Security in a Virtualised Environment

An Ethical Hacker's View

Peter Wood

Chief Executive Officer

First•Base Technologies LLP

Agenda

- Overview and Introduction to Virtualisation
- Security Risks in Virtualised Environments
- Controls in Virtualised Environments
- Summary and Conclusions

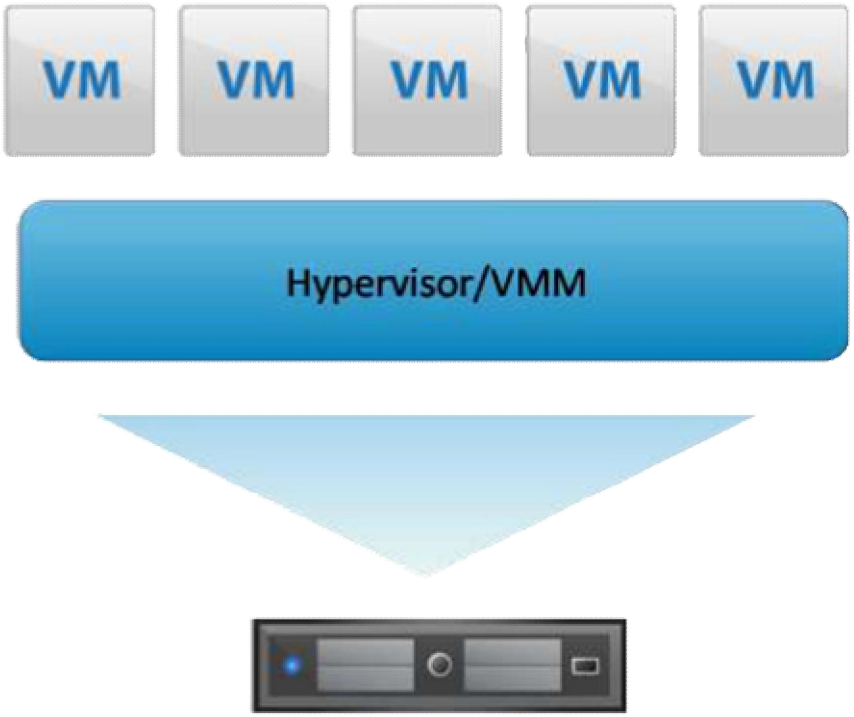
Overview and Introduction to Virtualisation

Types of Virtualisation

- Servers
- Operating systems
- Desktops
- Applications
- Storage
- Networks
- … etc.

Server Virtualisation (1)

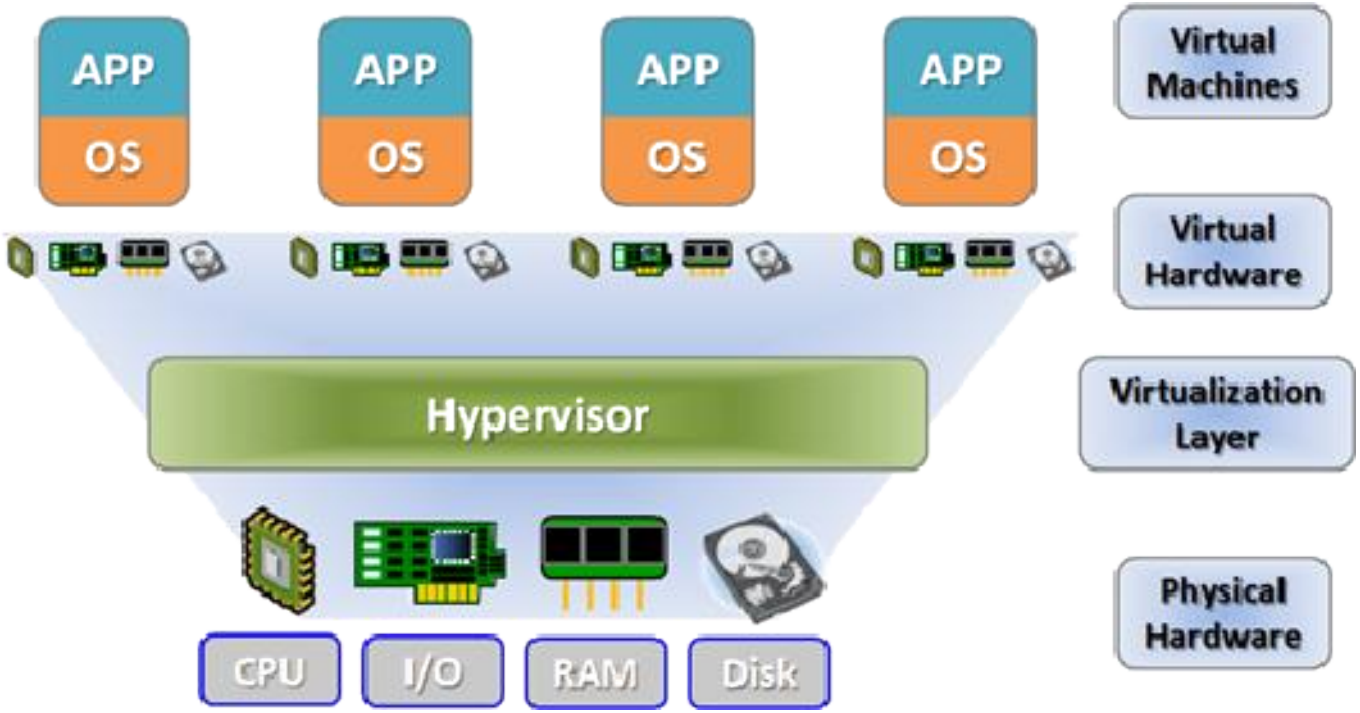
- Abstraction layer between software and hardware
- Hypervisor (or Virtual Machine Monitor) manages interaction of virtual machines and hardware
- The most common application of virtualisation



Server Virtualisation (2)

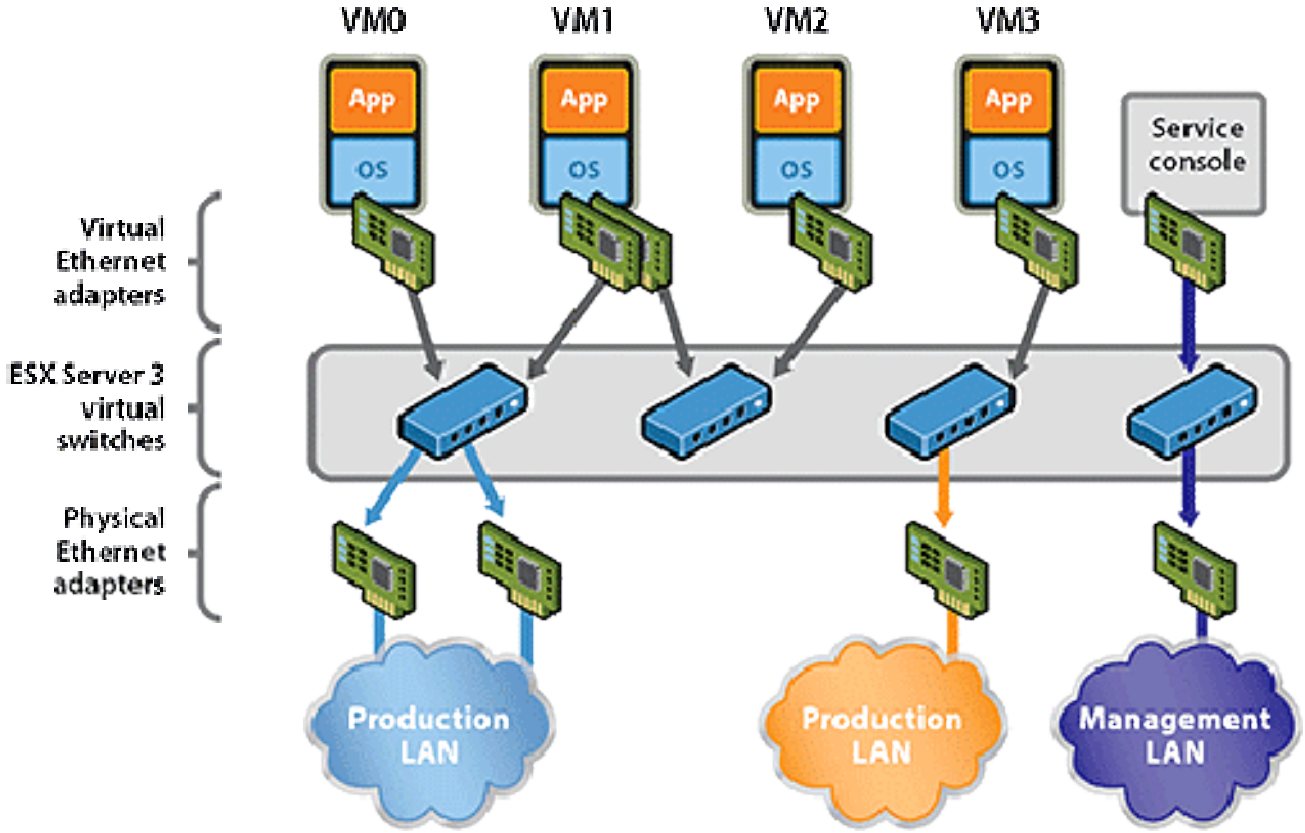
Logical rather than a physical view:

- Group of servers seen as a single pool of resources
- A single machine running multiple operating systems

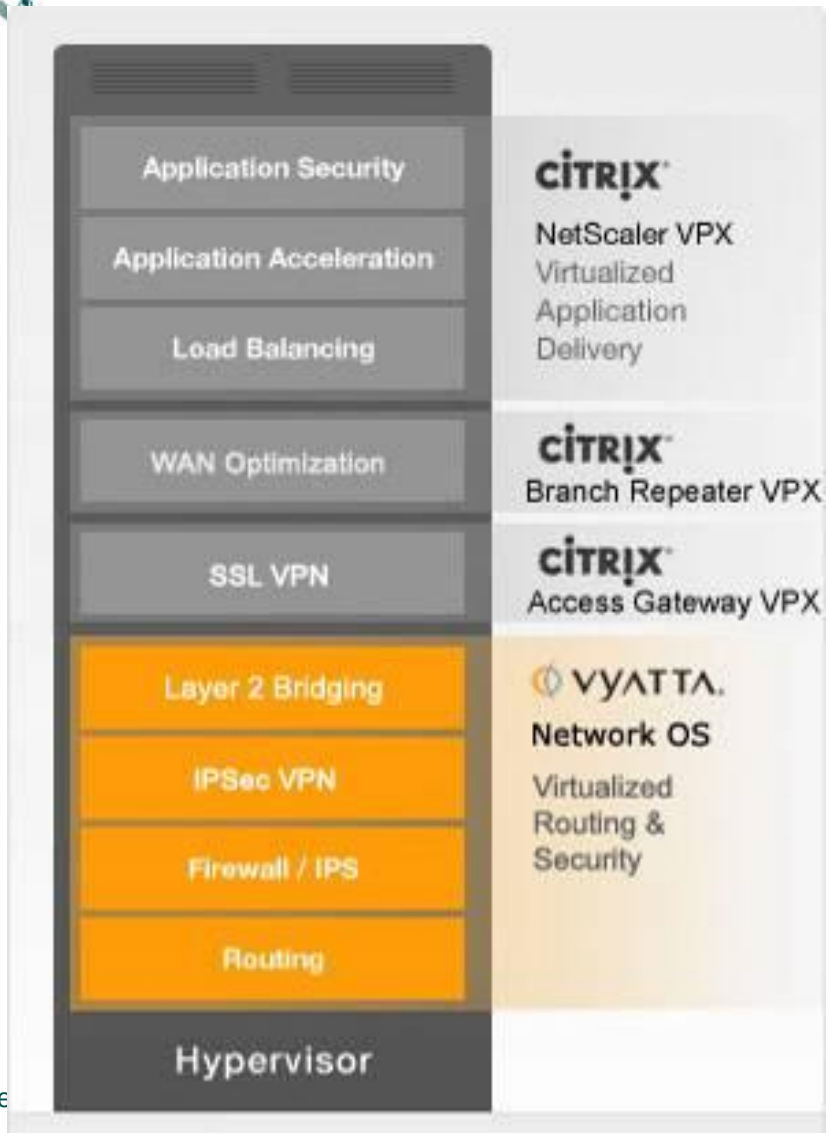


Network Virtualisation (1)

- External network virtualisation
- Networks combined or divided into VLANs to improve efficiency



Network Virtualisation (2)

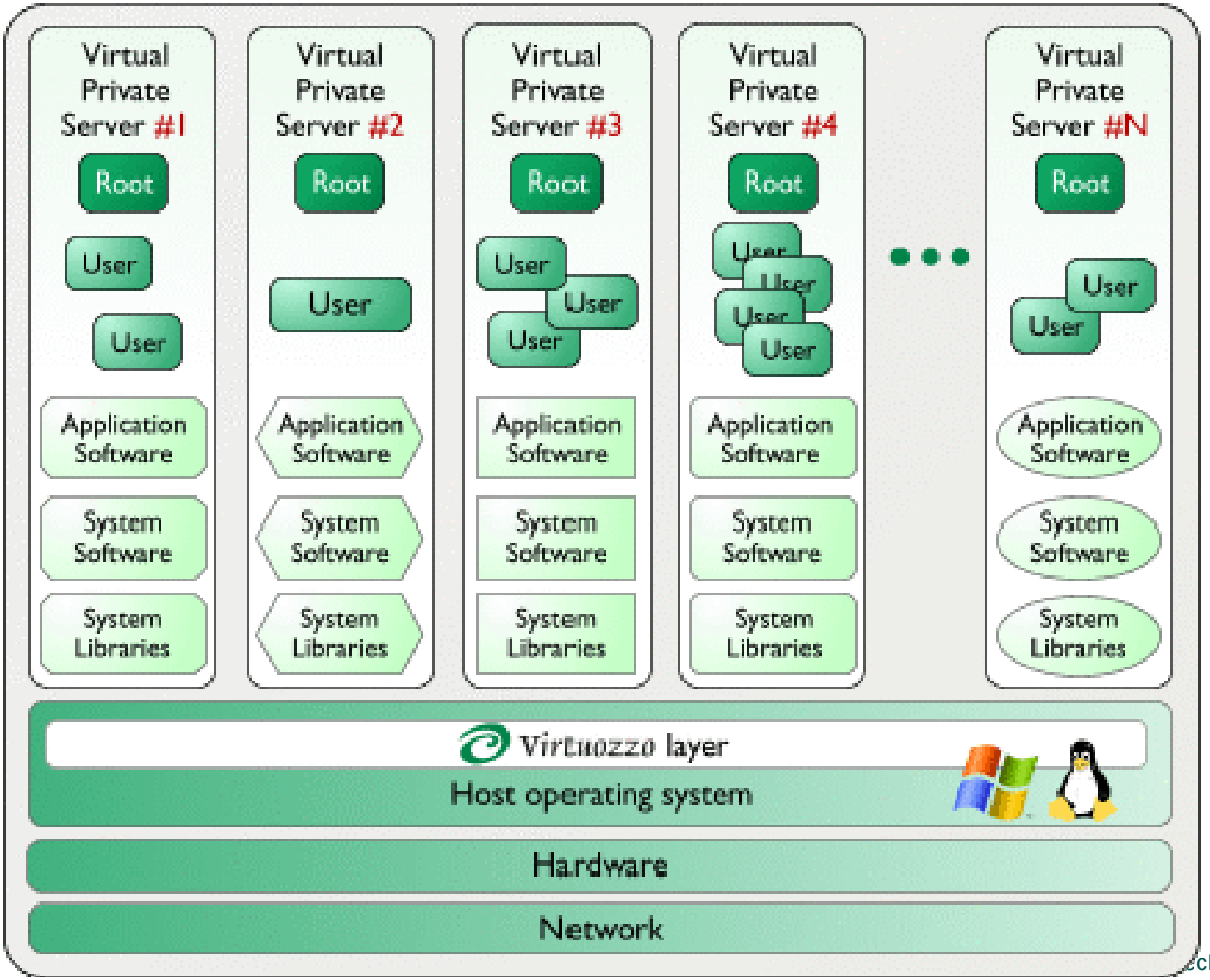


- "Network in a box"
- Migrate security and traffic management policies from physical to virtual infrastructures
- Cost savings from reduction in physical network infrastructure and optimal use of servers
- Securely connect physically separate datacentres and cloud networks
- Simplify migration of applications to the cloud

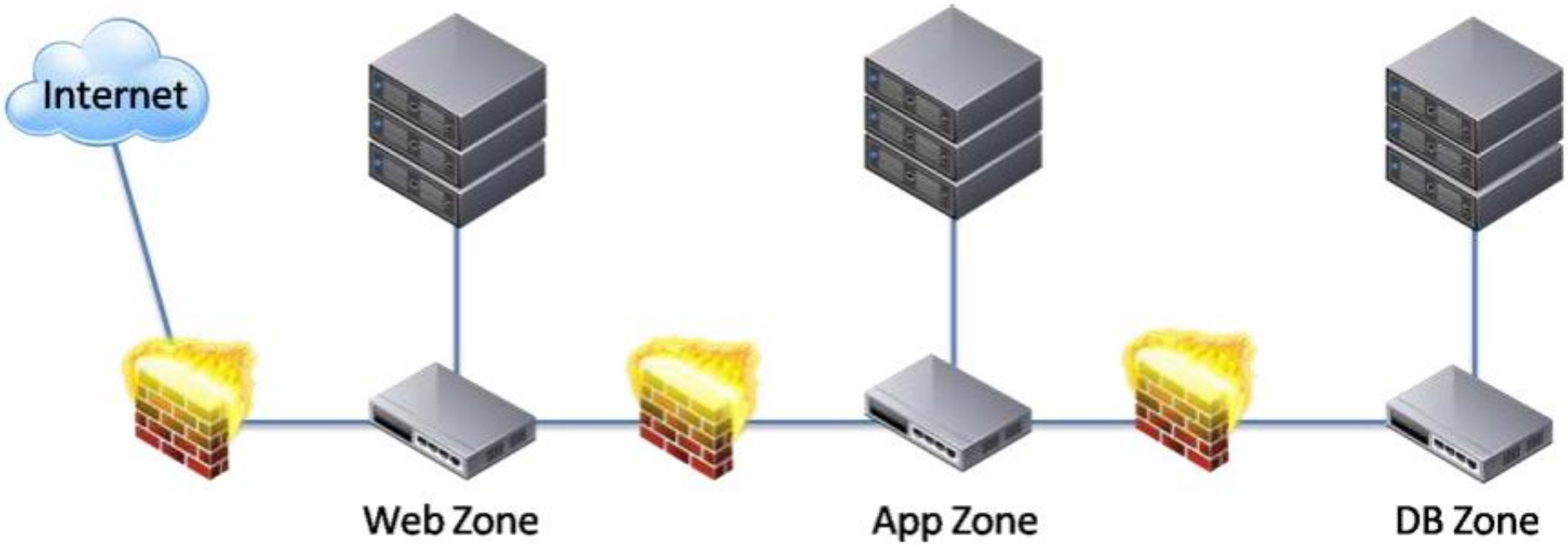
Virtual Private Servers

- Cloud providers can offer “virtual private servers”
- Each VPS:
  - has its own processes, users, files and provides full root access
  - can have its own IP addresses, port numbers, tables, filtering and routing rules
  - can have its own system configuration files and can house an application
  - can have its own versions of system libraries or modify existing ones
- A VPS is not a Virtual Machine – it runs the same OS as the root OS - Linux on Linux, etc.
- Also known as operating system-level virtualization

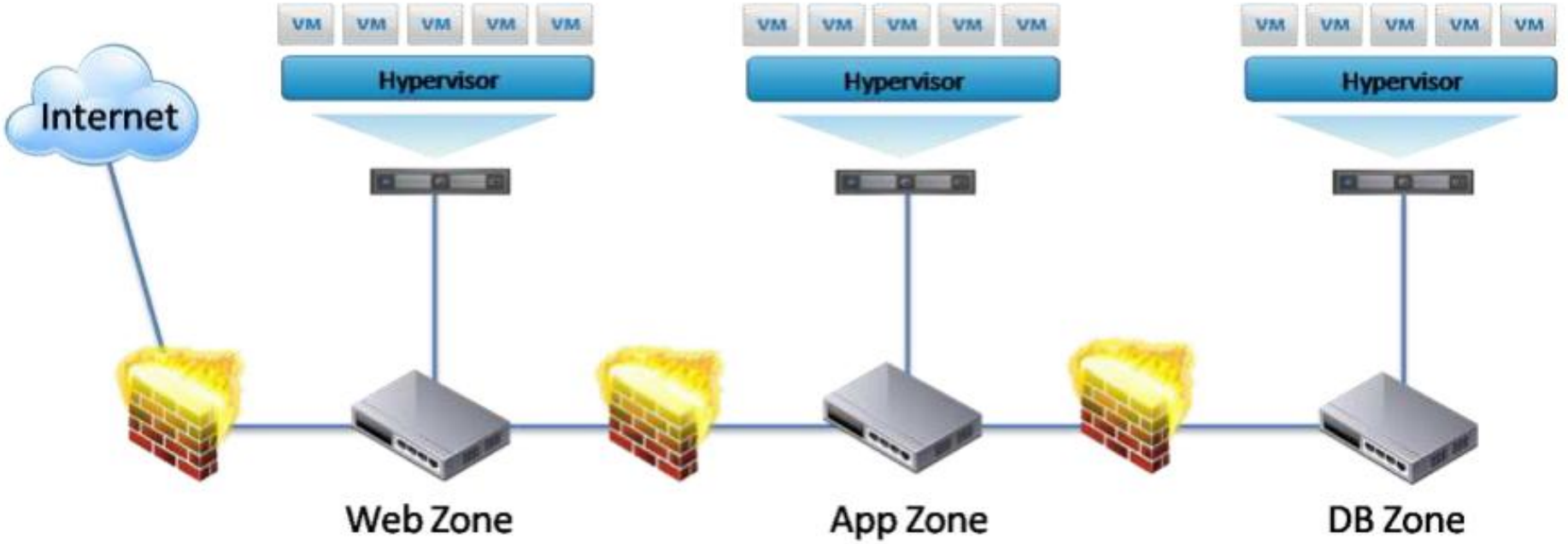
VPS Example


Virtual Private Server #1
Root
User
User
Application Software
System Software
System Libraries
Virtual Private Server #2
Root
User
Application Software
System Software
System Libraries
Virtual Private Server #3
Root
User
User
User
Application Software
System Software
System Libraries
Virtual Private Server #4
Root
User
User
User
User
Application Software
System Software
System Libraries
Virtual Private Server #N
Root
User
User
Application Software
System Software
System Libraries
Virtuozzo layer
Host operating system
Hardware
Network

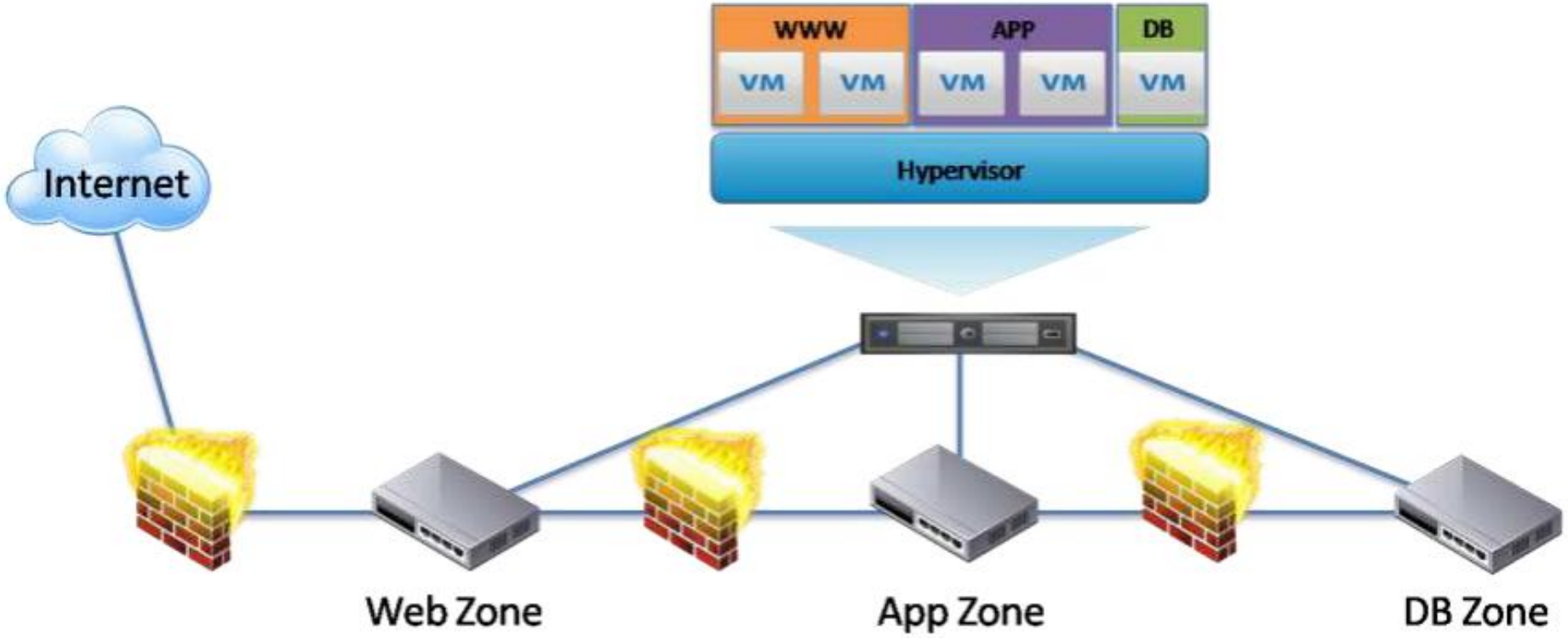
Traditional E-Commerce Architecture



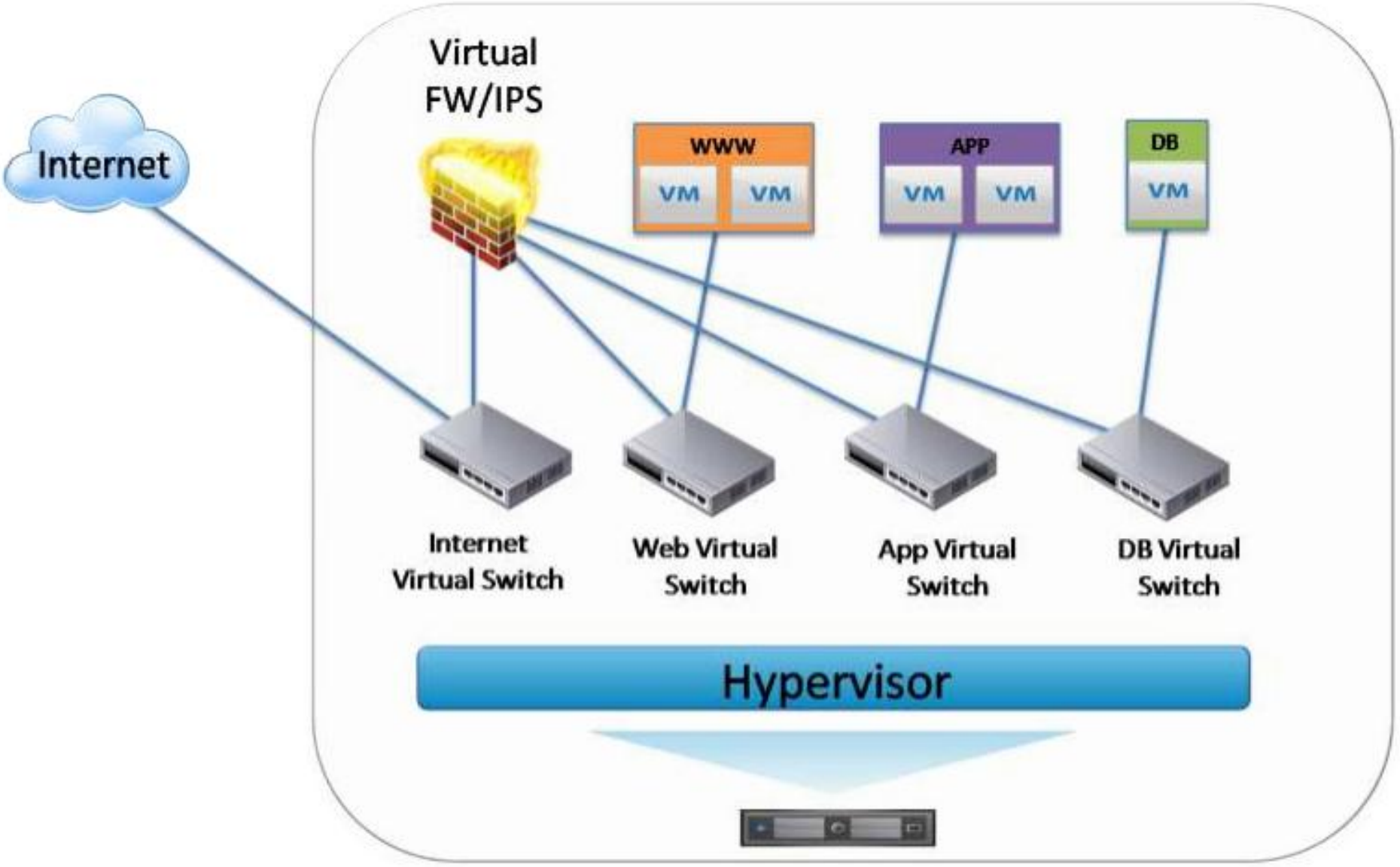
Virtualisation Within Trust Zones



Virtualisation Across Trust Zones



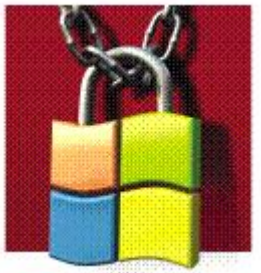
Fully Virtualised



Security Concerns in Virtualised Environments

Hyperjacking

- Injecting a rogue hypervisor between the target system and the hardware
- Proofs of concept: Blue Pill, SubVirt 2 and Vitriol
- Regular security measures are ineffective against these threats because the OS, running above the rogue hypervisor, is unaware that the machine has been compromised
- Hyperjacking is still only a theoretical attack scenario, but it has garnered considerable press attention due to the potential damage it could cause

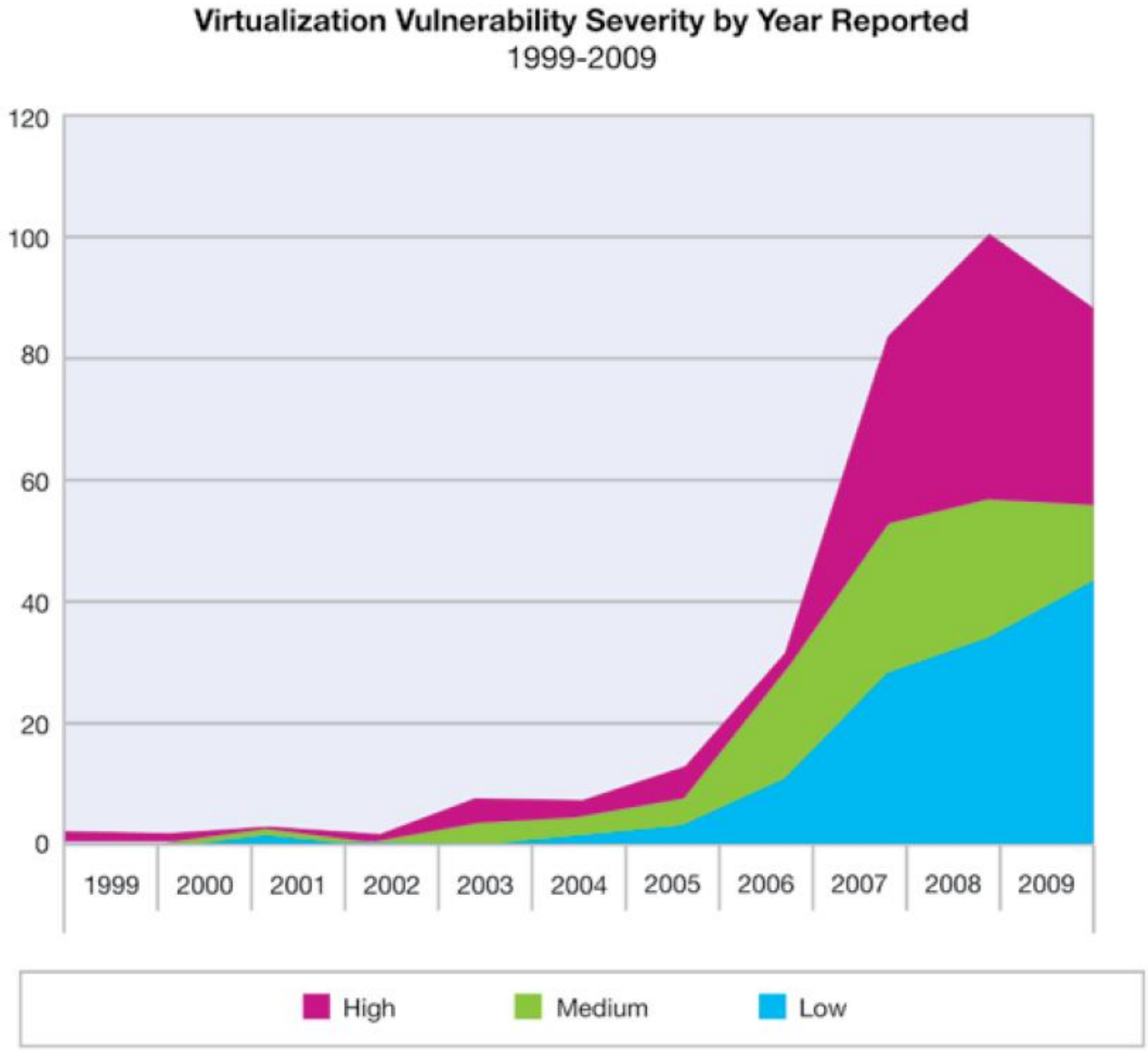


matasano SECURITY

VM jumping (guest hopping)

- Exploits vulnerabilities in hypervisors that allow malware or remote attacks to compromise VM separation protections and gain access to other VMs, hosts or even the hypervisor itself
- These attacks are often accomplished once an attacker has gained access to a low-value, thus less secure, VM on the host, which is then used as a launch point for further attacks on the system
- Some examples have used two or more compromised VMs in collusion to enable a successful attack against secured VMs or the hypervisor itself

Vulnerability Disclosure Trend



IBM X-Force ® 2010 Mid-Year Trend and Risk Report

373 vulnerabilities disclosed 1999 to 2009

A small fraction of all disclosures, having exceeded 1% only in 2007 through 2009.

Virtualisation Vulnerabilities by Type

Type	Description	Workstation	Server
Host	Affect host operating system without the involvement of any executing virtual machines	30.8%	0%
Guest	Affect a guest virtual machine without affecting the hypervisor or host operating system	26.3%	15%
Escape to host	Allow an attacker to “escape” from a guest virtual machine to affect the host operating system	24.1%	0%
Web app	Affect the system on which the client browser is running	9.8%	10%
Virtualisation system	Affect the entire virtualised environment, but do not arise from guest virtual machines	4.5%	37.5%
Escape to hypervisor	Allow an attacker to “escape” from a guest VM to affect other VMs or the hypervisor itself	3.8%	35%
Console	Affect custom management consoles	0.8%	0%
Web server	Affect a web server that implements a web application used by the virtualisation system	0%	2.5%

‘Escape to Hypervisor’

- Many believe there are no escape-to-hypervisor vulnerabilities affecting server-class systems (and therefore it is acceptable to run virtual servers with different security sensitivities on the same physical hardware)
- The IBM X-Force 2010 Mid-Year Report results show that these vulnerabilities do exist for server class systems, calling into question whether virtual servers with different levels of security sensitivity should run on the same physical machine
- This observation emphasises the importance of timely patch management for virtualisation systems

Security Concerns

- VM sprawl
  - Failure to patch
  - Problems with patching
  - Licensing issues
  - PCI compliance

- Segregation of duties
  - Hypervisor vs guest operating systems

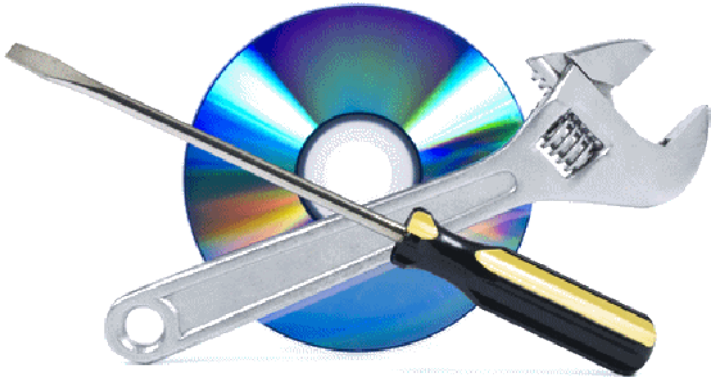
Security Concerns

- Infected VM can infect other VMs in same server
- Virtual networks may not use firewalls
- VM migration can introduce many vulnerabilities

Management issues

Each virtual machine requires *(including suspended and offline)*:

- Vulnerability analysis
- Security updates
- Patch management
- Network interface hardening and segmentation



Management issues

Each hypervisor requires:

- Prevention of single point of failure
- Regular software updates
- Controlled access to VMs
- Security of host OS
- Security policy

Management issues

- Configuration assessment
- Hypervisor configuration checks
- Change authorisation and documentation
- Configuration audit and control
- Approved templates for deployment
- Event monitoring

Controls and Standards in Virtualised Environments

Control Considerations

- Critical servers on a single machine
  - Risk increases if VMs can talk to each other
  - Do not run public-facing servers with LAN servers
- Hypervisor vulnerabilities
  - Patching is the highest priority
  - Protection of management console is critical
- Segregation of duties

Control Considerations

- Patch management & configuration
  - Offline VMs must be kept up to date
  - VM appliance images
  - Protection from tampering

Policies and Standards

- Patch management
- Change management
- Backup
- Audit and monitoring
- Firewalls
- Incident response and forensics
- Intrusion detection / prevention
- Network access control
- BCP
- Antivirus

Policies and Standards

Remember:

- Perimeter security appliances cannot see inter-VM traffic
- Traffic flows in virtualised environments are different
- Associate security policy with VM identities

Securing the VM

Secure the host OS, but also ...

- Secure guest OS as if it were a physical host
- Consider strong authentication
- Use segmentation – group applications of similar value or sensitivity

Securing the VM

- Secure the kernel
- Secure network traffic at all layers
- Protect the console (and thus access to the hypervisor)

Securing the VM

Securing virtualised environments requires:

- Understanding where and how virtualisation is used
- Creation and enforcement of policy and standards
- Selection of controls using defence in depth
- Integration of virtualisation into change and vulnerability management
- Auditing and enforcement

Summary and Conclusions

Summary

- Harden VMs, host OS and hypervisor
- Patch VMs, host OS and hypervisor
- Offline VMs must be kept up to date
- Risk increases if VMs can talk to each other
- Don’t mix VMs of different sensitivity
- Protection of management console is critical
- Protection from tampering
- Segregation of duties
- Informed, educated audit!

PCI DSS Virtualisation Guidelines

- If a VM is in scope so is the hypervisor (2.2.1)
- An entire VM is in scope if it stores, processes or transmits cardholder data (2.2.2)
- Virtual appliances are in scope (2.2.3)
- Virtual switches and routers are in scope (2.2.4)
- Virtual applications & desktops are in scope (2.2.5)

https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Conclusions

It's happening now:

almost 50 percent of servers will be virtualised by 2012 (Gartner)

We have to study:

security depends on knowledge of virtualisation technology for both installation and audit

References (1)

Chan, Jason; 'Virtualization: IT Audit and Security Perspectives' ISACA-SV Spring 2010 Conference
(jchan-isaca-sv-spring2010.pdf)

Chaudhuri, Abhik; von Solms, SH (Basie); Chaudhuri, Dipanwita; 'Auditing Security Risks in Virtual IT Systems', ISACA Journal volume 1, 2011
(jpdf11v1-auditing-security-risks.pdf)

Dai Zovi, Dino A.; 'Hardware Virtualization Rootkits', Black Hat USA 2006
(HVM_Rootkits_ddz_bh-usa-06.pdf)

Kirch, Joel; 'Virtual Machine Security Guidelines Version 1.0', September 2007, http://www.cisecurity.org/
(CIS_VM_Benchmark_v1.0.pdf)

Schreck, Galen; 'Server Virtualization Security: 90% Process, 10% Technology', Forrester Research, 30 July 2008

References (2)

Schultz, Eugene; 'Virtualization, Cloud Computing and Security', ISSA-Puget Sound, Bellevue, Washington, April 15, 2010

Williams, Brian; Cross, Tom; 'Virtualisation System Security', 2010, IBM *(VirtualizationSecurity.pdf)*

'IBM X-Force 2010 Mid-Year Trend and Risk Report' *(2010_XForce_Midyear_Report.pdf)*

'ISACA Virtualization Security Checklist' *(Virtualization-Security-Checklist-26Oct2010-Research.pdf)*

'Virtualization: Benefits and Challenges', 2010, ISACA *(Virtulization-WP-27Oct2010-Research.pdf)*

Need more information?

Peter Wood

Chief Executive Officer

First • Base Technologies LLP

peterw@firstbase.co.uk

http://firstbase.co.uk
http://white-hats.co.uk
http://peterwood.com

Blog: fpws.blogspot.com
Twitter: peterwoodx