Arista Delivers Multi-Domain Segmentation for Zero Trust Enterprise

2/2/2021

Simplified network segmentation with dynamic partner integrations

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Arista Networks (NYSE:ANET) today announced a new zero trust security framework for today's digital enterprise. Arista Multi-Domain Macro-Segmentation Service is a suite of capabilities for integrating security policy with the network through an open and consistent network segmentation approach across network domains. Enabled through Arista **EOS®** (Extensible Operating System) and **CloudVision®** capabilities, the latest **Arista MSS®** (Macro-Segmentation Service) functionality includes a new group segmentation approach, MSS-Group, intended to simplify access control for users and IoT devices in today's enterprise workspaces.

"Security and networking are coming together. Arista's zero trust strategy relies heavily on analytics and AI to identify mal-intent and is well positioned to capture what could be the biggest transition I've seen in networking," said Zeus Kerravala, Founder and Principal Analyst at ZK Research.

Zero Trust Security in a Cloud and IoT World

Traditional network security architectures guarded users only at the borders. This approach is no longer sufficient with distributed users and a myriad of IoT endpoints in today's enterprise. A zero trust architecture that assumes no user or thing can have free run of the network is needed to secure modern networks. Zero trust never trusts without verification, restricts access to only required connections and then continually monitors for good behavior. In this new decade, the implicit trust associated with network location needs to be replaced with continuous, proactive network monitoring with behavioral-based situational analysis for asset visibility and rapid incident response. Arista's zero trust security approach is designed to address this evolution, combining network-based multi domain segmentation, situational awareness and visibility for all network resources, and AI-driven network detection and response.

IoT-ready Group Segmentation

Secure segmentation grouping needs to be defined based on functional roles, such as cameras or DVRs, across enterprise workspaces and independent of traditional network addressing constructs. In addition, any network solution needs to be based on an open framework that allows for deployment in both greenfield and brownfield deployments.

Arista is introducing MSS-Group as a new network segmentation service for controlling authorized network communication between groups. Available on EOS-based switches, MSS-Group implements security policy enforcement based on logical groups rather than traditional approaches based on interfaces, subnets or physical ports. MSS-Group is built on an efficient data plane enforcement mechanism, avoiding the limitations of vendor lock-in solutions that utilize proprietary hardware tags and are limited by inefficient hardware resource mappings. The MSS-Group solution leverages CloudVision, the same management plane platform for multi-domain automation, telemetry and analytics, for security policy management and visibility. In addition, the MSS-Group solution is most powerful when CloudVision integrates with a dynamic identity provider through available APIs.

Arista has partnered with **Forescout** in building such a solution that streamlines policy design and management. Organizations can use **Forescout eyeSegment** to automatically apply real-time context to associate each connected device with its relevant security segmentation group, easily design and monitor group-based policies and communicate the appropriate segmentation policies to CloudVision. CloudVision is then responsible for the dynamic orchestration of the required policy to the Arista switches for enforcement.

Arista Multi-Domain Segmentation

Arista Multi-Domain Segmentation converges the network with security across the campus to data center to cloud. The solution avoids the proprietary siloed architectures from incumbent vendors.

With multi-domain and network-security convergence as the goal, Arista is also enhancing MSS for enterprise edge firewall and data center virtualization use cases, delivering comprehensive segmentation solutions for enterprise-wide use cases.

MSS Firewall provides security service insertion, allowing flexible placement of firewall policy across DMZ edge, data center and campus networks. Leveraging open-standards network constructs, MSS Firewall dynamically steers traffic to the firewall policy enforcement point, extending security policy enforcement to address broader traffic patterns. Using the same CloudVision orchestration, MSS Firewall integrates with Palo Alto Networks and other leading firewall solutions from Arista's security partner ecosystem.

MSS Host is a data center focused solution where security policies are extended from the virtualized host to the physical network. Through an API integration between CloudVision and VMware NSX platform, MSS Host extends NSX micro-segmentation policies to bare-metal workloads.

Arista enables through a broad set of security ecosystem partner integrations such as Aruba,Forescout, Palo Alto Networks, VMware (NSX), and Zscaler (see industry support **here**). In addition to advanced MSS-based dynamic segmentation services, Arista continues to support broad network segmentation models such as VXLAN/EVPN, VRFs, VLANs, and Access Control Lists.

Availability

MSS Firewall and MSS Host functionality are shipping as part of Arista CloudVision. The MSS-Group functionality will be available for trials in Q1'21.

Register **here** to learn more about Arista's multi-domain segmentation solution at our webinar on March 18th, 2021.

Read more about this announcement on Jayshree Ullal's blog **here**.

About Arista Networks

Arista Networks is an industry leader in cognitive cloud networking solutions for large data center and campus environments. Arista's award-winning platforms deliver availability, agility, automation analytics, and security through CloudVision® and Arista EOS®, an advanced network operating system. For more information, visit **www.arista.com**.

View source version on **businesswire.com**: **https://www.businesswire.com/news/home/20210202005316/en/**

Media Contact

Amanda Jaramillo

Corporate Communications

Tel: (408) 547-5798

amanda@arista.com

Investor Contact

Charles Yager

Product and Investor Advocacy

Tel: (408) 547-5892

cyager@arista.com

Source: Arista Networks, Inc.