Packet Sampling Firewalls
Austin Voecks

Outline

- Problem
- Abstract
- Subsampling
- Randomized Subsampling
- Dynamic Subsampling
- Heuristic Based Rules
- IPFW
- Benchmarking Performance
- Results
- Security Implications
- Related Work
- Conclusion
- References

Problem

Provide non-disruptive backend network monitoring to OneFS at 40Gb speeds.

Abstract

The performance of FreeBSDs IPFW can be increased to support 40Gb network interfaces without additional specialized hardware through dynamic probabilistic rule matching. The probability of rule matching will be based on current system load, allowing it to adapt to changing demands on the system. The efficacy of packet stream subsampling will also be explored.

Subsampling

Ideally, all network traffic would be carefully inspected; this is impractical due to the limitations of CPU and bus speeds. When logging, its also limited by disk speed. Subsampling traffic provides a way take the temperature of the network and increase chances of detecting abnormal behavior; some monitoring is better than none. To provide full packet inspection to every packet on system, the network links would have to be split into 10Gb links, each passed through dedicated hardware.