.conf2015

Stream Deployments in the Real World: Enhance Operational Intelligence Across Application Delivery, IT Ops, Security, and More

Stela Udovicic
Sr. Product Marketing Manager

Clayton Ching
Sr. Product Manager

Mike Dickey
Sr. Engineering Director

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.

Personal Introduction

- Stela Udovicic, Sr. Product Marketing Manager
  - Responsible for IT Operations/Applications Delivery, Stream, Strategic Partners
  - Over 15 years of experience with variety of data, networking and storage technologies
- Clayton Ching, Sr. Product Manager
  - Responsible for Splunk App for Stream strategic direction and roadmap
  - 20 years in enterprise software management
- Mike Dickey, Sr. Engineering Director
  - Responsible for Apps Architecture and Performance
  - Founder of Cloudmeter, the startup company where Stream originated from

Agenda

- Introduction: Market Challenges and Splunk Solution
- Customer Success
- Real-World Deployment and Architecture
- How to Manage Splunk App for Stream in Your Environment
- Performance Metrics
- Summary

Introduction: Market Challenges and Splunk Solution

splunk>

Market Challenges

Lack of Application Visibility Impacts Customer Experience

Limited Cloud Insights

Long MTTR Hurts the Business

Splunk App for Stream:
Real-time Applications Intelligence

Real-time Insights into Application Performance and Customer Experience

Visibility into Cloud Services

Quickly Deploys and Filters Streaming Network Data to Maximize Business Impact

Customer Success

splunk>

Cross-Tier Visibility Helps Break the Silos

"Stream and Splunk help us understand issues at the high level and if exec team wants to see the details we can drill down easily."

Kris Laxdal,
IT Manager & Security Analyst

Key Customer Benefits

IT Operations/Applications Delivery

- High executive level view with contextual drill-down ability
- Easy access and visibility into production MySQL environment helps app developers troubleshoot issues and roll out releases quicker
- Improved collaboration between teams: IT operations, QA (pre-production testing),security and development
- Improved customer response times due to real-time visibility into app issues

Security

- Correlation against indicators of compromise helps investigate and mitigate APTs, potential data exfiltration & other risks

Applications Visibility for Better Customer Experience

"The Splunk App for Stream helps us get real-time insight into the operational performance of applications, as well as the health of our claim-processing workflows."

IT Platforms Operations Manager
Medical Claims Processing Company

Key Customer Benefits

- Visibility into web applications for interactions across frontend, middle-tier and database servers help resolve issues quicker
- Business process insight to help understand customer experience and claims volume
  - Match applications and infrastructure to business demands
- Improved applications performance better customer experience

Applications Visibility Drives Better Digital Asset Management

"With Splunk and Stream, **we have this rich data platform** that is bridging all the different data silos. Our MTTR went from days to minutes while the granularity and insight improved. We went from having very little visibility into operational and security issues to full insight."

Systems Engineer, Major Media Company

Key Customer Benefits

- **IT Operations**: improved operational insight into digital asset management and streamlined lengthy processes
- **Application Delivery (DevOps)**: faster app releases due to visibility into app performance
  - Real-time insight into database queries and latencies
  - Cross-correlation with system-level performance and user access
- **Security**: Visibility into user behavior throughout entire asset management system helps protect digital assets

Real-World Deployment and Architecture

splunk>

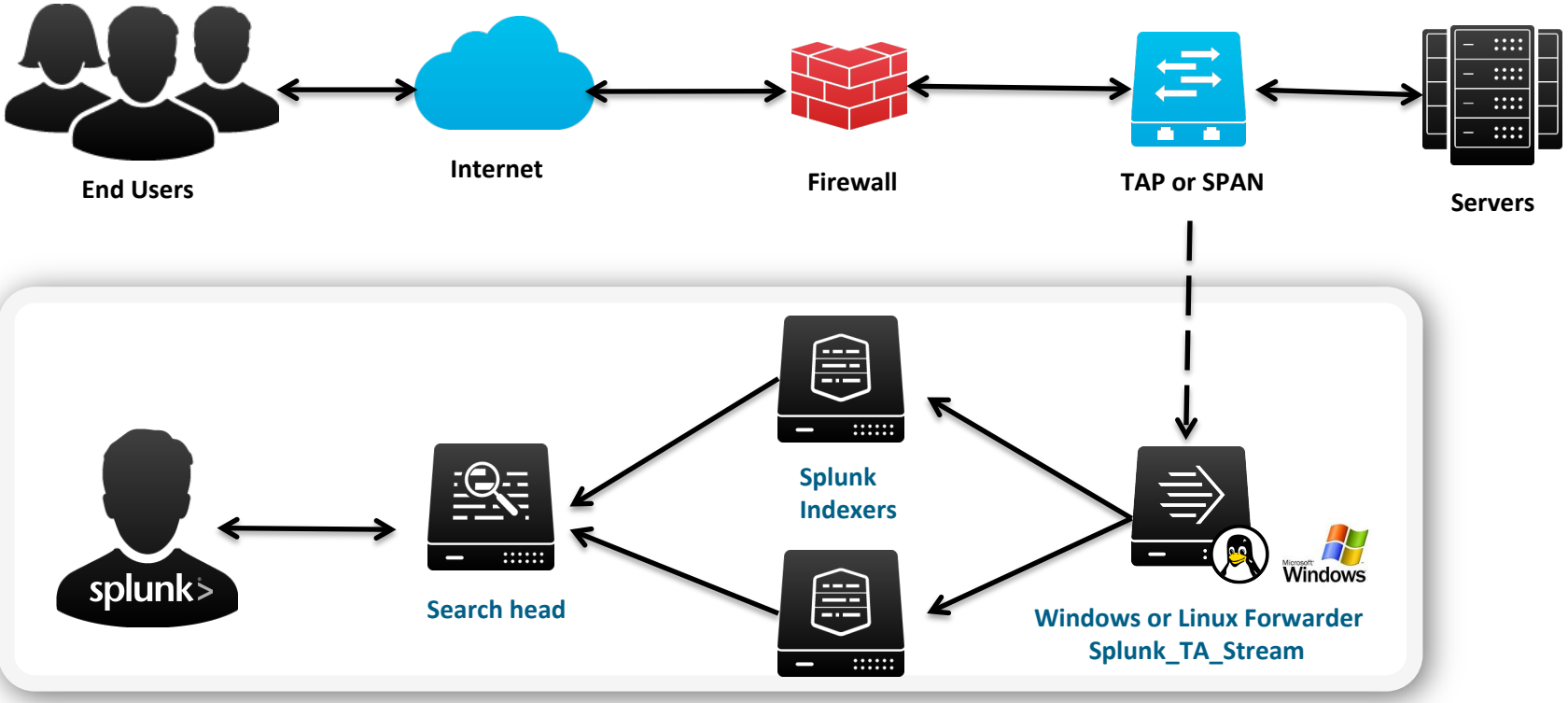
Quick Time to Value

Easy-to-Deploy Software Solution
Runs on any commodity hardware

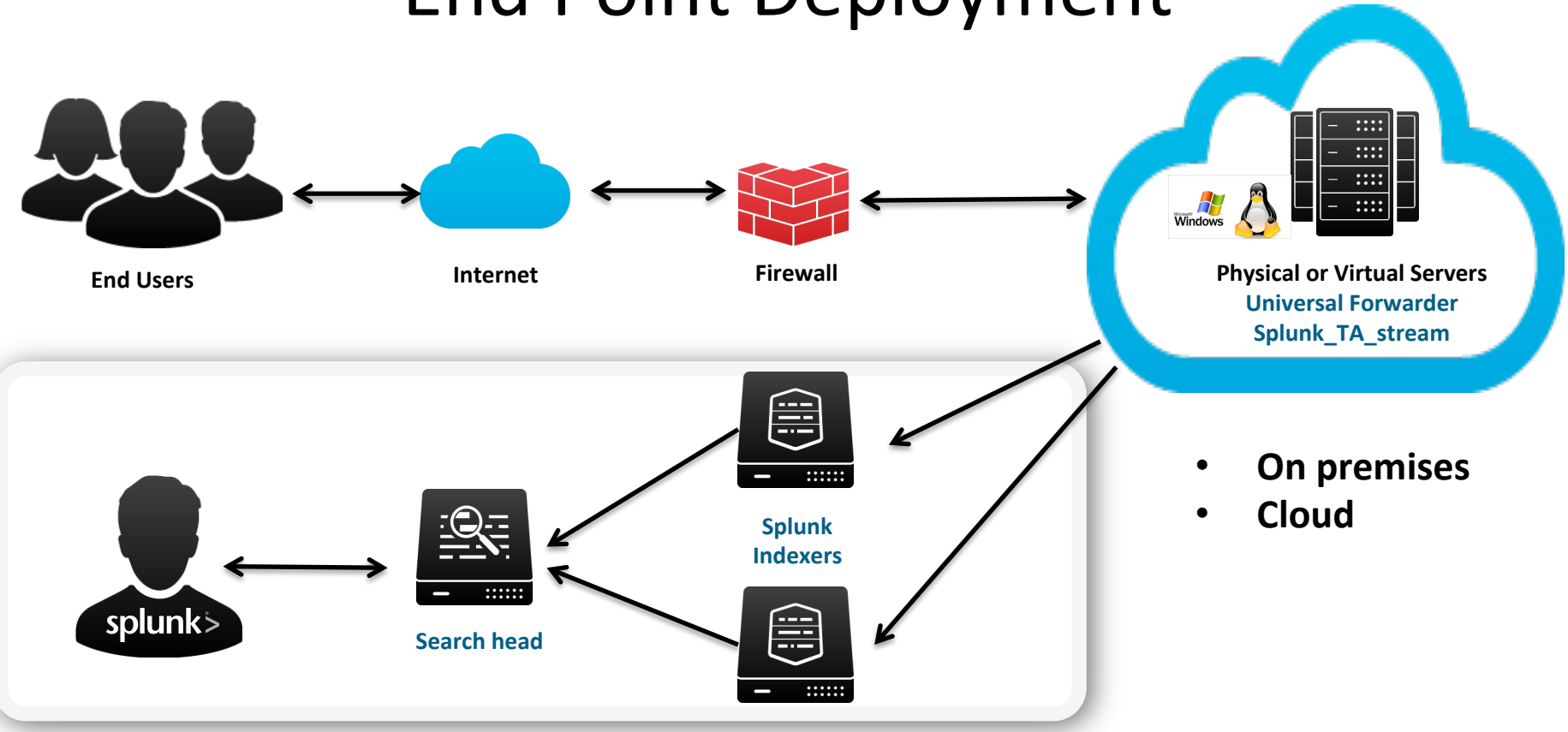
Passive Data Collection
Without application overhead

Low-cost Deployment
With flexible resource utilization

Dedicated Server Deployment

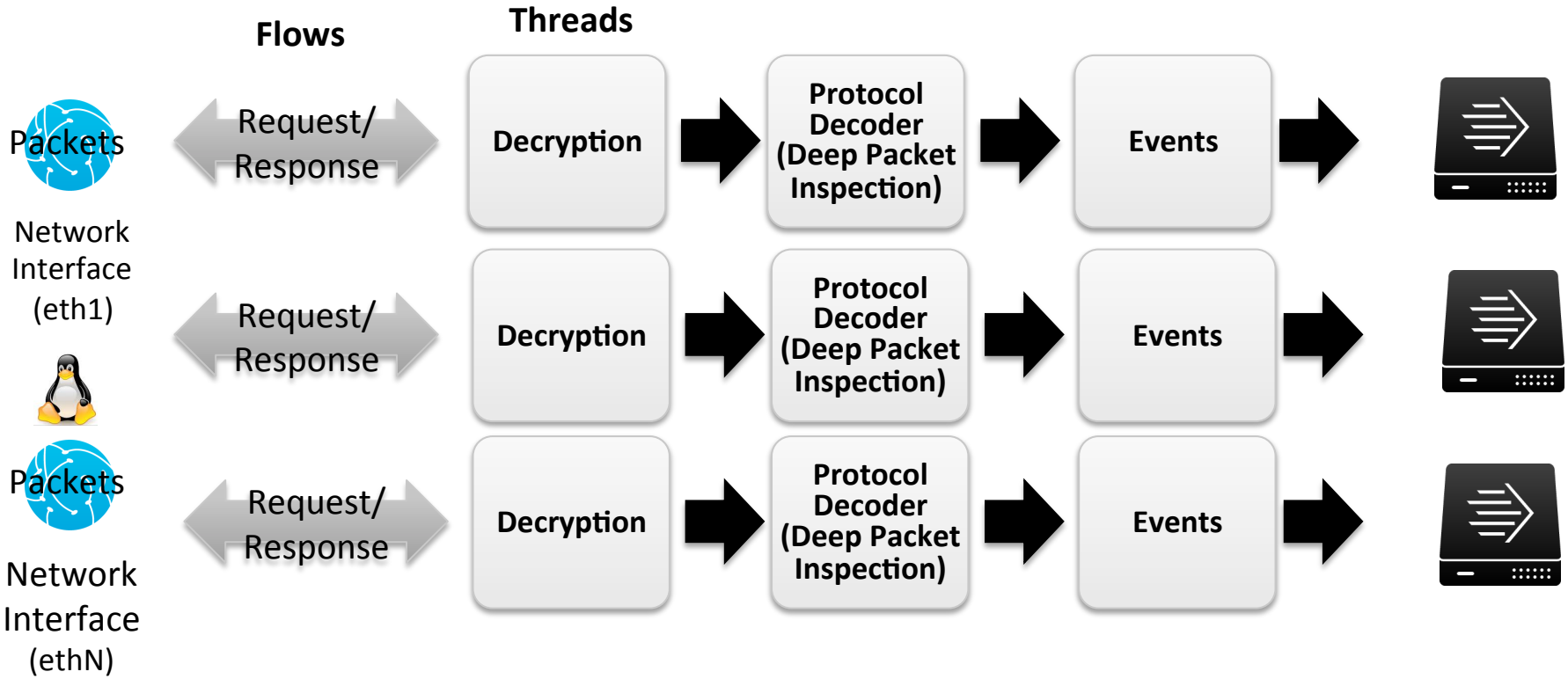


End Point Deployment



- On premises
- Cloud

Stream Forwarder Architecture



How to Manage Splunk App for Stream In Your Environment?

splunk>

Managing Your Streams

1. Manage your data collection
2. Analyze the volumes
3. Control the data volume
4. What if?

Distributed Forwarder Management

Maximize Control
Dynamic Data Collection
Adapt to Your Business Needs

Logical Group(s)

-http
-Diameter
-sip
-udp
-tcp
-dns
-pop3
-smtp
-Oracle
-MySql

-http
-udp
-tcp
-dns

-http
-tcp
-pop3
-smtp

-http
-udp
-tcp
-Oracle
-MySql

...

-http
-udp
-tcp

-http
-udp
-tcp

Security

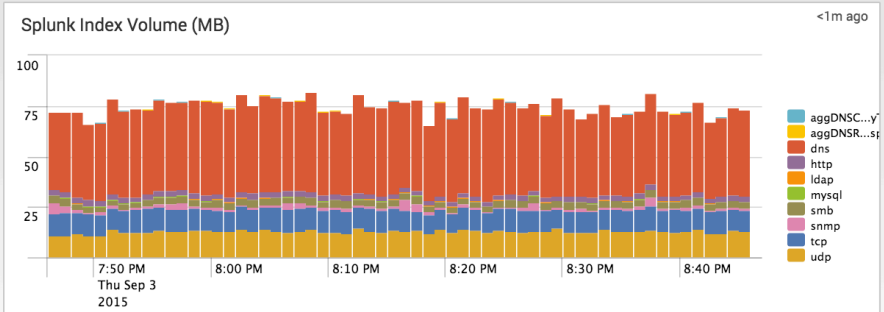
Email

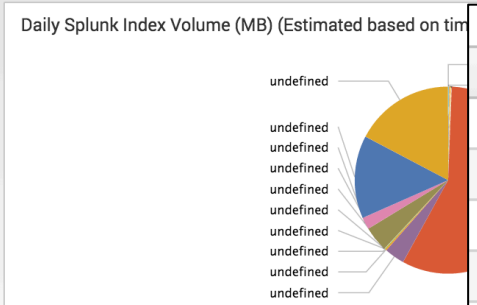
Database

eCommerce

STM = Splunk App for Stream

How Much Data?





Stream Stats

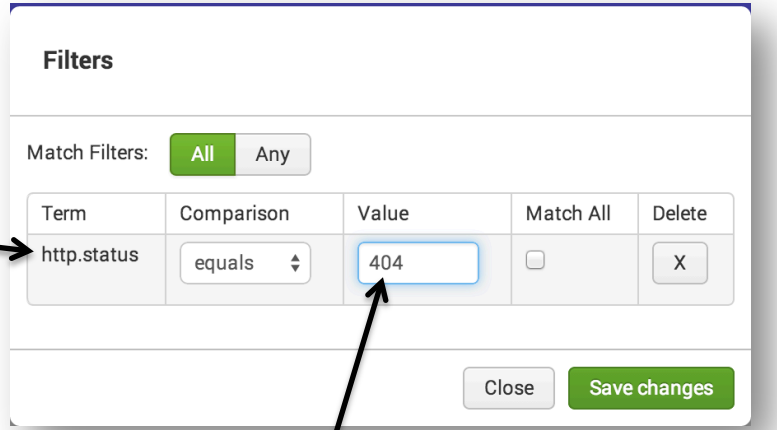
Stream Id	Total Events	Total Incoming Traffic (MB)	Total Outgoing Traffic (MB)	Total T	Splunk Index Volume (MB)
dns	2639899	180.15	14.65		2587.86
udp	1189837	331.65	45.48		779.37
tcp	540714	5411.08	11126.76		645.56
smb	261935	48.83	45.93		196.70
http	137157	2044.26	876.04		157.37
snmp	43962	9.31	6.26		93.49
ldap	6861	0.42	0.81		8.64
mysql	11509	0.60	0.60		7.80
aggDNSRequestResponse	0	0.00	0.00		5.89
aggDNSClientQueryTypes	0	0.00	0.00		5.34
aggHTTPURI	0	0.00	0.00		4.20
aggDNSIntegrity	0	0.00	0.00		3.82
dhcp	3379	0.56	0.00		3.05
nfs	3105	0.00	0.00	0.13	2.34

Control Data Collection

Select Fields

☑	src_mac	Client packets MAC address in hexadecimal format
☑	src_port	Client port number
☑	ssl_version	SSL protocol version used for encryption, or undefined if not encrypted
☑	status	The HTTP status code returned to the client
☑	time_taken	Number of microseconds that it took to complete a flow event, from the er
☑	title	Page title, extracted from HTML content
☑	transport	Transport layer protocol (udp or tcp)
☑	uri	The requested resource (including query)
☑	uri_parm	The parameters portion of the requested resource
☑	uri_path	The requested resource (excluding query)
☑	uri_query	The query portion of the requested resource

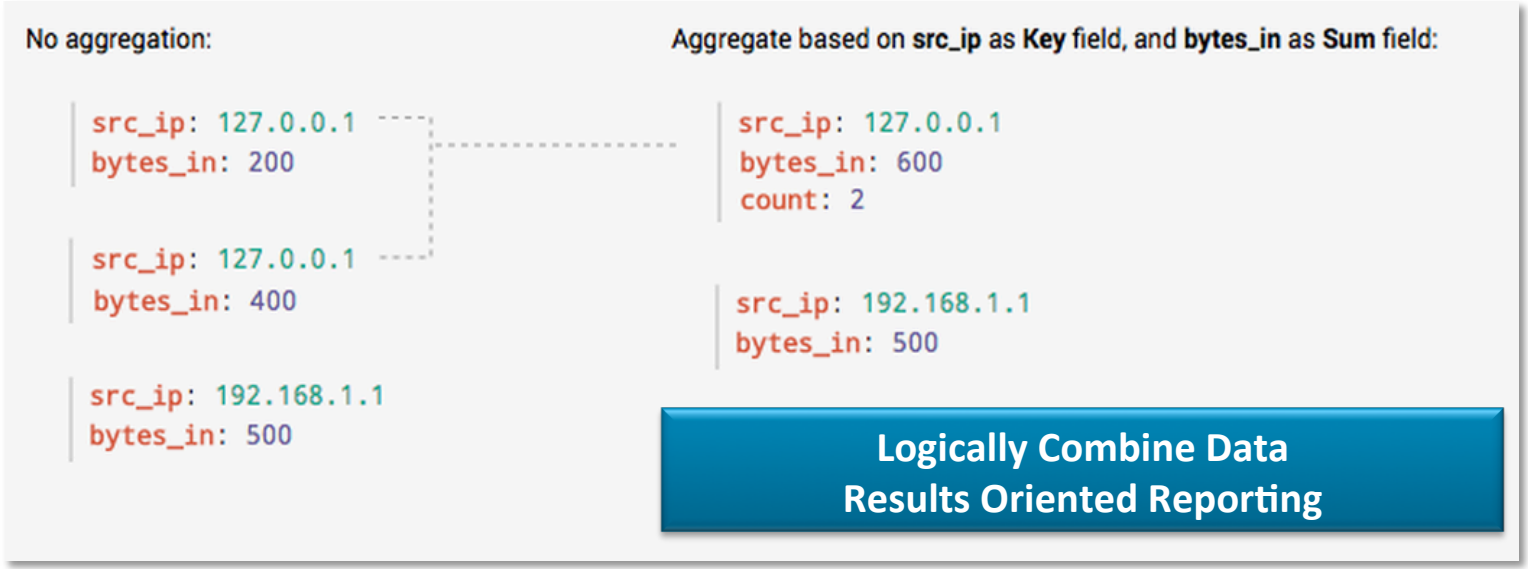
Specify Filtering



I only want to collect certain Application Errors HTTP with status=404 (File Not Found)

Control Data with Aggregates

Summarize Many Events to One



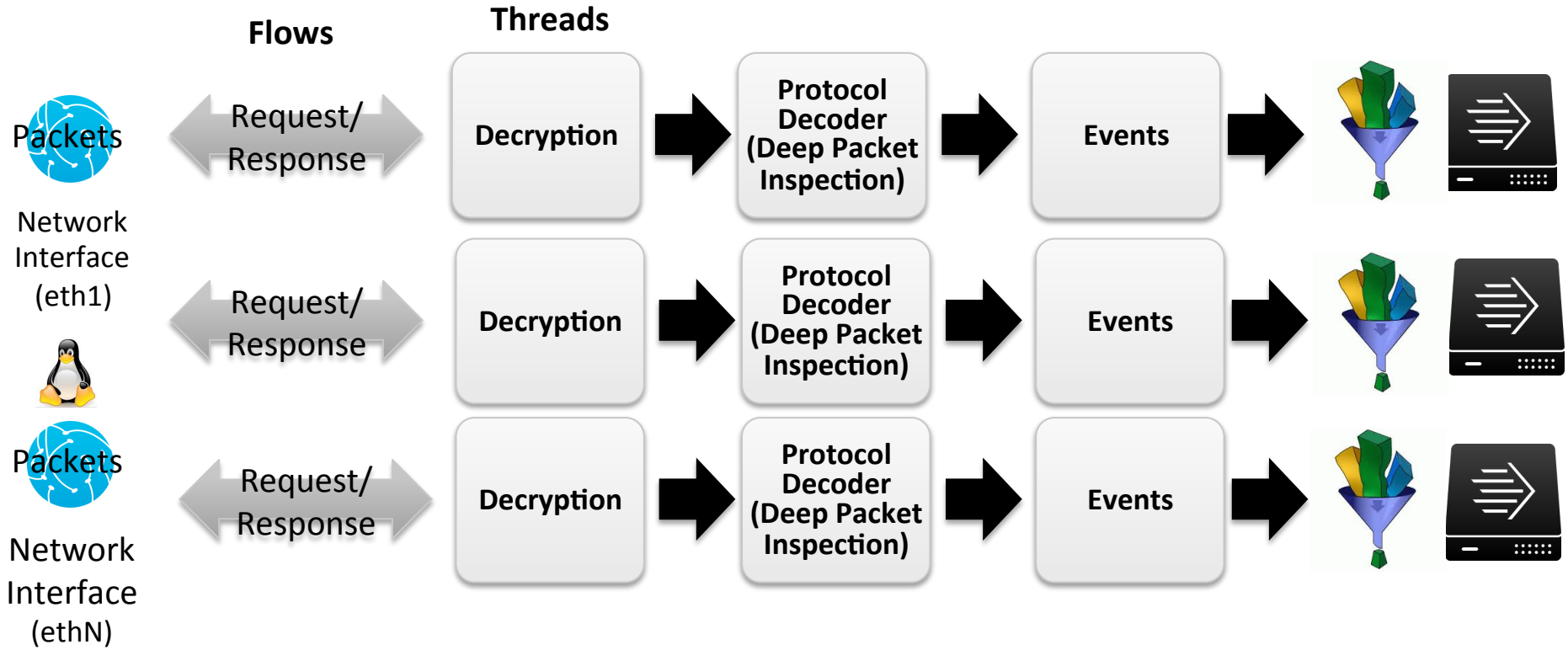
Applications Insights with Aggregation Dashboard

- Results Oriented Dashboards
- Better Insights
- Effective Data Management

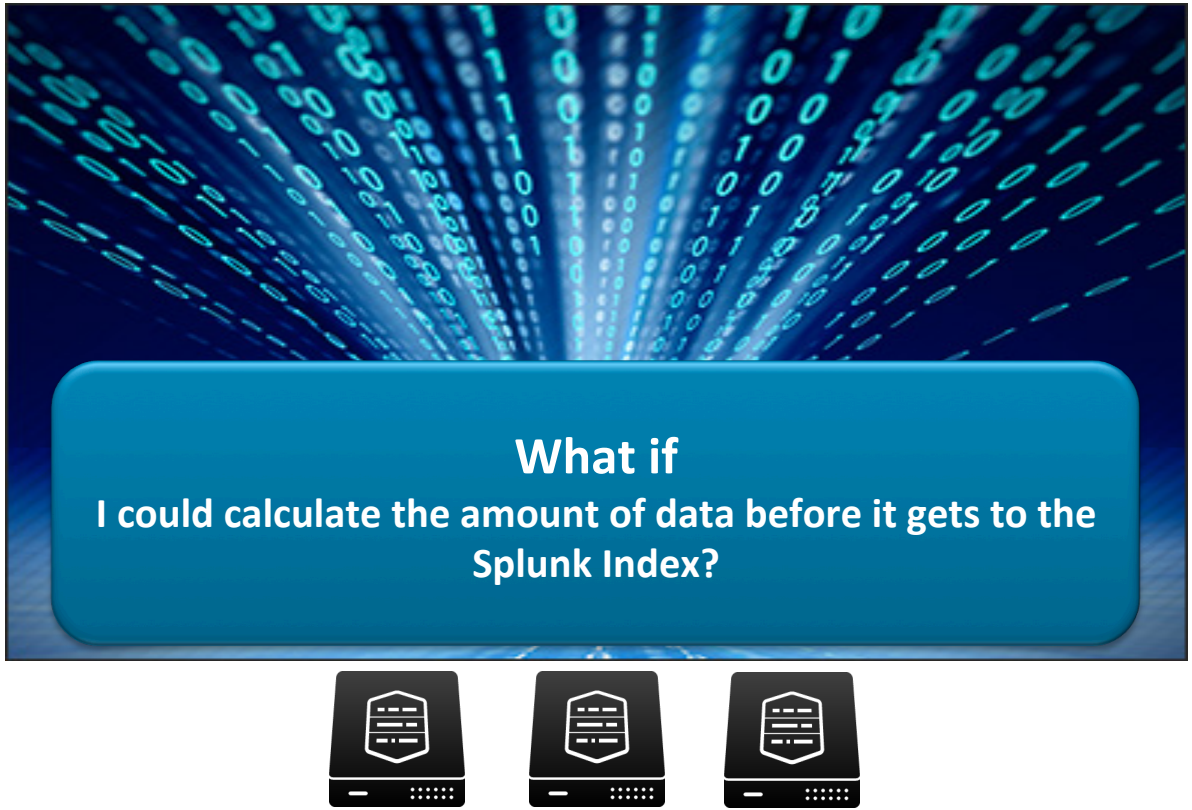
EndPoints (Clients) <1m ago

Client	Requests	Bytes In	Bytes Out	Response Time
10.14.6.25	10914	20218452	177649086	3.667237
10.14.6.58	5743	16370186	77400639	2.280381
10.14.6.103	4964	1714888	4055038	0.209458
10.14.6.86	4956	1716732	4126800	0.206394
10.14.6.74	4918	1703342	4061104	0.219022
10.141.50.23	4259	1422889	147968810	0.212421
10.14.6.49	3101	3009392	133237517	1.410947
10.14.6.99	2644	4129124	40591032	3.165039
10.14.6.94	2460	850172	2014330	0.215270
10.14.6.77	2448	847300	2039108	0.222155

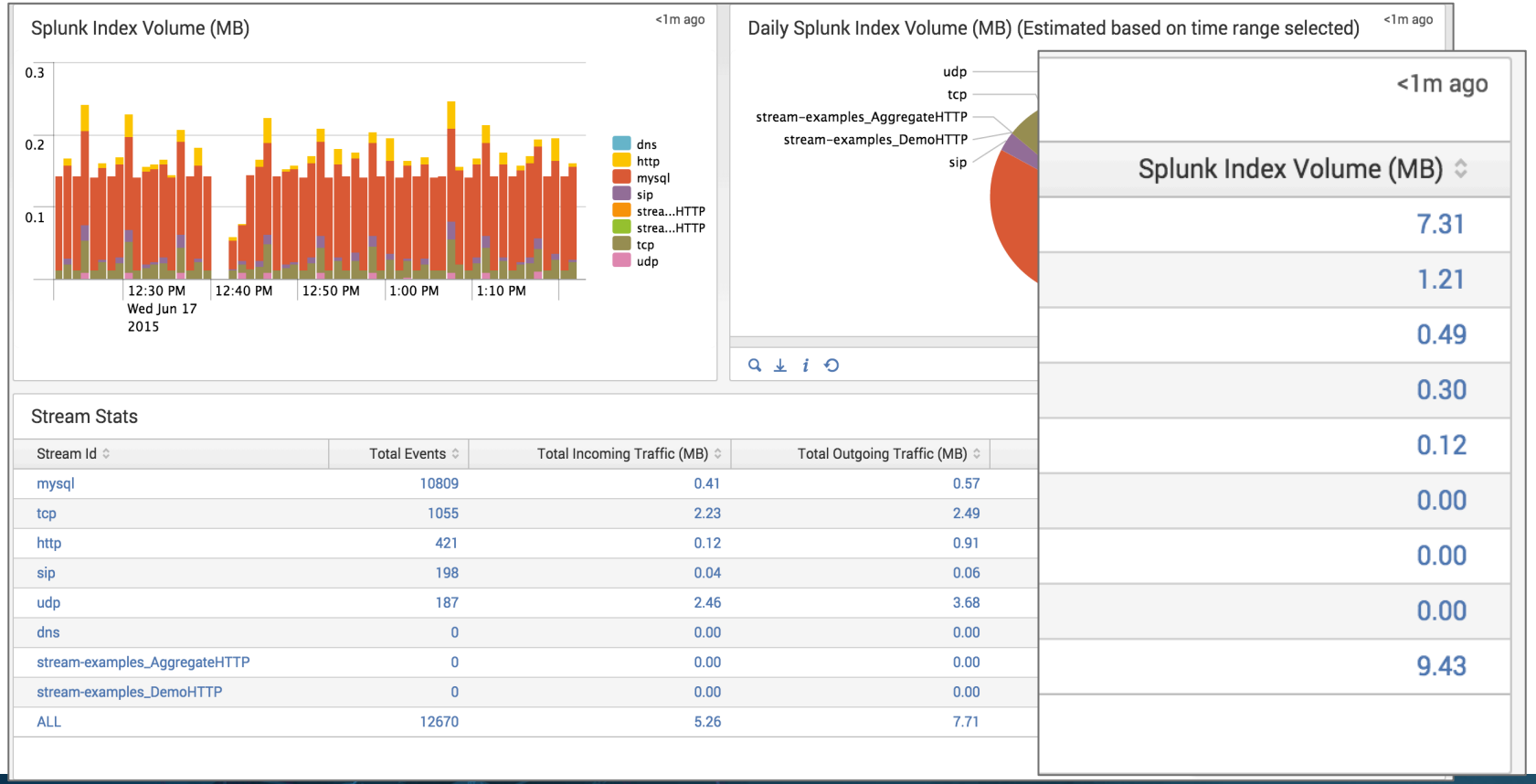
Stream Forwarder Architecture



Tailor Data Collection to Your Monitoring Needs



What If



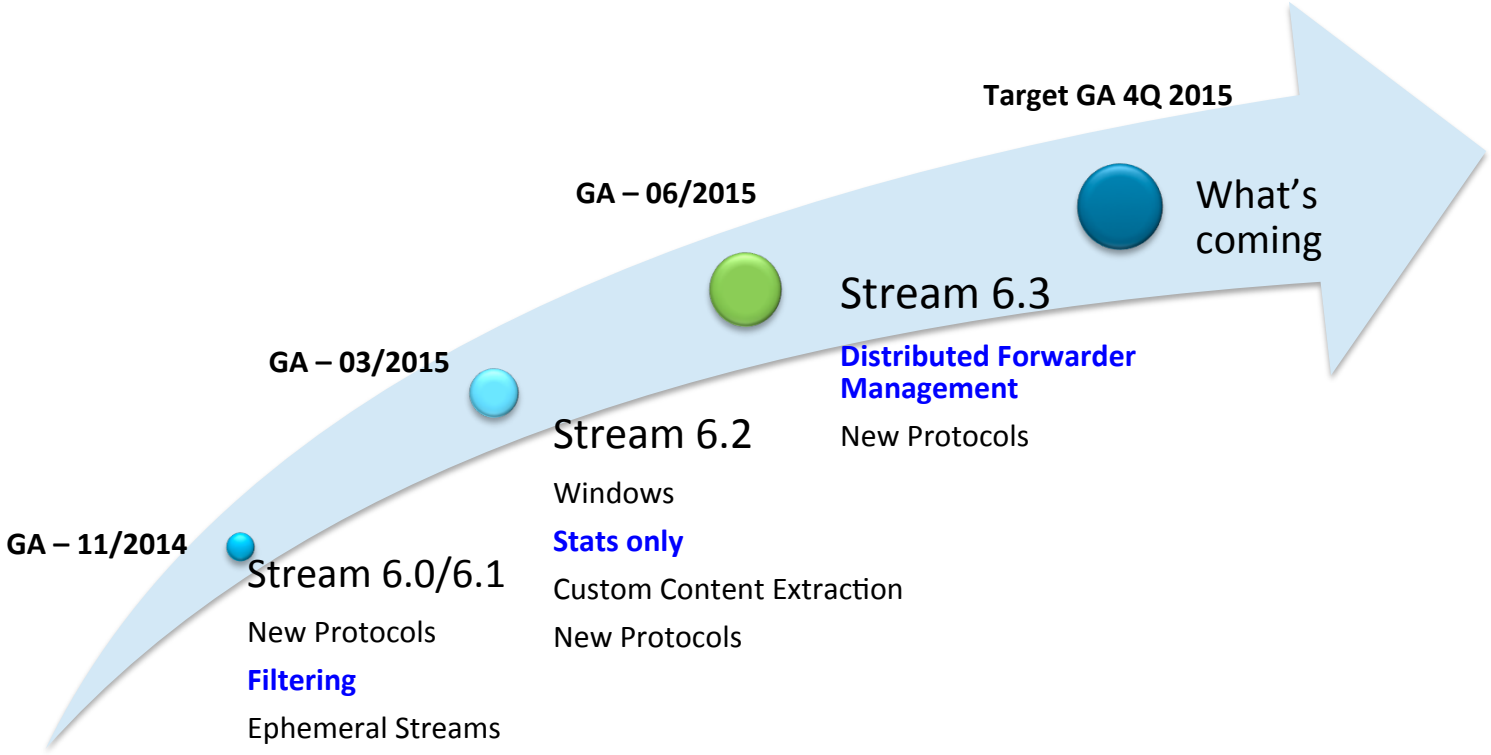
Stream Stats

Stream Id	Total Events	Total Incoming Traffic (MB)	Total Outgoing Traffic (MB)
mysql	10809	0.41	0.57
tcp	1055	2.23	2.49
http	421	0.12	0.91
sip	198	0.04	0.06
udp	187	2.46	3.68
dns	0	0.00	0.00
stream-examples_AggregateHTTP	0	0.00	0.00
stream-examples_DemoHTTP	0	0.00	0.00
ALL	12670	5.26	7.71

Demo
Splunk App for Stream

splunk>

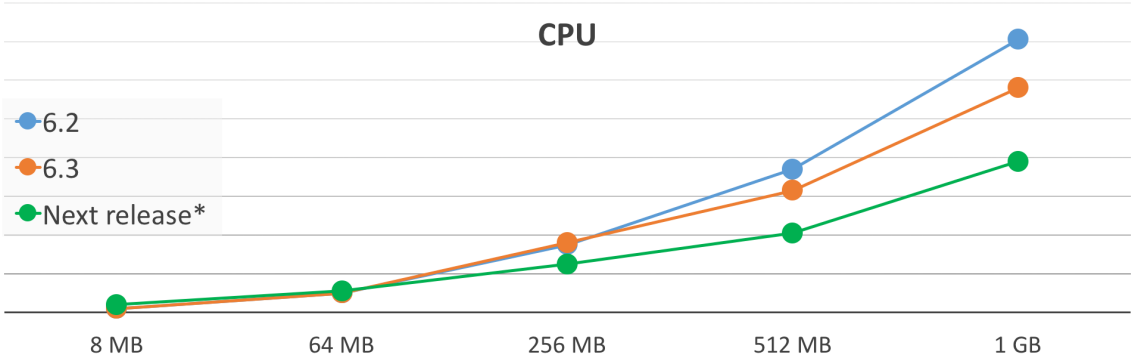
What's Up with Splunk App for Stream?



Performance Metrics

splunk>

Incremental Improvements



40% LESS CPU

70% LESS MEM

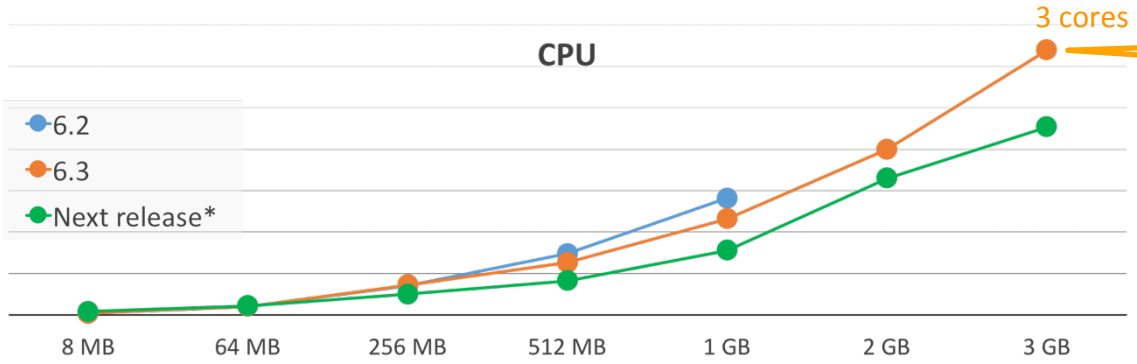
VS 6.2

Test Assumptions

- HTTP traffic (100K response size) was used to generate the graphs.
- Every request has its own TCP connection

***Note:** Data in this presentation recorded on September 3, 2015. Please refer to docs for up to date performance results.*

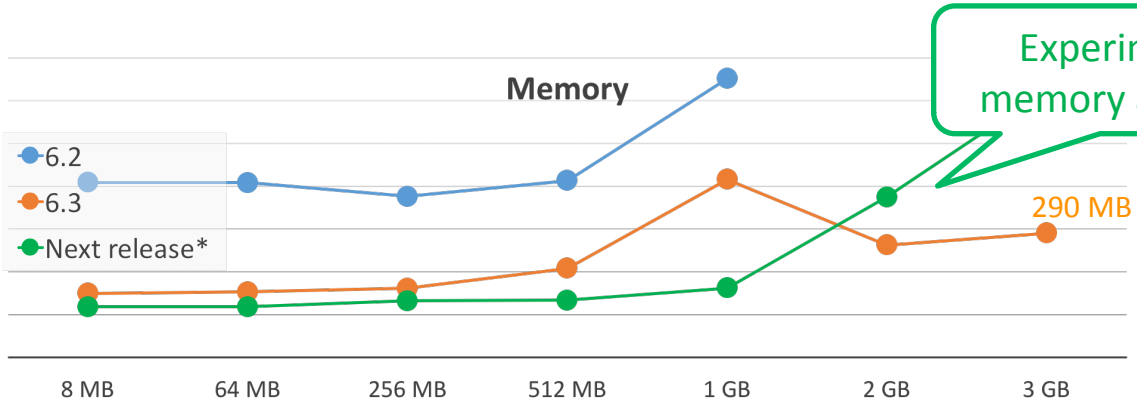
Scaling Beyond 1 Gbps



3-4 Gbps limit for current 6.3 release

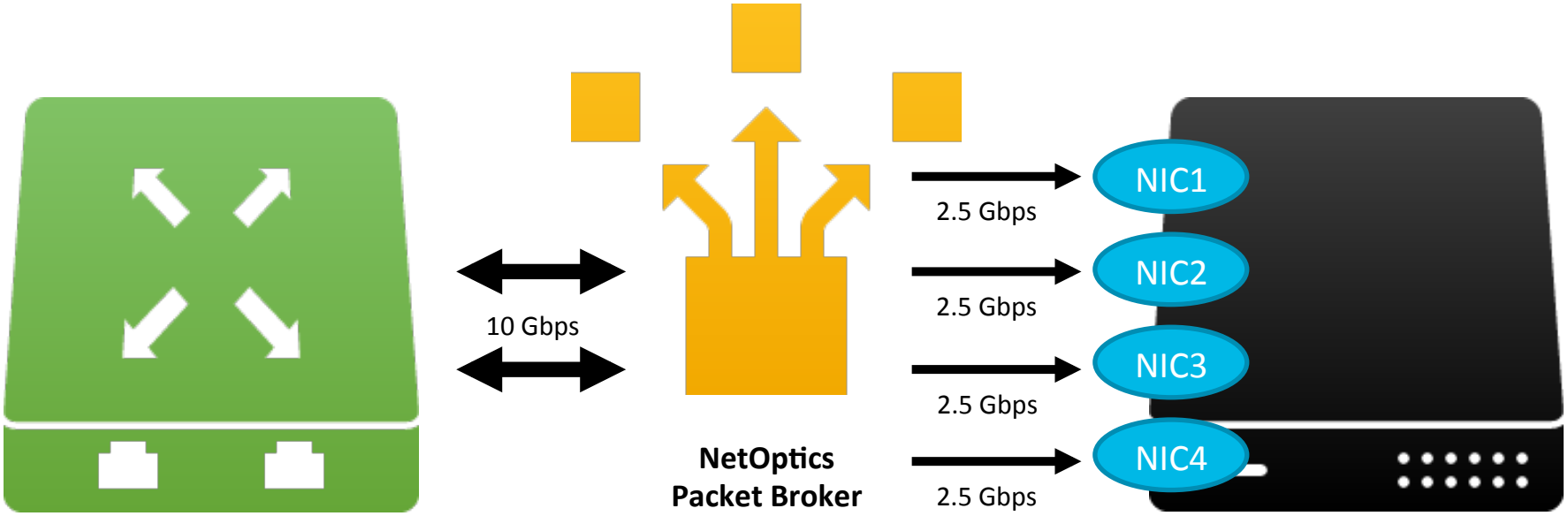
Test Assumptions

- HTTP traffic (100K response size) was used to generate the graphs.
- Every request has its own TCP connection



***Note:** Data in this presentation recorded on September 3, 2015. Please refer to docs for up to date performance results.*

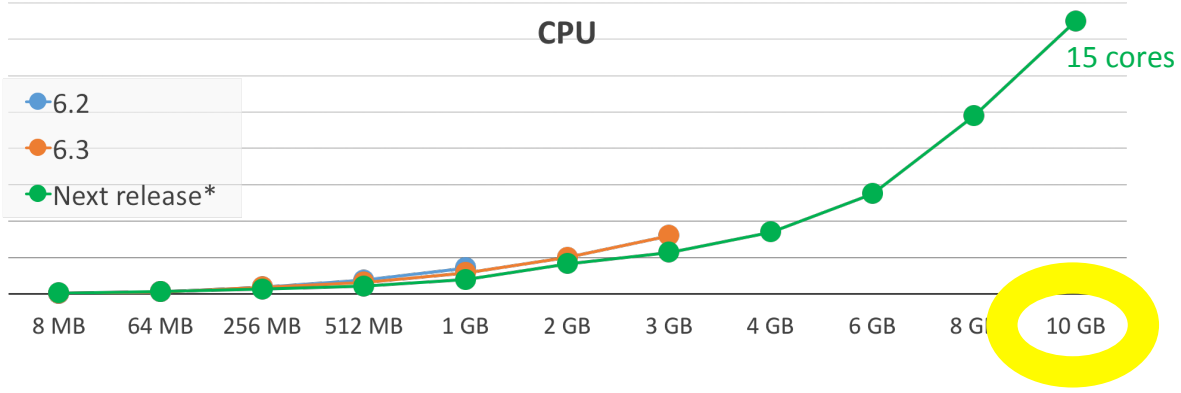
Performance Test Environment

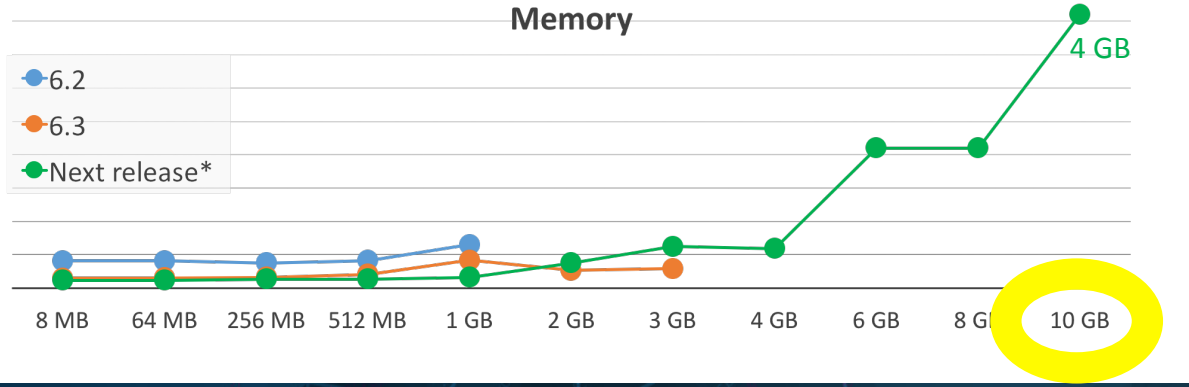


Ixia PS-100 w/ BreakingPoint

Streamfwd (16 cores)

10 Gbps Performance Results





16 cores, 4 GB mem, four 10 GB NICs < $5k

Test Assumptions

- HTTP traffic (100K response size) was used to generate the graphs.
- Every request has its own TCP connection
- Packet broker used to LB traffic across NICs

***Note:** Data in this presentation recorded on September 3, 2015. Please refer to docs for up to date performance results.*

Performance Summary

- Splunk App for Stream uses libpcap, which tops out at about 3-4 Gbps per NIC
- Packet broker spreads 10 Gbps traffic across four NICs
- Handle more traffic using multiple servers
  - 2 For 20 Gbps, 4 for 40 Gbps, and 10 for 100 Gbps
  - Use a packet broker to load balance the traffic across your servers
- Future Work
  - Removing libpcap limitations
  - Additional reductions in CPU & memory
  - Testing Splunk App for Stream with more traffic patterns

Summary

splunk>

Stream: See Everything. Now!

Get Real-time Applications Intelligence

Gain Visibility into Cloud Services

Reduce MTTR to Maximize Business Impact

Next Steps

Download and try Splunk App for Stream for free!

- Attend **Sierra-Cedar** session
  - Thursday, September 24, 2015 | Breakout 18
- Attend **Royal Caribbean Cruise Line** session
  - Wednesday, September 23, 2015 | Breakout 12
- Check out **CanDeal case-study**: Streamlining IT and Security
  - http://www.splunk.com/content/dam/splunk2/pdfs/customer-success-stories/splunk-at-candeal.pdf
- Chat with Stream experts in our IT operations booth

Questions?

THANK YOU

splunk>