

SALES AID: NSA SERIES FIREWALLS

Industry-validated security effectiveness and performance for mid-sized networks



Key message

The SonicWall Network Security Appliance (NSA) series provides mid-sized networks, branch offices and distributed enterprises with advanced threat prevention in a high-performance security platform. Combining next-generation firewall technology with our patented Reassembly-Free Deep Packet Inspection (RFDPI) engine on a multi-core architecture, the NSA series offers the security, performance and control organizations require.

- Superior threat prevention
- High-performance architecture
- Network control and flexibility
- 802.11ac Wave 2 wireless
- Broad mobility support
- Low TCO

Why your customers will care

Comprehensive security: Integrates patented reassembly-free deep packet inspection technology with on-box and cloud-based threat prevention featuring multi-engine sandboxing, anti-malware, intrusion prevention, web filtering and more

High-performance protection: Examines traffic simultaneously across all protocols – including encrypted SSL/TLS sessions – and ports, without any file size restrictions

Flexible remote access: The only next-generation firewall that does not rely on a third-party app, providing native VPN remote access client for Apple® iOS, Google® Android™, Windows, Mac OS, Kindle Fire, Chrome OS and Linux

Wireless network security: Combines NGFW protection with high-speed 802.11ac Wave 2 wireless to create a wireless network security solution

Greater visibility and control: Gain real-time insight into network activity – users, apps and bandwidth consumption – and make informed decisions

Differentiators

High-performance deep packet inspection (DPI) architecture: Realize the benefits of intrusion prevention, anti-malware, multi-engine sandboxing, DPI SSL and app control without slowing the network

Comprehensive DPI network security: Scan everything including encrypted traffic – no file size limits, no latency, no buffering/proxying – across any port

Advanced threat prevention: Use Capture Advanced Threat Protection, SonicWall's cloud-based multi-engine sandbox service, to detect and prevent zero-day threats.

Wireless network security: Combine an NSA series firewall with a SonicWall SonicWave 802.11ac Wave 2 access point to create a high-speed wireless network security solution

Eliminate unnecessary equipment and costs: Consolidate firewall, wireless access controller, IPS, gateway anti-malware, SSL VPN, and more into a single affordable solution

Whom to talk to

- Network administrator/architect
- IT director/manager
- Small/medium business owner
- Small and mid-sized organizations
- Companies with remote/branch offices
- School campuses and other public institutions

Competition

Fortinet

- NSA firewalls deliver better deep packet inspection performance due to our RFDPI engine which is not bound by file size limitations like Fortinet's is
- SonicWall firewalls running SonicOS have been found to contain only one vulnerability since 2015 compared to more than 15 in FortiOS according to NIST
- We have greater performance and scalability for decrypting SSL traffic and scanning it for threats

Palo Alto Networks (PAN)

- SonicWall firewalls running SonicOS have been found to contain only one vulnerability since 2015 compared to more than 22 in PAN-OS according to NIST
- We offer better price/performance than PAN which leads to a lower TCO
- SonicWall covers other areas of security that PAN cannot including email security, mobile access security and multi-engine sandboxing

Cisco Meraki

- We offer better price/performance than Cisco which leads to a lower TCO
- Our next-generation firewalls can be managed through a single interface or extended through GMS
- SonicWall covers other areas of security that Cisco cannot including network security, identity, clients and endpoint security and security services

	QUALIFYING QUESTIONS	WHAT TO LISTEN FOR
TECHNICAL	<ul style="list-style-type: none"> • Is your firewall over three years old? • Do you know which applications run on your network so you can prioritize business applications and throttle down or block unproductive apps? • Did you know that many web sessions are encrypted, and do you know if your firewall can decrypt and inspect them? 	<ul style="list-style-type: none"> • Securing our network against threats like ransomware is a big concern • We are worried that our existing firewall is not keeping up with the speed of the network • Our users access a lot of different applications and we don't really know which ones, so we want more insight into and control over apps • We don't know if our firewall can scan encrypted connections for threats
	<ul style="list-style-type: none"> • Do you want to provide your users with secure wireless access? • Are your employees/students using their own devices to connect to your network? • How familiar are you with the 802.11ac Wave 2 wireless standard? 	<ul style="list-style-type: none"> • We have employees who need access to the internet that is separate from guests and customers • We use many different personal and IT-issued device types • We're familiar with 802.11ac, but not with 802.11ac Wave 2 advantages
	<ul style="list-style-type: none"> • What would be the maximum number of devices connected to your network at any one time? How many total connections from those devices? • Do you need to manage multiple firewalls from a single location and create consistent policies for wired and wireless networks across your entire organization? 	<ul style="list-style-type: none"> • We're uncertain whether our firewall will deliver adequate protection against threats as our business grows • We manage each device separately • We need to save time by centrally managing multiple devices across different locations
BUSINESS	<ul style="list-style-type: none"> • Are you looking for ways to improve employee productivity? • Are your employees utilizing bandwidth-intensive applications? • Do your wireless users need a high-performance network connection? • Do you have compliance concerns around deploying a security solution? 	<ul style="list-style-type: none"> • We want to enable employee productivity through high-speed wireless connectivity • We need to support collaboration apps (e.g. WebEx), video and voice, etc. • We need a solution to ensure that the company can meet compliance requirements for security
	<ul style="list-style-type: none"> • 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? 	<ul style="list-style-type: none"> • We're concerned that our current firewall may not keep up with network infrastructure changes • We're forced to turn down/off security to get better performance
	<ul style="list-style-type: none"> • Do you have concerns about the cost of adding a security solution into your network? • What are you doing to reduce total cost of ownership across the organization? 	<ul style="list-style-type: none"> • Our budget is tight, so keeping costs to a minimum is important • Adding a complete solution would be nice if it's not too expensive • Lowering TCO is an organization-wide initiative

FOR MORE INFORMATION Contact your SonicWall Channel Account Manager

FOR ADDITIONAL INFORMATION VISIT www.sonicwall.com/en-us/products/firewalls/mid-range