Real-time SDN Analytics for DDoS mitigation

Ram (Ramki) Krishnan,
Muhammad Durrani
Brocade Communications

Joint work with

Peter Phaal
InMon Corporation
Brocade Strategic Partner

1 DDoS Mitigation Market Opportunity

DDoS Attack Megatrends [DDoS-TOP]

- High bandwidth, volumetric infrastructure layer (Layer 3 & 4) attacks increased approximately 30 percent
- DDoS attack volume also increased month-to-month in 2013, with 10 out of 12 months showing higher attack volume compared to 2012

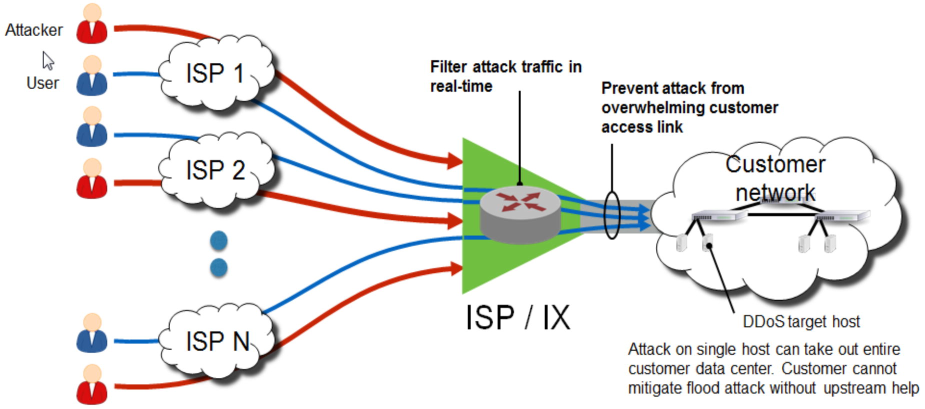
DDoS Mitigation Market Growth

- $870M market by 2017, 18.2% CAGR [DDoS-IDC]
- $1049M market by 2017, 25% CAGR [DDoS-Infonetics]

2 DDoS Mitigation Use Cases

2.1 ISP/IX Market Segment

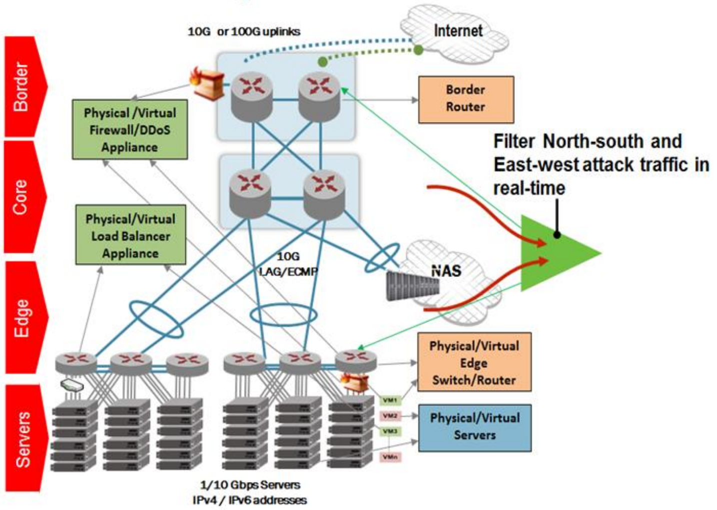
The ISP/IX use case is depicted in the figure below. The key elements of the value proposition are 1) ISP/IX is uniquely positioned to protect customers from DDoS flood attacks. 2) ISP/IX can offer a novel DDoS mitigation service to their customers; this enables a new source of revenue.


Attacker
User
ISP 1
ISP 2
ISP N
Filter attack traffic in real-time
Prevent attack from overwhelming customer access link
Customer network
ISP / IX
DDoS target host

Attack on single host can take out entire customer data center. Customer cannot mitigate flood attack without upstream help

2.2 Multitenant Cloud DC Market Segment

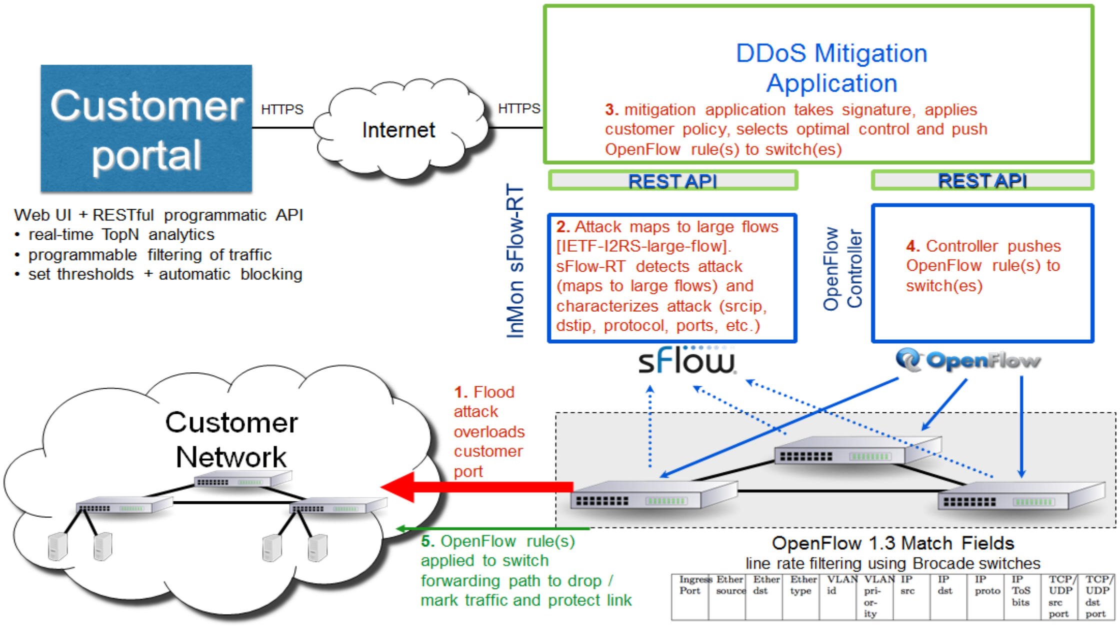
The Multitenant Cloud DC use case is depicted in the figure below. The key elements of the value proposition are 1) Cloud DCs are uniquely positioned to protect customers from DDoS flood attacks. 2) Cloud DCs can offer a novel DDoS mitigation service to their customers; this enables a new source of revenue.



Filter North-south and East-west attack traffic in real-time

3 Novel DDoS Mitigation solution using Real-time SDN Analytics

The novel solution involves real-time detection and mitigation of various Layer 2-4 DDoS Flood attacks. Layer 2-4 Flood attacks map to large flows in the network [IETF-I2RS-large-flow]. The key components of the solution involve 1) Brocade switches/routers with real-time sFlow visibility and Hybrid OpenFlow support 2) inMon sFlow-RT which performs real-time detection of large flows. This is described in detail in the figure below.


Customer portal
HTTPS
Internet
HTTPS
DDoS Mitigation Application
3. mitigation application takes signature, applies customer policy, selects optimal control and push OpenFlow rule(s) to switch(es)
REST API
REST API
Web UI + RESTful programmatic API
• real-time TopN analytics
• programmable filtering of traffic
• set thresholds + automatic blocking
InMon sFlow-RT
2. Attack maps to large flows [IETF-I2RS-large-flow]. sFlow-RT detects attack (maps to large flows) and characterizes attack (srcip, dstip, protocol, ports, etc.)
OpenFlow Controller
4. Controller pushes OpenFlow rule(s) to switch(es)
sFlow
OpenFlow
Customer Network
1. Flood attack overloads customer port
5. OpenFlow rule(s) applied to switch forwarding path to drop / mark traffic and protect link
OpenFlow 1.3 Match Fields
line rate filtering using Brocade switches

Ingress Port	Ether source	Ether dst	Ether type	VLAN id	VLAN pri-or-ity	IP src	IP dst	IP proto	IP ToS bits	TCP/ UDP src port	TCP/ UDP dst port

4 Competitive Differentiation

Deficiencies in the current solutions

- NetFlow exports flow data on end of flow, active-timeout or inactive-timeout; NetFlow learns all flows (long-lived/short-lived, large/small) – causes flow cache scalability and CPU utilization issues
- OpenFlow metering has similar architecture to NetFlow and similar limitations

Key advantages of sFlow

- Lightweight sampling technology; no performance overhead in switches/routers; supported in all Brocade Products

Key advantages of sFlow-RT

- Real-time detection of large flows; Approximate detection times – ~6s (10% link bandwidth), ~2s (20% link bandwidth) (Copyright © 2013 InMon Corp).

Key advantages of Brocade Hybrid OpenFlow

- OpenFlow and traditional packet forwarding enabled concurrently on same router ports
- No change to normal forwarding behavior; Use OpenFlow to selectively override forwarding of large /DDoS flows (block, mark, steer, rate-limit)
- Scalable, flows handled by existing control plane, only exceptions use OpenFlow; Robust, if controller fails, network keeps forwarding

5 References

[DDoS-TOP] http://www.itbriefcase.net/top-ddos-attack-trends-for-2013
[DDoS-IDC] IDC: Worldwide DDoS Prevention Products and Services 2013-2017 Forecast
[DDoS-Infonetics] Infonetics: Global DDoS Prevention Appliances 2012-2017 Forecast
[IETF-I2RS-large-flow] Krishnan, R. et al., “I2RS Large Flow Use Case,” April 2014.