

A Tool for Compliance and Depth of Defense Metrics



Cyber Security Division 2012 Principal Investigators' Meeting

11 October 2012

David M. Nicol

Franklin W. Woeltge Professor of Electrical and Computer Engineering

University of Illinois at Urbana-Champaign

dmnicol@illinois.edu

217 244 1925

Who We Are

TTA 2 : Enterprise-Level Security Metrics

David M. Nicol, Professor of ECE

William H. Sanders, Professor of ECE

Robin Berthier, Research Scientist

Mouna Bamba, Senior Programmer

Edmond Rogers, Security Analyst

Context

NERC Cyber Infrastructure Protection (CIP) requirements

- Includes requirements w.r.t. protection of “critical assets”
- Audit @ 3 year ; review @ year
- Compliance failure may induce large fines

Audit and preparation for audit very time-consuming

Automation extremely beneficial

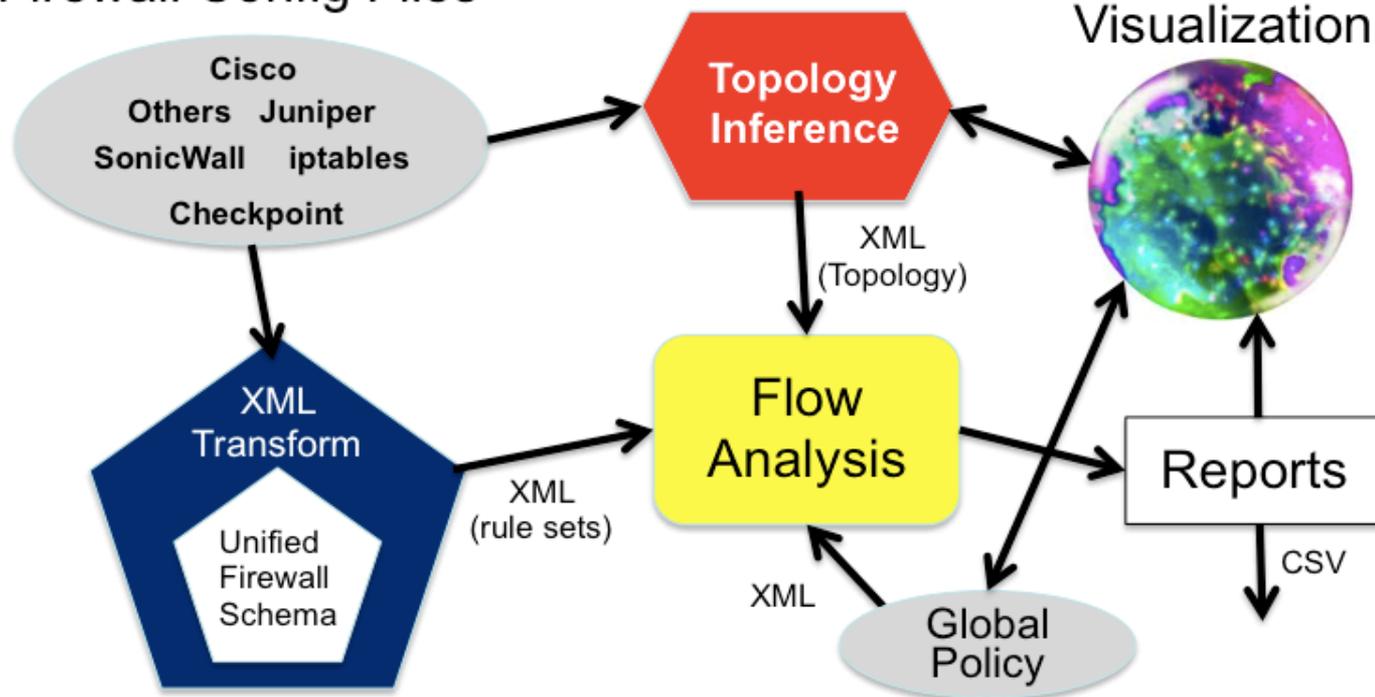
- Visualization
- Connectivity, open services analysis
- Compliance evaluation

Network Access Policy Toolset

NetAPT --- Firewallled network analysis

- Read firewall configurations, discover topology, identify permitted flows, identify violations with “Global Policy”

Firewall Config Files



Network Access Policy Toolset

NetAPT --- Firewallled network analysis

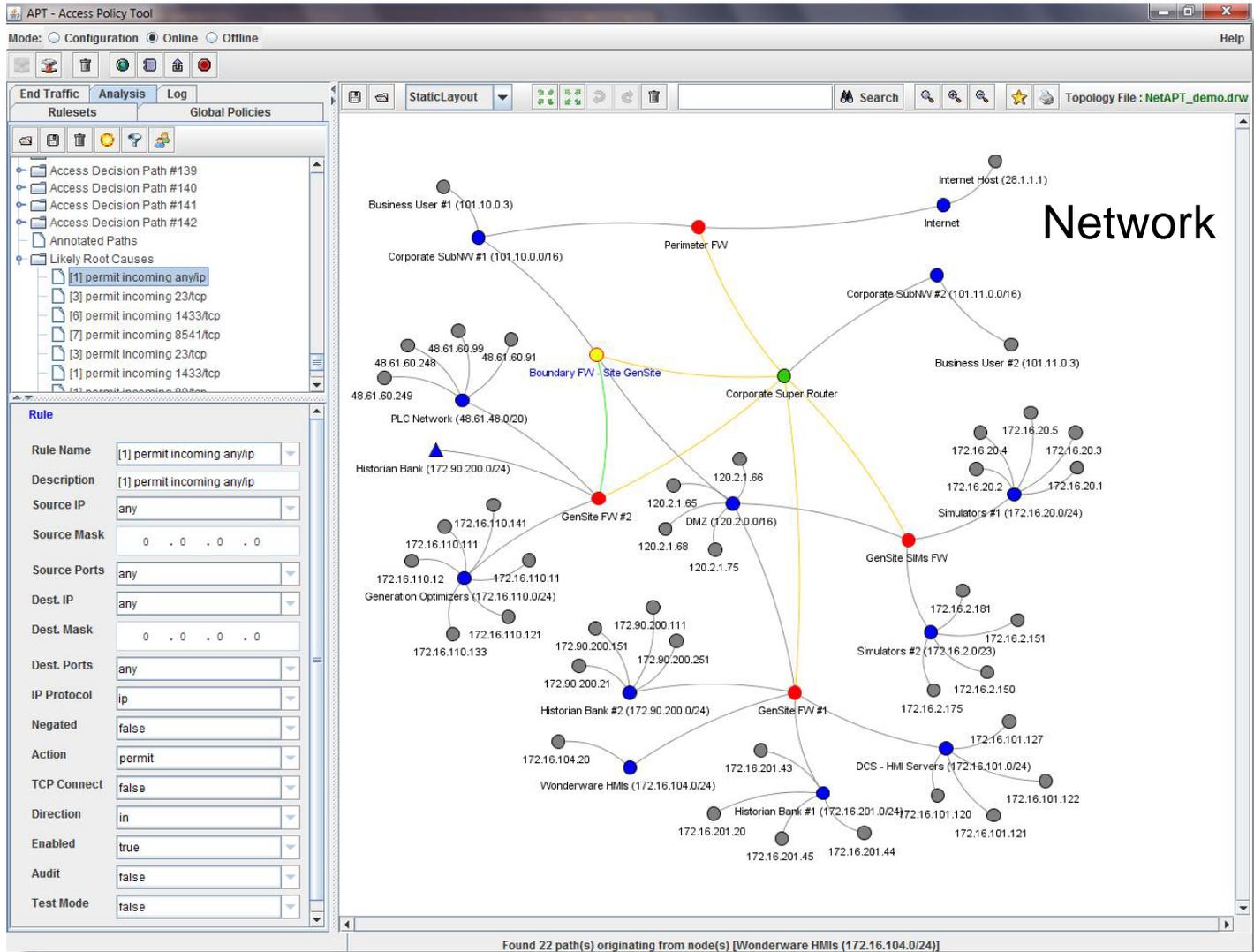
- Read firewall configurations, discover topology, identify permitted flows, identify violations with “Global Policy”

Mature technology developed through support of DHS & DOE

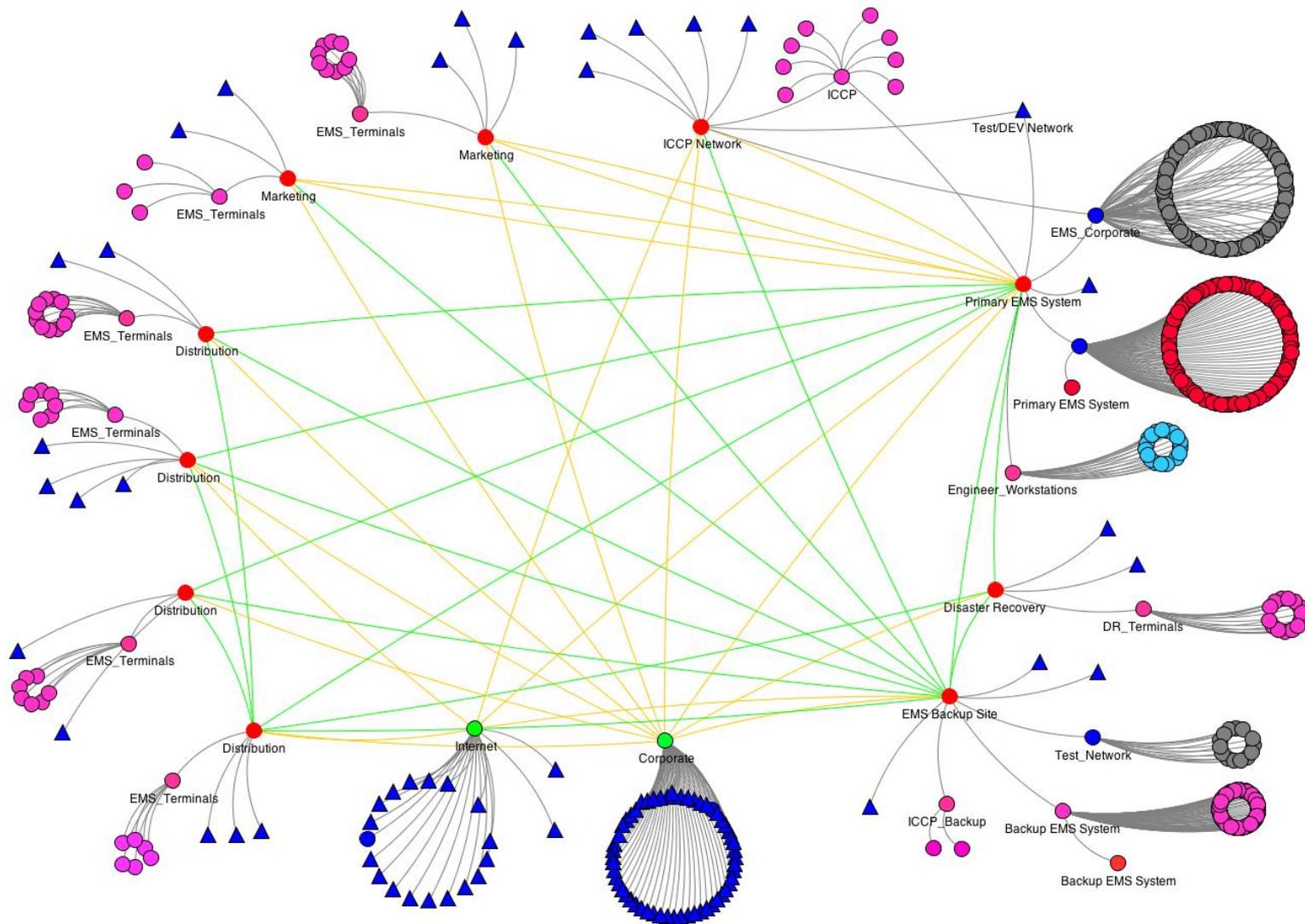
- Significant industrial influence : requirements and α -testing
 - Automated topology discovery
 - Templated search for problem rules
 - Templated global policy
 - Network visualization
 - Import/export support for reports and tracking

Screen shots : GUI

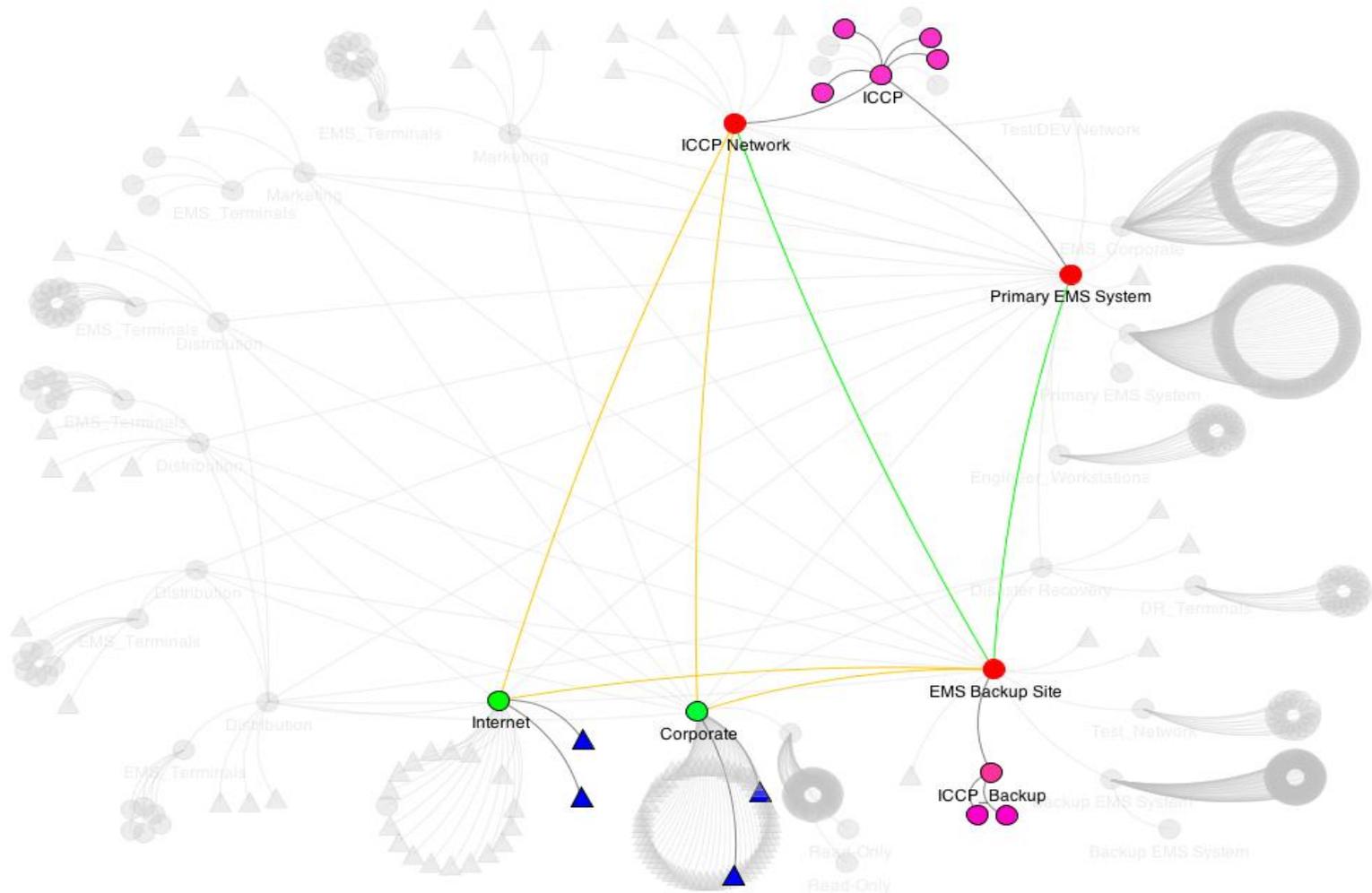
Data
Exploration



Screen Shots : Full EMS



Screen Shots : ICCP Traffic



Problem Statement

Prepare NetAPT for commercial deployment

- Transform advanced prototype code into industrial grade software
- Ensure tool can be used in ways that make sense to customers
 - Audits induce special circumstances
 - Large variation in customer size
- Augment tool with metrics that encourage use beyond audits

Solution Approach

Technical Component

- Optimize analysis algorithms and refactor code
 - Core code is 6 years old, built around Cisco view
- Integrate routing into flow analysis
 - current : “all possible pathways” assumption
- Develop / integrate metrics
 - NERC-CIP compliance measures
 - Measure impact on access to multiple penetrations

Solution Approach

Industrial Use and Evaluation Component

- Select core group of β -test users
 - Ideally auditors, and utilities being audited
 - They get all we have to offer free, in exchange for evaluation
 - Approximately 30 evaluation licenses out already
- Develop training materials
 - Documentation, short course, videos, case studies
- Educate on use beyond audit
 - e.g., daily compliance reports, training, assess impacts of network changes

Milestones, Deliverables, Schedule

Number	Name	Type	Version	Due
CDRL 001	Quarterly Status Report	Document	Final	14 working days after end of each quarter
CDRL 002	NetAPT release with enhanced metrics (1 st generation)	SW, Document	Draft	180 days
CDRL 003	NetAPT release with enhanced metrics (2 st generation) and layer two analysis capability added	SW, Document	Draft	270 days
CDRL 004	1 st Generation Training Materials	Document	Draft	90 days
CDRL 005	2 nd Generation Training Materials	Document	Final	360 days
CDRL 006	1 st generation refactored engine	SW, Document		180 days
CDRL 007	2 st generation refactored engine	SW, Document		360 days
CDRL 008	Project Review with Government, including demonstration of developed software	Meeting Presentations	Final	180 and 360 days
CDRL 009	NetAPT Final Release	SW	Final	365 days
CDRL 010	Final Report, including user's Manual	Document	Draft	365 days

Milestones, Deliverables, Schedule

Deliverables / Timeline

1st gen. document &
training materials

Nov.
2012

March
2013

Focus group selected
Test plan developed

Dec.
2012

NetAPT release
1st phase testing report
1st phase off-site analysis

June
2013

Sept.
2013

NetAPT release
2nd phase testing report

NetAPT release
3rd phase testing report

Tech Transition Plan

We're forming a company

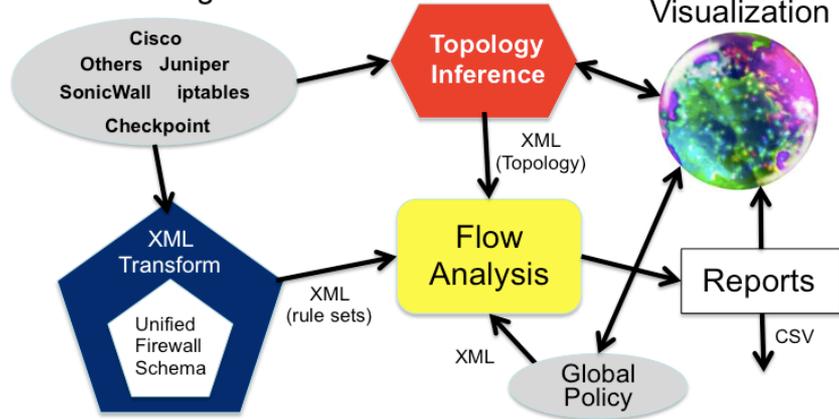
- Negotiating exclusive use license from Univ. of Illinois
- Awarded "iStart" grant for 1 year startup support
 - began 1 Oct.
- Aiming to incorporate within 4 weeks

We believe there is business **now** for us

- Especially in consulting, we use the tool

Quad Chart

Firewall Config Files



Operational Capability:

Performance Targets:

- Deepen compliance testing & accelerate audits
- Quantify Performance
- Complete flow analysis of system with 50 firewalls and 1000 hosts in under 24 hours.

Cost of Ownership

- Licensing terms are being studied

Meeting BAA Goals

- Delivers degree of compliance and defense-in-depth metrics at enterprise level
- Metrics provide practical decision aid for designing/modifying network architecture

Proposed Technical Approach

Will bring enterprise-scale network connectivity metrics into practice in a significant critical infrastructure

Tasks :

- * Develop training materials
- * Develop off-site NetAPT analysis capability
- * Develop/implement defense-in-depth metrics
- * Include layer-2 analysis

Status --- NetAPT in use under evaluation licenses.

Actions --- NetAPT used in NERC-CIP compliance testing of large electric utility

On-going --- small effort in bug fixes, documentation

Schedule, Cost, Deliverables, & Contact Info.

Deliverables

- NetAPT transitioned to commercial support
- Extensive training material
- Compliance and defense-in-depth metrics
- Vigorous promotion of use supporting NERC-CIP audits

Contact Information

Offeror : University of Illinois at Urbana-Champaign

POC : Professor David M. Nicol

Coordinated Science Lab

1308 West Main Street, Urbana, IL 61801

217 244-1925

dmnicol@illinois.edu