Access Policy Tool (APT): Verification of Security Policy Implementation*

David M. Nicol, William H. Sanders, Sankalp Singh, and Mouna Seri
University of Illinois at Urbana-Champaign

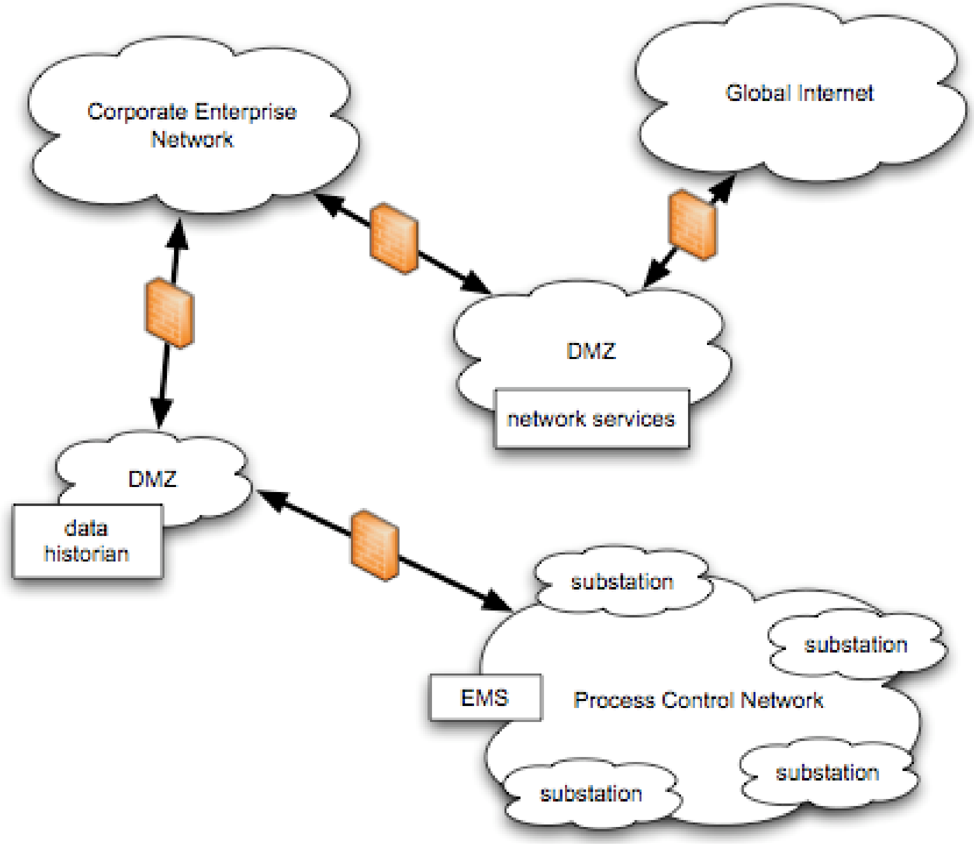
Feb. 2009

***supported by the I3P, through funding from DHS**

I3P
Institute for Information Infrastructure Protection

Problem

Process Control networks are connected in enterprise systems



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

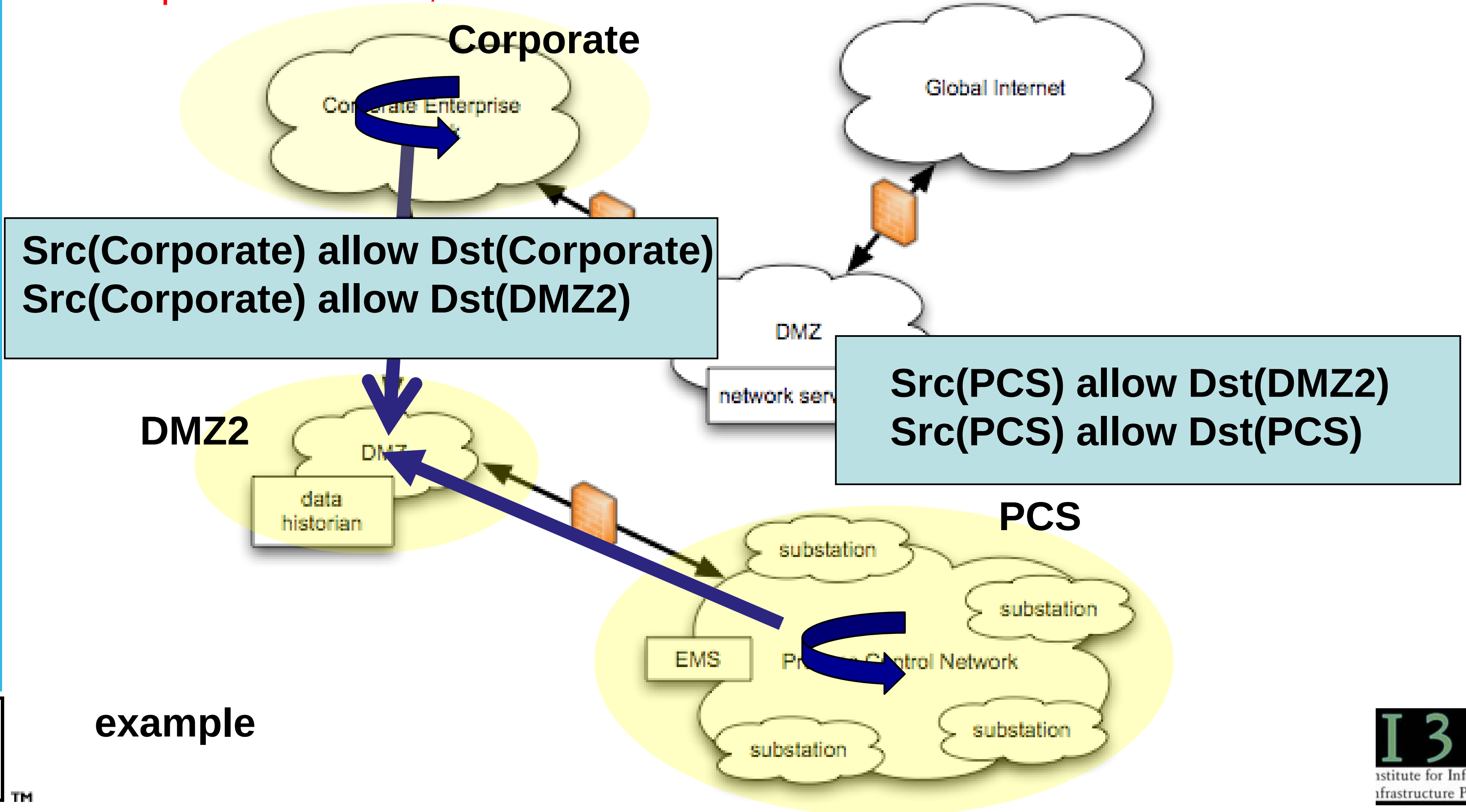
How can one express Best Practices as Global Access Policy in machine checkable form?

How can one detect violations of Global Access Policy?

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**.**



Src(Corporate) allow Dst(Corporate)
Src(Corporate) allow Dst(DMZ2)

Src(PCS) allow Dst(DMZ2)
Src(PCS) allow Dst(PCS)

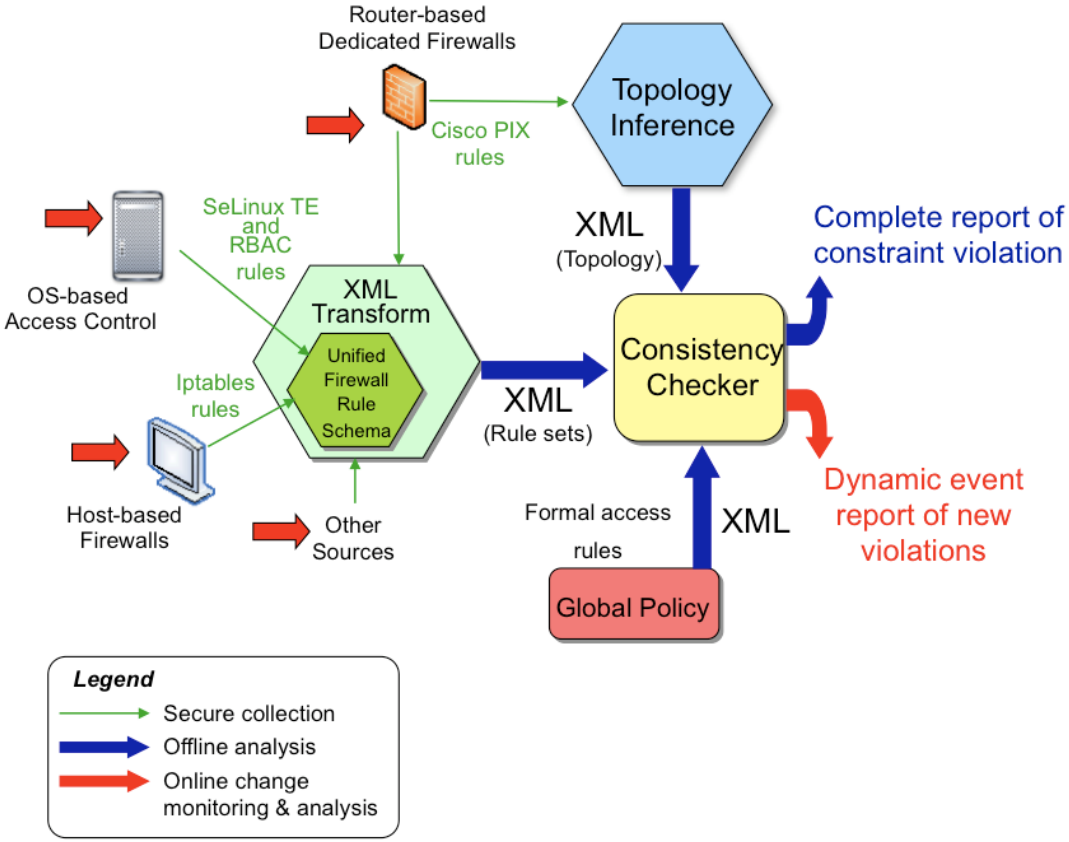
example

History

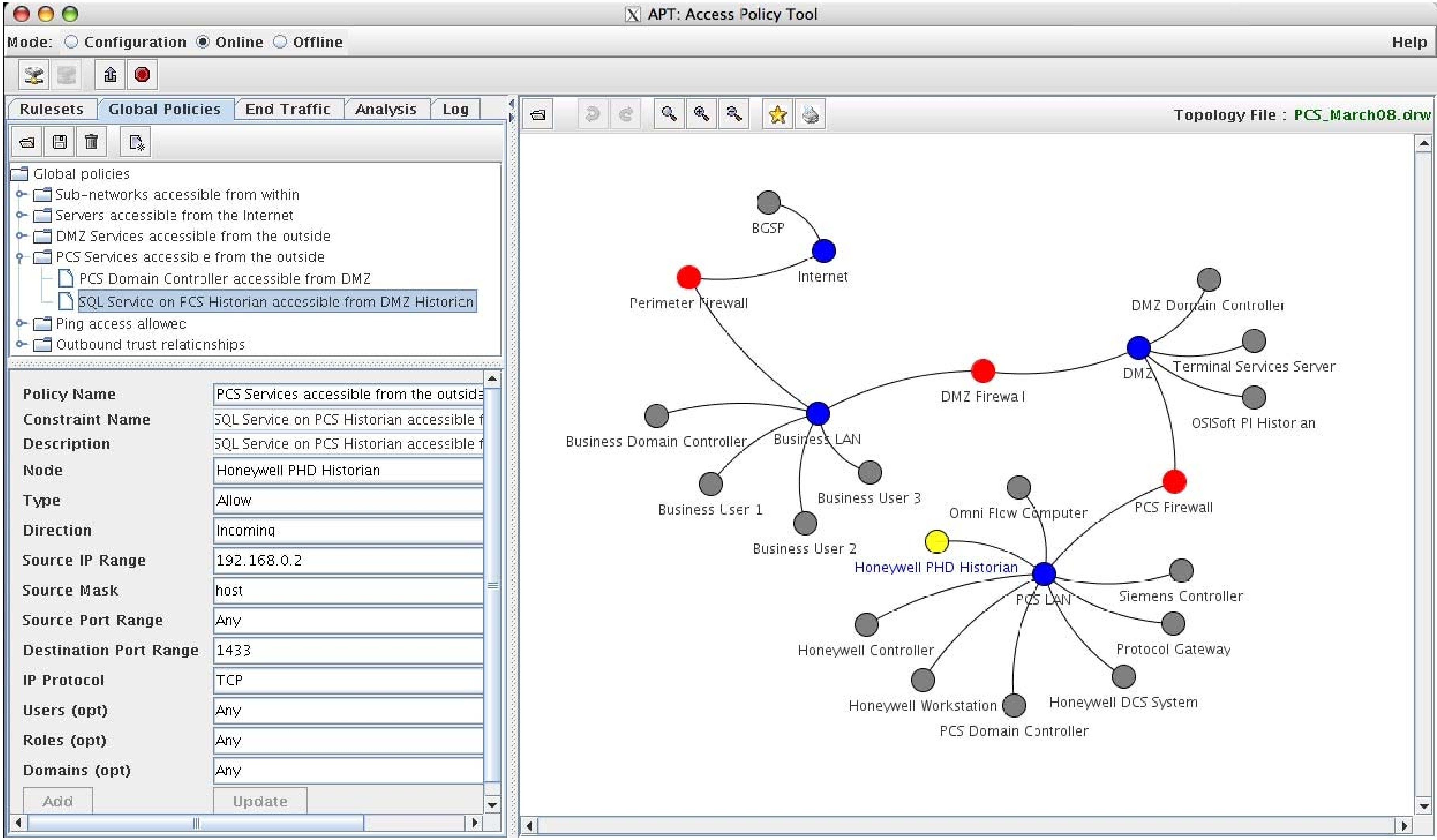
The Access Policy Tool (APT) developed under I3P support

- Started with focus on compliance checking
- Transitioning to industry…hence best practices question
- Some overlap with commercial products (Skybox, RedSeal)
  - APT adds value in scalability, integration of host policies

APT Architecture



APT - Prototype



APT: Access Policy Tool

Mode: ○ Configuration ● Online ○ Offline

Help

Rulesets | Global Policies | End Traffic | Analysis | Log

- Global policies
  - Sub-networks accessible from within
  - Servers accessible from the Internet
  - DMZ Services accessible from the outside
  - PCS Services accessible from the outside
    - PCS Domain Controller accessible from DMZ
    - SQL Service on PCS Historian accessible from DMZ Historian
  - Ping access allowed
  - Outbound trust relationships

Policy Name	PCS Services accessible from the outside
Constraint Name	SQL Service on PCS Historian accessible f
Description	SQL Service on PCS Historian accessible f
Node	Honeywell PHD Historian
Type	Allow
Direction	Incoming
Source IP Range	192.168.0.2
Source Mask	host
Source Port Range	Any
Destination Port Range	1433
IP Protocol	TCP
Users (opt)	Any
Roles (opt)	Any
Domains (opt)	Any

Add Update

Topology File : PCS_March08.drw

Interactions with Industrial Partners

APT as an “every night” checker **#1**

- Over 70 firewalls
- Drivers for authenticated traffic, connectivity map, network discovery, inclusion of multi-homed NATed subnets, scriptable

We’ve done analysis of a subset of actual rule-sets

- Network discovery and connectivity map---validated
- Inferred implicit global policy---validated

In progress : testing with full rule set

Much smaller number of firewalls **#2**

- Firewalls guard gateways between separated network islands
- Topology discovery from rule-sets requires deep analysis of all implicit connectivity information
- Global policy rules in formulation

Summary

APT helps to address the problem of verifying that PCS systems adhere to global policy encoding best practices

In transition for use by two major energy companies

- real installation helps drive development details

Has created solid research problems

Licensing available June 2009