

CloudVision® Macro-Segmentation Service

Inside

Address network-based security as a pool of resources, stitch security to applications and transactions, scale on-demand, automate deployment and mitigation, allow transparent application of security policies; do it all seamlessly without introducing gratuitous inter-dependencies, for both physical and virtualized resources:

- **Micro-Segmentation:** inserting services in the path of inter-VM traffic by defining policies in an overlay/virtualization controller for each individual workload — enforced within the hypervisor virtual switch, by application, workload, or other tag.
- **Macro-Segmentation™:** inserting services between workgroups (inter-tenant or inter-device) in the physical network by defining inter-segment service policies - enforced by the Arista cloud networking infrastructure.
- **AristaMacro-Segmentation Service (MSS™):** an extension in Arista EOS® software that utilizes Arista CloudVision® to automate security service insertion for next-generation firewalls and other networked devices.

It's no secret that information security has failed to keep up with the needs of business and the accelerating cyber-threat landscape. Data centers have increasingly virtualized and partitioned, becoming more dynamic while accommodating on-the-fly deployment of new applications within shared private, public and hybrid clouds. Meanwhile cyber-security has remained static and bounded — unable to protect the cloud environment from an increasingly threatening backdrop.

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 cloud environments. Infrastructures need to offer an unfettered selection of security technology options as opposed to siloed ecosystems of yesterdays solutions that limit flexibility and obstruct freedom of choice.

Introducing Macro-Segmentation Service

Arista Networks™ has unveiled a new Macro-Segmentation Service (MSS) capability for CloudVision® that 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.

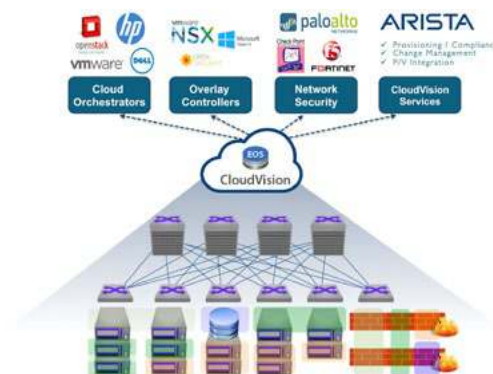


Figure 1: Arista CloudVision Services

Addressing a Growing Gap in Security Deployment Models

Macro-Segmentation Service is a new capability within Arista CloudVision that addresses a growing gap in security deployment models wherein embedded security in the virtualization hypervisors addresses inter-VM communication and physical firewalls address at-depth protection for north-south traffic leaving the data center. However, no solution exists yet to dynamically insert advanced security services for east-west 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.

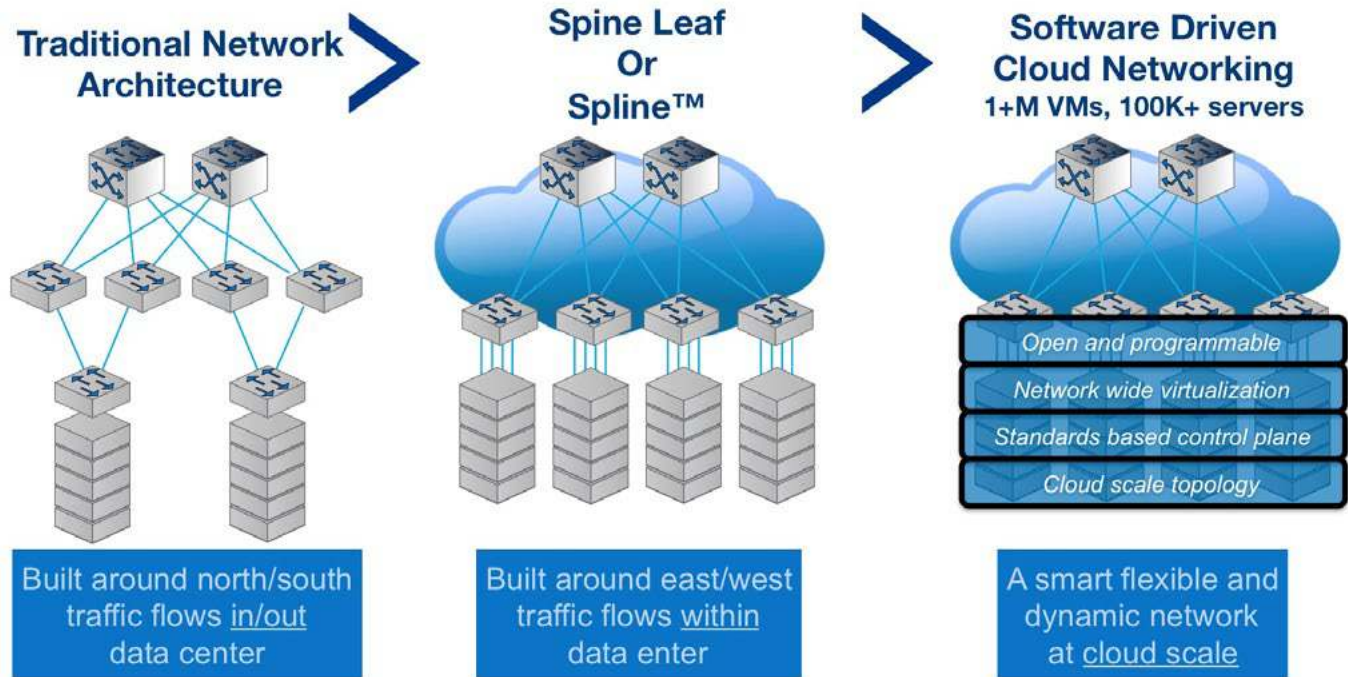


Figure 2: Evolution to Software Driven Cloud Networking

Complicating this current situation are the range of design considerations for the cloud data center operator and application users imposed by legacy applications and network architectures. Migrating from legacy three-tier architecture to two-tier leaf-spine network architecture improves network performance, but offers little mitigation for security risks as there is no longer a natural insertion point for firewalls. A more holistic network-wide segmentation approach at the macro- and micro-level is now becoming a mandate to mitigate security threats. This has been addressed in part by the implementation of distributed fine-grain security services within networking and computing hypervisors, often called micro-segmentation.

The current compromised security deployment models must change to allow dynamic placement of security services and devices within and around the cloud to protect workloads and data from outside threats as well as from those threats that have already breached the perimeter, while enabling the agility for which the cloud data center was built to begin with.

Table 1: CloudVision MSS - An open dynamic service for any workload and any application

Workload / Workflows	Requirement	Solution
Ingress-egress from the cloud	Stateful and heuristic protection from external cyber-threats and attacks	High performance next-generation firewalls and security monitoring
Inter-VM and Intra-Tenant (inside the tenant perimeter)	Isolation of workloads within tenant groups from each other and between tenants	Micro-segmentation of hypervisor workspace and embedded virtual instances of stateful firewalls
Extra-VM and intra-tenant (hybrid cloud environment)	For workloads utilizing bare-metal (non-virtualized) storage and server resources in combination with hypervisor resident components of micro-segmentation	Strong segmentation of resources within and across the cloud network with physical VLAN and VXLAN isolation, plus dynamic insertion of stateful next-generation firewalls and monitoring

The Role of Arista Macro-Segmentation Service

Macro-Segmentation Service is a complement to fine-grained security services delivered via micro-segmentation, which is implemented in the virtual switch of the physical host on which a VM is running. The delivery of enhanced micro-segmentation security via platforms like VMware NSX is one of the most significant features enabled by network virtualization. Macro-segmentation extends the concept of fine-grained intra-hypervisor security 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.

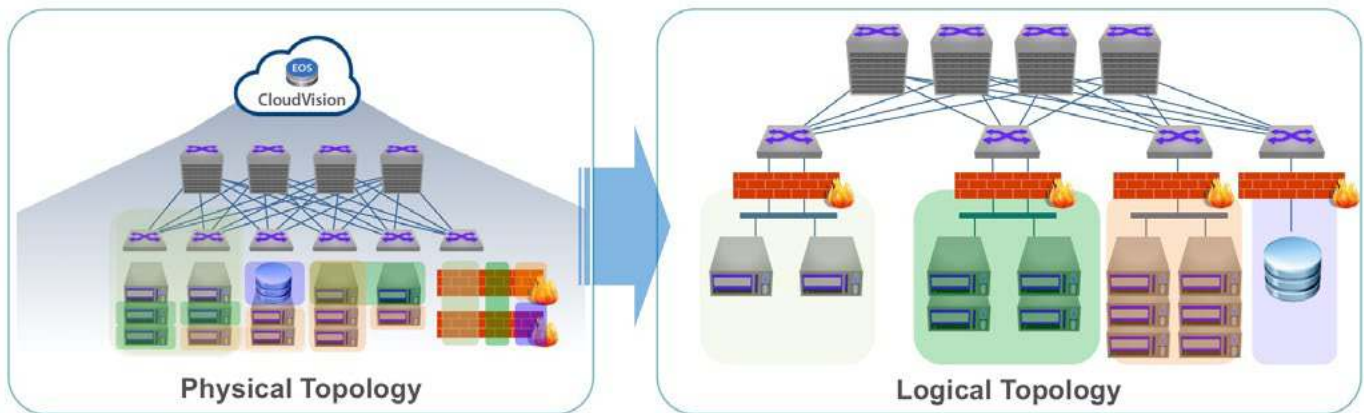


Figure 3: Placement of Security Platforms within Logical Topology with Macro-Segmentation Service

Macro-segmentation provides a software-driven dynamic and scalable network service to insert security devices into the path of traffic, regardless of whether the service device or workload is physical or virtual, and with complete flexibility on placement of service devices and workloads.

Arista MSS Key Characteristics

Macro-Segmentation is one of the services enabled by Arista CloudVision. Since CloudVision maintains a network-wide database of all state within the network, it is aware of where every workload is within the network, and it learns in real time

By integrating with native APIs provided by the leading next-generation firewalls — native APIs that already exist — macro-segmentation learns which workloads the security policy needs to address or monitor.

about new devices or workloads that are added or removed from the network, or moved across ports or servers.

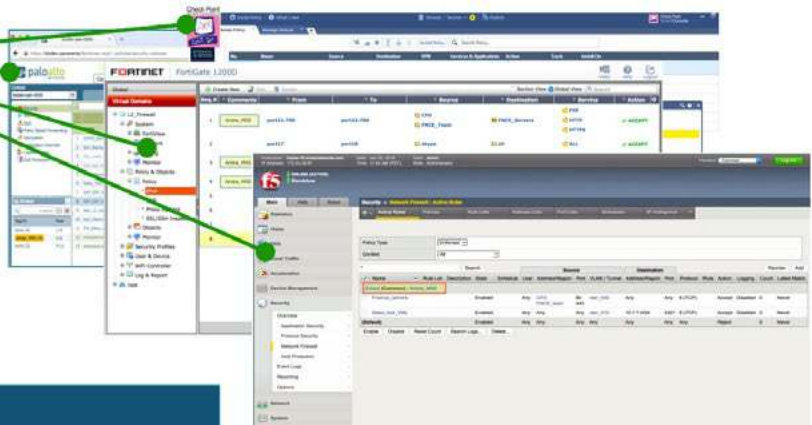
- **Complete flexibility on locality of devices:** Service devices such as firewalls or load balancers can be anywhere in the network on any switch. This allows larger datacenters to centralize their security devices in a service rack and insert them in the path between any workloads on-demand or based on a firewall policy. There are no restrictions or limitations on where the service devices are physically attached within the fabric. Likewise, devices to whom services are targeted can be located anywhere in the network with no restrictions or limitations on physical placement.
- **No new frame formats:** There is no requirement for any new frame format, traffic steering or metadata in any new header fields. Macro-Segmentation inserts service devices into the path of traffic without requiring any new frame format, protocol, or anything else that is proprietary. This allows traffic to be monitored by existing tools and ensures that any platform can be easily integrated without modifications.
- **Non-proprietary:** Standards-based forwarding is used to stitch service devices into the path of traffic. To emphasize just how open the approach is, Macro-Segmentation can fully function if the network is comprised of devices from multiple vendors.
- **Dynamic:** Hosts can and do move (vMotion and Disaster Recovery), so services and dynamic service insertion should move with them. This is automatically accomplished with Macro-Segmentation and Arista VM Tracer.
- **Enhances next-generation firewalls:** Arista's Macro-Segmentation Service does not try to "own policy" or run a controller-of-controllers that understands every application flow or interaction. Customers prefer to define security policies within the security tool framework, such as the next-generation firewall manager.

Support for Next Generation Security Platforms: An Open Ecosystem Approach

By integrating with native APIs provided by the leading next-generation firewalls — native APIs that already exist — macro-segmentation learns which workloads the security policy needs to address or monitor. If the security policy requires a specific logical network topology, then the macro-segmentation service can instantiate that topology into the network. The automation capabilities of Arista Macro-Segmentation security operate automatically, in real-time, 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 successful deployment of security in an enterprise private or hybrid cloud.

Security Admin owns the security policies

- NO network administrator involvement or software change is required on firewalls
- NO network-device configuration on firewalls (simply add user-defined tags to policies)



```

cvx#
cvx#
cvx#configure
cvx(config)#cvx
cvx(config-cvx)#service macro-segmentation
cvx(config-cvx-macro-segmentation)#macro-segmentation-?
macro-segmentation-group macro-segmentation-service

cvx(config-cvx-macro-segmentation)#macro-segmentation-group svc_name svc_node
cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#management-ip-address svc_node
cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#management-username admin password aSecr3T
cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#tag Arista_MSS
cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#state ?
activate Activate the service
dry-run Test or validate what a service would do
suspend Suspend the service

cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#state active
cvx(config-cvx-macro-segmentation-svc_name-service-svc_node)#exit
cvx#
    
```

Network Admin owns the configuration for network-wide services

Macro-Segmentation service is enabled within CloudVision as an automation rule

- Learns what tagged security policies exist
- Learns what end devices policies apply to and logically instantiates them into the path
- Reports results to firewall and log file

Figure 4: Example of Macro-Segmentation Configuration with Next Generation Firewall Policy

Conclusion

Macro-Segmentation Service with Arista CloudVision enables flexible deployment of security in the network, without forklift upgrades and without any proprietary lock-ins. It works in unison with server, storage, and network virtualization solutions from Arista's partners, including OpenStack, Docker, Microsoft and VMware. Macro-Segmentation Service complements the intelligence and functionality these provide with enhanced deployment of physical workloads and security services to enable deployment of the complete software defined data center.

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



Copyright © 2016 Arista Networks, Inc. All rights reserved. CloudVision, and EOS are registered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. 07/16