

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 and encryption
- 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.

SonicWall NGFWs offer a range of robust capabilities, including:

- Website/URL filtering (content filtering)
- Intrusion prevention service (IPS)

- Malware protection
- Application intelligence, control and real-time visualization
- Deep packet inspection of SSL-encrypted sessions (DPI-SSL)
- Virtual private networking (VPN) over SSL or IPsec
- Wireless security
- Stateful failover/failback

Moreover, by leveraging the unique SonicWall Global Response Intelligent Defense (GRID) worldwide attack identification and monitoring network, SonicWall firewalls deliver superior protection today and tomorrow.

SonicWall SuperMassive series

The SonicWall SuperMassive (E10000 and 9000) series NGFW platform is designed to deliver scalability, reliability and deep security at multi-gigabit speeds for large networks.

NSS Labs has demonstrated the SuperMassive E10000 series excels over comparable firewalls in security effectiveness, performance, scalability, reliability and TCO. Built to protect 10+ GB networks at very large data

centers, carriers and service provider deployments, SuperMassive E10000 firewalls set the standard for high-performance application control and threat prevention.

The SuperMassive 9000 series ensures the security, performance and scalability demanded by today's enterprises, government agencies and universities with 10+ GB infrastructures. Offering high-core-density architecture in an efficient one-rack appliance, SuperMassive 9000 firewalls save valuable rack space and reduce power and cooling costs.

SonicWall
SuperMassive NGFWs
deliver deep security,
high performance and
low latency for data
centers and large
enterprises.

*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 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.

SonicPoint 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 SonicPoint Series 802.11ac wireless access points with industry-leading SonicWall firewalls to achieve wired-like network security and performance on your wireless network, including intrusion prevention, 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, E-Class NSA, NSA and TZ 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/products/network-security-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)
- Comprehensive Gateway Security Suite bundle — 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
- Content filtering services
- Enforced client anti-virus and anti-spyware software
- Comprehensive anti-spam service
- Deep packet inspection of SSL-encrypted traffic (DPI-SSL)
- Application intelligence and control
- Capture advanced threat protection (ATP)
- Intrusion prevention system (IPS)

Learn more about network security services and add-ons at: sonicwall.com/network-security-services-add-ons.



Secure mobile access portfolio

The proliferation of mobile devices in the workplace, both employer-issued and personally owned, has increased the demand on organizations to enable secure mobile access to company applications, data and resources.

To address mobile workforce needs, SonicWall delivers a secure mobile access (SMA) solution that enables customers to easily provision role-based privileges for managed and unmanaged devices. With the SMA portfolio of solutions, organizations can provide their remote/mobile workers fast and easy access to their organization's applications, data and resources that they need. At the same time, they can ensure the network is protected from mobile security threats, such as unauthorized access and malware attacks.

For multi-layer threat protection, when integrated with a SonicWall NGFW, the SMA series decrypts and decontaminates all authorized SSL VPN traffic before it enters the network environment and the combined solution delivers centralized access control, malware protection, web application control and content filtering.

SonicWall SMA series

The SMA series provides mobile and remote workers using smart phones, tablets or laptops (whether managed or unmanaged) with policy-enforced SSL VPN access to mission-critical applications, data and resources without compromising security.

The SonicWall SMA series is compatible with Windows, iOS, Mac OS X, Android, Linux, Kindle Fire and Chrome OS mobile devices to provide secure access to network resources, including shared folders, client-server applications, intranet sites, email, and remote and virtual desktop services.

- Mobile devices are interrogated for essential security information such as jailbreak or root status, device ID, certificate status and OS versions prior to granting access.
- Laptops and PCs are also interrogated for the presence or absence of security software, client certificates and device ID.
- Devices that do not meet policy requirements are not allowed network access and the user is notified of non-compliance.

The SMA series allows administrators to quickly and easily provision secure mobile access and role-based privileges so end users get fast, simple access to the enterprise 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.

Secure Mobile Access (SMA) series delivers fast, easy, policy-enforced access to mission-critical apps, data and resources, across all mobile devices, without compromising security.



Recently introduced functionality enhancements in the high-end SMA models includes:

- Global High Availability offers a turnkey approach to delivering robust remote access where a high degree of business continuity is required, all without any downtime and aggressive SLAs. Global High Availability (G-HA) includes the patent pending Global Traffic Optimizer (GTO) for traffic load balancing with zero-impact failover for high resiliency across data centers. It also provides real-time monitoring across environment performance and user sessions, while delivering active/active configuration for high availability.

- Blended SSO technology enables organizations to move to the cloud utilizing a single pane of glass to access traditional campus resources and SaaS cloud applications, allowing service owners to seamlessly move resources to the cloud while maintaining a familiar access experience for their users.
- Rules based access control delivers best-in-class security to minimize surface threats, while making organizations more secure through cipher enhancements to the advanced suite B algorithms in accordance with the National Security Agency.
- An intuitive user experience through enhanced browser based clientless

access and native apps provides an updated and modernized user interface for both the administrative console and user workplace portals.

Learn more about SonicWall mobile security products at: sonicwall.com/products/secure-mobile-access.



Email Security products

SonicWall Email Security provides superior protection from email threats and compliance violations. Multiple proven, patented threat detection techniques deliver real-time protection from spam, phishing attacks and viruses. Compliance scanning and management prevent confidential data leaks and regulatory violations.

With integrated email encryption, policies may be configured to scan outbound email content and attachments for sensitive data. When detected, the email is encrypted for secure email exchange with customers and partners. Encrypted email can be tracked to confirm the time of receipt and time opened. A notification email is delivered to the recipient's inbox with instructions to simply log into a secure portal to read or securely download the email. The service is cloud-based with no additional client software necessary and, unlike competitive solutions, the encrypted email may be accessed and read from mobile devices or laptops. In addition, the solution includes Domain-based Message Authentication, Reporting and Conformance (DMARC), a powerful email authentication method that helps identify spoofed mail, reducing spam and phishing attacks. It also reports on sources and senders of email, so you can identify and shut down unauthorized senders falsifying email with your address and protect your brand.

Easy to set up and administer, the solution is designed to scale from 10 to 100,000 mailboxes, and may be deployed as a hosted service, hardware appliance, virtual appliance, or Windows Server software to best meet your infrastructure requirements. Configure

for high availability and scalable split mode, and centrally and reliably manage enterprise-class deployments.

Administration is intuitive, quick and simple. Safely delegate spam management to end users while still retaining ultimate control over security enforcement. Easily manage user and group accounts with seamless multi-LDAP synchronization. In 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 SonicWall Email Security deployment.

SonicWall Email Security appliances

SonicWall Email Security appliances offer comprehensive, effective and scalable email security for SMB, enterprise and MSSP environments. This powerful yet easy-to-manage solution combines anti-spam, anti-virus and anti-phishing capabilities with content filtering and outbound email management, preventing leaks of confidential information and violations of regulatory compliance laws. Its unique pre-emptive scanning MTA offers breakthrough message analysis and industry-leading message delivery rates, providing high-performance and enterprise-wide scalability.

SonicWall Email Security is available as a hardware appliance, software and virtual appliance.

SonicWall Hosted Email Security service

SonicWall Hosted Email Security offers superior cloud-based protection from inbound and outbound threats, including spam, phishing, zombie attacks and malware, at an affordable, predictable

and flexible monthly or annual subscription price. At the same time, it minimizes upfront deployment time and costs, as well as ongoing administration expenses. The service includes advanced compliance and management. With an optional add-on, it can also include email encryption to prevent confidential data leaks, regulatory violations and ensure the secure exchange of sensitive data.

SonicWall Hosted Email Security uniquely integrates multiple anti-virus technologies, including SonicWall Global Response Intelligent Defense (GRID) Anti-Virus™, SonicWall Time Zero Virus Protection, and premium anti-virus technologies, to deliver best-in-class email security. The SonicWall GRID network performs rigorous testing and evaluation of millions of emails every day, and then reapplies this constantly updated analysis to provide exceptional spam blocking results and anti-virus and anti-spyware protection.

SonicWall Time Zero Virus Protection uses predictive and responsive technologies to protect organizations from virus infections before anti-virus signature updates are available. The suspect emails are identified and immediately quarantined, safeguarding the network from the time a virus outbreak occurs until the time an anti-virus signature update is available. Moreover, premium anti-virus technology from industry-leading anti-virus partners provides an additional layer of anti-virus protection, resulting in protection superior to that provided by solutions that rely on a single anti-virus technology.

Learn more about SonicWall Email Security products at: sonicwall.com/products/email-security-appliance.



Management and reporting products

SonicWall management and reporting products enable you to take control of the health, performance and security of your network, with easy monitoring, alerting and reporting. Meet the unique challenges of your organization with a variety of flexible management and reporting products that complement and extend SonicWall security products and services, and help your business optimize security, manage growth and ease administrative burdens.

SonicWall Global Management System

The Global Management System (GMS) provides organizations, distributed enterprises and service providers with a powerful and intuitive solution to centrally manage and rapidly deploy SonicWall firewall, anti-spam and secure mobile access solutions.

Flexible deployment options include software, hardware and virtual appliances. SonicWall GMS also provides centralized real-time monitoring, and comprehensive policy and compliance reporting.

For enterprise customers, SonicWall GMS streamlines security policy management and appliance deployment, minimizing administration overhead. For service providers, SonicWall GMS simplifies the security management of multiple clients and creates additional revenue opportunities. For added redundancy and scalability, GMS can be deployed in a cluster configuration.

GMS is available as software or a virtual appliance.

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. Security is the only firewall vendor that provides a complete solution combining off-box application traffic analytics combined with granular statistical data generated by SonicWall firewalls. Analyzer is available as a Windows application and as a virtual appliance.

Learn more about SonicWall management and reporting products at: sonicwall.com/products/network-security-management-reporting.



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.



© 2017 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING,

BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

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