What's New in Sophos Firewall

SOPHOS
Cybersecurity evolved.

Key New Features in Sophos Firewall OS v18

Xstream Architecture

Sophos is pleased to introduce the new Xstream Architecture for Sophos Firewall, a new streaming packet processing architecture that provides extreme levels of protection and performance. The new architecture includes:

1. Xstream SSL Inspection: Organizations can enable SSL inspection on their networks without compromising network performance or user experience. It delivers high-performance, high connection-capacity support for TLS 1.3 and all modern cipher suites providing extreme SSL inspection performance across all ports, protocols, and applications. It also comes equipped with enterprise-grade controls to optimize security, privacy, and performance. A new widget on the Control Center provides unprecedented visibility into SSL-encrypted traffic enabling quick troubleshooting in the event of any compatibility issues, to maintain the ultimate user experience.
2. Xstream DPI Engine: Enables comprehensive threat protection in a single high-performance streaming DPI engine with proxyless scanning of all traffic for AV, IPS, and web threats as well as providing Application Control and SSL Inspection. Pattern matching on decrypted traffic makes patterns more effective and provides increased protection from hash/pattern changing applications such as Psiphon proxy.
3. Xstream Network Flow FastPath: Provides the ultimate in performance by intelligently accelerating traffic processing to transfer trusted traffic at wire speeds. The FastPath offloading can be controlled through policy to accelerate important cloud application traffic, or intelligently by the DPI engine based on traffic characteristics.

Threat Intelligence Analysis

Sophos Firewall gains an added layer of artificial intelligence protection. All suspicious files are now subject to threat intelligence analysis in parallel with full sandbox analysis. Files are checked against SophosLabs' massive threat intelligence database and subjected to our industry-leading deep learning, which identifies new and unknown malware quickly and efficiently – often rendering a verdict in seconds – to stop the latest zero-day threats before they get on the network. Threat Intelligence Analysis is a new feature that is included as part of the Sandstorm Protection license (all PLUS bundles) at no extra charge.

Threat Intelligence Reporting

Threat Intelligence Reporting adds a new Control Center widget to highlight all suspicious file downloads. The widget enables one-click drill-down to detailed forensics reports on all suspicious file activity. A quick summary view for each file provides a traffic-light style (red, yellow, green) indication of the analysis after antivirus scanning, threat intelligence analysis, and sandboxing. Detailed reports provide an-depth view of the verdict, including illustrated analysis by multiple machine learning models, details and screenshots of behaviors seen during Sandstorm analysis, and an in-depth breakdown of the file's features and attributes, together with malware scan results and insight from VirusTotal.

Sophos Central Firewall Reporting and Management

This release includes support for new firewall reporting and management capabilities being launched simultaneously on Sophos Central, including a rich, powerful new reporting suite and group firewall management tools.

NAT Enhancements – Decoupled NAT Rules and Linked NAT Rule

Sophos Firewall’s NAT configuration receives some major updates. NAT rules are now decoupled from firewall rules, enabling more powerful and flexible configuration options, including Source (SNAT) and Destination (DNAT) in a single rule. A new NAT rule wizard enables you to quickly and easily create complex NAT rules with just a few clicks.

In addition, a new linked NAT rule feature follows the matching criteria of the Firewall Rule. Linked NAT Rule can also be added and edited in place while creating/editing firewall rules. Only the source translation configuration needs to be selected for Linked NAT Rule.

Firewall Rules Management Improvements

Firewall rules management includes a new ‘Add Filter’ option with several fields/conditions from which to choose. Adding a filter makes it easier to find firewall rules based on the selected filter criteria. Once selected, filters stay selected even when the administrator moves to other configuration screens. Administrators can manage multiple firewall rules at the same time (e.g. select multiple rules to delete, enable/disable, attach to a group, etc.). Movement of rules across screens is possible, providing ease of use and management for larger rule sets. Within the firewall rule there is an exclusion feature that provides a “negate” option in the matching criteria to reduce the management and ordering overhead of multiple rules. There’s also a UI option to reset the data transfer counter for a firewall rule to improve troubleshooting.

Enhanced DDNS Support

Provides support for enhanced DDC service HTTPS-based DDNS by adding five more DDNS providers – No-IP, DNS-O-Static, Google DNS, Namecheap, and FreeDNS.

SD-WAN Application Routing and Synchronized SD-WAN

Optimized application routing and path selection is often an important objective in SD-WAN implementations – to ensure important business applications are routed over preferred WAN links. This release adds user and group application-based traffic selection criteria to Sophos Firewall’s SD-WAN routing configuration. Synchronized SD-WAN, a new Sophos Synchronized Security feature, offers additional benefits with SD-WAN application routing. Synchronized SD-WAN leverages the added clarity and reliability of application identification that comes with the sharing of Synchronized Application Control information between Sophos-managed endpoints and Sophos Firewall. Synchronized Application Control can positively identify 100% of all networked applications, including evasive, encrypted, obscure, and custom applications and now these previously unidentified applications can also be added to SD-WAN routing policies. This provides a level of application routing control and reliability that other firewalls can’t match.

Alerts and Notifications

There is a new option to choose from dozens of system- and threat-related alerts, and have notifications sent via email or SNMP.

Intelligent IPS Signature Selection

Sophos Firewall will receive IPS signatures based on a number of intelligent filtering criteria such as age, vendor, vulnerability type, and CVSS (Common Vulnerability Scoring System) to optimize protection and performance.

DKIM and BATV Anti-Spam Protection

Anti-spam protection is improved with support for DomainKeys Identified Mail (DKIM) which detects forged sender addresses and Bounce Address Tag Validation (BATV) to determine whether the bounce address specified in the received email is valid, and reject backscatter spam.

Kerberos Authentication and NTLM

This release adds Kerberos authentication alongside the existing NTLM support for Microsoft Active Directory SSO, extending the range of authentication tools available for customers.

Radius Timeout with Two-Factor Authentication (2FA)

For customers using 2FA with Radius Server Authentication, the timeout value is now configurable, allowing additional time to finish the authentication flow when necessary.

SNMPv3

Support for SNMPv3 is added providing more flexibility and security over SNMPv2.

Interface Renaming

Interfaces can be renamed, making networking configuration easier and more intuitive.

Improved Synchronized Application Control Verdict

In the event of a pattern-based match conflict, Synchronized Application Control Verdict will be adhered to for more accurate application control.

DHCP Relay Enhancements for Dynamic Routing

Synchronizes dynamic routing updates (learned routes from OSPF) to DHCP relay, eliminating the need for manual reconfiguration.

Secure Syslog and Logs in the Standard Syslog Format

Provides the option to fetch logs in the standard syslog format using secure TLS.

Dynamic GeoIP (IP to Country Mapping) Database

The GeoIP database is now updated dynamically in real time from Up2Date. Be sure to always use the appropriate country-specific filters and policies.

VMware Tools Upgrade and Integration with VMware Site Recovery Manager (SRM)

Supports virtual device integration of the latest VMware Tools version (v10.3.10) with reboot, shutdown, and clone-like functionalities. The release also supports integration with Site Recovery Manager (SRM), the disaster recovery and business continuity solution from VMware which automates the transfer of virtual machines to a local or remote recovery site.

Jumbo Frame Support

Jumbo frames with more than 1500 byte payloads are now supported for added networking flexibility in high-bandwidth environments.

Wildcard Domain Support in WAF

Sophos Firewall now supports wildcard domains for WAF (Web Application Firewall). Administrators can configure wildcard subdomains, (e.g. *.example.com) for both HTTP and HTTPS.

Log Viewer Enhancements

The log viewer gets several enhancements with one-click actions available right from the logs to narrow search results, filter log entries, or create or modify policies on the fly. Options include the choice to disable signatures, block a source IP address, edit interfaces, and modify IPS, App Control, or web filtering policies.

Web Policy Enhancements

Browsing quotas have been added to web policies, allowing administrators to set time quotas for browsing selected website categories. Users can choose how and when to consume their daily time quota.

High Availability (HA) Enhancements

New enhancements enable plug-and-play high availability deployments with greater flexibility and business redundancy. A preconfigured HA port on every device enables quick and easy HA deployments by simply connecting the two ports together and then acknowledging and activating HA. HA configurations also include a configurable failback strategy, ideal for remote-site HA deployments, with options for manual synchronization and time out tuning. It is now possible to perform firmware updates, rollbacks, and other tasks such as port monitoring lists and assigning multiple IP addresses to primary and auxiliary appliances while HA is active. In addition, deploying more than one HA pair in a single network is easier due to the elimination of conflicts arising from any dependency on a virtual MAC address HA architecture.

Bridge Interface Enhancements

Bridge interfaces now support ARP broadcasts, Spanning Tree Protocol (STP) traffic, and non-IP protocols by specifying the ethernet frame type.

Flow Monitoring Improvements

The new real-time flow monitor provides at-a-glance insights into active applications, users, and hosts along with current bandwidth utilization and other important information with convenient drill-down capabilities. Administrators can now analyze bandwidth in real time via the Live connections screen. Also, they can add users, source IP, and applications under a single view, all of which equips admins to analyze live bandwidth utilization from different pivots.

VLAN Bridge Support

VLANs are now supported on bridge interfaces, enabling greater networking flexibility and support for advanced inter-VLAN routing and bridging deployments.

Route-based VPN

Route-based VPN makes VPN setup easier to manage as it separates the VPN policy configurations from network topology configuration. In addition, it adds greater flexibility to how traffic is routed and how routes propagate over a VPN connection. Route-based VPN is the preferred choice in many deployments because it doesn't require the VPN policy to be reconfigured with changing networks.

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

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

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

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

SOPHOS