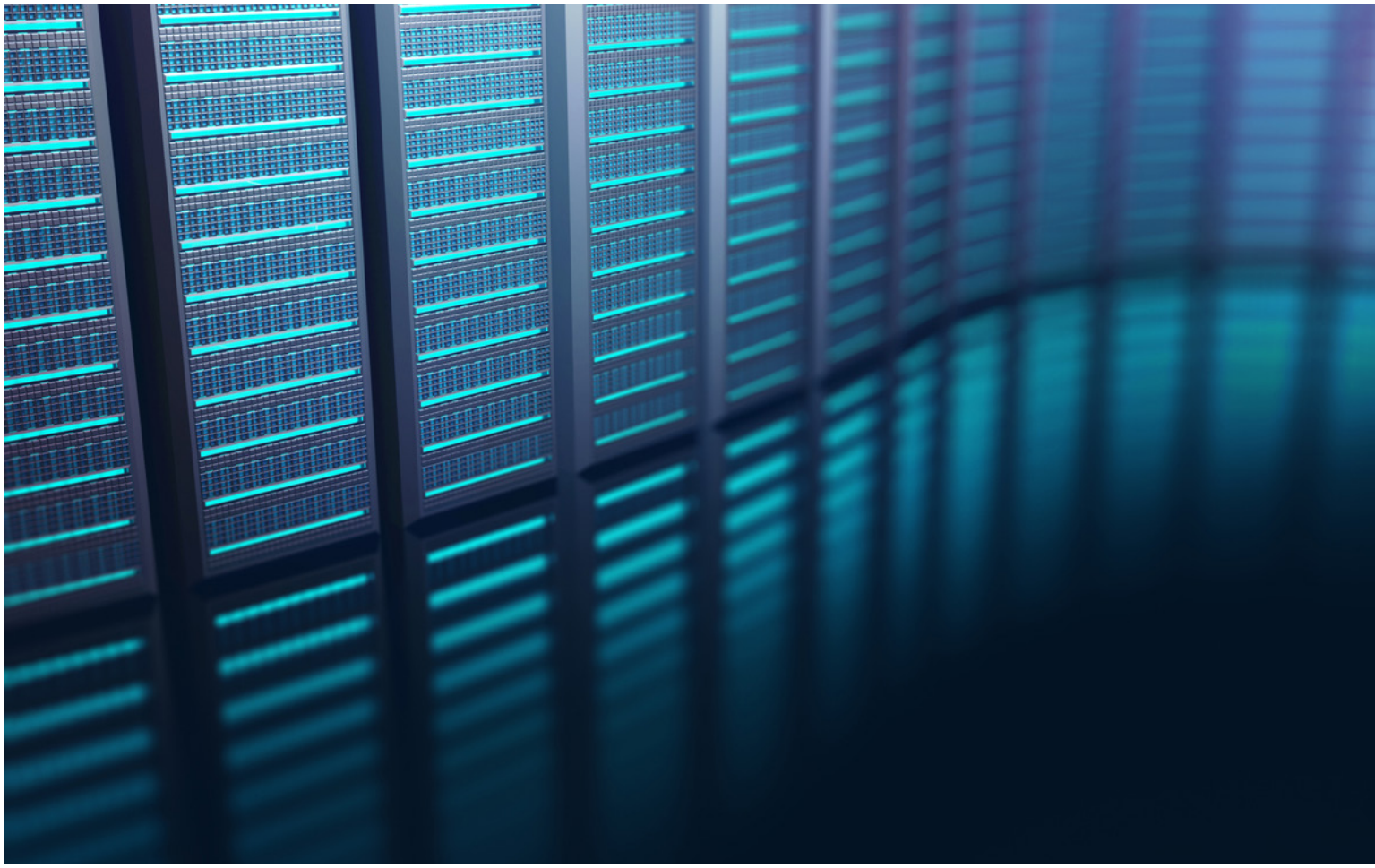
SonicWall product lines



Overview

Secure your organization's systems, users and data with a deep level of protection that won't compromise network performance. SonicWall wired and wireless security solutions are deployed in 200 countries by more than 250,000 customers, ranging from small and mid-sized businesses, to large enterprise environments, government, retail point-of-sale, education, healthcare and service providers.

SonicWall offers comprehensive, complementary product lines in each of the following areas:

- Network security
- Access security
- Email security
- Security management and reporting

Network security products

SonicWall is one of the leading providers of next-generation firewalls (NGFWs). The proven SonicOS firmware is at the core of every SonicWall NGFW. SonicOS leverages our scalable, multi-core hardware architecture and our patented*, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that scans all traffic regardless of port or protocol.

Our NGFWs ensure that every byte of every packet is inspected, while maintaining the high performance and low latency that busy networks require. Unlike competitive offerings, the single-pass RFDPI engine enables simultaneous, multi-threat and application scanning, as well as analysis of any size file, without packet reassembly. This enables SonicWall NGFWs to massively scale to extend state-of-the-art security to growing and distributed enterprise networks and data centers.

SonicWall NGFWs offer a range of robust capabilities, including:

- Capture cloud-based multi-engine sandboxing
- Threat API
- Decryption and inspection of encrypted traffic
- Intrusion prevention service (IPS)
- Malware protection
- Application intelligence, control and real-time visualization
- Website/URL filtering (content filtering)
- Virtual private networking (VPN) over SSL or IPSec
- Wireless security
- Stateful failover/failback

Moreover, SonicWall firewalls deliver fast response and continuous protection against zero-day threats from the Capture Labs research team. This team gathers, analyzes and vets cross-vector threat information from a variety of threat intelligence sources, including a million globally placed sensors within its Capture Threat Network.

SonicWall SuperMassive series

The SonicWall SuperMassive 9000 series NGFW platform is designed to deliver scalability, reliability and deep security at multi-gigabit speeds for large networks.

NSS Labs has assessed SonicWall firewalls using one of the most rigorous real-world performance test of NGFWs, and SonicWall excels in security effectiveness, performance, scalability, reliability and TCO. SonicWall firewalls set the standard for high performance application control and threat prevention in various deployment use cases, from small businesses to large data centers, carriers and service providers.

The SuperMassive 9000 series ensures high quality-of-service level with uninterrupted network availability and connectivity demanded by today's enterprises, government agencies and universities with 10/40 Gbps infrastructures. Offering high-core-density architecture in an efficient 1U and 2U rack appliance, SuperMassive 9000 firewalls save valuable rack space and reduce power and cooling costs.

U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

SonicWall Network Security Appliance (NSA) series

The SonicWall Network Security Appliance (NSA) series is the one of the most secure, highest performing NGFW lines. It delivers business-class security and performance without compromise, using the same architecture as the flagship SuperMassive NGFW line — initially developed for the world's most demanding carriers and enterprises. At the same time, it offers SonicWall's acclaimed ease of use and high value.

Based on years of research and development, the NSA series is designed from the ground up for distributed enterprises, small- to medium-sized businesses, branch offices, school campuses and government agencies. The NSA series combines a revolutionary multi-core architecture with a patented RFDPI single-pass threat-prevention engine in a massively scalable design. This offers industry-leading protection, performance, and scalability, with the highest number of concurrent connections, lowest latency, no file size limitations and superior connections-per-second in its class.

SonicWall TZ series

The SonicWall TZ series is comprised of highly reliable, highly secure unified threat management (UTM) firewalls designed for small- to medium-sized businesses (SMB), retail deployments, government organizations, and distributed enterprises with remote sites and branch offices. Unlike consumer-grade products, the TZ series delivers highly effective anti-malware, intrusion prevention, content/URL filtering and application control capabilities over wired and wireless networks — along with broad mobile platform support for laptops, smartphones and tablets. It provides full deep packet inspection (DPI) at very high performance levels, eliminating the network bottleneck that other products introduce, and enables organizations to realize productivity gains.

As with all SonicWall firewalls, the TZ series inspect the whole file, including TLS/SSL-encrypted files, to enable complete protection. Additionally, the TZ series offers application intelligence and control, advanced application traffic analytics and reporting, Internet Protocol Security (IPsec) and SSL VPN, multiple ISP failover, load balancing, optional integrated high-speed 802.11ac wireless and network segmentation, and also enables PCI compliance. Combined with Dell's X-Series switches, the TZ series firewalls provide the flexibility to securely grow the business without adding complexity.

SonicWave wireless network security series

SonicWall makes wireless networking secure, simple and affordable with the innovative SonicWall Wireless Network Security solution. The solution combines high-performance SonicWave Series 802.11ac Wave 2 wireless access points with industry-leading SonicWall firewalls to achieve wired-like network security and performance on your wireless network, including intrusion prevention, TLS/SSL decryption and inspection, application control and content filtering for enterprise-level performance and protection.

Our solution goes beyond mere secure wireless solutions by securing wireless networks with RFDPI technology and delivering dual protection by encrypting wireless traffic and decontaminating it from network threats, while also protecting the network from wireless attacks. SonicWall lowers total cost of ownership (TCO) by enabling administrators to avoid implementing and separately managing an expensive wireless-specific solution that runs in parallel to their existing wired network.

The TZ series offers a broad security platform to protect SMBs and retail/POS deployments.

SonicWall WAN Acceleration Appliance (WXA) series

The SonicWall WAN Acceleration Appliance (WXA) series reduces application latency and conserves bandwidth, significantly enhancing WAN application performance and user experience for small- to medium-sized organizations with remote and branch offices. After initial data transfer, the WXA series dramatically reduces all subsequent traffic by transmitting only new or changed data across the network. The WXA deduplicates data traversing the WAN, remembers previously transferred data, and replaces repeated byte sequences with an identifier, thus reducing application latency and conserving bandwidth. Other acceleration features include data caching, file deduplication, metadata caching, HTTP (web) caching and data-in-flight compression.

Unlike standalone WAN acceleration products, WXA solutions are integrated add-ons to SonicWall SuperMassive 9000, NSA and TZ series firewalls. This integrated solution streamlines the placement, deployment, configuration, routing, management and integration of the WXA with other components, such as VPNs. When deployed in conjunction with a SonicWall NGFW running Application Intelligence and Control Service, the WXA offers the unique combined benefit of both prioritizing application traffic and minimizing traffic between sites, resulting in optimal network performance.

Learn more about SonicWall network security products at: www.sonicwall.com/en-us/products.

Network security services and add-on products

SonicWall network security firewall services and add-ons offer highly effective, advanced protection for organizations of all sizes, to help defend against security threats, gain greater security control, enhance productivity and lower costs.

Services and add-ons include:

- TotalSecure bundle — Firewall plus the Comprehensive Gateway Security Suite bundle (anti-virus, anti-spyware, intrusion prevention, application intelligence, content/web filtering and 24x7 support)
- Advanced Gateway Security Suite bundle — Capture Advanced Threat Protection, Gateway anti-virus, anti-spyware, intrusion prevention, content/web filtering and 24x7 support
- Gateway security services — Gateway anti-virus, anti-spyware, intrusion prevention and application intelligence and control
- Capture advanced threat protection (ATP)
- Content filtering services
- Enforced client ant-virus and anti-spyware software
- Comprehensive anti-spam service
- Deep packet inspection of SSL-encrypted traffic (DPI-SSL)
- Application intelligence and control
- Intrusion prevention system (IPS)

Learn more about network security services and add-ons at: www.sonicwall.com/en-us/products/firewalls/security-services.

SONICWALL®

Access security products

SonicWall SMA is the unified secure access gateway for organizations facing challenges in mobility, BYOD and cloud migration. The solution enables organization to provide anytime, anywhere and any device access to mission critical corporate resources. SMA's granular access control policy engine, context aware device authorization, application level VPN and advanced authentication with single sign-on empowers organizations to embrace BYOD and mobility in a hybrid IT environment.

In addition, SMA reduces the surface area for threats by providing features such as Geo IP and Botnet detection, Web Application Firewall and Capture ATP sandbox integration.

Mobility and BYOD

For organizations wishing to embrace BYOD, flexible working or offshore development, SMA becomes the central enforcement point across them all. SMA delivers best-in-class security to minimize surface threats, while making organizations more secure by supporting latest encryption algorithms and ciphers. SonicWALL's SMA allows administrators to provision secure mobile access and role-based privileges so end-users get fast, simple access to the business applications, data and resources they require. At the same time, organizations can institute secure BYOD policies to protect their corporate networks and data from rogue access and malware.

Move to the cloud

For organizations embarking on a cloud migration journey, SMA offers a single sign-on (SSO) infrastructure that uses single web portal to authenticate users in a hybrid IT environment. Whether the corporate resource is on-premise, on the web or in a hosted cloud, the access experience is consistent and seamless. Users do not need to remember all the individual application URLs and maintain exhaustive bookmarks. With Workplace, a centralized access portal, you give users one URL to access all mission critical applications from a standard Web browser. SMA provides federated SSO to both cloud hosted SaaS applications that use SAML 2.0 and campus hosted applications that use RADIUS or Kerberos. SMA integrates with multiple authentication, authorization, and accounting servers and leading Multi-factor authentication (MFA) technologies for added security. Secure SSO is delivered only to authorized endpoint devices after checks for health status and compliance.

Managed service providers

For organizations with data centers or for managed service providers, SMA provides turnkey solution to deliver a high degree of business continuity and scalability. The SonicWALL's SMA can support up to 20,000 concurrent connections on a single appliance with the ability to scale upwards of hundreds of thousands users through intelligent clustering. Reduce costs at data centers with active-active HA clustering (Global High Availability) and built-in dynamic load balancer (Global Traffic Optimizer), which reallocates global traffic to the most optimized data center in real-time based on user demand. SMA empowers service owners through a series of tools to deliver a service with zero downtime and allows very aggressive SLAs to be fulfilled.

SonicWall SMA is a unified secure access gateway that enables organization to provide anytime, anywhere and any device access to mission critical corporate resources.

SMA Appliances

SonicWall SMA can be deployed as a hardened, high-performance appliance or as a virtual appliance leveraging shared computing resources to optimize utilization, ease migration and reduce capital costs. The hardware appliances are built on a multi-core architecture that offers high performance with SSL acceleration, VPN throughput and powerful proxies to deliver robust secure access. For regulated and federal organizations, SMA is available with FIPS 140-2 Level 2 certification. The SMA virtual appliances offer the same robust secure access capabilities on major virtual platforms such as Hyper-V and VMware. Whether you choose to deploy physical appliances, virtual appliances or a combination of the two, SMA fits seamlessly into your existing IT infrastructure.

Management and Reporting

SonicWall provides an intuitive he web-based management platform to streamline appliance management while providing extensive reporting capabilities. The easy-to-use GUI brings clarity to managing multiple machines. Unified policy management helps you create and monitor access policies and configurations. One single policy manages your users, devices, applications, data and networks. Automate routine tasks and schedule activities, freeing up security teams from repetitive tasks to focus on strategic security tasks like incidence response.

Empower your IT department to provide the best experience and the most secure access depending on the user scenario. Choose from a range of fully clientless web-based secure access for vendors and 3rd party contractors, or a more traditional client-based full tunnel VPN access for executives. Whether you need to provide reliable secure access to 5 users from a single data center or scale up to thousands' of users from globally distributed data centers, SonicWall SMA has a solution for you.

Learn more about SonicWall mobile security products at: www.sonicwall.com/en-us/products/remote-access.

SONICWALL

Email security products

Email is crucial for your business communication, but it can also expose your business to sabotage and productivity drains if email-based threats such as ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses flood your mail servers and user inboxes. What's more, government regulations now hold your business accountable for protecting confidential data and ensuring it is not leaked and that email containing sensitive customer data or confidential information is securely exchanged. Whether your organization is a growing small-to medium-sized business, a large, distributed enterprise or a managed service provider (MSP), you need a cost-effective way to deploy email security and encryption, and the scalability to easily grow capacity for — and delegate management across — organizational units and domains.

In addition, to manage costs and resources, organizations are adopting Microsoft Office 365. While Office 365 offers built-in security functionalities, to combat advanced email threats organizations require a next-generation email security solution that seamlessly integrates with Office 365, to protect them against today's advanced threats.

SonicWall Email Security Appliances

Easy to set up and administer, SonicWall Email Security is designed to cost-effectively scale from 10 to 100,000 mailboxes. It can be deployed as a hardware appliance, as a virtual appliance leveraging shared computing resources, or as software — including software optimized for Microsoft Windows server or Small Business Server. SonicWall Email Security physical appliances are ideal for organizations that need a dedicated on-premises solution. Our multi-layered solution provides comprehensive inbound and outbound protection, and is available in a range of hardware appliance options that scales up to 10,000 users per appliance. SonicWall Email Security is also available as a virtual appliance or as a software application that is ideal for organizations that require the flexibility and agility that come with virtualization. The solution can be configured for high availability in split mode, to centrally and reliably manage large-scale deployments.

SonicWall email security solution uses technologies such as Advanced Reputation Management, Advanced Content Management, Adversarial Bayesian filtering and a Support Vector Machine algorithm to deliver comprehensive inbound and outbound protection.

- Integrated with multi-engine Capture ATP sandbox
- Multiple AV engines
- Configurable Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC) settings
- Scans reputation of not only the sender IP but also message subject, content, embedded links and attachments
- Seamless integration with Office 365
- Encryption and Compliance add-on

Administration of the Email Security solution is intuitive, quick and simple. You can safely delegate spam management to end users, while still retaining ultimate control over security enforcement. You can also easily manage user and group accounts with seamless multi-LDAP synchronization. The solution also provides easy integration fort Office 365 to defend against advanced email threats.

For large, distributed environments, multi-tenancy support lets you delegate sub-administrators to manage settings at multiple organizational units (such as enterprise divisions or MSP customers) within a single Email Security deployment.

SonicWall Hosted Email Security service

Trust fast-to-deploy and easy-to-administer hosted services to protect your organization from email-borne threats such as ransomware, zero-day threats, spear phishing and BEC while meeting email compliance and regulatory mandates. Get the same level of advanced email protection with our hosted solution, which offers feature parity with physical and virtual appliances. The solution also offers email continuity to ensure that emails are always delivered and productivity is not impacted during planned and unplanned outages of on-prem email servers or a cloud provider such as Office 365.

SonicWall Hosted Email Security offers superior, cloud-based protection from inbound and outbound threats, at an affordable, predictable and flexible monthly or annual subscription price. You can minimize upfront deployment time and costs, as well as ongoing administration expenses without compromising on security.

SonicWall offers VARs and MSPs a greater opportunity to compete and grow revenue while minimizing risk, overhead and ongoing costs. SonicWall Hosted Email Security includes MSP-friendly features such as robust multi-tenancy, central management for multiple subscribers, Office 365 integration, flexible purchase options and automated provisioning.

Learn more about SonicWall Email Security products at: www.sonicwall.com/en-us/products/secure-email.

Management, reporting and analytics

SonicWall believes a connected approach to security management is not just fundamental to good preventative security practice, it also forms the basis for a unified security governance, compliance and risk management strategy. With SonicWall management, reporting and analytics solutions, organizations get an integrated, secured and extensible platform to establish a strong, uniform security defense and response strategy across their wired, wireless and mobile networks. The full adoption of this common platform gives organizations deep security insight to make informed security decisions, and move quickly to drive collaboration, communication and knowledge across the shared security framework.

SonicWall Global Management System

Deployable as software or a virtual appliance, the SonicWall Global Management System (GMS) cohesively manages network security operations by business processes and service levels as opposed to a less efficient device-by-device siloed approach. GMS enables organizations of varying sizes and types to easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities and federate all operational aspects of the security infrastructure. This includes centralized policy management and enforcement, real-time event monitoring, granular data analytics and reporting, audit trails and more under a unified enterprise platform.

GMS also meets the firewall change management requirements of organizations through workflow automation. This intrinsic, automated process assures the correctness and the compliance of policy changes by enforcing a rigorous process for configuring, comparing, validating, reviewing and approving security management policies prior to deployment. The approval groups are flexible, enabling adherence to company security policies and assuring the right firewall policies are deployed at the right time and in conformance to compliance regulations.

SonicWall Cloud GMS

Cloud GMS is an open, scalable cloud security management, monitoring, reporting and analytics platform that is delivered as a cost-effective Software-as-a-Services (SaaS). It is designed for organizations of various sizes and use cases including distributed enterprises and service providers that are adopting cloud computing for its cost efficiency. Cloud GMS is the ideal cloud security management platform to establish a sustainable, fully coordinated security operation across any networks.

For customers, Cloud GMS offers the ultimate in visibility, agility and capacity to govern the entire SonicWall network security ecosystem with greater clarity, precision and speed – all from one place regardless of location. With an enterprise-wide view of the security environment and real-time security intelligence reaching the right people in the organization, accurate security policies and controls decisions can be made towards a stronger security posture.

For service providers, Cloud GMS simplifies the discrete management of multiple clients' security operations. It creates opportunities for MSP/MSSPs to increase their security services agility while reducing the operating expenses and complexities of supporting a solely owned infrastructure.

SonicWall Analyzer

Analyzer is an easy-to-use web-based traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the network. Analyzer supports SonicWall firewalls and secure mobile access devices while leveraging application traffic analytics for security event reports. Organizations of all sizes benefit from enhanced employee productivity, optimized network bandwidth utilization and increased security awareness. Analyzer is available as a Windows application and as a virtual appliance.

Learn more about SonicWall management and reporting products at: www.sonicwall.com/en-us/products/firewalls/management-and-reporting.

SONICWALL®

SonicWall Enterprise Services

Achieve more from your SonicWall network security solution and get the support you need, when you need it. With SonicWall enterprise support and professional services, you'll gain superior long-term value from your solution.

Global Support Services

Get convenient support to keep your business humming along smoothly:

Technical Support

- **8x5** – Monday through Friday, 8 a.m. to 5 p.m. for non-critical environments.
- **7x24** – Around the clock support, including weekends and holidays, for business-critical environments.

Value Add Support

- **Premier Support** provides enterprise environments with a dedicated Technical Account Manager (TAM). Your TAM acts on your behalf as a trusted advisor who works with your staff to help minimize unplanned downtime, optimize IT processes, provide operational reports to drive efficiencies and is your single point of accountability for a seamless support experience.
- **Dedicated Support Engineer (DSE)** provides a named engineering resource to support your enterprise account. Your DSE will know and understand your environment, policies and IT objectives to bring you fast technical resolution when you need support.

Global Professional Services

Need help determining the best security solution for your business, as well as setting it up within your existing infrastructure? Let us take care of it. With Global Professional Services, you get a single point of contact for all your deployment and integration needs. You'll receive services tailored to your unique environment and assistance with:

- **Planning:** Scoping and understanding your firewall requirements.
- **Implementation/Deployment:** Assessing and deploying your solution.
- **Knowledge transfer:** Using, managing and maintaining your device.
- **Migration:** Minimizing disruption and ensuring business continuity.

SonicWall enterprise services are available with SuperMassive/NSAs/TZ Series/SRA/SMA/Email Security/GMS.

Learn more: https://support.software.com/essentials/support-offerings.

Conclusion

Discover SonicWall security products

Integrate your hardware, software and services for best-of-breed security. Learn more at www.sonicwall.com. Learn about purchase and upgrade options at www.sonicwall.com/how-to-buy. And try out SonicWall solutions for yourself at www.sonicwall.com/trials.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com