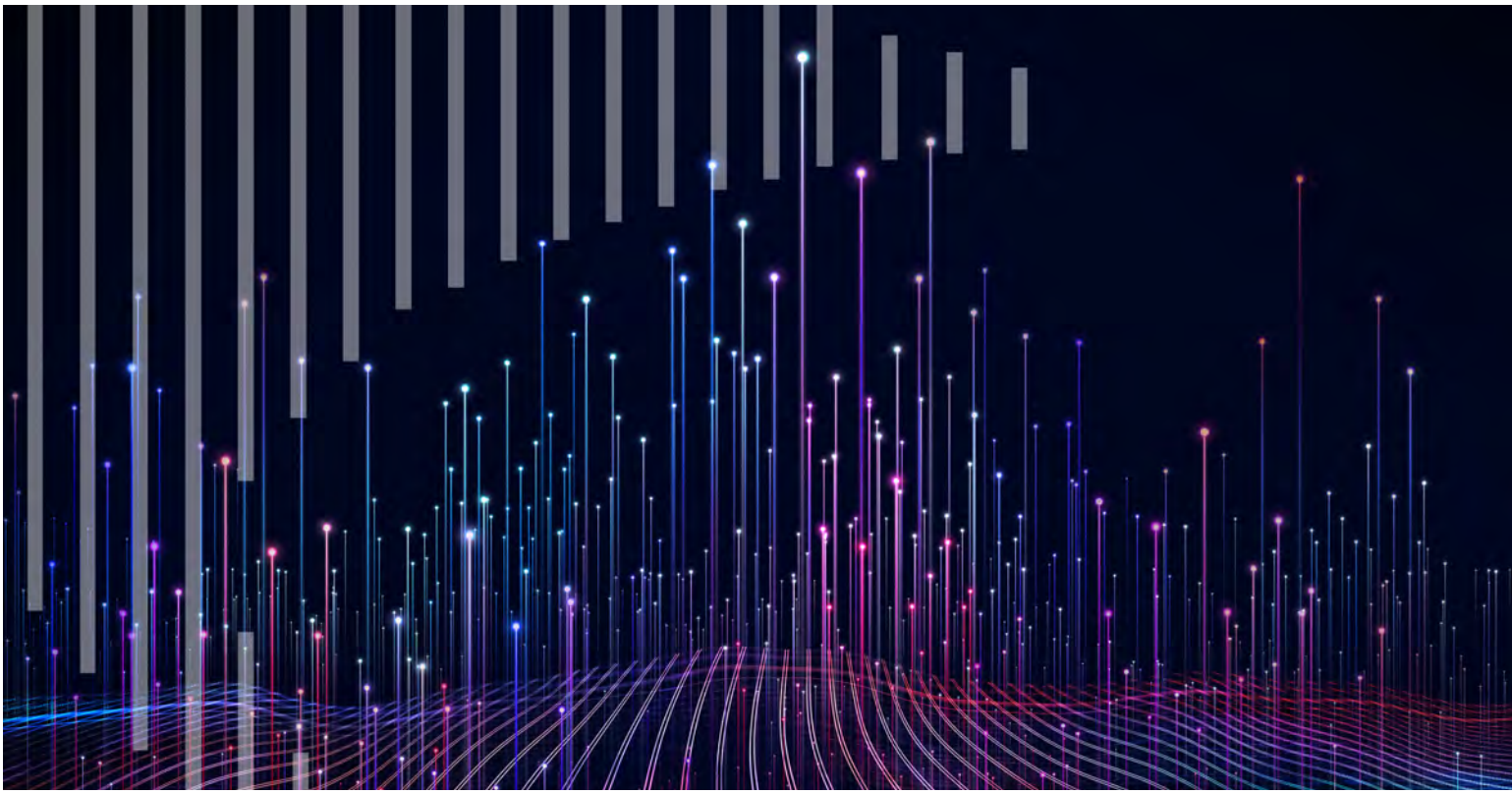
SonicWall Product Lines

June 2022



Overview

Secure your organization's public/private cloud, applications, users and data with a deep level of protection that won't compromise network performance. The SonicWall Capture Cloud Platform tightly integrates security, management, analytics and real-time threat intelligence across the company's portfolio of network, wireless, email, mobile, web and cloud security products. This approach enables small and mid-sized businesses, to large enterprise environments, government, retail point-of-sale, education, healthcare and service providers to experience our complete security ecosystem that harnesses the power, agility and scalability of the cloud.

The Capture Cloud Platform strategy and vision for the future are continuous innovation and development of containerized as-a-service security applications that are easily programmable and provisioned on-demand. It is comprised of the following key core components and capabilities:

- Network Security
- Wired Security
- Wireless Security
- Endpoint Security
- WAN Acceleration
- Advanced Security Services
- Cloud App Security
- Cloud Edge Secure Access
- Secure Mobile Access
- Email Security
- Management, Reporting and Analytics
- Professional Services and Support

The combination of these delivers mission-critical layered cyber defense, threat intelligence, analysis and collaboration, along with common management, reporting and analytics that work synchronously together.

Network Security

SonicWall is one of the leading providers of next-generation firewalls (NGFWs). Either the SonicOS or the SonicOSX firmware is at the core of every SonicWall NGFW. SonicOS leverages our scalable, hardware architecture plus our patent-pending Real-Time Deep Memory Inspection (RTDMI™) and our patented*, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engines that scan 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 ATP cloud-based multi-engine sandboxing
- SD-WAN
- REST APIs
- 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
- Hybrid and multi-cloud security
- Stateful failover/failback

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

SonicWall Network Security services platform (NS*sp*) series

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

ICSA Labs has tested SonicWall firewalls and found that they excel in security effectiveness with 100% detection rate without any false positives for the last five quarters in a row. SonicWall firewalls have 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.

For example, our high-end NS*sp* multi-instance firewall ensures high quality-of-service level with uninterrupted network availability and connectivity demanded by today's enterprises, government agencies, service providers and universities with 100/40/10 Gbps infrastructures. Leveraging innovative deep learning security technologies in the SonicWall Capture Cloud Platform, the NS*sp* series delivers proven protection from the most advanced threats without slowing performance.

Unified Policy with SonicOSX 7

The unified policy management feature in SonicOSX 7 offers integrated management of access and security policies across certain SonicWall high-end NS*sp* and NS*v* virtual firewalls.

It comes with a new web interface that is designed with a radically different approach. The emphasis is on user-first design, which leads to a more intuitive set up of contextual security policies through actionable alerts, and with point-and-click simplicity.

Visually, it is also more attractive than the classic interface. In a single-pane view of a firewall, the interface presents the user with information on the effectiveness of various security rules. It enables the user to modify the predefined rules for gateway anti-virus, anti-spyware, content filtering, intrusion prevention, geo-IP filtering and deep-packet inspection of encrypted traffic in a seamless fashion.

With this new unified policy interface, SonicWall delivers a more streamlined experience to control dynamic traffic changes in less time, and for a better overall security posture.

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

SONICWALL®

SonicWall Network Security appliance (NS*a*) series

The SonicWall Network Security appliance (NS*a*) series is the one of the most secure, high performing NGFW available in its class. It delivers business-class security without compromising performance, using the same architecture as the flagship NS*sp* NGFW series — developed for the world's most demanding enterprise networks.

Based on years of research and development, the NS*a* series is designed from the ground up for distributed enterprises, medium-sized businesses, branch offices, school campuses and government agencies. The NS*a* series combines a revolutionary multi-core architecture with cloud-based Real-Time Deep Memory Inspection (RTDMI) technology, a patented threat-prevention engine in a massively scalable design. This offers industry-leading protection, performance and scalability, with the high number of concurrent connections, low latency, no file size limitations and superior connections-per-second compared to other leading firewall vendors.

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 consolidates 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 inspects 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 and SD-WAN. Optional integrated Power over Ethernet (PoE) and high-speed 802.11ac wireless enable organizations to extend their network boundaries easily and securely. Combined with SonicWall switches, the TZ series firewalls provide the flexibility to securely grow the business with the ease of Zero-Touch Deployment, but without adding complexity.

The latest-generation TZ series is the first firewall in a desktop form factor to bring multi-gigabit (2.5/5/10G) or gigabit interfaces, Secure SD-WAN, built-in and expandable storage, TLS 1.3 support and 5G readiness while delivering ground-breaking performance. Redundant power supplies, 802.11ac Wave 2 support further enhance the capabilities of these devices. Designed for mid-sized organizations and distributed enterprise with SD-Branch locations, the new generation TZ series firewalls deliver industry-validated security effectiveness with best-in-class price-performance.

SonicWall Network Security virtual (NS*v*) series

SonicWall Network Security virtual (NS*v*) firewalls extend automated breach detection and prevention into hybrid and multi-cloud environments with virtualized versions of SonicWall next-generation firewalls. With full-featured security tools and services equivalent to a SonicWall firewall, NS*v* effectively defends your virtual and cloud environments from resource misuse attacks, cross-virtual-machine attacks, side-channel attacks and all common network-based exploits and threats.

NS*v* is easily deployed and provisioned in a multi-tenant virtual environment, typically between virtual networks (VNs). It establishes access control measures to preserve data and VM safety while capturing virtual traffic between virtual machines and networks for automated breach prevention.

With infrastructure support for high availability (HA) implementation, NS*v* fulfills scalability and availability

requirements of Software Defined Data Center (SDDC). Easily deployed as a virtual appliance in private cloud platforms such as VMWare ESXi, Linux KVM, Nutanix or Microsoft Hyper-V, or in AWS or Microsoft Azure public cloud environments. Leverage flexible BYOL and PAYG licensing models with NS*v* and provide organizations all the security advantages of a physical firewall with the operational and economic benefits of virtualization.

Certain NS*v* firewall models feature SonicOSX with Unified Policy, delivering a more streamlined experience to control dynamic traffic changes in less time, and provide a better overall security posture.

Learn more about SonicWall firewall products at: www.sonicwall.com/products/firewalls/

Capture Security appliance 1000 (CSa 1000)

To comply with regulations and privacy standards, you need a budget-friendly threat analysis platform that malicious code can't detect and evade. SonicWall Capture Security appliance (CS*a*) is an on-premises file analysis and malware detection solution featuring SonicWall Real-Time Deep Memory Inspection (RTDMI). RTDMI enables CS*a* to catch more malware, faster and more effectively. Its low false positive rate enhances security and the end user experience.

CS*a* lets you analyze malware hidden in a broad range of file types, file sizes and operating environments, for comprehensive zero-day threat detection. It detects and stops side-channel attacks through real-time memory-based inspection. By forcing malware to reveal its weaponry into memory, CS*a* proactively blocks mass-market, zero-day and unknown threats. CS*a* supports closed networks and can be used with the latest SonicWall next-generation firewalls.

SonicWall CS*a* deployment is quick and straightforward, requiring only configuration of basic networking, reporting and allowed device access to get started. The CS*a* is built to be IP-addressable and can therefore be deployed anywhere, as long as it's reachable by devices that will submit files for analysis. The CS*a* can also be deployed in closed or air-gapped networks.

Wired Security

SonicWall Switches deliver high-speed network switching with unparalleled performance and manageability. They feature high port density, optional Power over Ethernet (PoE) and 1- or 10-gigabit throughput. Ideal for SMBs and Software-Defined Branch (SD-Branch) networks, they enable any size businesses to undergo digital transformation and keep pace with the changing network and security landscape.

SonicWall Switches can be managed via SonicWall firewalls or Wireless Network Manager (WNM). WNM seamlessly integrates wired and wireless security end-to-end for a unified security posture. This simplifies deployment, management and troubleshooting, and eliminates gaps that may arise with third-party switches. SonicWall Switches can be rolled out quickly across distributed branches using Zero-Touch Deployment.

Wireless Security

SonicWall makes wireless networking secure, simple and affordable with the innovative SonicWall Wireless Network Security solution. The high-performance SonicWave Series 802.11ax wireless access points can be easily managed via Wireless Network Manager. SonicWave access points can be untethered from the firewalls and deployed independently.

In addition to the high-speed wireless access points and cloud-managed dashboard, SonicWall wireless security solution includes Wi-Fi Planner, an advanced site-survey tool to help admins plan and deploy Wi-Fi networks effectively. The solution also consists of SonicExpress mobile app for easy onboarding and monitoring of access points to provide admins real-time information on network status and security.

Our solution goes beyond mere secure wireless solutions by securing wireless networks with RTDMI and RFDPI technologies and delivers advanced security features such as multi-engine sandboxing, content filtering, Cloud AV directly on the access point, without the need for a firewall. Further enhance security and performance on your network with features including intrusion prevention, TLS/SSL decryption and inspection and application control for enterprise-level performance and protection.

SonicWave APs support fast roaming so that users can roam from one location to another seamlessly. Its feature-rich portfolio includes captive portal, auto channel selection, spectrum analysis, air-time fairness, band steering and signal analysis tools for monitoring and troubleshooting.

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.

Endpoint Security

The management and security of endpoints is critical in today's business climate. With end users in and out of the network with their devices, as well as encrypted threats reaching endpoints unchecked, something must be done to protect these devices.

With the growth of ransomware and application vulnerabilities, endpoints are the battleground of today's threat landscape.

Additionally, administrators struggle with the visibility and management of their security posture. They are also challenged by having to provide consistent assurance of client security, along with easy-to-use and actionable intelligence and reporting.

Endpoint security products have been on the market for years but administrators struggle with:

- Keeping security products up to date
- Enforcing policies on a global scale
- Getting reports and viewing health of tenants
- Threats coming through and creating encrypted channels
- Understanding alerts and remediation steps
- Cataloging applications and their vulnerabilities
- Stopping threats like ransomware
- Fileless attacks and infected USB devices bypassing perimeter defenses

SonicWall Capture Client is a unified client platform that will deliver multiple endpoint protection capabilities.

This solution features a cloud-based management console and an optional complete integration with SonicWall next-generation firewalls for a unified security experience for SonicWall customers. Combined with enforcement capabilities, SonicWall Capture Client can ensure that endpoints are running security software and/or have an embedded SSL certificate in place for the inspection of encrypted traffic. Furthermore, in order to make the inspection of SSL traffic (DPI-SSL) easier with a better end user experience, Capture Client enables administrators to push SSL certificates to the endpoint much easier than before.

On top of this, Capture Client features an advanced antivirus engine designed to stop the most ingenious malware with a rollback option to return to a previously uninfected state. Furthermore, Capture Client Advanced integrates with SonicWall Capture Advanced Threat Protection (ATP) to examine suspicious files to better stop attacks before they activate.

Administrators can now catalog all applications on every Capture Client protected endpoint with reporting on known vulnerabilities within the ecosystem.

The Global Dashboard has been designed to let MSSPs see the number of infections, what vulnerabilities are present and the version of Capture

Client installed by each tenant. They can see what and who is being blocked the most by Content Filtering, and they can see which devices are online and operating as well. Global Policy allows administrators to apply a single baseline policy to all tenants. This makes it easier to spin up new tenants and quickly create protections for new threats across all tenants on this policy.

SonicWall Capture Client features include:

- Security enforcement
- DPI-SSL certificate management
- Continuous behavioral monitoring
- Highly accurate determinations achieved through machine learning
- Multiple layered heuristic-based techniques
- Application Vulnerability Intelligence
- Unique rollback capabilities
- Capture Advanced Threat Protection network sandbox integration
- Global Dashboard and Global Policy with Inheritance
- One-click lookup of suspicious files against Capture ATP's threat intel database of convictions and acquittals
- Content Filtering to enforce web policies and block malicious IP address, URLs and domains on devices away from the network
- Policy-based Device Control to block potentially infected storage devices

Advanced Security Services

SonicWall network security firewall services 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.

SonicWall offers three subscription bundles on Gen 7 series firewalls: Threat Protection Services Suite, Essential Protection Services Suite and Advanced Protection Services Suite. The Threat Protection Services Suite includes basic security services needed to ensure that the network is protected from threats in a cost-effective bundle. Add SonicWall Essential bundle to gain essential security services needed to protect against known & unknown threats, while Advanced tier offers advanced security to extend the security of your network with added cloud essential security services.

Threat Protection Services Suite, available only on TZ270/370/470 series, includes Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Deep packet inspection of TLS/SSL-encrypted traffic (DPI-SSL) and 24x7 Support.

Essential Protection Services Suite includes Capture Advanced Threat Protection with RTDMI Technology, Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Comprehensive Anti-Spam Service, Deep packet inspection of TLS/SSL-encrypted traffic (DPI-SSL) and 24x7 Support.

Advanced Protection Services Suite includes Capture Advanced Threat Protection with RTDMI Technology, Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Comprehensive Anti-Spam Service, Deep packet inspection of TLS/SSL-encrypted traffic (DPI-SSL), 24x7 Support, Cloud Management, Cloud-based Reporting for 7 Days and optional Premier Support.

Inspect Deep Memory

A patent-pending technology, the SonicWall Real-Time Deep Memory Inspection (RTDMI) engine proactively detects and blocks unknown mass-market malware via deep memory inspection in real time. Available now with the SonicWall Capture Advanced Threat Protection (ATP) cloud sandbox service, the engine identifies and mitigates even the most insidious modern threats, including future Meltdown exploits.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Cloud App Security

The SonicWall Cloud App Security solution protects popular SaaS email, collaboration and productivity applications including Office 365 email, SharePoint, OneDrive, G-Suite, Dropbox and Box.
Its protection coverage includes:

- Business Email Compromise (BEC)
- Data Loss Prevention (DLP)
- Account Takeover (ATO)
- Advanced malware and zero-day threat in malicious attachments and stored files
- Targeted phishing
- Fraud attempts

Cloud App Security uses advanced user profiling and behavior analytics with over 300 threat indicators to determine if legitimate accounts are being exploited by cybercriminals. Using ML and AI capabilities, the solution blocks impersonation attacks, including retroactive scanning of activities.

For SaaS and file-sharing applications such as OneDrive, Cloud App Security applies SonicWall Capture ATP's multi-engine sandbox to detect never-before-seen malware. It does both historical and real-time scans of files and data, whether at rest or traversing a SaaS environment, internally or cloud-to-cloud. Additionally, the solution's DLP feature protects data at rest by limiting access to only sanctioned applications and preventing unauthorized data uploads.

As a SaaS service, Cloud App Security is can be activated and operational within minutes. With unlimited scalability, the solution helps any size organization immediately add protection for its SaaS application users, whether a few hundred or hundreds of thousands distributed across the globe. Every SaaS app has a separate policy engine, each with its own rules and enforcement capabilities. This way, you can commit a specific policy for each SaaS application based on your security requirements for each.

Without the need to install and manage hardware and software, Cloud App Security eliminates the capital expense, complex installation and on-going maintenance costs associated with deploying an on-prem alternative solution.

Learn more about SonicWall Cloud App Security at www.sonicwall.com/cloud-security

SONICWALL

Cloud Edge Secure Access

Evolution of Traditional VPN to Zero-Trust Security

Today's employees want the flexibility to work from anywhere — and today's organizations want to take advantage of the cost savings and operational efficiencies offered by the cloud.

But traditional VPN solutions weren't built for this new reality. Deploying one can take days or even weeks. Supply availability issues mean they may or may not be available, and once you have one in place, it can be difficult to schedule downtime.

Worse, they can offer a back door into your network, as any successful login grants broad network access and allows for lateral movement within the network subnet.

And because the user traffic loops through the on-premises VPN concentrator instead of going directly to the cloud, VPN creates latency that decreases efficiency and degrades users' cloud experience.

Gartner predicts that by 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of Zero-Trust Network Access (ZTNA).

Zero-Trust Network Security to Protect High-Value Assets

With Cloud Edge Secure Access, SonicWall offers a ZTNA solution that overcomes these problems while providing a host of other benefits. At the core of SonicWall Cloud Edge Secure Access are three essential capabilities:

- Least-Privilege access to protect corporate assets
- Fast self-service deployment
- Cloud-direct, reliable access from anywhere

As a cloud-native service, it delivers a simple Network-as-a-Service (NaaS) for site-to-site and hybrid cloud connectivity with integrated Zero-Trust and Least-Privilege security.

- Device Posture check (DPC) grants network access only to authenticated and compliant devices
- Software-defined micro-segmentation policies effectively prevent breaches from spreading
- Network Traffic Control (NTC) is a stateful firewall-as-a-service (FwaaS) that provides policy-based protection by defining who can access what resource and from where

Organizations can now empower remote workforces and protect high-value business assets at the same time.

Worldwide cloud-native service that takes minutes to deploy

SonicWall Cloud Edge is supported by over 30 global points of presence (PoPs).

The global service allows IT managers to connect a branch office and deploy the service in 15 minutes. And end-users can install the SonicWall Cloud Edge client and become productive in 5 minutes.

The infrastructure is built on the Software-Defined Perimeter (SDP) architecture, which separates the centralized controller from the gateways which act as trust brokers.

By distributing the SDP gateways, Cloud Edge Secure Access can scale rapidly, maintain high performance and deliver the best cloud experience possible.

Furthermore, the separation of functions also makes Cloud Edge Secure Access impervious to common cyber threats, such as DDoS, Log4j Exploits, public Wi-Fi hijacking, SYN flood, and Slowloris.

Additional Benefits:

- Security solution for distributed enterprises and remote workforce
- Instant, secure access to physical sites and resources on hybrid clouds
- Scales from 10 users to thousands of users
- Supports client-less web access with any public devices
- High-performance WireGuard encryption
- Cloud Identity Provider and SIEM integrations
- Modern SSO and MFA Integration
- SIEM integration
- Multi-tenancy for MSSPs
- Network Traffic Control (NTC) enables firewall-level protection by defining who can access specific network, services and from where
- Device Posture Check (DPC) grants network access only to authenticated and compliant devices.
- Available in USA, Europe, Middle East and Asia

Learn more about SonicWall Cloud Edge Secure Access at www.sonicwall.com/products/cloud-edge-secure-access

Secure Mobile Access

The SonicWall Secure Mobile Access (SMA) series is the unified secure access gateway for organizations

facing challenges in mobility, work-at-home, 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-premises, 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 a million 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.

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 and cloud platforms such as Hyper-V, VMWare ESX/ ESXi, KVM, AWS and Azure. Whether you choose to deploy physical appliances, virtual appliances or a combination of the two, SMA fits seamlessly into your existing IT infrastructure.

SMA Web Application Firewall

The SonicWall SMA100 series Web Application Firewall (WAF) enables a defense-in-depth strategy by augmenting perimeter security to protect your web applications running in a private, public or hybrid cloud environment. SMA100 series WAF offers web application protection and information disclosure protection while accelerating web application delivery capabilities that enable application-aware load balancing, SSL offloading for resilience and an enhanced digital engagement and experience.

Additional benefits also include:

- Protection against known and zero-day vulnerabilities with virtual patching and custom rules
- Defense against latest vulnerabilities and threats outlined by OWASP, including SQL injection and cross-site scripting (XSS)
- Supports clientless Zero-Trust Access via a web-browser for convenient use with any public device.

- Strong session management and authentication requirements such OTP, 2FA and SSO
- Ensure high-availability server protection against application DoS/DDoS attacks

Management and Reporting

SonicWall provides an intuitive 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 configuration can manage 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 third-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/products/remote-access/

Email Security

Email is crucial for your business communication, but it is also the number-one attack vector for threats such as ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses. 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.

Also, to manage costs and resources, organizations are adopting Microsoft Office 365 and Google G Suite. While these offer built-in security functionalities, to combat advanced email threats organizations require a next-generation email security solution that seamlessly integrates with Office 365 and G Suite, 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. It is available in a range of hardware appliance options that scale up to 10,000 users per appliance. SonicWall Email Security is also available as a virtual appliance or as a software application. This 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 machine learning, heuristics, reputation and content analysis, time-of-click URL protection, and sandboxing for attachments and URLs to deliver comprehensive inbound and outbound protection.

The solution also includes powerful email authentication standards to stop spoofing attacks and email fraud. These include Sender Policy Framework (SPF); Domain Keys Identified Mail (DKIM); and Domain-based Message Authentication, Reporting and Conformance (DMARC).

- Stop advanced threats before they reach your inbox
- Protect against email fraud and targeted phishing attacks
- Get up-to-date security with real-time threat intelligence
- Secure your cloud email service (Office 365, G-Suite)
- Enable email data loss prevention and compliance
- Easy management and reporting
- Flexible deployment options

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 for Office 365 and G suite 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 and G suite.

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 fundamental to good preventative security practice. It also forms the basis for 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 robust and uniform security defense and response strategy across their wired, wireless and multi-cloud networks. In addition, the total 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 Network Security Management

SonicWall Network Security Manager (NSM) offers your organization everything it needs for a unified firewall management system. It empowers you with tenant-level visibility, group-based device control and unlimited scale to centrally manage and provision your SonicWall network security operations. These operations include deploying and managing all firewall devices, device groups and tenants, orchestrating and enforcing consistent configurations and security policies across your SD-Branch and SD-WAN environments, and monitoring everything from one dynamic dashboard with detailed reports and analytics. NSM enables you to do all this from a single user-friendly cloud-native console that can be accessed from any location using any browser enabled device.

For service providers, NSM provides complete multi-tenant management and independent policy control isolation across all managed tenants. This separation encompasses all NSM's management features and functions that dictate the firewall operation for each tenant. As a result, you can construct every tenant to have its own set of users, groups and roles to conduct device group management, policy orchestration, and all other administrative tasks within the boundary of the assigned tenant account. These open opportunities for MSP/MSSPs to increase their security services agility while reducing the operating expenses and complexities of supporting a solely owned infrastructure.

SonicWall Analytics

SonicWall Analytics transforms data into decisions and decisions into actions that solve security problems and prevent them from reoccurring.

It is a robust traffic monitoring and analysis service, providing an eagle-eye view into everything inside the network security environment. The intelligence-driven analytic engine aggregates, normalizes and contextualizes security data, including network traffic and user activities flowing through the firewall and wireless access points, giving administrators a direct line of sight into the threat intelligence of their networks and users in near real-time.

Armed with insightful analytics and reports, organizations have the intelligence and capacity to find and tackle security and operational issues more efficiently. The drill-down capabilities let security teams investigate, analyze and take evidence-based actions against suspicious or risky user activities and behavior with greater visibility, accuracy and speed. Also, they can focus their valuable time and effort on orchestrating rapid response and remediation actions to those security risks that matter instead of reacting to every event.

[1] NSM SaaS includes reporting and analytics features.
[2] NSM On-Prem requires a separate SonicWall Analytics On-Prem install and license for the reporting and analytics features.

Moreover, weaving Analytics into the business process helps operationalize the analytics by automating real-time, actionable alerts; orchestrating security policies and controls in a proactive and automated fashion; and monitoring the results for security assurance.

SonicWall Wireless Network Manager

SonicWall Wireless Network Manager (WNM) globally integrates management of SonicWave Access Points and SonicWall Switches. As part of the SonicWall Capture Security Center ecosystem, it enables unified visibility and management across wired and wireless networks.

Cloud-based and user-friendly, WNM simplifies access, control and troubleshooting on a single-pane-of-glass dashboard. Using WNM admins can create single policies at the tenant level and push them down to various locations and zones, or drill down on managed devices for granular data. WNM is highly scalable, capable of managing from a single site to global enterprise networks with tens of thousands of managed devices.

Prior to access point deployment, a wireless site survey can help ensure performance and productivity. The WNM integrated Wi-Fi Planner tool helps strategically deploy access points to optimize Wi-Fi user experience and avoid costly mistakes.

SonicWave Access Points and SonicWall Switches use Zero-Touch Deployment to onboard automatically in minutes using the SonicExpress mobile app. Provisioning is easy and can be done remotely, saving time and money.

Automatic firmware and security updates keep managed devices up to date. In case of an Internet outage, access points and switches can continue to work without WNM, ensuring business continuity.

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

Professional Services and Support

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 NS*sp*/NS*a*/TZ Series/ SMA/Email Security/GMS.

Learn more: www.sonicwall.com/en-us/support

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 SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com

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

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

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