NSX
Seguridad de DC con la Microsegmentación

Esteban Prieto
Senior Systems Engineer
Como hace para:
Moverse tan rápido como necesita el negocio al mismo tiempo que atiende un entorno cambiante y creciente, sin la necesidad de empezar de Nuevo?
Usted necesita un **Nuevo enfoque** para el networking y la seguridad que le brinde:

La agilidad y velocidad que necesita para soportar su negocio, mientras que proporciona una infraestructura más segura.
The Software Defined Data Center

Software Defined Data Center (SDDC)
- Any Application
- SDDC Platform
  - Data Center Virtualization
- Any x86
- Any Storage
- Any IP network

Google / Facebook / Amazon Data Centers
- Custom Application
- Custom Platform
  - Software / Hardware Abstraction
- Any x86
- Any Storage
- Any IP network
Traditional network provisioning

Slow
Non-centralized configuration
Human Error
Network and Security Virtualization

Hardware independent
Non-disruptive on productive network and security equipment
Why are breaches still happening?

Unconstrained communication

Little or no lateral controls inside perimeter

Low priority systems are targeted first.

Attackers can move freely around the data center.

Attackers then gather and exfiltrate data over weeks or even months.
Security is needed everywhere, but we can’t have it everywhere

Why can’t we have individual firewalls for every VM?

With traditional technology, this is operationally infeasible.

- Physical firewalls: Expensive and complex
- Virtual firewalls: Slow, costly, and complicated
Problem: Data Center Network Security
Perimeter-centric network security has proven insufficient, and micro-segmentation is operationally infeasible.
Seguridad en Datacenter: Micro-Segmentación?
Seguridad en Datacenter: Micro-Segmentación?
Seguridad en Datacenter: Micro-Segmentación?
Los controles perimetrales son insuficientes
Seguridad en Datacenter: Micro-Segmentación con NSX
Solution: Leverage SDDC Approach for Micro-Segmentation

- Hypervisor-based, in kernel distributed firewalls
- Platform-based automated provisioning and workload adds/moves/changes
Advance Services Insertion
Security Automation

Security Group = Quarantine Zone
Members = {Tag = 'ANTI_VIRUS.VirusFound', L2 Isolated Network}

Security Group = Web Tier

Policy Definition

- Standard Server VM Policy
  - Anti-Virus – Scan

- Quarantined VM Policy
  - Firewall – Block all except security tools
  - Anti-Virus – Scan and remediate
Protección avanzada con Check Point vSEC

- Advanced security with micro-segmentation
- East-west multi-layer threat prevention
- Security orchestration and automation

VMware vCenter and NSX Manager

NSX Security Groups & VM objects dynamically fetched from NSX and vCenter

Check Point Management

Check Point updates NSX on infected VMs for quarantine and remediation

Check Point Security Admin

Check Point security automatically provisioned

VMware NSX

VMware ESXi

Context-aware policy dynamically tracks VM changes
Intelligent Policy Creation

Groups defined by workload characteristics, not IP, port and protocol
Security Automation

Service Composer

HOW you want to protect

WHAT you want to protect

Pros

Agility, Service Compliance

Guest Introspection Rules

Distributed Firewall Rules

Network Introspection Rules

Security Policy

- Anti-Malware / Anti-Virus
- Data Security
- Vulnerability Management
- File Integrity Monitoring
- L3 / L4 Firewall Rules
- IDS / IPS Services
- Firewall Services (L7)

VMware

vmworld
Security EcoSystem

- Anti-vírus
- Data Loss Prevention
- Vulnerability Scan
- Security tags

- NGFW
- IPS
- Malware
- Anti-Bot
NSX Value Proposition

Network virtualization is at the core of the software-defined data center approach.

- Virtualization layer
- Network, storage, compute
The Next-Generation Networking Model

- Switching
- Load balancing
- Routing
- Firewalling/ACLs

- East-west firewalling
- High throughput rates
- Hardware independent
- Network and security services now in the hypervisor

Network and security services now in the hypervisor

- Hardware independent
NSX Value Proposition
Granular Policy Enforcement

Enables zero trust security model with policy enforced at every workload.
Getting Started and Operations
vRealize Network Insight
Transformative Operations for NSX based Software-Defined Data Center

Plan Micro-segmentation Deployment and Audit Security Compliance

Optimize Network Performance with 360° Visibility & Analytics

Offers Best Practices, Health and Availability of NSX Deployment

Across Virtual, Physical and Cloud
NSX & vRealize Network Insight Journey

**Evaluating**
- Assess
  - East–West Data Center Traffic Profiling
  - Micro-Segmentation Recommendations
  - NSX ROI Modeling

**Day 1**
- Deploy
  - Map Application Connectivity
  - Security Groups and DFW Rule Recommendations
  - Best Practices

**Day 2**
- Manage
  - Overlay-Underlay, V-to-P Visibility
  - Google-like Search for Rapid Trouble-Shooting
  - Audit & Compliance
Get Started Today with a Free VMware Network Assessment

Understand how you can immediately benefit from micro-segmentation

Visibility

96% East-West

Recommendation

Micro Segments (By VLAN/VXLAN)

Value

Recommended Firewall Rules

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG-Lab-Dev</td>
<td>Internet</td>
<td>443 [https]</td>
<td>ALLOW</td>
</tr>
<tr>
<td>DC-Physical</td>
<td>SG-Lab-Dev</td>
<td>22 [ssh]</td>
<td>ALLOW</td>
</tr>
<tr>
<td>DC-Physical</td>
<td>SG-Lab-Test</td>
<td>22 [ssh]</td>
<td>ALLOW</td>
</tr>
<tr>
<td>SG-Lab-Test</td>
<td>Internet</td>
<td>443 [https]</td>
<td>ALLOW</td>
</tr>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
<td>DENY</td>
</tr>
</tbody>
</table>
“Data Paths” en el “Overlay” y el “Underlay”

Gráficos de conectividad
- VM a VM, VM a físico, VM a Internet
- “Hop-by-Hop Path” en el “Overlay” y el “Underlay”. Visibilidad de la frontera “V-to-P”
- Correlación de problemas y métricas de performance, tanto el mundo virtual como físico
- Reglas de DFW aplicadas, y las “Security Policies” de NSX
NSX-T 2.1

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere</td>
<td>Supported vSphere version</td>
</tr>
<tr>
<td>RHEL KVM</td>
<td>7.4 and 7.3</td>
</tr>
<tr>
<td>Ubuntu KVM</td>
<td>16.04.2 LTS</td>
</tr>
</tbody>
</table>

Distributed Firewall Using Objects and Tags in Rules
From NSX-T 2.0, distributed firewall using Grouping objects that use VM Names and/or Tags is supported.

Support for Containers
NSX-T enables micro-segmentation and networking capabilities for Kubernetes.
Thank you