Secure Cloud Segmentation with Arista Networks and Zscaler

The security framework that worked well for enterprises in the 1990s has become less relevant given the rise of applications hosted in the public cloud and the Internet as the new corporate network.

Arista provides a new,secure architecture related to public cloud hosting and Zscaler is offering solutions aiming to secure access across the public Internet. Taken together, the two companies are delivering cutting-edge security offerings for global enterprises.

2000 Era

Server virtualization in the data center created the need for scaling out the subnets and addresses needed for network access. When these VMs and workloads could be relocated to any physical server, the network needed to adjust its security services model to accommodate this motion.

Arista addressed these needs by developing MSS built on the VXLAN standard. East-West traffic in the data center can be selectively sent for inspection to firewalls without needing to place them in line to every traffic flow. The inspection and segmentation can be achieved for virtual and bare-metal workflows.

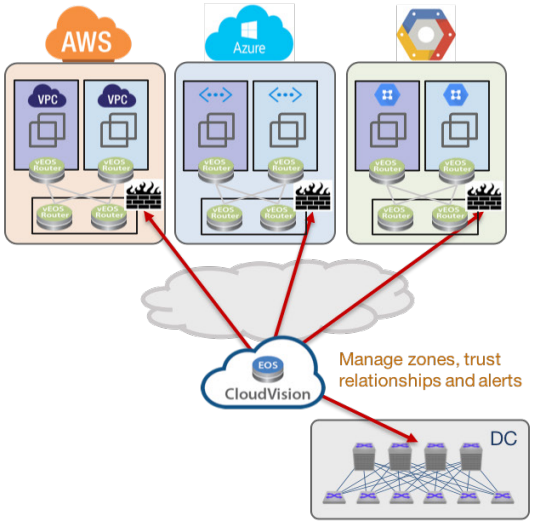
2010 Era

Era Cloud Phase consisted of virtual servers being relocated not just within the data center but also out to major cloud providers such as Amazon AWS, Microsoft Azure and Google Cloud. The data center network, implemented with physical switches, had to now be extended to the multi-cloud. The network was also expected to provide segmentation services consistent with the approach in the data center. Arista developed a virtual version of its EOS® (vEOS® Router), rich in routing, networking and VPN capabilities, and made it available to customers across the major cloud-provider marketplaces. The new AnyCloud network could now be deployed in a hub-and-spoke or mesh configuration over the Internet by leveraging the IPSec VPN capabilities of vEOS.

Meanwhile, Zscaler was building out the industry's first, cloud-native, security platform. Aggregated across hosted sites worldwide, and built in collaboration with Arista technologies, this platform powers secure access to sites and workloads across the public Internet.

2020 Era: Holistic Cloud Security

Arista is introducing another key aspect of network-based Any Cloud security. Arista Zone Segmentation Security is a key security feature of vEOS and an extension of our Macro Segmentation Service (MSSTM). It allows the vEOS Router to craft segmentation boundaries across groups of interfaces across any cloud network including AWS, Azure and GCP. Connections can be selectively allowed or precluded across these boundaries based on organizational needs. While MSS, along with Arista firewall partners segments for intra data center and intra private cloud Zone Segment Security (ZSS) will provide functionality for the inter-cloud network as shown in Figure 1.



Zone Segmentation

- vEOS Router feature
- Simplified policy definition
- Zone-based Classification
- Stateful enforcement
- Cloud-agnostic
- Automated centrally, via CloudVision
- Familiar to network Ops

Figure 1: Holistic Cloud Security

ZPA: Holistic approach to secure cloud adoption with ZPA

As workloads along with virtual machines migrate across the any-cloud. Arista secures and segments them leveraging MSS and ZSS network-based services. Now, secure application access can be delivered through application segmentation as well. Zscaler, an Arista partner, provides this level of segmentation via its Zscaler Private Access (ZPA) software-defined perimeter service. Combining the best of both worlds. ZPA secures access to internal applications running in any public cloud, private cloud or datacenter. It creates secure micro-tunnels each time a session is established to provide a secure segment of one between an authorized user and a named application.

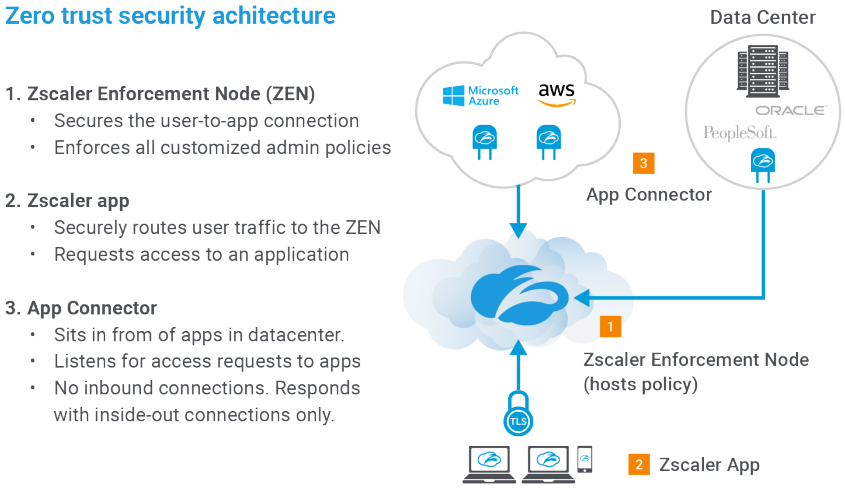


Figure 2: Arista and Zscaler - A compelling cloud security solution

In order to provide cloud security that unifies network-based and application-centric security for the cloud world Arista and Zscaler are working closely together. One of the primary components of ZPA's central authority is the App Connector, a lightweight piece of software that provides inside-out connectivity from an app to the Zscaler cloud, where the app to user connective is stitched together. The App Connector is now available as an optional add-on of Arista vEOS. When deployed together, this results in best in class network segmentation and application segmentation in a single, easy-to-manage cloud security offering as shown in this Figure 3.

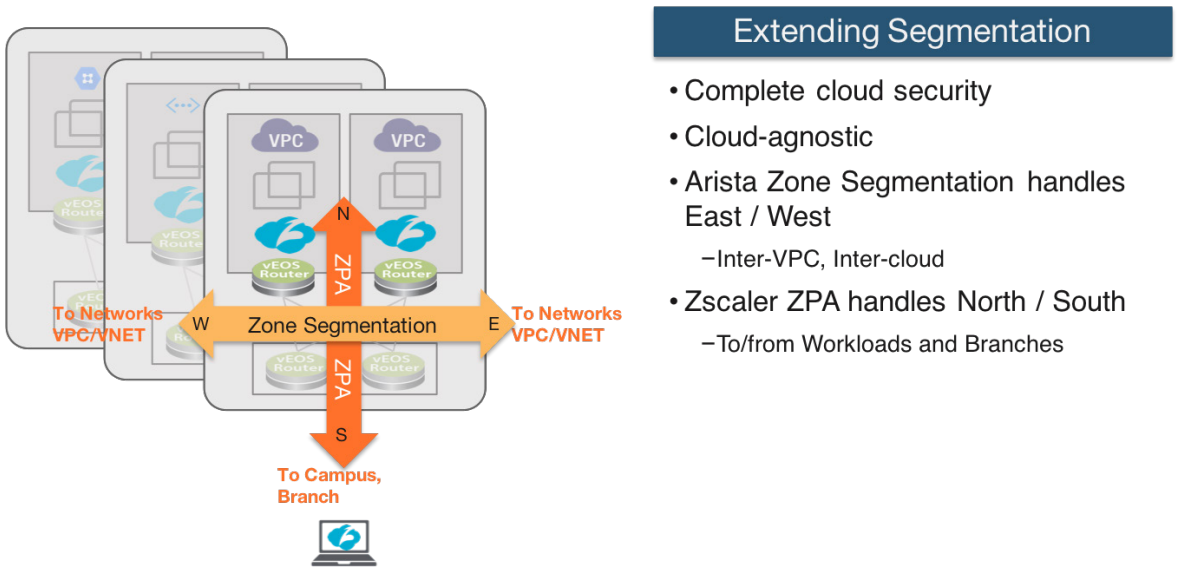


Figure 3: The best of North South Application Access and East West Network Security

Provisioning secure segmentation of workloads across the data center and branch offices and extending out to the any-cloud will remain challenging for many years to come. Arista and Zscaler will continue to work together to enable enterprises to implement this critical security capability seamlessly.

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