March 10, 2014

Fortinet Expands Existing Distributed Denial of Service (DDoS) Product Family With New Appliances for Mid- to Large-Sized Enterprises and MSPs

New High-Performance Behavior-Based DDoS Attack Mitigation Engine and Custom ASICs Stop More Types of Attacks and Do It 10X Faster Than Competitors

SUNNYVALE, CA -- (Marketwired) -- 03/10/14 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today expands its Distributed Denial of Service (DDoS) product family with four new appliances for data center managers and system architects at mid- to large-sized enterprises and managed service providers (MSPs). The new FortiDDoS-400B, FortiDDoS-800B, FortiDDoS-1000B and FortiDDoS-2000B appliances are designed to detect and help protect against today's most damaging and sophisticated DDoS attacks and feature an innovative 100 percent behavior-based DDoS attack mitigation engine. Combined with a new, single-path custom ASIC that both detects and mitigates DDoS attacks, FortiDDoS is able to detect more types of attacks and performs up to 10X faster than other competing DDoS mitigation appliances.

Innovative Attack and Mitigation Engine
The new behavior-based attack mitigation engine enables FortiDDoS to identify and mitigate current and future threats based on patterns and intent rather than content. Because these appliances don't require signatures, they are able to better protect against zero-day attacks by dynamically monitoring trends versus waiting for a signature file to be updated. A very short blocking period achieved using high-performance ASICs allows the appliance to continuously reevaluate attacks. This reduces the impact of false positives if traffic patterns return to normal. Competing appliances take much longer to detect attacks and block for much longer periods of time leading to higher false positive.

"We've dramatically improved the way we identify DDoS attack types since we released our first appliances in 2012. The adaptive, behavior-based attack monitoring introduced in today's models automatically identifies any type of DDoS attack, including zero-days, and almost immediately takes action to mitigate it," said John Maddison, vice president of marketing for Fortinet. "What's more, we're able to offer this class-leading performance at less than half the cost of our closest competitors."

The FortiASIC Advantage
Fortinet is the only company to use a 100 percent custom ASIC approach to its DDoS products, which eliminates the overhead with CPU or CPU/ASIC hybrid systems. The second-generation FortiASIC-TP2 traffic processor provides both detection and mitigation of DDoS attacks in a single processor that handles all layer 3, 4 and 7 traffic types. Competitors use different combinations of processors where some traffic is assigned to an ASIC, some to the CPU or on some models, everything goes to the CPU itself, which leads to bottlenecks and reduced overall system performance.

"Despite the best efforts by ISPs to defend against DDoS threats, residual and application layer attacks are still able to bring down services in an Internet data center," said Hemant Jain, vice president of engineering for Fortinet. "Fortinet now provides DDoS attack mitigation with up to 24 Gbps of full duplex throughput in the data center to ensure that critical services are always available."

FortiDDoS builds a baseline of normal application activity and then monitors traffic against it. Should an attack begin, FortiDDoS would see this as an anomaly and then immediately take action to mitigate it. Users are protected from known attacks and from unknown zero-day attacks, as FortiDDoS does not need to wait for a signature file to be updated.

FortiDDoS also handles attack mitigation differently than other hardware DDoS attack mitigation appliances. FortiDDoS uses a surgical bi-directional approach by monitoring normal inbound and outbound traffic and then using a reputation scoring system, rates IP addresses that are "good" and others that are participating in the attack. The good traffic is allowed to proceed, but the offending IP addresses are temporarily blocked. If they're determined to be a real threat after repeated reevaluation, they are blocked for a much longer period of time.

Product Specifications

- The FortiDDoS-400B features 4 Gbps full-duplex throughput, 16 1 Gbps RJ-45 copper and SFP ports for LAN and WAN connectivity with support for up to 1 million simultaneous connections.
- The FortiDDoS-800B features 8 Gbps full-duplex throughput, 16 1 Gbps RJ-45 copper and SFP ports for LAN and WAN connectivity with support for up to 2 million simultaneous connections.
- The FortiDDoS-1000B features 12 Gbps full-duplex throughput, 16 10 Gbps SPF+ slots for LAN and WAN connectivity with support for up to 3 million simultaneous connections.

- The FortiDDoS-2000B features 24 Gbps full-duplex throughput, 16 10 Gbps SPF+ slots and 4 10 Gbps SFP+ bypass ports for LAN and WAN connectivity with support for up to 6 million simultaneous connections.

Availability
The FortiDDoS-400B, FortiDDoS-800B, FortiDDoS-1000B and FortiDDoS-2000B are available now.

About Fortinet
Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet