Beyond Firewalls and Virtual Appliances: Making Micro-Segmentation Work

Micro-segmentation, enabled by VMware NSX®, makes "Zero Trust" model a reality

Securing the Modern Data Center Requires Micro-Segmentation

Analysts like Gartner and Forrester agree that data center security requirements have become far more complex than perimeter (physical) firewalls can handle. Here are a few of the reasons why:

- Designed to act more as guardians at the gate, perimeter firewalls, intrusion prevention and anti-virus mechanisms are designed to protect data traveling from client to server (north-south), not server to server (east-west)
- It's impractical to populate a data center with the number of physical firewalls (or physical firewalls with virtual firewalls) required to protect hundreds of workloads with fine-grained policies and centralized access control
- Physical firewalls have too much administrative overhead to adapt quickly to dynamic workloads that are in an almost constant state of change; they also don't have the context, granularity or automated capabilities to "follow" workload migration

As data centers continue to move towards virtualization for compute, networking and storage resources, traditional perimeter-based security becomes even less effective. The new model for data center security will be: a) software-based, b) use the principle of micro-segmentation, and c) embrace a Zero Trust[1] (ZT) model.

Until now, data centers were based on "trust zones," where traffic across similar compute systems was assumed to be trustworthy. But within trust zones, malware can move from server to server unchallenged. The ZT model says that in a more virtualized world there should be no distinction between trusted and untrusted networks or segments—protection must be pervasive and granular.

In order to build a ZT model, you need a virtualized network that provides micro-segmentation.

NEW MODEL FOR DATA CENTER SECURITY

- Software-based
- Use the principle of micro-segmentation
- Embrace a Zero Trust (ZT) model

1. Leverage Micro-Segmentation to Build a Zero Trust Network, Forrester Research, 2015

"What's the Difference Between Physical Network Segmentation and Micro-Segmentation?"

Physical network security in the data center is based on setting up security segments, creating subnets and virtual LANs, and creating policies around them. Essentially, this model requires locking policies to the physical location of workloads. Such a rigid construct leads to manual, time-consuming administration, frequent configuration errors, performance penalties, and application deployment delays—just to name a few constraints and frustrations.

With the VMware NSX platform, micro-segmentation is native to the network architecture, rather than bolted on. It's analogous to how plants can be engineered at the molecular or cellular levels for pest and disease resistance. That's why VMware describes micro-segmentation as the ability to "build security into your network's DNA."

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. The physical network becomes a pool of transport capacity.

Security policies are enforced by firewall controls that are integrated into the hypervisors already distributed throughout the data center with NSX. That means you have an instantly ubiquitous security blanket across the data center. (Your existing physical firewalls and physical network can all remain unchanged—although you'll gain greater freedom in mixing and matching vendors.)

Because of its place in the hypervisor, NSX offers both context and isolation: that means it's close enough to the applications and workloads to have rich context, yet removed enough to isolate these assets from threats.

Here are other significant benefits of micro-segmentation:

- Security policies are tied to your virtual network, virtual machine, and operating system, providing granularity down the virtual network interface card (in essence, micro-segmentation allows you to wrap security around each individual machine or workload, which is why security can be added, deleted, changed and moved like a file)
- You can define security policies with flexible parameters, such as virtual machine name, workload type, and guest operating system type
- Security policies can be updated in seconds—and even automatically—to respond to security threats or changes in application topologies
- Policies automatically move with the workload, even if the physical IP address changes

NSX offers both context and isolation: that means it's close enough to the applications and workloads to have rich context, yet removed enough to isolate these assets from threats.

VMWARE SECURITY PARTNER ECOSYSTEM

Security is inherently a multi-vendor environment in the data center. Security controls are native to NSX, which means it provides a platform for integration. Industry leading security products can be deployed automatically and adapt dynamically. Here are some of VMware's security partners:

- Check Point
- Fortinet
- Intel Security/McAfee
- Palo Alto Networks
- Symantec
- Trend Micro

"What Security Projects Benefit Most from Micro-segmentation?"

You can deploy network virtualization on your own timetable, starting with small steps and expanding in planned phases or opportunistically. Your security strategy can follow deployment of network virtualization or be a driver for network virtualization. Here are three project examples:

Data Center Security

We've covered how micro-segmentation can protect every workload in the data center with fine-grained security policies. Centralized control and automation are equally important for protecting hundreds and hundreds of workloads. When a VM is created, its security policies are automatically attached to it. When the VM moves, the policies follow. When the VM is decommissioned, the policies are automatically deleted. With automation, there's no possibility of firewall rules becoming stale and creating a potential vulnerability.

Secure Desktop User Environments

With micro-segmentation, you can create a personal perimeter defense around the individual desktop user. If the user downloads a virus, for example, the "personal DMZ" will prevent the spread from the desktop and any other desktops sharing information, and between the desktop and the data center.

DMZs Anywhere

Micro-segmentation gives you the ability to isolate any segment and place it within a DMZ. Advanced policies and enforcement are not dependent on IP addresses. Creating a DMZ is no longer restricted to a specific place in the network, but rather associated with the workload that it's protecting.

Even "attributes" don't have to be dictated by topology or arcane firewall naming conventions. Administrators can set policies and security services that map to an individual workload based on role, logical grouping (such as all HR systems), desktop operating system, or even "all VMs handling sensitive information."

Conclusion

High-profile breaches of data centers continue to cause costly damage and disruption. In response, IT organizations have increased spending on traditional physical security, but these hefty investments haven't stopped escalating attacks, for the simple reason that physical network security, especially perimeter firewalls, is not the full answer to securing the data center.

Micro-segmentation has been widely regarded as a better model for data centers, particularly as IT moves towards the Software-defined Data Center (SDDC) and hybrid cloud model. VMware NSX makes micro-segmentation a practical reality. For the first time, administrators can apply fine-grained policies to isolate and protect applications and workloads. Network security can be as pervasive as data centers require and as dynamic as the assets they're protecting.

Learn more: vmware.com/products/nsx

vmware

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