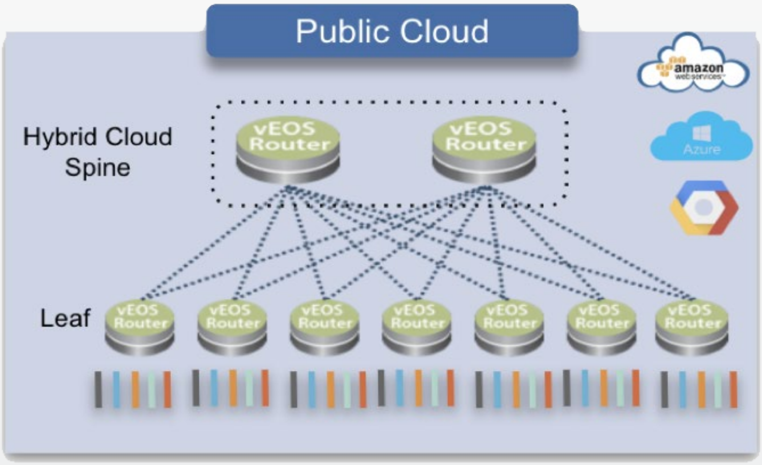
Zone Segmentation Security (ZSS)

Inside

Arista Networks Zone Segmentation Security provides reliable, secure cloud agnostic services by creating a uniform segmentation methodology across any public cloud provider or a private on-premise cloud.

Zone Segmentation Security secures the cloud with the power of EOS®

Each cloud provider provides the ability to secure workloads in the clouds, however, the management of network security policies are specific to each provider, thereby making it hard for security admins to holistically secure workloads in private and public clouds i.e. each cloud becomes its own security island.



Zone Segmentation Security (ZSS) is embedded natively within Arista's field proven EOS and allows Arista's vEOS® Router to extrapolate and consistently apply the same security policies across Virtual Private Cloud (VPC) or Virtual Network (VNET) and across any cloud provider, thereby tremendously reducing the total cost of ownership (TCO) to manage and monitor a cloud infrastructure.

Background - Cloud Security

When an IT administrator moves a workloads to the cloud, they are placing the workload into a private, virtual environment (i.e. a VPC or VNET). The application workload may be broken down into multiple components: Web, App & DMZ could reside in 3 separate VPC/VNETs for security zones. Customers may also have applications spread across multiple clouds.

Today to secure the virtual networks for cloud native applications, customers may end up using either:

a. Proprietary lock-in security groups per cloud policies which cannot be ported to other cloud providers or are inconsistent with on-prem security policies.

b. Deploy virtual firewalls. However, the costs involved typically reduce or entirely eliminate the scope of firewall enforcement.

c. In the worst case scenario, these customers do not deploy any security as it is too complex to manage, troubleshoot. Instead, they route all the traffic back to on-prem firewalls thereby incurring tremendous bandwidth charges from the cloud providers.

As such, customers may end up facing 3 or more challenges:

a. Within a specific cloud provider eg. AWS, how to secure applications using the same security configuration policies as in the on-prem data center?

b. How to consistently apply security configuration policies across multi-cloud providers as on-prem DC?

c. All the policies need to be applied or changed manually across any cloud depending on the hundreds of applications deployed in the cloud.

Cloud Security Groups

Security admins default to what is provided natively to them by cloud providers to protect their workloads. Cloud native security controls provide a base level of segmentation, controlling the traffic allowed to/from instances. For example, an AWS EC2 instance can have multiple security groups assigned to it, and the rules for security groups can be modified at any time.

The challenges of using cloud native security controls are:

a. Each cloud provider has a different way of implementing Each cloud provider has a different way of implementing security groups, which is entirely different from the way security is implemented on-prem,

b. Each cloud provider has a different way of logging the security policies from traffic being permitted or denied,

c. Each cloud provider security groups have their own caveats, scale limitations, all requiring the admins to individually track these issues.

All these can impose massive costs for enterprise customers, thereby increasing the TCO for migrating applications to the cloud.

Cloud Virtual Router ACL Limitations

Typically to secure cloud workloads using 3rd party virtual routers in VPC/VNETs, security admins have limited options of applying network security access-lists (ACLs). As such, ACLs are the simplest form of network cloud security i.e. based on source/destination ip address, source/destination/port and TCP/UDP and applied to specific interfaces.

However, there are a number of limitations by using ACLs on virtual routers:

a. ACLs cannot be logically grouped together when applying a consistent set of policies across multiple interfaces making it hard to manage, or

b. Due to lack of grouping, admins can experience ACL explosion to configure and manage hundreds of lines of ACLs between hosts between VPCs/VNETs, or

c. ACLs are not stateful i.e. don't track state of flow through a router's interface between VPC/VNETs.

Although ACLs can be applied on a vEOS router the ZSS feature is a more advanced form of security implementation.

ZSS Overview

ZSS places workloads (i.e. VM hosts / containers) into segments. A segment can be thought of as hosts within the same subnet, or specific ip addresses or grouping of interfaces.

By default:

a. Within a segment there is no security policy restriction, i.e. any host can talk to any other host.

b. Between segments there is a ZERO trust model i.e. no communication is allowed between segments.

ZSS provides the following benefits to network security admins:

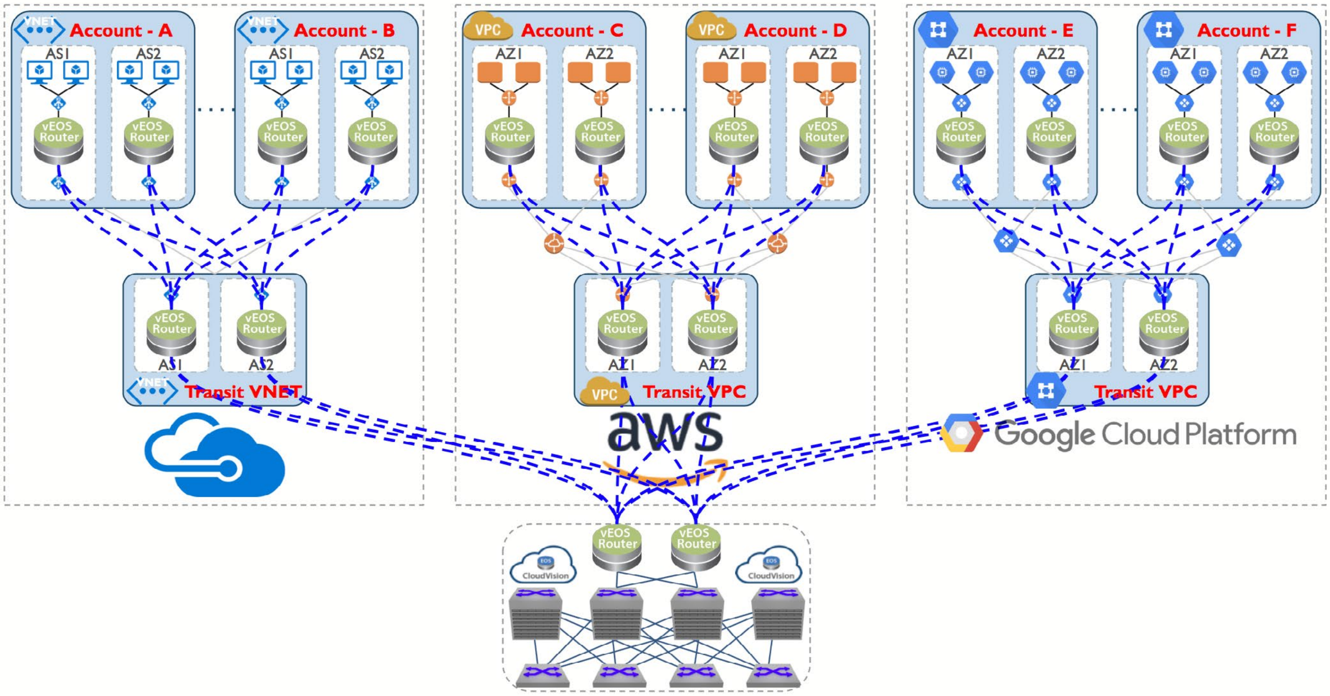
a. To group a set of endpoint hosts via common set of security policies.

b. Explicit rules {permit | deny} need to be configured to allow hosts to communicate between segments,

c. ZSS is configured either using industry standard CLI on the vEOS Router or orchestrated centrally via Arista CloudVision®.

d. Additionally, and most importantly ZSS allows the stateful tracking of flows, eg. if host 1 from segment A is making a web service request to host 2 from segment B over port 80, then the TCP state is tracked and the response from response from host 2 to host 1 is automatically allowed.

e. ZSS provide effective protection and traffic control regardless of the operating system your instances use.



By employing Arista vEOS Router as edge devices in the VPC's / VPNET's, customer can have these instances facilitate segmentation of traffic at the edge as opposed to the transit layer which makes it scalable.

Benefits of ZSS

Arista's ZSS helps security teams address:

a. **Consistent Security Policy** - Ability to secure traffic flows to/from or within microservices (i.e. inter & intra VPC/ Vnet) using same security policy mechanism as on-prem independently of public cloud provider lock-in security mechanisms,

b. **Any Cloud Security** - Cloud-agnostic approach with Arista's vEOS Router to build an overlay with standard segmentation framework across multi-cloud platforms.

c. **Automation** - Fully automated provisioning using Arista's CloudVision across any cloud platform.

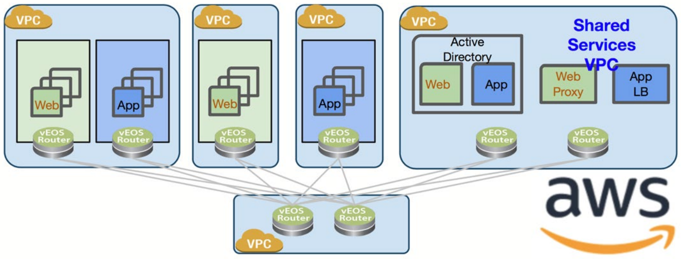
d. **Support** - Manage, monitor and troubleshoot secure policies in the any cloud using same security orchestration rules as on-prem.

ZSS Use Cases

There are two other common use cases for ZSS:

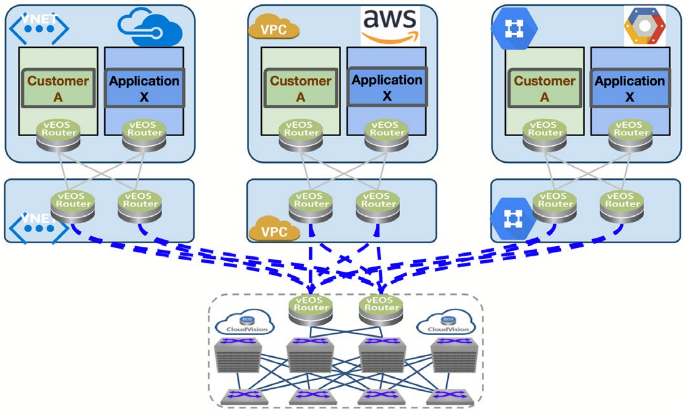
Use Case 1 - Shared Services

Shared services VPC/VNET is where centralized network services reside in a single instance eg DNS, DHCP, NTP, logging, etc. as shown in the figure below:



In a simple example, Web instances in every VPC have full bi-directional connectivity amongst each other. Similarly, app instances can communicate with each other as well. ZSS allows the security admin to deploy policies very easily for admins to securely have all the Web instances talk to only Web hosts in shared services VPC/VNET and App instances to talk to only App hosts in the shared services VPC/VNET. The ZSS policy would be applied on the leaf vEOS routers as a standard template configuration.

Use Case 2 - Multi-Tenant Cloud Infra & Applications



Enterprises often have central cloud/network teams which act as service providers for their own SILO internal customers. ZSS enables these teams to simply deploy consistent secure policies in a multi-tenancy environment rather than relying on public cloud specific network or application security groups. In the above figure 'Customer A' or 'Application X' could have storage / compute infrastructure present across any public cloud provider. Instead of leveraging per public cloud specific access controls to allow / disallow traffic, ZSS could be employed to enforce consistent security policies for Customer A across all the public cloud providers.

vEOS Router

Arista's vEOS Router modular EOS is designed to simplify fault detection, isolation, patching and extensibility. Modular, state-based software architectures are easier to maintain than legacy software "blobs". Feature errors don't impact other system functions. Targeted patches can be installed using RPM based tools to minimize service disruption. Proof of the reliability of Arista EOS is evident in the tens of thousands of systems deployed among the world's largest data centers.

The open Linux architecture inherent to Arista EOS allows easy installation of software extensions to add functionality and monitoring to the VM. Linux telemetry tools, some available as RPMs, can be installed without modification to add functionality and value. This simplifies standardized monitoring across the campus, datacenter, WAN and cloud.

Summary

Regardless of the service, location or workload, security must now transcend multi-cloud environments seamlessly. As an alternative to native cloud security controls, Arista's vEOS Router and ZSS simplify security policy across clouds,all of which can be automated, audited and visualized with Arista's CloudVision.

Consistent network segmentation with ZSS, or the broader Macro-Segmentation Service (MSS) from CloudVision, provides a powerful approach for applying the right security across applications, users, and 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