Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 21.0

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 21.0 GA Build 169

Released on October 17, 2024

New features

This page describes the new features introduced. For details, see the Sophos Firewall help.

SFOS 21.0 GA doesn't support XG and SG Series hardware appliances.

Active Threat Response with Third-party threat feeds

The firewall supports external threat feeds, making integration with third-party Security Operations Center (SOC) providers, MSPs, and industry-specific security consortiums easier.

- **Simple configuration**: Third-party threat feeds allow you to add threat intelligence from external threat feed sources to block threats. You can add custom feeds and industry-specific feeds. See the help page Third-party threat feeds.
- **Automatic detection and action**: The firewall automatically blocks or monitors any activity associated with the Indicators of Compromise (IoC) in the feed. It implements the action across all its security engines and doesn't require additional firewall rules.
- **Synchronized Security**: With its automated response based on a red Security Heartbeat, Synchronized Security is extended to threat feeds.. This includes enforcement of any firewall rules that contain Heartbeat conditions. The firewall automatically queries any Sophos-managed endpoint attempting to communicate with malicious servers for additional information, such as the host, user, and process, which enables you to determine any Indicators of Compromise (IoC). It prevents compromised endpoints from moving laterally or communicating outward, shutting down active threats in the network.

Watch the video Third-party threat feeds.

Let's Encrypt^{TM} certificates

The firewall automatically obtains Let's Encrypt certificates based on your certificate signing requests (CSRs) for these certificates. It also automatically renews the certificates.

You can use Let's Encrypt certificates with the following features:

- WAF
- SMTP TLS configuration
- Hotspot sign-in page
- Web admin console
- User, captive, VPN, and SPX portals.

See the help page Let's Encrypt certificate authority (CA).

Watch the video Sophos Firewall: Let's Encrypt.

New Gen.2 XGS Series desktop appliances

The new XGS Series desktop models XGS 88(w), 108(w), 118(w), and 128(w), and XGS 138 deliver higher performance, improved energy efficiency, high-speed connectivity options, and a streamlined architecture. The streamlined architecture is available in XGS 88(w) to 128(w) models. All models except the XGS 138 are available with optional built-in Wi-Fi 6, which supports concurrent dual-band use.

- **Accelerated performance**: XGS 88(w), 108(w), 118(w), and 128(w) deliver up to double the throughput of Gen.1 models with Xstream virtual FastPath acceleration for IPsec VPN in 21.0 and later versions. The XGS 138 benefits from an overall throughput increase of 1.6 times versus the previous models.
- **Built-in high-speed connectivity**: All Gen.2 models have 2.5 GE interfaces. XGS 138 has two built-in 10 GE SFP+ interfaces for high-speed fiber connectivity.
- **Concurrent dual-band Wi-Fi**: The Gen.2 wireless models support Wi-Fi 6 (802.11ax) with concurrent use of the 2.4 GHz and 5 GHz bands for better performance.
- **Optional connectivity**: The expansion bay can be equipped with an optional 5G module, providing a cost-effective connectivity option to support traffic peaks or add redundancy and failover, particularly for SD-WAN deployments.
- **Streamlined hardware architecture**: XGS 88(w) to XGS 128(w) models have a new single-CPU architecture that uses the virtual FastPath built into SFOS for traffic acceleration. The XGS 138 maintains the dual-processor architecture with a dedicated Xstream Flow processor for hardware acceleration. As our gateway model to the distributed edge, it benefits from new high-speed connectivity options, resulting in 1.6 times the overall performance compared to the equivalent Gen.1 model.

Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_210_rn.html

Sophos release notes

Product type: Network Security Product: Sophos Firewall Version: 21.0

Enhanced scalability and resilience

This version offers several enhancements in networking, providing improved performance and scalability.

High availability improvements

HA deployments offer additional resilience and smoother transitions, delivering reduced downtime.

- Seamless failover of dynamic routes.
- Significant improvement in SD-RED tunnel failover, enabling tunnels to reestablish within a few seconds of HA failover, reducing downtime.
- Improved interactions with Active Directory domains when HA failover occurs.

Site-to-site IPsec VPN

This version delivers improved performance and additional ease in configuring and managing IPsec VPNs.

- Optimized FQDN-based remote gateways have been optimized to improve scalability for distributed deployments.
- This version supports DHCP relay over XFRM interfaces to DHCP servers deployed behind the firewall.
- An increase of up to 20 times in XFRM interface up-time significantly minimizes disruption during tunnel flap and restart.
- You can activate and deactivate more than one site-to-site IPsec VPN connection at the same time.
- Automatic failback to the restored primary IPsec connection will be retried up to five times.

Watch the video Static route and VPN enhancements.

Authentication

- **Google Workspace**: Supports Google Workspace integration through the LDAP client and Google Chromebook SSO.
- **Authentication**: Performance for burst sign-ins has improved up to four times for RADIUS SSO, STAS, and Synchronized User ID. The enhancement enables the firewall to handle thousands of simultaneous sign-in requests in multiple SSO environments involving these authentication methods.
- **AD SSO**: More transparent AD SSO experience when HSTS is enforced, enabling Kerberos and NTLM handshakes over HTTP or HTTPS.

Web

- **IPv6 to IPv4 using explicit proxy**: The firewall enables IPv6-only clients to access IPv4 websites through explicit proxy.
- **Enhanced web protection**: This version delivers enhanced Web Protection performance with reduced system load when enforcing SafeSearch, YouTube restrictions, Google App login domain restrictions, and Azure AD tenant restrictions.

Routing

Dynamic routing: A new option to redistribute BGP-IPv6 routes into the OSPFv3 routing table.

Reports database

SFOS 21.0 and later versions store reports in a separate, updated database. So, you must select a date range before or after the firmware upgrade date for the corresponding reports. See Reports behavior.

Quality-of-life enhancements

- **Static route management**: You can clone static routes, turn them on or off, and add descriptions. The firewall offers a blackhole route option. It also supports Equal-Cost Multi-Path (ECMP) for load balancing.
- **Expanded object usage**: This version offers additional visibility into the usage of the following network objects: interfaces, zones, gateways, and SD-WAN profiles. It also offers XML API support to retrieve object usage counts, delivering visibility into unused objects.
- **Site-to-site IPsec VPN**: Option to activate and deactivate connections in bulk. It also provides improved filtering, covering the complete list across multiple pages. Filtering for XFRM interfaces is now available on the Interfaces page.
- **Interface listing**: Interfaces are listed in alphabetical followed by numeric order based on their display name instead of the hardware name.
- **User experience enhancements**:
  - A fresh look for the web admin console with the latest Sophos design style guide matching that of Sophos Central.
  - The Control center has been redesigned with new card views to enhance the visibility of important network events and data. An all-new Active threat response card consolidates threat information from MDR, Sophos X-Ops, and Third-party threat feeds into a single, easy-to-view section.
  - Optimized VPN configurations with free text and value search for objects, such as network, subnet, and users in remote access and site-to-site VPN configuration lists.

Watch the video Quality of life enhancements.

New Backup-restore assistant

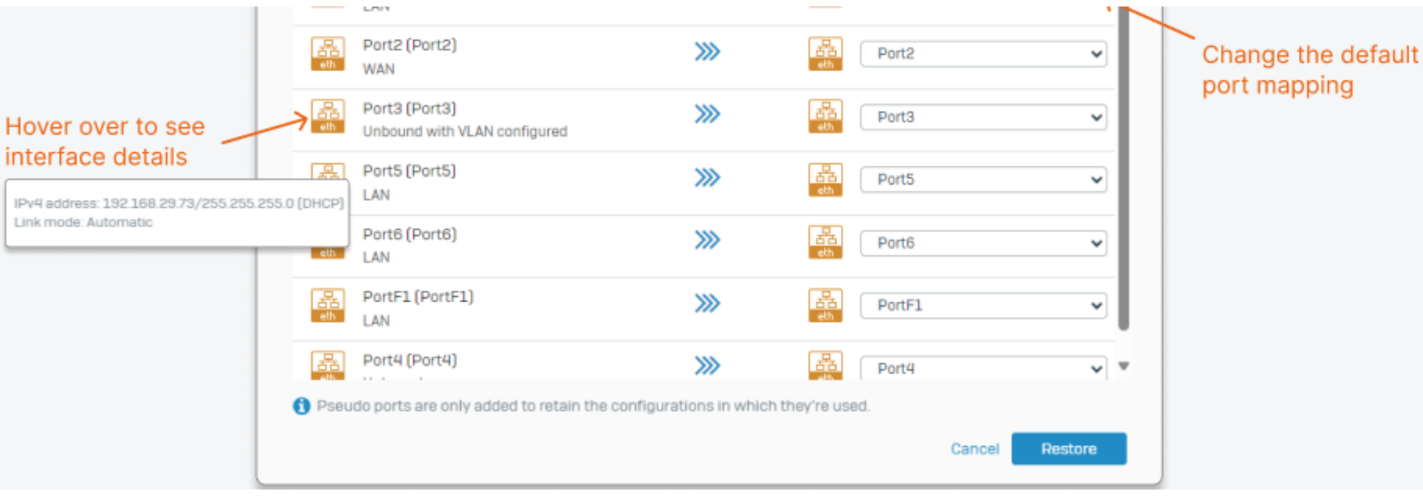
SFOS 21.0 GA includes backup-restore features first introduced in 20.0 MR2. These enhancements simplify firewall upgrades to the latest XGS Series firewalls. They also

Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_210_rn.html

Sophos release notes

Product type: Network Security
Product: Sophos Firewall
Version: 21.0

itions to a different firewall model. You can move from a higher to a lower-capacity appliance model and restore existing backups. You can also restore backups from one platform to another for hardware appliances, cloud, virtual, and software firewalls.



Hover over to see interface details

Change the default port mapping

IPv4 address: 192.168.29.73/255.255.255.0 (DHCP)
Link mode: Automatic

Port2 (Port2) WAN → Port2

Port3 (Port3) Unbound with VLAN configured → Port3

Port5 (Port5) LAN → Port5

Port6 (Port6) LAN → Port6

PortF1 (PortF1) LAN → PortF1

Port4 (Port4) → Port4

Pseudo ports are only added to retain the configurations in which they're used.

- **Flexible interface mapping**: The assistant supports port mapping, making upgrades to appliances with different port configurations easier. You can change the default interface mapping and map a physical interface to a different one, including higher-speed ports. You can also change the parent interfaces of VLAN and LAG interfaces.
- **High availability ports**: You can restore HA backups to devices with fewer or more interfaces. The dedicated HA link can be on a different port in the target device. The enhancement eliminates the previous limitation, which required the target device to have the same number of interfaces and the same dedicated HA link port as the backup.

Backup-restore links

- Use the tool to check whether you can restore backups between appliance models and platforms. Check compatible devices to restore backups.
- Watch the video Backup-restore enhancements.
- See the help page Backup-restore Assistant.

Direct link to these release notes: https://docs.sophos.com/releasenotes/output/en-us/nsg/sf_210_rn.html