SOLUTION BRIEF

Fortinet and Arista Security Solution

Security-driven Network Automation for Unparalleled Security, Scalability on Demand, and Optimal Performance in Data Centers

Executive Summary

By combining a best-of-breed security platform from Fortinet and the Macro-Segmentation Service–Firewall (MSS-FW) from Arista Networks, modern data centers are able to meet their security needs with greater scale and performance.

Business Challenge

The explosion of mobile, bring-your-own-device (BYOD), Software-as-a-Service (SaaS), and Internet-of-Things (IoT) trends has expanded the networks and blurred the edges. The advent of technologies has put strenuous demands on data centers to extend physical networks through virtualization to multi-cloud and hybrid architectures, resulting in networking and security challenges, such as segmentation and visibility requirements, that cannot be met with siloed legacy solutions.

While network devices are processing packets at higher and higher rates, ever-increasing demand can require seamless expansion of a network, presenting a large operational challenge to IT. In addition, as the network is scaling, IT is being asked to reduce operational expenses and increase responsiveness to changing business needs.

As data-center network speeds increase, service appliances such as firewalls must scale to keep pace and match the throughputs. The notion of security as an edge technology is long antiquated, and today network security must push deeper into the core of the internal network to segregate sensitive data and to detect malicious behavior of hackers probing and malware moving laterally within the data center.

Security needs to be an integral part of the modern network to cater to the modern applications leveraging virtualization, containerization, and microservices.

Joint Solution

Fortinet and Arista have partnered to deliver an industry-leading security solution to address these challenges. Macro-Segmentation Service (MSS)–Firewall (FW) is an Arista CloudVision-enabled application that provides a software-driven, dynamic, and scalable network service to dynamically insert service devices into the path of traffic. The integration of the service insertion capabilities of Arista's MSS-FW with the advanced security capabilities of a FortiGate next-generation firewall (NGFW), and the centralized management of FortiManager, which can manage multiple firewalls, enable users to benefit from greater scalability, advanced security, and cost savings, allowing network administrators to size the firewall to meet the data-center traffic and business needs.

Bringing the Fortinet FortiGate NGFW and Arista MSS-FW products together in an integrated solution delivers advanced data threat protection to organizations that can be placed anywhere in their physical, multi-cloud, or hybrid networks.

Joint Solution Components

- Arista Networks Macro-Segmentation Service – Firewall or MSS-FW
- Fortinet FortiGate Next-generation Firewall, FortiManager

Joint Solution Benefits

- **Service Insertion:** Service devices such as firewalls can be anywhere in the network on any switch.
- **Secure Segmentation:** Enhanced security between any physical and virtual workloads in the data center.
- **Automation:** The automatic and seamless service insertion ability of MSS-FW eliminates manual steering of traffic for a workload or a tenant.
- **Consistent Security:** Consistent security policies are applied to the host and application throughout the network.
- **Flexibility:** MSS-FW is flexible since there are no proprietary frame formats, tagging, or encapsulation.
- **Advanced Security:** Increased scale and performance for DoS Attack Mitigation, Elephant Flow Offload, Firewall Scaling, and Traffic redirection.

FORTINET FABRIC-READY

Joint Solution Components

Arista Networks Macro-Segmentation Service–Firewall

Arista Networks CloudVision software automates the insertion of security services with Macro-Segmentation Service–Firewall for both physical and virtualized (i.e., physical-to-physical [P-to-P] and physical-to-virtual [P-to-V]) workloads anywhere on the network with a leading ecosystem of service and security partners including Fortinet, Palo Alto Networks, and Check Point Software. This modern approach to security device deployment is enabled via integration of advanced security with the dynamic network segmentation of the cloud data center, by workload and by tenant, without any dependency on proprietary packet headers or protocols.

Further, the solution provides offload capability of firewall rules to the network (at Layer 3 and Layer 4), delivering a scaled solution for high-performance data centers.

Arista Networks Macro-Segmentation Service–Firewall

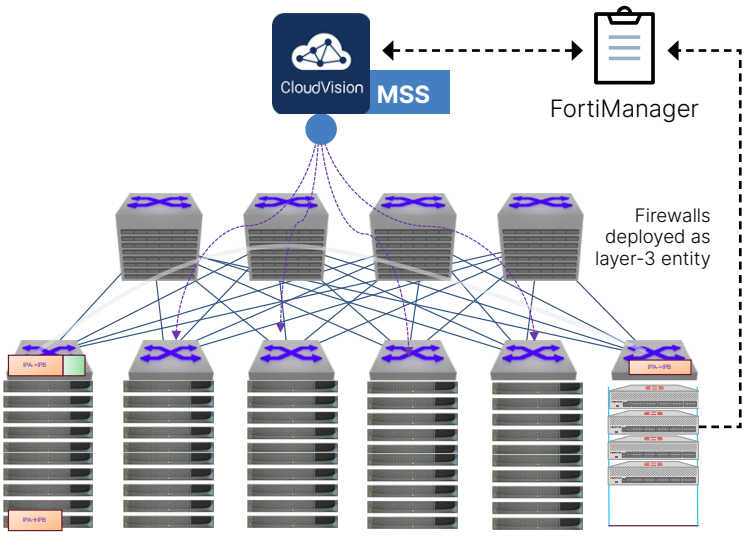
The FortiGate NGFW for data centers delivers high-performance NGFW capabilities for large enterprises and service providers. With multiple high-speed interfaces, high port density, and high throughput, ideal deployments are at the enterprise edge, hybrid data-center core, and across internal segments. Organizations can leverage industry-leading intrusion prevention (IPS), secure socket layer (SSL) inspection, and advanced threat protection to optimize your network's performance. The Fortinet Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Joint Solution Integration

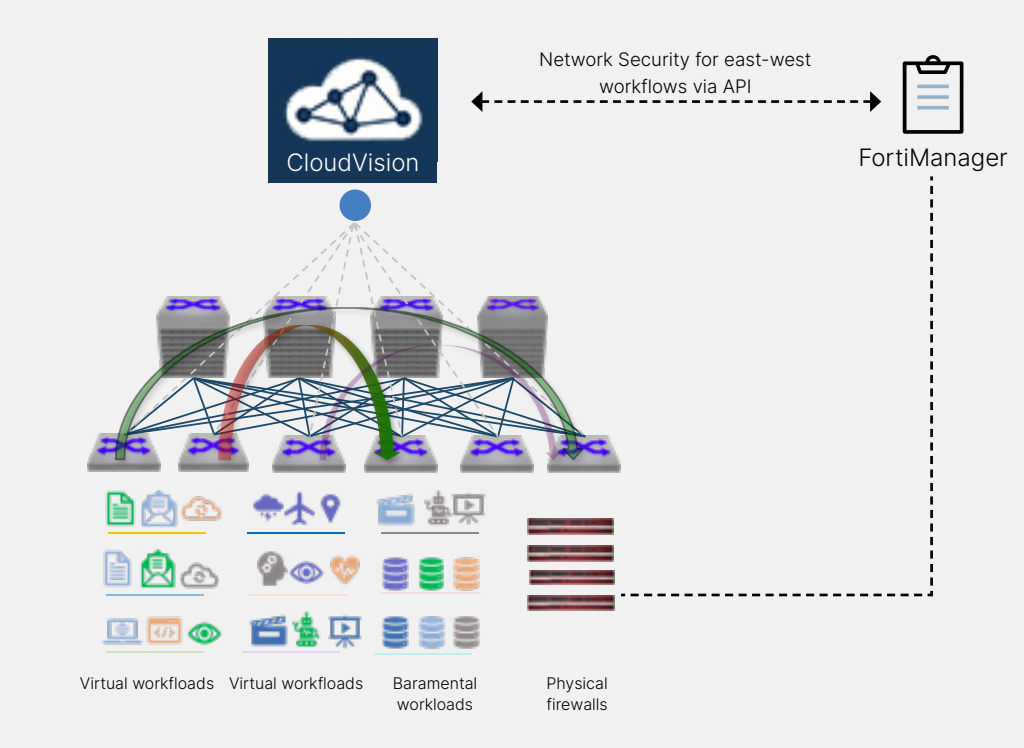
Arista's MSS-FW and Fortinet FortiGate integration solves the problem of securing traffic between workloads, virtual machines (VMs), and servers. Arista Macro-Segmentation Service–Firewall (MSS-FW) provides a software-driven dynamic and scalable network service to insert security devices into the path of traffic. It also gives flexibility on placement of service devices (firewall) and workloads.

In a typical DC environment, traffic flows across racks, when there is no policy instituted. Security admins program policies in the firewall, which are applied as rules. Arista CloudVision communicates with the Fortinet FortiManager to get the policies of interest and apply these policies to the network, to steer the traffic of interest to the firewalls. As the configuration is applied on the network leaf switches, the traffic starts to flow to the firewalls for further inspection. In the event of a policy change, for example, a policy change is needed to deny an existing flow. The security admin modifies the policies in the firewall. As these take effect, the network continues to steer traffic in accordance to the new policy. There is no change required on the network side. The firewall implements this new change.

MSS-FW Packet Walk Firewall Policy Redirect



1. Security admin programs rules in the firewall
2. MSS enabled in CloudVision, talks to FW/FW Manager to obtain tagged rules of interest
3. Upon receiving rules, MSS programs the intercept rules on the leaf switches
4. Once rules are programmed, TORs/Leaf switches intercept traffic of interest, on the access port
5. The intercept frames are encapsulated into a tunnel and sent to the ToR connecting the firewall
6. Firewall will apply "all" rules for the frame and will forward/log or drop the frame
7. If firewall forwards the frames, the ToR receives the original frame and forwards it to the intended destination



Arista Macro-segmentation Service—Firewall

Transparent insertion of firewall/service

- No new tagging or encapsulation
- One point of control—e.g., the security policy manager
  - For both physical and virtual firewalls
- Directly maps to security model—zones etc.
- No server reconfiguration
- No per application overhead

Figure 1: Fortinet FortiGate and Arista MSS-FW joint solution.

Joint Use Cases

Use case 1: Flexible deployment of firewalls anywhere in the network

Flexible deployment of firewalls anywhere in the network on any switch enables data centers to centralize their security devices in a service rack and logically 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.

What makes MSS-FW unique is that it places the control of policy enforcement directly in the hands of security administrators. This is accomplished using standards-based forwarding with no proprietary frame formats and without placing limitations on where the devices must exist within the network.

Use case 2: Securing east-west traffic between P-to-P and P-to-V servers

Prior to Arista's Macro-Segmentation, security was accomplished through a "firewall sandwich" approach where firewalls are placed in-line between security zones. A "firewall sandwich" represents significant architectural challenges and can impact both scalability and performance.

Use case 3: Dynamic policy migration

One of the key issues facing modern data centers is that the security policies are often dependent on network topology. With virtualization, workload mobility allows for independence of placement of workloads, based on compute power requirements. In case of a workload mobility event, network policies will need to be reconfigured on the switch(es) connected to the host, where the endpoint moved to, to redirect traffic to the firewall. This makes the network and the security administrators co-dependent and prone to errors/delays.

With MSS-FW, security admins own security policies, without any other domain admins getting involved. As the endpoint moves to another rack or leaf switch, the same security rules will be enforced.

Server virtualization and the help of EVPN-VXLAN Open Standard implementation adds Network Virtualization adds scalability and performance in the data center. This ensures workloads can be dynamically placed anywhere, removing traditional Layer 3 boundaries of the physical infrastructure. Using Arista MSS-FW, this restriction of firewall placement is removed. Firewalls can now be attached to a service leaf switch in the network fabric and still protect hosts without regard to their physical location.

About Arista

Arista Networks pioneered software-driven, cognitive cloud networking for large-scale datacenter and campus environments. Arista's award-winning platforms, ranging in Ethernet speeds from 10 to 400 gigabits per second, redefine scalability, agility and resilience. Arista has shipped more than 20 million cloud networking ports worldwide with CloudVision and EOS, an advanced network operating system. Committed to open standards, Arista is a founding member of the 25/50G consortium. Arista Networks products are available worldwide directly and through partners. Find out more at www.arista.com.

July 16, 2021 1:05 AM
1154101-A-0-EN