Real-Time SDN and NFV Analytics for DDoS Mitigation

DDoS Attacks Are Rising Dramatically

The number, size, and type of Distributed Denial of Service (DDoS) attacks have exploded over the last several years, the increasing majority being Layer 3 and 4 attacks targeting data centers. Traditional DDoS solutions are unable to respond in time or handle the immense bandwidth that these attacks impose on today's networks. Both service providers and enterprises need a scalable solution that can detect and mitigate these behavioral security threats, immediately preventing them from spreading through the network and disrupting the services of customers and users.

Efficient and Scalable DDoS Mitigation

The Real-Time SDN Analytics for DDoS Mitigation application from Brocade provides an efficient and high-performance solution to protect cloud data centers from these security threats. In this demonstration, the application leverages OpenFlow 1.3 in an OpenDaylight framework and s-Flow-RT for monitoring to handle large, long-lived flows separately from other flows at Layer 3 and 4. When an attack occurs, the application, within seconds, instructs the network comprised of OpenFlow-enabled Brocade MLXe Routers to rate-limit or drop the attack traffic flow, in hardware and without affecting the performance of the system or network. In addition, the industry's only true Hybrid Port Mode for OpenFlow allows the rest of the network to continue normally, so this solution can be seamlessly integrated with existing infrastructures today. Brocade Vyatta® vRouter is added to the solution for the increased speed, security and flexibility that Network Functions Virtualization provides. With this application, service providers can offer tiered DDoS services to customers, and enterprises can have stronger and more efficient DDoS mitigation.

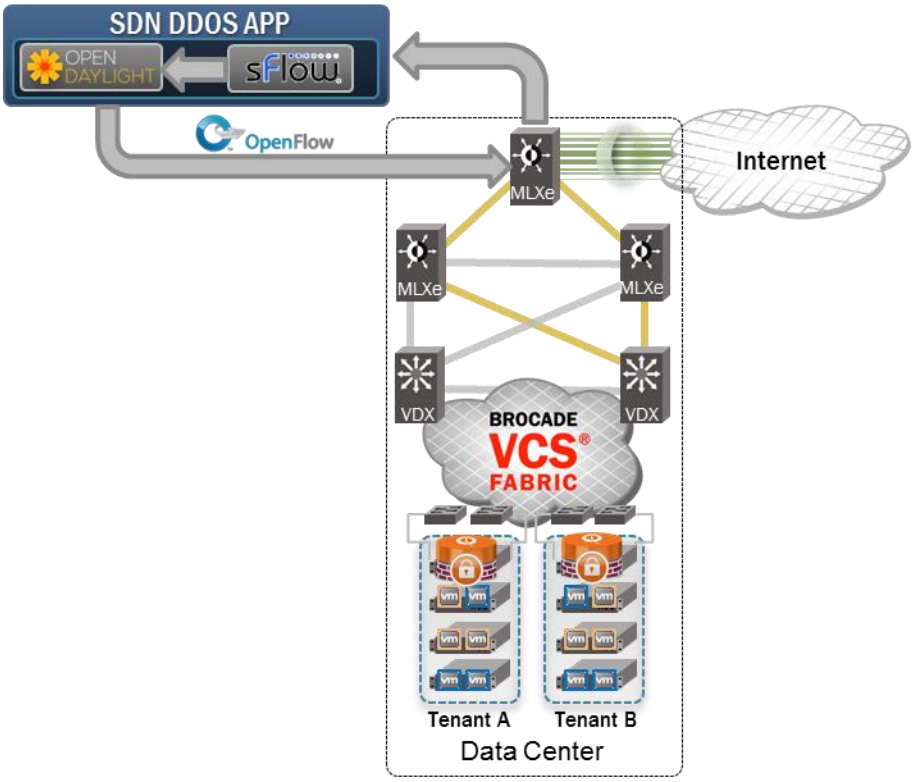
Demo Details:

In this demonstration, a Layer 4 DDoS attack will be simulated. sFlow-RT will detect the large, long-lived flows in real-time, and using RESTful API's will convey the attack to the SDN DDoS Application. The application maps the attack to a relevant QoS action, drop in this instance, and pushes the action using a RESTful API to the OpenDaylight controller, which maps it into an OpenFlow rule for the Brocade MLXe router to drop the traffic. In an additional, use case the Brocade Vyatta 5400 vRouter is used to show the power of Network Function Virtualization. This demonstrate how various Layer 2-4 DDoS attacks, e.g. NTP reflection attack, being handled in real-time and inline using a virtual router.

This demonstration consists of:

- Brocade MLXe Series Router with key software features:
  - OpenFlow 1.3
  - sFlow-RT
- Brocade Vyatta 5400 vRouter
- OpenDaylight Controller

Figure 1. Diagram of Real-Time SDN Analytics for DDoS Mitigation Application.



BROCADE