

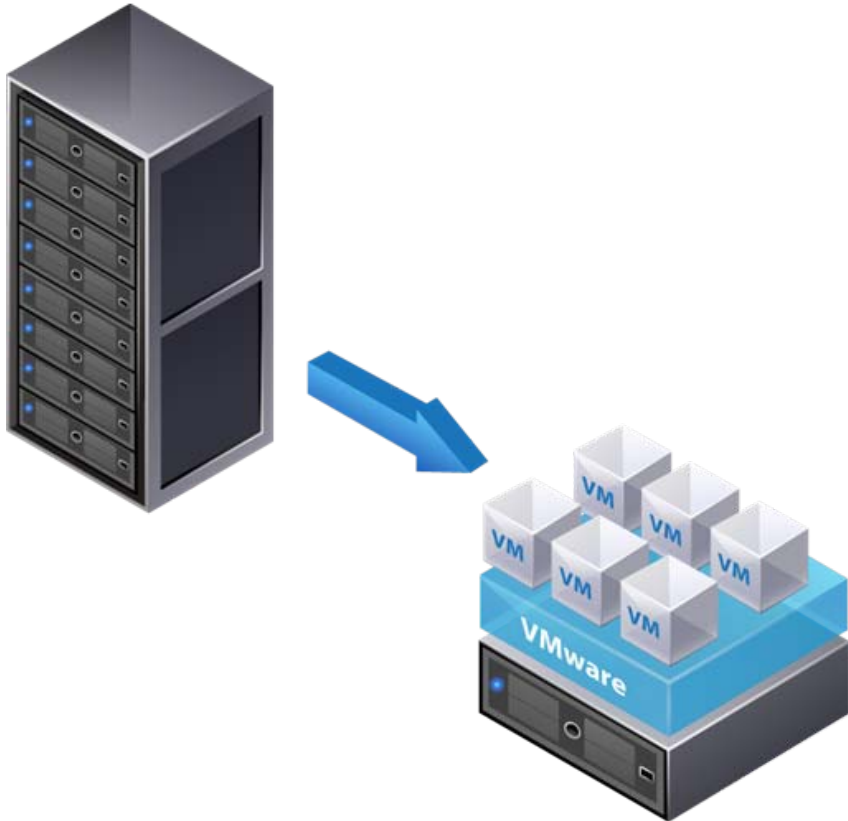


Securing The Virtualized DMZ



David Anderson
Data Center Solutions Architect
CCIE, CISSP

What Is Driving DMZ Virtualization?



Virtualization Benefits

- Lower Rack Space Utilization
- Power savings
- Better Utilization through resource consolidation
- Machine and Application mobility
- Reduced Deployment Times

Network Team Virtualization Concerns

- Policy Enforcement

 - Applied at physical server—not the individual VM
 - Impossible to enforce policy for VMs in motion

- Operations and Management

 - Lack of VM visibility, accountability, and consistency
 - Difficult management model and inability to effectively troubleshoot

- Roles and Responsibilities

 - Muddled ownership as server admin must configure virtual network
 - Organizational redundancy creates compliance challenges

- Machine Segmentation

 - Server and application isolation on same physical server
 - No separation between compliant and non-compliant systems...



Maintaining Compliance Through Virtualization

Common Requirements

- Access Controls
- Network Security
- Network resource segmentation
- Management and Monitoring
- Separation of Roles
- Limit Access to Virtual Infrastructure

Infrastructure

Nexus 1000V Features

- Access-lists, Layer 2 Anti-snooping features, QoS
- Private VLANs
- NetFlow, ERSPAN, Syslog
- Port Profiles
- AAA, RBAC

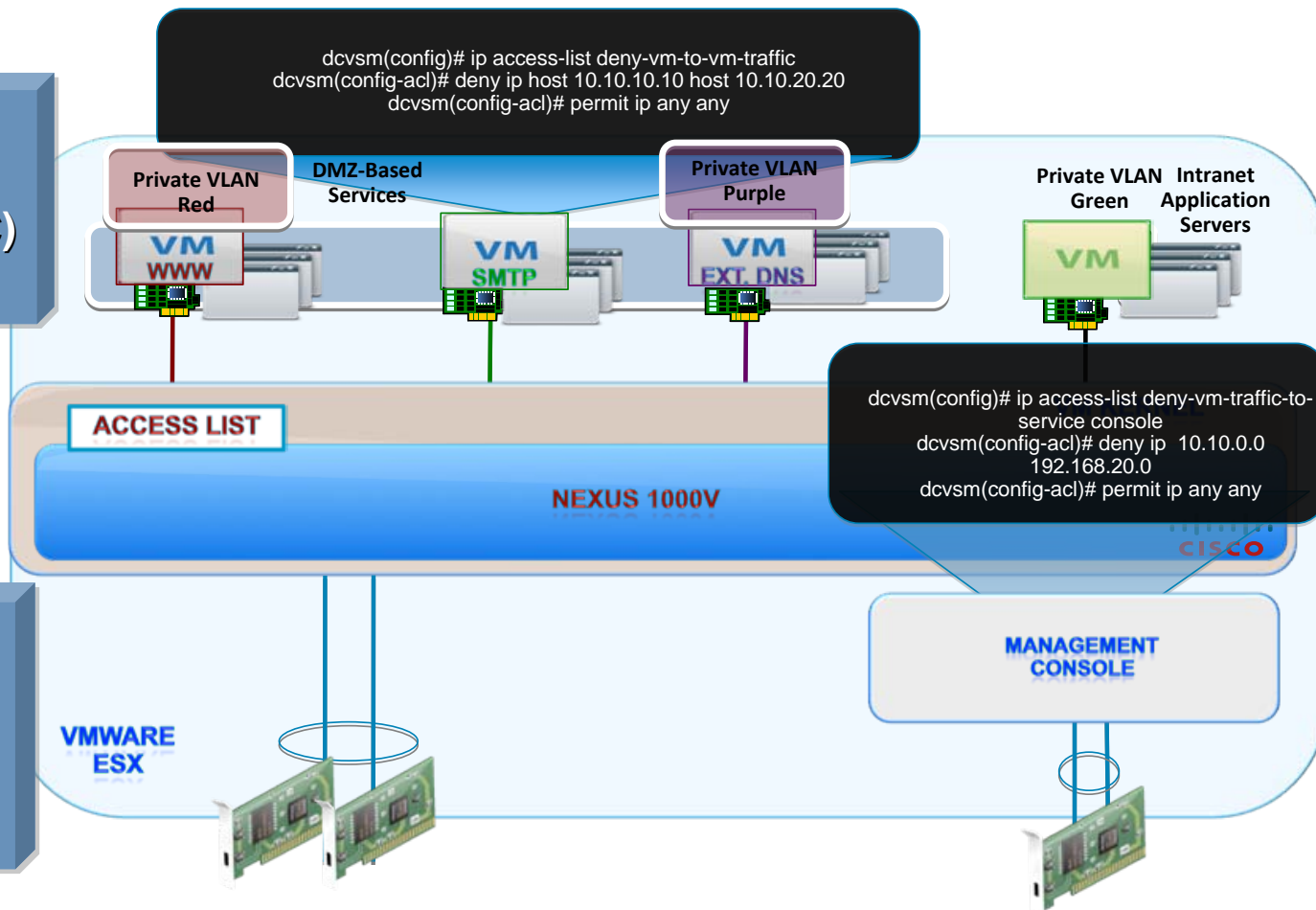
Nexus 1000V: Control and Isolation of Virtual Machine Traffic

Access Controls & Network Security

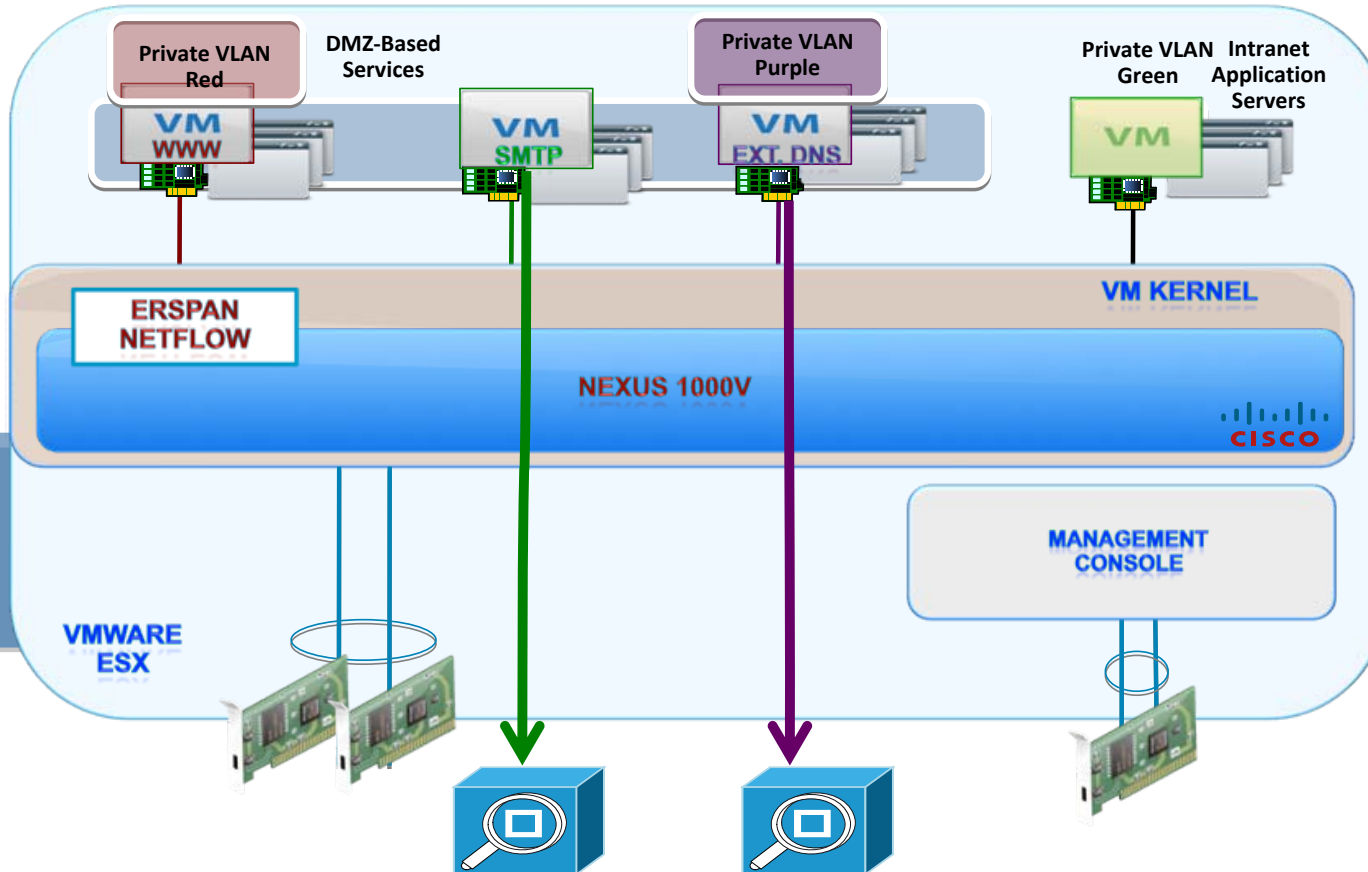
- Port ACLs (IP & MAC)

Network Segmentation

- VLANs
- Private VLANs



Nexus 1000V: Management and Monitoring Virtual Machine Traffic



VM Traffic Mirroring

- ERSPAN

VM Traffic Analysis and Reporting

- NetFlow
- Syslog

Nexus 1000V: Maintaining Roles & Workflows

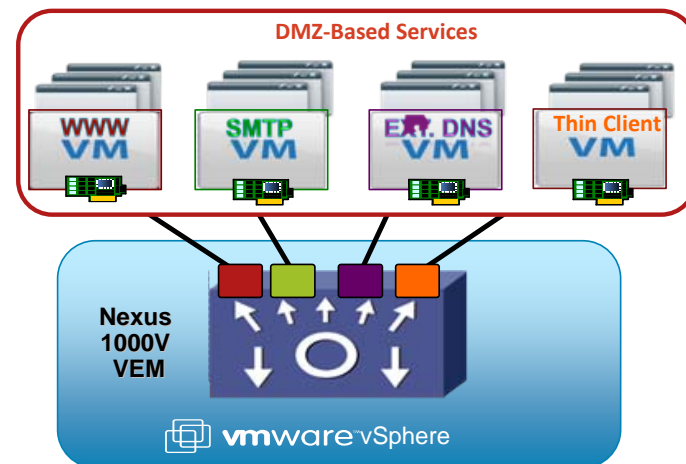
1. Nexus 1000V automatically enables port groups in Virtual Center via API
2. Server Admin uses Virtual Center to assign vnic policy from available port groups
3. Nexus 1000V automatically enables VM connectivity at VM power-on

VI Admin Benefits

- Maintains existing VM mgmt
- Reduces deployment time
- Improves scalability
- Reduces operational workload
- Enables VM-level visibility

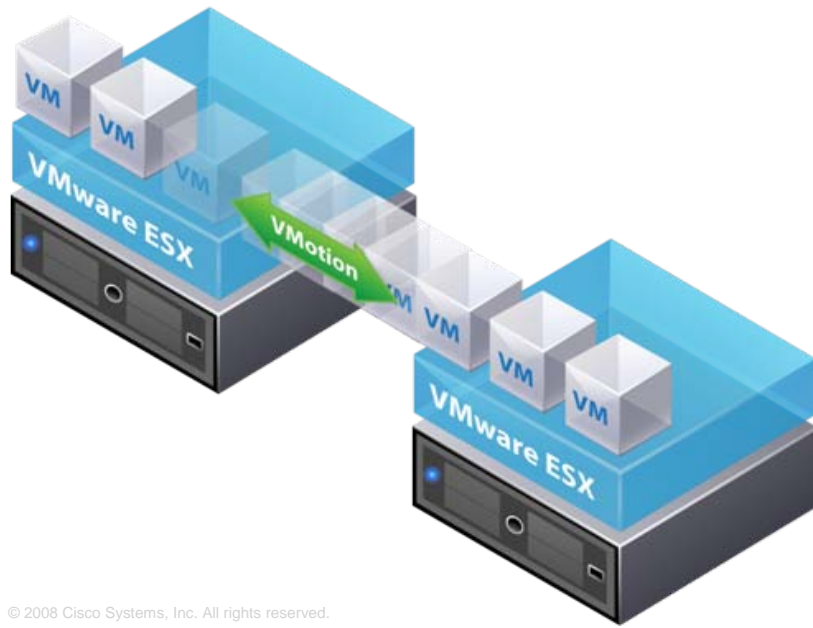
Network Admin Benefits

- Unifies network mgmt and ops
- Improves operational security
- Enhances VM network features
- Ensures policy persistence
- Enables VM-level visibility



Nexus 1000V: Security Policy Mobility with Vmotion

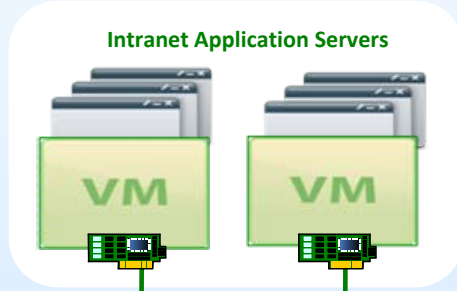
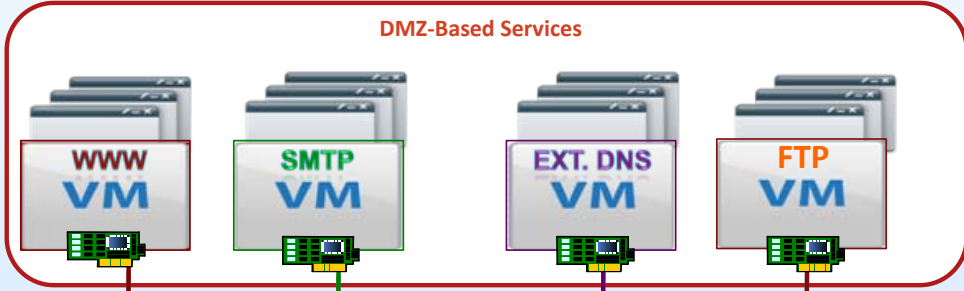
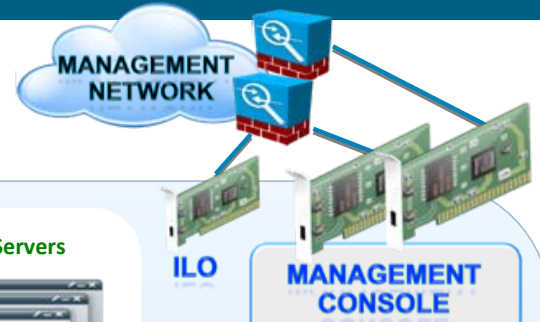
1. Virtual Center kicks off a VMotion (manual/DRS) & notifies Nexus 1000V
2. During VM replication, Nexus 1000V copies VM port state to new host
3. Once VMotion completes, port on new ESX host is brought up & VM's MAC address is announced to the network



Mobile Properties Include:

- Port policy
- Interface state and counters
- Flow statistics
- Remote port mirror session

The Virtualized DMZ: Nexus 1000V & VMware



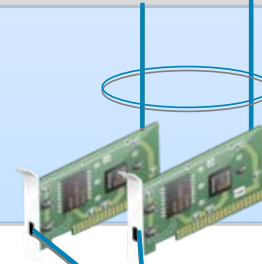
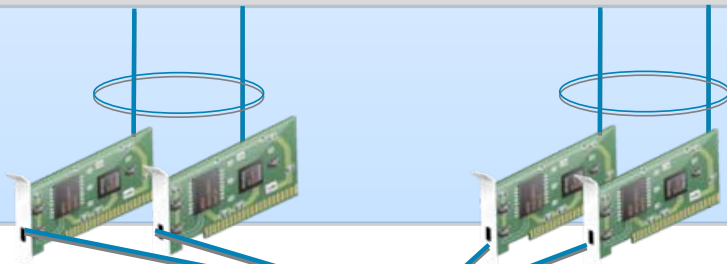
Virtual Ethernet (vnet) Adapters

Cisco Nexus 1000V Series

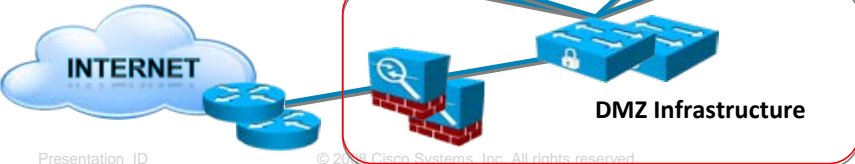
Uplink Ports

Uplink Ports

VM KERNEL



VMware ESX



Summary

Nexus 1000V:

- Supports traditional Network Capabilities
- Roles and workflows are unchanged
- VM security policies are the same as physical server policies
- Maintain Compliance requirements





For more information visit:
www.cisco.com/go/vmworld09



