

SonicWall Product Line: At-A-Glance

SONICWALL®



Next-Generation Firewalls

High End: NSsp 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: NSa 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.



SOHO & MicroSMBs: TZ80

Best-in-class threat protection for your small office, home office, IoT, and MicroSMBs, with easy cloud management for remote deployments.

NSV

Virtual: NSv 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 (CSa)

On-premises file testing and malware prevention.



Management & Analytics

Global Management System
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.



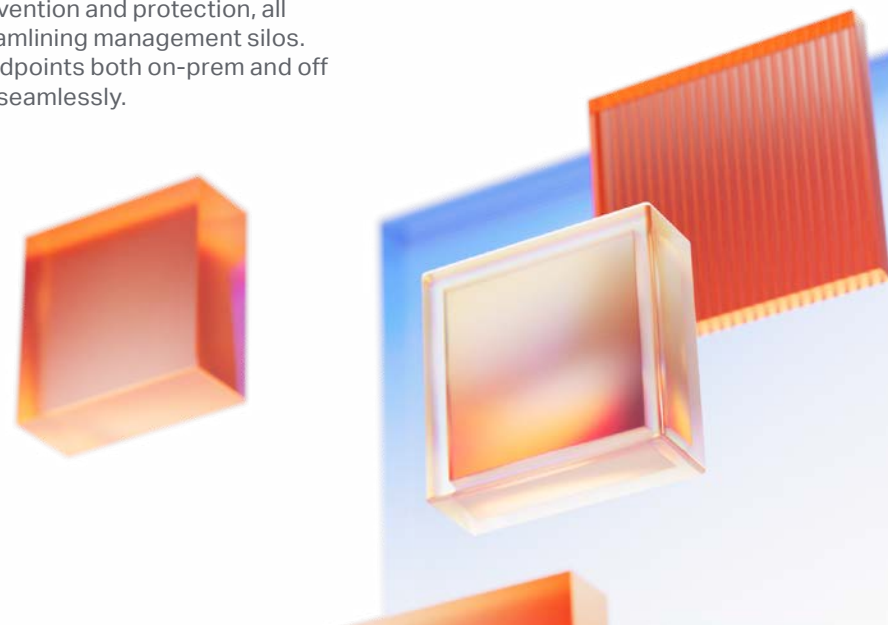
Capture Client

An easy-to-deploy unified client powered by a dual engine that delivers layered defenses and enterprise-grade threat prevention and protection, all while streamlining management silos. Secure endpoints both on-prem and off networks seamlessly.



Cloud Secure Edge

SonicWall Cloud Secure Edge (CSE), formerly Banyan Security, is an easy-to-adopt Security Service Edge (SSE) solution, enabling your workforce to access any resource from any device securely. It delivers simple, secure, zero-trust access to private and internet resources for all your employees and third parties, regardless of their network location. To accomplish that, CSE combines the functionality of multiple traditional network appliances – remote access VPN, web proxy, firewall, etc. – into a unified cloud-delivered solution, improving the security posture and user experience for the entire workforce.





Managed Security Services

Provides the power of a 24/7/365 expert SOC behind the entire attack surface for monitoring and incident response. All services are available without minimums or long-term commitments

Managed Detection and Response

secures endpoints by putting the SOC behind NGAV and EDR tools. SonicWall supports several NGAV/EDR options, including Capture Client, Sentinel One, and Windows Defender. The service includes twice-monthly configuration audits and a free 30-day proof of concept.

Cloud Detection and Response

comprises two offerings: Cloud Threat Analytics provides SOC monitoring for many common cloud-based business applications, like Microsoft 365, Salesforce, and Slack. Cloud Email Security uses machine learning to prevent phishing emails from reaching users' inboxes. SOC monitoring is available for CES when purchased with Cloud Threat Analytics or as an add-on.

Network Detection and Response

brings SOC monitoring to firewall logs. NDR can be applied to any firewall from any maker.



Next-Gen Firewall Subscription Services

Threat Protection Service Suite

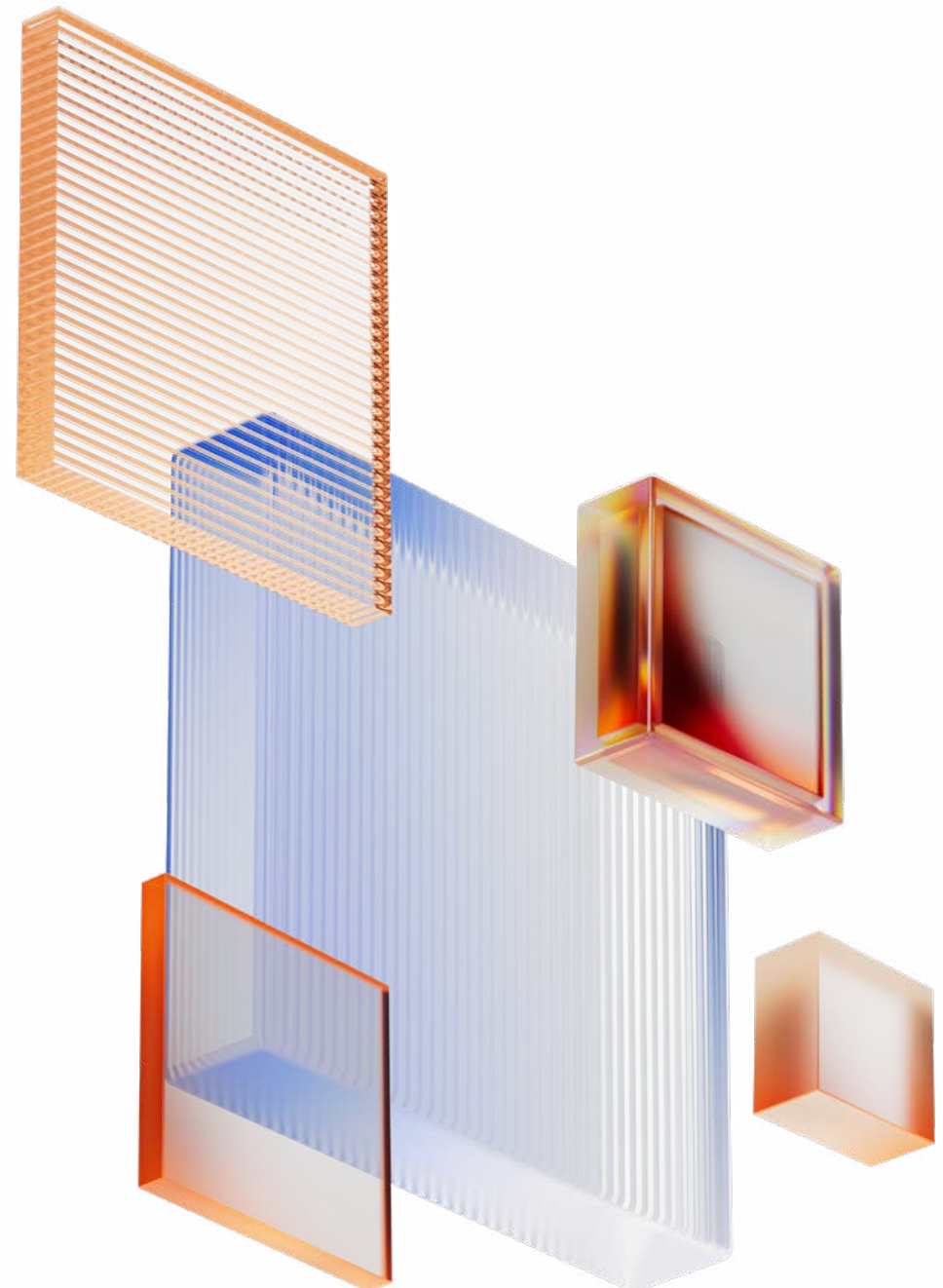
includes basic security services needed to ensure that the network is protected from threats in a cost-effective bundle. Available only on TZ270/370/470 series, this bundle includes Gateway Anti-Virus, Intrusion Prevention and Application Control, Content Filtering Service, Network Visibility and 24x7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



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?

Managed Security Services

- How do you address alerts that come in during weekends or off hours?
- How long, on average, does it take you to identify and deal with an alert?
- What steps does your team take to identify and respond to relevant threats?
- How does your team stay current on new threats in the cyber landscape?
- Do your clients' insurance companies require a 24/7 SOC?
- Do your clients use cloud apps like O365, Salesforce, Slack, etc.

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?

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.

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 Secure Edge

- Do you have users who need to access files outside the office or are moving to the cloud?
- Do you have a single solution to manage remote access, web access, and device posture checking for all your devices?
- Are you looking to limit access to users across your organization?
- Do you often find the need to provide temporary secure access to 3rd party users to your applications?
- What challenges do you face in managing your current security infrastructure?
- How do you balance the need for robust security with budget constraints?

Learn more at sonicwall.com

