Extending Microsegmentation with Arista CloudVision and VMWare NSX Datacenter

Inside

Sophisticated cyber attacks and ransomware in recent years have raised the bar for security requirements in the modern data center. The complexity of requirements around risk control and policy enforcement network wide are increasing due to the increased footprint of variety or workloads. Network segmentation is required to isolate these expanding footprint for reducing the threat exposure. This segmentation must be consistent across virtual and physical domains, to account for all workload types. Solutions today add complexity as each use case creates a distinct and separate set of security policies. Security teams must simplify their segmentation approach by applying a common policy model to inspect, control and audit application workloads at scale.

Operational Inefficiencies of Silos

Micro-segmentation from VMware NSX allows IT teams to secure virtual workloads and microservices. This is achieved by creating fine-grain policies targeting specific workflows between applications and integrating them directly into the workload.

However, many data centers have workloads that have not been virtualized, or cannot be virtualized, running on physical servers. To secure these segmented physical workloads, separate policies are implemented resulting in a divergence in policy enforcement between the virtual and the physical workload domain. Each administrative domain is independent and not in sync with others, leading to operational overhead, duplication of effort and inefficiency in application delivery and network utilization.

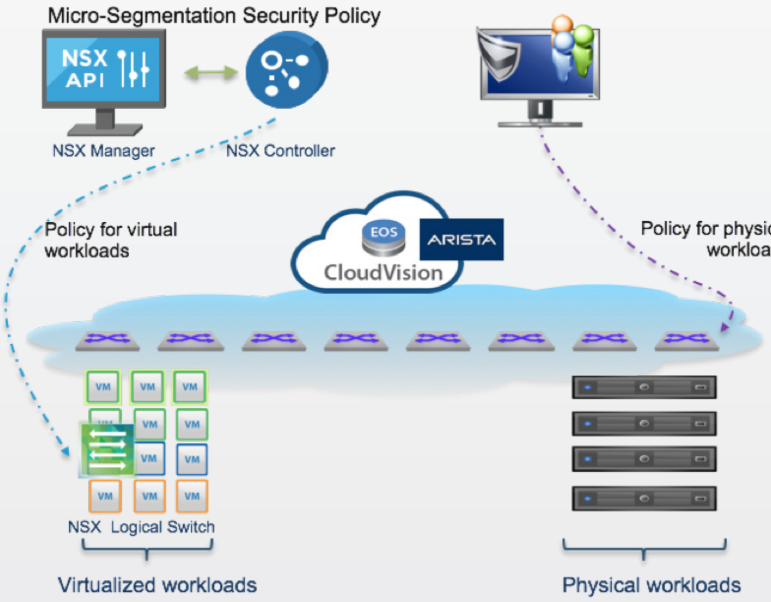

Figure 1: Multiple administrative domains implementing separate policies

What is needed is a way to extend the virtual domain segmentation policy to physical workloads, while maintaining a single policy engine. Mainstream enterprises with distinct IT teams, for virtual and physical infrastructure, are looking for such model for consistency and the operational efficiency, while simultaneously preserving the autonomous nature of the teams and systems.

> This integration provides a secure as well as open automation framework for resources to be deployed anywhere in the datacenter.

Extending micro-segmentation for bare-metal workloads

Arista and VMware have pioneered the solution for network virtualization in the Software Defined Data Center. While NSX Data Center micro-segmentation was originally introduced to secure virtual workloads, there are inherent benefits of extending the same for securing physical workloads. Applying the security policy at the network edge for the physical workloads brings uniformity and consistency.

Arista and VMWare are extending secure segmentation with an open API (REST/JSON) based exchange, which allows NSX to federate with CloudVision, to extend the micro-segmentation policy for physical workloads.

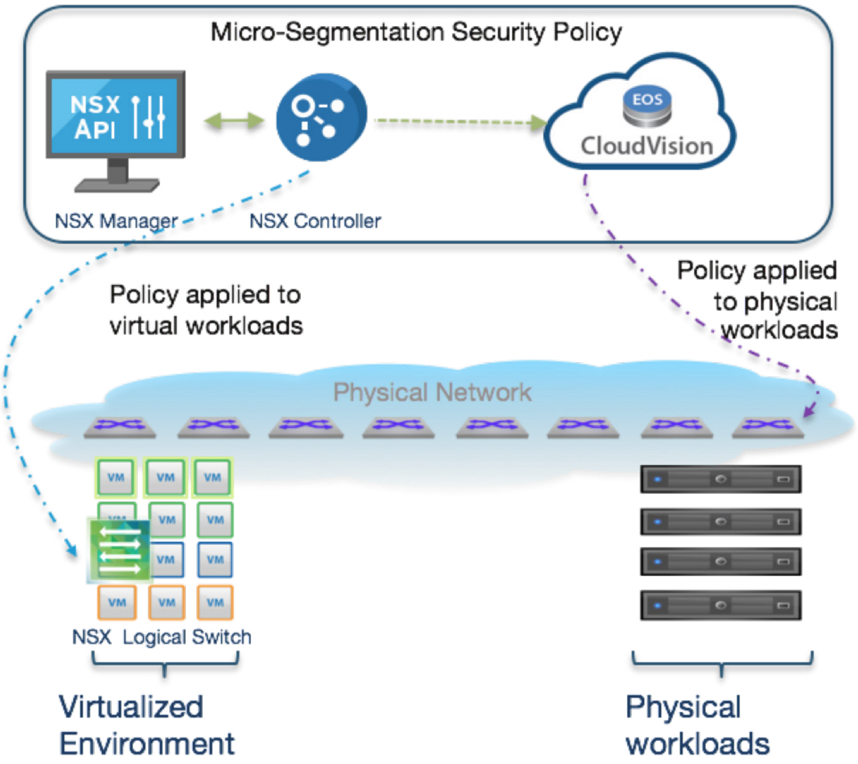

Figure 2: Extending micro-segmentation policy with VMWare NSX and CloudVision

In operation, Arista CloudVision will register with the NSX controller and receive the policies. CloudVision will appropriately program the Arista switch or switch pairs to allow of deny conversation between the physical and virtual workloads. This allows for dynamic synchronization of security policy as new policies are created and existing policies are modified. There is no new protocol or encapsulation or server reconfiguration required, allowing integration with existing networks, servers, and monitoring tools. Further, it allows the security admin have control on authoring policies and network control point to be managed by network admins, preserving the autonomy of both domain admins. This integration provides a secure as well as open automation framework for resources to be deployed anywhere in the datacenter. This automation based scalable framework allows enterprises to secure all assets with uniform policy implementation at scale, mitigating the overall risk and delivering agile services.

Arista's Secure Places-In-the-Cloud

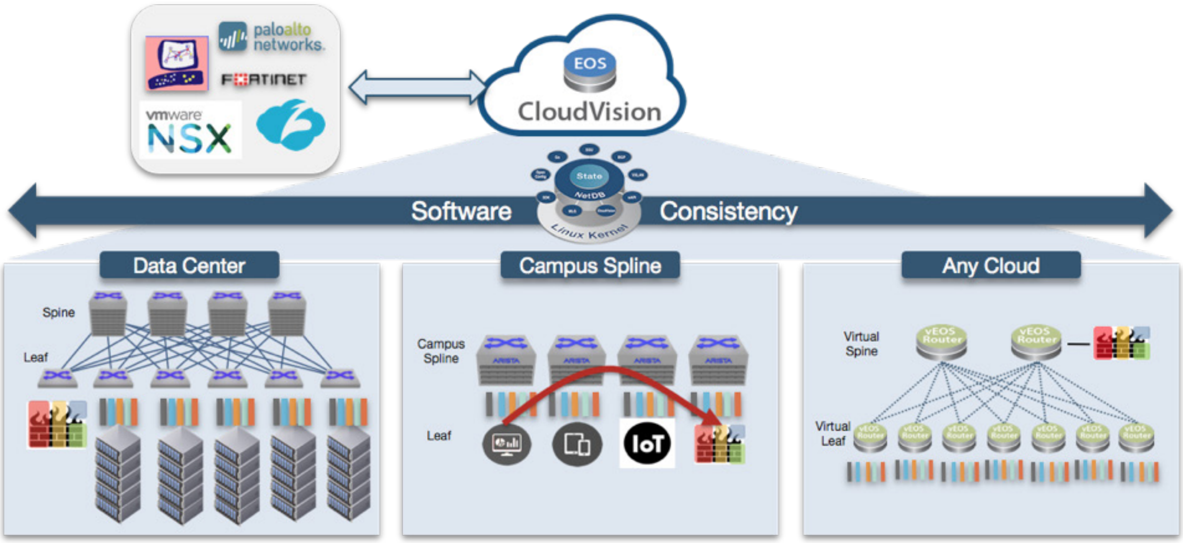

Figure 3: Securing Places-in-the-Cloud with segmentation, controls and connectivity

Extending Micro-segmentation with Arista CloudVision and NSX Datacenter addresses current challenges of common policy framework for both virtual and physical workloads, bringing flexibility, agility and scale to modern services deployment.

As part of Arista's overall security strategy, this micro-segmentation integration coupled with Arista's Macro-Segmentation Services (MSS) and a strong foundation of EOS and CloudVision security features, enables an end-to-end framework for consistent security across the places-in-the-cloud.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062