Event-Driven SDN

Steven Carter

Solutions Architect, Cisco Systems

Jason King

Solutions Architect, Cisco Systems

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Referenced customers for ITSI product participated in a limited release software program that included items at no charge.

About Me

- Steven Carter, Solutions Architect, Cisco Systems
  - 15 years of experience in the enterprise and public sector space
  - Specializes in Cloud, SDN, and DevOps Solutions for Public Sector Customers
  - Part of a team that built the World's first SDN network and the World's largest supercomputer, and took Linus Torvalds out for a burger… at Hooters
- Jason King, Solutions Architect, Cisco Systems
  - 15 years of experience in the enterprise and public sector space
  - Designed and operated large scale campus LANs and HPC networks
  - Specializes in solutions for the unique requirements of the scientific community
  - Extensive background in enterprise Systems, Storage, and Virtualization

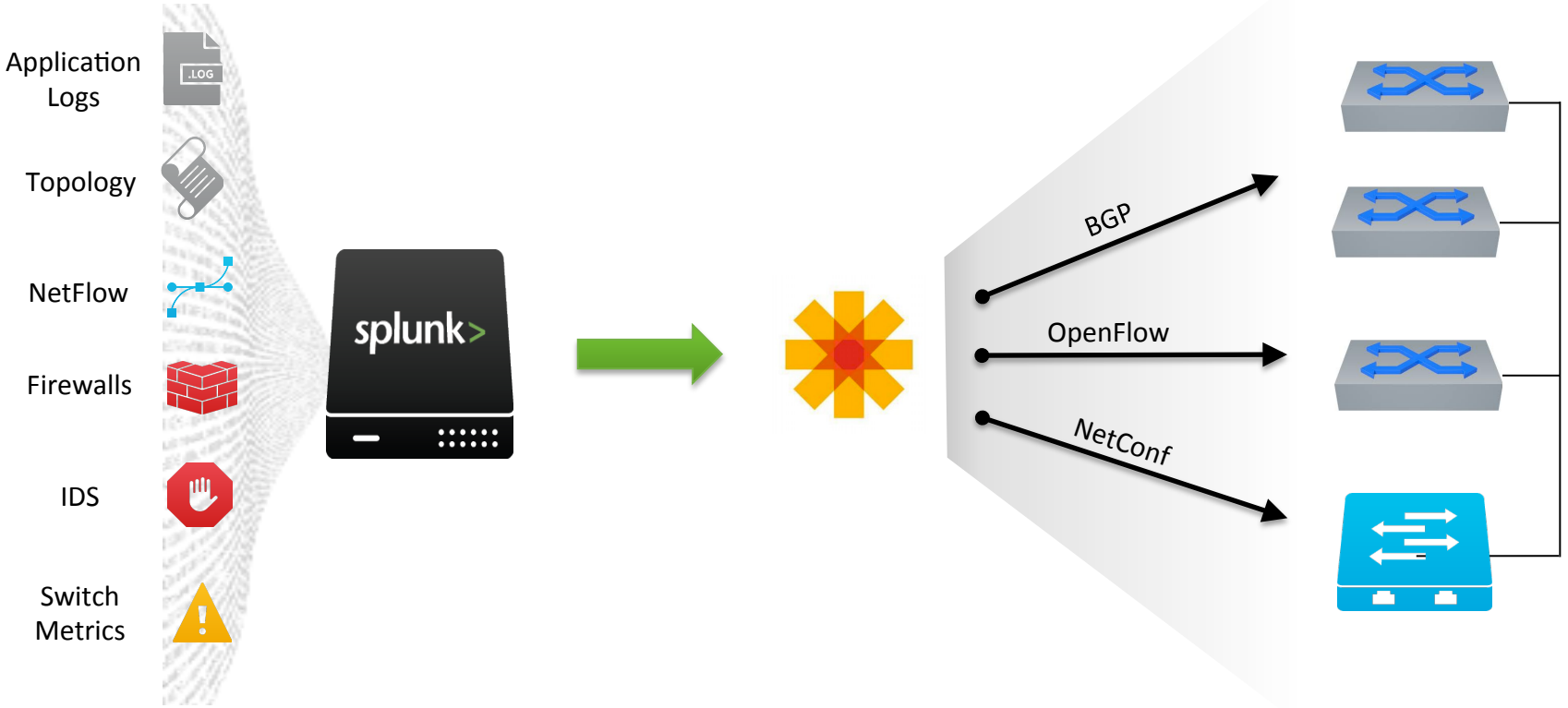
Agenda

- Background
- Solution Detail
- Demonstration
- Summary

Background

splunk>

What is Event-Driven SDN?



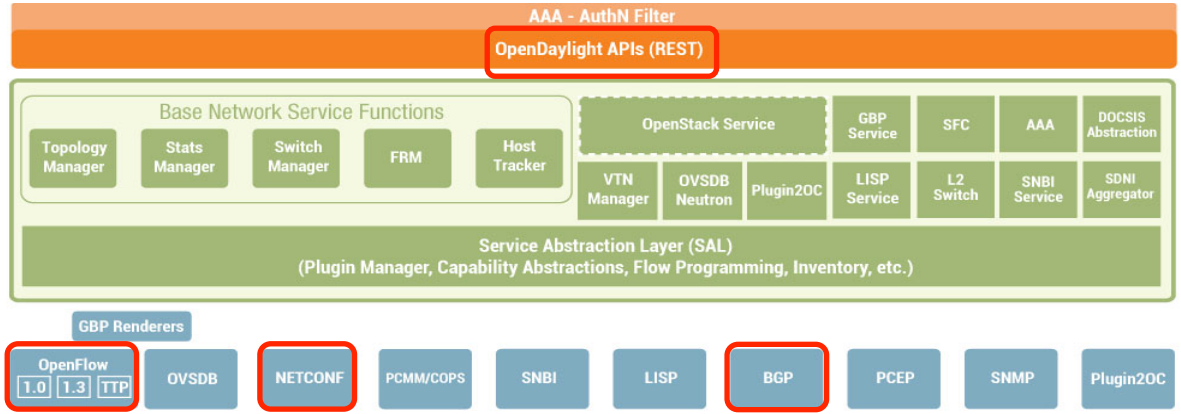
Why Event-Driven SDN?

- Probably already sending events to central logging
- Has the most informed view of the status of the network, servers, and apps
- Provides event correlation
  - Consolidates the number of devices sending REST commands
  - Correlates by severity, rate, and between events
- Provides for auditing and reporting capabilities
- Leverage existing skills by writing logic in Splunk Search Processing Language

Cisco Open SDN Controller

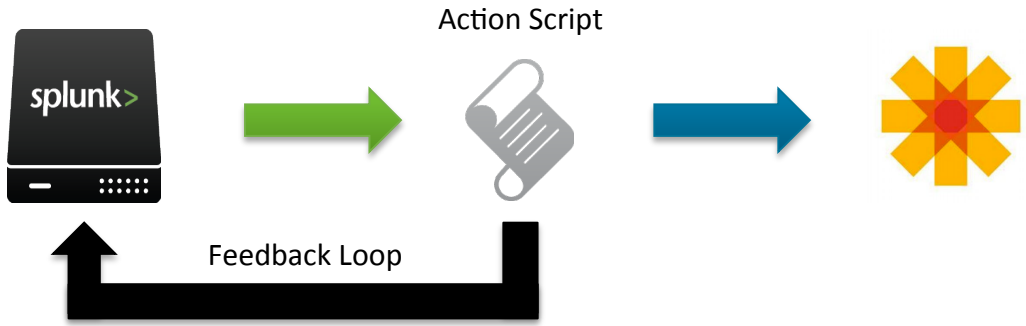
Open platform for SDN app development

Single Northbound REST Interface



Multiple Southbound Interfaces

Event Feedback Loop

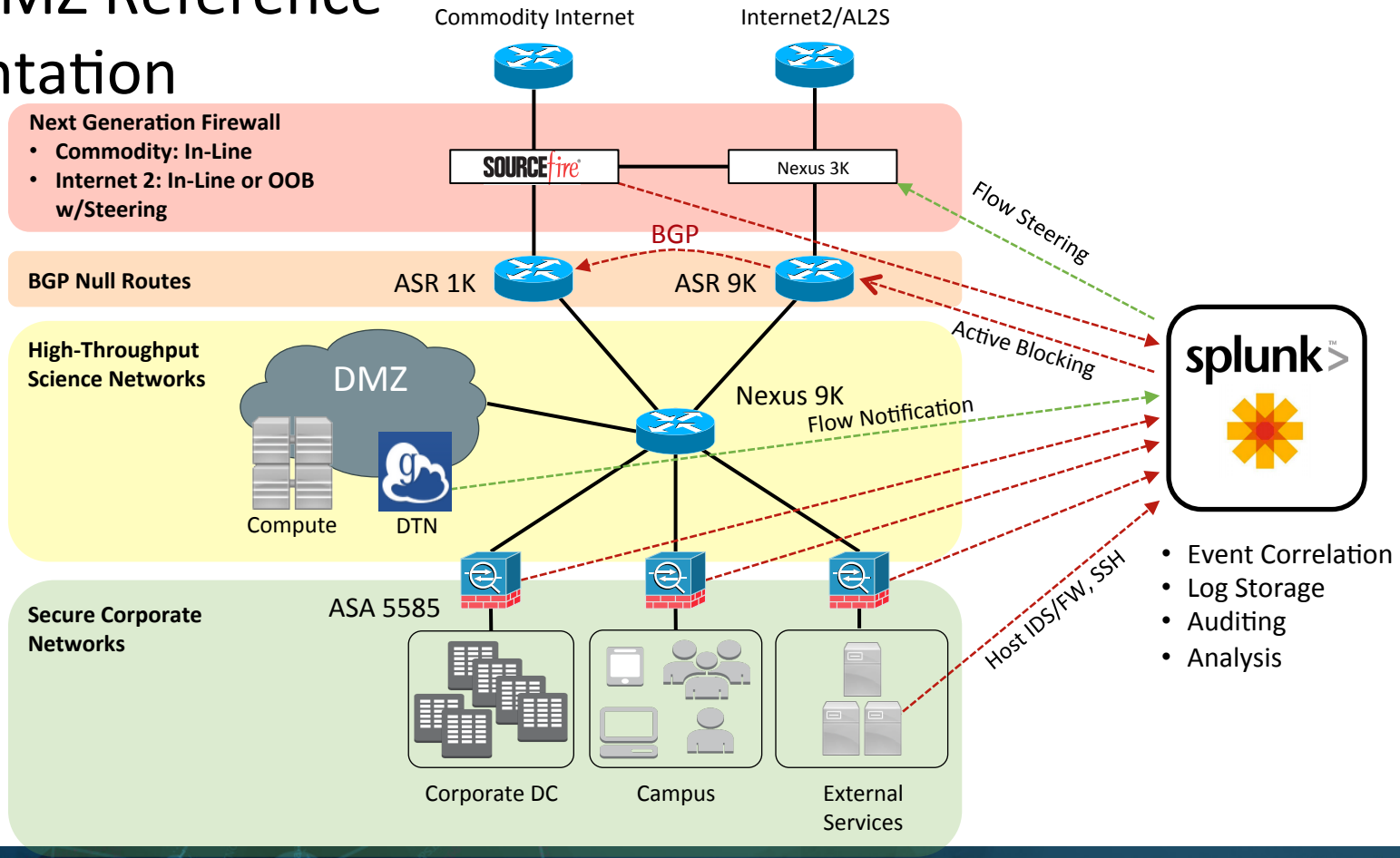


- Used to store state in Splunk software to avoid complexity
- State can be used to “remember” to unblock a host
- State can be used to elevate the threat level of an attacker

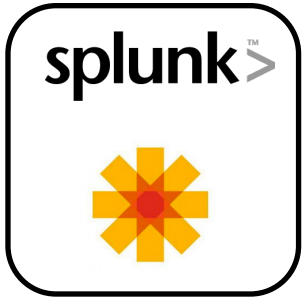
Science DMZ Solution Detail

splunk>

Science DMZ Reference Implementation



Example Event Actions



Real-Time, Immediate Action:

e.g. High Priority IDS Event: Block Host Immediately

```
index=estreamer sourcetype=estreamer (rec_type_simple=EVENT OR rec_type_simple="IPS EVENT") priority=high | eval params="action=block,event=ids-high"
```

Real Time With Sliding Window and Threshold:

e.g. SYN Attacks: Block host after 100 improper SYNs in 60 seconds

```
eventtype=cisco-security-events threat_reason="protocol abuse" | stats count by src_ip | search count > 100 | eval params="action=block,event=asa-protocol-abuse"
```

Scheduled with Fixed Window:

e.g. Block Timeout: Unblock host if it has not been seen in last 24 hours

```
sourcetype=splunk_odl_action action=block earliest=-48h | stats count by src_ip | table src_ip | search NOT [ search sourcetype=splunk_odl_action action=block earliest=-24h | stats count by src_ip | table src_ip ] | eval params="action=unblock,event=block_timeout"
```

Globus for Data Transfer

- A key service in the research networking ecosystem with more than 10,000 active endpoints
- Software-as-a-Service (SaaS) solution to manage transfers where users can direct requests to transfer or synchronize files and directories between two locations
- Uses GridFTP to provide secure, reliable, and efficient transfer of data across wide-area distributed networks
- GridFTP extensions provides parallelism (i.e., the use of multiple socket connections between pairs of data movers), restart markers, and data channel security.
- GridFTP control plane provides the source and destination information for the flows it sets up
- Effectively authenticates flows before they bypass security

OpenFlow Data Flow Steering

Base setup depending on mode:

Out-Of-Band IDS:

<priority>100</priority>

<in-port>54</in-port>

<output-node-connector>52</output-node-connector>

<output-node-connector>25</output-node-connector>

In-Band Firewall/IPS:

<priority>100</priority>

<in-port>54</in-port>

<output-node-connector>25</output-node-connector>

<in-port>25</in-port>

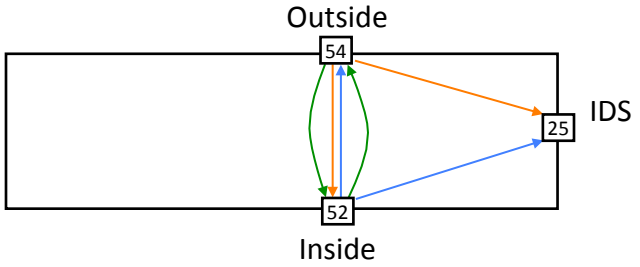
<output-node-connector>52</output-node-connector>

Bypass operation the same for both modes

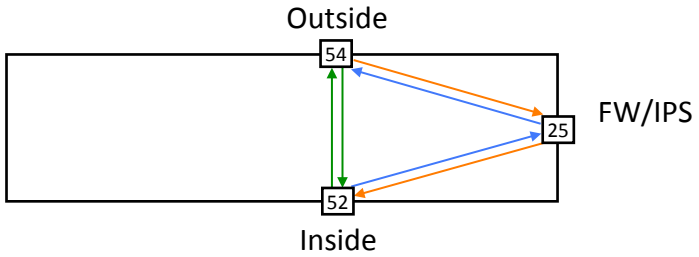
<priority>200</priority>

<in-port>54</in-port>

<output-node-connector>52</output-node-connector>



Out-Of-Band IDS



In-Band FW/IPS

Bypass Flows in “Tap” Switch

Flow start notification:

```
Jun 10 10:53:43 localhost splunk_odl_action: log_level=INFO, action=start, flow=199.66.189.10:50368-128.55.29.41:42600, status_code=200
```

Flows added to Nexus 3000:

```
Flow: 4
  Match:            tcp,in_port=54,nw_src=199.66.189.10,nw_dst=128.55.29.41,tp_src=50368,tp_dst=42600
  Actions:          output:52
  Priority:         200

Flow: 5
  Match:            tcp,in_port=52,nw_src=128.55.29.41,nw_dst=199.66.189.10,tp_src=42600,tp_dst=50368
  Actions:          output:54
  Priority:         200
```

Flow stop notification:

```
Jun 10 10:54:51 localhost splunk_odl_action: log_level=INFO, action=stop, flow=199.66.189.10:50368-128.55.29.41:42600, status_code=200
```

Remotely Triggered Black Hole Routing

Static routes added by COSC through Netconf on ASR 9000:

```
router static
 address-family ipv4 unicast
  1.0.184.115/32 Null0 tag 666
  1.161.169.139/32 Null0 tag 666
  2.25.74.127/32 Null0 tag 666
  2.50.153.67/32 Null0 tag 666
  12.197.32.116/32 Null0 tag 666
```

Export the Null routes setting next-hop to black hole IP:

```
route-policy as-11017-out
  if tag is 666 then
    set next-hop 192.0.2.1
    set community (no-export) additive
    pass
  else
    pass
 endif
end-policy
```

Enable uRPF on WAN interface on ASR 9000:

```
ipv4 verify unicast source reachable-via any allow-default
```

Route Black Hole IP to NULL 0 on other border routers:

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Enable uRPF on WAN interface on ASR 1000:

```
ip verify unicast source reachable-via any
```

Demo

splunk>

Summary

- The Splunk platform can be used as an SDN engine
- Leverage existing skillset in Spunk Search Processing Language
- You are already collecting the information that you need
- Increase your security posture by including ALL intelligence

THANK YOU

splunk>