SONICWALL PRODUCT LINE: AT-A-GLANCE

Next-Generation Firewalls

High End: NS*sp* 12000 Series
NS*sp* 12800/12400

Uncompromising security, performance, scalability, and visibility

Mid-Range: NS*a* Series
NS*a* 9650/9450/ 9250/6650/5650/4650/ 3650/2650

Fast, proven security against the latest threats for every connection, encrypted or unencrypted

Entry Level: TZ Series
TZ600/TZ500/TZ400/TZ300/ SOHO

Complete wired and wireless security and performance in an entry-level firewall

Virtual: NS*v* Series
Virtual firewalls to shield all critical components of your virtual and cloud environments

Wireless Security

SonicWave Series
SonicWave 432e/432i/432o

Security and performance for the mobile network

Secure Mobile Access

SMA Series SMA EX9000/8200v/7200/6200/ 500v/400/200

Simple, policy enforced secure access to network and cloud resources

Email Security Series

ESA 9000/7000/5000/ VM Software/Hosted Service

A multi-layered solution that protects against advanced email threats

Management & Analytics

Capture Security Center
Global Management System (GMS)
Analytics

Control and knowledge of your network is power

WAN Acceleration Series

WXA 6000 (SW)
WXA 5000 (VM)/500 (SW)

Significantly enhance application transfer performance and increase employee productivity

Capture Client

A unified platform for today's threat landscape that protects endpoints wherever they are

Web Application Firewall (WAF)

Web application security, data leak prevention and regulatory compliance, on prem or in the cloud

Cloud App Security

SonicWall Cloud App Security is a cloud service that provides CASB-like functionality, delivering real-time discovery, visibility and control of cloud application usage on the network.

Next-Gen Firewall Subscription Services

Included in Advanced Gateway Security Suite (AGSS); Combined with Next-Gen Firewall in TotalSecure Advanced Edition

- Capture Advanced Threat Protection (ATP) multi-engine cloud-based sandboxing
- Gateway Anti-virus and Anti-spyware
- Intrusion Prevention Service
- Application Control
- Content/Web Filtering Service
- 24x7 Support

Software-as-a-Service (SECaaS)

Outsource your network security with our turnkey solution

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.

Learn more at: www.sonicwall.com/en-us/products

Qualifying Questions

Next-Gen Firewalls

- How do you measure the effectiveness of your security controls?
- What is your remediation plan for identified security gaps?
- How do you reduce the risk of vulnerable web applications your users may access?
- What type of internet connection do you have? What is the speed?
- Do you need to sacrifice performance to get better security on your network?
- What are you doing to protect against new threats like zero-day attacks?
- How capable is your team at patching vulnerabilities within 12 hours of patch release?
- 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 most web sessions are encrypted, and if your firewall can decrypt and inspect them?
- 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?
- For virtualized environments, is your virtual firewall solution as robust as your physical firewall solution?
- How are you securing your public/cloud environments?

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?
- Does your current solution continuously monitor your system's health?

Web Application Firewall

- Are you confident your web applications are protected both on prem and in cloud environments?

Cloud App Security

- Do you have visibility into the cloud application usage in your network?
- Are you aware of the how much data is being transmitted to risky applications?
- How easily can you enforce control on sanctioned and unsanctioned IT applications?

Wireless Security

- 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 802.11ac Wave 2 wireless standard?

Secure Mobile Access

- Is your organization currently moving or planning to move business applications and resources to the cloud?
- Does your organization use SaaS applications such as Salesforce, Office 365 or Concur?
- Do your employees use Dropbox or personal email to share files?
- Are your employees managing multiple URLs and passwords?
- What is your current mobility/BYOD strategy?
- Do you have visibility into every device that is accessing your network?

Email Security

- Are you concerned about advanced email threats such as ransomware, spear-phishing and Business Email Compromise?
- Are you using, or planning to use Office 365 or G Suite for email?
- 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 & Reporting

- Do you have a distributed enterprise using 5 or more SonicWall appliances or software products?
- Is your distributed enterprise subject to regulations, such as PCI, SOX and HIPAA?
- If an MSP, are you managing 5 or more SonicWall appliances or software products for customers?
- Do you operate a managed services practice, with SonicWall products deployed at customer sites?

WAN Acceleration

- Does your organization have multiple remote office locations? How many?
- Are the offices networked through either a VPN or dedicated WAN circuit (MPLS) connection?
- Do your employees use apps such as Microsoft Windows File Sharing, SharePoint, Office or FTP?
- Would you like to reduce bandwidth consumption and cost without paying to increase capacity?

Learn more at: www.sonicwall.com/en-us/products

© 2018 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.

SONICWALL®