Managing SDN Using DPI

Steven O. Noble
Sideband Networks, Inc

Introduction. Deep Packet Inspection (DPI), the act of inspecting the data inside of a computer network packet is looked at to extract data that is then used to manage SDN including the creation and teardown. The data provided by DPI such as application data, routing updates, flow control packets, is processed by the SDN controller for use. When compared to extracting data from NetFlow, sFlow and SNMP; DPI provides real-time, high-value data.

Objective.

Utilize DPI as a data source to manage SDN solutions, providing real-time information that can be used to make decisions about deployment and configuration of software defined network devices and virtualized network functions (VNF).

Comparisons.

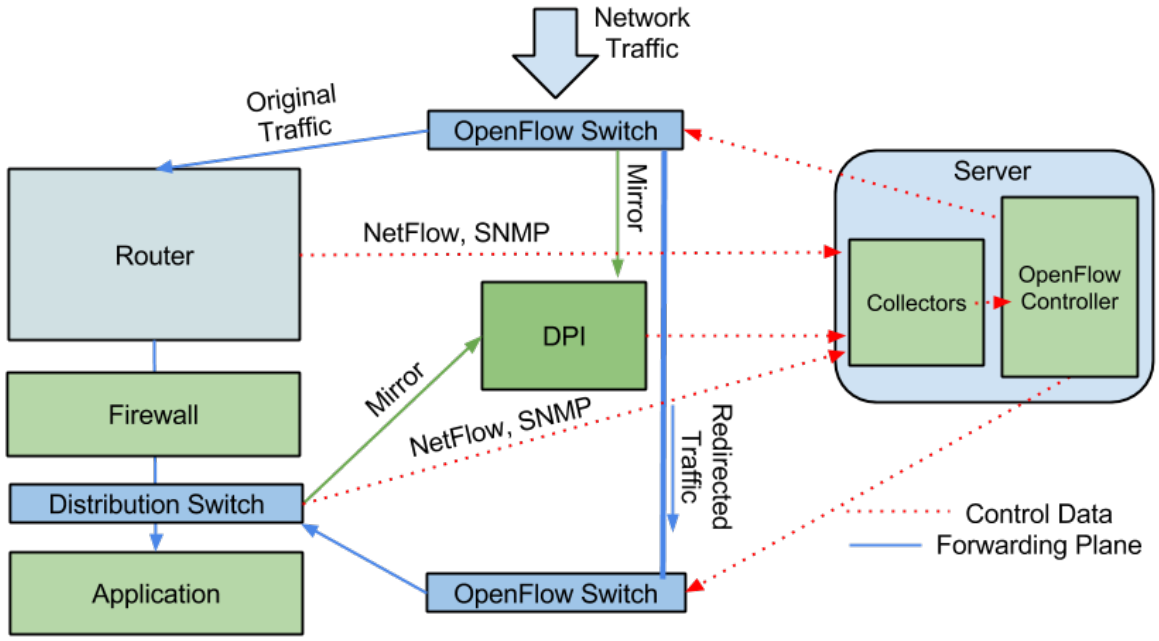
- SNMP – Immediate Value Low, Historical Value Medium
  - Traps come after-the-fact, when the link or device is already impacted
  - Must be polled to get data, excessive polling will impact network device performance
  - Useful for modeling traffic and looking at historical statistics
- NetFlow – Immediate Value Low, Historical Value High
  - Along with sFlow is available on most mid-high range networking devices
  - Provides historical data that can be used for network modeling
  - Generally provides data after the traffic flow has stopped
  - Can impact performance of networking devices
- DPI – Immediate Value High, Historical Value High
  - Provides a high level of traffic detail
  - Can be used in real-time to distribute software defined network devices
  - Can detect and provide value metrics to data traffic
  - Expensive with regard to CPU and Memory usage

How we tested.

Tests were done using purpose built NetFlow and SNMP collectors along with Sideband Networks' DPI code and generic network hardware to translate received data into usable information sent to Floodlight.

In each case, network traffic was sent into a Pica8 switch then to a Cisco router and mirrored to the DPI engine. The Cisco router sent both NetFlow and SNMP data to a server running our code and Floodlight.

The traffic was then fowarded through the Cisco router to a Sonicwall Firewall and then to a Dell switch doing ToR distribution. The Dell switch sent sFlow/SNMP data to the collection server and mirrored the post processed traffic flow back to the DPI engine. The DPI engine combined the traffic data with the original, unmodified traffic flow and a mimicing, transformative flow rule was created.



Information Gathered.

Utilizing NetFlow, we were able to see traffic from bigger flows moved over to the fast path between the two OpenFlow switches. For malicious traffic, null flows were added, but due to limitations in NetFlow's ability to break up long lived flows, the data is not very useful.

SNMP work has been limited to looking at interface traffic and routes.

DPI provided real-time data on traffic flows and applications. Using DPI we were able to compare pre and post forwarded traffic to determine flow rules that would create the same outcome.

Future Work.

Focus on balancing cost, benefit and performance. ….