

SONICWALL PRODUCT LINE: AT-A-GLANCE

Next-Generation Firewalls

High End: NSsp 12000 Series NSsp 12800/12400
Scalable, cutting-edge security for large distributed enterprises, data centers and service providers that leverages the power of cloud intelligence



Mid-Range: NSa Series NSa 9650/9450/9250/6650/5650/4650/3650/2650
Industry-validated security effectiveness and performance for mid-sized networks, branch offices and distributed enterprises



Entry Level: TZ Series TZ600/TZ500/TZ400/TZ350/SOHO 250
Integrated threat prevention and SD-WAN platform for small/medium organizations and distributed enterprises



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



Wireless Security SonicWave Series SonicWave 432e/432i/432o/231c/224w/231o
Security and performance built for the next wave of wireless devices, managed through the cloud or firewall



Secure Mobile Access

SMA Series SMA 8200v/7210/6210/500v/410/210
Simple, policy enforced secure access to network and cloud resources



Email Security Series

ESA 9000/7000/5000/VM Software/Cloud 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 client platform that delivers multiple endpoint protection capabilities, including advanced malware protection, sandboxing, device control, and roll back in case of infection



Web Application Firewall (WAF)

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

Cloud App Security

A CASB 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

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

Security-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.

Qualifying Questions

Next-Gen Firewalls

- How do you measure the effectiveness of your security controls?
- What is your remediation plan for identified security gaps?
- 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?
- 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?
- Does your current firewall integrate PoE/PoE+ support or do you need a switch to power PoE-enabled devices?
- Would you be interested in reducing costs by replacing MPLS with SD-WAN for secure private networking?
- Do you need subscription-based licensing for virtual firewalls?

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?
- Do you have the ability to block unknown and potentially infected devices from connecting with endpoints?

Web Application Firewall

- How are you currently protecting your business-critical web properties and web servers?
- What security measures do you have in place that help comply with PCI security requirements?

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)

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?
- Do you need flexibility to manage access points - cloud vs firewall management?
- Have you planned your WiFi network effectively?
- Would you need APs to be untethered from firewalls?
- Do you worry about providing advanced security functionalities on your WiFi network?
- Are guest services important to you? Would you require customized guest login portal for guest onboarding?

Secure Mobile Access

- Is your organization currently moving or planning to move business applications and resources to the cloud?
- Are you providing unified Single-Sign On for on-prem and cloud applications to your users?
- 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?
- 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

- What problems could you solve by unifying your security solutions under one common management platform with a single-pane of glass experience?
- What economic and operational challenges are you experiencing from managing your security infrastructure?
- How confident are you of your ability to demonstrate cyber-security compliance such as PCI, HIPAA 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?

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?