Micro-Segmentation Builds Security Into Your Data Center's DNA

With VMware NSX, Security Becomes as Nimble as the Applications They Protect

TECHNICAL WHITE PAPER

vmware®

Executive Summary

Most enterprise IT professionals agree that securing the network only at the perimeter is inadequate for today's data centers. Once malware has managed to make its way behind the firewall by latching onto an authorized user (or other means), it can move easily from workload to workload. This lateral movement is possible due to a lack of sufficient internal network controls regulating server-to-server or east-west network traffic.

Micro-segmentation, enabled by VMware NSX™, is a breakthrough model for data center security. Network security policies are enforced by firewall controls integrated into the hypervisors that are already distributed throughout the data center. This enables security that is both ubiquitous and granular. Security policies can also be changed more easily—even automatically—moving when VMs move and adapting to changes in workloads.

This security model, which reflects and supports the dynamic nature of data center operations, has never been possible before. The model goes beyond the idea of plugging gaps in perimeter security, or even trying to manipulate physical security within the data center to make it more effective. The micro-segmentation model is not about "building up" but "infusing into." Much like bioengineering plants to be more disease resistant, micro-segmentation changes the DNA of data center security to be resistant to threats at an extremely granular level. There are no gaps in defense because security is infused into the whole operational environment of the data center. Policies can be created and updated with an agility that can thwart the most determined attacker.

The Tortoise and the Hare: Security Isn't Keeping Up With Fast-Moving Workloads and Faster-Moving Threats

As virtualization and cloud technologies dominate the data center (accelerating the speed at which servers, storage and network resources are provisioned), administrators are under pressure to secure workloads faster. Increasingly, the name of the criminal game is not just disruption but financial gain through the theft of valuable information. By isolating workloads and blocking lateral movement, you can keep malware from starting in one place and moving around until it achieves maximum damage or successfully downloads sensitive information.

The cost of a data breach can easily reach millions or hundreds of millions of dollars when you factor in forensic experts, in-house investigations, loss of customers, lower customer acquisition rates, and providing free credit or identity monitoring subscriptions to bolster trust.

If the security breach succeeds in stealing valuable customer or employee information, the costs are virtually incalculable.

Following are just some of the data points that tell us the current model for data center security is not keeping up with threats:

1. **Companies continue to invest heavily in security.** In the U.S. alone, companies are collectively spending billions on security every year—and significantly boosting their annual security spending.

Network Virtualization Makes Micro-segmentation Possible

VMware NSX, the network virtualization platform for the Software-Defined Data Center (SDDC), creates a virtual network that is independent of the underlying IP network hardware. IT can simply treat the physical network as a pool of transport capacity.

Much like the server virtualization model, a "network hypervisor" reproduces Layer 2 to Layer 7 networking services in software. These services can be assembled in any combination—in a matter of seconds—to produce a new network configuration.

You can programmatically create, provision, snapshot, delete and restore complex networks all in software.

Because hypervisors are already distributed throughout the data center, with VMware NSX you can create network security policies enforced by firewall controls integrated into the hypervisors.

These security policies are tied to your virtual network, virtual machine, and operating system, providing granularity down the virtual network interface card.

2. **Attacks continue to be successful.** The average company experiences two successful attacks each week, according to a global survey by PriceWaterhouseCooper.[1]
3. **Attacks are taking a bigger toll.** The cost of data breaches to companies also continues to increase, according to the Ponemon Institute.

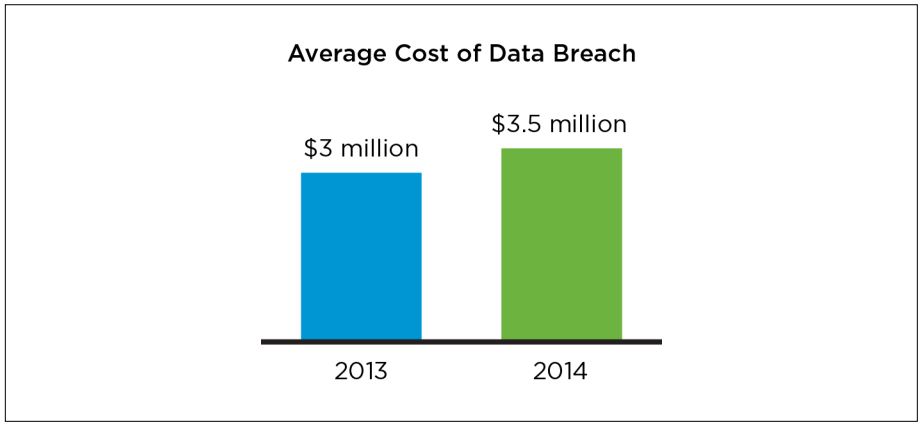

Figure 1: Cost of Data Breach Study 2014, Ponemon Institute, 2014

The Guards at the Gate are Fierce but not Sufficient

It isn't that physical security appliances aren't sophisticated enough. Given the purpose for which they were designed, today's adaptive firewalls and intrusion prevention systems are intelligent and formidable. But statistics show that they aren't sufficient to protect the data center. Here are some of the reasons why:

- Complex security mechanisms like physical firewalls are administratively intensive to maintain and update. CIOs are having a tough time justifying this rising overhead when they're under constant pressure to cut costs.
- Physical devices cannot be everywhere at once, or even too many places at once. It's simply too complicated and expensive to locate firewalls in every nook and cranny of the data center. If that's not possible, also imagine reconfiguring physical firewall policies within a matter of minutes to adapt to a new workflow or to contain an active attack.
- The perimeter-centric security model is designed to work from north to south, which means from the client to the server. It's not designed to handle east-west traffic, which is how communication between servers travels.

Most enterprise IT professionals agree that securing the network only at the perimeter with physical firewalls is inadequate for today's data centers. While perimeter defense is strong, it isn't impregnable.

Among the many ways that perpetrators can make their way into the data center is by creating malware that latches onto an authorized user and piggybacks on that user data to get behind the physical firewalls.

[1] Global State of Information Security Survey 2015, PriceWaterhouseCooper, 2014

The World is More than "Trusted" and "Untrusted"

Historically, using traditional network firewalls, similar compute systems are grouped into security or trust zones. Firewall policies can then be used to create a comfortable envelope around these siloed zones. Obviously, to contain complexity and cost, larger zones are easier to set up than smaller ones – the most immediate example being the practice of creating a "trusted" zone, separated from an "untrusted" zone. Large envelopes with more compute systems inside them are better for economics and ease of administration—but not, as it turns out, for better security.

Within a security or trust zone, access is completely unrestricted between systems—because anything in the zone is assumed to be trustworthy by everything else in that zone. The bigger the zone, the more havoc a single piece of malware can wreak. The malware can travel around unchallenged, disrupting operations or stealing sensitive data.

The typical data center might have a pair of firewalls at the perimeter and maybe a handful inside the data center, compared to hundreds and hundreds of workloads. To protect all of this east-west traffic would require the firewall-equivalent of the Incredible Hulk® comic book character.

Even if such a thing were feasible (which it isn't), you'd still have the problem of directing all VM-to-VM traffic through this monster firewall, and the performance impact would be frightening.

Since physical security is optimized in one direction (literally), a better model requires an entirely different approach: micro-segmentation enabled by network virtualization. Micro-segmentation can help your organization address all of these issues:

1. Stopping the spread of malware within the data center
2. Enabling faster delivery of networking and security services
3. Creating more flexible and even automated adaption to changing demands and security conditions

Until network virtualization with VMware NSX, a micro-segmentation model for data center security was not possible. Now it is not only feasible, but also streamlined and cost-effective to deploy and administer.

If Threats Can Start Anywhere, You Have to be Everywhere

In a sense, physical security is like using gloves to guard against germs. It is external, limited protection (if someone sneezes in your face, you're probably going to end up with a cold or flu). Micro-segmentation is like fortifying the immune system of the data center: germs (or malware) can't get it. Or, if something does, the system can shut it down (or limit its travels) so it can't spread.

Micro-segmentation is based on the assumption that threats can come from anywhere within the data center. So the micro-segmentation model makes security ubiquitous throughout the data center. This model not only provides pervasive coverage, but also the ability to create and change security policies with agility and speed that matches the dynamic workloads they must protect.

Micro-segmentation is not unlike how biotechnology is used to change plants at the molecular or cellular levels to be pest and disease resistant. That's what micro-segmentation can do to secure all of your data center resources.

Security becomes both pervasive and extremely granular, eliminating gaps and vulnerabilities. That's why VMware describes micro-segmentation as the ability to "build security into your network's DNA."

Figure 2. VMware NSX enables the three key functions of micro-segmentation: 1) isolation (no communication across unrelated networks), 2) segmentation (controlled communication within a network), and 3) security with advanced services (tight integration with leading third-party security solutions).

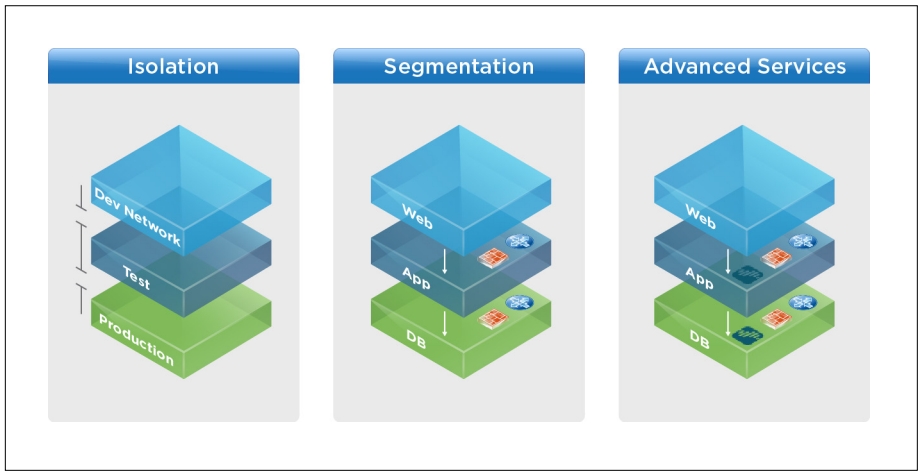

Figure 2: Micro-segmentation allows you to secure traffic between virtual machines, as well as between VMs and physical hosts. You can create and apply security policies down to the virtual network interface card level. And policies will automatically move with the workload, even if the physical IP address changes. Micro-segmentation makes it even easier than it is with physical security to integrate other types of security products into the data center.

Create More Flexible and Realistic Security Policies

As shown in Figure 3, rather than using the VM's IP address or VLAN, you can apply a flexible combination of attributes to describe each workload and create the appropriate security policy for that workload, e.g., by groups, such as all HR systems, by operating system, or perhaps "all VMs handling sensitive information" (a "secret data" type).

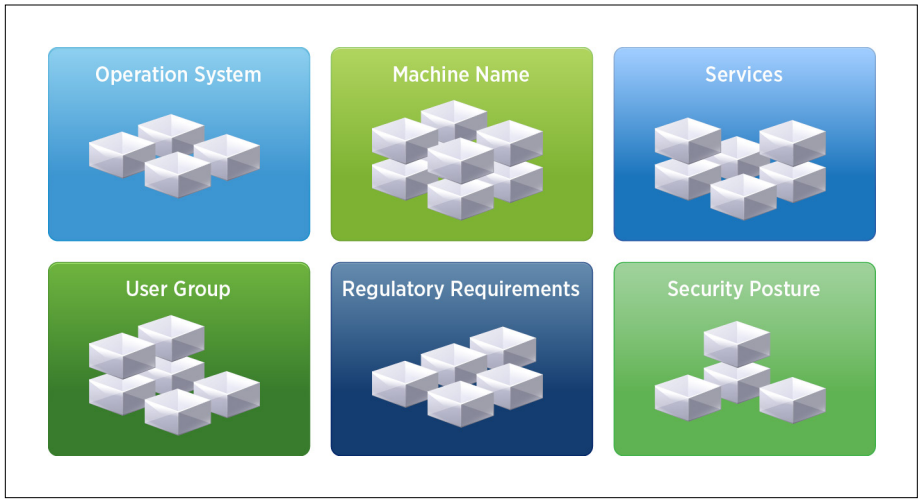

Figure 3. Because VMware NSX understands workloads, you can define groups in a way that actually reflects the function of the workload. These are just some examples of the logical ways you can define groups.

Keep Security in Synch with Dynamic Workflows

Keeping firewall rules in synch with actual workloads is virtually impossible with today's physical firewalls, whether they're outside or inside the data center. And an out-of-date policy is a vulnerability waiting to be exploited.

With the micro-segmentation model, security policies can be created in seconds. They are even automated—applied when a VM spins up, moved when a VM is migrated or changes IP addresses, and removed when a VM is deprovisioned.

Eliminate Inefficient Traffic Patterns that Lead to Overprovisioning

Figures 4 and 5. Enforcing security using VMware NSX and micro-segmentation eliminates some of the inefficient traffic patterns that are inevitable with physical security, such as hair-pinning, which results in core link oversubscription.

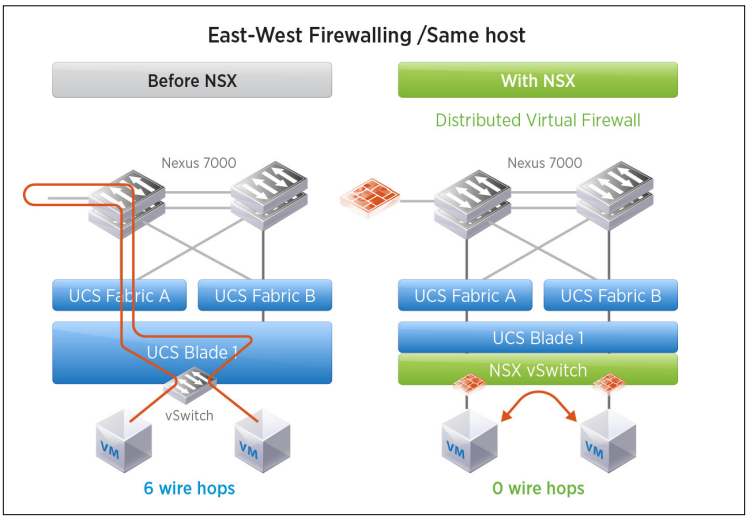

Figure 4: East-west firewalling on the same host using micro-segmentation with VMware NSX shows how you can create more efficient traffic patterns (in this case, reducing the number of hops from 6 to 0).

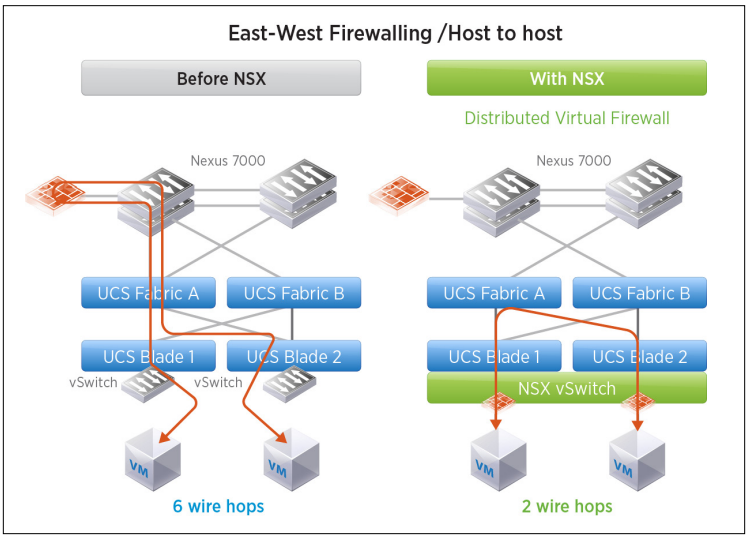

Figure 5: East-west firewalling from host to host using micro-segmentation with VMware NSX shows how you can create more efficient traffic patterns (in this case, reducing the number of hops from 6 to 2).

Enhance Security through VMware's Ecosystem of Technology Partners

NSX is the platform for an ecosystem of technology partners. These partner solutions ensure that you can continue to enhance your security capabilities to adapt to constantly changing conditions in the data center. For example, Palo Alto Networks is a partner in the VMware ecosystem. Palo Alto Networks' integration with VMware NSX adds the ability to:

- Efficiently add advanced, next-gen firewalling and IPS security to workloads inside the data center.
- Share intelligence with other security products in the VMware NSX ecosystem to adapt to emerging security conditions in the data center.

Ease of Implementation

If you have VMware NSX, you are ready to introduce micro-segmentation. Because hypervisors are already distributed throughout the data center, micro-segmentation is easy to implement:

NSX runs on top of any network hardware, so you don't have to buy or replace any appliances to deploy micro-segmentation. In addition, there's minimal disruption to the physical security infrastructure you have in place today.

Simplifying Complexity and Adapting Faster to Change

Following are two examples of how micro-segmentation can make even the most complex or fast-changing security scenarios easy to implement.

Figure 6 illustrates how easily micro-segmentation can make security more granular without adding complexity.

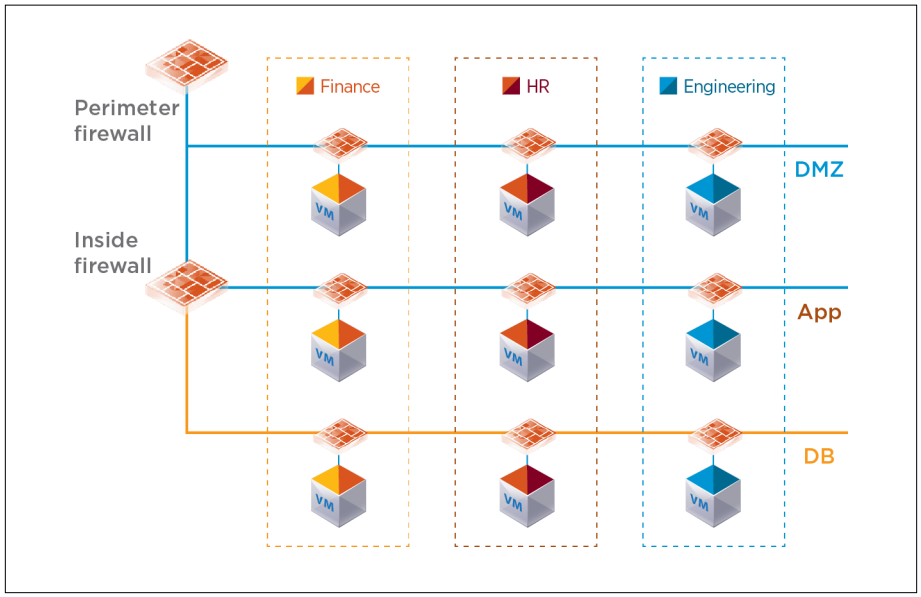

Figure 6. As shown here, micro-segmentation allows you to protect each VM with its own perimeter security (granularity that would not be practical with a physical firewall). With this granularity, it becomes easy to align policies with logical groups. It also prevents malware from spreading, as it is more likely to do in the old trust zone model.

VMware NSX Brings Realization of Software Defined Data Center Closer

The Software Defined Data Center (SDDC) is a data center model that enables administrators to bring up new applications in a matter of minutes, rather than weeks, and that includes compute, storage, network and security provisioning. SDDC is also easy to change, simpler to manage, and more responsive to your business.

A significant—and non-disruptive step—towards SDDC is VMware NSX, the network virtualization platform for SDDC. VMware NSX makes the network infrastructure more nimble in a myriad of ways. One of the most important benefits is the ability to build security into the DNA of your data center with micro-segmentation. But there are many more benefits of VMware NSX, including:

- Accelerate network provisioning and streamline operations.
- Facilitate an even greater degree of data center consolidation.
- Enable unrestricted workload mobility and placement.
- Enable push-button, zero-compromise disaster recovery.
- Save thousands if not millions of dollars in periodic and recurring costs associated with updating a physical infrastructure.

Figure 7 illustrates how micro-segmentation also simplifies the security for virtual desktop deployments. Consider an example in which the IT department has decided to virtualize the desktops throughout Human Resources (HR). With traditional hardware-based perimeter security, securing virtual desktops in the data center would add yet another level of complexity to the matrix of security policies, since the policies would have to be mapped back to the network position of the virtual desktops.

With micro-segmentation, however, creating and applying security policies is possible based on the flexible attributes of the desktops themselves: for instance, the type of operating system, the names of the machines, or in this case, the user group (HR). Deploying security for the virtual desktops for HR takes a matter of minutes. It is also non-disruptive to the security policies that are already in place for the other departments and applications. And there are no additional costs required for new appliances.

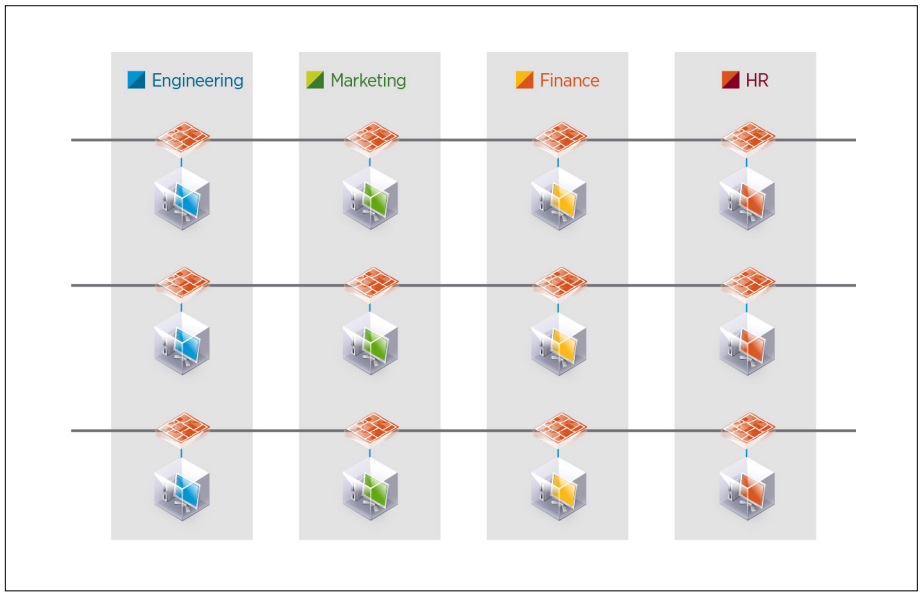

Figure 7. With micro-segmentation, creating a new policy based on VDI takes minutes and does not involve changing other policies already in place.

Conclusion

With network virtualization, micro-segmentation has become a practical and powerful reality. Data center administrators no longer have to predetermine where security needs to be located, because it's available anywhere. Policies can be created to match workloads and change as readily as workloads change. Security is pervasive, but not rigid. It's revolutionary, but not disruptive to your existing infrastructure.

Micro-segmentation enabled by VMware NSX blankets the data center itself with complete, adaptive protection. In short, your data center now has security infused into its operational DNA.

Learn more about micro-segmentatiion and VMware NSX at: http://www.vmware.com/products/nsx/.

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