CROSSBEAM® SYSTEMS

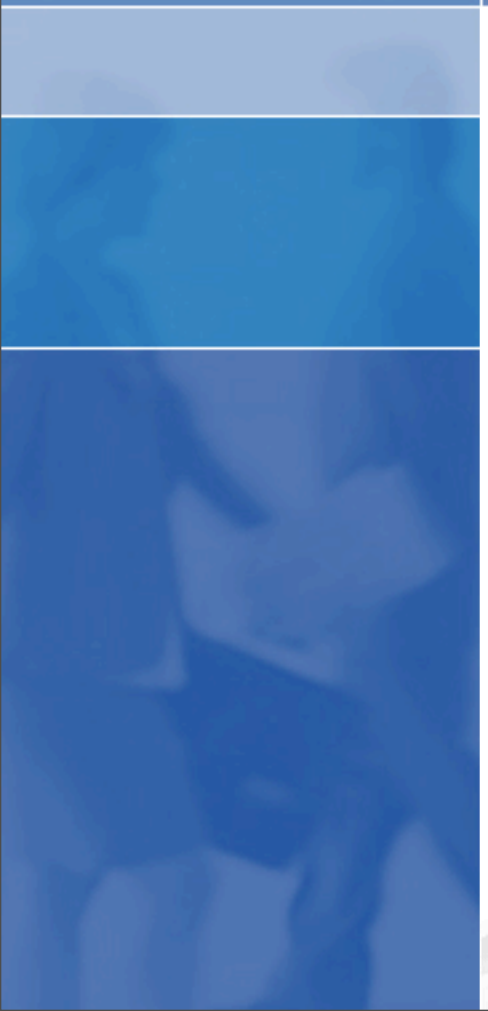
We secure the world's largest networks.

Virtualization & the End Of Network Security As We Know It.

...the Feel Good Hit of the Summer

Christofer Hoff, CISSP CISA CISM
Chief Security Strategist

April 2007 Charlotte ISSA Event



VIRTUALIZATION

Talking Points

- Virtualization: Floor Wax & Desert Topping
- Woot! Virtualization Rocks!
- But Mama says “Virtualization is da Devil!”
- Today’s Risk Model is Kaput!
- Threats, Vulnerabilities & Hype
- The Network *is* the Computer - Self Defending?
- Pragmatism & Perspective: Taking Action
- The Quest for the Holy Grail - VM Security
- I’m OK, You’re OK.

Virtualization: Floor Wax & Desert Topping

- Virtualization is really about two things:
  - Time
  - Money

- Virtualization is often technically defined as:

> "...an abstraction layer that decouples the physical hardware from the operating system to deliver greater resource utilization and flexibility"

Virtualization Concepts

- Server
- Client
- Network
- Storage
- Files
- Policy
- Access
- Application
- Operating System

Platforms

- Partitioning
- Isolation
- Encapsulation

Resources

Virtualization Concepts : Partitioning

- Server
- Client
- Network
- Storage
- Files
- Policy
- Access
- Application
- Operating System

- **Partitioning**
  - Multiple applications, networks and operating systems can be supported within a single physical system
  - Multiple physical machines can be consolidated into virtual machines on either a scale-up or scale-out architecture
  - Computing and network resources are treated as a uniform pool to be allocated to virtual machines in a controlled manner.

Virtualization Concepts : Isolation

- Server
- Client
- Network
- Storage
- Files
- Policy
- Access
- Application
- Operating System

- **Isolation**
  - Virtual machines are completely isolated from the host machine and other virtual machines
  - If a virtual machine abends, others are unaffected.
  - Data does not leak across virtual machines and applications can only communicate over configured connections

Virtualization Concepts : Encapsulation

- Server
- Client
- Network
- Storage
- Files
- Policy
- Access
- Application
- Operating System

- **Encapsulation**
  - Complete virtual machine environments are saved as a single image; easy to move, copy, backup and restore
  - Standardized virtualized hardware is presented to the application, allowing for transparent compatibility

Woot! Virtualization Rocks!

- Physical Consolidation
- Cost Reduction
- Ease and flexibility of Provisioning
- On-demand Resource Pooling
- Disaster Recovery
- Capacity on-Demand
- Application Availability
- Management of Service Levels

- Easy Backup
- Fault Tolerance
- Eases Application Lifecycle Management
- Provides Development Efficiencies
- Allows for ubiquitous Computing
- Application Portability
- Secure computing environments...

But Mama Says "Virtualization Is Da Devil!"

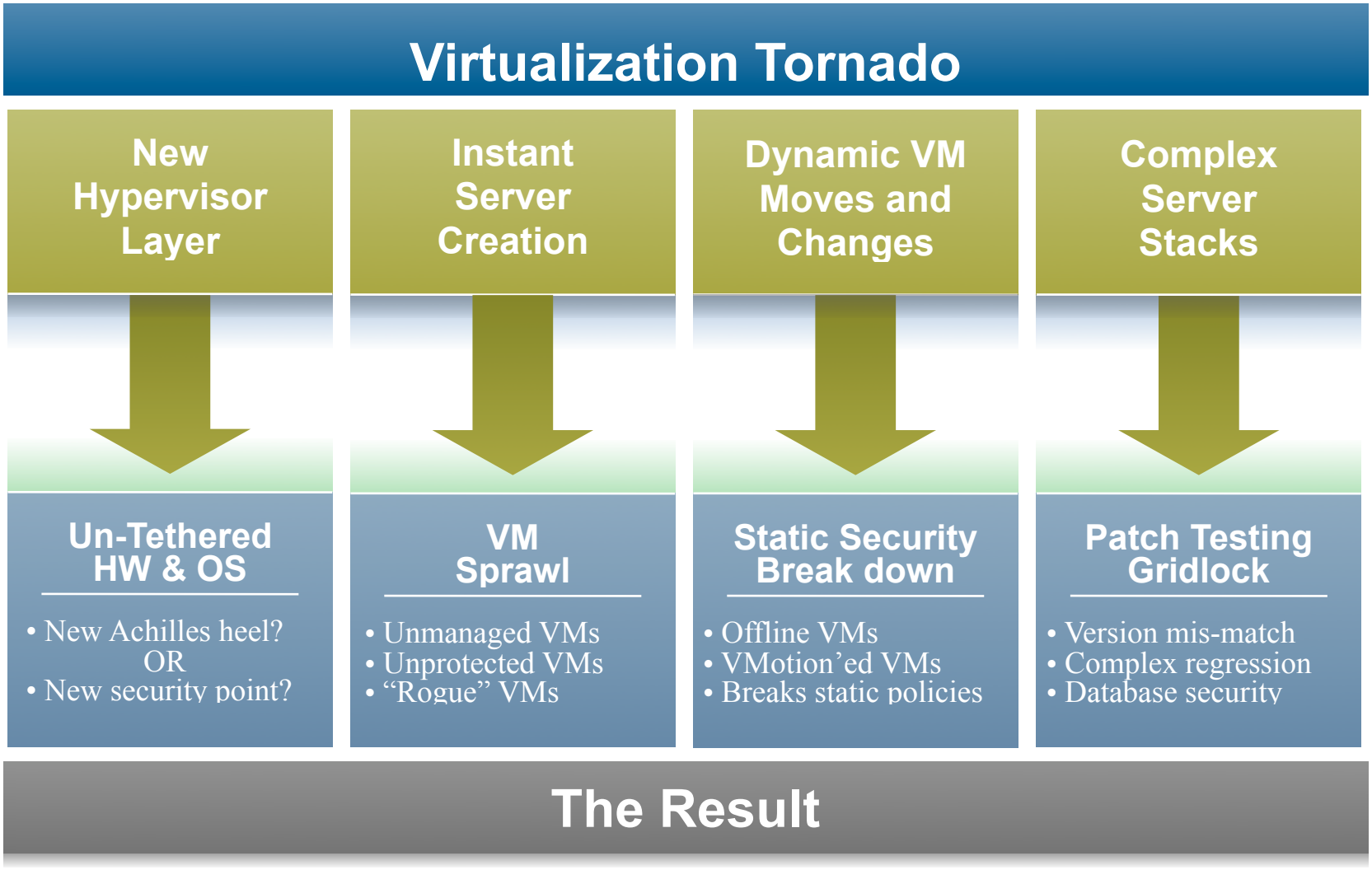
- Virtualization changes the way resources & networks are:
  - Designed
  - Provisioned
  - Administered
  - Patched
  - Recovered
  - Assessed
  - Protected
  - Audited

- ...and how all this data is:
  - Created
  - Stored
  - Controlled
  - Accessed
  - Destroyed
  - Backed up, and
  - **Secured**

Today's Risk Model of Today is Kaput!

- Virtualization takes every issue we have today in security and amplifies them.
- Hard on the outside and even more gooey in the middle! One moat, lots of castles
- We now must factor the incredibly dynamic nature of virtualization into our assessment of overall risk
- Operational risk becomes even more important
- The attack surfaces multiply exponentially, as do the threat vectors
- The ability to manage risk requires a new suite of technology, skills and expertise

Virtualization Makes Simplicity Complex (?)

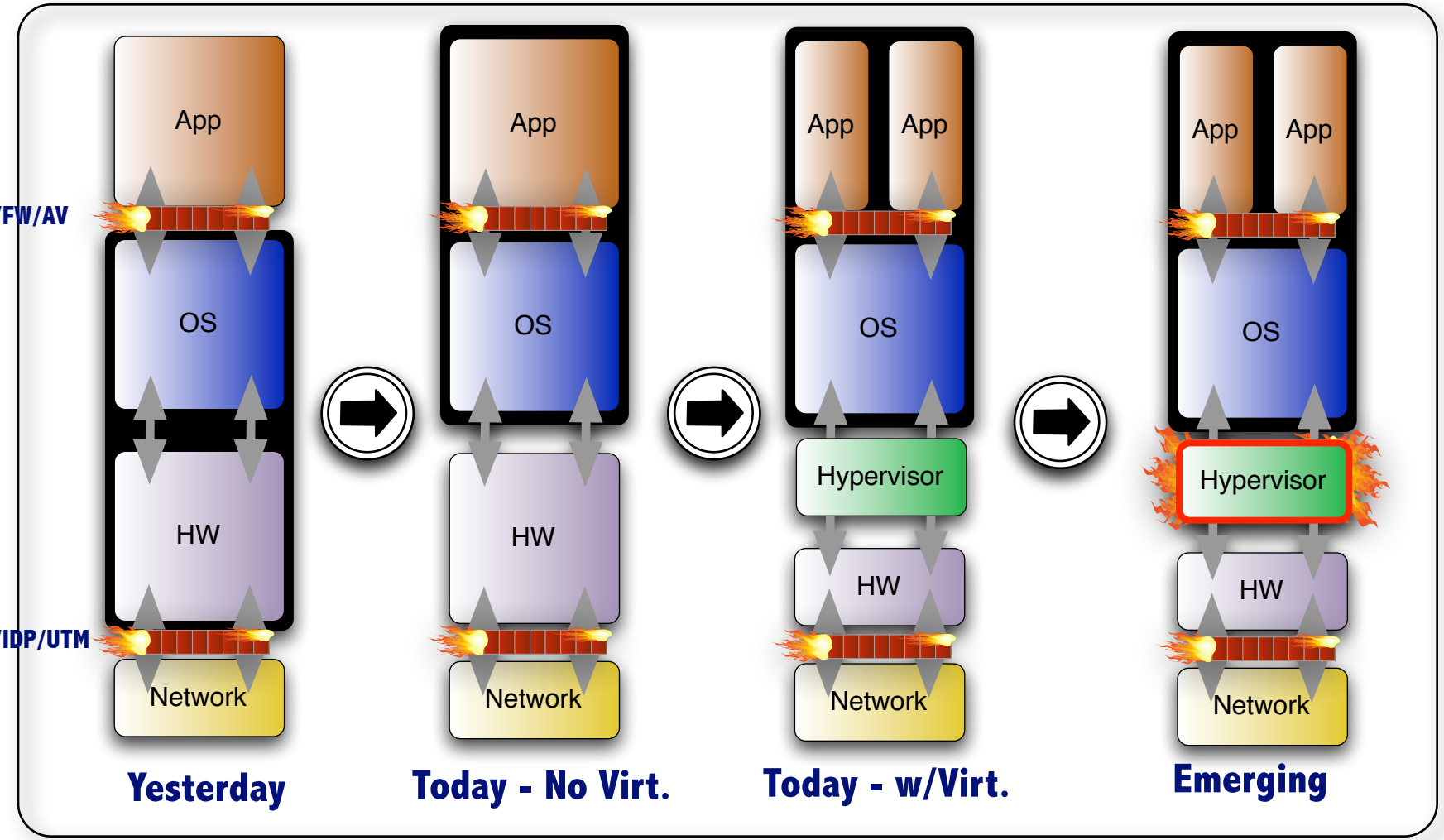


Slide Courtesy of: BlueLane

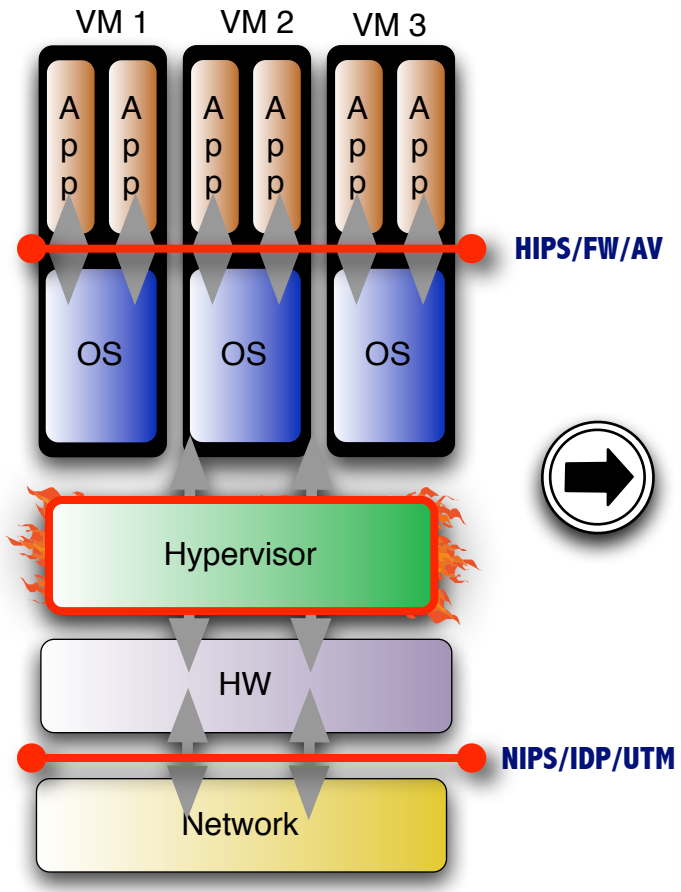
Threats, Vulnerabilities & Hype

- Theft of an intact VM
- Vulnerability Management Lifecycle
- Hypervisor Compromise
- Chipset Malware (Blue pill)
- Management Complexity
- Denial of Service(s)
- Botnet Bait!
- Rogue VM's
- Attack surface virtually expands
- Let's add Web2.0/SOA to the Mix...

AppStack Security Decomposed...

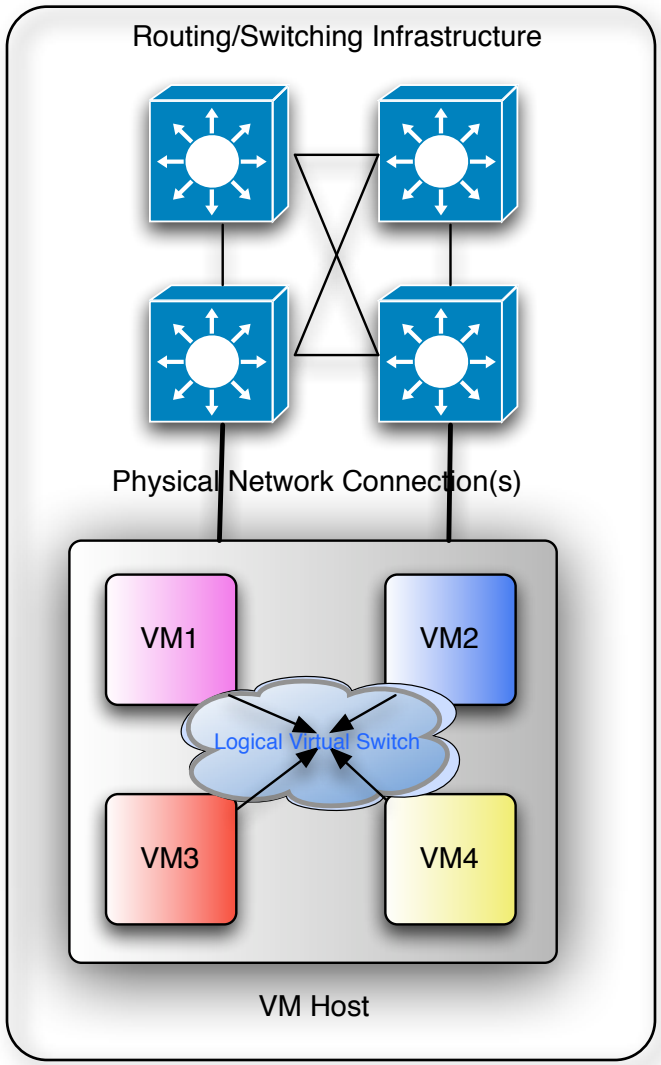


The “New” Model Explored



- Still requires legacy defense in depth solutions
- Introduces a need for a dedicated security layer between hypervisor and guest VMs irrespective of OS
- Provides “Micro-Perimeter” around VM’s providing policy-driven “network-like” enforcement
- Still requires hardware & software “rootkit” detection and evasion countermeasures
- Introduces another distributed security service layer with multiple instantiations of policy across hosts

The Network *is* the Computer - Self Defending?



- Let's say that we have a single physical host which is connected to the physical switched network via Gb/s Ethernet
- Further, we have 4 VM's in a that single physical host each representing components of an application stack
- The bulk of communications are between the the VM's utilizing intra-VM communications across the virtual switch fabric and does not touch the physical network
- Thus, the network ***is*** the computer
- **How does the "network" supposedly self-defend when it's not even used? The "network" by itself is not the answer...from *any* vendor**

Pragmatism & Perspective: Taking Action

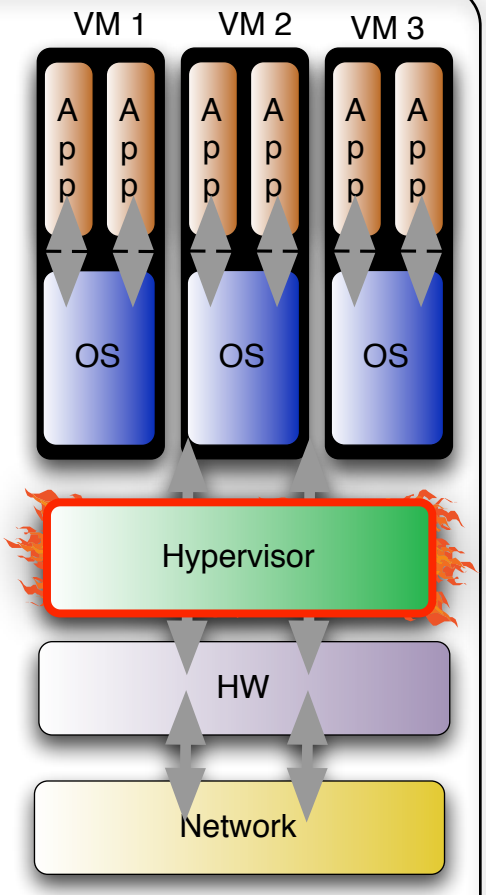
CHALLENGE	RESPONSE
OK, so how do I secure a virtualized data center?	Segmentation works. Virtualize the network topology and the security appliance so that any service can be applied to any endpoint or set of endpoints no matter where they are.
Does virtualization of security services simplify or make more complex the already complex network?	By virtualizing the actual security service and divorcing it from a specific hardware instance, the service can be moved to those processing point(s) best adapted for the service.
How can virtualization address improve reaction times to new vulnerabilities?	When the network topology and the appliance instance are virtualized a new service can be applied to any boundary transition simply via policy.

Pragmatism & Perspective: Taking Action

CHALLENGE	RESPONSE
What about securing the applications?	Integrate the application workflow into the overall security workflow; if you don't know how your applications work today in a flat network, you're sunk in a virtualized world.
What Do Web2.0/SOA technologies mean to virtualized environments?	it makes it harder to secure; not necessarily because there are more "vulnerabilities" but because the threat surface expands.
This sounds nasty, what should I start doing today?	Use what you already have, apply common sense, and press forward with new approaches to managing risk

How to Secure the VM Host/Guest OS Today

- Options:
  - Virtualize IDP at the VS Level
  - Adopt the virtual appliance model and add Security functionality (software) within the guest VM
  - Monitor inter and intra-VLAN traffic as much as possible
  - Provide security inside/around the hypervisor:
    - Provides an abstracted security service layer between VM's
    - Enforce policy at the "network layer" between VM instances
    - Provide for vulnerability shielding for containment
    - Application aware for contextual security disposition
  - **All of the above...**



How to Secure the Networks Hosting the VM Today

- Options:
  - Segment your network based on criticality, function or access
  - Defense-in-"duh"-Depth
  - Deploy embedded security across the network infrastructure
  - Integrate Host & Network Protection Schemes and tie in telemetry
  - Deploy Security as a best-of-breed overlay Virtualized Service Layer
  - Monitor, monitor, monitor
  - **All of the above**

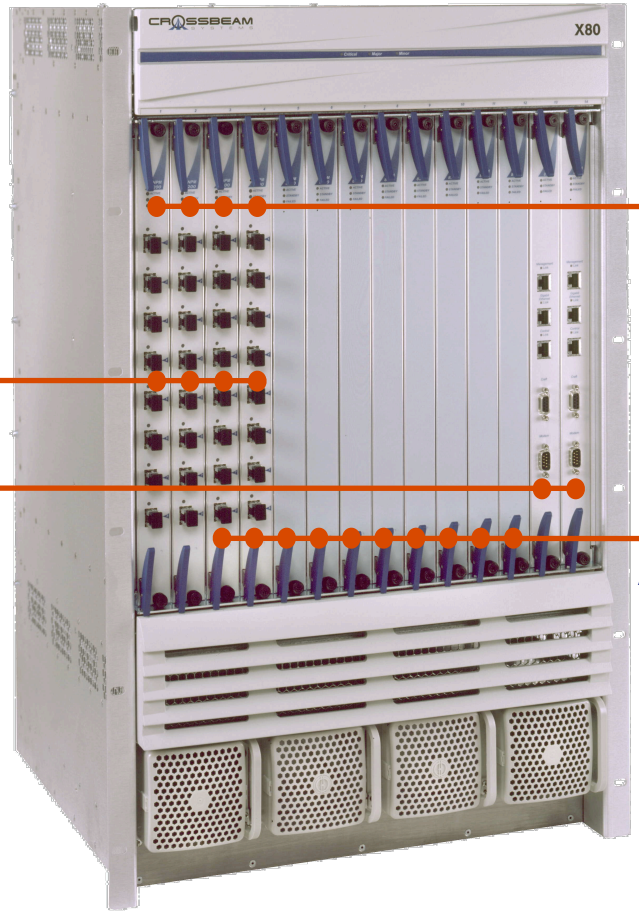
Securing Virtualization by Virtualizing Security

Network Processing Modules (NPMs)

- Up to 4 modules
- Provides Physical connectivity
- Network Processors that provide for intelligent flow classification and load balancing across APMs
- QoS and flow manipulation

Control Processing Modules (CPMs)

- Dual, redundant modules
- Provides secure management of chassis
- Applications installed here
- Provides interactive health checking of all modules



Backplane

- Dual non-blocking interconnects
- Dual, redundant multi-gigabit data links between all modules
- Redundant control links between all modules
- Cell-based Architecture

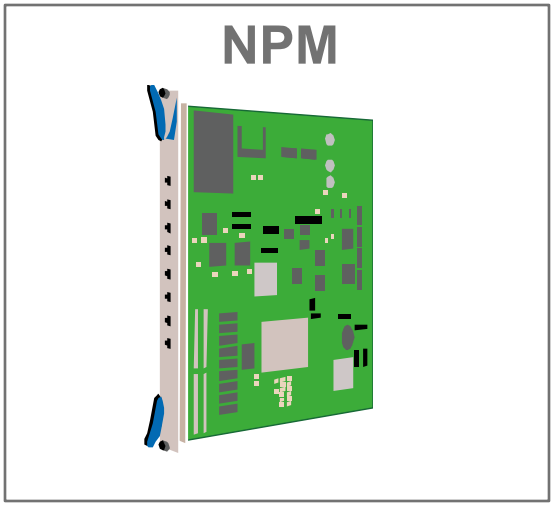
Application Processing Modules (APMs)

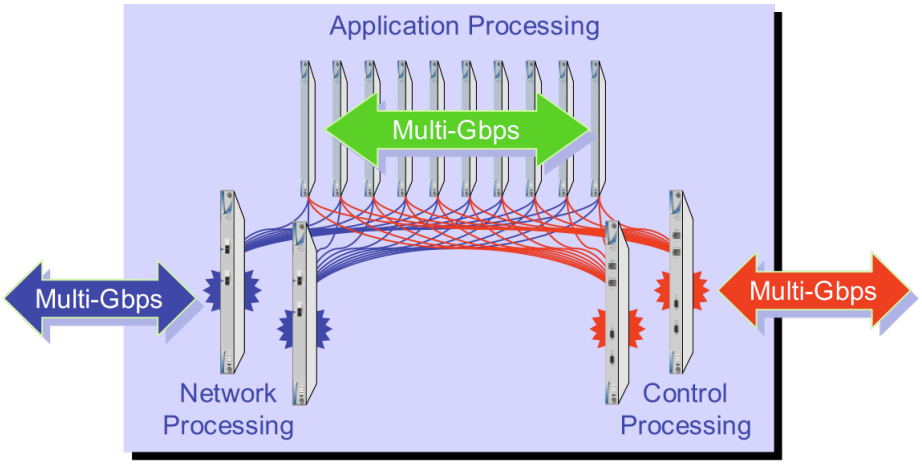
- Up to 10 modules
- Crossbeam-hardened Linux OS
- Generic Application Resource: No affinity of security applications to specific hardware
- Multiple simultaneous applications & multiple Linux kernels
- Self-Healing

A Practical Approach to Securing Virtualized Environments from the Bottom Up

Virtualization of Network Topology (HW)

The Network Processing Module (NPM) is a hardware device consisting of external interfaces, a telco class switch fabric, high speed NPUs and RISC processing elements. The NPM runs an embedded, proprietary operating system. The NPM is not addressable and cannot be fingerprinted.





Up to four independent data fabrics, two independent control fabrics

The NPM classifies flows, applies QoS parameters and load-balances flows via serialization or parallelization to virtualized interfaces and applications on the APMs.

Virtualization of Network Topology

- External interfaces on NPM are virtualized for the rest of the system
- Virtual interfaces may appear on one or multiple APMs (Fig. 1-3)
- Even VLANs can be virtualized!
- Interface properties like link aggregation are even virtualized (Fig. 3)

Interface Virtualization (VND)

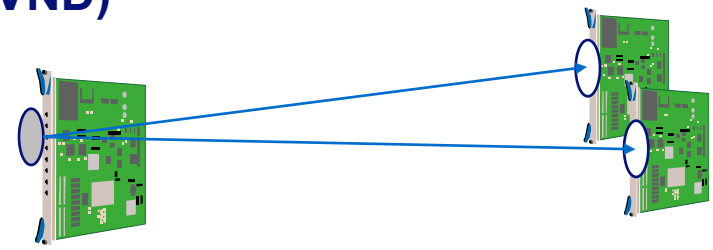


Fig. 1: One to many

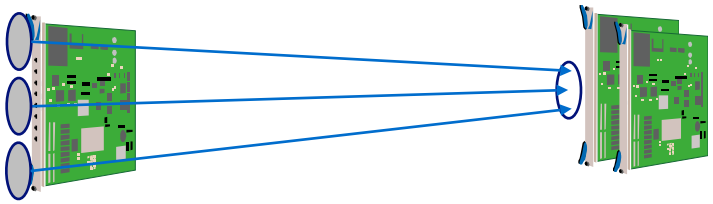


Fig. 2: Many to one

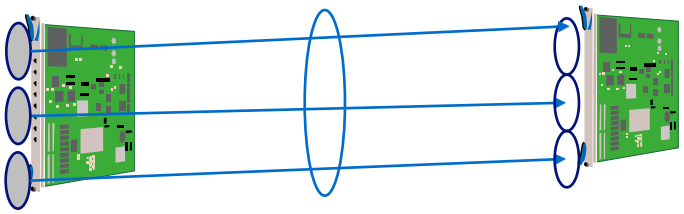
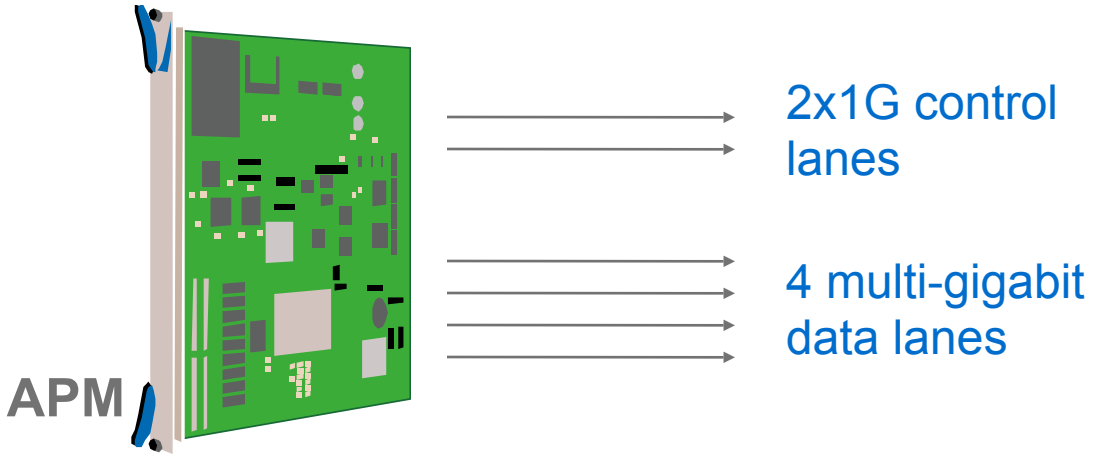


Fig. 3: Many to many

Virtualization of Software: the APM

The Application Processing Module (APM) is a hardware device consisting of high speed Intel Xeon processors and multiple storage and security acceleration slots.

The APM has no inherent profile. Its profile is virtualized and dynamically applied based on policy.

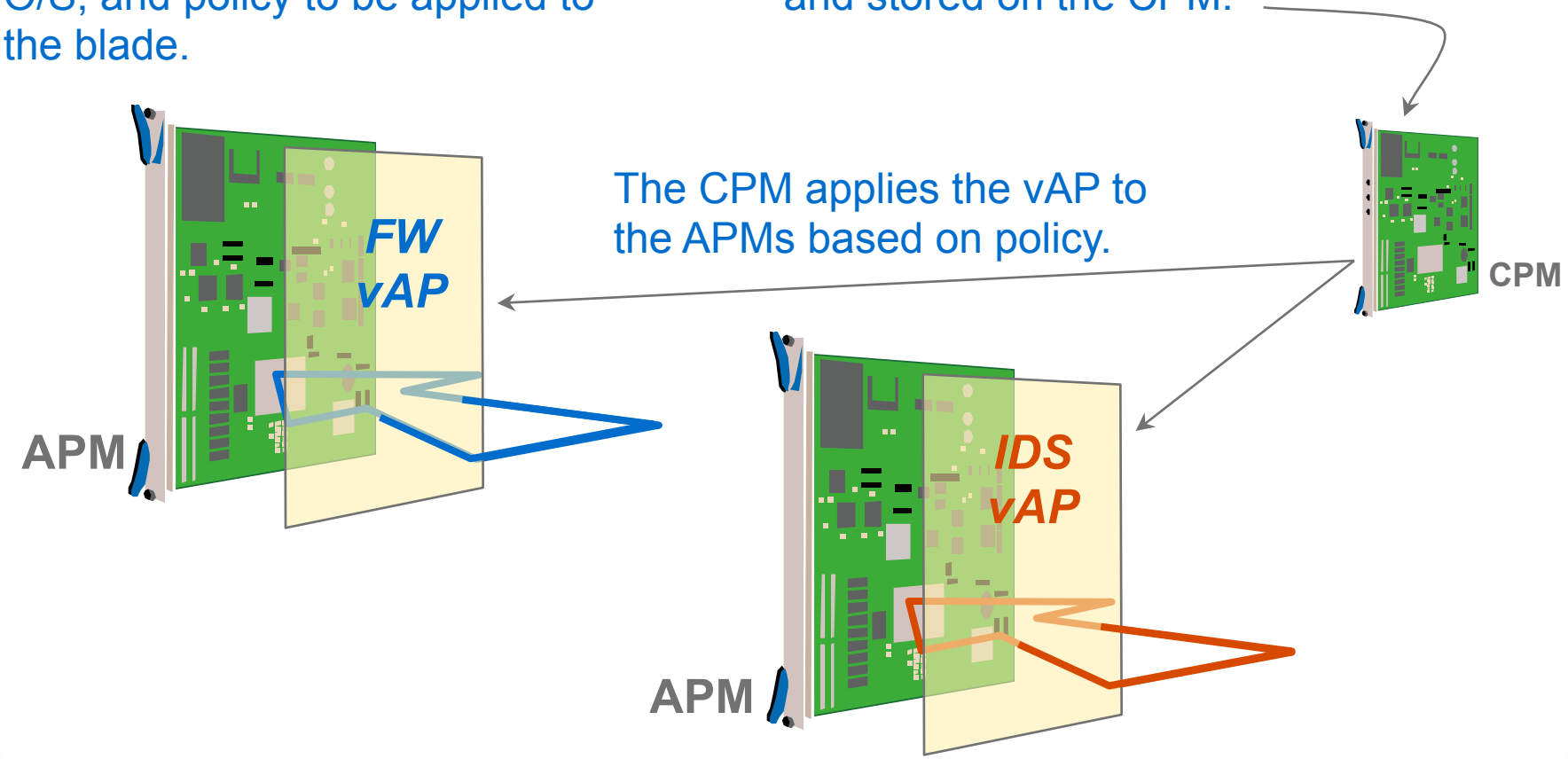


The APM is connected via on-board switches to the data path and, separately, to the control path. Its sole purpose in life is to apply security controls at wire speed.

Virtualization of Software: vAPs

A **v**irtual **A**pplication **P**rocessor (vAP) consists of the software, O/S, and policy to be applied to the blade.

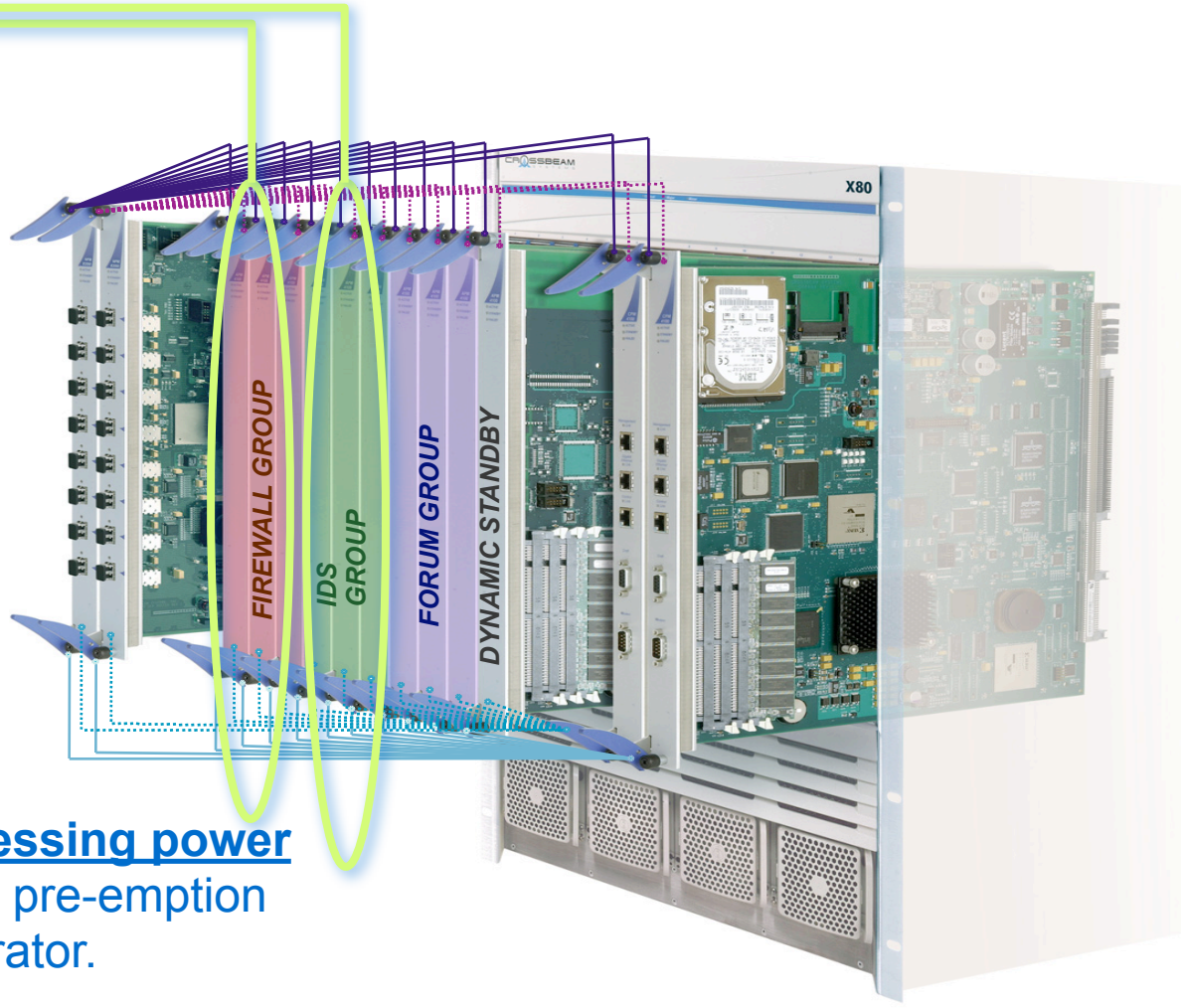
All vAPs are created via a management application and stored on the CPM.



Virtualization of Software (vAP Groups)

A single vAP may be applied to multiple APMs to form **a vAP Group** in which all members act exactly the same.

If an APM (hardware) in one vAP group fails, a dynamic standby can be **automatically profiled** with the vAP of the failed APM to restore capacity.

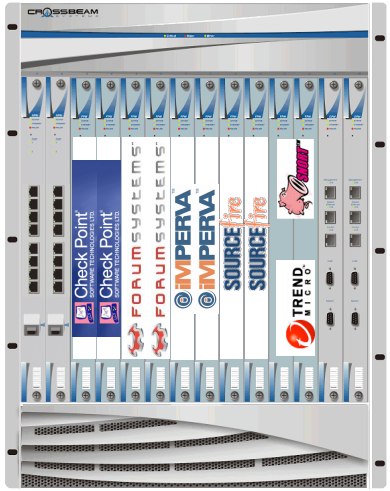


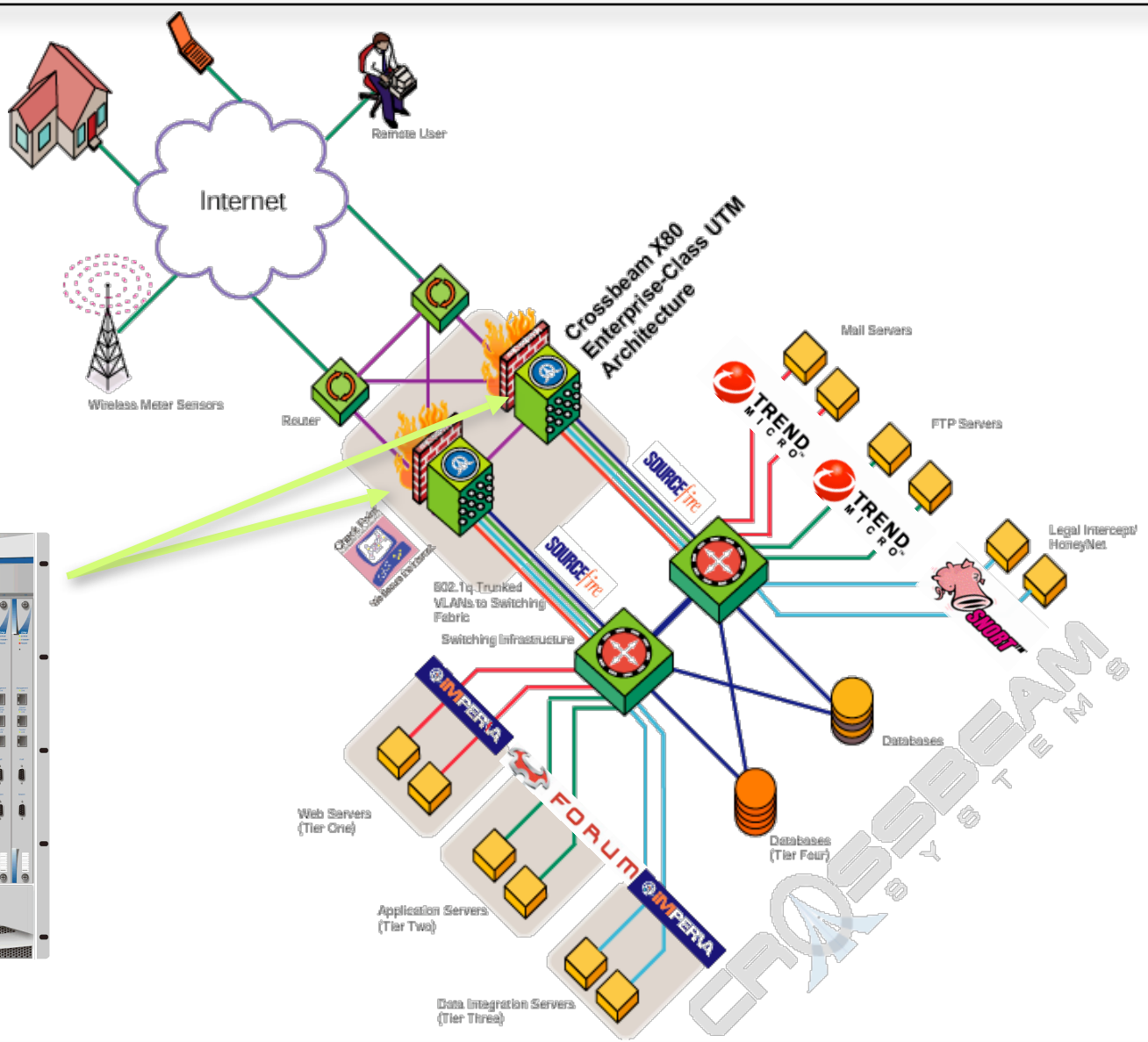
vAPs may "borrow" processing power from other blades based on pre-emption policies set by the administrator.

Virtualization of Policy

- Policy virtualization is also called “multi-domain support”
- Policy virtualization combines network topology and software virtualization with the security application vendor’s ability to “carve” up a single software entity into multiple, independent domains.
- Sourcefire MDE, ISS Proventia or Check Point VSX are examples of multi-domain support.

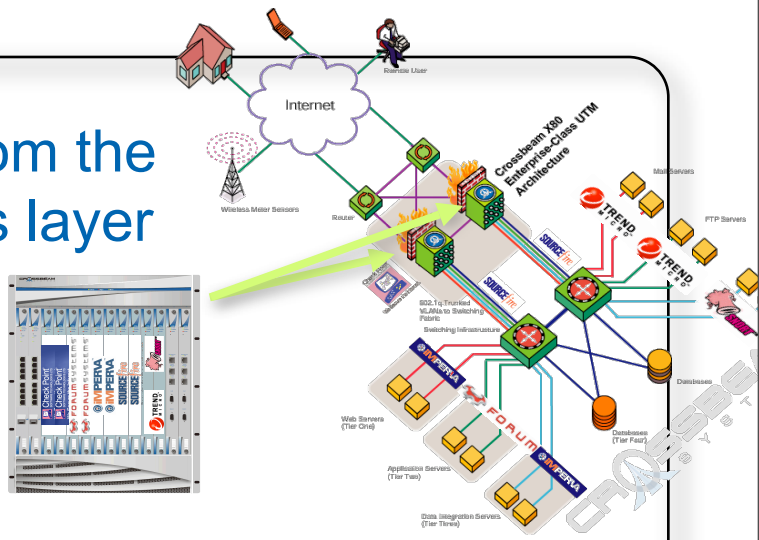
Virtualization (Network, Software & Policy) In Action





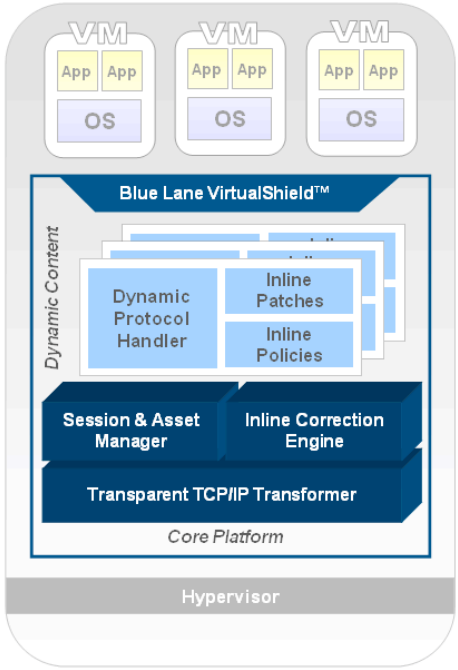
But What Happens Today When I Add Virtual Hosts?

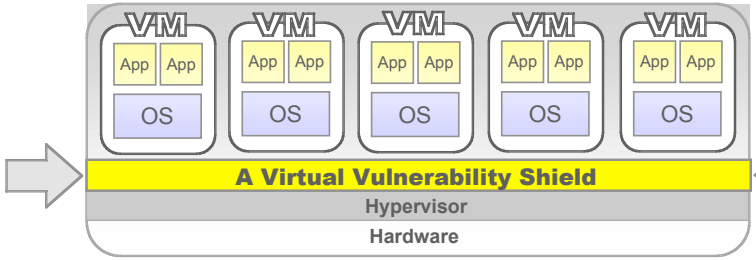
- The model doesn't change much from the virtualized network security services layer perspective:
  - Provision the VM on the Host.
  - Configure the Virtual Switch and IP subnet assignment to place the VM in the right VLAN
  - Configure the flow provisioning capabilities of the overlaid security services switch to force intra-VLAN traffic through vAP groups
  - Configure the virtualized network security policies across the service layer
  - **Deploy and activate Virtual Vulnerability Shielding and/ or VS IPS across the VM's...**



BlueLane's Vulnerability Shielding

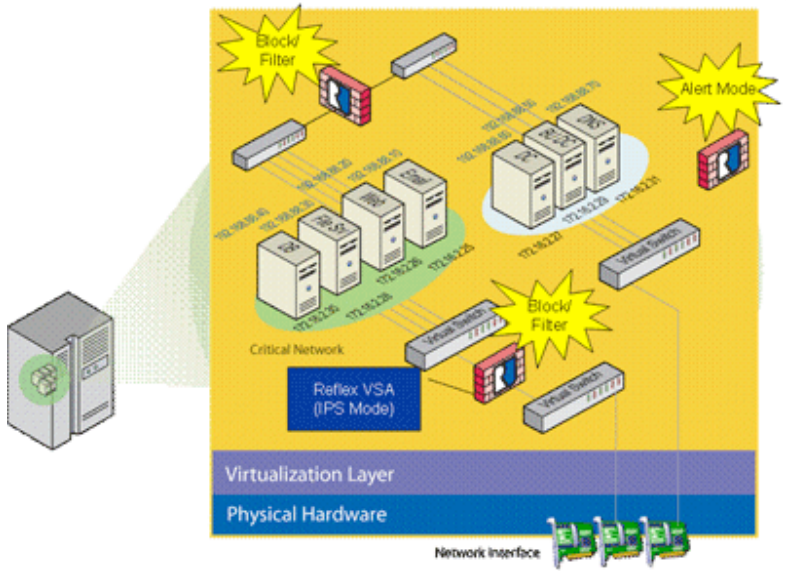
- Somewhat controversial - IPS and virtual patch emulation for the Hyper-visor or new approach?
- BlueLane's VirtualShield:
  - Purpose-built virtual appliance
    - No hardware assist required
    - Zero packet copies through appliance
    - Tight integration with the hypervisor
  - High-performance core platform
    - High throughput, low latency
    - Full session context & protocol decode
    - Integrated with Virtual Center
  - Dynamically loadable content
    - Breadth of coverage options
    - On-demand assignment & execution
  - Security function consolidation
    - Vulnerability detection/correction
    - App & server-specific policies
    - User, usage-based access control





Reflex's Virtual IPS for the VS

- Reflex VSA
  - Access firewall for permission enforcement for intra-VM and external network communication
  - Intrusion Prevention with inline blocking and filtering for virtual-ized networks
  - Anomaly, signature, and rate-based threat detection capability
  - Network Discovery to discover and map all virtual machines and applications
  - Centralized configuration and management console, comprehensive reporting tools, and real-time event aggregation and correlation



The Quest for the Holy Grail - Total VM Security

- We need affinity between the VM and protection schemes; security moves with the VM
- Centralized VM registration providing physical Hardware/VM Registration Services that prevents VM spin-up without authorization
- Agent and Agent-less discovery, profiling, dynamic protection of all VM's (think NAC on steroids - interacting with the hosts/network)
- Integrated Network Admission Control & Network Access Control with integrated IAM
- Strong authentication brokered for component access
- Behavioral Anomaly Detection (network & content)
- Rootkit Detection for both hardware and software layers
- Correlation of telemetry between VM Management and security planes
- Separate and secure control/data paths
- **Tie in network security functions, host controls and VM/ Hypervisor defenses into a consolidated single pane of glass for virtualized management**

I’m OK, You’re OK.

- Follow your virtualization environment provider’s guidelines for security.
- Apply at least the same strategies to your VM’s that you use for your non VM environments
- Segment your network; isolate by function, criticality and security
- Treat each VM Host as a perimeterized DMZ
- Monitor and extract really good telemetry and instrumentation
- Baseline your network NOW before something bad happens
- Explore New Technologies such as Blue Lane, Reflex
- Virtualize BoB Security Service Layers overlaid across network infrastructure using Enterprise UTM such as Crossbeam
- Use Risk Modeling to truly factor virtualization into risk quotient
- Enforce rigorous control over admins with auditing and device management (physical and logical)
- If in doubt, don’t Use virtualized systems in Production

In Summary...

- Virtualization is a useful thing; your CIO wants it, so you should, too. It's a great discussion around the 11th hole or so...
- The V-word highlights the need to speak the language of business and express problems in terms of balancing risk versus reward since it's all about time and money
- Don't hate the player, hate the game! Virtualization is unavoidable, don't try...you will be assimilated
- If your security sucks now, you'll be comforted by the lack of change when you deploy virtualization!
- The pendulum will eventually swing back the other direction when performance suffers and security becomes even more expensive
- Use the opportunity to bring your developers, the network and security teams closer...even if blunt-force trauma ensues
- There's no silver bullet, but a lot of silver buckshot...use it all

CROSSBEAM SYSTEMS

We secure the world's largest networks.

Thanks

Christofer Hoff, CISSP CISM CISA
Chief Security Strategist
choff@crossbeamsys.com
+1.978.349.8882

blog: http://rationalsecurity.typepad.com