SOLUTIONS OVERVIEW

NSX Micro-segmentation

Advanced security *inside* the data center network

"Given our work in the financial sector, security is very important to us, and the ability to do micro-segmentation was a key to our selection of VMware NSX™. We explored doing this at the hardware level, but quickly realized it was not feasible. The proven success of the NSX platform, and the integration of other industry leaders such as Arista Networks, and Palo Alto Networks, helped solidify our decision. NSX will help us maintain our competitive advantage in terms of security and agility – specifically moving applications around within our cloud safely and reliably. NSX will transform what's possible for our IT team in terms of network and security operations."

Trever Jackson
Enterprise Infrastructure Architect
Synergent

Micro-segmentation and fine-grained security inside the data center is operationally feasible for the first time with VMware NSX.

Deploy advanced security inside the data center with NSX and micro-segmentation.

The standard approach to securing data centers has emphasized strong perimeter protection to keep threats on the outside of the network. However, this model is ineffective for handling new types of threats – including advanced persistent threats and coordinated attacks. What's needed is a better model for data center security: one that assumes threats can be anywhere and probably are everywhere, then acts accordingly. Micro-segmentation, powered by VMware NSX™, not only adopts such an approach, but also delivers the operational agility of network virtualization that is foundational to a modern software-defined data center.

Threats to Today's Data Centers

Research shows that more than 30 percent of data center outages are caused by cyber attacks, and a 60 minute outage can cost businesses upwards of half a million dollars[i]. Cyber threats today are coordinated attacks that often include months of reconnaissance, vulnerability exploits, and "sleeper" malware agents that can lie dormant until activated by remote control. Despite increasing types of protection at the edge of data center networks – including advanced firewalls, intrusion prevention systems, and network-based malware detection – attacks are succeeding in penetrating the perimeter, and breaches continue to occur.

The primary issue is that once an attack successfully gets past the data center perimeter, there are few lateral controls to prevent threats from traversing inside the network. The best way to solve this is to adopt a stricter, micro-granular security model with the ability to tie security to individual workloads and the agility to provision policies automatically. The research firm Forrester calls this "Zero Trust," and micro-segmentation embodies this approach. With micro-segmentation, fine-grained network controls enable unit-level trust, and flexible security policies can be applied all the way down to a network interface. In a physical network, this would require deploying a physical firewall per workload, so up until now, micro-segmentation has been cost-prohibitive and operationally infeasible.

The Solution: VMware NSX & Micro-segmentation

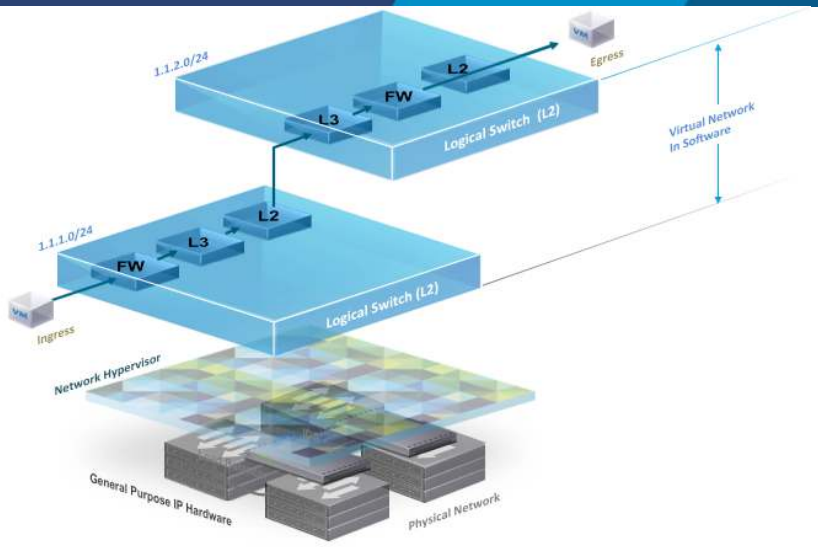
VMware NSX is a network virtualization platform that for the first time makes micro-segmentation economically and operationally feasible. NSX provides the networking and security foundation for the software-defined data center (SDDC), enabling the three key functions of micro-segmentation: isolation, segmentation, and segmentation with advanced services. Businesses gain key benefits with micro-segmentation:

1. **Network security *inside* the data center**: flexible security policies aligned to virtual network, VM, OS type, dynamic security tag, and more, for granularity of security down to the virtual NIC.
2. **Automated deployment for data center agility**: security policies are applied when a VM spins up, are moved when a VM is migrated, and are removed when a VM is deprovisioned – no more stale firewall rules.
3. **Integration with leading networking and security infrastructure**: NSX is the platform enabling an ecosystem of partners to integrate – adapting to constantly changing conditions in the data center to provide enhanced security. Best of all, NSX runs on existing data center networking infrastructure.

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

NSX Micro-segmentation

Advanced security *inside* the data center network



NSX virtual networks enable advanced security with micro-segmentation.

Isolation	Segmentation	Segmentation with Advanced Services
NSX enables parallel virtual networks using overlay technology – each fully isolated from other virtual networks and from the underlying physical network. Because NSX runs on top of existing network and data center equipment, businesses preserve their infrastructure investments.	NSX secures communication within a virtual network with flexible security policies that mirror business logic and workflows. Beyond using IP addresses, NSX policies incorporate virtual machine name, virtual network, OS, and more – streamlining configuration and reducing errors.	More than an SDDC virtual networking solution, NSX is a platform for advanced services, supporting an ecosystem of leading security vendors. IT admins continue using their existing security products from vendors such as Palo Alto Networks, Trend Micro, Symantec, McAfee, and Rapid 7. On NSX, these security products leverage dynamic security tags – sharing security information to adapt to changing security conditions.

Bringing it Together

These micro-segmentation capabilities make NSX ideal for securing intra-data center network traffic, for fully isolating disparate networks (e.g., for highly sensitive workloads or for multi-tenancy), and for simplifying networks that would otherwise require complex access policies – such as virtual desktop infrastructure (VDI).

Find Out More

For more information on NSX and micro-segmentation, visit the VMware NSX site at http://www.vmware.com/go/nsx. For information or to purchase VMware products, call 1-877-4VMWARE (outside of North America dial +1-650-427-5000), visit http://www.vmware.com/products, or search online for an authorized reseller.

[i] Security Week: "Cyber Attacks Are The Root Cause in 30 Percent of Data Center Outages: Study", December 13, 2013.