ARISTA EOS: DIRECTFLOW ASSIST FOR FORTIGATE FIREWALLS

As datacenter network speeds increase from 10Gbps to 40Gbps and 100Gbps, service appliances such as firewalls need to be scaled to match these throughputs. By leveraging the programmability of Arista's Extensible Operating System (EOS®) with the advanced security capabilities of a Fortinet next-generation firewall, Arista DirectFlow Assist enables a scale-out architecture where the switch can offload traffic from the firewall. This provides greater scalability and cost savings, allowing network administrators to size the firewall based on normal traffic patterns rather than having to over-engineer for exceptional traffic.

Fortinet provides best-in-class network security through its award-winning FortiGate® network security platform and the Fortinet Security Fabric. Fortinet's FortiGate enterprise firewalls provide high performance, consolidated advanced security and granular visibility for broad protection across the entire digital attack surface. FortiGate enterprise firewalls reduce complexity and improve overall security posture by providing full visibility into users, devices, applications and threats on the network, with the ability to apply advanced threat protection anywhere in the network.

Fortinet's purpose-built security processors (SPUs) deliver scalable performance of advanced security services, industry-leading VPN and SSL inspection throughput, and ultra-low latency for protecting internal segments and mission critical environments.

In addition, the Fortinet Security Fabric enables security components to collect and share intelligence between devices, systems and partners, support unified management, and synchronize and automate responses to threats. The open, end-to-end fabric of security solutions—woven together to scale and adapt as business demands change—enables organizations to address the full spectrum of challenges they currently face across the expanding attack surface.

ARISTA EOS

Arista EOS is designed to provide a foundation for the business needs of next-generation datacenters and cloud networks. One of the key highlights of EOS is that it is programmatic across all layers—Linux kernel, hardware forwarding tables, Virtual Machine orchestration, switch configuration, provisioning automation and detailed monitoring of the network. Leveraging EOS programmability, users can build EOS Extensions (scripts, APIs, daemons, etc.), which are applications built around EOS.

DIRECTFLOW ASSIST OVERVIEW

DirectFlow Assist (DFA) is an EOS extension that runs on an Arista switch to dynamically insert flow table entries via Arista's DirectFlow API, to offload or assist an attached in-line or out-of-band security platform such as a firewall. By providing integrated control over network forwarding to the firewall, DFA allows dynamic security policies to be applied in the network based on intelligence derived from out-of-band monitoring, deep packet inspection (DPI), and other analysis platforms.

The scaling and performance benefits of DFA integration allows security platforms to scale performance up to 10-50x over static in-line deployments and provide a scaling model that can be applied in any virtualized or cloud-based environment.

HIGHLIGHTS

ARISTA AND FORTINET

By combining a best of breed security platform from Fortinet, and the extensibility of the Arista EOS platform, datacenters are able to meet their security needs with greater scale and performance.

DIRECTFLOW ASSIST

Provides increased scale and performance for:

- DoS Attack Mitigation
- Elephant Flow Offload
- Firewall Scaling
- Traffic redirection

FORTINET Fabric-Ready

Use cases include:

- Denial of Service (DoS) Attack mitigation - Selectively block traffic based on DoS detection by the FortiGate.
- Elephant Flow Offload – Insert flow entries to bypass the firewall for high bandwidth traffic from a trusted application, such as backup data, after the firewall has identified the traffic.
- Firewall Scaling – Provide flow-by-flow bypass and filtering based on firewall DPI.
- Redirection of target traffic to a “honeypot” or decoy platform for profiling.

ARISTA DIRECTFLOW ASSIST AND FORTINET SOLUTION

The Arista DFA extension for FortiGate leverages the deep packet inspection and syslog functionality of a Fortinet next-generation firewall to insert DirectFlow entries onto the Arista switch for the use cases listed above. These entries will provide custom forwarding behavior on the switch to bypass the firewall or drop packets before reaching the firewall.

For the Elephant Flow use case (Figure 1), a firewall policy is configured to send syslog messages to the switch for a traffic flow that should be forwarded without further inspection. This syslog message is received by the DFA process, and is parsed to create a flow specification. The flow specification includes a unique flow name, match criteria, desired action, priority, and lifetime. Match criteria may include source and destination IP addresses, source and destination layer-4 ports and protocol (ICMP, TCP or UDP) depending on the type of flow and custom configuration file settings.

The action on the switch will be to output packets to a specific switch port in order to bypass the firewall. An additional flow specification is automatically created in the reverse direction for return traffic. Flow entries can use aging to delete the flow entry after a specified time interval, or flows can be explicitly removed by the firewall.

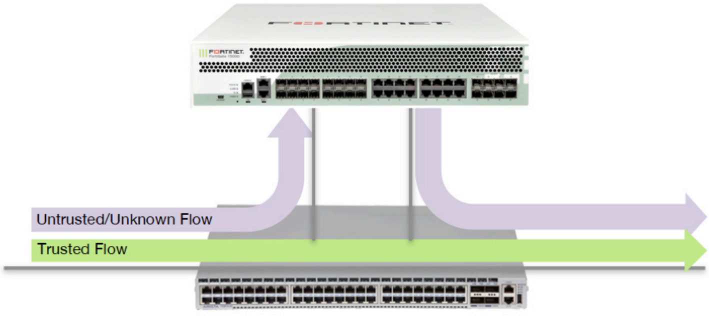

FIGURE 1: DFA FOR ELEPHANT FLOW OFFLOAD

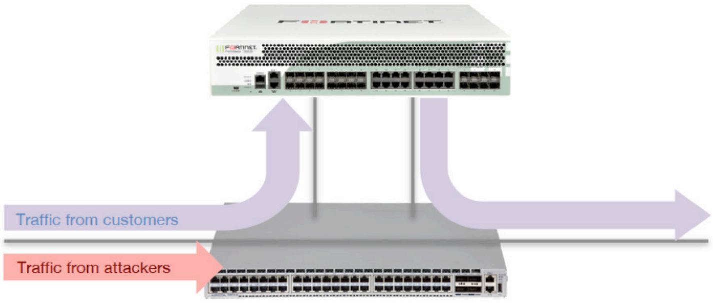

FIGURE 2: DFA FOR DOS ATTACK MITIGATION

In the DoS attack use case (Figure 2), the firewall policy is configured to send syslog messages to the switch for a traffic flow that has been marked as a DoS attack. As in the previous scenario, the syslog message is received by the DFA process, and is parsed to create a flow specification. In this case the action on the switch will be to drop matching packets entering a specific port, blocking the malicious traffic at the point of ingress. Once the flow is blocked, the firewall will no longer need to inspect the DoS traffic.

CONCLUSION

Direct Flow Assist is an example of the flexibility of Arista’s Software Driven Cloud Networking (SDCN) capabilities and the benefits of an open standards-based approach to data center networking. Arista’s SDCN, in combination with the advanced security platform from Fortinet, provides an effective, scalable security solution for modern cloud data centers. By combining the Fortinet Security Fabric with the extensibility of the Arista cloud networking solutions, including the Arista DFA and CloudVision MSS, modern datacenters are now able to meet their security needs with even greater flexibility, control and automation.

FORTINET

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990