Arista Introduces Secure Cloud Networking

8/21/2018

Partnerships with VMware and Zscaler for hybrid cloud security

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Arista Networks (NYSE:ANET) today announced security capabilities focused on private, hybrid and public cloud networking. Based on Arista's cloud-grade **EOS**® and **CloudVision**® state-of-the-art software, Arista's approach redefines silo security into holistic security designed for a multi-cloud environment. Key integration includes **VMware** NSX Data Center and **Zscaler** for holistic security.

The new security expansion delivers three attributes: extended network segmentation, improved compliance through cognitive controls and new platforms with integrated encryption for wide-area interconnect. These provide customers secure solutions, to reduce operational costs and mitigate threats in the emerging cloud era.

"The challenge to secure an enterprise network is getting more complicated and expensive every day. Siloed security solutions promise to make things easier but actually, have the opposite effect. Security needs to be simplified to be truly useful. Arista's network segmentation approach, to simplify security across the security islands, will help to address these challenges," said Golan Ben-Oni, Global Chief Information Officer, IDT Corporation.

Security in a Cloud and IoT World

Securing the network is a growing challenge, especially with the expanded boundaries of cloud, IoT, and mobility. Siloed security solutions do not align to the broader movement to cloud networking. As with other cloud networking principles, security needs to evolve from the legacy Places-in-the-Network (PIN) to a common approach to address Places-in-the-Cloud (PIC). With PIC-based security from Arista, enterprises can simplify their security architecture with a common framework and set of security capabilities across cloud networking use-cases.

Arista Zone Segmentation with Zscaler's Application Segmentation

As more workloads are deployed in the public cloud and IaaS services, there is a critical need to extend common

security policies both from datacenter to cloud as well as from cloud to cloud. Network segmentation in particular needs to follow a consistent implementation to ensure that security enforcement does not need to be rebuilt for each cloud architecture. Zone Segmentation Security (ZSS), a new capability of Arista's vEOS Router, provides segmentation for inter- and intra-cloud network traffic via stateful policy enforcement. The functionality simplifies the security policy definition and deployment for network operators. vEOS Router, a cloud-agnostic platform, can provide common segmentation functionality across any public cloud platform where vEOS Router is supported, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

Arista and Zscaler are partnering to provide secure access for cloud-based workloads. Zscaler Private Access™ (ZPA™) is a cloud service for securing connections between internal applications and authorized users and it integrates with the Arista vEOS Router, extending the security approach across multiple cloud platforms. This combination brings together Arista's control of east/west traffic with ZSS and Zscaler's zero trust access for all north/south application traffic, delivering secure segmentation from application to user.

Extending VMware's Micro-Segmentation across Virtual and Physical Environments

With a mix of virtual and physical workloads in the datacenter, network segmentation must extend across all workload types. Arista and VMware have collaborated to drive new integration between CloudVision and VMware NSX. Through these efforts, NSX security policies can be enforced natively on Arista switches across a multi-cloud enterprise, enforcing security policies across both virtual and physical workloads. Arista's **Macro-Segmentation Services** (MSS), a CloudVision based offering with Arista's security partner ecosystem (such as Palo Alto Networks, Checkpoint, and Fortinet), allows the enforcement of existing firewall security rules on the traffic to and from physical workloads. This expanded segmentation integrates Arista's MSS with VMware's micro-segmentation capabilities and our firewall partners for end-to-end security.

Compliance and Audit for Cognitive Controls

In today's operational model, it is challenging to manually confirm device software versions, security patch levels and configurations. Arista is introducing a new compliance dashboard designed to simplify operational audit and compliance. A part of CloudVision, the compliance dashboard provides alerts and reporting for configuration or software versions that deviate from the standard. Further, CloudVision automatically learns of new security vulnerabilities, giving the operator the ability to provision software security patches in an automated and hitless manner as well as assess the overall percentage of remediated devices. Arista's consistent software and cognitive API strategy across any EOS instance, be it the datacenter, public cloud, the wide-area network, branch or the campus, creates secure PICs.

New Encryption Platforms

In addition to secure segmentation and compliance, Arista is adding high performance encryption options and new use-cases to secure data transfer between locations:

- Enterprise WAN: the Arista 7020SRG is an all new 10G platform with integrated hardware-based IPSec for site-to-site VPNs over unprotected IP networks.
- Datacenter Interconnect: Expanded range of leaf system choices for point to point encryption with MACsec, including the new 7280CR2M-30 and 7280SRAM-48C6 for wirespeed encryption with 10G to 100G for up to 100km and the 7280SRM-40CX2 with 200G coherent interfaces for metro and long haul links up to 2,500km.
- Secure Service Provider access: Leaf platforms with MACsec options for secure hand-off for hosting, cable and mobile access networks.

Combined with the existing 7500R Series MACsec line cards, these new products expand the choices with additional secure use-cases, while maintaining the EOS advantages.

Availability

The vEOS Router-based Zone Segmentation Security and CloudVision compliance dashboard functionality, new 7020R and 7280R platforms will all be available this quarter in Q3 2018.

Zscaler integration will be demonstrated at the **Gartner Catalyst Conference**, August 20th-23rd in San Diego, CA at Zscaler's Booth #505.

VMware NSX Data Center integration will be demonstrated in the Arista booth at **VMworld**, August 27th-30th in Las Vegas, NV #1030.

Register here for the Secure Cloud Networking webinar on September 13.

For more information, please contact your local Arista sales representative.

Industry Support

'Customers are looking for consistent security policy across virtual and physical infrastructure. By extending VMware NSX Data Center micro-segmentation to physical workloads via Arista CloudVision, customers can eliminate siloed security operations, paving the way for an architectural shift towards holistic security for network wide enforcement.' Tom Gillis, senior vice president and general manager, networking and security business unit, VMware.

“We are excited to partner with Arista to provide our joint customers a SDP-based approach for secure access to private applications as a single, easy to manage solution,” said Manoj Apte, Chief Strategy Officer, Zscaler. “Zscaler Private Access deployed in conjunction with Arista vEOS Router enables an automatically segmented security model that connects users to applications, rather than networks to networks. This joint solution enables enterprises to achieve consistent secure access for applications hosted across multiple cloud platforms with granular visibility.”

About Arista Networks

Arista Networks pioneered software-driven, cognitive cloud networking for large-scale datacenter and campus environments. Arista’s award-winning platforms redefine and deliver availability, agility, automation, analytics and security. Arista has shipped more than fifteen million cloud networking ports worldwide with CloudVision and EOS, an advanced network operating system. Committed to open standards across private, public and hybrid cloud solutions, Arista products are supported worldwide directly and through partners.

 Additional information and resources can be found at **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 EOS, CloudVision and the enablement of security, performance and efficiency. 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.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20180821005228/en/**

Media Contact
Amanda Jaramillo, 408-547-5798
Corporate Communications
amanda@arista.com

or
Investor Contact
Charles Yager, 408-547-5892
Product and Investor Advocacy
cyager@arista.com

Source: Arista Networks