

# Firewall Feature Comparison Chart



January 17<sup>th</sup>, 2007

Feature Description	Advanced Firewall 2	Corporate Firewall 5	Express 2	Notes
<b>Firewall:</b>				
Stateful Inspection	Yes	Yes	Yes	
Local IP Addresses	Unlimited	Unlimited	Unlimited	F1
Users Supported	250 to 5000	n/a	n/a	F1
Dynamic Network Address Translation	Yes	Yes	Yes	
Static Network Address Translation	Yes	SmoothHost	No	F2
Outgoing (Egress) Traffic Control	Yes	Yes	No	F3
Support multiple public IP addresses	Yes	SmoothHost	No	F4
Port Forward from public IP address to DMZ/local IP	Yes	Yes	No	
"Round Robin" Port Forward to multiple DMZ servers	Yes	No	No	F5
Detection and blocking of port agile Peer to Peer traffic	Yes	Yes	No	F6
Administrator maintained IP Block list	Yes	Yes	No	
Internal firewall	Yes	No	No	F7, A6
Traffic Blocking includes drop and reject options for both source and destination addresses	Yes	Yes	No	
<b>Networking:</b>				
Total Network Interfaces	4 Standard, Maximum 20	3 Active + 1 Failover	3	N1
External Network (Internet) Interfaces	1 to 19 (of total)	1	1	N2
Internal Network Zones (Local Networks and DMZs)	1 to 19 (of total)	1 or 2 (of total)	1 Local + 1 DMZ	N3
Ethernet	Yes	Yes	Yes	
PPP connections (ISDN, ADSL and analog modem)	Yes	Yes	Yes	N4
PPPoA ADSL support	Yes	Yes	Yes	
PPPoE ADSL support	Yes	Yes	Yes	
PPTP ADSL support	Yes	Yes	No	
Load balancing between multiple external network interfaces	Yes	No	No	N5
Split traffic between multiple external network interfaces	Yes	No	No	N5
Split external traffic based on source or port	Yes	No	No	N5
Fail-over from one external interface to another	Automatic	Automatic	No	N6
Routing protocol support (RIP)	Yes	No	No	
Configure static routes	Yes	Yes	No	
VLAN Trunking (802.1Q) support	Yes	No	No	N7
Naming of Network Interfaces	Yes	Yes	No	
Multiple local network subnets	Yes	Yes	No	
Bind multiple IP addresses to a Green NIC	Yes	Yes	No	
Red interface MAC address spoofing	Yes	Yes	No	N8
Configurable Maximum Transmission Unit (MTU) and TCP transmit/receive window sizes	Yes	Yes	No	
Automatic Hardware Failover (HA)	Yes	No	No	N9
Inbound Load Balancing	Yes	No	No	N10
<b>Proxies and Application Helpers:</b>				
Web Proxy (Transparent and Non-Transparent Mode)	Yes	Yes	Yes	P1
GUI configuration of Web Proxy Server	Yes	Yes	No	P2
SMTP (Email) Relay / Proxy	SmoothZap	SmoothZap	No	P3
POP3 (Email) Transparent Proxy	SmoothZap	SmoothZap	No	P4
SIP (VoIP) Registering Proxy	Yes	Yes	No	P5
Transparent SIP (VoIP) Proxy	Yes	Yes	No	P6
H323 (VoIP) Application Helper	Yes	Yes	No	
PPTP Helper (for pass-through and forwarding)	Yes	Yes	No	
DNS Proxy Server	Yes	Yes	Yes	

<b>Hardware:</b>				
Multi Processor support (SMP)	Yes	No	No	
Hardware RAID (SCSI or SATA)	Yes	No	No	H1
Software RAID 1 (Disk Mirror) (SCSI, SATA or IDE)	Yes	Yes	No	H2
SCSI (Non RAID) Disk	Yes	Yes	No	H3
SATA Disk	Yes	Yes	Partial	H4
IDE Disk	Yes	Yes	Yes	
IDE DMA support	Yes	Yes	No	
IDE/SCSI CDROM support	Yes	Yes	Yes	
10/100/1000 (Gigabit) Ethernet card	Yes	Yes	Yes	H5
Multi-port Ethernet card	Yes	Yes	Yes	H6
Full VMWare support including network drivers	Yes	Yes	No	
USB ADSL modems and PCI ADSL modem cards	Yes	Yes	Yes	H7
ISDN cards and terminal adapters	Yes	Yes	Yes	H8
Analog modems	Yes	Yes	Yes	H9
Compact Flash support	Yes	Yes	No	H10
1 Gigabyte plus memory support	Yes	No	No	
USB keyboard support	Yes	Yes	No	
Serial Console	Yes	Yes	No	
Display ADSL modem signal strength information	Yes	Yes	No	H11
Un-interruptible Power Supply support	Yes	Yes	No	H12
UPS Network Slave Mode	Yes	Yes	No	H12
<b>Installation / Maintenance:</b>				
New streamlined / simplified installer with basic and advanced modes	Yes	Yes	No	IN1
Includes security hardened Linux operating system	Yes	Yes	Yes	IN2
SmoothWall and Linux security updates	Free	Free	Free	IN3
Installation from CDROM	Yes	Yes	Yes	
Installation from network server	Yes	Yes	Yes	
Installation from a USB CD/DVD Device	Yes	Yes	No	
Configuration backup to hard disk file/floppy and restore	Yes	Yes	No	
Backup/restore configuration from USB device	Yes	Yes	No	
Automatic configuration backup (time of day)	Yes	Yes	No	
Backup to multiple remote targets	Yes	Yes	No	
Partial configuration restore	Yes	Yes	No	IN4
Install new device drivers from floppy disk/CDROM	Yes	Yes	No	
Automatic download of new updates	Yes	Yes	No	IN5
Bulk application of updates from CD at installation time	Yes	Yes	n/a	IN6
Automatic installation of any modules present on the firewall installation CD	Yes	Yes	n/a	IN7
Ethernet cable status reporting	Yes	Yes	No	IN8
Un-install modules	Yes	Yes	n/a	
Pre-installed software	Yes	Yes	n/a	IN9
<b>Configuration:</b>				
Configured via a web browser GUI	Yes	Yes	Yes	
AJAX Enhanced GUI	Yes	Yes	No	
Network interfaces (IP Address) configured via Web GUI	Yes	Yes	No	
Restrict configuration access to specified public IP addresses	Yes	Yes	Yes	
Restrict config access to specified local IP addresses	Yes	Yes	No	
Administration users with limited access (eg log viewers, VPN, Guardian web content filtering)	Yes	Yes	No	
Drop down lists of common IP services/ports	Yes	Yes	No	
On-line Help appears in a separate pop-up window	Yes	Yes	Yes	
GUI Home page displays configurable information on the system status, VPN, firewall reports, traffic statistics etc.	Yes	Yes	No	C1
All rule lists and log files can be sorted by any column	Yes	Yes	No	C2
Validation of configuration parameters as they are typed	Yes	Yes	No	
Infrequently used options exposed by "Advanced" button	Yes	Yes	No	
Tooltips	Yes	Yes	No	
Config replication between master and slave systems	Yes	Yes	No	C3

<b>Authentication:</b>				
Microsoft Active Directory (LDAP) User Authentication	Yes	No	No	A1
OpenLDAP User Authentication	Yes	No	No	A2
Novell eDirectory (NDS) User Authentication	Yes	No	No	
Local User Authentication Database	Yes	Yes	No	A3
RADIUS Authentication	Yes	No	No	
Authentication via Ident client for Microsoft Windows	Yes	Yes	No	A4
SSL Login page (transparent mode user authentication)	Yes	Yes	No	A5
Microsoft NTLM User Authentication	Yes	Yes	No	
SmoothGuardian web access can be controlled by User/Group Name	Yes	Yes	n/a	
SmoothGuardian web access can be controlled by IP/IP Address Range/Network Address	Yes	Yes	n/a	
User Internet access controlled by User/Group Name as well as IP Address/IP Address Range/Network Address	Yes	No	n/a	
Inter-zone access controlled by user authentication	Yes	No	n/a	A6
VPN user access controlled by user authentication	Yes	No	n/a	A7
Multiple Admin/Configuration Users	Yes	Yes	No	A8
Login page with configurable login messages and log-out facility	Yes	Yes	No	
<b>Intrusion Detection:</b>				
Intrusion Detection System	Yes	Yes	Yes	
Intrusion Alert Messages by email or SMS text message	Yes	Yes	No	IDS1
Categorization of Intrusion Detection System signatures	Yes	Yes	No	
IDS signatures downloadable from SmoothWall	Yes	Yes	No	
<b>Virtual Private Network (VPN):</b>				
Site-to-site IPsec VPN	Yes	Yes	Yes	V1
Configure which Internet connection each IPsec tunnel should use	Yes	No	No	
Mobile (Road Warrior) or home user IPsec VPN	Yes	Add Module	No	V2
Mobile (Road Warrior) or home user L2TP VPN	Yes	Add Module	No	V3
VPN Tunnels	20 (Included) to 500	1 (included) to 100	See note	V4
AES Encryption	Yes	Yes	No	
3DES Encryption	Yes	Yes	Yes	
x509 Certificate Authentication	Yes	Yes	No	
Certificate Authority included	Yes	Yes	No	V5
Pre-Shared Key (PSK/Shared Secret) Authentication	Yes	Yes	Yes	
NAT Traversal (NAT-T)	Yes	Yes	No	V6
VPN secure local (wireless) connection	Yes	No	No	V7
Logging of Road Warrior VPN connections (with option to send alert messages)	Yes	Yes	No	V8
PPTP forwarding and pass-through	Yes	Yes	No	
<b>Logging and Reporting:</b>				
Disk logging of all firewall/IDS events, web traffic etc.	Yes	Yes	Yes	
Configure/enable individual logging functions	Yes	Yes	No	L1
Configure how long log files are retained (days/weeks)	Yes	Yes	No	L1
Forced log file rotation in the event of low free disk space	Yes	Yes	No	
Log files on RAM disk	Yes	Yes	No	
Log filtering (eg by Source IP/Port, Destination IP/Port)	Yes	Yes	No	
Google-like paginated log file viewers	Yes	Yes	No	
All rule lists and log files can be sorted by any column	Yes	Yes	No	L2
Scheduled firewall log analysis, IDS analysis, traffic reporting	Yes	Yes	No	L3
Reports produced in text, HTML, CSV format etc.	Yes	Yes	No	
Export Log Files and Reports in Excel® Format	Yes	Yes	No	
Outgoing (egress) traffic reporting/analysis	Yes	Yes	No	L4
Real-time AJAX traffic graphs and log viewers	Yes	Yes	No	
Selectively log blocked traffic	Yes	Yes	No	
Network analysis tool for displaying network traffic info	Yes	Yes	No	

SNMP Support	Yes	No	No	L5
Remote Syslog support	Yes	Yes	No	
Service availability checking (including systems behind the firewall)	Yes	Yes	No	
Physical hardware monitoring (eg disk status)	Yes	Yes	No	
<b>DHCP Server:</b>				
DHCP server support for local (Green) networks	Multiple	1 or 2	Single	
DHCP server support for DMZ	Multiple DMZ	Single DMZ	No	
View DHCP leases granted	Yes	Yes	No	
Display list of MAC addresses on local/DMZ networks	Yes	Yes	No	
DHCP Relay	Yes	Yes	No	
NTP, network boot, TFTP and automatic web proxy detection options	Yes	Yes	No	
<b>Miscellaneous:</b>				
NTP service for computers on local networks/DMZ	Yes	Yes	Yes	
Modularization of core services/components (eg Web Proxy server, DHCP server)	Yes	Yes	No	M1
Timed/delayed shutdown/reboot	Yes	Yes	No	
Inbuilt ClamAV anti-virus	Yes	Yes	No	M2
Network Doctor diagnostic tool	Yes	Yes	No	
<b>Available Modules</b>				
Web Security/Content Filtering (SmoothGuardian)	Yes	Yes	No	
Bandwidth Management/QoS (SmoothTraffic)	Yes	Yes	No	
VPN Gateway (SmoothTunnel)	Integrated	Integrated	No	V1-8
Internet Access Control/Outbound Rules (SmoothRule)	Integrated	Integrated	No	F3
Incident Alerting and Reporting (SmoothMonitor)	Integrated	Integrated	No	L3
Support for Multiple DMZ Servers (SmoothHost)	Integrated	Yes	No	F4
Email Security (Anti-spam/virus and relay) (SmoothZap)	Yes	Yes	No	
<b>System Requirements:</b>				
Processor	PIII 500 MHz	PIII 200 MHz	Pentium	S1
Memory	128 MBytes	128 MBytes	64 MBytes	S2
Hard Disk	4 GBytes	4 GBytes	1 GByte	S3
Flash Memory (alternative to Hard Disk)	256 MBytes	256 MBytes	n/a	S3
<b>Commercial Support:</b>				
Technical support by Phone and Email from SmoothWall	Yes	Yes	No	
Global support from SmoothWall Reseller Partners	Yes	Yes	No	
Technical Training Courses from SmoothWall Ltd.	Yes	Yes	No	

## **Firewall:**

- F1 Advanced Firewall supports 250 authenticated users as standard, expandable to 5000 users with the addition of user license packs. There is no restriction on the number of IP addresses supported, however it is recommended that Corporate Firewall should be limited to a maximum of 250 users.
- F2 Static Network Address Translation (SNAT) (Source Mapping) is an integral component of Advanced Firewall. For Corporate Firewall the SmoothHost add-on module introduces this facility.
- F3 Outbound (egress) traffic control (user access to Internet services) is an integral component of Advanced Firewall, and of Corporate Firewall from V5 onwards.
- F4 Support for multiple public aliased IP address is a standard feature of Advanced Firewall. For Corporate Firewall the SmoothHost add-on module introduces this facility.
- F5 For load balancing, where for example high traffic applications are served by multiple web servers responding to page requests from a single public IP address.
- F6 Egress Filtering incorporates traffic inspection technology to can detect and block Peer to Peer (P2P) traffic such as KaZaA, Bit Torrent and eDonkey, regardless of which port the file sharing software attempts to use.
- F7 Internal firewall segregation of local networks into physically independent zones. Inter zone access (bridging) controlled by user authentication (eg only system administrators allowed admin access to DMZ servers)

## **Networking:**

- N1 Advanced firewall will support 4 NICs as standard, license expandable to 20 NICs and VLAN trunk (802.1Q) interfaces by license. At least one NIC is required for Corporate Firewall's Local Protected Network (Green) network interface if used with a PPP/Dial-Up connection, a minimum of 2 NICs with an Ethernet connection to the External Network (Internet).
- N2 Corporate Firewall and SmoothWall Express support a single active External Network (Internet) connection. Corporate Firewall allows the 3 NICs can be configured as: a single External Internet (Red) interface plus either: one each of Local Protected Network (Green) and DMZ (Orange) or two Local Protected Network (ie no DMZ) or two DMZs (no Local Protected Network). SmoothWall Express supports a single External Internet (Red) interface, a DMZ (Orange) and a Local Protected Network (Green). Advanced Firewall can support multiple active External Network connections as any NIC can be designated as External (Red), Local Protected (Green) or DMZ (Orange).
- N3 Multiple internal network zones allow the physical separation of different user groups, internal servers, publicly accessible servers etc. Inter-zone access rules permit strictly limited access from one zone to another (by server/IP address, port/service etc.).
- N4 Advanced Firewall, Corporate Firewall and SmoothWall Express can all support a single active PPP (dial-up) connection (eg ISDN, ADSL modem or analog modem). Multiple connection profiles (eg ISP details) can be stored.
- N5 Outgoing traffic can be load balanced between multiple external network interfaces, with a weighting facility to control the proportion of the total traffic being routed via each interface in the load balancing pool. Both NAT and web proxy traffic can independently be subject to load balancing. Specific IP addresses, such as mail-servers can be excluded from being load balanced. Alternatively, traffic can be split between multiple external (Red) network interfaces according to the IP address, IP address range or network address of the originating computer. Traffic may also be split according to port (protocol) in order to separate web and email traffic, for example.
- N6 If an Internet connection should fail then Advanced Firewall can be configured to automatically route all traffic from the failed interface to another. There is no limit to how many interfaces can be set in the failure cascade path, nor is there any limitation on the type of interface that can be used (Ethernet, ADSL modem, ISDN or analog modem).
- N7 802.1Q VLAN trunking support allowing communication with VLAN capable switches and the routing of traffic between VLANs.
- N8 For easier support of cable modems which will typically only communicate with the MAC address from which the modem or Internet connection was initially configured.
- N9 Advanced Firewall can be used in an Active/Passive High Availability (HA) configuration with fully automatic failover should one appliance fail.
- N10 Inbound traffic may be load-balanced over two or more Internet connections for increased bandwidth availability and resilience (in the event of an Internet connection failure).

## **Proxies and Application Helpers:**

- P1 Squid caching web proxy server (reduces page display times and Internet bandwidth utilization).
- P2 Configuration options include: cache size, max object size, logging options and domains not to be cached.
- P3 Reconstructs and relays incoming email to a protected mail server located within a local network zone or DMZ, with support for an unlimited number of domains. Transparent relay of outgoing SMTP email.

- P4 Transparent POP3 proxy ensures that all POP3 email, whether company or personal email, is subject to anti-virus and anti-spam controls without any configuration changes to users' email client software.
- P5 SIP registering proxy for inbound connections to SIP phones and softphones (PC clients).
- P6 Transparent SIP proxy and gateway for the protection of VoIP telephone systems, supporting the use of a remote SIP proxy at an Internet Telephone Service Provider (ITSP).

#### **Hardware:**

See the Hardware Compatibility Guide: <http://www.smoothwall.net/support/hcg> for full information on the hardware supported by SmoothWall Security Software.

- H1 Supported RAID controllers will include Compaq, Dell PERC and DAC960.
- H2 Software RAID Software RAID 1 (Mirroring) using two IDE, SATA or SCSI disks which do not have to be of identical size. The firewall will remain operational in the event of a single disk failure. Automatic mirror rebuild.
- H3 SCSI controllers from Adaptec, Future Domain, Sym Bios, Initio, Advansys and BusLogic are supported.
- H4 SmoothWall Express 2 supports a limited set of SATA disk controllers. Advanced Firewall and Corporate Firewall support all common SATA controllers.
- H5 Gigabit Ethernet cards from Intel, 3Com, Broadcom and other manufacturers.
- H6 Multi-Port NIC support includes Intel quad and dual port cards, 3Com dual port cards and the DLink DE580 4 port card.
- H7 Over 30 types of USB ADSL modems are supported, along with Ethernet connected ADSL modems and the BeWAN PCI ADSL card modem.
- H8 Drivers for numerous PCI ISDN cards are included, together with support for USB ISDN and RS232 connected ISDN Terminal Adapters.
- H9 Hayes compatible RS232 connected analog modems and several ISA card modems are supported.
- H10 Compact Flash can be used as an alternative to hard disk for appliance applications. Minimum capacity is 256 MByte with 512 MByte recommended. The flash memory must present itself as an IDE device. Logs will be stored in a non-persistent (volatile) RAM disk, thus the use of Syslog for off-box log recording is recommended.
- H11 Bewan PCI ADSL modem.
- H12 Supports APC models. Advanced Firewall and Corporate Firewall can support UPS slave mode operation, where up to 5 systems (eg Advanced Firewall, Corporate Firewall, Corporate Guardian, Unix/Microsoft Windows system running apcupsd software) on the network can share the same UPS.

#### **Installation / Maintenance:**

- IN1 Advanced mode installation provides full set of Setup configuration options whereas Basic mode installation applies sensible default values to reduce the number of configuration questions presented during installation.
- IN2 SmoothWall Security Solutions are based on a cut-down security hardened version of the Linux operating system, where all unnecessary components have been removed from the operating system, reducing disk and memory utilization, improving security and performance.
- IN3 Security updates and bug fixes are supplied free of charge for all supported SmoothWall products.
- IN4 To be able to select which rules/configuration information to restore from a SmoothWall Configuration Backup (allowing specific rules, such as Port Forward rules, to be copied between systems).
- IN5 Option to automatically download and store any new updates on the firewall, which can then be applied at a convenient time by administrator command.
- IN6 All updates (patches) present on an installation CD will automatically be applied.
- IN7 Any modules present on the same CD as the firewall software will be automatically installed (single disk installation).
- IN8 MAC address of each Network Interface Card (NIC) displayed. Network cable status (present/not present) displayed to help identify a particular NIC when multiple NICs of the same type are installed.
- IN9 SmoothWall and its authorized Resellers can supply pre-installed versions of Advanced Firewall and Corporate Firewall, providing pre-configured installations.

#### **Configuration**

- C1 Configuration options allow the GUI Home (Control) page to display a variety of information, including alert messages, system status, VPN status, traffic statistics, firewall reports and update/blocklist status.
- C2 All rule lists and log files can be sorted on any column (eg IP address, source port etc.).
- C3 Master to slave configuration replication can be to automatically propagate configuration changes from say a head office system to remote branch office systems.

### **Authentication:**

- A1 Integrated Kerberos user authentication system to work with LDAP authentication systems such as Microsoft Windows 2000® and Microsoft Windows 2003® Server using Active Directory.
- A2 Support for the common InetOrgPerson (RFC2798) schema.
- A3 Corporate Firewall, in conjunction with the SmoothGuardian Web Content Filtering add-on module supports a user authentication database maintained on the SmoothWall firewall. This authentication system can only be used by the SmoothGuardian module to control web access. With Advanced Firewall, this authentication database can also be used to control users' access to Internet services (outbound/egress rules) and inter-zone access.
- A4 An Ident client for Microsoft Windows™ operating systems can be used to identify the computer user to the SmoothWall system.
- A5 The SSL Login page automatically senses from the users' browsers if it should display in English, German, Italian, Spanish, Danish, Dutch, French or Swedish.
- A6 Multiple internal network zones allow the physical separation of different user groups, internal servers, publicly accessible servers etc. Inter-zone access rules permit strictly limited access from one zone to another (by server/IP address, port/service etc.). User authentication can be used to control which access control policies (rule-sets) are applied to a user session.
- A7 Access for VPN users to internal servers and services can be controlled by user authentication, ie determines the policies (rule-sets) are applied to that VPN session.
- A8 Multiple users with configurable access rights (eg reporting only, network configuration etc.)

### **Intrusion Detection:**

- IDS1 Email and SMS text message alerting is an integrated into SmoothWall's commercial software. Alerts are generated based on intelligent monitoring of hardware, user and network activity, whilst reports are scheduled for regular delivery.

### **Virtual Private Networking (VPN):**

- V1 X509 certificate authentication is recommended or Pre-Shared Key (PSK)/Shared Secret authentication can be used. SmoothWall Express supports site-to-site VPN tunnels using Pre-Shared Key (PSK)/Shared Secret authentication.
- V2 IPSec VPN connectivity for single computers (mobile/laptop/home user/Road Warrior users) is an integral component of both Advanced Firewall and Corporate Firewall.
- V3 Layer 2 Tunneling Protocol (L2TP) VPN connectivity for single computers (mobile/laptop/home user/Road Warrior users) is an integral component of both Advanced Firewall and Corporate Firewall.
- V4 Advanced Firewall supports 20 VPN tunnels as standard (any combination of IPSec site-to-site, IPSec Road Warrior or L2TP Road Warrior tunnels). This can be expanded to a maximum of 500 tunnels by the addition of VPN license packs. Corporate Firewall supports 1 tunnel as standard - it is recommended that the VPN tunnel count should not exceed 100. The lack of individual tunnel management facilities in SmoothWall Express makes it impractical to establish and control more than a few VPN tunnels.
- V5 Advanced Firewall and Corporate Firewall both include a Certificate Authority (CA) for the creation and issue of self-signed x509 certificates. Alternatively an external Certificate Authority, such as Microsoft Windows 2000/2003 Server may be used, or an external certificate provider such as Verisign or Thawte.
- V6 NAT Traversal (NAT-T) mode for IPSec VPN connections is supported as standard.
- V7 Either L2TP or IPSec VPN can be used for local as well as remote (Internet) VPN connections with Advanced Firewall. This is principally used for Wireless (WiFi) access, providing secure L2TP connections with the user PC authenticated using an x509 certificate and the data encrypted using the 3DES encryption algorithm. IPSec internal subnet routing can also be configured.
- V8 The Firewall will log each connection and disconnection by mobile/laptop/home user/Road Warrior VPN users, with option to display an alert message on the GUI Home (Control) page or send Alert message by email or SMS text message.

### **Logging and Reporting:**

- L1 To reduce disk space utilization for non hard-disk operation (eg flash memory).
- L2 All log files and rule lists can be sorted on any column (eg IP address, port, time etc.)
- L3 Advanced Firewall and Corporate Firewall both include scheduled reporting, which is available for most reports and integrates with all add-on modules.
- L4 Advanced Firewall and Corporate Firewall provide more detailed traffic statistics than SmoothWall Express, with the option to generate an alert message reports if the current inbound or outbound traffic exceeds a configurable threshold. There is also a volume threshold where an alert can be generated if the total traffic volume exceeds a configurable limit for a daily/weekly/monthly limit.
- L5 Query an Advanced Firewall system to report management information, including disk utilization and traffic information.

**Miscellaneous:**

- M1 Modularization of many components/services, such as the DHCP server and the Web Proxy, allows them to be removed as desired. This allows the system to be customized and the memory/system requirements reduced if desired. The required modules can be configured at install time, thus the system can be tailored to the target hardware.
- M2 The ClamAV anti-virus engine supports the SmoothGuardian (web security/content filtering) and SmoothZap (email security/anti-spam) modules. Automatic updates to virus signatures.

**System Requirements:**

- S1 For Advanced Firewall the minimum recommended processor is a Pentium III 500 MHz (2 GHz+ recommended). For Corporate Firewall any Intel Pentium compatible processor of 200 MHz or greater, with 500 MHz recommended. Compatible processors from AMD and VIA are supported.
- S2 For Advanced Firewall and Corporate Firewall the minimum recommended memory is 128 Mbytes DDR or similar fast RAM. For SmoothWall Express minimum memory is 64 Mbytes with 96 Mbytes recommended. For Advanced Firewall and Corporate Firewall the maximum useable memory is 4 GBytes; for SmoothWall Express the maximum useable memory is 950 MBytes. More RAM memory is beneficial for web proxy cache performance and is necessary for operation of the SmoothGuardian web content filtering module.
- S3 For Advanced Firewall and Corporate Firewall the minimum recommended hard disk capacity is 4 GBytes. Alternatively Advanced Firewall and Corporate Firewall can utilize compact flash memory instead of a hard disk, when 256 Mbytes flash memory is the minimum recommended figure. The compact flash must appear as an IDE device, with logging to non-persistent (volatile) RAM disk.

For the latest information and prices for currently available products please see our web site:

[www.smoothwall.net](http://www.smoothwall.net).