White Paper

FIVE BEST PRACTICES TO PROTECT YOUR VIRTUAL ENVIRONMENT

Realizing the Benefits of Virtualization Without Sacrificing Security

Table of Contents

Executive Summary

Latest research from the Yankee Group shows that nearly half of all businesses have virtualized some portion of their data centers. This means that there is a very good chance you are in the midst of a virtualization initiative, or soon will be, in order to cut the costs of operating your data center, DMZ, mission critical applications, or desktop environment. Standing in the way of realizing virtualization's promise, however, is security. And going forward with your virtualization initiative without addressing visibility, protection, and compliance can prove problematic, as malware targeting virtual networks proliferates, and standards mandating granular virtualization security become ratified. This paper lays out five "best practice" ways to fortify your planned or existing virtualized environment, ensuring that it is architected for security, malware suppression, and regulation compliance.

Introduction—Virtualization's Big Hurdle

Virtualization stands to bring enormous cost savings to enterprises by significantly reducing the space and electrical power required to run data centers, and by streamlining the management of an ever growing number of servers. It is no wonder, then, that adoption of virtualization is proceeding at a very rapid clip, further accelerated by trying economic times and cost-cutting mandates. In a rush to implement virtualized networks and data centers, some organizations have been forced to shelve security concerns in favor of rapid project completion. Others are struggling with how to reconcile competing priorities to virtualize their environments while still ensuring that existing requirements for protection and visibility are maintained. These challenges are much bigger than an initial glance might suggest. Collapsing multiple servers into a single one comprised of several virtual machines (VMs) literally eliminates all firewall, intrusion detection, and other protections in use prior to virtualization. Physical security measures literally become "blind" to traffic between VMs, since they are no longer in the data path. Consequently, they cannot enforce protections and maintain control. Further increasing the risks to virtualized traffic are the very features and functions that make virtualization highly desirable for optimal resource use.

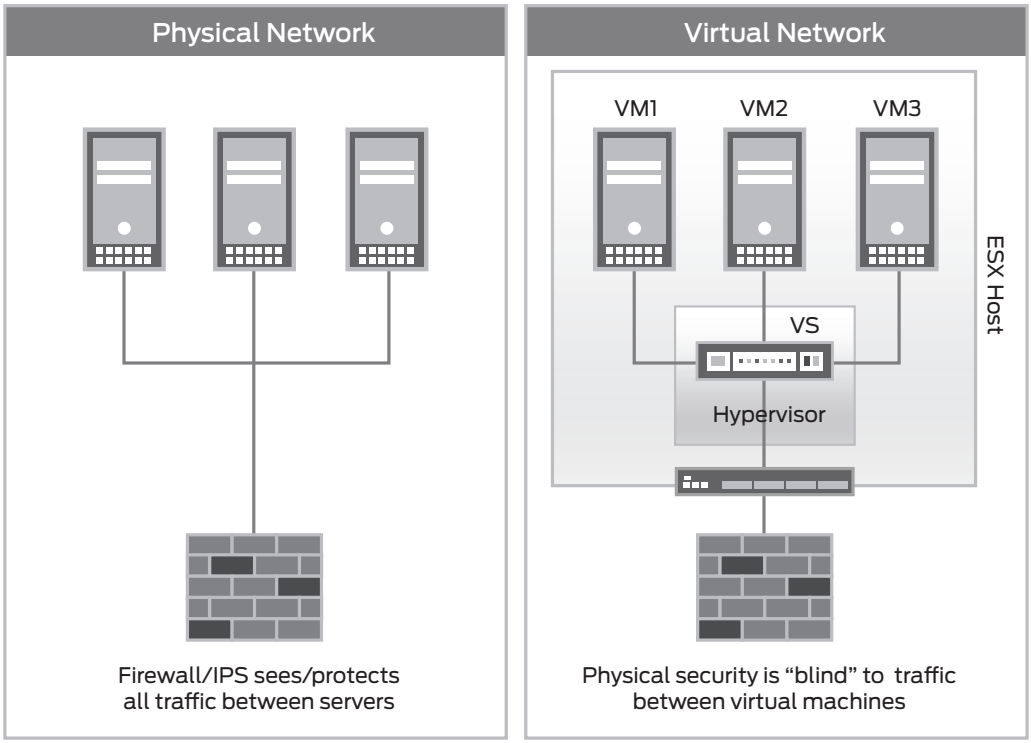

Figure 1: The security implications of virtualizing.

VMware provides features like VMotion and Distributed Resource Scheduling (DRS), which allow for hardware and capacity pooling by enabling VMs to move from physical host to physical host as performance needs dictate. VM provisioning is also very quick and easy. IT operations personnel and department administrators can create new VMs using templates or cloning existing ones. So, while virtual environments can scale in a flash, the security policies that control access and suppress malware proliferation cannot—unless the process for doing so is equally automated and scalable. Consequently, the contents of VMs and the applications they host are at high risk from inappropriate access, malicious traffic, and poor (in some cases inherited) security posture.

Why Old Style Protections Fall Short

As you have looked for ways to secure your virtual network, you have probably found a limited number of possible approaches. Most discussions focus on how to use existing tools to secure virtual network traffic. Two common approaches are: 1) using VLANs to separate VMs into groups and enforce access control via physical firewalls/routers; and 2) taking software-based firewalls and running them as agents on each VM. Let's examine each approach.

1. VLAN segmentation extends the notion of LAN resource segmentation to include VMs. The approach essentially requires that VMs, which can naturally be grouped (e.g., by function or user base), be isolated from other VMs by use of virtual switches and routing (e.g., the HR VLAN contains HR serving VMs). However, VLAN segmentation is not a permanent solution to securing virtual environments because of the networking complexities, performance degradation, and security limitations of the approach. The use of VLANS requires routing VM traffic out of the ESX host (the VMware virtualization solution) and directing it to a physical firewall. This not only introduces latency affecting performance, it also requires some fairly complex networking in order to support dynamic resource pooling and live migration. Further, despite all of the effort invested in VLAN-based segmentation, VM-to-VM communication within a VLAN is not inspected or secured. For instance, malware which infects one VM can't be stopped from spreading to other VMs on the same VLAN.
2. Software-based firewalls used as agents that run on each virtual machine also seem like a reasonable approach at first glance because it lets users buy a product with which they are familiar. But as the number of VMs increase or "sprawl," so does the number of agents that must be managed, making this a costly solution. Security, too, is less than optimal with the agent-based model, in that there is no protection for the hypervisor (i.e., the virtualization operating system), so attacks that strike by turning "off" VM-based services like the Conficker Worm can bypass agent-based protection.

Best Practices

Create a VM Service "Good List"

One of the best ways to create an optimal access policy for a virtual machine is to create a list of what are appropriate and warranted applications and services to be run on that VM. This list will vary based on the type of server, its use in your organization or business, and the group of users and applications it enables. Let's take a VM that is a database back-end as an example. There are certain applications and protocols that must flow in and out of this VM in order to enable its function, yet others that are completely inappropriate. For instance, it may not be necessary to allow FTP on this server, since the need to transfer files into and out of a database using this protocol is rare and constitutes a way in for someone with malicious intent. An optimal security policy for this server might allow only the services that enable the database's function (SQL, for example) and block all others. This significantly reduces the security risks to this server from exploits that leverage protocols other than database-specific ones. Taking then each type of VM that you have in your network (e.g., databases, Web servers, file shares) and creating a "good list" (or whitelist) of commonly used and expected applications and services will help you create a security baseline for each type of VM. You can then use this list to a) craft a security policy that restricts access to warranted use; and b) optimize the policy over time to reflect new uses and services needed by the business.

For those environments where security is introduced after virtualizing, the whitelist can help "lock down" VM use. Virtual firewalls can show administrators the services and protocols present on each VM. A comparison to the whitelist will reveal any potential security risks as well as unexpected use cases, thereby enabling the construction of an appropriate access control policy. This will also ensure that new VMs cloned from existing types inherit the appropriate security settings.

Monitor and Protect the Hypervisor

Part of the security regimen for virtualization needs to include not only the VMs but the hypervisor itself. VMware created the VMsafe technology, which uses vSphere-specific capabilities to enable third-party security solutions for virtualized environments. VMsafe gives tremendous visibility into virtual machine resources, making it possible to monitor every aspect of the execution of the system and stop previously undetectable viruses, rootkits, and malware before they can do harm. For firms looking to maximize security for VMs and the hypervisor, it will be important to ensure that their VMware environment is vSphere-enabled. This will give organizations access to the VMware partner solutions that offer layered defense capabilities from within the hypervisor.

Enforce Access Control per VM

Virtual machines are the physical environment's server constituent. Just like the physical network, VMs can serve as file shares, databases, Web servers, application servers, extranets, and more. And while VMs of many different types may reside on one physical host, traffic flowing among them can easily proliferate malware, worms, or the activities of malicious persons. For this reason, it is very important to monitor all traffic between VMs and apply the access controls needed to block unwanted protocols. Additionally, you will want to examine sanctioned applications and services for the presence of intrusion or malicious traffic. In this way, business critical communications can flow with all of the flexibility that virtualization affords, and it can do so securely with the threat from unwarranted and unwanted access severely reduced.

Layered Defenses

As in the physical world, it is important to employ a system of defenses to protect traffic within the virtualized environment. This means applying the security policies and controls that will block unwanted services into and out of a particular VM. This first layer reduces the probability of these types of attacks to nearly zero. The next layer of protection comes in the form of monitoring and inspecting the traffic that is warranted but may have embedded within it the malicious intentions of an insider looking to steal or otherwise misuse resources. Protection for this sort of attack entails inspecting the traffic against a set of known attack signatures and behaviors, such as the functionality provided by intrusion prevention systems (IPS). Other types of protections, including log aggregation and analysis, antivirus protection, and means for alerting when malicious activity has been detected, are also important defense mechanisms. In general, all of the layers of protection applied to traffic in the physical world need to be considered for the virtualized environment. The key is to ensure that these protections do not provide security at the expense of the flexibility and scalability of virtualizing. This is the focus of the next section.

Insist on Purpose-Built

Your virtual network has a lot of unique features and functionality that help you make the most out of your data center hardware investments and give you the means for infinite and expedient scalability. To start, a VM can move from ESX host to ESX host in order to take advantage of capacity and memory that will optimize performance. Traffic flowing through this VM should not be impeded. If, for instance, a virtual firewall is statefully handling a session into and out of a VM, the session should continue without disruption, as should the application of the security inspection.

Additionally, one of the big advantages with virtualization is the near instant time required to provision a new VM. Rather than having IT personnel prepare and connect a physical server, they can simply clone an existing VM and have it up and running in minutes. The new VM will simply inherit the settings of the parent, including the security policies and applications in existence for a VM of that type. This will ensure that security for the new resource is automatically provisioned, thus reducing the risk of exposure to malicious traffic.

Finally, in addition to IP and media access control (MAC) addresses for virtual network interface cards (NICs), VMs also have, in the VMware environment, Universally Unique Identifiers (UUIDs). These fixed identifiers follow the VM wherever it is in the virtual network, and remain "unique" (unlike IP addresses) throughout the life of the VM (which may change if the VM power cycles, for instance). To avoid networking complexities and risks to security-policy enforcement, it is best to tether the security policy to the VM's UUID as opposed to the IP or MAC address.

The discussion above highlights that the system and technology for protecting inter-VM traffic must be able to render its defense without detracting from virtualization's value. When it comes to selecting a firewall, IPS, and security for virtualization in general, ask whether the proposed product provides support for: VMotion, DRS, UUID, and vCenter. You also need to understand what latency, if any, the security inspection will introduce by asking for specific data on throughput at different ESX host load conditions. Any vendor that has done the heavy lifting to build a true virtual security platform should have no issue with providing this data.

Conclusion

Virtualization's undeniable cost and scalability benefits are making it a near de facto choice for data centers and clouds. If virtualizing your servers isn't on your current project short list, it should be soon. While planning or augmenting your virtual environment, it is important to include the integration of monitoring and access control in the mix. Seeing your inter-VM traffic can help you troubleshoot and optimize your virtual network. It can also help you define and refine access controls so that all traffic is business appropriate and enabling. While it is natural to think existing security tools might have these concerns covered, the fact is that many use legacy technologies as far as virtualization is concerned. And if threats by insiders seem somehow less likely, they are on the rise. For this reason, updates to regulations are underway. However, you don't have to wait for a forced mandate to have the benefit of virtual security. The technology to monitor and protect your inter-VM traffic exists and is in broad use worldwide. Your biggest challenge is in understanding the different offerings and choosing the one that best protects your security and virtualization investment.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000379-002-EN Mar 2012

Printed on recycled paper