The SonicWALL PRO 5060 is a powerful, multi-service gigabit network security platform that protects users and critical network resources from the dynamic, sophisticated threats that put today’s corporate networks at risk.

The PRO 5060 integrates high-speed gateway anti-virus, anti-spyware, intrusion prevention, secure wireless LAN features, deep packet inspection firewall and IPSec VPN into a single, easy to deploy and manage solution. Available in both 10/100/1000 copper and copper/fiber interface versions, the PRO 5060 incorporates a wide array of networking and security features, making it the ideal solution for a multitude of applications.

Features and Benefits

- **Powerful deep packet inspection firewall** protects against malicious application layer attacks originating from either internal or external sources.

- **Integrated gateway anti-virus, anti-spyware and intrusion prevention** secures the network against a comprehensive array of dynamic threats including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits and other malicious code.

- **802.1q VLAN support** using virtual interfaces with VLAN ID tag assignments provides many of the same features as physical interfaces, including zone assignment, DHCP Server, and NAT and Access Rule controls.

- **Stand-alone, in-line gateway anti-virus, anti-spyware and intrusion prevention** appliance for legacy firewall deployments.

- **Secure wireless LAN services** enable the appliance to function as a secure wireless switch and controller that automatically detects and configures SonicPoints™, SonicWALL wireless access points, as they are added to the network while simultaneously enforcing security policies on all wired and wireless traffic.

- **Real-time blacklist spam filtering** provides the ability to use DNS to query Real-time Black List (RBL) services that track well-known spam and open-relay SMTP servers and to deny SMTP connections from servers that appear on the lists.

- **Onboard Quality of Service (QoS) features** use industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators to provide powerful and flexible bandwidth management that is vital for Voice over IP (VoIP), multimedia content and business-critical applications.

- **2.4 Gbps stateful packet inspection firewall** provides high-performance L2-4 protection.

- **Standards-based Voice over IP (VoIP) capabilities** provide the highest levels of security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.

- **Advanced routing services** provide full support for OSPF (Open Shortest Path First) and RIP (Router Information Protocol) dynamic routing protocols to ensure network route availability and integration with existing routing infrastructures.

- **Advanced security and networking features** such as DMZ, WAN/WAN failover and policy-based routing.

- **Global management and reporting**
Applications

Central-site Primary Gateway
The PRO 5060 is ideal as a security gateway for critical, centralized networks. Its high-performance and advance networking features allow seamless deployment into virtually any environment.

Features
- Suite of advanced security services for comprehensive multi-layer protection
- Zone security for segmenting internal groups
- Object-based management for easy administration
- Enhanced workforce productivity with Content Filtering Service
- DHCP server and DHCP relay ability
- Hardware and WAN/WAN failover with round-robin, percent-based and spill-over load balancing

Distributed Office and Remote User Security
With its powerful VPN performance and enhanced NAT modes, the PRO 5060 is ideal for securely and easily linking remote/branch offices, partner sites and remote workers.

Features
- 700 Mbps hardware-accelerated IPSec VPN
- Advanced NAT modes for flexible site-to-site connectivity and management
- Compatibility with most major security and VPN appliance manufacturers
- Secondary VPN gateway support with “Dead Peer Detection” for automatic VPN failover
- Easy-to-use Global Security Client/Global VPN Clients for remote users
- Third-party CA certificate support
- Flexible application of firewall rules for VPN traffic on a user or group basis
- DHCP over VPN capability for centralized IP management
- Award-winning Global Management System (GMS) and SonicWALL ViewPoint® for comprehensive management and reporting

Secure WLAN Security and Management
The PRO 5060’s secure WLAN capabilities rival those of the most sophisticated WLAN switch vendors on the market. With SonicWALL, you can easily integrate advanced WLAN services within the organization’s existing network and security architectures. And with over 700 Mbps of IPSec VPN throughput, the PRO 5060 can aggregate a massive number of access points (APs) for large WLAN deployments.

Features
- Complete integration of WLAN security into overall network security management and reporting system
- Centrally manage and configure SonicPoints from PRO 5060 security appliances
- SonicPoints are intelligent, 802.11a/b/g dependent APs that allow wireless intrusion detection, secure wireless roaming, wireless guest services and more
- Standards-based WEP, WPA and IPSec encryption options
- Automatic discovery and provisioning enabled by the SonicWALL Discovery Protocol (SDP) and SonicWALL Simple Provisioning Protocol (SSPP)
- Utilizes the easy-to-use SonicWALL Global VPN Client software for secure IPSec wireless communications

One of the industry’s most comprehensive unified threat management solutions
The nature of network security threats has evolved. While basic L2-4 firewall functionality is still a mandatory element of network security, new breeds of dynamic attacks are wreaking more havoc than ever before. Not only can these attacks render a traditional firewall useless, they also require a constantly updated attack database that guarantees protection. And they absolutely must have a hardware platform that can withstand the rigors of real-time gateway anti-virus, anti-spyware and intrusion prevention while maintaining high levels of performance.

The SonicWALL Deep Inspection Architecture is a highly scalable approach to layered network security. Combining parallel stream processing with our custom-developed flow classification and flow vector bus technology, SonicWALL appliances deliver exceptional levels of performance under the most demanding of security requirements.
Specifications

SonicWALL PRO 5060

Firewall

Nodes Supported: Unrestricted
Statusful Throughput*: 2.4 Gbps
Deep Packet Inspection: Protection from viruses, spyware, worms, Trojans and application layer attacks. Requires Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service for signature updates
Gateway Anti-Virus Throughput**: 340 Mbps
Intrusion Prevention Throughput**: 280 Mbps
Connections: 75,000
Policies: 15,000
Denial of Service Attack Prevention: 22 classes of DoS, UDPs and scanning attacks

VPN

3DES/AES Throughput***: 700 Mbps (MD5, 168-bit)
Site-to-Site VPN: 4,800 tunnels max
Remote Access VPN: 6,800 tunnels max (3,000 clients bundled)
Encryption: DES, 3DES, AES (128, 192, 256-bit)
Authentication: MD5, SHA-1
Key Exchange: Manual Key, PKI (X.509), IKE
XLNS/RADIUS: Yes
L2TP/IPSec: Yes
Flexible VPN Termination: Any port for site-to-site and remote access tunnels
Certificate Support: V3sign, X.509, Baltimore, RSA Keen, Entrust, and Microsoft® CA for SonicWALL-to-SonicWALL VPN
Dead Peer Detection: Yes
DHCP Over VPN: Yes
IPsec NAT Traversal: Yes, NATv6 and v03
Redundant VPN Gateway: Yes
Single-arm VPN: Yes (SonicOS Standard)

Deep Inspection Security Services

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service: Dynamic signature database prevents intrusions, worms and application exploits. Peer-to-peer and instant messaging control and signature updates through Distributed Enforcement Architecture
Content Filtering Service (CFS): Premium Edition
URL, keyword and content scanning
ActiveX®, Java Applets, and Cookie blocking
Gateway- enforced Network Anti-Virus: HTTP, HTTPS, FTP, FTPS, IMAP and POP3, Enforced
McAfee® Clients v6email attachment blocking

Networking

DHCP: Relay, internal server (4,096 leases)
NAT Modes: 1:1, Many-to-many, NAT (overlapping IPs), PAT, transparent mode
Authentication: RADIUS, internal user database, LDAP, Active Directory
VoIP: Full H.323v1-5, SIP, gatekeeper support, inbound and outbound bandwidth management, call tracking and monitoring, full interoperability with most VoIP gateway and communications devices

System

Zone Security: Yes
Object-based Management: Yes
Management: Local CLI, Web GUI, SNMP V2, Webblends, Global management with SonicWALL GMS
Reporting: Comprehensive reporting and graphing, automated scheduling, bandwidth monitoring with SonicWALL ViewPoint™ reporting suite
WAN/WAN Failover: Yes, with percent-based, round-robin and split-over load balancing
Hardware Failure: Active/Passive

Hardware

Interfaces: 10/100/1000 auto-sensing copper Ethernet, (1) Serial Port
10/100/1000 auto-sensing copper Ethernet, (2) Sx/Sc multimode fiber, (1) Port Serial
10/100/1000 auto-sensing copper Ethernet, (1) Serial Port
Relay, internal server (4,096 leases)
NAT Modes: 1:1, Many-to-many, NAT (overlapping IPs), PAT, transparent mode
Authentication: RADIUS, internal user database, LDAP, Active Directory
VoIP: Full H.323v1-5, SIP, gatekeeper support, inbound and outbound bandwidth management, call tracking and monitoring, full interoperability with most VoIP gateway and communications devices

SonicWALL Value-added Security Services

SonicWALL Internet security appliances integrate seamlessly with an expanding array of value-added security services to provide a comprehensive security solution. Gateway anti-virus, anti-spyware, intrusion prevention and content filtering can be deployed over both the wired and wireless LANs.

For more information on SonicWALL security services, including gateway anti-virus, anti-spyware, intrusion prevention and content filtering, please visit our Web site at http://www.sonicwall.com/products/vpnsoft.html

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

©2005 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice. G085_SW1292.US.v10