Virtualization Systems and Security Management– Two faces of the same coin

By now it is clear that virtualization is the next major paradigm shift in enterprise computing. The cost savings realized by consolidating underutilized computing resources is hard to ignore in these tough economic times. Even the current hype around "cloud computing" pays homage to on-demand computing made possible by virtualization. The Gartner Group estimates that over 50% of all servers will be virtualized by 2012[i]. It is no longer a question of if we will virtualize the datacenter; it is a question of when.

So if we concede that a virtual datacenter is in our future, the question becomes, "How will we manage and secure these virtual systems?" Although management and security used to be thought of as sub disciplines of systems management, since the advent of the Internet and distributed computing they have evolved into separate silos. Tools for network and systems management (think ESM products from the likes of HP, IBM/Tivoli, CA, BMC, etc.) are usually isolated from security tools like firewalls, intrusion prevention systems (IPSs), vulnerability scanning and the like. Oh sure, security information managers (SIMs) may provide some integration and correlation of events or logs, but I am talking about operational integration.

As we move from the physical datacenter to the virtual one will we continue this type of silo-based management? I believe that answer depends on your view of the virtual infrastructure and how you are organized. If your strategy is to try and replicate your physical infrastructure in the virtual environment, then you will likely have separate groups like server, network and server administration. You will probably attempt to force fit your existing management and security solutions into the virtual world in order to preserve the policy and procedures from your physical environment.

If, however, you truly appreciate how different the virtual environment is from the physical one, then you will realized that IT organizations, as well as management and security tools, must radically adapt to the new paradigm. If you carry the concept of virtualization to its logical conclusion then you will understand that by embracing the right management and security tools and processes, you can you achieve a level of automation not possible in a physical datacenter.

Here are a few examples of why the virtual environment requires a different approach to management and security:

- Server, desktop, CPU, memory, networking, storage, etc., are all virtual concepts that exist only in software.
- Provisioning a virtual machine (server or desktop) can be done with the click of a mouse or even automatically, without human intervention.
- Virtual networks, network interfaces, port groups, etc., can be created with the click of a mouse.
- Virtual machines can easily (and even automatically) move from one physical host to another. From one cluster to another. From one datacenter to another. Even from the datacenter or private cloud to a public cloud.
- IP and MAC addresses are no longer sufficient as building blocks of the network.
- The hypervisor introduces another layer to the infrastructure with new configuration, compliance and security challenges.

Because of the dynamic nature of a virtual environment, computing, networking, storage, applications and security are more tightly intertwined than ever before. A change to any one of these has profound impacts on all the others. Managing one layer in isolation from the other can lead to configuration errors, security and compliance gaps, and ultimately higher management cost. Moreover, managing a virtual infrastructure in silos fails to take advantage of the high degree of automation that virtualization makes possible.

Network and host security are often managed separately from the rest of systems management. There is a credible argument to be made that you should never let the "fox guard the henhouse." However, virtual security requirements differ greatly from physical network and host security. For one thing, the virtual datacenter resides behind perimeter defenses such as firewalls and IPSes. Therefore, virtual security is less about threat protection and more about segmenting the virtual infrastructure and meeting compliance guidelines.

Since virtual machines, networks, and storage are in a constant state of flux (one large virtual datacenter estimated over 100 changes per minute), virtual security must be aware of these changes and adapt automatically. Static approaches such as virtual firewalls that have been adapted from physical ones cannot possibly keep up with this many changes. Anyone that has had to update firewall rules any time a new machine is added, a network is changed, a new switch added, new software is installed, or an existing server is relocated, can testify to this.

Take this scenario: We create a set of security rules for virtual machines running IIS Web services. We identify all IIS Web servers (probably by IP address) and enforce this policy with firewall technology derived from the physical world. What happens when someone provisions a new Web server or an existing Web server is automatically moved to another host, cluster or datacenter? How does the firewall know about it? How long would that Web server run without the right security policy?

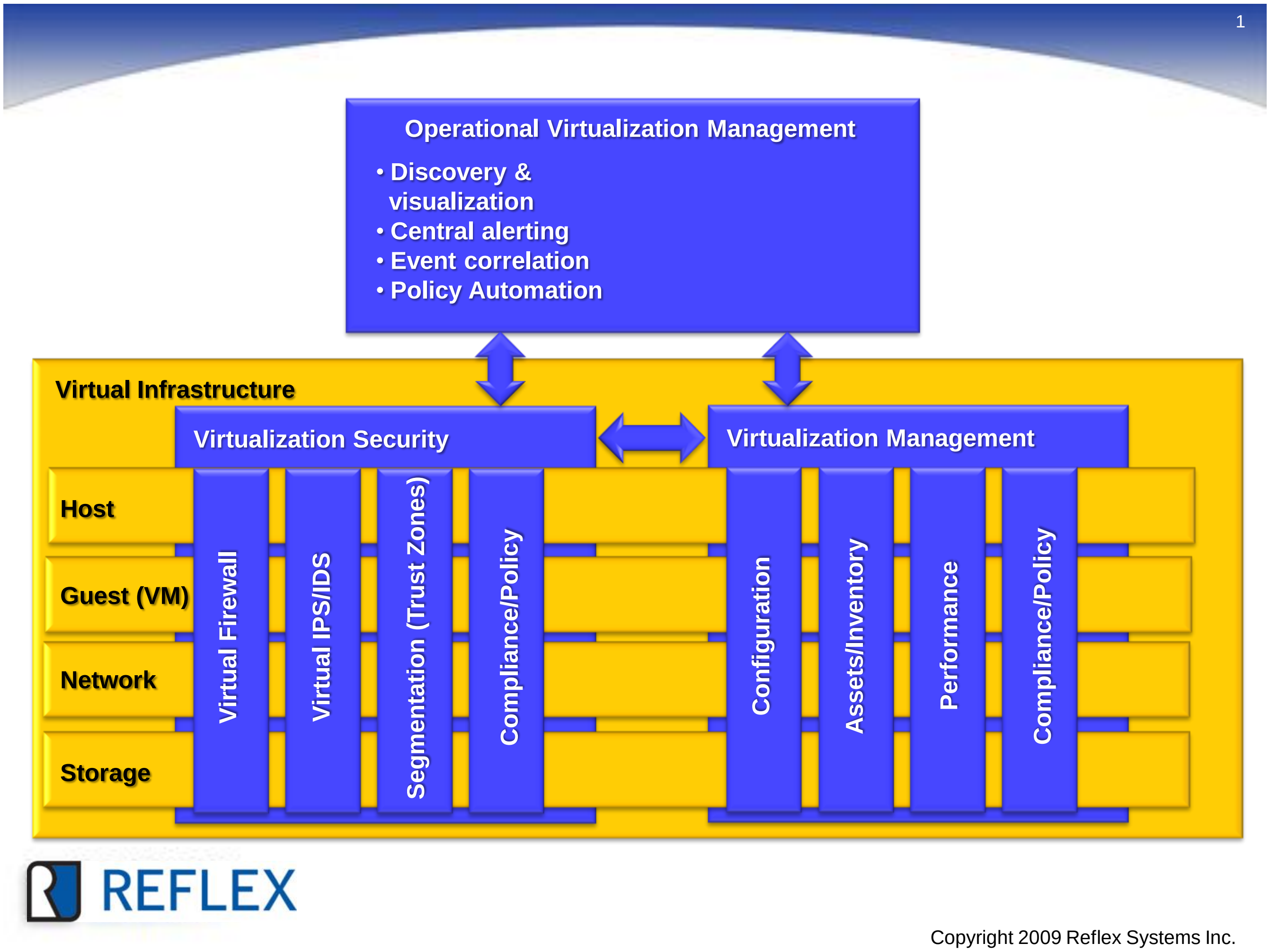
Obviously a new approach is needed which automatically detects changes to the virtual infrastructure. Next-generation virtualization security, designed to leverage the virtual infrastructure, should be capable of detecting any virtual machine running IIS and automatically apply the security policy inside the hypervisor regardless of where the virtual machine actual runs.

A conventional approach to segmentation based on VLANs is highly inflexible in a large-scale virtual infrastructure. As the virtual infrastructure grows, new networks are created, or virtual machines are automatically relocated to take advantage of new capacity, much manual effort (think Cisco CLI) must be done to reconfigure the network. At 100 changes per minute, how many new certified network engineers will you need to keep up with these changes? VLANs rely on costly physical network switches and severely limit many advanced features of virtualization. Virtualization security solutions segment the virtual datacenter using software which dynamically responds to any changes to the virtual environment.

Isolating servers on separate VLANs can control communications between machines, but if two virtual machines on separate VLANs are connected to the same virtual storage, that separation is abrogated. In virtualization, storage segmentation is just as important as server segmentation. Unlike their physical counterparts, virtualization security solutions must work equally well across the hypervisor host, virtual machine, virtual network, and the storage platform.

In addition, the hypervisor host introduces new security and configuration management issues that did not exist in the physical world. The hypervisor host has thousands of configuration settings. Since all traffic passes through the hypervisor, a miss configuration of any number of these settings could have broad security, not to mention performance and availability, implications.

For all these reasons it is difficult, if not impossible, to separate virtualization security from virtualization management. Virtualization security must be tightly integrated with discovery, visualization, configuration, performance, storage, asset, application and compliance management. Yes, best practices should include separation of duties. Those that define policies should not be the ones who deploy it. But trying to separate management from security would be like trying to separate two faces of the same coin.



1

Operational Virtualization Management

- Discovery & visualization
- Central alerting
- Event correlation
- Policy Automation

Virtual Infrastructure

Virtualization Security

Virtualization Management

Host

Guest (VM)

Network

Storage

Virtual Firewall

Virtual IPS/IDS

Segmentation (Trust Zones)

Compliance/Policy

Configuration

Assets/Inventory

Performance

Compliance/Policy

REFLEX

[i] Gartner Group Press Release, October 21, 2009