The Four Horsemen Of the Virtualization Security Apocalypse

...the “My Little Pwnie Edition”
Welcome To The Jungle...

- Setup
- Virtualization In Context
- Virtual Networking Architecture
- VirtSec Solutions Landscape
- The Four Horsemen
- Wrap-Up
Topics and Goals Of Our Chat:

- Discuss the operational realities of virtualizing networking and security today: performance, scalability and resiliency
- Describe the broad impact of immaturity in VirtSec technology/solutions
- Illustrate how the melange of security in the ISV Software, hypervisor, OS, network and embedded in hardware opens a security wormhole
Some security things you do today are perfectly reasonable and work well in virtualized environments, others simply don’t work at all.
Reality Bites

“It ain’t all rainbows and unicorns...”
Replicating many highly-available security applications and network topologies in virtual switches doesn’t work.
Bumpy Road Ahead

“Everything’s Under Construction...”
Monolithic security vendor virtual appliances are the virtualization version of the UTM argument.
If It Ain’t Fixed, Don’t Break It

“She just don’t run like she used to...”

Virtualized Security can seriously impact performance, resiliency and scalability.
Virtualized Security can seriously impact performance, resiliency and scalability
Penny Wise & Pound Foolish

“Money for nuthin’ and my chips for free…”
Virtualizing security will not save you money, it will cost you more
Where To Start?

- Setup
- Virtualization In Context
- Virtual Networking Architecture
- VirtSec Solutions Landscape
- The Four Horsemen
- Wrap-Up
Caveats

- This presentation focuses on VMware VI3 as the virtualization platform example; Microsoft’s and Citrix’s networking/security architectures are different.
- There are a number of interesting new capabilities in VI4; I make reference to some of them, but many are futures and not shipping but change things dramatically...
- In the interest of scope and time, it’s focused on server virtualization and data networking only; storage, client, application virtualization are a whole other universe of security fun...
- It’s true you can achieve very robust/resilient integrated network and virtual infrastructure designs, but the moment you try and integrate security...not so much...
x86 Virtualization* Overview

From This

- Application
- Application
- Application

- Operating System

- x86 Architecture

To This

- Application
- Application
- Application

- Operating System

- Virtualization Layer

- Application
- Application
- Application

- Operating System

- x86 Architecture

*Represents “Type 1” or Bare Metal “Server” Virtualization
x86 Hierarchical Protection Domains/Rings

Most Privileged

Least Privileged

Adapted from: http://en.wikipedia.org/wiki/Supervisor_mode
The Four Horsemen Of the Virtualization Security Apocalypse | Hoff | SeeTor 2008

Virtualized: Software Only

Physical/Non-Virtualized

Virtualized: Hardware Assisted

- The Guest OS is de-privileged into Ring 1 and the VMM takes its place in Ring 0
- The Guest OS still thinks it is running in Ring 0 with all the privileges thereof
- Can cause issues/conflicts due to contention for the 17 x86 privileged platform control instructions

In this example, Intel VT provides the VMM with an exclusive privileged level where it resides and executes (Ring -1)

- The Guest OS is not de-privileged and is running in Ring 0
- Context switching between VMM and Guest OS's are hardware supported

*There is also para-virtualization, not covered here...*
Hypervisors Are a Disruptive Commodity...

*Yes, there are others, but these have pretty logos...*

They’re breedin’ like wabbits!
...and they're showing up everywhere
Which means:

- Companies will likely end up with many virtualization platforms/VMM's spread out across the horizon of their enterprise.

The key differentiators?

- Management, integration, extensibility and security.

We need open standards for solution interoperability, management & security.

- If you have issues with the “simple complexity” of a single virtualization platform, imagine when you have many.
Many debates and much ado stems from the inability to distinguish between three fundamental concerns:

- Securing Virtualization
- Virtualizing Security
- Security Via Virtualization

Separate the technical, architectural, and philosophical from the functional, operational and organizational.
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
Threat Models In Review

1. Guest to Guest
2. Guest to Host/VMM/HW
3. Guest to Self
4. External to Host/VMM/HW
5. External to Guest
6. Host/VMM to All...
7. Hardware to VMM
But d00d, What About Virtualization Malware!??
There are many really interesting topics to discuss here:

- Hypervisor malware, rootkits & hyperjacking
- Exploiting virtualization-enabled chipsets for fun and profit
- Peripheral Hardware/Firmware abuse
- Control channel manipulation

I’m neither qualified or motivated to talk about these topics and we’ve got much more profound and fundamental sets of issues to discuss.

There are lots of other talks featuring this stuff...
Time For Sublime Design

Setup
Virtualization In Context
Virtual Networking Architecture
VirtSec Solutions Landscape
The Four Horsemen
Wrap-Up
A Basic Virtual Switch Defined

A Virtual Switch:

- Is a software-based networking construct that runs in the virtualization platform’s kernel
- Purposely-designed layer-2 (L2) switch which is loaded dynamically at runtime with functional modules such as:
  - Core L2 forwarding engine
  - VLAN tagging, stripping & filtering
  - L2 security, checksum and segmentation offload
- Some features normally found in physical L2 switches are not present by design to provide for integrity, isolation and secure connectivity (no STP, VTP, ISL, etc...)
VMware’s Virtual Switch Visualized

Abstracted Model

- Apps
- OS
- vNIC

Port Group: Production Network

vSwitch0

- vmNIC0 (Uplink)

VMware Virtual Infrastructure Client View

- vNIC

* I purposely left off the VMotion and Service Console networks in the model for clarity
vSwitch Correctness

The Four Horsemen Of the Virtualization Security Apocalypse | Hoff | SecTor 2008

Packet Filter
vSwitch Security Options

vSwitches offer some nifty security features:

- Configure promiscuous mode (per portgroup) for selective mirroring
- MAC Address changes prevents VM’s from changing/spoofing their MAC addresses
- Can restrict “forged transmissions” that would potentially allow VM’s to send traffic from nodes other than themselves
• Network Security in a VMware environment is reduced down to 3 checkboxes in VirtualCenter

• “Network Security” within the virtualized construct of a host is now administered by folks whose competency is neither networking or security

• This is the visibility we security folks have into these environments...
You’re Making Me All Weepy!

Setup & Context
Virtualization In Context
Virtual Networking Architecture
VirtSec Solutions Landscape
The Four Horsemen
Wrap-Up
• Evolving solutions from existing players as well as emerging startups & the virtualization platform providers

• You will need to invest differently in order to effectively manage risk in a virtualized environment

• The next 12 - 18 months will be difficult due to the gold rush effect

• There is (still) no silver bullet, just a lot of silver buckshot
Where We Are Today

December 31, 2008
VirtSec Examples: No Controls (FUD)

No Security

VLAN 2  VLAN 2  VLAN 2  VLAN 2

Virtual Server 1

Virtual Server 2

Physical Switch

Virtual Server 3

Virtual Server 4

Assumptions/Caveats:
* VM’s connected to the same vSwitch, portgroup, VLAN
* No attempt at containment
* No segmentation/protection
* Not very realistic...

Firewall/IDP Appliance
Myth/Security Team Says:

✦ “Consolidating servers onto the same virtualized host is insecure because you can’t secure intra-vm traffic!”

Reality/I ask:

✦ “When you have two physical servers plugged into the same physical switch in the same VLAN, how do you secure intra-machine traffic?”

Response/Security Team Blushes:

✦ “Uh, we don’t...”
The Reality: Same Ol' Software In the VM

Most anything you run today in your conventional environments will work here...

- Firewalls
- HIDS
- HIPS
- Anti-virus
- NAC
- Endpoint Assurance
- Patch Management
- Inventory
- Configuration Audit & Control

Installed at the OS or Application Layers
VirtSec Examples: Interacting with External Security

Assumptions/Caveats:
- Still utilizes host-based security software
- VM’s connected on same/different vSwitches but different VLAN’s
- Traffic redirected/routed through external switch fabric and security infrastructure
The trick is forcing the traffic through the virtual appliances (if prevention is required) versus merely monitoring via SPAN for detection/monitoring.

- Requires careful (and potentially extensive) virtual networking configuration.
- Don’t protect against intra-VM compromise in the same VLAN.
- Does not directly protect the Hypervisor.
- Many of these tools are more about visibility & visualization than they are pure security.
- Virtual Appliances are VM’s! They are software & exploitable!
VirtSec Examples: Virtual Appliance with VM to VM On Different vSwitch/VLAN

Virtual Appliances

Assumptions/Caveats:
- Traffic redirected/routed through VA which does NAT/VLAN isolation
- Thus, to go from VLAN 4 to VLAN 2, you have to go through VLAN3 (VA)
- Requires significant virtual/physical networking reconfiguration
VirtSec Examples: Virtual Appliance with VM to VM On Same vSwitch/VLAN

Virtual Appliances

VLAN 4  VLAN 3  VLAN 2

Virtual Server 1  Virtual Server 2  Virtual Server 3  Virtual Server 4

Physical Switch

Firewall/IDP Appliance
Here we have a basic multi-VM configuration without a virtual security appliance:

- Two VM’s, sharing a single vSwitch
- Each VM sits on its own VLAN/Portgroup
- For traffic to make it’s way from VLAN A to VLAN B, the traffic must traverse the Uplinks to the external switching/routing fabric
- VLANs A and B are advertised to the rest of the network via VLAN/Subnet C
Virtual Appliances: The Devil’s In the Details

The Revised Configuration:

- VLANs A and B are now isolated on vSwitch0 with no uplinks.
- VM1 and VM2 bridged/routed by VM3 (Virtual Appliance).
- VM3 also connected to vSwitch1.
- For traffic to make its way from VLAN A to VLAN B, the traffic must traverse VM3 (the virtual appliance).
- VLANs A and B are no longer advertised to the rest of the network.
- VLAN D transports and thus the VA controls all intra-VM traffic and processes all externally-bound traffic.
What's Coming...

The Future

NEXT EXIT
VirtSec Examples: VMM/ISV API’s

**VMware VMsafe**
Enables ISV partners to build security solutions in the form of a virtual appliance utilizing API’s that interact with hypervisor extensions to provide for monitoring and protection of memory/CPU, networking, process execution and storage.

**XenAccess**
XenAccess is a library that simplifies the process of memory introspection for virtual machines running on the Xen hypervisor.
VMSafe API’s: Network Introspection

Assumptions/Caveats:

- Does not require virtual networking reconfiguration
- Requires API-Capable VMM & ISV Apps.
- Utilizes VMM Kernel Plug-Ins & Filters
- Exposes Hypervisors to potential exploit
Simplified VMSafe - Net API Example

1. Traffic enters via physical NIC destined for Protected VM2 and intercepted by API-enabled VMM.

2. vNetwork/VMsafe API configured via Filters to send traffic destined for PVM2 to Security VM/VA.

3. API passes traffic to Security VM/VA VMM Fast-Path Plug-in Driver.

4. Traffic now passed between fast-path & slow path drivers in VA/VM.

5. Processing/Disposition effected by security VA/VM and passed back from slow-path to fast-path drivers.

6. Traffic passed back via API/Drivers.

7. Traffic sent on its way via the virtual switching infrastructure to PVM2.
VMware vNetwork API’s (Networking)

DVS Extends the virtual switch concept from the individual host to the cluster/datacenter level.

...this provides for networking configurations that allow for simplified management, VM-configuration/mobility awareness & policy affinity, the preservation of VM state, and...
Third Party vSwitches

- Acts as a policy-driven intelligent disposition director to 3rd party security functions
- Allows integration/replication of external software, fabric capabilities and policy
- Consistency in networking capabilities
- Additional networking functionality (load-balancing, QoS, L3-7, etc...)
- Starting to appear in some very interesting places
- ...and will introduce some very interesting security and management challenges

Virtual Appliance (Pre-Bundled/Tuned OS & Apps) with vNetwork API & 3rd Party vSwitch
Example: The Cisco Nexus 1000V

Cisco Nexus 1000V Architecture

Cisco Nexus 1000V Enables:
- Policy-based VM connectivity
- Mobility of network and security properties
- Non-disruptive operational model

Virtualizing the Network Domain

Policy Based VM Connectivity | Mobility of Network and Security Properties | Non-Disruptive Operational Model
A Fly In the (Virtual) Ointment

Will Work For DMA (Or Food)

I/O Virtualization
IOV is great for solving performance/scalability issues, but how will it affect security?

- It’s already becoming difficult to grasp where “the network” is, who owns it, how we manage it and how to secure it.
- A mélange of components providing the networking functions will add complexity, expand the attack surface and potentially limit visibility further.
- What will technologies/approaches such as direct assignment bypassing the VMM and SR-IOV in NICs mean to security virtual appliances running on the hosts?
- Crossing the streams is “bad.” Allowing some networking via vSwitches, some in the CPU, some in software and some in the NIC sounds awfully messy.
- What happens when the hardware is not homogenous? It’s great to see partnerships that deliver things like VMDirectPath, but what about Citrix, Hyper-V, etc...?
w00t! World Domination!

- Single network connection provides virtualized fabric interconnectivity for LAN & SAN
- Ultimately your VM’s run in the switch
- All your VM’s (and security) are belong to us!
Where Isn’t the Network?

"Networking" Element Stack

- Routing/Bridging/Switching/NAT in "closed" Virtual Appliances
- Hypervisor-based Distributed Virtual Networking (vSwitches)
- Network Security API’s
- Embedded Networking/Virtualization-Enabled CPU/Chipsets
- Physical NIC Cards
- Embedded Switches
- Data Fabrics
- Physical "Network" Switches
- Storage Fabrics
- Network Switching API’s
- IOV

Examples

- Customized networking stacks/slowpath driver/network stacks in virtual appliances and IPv4/6 network stacks with iptables/brctl (e.g. Linux)
- vNetwork VMsafe & Switching API’s across distributed virtual switches using fastpath kernel modules integrated with VMware vSwitch and Cisco Nexus 1000V
- Intel CPU’s with VT-d and SR-IOV
- Converged Network/Storage Adapters and/or NICs with embedded switching and offload
- Physical Cisco Catalyst/Nexus Switches for both networking and storage

The Four Horsemen Of the Virtualization Security Apocalypse | Hoff | SecTor 2008

Packet Filter
...and the hits keep comin’

- Virtualization is simply the platform enabler
- Real Time Infrastructure (RTI) with self-governing adaptation, provisioning and autonomies is here
- MSSP/IaaS/SaaS/Clean Pipes/Cloud/Grid/Utility/Distributed computing is maturing
- How are we going to secure the abstraction of a cloud-based, dispatched virtualized set of processes, memory space, storage and I/O?
Virtualization is to infrastructure as SOA is to application architecture...

...and we all know how simple securing SOA is, right?
The End Is Nigh! Run Away!

- Setup
- Virtualization In Context
- Virtual Networking Architecture
- VirtSec Solutions Landscape
- The Four Horsemen
- Wrap-Up
The Four Horsemen of the Apocalypse represent the "...forces of man’s destruction described in the Bible in the Book of Revelations" and are "...named after the powers they represent"*

- War
- Pestilence
- Death
- Famine

*Wikipedia
1. Monolithic security vendor virtual appliances are the virtualization version of the UTM argument

2. Virtualized Security can seriously impact performance, resiliency and scalability

3. Replicating many highly-available security applications and network topologies in virtual switches don’t work

4. Virtualizing security will not save you money, it will cost you more
Typical Screened-Subnet DMZ:

- Trust zones separated by physical controls on separate switches & host groups/clusters.

*Images/Concept from VMware Whitepaper: DMZ Virtualization with VMware Infrastructure

---

Example: Virtualizing the DMZ*

*Images/Concept from VMware Whitepaper: DMZ Virtualization with VMware Infrastructure
Example: Virtualizing the DMZ*

Partially Virtualized Screened-Subnet DMZ:

- Trust zones separated by both physical controls but VM’s on multiple ESX clusters

*Images/Concept from VMware Whitepaper: DMZ Virtualization with VMware Infrastructure
Example: Virtualizing the DMZ*

**Completely Virtualized Screened-Subnet DMZ:**

* **Trust zones separated by virtual controls on a single ESX Cluster**

---

*Images/Concept from VMware Whitepaper: DMZ Virtualization with VMware Infrastructure*
Pwnie #1: War

Image: Mari Kasurinen | spippodeviantart.com
Monolithic security vendor virtual appliances are the virtualization version of the UTM argument:

- The notion that we will deploy a single vendor/monolithic security VA in each host is silly
- If you’re still stuck on “defense in breadth,” you’re going to deploy more than one security virtual appliances on each host
- UTM performance sucks when you flip all the switches
How do you ensure that traffic is statefully directed to the appropriate individual in-line security bumps in the stack?

The more security VAs you add, the less VM’s you can service
Pwnie #2: Pestilience

Image: Mari Kasurinen | spippodeviantart.com
Virtualized Security can seriously impact performance, resiliency and scalability

- Performance overhead of in-line security VA/VMs & API’s is extremely difficult to predict.
- Today we rely on multiple load-balanced high-performance multi-core COTS H/W or dedicated ASIC/FPGA equipped appliances for acceptable throughput/low latency...
- We’re now going to expect that software based VA’s which are not optimized or do not utilize paravirtualized drivers to perform the same?
- Security functions are competing for the same resources as the VM’s you’re trying to protect.
VMware showed tests* with linux-based VM-VM throughput on the same vSwitch of ~2.5Gb/s

Most dedicated hardware appliances have trouble at those rates at small packets/low latency

What happens when you try to choke every flow through a non-optimized, software-only virtual appliance in/out of every VM?

What happens when we add multiple 1Gb/s or 10Gb/s bonded pipes feeding our servers?

Figure 9. Linux Virtual Machine to Virtual Machine TCP Throughput

Thus, the virtual machine to virtual machine TCP throughput on ESX Server 3.5 can exceed 2.5 Gbps for some operating systems while speeds of physical networks with 1 Gbps NICs are limited to approximately 950 Mbps.
Every time you deploy a security virtual appliance... God kills a kitten.
Pwnie #3: Death

Image: Mari Kasurinen | spippodeviantart.com
Replicating many highly-available security applications and network topologies in virtual switches don’t work

- Security applications are incredibly topology sensitive
- Affinity between the physical, logical and policy elements breaks when things move
- It’s not that you can’t get network-based HA to work, it’s the support of the applications and their secret sauce that breaks.
- Most physical appliances use heavily tweaked kernels and drivers which aren’t supported natively in virtualization stacks; performance suffers and HA may no longer work
- Failover and HA/LB options for stateful security applications currently suck
The magic pixie dust is needed when you really get into the nitty-gritty of the collapsed access layer.
What happens when these security virtual appliances fail?

- Application-level and VMware HA clustering do not take into consideration the network topology sensitivities of security applications.
- Security applications and the networking stacks are not stateful and do not exchange telemetry.
- Moving the security VA to another box leaves the VM’s unprotected or disconnected/isolated on the original.
- Failing over an entire cluster-member’s inventory of VM’s due to the failure of a security component is ludicrous.

*The upcoming distributed virtual switching (vNetworking) and Cisco Nexus 1000v will change things.*
I would really have liked to show you a cool demo with the help of my friends from ERNW (Germany) using their modified L2 Sulley fuzzing framework, abusing the HA protocols of a few security software vendors to show you how fragile these security virtual appliances are in terms of performance/resiliency.

We set up our test bed to compare the physical appliance versions with the virtual but quickly stopped when we realized:

- Most vendors still don’t offer production-ready security virtual appliances for lots of interesting reasons...
- Most of them do not offer active/active, load-balanced HA in their products
- When they do, they are loaded with untenable caveats that make the products impractical

...and yet we’re being told that virtual appliances are the centerpiece of the security portfolios in these environments?
The Four Horsemen Of the Virtualization Security Apocalypse | Hoff | SectoR 2008

Image: Reality Distortion Field

Diagram:
- VMware ESX
- vmkernel
- NIC Teams
- Internet VS
- Intranet VS
- Web VS
- App VS
- Database VS
- Web Servers
- App Servers
- Database Servers
- Firewall IDS/IPS Virtual Appliance(s)
- Service Console

Figure 5 — Fully collapsed DMZ

*Images/Concept from VMware Whitepaper: DMZ Virtualization with VMware Infrastructure
Virtualizing security will not save you money, it will cost you more

- For most of this to work, we need to buy new hardware with virtualization-aware chipsets, more memory, faster/more CPU's, new vSwitches, extended management...
- We won't get rid of host-based security software
- We won't get rid of physical appliances or security line cards in switches, in fact, we'll probably have to buy more and buy bigger/more powerful switches with converged I/O
- That means that when we add VirtSec solutions, these solutions & their licenses are cost-additive
- As we add more solutions, we add complexity
Parting Is Such Sweet Sorrow

Setup
Virtualization In Context
Virtual Networking Architecture
VirtSec Solutions Landscape
The Four Horsemen
Wrap-Up
1. Monolithic security vendor virtual appliances are the virtualization version of the UTM argument
2. Virtualized Security can seriously impact performance, resiliency and scalability
3. Replicating many highly-available security applications and network topologies in virtual switches don’t work
4. Virtualizing security will not save you money, it will cost you more
Hope Is Not a Strategy, But It Doesn't Hurt

- We need a unified approach toward virtualization with a consolidated trust model in hardware & software.
- We need affinity between the VM and protection schemes/policies.
- Comprehensive discovery, profiling, dynamic configuration & security management of all VM's -- online or offline.
- Centralized VM registration providing telemetry that controls spin-up, state and mobility capabilities regardless of vendor based upon policies.
- Intelligent networking capabilities within the virtual switching infrastructure for consistency, visibility and security including integrated virtual network admission control & access Control (vNAC).
- Correlation of telemetry between VM Management and internal/external security planes to tie in virtualization, network and security provisioning/management into a consolidated single pane of glass.
What Does This All Mean?

- Networking & Security are supposed to be getting easier, simpler and cheaper with virtualization...
- Security is going to get harder and our solution portfolios are immature at best
- We’re in the midst of the cyclic flip-flop between the virtualization-powered abstraction of resources as a software-enabled layer and the realities that hardware isn’t going away and is flexing its muscle
- We can’t afford virtualization to continue to be siloed; the compute, security, networking, and storage fiefdom approach is dangerous
Thank You Cleveland!

Christofer Hoff
Chief Security Architect - Unisys
Christofer.Hoff@Unisys.com (work)
choff@packetfilter.com (not work)
+1.978.631.0302
Blog:
http://rationalsecurity.typepad.com