Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 22.0

Sophos Firewall

These release notes are for Sophos Firewall (formerly known as Sophos XG Firewall).

Latest version | Previous versions | Resolved issues | Known issues | Upgrade information | Supported platforms | Support

Version 22.0 GA Build 411

Released on January 20, 2026

New features

This page describes the new features introduced in this release. For more information, see Sophos Firewall help.

SFOS 22.0 GA and later versions do not support XG and SG Series hardware appliances.

Firewall health check

The new Firewall health check feature helps you quickly assess your overall firewall configuration and identify configurations that may pose a security risk. The feature evaluates dozens of configurations against CIS benchmarks and other best practices, providing immediate insight into potential vulnerabilities.

A new panel at the top of the Control center page shows the health check status. "Firewall health check" in the main menu shows the detailed report.

The feature strengthens your security posture by helping you keep your firewall up to date and optimally configured with minimal assessment effort. The key benefits are as follows:

- Comprehensive evaluation of your firewall configuration
- Risk identification for high-risk configurations
- Actionable recommendations with a quick drill-down into areas of concern, including the need for a firmware update
- The ability to go directly to the configuration that requires change

For more information, watch Firewall health check.

Secure by Design

Next-generation Xstream architecture: New control plane

The key features and benefits are as follows:

- The version introduces an all-new control plane specifically architected for maximum security, scalability, and future-readiness.
- The new control plane enables modularization, isolation, and containerization, allowing services such as IPS to run like apps on the firewall platform.
- The control plane also enables complete separation of privileges, delivering additional security.
- The firewall's self-healing capability continuously monitors system status and automatically corrects any deviations, ensuring optimal performance for SFOS.

Hardened kernel

The key features and benefits are as follows:

- The next-generation Xstream architecture is built on a new hardened kernel (v6.6+), which provides enhanced security, performance, and scalability that can maximize usage in current and future hardware.
- The new kernel delivers tighter process isolation and advanced mitigations for side-channel attacks and CPU vulnerabilities, such as Spectre, Meltdown, L1TF, MDS, Retbleed, ZenBleed, and Downfall.
- The enhancement includes hardened usercopy, stack canaries, and Kernel Address Space Layout Randomization (KASLR) for enhanced memory safety and protection against exploitation.

Remote monitoring for system integrity

Remote monitoring is an additional security capability unique to Sophos Firewall.

- SFOS now integrates Sophos XDR Sensor for Linux, which continuously monitors system integrity in real-time, detecting unauthorized configurations, rule exports, attempts to execute malicious programs, and file tampering.
- The integration enhances Sophos' security team's ability to proactively monitor the entire Sophos Firewall installation base, enabling them to identify and investigate more effectively and respond faster to attacks.

New anti-malware engine

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_220_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 22.0

Security and scalability: Other enhancements

The key features and benefits are as follows:

- **Active threat response**:
  - **Taegis XDR, MDR integrated with SFOS**: Taegis XDR and MDR is now integrated with Active Threat Response, enabling seamless network-level threat blocking. You can push malicious IP addresses, domains, and URL information from the Taegis portal to the firewall and block threats across all relevant firewall subsystems. No manual configuration is needed.
  - **Logging improvements**: We introduced granular logging controls for inbound and outbound traffic to reduce noise from repetitive events, such as brute-force attacks. The firewall identifies and matches inbound, forwarded traffic, such as WAF and DNAT traffic, with MDR threat feeds, NDR Essentials, and third-party threat feeds, improving detection of externally initiated threats. Additionally, the enhancement matches the source of outgoing traffic for NDR Essentials and third-party threat feeds, complementing the existing MDR threat feed support.
- **NDR Essentials**:
  - **Threat score in logs**: The assigned threat score is now included in the Active threat response logs for enhanced visibility, reporting, and analytics.
  - **Data center selection**: You can now select the data center region for flow analysis performed by NDR Essentials, helping meet regional and data residency requirements. By default, the system chooses the region with the lowest latency.
- **Syslog enhancements**: The `device_name` field identifies the hostname of the firewall that produced the logs, enabling clear identification across multiple firewalls. This facilitates effective syslog-based integrations and helps XDR and Taegis administrators in differentiating the data sources.
- **Active Directory SSO**: The firewall includes a major upgrade to the Samba components that connect it to Active Directory services for Kerberos and NTLM authentication. Key benefits include improved support for Windows Server 2025 and the removal of support for older encryption protocols.
- **Access control for XML API**: API access settings have been moved to the Administration menu. Additionally, you can allow API access based on IP hosts, which can include IP addresses, IP ranges, and networks. Previously, you could only add IP addresses. You can now add up to 64 IP hosts compared to the previous maximum limit of 10 IP addresses. The firewall automatically converts the allowed IP addresses into IP host objects when you upgrade. These migrated objects are named using the prefix "apiconfig".
- **Instant alerts for web categories and keywords**: The firewall can raise immediate alerts based on browsing intent and behavior when you turn the feature on in **Web** > **Categories**. This capability helps schools move from reactive reporting to proactive safeguarding, protecting students when it matters most and ensuring compliance with the latest digital standards, including mandatory UK requirements for educational institutions. Real-time email notifications include a comprehensive report with details, such as date, time, user, category, and domain.
- **TLS 1.3 support for device access**: The web admin console, VPN portal, and user portal support TLS 1.3, providing stronger encryption.
- **Public key authentication for admin**: Only the default admin can add and delete public keys for SSH authentication.
- **FastPath**: The firewall has optimized memory in the Data Plane Development Kit (DPDK) of the Data Acquisition (DAQ) layer, eliminating many out-of-memory instances in the following desktop firewalls: XGS 87/87w, 107/107w, and 116/116w.

Streamlined management and Quality-of-life enhancements:

The key features and benefits are as follows:

- **Enhanced navigation performance**: You can go to any menu item or tab without waiting for the current page to load, making the web admin console faster and more responsive.
- **XFRM interface enhancements on the web admin console**: Pagination support has been added for XFRM interfaces, along with search and filter options to simplify managing large numbers of XFRM interfaces.
- **Enhanced firewall rule creation for site-to-site IPsec VPNs**: Individual incoming and outgoing firewall rules with zone-based traffic control are created instead of a single firewall rule for site-to-site IPsec connections, providing improved security and streamlined management.
- **NTP server settings**: In fresh installations, the default NTP server setting is now "Use pre-defined NTP server".
- **Hardware monitoring through SNMP**: The MIB file now supports the following hardware metrics:
  - CPU temperature: All XGS models
  - NPU temperature: XGS models other than 88/88w, 108/108w, 118/118w, 128/128w
  - Fan speed: XGS models other than 88/88w and 108/108w
  - Power supply status: XGS 2100 and higher models
  - PoE measurements: XGS models other than XGS 116/116w
- **SNMPv1/v2c community**: You can add the community string and select IPv4 or IPv6 versions in SNMPv1/v2c configurations. When you upgrade, the firewall copies the Name as the Community string to maintain continuity. It uses a hash of the name and IP address as the Name. The migrated name has the prefix "snmp".
- **sFlow monitoring**: The feature provides real-time data about network traffic based on the packet sampling rate you configure. sFlow enables network troubleshooting, capacity planning, and security monitoring. It supports all physical interfaces, including dependent interfaces, such as aliases and VLANs. You can configure up to five collectors.
- **Cellular WAN**: You can check signal strength using the following CLI command: `system cellular_wan show`
- **Automatic firewall rules for site-to-site IPsec VPN**: When you select Create firewall rule in site-to-site IPsec connections, the firewall now creates two separate rules, one for incoming traffic and another for outgoing traffic, instead of the previous single rule. The corresponding prefixes for these rules are as follows: "Incoming" and "Outgoing".
- **MTU of XFRM interfaces**: To prevent packet fragmentation and ensure reliable TCP connectivity in route-based VPN tunnels, the firewall automatically assigns an XFRM MTU value after subtracting the maximum IPsec overhead from the physical interface MTU. You can change this value to meet your network requirements.
- **Identifying firewalls from backup emails**: The subject line of backup emails now includes the firewall's hostname, firmware version, serial number, and model. This enhancement makes it easier to identify which firewall a backup belongs to when you manage multiple firewalls.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_220_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 22.0

ction, you can fully offload authentication to the firewall when authentication forwarding isn't needed, reducing exposure of the internal WAF server.

- **SHA-256 and SHA-512 for OTP tokens**: You can configure SHA-256 and SHA-512 in addition to the previously supported SHA-1 algorithm for MFA. Sophos Intercept X and third-party authenticators, such as Google Authenticator and DUO, support these stronger algorithms. The algorithm you select also applies to the default admin.
- **Audit trail logs**: The firewall provides comprehensive audit logs in the `configuration-audit.log` file with before-and-after tracking of configuration changes to comply with the latest NIS2 standards. The current phase 1 offering supports audit logs for Firewall rules, Interfaces, and Hosts and services. You can download the detailed log from **Diagnostics** > **Troubleshooting logs**. All configuration changes are recorded in XML format.

 Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_220_rn.html