

TECHNOLOGY BRIEF

STRATEGIES FOR SECURING VIRTUALIZED ENVIRONMENTS

KNOW MORE NETWORK RISKS
NO MORE GUESSING



SOURCEfire®

INTRODUCTION

Virtualization is a concept that has become highly visible in the last few years because of its perceived benefits in reducing costs, enabling rapid deployment, and improving system availability. According to a survey conducted by Symantec in late 2007, 90 percent of the survey respondents have implemented or are considering virtualization for their data centers, and 50 percent have actually implemented it. Virtualization projects range from server consolidation and disaster recovery to the simplification of provisioning for desktops and associated applications.

Virtualization's benefits are rooted in its ability to separate a physical host into discrete subenvironments known as virtual machines (VMs). Virtual machines operate like physical machines in that they run their own operating system and applications. Yet virtual machines exist as file images and can be quickly provisioned, copied, moved, and restored. This type of virtualization, known as server virtualization, is the most prevalent for production purposes.

SECURITY RISKS

Organizations are building out virtual infrastructure at a very rapid rate to capture the various operational and financial benefits of virtualization. In their rush to implement virtual networks, however, security may not receive the attention that it should. Here is an excerpt from a November 2007 article from CIO Magazine¹:

Many IT organizations say they prioritized operational speed over most other factors, including security planning, when they started creating hundreds of new VMs in 2007. (That's not surprising, when you consider that most enterprises started with virtualization on their testing and application development boxes, not their servers running core business apps.)

"We're finding security is the forgotten stepchild in the virtualization build-out," says Stephen Elliott, IDC's research director for enterprise systems management software. "That's scary when you think about the number of production-level VMs."

Some IT organizations are making a fundamental mistake right now: They're letting the server group run the virtualization effort almost single-handedly - leaving the IT team's security, storage and networking experts out of the loop. This can create security problems that have nothing to do with inherent weaknesses of the virtualization technology or products.

Many of the risks of virtualization can be divided into several types:

- Virtual machine sprawl
- Lack of separation of duties
- Lack of visibility into virtual network traffic

¹ Laurianne McLaughlin, "How to Find and Fix 10 Real Security Threats on Your Virtual Servers," November 14, 2007, <<http://www.cio.com/article/154950>> (10 September 2008)

- Hypervisor vulnerabilities

Virtual Machine Sprawl

Virtual machine sprawl, or VM sprawl, is the propagation of virtual machines without adequate coordination or oversight. VM sprawl is caused by a variety of factors:

- System administrators deploy new VMs without sufficient planning. Little attention is paid to such lifecycle elements as support, patching, configuration, and end of life because of the ease and speed in provisioning the VMs.
- Administrators and users copy VMs to new hosts throughout the network because the VMs exist as file images and can be easily transferred via portable USB drives or network transfer.
- Snapshots enable a VM to be rolled back to a previous state, which means that patches can now be undone.

The result of VM sprawl is that VMs are distributed across multiple physical hosts, in various states of patching and configuration. No single group tracks where a VM is located, what its patching and configuration status is, or what its purpose is. Security risks become more tangible because a VM that is not properly tracked and managed may not have updated patches or proper configuration control, leading to vulnerabilities that can be exploited.

Lack of Separation of Duties

Historically, different groups have owned different physical devices. Server operations owned the servers, network operations owned the routers and switches, and security owned the intrusion detection systems and possibly firewalls.

Virtualization has disrupted this paradigm so now the server administrators that typically deploy a virtual system own all of the virtual infrastructure. They configure the virtual switches and virtual storage. They usually do not deploy any virtual security devices such as firewalls or IDSes because these products mainly do not exist today. Because of various time and financial pressures to meet deadlines, server administrators may not be able to get the networking and security groups involved in the virtualization process. Unfortunately, this change in paradigm will lead to more misconfigurations and vulnerabilities because the groups now doing the virtual infrastructure configuration are often not the subject matter experts.

Here are a few anecdotes reported from various enterprises implementing virtualization:

- New VMs being rolled out without any antivirus or antispyware protection
- Production VMs and development VMs running on the same host, where the development VMs contain proprietary source code
- VMs being connected to multiple virtual networks such as production and test that should otherwise be segmented

Lack of Visibility into Virtual Machine Traffic

Most enterprises today do not have full visibility into their network traffic. If they monitor their traffic at all, they typically follow best practices in only deploying sensors in various monitoring zones such as inside the DMZ, between an enterprise's wireless and wired segments, or between partner networks. The assumption is that malicious traffic will be detected as it is entering or exiting a monitoring zone.

So enterprises do not usually monitor traffic between hosts in the same zone. Monitoring requirements for virtual network traffic, however, are different. This is because of the degree to which virtual hosts and networks can be arbitrarily combined. As the previous sections of this paper have illustrated, it is now extremely easy for enterprises to run production and nonproduction VMs on the same host, or bridge VMs between different monitoring zones. The physical world enforces a certain discipline by requiring hosts to be located in specific physical racks or connected to certain switches. This discipline is now lost and it becomes possible for any virtual host to communicate with any other virtual host, due to misconfiguration or lack of policy enforcement. All of this inter-VM traffic is not visible to physical sensors that remain deployed at their traditional locations, i.e. between monitoring zones.

Hypervisor Vulnerabilities

The presence of a hypervisor in a virtualized environment also creates the possibility of new types of vulnerabilities. The hypervisor is a control program that manages physical hardware resources such as the processor and memory and makes these resources available to VMs. Tavis Ormandy, a security researcher at Google, has already proven it is possible to crash the hypervisor from a VM by sending random data sequences to the VM's virtual hardware. A malicious user could potentially gain control of the hypervisor by exploiting a hypervisor vulnerability from a VM. This user could then compromise all other VMs on that host because of the hypervisor's privileged access.

Various vulnerabilities have been discovered in virtualization products such as VMware Workstation but none have been publicly disclosed in VMware's ESX or Virtual Infrastructure products, its primary server virtualization products. While it is only a matter of time before such a vulnerability is discovered and disclosed, it is still theoretical. The closest concrete example of hypervisor exploitation is a proof-of-concept rootkit known as Blue Pill. Blue Pill, designed by researcher Joanna Rutkowska, compromises a physical system's operating system and moves it into a virtual machine. The rootkit itself becomes the hypervisor and conceals its presence from malware detection technologies. Blue Pill has been claimed to be completely undetectable, a claim that is disputed by various security researchers. Regardless of Blue Pill's

effectiveness, future hypervisor exploits could work similarly in taking over the physical system and all VMs and attempting to conceal their presence.

ROLE OF BEST PRACTICES

Sourcefire endorses the general concept that security is a process, not a technology or product. One of the most effective ways to secure one's organization is to implement organizational processes that recognize the inherent insecurity in any security product.

With this in mind, Sourcefire recommends a number of best practices to help mitigate the security risks that may be created when an enterprise implements virtualization:

1. Apply standard security practices to virtual machines as if they were physical. These include antivirus and antispyware agents, configuration control, and vulnerability scanning.
2. Segment virtual machines by the data they contain. Do not combine VMs containing sensitive data with VMs designated for QA or testing, for example.
3. Enforce isolation between network segments. Do not combine VMs in the same host if they are connected to network segments at different trust levels. For example, do not put a VM connected to the production data center segment with a VM connected to the internal office LAN or test network. If possible, do not virtualize hosts in the DMZ, especially if these hosts cross trust levels, e.g., firewalls.
4. Guard against VM sprawl by maintaining an inventory of VMs and the physical host they reside on. All migrations should be documented and potentially subject to an approval process.

Unfortunately, the general assessment of enterprise virtualization so far is that these best practices are not being followed closely. This observation has been confirmed by articles in trade publications, observations by industry analysts, and conversations with customers. Security is the "forgotten stepchild" in the virtualization buildout, as IT organizations work to implement virtual environments as quickly as they can to capture the financial and operational benefits. Many have not yet changed their processes to ensure proper security. There is also no regulatory pressure, because auditors do not yet require organizations to address the potential risks caused by virtualization.

What compounds this situation is a technology known as live migration. VMware's VMotion is capable of moving virtual machines between physical hosts without any VM downtime. This is a very powerful feature, but it has the effect of making it even easier to violate security best practices. The ease of migration makes it easy to bypass policies requiring trust level as a criterion for migrating VMs. Organizations can simply look for a physical host that has available resources and then migrate VMs to it.

In the midst of this environment, security analysts and server administrators need tools that can help them do their jobs effectively. They need visibility into their virtual infrastructure, tracking where VMs reside, where they move to, and what other hosts they are communicating with. They also need a means of applying the proper security processes to their VMs, providing the same level of security to their virtual infrastructure that they do to their physical infrastructure.

SOURCEFIRE VIRTUALIZATION SOLUTIONS

Sourcefire Realtime Network Awareness (RNA) is well suited to help provide visibility into an organization's virtual infrastructure. RNA itself was originally developed to help address the user problem, "I don't know what is going on in my network." RNA is a passive technology that detects network assets in real-time and tracks their configuration changes and network behavior. Sourcefire's vision is for RNA to provide visibility into both physical and virtual networks from a common management console.

Dealing with VM Sprawl

RNA directly addresses the VM sprawl issue by detecting new and existing VMs. Sourcefire accomplishes this by looking up the vendor assigned to the first six digits of a network card's MAC address, which is known as an Organizationally Unique Identifier, or OUI. VMware has registered multiple OUIs in the OUI database. When a VMware administrator deploys new VMs on a network segment monitored by RNA, Sourcefire will display "VMware" as the name of the (virtual) network card manufacturer in each VM's RNA host profile. This enables Sourcefire users to distinguish newly detected hosts as either physical or virtual machines. If it's a virtual machine, IT security can be alerted to audit the virtual machine for compliance.

Providing Virtual Network Visibility

Virtualization now makes it possible to implement architectures that would be improbable or difficult to build in the physical world, such as combining production and development VMs on the same host or bridging VMs between different monitoring zones. RNA Virtual Appliance will provide visibility into these virtual networks and identify network behavior that violates IT policy.

For example, a Sourcefire user may use host attributes to label hosts by department or trust zone. If VMs in different trust zones are accidentally combined on the same physical host or bridged together to the same

virtual network, the user can create a compliance rule that will detect whether these two VMs ever communicate with one another and then take appropriate action.

Protecting Against Hypervisor Vulnerabilities

As stated earlier, no vulnerabilities have yet been disclosed in VMware's ESX or Virtual Infrastructure products. Some disclosed vulnerabilities have been associated with VMware ESX but they actually pertain to the Linux operating system that the VMware ESX service console uses. Sourcefire's existing 3D Sensors already monitor traffic for these vulnerabilities and can block them if required.

If an exploit directly affecting VMware ESX or ESXi were to be released and it was detectable in network traffic, the Sourcefire Vulnerability Research Team (VRT) would work immediately to create, test and publish new Snort rules to defend customers against such exploits. The VRT is always conducting threat research into new and emerging threats. Hypervisor exploit research is an area that the VRT is actively investigating.

ROLE OF TRADITIONAL SECURITY DEVICES

The rapid implementation of virtualization in the enterprise does not replace the need for traditional physical security infrastructure by any means. Physical intrusion sensors placed at an enterprise's typical monitoring points are crucial for protecting the enterprise because they are monitoring traffic that is either entering or exiting the enterprise network.

Sourcefire therefore believes that a virtualization security solution should not exist as a separate silo but instead as an extension of a physical security solution. Users already have many products to manage, and there are financial and operational benefits to leverage a common platform to protect both physical and virtual networks.

CONCLUSION

The rapid deployment of virtualization in many enterprise environments has created the need to track and monitor the deployment of virtual machines throughout the network. Sourcefire recognizes this need and provides RNA as a means of accomplishing these tasks. These tools offer a single framework for managing both physical and virtual network security. The flexibility of RNA will enable users to deploy it throughout the network wherever it is needed.