SonicWall Product Line: At-A-Glance

Next-Generation Firewalls

High End: NS*sp* Series
Firewalls are designed for large distributed enterprises, data centers and MSSPs, offering high-speed protection, high port density and up to 100 Gbps firewall inspection throughput.

Mid-Range: NS*a* Series
Industry-validated security effectiveness and performance for mid-sized networks, branch offices and distributed enterprises.

Entry Level: TZ Series
Integrated threat prevention and SD-WAN platform for home, small/ medium organizations and SD-Branch deployments.

Virtual: NS*v* Series
Virtual firewalls with flexible licensing models to shield all critical components of your public and private cloud infrastructure.

SonicWall firewalls include DNS and reputation-based content filtering to block malicious websites and applications, and help guide policies on web content display using reputation scores. Expanded storage for audit files, Network Access Control (NAC) integration and automated updates increase ease-of-use.

SonicWave Series

Advanced security, performance and scalability enhanced by Wi-Fi 6 support, managed through the cloud with SonicWall Wireless Network Manager or Network Security Manager.

SMA Series

Simple, policy enforced secure access to network and cloud resources.

SonicWall Switch

Delivers intelligent switching for next-generation secure connectivity of SMB and SD-Branch deployments.

Email Security

ESA Series
A multi-layered solution that protects against advanced email threats; delivered in appliance, VM, and cloud SaaS form factors.

Capture Security appliance (CS*a*)

On-premises file testing and malware prevention.

Management & Analytics

Global Management System (GMS)
Network Security Manager
Wireless Network Manager
Govern centrally, manage risks and comply. Provide reporting and gain insights into traffic and threats. Automate workflows and updates.

Capture Client

A unified client platform with a global dashboard that delivers multiple endpoint protection capabilities, including advanced malware protection, sandboxing, Application Vulnerability Intelligence, and roll back in case of infection.

Cloud Edge Secure Access

A powerful SaaS application that delivers simple network-as-a-service for site-to-site and hybrid cloud connectivity to AWS, Azure, and Google Cloud. In the process, it combines Zero-Trust and Least-Privilege security approaches into one integrated offering.

Cloud App Security

A cloud-native solution that delivers next-gen security for SaaS applications, such as Office 365 and G Suite, to protect email, data and user credentials from advanced threats while achieving compliance in the cloud.

Next-Gen Firewall Subscription Services

Threat Protection Service Suite
includes basic security services needed to ensure that the network is protected from threats in a cost-effective bundle. Available only on TZ270/370/470 series, this bundle includes Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Network Visibility and 24x7 Support.

Essential Protection Services Suite
provides all essential security services needed to protect against known & unknown threats. This includes Capture Advanced Threat Protection with RTDMI Technology, Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Comprehensive Anti-Spam Service, Network Visibility and 24x7 Support.

Advanced Protection Services Suite
provides advanced security for the network. This bundle includes essential bundle services along with cloud management and cloud-based reporting for 7 days.

Learn more at sonicwall.com

Qualifying Questions

Next-Gen Firewalls

- How do you prevent access to malicious websites or avoid inappropriate content display?
- Do you have different solutions for DNS and content filtering?
- Can you keep up with the increase in bandwidth resulting in gigabit or multi-gigabit performance needs?
- Is your current firewall able to perform threat inspection at the rate of incoming threats?
- What are your performance requirements criteria?
- Total number of users/networks behind the firewall?
- Total number of sessions/connections at peak?
- How many remote sites and users will be connecting to the firewall?
- How do you measure the effectiveness of your security controls?
- What type of internet connection do you have? What is the speed?
- What are you doing to protect against new threats like zero-day attacks?
- Can your sandbox detect and block threats hidden in deep memory?
- How many engines does your sandbox incorporate?
- Can your sandbox hold the files at the gateway before being released?
- Do you know whether or not your organization's firewall is inspecting HTTPS traffic?
- Have you had network service disruptions or downtime due to inspecting HTTPS traffic?
- Is your virtual firewall as robust as your physical firewall?
- How are you securing your public or private cloud environments?
- Are you able to implement proper security zoning and micro-segmentation on your virtual network?
- Do you have complete visibility and control of your virtual traffic?
- Would you be interested in reducing costs by replacing MPLS with SD-WAN for secure private networking?

Capture Client

- Do your endpoints need consistent advanced protection against ransomware and encrypted threats?
- How easily can you enforce policy compliance and license management across all endpoints?
- Do you struggle with the visibility of endpoints and management of your security posture?
- Does your endpoint security product connect to a sandbox environment?
- Can you catalog the applications installed on endpoints and know how many vulnerabilities are contained within them?
- Does your current solution continuously monitor your system's health?
- Can you roll back the damage caused by ransomware to a previously known clean state?
- How quickly can you add or change policies for tenants?

Cloud App Security

- Do you use O365 or G Suite?
- Are you using Proofpoint or Mimecast to secure O365/G Suite?
- Are you scanning internal O365 email?
- How many sanctioned SaaS apps is your organization using?
- Do you struggle with enforcing compliance for data stored in SaaS applications?
- How will you know if your users' credentials are compromised?
- Do you have visibility into who is accessing the data, from where, and when? (BYOD)

Inspect Deep Memory

A patented 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.

SonicWave Series

- Are your employees/partners/customers complaining about slow Wi-Fi performance?
- What would be the maximum number of wireless users at any one time?
- Do you have concerns about the cost of adding a secure wireless solution into your network?
- How familiar are you with the 802.11ax wireless standard?
- Do you need flexibility to manage access points in multiple locations?
- Have you planned your Wi-Fi network effectively?
- Would you need APs to be untethered from firewalls?
- Do you worry about providing advanced security functionalities on your Wi-Fi network?
- Are guest services important to you?
- Would you require customized guest login portal for guest onboarding?

SonicWall Switch

- Do you need gigabit-capable access switches to power PoE-enabled devices?
- Is a unified security posture with unified visibility and management important to you?
- Are you facing solution challenges with 3rd party switches that work with SonicWall ecosystem?
- Do you need your switches untethered from firewalls?

Secure Mobile Access

- What is your current remote workforce access strategy?
- What are your thoughts about employing a zero-trust network access approach?
- How are you providing users secure access to company resources and applications hosted on-prem and cloud?
- Do you have visibility into every users and device that is accessing your network?
- How are you currently protecting your business-critical web properties and web servers?

Email Security

- Are you concerned about advanced email threats such as ransomware, spear-phishing and Business Email Compromise?
- Does your current email security solution provide Advanced Threat Protection capabilities?
- Are you concerned that emails containing confidential information might be leaked?
- How do you comply with regulations such as GDPR, Sarbanes-Oxley, GLBA or HIPAA?
- Are you interested in offering managed email security services to your clients? (MSSPs)

Management & Analytics

- How do you keep up with firmware updates?
- How do you enforce security policies across your organization?
- What problems could you solve by unifying your security solutions under one common management platform with a single-pane of glass experience?
- What operational advantages will you gain if you can centrally manage all your firewalls, APs and switches from any location using one cloud-console?
- How confident are you of your ability to demonstrate cyber-security compliance such PCI, HIPPA and GDPR?
- How would it change your security posture if you were able to better detect and respond to threats and risks with speed and accuracy?
- What value would you and your leadership team gain from full visibility into cyber threats and risks to your business?
- Do you need integrated wireless and switch management in a single dashboard?

Cloud Edge Secure Access

- Do you have a lot of sensitive data? Are you concerned about over-privilege users?
- Are you concerned about the increasing regulations for data protection and information security?
- Do you need to control the interactions between employees, external business partners, and sensitive resources?
- How many branch offices do you have? How efficiently can you onboard a new one?
- How long does it take you to securely onboard a remote user?

Datasheet-ProductLineAtAGlance-JK-10098