SciPass
Secur*ish* OpenFlow Based Science DMZ

Edward Balas
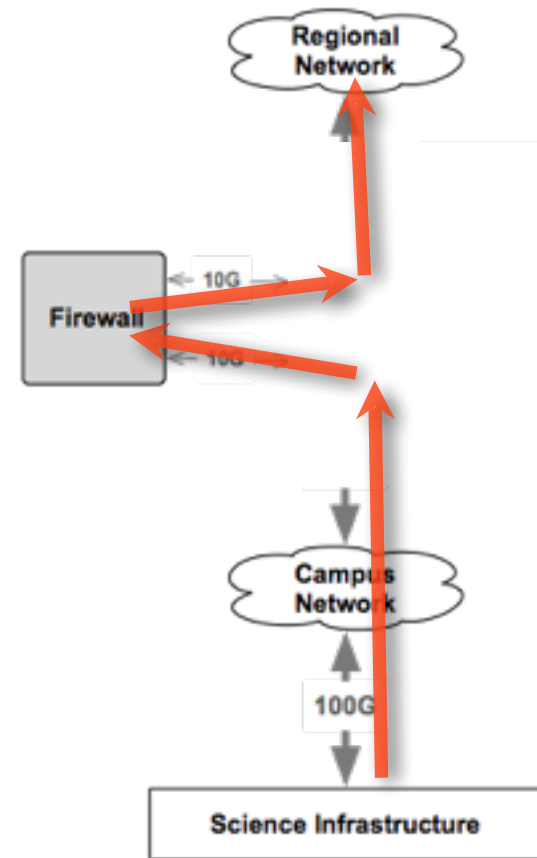
GlobalNOC

Indiana University

June 15, 2015

GlobalNOC

1

Problem

- Campus Networks are enterprise infrastructure
  - large number of small flows
  - security is a required capability
- not elephant flow friendly
- could just bypass but that doesn't provide required security
- what about performance assurance?

GlobalNOC

Science DMZ

- design to support high performance science apps

  – reduce loss that impacts TCP perf

  – appropriate security for 100Gbps

  – integrate network test points

- go fast, keep it controlled

This

I should try rear engine

Not This

GlobalNOC

3
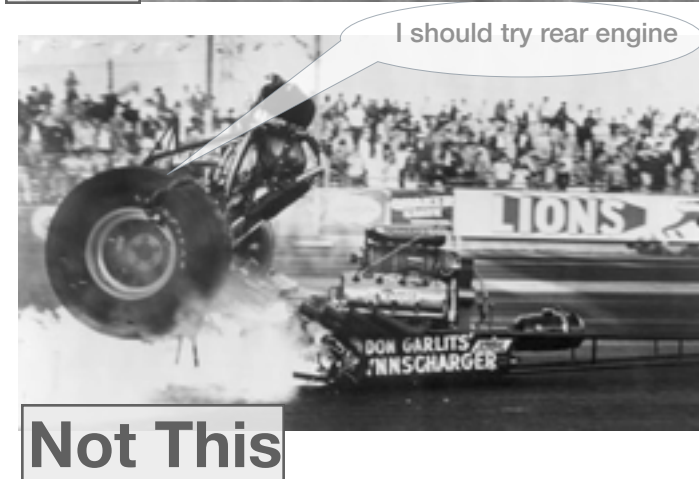
Objective:

- reconfigure existing components for better experience
- Correct, Consistent, Performant, Affordable
- 100G Science DMZ with security features baked in.
  - adaptive IDS load balancing
  - hardware block / forward traffic
  - controlled bypass of institutional firewall
  - integrated measurement

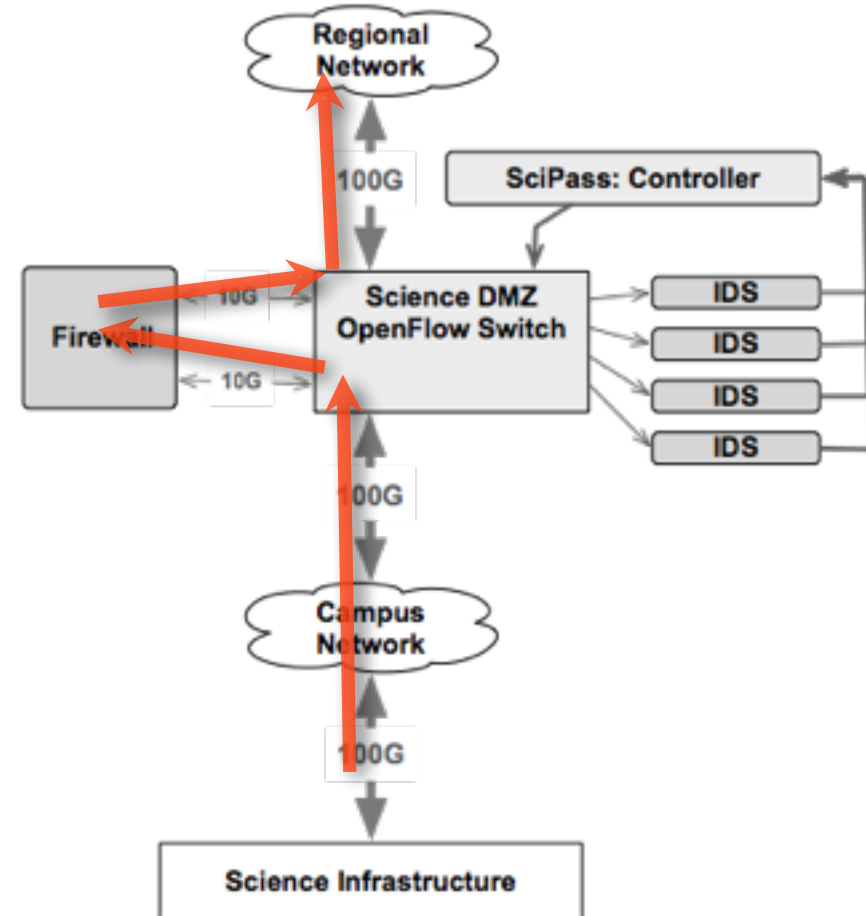**Even Better, engine in rear**

GlobalNOC

4

Approach

- Combine
  - OpenFlow Switch
  - Bro
  - PerfSonar
- create reactive system
- default to secure / slow path
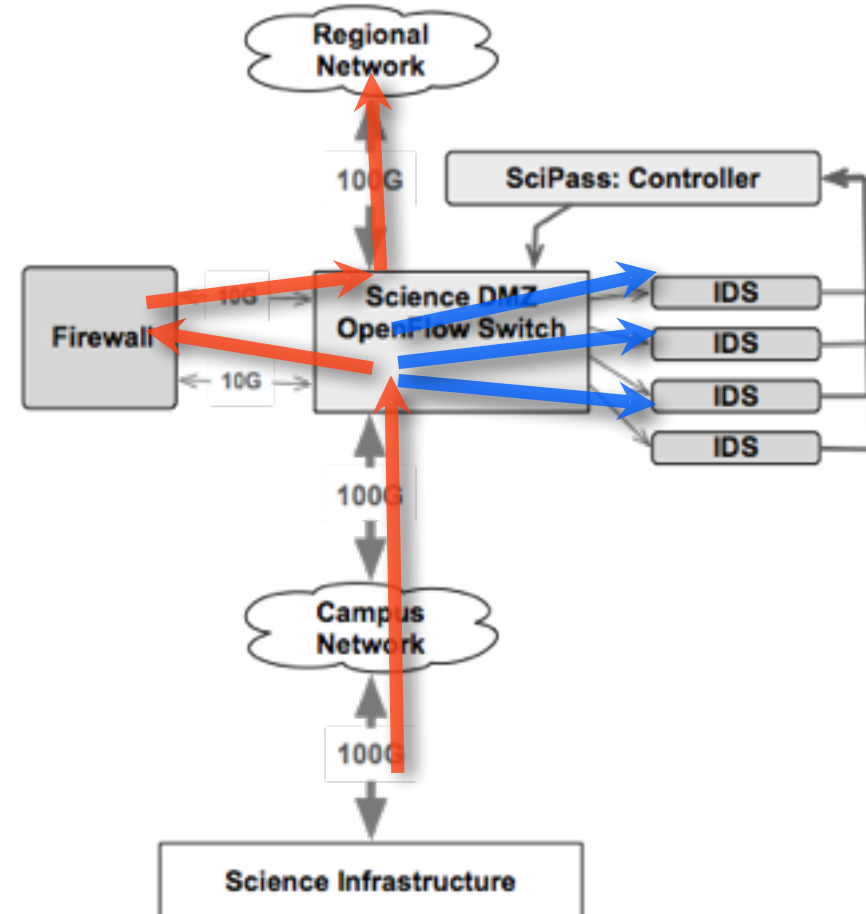- use IDS to control what goes on fast path
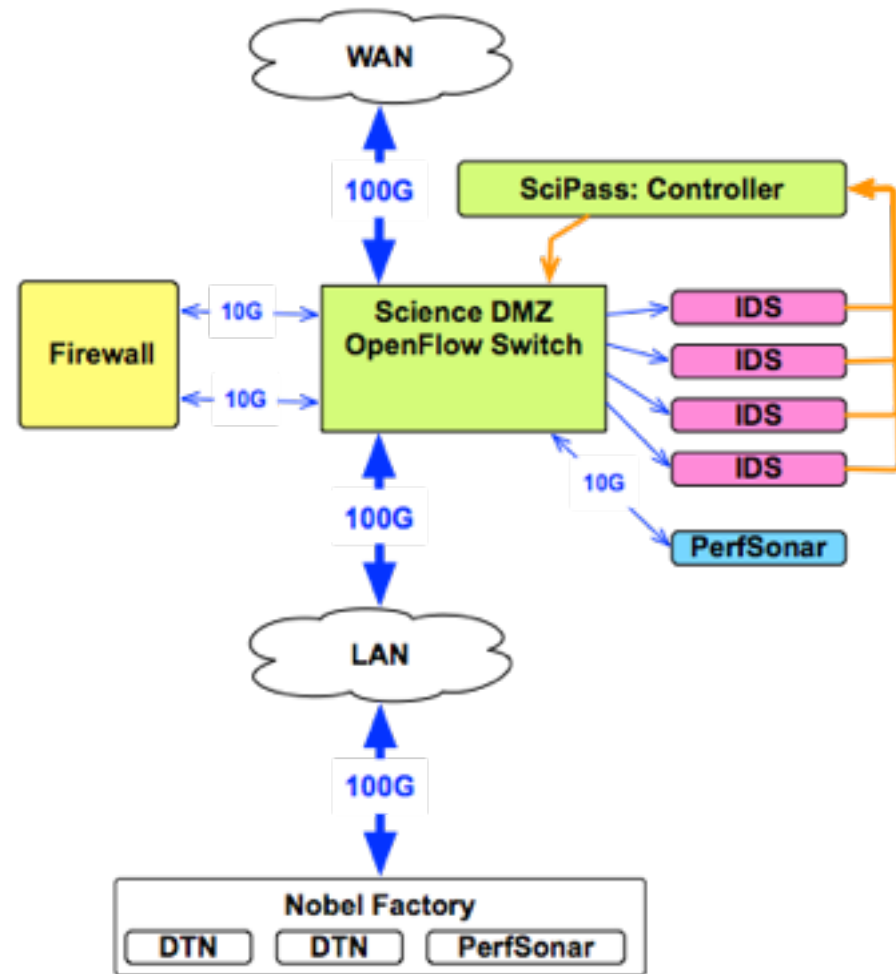
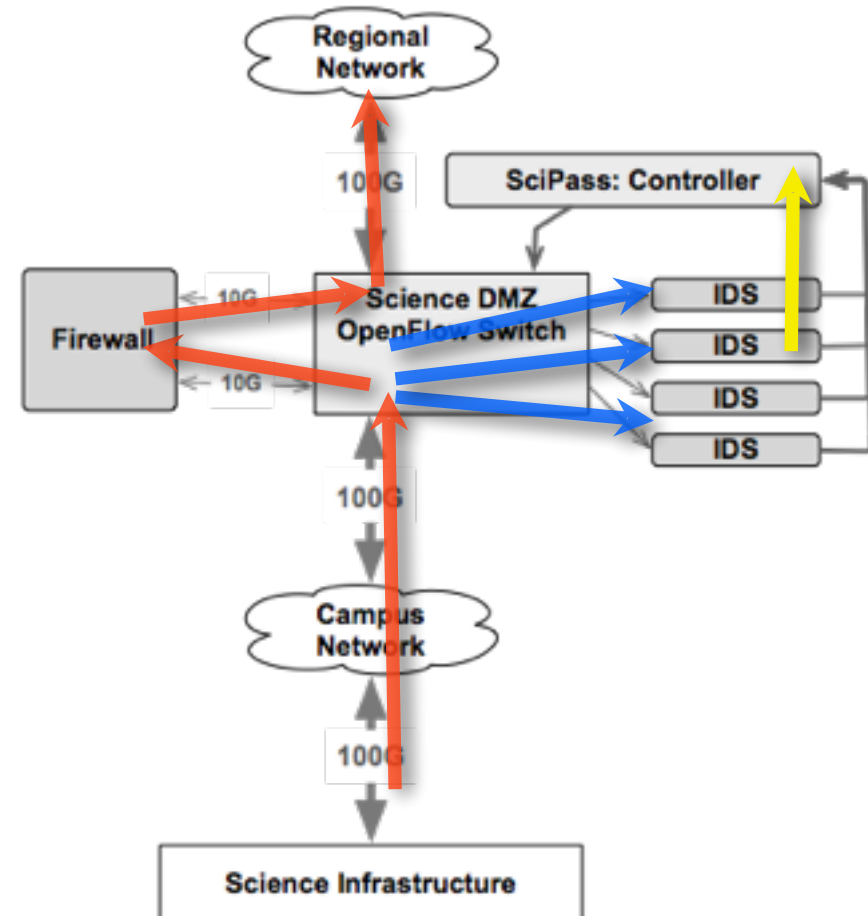# Default Behavior

- traffic goes through firewall

Default Behavior

- In parallel, copies of packets are sent to IDS ports

- copies are sent to array of IDS

- load balancing techniques
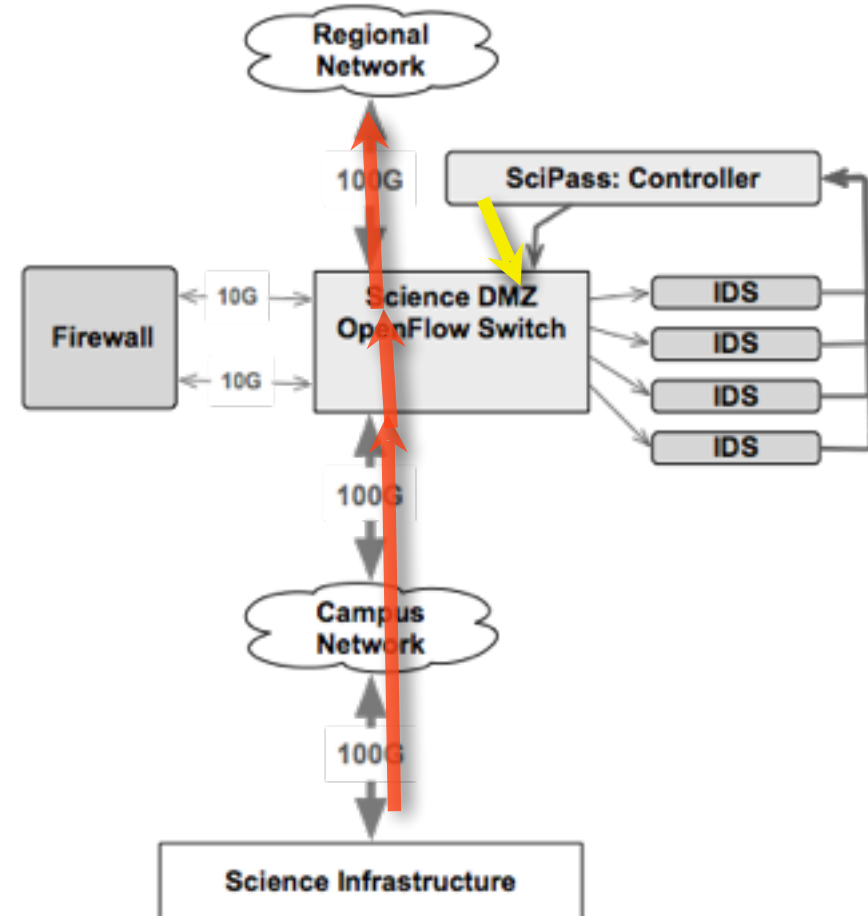
IDS detects **good**

- As IDS inspects traffic
- identifies science flows
- signals SciPass setup fast path and not send data to IDS for flow

SciPass Bypasses Firewall

- Based on IDS input SciPass installs fast path rule for a transfer
  - Firewall is bypassed
  - Traffic not sent to IDS

Technical Details

- stand alone / appliance SDN Deployment
- combines Bro with SciPass to create a reactive / adaptive system
- The **new thing** here is that we are **fingerprinting GOOD** traffic and enhancing its path through the DMZ.
- Oh and we can do fine grained 5-tuple based blocking

Simple Load Balancing

- Similar to binary search
1. Divide IP space into the number of sensors on start
2. check the sensor load, if above threshold
   a. split prefix with largest load but leave on same sensor
   b. observe load by subnet
   c. if highest load subnet too big to move to other sensor, goto 3
   d. if subnet will fit on other, move subnet to less loaded sensor
3. repeat periodically

GlobalNOC

Who is doing this?

- Indiana University
  - GlobalNOC
  - Indiana University Security Office
- Collaborating with
  - Bro Team
- Looking for other participants

Testing

- DMZ deployed in Indianapolis lab
  - Brocade MLXe switch
  - Netscreen 5200
  - IBM G8264
- Tested to ESnet well known test points
  - 7ms of delay to the Argonne server
  - http://fasterdata.es.net/performance-testing/DTNs/

Manual Bypass after 8 sec
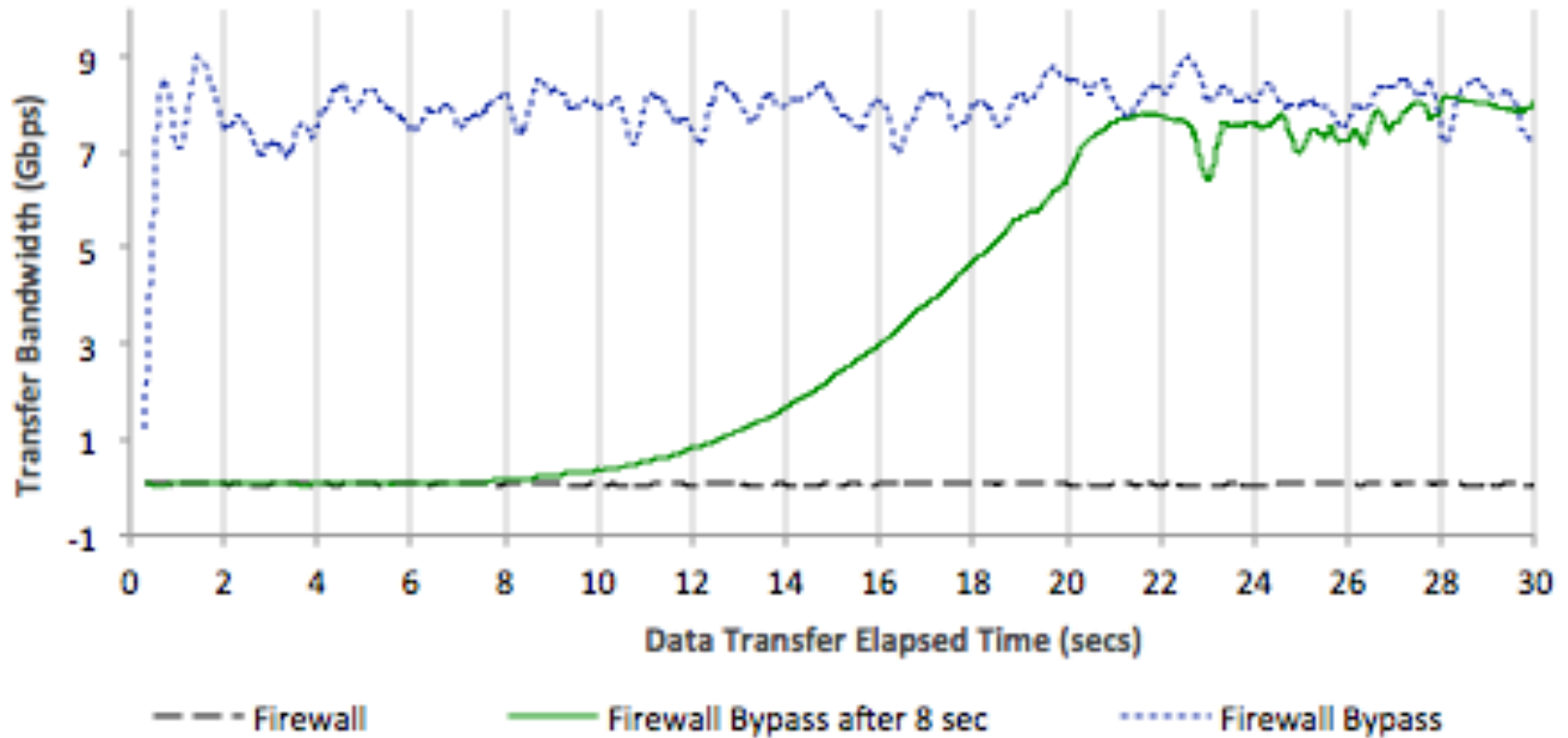
Reactive Bypass Performance

- 64 ms - time to detect and bypass
- 250 ms - doubled throughput of firewall
- 1.5 sec - same throughput as no firewall
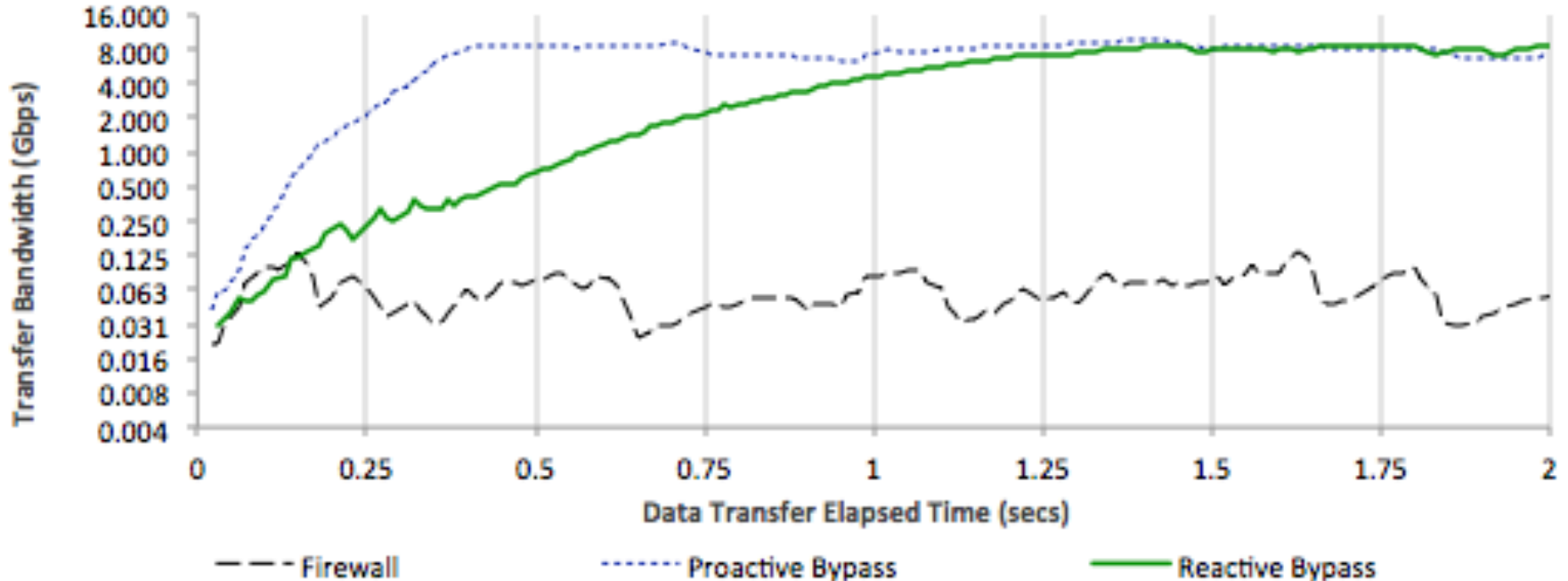
IU Campus Trial

- Deployed temporarily for IDS load balance
- Mix of Bro and Snort
- 8 sensor groups
  - each group contains 1 bro + 1 snort
- 18,000,000 possible local addresses
- 10 to 20Gbps of traffic avg
- Test effectiveness of balance

GlobalNOC

16

Trial Results

- 20% traffic load delta after 10 balancing rounds
- 10% traffic load delta after 20 rounds
- stopped short of 5% due to traffic patterns
- results encouraging

GlobalNOC

Status

- IDS load balancer deployment in June
- Planning for field trials of DMZ use case
- First "production" release available
- Investigating non-sampled flow at 100g
  - netsage project
  - IDS load balancer deployment

GlobalNOC

More Info

- Project Page
  - **http://globalnoc.iu.edu/sdn/scipass.html**
- Code Repository
  - **https://github.com/GlobalNOC/SciPass**
- email
  - **ebalas@iu.edu**

GlobalNOC