SOPHOS

KEY NEW FEATURES IN

Sophos Firewall OS v22

Secure By Design

Sophos Firewall Health Check

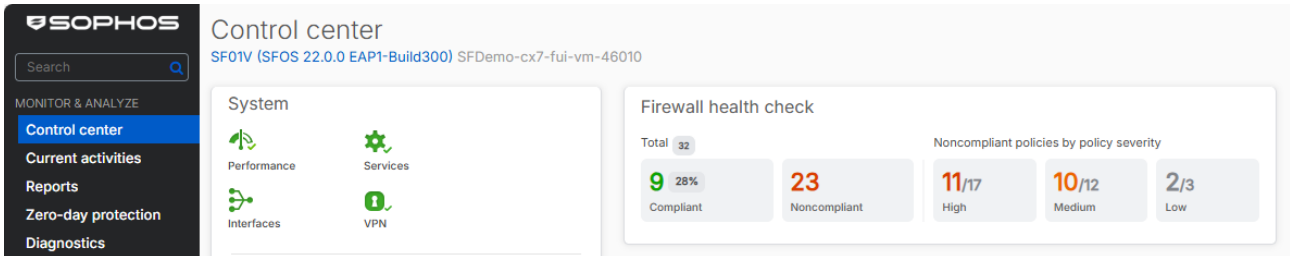
Network infrastructure exposed to the Internet, such as firewalls, are increasingly targeted by attackers as a potential entry point to launch further attacks. This has put a renewed focus on hardening and securing this network infrastructure.

At Sophos, we take security seriously. We support and embrace the principles of Secure by Design as outlined by CISA that prioritizes the security of customers as a core requirement. Over the last several releases, we have continued to invest in implementing Secure by Design principles into all our products, including Sophos Firewall. Sophos Firewall has had numerous updates in the last few years to aggressively harden the product, make it easier to patch vulnerabilities, and to identify when a customer is under attack. As you probably know, Sophos Firewall is unique in offering over-the-air hotfix security updates that can be used to patch new vulnerabilities without scheduling downtime. Sophos is also the only vendor that is actively monitoring our install base to help identify signs of an attacks early.

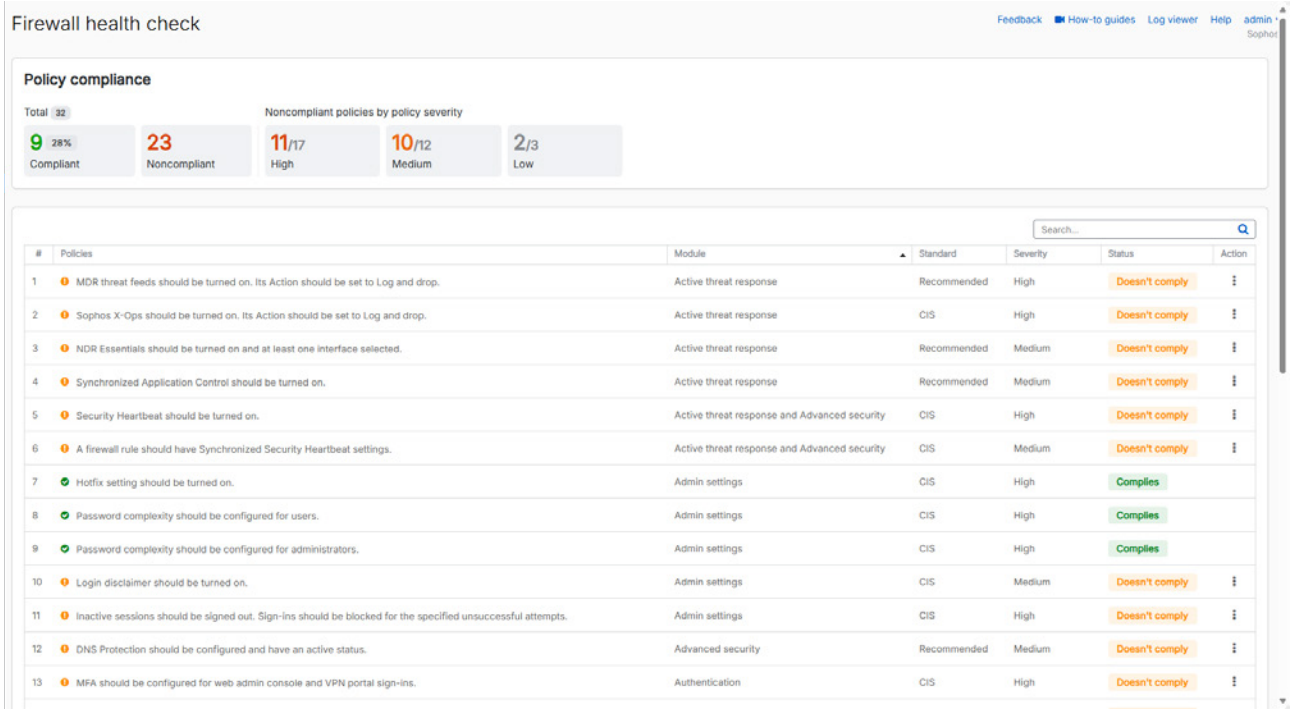
However, it's important that you, as our partners and customers, do your part to keep your network security infrastructure as secure as possible. This means keeping firmware up to date, and ensuring your firewall is optimally configured – following network security best practices to maximize your security posture and eliminate any unintentional weak points that might be exploited by attackers.

Sophos Firewall v22 makes your job of optimally securing your firewall much easier with a new Health Check feature. This new feature evaluates dozens of different configuration settings on your firewall and compares them with CIS benchmark and other best practices, providing immediate insights to areas that may be at risk. It will identify all high-risk settings and provide recommendations with easy drill-down to the areas of concern so you can easily address them.

This new capability includes a new Control Center dashboard widget overview as well as a detailed view available via a click-through or on the main menu under "Firewall health check".



A Health Check summary is presented in a new control center widget that enables a one-click drill-down to the new Health Check feature...



Navigate to the new Health Check feature under the "Monitor and Analyze" section of the main menu or via the Control Center widget to get full details on areas of your configuration that may be at risk and benefit from optimization.

Next-Gen Xstream Architecture

Sophos Firewall introduced the Xstream Architecture as a key component of v18, enabling the XGS Series appliances to take full advantage of the added processing power and capabilities it provided. Since then, Sophos Firewall's Xstream Architecture has been constantly scaling and adapting to bring additional performance to customer networks. This is all thanks to the programmable nature of Sophos Firewall's Xstream Architecture that is NOT dependent on custom silicon ASICs – and in fact works equally well on general-purpose CPUs, virtual CPUs, and our XGS Series models that have dedicated flow processors.

Sophos Firewall v22 introduces our next-generation Xstream Architecture which has an all-new control plane re-architected for maximum security and scalability to take us into the future. The new control plane enables modularization, isolation, and containerization of services like IPS for example, to run like "apps" on the firewall platform. It also enables complete separation of privileges for added security. In addition, High-Availability deployments now benefit from a self-healing capability that is continuously monitoring system state and fixes deviations between devices automatically

The net result is an ultra-secure, scalable, and streamlined architecture built for the future. This next-gen Xstream Architecture lays a foundation for highly secure, scalable, and modular containerized services, n-node clustering, and full RESTful APIs for high-performance remote management and automation.

Hardened Kernel

The next-gen Xstream Architecture in Sophos Firewall OS is built upon a new hardened kernel (v6.6+) that provides enhanced security, performance, and scalability to maximize current and future hardware. The. new kernel offers tighter process isolation and better mitigation for side-channel attacks as well as mitigations for CPU vulnerabilities (Spectre, Meltdown, L1TF, MDS, Retbleed, ZenBleed, Downfall). It also offers hardened usercopy, stack canaries, and Kernel Address Space Layout Randomization (KASLR).

Remote Integrity Monitoring

Sophos Firewall OS v22 now integrates our Sophos XDR Linux Sensor that enables real-time monitoring of system integrity, including unauthorized configuration, rule exports, malicious program execution attempts, file tampering, and more. This helps our security teams who are proactively monitoring our Sophos Firewall install base to better identify, investigate, and respond more quickly to any attack. This is an added security capability that no other firewall vendor provides.

New Anti-Malware Engine

Sophos Firewall OS v22 integrates the latest Sophos anti-malware engine with enhanced zero-day real-time detection of emerging threats. It utilizes SophosLabs global reputation lookups with our massive cloud database of known malicious files, updated every 5 mins or less. It also introduces AI and ML model detections and delivers enhanced telemetry to SophosLabs for accelerating their emerging threat detection analysis.

Other Security and Scalability Enhancements

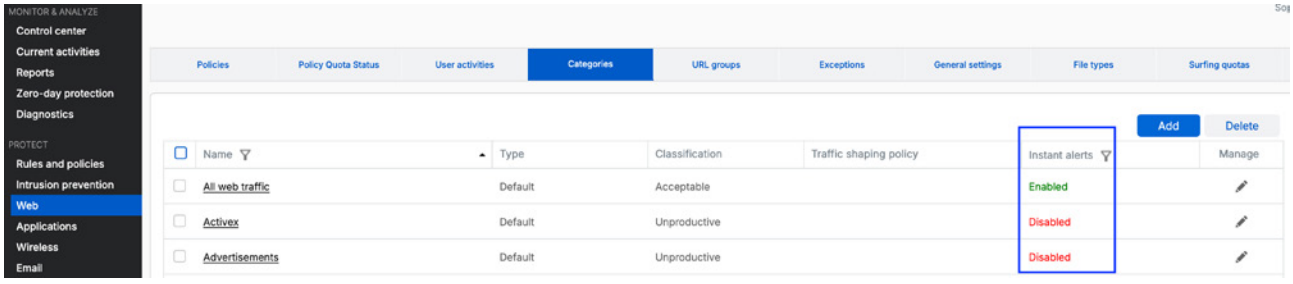
Firmware Updates via SSL and Certificate Pinning – Ensures the authenticity of update servers to prevent potential compromises through this vector.

Active Threat Response Logging Improvements – adds granular logging controls for both inbound and outbound traffic to reduce noise from brute-force and similar repetitive events. Adds support for identifying and matching inbound forwarded traffic (WAF, DNAT, etc) with third-party, NDR Essentials, and MDR threat feeds, improving detection of externally initiated threats. Also adds support for matching the source IP for NDR-Essentials and Third-party threat feeds for outgoing traffic to identify and block IP addresses of compromised unmanaged devices.

NDR Essentials Threat Score in Logs – The assigned threat score is now included in active threat response logs for enhanced visibility, reporting and analytics.

NDR Essentials Data Center – You can now select the data center region for NDR Essentials flow analysis for regional or data residency requirements. By default, the system will choose the lowest latency region.

Instant Web Category Alerts – organizations can now setup instant alerting for restricted web categories which is particularly helpful for UKI education institutions that require this. Emails will be sent as frequently as every 5 minutes with new alerts with a full report showing date, time, user, category, domain, and more. This new feature can be found under Web > Categories.



Easily add instant alerts to any web category

XML API Access Control Enhancements – API configuration has now been moved under the "Administration" main menu entry. You can now define API access by IP addresses, IP ranges, and network objects with up to 64 objects supported (an increase from 10 IPs previously).

HTTP2/TLS1.3 Support for Device Access – The Web Admin Console, VPN Portal, and User Portal now support TLS 1.3, providing stronger encryption.

Streamlined Management and Quality of Life Enhancements

As with every Sophos Firewall release, this version includes several quality-of-life enhancements that makes day-to-day management easier.

Enhanced Navigation Performance – you can now navigate to any menu item or tab without waiting for the current page to finish loading which makes UI navigation faster.

Hardware monitoring via SNMP – Adds a top requested feature from many partners and customers with a downloadable MIB file from the SFOS UI. Metrics supported include CPU Temp, NPU Temp, Fan speeds, power supply status (on XGS 2100 and above), and PoE measurements for all XGS models with PoE support except XGS 116(w).

sFlow Monitoring – Provides real-time data based upon your set sampling rate (400 by default with a minimum sample rate of 10). Works on any physical interface, including sub interfaces (alias, VLAN, etc.) with a maximum of 5 collectors. Note that the FastPath will be disabled for the monitoring interface.

NTP Server Settings – NTP server settings now defaults to “Use pre-defined NTP server”

UI Enhancements for XFRM Interfaces – adds pagination support for XFRM interaces and an option to search and filter to easily manage a large number of XFRM interfaces.

SG UTM Features

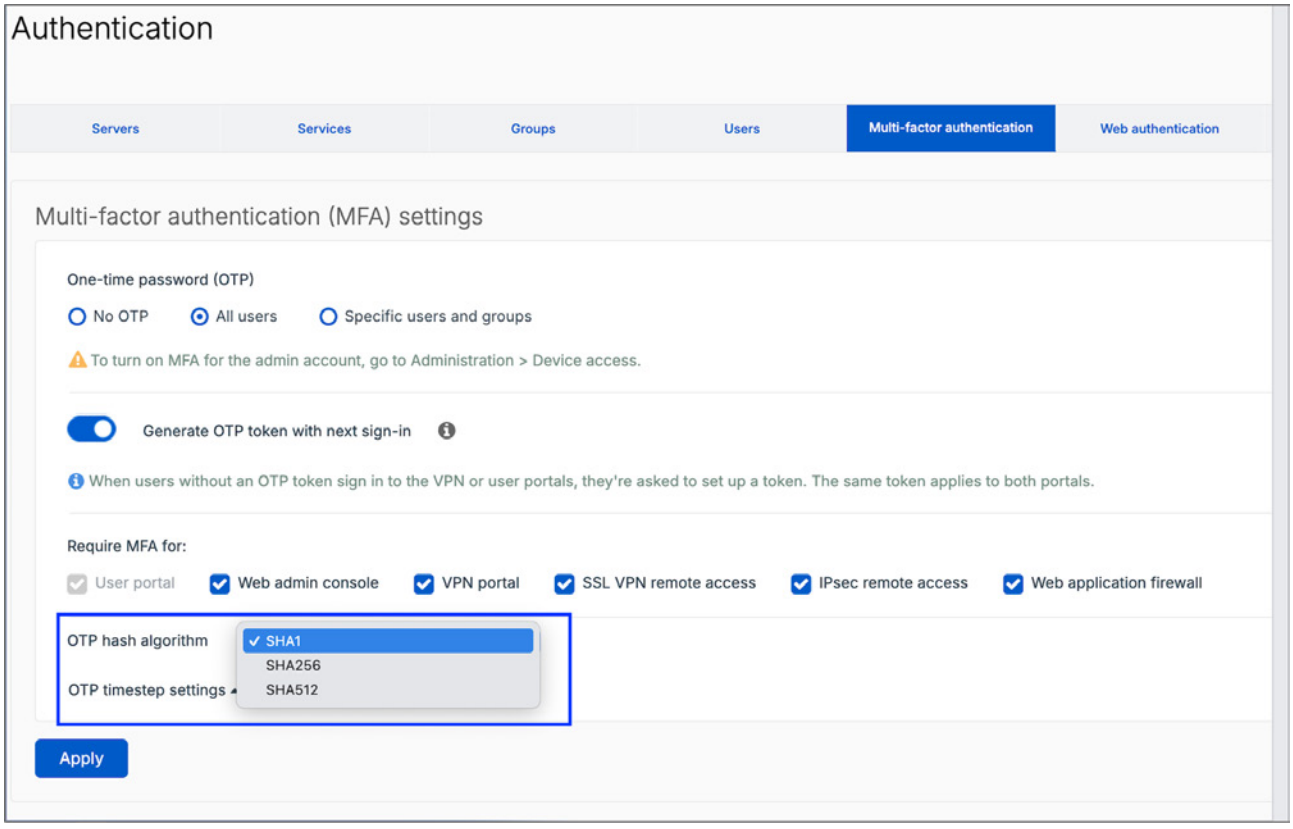
With the SG UTM product line coming to end-of-life very soon (July 30, 2026), some customers making the transition to Sophos Firewall will find these new features welcome additions:

SHA 256 and 512 Support for OTP Tokens – Another popular request from SG UTM customers is now an option on Sophos Firewall for Google and Sophos apps as well as Admin users.

MFA Support for WAF – Brings multi-factor authentication to the integrated Web Application Firewall (form-based authentication) on Sophos Firewall to provide added security and feature parity in this area.

Audit trail logs – enables comprehensive audit logs with before and after tracking to meet the latest NIST standards. In phase 1, detailed audit logging is supported for firewall rules, objects, and interfaces. Detailed audit logs can be downloaded from Diagnostics > Logs. XML is used to highlight before and after changes. Future phases will show the delta change in the log viewer.

Stronger WAF Security – Sessions are now managed by SFOS instead of client-side cookies, making them harder to hijack and enhancing overall protection. When auth forwarding isn't required, authentication can be fully offloaded to SFOS, reducing exposure of the internal WAF server.



MFA support has been extended to WAF and now supports SHA256/512

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

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

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

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

© Copyright 2025. 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.

2025-10-16 EN (DD)