Securely Architecting the Internal Cloud

Rob Randell, CISSP

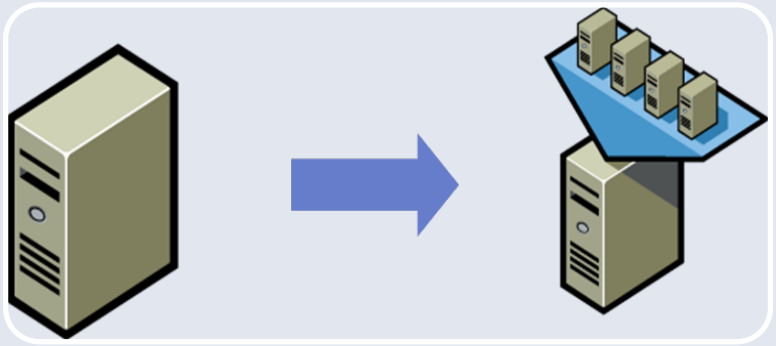
Senior Security and Compliance Specialist

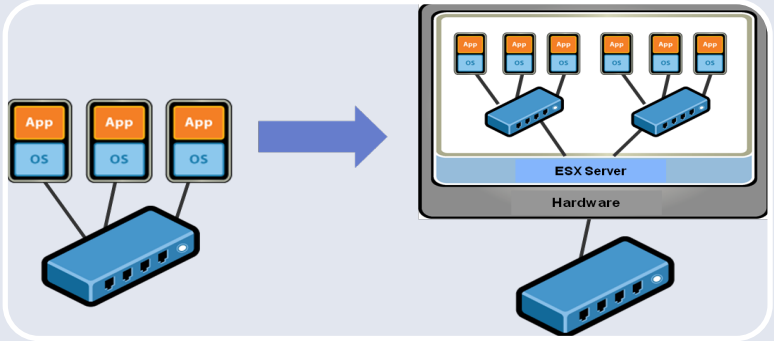
VMware, Inc.

Securely Building the Internal Cloud

- Virtualization is the Key
- How Virtualization Affects Data Center Security
- How Do We Secure Our Internal Cloud?

How Virtualization Affects Datacenter Security





Abstraction and Consolidation

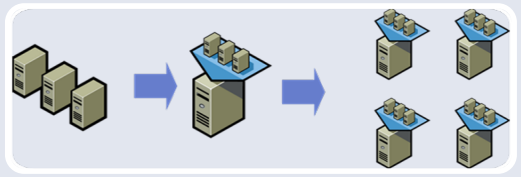
- ↑ Capital and Operational Cost Savings
- ↓ New infrastructure layer to be secured
- ↓ Greater impact of attack or misconfiguration

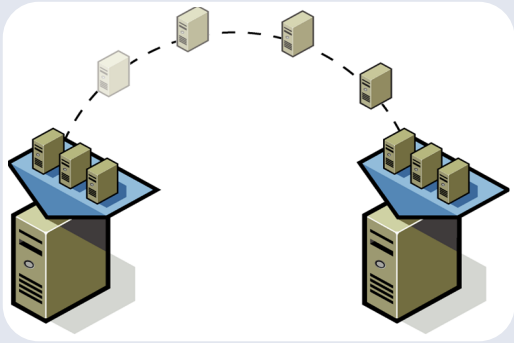
Collapse of switches and servers into one device

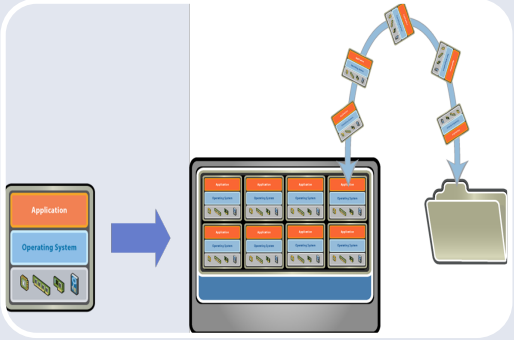
- ↑ Flexibility
- ↑ Cost-savings
- ↓ Lack of virtual network visibility
- ↓ No separation-by-default of administration

vmware

How Virtualization Affects Datacenter Security







Faster deployment of servers

- ↑ IT responsiveness
- ↓ Lack of adequate planning
- ↓ Incomplete knowledge of current state of infrastructure
- ↓ Poorly Defined Procedures
- ↓ Inconsistent Configurations

VM Mobility

- ↑ Improved Service Levels
- ↓ Identity divorced from physical location

VM Encapsulation

- ↑ Ease of business continuity
- ↑ Consistency of deployment
- ↑ Hardware Independence
- ↓ Outdated offline systems
- ↓ Unauthorized Copy

vmware

How do we secure our Internal Cloud?

Use the Principles of Information Security

- Hardening and Lockdown
- Defense in Depth
- Authorization, Authentication, and Accounting
- Separation of Duties and Least Privileges
- Administrative Controls

Securely Architecting Your Internal Cloud

- Creating Security Zones
  - Physical or Virtual Segmentation?
  - Separate vSwitches vs. 802.1q VLANs
  - Subzones
- Isolation of Management Interfaces
  - Access Options to Management Network

Securely Architecting Your Internal Cloud

- Designing in Separation of Duties and Least Privilege
  - Roles and Permissions
  - Key Roles
    - Network Administrator
    - Storage Administrator
    - VM Administrator
    - Other?
  - 3rd Party Virtual Switches
- Library of Secure and Up to Data Templates
  - True Gold Image Capability
- Resource Management
  - Prevention of DoS

Securely Architecting Your Internal Cloud

Hardening the Platform

- Hardening the Management Interfaces
  - Follow Guidance
    - VMware Hardening Guide
    - STIG
    - CIS
- Securing the VMs
- Auditing Administrator Activities

Defense in Depth

- Security Tools for the Cloud
  - Virtual Firewalls/IDS/IPS
  - Offline AV
  - Encryption
  - Other?

Creating Security Zones

Three Primary Configurations:

- Physical Separation of Trust Zones
- Virtual Separation of Trust Zone with Physical Security Devices
- Fully collapsing all servers and security devices into a VI3 infrastructure

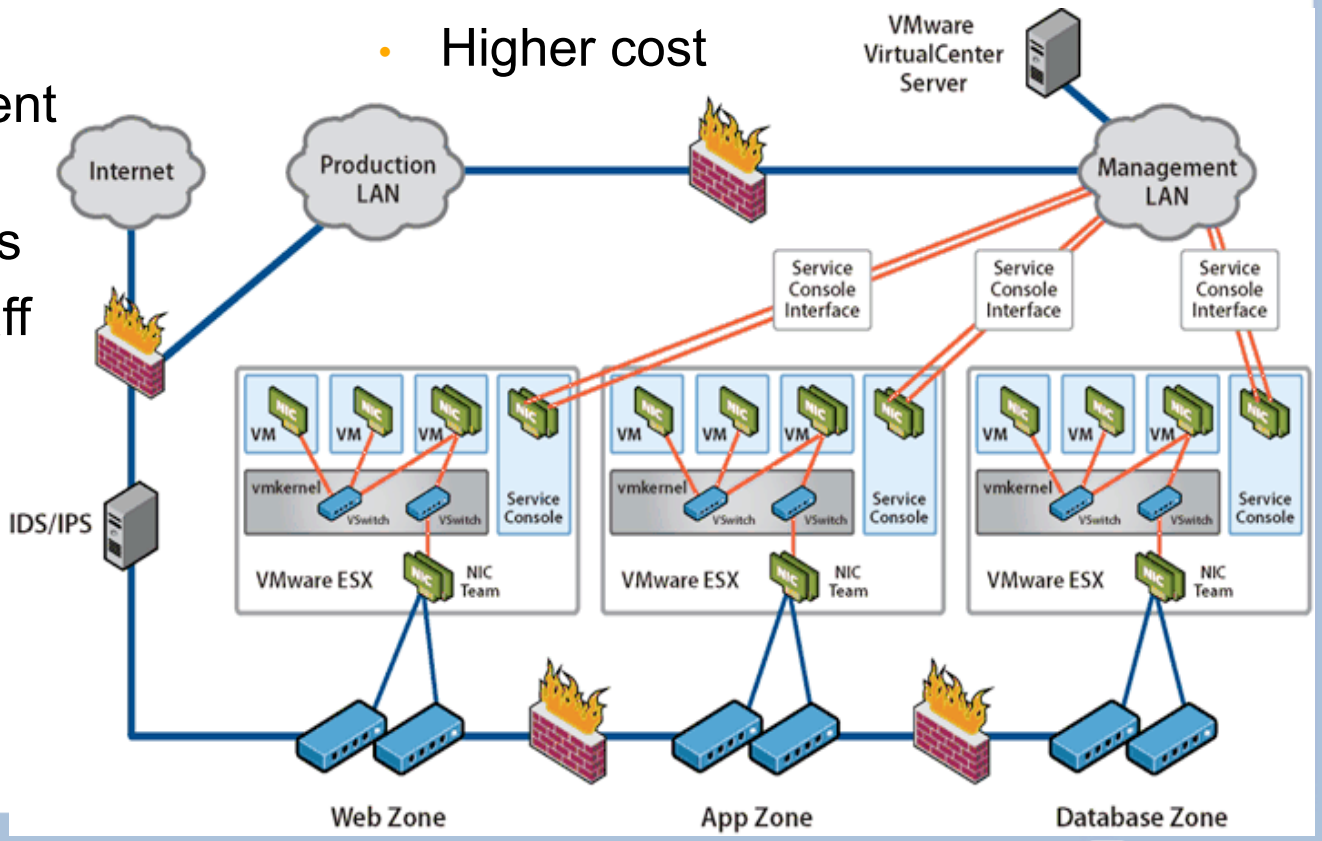
Physical Separation of Trust Zones

Advantages

- Simpler, less complex configuration
- Less change to physical environment
- Little change to separation of duties
- Less change in staff knowledge requirements
- Smaller chance of misconfiguration

Disadvantages

- Lower consolidation and utilization of resources
- Higher cost



vmware

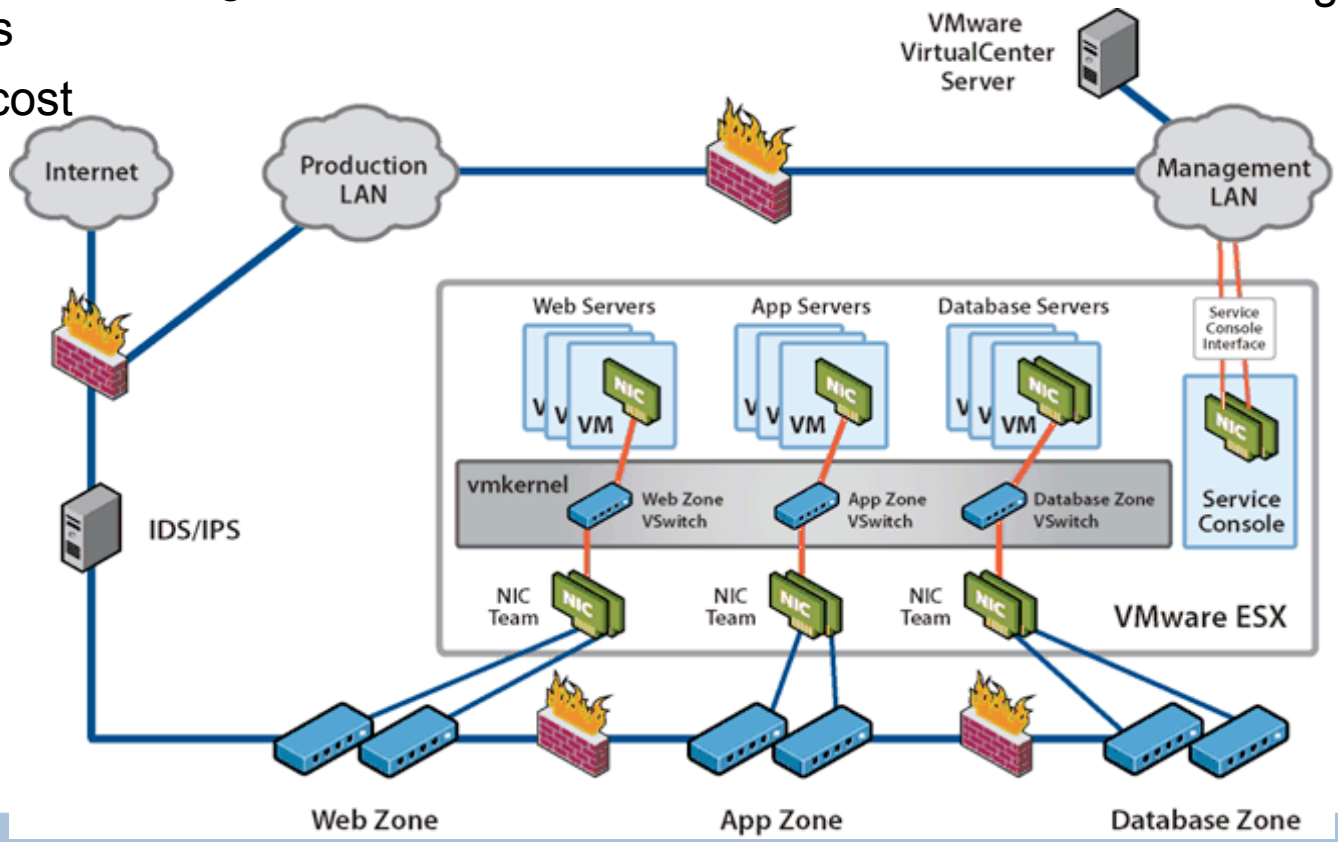
Virtual Separation of Trust Zones with Physical Security Devices

Advantages

- Better utilization of resources
- Take Full Advantage of Virtualization Benefits
- Lower cost

Disadvantages (can be mitigated)

- More complexity
- Greater chance of misconfiguration

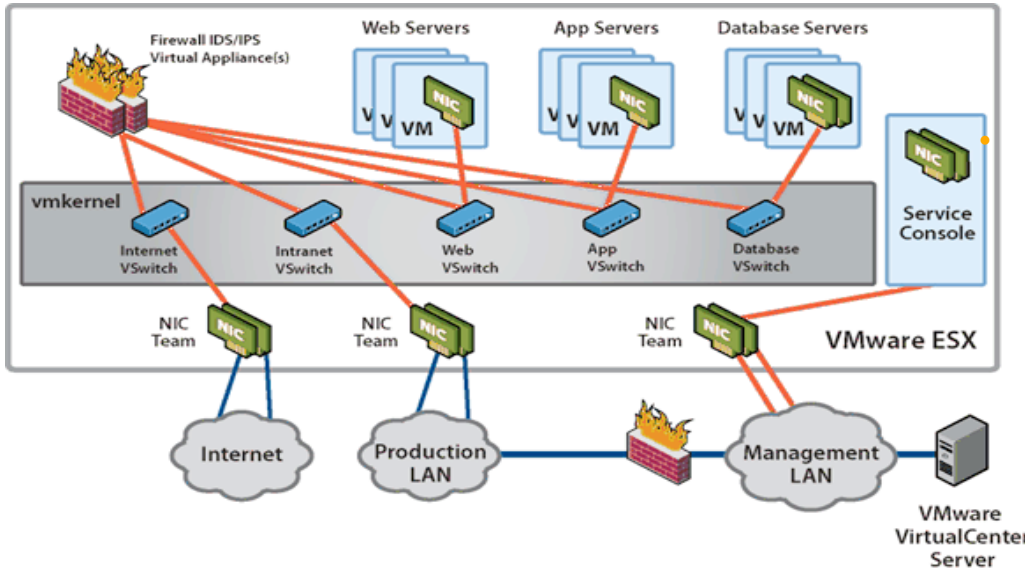


vmware

Fully Collapsed Trust Zones Including Security Devices

Advantages

- Full utilization of resources, replacing physical security devices with virtual
- Lowest-cost option
- Management of entire DMZ and network from a single management workstation



Disadvantages (can be mitigated)

- Greatest complexity, which in turn creates highest chance of misconfiguration
- Requirement for explicit configuration to define separation of duties to help mitigate risk of misconfiguration; also requires regular audits of configurations

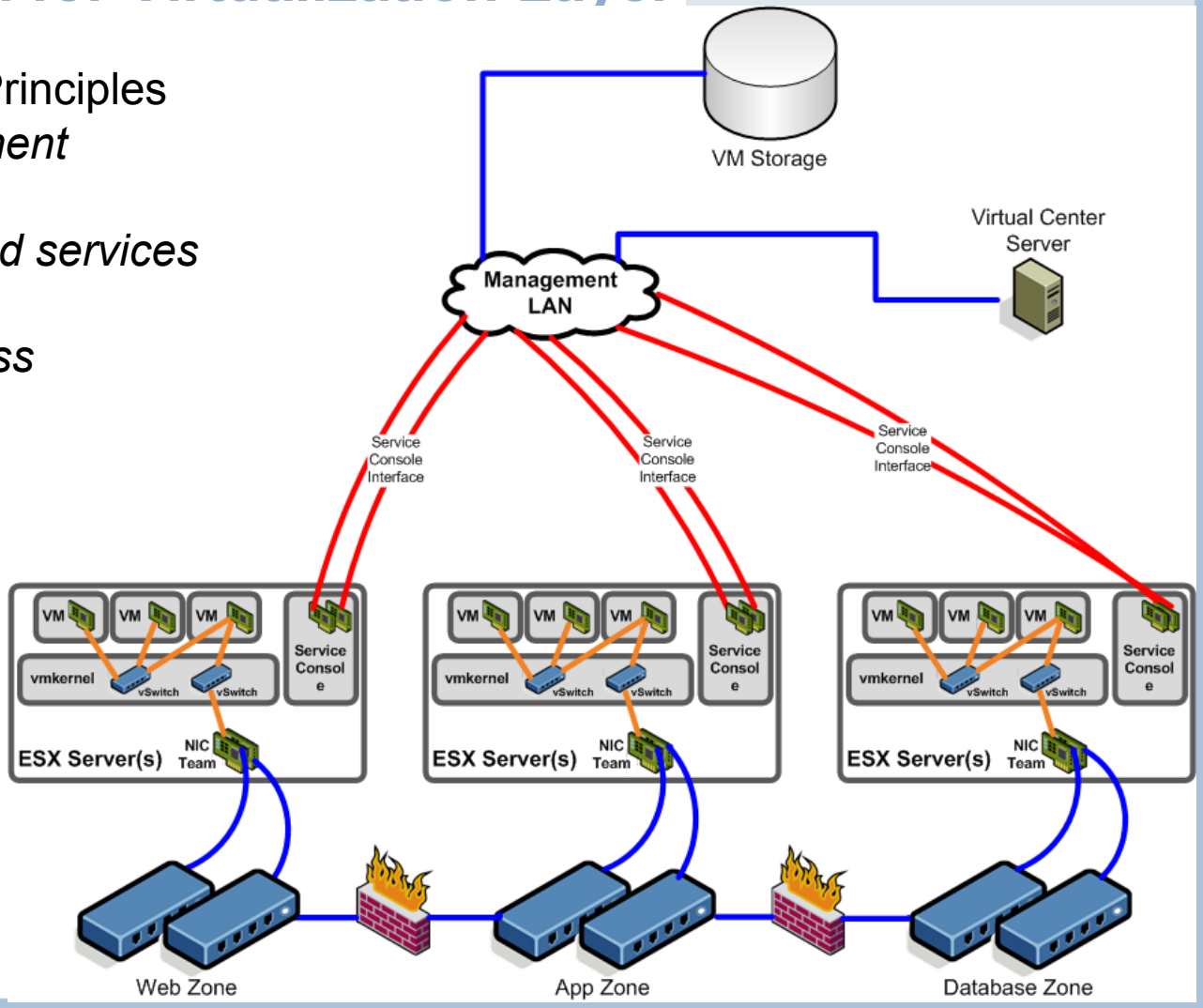
Potential loss of certain functionality, such as VMotion (Being mitigated by vendors and VMsafe)

vmware

Secure Design for Virtualization Layer

Fundamental Design Principles

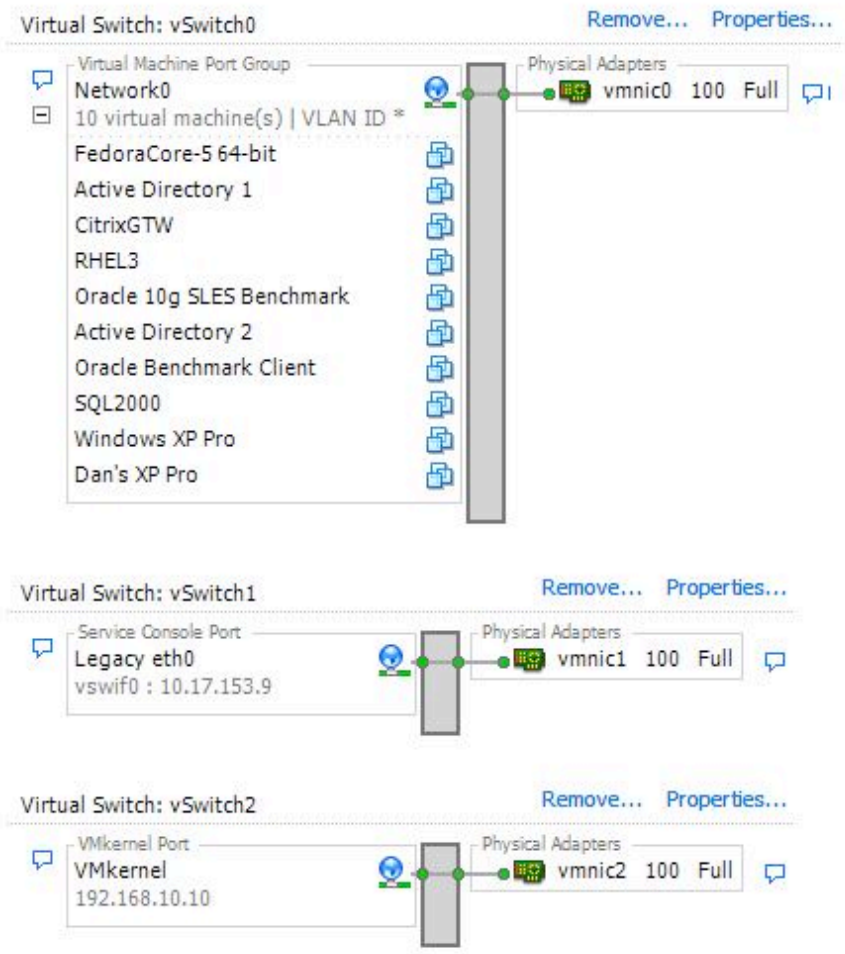
- *Isolate all management networks*
- *Disable all unneeded services*
- *Tightly regulate all administrative access*



Providing an Isolated Locked Down Network

Option 1: Maintain separate dedicated switches for network

- Provides strongest isolation
- Rapidly uses up NICs
- Greatly limits availability options



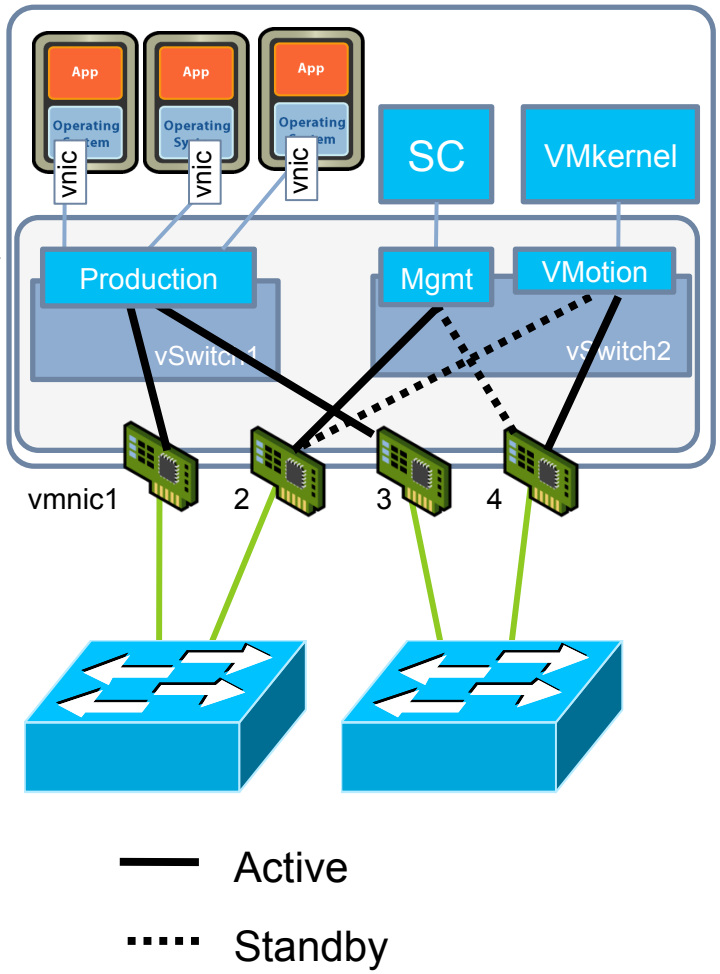
Providing an Isolated Locked Down Network

Option 2: Maintain separate dedicated VLAN on shared vSwitches

- Allows for greater redundancy for performance and availability
- Greater risk of misconfiguration

Example (pictured)

- 2 x 2-NIC teams
  - Production vSwitch
  - Mgmt vSwitch: Active/Standby reversed for Mgmt, VMotion
- VLANs for portgroup separation



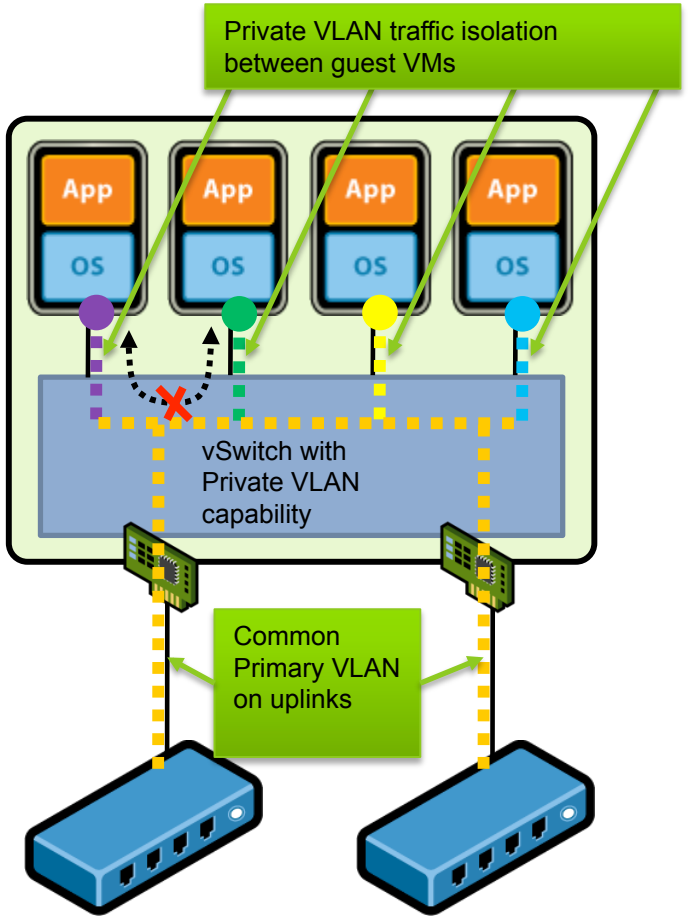
Providing an Isolated Locked Down Network

PVLAN (Private VLAN)

- Enables Layer-2 isolation between VMs on the same switch, even though they are on the same subnet
- Traffic from one VM forwarded out through uplink, without being seen by other VMs
- Communication between VMs on PVLANs can still occur at Layer-3

Benefits

- Scale VMs on same subnet but selectivity restrict inter-VM communication
- Avoids scaling issues from assigning one VLAN and IP subnet per VM



Providing an Isolated Locked Down Network

Virtual switches provide protection by design against typical layer 2 attacks:

- MAC flooding, 802.1q and ISL tagging attacks, Double-encapsulation attacks, Multicast brute-force attacks, Spanning-tree attacks, Random frame attacks
- Reason for immunity
  - vSwitches don't have to learn MAC address -- they know *exactly* what endpoints are attached to them
  - vSwitches have as many ports as you need -- don't require any mechanism to trunk or bridge them

Decision factors for using VLANs

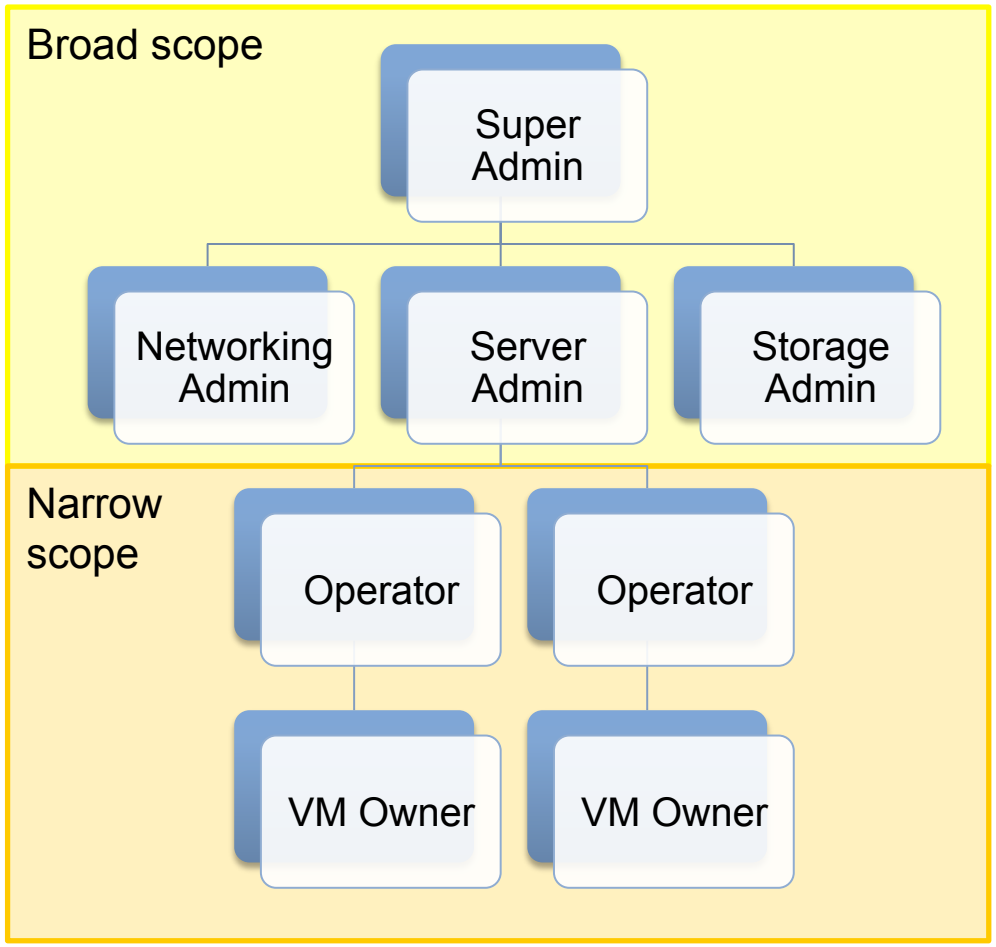
- Beliefs on isolation: is VLAN technology is mature/secure enough?
- Operational Security: can you maintain a secure configuration?
- Cost: Can you afford to not do it?

Providing an Isolated Locked Down Network

Options for Client Access

- Set up VPN access to Management network
- Create one or more “jump boxes” inside or outside the Management Network
  - Client applications (VI Client, VI SDK application) run on these
  - Access jump box only via RDP or other remote display protocol
  - Close off all other means of access to jump boxes
- Choose according to factors such as
  - Amount of trust placed in administrators and their environs
  - Level of inconvenience that’s tolerable
  - Cost

Separation of Duties

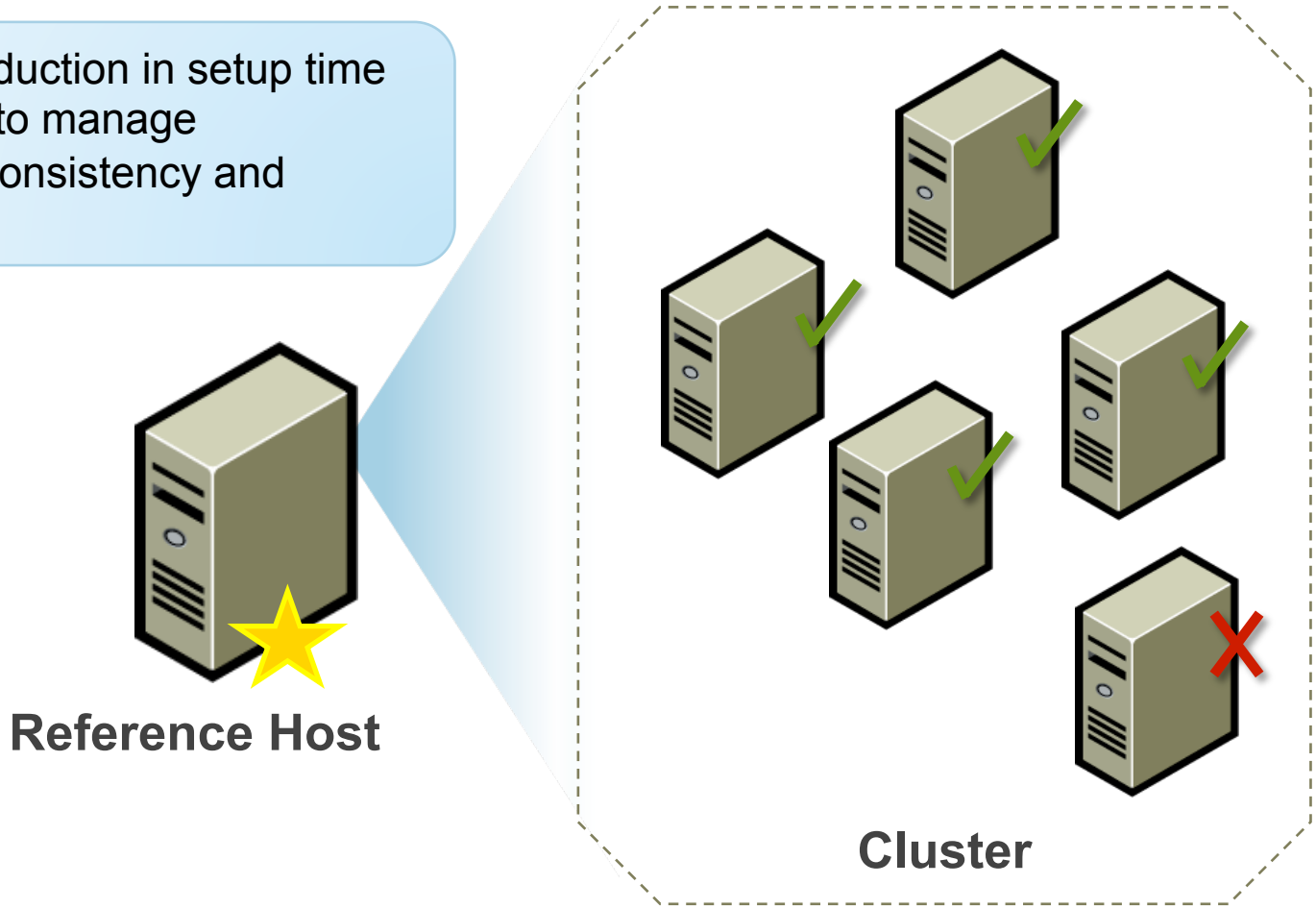


VM Templates: True “Gold” Images

- Hardware Independence Allows for True “Gold” Images
- Maintain a Library of Templates
  - Base Image of Each OS
  - Keep Fully Patched
    - Use an automated offline patch management tool if possible.
  - Regular Malware Scanning on Templates
    - Use a tool that can scan offline images
    - Ensures no latent malware embedded in templates
- Require the use of templates for ALL deployments
  - Exceptions must be approved for any other deployments
  - Put Controls In Place to Enforce This

Host Profiles

Allows for a reduction in setup time and allow you to manage configuration consistency and correctness.

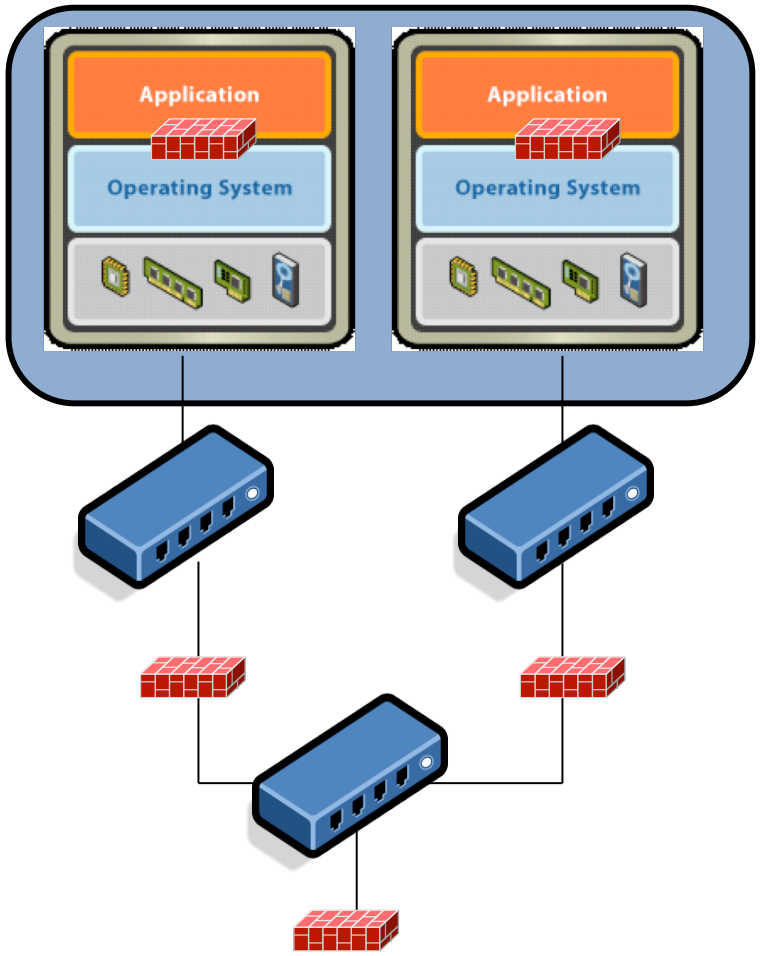


Containment: constrain guest behavior

Prevent resource Denial-of-Service

- Load balancing of CPU according to sharing policy
- Storage I/O limited according to sharing policy.
- Traffic-shaping available for virtual networks

Securing Virtual Machines



Provide Same Protection as for Physical Servers

Host

- Anti-Virus
- Patch Management

Network

- Intrusion Detection/ Prevention (IDS/IPS)
- Firewalls

Conclusion

- The Internal Cloud Had Great Benefits and Associated Risks
- Risks Can Be Mitigated With Proper Controls
- The Classic Principles of Information Security Should be Applied
- Key Architecture Decisions Must Be Made for Security

Questions?

Rob Randell, CISSP

Senior Security and Compliance Specialist

VMware, Inc.