

Micro-segmentation and distributed firewall: Implementing to Secure virtualized network in Software Defined Data center

Submitted To

Yogesh G

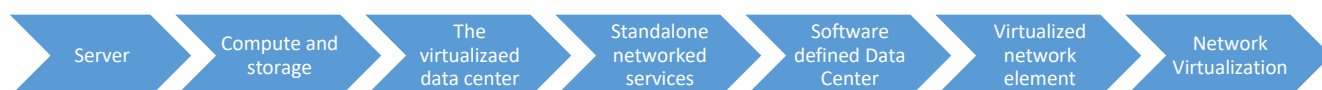
Submitted by

Praful Tamrakar

Introduction

Enterprises and public sectors in IT organizations are trying to embrace SDDC (Software Defined Data Centre) which consist of virtualize compute, network, and storage. An SDDC approach applies the principles of abstraction to deliver an entire data centre 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.

Network virtualization technology truly decouples network resources from underlying hardware. Virtualization principles are applied to physical network infrastructure, abstracting network services to create a flexible pool of transport capacity that can be allocated, utilized and repurposed on demand. Network virtualization provides a complete set of logical networking elements and services including logical switching, routing, firewalling, load balancing, VPN, Quality of Service , and monitoring. This transformative approach to networking unleashes the full potential of the software defined data centre – enabling data centre managers to achieve orders of magnitude better agility, economics, and choice.



Challenges for Automation of IT infrastructure and services for application testing and quick deployment and virtual network deployment for multiple tenants, providing security for dynamic and distributed network within and outside datacentre, automating security workflows, Enabling faster recovery and reduce downtime ,achieving high availability during disaster can be some of the challenged in virtualized network infrastructure .

Distributed Firewalls and micro-segmentation can be solution for meeting those challenges in wide virtual networks that exist on Software Defined Datacentre.

Distributed firewall (DFW) is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on Data Center objects like clusters and virtual machine names; network constructs

like IP or IPSets, VLAN , portgroups, VXLAN (logical switches), security groups, as well as user group identity from Active Directory.

Micro-segmentation enables organizations to logically divide the datacenter into distinct security segments down to the individual workload level , and then define security controls and deliver services for each unique segment. This restricts an attacker's ability to move laterally in the data center, even the perimeter has been breached – much like safe deposit boxes in a bank vault protect the valuables of individual bank customers , even if the safe has been cracked.

Abstract

we will explore how the distributed firewall helps protect a 3-tier application. We will also demonstrate the firewall rule creation process based on security groups rather than IP address based rules. This module is based on four guest VMs making up a common 3-tier application. The web tier has two web servers. The web tier communicates to a VM that is running an application software, acting as the application tier. The app tier VM in turn communicates to a VM is running MySQL in the database tier. Enforcement of access rules between the tiers is provided by NSX DFW Firewall. The outcome will be secure access to the web application tier and database tiers when VM from one tier is trying to access another tier.

Then we will explore how the Distributed Firewall (DFW) functionality in NSX allows customers to collapse traditional multi-tier network architectures into single, flat networks while maintaining application isolation at the same time. This is essential to getting away from a network-centric approach to security and moving to a workload centric approach. You will be using two different applications, (Finance and HR) that have been placed on the same logical switch and subnet.

You will then configure and testing communication between the HR and Finance application VMs on the same network prior to isolation ,creating logical groups of VMs using Security Groups ,creating Distributed Firewall rules to protect communication between the

applications ,outcome will be each application can still function correctly and that communication is blocked between the HR and Finance application VMs

Finally ,we will create firewall rules using the NSX Identity Based Firewall feature. This feature uses a connection to Active Directory from the NSX manager. The NSX manager scans the event log of the AD Server to determine log on credentials and events. Users logging on to VMs can have their VMs instantly assigned to Security Groups based on their AD groups. The Security Groups combined with firewall rules allow us to control access within our environment. There are two different Active Directory groups and two different users. The first user, a network administrator who should be able to get to any application in the environment and a Engineering administrator who should only have access to a specific Engineering web based application.

Project Category

Virtual networks or sometime referred as software defined networking is one of the main component of the software defined data centre. In virtual networks we are virtualizing the network so, this project falls under the category of Virtualization. Along with the virtualization it covers the part of datacentres tier networking and security.

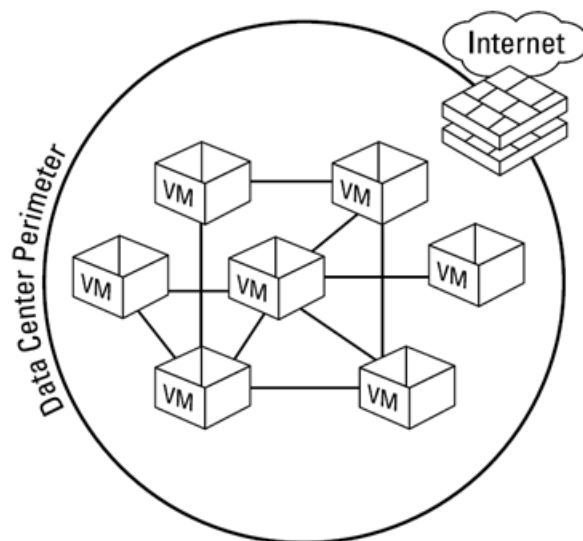
As I am pursuing MCA with specialization on Storage and Cloud Technology, my project matches with the curriculum and the syllabus of the subjects Advance virtualization and Fundamentals of Data Center. Considering the projects we have already been familiar with how to configure the virtual machine, clusters, ESXi host using VMware vSphere vCenter and VMware vSphere Web client.

Technical specification

Minimum Require	Server Side
Hardware Requirements	<ul style="list-style-type: none"> • Memory NSX Manager: 12 GB(with vCenter :10 GB) NSX Edge : 1 GB NSX Data Security: 512 MB EXSI Host : 4 GB per host • Disk Space NSX Manager: 60 GB (with vCenter) NSX Edge :512 MB NSX Data Security: 6GB per ESX host ESXI Host : 8GB per host • vCPU(To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs. NSX Manager: 4(with vCenter :4) NSX Edge : 1 NSX Data Security: 1 ESXI Host: 2
Software Requirements	<ul style="list-style-type: none"> • OS: Windows Server 2008 R2 or higher • VMware vSphere Web Client 6.0 • VMware vCenter 6.0 u2 or higher • VMware NSX 6.2 • VMware vSphere ESXi 6.5 • Web Browser : latest Google Chrome/Microsoft Edge / Mozilla Firefox (64 bit only)

Existing and traditional System

Traditional datacenter security (prior to infrastructure virtualization) involved building a very high performance hard-shell around the perimeter of the datacentre (firewalls, DDoS mitigation), and then embedding some advanced threat (IPS) in the datacentre. Although datacentres have been multi-tenant for a long time, the infrastructure wasn't shared the way it is in a SDDC, so internal segmentation was typically handled by VLANs. Occasionally hardware firewalls would be deployed inside the perimeter to provide a more secure segmentation, or when dedicated hosting or colocation customers ordered additional layers of security for their own services, but there was essentially trust, because the traffic itself was almost entirely moving north-south (in and out of the datacentre), and passing through security layers as it travelled.



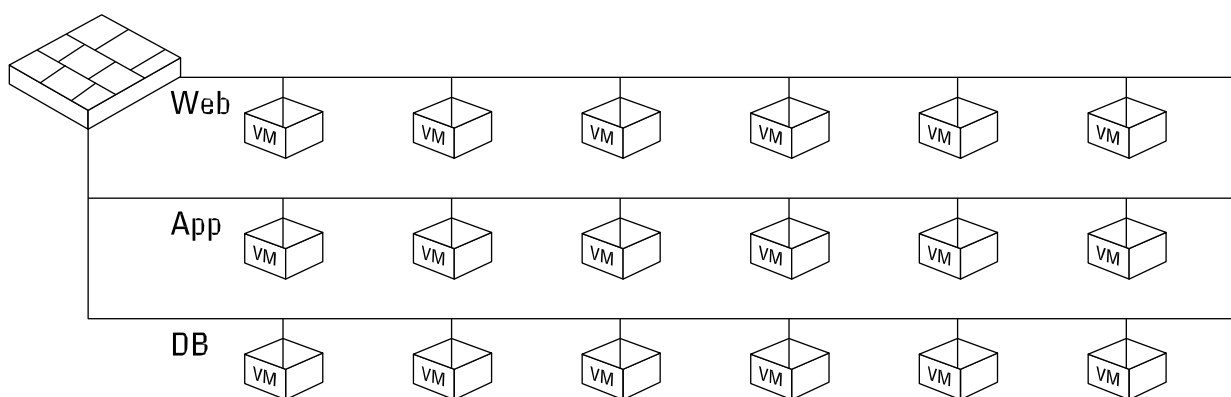
Perimeter-based security is insufficient in a data center where security is needed everywhere.

Although segmentation does exist in data centers today, the network segments are much too large to be effective and are typically created to restrict north-south traffic between the Internet and the data center or between client workstations and the data center. For example, a network may be segmented into multiple trust levels using additional firewalls to create a DMZ or separate department networks (such as finance, human resources, and R&D). To be completely effective, segmentation (and firewalling) needs to be possible down

to the level of the individual workload. But a typical data center may have thousands of workloads, each with unique security conditions. And again, the primary focus is on controlling north–south traffic in and out of the data center, rather than the east–west traffic within the data center upon which modern attacks are predicated.

Problem with VLANs

Many organizations logically partition their data center networks into different security segments, which then need to be translated to networking constructs, such as subnets and virtual LANs (VLANs). These techniques provide only rudimentary access control and result in security constructs that are too rigid and too complex, because security policies are largely defined by where a workload is physically deployed in the network topology. Segmenting the data center with such large zones creates a significant attack surface and enables threats to move throughout large portions of the data center unrestricted, once an attacker has overcome the data center's perimeter defences. These segmentation techniques also result in significant delays when deploying new workloads or changing existing workloads, because they must be manually configured to reflect a rigid and static network topology.



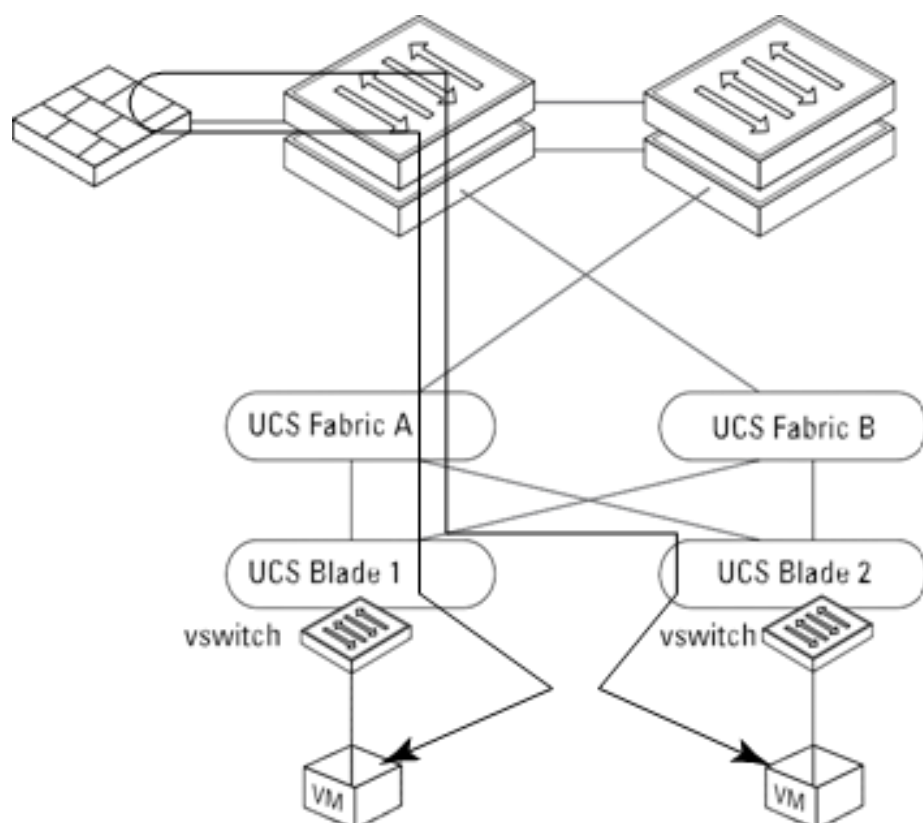
Hairpinning east-west server traffic

In addition to inadequate logical segmentation, another unfortunate consequence of traditional data center design that adds complexity and degrades network performance is hairpinning east-west server traffic — communications between servers that would not otherwise traverse a firewall boundary — through a firewall

Hairpinning is incredibly inefficient and greatly increases complexity in the data center by

Creating unnecessary performance choke points in the network and potential points of failure. Backhauling as much as 60 percent of all network traffic across firewalls, adding congestion and latency on the network

Contributing to firewall rule sprawl and performance bottlenecks as security administrators are increasingly reluctant to modify or remove complex rulesets when workloads are decommissioned, fearful of causing an outage or security breach



Proposed system

My Purposed system uses VMware NSX(Network Virtualization and Security) . VMware NSX provides Virtualized network elements such as DFW (Distributed Firewall) to meet all the disadvantages of simple segmentation as mentioned in existing system. DFW with micro-segmentation provides significant benefits such as Automation of network security workflow with the help of policy based segmentation, isolation of networks providing firewalls for tons of server with single logical firewall, provides us the power to quickly build DMZ anywhere inside the datacentre infrastructure.

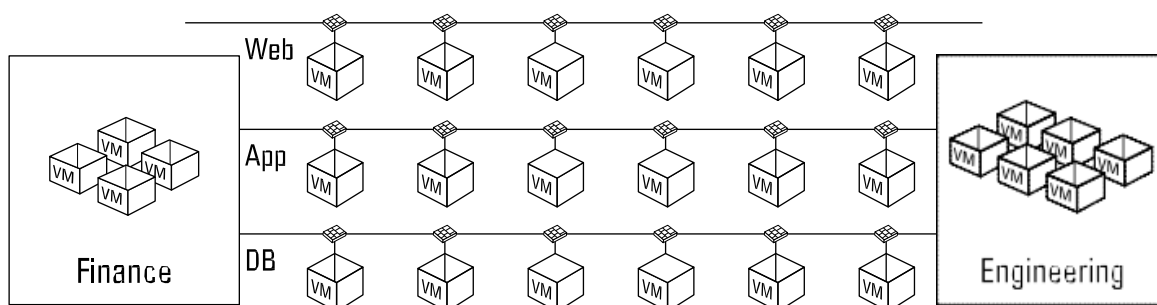
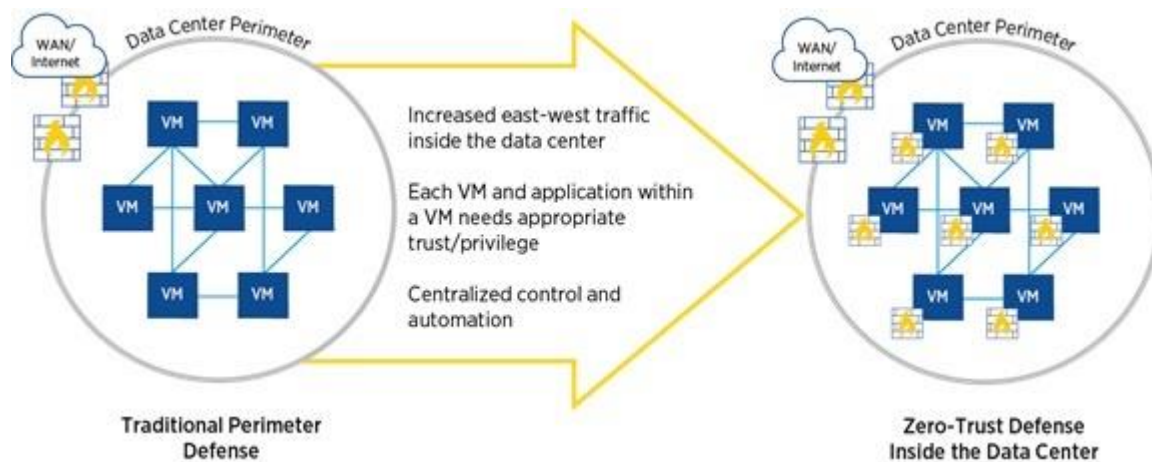
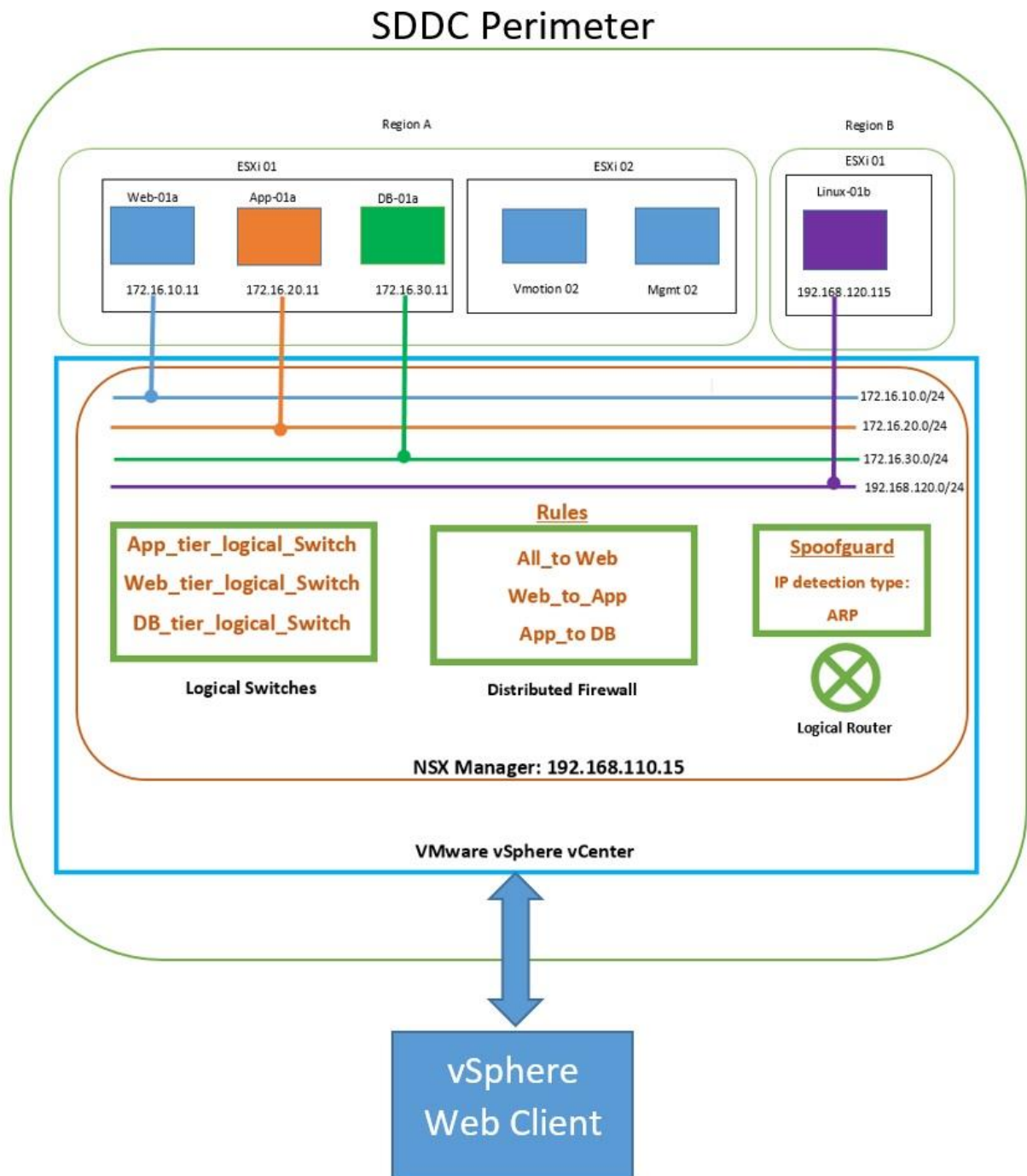
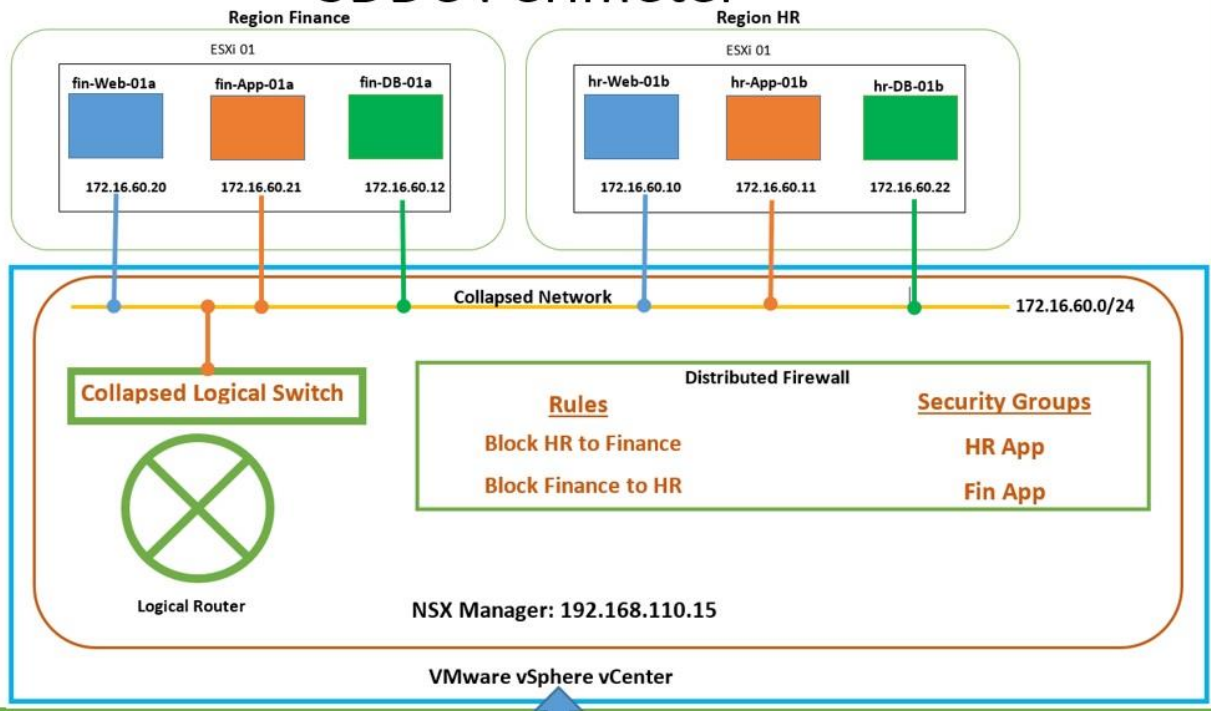


Fig : VLAN AND Multi-tier micro-segmentation with DFW

System Architecture



SDDC Perimeter



Vsphere Web
Client

Innovations and Usefulness/ benefits

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 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 savings in enterprise data centers

Environment & Capacity	
Number of VMs	2,500
VMs per CPU	5
CPUs per server	2
Servers	250
% of VMs requiring FW controls	40%
Gbps - Average Application throughput per host	7
Gbps - Required Firewall throughput in Gbps for all VMs	1,750
Gbps - Effective Required Firewall Throughput	700
Firewalls (20 Gbps each x2 for HA)	70
Cost for Hardware	
List cost of each 20 Gbps FW	\$135,000
Total Hardware Firewall Cost (But Operationally Infeasible)	\$9,450,000
Cost for NSX	
NSX List Cost per CPU	\$5,995
NSX Total Cost	\$2,997,500
CapEx Savings with NSX	\$6,452,500 68%

Lower Operating Expenses

Micro-segmentation dramatically reduces the manual effort and cycle time for security tasks, including provisioning, change/adaptation, scaling, and troubleshooting/remediation.

Generally, micro-segmentation reduces the effort from hours to minutes and the 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, you begin to see all the opportunities for reducing operational costs.

As the analysis in Figure shows, micro-segmentation dramatically speeds the initial provisioning of security services into production. With traditional hardware, the associated cycle time to provision security services for a new application forces enterprises to wait 23 days. Network virtualization reduces that to minutes — nearly a 100 percent reduction and a massive time-to-market win. Likewise, provisioning security services for a new application takes 14 person hours or close to two days of person effort. Micro-segmentation reduces that to less than 2 person hours — a substantial 87 percent reduction.

	Task Effort (Hours)		Cycle Time (Days)	
	Manual	Automated - NSX	Manual	Automated - NSX
Request & Review Network & Security Resources	1.00	0.00	1	0
Define Network & Security Environment	4.50	1.00	3	0
Determine Changes Required (Capacity Availability)	4.50	0.00	3	0
Review & Approval Process (Change Approval Board)	0.50	0.50	5	0
Change Order Scheduling	0.50	0.00	5	0
Configure the Network (VLAN, Routing)	1.00	0.00	2	0
Configure the Security (Firewall)	1.00	0.00	2	0
Configure the Load Balancer	1.00	0.00	2	0
Provision the Environment	0.30	0.30	0	0
Total	14.30	1.80	23	0
OpEx Savings with NSX	12.50 Hours		23 Days	
	87%		100%	

Securely Enable Business Agility

Network virtualization makes micro-segmentation in the software-defined data center a reality and enables businesses to rapidly — and securely — innovate to achieve competitive advantage, while maintaining ubiquitous and persistent security in the data center. Businesses everywhere are enjoying the many security and performance benefits of micro-segmentation in the data center, and will continue to discover innovative uses and applications for this truly disruptive technology.

Project Planning and Scheduling

Presentation 1: Explanation about Synopsis

Presentation 2: Implementation of the project.

Bibliography

- <https://www.vmware.com/radius/future-networking-5-key-themes/>
- <https://www.vmware.com/in/solutions/software-defined-datacenter/in-depth.html>
- https://blogs.vmware.com/networkvirtualization/2013/07/what-is-a-distributed-firewall.html#.WJ_WB4VOJu0
- <https://featurewalkthrough.vmware.com/#!/nsx/nsx-partner-integration-1/micro-segmentation-with-distributed-firewall>
- https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf?src=vmw_so_vex_cyola_760
- <https://blogs.vmware.com/networkvirtualization/2016/06/micro-segmentation-defined-nsx-securing-anywhere.html#.WKbX74VOljZ>
- http://docs.hol.vmware.com/HOL-2017/hol-1703-use-2_pdf_en.pdf, Lab Overview - HOL-1703-USE-2 - VMware NSX: Distributed Firewall with Micro-Segmentation
- <https://pubs.vmware.com/NSX-6/index.jsp?topic=%2Fcom.vmware.nsx.install.doc%2FGUID-311BBB9F-32CC-4633-9F91-26A39296381A.html>
- <http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-network-virtualization-design-guide.pdf>

Books:

- Micro-segmentation using NSX Distributed Firewall: Getting Started, VMware NSX for vSphere, release 6.0.x
- Micro-segmentation For Dummies®, VMware Special Edition, by ,Lawrence Miller , and Joshua Soto