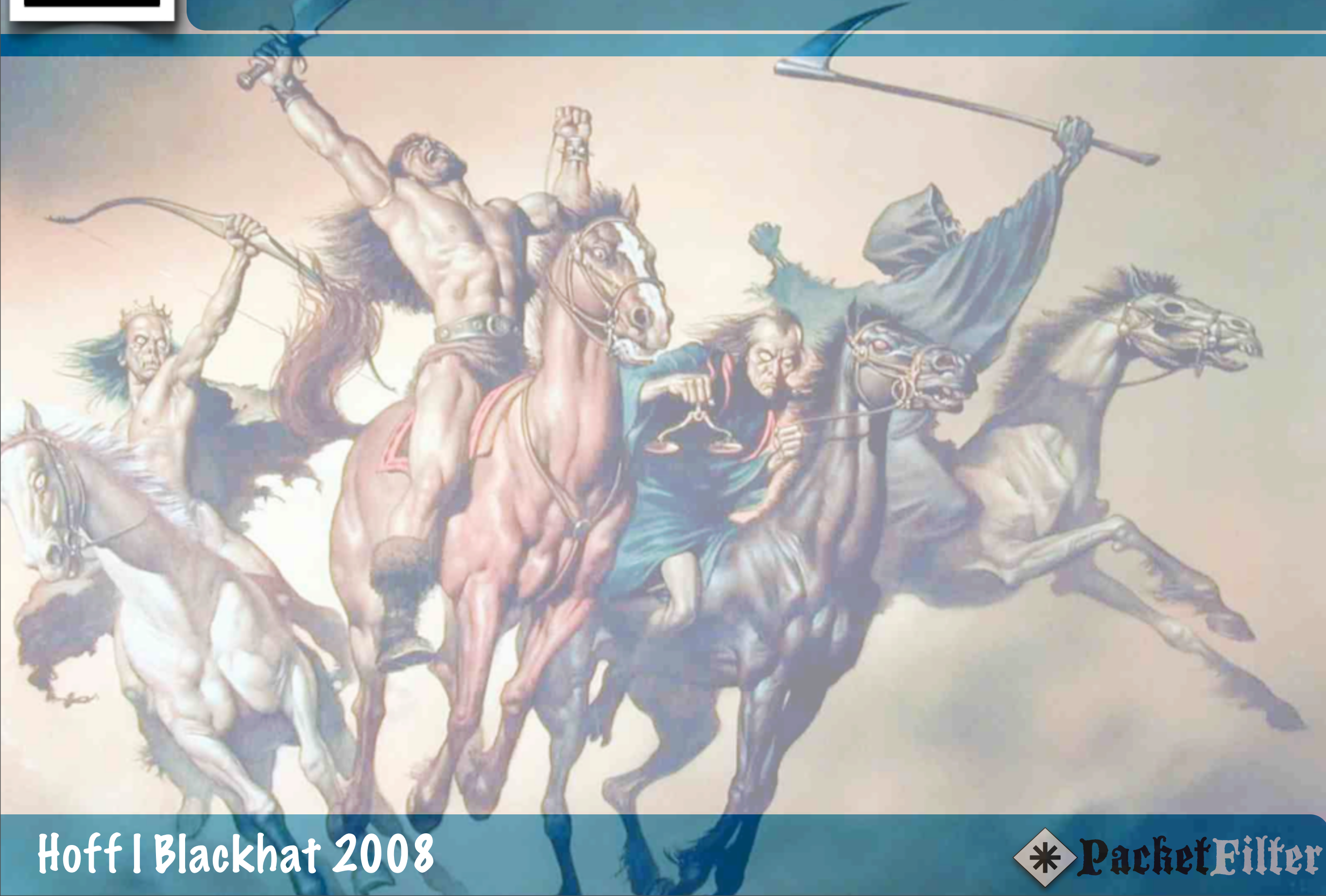




The Four Horsemen Of the Virtualization Apocalypse



Hoff | Blackhat 2008

✱ PacketFilter



A Few Words From the Jackass Who Created This...

Hi there.

This presentation is the full content of the presentation I delivered at Blackhat 2008 in Vegas. It's an update to what was delivered on the CD.

My slides are designed to accompany me, not the other way around. My narrative is pretty important in many sections.

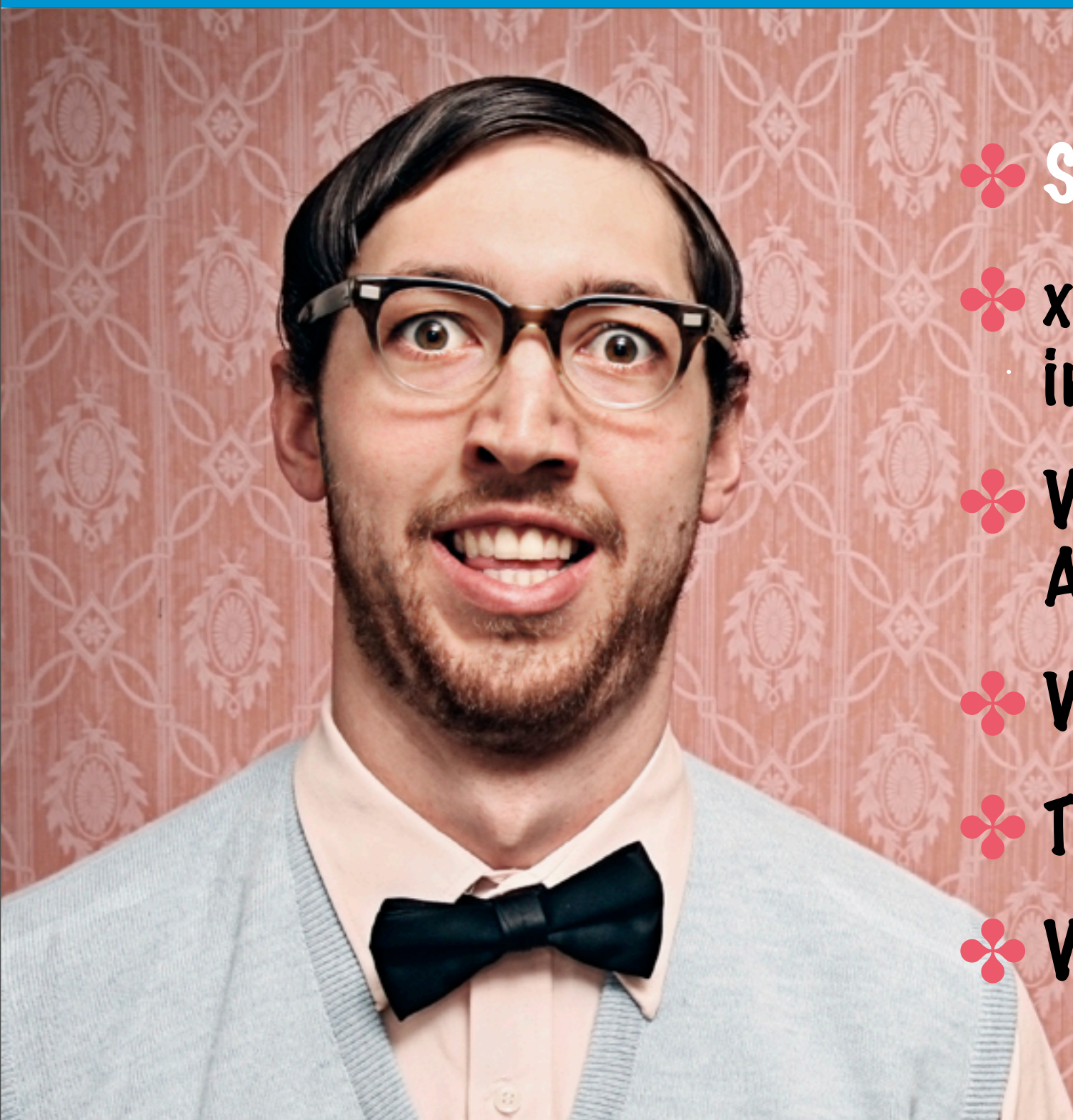
Thus, if you have a question or a comment about something, email me [lchoff@packetfilter.com], call me [978.631.0302], or post a comment on my blog [rationalsecurity.typepad.com]

I hope you find this useful. If you're going to use anything from my presentations, I'd like to know about it. Who knows, I might have new content for you...





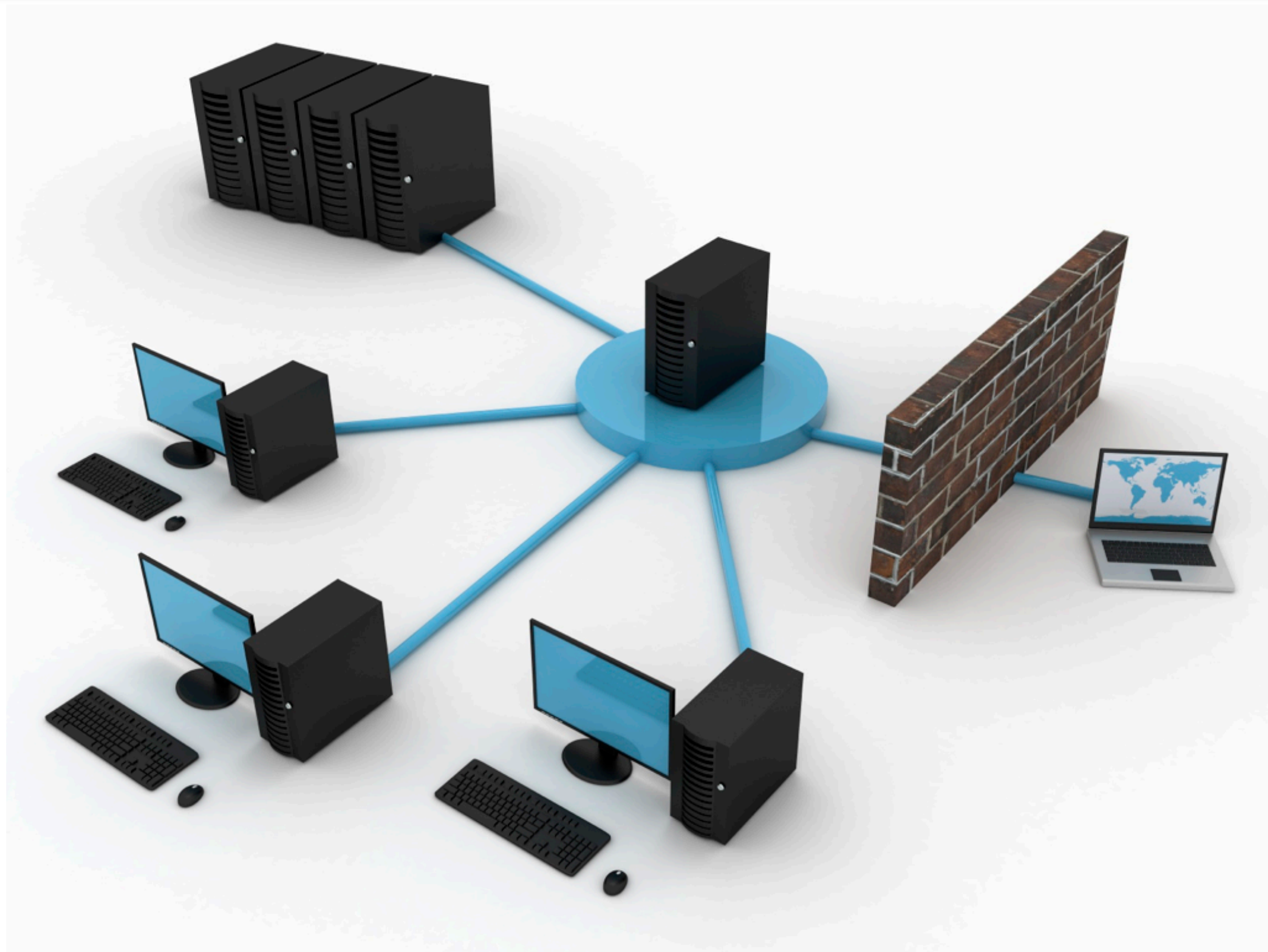
Geekin' :: VirtSec Style



- ❖ Setup & Context
- ❖ x86 Virtualization Overview in 90 Seconds
- ❖ Virtual Networking Architecture
- ❖ VirtSec Solutions Landscape
- ❖ The Four Horsemen
- ❖ Wrap-Up



Status Quo = **FAIL?**





Status Quo = **FAIL?**

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...”



Reality Bites

Replicating many highly-available security applications and network topologies in virtual switches doesn't work



Bumpy Road Ahead

“Everything’s Under Construction...”





Bumpy Road Ahead

**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..."





If It Ain't Fixed, Don't Break It

**Virtualized Security can
seriously impact performance,
resiliency and scalability**



Penny Wise & Pound Foolish



“Money for nuthin’ and my chips for free...”



Penny Wise & Pound Foolish

**Virtualizing security will not
save you money, it will cost you
more**



Where To Start?

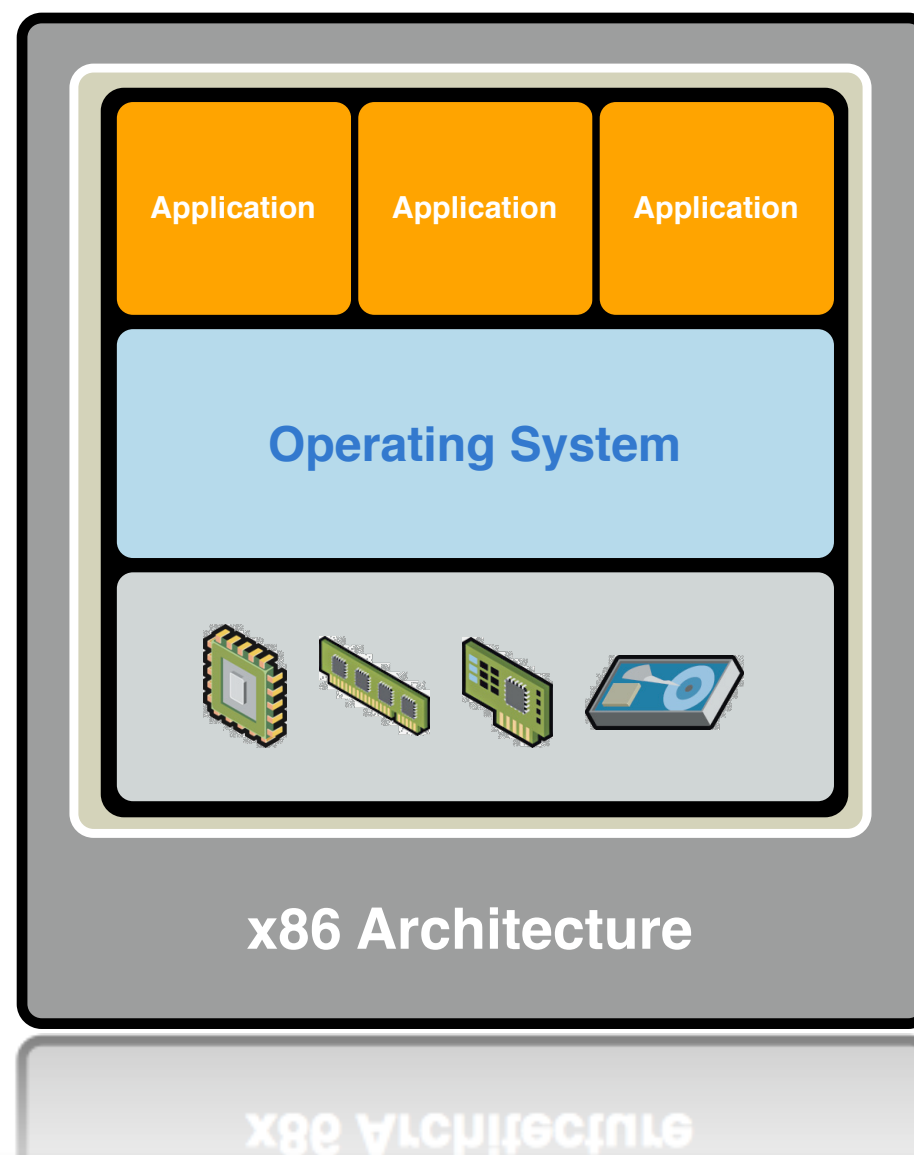
- ❖ Setup & Context
- ❖ x86 Virtualization Overview in 90 Seconds
- ❖ Virtual Networking Architecture
- ❖ VirtSec Solutions Landscape
- ❖ The Four Horsemen
- ❖ Wrap-Up





x86 Virtualization* Overview

From This

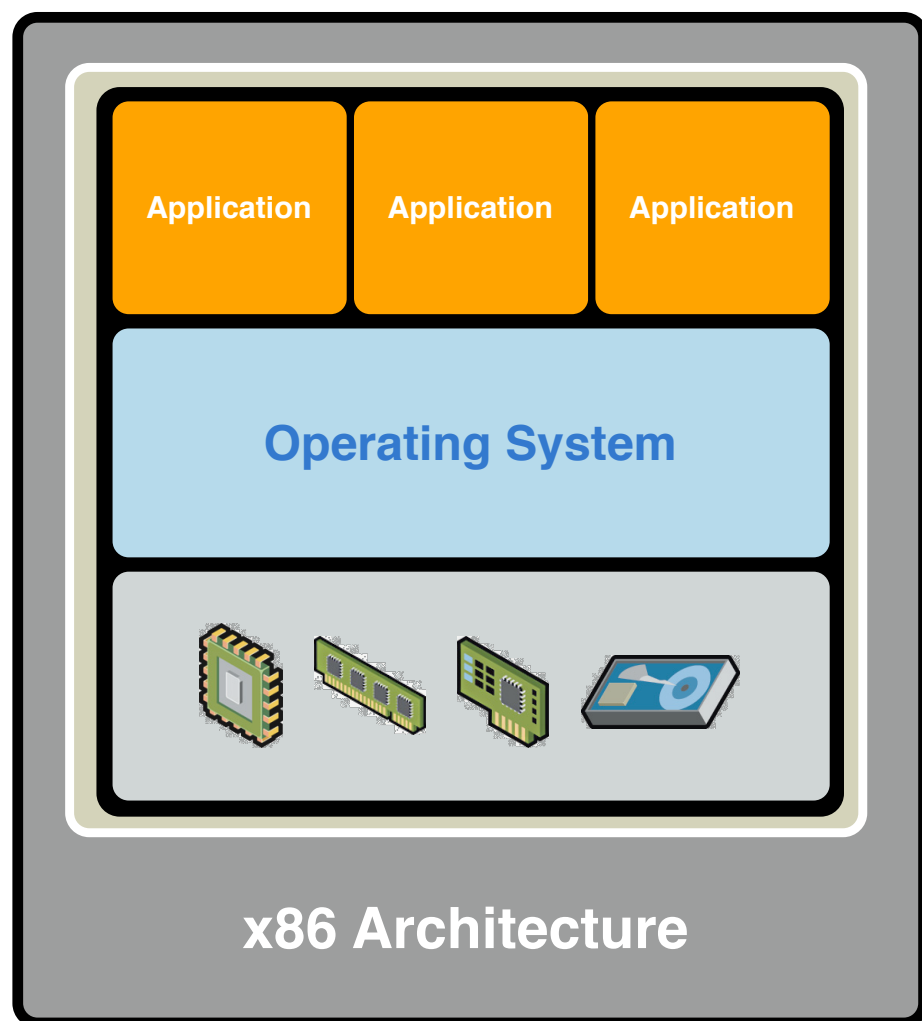


*Represents "Type 1" or Bare Metal "Server" Virtualization

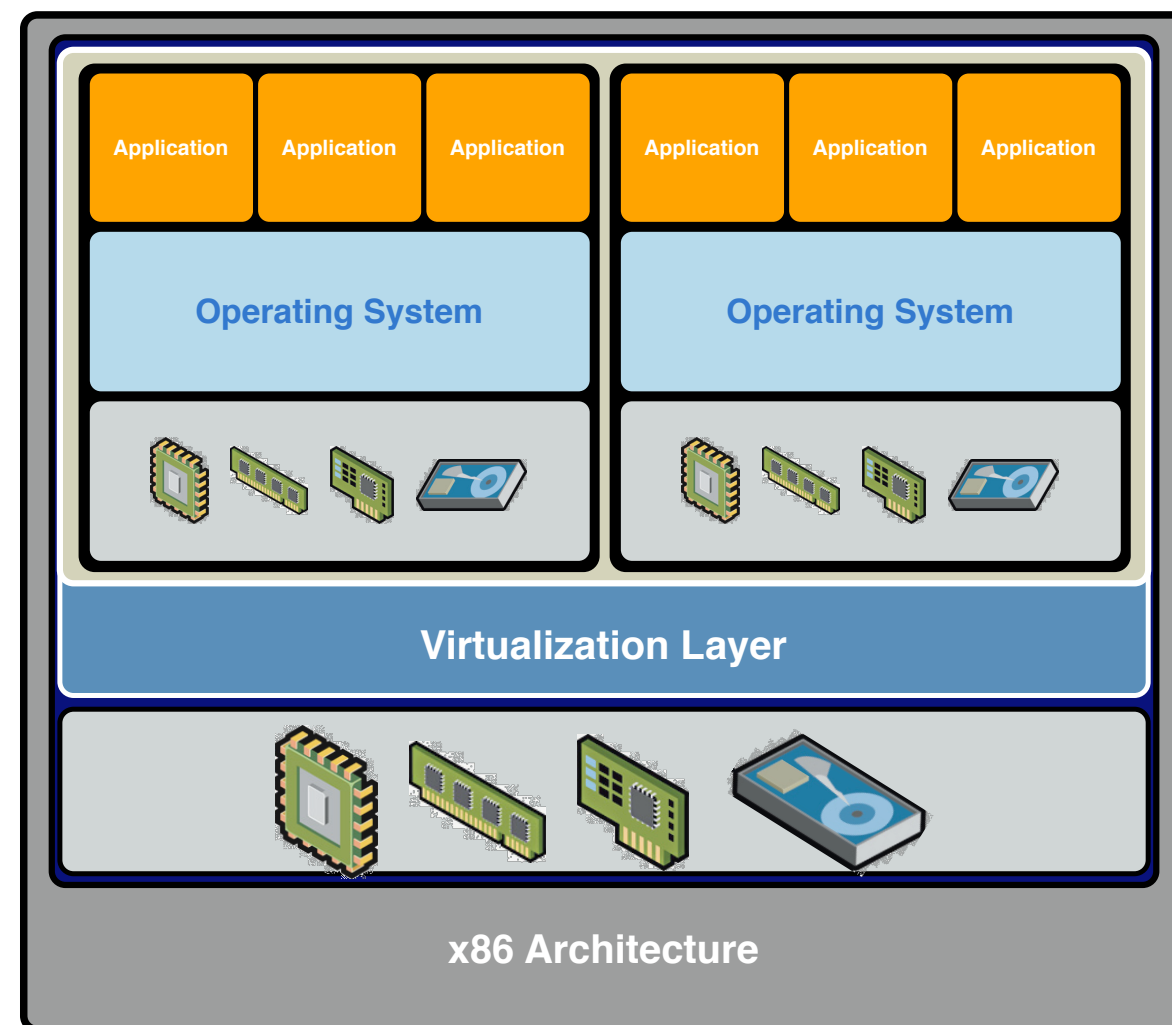


x86 Virtualization* Overview

From This



To This

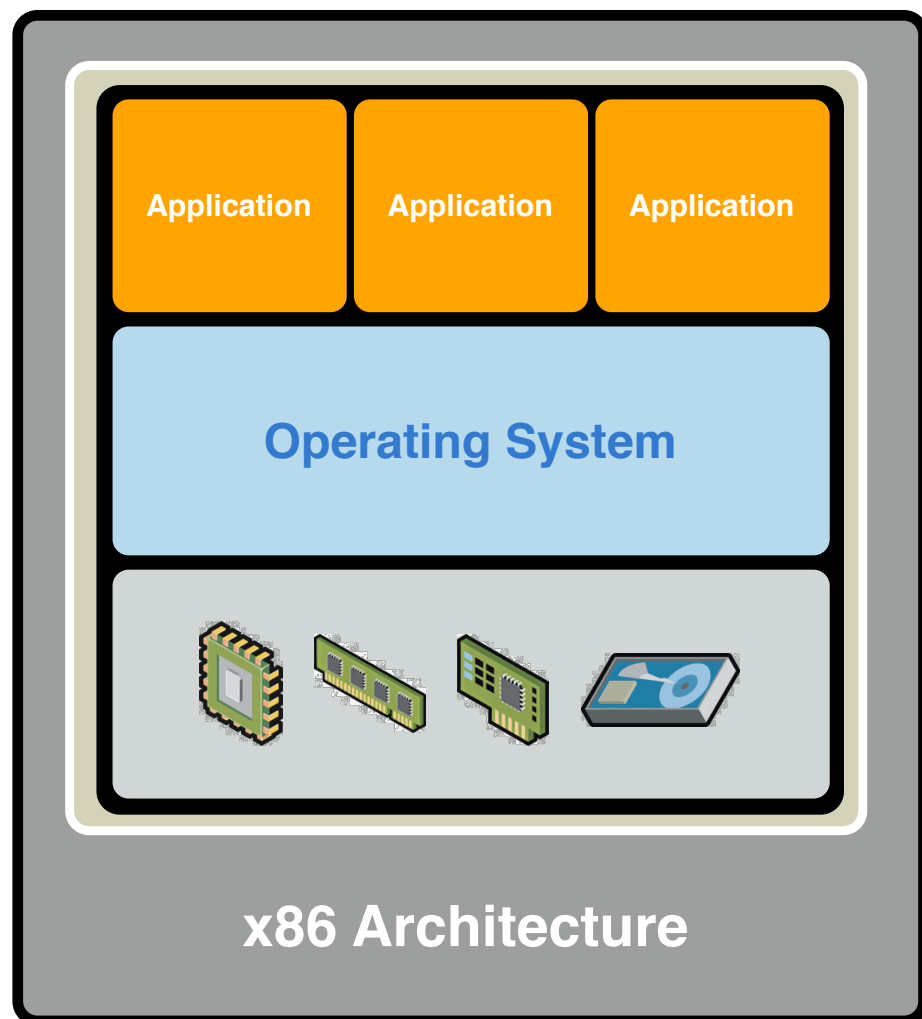


*Represents "Type 1" or Bare Metal "Server" Virtualization

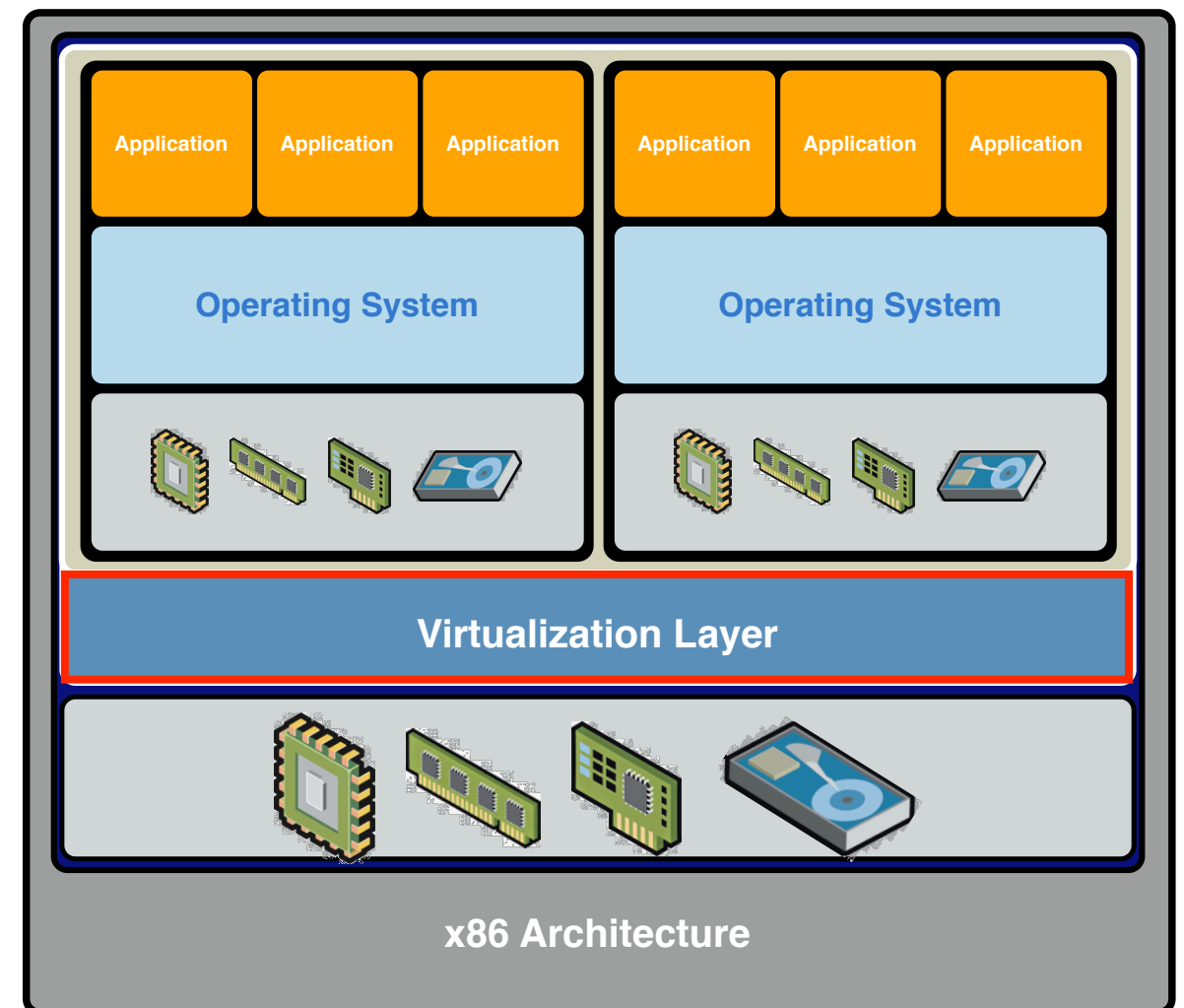


x86 Virtualization* Overview

From This



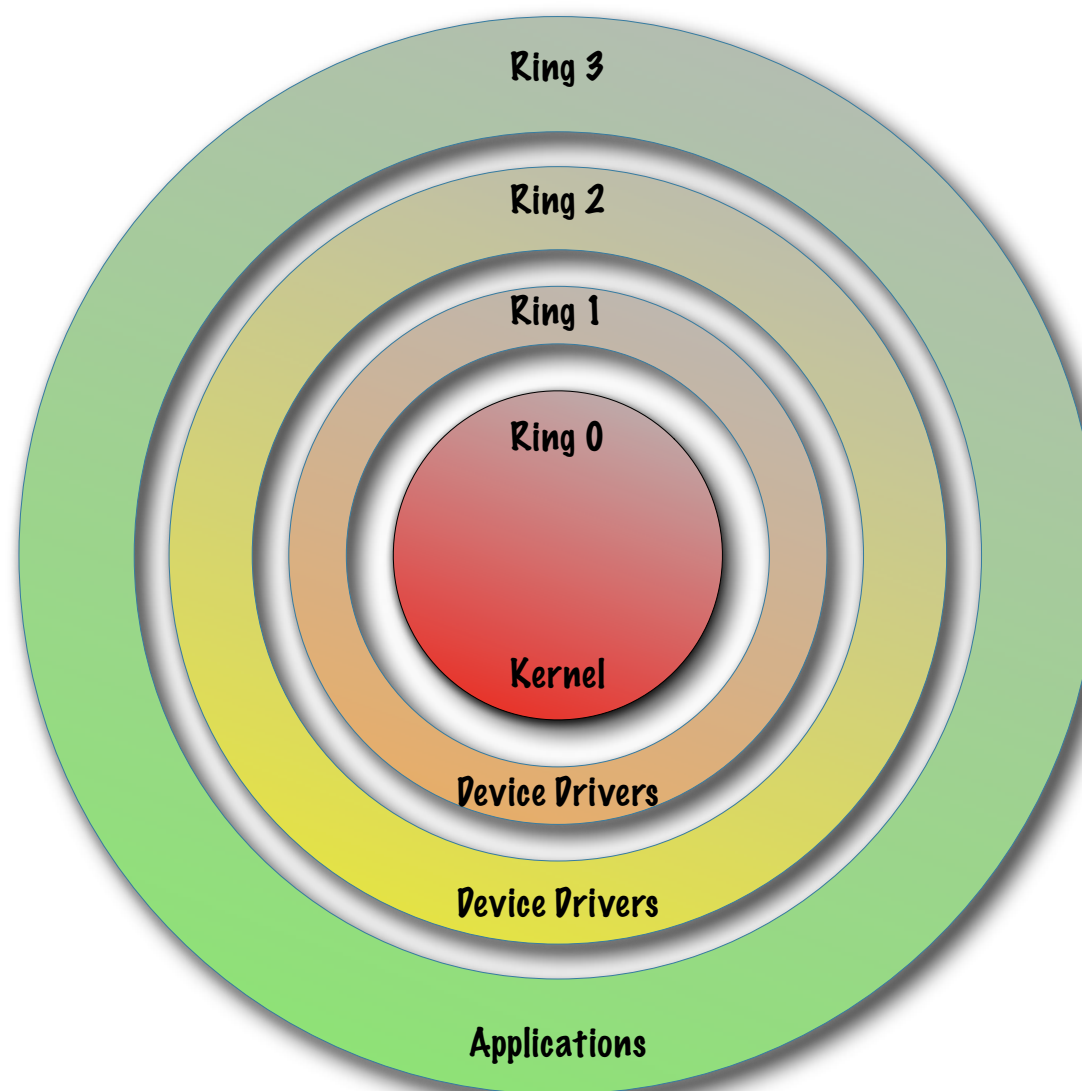
To This



*Represents "Type 1" or Bare Metal "Server" Virtualization



x86 Hierarchical Protection Domains/Rings



Most Privileged



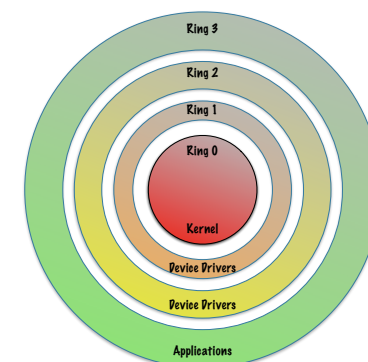
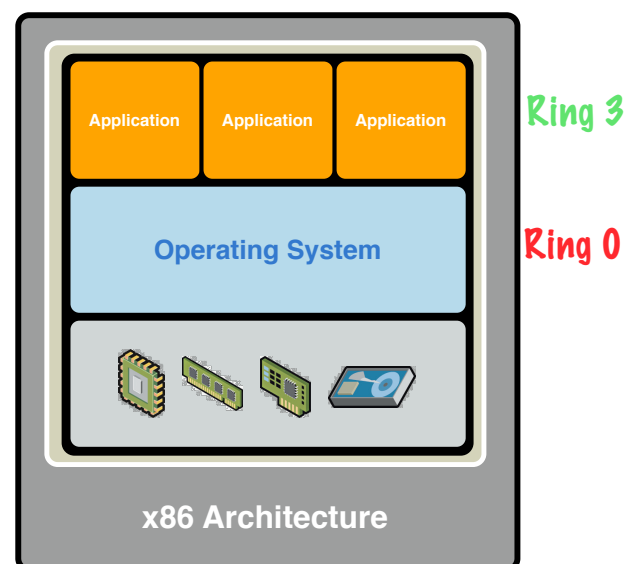
Least Privileged

Adapted from: http://en.wikipedia.org/wiki/Supervisor_mode



x86 Protection Ring Compression For Dummies

Physical/
Non-Virtualized



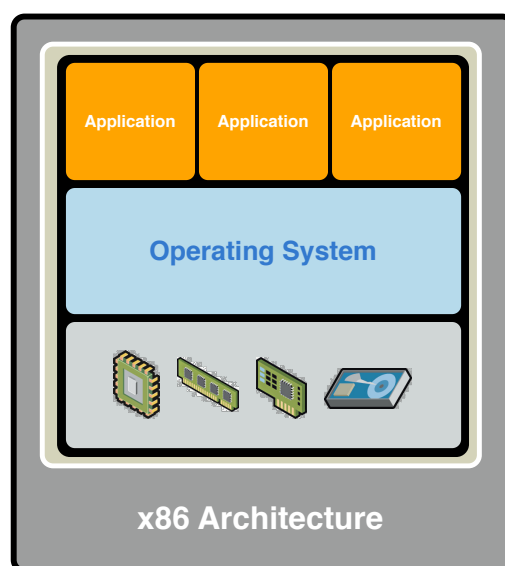
Most Privileged ■ ■ ■ Least Privileged

**There is also para-virtualization, not covered here...*

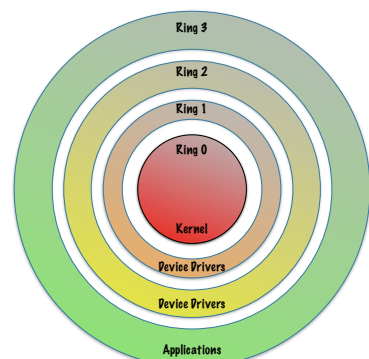
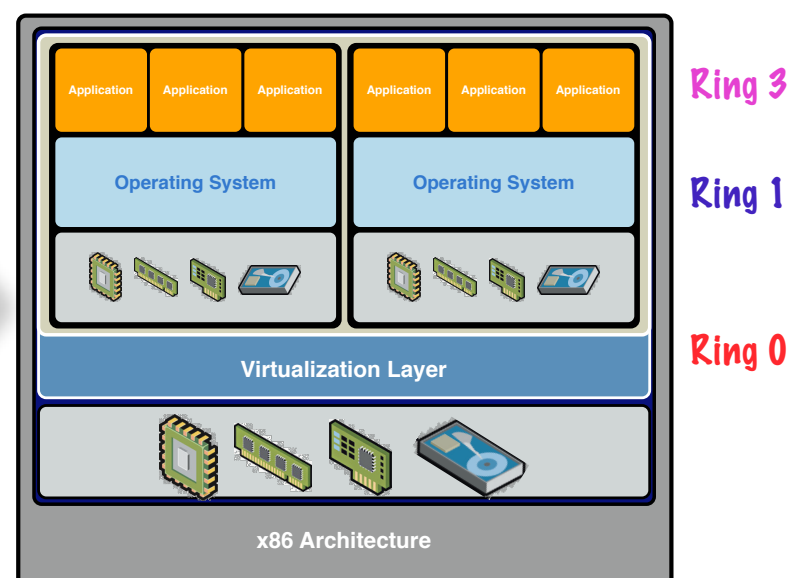


x86 Protection Ring Compression For Dummies

Physical/ Non-Virtualized



Virtualized: Software Only



Most Privileged ■ ■ ■ ■ Least Privileged

❖ 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

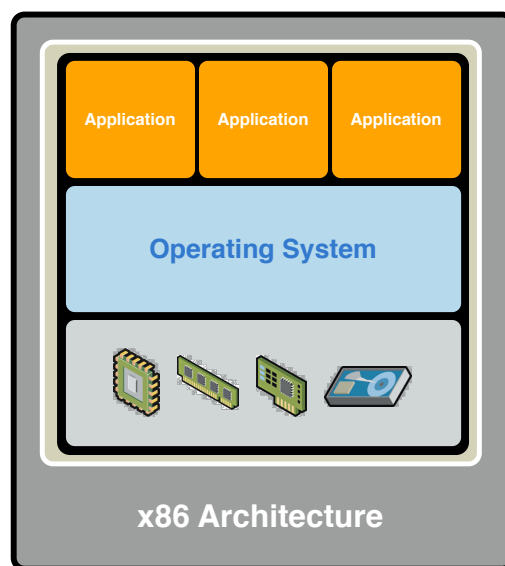
❖ Can cause issues/conflicts due to contention for the 17 x86 privileged platform control instructions

*There is also para-virtualization, not covered here...

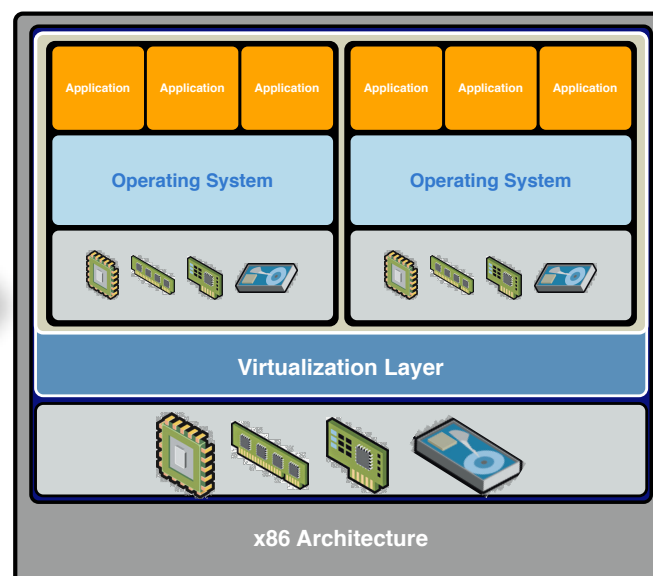


x86 Protection Ring Compression For Dummies

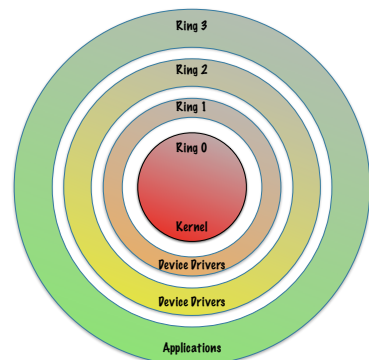
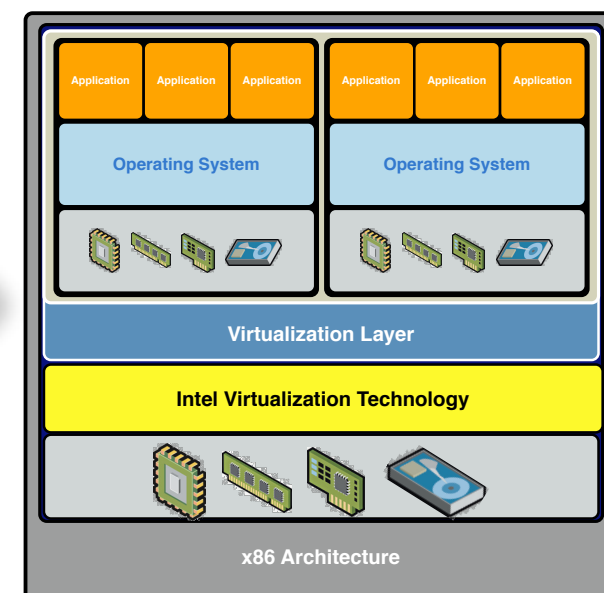
Physical/ Non-Virtualized



Virtualized: Software Only



Virtualized: Hardware Assisted



Most Privileged ■ ■ ■ ■ Least Privileged

❖ 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...



...and they're showing up everywhere





No One Ring0 To Rule Them All!



Which means:

- ▶ You will likely end up with 4-5 virtualization platforms/VMM's spread out across the horizon of your enterprise

The key differentiators?

- ▶ Management, integration, extensibility and security

We need open standards for solution interoperability

- ▶ If you have issues with the "simple complexity" of a single virtualization platform, imagine when you have many





Debating Virtualization & Security

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



Debating Virtualization & Security

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



Time For Sublime Design

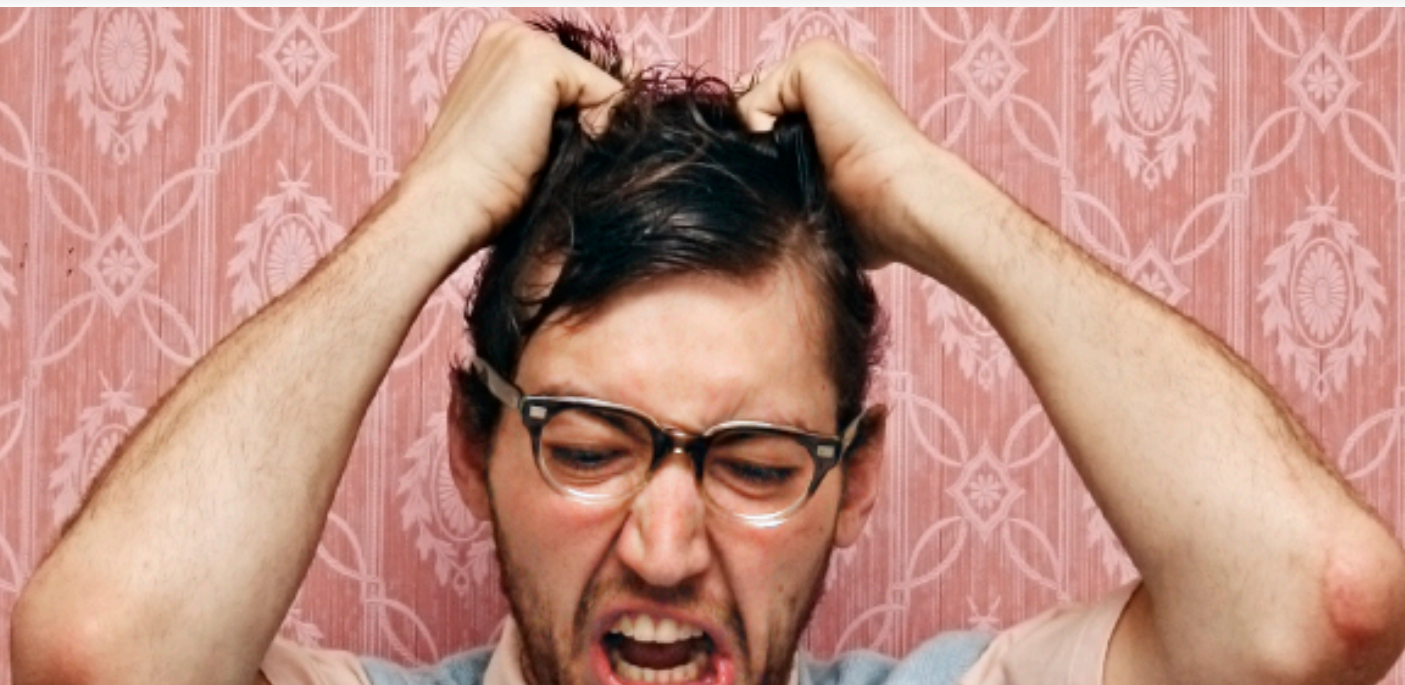
- ❖ Setup & Context
- ❖ x86 Virtualization Overview in 90 Seconds
- ❖ Virtual Networking Architecture
- ❖ VirtSec Solutions Landscape
- ❖ The Four Horsemen
- ❖ Wrap-Up





Caveats

- ❖ This presentation uses VMware ESX as my virtualization platform example featuring data networking only; storage is a whole other universe of security fun...
- ❖ We're also intentionally not covering client virtualization to keep things streamlined
- ❖ 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...
- ❖ There are far too many dirty little secrets and unspoken truths regarding implementing VirtSec today; we're going to talk about them here





But d00d, What About Virtualization Malware!?



But d00d, What About Virtualization Malware!?





But d00d, What About Virtualization Malware!?

There are many really interesting topics to discuss here:

- ❖ Hypervisor Malware & Hyperjacking
- ❖ Exploiting the virtualization chipsets for fun and profit
- ❖ Hardware/Firmware abuse
- ❖ Control channel manipulation

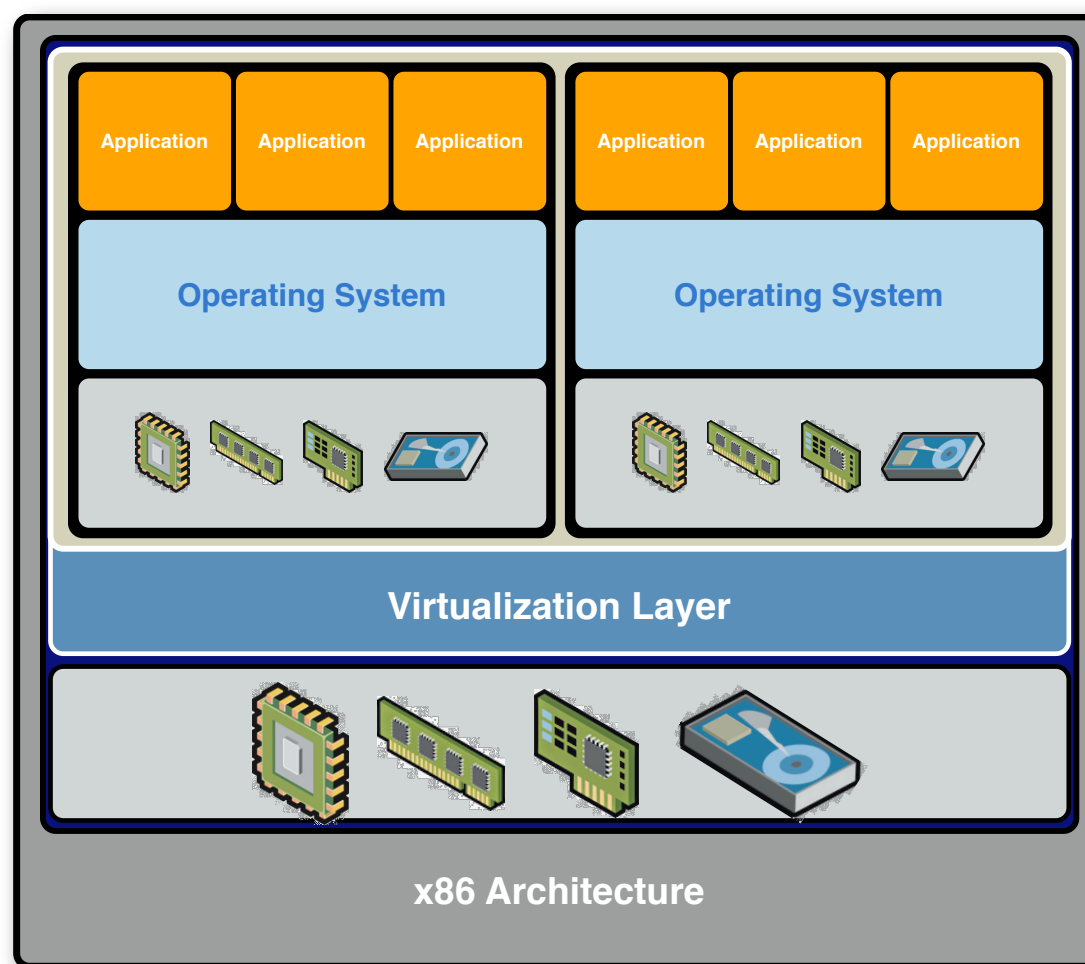
I'm neither qualified or motivated to talk about these topics and we've got much more profound and fundamental sets of issues to discuss.

There's an entire track dedicated to this stuff. Go there.



Virtual Networking Architecture

Virtual System

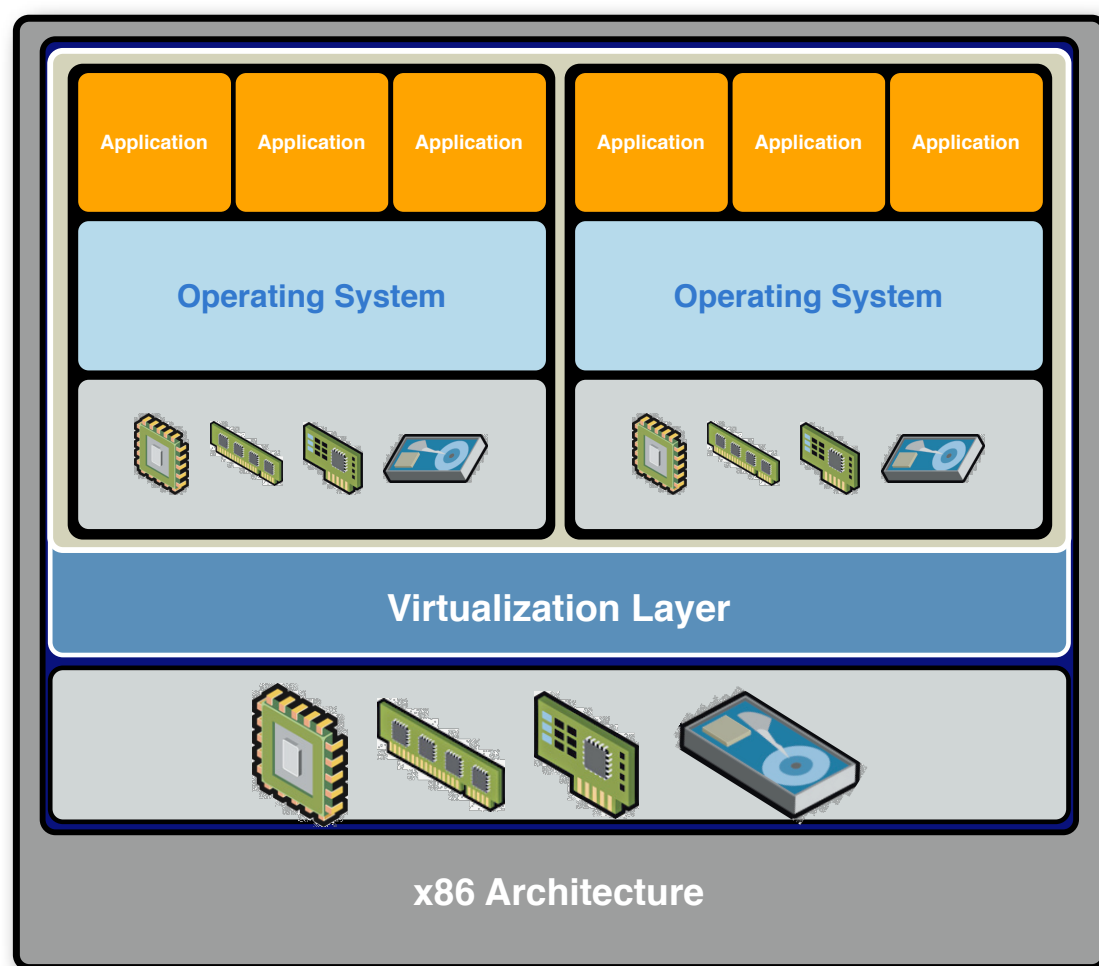


*Not shown for clarity: Service Console/VMKernel/Storage Networking

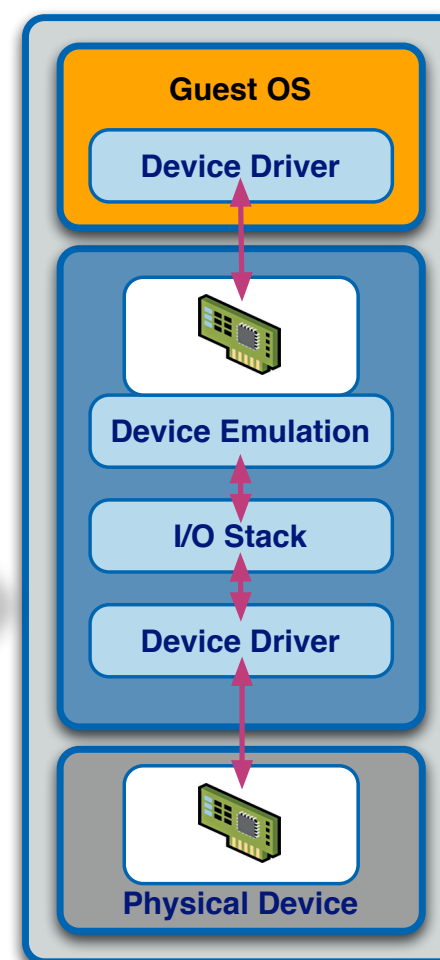


Virtual Networking Architecture

Virtual System



Virtual Networking

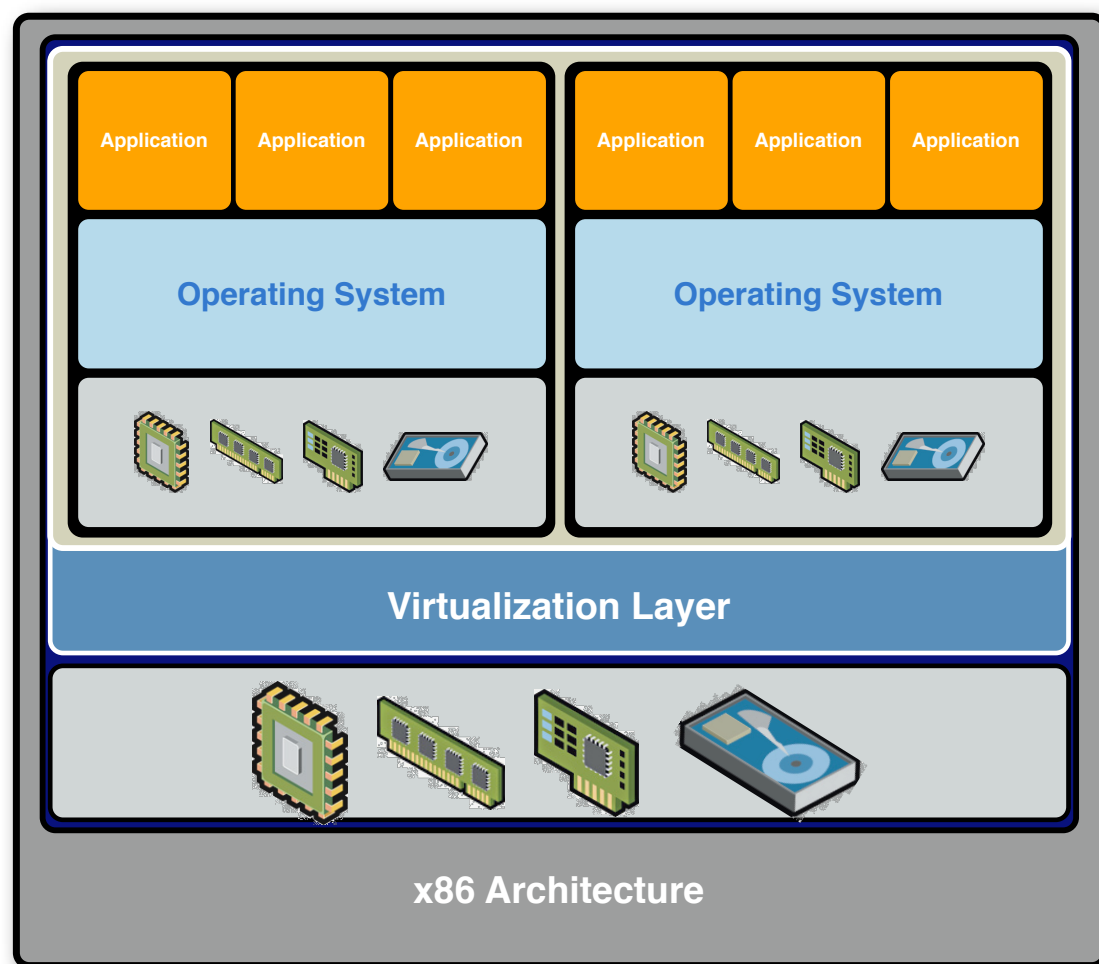


*Not shown for clarity: Service Console/VMKernel/Storage Networking

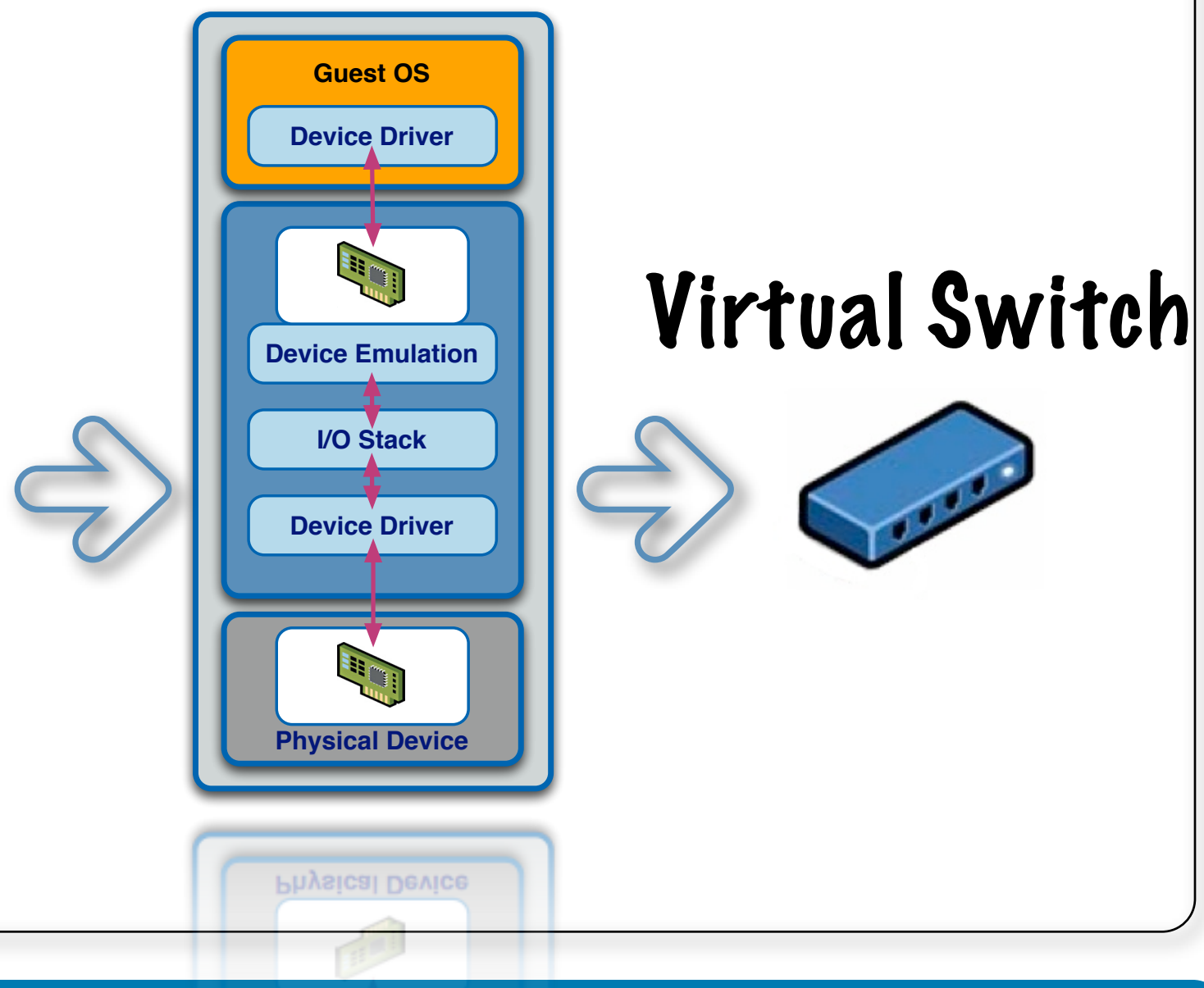


Virtual Networking Architecture

Virtual System



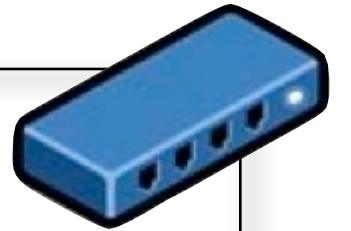
Virtual Networking



*Not shown for clarity: Service Console/VMKernel/Storage Networking



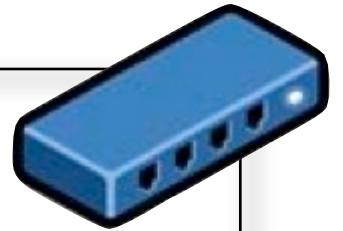
Virtual Switch Defined





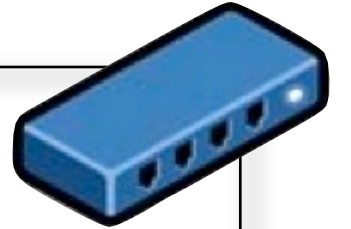
Virtual Switch Defined

A Virtual Switch:





Virtual Switch Defined

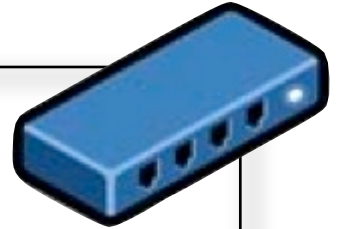


A Virtual Switch:

- ❖ Is a software-based networking construct that runs in the virtualization platform's kernel



Virtual Switch Defined

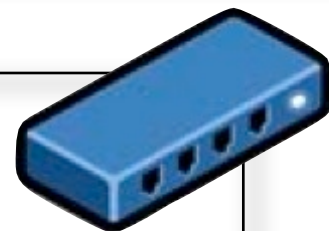


A Virtual Switch:

- ❖ 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:



Virtual Switch Defined

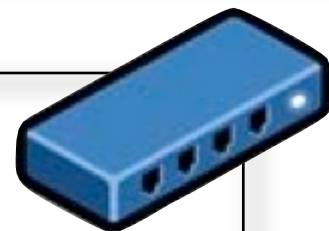


A Virtual Switch:

- ❖ 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



Virtual Switch Defined

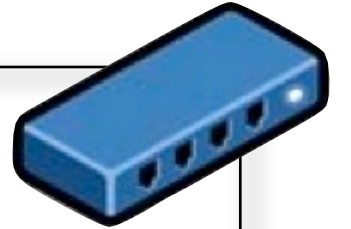


A Virtual Switch:

- ❖ 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



Virtual Switch Defined

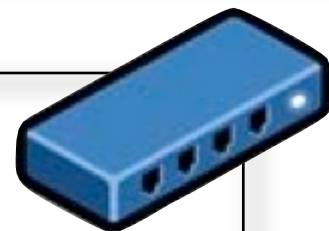


A Virtual Switch:

- ❖ 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



Virtual Switch Defined



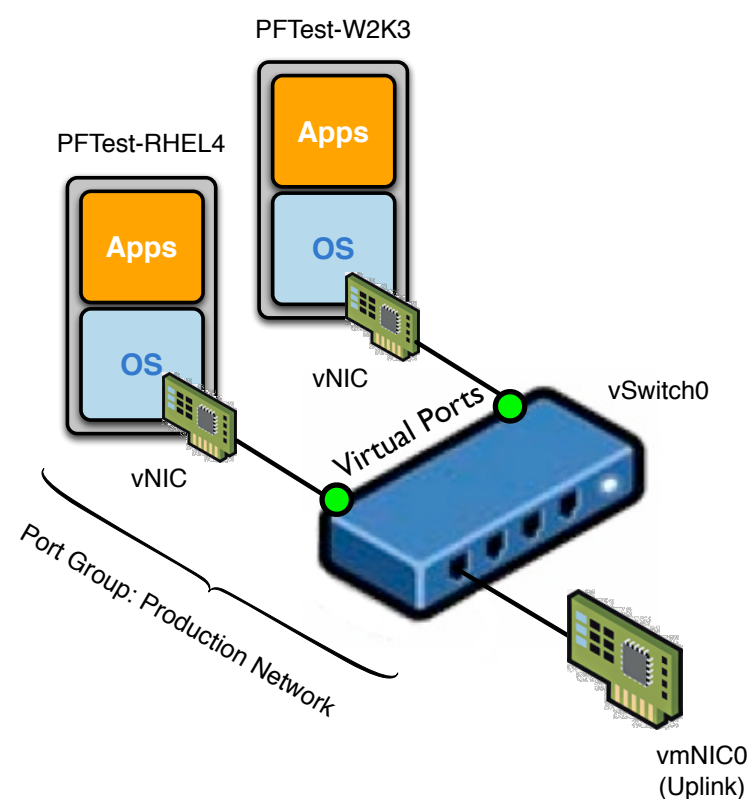
A Virtual Switch:

- ❖ 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...)



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

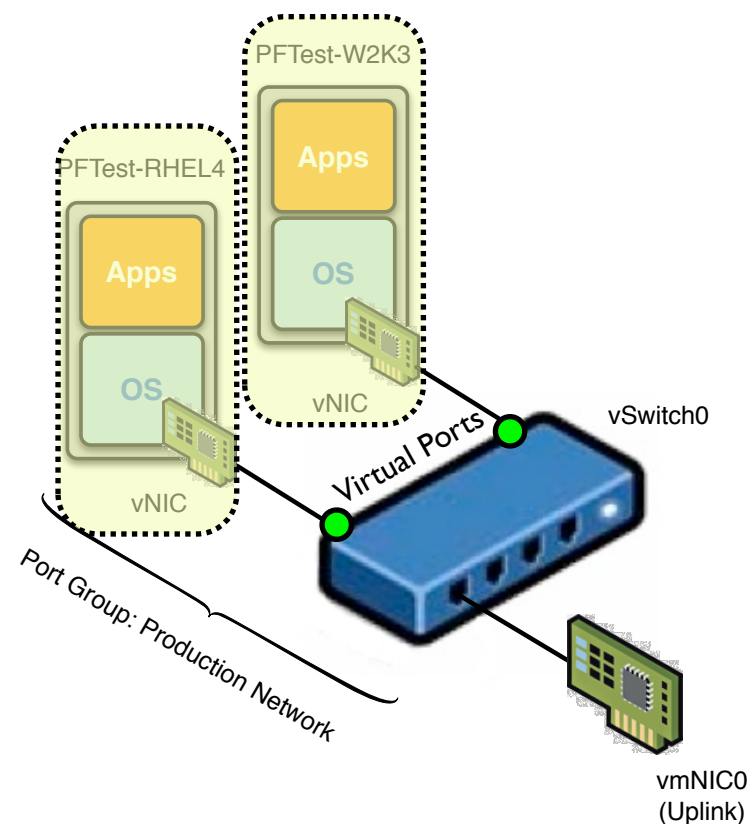


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

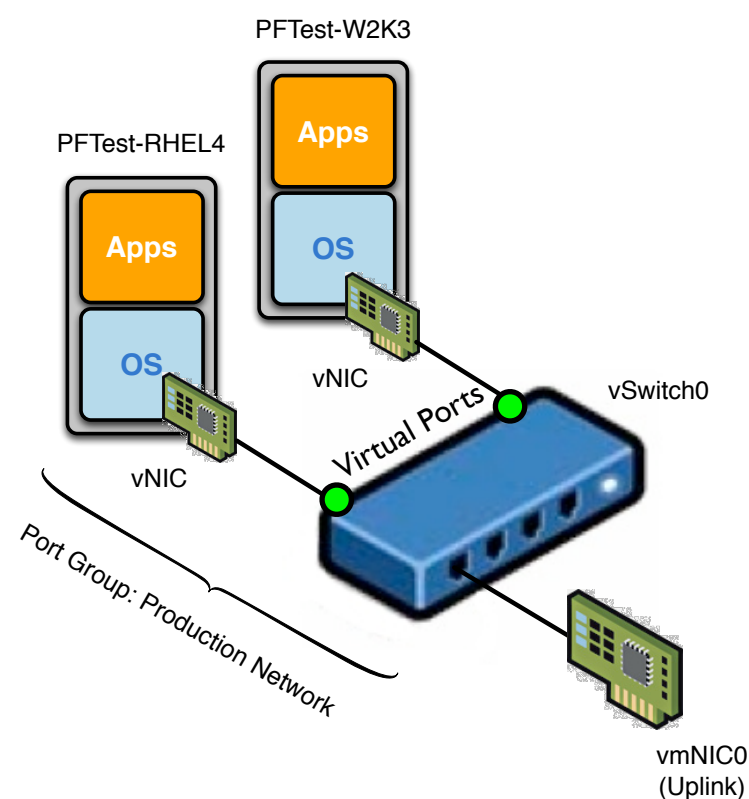


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

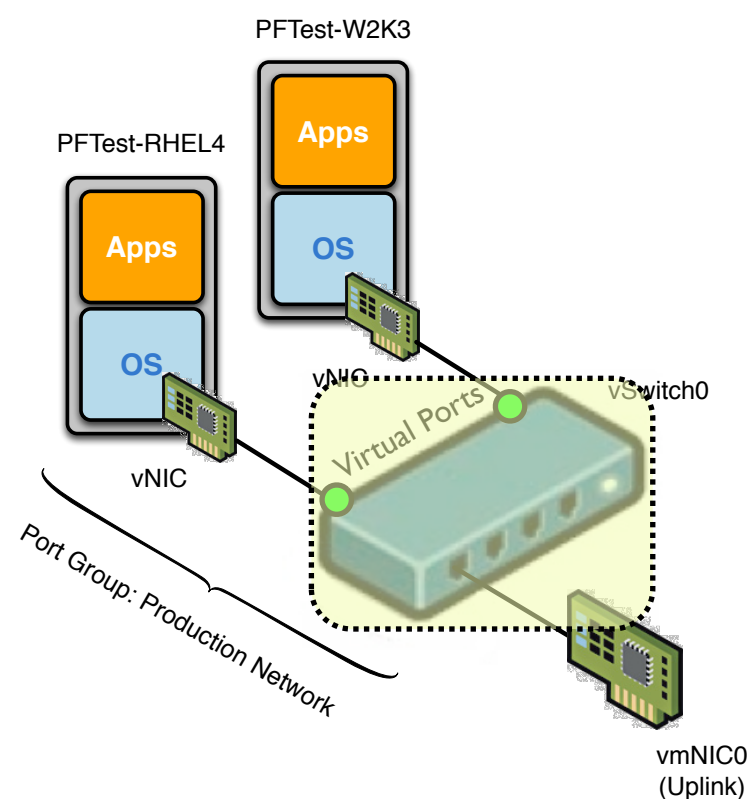


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

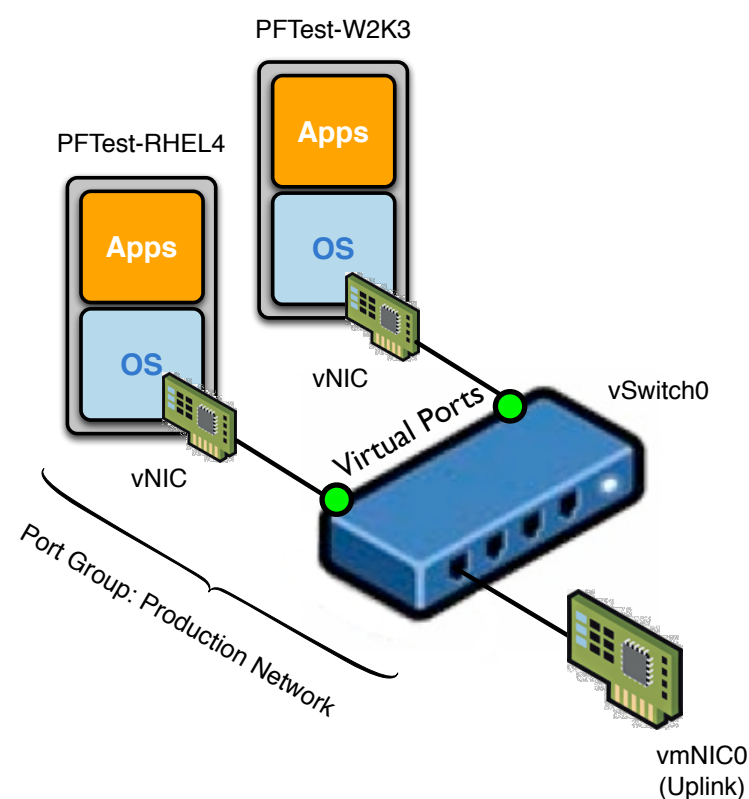


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

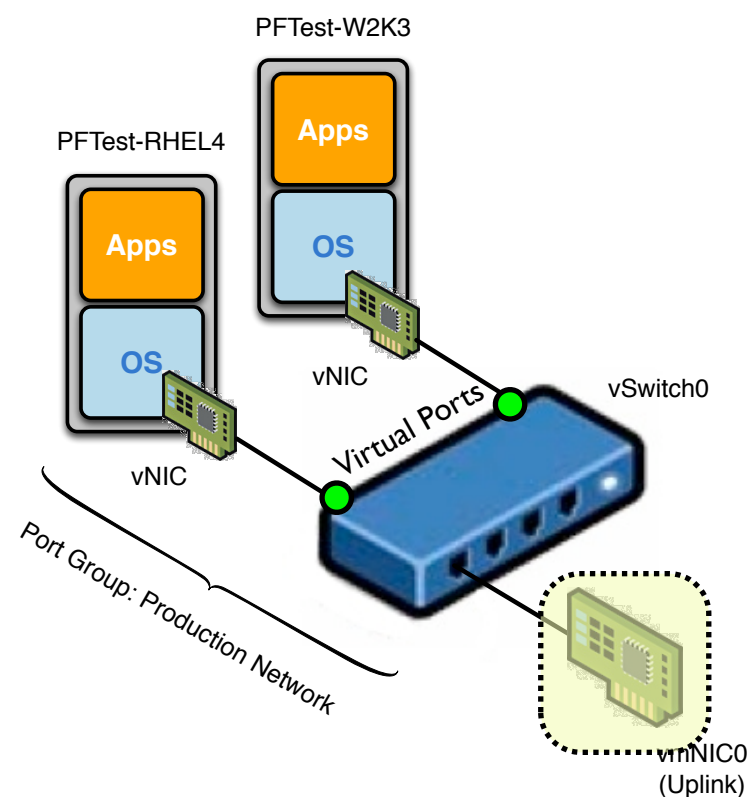


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



VMware Virtual Infrastructure Client View

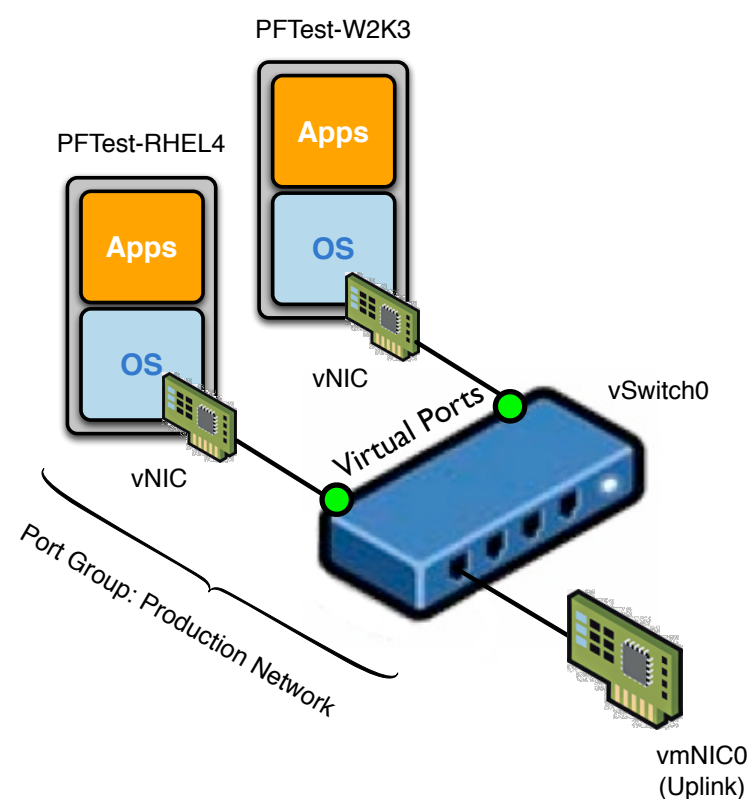


* I purposely left off the VMotion and Service Console networks in the model for clarity



Virtual Switch Visualized

Abstracted Model



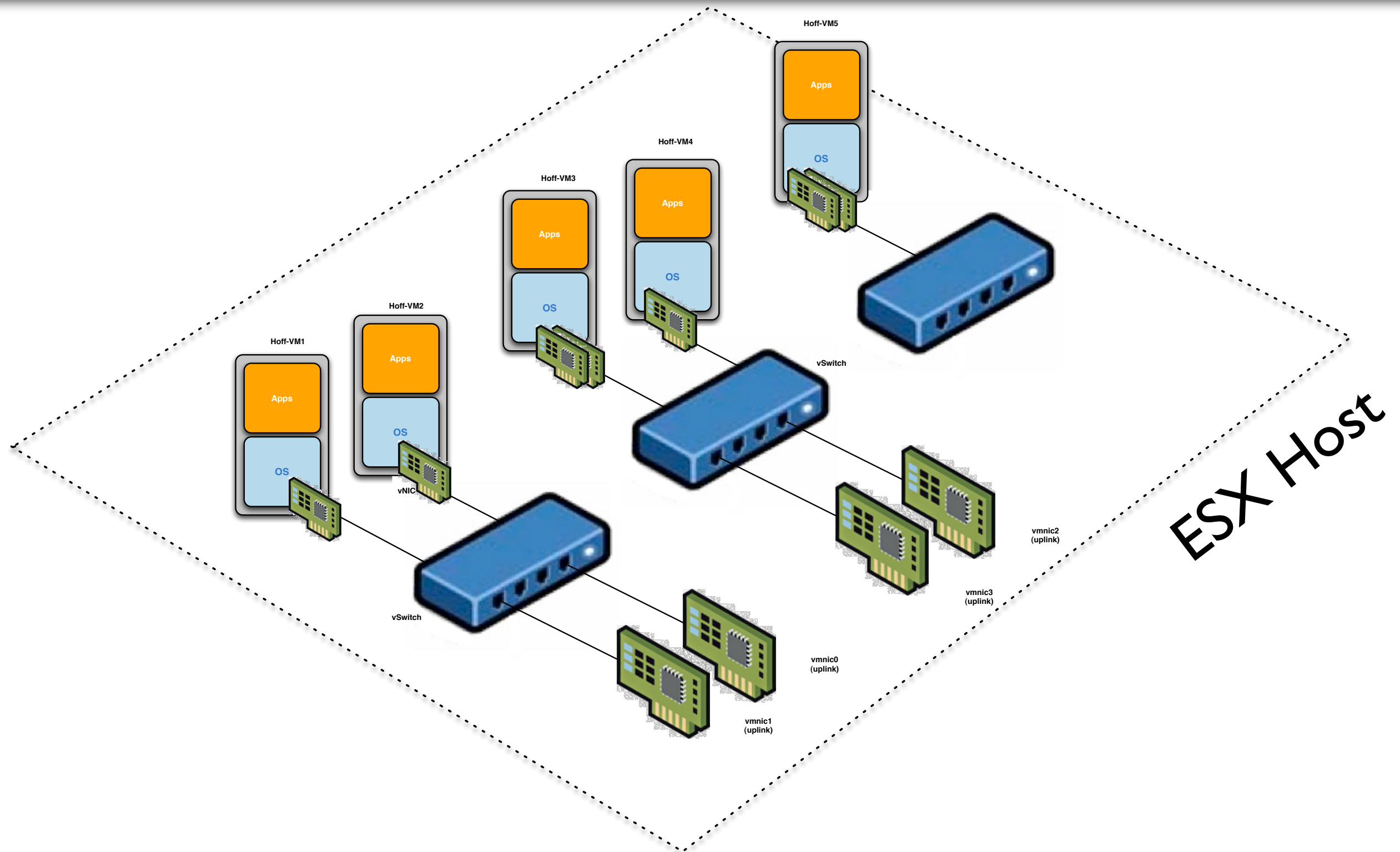
VMware Virtual Infrastructure Client View



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

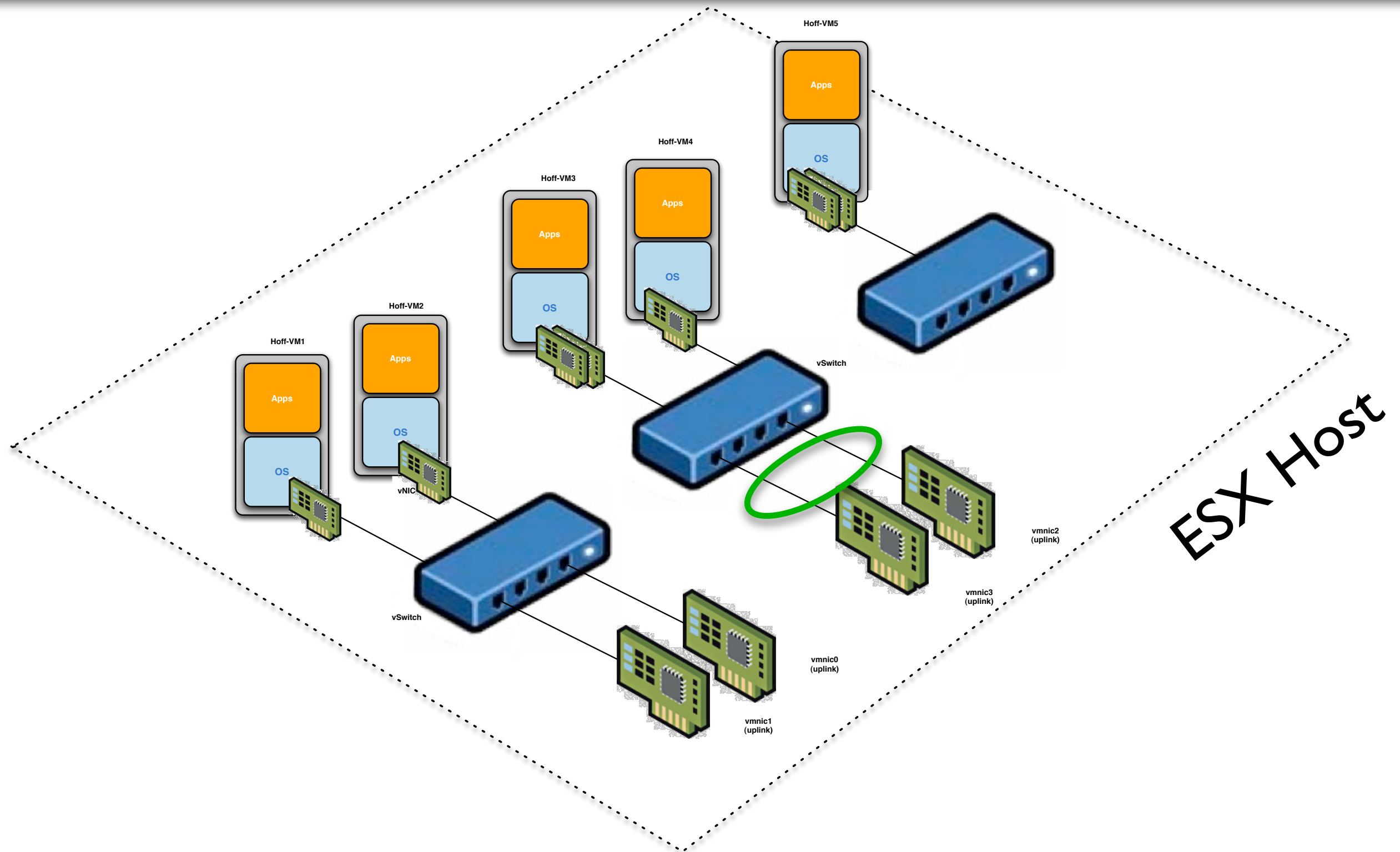


vSwitch Correctness



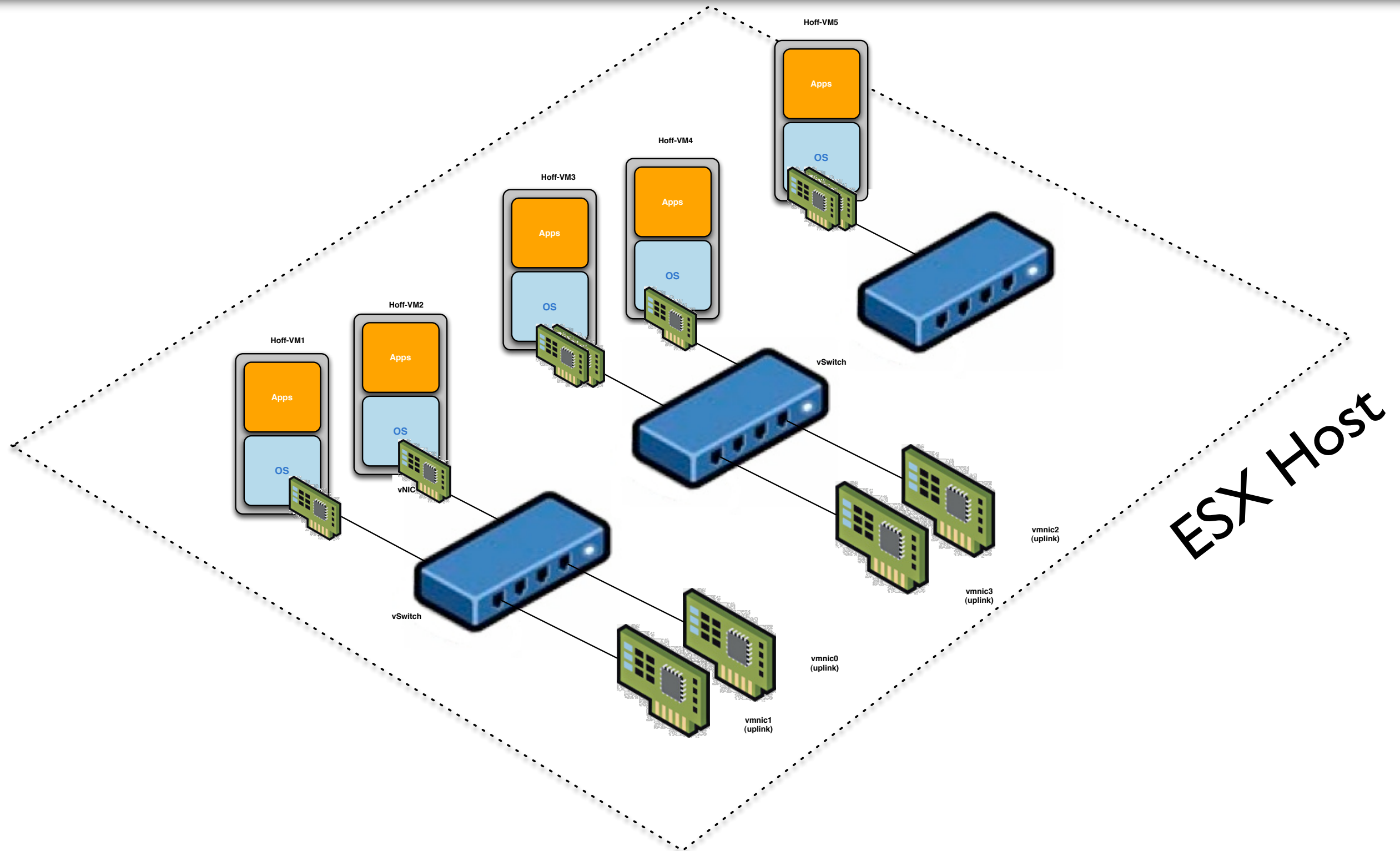


vSwitch Correctness



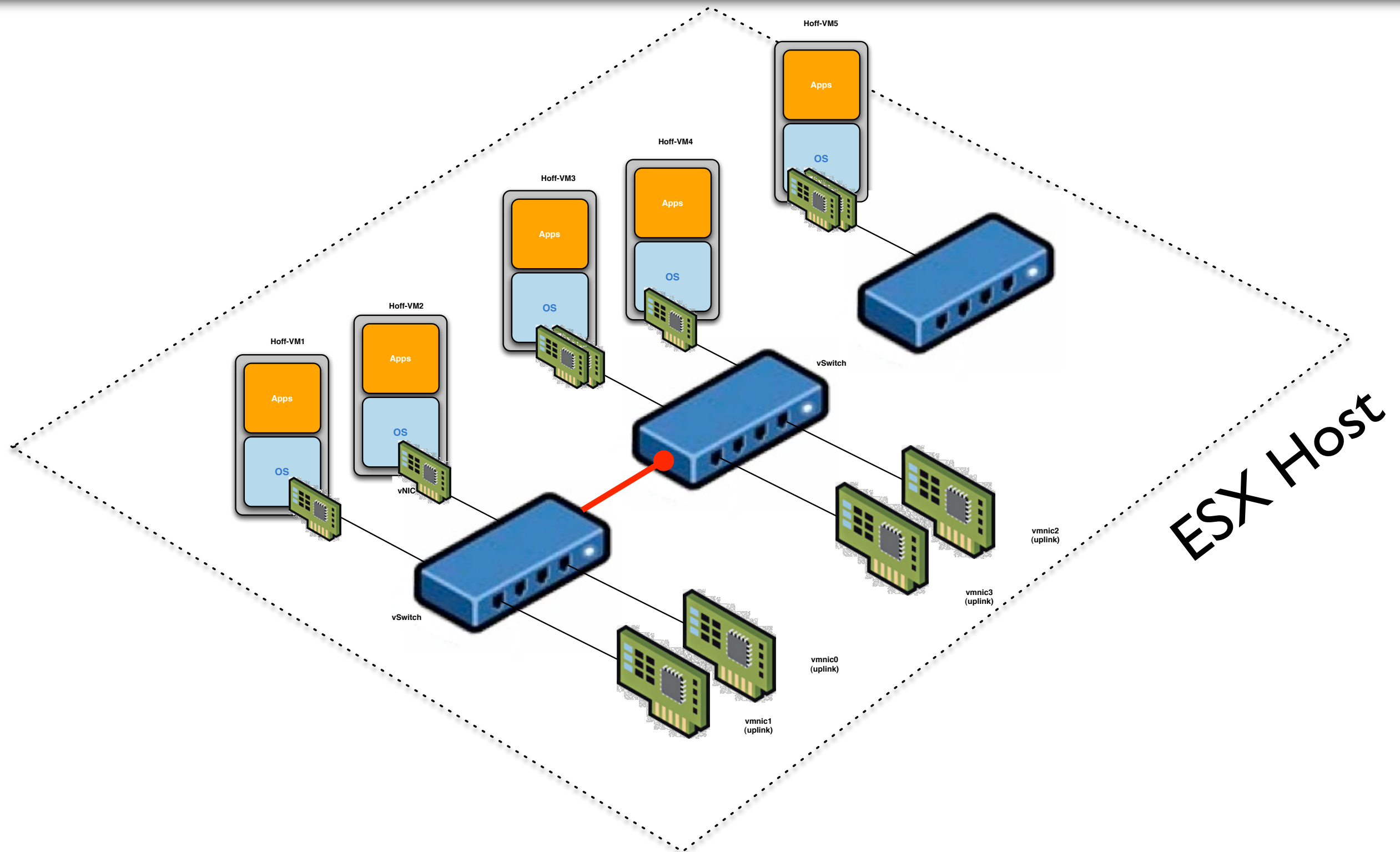


vSwitch Correctness



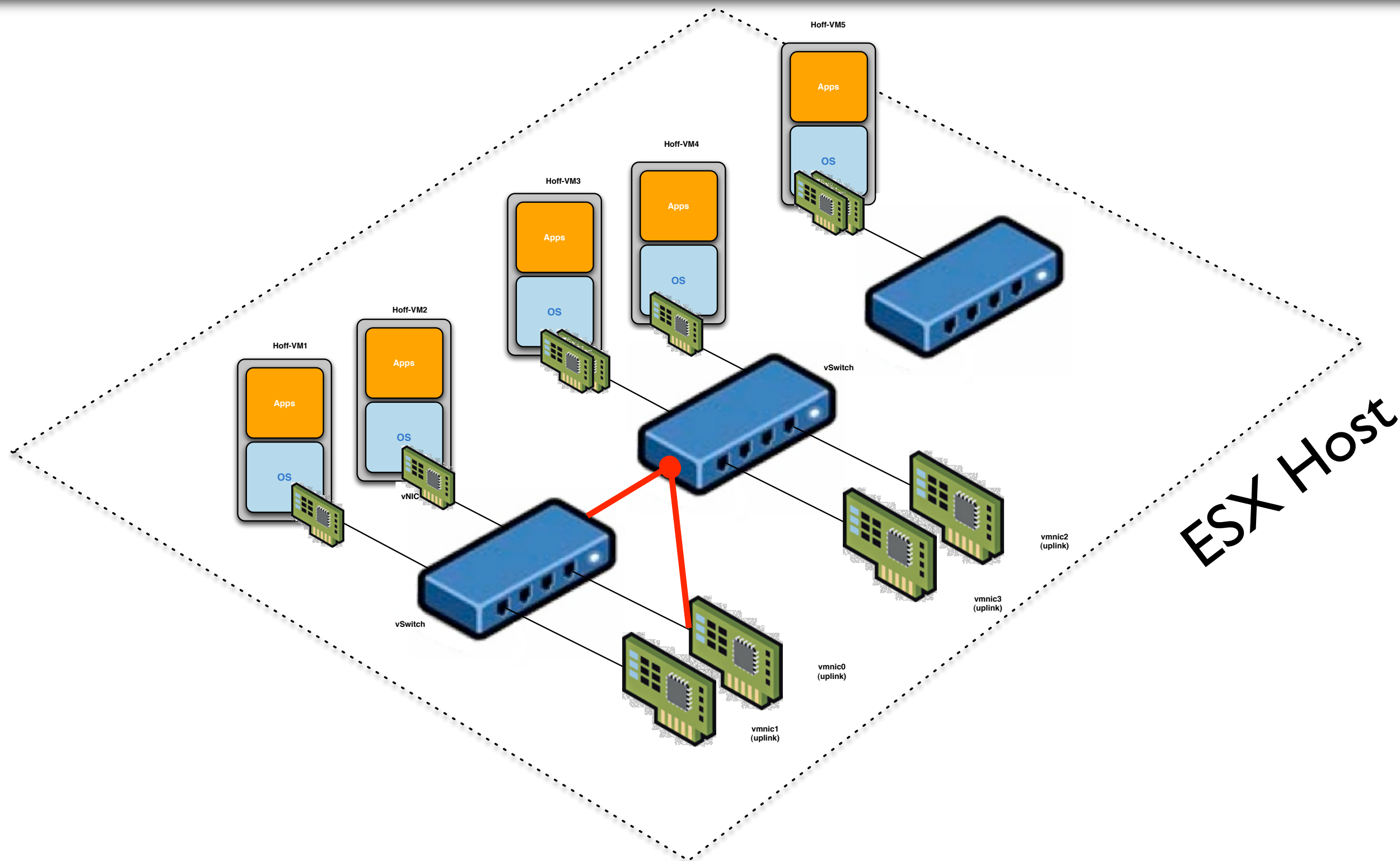


vSwitch Correctness



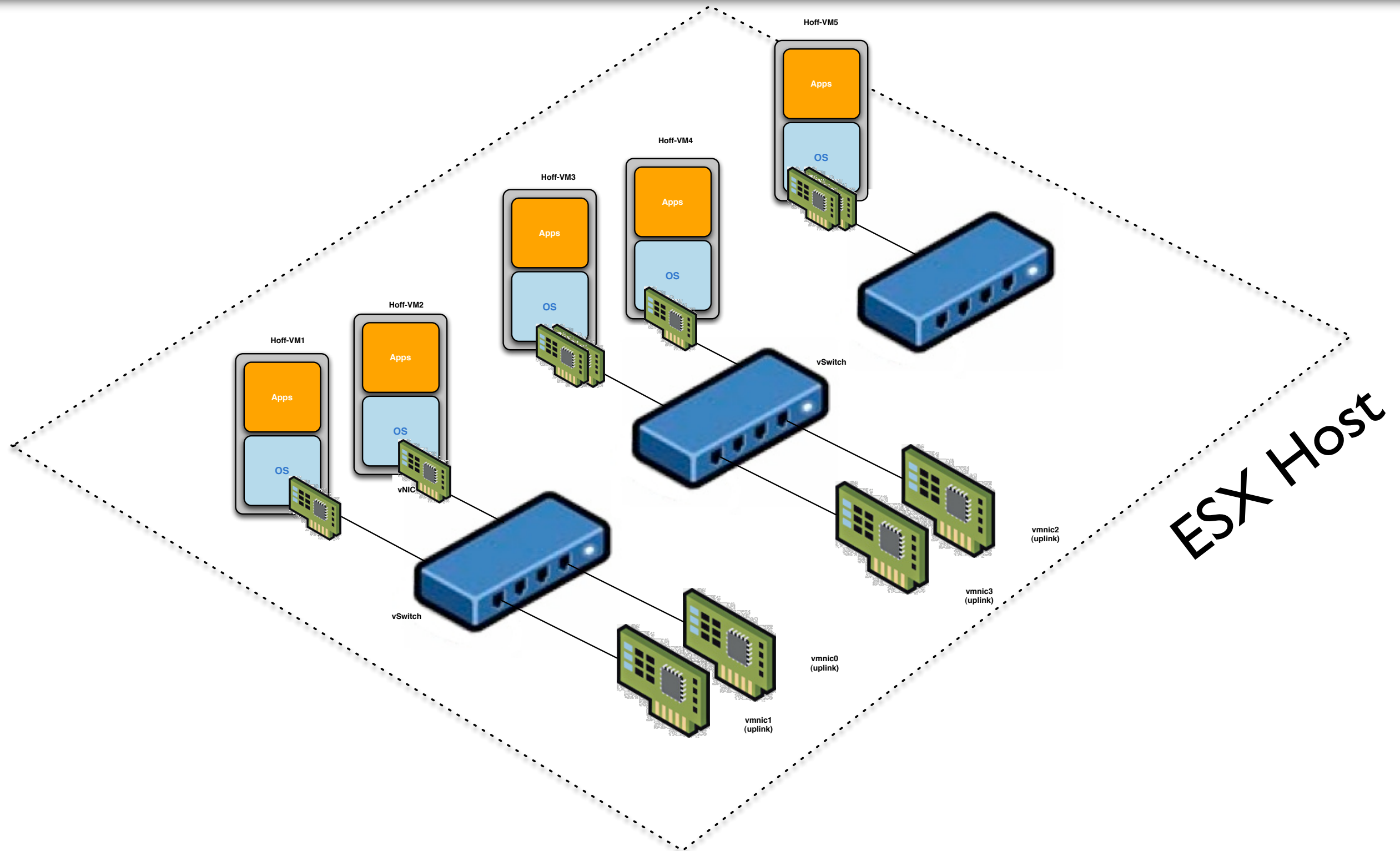


vSwitch Correctness



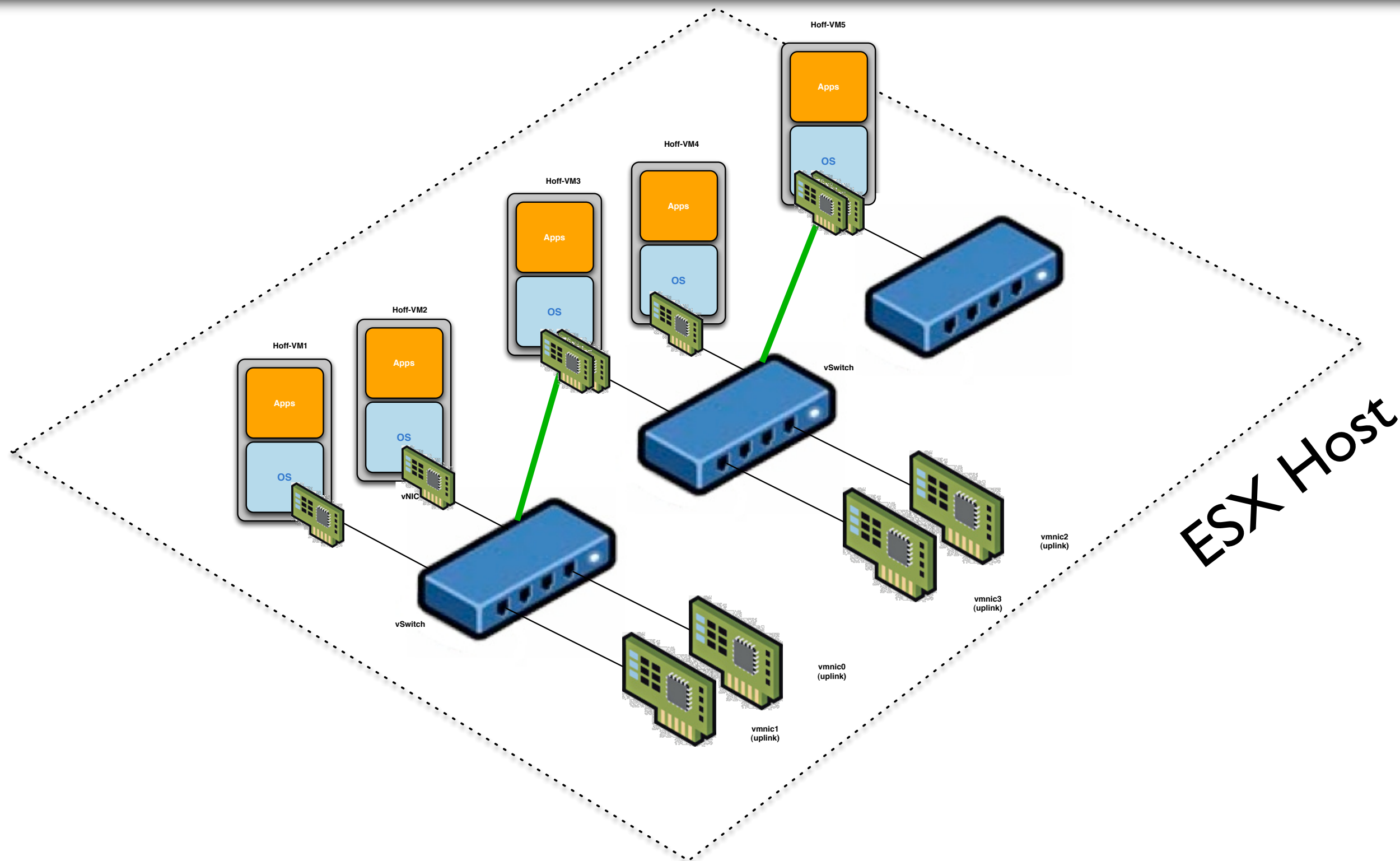


vSwitch Correctness



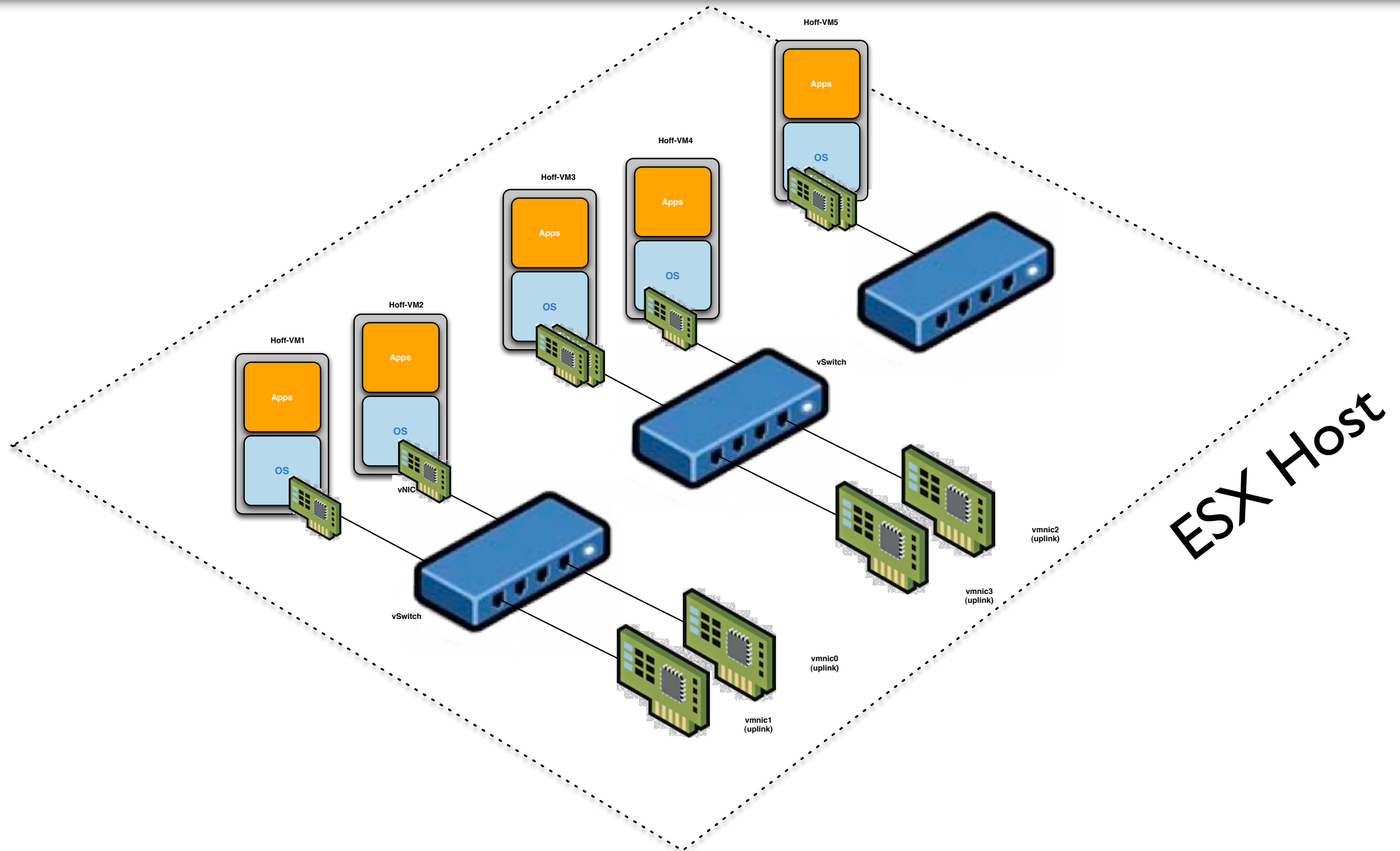


vSwitch Correctness



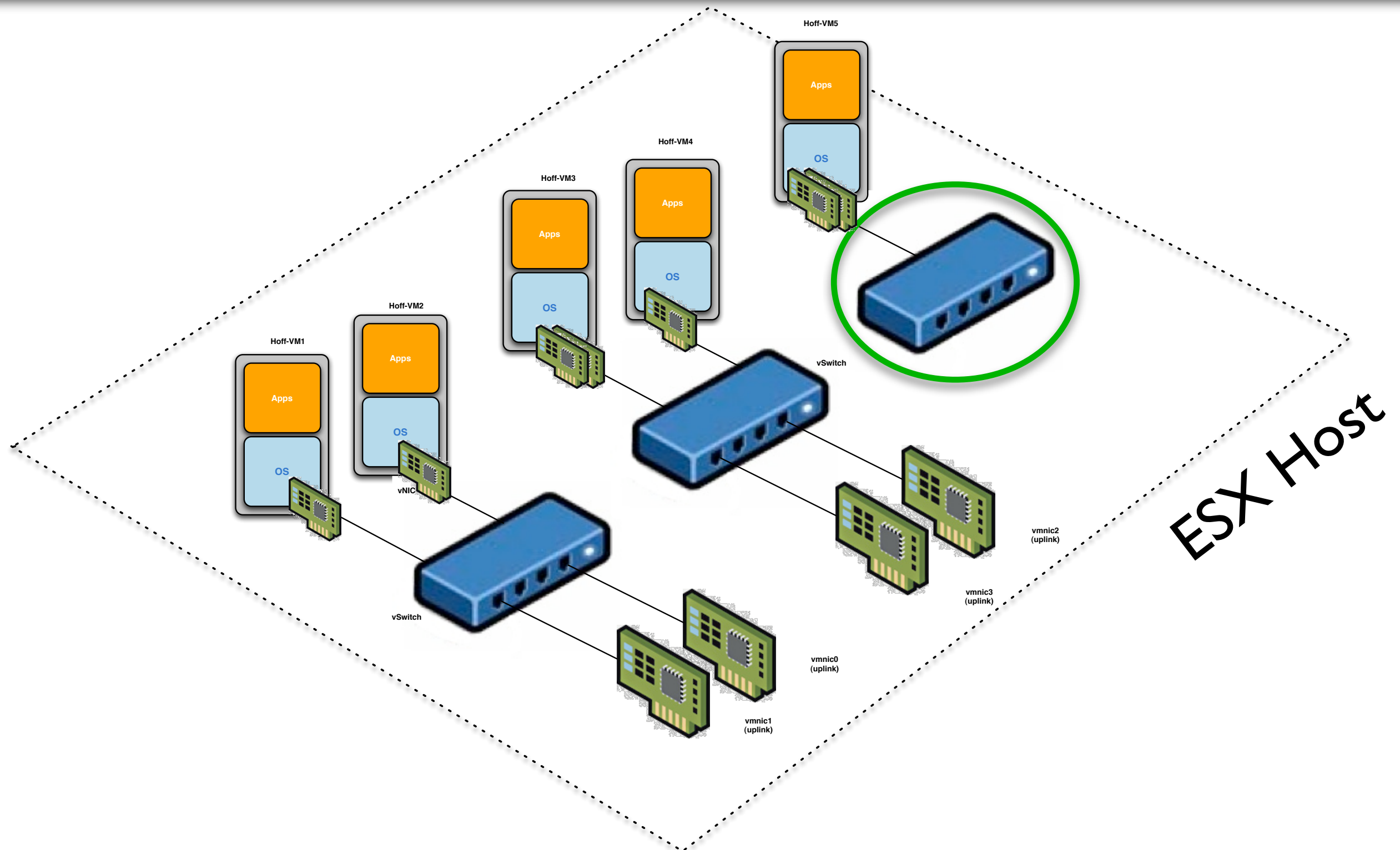


vSwitch Correctness



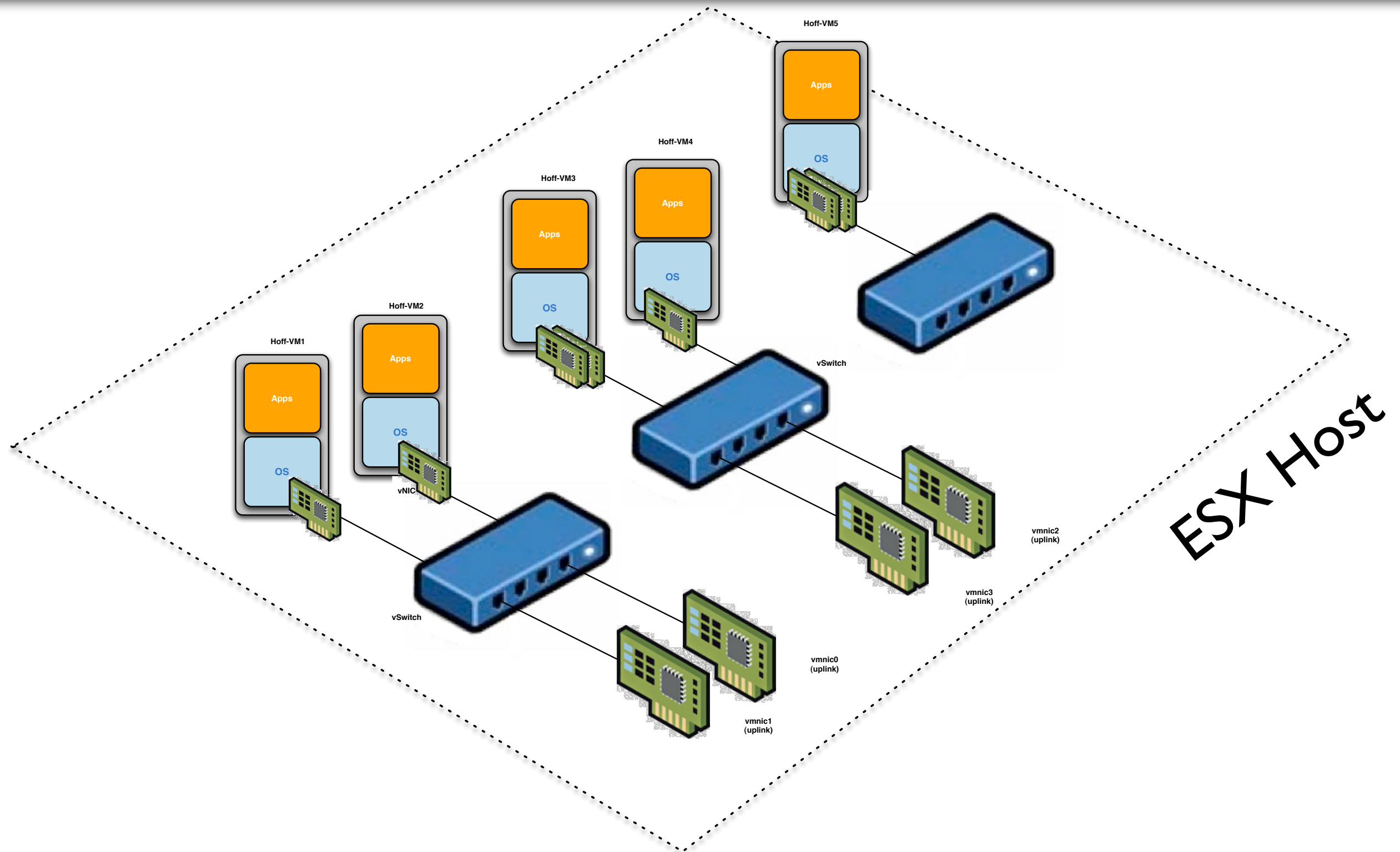


vSwitch Correctness



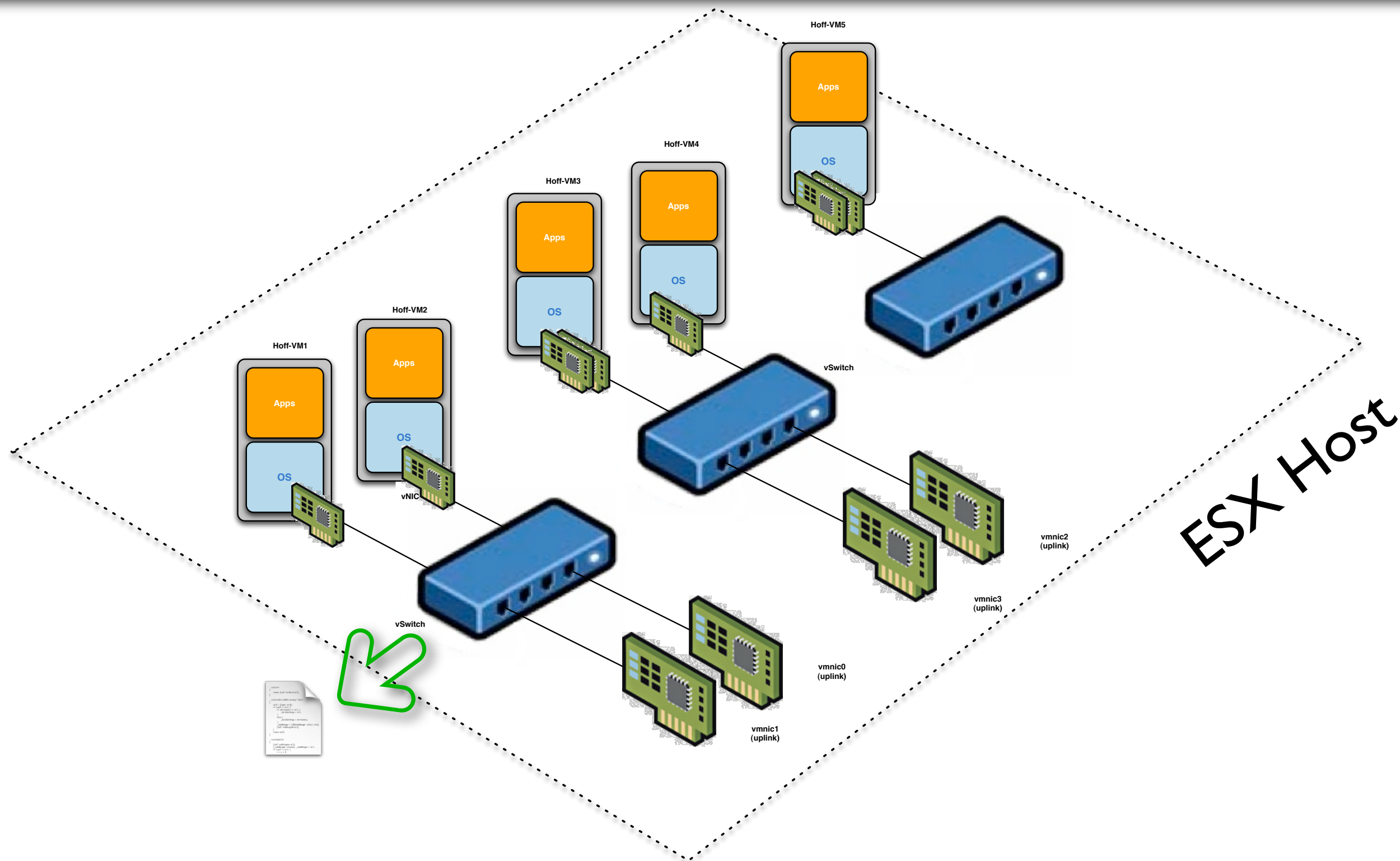


vSwitch Correctness



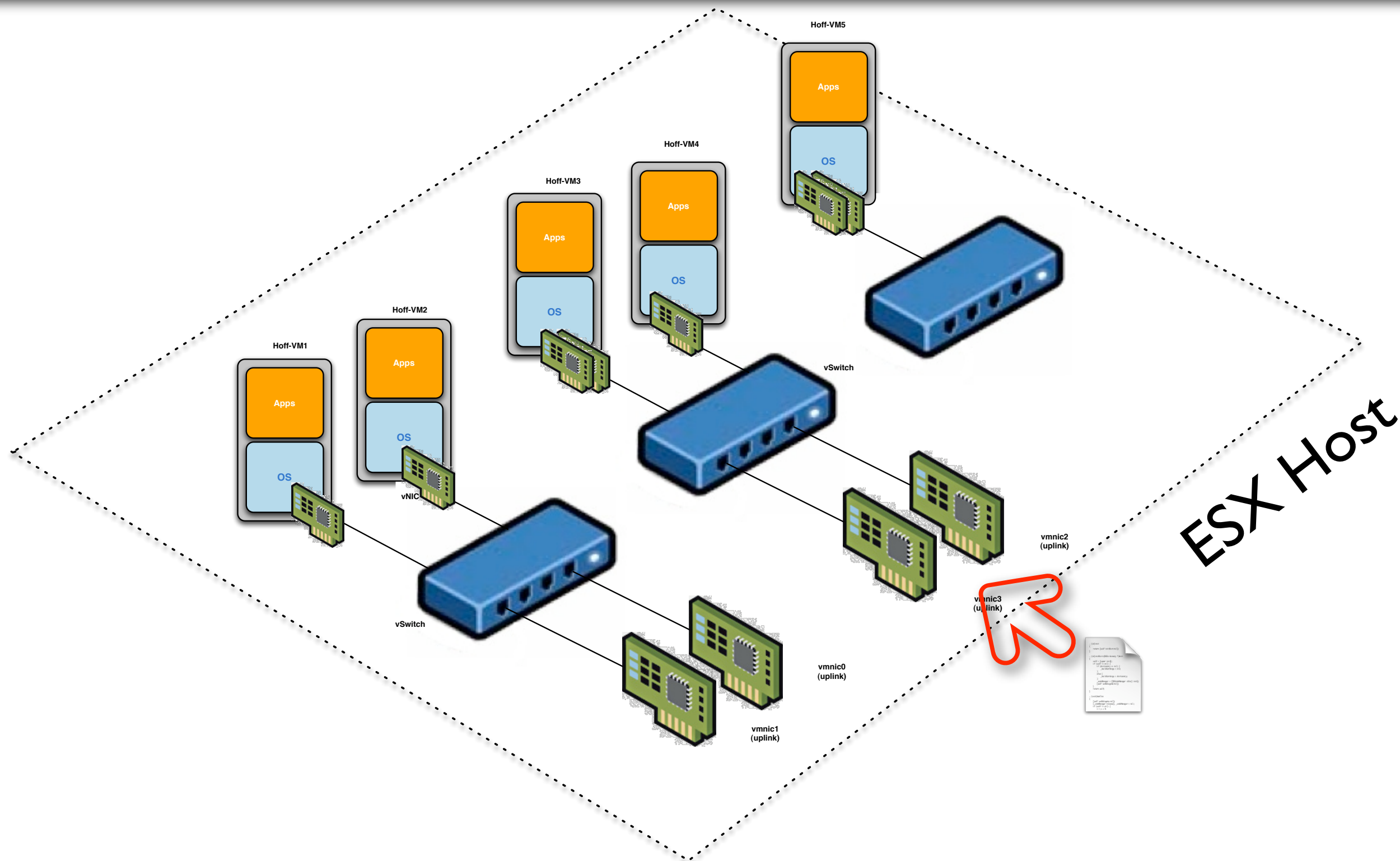


vSwitch Correctness



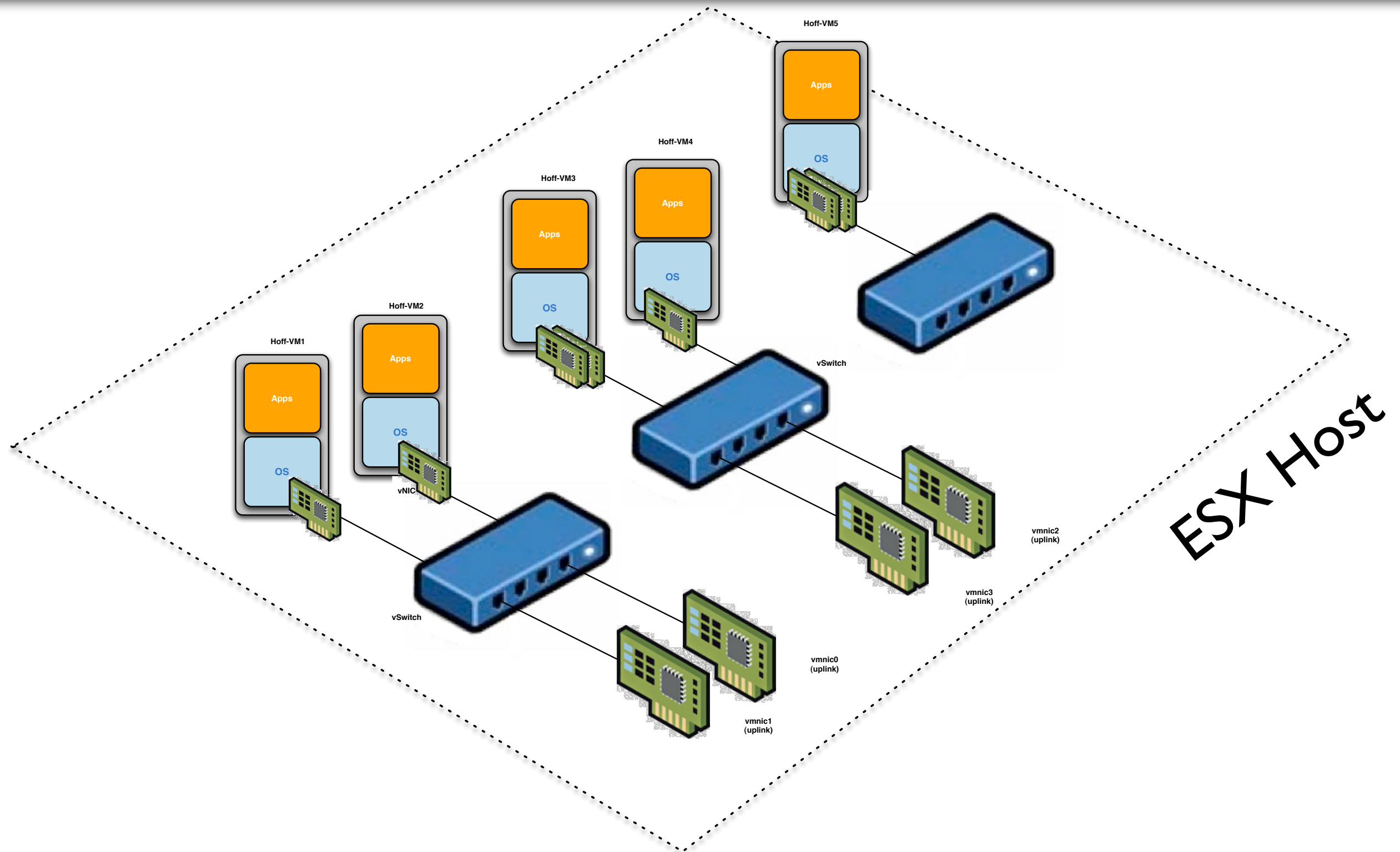


vSwitch Correctness





vSwitch Correctness





Comparing vSwitches to pSwitches

--	--



Comparing vSwitches to pSwitches

Similar

- ❖ It's a basic Layer-2 switch
- ❖ vSwitches maintain MAC forwarding tables & perform frame destination lookup and forwarding
- ❖ vSwitches support VLAN segmentation per port (access/trunk)
- ❖ Supports copying packets to a mirror port via promiscuous mode



Comparing vSwitches to pSwitches

Similar

- ❖ It's a basic Layer-2 switch
- ❖ vSwitches maintain MAC forwarding tables & perform frame destination lookup and forwarding
- ❖ vSwitches support VLAN segmentation per port (access/trunk)
- ❖ Supports copying packets to a mirror port via promiscuous mode

Dissimilar

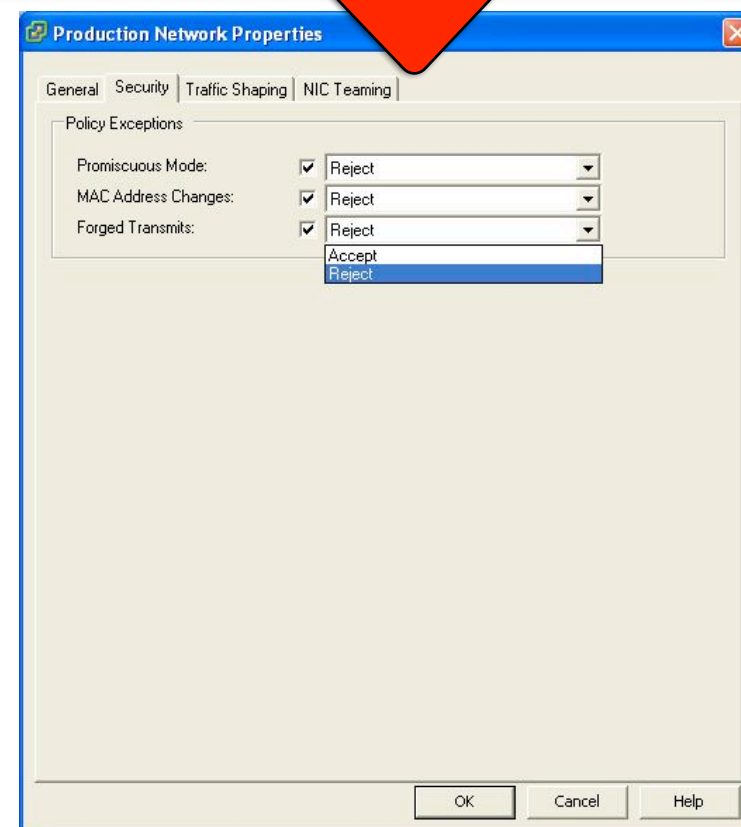
- ❖ Cannot cascade vSwitches
- ❖ vSwitches do not learn from the network to populate forwarding tables; no learning of unicast addresses and no IGMP snooping to learn multicast group membership
- ❖ vSwitches make private copies of frame data used to make forwarding or filtering decisions
- ❖ Frame data is carried outside the frame as it passes through the virtual switch
- ❖ vSwitches have no dynamic trunking protocol support or protocols such as STP and therefore enforce a single-tier network topology



vSwitch Security Options

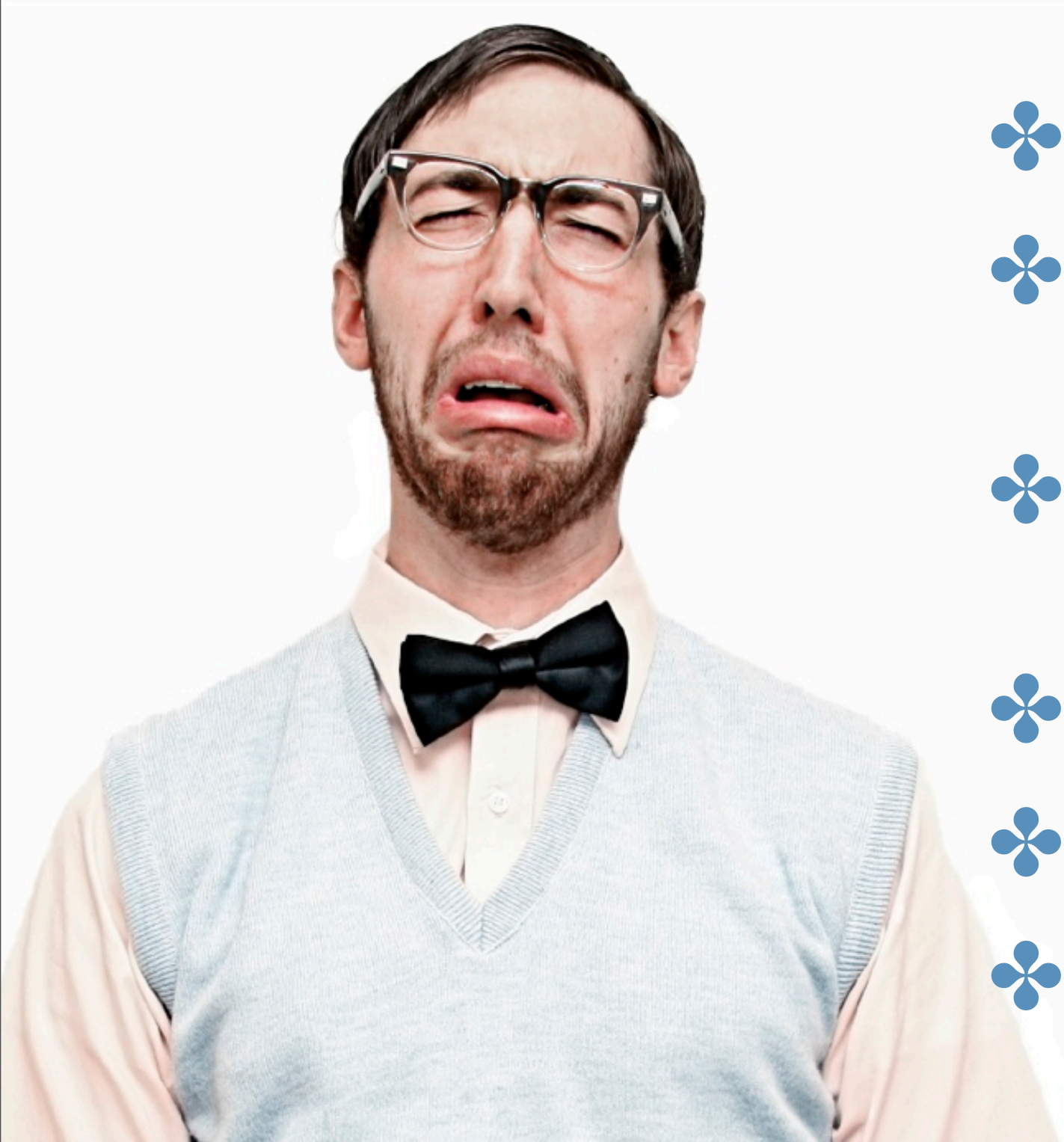
vSwitches offer some nifty security features:

- ❖ 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





You're Making Me All Weepy!



- ❖ Setup & Context
- ❖ x86 Virtualization Overview in 90 Seconds
- ❖ Virtual Networking Architecture
- ❖ **VirtSec Solutions Landscape**
- ❖ The Four Horsemen
- ❖ Wrap-Up



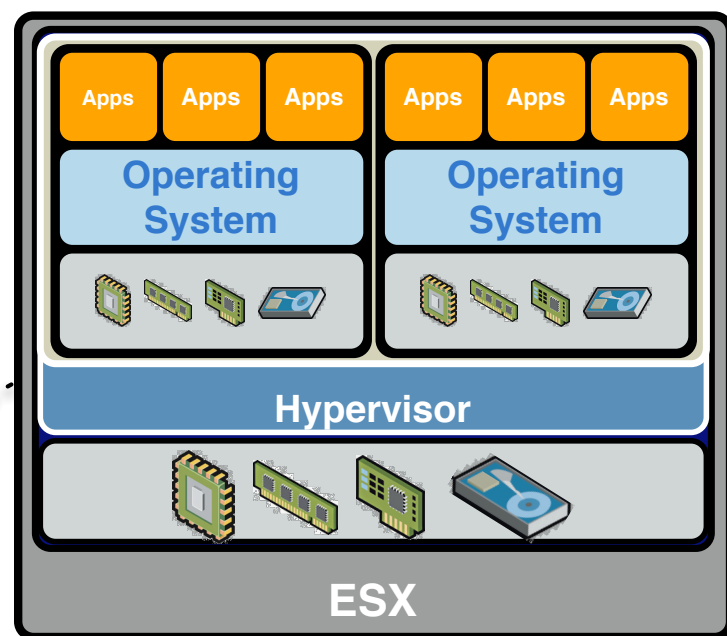
VirtSec Technology Landscape

- ❖ 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

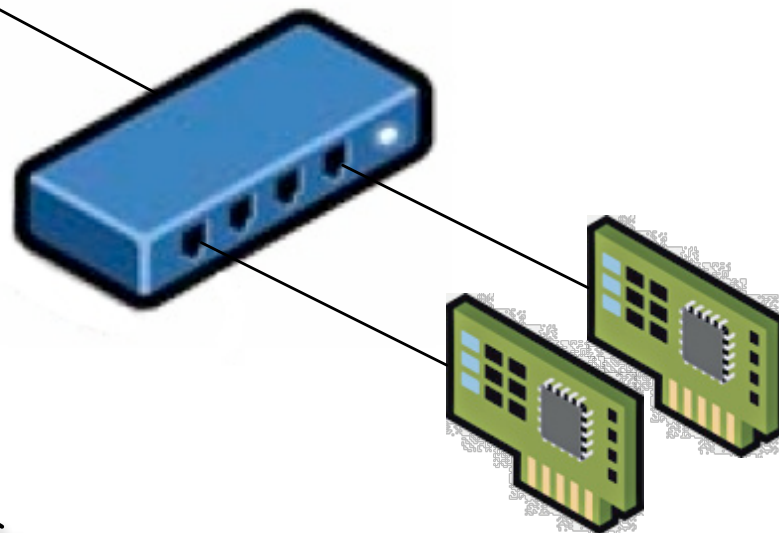




Threat Models

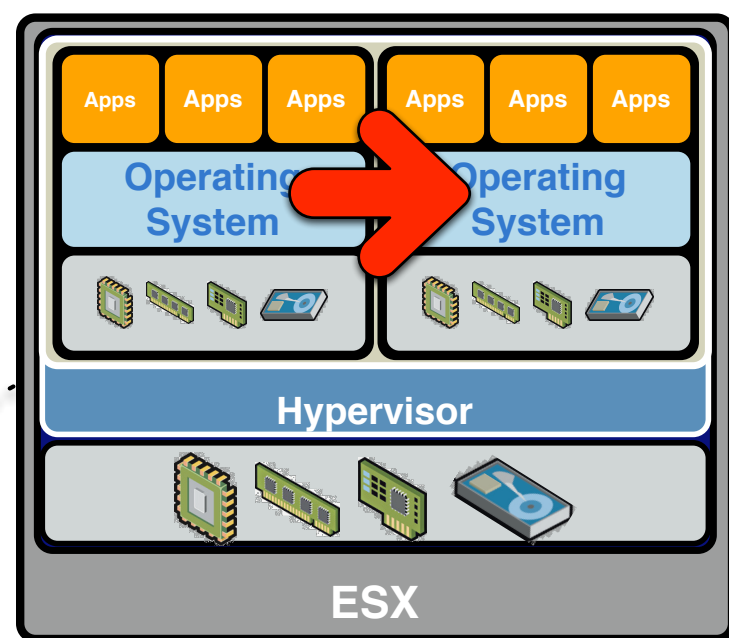


1. Guest to Guest
2. Guest to Host
3. Guest to Self
4. External to Host
5. External to Guest

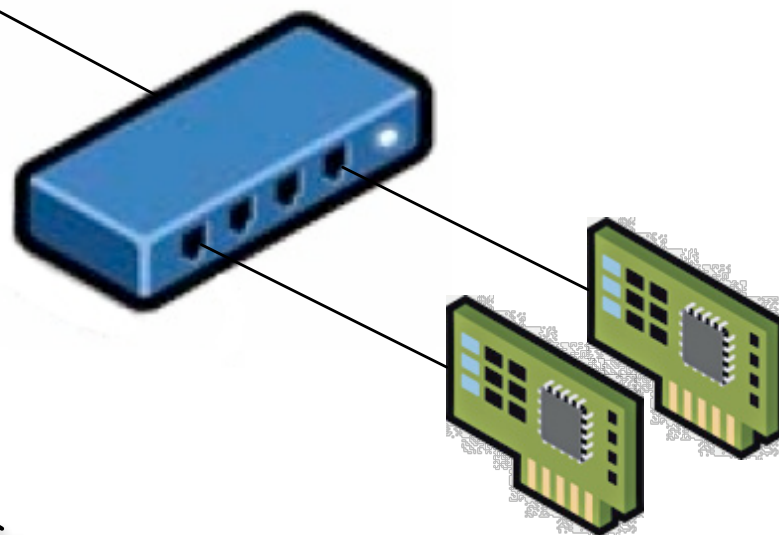




Threat Models In Review

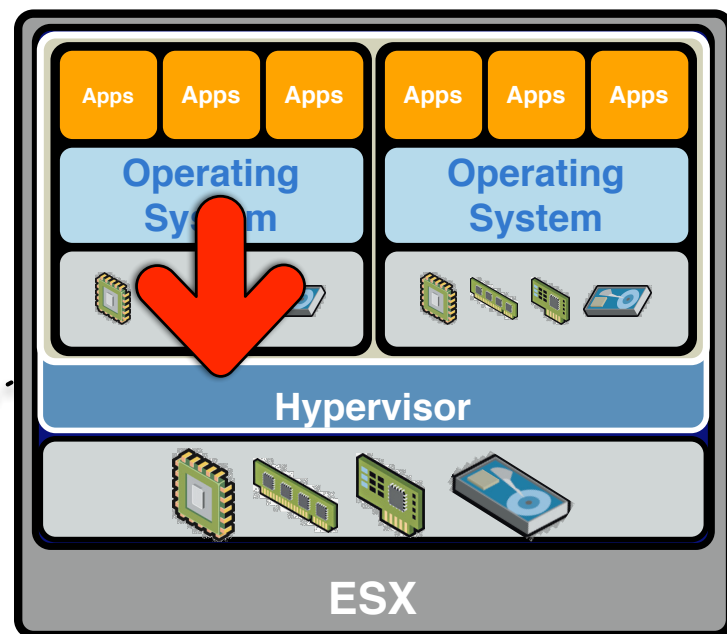


1. Guest to Guest
2. Guest to Host
3. Guest to Self
4. External to Host
5. External to Guest

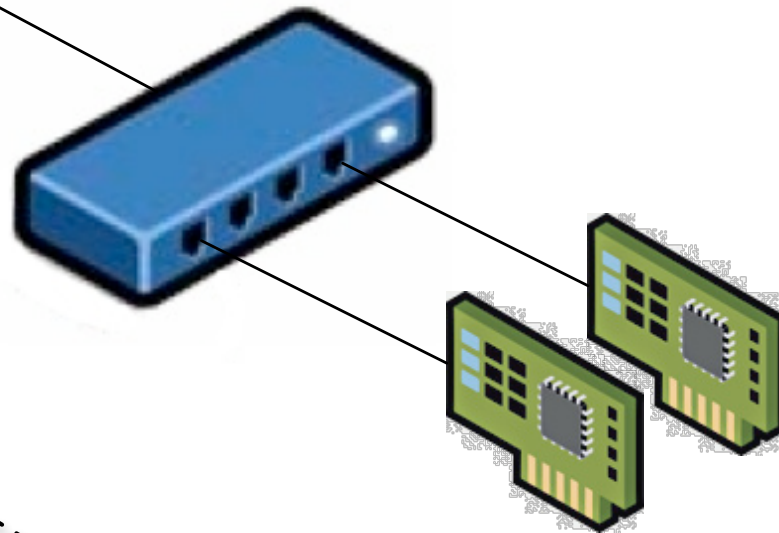




Threat Models

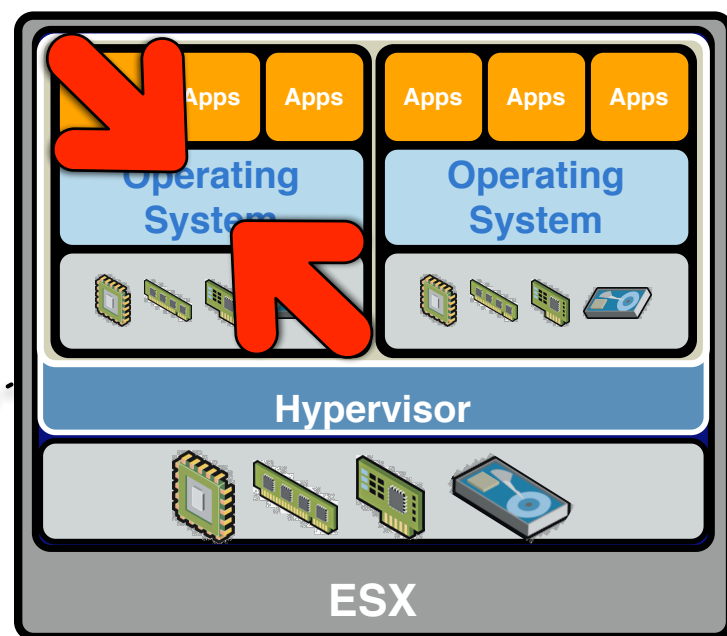


1. Guest to Guest
- 2. Guest to Host**
3. Guest to Self
4. External to Host
5. External to Guest

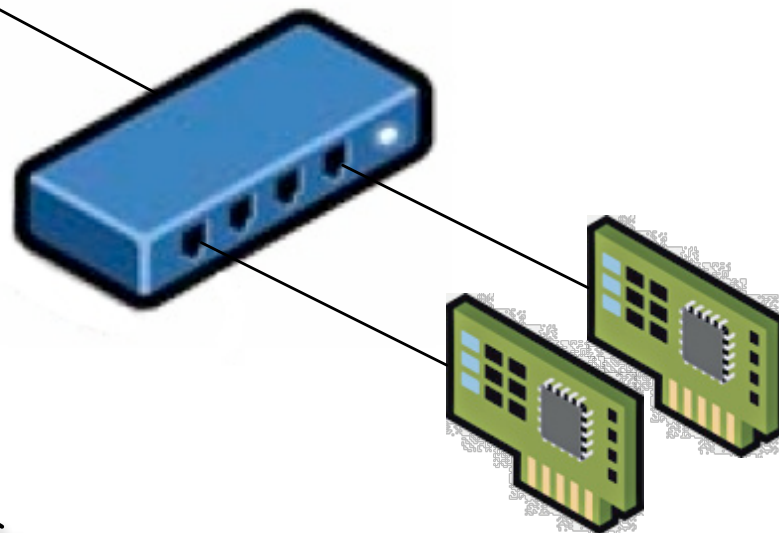




Threat Models

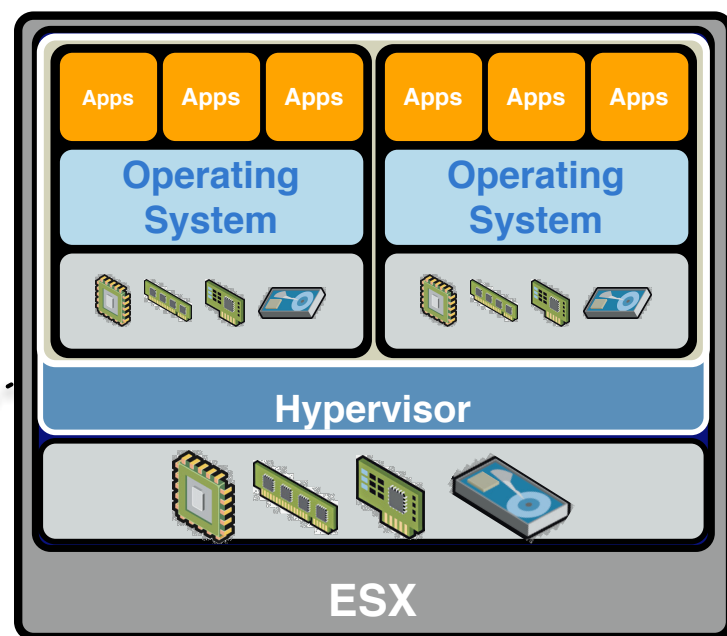


1. Guest to Guest
2. Guest to Host
- 3. Guest to Self**
4. External to Host
5. External to Guest

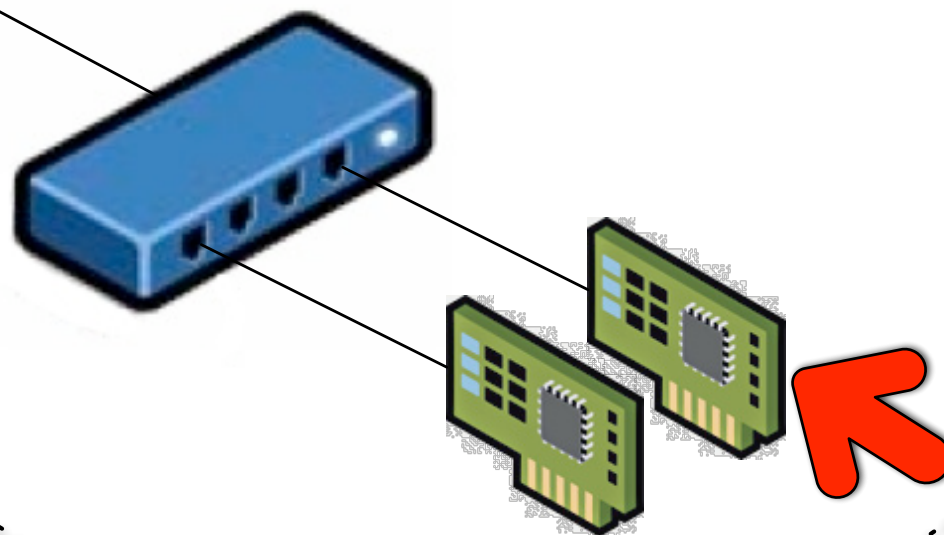




Threat Models

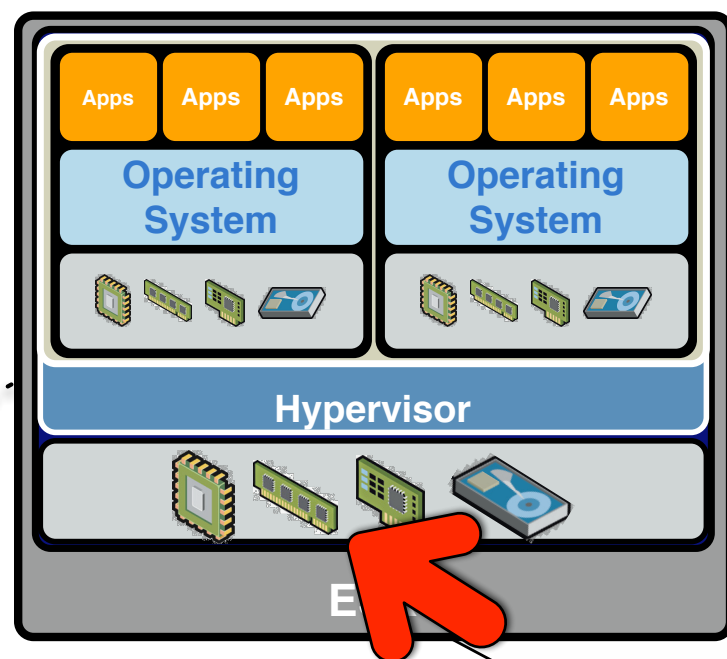


1. Guest to Guest
2. Guest to Host
3. Guest to Self
- 4. External to Host**
5. External to Guest

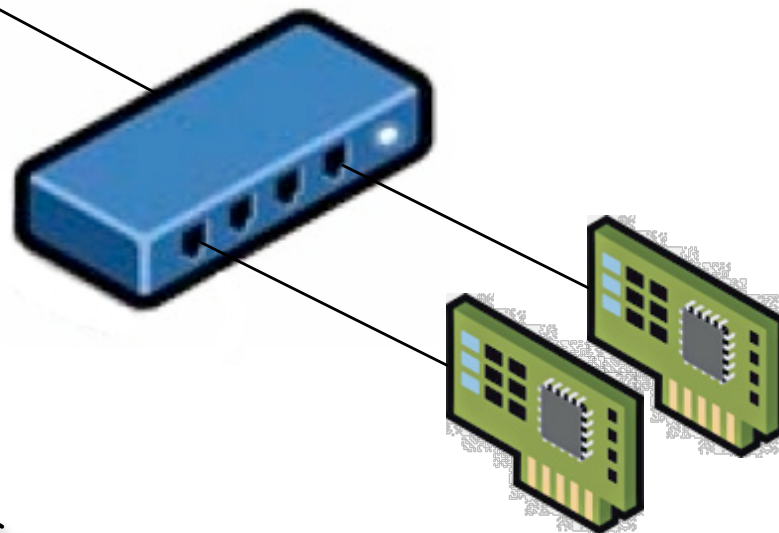




Threat Models

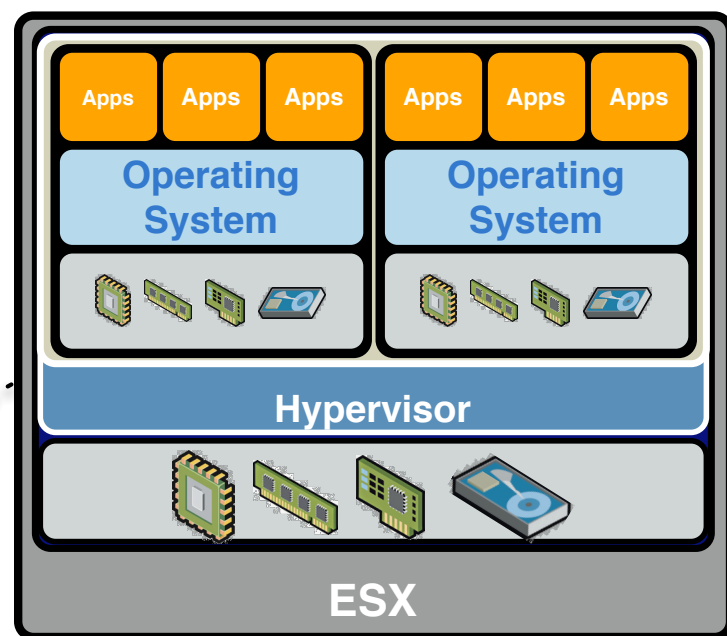


1. Guest to Guest
2. Guest to Host
3. Guest to Self
- 4. External to Host**
5. External to Guest

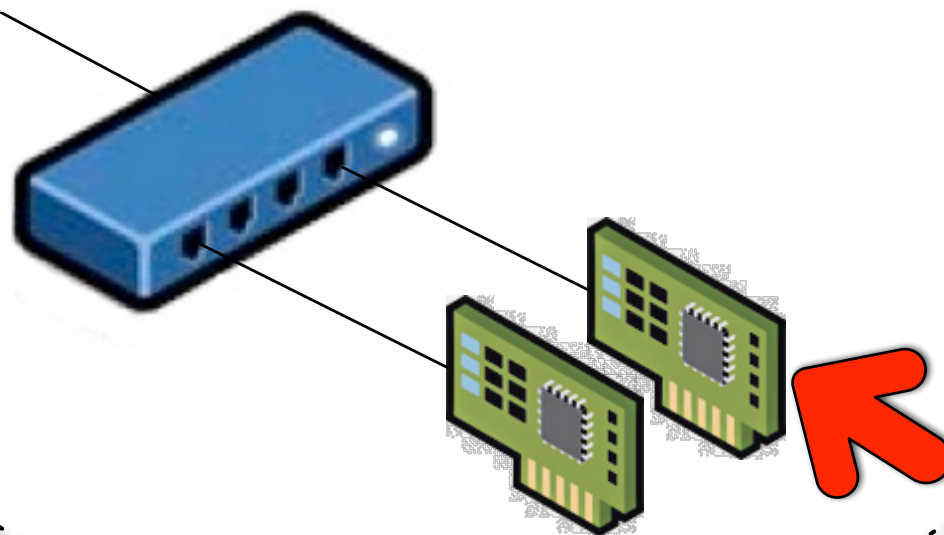




Threat Models

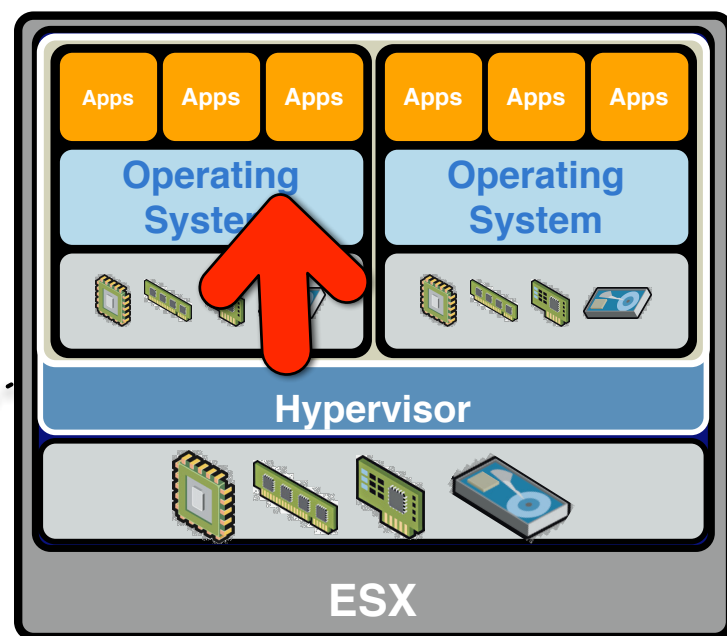


1. Guest to Guest
2. Guest to Host
3. Guest to Self
4. External to Host
- 5. External to Guest**

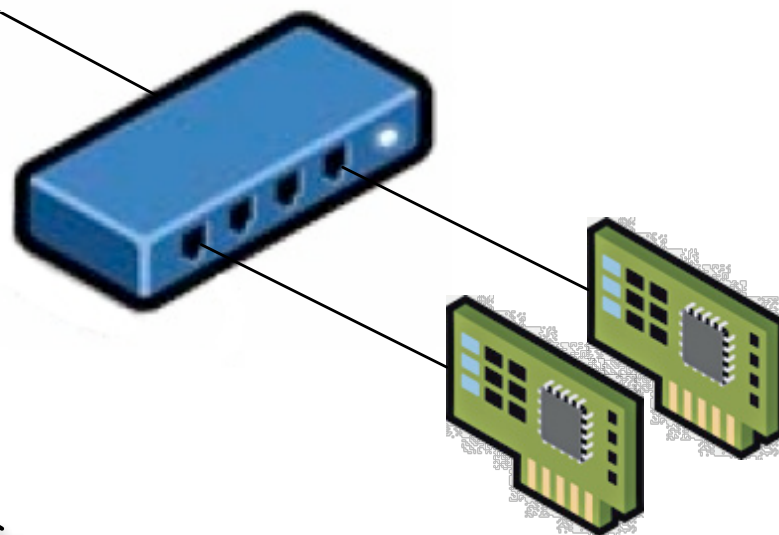




Threat Models

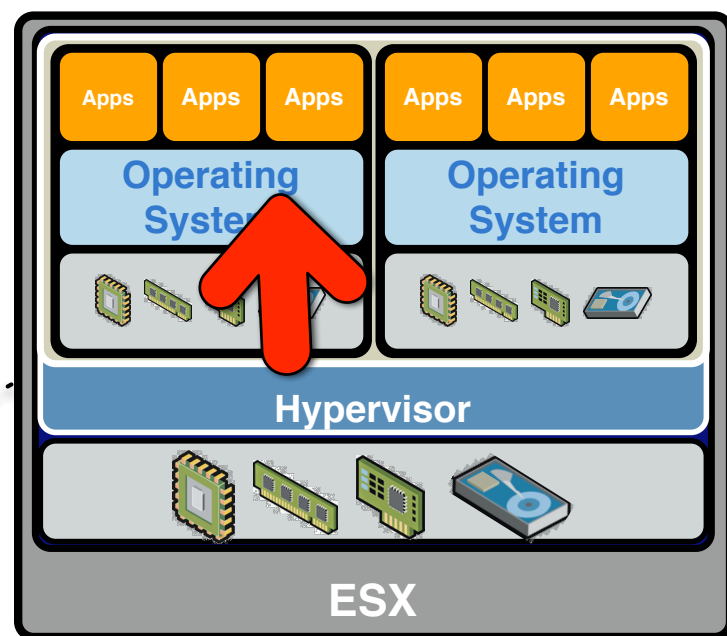


1. Guest to Guest
2. Guest to Host
3. Guest to Self
4. External to Host
- 5. External to Guest**

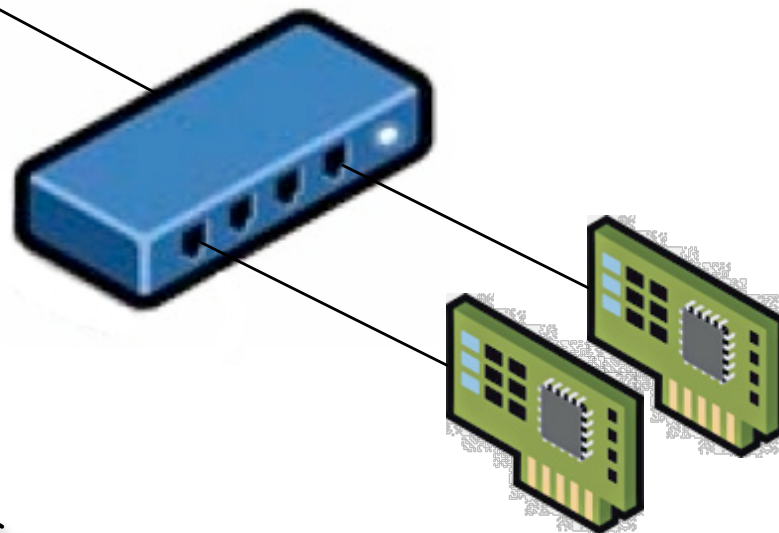




Threat Models



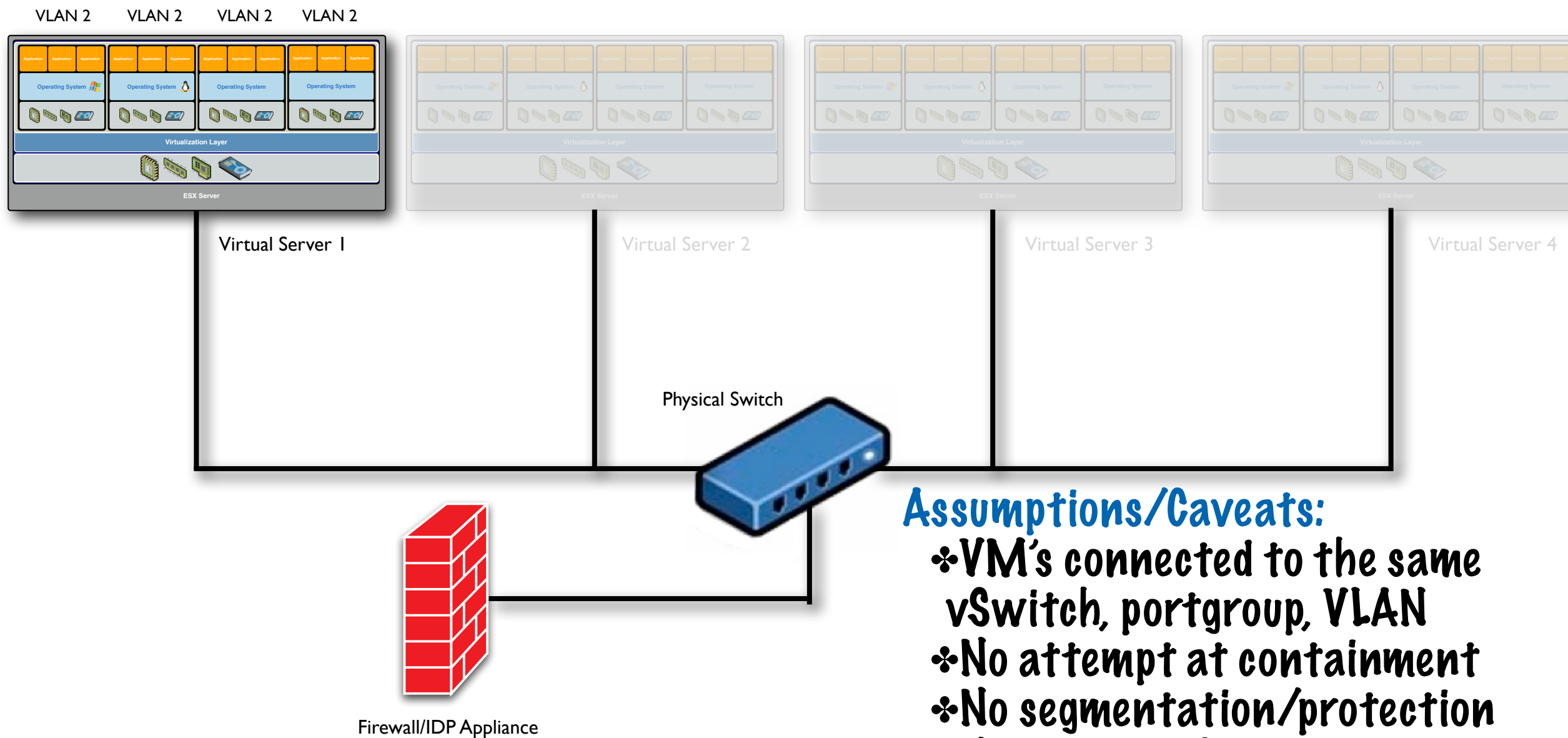
1. Guest to Guest
2. Guest to Host
3. Guest to Self
4. External to Host
- 5. External to Guest**





VirtSec Examples: No Controls (?)

No Security



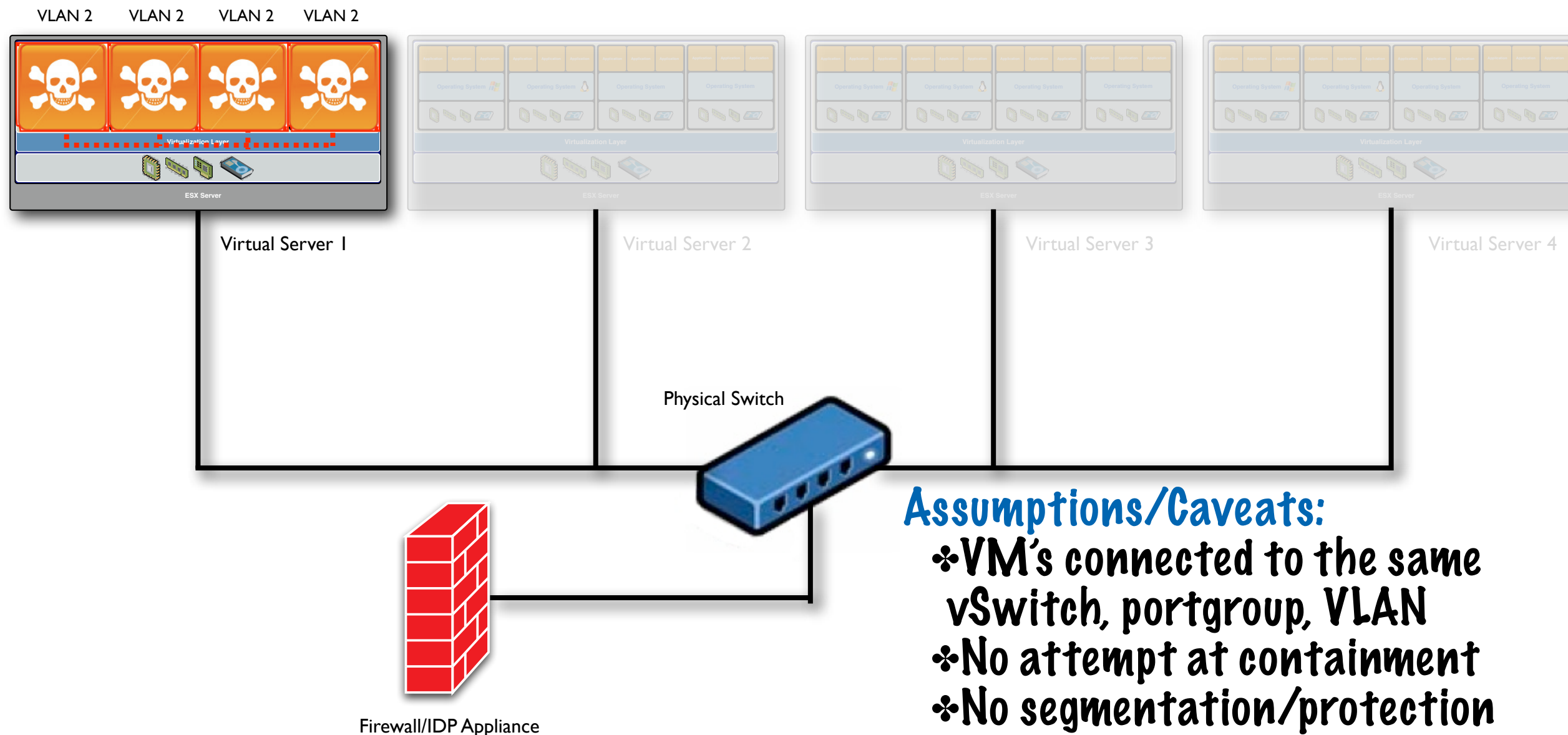
Assumptions/Caveats:

- ❖ VM's connected to the same vSwitch, portgroup, VLAN
- ❖ No attempt at containment
- ❖ No segmentation/protection
- ❖ Not very realistic...



VirtSec Examples: No Controls (?)

No Security

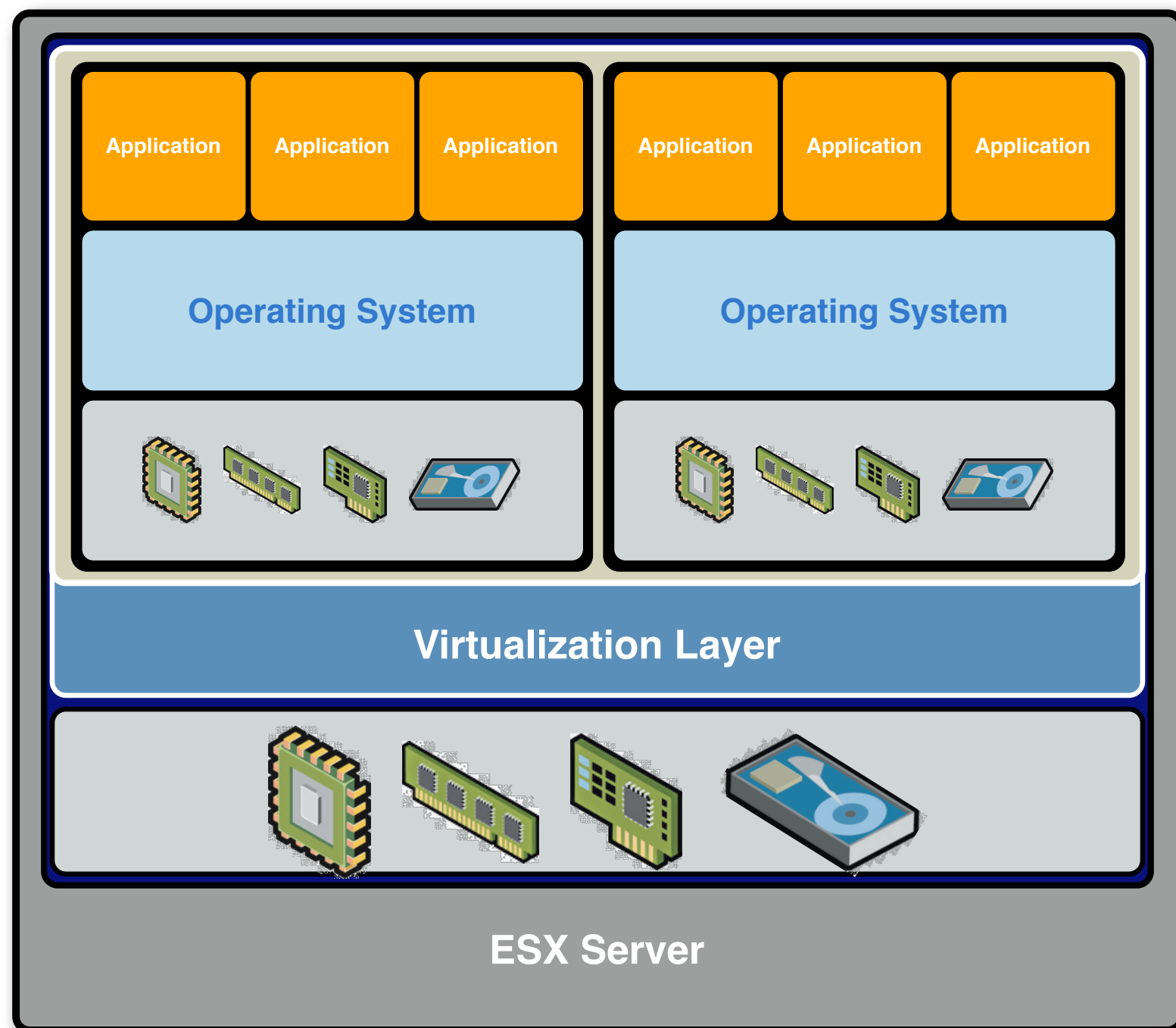


Assumptions/Caveats:

- ❖ VM's connected to the same vSwitch, portgroup, VLAN
- ❖ No attempt at containment
- ❖ No segmentation/protection
- ❖ Not very realistic...



VirtSec Examples: Software On 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
- ❖ Insert product here

McAfee®

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

symantec.

CISCO

tripwire

Configuresoft

BIG FIX

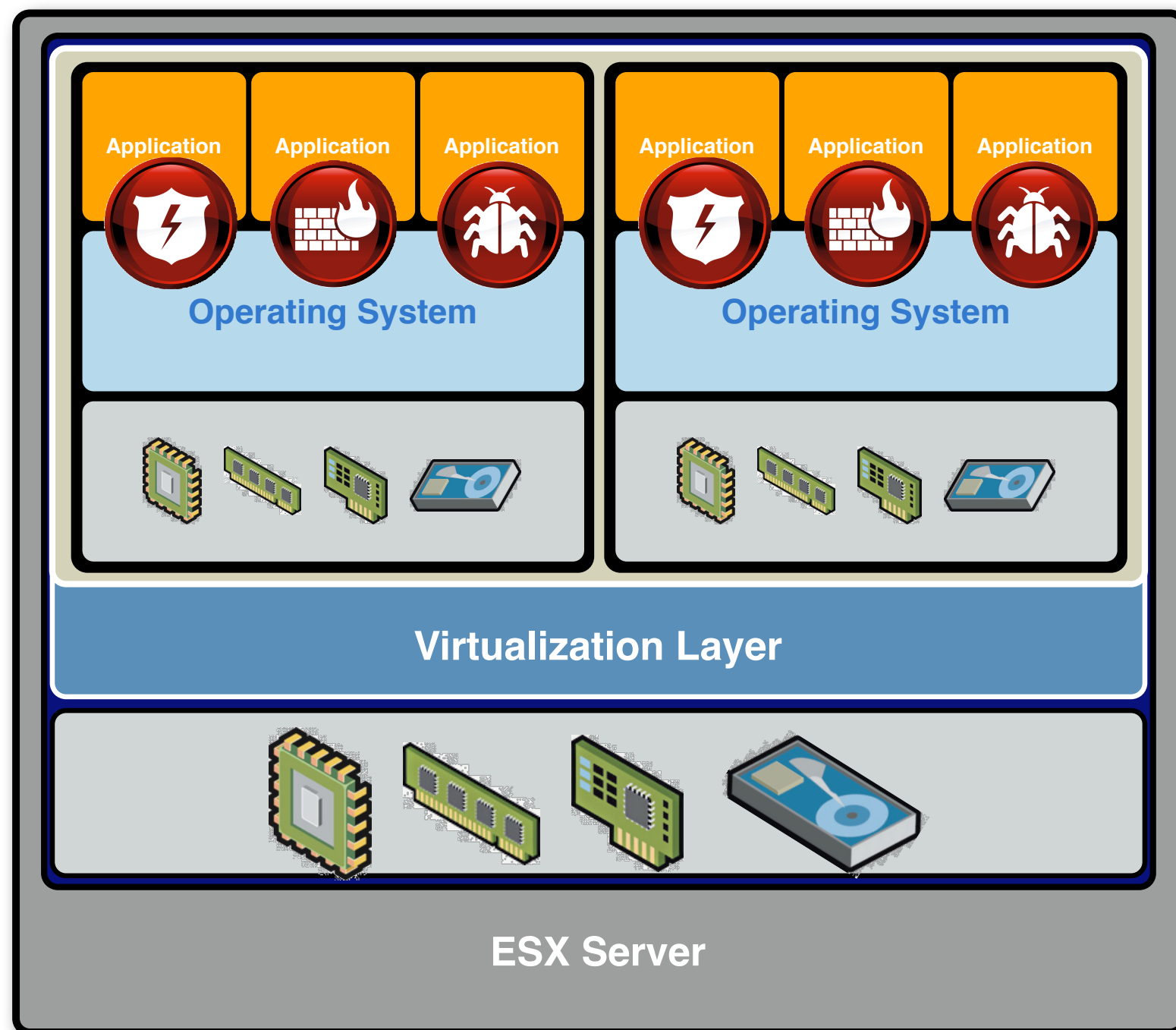
TREND
MICRO

netIQ

Microsoft



VirtSec Examples: Software On 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
- ❖ Insert product here

McAfee®

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

symantec.

CISCO

tripwire

Configuresoft

BIG FIX

TREND
MICRO

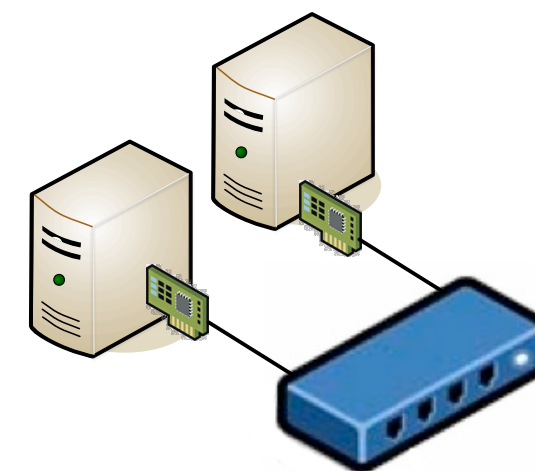
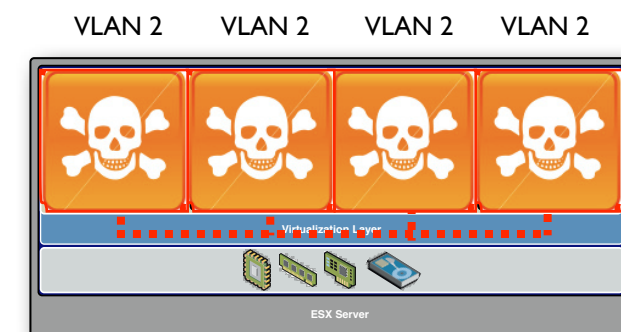
netIQ

Microsoft



Reality Check: The Intra-VM (In)Security Myth

Virtualized



Real World

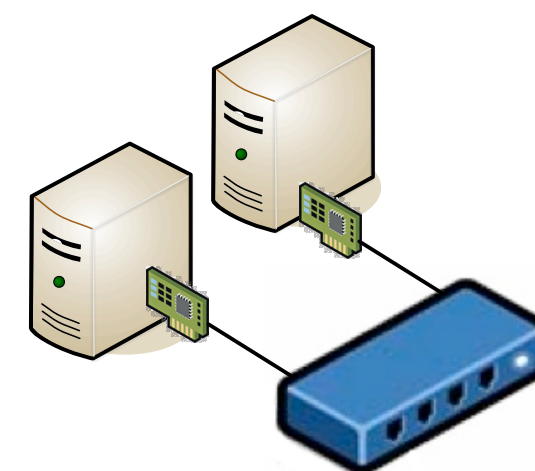
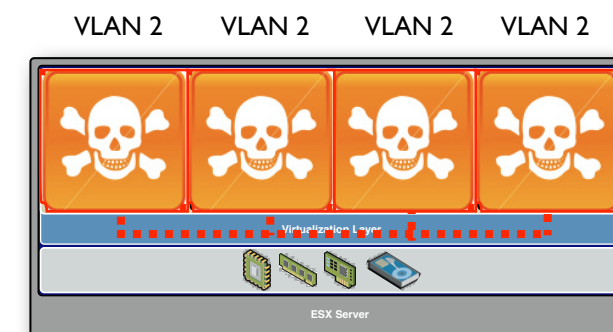


Reality Check: The Intra-VM (In)Security Myth

Myth/Security Team Says:

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

Virtualized



Real World



Reality Check: The Intra-VM (In)Security Myth

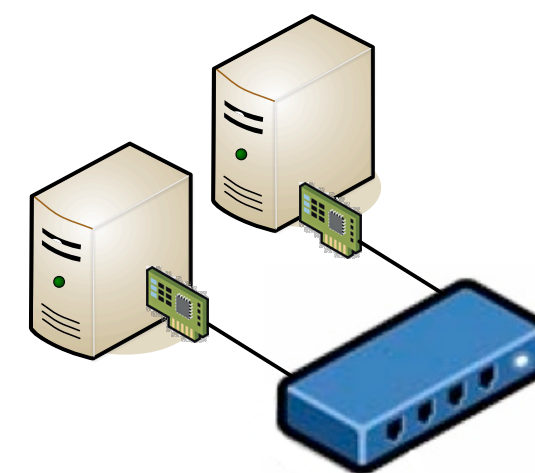
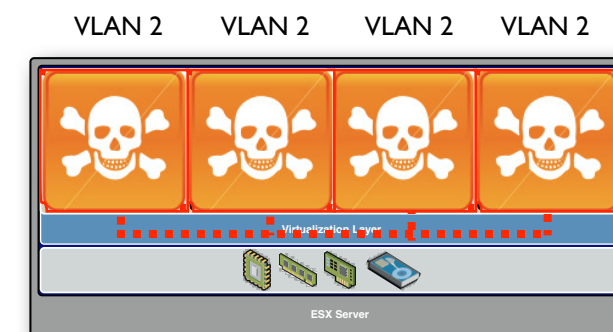
Myth/Security Team Says:

- ❖ “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?”

Virtualized



Real World



Reality Check: The Intra-VM (In)Security Myth

Myth/Security Team Says:

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

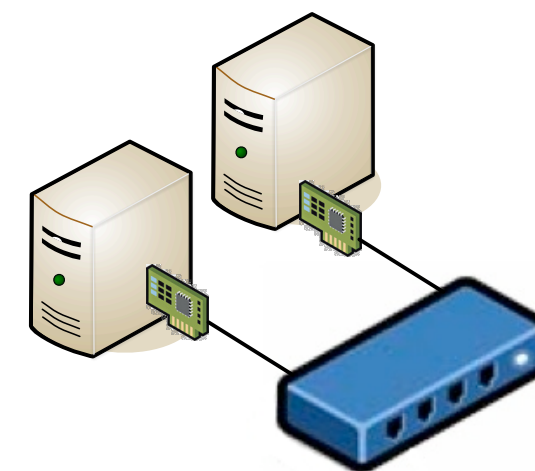
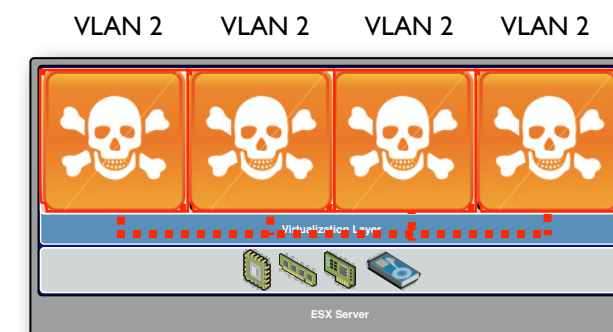
Reality/I ask:

- ❖ “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...”

Virtualized



Real World



Doh!



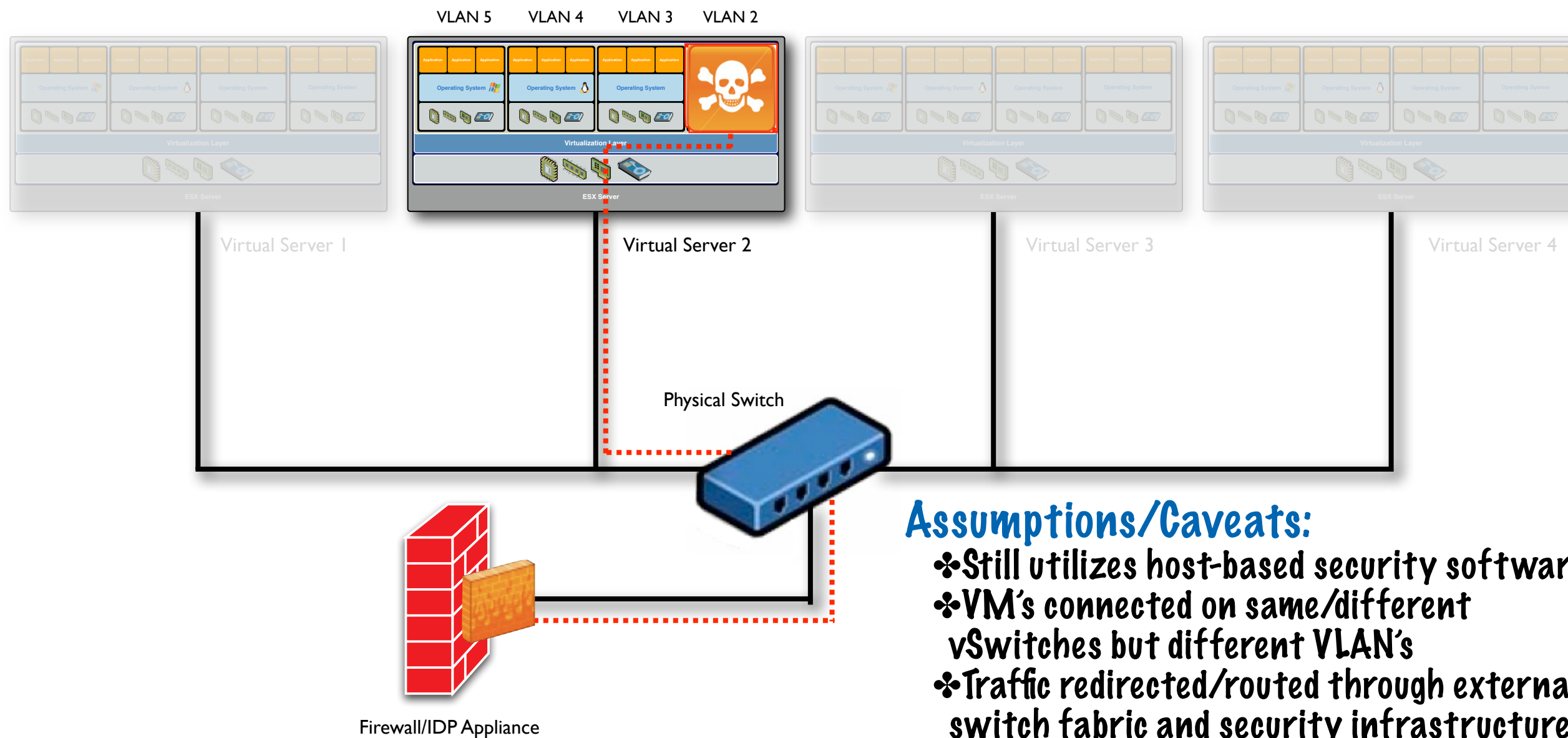


- ❖ Still utilizes host-based security software
- ❖ VM's connected on same/different vSwitches but different VLAN's
- ❖ Traffic redirected/routed through external switch fabric and security infrastructure



VirtSec Examples: Interacting with External Security

External Security



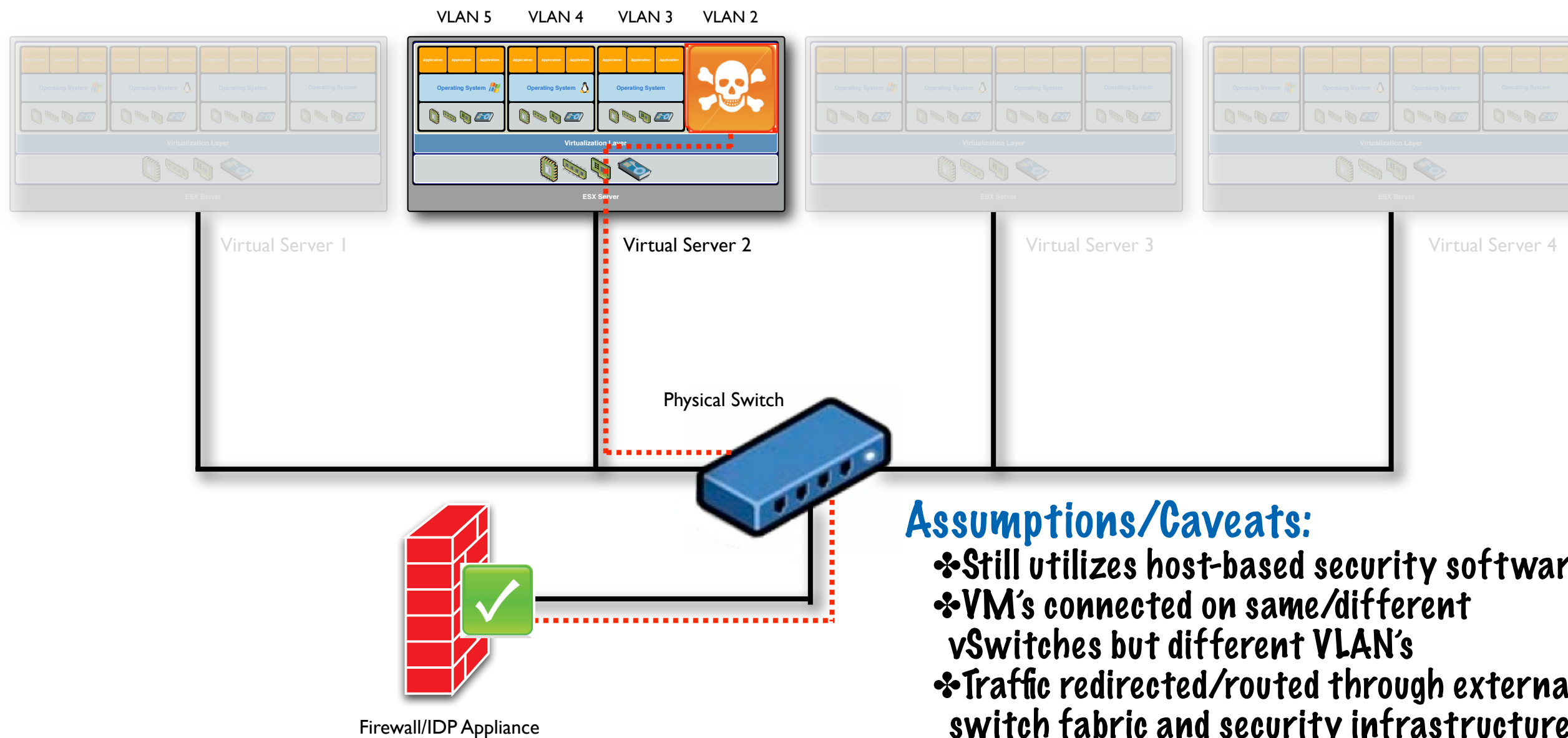
Assumptions/Caveats:

- ❖ 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



VirtSec Examples: Interacting with External Security

External Security



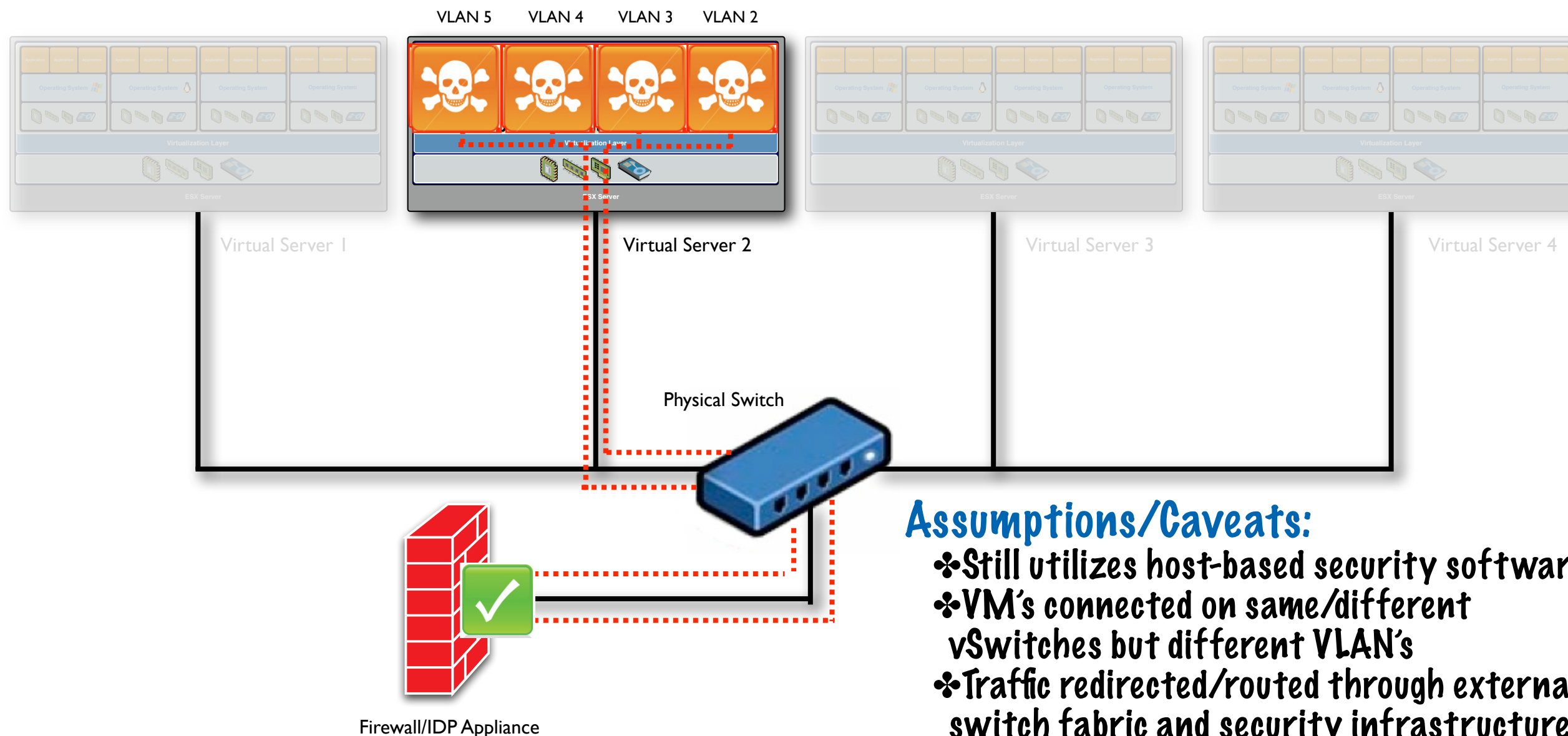
Assumptions/Caveats:

- ❖ 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



VirtSec Examples: Interacting with External Security

External Security

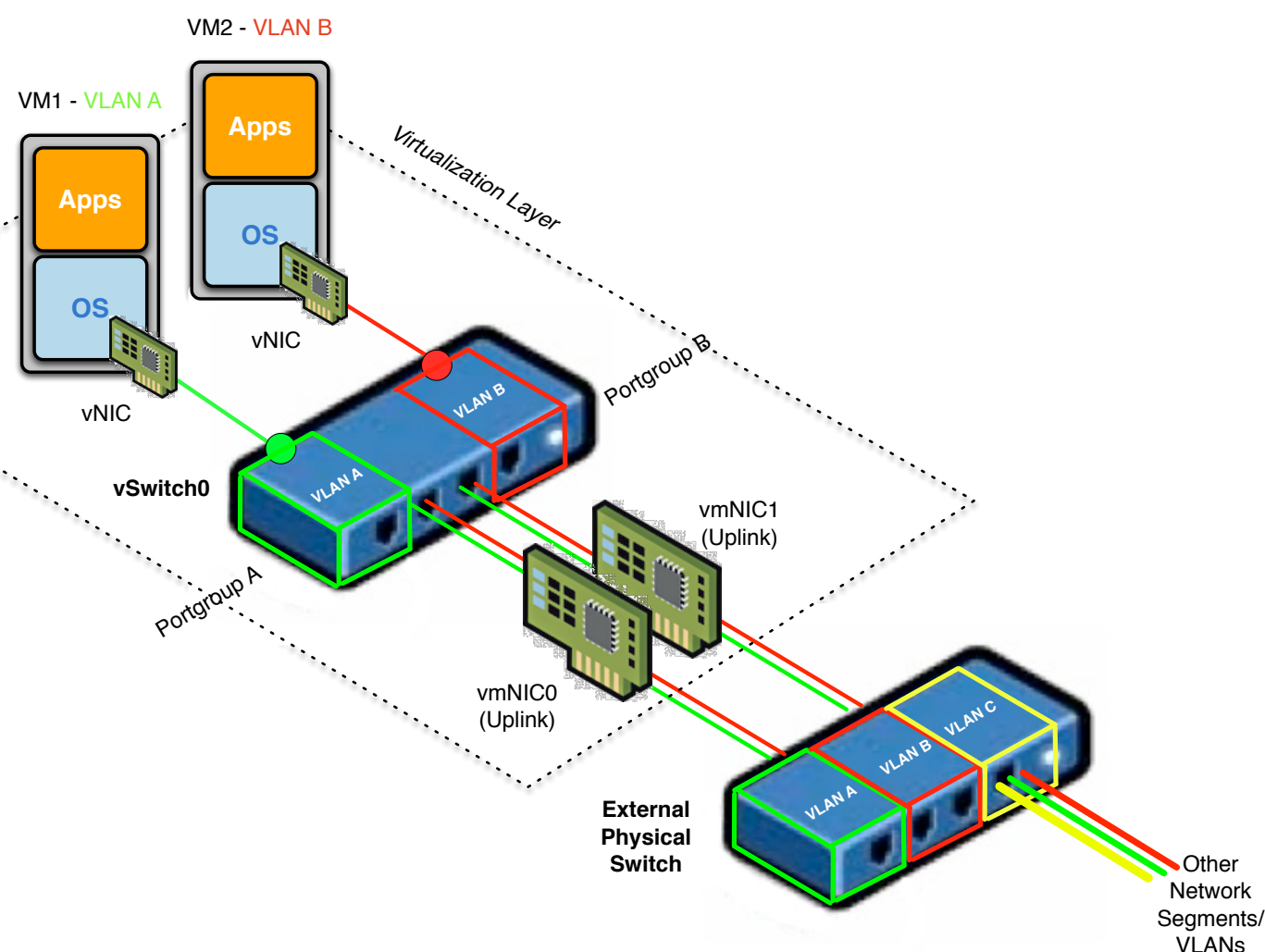


Assumptions/Caveats:

- ❖ 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



Virtual Appliances: The Devil's In the Details

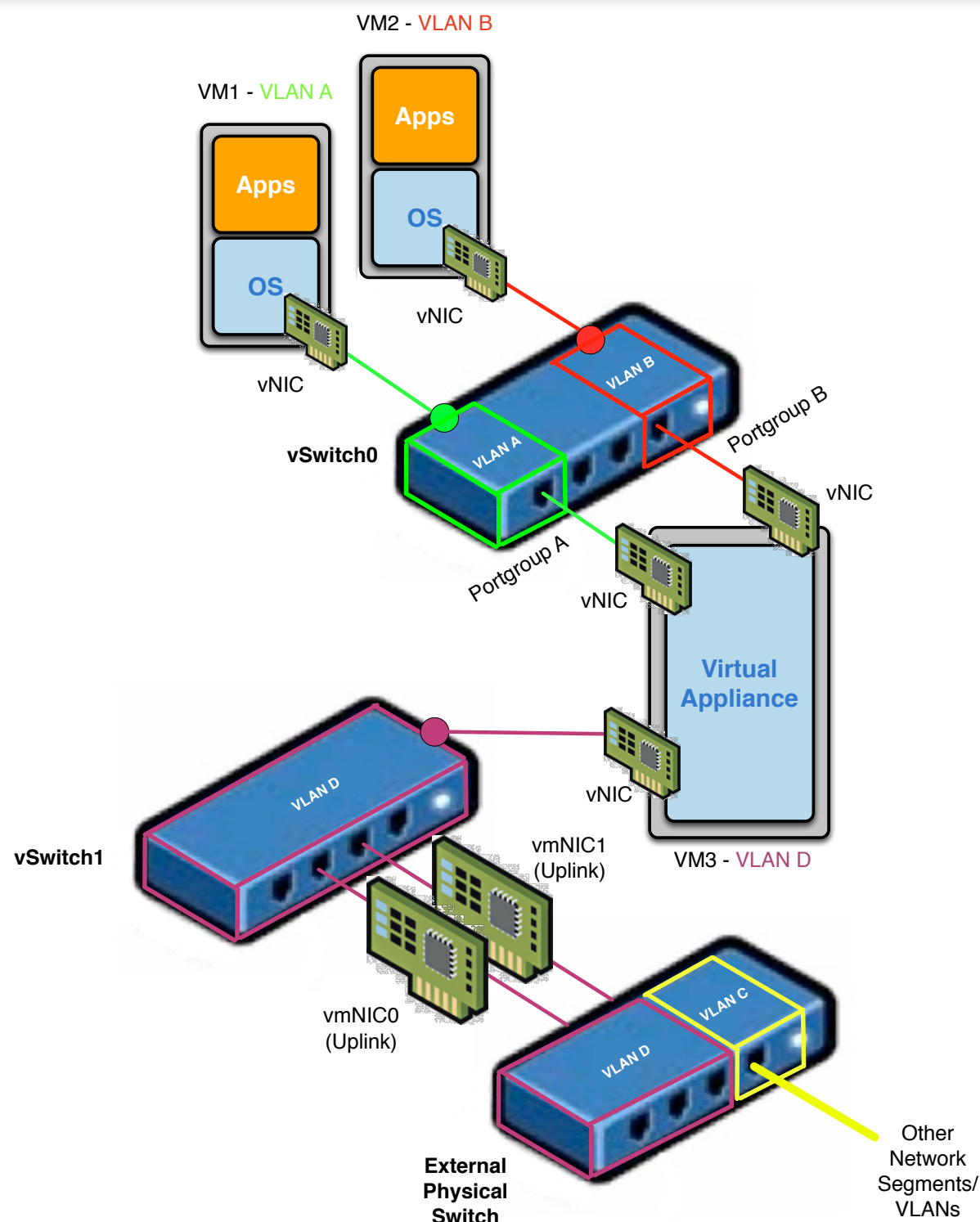


Here we have a basic multi-VM configuration without a virtual security appliance:

- ❖ 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

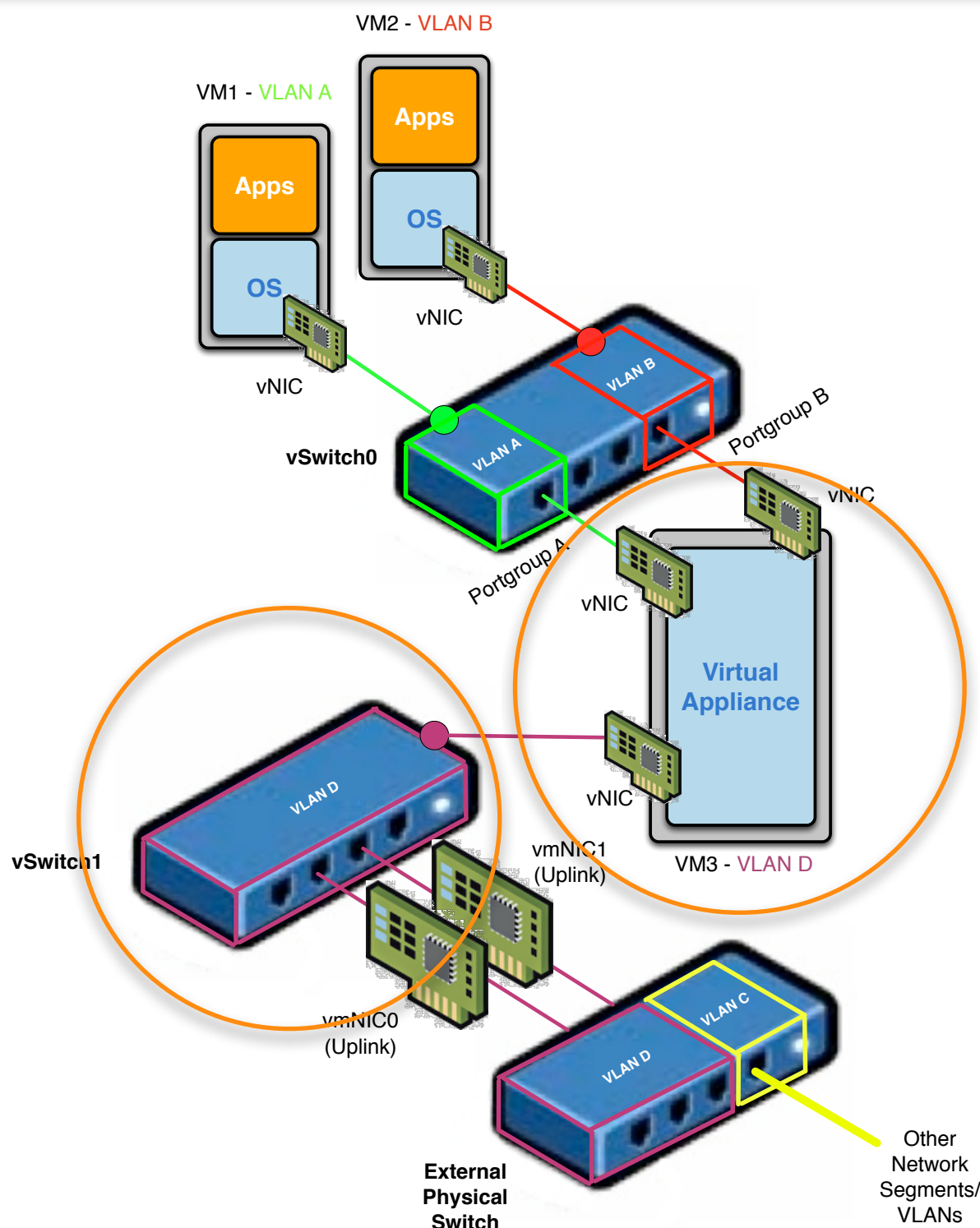


The Revised Configuration:

- ❖ 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 it's 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



Virtual Appliances: The Devil's In the Details

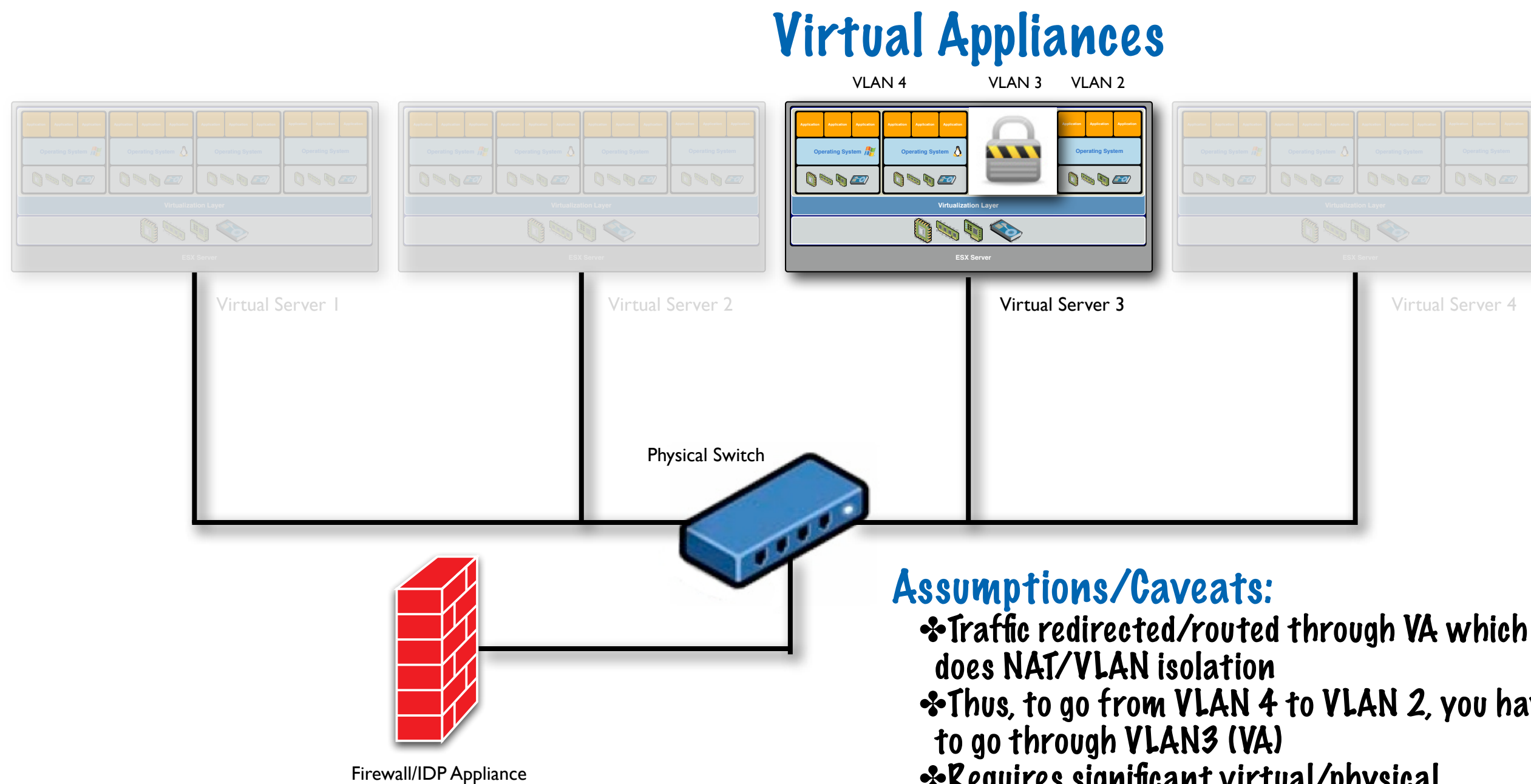


The Revised Configuration:

- ❖ 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 it's 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



VirtSec Examples: Virtual Appliance w/External Security Interaction & VM to VM On Different VLAN/vSwitch

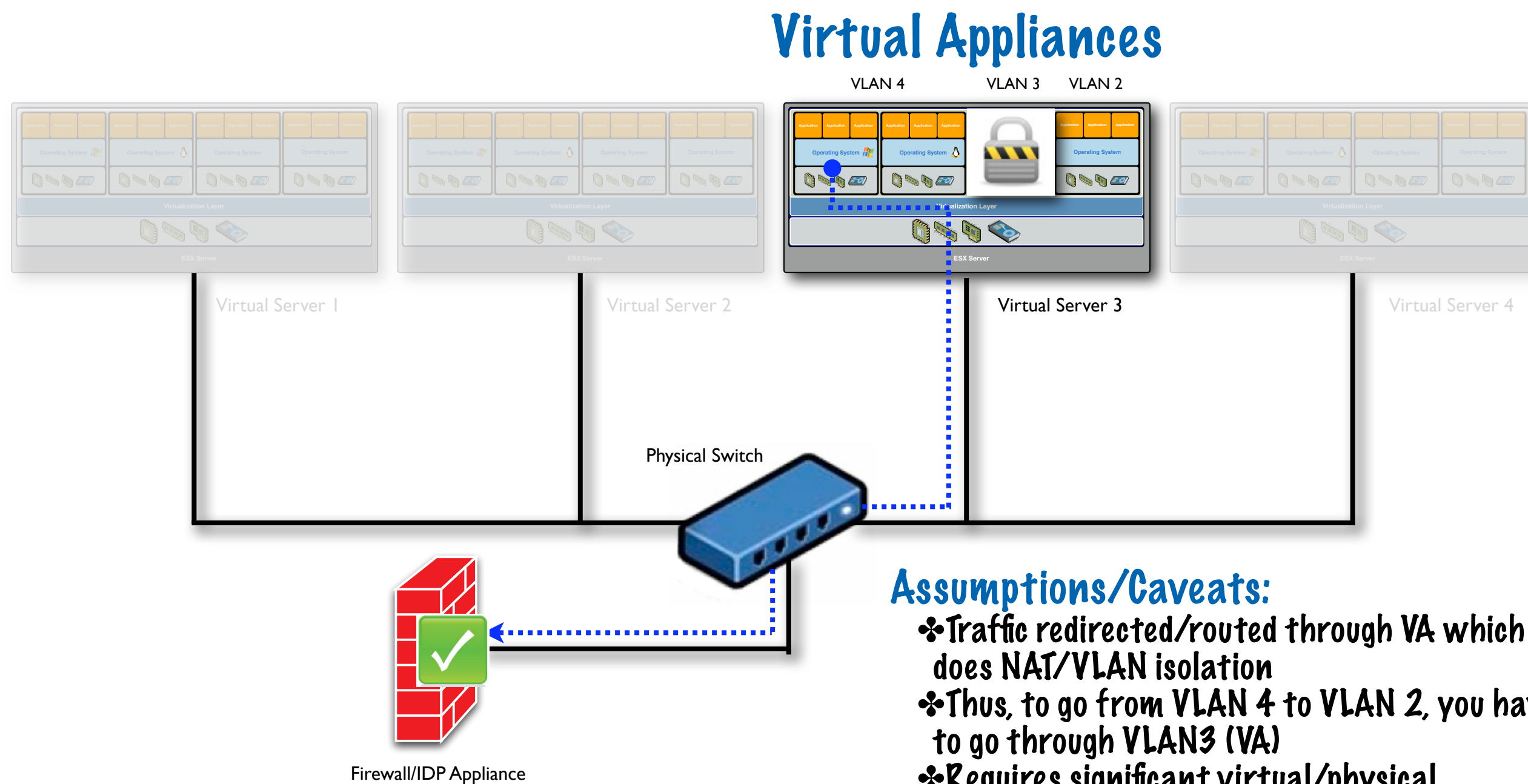


Assumptions/Caveats:

- ❖ Traffic redirected/routed through VA which does NAT/VLAN isolation
- ❖ Thus, to go from VLAN 4 to VLAN 2, you have to go through VLAN 3 (VA)
- ❖ Requires significant virtual/physical networking reconfiguration



VirtSec Examples: Virtual Appliance w/External Security Interaction & VM to VM On Different VLAN/vSwitch

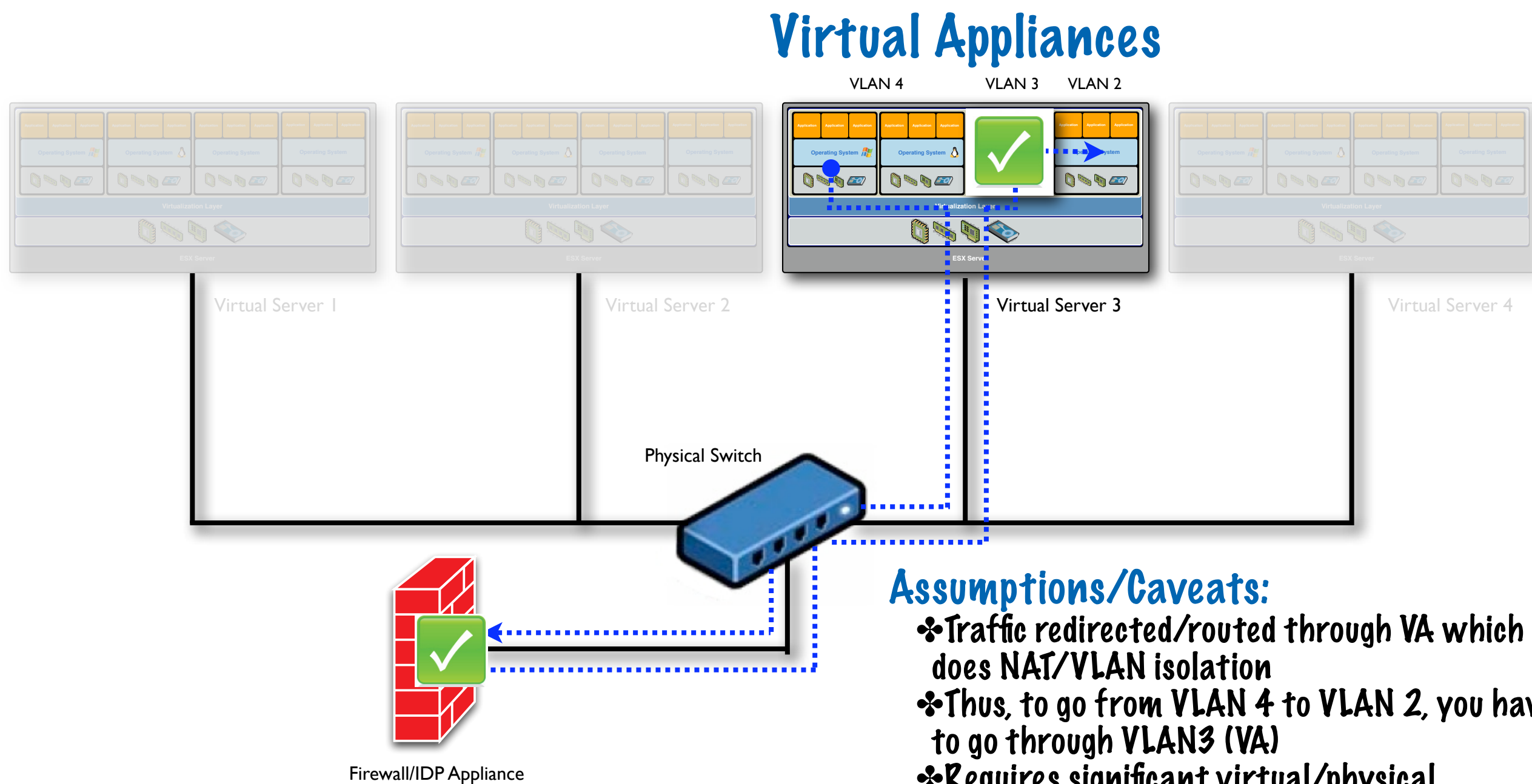


Assumptions/Caveats:

- ❖ Traffic redirected/routed through VA which does NAT/VLAN isolation
- ❖ Thus, to go from VLAN 4 to VLAN 2, you have to go through VLAN 3 (VA)
- ❖ Requires significant virtual/physical networking reconfiguration



VirtSec Examples: Virtual Appliance w/External Security Interaction & VM to VM On Different VLAN/vSwitch

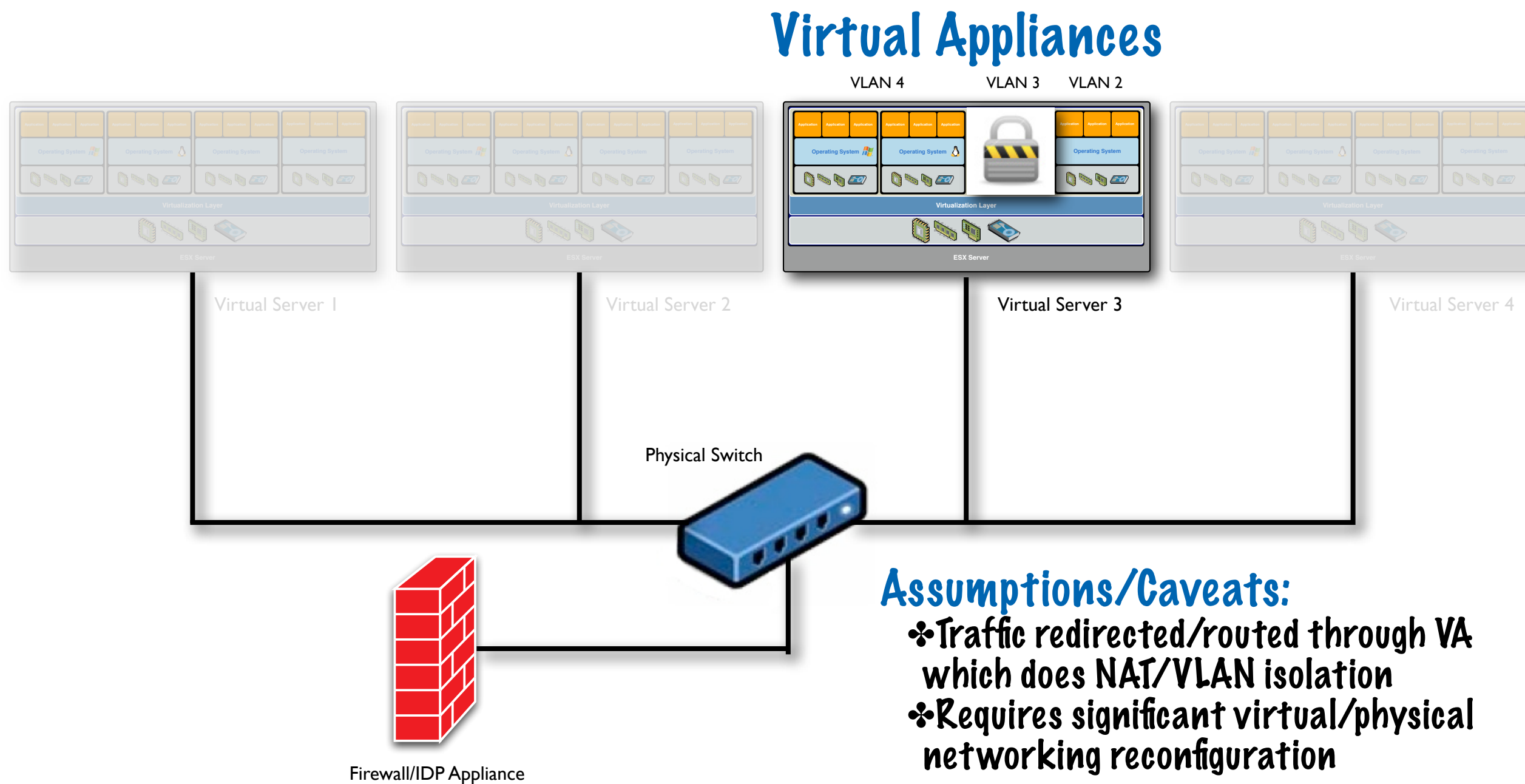


Assumptions/Caveats:

- ❖ Traffic redirected/routed through VA which does NAT/VLAN isolation
- ❖ Thus, to go from VLAN 4 to VLAN 2, you have to go through VLAN 3 (VA)
- ❖ Requires significant virtual/physical networking reconfiguration

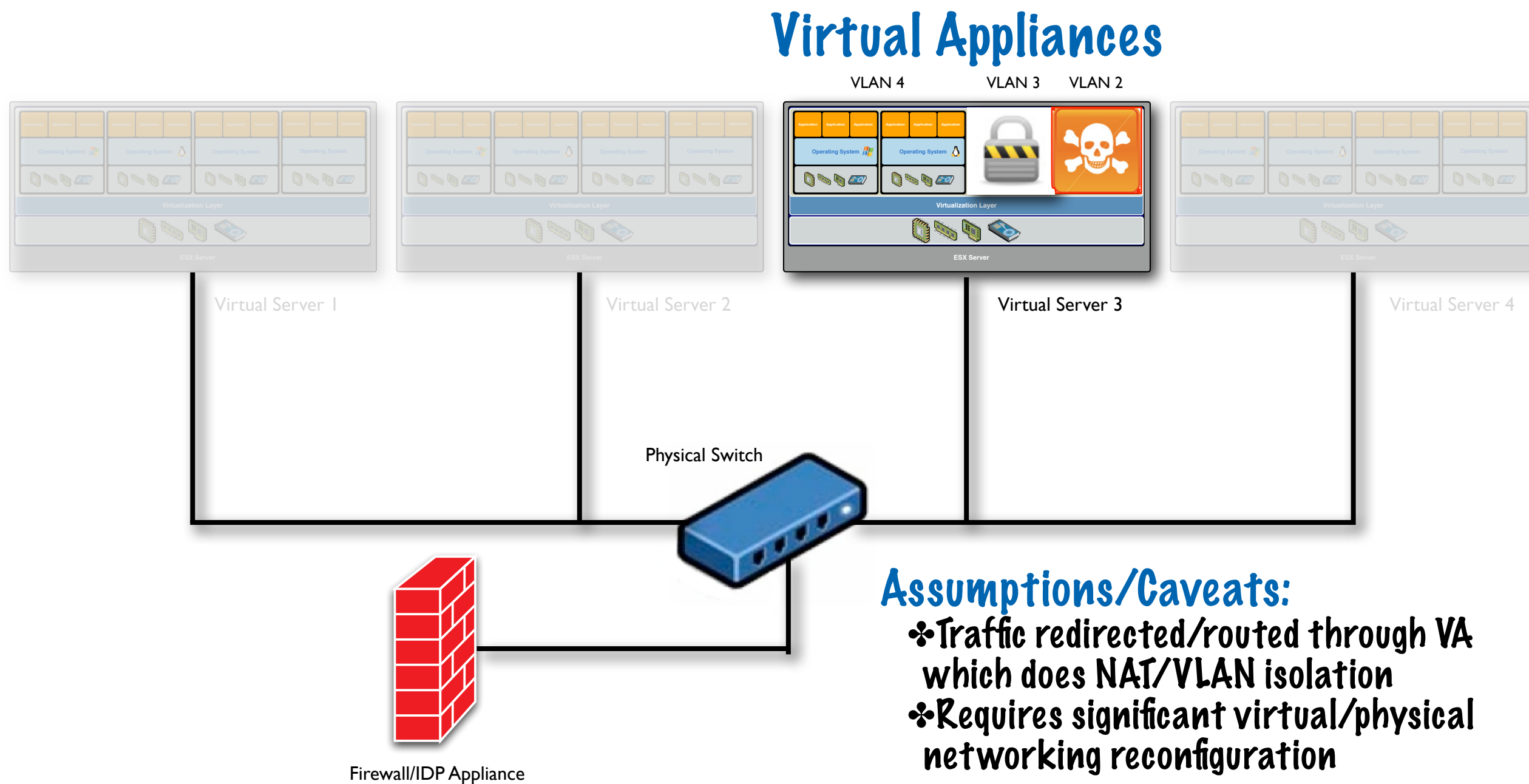


VirtSec Examples: Virtual Appliance with VM to VM On Different vSwitch/VLAN



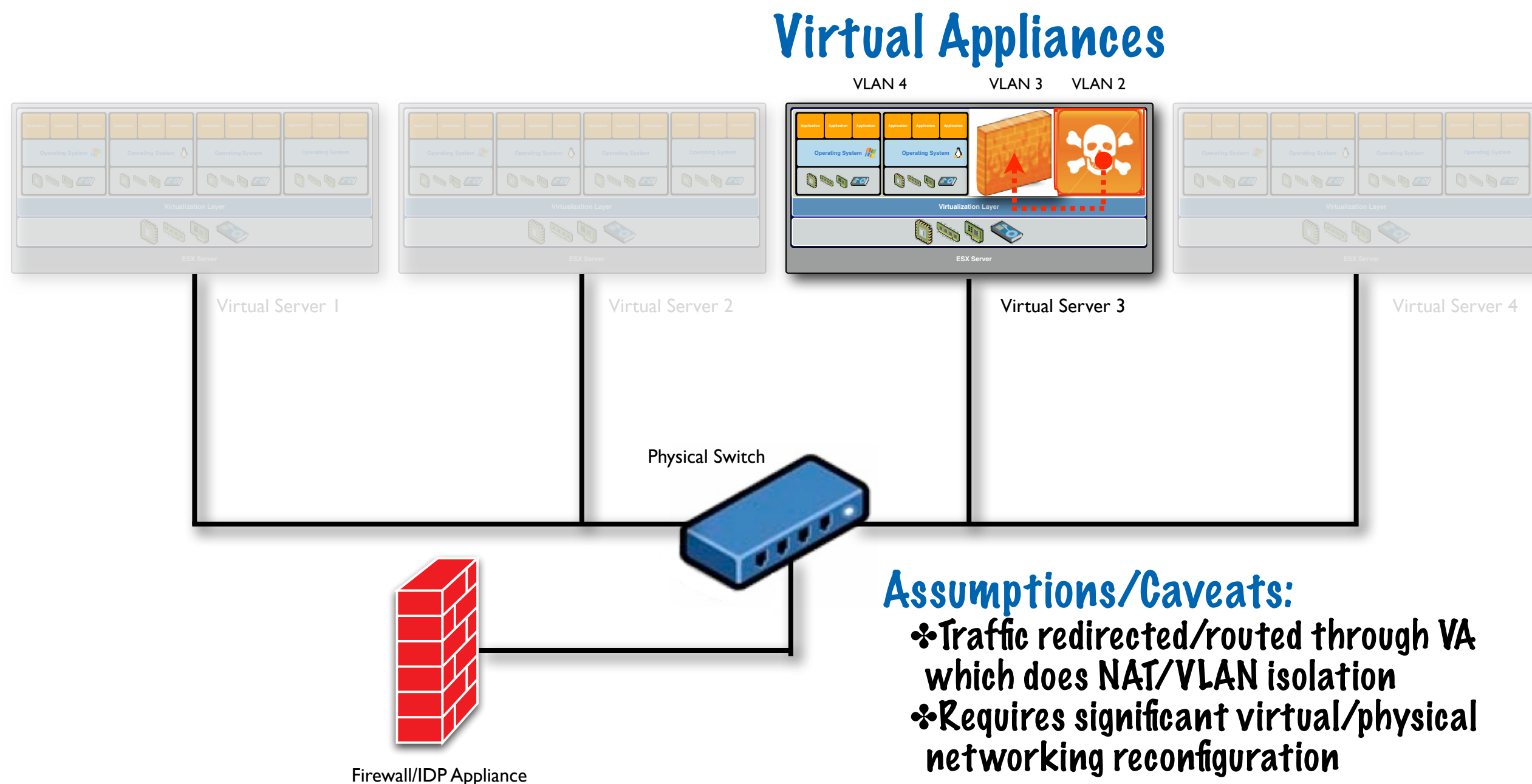


VirtSec Examples: Virtual Appliance with VM to VM On Different vSwitch/VLAN



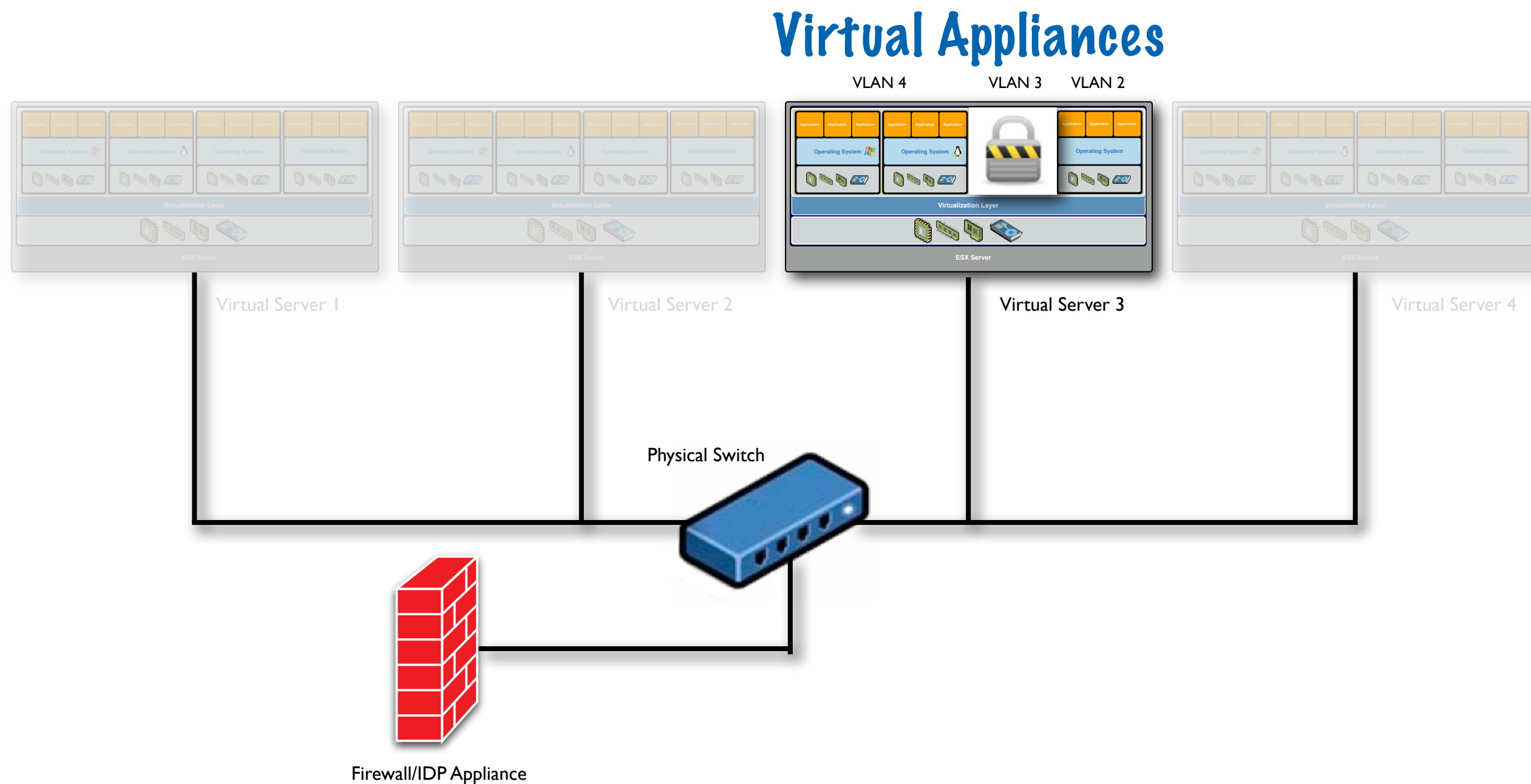


VirtSec Examples: Virtual Appliance with VM to VM On Different vSwitch/VLAN



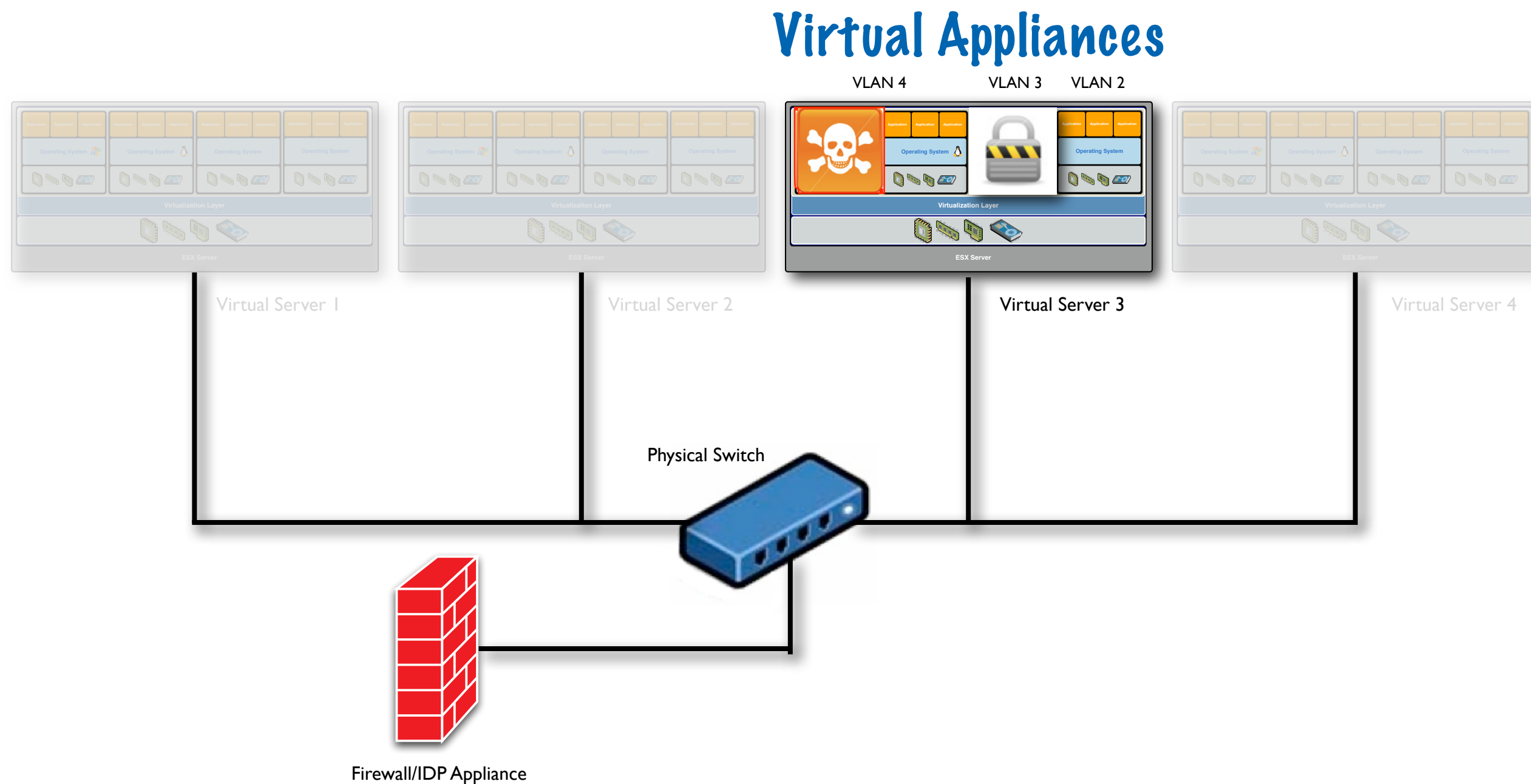


VirtSec Examples: Virtual Appliance with VM to VM On Same vSwitch/VLAN



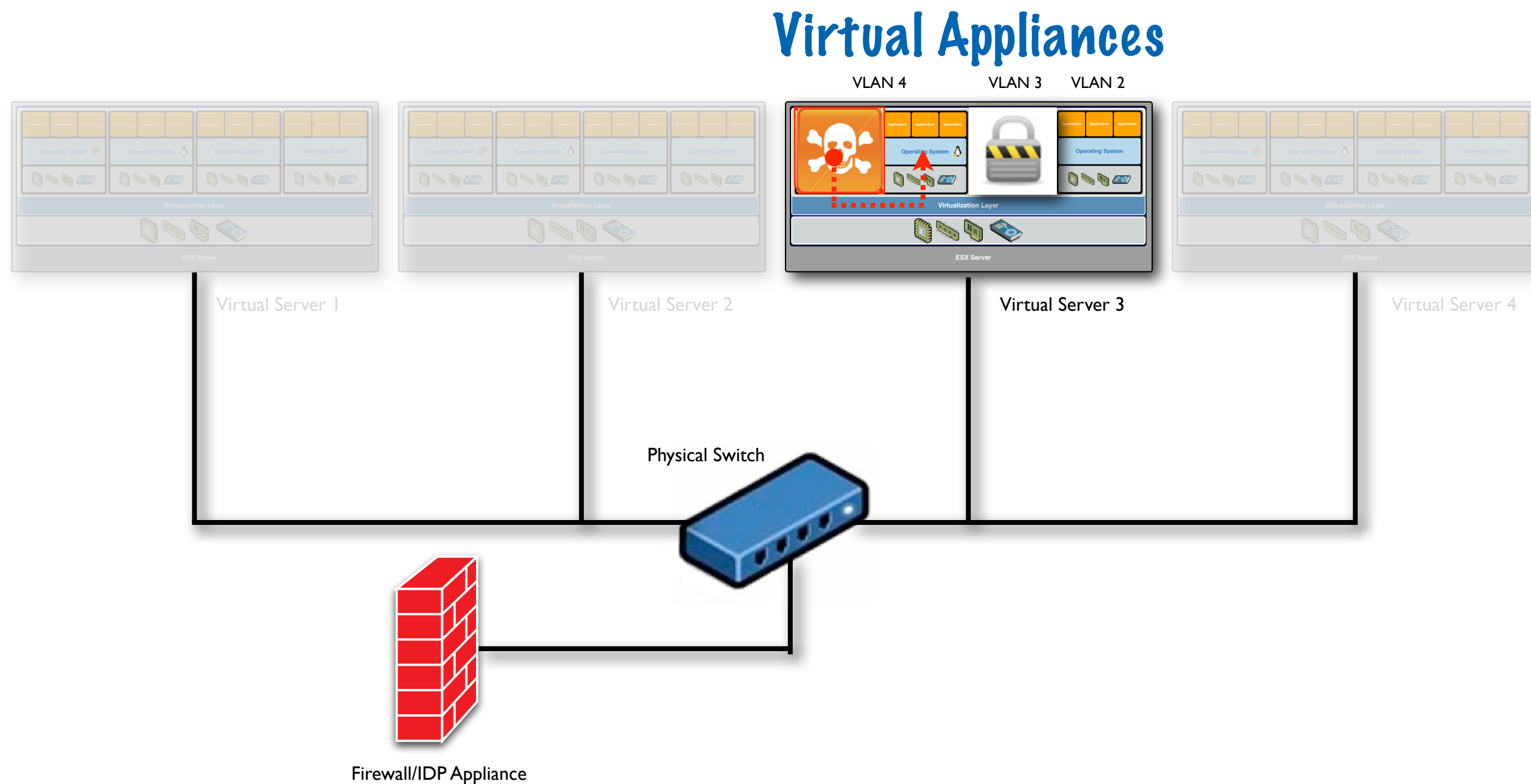


VirtSec Examples: Virtual Appliance with VM to VM On Same vSwitch/VLAN



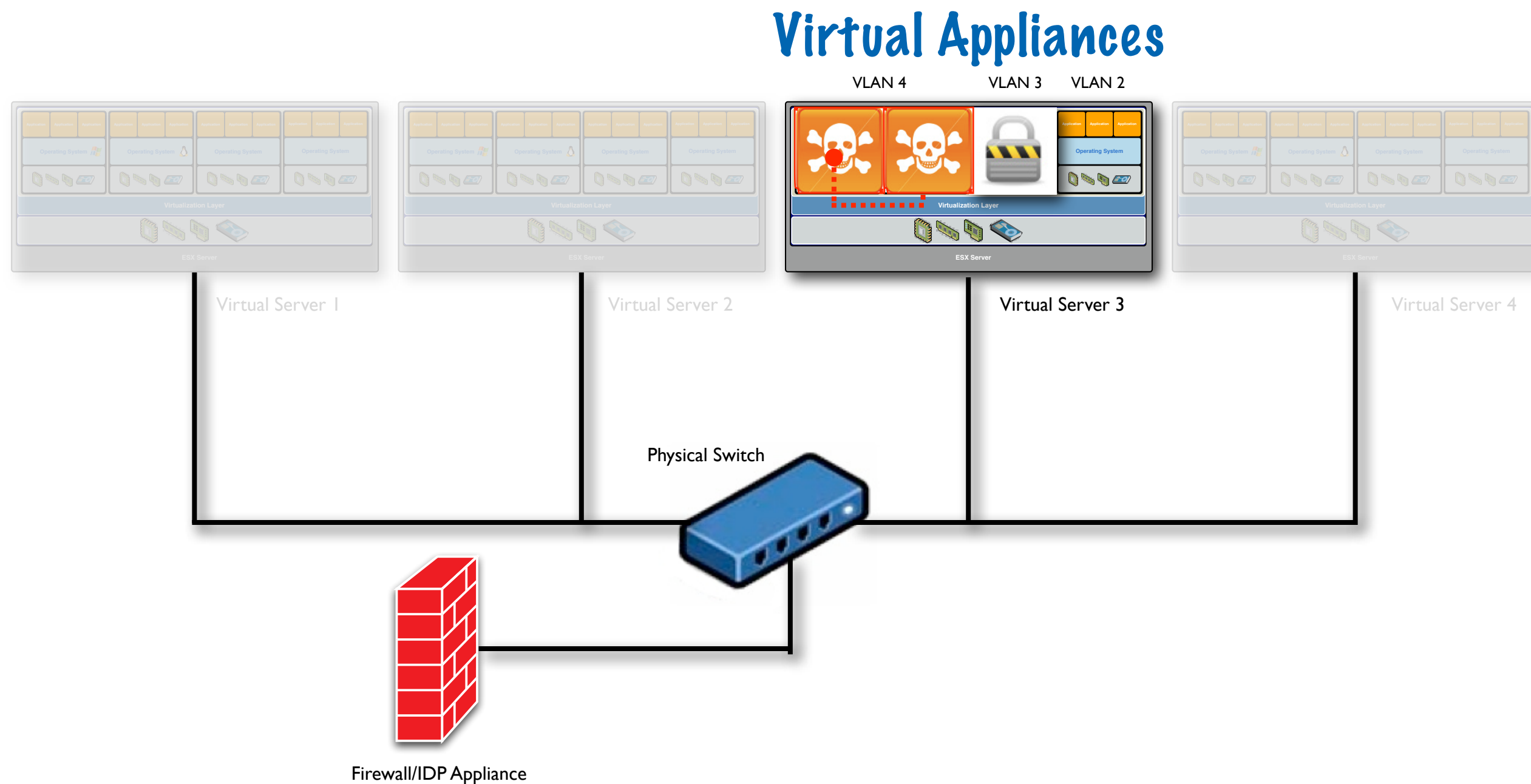


VirtSec Examples: Virtual Appliance with VM to VM On Same vSwitch/VLAN



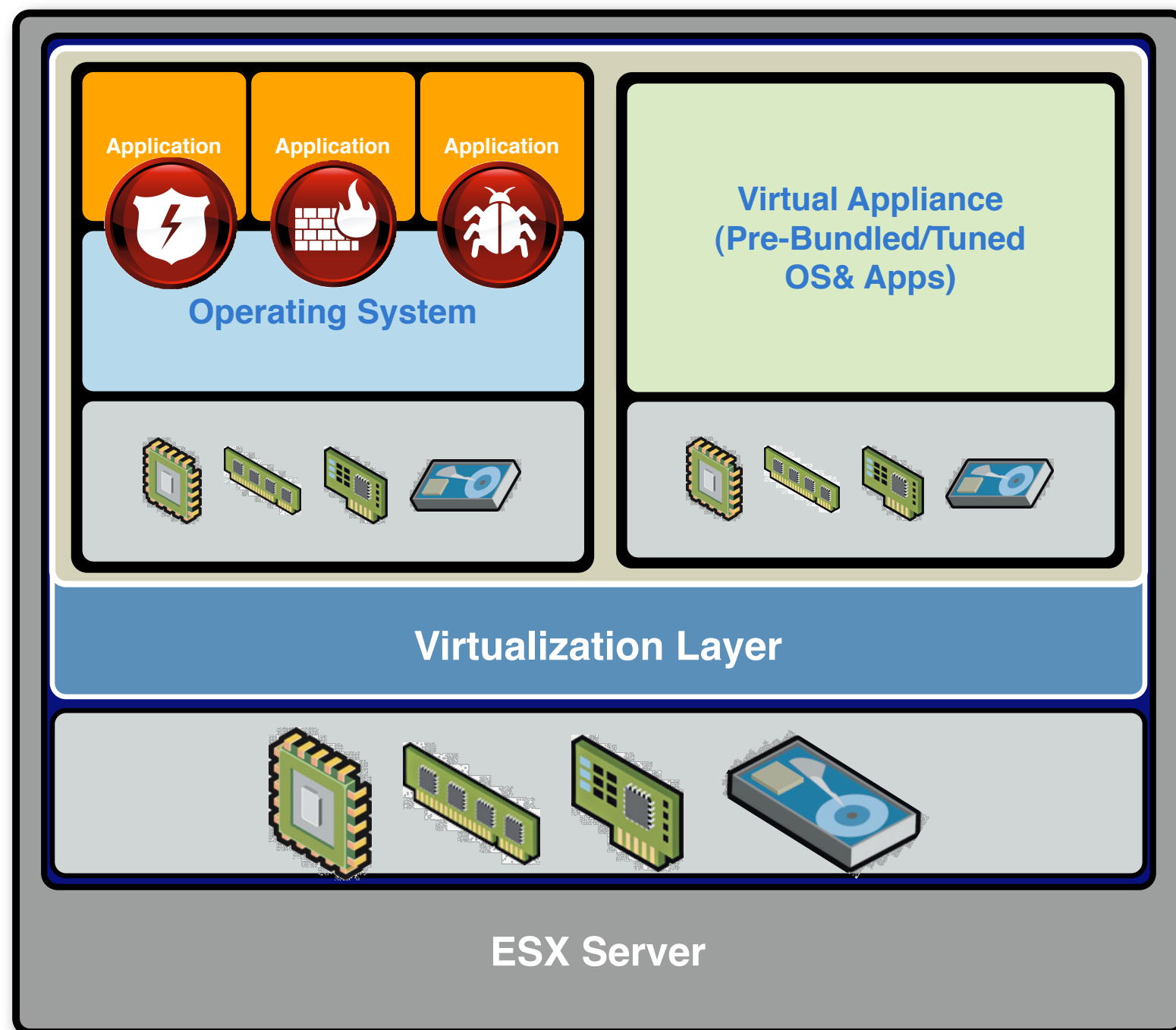


VirtSec Examples: Virtual Appliance with VM to VM On Same vSwitch/VLAN





VirtSec Examples: Virtual Appliances



- ❖ The trick is forcing the traffic through the virtual appliances (if prevention is required) versus merely monitoring via SPAN for detection/monitoring
- ❖ ARP Spoofing/TCP RST's are also used by some vendors for VM's in the same portgroup/VLANs
- ❖ Requires careful (and potentially extensive) virtual networking configuration
- ❖ Doesn't protect against VM's in the same VLAN
- ❖ Does not directly protect the Hypervisor
- ❖ HA/Resilience an issue
- ❖ Consumes Host Resources
- ❖ There are lots of gotchas currently which VMsafe API's will certainly help with...

ALTOR
networks

BlueLane

REFLEX
SECURITY

catbird

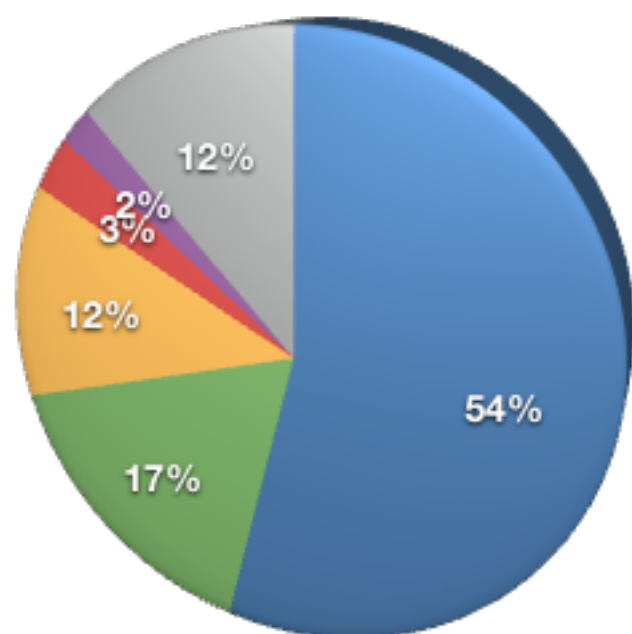
Montego Networks
Secure Switching for Virtual Environments

Apani



How Are Folks Securing Their VM's?

Addressing Security Concerns in Virtualized Environments



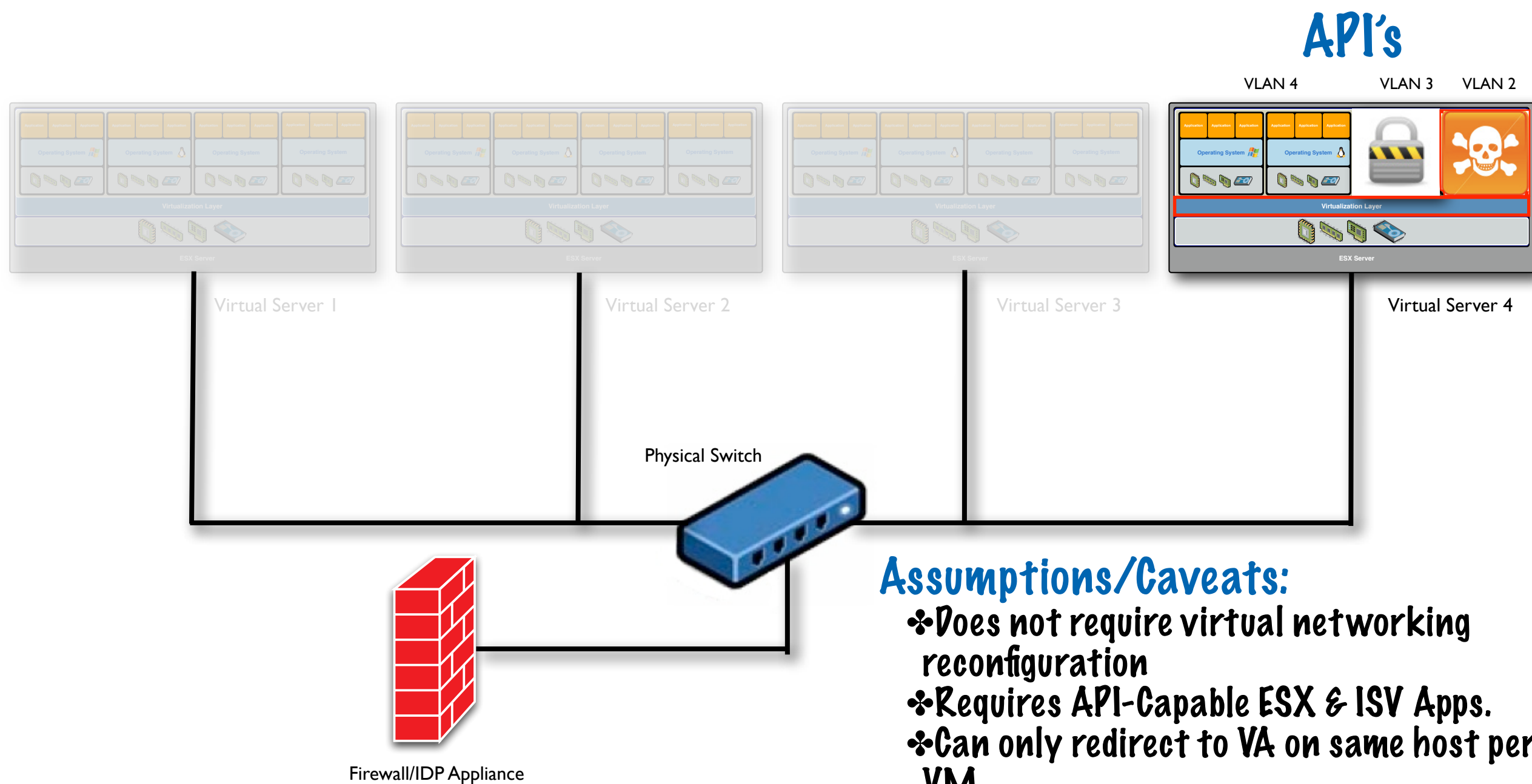
- Traditional infrastructure tools w/NO specific provisions for virtualization (54%)
- Traditional infrastructure tools w/virtualization modules/plugin-ins (17%)
- Utilize virtualization-specific security tools provided by virtualization vendor (12%)
- Utilize third-party security tools designed for VM's (3%)
- Utilize third-party virtualization-only security tools (2%)
- No security provisions in place (12%)

Data: June 2008 InformationWeek Analytics:VMware Security Survey





VirtSec Examples: VMM/ISV API's

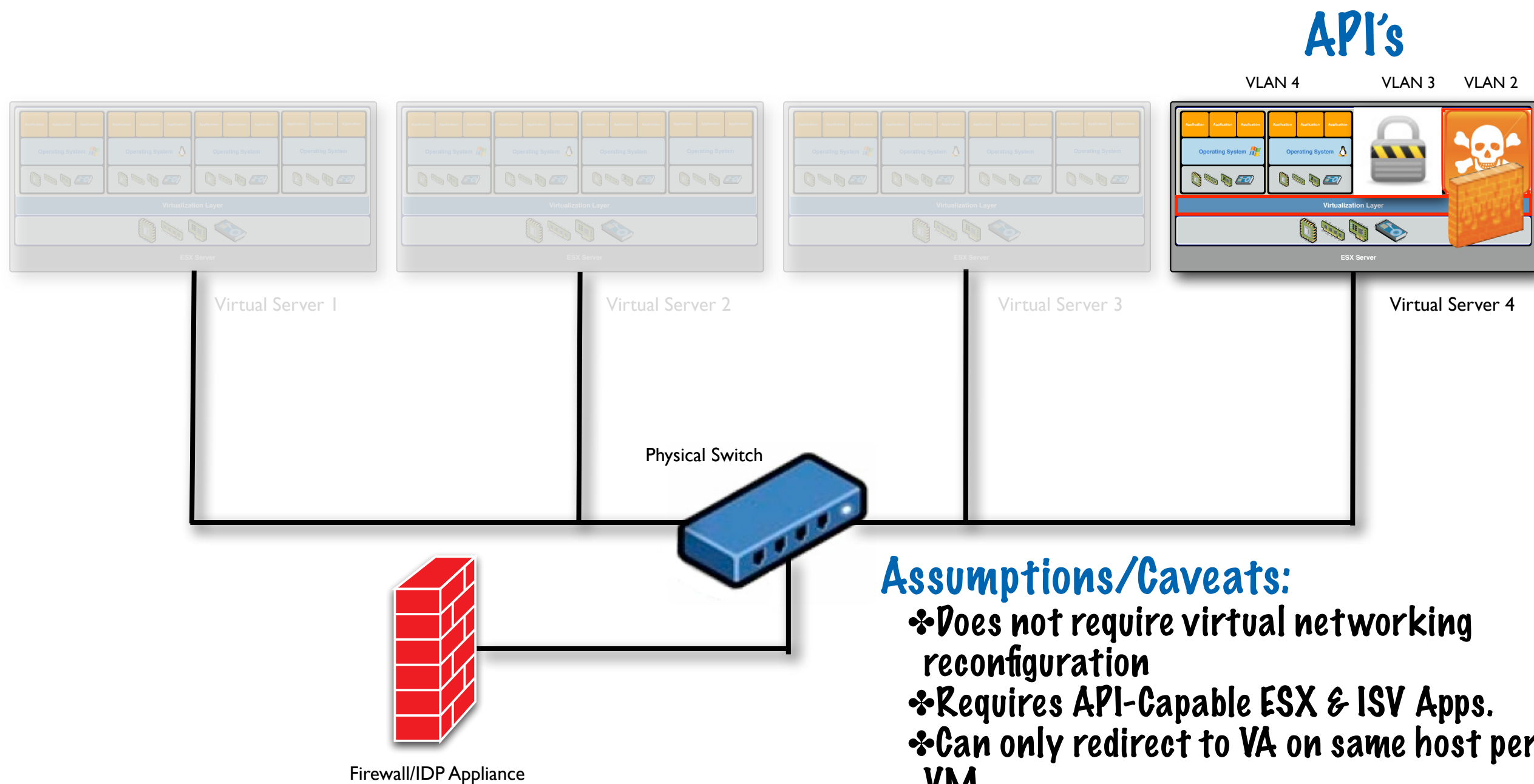


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM



VirtSec Examples: VMM/ISV API's

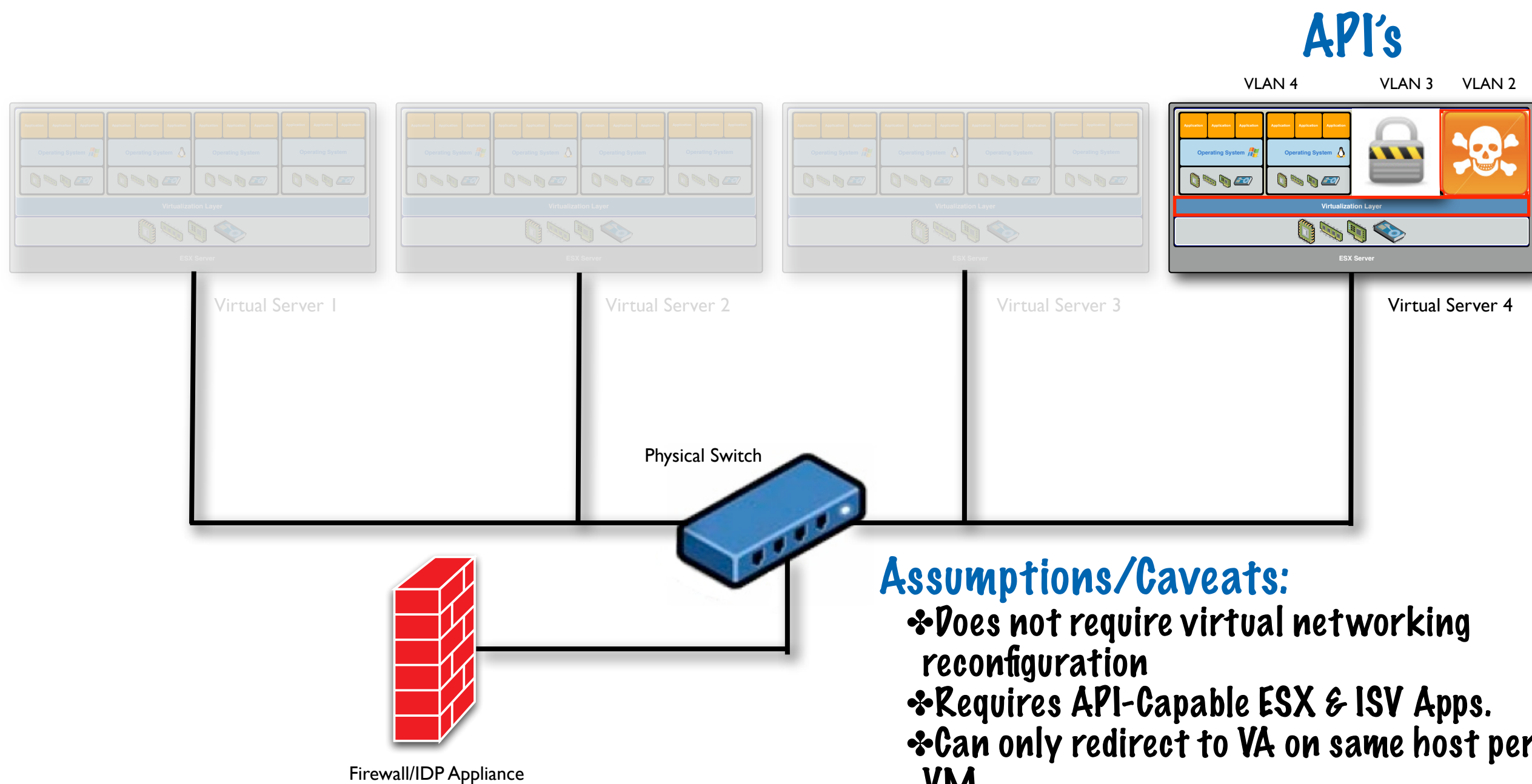


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM



VirtSec Examples: VMM/ISV API's

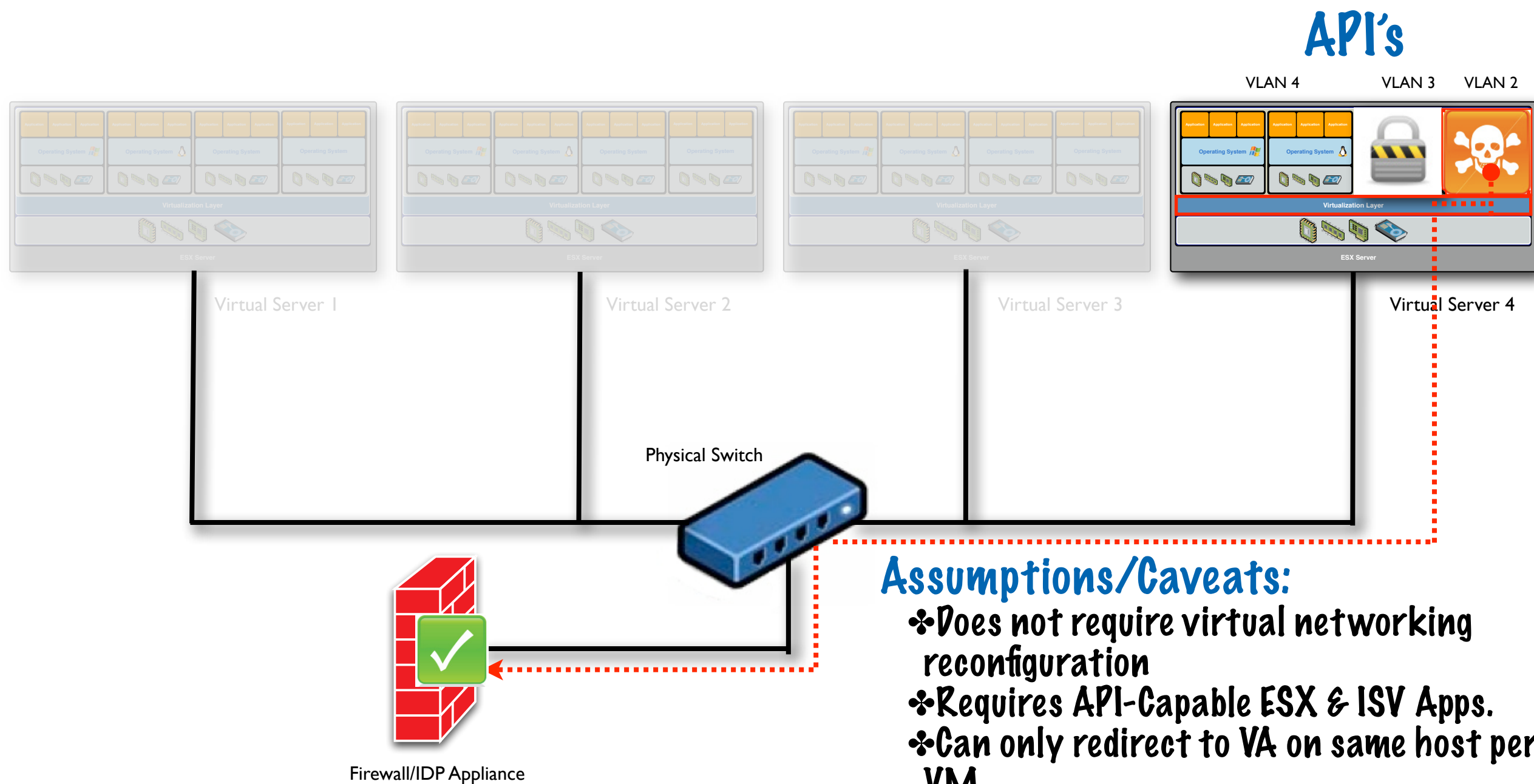


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM

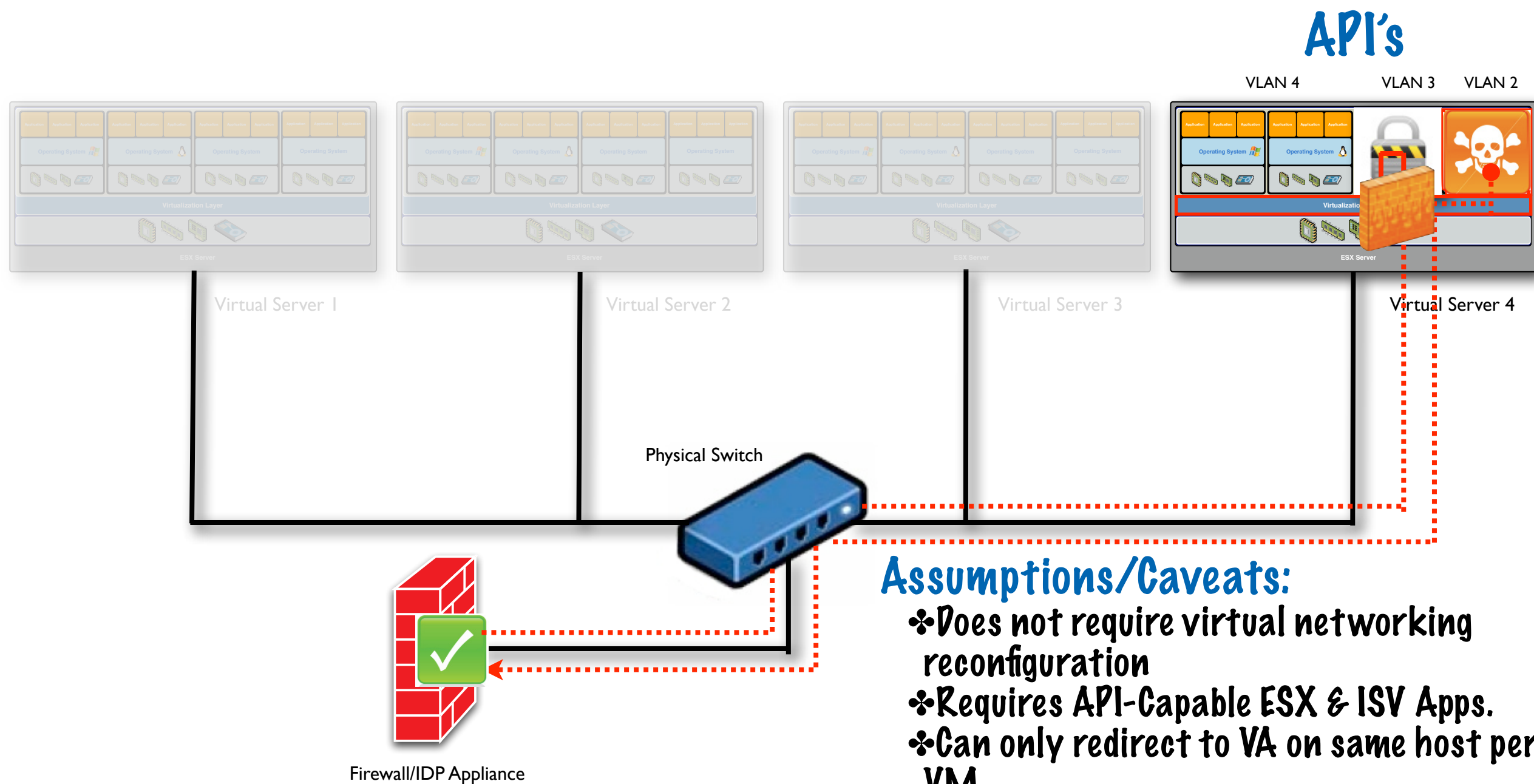


VirtSec Examples: VMM/ISV API's



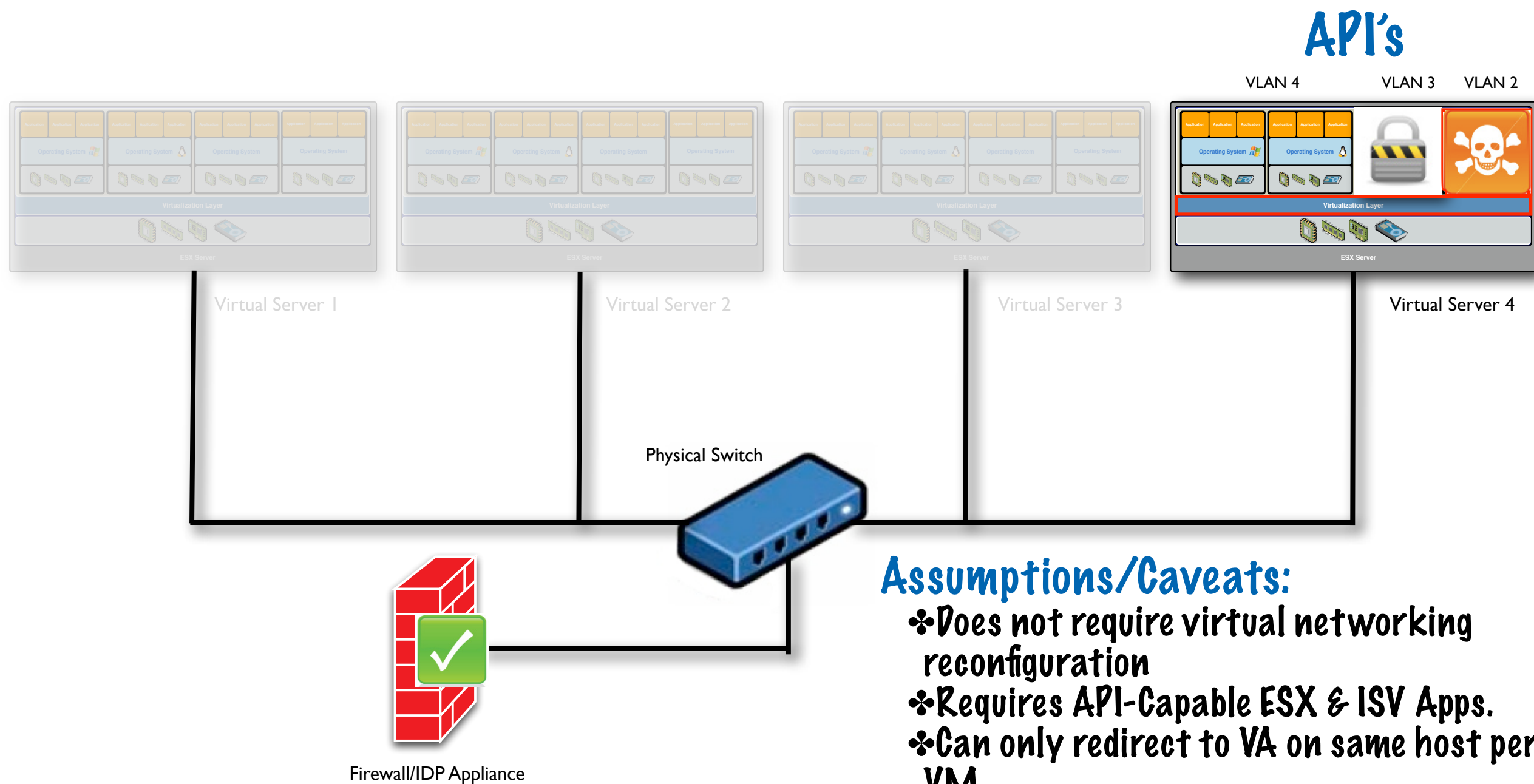


VirtSec Examples: VMM/ISV API's





VirtSec Examples: VMM/ISV API's

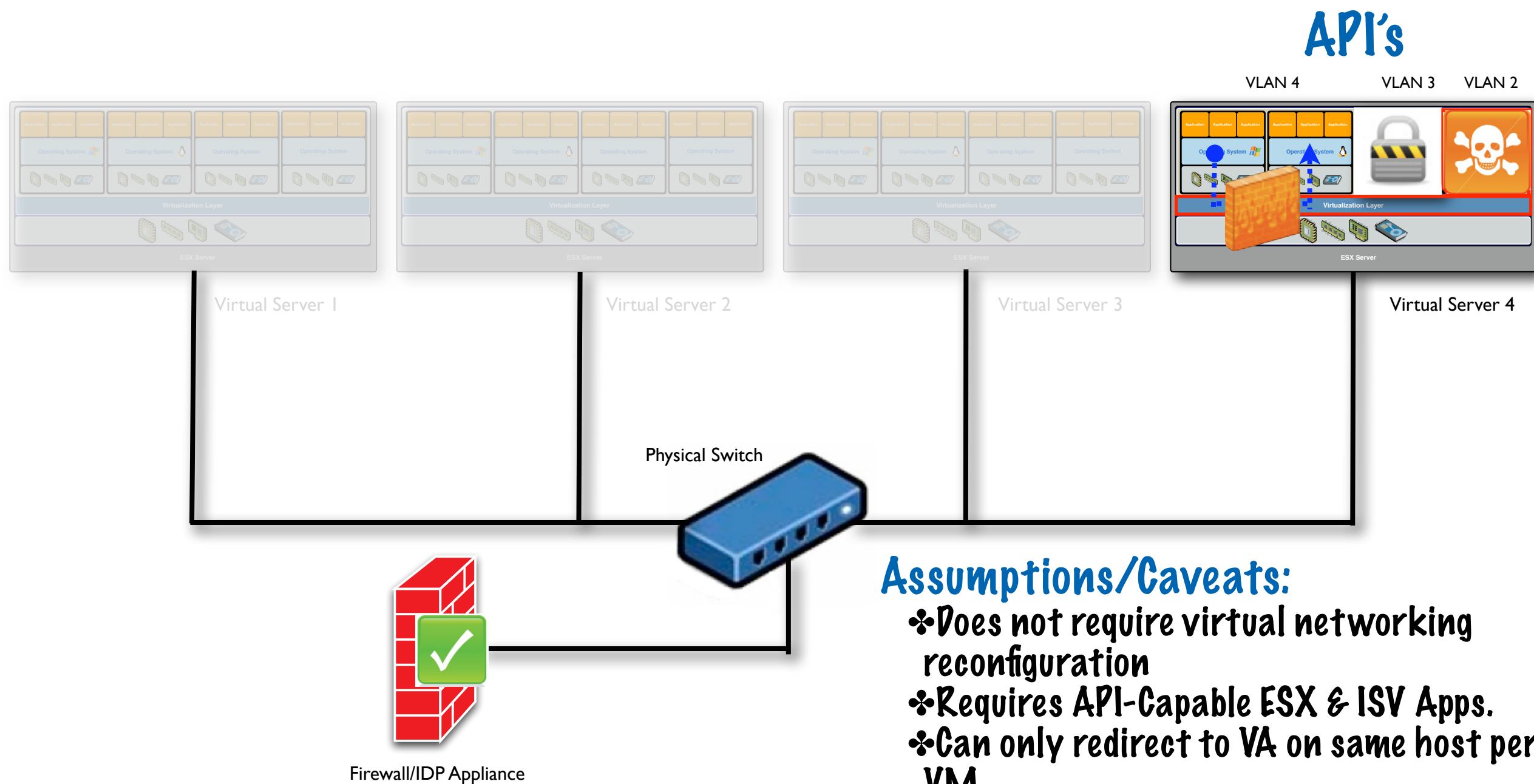


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM



VirtSec Examples: VMM/ISV API's

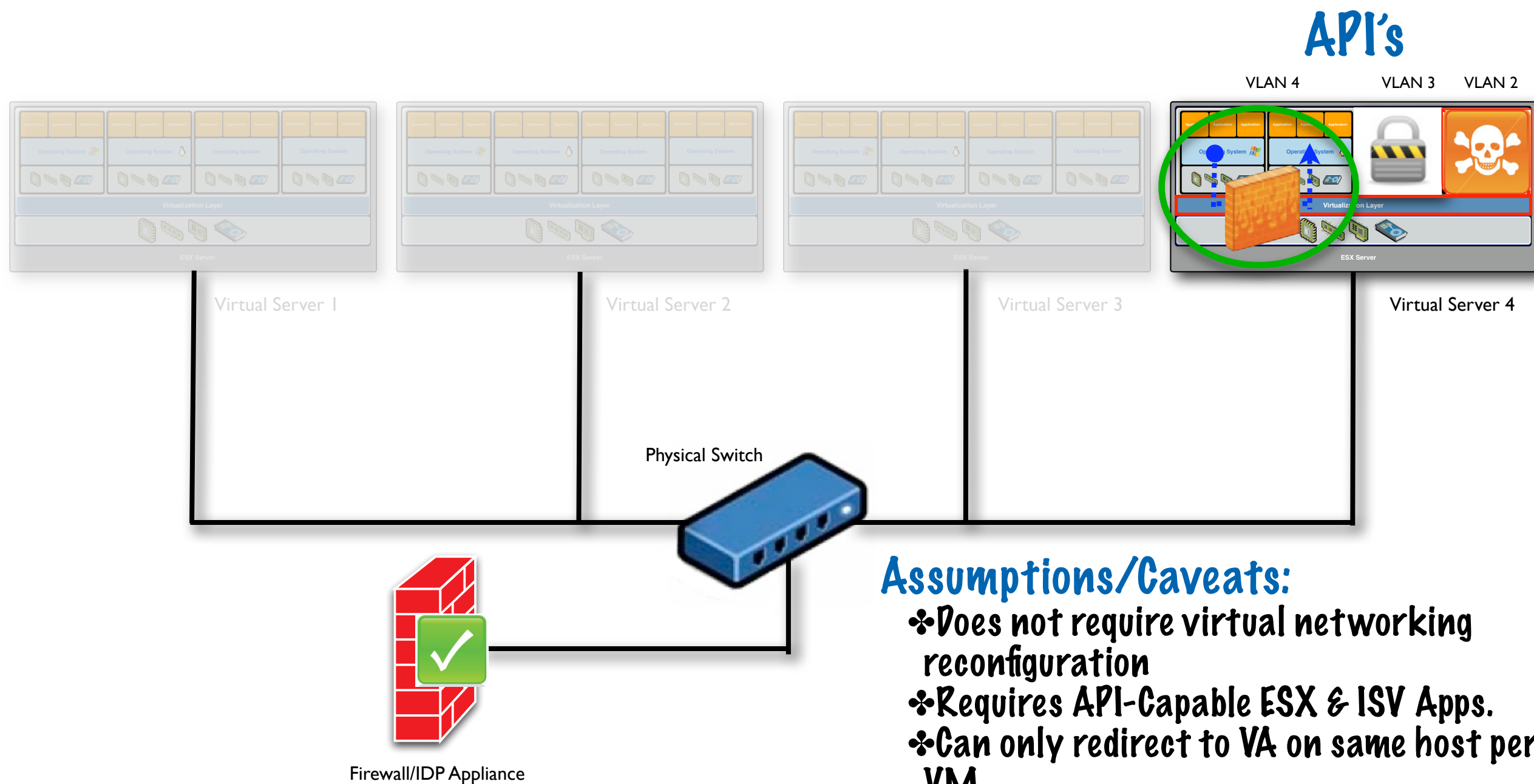


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM



VirtSec Examples: VMM/ISV API's

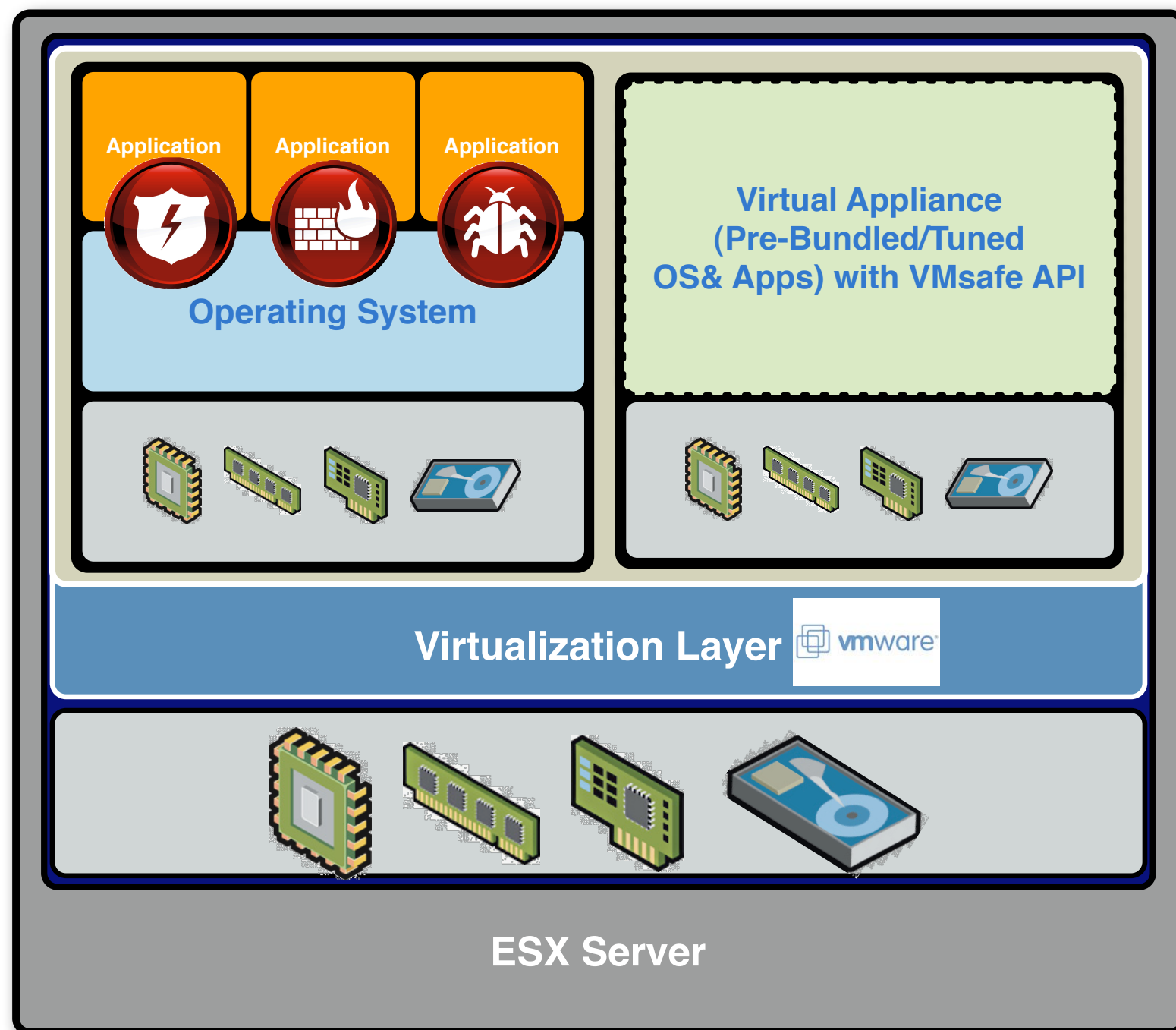


Assumptions/Caveats:

- ❖ Does not require virtual networking reconfiguration
- ❖ Requires API-Capable ESX & ISV Apps.
- ❖ Can only redirect to VA on same host per VM



VirtSec Examples: VMM/ISV API's



VMware VMsafe:

Security solutions built with VMware VMsafe will provide customers better granularity, visibility, correlation and scalability in virtual machine deployments.

Enables partners to build security solutions in the form of a virtual machine that can access, correlate and modify data to help control and protect:

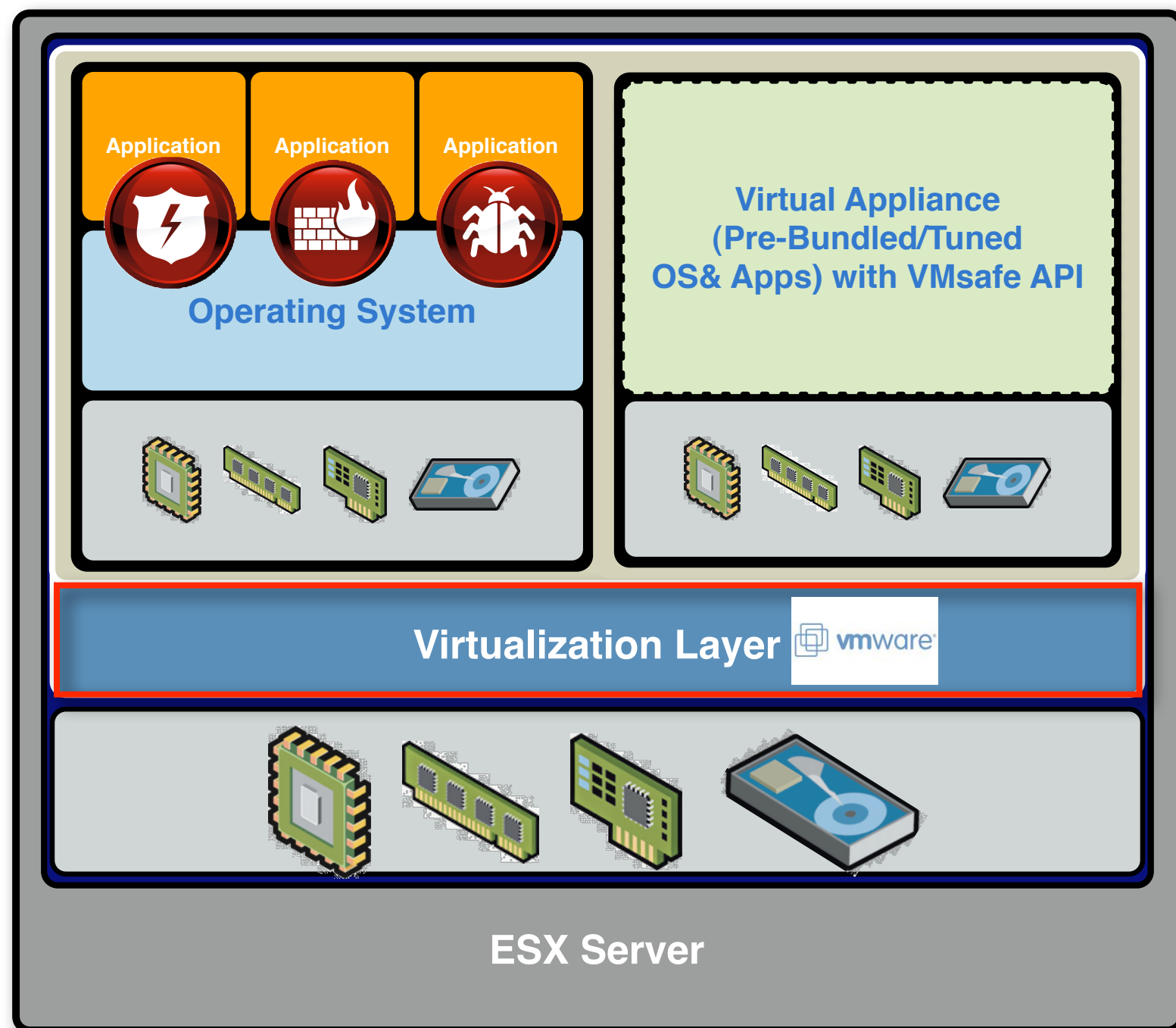
- ❖ Memory and CPU
- ❖ Networking
- ❖ Process execution
- ❖ Storage

Note:

- ❖ Requires re-tooled ISV software & virtualization platforms
- ❖ Per-VM policies can only redirect to a VA/VM within the same host
- ❖ Coarse triggers
- ❖ Dispositions are limited



VirtSec Examples: VMM/ISV API's



VMware VMsafe:

Security solutions built with VMware VMsafe will provide customers better granularity, visibility, correlation and scalability in virtual machine deployments.

Enables partners to build security solutions in the form of a virtual machine that can access, correlate and modify data to help control and protect:

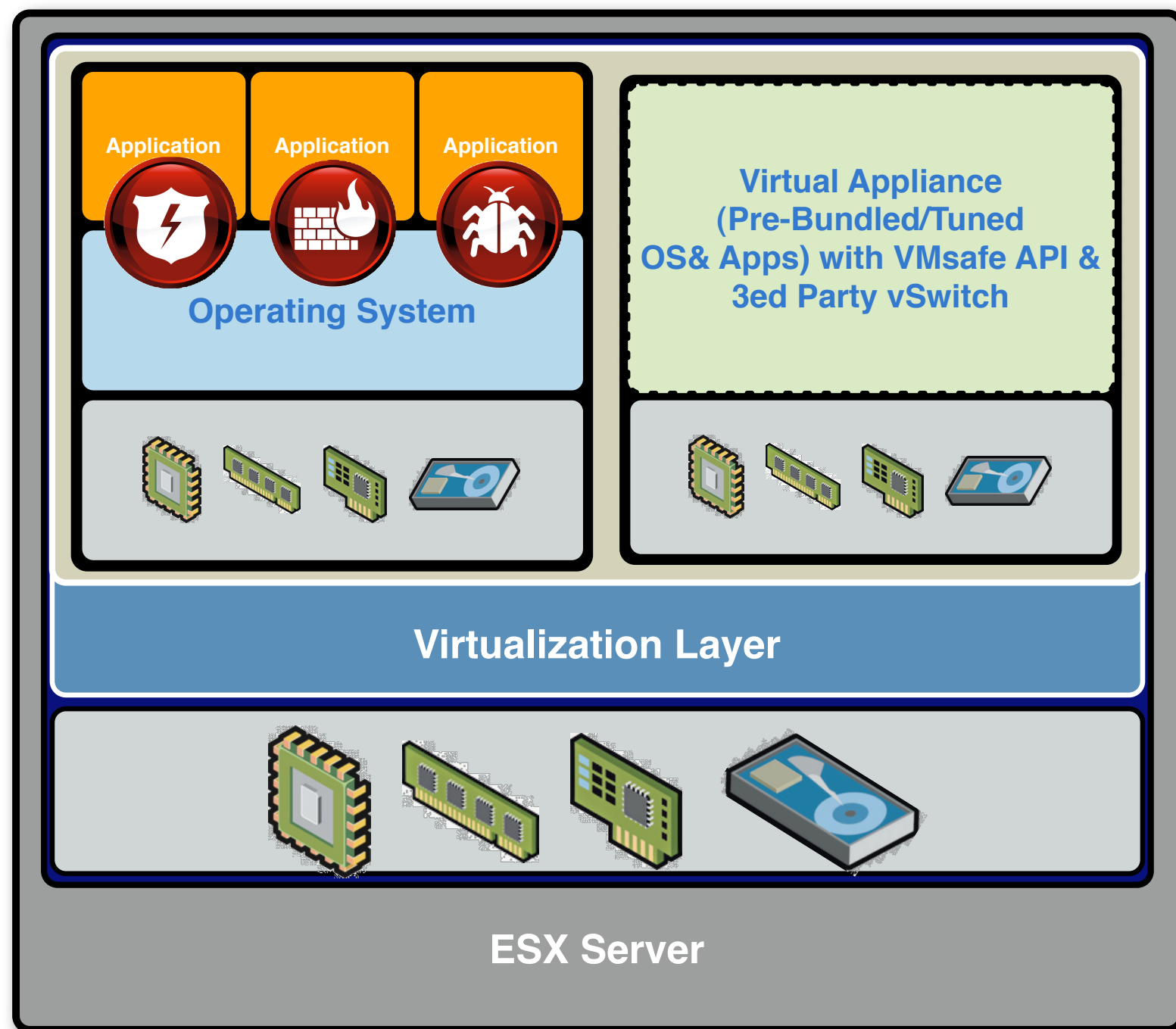
- ❖ Memory and CPU
- ❖ Networking
- ❖ Process execution
- ❖ Storage

Note:

- ❖ Requires re-tooled ISV software & virtualization platforms
- ❖ Per-VM policies can only redirect to a VA/VM within the same host
- ❖ Coarse triggers
- ❖ Dispositions are limited



VirtSec Futures: 3rd Party vSwitches



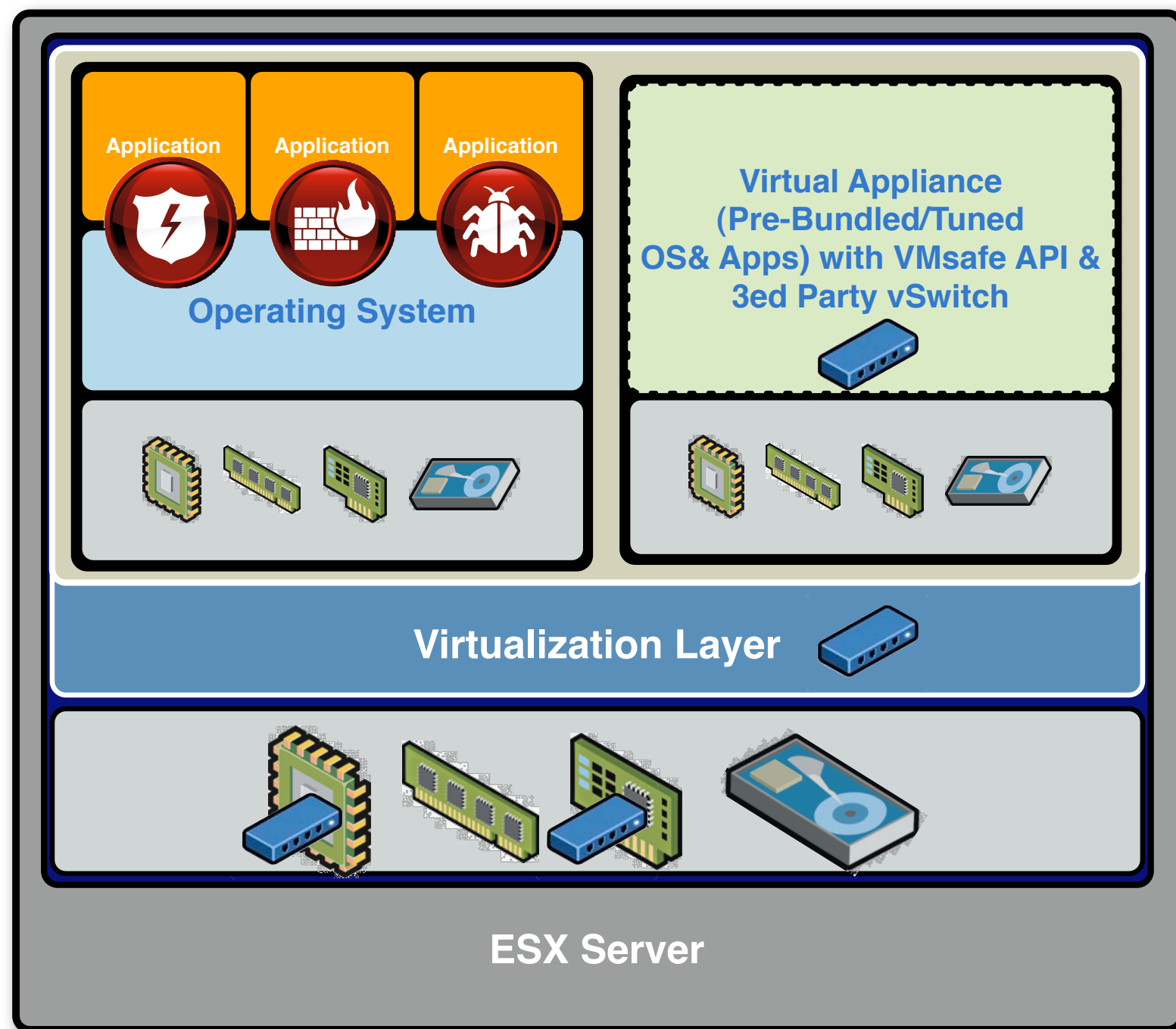
Third Party vSwitches

- ❖ 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 (load-balancing, QoS, L3-7, etc...)
- ❖ vSwitches evolving to reside in hardware & software:
 - ❖ Hypervisor
 - ❖ VA/VM
 - ❖ Underlying Virtualization-enabled CPU's
 - ❖ In "new" breed of NIC cards





VirtSec Futures: 3rd Party vSwitches



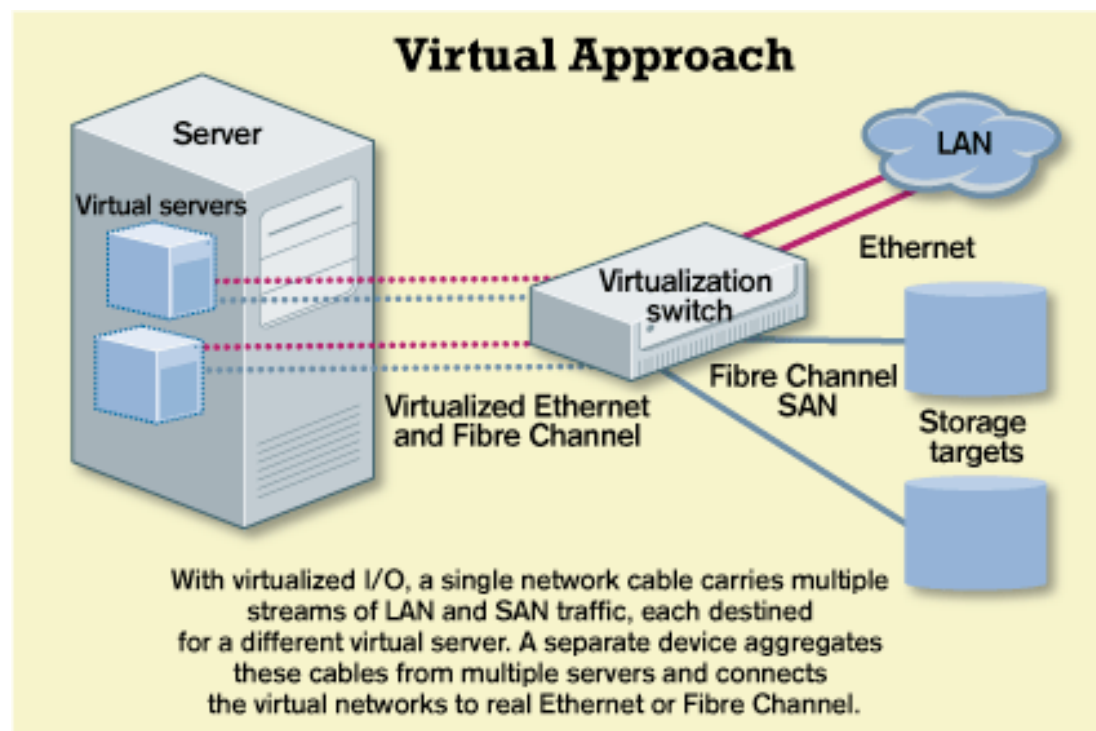
Third Party vSwitches

- ❖ 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 (load-balancing, QoS, L3-7, etc...)
- ❖ vSwitches evolving to reside in hardware & software:
 - ❖ Hypervisor
 - ❖ VA/VM
 - ❖ Underlying Virtualization-enabled CPU's
 - ❖ In "new" breed of NIC cards





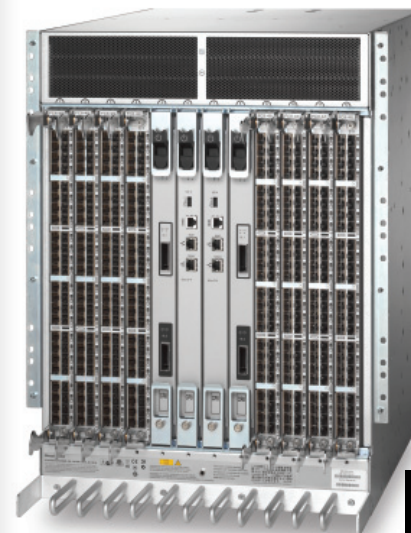
VirtSec Futures: I/O Virtualization



InformationWeek

I/O Virtualization:

- Single network connection provides virtualized fabric interconnectivity for LAN & SAN
- Ultimately your VM's run in the switch
- All your VM's are belong to us!



- Cisco 7000 Nexus
- Brocade DXC Backbone
- 3Leaf V-8000 Virtual I/O Server
- Xsigo I/O Director





My Head's In the Cloud(s)

- ▶ Today's virtualization offerings are just the beginning
- ▶ Cloud/Grid/Utility computing is real
- ▶ SaaS, Amazon's EC2, Clean Pipes are all great examples today of what's coming tomorrow
- ▶ How are we going to secure the abstraction of a cloud-based virtualized processes, memory space, I/O?



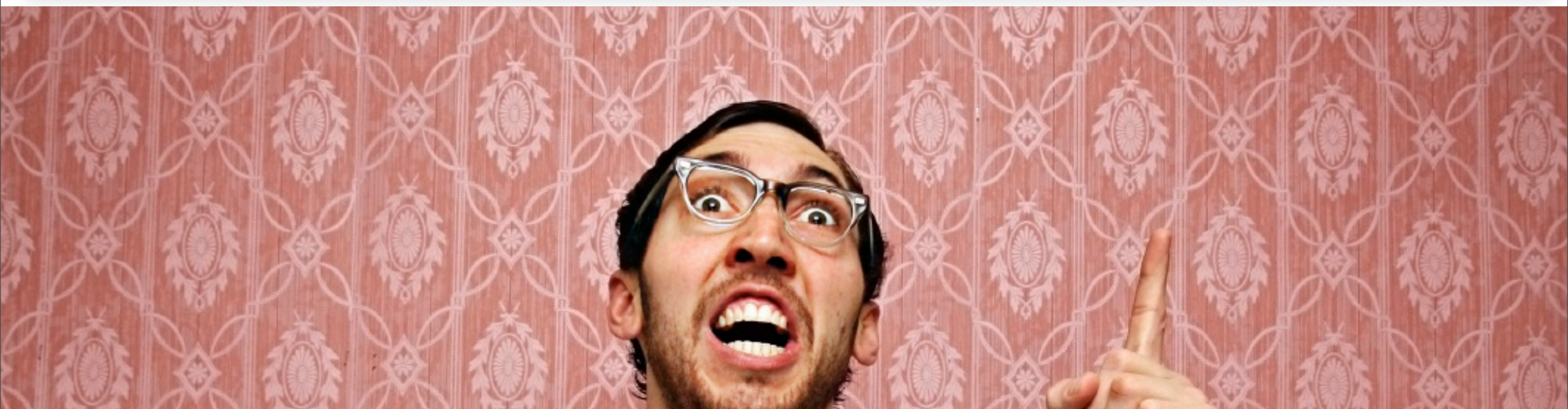
The End Is Nigh! Run Away!

- ✿ Setup & Context
- ✿ x86 Virtualization Overview in 90 Seconds
- ✿ Virtual Networking Architecture
- ✿ VirtSec Solutions Landscape
- ✿ The Four Horsemen
- ✿ Wrap-Up





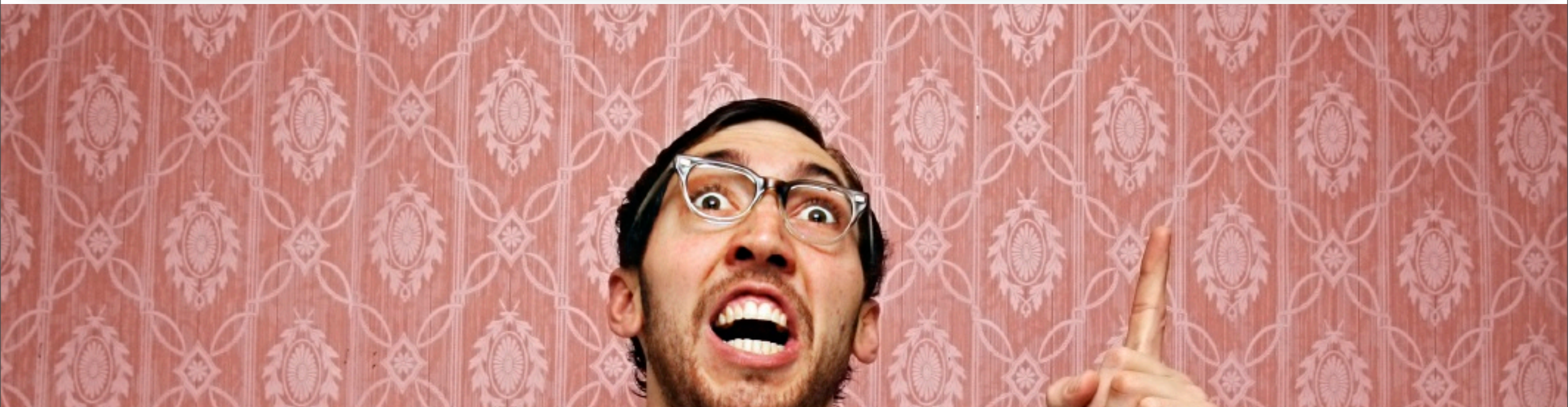
Vini, Vidi, Wiki...





Vini, Vidi, Wiki...

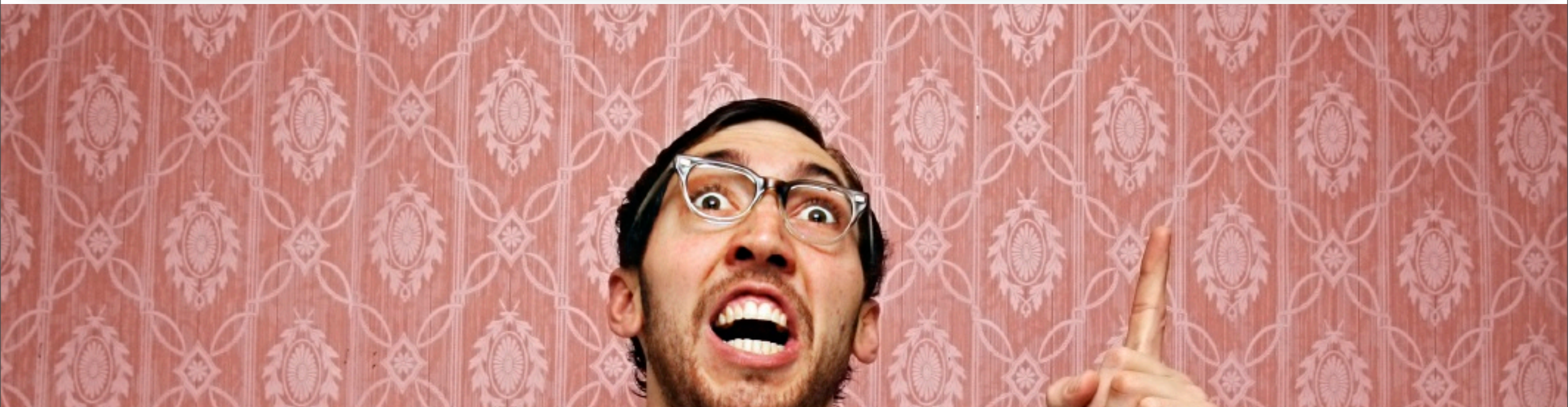
- ❖ **Monolithic security vendor virtual appliances are the virtualization version of the UTM argument**





Vini, Vidi, Wiki...

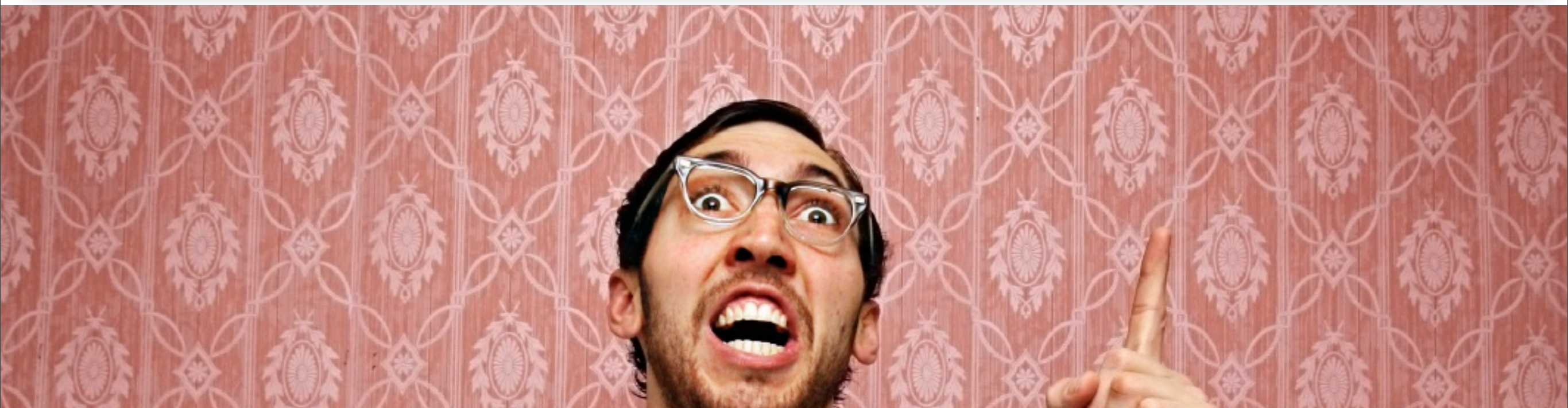
- ❖ **Monolithic security vendor virtual appliances are the virtualization version of the UTM argument**
- ❖ **Virtualized Security can seriously impact performance, resiliency and scalability**





Vini, Vidi, Wiki...

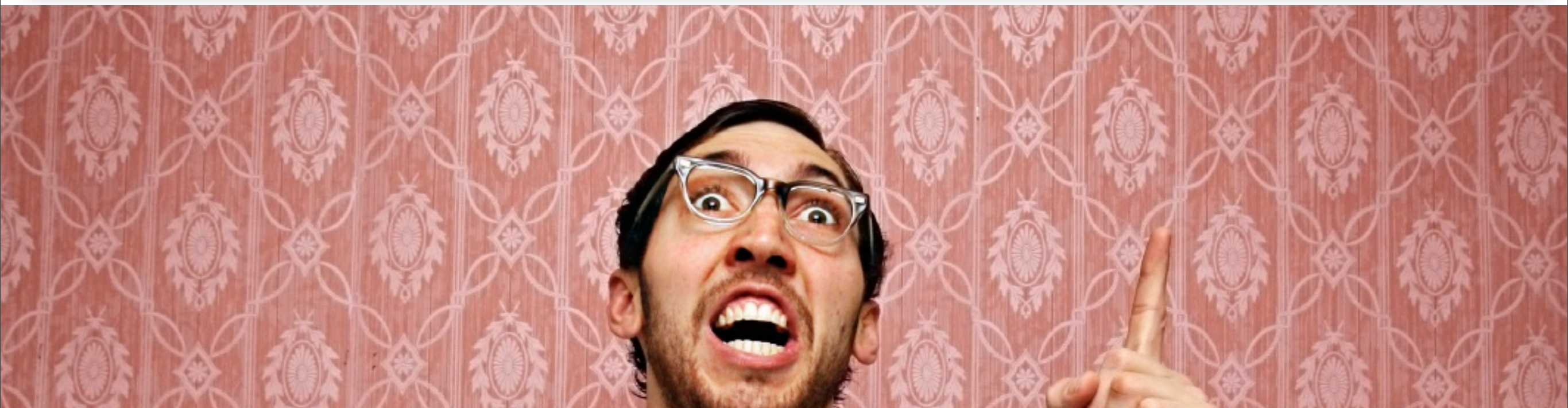
- ❖ **Monolithic security vendor virtual appliances are the virtualization version of the UTM argument**
- ❖ **Virtualized Security can seriously impact performance, resiliency and scalability**
- ❖ **Replicating many highly-available security applications and network topologies in virtual switches don't work**





Vini, Vidi, Wiki...

- ❖ **Monolithic security vendor virtual appliances are the virtualization version of the UTM argument**
- ❖ **Virtualized Security can seriously impact performance, resiliency and scalability**
- ❖ **Replicating many highly-available security applications and network topologies in virtual switches don't work**
- ❖ **Virtualizing security will not save you money, it will cost you more**





Example: Virtualizing the DMZ*

Typical Screened-Subnet DMZ:

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

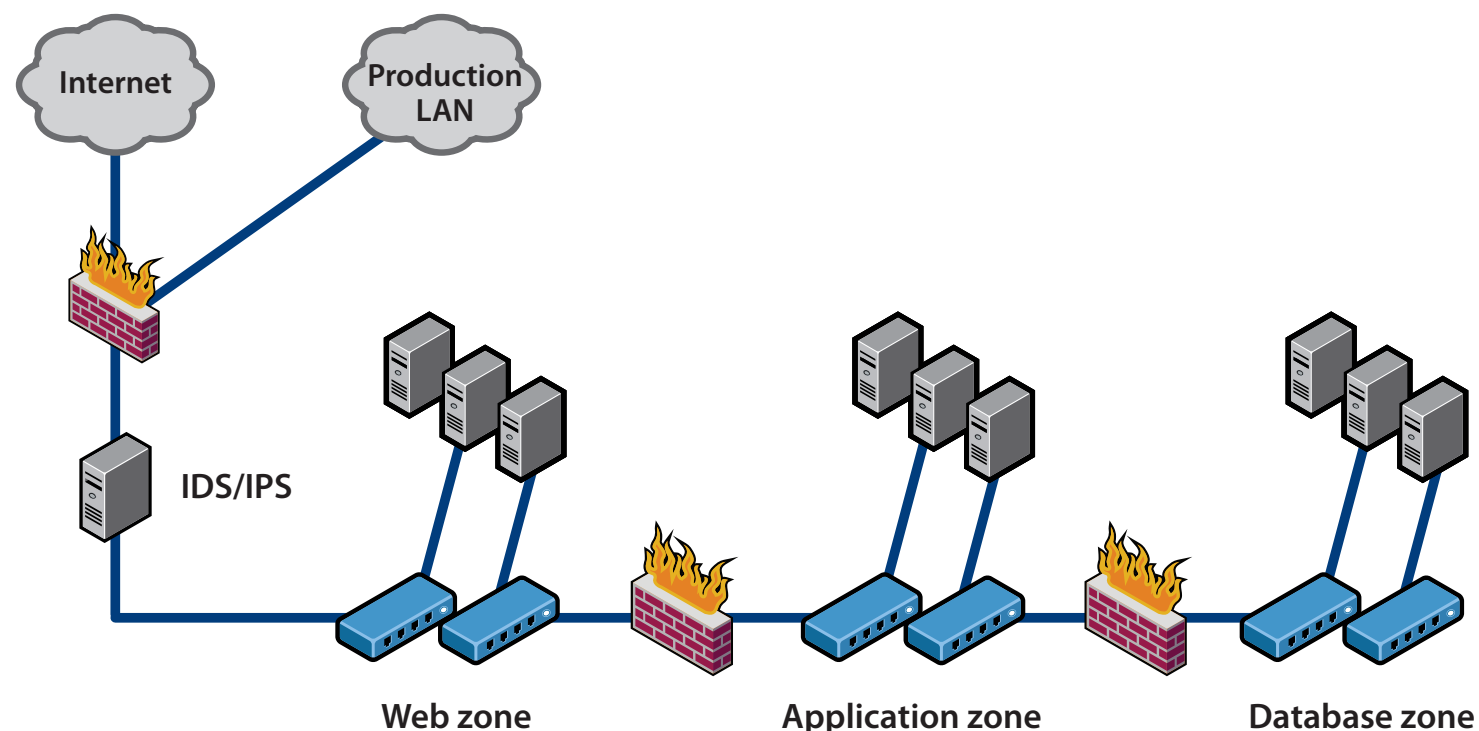


Figure 1 — A typical DMZ in a physical environment

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



Example: Virtualizing the DMZ*

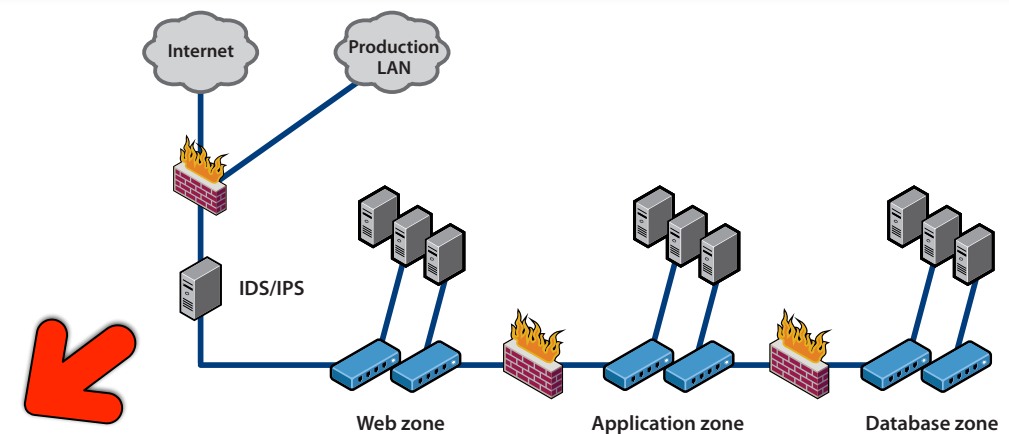


Figure 1 — A typical DMZ in a physical environment

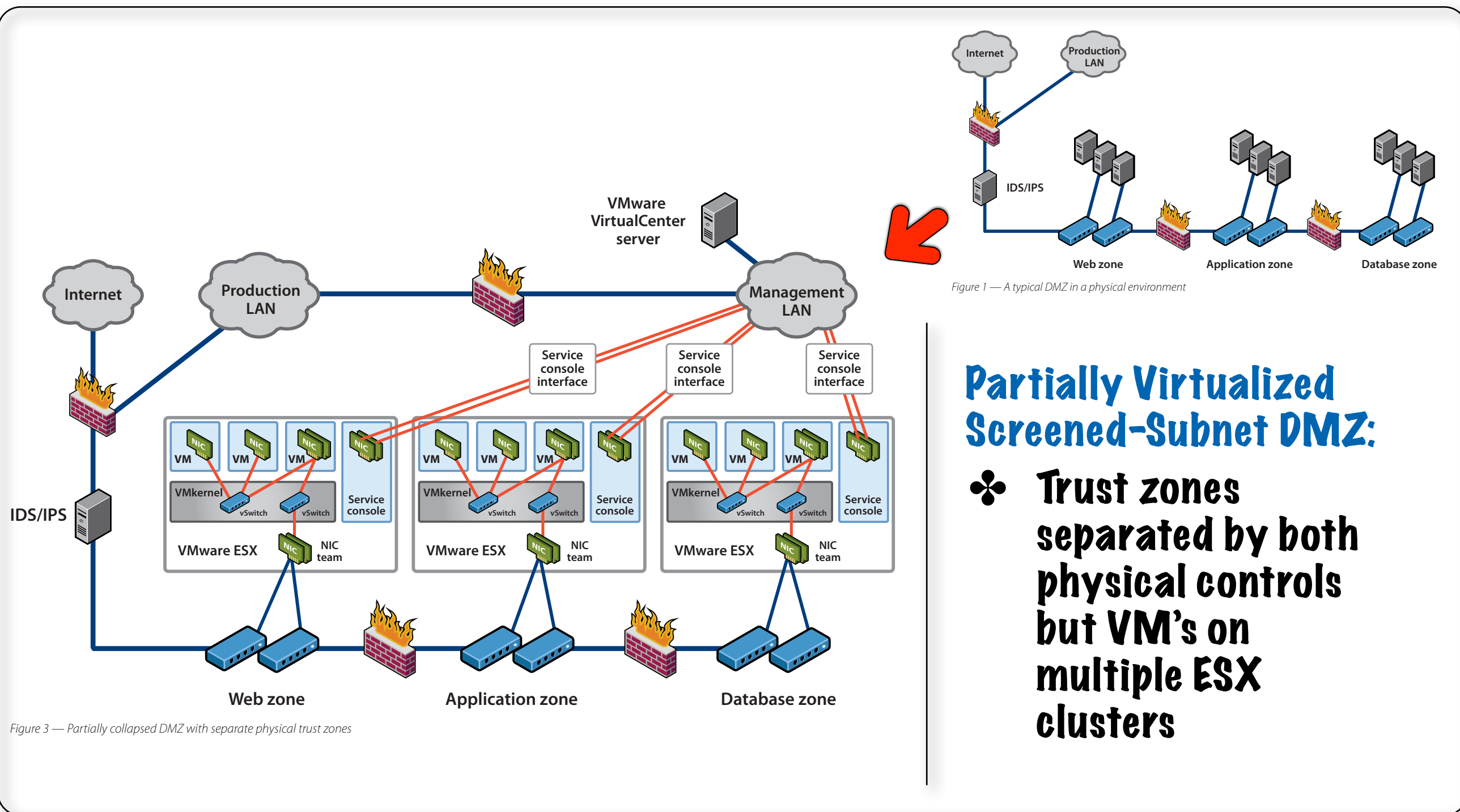
Partially Virtualized Screened-Subnet DMZ:

- ❖ 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*



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



Example: Virtualizing the DMZ*

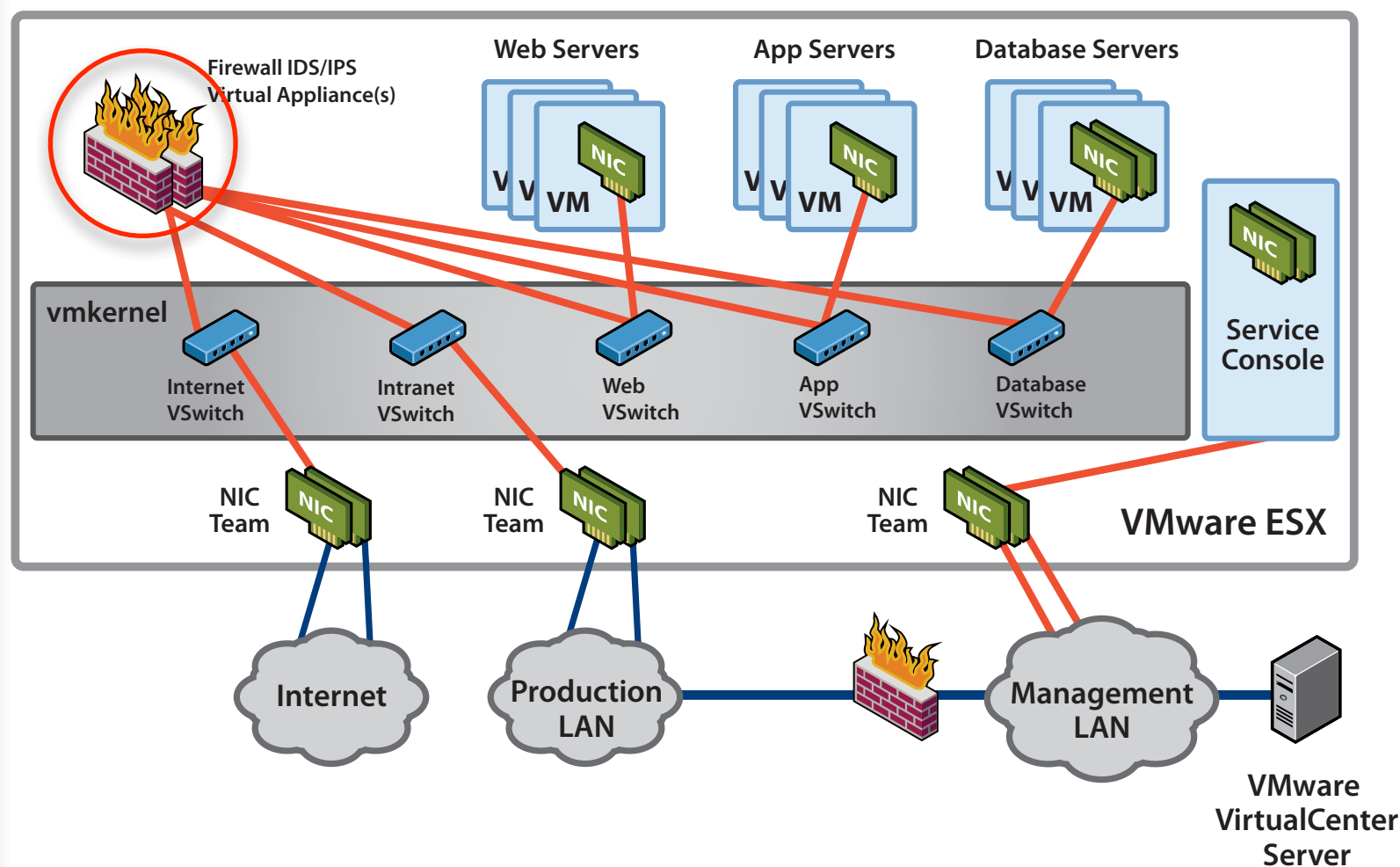


Figure 5 — Fully collapsed DMZ

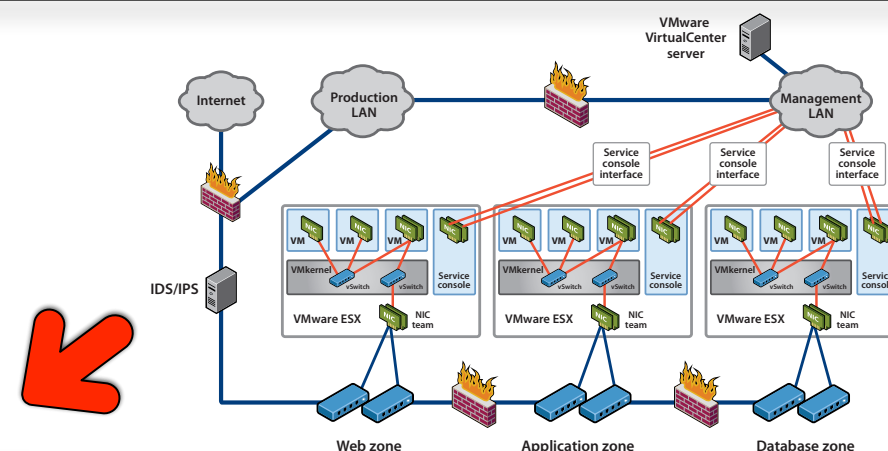


Figure 3 — Partially collapsed DMZ with separate physical trust zones

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



Who Are the Four Horsemen?

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**



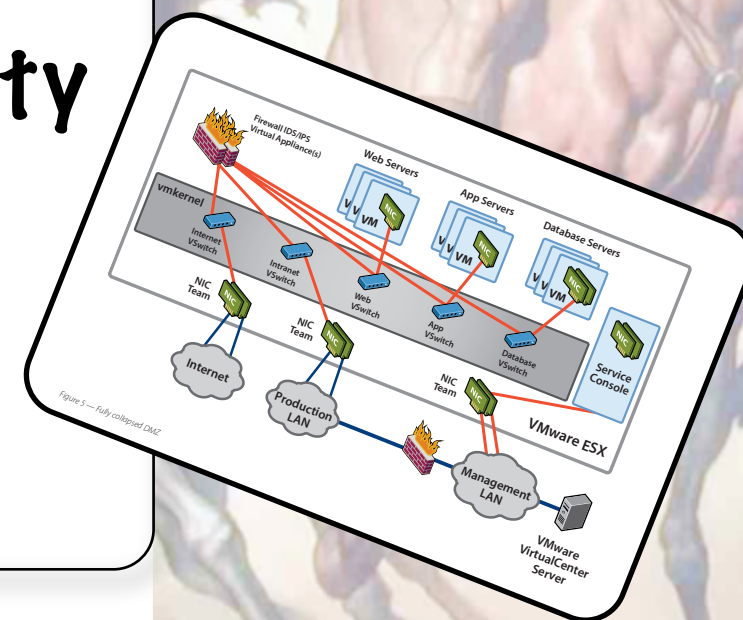
*Wikipedia



War I Episode 7: Revenge Of the UTM Clones

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

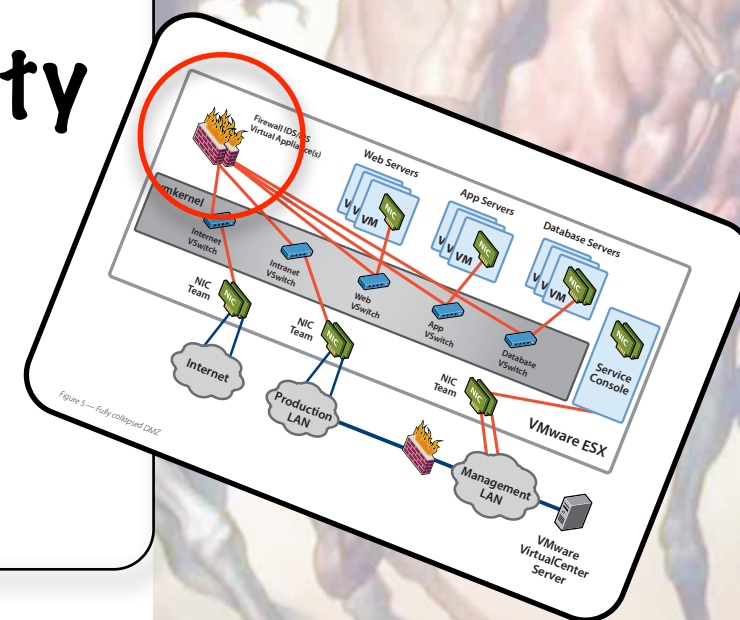




War I Episode 7: Revenge Of the UTM Clones

Monolithic security vendor virtual appliances are the virtualization version of the UTM argument:

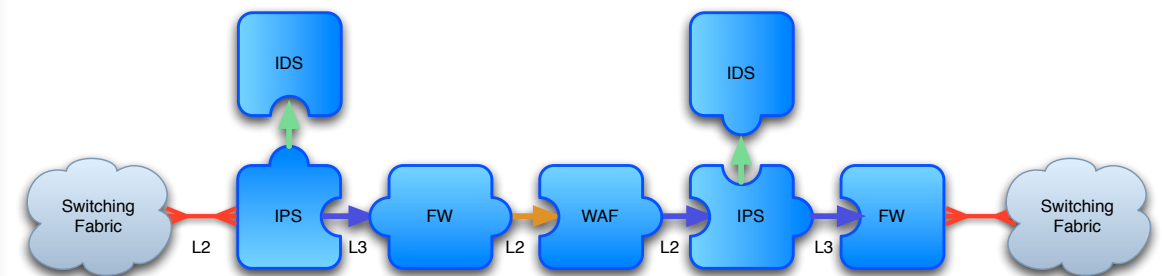
- ❖ The notion that we will deploy a single vendor/monolithic security VA in each host is silly
- ❖ If you're still stuck on "defense in breadth," you're going to deploy more than one security virtual appliances on each host
- ❖ UTM performance sucks when you flip all the switches





The VAUTM Conundrum

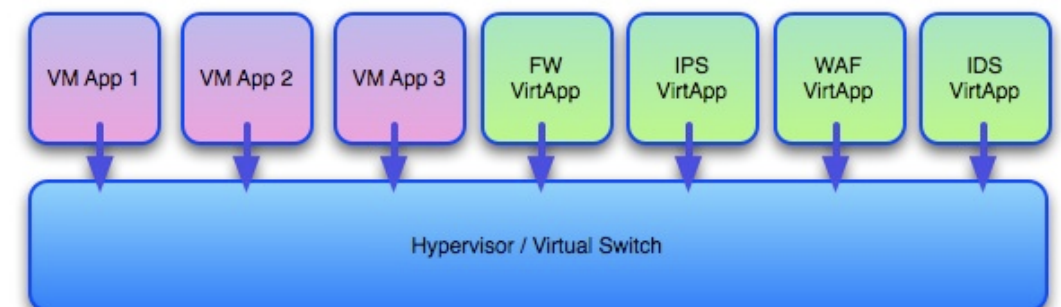
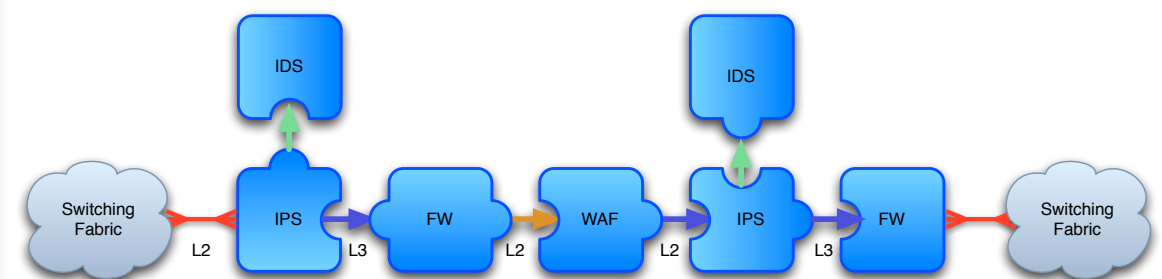
❖ How do you ensure that traffic is statefully directed to the appropriate individual in-line security bumps in the stack?





The VAUTM Conundrum

- ❖ How do you ensure that traffic is statefully directed to the appropriate individual in-line security bumps in the stack?
- ❖ The more security VA's you add, the less VM's you can service

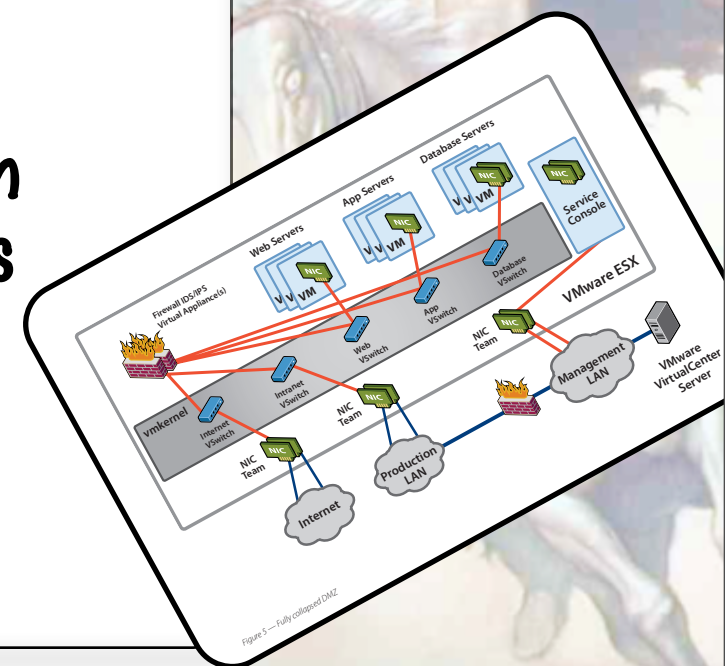




Pestilence | VirtSec Screws the Capacity Planning Pooch!

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

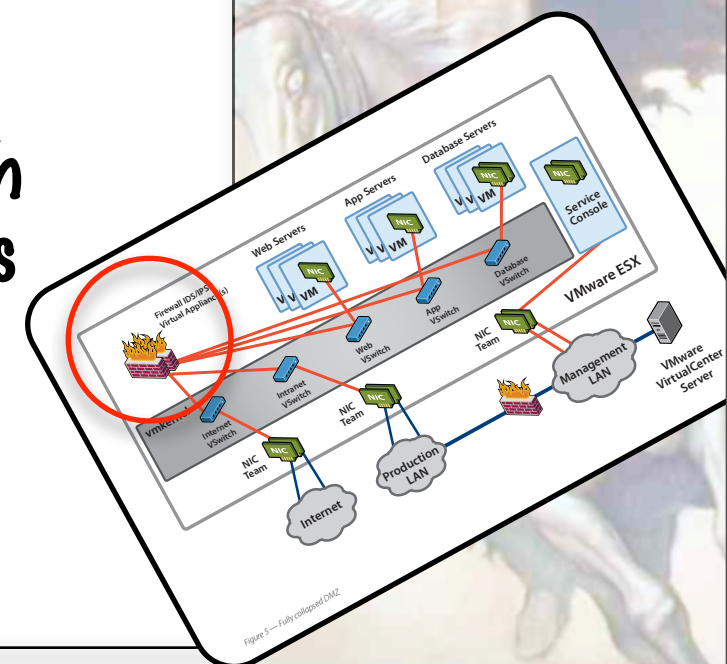
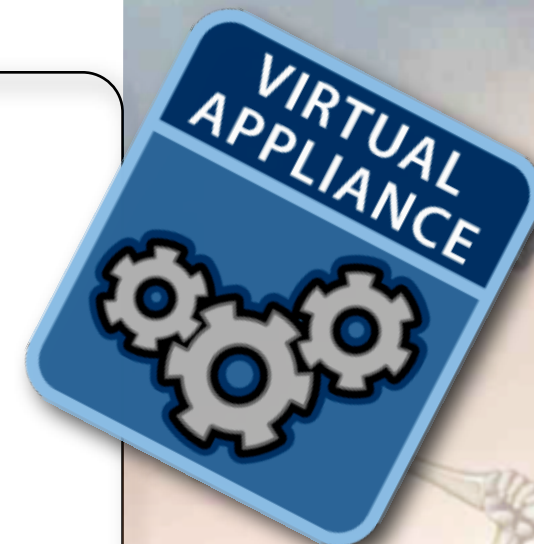




Pestilence | VirtSec Screws the Capacity Planning Pooch!

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

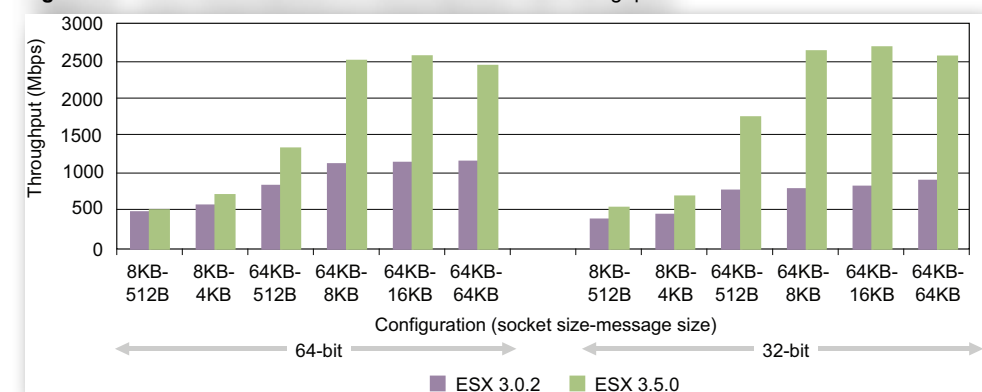




Drinking From the Firehose

- ❖ 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.

*Networking Performance VMware® ESX Server 3.5



Public Service Announcement

Every time you deploy a security virtual appliance...



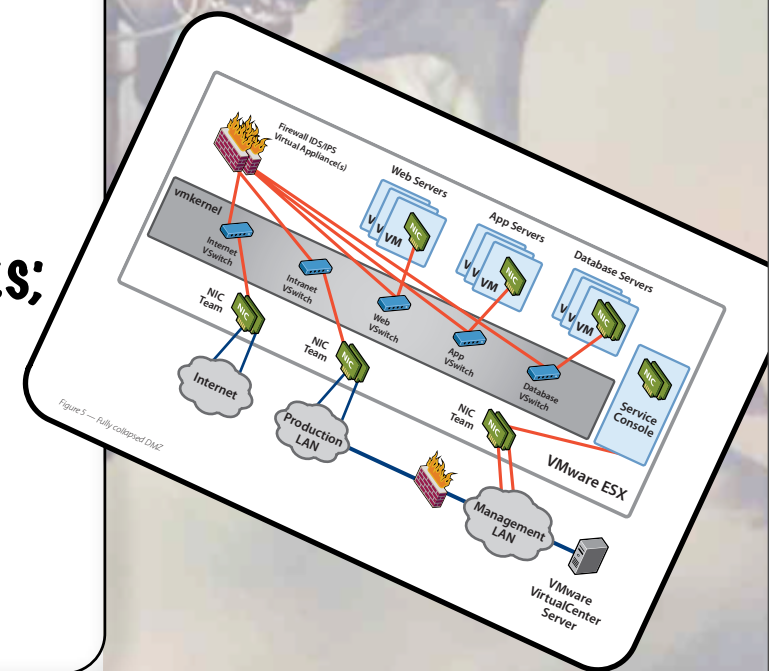
God kills a kitten.



Death | The Network Is The Computer?

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 options for stateful security applications currently suck

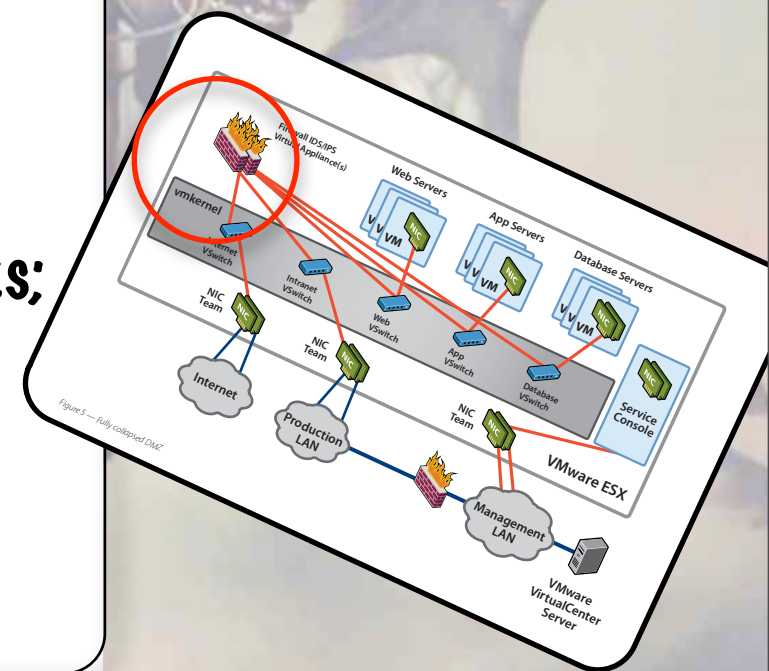




Death | The Network Is The Computer?

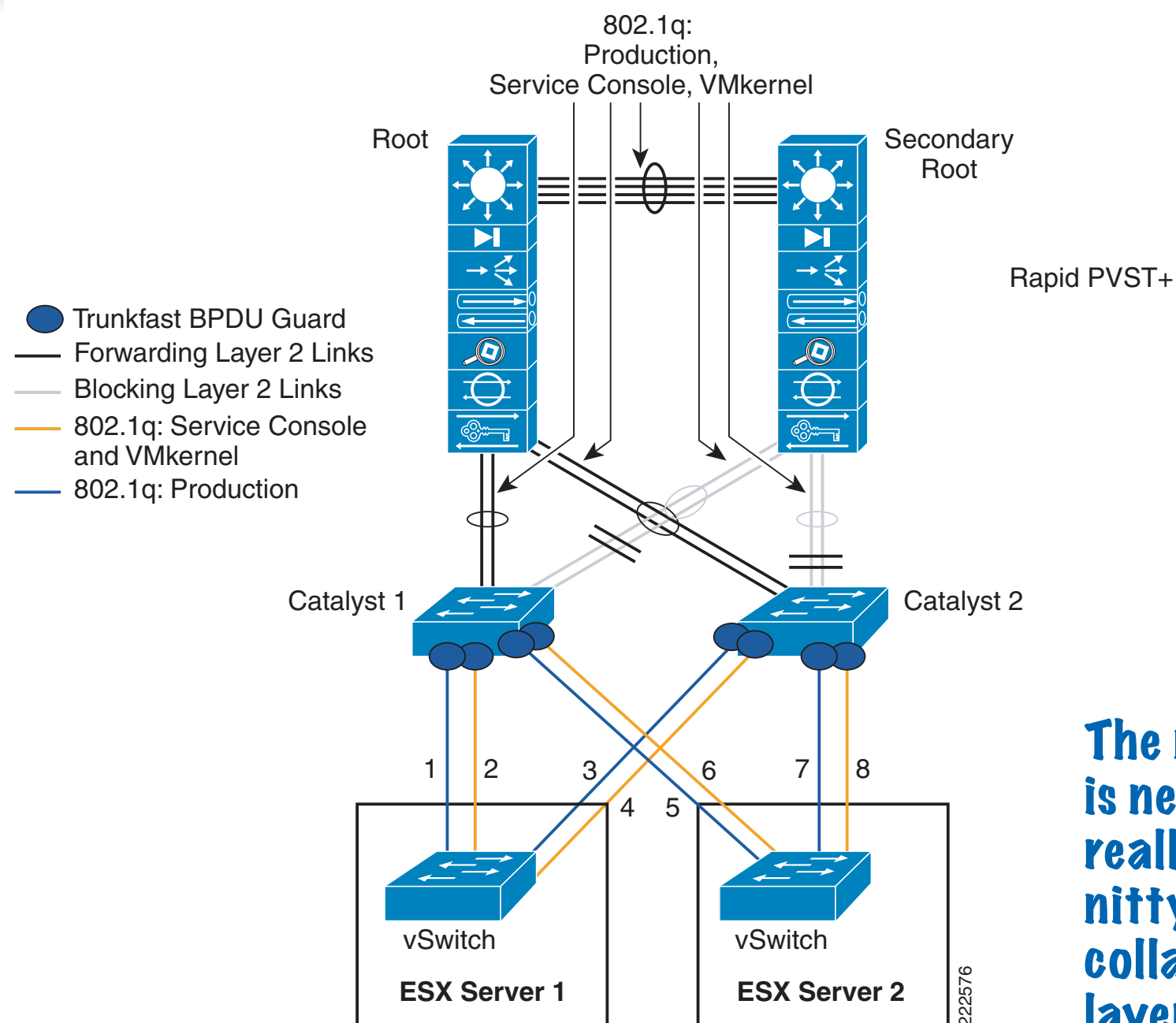
Replicating many highly-available security applications and network topologies in virtual switches don't work

- ❖ 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 options for stateful security applications currently suck





Resilient Network Designs Are Achievable



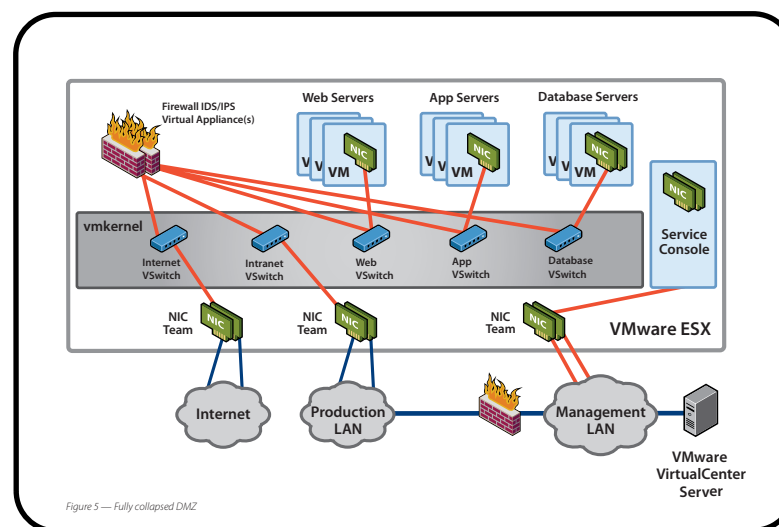
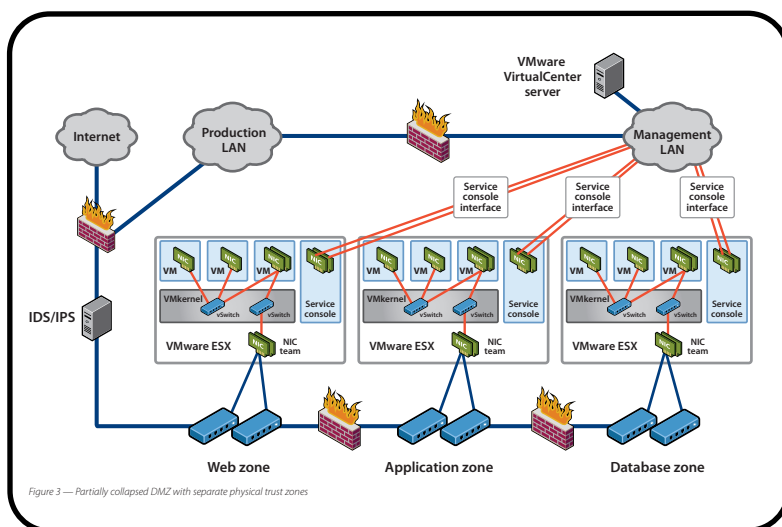
*Image from Cisco Whitepaper: VMware Infrastructure 3 in a Cisco Network Environment



...But the Security Application Failure Recovery Options Suck

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

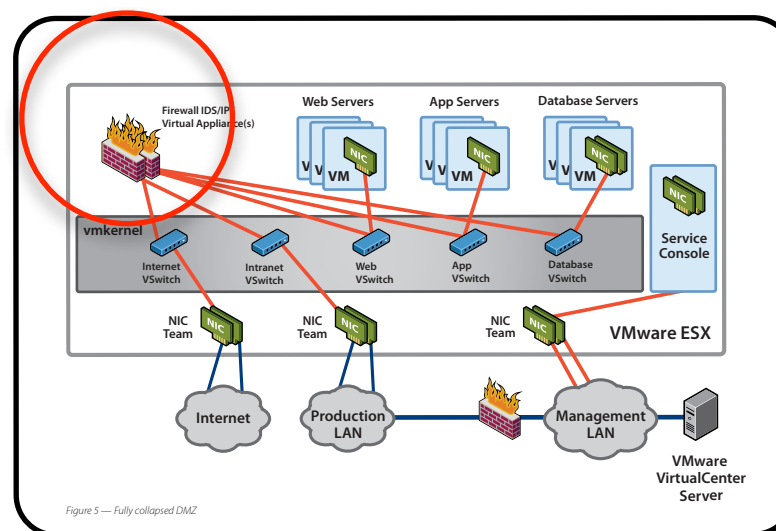
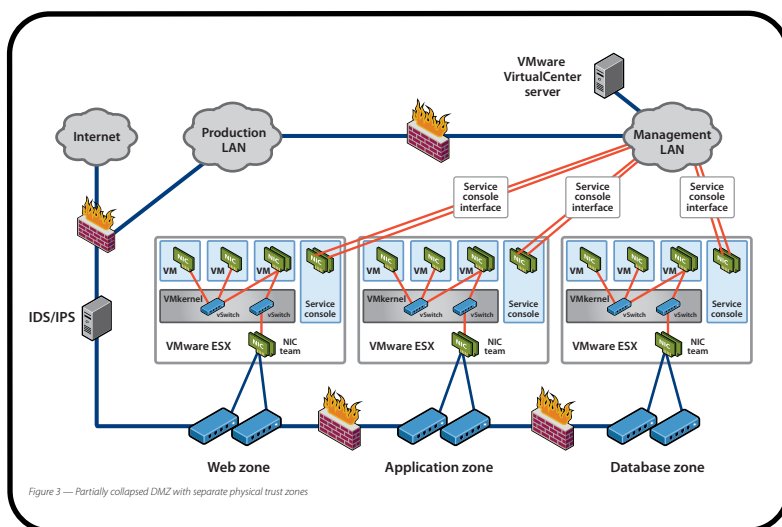




...But the Security Application Failure Recovery Options Suck

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





Run...It's the Fuzz!





Run...It's the Fuzz!

I was going to show you a really cool demo with ERNW using their modified L2 Sulley fuzzing framework abusing the HA protocols of a well-known firewall vendor to show you how fragile this stuff is in terms of performance/resiliency, but:





Run...It's the Fuzz!

I was going to show you a really cool demo with ERNW using their modified L2 Sulley fuzzing framework abusing the HA protocols of a well-known firewall vendor to show you how fragile this stuff is in terms of performance/resiliency, but:

- ❖ The version that runs under ESX doesn't utilize VRRP





Run...It's the Fuzz!

I was going to show you a really cool demo with ERNW using their modified L2 Sulley fuzzing framework abusing the HA protocols of a well-known firewall vendor to show you how fragile this stuff is in terms of performance/resiliency, but:

- ❖ The version that runs under ESX doesn't utilize VRRP
- ❖ The version that runs under ESX doesn't use the native clustering functionality





Run...It's the Fuzz!

I was going to show you a really cool demo with ERNW using their modified L2 Sulley fuzzing framework abusing the HA protocols of a well-known firewall vendor to show you how fragile this stuff is in terms of performance/resiliency, but:

- ❖ The version that runs under ESX doesn't utilize VRRP
- ❖ The version that runs under ESX doesn't use the native clustering functionality
- ❖ In fact, the version that runs under ESX doesn't support load balanced HA in any way...





Run...It's the Fuzz!

I was going to show you a really cool demo with ERNW using their modified L2 Sulley fuzzing framework abusing the HA protocols of a well-known firewall vendor to show you how fragile this stuff is in terms of performance/resiliency, but:

- ❖ The version that runs under ESX doesn't utilize VRRP
- ❖ The version that runs under ESX doesn't use the native clustering functionality
- ❖ In fact, the version that runs under ESX doesn't support load balanced HA in any way...

Get used to it, as no VirtSec virtual appliance vendor I've spoken to currently supports native HA/LB in the virtual appliance version of their products!





Reality Distortion Field

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



Reality Distortion Field

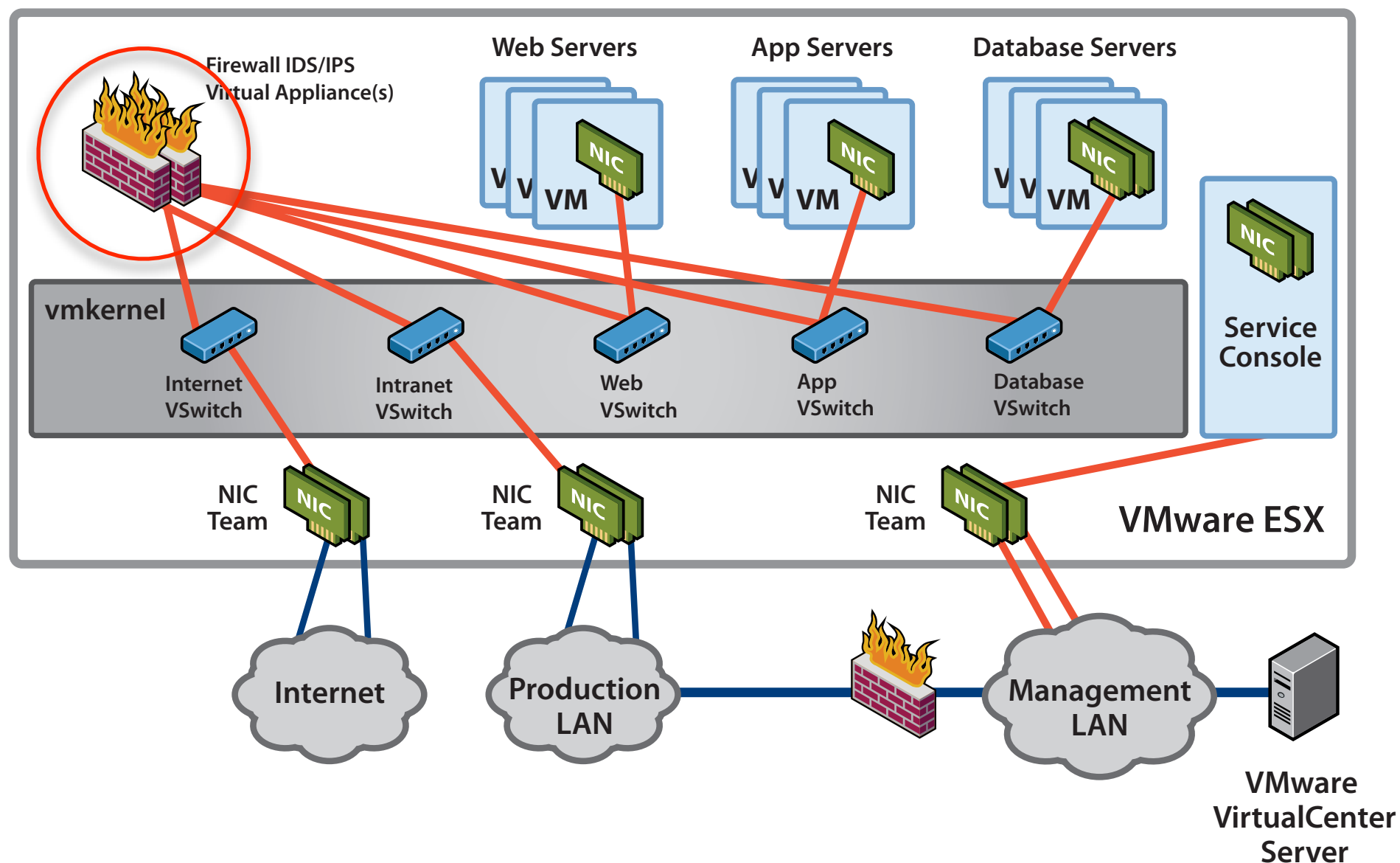


Figure 5 — Fully collapsed DMZ

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



Doh!

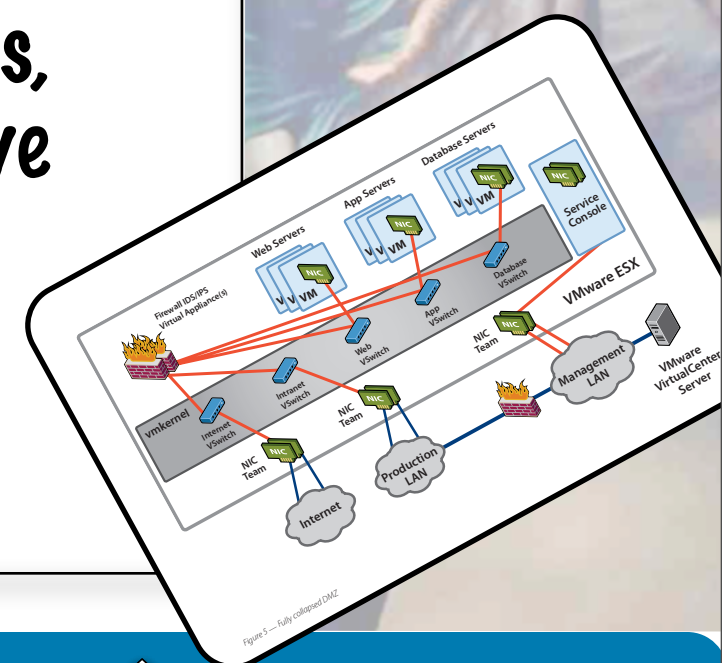




Famine | Spinning VM Straw Into Budgetary Gold

Virtualizing security will not save you money, it will cost you more

- ❖ We won't get rid of physical appliances or security line cards in switches, in fact, we'll probably have to buy more...
- ❖ We won't get rid of host-based security software
- ❖ That means that when we add VirtSec solutions, these solutions & their licenses are cost-additive
- ❖ As we add more solutions, we add complexity
- ❖ Who's going to administer these solutions?

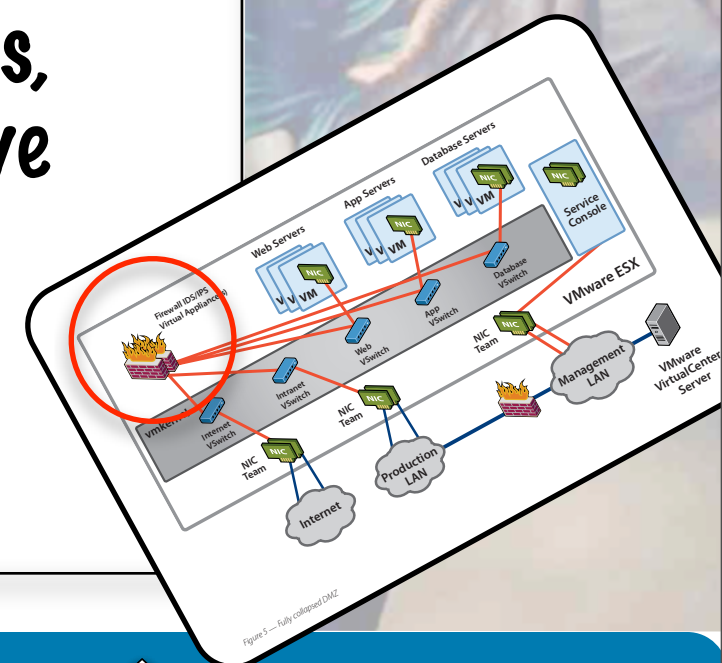




Famine | Spinning VM Straw Into Budgetary Gold

Virtualizing security will not save you money, it will cost you more

- ❖ We won't get rid of physical appliances or security line cards in switches, in fact, we'll probably have to buy more...
- ❖ We won't get rid of host-based security software
- ❖ That means that when we add VirtSec solutions, these solutions & their licenses are cost-additive
- ❖ As we add more solutions, we add complexity
- ❖ Who's going to administer these solutions?





Fear The Reapers!





Parting Is Such Sweet Sorrow

- ❖ Setup & Context
- ❖ x86 Virtualization Overview in 30 Seconds
- ❖ Virtual Networking Architecture
- ❖ VirtSec Solutions Landscape
- ❖ The Four Horsemen
- ❖ Wrap-Up



Great, So What Can I Do Today?





Great, So What Can I Do Today?

Guidelines:





Great, So What Can I Do Today?

Guidelines:

- ♣ Use risk assessment and threat modeling





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains
- ❖ Thoroughly evaluate existing and emerging tools to determine value vs. disruption





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains
- ❖ Thoroughly evaluate existing and emerging tools to determine value vs. disruption
- ❖ Dig deep on performance, HA/LB and scalability on virtual appliances





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains
- ❖ Thoroughly evaluate existing and emerging tools to determine value vs. disruption
- ❖ Dig deep on performance, HA/LB and scalability on virtual appliances
- ❖ Understand what impact VMotion, VRS, HA have on security solutions





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains
- ❖ Thoroughly evaluate existing and emerging tools to determine value vs. disruption
- ❖ Dig deep on performance, HA/LB and scalability on virtual appliances
- ❖ Understand what impact VMotion, VRS, HA have on security solutions
- ❖ Be able to quantify performance impacts on hosts/networks





Great, So What Can I Do Today?

Guidelines:

- ❖ Use risk assessment and threat modeling
- ❖ Design and provision your virtual network very carefully or find someone you can convince to do so
- ❖ Provide for zoned/screened VM's that are grouped based on risk/value requiring like policies and failure domains
- ❖ Thoroughly evaluate existing and emerging tools to determine value vs. disruption
- ❖ Dig deep on performance, HA/LB and scalability on virtual appliances
- ❖ Understand what impact VMotion, VRS, HA have on security solutions
- ❖ Be able to quantify performance impacts on hosts/networks
- ❖ Push virtualization platform providers to reveal roadmaps





Hope Is Not a Strategy, But It Doesn't Hurt





Hope Is Not a Strategy, But It Doesn't Hurt



♣ We need a trust model in hardware & software



Hope Is Not a Strategy, But It Doesn't Hurt



- ♣ We need a trust model in hardware & software
- ♣ We need affinity between the VM and protection schemes/policies



Hope Is Not a Strategy, But It Doesn't Hurt



- ❖ We need a trust model in hardware & software
- ❖ We need affinity between the VM and protection schemes/policies
- ❖ Centralized VM registration providing telemetry that controls spin-up, state and mobility capabilities regardless of vendor



Hope Is Not a Strategy, But It Doesn't Hurt



- ❖ We need a trust model in hardware & software
- ❖ We need affinity between the VM and protection schemes/policies
- ❖ Centralized VM registration providing telemetry that controls spin-up, state and mobility capabilities regardless of vendor
- ❖ Comprehensive discovery, profiling, dynamic configuration & security management of all VM's -- online or offline



Hope Is Not a Strategy, But It Doesn't Hurt



- ❖ We need a trust model in hardware & software
- ❖ We need affinity between the VM and protection schemes/policies
- ❖ Centralized VM registration providing telemetry that controls spin-up, state and mobility capabilities regardless of vendor
- ❖ Comprehensive discovery, profiling, dynamic configuration & security management of all VM's -- online or offline
- ❖ Intelligent networking capabilities within the virtual switching infrastructure for consistency, visibility and security including integrated virtual network admission control & access Control (vNAC)



Hope Is Not a Strategy, But It Doesn't Hurt



- ❖ We need a trust model in hardware & software
- ❖ We need affinity between the VM and protection schemes/policies
- ❖ Centralized VM registration providing telemetry that controls spin-up, state and mobility capabilities regardless of vendor
- ❖ Comprehensive discovery, profiling, dynamic configuration & security management of all VM's -- online or offline
- ❖ 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



Vini, Vidi, Wiki...



- ❖ **Monolithic security vendor virtual appliances are the virtualization version of the UTM argument**
- ❖ **Virtualized Security can seriously impact performance, resiliency and scalability**
- ❖ **Replicating many highly-available security applications and network topologies in virtual switches don't work**
- ❖ **Virtualizing security will not save you money, it will cost you more**



Thanks For Not Leaving :)



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>