# Secure VCF Management Workload Domain with VMware vDefend

Technology Product Management
ANS Division, Broadcom

Autor: Nikodim Nikodimov
October 2024

# Table of contents

# Introduction

This white paper provides technical guidance for securing the VCF Management Workload Domain, also known as the VCF Management Domain, with VMware vDefend. The document directs the steps to enable VCF architects, infrastructure, and security administrators to implement vDefend Distributed Firewall (DFW) and protect the Management domain components. It includes examples of security policies, recommendations, and implementation workflows.

VMware Cloud Foundation combines the best on-prem virtual infrastructure with the flexibility of the public cloud. It allows customers to have their own private cloud, offering scalability, rapid innovation, and cost management - features traditionally attributed to the public cloud - within their own data center's secure and controlled environment.

VMware vDefend provides defense in depth through a distributed, scale-out internal firewall that is purpose-built to protect east-west traffic. The vDefend DFW is uniquely positioned outside the guest operating system but within the host itself, allowing it to protect customer workloads in a way other solutions cannot.

Note that the formerly known VMware NSX Security Solutions was rebranded to VMware vDefend. Still, the technology and focus are on detecting and preventing advanced persistent threats with a distributed network security architecture delivered in software and embedded into the VCF infrastructure.

## Document Scope

This document is intended to outline a potential approach for safeguarding the VCF Management Domain. As such, some topics are outside the scope of this document:

- The configuration and implementation steps can vary based on multiple factors, such as network and data center design, existing physical security policies, and topology.
- The document covers a single VCF Instance deployment. Securing NSX Federated Management domain is out of scope.
- The proposed implementation depends on VCF 5.2 (NSX 4.2) or later.
- The actual DFW policy implementation may differ, as vDefend DFW offers a wide range of implementation possibilities.
- General knowledge of VCF networking, as well as of VMware vDefend concepts, is required.

This document is not intended to be a comprehensive implementation manual but to deliver general recommendations and best practices for protecting the VCF Management Domain with vDefend DFW.

## Reviewers

| Name | Role |
|---|---|
| Pooja Patel | Director, ANS Division, Broadcom |
| Stijn Vanveerdeghem | Senior Manager, ANS Division, Broadcom |

# Problem Statement

A VMware Cloud Foundation instance consists of two main building blocks: a single Management Workload Domain (WLD) and multiple Virtual Infrastructure (VI) WLDs. The Management WLD provides the resources that power VCF. It is essentially a cluster of physical hosts containing the management components VMs. This domain runs a dedicated VMware vCenter Server with vSAN storage alongside the SDDC Manager and NSX Managers. It also hosts all VI WLDs management planes: vCenter Servers and NSX Managers. The VI WLD is an individual pool of compute resources (vSphere cluster/s) to run the customers' virtual workload.

By default, the Management WLD configuration allows all inbound and outbound traffic. Any external or internal host can connect to the SDDC Manager, vCenter Servers, NSX Managers, Aria Suite, and other components that reside in the Management domain.

Nevertheless, VCF instances are usually deployed behind customers' Perimeter or DC Firewall (or both), and these FWs are configured to stop external intruders; nowadays, this is not enough. Lateral movement is a common technique by which attackers spread from an entry point to the rest of the network using various methods. For example, attackers infect

employees' desktop computers with malware and leverage techniques like remote services or exploitation of services to move laterally and get access to essential customer data and services." (ref: https://attack.mitre.org/tactics/TA0008/)

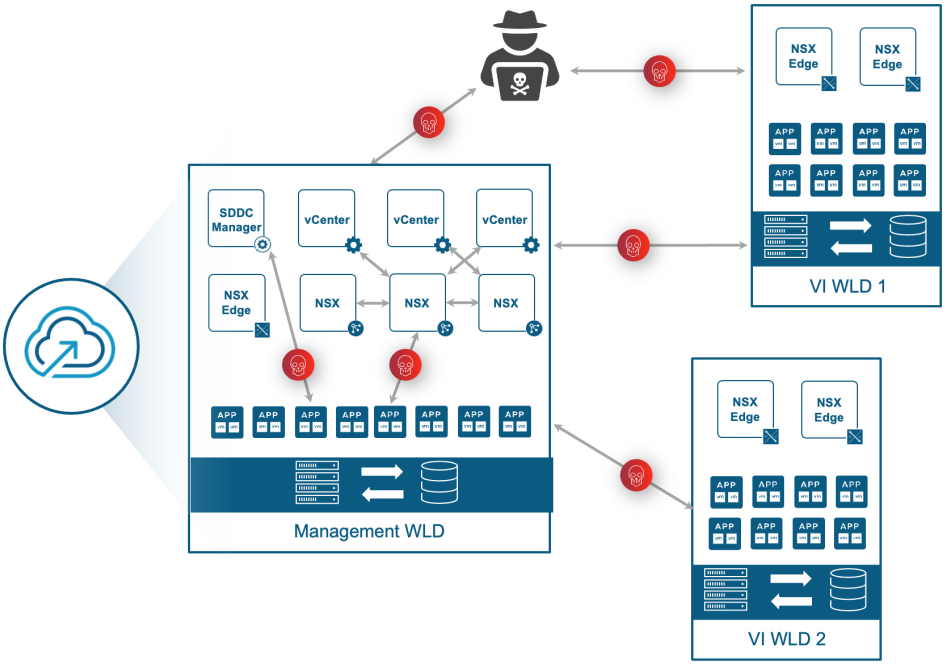


**Figure 1:** Ingress and egress traffic is permitted in the VCF Management domain, by default

The VCF private cloud workload and its management components must be equally protected at the required level to lower any potential attacker's chances of compromising the environment. It is essential to gain ultimate security for the private cloud by utilizing the zero trust approach. Traditional FW hardware or virtual appliances cannot accomplish this.

VMware vDefend provides an all-in-one security solution for zero-trust lateral security, available out-of-the-box for VMware Cloud Foundation (VCF).

## VMware Cloud Foundation Concepts Recap

The following section briefly outlines the various VCF concepts, like architecture models and components. If you are familiar with these concerns, feel free to skip it.

### Architectural Models and Workload Domains

VMware Cloud Foundation is available in two architectural frameworks: Consolidated and Standard.

The consolidated architecture design targets smaller VMware Cloud Foundation deployments and special use cases. In this model, the management components and user workload run together on a shared Management WLD. The environment is managed from a common vCenter Server and NSX Manager cluster, and vSphere resource pools are used to ensure sufficient resources for management components are in place.

In the standard architecture, management workloads run on a dedicated Management domain, and customer workloads are deployed in separate VI WLDs. Each workload domain is managed independently, which delivers better scalability and allows for autonomous licensing and life cycle management.

*Note: Although the following guidance follows the standard VCF architecture, it can be applied to the consolidated one straightforwardly.*

VCF provides flexibility for the VI WLDs deployment when using standard architecture:

- The VI WLD vCenter Server can be associated with the Management domain vCenter Single Sign-On Domain (SSO) to determine the local authentication space, joined together with vCenter Enhanced Linked Mode. Prior to VCF 5.0, this was the only option possible.

- Isolated VI WLDs were introduced in VCF 5.0. Each Isolated WLD has a distinct vCenter Single Sign-On and identity provider configuration.

## Management Components

### SDDC Manager

The SDDC Manager streamlines the complete VCF instance lifecycle, from setting up and deploying to updates and patching, installing new private cloud resources, and infrastructure modifications.

### vCenter Servers

vCenter Server is the component through which the pools of vSphere host resources are centrally managed. Each VI WLD gets its own vCenter Server, but there are variations from the perspective of the vCenter Single Sign On (SSO) as described previously.

### NSX Managers

NSX provides the foundation of the network virtualization layer for VCF, delivering software-defined networking and security controlled and managed by the NSX Manager.

- The first VI WLD requires a dedicated NSX Manager deployment (the Management WLD and VI WLDs never share an NSX instance). Any subsequent VI WLD can either use the pre-existing VI WLD NSX Manager cluster or set up a new one. A single NSX Instance can be shared across 16 VI WLDs maximum.
- Starting with VCF 5.2, NSX instance can be shared not only between VI WLDs that have their vCenter Servers in SSO with the Management WLD but also between WLDs that utilize independent SSO domains (Isolated WLDs).

### Aria Suite

VMware Aria Suite provides cloud management, monitoring, and capacity planning for the VCF private cloud. The Aria Suites comprises multiple products, each with its own management plane.

### Avi Load Balancer

Starting with VCF 5.2, the SDDC Manager can deploy and lifecycle VMware Avi Load Balancer, implementing a centrally managed distributed load balancing solution for VCF private cloud workloads.

### vSphere IaaS Control Plane

The vSphere IaaS Control Plane (previously vSphere with Tanzu) delivers Kubernetes workloads directly on ESXi hosts and also facilitates the creation of upstream Kubernetes clusters—Tanzu Kubernetes Grid (TKG). From the current white paper subject perspective, the Management domain Supervisor cluster and TKG clusters deployed on top will accommodate all individual VCF workload domains NSX Application Platform instances.

### Other Component

Other various management components might reside in the VCF Management domain, which are outside the SDDC Manager governance. For instance, VMware Cloud Service Provider products and solutions, such as VMware Cloud Director, VMware Cloud Director Availability, Usage Meter, VMware Chargeback, etc.

The vSphere IaaS Control Plane (previously vSphere with Tanzu) could be another component in the VCF Management domain to deliver Kubernetes workloads directly on ESXi hosts and to facilitate the creation of upstream Kubernetes clusters—Tanzu Kubernetes Grid (TKG). From the current white paper subject perspective, the Management domain vSphere IaaS Control Plane supervisor cluster and TKG clusters deployed on top will accommodate all individual VCF workload domains NSX Application Platform instances.

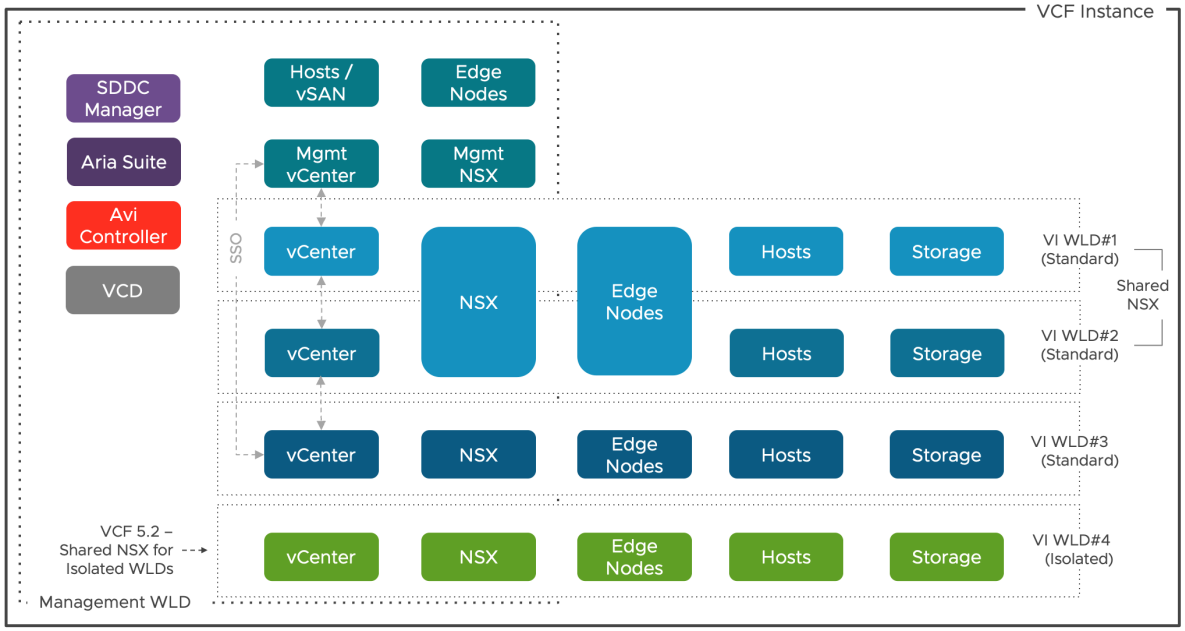


**Figure 2:** VMware Cloud Foundation components

## DFW on vSphere Distributed Port Groups

A key technology of vDefend is the Distributed Firewall (formerly known as NSX Distributed Firewall), which enables a software-defined firewall to protect VMs, physical servers, and containers.

Before VCF 5.2 (NSX 4.2), customers could not secure VCF workloads connected to vSphere VLAN distributed port groups (DVPGs) using the DFW. Despite NSX starting to support DFW on DVPGs from version 3.2, this capability was only available with the "Security Only" NSX deployment model, which was never supported in VCF.

### NSX on DVPGs

Starting with VCF 5.2, the new "NSX on DVPGs" feature provided in NSX 4.2 enables VCF customers to apply DFW security posture to any VM,  regardless of the network backing (NSX VLAN and Overlay segments and vSphere DVPGs).

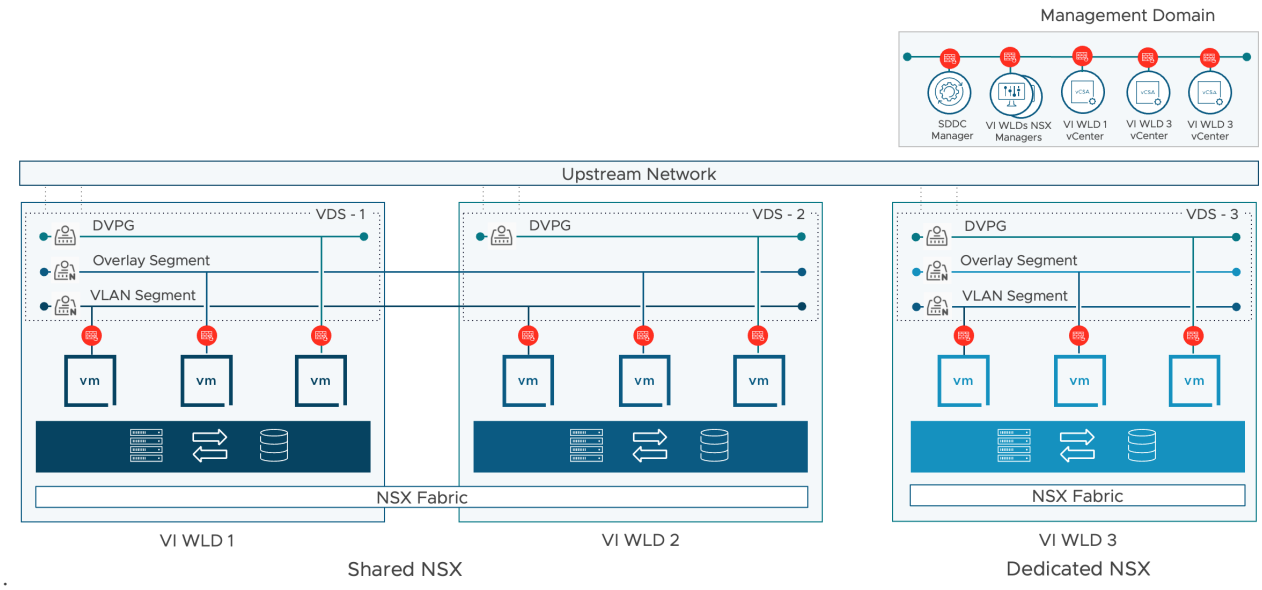


**Figure 3:** vDefend distributed security for any network attachment type

The new NSX and vDefend capability simplifies VCF customers' security journey. It allows them to enforce security without the need for workload migration from vSphere virtual distributed switch (VDS) networking backing to NSX segments. Additionally, this offers a straightforward, built into the platform approach of securing the VCF management components (SDDC Manager, vCenter Servers, NSX Managers, etc.) connected to DVPGs.

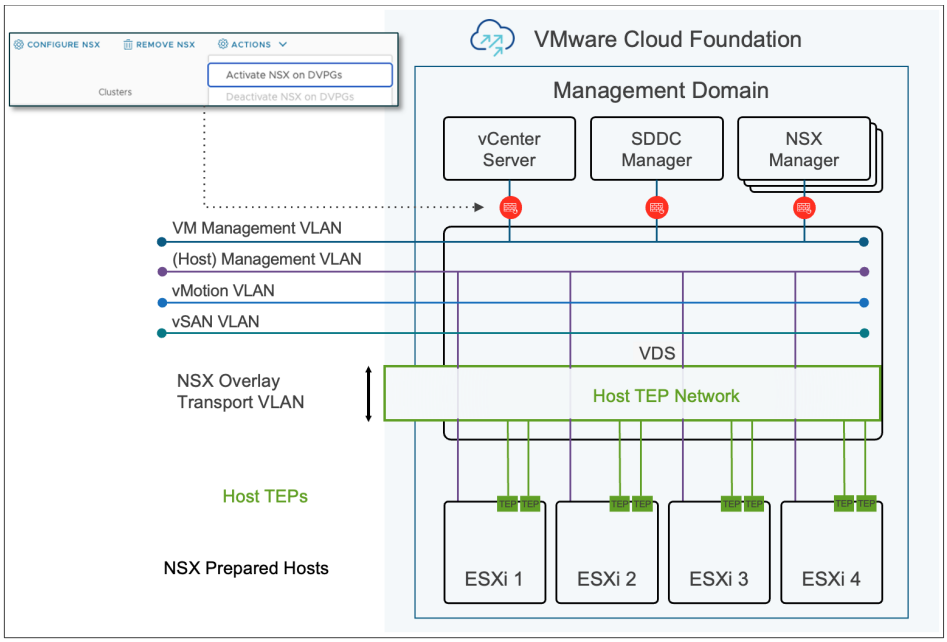


**Figure 4:** VCF 5.2 - DFW support for the VCF Management components

## Considerations & Recommendations

There are several important factors to consider when utilizing NSX on DVPGs to ensure a successful configuration and smooth operations:

- The feature default state for greenfield deployments or upgrades to NSX 4.2.0 is "disabled." For post 4.2.0 upgrades it will be based on the previous state.
- To enable the feature, vSphere Distributed Switch v7.0.3 or later version is required.
- NSX on DVPG is activated per vSphere cluster but only affects the NSX-prepared cluster VDSs. Only the NSX-prepared VDSs carry the system-generated VLAN Transport Zone to manage the DVPGs.
- Before enabling the feature, the vSphere cluster had to be prepared for NSX (VLAN TZ, Overlay TZ, or both).
- VCF bring-up process: If a multiple-VDS profile is being used, the VDS that handles the Management traffic has to be configured for VLAN TZ preparation. Otherwise, a Host Switch will not be created for this VDS in the Transport Node Profile, used to bootstrap the cluster for NSX, and must be done manually afterward.
- NSX on DVPGs can be activated or deactivated at any time, with no disruption to existing workloads, which is adequately addressed by existing DFW policy.
- After activation of the feature, the discovered vSphere DVPGs will have the default Security, IP Discovery, and Spoof Guard segment profiles applied.
- Any existing DFW policy immediately affects the DVPGs' connected workload after activation. Consider DFW policy verification before enabling it, to not block required traffic.
- Out of the box, VCF places the SDDC Manager, vCenter Servers, and NSX Managers in the DFW User Excluded Group. To enforce DFW, remove the required VMs from the group, except the Management domain NSX Managers.

- The Management domain NSX Edges are placed in the system-excluded VMs list, which is not editable. Although DFW cannot be applied to the management vNIC on these VMs, they have to be considered when building the policy to handle their management traffic properly.

## Securing the VCF Management Workload Domain

### Segmentation Strategy

Segmenting the data center infrastructure into macro-security zones is the first step of the zero-trust approach. This provides a quick way to deliver traffic controls and prevents lateral movement between individual zones and access to critical data. Using this security architectural technique, we have to partition the VCF infrastructure into distinct, logical groups with similar security requirements.

VCF is built to provide flexible lifecycle management of the customer's private cloud by employing the concepts of separated Management and VI workload domains. Usually, the first criteria when developing a segmentation model is to align with the natural boundaries of the data center virtual infrastructure, which in our use case are the individual VCF workload domains. Each VCF workload domain can be easily selected as an independent top-level security zone.

To guarantee the complete protection of the Management WLD, additional low-level security zones must be defined according to the functional characteristics of the VCF management components and the different access needs of other VCF elements.

For example:

- SDDC Zone - common VCF instance management components, like
  - SDDC Manager
  - Aria Suite products
  - Avi Controllers
  - VMware Cloud Director
- vCenter Zone - vCenter Servers within a Single-Sign-On (SSO)
- Infrastructure Zone – common infrastructure services like DNS Servers, AD Servers, NTP Servers, Backup Servers, etc.
- Bastion Zone – JumpHost Servers
- Tools Zone – automation and any additional operation and management tools

The general principle to follow is that whenever there is a logical division of functionality, application usage, or user access privileges, a separate zone can be created to isolate and protect that area. This will allow VCF Management domain delivery with appropriate security policies to prevent unnecessary access to data and applications that only specific services require.

In addition, it is important to understand how the different VCF management components, such as SDDC Manager, vCenter Server and NSX Manager, and data plane ones, like ESXi Hosts, Storage, and NSX Edge Nodes, are placed from the perspective of the Management domain NSX Manager, where we will build the DFW security policies.

This is essential for the design of the DFW policy concerning two fundamental items:

- The DFW will be enforced only on VMs that reside on the Management WLD.
- What kind of NSX mechanism can be used for grouping - Tags, VM Names, DVPGs etc., or only IP Sets.

The following diagram depicts the various VCF common components and their corresponding zones, which will be utilized to architect the distributed firewall policies in this guide.

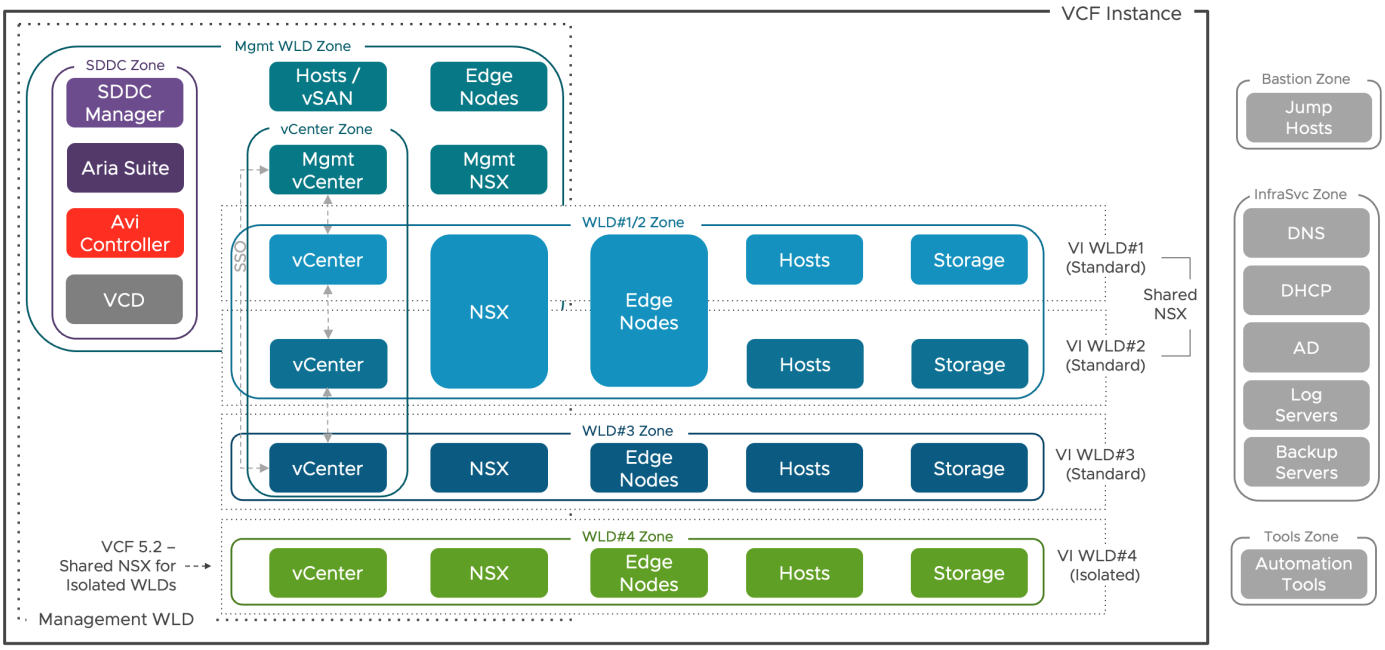


**Figure 5:** Management WLD Security – Macro-segmentation Planning

The diagram also incorporates essential components for any private cloud, such as Infrastructure Services (DNS, NTP, AD, DHCP, etc.), Bastion Hosts, and Automation Tools. These elements, though, are shown outside of the VCF instance; they can also be deployed as VMs, part of the Management WLD. This is an important consideration when constructing the vDefend grouping and policy strategy.

Usually, as a Day-2 operation, a higher level of protection and control within each of the above-defined security zones should be established to allow only the necessary traffic per WLD's vCenter, NSX Managers, Hosts, and NSX Edge Nodes. The security policy can be deepened, and its granularity can be increased (zero-trust) based on DFW logs or by employing VMware vDefend Security Intelligence (formerly NSX Intelligence). Later in this document, we provide an example of how we can utilize Security Intelligence for policy verification and deliver a micro-segmentation.

## Workload Grouping

vDefend provides multiple options for grouping the workload target to be secured. We can use various criteria for the VCF Management components (VMs) with static and dynamic membership. However, these management components manage vSphere infrastructures (VI WLDs), which are not part of the Management domain NSX fabric. These individual VI WLD elements can be grouped only by using their IP addresses.

Groping options:

- Management WLD components - VMs, VM Names, NSX Tags, DVPGs, DVPG Ports, NSX Segments, Groups, with dynamic or static membership
- Hosts, IP-based Storage, NSX Edge Node—static membership with IP Sets. Note that object-based grouping criteria, such as VM Name, Tags, VIFs, etc., for the Management domain Edge Nodes, will not work either; they must be grouped using their management IPs.

The grouping and criteria types usually depend on the granularity of the security policy and rules set, the size and dynamicity of the virtual environment to protect, and whether automation will be used to deliver the policy.

VCF currently uses a single VM Management network for all workload domains, meaning that all management components will get connected to the same vSphere distributed port group and will receive IPs from the same CIDR block. If there is no plan to deliver granular, per WLD security, using the VM Management DVPG or the management subnet with static membership will be an appropriate mechanism for grouping.

After the initial deployment of the VI WLDs, the VCF Management domain is a relatively static environment. So, using static membership based on the VM or DVPG port will also be a suitable and quick groping mechanism.

However, if the VCF instance is more dynamic, for example, in the Cloud Service Provider area, where it might be shared between multiple tenants, a dynamic group membership using NSX Tags or VM Names (contain/equal/starts/not-equals with the string as part of their name) would be a better choice.

The same applies if an automation tool is planned to deliver the grouping and security policy, where Tags should be the most appropriate and flexible option for membership.

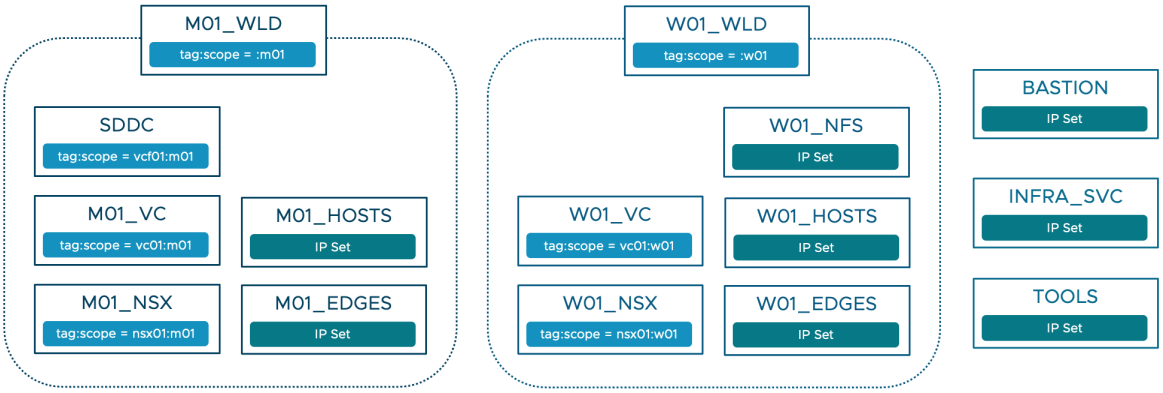


**Figure 6:** VCF Workload Grouping

## Policy Model Considerations

The Management domain traffic is prescriptive for the components installed and lifecycle managed by VCF. The policy design will depend on the level of isolation and protection required. Following the top-down approach, we have to design a macro-segmentation policy to allow the ensuing communication:

- Allow Bastion hosts to the VCF instance
- Allow traffic to Infrastructure Services (DNS, DHCP, NTP, AD, Backup etc.)
- Allow SDDC Manager to vCenters, NSX Managers, Edge Nodes, Avi Controllers, Hosts, and IP-based Storage
- Allow vCenters to vCenters Linked Mode (if used)
- Allow common VCF management tools (Aria, Avi, VCD) to respective WLD components
- Allow traffic within WLD
- Block traffic between different WLDs, if necessary
- Allow VCF management components egress (Internets, Corporate backbone, etc.) traffic if necessary

The below tables provide the security policy structure split into DFW Infrastructure and Environment categories according to our segmentation model.

| Infrastructure Category | | | | | | |
|---|---|---|---|---|---|---|
| **Name** | **Source** | **Destination** | **Service** | **Context Profile** | **Applied To** | **Action / Logging** |
| **VCF Infrastructure Policy** | **Applied: MGMT_WLD; VI_WLD(…)** | | | | | |
| Allow Bastion Zone to VCF | BASTION | MGMT_WLD<br>VI_WLD(…) | Any | None | DFW | Allow |
| Allow VCF to InfraSvc | MGMT_WLD<br>VI_WLD(…) | INFRA_SVC | DNS-TCP<br>DNS-UDP<br>DHCP, DHCPv6 | None | DFW | Allow |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | NTP<br>Syslog (TCP/UDP)<br>SSH<br>ICMP | | | |
| Allow LDAP | MGMT_WLD<br>VI_WLD(…)<br>INFRA_SVC | MGMT_WLD<br>VI_WLD(…)<br>INFRA_SVC | | LDAP | DFW | Allow |
| Allow AD | MGMT_WLD<br>VI_WLD(…)<br>INFRA_SVC | MGMT_WLD<br>VI_WLD(…)<br>INFRA_SVC | | ACTIVDIR | DFW | Allow |
| Allow Backup Traffic | MGMT_WLD<br>VI_WLD(…) | BACKUP_SERVERS | ICMP<br>HTTPS | None | DFW | Allow |
| Allow 3rd Automation and Management Tools | TOOLS | MGMT_WLD<br>VI_WLD(…) | HTTPS<br>SSH<br>ICMP | None | DFW | Allow |

Building a security policy is usually a multi-step, iterative process. The VCF Management domain comprises of multiple components that communicate with one another using various protocols and ports. Because of that, a good approach is to start safely with a "Default Allow" rule with logging enabled and observe if the default rule matches any traffic that should be allowed, and you might have been missed in the policy rules above.

When confident with the policy, the default rule action should be changed to Drop. Logging might be kept for some time to ease the troubleshooting for any unforeseen problem.

| Environment Category | | | | | | |
|---|---|---|---|---|---|---|
| **Name** | **Source** | **Destination** | **Service** | **Context Profile** | **Applied To** | **Action / Logging** |
| **VCF Environment Policy** | **Applied: MGMT_WLD; VI_WLD(…)** | | | | | |
| Allow VCF Management | SDDC | MGMT_WLD<br>VI_WLD(…) | ICMP<br>HTTPS<br>SSH<br>TCP-5480 | None | DFW | Allow |
| Allow vCenter ELM | MGMT_VC<br>VI_WLD(…)_VC<br>SDDC_MGR | MGMT_VC<br>VI_WLD(…)_VC<br>SDDC_MGR | HTTPS<br>LDAP<br>LDAP-over-SSL<br>TCP- 2012,2020 | None | DFW | Allow |
| Allow Mgmt WLD to itself | MGMT_WLD | MGMT_WLD | Any | None | DFW | Allow |
| Allow WLD to Itself (rule per WLD) | VI_WLD(…) | VI_WLD(…) | Any | None | DFW | Allow |
| Block traffic between WLDs (if needed) | MGMT_WLD<br>VI_WLD(…) | MGMT_WLD<br>VI_WLD(…) | Any | None | DFW | Drop / Log |
| Allow VCF Outbound | MGMT_WLD<br>VI_WLD(…) | Any | HTTPS | TLS 1.2<br>TLS 1.3 | DFW | Allow |
| VCF Default Deny Any | Any | Any | Any | None | DFW | Drop / Log |

*Note:*

1. *For simplicity, the policies are applied to the top-level zone groups (MGMT_ WLD and VI_ WLD(…)), which also include child IP-based groups (Hosts, NSX Edges, and IP Storage).*
2. *The required protocols and communication ports can be found at https://ports.esp.vmware.com/*

## Implementation Workflow

This section provides a quick guide on the essential configuration tasks VCF administrators should execute to set up vDefend DFW to secure the Management WLD.

Please note that the actual implementation and security policy will differ in your environment and depend on the individual data center and VCF architecture specifics and components.

### Management Domain Initial State

Before starting with the implementation, please confirm that the VCF Management WLD and its components are in a healthy state.

Additionally, on the Management domain NSX Manager, we should confirm:

- Out of the box, the VCF Management components (SDDC Manager, vCenters, NSX Managers, etc.) are placed in the DFW User Excluded Group.
- For brownfield environments with existing DFW rules set, we must verify that the policy will not block traffic to any additional VMs connected to DVPGs that reside on the Management WLD.
- Additional VMs can be placed in the DFW User Excluded Groups to leave nothing to chance.

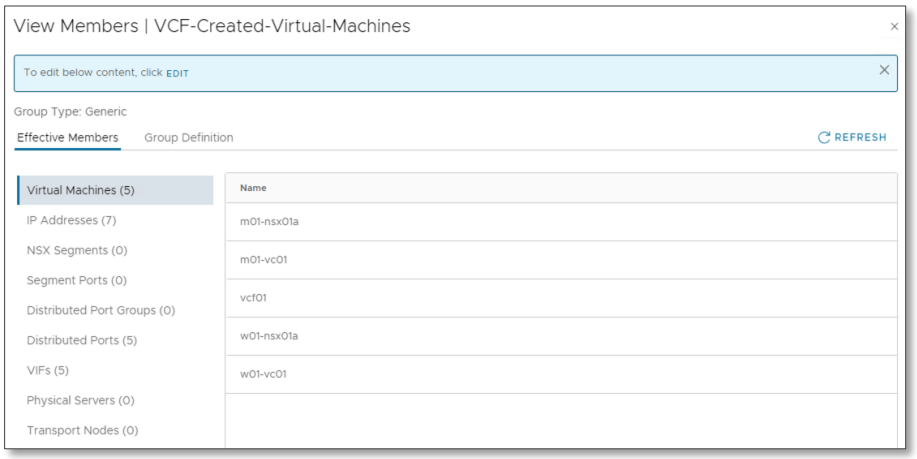


**Figure 7:** Management domain NSX – User Excluded Group

As mentioned above, NSX on DVPGs is inactive by default. This can be verified from the NSX UI by navigating to **System > Fabric > Hosts**. Note that in a brownfield environment, the VCF Management domain might have multiple clusters.

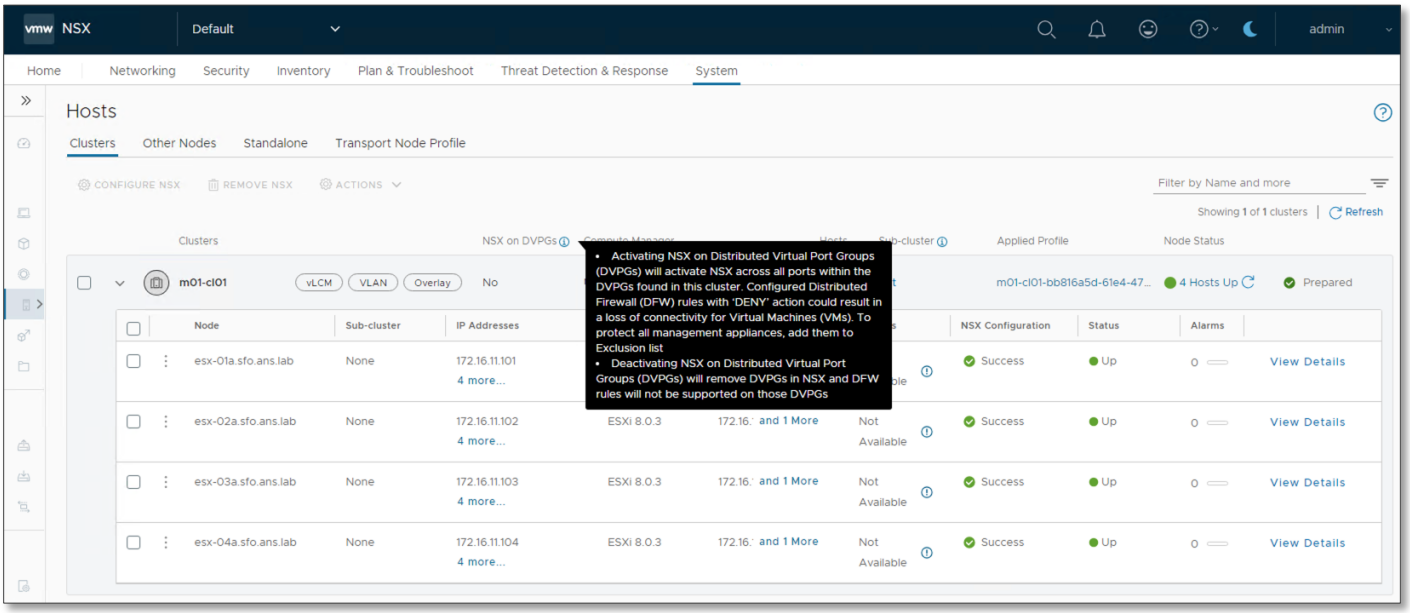


**Figure 8:** NSX on DVPGs is disabled by default

Additional verification for the current DFW state can be done on the Management domain Hosts where the respective VMs reside. To access the list of DFW rules, first, we need to find the name of the *dvfilter* used on the VM's network adapter using the ***summarize-dvfilter*** command. We can use the less pager and regex (***summarize-dvfilter|grep -A2 <VM name>***) to filter the output for the target *dvfilter* name. The information from the output is the name of the filter driver on slot 2 of the vNic, where the distributed firewall is placed.

With the command ***vsipioctl getrules -f <filter-name>***, we list the effective firewall rules for the vNic.

When NSX on DVPGs is disabled, the rules output should be completely empty for any VMs connected to vSphere DVPGs.

```
[root@esx-04a:~] summarize-dvfilter|grep -A2 vcf01
world 2211767 vmm0:vcf01 vcUuid:'50 00 d7 37 5b ac 5d 9d-f8 72 09 a5 2e d0 f4 fe'
 port 67108891 vcf01.eth0
  vNic slot 2
    name: nic-2211767-eth0-vmware-sfw.2
[root@esx-04a:~]
[root@esx-04a:~] vsipioctl getrules -f nic-2211767-eth0-vmware-sfw.2
No root rule set.
[root@esx-04a:~]
```

**Figure 9:** Example for SDDC Manager vNic dvfilter – NSX on DVPGs is disabled by default

## Enable NSX on DVPGs

Enabling the feature is straightforward: we select the target cluster and, from the Actions drop-down menu, choose the **Activate NSX on DVPGs** option.

The system will display a confirmation pop-up informing us that this will activate NSX across all ports within the DVPGs in this cluster. It will also warn us that the existence of DFW rules with 'DENY' action could result in a loss of connectivity for VMs.

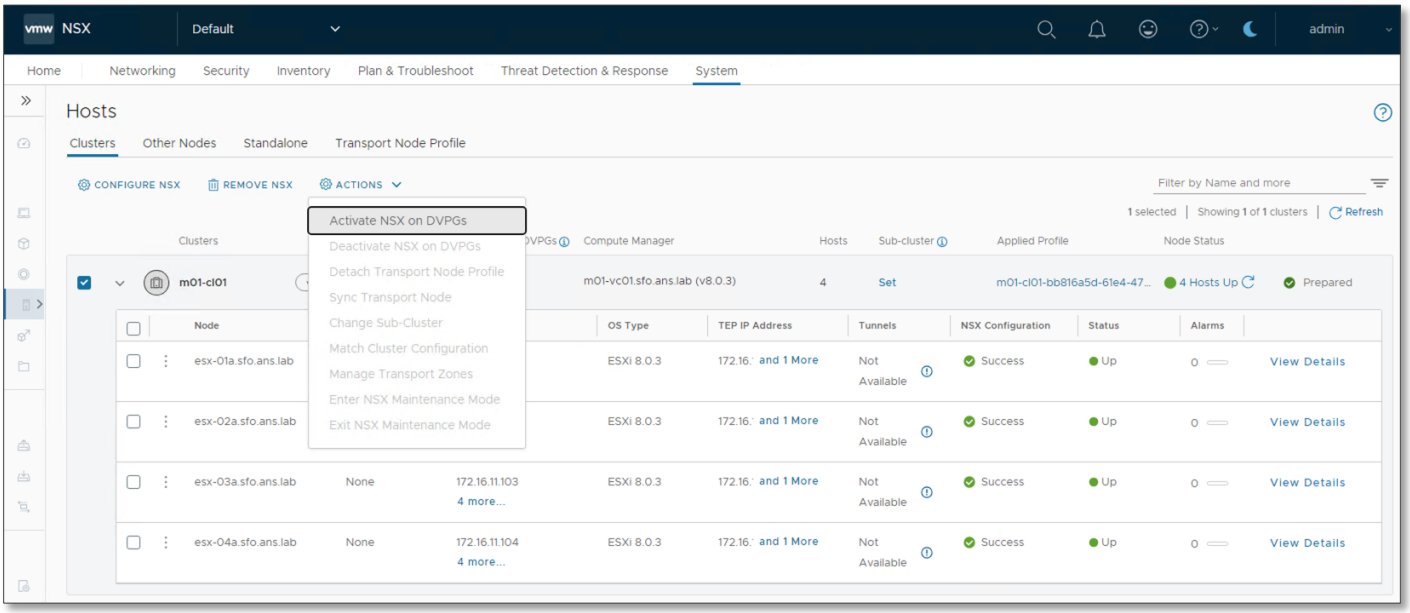


**Figure 10:** Activate NSX on DVPGs

## Post-activation Verification

The NSX Manager will reconfigure the cluster hosts, enabling the feature. For each VDS prepared for NSX, a unique, system-created VLAN Transport Zone (*nsx.vlan-tz.security.<UUID>.<VDS name>)* is enabled to handle the DVPGs and their ports.

As mentioned above, the VDS conducting the VCF Management traffic has to be prepared for NSX before enabling the feature. This is an important consideration for VCF bring-up, with hosts having 4 or 6 pNICs and more than one VDS configured on the Management WLD. If the VCF VM Management VLAN port group resides on a VDS, not prepared for NSX during the bring-up, this must be done manually afterward before activating NSX on DVPGs.

NSX will discover the respective VDS distributed port groups and ports only for the VDSs that have the *nsx.vlan-tz.security.<UUID>.<VDS name>* enabled.

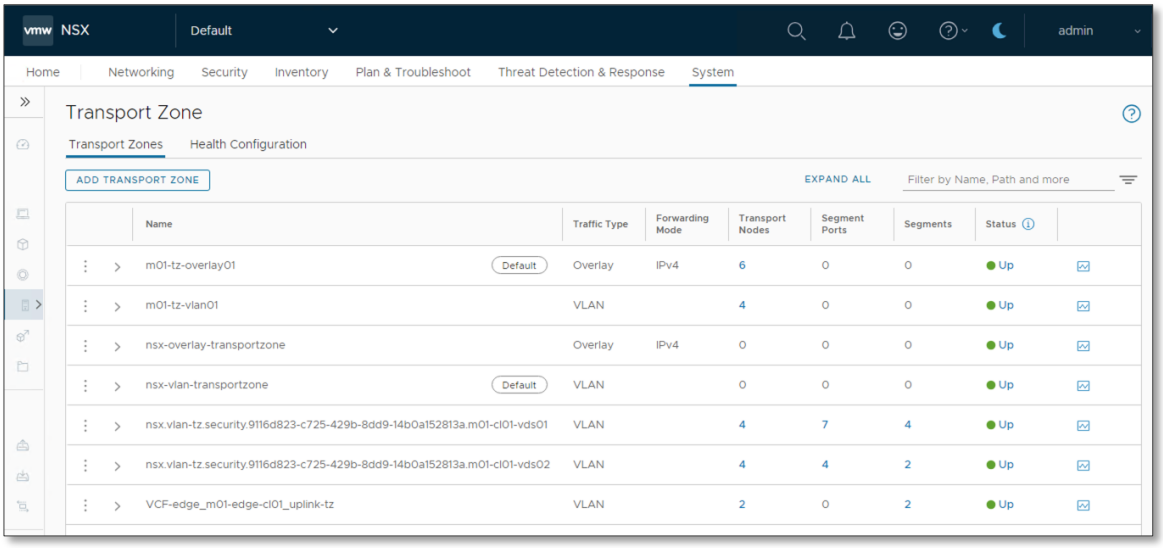


**Figure 11:** NSX System VLAN Transport Zone per VDS

The DVPGs and their ports will also be visible in the **Networking > Segments > Distributed Port Groups** UI section. Having these objects in the NSX Manager database makes it possible to create NSX grouping using DVPGs and DVPG-specific ports. They can also be tagged, and grouping can be made based on the tagging criteria.

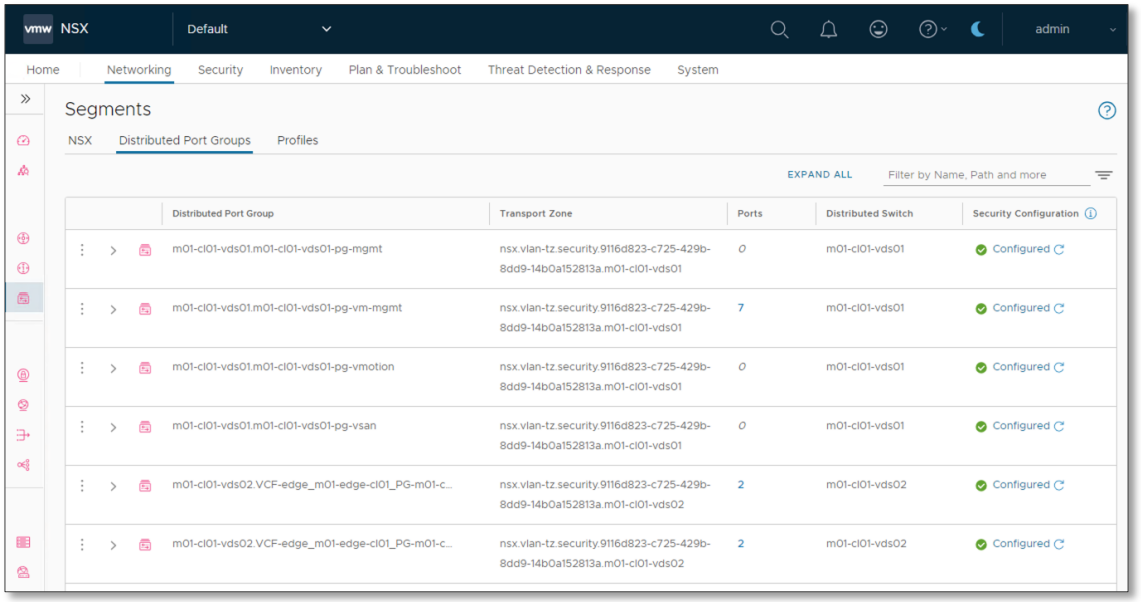


**Figure 12:** vSphere Distribute Port Groups are discovered by NSX after activating NSX on DVPGs

When the NSX on DVPGs is activated, the *dvfilter* for the VMs part of the DFW User Excluded Groups is disabled on their respective vNIC. This also means that vDefend distributed security features relaying on *dvfilter* (Distributed Firewall, Distributed IDS/ IPS,) are suspended for the respective VMs

```
[root@esx-04a:~] summarize-dvfilter|grep -A2 vcf01
world 2211767 vmm0:vcf01 vcUuid:'50 00 d7 37 5b ac 5d 9d-f8 72 09 a5 2e d0 f4 fe'
 port 67108891 vcf01.eth0
  vNic slot 2
   name: nic-2211767-eth0-vmware-sfw.2
[root@esx-04a:~]
[root@esx-04a:~] vsipioctl getrules -f nic-2211767-eth0-vmware-sfw.2
No root rule set.
[root@esx-04a:~]
[root@esx-04a:~] summarize-dvfilter|grep -A2 vcf01
[root@esx-04a:~]
[root@esx-04a:~] vsipioctl getrules -f nic-2211767-eth0-vmware-sfw.2
ERROR: failed to get total rulesets: switch port not found
[root@esx-04a:~]
```

**Figure 13:** vNic dvfilter is disabled for VMs, part of the User Excluded Groups after activating NSX on DVPGs

## Configure DFW Policy

Configuring the vDefend DFW policy can be done through the NSX UI or by using an automation tool based on individual preference. The detailed process for creating NSX groups and DFW rules is outside the scope of this white paper, but it is very well documented in the NSX administration manual.

To conduct the research for this document, we are using Terraform for fast and agile implementation and control of the DFW ruleset, in accordance with the security policy architecture outlined above. The Terraform config files can be found in the Appendix section and can be utilized if suitable.

According to our architecture approach, the overall VCF Management workload domain DFW security implementation is separated into two categories:

- Infrastructure policy protects traffic to common infrastructure services, such as DNS, AD, NTP, and Backup, as well as services external to the VCF infrastructure servers and tools.
- Environment policy that defines the rules and secures the traffic for the VCF instance itself.

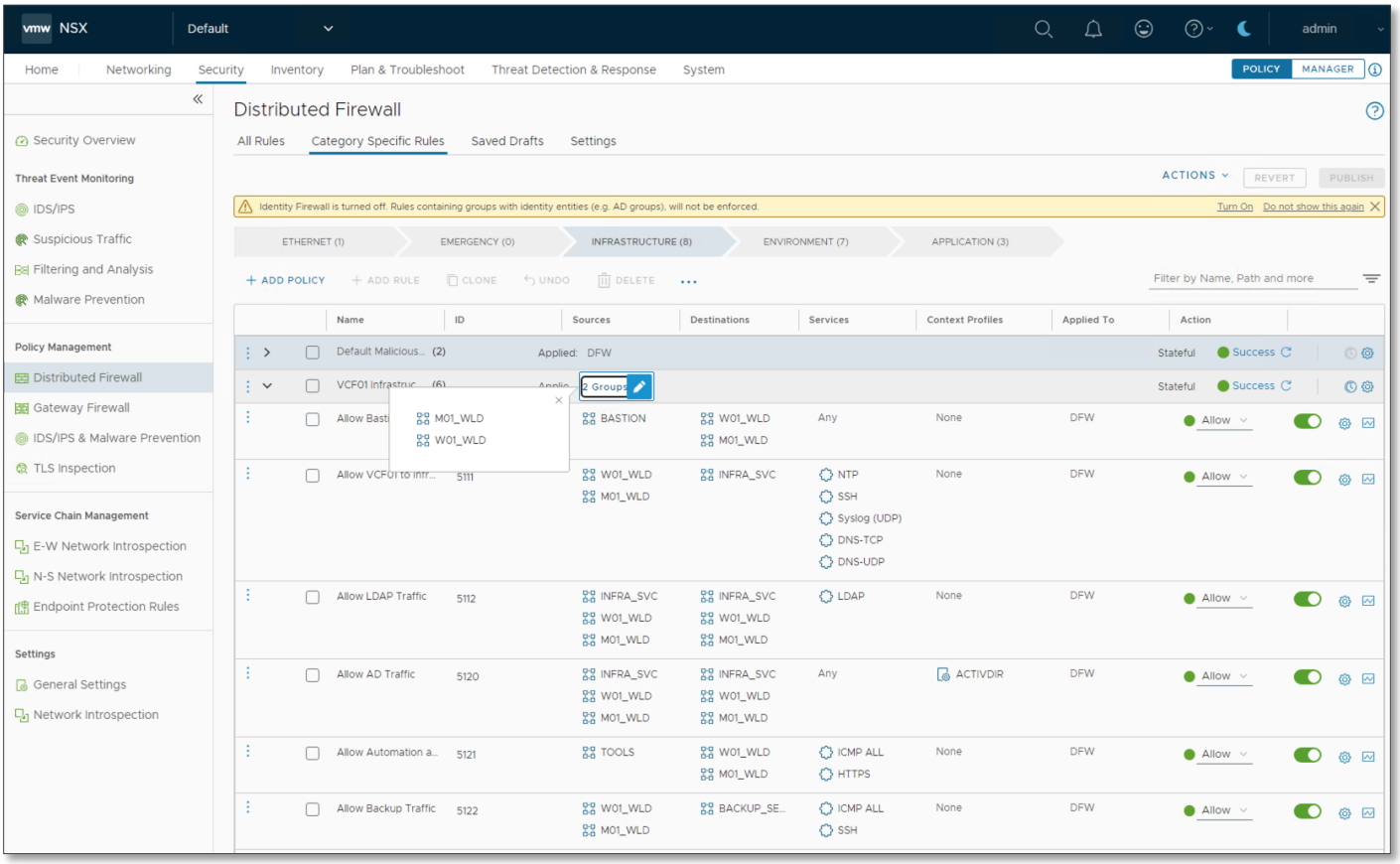


**Figure 14:** VCF Management domain Infrastructure DFW rules

Both policies are applied to the VCF Management and VI WLDs groups (top-level security zones), so the rules' "Applied To" fields are left with the default one (DFW). This approach provides a quick and fast start for security posture. The policy can be refined as a Day 2 operation, and the rules "Applied To" the field can be populated with the workload to which this rule applies. Remember that the policy "Applied To" field takes precedence over the specific rule one.

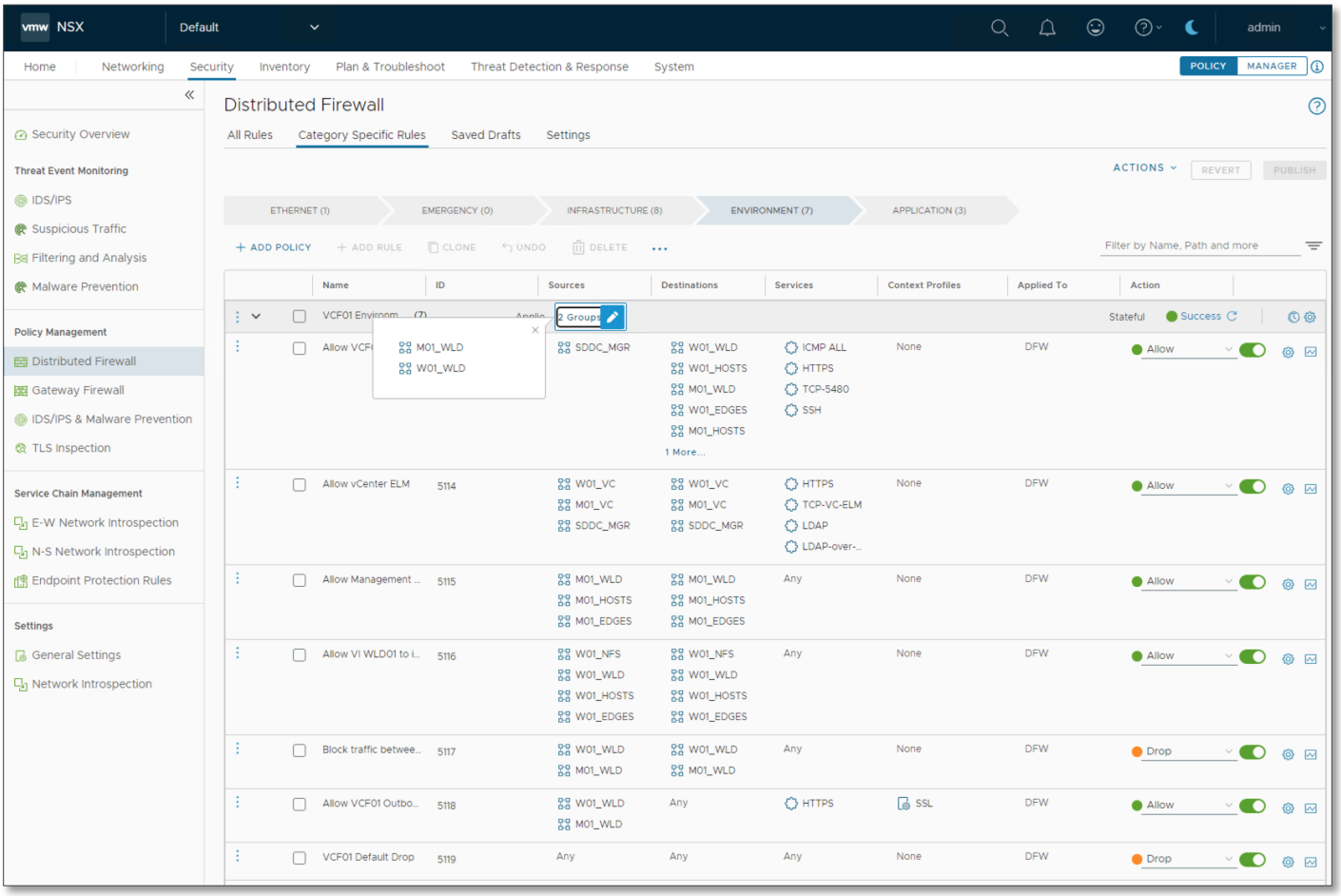


**Figure 15:** VCF Management domain Environment DFW rules

The respective VCF management components (VMs) are still part of the DFW Excluded Group, so the delivered policy will not affect them. This is an excellent stage to double-check the policy and verify that it allows all the necessary Management WLD components traffic and that nothing is overlooked.

As a double precious measure, we can also initially switch the policy “catch-all rule” at the bottom to "Allow and Log" and monitor for a period of time to see if the default rule matches any traffic that should be permitted. If such traffic is discovered, we must change the policy appropriately to handle it.

## Remove VMs from the User Excluded Group

To activate the DFW on the respective VCF management domain VMs, we have to remove them from the User Excluded Group, which was automatically created during the VCF bring-up process.

This is done from the **Security > Distributed Firewall > Settings > User Excluded Groups**. We unselect all VMs, except the Management domain NSX Managers. It is essential to leave these NSX Managers in the Excluded Group because we don't want to take any chances and potentially block access to this component with the DFW that it manages.

Note that because the provided screenshots are taken from a Lab environment, there is a single NSX per WLD. For production deployment, you will have three NSX Managers in a cluster per WLD, so all three Management domain NSX Managers must be left in the User Excluded Group.

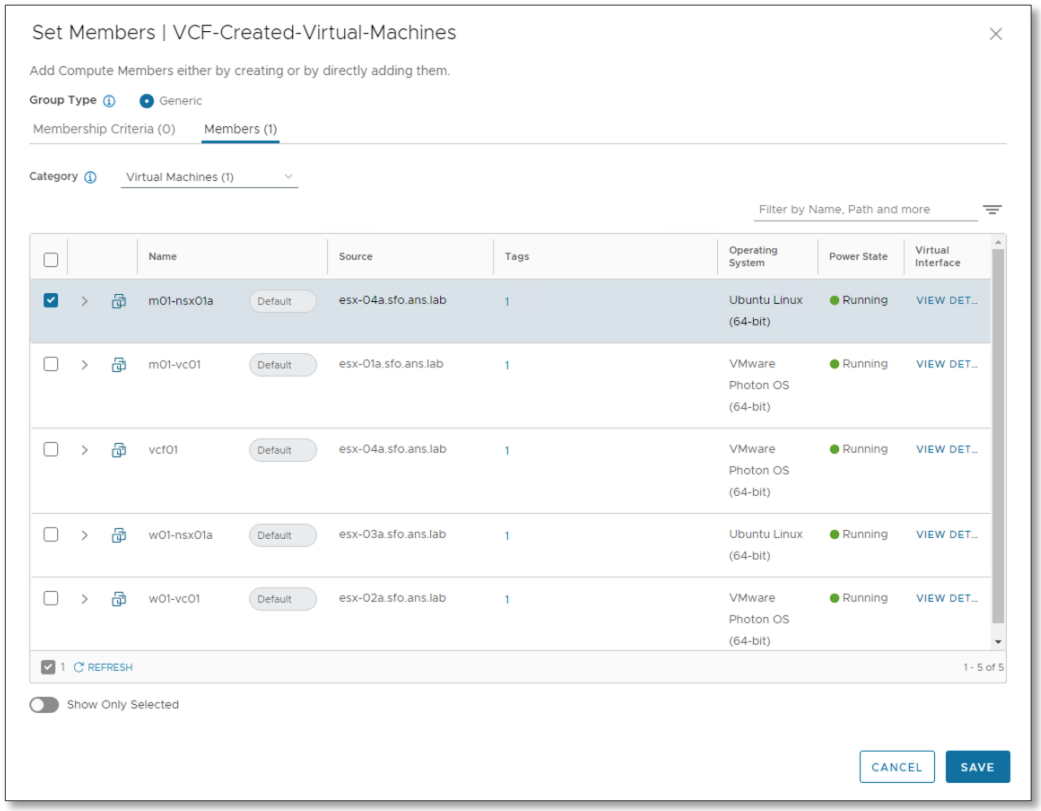


**Figure 16:** VCF Management NSX User Excluded Group

## Policy Realization

As soon as the VMs are removed from the User Excluded Group, the security policy will be applied to them, and the traffic to and from this component will be subject to the DFW inspection. From the respective ESXi hosts, where the VMs reside, we can verify that the *dvfilter* is active on the target vNICs, and that the appropriate DFW rules are configured.

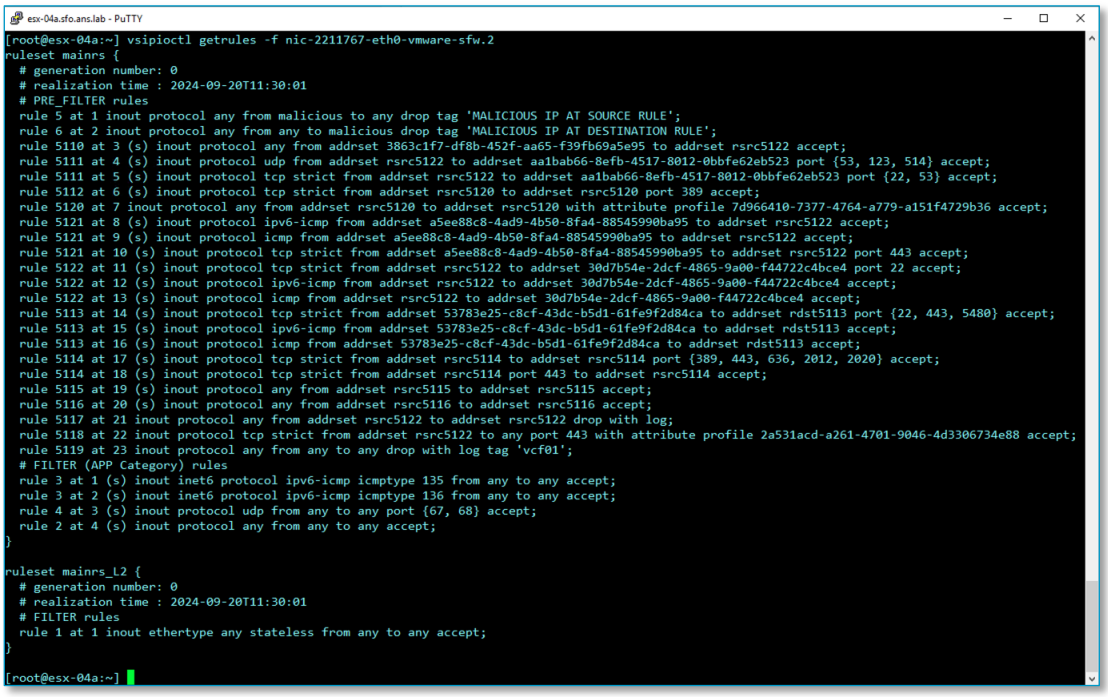


**Figure 17:** DFW applied on the SDDC Manager when placed outside of the DFW Excluded Group

A standard final step will be to verify the policy accuracy by initiating test traffic from different sources and also check that all VCF components communicate appropriately in between and with external devices and services.

## Utilizing Security Intelligence

### Security Intelligence for Policy Verification

vDefend Security Intelligence can help us verify the existing policy and ensure our segmentation policies are allowing all traffic that is required. To do that, we can create and trigger recommendations for the two groups that identify the VCF workload domains and on which the above Infrastructure and Environment policies are applied (M01_WLD and W01_WLD).

The workflow output will have nothing to recommend if the policy is accurate and allows all the necessary traffic.

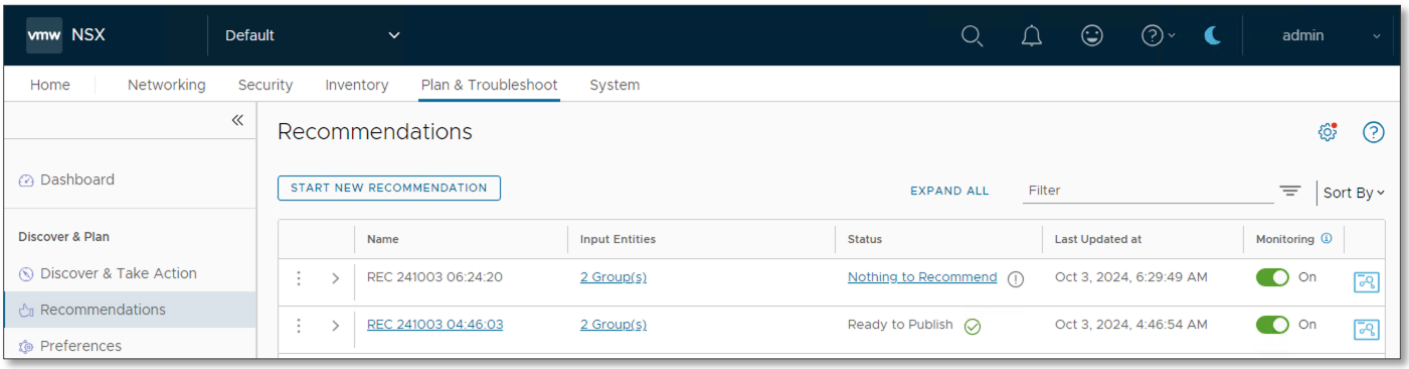


**Figure 18:** Using Security Intelligence for Policy Verification

### Per-WLD Micro-segmentation Example

Implementing a zone-based (macro-segmentation) policy is the foundational, first step in securing the VCF Management domain and its components. Delivering a more granular micro-segmentation policy is the second essential step, and ultimately, adopting a zero-trust approach within each security zone. Building such security policies is usually cumbersome, so it will be beneficial to utilize Security Intelligence recommendations for this task.

In our scenario, an important consideration when using Security Intelligence will be that an existing DFW policy is delivered, allowing traffic between all the management and infrastructure components per WLD. Security Intelligence generates recommendations only for unprotected traffic, which is traffic that hits a DFW rule with both source and destination fields set to "Any". So, if we want to trigger a rule recommendation, for instance, for the W01_WLD group (ref. to Figure 15 above), rule 5116 has to be considered while generating flow recommendations.

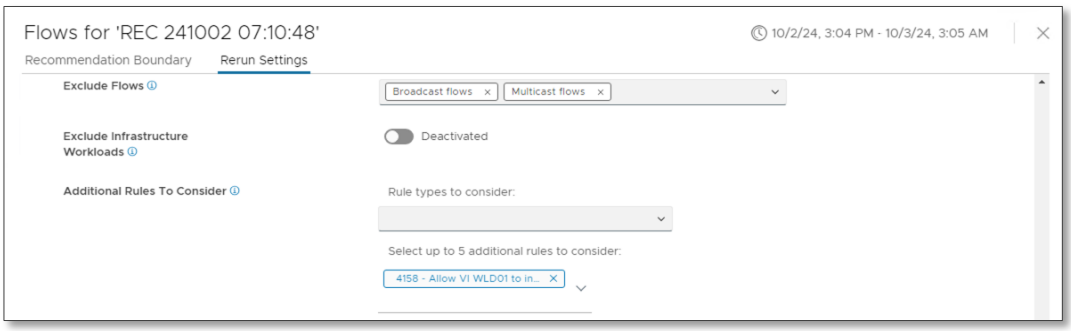


**Figure 19:** Security Intelligence recommendation configuration

The flow assessment and the rule generation take a few minutes to complete. After the task is completed successfully, we receive the suggestions provided in the recommendations output. Please note that because we are using a lab environment, the output provided in the figure below might have only some of the necessary rules for a production

environment. The intention here is to illustrate how Security Intelligence can facilitate quick and easy micro-segmentation implementation.

Also note that if you decide to use the policy recommendation and publish it, the preceding macro-segmentation rule/s (5116 in our case) has to be disabled.

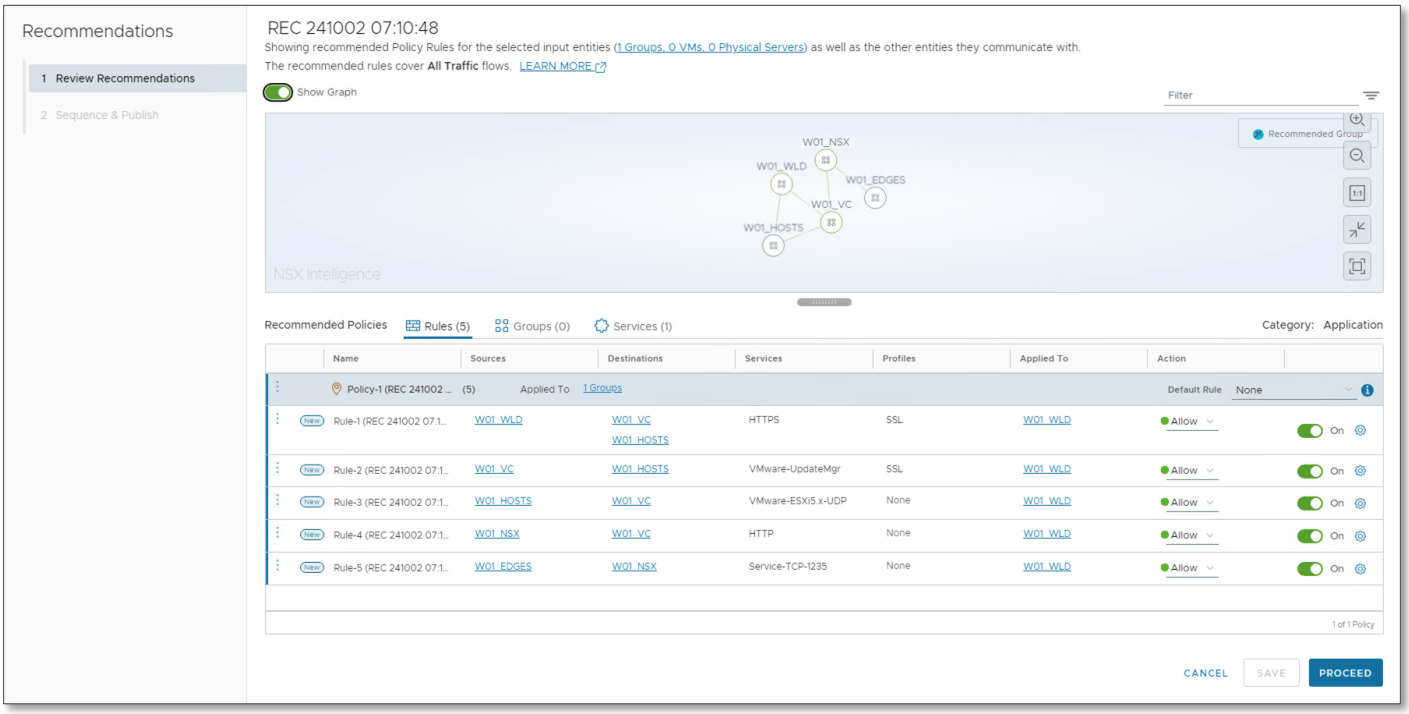


**Figure 20:** Security Intelligence micro-segmentation rule recommendation

## Conclusions

The Management workload domain is a critical component of the VCF stack as it hosts the entire management infrastructure, such as the SDDC Manager, vCenter Server, NSX Managers, Aria Sure, etc. Thus, it is essential to protect the Management domain and its applications from potential network intrusion activities and misuse and establish a secure VCF private cloud operation.

VMware vDefend provides cutting-edge capabilities for zero-trust lateral security. It is an integrated component of VMware Cloud Foundation, available immediately for consumption without the need redesigning the data center network infrastructure, thus making it the perfect solution for VCF customers to protect their private cloud.

## Appendix

**Terraform config files GitHub repository**

https://github.com/vmware-nsx/vcf-mgmt-wld-security

vmware by Broadcom


Item No: vmw-bc-wp-tech-temp-a4-word-2024 1/24