SonicWall Triples Threat Performance, Dramatically Improves TCO with Trio of New Enterprise Firewalls

Submitted by: SonicWall
Tuesday, 29 June 2021

With triple the firewall throughput compared to previous SonicWall appliances, new NSa and NSsp models help organizations keep pace with the speeds of their growing networks

MILPITAS, Calif. — JUNE 29, 2021 — SonicWall today announced three new high-performance firewall models for enterprises and large organizations — NSa 4700, NSa 6700 and NSsp 13700 — designed to accelerate network throughput, stop advanced cyberattacks like ransomware, and securely connect millions of users. Featuring some of the highest port densities in their class, the new appliances help enterprises keep pace with the speeds of their growing networks — all while drastically reducing total cost of ownership (TCO).

“The growing volume of ransomware attacks has enterprises and government agencies moving quickly to evaluate their mitigation capabilities and strengthen their security postures,” said SonicWall President and CEO Bill Conner. “The recent string of highly publicized cyberattacks has catapulted security to the top of the priority list. We’re there to help by delivering multiple options to cost-effectively protect even the largest environments. With higher port densities and more capacity, the new offerings dramatically disrupt the traditional cost structure as organizations need fewer appliances to secure the same environment.”

New NSa Firewalls Disrupt Cost Expectations by Tripling Throughput, Expanding Port Densities
The new SonicWall NSa 4700 and NSa 6700 next-generation firewalls deliver 18 and 36 Gbps of firewall throughput — three times the previous comparable SonicWall appliances. Both also support critical TLS 1.3 encryption standards.

“When designing large networks, high-bandwidth interfaces are a critical component,” said NW Technology owner Ryan Oord. “SonicWall’s new NSa series provides interface options that fit the different needs of varying and sizable networks.”

The NSa models boast some of the highest port densities in their class; the NSa 6700 even offers both 40G and 25G connectivity, delivering multi-gigabit threat protection for large environments. These higher port densities, coupled with hardware redundancy and high availability, allow distributed enterprises to purchase fewer appliances while supporting more secure connections as their networks grow.

The NSa 4700 and NSa 6700 provide up to 115,000 and 153,000 connections, respectively, per second. They also support up to 2 million or 6 million concurrent DPI connections, and up to 4,000 or 6,000 site-to-site VPN tunnels.

High-Performance NSsp 13700 Firewalls Designed To Protect The Fastest, Most Complex Environments
The new SonicWall NSsp 13700 is an advanced next-generation firewall for high-speed threat protection designed for enterprise-class networks and MSSPs that supports millions of encrypted connections.

The NSsp 13700 next-generation firewall delivers elite speeds for threat prevention throughput (45.5

Gbps), IPS (48 Gbps) and IPsec (29 Gbps), and include scalable hardware architecture with high port density. Like SonicWall's other new offerings, the NSsp 13700 supports the latest TLS 1.3 encryption standard.

New Capture Labs Portal Delivers Research Tools, Centralized Repository
Information-sharing and collaboration is a critical component of an organization's defensive posture. SonicWall is consolidating access to threat research and security news through the Capture Labs Portal (http://capturelabs.sonicwall.com/), a free and centralized repository of research tools available to the public where visitors can track malicious actors and remain up to date with latest zero-day vulnerabilities.

To help expedite remediation, the Capture Labs Portal offers a single repository to look up threat signature, CVE details, IP reputation, and URL reputation, making it effortless to do your threat research from a single interface. SonicWall PSIRT advisories and Capture Labs threat researcher blogs with news regarding the latest vulnerabilities can be easily and quickly found out to take actions in response to emerging threats, attack vectors or vulnerabilities.

Simplify Secure SD-WAN Deployment, Management with New Orchestration and Monitoring Capabilities
Enterprises, service providers, government agencies and MSSPs can efficiently manage large-scale deployments with SonicWall's cloud-native Network Security Manager (NSM), which delivers a single, easy-to-use cloud interface for streamlined management, analytics and reporting.

With NSM 2.3, network infrastructure teams can quickly troubleshoot and resolve issues as they monitor secure SD-WAN landscapes in real time. Administrators can monitor the health and performance of complete SD-WAN environments to ensure consistent configurations and drive optimal application performance.

SD-WAN environments are now easily organized using SonicWall's new and intuitive self-guided workflow as well as the use of Templates that allow the provisioning of thousands of remote firewalls efficiently.

Enterprises also can leverage the NSM wizard-based setup process to ensure proper configuration for site-to-site VPN connectivity, and use the monitoring tools to track the connections and ensure optimum performance.

Optimize Productivity with Enhanced Network Visibility, Monitoring and Reporting
Managing employees' internet utilization and behavior can be a substantial challenge for organizations. SonicWall has enhanced network visibility and reporting capabilities across security devices, users, VPN connections and more.

SonicWall Analytics 3.1 delivers Productivity Reports to provide insights into employees' internet utilization and behavior. Generated snapshots and drill-down reports can classify users' web activities into productivity groups such as productive, unproductive, acceptable, unacceptable or custom-defined groups.

Drill-down capabilities enable analysts to easily and quickly pivot and investigate data points of

interest at the user level, and establish evidence-backed, policy-controlled measures for risky users and applications as they unfold in the discovery process.

New VPN Reports allow organizations to summarize what company resources are being accessed inside VPN tunnels, how much bandwidth they are consuming and by whom. Network admins can leverage this information for monitoring business-critical applications, controlling or shaping traffic, and planning for capacity growth.

Zero-Trust Security Offering Expanded to Include More Granular Control
SonicWall also introduced Device Posture Check with SonicWall Cloud Edge Secure Access 1.1, and the addition of new Network Traffic Control that enforces access control to the resources based on user groups, IP addresses, ports and network protocols.

About SonicWall
SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.