FORTINET

October 7, 2015

# Fortinet Complements Cisco Application Centric Infrastructure With High-Performance SDN Security

## New FortiGate Connector for Cisco ACI Delivers App-Centric Security Automation for Data Center Agility

SUNNYVALE, CA -- (Marketwired) -- 10/07/15 -- Fortinet® (NASDAQ: FTNT) -- the global leader in high-performance cybersecurity solutions, today announced the integration of the Fortinet FortiGate firewall solution into the Cisco® Application Policy Infrastructure Controller™ (APIC)APIC is the controller for Cisco Application Centric Infrastructure (ACI), the industry's most comprehensive SDN architecture, which dramatically reduces TCO, automates IT tasks and accelerates data center application deployments. The new FortiGate Connector for Cisco ACI is designed with the security needs of software-defined data centers in mind, enabling physical and virtual networks to deploy policy-driven application services across Layer 4 - 7 fabrics. This integration further extends the Fortinet Software-Defined Network Security (SDNS) Framework, a first of its kind offering designed to provide advanced threat protection through the integration of security into modern, agile data center environments. Fortinet's leading high-performance cybersecurity solutions integrated with Cisco's Application Centric Infrastructure (ACI) can help joint Cisco and Fortinet customers to significantly reduce data center operating costs without compromising on security or performance.

### *Agile Data Center Security Services*

The promise of the modern data center lies in the business agility that it can facilitate. Traditionally, networking and layer 4 - 7 application services have required manual configuration and constant management to keep pace with changes in the data center. Today, organizations can more nimbly provide rapid, cloud-like services to users, customers and partners. They are also able to consolidate infrastructure components and services so that they are automated, driven by business policies and centrally managed for performance.

The new FortiGate Connector for Cisco ACI delivers application-centric security automation to modern data centers. The solution provides automated and pre-defined policy-based security provisioning for next-generation firewall services, enabling transparent security services insertion anywhere in the network fabric with single-pane-of-glass network management for full visibility on security policy enforcement.

"ACI delivers unique benefits to customers through policy-based automation, greater scalability through a distributed enforcement system, and greater network visibility through the integration of physical and virtual environments," said Ish Limkakeng, vice president, product management at Cisco. "The FortiGate Connector for Cisco ACI delivers security protection for enterprise applications and workloads, while enabling automation for greater business efficiencies and cost savings."

### *FortiGate Connector for Cisco ACI*

The open framework of Cisco ACI enables ecosystem partners such as Fortinet to seamlessly interoperate with the Cisco ACI fabric. The Fortinet SDNS framework provides the visionary path for security integration in a SDN or Network Function Virtualization (NFV) deployment and allows for a seamless experience with Cisco's Layer 2 and Layer 3 network fabric. The FortiGate Connector for Cisco ACI requires two components from Fortinet, the FortiGate device package to Cisco APIC; and FortiGate physical and virtual appliances. The connector allows customers to choose pre-defined application firewall policies and automate security orchestration for FortiGate appliances across Layer 4 - 7 fabrics.

"With the shift to agile, software-defined data centers comes increased security concerns for many organizations," said John Maddison, vice president of product and solutions at Fortinet. "The data center is the heart of the network where application workloads are modified, added, changed, or deleted through manual security provisioning-processes prone to human error. FortiGate Connector for Cisco ACI eliminates these cumbersome processes and automates security policies so they can be centrally orchestrated with better traffic visibility and scalability based on application workloads."

With this new offering, IT administrators can easily define the application security rules for different workloads in the Cisco APIC and configure the policies within FortiGate appliances. When a security policy is triggered during the application deployment lifecycle, Cisco's APIC redirects the application traffic through Fortinet FortiGate appliances for advanced firewall inspection including IP reputation, web filtering, anti-virus, DNS filtering, SSH inspection, IPS, and DDoS without manual intervention.

In addition, the integrated solution enables:

- Better visibility and security correlated with overlay and underlay networks
- Lower TCO from reduced OpEx
- Accelerated application and Layer 4 - 7 network security deployment
- Increased efficiency in service provisioning and network security segmentation

***Supporting Quotes***

"As a long-term joint customer, we see the commitment Fortinet and Cisco share in delivering applications while ensuring IT flexibility. The solution provides the capabilities to configure policies that simplify and automate next-generation firewall services efficiently throughout our infrastructure." - Erik Sohlman, senior manager infrastructure, Axians

***Availability***

The FortiGate Connector for Cisco ACI will be available in Q4 2015.

For more information, please visit: http://www.fortinet.com/products/fortigate/cisco-aci.html.

***About Fortinet***

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments -- be it virtualized/cloud or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at http://www.fortinet.com, the Fortinet Blog or FortiGuard Labs.

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 product 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.

***FTNT-O***

Media Contact
Sandra Wheatley
Fortinet, Inc.
408-391-9408
swheatley@fortinet.com

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

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

Source: Fortinet

News Provided by Acquire Media