SOPHOS

Sophos Firewall Features

Sophos Firewall

Highlights

- Xstream Architecture provides extreme levels of visibility, protection, and performance through stream-based packet processing
- Xstream TLS inspection offers high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade policies with pre-packaged exceptions, unique dashboard visibility, and compatibility troubleshooting
- Xstream DPI Engine provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single-high performance engine
- Xstream Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
- Purpose-built user interface with interactive control center utilizes traffic-light indicators (red, yellow, green) to instantly identify what needs attention at a glance
- Control Center offers instant insights into endpoint health, unidentified Mac and Windows applications, cloud applications and Shadow IT, suspicious payloads, risky users, advanced threats, network attacks, objectionable websites, and much more
- Optimized two-clicks-to-anywhere navigation
- Policy Control Center widget monitors policy activity for business, user and network policies and tracks unused, disabled, changed, and new policies
- Unified policy model combines all business, user, and network firewall rules onto a single screen with grouping, filtering, and search options
- Streamlined firewall rule management for large rule sets with custom auto and manual grouping plus at-a-glance mouse-over feature and enforcement indicators
- All firewall rules provide an at-a-glance summary of the applied security and control for AV, sandboxing, IPS, Web, App, Traffic Shapping (QoS), and Heartbeat
- Pre-defined IPS, Web, App, and Traffic Shaping (QoS) policies enable quick setup and easy customization for common deployment scenarios (e.g. CIPA, typical workplace policies, and more)
- IPS, Web, App, and Traffic Shaping (QoS) policies snap into firewall rules and can be edited in-place providing a powerful yet intuitive model for configuring and managing security and control
- Sophos Security Heartbeat™ connects Sophos endpoints with the firewall to share health status and telemetry enabling instant identification of unhealthy or compromised endpoints
- Dynamic firewall rule support for endpoint health (Sophos Security Heartbeat) automatically isolates and limits network access to compromised endpoints
- Synchronized Application Control automatically, identifies, classifies, and controls all unknown Mac/Windows applications on the network
- Cloud Application Visibility enables Shadow IT discovery instantly and offers one-click traffic shaping
- Policy test simulator tool enables firewall rule and web policy simulation and testing by user, IP, and time of day
- User Threat Quotient identifies risky users based on recent browsing behavior and ATP triggers
- Configuration API for all features for RMM/PSA integration
- Discover Mode (TAP mode) for seamless integration in trials and PoCs with support for Synchronized Security
- SD-WAN connects remote/branch sites across a geographically-distributed network
- Remote Access VPN with a free and easy client for Windows/Macs
- Sophos Central cloud-based management and reporting for multiple firewalls provides group policy management and one console for all your Sophos IT security products
- Easy streamlined setup wizard enables fast out-of-the box deployment in just a few minutes
- Zero-touch deployment and configuration in Sophos Central for new firewalls

Base Firewall

General Management

- Purpose-built, streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
- Two-factor authentication (One-time-password) support for administrator access, user portal, IPSec and SSL VPN
- Advanced troubleshooting tools in GUI (e.g., Packet Capture)
- High Availability (HA) support clustering two devices in active-active or active-passive mode with plug-and-play Quick HA setup
- Full command line interface (CLI) accessible from GUI
- Role-based administration
- Automated firmware update notification with easy automated update process and roll-back features
- Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients, and servers
- Self-service user portal
- Configuration change tracking
- Flexible device access control for services by zones
- Email or SNMP trap notification options
- SNMP v3 and Netflow support
- Central management support via Sophos Central
- Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
- API for third-party integration
- Interface renaming
- Remote access option for Sophos Support
- Cloud-based license management via MySophos

Sophos Central Management

- Sophos Central cloud-based management and reporting for multiple firewalls provides group policy management and a single console for all your Sophos IT security products
- Group policy management allows objects, settings, and policies to be modified once and automatically synchronized to all firewalls in the group
- Task Manager provides a full historical audit trail and status monitoring of group policy changes
- Backup firmware management in Sophos Central stores the last five configuration backup files for each firewall with one that can be pinned for permanent storage and easy access
- Firmware updates from Sophos Central offer one-click firmware updates to be applied to any device
- Zero-touch deployment enables the initial configuration to be performed in Sophos Central and then exported for loading onto the device from a flash drive at startup, automatically connecting the device back to Sophos Central

Firewall, Networking, and Routing

- Stateful deep packet inspection firewall
- Xstream packet processing architecture provides extreme levels of visibility, protection, and performance through stream-based packet processing
- Xstream TLS inspection with high performance, support for TLS 1.3 with no downgrading, port agnostic, enterprise-grade polices, unique dashboard visibility, and compatibility troubleshooting
- Xstream DPI Engine provides stream scanning protection for IPS, AV, Web, App Control, and TLS Inspection in a single high-performance engine
- Xstream Network Flow FastPath delivers policy-driven and intelligent acceleration of trusted traffic automatically
- User, group, time, or network-based policies
- Access time polices per user/group
- Enforce policy across zones, networks, or by service type
- Zone isolation and zone-based policy support.
- Default zones for LAN, WAN, DMZ, LOCAL, VPN, and Wi-Fi
- Custom zones on LAN or DMZ
- Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule with a convenient NAT rule wizard to quickly and easily create complex NAT rules in just a few clicks
- Flood protection: DoS, DDoS, and portscan blocking
- Country blocking by geo-IP
- Routing: static, multicast (PIM-SM), and dynamic (RIP, BGP, OSPF)
- Upstream proxy support
- Protocol-independent multicast routing with IGMP snooping

- Bridging with STP support and ARP broadcast forwarding
- VLAN DHCP support and tagging
- VLAN bridge support
- Jumbo frame support
- WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
- Wireless WAN support (n/a in virtual deployments)
- 802.3ad interface link aggregation
- Full configuration of DNS, DHCP, and NTP
- Dynamic DNS (DDNS)
- IPv6 Ready Logo Program Approval Certification
- IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec

SD-WAN

- Support for multiple WAN link options including VDSL, DSL, cable, and 3G/4G/LTE cellular with essential monitoring, balancing, and failover
- Application path selection and routing, which is used to ensure quality and minimize latency for mission-critical applications such as VoIP
- Synchronized SD-WAN, a Synchronized Security feature, 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
- Application routing over preferred links via firewall rules or policy-based routing
- Affordable, flexible, and zero-touch or low-touch deployment
- Robust VPN support including IPSec and SSL VPN
- Centralized VPN orchestration
- Unique RED Layer 2 tunnel with routing

Base Traffic Shaping and Quotas

- Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options included with the Web Protection subscription)
- Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
- Real-time VoIP optimization
- DSCP marking

Secure Wireless

- Simple plug-and-play deployment of Sophos wireless access points (APs) — automatically appear on the firewall control center
- Central monitoring and management of APs and wireless clients through the built-in wireless controller
- Bridge APs to LAN, VLAN, or a separate zone with client isolation options
- Multiple SSID support per radio including hidden SSIDs
- Support for diverse security and encryption standards including WPA2 Personal and Enterprise
- Channel width selection option
- Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
- Support for 802.11r (fast transition)
- Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
- Wireless guest Internet access with walled garden options
- Time-based wireless network access
- Wireless repeating and bridging meshed network mode with supported APs
- Automatic channel selection background optimization
- Support for HTTPS login

Authentication

- Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between Sophos endpoints and the firewall without an agent on the AD server or client
- Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Server authentication agents for Active Directory SSO, STAS, SATC
- Single sign-on: Active directory, eDirectory, RADIUS Accounting
- Client authentication agents for Windows, Mac OS X, Linux 32/64
- Browser SSO authentication: Transparent, proxy authentication (NTLM) and Kerberos
- Browser Captive Portal
- Authentication certificates for iOS and Android
- Authentication services for IPSec, SSL, L2TP, PPTP

- Google Chromebook authentication support for environments with Active Directory and Google G Suite
- API-based authentication

User Self-Serve Portal

- Download the Sophos Authentication Client
- Download SSL remote access client (Windows) and configuration files (other OS)
- Hotspot access information
- Change user name and password
- View personal Internet usage
- Access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)

Base VPN Options

- Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- Sophos RED site-to-site VPN tunnel (robust and light-weight)
- L2TP and PPTP
- Route-based VPN
- Remote access: SSL, IPSec, iPhone/iPad/ Cisco/Android VPN client support
- IKEv2 Support
- SSL client for Windows and configuration download via user portal

Sophos Connect Client

- Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
- Enables Synchronized Security and Security Heartbeat for remote connected users
- Intelligent split-tunneling for optimum traffic routing
- NAT-traversal support
- Client-monitor for graphical overview of connection status
- Mac and Windows Support

Network Protection

Intrusion Prevention (IPS)

- High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
- Thousands of signatures
- Granular category selection
- Support for custom IPS signatures
- IPS Policy Smart Filters enable dynamic policies that automatically update as new patterns are added

ATP and Security Heartbeat

- Advanced Threat Protection (detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
- Sophos Security Heartbeat instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
- Sophos Security Heartbeat policies can limit access to network resources or completely isolate compromised systems until they are cleaned
- Lateral Movement Protection further isolates compromised systems by having healthy Sophos -managed endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain

SD-RED Device Management

- Central management of all SD-RED devices
- No configuration: Automatically connects through a cloud-based provisioning service
- Secure encrypted tunnel using digital X.509 certificates and AES 256-bit encryption
- Virtual Ethernet for reliable transfer of all traffic between locations
- IP address management with centrally defined DHCP and DNS Server configuration
- Remotely de-authorize SD-RED devices after a select period of inactivity
- Compression of tunnel traffic
- VLAN port configuration options

Clientless VPN

- Sophos unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC

Web Protection

Web Protection and Control

- Fully transparent proxy for anti-malware and web filtering
- Enhanced Advanced Threat Protection
- URL Filter database with millions of sites across 92 categories, backed by SophosLabs

- Surfing quota time policies per user/group
- Access time polices per user/group
- Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email
- Advanced web malware protection with JavaScript emulation
- Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- Second independent malware detection engine (Avira) for dual-scanning
- Real-time or batch mode scanning
- Pharming protection
- HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions
- SSL protocol tunnelling detection and enforcment
- Certificate validation
- High performance web content caching
- Forced caching for Sophos Endpoint updates
- File type filtering by mime-type, extension, and active content types (e.g. Activex, applets, cookies, etc.)
- YouTube for Schools enforcement per policy (user/group)
- SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
- Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload customs lists
- Block Potentially Unwanted Applications (PUAs)
- Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
- User/Group policy enforcement on Google Chromebooks

Cloud Application Visibility

- Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
- Discover Shadow IT at a glance
- Drill down to obtain details on users, traffic, and data
- One-click access to traffic shaping policies
- Filter cloud application usage by category or volume
- Detailed customizable cloud application usage report for full historical reporting

Application Protection and Control

- Synchronized App Control to automatically, identify, classify, and control all unknown Windows and Mac applications on the network by sharing information between Sophos-managed endpoints and the firewall
- Signature-based application control with patterns for thousands of applications
- Cloud Application Visibility and Control to discover Shadow IT
- App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
- Micro app discovery and control
- Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g. P2P), and risk level
- Per-user or network rule application control policy enforcement

Web and App Traffic Shaping

- Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

Zero-Day Protection

Dynamic Sandbox Analysis

- Full integration into your Sophos security solution dashboard
- Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- Aggressive behavioral, network, and memory analysis
- Detects sandbox evasion behavior
- Machine Learning technology with Deep Learning scans all dropped executable files
- Includes exploit prevention and Cryptoguard Protection technology from Sophos Intercept X
- In-depth malicious file reports with screen shots and dashboard file release capability

- Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
- Supports one-time download links

Static Threat Intelligence Analysis

- All files containing active code downloaded via the web or coming into the firewall as email attachments such as executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, docm, and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) are automatically sent for Threat Intelligence Analysis
- Files are checked against SophosLabs' massive threat intelligence database and subjected to multiple machine learning models to identify new and unknown malware
- Extensive reporting includes a dashboard widget for analyzed files, a detailed list of the files that have been analyzed and the analysis results, and a detailed report outlining the outcome of each machine learning model.

Central Orchestration

(Expected Soon)

SD-WAN Orchestration

- SD-WAN and VPN orchestration with easy and automated wizard-based creation of site-to-site VPN tunnels between network locations using an optimal architecture (hub-and-spoke, full mesh, or some combination). Supports IPSec, SSL or RED VPN tunnels. Integrates seamlessly with SD-WAN features for application prioritization, routing optimization, and leveraging multiple WAN links for resiliency and performance.

Central Firewall Reporting Advanced

- 30-days of cloud data storage for historical firewall reporting with advanced features to save, schedule and export custom reports.

XDR and MTR Connector

- Ready to integrate with Sophos Extended Threat Detection and Response (XDR) for cross-product threat hunting and analysis
- Support for Sophos 24/7 Managed Threat Response (MTR) service

Email Protection

Email Protection and Control

- Email scanning with SMTP, POP3, and IMAP support
- Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology
- Block spam and malware during the SMTP transaction
- DKIM and BATV anti-spam protection
- Spam greylisting and Sender Policy Framework (SPF) protection
- Recipient verification for mistyped email addresses
- Second independent malware detection engine (Avira) for dual scanning
- Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- Automatic signature and pattern updates
- Smart host support for outbound relays
- File type detection/blocking/scanning of attachments
- Accept, reject or drop over-sized messages
- Detects phishing URLs within e-mails
- Use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions
- TLS encryption support for SMTP, POP, and IMAP
- Append signature automatically to all outbound messages
- Email archiver
- Individual user-based block and allow sender lists maintained through the user portal

Email Quarantine Management

- Spam quarantine digest and notifications options
- Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- Self-serve user portal for viewing and releasing quarantined messages

Email Encryption and DLP

- Patent-pending SPX encryption for one-way message encryption
- Recipient self-registration SPX password management
- Add attachments to SPX secure replies
- Completely transparent, no additional software or client required
- DLP engine with automatic scanning of emails and attachments for sensitive data

- Pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by SophosLabs

Web Server Protection

Web Application Firewall Protection

- Reverse proxy
- URL hardening engine with deep-linking and directory traversal prevention
- Form hardening engine
- SQL injection protection
- Cross-site scripting protection
- Dual-antivirus engines (Sophos and Avira)
- HTTPS (TLS/SSL) encryption offloading
- Cookie signing with digital signatures
- Path-based routing
- Outlook anywhere protocol support
- Reverse authentication (offloading) for form-based and basic authentication for server access
- Virtual server and physical server abstraction
- Integrated load balancer spreads visitors across multiple servers
- Skip individual checks in a granular fashion as required
- Match requests from source networks or specified target URLs
- Support for logical and/or operators
- Assists compatibility with various configurations and non-standard deployments
- Options to change Web Application Firewall performance parameters
- Scan size limit option
- Allow/Block IP ranges
- Wildcard support for server paths and domains
- Automatically append a prefix/suffix for authentication

Reporting

Central Firewall Reporting

- Pre-defined reports with flexible customization options
- Reporting for Sophos Firewalls - hardware, software, virtual, and cloud
- Intuitive user interface provides graphical representation of data
- Report dashboard provides an at-a-glance view of events over the past 24 hours
- Easily identify network activities, trends, and potential attacks
- Easy backup of logs with quick retrieval for audit needs
- Simplified deployment without the need for technical expertise

Central Firewall Reporting Advanced

- Multi-firewall aggregate reporting
- Save custom report templates
- Scheduled reporting
- Export reports in PDF, CFV or HTML format
- Up to 1 year data storage per firewall
- MTR/XDR Connector

On-box Reporting

NOTE: Sophos Firewall reporting is included at no extra charge but individual log, report, and widget availability may be dependent on their respective protection module licenses.

- Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Current Activity Monitoring: system health, live users, IPSec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
- Report anonymization
- Report scheduling to multiple recipients by report group with flexible frequency options
- Export reports as HTML, PDF, Excel (XLS)
- Report bookmarks
- Log retention customization by category
- Full-featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization

Sophos Firewall Features by Subscription Summary

	Xstream Protection Bundle					*Available Separately*		
	Standard Protection Bundle			*Available Separately*				
	Base Firewall	Network Protection	Web Protection	Zero-Day Protection	Central Orchestration*	Central Firewall Reporting Adv.	Email Protection	Web Server Protection
General Management (incl. HA)	●							
Xstream Architecture	●							
Firewall, Networking and Routing	●							
Base Traffic Shaping and Quotas	●							
Secure Wireless	●							
Authentication	●							
Self-Serve User Portal	●							
Base VPN Options	●							
RED Site-to-Site VPN	●							
Sophos Connect VPN Client	●							
Intrusion Prevention (IPS)		●						
ATP and Security Heartbeat™		●						
SD-RED Device Management		●						
Clientless VPN		●						
Synchronized Application Control			●					
Web Protection and Control			●					
Application Protection and Control			●					
Cloud Application Visibility			●					
Web and App Traffic Shaping			●					
Dynamic Sandbox Analysis				●				
Threat Intelligence Analysis				●				
SD-WAN Orchestration					●			
Central Firewall Reporting Data	7 Days				30 Days	Up to 1 Year		
CFR Advanced Features					●	●		
XDR and MTR Connector					●	●		
Email Protection and Control							●	
Email Quarantine Management							●	
Email Encryption and DLP							●	
Web Application Firewall Protection								●
Logging and Reporting	●	●	●	●	●	●	●	●
Sophos Central Management	●	●	●	●	●	●	●	●

* Expected soon

Please note:

- Some features are not supported on XGS 87 and XG 86 models (on-box reporting, dual AV scanning, WAF AV scanning and email message transfer agent (MTA) functionality)
- MSP licensing options differ slightly to the above
- For XG Series hardware/virtual licensing, see the brochure under sophos.com/compare-xg

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

North American 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

© Copyright 2021. 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.

SOPHOS

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd (828358 - X)
No.7, Jalan 109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my

www.secureone.com.my