Sophos XGS 2100

Sophos XGS 2100 Next-Gen Firewall User Manual

Model: XGS 2100 (XG2ATCHUS)

1. Introduction

The Sophos XGS 2100 is a high-performance Next-Gen Firewall designed to provide robust network security for businesses. It integrates advanced threat protection, application acceleration, and high-performance TLS inspection capabilities through its dedicated Xstream Flow Processors. This manual provides essential information for the proper installation, configuration, and maintenance of your Sophos XGS 2100 appliance.

2. Product Overview

2.1 Key Features

- **TLS 1.3 Inspection:** Provides intelligent and efficient decryption and inspection of encrypted web traffic, including TLS 1.3, to eliminate blind spots for malware and unwanted applications without significant performance impact.
- **Deep Packet Inspection (DPI):** Utilizes a high-speed DPI engine to scan network traffic for threats, including next-gen IPS, web protection, and application control, powered by SophosLabs Intelix for advanced threat detection.
- **Xstream Flow Processors:** Dedicated hardware for application acceleration, high-performance TLS inspection, and powerful threat protection, ensuring optimal network performance even under heavy security loads.
- **Threat Protection:** Stops ransomware and breaches with advanced security features, including deep learning and sandboxing.
- **Sophos Firewall OS:** Operates on Sophos Firewall OS, offering comprehensive security management.

2.2 Package Contents

Verify that your package contains the following items:

- Sophos XGS 2100 Next-Gen Firewall Appliance

- US Power Cord
- Documentation (Quick Start Guide, Safety Information)

2.3 Appliance Layout

Familiarize yourself with the ports and indicators on the Sophos XGS 2100 appliance.

Figure 1: Rear Panel of Sophos XGS 2100. This image displays the rear panel of the Sophos XGS 2100 firewall, showing the power input, USB ports, and cooling fans. The power switch is also visible.

The rear panel includes the power input, power switch, USB ports, and cooling fan vents. Specific port configurations may vary based on optional modules.

Figure 2: Front Panel of Sophos XGS 2100. This image shows the front panel of the Sophos XGS 2100 firewall, featuring the multi-function LCD display, console port, USB ports, and various network ports (LAN 1-8 GE copper, SFP/SFP+ ports, and an expansion bay).

The front panel typically features a multi-function LCD display, console port (Micro USB, RJ45), USB ports, and a range of network interfaces including copper GE ports and SFP/SFP+ ports for flexible connectivity. An expansion bay allows for additional modules.

2.4 Model Comparison (XGS Series)

The Sophos XGS Series offers various models with differing specifications. The XGS 2100 is part of this series, providing a balance of performance and features suitable for many business environments.

Figure 3: Sophos XGS Series Product Matrix. This table provides a comparison of various Sophos XGS Series firewall models, detailing their form factor, ports/slots, technical specifications, and throughput capabilities for firewall, IPSec VPN, threat protection, and Xstream SSL/TLS.

Refer to the product matrix for a detailed comparison of throughput and port configurations across the XGS series.

3. Setup

3.1 Initial Hardware Connection

1. **Mounting:** The XGS 2100 is a 1U rackmount appliance. Secure it in a standard 19-inch server rack using appropriate mounting hardware (not included).
2. **Power Connection:** Connect the provided US power cord to the appliance's power input on the rear panel and then to a suitable power outlet.
3. **Network Connections:** Connect your WAN (Internet) and LAN (internal network) cables to the designated network ports on the front panel. Refer to the port labels for correct connections.
4. **Console Connection (Optional):** For initial command-line interface (CLI) access, connect a console cable (Micro USB or RJ45) from your computer to the console port on the front panel.
5. **Power On:** Press the power switch on the rear panel to turn on the appliance. Observe the status indicators

on the front panel.

3.2 Initial Configuration

Upon first boot, the Sophos XGS 2100 will initialize its Sophos Firewall OS. Initial configuration is typically performed via a web browser or the console interface. Refer to the Sophos documentation for detailed steps on accessing the web administration interface and completing the initial setup wizard.

3.3 Zero-Touch Deployment

The Sophos XGS 2100 supports zero-touch deployment through Sophos Central. This allows for remote configuration without on-site technical staff. To utilize this feature, create a configuration for your firewall in Sophos Central, store the configuration file on a USB key, and boot the appliance with the USB key connected. The appliance will automatically retrieve and apply the configuration.

4. Operating Instructions

4.1 Xstream Protection Overview

The Sophos XGS 2100 leverages the Xstream Protection bundle to deliver comprehensive next-generation security. This includes:

- **Base Firewall Features:** Networking and SD-WAN capabilities, application-aware routing, traffic shaping, and robust protection architecture with network flow.
- **Network Protection:** Xstream TLS inspection, deep packet inspection, IPS (Intrusion Prevention System), Advanced Threat Protection, and Synchronized Security Heartbeat.
- **Web Protection:** Xstream TLS inspection, web control, malware and potentially unwanted application detection, and synchronized app control.
- **Zero-Day Protection:** Analyzes unknown files using AI, ML, and sandboxing, powered by SophosLabs Intelix.

Figure 4: Sophos Xstream Protection Overview. This diagram illustrates the components of Sophos's Xstream Protection bundle, including Base Firewall Features, Network Protection, Web Protection, and Zero-Day Protection, highlighting key functionalities within each category.

4.2 Sophos Central Management

Sophos Central provides a unified cloud management platform for your Sophos XGS 2100 firewall and other Sophos products. It simplifies daily setup, monitoring, and management tasks.

- **Central Management:** Manage multiple firewalls from a single console, including group firewall management and policy application.
- **Central Reporting:** Access powerful reporting tools to visualize network activity, security events, and compliance.
- **Backup and Firmware Updates:** Facilitates easy backups and streamlined firmware updates.

Figure 5: Sophos Central Dashboard Example. This image shows examples of the Sophos Central interface, demonstrating dashboards for central firewall management and reporting, providing a consolidated view of network security status.

For more information on Sophos Central, visit sophos.com/firewall-central.

4.3 Synchronized Security

Sophos Synchronized Security integrates your firewall with other Sophos endpoints and security solutions to provide a coordinated defense against cyber threats. This allows for real-time threat intelligence sharing and automated responses.

- **Security Heartbeat:** Shares health status between endpoints and the firewall, enabling automatic isolation of compromised systems.
- **Synchronized Application Control:** Automatically identifies, classifies, and controls applications, including those currently unidentified.
- **Lateral Movement Protection:** Isolates compromised systems to prevent threats from spreading across the network.
- **Synchronized User ID:** Enhances user authentication and policy enforcement.
- **Synchronized SD-WAN:** Optimizes traffic routing based on security and application needs.

Figure 6: Sophos Synchronized Security. This diagram illustrates how Sophos Synchronized Security works, showing the integration between the firewall and endpoints to provide comprehensive threat visibility and automated response capabilities.

5. Maintenance

Regular maintenance ensures the optimal performance and security of your Sophos XGS 2100 firewall.

- **Firmware Updates:** Regularly check for and apply the latest firmware updates through Sophos Central or the local administration interface. Updates often include security patches and new features.
- **Configuration Backups:** Perform regular backups of your firewall configuration. This allows for quick restoration in case of an issue. Sophos Central provides tools for easy backup management.
- **Monitoring:** Monitor system logs and performance metrics through Sophos Central or the local interface to identify potential issues early.
- **Physical Inspection:** Periodically inspect the appliance for proper ventilation and ensure all cables are securely connected.

6. Troubleshooting

This section provides basic troubleshooting steps for common issues. For more complex problems, refer to the Sophos support documentation or contact technical support.

6.1 Common Issues and Solutions

- **No Power:**
  - Ensure the power cord is securely connected to both the appliance and the power outlet.
  - Verify the power switch on the rear panel is in the 'On' position.
  - Check the power outlet with another device.
- **No Network Connectivity:**
  - Check that Ethernet cables are properly connected to the correct WAN/LAN ports.
  - Verify the link/activity lights on the network ports are active.
  - Confirm network settings (IP addresses, subnet masks, gateways) are correctly configured in the

firewall's interface.

- **Slow Performance:**
  - Check the firewall's resource utilization (CPU, memory) through the administration interface.
  - Ensure the appliance is adequately ventilated and not overheating.
  - Review security policies and rules for any misconfigurations that might be causing bottlenecks.
- **Cannot Access Web Interface:**
  - Ensure your computer is on the correct network segment to access the firewall's management interface.
  - Verify the IP address used to access the interface is correct.
  - Try clearing your browser's cache or using a different browser.

If issues persist, consult the comprehensive Sophos documentation available online or contact Sophos Technical Support.

7. Specifications

The following table details the technical specifications and performance metrics for the Sophos XGS 2100 Next-Gen Firewall.

Figure 7: Sophos XGS 2100 Technical Specifications. This table provides detailed technical specifications for the Sophos XGS 2100 and XGS 2300 models, including performance throughputs (Firewall, IMIX, IPS, Threat Protection), physical interfaces, storage, and environmental conditions.

Sophos XGS 2100 Key Specifications

Feature	Detail
Brand	Sophos
Model Name	XGS 2100 US Power Cord
Model Number	XG2ATCHUS
Firewall Throughput	30,000 Mbps
IPS Throughput	5,800 Mbps
Threat Protection Throughput	1,250 Mbps
Operating System	Sophos Firewall OS
Connectivity Technology	Ethernet
Security Protocol	WPA2-PSK, WPA2-Enterprise (Note: This refers to wireless compatibility, the firewall itself handles broader protocols)
Included Components	US power cord
Item Weight	16 Pounds
Dimensions (H x W x D)	438 x 44 x 503 mm (from image)

Feature	Detail
Power Supply	Internal auto-ranging DC 100-240VAC, 3-6A/50-60 Hz

8. Warranty and Support

Sophos provides comprehensive support for its products. For detailed warranty information, please refer to the official Sophos website or the documentation included with your appliance.
For technical assistance, product documentation, and software downloads, visit the official Sophos Support Portal: https://www.sophos.com/support
You can also find more information about Sophos products and solutions on their main website: https://www.sophos.com