Solution Brief

Arista EOS: DirectFlow Assist for Palo Alto Networks Firewalls

Inside

Arista and Palo Alto Networks

By combining a best of breed security platform from Palo Alto Networks, and the extensibility of the Arista EOS platform, data centers 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

As data center network speeds increase from 40Gbps and 100Gbps, service appliances such as firewalls need to be scaled up to match these throughputs. By leveraging the programmability of Arista Extensible Operating System (EOS) with the advanced security capabilities of a Palo Alto Networks 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.

Palo Alto Networks Next-Generation Firewalls

The Palo Alto Networks next-generation firewall natively inspects all traffic, inclusive of applications, threats and related content. The identity of the traffic, irrespective of port, protocol, evasive tactic, or SSL encryption then becomes the basis for all firewall policy decisions. The result is an improved ability to safely enable the applications traversing the network and block sophisticated cyber attacks—known and unknown.

Arista EOS

Arista EOS® (Extensible Operating System) 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.

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.

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 provides 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 Palo Alto Networks firewall
- 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 Palo Alto Networks Solutions

The Arista DFA extension for PAN leverages the deep packet inspection and syslog functionality of a Palo Alto Networks 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.

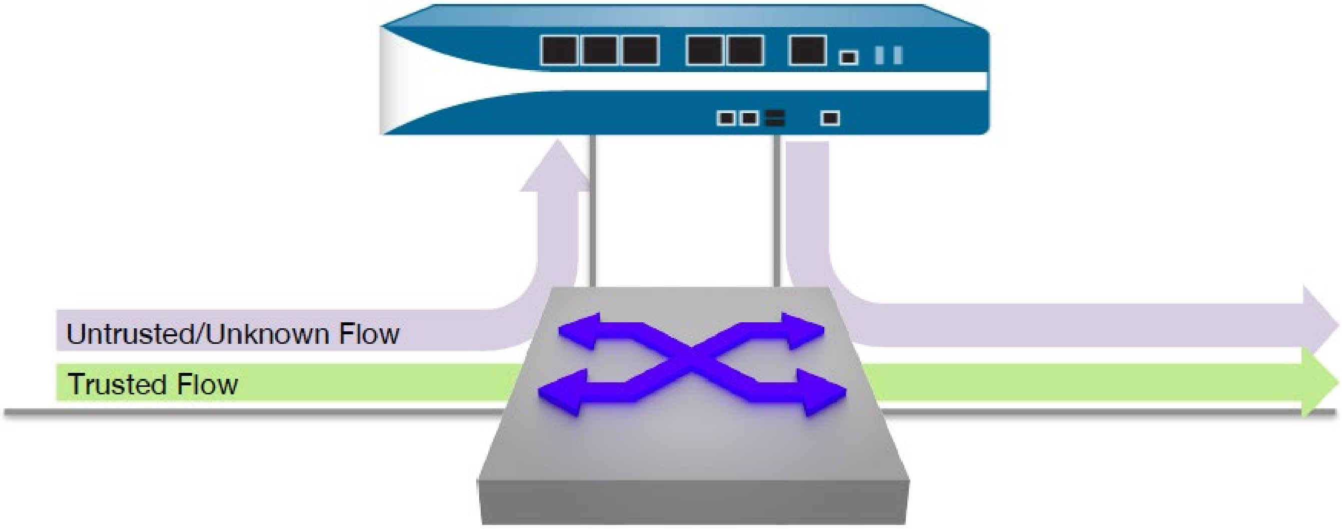

Figure 1: DFA for Elephant Flow Offload

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.

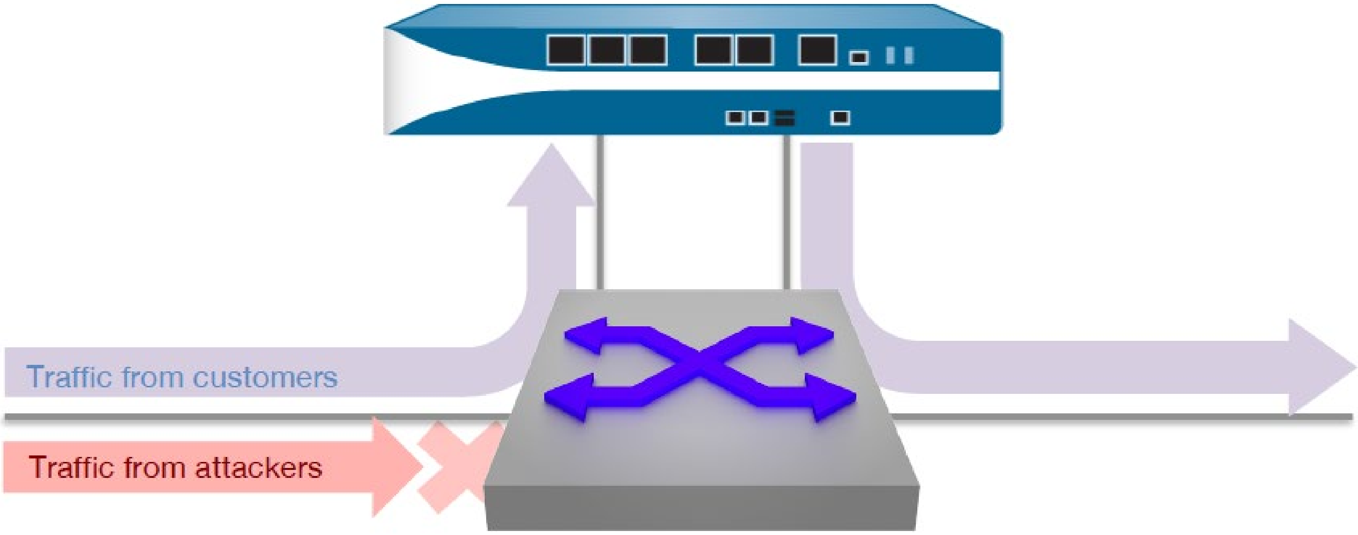

Figure 2: DFA for DoS attack mitigation

DFA 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.

Conclusion

DFA 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 Palo Alto Networks, provides an effective, scalable security solution modern cloud data centers.

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