NSX - La piattaforma di sicurezza e virtualizzazione di rete

Daniele Zecchinato Systems Engineer @VMware



© 2016 VMware Inc. All rights reserved.

Agenda

- 1 La Visione di VMware nel Software Defined Data Center
- 2 Introduzione alla Virtualizzazione di Rete con NSX
- 3 Il Paradigma della Micro-Segmentazione
- 4 Principali Casi d'Uso



Software-Defined Data Center (SDDC): The Foundation of the New Model of IT



The Network Is a Barrier to Software Defined Data Center!!

Software Defined Data Center



NSX - Distributed Services in the Hypervisor

Automated operational model of the SDDC





Pooled compute, network and storage capacity; Vendor independent, best price/perf; Simplified config and mgt.

Location Independence



Network & Security Services Now in the Hypervisor





Load Balancing

L3 Routing





L2 Switching

Firewalling/ACLs





The 3 Advantages of Distributing Services

1. Routing - more efficient networking, fewer hops

East-West Routing / Same host

East-West Routing / Host to host



Mware[®]

The 3 Advantages of Distributing Services 2. Operational Model of a VM Security Policy Cloud Management Platform VM VM VM Internet VM VM vSwitch vSwitch Perimeter Hypervisor Hypervisor Firewalls Physical-Host Physical Host-Accurate firewall policies follow workloads as they move **M**ware[®]

The 3 Advantages of Distributing Services

3. Provisioning Automation with Scale-Out Performance



vmware[®]

Platform-based automation

 Automated provisioning and workload adds/moves/changes

Hypervisor-based, in kernel distributed firewalling

- High throughput rates on a per hypervisor basis
- Every hypervisor adds additional eastwest firewalling capacity

Gartner Magic Quadrant Data Center Networking 2015

"We believe VMware has the largest installed base of any SDN solution in the market today" "VMware NSX can run on top of any appropriately provisioned IP-based Ethernet network"

"VMware should be considered for organizations looking to increase networking agility or security within highly virtualized data centers"

"NSX microsegmentation is an innovative mechanism to provide intra-data-center security (east-west) in a cost-effective manner compared with traditional appliance-based approaches."

"Due to its pricing models, VMware's NSX allows organizations to incrementally adopt SDN without requiring large upfront capital investments."

vmware[®]

Organizations are Facing Multiple Issues with Security



vmware[®]

Problem: Data Center Network Security

Perimeter-centric network security has proven insufficient, and micro-segmentation is operationally infeasible



VMware NSX Micro-Segmentation



vmware[®]

Microsegmentation is now possible in dynamic, multi-tenant environments:

- High performance, in kernel distributed stateful firewall
- Security between VMs on same IP Subnet
- Integration with best-of-breed security partners

VMware NSX Ecosystem: <u>http://www.vmware.com/products/nsx/resources</u> Developing a Framework to Improve Critical Infrastructure Cybersecurity: <u>http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf</u>

NSX Distributed Firewall is Optimized for SDDC

Web

App

DB

NSX Distributed Firewall

Src	Dst
ANY	Shared Service
Desktop	WEB_GROUP

Rules based on logical containers

Application

20

vmware

- **Delivers Micro-Segmentation**
- Efficient rule management ٠
- Dynamic Policy (e.g: AV, DLP, Vulnerability Scan)
 No choke points with scale out performance (Near Line Rate)

VM

Application

80

Enabled for cloud automation

Application

20

Firewall policies are preapproved, used repeatedly by cloud automation

☑ Firewall – allow inbound HTTP/S. allow outbound ANY

"Web Policy"

The 3 Advantages of Distributing Services

Firewalling – much simpler operations

East-West Firewalling / Same host

East-West Firewalling / Host to host

NSX DFW Policy Objects

• Policy rules construct:

Rule Name Source Destination

Service Action Applied To

• Rich dynamic container based rules apart from just IP addresses:

Rule ID

Configure Policies with Security Groups

Micro-segmentation simplifies network security

- Each VM can now be its own perimeter
- Policies align with logical groups
- Prevents threats from spreading

Improved Server Utilization – less overprovisioning of servers

Without Network Virtualization 60% Asset Utilization

With Network Virtualization 90% Asset Utilization

Micro-segmentation in detail

No communication path between unrelated networks

• No cross-talk between networks

 Overlay technology assures networks are separated by default

Segmentation Web App 28 DR

Controlled communication path within a single network

- Fine-grained enforcement of security
- Security policies based on logical groupings of VMs

Advanced services

Advanced services: addition of 3rd party security, as needed by policy

- Platform for including leading security solutions
- Dynamic addition of advanced security to adapt to changing security conditions

Third-Party Firewall, Network Security Options for NSX Integration

Src	Dst	Action	
ANY	Shared Service	Allow	
Desktop	WEB_GROUP	Redirect to 3 rd party	-(

Redirect via global rule to 3rd party

3rd party can program NSX distributed firewall directly – and set/get context to inform policy

Example : Orchestrating Security Between Multiple Services (Vulnerability Scan)

1.Web Server VM running IIS is deployed, unknowingly having a vulnerability

- 2. Vulnerability Scan is initiated on web server (3rd party AV product)
- 3.VM is tagged in NSX Manager with the CVE and CVSS Score
- 4.NSX Manager associates the VM with the Quarantine (F/W Deny)
- 5.[Externally] Admin applies patches, 3rd party AV product re-scans VMs, clears tag
- 6.NSX Manager removes the VM from Quarantine ; VM returns to it's normal duties

vmware NSX Partne®

NSX Partners and Service Categories

http://www.vmware.com/products/nsx/resources.html

VMware NSX – Use Cases

DevOps Cloud On-boarding M&A

Key Capabilities

Application specific networking Flexible IP Address Mgmt Simplified consumption

Examples

Micro-segmentation of App Simplifying Compute Silos DMZ Deployments

Key Capabilities

Programmatic Consumption Full featured stack Visibility and ops

Public Clouds

Examples

XaaS Clouds Vertical Clouds

Key Capabilities

Multi-tenant Deployment Programmatic L2, L3, Security Overlapping IP Addressing Any Hypervisor, Any CMP

Use Case : Multi-tenancy with Segmentation and Advanced Services

No traffic between networks

- Completely separate unrelated networks
- Add advanced services based on virtual network, network segment, or Security Group

isolation

27

Use Case: Networking and Security for VDI

Traditional Data Center

NSX Data Center

Simplify VDI deployments

vmware[®]

Eliminate complex policy sets and topologies
 Align policies to logical grouping
 Decouple network topology from VDI security

Use Case: Infrastructure Management with vRealize Automation

Dynamically Provision and Decommission NSX Logical Services

New Features

- Simplified Multi-Tier App Deployment
- Improved Connectivity
 Deployment of logical switches and networks
- Enhanced Security
 - Intelligent placement of workloads in security groups protected by firewalls

Increased Availability

 Via deployment of NSX distributed firewalls and load balancers

Benefits

 Deliver <u>secure</u>, <u>scalable</u>, <u>performing</u> application-specific infrastructure on-demand

Use Case: Multi Datacenter 1

NSX L2 VPN for Data Center Migration and L2 Extension

Use Case: Disaster Recovery NSX + SRM

Active-Standby Application Pair

Cross vC NSX Logical Networks with L2/L3/DFW

Use Case: A Mixed Deployment

Active-Active, DR and Stretched Application Deployment

32

NSX Customer and Business Momentum

Production Deployments (adding 25-50 per QTR)

Organizations have spent over US\$1M on NSX

Stats as of end of Q4 2015

VMware NSX Value Prop

VMware NSX Transforms the Operational Model of the Network

Mware[®]

What's Next...

Play

VMware NSX Hands-on Labs labs.hol.vmware.com

Learn **#Virtualize**YourNetwork Road to Software-Defined Data Center Home > Blogs > The Network Virtualization Blog The Network Virtualization Blog **vm**ware^{*} Products Home / Products / NSX NSX Explore, Engage, Evolve virtualizeyournetwork.com Network Virtualization Blog blogs.vmware.com/networkvirtualization

NSX Product Page vmware.com/go/nsx

NSX Training & Certification www.vmware.com/go/NVtraining Deploy

NSX Technical Resources Reference Designs vmware.com/products/nsx/resources

VMware NSX YouTube Channel youtube.com/user/vmwarensx

VMware NSX Community communities.vmware.com/community/vmtn/nsx

Thank you.

STORE THE FEET OF LESS IN THE LESS

and the second se