DirectFlow Assist for DDoS Mitigation

Arista Networks EOS and A10 Networks TPS

Inside

Arista and A10 Networks

By combining a best of breed security platform from A10 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:

- DDoS Attack Mitigation
- TPS Scaling
- Traffic redirection

As data center network speeds increase from 10Gbps to 40Gbps and 100Gbps, service appliances that protect the network from malicious attacks need to scale up to match these throughputs. By leveraging the programmability of Arista Extensible Operating System (EOS) with the advanced security capabilities of the A10 Thunder™ Threat Protection System (TPS), Arista DirectFlow Assist enables a scale-out architecture where the switch can mirror traffic to the A10 TPS for DDoS inspection. Based on threat notifications from A10's TPS, the switch redirects the traffic for the servers that are under attack towards the TPS, which in turn mitigates the attack. The switch passes through good traffic and allows optimization of TPS resources to address real attacks. This provides greater scalability and cost savings, allowing network administrators to size the security resources based on normal traffic patterns, rather than having to over-engineer for exceptional traffic.

A10 Thunder Threat Protection System (TPS)

A10 Thunder TPS provides high-performance, network-wide protection against distributed denial of service (DDoS) attacks, and enables service availability against a variety of volumetric, protocol, resource and other sophisticated application attacks. Built on A10's Advanced Core Operating System (ACOS), Thunder TPS provides efficient, hardware accelerated performance to detect and mitigate the largest attacks, with capacity ranging from 10-155 Gbps in one single rack unit.

By providing integrated control over network forwarding of flows to the TPS, 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.

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 Threat Protection System (TPS). By providing integrated control over network forwarding of flows to the TPS, 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 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:

- Distributed Denial of Service (DDoS) Attack mitigation - Selectively block traffic based on DDoS detection by the A10 TPS.
- Threat Mitigation Scaling – Provide flow-by-flow bypass and filtering based on TPS scrubbing and analysis.
- Redirection of target traffic to suite of tools for profiling.
- Rapid service insertion for DDoS mitigation
- Lower cost and latency for traffic vs. full-time symmetric deployment of the DDoS solution
- DirectFlow mirroring and relative flow priorities enables redirection to scrubbing/mitigation with a higher priority flow than the detection stream to avoid duplicate detection
- DirectFlow enables precise fine-grain flow redirection to DDoS mitigation device. Currently most other solutions are reliant on BGP for redirection at scale which is limiting and not surgical enough.

Arista DirectFlow Assist and A10 Thunder TPS Solution

The Arista DFA extension for A10 Thunder TPS leverages the deep packet inspection, detection, mitigation and syslog functionality of the A10 Thunder TPS to insert DirectFlow entries onto the Arista switch for various use cases, some of which are listed above. These entries will provide custom forwarding behavior on the Arista switch to redirect suspicious traffic and flows flagged by the TPS to its DDoS mitigation subsystem whilst allowing good traffic to flow through the network.

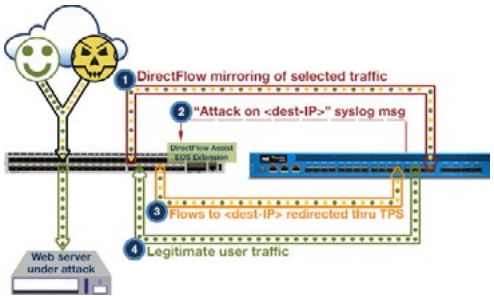

Figure 1: DFA for DDoS attack mitigation

A TPS policy is configured to send syslog messages to the switch for a traffic flow that should be redirected for mitigation. 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.

In the DDoS attack use case (Figure 1), the TPS policy is configured to send syslog messages to the switch for a traffic flow that has been marked as a DDoS 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 redirect matching packets entering a specific port, blocking the malicious traffic at the point of ingress and redirecting them to the scrubber port on the TPS for further analysis and profiling.

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 next-generation DDoS protection platform from A10 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