150W Optional second redundant power supply
Power consumption	126/136: 30 W/102 BTU/hr (idle) 126w/136w: 32 W/109 BTU/hr (idle) 126: 59 W/202 BTU/hr (max.) 126w/136: 62 W/212 BTU/hr (max.) 136w: 65 W/222 BTU/hr (max.)
PoE addition enabled	76 W/260 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*

* Certification may not be available from launch

Performance	XGS 126(w)	XGS 136(w)
Firewall throughput	10,500 Mbps	11,500 Mbps
Firewall IMIX	4,000 Mbps	4,700 Mbps
Firewall Latency (64 byte UDP)	8 µs	8 µs
IPS throughput	2,600 Mbps	3,300 Mbps
Threat Protection throughput	900 Mbps	1,000 Mbps
Concurrent connections	5,000,000	6,400,000
New connections/sec	69,900	74,500
IPsec VPN throughput	-	-
Xstream SSL/TLS Inspection	800 Mbps	950 Mbps
Xstream SSL/TLS Concurrent connections	12,288	18,432

Note: For performance testing methodology see page 12

Wireless Specification (XGS 126w and XGS 136w only)	
No. of antennas	3 external
MIMO capabilities	3 x 3:3
Wireless interface	Wi-Fi 5/802.11a/b/g/n/ac (2.4 GHz / 5 GHz)
Optional 2nd Wi-Fi Module	Wi-Fi 5/802.11a/b/g/n/ac

Physical interfaces		
Storage (local quarantine/logs)	Integrated 64 GB SSD	
Ethernet interfaces (fixed)	12 x GbE copper 2 x SFP fiber*	10 x GbE copper 2 x 2.5 GbE copper 2 x SFP fiber*
Power-over-Ethernet (fixed)	2 x GbE (30W max. per port)	2 x 2.5 GbE (30W max. per port)
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	1	
Optional add-on connectivity	SFP DSL module (VDSL2) 3G/4G module Second Wi-Fi radio (XGS 126w/136w only) SFP transceivers	

* SFP transceivers sold separately

Image 2.2: Front view of the Sophos XGS 136 firewall. This image shows the status LEDs, USB 2.0 port, and the Sophos branding on the front panel.

2.2 Rear Panel

The rear panel provides all necessary connectivity options, including power inputs, network interfaces, and a console port for initial configuration.

Sophos XGS Series Appliances

All XGS Series firewall appliances are built upon a dual-processor architecture, combining a high-performance, multi-core CPU with a dedicated Xstream Flow Processor for targeted acceleration at the hardware level. This gives you all the flexibility and adaptability of an x86 based firewall plus a significant performance boost over legacy firewall designs.

Product Matrix

Model		Tech Specs			Throughput			
	Form Factor	Ports/Slots (Max Ports)	w-model*	Swappable Components	Firewall (Mbps)	IPsec VPN (Mbps)	Threat Protection (Mbps)	Xstream SSL/TLS (Mbps)
XGS 87(w)	Desktop	5/- (5)	Wi-Fi 5	n/a	3,700	-	240	375
XGS 107(w)	Desktop	9/- (9)	Wi-Fi 5	Second power supply	7,000	-	330	420
XGS 116(w)	Desktop	9/1 (9)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	7,700	-	685	650
XGS 126(w)	Desktop	14/1 (14)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	10,500	-	900	800
XGS 136(w)	Desktop	14/1 (14)	Wi-Fi 5	Second power supply, 3G/4G, Wi-Fi**	11,500	-	1,000	950
XGS 2100	1U	10/1 (18)	n/a	Optional external power	30,000	-	1,250	1,100
XGS 2300	1U	10/1 (18)	n/a	Optional external power	35,000	-	1,400	1,450
XGS 3100	1U	12/1 (20)	n/a	Optional external power	38,000	-	2,000	2,470
XGS 3300	1U	12/1 (20)	n/a	Optional external power	40,000	-	2,770	3,130
XGS 4300	1U	12/2 (28)	n/a	Optional external power	75,000	-	4,800	8,000
XGS 4500	1U	12/2 (28)	n/a	Optional internal power	80,000	-	8,390	10,600
XGS 5500	2U	16/3 (48)	n/a	Power, SSD, Fan	100,000	-	12,390	13,500
XGS 6500	2U	20/4 (68)	n/a	Power, SSD, Fan	115,000	-	17,050	16,000

* 802.11ac Wave 2

** Second Wi-Fi module option for XGS 116w, 126w and 136w only

Performance Test Methodology

General: Maximum throughput measured under ideal test conditions using industry standard Keysight-Ixia BreakingPoint test tools. Actual performance may vary depending on network conditions and activated services.

- **Firewall:** Measured using HTTP traffic and 512 KB response size.
- **Firewall IMIX:** UDP throughput based on a combination of 66 byte, 570 byte and 1518 byte packet sizes.
- **IPS:** Measured with IPS with HTTP traffic using default IPS ruleset and 512 KB object size.
- **IPsec VPN:** HTTP throughput using multiple tunnels and 512 KB HTTP response size.
- **TLS inspection:** Performance measured with IPS with HTTPS sessions and different cipher suites.
- **Threat Protection:** Measured with Firewall, IPS, Application Control, and malware prevention enabled using HTTP 200 KB response size.

Image 2.3: Rear view of the Sophos XGS 136 firewall. This image displays the dual DC power inputs, console port, USB 3.0 ports, 10 GE copper ports, and SFP ports.

3. Setup and Installation

Follow these general steps for initial setup of your Sophos XGS 136 firewall:

1. **Unpack the Device:** Carefully remove the firewall from its packaging. Ensure all components, including the US power cord, are present.
2. **Physical Placement:** Place the device on a stable, flat surface in a well-ventilated area. Ensure adequate space around the unit for airflow.
3. **Connect Power:** Connect the provided US power cord to the device's power input and then to a suitable power outlet. The device supports dual DC power inputs for redundancy.

4. **Network Connections:** Connect your network cables to the appropriate LAN and WAN ports on the rear panel. Refer to the rear panel diagram for port identification.
5. **Initial Configuration:** Connect a computer to the console port using a serial cable (if required) or use a network port for web-based management. Follow the Sophos documentation for initial configuration steps, including setting up network interfaces and basic security policies.

4. Operating Principles and Protection Features

The Sophos XGS 136 leverages Sophos Firewall's Xstream Protection architecture to provide comprehensive security. This includes advanced threat protection, deep packet inspection, and intelligent traffic management.

Image 4.1: Xstream Protection - A Single Bundle For Ultimate Protection. This image outlines the key features of the Xstream Protection bundle, including Base Firewall, Network Protection, Web Protection, and Zero-Day Protection.

4.1 Protection Modules

The XGS 136 offers a variety of protection modules that can be customized to meet specific security requirements:

- **Base Firewall:** Includes networking, wireless, SD-WAN, application awareness, traffic shaping, and VPN capabilities.
- **Network Protection:** Provides intrusion prevention, advanced threat protection, synchronized security heartbeat, and clientless VPN.
- **Web Protection:** Offers web control, application control, synchronized app control, and extensive reporting.
- **Zero-Day Protection:** Utilizes deep packet inspection, machine learning, cloud sandboxing, and advanced threat intelligence to block unknown threats.

Image 4.2: Blocks Unknown Threats. This image highlights the firewall's capability to block new and emerging threats.

Image 4.3: Exposes Hidden Risks. This image emphasizes the firewall's ability to identify and mitigate hidden network vulnerabilities.

Image 4.4: Automatically Responds to Incidents. This image illustrates the firewall's automated response capabilities to security incidents.

5. Licensing Options

Sophos offers various licensing bundles to customize the protection level for your firewall. These bundles provide different levels of security features and support.

Image 5.1: All Licensing Options for Sophos XGS Series. This image details the various protection bundles available, including Xstream Protection, Standard Protection, and additional modules.

For detailed information on each protection bundle and its included features, refer to the Sophos Firewall Feature List documentation.

6. Specifications

The following tables provide detailed technical specifications and performance metrics for the Sophos XGS 136 firewall.

All Licensing Options

We recommend the Xstream Protection bundle for the ultimate in security, but if you prefer to customize your protection, all subscriptions are also available for individual purchase.

Xstream Protection Bundle:	
Base License	Networking, Wireless, Xstream Architecture, Unlimited Remote Access VPN, Site-to-Site VPN, reporting
Network Protection	Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
Web Protection	Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting
Zero-Day Protection	Machine Learning and Sandboxing File Analysis, reporting
Central Orchestration*	SD-WAN VPN Orchestration, Central Firewall Advanced Reporting (30-days), MTR/XDR ready
Enhanced Support	24/7 support, feature updates, advanced replacement hardware warranty for term

* Expected soon

Custom Protection: If you only require basic protection or want to customize your protection, you can choose the Standard Protection Bundle or purchase any of the protection modules separately.

Standard Protection Bundle:	
Base License	Networking, wireless, Xstream Architecture, unlimited Remote Access VPN, Site-to-Site VPN, reporting
Network Protection	Xstream TLS and DPI engine, IPS, ATP, Security Heartbeat, SD-RED VPN, reporting
Web Protection	Xstream TLS and DPI engine, Web Security and Control, Application Control, reporting
Enhanced Support	24/7 support, feature updates, advanced replacement hardware warranty for term

Additional Protection Modules:	
Email Protection	On-box antispam, AV, DLP, encryption
Web Server Protection	Web Application Firewall

Sophos Central Management and Reporting: All Sophos Firewalls include cloud management and reporting at no extra charge.

Sophos Central Management and Reporting (included at no charge):	
Sophos Central Management	Group firewall management, backup management, firmware update scheduling
Sophos Central Firewall Reporting	Prepackaged and custom report tools with seven days cloud storage for no extra charge (see other options)

Additional Protection: Extend your protection further with these additional products and services.

Additional Protection Services, Products and Modules:	
Managed Threat Response	24/7 threat hunting, detection and response delivered by an expert team (more info)
Sophos Intercept X Endpoint with XDR	Sophos Central managed next-gen endpoint protection with EDR (more info)
ZTNA	Sophos Central managed Zero Trust Network Access (more info)
Central Email Advanced	Sophos Central managed antispam, AV, DLP, encryption (more info)

Support: Enhanced support is included in all protection bundles, but you can enhance your support experience further by upgrading.

Additional Support Options:	
Enhanced Plus Support Upgrade	Upgrade your support with VIP support, HW warranty for add-ons, TAM option (extra cost)

Cloud, Virtual and Software Appliance Licensing Options: If you're deploying Sophos Firewall in the cloud, in a virtual environment, or as software on your own hardware, the licensing guide below can help you find the right option.

Model	*Equivalent AWS Instance*	*Equivalent Azure VM*	*Software/ Virtual License**
XGS 87	t3.medium	Standard_ F2s_v2	2C4
XGS 107			
XGS 116			
XGS 126	c5.large		
XGS 136	m5.large	Standard_ F4s_v2	4C6
XGS 2100			6C8
XGS 2300	c5.xlarge		
XGS 3100	m5.xlarge	Standard_ F8s_v2	8C16
XGS 3300			
XGS 4300	c5.2xlarge		
XGS 4500			
XGS 5500	c5.4xlarge	Standard_ F16s_v2	16C24
XGS 6500			Unlimited

** Based upon CPU cores and RAM

For a complete list of features included in each protection subscription see the Sophos Firewall Feature List.

Image 6.1: Sophos XGS Series Desktop Technical Specifications. This image presents a table with performance data, physical interfaces, dimensions, weight, power consumption, and certifications for XGS 126, XGS 126w, XGS 136, and XGS 136w models.

6.1 Product Matrix

The product matrix below outlines the key differences and capabilities across various Sophos XGS Series Appliances.

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 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.

Network Protection

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

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.

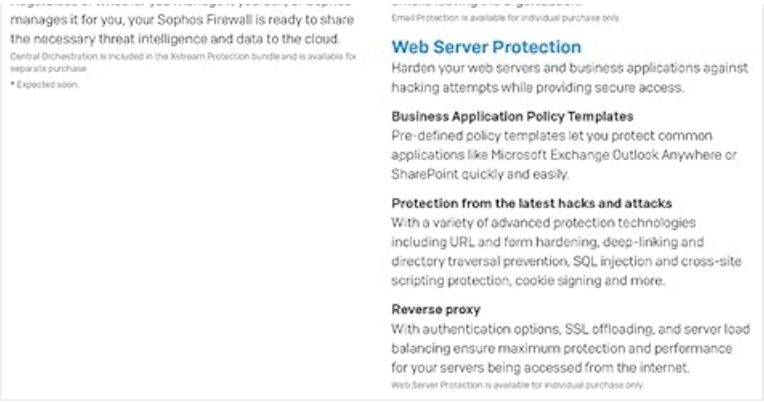


Image 6.2: Sophos XGS Series Appliances Product Matrix. This image provides a comparative table of different XGS models, detailing their form factor, ports/slots, tech specs, and throughput performance metrics.

6.2 Performance Test Methodology

Performance figures are based on maximum throughput measured under ideal test conditions using industry-standard Keysight-Ixia BreakingPoint test tools. Actual performance may vary depending on network conditions and activated services.

- **Firewall:** Measured using HTTP traffic and 512 KB response size.
- **Firewall IMIX:** UDP throughput based on a combination of 66 byte, 570 byte and 1518 byte packet sizes.
- **IPS:** Measured with IPS with HTTP traffic using default IPS ruleset and 512 KB object size.
- **IPsec VPN:** HTTP throughput using multiple tunnels and 512 KB HTTP response size.
- **TLS Inspection:** Performance measured with IPS with HTTPS sessions and different cipher suites.
- **Threat Protection:** Measured with Firewall, IPS, Application Control, and malware prevention enabled using HTTP 200 KB response size.

7. Maintenance

To ensure optimal performance and security of your Sophos XGS 136 firewall, regular maintenance is recommended:

- **Software Updates:** Regularly check for and apply the latest firmware and software updates provided by Sophos. These updates often include security patches and performance enhancements.
- **Configuration Backup:** Periodically back up your firewall configuration. This allows for quick restoration in case of unexpected issues or hardware replacement.
- **Physical Inspection:** Ensure the device is free from dust and that ventilation openings are not obstructed. Maintain a stable operating environment within specified temperature and humidity ranges.
- **Log Review:** Regularly review system logs and security reports for any unusual activity or potential threats.

8. Troubleshooting

If you encounter issues with your Sophos XGS 136, consider the following basic troubleshooting steps:

- **Check Power and Connections:** Verify that the power cord is securely connected and the device is receiving power. Ensure all network cables are properly seated in their respective ports.
- **Status Indicators:** Observe the front panel LEDs. Refer to the Sophos documentation for the meaning of different LED states to diagnose issues.
- **Network Connectivity:** Confirm that connected devices have proper IP configurations and can reach the firewall. Test connectivity to external networks.

- **Restart Device:** As a first step for many issues, try restarting the firewall. Power it off, wait for 30 seconds, and then power it back on.
- **Consult Documentation:** Refer to the official Sophos support documentation and knowledge base for specific error messages or symptoms.
- **Contact Support:** If problems persist, contact Sophos technical support for assistance.

9. Warranty and Support

The Sophos XGS 136 typically includes a standard warranty and can be augmented with various protection plans for extended coverage and support.

- **Standard Protection:** The product includes a 1-year standard protection plan, which covers basic support and hardware replacement.
- **Extended Protection Plans:** Additional protection plans, such as the 4-Year Protection Plan or the monthly Complete Protect plan, are available for purchase to extend coverage and enhance support services. These plans may include advanced threat protection, 24/7 support, feature updates, and expedited hardware replacement.
- **Technical Support:** For technical assistance, please refer to the Sophos support portal or contact your Sophos partner. Ensure you have your product serial number and details of your protection plan readily available.