Palo Alto Networks and Arista Networks

Network-based security integration providing dynamic automated deployment, deep visibility, and robust security for physical and virtual workloads

Benefits of the Integration

- Dynamic service insertion
- Complete flexibility on locality of devices
- No new frame formats or protocols required
- Network security integration driven by automation

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. Due to the advent of IoT, 5G and AI/ML workloads, enterprises are faced with the complexity of implementing agile security architectures to address a hybrid environment of microservices, virtual workloads, and legacy applications to protect critical assets from modern threats. This includes securing traffic between modern application clusters and bare metal workloads. SecOps teams are moving towards a Zero Trust Security model to gain pervasive visibility across their data centers to monitor and maintain control over traffic, detect any compromised assets within the data center and enforce policy to isolate them and prevent the spread of the attack.

Arista Networks Macro-Segmentation Service

Arista Networks™ Macro-Segmentation Service (MSS) - Firewall or MSS-FW capability for CloudVision® allows a variety of platforms, such as next-generation firewalls, to be deployed automatically for specific workloads and workflows across modern overlay network virtualization (EVPN) fabrics.

MSS-FW addresses a growing gap in security deployment for hybrid data centers. It extends the concept of fine-grained intra-hypervisor security for virtual machines (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 and physical-to-virtual workloads, with complete flexibility on the placement of service devices and workloads.

MSS-FW 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

Palo Alto Networks Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

Next-Generation Firewalls inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Arista MSS-FW

By integrating with native APIs provided by Next-Generation Firewalls in the data center and Palo Alto Networks Panorama™ network security management, MSS-FW learns the security policies, identifies the workloads the firewall needs to inspect, and takes action. Upon identification, MSS-FW can now steer relevant traffic to the firewall, inserting the firewall in the path of workload flows.

The automation capabilities of Arista MSS-FW operate in real time without any need for a network operator to engage the security administrator. 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, Next-Generation Firewalls can create security policies from a central point and implement them across the network.

Use Case 1: Intelligent Inspection of East-West Traffic on Demand

MSS-FW 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 Panorama.

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

Use Case 2: Complete Flexibility on Security Device Location

Next-Generation Firewalls 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 security devices are physically attached within the fabric. Palo Alto Networks firewalls are discovered via Link Layer Discovery Protocol (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 3: Offload Traffic Inspection with Intelligent Security Policies

In addition to redirecting traffic to the firewall, security administrators can define rules within Panorama to offload predictable traffic from the firewall. MSS-FW enforces these policies on the switches. In a legacy architecture, all traffic would be steered to the firewall for processing, consuming bandwidth and CPU resources. This offloading function enables the firewall to provide high-performance deep packet inspection and intrusion prevention services for unknown traffic, reducing the risk of malware or threats gaining footholds.

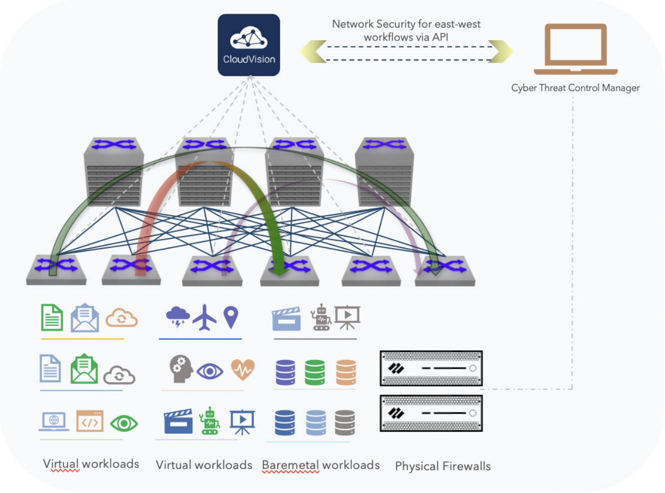

Figure 1: Palo Alto Networks and Arista Networks integration architecture

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. 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