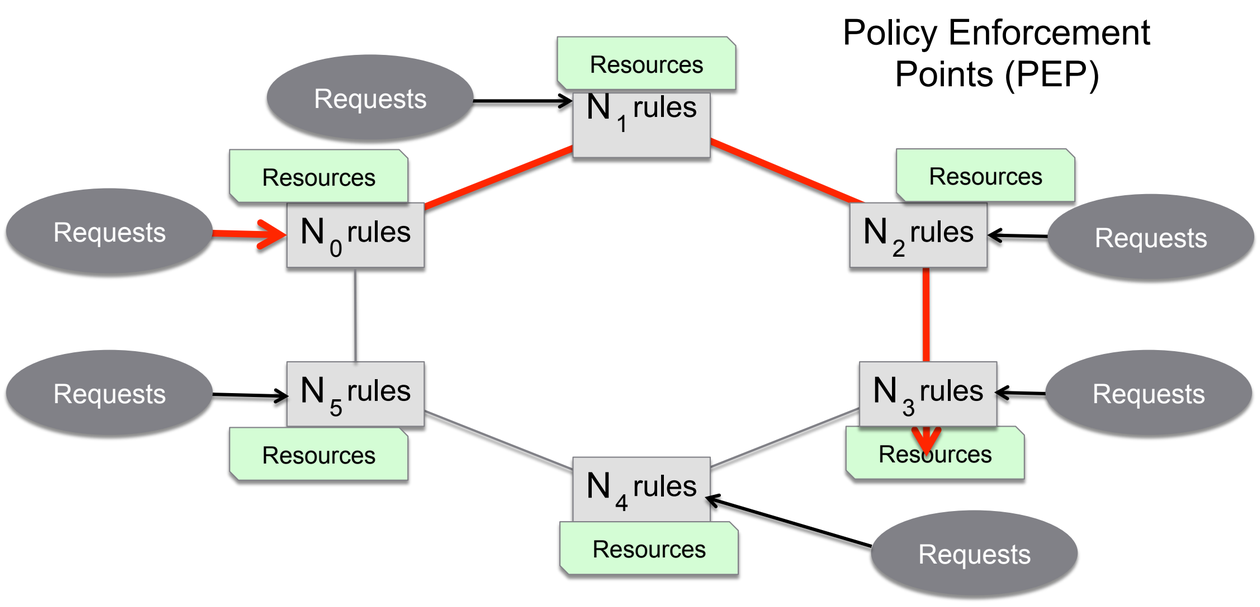
Quantitative Assessment of Access Control Compliance

David M. Nicol, William Sanders, University of Illinois at Urbana-Champaign

Objective : Test hypothesis "smart statistical sampling is effective at estimating metrics that measure compliance of access control *implementation* with access control *policy*."

Advancement of SoS : Demonstration of mathematically sound technique to deal with enormous state spaces

Problem : Access control in distributed system has combinatorially many paths



Every PDP exercises some aspect of policy implementation

Number of unique access paths is O((#rules per PEP)^{diameter})

Computationally intractable to assess compliance of **every p**ath in large, deep networks

Approach

Define compliance metrics, e.g.,

- fraction of compliant paths
- Average number of violations @ path
- Weighted score on critical resources

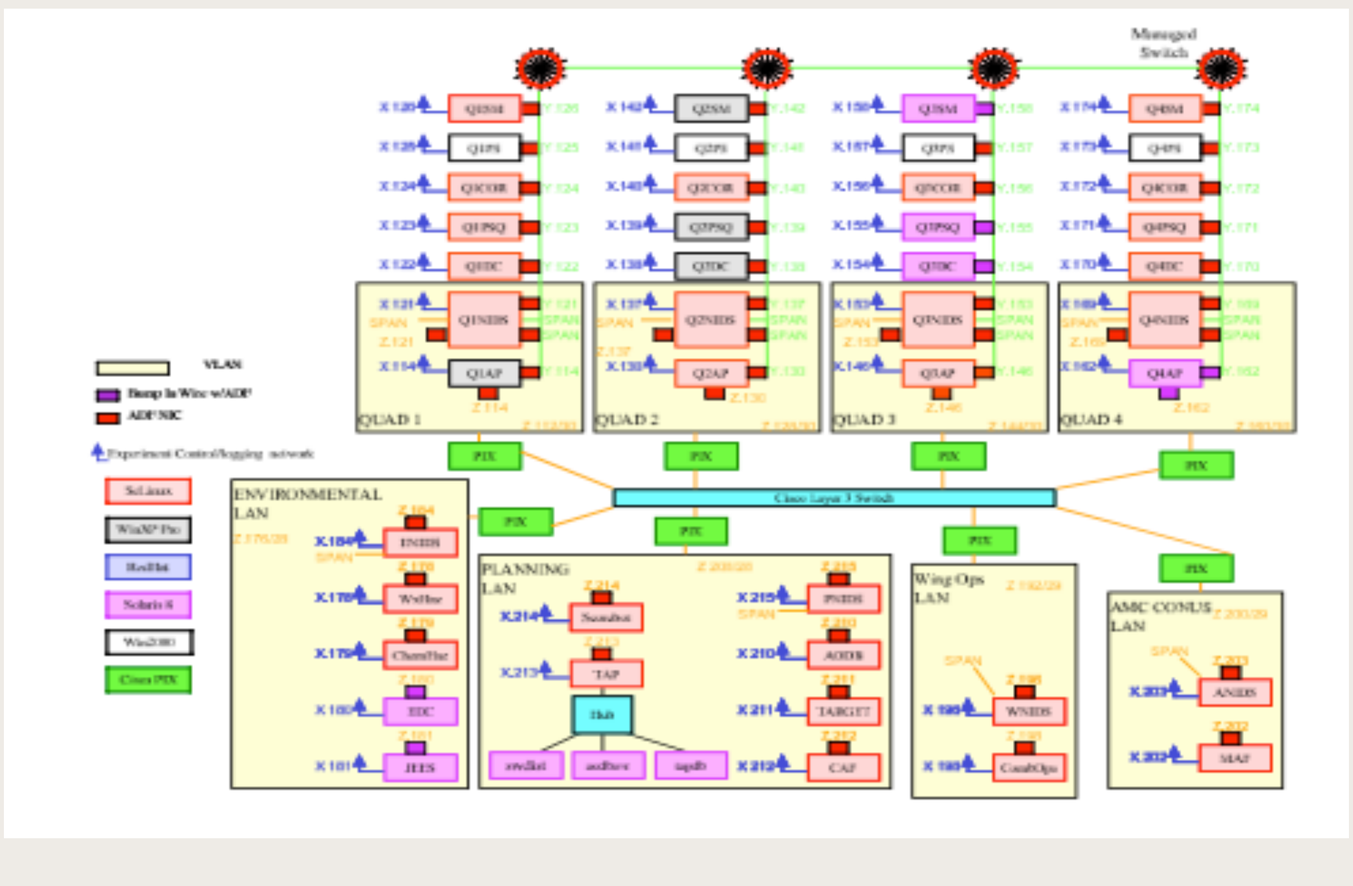
Dramatically reduce confidence interval using biased sampling

- Importance sampling
- Splitting

Embed in tool that analyzes systems with distributed firewalls (NetAPT)

- Policy includes NERC-CIP requirements, NIST Best Practices recommendations

Example



Challenges

- Uniform sampling of paths
- Biasing Heuristics
- Proofs of variance reduction
- Demonstration on large systems

Intrusion tolerant pub-sub (DARPA DPASA), host-based firewalls

- 50+ PEPs, 10s of rules each
- Exhaustive analysis does not complete in 3 hrs
- Importance sampling estimates fraction of non-compliant paths, with 10% relative error, in 1 minute

2012 Science of Security Community Meeting
Nov. 29-30, 2012
National Harbor, MD
http://cps-vo.org/group/sosmtg