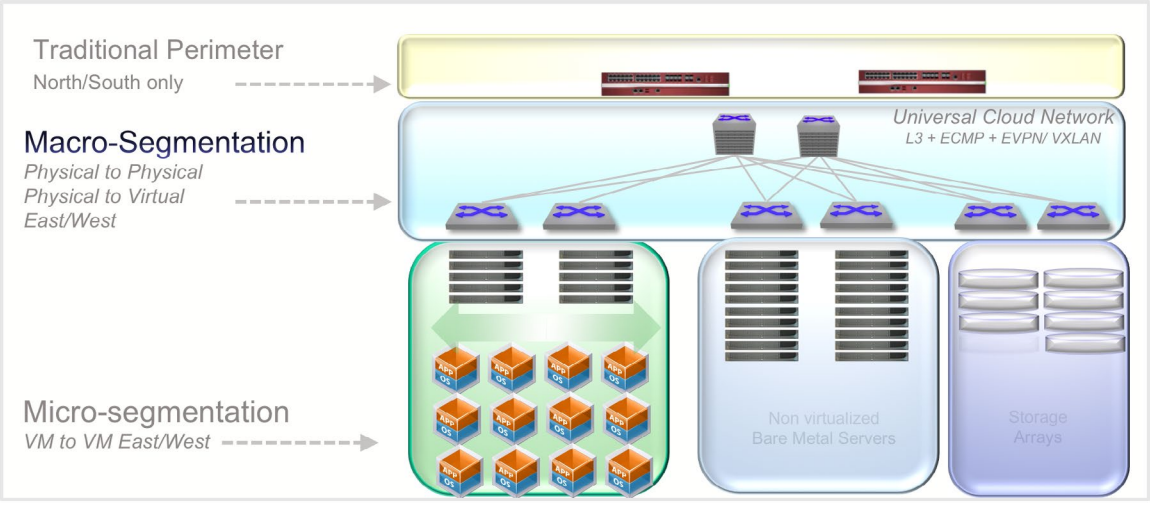
Arista Macro Segmentation Service - Firewall At-A-Glance

Introduction

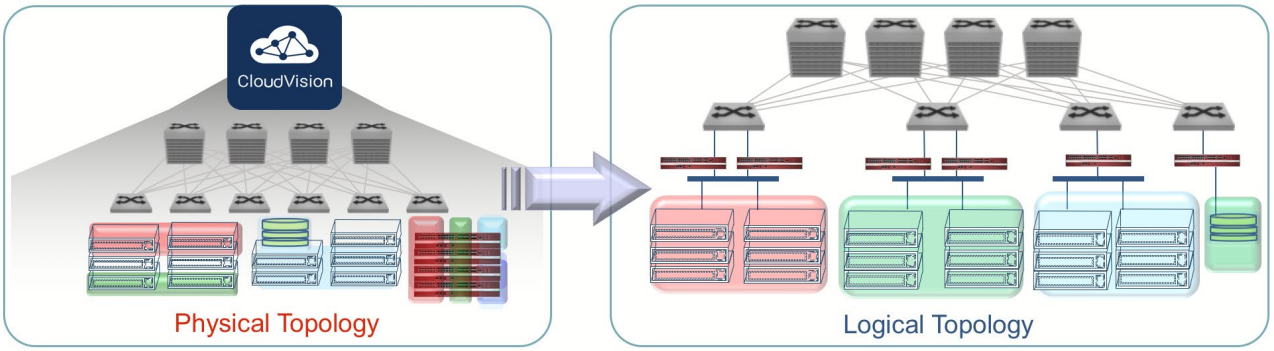
Today's cloud environments need a more flexible approach to deploying security that adapts to constant workload changes, additions, and movements. The capacity of the security solution needs to scale upward to match the broadened attack surface of multi-tenant shared environments.

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

With east-west traffic dominating the traffic flows, no solution exists yet to dynamically insert advanced security services for this traffic in hybrid data centers utilizing a combination of hypervisors, or containing non-virtualized workloads like big data and storage, or attaching legacy systems to the same networks as new cloud applications.



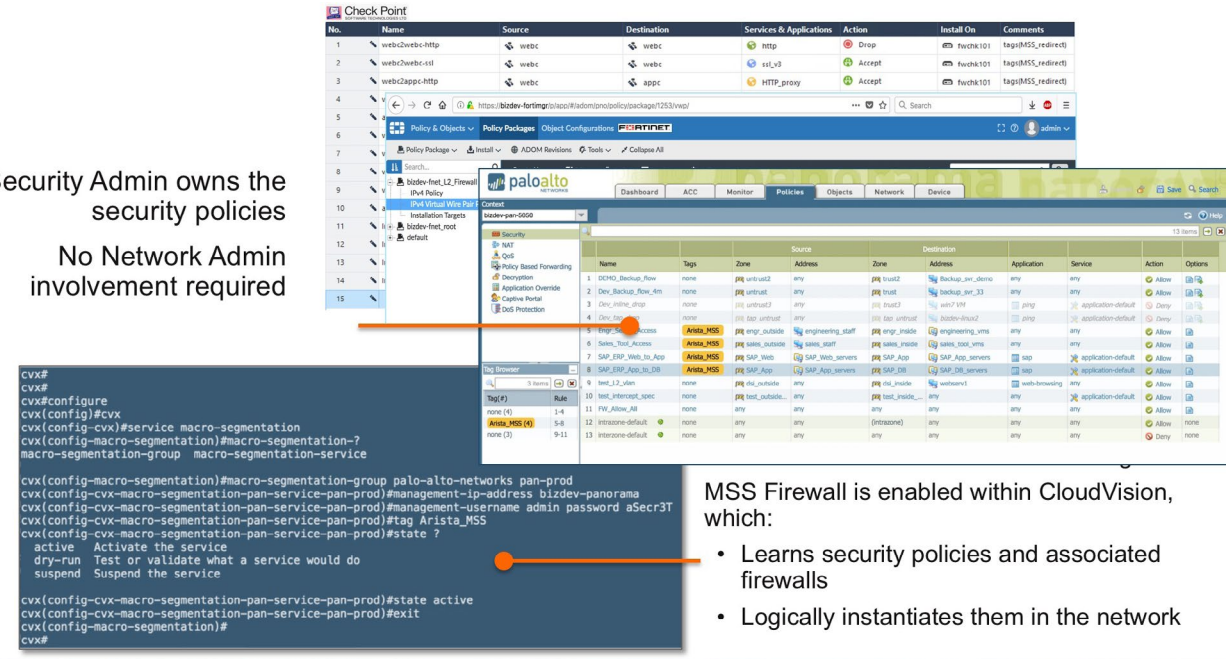
Arista Macro Segmentation Service - Firewall is a CloudVision service that enables an administrator to logically insert a firewall into the data path for traffic inspection.



With Arista MSS, SecOps and NetOps benefit from a tight integration, and at the same time gain operational independence. InfoSec creates and updates policies to monitor or inspect traffic.

Security Admin owns the security policies

No Network Admin involvement required



MSS Firewall is enabled within CloudVision, which:

- Learns security policies and associated firewalls
- Logically instantiates them in the network

This service is enabled in CloudVision and connects with a supported firewall or firewall manager to obtain policies of interest. CloudVision maintains a network-wide database of all state within the network called NetDB. NetDB is aware of where every workload is within the network, it learns in real time about new devices or workloads that are added, moved or removed from the network. Once CloudVision receives the tagged policies from firewall, MSS service can use NetDB to get more information on workloads to configure the appropriate switch. The switch can be programmed in real-time by CloudVision to redirect specified traffic to the firewall or to offload enforcement to the switch, which can allow or drop selected traffic, without sending it to the firewall.

Large data centers can centralize their firewalls in a service rack and logically insert them in the path between any workloads on-demand or based on a firewall policy. This model allows optimizing traffic inspection and logging to match the growth of traffic within the data center and detect threats from within.

Benefits

Dynamic:
- Automatic and seamless service insertion
- Follows host and application throughout the networks

Open:
- No proprietary frame formats works in multi-vendor network architecture
- Works in multi-vendor network architecture
- Open APIs

Software Driven:
- Leverage automation to integrate network fabric and firewalls
- Control through deeper programmability at all layers

Arista Macro Segmentation Service - Firewall enabled by Arista CloudVision provides the following benefits:

Complete flexibility on the locality of devices: Service devices such as firewalls can be anywhere in the network on any switch. This allows larger data centers to centralize their security devices in a service rack and insert them logically in the path between any workloads on-demand or based on a firewall policy.

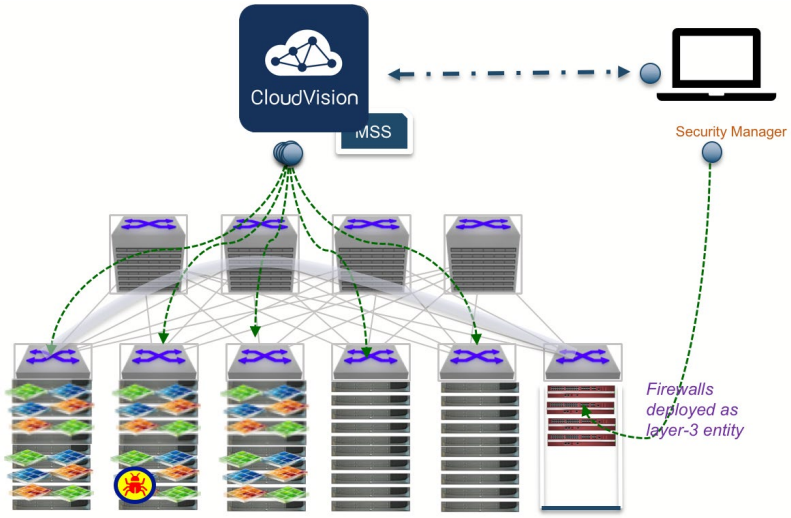
No new frame formats: There is no requirement for any new frame format, traffic steering or meta data in any new header fields.

Open: Standards-based forwarding is used to stitch service devices into the path of traffic.

Dynamic: As Hosts can and do move (vMotion and Disaster Recovery), Arista MSS provides the ability to have policy move with the host without admin intervention.

Enhances next-generation firewalls: Macro-Segmentation Service does not try to "own policy". InfoSec owns security policies and updates per business intent. Arista MSS provides tighter integration with Next-gen firewall capabilities with policy offload function.

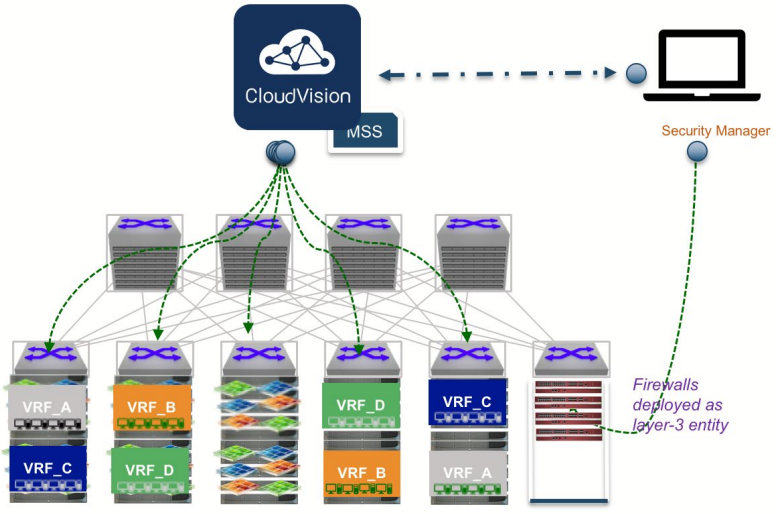
Rapid Threat Containment



Enterprises are faced with implementing an agile security architecture to protect critical assets from ever evolving sophisticated threats. When such threats in the form of exploits, ransomware, compromised systems etc. are detected, the SecOps is challenged to react fast to protect critical assets and infrastructure. Security vulnerability fixes or updates to mitigate malware may not be available to mitigate the threat in a timely manner.

The security administrator can leverage the power of Arista MSS to separate infected hosts from the rest of the network, block specific known communication patterns directly related to malware or redirect traffic from these hosts to the firewall by simply changing the policy on the firewall to quarantine the compromised host. The physical location of the compromised host within the campus or data center network need not be known. CloudVision has this information in its database and can implement the quarantine policies where they are needed.

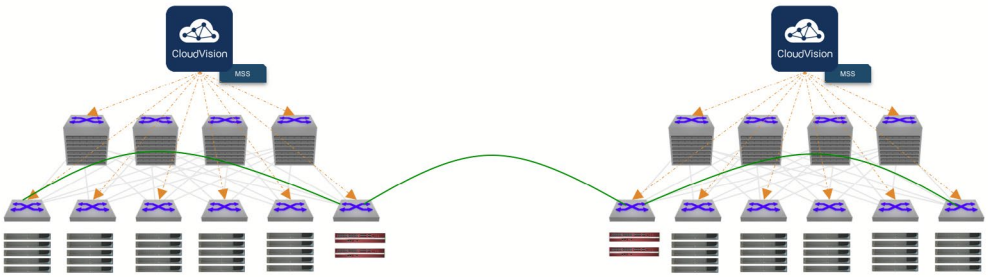
Multi-VRF Deployment



When designing modern Data center or Campus networks, segmentation/tenancy is often an important security requirement to split the network into different security zones and apply security services between and within them. The toolkit to accomplish these tasks, from the network side, are virtual routing and forwarding instances (VRFs), VLANs and often vendor specific proprietary mechanisms. Implementing these tools in the network drastically increases its complexity and complicates operations and maintenance of the IT ecosystem.

A new automated approach would be to use firewall as the only configuration entity for segmentation and allow MSS to provide necessary network isolation for a multi-tenant environment. A new tenant can be placed in an isolated firewall zone with corresponding set of policies. The most common objective would be to restrict inter-tenant traffic. When MSS is used, no manual VRF configuration is necessary to achieve this objective. In addition, MSS can provide more granular segmentation on top of this bare minimum. One added benefit of this approach is that a tenant's workload can be placed anywhere in the fabric.

Brownfield and Multi-Site



Arista Macro-Segmentation Service-Firewall can be deployed in a brownfield environment with a mix of non-Arista switches. This solution targets a EVPN/ VXLAN based network where both Arista and non-Arista Virtual Tunnel Endpoints (VTEPs) share the overlay reachability using the EVPN control plane.

In order to enable security enforcement with MSS, the user can put the resources that they would want to protect behind Arista VTEPs and express the security objectives using firewall policies.

The Customer can now enable MSS in a multiple data center (DC) environment where a VXLAN fabric is extended between DCs. In such an environment each DC has its own firewalls and may want to enforce security policies independent of other DCs.

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