

Feature (Firewall/VPN)	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 Detection System (IDS)	Logs intrusion attempts 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 file transfers/downloads (P2P traffic, etc).
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).
Feature (Filtering)	Benefit
Dynamic Content Analysis™	Screens the content, context and construction of web pages in detail, accurately detecting and blocking all objectionable, inappropriate, hidden or malicious content (including anonymous and secure/SSL proxies).
SSL Interception	HTTPS/SSL encrypted traffic is intercepted and filtered using Dynamic Content Analysis and scanned for security vulnerabilities. Allows all unknown secure traffic to be decrypted and inspected, so inappropriate content (such as SSL proxies) can be effectively blocked.
Customizable URL Blocklists	Current and categorized URL blocklists (updated daily with the latest content from the IWF database) control access to a pre-defined list of undesirable websites. Blocklists can be customized and include a reverse-lookup option to block users attempting to access sites using IP addresses instead of domain names.
MIME, File extension, download size, advert, cookie & PICS blocking	Filtering policies can be set to detect and block PICS codes, file types, download sizes, adverts and cookies. PICS codes indicate the nature/severity of the website content and MIME type checking stops the downloading of viruses and malicious code from websites, as well as music and other copyright material.
Policy based controls	Different filtering policies can be set for different groups of users, in accordance with organization policy or the AUP.
Temporary 'Banned User' list	Ban users until a selected date or time and run 'banned user' reports.
Time and room based controls	Filtering can be set at different levels for different times of the day (enables filtering to be relaxed outside of core hours) and for different rooms or departments, defined by IP address or computer names.
Logging, Filtering and Censoring of Instant Messenger applications	Control and monitor the use of Instant Messaging applications such as MSN, Yahoo, AOL and ICQ. IM file transfers and attachments can be logged or blocked and selected words or phrases (including mis-spellings) can be censored and set to trigger alerts with responses sent direct to messaging clients (i.e. your message has been blocked/censored). Encrypted Instant messaging is also supported.
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.
Force SafeSearch	Enforce safe search usage on popular search engines, including image search.
Temporary bypass controls	Block page includes options to bypass the filter on a temporary basis.
Configurable 'Site Blocked' page	The 'site blocked' page can be customized to include a logo, message, reason for blocking and bypass controls (un-block buttons) alongside user details.
'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 actually blocked, allowing administrators to monitor web activity without affecting users. This feature is particularly useful when testing a new installation as it allows the filtering rules to be fine-tuned before 'going live'.
Flexible request and content modification	Modify web page requests and content 'on the fly' to neutralize malicious JavaScript.
Anti-Virus Scanning	Automatically scan web content for viruses, using either built-in ClamAV scanning, or offload to an external server via the ICAP protocol.
Default 'safe' configuration	Filters out a standard range of illegal and objectionable content that most organizations would want to block. Note: Guardian's default 'safe' configuration matches the requirements of CIPA and BECTA filtering tests.
Rate limiter & QoS by URL	The speed or rate at which the proxy server can download web content can be limited to ensure downloads don't use up too much of the available bandwidth. QoS can also be limited for specific URLs (e.g. YouTube). Direct Server Return (DSR) load balancing is supported.
Web proxy Cache	Reduce bandwidth utilization by storing and retrieving frequently accessed web pages from local disk storage.

Feature (Networking)	Benefit
Up to 20 interfaces (7 ports)	Allows segregation not only of servers & clients, but different client types (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 leased line fails
Automatic failover to a standby UTM appliance (in the event of hardware failure)	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 on all NICs, for applications like VoIP.
Feature (Authentication)	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.
Feature (Email Security)	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)	SmoothZap has 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).
Feature (Anti-Spam Add on Module)	Benefit
Content Analysis (Mailshell 3.0 Spam Content ¹)	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 UTM is updated every 5 minutes with the latest email fingerprints and detection rules.

¹Annual subscription payable

Feature (Anti-Virus)**Benefit**

Integrated Clam Anti-Virus Engine

Scans all web traffic, SMTP email and incoming POP3 email for viruses and other malware.

Free Automatic Anti-Virus Updates

Provides up-to-date protection against emerging security threats.

Feature (Reporting)**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 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.