Seven Reasons Why Micro-Segmentation is Powerful to Have and Painless to Add

WHY THE DATA CENTER NEEDS A STRONGER IMMUNE SYSTEM

Attacks on the data center are increasing, and physical security appliances aren't sufficient to stop them. Independent research shows that successful attacks are happening with startling regularity and are increasingly costly to companies. There's no question that we need a new model for data center security if the industry is going to turn these statistics into ancient history, rather than unstoppable trends.

Perimeter firewalls may be stalwart and steady as guards at the gate. But once malware gets inside the data center (often by piggybacking on legitimate traffic), there are virtually no restrictions on how much malware can spread.

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. It isn't technically or economically feasible to populate a data center with enough physical firewalls to protect hundreds and hundreds of workloads.

Pervasive, Granular, Dynamic Security Must Be Part of the Data Center's DNA

Micro-segmentation is one of the breakthrough benefits of the VMware NSX™ network virtualization platform. NSX creates a virtual network that is independent of the underlying IP network hardware. Administrators can programmatically create, provision, snapshot, delete and restore complex networks all in software.

VMware describes micro-segmentation as the ability to "build security into your network's DNA." The best analogy is how plants can be engineered at the molecular or cellular levels to be pest and disease resistant.

Because hypervisors are already distributed throughout the data center, with VMware NSX you can create policies anywhere to protect anything, making security truly pervasive. In a sense, physical security is like using gloves to guard against germs. It's 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 at it. Or, if something does, the system can shut it down before it spreads.

Policies are tied to virtual machines, with enforcement all the way down to the virtual network interface card, creating granularity that also isn't possible with traditional hardware appliances.

You can also define security policies with flexible parameters, such as virtual machine name, workload type, and guest operating system type.

Seven Reasons Why Micro-Segmentation is Powerful to Have and Painless to Add

1. **No Ripping or Replacing What you Have in Place**
   VMware NSX runs on top of any network hardware, so you don't have to buy or replace any appliances. In addition, there's no disruption to your computer and networking infrastructure or applications.

2. **Reduce Escalating Hardware Costs**
   Deploying more physical appliances to handle the growing volume of workloads inside the data center is cost-prohibitive. Looking at the capital expense alone, VMware NSX is enabling actual enterprise organizations to save 68%[1]. This savings is based on estimating what physical firewalls would cost if IT administrators tried to approximate the same degree of control that micro-segmentation provides.

3. **Curtail Firewall Rule Sprawl**
   Bloated firewall rules are a real problem in security management. Over the years, administrators can inherit unnecessary and redundant rules, and there's no easy way to figure out which rules are no longer needed. Firewall rule sprawl can make security audits nightmarish. Out-of-date and conflicting rules can even be an unintended source of security vulnerabilities.

[1] "Network Virtualization and Security with VMware NSX", Business Case White Paper; Analysis based on comparative costs using firewall technology.

With micro-segmentation and VMware NSX, policies are orchestrated centrally and linked to the VMs they protect, so you can automate security policy management throughout the entire data center via a single interface. When a VM is provisioned, moved or deleted, its firewall rules are also added, moved or deleted.

4. **Tune-Up Performance with more Efficient Traffic Patterns**
   With physical networks, workload traffic is often required to traverse more than one network segment to reach routers and firewalls, only to come back to an adjacent workload (an inefficient pattern called hair-pinning). With micro-segmentation, traffic can usually stay in the same virtual network segment, reducing the impact on the physical network. As a result, you eliminate the extra costs and inefficiencies associated with over-subscribing core links.

5. **Meet the Individual Needs of LOBs and Departments**
   Because VMware NSX and micro-segmentation work independently of your physical infrastructure, you gain tremendous flexibility in moving resources around and keeping security in lockstep with change. Because security is handled through software, policies can be created and operational within minutes, eliminating the lag time associated with installing more security hardware or reconfiguring network systems.

   Figure 1 shows how easily you can update security policies to match the needs of individual LOBs and departments. In this example, the IT department has decided to virtualize the desktops throughout Human Resources (HR). With micro-segmentation, creating and applying the security policies for the virtual desktops for HR takes a matter of minutes. You simply tag all relevant systems "HR" and VMware NSX automatically applies the correct security policies.

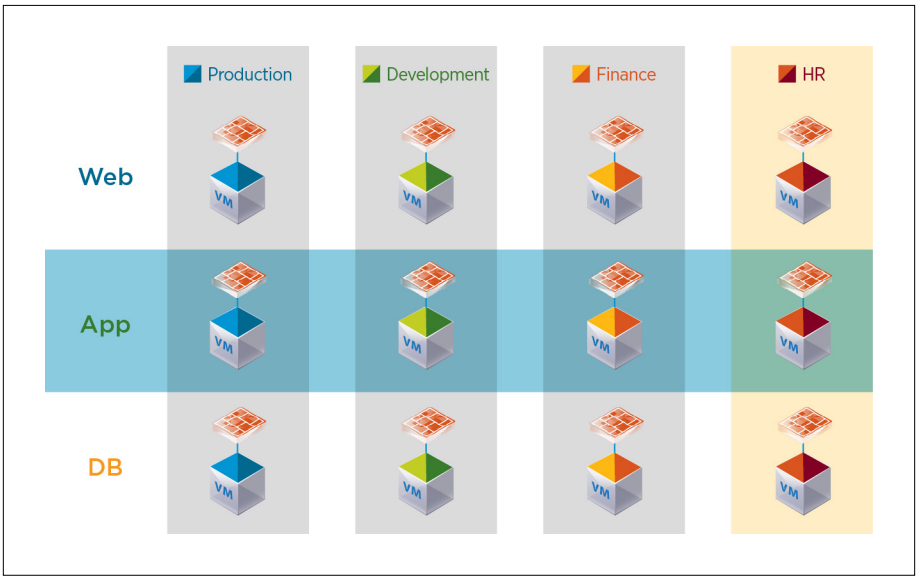

Figure 1 With micro-segmentation, creating a new security policy based on VDI takes minutes and doesn't involve changing other policies already in place.

6. **Add a Valuable New Knowledge Area for your Networking Specialists**
   Administrators use the same skill sets that they have acquired around VMware virtualization, so major security improvements don't require a major learning curve. Hardware networking specialists acquire new software skills that keep them at the leading edge of both hardware and software networking security technologies. Developing expertise in the Software-Defined Data Center (SDDC) and network virtualization areas are a tremendous addition to the professional skills of network administrators and architects.

7. **Future Proof your Operations**
   Micro-segmentation makes securing workloads much easier, faster and less expensive. As a result, you can support changes with greater confidence, and even reallocate resources to new project areas.

   Network virtualization with VMware NSX is also a significant—and non-disruptive—step towards the SDDC model. Which means you're not only strengthening security today, you're laying important groundwork for SDDC in the future.

Learn More

For information visit www.vmware.com/go/nsx. For detailed product specifications and system requirements, refer to the VMware NSX documentation.

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