Fermilab

U.S. DEPARTMENT OF ENERGY | Office of Science

FNAL Site SDN Perspective(s)

Phil DeMar

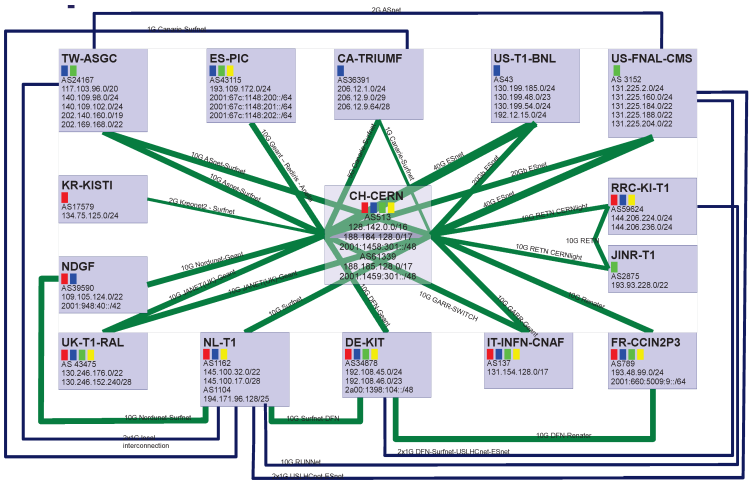
SDN Workshop

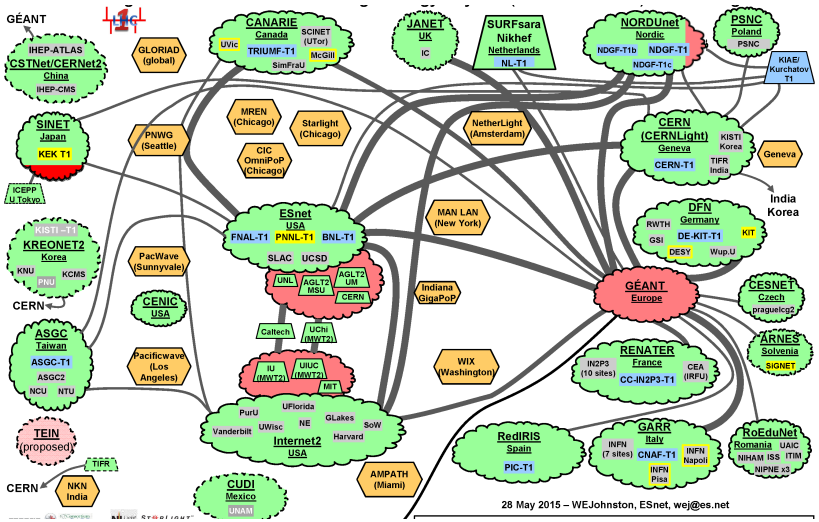
LBNL

July 14, 2015

LHC WAN Data Movement at FNAL

- ~95% of FNAL WAN traffic
- Well understood:
  - Source/destination
  - Traffic characteristics
- Traverses “special” WAN paths:
  - LHC Optical Private Network
  - LHC Open Network Exchange
  - Pt-to-Pt OSCARs circuits
  - But also use general R&E network paths
- Distributed computing model
  - With global scope
- Inherently multi-domain paths



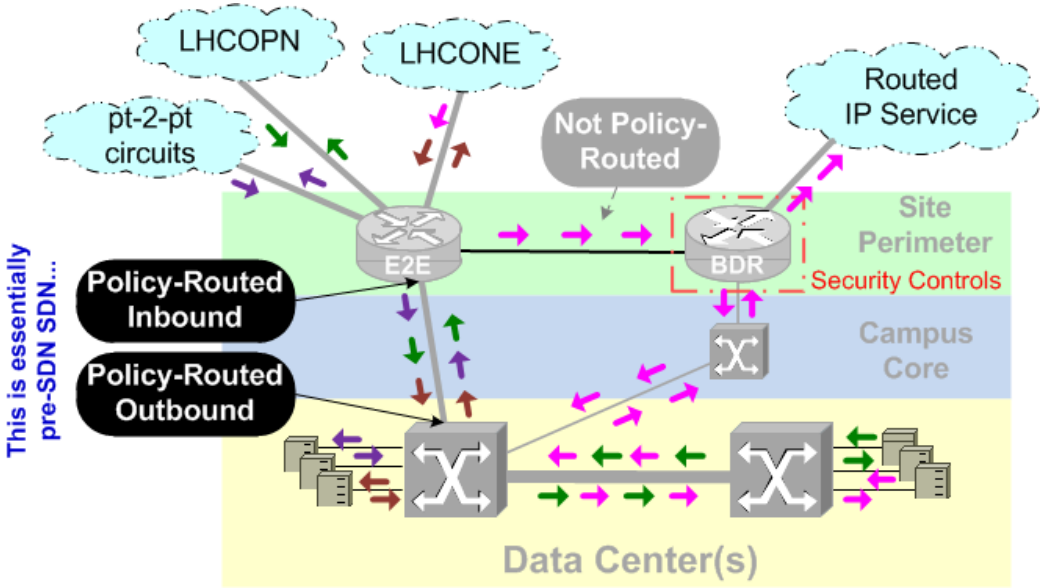


Internal Isolation of LHC WAN Traffic

- FNAL separates LHC WAN traffic to special network paths
  - Consistent with general philosophy to isolate high impact traffic
- Keyed on Policy-Based Routing (PBR)
  - Essentially source/destination ACLs
- Satisfies site security policy for bypass:

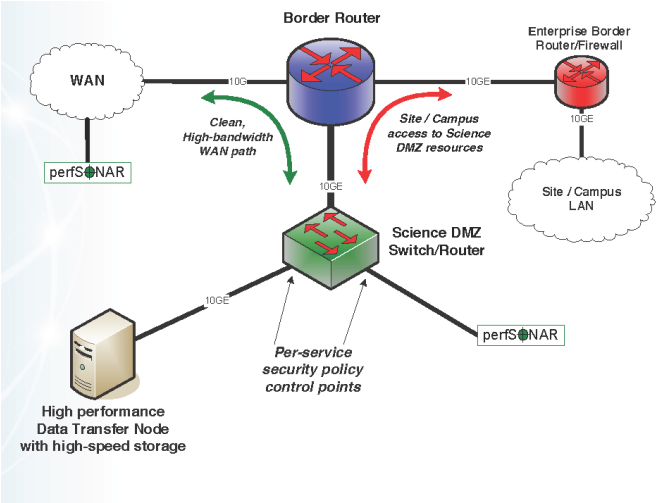
"Known traffic from well-managed systems at trusted sites"

- Non-PBR traffic follows routed IP path
  - May create path asymmetry issues

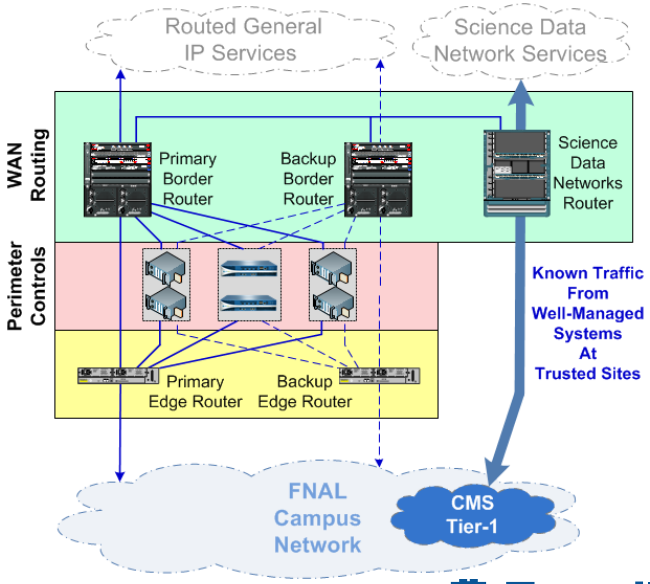


Science DMZ vs FNAL LHC Data Movement

- Science DMZ(s):
  - Bypass network paths
  - DTNs (tuned)
  - Monitoring component (PS)
  - Typically:
    - Dedicated physical infrastructure
    - Modest scaling issues



- FNAL LHC "DTNs":
  - Integrated into data center networks
  - Serve as storage & internal workflow servers
  - Large in number (~300)

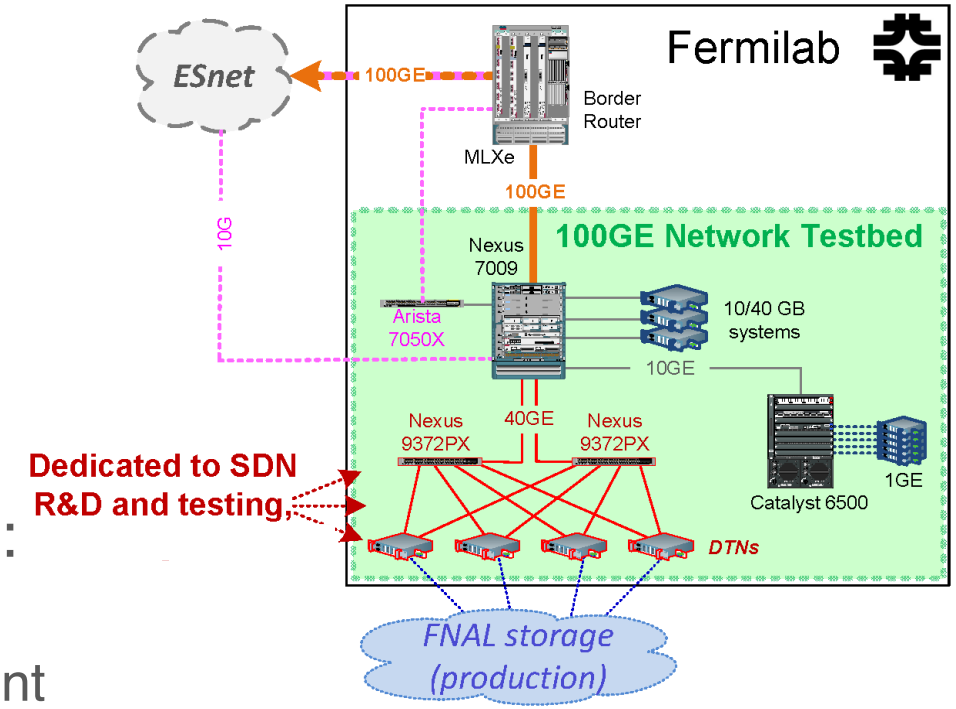


FNAL High-Level SDN Interests

- Current focus is on intra-domain SDN scope:
  - Inter-domain “vision” important, but site model comes first
- Potential SDN use cases:
  1) Science Data Express Path
     - SDN to separate science data from general network traffic
  2) Storage/archiving service for external organizations
  3) Virtual “SuperFacilities”
  4) Logical large-scale test facility
  5) Extreme high performance data movement
- Strong desire to rationalize these to a common site SDN support model

FNAL SDN Development Environment

- Multi-purpose network R&D test environment:
  - 100GE WAN link
    - 10GE alternate WAN paths available
  - (some…) 100GE LAN
- Test bed component dedicated to SDN evaluation & development:
  - For both infrastructure & application level development
  - Currently being deployed

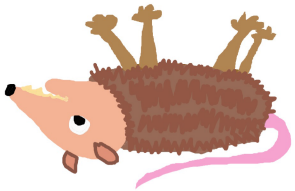


~~FNAL~~ My View of SDN Evolution (Inter-domain…)

- Target should be "true" end-to-end, where E2E extends into the data center…):
  - Not just site perimeter to site perimeter…
- To facilitate that, science DMZ architecture needs to become virtual in nature
  - And extend into the data center
- A wide spectrum of site security models need to be served:
  - Argues for a generic perimeter control service that's flexible enough to support a wide spectrum of site security policies
  - Risk assessment templates could facilitate more flexible site security policies

Major (unaddressed….) **Challenges,** as I see them:

- Site perimeter security issues:
  - Authorization
  - Negotiation (including termination capabilities…)
  - Traffic mirroring
- Site Path & Configuration Control
  - Conventional wisdom of topology info → optimal path decision is a:



Really Dead!!!

  - Expect preferred & (probably) predetermined paths
    - Even this is a daunting challenge to do in a "standard" way…
- Instrumentation
  - Need real-time visual representation(s) of SDN paths and what's happening within them

Questions?