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

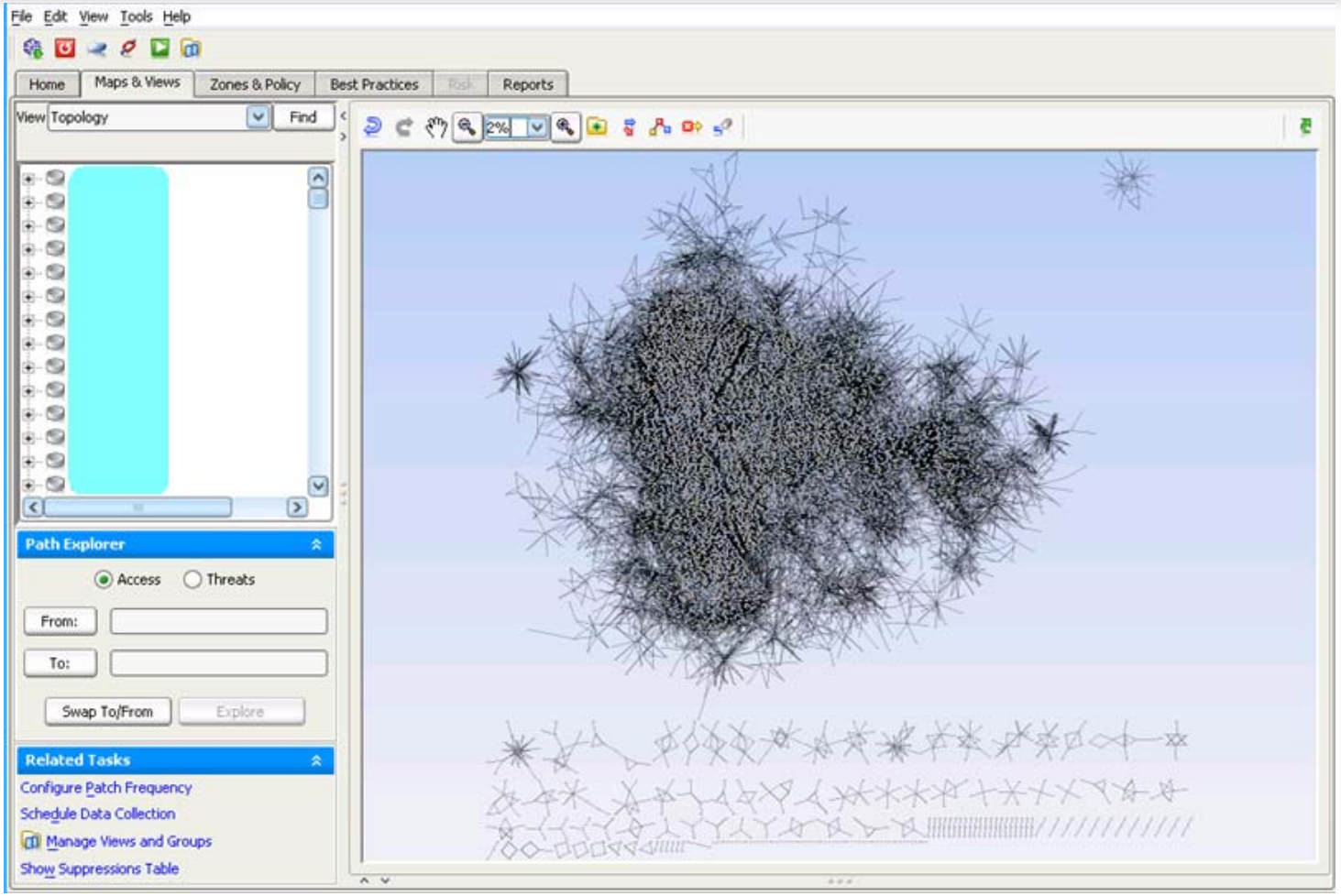
3. **Whole network analysis is the next level**
   - You can't detect a route around the firewall by reading the firewall
   - Requires systemic understanding—not just individual devices
   - This is an extraordinarily complex problem

Cisco's "Project Atlas"

- **Objective:**
  - Map the global Cisco environment
  - Review major site interconnections
  - Audit access to sensitive locations

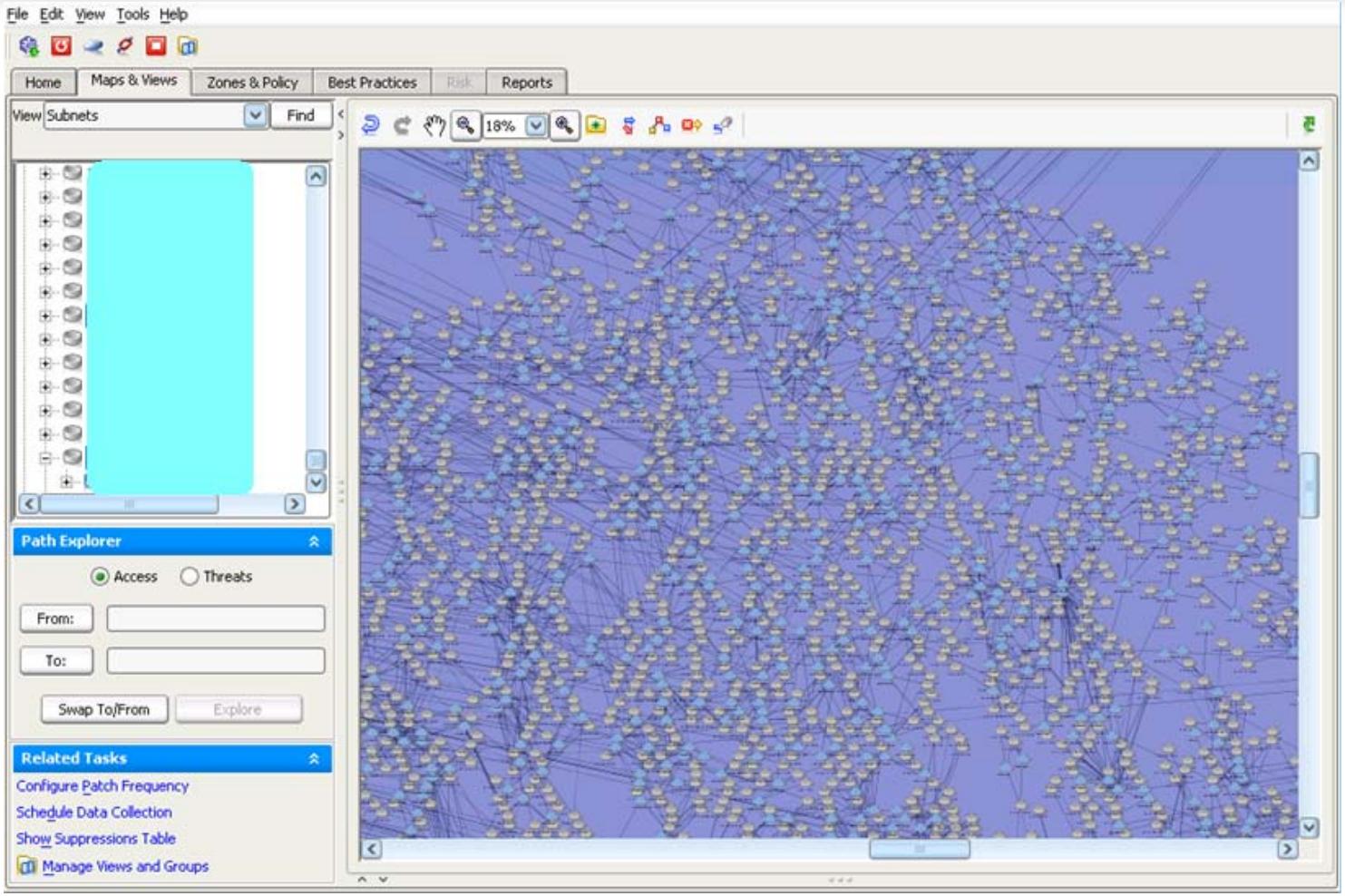
- **Resources:**
  - Installed RedSeal software
  - ~$5K server (quad core, 32G RAM)
  - Two weeks
  - 27,000 configuration files
  - One RedSeal employee, part time
    - Initially a "science project"
    - Now delivering operational payoff

Raw Network



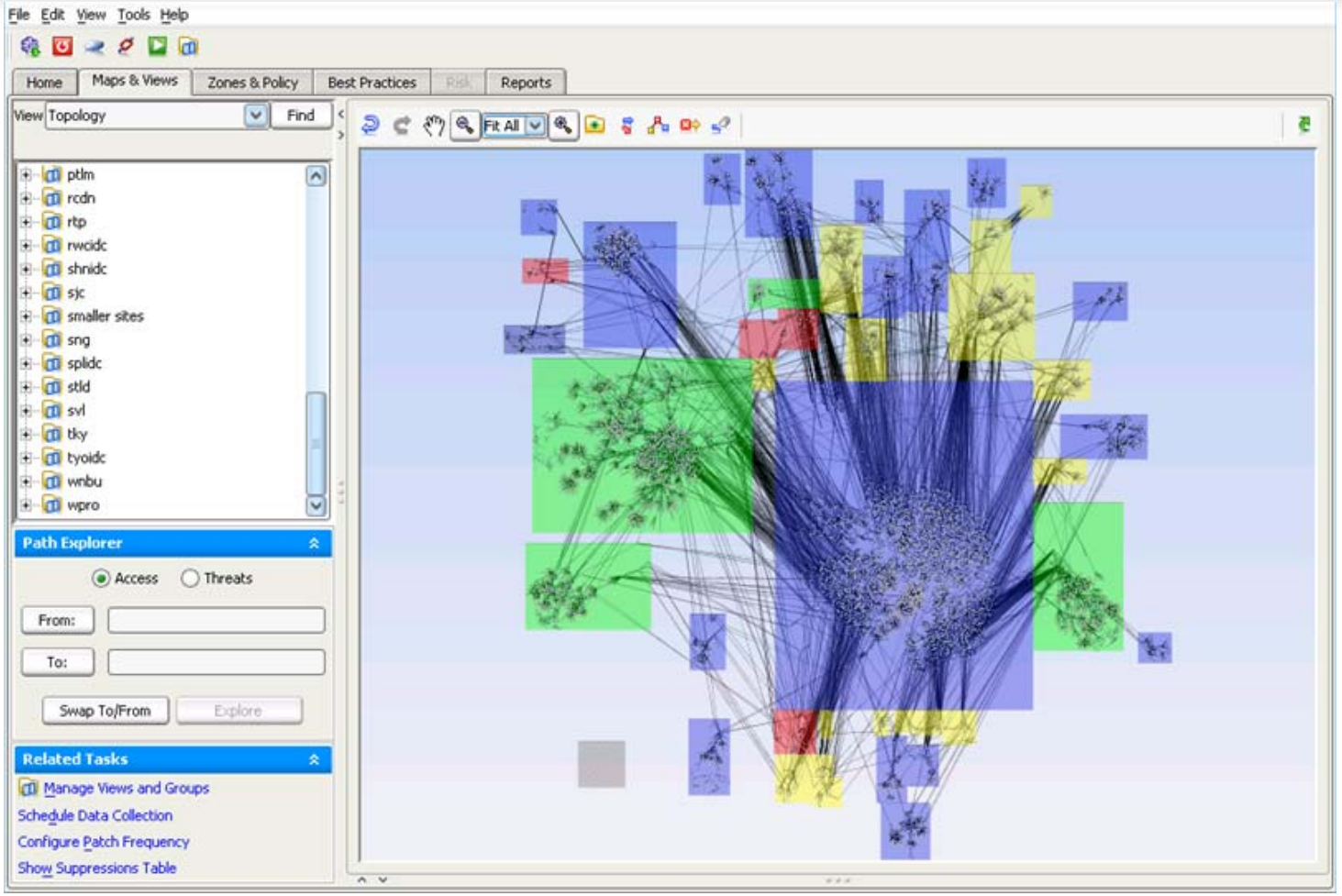
- **Note visual clue – some devices are missing**

Complexity level is high



RedSeal

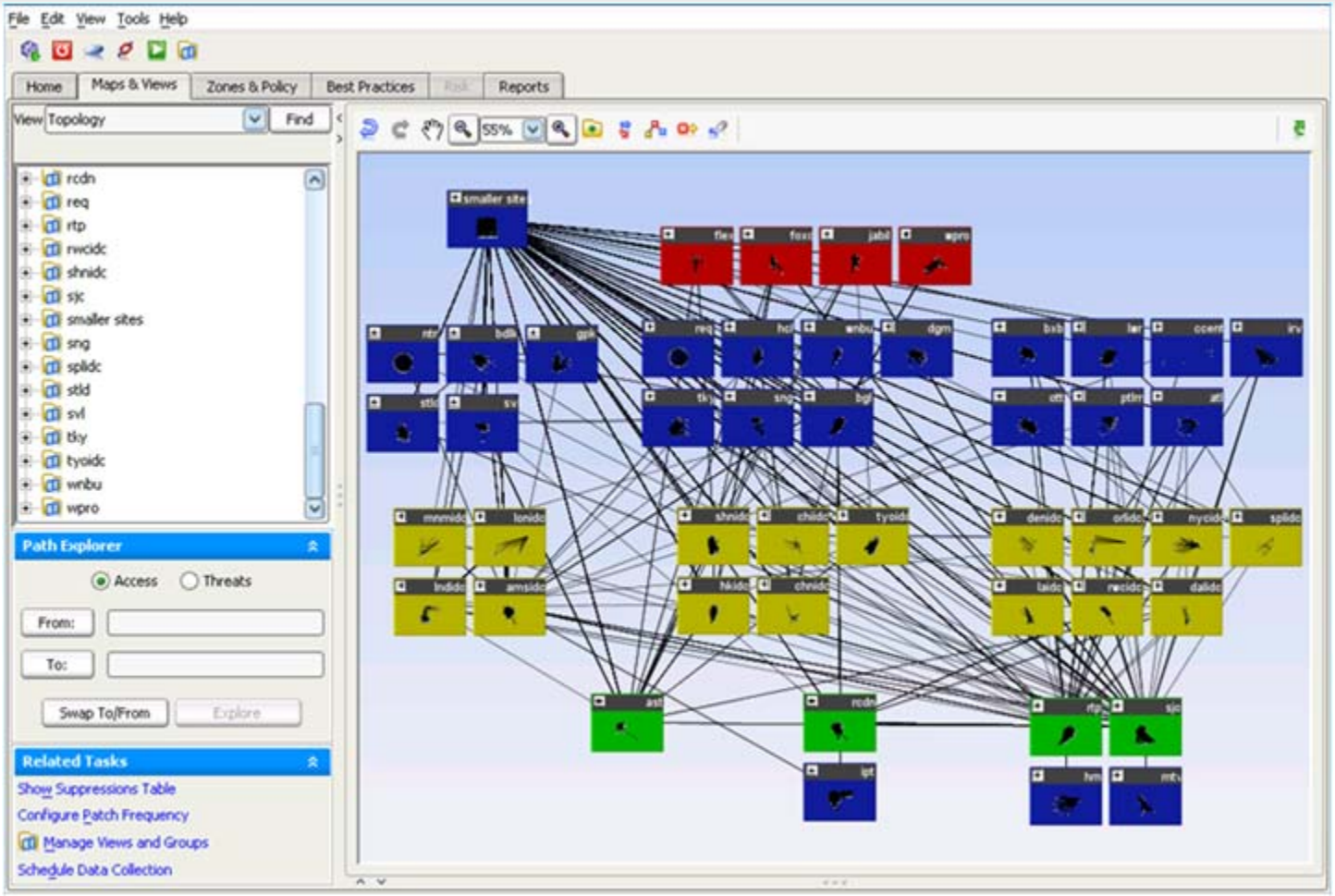
Organizing Cisco's Worldwide Network



- **Zoning from location codes, without input from Cisco**

RedSeal

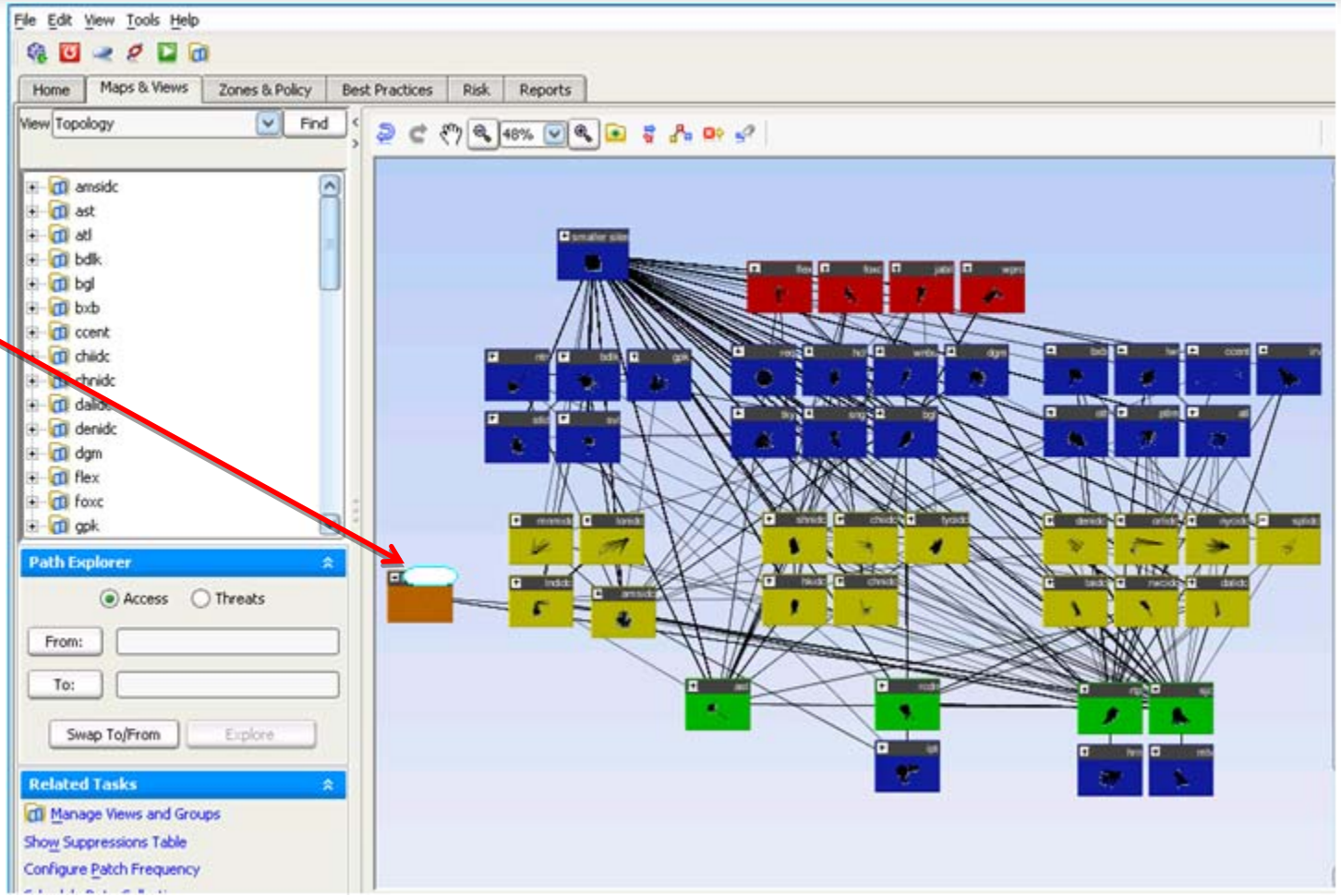
Emerging Patterns



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

Access analysis of 6 identified critical servers

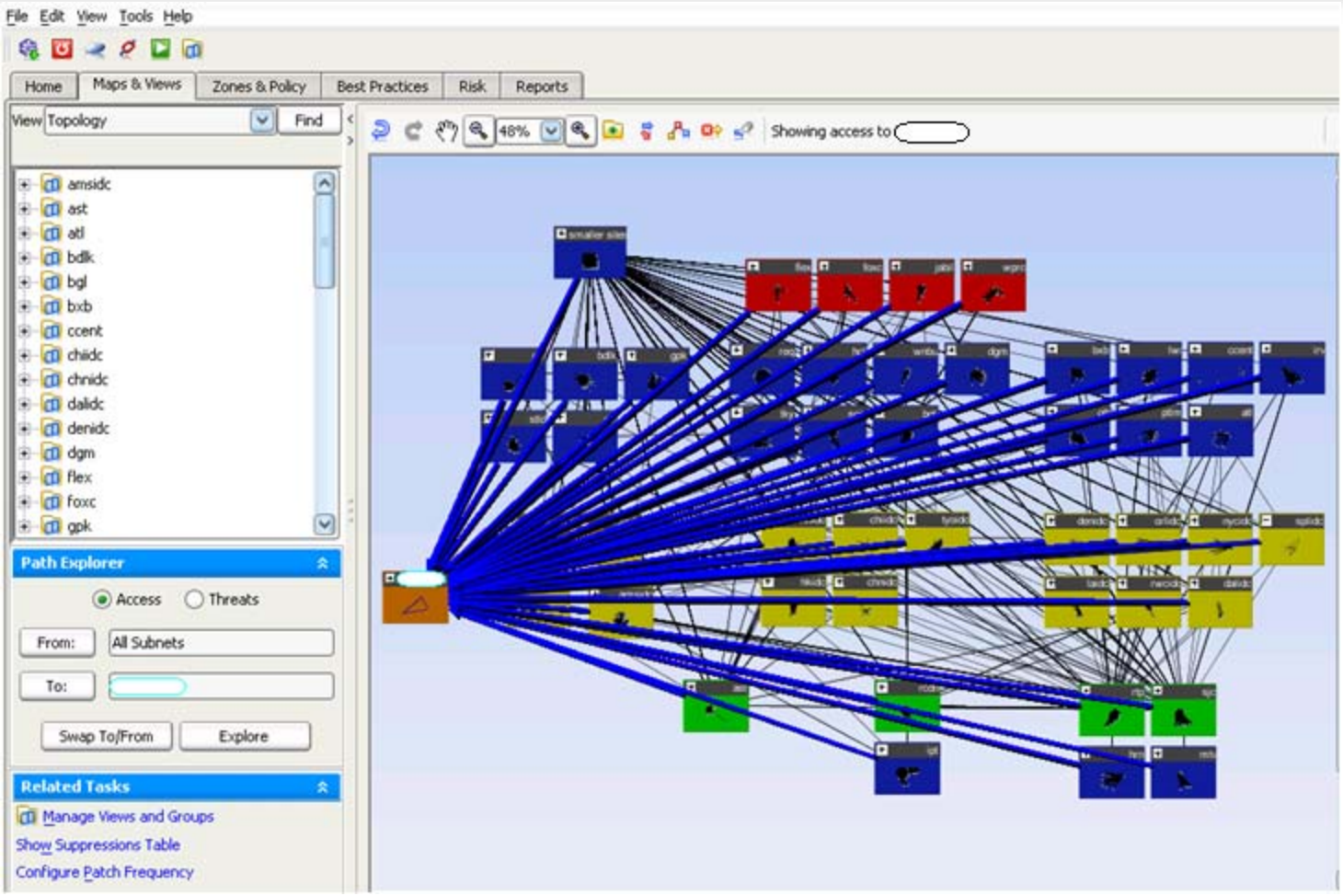
Sensitive servers



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

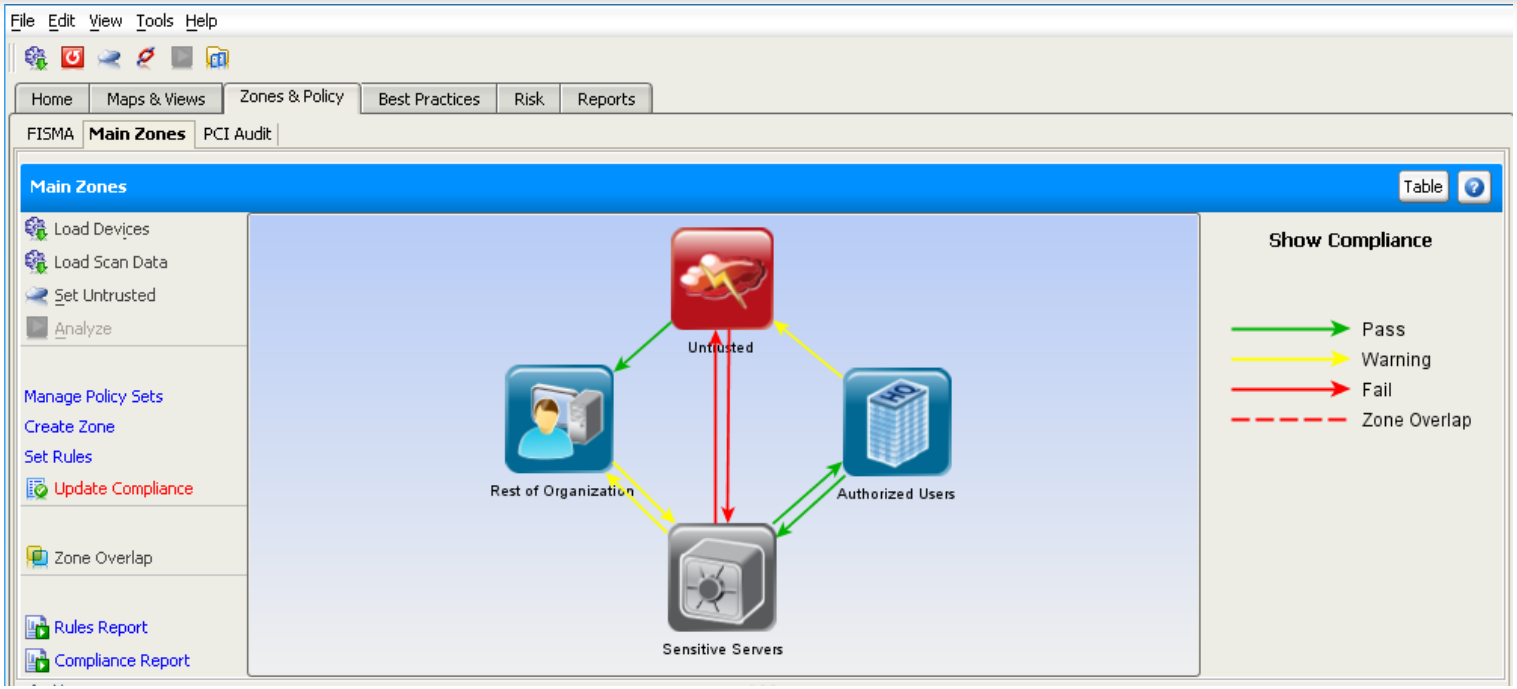
RedSeal

Automatic calculation of access



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

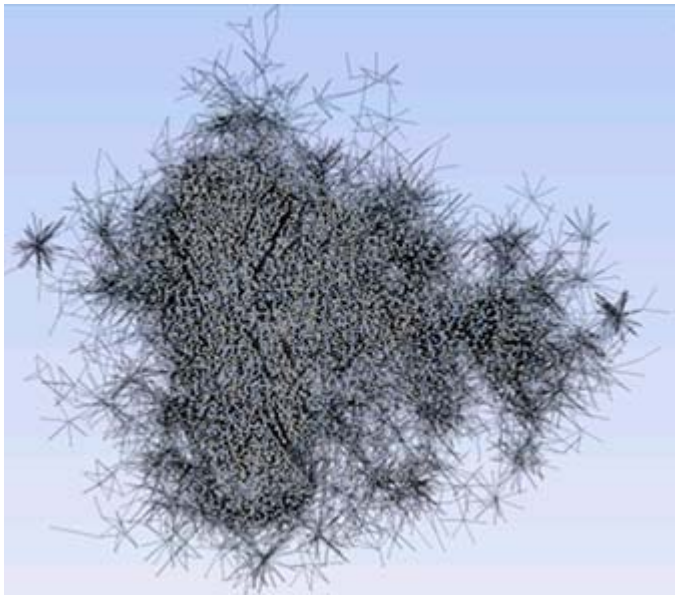
Logical zones capture business requirements



- **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?**

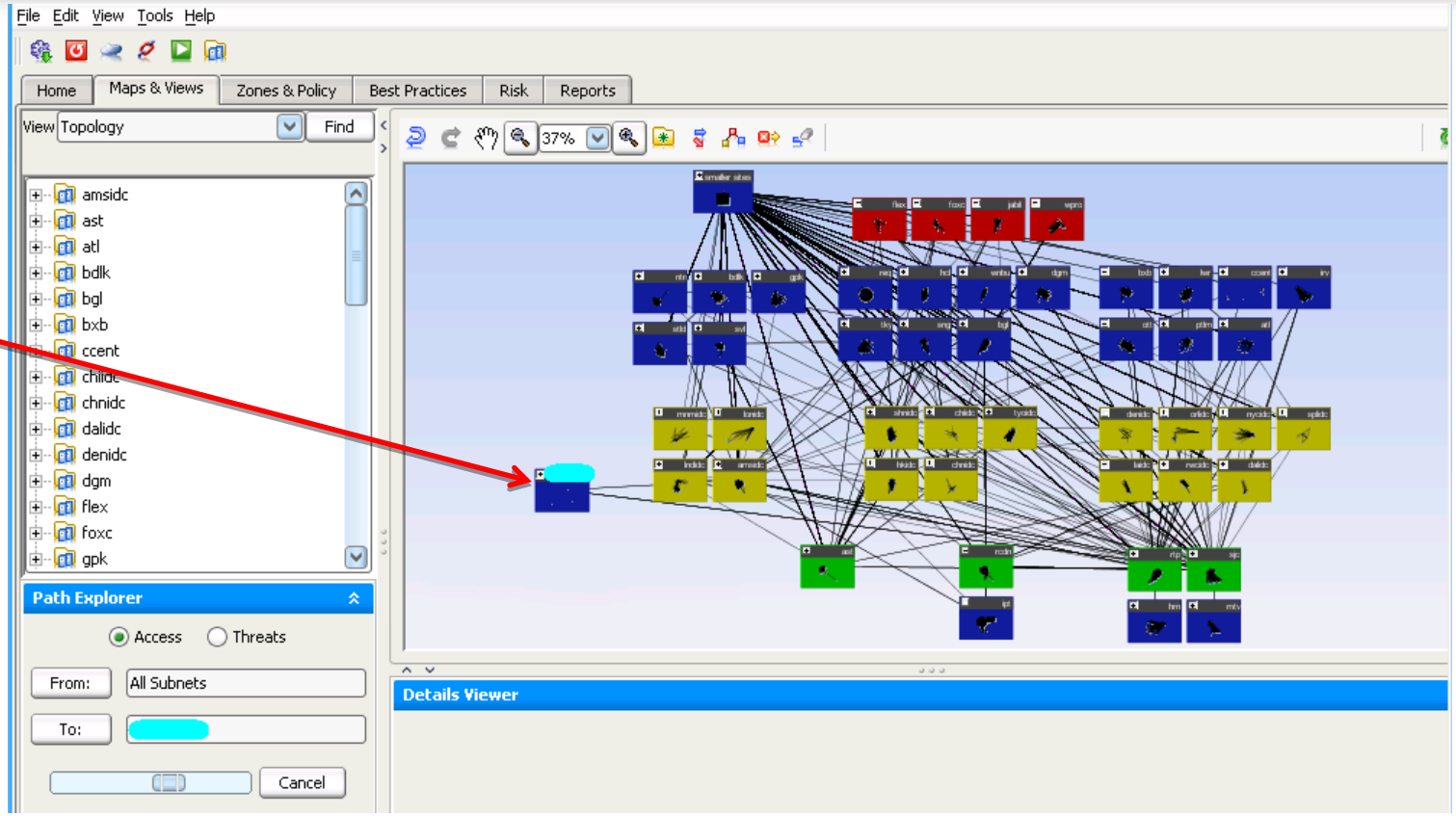
- **Contact:**
  - drmike@redseal.net
  - http://www.redseal.net

  - ddexter@cisco.com

- **Interested? Please hand us a business card.**

Next level: access analysis

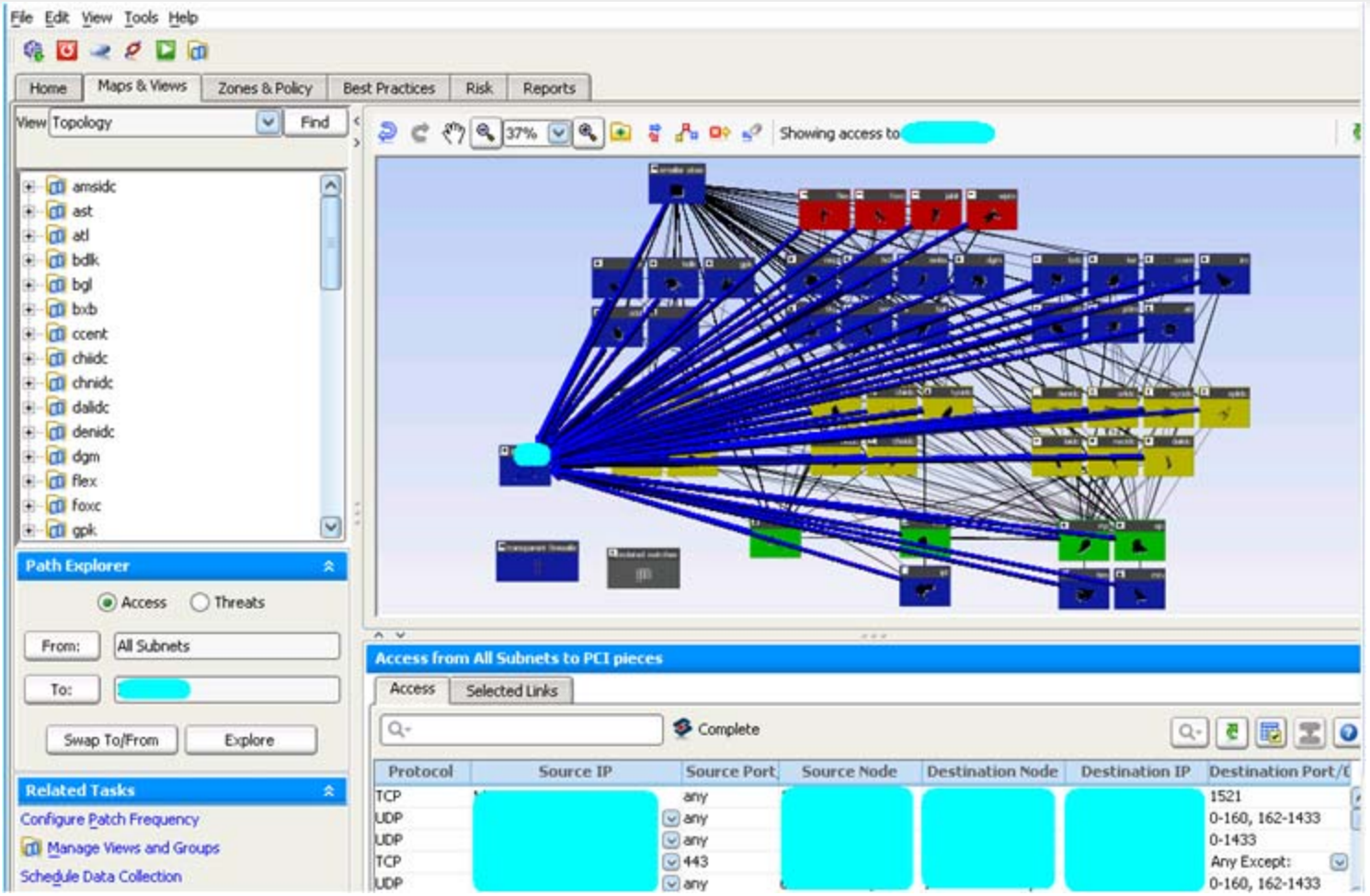
Sensitive servers



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

RedSeal

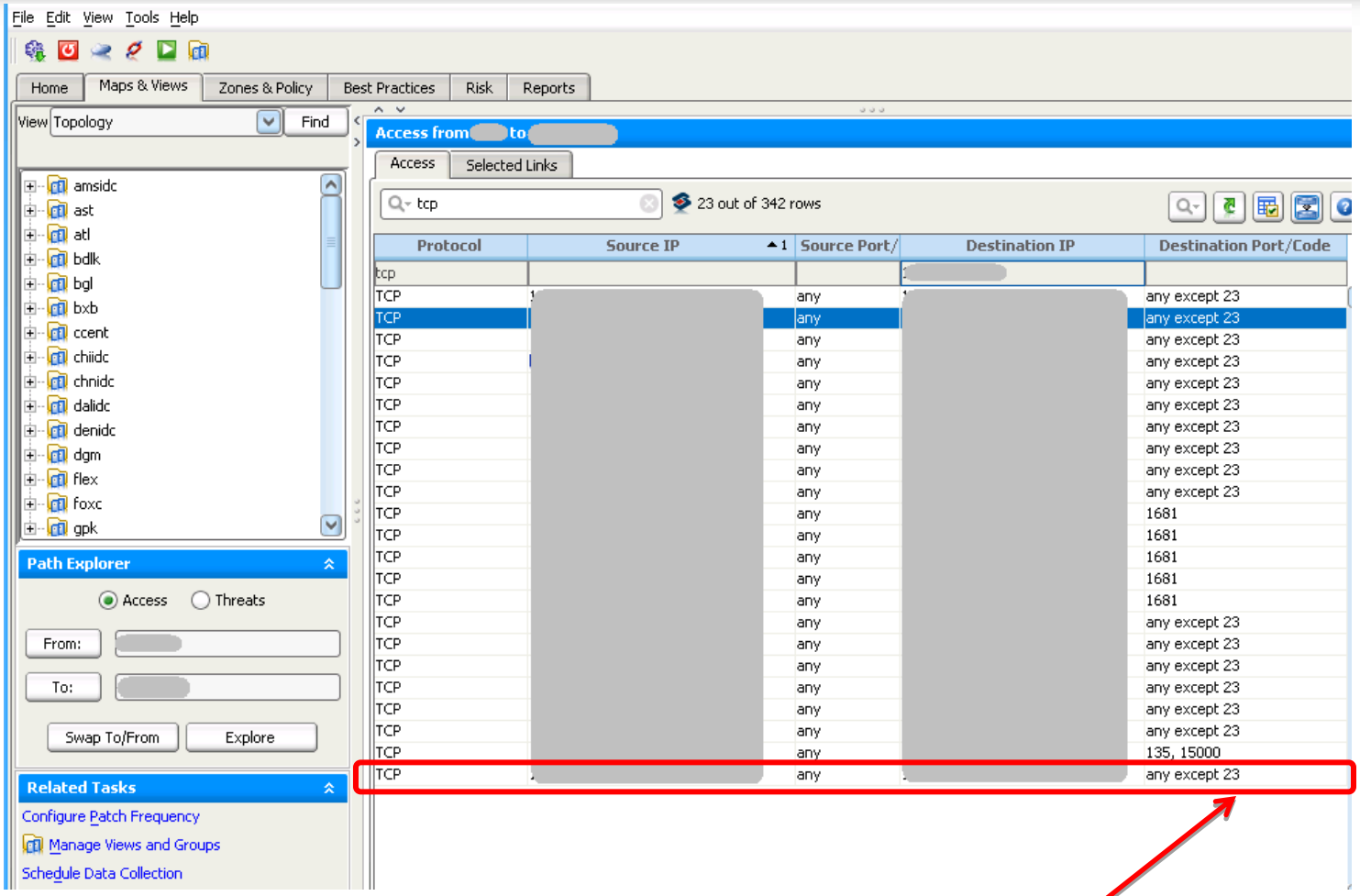
Automatic calculation of access



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

RedSeal

From red to blue

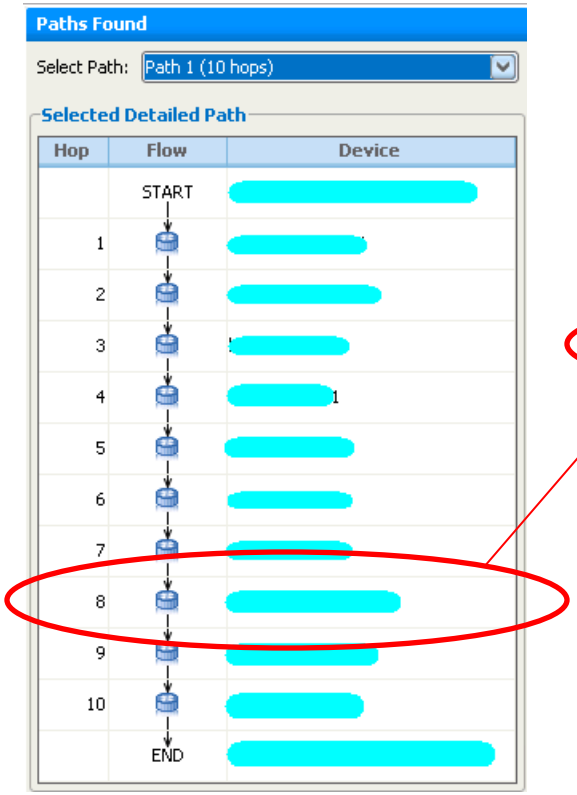


- Access details from one spot to one server
- "Any port you want, except for telnet"

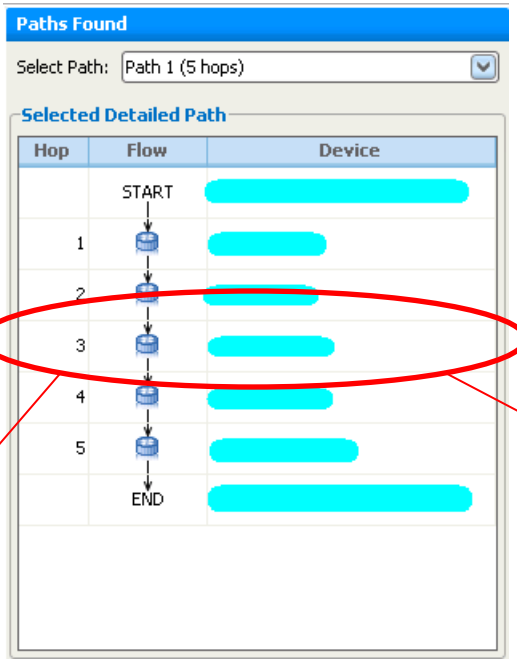
RedSeal

How do you fix this?

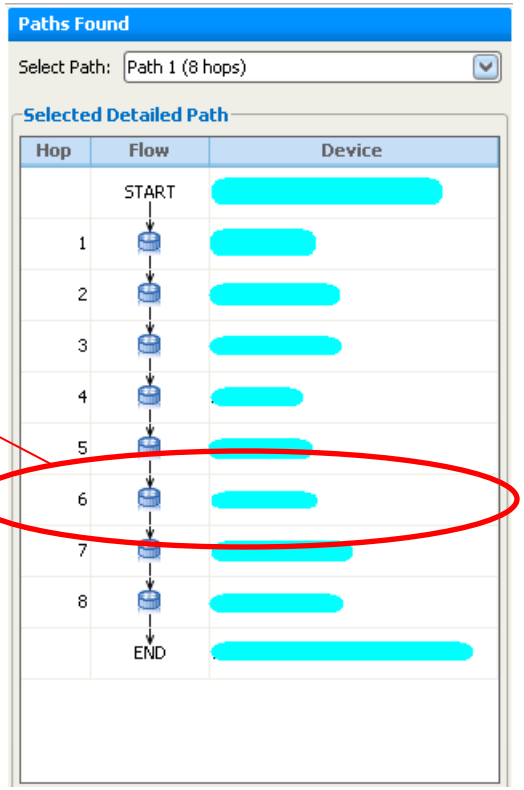
From India



From Brazil



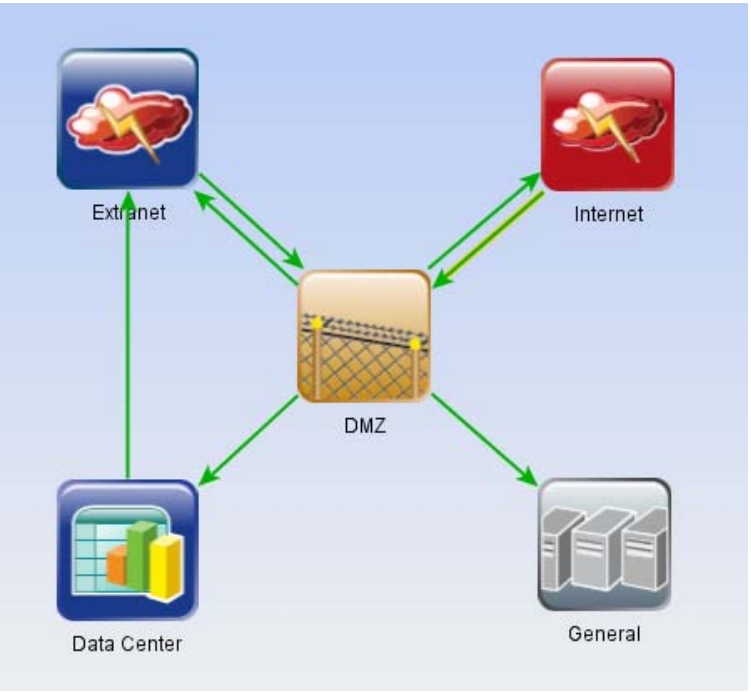
From Hawai'i



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

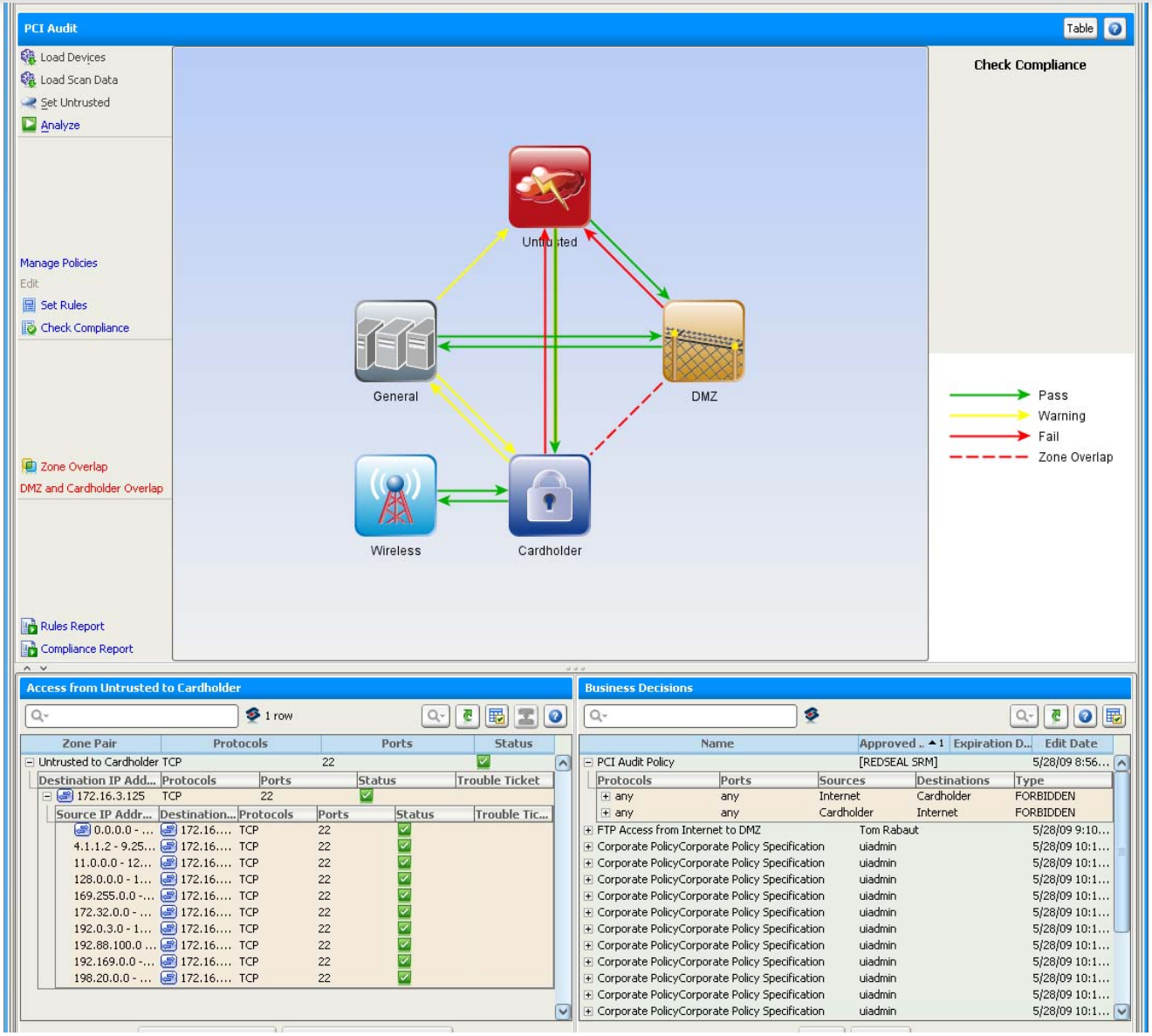
RedSeal

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



RedSeal

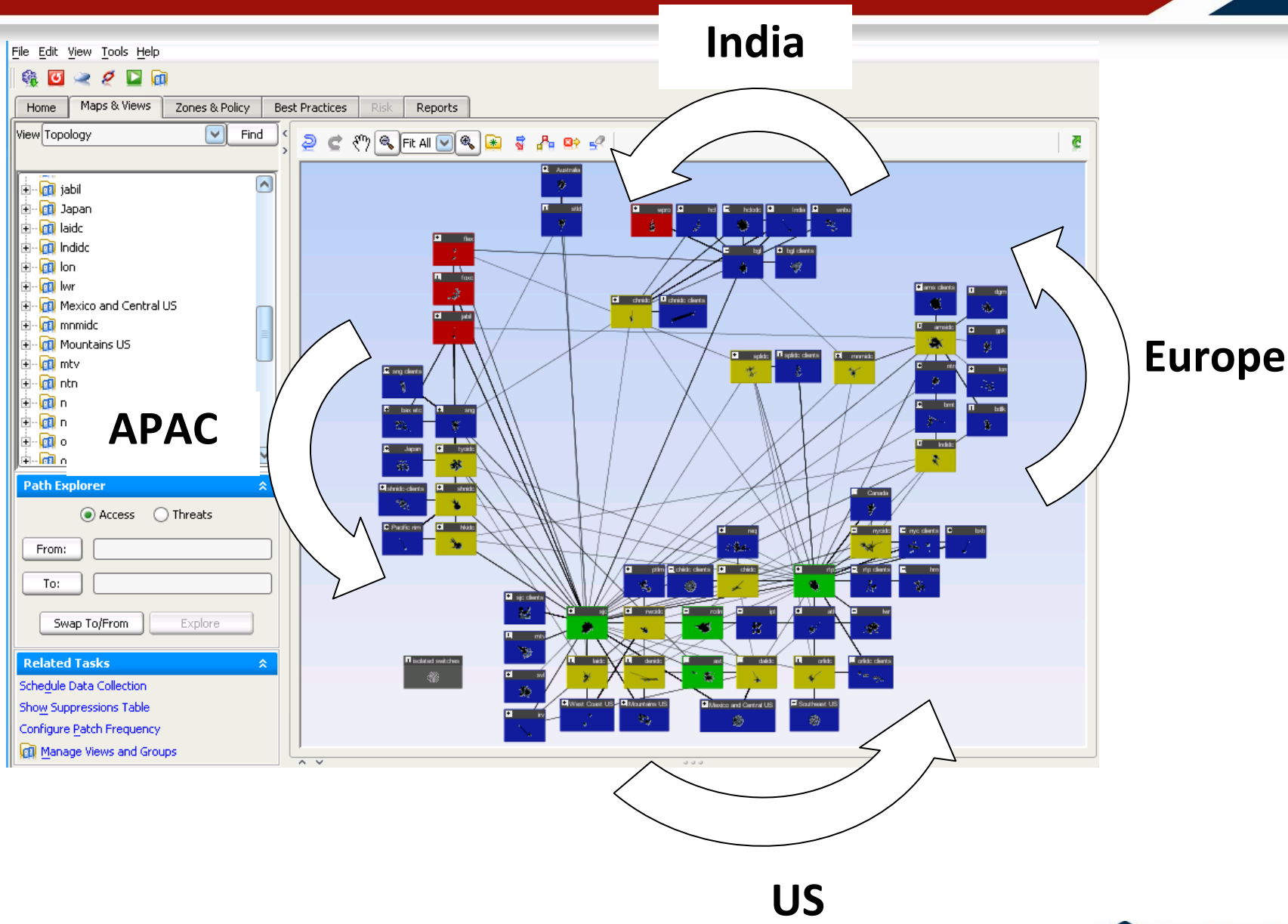
Network assessment – what's different?

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

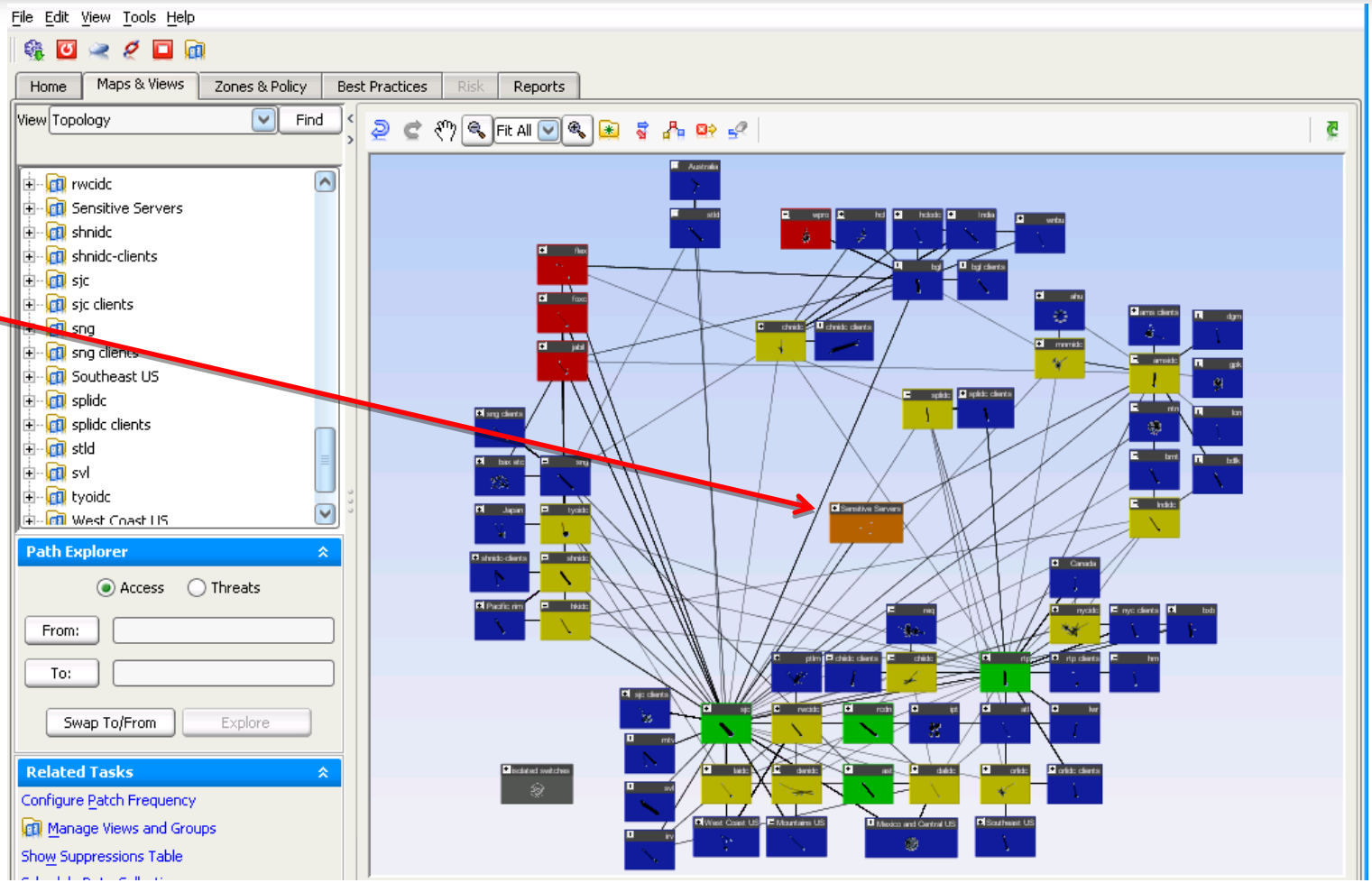
Final “circumpolar” zoned view



RedSeal

Access analysis of 6 identified critical servers

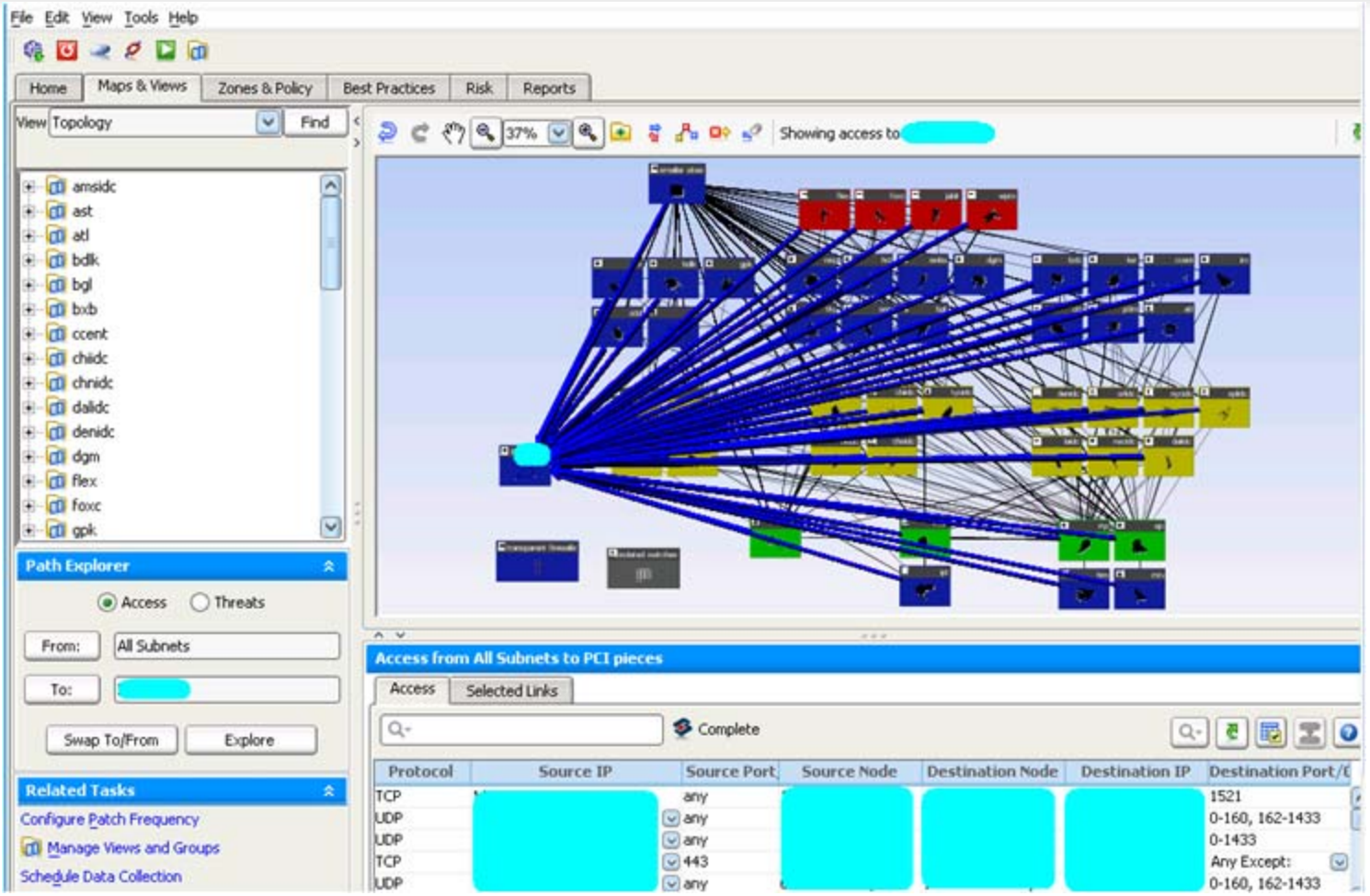
Sensitive servers



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

RedSeal

Automatic calculation of access



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

RedSeal