smoothwall®

03 | 2011

Product Datasheet

Unified Threat Management

FIREWALL FEATURES	BENEFITS
Perimeter Firewall	Block threats at the boundary - before 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, based on destination IP address as well as port, protocol, AD group and source IP address.
Port Grouping	Group ports into types (e.g. web, email, remote access) to simplify configuration and deployment.
Port-agile traffic blocking	Detects & blocks file transfers/downloads (P2P traffic such as KaZaa, BitTorrent, etc
Multiple rule sets	Increased flexibility with configuration options.
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.
Internal Firewall including DMZ, other zones & inter-zone	Segregate local networks into physically independent zones – useful for controlling inter-zone access & in the event of server compromise. (Also integrates with User Authentication systems)

VPN FEATURES	BENEFITS
Layer 2 Tunneling Protocol (L2TP)	Secure connections for remote workers.
IPSec	Compatible gateway for both site-to-site and laptop VPN connections.
SSL VPN	Simplified access from laptop VPN connections. Able to cross network filters where L2TP or IPSec might fail, such as hotel room wireless. Support for Internal SSL VPN also allows VPN connections to be made inside the network.
Data Compression - IPComp (RFC 2393)	To improve VPN throughput, supporting more VPN connections.
3DES data encryption (+ AES Rijndael, Twofish, Blowfish	Prevents eavesdroppers reading confi dential information & provides interoperability with other existing VPN products.
NAT Traversal (NAT-T) option	Seamless operation even when the peer gateway or client is behind a NAT router.
Activation/deactivation of individual VPN	Gives administrators full control over who is accessing the network.

NETWORKING FEATURES	BENEFITS
Up to 20 interfaces	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.
Auto 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.

VIPRE ANTI-MALWARE FEATURES	BENEFITS
VIPRE Anti-Malware Engine (Note: subscription	New codebase delivering high speed threat scanning using an advanced technology stack with low impact on CPU and memory.
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-Virtualisation™ (MX-V)	The fastest most adaptable Dynamic Translation technique for malware analysis which analyses 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.

WEB FILTERING FEATURES*	BENEFITS
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).
'Who, What, When, Where' Policy Tools	True 'who, what, when, where' filtering with flexible user, group, time and location based controls.
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 even in transparent proxy mode.
Unified Policy Tools and Wizards	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'	'Quick Block' and 'Quick Allow' buttons for fast one click fixes
Advanced Categorization	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
'Soft-blocking' per content category	Delivering a better user browsing experience with compromising safety, security or control.
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 &	Monitors and blocks text posted on the web (i.e. inappropriate blog / forum / Social Networking / Twitter posts) using a keyword analysis system.
Customisable URL blocklists	Current, categorised and customisable 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 customised 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 and be automatically blocked.
Policy based controls	Different filtering policies can be created and set for different groups of users, in accordance with organisation policy or the AUP.
Search engine filtering	Filter, monitor and report upon search terms used and force "safe search" on popular search engines.

Logging, filtering and censoring of Instant Messenger	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 reponses sent direct to users' messaging clients. Encrypted Instant Messaging is also supported.
Temporary bypass controls	Block page includes password protected options to bypass the filter on a temporary basis.
Configurable 'Site Blocked' page	'Site blocked' page can be customised 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	Modify web page requests and content 'on the fly' to enable neutralisation of malicious JavaScript and other web threats.
Web proxy cache	Reduce bandwidth utilisation 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.

EMAIL SECURITY & ANTI-SPAM OPTIONAL MODULE

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 utilise 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 standardised 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.

AUTHENTICATION FEATURES	BENEFITS
Authentication Features Integrates with User Authentication	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.

REPORTING & LOGGING FEATURES	BENEFITS
Report templates	Users can create, customise and save their own report templates and utilise an extensive range of over 350 report templates including most visited domains, bandwidth utilisation 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

* 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

UK + INTERNATIONAL

Smoothwall Ltd
1 John Charles
Way Leeds LS12
6QA United

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

PHILIPPINES

SAV25 Data Systems
7869 mckinley Street
Makati City
Philippines 1230

+ 632 893-2488
+ 632-984-6055
sales@sav25.com
www.sav25.com