smoothwall®
Web Filtering + Security

01 | 2012
Product Datasheet

Advanced Firewall

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 bridges	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)

NETWORKING FEATURES	BENEFITS
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 leased line fails.
Automatic failover to a standby Advanced Firewall system (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 NIC's, for applications like VoIP.

AUTHENTICATION FEATURES	BENEFITS
Integrates with User Authentication systems including Microsoft Active Directory®, Novell eDirectory, and other LDAP systems	Control access based on authenticated identity as opposed to assumed identity derived from a computer's IP address. Up to 100 groups can be used to define outgoing firewall, inter-zone bridging, VPN and web filter access policies against directory services.
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 the firewall or enter their Windows ID/password again.

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 and CAST encryption algorithms)	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 tunnels	Gives administrators full control over who is accessing the network.

PROXIES & SERVICES FEATURES	BENEFITS
Caching web proxy server	Reduces page display times & bandwidth utilisation.
Transparent SIP proxy	Enhances VoIP.
DHCP server with static address allocation facility	Use an on-board DHCP server or relay.
DNS proxy	Speeds up DNS resolutions.
NTP time server	Allows all servers & workstations on the network to set time from the firewall.
Logging, reporting and censoring of Instant Messaging applications	Control and monitor the use of Instant Messaging applications such as MSN, Yahoo, AOL and ICQ. File transfers/attachments can be logged or blocked and selected words or phrases can be censored and set to trigger alerts, with responses (e.g. your message has been censored/blocked). Encrypted Instant Messaging is also supported (e.g. Jabber/GoogleTalk)

REPORTING FEATURES	BENEFITS
SMS/email incident alerts	For immediate response to urgent incidents.
Editable report templates	Users can create, customise and save their own report templates and utilise an extensive range of standard reports. (20+ including firewall and IDS log analysis, server information, status of VPN tunnels, network usage, traffic & web cache) IM reports include time spent messaging and no. of chat friends per user.
Drill down to a single user or IP	A drill-down facility allows report data to be explored to a greater depth (e.g. per user or IP address) so AUP violators can be quickly identified.
Automatic scheduling & distribution of reports	Effortlessly produce and distribute regular reports.
Real time (AJAX) logging and monitoring of traffic	Activity can be monitored instantaneously using the real-time viewer.
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.

OPERATION FEATURES	BENEFITS
User Portal	Provides selected users (or groups of users) with limited access for viewing reports/logs and downloading SSL VPN clients.
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) and network intrusions or violations.
Default 'safe' configuration	Install with a default 'safe' configuration with egress rules and filter policies pre-set.
VMWare support	Full VMWare compatibility (including network drivers) so multiple instances of Advanced Firewall can be installed on 'virtual machines'.
Hardware and Software RAID	RAID1 mirrored support for SCSI, SAS, SATA or IDE disks.

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