PALO ALTO NETWORKS AND ARISTA NETWORKS

Network-Based Security Integration Providing Dynamic Automated Deployment, Deep Visibility, and Robust Security for Both Physical and Virtual Workloads

Key Benefits of the Integration

- Dynamic service insertion
- Complete flexibility on locality of devices
- No new frame formats or protocol required
- Software-driven: leverages automation for network security integration

The Challenge

Data centers have increasingly virtualized and partitioned their networks, becoming more dynamic while accommodating on-the-fly deployment of new applications within shared private, public, and hybrid clouds. Furthermore, the threat landscape is changing. Hackers are finding new ways to breach the data center with an influx of new vulnerabilities and threats that need to be protected. Enterprises are faced with the complexity of implementing an agile security architecture to address a hybrid environment of microservices, virtual workloads, and legacy applications to protect critical assets from modern threats. This includes securing traffic between the modern application clusters and bare metal workloads. SecOps is challenged to maintain control over traffic in order to detect any compromised assets within the data center.

Arista Macro-Segmentation Service

Arista Networks Macro-Segmentation Service® (MSS®) capability for CloudVision® allows a variety of platforms, such as next-generation firewalls, to be deployed automatically for specific workloads and workflows across any network topology, including Layer 2, Layer 3, and overlay network virtualization frameworks.

Macro-Segmentation Service is a capability within Arista CloudVision that addresses a growing gap in security deployment for hybrid data centers. It extends the concept of fine-grained intra-hypervisor security for VMs to the rest of the data center by enabling dynamic insertion of services for physical devices and non-virtualized devices. It is specifically aimed at physical-to-physical (so-called P-to-P) and physical-to-virtual (P-to-V) workloads, with complete flexibility on the placement of service devices and workloads.

MSS components include:

- Arista leaf-spine switch fabric
- Arista CloudVision
- Vendor firewall attached to a service leaf switch. Firewalls can be attached in high availability configuration (active-standby or active-active) as well.

Palo Alto Networks

The Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities, at the right place, across all stages of an attack lifecycle.

Palo Alto Networks and Arista MSS

By integrating with native APIs provided by the leading Palo Alto Networks Next-Generation Firewalls in the data center (PA-3200 Series, PA-5200 Series, and PA-7000 Series) and Panorama—native APIs that already exist—Arista Macro-Segmentation Service learns the security policies, identifying the workloads the firewall needs to inspect the traffic and take action. Upon identification, MSS can now steer interesting traffic to the firewall, thus enabling a logical topology of the firewall in the path of workload flows.

The automation capabilities of Arista Macro-Segmentation security operate in realtime, and without any need for a network operator to engage the security administrator (or vice versa). Furthermore, there is no need for the network to be architected in a manner specific to a particular workload. This flexibility is crucial to the successful deployment of security in an enterprise private or hybrid cloud. With this new integration, security policies in Palo Alto Networks Next-Generation Firewalls can be instantiated from the central point and implemented across the network topology.

Use Case No. 1: Intelligent Inspection of East-West Traffic on Demand

Arista's Macro-Segmentation Service does not try to "own security policy" or need to run a controller-of-controllers that understands every application flow or interaction. Customers can define security policies within Palo Alto Networks Panorama™, a centralized network security management console.

Using the API plane, Arista CloudVision obtains the interesting rules from Panorama and programs the Arista switches to steer intercepted east-west workload traffic to the Palo Alto Networks Next-Generation Firewall for robust traffic and content inspection as well as policy enforcement. Security admins can now have the flexibility to add or remove policies to monitor traffic between workloads on demand, and they can profile traffic to detect malware or DoS attacks from within the enterprise proactively.

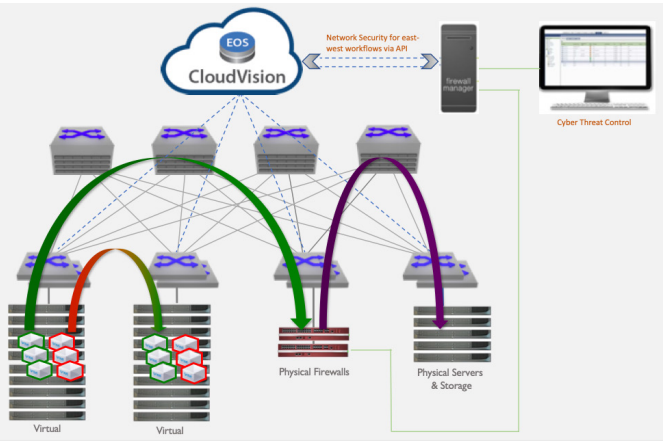

Figure 1: Palo Alto Networks and Arista Networks integration architecture

Use Case No. 2: Complete Flexibility on Devices Across the Network

Service devices such as the Palo Alto Networks Next-Generation Firewall can be connected anywhere in the network on any switch. This allows larger data centers to centralize their security devices in a service rack and logically insert them in the path between any workloads on demand or based on a firewall policy. There are no restrictions or limitations on where the service devices are physically attached within the fabric. Palo Alto Networks firewalls are discovered via LLDP. Likewise, devices to which services are targeted can be located anywhere in the network with no restrictions or limitations on physical placement.

Use Case No. 3: Intelligent Security Policies Offload to Network

As stated earlier, Arista's Macro-Segmentation Service does not try to "own security policy." In addition to redirection of interesting traffic to the firewall, security administrators can define rules within Palo Alto Networks Panorama, marking them as offload policy. The offload tag, when applied to a policy, identifies a 5-tuple and the action (permit/deny).

These policies can be programmed and enforced on the TOR switches via MSS. This allows the firewall admin to offload predictable traffic, which need not be inspected, or disallow traffic between any pair of segments. In legacy architecture, this traffic would need to be steered to the firewall for processing, thus consuming firewall bandwidth and CPU resources. This new offload function enables the firewall admin to have a central control point and expand the security domain. In addition, this allows the firewall to provide high-performance, deep packet inspection and intrusion prevention services.

About Arista

Arista Networks pioneered software-driven, cognitive cloud networking for large-scale datacenter and campus environments. Arista's award-winning platforms, ranging in Ethernet speeds from 10 to 400 gigabits per second, redefine scalability, agility and resilience. Arista has shipped more than 20 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 25/50G consortium. Arista Networks products are available worldwide directly and through partners. Find out more at www.arista.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

palo-alto-networks-and-arista-tpb-062619