Network Security Policy Validation

Netsecure '09

Susan Hinrichs
Network Geographics
shinrich@network-geographics.com

networkGEOGRAPHICS
guides to your network

Outline

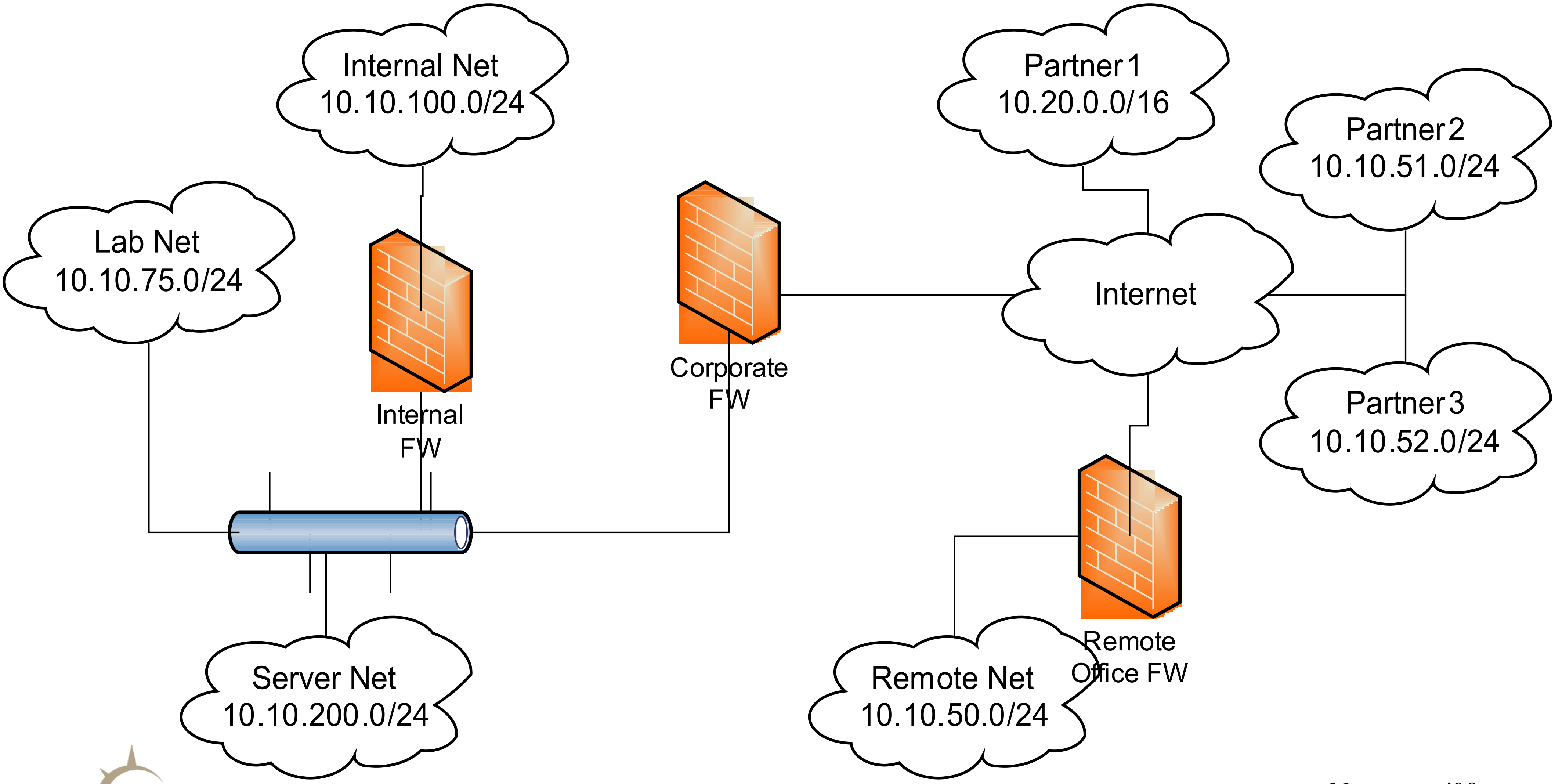
- Basics of Firewalls and Security Appliances
- Network Security Policy
- Network Security Policy Validation
- Policy Validation Scenario

Who am I?

- Currently
  - Part-time lecturer on Computer Security at UIUC
    - http://www.cs.illinois.edu/class/sp09/cs460
  - Develop network security analysis algorithms at Network Geographics
    - http://www.network-geographics.com
  - Working with netfilter and embedded systems
  - Certified Information Systems Auditor, CISA
- In the past
  - Security management architect at Cisco Systems
  - Developed NT firewall with Monticello startup
  - Worked on NT multi-level security feasibility study
  - PhD in Computer Science from Carnegie Mellon
  - BS from UIUC

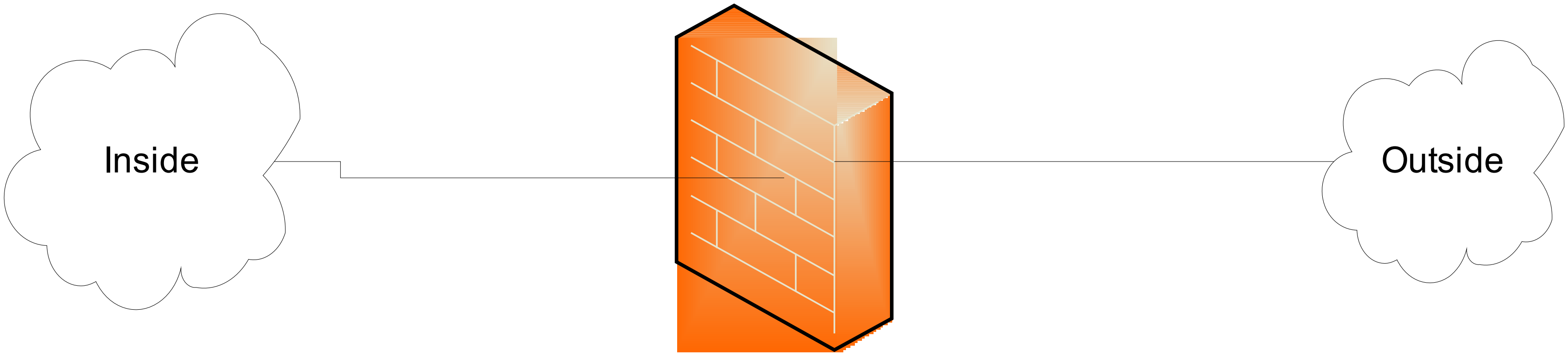
Security is not a point product

But Firewalls Can Be Important Enforcement Element



Firewall Goal

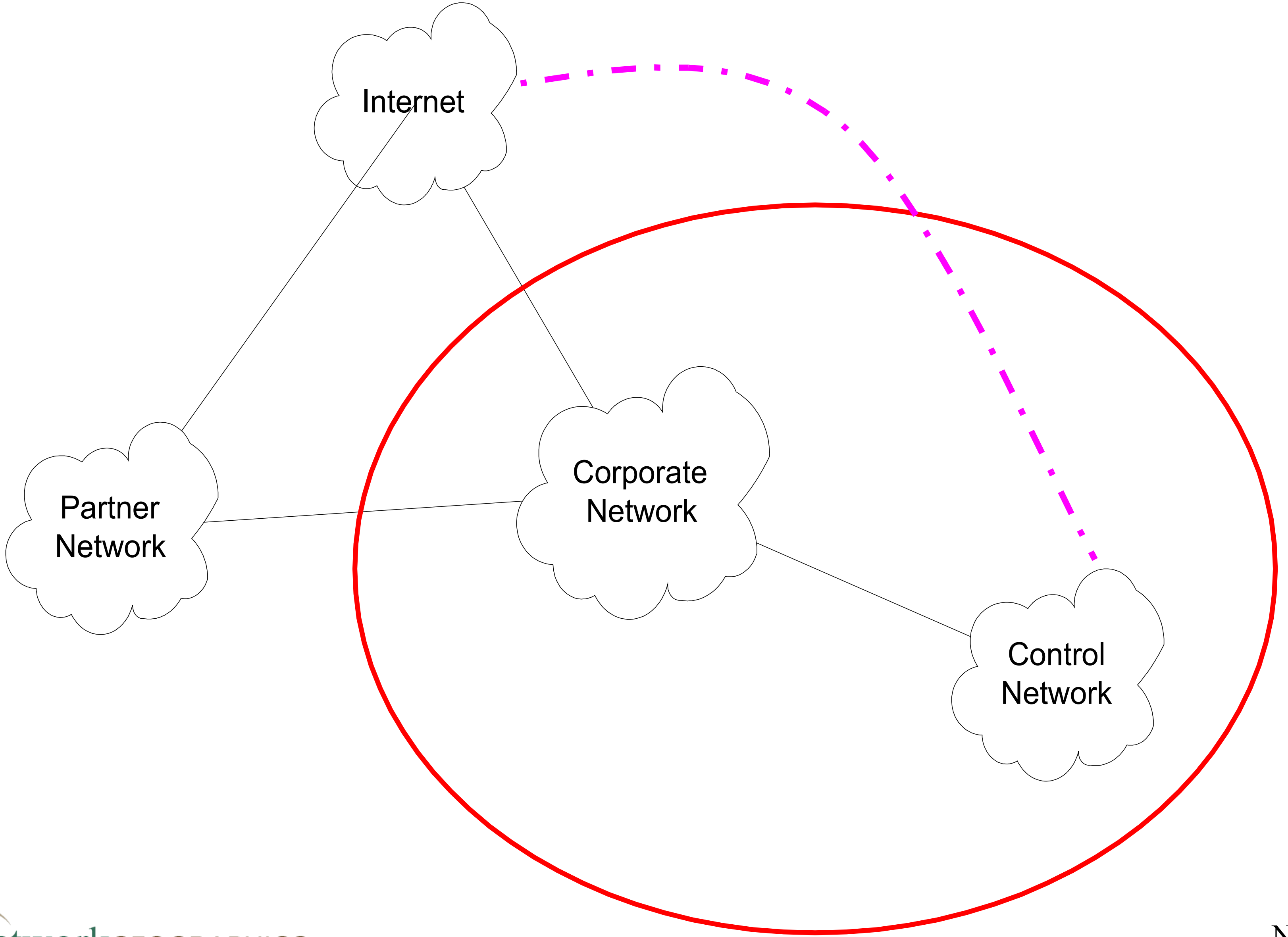
- Control traffic flow
- Insert after-the-fact security by wrapping or interposing a filter on network traffic



Firewall Deployments Expanding

- Network Security Architectures become more extensive
- No longer sufficient to have a single firewall protecting you from “Internet”
  - Must coordinate multiple sites
  - May have multiple levels of traffic paranoia within an organization
  - May have multiple paths
- Must understand traffic flow

Security Domain/Zone



networkGEOGRAPHICS
guides to your network

Firewall Functions Expanding

Firewalls evolve to security appliances and UTMs

- Perform more functions as long as they have reconstructed the traffic

Common today:

- Packet filtering, address translation, stateful inspection, IPSec

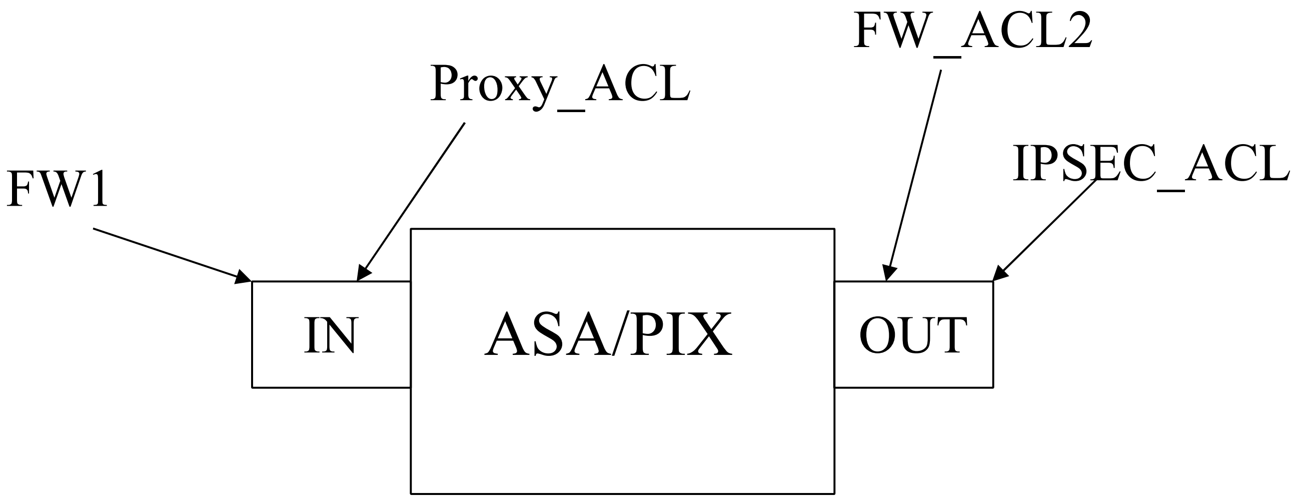
Common tomorrow?

- Deeper HTTP filtering, Spam filtering, virus scans, IDS, QoS

Access Control Lists (ACLs)

- Used to define traffic streams
  - Bind ACL’s to interface and action
- Multiple features can be controlled by ACLs
  - Packet filtering, NAT, stateful inspection, AAA, IPSec, URL filtering
- Access Control Entry (ACE) defines the 5-tuple
- ACL runtime lookup
  - Linear
  - N-dimensional tree lookup (PIX/ASA Turbo ACL)
  - HW classification assists

Example Action Bindings

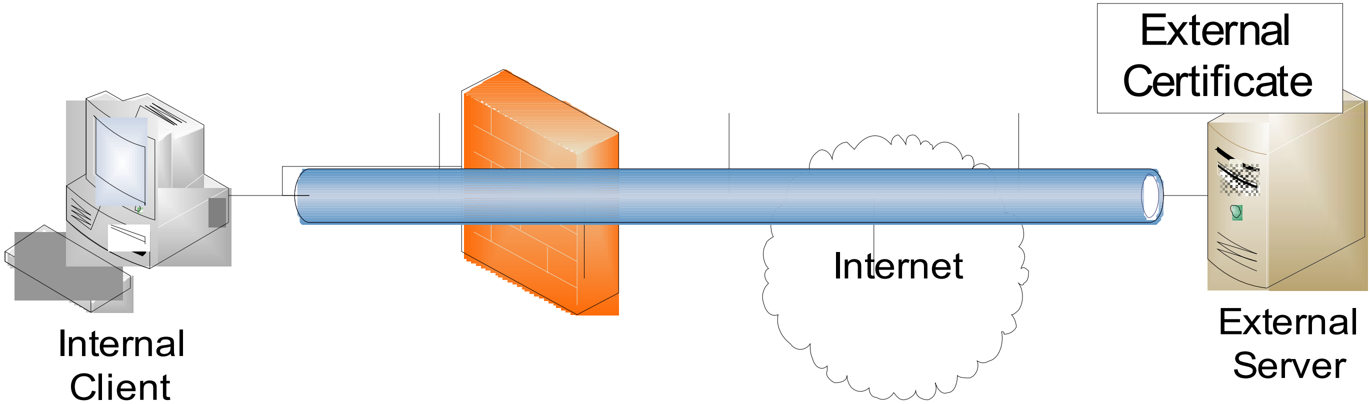


```
access-list FW1 permit tcp 192.168.1.0 255.255.255.0 any eq 80
access-list FW1 ...
access-group in inside FW1
```

networkGEOGRAPHICS
guides to your network

Tunnels in the Evolving Network Environment

- Firewalls cannot look into tunneled traffic
- At most can do some header filtering
  - Can tunnel many protocols through HTTP

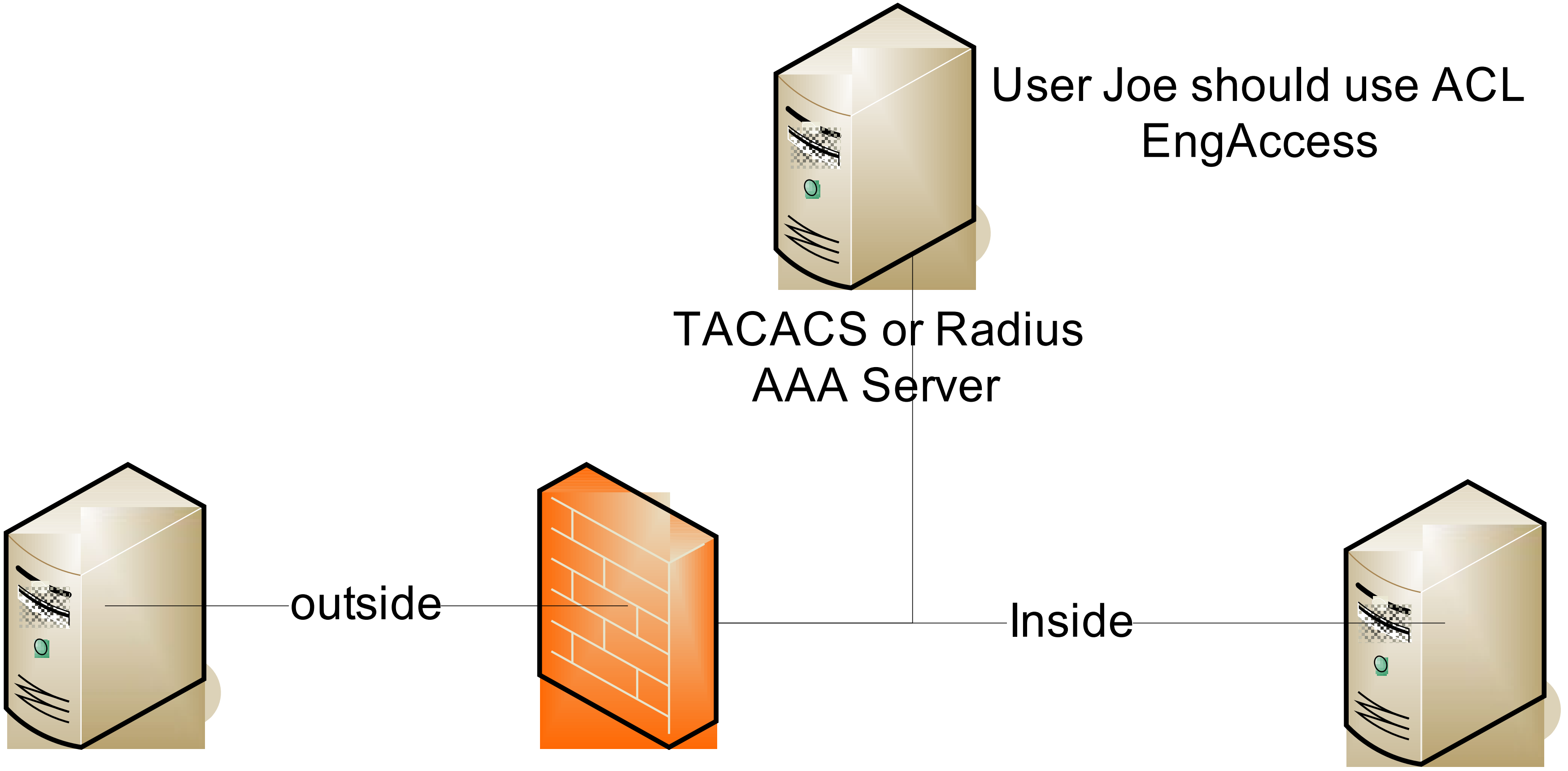


networkGEOGRAPHICS
guides to your network

Challenge of Faster Rate of Change

- Attacks change too quickly
  - Traditional FW protocol analysis is relative fixed
    - Changes with new device image
  - Intrusion Protection Systems (IDS inline) may evolve to replace traditional firewall protocol analysis
- Blurring security domain perimeters
  - Who are you protecting from whom?
  - User-aware enforcement
    - AAA servers
    - Network Admission Control/Network Access Protection

AAA Scenario



User Joe should use ACL EngAccess

TACACS or Radius AAA Server

Traffic from X must be authenticated via HTTP

NAC/NAP

- Cisco white paper
  - http://www.cisco.com/en/US/solutions/collateral/ns340/ns394
- Microsoft white paper
  - http://technet.microsoft.com/en-us/network/bb545879.aspx
- Enforcement remains in the network but knowledge of endpoint is added
  - Requires software on the client to communicate client state to enforcement device
  - New client to enforcing device protocol. Must detect subversive clients
  - Must ensure that this software runs on all clients
- Enforcement devices uses TACACS to query AAA Server about policy that applies to client profile.

Is the Firewall Dead?

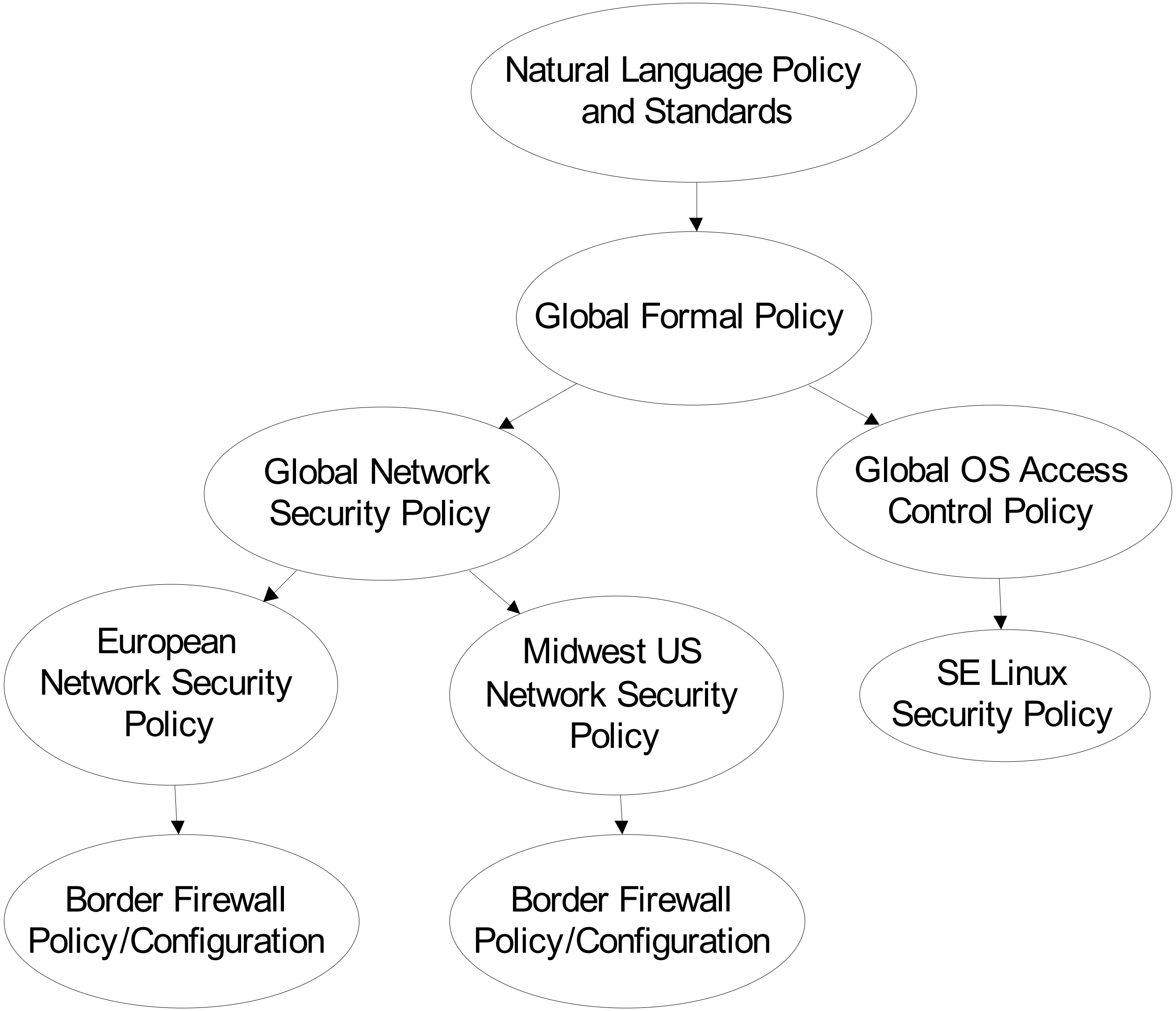
- I don't think so
- Firewall Technology continues to emerge
- Endpoint enforcement will continue
  - Personal firewalls
  - But network firewalls provide layered security
- IPv6 Roll Out may reveal many implementation flaws well addressed by network firewalls
  - Reminiscent of IPv4 roll out on Windows

Network Security Policy

Good Policy Means Effective Network Security

- Good security policy separates secure from insecure states
  - Defines what it means to be secure
- Implementation enforces the policy
- Policy is no good unless it is accurately enforced
- A “quality” network deployment accurately reflects policy

Policy Refinement Hierarchy



Natural Language Policy and Standards
Global Formal Policy
Global Network Security Policy
Global OS Access Control Policy
European Network Security Policy
Midwest US Network Security Policy
SE Linux Security Policy
Border Firewall Policy/Configuration
Border Firewall Policy/Configuration

Policy Refinement

- The layers between the organizational policy and the implementation may be sketchy
  - Visio Diagram
    - ok
  - Organizational standards
    - good
  - Something Bob wrote on the back of a napkin
    - better than nothing I guess
  - Knowledge in Bob's head
    - Bad!

Example Partner Policy

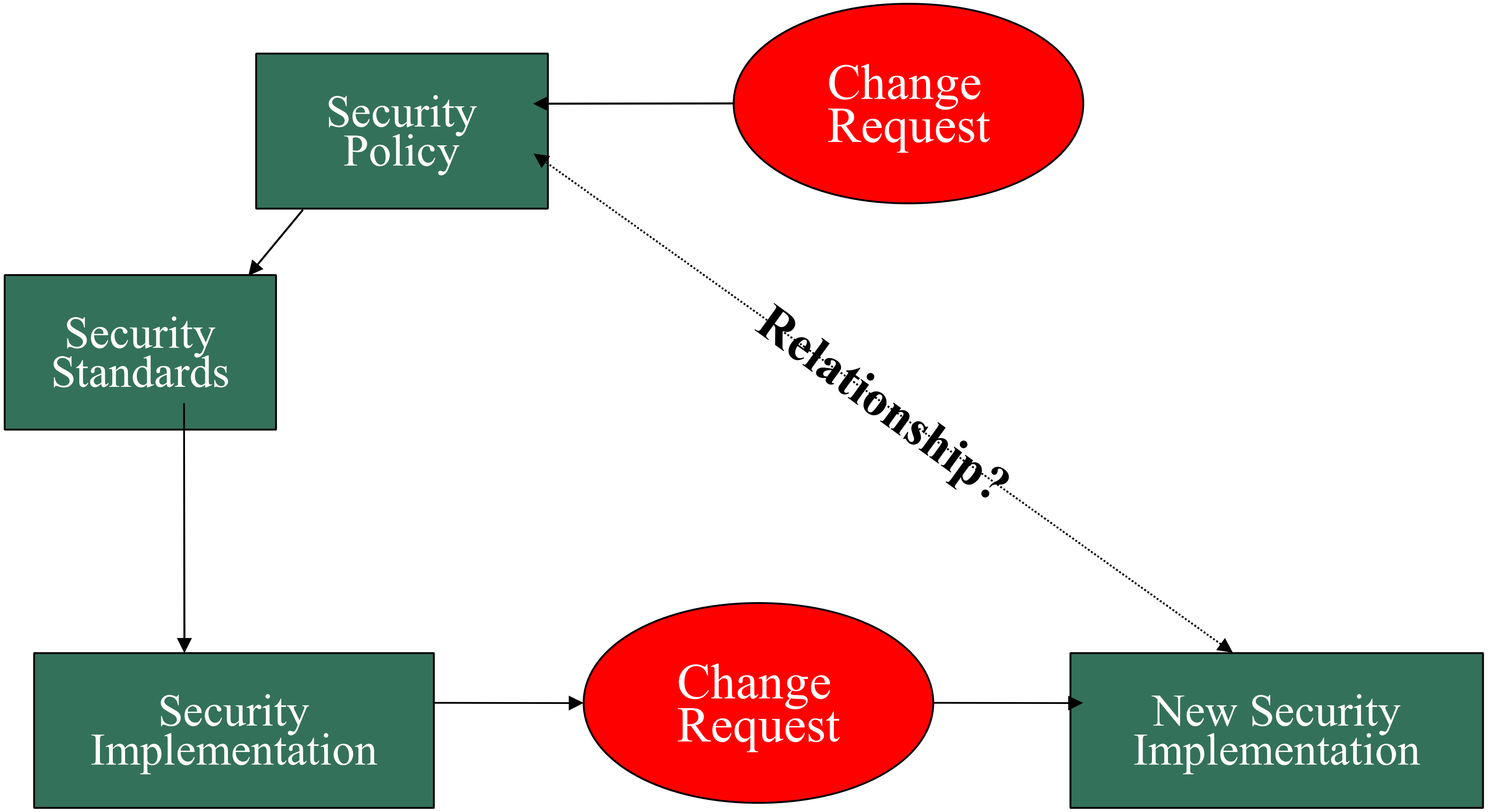
- Organizational Policy
  - “Partners should only be given access to a specific set of partner servers and only necessary communication protocols should be permitted. Partner traffic must be filtered and analyzed before reaching company servers”
- Refine into firewall policy
  - Ensure that traffic from partner networks can only access shared servers using protocols http, ssh, and https. All communication should be proxied

Example Partner Policy

- Can express firewall policy as a formal constraint

-
  ```
  source_address ^ (partner_net1 | ...  |
  partner_net_n) &
    destination_address ^ (internal_server_net) &
    destination_svc ^ (HTTP | HTTPS | SSH) &
    action = (permit & inspect)
  otherwise action = deny
  ```

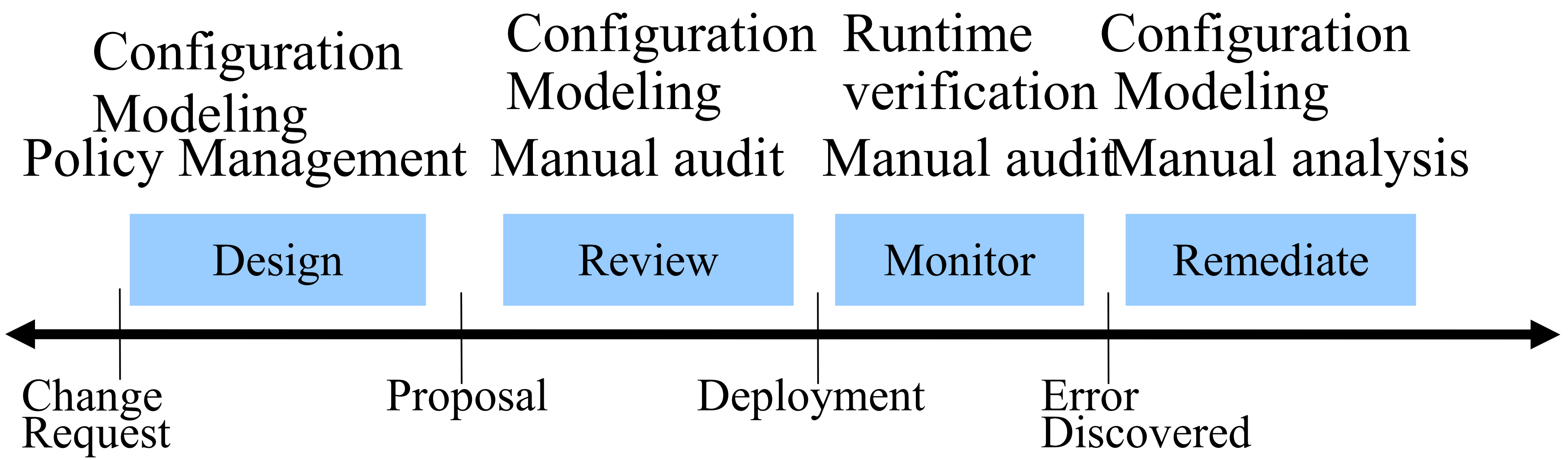
Policy/Implementation Drift



networkGEOGRAPHICS
guides to your network

Policy Validation

Security Implementation Timeline



Configuration Modeling
Policy Management

Design

Configuration Modeling
Manual audit

Review

Runtime verification
Manual audit

Monitor

Configuration Modeling
Manual analysis

Remediate

Change Request

Proposal

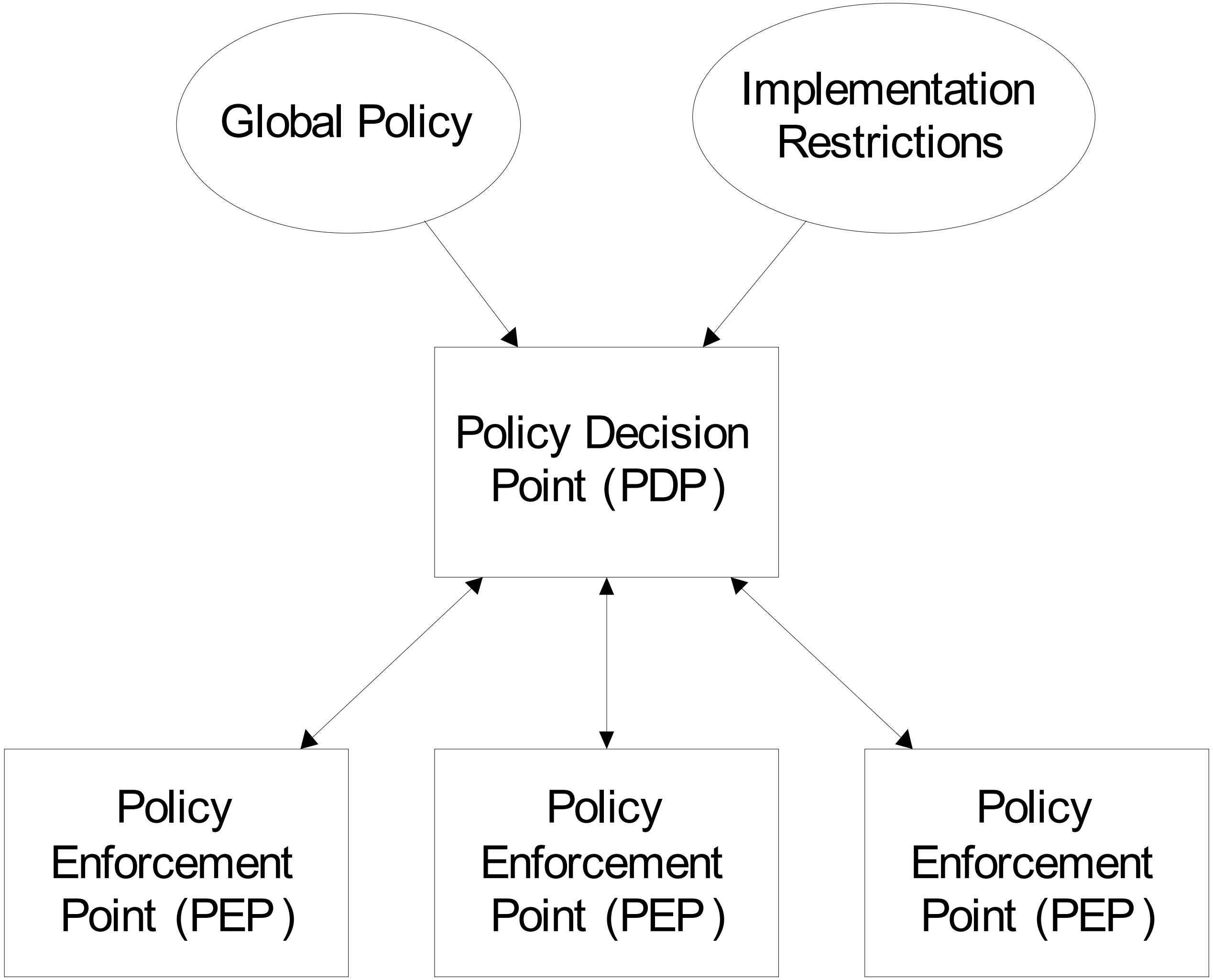
Deployment

Error Discovered

Manual Audit

- Look at configuration files
  - Compare to policy/standard expectations
- Tedious and error prone
- Requires expert knowledge of the technology to correctly interpret the configuration files.

IETF Policy Management Model


Global Policy
Implementation Restrictions
Policy Decision Point (PDP)
Policy Enforcement Point (PEP)
Policy Enforcement Point (PEP)
Policy Enforcement Point (PEP)

Firewall Policy Management

- Single Device GUI
  - Offered by most vendors
  - Raise abstraction from CLI
- Multi-Device Management
  - CSM, NSM, Checkpoint
  - Able to share some implementation specification between devices
- Network-Aware Policy Management
  - Solsoft and Cisco Secure Policy Manager (CSPM)
  - Define network topology and desired policy
  - Management tool calculates the configuration for managed devices

Auditing and Policy Management

- If policy is used to drive operation
  - Auditing can also occur at a higher layer of abstraction
- Most likely there is still a gap between the organizational policy and the device policy
  - Must be bridged by reviewer

Runtime Verification Tools

- Network Scanning tools
  - ISS, nmap, nessus
  - Verifies policy by sending packets
    - Indicates whether traffic is permitted or not, relative to scanner position in network
  - Must coordinate scans
    - Scan traffic is generally seen as hostile by the network security environment
  - Black box
    - Doesn't give indication of how packet is processed (Are proxies applied? Are URL's filtered?)
  - Still need remediation

Nmap output

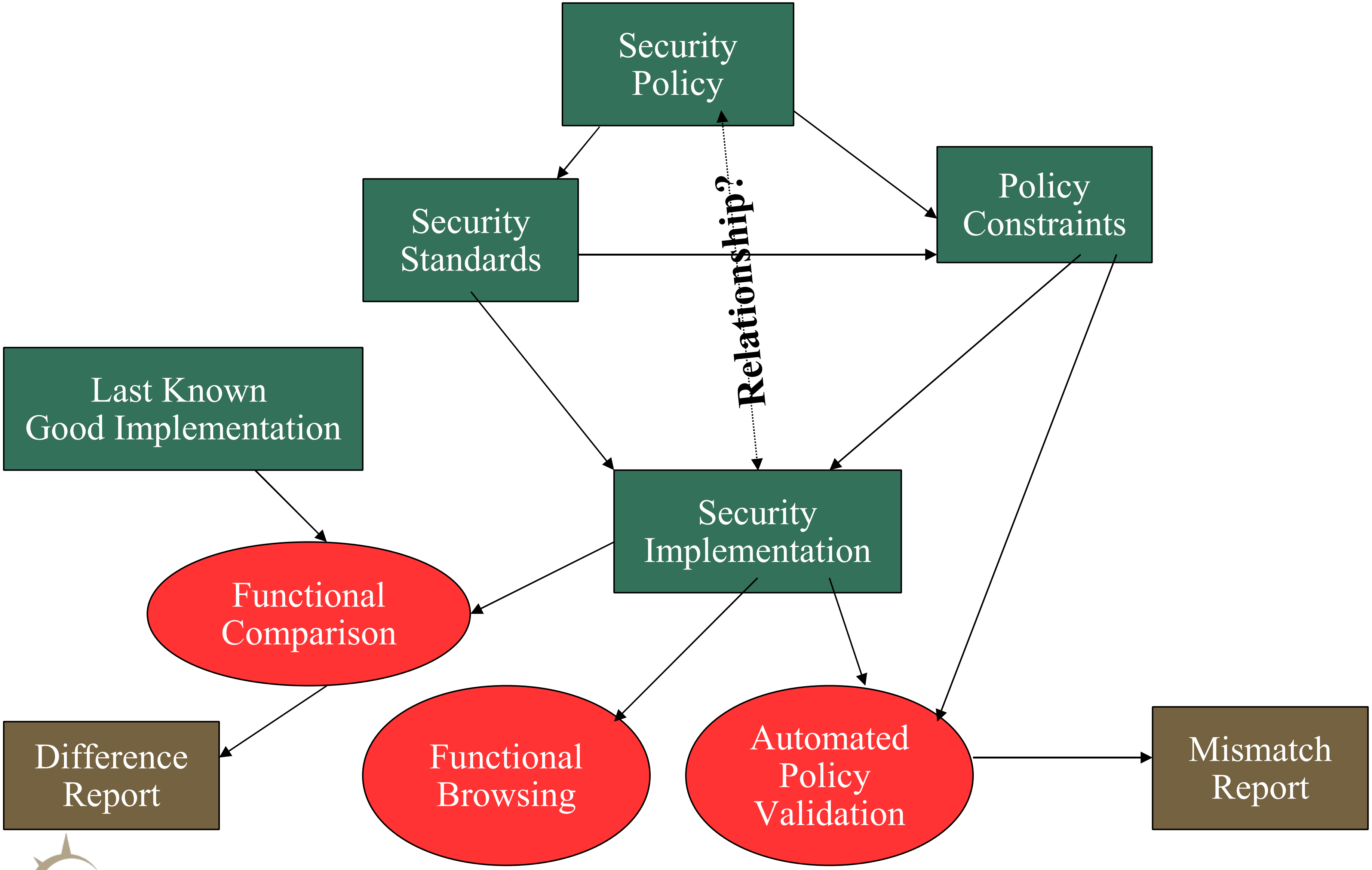
- Can indicate open ports and make guesses at SW versions

```
Interesting ports on 192.168.56.58:
Not shown: 1692 closed ports
PORT     STATE SERVICE      VERSION
80/tcp   open  http         HP PhotoSmart 8450 printer http config (Virata embedded
httpd 6_0_1)
139/tcp  open  netbios-ssn?
9100/tcp open  jetdirect?
9101/tcp open  jetdirect?
9102/tcp open  jetdirect?
Service Info: Device: printer

Interesting ports on 192.168.56.102:
Not shown: 1695 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 4.7 (protocol 2.0)
111/tcp open  rpc

Interesting ports on 192.168.56.107:
Not shown: 1692 filtered ports
PORT     STATE  SERVICE        VERSION
80/tcp   open   http           Apache httpd 2.0.55 ((Win32) PHP/4.4.2)
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds   Microsoft Windows XP microsoft-ds
3306/tcp open   mysql          MySQL (unauthorized)
4000/tcp closed remoteanything
Service Info: OS: Windows
```

Config Modeling in Security QA



networkGEOGRAPHICS guides to your network

Network Configuration Analysis Types

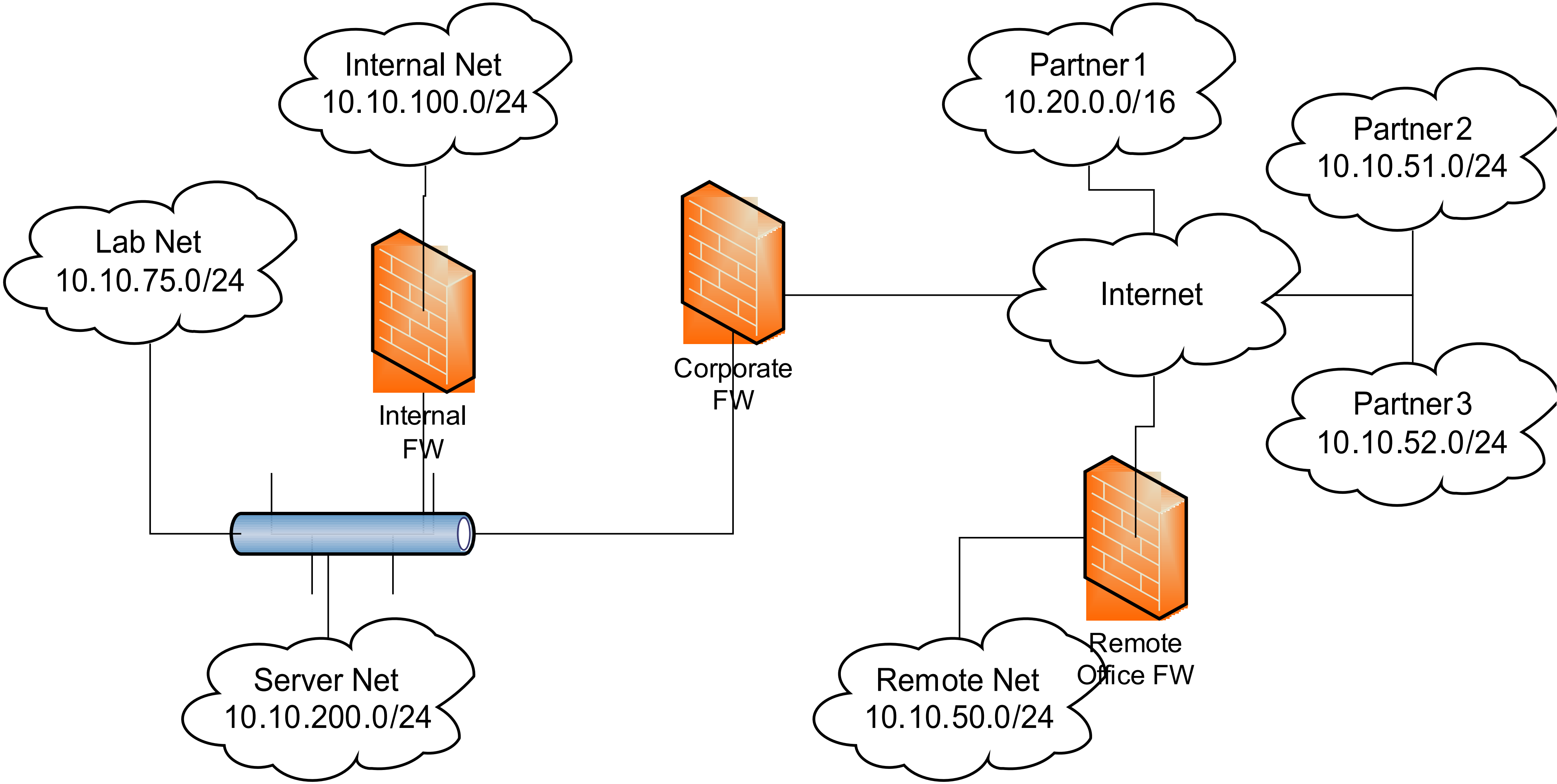
- Rule list conflict analysis
  - Find entries in the rule list (ACL) that conflict with each other
  - Many tools provide this including Netscreen device and CSM
- Flow Analysis
  - Determine how particular addresses will flow through a network
  - Provided in many larger compliance tool sets including Red Seal, and OpNet

Network Configuration Analysis Types

- All communication
  - Normalize and report on how all packets will be processed
  - InfoSecter and AlgoSec
- Functional Comparison
  - Given two configuration descriptions identify the sets of packets that will be processed differently
  - InfoSecter
- Constraint Analysis
  - Define and enforce formal constraint on packet processing
  - InfoSecter and Skybox

Validation Example

Example Network



networkGEOGRAPHICS
guides to your network

InfoSecter, Tool for Network Security Professionals

- Implements analysis on efficient model built from security device configuration
- Multi-vendor
  - Cisco (PIX, ASA, FWSM, IOS), Netscreen, Checkpoint
- Cross platform
  - Windows and Linux
- Released 1.1 in October '08

Change Request

- You've been told to deploy a new Wiki Server and make it available to all company employees.

Design

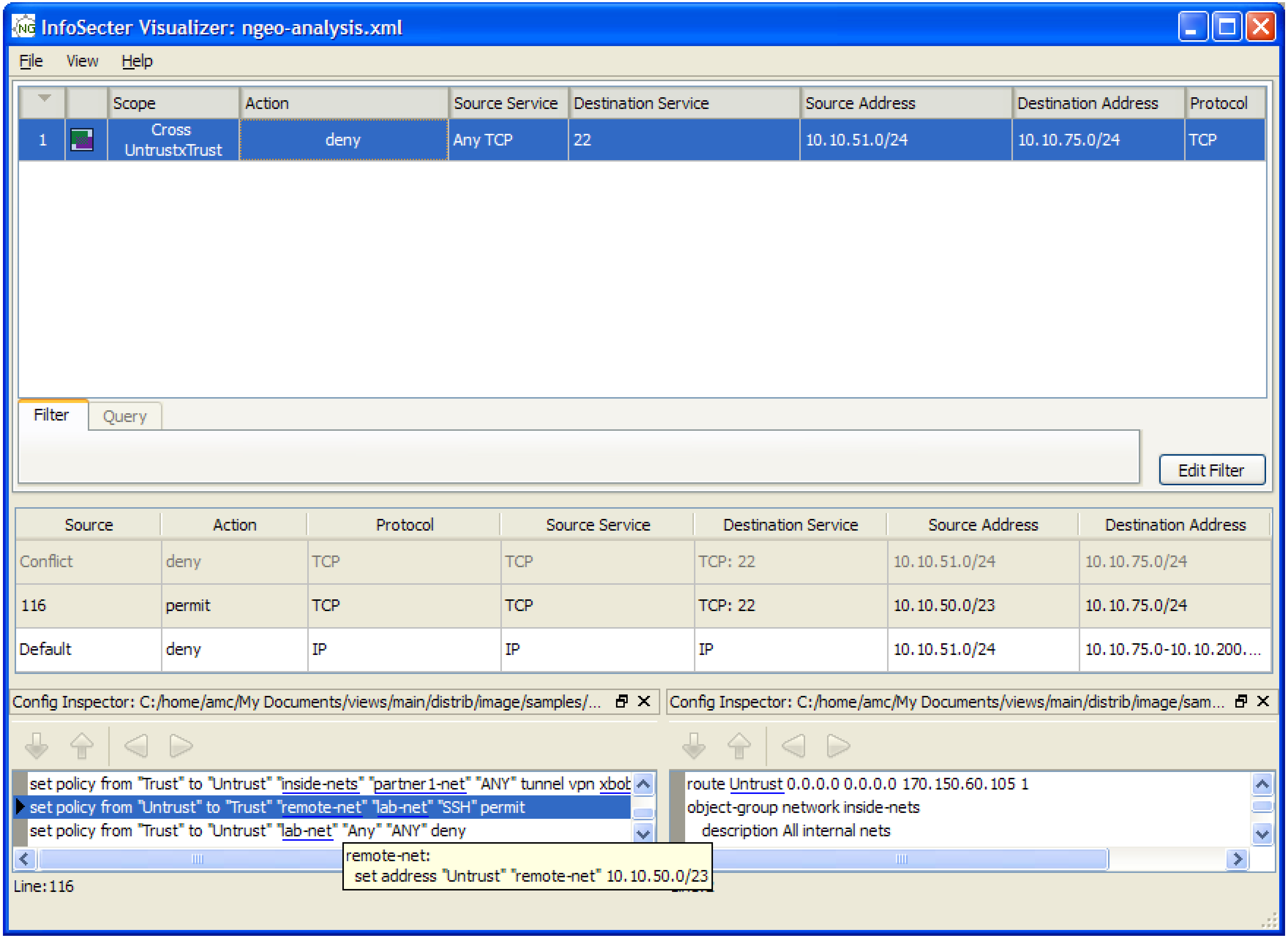
- Use Policy Management
  - Enter change into global policy
  - Policy System derives new config for external firewall and remote office firewall
- Do equivalent manual analysis to determine what changes need to be made

Review

- Manual Audit
  - Have a review meeting. Look at the new configuration. Perform a text different to see what lines have changed.
  - Maker/checker model. Review by someone who is not the configuration author is more likely to catch errors
- Configuration Modeling
  - Perform a functional difference to determine how packets will be processed differently

Cross Configuration Conflicts

- Goal: Find functional changes in config
  - Functional configuration comparison
  - Focus reviews to subset of lines that cause functionality to change
- Addresses review and design stages



		Scope	Action	Source Service	Destination Service	Source Address	Destination Address	Protocol
1	🟩	Cross UntrustxTrust	deny	Any TCP	22	10.10.51.0/24	10.10.75.0/24	TCP

Source	Action	Protocol	Source Service	Destination Service	Source Address	Destination Address
Conflict	deny	TCP	TCP	TCP: 22	10.10.51.0/24	10.10.75.0/24
116	permit	TCP	TCP	TCP: 22	10.10.50.0/23	10.10.75.0/24
Default	deny	IP	IP	IP	10.10.51.0/24	10.10.75.0-10.10.200....

Config Inspector: C:/home/amc/My Documents/views/main/distrib/image/samples/...

```
set policy from "Trust" to "Untrust" "inside-nets" "partner1-net" "ANY" tunnel vpn xbot
set policy from "Untrust" to "Trust" "remote-net" "lab-net" "SSH" permit
set policy from "Trust" to "Untrust" "lab-net" "Any" "ANY" deny
```

```
remote-net:
 set address "Untrust" "remote-net" 10.10.50.0/23
```

Line:116

Config Inspector: C:/home/amc/My Documents/views/main/distrib/image/sam...

```
route Untrust 0.0.0.0 0.0.0.0 170.150.60.105 1
object-group network inside-nets
  description All internal nets
```

Monitoring

- Manual Audit
  - Periodically bring in external auditors to review configurations. Ensure that they are accurately implementing the network security policy.
- Runtime verification
  - External auditors are likely to supplement manual reviews of configuration with black box scanning of the environment.
- Configuration Modeling
  - Run constraints daily or on each change to catch policy problems.

Query and Constraint Checks

- Goal: Automate policy validation
  - Create formal statements about packet handling from policy
  - Report matches (query) or mismatches (constraint)
  - Analyzer is completely scriptable
    - Check automatically at key points in process
    - Rapidly check multiple configurations
  - Allow contributions from multiple stake holders
- Addresses review and monitoring stages

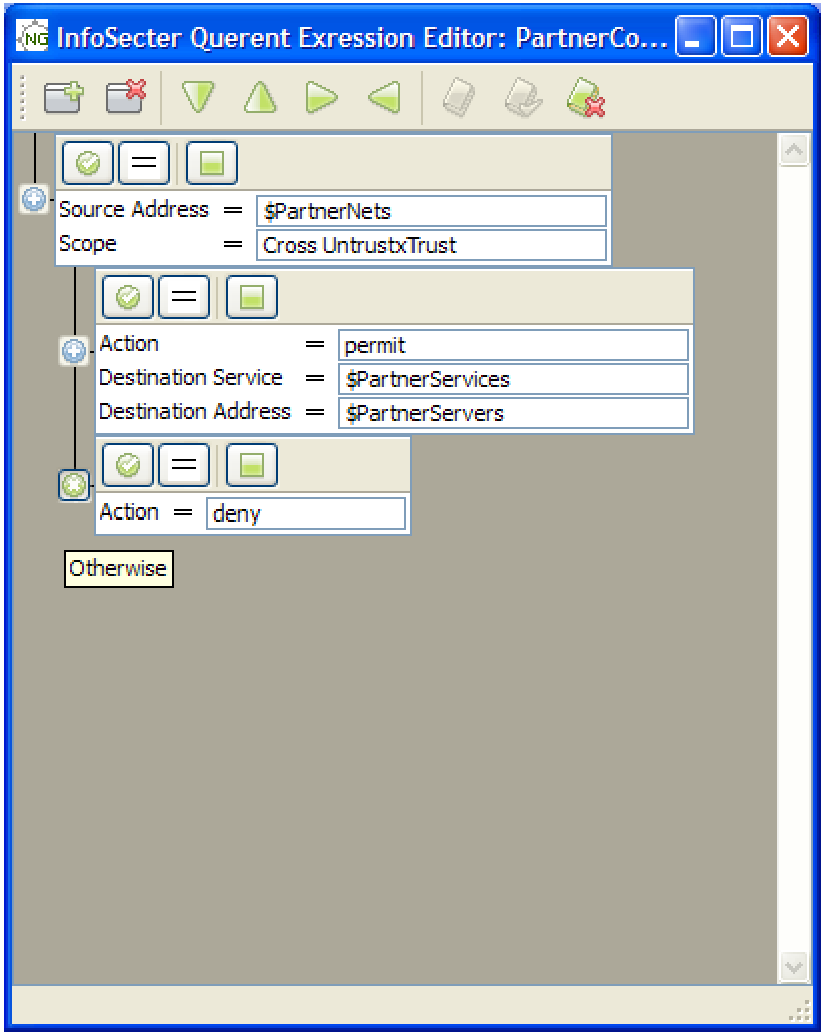
Example Partner Constraint

- Source Address in PartnerNets &

  ((Destination Address = SharedServer &
  Destination Service in PartnerServices &
  Action = Permit)

  (Otherwise Action = Deny))

Constraint in Expression Editor

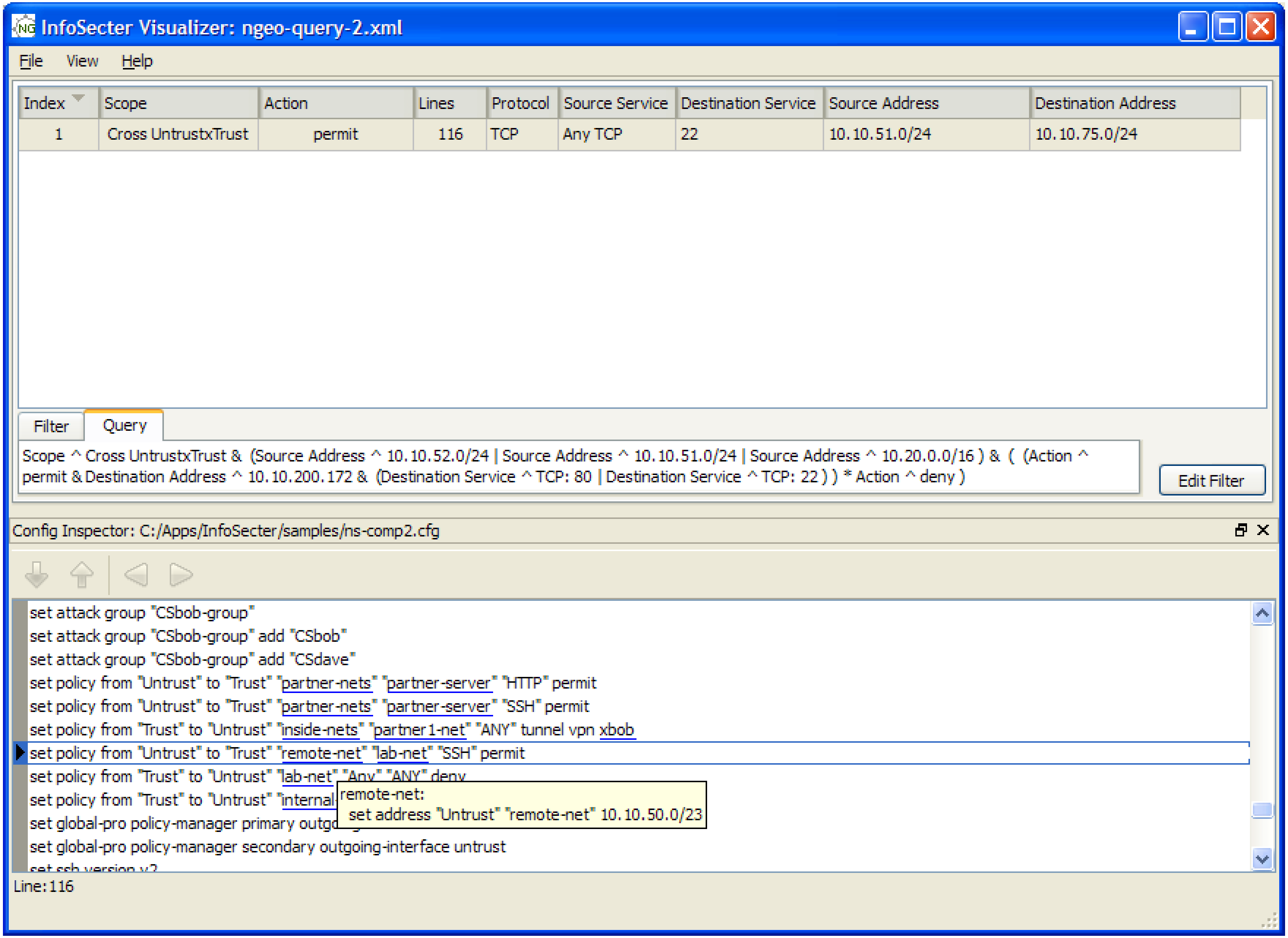


InfoSecter Querent Exression Editor: PartnerCo...

Source Address	=	$PartnerNets
Scope	=	Cross UntrustxTrust

Action	=	permit
Destination Service	=	$PartnerServices
Destination Address	=	$PartnerServers

Action	=	deny


InfoSecter Visualizer: ngeo-query-2.xml
File
View
Help
Filter
Query
Edit Filter
Config Inspector: C:/Apps/InfoSecter/samples/ns-comp2.cfg

Index	Scope	Action	Lines	Protocol	Source Service	Destination Service	Source Address	Destination Address
1	Cross UntrustxTrust	permit	116	TCP	Any TCP	22	10.10.51.0/24	10.10.75.0/24

Scope ^ Cross UntrustxTrust & (Source Address ^ 10.10.52.0/24 | Source Address ^ 10.10.51.0/24 | Source Address ^ 10.20.0.0/16) & ((Action ^ permit & Destination Address ^ 10.10.200.172 & (Destination Service ^ TCP: 80 | Destination Service ^ TCP: 22)) * Action ^ deny)

```
set attack group "CSbob-group"
set attack group "CSbob-group" add "CSbob"
set attack group "CSbob-group" add "CSdave"
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "HTTP" permit
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "SSH" permit
set policy from "Trust" to "Untrust" "inside-nets" "partner1-net" "ANY" tunnel vpn xbob
set policy from "Untrust" to "Trust" "remote-net" "lab-net" "SSH" permit
set policy from "Trust" to "Untrust" "lab-net" "Any" "ANY" deny
set policy from "Trust" to "Untrust" "internal
set global-pro policy-manager primary outgo
set global-pro policy-manager secondary outgoing-interface untrust
set ssh version v2
```

```
remote-net:
 set address "Untrust" "remote-net" 10.10.50.0/23
```

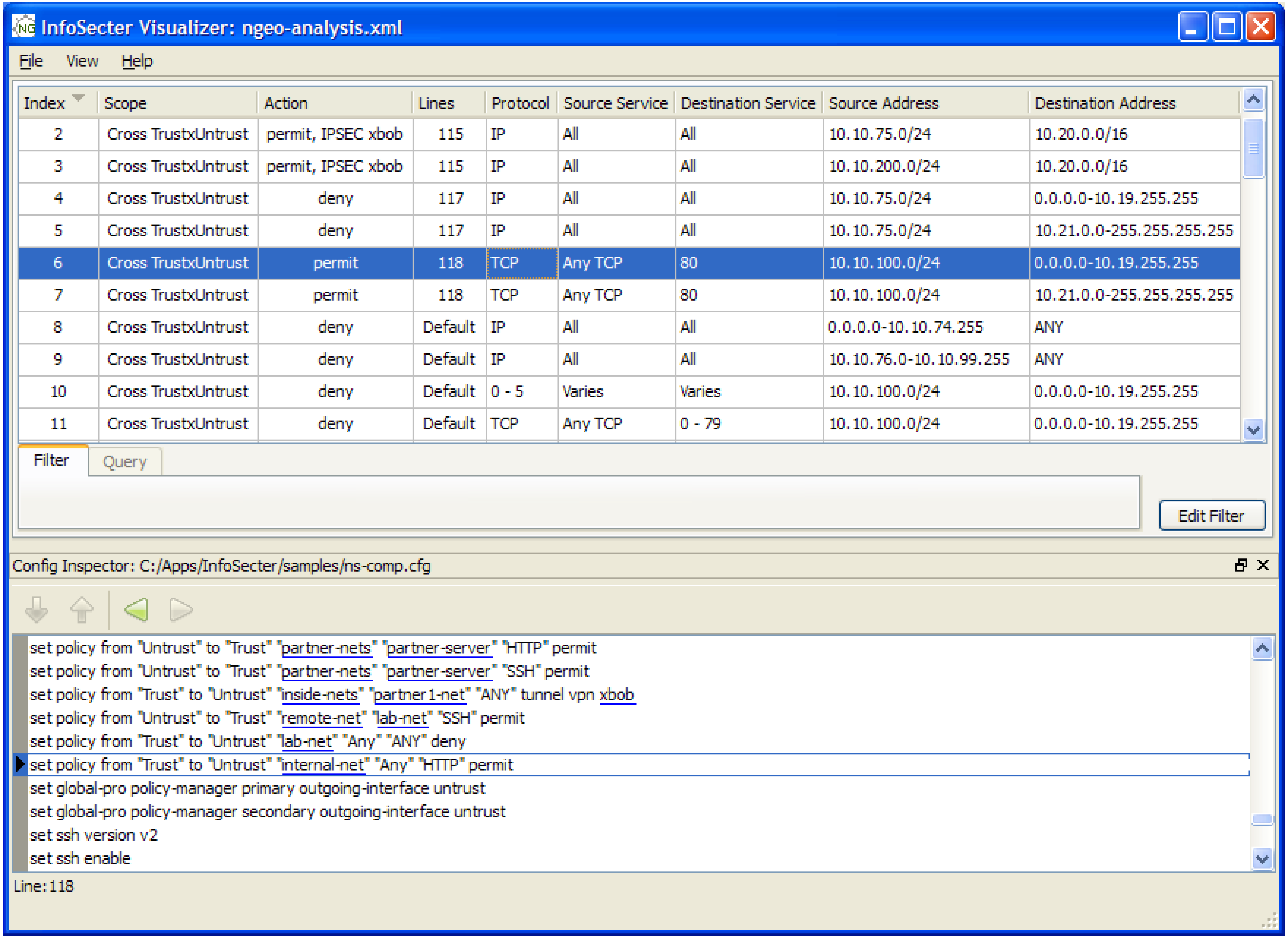
Line: 116

Remediation

- You've been told of a security or functionality error. Now you must fix it.
- Manual Audit
  - Look at configurations for the error.
- Configuration Modeling
  - Use a dissection and browsing to hone in on the configuration lines that affect the problem behavior

Dissection and Browsing

- Goal: Debug known config or learn about new config
  - Disambiguate configuration. Each potential packet matches exactly one slice.
  - Use filtering to focus on areas of interest
  - Find effective rules rapidly and reliably
  - Identify lines to address for remediation
- For design, review and remediation stages



Index	Scope	Action	Lines	Protocol	Source Service	Destination Service	Source Address	Destination Address
2	Cross TrustxUntrust	permit, IPSEC xbob	115	IP	All	All	10.10.75.0/24	10.20.0.0/16
3	Cross TrustxUntrust	permit, IPSEC xbob	115	IP	All	All	10.10.200.0/24	10.20.0.0/16
4	Cross TrustxUntrust	deny	117	IP	All	All	10.10.75.0/24	0.0.0.0-10.19.255.255
5	Cross TrustxUntrust	deny	117	IP	All	All	10.10.75.0/24	10.21.0.0-255.255.255.255
6	Cross TrustxUntrust	permit	118	TCP	Any TCP	80	10.10.100.0/24	0.0.0.0-10.19.255.255
7	Cross TrustxUntrust	permit	118	TCP	Any TCP	80	10.10.100.0/24	10.21.0.0-255.255.255.255
8	Cross TrustxUntrust	deny	Default	IP	All	All	0.0.0.0-10.10.74.255	ANY
9	Cross TrustxUntrust	deny	Default	IP	All	All	10.10.76.0-10.10.99.255	ANY
10	Cross TrustxUntrust	deny	Default	0 - 5	Varies	Varies	10.10.100.0/24	0.0.0.0-10.19.255.255
11	Cross TrustxUntrust	deny	Default	TCP	Any TCP	0 - 79	10.10.100.0/24	0.0.0.0-10.19.255.255

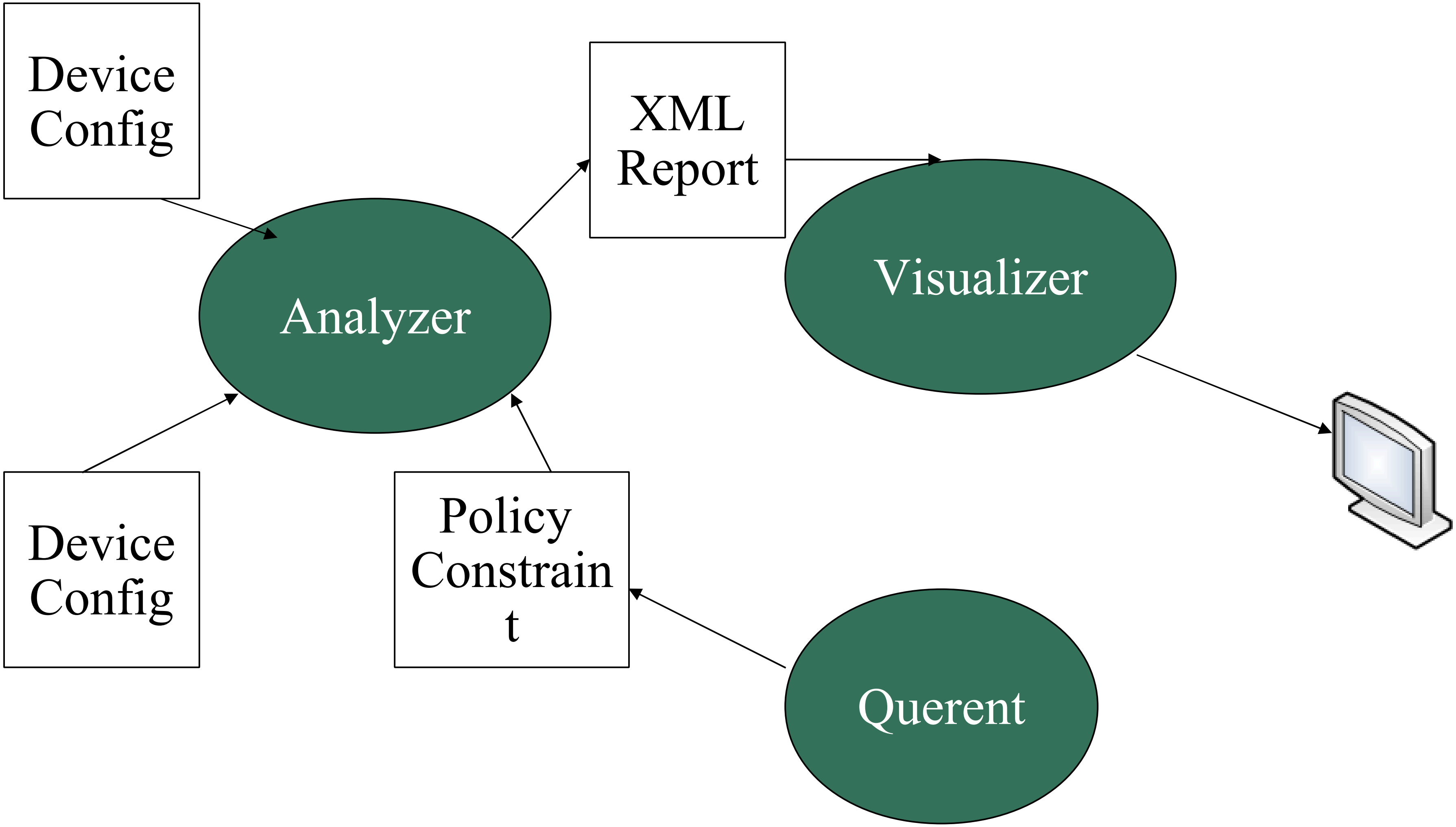
Config Inspector: C:/Apps/InfoSecter/samples/ns-comp.cfg

```
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "HTTP" permit
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "SSH" permit
set policy from "Trust" to "Untrust" "inside-nets" "partner1-net" "ANY" tunnel vpn xbob
set policy from "Untrust" to "Trust" "remote-net" "lab-net" "SSH" permit
set policy from "Trust" to "Untrust" "lab-net" "Any" "ANY" deny
set policy from "Trust" to "Untrust" "internal-net" "Any" "HTTP" permit
set global-pro policy-manager primary outgoing-interface untrust
set global-pro policy-manager secondary outgoing-interface untrust
set ssh version v2
set ssh enable
```

Line:118

networkGEOGRAPHICS
guides to your network

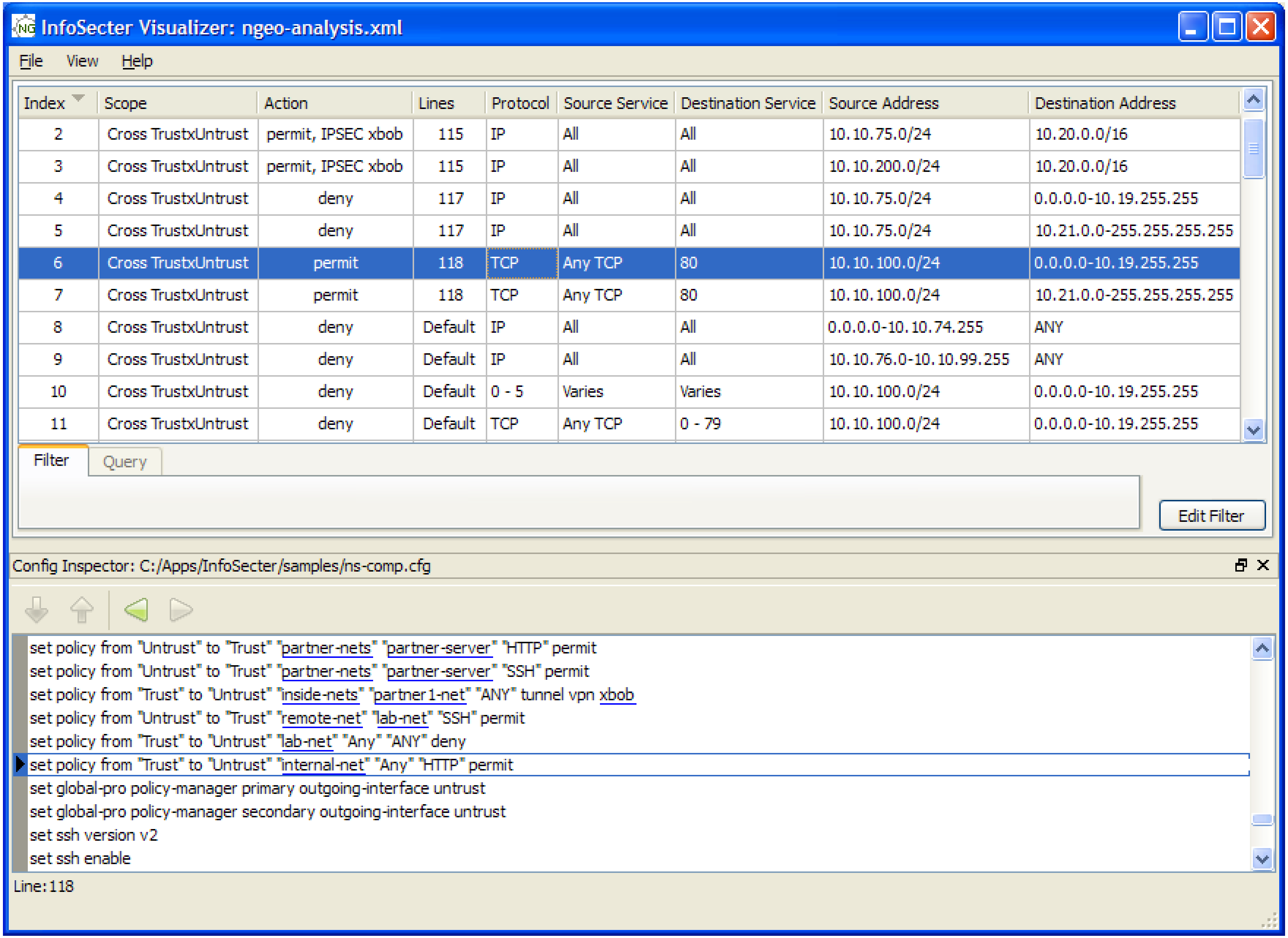
InfoSecter Architecture



networkGEOGRAPHICS
guides to your network

Dissection and Browsing

- Goal: Debug known config or learn about new config
  - Disambiguate configuration. Each potential packet matches exactly one slice.
  - Use filtering to focus on areas of interest
  - Find effective rules rapidly and reliably
  - Identify lines to address for remediation
- For design, review and remediation stages



Index	Scope	Action	Lines	Protocol	Source Service	Destination Service	Source Address	Destination Address
2	Cross TrustxUntrust	permit, IPSEC xbob	115	IP	All	All	10.10.75.0/24	10.20.0.0/16
3	Cross TrustxUntrust	permit, IPSEC xbob	115	IP	All	All	10.10.200.0/24	10.20.0.0/16
4	Cross TrustxUntrust	deny	117	IP	All	All	10.10.75.0/24	0.0.0.0-10.19.255.255
5	Cross TrustxUntrust	deny	117	IP	All	All	10.10.75.0/24	10.21.0.0-255.255.255.255
6	Cross TrustxUntrust	permit	118	TCP	Any TCP	80	10.10.100.0/24	0.0.0.0-10.19.255.255
7	Cross TrustxUntrust	permit	118	TCP	Any TCP	80	10.10.100.0/24	10.21.0.0-255.255.255.255
8	Cross TrustxUntrust	deny	Default	IP	All	All	0.0.0.0-10.10.74.255	ANY
9	Cross TrustxUntrust	deny	Default	IP	All	All	10.10.76.0-10.10.99.255	ANY
10	Cross TrustxUntrust	deny	Default	0 - 5	Varies	Varies	10.10.100.0/24	0.0.0.0-10.19.255.255
11	Cross TrustxUntrust	deny	Default	TCP	Any TCP	0 - 79	10.10.100.0/24	0.0.0.0-10.19.255.255

Config Inspector: C:/Apps/InfoSecter/samples/ns-comp.cfg

```
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "HTTP" permit
set policy from "Untrust" to "Trust" "partner-nets" "partner-server" "SSH" permit
set policy from "Trust" to "Untrust" "inside-nets" "partner1-net" "ANY" tunnel vpn xbob
set policy from "Untrust" to "Trust" "remote-net" "lab-net" "SSH" permit
set policy from "Trust" to "Untrust" "lab-net" "Any" "ANY" deny
set policy from "Trust" to "Untrust" "internal-net" "Any" "HTTP" permit
set global-pro policy-manager primary outgoing-interface untrust
set global-pro policy-manager secondary outgoing-interface untrust
set ssh version v2
set ssh enable
```

Line:118

Policy Validation

- Deploying security devices without an understanding of policy is useless
  - Adding complexity without knowing what you are securing
- Policy validation should be considered at all points in the network security life cycle
- There are many techniques to ensure that your network security is accurately implemented
  - Use multiple techniques
  - Introduce automation to catch problems early

Questions?

http://network-geographics.com

shinrich@network-geographics.com

amc@network-geographics.com