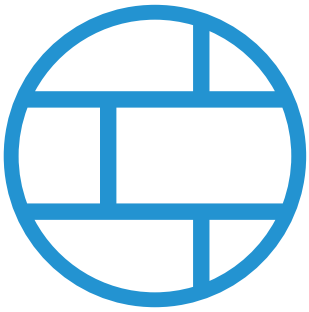
SOPHOS

Security made simple.



XG Firewall Features

Sophos XG Firewall

Key Features

- Purpose-built user interface with interactive control center
- Optimized 3-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 enabling all business, user and network policies to be managed on a single screen with powerful filtering and search options
- Policy 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 policy on a single screen
- Layer-8 user identity awareness across key areas of the firewall
- Sophos Security Heartbeat connecting Sophos endpoints with the Firewall to share health status and telemetry to enable instant identification of unhealty or compromised endpoints
- Policy support for Sophos Security Heartbeat to automatically isolate or limit network access to compromised endpoints
- 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 (command-line only initially)
- Full-featured centralized management with Sophos Firewall Manager available as a hardware, software, or virtual appliance

General Management

- Purpose-built streamlined user interface
- 3-clicks-to-anywhere navigation
- Self-documenting menu system
- Advanced trouble-shooting tools in GUI (e.g. Packet Capture)
- 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 for one-click VPN setup
- Configuration change tracking
- Email or SNMP trap notification options
- SNMP support

Firewall Routing and Services

- Zone isolation and zone-based policy support.
- Default zones for LAN, WAN, DMZ, LOCAL, VPN and WiFi
- Custom zones on LAN or DMZ
- Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF)
- Protocol independent multicast routing with IGMP snooping
- Bridging with STP support and ARP broadcast forwarding
- WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules
- 802.3ad interface link aggregation
- Full configuration of DNS, DHCP and NTP
- IPv6 support with tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec
- Sophos Remote Ethernet Device (RED) support
- VLAN DHCP support and tagging
- Multiple bridge support

Advanced Threat Protection and Synchronized Security

- Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, HTTP Proxy 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

Network Protection and Control

- Stateful deep packet inspection firewall
- FastPath Packet Optimization
- Intrusion protection: high-perofrmance, next-gen IPS deep packet inspection engine
- Selective IPS patterns for maximum performance and protection
- Flood protection: DoS, DDoS and portscan blocking
- Country blocking by geo-IP
- Site-to-site VPN: SSL, IPSec, 256- bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- Remote access: SSL, IPsec, iPhone/iPad/Cisco VPN client support
- Network, user, or web-based traffic shaping (QoS)
- Network traffic quotas allow unlimited customization for total or individual network traffic quotas.
- Real-time VoiP optimization

Authentication

- Transparent, proxy authentication (NTLM/Kerberos) or client authentication
- Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- Server authentication agents for Active Directory SSO, STAS, SATC
- Client authentication agents 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

VPN Options

- IPSec, SSL, PPTP, L2TP, Cisco VPN (iOS), OpenVPN (iOS and Android)
- Clientless Portal using Sophos unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet and VNC
- Sophos Remote Ethernet Device (RED) support

VPN IPsec Client

- 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

VPN SSL Client

- Proven SSL-(TLS)-based security
- Minimal system requirements
- Profile support for varying levels of access
- Supports MD5, SHA, DES, 3DES and AES
- Works through all firewalls, regardless of proxies and NAT
- Support for iOS and Android

Remote Ethernet Device (RED) VPN

- Central Management of all RED appliances
- No configuration: Automatically connects through a cloud-based provisioning service
- Secure encrypted tunnel using digital X.509 certificates and AES256- encryption
- RED sites are fully protected by the Network, Web and Mail security subscriptions of the Firewall.
- 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 (RED 50, RED 10 revision 2, 3)
- VLAN port configuration options (RED 50)

Secure Wireless

- Simple plug-and-play deployment of Sophos wireless access points - automatically appear on the firewall control center
- Central monitor and manage all access points (APs) and wireless clients through the built-in wireless controller
- Integrated security: All Wi-Fi traffic is automatically routed through the Firewall
- Multiple SSID support per radio
- Strong encryption supports state-of-the-art wireless authentication including WPA2-Enterprise and IEEE 802.1X (RADIUS authentication)
- 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

Web Protection and Control

- Fully transparent user-based web filtering without the need for any proxy settings
- URL Filter database with millions of sites across 92 categories backed by SophosLabs
- User, group, time, or network based policies
- Browsing quota time
- 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 on a per user or network policy basis with 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

Application Protection and Control

- Enhanced application control with signatures and Layer 7 patterns for thousands of applications
- 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
- Custom application traffic shaping options to limit or guarantee upload or download priority and bitrate individually or shared

Email Protection and Control

- Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology
- Block spam and malware during the SMTP transaction
- Detects phishing URLs within e-mails
- Global & per-user domain and address black/white lists
- Recipient Verification against Active Directory account
- E-mail scanning with SMTP, POP3, and IMAP support
- Dual antivirus engines (Sophos & Avira)
- True-File-Type detection/scan within archive files
- Scan embedded mail formats: Block malicious and unwanted files with MIME type checking
- Quarantine unscannable or over-sized messages
- Filter mail for unlimited domains and mailboxes
- Automatic signature and pattern updates
- Sophos Live Anti-Virus real-time cloud lookups

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
- Transparent en-/decryption and digital signing for SMTP e-mails
- Completely transparent, no additional software or client required
- Allows content/virus scanning even for encrypted e-mails
- Central management of all keys and certificates - no key or certificate distribution 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

User Self-Serve Portal

- SMTP quarantine: view and release messages held in quarantine
- Sender blacklist/whitelist
- Hotspot access information
- Download the Sophos Authentication Agent (SAA)
- Download remote access client software and configuration files
- HTML5 VPN portal for opening clientless VPN connections to predefined hosts using predefined services
- Download HTTPS Proxy CA certificates

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

- Hundreds of on-box reports with dozens of custom report options
- Data anonymization
- Report scheduling to multiple recipients by report group with flexible frequency options
- Log retention customization by category
- Full log viewer
- Dashboards for traffic, security, and user threat quotient
- Application reports for user app risks, blocked user apps, web risks, blocked web attempts, search engine, web server usage, web server protection, and user data transfer and FTP traffic
- Network and threat reports for intrusion attacks, advanced threat protection, wireless, and Security Heartbeat
- VPN reports
- Email usage and protection reports
- Compliance reports for HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, and CIPA

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

Oxford, UK | Boston, USA

1129-02.13DD.dsna.simple