SOPHOS
Security made simple.

XG Firewall Features

Sophos XG Firewall

Product Highlights

- Innovative next-gen firewall user experience with interactive control center and streamlined workflows
- Optimized 2-clicks-to-anywhere navigation*
- Firewall rule Control Center widget monitors firewall rule activity for business, user and network policies and tracks unused, disabled, changed and new policies
- New unified policy model enabling all business, user and network rules to be managed on a single screen with powerful filtering and search options
- Firewall rule templates for common business applications like Microsoft Exchange, SharePoint, Lync, and much more defined in XML enabling customization and sharing.
- Policy natural language descriptions and at-a-glance policy enforcement indicators
- Custom IPS, Web, App, and Traffic Shapping (QoS) settings per user or network rule on a single screen
- Layer-8 user identity awareness across key areas of the firewall
- Sophos Security Heartbeat™ connecting Sophos Central managed endpoints with the Firewall to share health status and telemetry
- Policy support for Sophos Security Heartbeat to automatically isolate or limit network access to compromised systems
- 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
- Discover Mode (TAP mode) for seamless integration for trials and PoCs
- Full-featured centralized management with Sophos Firewall Manager available as a hardware, software, or virtual appliance

Base Firewall

General Management

- Rich graphical interactive control center with traffic-light style indicators for important alerts
- 2-clicks-to-anywhere navigation*
- Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
- High Availability (HA) support clustering 2 devices in active-active or active-passive mode.
- HA Support for dynamic addresses on WAN interfaces*
- 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 3rd party integration
- Remote access option for Sophos Support
- Cloud-based license management via MySophos
- Deployment options include XG Series hardware appliances, Software or Virtual, and Microsoft Azure*

Firewall, Networking & Routing

- Stateful deep packet inspection firewall
- FastPath Packet Optimization
- User, network, or business application based firewall rules
- 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
- Flood protection: DoS, DDoS and portscan blocking
- Country blocking by geo-IP with simple country and continent selections*
- Routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)
- Per-rule and policy based routing by source, destination, user/group or layer-4 servce*
- Upstream proxy support
- Protocol independent multicast routing with IGMP snooping
- Bridging with STP support and ARP broadcast forwarding
- VLAN DHCP support and tagging
- Simultaneous DHCP Server and Relay support*
- 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 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec

Base Traffic Shaping & 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

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
- Support for IEEE 802.1X (RADIUS authentication)
- 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
- Rogue AP detection

Authentication

- Transparent, proxy authentication (NTLM) or client authentication
- Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Sophos Transparent Authentication Suite (STAS) server authentication agents for Active Directory SSO
- Client authentication agents for Windows, Mac OS X, Linux 32/64

- Authentication certificates for iOS and Android
- Single sign-on: Active directory, eDirectory
- Authentication services for IPSec, L2TP, PPTP, SSL
- Captive Portal
- Two factor authentication (one-time password support) for IPSec and SSL VPN, user portal, and Webadmin*

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 (requires Email Protection)
- Setup two-factor authentication with QR Code*

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
- SSL client for Windows & configuration download via user portal

IPSec Client (sold separately)

- Authentication: Pre-Shared Key (PSK), PKI (X.509), Smartcards, Token and XAUTH
- Encryption: AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (up to 2048 Bit), DH groups 1/2/5/14, MD5 and SHA-256/384/512
- Intelligent split-tunneling for optimum traffic routing
- NAT-traversal support
- Client-monitor for graphical overview of connection status
- Multilingual: German, English and French

Network Protection Subscription

Intrusion Prevention (IPS)

- High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns for maximum performance and protection
- Thousands of signatures
- Support for custom IPS signatures
- Flexible IPS policy deployment as part of any network or user policy with full customization

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
- Destination Security Heartbeat™ automatically protects healthy systems from connecting to compromised endpoints and servers*
- Block all traffic to or from non-managed devices and endpoints without a Sophos Security Heartbeat™*

Clientless VPN

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

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)
- Firewall-to-Firewall RED Tunnels*

Web Protection Subscription

Web Protection and Control

- Enterprise-grade Secure Web Gateway web policy engine with top-down execution and inheritence with flexible user/group policy definitions, customizable activities, block/warn/allow actions, and time-of-day and day-of-week constraints*
- High-performance 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
- SafeSearch enforcement
- Creative commons image search enforcement*
- Google Apps domain enforcement*
- Unscannable content handling options*
- Support for adding custom 3rd party URL databases*

Application Protection and Control

- Enhanced application control with signatures and Layer 7 patterns for thousands of applications
- Dynamic application identification utilizes the Synchronized Security Heartbeat™ link with the endpoint to determine apps responsible for generating unknown traffic on the network*
- 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 & 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

- Per-domain mail routing*
- Integrated MTA (Message Transfer Agent) to store-and-forward mail in the event servers are unavilable*
- 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
- 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
- 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
- TLS Encryption support for SMTP, POP and IMAP
- Append signature automatically to all outbound messages
- Email archiver

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
- SPX Reply Portal for recipients to reply to encrypted messages securely*
- 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 & 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 WAF 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: individual log, report and widget availability depends on enabled software subcriptions.

- Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Search Engines, Web Servers, FTP), Network & Threats (IPS, ATP, Wireless, Security Heartbeat), 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
- Full log viewer available from every screen that pops-open in a new window*
- Customized log viewer refresh period and color coded log lines for easy trouble-shooting*
- Log retention customization by category

XG Firewall Features by Subscription Summary

Features (as listed above)		FullGuard (including Enhanced Support)			
		EnterpriseGuard (incl. Enhanced Support)			
	Base Firewall	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●				
Firewall, Networking & Routing	●				
Base Traffic Shaping & Quotas	●				
Secure Wireless	●				
Authentication	●				
Self-Serve User Portal	●				
Base VPN Options	●				
IPSec Client	Sold seperately				
Intrusion Prevention (IPS)		●			
ATP & Security Heartbeat™		●			
Remote Ethernet Device (RED) VPN		●			
Clientless VPN		●			
Web Protection and Control			●		
Application Protection and Control			●		
Web and App Traffic Shaping			●		
Email Protection and Control				●	
Email Quarantine Management				●	
Email Encryption and DLP				●	
Web Application Firewall Protection					●
Logging and Reporting	●	●	●	●	●

* New in XG Firewall v16

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