

## Filtering Features

## 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 proxies).
SSL interception	Allows all unknown secure traffic to be decrypted and inspected (using Dynamic Content Analysis), so harmful HTTPS/SSL content (including SSL proxies) can be effectively blocked.
VIPRE Anti-Malware Engine (Note: subscription payable)	Uses heuristic, behavior and pattern-based technologies, alongside the fastest emulation technique available (MX-V™) which protects users from unidentified or new variants of malware.
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 & 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 control access to a pre-defined list of undesirable websites.
Internet Watch Foundation	Blocklists are updated daily with IWF datafeeds.
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 and run reports with lists of 'banned users' and the duration of their bans.
Manage MIME, file extension and download size	Filtering policies can be set to manage specific file types, and limit download sizes.
Block advertising and cookies	Advertising and cookies can be automatically blocked.
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 or phrases can be censored and set to trigger alerts with responses sent direct to users' messaging clients. Encrypted Instant Messaging is also supported.
Search engine filtering	Filter, monitor and report upon search terms 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 administrators to monitor activity without affecting users (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 enable neutralization of malicious JavaScript and other web threats.
Web proxy cache	Reduce bandwidth utilization by storing and retrieving frequently accessed web pages from local disk storage.
Default 'safe' configuration	Guardian can be installed with a default 'safe' configuration which filters out a standard range of illegal and objectionable content. Note: Guardian's default 'safe' configuration matches the requirements of CIPA and BECTA standards.

Authentication Features	Benefit
Integrates with User Authentication systems including, AD, Novell etc	Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address.
Multiple filter groups	Different filter policies can be allocated to up to 100 different groups of users. Particular users can also be configured to not 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 into Guardian or enter their ID/password again.
Reporting Features	Benefit
Built-in report templates	Users can create, customize and save their own report templates and utilize an extensive range (300+) of report templates. 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 (including time spent browsing) 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 activity instantaneously, with the option to filter by user name, IP address, web site, category or group.
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.
User portal	Selected users (or groups of users) can be given access to a separate Guardian interface specifically for viewing reports/logs, controlling temporary bans and downloading SSL VPN clients.
Reports on domains or categories	Report on top domains, categories, page visits and offenders based on user, group and/or IP address
Group/aggregate reports	Automatic data aggregation from multiple remote systems provides district wide reporting.
Incident alerts	Alert messages can be sent by both email and SMS text message to cell (mobile) phones for issues requiring immediate attention.
Operation Features	Benefit
Optional Bridge Mode (Transparent Inline Proxy)	'Drop in' deployment - allows the appliance to be deployed inline between a switch and a perimeter firewall for ease of installation and configuration.
Rate limiter by URL	The speed or rate at which the proxy server can download information from the Internet can be limited. Bandwidth use can also be limited for specific URLs.
Support for browser autoconfiguration files	Provides WPAD (Windows Proxy Auto-Detection) and PAC file support, for automatic configuration of proxy settings in client browsers.
Hardware healthcare alerts	Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures).