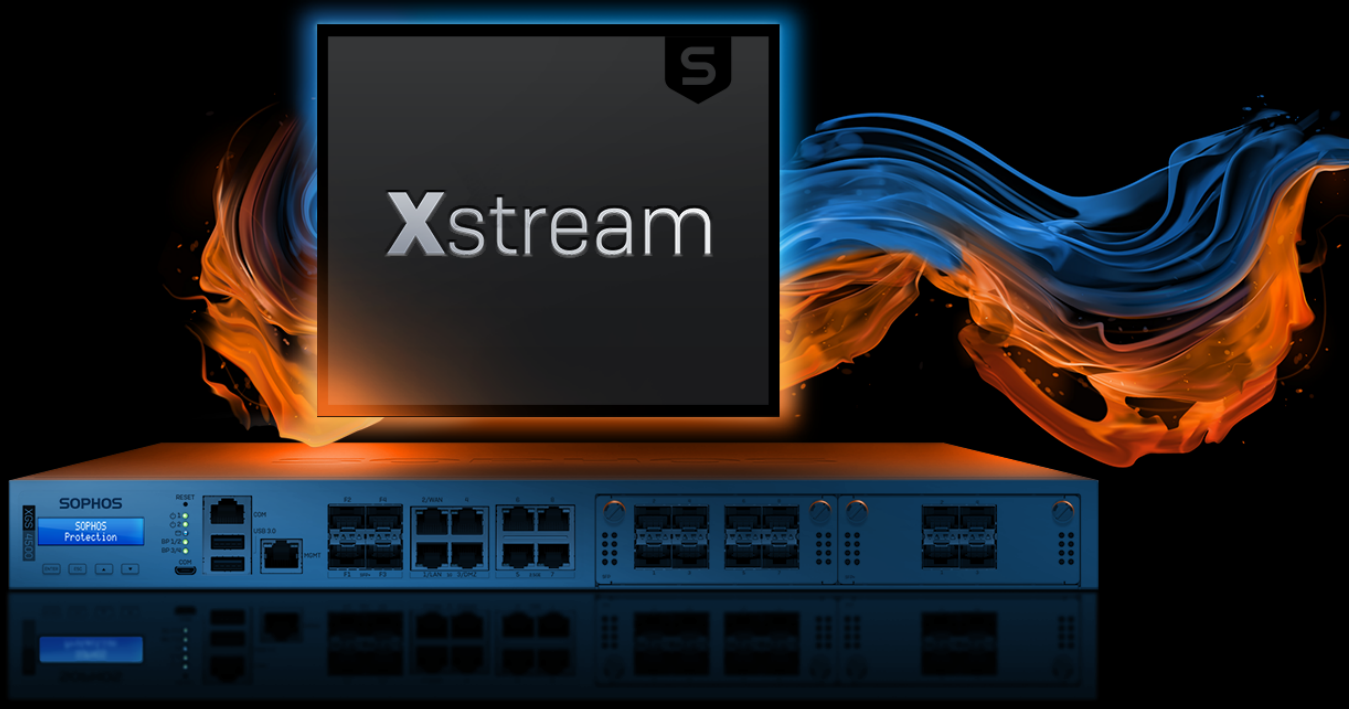
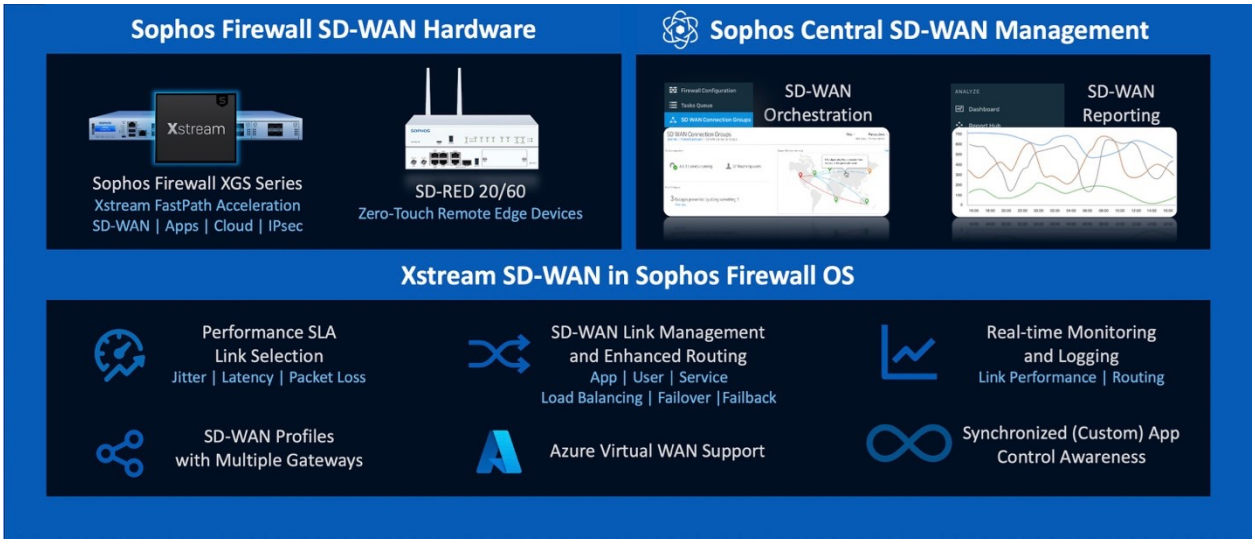
What's New in Sophos Firewall



SOPHOS
Cybersecurity evolved.

Key New Features in Sophos Firewall OS v19

Xstream SD-WAN



SD-WAN Profiles and Performance based SLA

SFOS v19 introduces a new SD-WAN link management solution for easily setting up WAN routing strategies. SD-WAN profiles define a routing strategy across multiple WAN link gateways (includes support for more than 2 links) enabling seamless and efficient rerouting of application connections based on WAN Link performance with zero impact. This optimizes performance for your SD-WAN network and helps ensure great continuity, application performance, and the best end-user experience in even the most disruptive or unstable ISP environments.

SD-WAN profile routing strategies can be based on first available or performance-based link criteria. Performance monitoring criteria includes jitter, latency and packet loss and can utilize multiple probe targets for PING and TCP probes. SD-WAN profiles can automatically select the best link based on performance or according to your custom SLA policies that define specific values for maximum acceptable jitter, latency, or packet loss before re-routing over a better performing link with absolutely zero impact to any active connections.

SD-WAN Monitoring Graphs

A new SD-WAN performance monitoring tool is now available under the diagnostics section of the product. You can monitor SD-WAN link performance in real-time with separate graphs for latency, jitter, and packet loss. Timeline selections for real-time, the last 24 or 48 hours, or over the last week or month are provided.

Xstream FastPath Acceleration for IPsec VPN Tunnel Traffic

Sophos Firewall OS v18 introduced the Xstream Architecture that enables FastPath acceleration of trusted traffic flows. The new XGS Series hardware appliances added dedicated Xstream Flow Processors for hardware acceleration of trusted traffic flows. One of the great benefits of the programmable flow processor is that additional features and capabilities can be added over time to further improve performance.

SFOS v19 adds IPsec VPN hardware FastPath acceleration for XGS Series appliances which automatically puts IPsec tunnel flows on the FastPath through the Xstream Flow Processor. This dramatically improves performance, moving some of the CPU-intensive processing required for IPsec tunnels to the Xstream Flow Processor such as ESP-encapsulation/encryption and decapsulation/decryption. This new feature takes full advantage of the hardware crypto capabilities within the Xstream Flow Processor and has the added benefit of freeing up CPU resources for other tasks like deep-packet inspection of traffic that needs it.

Xstream FastPath Acceleration for IPsec traffic works for both site-to-site and remote access VPN traffic, however, IPsec connections with weak cipher or auth algorithms (DES, 3DES, Two Fish, MD5) will not be off-loaded.

SD-WAN Logging

SD-WAN routing information has been added to the logs along with a new SD-WAN log viewer module allowing you to focus on log entries specific to SD-WAN routing and health. Log entries include SD-WAN rule ID and name for both route request and reply directions.

VPN

VPN User Experience Enhancements

The navigation and user interface for various VPN administration options has been reorganized to make it easier and more intuitive:

- Remote access and Site-to-Site VPN settings now have their own separate main menu nav items
- Submenu has been added to the IPsec, SSL, and L2TP tabs to easily access settings, client downloads and the log viewer
- IPsec policies have been renamed to profiles and has been moved to the System > Profiles area of the system
- SSL Remote Access now includes a new wizard assistant to greatly streamline and easily configure everything required for remote access.
- Clientless polices, bookmarks and bookmark groups have all been consolidated onto a single tab
- A new tab has been added for easy setup of Amazon Web Services VPC tunnels with an option to import the VPC configuration file or AWS security credentials

VPN Performance Enhancements

SFOS v19 includes significant performance enhancements (nearly 5x) to SSL VPN capacity thanks to the addition of multi-instance support.

VPN Operational Enhancements

- Custom policy support for IPSEC RA:
  - Helps address a potential PCI compliance issue with the default IPsec RA policy
  - Enables the configuration of a custom rekey time to avoid regular MFA prompts every four hours.
  - Adds a new option to increase idle timeout from 10-minutes up to 6-hours.
- Route-Based VPN (RBVPN) Enhancements:
  - Added support for static multicast routes
- Support traffic selectors in Route-Based VPNs (RBVPN)
  - Supports the definition of traffic selectors within a specific RBVPN, which only permits traffic through the tunnel if the traffic matches the specified pair of local and remote addresses.
- GCM and Suite-B cipher suite support for IPsec
  - AES-GCM for IPSec significantly improves IPsec VPN performance
- SSL VPN:
  - Upgrades Open VPN / Open SSL
  - Default TLS 1.3 support on SSL VPN tunnels
  - AES-NI path enabled
  - GCM Encryption support for SSL VPN

VPN Logging Enhancements

A new log viewer module selection for VPN is available making it easy to monitor and troubleshoot VPN connections for both remote access and site to site type tunnels using either IPsec or SSL.

Also, IPsec logging messages are enriched with more details for better understanding.

AWS VPC

A popular feature carried over from our SG UTM platform, this enables the easy connection of your on-premise firewall to your AWS network infrastructure. You can now import the VPC configuration XML file from AWS to automate the tunnel setup on your Sophos Firewall including related routing and the associated IPsec policies. There is a new tab in the VPN section of the product for importing, monitoring and managing your AWS VPC connections.

Web Protection

Per Connection Authentication

In explicit proxy mode authentication can now handle multiple different users coming from the same source address. This is ideal for terminal services, Windows remote desktop, or direct access systems. Network administrators familiar with the proxy authentication on SG UTM will appreciate this new feature.

Enforce Tenant Restrictions for O365

Enables the use of the Tenant Restriction feature of O365 to restrict which domains user can login to by adding headers to outbound HTTPS requests to enable Microsoft Azure AD to enforce restrictions.

Typically used to restrict personal accounts from accessing O365 from Sophos Firewall protected networks.

X-Forwarded-For Header

Allows the source IP address to be passed up-stream to load balancers or proxies.

Search

Global Menu Search

A new intelligent Search box with auto-complete now appears at the top of the main menu and allows you to find any screen or feature in the system. It's perfect for new Sophos Firewall users who are still learning the navigation, and even for veterans as a quick navigation shortcut. It works simply by typing any portion of the feature or label for that feature. Many features have had meta search tags associated with them making it intuitive and easy to find any feature in the system. For example, searching for "NAT" or "SNAT" or "port forwarding" will take you to the NAT Rules tab. It will work across all supported UI languages at release.

Object Search

SFOS v19 significantly enhances the user experience when searching for a network object or service for inclusion in rules. The layout now includes a free-text search option which enables searching by label or value. For example, if you have a server object "FileServer" at 10.10.1.20, searching for "file" or "10.10" or "20" will return the desired object. Or if you have a SIP service using port 5060, searching either "SIP" or "5060" will return the desired object. The enhanced search and selection has been added to all firewall, NAT, TLS, and routing rules making it easy to find the desired network object or service anywhere in the system.

Other Enhancements

Authentication Performance – Improves performance that will be appreciated most in high-load situations with thousands of users.

Global IPS Switch – A new global switch has been added to the Intrusion Prevention > IPS policies tab to enable or disable IPS. This switch will be set automatically when migrating to v19: if you were previously using IPS it will be set to ON.

Synchronized Security – an update to Lateral Movement Protection to guard against the use of spoofed MAC addresses to disrupt legitimate traffic.

Flow Monitor – Enhanced the user interface and layout of the flow monitor to make the headers persistent and eliminate horizontal scrolling.

Multi-Factor Authentication – Improved security, workflow, and usability with the option to enable One-Time-Password MFA access to WebAdmin for the default admin account.

Log suppression – Repetitive firewall logs within a given module are aggregated into one event with a repeat count to improve troubleshooting as well as optimize logging scalability and storage efficiency.

Zero-Day Protection – An additional data center location for cloud-based machine learning file analysis is available in Asia Pacific: Sydney, Australia. This adds to the existing data center locations in Japan, Germany, the UK, and the USA. It is expected to be active as of the end of February, 2022.

Device and Management Identity – The device hostname is now shown in the browser tab and the active user ID in the upper right corner of the management console which makes managing multiple firewalls and admin accounts easier