ARISTA

NEWS RELEASE

Arista Extends CloudVision for Secure Cloud Networking

10/6/2015

Introduces Macro-Segmentation Services with Check Point, F5 Networks, Fortinet, Palo Alto Networks and VMware

SANTA CLARA, Calif. – October 6, 2015 -- Arista Networks (NYSE:ANET) today announced a new capability for **CloudVision®**, **Macro-Segmentation Services (MSS™)**, that allows next-generation firewalls and Application Delivery Controllers to be enabled automatically for specific workloads and workflows across any network topology. This includes Layer-2, Layer-3 and overlay network virtualization frameworks.

MSS addresses a growing gap in current security deployment models wherein embedded security in the virtualization hypervisors addresses inter-VM communication and physical firewalls address north-south traffic. Yet no solution exists to dynamically insert security services for data centers consisting of a mixture of physical and virtualized workloads. Arista is working with leaders in the industry such as **Check Point**, **F5 Networks**, **Fortinet**, **Palo Alto Networks** and **VMware** to advance and simplify the integration of physical and virtualized resources with its cloud networking technologies.

“We look forward to deepening our partnership with Arista,” said Chad Kinzelberg, senior vice-president of business and corporate development at Palo Alto Networks, “The next phase of our integration efforts aims to offer a seamless bridge between virtual and physical networks and deliver on the security and network segmentation requirements for complex and dynamic cloud networks.”

MSS provides a dynamic and scalable network service to logically insert security devices into the path of traffic, regardless of whether the security device or workload is physical or virtual and with complete flexibility on placement of security devices and workloads.

MSS has the following characteristics:

- Location Independent: This allows larger data centers to centralize and insert security in the path between workloads on demand.
- Easy Integration: By not changing any frame formats, it ensures that any platform can be easily integrated.
- Open: It can fully function if the network is multi-vendor without lock-in or proprietary protocols.
- Agile: Hosts can and do move, so services dynamically move with them to secure the deployment model.
- Seamless Co-existence: It co-exists with defined firewall rules within the security policy framework.

Security as a Service with CloudVision

MSS is one of the services enabled via Arista CloudVision. Since CloudVision maintains a network-wide database of all state within the network, as well as direct integration with hypervisor resources like VMware vSphere and NSX, it is aware of where every workload is within the network and it learns in real time about new devices or workloads that are added to the network, removed from the network, or moved across ports or servers.

Macro-segmentation extends the concept of fine-grained inter-hypervisor security to cloud networks by enabling dynamic security and services of physical to virtual workloads. Macro-segmentation security is a complement to fine-grained security delivered via micro-segmentation that is implemented in the virtual switch of the physical host on which a VM is running.

“We are experiencing accelerated mainstream adoption of VMware NSX network virtualization as enterprise customers recognize the operational, security and economic benefits achieved through a software defined data center approach,” said Hatem Naguib, vice president network and security for VMware. “Working with our strategic partner Arista Networks enables customers to augment NSX micro-segmentation controls by addressing bare metal or physical layer security requirements, ensuring that the agility and security advantages of NSX apply to any workload, anytime, any place.“

By integrating with native APIs provided by leading next-generation firewalls – native APIs that already exist, and with no specific version dependencies – MSS learns what workloads the security policy needs to address or monitor. If the security policy requires a specific logical network topology, Arista’s MSS can instantiate that into the network. The automation capabilities of MSS operate in real-time without any need for network operations to engage a security administrator or vice-versa, and without the network needing to be architected in a manner specific to a specific workload. This capability is critical to successful deployment of security in an enterprise private or hybrid cloud.

MSS with Arista CloudVision enables flexible deployment of services in the network, without forklift upgrades and

without any proprietary lock-ins. Macro-segmentation services is in field trials today and will be generally available in the first half of 2016. Arista will be hosting a webinar on Macro-Segmentation with key partners on **November 19, at 10:00 a.m. PT.**

Supporting Partner Quotes

“Check Point is excited to deliver its industry-leading security protections at the scale and speed of the cloud in conjunction with Arista Macro-Segmentation Services security insertion architecture," said Alon Kantor, vice president of business development, Check Point. "Working with Arista on this innovative cloud security offering will strengthen our mission of protecting private and public cloud infrastructures worldwide."

“Customers have identified a need to respond more quickly to frequent changes in their business. As a result, F5 and Arista are collaborating to enable them to automatically apply a wide variety of **BIG-IP®** network and security services wherever and whenever the applications need them. Our joint goal is to simplify and accelerate application deployment processes as much as possible,” said Phil de la Motte, Senior Director of Business Development, Infrastructure Alliances.

“Fortinet’s Internal Segmentation Firewall (ISFW) secures the Data Center and Cloud across physical and virtual domains,” says John Whittle, vice president of corporate development and strategic alliances at Fortinet. “We are pleased to work with our partner Arista to facilitate the adoption of advanced security services within an open cloud framework.”

About Arista Networks
Arista Networks was founded to pioneer and deliver software-driven cloud networking solutions for large data center storage and computing environments. Arista’s award-winning platforms, ranging in Ethernet speeds from 10 to 100 gigabits per second, redefine scalability, agility and resilience. Arista has shipped more than five million cloud networking ports worldwide with CloudVision and EOS, an advanced network operating system. Committed to open standards, Arista is a founding member of the 25/50GbE consortium. Arista Networks products are available worldwide directly and through partners.

ARISTA, EOS and Spline are among the registered and unregistered trademarks of Arista Networks, Inc. in jurisdictions around the world. F5 and BIG-IP are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries. Other company names or product names may be trademarks of their respective owners.

Additional information and resources can be found at: **https://www.arista.com**

This press release contains forward-looking statements including, but not limited to, statements regarding the

benefits and best practices utilized in the design and implementation of Arista's Cloud Networking Portfolio and the enablement of opex savings and higher service level agreements. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Forward looking statements are subject to risks and uncertainties that could cause actual performance or results to differ materially from those expressed in the forward looking statements including: our limited operating history and experience with developing and releasing new products; product, support or service quality problems; rapidly evolving changes in technology, customer requirements and industry standards as well as other risks stated in our filings with the SEC available on Arista's website at www.arista.com and the SEC's website at www.sec.gov. Arista disclaims any obligation to publicly update or revise any forward-looking statement to reflect events that occur or circumstances that exist after the date on which they were made.

Media Contact:
Amanda Jaramillo
Corporate Communications
amanda@arista.com
Tel: (408) 547-5798

Investor Contact:
Chuck Elliott
Product and Investor Advocacy
chuck@arista.com
Tel: (408) 547-5549