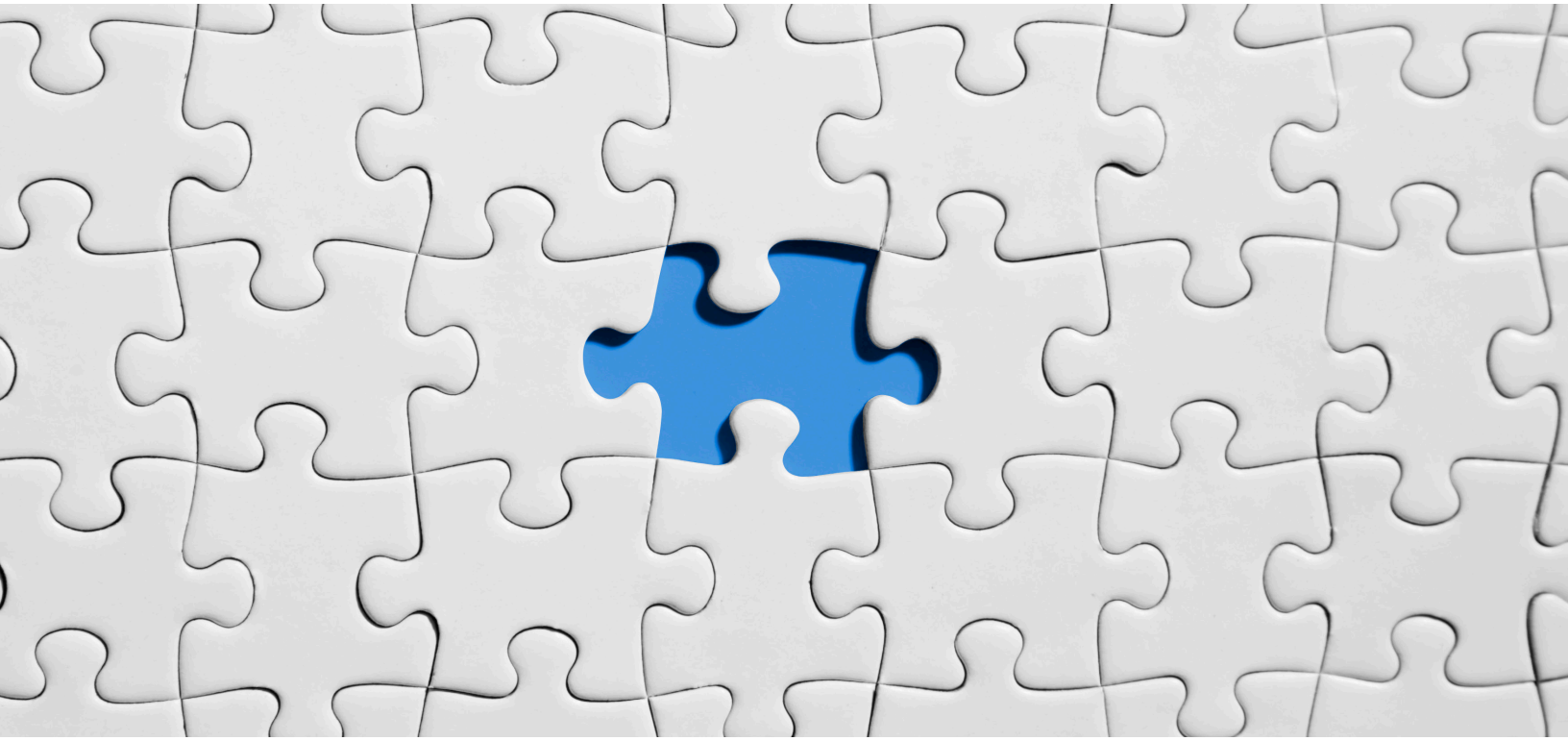
DELL Technologies

MICROSEGMENTATION: DEFENSE IN DEPTH



Sathish Kumar Ekambaram

Systems Engineer Analyst

Dell EMC

Sathishkumar.ekambar@dell.com

Varun M

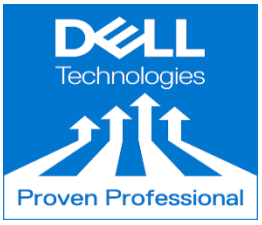
Systems Engineer Analyst

Dell EMC

Varun.m1@dell.com

DELL Technologies Proven Professional

Knowledge Sharing Article



The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

1. What is Microsegmentation?

Microsegmentation is a method of creating zones in data centers and cloud environments to isolate workloads from one another and secure them individually. With microsegmentation, system administrators can create policies that limit network traffic between workloads based on a Zero Trust approach. Organizations use microsegmentation to reduce the network attack surface, improve breach containment and strengthen regulatory compliance. In this article, we review microsegmentation technology, traditional models of VM security and why the future of virtualization security is microsegmentation, with a focus on VMware NSX.

1.1 How it works

Microsegmentation helps provide consistent security across data centers and hybrid cloud platforms alike by virtue of three key principles: visibility, granular security and dynamic adaptation. Unlike north-south communications, east-west traffic is usually not subject to firewall inspection and is, for all practical purposes, invisible to the network security team. To be effective, microsegmentation requires visibility into all network traffic. While there are several ways to monitor traffic, the hypervisor touches every packet on the network and is therefore uniquely positioned to provide the necessary visibility. Granular security means network administrators can strengthen and pinpoint security by creating specific policies for highly sensitive workloads. The goal is to prevent lateral movement of threats with policies that precisely control traffic in and out of specific workloads, such as weekly payroll runs or updates to human resource databases. Dynamic adaptation ensures these protections remain in place as workloads move around in today's highly dynamic environments. In microsegmentation, security policies are expressed in terms of abstract concepts such as application tiers rather than network constructs such as IP addresses and port numbers. Changes to the application or infrastructure trigger automatic revisions to security policies in real time, requiring no human intervention.

This technique helps to apply rules to each VM rather than protecting the physical environment with a firewall. Microsegmentation is a security model, which reflects and supports the dynamic nature of data center operations that has never been possible before. The model goes beyond the idea of plugging gaps in perimeter security, or even trying to manipulate physical security within the data center to make it more effective. The micro-segmentation model is not about "building up" but "infusing into." Much like bioengineering plants to be more disease resistant, microsegmentation changes the DNA of data center security to be resistant to threats at an extremely granular level. The landscape of the modern data center is rapidly evolving. The migration from physical to virtualized workloads, the move towards software-defined data centers, the advent of a multi-cloud landscape, the proliferation of mobile devices accessing the corporate data center, and the adoption of new architectural and deployment models (e.g. micro-services and containers) are all driving a constant evolution.

2. Traditional models of security — Firewalls and IDPS

Firewalls are aligned to IT Security similarly to how anti-virus programs are for Personal Computers. Firewalls are software programs or hardware devices that inspects the information coming through our internet connection. They are our first line of defense because they are mainly built to avoid attackers and malicious programs attempting to gain access to our networks. In essence, consider firewalls as security guards. They stand at the door of the corporate networks, databases, applications and other important resources examining both inward and outward data traffic. The firewalls sole responsibility is to decide what should enter the door and what should be prohibited.

Important types of firewalls that organizations incubate with respect to their requirements are Network firewalls, Next-Generation firewalls, Database firewalls, Cloud firewalls, Web Application firewalls, Container firewalls and so on.

Intrusion detection is the process of keeping events occurring in a computer or a corporate network and then analyzing them for violation of security policies. Intrusion prevention is the process of carrying out intrusion detection and trying to avoid detected incidents. Intrusion detection and prevention systems (IDPS) primarily focus on detecting the possible incidents, recording information about them, trying to stop them and finally reporting it to security admin of the organization.

Types of prominent IDPS technologies which most organization incorporate are Host-based IDPS, Network-based IDPS, Network Behavior Analysis (NBA)-based IDPS and Wireless-based IDPS.

While traditional Firewalls and IDPS are intelligent, they are not enough to protect the modern data center. Here are some the main reasons:

1. These traditional security models mainly focus on network perimeter. Since they are perimeter-centric models, they are designed to work from client to the server. But these models were not designed to handle data traffic between servers.
2. It is evident that security administrators find it very difficult to update and maintain physical firewalls.
3. It is impossible to have physical devices everywhere at once. It is too complex and expensive to install firewalls in every nook and corner of the data center.

3. Major security attacks on Virtualized systems

3.1 Hypervisor vulnerabilities

Hypervisors are mainly designed to run many guest Virtual Machines (VMs) and applications concurrently in a single host. Thought the majority assume hypervisors are secured, they remain accessible to attacks. If attackers gain command over the hypervisor, the entire VMs and data can be accessed by the attackers.

3.1.1 Escape of VM

VMs are usually designed in such a way that they need to support well-built isolation between the hosts and the VMs. But the defects in operating systems functioning inside the VMs can help attackers launch malicious programs. When these malicious programs run, the VM smashes the

isolated boundaries and they will start interacting with the operating system by bypassing the VMM Layer. This opens the door to attackers to further launch attacks on the host machine.

3.1.2 VM Sprawl

VM Sprawl occurs when there are a large number of VMs in the environment without any proper maintenance or management. Because these VMs hold system resources like compute, storage and network during this period, these resources cannot be provisioned to other VMs and they are lost.

3.1.3 Single point of failure

It is evident that the current virtualized infrastructure is mainly based on hypervisor-based technology. Hypervisors completely control access of the VMs to physical resources and this plays a major role in the overall functioning of the system. Hence, Hypervisor failure due to software defects or over-utilized infrastructure leads to failure of the entire system.

3.1.4 Outside-VM attack

Attacks from the host OS and VMs are considered Outside-VM attacks. It is very difficult for customers to defeat such an attack. The malicious VM can easily access other VMs through shared resources like compute, storage and network. For instance, if a malicious VM determines the exact location of provisioned memory of other VMS, it can easily perform read or write operation to that location and alter other operations.

3.1.5 VM footprint

VM footprint is a process used to gain information such as Operating system, packages installed, and types of services being run on the target VMs. This primarily falls under the pre-attack phase. VM Footprint is carried out before the actual attack is performed.

4. Why Microsegmentation?

In section 2 and 3, we discussed the security threats and traditional models of VM security to gain an understanding of the importance of microsegmentation for virtualization security. Now, let us look how organizations can leverage tangible benefits of microsegmentation in the form of a reduced attack surface, improved breach containment, stronger compliance posture and streamlined policy management.

- **Reduced attack surface:** Microsegmentation provides visibility of the entire network environment without slowing development or innovation. Thus, developers can integrate security and policy definition early in the development cycle to ensure that neither application deployments nor updates create new attack vectors. This is particularly important in the fast-moving world of DevOps or the DevSecOps world.

- **Improved breach containment:** Microsegmentation enables security teams to monitor network traffic against predefined policies as well as shorten the time to respond to and remediate breaches.

- **Stronger regulatory compliance:** Using microsegmentation, policies can be created that can isolate systems subject to regulations from the rest of the infrastructure. Having granular control of communications over regulated systems reduces the risk of noncompliant use.

- **Streamlined policy management:** Microsegmentation architecture provides an opportunity to simplify management of firewall policies. This emerging best practice uses a single consolidated policy for subnet access control, threat detection and mitigation, rather than performing these functions in different parts of the network. This approach reduces the attack surface and strengthens the organization's security posture.

5. VMware NSX

Software Defined Data Center (SDDC) is the modern data center model that empowers administrators to deploy new applications in a fraction of seconds. This includes compute, storage, security and network provisioning. SDDC is easy to manage and is more effective for your business in this new digital world. The most significant step towards the dream of SDDC is VMware NSX, the network virtualization platform for SDDC. VMware NSX will make the network infrastructure of the organization more agile. The biggest benefit of VMware NSX is that it will enable the organization to inject security into the DNA of its data center with microsegmentation.

1. **Network security within the data center:** Flexible security policies tied to virtual network, VM, and OS type for more 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 they are removed when a VM is deprovisioned – no more stale firewall rules.

3. **Integration with leading networking and security infrastructure:** The NSX platform empowers an ecosystem of partners to integrate – adapting to continuously changing conditions in the data center to provide enhanced security. The best feature of NSX is that it runs on existing data center networking infrastructure.

NSX-based microsegmentation enables customers to increase data center agility and efficiency while maintaining an acceptable security posture that provides effective security controls within the modern data center and demonstrate how NSX goes beyond automation of legacy security paradigms in enabling security through microsegmentation.

6. Conclusion

Microsegmentation with NSX has paved the way for thousands of organizations to improve their security posture of SDDC by fundamentally changing how they approach security architecture. Virtualization, cloud, and software-defined services have contributed greatly to modernization of the data center, with the use of established IT models of resource provisioning and consumption. This modernization drives the need to evolve security solutions from static, legacy models to dynamic, policy-driven, granular, flexible models that can protect today's agile workloads with the necessary security controls. Microsegmentation enables a fundamental architectural shift, making an allow list/Zero Trust Model feasible within the modern dynamic data center. NSX microsegmentation provides the tools and capabilities needed to build a firm foundation, securing the modern data center.

7. References

https://www.gartner.com/en/documents/3907011/solution-comparison-for-microsegmentation-products

https://www.hillstonenet.com/blog/gartner-delivers-clarity-and-guidance-for-micro-segmentation-technology/

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutionbrief/partners/intel/vmware-micro-segmentation-builds-security-into-your-data-centers-white-paper.pdf

https://blogs.vmware.com/networkvirtualization/2016/06/micro-segmentation-defined-nsx-securing-anywhere.html/