

Best Practices in Firewall Configuration: Checking for Compliance

**David M. Nicol, William H. Sanders, Sankalp Singh,
and Mouna Seri**

University of Illinois at Urbana-Champaign

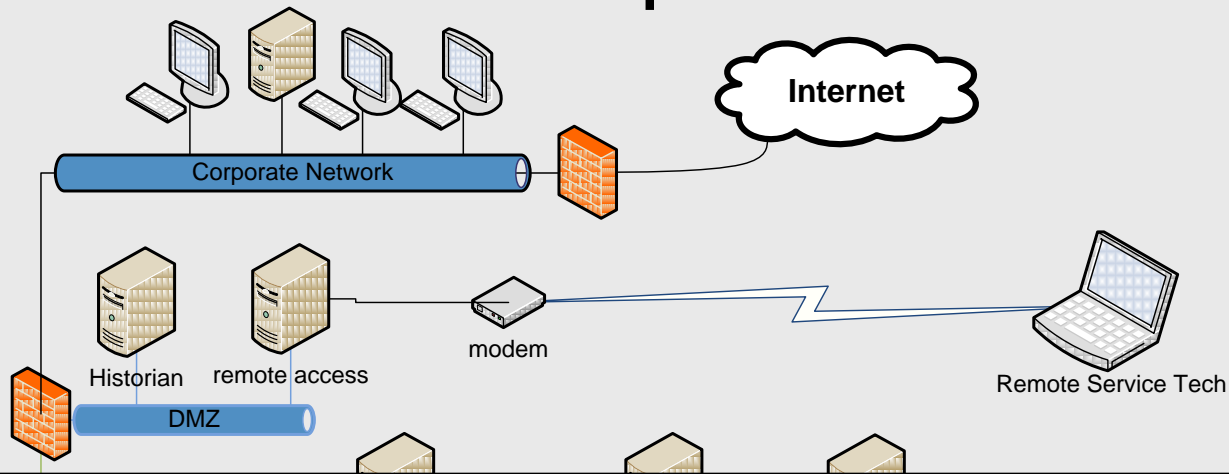
April 2009

Penetration of PCS

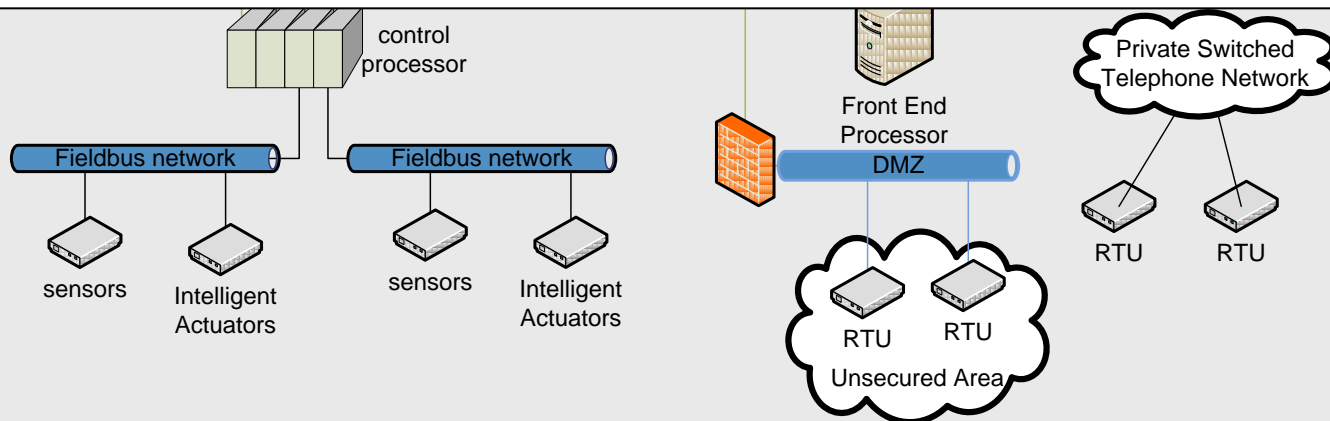
A PCS might be compromised in a variety of ways, e.g.

- infection through external media, e.g., USB drive
- a malicious insider
- access direct to PCS through modem, wireless
- access PCS through enterprise network
 - April 8, 2009 WSJ report on foreign penetration of power grid PCS's

PCS in Enterprise Networks



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



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

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?

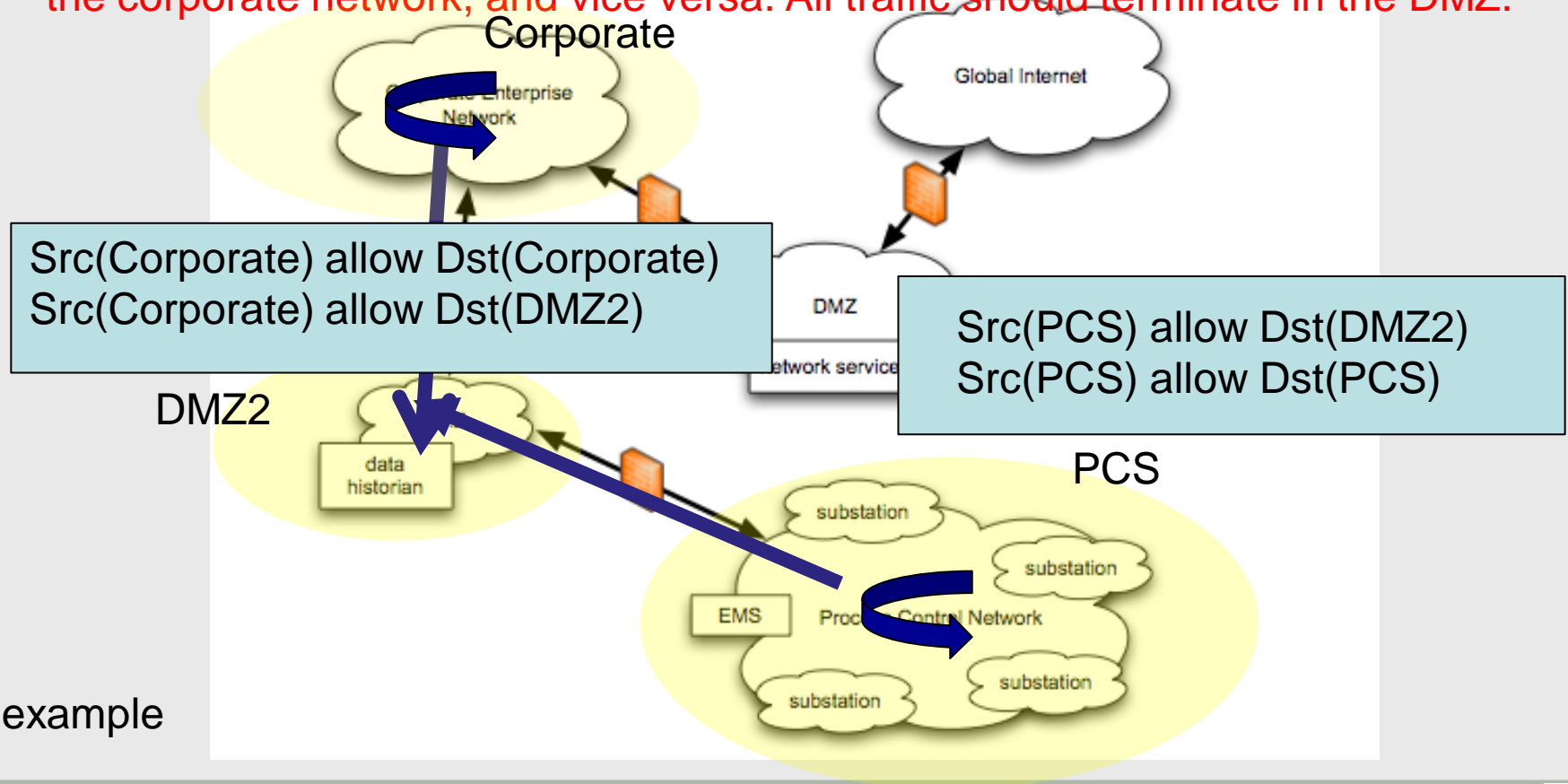
How can one demonstrate compliance with configuration standards?

Solution : Use the Access Policy Tool!

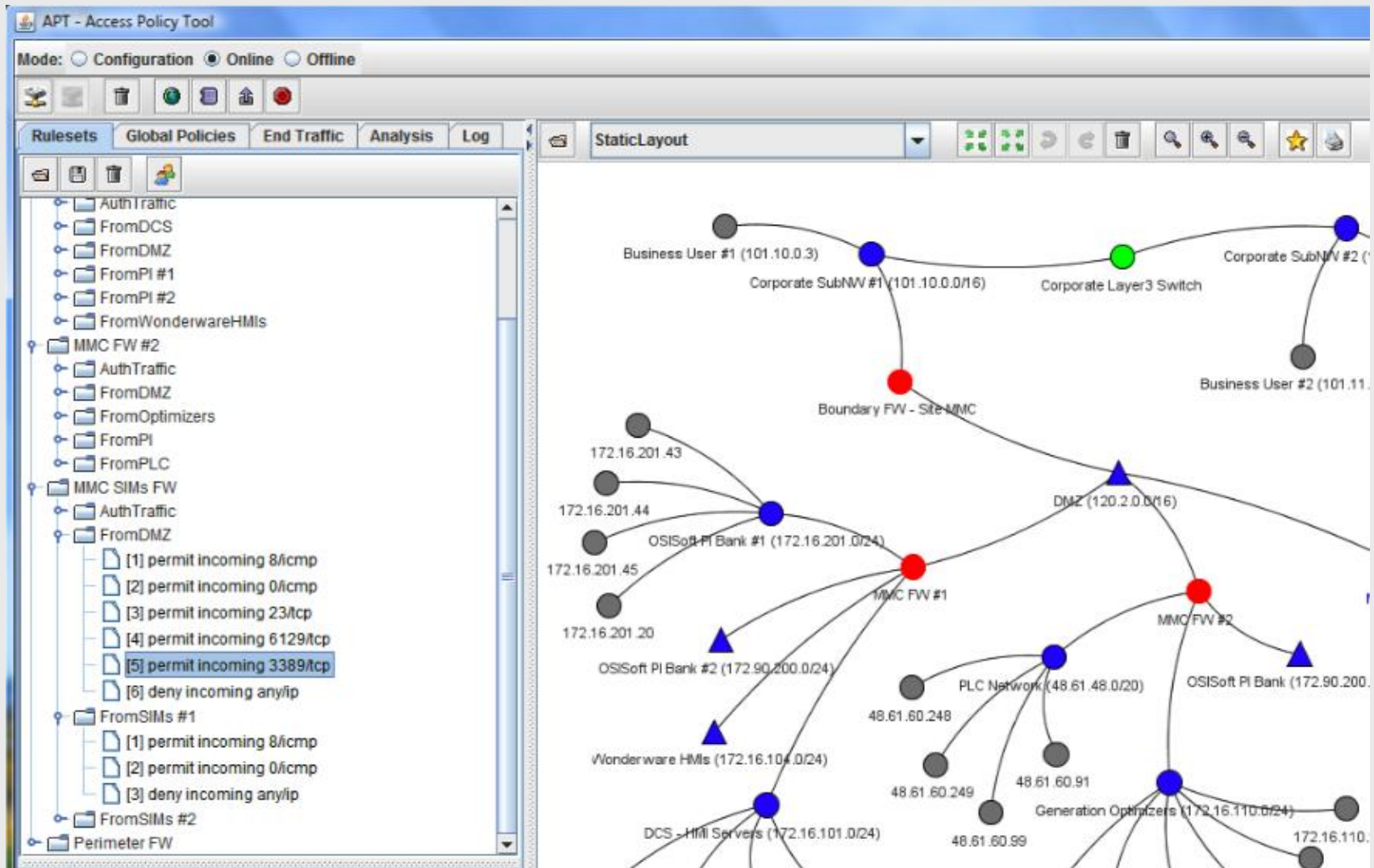
Global Policy

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.



APT - Prototype



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

Licensing available June 2009