Cloud INsecurity Summit

June 08, 2018  
Friday  
9:30 – 10:15 a.m.  
Crystal City, VA
Overview
Topics

• Solution Overview
• Technical Design
• Security Protections
• Lessons Learned
• Q/A
Solution Overview
Solution Overview: The What & Why’s?

The What:
• Network Security Platform
• Traffic Aggregation and Inspection Points
• Redundant, logically isolated, and geographically diverse points of presence

The Why:
• Provide like or better capabilities as part of a migration of all applications to the cloud
• Future support for multi-cloud with connectivity being the only needed item
• Layer 4 to Layer 7 protections never provided on-premises
Solution Overview: The Goals

- Provide **Highly Available** network access to **Multiple Clouds**
- Provide **Visibility** of traffic into, out of, and between applications
- Provide **Next-Gen Firewall** protections such as IPS and Antivirus
- Provide **Simpler Configuration** through inline filtering
### Solution Overview: Other Options

<table>
<thead>
<tr>
<th>Security Agents</th>
<th>Inline Virtual Firewalls</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Easier configuration</td>
<td>+ Proactive response</td>
</tr>
<tr>
<td>+ No additional overhead costs</td>
<td>+ Cheaper for customers</td>
</tr>
<tr>
<td>+ Provides easy multi-cloud options</td>
<td>+ Cloud network capability dependent</td>
</tr>
<tr>
<td>- More expensive for end customers</td>
<td>- Very high overhead costs</td>
</tr>
<tr>
<td>- Reactive response</td>
<td>- Complex VPC routing</td>
</tr>
</tbody>
</table>
Solution Overview: The Decision Point
Technical Design
Technical Design: Direct Connect in 2015
Technical Design: DX Proposed 2016 End State
Technical Design: DX Actual 2016
Technical Design: DX Today
Technical Design: Network Design
Technical Design: Automation

• Developed a server-less architecture for a Manager of Managers

• Built on Python and overlays 5 different network management products or networking devices

• Utilized a managed NoSQL database to pass state between different components
Technical Design: Automation
Technical Design: Future Changes

**Short Term:**
- Per-App Protections (e.g. Web filter rules) by tags on the instance
- Support for newer Direct Connect offerings (e.g. DX Gateway)
- Multi-cloud offering

**Long Term:**
- Revisit and validate the entire solution
Security Protections
Security Protections: Capabilities

Inbound:
• Signature based IPS & Antivirus
• Rate Limiting on layer 4 characteristics
• Per-application access identification

Outbound:
• Full deep packet inspection
• Signature based IPS & Antivirus
• Web filter by Category or Whitelist (depending on source system)
Security Protections: Additional Gaps

Being network centric still leaves gaps:

- API Calls to AWS
- S3 Buckets across endpoints
- Realtime replication needs between VPC’s
- Cracking SSL helps provide more complete protections (but it is more fragile)
- It helps to “own” the client and the server, enterprises face significant challenges which platforms or SMB’s do not
Security Protections: What’s next?
Security Protections: What’s next?
Lessons Learned
Lessons Learned: Business

- Ensure network security is in place first
- Align with your technology providers and vendors
- Have key business sponsors
- Constant communication is essential
Lessons Learned: Network Design

- Stateful failover isn't practical
- Failing over sites periodically is a must
- Network interoperability is a myth
Lessons Learned: Connectivity

- Path selection is critical and hard
- The price of a service does not imply quality of a service
- Use multiple Direct Connect endpoints
Lessons Learned: Orchestration

- Not all API’s are created equal (or exist)
- Network vendors are not software engineers
- Ensure all values are externally configurable

28
Lessons Learned: Security

• SSL everywhere hinders enterprises’ ability to protect themselves
• Security is only an annoyance to the determined
• Too much data or too little data causes equal levels of inaction and confusion
Questions?
Thank you!