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 throughout while offering the insurance of on-demand scalability.

Analysis

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Hardware Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet drop</td>
<td>=&gt; 5%</td>
</tr>
<tr>
<td>Memory Utilization</td>
<td>=&gt; 85%</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>=&gt; 75%</td>
</tr>
</tbody>
</table>

Packet Flow

- 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 then $MgC$ else $ContH$
  - If $Scen1$ is null then $ContH$ else $MgC$