The Virtual Application Data Center

Kevin Foltz and William Simpson
Institute for Defense Analyses
ISSE 2016
Talk Outline

• Enterprise Level Security (ELS)
• Virtual Application Data Center (VADC)
  – Security
  – Resources
ELS

- End-to-end
  - Authentication
  - Encryption
  - Integrity

- Secure keys
  - No proxies
ELS

- End-to-end
  - Authentication
  - Encryption
  - Integrity

- Secure keys
  - No proxies

- Shared keys
  - Multiple MITM

Broken Appliance Stack

IDS/IPS
Packet Inspection
WAN Accelerator
Virus Scanner
Application Layer Firewall
DDoS Prevention
Executable Sandbox
Protocol Analyzer
ELS

• End-to-end
  – Authentication
  – Encryption
  – Integrity

• Secure keys
  – No proxies
ELS

- End-to-end
  - Authentication
  - Encryption
  - Integrity

- Secure keys
  - No proxies
VADC Motivation

• Virtual Machines allow portability of an OS
  – Decouple OS instance from physical hardware
• Why not do the same for entire data center?
  – Enable portability across cloud platforms
VADC

- Capture appliance functionality in software
- Instantiate appliances as handlers on servers
- Tailor appliances to individual servers
Software Appliance Evolution

• Start with hardware for performance
  – Not portable or secure
• Encapsulate in VM image
  – Portable but not secure
• Create handler to call VM
  – Portable and secure, but messy
  – Must secure connection from handler to VM
• Pull all code into handler
  – Portable, secure, and simple
VADC Security

• No sharing of server keys
• End-to-end security maintained
• Portable appliance stack tailored to application needs
## VADC Resources

### Four Applications

<table>
<thead>
<tr>
<th>App #</th>
<th># req/ms</th>
<th>ms/req</th>
<th># servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>38</td>
<td>76</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>28</td>
<td>84</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>19</td>
<td>95</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>11</strong></td>
<td><strong>259</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Five Appliances

<table>
<thead>
<tr>
<th>Appliance #</th>
<th>Function</th>
<th>Throughput Options (req/ms)</th>
<th>Needed for App?</th>
<th>Needed req/ms</th>
<th>wasted capacity</th>
<th>ms/req</th>
<th># servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Virus scanner</td>
<td>5 10 20</td>
<td>1 1 1</td>
<td>7</td>
<td>3 2</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Firewall black/white list</td>
<td>8 16 32</td>
<td>1 1 1</td>
<td>9</td>
<td>7 1</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>web Application firewall</td>
<td>8 16 32</td>
<td>1 1 1</td>
<td>10</td>
<td>6 5</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Web accelerator</td>
<td>5 10 20</td>
<td>1 1 1</td>
<td>4</td>
<td>1 8</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Official/unofficial filter</td>
<td>6 12 24</td>
<td>1</td>
<td>3</td>
<td>3 3</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>61%</strong></td>
<td><strong>114</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VADC Resources

Hardware Appliance Resources vs. Software Appliance Resources

1

2

3

4

5
VADC Resources

Hardware Appliance Resources

Server Resources

Server + Software Appliance Resources

Custom Hardware

Cloud Machines
VADC Summary

• Appliances in Software at Server
• End-to-end Security Preserved
• Portability Achieved
• Reduce Resource Requirements
Questions