Arista EOS: DirectFlow Assist for FortiGate Firewalls

INSIDE

EXECUTIVE SUMMARY
As data center 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 NEXT-GENERATION FIREWALLS

Fortinet's industry-leading, high capacity Firewall technologies provide broad security functionality along with exceptional throughput and ultra-low latency, enabling hyper-scale security, flexibility, and manageability. FortiGate appliances and chassis-based devices combine Fortinet's high-performance Firewall with the flexibility to enable multiple additional fully-integrated layers of sophisticated security functionality, such as Intrusion Prevention, VPN, and Application Control, for extensive protection and in-depth defense. Fortinet built the FortiGate line of Network Security Platforms, and the accompanying management and reporting tools, to exceed the requirements of even the most demanding data center and carrier environments.

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.

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.

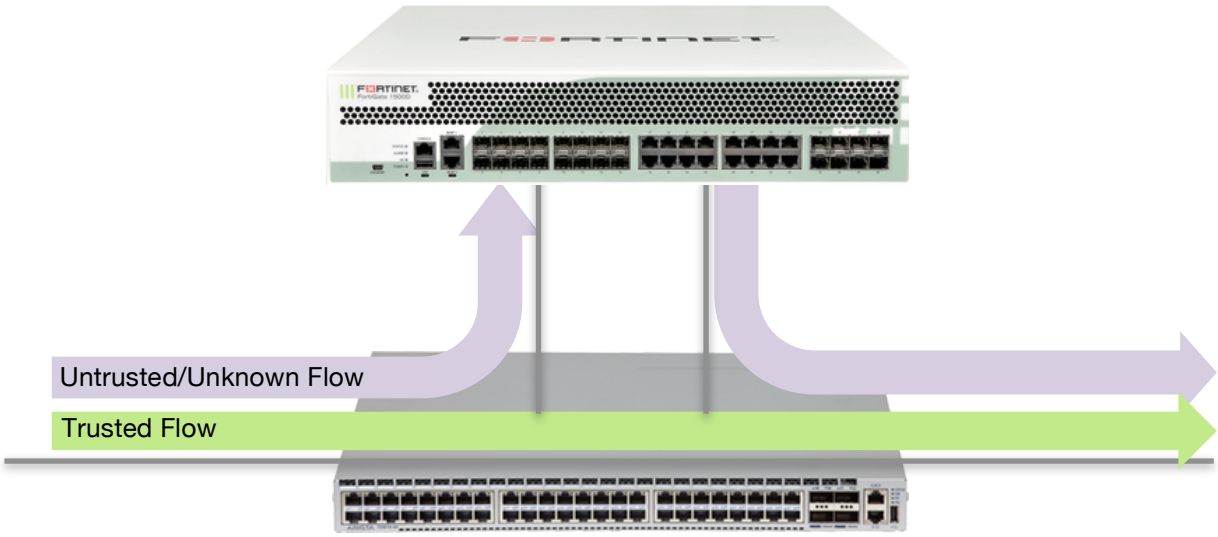

Figure 1: DFA for Elephant Flow Offload

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.

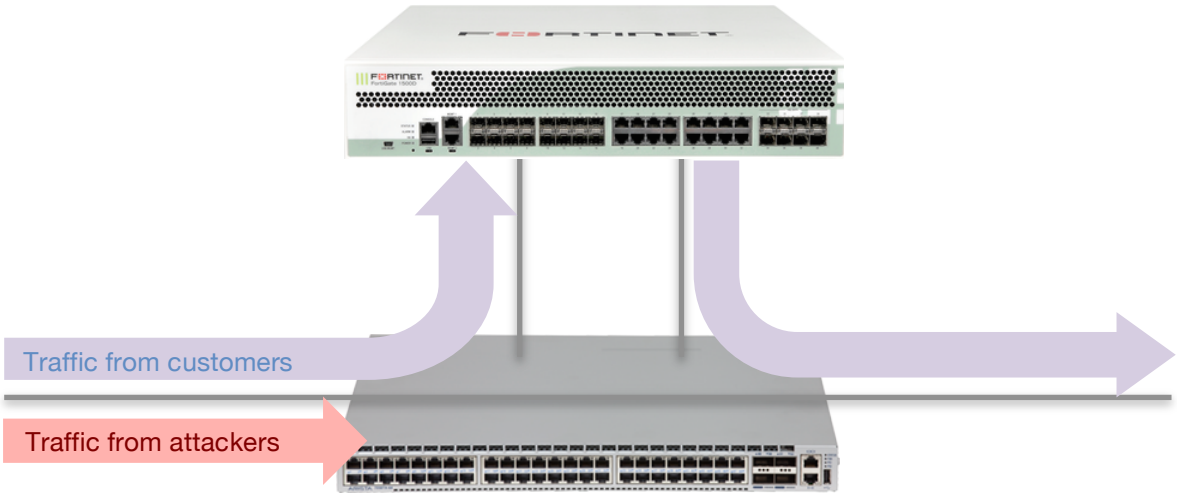

Figure 2: DFA for DoS attack mitigation

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.

Fortinet, Inc.
Sunnyvale—Corporate Headquarters
899 Kifer Road
Sunnyvale, CA 95086
Tel: 408-235-7700

ARISTA

Santa Clara—Corporate Headquarters
5453 Great America Parkway
Santa Clara, CA 95054
Tel: 408-547-5500
www.arista.com

Ireland—International Headquarters
4130 Atlantic Avenue
Westpark Business Campus
Shannon
Co. Clare, Ireland

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989