Computer System, Cluster, Networking Summer Institute

COST OF SECURITY: FIREWALL FOCUS

Charles "David" Warner

Michigan Technological University

Estevan Trujillo

New Mexico Institute of Mining and Technology

Kyle Sandoval

California State University, San Bernardino

Los Alamos NATIONAL LABORATORY EST. 1943

New Mexico CONSORTIUM

NM STATE UNIVERSITY · NEW MEXICO TECH · The University of New Mexico

LA-UR 11-11198

PRObE Parallel Reconfigurable Observational Environment

SPECIAL THANKS TO:

Alex Malin, *HPC-DO*

Susan Coulter, *HPC-3*

Ed Brown, *NIE-2*

Andree Jacobson, *Probe*

Los Alamos
NATIONAL LABORATORY
EST. 1943

New Mexico
CONSORTIUM

NM STATE UNIVERSITY | NEW MEXICO TECH | The University of New Mexico

PRObE
Parallel Reconfigurable Observational Environment

OVERVIEW

- What & Why
- Methods
- Results
- Recommendations
- Further Research

WHAT & WHY

THE PROBLEM

- Security Issues
- No host based security on compute clusters
- High Target data is at risk

THE PROPOSAL

- Implement an IPTables Firewall
- Study the cost involved, with this type of safe guards in place.
- We create multiple IPTables rulesets and run a series of benchmarking tools that measure bandwidth, latency, and CPU performance.

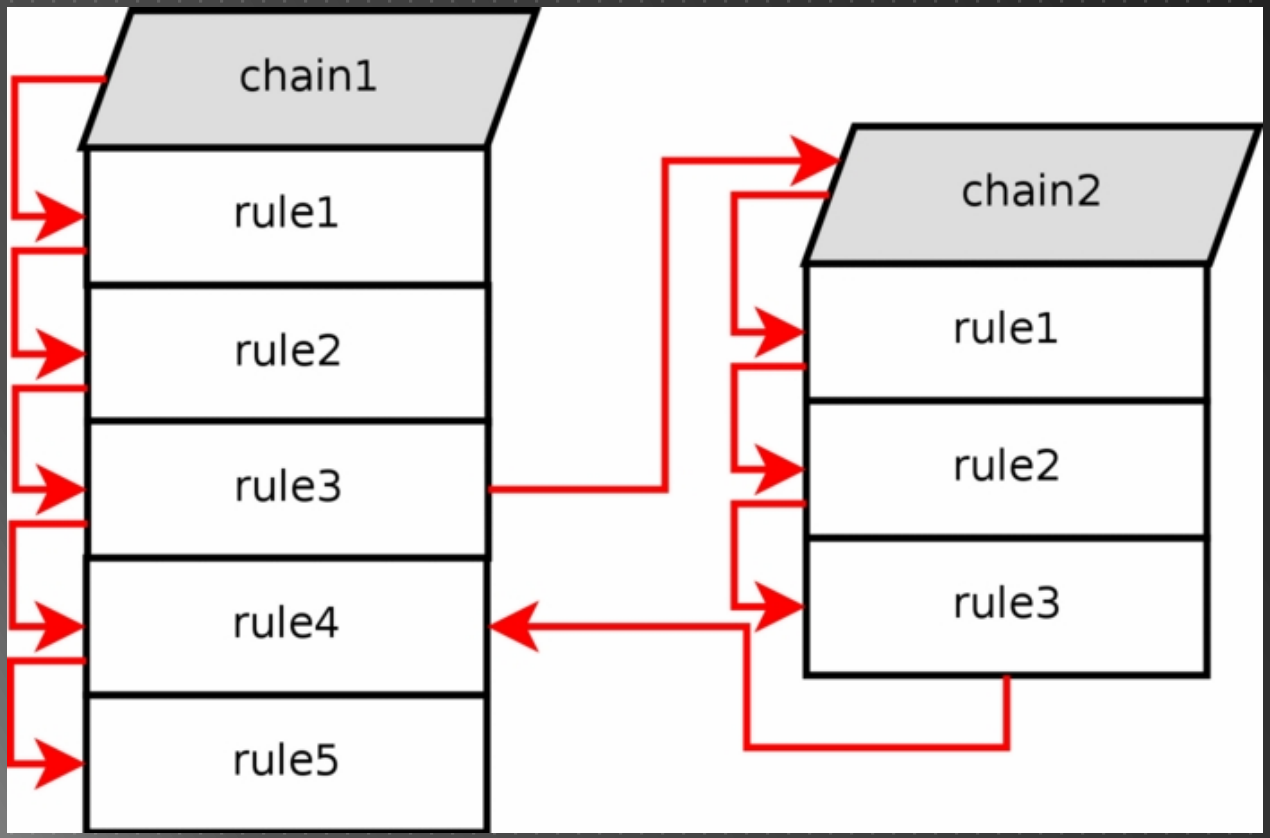
THE FOCUS

- Enabled firewalls on the compute nodes and/or head nodes
- Test latency between nodes
- Test bandwidth of nodes
- Measured boot time of nodes with the head node running a firewall
- Important. We tested different rule-sets to see where we would start to see significant loss in performance

METHODS

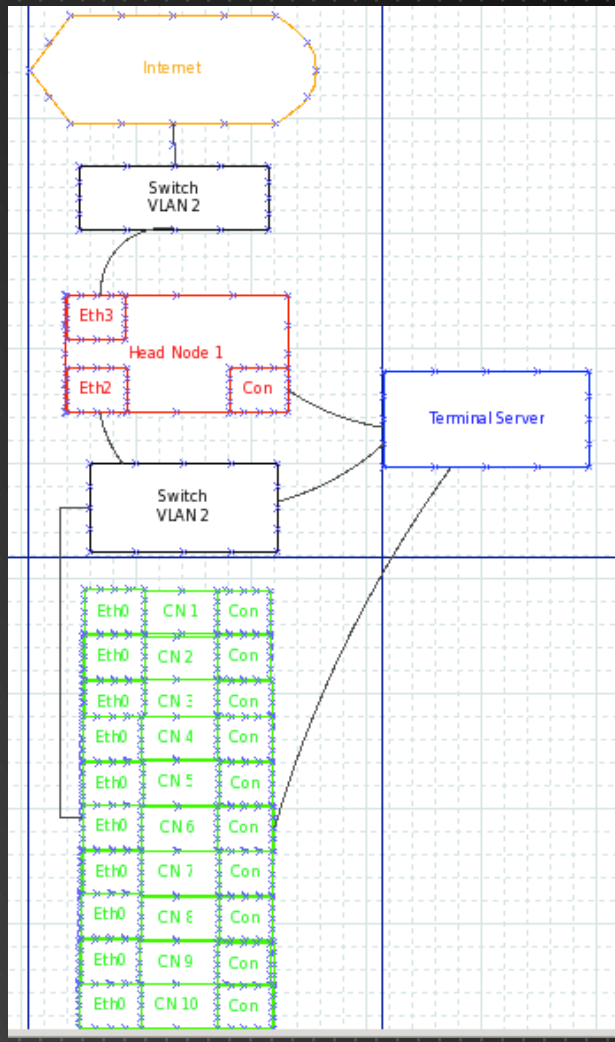
Los Alamos
NATIONAL LABORATORY
EST. 1943

THE FIREWALL PROCESS



THE HARDWARE

- Head Node
  - 8 Cores Intel(R) Xeon(R) CPU @ 2.33GHz
  - 16 GB RAM
  - Running Perceus and CentOS
- 10 Compute Nodes
  - 4 Cores Dual-Core AMD Opteron(tm) Processor 2214
  - 4 GB RAM
  - 1 Gb Ethernet



Los Alamos
NATIONAL LABORATORY
EST. 1943

THE RULE-SETS

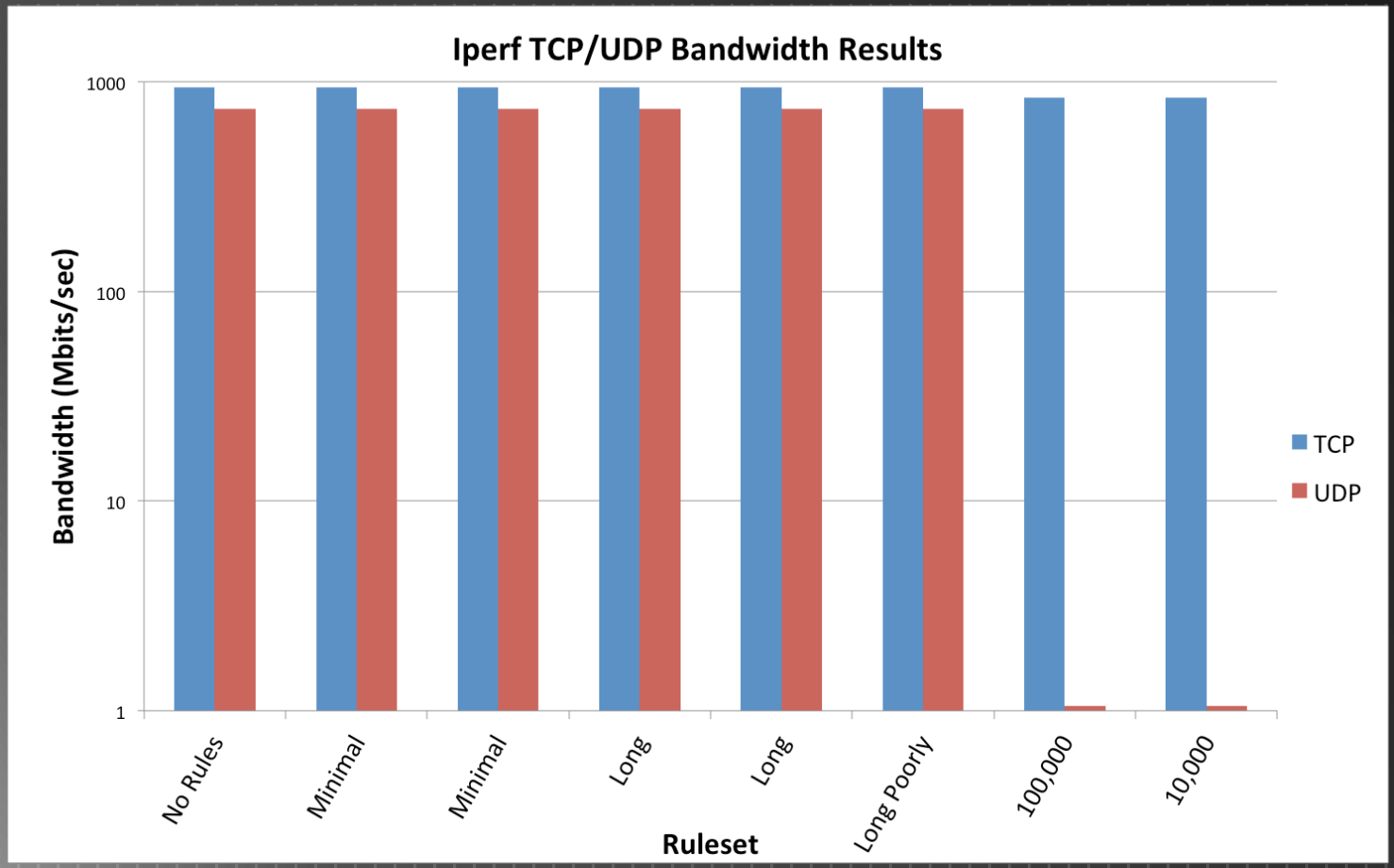
- Baseline
- Accept all
- Accept all W/ logging
- Optimized
- Optimized W/ Logging
- Poorly Written Rule-sets (~1000, 10,000, 100,000)

THE TESTS

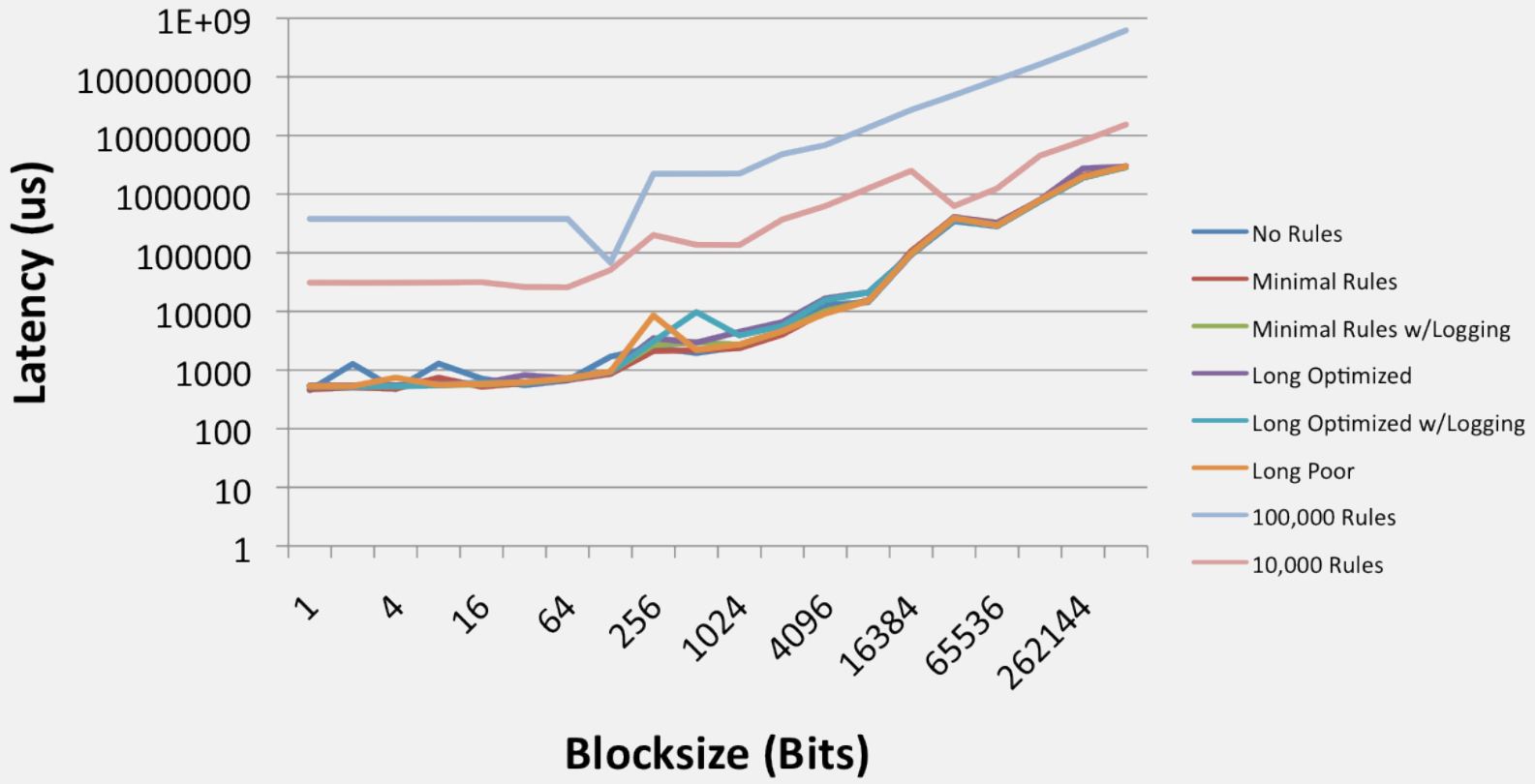
- Iperf
  - TCP and UDP protocols
  - Triggered logging in the rule-sets with a log function
- OSU MPI job
- Boot times

RESULTS

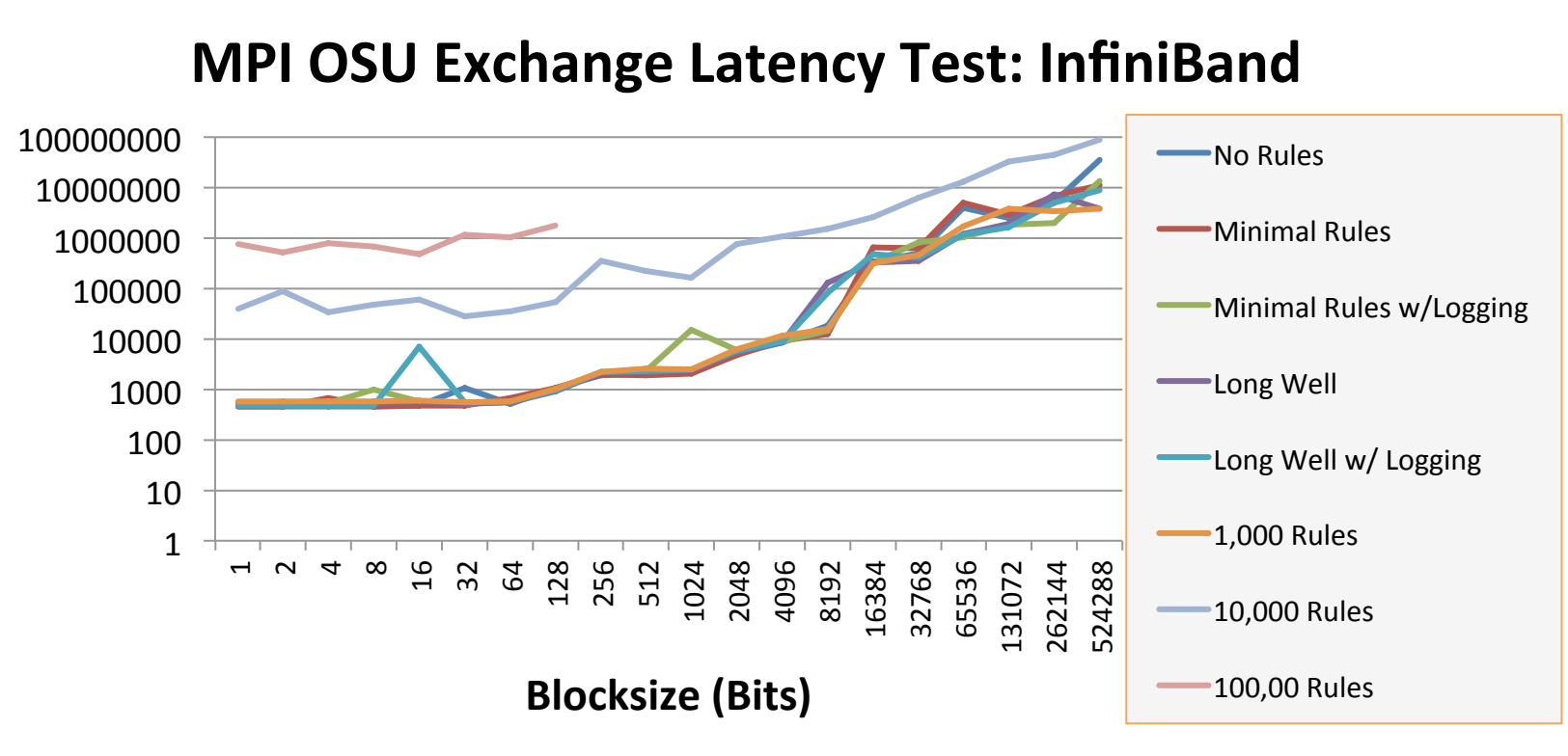
IPERF


Iperf TCP/UDP Bandwidth Results
Bandwidth (Mbits/sec)
1000
100
10
1
No Rules
Minimal
Minimal
Long
Long
Long Poorly
100,000
10,000
Ruleset
TCP
UDP

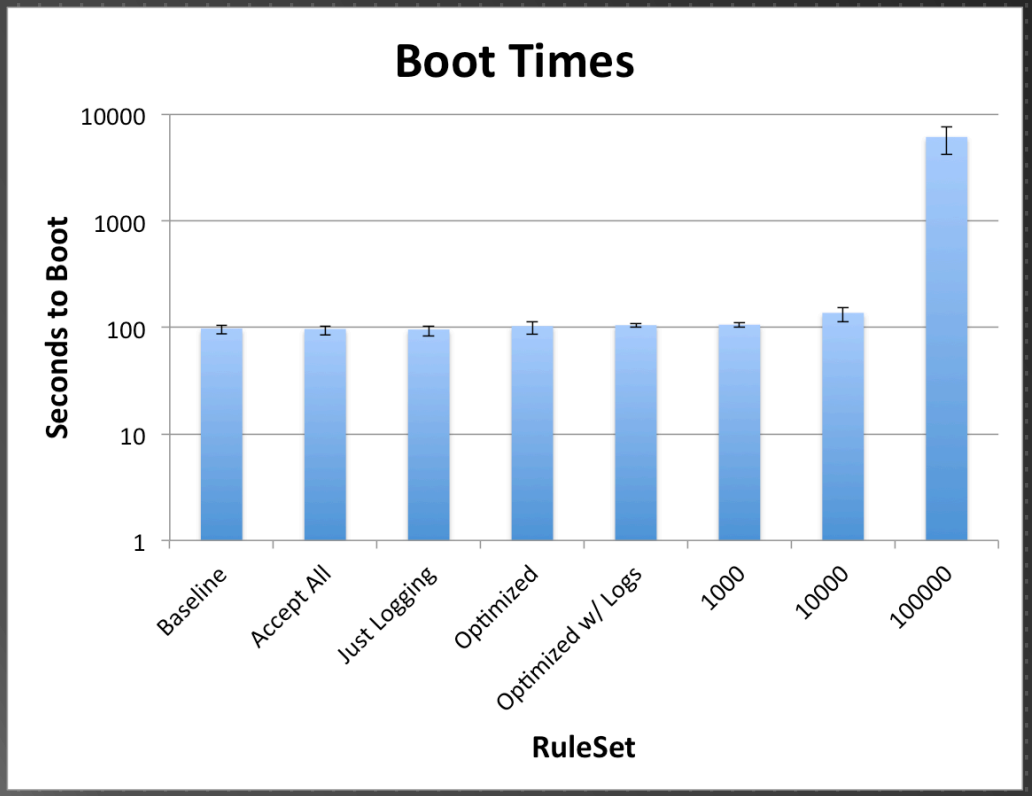
OSU'S MPI BENCHMARK



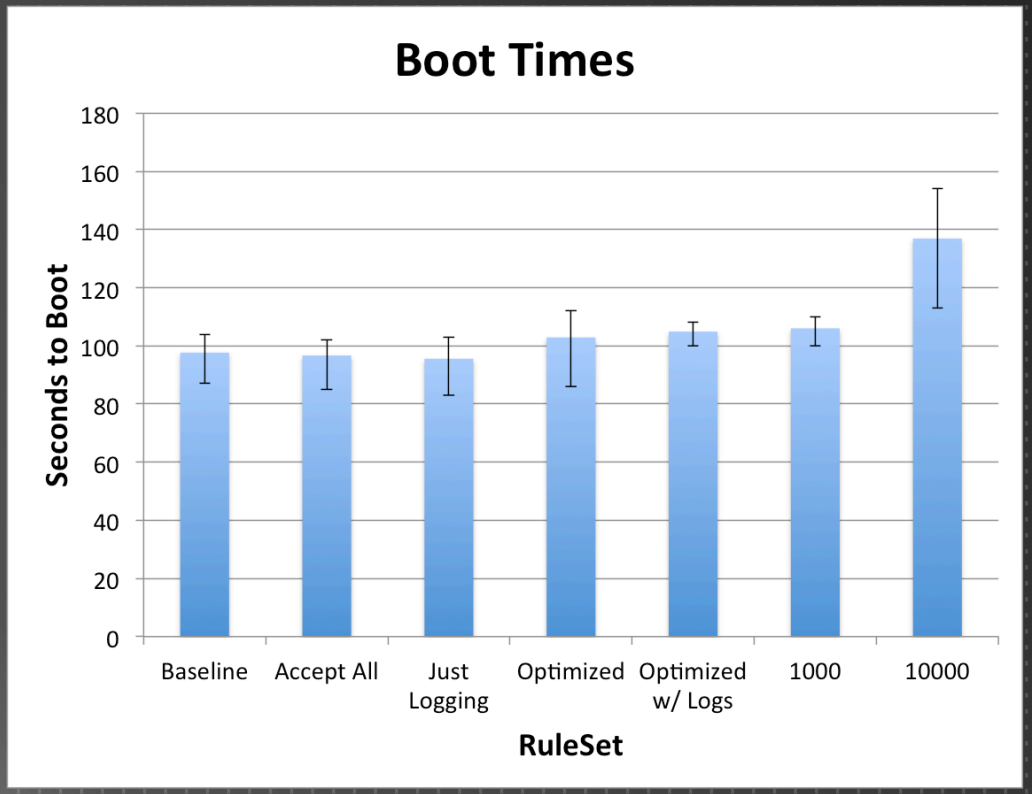
INFINIBAND LATENCY



BOOT TIMES


Boot Times
Seconds to Boot
10000
1000
100
10
1
Baseline
Accept All
Just Logging
Optimized
Optimized w/ Logs
1000
10000
100000
RuleSet

BOOT TIMES


Boot Times
Seconds to Boot
180
160
140
120
100
80
60
40
20
0
Baseline
Accept All
Just Logging
Optimized
Optimized w/ Logs
1000
10000
RuleSet

WHAT NOW?

RECOMMENDATIONS

As a result of these tests our team has concluded that running IPTables on compute nodes in a cluster that is using a one Gigabit interconnect has a negligible effect of the performance of a cluster using a moderately sized rule set.

FURTHER RESEARCH

- We hypothesize that there is an inverse liner relationship between the bandwidth of the interconnects and the number of rules in a rule-set before you get a significant performance hit.
- We were also unable to accurately measure the effect IPTables has on jitter. We do believe that by adding more and more nodes, this will become an increasing problem, and will waste costly compute time.

QUESTIONS ?

Los Alamos
NATIONAL LABORATORY
EST. 1943