SOPHOS
Security made simple.

Sophos UTM Feature List

General Management

‣ Customizable dashboard
‣ Role-based administration: Auditor, read-only and manager for all functions
‣ No-charge, centralized management of multiple UTMs via Sophos UTM Manager (SUM)
‣ Configurable update service
‣ Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
‣ Point & Click IPS rule management
‣ Self-service user portal for one-click VPN setup
‣ Configuration change tracking
‣ Manual or fully automated backup and restore options
‣ Email or SNMP trap notification options
‣ SNMP support
‣ One-time password (OTP) / Two-factor authentication (2FA) supports OATH protocol for WebAdmin, User Portal, SSL VPN, IPSec VPN, HTML5 Portal and SSH Login*

Network Routing and Services

‣ Routing: static, multicast (PIM-SM) and dynamic (BGP, OSPF)
‣ NAT static, masquerade (dynamic)
‣ Protocol independent multicast routing with IGMP snooping
‣ Bridging with STP support and ARP broadcast forwarding
‣ WAN link balancing: 32 Internet connections, auto-link health check, automatic failover, automatic and weighted balancing and granular multipath rules
‣ Zero-config active/passive high- availability
‣ Active/active clustering for up to 10 appliances
‣ 802.3ad interface link aggregation
‣ QoS with full control over bandwidth pools and download throttling using Stochastic Fairness Queuing and Random Early Detection on inbound traffic
‣ Full configuration of DNS, DHCP and NTP
‣ Server load balancing
‣ IPv6 support
‣ RED support

Network Protection

‣ Intrusion protection: Deep packet inspection engine, 18,000+ patterns
‣ Selective IPS patterns for maximum performance and protection
‣ IPS pattern aging algorithm for optimal performance*
‣ Flood protection: DoS, DDoS and portscan blocking
‣ Country blocking by region or individual country (over 360 countries) with separate inbound/outbound settings and exceptions
‣ 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
‣ VoIP handling for SIP and H.323 connections
‣ Connection tracking helpers: FTP, IRC, PPTP, TFTP
‣ Identity-based rules and configuration with Authentication Agent for users

Advanced Threat Protection*

‣ Detect and block network traffic attempting to contact command and control servers using DNS, AFC, HTTP Proxy and firewall
‣ Identify infected hosts on the network and contain their network activity
‣ Selective sandboxing of suspicious code to determine malicious intent

Authentication

‣ Transparent, proxy authentication (NTLM/Kerberos) or client authentication
‣ Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
‣ Single sign-on: Active directory, eDirectory
‣ SSL support
‣ Tools: server settings check, username/password testing and authentication cache flush
‣ Graphical browser for users and groups
‣ Automatic user creation
‣ Scheduled backend synchronization prefetch
‣ Complex password enforcement

Web Protection

- URL Filter database with 35 million+ sites in 96 categories and 65+ languages
- Application Control: Accurate signatures and Layer 7 patterns for thousands of applications
- Dynamic application control based on productivity or risk threshold
- View traffic in real-time, choose to block or shape
- Malware scanning: HTTP/S, FTP and web-based email via dual independent antivirus engines (Sophos & Avira) block all forms of viruses, web malware, trojans and spyware
- Fully transparent HTTPS filtering of URLs*
- Advanced web malware protection with JavaScript emulation*
- Live Protection real-time in-the-cloud lookups for the latest threat intelligence
- Potentially unwanted application (PUA) download blocking*
- Malicious URL reputation filtering backed by SophosLabs
- Reputation threshold: set the reputation threshold a website requires to be accessible from internal network
- Active content filter: File extension, MIME type, JavaScript, ActiveX, Java and Flash
- YouTube for Schools enforcement
- SafeSearch enforcement
- Google Apps enforcement*

Web Policy

- Authentication: Active Directory, eDirectory, LDAP, RADIUS, TACACS+ and local database
- Single sign-on: Active Directory, eDirectory, Apple Open Directory
- Proxy Modes: Standard, (Fully) Transparent, Authenticated, Single sign-on and Transparent with AD SSO*
- Transparent captive portal with authentication
- Support for separate filtering proxies in different modes
- Time, user and group-based access policies
- Allow temporary URL filter overrides with authentication
- Client Authentication Agent for dedicated per-user tracking
- Cloning of security profiles
- Customizable user-messages for events in local languages
- Custom HTTPS verification CA support
- Setup wizard and context sensitive online help
- Customizable block pages
- Custom categorization to override categories or create custom categories*
- Authentication and filtering options by device type for iOS, Android, Mac, Windows and others*
- Policy testing tool for URLs, times, users and other parameters*

Email Protection

- Reputation service with spam outbreak monitoring based on patented Recurrent-Pattern-Detection technology
- Advanced spam detection techniques: RBL, heuristics, SPF checking, BATV, URL scanning, grey listing, RDNS/HELO checks, expression filter and recipient verification
- 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 and POP3 support
- Dual antivirus engines (Sophos & Avira)
- Archived and compressed attachment scanning with deep-level support
- 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

Email Encryption and DLP

- Patent-pending SPX encryption for one-way message encryption*
- Transparent en-/decryption and digital signing for SMTP e-mails
- Completely transparent, no additional software or client required
- Supports S/MIME, OpenPGP, and TLS standards
- PGP key server support
- 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*

Email Management

- User-quarantine reports mailed out daily at customizable times
- Log Management service support
- Customizable User Portal for end-user mail management, in 15 languages
- Anonymization of reporting data to enforce privacy policy
- Over 50 Integrated reports
- PDF and CSV exporting of reports
- Customizable email footers and disclaimers
- Setup wizard and context sensitive online help

End-User 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

VPN Options

‣ PPTP, L2TP, SSL, IPsec, HTML5-based and Cisco
client-based remote user VPNs, as well as IPsec, SSL,
Amazon VPC-based site-to-site tunnels and Sophos
Remote Ethernet Device (RED) plug-and-play VPN

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
‣ IPsec Tunnel Binding

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

Clientless VPN

‣ True clientless HTML5 VPN portal for accessing
applications securely from a browser on any device

VPN One-Click

‣ Easy setup and installations of every client within minutes
‣ Download of client-software, individual configuration
files, keys and certificates one click away from
the Security Gateway end-user portal
‣ Automatic installation and configuration of the client
‣ No configuration required by end user

VPN RED

‣ Central Management of all RED
appliances from Sophos UTM
‣ 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 Central UTM.
‣ 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 Wi-Fi

‣ Simple plug-and-play deployment,
automatically appearing in the UTM
‣ 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 UTM
‣ Wireless 802.11 b/g/n at 2.4 GHz and 5GHz (AP 50)
‣ Power-over-Ethernet 802.3af (AP 30/50)
‣ Multiple SSID support: Up to 8
‣ Strong encryption supports state-of-the-art
wireless authentication including WPA2-Enterprise
and IEEE 802.1X (RADIUS authentication)
‣ Wireless guest Internet access with customizable
splash pages on your captive portal
‣ Voucher-based guest access for daily or weekly access
‣ Time-based wireless network access
‣ Wireless repeating and bridging meshed
network mode with AP 50
‣ Hotspot backend authentication support*
(RADIUS, TACACS, LDAP, AD)

Web Application Firewall Protection

‣ Reverse proxy
‣ URL hardening engine
‣ Form hardening engine
‣ Deep-linking control
‣ Directory traversal prevention
‣ 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*

Web Application Firewall Management

‣ Auto server discovery scans attached networks and identifies web servers
‣ Integrated load balancer spreads visitors across multiple servers
‣ Predefined firewall profiles for Microsoft Outlook Web Access (OWA)
‣ Quick server switch allows easy maintenance
‣ 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

UTM Endpoint Protection

‣ Windows endpoint protection with Sophos Antivirus and device control
‣ On-access, on-demand or scheduled scanning for malware, viruses, spyware and Trojans
‣ PUA scanning
‣ Live Protection Antivirus provides real-time, in-the-cloud lookups for the latest threat intelligence
‣ HIPS with suspicious behavior detection
‣ Web protection with malicious site protection
‣ Download scanning
‣ Device control for hundreds of popular device types include removable storage, optical media, modems, Bluetooth, wireless, infrared and more
‣ Web in Endpoint enforcement of user and group web policy and web malware scanning on the endpoint with full policy and reporting synchronization

UTM Endpoint Management

‣ Fully managed within the UTM
‣ Easy deployment from the UTM using using our installer
‣ Monitor connected endpoints, threat status and device utilization with full log access
‣ Alerts for infected endpoints*

SEC Endpoint Integration*

‣ Integration with Sophos Enterprise Console Endpoint Management provides UTM web policy and reporting for Web in Endpoint

Logging and Reporting

‣ Logging: Remote syslog, nightly rotation, email/ftp/ SMB/SSH archiving and log management service
‣ On-box reporting: Packet filter, intrusion protection, bandwidth and day/week/month/year scales
‣ Identity-based reporting
‣ PDF or CSV report exporting
‣ Executive report scheduling and archiving
‣ Reactive reporting engine crafts reports as you click on data
‣ Save, instantly email or subscribe recipients to any reports
‣ PDF and CSV exporting of reports
‣ Nightly compression and rotation of logs
‣ Log file archiving: On-box, FTP, SMB, SSH, Email and Syslog
‣ Hundreds of on-box reports
‣ Daily activity reporting
‣ URL filter override report
‣ Per-user tracking and auditing
‣ Anonymization of reporting data to enforce privacy policy
‣ Full transaction log of all activity in human-readable format
‣ Web log searching parameters per user, URL or action*

* New in UTM 9.2 Accelerated

Try it now for free

Register for a free 30-day evaluation at sophos.com/try-utm

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

SOPHOS