CONTEXT-AWARE MICRO-SEGMENTATION WITH VMWARE NSX DATA CENTER

Protect the Network from the Lateral Spread of Threats

Modern Applications Are Complex, Distributed, and Dynamic

Every organization is figuring out how to operate their business in the hyper-connected world in which applications and data are the lifeblood. Modern applications are distributed across multiple data centers and clouds, and extended out to the edge of the environment.

Virtualization, along with the advent of DevOps, containerization, and microservices, have enabled applications to be built and changed faster than ever. The distributed nature of modern applications and the speed with which they change make maintaining security a major challenge.

Legacy Security Strategies Are No Longer Effective

As the sprawl of applications continues, legacy perimeter-centric security approaches prove to be insufficient for protecting applications and data. Attackers have proven they can penetrate or circumvent perimeter security measures time and again. Once inside, they move laterally—from server to server—unimpeded, looking for information to steal or hold for ransom.

In the world of modern distributed applications, IT security and networking teams are often challenged with maintaining disparate security policies across different parts of their environment, leading to gaps in the overall security posture.

Consistent Security from the Data Center, to the Cloud, to the Edge

With VMware NSX® Data Center, security policies can be defined consistently across the entire environment, regardless of the type of application or where it has been deployed. Policies are enforced at the individual workload level, which enables the segmentation of workloads that live on the same physical host without having to hairpin traffic out through an external physical or virtual firewall. This granular level of security is called micro-segmentation.

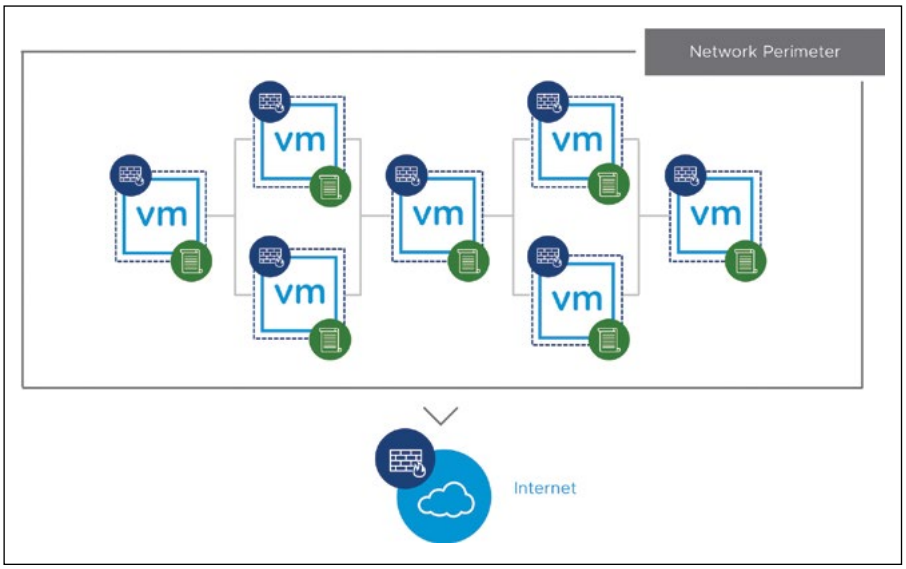

Figure 1. Micro-segmentation refers to the enforcement of network security policy at the individual workload level.

"With the increasing number of IoT devices, the more segmented our network is, the better off we are...That way, threats can't move laterally within the data center."

CHRISTOPHER FRENZ
DIRECTOR OF INFRASTRUCTURE
INTERFAITH MEDICAL CENTER

KEY HIGHLIGHTS

- The distributed, dynamic nature of modern applications makes legacy, perimeter-centric security insufficient.
- VMware NSX Data Center enables micro-segmentation to protect applications from the lateral spread of threats.
- Security policy gets defined based on application context and enforced on the individual workload.
- Security is delivered consistently from the data center, to the cloud, to the edge.

Micro-segments built with NSX Data Center are defined and managed in software, making them agile and automatable. As new workloads get deployed, they automatically inherit the security policies that stay with the workload throughout its lifecycle, no matter where it has been provisioned or where it might move to.

Context-Aware Micro-Segmentation, Security Aligned to Applications and Data

The ability to define security policies based on what matters most is equally as important as consistent delivery of the policies. NSX Data Center decouples security policy from static network attributes like IP address, port, and protocol, and allows for the definition of policies based on a contextual understanding of the application and the infrastructure. These contexts include user and identity attributes, workload attributes (like operating system), or even regulatory compliance scopes.

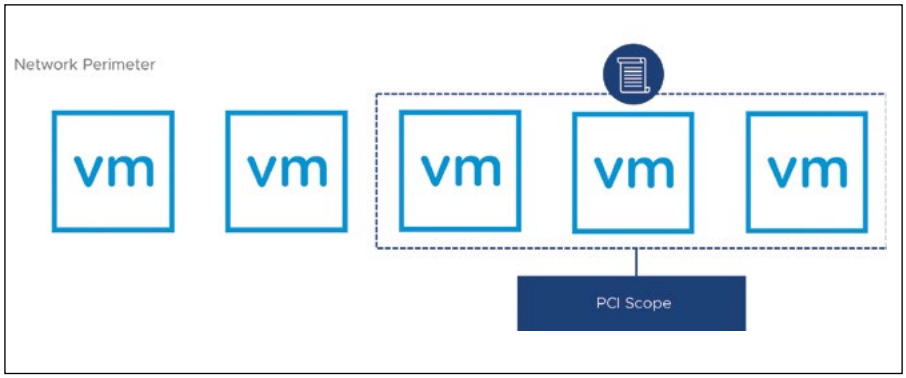

Figure 2. Micro-segments in NSX Data Center can be defined based on a number of different contexts, including regulatory compliance scopes.

Context-aware micro-segmentation with NSX Data Center gives network security teams the flexibility they need to secure their applications and data based on the factors that matter most. For example, NSX Data Center can be used to secure a virtual desktop infrastructure (VDI) deployment by enforcing network policy based on user context down to the level of the individual RDSH session. Or security policies could be applied to all workloads that fall under payment card industry (PCI) standards, regardless of where they physically exist within the environment.

Advanced Security Services When and Where They Are Needed

NSX Data Center allows for the insertion of advanced third-party security services into a given micro-segment. Rather than routing all network traffic through a physical device or virtual appliance, like a next-generation firewall (NGFW) or intrusion detection system (IDS)/intrusion prevention system (IPS), NSX Data Center can dynamically steer specific traffic to these services at the virtual network layer. By doing so, advanced security services can be inserted at the right places, at the right time, maximizing network traffic efficiency while increasing the efficacy of the security services themselves.

Get Visibility into Network Traffic Across the Entire Environment

The first step to micro-segmentation is understanding how network traffic flows today. VMware Network Insight™ provides a comprehensive view of all network traffic within the data center, including both physical and virtual network traffic. After analyzing network traffic, VMware Network Insight will automatically recommend micro-segmentation policies that can be consumed by NSX Data Center for implementation.

Get started today with a free virtual network assessment to analyze your current network traffic and begin planning your micro-segmentation project. To learn more, visit www.vmware.com/products/nsx/security.

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