Automating Security Workflows: The SDDC Approach

Josh Soto
Product Marketing Manager
VMware

Catherine Fan
Product Line Manager
VMware
Impressive rates of change

First year this event was named "RSA Conference"

Compute Virtualization
The pressure on security

New App Requested
Provision VM
Provision Network
Policies are Set
Security Services Configured
Security Mapped to Network
App Deployed
Change Happens
Change is inevitable

SQL database server provision request

Database policy assumptions are:
- No confidential information
- No personal privacy information
- Vanilla DB policies

Sensitive data is added to the new database VM

555-55-5555
Ideally, every app would have dedicated resources
Manageability necessitates grouping

- Security Zones
- VLANS
  - 192.168.10.4
  - 192.168.10.12
  - 192.168.20.6
  - 192.168.20.11
  - ...

[Image of server rack with VLANs 192.168.10.4, 192.168.10.12, 192.168.20.6, 192.168.20.11, and others marked with various colors and numbers]
Today, security is tied to a complex and rigid network topology
And further complicated with three tier, consolidated application infrastructure
All of this results in a universal loss

<table>
<thead>
<tr>
<th>Strain on Business</th>
<th>Strain on Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed Business Opportunities</td>
<td>Security Compromises</td>
</tr>
<tr>
<td>Inability to adapt to market changes</td>
<td>Slow response to threats and changes</td>
</tr>
</tbody>
</table>
“We cannot solve our problems with the same way of thinking that created them.”

-Albert Einstein
What’s needed: a new architectural approach

Software-Defined Data Center

Applications
- Virtual Machines
- Virtual Networks
- Virtual Storage

Data Center Virtualization
- Compute Capacity
- Network Capacity
- Storage Capacity

Location Independence
The next-generation networking model

Network and Security Services
Now in the Hypervisor

- Load Balancing
- L3 Routing
- L2 Switching
- Firewalling/ACLs
Visibility

NSX is uniquely positioned to see everything
Granular control becomes possible

Built-in Services
- Firewall
- Data Security
- Server Activity Monitoring
- VPN (IPSEC, SSL)

Third-party Services
- Antivirus
- Next Gen Firewall
- Intrusion Prevention
- Security Policy Management
- Vulnerability Management
- Identity and Access Mgmt
- ...and more in progress
Intelligent grouping
Intelligent grouping
Groups defined by customized criteria

- Operating System
- Machine Name
- Services
- Application Tier
- Regulatory Requirements
- Security Posture
Use case: intelligent grouping for unsupported operating systems

OS no longer supported on several systems
These systems need policy which restricts access to only email servers
Policy and services assigned to groups

Define Once

- Define Policy
- Assign Services
- Automate Response

Apply Repeatedly

Web
App
DB
HR
Consistent policy and services
Adaptable and proactive security

**UNIQUE POLICY DEFINITIONS**

Policy and services defined with future changes in mind

*Vulnerability scan. If vulnerability found, tag workload with CVE Score.*

**UNIQUE POLICY DEFINITIONS**

Remediate changes with preset policy definitions

*If tagged, remediate with IPS.*
Automated Security in a Software Defined Data Center

**UNIQUE POLICY DEFINITIONS**

Policy & services defined with future changes in mind

Scan to ensure no private information is stored. If found, tag.

**SN# 555-55-5555**

**UNIQUE POLICY DEFINITIONS**

Remediate changes with preset policy definitions

If tagged, move workload to more secure PII group.

---

Copyright © 2015 VMware. All rights reserved.
SDDC with NSX is fundamentally a more effective security solution.

Removing grouping decisions from the network topology enables intelligent security decisions.

NSX equips security teams with the ability to automate and adapt to changes.
Learn more

- Visit the VMware booth: South Hall (#1315)
- Learn more about network virtualization and micro-segmentation: http://www.vmware.com/go/nsx
Thank you

Josh Soto  jsoto@vmware.com
Catherine Fan  cfan@vmware.com