

# CHECK POINT + ARISTA

## WITH CLOUDVISION MACRO-SEGMENTATION SERVICE

### Benefits

Today's cloud data center environments need a more flexible approach to deploying security infrastructure that adapts to constant workload changes, additions and movements. Capacity of security solutions need to scale upward to match the broadened attack surface of multi-tenant shared cloud environments.

How can customers address network based security as a dynamic pool of resources, stitching security to applications and transactions, scaling on demand, automating deployment and mitigation, and allowing transparent application of security policies?

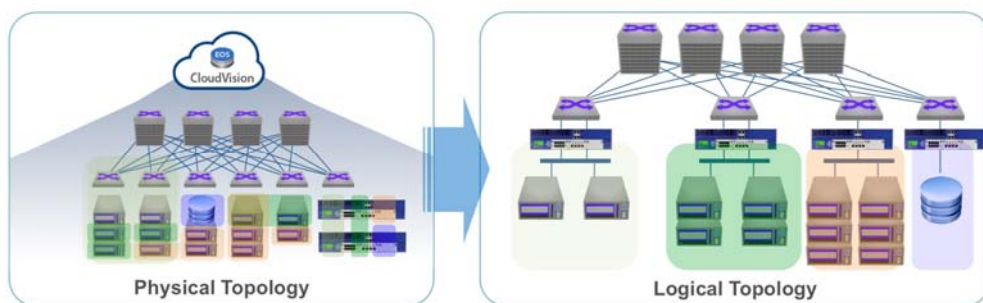
- *Arista's Macro-Segmentation™*: inserting services between workgroups (inter-tenant or inter-device) in the physical network by defining inter-segment service policies - enforced by the Arista cloud networking infrastructure.
- *CloudVision® Macro-Segmentation Service (MSS™)*: an extension in Arista EOS® software that utilizes Arista CloudVision® to automate security service insertion for Check Point's industry-leading next-generation firewalls and other networked devices.

ARISTA®, EOS®, CloudVision™, Macro-Segmentation™ and MSS™ are trademarks of Arista Networks, Inc.

### INSIGHTS

Data centers have increasingly virtualized and partitioned, becoming more dynamic and accommodating on-the-fly deployment of new applications in private, public and hybrid clouds. As the IT environment becomes more open and less controlled, the threat landscape is evolving so fast with new threats, new techniques, new actors and new targets. Businesses need to protect their private, public or hybrid environments from an increasingly threatening backdrop within the cloud.

Today's cloud environments need a more flexible approach to deploying security that adapts to constant workload changes, additions and movements. Modern data centers need a solution for insertion of high-performance security platforms into the physical and logical topology using an open, programmable and integrated network framework.



**Figure 1.** Placement of Security Platforms within a Logical Topology

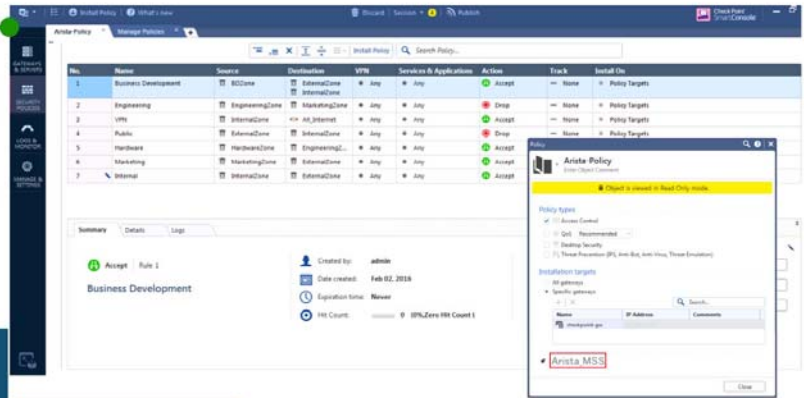
Arista Networks™, the leading provider of cloud networking solutions, has unveiled a new Macro-Segmentation Service (MSS™) capability for CloudVision® that allows Check Point Next-Generation Firewalls to be deployed automatically in a cloudified data center. With CloudVision MSS, Arista provides automated service insertion for specific workloads and workflows across any network topology including layer-2, layer-3 and VXLAN overlay network virtualization frameworks without introducing proprietary network fabrics or protocols.

### JOINT SOLUTION

With Check Point and Arista CloudVision MSS, Check Point's data center firewalls can be attached anywhere in the network on any Arista switch port. Traffic forwarding to and from the Check Point firewall is automatically routed through Arista's non-blocking and loss-less IP fabric based on the policies defined in the firewall. This allows larger data-centers to centralize security devices in a service-rack and insert them in the path between any workloads or physical devices logically, on demand, while maintaining isolation between the administrative domains of the security and network operators.

## 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 ckpt ckpt-61A
cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#management-ip-address ckpt-61A
cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#management-username admin password aSec3T
cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#tag Arista_MSS
cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#state ?
activate Activate the service
dry-run Test or validate what a service would do
suspend Suspend the service

cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#state active
cvx(config-cvx-macro-segmentation-ckpt-service-ckpt-61A)#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 2: Configuration of Check Point and Arista Solution for Cloud Data Centers

## A BETTER APPROACH TO SECURING CLOUD DATA CENTERS

By integrating with native APIs provided by Check Point data center firewalls, Arista MSS learns what workloads the security policy should address or monitor. If the security policy requires a specific logical network topology, the CloudVision Macro-Segmentation Service can instantiate that topology into the network IP fabric automatically. The automation capabilities of CloudVision MSS operate in real-time without any need for a network operator to engage a security administrator or vice-versa, and without the network needing to be architected in a manner specific to any workload. This capability is critical to successful deployment of security in an enterprise private or hybrid cloud.

Macro-Segmentation Service with Arista CloudVision is integral to Arista's non-blocking and loss-less IP fabric and Arista EOS software. With Check Point next-generation firewalls, CloudVision MSS enables flexible deployment of security in the network without forklift upgrades and without any proprietary lock-ins. MSS works in unison with server, storage, and network virtualization solutions from Check Point and Arista's partners including OpenStack, Microsoft and VMware. Macro-Segmentation Service complements the intelligence and functionality that these partners provide with enhanced deployment of physical workloads and security services to enable deployment of the complete cloudified data center.

## ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is the largest pure-play security vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 businesses and millions of users worldwide.

## ABOUT ARISTA NETWORKS

Arista Networks (www.arista.com) defined software-driven cloud networking for cloudified data centers with award-winning networking platforms that redefine scalability, agility and resilience. Arista has shipped more than five million 10-100GbE cloud networking ports worldwide with CloudVision and Arista EOS, its advanced network operating system. Committed to open standards, Arista Networks products are available worldwide directly and through partners.

### CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com  
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com