WHITE PAPER

MICRO-SEGMENTATION: DON'T BE FOOLED BY THE IMITATION

vmware®

Table of Contents

Beware the Imitations 3

Modern Threats Require Modern Defenses 3

- Traditional Firewalls Are Not the Answer 4

Enter Micro-segmentation 4

Distinguishing True Micro-segmentation from Imitations 5

Network Virtualization: the Key to Micro-segmentation 6

- A Brief Overview of Network Virtualization 6
- Increasing Security with Micro-segmentation 6
- Establishing and Defining Trust Boundaries 6
- Ensuring Application Continuity 7
- Automation 7

Key Features and Benefits of Micro-segmentation 7

- Minimize Risk and Impact of Data Center Security Breaches 7
- Simplify Network Traffic Flows 8
- Enable Advanced Security Service Insertion, Chaining, and Traffic Steering . . 8
- Leverage Existing Infrastructure 8
- Reduce Capital Expenditures 9
- Lower Operating Expenses 9
- Securely Enable Business Agility 9

For True Data Center Security, Deploy Only True Micro-segmentation 9

Beware the Imitations

There's an old adage that states that imitation is the sincerest form of flattery. Taking this statement to its logical end, you might add the corollary: If you are the leader in something, imitators will eventually and inevitably follow.

Today, micro-segmentation is the leading security approach that others are attempting to imitate.

Although the concept of micro-segmentation is nothing new, only recently has actually achieving it become a reality, thanks to game-changing advances in network virtualization and security distributed to the hypervisor. But along with this innovative security strategy have come several imitations purporting to enable true micro-segmentation, but which, in fact, fall short across a number of different areas. It is the purpose of this paper to draw a distinction between these imitations and genuine micro-segmentation, to examine the key capabilities and features that true micro-segmentation must necessarily offer, and to discuss the benefits your organization can expect from deploying micro-segmentation throughout the data center. We'll also take a look at the current state of security across many modern enterprises, and why such perimeter-centric models are no longer adequate against today's sophisticated threats.

Modern Threats Require Modern Defenses

Despite a heightened focus on enterprise security and staggering increases in security investments, data center breaches continue to occur at an alarming rate, and with growing severity. In fact, if national news broadcasts are any indication, it would seem that every new security breach eclipses the previous one in terms of the volume and value of the data that was lost, and its overall damage to the business.

While recent, well-publicized attacks on major retailers, entertainment companies, and even government entities have varied in nature, they all nonetheless share a common denominator: Once the security perimeter was breached, the attacks were able to propagate laterally inside the data center with essentially no security controls in place to stop them.

How—and more importantly, why?

The answer to both those questions calls attention to one major weakness of modern data centers and highlights the flawed thinking behind their current security strategies—namely, a singular focus on securing the perimeter of the data center, with very little regard for security inside the data center. In a world where cyber threats are composed of coordinated attacks that often include months of reconnaissance, vulnerability exploits, and "sleeper" malware agents that can lie dormant until activated by remote control, this perimeter-centric thinking and approach to network security is both profoundly misguided and seriously outdated. To defend against such sophisticated attacks, today's enterprises need an equally sophisticated and modern approach to data center security—one that emphasizes protecting the inside of the data center.

Traditional Firewalls Are Not the Answer

To date, the firewall has been the primary defender of the data center, but only against attacks originating from the outside—which is to say, firewalls have almost only protected traffic moving from client to server (i.e., north-south). But what happens once a threat has breached the perimeter and made its way inside the data center? In this instance, firewalls are all but ineffective against threats now moving from server to server (east-west)—which immediately raises the question: How do you protect internal data center resources from these laterally moving attacks?

One answer is through a security approach called segmentation. At its most basic level, segmentation occurs when two or more networks—such as an internal network (the data center) and an external network (the Internet)—are separated by a perimeter firewall. This firewall then acts as a gatekeeper regulating traffic between the different segmented networks.

With this approach, however, the network segments tend to be too large to provide any sort of consistent or reliable protection. To maximize effectiveness, segmentation (and hence firewalling) would ideally need to scale to the level of the individual workload, a strategy better known as micro-segmentation. The problem here is that applying security policies at the individual workload, across thousands of workloads inside the data center, is both massively cost-prohibitive and operationally infeasible—you simply cannot purchase and deploy a virtual or appliance-based firewall for every workload, much less manage those thousands of firewalls. But even if cost and management were no obstacle, the focus of firewalls is still on controlling north-south traffic in and out of the data center, rather than on the east-west traffic inside the data center that is typically the target of most modern attacks. So now we're right back to where we started—or are we?

Enter Micro-segmentation

As just mentioned, micro-segmentation essentially scales segmentation to the level of the individual workload, delivering firewalling capabilities at every virtual machine (VM). It enables you to use fine-grained policies and network controls to establish security inside the data center and thus prevent the lateral spread of threats in the event they overcome perimeter defenses. How does micro-segmentation accomplish this? First and foremost, you need to virtualize the network—this is a prerequisite for micro-segmentation. Once the network is virtualized, all security functions (and indeed, all networking functions) are then embedded into a hypervisor layer—a "network hypervisor," if you will—that provides firewalling all the way down to the individual virtual network interface, creating a granular level of security that's simply unattainable with legacy physical or virtual appliances. Furthermore, with network virtualization, networks are isolated by default, which means that workloads on two unrelated networks have no possibility of communicating with one another unless you specifically decide to connect them. Since there is no communication between unrelated workloads, malicious code is unable to propagate from one server to the next, thus isolating the attack. Similarly, since virtual networks are decoupled from the underlying physical network, your hardware infrastructure is also protected from any attacks launched from workloads within your virtual networks. No physical subnets, VLANs, ACLs, or firewall rules are required to achieve this level of isolation—network virtualization enables this by default.

Distinguishing True Micro-segmentation from Imitations

At first glance, from a strictly high-level perspective, many products purporting to enable micro-segmentation might look quite similar to the genuine article. It's only when you look deeper into the finer details that some very stark differences in their respective capabilities begin to emerge. For a solution to enable true micro-segmentation, it will need to deliver the following capabilities:

- **Provide stateful inspection of east-west traffic**
  Stateful inspection is a firewall technology that tracks the operating state and characteristics of network connections traversing it, monitoring the state of active connections and using this information to determine which network packets to allow through. In contrast, stateless inspection provides only simple packet filtering, evaluating packet contents statically and neglecting to keep track of the state of network connections. By far, stateful inspection is the better, more easily managed, and vastly more secure firewall technology.
- **Protect VM-to-VM traffic in the same group**
  When it comes to VM-to-VM traffic, many would-be solutions simply provide for "block all" or "allow all" communication between VMs in the same group. True micro-segmentation lets you establish policies at the granular level, including VM-to-VM traffic in the same group.
- **Same-host redirection to VM-based third-party services**
  Frequently, third-party services need to be applied to virtual network traffic, a requirement most efficiently accomplished by steering or redirecting that traffic to third-party services residing on the same host—a capability found in true micro-segmentation. By contrast, an inauthentic solution will force this same east-west traffic through firewalls, a practice known as hairpinning that creates choke points, unnecessarily backhauls server traffic, and contributes to sprawling firewall rulesets and complexity. Similarly, an inauthentic solution might also redirect traffic through a third-party security service without being selective about the traffic it's steering, making that third-party security service a potential choke point as well.
- **Scalable to complex application policies**
  Many solutions claiming to enable micro-segmentation are bound to hardware—that is, policies are centrally enforced in hardware—which means that their ability to scale is tied directly to the limitations of the associated hardware. True micro-segmentation offers near-limitless scalability to complex applications.
- **Integration with cloud management platforms**
  Genuine micro-segmentation offers seamless integration with cloud management platforms (CMPs) to enable the provisioning of virtual networks. At best, imitating solutions will offer disjointed and inconsistent integration with CMPs.

Network Virtualization: the Key to Micro-segmentation

A Brief Overview of Network Virtualization

Virtualization, as a general category, is the ability to simulate an otherwise hardware-based platform in software, such as a server, storage device, or network resource. Similarly, network virtualization is the ability to programmatically create, provision, and manage networks entirely in software, using the underlying physical network as a simple packet-forwarding backplane. Here, network and security services in software are distributed to hypervisors and "attached" to individual virtual machines (VMs) in accordance with networking and security policies defined for each connected application. The advantage of this approach is that when a VM is moved to another host, its networking and security services move with it. Likewise, when new VMs are created to scale an application, the necessary policies are dynamically applied to those VMs as well.

Increasing Security with Micro-segmentation

Network virtualization provides a number of key capabilities that enable micro-segmentation: automated provisioning, automated move/add/change for workloads, distributed enforcement at every virtual interface, and in-kernel, scale-out firewalling performance. Network virtualization's ability to create entire networks in software has exciting and profound implications for how security can be applied. First, as we've already described, virtual networks are completely isolated from one another, which means that there's no risk of unrelated data streams communicating with each other (thus minimizing threats moving along east-west traffic). Second, by embedding security functions into the hypervisor, firewalling capability is provided at the kernel and network interface level—something you simply cannot accomplish with physical hardware. Collectively, these capabilities represent the very definition of the term "micro-segmentation"—the use of fine-grained policies and network controls to enable security inside the data center, thus preventing the lateral spread of threats should they overcome perimeter defenses.

Establishing and Defining Trust Boundaries

Micro-segmentation, enabled by network virtualization, allows you to adopt an effective security posture by intelligently grouping workloads based on their attributes and then applying the appropriate security policies. Security policy rules can be created in various ways with network virtualization, including:

- **Network-based policies** that group elements based on network constructs (i.e., Layer 2 or Layer 3 elements), such as media access controls or IP addresses. This approach is better utilized with static environments, as it generally cannot keep pace with data center environments with high workload mobility.
- **Infrastructure-based policies** where grouping is based on the type of data center infrastructure element, such as clusters, logical switches, distributed port groups, and the like. Although well suited for more dynamic environments, an infrastructure-based policy approach is not feasible if there are no physical or logical boundaries in the data center.

- **Application-based policies** group data center elements based on a wide variety of customizable mechanisms, such as the application type, application environment and application security posture. The advantage of this approach is that the security posture of the application is not tied to network constructs or the data center infrastructure—security policies can move with the application irrespective of network or infrastructure boundaries, and policy templates can be created and reused across similar application types and workload instances. Needless to say, an application-based policy approach is very well suited for dynamic data center environments.

Ensuring Application Continuity

Keeping applications up and running is a top mandate for today's IT organizations. Network virtualization can help you maintain the availability of applications and services by serving as a complement to your existing disaster recovery (DR) solutions and through multi data center pooling. For DR, network virtualization enables you to replicate the entire network and its security environment, then store this copy at a recovery site, where it sits in standby mode ready for push-button activation should a disaster occur. With multi data center pooling, network virtualization lets you pool compute resources that are in different physical locations, then treat these disparate resources as a unified set. The advantage here is that applications can be deployed in any location, yet seamlessly connect to the resources located across the sites.

Automation

Automation allows for the quick, secure, and automatic deployment of applications and services—whenever and wherever they're needed—through the use of a self-service portal and catalog items. Capabilities like service blueprints and network profiles enable the fast, consistent, and secure provisioning of resources anytime and anywhere they're required. Apps and services can be deployed across organizational and geographic boundaries with ease, delivering business value in minutes rather than days, weeks, or months.

Key Features and Benefits of Micro-segmentation

Minimize Risk and Impact of Data Center Security Breaches

If a threat infiltrates the data center, micro-segmentation contains and blocks its lateral movement to other servers, which dramatically reduces the attack surface and risk to the business. Micro-segmentation isolates each workload with its own security policy, preventing attackers from exploiting other systems and stealing valuable data. By reducing the attack surface, micro-segmentation helps organizations avoid or minimize the cost and impact when a data breach occurs.

Simplify Network Traffic Flows

The volume of east-west/server-to-server traffic generated by modern applications inside the data center continues to grow exponentially, which consumes network bandwidth, increases latency, adds complexity, and increases oversubscription on the data center network core. Network virtualization and micro-segmentation enable direct east-west communication between server workloads through a virtual switch or aggregation fabric which:

- Significantly reduces east-west traffic hops for better application performance.
- Eliminates inefficient hairpinning (i.e., forcing east-west traffic through physical firewalls, which severely degrades performance).
- Enables workload mobility by allowing individual workloads to be deployed anywhere in the data center with their own security policies, instead of being tied to the physical network topology.

Enable Advanced Security Service Insertion, Chaining, and Traffic Steering

Environments that require advanced, application-level network security capabilities can leverage micro-segmentation to distribute, enable, and enforce advanced network security services in a virtualized network context. Micro-segmentation also offers the ability to build unit-level policies for individual VM workloads, which leverage service insertion, chaining, and steering to drive service execution in the logical services pipeline based on the result of other services. This capability makes it possible to coordinate and correlate otherwise completely unrelated network security services from multiple vendors.

Leverage Existing Infrastructure

Micro-segmentation is not an all-or-nothing proposition. Because virtual networks require no configuration changes to the underlying physical network, they can transparently coexist on the physical network—with as much or as little micro-segmentation of existing application workloads as needed. This gives IT departments the flexibility to virtualize and segment portions of the network simply by adding hypervisor nodes to the virtualization platform. This means that organizations can deploy micro-segmentation in their data centers at a pace that suits their unique business needs—whether in a proof-of-concept pilot project, a high-value multitiered application, or a full-scale data center build-out. Additionally, micro-segmentation enables organizations to leverage their existing physical network and security equipment and, in many cases, significantly extend the useful life of their existing infrastructure.

Reduce Capital Expenditures

Deploying additional physical firewalls to control increasing volumes of east-west traffic inside the data center is cost prohibitive for most enterprises. Additionally, the sheer number of devices needed and the effort required to set up and manage a complex matrix of firewall rules make such an approach operationally infeasible. Micro-segmentation enables complete control of individual workloads in the data center without purchasing additional physical firewalls for each workload, resulting in significant up front savings in enterprise data centers.

Lower Operating Expenses

Micro-segmentation dramatically reduces the manual effort and cycle time for security tasks, including provisioning, change/adaptation, scaling, and troubleshooting/remediation. Typically, it reduces effort from hours to minutes and cycle times from days to minutes. If you consider all the manual tasks required to provision and manage security for a physical network—across development, testing, staging, and production environments—and the fact that micro-segmentation automates these tasks, the opportunities for reducing operational costs are substantial and add up quickly.

Securely Enable Business Agility

Historically, businesses have been forced to choose between speed and security, often times resulting in a contentious relationship between IT security teams and business units. Network virtualization makes micro-segmentation a reality, enabling businesses to rapidly—and securely—innovate to achieve a competitive advantage while maintaining ubiquitous and persistent security in the data center.

For True Data Center Security, Deploy Only True Micro-segmentation

The increasing frequency and severity of cyber attacks is causing many organizations to re-examine and rethink their current approach to data center security. Many are discovering that their traditional perimeter-centric strategies are no longer effective against today's highly sophisticated attacks, and so are turning to an innovative security strategy called micro-segmentation. While there are multiple solutions in the market claiming to enable micro-segmentation, very few of them are true, authentic solutions that can deliver the full range of security capabilities required to protect internal data center resources. Accordingly, enterprises looking to virtualize their networks and implement micro-segmentation need to verify and confirm that their chosen solution delivers all the capabilities needed to secure the data center, such as stateful inspection of east-west traffic, CMP integration, protection of VM-to-VM traffic, and scalability to complex application policies, among others.

To learn more about the features, capabilities, and benefits of true micro-segmentation enabled by the VMware NSX® network virtualization platform, visit vmware.com/products/nsx.

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