SOPHOS
Security made simple.

XG Firewall Features

Sophos XG Firewall

Highlights

- Purpose-built user interface with interactive control center utilizing traffic-light indicators (red, yellow, green) to instantly identify what needs attention at-a-glance
- The 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
- New 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 with 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, SSL, IPS, Web, App, Traffic Shapping (QoS), routing, 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 but intuitive model for configuring and managing security and control
- Policy Templates for common business applications including Microsoft Exchange, SharePoint, Lync, and much more defined in XML enabling customization and sharing.
- Sophos Security Heartbeat connecting Sophos endpoints with the Firewall to share health status and telemetry to enable instant identification of unhealty or compromised endpoints
- Dynamic firewall rule support for endpoint health (Sophos Security Heartbeat) to automatically isolate or limit network access to compromised endpoints
- Synchronized Application Control to automatically, identify, classify and control 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 to enable firewall rule and web policy simulation and testing by user, IP and time of day
- User Threat Quotient for identifying risky users based on recent browsing behavior and ATP triggers
- Application Risk Meter provides and overall risk factor based on the risk level of applications on the network
- Configuration API for all features for RMM/PSA integration
- Discover Mode (TAP mode) for seamless integration for trials and PoCs with support for Synchronized Security
- Full-featured centralized management of multiple firewalls with Sophos Firewall Manager available as a hardware, software, or virtual appliance
- Central management of multiple firewalls from Sophos Central providing one management console for all your Sophos IT security products.
- Easy streamlined setup wizard to enable quick out-of-the box deployment in just a few minutes
- Zero-touch setup and configuration in Sophos Central for new firewalls that remote staff can utilize during the initial startup to configure the device

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 trouble-shooting tools in

GUI (e.g., Packet Capture)

- High Availability (HA) support clustering two devices in active-active or active-passive mode.
- 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 and Netflow support
- Central managment support from Sophos Firewall Manager or Sophos Cloud Firewall Manager
- Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly
- API for third party integration
- Remote access option for Sophos Support
- Cloud-based license management via MySophos

Firewall, Networking, and Routing

- Stateful deep packet inspection firewall
- FastPath Packet Optimization
- 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 WiFi
- 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
- 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
- Multiple bridge 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
- IPv6 Ready Logo Program Approval Certification
- IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec

Base Traffic Shaping and Quotas

- Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options are 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 monitor and manage all 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 the latest security and encryption including WPA2 Personal and Enterprise
- Channel width seletion 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)
- 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 Gsuite
- 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
- L2TP and PPTP
- Remote access: SSL, IPsec, iPhone/iPad/ Cisco/Andriod VPN client support
- IKEv2 Support
- SSL client for Windows and configuration download via user portal

Sophos Connect IPSec 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

Sandstom Protection Subscription

Sandstorm Cloud Sandbox Protection

- 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 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

Network Protection Subscription

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
- Top rated by NSS Labs
- Thousands of signatures
- Granular category selection
- Support for custom IPS signatures
- IPS Policy Smart Filters that enable dynamic policies which 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 up
- Lateral Movement Protection further isolates compromised systems by having healthy Sophos endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain

Remote Ethernet Device (RED) VPN

- Central Management of all RED devices
- No configuration: Automatically connects through a cloud-based provisioning service
- Secure encrypted tunnel using digital X.509 certificates and AES256-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 RED devices after a select period of inactivity
- Compression of tunnel traffic
- VLAN port configuration options (RED 50)

Clientless VPN

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

Web Protection Subscription

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

- 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 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

Email Protection Subscription

Email Protection and Control

- E-mail 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
- Spam greylisting and Sneder 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 Subscription

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 (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 Appliaction FIrewall performance parameters
- Scan size limit option
- Allow/Block IP ranges
- Wildcard support for server paths
- Automatically append a prefix/suffix for authentication

Logging and Reporting

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

- 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

XG Firewall Features by Subscription Summary

Features (as listed above)		FullGuard Plus (included in TotalProtect Plus)				
			FullGuard (included in TotalProtect)			
		EnterpriseGuard Plus (included in EnterpriseProtect Plus)				
			EnterpriseGuard (included in EnterpriseProtect)			
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Firewall, Networking and Routing	●					
Base Traffic Shaping and Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
Sophos Connect IPSec Client	●					
Sandstorm Protection		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
Clientless VPN			●			
Synchronized Application Control				●		
Web Protection and Control				●		
Application Protection and Control				●		
Cloud Application Visibility				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●	●	●	●	●	●

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

16-12 FLNA (SM)