Security for Hyper-Converged Solutions:

Dell EMC VxRAIL Appliances - VMware vSAN Readynodes

with VMware NSX-V

NSBU
UPDATED 08/24/2017

VERSION 1.0

Revision History / Notes

Version	Date	Updates/Notes
1.0	08-24-2017	Initial Public Release

Table of Contents

Executive Summary

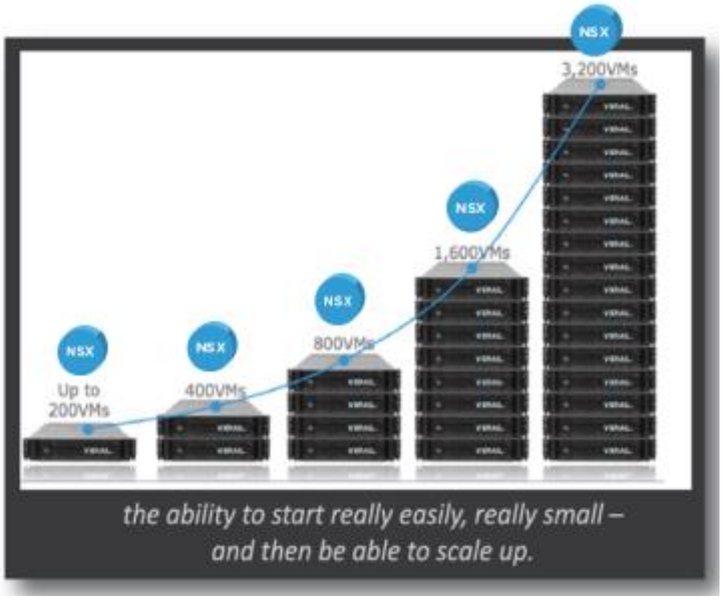
The VMware VxRAIL solution is a highly automated, hyper-converged infrastructure appliance. The appliance helps lower capital and operational costs while providing a fully integrated, preconfigured, and pre-tested VMware hyper-converged solution. VxRAIL provides several benefits in terms of ease of management, scalability, rapid deployment, operational simplicity, and capital/operational cost savings. See the following Dell EMC webpage for additional information.

FIGURE 1: VMWARE VXRAIL UNIT

By having the option to add VMware NSX-V network virtualization and security technology to VxRAIL, NSX helps further consolidate aspects of security and networking into the appliance.

By replicating the physical networking constructs in software and decoupling the networking from the physical hardware, VMware NSX provides similar benefits as server virtualization did with VMs: increased efficiency, productivity, flexibility, agility, and overall lower capital and operational costs. Further, as VxRAIL scales, NSX can scale with it.

The software-based approach taken by NSX for networking and security solves several challenges with traditional solutions for security, automation, and application continuity.



the ability to start really easily, really small – and then be able to scale up.

FIGURE 2: NSX-V CAN SCALE EASILY WITH VXRAIL

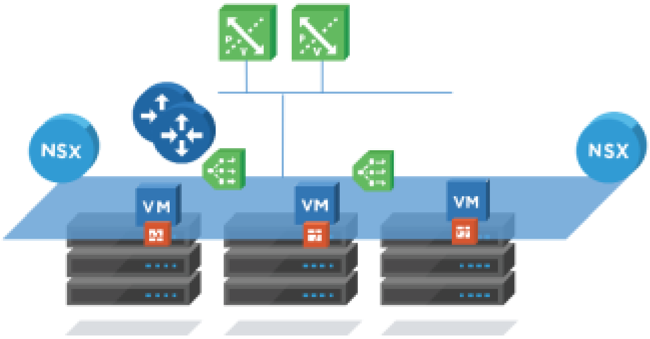


FIGURE 3: NETWORK VIRTUALIZATION & SECURITY WITH NSX

By optionally adding NSX to VxRAIL, maximum hyper-convergence and associated benefits and cost savings can be achieved. This document focuses on converged solutions leveraging VxRAIL with NSX for security.

Before looking at how VxRAIL and NSX can provide hyper-converged solutions with built-in security for different use cases, it's important to understand traditional security challenges and hyper-convergence with VxRAIL in general.

Traditional Challenges with Security

Traditional challenges with security include:

- Silos exist for computer, networking, storage, and security. This results in additional delay in implementing new or changes to security policies. Typically, a procedure is followed where a change request is submitted to the security team to make an update.
- Space and power limitations within a data center (DC), branch, or remote office may restrict the ability to deploy proposed hardware for solution. Traditional security appliances typically require the deployment of a separate dedicated physical security appliance which requires an additional physical/power footprint.
- Complexity in terms of management and updating of different components. In a traditional solution, since there typically is not much integration, all components have to be updated separately and interoperability has to be verified; many times the components are from different vendors.
- Traditional security policies are based on IP addresses which can change, are difficult to manage, and inherently the policies are not application centric.
- As security policies are based on IP addresses, security appliances typically run into policy rule sprawl, where, as applications increase, policy rules have to be constantly added/modified.
- Workload migration is restricted if the destination does not have appropriate security policies.
- Traditional firewalls/security appliances are perimeter-centric (hard shell, soft core), leaving the internal data center vulnerable if the perimeter or internal workload is compromised.

Figure 4 below shows a visualization of going from a traditional silo-based solution to a converged solution leveraging VxRAIL with NSX for Security. Hyper-converged solutions such as VxRAIL solve the above mentioned traditional challenges via a single integrated vSphere stack and validated solution. The optional NSX add-on provides security baked into the VxRAIL converged appliance.

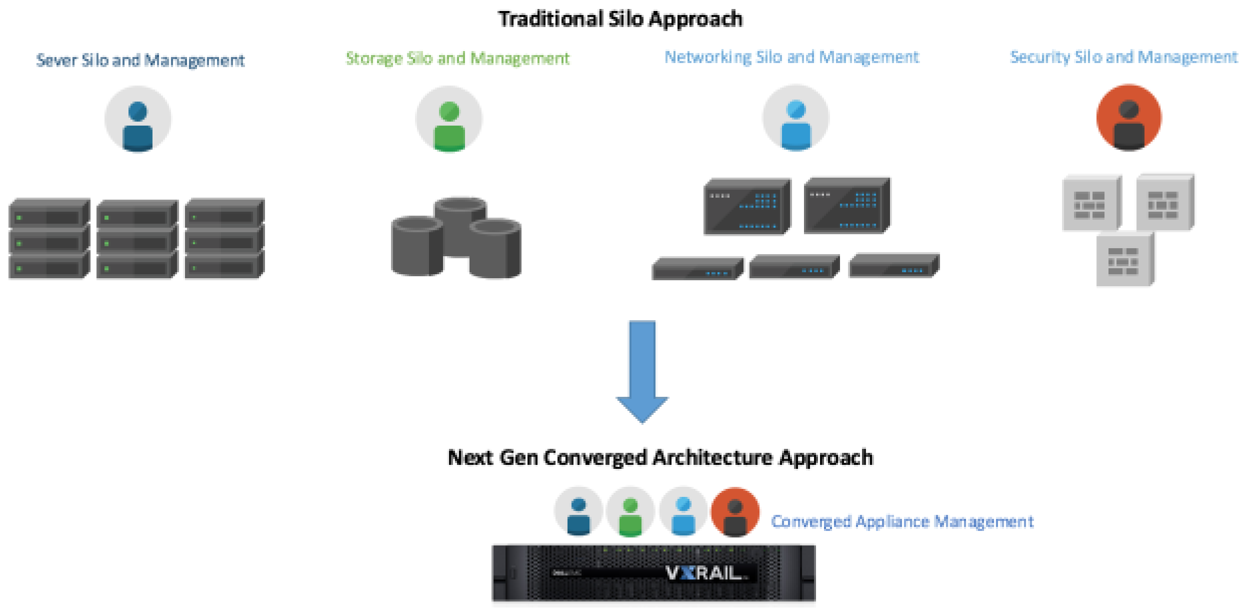

Traditional Silo Approach
Sever Silo and Management
Storage Silo and Management
Networking Silo and Management
Security Silo and Management
Next Gen Converged Architecture Approach
Converged Appliance Management
VXRAIL

FIGURE 4: FROM TRADITIONAL TO NEXT GEN CONVERGED ARCHITECTURE

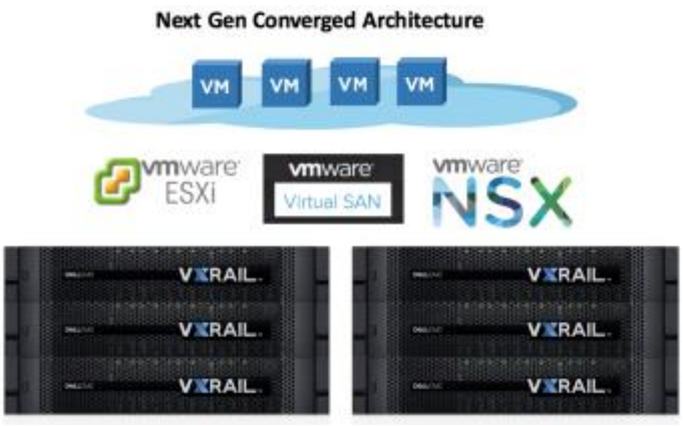


FIGURE 5: NEXT GEN CONVERGED ARCHITECTURE WITH VXRAIL AND NSX

Although there is innovation in terms of the different form factors offered for VxRAIL and the ability to easily scale-up, the true magic and what makes this truly a hyper-converged appliance is the industry leading software for virtualized servers (ESXi), virtualized storage (vSAN), and the option of installing NSX for virtualized networking and security.

In effect, the solution provides a software defined data center (SDDC) in a box. In the following sections we discuss the specifics of the VxRAIL solution and NSX in more detail.

Understanding VxRAIL

VxRAIL is a hyper-converged appliance offering SDDC in a box; it has a distributed system architecture consisting of common modular building blocks that scale linearly from 3 to 64 nodes in a cluster. As VxRAIL units are added, an auto-discovery mechanism consisting of a service on the vCenter server appliance (VCSA) and on each node is used for discovery of the additional VxRAIL nodes.

A key strength of the VxRAIL offering is the flexibility you have in form factor/hardware and the ability to easily scale-out horizontally. Multiple specifications/models are available from a 1U1Node appliance to a 2U4Node appliance. CPU/Ram/Storage/Network Connectivity and other options also vary considerably providing for maximum flexibility. For example, a VxRAIL appliance with 4 x 1GbE NICs may be sufficient for one customer while another customer may require an appliance with 6 x 10 GbE SFP+ connectivity. See the Dell EMC VxRAIL Appliance Specification Sheet for more detail.

In addition to the flexibility in hardware choice, VxRAIL comes loaded with software including:

- VMware vCenter
- VMware ESXi
- VMware vSAN (Software-Defined Storage)
- VMware vRealize Log insight
- VxRAIL Manager (automates VM provisioning)

Also, the option exists to have NSX-V installed as an add-on which provides all the benefits of NSX-V network virtualization, security, and automation. In a following section we look at security use cases for VxRAIL and NSX-V.

The scope of this paper in terms of scale is 4 x VxRAIL units consisting of 4 nodes each scaling to 16 nodes; however, it is possible to scale up to 64 nodes. Further, two options exist for expansion:

1: Add nodes in new VxRAIL appliance to existing Cluster/VDS
2: Add nodes in new VxRAIL appliance to different Cluster/VDS

The scope of this paper focuses on the first option and demonstrates how NSX-V can be deployed on to VxRAIL for use with different use cases. In this first option, some facts to be aware of in terms of design are:

- Only embedded vCenter support
- Single Cluster
- Single VDS
- Scale out max is 64 nodes in a cluster (16 VxRAIL appliances)

Why NSX-V with VxRAIL

The reason(s) an organization may desire a hyper-converged solution are:

- Rapid deployment
- Ease of scale-out
- Ease of management
- Operational simplicity

- Capital and Operation cost savings

All of the above-mentioned reasons can lead to an organization either already having (brownfield) or desiring (greenfield) a hyper-converged solution/model. In most cases, the driver will be to have rapid deployment with ease of management for workloads and infrastructure.

There are several use cases for running NSX-V on VxRAIL. This paper focuses on the security use cases when leveraging the NSX-V platform for security within VxRAIL.

By utilizing NSX-V for security with VxRAIL, deployment time is decreased further, as now the appliance itself handles security and no additional security hardware deployment for the applications is required. NSX-V also scales orthogonally to VxRAIL. As VxRAIL nodes are added to a cluster where NSX-V security is installed, the NSX-V security components are automatically installed on the new host(s). Further, as security with NSX-V is integrated into the vSphere platform, the same familiar vSphere Web Client is used and management is streamlined.

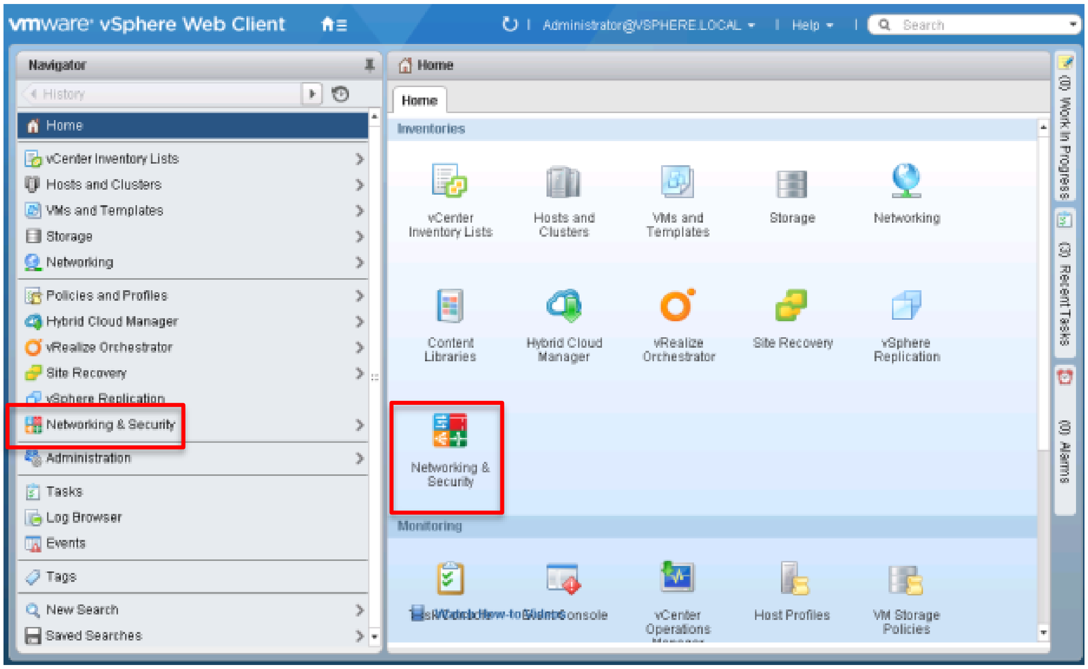


FIGURE 6: NSX-V MANAGEMENT FROM VSPHERE WEB BROWSER

Dell EMC VxRAIL, powered by vSAN and offered with Dell PowerEdge servers with the option of NSX-V, is the only specifically developed and fully optimized hyper-converged appliance co-designed and built with VMware.

In addition to being aligned with the converged architecture, VMware NSX-V also provides an enhanced security model where security policies are applied at the vNIC-level of workloads allowing for a more segmented approach of the environment. The ability to segment the data center at this granular level while providing advanced stateful security capabilities is called micro-segmentation and is discussed in more detail in the next section. In effect, NSX-V micro-segmentation is a specific security capability that decreases the level of risk and increases the security posture for workloads within a data center.

Additionally, it should be noted that NSX-V is the only micro-segmentation solution to have achieved all of the following industry standards:

- Common Criteria certification (EAL) 2+; read more here
- ICSA Labs certified firewall
- FIPS 140-2 certification
- Satisfies all NIST cybersecurity recommendations for protecting virtualized workloads

A publicly available Micro-segmentation Cybersecurity Benchmark report by Coalfire, an independent cyber risk management advisor and assessor, is also available here.

Intro to NSX-V and Micro-segmentation

The scope of this paper is limited to leveraging NSX-V for security, however, NSX-V is a complete network virtualization and security platform. NSX-V allows for creating entire virtual networks within software; this allows for efficiency and agility in terms of deployment, provisioning, and utilization of resources.

Network virtualization decouples the workloads from the physical underlying infrastructure by leveraging a network overlay technology and moves the intelligence of the network from hardware to software. Overall, this provides a very agile environment where workload provisioning can occur quickly and workload mobility is no longer constrained by artificial network boundaries. Further, since the network components and

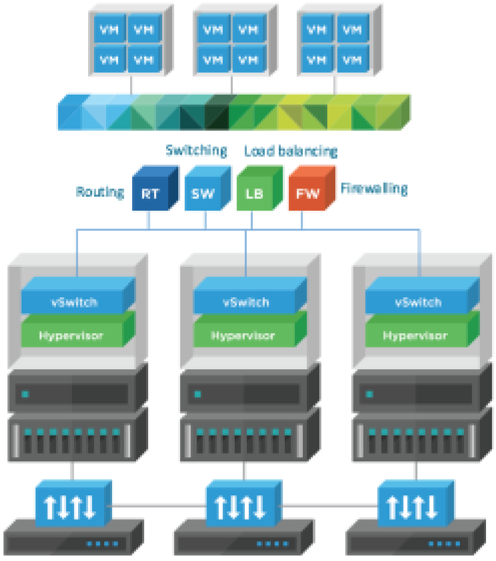


Figure 7: NSX-V as a Platform for Networking and Security

intelligence has been moved to software, the environment can be highly automated.

A key innovation of NSX-V is the ability to provide network and security functions such as switching, routing, and firewalling in a distributed fashion across all hosts and within the kernel-level module of the hypervisor. This allows for spreading the load across all hosts in the environment, and, at the same time, providing close to line-rate performance due to the functions occurring at the kernel-level.

VMware NSX-V targets the following three high-level use case buckets:

1.) Security:

NSX-V provides for an enhanced distributed security model where security policies are applied closer to the workload using higher-level security constructs and where security polices move with the workload. NSX-V helps segment the environment, decreasing risk and the attack surface while increasing security. The many advantages of leveraging NSX-V for security are discussed in this paper.

2.) Automation

NSX-V also provides a platform for automation. By providing a suite of automation tools that integrate with NSX-V such as vRealize Automation for management and vRealize Orchestrator for orchestration, NSX-V allows for advanced automation workflows. Additionally, the NSX-V REST API allows for automation through a REST API interface or through popular programming languages like Python, PowerShell, and Perl.

3.) Application Continuity

Application Continuity is defined as the ability of an application to continuously run with little to no downtime. NSX-V provides a platform for application continuity use cases such as workload mobility, disaster avoidance, and disaster recovery by providing consistent networking/security and automation between sites.

This paper focuses on the first use case of security. Specifically, this paper discusses leveraging NSX-V security and micro-segmentation within a VxRAIL environment.

NSX-V micro-segmentation is a specific security capability that decreases the level of risk and increases the security posture of a data center. It does so by providing the following:

- **Distributed Stateful Firewalling**
  NSX-V security is implemented at the kernel-level of the ESXi hypervisor and distributed across all hosts in the environment. This approach allows for stateful security that scales with the compute infrastructure, allowing protection and visibility on a per application basis.

- **Smaller Attack Surface via Segmentation**
  As security policies are applied at the vNIC level, the environment is effectively segmented as security policies are pushed and enforced at the workload vNIC. Therefore, the attack surface is greatly minimized as segmentation enforced at the vNIC-level allows communication only between permitted entities.

- **Topology Agnostic Segmentation**
  NSX-V segmentation via distributed firewall (DFW) can be utilized for protection regardless of the physical underlying infrastructure. The underlying infrastructure can be L2, L3, or a combination of L2/L3. Additionally, NSX-V can provide segmentation for workloads on conventional VLANS or workloads on network overlays using network virtualization technology provided by NSX-V.

- **Use of Higher-Level Security Constructs**
  With NSX-V, security policies can be applied with per-workload granularity. A grouping construct called **Security Group** can be leveraged to dynamically identify workloads based on matching criteria such as VM Name, Security Tag, OS type, Active Directory groups, and more. These security groups can then be used within the NSX-V security policies and are completely independent from the underlying physical infrastructure.

- **Security Policies that Move with the Workload**
  NSX-V decouples the workloads from the underlying physical infrastructure and enables ease of workload mobility. As workloads are moved/vMotioned across hosts, the security policies move with the workloads. Thus, no longer is mobility of workloads constrained by underlying physical infrastructure.

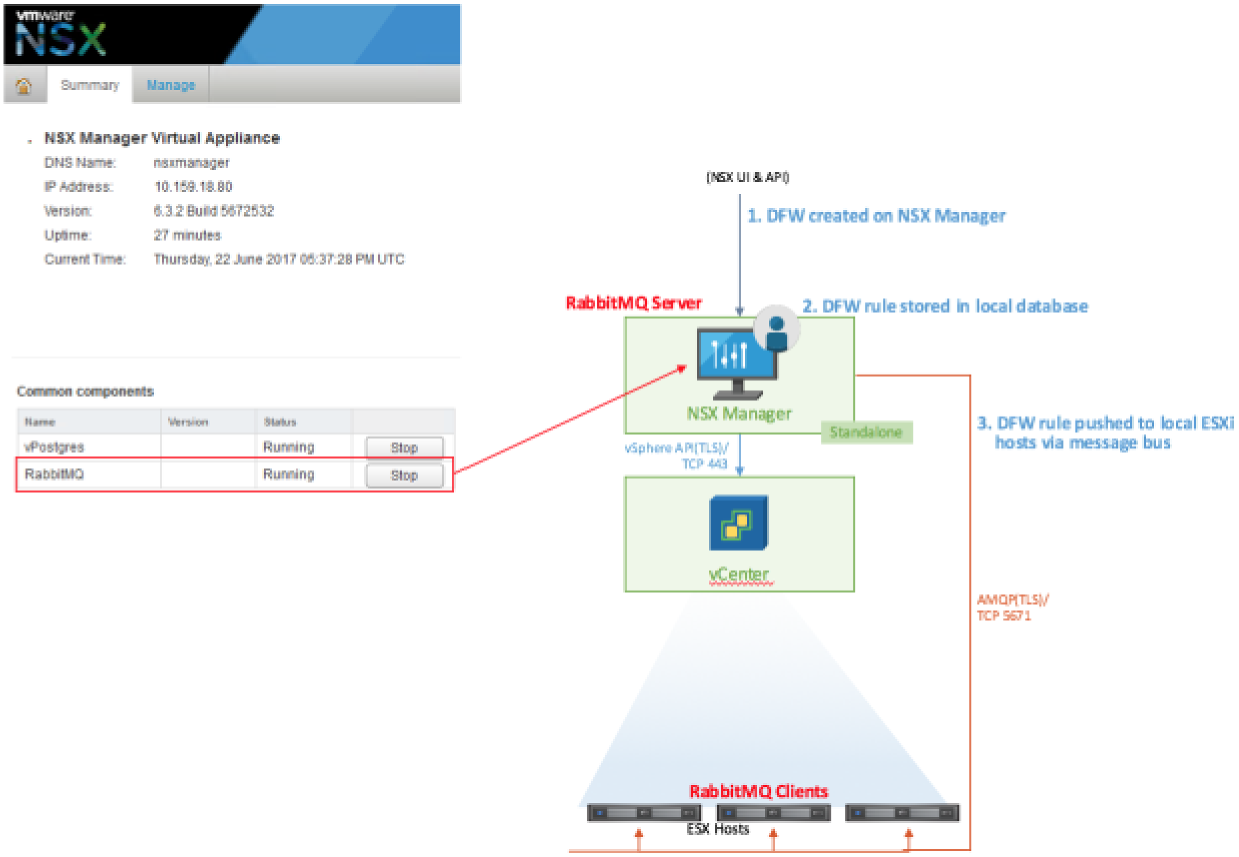
- **Central Management**
  Although NSX-V provides all the functionality and benefits of a stateful distributed firewall such as scalability and enhanced segmentation of the data center, another benefit is central management of the security policies which are ultimately distributed across all hosts. One central location to construct and apply security policies across all hosts allows for increased productivity and faster provisioning of applications.

- **3rd Party Service Insertion**
  VMware NSX-V provides up to L4-level security via the stateful distributed firewall. In addition to this, NSX-V also provides the option for L7 application-level security by redirecting desired traffic to 3rd party services from vendors like Palo Alto Networks VM-Series or Check Point vSEC. Vendors for both guest introspection and network introspection services are supported.

NSX-V Security Architecture

To take advantage of NSX-V as a security platform, only one appliance, the NSX Manager, needs to be installed on an ESXi host. The NSX Manager is provided as an OVF file which can be imported and installed directly onto a ESXi host. The NSX Manager must also be registered to a vCenter at which point the NSX Manager plugin gets installed in the vSphere web client and through which configuration of NSX-V and configuration of logical networking and security policies can be done.

Figure 8 below provides a visualization of the NSX-V security architecture.


vmware NSX
Summary
Manage

NSX Manager Virtual Appliance

DNS Name: nsxmanager
IP Address: 10.159.18.80
Version: 6.3.2 Build 5672532
Uptime: 27 minutes
Current Time: Thursday, 22 June 2017 06:37:28 PM UTC

Common components

Name	Version	Status	
vPostgres		Running	Stop
RabbitMQ		Running	Stop

(NSX UI & API)
1. DFW created on NSX Manager
RabbitMQ Server
2. DFW rule stored in local database
NSX Manager
Standalone
3. DFW rule pushed to local ESXi hosts via message bus
vSphere API(TLS)/ TCP 443
vCenter
AMQP(TLS)/ TCP 5671
RabbitMQ Clients
ESX Hosts

FIGURE 8: VMWARE NSX-V SECURITY ARCHITECTURE

Once the NSX Manager OVF is deployed, a message broker server called RabbitMQ is started on the NSX Manager. A messaging protocol called Advanced Message Queuing Protocol (AMQP) is used by the message broker server in NSX-V to communicate to the ESXi hosts.

NSX Manager has a 1:1 relationship with vCenter meaning only one vCenter can be registered with NSX Manager. When the vCenter is registered with NSX Manager and host preparation is done installing the NSX-V VIBs on the vSphere clusters, a message bus connection is formed from the RabbitMQ server to the ESXi hosts within the clusters where NSX-V has been enabled. The RabbitMQ server runs on the NSX Manager and the RabbitMQ clients run on the respective ESXi hosts. This message bus is used to install and configure NSX-V components on ESXi hosts. All security configuration and policy is pushed down the message bus to respective ESXi hosts.

The sequence is as follows for implementation flow of a DFW rule:

1. DFW rule is created on NSX Manager

2. DFW rule is stored in NSX Manager local database

3. DFW rule is pushed down to respective ESXi hosts via message bus

Introducing NSX-V into VxRAIL

I. Initial VxRAIL Setup

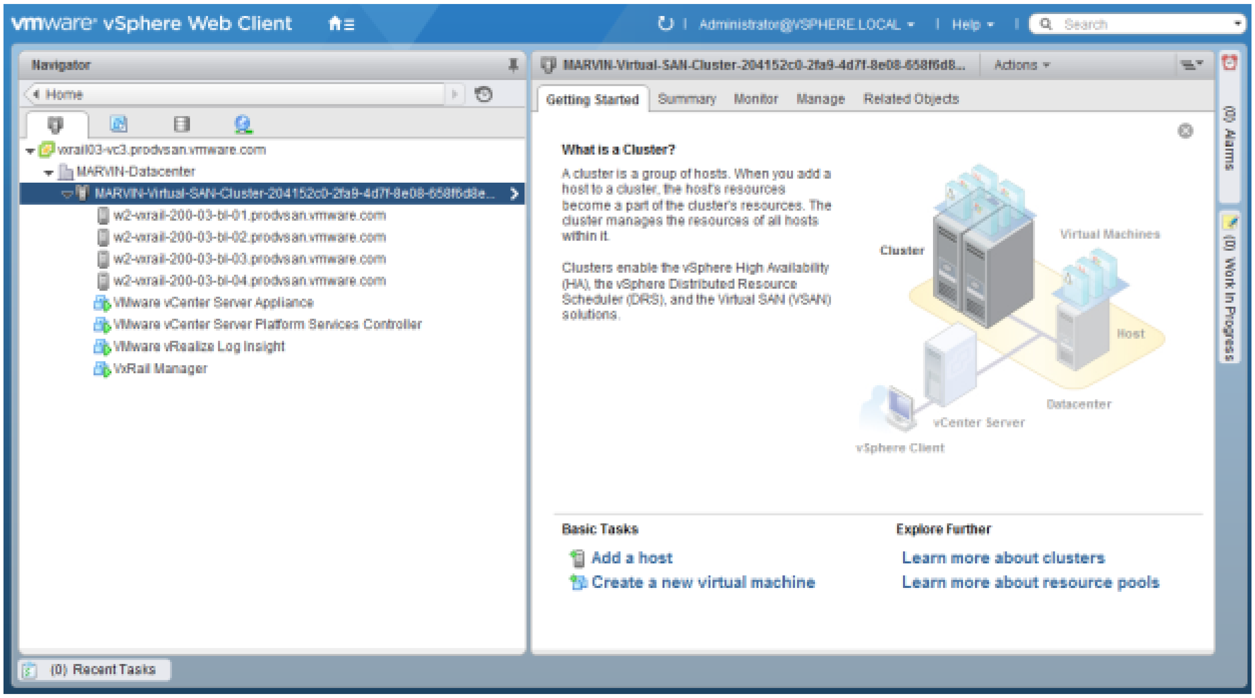
One of the benefits of VxRAIL is that it is shipped preconfigured with inputs customer has provided. Figure 9 below displays the front of a VxRAIL G Series with 4 enclosed server nodes.

FIGURE 9: FRONT VIEW OF VXRAIL G-SERIES

The VxRAIL appliance by default has all nodes as part of one cluster consisting of a vSAN datastore and one VDS. A VxRAIL can be configured such that the vCenter is embedded/installed on a hypervisor it is managing or external to the environment. NSX-V supports both models. The external model is typically preferred in certain deployments such as when NSX-V is running on multiple vCenters and advanced multi-vCenter NSX-V capabilities are needed. The focus here will be on embedded vCenter as we are specifically concerned with a single vCenter/site and a one cluster/VDS design.

Also, the option exists to have the Platform Services Controller (PSC) either embedded within vCenter or external to it. Although both models are supported, external PSC is again preferred in certain deployments where multi-vCenter NSX-V capabilities are needed. Again, the focus here will be on embedded vCenter as we are specifically concerned with a single vCenter/site and a one cluster/VDS design.

Figure 10 and 11 below show the default Cluster and VDS setup for VxRAIL.

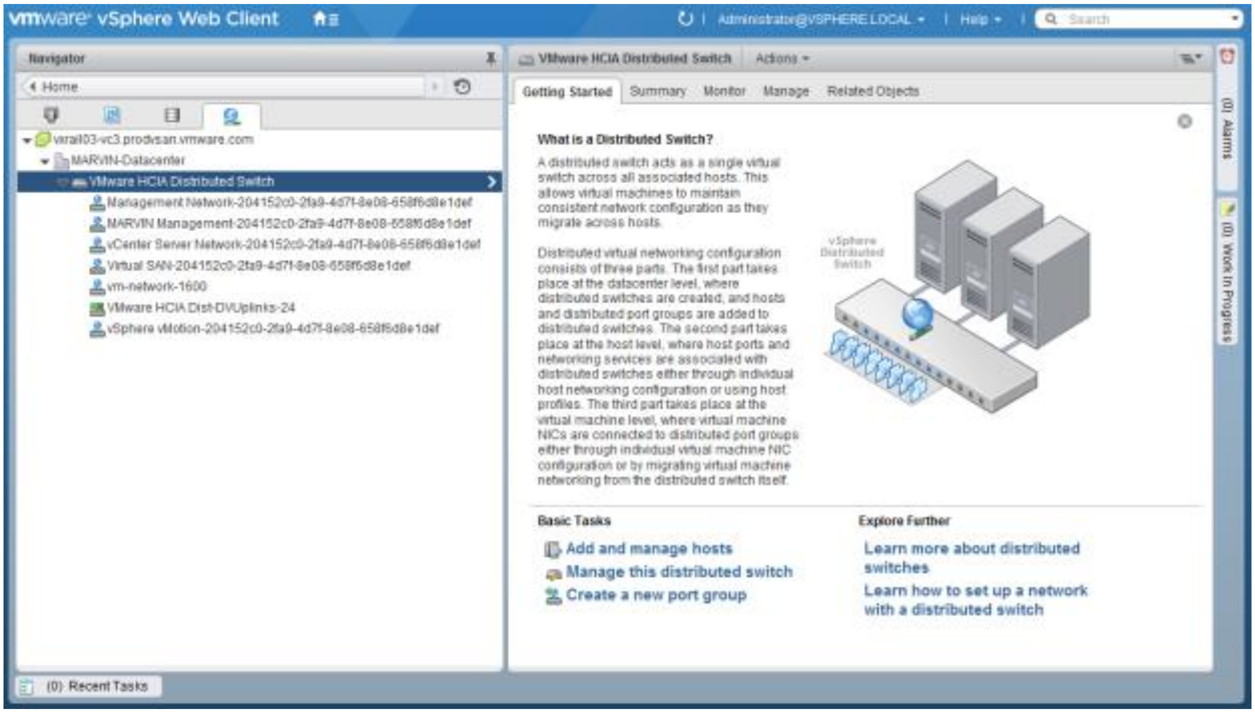

vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
vxrail03-vc3.prodvsan.vmware.com
MARVIN-Datacenter
MARVIN-Virtual-SAN-Cluster-204152c0-2fa9-4d7f-8e08-658f6d8e...
w2-vxrail-200-03-bl-01.prodvsan.vmware.com
w2-vxrail-200-03-bl-02.prodvsan.vmware.com
w2-vxrail-200-03-bl-03.prodvsan.vmware.com
w2-vxrail-200-03-bl-04.prodvsan.vmware.com
VMware vCenter Server Appliance
VMware vCenter Server Platform Services Controller
VMware vRealize Log Insight
VxRail Manager
MARVIN-Virtual-SAN-Cluster-204152c0-2fa9-4d7f-8e08-658f6d8...
Actions
Getting Started
Summary
Monitor
Manage
Related Objects
Cluster
Virtual Machines
Host
Datacenter
vCenter Server
vSphere Client
Basic Tasks
Add a host
Create a new virtual machine
Explore Further
Learn more about clusters
Learn more about resource pools
(0) Alarms
(0) Work In Progress
(0) Recent Tasks

What is a Cluster?

A cluster is a group of hosts. When you add a host to a cluster, the host's resources become a part of the cluster's resources. The cluster manages the resources of all hosts within it.

Clusters enable the vSphere High Availability (HA), the vSphere Distributed Resource Scheduler (DRS), and the Virtual SAN (VSAN) solutions.

FIGURE 10: DEFAULT SINGLE CLUSTER ON VXRAIL


vmware vSphere Web Client
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Home
vxrail03-vc3.prodvsan.vmware.com
MARVIN-Datacenter
VMware HCIA Distributed Switch
Management Network-204152c0-2fa9-4d7f-8e08-658f6d8e1def
MARVIN Management-204152c0-2fa9-4d7f-8e08-658f6d8e1def
vCenter Server Network-204152c0-2fa9-4d7f-8e08-658f6d8e1def
Virtual SAN-204152c0-2fa9-4d7f-8e08-658f6d8e1def
vm-network-1600
VMware HCIA Dist-DVUplinks-24
vSphere vMotion-204152c0-2fa9-4d7f-8e08-658f6d8e1def
VMware HCIA Distributed Switch
Actions
Getting Started
Summary
Monitor
Manage
Related Objects
vSphere Distributed Switch
Basic Tasks
Add and manage hosts
Manage this distributed switch
Create a new port group
Explore Further
Learn more about distributed switches
Learn how to set up a network with a distributed switch
(0) Alarms
(0) Work In Progress
(0) Recent Tasks

What is a Distributed Switch?

A distributed switch acts as a single virtual switch across all associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate across hosts.

Distributed virtual networking configuration consists of three parts. The first part takes place at the datacenter level, where distributed switches are created, and hosts and distributed port groups are added to distributed switches. The second part takes place at the host level, where host ports and networking services are associated with distributed switches either through individual host networking configuration or using host profiles. The third part takes place at the virtual machine level, where virtual machine NICs are connected to distributed port groups either through individual virtual machine NIC configuration or by migrating virtual machine networking from the distributed switch itself.

FIGURE 11: DEFAULT SINGLE VDS ON VXRAIL

Taking a deeper look at the default VDS, we can see it already has networks setup for management, storage (vSAN), vMotion, management of infrastructure (ESXi hosts), management for vCenter, and separate management for the MARVIN VxRAIL application which is used by VxRAIL manager to detect and add new VxRAIL nodes. Installing NSX-V DFW security does not change any of the VDS design. NSX-V DFW components are installed within the hypervisor kernel. No changes are made to either the VDS or network design.

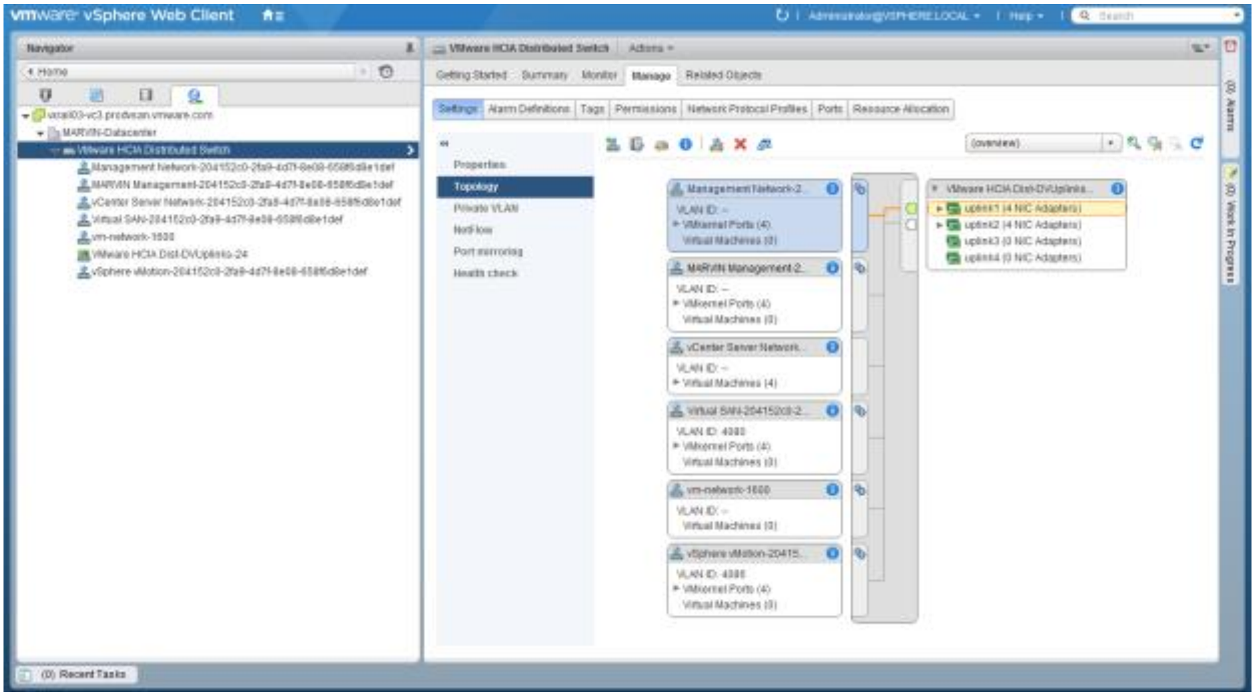


FIGURE 12: DEFAULT SINGLE VDS ON VXRAIL

II. NSX-V Cluster and VDS Design for VxRAIL

For converged architectures such as VxRAIL where a preconfigured setup dictates some of the design decisions, for NSX-V security implementation, the default single cluster and single VDS design can be leveraged. As additional VxRAILs/hosts are added, the cluster expands to incorporate the additional hosts. Once, NSX-V security components/kernel level modules are installed on the vSphere cluster, as hosts are added and the cluster expands, the new hosts will automatically have the NSX-V security components installed. NSX-V scales in-sync along with VxRAIL.

III. Installing NSX-V on VxRAIL

Note, VxRAIL is a hyper converged appliance which NSX can run on. NSX follows its own lifecycle orthogonal to underlying hardware.

To take advantage of NSX-V as a security platform, only one appliance, the NSX Manager, needs to be installed on an ESXi host. The NSX Manager is provided as an OVF file which can be imported and installed directly onto a ESXi host. The NSX Manager must also be registered to a vCenter at which point the NSX Manager plugin gets installed in the vSphere web client and through which NSX-V configuration and security policies are configured and applied.

The NSX Manager is deployed on the management network and this often is the same network vCenter and other management components is installed on. It must have connectivity to vCenter and all the ESXi hosts over this management network; the network connectivity can be either L2 or L3. For example, in the below initial setup of VxRAIL, we can see vCenter and other management components have been installed in the network labeled as **vCenter Server Network**. This is where NSX Manager would typically be installed by deploying the NSX Manager OVF.

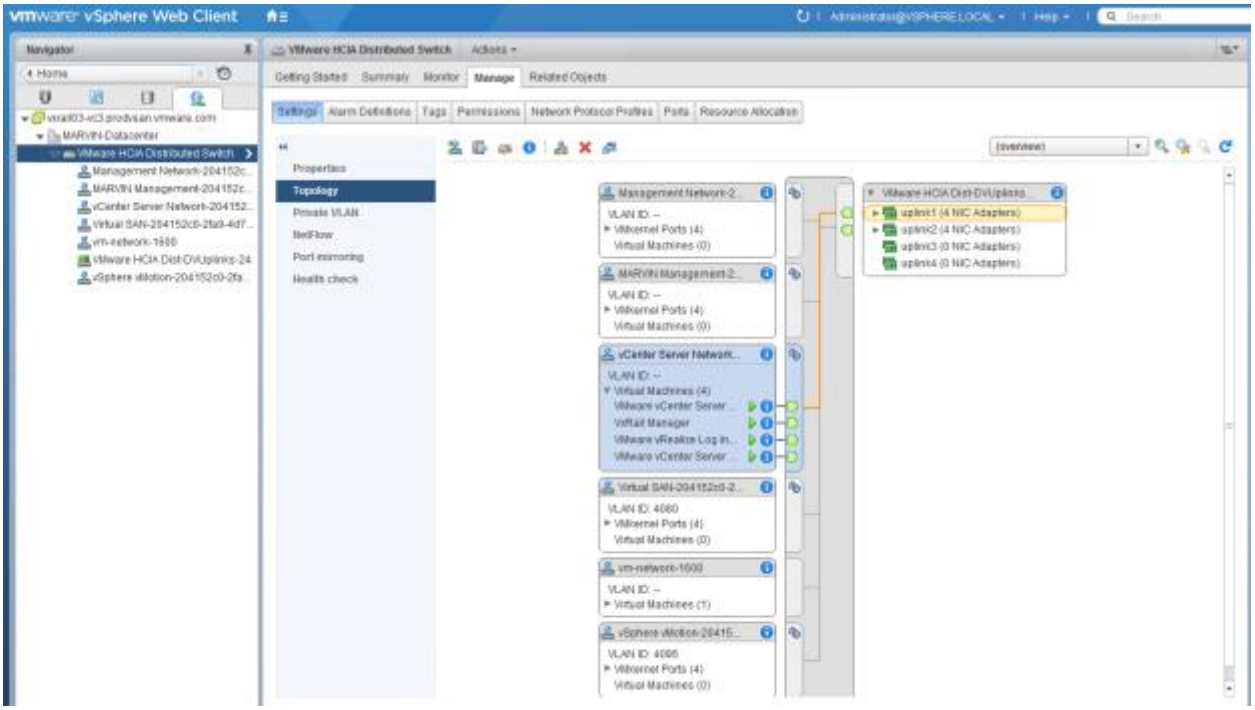
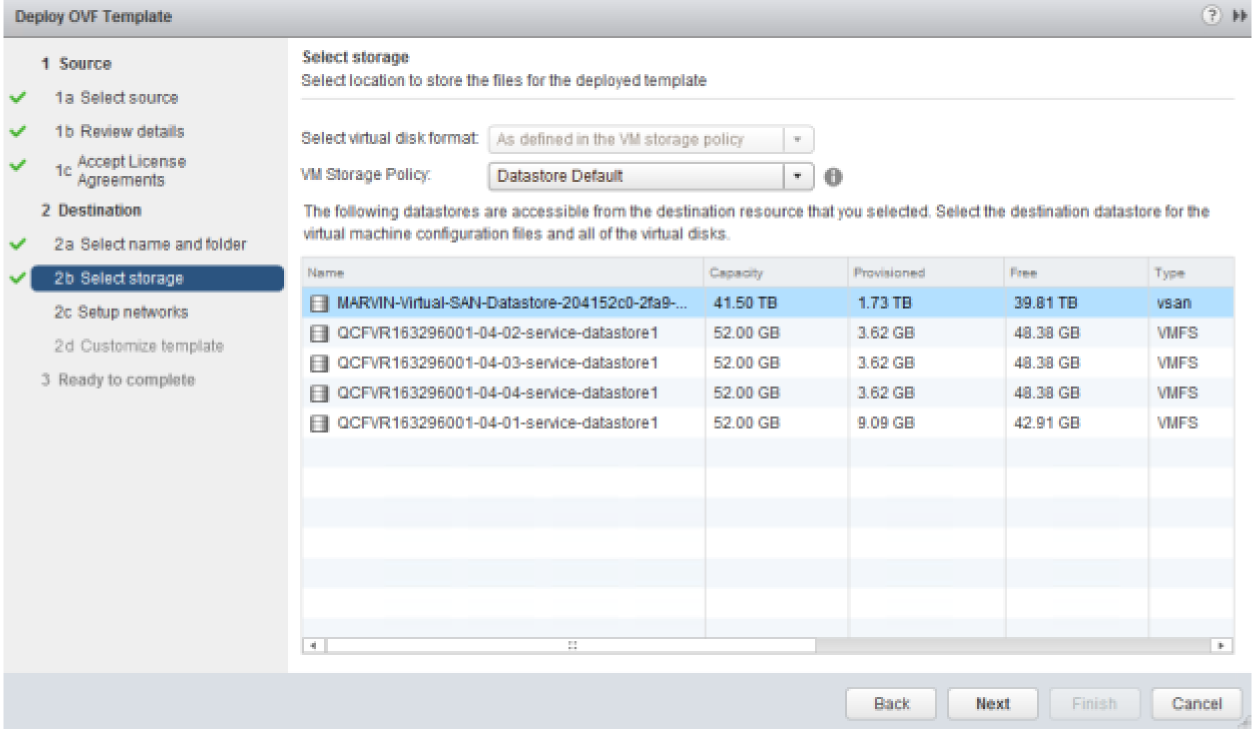


FIGURE 13: INITIAL VDS CONFIGURATION OF VXRAIL

It's important to note that when the NSX-V OVF is deployed, the datastore of **Type vSAN** should be selected. The other devices seen are satadom boot devices not meant to be used for

VMs. Since NSX Manager is installed on vSAN, it inherits all the protection attributes associated with vSAN for additional resiliency.



1 Source
- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept License Agreements

2 Destination
- ✓ 2a Select name and folder
- ✓ 2b Select storage
- 2c Setup networks
- 2d Customize template

3 Ready to complete

Select storage

Select location to store the files for the deployed template

Select virtual disk format: As defined in the VM storage policy

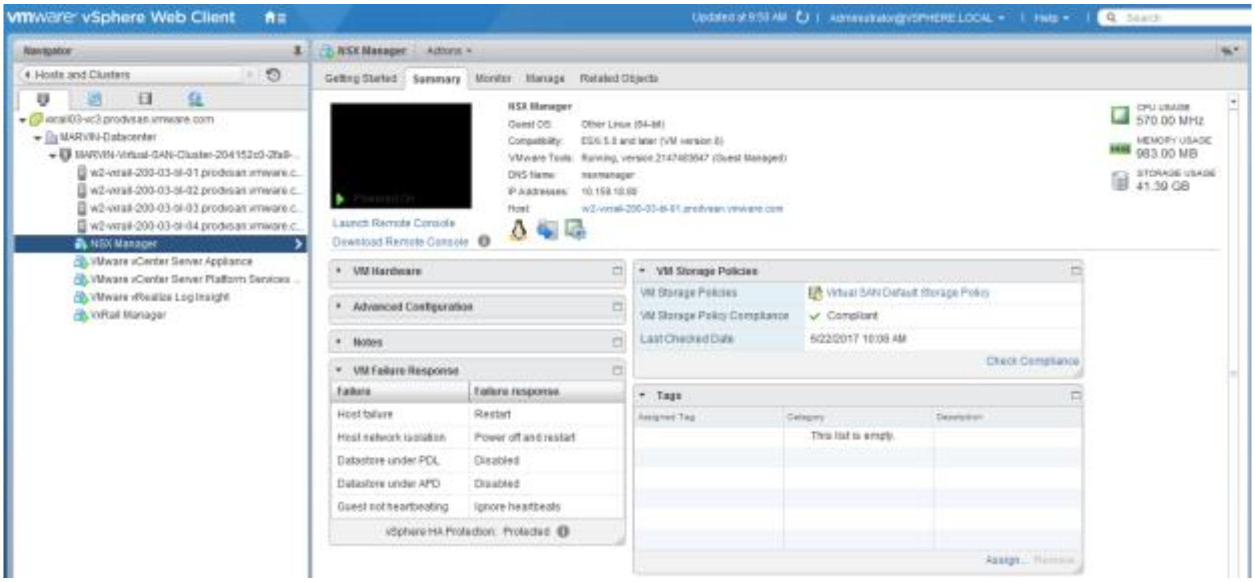
VM Storage Policy: Datastore Default

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type
MARVIN-Virtual-SAN-Datastore-204152c0-2fa9-...	41.50 TB	1.73 TB	39.81 TB	vsan
QCFVR163296001-04-02-service-datastore1	52.00 GB	3.62 GB	48.38 GB	VMFS
QCFVR163296001-04-03-service-datastore1	52.00 GB	3.62 GB	48.38 GB	VMFS
QCFVR163296001-04-04-service-datastore1	52.00 GB	3.62 GB	48.38 GB	VMFS
QCFVR163296001-04-01-service-datastore1	52.00 GB	9.09 GB	42.91 GB	VMFS

FIGURE 14: SELECTING VSAN STORAGE TO INSTALL NSX MANAGER ON

Once deployed, the NSX Manager VM should be running within the cluster as shown below.



- vxrail03-vc3.prodvsan.vmware.com
  - MARVIN-Datacenter
    - MARVIN-Virtual-SAN-Cluster-204152c0-2fa9-...
      - w2-vxrail-200-03-bl-01.prodvsan.vmware.c...
      - w2-vxrail-200-03-bl-02.prodvsan.vmware.c...
      - w2-vxrail-200-03-bl-03.prodvsan.vmware.c...
      - w2-vxrail-200-03-bl-04.prodvsan.vmware.c...
      - NSX Manager
      - VMware vCenter Server Appliance
      - VMware vCenter Server Platform Services ...
      - VMware vRealize Log Insight
      - VxRail Manager

NSX Manager

Guest OS: Other Linux (64-bit)
Compatibility: ESXi 5.5 and later (VM version 8)
VMware Tools: Running, version 2147483647 (Guest Managed)
DNS Name: nsxmanager
IP Addresses: 10.159.10.88
Host: w2-vxrail-200-03-bl-01.prodvsan.vmware.com

CPU USAGE 570.00 MHz
MEMORY USAGE 983.00 MB
STORAGE USAGE 41.39 GB

VM Failure Response

Failure	Failure response
Host failure	Restart
Host network isolation	Power off and restart
Datastore under PDL	Disabled
Datastore under APD	Disabled
Guest not heartbeating	Ignore heartbeats

vSphere HA Protection: Protected

VM Storage Policies

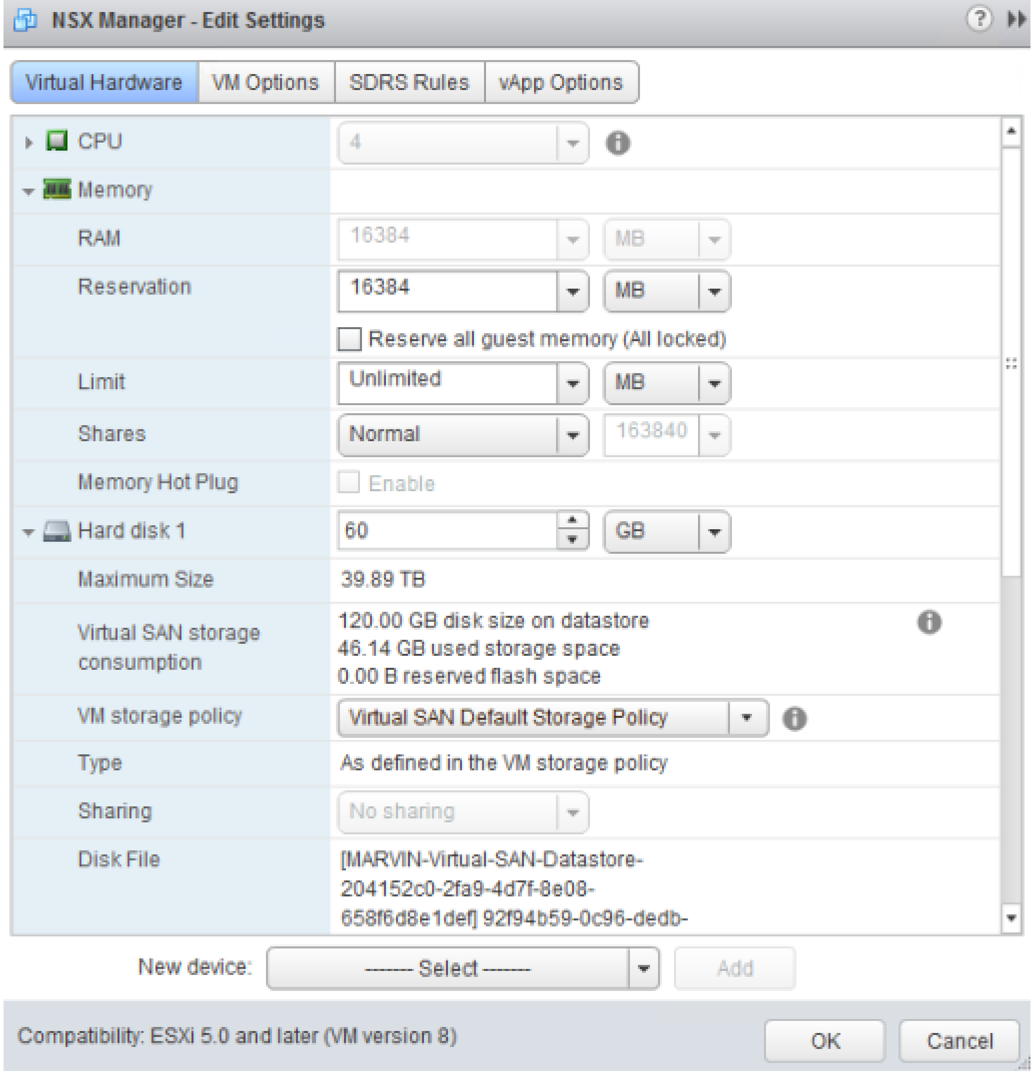
VM Storage Policies	Virtual SAN Default Storage Policy
VM Storage Policy Compliance	✓ Compliant
Last Checked Date	6/22/2017 10:08 AM

Tags

Assigned Tag	Category	Description
	This list is empty.	

FIGURE 15: NSX MANAGER DEPLOYED

If we look at the NSX Manager settings shown in Figure 16, we can confirm it automatically consumes 4 vCPUs and reserves 16 GbE of memory while using 60 GB in disk. It is recommended to use DRS resource pools so NSX Manager is deployed automatically on the host with best available resources. If DRS is disabled and because VM placement is based on storage capacity and vSAN provides distributed storage, any OVA/OVF deployment is handled by the storage policy and out of the users control when selecting the cluster for placement. An alternative option is to manually recommend host or resource pool selection.



CPU	4
Memory	
RAM	16384 MB
Reservation	16384 MB □ Reserve all guest memory (All locked)
Limit	Unlimited MB
Shares	Normal 163840
Memory Hot Plug	□ Enable
Hard disk 1	60 GB
Maximum Size	39.89 TB
Virtual SAN storage consumption	120.00 GB disk size on datastore 46.14 GB used storage space 0.00 B reserved flash space
VM storage policy	Virtual SAN Default Storage Policy
Type	As defined in the VM storage policy
Sharing	No sharing
Disk File	[MARVIN-Virtual-SAN-Datastore-204152c0-2fa9-4d7f-8e08-658f6d8e1def] 92f94b59-0c96-dedb-

New device: ------- Select -------

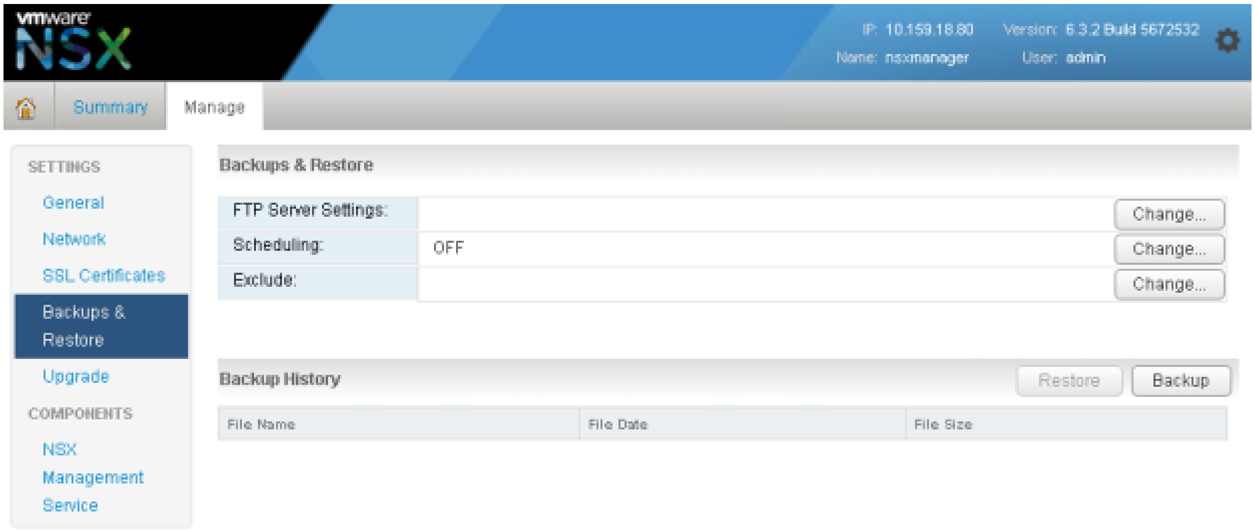
Compatibility: ESXi 5.0 and later (VM version 8)

FIGURE 16: NSX MANAGER RESOURCE UTILIZATION

For resiliency of NSX Manager the following should be noted:

- vSphere HA is recommended on the respective cluster
- DRS is recommended on the respective cluster (DRS is available only in Enterprise license)

- NSX Manager should be configured for automatic configuration backups. This can be done in the NSX Manager GUI as shown below in Figure 17 and Figure 18.



IP: 10.159.18.80 Version: 6.3.2 Build 5672532
Name: nsxmanager User: admin

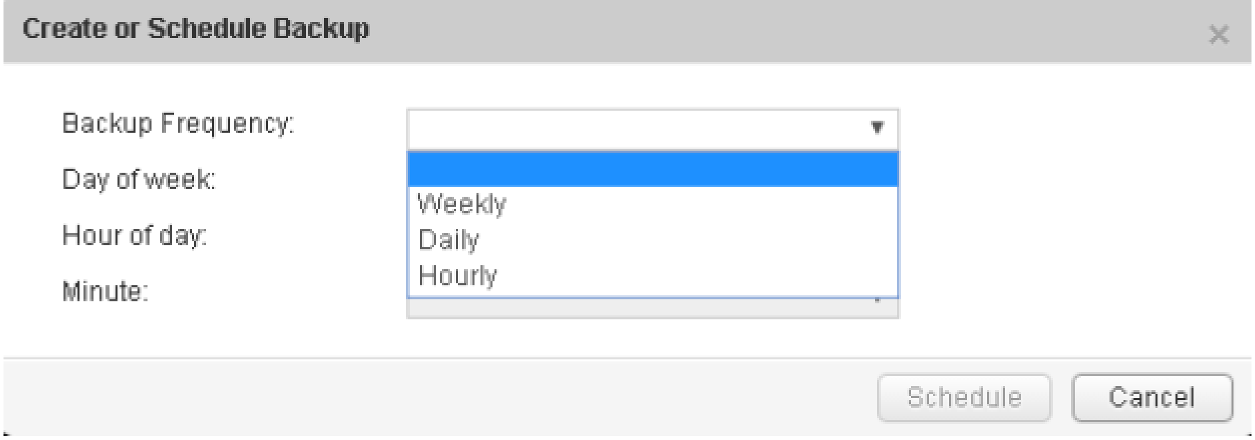
Backups & Restore

FTP Server Settings:
Scheduling: OFF
Exclude:

Backup History

File Name	File Date	File Size

FIGURE 17: NSX MANAGER GUI BACKUPS & RESTORE TAB



Create or Schedule Backup

Backup Frequency:
Day of week:
Hour of day:
Minute:

Weekly
Daily
Hourly

FIGURE 18: SCHEDULING AN AUTOMATIC BACKUP WITHIN THE NSX MANAGER GUI

- Since vSAN is used by VxRAIL, the storage is distributed across all hosts, and, with four hosts, the Failures to Tolerate (FTT) is 1 meaning one host or vSAN node can fail and NSX Manager can still be recovered on the vSAN, for example, with vSphere HA. This is possible because vSAN is using RAID 1 striping across multiple host nodes used for vSAN.

Since NSX-V is being leveraged here as a security platform, we can see in Figure 19 that installation of the NSX Manager appliance does not alter the VDS topology. NSX Manager now appears in the **vCenter Server Network** distributed port group.

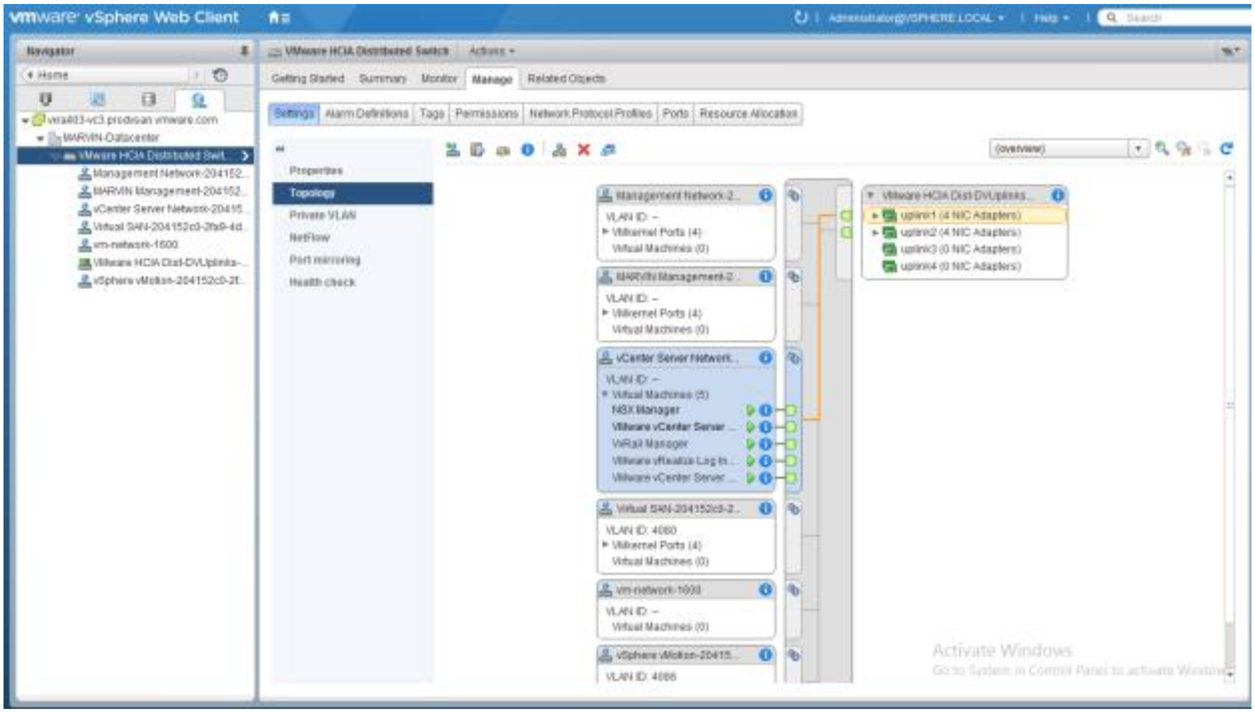


FIGURE 19: NO CHANGE TO VDS TOPOLOGY AFTER NSX MANAGER INSTALL

The NSX Manager appliance GUI can then be accessed from the respective IP address/domain name and configured.

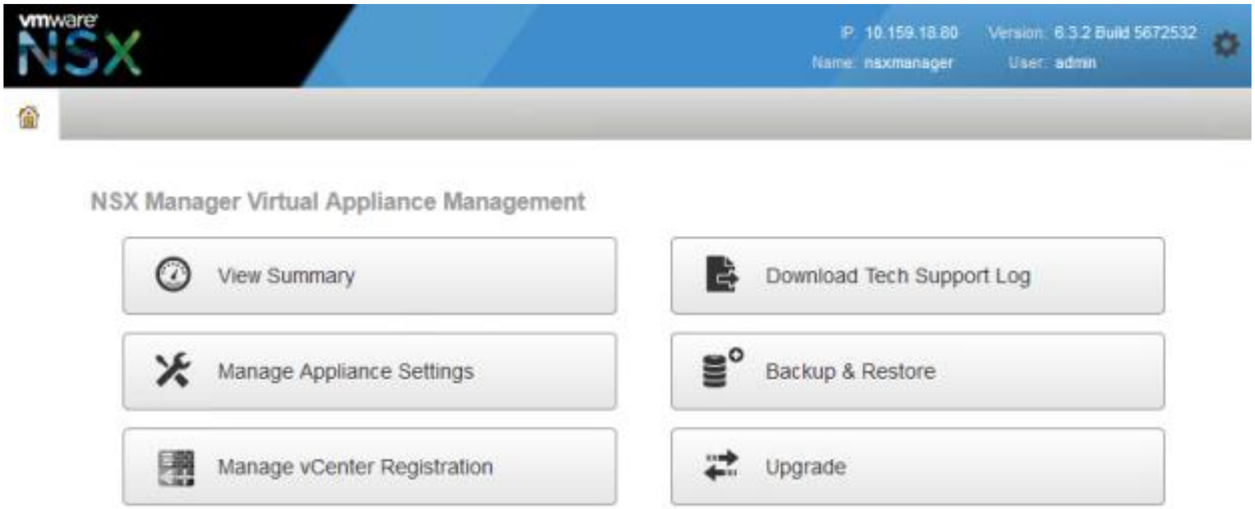
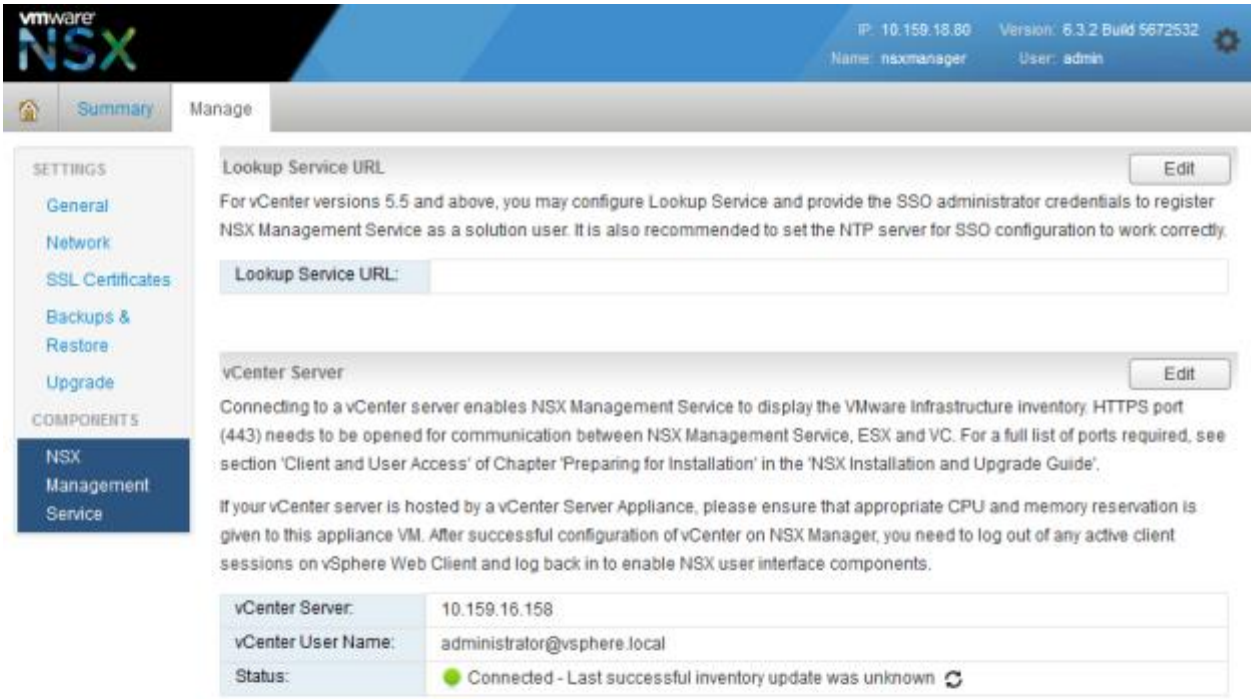

vmware NSX
IP: 10.159.18.80
Version: 6.3.2 Build 5672532
Name: nsxmanager
User: admin
NSX Manager Virtual Appliance Management
View Summary
Download Tech Support Log
Manage Appliance Settings
Backup & Restore
Manage vCenter Registration
Upgrade

FIGURE 20: VMWARE NSX MANAGER APPLIANCE GUI

The NSX Manager must next be registered with a vCenter by clicking the **Manage vCenter Registration** and providing the vCenter credentials. Once registered, the status of the vCenter Server should show as connected as shown below.



IP: 10.159.18.80 Version: 6.3.2 Build 5672532
Name: nsxmanager User: admin

Lookup Service URL

For vCenter versions 5.5 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service URL:	

vCenter Server

Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation and Upgrade Guide'.

If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.

vCenter Server:	10.159.16.158
vCenter User Name:	administrator@vsphere.local
Status:	● Connected - Last successful inventory update was unknown

FIGURE 21: REGISTERED NSX MANAGER WITH VCENTER

Once NSX Manager is registered with vCenter, the NSX Manager plugin is installed within the vSphere Web Client. A new **Networking & Security** tab is visible as shown below in Figure 22.

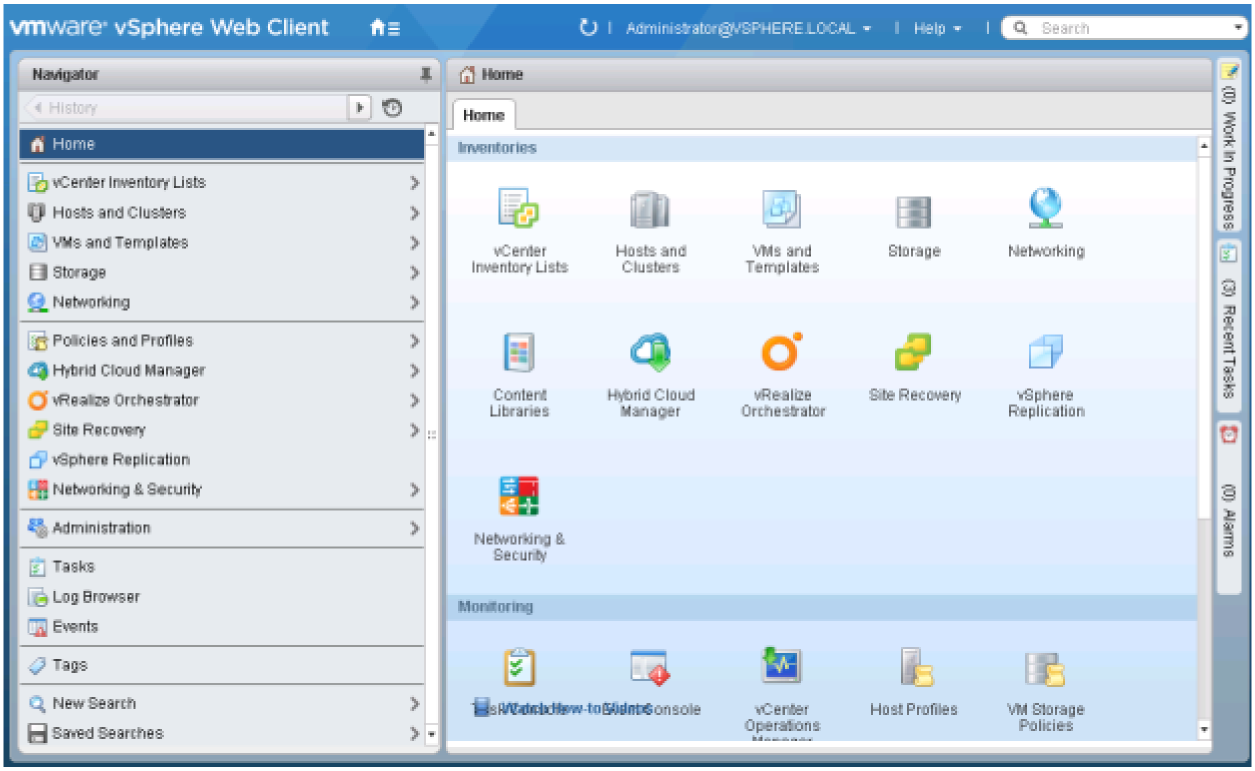
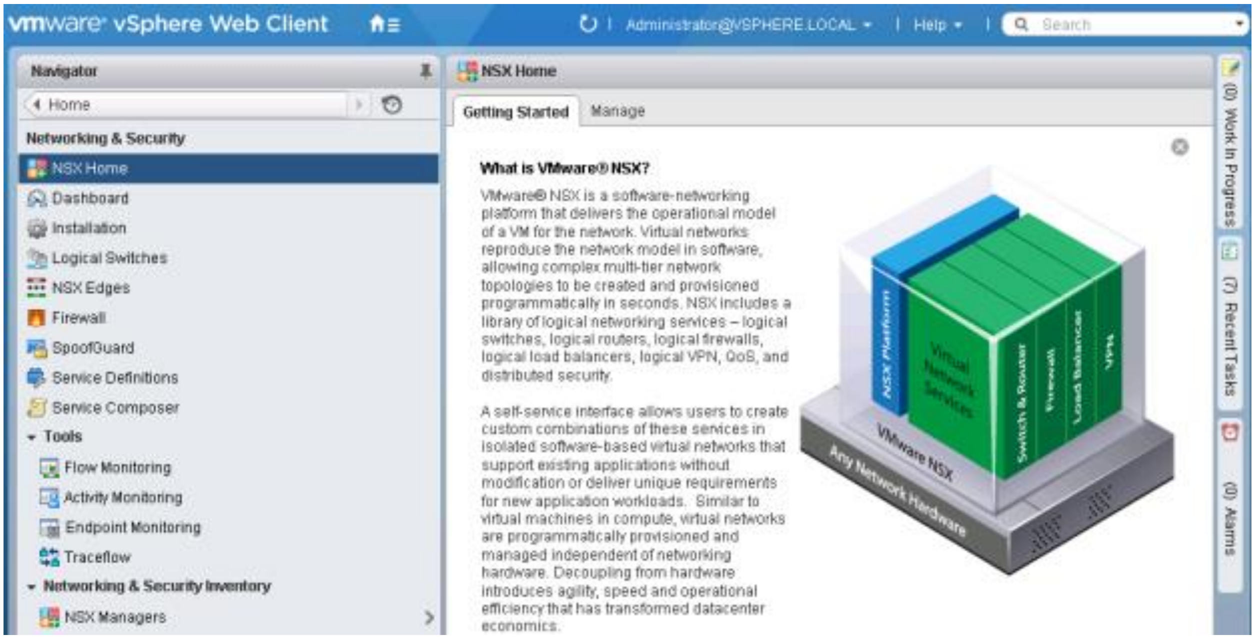


FIGURE 22: NSX MANAGER PLUGIN INSTALLED WITHIN VSPHERE WEB CLIENT

From the NSX Manager all the other NSX-V components for Logical Networking and Security are installed. Clicking the **Networking & Security** tab displays the interface of the NSX Manager plugin as shown in Figure 23 below. In this paper we are interested specifically with leveraging NSX-V security with VxRAIL, thus the tabs that are most relevant are Firewall, Service Composer and SpoofGuard.



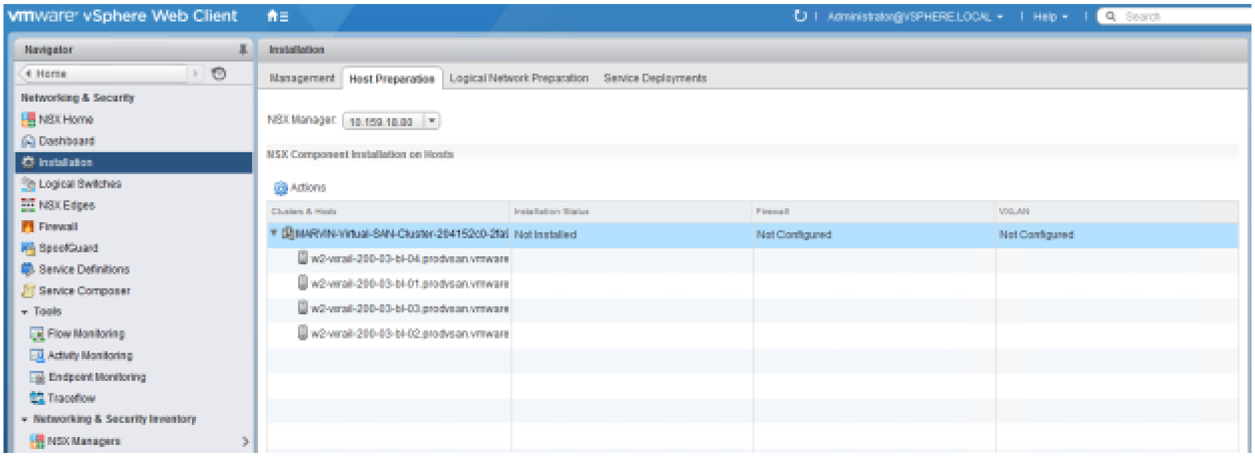
What is VMware® NSX?

VMware® NSX is a software-networking platform that delivers the operational model of a VM for the network. Virtual networks reproduce the network model in software, allowing complex multi-tier network topologies to be created and provisioned programmatically in seconds. NSX includes a library of logical networking services – logical switches, logical routers, logical firewalls, logical load balancers, logical VPN, QoS, and distributed security.

A self-service interface allows users to create custom combinations of these services in isolated software-based virtual networks that support existing applications without modification or deliver unique requirements for new application workloads. Similar to virtual machines in compute, virtual networks are programmatically provisioned and managed independent of networking hardware. Decoupling from hardware introduces agility, speed and operational efficiency that has transformed datacenter economics.

FIGURE 23: NSX MANAGER PLUGIN INTERFACE VIA VSPHERE WEB CLIENT

From the installation tab, under host preparation, it can be seen that none of the NSX-V components are initially installed as shown in Figure 24.



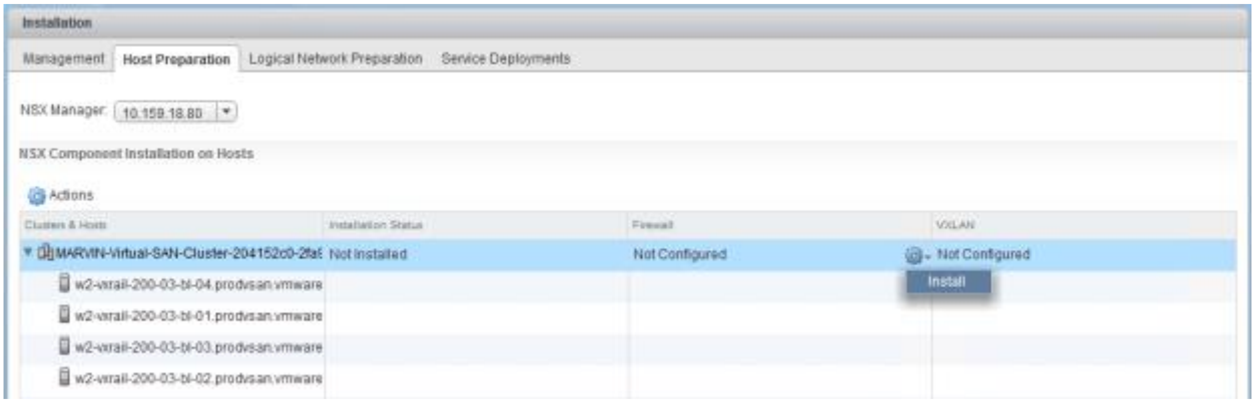
NSX Manager: 10.159.18.80

NSX Component Installation on Hosts

Clusters & Hosts	Installation Status	Firewall	VXLAN
MARVIN-Virtual-SAN-Cluster-204152c0-2fa	Not Installed	Not Configured	Not Configured
w2-vxrail-200-03-bl-04.prodvsan.vmware			
w2-vxrail-200-03-bl-01.prodvsan.vmware			
w2-vxrail-200-03-bl-03.prodvsan.vmware			
w2-vxrail-200-03-bl-02.prodvsan.vmware			

FIGURE 24: NO NSX-V COMPONENTS INITIALLY INSTALLED

Since the VxRAIL configuration used involves only one VxRAIL Cluster, we can select Install on the cluster for **Firewall** as shown in Figure 25. This installs the NSX-V DFW VIBs within the kernel module on every ESXi host in the cluster. Note, NSX-V components are installed at a cluster level.

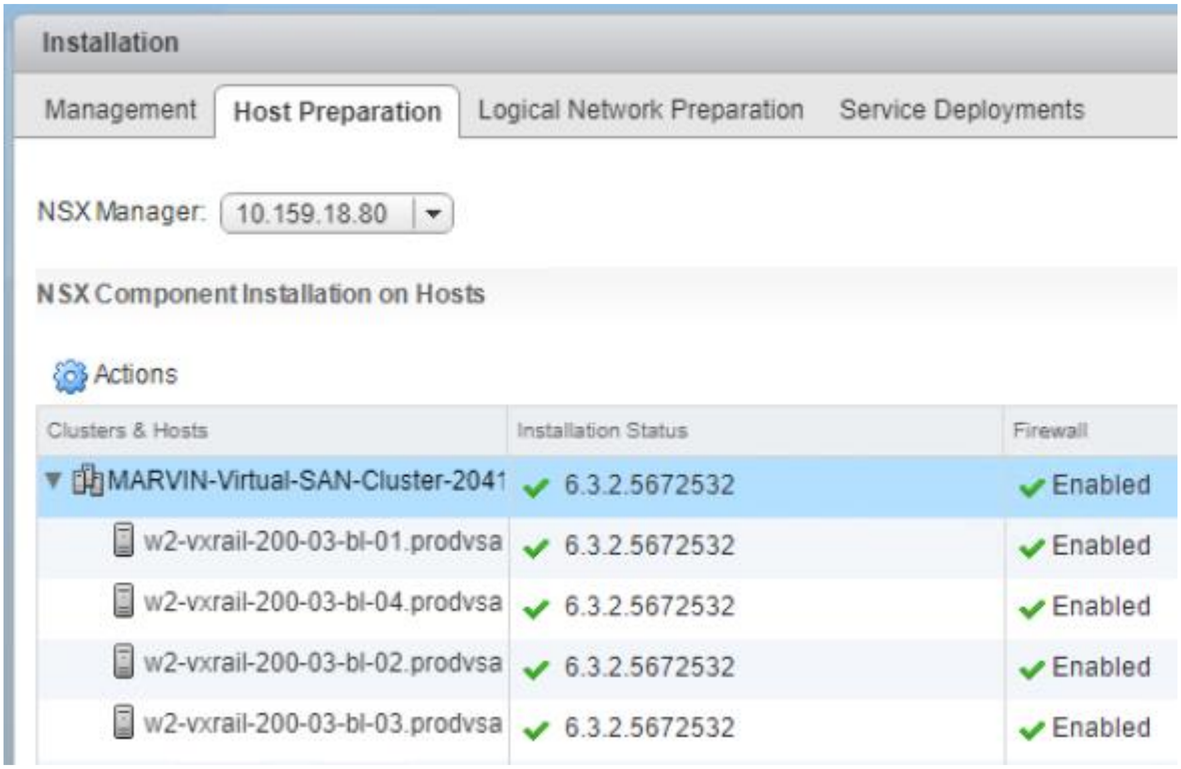


NSX Manager: 10.159.18.80

Clusters & Hosts	Installation Status	Firewall	VXLAN
MARVIN-Virtual-SAN-Cluster-204152c0-2fa8	Not Installed	Not Configured	Not Configured
w2-vxrail-200-03-bl-04.prodvsan.vmware			
w2-vxrail-200-03-bl-01.prodvsan.vmware			
w2-vxrail-200-03-bl-03.prodvsan.vmware			
w2-vxrail-200-03-bl-02.prodvsan.vmware			

FIGURE 25: INSTALLING NSX-V DFW VIBS ON CLUSTER

Once the NSX-V Firewall VIBs are installed, the status in NSX-V under **Installation->Host Preparation** should show as successful as shown below in Figure 26. The **Firewall** column should show **Enabled** for each of the four server nodes.

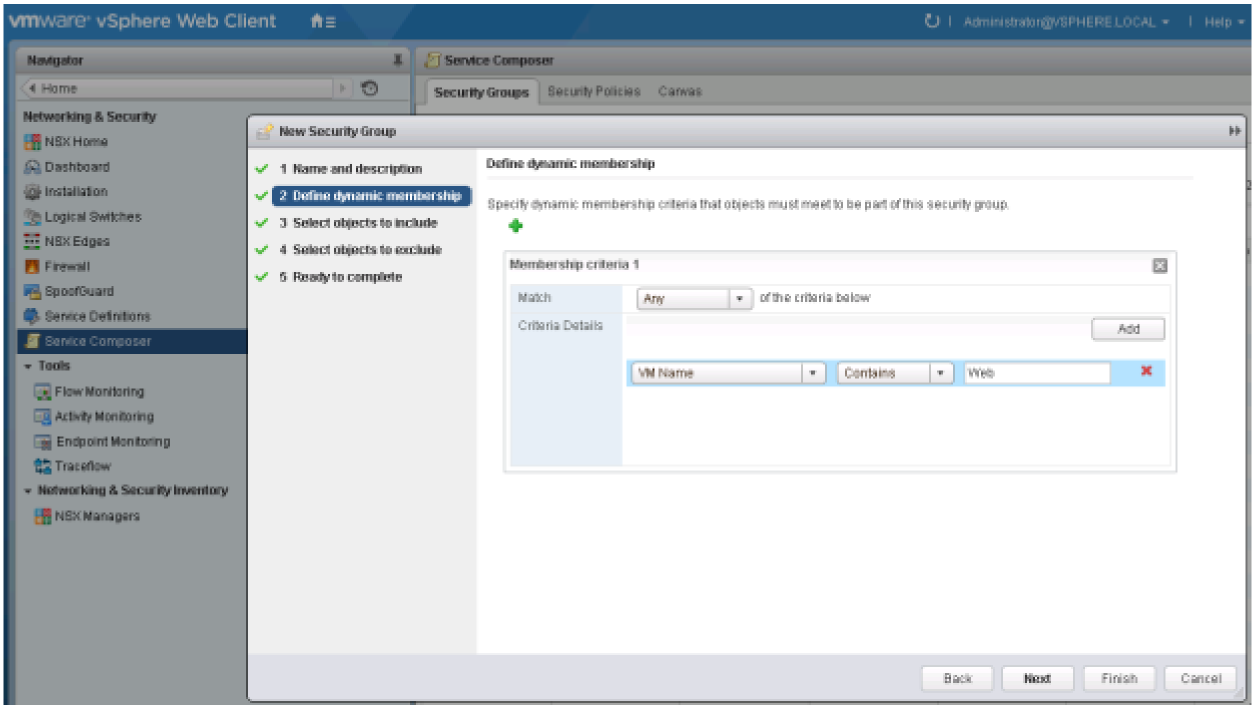


NSX Manager: 10.159.18.80

Clusters & Hosts	Installation Status	Firewall
MARVIN-Virtual-SAN-Cluster-2041	✓ 6.3.2.5672532	✓ Enabled
w2-vxrail-200-03-bl-01.prodvsa	✓ 6.3.2.5672532	✓ Enabled
w2-vxrail-200-03-bl-04.prodvsa	✓ 6.3.2.5672532	✓ Enabled
w2-vxrail-200-03-bl-02.prodvsa	✓ 6.3.2.5672532	✓ Enabled
w2-vxrail-200-03-bl-03.prodvsa	✓ 6.3.2.5672532	✓ Enabled

FIGURE 26: SUCCESSFUL HOST PREPARATION FOR NSX DFW INSTALL

Now that NSX-V security components are installed, NSX-V Security Policies can be created and applied to VMs. In the below example, two security groups called **Web** and **DB** are created as shown in Figure 27 and Figure 28. The security groups automatically identify VMs within the environment based on the matching criteria used.



1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete

Define dynamic membership

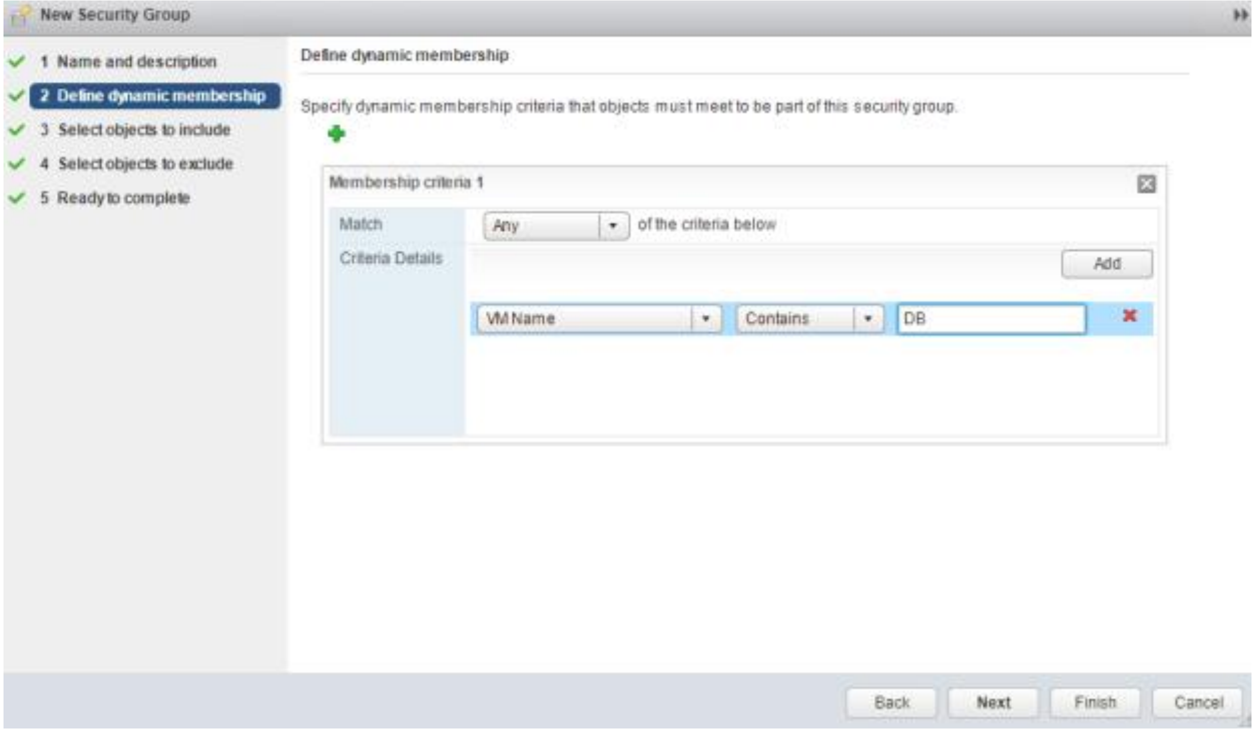
Specify dynamic membership criteria that objects must meet to be part of this security group.

Membership criteria 1

Match: Any of the criteria below

Criteria Details: VM Name | Contains | Web

FIGURE 27: CREATING A SECURITY GROUP 'WEB'



1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

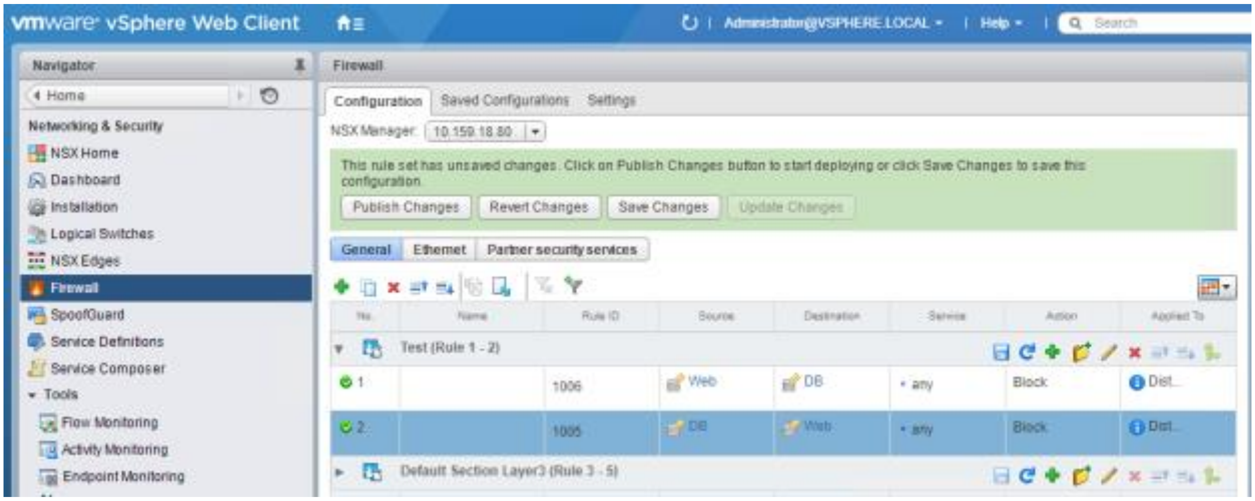
Membership criteria 1

Match: Any of the criteria below

Criteria Details: VM Name | Contains | DB

FIGURE 28: CREATING A SECURITY GROUP 'DB'

Now the security policy can be created leveraging the security groups. In the below example, the DFW tab is used to create a security policy where communication is denied between the **Web** and **DB** tiers. Clicking **Publish Changes** puts the policy into effect.



NSX Manager: 10.159.18.80

This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
Test (Rule 1 - 2)							
1		1006	Web	DB	any	Block	Dist...
2		1005	DB	Web	any	Block	Dist...
Default Section Layer3 (Rule 3 - 5)							

FIGURE 29: APPLYING SECURITY POLICY

Additional details on configuring security policies and NSX-V security capabilities are discussed in relevant use cases in the next section. For more detailed information on implementing NSX security policies, please see the VMware NSX Network Virtualization Design Guide and the latest NSX-V Administration Guide and other documents located here.

VxRAIL + NSX-V Use Cases for Security

The scope of this paper in terms of scale is 4 x VxRAIL units consisting of 4 nodes each scaling to 16 nodes; however, it is possible to scale up to 64 nodes. NSX-V scales orthogonally to VxRAIL.

There are several use cases for running NSX-V on VxRAIL. This paper focuses on the security use cases when leveraging the NSX-V platform for security within VxRAIL.

By leveraging the VMware NSX-V platform for security with NSX-V, the firewall and security policies for the application are converged and built into the appliance thus providing a truly converged appliance with security baked in as opposed to security for applications sitting externally at the perimeter on a dedicated appliance where traffic is inefficiently hair-pinned to.

I. VDI with NSX-V Providing for Enhanced Security Services

In this security use case, the organization is utilizing VDI desktops and has a need to secure the VDI nodes and back-end services being utilized; for this NSX-V DFW is utilized as shown in Figure 30 below.

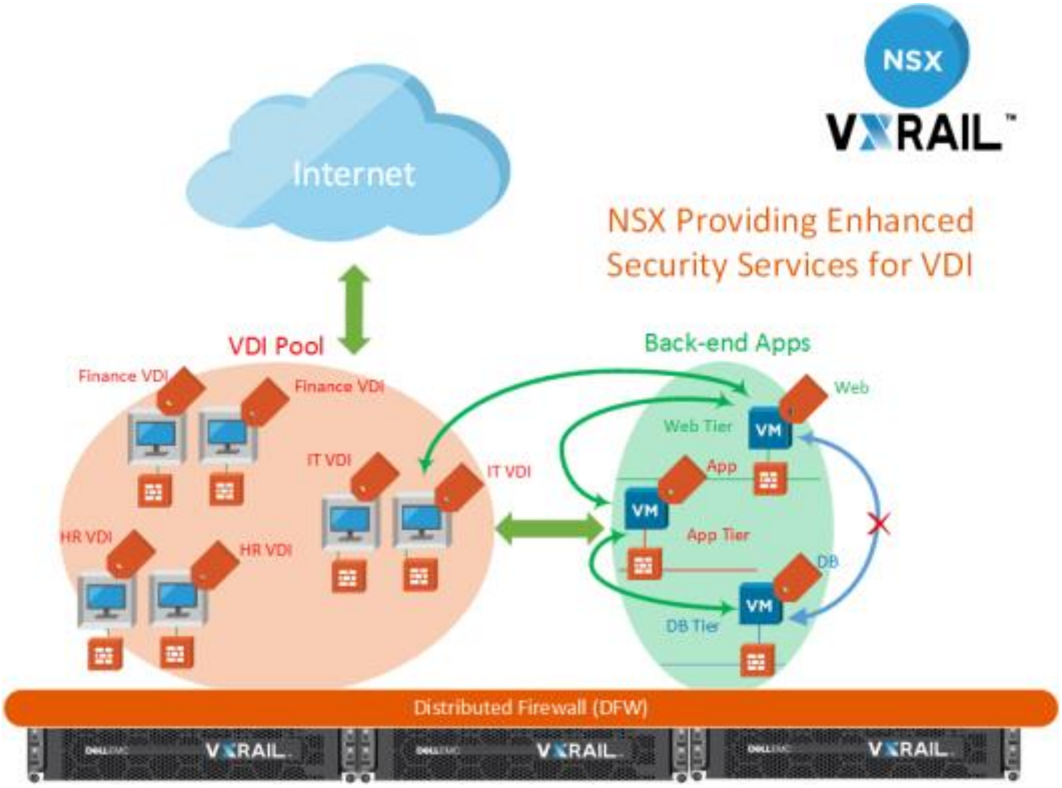


FIGURE 30: NSX-V PROVIDING SECURITY SERVICES FOR VDI WITH DFW

In the above example, the back-end apps consist of three tier applications. With the 3-tier application, it's displayed how NSX-V micro-segmentation prevents the workloads on the Web tier from communicating directly to the workloads on the DB tier; the requirement here is that the Web tier must always communicate to the DB tier through the App tier. Each of the workloads has a NSX-V security tag attached and this automatically determines the security policy assigned to the workload. There can also be policies created that prevent communication between specific applications.

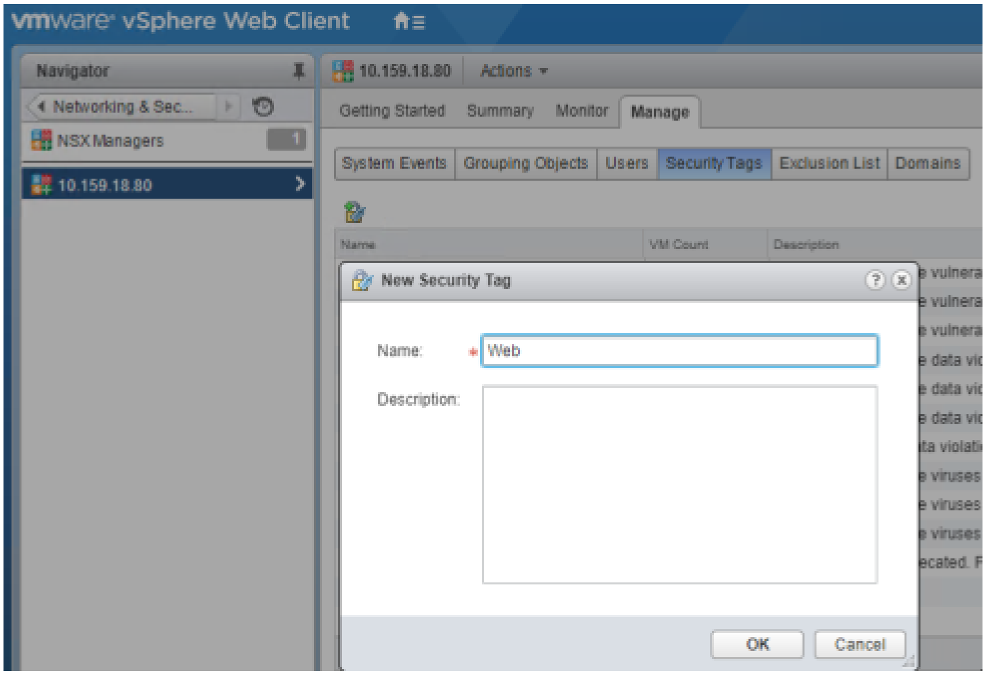
Additionally, it can be seen that there are also security policies between the VDI Pool and the back-end apps; some business units (Finance, HR, IT) may have permission to access certain apps, while other business units may not. Here, it can be seen that each business unit VDI desktop is identified with a NSX-V security tag; this security tag determines the security policy assigned to the respective desktop.

Workloads can also have multiple security tags. For example, certain VDI desktop may have a security tag of **Finance VDI** as it is a VDI desktop workload within the Finance group, but, it may also have another security tag associating it with a group that has access to additional confidential information, for example, managers within the Finance group.

With NSX-V, inherent security is part of the VxRAIL converged platform. This micro-segmentation capability within VxRAIL has several benefits:

- Security is inherent and minimizes footprint due to no virtual/physical appliance firewalls
- Security is integrated as part of the vSphere stack and managed centrally
- Enhanced security due to security policies applied at the vNIC level via micro-segmentation
- Since the security policy is applied at the vNIC level, traffic is not hair-pinned to a virtual/physical security appliance, allowing for lower application latency and efficient bandwidth usage
- By leveraging NSX-V security groups, workloads can automatically be identified dynamically and placed within the correct security posture. These security groups can then be leveraged by NSX-V security policies where the higher level constructs like VM name or security tag can be leveraged rather than just IP addresses which provide no context and are difficult to manage.

  As shown in Figure 31 and Figure 32, NSX-V security tags can be created and assigned to specific workloads to provide more context. Based on these security tags, workloads can automatically be placed in the correct security groups and assigned the correct security policies.



New Security Tag

Name: * Web

Description:

FIGURE 31: CREATING A NEW NSX-V SECURITY TAG 'WEB'

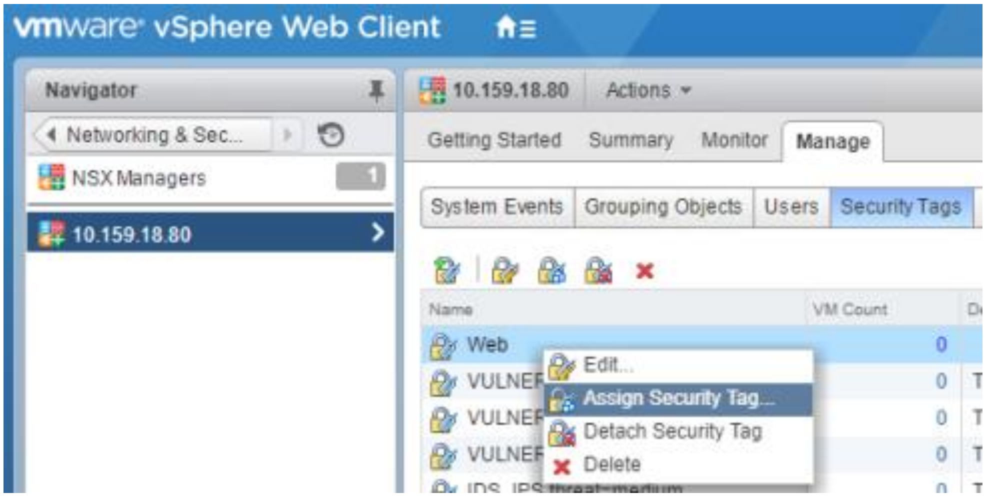
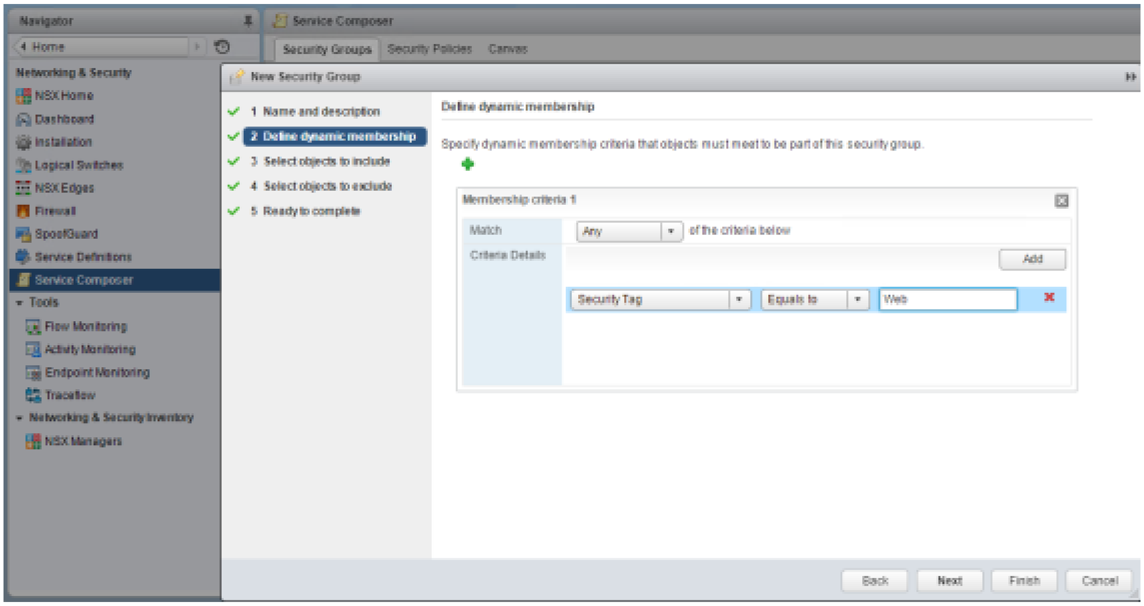


FIGURE 32: ASSIGNING THE SECURITY TAG TO A WORKLOAD

Figure 33 below shows a security group being created in NSX-V that automatically identifies VMs with the **Web** security tag.



1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

Membership criteria 1

Match: Any of the criteria below

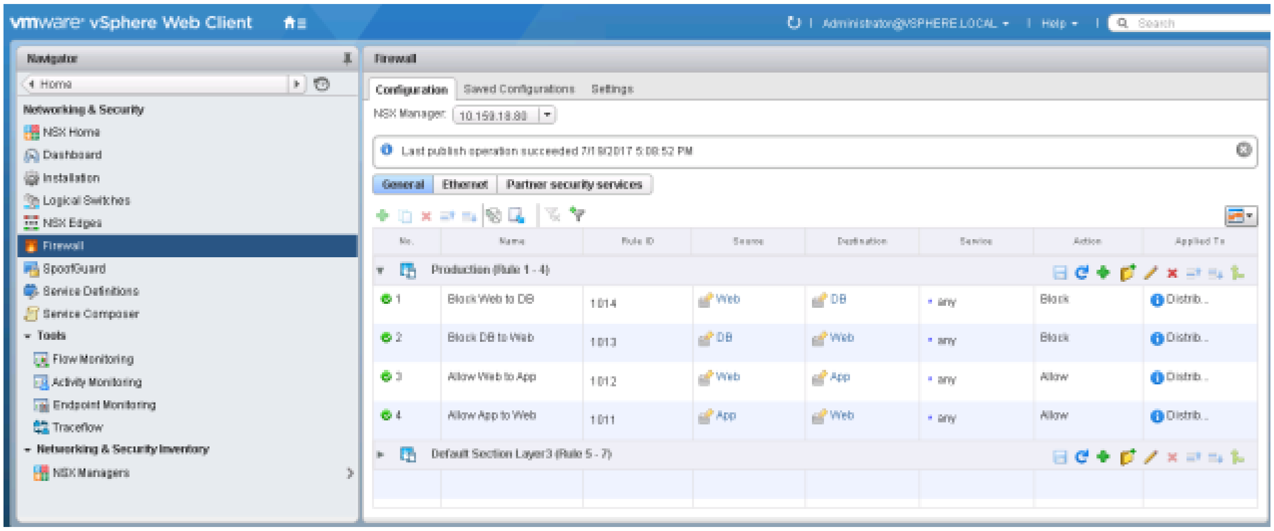
Criteria Details: Security Tag | Equals to | Web

FIGURE 33: CREATING A SECURITY GROUP THAT AUTOMATICALLY IDENTIFIES VMS WITH 'WEB' SECURITY TAG

- Security policies can be based off higher level constructs like VM name or security tag rather than just IP address used in traditional security models. IP address security polices provide no context, IP addresses for applications can easily change, and the IP-based policies are hard to maintain.

  Figure 34 below shows NSX-V DFW rules created leveraging the Web, App, and DB security groups which identify workloads based on security tags. These rules correspond to the diagram shown in Figure 30 where communication to the DB tier is only allowed through the App tier.

  The same approach can be used for identifying VDI desktops for respective business units. Respective security tags, security groups, and security policies can also be created for the different business units who consume the VDI desktops to ensure the correct security posture is applied based on respective user.



NSX Manager: 10.159.18.80

Last publish operation succeeded 7/19/2017 5:08:52 PM

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
Production (Rule 1 - 4)							
1	Block Web to DB	1014	Web	DB	any	Block	Distrib...
2	Block DB to Web	1013	DB	Web	any	Block	Distrib...
3	Allow Web to App	1012	Web	App	any	Allow	Distrib...
4	Allow App to Web	1011	App	Web	any	Allow	Distrib...
Default Section Layer3 (Rule 5 - 7)							

FIGURE 34: NSX-V DFW RULES LEVERAGING SECURITY GROUPS THAT IDENTIFY WORKLOADS VIA SECURITY TAGS

II. Micro-segmentation for Applications

In this use case, the organization has multiple applications running within a VxRAIL environment and desires to provide enhanced security to the application by further segmenting the data center/network and providing security closer to the application; this approach is called micro-segmentation and accomplished by VMware NSX-V as shown in Figure 35 below.

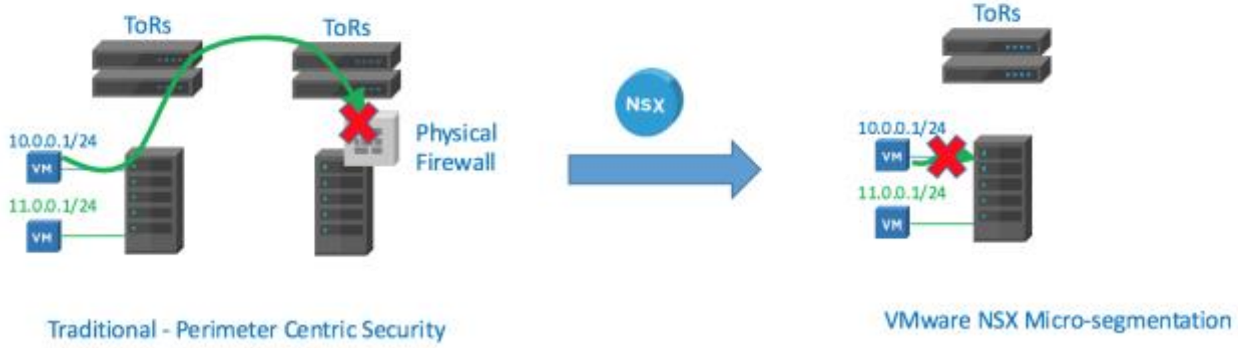


FIGURE 35: LEVERAGING VMWARE NSX-V FOR MICRO-SEGMENTATION

The diagram on the left in Figure 35 above shows the traditional security model has been to leverage a physical security appliance at the perimeter. There are two major issues to this this approach:

1.) Inefficient traffic flow and application latency

Even if workloads are sitting next to each other on the same server, traffic has to be hair-pinned to the physical firewall. In the above example, the security policy states that VMs on subnet 10.0.0.0/24 are not allowed to communicate to VMs on subnet 11.0.0.0/24. In the traditional model, the traffic has to be hair-pinned to the physical security appliance, which might be sitting on a different rack, just to be denied communication to the destination. In turn, the effect is wasted bandwidth on the network and application latency.

2.) Data Center Vulnerability - Hard Shell Soft Core

In the traditional security approach, security for the data center relies solely on the perimeter firewall. If the physical firewall is misconfigured or compromised the rest of the network is not segmented and vulnerable. Additionally, if a workload within the data center is compromised, the data center/network is not segmented in such a way to protect other workloads.

VMware NSX-V solves both of these challenges faced by traditional security models. As shown in Figure 36, VMware NSX-V provides micro-segmentation capabilities where security policies are applied at the vNIC-level of workloads. Thus, it can be seen for the same security policy where it states that VMs on subnet 10.0.0.0/24 are not allowed to communicate to VMs on subnet 11.0.0.0/24, the traffic is denied before it even hits the network. There is no hair-pinning, wasted bandwidth, or unnecessary application latency. Additionally, the application is more secure due to the security policy applied at the vNIC-level providing for additional segmentation/isolation.

VMware NSX-V leverages micro-segmentation capabilities to provide enhanced security for the applications and segment the environment. As shown below in Figure 36, NSX-V in this case provides security at the vNIC-level via distributed firewall inherently micro-segmenting the network. As such, a three tier app consisting of Web, App, and DB tiers can easily consume NSX-V security services to provide micro-segmentation and security services in-between tiers.

The example below using a 3-tier applications displays how NSX-V micro-segmentation prevents the workloads on the Web tier from communicating directly to the workloads on the DB tier; the requirement here is that the Web tier must always communicate to the DB tier through the App tier.

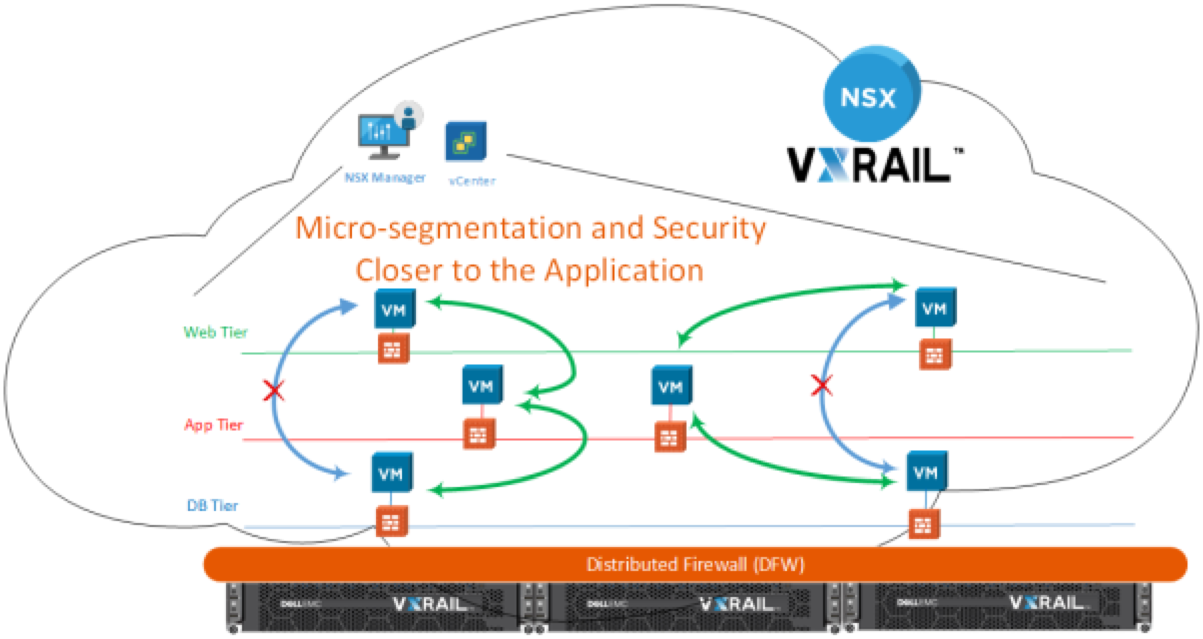

NSX
VXRAIL
NSX Manager
vCenter
Micro-segmentation and Security
Closer to the Application
Web Tier
App Tier
DB Tier
VM
Distributed Firewall (DFW)
DELL EMC
VXRAIL

FIGURE 36: NSX MICRO-SEGMENTATION AND SECURITY FOR APPLICATIONS RUNNING ON VXRAIL

Similar to providing micro-segmentation and security between the different tiers of an application, security policies can be applied between applications as shown in Figure 37; in this case the NSX-V security policy prevents communication between App 1 and App 2. Whether the underlying network is L2, L3, or a combination of L2/L3 is irrelevant and abstracted away in terms of security policy application with NSX-V. The same grouping object and micro-segmentation approach is used is in the VDI use case to provide enhanced security and decrease the attack surface.

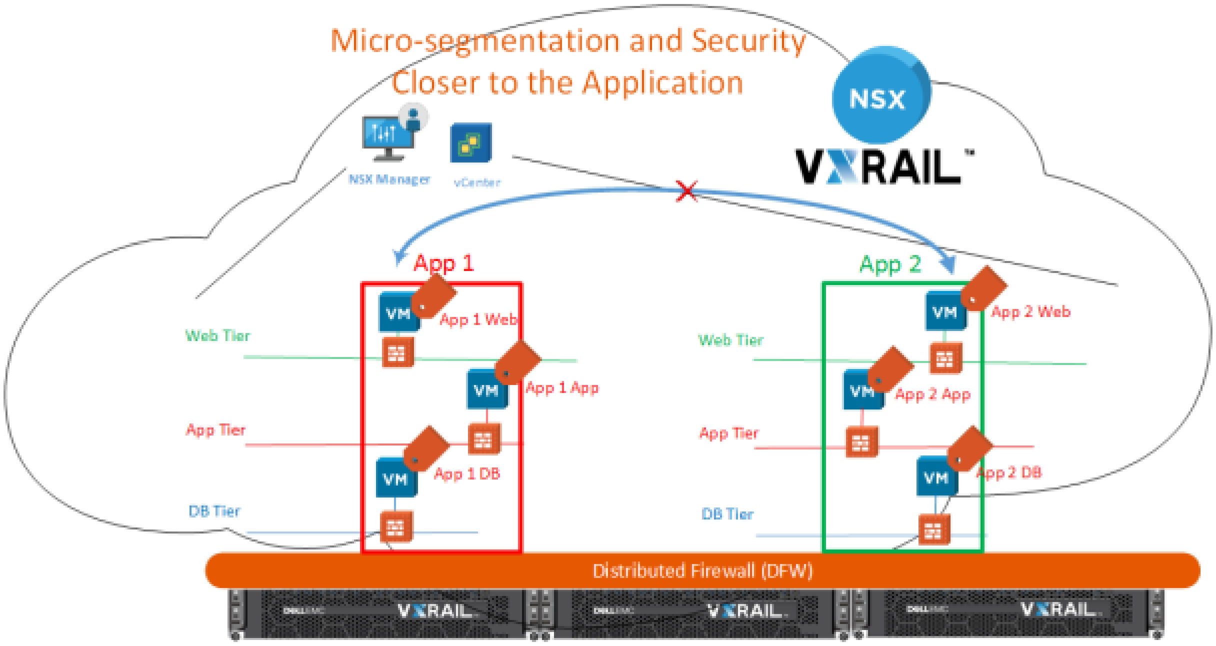


FIGURE 37: NSX-V MICRO-SEGMENTATION AND SECURITY BETWEEN APPLICATIONS

In the example in Figure 37, security tags are used to ensure the relevant security policies are applied to the correct workloads. Thus, the respective workloads each have the correct security policies applied based on, not IP addresses which can change, but higher-level constructs like security tags. Each application has an isolated environment even if on the same appliance regardless of if they are leveraging the same or different networks.

Figure 38 below, contrary to Figure 37 where the applications are on different networks, shows three applications which happen to be on the same 3-tier network but are still completely isolated from each other via NSX-V DWF rules.

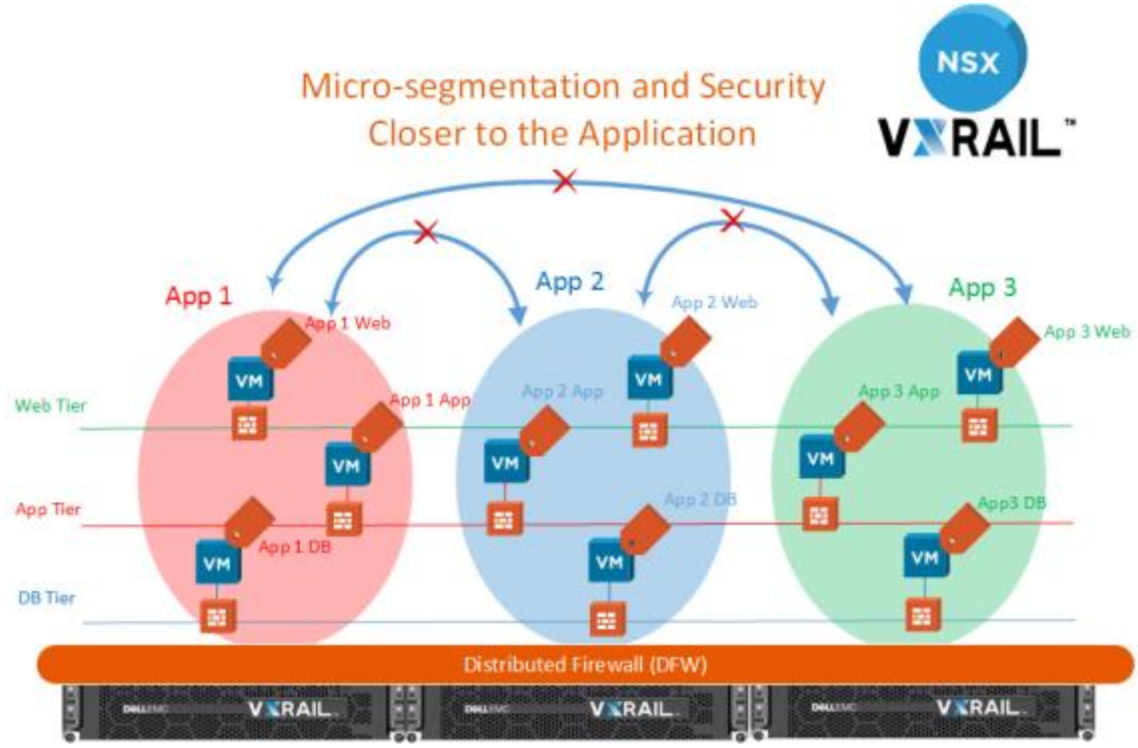
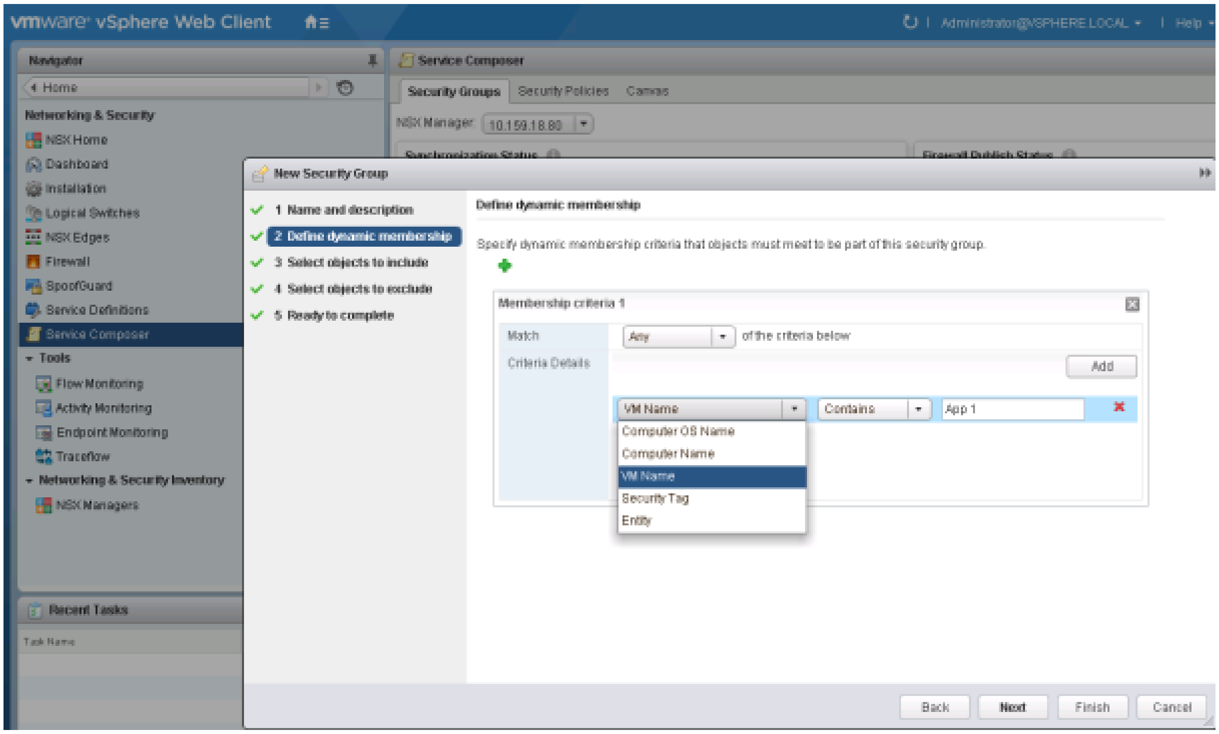


FIGURE 38: NSX-V MICRO-SEGMENTATION AND SECURITY BETWEEN APPLICATIONS

NSX-V security tags are useful as only those who are a NSX-V Administrator or NSX-V Security Admin through NSX-V role-based access control (RBAC) can change the security tag thus preventing circumventing applied security policies. However, other attributes such as Computer OS Name, Computer Name, and VM Name, can also be used along with conditions such as if a VM resides in a specific cluster or folder or is connected to a specific port group.

Figure 39 below shows a security group being created that automatically identifies workloads based on VM name. In this example, all VMs that have a name containing the words **App 1** will be placed in this security group.



NSX Manager: 10.159.18.80

New Security Group

1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

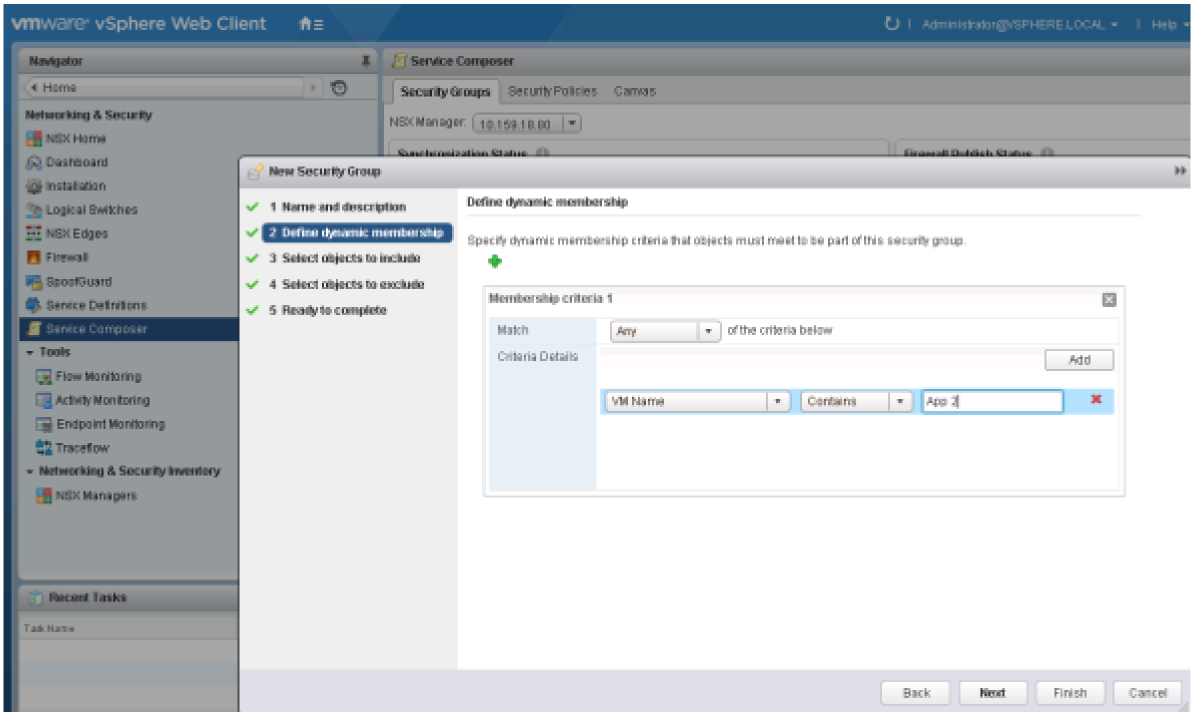
Membership criteria 1

Match: Any of the criteria below

Criteria Details: VM Name | Contains | App 1

FIGURE 39: CREATING A SECURITY GROUP THAT AUTOMATICALLY IDENTIFIES VMS WITH 'APP 1' IN VM NAME

Figure 40 below shows a security group being created that automatically identifies all VMs that have a name containing the words **App 2**.



New Security Group

1 Name and description
2 Define dynamic membership
3 Select objects to include
4 Select objects to exclude
5 Ready to complete

Define dynamic membership

Specify dynamic membership criteria that objects must meet to be part of this security group.

NSX Manager: 10.159.18.80

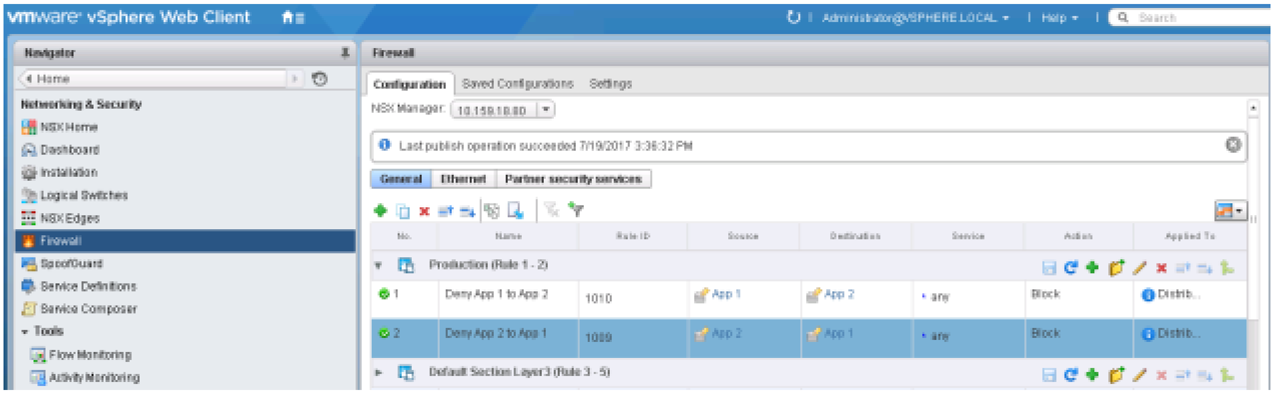
Membership criteria 1

Match: Any of the criteria below

Criteria Details: VM Name | Contains | App 2

FIGURE 40: CREATING A SECURITY GROUP THAT AUTOMATICALLY IDENTIFIES VMS WITH 'APP 2' IN VM NAME

Once the security groups are created that identify all the relevant workloads, a DFW security rule can be created leveraging the security groups as shown below in Figure 41. This example aligns with the diagram in Figure 38 where **App 1** and **App 2** are prohibited from communicating with each other.



NSX Manager: 10.159.18.80

Last publish operation succeeded 7/19/2017 3:36:32 PM

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
Production (Rule 1 - 2)							
1	Deny App 1 to App 2	1010	App 1	App 2	any	Block	Distrib...
2	Deny App 2 to App 1	1009	App 2	App 1	any	Block	Distrib...
Default Section Layer3 (Rule 3 - 5)							

FIGURE 41: CREATING A DFW RULE USING 'APP 1' AND 'APP 2' SECURITY GROUPS

III. DMZ Anywhere

In this last security use case, the organization is leveraging NSX-V to easily create a DMZ environment anywhere within the network simply by leveraging native NSX-V security capabilities.

In such a use case, NSX-V DFW segments the network. A perimeter firewall provides another layer of separation and security at the edge of the data center where traffic ingresses/egresses for both internal clients and external clients from the Internet; this is shown in Figure 42 below.

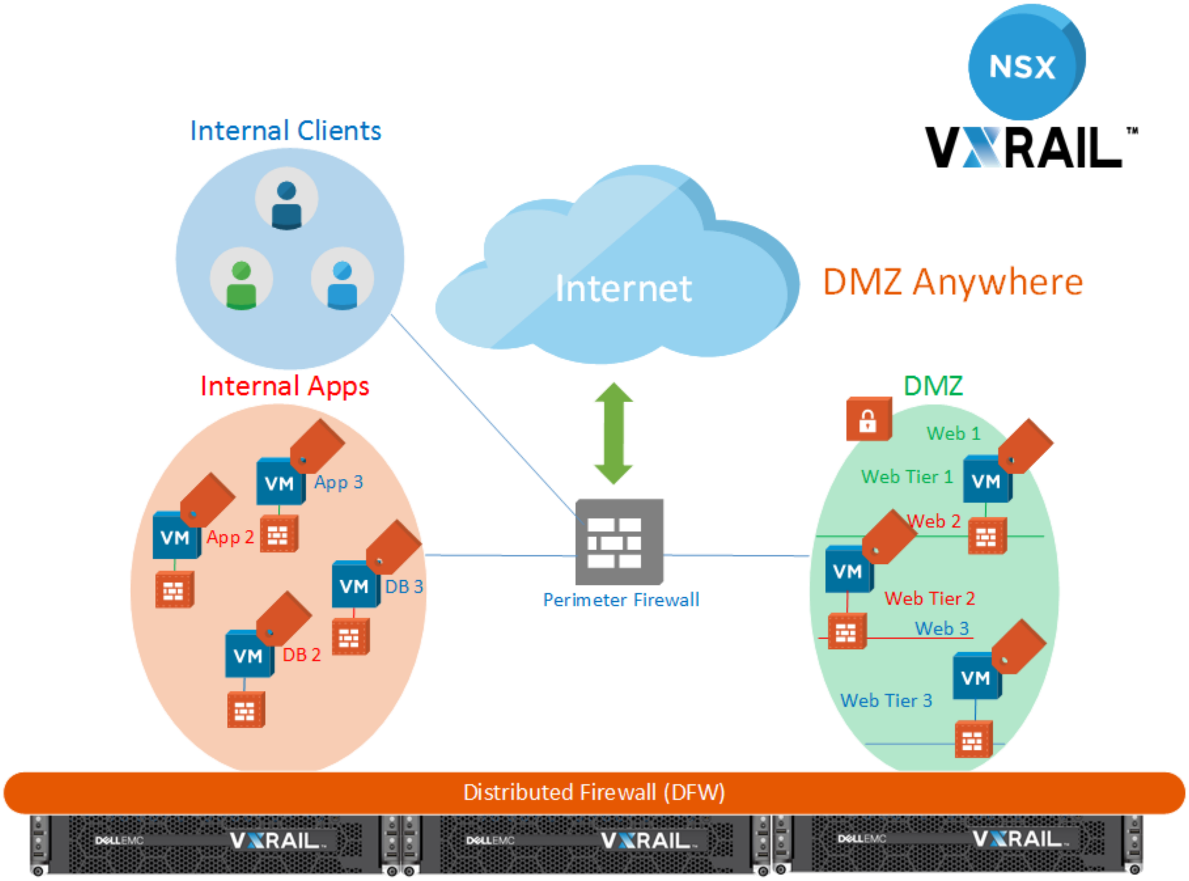
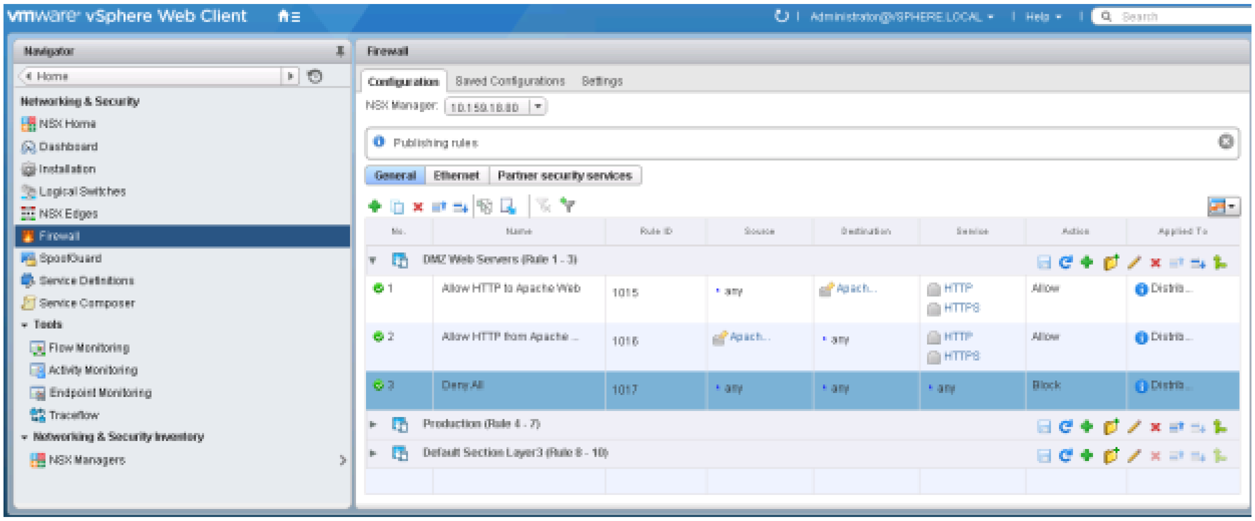


FIGURE 42: NSX-V PROVIDING A DMZ ANYWHERE ARCHITECTURE LEVERAGING NSX-V DFW

The DMZ setup in Figure 42 provides micro-segmentation and security between groupings of objects called security groups similar to prior use cases. In this use case NSX-V DFW helps create a DMZ environment by providing segmentation of the DMZ from the rest of the environment. Additionally, NSX-V DFW is being used within the DMZ to provide micro-segmentation and to employ a zero-trust model where security is tightly defined by denying/blocking all traffic/services except traffic that meets the criteria of the security policies defined.

In the example in Figure 43 below, the DFW rules prohibit all communication to and from the Apache Web servers in the DMZ except and HTTP/HTTPS. Note the **Deny Any** rule which denies any other type of traffic thus ensuring a zero trust model. When deploying a zero trust model, it's important to ensure communication to and from vCenter is not blocked; this can be done either by creating an exception excluding vCenter from DFW policies, or, more preferred, by allowing only specific types of required traffic to vCenter. The Secure Configuration of NSX-V guide provides more detail on securing NSX-V and relevant types of traffic and associated ports that should be allowed to communicate. The Incoming and Outgoing Firewall Ports for ESXi Hosts and the Configuring vSAN Network docs provide additional information on traffic/ports associated with ESXi and vSAN that should be allowed to communicate.



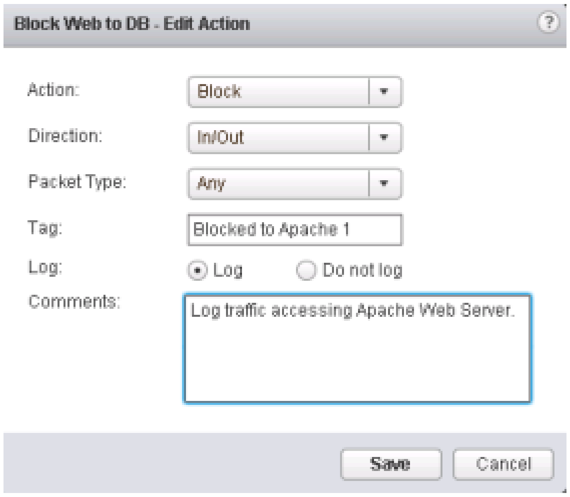
NSX Manager: 10.159.18.80

Publishing rules

No.	Name	Rule ID	Source	Destination	Service	Action	Applied To
DMZ Web Servers (Rule 1 - 3)							
1	Allow HTTP to Apache Web	1015	any	Apach...	HTTP HTTPS	Allow	Distrib...
2	Allow HTTP from Apache ...	1016	Apach...	any	HTTP HTTPS	Allow	Distrib...
3	Deny All	1017	any	any	any	Block	Distrib...
Production (Rule 4 - 7)							
Default Section Layer3 (Rule 8 - 10)							

FIGURE 43: NSX-V DFW RULES FOR DMZ

Within the **Action** column for each DFW rule, as shown in Figure 43, logging can be enabled for traffic that hits a specific rule. The log will be sent to any configured syslog server. In addition, the **Tag** field allows a specific note/description to be added to the log in addition to the details on the source, destination, and type of traffic.



Block Web to DB - Edit Action

Action: Block

Direction: In/Out

Packet Type: Any

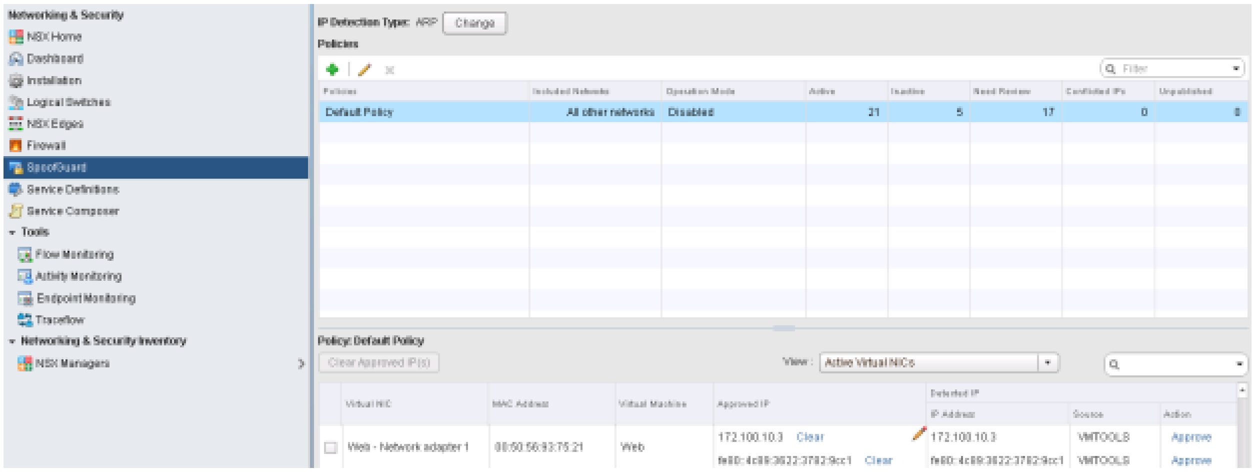
Tag: Blocked to Apache 1

Log: ● Log ○ Do not log

Comments: Log traffic accessing Apache Web Server.

FIGURE 44: LOGGING DFW RULE HITS

NSX-V also provides SpoofGuard functionality so any spoofing of workload/VM IP addresses can be detected and network access for compromised workloads/VMs blocked until manually re-enabled by an admin. These additional security features become even more important in DMZ-type environments. Figure 45 below shows the IP address detected and bound to the **Web** VM.



IP Detection Type: ARP

Policies

Policies	Included Networks	Operation Mode	Active	Inactive	Need Review	Conflicted IPs	Unpublished
Default Policy	All other networks	Disabled	21	5	17	0	0

Policy: Default Policy

	Virtual NIC	MAC Address	Virtual Machine	Approved IP	Detected IP		
					IP Address	Source	Action
□	Web - Network adapter 1	00:50:56:93:75:21	Web	172.100.10.3 Clear fe80::4c89:3622:3782:9cc1 Clear	172.100.10.3 fe80::4c89:3622:3782:9cc1	VMTOOLS VMTOOLS	Approve Approve

Figure 45: NSX-V SpoofGuard Functionality Protecting Against IP Address Spoofing

Optionally, advanced 3rd party security services with Palo Alto Networks, Check Point, etc. can be leveraged within the virtual environment leveraging the NSX-V network introspection framework as shown below in Figure 46. Alternatively, these advanced services can also be provided at the physical perimeter firewall, but leveraging the NSX-V redirection framework with integration to 3rd party security services allows for using L7 application-level security in a distributed manner similar to NSX-V DFW and also similarly follows the enhanced security model of NSX-V micro-segmentation.

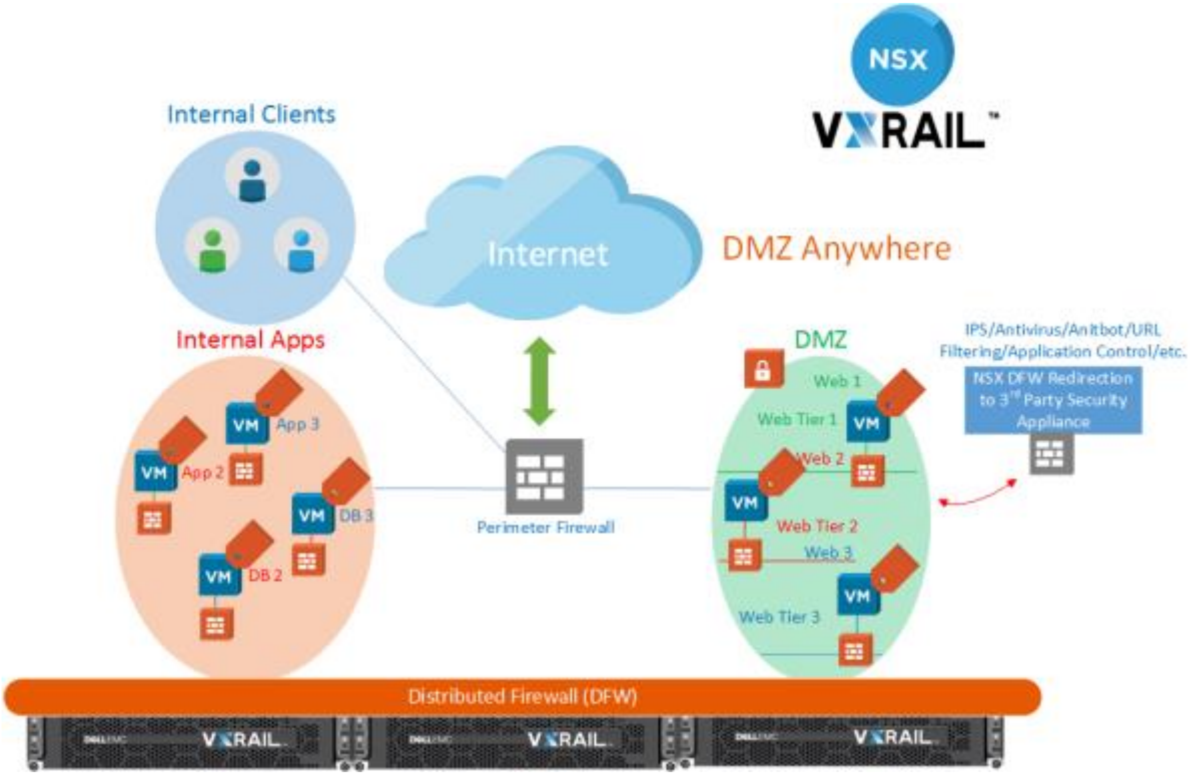
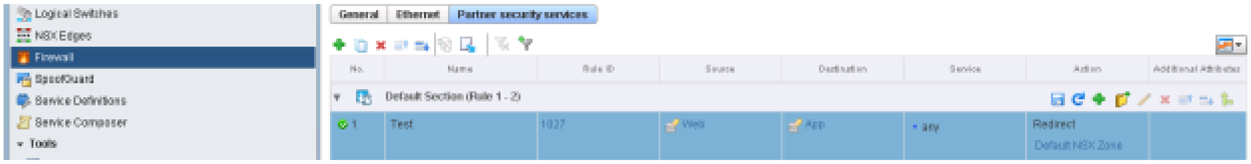


FIGURE 46: NSX-V PROVIDING A DMZ ANYWHERE ARCHITECTURE LEVERAGING NSX-V DFW AND 3RD PARTY SECURITY

In the model in Figure 46, a 3rd Party Service VM (SVM) is deployed at the vSphere cluster-level. Every host in the respective cluster has a SVM deployed on it. Based on the NSX-V redirection policy, traffic to and from the workload VM is redirected to the SVM through kernel-level modules, so traffic never hits the network. The 3rd Part Service VM is where any additional security deep packet inspection or scanning is performed.

Traffic redirection to a 3rd party can be configured either under the **Partner Security Services** tab under the DFW **Firewall** configuration section or under the **Service Composer** section. In Figure 47, traffic from workloads in the **Web** security group going to workloads in the **App** security group is being redirected to a 3rd Party Security service, in this case Palo Alto Networks VM-Series.

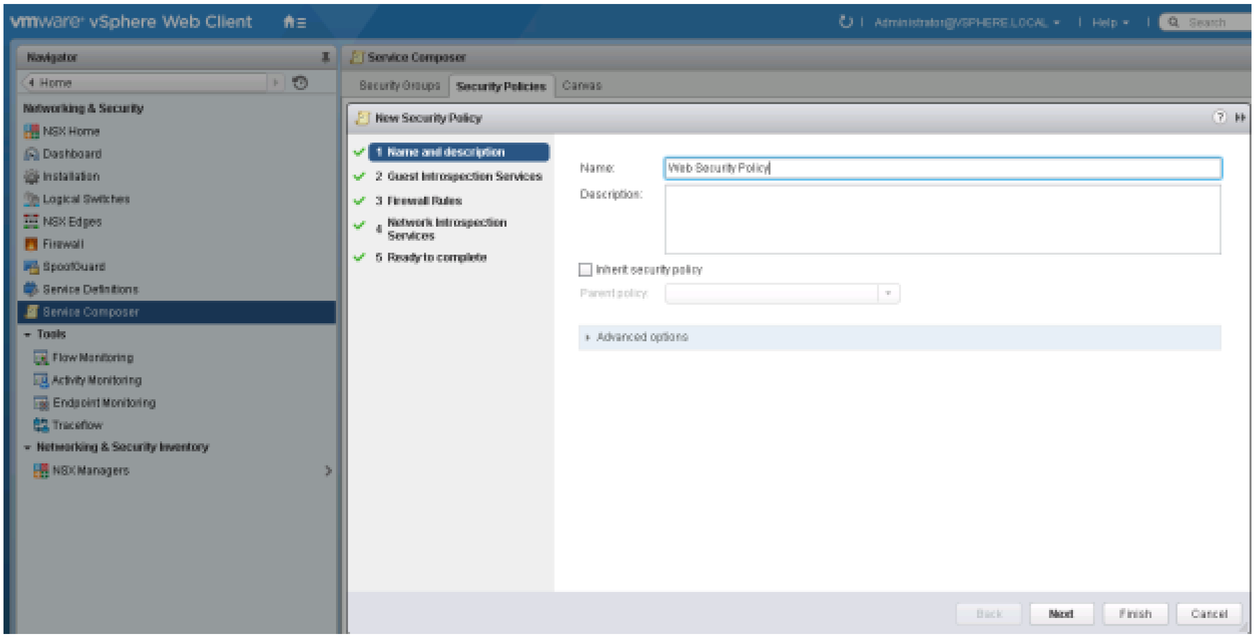


No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes
Default Section (Rule 1 - 2)							
1	Test	1027	Web	App	any	Redirect Default NSX Zone	

FIGURE 47: TRAFFIC REDIRECTION RULE

NSX-V redirection rules can also be configured under the **Service Composer** section.

NSX-V Service Composer allows advanced features such as service chaining capabilities. Figure 48 displays how from Service Composer additional 3rd party security services along with DFW can be leveraged within one security policy. In such a way, NSX-V DFW can be used for up to L4 security and a 3rd party security vendor can be used for up to L7 application-level security and advanced services like IDS/IPS, Application and URL Filtering, Anti-virus, Anti-bot, etc.



Name: Web Security Policy

FIGURE 48: SECURITY POLICY VIA SERVICE COMPOSER

Conclusion

VMware NSX-V provides an enhanced security model that aligns with the converged architecture of VxRAIL and provides for a minimal footprint, integrated security solution within the VxRAIL appliance. NSX-V provides for micro-segmentation by applying security policies at the vNIC-level of workloads and providing for a highly secure segmented data center. Additionally, NSX-V allows for use of security policies based on higher level constructs such as VM name and security tag. By leveraging NSX-V for security, VxRAIL users can easily provide micro-segmentation for applications, secure/isolate different tenant workloads, provide enhanced security for VDI deployments, and easily create DMZ environments.