

FIREWALL FEATURES

- Perimeter Firewall**
- Stateful Packet Inspection**
- Intrusion Prevention System (IPS)**
- Outbound (egress) filtering rules**
- Port Grouping**
- Port-agile traffic blocking**
- Multiple rule sets**
- Dynamic NAT (DNAT) and Static NAT (SNAT) operation**
- Internal Firewall including DMZ, other zones & inter-zone**

BENEFITS

- Block threats at the boundary - before they enter your network.
- Keeps out invalid traffic by ensuring all packets are part of a legitimate sequence.
- Monitors and reacts to malicious activity and gives, through reporting, an overall view of the attacks occurring to your systems.
- 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.
- Group ports into types (e.g. web, email, remote access) to simplify configuration and deployment.
- Detects & blocks file transfers/downloads (P2P traffic such as KaZaa, BitTorrent, etc)
- Increased flexibility with configuration options.
- Allowing a range of Internet accessible servers to be positioned on the internal network with multiple IPs supported.
- 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

- Up to 20 interfaces**
- Multiple external connections**
- Ethernet, DSL, (PPPoA, PPPoE and PPTP) and analogue modem support**
- Automatic failover to a standby Advanced Firewall system (in the event of hardware)**
- Routing protocol support**
- VLAN trunking (802.1Q)**

BENEFITS

- Allows segregation not only of servers & clients, but different types of client (wireless laptop users, servers, critical servers, guest workstations, different departments, etc)
- Allows load balancing between a number of Internet connections.
- Allows failover to 'lower tech' connections when the main leased line fails.
- Allows connectivity continuation in the event of hardware dropout.
- Facilitates integration into existing network infrastructures.
- Allows creation of VLANs on all NIC's, for applications like VoIP.

AUTHENTICATION FEATURES

- Integrates with User Authentication systems including Microsoft Active Directory®, Novell eDirectory, and other LDAP systems**
- 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. Up to 100 groups can be used to define outgoing firewall, inter-zone bridging, VPN and web filter access policies against directory services.
- 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 the firewall or enter their Windows ID/password again.

VPN FEATURES

Layer 2 Tunneling Protocol (L2TP)

IPSec

SSL VPN

Data Compression - IPComp (RFC 2393)
connections.

3DES data encryption
(+ AES Rijndael, Twofish, Blowfish)

NAT Traversal (NAT-T) option

**Activation/deactivation
of individual VPN**

BENEFITS

Secure connections for remote workers.

Compatible gateway for both site-to-site and laptop VPN connections.

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.

To improve VPN throughput, supporting more VPN

Prevents eavesdroppers reading confidential information & provides interoperability with other existing VPN products.

Seamless operation even when the peer gateway or client is behind a NAT router.

Gives administrators full control over who is accessing the network.

PROXIES & SERVICES FEATURES

Caching web proxy server

Transparent SIP proxy

**DHCP server with static address
allocation facility**

DNS proxy

NTP time server

**Logging, reporting and censoring
of Instant Messaging**

BENEFITS

Reduces page display times & bandwidth utilisation.

Enhances VoIP.

Use an on-board DHCP server or relay.

Speeds up DNS resolutions.

Allows all servers & workstations on the network to set time from the firewall.

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.

REPORTING FEATURES

SMS/email incident alerts

Editable report templates

Drill down to a single user or IP

**Automatic scheduling
& distribution of reports**

**Real time (AJAX) logging
and monitoring of traffic**

**Export into PDF, HTML,
Excel, Crystal Reports®**

BENEFITS

For immediate response to urgent incidents.

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.

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.

Effortlessly produce and distribute regular reports.

Activity can be monitored instantaneously using the real-time viewer.

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

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.

BENEFITS

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