First Look

Reinforcing Zero Trust Posture with Arista Multi-Domain Segmentation Services - Group

Date: February 2021 **Author:** Alex Arcilla, Validation Analyst

Network Security Challenges:[1]

47% Of organizations believe that ***cybersecurity*** is one of the business initiatives that will drive the most technology spending within their organization over the next 12 months.

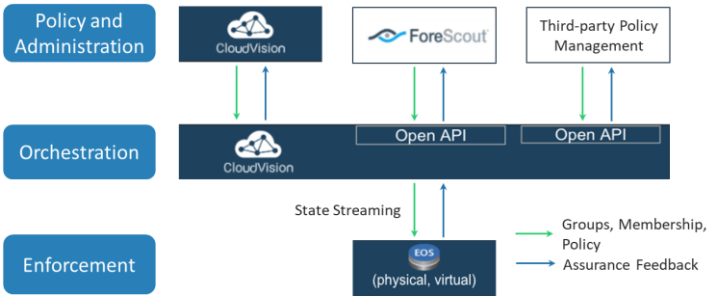
52% Of organizations will increase their spending specifically in ***network security*** over the next 12 months.

Protecting against security attacks and breaches has become more difficult for organizations as the attack surface has expanded throughout their networks. The emergence of the internet of things (IoT) has resulted in a proliferation of devices within enterprise networks that are potential security gaps when left unchecked. And while more organizations have extended their IT environments to embrace public cloud infrastructure services and applications, security and network access policies enforced on-premises are most likely inconsistent with those implemented in the public cloud.

Traditional methods of traffic segmentation, while proven, are ill-suited for securing the increased amount and diversity of network traffic. Port-based access control lists (ACLs) enabled organizations to segment traffic by assigning whitelists on select switch ports. However, as organizations have increased the number and complexity of ACLs, switching platform resources were limited to accommodate. Vendors then attempted to overcome this limitation by creating proprietary L2 tags to segment and isolate traffic at the packet level. However, vendors did not design these tags to interoperate with one another. For many organizations, implementing the use of these tags in a heterogeneous network either required hardware upgrades or workarounds to manage differences in segmentation tagging, such as implementing overlay networks. Using tags potentially restricted organizations to deploy hardware from a single vendor, incurring unnecessary IT capital and increasing the operational expenses.

Arista Multi-Domain Segmentation Services – Group for Zero Trust Networks

With its recently announced zero trust security framework, Arista introduced Multi-Domain Segmentation Services – Group (MSS-Group) to provide granular segmentation of end-users and devices accessing an organization's network. Along with Multi-Domain Segmentation Services – Firewall (MSS Firewall) and Multi-Domain Segmentation Services – Host (MSS Host), MSS-Group is part of Arista's Multi-Domain Macro-Segmentation Service offering.



Arista MSS-Group offers a simpler, efficient method of group segmentation enforcement and policy management by taking advantage of the forwarding decisions applied to incoming packets at the switch level. Organizations can leverage Arista MSS-Group in both Arista-centric and multi-vendor environments.

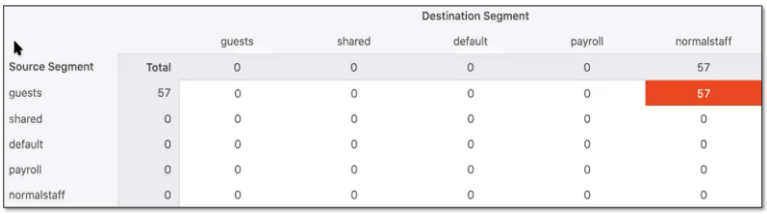
With Arista MSS-Group, organizations can leverage Arista CloudVision to set segmentation policies and orchestrate how Arista EOS enforces them throughout the network. Organizations that already use Forescout, an Arista ecosystem partner that enables a dynamic identity layer, can use Arista MSS-Group to deploy and enforce policies via CloudVision. Arista also supports organizations that already have implemented identity and access management (IAM) or network access control (NAC) products into their network by enabling interoperability with Arista MSS-Group via OpenAPIs. Organizations

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

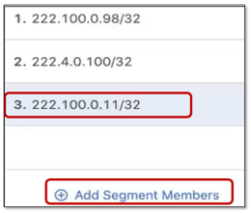
can continue to use third-party security solutions to set and manage policies while Arista CloudVision dynamically applies those policies in real time.

ESG Demo Highlights

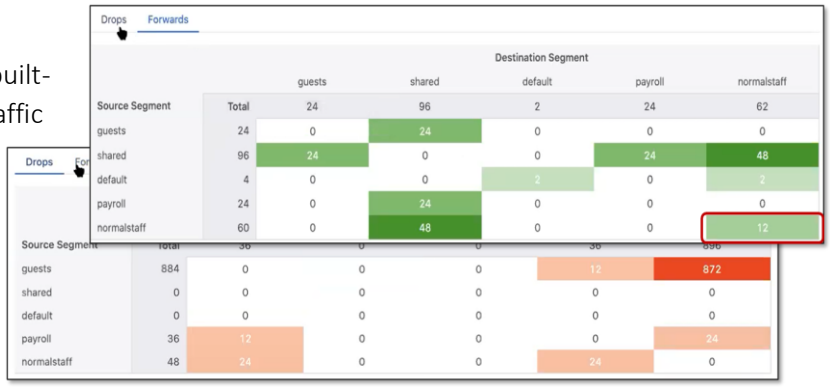
ESG performed testing on the use of Arista MSS-Group using a test bed that consisted of an Ixia network traffic generator feeding packets into an Arista 720XP. The goal was to validate the simplicity of implementing segmentation policy at the Arista switch level and show how the policy is enforced throughout this test network. Using the CloudVision Portal (CVP), we observed the following.



- ESG navigated to the ***Device Overview*** of the Arista 720XP and selected ***Segmentation***. We viewed one policy that noted any traffic from any IP address assigned to the "guests" segment will be dropped if attempting to reach anyone within the "normalstaff" segment. We then prompted the Ixia device to generate network packets from a member (single IP address) assigned to "guests" and saw that all traffic was dropped when attempting to reach "normalstaff." (The heat map above shows the number of dropped packets in red.)



- ESG then navigated to ***Provisioning*** -> ***Studios*** to create a new segmentation policy on the Arista 720XP. We removed the IP address that was blocked from sending traffic from "guests" and placed it in the "normalstaff." Because pre-defined segmentation policies allowed any member within "normalstaff" to communicate with any other member, traffic originating from the added IP address will no longer be blocked.



- After reviewing and approving the change via the built-in change control processes, we then generated traffic on all ports of the Arista 720XP and observed packets being forwarded amongst "normalstaff" members. We noted that the heat maps displaying both dropped (in red) and forwarded (in green) packets mirror each other, showing that segmentation polices have been applied correctly and consistently.

First Impressions

Approaches to group segmentation have been limited in managing the proliferation of security attacks in light of the explosion of sources of traffic bought about by IoT and increased usage of the public cloud. In turn, organizations face greater challenges in ensuring network security. Organizations cannot rely on port ACLs or proprietary L2 tagging to reinforce a robust zero trust posture within their networks without incurring IT overhead.

ESG verified that Arista's MSS-Group can support organizations in implementing group segmentation policies simply and consistently. We verified that Arista's straightforward and intuitive approach can support both Arista-centric and heterogenous networks, thus ultimately saving on both capital and operational expenses.