Carrier/WAN SDN

Brocade Flow Optimizer
Making SDN Consumable
Carrier/WAN SDN

Business And IT Are Changing Like Never Before
Changes in Application Type, Delivery and Consumption

78% of IT Professionals claim the network is critical to delivering applications.
60% of IT Professionals cite network performance as key challenge for Cloud.
Today’s Network Challenges

- Do I have enough bandwidth/capacity in the network?
- Do I have any bad flows? Can I isolate/eliminate them?
- Can my network automatically re-route traffic around congestion points?
- Which applications are consuming the most bandwidth?

**Network Intelligence = Visibility + Control + Automation**
Brocade Flow Optimizer Application
What is the Brocade Flow Optimizer?

- An SDN policy-based application that works with an OpenDaylight compliant controller
  - Supports Open Networking
- Uses Policy to detect and manage large flows providing fine-grained control and automation for optimal flow management
- User friendly GUI provides interactive and real-time events logs and traffic statistics
Carrier/WAN SDN

How does it work?
Solution Components

1. Network Devices
Send sFlow samples

2. sFlow Collector(s)
Collect flow sample data

3. Brocade SDN Application
Policy-based UI and REST APIs
Analyzes and manages flows

4. SDN Controller
Programs OpenFlow 1.3 rules
OpenDaylight or Brocade SDN Controller
Carrier/WAN SDN

Brocade Flow Optimizer Dashboard

• Real Time Attacks Information Per Profile
• Real Time Monitoring of selected attacks
• Real Time Bandwidth/Application Control
• Real Time Events
• Overall Traffic Rate Report
# Carrier/WAN SDN

## Key Features and Benefits

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive Visibility</td>
<td>Proactive visibility and allows for early detection and avoids network issues prior to occurrence enabling better network resource and capacity planning</td>
</tr>
</tbody>
</table>
| Traffic Engineering                        | Proactively traffic engineer customer flows and eliminate network congestion to avoid service interruption/failure:  
  - Increase/Decrease priority  
  - Avoid latency  
  - Throttle bandwidth up or down |
| L2-L4 Denial of Service Attacks            | Manage customer flows based on set policies and identify malicious flows avoiding network flooding and/or shut down.                     |
| Real-time Events logging and traffic reporting | Provide real-time network information using web-based, user-friendly and interactive graphical user interface which easily integrates into 3rd party cloud orchestration systems |

**Network Intelligence = Visibility + Control + Automation**
<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Reflection Attack Group</th>
<th>Flood Attack Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Name</td>
<td>Reflection Attack Group</td>
<td>Flood Attack Group</td>
</tr>
<tr>
<td>NTP Reflection</td>
<td>IP Protocol: UDP</td>
<td>IP Protocol: UDP</td>
</tr>
<tr>
<td></td>
<td>UDP Src Port: 123</td>
<td>UDP Src Port: 53</td>
</tr>
<tr>
<td></td>
<td>(NTP)</td>
<td>(DNS)</td>
</tr>
<tr>
<td></td>
<td>Destination IP: Any</td>
<td>Destination IP: Any</td>
</tr>
<tr>
<td></td>
<td>UDP Dest Port: Any</td>
<td>UDP Dest port: Any</td>
</tr>
<tr>
<td>DNS Reflection</td>
<td>IP Protocol: UDP</td>
<td>IP Protocol: UDP</td>
</tr>
<tr>
<td></td>
<td>UDP Src Port: 53</td>
<td>UDP Src Port:</td>
</tr>
<tr>
<td></td>
<td>(DNS)</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Destination IP: Any</td>
<td>Destination IP: Any</td>
</tr>
<tr>
<td></td>
<td>UDP Dest Port: Any</td>
<td>UDP Dest port: Any</td>
</tr>
<tr>
<td>UDP Flood</td>
<td>IP Protocol: UDP</td>
<td>IP Protocol: UDP</td>
</tr>
<tr>
<td></td>
<td>Destination IP: Any</td>
<td>Destination IP: Any</td>
</tr>
<tr>
<td>ICMP Ping Flood</td>
<td>IP Protocol: UDP</td>
<td>ICMP Protocol Ping</td>
</tr>
<tr>
<td></td>
<td>Destination IP: Any</td>
<td>Destination IP: Any</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Headers Used for Detection</th>
<th>Bandwidth Threshold: MBps / GBps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Observation Period: Sec / Min</td>
</tr>
</tbody>
</table>

**Thresholds**
# Brocade Flow Optimizer

## Attack Detection Custom Profile

### Custom Profile

<table>
<thead>
<tr>
<th>Layer</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| **L2** | Source Mac – Name / IP Address / Any  
\ Destination MAC – Name / Address / Any  
\ VLAN – Name / ID / Any  
\ 801.1p – Name / Value / Any |
| **L3** | Source IP (host or network) – Name / IP Address / Any  
\ Destination IP (host or network) – Name / IP Address / Any  
\ IP Protocol – TCP/UDP/ICMP/Number/Any  
\ DSCP or TOS/Precedence – Name / Value / Any  
\ IP Fragment – Yes / No  
\ TTL – Value / Any  
\ IP Option – Yes / No |
| **L4** | TCP/UDP Source port – Name / Number / Any  
\ TCP/UDP Destination port – Name/ Number/ Any  
\ TCP Flags – SYN/ FIN/ ACK/ RST/ URG/ PSH/ Any |
Use Cases
Carrier/WAN SDN

Network Attack Mitigation
Carrier/WAN SDN

Application Traffic Control

Limit traffic from:
Netflix, YouTube, iTunes

Policy-based Application Traffic Control (such as rate limit, drop, and QoS re-mark)

Brocade SDN Controller
Open Daylight

OpenFlow

sFlow

Brocade Flow Optimizer

WAN/Internet

A
B
C

Limit Drop Re-mark

Brocade MLXe Router

Campus Network

Brocade ICX
Carrier/WAN SDN

Flow-Based Traffic Mirroring

Full 12-tuple OpenFlow matching supported
Carrier/WAN SDN

1. Incoming flow from upstream network
2. Sent to Firewall for processing
3. Brocade MLXe sends sFlow samples to Brocade Flow Optimizer
4. Brocade Flow Optimizer recognizes this as a trusted flow and programs Brocade MLXe using the controller to bypass the firewall for this flow
5. Flow now bypasses Firewall and data transfer is faster and more efficient

HPC: High Performance Computing
DTN: Data Transfer Nodes

Brocade SDN Controller
Brocade Flow Optimizer
WAN/Internet

Brocade MLXe Router

HPC/DTN Network
Thank You