Data Center Micro-Segmentation

A Software Defined Data Center Approach for a ”Zero Trust” Security Strategy

WHITE PAPER

vmware®

Table of Contents

Executive Summary

The software-defined data center (SDDC), while well understood architecturally, is beginning to reveal some of its benefits beyond agility, speed, and efficiency as organizations deploy and discover other areas of improvement. One critical area organizations are driving SDDC deployment from is security.

When enterprises and public sector IT organizations embrace SDDC and virtualize compute, network, and storage, they automate provisioning and greatly reduce time-to-market for IT applications and services. They also streamline and de-risk infrastructure moves, adds, and changes. This new operations model has some additional benefits. Where customers build their SDDC with the automation and "baked-in" security of VMware's NSX platform, they've discovered some significant security benefits – fortuitously – as many organizations are trying to move to an increasingly fine-grained network segmentation approach (e.g., Forrester Research's Zero-Trust Network Architecture) for their data center networks in response to the increasing incidence of attackers moving freely within the enterprise data center perimeter. These approaches wrap security controls around much smaller groups of resources – often down to a small group of virtualized resources or individual VMs. Micro-segmentation has been understood to be a best practice approach from a security perspective, but difficult to apply in traditional environments. The inherent security and automation capabilities of the NSX platform are making micro-segmentation operationally feasible in the enterprise data center for the first time.

VMware NSX deploys three modes of security for data center networks – fully isolated virtual networks, segmented virtual networks (via high-performance, fully automated firewalling native to the NSX platform), and segmentation with advanced security services with our security partners. Examples of partner integration include Palo Alto Networks for network segmentation with next-generation firewalls or Rapid7 for vulnerability scanning.

When it comes to the business case, network micro-segmentation is not only operationally feasible using VMware NSX, but cost-effective, enabling the deployment of security controls inside the data center network for a fraction of the hardware cost.

Many large data centers are using security as one of the big first benefits of the software defined data center. In the very near future, a more secure data center will become the new normal.

The Software Defined Data Center is the Future

A Software Defined Data Center (SDDC) is an architectural approach to data center design, which leverages a fundamental principle of computer science, abstraction. Operating systems, higher-level programming languages, networking protocols, and most recently server virtualization are all examples of abstractions whose introductions resulted in major industry innovation cycles over the past 25 years. The introduction of an abstraction layer allows systems and services above and below the abstraction layer to operate and innovate independently, while maintaining agreed-upon communication paths and exposing services between layers through well-defined interfaces. An SDDC approach applies the principles of abstraction to deliver an entire data center construct in software, decoupling service delivery from the underlying physical infrastructure. This allows the underlying hardware to be utilized as generalized pools of compute, network and storage capacity which can be combined, consumed and repurposed programmatically, without modification to the hardware.

The SDDC approach has been proven by many of the largest, most agile and efficient data centers in the world, including Google, Facebook and Amazon. Over the past 10 years, these “mega data center” operators have engineered an SDDC abstraction layer into their custom applications and platforms, allowing them to automate almost every aspects of data center operations, while completely decoupling from the underlying compute, network and storage hardware. This decoupling dramatically reduces both the capital and operational expense of their physical infrastructure and allows them to deliver services orders of magnitude faster than most enterprise IT organizations.

Today, enterprise IT can achieve the same level of agility and efficiency as “mega data centers” in their own data centers, without modification to their existing hardware infrastructure.

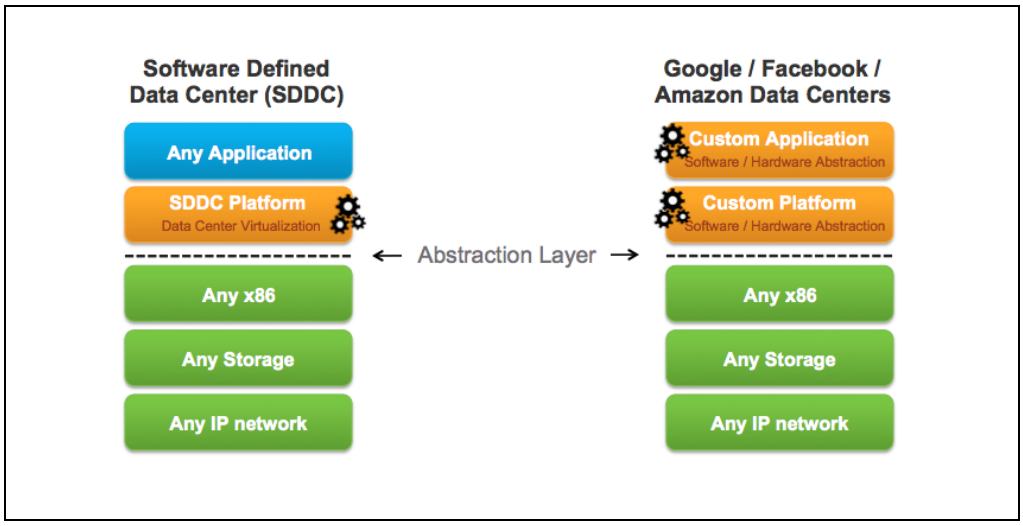

Figure 1 - Intelligence is moved into software to create an abstraction layer between software and the underlying physical infrastructure. Large data centers have been doing this for a decade by putting intelligence in their custom application or platform software. Today enterprise data centers can achieve the same decoupling by leveraging software in the data center virtualization layer.

VMware has built the data center abstraction layer into its NSX network virtualization platform. The platform is based on a distributed system controller combined with the traditional hypervisor and vSwitch to allow the entire data center construct to be faithfully reproduced non-disruptively in software, independent of the existing physical infrastructure. The VMware NSX platform has been proven in production deployments, some over three years old and is now being deployed at two of the top three service providers in the world, four out of top five global financial services companies, and over 100 enterprise class datacenters in almost every business sector including healthcare, manufacturing, retail, consumer products, banking, insurance, transportation, federal, state and local government and high tech.

The SDDC is More Agile, More Flexible, and More Secure

An SDDC approach takes the benefits of virtualization and automation and extends it to incorporate the entire data center construct. The ability to programmatically create, snapshot, move, delete and restore virtual machines in software transformed the operational model of compute for IT. Now, an SDDC approach allows IT to programmatically create, snapshot, move, delete and restore an entire data center construct of compute, storage, and network in software. Data center automation, self-service IT, and a complete transformation of the network operational model have proven to be huge benefits of an SDDC approach. In deployments, business and IT leadership agree that an SDDC approach delivers measureable differences in IT speed, agility, and competitive advantage. IT operations leaders quickly benefit from automated change management and simplification of the underlying hardware configuration and management. Perhaps most profoundly, the SDDC approach powers the infrastructure and security teams' ability to achieve investment flexibility (build to mean and burst to hybrid) and protection (utilize existing hardware), increased utilization, and never before possible security in the data center. In fact, security has proven to be one of the most compelling applications of the SDDC platform.

The SDDC – A Weapon, not a Target

At first glance, most IT network security professionals will view a new approach like a SDDC as a new potential target. The reality is, the impact to the way IT does security is far greater (and more positive) than the changes to what needs to be secured. In other words, for IT security teams, SDDC is more of a weapon than a target. An SDDC approach actually delivers a platform that inherently addresses some fundamental architectural limitations in data center design, which have restricted security professionals for decades.

Consider the trade-off that is often made between context and isolation in traditional security approaches. Often, in order to gain context we place controls in the host operating system. This approach allows us to see what applications and data are being accessed and what users are using the system, resulting in good context. However, because the control sits in the attack domain, the first thing an attacker will do is disable the control. This is bad isolation. This approach is tantamount to putting the on/off switch for a home alarm system on the outside of the house. An alternative approach, which trades context for isolation, places the control in the physical infrastructure. This approach isolates the control from the resource it's securing, but has poor context because IP addresses, ports and protocols are very bad proxies for user, application, or transaction context. Furthermore, there has never been a ubiquitous enforcement layer built into the infrastructure…until now.

The data center virtualization layer used by the SDDC offers the ideal location to achieve both context and isolation, combined with ubiquitous enforcement. Controls operating in the data center virtualization layer leverage secure host introspection, the ability to provide agentless, high definition host context, while remaining isolated in the hypervisor, safe from the attack being attempted.

The ideal position of the data center virtualization layer between the application and the physical infrastructure combined with automated provisioning and management of network and security policies, kernel embedded performance, distributed enforcement, and scale-out capacity is on the verge of completely transforming data center security and allowing data center security professionals to achieve levels of security that in the past were operationally infeasible.

The Dawning of the Truly Micro-segmented Data Center Network

The perimeter-centric network security strategy for enterprise data centers has proven to be inadequate. Modern attacks exploit this perimeter-only defense, hitching a ride with authorized users, then move laterally within the data center perimeter from workload to workload with little or no controls to block their propagation. Many of the recent public breaches have exemplified this – starting with spearphishing or social engineering, leading to malware, vulnerability exploits, command and control, and unfettered lateral movement within the data center until the attackers find what they are looking for – which is then exfiltrated.

Micro-segmentation of the data center network can be a huge help to limit that unauthorized lateral movement, but hasn't been operationally feasible in traditional data center networks. Why?

Traditional and even advanced next-generation firewalls implement controls as physical or virtual "choke points" on the network. As application workload traffic is directed to pass through these control points, rules are enforced and packets are either blocked or allowed to pass through. Using the traditional firewall approach to achieve micro-segmentation quickly reaches two key operational barriers – throughput capacity and operations/change management. The first, capacity, can be overcome at a cost. It is possible to buy enough physical or virtual firewalls to deliver the capacity required to achieve micro-segmentation. However, the second, operations, increases exponentially with the number of workloads and the increasingly dynamic nature of today's data centers. If firewall rules need to be manually added, deleted and/or modified every time a new VM is added, moved or decommissioned, the rate of change quickly overwhelms IT operations. It's this barrier that has been the demise of most security team's best-laid plans to realize a comprehensive micro-segmentation or "Zero-trust" strategy.

A VMware SDDC approach leverages the NSX network virtualization platform to offer several significant advantages over traditional network security approaches – automated provisioning, automated move/add/change for workloads, distributed enforcement at every virtual interface and in-kernel, scale-out firewalling performance, distributed to every hypervisor and baked into the platform.

Performance

It's important to note that the firewalling performance offered in the NSX platform is not intended to replace hardware firewall platforms used for North-South perimeter defense. The performance capacity of hardware firewall platforms is design to control traffic flowing from hundreds or thousands of workloads entering or leaving the data center perimeter.

That said, the firewalling performance and capacity of the NSX platform is more than impressive. The NSX platform delivers 20Gbps of firewall throughput and supports over 80K connections per second, per host. This performance is only applied to the VMs on its hypervisor and every time another host is added into the SDDC platform, another 20Gbps or throughput capacity is added.

Automation

The automated provisioning and move/add/change enables the correct firewall policies to be provisioned when a workload is programmatically created and those policies follow the workload as it is moved anywhere in the data center or between data centers. And, if the application is every deleted, it's security policies are removed from the system with it. This eliminates the key barrier, which has made the delivery of a true micro-segmentation solution infeasible.

Furthermore, the NSX partner ecosystem can also take advantage of the distribution and automation capabilities of the SDDC/NSX platform to enable enterprises apply a combination of different partner capabilities by chaining advanced security services together and enforcing different services based on different security situations. For example, a workload may be provisioned with standard firewalling policies, which allow or restrict its access to other types of workloads. The same policy may also define that if a vulnerability is detected on the workload during the course of normal vulnerability scanning, a more restrictive firewalling policy would apply, restricting the workload to access by only those tools used to remediate the vulnerabilities. All automated, always on, without human intervention.

The combination of performance and automation delivered by the NSX platform allows operationally feasible micro-segmentation to be designed and implemented all the way down to every virtual interface.

Native Security in NSX-Powered SDDC: Isolation and Segmentation

The VMware NSX platform inherently delivers three levels of security in data centers – isolation, segmentation, and segmentation with advanced services.

Isolation

Isolation is the foundation of most network security, whether for compliance, containment or simply keeping development, test and production environments from interacting. While manually configured and maintained routing, ACLs and/or firewall rules on physical devices have traditionally been used to establish and enforce isolation, isolation and multi-tenancy are inherent to network virtualization. Virtual networks are isolated from any other virtual network and from the underlying physical network by

default, delivering the security principle of least privilege. No physical subnets, no VLANs, no ACLs, no firewall rules are required to enable this isolation. This is worth repeating…*NO configuration required*. Virtual networks are created in isolation and remain isolated unless specifically connected together.

Any isolated virtual network can be made up of workloads distributed anywhere in the data center. Workloads in the same virtual network can reside on the same or separate hypervisors. Additionally, workloads in several isolated virtual networks can reside on the same hypervisor. One very useful example: isolation between virtual networks allows for overlapping IP addresses, making it possible to have isolated development, test and production virtual networks, each with different application versions, but with the same IP addresses, all operating at the same time, all on the same underlying physical infrastructure.

Virtual networks are also isolated from the underlying physical infrastructure. Because traffic between hypervisors is encapsulated, physical network devices operate in a completely different address space then the workloads connected to the virtual networks. For example, a virtual network could support IPv6 application workloads on top of an IPv4 physical network. This isolation protects the underlying physical infrastructure from any possible attack initiated by workloads in any virtual network. Again, all of this is independent from any VLANs, ACLs, or firewall rules that would traditionally be required to create this isolation.

Segmentation

Related to isolation, but applied within a multi-tier virtual network, is segmentation. Traditionally, network segmentation is a function of a physical firewall or router, designed to allow or deny traffic between network segments or tiers. For example, segmenting traffic between a web tier, application tier and database tier. Traditional processes for defining and configuring segmentation are time consuming and highly prone to human error, resulting in a large percentage of security breaches. Implementation requires deep and specific expertise in device configuration syntax, network addressing, application ports and protocols.

Network segmentation, like isolation, is a core capability of VMware NSX network virtualization platform. A virtual network can support a multi-tier network environment, meaning multiple L2 segments with L3 segmentation or micro-segmentation on a single L2 segment using distributed firewalling defined by workload security policies. As in the example above, these could represent a web tier, application tier and database tier. Physical firewalls and access control lists deliver a proven segmentation function, trusted by network security teams and compliance auditors. Confidence in this approach for cloud data centers, however, has been shaken, as more and more attacks, breaches and downtime are attributed to human error in manual network security provisioning and change management processes.

In a virtual network, network services (L2, L3, ACL, Firewall, QoS etc.) that are provisioned with a workload are programmatically created and distributed to the hypervisor vSwitch. Network services, including L3 segmentation and firewalling, are enforced at the virtual interface. Communication within a virtual network never leaves the virtual environment, removing the requirement for network segmentation to be configured and maintained in the physical network or firewall.

Segmentation with advanced security service insertion, chaining and traffic steering

The base VMware NSX network virtualization platform provides basic stateful inspection firewalling features to deliver segmentation within virtual networks. In some environments, there is a requirement for more advanced network security capabilities. In these instances, customers can leverage the SDDC platform to distribute, enable and enforce advanced network security services in a virtualized network environment. The NSX platform distributes network services into the vSwitch to form a logical pipeline of services applied to virtual network traffic. Third party network services can be inserted into this logical pipeline, allowing physical or virtual services to be consumed in the logical pipeline.

Every security team uses a unique combination of network security products to meet the needs of their environment. The VMware NSX platform is being leveraged by VMware's entire ecosystem of security solution providers. Network security teams are often challenged to coordinate network security services from multiple vendors in relationship to each other. Another powerful benefit of the NSX approach is its ability to build policies that leverage NSX service insertion, chaining and steering to drive service execution in the logical services pipeline, based on the result of other services, making it possible to

coordinate otherwise completely unrelated network security services from multiple vendors.

For example, our integration with Palo Alto Networks (see blog post here) leverages the VMware NSX platform to distribute the Palo Alto Networks VM-Series next-generation firewall, making the advanced features locally available on each hypervisor. Network security policies, defined for application workloads provisioned or moved to that hypervisor, are inserted into the virtual network's logical pipeline. At runtime, the service insertion leverages the locally available Palo Alto Networks next-generation firewall feature set to deliver and enforce application-, user-, and content-based controls and policies at the workloads virtual interface.

Another example includes our partner Rapid7, which can enable automatic, regular vulnerability scanning of VMs, and enables a policy that automatically quarantines VMs if they don't meet a certain standard. Combining this with Palo Alto Networks' NGFW, we could have an automatic quarantine of vulnerable workloads when failing Rapid7 vulnerability scans, and the quarantine segment would be protected with a Palo Alto Networks NGFW policy that only admitted remediation tools inbound, and nothing outbound.

Cost

An SDDC approach leveraging VMware NSX not only makes micro-segmentation operationally feasible, it does it cost effectively. Typically, micro-segmentation designs begin by engineering east-west traffic to "hairpin" through high-capacity physical firewalls. As noted above, this approach is expensive and operationally intensive, to the point of infeasibility in most large environments. The entire NSX platform typically represents a fraction of the cost of the physical firewalls alone in these designs, and scales out linearly as customers add more workloads.

More Secure Data Centers – the Software Defined New Normal

Perimeter security controls will still be required, but controls internal to the data center network are not only now necessary, but fortunately now possible. As a key pillar of a software defined data center architecture, the VMware NSX network virtualization platform has opened the door to a new operational model for the security team, on the physical infrastructure you already have. No new networking hardware. Virtualize as much or as little of your data center environment as you are ready.

This paper has only scratched the surface of the security capabilities made possible by an SDDC approach and the VMware NSX network virtualization platform. As more and more data centers adopt a software-defined data center architecture, we'll see a broad range of VMware and partner solutions emerge to leverage the unique position the SDDC data center virtualization layer offers. Detailed knowledge of VMs and application process owners, combined with automated provisioning speed and operational efficiency, is the foundation for an exciting new approach to some very old data center security challenges.

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