Fortinet Expands Network Security Solution Suite With New Dedicated Distributed Denial of Service (DDoS) Protection Products

Family of High Performance Appliances Helps Today's Enterprises to Defend Against DDoS Attacks

SUNNYVALE, CA -- (Marketwire) -- 04/24/12 -- Fortinet® (NASDAQ: FTNT), a world leader in high-performance network security, today introduced the FortiDDoS product family for enterprises, Web hosting and cloud service providers. The new FortiDDoS-100A, FortiDDoS-200A and FortiDDoS-300A are dedicated appliances that are designed to detect and help protect against today's most damaging and sophisticated DDoS attacks. The appliances feature custom ASICs that are capable of mitigating DDoS attacks while maintaining incredibly-low latency (less than 26 microseconds), preventing loss of availability to critical systems, servers and applications.

Providing granular real-time network traffic visibility and automatic protection against targeted DDoS attacks, the FortiDDoS appliances will be the only solution on the market that supports network virtualization and automatic and continuous traffic baselining. Network virtualization helps prevent attacks on one segment of the network from affecting other segments, thereby preserving availability in virtualized environments of datacenters and cloud-based service providers. The automatic traffic baseline model building is also unique, enabling the FortiDDoS products to build a network behavior model initially and adaptively update it continuously with practically no end-user intervention, resulting in significantly reduced administrative overhead.

"DDoS attacks aren't just an annoyance and minor inconvenience, they are a serious problem that could cause significant liability to businesses today," said Michael Xie, chief technology officer and vice president of engineering at Fortinet. "The damage from a DDoS attack can include loss of revenue, loss of customer confidence, loss of brand equity and potentially huge legal liabilities. A FortiDDoS appliance installed in front of a network infrastructure can act as a shield against DDoS attacks."

"FortiDDoS appliances are easy to deploy and manage, and are designed to recognize today's attack vectors and deliver hardware-accelerated performance to block attacks quickly," said Hemant Jain, vice president of engineering at Fortinet.

"Fortinet appliances' support of virtual instances is a valuable feature," said Michael Suby, Stratecast vice president of research at Frost and Sullivan. "This feature is not only beneficial in supporting multiple layers of defense but also is a cost containment and administration-friendly feature for organizations that have multiple Web properties to protect, and need unique policies for each. Virtual instances can also be effectively used in defense escalation. Rather than have a single set of policies, multiple policy sets can be defined in advance, such that the organization can apply a more stringent set of policies if the preceding policies were inadequate."

Hacktivism via botnets and network testing applications has increased significantly in the last year, which has led to an increase in volumetric and application layer attacks. These attacks bring down sites by filling up Internet pipes and overloading application servers. As businesses consume more software as a service (SaaS) offerings and other public cloud-based services, DDoS attacks have become a serious concern for CIOs and CSOs whether they are moving to the cloud or keeping their systems and data on-premise.

The most common motivations for DDoS attacks today are either financial or political. Financially motivated attackers seek to extort funds from sites by launching an initial attack and demanding payment to avoid future attacks. Politically motivated attackers launch an attack in response to an organization's policies by disrupting the victim's business operations. Regardless of the motive, any downtime affects not only a victim organization's customers, partners and employees, but can damage its brand and credibility as well.

FortiDDoS Highlights
All FortiDDoS appliances feature eight virtualized network partitions with independent protection policies for virtualized environments, automatic traffic profiling and rate limiting context-aware policy enforcement for maximum effectiveness. They also provide real-time and historic attacking traffic analysis that delivers unmatched granular visibility on top attacks, top sources and top attackers. The FortiDDoS family will also utilize an innovative design that eliminates a common performance bottleneck by ensuring there is no CPU or operating system in the path of the packets.

- The FortiDDoS-100A features 1 Gbps full-duplex anti-DDoS throughput, four 1GbpsRJ-45 copper and SFP ports for LAN and WAN connectivity and one terabyte of storage. This model can be used to protect 2 Internet links.
- The FortiDDoS-200A features 2Gbps full-duplex anti-DDoS throughput, eight 1Gbps RJ-45 copper and SFP ports for LAN and WAN connectivity, a redundant power supply and two terabytes of RAID storage. This model can be used to

protect up to 4 Internet links.
- The FortiDDoS-300A features 3Gbps full-duplex anti-DDoS throughput, twelve 1Gbps RJ-45 Copper and SFP ports for LAN and WAN connectivity, a redundant power supply and two terabytes of RAID storage. This model can be used to protect up to 6 Internet links.

Fortinet acquired technology powering these products through its asset purchase from Silicon Valley-based IntruGuard Devices, Inc., which occurred during Q1 2012. The terms of asset purchase are confidential and the amount paid by Fortinet as consideration for the assets is considered immaterial to Fortinet's business.

Availability
The FortiDDoS-100A, FortiDDoS-200A and FortiDDoS-300A are scheduled for release in June 2012.

Follow Fortinet Online: Subscribe to threat landscape reports: http://blog.fortinet.com/feed/; Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2011 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

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