

VMware Security Briefing

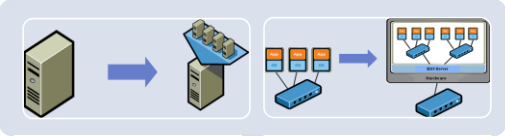
Rob Randell, CISSP
Senior Security Specialist SE

VMware Security Strategy

 <p>Core Platform Security</p> <ul style="list-style-type: none"> □ New platform hardening features further enhance robust security capabilities □ Thin-hypervisor strategy □ Memory Protection □ Kernel Module Protections 	 <p>Operationalize Security</p> <ul style="list-style-type: none"> □ Integrate VMware products into existing operational policies in the enterprise 	 <p>Security Virtual Appliances</p> <ul style="list-style-type: none"> □ Enable broad-based security for every VM in the environment □ "Democratize" security 	 <p>Better Than Physical: Adaptive Security Infrastructure</p> <ul style="list-style-type: none"> □ Self-describing, Self-configuring security □ Impact security by taking advantage of unique VMware technologies □ Focus on products and operations
---	--	---	--

VMware Confidential/Proprietary

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

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- ↓ Outdated offline systems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

Biggest Security Risk: Misconfiguration

Neil MacDonald – "How To Securely Implement Virtualization"



"Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement"

What *not* to worry about

Hypervisor Rootkits

- Examples: Blue Pill, SubVirt, etc.
- These are ALL theoretical, highly complex attacks
- Widely recognized by security community as being only of academic interest

Irrelevant Architectures

- Example: numerous reports claiming guest escape
- Apply only to hosted architecture (e.g. Workstation), not bare-metal (i.e. ESX)
- Hosted architecture generally suitable only when you can trust the guest VM

Contrived Scenarios

- Example: VMotion intercept
- Involved exploits where
- Best practices around hardening, lockdown, design, for virtualization etc, not followed, or
- Poor general IT infrastructure security is assumed

Security Advantages of Virtualization

- Allows Automation of Many Manual Error Prone Processes
- Cleaner and Easier Disaster Recovery/Business Continuity
- Better Forensics Capabilities
- Faster Recovery After an Attack
- Patching is Safer and More Effective
- Better Control Over Desktop Resources
- More Cost Effective Security Devices
- App Virtualization Allows de-privileging of end users
- Better Lifecycle Controls
- Security Through VM Introspection

vmware

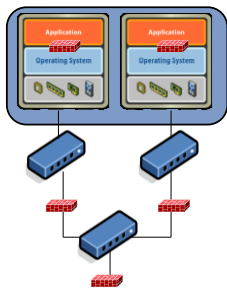
How do we secure our Virtual Infrastructure?

Use the Principles of Information Security

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

vmware

Securing Virtual Machines



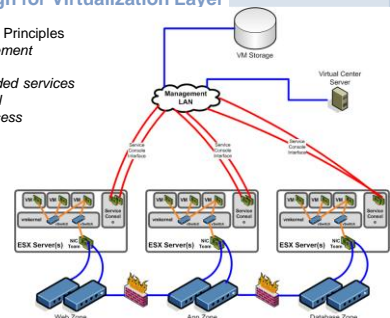
Provide Same Protection as for Physical Servers

- Host**
- > Anti-Virus
 - > Patch Management
- Network**
- > Intrusion Detection/Prevention (IDS/IPS)
 - > Firewalls

vmware

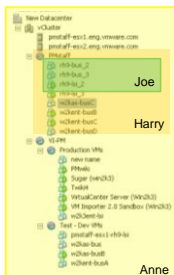
Secure Design for Virtualization Layer

- Fundamental Design Principles
- Isolate all management networks
 - Disable all unneeded services
 - Tightly regulate all administrative access



vmware

Enforce Strong Access Controls



Security Principle	Implementation in VI
Least Privileges	Roles with only required privileges
Separation of Duties	Roles applied only to required objects

- Administrator
- Operator
- User

vmware

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

vmware

Use Case: Virtualizing the DMZ / Mixing Trust 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 the virtual environment

vmware

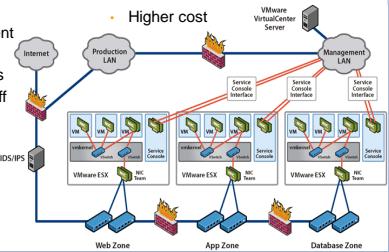
Physical Separation of Trust Zones

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

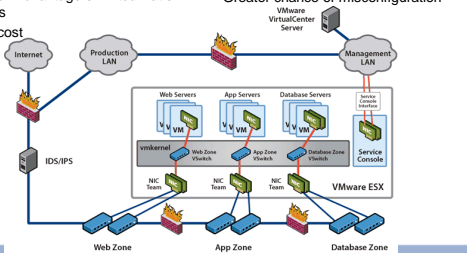
Virtual Separation of Trust Zones with Physical Security Devices

Advantages

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

Disadvantages (can be mitigated)

- More complexity
- Greater chance of misconfiguration



vmware

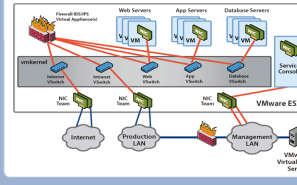
Fully Collapsed Trust Zones Including Security Devices

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



vmware

vmware

Questions?

Rob Randell, CISSP
Senior Security Specialist SE