

FILTERING FEATURES

Dynamic Content Analysis™

'Who, What, When, Where' Policy Tools

SSL interception

Unified Policy Tools and Wizards

'Quick Block' and 'Quick Allow'

Advanced Categorization

'Soft-blocking' per content category

Flash filtering

Outbound (web post) monitoring & blocking

Customisable URL blocklists

Internet Watch Foundation

Whitelist mode

Temporary 'Banned User' list

Manage MIME, file extension and download size

Block advertising and cookies

Policy based controls

Logging, filtering and censoring of Instant Messenger applications

Search engine filtering

Temporary bypass controls

BENEFITS

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).

True 'who, what, when, where' filtering with flexible user, group, time and location based controls.

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 even in transparent proxy mode.

Unified, easy to use policy setting tools with policy and configuration wizards. With unlimited groups and 'per user' policies and the ability to combine policies with multi-group membership.

'Quick Block' and 'Quick Allow' buttons for fast one click fixes

Add-to-category functionality allows in-built categorisation to be adjusted with ease. Enhanced real-time categorisation - delivers higher accuracy, better reporting and fewer over-blocks

Delivering a better user browsing experience without compromising safety, security or control.

Screens actual SWF file code to accurately detect and block undesirable Flash content such as online games and video players.

Monitors and blocks text posted on the web (i.e. inappropriate blog / forum / Social Networking / Twitter posts) using a keyword analysis system.

Current, categorised and customisable URL blocklists control access to a pre-defined list of undesirable websites.

Blocklists are updated daily with IWF datafeeds.

Users can only access a customised list of 'allowed' sites.

Ban selected users until a selected date or time and run reports with lists of 'banned users' and the duration of their bans.

Filtering policies can be set to manage specific file types, and limit download sizes.

Advertising and cookies can be automatically blocked.

Different filtering policies can be created and set for different groups of users, in accordance with organisation policy or the AUP.

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.

Filter, monitor and report upon search terms used and force "safe search" on popular search engines.

Block page includes password protected options to bypass the filter on a temporary basis.

FILTERING FEATURES

SWURL Devolved Personal Block/Allow List Management

YouTube.com/education Channel Support

Configurable 'Site Blocked' page

'Softblock' option

Stealth mode

Flexible request and content modification

Web proxy cache

Default 'safe' configuration

Mobile Device Filtering

Guest Mobile Device Filtering

BENEFITS

SWURL allows specified users to manage their personal block/allow list via a portal - enabling miscategorised content to be accessed whilst being logged.

Allows access to youtube.com/education channel without removing restrictions on other YouTube content.

'Site blocked' page can be customised to include a logo, message text, a reason for blocking, un-block buttons, IP address and username.

Instead of automatically blocking inappropriate content, users are issued warning messages about content and given options to either continue or cancel.

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').

Modify web page requests and content 'on the fly' to enable neutralisation of malicious JavaScript and other web threats.

Reduce bandwidth utilisation by storing and retrieving frequently accessed web pages from local disk storage.

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.

Mobile Guardian allows many devices (iOS,OSX,Windows) to be actively filtered and controlled according to the organization's policies in or out of the home network. *Android will be supported during 2012.*

Guest devices can be accommodated on the network and filtered according to the organization's policies.

AUTHENTICATION FEATURES

Integrates with User Authentication systems including, AD, Novell etc

Multiple filter groups

Transparent proxy mode

Password-protected authentication

BENEFITS

Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address.

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.

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.

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.

OPERATION FEATURES

Optional Bridge Mode (Transparent Inline Proxy) SWG Appliance Only

Rate limiter by URL

Support for browser autoconfiguration files

Hardware healthcare alerts

BENEFITS

'Drop in' deployment - allows the appliance to be deployed inline between a switch and a perimeter firewall for ease of installation and configuration.

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.

Provides WPAD (Windows Proxy Auto-Detection) and PAC file support, for automatic configuration of proxy settings in client browsers.

Notifications about system resource issues (eg low disk space, high memory use, high CPU loads, UPS failures).

REPORTING FEATURES

Built-in report templates

Users can create, customise and save their own report templates and utilise 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.

BENEFITS

UK + INTERNATIONAL

Smoothwall Ltd
1 John Charles Way
Leeds LS12 6QA
United Kingdom

+44 (0)800 5 999 040 UK
+44 (0)870 1 999 500 International
sales@smoothwall.net
www.smoothwall.net

USA + CANADA

Smoothwall Inc.
6201 Fairview Road, Suite 320
Charlotte, NC 28210-4274
United States of America

1-800-959-3760 US + Canada
1-888-899-9164 Fax
sales@smoothwall.com
www.smoothwall.com