UTM FIREWALL SPECS

HARDWARE SPECIFICATIONS

ASIC-Based Standalone Appliance	
GbE RJ45 Ports	42
Internal Storage	64 GB

SYSTEM PERFORMANCE

Firewall Throughput (1518 / 512 / 64 byte UDP packets)	4 / 4 / 4 Gbps
Firewall Latency (64 byte UDP packets)	6 µs
Firewall Throughput (Packets Per Second)	6 Mpps
Concurrent Sessions (TCP)	3 Million
IPS Throughput	2 Gbps
Antivirus Throughput (Proxy Based / Flow Based)	600 / 1,100 Mbps
Virtual Domains (Default / Max)	10

Network Services and Support

Built-in DHCP, NTP, DNS Server and DNS proxy
NTP, DDNS and DNS service
Interface modes: Sniffer, Port Aggregated, Loopback, VLANs (802.1Q and Trunking), hardware and software switches
Static and Policy rRouting
WAN load balancing with ECMP (Equal Cost Multi-Path) and redundancy
Dynamic routing protocols:
- RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4
Multicast traffic: sparse and dense mode, PIM support
Content routing: WCCP and ICAP
IPv6 Support: Management over IPv6, IPv6 routing protocols, IPv6 tunnelling, firewall and UTM for IPv6 traffic, NAT46, NAT64, IPv6 IPSEC VPN

User & Device Identity Control

Local user database
Remote user authentication service support: LDAP, Radius and TACACS+
Single-sign-on: Windows AD, Novell eDirectory, Citrix and Terminal Server
Agent, Radius (accounting message), user access (802.1x, captive portal) authentication
PKI and certificates: X.509 certificates, SCEP support, Certificate Signing Request (CSR) creation, auto-renewal of certificates before expiry, OCSP support
2-factor authentication: 3rd party support, integrated token server with physical, SMS and Soft Tokens
Device Identification: device and OS fingerprinting, automatic classification, inventory management
User and device-based policies

Firewall

Operating modes: NAT/Route and Transparent
Schedules: One-time, Recurring
Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle)
VoIP traffic support: SIP/H.323 /SCCP NAT traversal, RTP pin holing
Protocol type support: SCTP, TCP, UDP, ICMP, IP
Section or global policy management view
Policy objects: predefined, customs, object grouping, tagging and coloring
Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN
NAT configuration: per policy based and central NAT Table
NAT support: NAT64, NAT46, static NAT, dynamic NAT, PAT, Full Cone NAT, STUN
Traffic shaping and QOS: shared policy shaping, per-IP shaping, maximium & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ) support

VPN

IPSEC VPN:
- Remote peer support: IPSEC-compliant dialup clients, peers with static IP/dynamic DNS
- Authentication method: certificate, pre-shared key
- IPSEC Phase 1 mode: aggressive and main (ID protection) mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- supports IKEv1, IKEv2 (RFC 4306)
- IKE mode configuration support (as server or client), DHCP over IPSEC
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128. AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman Group support: 1, 2, 5, 14
- XAuth support as client or server mode

- XAuth for dialup users: Server type option (PAP, CHAP, Auto), NAT Traversal option
- Configurable IKE encryption key expiry, NAT traversal keepalive frequency
- Dead peer detection
- Replay detection
- Autokey keep-alive for Phase 2 SA

IPSEC VPN deployment modes: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN termination in transparent mode,
IPSEC VPN Configuration options: route-based or policy-based
Customizable SSL VPN portal: color themes, layout, bookmarks, connection tools, client download

IPS

IPS engine: 7,000+ up-to-date signatures, protocol anomaly detection, custom signatures, manual, automatic pull or push signature update, threat encyclopedia integration
IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time
Filter Based Selection: severity, target, OS, application and/or protocol
Packet logging option
IP(s) exemption from specified IPS signatures
IPv4 and IPv6 Rate based DOS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCTP/ICMP session flooding (source/destination)
IDS sniffer mode

Application Control

Detects over 3,000 applications in 19 Categories:
Botnet, Collaboration, Email, File Sharing, Game, General Interest, IM, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Special, Web (Others)
Custom application signature support
Advanced Instant Messenger (IM) & Facebook control
Filter based selection: by category, popularity, technology, risk, vendor and/or protocol
Actions: block, reset session, monitor only, application control traffic shaping
SSH Inspection

Threat Protection

Inspect SSL Encrypted traffic option for IPS, Application Control, Antivirus, Web Filtering and DLP
Botnet server IP blocking with global IP reputation database
Flow-based Antivirus: protocols supported - HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, SMB, ICQ, YM, NNTP
Proxy-based Antivirus:
Protocol Support: HTTP/HTTPS, STMP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP
External cloud-based file analysis (OS sandbox) support
File submission blacklisting and whitelisting
Heuristic scanning option

Feature Summary

Web filtering inspection mode support: proxy-based, flow-based and DNS
Manually defined web filtering based on URL, web content & MIME header
Dynamic web filtering with cloud-based realtime categorization database: over 250 Million URLs rated into 78 categories, in 70 languages
Safe Search enforcement: transparently inserts Safe Search parameter to queries. Supports Google, Yahoo!, Bing & Yandex, definable YouTube Education Filter
Additional features offered by proxy-based web filtering:
- Filter Java Applet, ActiveX and/or cookie
- Block HTTP Post
- Log search keywords
- Rate images by URL
- Block HTTP redirects by rating
- Exempt scanning encrypted connections on certain categories for privacy
- Web Browsing quota by categories

Web filtering local categories & category rating override
Web filtering profile override: allows administrator to temporarily assign different profiles to user/user grou
Proxy avoidance prevention: proxy site category blocking, rate URLs by domain & IP address, block redirects from cache & translation sites, proxy avoidance application blocking (application control), proxy behavior blocking (IPS)

DLP message filter:
- Protocol supported: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP
- Actions: log only, block, quarantine user/IP/Interface
- Predefined filter: credit card number, Social Security ID
DLP File Filter:
- Protocol Supported: HTTP-POST, HTTP=-GET,SMTP, POP3, IMAP, MAPI, FTP, NNTP
- Filter options: size, file type, watermark, content, if encrypted
DLP watermarking: allows filter files that pass through the unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark. Support Windows and Linux free watermarking tools.
DLP fingerprinting: generates a checksum fingerprint from intercepted files and compare it to those in the fingerprint database.
DLP archiving: records full content in email, FTP, IM, NNTP, and web traffic

Administration

Management Access: HTTPS via web browser, SSH, telnet, console
Systems Integration: SNMP, sFlow, syslog, alliance partnerships
Rapid deployment: USB auto-install, local and remote script execution
Dynamic, real-time dashboard status & monitoring widgets

Certification

ICSA Firewall, SSL VPN, IPSEc VPN, AV and IPS certification
USGv6 IPv6 Certified

ɔ/IP