Flow-Aware Real-Time SDN Analytics

Brocade Volumetric Traffic Management Solution and Thought Leadership

Santosh Rajvaidya, Sr. Product Manager, Brocade

Ram (Ramki) Krishnan, Director of Architecture, Brocade
Brocade Volumetric Traffic Management Solution

CONTENTS

• Security Attack Types
• Brocade Solution
• How It Works
• Demo
• Future Work
Network Security Attacks

Attack Types

• **Volumetric Attacks**
  – Overwhelm the network resources
    • NTP Reflection
    • DNS Reflection
    • UDP Flood
    • ICMP Ping Flood

• **Application Layer Attacks**
  – Targets specific characteristics of well-known applications such as HTTP, DNS, VoIP or Simple Mail Transfer Protocol (SMTP)
Brocade’s Solution
SDN based volumetric attack mitigation

• SDN application that works with Open Daylight controller
• Provides volumetric attack mitigation without disrupting the traffic path
• Policy based attack detection and mitigation with fine-grained control
• Dashboard and reports for visibility into attacks and traffic flow
• Scales to 100G capacity to counter large attacks
How It Works

1. Data Center Devices
   • Send sFlow samples to the collector

2. sFlow Collector
   • Collects and Analyzes volumetric flow sample data

3. SDN App with policy based UI and REST APIs
   • Provides Visibility and Mitigates volumetric flows

4. OpenDayLight Controller
   • Program OpenFlow 1.3 rules in MLX
Demo
Brocade Thought Leadership (1)

- “Behavioral Security Threat Detection Strategies for Data Center Switches and Routers,” IEEE International Workshop on Data Center Performance (DCPerf’14) – Published
  http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6888844

- Summary
  - Layer 2-4 DDoS SDN Application (discussed so far)
  - Embedded Layer 2-4 DDoS Mitigation (NFV complementing SDN)
  - Behavioral Security Threat Detection Assist
  - Layer 7 DDoS Assist

- Authors
  - Ram (Ramki) Krishnan (ramk@brocade.com); Dilip Krishnaswamy (dilikris@in.ibm.com); Dave Mcdysan (dave.mcdysan@verizon.com)
Brocade Thought Leadership (2)

• "Analysis of Data Center SDN Controller Architectures: Technology and Business Impacts," IEEE International Conference on Computing, Networking and Communications (ICNC) 2015 - Accepted

• Summary
  – Technology and Business Impacts of Loosely and Tightly coupled models between software overlay and hardware underlay in a Data Center
  – Fundamentally different ideas for maximizing the value of the underlay in a Commercial-off-the-shelf (COTS) ASICs environment

• Authors
  – Ram (Ramki) Krishnan (ramk@brocade.com); Norival Figueira (nfigureir@Brocade.com);
Brocade Thought Leadership (3)

• "SDN Multi-Domain Orchestration and Control: Challenges and Innovative Future Directions," IEEE International Conference on Computing, Networking and Communications (ICNC) 2015 Workshop – Accepted

• Summary
  – Proposes Hierarchical SDN Multi-Domain Orchestration and Control solution framework to address complex multi-tier governance domain deployments by Carriers, SP, CSPs, large Enterprises, NFVIaaS and NFVPaaS providers.
  – Proposed framework allows for simpler networking control and orchestration, more agile development processes, accelerated pace of innovation, and increased speed of deployment, while improving scalability and configuration automation as compared to existing frameworks.

• Authors
  – Norival Figueira (nfigureir@Brocade.com); Ram (Ramki) Krishnan (ramk@brocade.com);