Information Trust INSTITUTE

Integrated Analysis of Host-based and Network-based Access Control Policies in a Critical Infrastructure Control System

David M. Nicol
ECE, CSL, & ITI
University of Illinois, Urbana-Champaign

January 2007

Other contributors are Bill Sanders, Sankalp Singh, and Hamed Okhravi

Integrated Access Policies

Systems impose access policies at the network level, and at the host level

E.g.,

- Firewalls (at network borders and in hosts themselves)
- SeLinux policies (role-based access, domain-oriented access)

Question : If high level “global policy” specifies requirements and prohibitions w.r.t. actors within a network, does the system of rules governing access faithfully implement it?

i.e., is the system misconfigured? If so, where?

Network Access in PCS 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)

🟦 Remote access to DMZ host

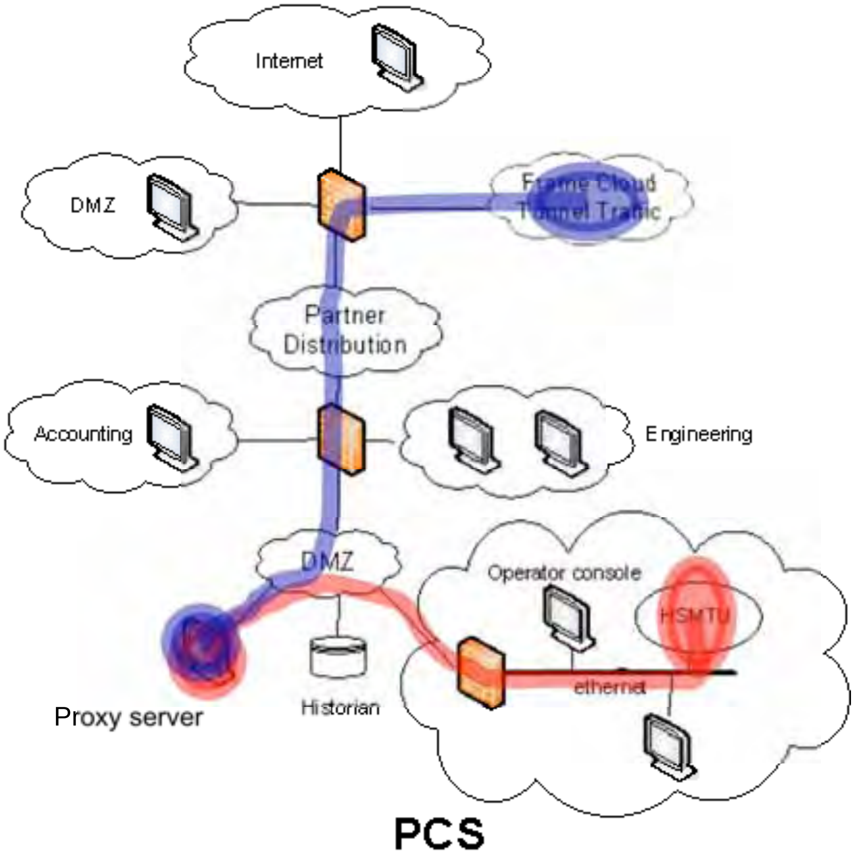
🟥 VNC access allowed from DMZ

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 information management system



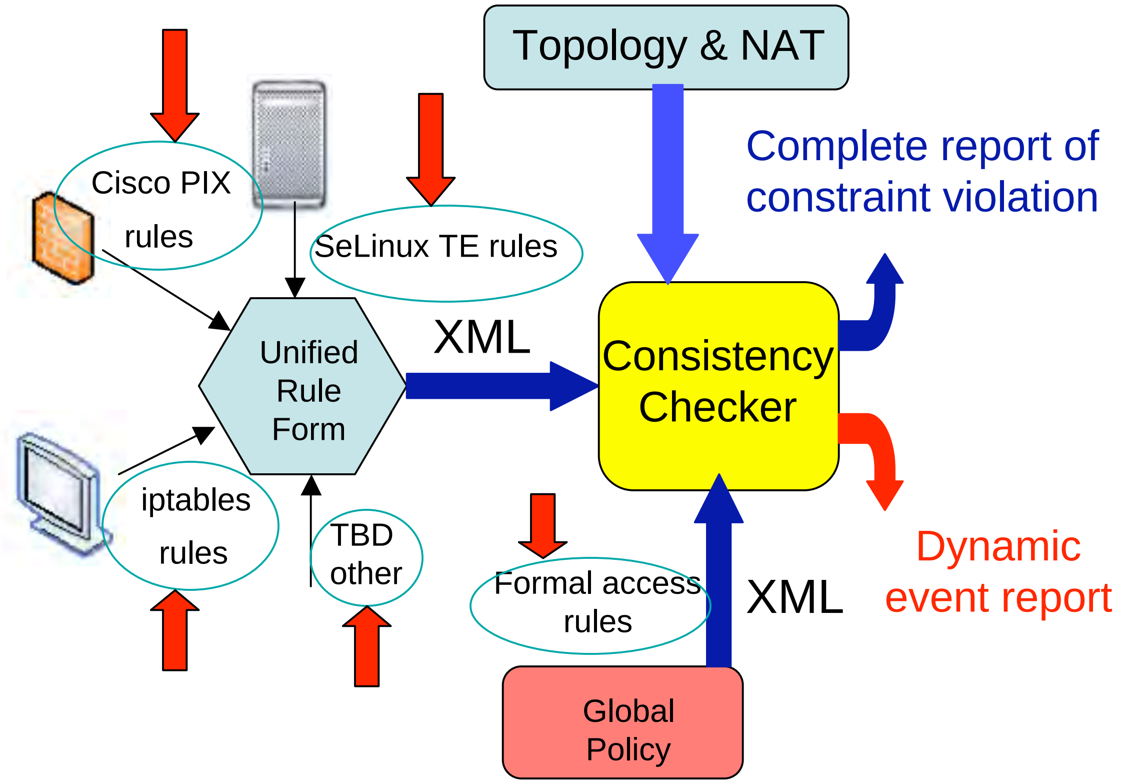
Firewall Rules

- 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

Global Access Policy

- Global Access Policy (GAP)is composed of statements about sources being able to reach (or not) destinations
  - Sets of sources and destinations used in statement
    - e.g. “No host outside the PCS may communicate with any host inside the PCS using tftp”
- A GAP statement is a logical expression of a set of statements, each specifying a particular source and particular destination
- Given a particular <source,destination,protocol> triple that admits access (or not), we can in principle check compliance with GAP

APT Operation Overview



Topology & NAT

Cisco PIX rules

SeLinux TE rules

Unified Rule Form

XML

Consistency Checker

Complete report of constraint violation

iptables rules

TBD other

Formal access rules

XML

Dynamic event report

Global Policy

Secure collection

Offline analysis

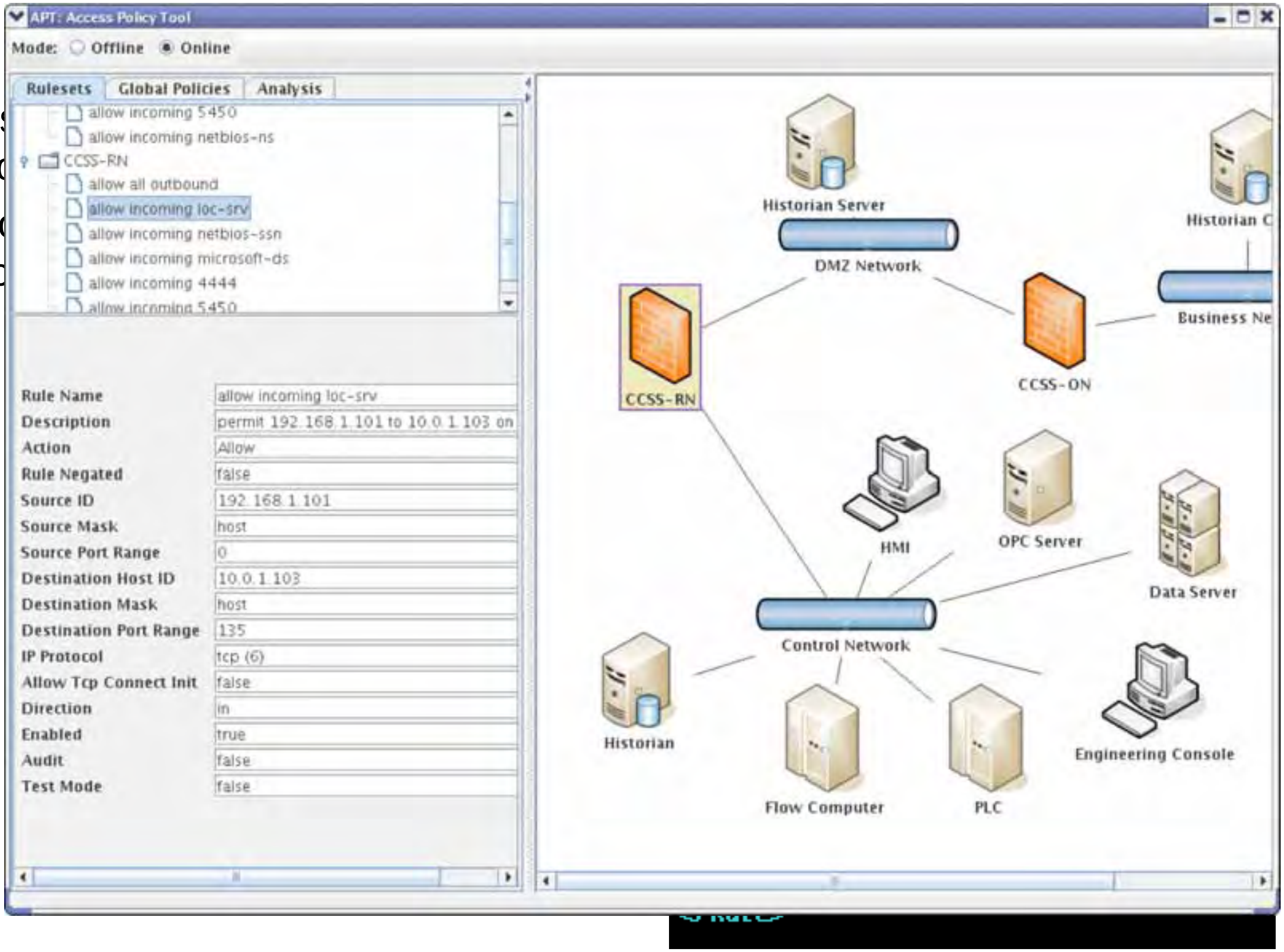
Online change monitoring & analysis

Sticky but solved (or solvable) problems

- NAT, proxies, tunnels
- Stateful connections

Access Rules in APT

- Us ho
- Co sc



APT: Access Policy Tool

Mode: ○ Offline ● Online

Rulesets | Global Policies | Analysis

- allow incoming 5450
- allow incoming netbios-ns
- CCSS-RN
  - allow all outbound
  - allow incoming loc-srv
  - allow incoming netbios-ssn
  - allow incoming microsoft-ds
  - allow incoming 4444
  - allow incoming 5450

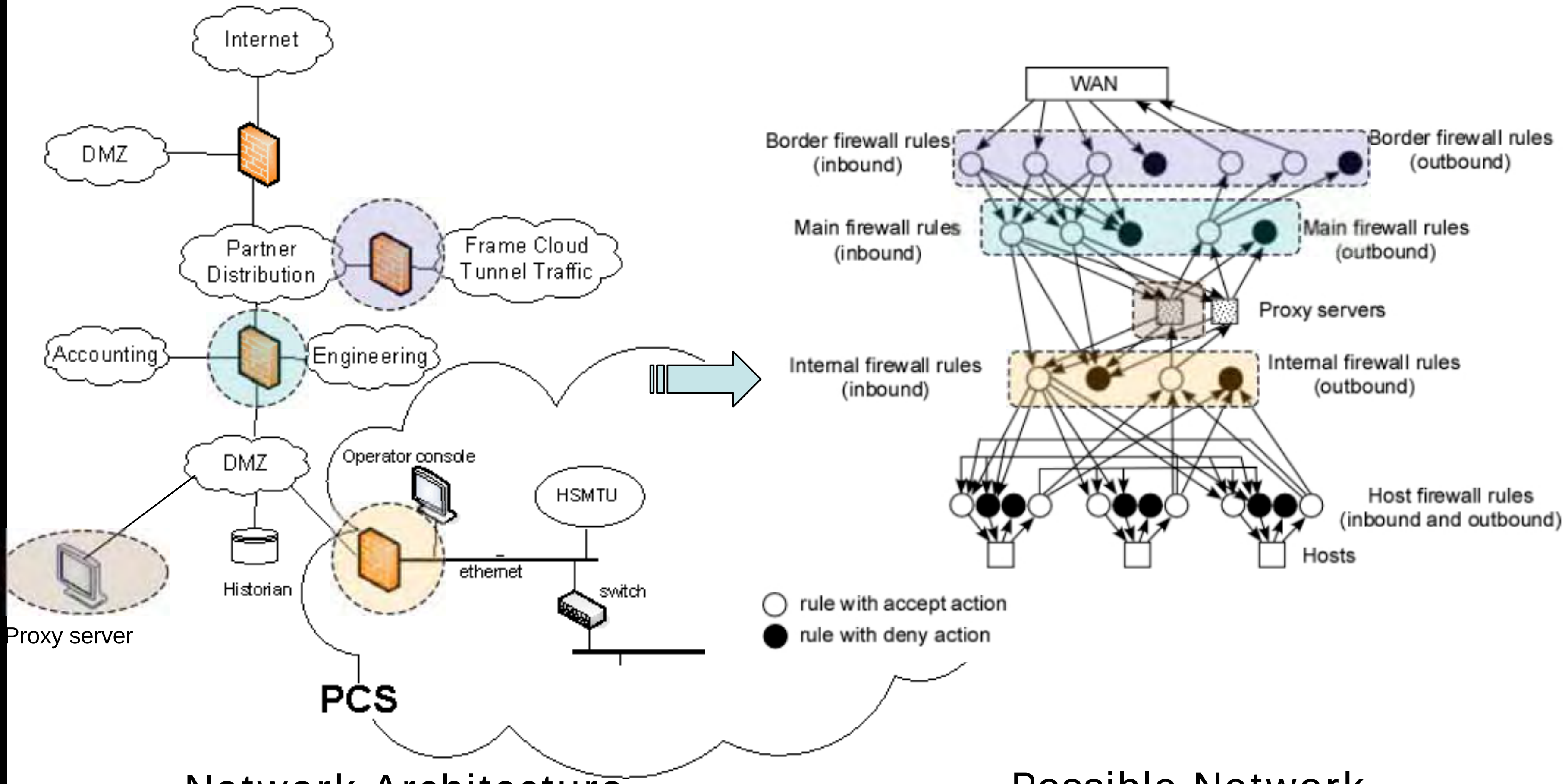
Rule Name	allow incoming loc-srv
Description	permit 192.168.1.101 to 10.0.1.103 on
Action	Allow
Rule Negated	false
Source ID	192.168.1.101
Source Mask	host
Source Port Range	0
Destination Host ID	10.0.1.103
Destination Mask	host
Destination Port Range	135
IP Protocol	tcp (6)
Allow Tcp Connect Init	false
Direction	in
Enabled	true
Audit	false
Test Mode	false

APT Analysis Overview

- Construct "*rule graph*," using as input:
  - Network topology
  - Configuration rule-sets
- Rule graph represents network interconnectivity and data flow among policy enforcement rules
- Rule graph analyzed for global access violations
  - Exhaustive analysis (easily parallelizable)
    - Polynomial complexity, exponent related to path length
  - Statistical analysis (importance sampling)
    - Significant research issues being explored

ITI

Rule Graph Construction

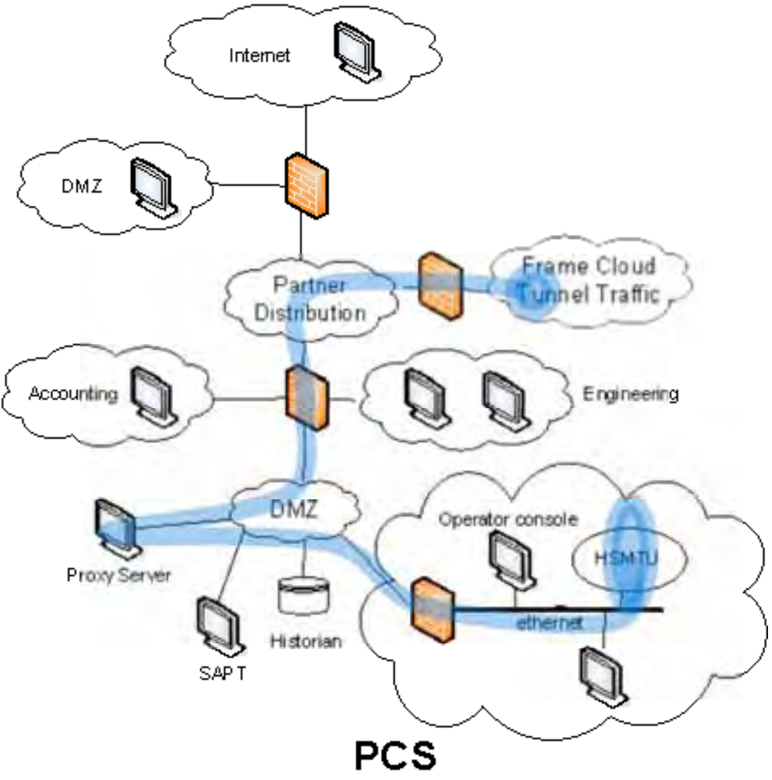

Internet
DMZ
Partner Distribution
Frame Cloud Tunnel Traffic
Accounting
Engineering
DMZ
Operator console
HSMTU
Historian
ethernet
switch
Proxy server
PCS
WAN
Border firewall rules (inbound)
Border firewall rules (outbound)
Main firewall rules (inbound)
Main firewall rules (outbound)
Proxy servers
Internal firewall rules (inbound)
Internal firewall rules (outbound)
Host firewall rules (inbound and outbound)
Hosts
○ rule with accept action
● rule with deny action

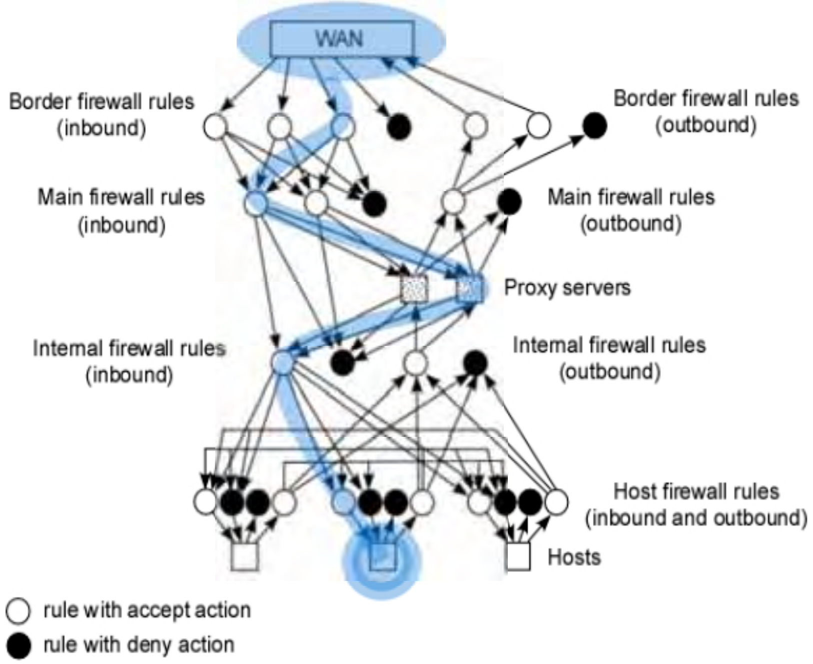
Network Architecture

Possible Network Layer Rule Graph

Rule Graph Analysis

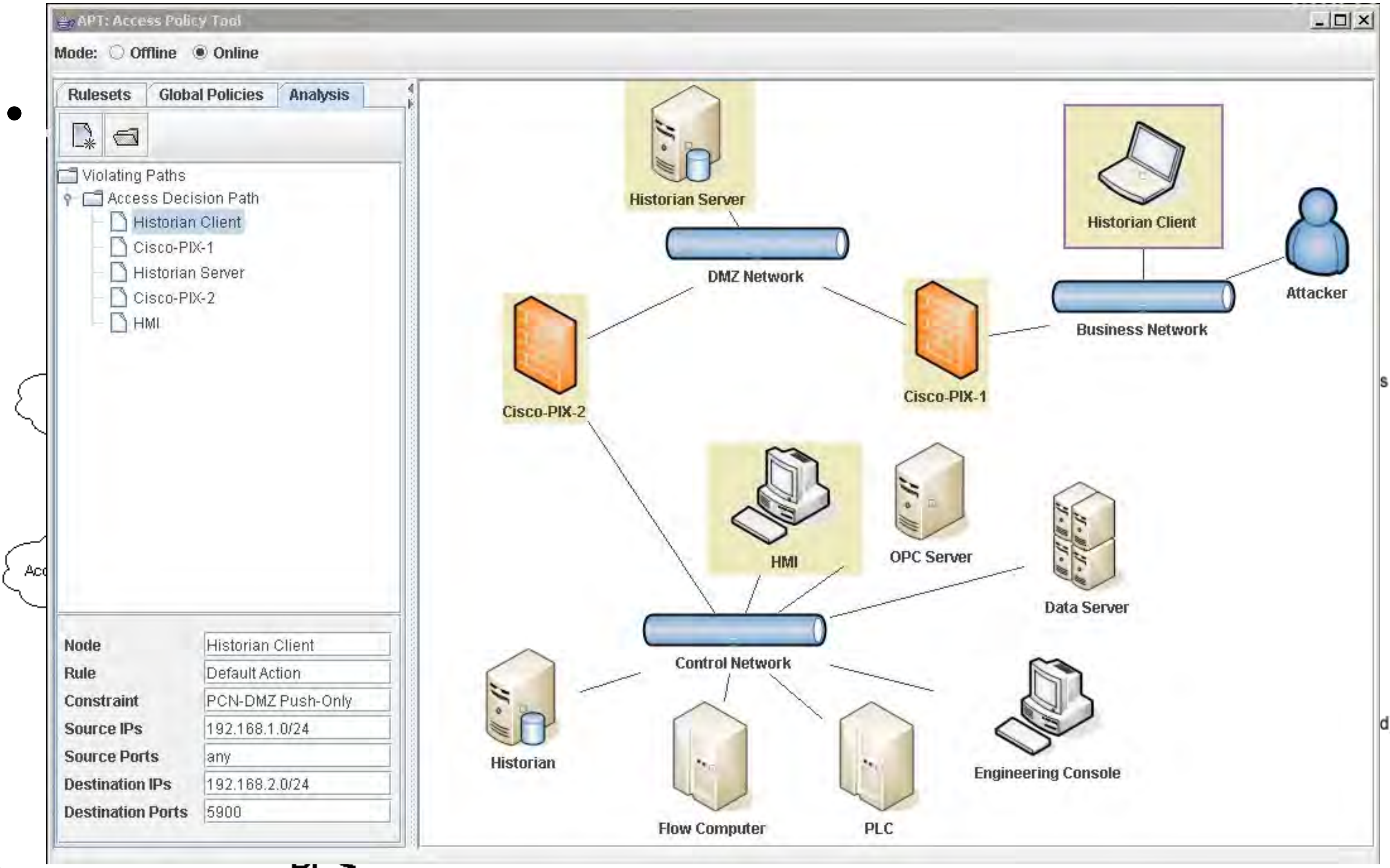
- For each path through Rule Graph, determine whether path attribute set violates any global access constraints
  - Analysis based on computation of multi-dimensional intersections
  - Sets of traffic attributes are “pushed” along paths




WAN
Border firewall rules (inbound)
Border firewall rules (outbound)
Main firewall rules (inbound)
Main firewall rules (outbound)
Proxy servers
Internal firewall rules (inbound)
Internal firewall rules (outbound)
Host firewall rules (inbound and outbound)
Hosts
○ rule with accept action
● rule with deny action

Full computation yields all attributes reaching all hosts

Rule Graph Analysis



APT: Access Policy Tool

Mode: ○ Offline ● Online

- Violating Paths
  - Access Decision Path
    - Historian Client
    - Cisco-PIX-1
    - Historian Server
    - Cisco-PIX-2
    - HMI

Node	Historian Client
Rule	Default Action
Constraint	PCN-DMZ Push-Only
Source IPs	192.168.1.0/24
Source Ports	any
Destination IPs	192.168.2.0/24
Destination Ports	5900

Acc

s

d)

PCS

Host-based Policies

- SeLinux developed by NSA
  - Adds a variety of security mechanisms to Linux
  - All requests of kernel viewed through the lens of access policy
- Type Enforcement
  - Subjects with a specified “type” can access objects of the same type
    - Dynamic type transitions are possible
- Role-based Access Control
  - A subject with a specified role can access specific objects
    - Roles may dominate each other
    - A subject’s role may transition
- SeLinux philosophy : “If not explicitly allowed, then prohibited”

Analysis of SeLinux Policy

- Analysis has no idea of what a subject may attempt to access, only what it is permitted to access
- One approach uses a state-machine
  - State is essentially vector of roles subjects have
    - Access to objects derivable from these
    - Transitions correspond to role changes or assertions of domination
  - Question “Can subject S ever access object O” means trying to find a set of transitions in the FSM
- However, a “transitive closure” style analysis on all subjects and objects is useful for checking GAP compliance

Analysis of SeLinux Policy : State machine

Myla Archer, Elizabeth Leonard ,"Analyzing Security-Enhanced Linux Policy Specifications", IEEE POLICY'03, 2003

Myla Archer, Elizabeth Leonard , "Modeling Security-Enchanced Linux Policy Specifications for Analysis", IEEE DISCEX'03, 2003

One approach uses a state-machine

- State : All objects and their security context (type, user,role…)
- Initial state : when Linux boots up
- Transitions : Access control decisions (e.g. new objects, type or role transitions) and modifications of security context)

- Map high level objectives (e.g. 8 NSA goals) into state and transition invariants, e.g.

  <Protect integrity of kernel> to "If an action changes the content of an object /w security context c1, the action must have resulted from a successful request of a subject /w security context c2"

- Use model checking tool to evaluate such invariants

High level properties can be proven

- human effort needed to map high level objectives into invariants

Analysis of SeLinux Policy : Sets

Giorgio Zanin, Luigi Vincenzo Mancini, "Towards a formal model for security policies specification and validation in the selinux system", ACM Symposium on Access Control Models and Technologies, 2004

- Compute transitive closure of possible subject and object transitions
  - For each subject obtain a set of all objects for which it is possible (through some sequence of transitions) to gain access
  - Significant computational effort required
  - Once performed, access policy questions mesh with network access policy---

Observe :

- Ports are objects
- Processes that read from and write to ports may
  - Alter objects to which they have w-access
  - Copy objects to which they have r-access

Integrated Analysis

- Global Access Policy may now be stated in terms of subjects on hosts accessing objects on other hosts
- Subject A on host h may write to object O on host j if
  - There exist ports p1 on h and p2 on j, protocol P, with some subject B on j such that
    1. A has w-access to p1 and uses P
    2. (h,p1,P) can reach (j,p3,P)
    3. B has r-access to p3 and w-access to O
- Similar requirements for A on h to read O on j
- Sets analysis connects objects and ports
  - Defines possible attributes for intra-network sources
- APT analysis connects sources and destinations
- Combined analysis identifies cross-intranet access to objects

Status

- APT going operational in 2nd quarter 2007
- Metrics development
- Research in SeLinux integration ongoing
  - Efficient algorithms
  - Statistical analysis
  - metrics