Sophos Firewall OS

Cyberoam and Sophos come together to introduce an all-new operating system

Our latest firmware, Sophos Firewall Operating System (SFOS) takes simplicity and protection to a whole new level. Here are the key highlights of what’s new and exciting in SFOS for Cyberoam users.

**Highlights**
- Sandstorm protection
- Advanced threat protection for your network
- Web caching and SNI-based protection
- Extends main office security to remote offices
- Policy-based routing
- New Control Center for instant insight and control
- Security Heartbeat connects firewall and endpoints for smarter security
- Stronger email protection with SPX encryption, and built-in DLP

**A Firewall That Makes Security Easier**
- The new SFOS offers a smarter, task-oriented user interface
  - Simplified policy configuration
    - Business application rule — Allows internal or external users to access your secure servers and services
    - User/network rules — Controls your traffic by source, service, destination, zone by using a network policy. User rules allow a user identity to be attached to a network rule to manage access to web and application content.
  - Support for country or continent-based filtering in firewall rules
- Network security control center
  - Provides instant insight into system performance, traffic patterns, alerts, and active policies

**Sandstorm Protection**
- Effective affordable cloud-sandboxing protection
  - Identifies suspicious files with active content for further sandboxing analysis
  - Can identify and block ransomware and other advanced threats before they enter the network

**Advanced Threat Protection (ATP)**
- Protects your network from advanced threats and botnets by identifying infected or compromised hosts inside the network and preventing their communication with command-and-control servers

**Policy Routes**
- Route select traffic to a custom gateway based on source, destination, or layer-4 service

**Per Domain Routing**
- Route incoming mail to the correct destination server, based on the target domain
**Firewall Hostname**
- Assign a custom hostname to your firewall

**Authentication**
- Improved access security with support for OATH-TOTP one-time passwords directly on the firewall, eliminating the need for a separate 2FA solution
- Supports IPSec, SSL VPN, User Portal, and WebAdmin access (We recommend using the free Sophos authenticator app for iOS and Android)
- Sophos Transparent Authentication Suite (STAS) configuration has been added to the interface, enabling easy setup without requiring the CLI

**Enhancements in Web Filtering**
- Web Caching allows the Web Filter to speed up requests for frequently visited sights, when enabled
- Endpoint update data can also be cached for Sophos Endpoints
- Server name indication (SNI)-based categorization for better classification of HTTPS websites
- Intuitive, easy-to-maintain web policies dramatically reduce firewall rule counts
- Addition of a ‘Warn’ action for situations where Block and Allow aren’t the suitable option
- Limited access to a selected Google Apps domain, reducing the risk of data loss from users transferring documents to their personal Google Apps.
- Enforcing search engine filters for content with a Creative Commons license, reducing the exposure to inappropriate images

**Affordable Remote Office Security**
- Extends security of your main office to remote offices
- A Remote Ethernet Device (RED) in the remote office connects to the main office’s firewall, safely routing all branch traffic through the main office
- RED appliances can be centrally managed through your Cyberoam UTM/next-gen firewall devices (after upgrading to SFOS)

**Heartbeat Links Your Firewall and Endpoint**
- Security Heartbeat combines the intelligence of your firewall and endpoints into a single system, providing advanced threat protection
- Offers instant discovery, positive identification, and automated action to detect and isolate threats
- Integrates host health status into the security policy settings of your firewall, allowing you to isolate or limit the access for compromised systems until they are cleaned up
- Enhanced Application Control helps your firewall determine the application responsible for generating uncategorized network traffic
- Limits access to destinations and servers based on the status of their Heartbeat

**Enhanced Wireless Controls**
- Cyberoam’s UTM/next-gen firewall wireless controller in CyberoamOS 10.6.2 includes secure hotspots, support for all Sophos Access Point models, time-based SSIDs, and more
- Three modes of secure hotspots or Guest Wi-Fi access include: Terms of Use Acceptance, Password of the Day, and Vouchers for Internet Access

**Stronger Email Protection with Built-in DLP**
- Supports secure POP and secure IMAP protocols
- New Secure PDF Exchange (SPX) encryption encapsulates emails and attachments into an encrypted, password-protected PDF, allowing access only to the intended recipient
- Built-in DLP scans your outgoing emails for sensitive information
- Dual antivirus provides maximum recognition rate by scanning the traffic twice using different virus scanners
- Offers full store-and-forward support for MTA that allows the firewall to store mail when target servers are unavailable — ensuring business continuity
SSL VPN
- Access site-to-site VPN tunnels that can be established via an SSL connection

Enhanced Web Application Firewall/Web Server Protection
- Reverse Authentication verifies users with a web application firewall when a real web server does not support authentication
- Ensures a user only needs to authenticate once, even when there are more than one real web servers assigned to a virtual web server
- Defines real web servers using site path routing, ensuring incoming requests are forwarded
- Web Application Firewalls now supports HTML rewriting, MSRPC support, antivirus scanning, and SQL injection/XSS protection

On-appliance Reporting
- Additional reports are available for new features, including ATP, Security Heartbeat, Wireless Access Points, Email Protection, SPX and DLP, and RED
- The enhanced User Threat Quotient includes advanced threats triggered from user endpoints, in addition to their web behavior

Microsoft Azure Platform Support
- Supports deployment in Microsoft Azure as a preconfigured virtual machine from the Microsoft Azure Marketplace, with pay-as-you-go or bring-your-own-licensing (BYOL) pricing and licensing options

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