# Virtualization Security and Best Practices

Rob Randell, CISSP

Senior Security Specialist SE

# Agenda

General Virtualization Concepts
- Hardware Virtualization and Application Virtualization
- Types of Hardware Virtualization

Virtualization Specific Security Issues and Advantages
- Security Concepts in Virtualization Architecture
- Operational Security Issues with Virtualization
- Other Concerns
- Security Advantages of Virtualization

Security Best Practices
- Secure Design
- Secure Deployment
- Secure Operations

Common Virtualization Security Concerns and Misconceptions
- Are there any Hypervisor Attack Vectors?
- Virtualizing the DMZ
- Common Misconceptions about Virtualization Security

# Virtualization Concepts

Hardware Virtualization

- Makes an OS think it is running on it own hardware
- Abstracts the hardware from the OS
- VMware, MS Virtual PC, Xen are forms of hardware virtualization

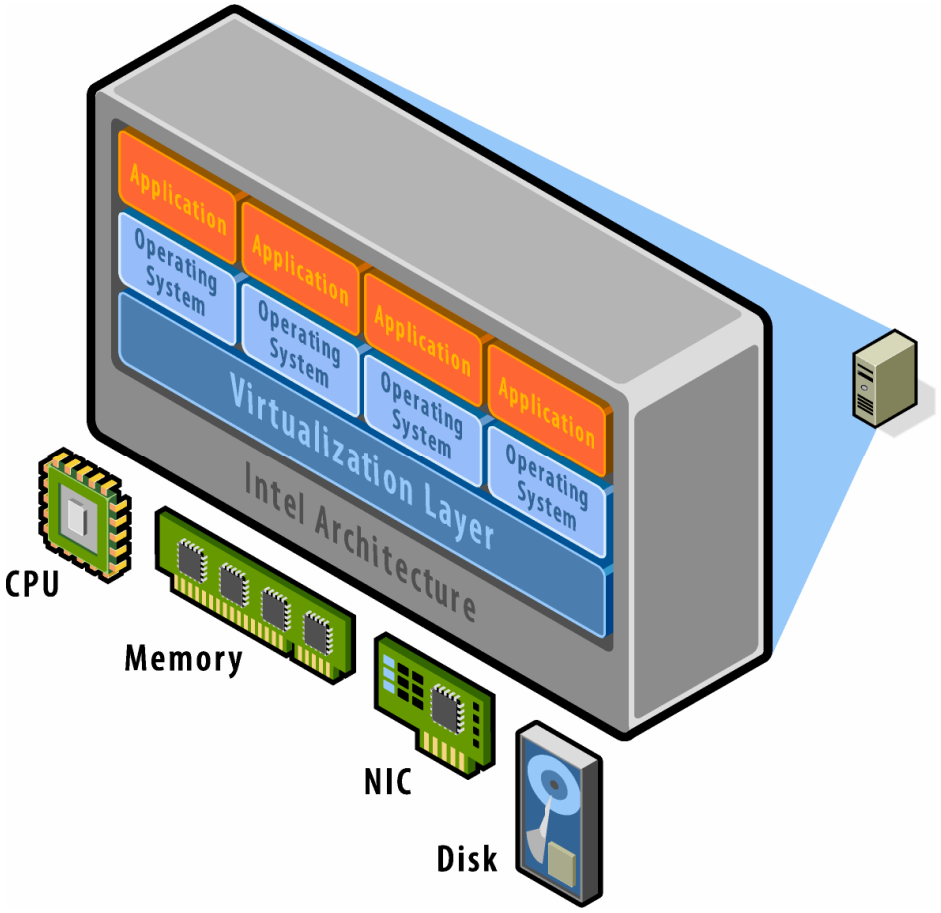
Application Virtualization

- Makes an application thinks it is running in its own OS
- Abstracts the services and kernel from an application
- Thinstall and Softgrid are forms of application virtualization

# Bare Metal Hardware Virtualization

Bare Metal (Hypervisor)

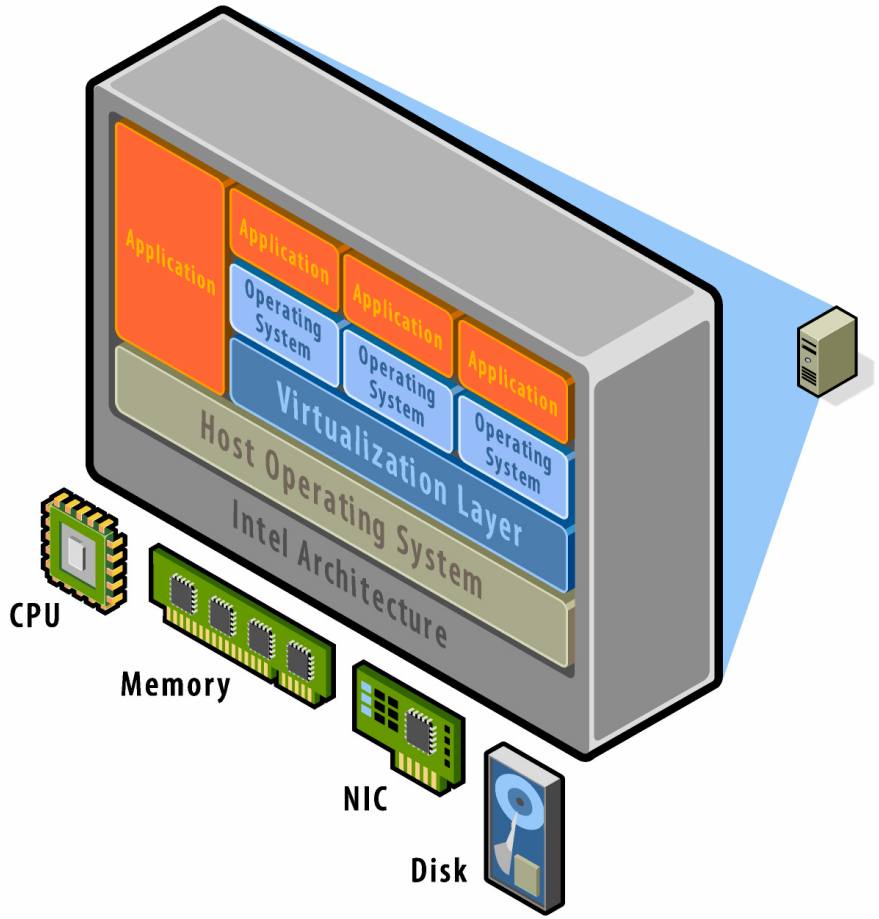
- Virtualization Engine Installs Directly on Hardware
- No reliance on an underlying OS
- VMware ESX Server, XEN, MS Hyper-V



# Hosted Hardware Virtualization

Hosted

- Relies on an underlying OS
- More security implications because of the reliance on the underlying OS
- VMware Workstation, VMware Server, VMware Player, MS Virtual PC and Server



# Security Concepts in Architecture

Extended computing stack

- New privileged layers (Hypervisor) exist underneath the operating system that need to be considered

Guest isolation

- One guest VM cannot be allowed to access or even address the “hardware resources” of another guest VM or the host/hypervisor

Host Visibility from the Guest

- Can the guest OS detect that it is virtualized and if so can it see anything on the host.

Virtualized interfaces

- Physical connectivity between guests is recreated, e.g. IP network, file shares, may be more or less like true physical counterparts

Management interfaces

- The protection of management interfaces (Console OS, VirtualCenter, etc…) very important.
- Root or Administrator Access to these interfaces provides “keys to the kingdom”.

Greater co-location of data and assets on one box

- Concept of mixing of Trust/Security Zones on a single physical box

# Operational Security Issues

Most security issues arise not from the virtualization infrastructure itself but from operational issues

- Adapting existing security processes and solutions to work in the virtualized environment
- Most security solutions don't care whether a machine is physical or virtual
- The datacenter and its workloads just became a much more dynamic and flexible place
- The risk of misconfiguration requires use of best practices specific to virtualization

# Security Advantages of Virtualization

Better Forensics and Faster Recovery After an Attack

- A compromised machine can be **cloned in it current compromised state for forensic analysis**
- Once cloned the **VM can be immediately restored to a known good snapshot** which is much faster than a physical server, reducing the impact of a security-related event

Patching is Safer and More Effective

- You can **quickly revert to a previous state if a patch is unsuccessful**, making you more likely to install security patches sooner
- You can create a clone of a production server easily, making you **more likely to test security patches** and more likely to install security patches
- VMware Update Manager does patch scanning and compliance reporting, along with **patch remediation for both online and offline VMs** – again, making it more likely that security patches will be installed

More Cost Effective Security Devices

- You can put in place cost effective intrusion detection, vulnerability scanning, and other security related appliances, because you can put them in a VM instead of a physical server

Future: Leveraging Virtualization to Provide Better Security

- Better Context – Provide protection from outside the OS, from a trusted context
- New Capabilities – view all interactions and contexts
  - CPU
  - Memory
  - Network
  - Storage

# Security Best Practices

# Security Best Practices

## Secure Design

Separate and Isolate Management Networks

- Service Console
- Vmkernel: Vmotion and NFS & iSCSI datastores

Plan for VM mobility: 3 options

- Partition trust zones
- Combine trust zones using virtual network segmentation and virtual network management best practices
- Combine trust zones using portable VM protection with 3rd-party tools (Blue Lane, etc)

# Security Best Practices

## Secure Deployment

Harden VMware Infrastructure 3 according to guidelines

- VMware-provided
- 3rd-party: STIG, CIS, Xtravirt Security Risk Assessment template, etc.

Always secure virtual machines like you would physical servers

- Anti-virus
- Patching
- Host-based intrusion detection/prevention
- Use Templates and Cloning to enforce conformity of virtual machines

## Secure Operations

Strictly control administrative access

- Favor controlled management interfaces (VI Client, Web Access) over unstructured interfaces (Service Console)
- Avoid VI Console access except when absolutely necessary; favor OS-based access to VM (RDP, ssh, etc).
- Use roles-based access control to limit administrative capabilities and enforce separation of duties, and never use anonymous accounts (e.g. “Administrator”)
- Allow powerful access only to small, privileged group; implement break-glass policy for top level administrative account

# Security Best Practices

## Secure Networking

Restrict access to privileged networks

- Closely restrict administrative access on any host with privileged network
- For less privileged users, only allow template-based provisioning on those hosts

Guard against misconfiguration

- Clearly label sensitive virtual networks
- Generate audit reports that flag suspicious configurations
- Routinely inspect event and task logs

# Best Practices References

## Detailed Prescriptive Guidance

- Security Design of the VMware Infrastructure 3 Architecture (http://www.vmware.com/resources/techresources/727)
- VMware Infrastructure 3 Security Hardening (http://www.vmware.com/vmtn/resources/726)
- Managing VMware VirtualCenter Roles and Permissions (http://www.vmware.com/resources/techresources/826)
- STIG (Secure Technology Implementation Guide) draft (http://iase.disa.mil/stigs/draft-stigs/index.html)
- CIS (Center for Internet Security) Benchmark (http://www.cisecurity.org/bench_vm.html)
- Xtravirt Virtualization Security Risk Assessment (http://www.xtravirt.com/index.php?option=com_remository&Itemid=75&func=fileinfo&id=15)

# Common Virtualization Security Concerns

# Are there any Hypervisor Attack Vectors?

There are currently no known hypervisor attack vectors to date

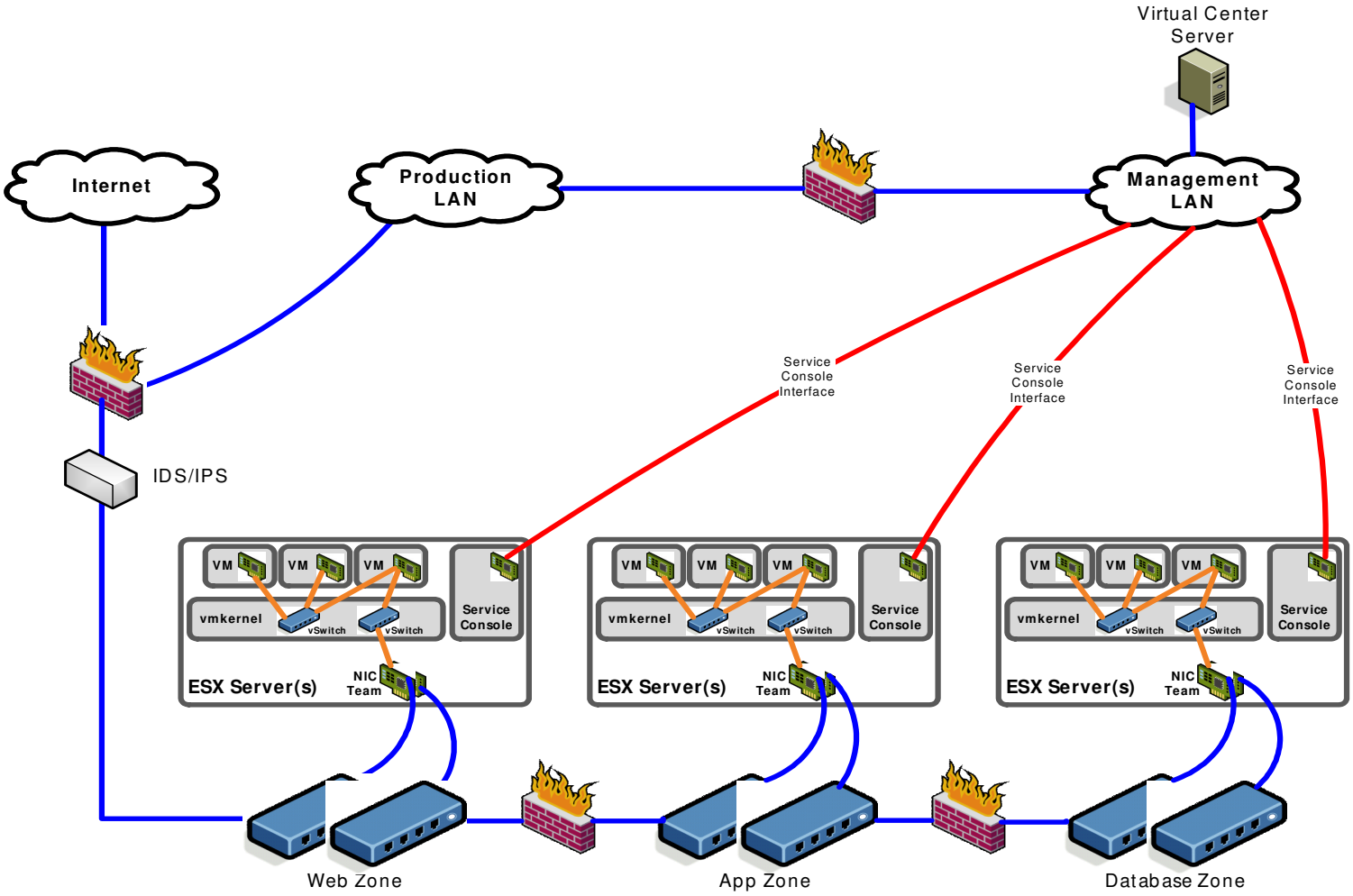
- The ESX Server Hypervisor has not been known to be compromised to date.
  - Concern is the potential for “VM Escape”
- Potential Vectors?
  - Architectural Vulnerability
    - Small Code Footprint of Hypervisor is Big Advantage
    - Must be Designed specifically with Isolation in Mind
  - Software Vulnerability
    - Possible like with any code written by humans
    - If a software vulnerability is found, exploit difficulty will be very high
    - Depends on Vendor’s Security Response and Patch Release Speed
  - Configuration Risk
    - Biggest Risk to Virtual Infrastructure
    - Follow Best Practices to Avoid

# Concern: Virtualizing the DMZ

Multiple different configurations can be used depending on environment

- Collapsing of servers in each trust zone into their own cluster of ESX Servers
  - Safer for those that won't or can't fully trust our isolation ability
  - Small risk of misconfiguration creating a security hole
  - Does not take full advantage of consolidation benefits.

# Partial Collapse of DMZ








vmware

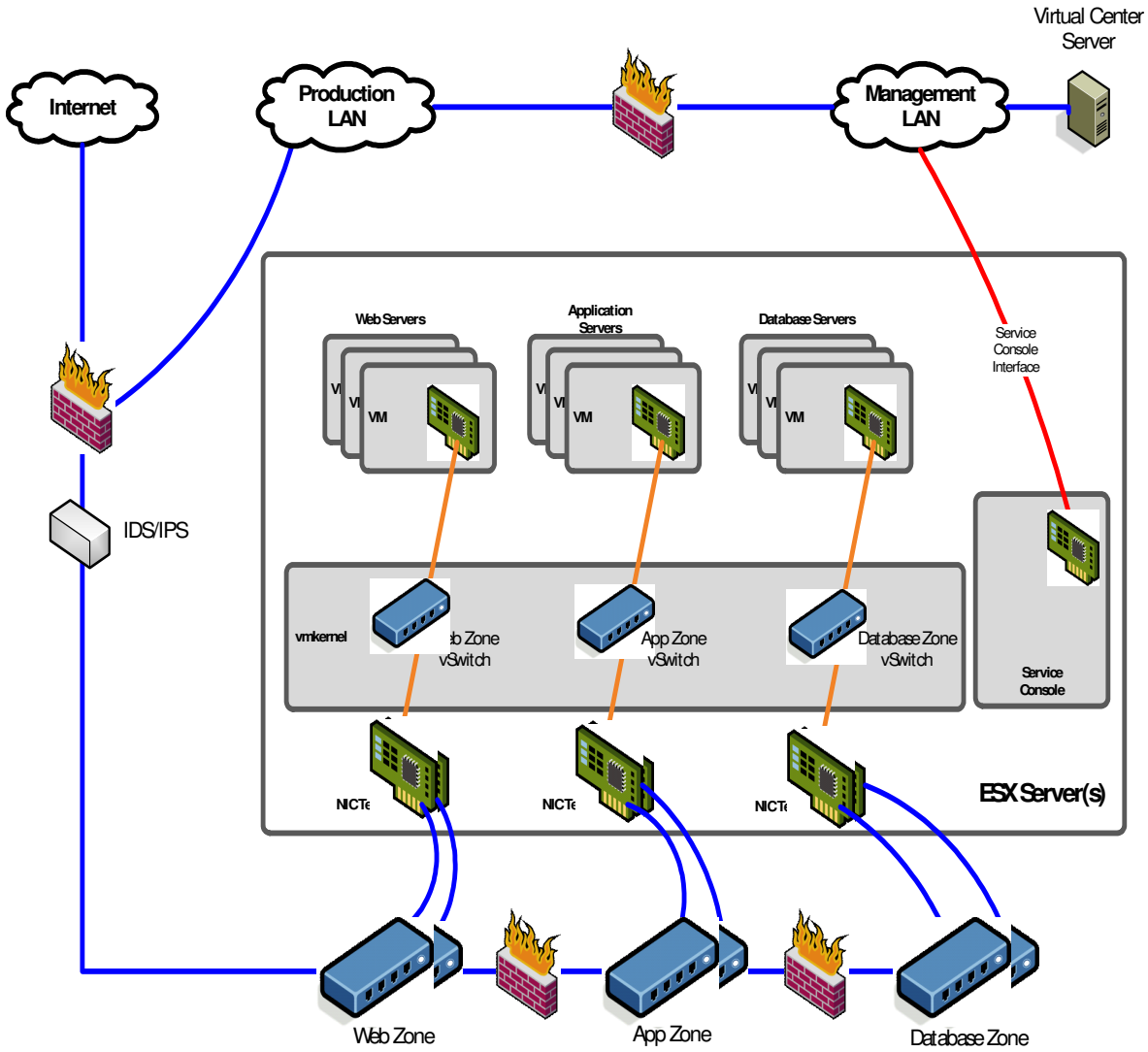
# Concern: Virtualizing the DMZ

Multiple different configurations can be used depending on environment

- Collapsing of servers in each trust zone into their own cluster of ESX Servers
  - Safer for those that won't or can't fully trust our isolation ability
  - Small risk of misconfiguration creating a security hole
  - Does not take full advantage of consolidation benefits.

- Collapsing all servers in multiple trust zones to a single cluster of ESX Servers using virtual networking and physical security devices to enforce isolation
  - Takes full advantage of virtualization benefits so it is more cost effective.
  - Bigger risk of misconfiguration creating a security hole.
  - Not an option if an organization doesn't or can't trust our isolation ability

# Hybrid of Partial and Full Collapse



# Concern: Virtualizing the DMZ

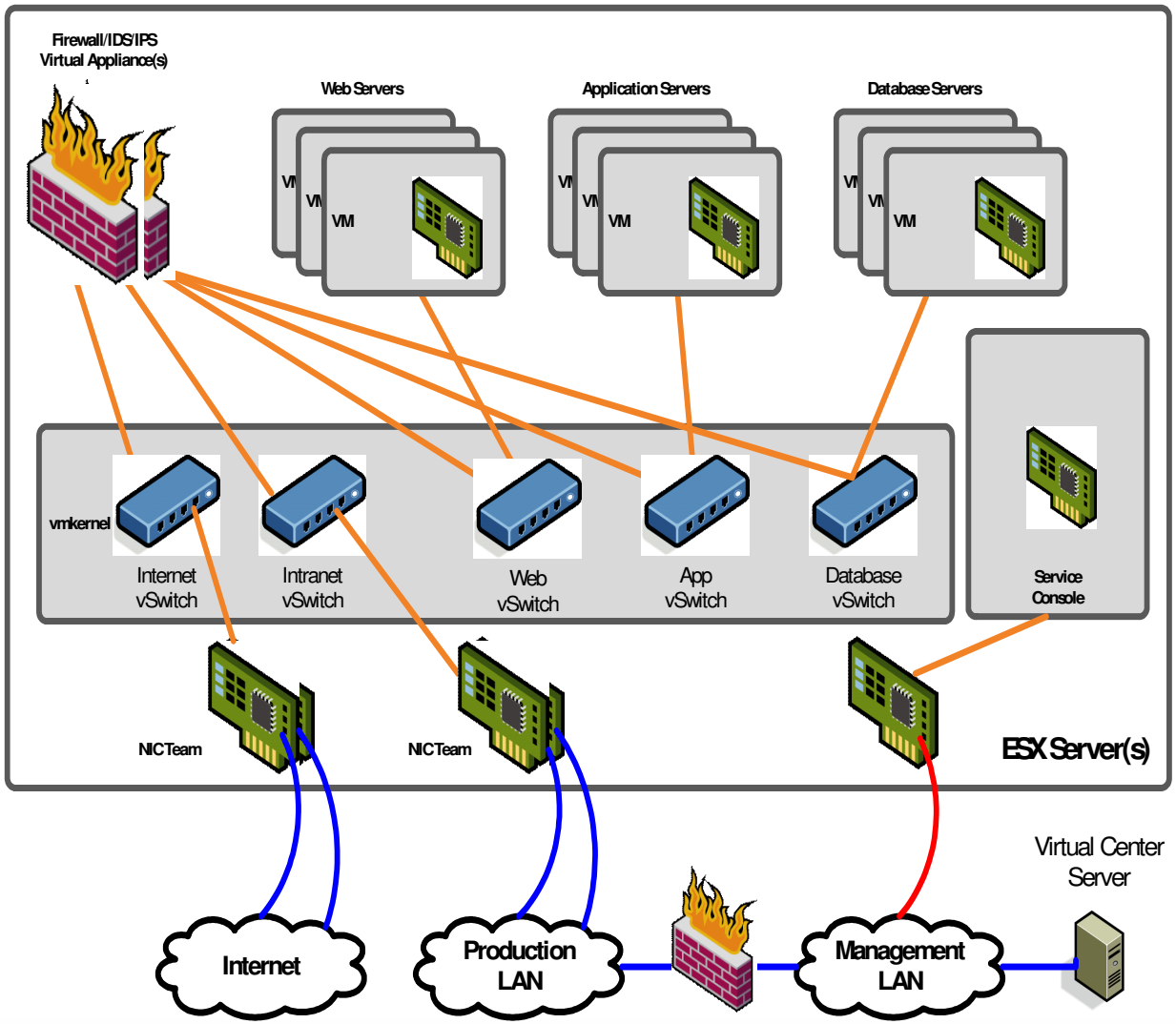
Multiple different configurations can be used depending on environment

- Collapsing of servers in each trust zone into their own cluster of ESX Servers
  - Safer for those that won't or can't fully trust our isolation ability
  - Small risk of misconfiguration creating a security hole
  - Does not take full advantage of consolidation benefits.

- Collapsing all servers in multiple trust zones to a single cluster of ESX Servers using virtual networking and physical security devices to enforce isolation
  - Takes full advantage of virtualization benefits so it is more cost effective.
  - Bigger risk of misconfiguration creating a security hole.
  - Not an option if an organization doesn't or can't trust our isolation ability

- Fully collapsing all servers and security devices into a Virtual Infrastructure
  - Takes even more advantage of consolidation by virtualizing security devices,
  - Lose some capabilities due to current limitations of those virtual security devices
  - Future developments in virtual security devices will remove those limitations

# Full Collapse



# Common Misconceptions about VMware Security

## Commonly cited: Blue Pill, SubVirt

- These are **NOT hypervisor vulnerabilities**, but use the concept of a hypervisor to embed themselves underneath an OS by leveraging hardware enabled virtualization (AMD Pacifica Chipset)
- These can only affect non-virtualized operating systems
- Therefore, you are safer running in a VM

## Various Claims of Guest Escape

- **Don't affect Bare-Metal Platforms** only hosted platforms
- Not exactly escape nor a hypervisor vulnerability
- Uses documented communication interface for "hosted" features such as drag-n-drop, cut –n-paste, and shared folders.
- This communication interface can be disabled (on by default)

# Other Concerns

Restricted view into inter-VM traffic for inspection by intrusion detection/prevention systems (IDS/IPS).

- This is possible currently with the use of a helper VM or forcing traffic out to physical network
- Vendors need to address this and provide this capability
- Interesting issue to be brought up though because few organizations monitor traffic that deep in the network.

Limited visibility into the host OS and virtual network to find vulnerabilities and assess correct configuration.

- VMware is working closely with leading security vendors to help create virtualization specific security tools and give the needed visibility for these tools.
- VMSafe will provide APIs for Security Vendors for unparalleled visibility and security capabilities

Patching, signature updates, and protection from tampering for offline VM images.

- Virtualization Vendor should provide capability for the patching of both online and offline VMs
- Patching VMs is safer than patching physical systems with the use of “snapshot” feature for testing and deployment of patches
- Some major security vendors are near release for the ability to update AV and HIPS signatures for offline VMs

# Questions?

Rob Randell, CISSP

Senior Systems Engineer - Security Specialist