Security in the Software Defined Data Center

Francesco Vigo
Senior Systems Engineer, VMware
fvigo@vmware.com

Ugo Piazzalunga
Technical Manager, SafeNet
ugo.piazzalunga@safenet-inc.com
Agenda

• *Software Defined Data Center (SDDC)*
• *Network & Security Virtualization*
• *Impacts on security, compliance, audit*
• *Partner Ecosystem - Safenet*
Workloads Virtualized

- 25% in 2008
- 60% in 2012
- >90% in the future
<table>
<thead>
<tr>
<th>Weeks</th>
<th>Days/Hours</th>
<th>Minutes/Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>2008</td>
<td>2012</td>
<td>Future</td>
</tr>
</tbody>
</table>
Software-Defined Datacenter

All infrastructure is virtualized and delivered as a service, and the control of this datacenter is entirely automated by software.

Network & Security Virtualization
Impeding the Journey to the Cloud

Network and security challenges restrict options for applications in the cloud.

Network Challenges
- Provisioning is slow
- Placement is limited
- Mobility is limited
- Hardware dependencies
- Operationally intensive

Security Challenges
- Often restricted to perimeter
- Bolted-on
- Lacks visibility
- Location & hardware dependent
- Operationally intensive

Efficiency, agility, savings
The Solution – Virtualize the Network

Software Defined Data Center One

- Provisioning is slow
- Placement is limited
- Mobility is limited
- Hardware dependent
- Operationally intensive

Network Virtualization Abstraction Layer

Compute Virtualization Abstraction Layer

Physical Infrastructure
What is Network Virtualization?

- **x86 Environment**
  - Virtual Machine
  - Requirement: x86

- **Server Hypervisor**

- **Network Virtualization Platform**
  - L2, L3, L4-7 Network Services
  - Virtual Network
  - Decoupled
  - Requirement: IP Transport

- **Physical Compute & Memory**
  - Physical Network
Network Virtualization must...

1. Decouple

Virtual

Decoupling physical from virtual

Physical

Hardware independence

2. Reproduce

Virtual

Reproducing from physical to virtual

Physical

No change to network from end host perspective

3. Automate

Network Operations

Cloud Operations

Operational benefits of virtualization
SDDC impacts
On security, compliance, audit
Workloads Can Live Anywhere, but are managed centrally
IMPACT: Leverage Cloud asset inventory

Legacy

- Software agent
- Network scanners
- Use multiple, inaccurate tools

SDDC-Aware

- Get all cloud asset info from cloud management solution
- Use SDDC-Aware for more accurate asset information
IMPACT: policies tight to workloads, not IP addresses

Legacy

Identifier = IP or MAC Address

SDDC-Aware

Identifier = VM, vApp, Org, Security Group

192.168.20.1

192.168.30.2

Bound to Physical Constructs

Cloud Aware

✔✔✔✔

vmware
Enable Providers and Consumers … Independently

Consumption Model
*Request workloads and services*

Single Resource Model
*The Software-Defined Data Center*

Provider Model
*Provisions workloads and services*
IMPACT: Resource Isolation & Separation of Duties

Legacy

Admins dedicated for each infrastructure service

Infrastructure silos, separate failure domains

SDDC-Aware

Single admin could manage it all, but is that desirable?

Simplified infrastructure audit – all in software, same management plane

Single point of failure, platform security essential – Does the entire data center or a complete service go down?
IMPACT: Visibility, Control, Efficiency – At what cost?

Legacy

Network services lack visibility and control over virtual network

- Software agents impact consolidation ratios.
- Security scans tax underlying resources.

Automation of network and security services is close to impossible since these services are still tied to physical infrastructure.

SDDC-Aware

Software Defined Data Center

• Partners provide best of breed services in these categories:
  - Anti-Virus (AV), Anti-Malware
  - Application Delivery Controller (ADC)
  - Application Whitelisting
  - Application Firewall
  - Data Loss Prevention (DLP)
  - Encryption
  - File Integrity Monitoring (FIM)
  - Firewall (Host/network)
  - Identity and Access Management
  - Intrusion Detection/Prevention System (IDS/IPS)
  - Load Balancer
  - Network Gateway (VLAN)
  - Network Port Profile
  - Network Switch
  - Policy and Compliance Solution
  - Security Intelligence and Event Management (SIEM)
  - User Access Control (least to our SAML)
  - Vulnerability Management
  - WAN Optimizer
  - Web Filter

How do you ensure that network and security services follow the workload, if workloads are dynamic?

Should the individual who provisions network infrastructure also be allowed to secure it?

Will this approach pass muster with your auditors?
vCloud Networking & Security

Integrated Management with vCenter/vCD

VMware Networking & Security

VDC 1
VM VM VM
VM VM

VDC 2
VM VM
VM VM

vCloud Ecosystem Framework: Integrate 3rd party services

vShield Manager: Seamless integration with datacenter management

Data Security: Protect against data leaks

App: Isolate and protect applications and virtual machines

Edge Gateway: Secure the edge of the virtual datacenter and provide gateway services

VXLAN: Foundation for elastic portable virtual datacenters
SDDC enables Best of Breed

Vendors provide best of breed services in these categories:
- Anti-Virus (AV), Anti-Malware
- Application Delivery Controller (ADC)
- Application Whitelisting
- Application Firewall
- Data Loss Prevention (DLP)
- **Encryption and Key Management**
- File Integrity Monitoring (FIM)
- Firewall (Host/Network)
- Identity and Access Management
- Intrusion Detection/Prevention System (IDS/IPS)
- Load Balancer
- Network Gateway (VXLAN)
- Network Port Profile
- Network Switch
- Policy and Compliance Solution
- Security Intelligence and Event Management (SIEM)
- User Access Control (closest to our SAM)
- Vulnerability Management
- WAN Optimizer
- Web Filter

Properties of virtual services:
- Programmatic provisioning
- Place any workload anywhere
- Move any workload anywhere
- Decoupled from hardware
- Operationally efficient
Thank you!