Visualizing Firewall Configurations Using Created Voids

Shaun P. Morrissey
Georges Grinstein

Proof of Concept: Visualize a Firewall Configuration

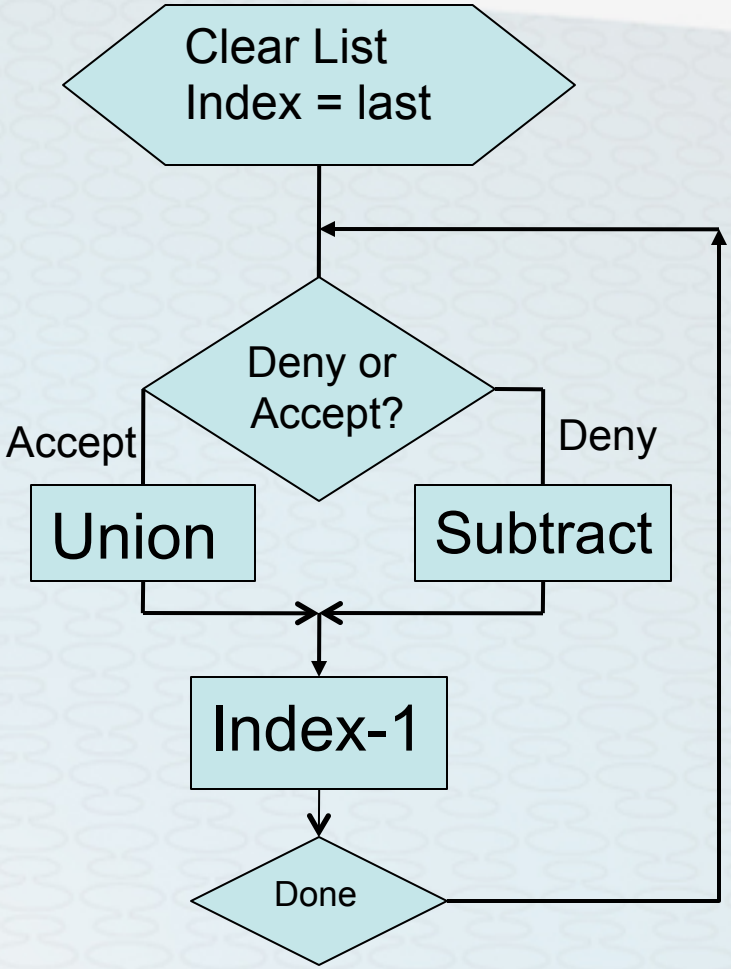
- Firewall rulesets are large, order-dependent, legacies
  - Current tools are text-editors
- Goal: Apply visualization to management & comprehension
  - Problem: no known work
- Solution: Proof of Concept
  - Build Interactive Ruleset Editor
  - Create Graphics Pipeline for Firewall Configuration
  - Try lossless visualization to start
  - Find usable dataset

Rules & Ruleset Semantics

- Firewall rule as sextuple in two parts
  - Predicate – range or interval (upper and lower limit) in five dimensions
    - Dimensions: Source Address, Source Port, Protocol Number, Destination Port, Destination Address
  - Action: Accept or Deny
- Packets processed one at a time by
  - Testing against predicates in rule order
  - First match determines action (“rule firing”)
- Predicate overlap and order-dependence can create problems

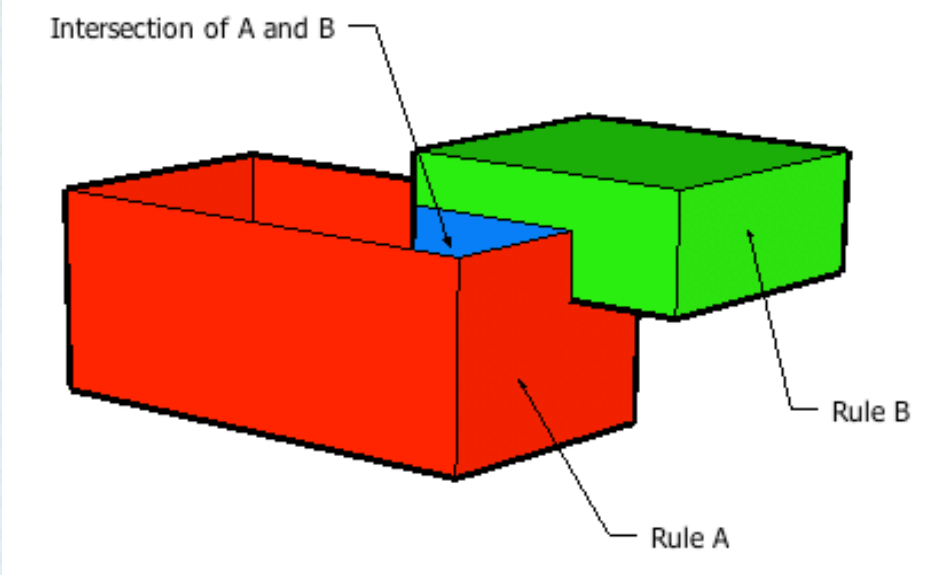
Calculate Acceptance Volume

- Guttman algorithm
- Constructive Solid Geometry
  - Integer lattice
  - 5 dimensions - Penteracts
  - Axis-aligned – intervals only
- Modifications
  - Add Provenance (rules)
  - Add Created Voids
  - Convex solid decomposition



Penteract Constructive Solid Geometry (3D analogue)

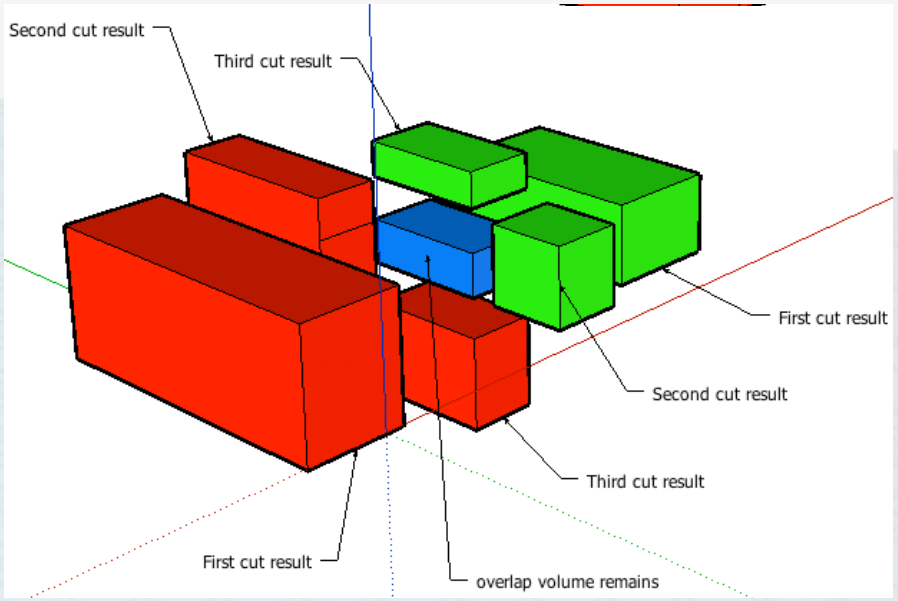
- Add Provenance of rules
  - List of rules
  - Connected to editor
- Modify Guttman: B - A
  - Normal: discard B ∩ A
  - Created Void: retain & label with joint provenance
  - Creates visualizable artifact



Top face of rule A box (red) has been opened to expose A ∩ B

Use Convex Solid Decomposition

- Simple Data Structure
  - Only penteracts required
- Calculation Complexity
  - 371,293 types of overlap
  - CSD allows one dimension at a time, five cuts, 13 cases
  - Cost: longer list
- Convex penteract can be visualized easily
  - Parallel Set Enclosure

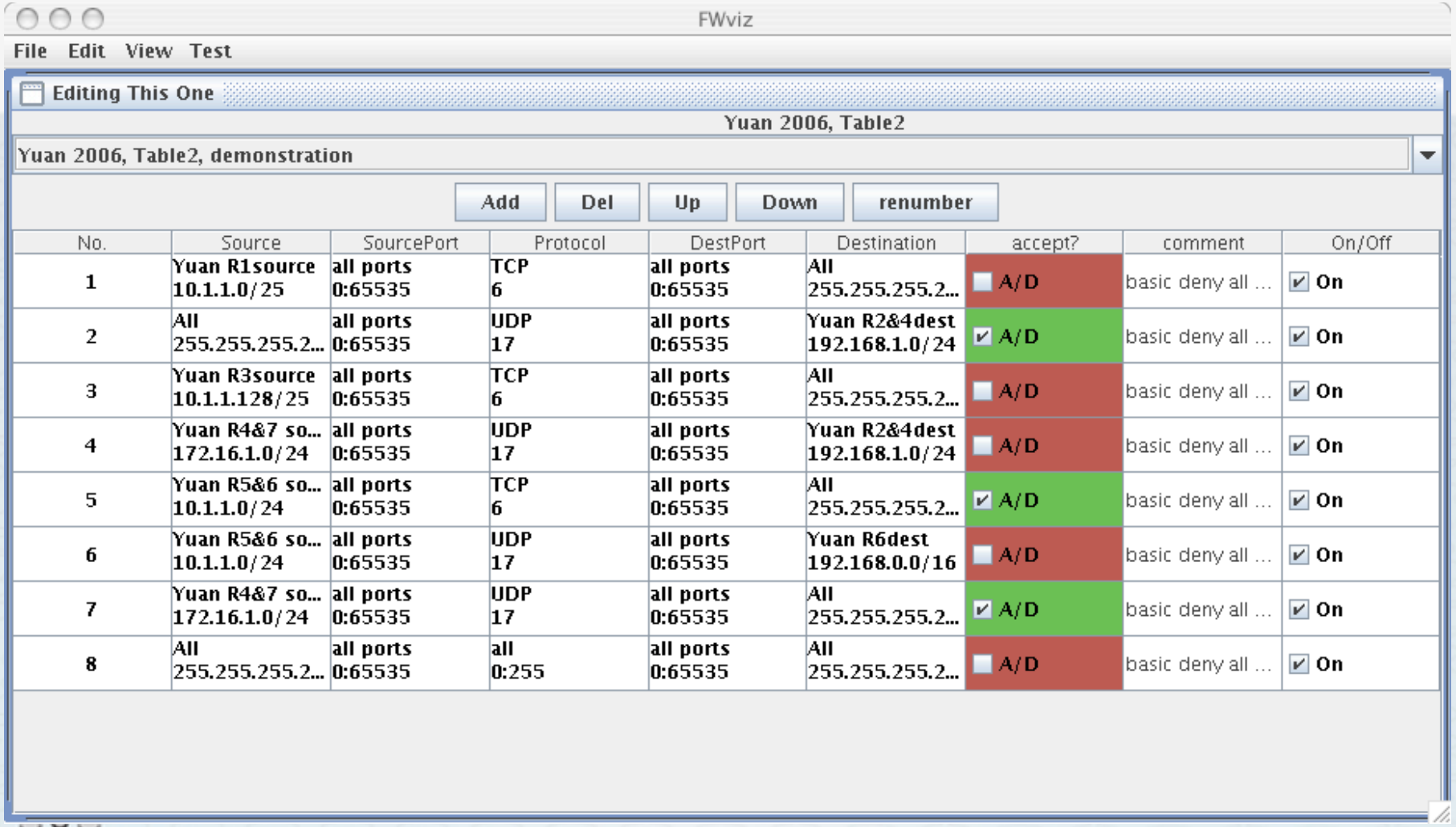


Rule A: red volumes
Rule B: green volumes
B ∩ A : blue volume
1-D cuts

Set operations as disposition rules for convex solid decomposition lists

Operation	A – B	A ∩ B	B – A
Union	Keep	Keep	Keep
Intersection	Discard	Keep	Discard
Set Difference	Keep	Discard	Discard
Void Difference	Keep	Re-label & Keep	Discard

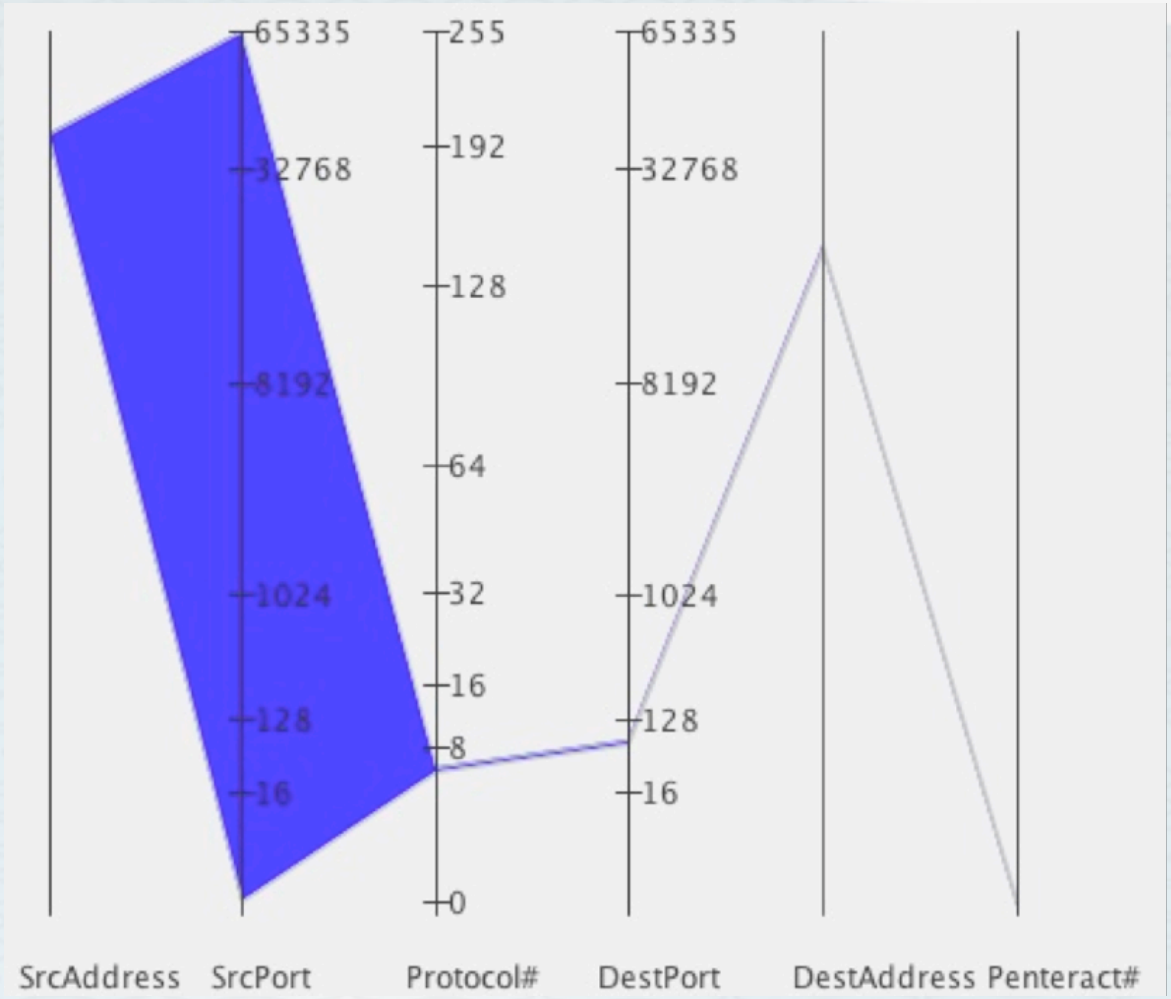
The Editor



No.	Source	SourcePort	Protocol	DestPort	Destination	accept?	comment	On/Off
1	Yuan R1source 10.1.1.0/25	all ports 0:65535	TCP 6	all ports 0:65535	All 255.255.255.2...	A/D	basic deny all ...	On
2	All 255.255.255.2...	all ports 0:65535	UDP 17	all ports 0:65535	Yuan R2&4dest 192.168.1.0/24	A/D	basic deny all ...	On
3	Yuan R3source 10.1.1.128/25	all ports 0:65535	TCP 6	all ports 0:65535	All 255.255.255.2...	A/D	basic deny all ...	On
4	Yuan R4&7 so... 172.16.1.0/24	all ports 0:65535	UDP 17	all ports 0:65535	Yuan R2&4dest 192.168.1.0/24	A/D	basic deny all ...	On
5	Yuan R5&6 so... 10.1.1.0/24	all ports 0:65535	TCP 6	all ports 0:65535	All 255.255.255.2...	A/D	basic deny all ...	On
6	Yuan R5&6 so... 10.1.1.0/24	all ports 0:65535	UDP 17	all ports 0:65535	Yuan R6dest 192.168.0.0/16	A/D	basic deny all ...	On
7	Yuan R4&7 so... 172.16.1.0/24	all ports 0:65535	UDP 17	all ports 0:65535	All 255.255.255.2...	A/D	basic deny all ...	On
8	All 255.255.255.2...	all ports 0:65535	all 0:255	all ports 0:65535	All 255.255.255.2...	A/D	basic deny all ...	On

Lossless Parallel Coordinate View

Rule allowing a Class A address access to an HTTP server



Finding Firewall Data for Analysis, Comparison, & Publication

- Requests for firewall configuration examples
  - Occasional examples provided for internal use
  - Uniform ***Absolute*** Denial of Permission to Expose
  - One use case released
- Text Firewall Correctness tools appear in the literature
  - Al-Shaer and Hamed 2003, Firewall Policy Analyzer
  - Yuan, et al. 2006, FIREMAN (modeling and analysis)
- Firewall Anomalies – predicate overlaps
  - Al-Shaer & Hamed – defined all possible anomalies

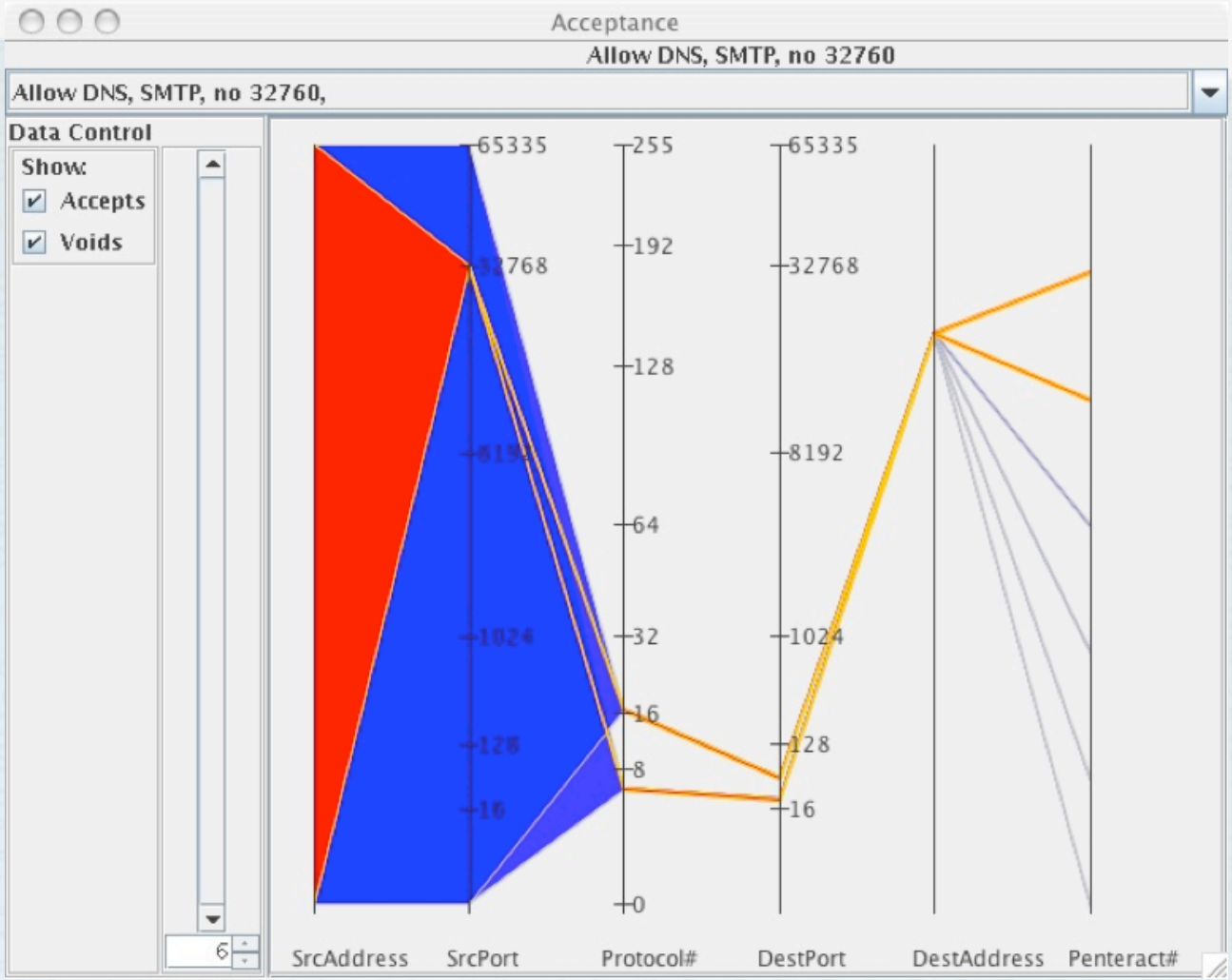
Compact Created Example Includes All Anomalies: Al-Shaer & Hamed

Protocol		Source		Destination		Action
		Address	Port	Address	Port	
1	tcp	140.192.37.20	any	*.*.*.*	80	deny
2	tcp	140.192.37.*	any	*.*.*.*	80	accept
3	tcp	*.*.*.*	any	161.120.33.40	80	accept
4	tcp	140.192.37.*	any	161.120.33.40	80	deny
5	tcp	140.192.37.30	any	*.*.*.*	21	deny
6	tcp	140.192.37.*	any	*.*.*.*	21	accept
7	tcp	140.192.37.*	any	161.120.33.40	21	accept
8	tcp	*.*.*.*	any	*.*.*.*	any	deny
9	udp	140.192.37.*	any	161.120.33.40	53	accept
10	udp	*.*.*.*	any	161.120.33.40	53	accept
11	udp	*.*.*.*	any	*.*.*.*	any	deny

Ruleset created to exercise Firewall Policy Analyzer

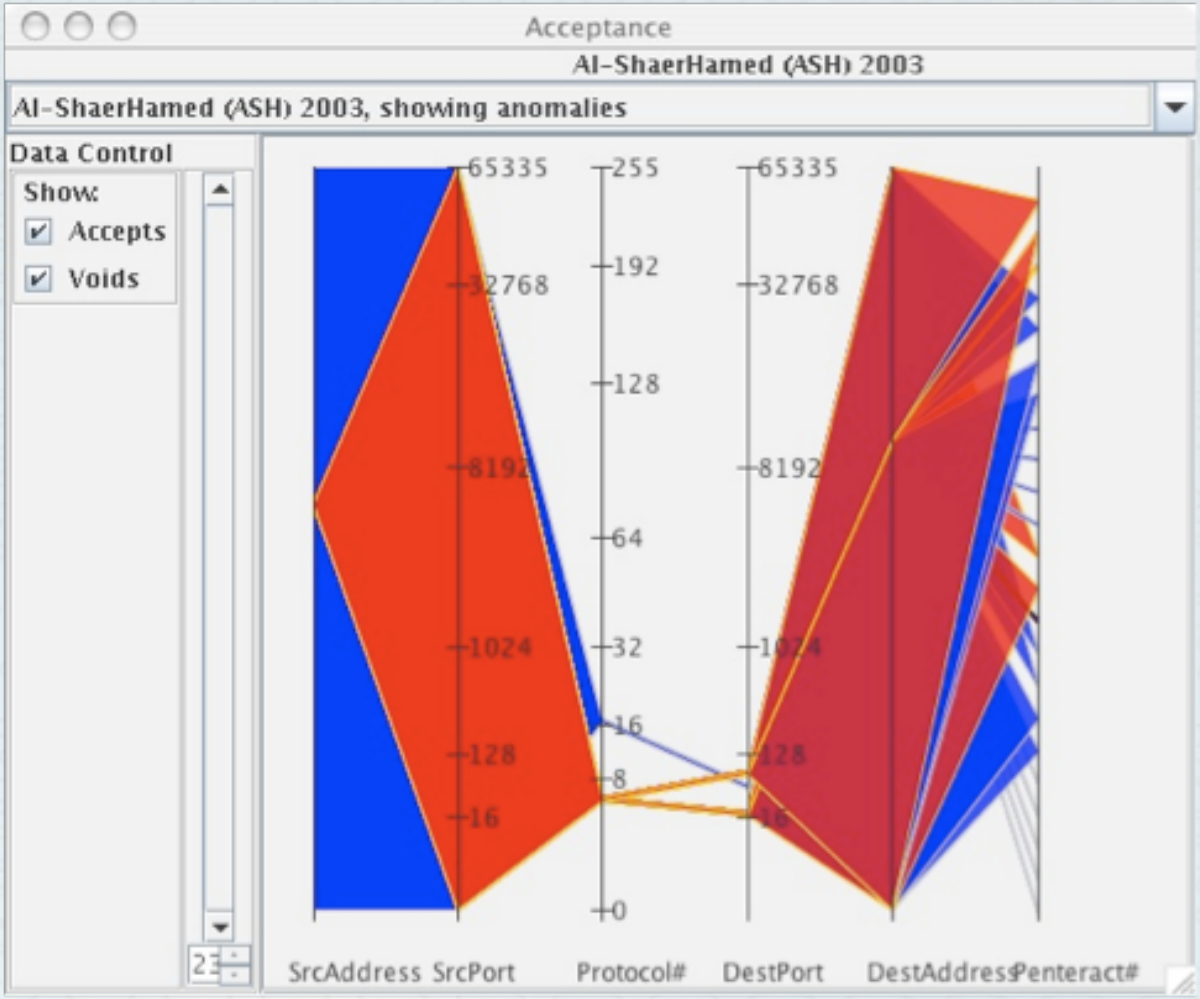
Use Case: Email server collision with legacy service protection rule

DNS and SMTP Created Voids. Six total penteracts with two voids created by the interaction of the 32760 deny rule's cleaving. The two voids are contained within the remainder of the DNS and SMTP accept rules



All Anomalies Combined: PC Visual of Al-Shaer & Hamed 2003

23 penteracts are presented clearly highlighting the need for interactive data zooming and multiple views

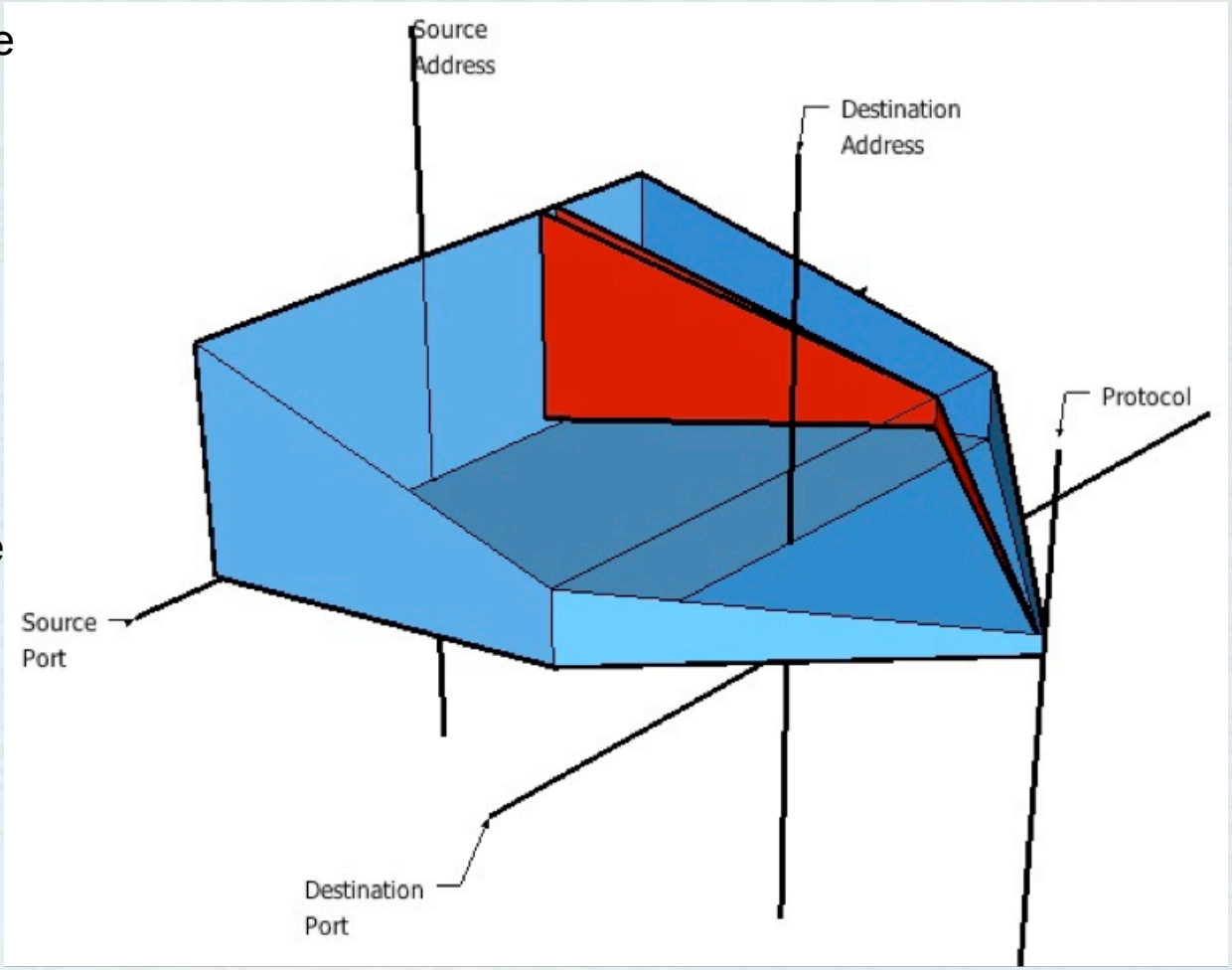


Contributions & Directions

- Configuration visualization is feasible
- Created Voids useful for interaction and visualization
- Occlusion quickly becomes issue
- PC view does not capture containment of one volume or void within another, the set-subset relationship
- Development Directions
  - Data windowing controls
    - Specialized two-dimensional controls
  - Alternate Visualization

Flow Picture Mockup: Pipe-Through-the-Wall Metaphor

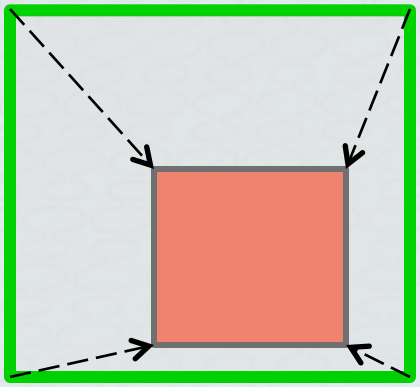
FP Representation. The plane in the left of the object represents the source address and source port axes. The destination address and destination port are similarly set up as a two-dimensional plane. The remaining value, the protocol number, is treated as a single axis.



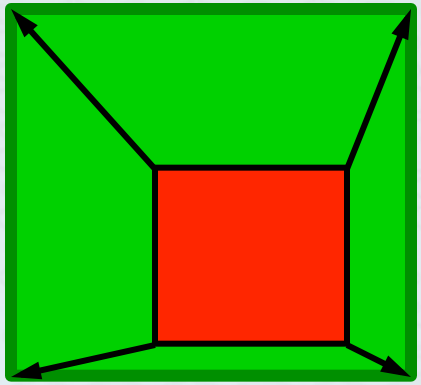
Backups

Anomaly Examples in 2-D

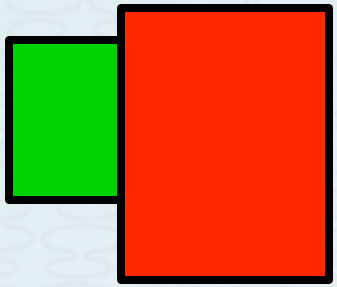
Shadowing



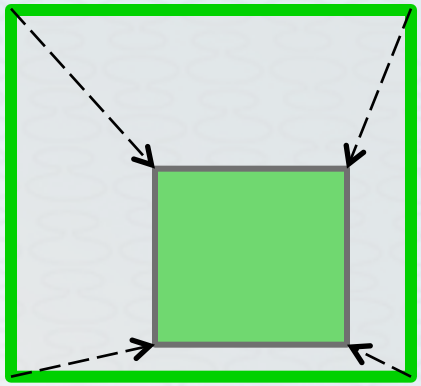
Generalization



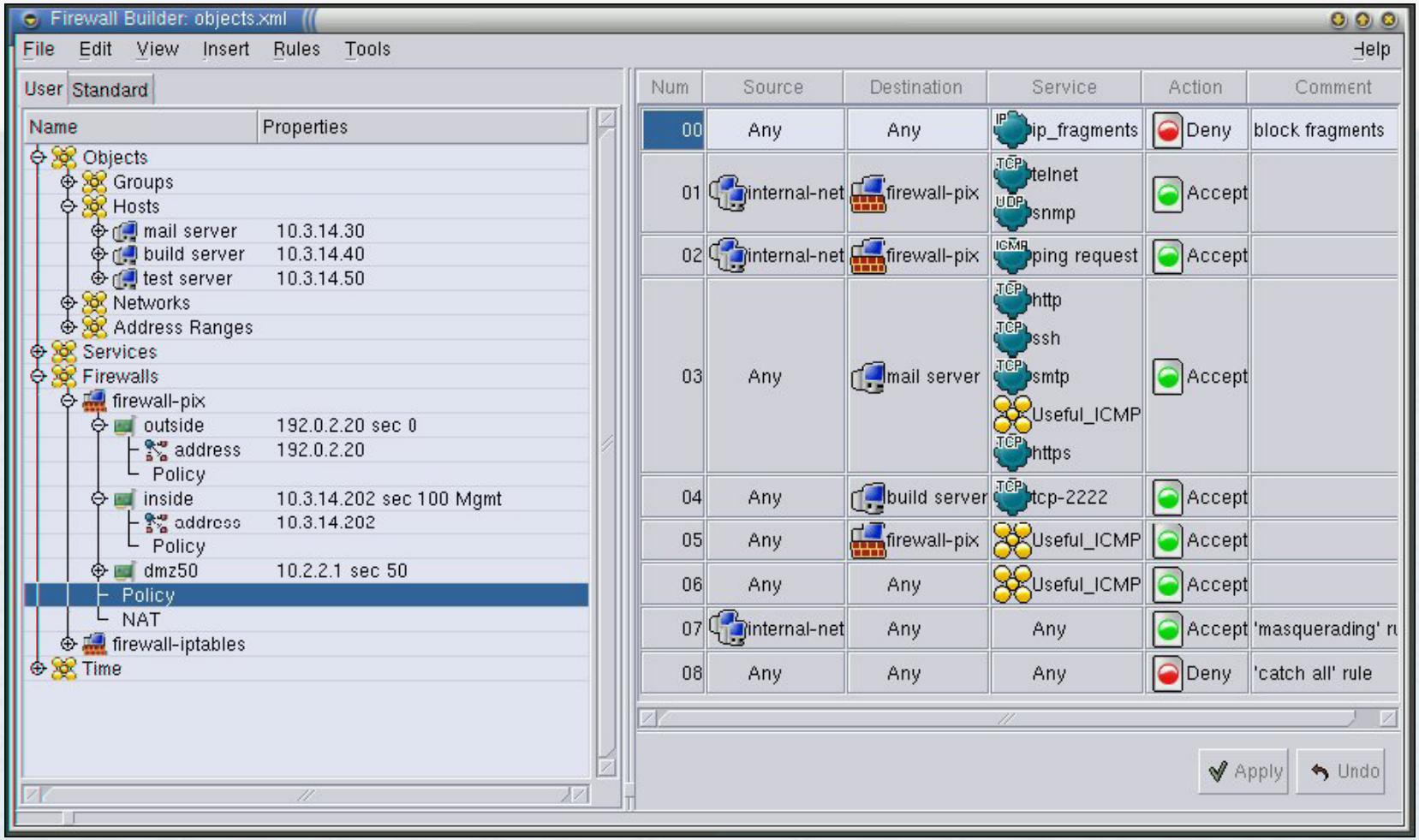
Correlation



Redundancy



What's out there?



And the research literature on firewall visualization was simply "None" until 2007.

PolicyVis – Tran et al., 2007