



November 13, 2017

Fortinet Redefines Expectations for Next-Generation Firewalls in the Enterprise

The FortiGate 500E and 300E Series Set a New Benchmark for Performance, Capabilities and Value

SUNNYVALE, Calif., Nov. 13, 2017 (GLOBE NEWSWIRE) -- **John Maddison, senior vice president of products and solutions at Fortinet**

"Encrypted traffic is becoming a growing hole in enterprise defenses as organizations move to the cloud and increasingly adopt web-based applications and services. This is a struggle for IT and security teams as many firewall solutions simply don't have the power to inspect encrypted SSL traffic and the solutions that do are far more expensive. Fortinet continues to push the boundaries of security performance with our new E-Series NGFWs that enable our customers to thoroughly inspect encrypted traffic without impacting performance."

News Summary

[Fortinet](#)® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced its newest series of Next-Generation Firewalls (NGFW) that enable enterprises to deploy advanced threat protection and SSL inspection at their campuses and branch offices without performance bottlenecks. This industry-leading combination of performance and value helps organizations securely embrace new cloud architectures and web-based services that provide a business advantage in today's digital economy.

- 1 The FortiGate 500E and FortiGate 300E are engineered to serve as the security foundation for enterprise campuses and branch offices - more than doubling the performance of the previous generation without increasing cost.
- 1 The FortiGate 500E is the most affordable security appliance to offer 10GbE connectivity with class-leading threat protection performance.
- 1 The FortiGate 300E delivers the highest SSL performance in its class and provides enhanced features to enable secure SD-WAN.

Enterprise Networking and Security Demands are Changing

Increased adoption of the cloud and web-based applications and services are rapidly changing the security and networking requirements for enterprises who are embracing digital transformation, but also want to ensure they can do so securely. This has increased the demands on firewalls as they provide a natural gateway to manage and secure all the traffic while also providing enhanced networking features required by modern enterprises.

Gartner predicts that: "by 2020, 50% of new enterprise firewalls deployed will be used for outbound TLS inspection, up from less than 10% today." Gartner also states that "many enterprises are looking to firewall vendors to provide cloud-based malware-detection instances to aid them in their advanced threat detection efforts, as a cost-effective alternative to stand-alone sandboxing solutions."¹

It's clear that expectations for firewall capabilities are growing to meet the needs of enterprise networks and [modern NGFWs must evolve](#) to keep up with changing infrastructure and a constantly expanding threat landscape.

Setting New Standards for Security

Both of Fortinet's latest E-series NGFWs leverage the benefits of the Fortinet Security Fabric which enables tightly integrated advanced threat protection capabilities like cloud sandboxing, endpoint protection and threat intelligence. All of the integrated capabilities are orchestrated through Fortinet's FortiOS security operating system which provides top-down fabric topology views for management and visibility that spans the entire infrastructure. FortiOS also enables granular visibility beyond typical application traffic, including individual users, IoT devices, end-point clients and access points.

The FortiGate 500E and 300E also employ Fortinet's CP9 discrete Security Processing Unit that accelerates hardware-intensive intrusion prevention capabilities and SSL inspection to identify threats hidden in encrypted traffic.

Fortinet was recognized as a Leader in the [2017 Gartner Magic Quadrant for Enterprise Network Firewalls](#).¹, Fortinet considers its inclusion as a testament to its continually increasing security capabilities, networking functionality and performance of its solutions to help customers stay ahead of the rapidly evolving threat landscape.

The combination of industry leading security, best-in-class performance and incredible value sets a new benchmark for NGFW appliances in the enterprise.

FortiGate 500E

The FortiGate 500E is ideally suited as a high-performance NGFW for enterprise campus environments and is the industry's most affordable NGFW appliance to offer 10GbE connectivity. This connectivity supports increased throughput performance, especially for hardware-intensive threat protection and deep inspection features needed to secure digital enterprises.

- | 5 Gbps NGFW Throughput
- | 4.7 Gbps Threat Protection Throughput
- | 6.8 Gbps SSL Inspection Throughput

FortiGate 300E

The FortiGate 300E is engineered to suit the needs of branch offices that require NGFW protection with high port density and integrated secure SD-WAN networking capabilities to ensure that locations are always connected through highly reliable, efficient and secure wide area networks.

- | 3.5 Gbps NGFW Throughput
- | 6.8 Gbps SSL Inspection Throughput
- | 3 Gbps Threat Protection Throughput

Additional Resources

- | Please visit the FortiGate Next-Generation Firewall [Homepage](#) for more details about Fortinet's solutions.
 - | Additional details and specifications for the FortiGate 500E can be found [here](#).
 - | Additional details and specifications for the FortiGate 300E can be found [here](#).
- | Follow Fortinet on [Twitter](#), [LinkedIn](#), and [Facebook](#).
- | Join the conversation on the [Fortinet blog](#).
 - | [New FortiGate 300E and 500E, the Next Era of NGFW Has Arrived](#)

¹ Gartner, Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, 10 July 2017

Gartner Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Fortinet

Fortinet (NASDAQ:FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 330,000 customers trust Fortinet to protect their businesses. Learn more at <http://www.fortinet.com>, the [Fortinet Blog](#), or [FortiGuard Labs](#).

FTNT-O

Copyright © 2017 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCloud, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiSIEM, FortiAP, FortiDB, FortiVoice, FortiWeb and FortiCASB. Other trademarks belong to their respective owners.

Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions, such as statements regarding technology releases. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the

uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

Media Contact:

Dan Mellinger
Fortinet, Inc.
408-235-7700
pr@fortinet.com

Investor Contact:

Kelly Blough
Fortinet, Inc.
408-235-7700 x 81612
kblough@fortinet.com

Analyst Contact:

Ron Davis
Fortinet, Inc.
415-806-9892
rdavis@fortinet.com

Source: Fortinet, Inc.

News Provided by Acquire Media