CERIAS

The Center for Education and Research in Information Assurance and Security

Hardware to Virtual Firewall Migration Heuristic Rules

Ibrahim Waziri Jr, *CERIAS - Purdue University*

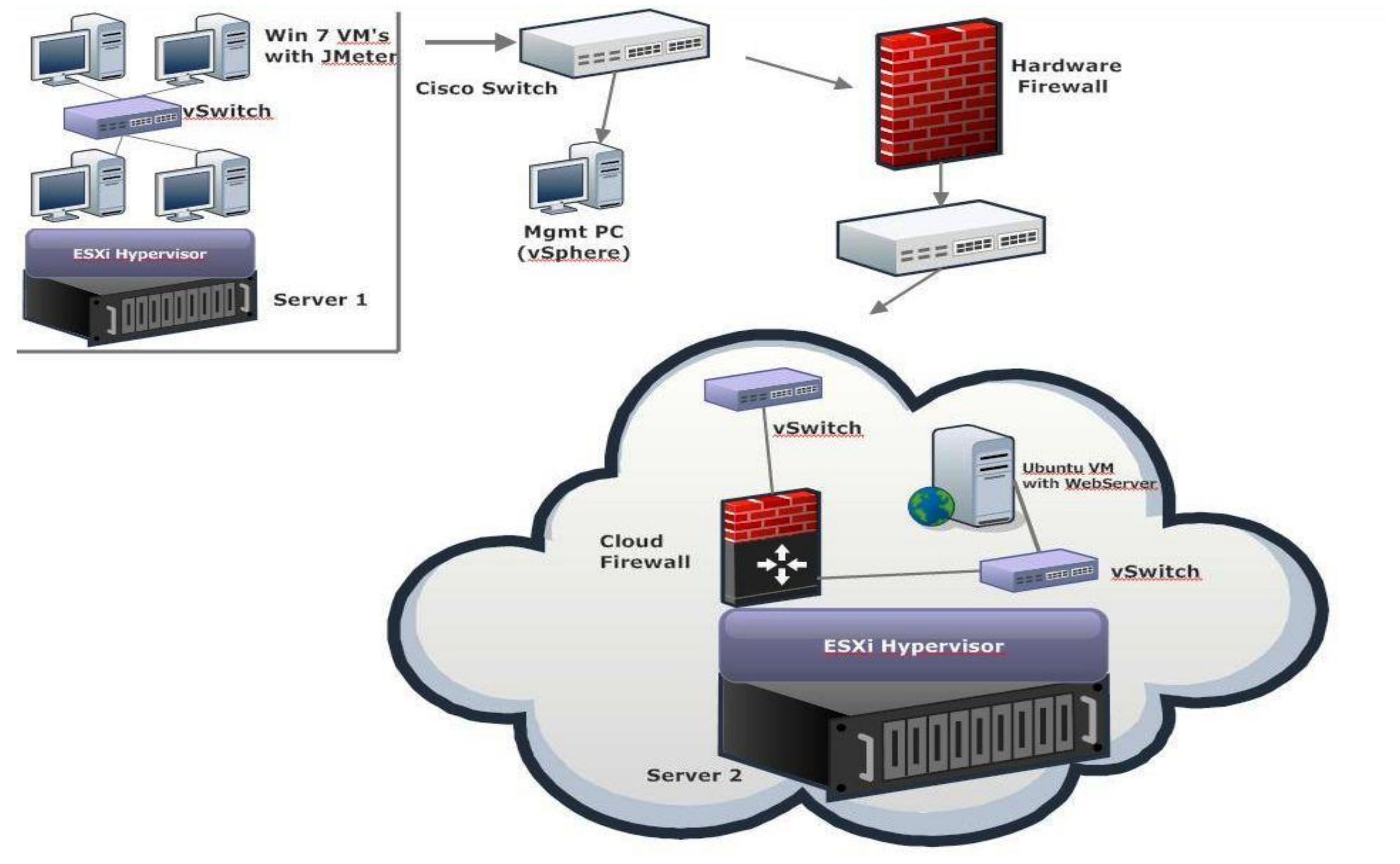
Under the direction of: Dr. Jordan Shropshire, *University of South Alabama*

To appear in 2015 IEEE SouthEastCon *(Fort Lauderdale, Florida)*

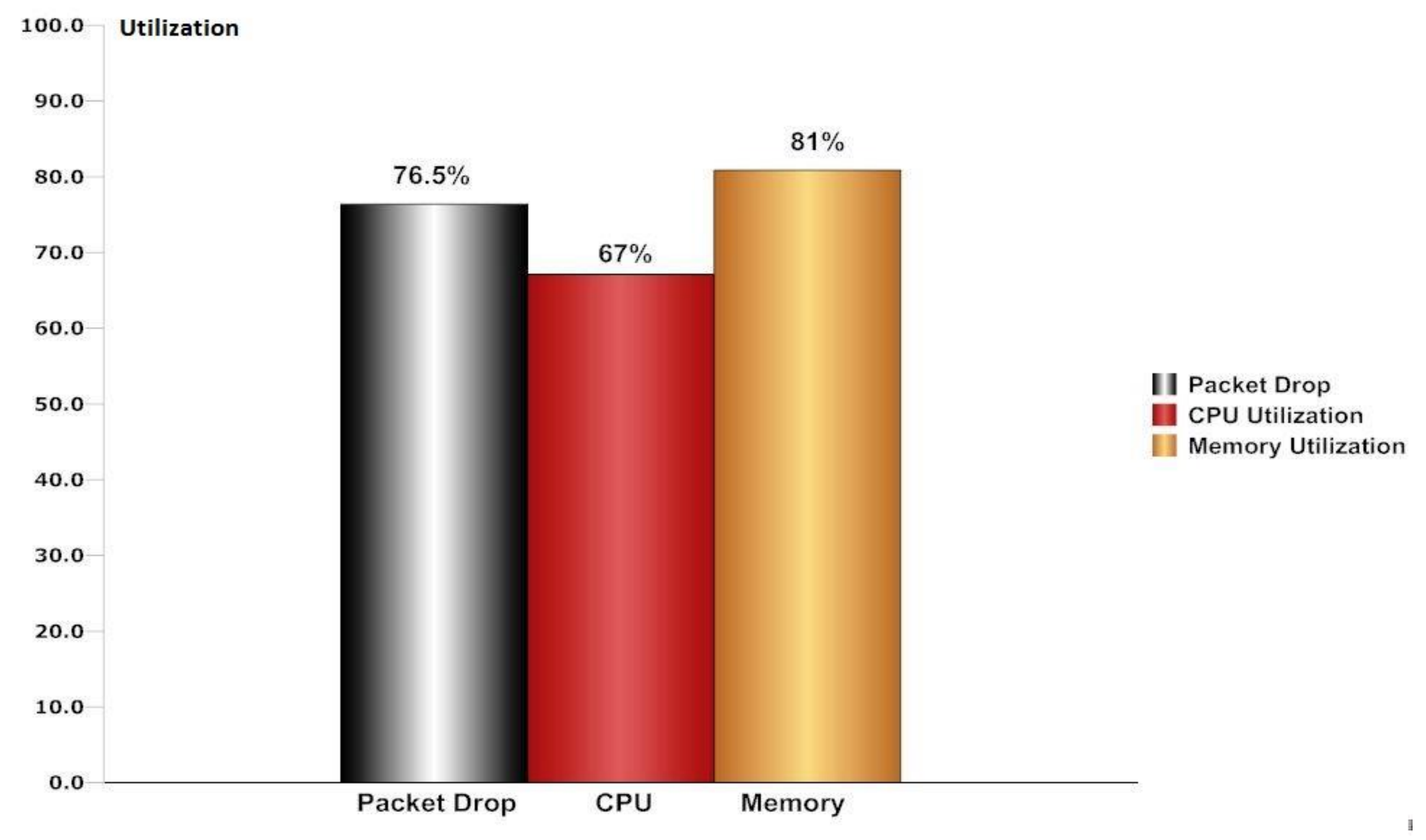
Motivation

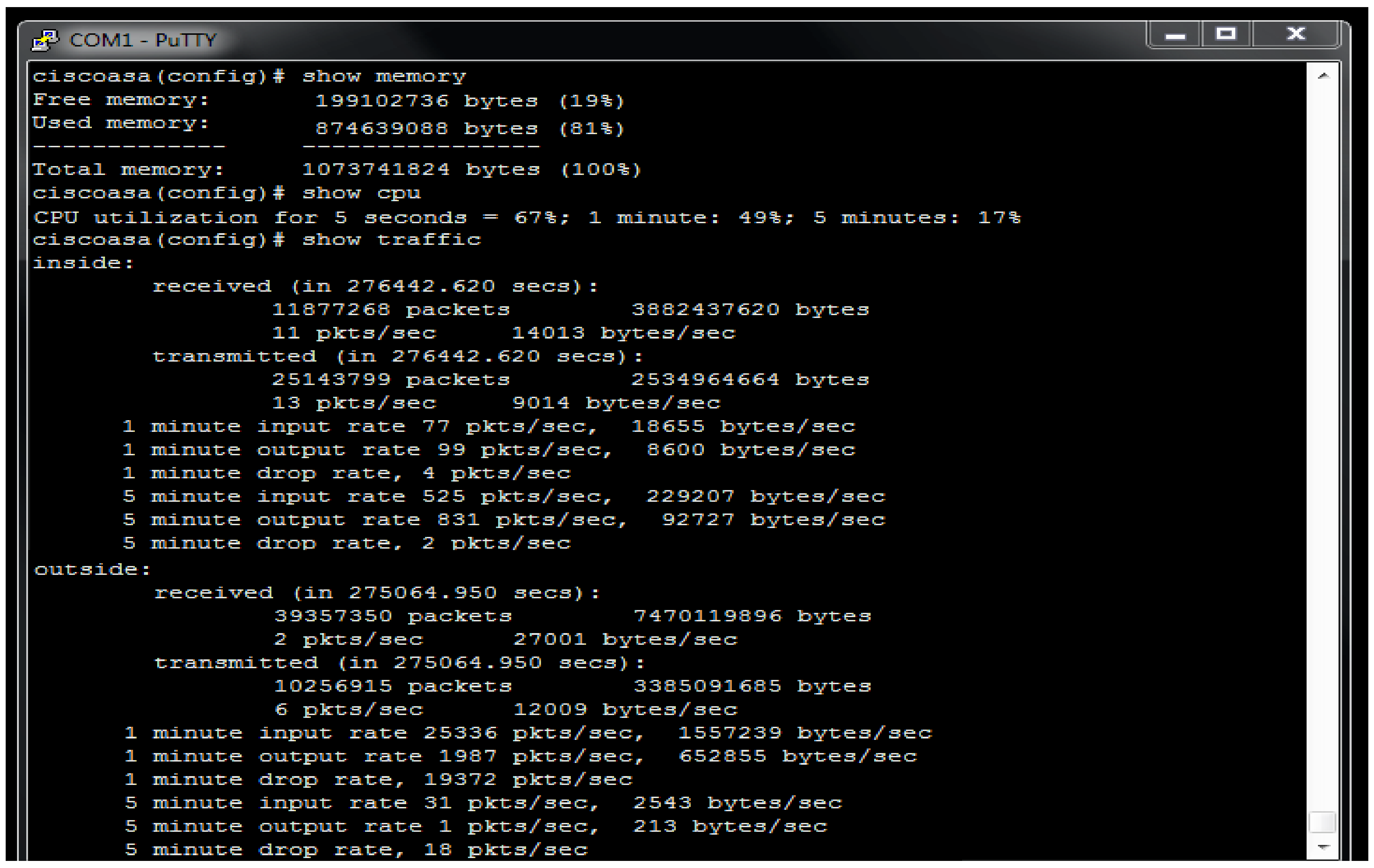
In this era of cloud computing, many data centers rely on a composite security framework consisting of hardware and virtual firewalls. Hardware firewalls are optimized for greater throughput while virtualized firewalls can only scale to match DoS attempts. To maximize the utility of each form factor, we developed an in-line firewall scheme with variable filtering point. The primary filtering point changes between hardware and virtual firewalls based on real-time conditions. The architecture incorporates heuristic-based migration logic. To define the heuristics, a performance evaluation was conducted following two test scenarios: spike tests and endurance test. Packet throughput was also assessed using JMeter. The results indicate that a threshold approach to filter-point migration maximizes network throughput while offering the insurance of on-demand scalability.

Architecture



Analysis

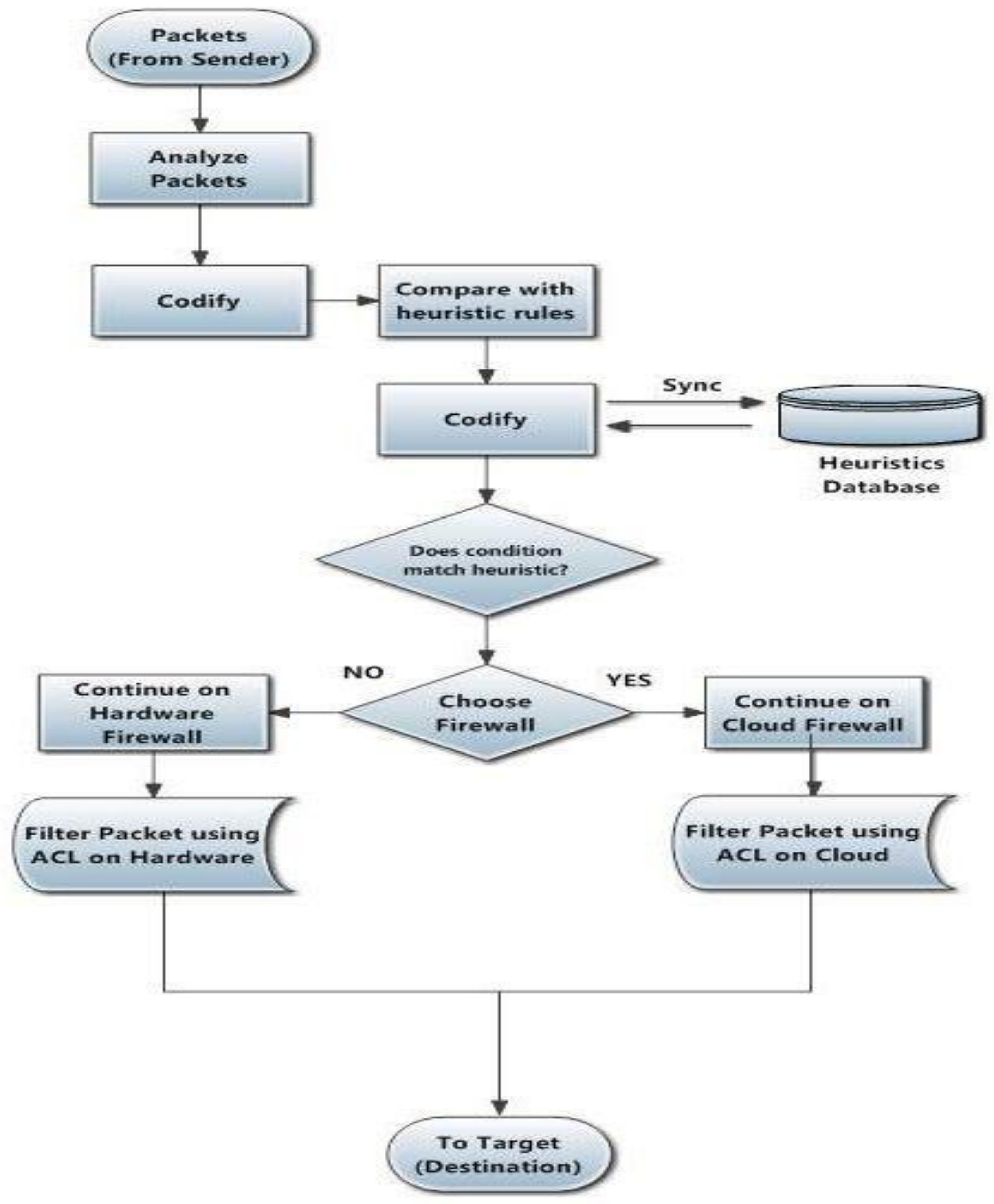




```
ciscoasa(config)# show memory
Free memory:        199102736 bytes (19%)
Used memory:        874639088 bytes (81%)
-------------      ----------------
Total memory:      1073741824 bytes (100%)
ciscoasa(config)# show cpu
CPU utilization for 5 seconds = 67%; 1 minute: 49%; 5 minutes: 17%
ciscoasa(config)# show traffic
inside:
        received (in 276442.620 secs):
                11877268 packets        3882437620 bytes
                11 pkts/sec     14013 bytes/sec
        transmitted (in 276442.620 secs):
                25143799 packets        2534964664 bytes
                13 pkts/sec     9014 bytes/sec
      1 minute input rate 77 pkts/sec,  18655 bytes/sec
      1 minute output rate 99 pkts/sec,  8600 bytes/sec
      1 minute drop rate, 4 pkts/sec
      5 minute input rate 525 pkts/sec,  229207 bytes/sec
      5 minute output rate 831 pkts/sec,  92727 bytes/sec
      5 minute drop rate, 2 pkts/sec
outside:
        received (in 275064.950 secs):
                39357350 packets        7470119896 bytes
                2 pkts/sec      27001 bytes/sec
        transmitted (in 275064.950 secs):
                10256915 packets        3385091685 bytes
                6 pkts/sec      12009 bytes/sec
      1 minute input rate 25336 pkts/sec,  1557239 bytes/sec
      1 minute output rate 1987 pkts/sec,  652855 bytes/sec
      1 minute drop rate, 19372 pkts/sec
      5 minute input rate 31 pkts/sec,  2543 bytes/sec
      5 minute output rate 1 pkts/sec,  213 bytes/sec
      5 minute drop rate, 18 pkts/sec
```

Result from Hardware Firewall

Packet Flow



Hardware Thresholds – (Defined):

- Packet drop => 5%
- Memory Utilization => 85%
- CPU Utilization => 75%

Parameters:

- Packet Drop
- CPU Utilization
- Memory Utilization
- Throughput
- Endurance & Spike

Heuristic Rules:

- If $Pd is high then $MgC else $ContH
- If $Tp is low then $MgC else $ContH
- If $CPUU is high then $MgC else $ContH
- If $MemU is high the $MgC else $ContH
- If $Scen1 is null then $ContH else $MgC