



Automating Network Security Assessment



Doug Dexter
Audit Team Lead

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

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

Automating Network assessment

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"

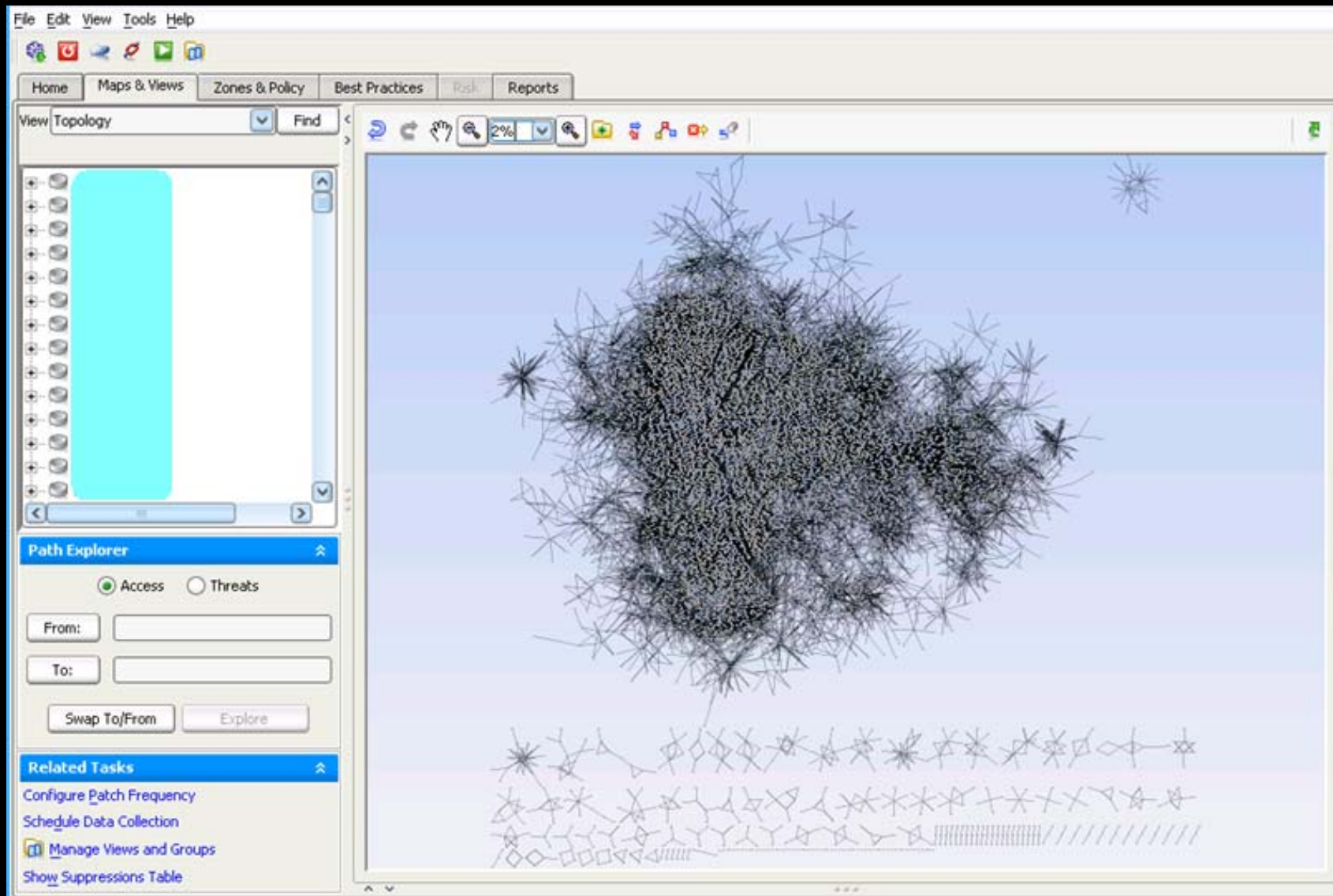
- Objective:

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

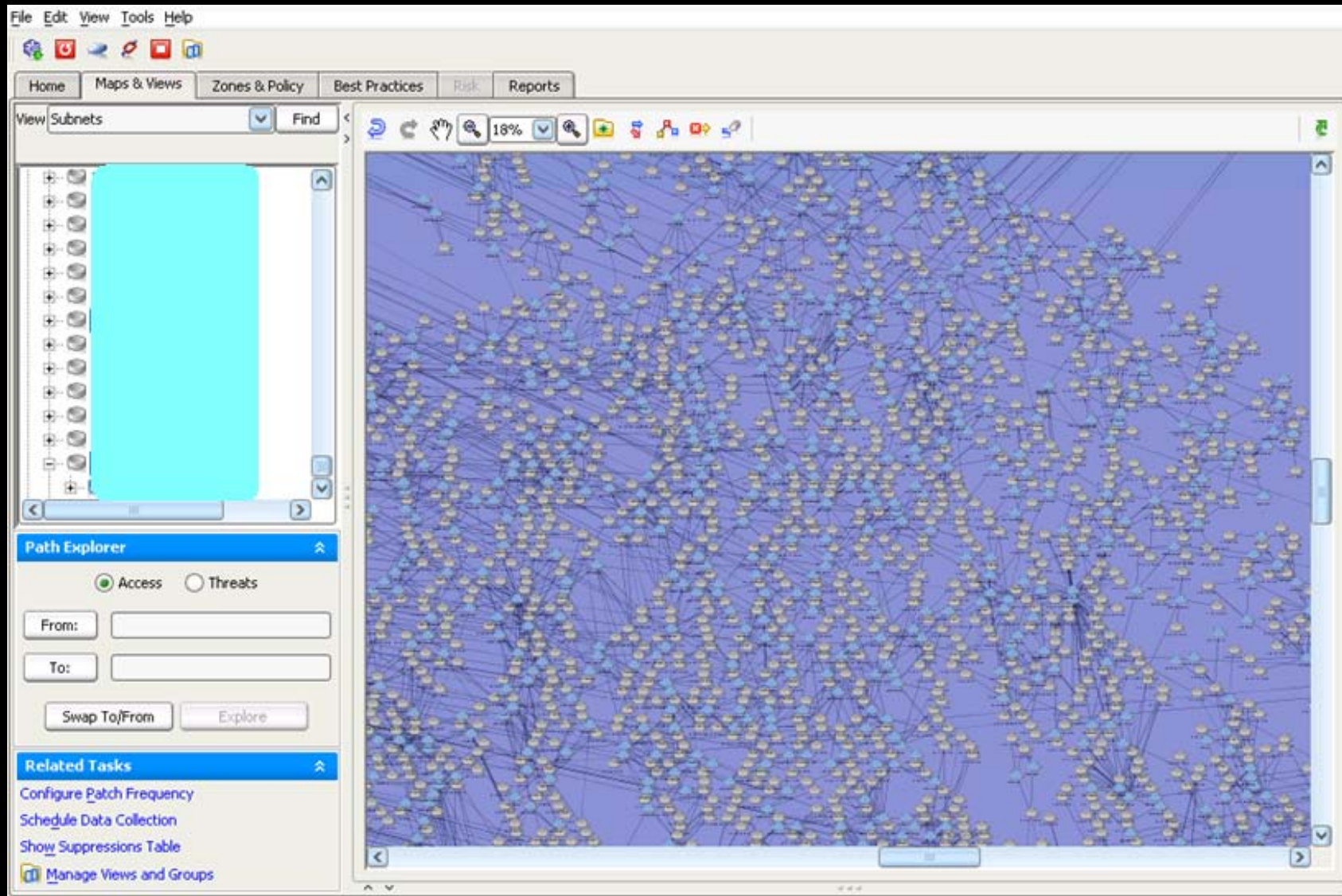
- Resources:

- 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

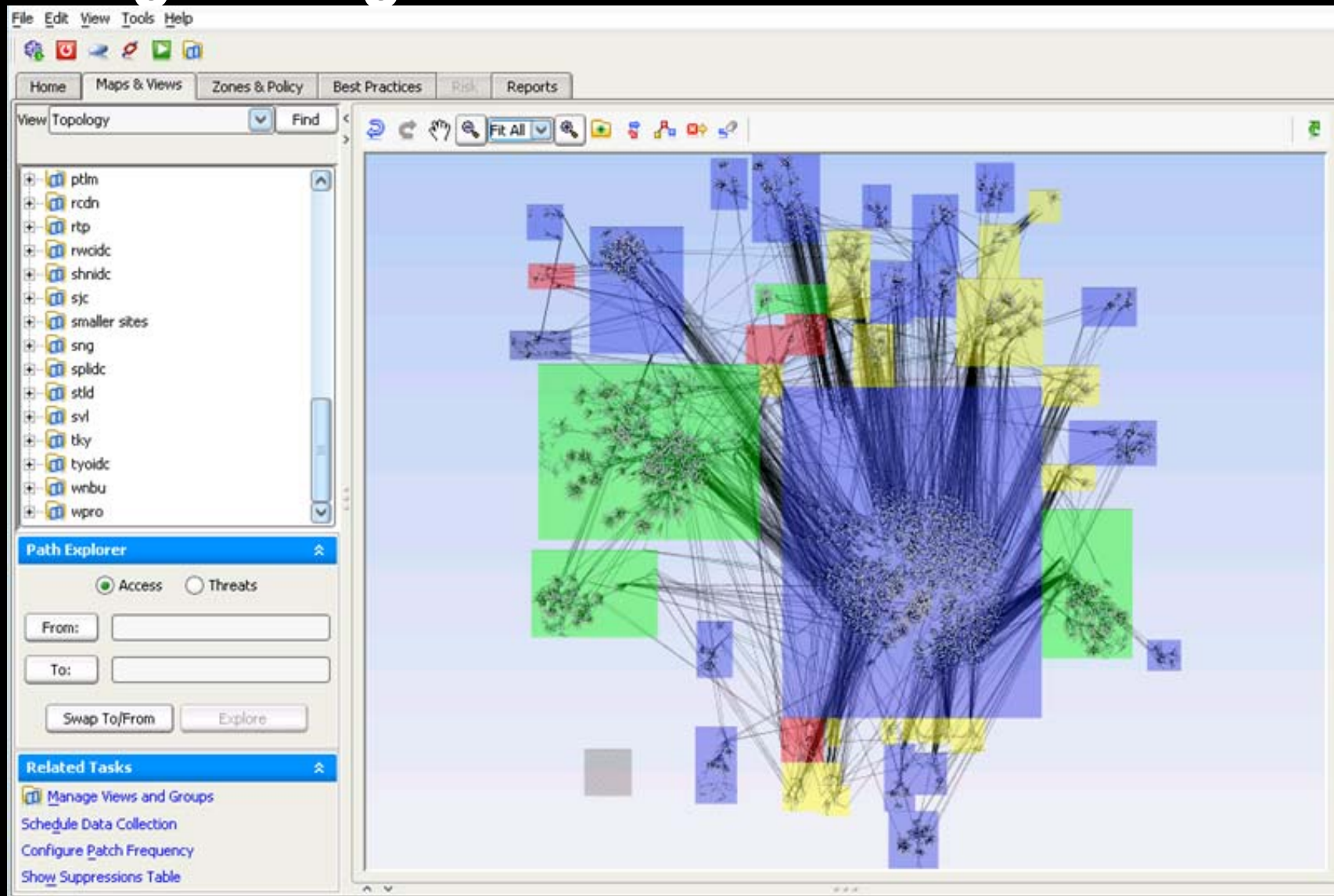
Raw Network (aka “The Bug Splat”)



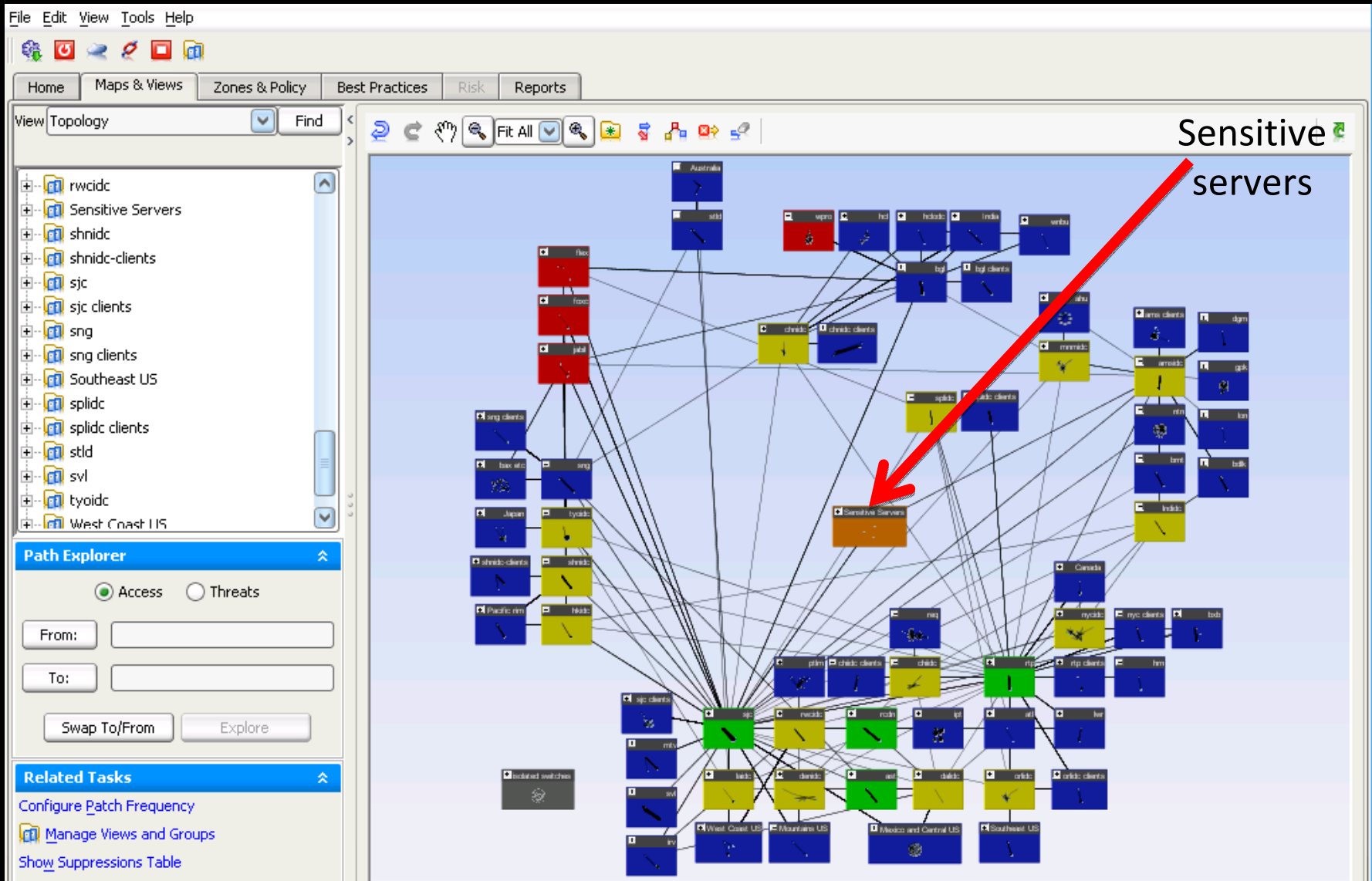
Complexity level is high



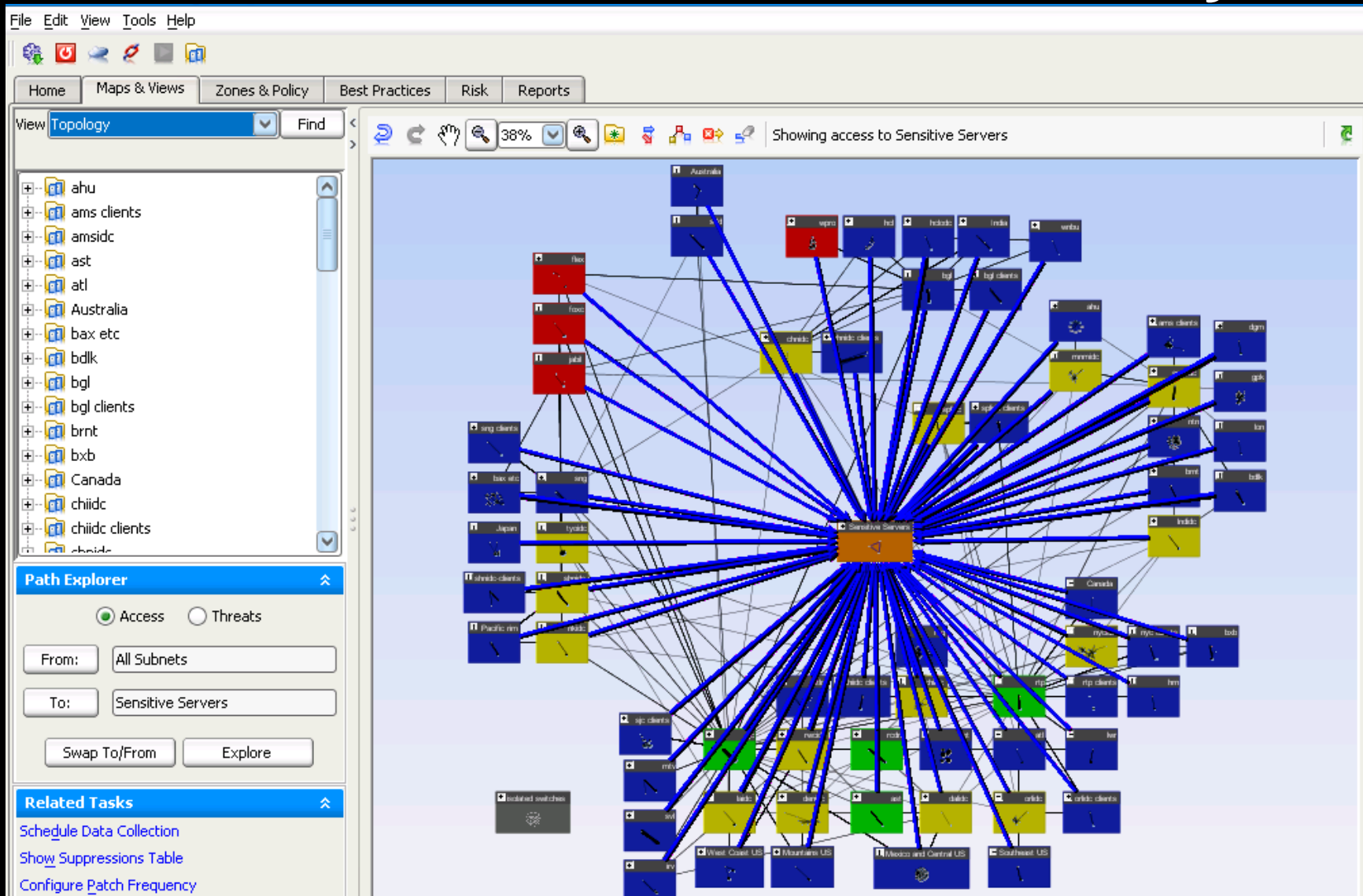
Organizing Cisco's Worldwide Network



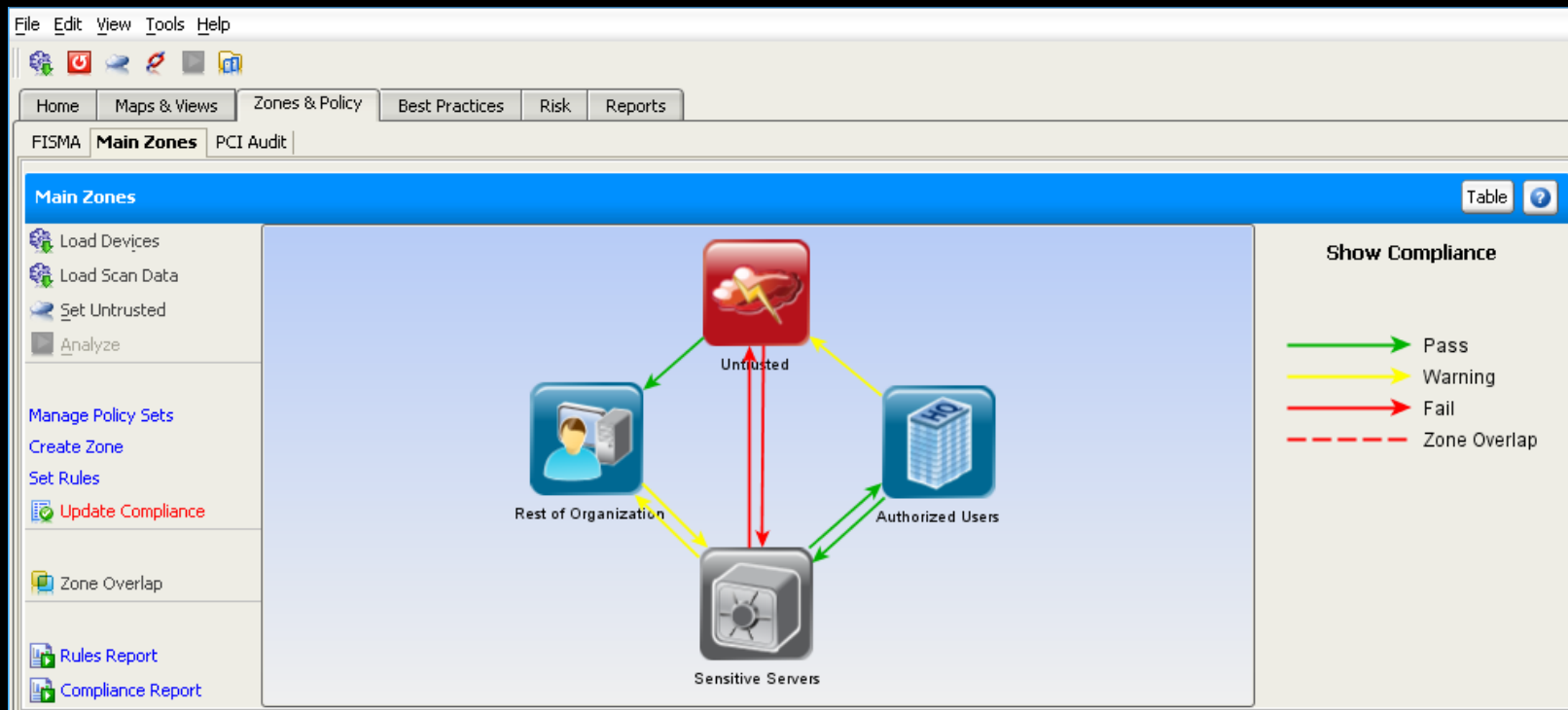
Connectivity to six sensitive servers



Automatic calculation of connectivity



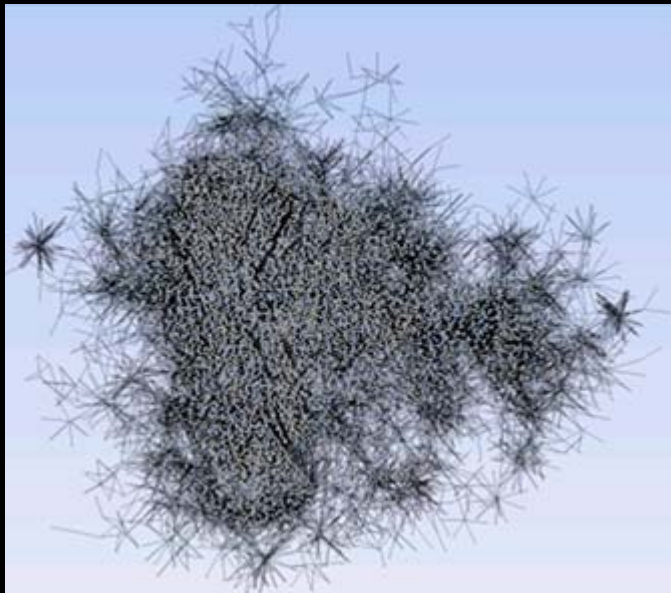
Logical zones capture business requirements



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

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

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**

Thank you

- Questions?

- Contact:

ddexter@cisco.com