

Feature (Firewall)	Benefit
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 Detection System (IDS)	Logs intrusion attempts 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.
Feature (Networking)	Benefit
3x interfaces	Allows segregation not only of servers & clients, but different types of client (wireless laptop users, servers, critical servers, guest workstations, different departments, etc).
Ethernet, DSL, (PPPoA, PPPoE and PPTP) and analogue modem support	Allows failover to 'lower tech' connections when the main leased line fails.
VLAN trunking (802.1Q)	Allows creation of VLANs on all NICs, for applications like VoIP.
Feature (VPN)	Benefit
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 confidential information & provides interoperability with other existing VPN products.
NAT Traversal (NAT-T) option	Seamless operation even when the peer gateway/client is behind a NAT router.
Activate/deactivate individual VPN tunnels	Gives administrators full control over who is accessing the network.
Feature (Proxies & Services)	Benefit
Caching web proxy server	Reduces page display times & bandwidth utilization.
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 sent direct to IM clients (e.g. your message was censored/blocked). Encrypted Instant Messaging (e.g. Jabber/GoogleTalk) is also supported.

Feature (Reporting)	Benefit
SMS/email incident alerts	For immediate response to urgent incidents.
Editable report templates	Users can create, customize and save their own report templates and utilize 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.

Feature (Operation)	Benefit
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.