



Automating Network Security Assessment

Maj Doug Dexter, Cisco
Dr Mike Lloyd, RedSeal

What we will cover

- **Why Network Assessment is different**
 - From host assessment
 - From single network device compliance
- **Automation of Network Assessment**
- **Case study: Network Assessment at Cisco**
- **Implications for SCAP**

Why Network Security Assessment?

- **Overall objective: “Near-real time risk management”**
- **Determining risk (NIST 800-30)**
 - “likelihood of a given threat-source’s exercising a particular potential vulnerability”
 - “impact of that adverse event on the organization”
- **Network context is critical missing element**
 - Likelihood: Do network controls prevent exploitation of the vulnerability?
 - Organization impact: Do network controls compartmentalize the attack?
- **Problem: network controls are complex**
- **Approach: apply automated assessment**

Network assessment in SCAP context

Three levels to consider:

1. Host analysis

- “Classic” concepts of vulnerability, patching and remediation
- CVE; CVSS; CPE

2. Network devices are (slightly) different

- “Vulnerabilities” more often mis-configurations, not software defects
- Testing is specific (good for XCCDF, OVAL)
- Remediation is more involved

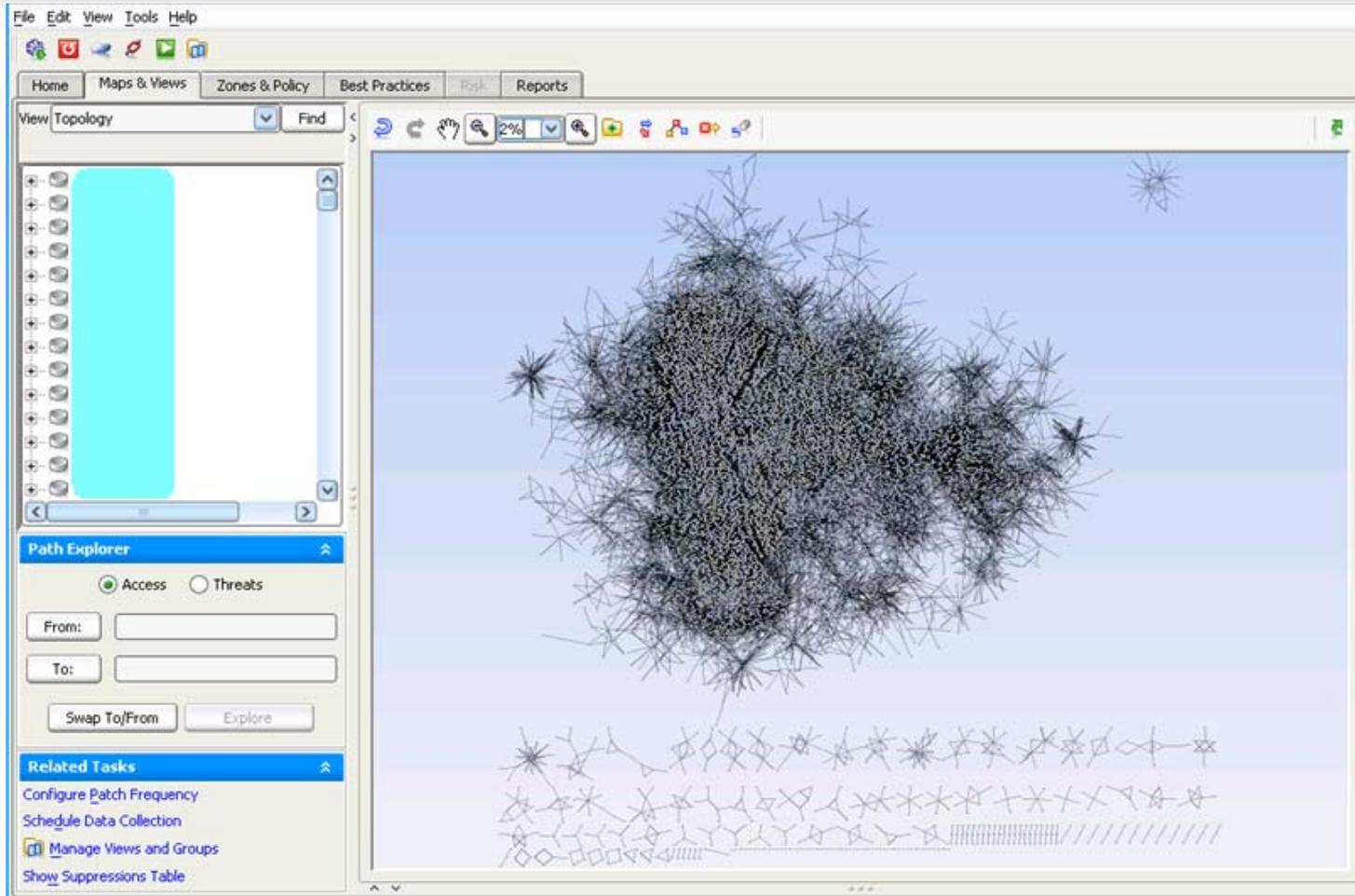
3. Whole network analysis is the next level

- You can’t detect a route around the firewall by reading the firewall
- Requires systemic understanding—not just individual devices
- This is an extraordinarily complex problem

Cisco's "Project Atlas"

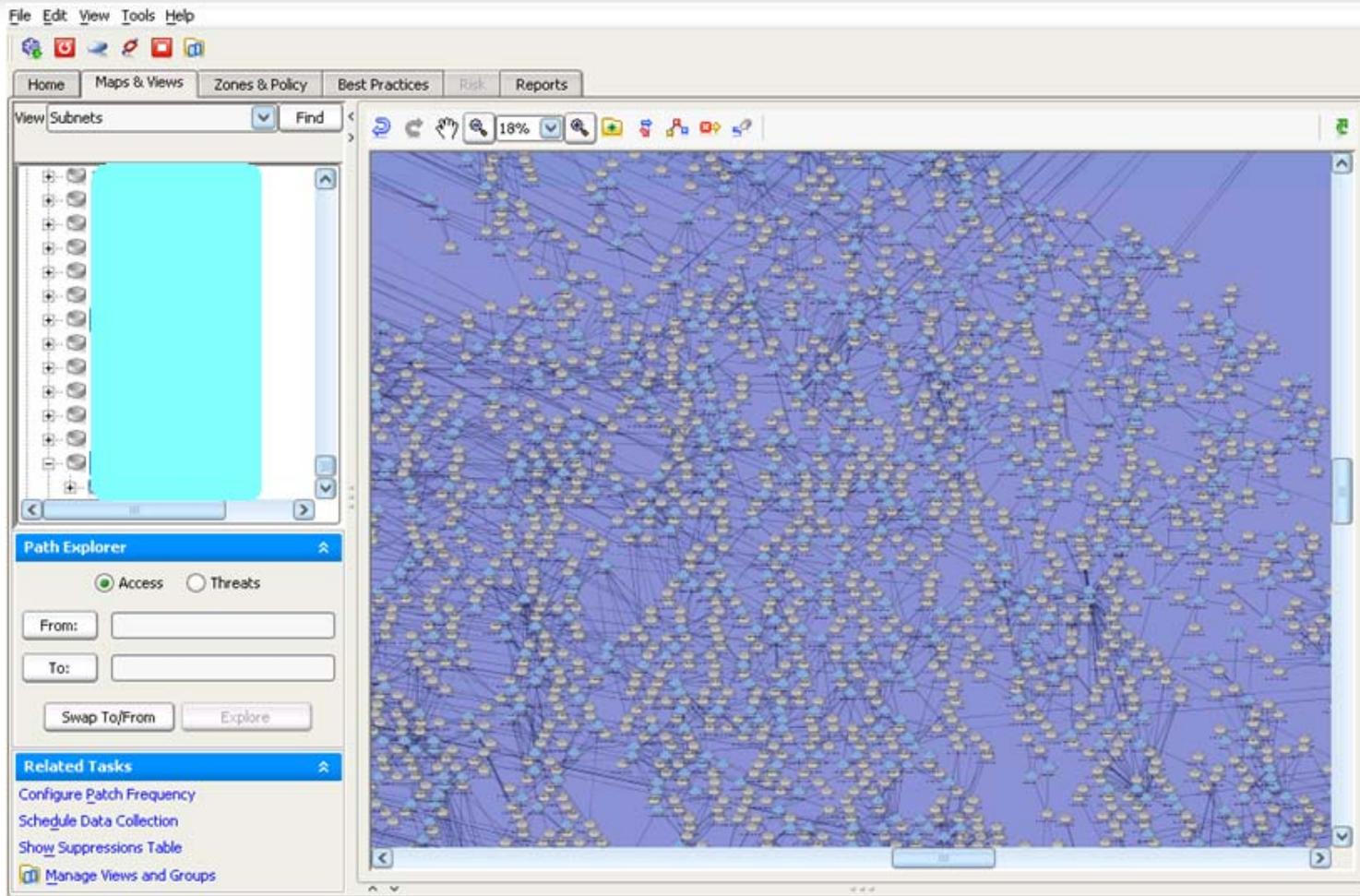
- **Objective:**
 - Map the global Cisco environment
 - Review major site interconnections
 - Audit access to sensitive locations
- **Resources:**
 - Installed RedSeal software
 - ~\$5K server (quad core, 32G RAM)
 - Two weeks
 - 27,000 configuration files
 - One RedSeal employee, part time
 - Initially a "science project"
 - Now delivering operational payoff

Raw Network

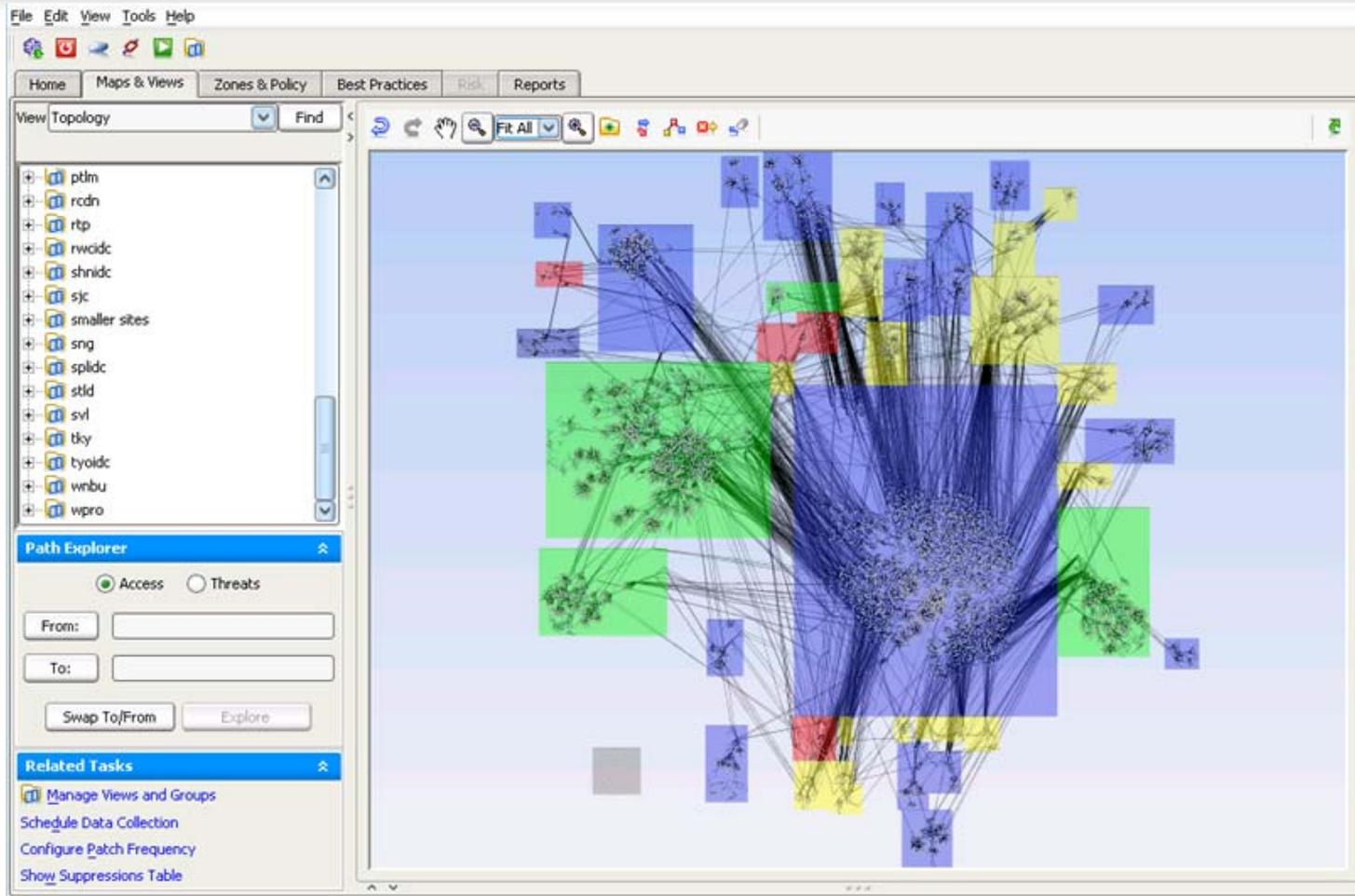


- Note visual clue – some devices are missing

Complexity level is high

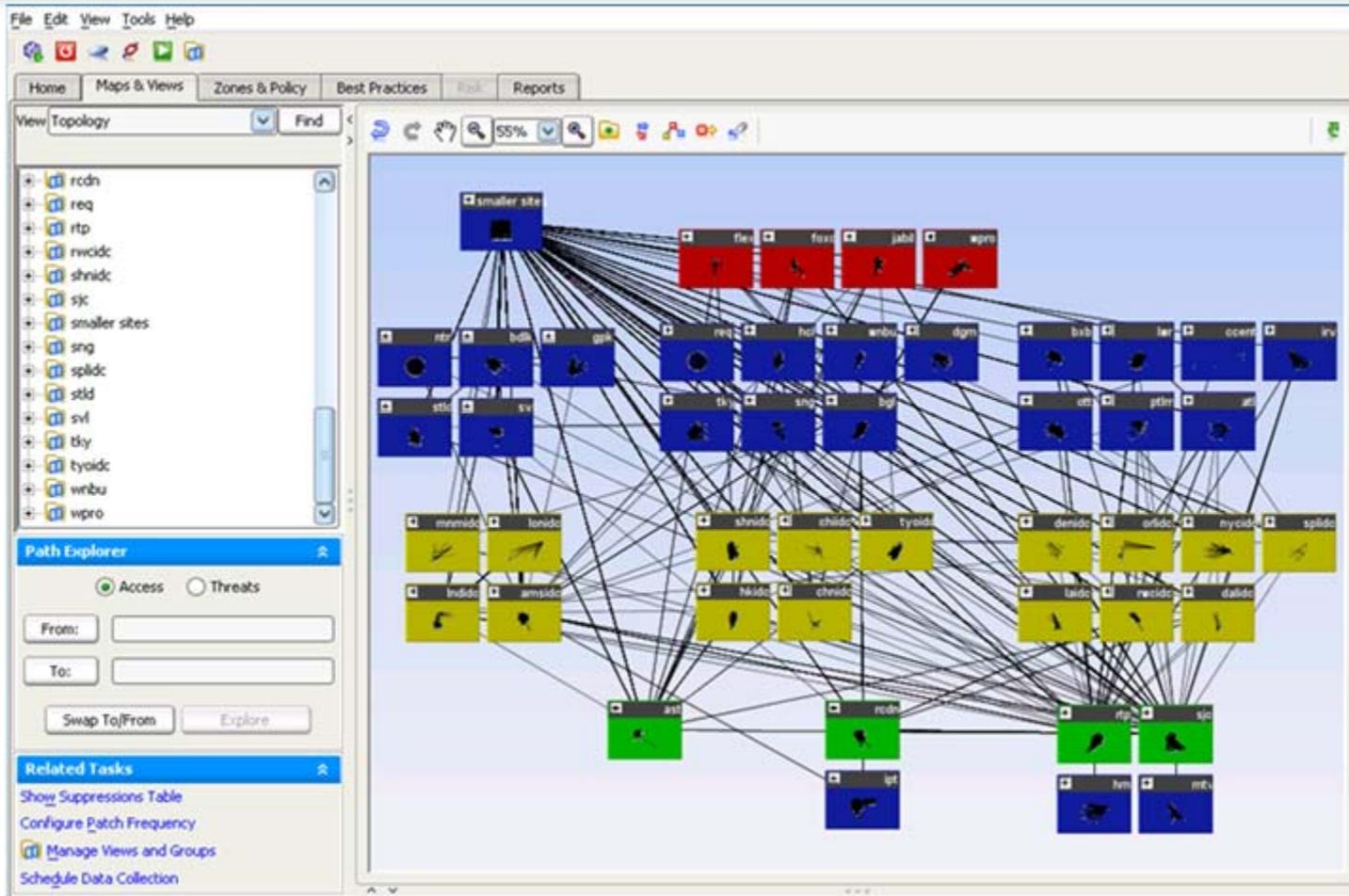


Organizing Cisco's Worldwide Network



- Zoning from location codes, without input from Cisco

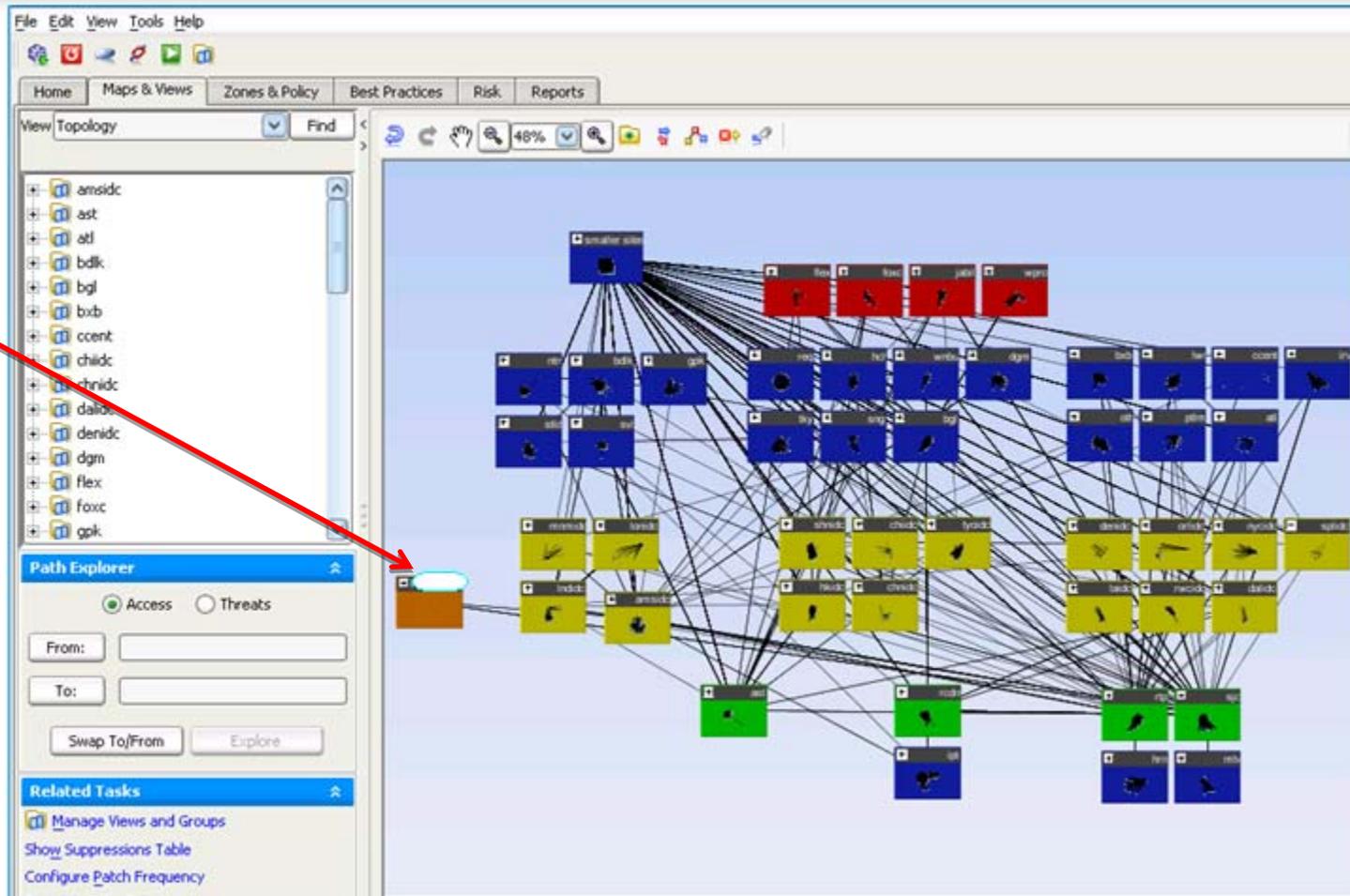
Emerging Patterns



- After collapsing each major group
- EMEA on left, APAC in middle, US on right

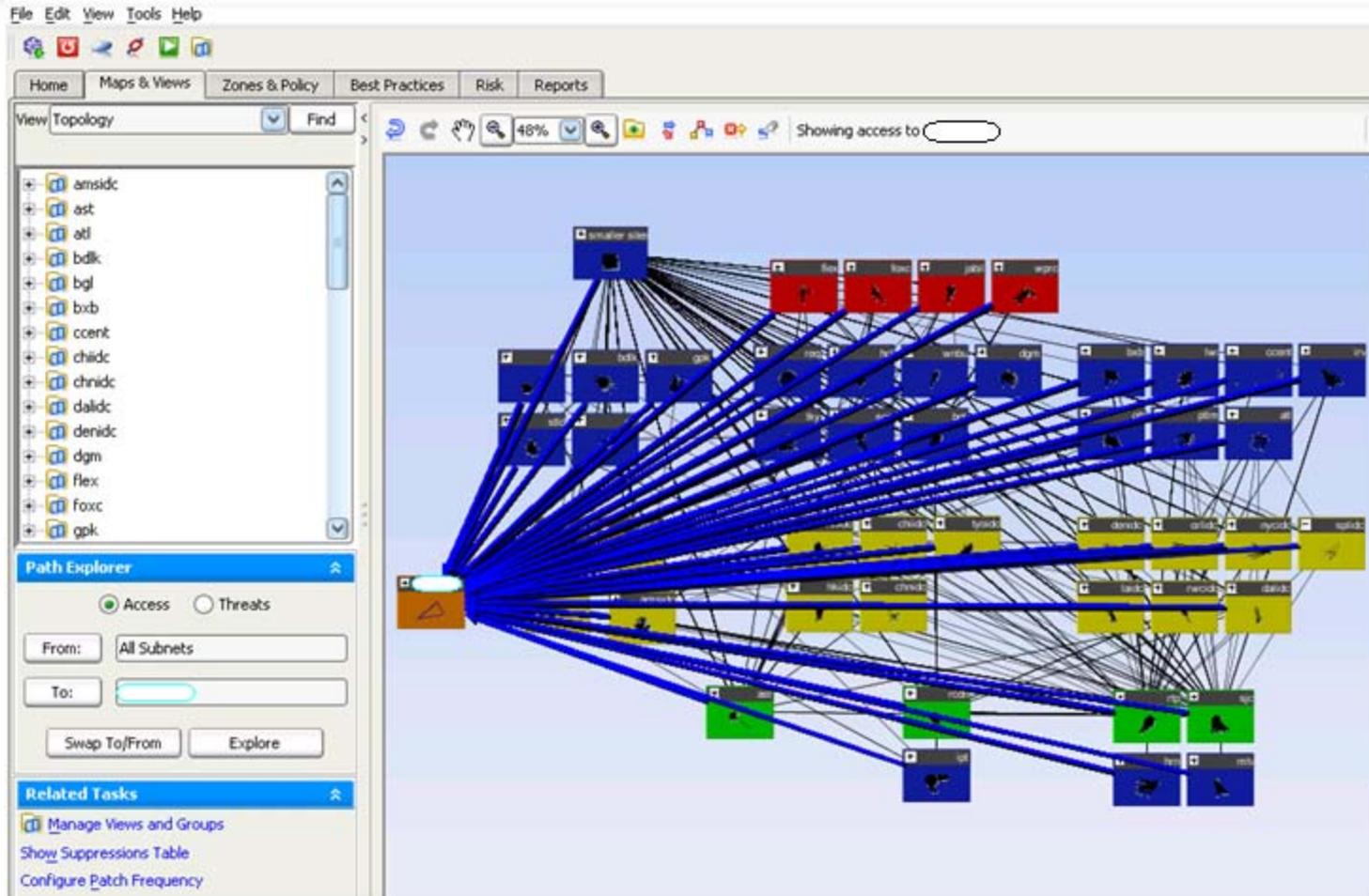
Access analysis of 6 identified critical servers

Sensitive servers



- Question: are these sensitive servers already segmented?
- How would you answer that without automated analysis?

Automatic calculation of access



- Blue lines show open access paths to sensitive servers
- Clearly shows the need for segmentation

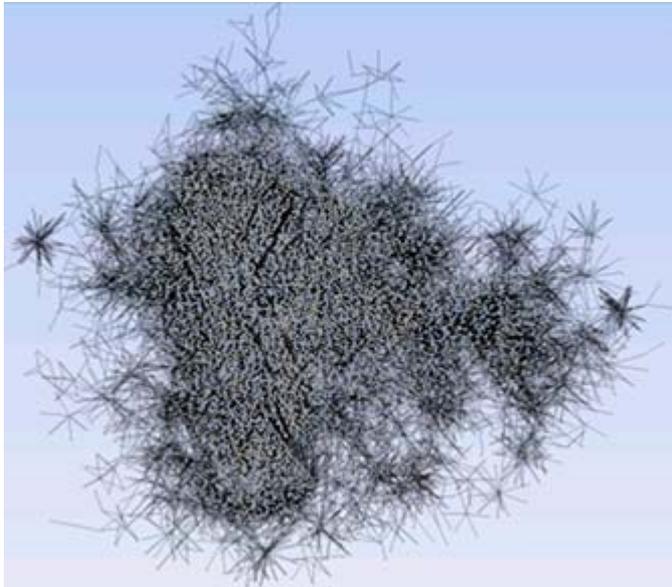
Logical zones capture business requirements



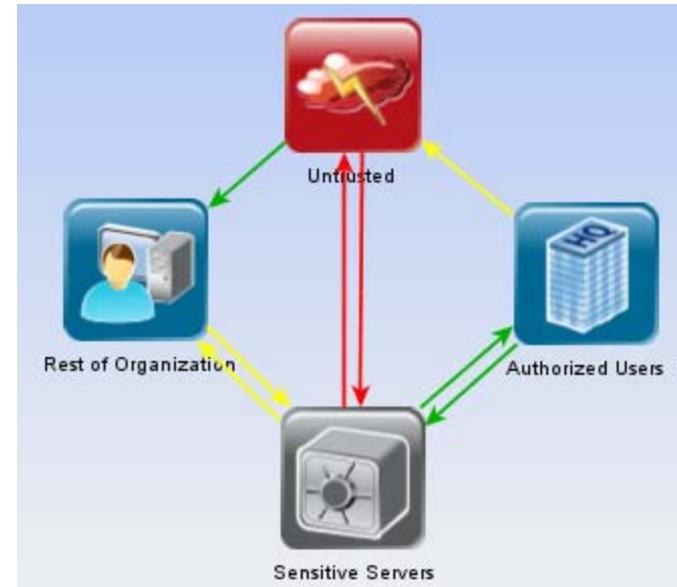
- Maps high-level policies down to technical specifics
- Continuous compliance

Logical zone summarization

Before:



After:



The necessity of automation

- **Doing this manually is:**
 - Hard work
 - Error prone
 - Demanding of esoteric skills
 - “Does this box want 0.0.255.255, or 255.255.0.0?”
- **How long would this take manually?**
 - Assume you had a (super-)human network analyst
 - Reads a device configuration in 1 hour
 - Checks a firewall rule in 1 minute
 - Roughly 27,000 X 1 hour + 637,000 X 1 minute
 - **4 person-years** (working 24x7x365)
- **Ultimately, there is no manual option**

Back to SCAP: Zone-based Policies

- **Prohibitions**
 - “No direct access to HIPAA data from the Internet”
- **Restrictions**
 - “Only logging traffic is allowed from the SCADA systems DMZ”
- **Justification**
 - “All access to cardholder data from the general network must be explicitly justified”
- **Containment**
 - “No direct access from Coalition Networks to NIPRNet”
- **All organizations have zone-based policies**

Zone-based policies need not be organization specific

Implications for SCAP

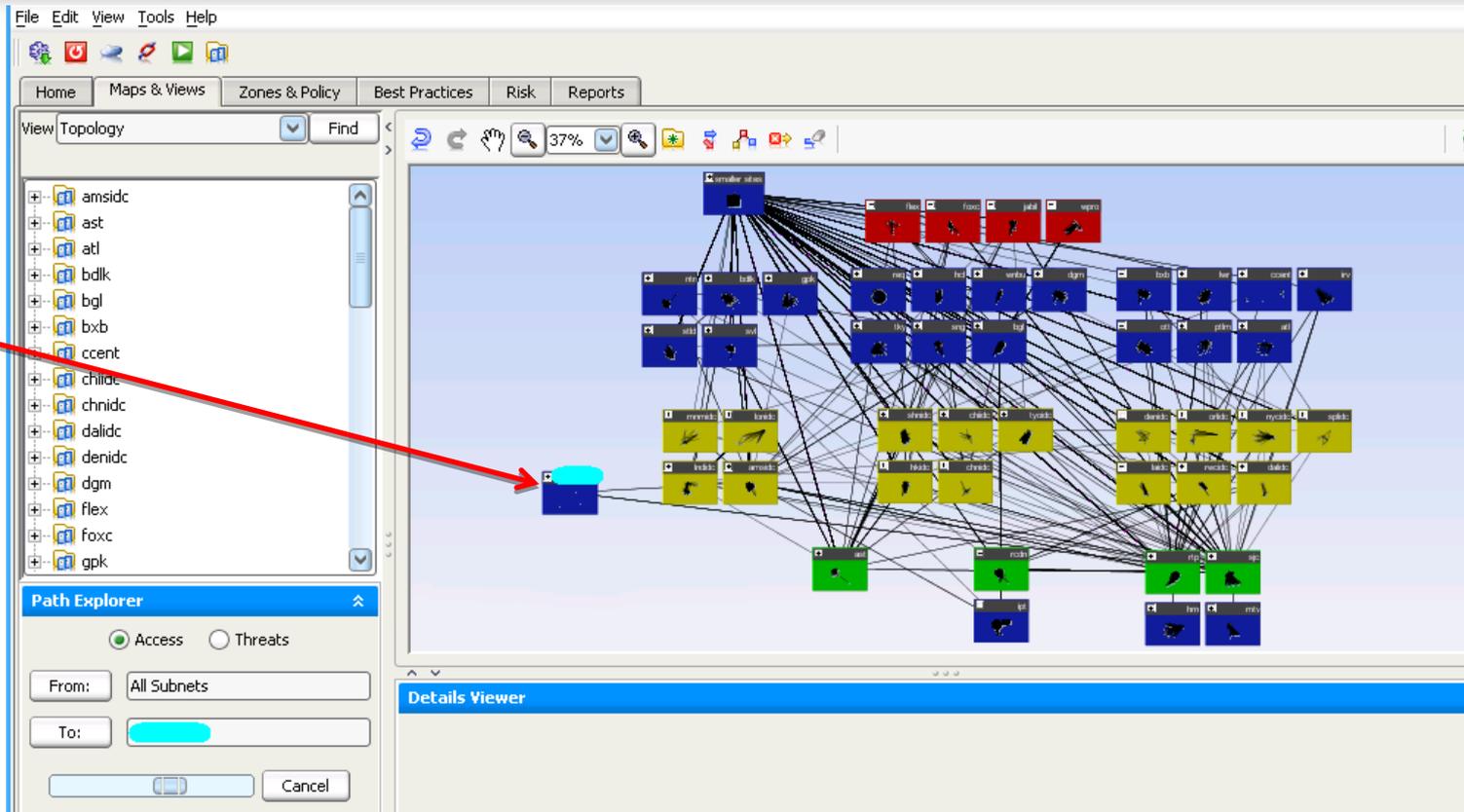
- **SCAP can provide an ideal framework for automation**
- **Standardized zone definitions**
- **Standardized mechanism for expressing policies**
 - Machine readable
- **Benefits**
 - Exchange of security best practices and standards
 - Automation of compliance
 - Real-time understanding of risk

Thank you

- **Questions?**
- **Contact:**
 - drmike@redseal.net
 - <http://www.redseal.net>
 - ddexter@cisco.com
- **Interested? Please hand us a business card.**

Next level: access analysis

Sensitive servers



- IT identified 6 servers worldwide needing protection
- Question: are these servers already segmented?
- How would you answer that without automated analysis?

Automatic calculation of access

The screenshot displays the RedSeal Systems network visualization interface. The main window shows a network topology with various nodes and connections. A specific path is highlighted with thick blue lines, indicating open access from a source node to several destination nodes. The interface includes a menu bar (File, Edit, View, Tools, Help), a toolbar, and a left sidebar with a tree view of subnets. The bottom panel shows a table of access paths.

Protocol	Source IP	Source Port	Source Node	Destination Node	Destination IP	Destination Port/C
TCP	[redacted]	any	[redacted]	[redacted]	[redacted]	1521
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-160, 162-1433
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-1433
TCP	[redacted]	443	[redacted]	[redacted]	[redacted]	Any Except:
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-160, 162-1433

- Blue lines show open access paths to sensitive servers
- Easily shows the need for segmentation

From red to blue

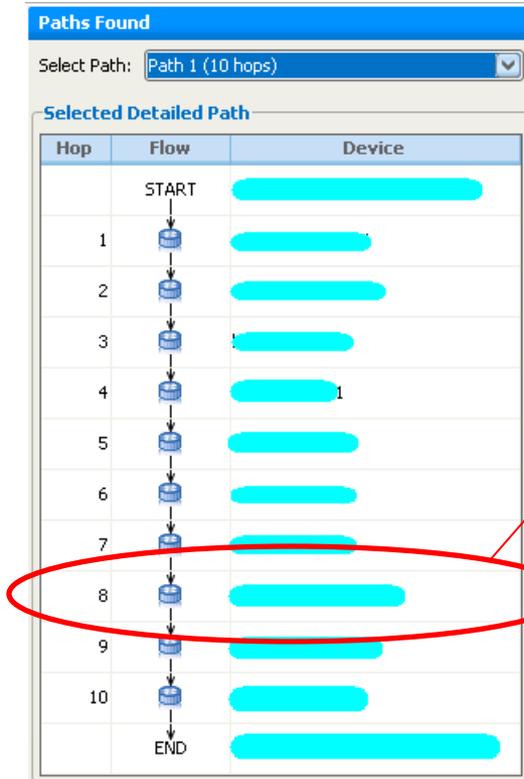
The screenshot shows a network security tool interface. The main window displays a table of access rules. The table has the following columns: Protocol, Source IP, Source Port/, Destination IP, and Destination Port/Code. The table contains 23 rows of data, all with 'TCP' as the protocol. The Source IP and Destination IP columns are redacted with grey boxes. The Destination Port/Code column shows various ports, including 'any except 23', '1681', and '135, 15000'. A red box highlights the last row, which has 'TCP' as the protocol and 'any except 23' as the destination port. A red arrow points from this row to the text below.

Protocol	Source IP	Source Port/	Destination IP	Destination Port/Code
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		1681
TCP		any		1681
TCP		any		1681
TCP		any		1681
TCP		any		1681
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		any except 23
TCP		any		135, 15000
TCP		any		any except 23

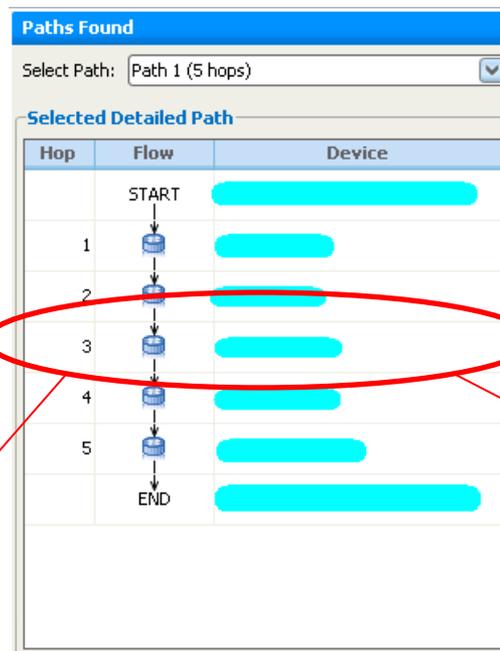
- Access details from one spot to one server
- “Any port you want, except for telnet”

How do you fix this?

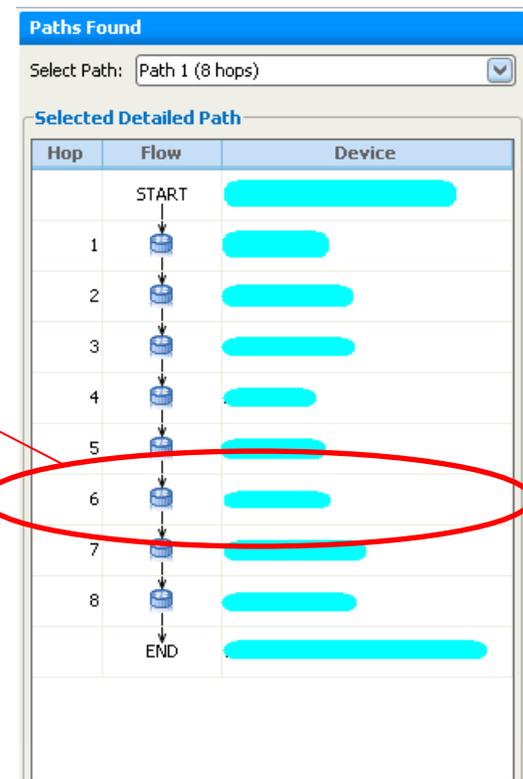
From India



From Brazil

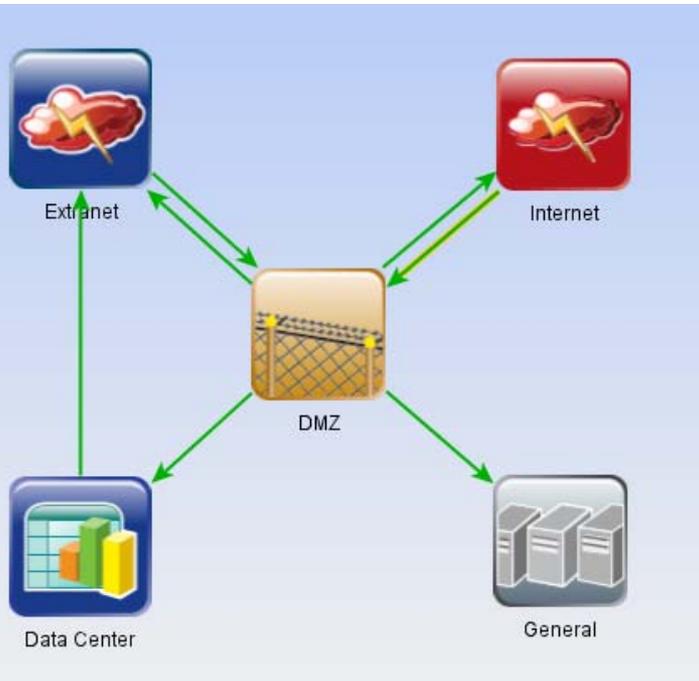


From Hawai'i



- These “subway maps” display access paths in detail
- Highlighted hop is the same device
- Ideal choke point to enforce better segmentation

Expressing Security Policy: Zoning



- **Organize network by function**
- **Protected Information Systems**
 - Cardholder Data (PCI)
 - Protected Health Information (HIPAA)
 - Control Systems (NERC CIP, CFATS)
 - Classified data
- **Access zones**
 - Internet, Extranet
 - Wireless
 - General user network
- **DMZs**
 - Inbound, outbound DMZ
 - Control System Perimeter
- **Express policy between zones**

Automated, Continuous Monitoring

PCI Audit Table ?

Load Devices
 Load Scan Data
 Set Untrusted
 Analyze

Manage Policies
 Edit
 Set Rules
 Check Compliance

Zone Overlap
 DMZ and Cardholder Overlap

Rules Report
 Compliance Report

Check Compliance

→ Pass
 → Warning
 → Fail
 - - - Zone Overlap

Access from Untrusted to Cardholder 1 row

Zone Pair	Protocols	Ports	Status
Untrusted to Cardholder TCP		22	✓

Business Decisions

Name	Approved ..	Expiration D..	Edit Date	
PCI Audit Policy	[REDSEAL SRM]		5/28/09 8:56...	
Protocols	Ports	Sources	Destinations	Type
any	any	Internet	Cardholder	FORBIDDEN
any	any	Cardholder	Internet	FORBIDDEN
FTP Access from Internet to DMZ	Tom Rabaut		5/28/09 9:10...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	
Corporate PolicyCorporate Policy Specification	uiadmin		5/28/09 10:1...	

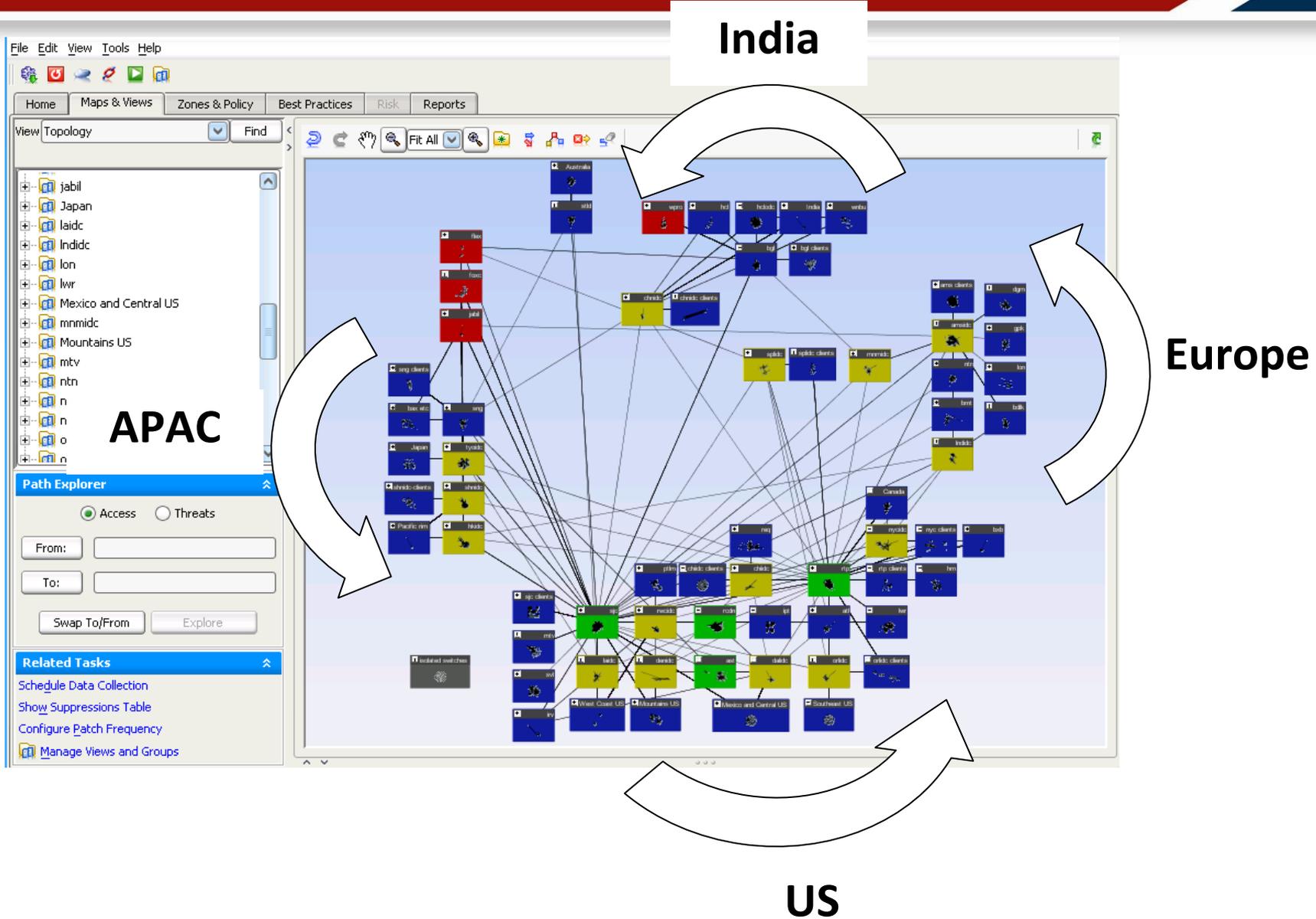
Network assessment – what's different?

Network analysis requires a systems approach

Steps:

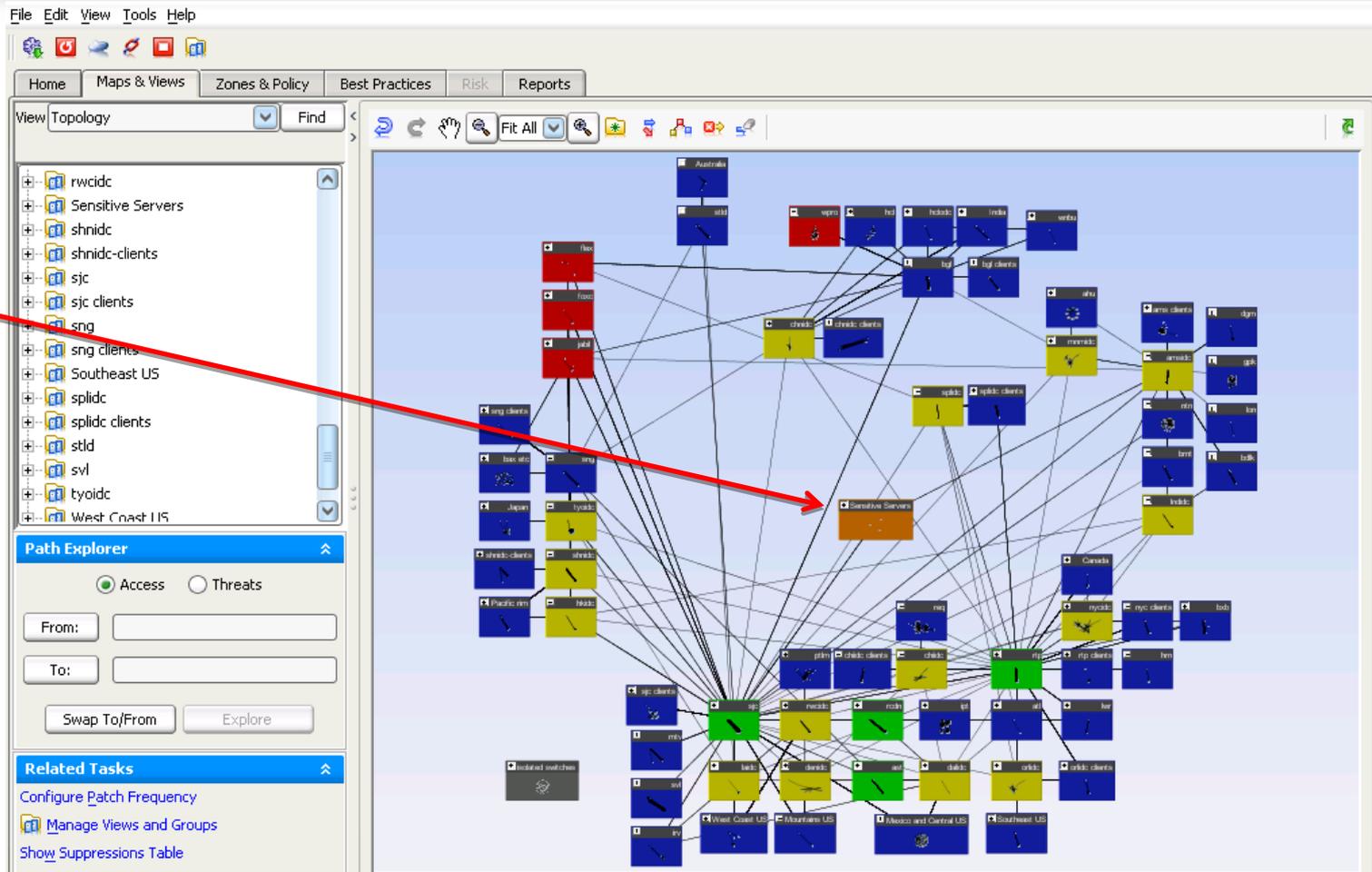
1. Gather configuration inventory
2. Build map
 - What's directly connected to what?
 - What's missing?
3. Compute access
 - Who has access to what?
4. Compare to objectives and regulatory requirements

Final "circumpolar" zoned view



Access analysis of 6 identified critical servers

Sensitive servers



- **Question: are these sensitive servers already segmented?**
- **How would you answer that without automated analysis?**

Automatic calculation of access

The screenshot displays a network visualization tool interface. The main window shows a network topology with various nodes and connections. A path explorer on the left shows a path from 'All Subnets' to a specific destination. Below the path explorer, a table titled 'Access from All Subnets to PCI pieces' lists the access paths.

Protocol	Source IP	Source Port	Source Node	Destination Node	Destination IP	Destination Port/C
TCP	[redacted]	any	[redacted]	[redacted]	[redacted]	1521
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-160, 162-1433
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-1433
TCP	[redacted]	443	[redacted]	[redacted]	[redacted]	Any Except:
UDP	[redacted]	any	[redacted]	[redacted]	[redacted]	0-160, 162-1433

- Blue lines show open access paths to sensitive servers
- Clearly shows the need for segmentation