U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

William H. Sanders

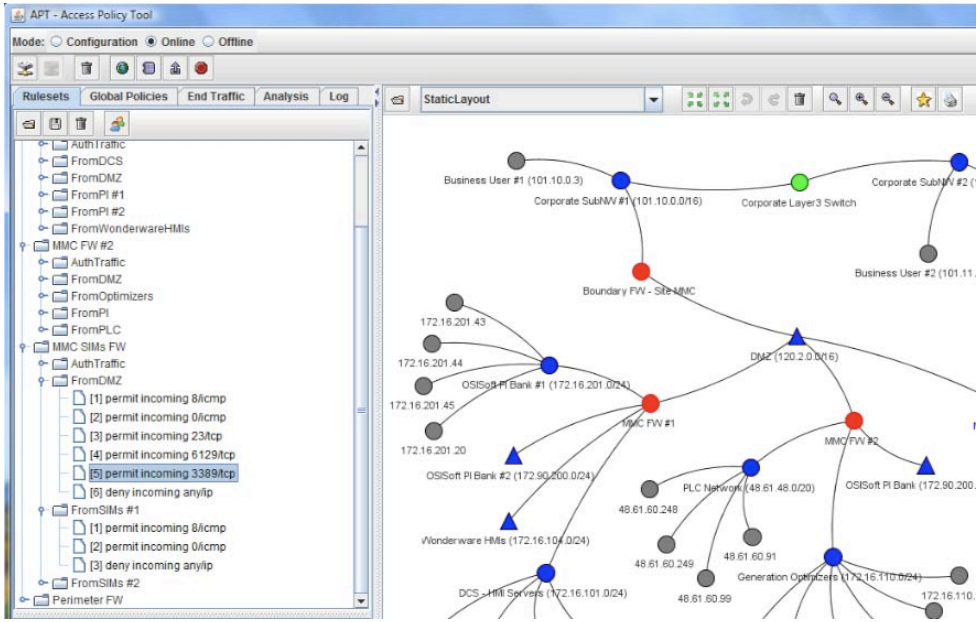
University of Illinois

TCIPG: Network Access Policy Tool (NetAPT)

(Joint work with David Nicol, Mouna Seri, and Sankalp Singh)

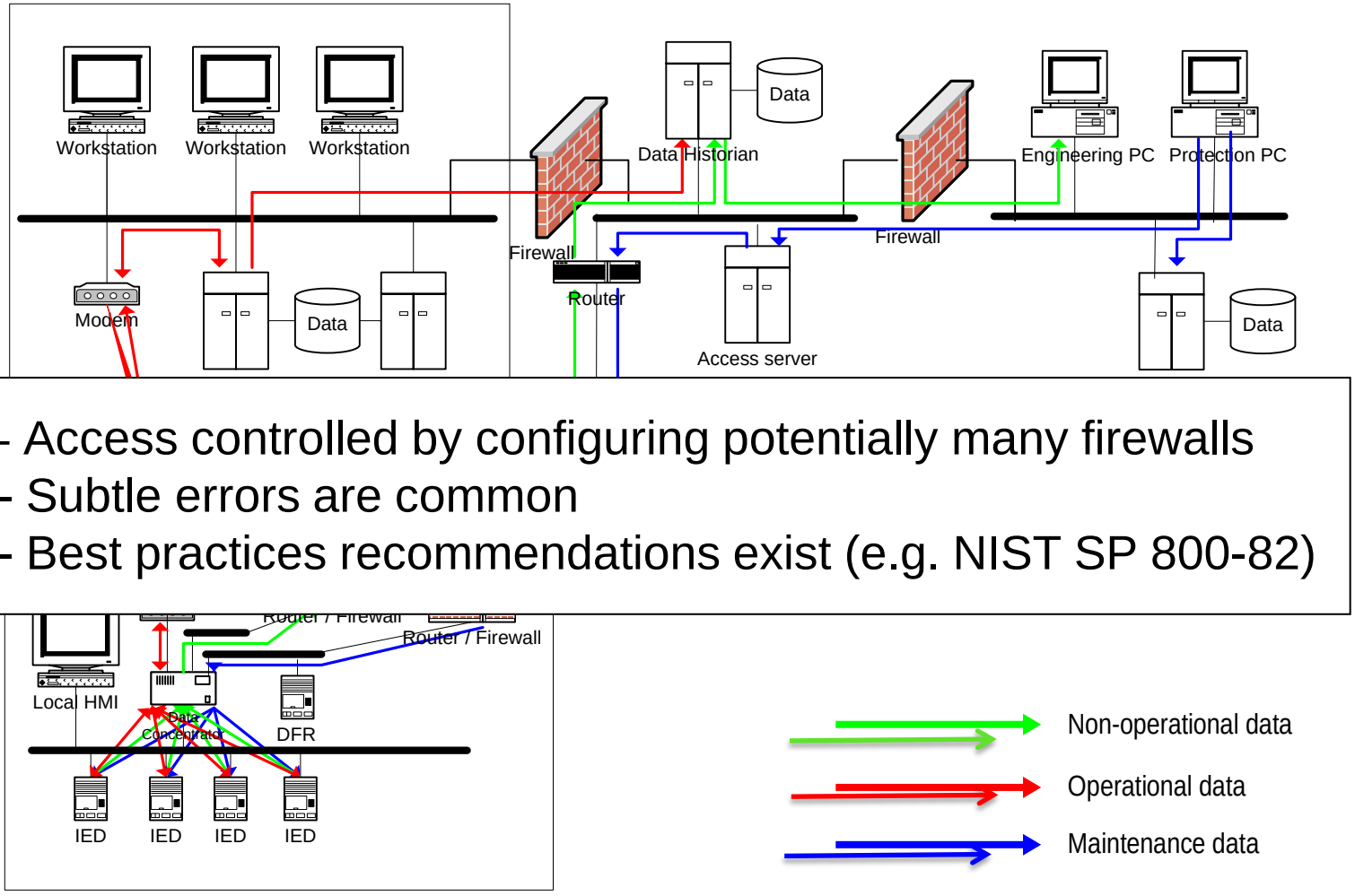
Summary Slide: NetAPT

- **Outcomes: Tool to *prove* correctness and compliance of firewall settings in networked setting.**
- **Roadmap Challenge:** Limited ability to measure and assess cyber security posture
- **Major Successes (since transition to TCIPG):** NetAPT used in major internal audit of industrial partner's control system network. Tool significantly enhanced as based on experience gained during use.



- **Schedule:** Original tool developed with TCIP and I3P funding. Transitioned to TCIPG 2/10.
- **Level of Effort:** TCIPG Funding
- **Funds Remaining:** TCIPG Funding
- **Performers:** University of Illinois
- **Partners:** Ameren, Sandia

Background: Control Systems Networks Today



- Access controlled by configuring potentially many firewalls
- Subtle errors are common
- Best practices recommendations exist (e.g. NIST SP 800-82)

PCS Diagram Source: Scott Mix Lecture 04/07

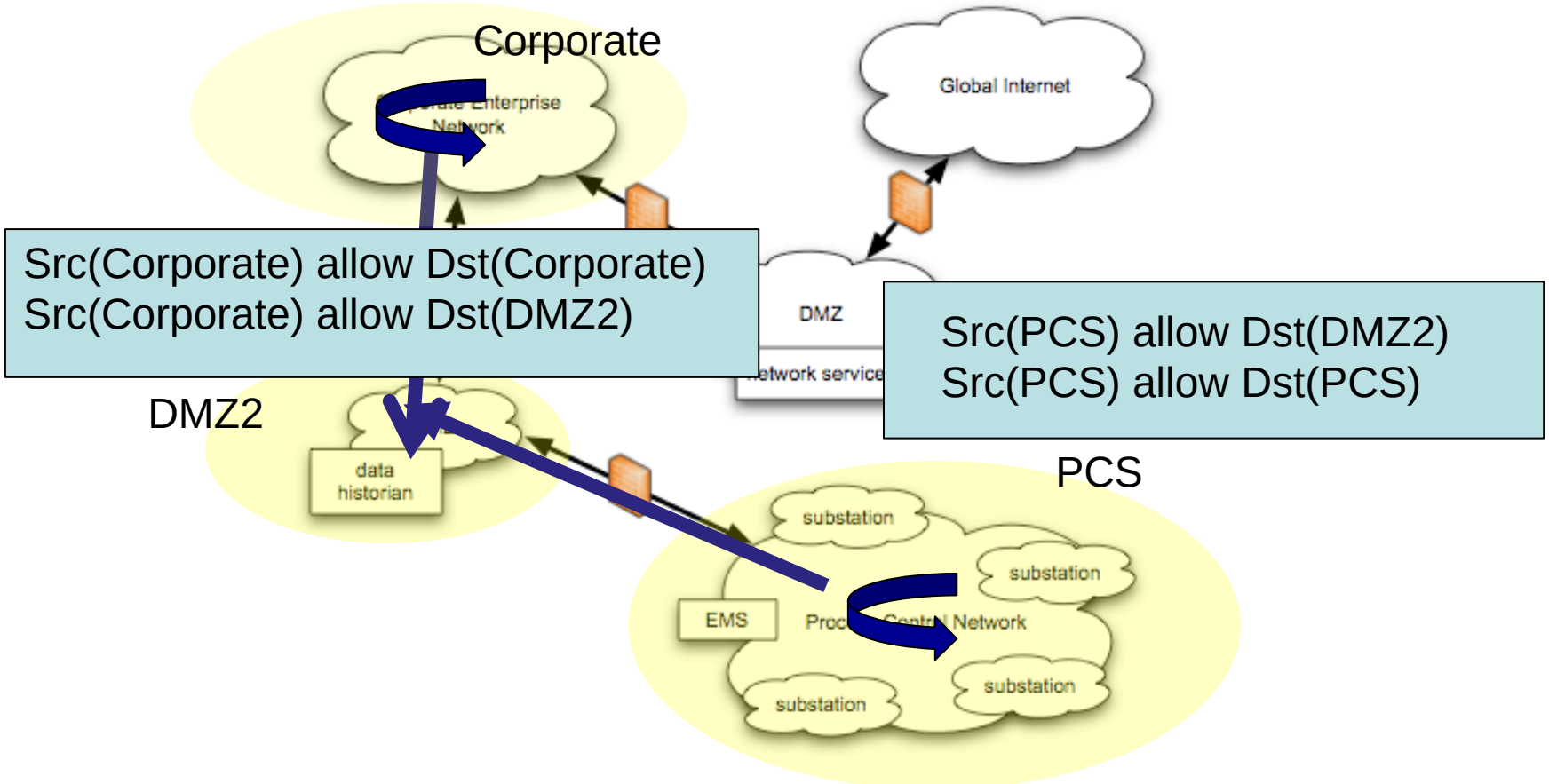
Examples of Best Practices

- The base rule set should be deny all, permit none
- All permit rules should be both IP address and TCP/UDP port specific
- All traffic should terminate in the DMZ
- All traffic should be prevented from transiting directly from the control network to the corporate network, and vice-versa
- Any protocol allowed between control network and DMZ should NOT be allowed between DMZ and corporate network

Need to Precisely Define Global Policy

Define global names for sets of hosts, sets of subnets, sets of protocols, ports, etc. Define global policy like a system-wide firewall

Traffic should be prevented from transiting directly from the control network to the corporate network, and vice versa. All traffic should terminate in the DMZ.



Issues to Address

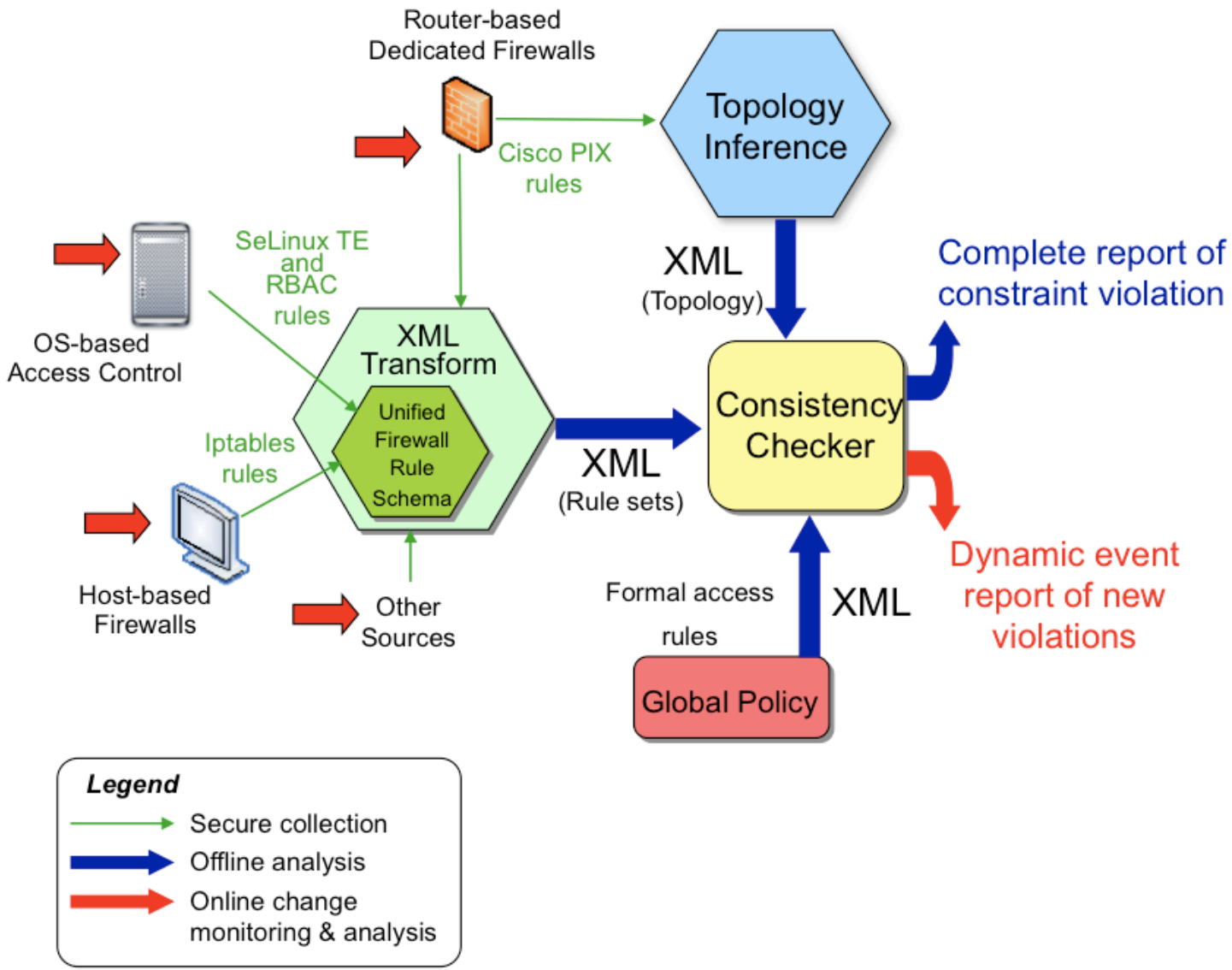
How can one express Best Practices as Global Access Policy in machine checkable form?

How can one detect violations of Global Access Policy?

How can one demonstrate compliance with configuration standards?

Solution: Use the Access Policy Tool!

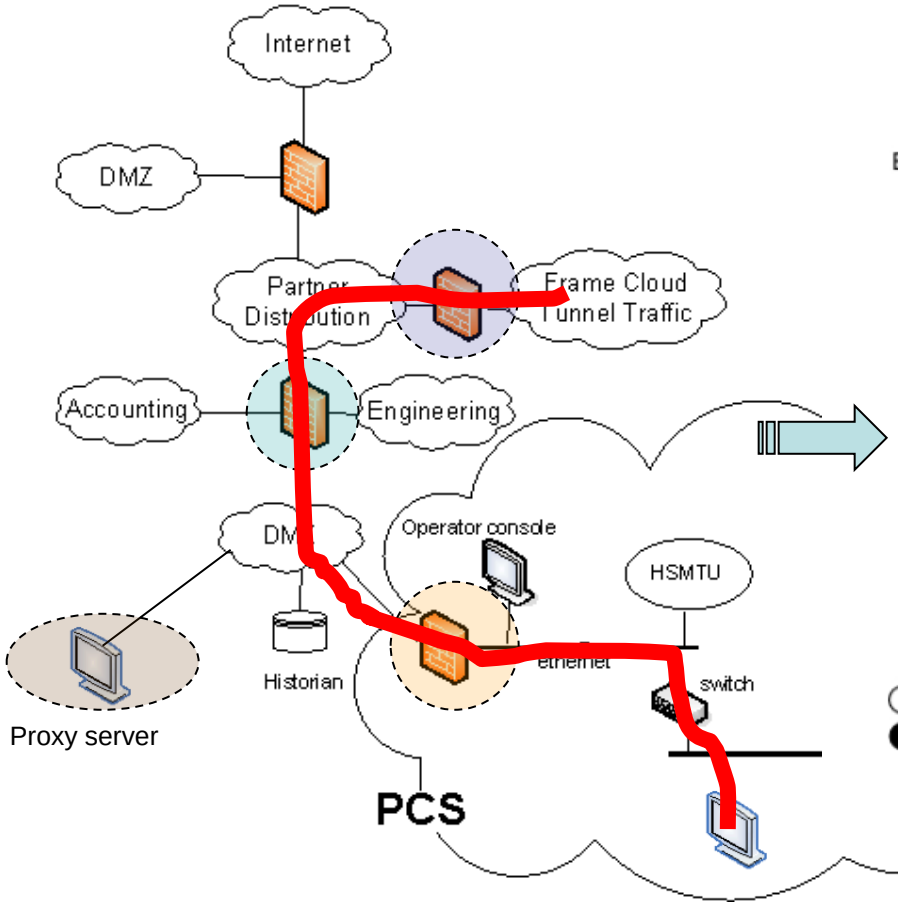
Review: NetAPT Architecture



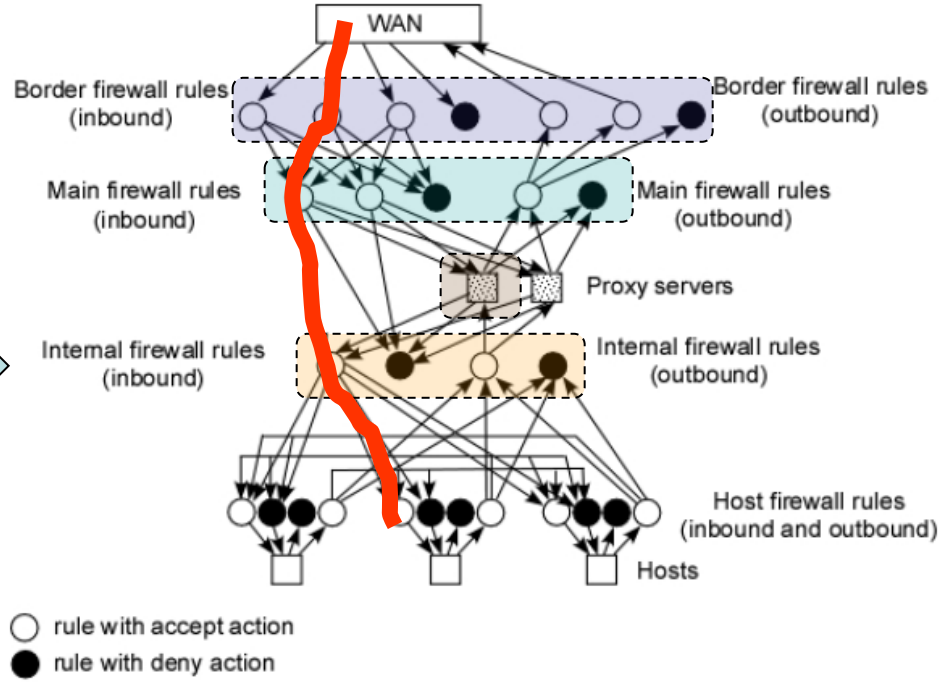
Heart of the Analysis: Rule Graph

Analysis based on identifying paths through “rule graph”

- Each hop in path corresponds to “policy implementation”



Network Architecture



Possible Network Layer Rule Graph

Research Issues Addressed in Developing NetAPT

Performance Optimization

- Compact rule graph representation
- Fast algorithms on compacted rule graph

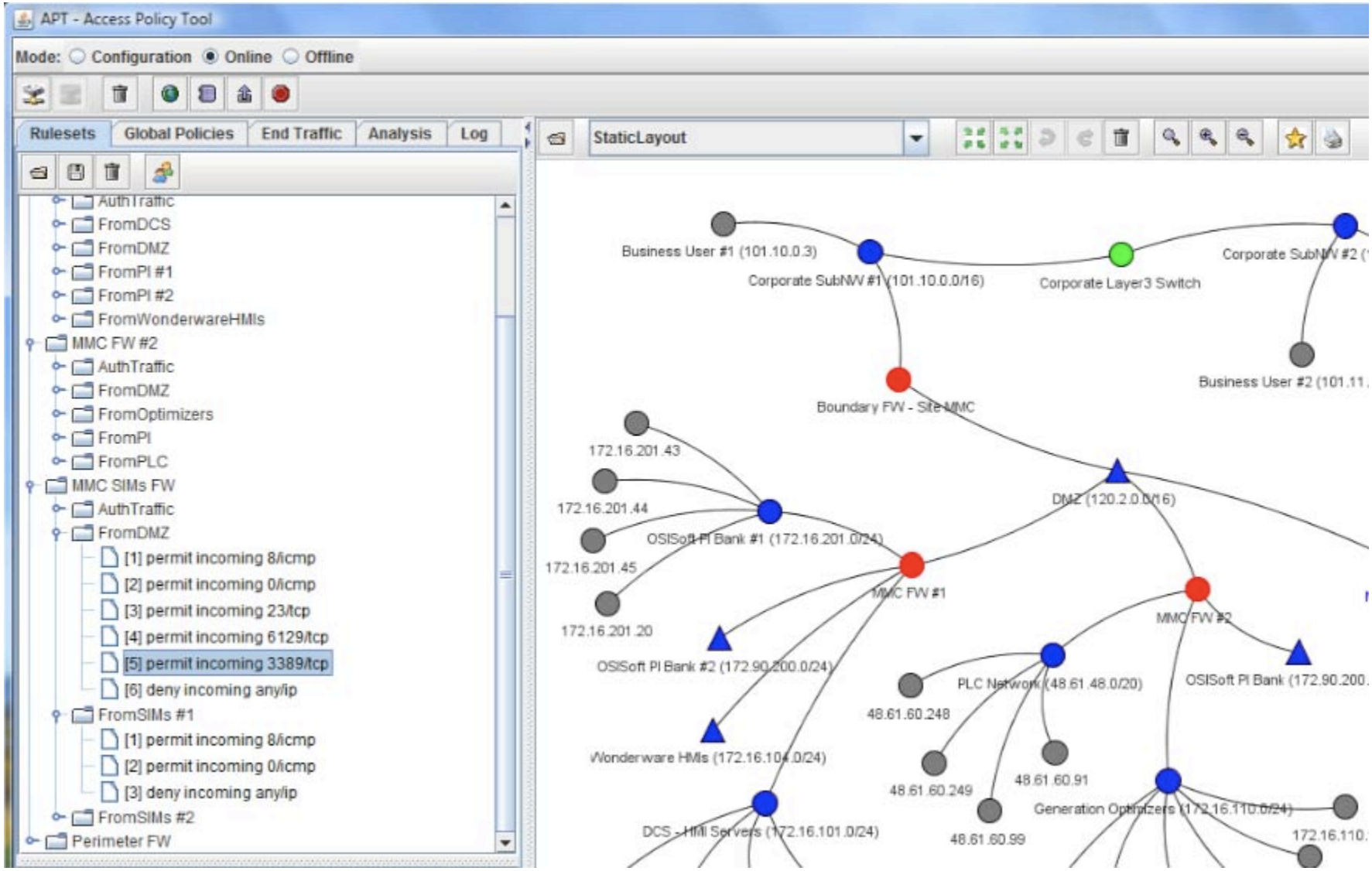
Intelligent partial graph exploration

- Prioritize path exploration on rule graph paths
  - e.g., importance sampling to estimate compliance metric

Properties of analysis based on “discovered” topologies

Generation of firewall rules to implement global policy

APT - Prototype



TCIPG Activities – 2/10 to 7/10

Major Focus on Collaboration and Technology Transfer:

- Test NetAPT in major internal audit at conducted on industrial partner's network.
- Enhance NetAPT based on experience gained in use

NetAPT Test

- Over 70 firewalls, large scale network
- Support:
  - Analysis of authenticated traffic
  - Automatic generation of connectivity map
  - Analysis of multi-homed NATed subnets

APT Enhancements Motivated by Industrial Interaction

- Support firewall filtering that requires authentication
- Support object group definitions within firewall configurations
- Automate discovery of network topology from the firewall rules and other configuration information
- Incorporate configuration information that indicates that flows can pass between network “islands”
- Make it possible to run APT functions from the command line in such a way that they can be run using the Unix command “cron”
- Enhance the graphical user interface to automate the layout of a network, and to allow hierarchical graphical encapsulation of subnetworks as graphical nodes
- Enhance number of firewall models supported by APT
- Provide global policy templates for common best practices
- Improve conflict detection/resolution in global policy specification

Future Collaboration/Technology Transfer

- Use experience gained in Ameren Audit to enhance tool to directly support analysis of NERC CIP 005
  - With help of Ameren, begin discussions with Matt Stryker at SERC
- Further specialize NetAPT to control systems environment.
- Work with UIUC technology transfer office to determine best path to get NetAPT in the hands of users

Questions?