ANALYST BRIEF | FEBRUARY 2021

SONICWALL NSa 2700 NEXT-GENERATION FIREWALL (NGFW)

Strategic Analysis vs. Fortinet Fortigate 100F NGFW

Tolly. Analyst Brief

#221102

February 2021

Commissioned by SonicWall

SonicWall NSa 2700 Next-Generation Firewall (NGFW)

Strategic Analysis vs. Fortinet FortiGate 100F NGFW

EXECUTIVE SUMMARY

The term firewall has been part of the IT lexicon for over two decades. Today's threats are radically more sophisticated than in the past and today's next-generation firewalls have came a long way compared to the original invention - and all NGFWs are not the same. It is important to focus on the security features and performance needs that are most important for your environment. SonicWall has designed its NSa 2700 to excel in protection while maintaining an industry-leading price-performance ratio.

SonicWall commissioned Tolly to review the published specifications of its NSa 2700 and compare it to Fortinet's FortiGate 100F. Analysis was mainly focused on evaluating key total cost of ownership (TCO) metrics of the comparable solutions.

The Tolly analysis shows that the SonicWall has a dramatically lower 3-year TCO for HA deployments compared to Fortinet while providing comparable or better security feature set and performance characteristics. The TCO is enhanced by SonicWall's High Availability (HA) licensing policy allowing a single firewall license to be used for both the primary and backup (HA) appliance.

THE BOTTOM LINE

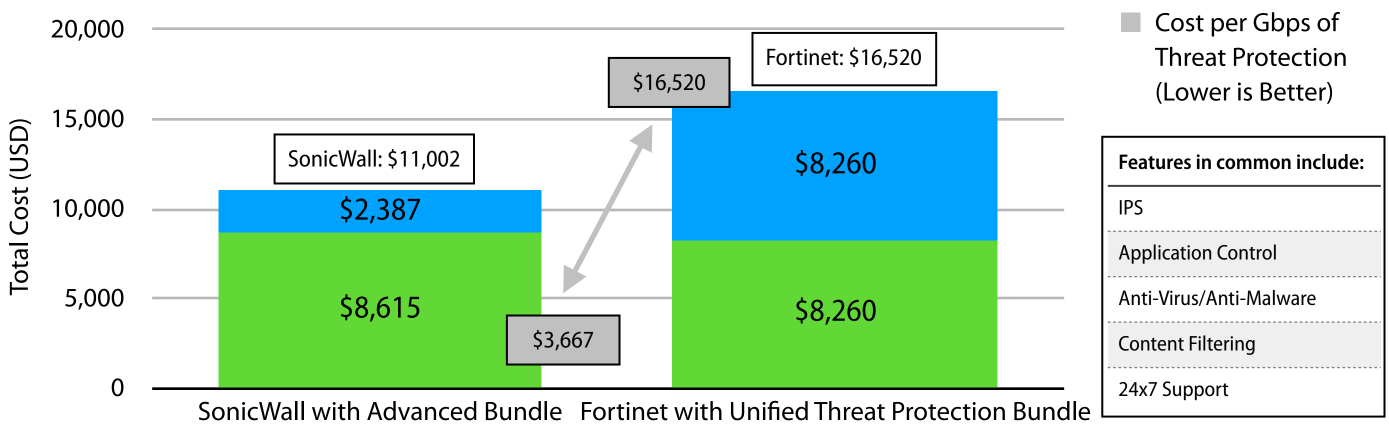
SonicWall NSa 2700 NGFW High Availability solution provides:

1 3-Year TCO that is less than two-thirds that of Fortinet FortiGate (FG) 100F

2 Advertised threat protection throughput that is 3X that of the FG 100F

3 Dramatically lower cost per Gbps for threat protection throughput at $3,667 compared to $16,520 for FG 100F

SonicWall NSa 2700 vs. Fortinet FortiGate 100F
3-Year TCO of High-Availability (HA) Deployment



Features in common include:
IPS
Application Control
Anti-Virus/Anti-Malware
Content Filtering
24x7 Support

Note: List prices include hardware and license costs for 3 years. Fortinet FG-100F-BDL-817-36 x2 for HA.
SonicWall NSa 2700 Total Secure Advanced Edition 3YR 02-SSC-8201, Stateful HA 02-SSC-7367 and 02-SSC-8389.
Fortinet prices from cdw.com, SonicWall prices from SonicWall both as of January 2021.

Figure 1

When making a TCO decision for a security solution, there are three key considerations: price, protection, and performance. The ideal choice is the device that costs the least while providing comparable or better feature set and performance than the alternative.

This analysis is focused on quantifying the cost for a high-availability deployment of an enterprise-class next-generation firewall including all of the essential security features. This type of deployment requires two physical firewall appliances, one that is active and one that is on standby should the primary unit fail.

For similar Fortinet and SonicWall devices providing comparable feature sets, the costs are not similar at all. At $16,520, the Fortinet FG 100F 3-year TCO is more than 1.5x the $11,002 of the SonicWall NSa 2700. See Figure 1.

Price-performance is another useful way of comparing cost. With firewalls, there are many metrics to choose from. Since firewalls are generally configured to provide threat protection (rather than just port filtering), this is a good metric to use. See sidebar "Understanding Firewall Performance."

Fortinet advertises that the FG-100F provides 1Gbps of threat protection throughput. SonicWall advertises that the NSa 2700 provides 3Gbps of throughput[1].

The cost per 1Gbps of threat protection throughput for Fortinet is 4.5X higher than SonicWall at $16,520 compared to $3,667.

Licensing Approaches

SonicWall and Fortinet take dramatically different approaches on how firewall license(s) are handled in HA deployments. Although only one NGFW appliance will ever be active, Fortinet requires customers to buy licenses for two firewalls. In fact, the cost is the same as if customers have deployed two single, non-HA firewalls.

SonicWall does not charge for a separate license for the standby unit. Since that unit will only become active should the primary unit fail, SonicWall allows the standby unit to inherit and use the single, primary license. For SonicWall, that means purchasing two appliances but only a single license.

Understanding Firewall Performance

Customers need to be careful in choosing a firewall solely based on datasheet numbers as test methodologies vary across vendors. While measuring performance some vendors may configure a firewall in less secure mode like flow mode instead of proxy mode and may not turn on needed security features like NAT, IPS, Application Control and AV.

Before comparing performance results between two given firewalls, be certain that the feature configurations were equivalent and that the test traffic scenarios were also equivalent.

In summary, be certain to test traffic profiles and feature sets that are relevant to your deployment environment.

SonicWall notes that its Threat Prevention throughput is measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled in proxy mode.

NGFW High-Availability TCO & Price-Performance Details

Description	SonicWall NSa 2700		Fortinet FG 100F	
	SKU	List Price	SKU	List Price
Primary Appliance + 3-Year Licensing and Support	SonicWall NSa 2700 Total Secure Advanced Edition 02-SSC-8201	$8,615	Fortinet FG-100F-BDL-950-36 (Unified Threat Protection)	$8,260
Secondary (Standby) Appliance + 3-Year Licensing and Support	SonicWall NSa 2700 Total Secure Advanced EditionStateful HA 02-SSC-7367and 02-SSC-8389	$2,387	Fortinet FG-100F-BDL-950-36 (Unified Threat Protection)	$8,260
Total 3-Year TCO		***$11,002***		***$16,520***
Cost Per 1Gbps Threat Protection*		***$3,667***		***$16,520***

Note: Fortinet prices from cdw.com, SonicWall prices from SonicWall both as of January 2021. *SonicWall claims 3Gbps, Fortinet claims 1Gbps. Table 1

[1] Throughput claims not verified by Tolly.

The financial bottom line is impressive. Lower cost for the hardware combined with no license charge for the standby unit and higher throughput claims add up to an impressive financial value.

Performance

Both systems provide 10 or more GbE links along with several 10GbE links and SFP slots for additional media flexibility. Only the SonicWall provides 64GB of system storage, the FG 100F does not provide any. The upper section of Table 2 summarizes all items discussed in this section of the report.

As noted earlier, throughput is directly related to the security task being performed. Vendor-provided performance estimates show that the SonicWall NSa 2700 is specified to provide higher throughput in three key categories: threat protection, IPS, and application control.

Performance also relates to scalability. Both SonicWall and Fortinet are specified to provide 2,000 or more site-to-site tunnels. This likely far exceeds the needs of most deployments. Each device also provides support for 500 concurrent SSL-VPN users.

Feature/Support Bundles

Feature and support bundles naturally vary between vendors. For this comparison Tolly identified key elements in both vendor packages that are likely of high importance to many customers. The lower section of Table 2 summarizes all items discussed in this section of the report.

IPS (Packet Inspection)

The SonicWall IPS features include intra-zone IPS protection, botnet command and control (CnC) detection and blocking, protocol abuse/anomaly identification, anti-evasion technology and zero-day protection against thousands of individual exploits and benefits from automatic signature updates.

The Fortinet data sheet notes that its IPS provides low latency and optimized network performance. Elsewhere, Fortinet notes that its FortiGuard IPS "provides the most up-to-date defenses against stealthy network-level threats. With over 13,000+ IPS signatures covering known vulnerabilities and exploits, the FortiGuard IPS service protects enterprises both from known threats and zero-day vulnerabilities."

Application Control

SonicWall controls applications, or individual application features that are identified by the reassembly free deep packet inspection (RFDPI) engine against a continuously expanding database of over thousands of application signatures. This increases network security.

NGW Comparison of Select Features

Feature	SonicWall NSa 2700 NGFW	Fortinet FG 100F
Performance		
Ethernet Ports	16 GbE, 1 Mgmt., 3 10GbE SFP+	12 GbE, 2 Mgmt./ DMZ, 2 WAN, 2 HA, 2 10Gbe SFP+, 4 SFP Slots, 4 GbE/SFP Shared media pairs
System Storage	64GB	None (requires upgrade to FG 101F)
Threat Protection Throughput	3.0 Gbps	1.0 Gbps
IPS Throughput	3.4 Gbps	2.6 Gbps
Application (Control) Throughput	3.6 Gbps	1.6 Gbps
Site-to-Site IPSec Tunnels	2000	2500
SSL-VPN Users	500	500
Feature/Support Bundles: Key Elements		
	SonicWall Total Secure Advanced Edition	**Fortinet Unified Threat Protection Bundle**
IPS	Yes	Yes
Application Control	Yes	Yes
Anti-Virus/ Anti-Malware	Yes	Yes
Content Filtering	Yes	Yes
DNS Security	Yes	No
24x7x365 Support	Yes	Yes
Cloud Management	Yes	No

Note:Fortinet FG 100F feature and performance data (upper table) excerpted from the Fortinet dataset. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-100f-series.pdf

Table 2

The FortiGate 100F data sheet makes no direct reference to application control. Elsewhere, it notes that its Application Control Service can "improve security and meet compliance with easy enforcement of your acceptable use policy through unmatched, real-time visibility into the applications your users are running. With FortiGuard Application Control, you can quickly create policies to allow, deny, or restrict access to applications or entire categories of applications."

Anti-Virus/Anti-Malware

SonicWall provides multi-layered protection noting that its support is built around the SonicWall Capture Advanced Threat Protection (Capture ATP) that provides sandboxing to analyze suspicious code and block malware from entering the customer network.

Fortinet notes that its FortiGuard Advanced Malware Protection (AMP) is provided with the Unified Threat Protection. This includes anti-virus, mobile malware, botnet, CDR, Virus Outbreak Protection, and FortiSandbox Cloud Service.

Content Filtering

Both SonicWall and Fortinet provide content filtering services (also known as web filtering).

DNS Security

More and more hackers are using the DNS protocol for both inbound hacking and outbound data exfiltration.

SonicWall provides a basic DNS filtering service that can monitor DNS record access and block interaction with domains known to be malicious.

Fortinet does not appear to offer a comparable feature in its Unified Threat Protection bundle.

Management & Support

Both vendors provide 24x7x365 support, but only SonicWall provides cloud management of the devices in the bundle.

Protection

Both SonicWall and Fortinet are members of the NetSecOPEN consortium and have had their products tested by NetSecOPEN labs in 2020 and detailed results of those tests are available on the consortium website.

The information in Table 3 is excerpted from the relevant SonicWall and Fortinet test reports. While the tests were of models other than those discussed in this report, one assumes that the detection capabilities would be the same.

In the NetSecOPEN CVE tests, the SonicWall firewall had an overall block rate of 99.43% compared with an overall block rate of 93.98% for the Fortinet firewall.

NetSecOPEN Common Vulnerabilities and Exposures (CVE) Block Rates (%)

Scenario	SonicWall	Fortinet
Private CVE Test	100%	93.93%
Public CVE Test	98.85%	94.03%
Overall Block Rate	99.43%	93.98%

Tolly Group is not affiliated with NetSecOPEN and this information is presented as a courtesy to the reader. The information presented in this table is publicly available at https://www.netsecopen.org/certifications. The specific products tested by NetSecOPEN were SonicWall NSa 4650 and Fortinet FortiGate 500E. Presumably the products discussed in this paper would have the same results. The reports cited were published in February 2020. For all details, see NetSecOPEN certification documents.

Note: Private indicates CVEs that are not found on the (US) national vulnerability database (NVD) where public indicates threats that are recorded to the NVD.

Source: NetSecOPEN February 2020

Table 3

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at
+1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

td-1-wt-2021-02-19-VerN

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.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

© 2021 SonicWall Inc.

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. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profit, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries. The materials and information contained in this document, including, but not limited to, the text, graphics, photographs, artwork, icons, images, logos, downloads, data and compilations, belong to SonicWall or the original creator and is protected by applicable law, including, but not limited to, United States and international copyright law and regulations.