WHITE PAPER–JUNE 2019

NSX-T End User Computing Design Guide

NSX-T Data Center 2.5 and Horizon 7.9

vmware

Table of Contents

1. Intended Audience

This guide highlights design and deployment considerations when using NSX-T Data Center (NSX-T) to implement network virtualization, create a secure end user computing environment, and load balance Horizon infrastructure.

The intended audience is virtualization, networking, and security architects who are interested in deploying Horizon for virtual desktops and NSX in a vSphere environment. Solid conceptual understanding and hands-on experience with both NSX-T and Horizon products is recommended for successfully understanding this design guide. While this document is not specifically meant for comparing and contrasting the differences in NSX for vSphere (NSXv) and NSX-T, there may be times where the comparison is necessary to differentiate the two platform design differences as they relate to Horizon. NSX-T does provide additional benefits and simplicities to the overall Horizon and NSX-T deployment.

REVISION HISTORY		
Version	Updates	Comments
1.0	None	First Release

2. Introduction

The Software Defined Data Center (SDDC) is defined by server virtualization, storage virtualization, and network virtualization. Server virtualization has already proven the value of SDDC architecture by reducing costs and complexity of compute infrastructure. VMware NSX-T addresses the third critical pillar of SDDC, extending the same benefits obtained from the virtualization of compute to the data center network. NSX-T accelerates the provisioning of core network and security services, simplifying operations and improving economics.

With network virtualization, the functional equivalent of a network hypervisor, NSX-T reproduces the complete set of Layer 2 through Layer 7 networking services (e.g., switching, routing, firewalling, and load balancing) in software. It allows these services to be programmatically assembled in any arbitrary combination to produce unique, isolated virtual networks in a matter of seconds. NSX-T also provides a platform for various security services – both network and endpoint based. NSX-T provides various built-in services, including L2-L7 firewall and contextual-based security. Additionally, security vendors can leverage its Guest Introspection and Network Introspection frameworks to deliver service chained next-generation firewall, IDS/IPS, agentless anti-virus/anti-malware, file integrity monitoring, and vulnerability management capabilities.

Horizon delivers hosted virtual desktops and applications to end users through a single platform. These desktop and application services - including RDS-hosted applications, packaged applications with VMware ThinApp®, software-as-a-service (SaaS) applications, and virtualized applications from Citrix - can all be accessed from a single unified workspace across devices, locations, media, and connections. Leveraging closed-loop management and optimized for the software-defined data center, Horizon helps IT control, manage, and protect the Windows resources that end users want at the speed they expect while delivering the efficiency that business demands.

This design guide provides recommended practices and topologies to optimize interoperability between the NSX-T and Horizon platforms, enabling deployment of a secure end user SDDC environment. It is intended for customers who would like to utilize the benefits of network virtualization, micro-segmentation, and load-balancing in their brownfield/greenfield Horizon virtual desktop environment.

2.1 Horizon 7 Reference Architecture

All Horizon architecture information referenced in this document comes from the VMware Workspace ONE and VMware Horizon Reference Architecture.

2.2 NSX-T Design Guide

All NSX-T architecture information referenced in this document comes from the NSX-T Design Guide.

3. NSX-T and Horizon Architecture and Components

3.1 NSX-T Component Definitions

Before starting design discussions and recommendations, it makes sense to describe the fundamentals of NSX-T Data Center and the components associated with it for a complete understanding of how its features provide benefits to the Horizon platform. This section is not meant to be an exhaustive guide for covering NSX-T and every component. For a more in-depth look at the NSX-T components and design decisions, please reference the NSX-T Design Guide and official VMware NSX-T documentation.

3.1.1 NSX-T Architecture

NSX-T architecture consists of the following components:

- **NSX-T Manager Cluster**

  The NSX-T Manager Cluster is deployed as a virtual appliance in a set of three appliances for redundancy and scalability. The NSX-T Manager Cluster represents the Management and Control Plane of the NSX-T deployment. The NSX-T Manager Cluster operates a separate user-interface for administration unlike NSXv where it was managed through the vSphere Web Client.

- **Transport Node**

  A Transport Node is a device that is prepared with NSX-T and is participating in traffic forwarding.

  - **Edge Transport Node**

    The NSX-T Edge Node can be deployed in two form factors, as a virtual appliance in various sizes (Small, Medium, and Large) and also in a bare metal form factor. The NSX-T Edge Nodes provide North/South connectivity as well as centralized services such as NAT, Load Balancing, Gateway Firewall and Routing, DHCP, and VPN capabilities. NSX-T Edge Nodes provide pools of capacity for running these services.

  - **Hypervisor Transport Node**

    Hypervisor transport nodes are hypervisors prepared and configured to run NSX-T. The N-VDS provides network services to the virtual machines running on those hypervisors. NSX-T currently supports VMware ESXi and KVM hypervisors but also works on Bare Metal workloads as well.

- **NSX Virtual Distributed Switch (N-VDS)**

  The N-VDS is a software switch based on the ESXi vSwitch that provides switching functionality for NSX-T and is installed in the hypervisor, in the case of Horizon, VMware ESXi, and managed by NSX-T. The N-VDS provides the capability for building networks using overlay encapsulation/decapsulation. The N-VDS has similarities to the Virtual Distributed Switch that vCenter can build for ESXi hypervisors in concept, but is fully managed by NSX-T and has no dependency on vCenter or vSphere.

- **Transport Zone**

  An NSX-T Transport Zone represents the span of an NSX-T Segment and can be either an Overlay or VLAN type. It is associated with an N-VDS which binds it to a Transport Node.

- **NSX-T Segment**

The NSX Segment is virtual Layer 2 broadcast domain. Segments are created and attached to a Transport Zone. The span of a Segment is defined by the Transport Zone. An NSX-T Segment can either be a type Overlay or VLAN and inherits the type from the Transport Zone of which it's attached. An NSX-T Overlay Segment represents a software construct of a layer 2 broadcast domain. It can be associated with a network subnet and its default gateway is typically the tier-0 or tier-1 logical NSX-T router. A VLAN Segment represents a software extension of a physical layer 2 broadcast domain into the virtualized environment. The subnet ID of the underlying physical network is associated with the VLAN Segment, and the default gateway is typically the physical router that already provides the gateway in the underlay network.

- **NSX-T Kernel Modules**

  The NSX-T kernel modules are installed on each hypervisor that NSX-T is managing and build a distributed routing and firewalling model that scales out as a customer adds more hosts to their environment. Deploying NSX-T to the hypervisors installs the software packages that enable in-kernel routing and firewalling for local workloads. NSX-T manages these local firewalls and routing instances through the NSX-T Simplified UI.

NSX-T is broken up into 3 basic planes, Management, Control, and Data. Each of these planes is independent from the other. Loss of function in one plane does not equate loss of function in another plane. Figure 1 shows the NSX-T Logical architecture and the breakdown of the components in each plane.

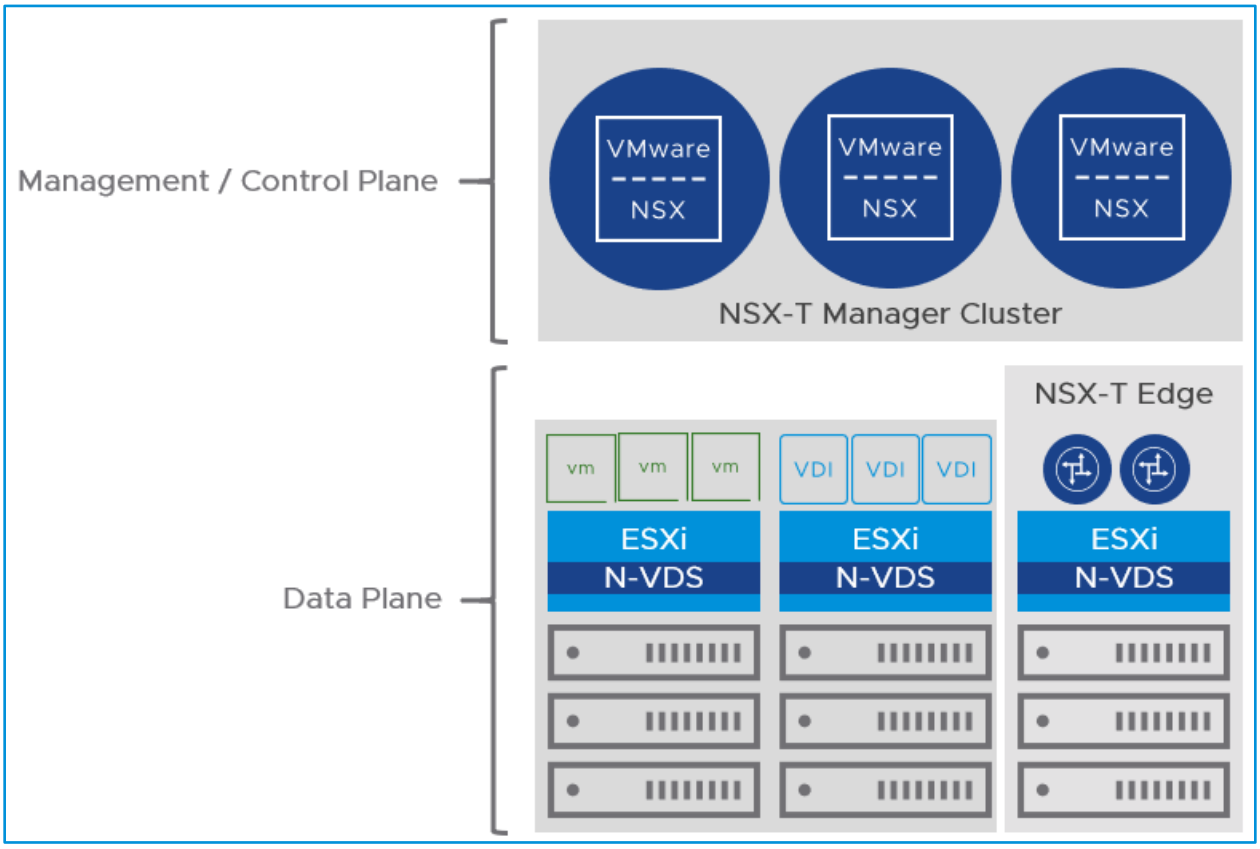

Figure 1 - NSX-T Architecture - Logical

Figure 2 shows the NSX-T internal logical architecture of the NSX-T components that are installed into the hypervisor as well as the distributed services that reside in all NSX-T prepared hypervisors.

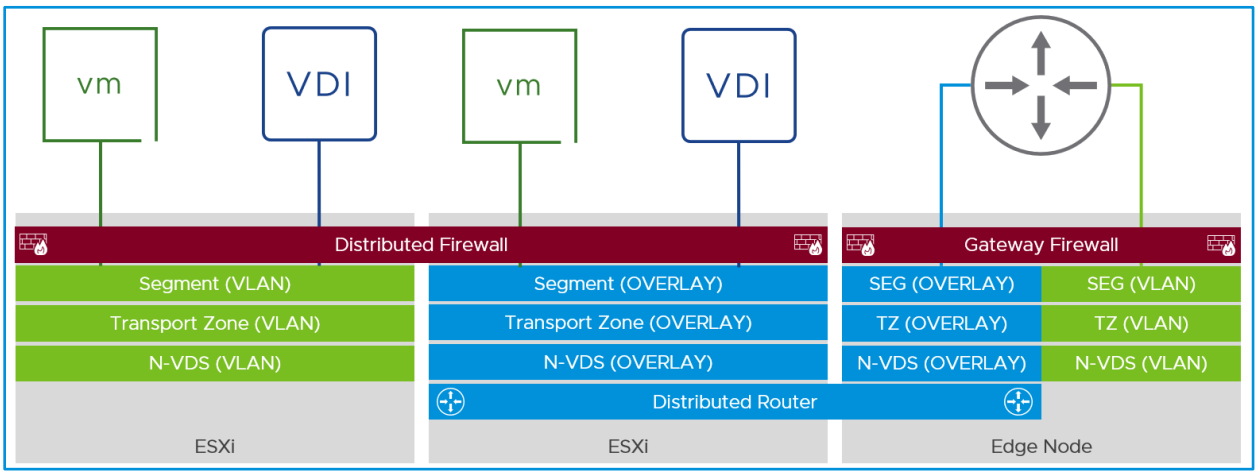

Figure 2 - NSX-T Internal Hypervisor Architecture - Logical

3.2 Horizon Core Component Definitions

Being able to design an NSX-T deployment for Horizon requires basic understanding with how Horizon deployments are architected and built for scalability as well as an understanding of the core architecture of Horizon. The core architecture of Horizon consists of the following components:

- **Horizon Client**

Client-device software that allows a physical device to access a virtual desktop or RDSH-published application in a Horizon 7 deployment. You can optionally use an HTML client for devices for which installing software is not possible.

- **Horizon Agent**

A software service installed on the guest OS of all target VMs, physical systems, or RDSH servers. This allows them to be managed by Connection Servers and allows a Horizon Client to form a protocol session to the target VM.

- **Horizon Console**

A web application that is part of the Connection Server, allowing administrators to configure the server, deploy and manage desktops, control user authentication, initiate and examine system and user events, carry out end-user support, and perform analytical activities.

- **Horizon Connection Servers**

An enterprise-class desktop management server that securely brokers and connects users to desktops and published applications running on VMware vSphere® VMs, physical PCs, blade PCs, or RDSH servers.

Authenticates users through Windows Active Directory and directs the request to the appropriate and entitled resource.

- **Horizon Unified Access Gateways**

Virtual appliance that provides a method to secure connections in access scenarios requiring additional security measures, such as over the Internet.

- **Horizon RDSH Servers**

Microsoft Windows Servers that provide published applications and session-based remote desktops to end users.

- **Horizon Virtual Desktops**

Microsoft or Linux-based operating system desktops that provide digital workspaces that can be delivered on-demand.

- **vSphere and vCenter Servers**

The vSphere product family includes VMware ESXi™ and vCenter Server, and it is designed for building and managing virtual infrastructures. The vCenter Server system provides key administrative and operational functions, such as provisioning, cloning, and VM management features, which are essential for VDI.

3.2.1 Horizon Architecture - Pod and Block

Horizon instances are deployed in pods and divided into multiple blocks in order to scale the Horizon deployment. Each pod contains two physical blocks – the Horizon Management Block and Horizon Resource Block. Figure 4 shows the logical Horizon pod topology.

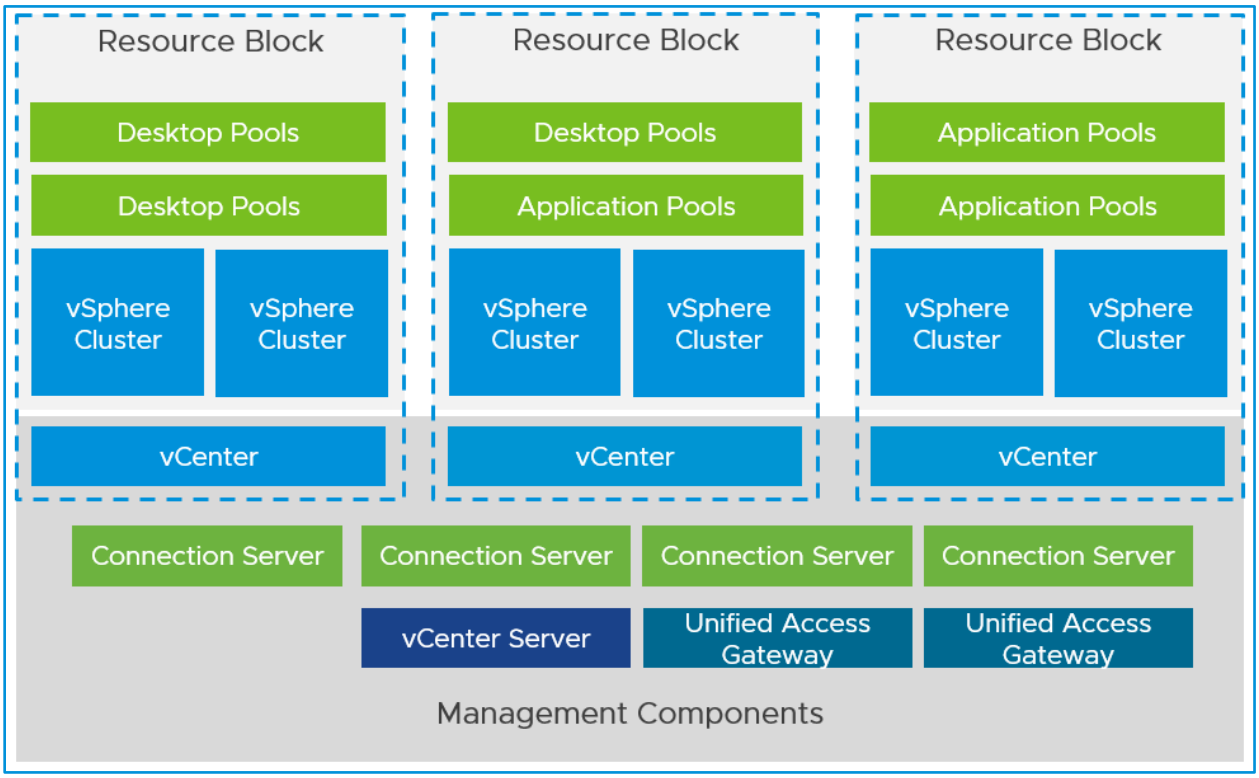

Figure 3 - Horizon Pod Configuration - Logical

The Horizon Management Block consists of VMware ESXi hosts that contain all the management components deployed for the Horizon infrastructure. The Horizon Desktop Block contains the ESXi hosts where virtual desktops will be created. Each of the blocks is managed by a separate vCenter Server that manages each block independently.

Horizon consists of other components that make up an enterprise deployment of Horizon.

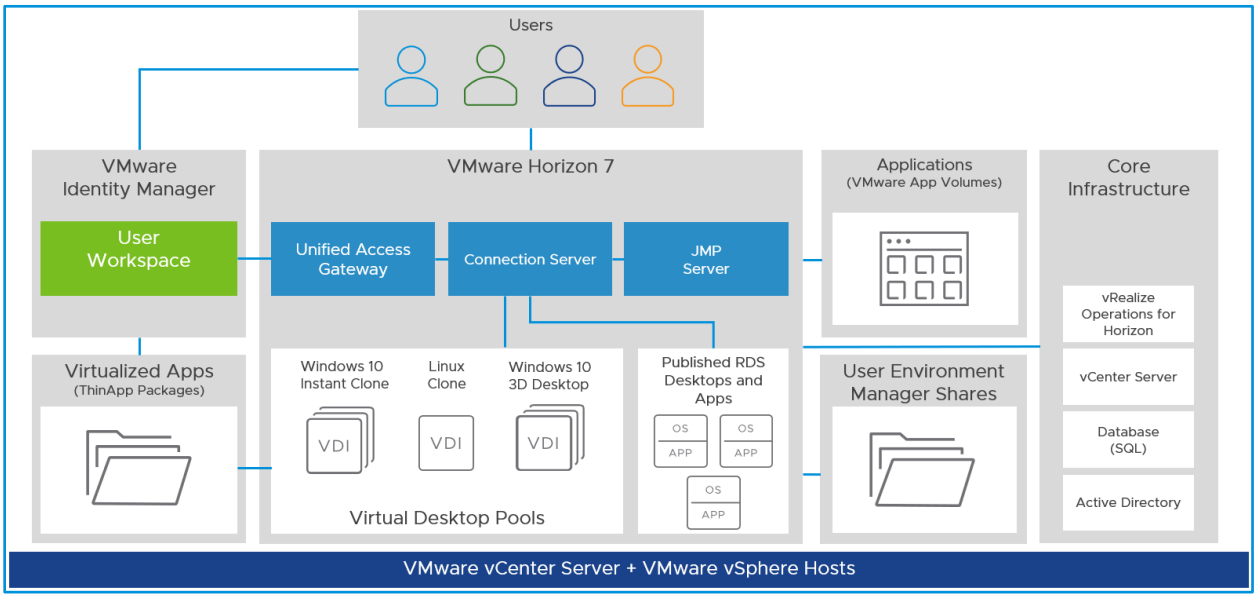

Figure 4 - Horizon Enterprise Deployment Topology

For more details about what each of these components do, design decisions, and recommendations, take a look at the VMware Workspace ONE and VMware Horizon Reference Architecture design where they are defined.

4. NSX-T and Horizon Use Cases

The Horizon suite of products supports several features and deployment options for the desktop infrastructure it provides for areas such as rapid deployment agility, security, and availability. When coupled with NSX-T, the Horizon platform can take advantage of several features that NSX-T can provide in the areas of contextual security, edge and partner services, and network virtualization.

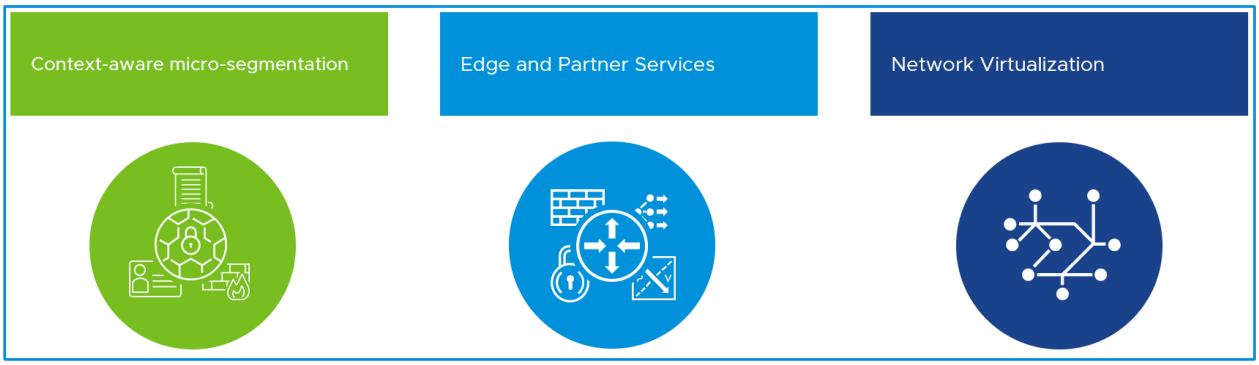

Figure 5 - NSX-T Use Cases for Horizon

Figure 5 showcases the features that NSX-T provides for a Horizon end user computing environment.

- **Context-aware micro-segmentation**

NSX-T provides contextual security solutions for micro-segmentation of Horizon VDI workloads by providing granular Layer 2 through Layer 7 firewalling capabilities between workload VMs and also providing user-based context for VDI and Remote Desktop Session Host (RDSH) workloads.

- **Edge and Partner Services**

  NSX-T provides software solutions for Equal Cost Multipath (ECMP), NAT, SSL-Offloading, DHCP Relay, Gateway Firewalling and Routing, and Load Balancing for the Horizon infrastructure and the workloads Horizon manages and deploys. NSX-T also provides the Guest and Network Introspection platform for 3rd party partners to inject their services such as IDS/IPS, agent-less Anti-Virus/Malware, and Next-generation Firewalling capabilities.

- **Network Virtualization**

  NSX-T provides core networking services in software (e.g., switching and routing) that can be automatically provisioned to create various topologies. This allows for elastic spin up of new desktop pools or expansion of pools in an existing infrastructure. Network virtualization is also a key tenant of micro-segmentation, enabling the rapid provisioning of isolated network segments.

5. NSX-T Features for Horizon

5.1 NSX-T Virtual Networking for Horizon

NSX-T provides network virtualization capabilities using industry standard GENEVE encapsulated overlay networks. This section examines design considerations for a logical topology deployment of Horizon on an overlay network. It covers deploying both the Horizon infrastructure components and Horizon desktop pools connected to overlays created by NSX. Network virtualization requires a basic understanding of how switching and routing are done with NSX-T. Below are the components associated with NSX-T network virtualization and how they can be used together in a Horizon design.

- **NSX-T Logical Routing**

  NSX-T provides capabilities to interconnect both physical and virtual workloads in different logical Layer 2 networks. NSX-T does this using software to create these logical constructs and embeds them into the hypervisor layers, abstracted from the physical hardware. Since these network elements are logical entities, multiple logical routers can be created in an automated and agile fashion. NSX-T routing is instantiated for East/West traffic flows in a distributed manner within each hypervisor. NSX-T routing is instantiated for North/South traffic flows in a centralized manager within the NSX-T Edge Node.

- **NSX-T Two-Tier Routing**

  In addition to providing optimized distributed and centralized routing functions, NSX-T supports a multi-tiered routing model with logical separation between provider router function and tenant routing function. The concept of multi-tenancy is built into the routing model. The top-tier logical router is referred to as tier-0 while the bottom-tier logical router is tier-1. This structure gives both provider and tenant administrators complete control over their services and policies. The provider administrator controls and configures tier-0 routing and services, while the tenant administrators control and configure tier-1. Configuring two tier routing is not mandatory and NSX-T Segments can be attached to the Tier-0 Gateway just like they can with a Tier-1 Gateway.

- **NSX-T Segment**

  The NSX Segment is virtual Layer 2 broadcast domain. Segments are created and attached to a Transport Zone. The span of a Segment is defined by the Transport Zone. An NSX-T Segment can either be a type Overlay or VLAN and inherits the type from the Transport Zone of which it's attached. It can be associated with a network subnet and its default gateway is typically the tier-0 or tier-1 logical NSX-T router. A VLAN Segment represents a software extension of a physical layer 2 broadcast domain into the virtualized environment. The subnet ID of the underlying physical network is associated with the VLAN Segment, and the default gateway is typically the physical router that already provides the gateway in the underlay network.

5.1.1 NSX-T Networking Logical View

The following Figures, showcase the logical view of how the NSX-T Routing functions work in relation to the description above.

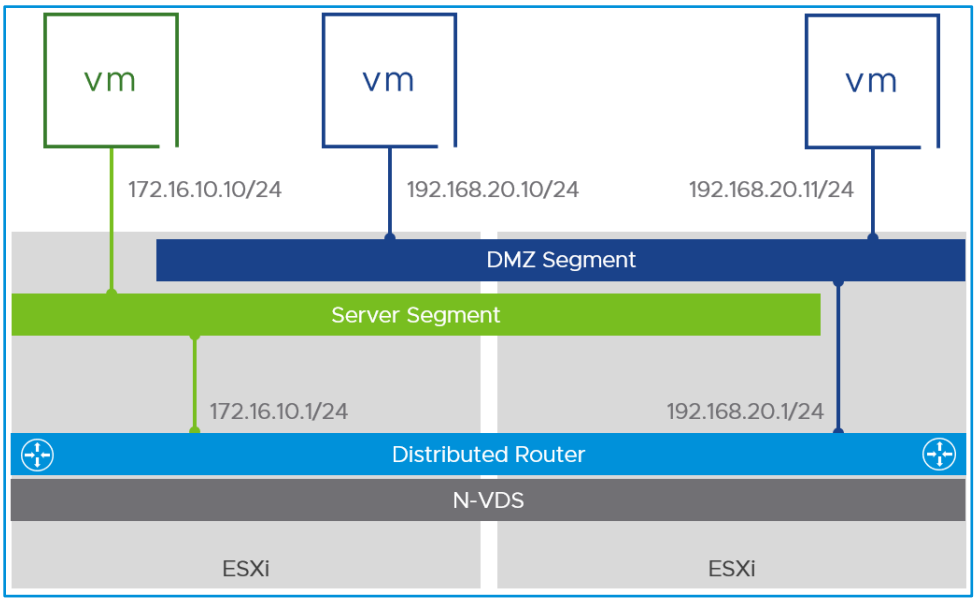

Figure 6 - NSX-T East/West Logical Routing in the Same and Across Hypervisors

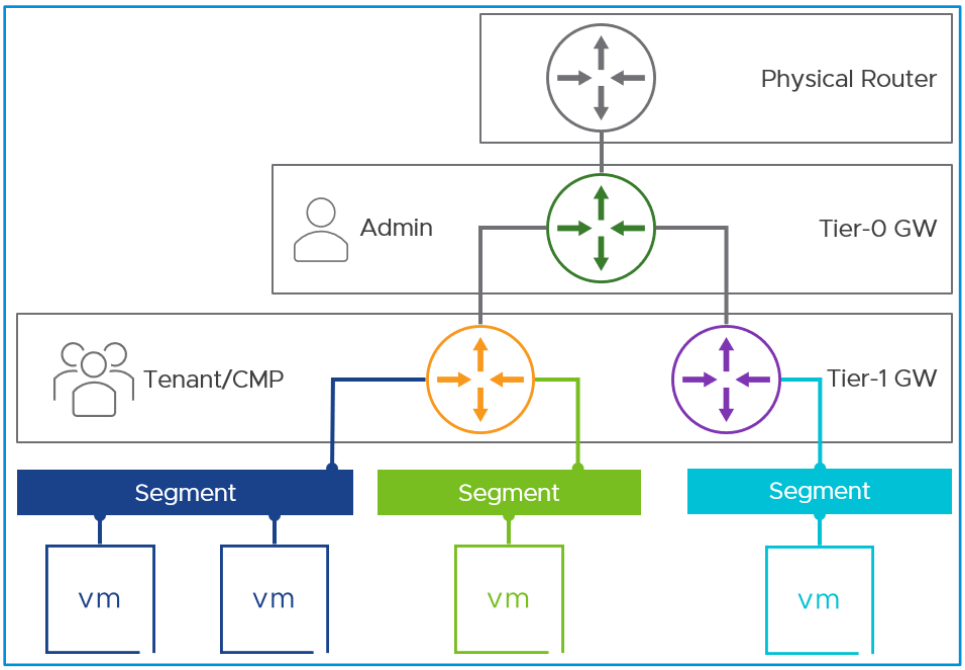

Figure 7 - NSX-T Two-Tier Logical Routing

5.2 NSX-T Security for Horizon

NSX-T provides several security benefits to enhance an existing or new Horizon deployment for the Horizon infrastructure machines, RDSH Farms and VDI desktops pools. In a virtual desktop infrastructure, it is difficult to provide security at a granular level be it, user-based, application-based, or function-based. NSX helps secure desktop pools and allow communications as necessary based on the context of the communication, to applications that should be allowed, and denies the rest. NSX-T is able to provide this level of security by using a concept called Context-aware micro-segmentation.

Context-aware micro-segmentation provides three foundational security capabilities: Isolation, Segmentation, and Advanced Services.

- **Network Isolation**

Isolation is the foundation of most network security, whether for compliance, containment, or separation of distinct operational environments. Manually configured and maintained routing, ACLs, and firewall rules on physical devices have traditionally been used to establish and enforce isolation and multi-tenancy. These properties are now inherent to network virtualization. Virtual networks (e.g., leveraging GENEVE technology) are isolated from other virtual networks as well as from the underlying physical infrastructure by default, delivering the security principle of least privilege. Virtual networks are created in isolation and remain isolated unless specifically connected. No physical subnets, VLANs, ACLs, or firewall rules are required to enable this isolation.

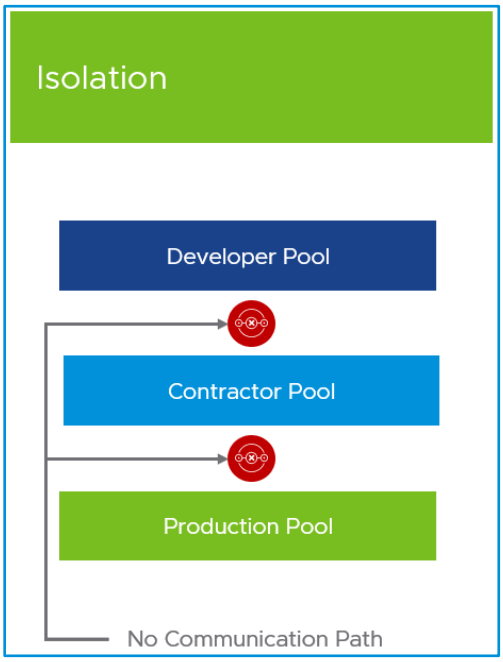

Figure 8 - Micro-segmentation Isolation Concept

Any isolated virtual network can be made up of workloads distributed anywhere in the data center. Workloads in the same virtual network can reside on the same or separate hypervisors. Additionally, workloads in several multiple isolated virtual networks can reside on the same hypervisor. Isolation between virtual networks allows for overlapping IP addresses. This makes it possible to have isolated development, test, and production virtual networks - each with different application versions but with the same IP addresses - all operating at the same time and on the same underlying physical infrastructure. Virtual networks are also isolated from the underlying physical network. Since traffic between hypervisors is encapsulated, physical network devices operate in a distinct address space from the workloads connected to the virtual networks. A virtual network could support IPv6 application workloads on top of an

IPv4 physical network. This isolation protects the underlying physical infrastructure from possible attack initiated by workloads in any virtual network, independent from VLANs, ACLs, or firewall rules that would traditionally be required to create this isolation.

- **Network Segmentation**

Segmentation is related to isolation, but applied within a multi-tier virtual network. Network segmentation is traditionally a function of a physical firewall or router, designed to permit or deny traffic between network segments or tiers (e.g., segmentation between a web, application, and database tiers). Traditional processes for defining and configuring segmentation are time consuming and highly prone to human error, resulting in a large percentage of security breaches. Implementation requires deep and specific expertise in device configuration syntax, network addressing, application ports, and protocols.

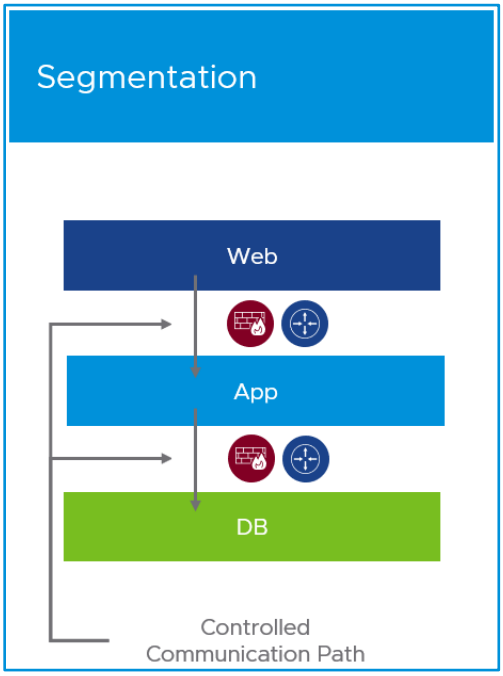

Figure 9 - Micro-segmentation Segmentation Concept

Network segmentation, like isolation, is a core capability of VMware NSX network virtualization. A virtual network can support a multi-tier network environment, either multiple L2 segments with L3 segmentation or a single-tier environment where workloads are all connected to a single L2 segment using distributed firewall rules. Both scenarios achieve the same goal of micro-segmenting the virtual network to offer workload-to-workload traffic protection, also referred to as east-west protection.

- **Advanced Services**

NSX-T as a security platform provides Layer 2 – Layer 7 stateful firewalling features that deliver segmentation within virtual networks. Some customers require more advanced network security capabilities; these environments can leverage VMware NSX-T to distribute, enable, and enforce advanced network security services in a virtualized network environment. NSX-T distributes network services into the vNIC context to form a logical pipeline of services applied to virtual network traffic. Third party network services can also be inserted into this logical pipeline, supporting integration of both physical and virtual services.

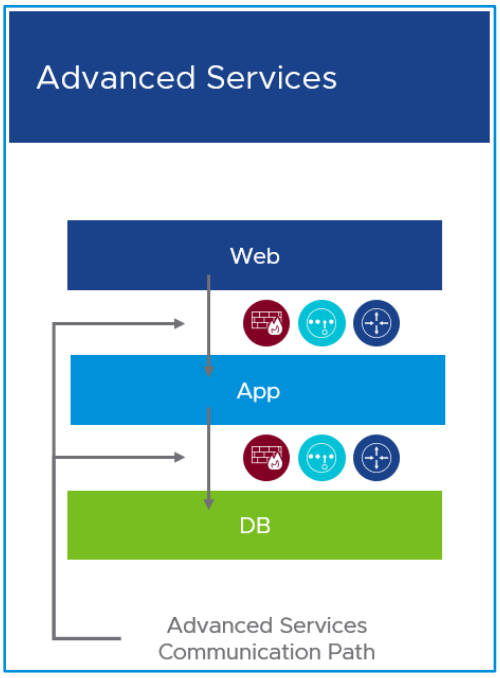

Figure 10 - Micro-segmentation Advanced Services Concept

Security teams use specific combinations of network security products to meet the needs of their unique environments. Network security teams are often challenged to coordinate and integrate network security services from multiple vendors. A powerful benefit of NSX-T is its ability to build policies that leverage Guest Introspection and Network Introspection through service insertion to drive service execution in the logical services pipeline based on the result of other services. This functionality makes it possible to coordinate otherwise completely unrelated network security services from multiple vendors.

5.2.1 NSX-T Context Micro-segmentation for Horizon

One of the main use cases for NSX-T security for Horizon is around the use of micro-segmentation to provide granular security around the Horizon infrastructure and RDSH Farms and VDI desktop pools. NSX-T provides the following capabilities that enable context micro-segmentation for Horizon environments:

- **Distributed Stateful and Identity Firewalling**

A topology agnostic segmentation approach that reduces the attack surface within the data center perimeter through the NSX-T Distributed Firewall (DFW). This functionality operates on a per-workload regardless of the underlying L2 network topology offering Layer 2-7 security as well as Active Directory User Group per-user context.

- **Centralized and Granular Policy Control**

NSX-T provides a single user-interface and single RESTful API entry point for interacting and distributing security policy across the Horizon deployment. NSX-T Groups can be configured with a variety of different combinations of object constructs for granular use. Examples include: VM Name, OS Name, Active Directory Group, Segment, Segment Port, and IP Sets.

- **Overlay Network Isolation and Segmentation**

NSX-T provides logical network-based isolation and segmentation that can span racks or data center regardless of underlying network hardware. Also enables integration with 3rd party solutions for IDS/IPS and Guest Introspection capabilities.

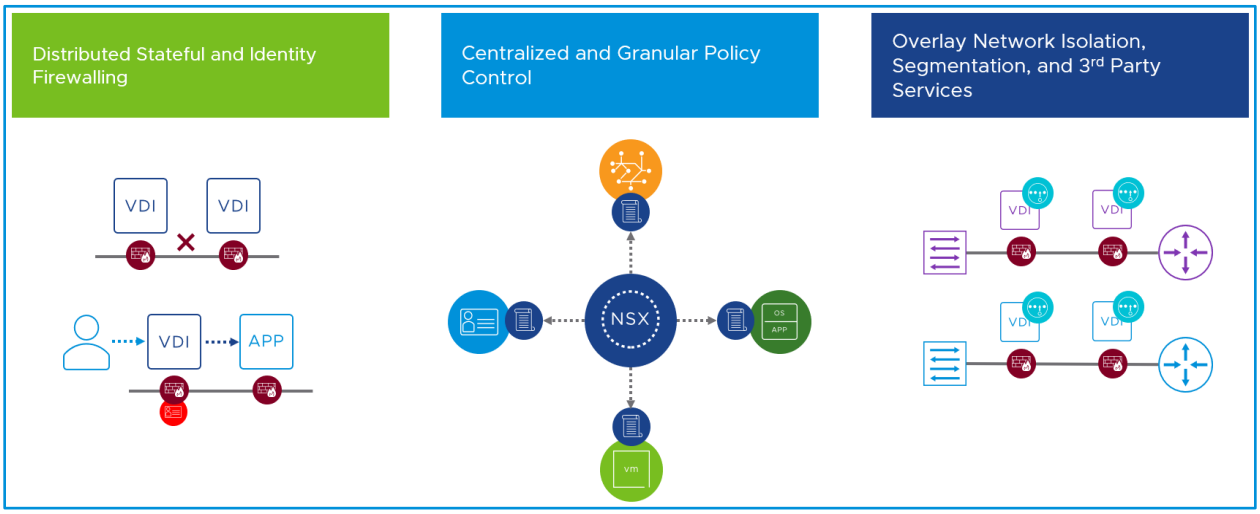

Figure 11 - NSX-T and Horizon Benefits

Taking these main use cases, we can apply them to provide various protections around the Horizon components and infrastructure.

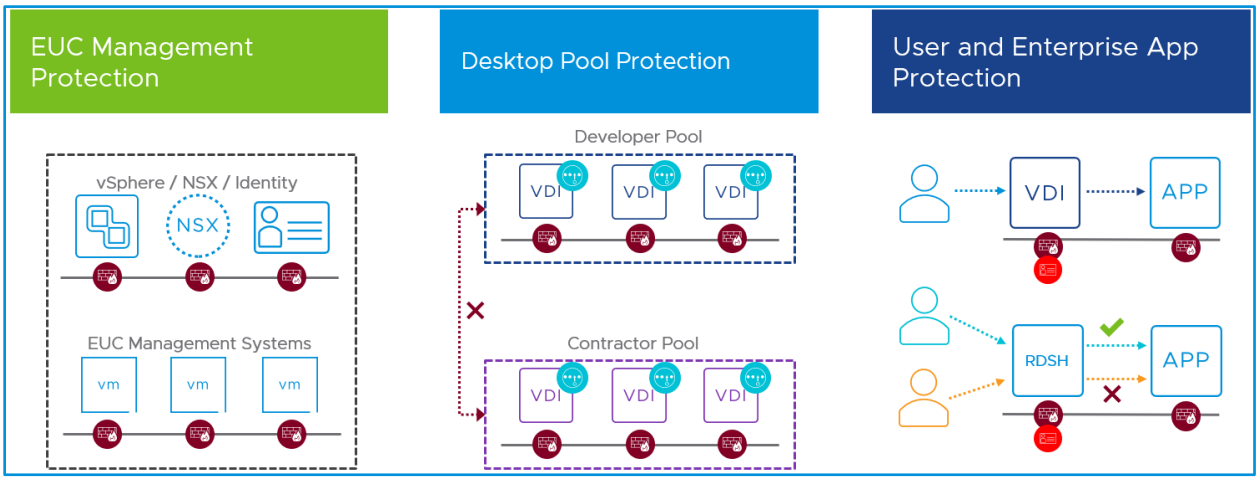

Figure 12 - NSX-T Use Cases for Horizon

- **EUC Management Protection**

The Horizon Management infrastructure consists of multiple components whose interaction allow administrators to provision desktops and users to connect to them. NSX-T secures inter-component communication within this infrastructure.

- **Desktop Pool Protection**

Virtual desktops rarely need to communicate with each other and some organizations may require external contractors have their own desktop pool to connect into. NSX-T secures the communications between desktops in the same pool and between desktops in different pools creating complete isolation based on requirements. NSX-T also provides desktop machines with access to 3rd party services such as IDS/IPS and Guest Introspection to off-load additional security protections.

- **User and Enterprise App Protection**

NSX-T allows user level context micro-segmentation using the identity of the user to allow or disallow access from the desktop or RDS host to the enterprise application. This enables creation of fine-grained access control and visibility for each desktop or RDSH session based on the individual user.

5.2.2 Context-aware Micro-segmentation Design Methodologies

Designing a micro-segmentation security posture starts with identifying the methodology in building the security posture. There are three approaches that can be used:

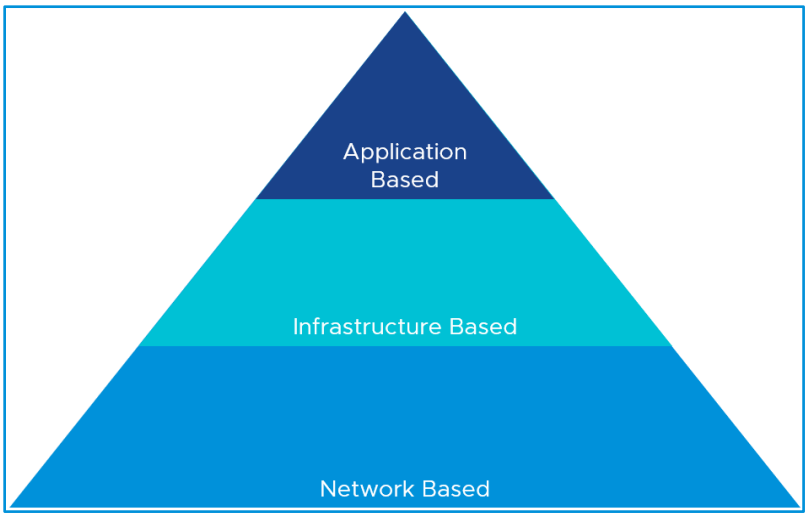

Figure 13 - Micro-segmentation Methodologies

- **Application Based**

The policies created are application-centric and tend to group by the logical constructs with how an application is composed, i.e. Web, App, and DB Tiers of the application. Advanced Services are typically used in these policies as they focus on the context and users associated with using the application. Application Based policies are best used when the data center is highly dynamic with workloads moving around.

- **Infrastructure Based**

The policies created are infrastructure-centric with a focus on the logical constructs of the data center, i.e. Segments, Segment Ports, etc. Data centers in these cases are usually static with very little change to the logical structure of the networking.

- **Network Based**

Network based policies are very similar to traditional security approaches that focus on IP and MAC addresses are their logical constructs.

Horizon deployments could use any one of these approaches, however an Application Based approach would provide the most flexibility in terms of consistent policy model in the data center. Highly virtualized customers have workloads that can be under constant movement from virtual host to virtual host. NSX-T security policies follow the virtual workloads regardless of location or context.

5.2.3 NSX-T Distributed Firewall

The NSX-T Distributed Firewall is the component that provides the bulk of the security functionality for Horizon. The DFW is a distributed component of NSX-T that resides in every hypervisor that is prepared with NSX-T. Every workload that is hosted on the VMware ESXi host has a stateful Layer 2 – Layer 7 contextual firewall in line with its virtual network card.

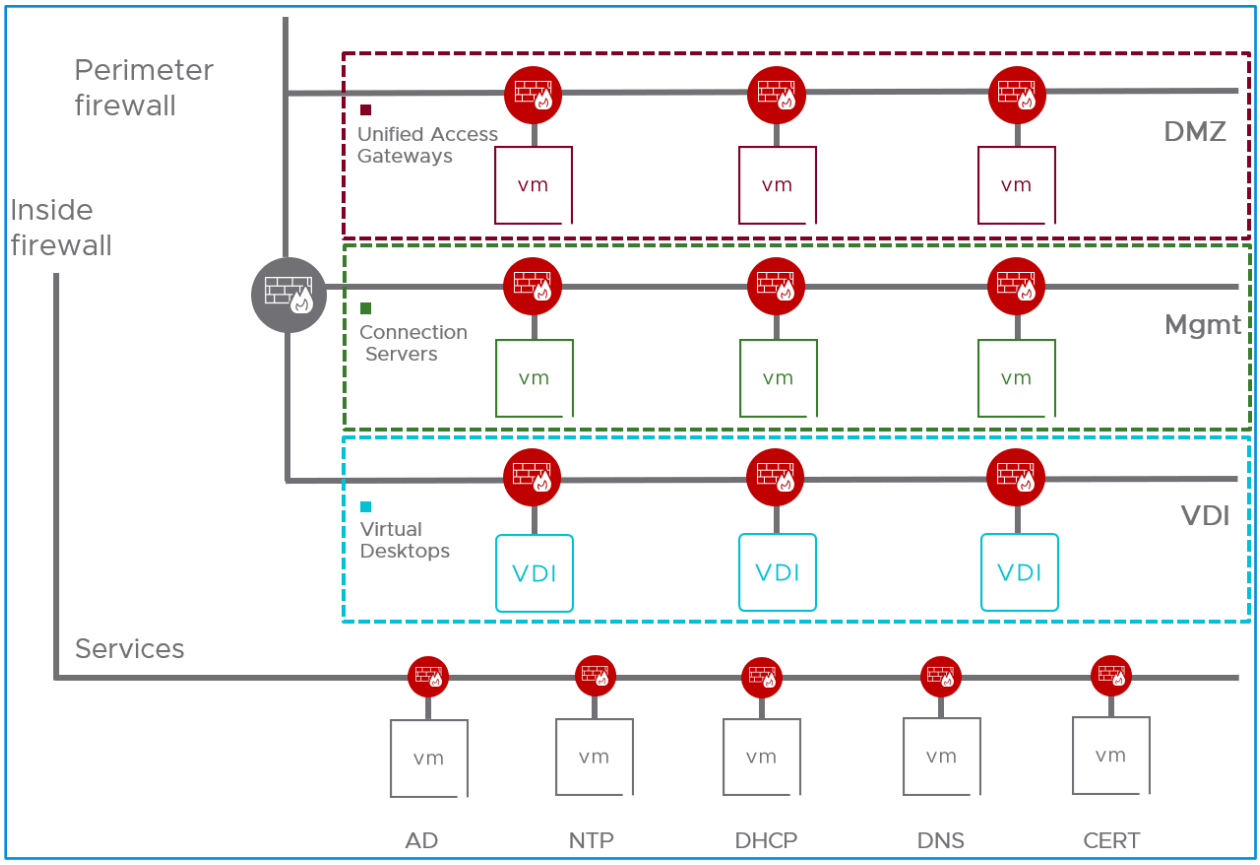

Figure 14 - NSX-T Granular Policy Distribution

5.2.3.1 NSX-T Distributed Firewall Security Definitions

NSX-T has several security components that are used in building an NSX-T Security Policy. The following chart explains what each security component is, and what it does:

SECURITY TERMINOLOGY	
Construct	Definition
Security Policy	A security policy includes various security elements including firewall rules and service configurations. Policy was previously called a firewall section.
Rule	A set of parameters with which flows are evaluated against, and define which actions will be taken upon a match. Rules include parameters such as source and destination, service, context profile, logging, and tags.

Group	Groups include different objects that are added both statically and dynamically, and can be used as the source and destination field of a firewall rule. Groups can be configured to contain a combination of virtual machines, IP sets, MAC sets, segment ports, segments, AD user groups, and other nested groups. Dynamic inclusion of groups can be based on tag, machine name, OS name, or computer name. Groups were previously called Group or security group.
Service	Defines a combination or port and protocol. Used to classify traffic based on port and protocol. Pre-defined services and user-defined services can be used in firewall rules.
Service Entry	Defines the type of service, IP, IGMP, ICMPv4, ICMPv6, ALG, TCP, UDP, and Ether
Context Profile	Defines context aware attributes including APP-ID and domain name. Also includes sub attributes such as application version, or cipher set. Firewall rules can include a context profile to enable Layer-7 firewall rules.

5.2.3.3 NSX-T Distributed Firewall Connectivity Strategy

NSX-T provides a mechanism for security policy to have a default connectivity strategy for a customer firewall policy set. By choosing any of these options, NSX-T will automatically place a default explicit allow or deny rule at the bottom of the Distributed Firewall. The following table discusses the options available:

DISTRIBUTED FIREWALL CONNECTIVITY STRATEGY	
Strategy	Definition
Blacklist with/without Logging	This is the default option and creates an allow-all rule on the DFW. Capable of being used with and without logging.
Whitelist with/without Logging	Creates a deny-all traffic firewall rule. Only communication from sites or applications that have been defined in the firewall rules is allowed, and all other communication is denied access. This include DHCP traffic as well. Capable of being used with and without logging.
None	Select this option to disable both blacklisting or whitelisting of firewall rules. This is useful if you have a set of rules already configured using previous versions of NSX-T Data Center.

The DFW for NSX-T operates much like a traditional firewall with a top-down approach to rule enforcement. NSX-T also offers various categories in which to group DFW security policies. These categories modify the workflow with how an NSX-T DFW security policy is enforced from not only top-down, but left-right. Traffic flows are evaluated on category first then on security policies contained in that category, until a match is made.

DISTRIBUTED FIREWALL CATEGORIES	
Category	Definition
Ethernet	Used for Layer 2 based rules
Emergency	Use for quarantine and allow rules
Infrastructure	Define access to shared services. Global Rules – AD, DNS, NTP, DHCP, Backup, Management Servers
Environment	Rules between zones – production vs development, inter-business unit rules

Application	Rules between applications, application tiers, or the rules between micro services

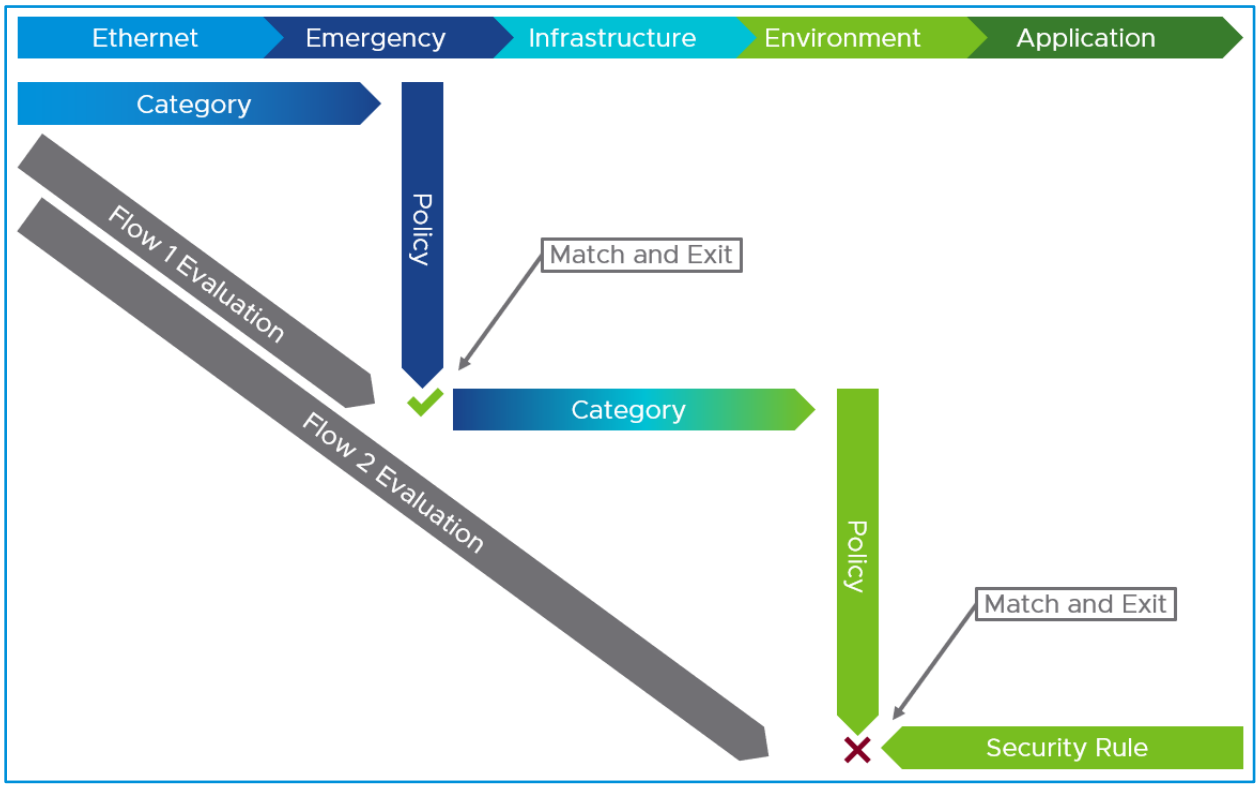

Figure 15 - NSX-T Firewall Rule Processing Workflow

5.2.3.4 NSX-T Distributed Firewall Enforcement

The NSX-T DFW provides enforcement using a multi-tuple configuration for the security rules that are built. The DFW can use network context in the form of Layer 2 to Layer 4 port, protocol, source and destination for writing rules. The DFW can expand the traffic flow context past 5-tuple to Layer 7 App ID as well. The following diagram depicts how the NSX-T DFW works with a typical Horizon protocol, Blast. Using this approach greatly simplifies the number of rules necessary to provide micro-segmented security around the Horizon infrastructure and desktops.

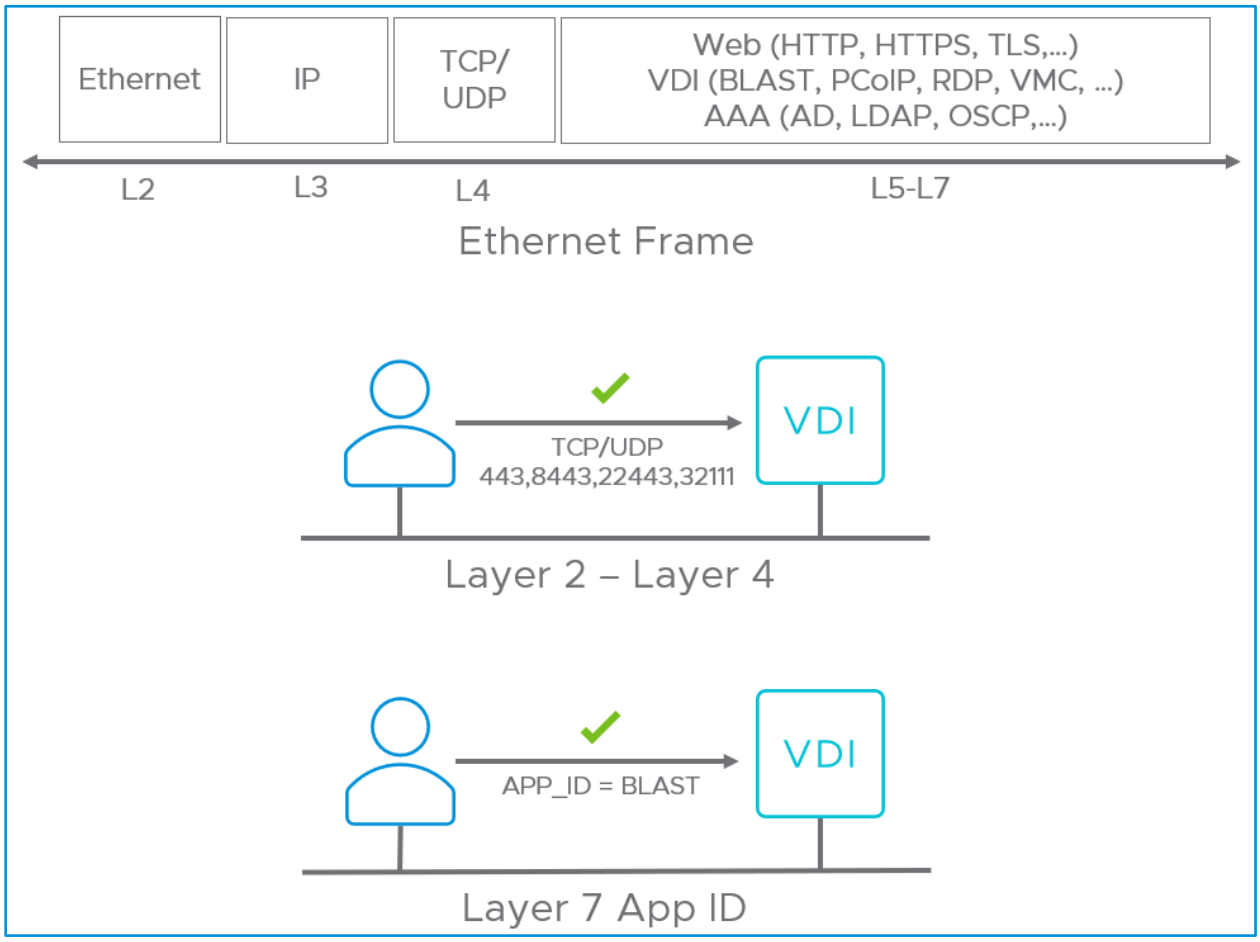

Figure 16 - NSX-T and Horizon Firewall Traffic Identification

5.2.4 NSX-T Identity Firewall

User-based context provided by the NSX-T platform enhances the Distributed Firewall to function with Identity Firewalling (IDFW) capabilities. The NSX-T IDFW couples user information from Microsoft Active Directory (AD) and the NSX-T DFW to allow administrators to create firewall security rules using AD Groups as the source and control communications between NSX-T protected systems by the user logged into a system. Users that log into Horizon virtual desktops or RDS hosts, can now have their allowed communication behavior controlled on a per-user granular basis. Virtual desktop systems are typically a 1:1 user to desktop relationship, but RDS hosts can have multiple users logged into the same RDS host at the same time. NSX-T IDFW can control each user granularly regardless how many users are logged into the same RDS host.

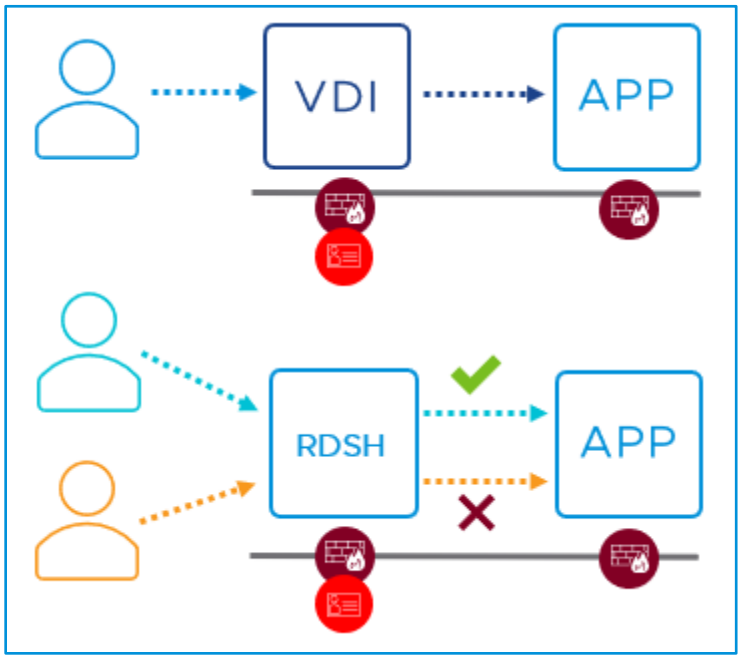

Figure 17 – NSX-T Identity Firewall for VDI and RDSH Use Case

Identity Firewall can be enabled cluster and host independent. While it is enabled globally in the NSX-T UI, it can be constrained to specific hosts added as standalone hosts or clusters of hosts based on the Compute Managers that NSX-T is connected to. This is especially useful for Horizon VDI and RDS Hosts, as the administrator does not have to enable Identity Firewall on clusters that are not consuming it, only on the clusters where it might require, i.e. VDI and RDS Host workload clusters.

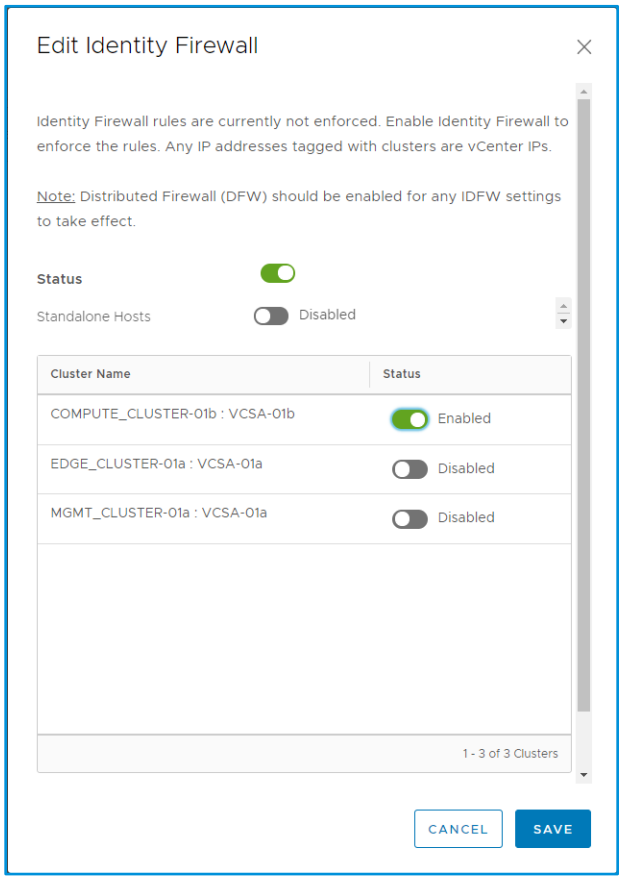

Figure 18 - Enable Identity Firewall in NSX-T

Identity Firewall requires a connection and only supports Microsoft Active Directory. Refer to the NSX-T Administration guide for guidance on the supported OS types for IDFW and Domain Controllers.

The NSX-T Identity Firewall processes the user identity at the Source only in DFW rules. General guidance in creating a security policy around using the IDFW is the following example:

HORIZON IDFW SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon – VDI/RDSH IDFW Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
AD Group 1 to Web App	AD_GRP_1	WEB-APP-GRP	HTTPS	HTTPS	VDI-GRP RDSH-GRP	Allow
Block All	Any	WEB-APP-GRP	Any	Any	VDI-GRP RDSH-GRP	Block

Horizon – Web App Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Web App	VDI/RDSH	Web App	HTTPS	HTTPS	WEB-APP-GRP	Allow

This policy performs the following:

- Section 1
    - Allows a User in the AD_GRP_1 NSX Group to communicate with the Web App over HTTPS and applies the security policy to the VDI/RDSH.
    - Blocks any other communications from VDI/RDSH to Web App and applies the security policy to VDI/RDSH.
- Section 2
    - Allows the VDI/RDSH to communicate to the Web App over HTTPS and applies the security policy to the Web App. Functionally only allows inbound communications from VDI/RDSH to Web App.

The use of Applied To in these examples shows how you can constrain IDFW without using directionality from DFW rules.

5.2.5 NSX-T Security Consumption

NSX-T Security is easily consumed using native NSX-T and vSphere objects.

- **Inventory**

NSX-T keeps track of the objects it knows about by using an extensive list of services, groups, virtual machines, and context-profiles and keeps them in Inventory. The Information stored in the NSX-T inventory and can be used as an object with which security policy can be consumed with.

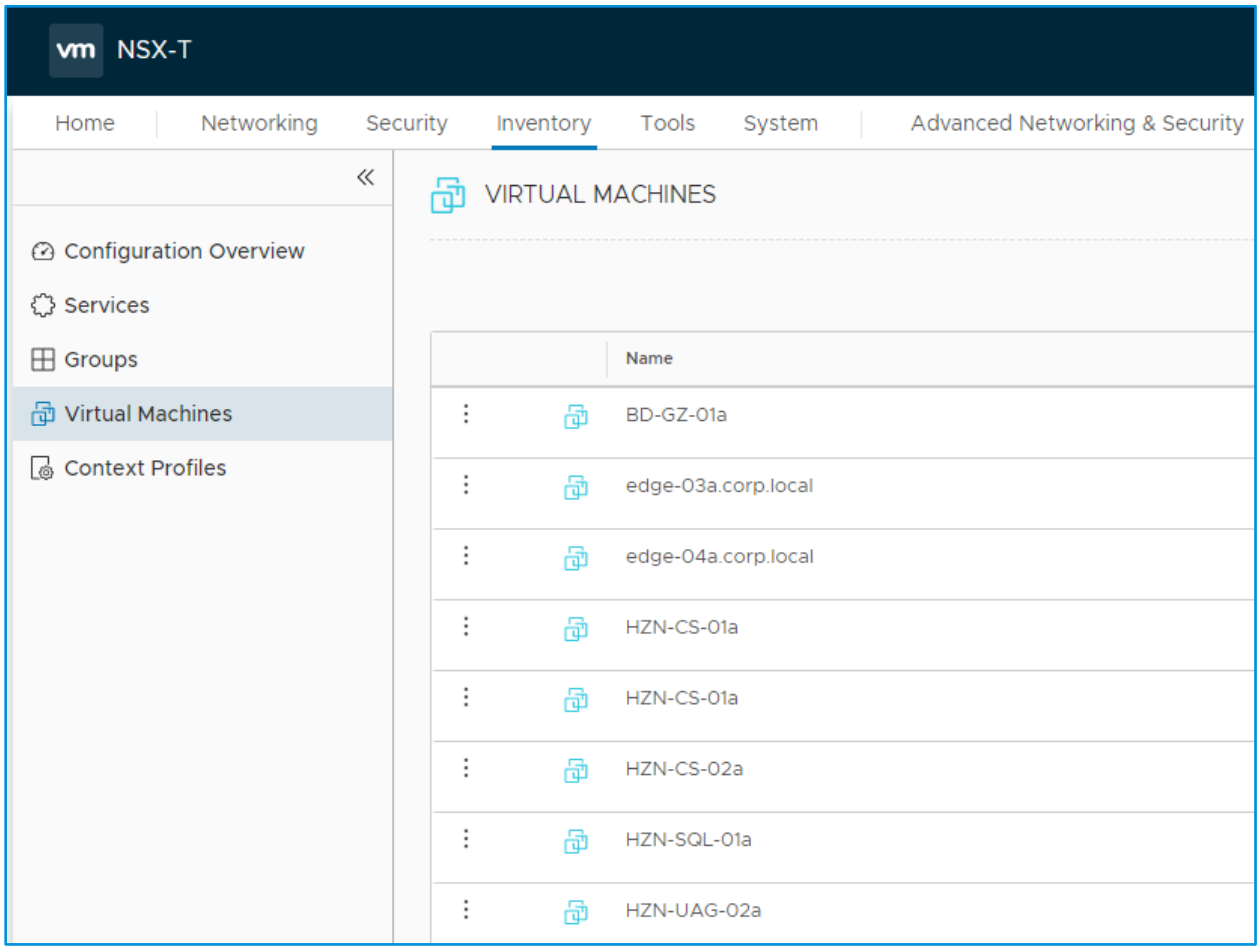

Figure 19 - NSX-T Inventory Objects - Virtual Machines

- **Tags**

NSX-T has the ability to place a tag onto many types of objects in NSX-T. Tags can be used in searching for objects, as criteria for grouping, or for applying a specific scope to an object. Tags are dynamic in nature, can be updated on the fly which can modify the status of an NSX-T object. Tags can also be used by 3rd party services to apply a specific tag and are an essential part of applying security with NSX-T.

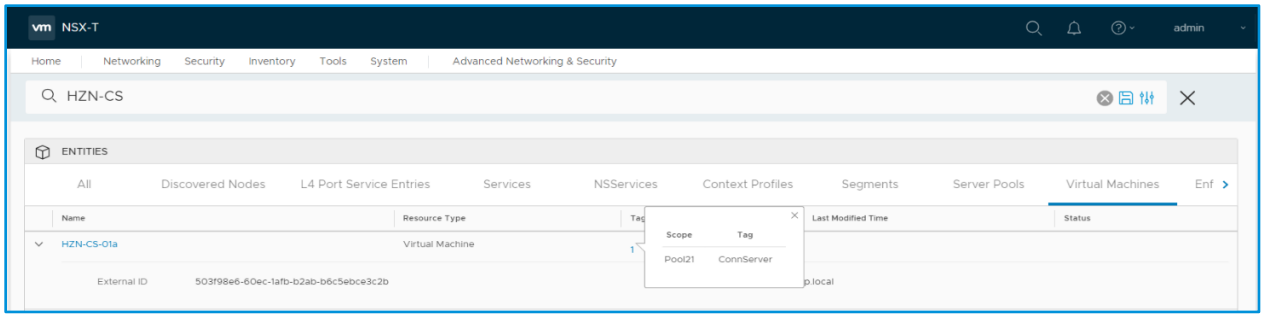

Figure 20 - NSX-T Inventory Objects - Tags

- **Groups**

Groups include different objects that are added both statically and dynamically and can be used as the source and destination field of a firewall rule. Groups can be configured to contain a combination of virtual machines, IP sets, MAC sets, logical ports, segments, Active Directory user groups, and other nested groups. Dynamic inclusion of groups can be based on tag, machine name, OS name, or computer name. A single ID based group can be used within a firewall rule. If IP and ID based groups are needed at the source, create two separate firewall rules.

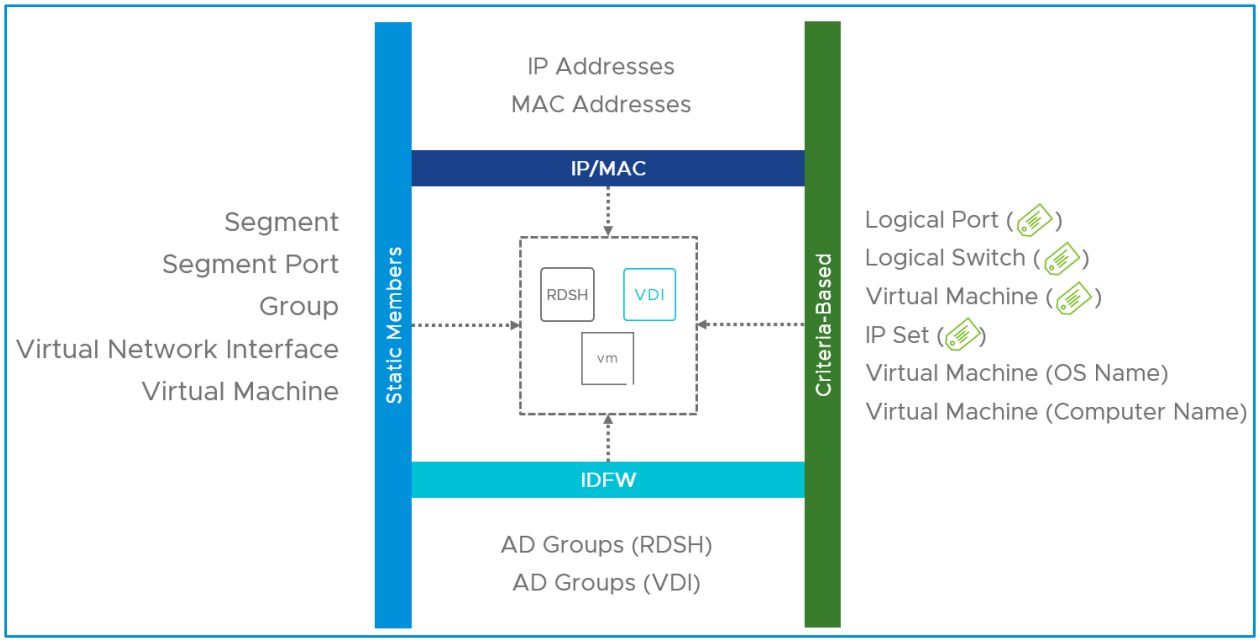

Figure 21 - NSX-T Grouping Object Criterion

Figure 22 shows how Groups evaluate membership of objects.

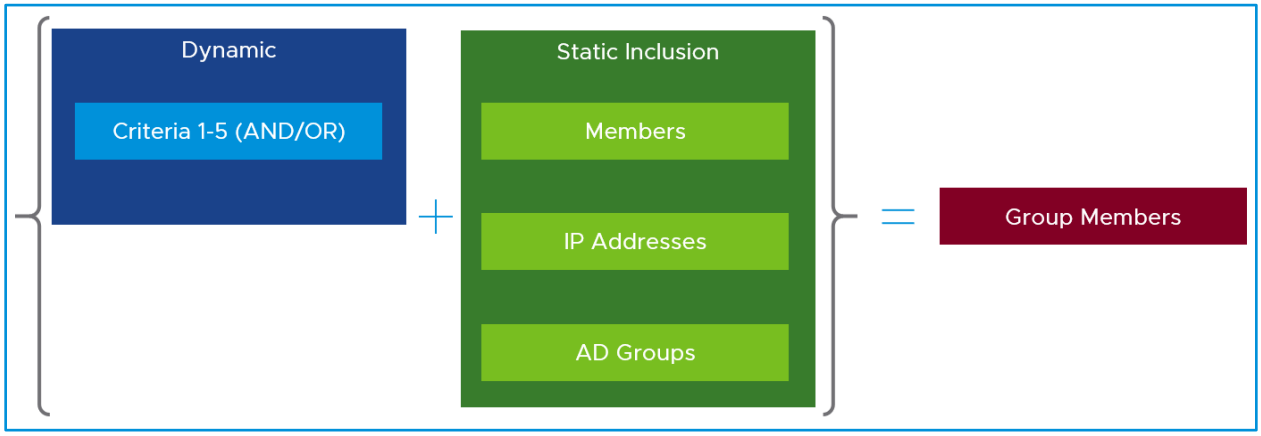

Figure 22 - NSX-T Grouping Criterion Evaluation

5.3 NSX-T Edge and Partner Services

Not all services are distributed within the hypervisor and require pools of resources to be used. NSX-T Edge Clusters provide the pool of resources for non-distributed services to consume. Horizon uses these Edge Nodes for external connectivity through North-South routing, Gateway Firewalling, Load Balancing for Horizon components such as Unified Access Gateways and Connection Servers, and DHCP relay for desktop pools to get IP addresses when they're created.

NSX-T also offers 3rd party partners platforms such as Guest Introspection and Network Introspection to integrate their services into NSX-T. Most notably, Horizon deployments can take advantage of agentless offload of anti-virus/anti-malware functions using the Guest Introspection platform.

The following sections quickly detail the functions that are provided by the NSX-T Edge and also additional NSX-T platforms with Guest Introspection and Network Introspection.

5.3.1 NSX-T Gateway Routing

NSX-T Gateways provide the North-South connectivity for workloads both outside and inside the virtualized data center to traverse. The Gateways can be configured in an Active/Standby configuration for stateful services, such at Gateway Firewalling, or configured in Active/Active for ECMP services. Networking services are provided by the Tier-0 gateway that is instantiated on the Edge Nodes. NSX-T supports static routing, dynamic routing with BGP, and support for IPv4 and IPv6. With Horizon, the RDS and Desktop Pools that reside on NSX-T segments would require connectivity from the Horizon Client and Connection Servers to the Horizon Agent on the desktop and application resources.

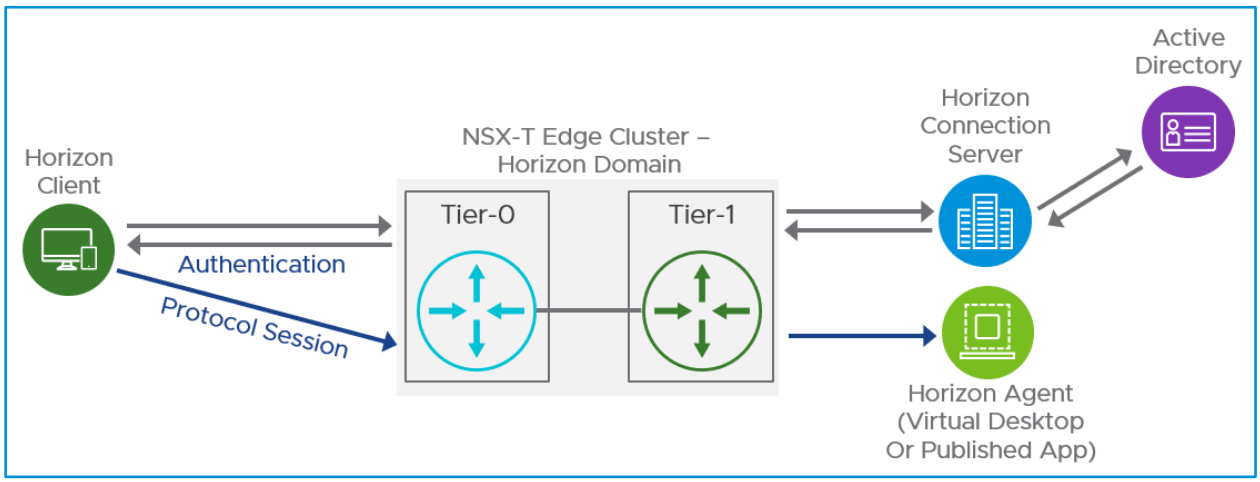

Figure 23 - NSX-T Gateway Routing for Horizon Connection Servers

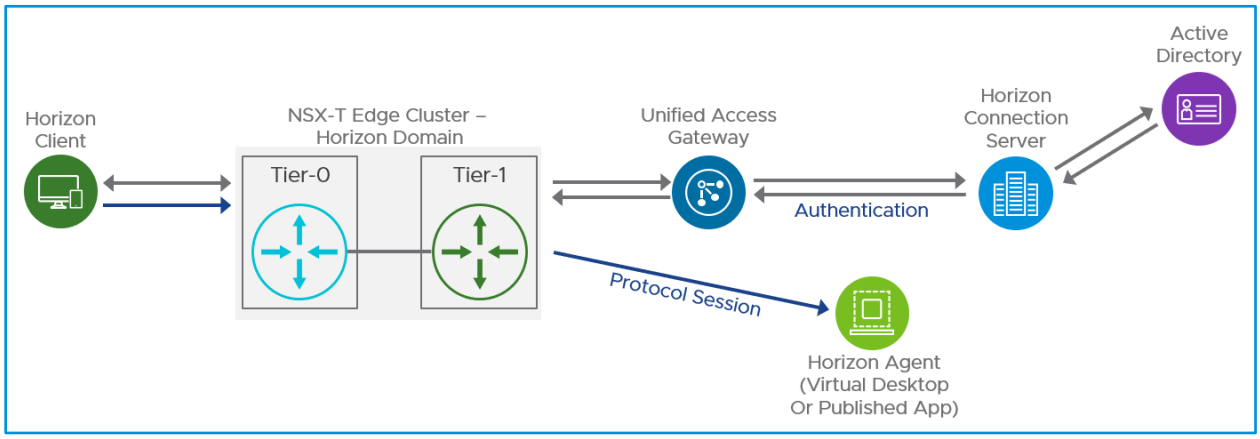

Figure 24 - NSX-T Gateway Routing for Horizon Unified Access Gateways

5.3.2 Load Balancing

NSX-T Edge Nodes provide pooled resources for building a robust load balancing infrastructure for Horizon to consume. The NSX-T Load Balancer (LB) provides standard L4 TCP/UDP and L7 HTTP/HTTPS for application high availability and traffic distribution across multiple servers. NSX-T LBs also provide health check monitors, one-arm and inline modes, multiple sizing for scale, and support for VM and Bare metal Edge Node form factors. The NSX-T LB can only be instantiated on a Tier-1 gateway, however multiple VIPs, can be placed on that LB to support a scalable server pool the VIP maintains.

Horizon has many requirements for load balancers to provide highly available access to its components. The following components all benefit from using an LB to provide high availability of Enterprise Horizon:

- **Unified Access Gateways**
- **Connection Servers**
- **AppVolumes**
- **VMware Identity Manager**

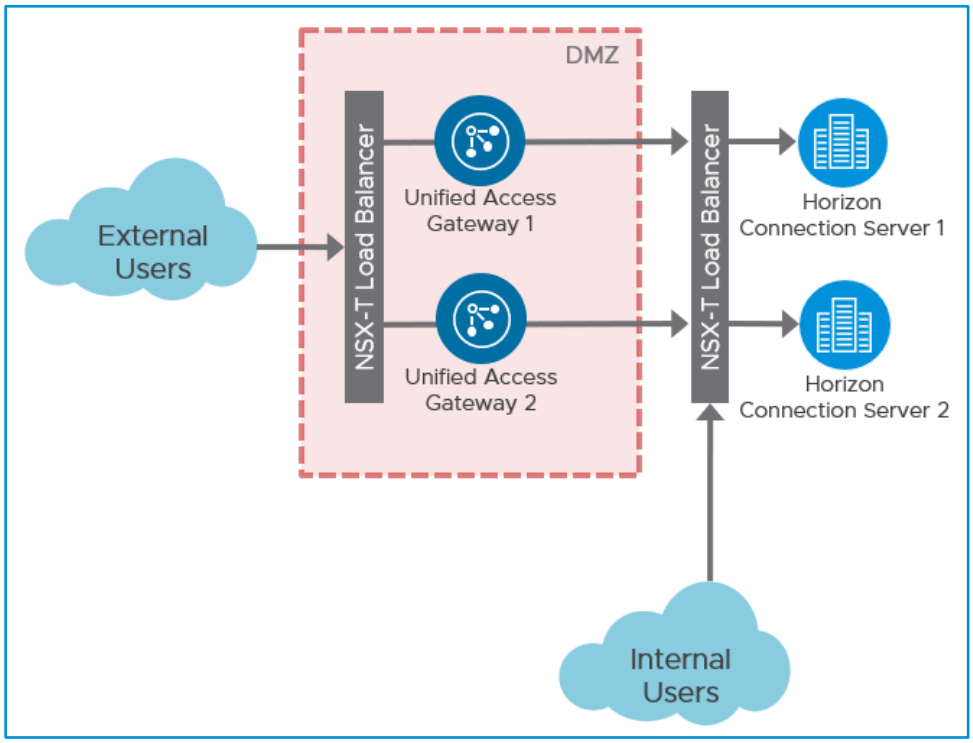

Figure 25 - Horizon Load Balancing for Unified Access Gateway and Connection Servers

5.3.3 Gateway Firewall

NSX-T Tier-0 gateway provides the North-South access from the physical environment into the virtual NSX-T environment. These Edge Nodes are also capable of providing North-South Gateway Firewalling for systems that reside south. The NSX-T Gateway Firewall provides Layer 2 – Layer 4 security for flows coming in and out of the NSX-T virtualized environment. Gateway Firewalling can be instantiated on either the Tier-0 or Tier-1 gateway. This enables tenant-based firewalling that can be configured independently for the workloads behind each Tier-1.

5.3.4 DHCP Relay

NSX-T offers capabilities to relay DHCP requests to a DHCP infrastructure for overlay networks created in NSX-T. VDI desktop pools often require DHCP IP addressing for the virtual desktop systems to consume. In traditional VLAN networks, this is handled by relaying DHCP traffic requests through the underlying physical network hardware to the DHCP provider. In the case of NSX-T where an NSX-T Overlay Segment is used to create an overlay Layer 2 network, NSX-T provides a DHCP relay mechanism to forward the request to the DHCP infrastructure.

5.3.5 Partner Service – Guest Introspection

NSX-T provides the Guest Introspection platform to allow 3rd party partners to run agentless Anti-Virus/Anti-Malware (AV/AM) capabilities for virtualized workloads on ESXi. Traditional AV/AM services require agents be run inside the guest operating system of a virtual workload. These agents can consume small amounts of resources for each workload on an ESXi host. In the case of Horizon, VDI desktop hosts typically attempt to achieve high consolidation ratios on the ESXi host, providing 10s to 100s of desktops per ESXi host. With each AV/AM agent inside the virtualized workload consuming a small amount of virtual CPU and memory, the resource costs can be noticeable and possibly reduce the overall number of virtual desktops an ESXi host can accommodate, thus increasing the size and cost of the overall VDI deployment. The Guest Introspection platform allows the AV/AM partner to remove their agent from

the virtual workload and provide the same services using a Service Virtual Machine (SVM) that is installed on each host. These SVMs consume much less virtual CPU and memory overall than running agents on every workload on the ESXi host.

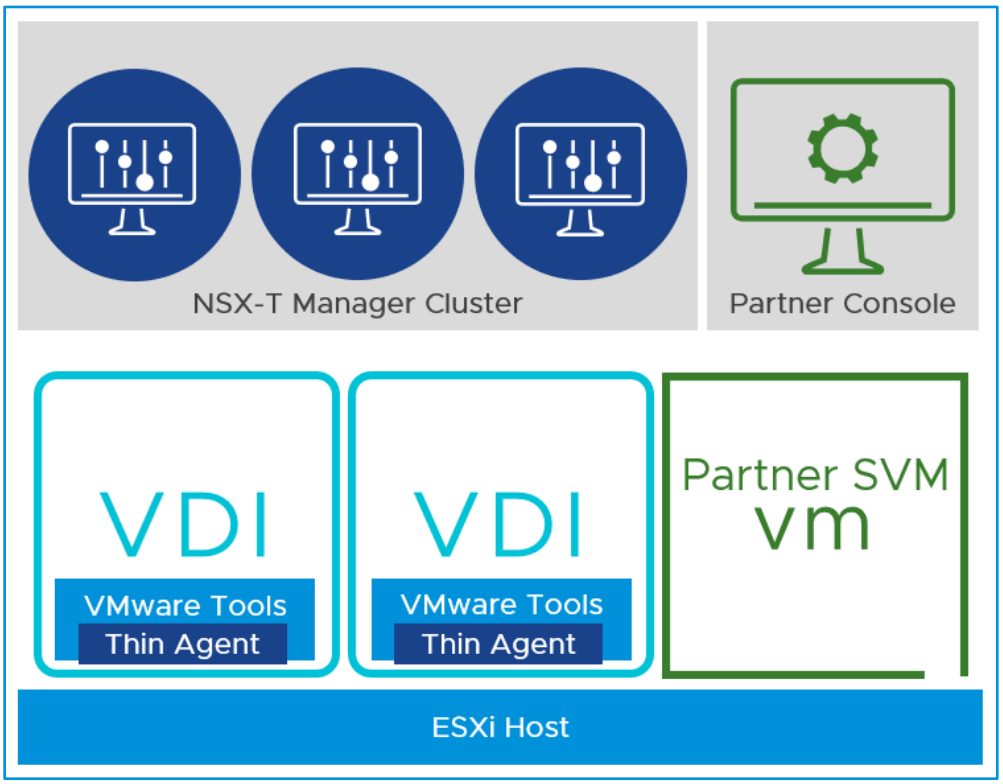

Figure 26 - Endpoint Protection Architecture Logical

The Guest Introspection platform for NSX-T following a simple 3 step process to use.

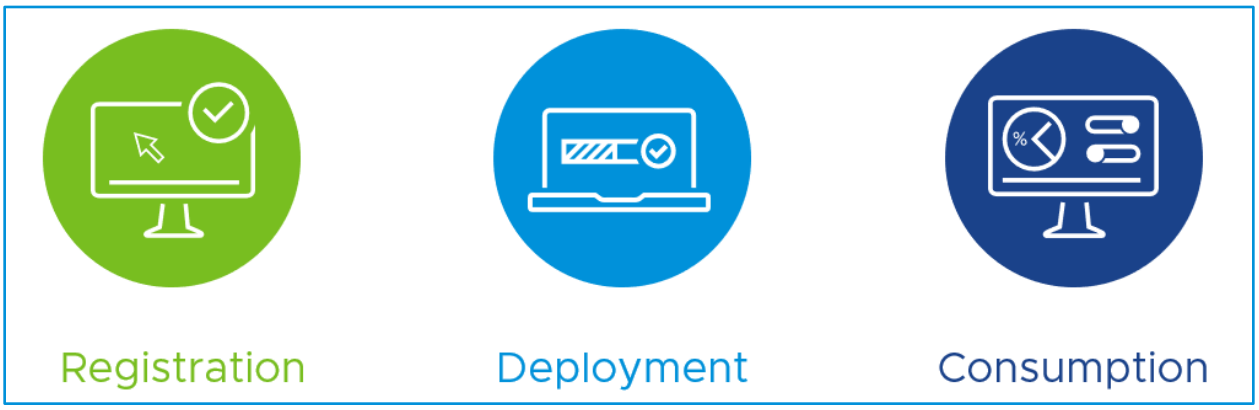

Figure 27 - Endpoint Protection Workflow

- **Registration**

Registration of the VMware Partner console with NSX-T and vCenter.

- **Deployment**

Creating a Service Deployment of the VMware Partner SVM and deployment to the ESXi Clusters. The SVMs require a Management network with which to talk to the Partner Management Console. This can be handled by IP Pool in NSX-T or by DHCP from the network. Management networks must be on a VSS or VDS switch.

- **Consumption**

Consumption of the Guest Introspection platform consists of creating a Service Profile of which references the Service Deployment and then creating Service Endpoint Protection Policy with Endpoint Rule that specifies which Service Profile should be applied to what NSX-T Group of Virtual Machines.

6. Deployment Topology for Horizon with NSX-T

A design for Horizon with NSX-T starts with the foundational deployment of NSX-T and the components that Horizon will consume. Horizon deployments are designed to be highly resilient and NSX-T should be designed to provide a resilient networking, networking services, and security infrastructure which Horizon can consume.

6.1 NSX-T and Horizon – Pod and Block

Horizon instances are deployed in pods and divided into multiple blocks in order to scale the Horizon deployment. Each pod contains two physical blocks – the Horizon Management Block and Horizon Resource Block. Figure 28 shows the addition of NSX-T to the pod and block architecture of Horizon.

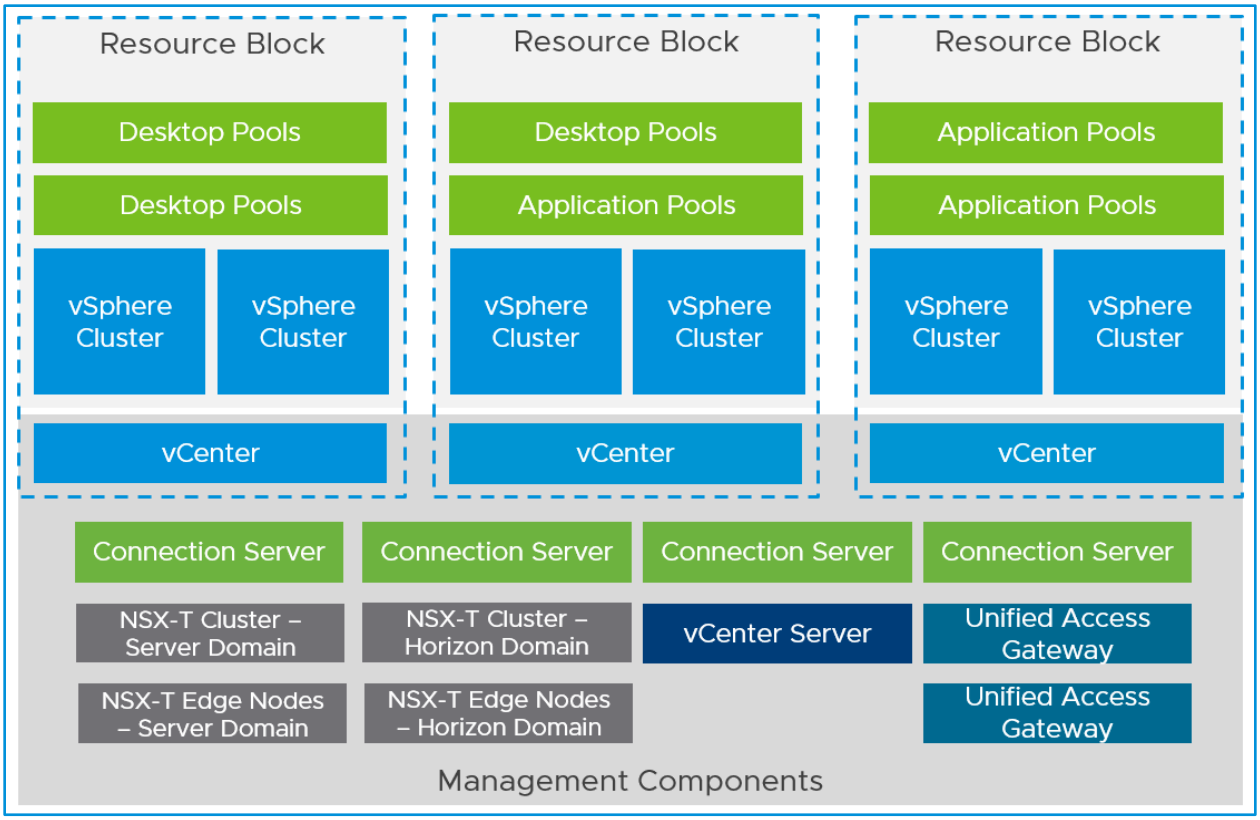

Figure 28 - Horizon and NSX-T Pod Configuration

NSX-T DESIGN DECISION	
Decision	Justification
Independent NSX-T Management Clusters for a Horizon single-site pod deployment topology	Splits NSX-T domain into Server and Horizon for NSX-T Management and Services. Allows independent domain scalability similar to Horizon Pod scale out. Horizon 7.9 supports up to 10,000 VMs per vCenter, 8000 recommended. A single NSX-T 2.5 Management Cluster supports a maximum of 25,000 Segment ports which aligns with expected and supported Horizon recommendations. A single NSX-T Management Cluster supports up to 16 vCenter Servers as Compute Managers. Per Horizon Pod, there will be a minimum of 3 vCenter Servers. Two vCenters for the Horizon Domain, one for the Server Domain.
NSX-T Edge Nodes will be placed in separate Edge Clusters for the Server and Horizon Domain	Placement of NSX-T Edge Nodes into separate clusters puts the Edge Nodes and the services they provide as close to the workloads as possible. Positioning spreads out the failure domain of the Edge Nodes to align with the Server and Domain logical layout.

6.2 NSX-T and Horizon – Server and Horizon Domain

When incorporating NSX-T with a Horizon deployment, failure domains need to be established that align to both Horizon and NSX-T to maintain consistent resiliency between platforms. Horizon establishes failure domains by breaking pods into blocks. NSX-T establishes failure domains by using guidance in the NSX-T Design Guide and recommends distinct management, compute, and edge clusters for large scale deployments utilizing NSX-T micro-segmentation, edge services, and network virtualization capabilities. Breaking the Horizon pod architecture into NSX-T Server and Horizon Domains, allows a separation of failure domains for Horizon that can align with NSX-T design. Each domain consists of its own NSX-T Manager Cluster as well as NSX-T Edge Nodes.

- **Server Domain**

The Server Domain consists of all of the clusters that provide the resources for managing, servicing, and monitoring a Horizon deployment. NSX-T provides networking and security services for all of the objects in this Domain. This Domain encompasses the management components for the entire data center, typically, and includes the Horizon management infrastructure as well. Enterprise Applications and even Horizon components such as Connection Servers, reside on the Compute Clusters in this Domain. Edge connectivity is handled by NSX-T Edge Nodes and is also separated so that a failure in the Horizon Domain does not impact the Server Domain.

- **Horizon Domain**

The Horizon Domain consists of all of the clusters that provide the resources for hosting, servicing, and maintaining a Horizon VDI and/or RDS Farm deployment. NSX-T provides networking and security services for all of the objects in this Domain. The Horizon Domain scales out independently as NSX-T supports more than one vCenter Server as a Compute Manager and supports large scale numbers of virtual machines under its services. Edge connectivity is handled by NSX-T Edge Nodes and is also separated so that an Edge failure in the Server Domain does not impact the Horizon Domain.

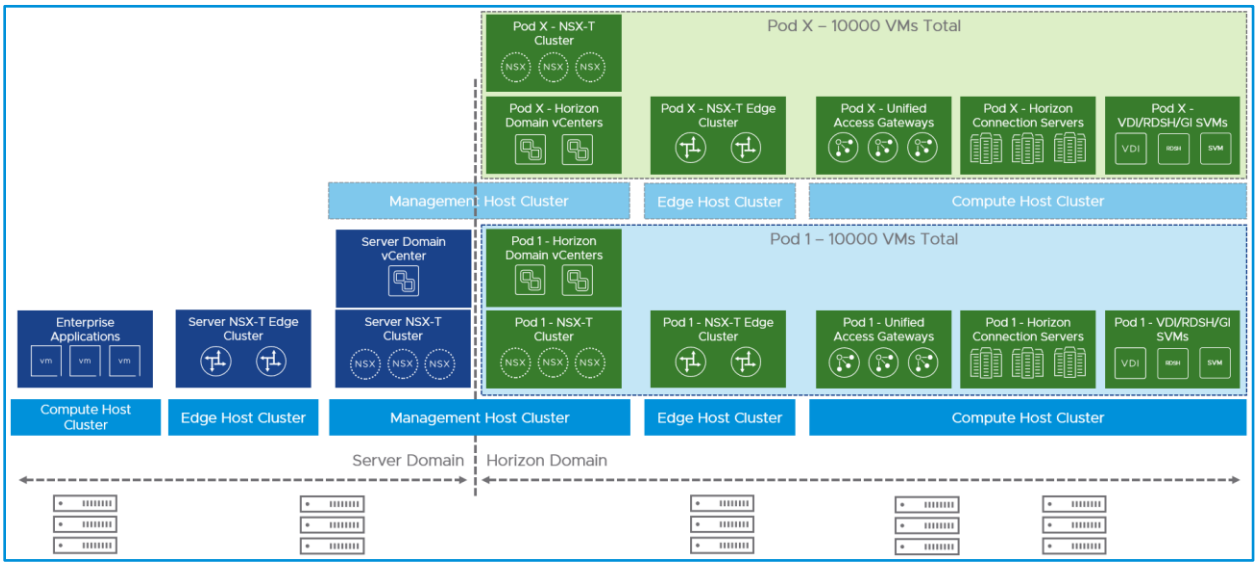

Figure 29 – Example Horizon and NSX-T Large Topology Single-Site Deployment - Logical

Figure 29 takes the Server and Horizon Domain and Management and Resource Block logical constructs and lays them out in a typical physical data center design image and shows the placement of each of these constructs within multiple and separate rack hardware infrastructures. The splitting up into separate rack designs creates separate failure domains for the server and Horizon Domains so that a failure in one domain, does not impact the other domain and each block can be independent from each other as well.

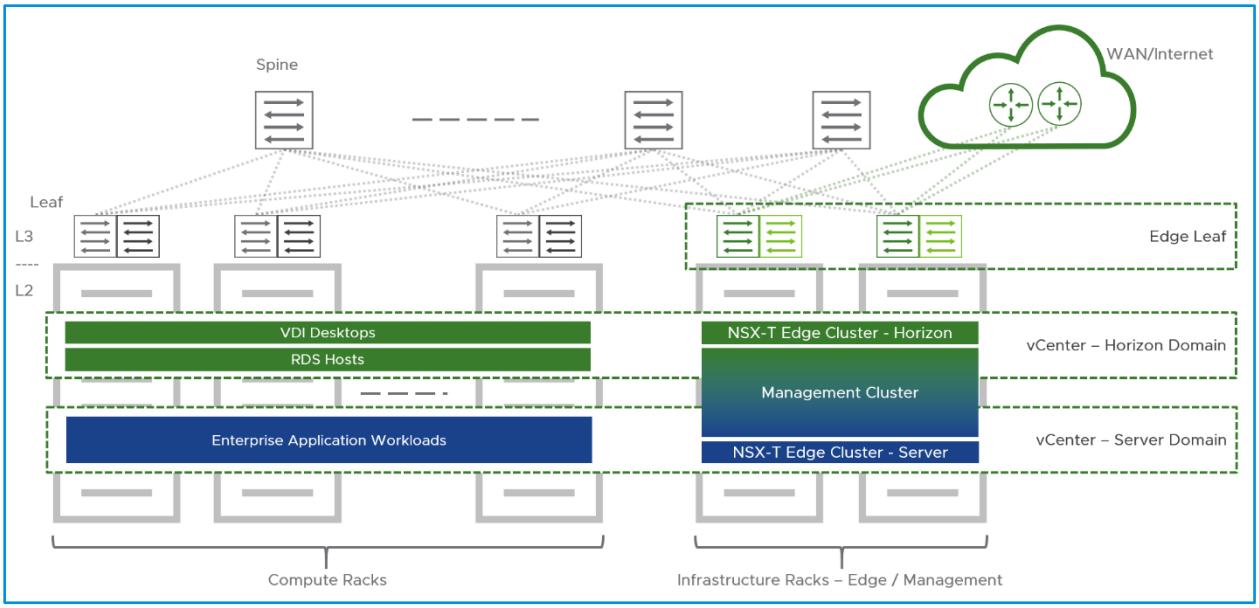

Figure 30 – Example Horizon and NSX-T Large Topology Single-Site Deployment - Physical

- **Management Host Cluster**

This cluster will contain most of the management appliances from both Horizon and NSX-T as well as any operational or security management consoles. It is shared between the Server and Horizon Domain as management resources from both reside on this cluster. It is made resilient through vSphere HA and vSphere Clustering.

- **Edge Host Cluster**

This cluster represents the ESXi servers that the NSX-T Edge Nodes will reside on and provides the offramp network access from the physical and virtual data center resources. NSX-T Edge Clusters are built independently for the Server and Horizon Domain.

- **Compute Host Cluster**

The Compute cluster in the Server domain consists of Enterprise Applications and for the Horizon Domain consists of the Horizon Connection Servers, Horizon Unified Access Gateways, VDI desktop pools, Endpoint Protection SVMs and/or RDS Host Farms. This can be one or multiple computer clusters depending on the size of the organization's virtual environment.

6.3 NSX-T and Horizon Cross-vCenter Topology

NSX-T supports connectivity of multiple vCenter Servers as Compute Managers. This allows NSX-T administration and policy configuration for both the Server and Horizon Domains to be managed through a single UI, reducing operational overhead with managing NSX policies in two different interfaces.

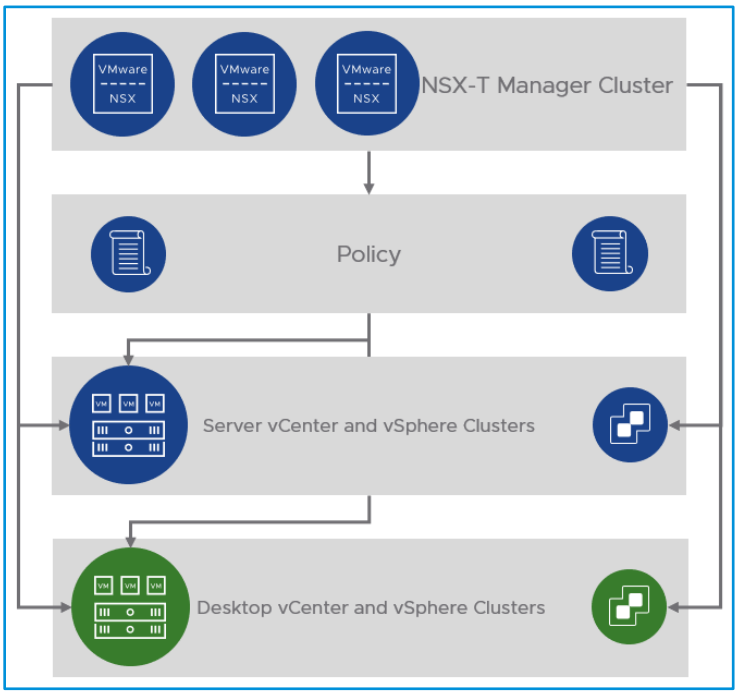

Figure 31 - NSX-T Cross-vCenter Policy Distribution

6.4 NSX-T and Horizon Topologies

Horizon deployments, like NSX-T deployments, can accommodate a wide ranges of deployment topologies and options. NSX-T needs to align at logical boundaries with Horizon to scale similarly. Not every customer requires a topology that scales to the Horizon Cloud Pod Architecture limits but guidance is helpful for showcasing the options. The following sections represent the three Horizon and NSX-T topologies that align NSX-T at the Horizon pod boundary as well as providing guidance for customers that fall into the sizing categories. All scale recommendations are based on maximums of both NSX-T Data Center 2.5 and Horizon 7.9. These topologies are

not meant to be comprehensive or to replace a services-led engagement recommendation, but provide guidance on what would be required to build each scenario based on each platform's provided maximums.

6.4.1 NSX-T and Horizon – Small (Converged Cluster) Topology – Single Pod up to 4000 VMs

The 'Small' topology represents a converged cluster design where the Management, Edge, and Compute Clusters of both the Server and Horizon domains reside on the same logical ESXi compute cluster. This topology would be similar to using hyper-converged hardware to run Horizon, Enterprise Servers, and the Management components where the compute infrastructure consists of a single ESXi cluster. This Horizon and NSX-T topology aligns from an NSX-T design perspective with the Collapsed Management and Edge Cluster design in the NSX-T Reference Architecture.

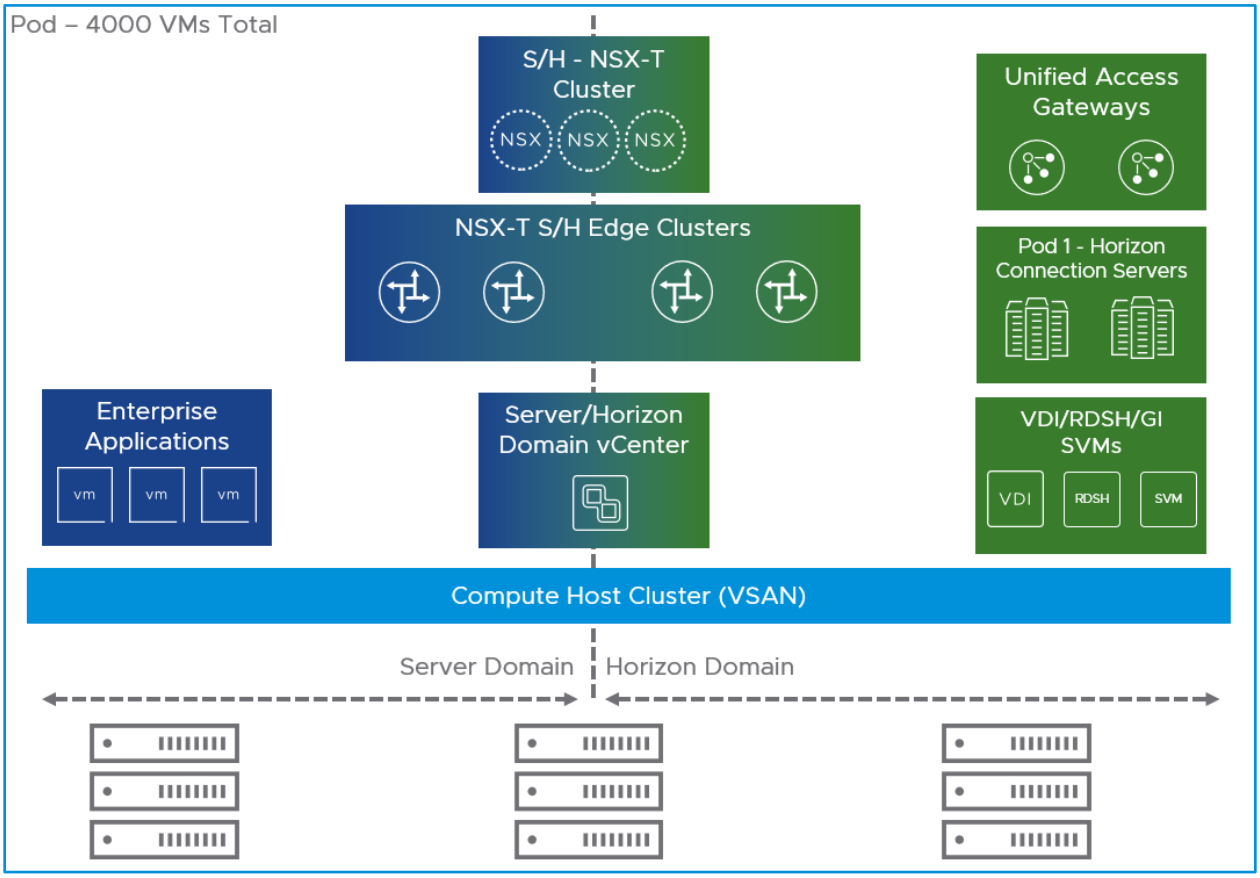

Figure 32 - Example NSX-T and Horizon Small Converged Pod Architecture

NSX-T DESIGN RECOMMENDATIONS	
Recommendation	Justification
Collapsed Management, Edge, and Compute Clusters into one cluster for both Server and Horizon Domains	A converged cluster consists of a minimum of 4 ESXi hosts to provide redundancy and high availability of the infrastructure. High Availability provided by vSphere HA

One NSX-T Cluster - Singular UI for Policy Enforcement	NSX-T supports 16 vCenters for unified policy enforcement across vCenter Inventory No IP Sets required for Security Policies across vCenter Inventory
One Server and One Horizon Edge Clusters	Dedicated Edge Nodes for pools of resources for Horizon Domain. Dedicated Edge Nodes for pools of resources for Server Domain.
Four Large NSX-T Edge Nodes for two clusters of two Edge Nodes.	One Edge Cluster in HA for the Server Domain. One Edge Cluster in HA for the Horizon Domain. Large NSX-T Edge Nodes for all services necessary • One Large Load Balancer
One vCenter Server	Converged clusters can only have one vCenter as the data store is shared across the entire cluster
One Tier-0 Gateway	Each Tier-0 Gateway supports 400 Tier-1 Logical Routers
One Tier-1 Gateway	Each Tier-1 Gateway supports 20,000 ARP entries for VMs attached to Segments
One Large LB on Tier-1 Gateway	1000 Virtual Servers 3000 Pools 7500 Pool Members

HORIZON DESIGN RECOMMENDATIONS WITH NSX-T	
Recommendation	Benefit
1 VSAN datastore	Converged clusters cannot have more than 1 VSAN datastore per cluster
4000 VMs total	Horizon 7.9 supports 4000 VMs per VSAN datastore VMs is used as this could be a combination of Server and Horizon workloads
3 Horizon Unified Access Gateways for N+1 design	Horizon recommends N+1 for UAGs and UAGs support 2000 connections per appliance
3 Horizon Connection Servers for N+1 design	Horizon recommends N+1 for Connection Servers and Connection Servers support 2000 recommended connections per server

6.4.2 NSX-T and Horizon – Medium Topology – Single Pod up to 10000 VMs

The 'Medium' topology represents the physical splitting of the Management, Edge, and Compute clusters. This Horizon and NSX-T topology aligns from an NSX-T design perspective with the Collapsed Management and Edge Cluster design in the NSX-T Reference Architecture. This topology collapses the Management and Edge Clusters into one cluster to minimize the amount of hardware required for deployment.

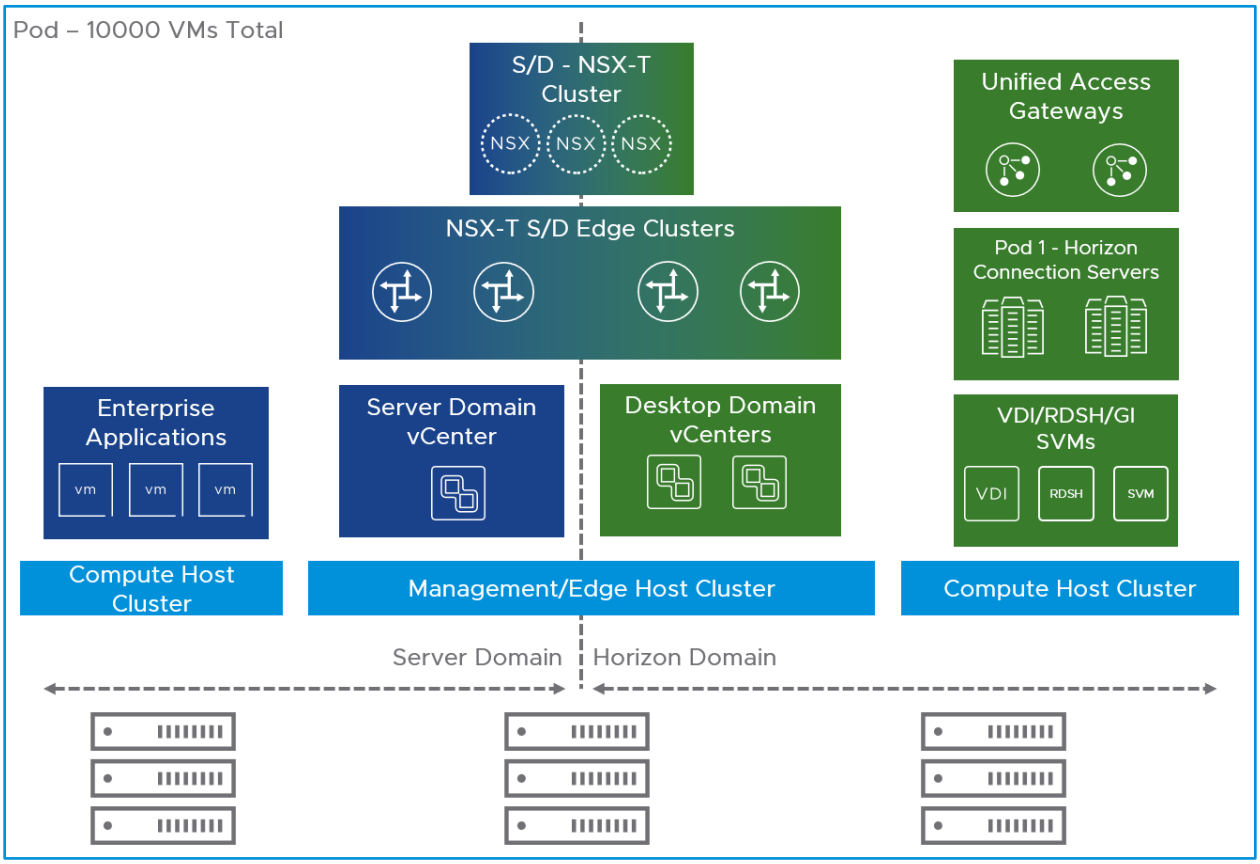

Figure 33 - Example NSX-T and Horizon Medium Topology Architecture

NSX-T DESIGN BENEFITS	
Recommendation	Benefit
Collapsed Management and Edge, and Separate Compute Clusters for both Server and Horizon Domains	A collapsed Management and Edge cluster reduces the amount of hardware equipment to provide physical separation of Management and Edge. High Availability provided by vSphere HA
One NSX-T Cluster - Singular UI for Policy Enforcement	NSX-T supports 16 vCenters for unified policy enforcement across vCenter Inventory No IP Sets required for Security Policies across vCenter Inventory
NSX-T - Singular UI for Policy Enforcement	NSX-T supports 16 vCenters for unified policy enforcement across vCenter Inventory No IP Sets required for Security Policies across vCenter Inventory
One Server and One Horizon Edge Clusters	Dedicated Edge Nodes for pools of resources for Horizon Domain. Dedicated Edge Nodes for pools of resources for Server Domain.

Four Large NSX-T Edge Nodes for two clusters of two Edge Nodes.	One Edge Cluster in HA for the Server Domain. One Edge Cluster in HA for the Horizon Domain. Large NSX-T Edge Nodes for all services necessary • One Large Load Balancer
One vCenter Server for Server Domain	Logical separation of the vCenter that manages the Enterprise Application Servers VMs and the Horizon workloads.
Two vCenter Servers for Horizon Domain	Horizon 7.9 supports 8000 instant-clones per vCenter. Two vCenters are necessary to achieve 10,000 desktops total. One vCenter could be used if less than 8000 desktops in pod.
One Tier-0 Gateway	Each Tier-0 Gateway supports 400 Tier-1 Logical Routers
One Tier-1 Gateway	Each Tier-1 Gateway supports 20,000 ARP entries for VMs attached to Segments
One Large LB on Tier-1 Gateway	1000 Virtual Servers 3000 Pools 7500 Pool Members

HORIZON DESIGN RECOMMENDATIONS WITH NSX-T	
Recommendation	Benefit
Single Horizon Pod	Horizon 7.9 supports 10,000 VMs per Pod
10,000 VMs total	Horizon 7.9 supports 10,000 VMs per Pod VMs is used as this could be a combination of Server and Horizon workloads
6 Horizon Unified Access Gateways for N+1 design	Horizon recommends N+1 for UAGs and UAGs support 2000 connections per appliance
6 Horizon Connection Servers for N+1 design	Horizon recommends N+1 for Connection Servers and Connection Servers support 2000 recommended connections per server

6.4.3 NSX-T and Horizon – Large Topology – Multi-Pod for 10000+ VMs

The 'Large' topology represents the scalable Horizon and NSX-T deployment for the large deployments and able to support multiple Horizon pods. This Horizon and NSX-T topology aligns from an NSX-T design perspective with the Enterprise ESXi Based Design in the NSX-T Reference Architecture. All clusters are split out completely and separately from each other to isolate fault domains for each aspect of the design. The only aspect which is shared is/could be the management cluster for both domains. It could also be split out as needed, but can be collapsed to reduce the overall hardware needed and reduce some complexity of the design. While this design does require more hardware to accomplish, it provides maximum and independent scalability for large Horizon deployment needs.

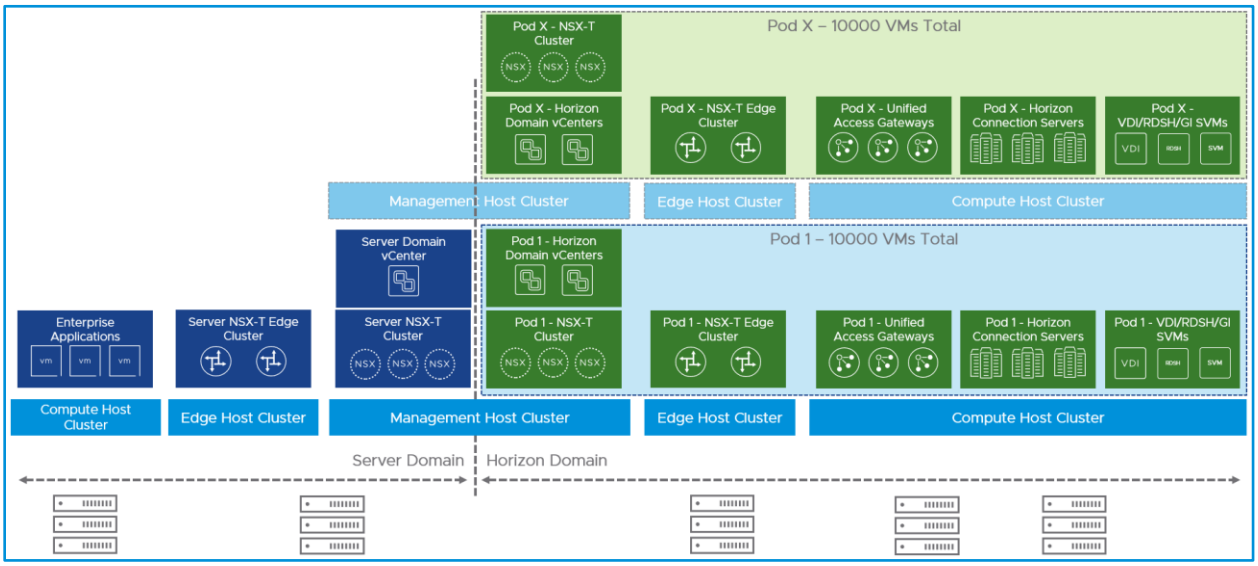

Figure 34 - Example NSX-T and Horizon Large Topology Architecture

NSX-T DESIGN DECISION	
Decision	Justification
Shared Management Host Cluster for Server and Horizon Domains	A shared Management Cluster for the Server and Horizon Domains reduce the amount of hardware equipment necessary to provide physical separation of the Management components of the Server Domain and each per Pod Horizon Domain. Could also be separated as necessary.
Separate Edge Host and Compute Host Cluster per Pod per Horizon Domain	Separated to allow independent scaling as needed.
Separate Edge Host and Compute Host Cluster for Server Domain	Separated to allow independent scaling as needed.
Two Large NSX-T Edge Nodes for Server Domain	One Cluster in HA for the Server Domain. Large NSX-T Edge Nodes for all services necessary for each Pod • One Large Load Balancer per Pod
Two Large NSX-T Edge Nodes for Horizon Domain per Pod	One Cluster in HA for the Horizon Domain for each Pod Large NSX-T Edge Nodes for all services necessary for each Pod • One Large Load Balancer per Pod
One NSX-T Cluster - Singular UI for Policy Enforcement per Pod	NSX-T supports 16 vCenters for unified policy enforcement across vCenter Inventory IP Sets required for Security Policies across Server and Horizon Domains

HORIZON DESIGN RECOMMENDATIONS WITH NSX-T	
Recommendation	Benefit

One or multiple Horizon Pods	Horizon 7.9 supports 10,000 VMs per Pod, 50 pods per Cloud Pod Architecture, 250,000 sessions total
10,000 VMs total per Pod	Horizon 7.9 supports 10,000 VMs per Pod
6 Horizon Unified Access Gateways for N+1 design per Pod	Horizon recommends N+1 for UAGs and UAGs support 2000 connections per appliance
6 Horizon Connection Servers for N+1 design per Pod	Horizon recommends N+1 for Connection Servers and Connection Servers support 2000 recommended connections per server
Global Site Load Balancer	Global Site Load Balancer required for access to multiple Pods (NSX-T does not support GSLB capabilities in NSX-T Data Center 2.5)

7. NSX-T for Horizon Core Architecture Design Recommendations

The following sections break down design recommendation for Horizon Core components with NSX-T. Each design decision provides a justification for why each decision was made. Any configuration numbers in the following sections were based on the numbers listed for NSX-T Data Center 2.5 and Horizon 7.9.

7.1 NSX-T Core Network Infrastructure Layout

Regardless of the topology chosen from an NSX-T or Horizon standpoint, the following diagram is a logical networking representation of the configuration of a typical Horizon deployment within those topologies. The specifics of the networking configurations for each of the Horizon components is covered in the following sections.

The following tables represent a default configuration for the Horizon NSX-T networking deployment that matches the infrastructure layout in Figure 34.

HORIZON EDGE CLUSTER CONFIGURATION				
Transport Node	Edge Cluster Profile	Name	Tag	Scope
Edge Node1	nsx-default-edge-high-availability-profile	HZN-EC-POD1	HZN-EC-POD1	HZN-POD1
Edge Node2	nsx-default-edge-high-availability-profile	HZN-EC-POD1	HZN-EC-POD1	HZN-POD1

HORIZON TIER-0 LOGICAL ROUTER CONFIGURATION	
Tier-0 GW Name	HZN-GW-T0-POD1
HA Mode	Active Standby
Linked Tier-1 GW	HZN-GW-T1-POD1
Fail Over	Non Preemptive
Edge Cluster	HZN-EC-POD1
HA VIP	IP Address and Uplinks from Edge Nodes
Tag	HZN-GW-POD1

Scope	HZN-POD1

Route Re-distribution	Advertised Tier-1 Subnets
	• Static Routes
	• Connected Interfaces & Segments
	  ○ Service Interface Subnet
	  ○ Connected Segment
	• LB VIP

There are other configurations for the Tier-0 router that are directly related and reliant on the environment which the NSX-T deployment in. NSX-T supports BGP and Static routing with the physical infrastructure.

HORIZON TIER-1 LOGICAL ROUTER CONFIGURATION	
Tier-1 GW Name	HZN-GW-T1-POD1
Linked Tier-1 GW	HZN-GW-T0-POD1
Fail Over	Non Preemptive
Edge Cluster	HZN-EC-POD1
HA VIP	IP Address and Uplinks from Edge Nodes
Tag	HZN-GW-POD1
Scope	HZN-POD1

Route Re-distribution	Advertised Tier-1 Subnets
	• Static Routes
	• Connected Interfaces & Segments
	  ○ Service Interface Subnet
	  ○ Connected Segment
	• LB VIP

7.1 Horizon Access

Horizon provides infrastructure for allowing Horizon Client to connection from both Externally, outside the data center perimeter, and Internally, inside the data center perimeter. There are slight differences in the connection methods and flows of how a Horizon Client connects from External and Internal.

7.1.1 External Access

External Access to the Horizon environment typically comes from outside the perimeter firewall. External access to the Horizon infrastructure is provided to the Horizon Client through the Horizon Unified Access Gateway.

7.1.1.1 External Access – Services

Table X represents the Horizon Services that are representative of Internal Access.

HORIZON EXTERNAL ACCESS SERVICES CONFIGURATION

Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon 7 Horizon Client to Unified Access Gateway	HZN-SVC-HTTPS-443	443	TCP	HZN-CP-HTTPS	SSL
Horizon 7 Browser to Unified Access Gateway HTML Access	HZN-SVC-HTTPS-443	443	TCP	HZN-CP-HTTPS	SSL
Horizon 7 Blast Extreme TCP 443 Excellent Typical Horizon Client to Unified Access Gateway	HZN-SVC-BLAST	443	TCP	HZN-CP-BLAST	BLAST
Horizon 7 Blast Extreme TCP 8443 Excellent Typical Horizon Client to Unified Access Gateway	HZN-SVC-BLAST	8443	TCP	HZN-CP-BLAST	BLAST
Horizon 7 Blast Extreme UDP 443 Poor Typical Horizon Client to Unified Access Gateway	HZN-SVC-BLAST	443	UDP	HZN-CP-BLAST	BLAST
Horizon 7 Blast Extreme UDP 8443 Poor Typical Horizon Client to Unified Access Gateway	HZN-SVC-BLAST	8443	UDP	HZN-CP-BLAST	BLAST
Horizon 7 PCoIP TCP Horizon Client to Unified Access Gateway	HZN-SVC-PCOIP	4172	TCP	HZN-CP-PCOIP	PCOIP
Horizon 7 PCoIP UDP Horizon Client to Unified Access Gateway	HZN-SVC-PCOIP	4172	UDP	HZN-CP-PCOIP	PCOIP

7.1.1.2 External Access – Security

Table X represents the NSX-T DFW Security Policies for securing External Access for Horizon. Security Policies and their rules are placed in the Application Category in the NSX-T DFW.

HORIZON EXTERNAL ACCESS SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon - External Access Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
External – Horizon Client to UAG HTTPS	Any	HZN-GRP-UAG-VIP-POD1	HZN-SVC-HTTPS-443	HZN-CP-HTTPS	HZN-GRP-UAG-POD1	Allow
External – Horizon Client to UAG PCoIP	Any	HZN-GRP-UAG-VIP-POD1	HZN-SVC-PCOIP	HZN-CP-PCOIP	HZN-GRP-UAG-POD1	Allow
External – Horizon Client to UAG BLAST	Any	HZN-GRP-UAG-VIP-POD1	HZN-SVC-BLAST	HZN-CP-BLAST	HZN-GRP-UAG-POD1	Allow

7.1.2 Internal Access

Internal Access to the Horizon environment typically comes from within the perimeter of the organization and refers to 'internal users. Internal Access to the Horizon infrastructure is provided to the Horizon Client through the Horizon Connection Server.

7.1.2.1 Internal Access – Services

Table X represents the Horizon Services that are representative of Internal Access.

HORIZON INTERNAL ACCESS SERVICES CONFIGURATION					
Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon Client to Horizon Agent Blast Extreme TCP 22443	HZN-SVC-BLAST-EXTREME-22443	22443	TCP	HZN-CP-BLAST	BLAST
Horizon Client to Horizon Agent Blast Extreme UDP 22443	HZN-SVC-BLAST-EXTREME-22443	22442	UDP	HZN-CP-BLAST	BLAST
Horizon Client to Horizon Agent PCoIP TCP 4172	HZN-SVC-PCOIP	4172	TCP	HZN-CP-PCOIP	PCOIP
Horizon Client to Horizon Agent PCoIP UDP 4172	HZN-SVC-PCOIP	4172	UDP	HZN-CP-PCOIP	PCOIP
Horizon Client to Horizon Agent RDP	HZN-SVC-RDP	3389	TCP	HZN-CP-RDP	RDP
Horizon Client to Horizon Agent CDR MMR	HZN-SVC-CDR-MMR	9427	TCP	N/A	N/A
Horicon Client to Horizon Agent USB Redirection	HZN-SVC-32111	32111	TCP	N/A	N/A
Horizon 7 Browser to Horizon Agent HTML Access	HZN-SVC-HTTPS-8443	8443	TCP	HZN-CP-HTTPS	SSL
Horizon 7 HTTP Horizon Client to View Connection Servers Standard	HZN-SVC-HTTP	80	TCP	HZN-CP-HTTP	HTTP
Horizon 7 HTTPS Horizon Client to View Connection Servers SSL	HZN-SVC-HTTPS-443	443	TCP	HZN-CP-HTTPS	SSL

7.1.2.2 Internal Access – Security

Table X represents the NSX-T DFW Security Policies for securing Internal Access for Horizon. Security Policies and their rules are placed in the Application Category in the NSX-T DFW.

HORIZON INTERNAL ACCESS SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon - Internal Access Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Internal – Horizon Client to Horizon Agent via PCoIP	Any	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-PCOIP	HZN-CP-PCOIP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	Allow

Internal – Horizon Client to Horizon Agent via Blast Extreme	Any	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-BLAST-EXTREME-22443	HZN-SVC-BLAST-EXTREME-22443	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	Allow
Internal – Horizon Client to Horizon Agent via RDP	Any	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-RDP	HZN-CP-RDP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	Allow
Internal – Horizon Client to Horizon Agent CDR MMR	Any	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-CDR-MMR	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	Allow
Internal – Horizon Client to Horizon Agent USB Redirection	Any	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-32111	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	Allow
Internal – Browser to Connection Server HTML Access	Any	HZN-GRP-CS-VIP-POD1	HZN-SVC-HTTPS-8443	HZN-CP-HTTPS	HZN-GRP-CS-POD1	Allow
Internal – Horizon Client to Connection Server HTTP	Any	HZN-GRP-CS-VIP-POD1	HZN-SVC-HTTP	HZN-CP-HTTP	HZN-GRP-CS-POD1	Allow
Internal – Horizon Client to Connection Server HTTPS	Any	HZN-GRP-CS-VIP-POD1	HZN-SVC-HTTPS-443	HZN-CP-HTTPS	HZN-GRP-CS-POD1	Allow

7.2 Unified Access Gateways

The Horizon Unified Access Gateway acts as a proxy host for connections inside your company's trusted network and is a key component for External Access. Unified Access Gateways provide a layer of security from exposing virtual desktops, application hosts, and servers directly to the public Internet. The Horizon UAGs require networking and load balancing to function in a highly available configuration. NSX-T can provide each of these functions as well as enhancing security around the communications in and out of the UAGs as well.

7.2.1 Unified Access Gateways – Networking

External Horizon connectivity consists of Unified Access Gateways and VMware Identity Manager systems, which reside in a DMZ networking architecture. NSX-T can be used to build an entirely separate virtual DMZ network using NSX-T Overlay Segments.

Unified Access Gateways have several form factors and configurations. Typical deployment of the UAG is a 2 vNIC model. The first vNIC resides on the Internet/DMZ-facing network and the second vNIC for the backend management connection residing on an internal network. Figures 35 and 36 show how NSX-T can be architected to support both an extension of an existing DMZ network and how to connect the UAGs using an NSX-T Segment.

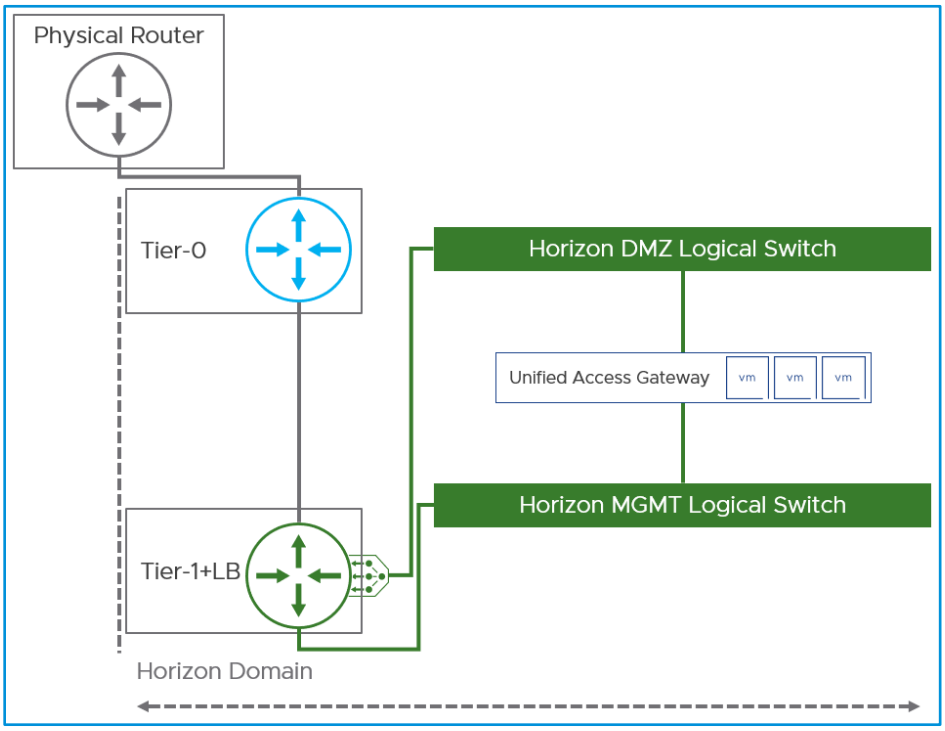

Figure 35 - Example NSX-T and Unified Access Gateway Networking

HORIZON UNIFED ACCESS GATEWAY NETWORK CONFIGURATION						
Segment Name	Connected Gateway & Type	Subnet	Transport Zone	VLAN	Tag	Scope
HZN-SEG-DMZ-POD1	HZN-GW-T1-POD1 - Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-UAG-POD1	HZN-POD1
HZN-SEG-MGMT-POD1	HZN-GW-T1-POD1 – Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-UAG-POD1	HZN-POD1

7.2.2 Unified Access Gateways – Edge and Partner Services

Horizon Unified Access Gateways are hardened virtual appliances. They do not require Guest Introspection protection with 3rd party services.

7.2.3 Unified Access Gateways – Load Balancing

Horizon Unified Access Gateways are deployment in a scalable fashion with a requirement for at least N+1 redundancy. To achieve this redundancy, UAGs can take advantage of NSX-T Load Balancing services provided for the XML-API authentication traffic to the Horizon Connection Servers. The following tables are an example configuration for NSX-T LB with Horizon Unified Access Gateways.

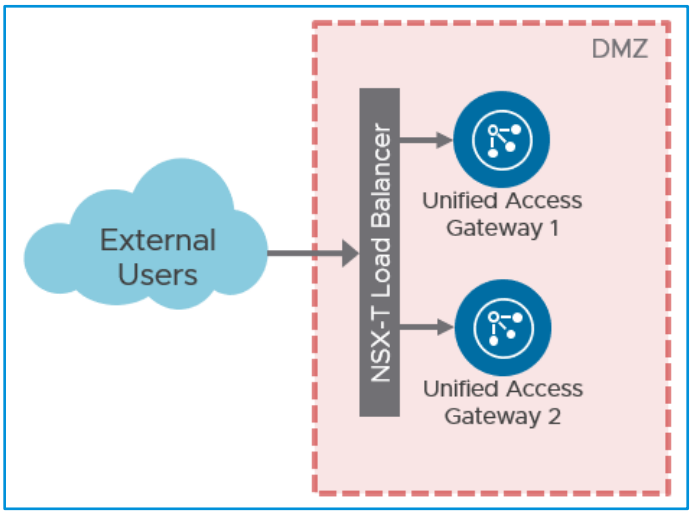

Figure 36 - Horizon Unified Access Gateway Load-balancing Topology

HORIZON UNIFED ACCESS GATEWAY LOAD BALANCER CONFIGURATION				
Name	Size	Tier-1 Gateway	Tag	Scope
HZN-LB-POD1	Large	HZN-GW-T1-POD1	HZN-UAG-POD1	HZN-POD1

HORIZON UNIFED ACCESS GATEWAY LOAD BALANCER VIRTUAL SERVER CONFIGURATION – PART 1			
Name	HZN-VIP-UAG-TCP-4172	HZN-VIP-UAG-TCP-443	HZN-VIP-UAG-TCP-8443
IP Address	1.1.1.1 <Example>	1.1.1.1 <Example>	1.1.1.1 <Example>
Ports	4172	443	8443
Type	L4 TCP	L4 TCP	L4 TCP
Load Balancer	HZN-LB-UAG-POD1	HZN-LB-UAG-POD1	HZN-LB-UAG-POD1
Server Pool	HZN-LB-POOL-UAG-POD1	HZN-LB-POOL-UAG-POD1	HZN-LB-POOL-UAG-POD1
Application Profile	default-tcp-lb-app-profile	default-tcp-lb-app-profile	default-tcp-lb-app-profile
Persistence	HZN-LB-PERSIST-UAG-POD1	HZN-LB-PERSIST-UAG-POD1	HZN-LB-PERSIST-UAG-POD1
Default Pool Member Ports	4172	443	8443
Tag	HZN-UAG-POD1	HZN-UAG-POD1	HZN-UAG-POD1
Scope	HZN-POD1	HZN-POD1	HZN-POD1

HORIZON UNIFED ACCESS GATEWAY LOAD BALANCER VIRTUAL SERVER CONFIGURATION – PART 2

Name	HZN-VIP-UAG-UDP-4172	HZN-VIP-UAG-UDP-443	HZN-VIP-UAG-UDP-8443
IP Address	1.1.1.1 <Example>	1.1.1.1 <Example>	1.1.1.1 <Example>
Ports	4172	443	8443
Type	L4 UDP	L4 UDP	L4 UDP
Load Balancer	HZN-LB-UAG-POD1	HZN-LB-UAG-POD1	HZN-LB-UAG-POD1
Server Pool	HZN-LB-POOL-UAG-POD1	HZN-LB-POOL-UAG-POD1	HZN-LB-POOL-UAG-POD1
Application Profile	default-udp-lb-app-profile	default-udp-lb-app-profile	default-udp-lb-app-profile
Persistence	HZN-UAG-PERSIST-POD1	HZN-UAG-PERSIST-POD1	HZN-UAG-PERSIST-POD1
Default Pool Member Ports	4172	443	8443
Tag	HZN-UAG-POD1	HZN-UAG-POD1	HZN-UAG-POD1
Scope	HZN-POD1	HZN-POD1	HZN-POD1

HORIZON UNIFIED ACCESS GATEWAY LOAD BALANCER SERVER POOL CONFIGURATION	
Name	HZN-LB-POOL-UAG-POD1
Algorithm	Least Connection
Members/Group	HZN-GRP-UAG-POD1
SNAT Translation Mode	Disabled
Active Monitor	HZN-LB-AMON-UAG-XMLAPI-POD1
Tag	HZN-UAG-POD1
Scope	HZN-POD1

HORIZON UNIFIED ACCESS GATEWAY LOAD BALANCER PROFILE CONFIGURATION	
Profile Type	Persistence
Name	HZN-LB-PERSIST-UAG-POD1
Share Persistence	Enabled
Tag	HZN-UAG-POD1
Scope	HZN-POD1

7.2.4 – Unified Access Gateways – Grouping and Tagging

Grouping for Unified Access Gateways consists of one NSX-T Group for all UAGs and an NSX-T Group with the UAG VIP IP Address as it's member.

NSX-T DESIGN DECISION	
Decision	Justification
One NSX-T Group for all Unified Access Gateways per Pod	NSX-T supports 5000 VMs per Group. Horizon single pod deployments scale to a minimum of 6 UAGs to support the 10000 connection per pod maximum and provide N+1 redundancy.
One NSX-T Group for Unified Access Gateway VIP IPs	NSX-T supports 4000 IP Addresses per IP Set. UAGs require 5 Virtual Server IPs.

Tagging for Horizon UAGs follows the pattern in Table X. Scope should coincide with the Horizon pod number if using the Large Horizon deployment model.

HORIZON UNIFIED ACCESS GATEWAY TAG CONFIGURATION		
Objects	Tag	Scope
Virtual Machines	HZN-UAG-POD1	HZN-POD1
Group	HZN-UAG-POD1	HZN-POD1
Virtual Machines	HZN-UAG-POD(x)	HZN-POD(x) – for Large Model
Group	HZN-UAG-POD(x)	HZN-POD(x) – for Large Model

Horizon UAG Group configuration follows a similar pattern to the tagging table. Tag Scope should coincide with the Horizon pod number if using the Large Horizon deployment model.

HORIZON UNIFIED ACCESS GATEWAY GROUP CONFIGURATION			
Name	Members	Tag	Tag Scope
HZN-GRP-UAG-POD1	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-UAG-POD1* SCOPE *HZN-POD1*	HZN-UAG-POD1	HZN-POD1
HZN-GRP-UAG-VIP-POD1	UAG-LB-VIP-POD1 IP Address	HZN-UAG-POD1	HZN-POD1
HZN-GRP-UAG-POD(x)	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-UAG-POD(x)* SCOPE *HZN-POD(x)*	HZN-UAG-POD(x)	HZN-POD(x)
HZN-GRP-UAG-VIP-POD(x)	UAG-LB-VIP-POD(x) IP Address	HZN-UAG-POD(x)	HZN-POD(x)

7.2.5 Unified Access Gateways – Services

Table X represents the Horizon Services that are representative of the Unified Access Gateways.

HORIZON UNIFIED ACCESS GATEWAY SERVICES CONFIGURATION

Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon 7 Unified Access Gateway to View Connection Server Login	HZN-SVC-HTTPS-443	443	TCP	HZN-CP-HTTPS	SSL
Horizon 7 Unified Blast Extreme TCP Unified Access Gateway to Horizon Agent	HZN-SVC-BLAST-EXTREME-22443-22443	22443	TCP	HZN-CP-BLAST-EXTREME-22443	BLAST
Horizon 7 Unified Blast Extreme UDP Unified Access Gateway to Horizon Agent	HZN-SVC-BLAST-EXTREME-22443-22442	22443	UDP	HZN-CP-BLAST-EXTREME-22443	BLAST
Horizon 7 PCoIP TCP Unified Access Gateway to Horizon Agent	HZN-SVC-PCOIP	4172	TCP	HZN-CP-PCOIP	PCOIP
Horizon 7 PCoIP UDP Unified Access Gateway to Horizon Agent	HZN-SVC-PCOIP	4172	UDP	HZN-CP-PCOIP	PCOIP
Horizon 7 RDP Unified Access Gateway to Horizon Agent	HZN-SVC-RDP	3389	TCP	HZN-CP-RDP	RDP
Horizon 7 CDR MMR Unified Access Gateway to Horizon Agent	HZN-SVC-CDR-MMR	9427	TCP	N/A	N/A
Horizon 7 USB Unified Access Gateway to Horizon Agent USB Redirection	HZN-SVC-32111	32111	TCP	N/A	N/A

7.2.6 Unified Access Gateways – Security

Table X represents the NSX-T DFW Security Policies for securing Unified Access Gateways for Horizon. Security Policies and their rules are placed in the Application Category in the NSX-T DFW.

HORIZON UNIFIED ACCESS GATEWAY SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon – Unified Access Gateway Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Horizon UAG – UAG to Connection Server	HZN-GRP-UAG-POD1	HZN-GRP-CS-VIP-POD1	HZN-SVC-HTTPS-443	HZN-CP-HTTPS	HZN-GRP-UAG-POD1 HZN-GRP-CS-POD1	Allow
Horizon UAG – UAG to Horizon Agent via BLAST Extreme	HZN-GRP-UAG-VIP-POD1	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-BLAST-EXTREME-22443	HZN-CP-BLAST-EXTREME-22443	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-UAG-POD1	Allow

Horizon UAG – UAG to Horizon Agent via PCoIP	HZN-GRP-UAG-VIP-POD1	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-PCOIP	HZN-CP-PCOIP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-UAG-POD1	Allow
Horizon UAG – UAG to Horizon Agent via RDP	HZN-GRP-UAG-VIP-POD1	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-RDP	HZN-CP-RDP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-UAG-POD1	Allow
Horizon UAG – UAG to Horizon Agent CDR MMR	HZN-GRP-UAG-VIP-POD1	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-CDR-MMR	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-UAG-POD1	Allow
Horizon UAG – UAG to Horizon Agent USB Redirection	HZN-GRP-UAG-VIP-POD1	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1	HZN-SVC-32111	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-UAG-POD1	Allow

7.3 Connection Servers

The Horizon Connection Server is an enterprise-class desktop management server that securely brokers and connects users to desktops and published applications and is the key component for Internal Access. Connection Servers authenticate users through Windows Active Directory and direct the request to the appropriate and entitled resource. The Horizon Connection Servers also provide access to the Horizon Administrator Console.

Horizon Connection Servers require networking and load balancing to function in a highly available configuration. NSX-T can provide each of these functions as well as enhancing security around the communications in and out of the Connection Servers well.

7.3.1 Connection Servers – Networking

Horizon Connection Servers are Windows-based machines that only require one connection to the network and can be connected to the same Management Network as the second vNIC of the Horizon Unified Access Gateways.

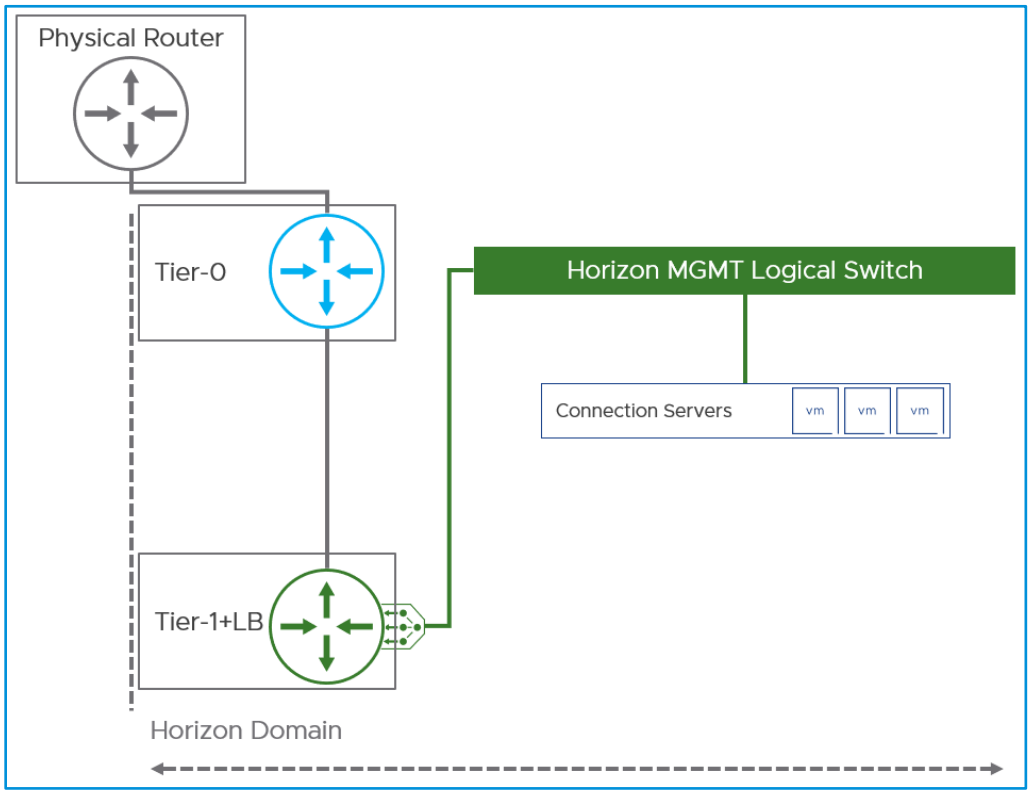

Figure 37- Example NSX-T and Connection Servers Networking

HORIZON CONNECTION SERVER NETWORK CONFIGURATION						
Segment Name	Connected Gateway & Type	Subnet	Transport Zone	VLAN	Tag	Scope
HZN-SEG-MGMT-POD1	HZN-GW-T1-POD1 – Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-UAG-POD1	HZN-POD1

7.3.1 Connection Servers – Edge and Partner Services

Horizon Connection Servers do not require any Edge Service other than Load Balancing, but Horizon Connection Servers run a Windows operating system and can take advantage of Partner Services provided by agentless anti-virus and anti-malware with Endpoint Protection.

HORIZON ENDPOINT PROTECTION CONFIGURATION			
Horizon – Connection Servers AV/AM Policy			
Name	Groups	Service Profiles	Service Deployment
HZN-EPP-CS-POD1	HZN-GRP-CS-POD1	SP-AVAM-PARTNER1-POD1	SD-AVAM-PARTNER1-POD1

7.3.2 Connection Servers – Load Balancing

Horizon Connection Servers are deployment in a scalable fashion with a requirement for at least N+1 redundancy. To achieve this redundancy, Connection Servers can take advantage of NSX-T Load Balancing services provided for the XML-API authentication traffic from the UAGs as well as providing access to the Horizon Administrator Console. The following tables are an example configuration for NSX-T LB with Horizon Connection Servers.

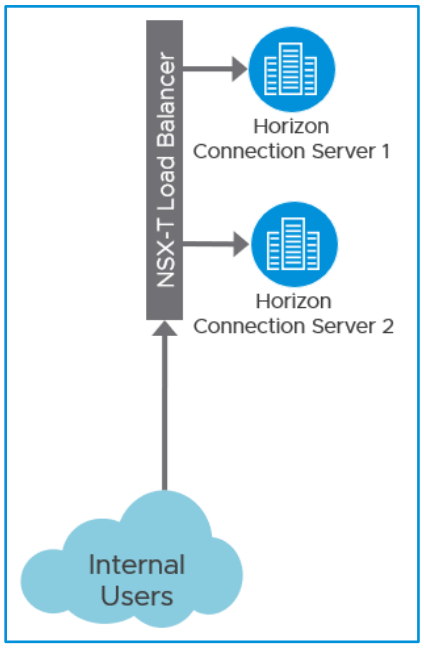

Figure 38 - Horizon Connection Server Load-balancing Topology

HORIZON CONNECTION SERVER LOAD BALANCER CONFIGURATION				
Name	Size	Tier-1 Gateway	Tag	Scope
HZN-LB-POD1	Large	HZN-GW-T1-POD1	HZN-CS-POD1	HZN-POD1

The Horizon Connection Servers require an SSL certificate by installed into the NSX-T Certificates repository for use in the Load Balancer configuration. This document does not go through how to generate an SSL certificate, and you can find detailed instructions for adding the certificate to the NSX-T Manager in the official NSX-T Documentation.

HORIZON CONNECTION SERVER LOAD BALANCER VIRTUAL SERVER CONFIGURATION	
Name	HZN-VIP-CS-XMLAPI-POD1
IP Address	2.2.2.2<Example>
Ports	443
Type	L7 HTTP
Load Balancer	HZN-LB-POD1

Server Pool	HZN-LB-POOL-CS-POD1
Application Profile	Default-http-lb-app-profile
Persistence	Cookie
SSL Configuration	Client SSL – Enabled Default Certificate – Installed CS VIP certificate Client SSL Profile – default-balanced-client-ssl-profile
Cookie	default-cookie-lb-persistence-profile
Default Pool Member Ports	443
Tag	HZN-CS-POD1
Scope	HZN-POD1

HORIZON CONNECTION SERVER LOAD BALANCER SERVER POOL CONFIGURATION	
Name	HZN-LB-POOL-CS-POD1
Algorithm	Least Connection
Members/Group	HZN-GRP-CS-POD1
SNAT Translation Mode	Disabled
Active Monitor	HZN-LB-AMON-CS-HTTPS-POD1
Tag	HZN-CS-POD1
Scope	HZN-POD1

HORIZON CONNECTION SERVER LOAD BALANCER MONITOR CONFIGURATION	
Name	HZN-LB-AMON-CS-HTTPS-POD1
Protocol	HTTPS
Monitoring Port	443
Monitoring Interval	5
Timeout Period	15
Fall Count	3
Rise Count	3
Tag	HZN-CS-POD1
Scope	HZN-POD1
HTTP Request	HTTP Method – GET HTTP Request URL - /favicon.ico HTTP Request Version - 1

HTTP Response	HTTP Response Code - 200
SSL Configuration	No Configuration

7.3.4 Connection Servers – Grouping and Tagging

NSX-T DESIGN DECISION	
Decision	Justification
One NSX-T Group for all Connection Servers per Horizon Pod	NSX-T supports 5000 VMs per Group. Horizon single pod deployments scale to a minimum of 6 Connection Server to support the 10000 connection per pod maximum and N+1 redundancy.
One NSX-T Group for Connection Server VIP IPs	NSX-T supports 4000 IP Addresses per IP Set. Connection Servers require 1 Virtual Server IPs.

Tagging for Horizon Connection Servers follows the pattern in Table X. Scope should coincide with the Horizon pod number if using the Large Horizon deployment model.

HORIZON CONNECTION SERVER TAG CONFIGURATION		
Objects	Tag	Scope
Virtual Machines	HZN-CS-POD1	HZN-POD1
Group	HZN-CS-POD1	HZN-POD1
Virtual Machines	HZN-CS-POD(x)	HZN-POD(x) – for Large Model
Group	HZN-CS-POD(x)	HZN-POD(x) – for Large Model

Horizon Connection Server Group configuration follows a similar pattern to the tagging table. Tag Scope should coincide with the Horizon pod number if using the Large Horizon deployment model.

HORIZON CONNECTION SERVER GROUP CONFIGURATION			
Name	Members	Tag	Tag Scope
HZN-GRP-CS-POD1	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-CS-POD1* SCOPE *HZN-POD1*	HZN-CS-POD1	HZN-POD1
HZN-GRP-CS-VIP-POD1	CS-LB-VIP-POD1 IP Address	HZN-CS-POD1	HZN-POD1
HZN-GRP-CS-POD(x)	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-CS-POD(x)* SCOPE *HZN-POD(x)*	HZN-CS-POD(x)	HZN-POD(x)

HZN-GRP-CS-VIP-POD(x)	CS-LB-VIP-POD(x) IP Address	HZN-CS-POD(x)	HZN-POD(x)
HZN-GRP-CS-ALL-PODS	Groups = HZN-GRP-CS-POD1 – HZN-GRP-CS-POD(x)	HZN-CS-POD-ALL	HZN-POD-ALL

7.3.5 Connection Servers – Services

Table X represents the Horizon Services that are representative of the Horizon Connection Servers.

HORIZON CONNECTION SERVER SERVICES CONFIGURATION					
Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon 7 View Connection Server to MSSQL	HZN-SVC-MSSQL	1433	TCP	HZN-CP-MSSQL	MSSQL
Horizon 7 Blast Extreme TCP View Connection Server to Horizon Agent	HZN-SVC-BLAST-EXTREME-22443	22443	TCP	HZN-CP-BLAST-EXTREME-22443	BLAST
Horizon 7 Blast Extreme UDP View Connection Server to Horizon Agent	HZN-SVC-BLAST-EXTREME-22443	22443	UDP	HZN-CP-BLAST-EXTREME-22443	BLAST
Horizon 7 PCoIP TCP View Connection Server to Horizon Agent	HZN-SVC-PCOIP	4172	TCP	HZN-CP-PCOIP	PCOIP
Horizon 7 PCoIP UDP View Connection Server to Horizon Agent	HZN-SVC-PCOIP	4172	UDP	HZN-CP-PCOIP	PCOIP
Horizon 7 RDP View Connection Server to Horizon Agent	HZN-SVC-RDP	3389	TCP	HZN-CP-RDP	RDP
Horizon 7 CDR MMR View Connection Server to Horizon Agent	HZN-SVC-CDR-MMR	9427	TCP	N/A	N/A
Horizon 7 HTTPS View Connection Server to vCenter Server SOAP	HZN-SVC-SOAP	443	TCP	N/A	N/A
Horizon 7 JMS View Connection Server to View Connection Server Legacy	HZN-SVC-JMS-LEGACY	4100	TCP	N/A	N/A
Horizon 7 JMS View Connection Server to View Connection Server SSL	HZN-SVC-JMS-SSL	4101	TCP	N/A	N/A
Horizon 7 View Connection Server Install Replica	HZN-SVC-REPLICA-32111	32111	TCP	N/A	N/A
Horizon 7 View Connection Server to View Connection Server MS_RPC	HZN-SVC-ALG-MS-RPC	135	TCP	N/A	N/A
Horizon 7 View Connection Server to View Connection Server Replica Install	HZN-SVC-REPLICA-389	389	TCP	N/A	N/A

7.3.6 Connection Servers – Security

Table X represents the NSX-T DFW Security Policies for securing Connection Servers for Horizon. Security Policies and their rules are placed in the Application Category in the NSX-T DFW.

HORIZON CONNECTION SERVER SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon – Connection Server Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Horizon CS – CS to MSSQL	HZN-GRP-CS-POD1	HZN-GRP-MSSQL-POD1	HZN-SVC-MSSQL	HZN-CP-MSSQL	HZN-GRP-CS-POD1 HZN-GRP-MSSQL-POD1	Allow
Horizon CS – CS to Horizon Agent via BLAST Extreme	HZN-GRP-CS-POD1	HZN-GRP-VDI-POOL1 HZN-GRP-RDS-FARM1	HZN-SVC-BLAST-EXTREME-22443	HZN-CP-BLAST-EXTREME-22443	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-CS-POD1	Allow
Horizon CS – CS to Horizon Agent via PCoIP	HZN-GRP-CS-POD1	HZN-GRP-VDI-POOL1 HZN-GRP-RDS-FARM1	HZN-SVC-PCOIP	HZN-CP-PCOIP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-CS-POD1	Allow
Horizon CS – CS to Horizon Agent via RDP	HZN-GRP-CS-POD1	HZN-GRP-VDI-POOL1 HZN-GRP-RDS-FARM1	HZN-SVC-RDP	HZN-CP-RDP	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-CS-POD1	Allow
Horizon CS – CS to Horizon Agent CDR MMR	HZN-GRP-CS-POD1	HZN-GRP-VDI-POOL1 HZN-GRP-RDS-FARM1	HZN-SVC-CDR-MMR	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-CS-POD1	Allow
Horizon CS – CS to Horizon Agent USB Redirection	HZN-GRP-CS-POD1	HZN-GRP-VDI-POOL1 HZN-GRP-RDS-FARM1	HZN-SVC-32111	None	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-RDS-FARM1-POD1 HZN-GRP-CS-POD1	Allow
Horizon CS – CS to Horizon Domain vCenter	HZN-GRP-CS-POD1	HZN-GRP-VCENTER1	HZN-SVC-BLAST-EXTREME-22443	HZN-SVC-BLAST-EXTREME-22443	HZN-GRP-VCENTER1-POD1 HZN-GRP-CS-POD1	Allow

Horizon CS – JMS CS to CS Legacy	HZN-GRP-CS-POD1	HZN-GRP-CS-POD1	HZN-SVC-JMS-LEGACY	None	HZN-GRP-CS-POD1	Allow
Horizon CS – JMS CS to CS SSL	HZN-GRP-CS-POD1	HZN-GRP-CS-POD1	HZN-SVC-JMS-SSL	None	HZN-GRP-CS-POD1	Allow
Horizon CS – CS to CS Replica Install	HZN-GRP-CS-POD1	HZN-GRP-CS-POD1	HZN-SVC-REPLICA-389	None	HZN-GRP-CS-POD1	Allow
Horizon CS – CS to CS MS-RPC	HZN-GRP-CS-POD1	HZN-GRP-CS-POD1	HZN-SVC-ALG-MS-RPC	None	HZN-GRP-CS-POD1	Allow

7.4 Virtual Desktops

Horizon provides the capabilities to create desktop pools that can include thousands of virtual desktops. This process is done by creating a master image and then cloning the image to create more virtual desktops of the same type in the pool. Each virtual desktop needs to be attached to a networking construct for users to be able to access them and for security to be applied. NSX-T can be used to build NSX-T Segments that virtual desktops will be placed on to provide the necessary network and security services.

7.4.1 Virtual Desktops – Networking

Networking for Virtual Desktop VMs consists of one NSX-T Overlay Segment per Horizon VDI Desktop Pool.

NSX-T DESIGN DECISION	
Decision	Justification
One Tier-1 Router for VDI desktops	NSX-T supports 1000 ports per Tier-1 Logical Router and each Segment will have one router port.
One NSX-T Segment Per VDI Desktop Pool	Horizon supports 2000 recommended Instant-Clone desktops per Pool. NSX-T supports 2048 MAC Addresses per NSX-T Segment.
Minimum of Five NSX-T Overlay Segments per Horizon Pod	Horizon supports 10000 desktops per pod. NSX-T will provide a minimum of five NSX-T Overlay Segments to support a full Horizon pod. More Segments can be used as necessary.
No larger than a /21 IP Network per NSX-T Segment	Recommendation for One NSX-T Overlay Segment per VDI Desktop Pool can have a maximum of 2000 Instant-Clone Desktops per NSX-T Overlay Segment. IP Subnet should be no larger than a subnet with a mask larger than /21 which supports 2046 Hosts per subnet
IP Addressing for Partner SVMs for Endpoint Protection	If using Endpoint Protection, partner SVMs require a management IP address on a per SVM, per host basis.

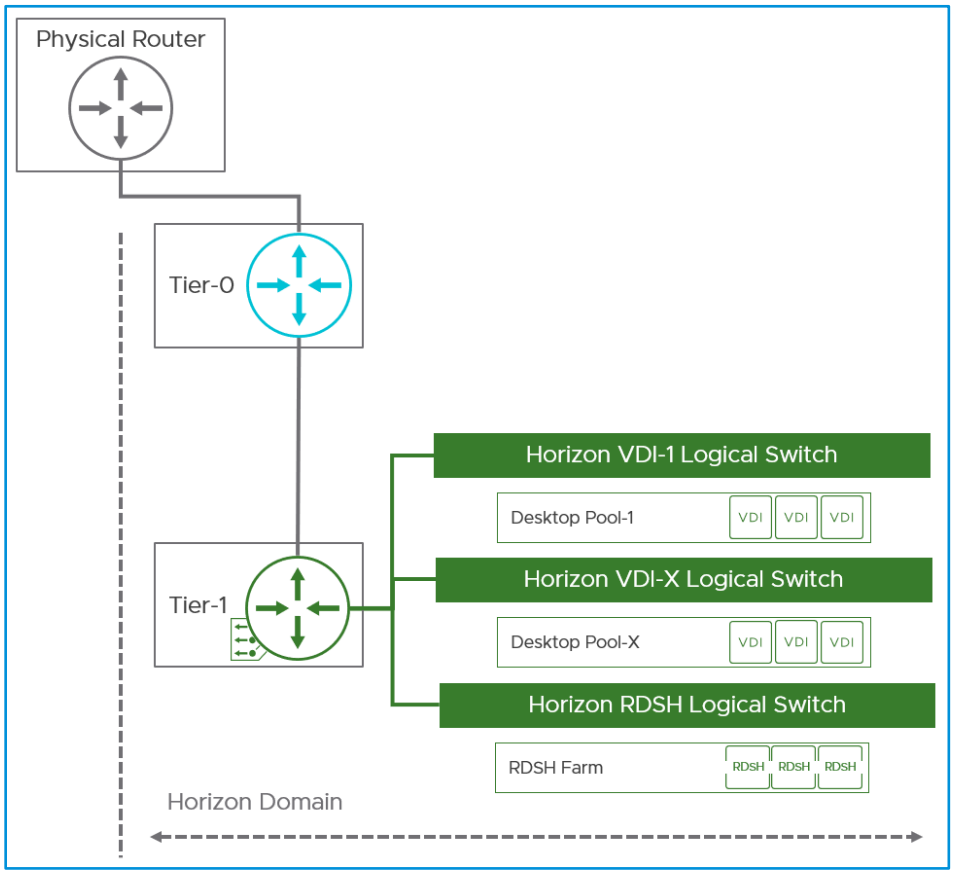

Figure 39 - Example NSX-T and Horizon VDI and RDSH Networking Topology

HORIZON VDI DESKTOP NETWORK CONFIGURATION						
Segment Name	Connected Gateway & Type	Subnet	Transport Zone	VLAN	Tag	Scope
HZN-SEG-VDI-POOL1-POD1	HZN-GW-T1-POD1 – Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-VDI-POOL1-POD1	HZN-POD1
HZN-SEG-VDI-POOL(x)-POD1	HZN-GW-T1-POD1 – Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-VDI-POOL(x)-POD1	HZN-POD1

7.4.2 Virtual Desktops – Edge and Partner Services

Virtual Desktop pools don't typically require Edge based services, but Partner services can include solutions such as anti-virus and anti-malware products. Since there are no native features within NSX-T to provide these functions, NSX-T includes the Guest Introspection platform to integration of 3rd party partner anti-virus and anti-malware solutions.

7.4.3 Virtual Desktops – Guest Introspection

Guest Introspection requires that a partner service is registered with the NSX-T Manager, a Service Deployment has been deployed to the ESXi clusters, and a Service Profile is created. Refer to the Endpoint Protection documentation for NSX-T for step-by-step

instructions on how to add a partner service. With a partner service configured, an Endpoint Protection Policy can be created and applied to the virtual desktop/RDSH NSX-T Groups. Table X represents the Endpoint Protection Policy and Rule for providing agentless AV/AM services to the Horizon desktops and RDS hosts.

HORIZON ENDPOINT PROTECTION CONFIGURATION			
Horizon – Desktop/RDSH AV/AM Policy			
Name	Groups	Service Profiles	Service Deployment
VDI AV/AM	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-VDI-POOL2-POD1 HZN-GRP-VDI-POOL3-POD1 HZN-GRP-VDI-POOL4-POD1 HZN-GRP-VDI-POOL5-POD1	SP-AVAM-PARTNER1-POD1	SD-AVAM-PARTNER1-POD1
RDSH AV/AM	HZN-GRP-RDSH-FARM1-POD1	SP-AVAM-PARTNER1-POD1	SD-AVAM-PARTNER1-POD1

7.4.4 Virtual Desktops – Grouping and Tagging

Grouping for Horizon Virtual Desktops consists of one NSX-T Group per Desktop Pool. Use of dynamic criteria that matches the name of the desktop pool VM names that are created is the recommended approach to placing the desktops into the correct NSX-T Group.

NSX-T DESIGN DECISION	
Decision	Justification
One NSX-T Group for each desktop pool	NSX-T supports 5000 VMs per Group. Horizon supports a recommendation of 2000 VDI desktops per desktop pool.
Five NSX-T Groups for each Horizon Pod (if maxed)	Five pools and 5 NSX-T Groups would be necessary to support the 10000 desktops per Horizon pod.

Tagging for Horizon Virtual Desktop Pools follows the pattern in Table X. Scope should coincide with the Horizon pod number if using the Large Horizon deployment model.

HORIZON VIRTUAL DESKTOP POOL TAG CONFIGURATION		
Objects	Tag	Scope
Virtual Machines	HZN-VDI-POOL1-POD1	HZN-POD1
Group	HZN-VDI-POOL1-POD1	HZN-POD1
Virtual Machines	HZN-VDI-POOL(x)-POD(x)	HZN-POD(x) – for Large Model
Group	HZN-VDI-POOL(x)-POD(x)	HZN-POD(x) – for Large Model

HORIZON VIRTUAL DESKTOP POOL GROUP CONFIGURATION			
Name	Members	Tag	Tag Scope

HZN-GRP-VDI-POOL1-POD1	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-VDI-POOL1* SCOPE *HZN-POOL1-POD1*	HZN-VDI-POOL1-POD1	HZN-POD1
HZN-GRP-VDI-POOL(x)-POD(x)	Criteria – VIRTUAL MACHINE TAG EQUALS *HZN-VDI-POOL(x)* SCOPE *HZN-POD(x)*	HZN-VDI-POOL(x)-POD(x)	HZN-POD(x)

7.4.5 Virtual Desktops - Services

HORIZON VIRTUAL DESKTOP SERVICES CONFIGURATION					
Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon 7 JMS Horizon Agent to Connection Server Enhanced	HZN-SVC-JMS-ENHANCED	4002	TCP	N/A	N/A
Horizon 7 JMS Horizon Agent to Connection Server Legacy	HZN-SVC-JMS-LEGACY	4001	TCP	N/A	N/A

7.4.6 Virtual Desktops – Security

Virtual Desktop systems rarely need to communicate with each other, however the Horizon Agent inside the virtual desktop does require communication from the Horizon Agent installed in the virtual desktops to the Horizon Connection Servers. Table X shows how to write a Security Policy for the Horizon Virtual Desktops without IDFW.

HORIZON VDI POOL SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon – VDI Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Horizon VDI Pool – VDI Pool to Connection Server JMS	HZN-GRP-VDI-POOL1-POD1	HZN-GRP-CS-POD1	HZN-SVC-JMS-ENHANCED HZN-SVC-JMS-LEGACY	None	HZN-GRP-CS-POD1 HZN-GRP-VDI-POOL1-POD1	Allow

7.5 RDS Hosts

Horizon provides the means to distribute applications and published desktops using Microsoft Remote Desktop Session Host capabilities and the Horizon Agent. These systems are provisioned into RDS Farms to facilitate the management of the hosts. From these RDS Farms, Application and RDS Desktop Pools can be created for users to access. Each RDS Hosts needs to be attached to a networking construct for users to be able to access them and for security to be applied. NSX-T can be used to build NSX-T Overlay Segments that RDS Hosts will be placed on to provide the necessary network and security services.

7.5.1 RDS Hosts – Networking

Networking for RDS Hosts consists of at least one NSX-T Overlay Segment that is placed behind a Tier-1 router on the Horizon Domain Compute Cluster.

NSX-T DESIGN DECISION	
Decision	Justification
One NSX-T Overlay Segment Per RDS Host Farm	Horizon supports 500 RDS Hosts per Farm and 10000 sessions per pod. NSX-T supports 2048 MAC Addresses per NSX-T Segment.

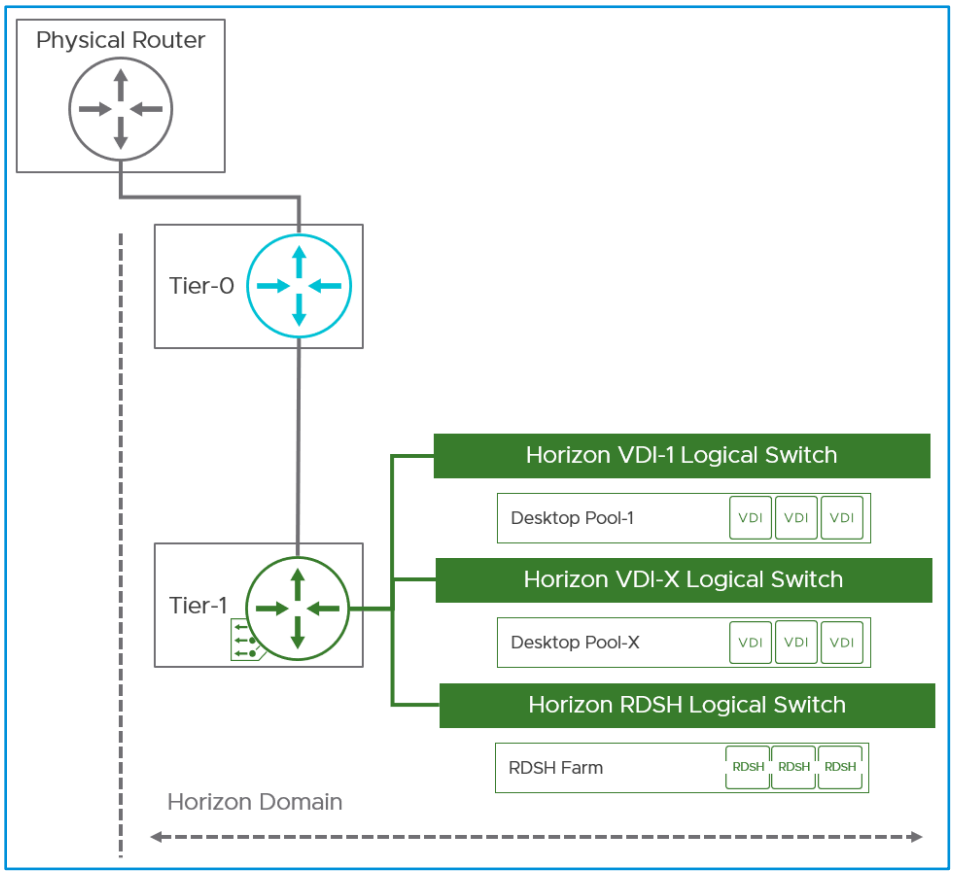

Figure 40 - Example NSX-T and Horizon VDI and RDSH Networking Topology

HORIZON VDI DESKTOP NETWORK CONFIGURATION						
Segment Name	Connected Gateway & Type	Subnet	Transport Zone	VLAN	Tag	Scope
HZN-SEG-RDSH-FARM1-POD1	HZN-GW-T1-POD1 – Flexible	<varies>	Overlay or VLAN	Only used in VLAN TZ case	HZN-RDSH-FARM1-POD1	HZN-POD1

7.4.2. RDS Hosts – Edge and Partner Services

RDS Hosts don't typically require Edge based services, but Partner services generally include solutions such as anti-virus and anti-malware products. Since there are no native features within NSX-T to provide these functions, NSX-T includes the Guest Introspection platform to integration of 3rd party partner anti-virus and anti-malware solutions to provide the necessary protection of these systems.

7.5.2 RDS Hosts – Guest Introspection

Guest Introspection requires that a VMware certified partner Service is registered with the NSX-T Manager, a Service Deployment has been deployed to the ESXi clusters, and a Service Profile is created. Refer to the Endpoint Protection documentation for NSX-T for step-by-step instructions on how to add and configure a partner service. With a partner service configured, an Endpoint Protection Policy can be created and applied to the virtual desktop/RDSH NSX-T Groups. Table X represents the Endpoint Protection Policy and Rules for providing agentless AV/AM services to the Horizon desktops and RDS hosts.

HORIZON ENDPOINT PROTECTION CONFIGURATION			
Horizon – Desktop/RDSH AV/AM Policy			
Name	Groups	Service Profiles	Service Deployment
VDI AV/AM	HZN-GRP-VDI-POOL1-POD1 HZN-GRP-VDI-POOL2-POD1 HZN-GRP-VDI-POOL3-POD1 HZN-GRP-VDI-POOL4-POD1 HZN-GRP-VDI-POOL5-POD1	SP-AVAM-PARTNER1-POD1	SD-AVAM-PARTNER1-POD1
RDSH AV/AM	HZN-GRP-RDSH-FARM1-POD1	SP-AVAM-PARTNER1-POD1	SD-AVAM-PARTNER1-POD1

7.5.3 RDS Hosts – Grouping and Tagging

HORIZON VIRTUAL DESKTOP POOL GROUP CONFIGURATION			
Name	Members	Tag	Tag Scope
HZN-GRP-RDSH-FARM1-POD1	Criteria – **VIRTUAL MACHINE TAG EQUALS** *HZN-RDSH-FARM1-POD1* **SCOPE** *HZN-POD1*	HZN-RDSH-FARM1-POD1	HZN-POD1
HZN-GRP-RDSH-FARM1-POD(x)	Criteria – **VIRTUAL MACHINE TAG EQUALS** *HZN-RDSH-FARM1-POD(x)* **SCOPE** *HZN-POD(x)*	HZN-RDSH-FARM1-POD(x)	HZN-POD(x)

HORIZON RDSH SERVER FARM SERVER TAG CONFIGURATION		
Objects	Tag	Scope
Virtual Machines	HZN-RDSH-FARM1RDSH-FARM1-POD1	HZN-POD1
Group	HZN-RDSH-FARM1RDSH-FARM1-POD1	HZN-POD1
Virtual Machines	HZN-RDSH-FARM1RDSH-FARM1-POD(x)	HZN-POD(x) – for Large Model
Group	HZN-RDSH-FARM1 RDSH-FARM1-POD(x)	HZN-POD(x) – for Large Model

7.5.4 RDS Hosts – Services

HORIZON RDS HOST SERVICES CONFIGURATION					
Horizon Service	NSX-T Service	Port	Protocol	Context Profile	App ID Attribute
Horizon 7 JMS Horizon Agent to Connection Server Enhanced	HZN-SVC-JMS-ENHANCED	4002	TCP	N/A	N/A
Horizon 7 JMS Horizon Agent to Connection Server Legacy	HZN-SVC-JMS-LEGACY	4001	TCP	N/A	N/A

7.5.5 RDS Hosts – Security

HORIZON RDSH FARM SECURITY POLICY CONFIGURATION						
CATEGORY - APPLICATION						
Horizon – RDSH Policy - Applied To DFW						
Name	Sources	Destination	Services	Profiles	Applied To	Action
Horizon VDI Pool – VDI Pool to Connection Server JMS	HZN-GRP-RDSH-FARM1-POD1	HZN-GRP-CS-POD1	HZN-SVC-JMS-ENHANCED HZN-SVC-JMS-LEGACY	None	HZN-GRP-CS-POD1 HZN-GRP-RDSH-FARM1-POD1	Allow

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