MAKING MICRO-SEGMENTATION A REALITY

Building and Operating a VMware NSX and Palo Alto Networks Firewalls Based SDDC Using vRealize Network Insight

AT A GLANCE

Capacity Planning for East-West security ensures accurate and predictable sizing and placement of virtual firewalls based on VM and host level traffic analysis across applications and application tiers

Secure 100% of your applications by accelerating micro- segmentation deployment by modeling out, at a granular level, the security groups and firewall rules for existing and new applications. See a map of who is talking to whom and what's unprotected

Use vRealize Network Insight Assured Security Model to eliminate operational and audit risks associated with the new dynamic, distributed security model based on virtual firewalls

VMware and Palo Alto Networks Partnership

As organizations adopt a software-defined security strategy and virtualize their firewalls with Palo Alto Networks VM-Series appliances, proper security capacity planning, and operational visibility across virtual and physical layers is paramount. Security teams need to understand capacity needs of East-West firewalls, have access to comprehensive network flow analytics, be able to model out, create and deploy security groups and relevant firewall rules to protect their applications and associated sensitive data in East-West direction, 80% of which is unprotected today.

Operations teams need to have complete visibility across virtual and physical layers to ensure firewall rules are being applied consistently. Additionally, these teams have overall responsibility to ensure security group membership fidelity, as well as meeting audit and compliance needs.

Capacity Planning for Virtual Firewalls

With broad virtualization, the data center has become truly dynamic. Application components could migrate across hosts without much notice. Under such circumstances, how does IT ensure East-West firewall capacity to serve the underlying application needs? vRealize Network Insight sheds light on firewall sizing and placement using actual traffic patterns. Firewall requirements and needs can be segregated by obtaining peak and average flow statistics per host for East-West traffic, segregated into intra and inter application tiers, North-South, management, and storage traffic. Based on existing flows and Palo Alto Network Virtual Firewall application, users are better equipped, with the vRealize Network Insight platform, to be able to predict capacity shortfalls and eliminate bottlenecks. Advanced use cases include usage monitoring and dynamic workload placement analytics.

	Total		E- W		N - S		Inter Segment		Intra Segment	
Host	Peak (Kbps)	Average (Kbps)	Peak (Kbps)	Average (Kbps)	Peak (Kbps)	Average (Kbps)	Peak (Kbps)	Average (Kbps)	Peak (Kbps)	Average (Kbps)
esx049	5136	927	5136	911	42	16	3758	392	1978	518
esx045	4690	891	4690	879	37	12	3079	326	1871	553
esx035	4166	865	4147	852	35	13	2481	180	2214	672
esx048	4028	697	4028	686	36	12	2765	267	1488	419
esx043	3667	696	3649	686	28	10	2165	152	1853	534
esx044	3587	594	3587	590	18	4	2472	171	1569	419

Figure 1: Data Center Traffic Profile for Firewall Capacity Planning

KEY BENEFITS

Enterprises, in their journey towards a software-defined data center, are embracing newer software-defined security models based on network virtualization platforms and virtual firewall offerings from vendors such as VMware (NSX) and Palo Alto Networks (VM-Series). vRealize Network Insight accelerates software-defined data center adoption by providing a radically simple and automated approach to micro- segmentation, virtual firewall capacity planning, and ongoing security operations. vRealize Network Insight provides a communication map of the data center using in-depth flow visibility and analytics. vRealize Network Insight also suggests security groups and firewall rules based on VM configuration and run time flow data. On a continuous basis, vRealize Network Insight brings visibility into the effective firewall rules and security group memberships of workloads and virtual machines. vRealize Network Insight makes micro-segmentation simple, automated and predictable.

Implementing Software-Defined Security

Secure 100% of your applications using micro-segmentation

The vRealize Network Insight platform provides comprehensive network flow assessment and East-West analytics to model out security groups and firewall rules, thus significantly easing out the path to micro-segmentation. This analysis helps organizations to understand what's unprotected, group VMs into meaningful security groups and model the right set of firewall rules to obtain a Zero Trust Security Model, thus ensuring maximum application security without compromising application connectivity and availability. vRealize Network Insight fully supports VMware NSX distributed firewall as well as Palo Alto Networks VM-Series Virtual Firewalls.

Designed for agent-less implementation, the vRealize Network Insight platform, delivered as virtual appliance leverages IPFIX information from sources such as VMware vSphere Distributed Virtual Switches to provide micro-segmentation models. Network and security teams can leverage vRealize Network Insight to effectively micro-segment their network.

Using vRealize Network Insight for Micro-segmentation

The vRealize Network Insight platform is used by IT organizations to (a) understand and quantify the benefits of micro-segmentation, (b) model out the capacity requirements, security grouping and firewall rules, and (c) implement security groups and firewall rules inside VMware NSX and Palo Alto Networks VM-Series Virtual Firewalls.

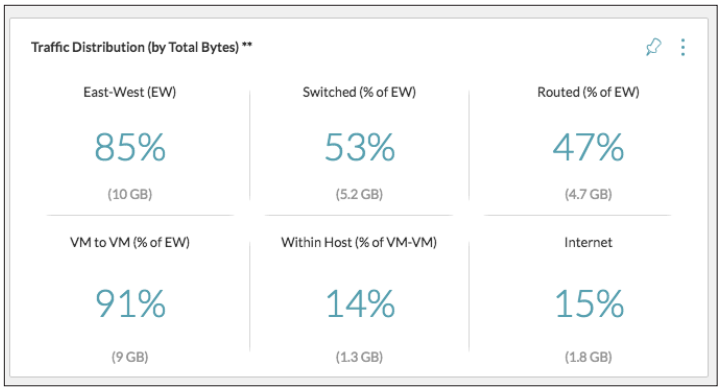

Figure 2: Data Center Security Coverage

Often there is not a good understanding of how various elements in the data center communicate in the East-West direction and what part of such communication is unprotected. The vRealize Network Insight platform generates an instant report of the Data Center Security Coverage and highlights the amount of traffic that is flowing in an unsecured or un-optimized manner.

vRealize Network Insight breaks down the traffic distribution into East-West, North- South, Internet, VM to VM, VM to Physical, Hair-pinned and overall Unprotected. Users can thus get a clear assessment of the benefits of deploying micro-segmentation to secure and optimize the unprotected part of their data center.

Model Out the Security Groups and Firewall Rules

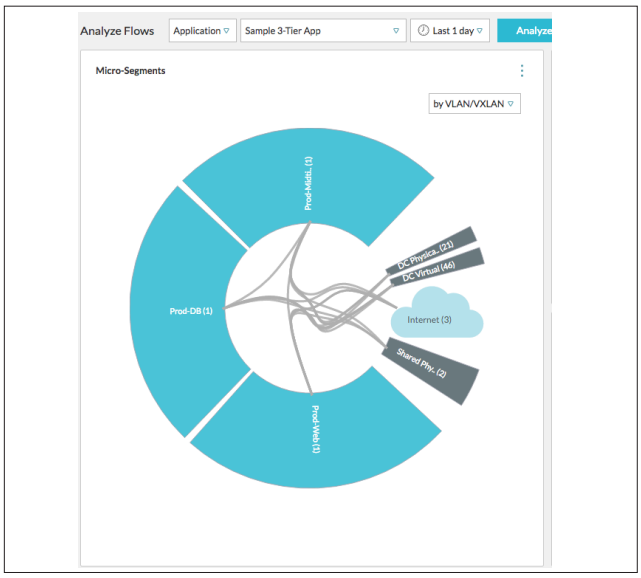

Figure 3: Micro-Segmented View of Data Center

One of the key challenges with micro-segmentation is where to start and what security groups to create and what firewall rules to put in place. Organizations need to ensure that a zero trust model is properly implemented without compromising application availability. The security planner organizes virtual and physical machines into logical groups based on compute and network characteristics and provides a blueprint to put fine-grained security controls (security groups and firewall rules) in place. Using the analysis, modeling and visualization capabilities provided by vRealize Network Insight, IT can easily design and implement security groups and firewall rules.

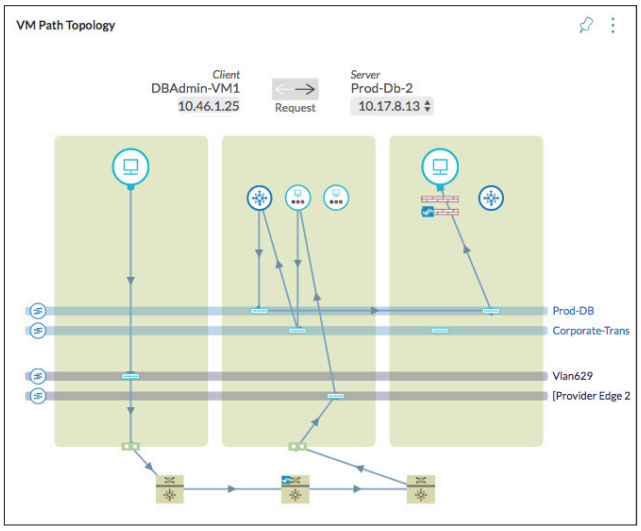

Figure 4: Operating A Virtual and Physical Firewall Based Environment

Operating a Software-Defined Security Environment

In a micro-segmented environment, it could be challenging to keep track of the applicable firewall rules for different entities such as virtual machines and security groups. The vRealize Network Insight platform calculates the “effective” firewall rules applicable for and between any entities in the data center. vRealize Network Insight provides end to end path visibility covering overlay and underlay as well as virtual and physical firewalls.

Entities covered in this release of the solution include—virtual machines, security groups, address groups, firewall rules, vSys, zones, router interfaces, and VRF.

The vRealize Network Insight platform continuously monitors the security state and memberships, tracking any changes on a historical time-line. The platform provides comprehensive visibility into security group configurations such as child groups, parent groups, virtual machines in a group, traffic flow between groups, and direct and indirect firewall rules. The platform ensures health and consistency across Palo Alto Networks Panorama and VMware NSX.

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