Securing Your Enterprise Applications in Amazon AWS

Jigar Shah
Sr. Product Manager
Our next-generation enterprise security platform

**Next-Generation Firewall**
- Inspects all traffic
- Blocks known threats
- Sends unknown to cloud
- Extensible to mobile & virtual networks

**Advanced Endpoint Protection**
- Inspects all processes and files
- Prevents both known & unknown exploits
- Integrates with cloud to prevent known & unknown malware

**Threat Intelligence Cloud**
- Gathers potential threats from network and endpoints
- Analyses and correlates threat intelligence
- Disseminates threat intelligence to network and endpoints
Ports and protocols have lost their meaning

But how does this relate to your applications in AWS?
Is datacenter security that different for workloads in AWS?

Applications

Users

Content
Cloud security challenge #1

Incomplete security features on existing virtual security solutions

- Applications of different trust levels now run on shared infrastructure
  - Port and protocol-based security is not sufficient
  - Virtualized next-generation security is needed to:
    - Safely enable application traffic between VMs
    - Protect against cyber attacks
Cloud security challenge #2

Static policies cannot keep pace with dynamic workload deployments

- Application provisioning can occur in minutes; attribute changes are frequent
- Security approvals and configuration changes may take weeks
- Removal of old servers from security policy rules is slow or does not occur
- Dynamic security policies that understand application context are needed

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2</td>
<td>10.1.2.2</td>
<td>HTTP:80</td>
<td>Allow</td>
</tr>
<tr>
<td>10.1.2.2</td>
<td>10.1.3.2</td>
<td>TCP:1433</td>
<td>Deny</td>
</tr>
<tr>
<td>....</td>
<td>....</td>
<td>....</td>
<td>....</td>
</tr>
</tbody>
</table>
Cloud security challenge #3

*Consistent management of network security is difficult*

- Security administrators need an consistent way to manage policy
- Require consistent auditing and analysis tools such as logging and reporting
- Simplify administrator roles and access controls
VM-Series for Amazon Web Services

- Palo Alto Networks Next-Gen Firewall as an AMI
- Can be centrally managed from Panorama
- Automation features enable policies to dynamically keep pace with EC2 changes
VM-Series in Amazon AWS – How it works
VM-Series for AWS Use Cases

- Deploy the VM-Series through AWS console
  - Use case: Perimeter gateway applying NGFW protection to traffic traversing the Virtual Private Cloud (VPC)
  - Use case: IPSec VPN connecting back to corporate DC
  - Use case: VM-to-VM security based on application, blocking lateral movement of threats

- Automation features enable policies to dynamically keep pace with EC2 changes
Availability in AWS Marketplace

- BYOL available Now
- Paid-subscription expected 1H 2015
AWS demo logical topology

Internet

Main Router

IGW

Mgt, .100

E1/1, External, 10 (.11 and .12)

E1/2, Web, .1

10.0.1.0/24

E1/3, DB, .10

10.0.2.0/24

10.0.0.0/24

Web

DB

VPC