Well-Architected Design: Distributed Firewalls Uses Cases and Scope

Table of contents

Well-Architected Design: Distributed Firewalls Uses Cases and Scope

Introduction

In today's digital landscape, gaining unauthorized access to systems and moving laterally within the infrastructure is a major concern for organizations. This not only results in a security breach but also compromises the entire data center as well as SDDC. Traditional legacy and physical firewalls have been ineffective in preventing such breaches.

However, NSX Distributed Firewall (DFW), a software-defined firewall, has emerged as a solution to this problem. It is designed to secure east-west traffic and block lateral movement of threats by using a software-based approach that is built into the hypervisor and delivered at each workload. DFW is a Layer 2 – Layer 7 control point that is situated logically at every Virtual NIC (vNIC) of all Virtual Machines (VMs). This enables it to enforce access controls and inspect every flow for threats.

NSX Distributed firewalls are ideal for various use cases, including on-premises data center extension to the cloud, disaster recovery solutions, new VMware cloud deployments, and on-premises NSX deployments. In this design we will explore the benefits of NSX Distributed Firewall and how it can help organizations protect their digital assets.

Scope of the Document

The NSX Distributed Firewall provides various security offerings for both on-premises and VMware Cloud environments, which can be utilized to enhance and strengthen the security of workload virtual machines. This design outlines the different use cases and scopes that architects, security and infrastructure administrators should consider while designing the distributed firewall for VMware Cloud. Whether coming from an on-premises environment with or without NSX, this design aims to give a comprehensive understanding of the distributed firewall and its capabilities.

Summary and Considerations

Use Cases	
Pre-requisites	
General Considerations/Recommendations	
Performance Considerations	The DFW exists in the kernel of the hypervisor or platform itself, which means it delivers line rate performance DFW optimizations. As DFW is distributed in the kernel of every ESXi host, firewall capacity scales horizontally when you add hosts to the clusters. Adding more hosts increases the DFW capacity. As your infrastructure expands and you buy more servers to manage your ever-growing number of VMs, the DFW capacity increases.
Network Considerations/Recommendations	Consider implementing a Least Privilege access model with the DFW's rules which can leverage advanced constructs like tags and grouping in addition to the traditional source and destination addresses.
Cost Implications	https://www.vmware.com/products/aria-operations-for-logs.html https://www.vmware.com/products/aria-operations-for-networks.html
Document Reference	For NSX recommended limits, use the VMware Configuration Maximums tool.
Last Updated	April 2023

Infrastructure Overview

VMware Cloud SDDCs have both gateway firewall and distributed firewall functionality. The gateway firewall protects the north-south traffic while distributed firewall functionality protects the east-west traffic. The gateway and distributed firewall can work in conjunction to provide better security to workloads.

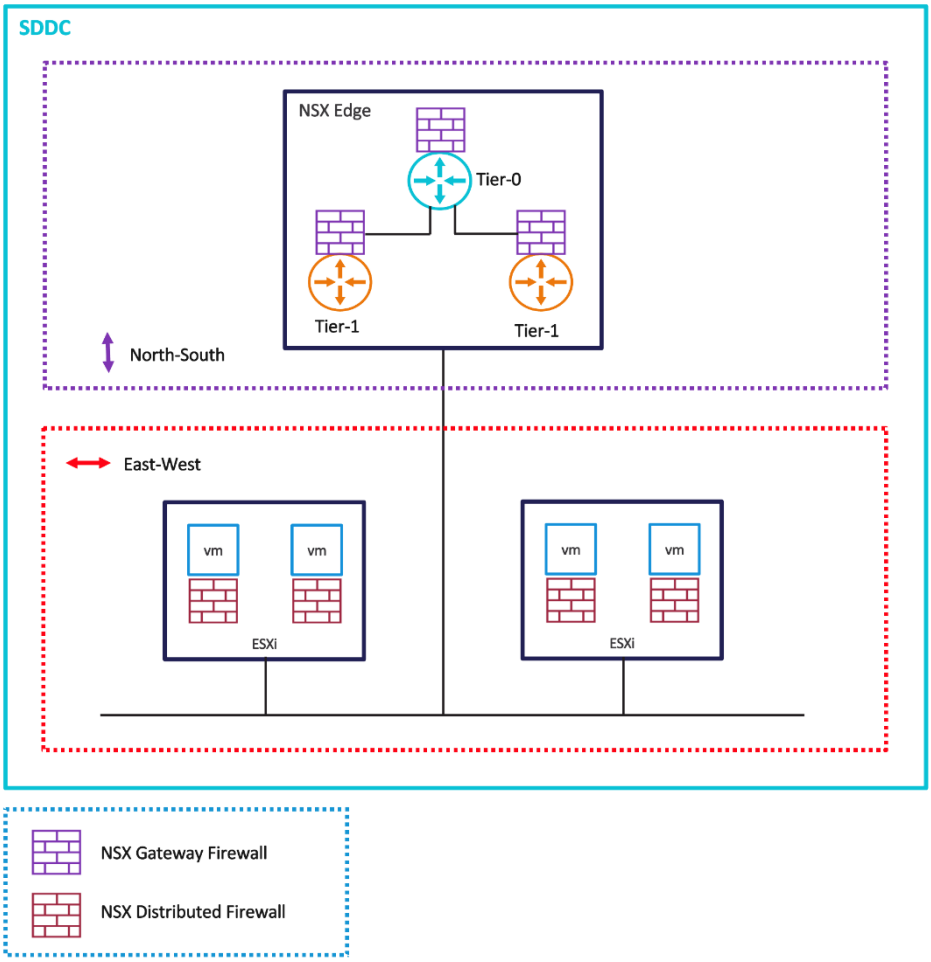

Figure 1 - SDDC Firewall Types

Deployment Scenarios

Deployment Scenario	Description	Recommendations
Greenfield SDDC deployment on VMware Cloud	For greenfield deployments, DFW security is needed for applications and workloads.	Start building the security posture from day one for DFW capabilities with zone segmentation followed by application and micro-segmentation
On-premises data-center extension to VMware Cloud	After an SDDC is built in VMware Cloud, you can apply the same posture for your workload VMs as in-on-premises. When using NSX in your on-premises environment, use similar security constructs to build the Cloud SDDC as you have used on-premises with NSX.	Start building the security posture from day one for DFW capabilities using zone, application, and micro-segmentation. Explore APIs (Application Programmable Interfaces) to provision the similar policies for DFW firewalls rules across on-premises and VMware Cloud environments.
On-premises data-center evacuation to VMware Cloud	You may consider evacuating your complete on-premises data center to VMware Cloud for various business needs. You can deliver an equivalent or increased level of protection using VMware Cloud.	Take a backup of your on-premises security configuration and start designing DFW capabilities in pre-migration phase. Start your VMware Cloud journey by applying a combination of Gateway and DFW firewalls using your existing backup configuration as reference.
Disaster Recovery VMware Cloud SDDC	A Disaster Recovery SDDC contains mission critical VMs. Plan DFW security design for disaster recovery VMs prior to a disaster.	In a disaster scenario, you may not be in a place to implement new security policies. Plan and protect DFW policies and rules from day 0 for recovery SDDC VMs while you have recovery plan in place.

Resiliency and Availability

Distributed firewalls are built around a software defined policy construct. In the event of host failures or DRS (Distributed Resource Scheduler) moving VMs (Virtual Machines) to another host, the DFW rules for that workload remain intact. This is because the DFW exists in the kernel of each host’s hypervisor. When a VM moves across hosts, the DFW rules are still applied to that VM and are independent of any guest OS (Operating System) or host-level configuration.

Scalability

In the case of host addition or data center expansion with more nodes added to the SDDC, there is no change needed. Distributed firewalling capacity dynamically scales linearly as you add more compute to accommodate the organization's growth.

Performance

The DFW exists in the kernel of the hypervisor or platform itself, which means Layer 4 DFW delivers line rate performance. Distributed Firewall is independent of the guest operating system and OS firewall.

Integration

DFW is a component of NSX, a networking platform for VMware's SDDC that is deployed on-premises or in the VMware Cloud. NSX controls the life cycle management, which is completely included in the product.

Operations Overview

Security

Zone, Application and Micro-Segmentation security for VM workloads along with VDI (Virtual Desktop Infrastructure) environments are supported through DFW taking your organization journey towards zero trust.

While VMware NSX Advanced Firewall for VMware Cloud on AWS includes capabilities like L7 firewall, user ID/identity firewall, FQDN filtering, distributed IDS/IPS and threat prevention, are not addressed in this document. For more information about these topics, see this additional document https://www.vmware.com/products/nsx-advanced-firewall-for-vmc.html

Monitoring and Alerting

DFW supports monitoring and alerts. Monitor distributed firewall rules through VMware Aria Operations for Logs when a firewall rule is created, changed or deleted.

Alerts are sent if the rules cannot be configured or if there are memory issues.

Logging

Logs for distributed firewall can be enabled on per rule basis and are disabled by default. Once logging is enabled on a rule, the logs are available from VMware Aria Operations for Logs subscription. The logs contain detailed information:

- Per rule firewall packet logs with L3/L4/L7 context, rule id & Log label
- Detailed audit log for FW config changes with info on change, time, user etc.
- Flow & session stats for each rule with popularity Index
- Policy realization state per DFW policy

VMware Aria Operations for Log https://www.vmware.com/products/aria-operations-for-logs.html

Capacity Management

When deploying the NSX Distributed Firewall (DFW), it is important to consider the potential overhead on system resources, especially CPU and memory. To mitigate the impact of DFW on system resources, several best practices can be followed:

- Start with a basic security policy: Initially, start with a basic security policy and test its performance under realistic traffic loads. This allows you to monitor system resources and identify potential bottlenecks.
- Use Tags, Grouping, “Applied to” to reduce traffic: Use filters to optimize DFW rules and decrease the number of rules that the DFW must process. This can help to reduce the CPU and memory consumption of the DFW.
- Scale out NSX Edge nodes: Scale out NSX Edge nodes to distribute the load of the DFW and avoid a single point of failure. This can also help to improve performance by allowing traffic to be processed in parallel by multiple Edges.
- Keep monitoring resource utilization: Monitor the CPU and memory utilization of the NSX DFW to identify any performance issues and optimize the deployment accordingly.

For NSX recommended configuration maximums, use the VMware Configuration Maximums tool to evaluate maximum number of DFW rules created and stay within the recommended limits.

Cost

Layer 4 DFW capabilities are part of VMware Cloud deployments and do not incur additional costs. Advanced DFW capabilities like IDS/IPS, L7 App ID FW, Identity FW and FQDN filtering are available as single add-on pack. The details on this Adv FW add-on pack is not covered in this document.

VMware Aria Operations for Logs and VMware Aria Operations for Networks are not included with default VMware Cloud subscription and are sold separately.

DFW differences from traditional firewalls

For security and infrastructure administrators it is critical to know the differences between traditional legacy firewall and distributed firewall. Some security administrators may follow the standard zone or VPC-based approach and then control all security scanning at the Edge, DMZ, or Perimeter VPC/zone.

DFW policies and rules are configured with a different mindset and may require additional effort in identifying the appropriate environment and VMs to include. A policy framework should be considered to ensure all DFW rules are created with the correct settings that adhere to an organization's security objectives.

Traditional firewalls and Distributed firewalls have some similarities along with many differences.

Traditional Firewalls	Distributed Firewalls
Physical or virtual appliance firewalls have network topology dependencies, so firewalling can be done only at the network boundary and for north-south traffic.	Distributed virtual firewalls are network agnostic and can firewall east-west traffic.
Broader network segmentation is the only possibility.	Granular application and micro-segmentation.
Static policy based on based on IP or gateway interface.	Dynamic workload context-based policy.
Cannot secure endpoints on the same VLAN, unless they are deployed in Layer 2 mode.	Can easily secure endpoints on same segments.
Legacy firewalls are built around IP address constructs.	
Runs on specific dedicated hardware/server.	Runs on every hypervisor or physical server and is an east-west firewall.
Centralized, network dependent.	Decentralized, distributed and network agnostic.
Perimeter Firewall rules must be updated for every new entry. Flat network split into zones/subnets.	DFW applied to every vNIC of every workload VM. These are dynamic application-centric policies.
Hair-pinning if workloads are hosted on the same host.	No hair-pinning of traffic for inspection
Fixed architecture	Scaled out architecture

Distributed Firewall Design Journey

Plan and design the segmentation in phases where you can begin the design and implement with zone/macro segmentation. Follow up by adding more granular application segmentation, then gradually moving towards micro-segmentation. All of these are part of baseline DFW features and can be phased in as needed to meet your technical and business requirements.

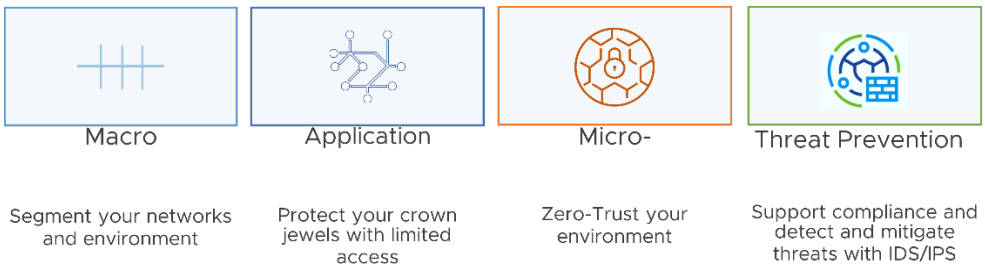

Figure 2 - DFW Journey

The table below outlines a DFW design journey that you can use to build a phased implementation plan:

Phase	Segmentation/ Add-on	Description	Planning	Deployment Recommendations
Phase 1	Zone Segmentation	Start your DFW journey with broader network segmentation. Plan to create multiple virtual zones to divide the data center into smaller zones.	Define the necessary NSX firewalling policies based on the organization's zonal security requirements. NSX Tag/Object-based dynamic grouping can be leveraged to create groups such as DMZ, Prod, Non-Prod, or Services zones. Define virtual zones by grouping virtual interfaces, using tag for the relevant workloads, and plan define relevant DFW policies.	Infrastructure Design - Define access to shared services under this category. For example: AD, DNS, NTP, DHCP, Backup and Management servers Environment Design - Define access between zones under this category. For example: Production vs development, PCI vs non-PCI, Inter-business unit rules.
Phase 2	Application Segmentation	Start with a zero-trust model design to reduce the attack surface. This phase builds a fence around each application.	Start with a few critical applications to segment and begin building this security posture for all applications over time.	Define access to workloads such that all workloads within an application can communicate. Any outside communication is restricted by application-segmentation policy.
Phase 3	Micro-Segmentation	Complete your final state towards zero-trust model. Necessary traffic is allowed between any application /application-tiers/services.	Plan to do this part again in stages, starting with a few applications, and extending to all applications over time. Requires understanding ports and protocols used for all applications.	Use tools like NSX Intelligence or VMware Aria Operations for Networks to further understand the details.
Phase 4	Threat prevention and advanced DFW Integration	L7 Firewall, User ID/Identity Firewall, FQDN filtering, distributed IDPS	Plan and design threat prevention, the applications and ports allowed may still be vulnerable and exposed to malicious attacks.	Advanced DFW becomes more useful to deploy once you have the required micro-segmentation.

Design Considerations for Deployment of Distributed Firewall Rules

Design Considerations	Design Justification	Design Implication
Plan to create the DFW rule in appropriate category based on traffic type	DFW Categories are evaluated from left to right (Ethernet > Emergency > Infrastructure > Environment > Application), and the distributed firewall rules within the category are evaluated top down.	Traffic is evaluated against Emergency rules first, then by the Infrastructure rules, the Environment rules, the Application rules and finally the default rule.
Segments should be used to create broader and generic groups like environment/zone that are at higher level	Helps in defining targeted policy at specific zones/tenants without stepping on policy defined on other tenants/zones.	Applying the most broadly applicable rules at the higher levels helps reduce complexity and duplicated effort.
For application/application tier grouping, use dynamic grouping with VM Tags, VM names or a combination. Recommend using, Tag/name “Equals-to” instead of other regex conditions like contains/starts with/ends-with/not-equal	VM Tags reduce the complexity of static rules and rules get automatically applied after VM creation matching the criteria.	Provides scale-out architecture with security first principle to the workload VMs lifecycle from creation, updating and deletion.
With Nested Groups, it recommended to use no more than 3 levels of nesting	Manageability and Resource optimization	Planning ahead is needed to create a group structure that accounts for this recommendation.
“Applied To” defines the scope of enforcement per rule	Optimizes the resource utilization on the ESXi hosts.	The default option is “DFW” where rules are applied to all workloads, resulting in non-optimized rulesets.
With the “Applied to” field option using Grouping, you must ensure that virtual machines are included that are part of inbound and outbound traffic (source as well as destination VMs).	Optimize and apply the DFW rules at specific source and destination VMs with Applied-to field.	If Applied-to field is not used, the DFW firewall rule is applied on the vNICs of all the workload VMs.
Denylist or allowlist	For micro-segmentation, you may prefer to allowlist i.e., deny all traffic other than what is specifically allowed.	With allowlist, all the traffic that you allow is only permitted. Ensure that you have looked at all the protocols and ports to have zero impact on your applications.

Ethernet Rules	**Emergency**	**Infrastructure**	**Environment**	**Application**
Include Layer 2 rules for this category.	Include quarantine and allow rules for this category.	Include rules which define access to shared services for this category. For example: AD, DNS, NTP, DHCP, Backup, Management server.	Include rules between zones for this category. For example: Production vs development PCI vs non-PCI Inter business unit rules.	Include rules between: Applications Application tiers Micro services

Use Cases for Distributed Firewall

Virtual Zones with Zone Segmentation

If you need to provide centralized infrastructure services to different lines of business or to external partners with access to some of their applications and data, you may need to deploy proper segmentation between DMZ workloads that are exposed to the outside and the internal applications and data.

Traditionally, segmentation between tenants or between the DMZ and the rest of the environment is done by physically separating the infrastructure. This means that workloads and data for different tenants or different zones were hosted on different servers with their own dedicated firewalls which leads to sub-optimal use of hardware resources.

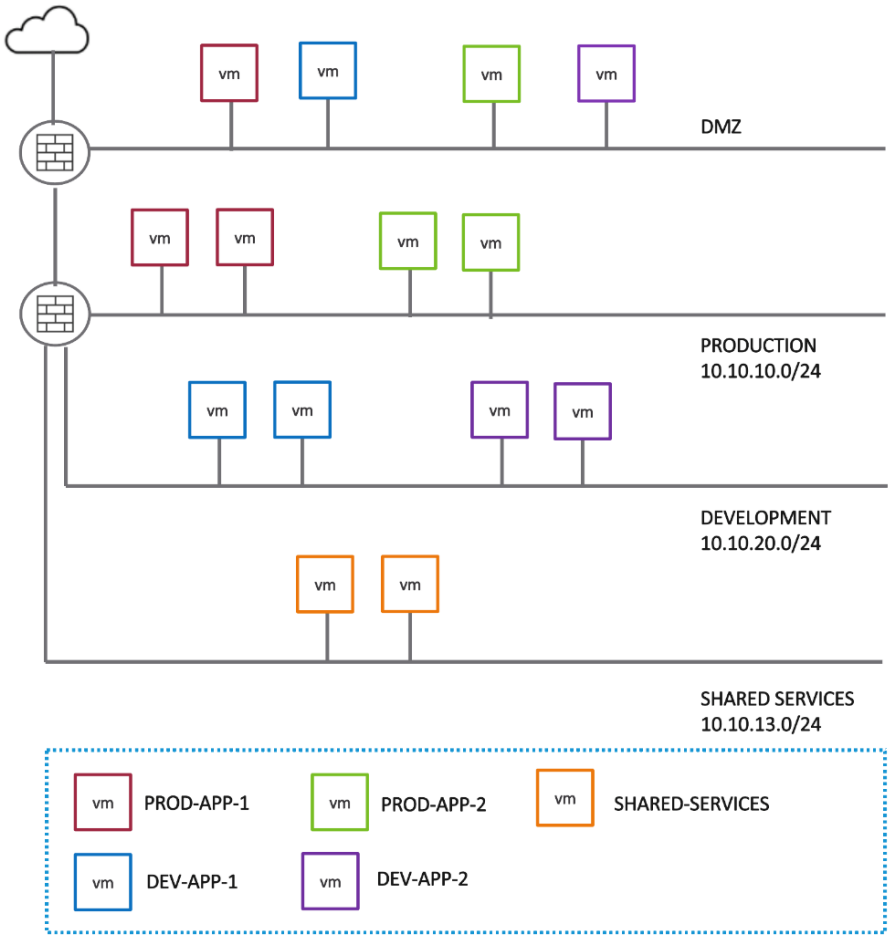

Figure 3 - Segmentation with native firewall

The NSX Distributed firewall allows customers to run workloads that belong to different tenants and different zones on the same hypervisor clusters. This provides the same level of segmentation that would be provided by physical firewalls while allowing much higher consolidation ratios.

This example clearly articulates how you can implement a distributed firewall design with virtual zone firewalling while planning for broader network/zone segmentation in the early phase of distributed firewall adoption.

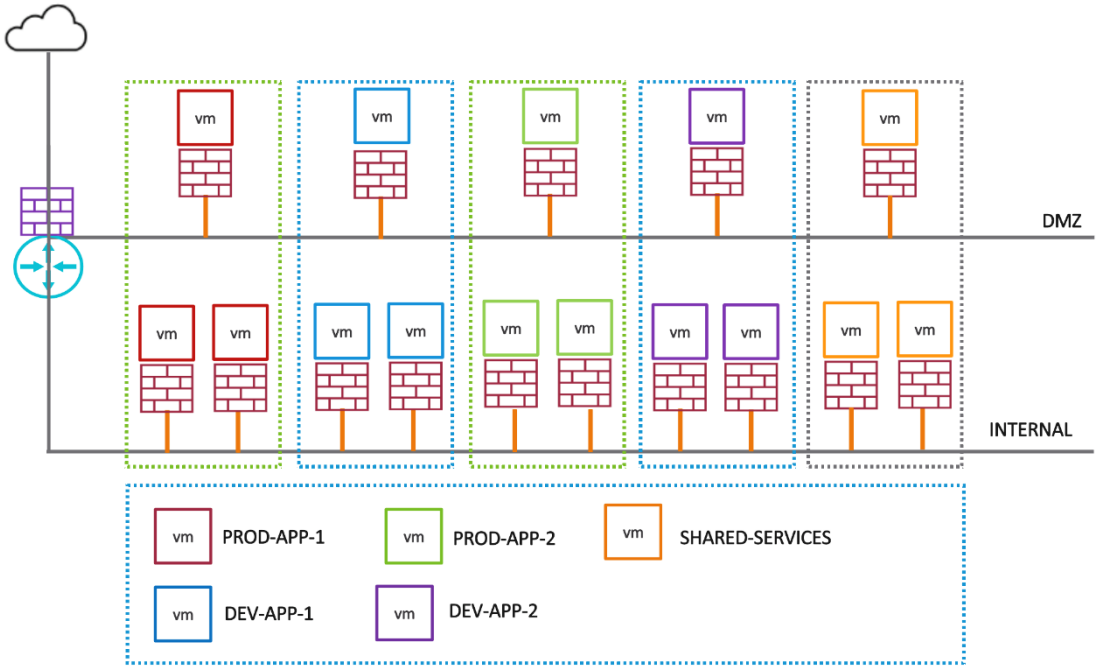

Figure 4 - Virtual Zone Firewalling with Distributed Firewall

On-premises security using native firewall	VMware Cloud security using DFW
Firewall rules between PROD, DEV, SHARED Services and DMZ applied on firewall interface. Use of static objects for creating rules. Any new VMs may be covered if already part of the existing segment.	Create NSX Tag/Object-based dynamic grouping to create PROD, DEV, and SHARED Services. Use above Tags to create DFW firewall rules for required allow, deny access. Policies will apply to existing VMs in the above virtual zones based on the Tag policies. DFW will automatically apply policies to added VMs based on dynamic grouping.

Application Segmentation

Application segmentation provides higher security than a zone model and is closer to achieving a zero-trust model which will reduce the attack surface further. This phase builds a fence around an application so that all workloads within an application can communicate but outside communication is restricted by application-segmentation policy.

Since most organizations have many applications, it may be necessary to start with a few critical or simpler applications and expand this security posture to all applications over time.

Micro-Segmentation

Micro-Segmentation is a security model where communication between elements is defined as explicitly as possible. At its extreme, micro-segmentation would be the explicit definition of communication between pairwise elements. NSX offers micro-segmentation based on tags which allows explicit definition by groups.

In this final state, an organization will be able to provide a zero-trust model where only necessary traffic is allowed between any application, any application tiers and any service. This is a challenging phase due to the knowledge needed of ports and protocols for all applications. Like application segmentation, this can be done in stages, starting with few applications, and extending to all applications over time.

VMware Aria Operations for Network can help profile applications at scale and reduce the time needed to achieve micro-segmentation. Aria uses NetFlow/IPFIX to understand traffic patterns and has visibility to the virtual and physical world by tapping

the switches and routers in both worlds. This provides an understanding not only of what machines are communicating on which ports, but also a sense of the volume of each traffic flow. VMware NSX Intelligence may also be used to help in this process.

Compliance

For sensitive applications that deal with healthcare or financial data and require compliance with regulations such as HIPAA, PCI-DSS, SOX, etc., the use of IDS/IPS is often mandated to mitigate risks of data theft. The NSX distributed firewall facilitates such regulatory compliance by enabling micro-segmentation to reduce the scope and enable selective application of IDS/IPS to the workloads that require compliance.

The NSX distributed firewall architecture and micro-segmentation capabilities help propagate regulation-specific security policies to all relevant workloads and track traffic flows to and from sensitive applications, regardless of workload location. This eliminates the need to purchase and deploy separate appliances to support compliance.

For example, to meet the Payment Card Industry Data Security Standard (PCI DSS, often abbreviated PCI) compliance requirement, the NSX firewall can be used to define a virtual PCI zone and protect it using firewall and IDPS security controls, as mandated by PCI. Distributed firewalls enable this without the need to rearchitect the network topology, allowing every workload to have its own firewall/IDPS at the vnic level. Additionally, NSX firewalling/IPS policies/profiles can be customized for PCI workloads, including both zone segmentation and micro-segmentation to protect critical PCI workloads.

VMware tools like Aria Operations can be used to streamline audit requirements, leading to a tangible ROI for customers and facilitating compliance requirements for discovery and audits, such as the PCI Compliance report.

Ransomware Protection

When effectively designed and implemented, the Distributed Firewall can minimize the risk of ransomware attacks within the data center by preventing lateral movement. Attackers usually have a different objective than their initial point of entry, meaning they will attempt to move through the environment to reach the valuable data they are after. Thus, preventing unwanted lateral movement is just as crucial as securing the initial attack vector.

The distributed firewall's micro-segmentation capability can significantly reduce attack surfaces and make lateral movement much more challenging. With the DFW, t is now operationally feasible to use an Intrusion Detection and Prevention service to front-end each workload, detecting and blocking attempts to exploit vulnerabilities, regardless of whether the attacker is trying to gain initial access or has already compromised a workload on the same VLAN and is attempting to move laterally.

For more advanced ransomware protection, it is possible to implement L7 firewalling, IDPS and FQDN filtering along with the L4 distributed firewall and micro-segmentation.

Distributed Firewall Examples

Using DFW on VMware Cloud with 3-tier application using micro-segmentation

Consider the following example of a 3-tier application consisting of Web, Application and Database servers.

Topology:

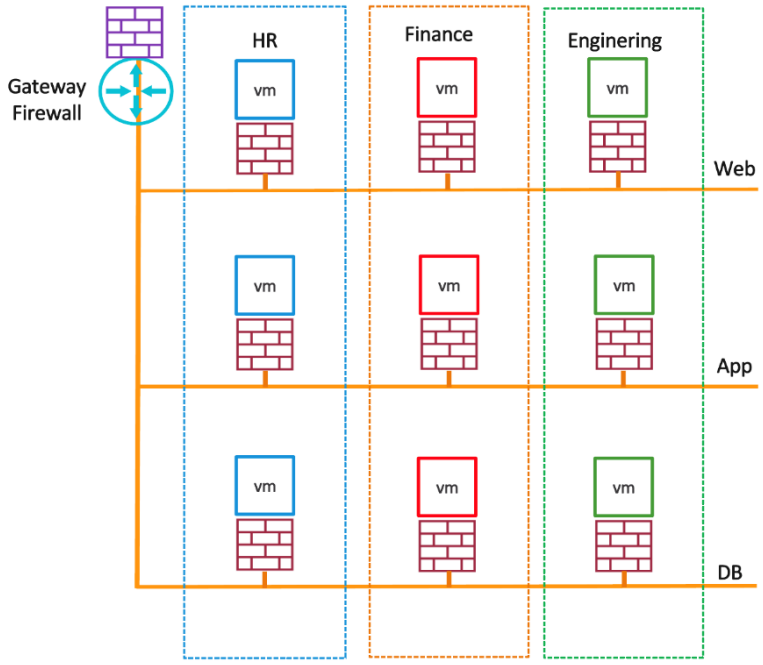

Figure 5 - 3-tier Application

3 Tier Application Security	Design Considerations	Description
Web Server	Create DFW rule from Any to web servers for HTTP and HTTPS services	The Gateway firewall rule may be over public IP for HTTP, HTTPS while web servers may be in pool behind a load balancer or there could be just one web server NATed 1:1 to the private IP of the web server as per your design.
Application Server	Create DFW rules from web servers to application servers for specific application port/s	Access to application servers is limited to web servers; other access is prohibited.
Database Server	Create DFW firewall rules from application servers to database server for database port/s	Access to the database server is limited to application servers, on database access ports.
Common DFW Rules	Prefer to allowlist i.e., deny all traffic other than what is specifically allowed.	Allow traffic for common shared services DHCP, NTP, etc.
DFW rules fields	Group the source/destination virtual machines. The Applied to field can be applied specifically to the targeted servers where we would like DFW rules to be present instead of present anywhere.	The source and destination for DFW rules can be groups based on the VM tags. (i.e., web-01, web-02, web-03 are tagged as “web server” and similar for application and database servers. Grouping you must ensure to include virtual machines to specify the inbound and outbound rules for “Applied to” field. This makes rules present only at source and destination VM kernel vNic when applying micro-segmentation, while all other traffic being dropped. Otherwise, if the DFW rule is applied by default to DFW, rules are available at all the VMs in the SDDC.

Using DFW when on-premises workloads are connected to VMware Cloud

You may have extended your on-premises data center or SDDC to VMware Cloud. The on-premises SDDC could be with or without NSX-T.

In such a complex environment, hybrid cloud configuration where there is a connection from an on-premises environment to a VMware Cloud based SDDC over L3VPN/L2VPN/HCX and shared common services like DNS, DHCP, NTP exist in the on-premises environment. After your on-premises SDDC is connected to VMware Cloud using any of the technologies, you can apply the same or better security posture for your workload VMs as in-on-premises using Distributed firewalls.

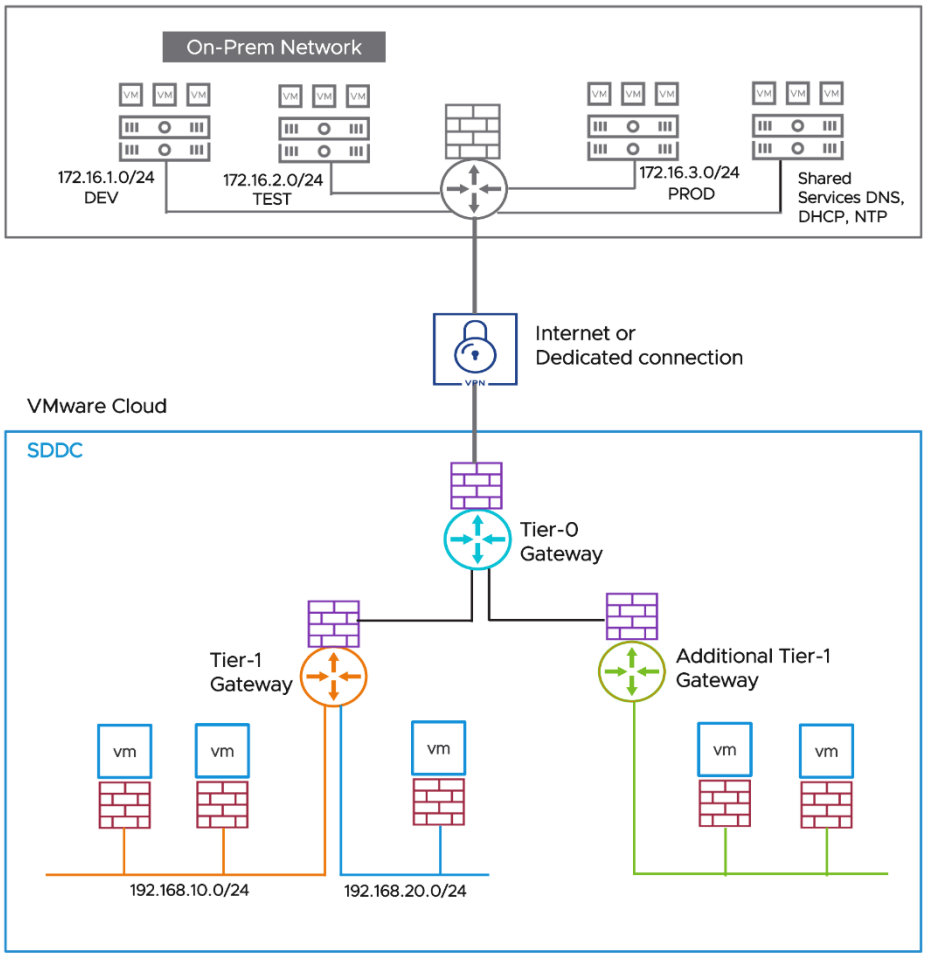

Figure 6 - On-premises connectivity considerations

With the following network requirements for this environment:

172.16.1.0/24 DEV, 172.16.2.0/24 TEST requires access to 192.168.10.0/24 SDDC segment

For the TEST and DEV network to access the VMware cloud segment 192.168.10.0/24, firewall rules are required at the on-premises gateway. Similar rules can be provisioned for on-premises PROD access to SDDC segment or vice versa.

Use Case	On-premises Recommendations	VMware Cloud Recommendations
Using Distributed Firewall when on-premises workloads are connected to VMware Cloud.	Check the gateway firewall rules at on-premises for 172.16.1.0/24 DEV, 172.16.2.0/24 TEST access to 192.168.10.0/24	Create the DFW rule to allow traffic from 172.16.1.0/24 DEV, 172.16.2.0/24 TEST access to 192.168.10.0/24 Create the DFW rule to deny any other traffic to 192.168.10.0/24
Using Distributed Firewall with VMware Cloud when **DNS, DHCP, NTP,** etc. common shared services are located on-premises.	DNS, DHCP and NTP Servers are located on-premises. Create firewall rule to allow traffic from VMware Cloud segments/workloads to these services.	Create a DFW rule to allow traffic between Workload VMs and DNS, DHCP and NTP Servers. DFW Rules in Infrastructure category is recommended for the shared services.
On-premises data center extension to VMware Cloud using HCX or Layer 2 VPN	Create a DFW rule to allow traffic between Workload VMs and the on-premises network, applications, or services. Gateway firewalls do not control any traffic over HCX/L2 extensions	Create a DFW rule to allow traffic between Workload VMs and the on-premises network, applications, or services. Gateway firewalls do not control any traffic over HCX/L2 extensions

Troubleshooting Considerations

Troubleshooting Considerations	Details
Logging	DFW Logs, once enabled are available as part of Aria Operations for Logs subscription
DFW default log setting is disabled by default and can only be enabled per rule	Enable logging rule by rule based on specific log requirements. With log enablement, log message will display the flow start, and then the flow end with the size/packet info. The logs are available as part of Aria Operations for Logs and once the log data daily limit is reached, no new log entries will be logged. For logs retention you may forward the logs to on-premises and SaaS destinations.
Distributed firewall reaches limit for maximum number of supported flows	A syslog message states that - the distributed firewall cannot create new connections due to the shortage. If the rule relating to the flow creation has logging turned on, a second message is generated to indicate that the packet was also dropped.
Distributed firewall virtual CPUs reach a maximum limit	Packets might start dropping. If logging is enabled for that flow, a log message is generated for the dropped packets.
Memory Availability	The VMware NSX distributed firewall must have enough memory to avoid dropping traffic. The firewall administrator will be notified of the lack of available memory by the following methods: An alert is sent when a new rule cannot be configured due to the memory shortage. In an All-Failure scenario, packets are discarded, and the distributed firewall operates in a fail-closed mode until the failure is remedied.
Traffic troubleshooting	Traceflow is a built-in utility available in NSX manager via UI/API on VMware Cloud
Traffic that is supposed to go through is getting dropped	Traceflow the source to destination. Traceflow displays DFW as one of the intermediate hops for the traffic that is passing or dropped by DFW with reason of failure.
Document	https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-A85621BC-1CFD-4703-846A-2B3D36E7ABAC.html?hWord=N4IghgNiBcIC4CcwGMCmAzCB7A7iAvkA
NSX Intelligence/Aria Operations for Log/Aria Operations for Networks	Discovers the applicable policies, groups, and services and detects suspicious activity. Check NSX Intelligence/Aria Operations documentation for additional details.