June 30, 2008 - IFIP Working Group 10.4 Research Report

Information Trust
INSTITUTE

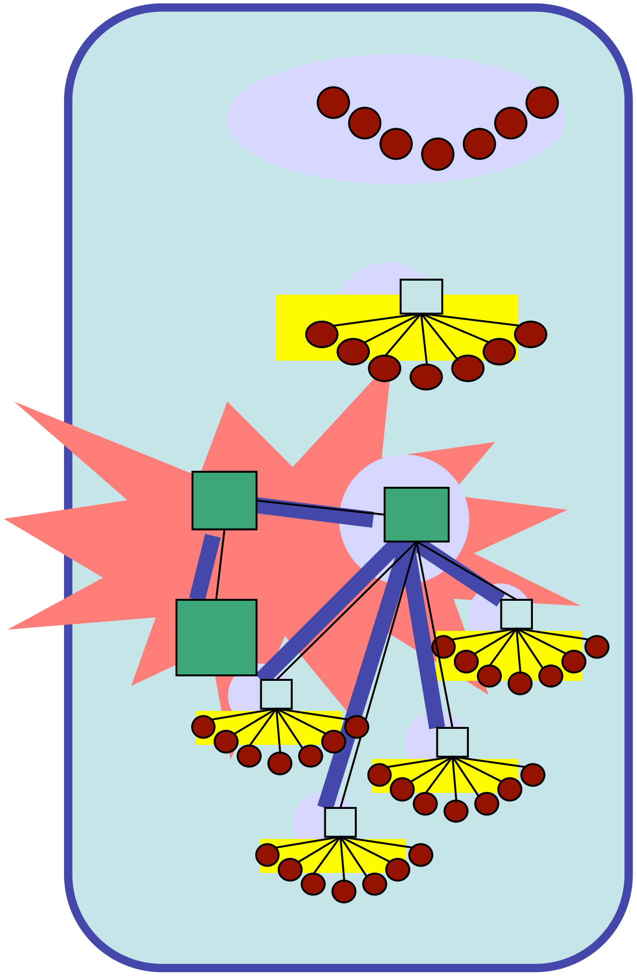
Access Control Policies and Their Impact on Survivability

William H. Sanders
w/ David Nicol, Mouna Seri, and Sankalp Singh
Professor, Electrical and Computer Engineering
Director, Information Trust Institute

www.iti.uiuc.edu

TCIP: Trustworthy Cyber Infrastructure for Power

- Drive the design of *an adaptive, resilient, and trustworthy cyber infrastructure for electric power*, which:
  - Operates through malicious attacks
  - Makes use of cyber and physical state information to guide adaptation
  - Supports greatly increased throughput and timeliness requirements
  - Supports dynamically varying trust requirements
- 5 Year project, funded by NSF, DOE, and DHS
- 20 Senior Researchers, ~20 Graduate Students
- Illinois, Cornell, Dartmouth, Washington State University
- tcip.iti.uiuc.edu



APT: The Need

- Access in networked process control systems controlled by configuration of myriad policies
  - Router-based firewalls
  - Host-based firewalls (software or hardware-based)
  - OS-based or middleware-based mechanisms
- The (usually implicit) global policy implemented through these local mechanisms is difficult to discern
  - Complex interactions can lead to subtle errors and mask problems
- Misconfigurations (implementation deviates from intention)
  - Major source of security vulnerabilities

Misconfigurations are Common

[From: Avishai Wool, A Quantitative Study of Firewall Configuration Errors, IEEE Computer, 2004]

Between 2000 and 2001, studied 37 Check Point FireWall-1 rule sets:

- Almost all of the firewalls had configuration errors.
- The more complex the rule set (in size), the more configuration errors tended to be found.

Need Disciplined Process to Globally Manage Access Control

- Understand what access policies should be globally enforced on your network
- Implement those policies (in a necessarily distributed way)
- Test that the policies have been implemented as intended.
- Manage all subsequent changes to policy to insure that global policies are maintained as intended.

The Access Policy Tool (APT) Supports This Process

- APT analyzes security policy *implementation* for conformance with global security policy *specification*
  - Integrates policy rules (configuration information)
  - Comprehensive offline analysis
  - Dynamic online analysis of incremental configuration
- APT supports
  - Integration of diverse access policy types
  - Exhaustive analysis
  - Statistical analysis
    - Works on large models, estimates global compliance metric

Tutorial: Firewall Rules

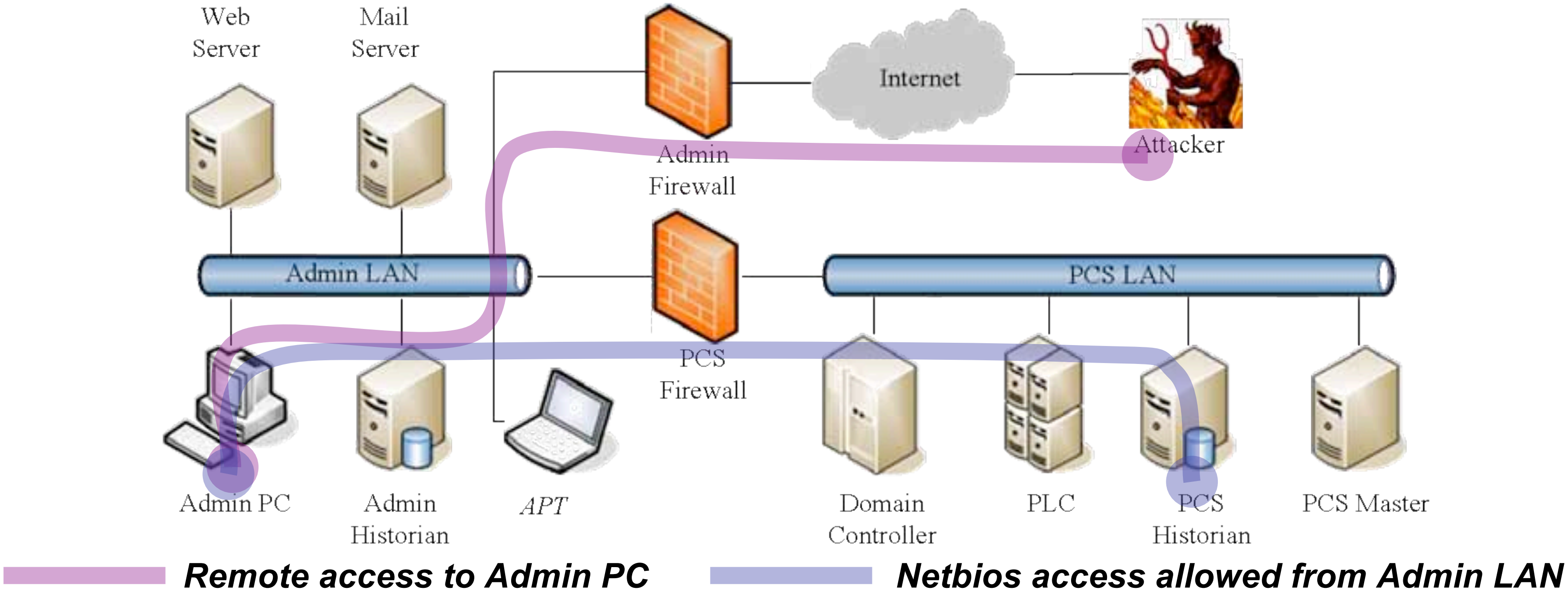
- A firewall subjects each packet to a sequence of rules
  - Each rule identifies a subset of traffic attributes
    - Protocol
    - Source IP address range, source port range
    - Destination IP address range, destination port range
  - A rule admits, or rejects a packet matching the rule’s attribute specification
  - A packet not matching a rule is passed to the next rule
    - Last rule typically a “default” action
- For any packet we can identify which rule admits or rejects it

Tutorial: Global Access Policy

- Global Access Policy (GAP) is composed of statements about sources being able to reach (or not) destination
  - Sets of sources and destinations used in statement
    - e.g. "No host outside the PCS may communicate with any host inside the PCS, except the SQL service on the Historian"
  - Formally, a statement about structured sets of traffic attributes
- We use a policy language based on XACML
  - sublanguage constrained to express connectivity
    - Constraints from application domain avoid undecidability issues

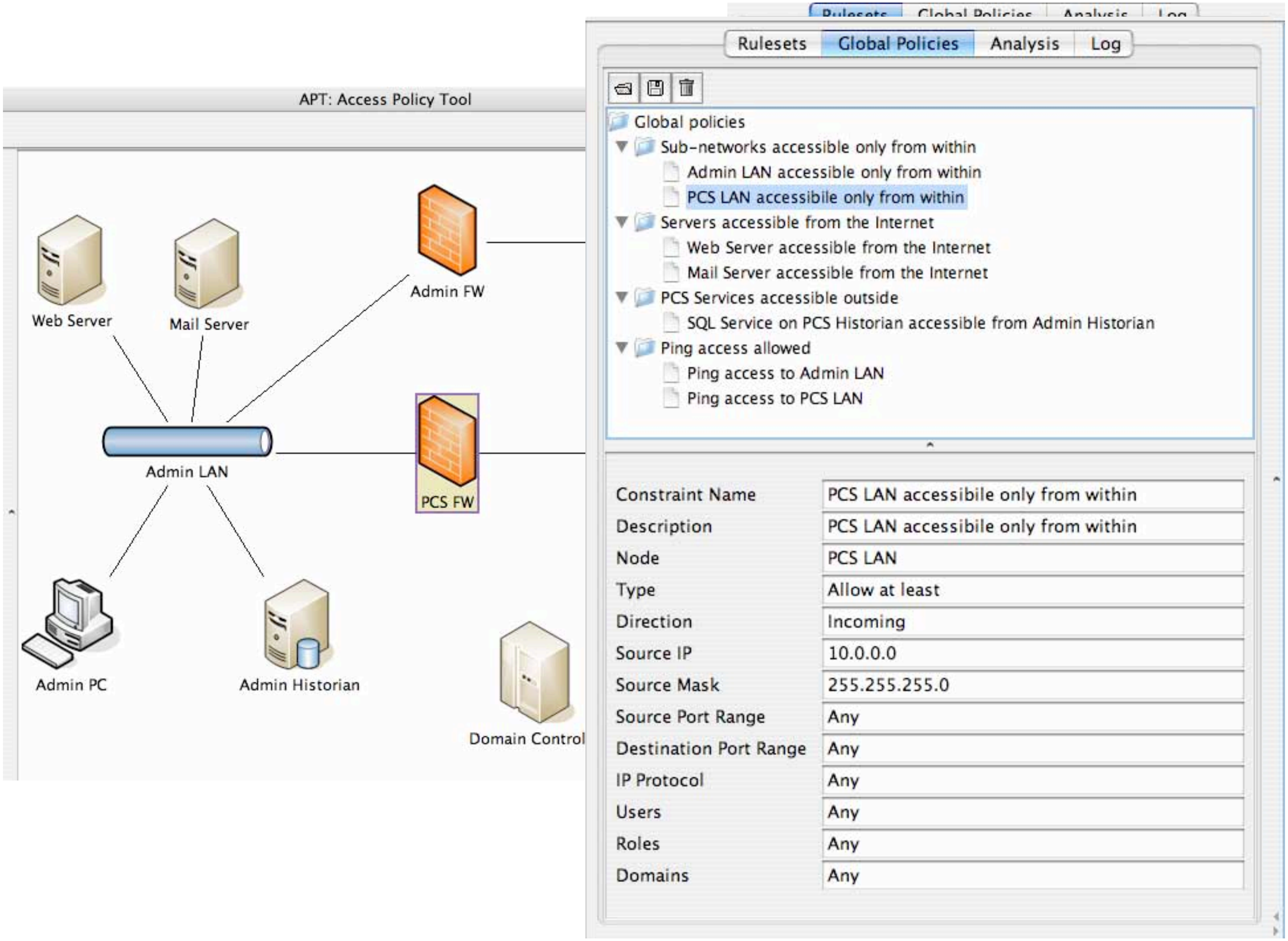
Network Access in Process Control Systems

- **Motivation** : Access security mechanisms try to enforce separation between Process Control Network and the rest of the system
- Addressed by our Access Policy Tool (APT)



- **APT ensures that global access constraints are reflected in configuration**
- **Configuration may permit security holes. APT provides**
  - **extensive design time analysis**
  - **online monitor, alert for security management system**

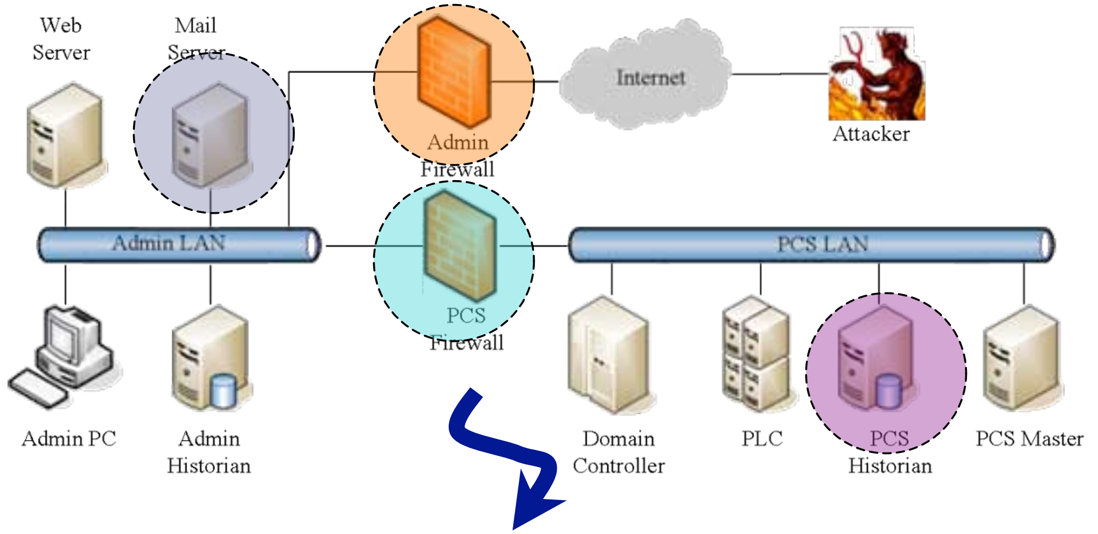
Illustrative Example



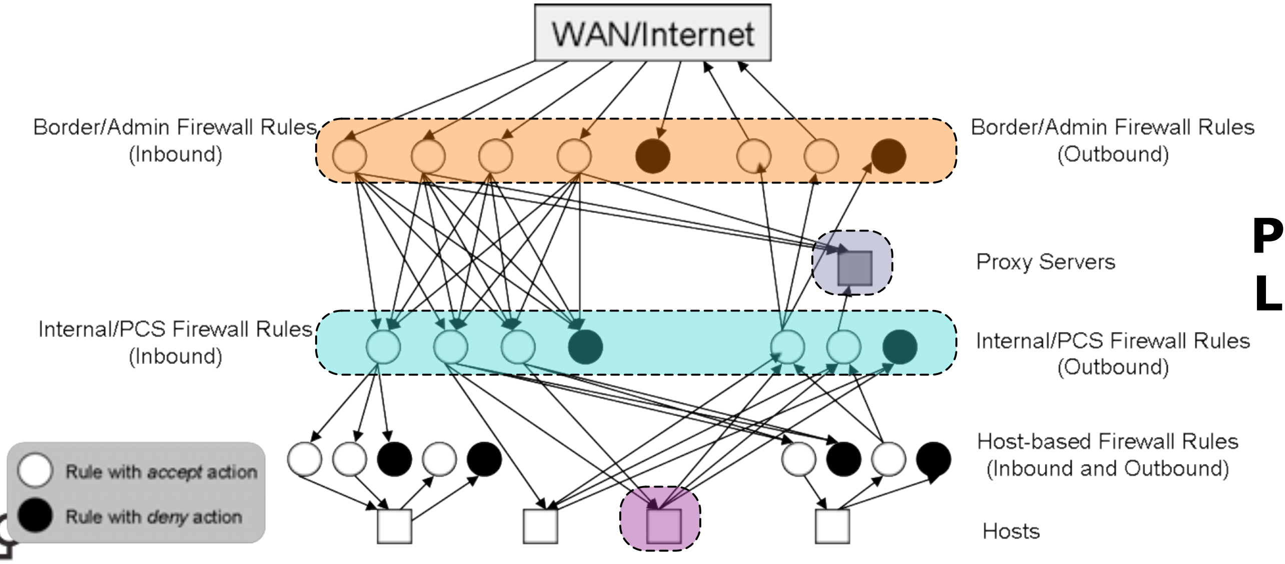
- Global policies
  - Sub-networks accessible only from within
    - Admin LAN accessible only from within
    - PCS LAN accessibile only from within
  - Servers accessible from the Internet
    - Web Server accessible from the Internet
    - Mail Server accessible from the Internet
  - PCS Services accessible outside
    - SQL Service on PCS Historian accessible from Admin Historian
  - Ping access allowed
    - Ping access to Admin LAN
    - Ping access to PCS LAN

Constraint Name	PCS LAN accessibile only from within
Description	PCS LAN accessible only from within
Node	PCS LAN
Type	Allow at least
Direction	Incoming
Source IP	10.0.0.0
Source Mask	255.255.255.0
Source Port Range	Any
Destination Port Range	Any
IP Protocol	Any
Users	Any
Roles	Any
Domains	Any

Rule Graph Construction/Analysis



Network Architecture


WAN/Internet
Border/Admin Firewall Rules (Inbound)
Border/Admin Firewall Rules (Outbound)
Proxy Servers
Internal/PCS Firewall Rules (Inbound)
Internal/PCS Firewall Rules (Outbound)
Host-based Firewall Rules (Inbound and Outbound)
Hosts
○ Rule with accept action
● Rule with deny action

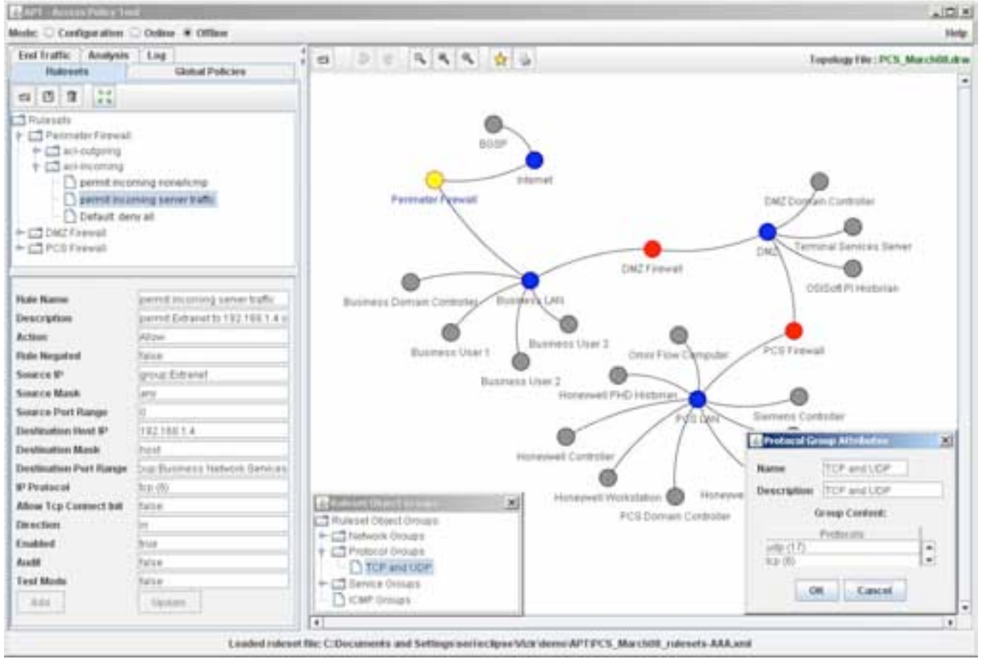
Possible Network Layer Rule Graph

Technology Transfer/Collaboration

- Currently in beta test. Partners include Ameren, Alyeska Pipeline, Sandia.
- PCS Vendors: system design aid.
- PCS System Operators: to pinpoint problems with global access compliance and augment on-line security monitoring by identifying policy holes during operational use. APT:
  - Allows to reason at high-level about global access policy.
  - Check the implementation (configuration of security devices) against a specification of policy.
  - Ease of information management, highly automated and extensible, avoids misconfigurations in access policy implementation during design as well as operational use.
  - Generate complete network connectivity map

Summary Slide: Access Control Policies and Their Impact on Survivability

- **Outcomes:** APT analyzes security policy implementation for conformance with global security policy specification
- **Roadmap Challenges:** Measure and Assess Security Posture, Develop and Integrate Protective Measures
- **Approach:** 1) Integrates policy rules (configuration information); 2) Comprehensive offline analysis; 3) dynamic, on-line, analysis
- **Progress/accomplishments:** Theory developed, prototype tool implemented, test cases developed, beginning beta test



Rule Name: permit incoming server traffic
Description: permit Extranet to 192.168.1.4 s
Action: Allow
Rule Negated: false
Source IP: group: Extranet
Source Mask: any
Source Port Range: 0
Destination Host IP: 192.168.1.4
Destination Mask: host
Destination Port Range: tcp Business Network Services
IP Protocol: tcp (6)
Allow Tcp Connect bit: false
Direction: in
Enabled: true
Audit: false
Test Mode: false

Name: TCP and UDP
Description: TCP and UDP

Loaded ruleset file: C:\Documents and Settings\...\eclipse\Viz\demo\APT\PCS_March08_rulesets-AAA.xml

- **Funders: DHS I3P Control System Security Project; NSF/DHS/DOE TCIP Center**
- **Performer: Univ. of Illinois**
- **Partners: Ameren, Alyeska Pipeline, Sandia, others**