BUSINESS GROUP
IT Operations

SOLUTION:
Implement network micro-segmentation, enabling the deployment of security controls inside the data center, improving insight into network traffic while improving security at a fraction of the cost of hardware-based approaches. Implement VMware NSX ™ Distributed Firewall to eliminate the traditional "chokepoints."

BUSINESS BENEFITS

- Move control closer to the application with no compromise in security, performance or features, unlike traditional networks.
- Dramatically improve provisioning speed, operational efficiency and service quality.
- Evolve VMware's own journey to the software-defined enterprise through virtualized networking.

Business Transformation Through IT Transformation: VMware IT Improves Application and Network Security Through VMware NSX™

It's not getting any easier out there. Data centers are increasingly vulnerable to new and more sophisticated ways to attack, such as "hitching a ride" on authorized users to get behind the firewall, then traveling laterally inside the enterprise data center perimeter. Many IT organizations today are turning to network micro-segmentation for better visibility into east-west traffic—that is, the traffic that flows between data center devices and applications within VMs—while keeping a wary eye on costs.

The Challenge

VMware IT faced the same challenges as other enterprise IT organizations and turned to its own product—VMware NSX —for a software-defined approach to micro-segmentation at a fraction of the cost of a hardware-based approach.

Network micro-segmentation wraps security controls around much smaller groups of resources—often down to a small group of virtualized resources or individual virtual machines. Micro-segmentation has been understood to be a best practice approach from a security perspective, but has been difficult to apply in traditional environments.

"With NSX, micro-segmentation became operationally feasible—and cost effective—for the first time," said Swapnil Hendre, solutions architect with IT Operations at VMware. "This is due to the inherent security and automation capabilities of NSX and its approach to distributed firewalling."

The perimeter-centric network security strategy for enterprise data centers has proven to be inadequate, Hendre noted. Modern attacks exploit this perimeter-only defense, moving laterally within the data center from workload to workload with little or no controls to block their propagation.

Micro-segmentation in the data center is one way to limit that unauthorized lateral movement, but it hasn't been operationally feasible in traditional data center networks.

"Using the traditional firewall approach to achieve micro-segmentation quickly reaches two key operational barriers; throughput capacity and operations management," explained Hendre. "The capacity issue can be overcome at a cost. It is possible to buy enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation. However, operations increase exponentially with the number of workloads and the increasingly dynamic nature of today's data centers. If firewall rules need to be manually added, deleted or modified every time a new virtual machine is added, moved or decommissioned, the rate of change quickly overwhelms IT operations."

"With NSX, micro-segmentation became operationally feasible—and cost effective—for the first time."

Swapnil Hendre
Solutions Architect with IT Operations, VMware

The Solution

VMware IT implemented VMware's NSX DFW (Distributed Firewall) to gain insight and increase security for east-west traffic layers instead of just north-south traffic, which is generally limited to traffic that enters and exits data center, noted Hendre.

Through its unique distributed firewall feature, VMware NSX delivers both insight and security within layers of traffic, not just between them, he added.

No More Hairpinning

Traditional firewalling solutions suffer from performance choke points and increased network capacity costs due to the need for "hairpinning"—the process of routing traffic out of the data center for inspection, then rerouting it back into its data path. This adds additional "hops" to route traffic through essential network services, explained Hendre.

Increased east-west traffic in a data center exacerbates this problem, he added. NSX has been architected for performance at scale and avoids the security and service blind spots.

Improved Application Security

"This solution has enabled better application security by allowing us to define relationships between applications," said Hendre. "Overall lifecycle management of our customer-facing applications is thereby improved."

"NSX-DFW is built directly into the Hypervisor, hence no virtual machine can circumvent the firewall," said Hendre. "This is critical for customers with high security needs."

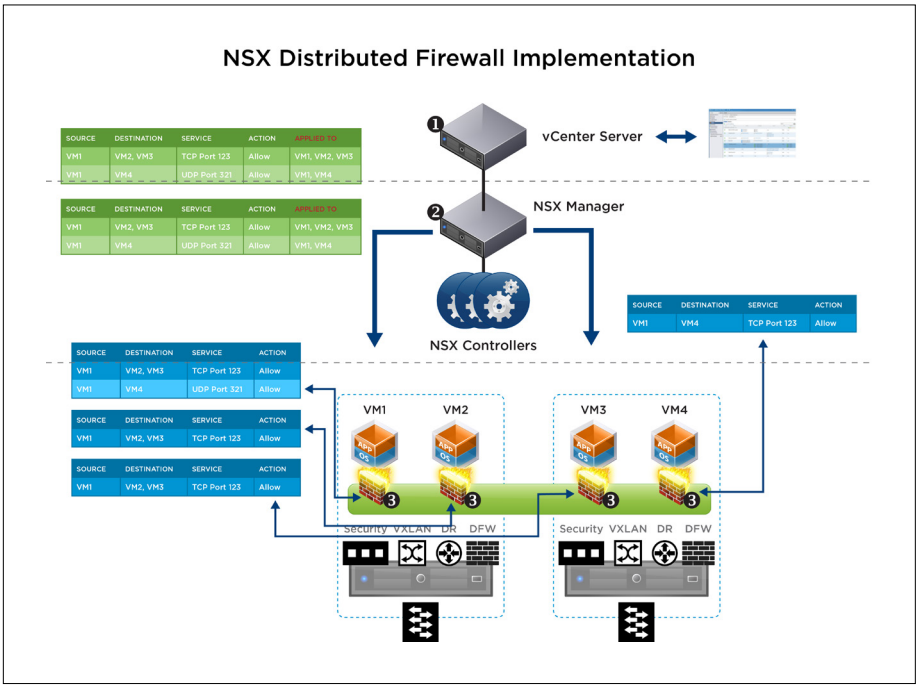
"Distributed Firewall (DFW) is the perfect approach for enterprises needing increased security and significant application scalability. With NSX DFW, egress and ingress packets are always processed by the firewall," he added.

"NSX allowed us to create a three-tiered architecture within existing applications without having to re-IP or re-engineer any of the application," said Paul Kincaid, director of security architecture.

"'Security Groups' provide the ability to easily apply firewall rules based on functionality and access requirements. These Security Groups also allow us to easily contain VMs that may be vulnerable to certain highly critical vulnerabilities or which may be infected with malicious code," added Kincaid.

With the distributed firewall, there is no chokepoint as in traditional network design; rather, kernel-embedded modules sit on top of ESXi.

"What this is essentially is a scale-out firewall," noted Hendre. "NSX can be deployed on existing virtual infrastructure."



Implementing NSX Distributed Firewall

Implementation is easy, noted Hendre. Using VMware vSphere, an IT admin simply deploys NSX Manager as an appliance, points it to vCenter, then prepares clusters for network virtualization by installing NSX on ESXi hosts. The firewall is then deployed on each hypervisor in ESXi clusters, ready to be configured.

The challenging part of this project came in the planning side of implementing new technology, Hendre noted.

"We had to redefine some of the roles and responsibilities in our teams," said Hendre. "Managing in the era of the software-defined data center means admins handle networking along with elements of application, storage and server administration."

VMware's network admins have been trained on VMware vCenter, now part of VMware vRealize.

"Organizationally, we are drawing the line at the logical level rather than the physical one," Hendre explained.

Hendre's "best practices" for NSX DFW deployment:

- Identify one application and do evaluation.
- Perform proof of concept in lab.
- Develop and share key findings.
- Define roles and responsibilities.
- Use Flow monitoring to get insight into application traffic.
- Finalize micro-segmentation rules to be implemented.
- Do a production pilot.
- Define reference architecture and repeatable process for deployment.
- Rollout wide deployment.

The project took about six months from initial scoping to go-live in July 2014. The actual technology rollout was a small part of that; a lot of the work was performing Proofs of Concept and Pilots, developing reference architecture, organizational realignment, training teams and creating repeatable processes to support IT Ops' continued journey to the fully automated software-defined data center. Now VMware IT has well-defined, repeatable processes for NSX-DFW deployment.

NSX DFW was deployed for the VDI environment and now VMware IT is in the process of deploying NSX DFW to more customer-facing, mission-critical applications. One example he cited was MyLearn, VMware's education portal.

"VMware IT is now securing applications better than ever before," said Hendre.

VMWARE ON VMWARE

As the leading proponent of our own products, VMware is committed to passing on the lessons learned by our internal IT group in applying virtualization and cloud management technology to solve business challenges.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com