Firewall Architectures for High-Speed Networks

Errin W. Fulp

WAKE FOREST UNIVERSITY
Computer Science
Network Security Group
nsg.cs.wfu.edu

US Department of Energy
Office of Science
U.S. DEPARTMENT OF ENERGY
MISC Division

DOE Network Research PI Meeting
September 28, 2005

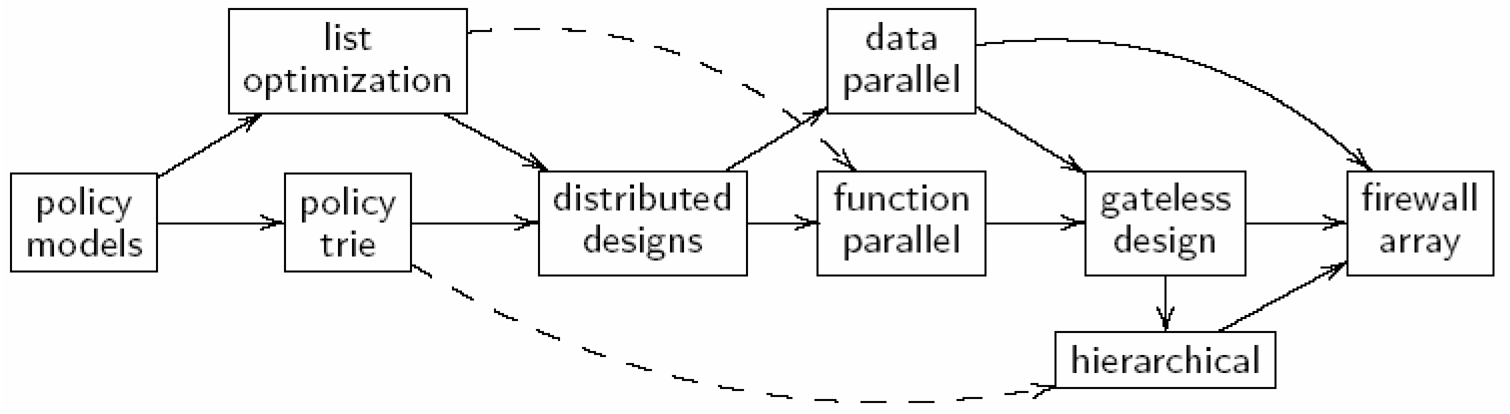
Project Objectives

Methods that improve network firewall performance

1. Develop **policy optimization** techniques
   - Formal models for rules and security policies
   - Reduce processing requirement per packet
   - Low impact solutions for current and future firewalls
   - Models used to distribute rules in parallel firewalls
2. High-speed **firewall designs**
   - One policy, distributed firewalls, parallel processing
   - Maintain QoS requirements and differentiation
   - Scalable with increasing speeds and volumes
   - Robust (highly available), able to survive DoS attacks

Research Progress

- Three year DOE ECPI project
  - **First year**: firewall policies and analytical models
  - **Second year**: firewall designs and rule distribution

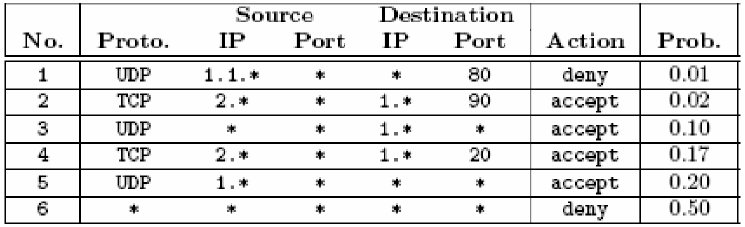


  - **Third year**: hybrid and dynamic firewall designs
- Network Security Group at Wake Forest University
  - Errin Fulp, Ryan Farley, and Steve Tarsa

Policy Optimization

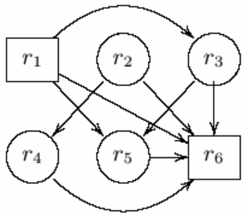
Reduce comparisons while maintaining integrity

1. **Optimize** the policy, best arrangement (NP-hard)

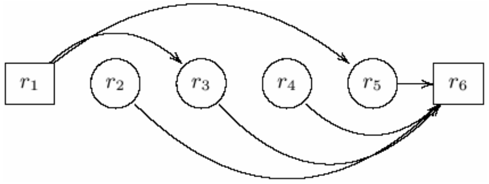


No.	Proto.	Source IP	Source Port	Destination IP	Destination Port	Action	Prob.
1	UDP	1.1.*	*	*	80	deny	0.01
2	TCP	2.*	*	1.*	90	accept	0.02
3	UDP	*	*	1.*	*	accept	0.10
4	TCP	2.*	*	1.*	20	accept	0.17
5	UDP	1.*	*	*	*	accept	0.20
6	*	*	*	*	*	deny	0.50

Firewall policy



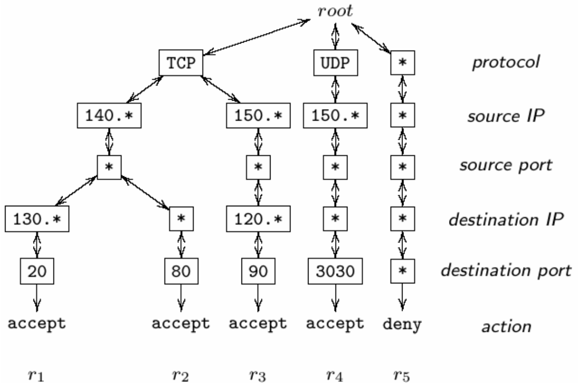
Policy DAG



Linear arrangement

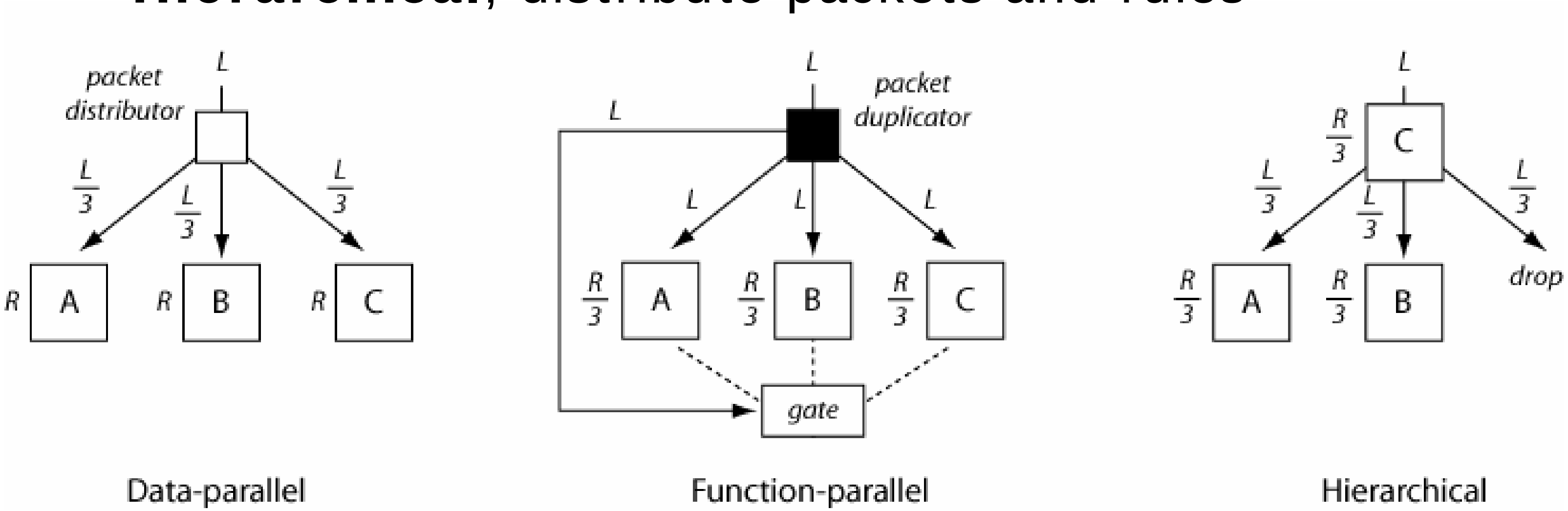
- *Optimized* list reduces number of compares (upto 80%)
- Rule compression and expansion

2. New **non-linear** representation
   - Policy trie requires $1/k$ compares
   - Policy trie optimization



Distributed Firewall Designs

- Three distributed designs
  - **Data parallel**, distribute packets
  - **Function parallel**, distribute rules
  - **Hierarchical**, distribute packets and rules



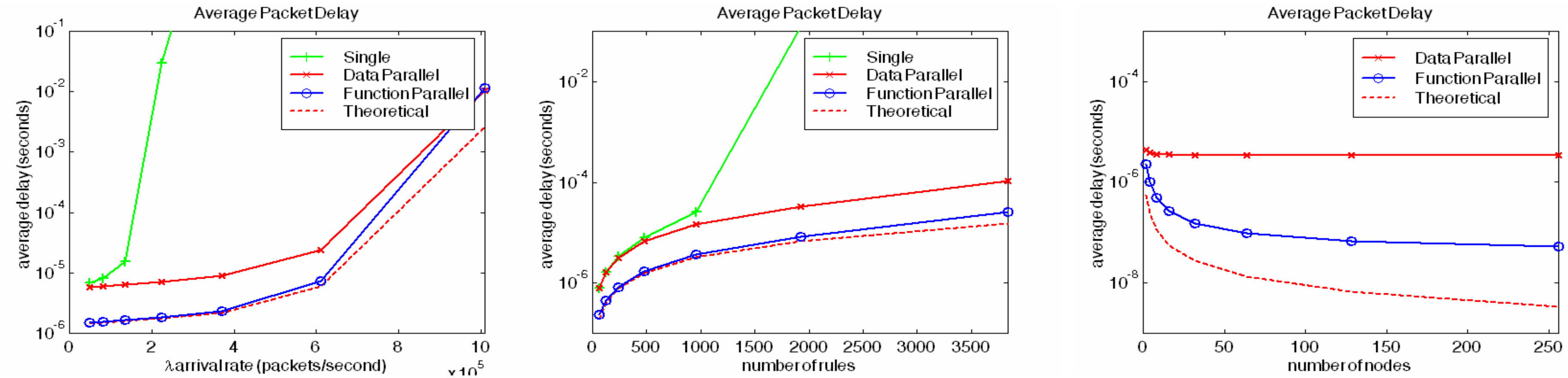
scalable, redundant, stateful inspection difficult, no differentiation

faster than data, scalable stateful, redundant?, no differentiation

potentially fastest, stateful, differentiation possible, rule distribution difficult

Function Parallel

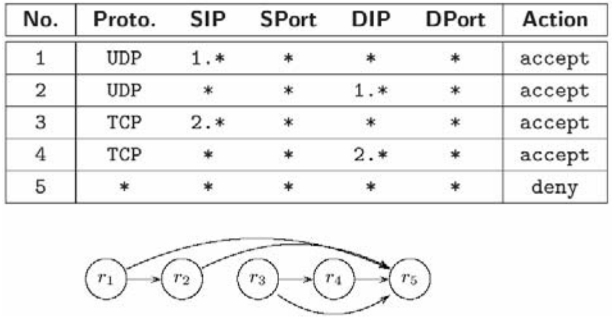
- Each node has a portion of the policy
  - Every packet processed by each node, and informs gate
  - Gate make final decision based on the policy DAG
- Results for 4-node parallel firewall



  - Function parallel 3 to 3.5 times better than data-parallel
- Gate is an additional delay, prefer to eliminate

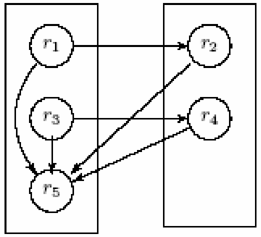
Eliminating the Gate

- Possible to remove the gate machine
  - Must distribute rules so only one node accepts
  - Use policy DAG and trie to guide decisions (*integrity*)
- Consider a policy and two node function-parallel

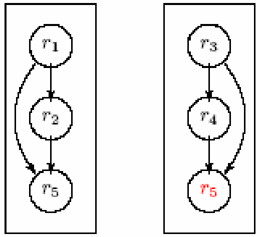


No.	Proto.	SIP	SPort	DIP	DPort	Action
1	UDP	1.*	*	*	*	accept
2	UDP	*	*	1.*	*	accept
3	TCP	2.*	*	*	*	accept
4	TCP	*	*	2.*	*	accept
5	*	*	*	*	*	deny

r_1
r_2
r_3
r_4
r_5



Odd-even distribution, requires gate

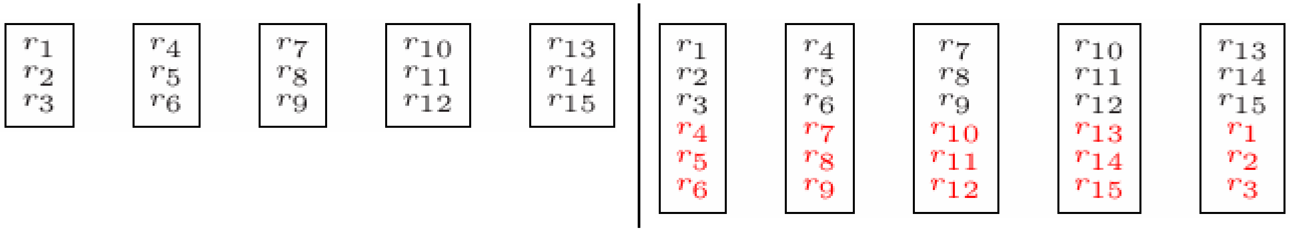


Distribution using DAG, requires no gate

- *Function parallel design is becoming hierarchical*
  - Nodes are designed to handle certain types of traffic
  - Maintains QoS, isolate DoS attacks

Continuing Research

- Finalize proofs for rule distribution
  - Eliminate gate and maintaining integrity
  - Use policy profile to optimize performance
- Create a redundant gate-less design


r_1 r_2 r_3
r_4 r_5 r_6
r_7 r_8 r_9
r_{10} r_{11} r_{12}
r_{13} r_{14} r_{15}
r_1 r_2 r_3 r_4 r_5 r_6
r_4 r_5 r_6 r_7 r_8 r_9
r_7 r_8 r_9 r_{10} r_{11} r_{12}
r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
r_{13} r_{14} r_{15} r_1 r_2 r_3

  - Use policy DAG and trie to distribute rules
  - Gateless performance with redundant attributes
- Dynamic array of firewall nodes
  - *Function parallel is not always better…*
  - Use queueing theory to determine optimal design
  - Data and/or function parallel distribution

Synergistic Activities

- **Cyber Security Group at PNNL**, *Summer 2005*
  - Deborah Frincke, John McCoy, Tom McKenna, and Patrick Wheeler (UC Davis)
  - High-speed firewall and IPS designs
  - Developed policy optimization techniques
- New **Start-up Company**, *Spring 2005*
  - High-speed firewall and IDS/IPS solutions
  - Two patents pending (*firewall optimization, rule distribution, and distributed architectures*)
  - Business plan developed
  - Initial implementation at WFU and testing at NC State
  - Seeking funding/initial investors, *possible SBIR*