PALO ALTO NETWORKS AND ARISTA NETWORKS

Delivering Best-of-Breed Security and High-Performance Cloud Networking

Key Benefits of the Integration

Provides increased scale and performance for:

- DoS attack mitigation
- Elephant flow offload
- Firewall scaling
- Traffic redirection

The Challenge

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

Arista EOS and DirectFlow Assist

Arista DirectFlow Assist (DFA) is an EOS extension to assist attached security appliances such as firewalls, which 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 technologies.

Palo Alto Networks

Palo Alto Networks Security Operating Platform® prevents successful cyberattacks through intelligent automation. The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities, at the right place, across all stages of an attack lifecycle.

Palo Alto Networks and Arista DirectFlow Assist

The Arista DFA extension for Palo Alto Networks Next-Generation Firewalls in the data center (PA-3200 Series, PA-5200 Series, and PA-7000 Series) leverages the deep packet inspection and syslog functionality of a Palo Alto Networks Next-Generation Firewall to insert DirectFlow entries into the Arista switch for the use cases listed below. These entries will provide custom forwarding behavior on the switch to bypass the firewall in the data plane or drop packets before reaching the destination.

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 as well as traffic and content inspection (from the firewall platforms) to quickly detect and protect against threats across the Arista data center fabric (north-south and east-west traffic flows).

Use Case No. 1: 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 policy is configured to send syslog messages to the Arista switch for a traffic flow that should be forwarded without further inspection. This syslog message is received by the DFA process and 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.

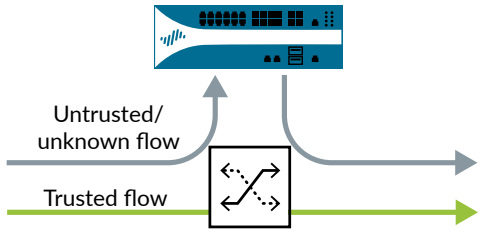

Figure 1: DFA for Elephant Flow Offload

Use Case No. 2: Denial-of-Service Attack Mitigation

Selectively block traffic based on DoS detection by the Palo Alto Networks firewall

Firewall policy is configured to send syslog messages to the switch for a traffic flow that has been marked as a DoS attack. The syslog message is received by the DFA process and 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. This provides 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.

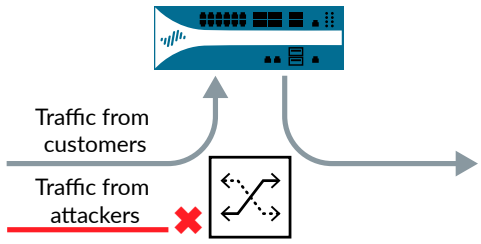

Figure 2: DFA for DoS mitigation

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.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

palo-alto-networks-and-arista-tpb-062619