SciPass
Secure OpenFlow Based Science DMZ

Edward Balas

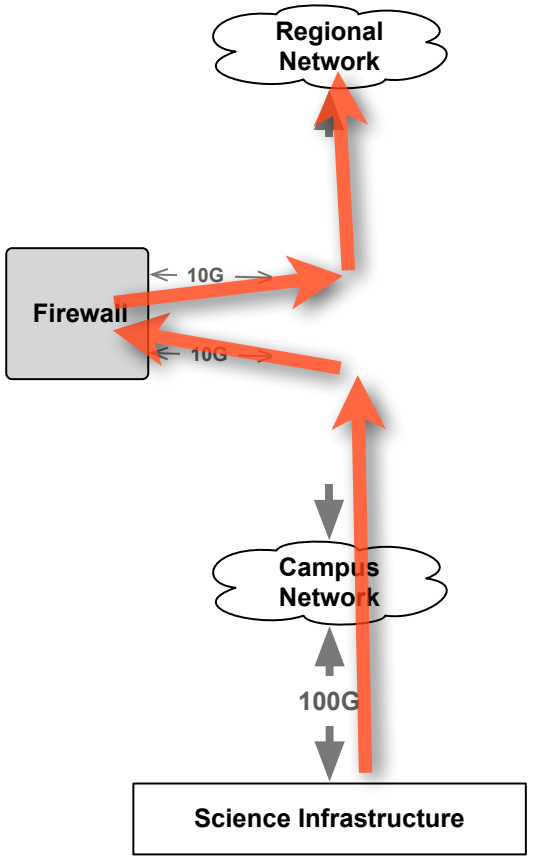
July 9, 2014

OIN Operating Innovative Networks

GlobalNOC

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?



OIN Operating Innovative Networks

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

OIN Operating Innovative Networks

GlobalNOC

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

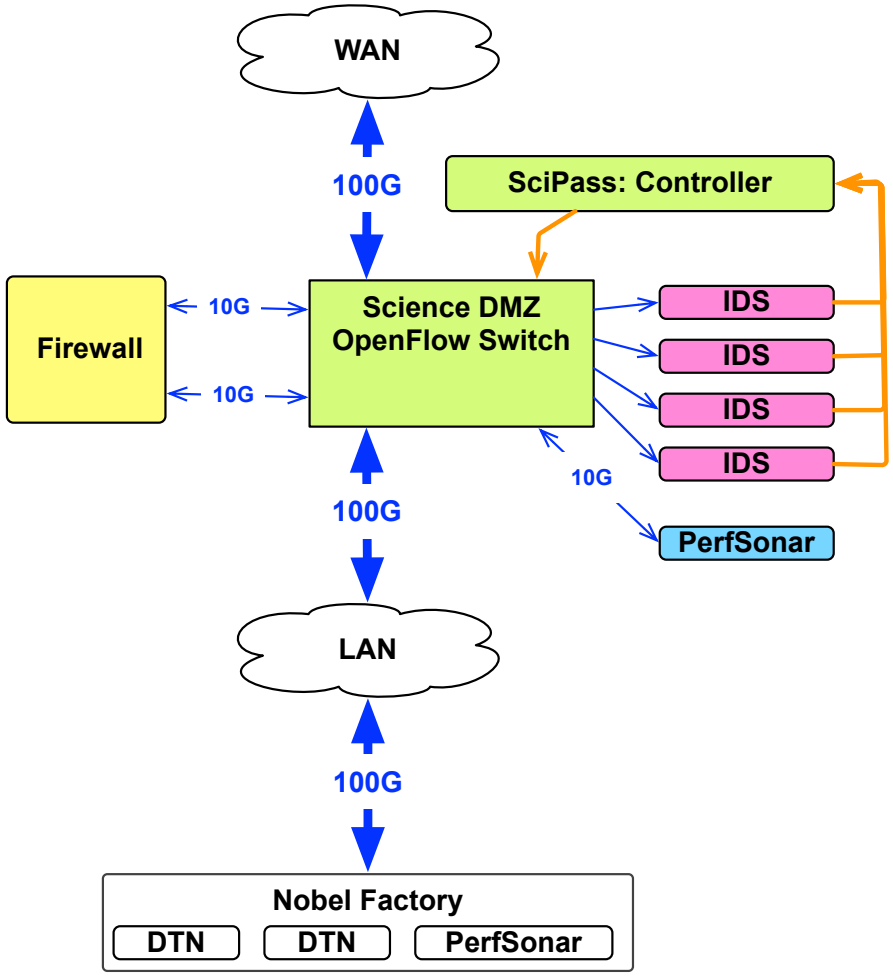
Even Better, engine in rear

OIN Operating Innovative Networks

GlobalNOC

Approach

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

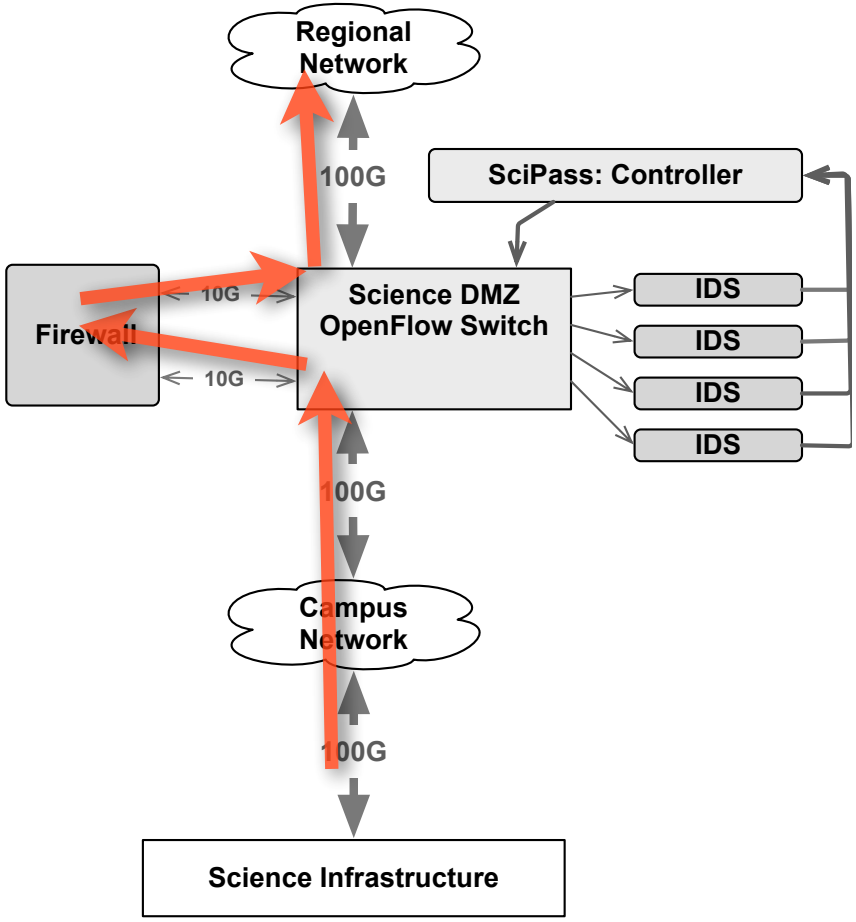


OIN Operating Innovative Networks

GlobalNOC

Default Behavior

- traffic goes through firewall

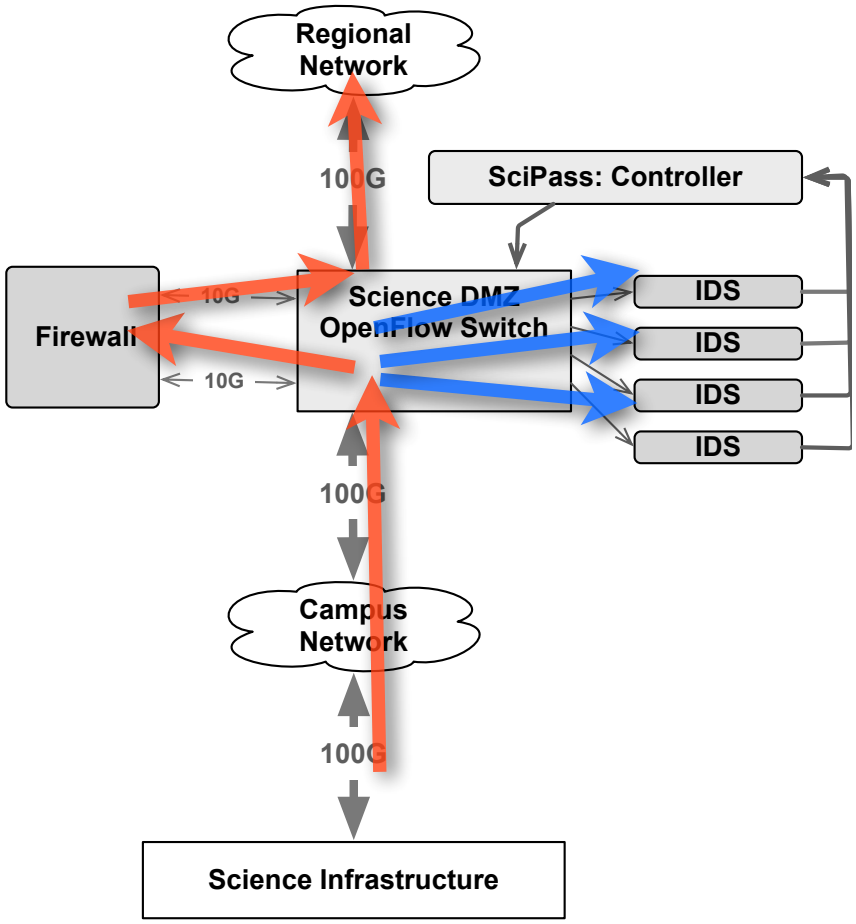


OIN Operating Innovative Networks

GlobalNOC

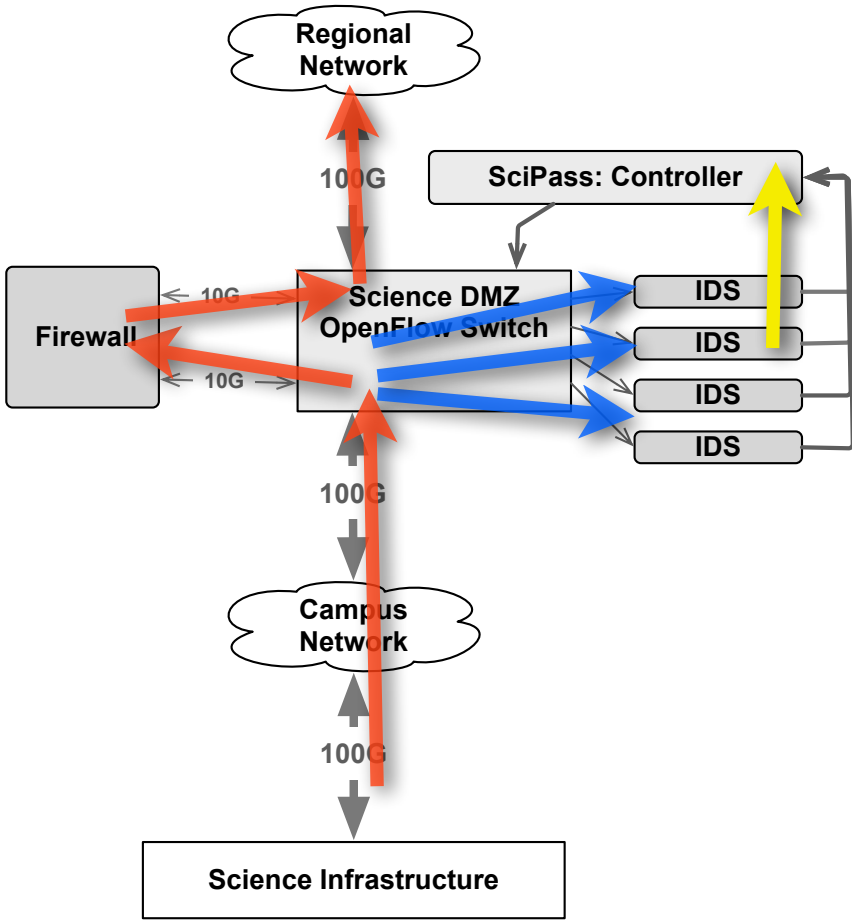
Default Behavior

- 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

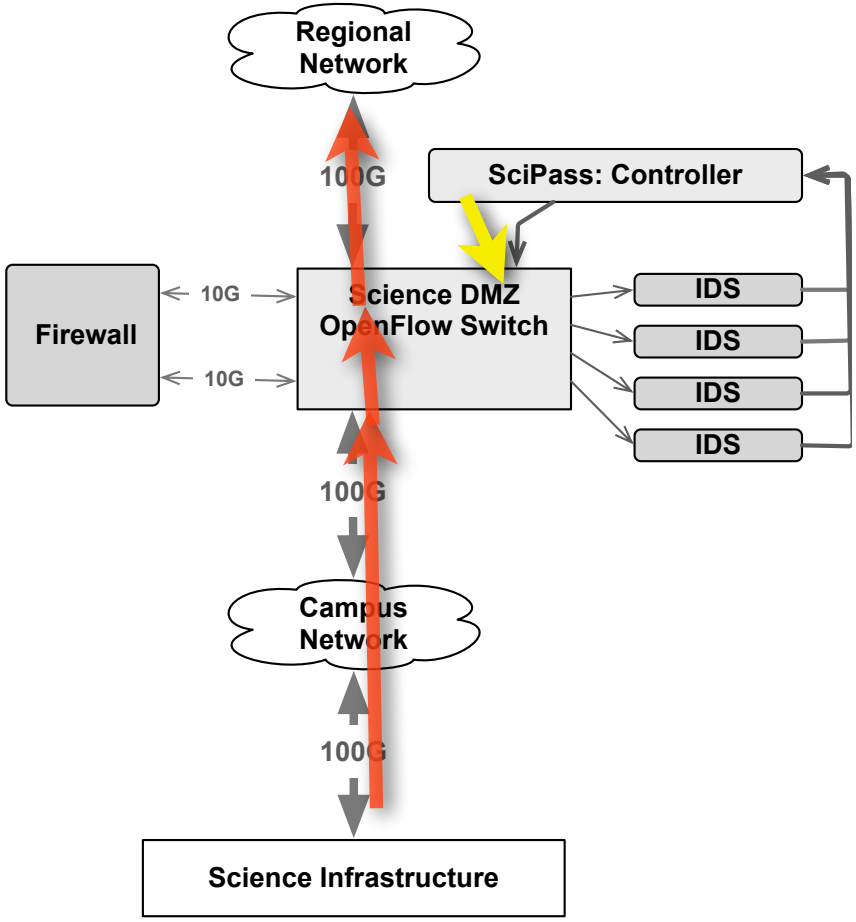


OIN Operating Innovative Networks

GlobalNOC

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

OIN Operating Innovative Networks

GlobalNOC

Who is doing this?

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

Status

- code for balancing working against mininet
- bypass features should be done in 2 weeks
- live testing with Brocade MLX in InCNTRE lab in August 2014
- demo or die
  - Layer123
  - Internet2 Technology Exchange
  - SC14

More Info

- Code Repository
  - **https://github.com/GlobalNOC/SciPass**
- email
  - ebalas@iu.edu

OIN Operating Innovative Networks

GlobalNOC