

Firewall/VPN Features	Benefit
Perimeter Firewall	Block threats at the boundary - <i>before</i> they enter your network.
Stateful Packet Inspection	Keeps out invalid traffic by ensuring all packets are part of a legitimate sequence.
Intrusion Prevention System (IPS)	Monitors and reacts to malicious activity and gives, through reporting, an overall view of the attacks occurring to your systems.
Outbound (egress) filtering rules	Controls what Internet services and ports users can access.
Port-agile traffic blocking	Detects & blocks port agile traffic such as peer to peer downloads.
Dynamic NAT (DNAT) and Static NAT (SNAT) operation	Allowing a range of Internet accessible servers to be positioned on the internal network with multiple IPs supported.
Support for SSL, IPSec & L2TP VPN	Secure Remote Access for mobile/home users with site-to-site VPN connectivity and support for Internal SSL VPN.
Internal Firewall	Segregate local networks into physically independent zones (useful for controlling interzone access and in the event of server compromise).
Web Filtering Features*	Benefit
Dynamic Content Analysis™	Screens the content, context and construction of web pages, accurately detecting and blocking all undesirable, hidden or malicious content (incl. anonymous proxies).
SSL Interception	All unknown secure traffic can be decrypted and inspected (using Dynamic Content Analysis) so inappropriate and malicious HTTPS/SSL content (including SSL proxies) can be effectively blocked.
VIPRE Anti-malware engine (Note: subscription payable)	Behavior-based and heuristic detection of zero-day web borne threats using Sunbelt Software's award winning VIPRE anti-malware engine.
Flash Filtering	Screens actual SWF file code to accurately detect and block undesirable Flash content such as online games and video players.
Outbound (web post) monitoring and blocking	Monitors and blocks text posted on the web (i.e. inappropriate blog/forum/Social Networking/Twitter posts) using a keyword analysis system.
Customizable URL Blocklists	Current, categorized and customizable URL blocklists (updated daily with content from IWF database) control access to a pre-defined list of undesirable websites (includes reverse-lookup option).
Whitelist mode	Users can only access a customized list of 'allowed' sites
Temporary 'Banned User' List	Ban selected users until a selected date or time
MIME, File extension, download size, advert, cookie & PICS blocking	Filtering policies can be set to detect PICS codes, file types, download sizes, adverts and cookies; and block such content as required (prevents download of viruses and other malicious code from websites, as well as music and other copyright material).
Policy based controls	Different filtering policies can be created and set for different groups of users, in accordance with organization policy or the AUP.
Time and room based controls	Filtering can be set at different levels for different times of the day and for different rooms or departments, defined by IP or computer names.
Logging, filtering and censoring of Instant Messenger applications	Control and monitor the use of Instant Messaging applications. IM file transfers and attachments can be logged or blocked and selected words/phrases can be censored and set to trigger alerts with responses sent direct to users' messaging clients.
Deep URL analysis	Selectively block the results of a Google image search if the images found are from a domain that is configured to be blocked.
Search Engine Filtering	Filter, monitor and report upon search terms/strings used and force safe search on popular search engines.
Temporary bypass controls	Block page includes options to bypass the filter on a temporary basis
Configurable 'Site Blocked' page	'Site blocked' page can be customized to include a logo, message text, a reason for blocking, un-block buttons, IP address and username.
'Softblock' option	Instead of automatically blocking inappropriate content, users are issued warning messages about content and given options to either continue or cancel.
Stealth mode	Web pages are filtered and logged as normal, but are not blocked, allowing activity/policies to be monitored without affecting users (useful when testing a new installation).
Flexible request and content modification	Modify web page requests and content 'on the fly' to enable neutralization of malicious JavaScript and other web threats.

Networking Features	Benefit
Up to 20 interfaces (4 or 6 ports)	Allows segregation not only of servers & clients, but different types of client (wireless laptop users, servers, critical servers, guest workstations, different departments, etc).
Multiple external connections	Allows load balancing between a number of Internet connections.
Ethernet, DSL, (PPPoA, PPPoE and PPTP) and analogue modem support	Allows failover to 'lower tech' connections when the main connection fails.
Automatic failover to a standby appliance	Allows connectivity continuation in the event of hardware dropout.
Routing protocol support	Facilitates integration into existing network infrastructures.
VLAN trunking (802.1Q)	Allows creation of VLANs for easier network management.
Authentication Features	Benefit
Integrates with User Authentication systems	Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address (Supports Microsoft Active Directory®, Novell eDirectory, and other LDAP systems).
Multiple filter groups	Different filter policies can be allocated to up to 100 different groups of users. Particular users can also be configured not to be subject to any filtering at all.
Transparent proxy mode	System administration is simplified with support for NTLM authentication in transparent proxy mode; which avoids the need to configure proxy settings for each user computer.
Password-protected authentication	The use of NTLM with password verification provides seamless single sign-on without the need for users to log in or enter their Windows ID/password again.
Ident integration	Ident (Windows User Identification) can be enforced so that any user that has not been identified from Ident information (ie their PC is not running an Ident client) will be not be allowed to browse the web.
Email Security & Anti-Spam Optional Module	Benefit
SMTP Validity Checking	Checks for malformed email (usually either spam or designed to attack mail server/client vulnerabilities).
Grey Listing	Mail from unknown senders may be temporarily rejected. Genuine email servers (as opposed to zombies or botnets) usually resend after a short delay - if a second attempt is made, the sender is then automatically added to the list of known senders.
Remote Blackhole List (RBL)	The option to utilize RBL services (maintained databases of IP addresses that are acting as open mail relays for bulk spamming).
Sender Domain Spoofing Prevention	Rejects any incoming email that falsely uses an internal domain in the 'from' address.
Disclaimer Footers	Ability to add standardized disclaimers to the footer of outgoing emails. Different disclaimers can be used for different domains.
Attachment Removal	Allows dangerous or unwanted attachments to be discarded based on type (e.g. executable files, documents and multimedia files).
Content Analysis (Mailshell 3.0 Spam Content)	Examines the content of messages in detail, including address fields, subject, headers, SMTP envelope content, email format, design and layout, image layout, hyperlinks, contact information, language and origin.
Reputation Checking	Sender reputations are determined using comprehensive 'real-time' databases of IP addresses, domains and email addresses of known spammers. Bayesian analysis is used to combat attempts to hide sender identity.
Bulk Mail Detection	Identifies if a message or similar messages were sent in bulk by creating 'fingerprints' based on message elements that are tough for spammers to fake or change.
Phishing	Identifies special formatting used to evade spam filters and for phishing attacks and economical bulk mailings (including image-only messages, HTML obfuscation and manipulation using relays). Analysis of the message header includes time stamps and the SMTP envelope.
User-configurable Spam Treatment Controls	Users have the option to add email addresses to their own blacklists or whitelists and set automatic rules for changing subjects, replacing content or sending to a quarantine mailbox. Quarantines can be set up for individual email addresses with daily 'spam trapped' email reports sent to users so they can view and release emails.
Near Real-Time Updates	The software is updated every 5 minutes with the latest email fingerprints and detection rules.

VIPRE Anti-Malware Features	Benefit
Next Generation Anti-Malware	New codebase delivering high speed threat scanning using an advanced technology stack with low impact on CPU and memory.
Real-time behavioral analysis technology	Protection against known and unknown “zero-day” malware threats by using proprietary detection methods which include; traditional signature-based, behavioral analysis, heuristics and most importantly dynamic translation.
Certification	VB100 and Checkmark Certified with exceptional detection rates and fast updates.
MX-Virtualization™ (MX-V)	The fastest most adaptable Dynamic Translation technique for malware analysis which analyzes potential threats by observing their behavior in a safe virtual environment.
Genscan™ and Cobra™ heuristics	Dynamic pattern assessment to determine if a source is malware.
ThreatTrack™	Data feeds of the latest harmful URLs identifying malware hosts and phishing sites.
SteadyStream™	Real-time live threat data integration with continuous and compact updates at least once an hour.
Reporting & Logging Features	Benefit
Report templates	Users can create, customize and save their own report templates and utilize an extensive range of over 350 report templates including most visited domains, bandwidth utilization by user, commonly blocked search terms and the worst offending users (in terms of requesting pages that were blocked by Guardian). Report options include site-specific reports (e.g. YouTube top viewed videos) and IM reporting (time spent messaging and chat friends per user).
Drill down to a single user or IP	Reports include the user name and IP address of the user PC so AUP violators can be quickly identified. A drill-down facility allows data to be explored to a greater depth – e.g. from a list of blocked sites that users have attempted to access, drill-down to find out which users have been trying to access any particular site. It is possible to view the entire browsing history of a single user.
Automated reports	User-specific reports can be automatically time-scheduled to run on a daily or weekly basis. Reports can also be automatically saved or distributed to recipient lists via email.
AJAX real-time logs & traffic graphs	View web, email or IM activity instantaneously, with the option to filter by user name, IP address or web site.
Export into PDF, HTML, Excel, Crystal Reports®	Reports can be produced in a range of formats for ease of viewing (with pie charts/graphs) and to aid integration with existing systems.
Reports via domains or categories	Report on top domains, categories, page visits and offenders based on user, group and/or IP address.
User Portal	Provides selected users (or groups of users) with limited access for viewing reports/logs, controlling temporary bans and downloading SSL VPN clients.
Incident Alerts	Alert messages can be sent by both email and SMS text message to cell (mobile) phones for issues requiring immediate attention.
Hardware healthcare alerts	Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures) and network intrusions or violations.
Notes	<p>*Features with an asterisk are not included in the UTM-100 Series. For more information see the UTM feature comparison matrix on our website: www.smoothwall.net</p>