WHITE PAPER – **MAY 2017**

VMWARE HORIZON CLOUD WITH HOSTED INFRASTRUCTURE: NETWORKING OVERVIEW

vmware®

Table of Contents

Introduction

VMware Horizon® Cloud Service™ is a family of cloud services from VMware that enables the delivery of virtual desktops and applications to end users on any supported device. Horizon Cloud is available in two ways: as a VMware-hosted infrastructure, in which the entire infrastructure is hosted by VMware, or as an on-premises infrastructure in which you leverage infrastructure available from partners to deploy virtual desktops in your organization's data center. In both scenarios, the infrastructure is managed from the Horizon Cloud application hosted in the cloud.

Purpose

This white paper focuses on the network connectivity options available for Horizon Cloud with Hosted Infrastructure and provides an overview of networking architecture and requirements. It contains the information necessary to obtain approval from your networking, security, and other infrastructure stakeholders during an implementation of Horizon Cloud Services with Hosted Infrastructure. Examples use the fictional MYCOMPANY.

Note: Not all sections are necessarily applicable to your deployment. Optional sections are clearly marked. If you have questions about the specifics of your order, see your Horizon Cloud-Hosted Setup web form, or speak to VMware or a Value- Added Reseller for VMware.

For deployment information beyond networking considerations, see the VMware Horizon Cloud Service with Hosted Infrastructure Deployment Considerations white paper.

Audience

This paper is for network architects, engineers, and administrators who want to familiarize themselves with, or are in the process of, a Horizon Cloud with Hosted Infrastructure implementation. You should be familiar with Windows data center technologies, such as Active Directory, SQL, and Microsoft Management Console. You should also be familiar with cloud computing, network routing, firewall security architecture, site-to-site (S2S) VPNs, and Multi-Protocol Label Switching (MPLS) networks.

Deployment Overview

You can customize connectivity to your Horizon Cloud Hosted Infrastructure tenant based on your use case needs and networking and security requirements. At its most basic, you can set up Horizon Cloud as an isolated, standalone environment with its own network and user services. At its most complex, you fully integrate Horizon Cloud into your organization's network services environment. Figure 1 shows a typical deployment model that includes a Horizon Cloud instance integrated with your organization's environment:

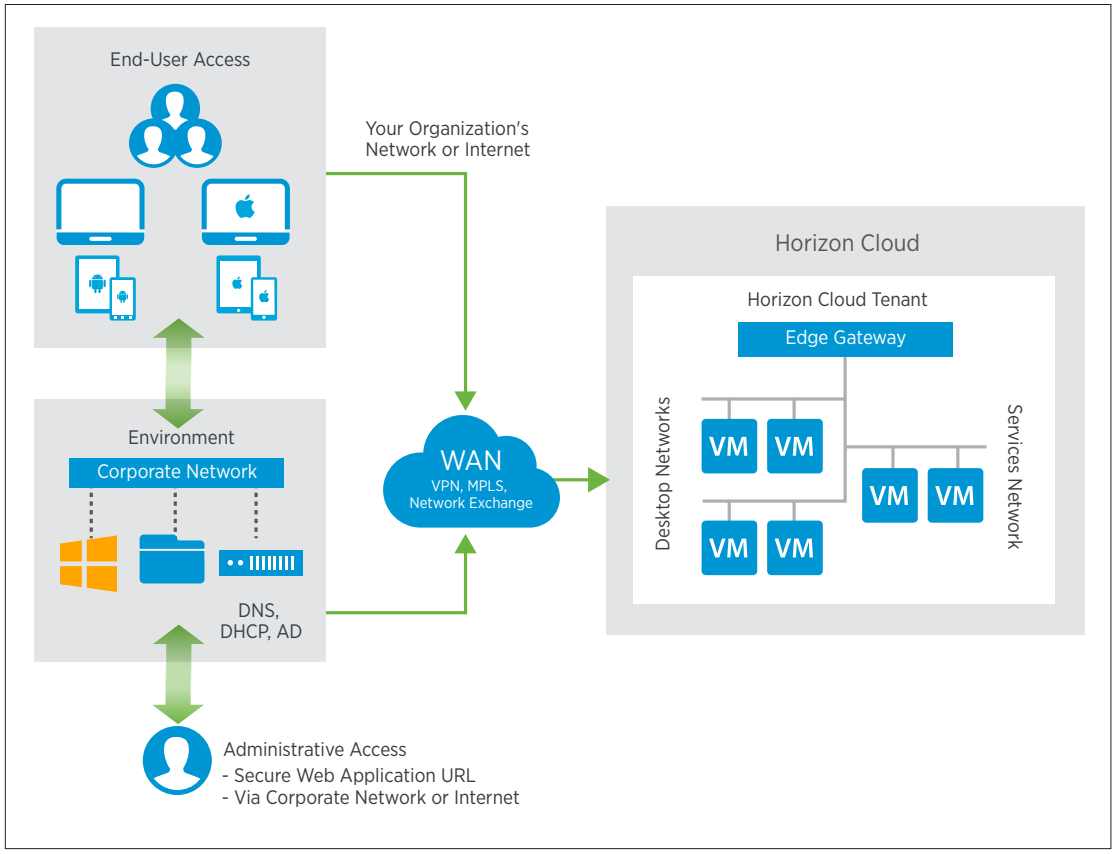

Figure 1: Typical Deployment Mode

This example Horizon Cloud instance includes a connection to your organization's environment using IPsec VPN, Dedicated Connection, MPLS, or Network Exchange to leverage your organization's network, file, and application services. An optional connection can also be made to an infrastructure-as-a-service (IaaS) instance—which can reside in the same data center as Horizon Cloud or in another data center—so that applications and user data can be stored closer to the virtual desktops due to application requirements, potential traffic, or latency concerns over the WAN.

Before You Begin: Decisions and Responsibilities

A successful and expedient deployment depends on good communication between the teams participating in Horizon Cloud so that they work together in a well-integrated manner before, during, and after the kickoff. There are several considerations to keep in mind when deciding what the best configuration options are for your deployment. Collaborate with multiple stakeholders and subject matter experts to find the best option.

Your Decisions

When planning a Horizon Cloud deployment, prepare to answer the following questions:

1. Do I want to integrate the cloud-hosted desktops and hosted applications with my environment to use my existing directory, file, application, and print services?
   a. If yes, how do I want to direct my users' Internet-bound desktop traffic?
      - Through the VMware data center?
      - Through my organization's network?
   b. If yes, how much traffic must traverse the connection between my virtual desktops and hosted applications and my organization's network to access those resources?
      - Is an IPsec VPN sufficient?
      - Or do I need a dedicated connection such as MPLS?
      - Do I need manual or automatic failover for my connection?
   c. If no, which infrastructure do I need to support my use case and where do I put it?
      - Do I need directory, file, and application services?
      - Can I put everything required in the Horizon Cloud tenant?
      - Or do I need an IaaS tenant?
2. Do I want my employees to have access to their desktops from outside my organization's network?
   a. If yes, do I want to use a custom URL or one provided by VMware?
      - Do I want to use `desktop.mycompany.com?`
      - Or do I want to use `mycompany.horizon.vmware.com?`

Note: For questions about desktop subnets and IP addresses, see Appendix B: Subnet Considerations and the VMware Horizon Cloud Service with Hosted Infrastructure Deployment Considerations white paper.

Your Responsibilities

It is important to understand what your responsibilities include and which are shared between your teams and the VMware team. Deploying Horizon Cloud with Hosted Infrastructure can be divided into several basic areas of responsibility, as shown in Table 1.

<table>
<tr><th>PHASE</th><th colspan="4">AREAS OF RESPONSIBILITY</th></tr>
<tr><td>Project Kickoff</td><td colspan="4">Your SMEs with VMware:
• Meet (your lead and VMware lead)
• Include desktop manager, desktop engineering, security, and network SMEs in your team
• Review and discuss provisioning requirements
• Collect information using the Horizon Cloud-Hosted Setup web form
• Establish success criteria via the VMware-supplied template
• Plan next steps</td></tr>
<tr><td>Capacity Order</td><td colspan="4">VMware:
• Orders tenant capacity from data center infrastructure
• Configures capacity for Horizon Cloud with Hosted Infrastructure</td></tr>
<tr><td>Network Setup</td><td colspan="2">VMware:
• Establishes VPN and Direct Connect configurations and access
• Configures DHCP, DNS, VPN, and Direct Connect</td><td colspan="2">Your SMEs
• Configure DHCP, Active Directory, and DNS
• Provide SSL certificates
• Provide VPN and Direct Connect information</td></tr>
<tr><td>Tenant Setup</td><td colspan="4">VMware:
• Sets up Horizon Cloud with Hosted infrastructure
• Configures storage
• Sets up the Unified Access Gateway
• Installs tenant appliances
• Sets standard desktop capacity</td></tr>
<tr><td>Network Interconnect</td><td>VMware:
• Installs SSL certificates</td><td>Your SMEs with VMware:
• Test and validate connectivity</td><td>VMware:
• Provides Horizon Cloud Administration Console URL
• Provides starter image templates</td><td>Your SMEs:
• Perform Active Directory registration
• Perform post-test (optional) and install your apps</td></tr>
<tr><td>Final Setup and Test</td><td>Your SMEs:
• Install applications into VMware-supplied starter image templates</td><td>VMware:
• Imports and moves starter image templates to tenant</td><td>Your SMEs:
• Create images
• Create assignments
• Assign test desktops and validate</td><td>VMware:
• Conducts knowledge transfer
• Establishes support</td></tr>
<tr><td>Complete</td><td colspan="4">Your SMEs with VMware:
• Agree that setup is complete
• VMware provides advanced onboarding services (optional)
• Verify that all success criteria are met</td></tr>
</table>

Table 1: Overview of the Horizon Cloud with Hosted Infrastructure Deployment Process

Your responsibilities – Ensure that all required internal and external network traffic ports for the protocols are enabled (see Prerequisites for Firewall and Ports). You are also responsible for your organization's side of the IPsec VPN tunnel, if you choose to deploy in that configuration. If you deploy a dedicated connection, MPLS, or Network Exchange, you are responsible for working with your preferred carrier or telecommunications provider to establish connectivity to the VMware data center.

VMware responsibilities – Depending on the network connection option you select, VMware provides you with the information you need for success.

- **IPsec VPN** – VMware provides the information required to establish the IPsec tunnel and is responsible for the VMware side of the VPN IPsec tunnel configuration.
- **Dedicated connection, MPLS, Network Exchange, or an existing rack** – VMware configures the interconnect between the Network Service Provider and your networking equipment and your Horizon Cloud tenant in the VMware data center. You must purchase the Direct Connect with Cross Connect option or Direct Connect with Network Exchange option from VMware. For all connectivity types, VMware works with you to perform the necessary network tests to ensure a successful connection.
- **Island tenant** – If you deploy an island tenant without integration between VMware and your infrastructure, VMware provides a utility server to use as an Active Directory, DNS, and DHCP server. To function properly, cloud-hosted desktops require that an Active Directory Domain controller and supporting services be deployed in the tenant.

Prerequisites for Firewall and Ports

The following tables list the ports to use for a successful connection to your Horizon Cloud environment. Open firewall ports include all remote connections going to or from the endpoint device, tenant appliance, and VMware Unified Access Gateway™. You might need additional ports depending on your Active Directory design. For more information, see Active Directory and Active Directory Domain Services Port Requirements. Check with your Horizon Cloud representative to verify that this information is appropriate for your environment.

Local Connections

To successfully connect to Horizon Cloud, allow the ports listed in Table 2 across the IPsec VPN, Dedicated Connection, MPLS, Network Exchange, or existing rack.

SOURCE	DESTINATION	PORTS IN USE	DESCRIPTION
Horizon Cloud	Your Active Directory infrastructure	TCP/389 UDP/389	Authenticates users to the Horizon Client VMware Horizon Cloud Desktop Portal and the VMware Horizon Cloud Administration Console using LDAP or LDAP SASL GSSAPI for secure authentication. The configured user groups and their members are cached in the tenant infrastructure for performance purposes.
Horizon Cloud	Your Active Directory infrastructure	TCP/3268	Performs Active Directory Global Catalog lookup and searches
Horizon Cloud	Your Active Directory infrastructure	TCP/88 UDP/88	Used for Kerberos authentication
Horizon Cloud	Your DNS	TCP/53 UDP/53	Used for DNS
Horizon Cloud	Your DHCP or DHCP relay server	UDP/67 UDP/68	Used for DHCP and DHCP relay
Horizon Cloud	RSA authentication manager	UDP/5500	Communicates with the RSA authentication manager when the tenant is using SecurID. The authentication manager can be located in a different data center from the tenant appliances. A high-availability authentication manager used for failover can also be located remotely.
Horizon Cloud	Your RADIUS server	UDP/1812 UDP/1813	Communicates with RADIUS-based authentication when the tenant is using RADIUS
Your Site and Endpoint Device	Horizon Cloud	TCP/8443 UDP/8443	Used for Blast Extreme
Your Site and Endpoint Device	Horizon Cloud	TCP/443 UDP/443	Used for Blast Extreme
Your Site and Endpoint Device	Horizon Cloud	TCP/4172 UDP/4172	Used for PCoIP

SOURCE	DESTINATION	PORTS IN USE	DESCRIPTION
Your Site and Endpoint Device	Horizon Cloud	TCP/80, TCP/443	Accesses the VMware Horizon Cloud Desktop Portal and the VMware Horizon Cloud Administration Console. Also used by the native Horizon Client to initially connect to Horizon Cloud resources. If remote access is enabled, the desktop portal must be publicly available. Port 80 redirects to port 443.
Your Site and Endpoint Device	Horizon Cloud	TCP/12443	Used for console access within Horizon Helpdesk Console

Table 2: Local Connections

Remote Connections

For a successful connection to a virtual desktop or application from a public (Internet) location, allow the ports listed in Table 3.

SOURCE	DESTINATION	PORTS IN USE	DESCRIPTION
Your Site and Endpoint Device	Horizon Cloud	TCP/8443 UDP/8443	Used for Blast Extreme
Your Site and Endpoint Device	Horizon Cloud	TCP/443 UDP/443	Used for Blast Extreme
Your Site and Endpoint Device	Horizon Cloud	TCP/4172 UDP/4172	Used for PCoIP
Your Site and Endpoint Device	Horizon Cloud	TCP/12443	Used for console access within Horizon Helpdesk Console
Your Site and Endpoint Device	Horizon Cloud	TCP/80, TCP/443	Accesses the VMware Horizon Cloud Desktop Portal and the VMware Horizon Cloud Administration Console. Also used by the native Horizon Client to initially connect to Horizon Cloud resources. If remote access is enabled, the desktop portal must be publicly available. Port 80 redirects to port 443.

Table 3: Remote Connections

Endpoint Operating System Firewall Ports

If you have an endpoint-based firewall solution, make sure that the ports listed in Table 4 are open on your virtual desktops or Remote Desktop Session Host (RDSH) servers for a successful connection.

SOURCE	DESTINATION	PORTS IN USE	DESCRIPTION
Horizon Cloud	Desktop or RDSH server	TCP/22443 UDP/22443	Used for Blast Extreme
Horizon Cloud	Desktop or RDSH server	TCP/32111	Used for USB
Horizon Cloud	Desktop or RDSH server	TCP/9427	Used for client drive redirection (CDR) and multimedia redirection (MMR)
Horizon Cloud	Desktop or RDSH server	TCP/4172 UDP/4172	Used for PCoIP

Table 4: Endpoint Operating System Firewall Ports

Bandwidth Considerations

Challenges in providing a good user experience include latency, protocol choice, distance, bandwidth, and connection outages. Consider the following elements when choosing your networking solution:

- **Requirements of your organization** – The needs of every organization are different. Assess your needs, such as the type of computing tasks and workloads expected, graphics intensity, user location, peripherals used, and average bandwidth usage of each type of user.
- **Bandwidth consumption** – Many elements can affect network bandwidth, including protocol choice, monitor resolution and configuration, and the amount of multimedia content in the workload. Concurrent launches of streamed applications can also cause usage spikes. Because the effects vary widely, many organizations monitor bandwidth consumption as part of a pilot project.
- **Traffic traversing the connection** – Consider the amount of traffic required for accessing your organization's applications, file servers, and authentication.
- **CPU and RAM saturation** – Examine the physical network device used for the connection to Horizon Cloud to understand your current CPU and RAM saturation and available throughput. Older devices might not be able to simultaneously maintain high speeds, encryption, and multiple tunnels.
- **Bandwidth** – When deploying Horizon Cloud and leveraging Horizon Cloud–provided Internet connectivity, a specific amount of network bandwidth is guaranteed, called *peak bandwidth*, which is based on the number and model of desktops deployed. This is the bandwidth allotted for as a part of the connection to the Internet from the Horizon Cloud Service. For more information, see the Service Description: VMware Horizon Cloud Service with Hosted Infrastructure.
- **Network and application assessment** – To ensure a successful Horizon Cloud deployment, perform a thorough network and application assessment to determine the configuration to support the necessary bandwidth while meeting latency and packet loss requirements. Include all active application traffic across the end-to-end network to ensure that sufficient minimum bandwidth is available, even with network congestion. For more information about tools for application assessment, see SysTrack Desktop Assessment, Part 1: Moving to VDI? Details You Should Know.
- **Optimization controls available with PCoIP and Blast Extreme** – If you use the PCoIP or Blast Extreme display protocol from VMware, you can adjust several elements that affect bandwidth usage. For more information, see the *PCoIP General Settings* and *VMware Blast Policy Settings* sections in Setting Up Desktop and Application Pools in View – VMware Horizon 7.0.

VPN and Direct Connect

Before deploying Horizon Cloud, determine the type of network connection to implement. The network connection delivers Horizon Cloud desktops and RDSH server access to applications and data in your data center and network. It also provides a path for users—both inside and outside your network—to connect to Horizon Cloud desktop and application resources. It is important to engage the necessary management and networking personnel with the appropriate skill sets to address the following considerations and efficiently facilitate the integration of Horizon Cloud with your environment.

Figure 2 shows the network access options using IPsec VPN and Direct Connect, which is either a dedicated connection, MPLS, Network Exchange, or your rack.

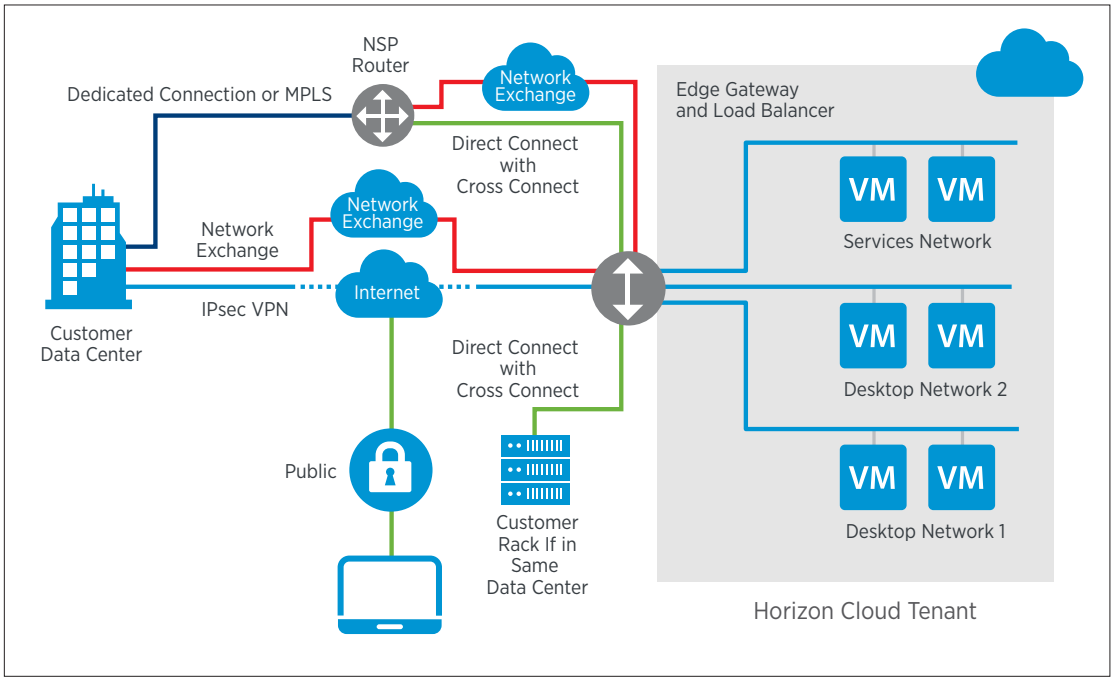

Figure 2: Access Strategies for a Horizon Cloud with Hosted Infrastructure Deployment

Accessing Horizon Cloud from the Internet

Horizon Cloud supports direct Internet access to Horizon Cloud with hosted-infrastructure desktops and RDSH applications without passing through your organization's infrastructure first. This type of connection is particularly convenient for users working from home or other remote locations. The connection can be secured with RSA SecurID or RADIUS-compliant two-factor authentication solutions. Internet-based connections are part of the standard Horizon Cloud service offering.

Choosing the Ideal Type of Network Connection

Consult the Horizon Cloud team when choosing between the two main connectivity options. The choice depends on a number of variables within your environment, including the number of desktops, RDSH servers, and the type of traffic occurring over the network connection, as follows:

- **IPsec VPN** – An IPsec VPN can be used for a variety of scenarios, although with a maximum bandwidth of 1 GB, VPN tends to be used in smaller implementations.
- **Dedicated connection, MPLS, or Network Exchange** – A dedicated connection, MPLS Direct Connect, or Network Exchange is usually recommended for large numbers of desktops and RDSH servers and for heavy use, such as multiple users accessing the platform simultaneously, accessing multiple applications, or performing large file transfers.

Note: Ease of troubleshooting differs between these two options. Troubleshooting an IPsec VPN can be challenging because an IPsec VPN runs over the public Internet. When troubleshooting a dedicated connection, MPLS Direct Connect, or Network Exchange, the circuit is yours from end to end, and you can call the provider to resolve issues.

Understanding VPN

Take VPNs, router hardware, and the IPsec configuration into account when setting up network connectivity to Horizon Cloud.

Sending Traffic Through a Site-to-Site IPsec VPN

Site-to-site IPsec VPNs connect separate networks to each other through the public Internet. For example, a branch office network can connect by site-to-site VPN to a headquarters network. Each site on the network is equipped with a VPN gateway, such as a router, firewall, VPN concentrator, or security appliance. For more information, see Virtual private network (VPN).

Setting up an IPsec VPN connection from a remote network to Horizon Cloud is the most common scenario, because of the relative simplicity and short amount of time necessary to establish the IPsec VPN tunnel. When using IPsec VPN, maximum bandwidth is approximately 1 Gbps because of the limitation of the Edge Gateway.

The site-to-site IPsec VPN tunnel includes logical and encrypted point-to-point connections between Horizon Cloud instances and your organization's site. These connections provide secure access to your organization's data center services, such as business applications, Active Directory, DNS, and DHCP servers. They also provide secure access for protocol traffic originating from your organization's networks.

When setting up an IPsec VPN connection from a remote network to Horizon Cloud, keep the following in mind:

- **Latency spikes** – The IPsec VPN tunnel is built through the public Internet and is subject to congestion or other network-related problems common on public Internet connections that can increase latency. Latency spikes caused by the public Internet are beyond the control of both your enterprise and Horizon Cloud.
- **Setup** – When setting up IPsec VPNs, it is recommended that the VPNs be managed using router hardware for performance reasons. Setting up VPNs using a Windows server is not recommended. Multiple VPN connections are supported, although they must not have the same source and destination lists because the Edge Gateway cannot determine which IPsec tunnel to route traffic to.
- **Redundancy** – Incorporating two IPsec VPNs for redundancy is an option, but bonding the VPNs is not supported. The first VPN is set as active, and the secondary VPN is disabled. Horizon Cloud does not provide automated failover for VPNs. If a failure occurs, the VPN must be manually failed over.
- **Horizon Cloud Hosted Setup web form** – During the VPN setup, you provide information in the Horizon Cloud Hosted Setup web form, including your router vendor, router model, and endpoint IP address. VMware provides the endpoint IP address of your Horizon Cloud tenant, which is used in establishing the IPsec VPN tunnel. This IP address is provided during the deployment of the Horizon Cloud service.
- **Subnets** – You must provide which subnets are allowed across the VPN connection, commonly referred to as the Protected Networks list or source and destination lists. The list defines the internal networks that can traverse the VPN to access your virtual desktops and RDSH-hosted applications from within your network, along with what the virtual desktops and RDSH-hosted applications are able to access across the VPN for different services within your network.
- **Network routing** – For VPN-based connections to Horizon Cloud, static routing is configured during the VPN peering process. If other networking routing questions arise, notify the Horizon Cloud team as soon as possible so that they can be addressed.

IPsec VPN Parameters

The Horizon Cloud Hosted Setup web form lists the required and optional IPsec VPN protocols and parameters if you choose to set up a site-to-site VPN between your network and the VMware data center. For IPsec VPNs, Horizon Cloud uses Edge Gateway, a virtual appliance that provides additional security options and features. Edge Gateway supports Main mode for Phase 1 and Quick mode for Phase 2. For an explanation of these terms, consult your networking engineer or the VMware NSX Administration Guide.

Table 5 lists the protocols and parameters to use in each phase. You must set the same protocols and parameters for each phase on your network as in Horizon Cloud. For example, ISAKMP parameters are used for Phase 1, IKE parameters are used for Phase 2, and Oakley protocols are used for authentication as well as MODP Group 2. All parameters are required. In the upgrade to Edge Gateway, the Phase 2 Perfect Forward Secrecy (PFS) for rekeying is optional.

PROTOCOLS AND PARAMETERS	PHASE 1	PHASE 2
Hash (SHA or MD5)	SHA1	SHA1
Authentication mode	Main	Quick
Encryption	AES, AES256, Triple DES, AES-GCM	AES, AES256, Triple DES, AES-GCM
Diffie-Hellman Group (2, 5, 14, 15, or 16)	2	2
Encapsulation (AH or ESP)	N/A	ESP
Lifetime	28800	3600
Perfect Forward Secrecy	N/A	True. Requirements of shared secret: You can provide your own shared secret, or Horizon Cloud can generate a random shared secret to use on both sides. • Between 32 and 128 characters • At least 1 uppercase letter • At least 1 lowercase letter • At least 1 number • No special characters

Table 5: Recommended IPsec VPN Configuration

Note: Some IPsec VPN parameters, such as the Security Association (SA) lifetime timers, which define the lifetime that a given tunnel uses to encrypt data, cannot be changed in Edge Gateway. These parameters must be changed on the tenant equipment to match those in Edge Gateway. The deployment process includes two phases, and both Phase 1 and Phase 2 include SA lifetime timers. When the SA timer expires, it renegotiates authentication for both sides. However, Edge Gateway does not re-authenticate on traffic, it re-authenticates only on the lifetime timer. Therefore, if the timers are not set on the tenant side to match those on the Horizon Cloud side, they can cause problems in the VPN tunnel.

VPN Connectivity Options

You have several connectivity options to choose from when using a VPN to connect from your enterprise to Horizon Cloud. One option, known as an *island tenant*, does not use a dedicated VPN or permanent connection to your enterprise. The other two options highlight the different routing configurations available for in-guest Internet and user traffic flow based on how you prefer to leverage the VPN connection. A key consideration in the process is choosing how Internet traffic is routed from Horizon Cloud desktops and applications: through an Internet connection provided by Horizon Cloud or through your own network.

Connectivity Option 1: Island Tenant (No VPN)

The fastest and easiest option for deploying Horizon Cloud is to set up an island tenant. As shown in Figure 3, all protocol and in-guest traffic traverses through the Horizon Cloud gateway into the Horizon Cloud tenant. There is no connection between the customer network and the Horizon Cloud tenant. All desktop users, published applications, and RDSH servers connect through the Internet. For more information about possible use cases for island tenants, see Appendix A: Choosing Between Integrated or Isolated Active Directory.

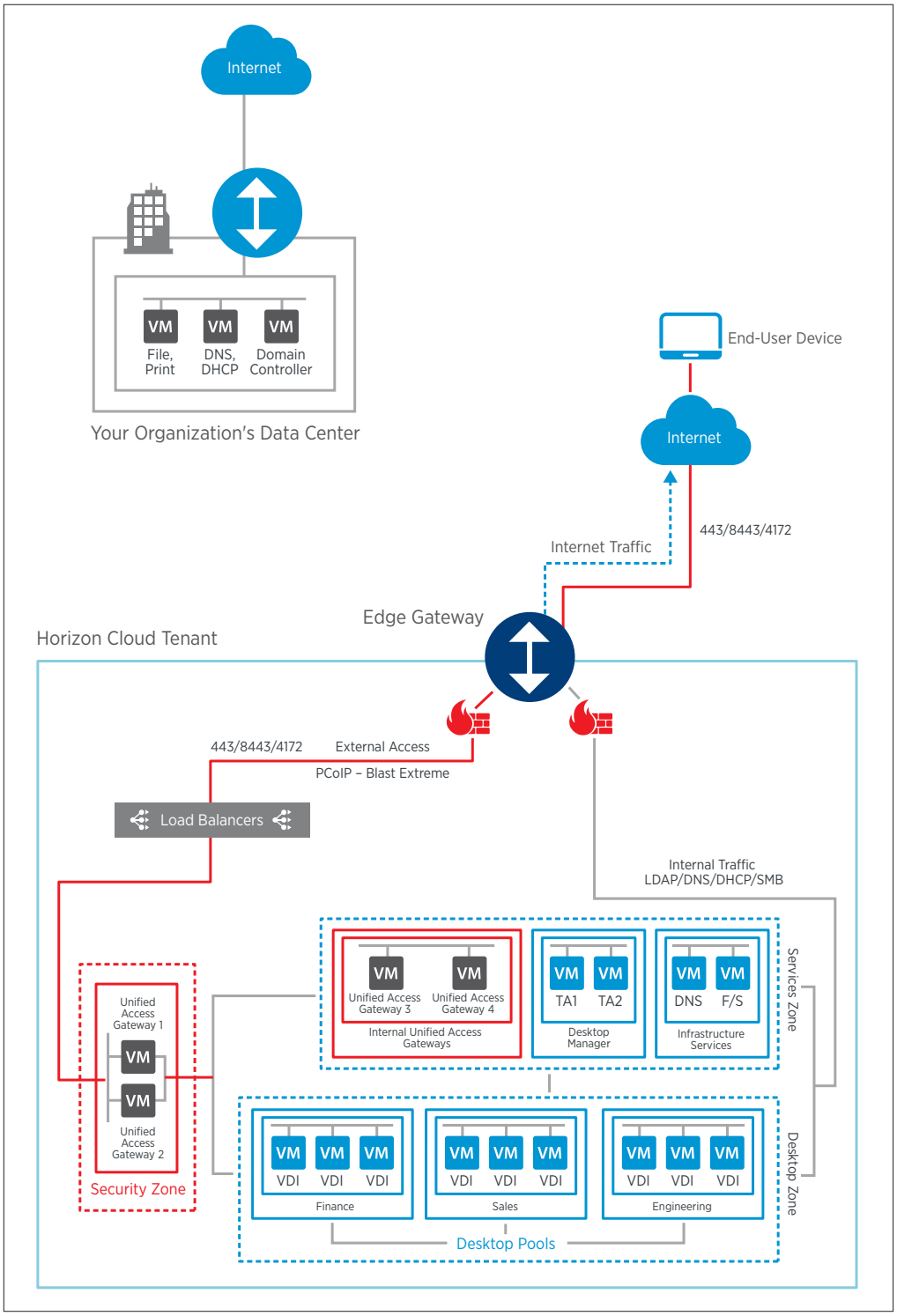

Figure 3: Isolated Island Tenant Deployment Model

Connectivity Option 2: VPN Using the Horizon Cloud Internet Connection

The most common method of connectivity for Horizon Cloud deployments is to configure a VPN between your organization's network and your Horizon Cloud tenant. This method most closely resembles a branch office environment.

This option routes users' desktop Internet-bound traffic out through the Horizon Cloud gateway, while all in-guest traffic, such as desktop applications, authentication, DHCP, and DNS, traverses the VPN to your organization's network. You also have the option of allowing all users to connect through the Internet or allowing only local users to connect over the VPN while external users connect through the Internet into the Horizon Cloud desktops and RDSH servers.

As shown in Figure 4, protocol traffic for external users connecting to the desktops and RDSH servers also passes through the Horizon Cloud gateway to the Unified Access Gateway. The Unified Access Gateway acts as a secure proxy for your connection into the Horizon Cloud environment and proxies Horizon Cloud traffic to and from the Security Zone. Protocol traffic for users connecting from your organization's network can be configured to connect through the Internet or to traverse the VPN to reach the desktops and RDSH servers. Internal users also connect through Unified Access Gateways that are located in internal trusted zones.

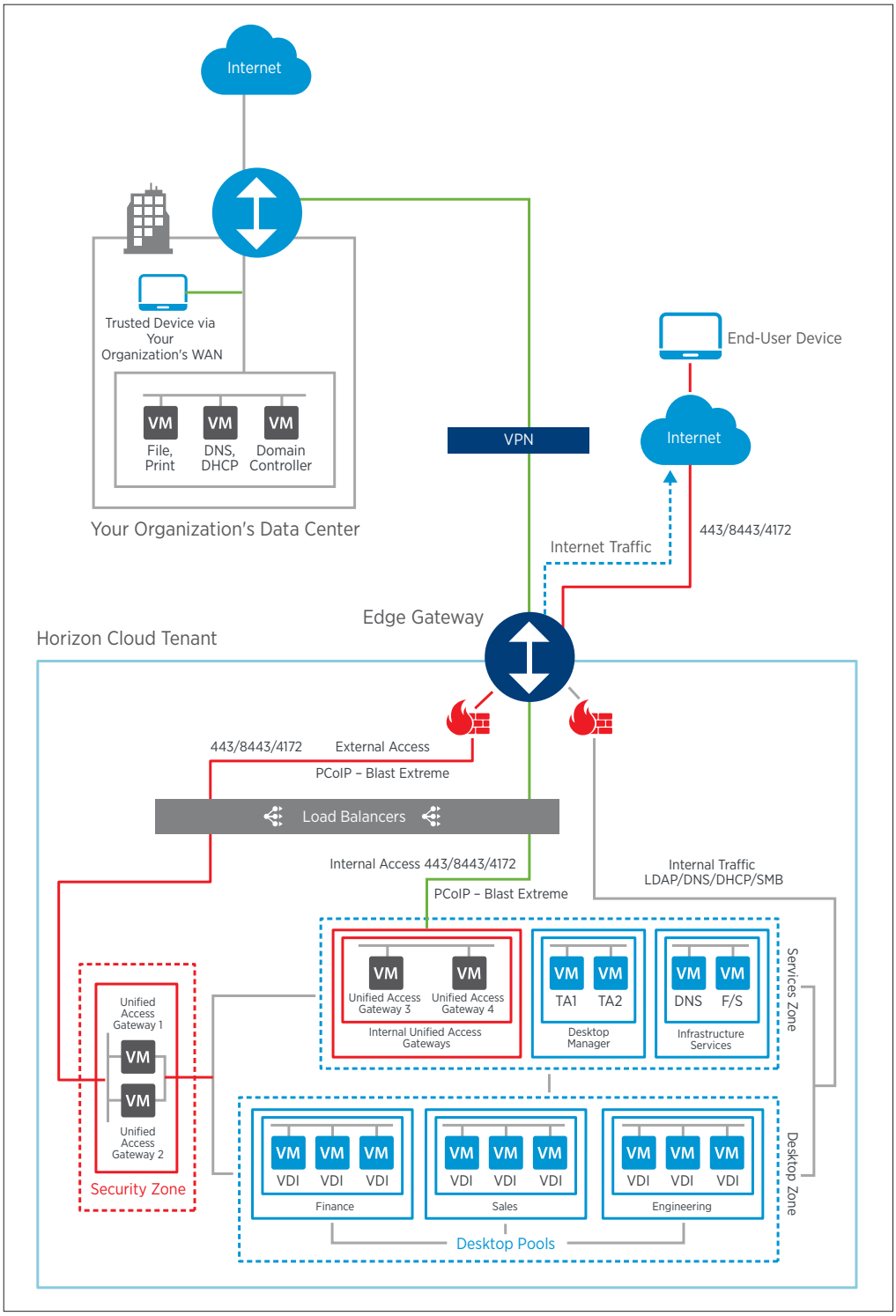

Figure 4: VPN with Internet Traffic

Connectivity Option 3: VPN with Internet-Bound Traffic Through Your Organization's Gateway

This option routes all user Internet-bound and in-guest traffic across the VPN to your organization's network. You maintain the ability to allow all users to connect to Horizon Cloud through the Internet, over the VPN, or a combination of the two.

All in-guest traffic, such as desktop applications, authentication, DHCP, and DNS, as well as the Internet-bound desktop traffic, traverses the VPN and passes through your organization's gateway. The Internet-bound traffic can then be subjected to any web filtering that you have in place. Protocol traffic for external users who are connecting to the desktops and RDSH servers passes through the Horizon Cloud gateway, which provides access through the Internet.

As shown in Figure 5, this option increases the traffic over the VPN, but provides the business advantage of enabling full visibility and control over user and desktop activity. This configuration provides additional options to ensure the highest levels of security and regulatory compliance.

Note: This option does not directly work when moving to a Direct Connect configuration. If you anticipate scaling past the available VPN bandwidth, consult your Horizon Cloud representative to fully understand your options and considerations.

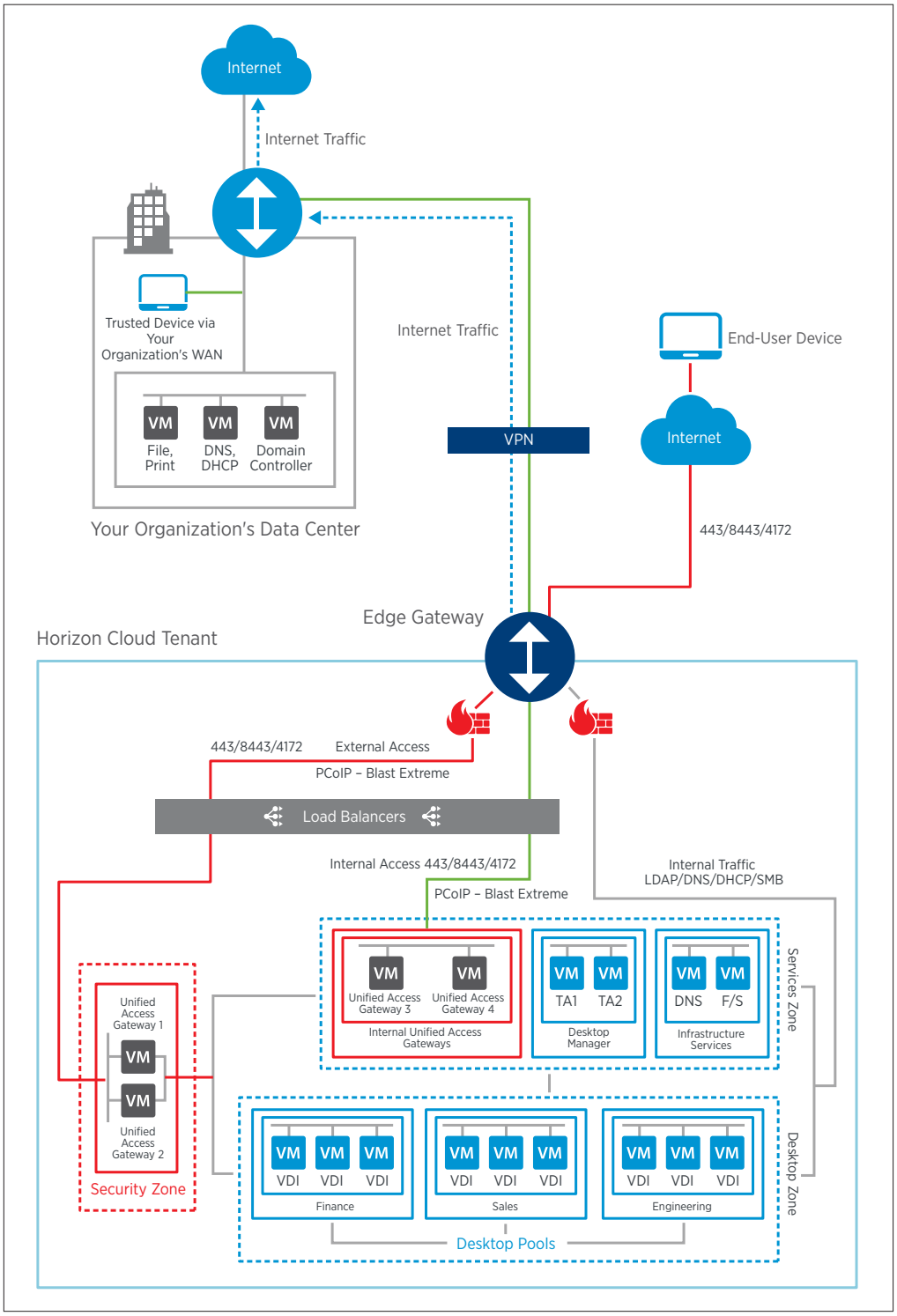

Figure 5: VPN with Desktop Internet Through Your Organization's Gateway

Understanding Direct Connect

Direct Connect allows you to set up an end-to-end private connection with your Horizon Cloud tenant through a dedicated connection, MPLS, Network Exchange, or your own networking equipment located in the same data center. Horizon Cloud offers a 1 GB or 10 GB port when extending your data center and services, such as business applications, Active Directory, DNS, and DHCP servers, into Horizon Cloud. A Direct Connect gives you full control of the connection from your data center to the VMware data center by contract through your network service provider. The supported Direct Connect options are Direct Connect with Cross Connect 1 GB or 10 GB and Direct Connect with Network Exchange 1 GB or 10 GB. Direct Connect with Cross Connect is used with a dedicated connection, MPLS, or your own networking equipment located in the same data center. Direct Connect with Network Exchange is used when connecting to a network or cloud exchange, such as Equinix Cloud Exchange.

Areas of Ownership for Direct Connect Options

As shown in Figure 6, the areas of ownership are divided in a typical Horizon Cloud with Hosted Infrastructure deployment for Direct Connect options. The Meet Me Room represents the point of demarcation where the outside connections come into the data center, such as an outside dedicated connection, MPLS line, or network exchange connecting with the Horizon Cloud network.

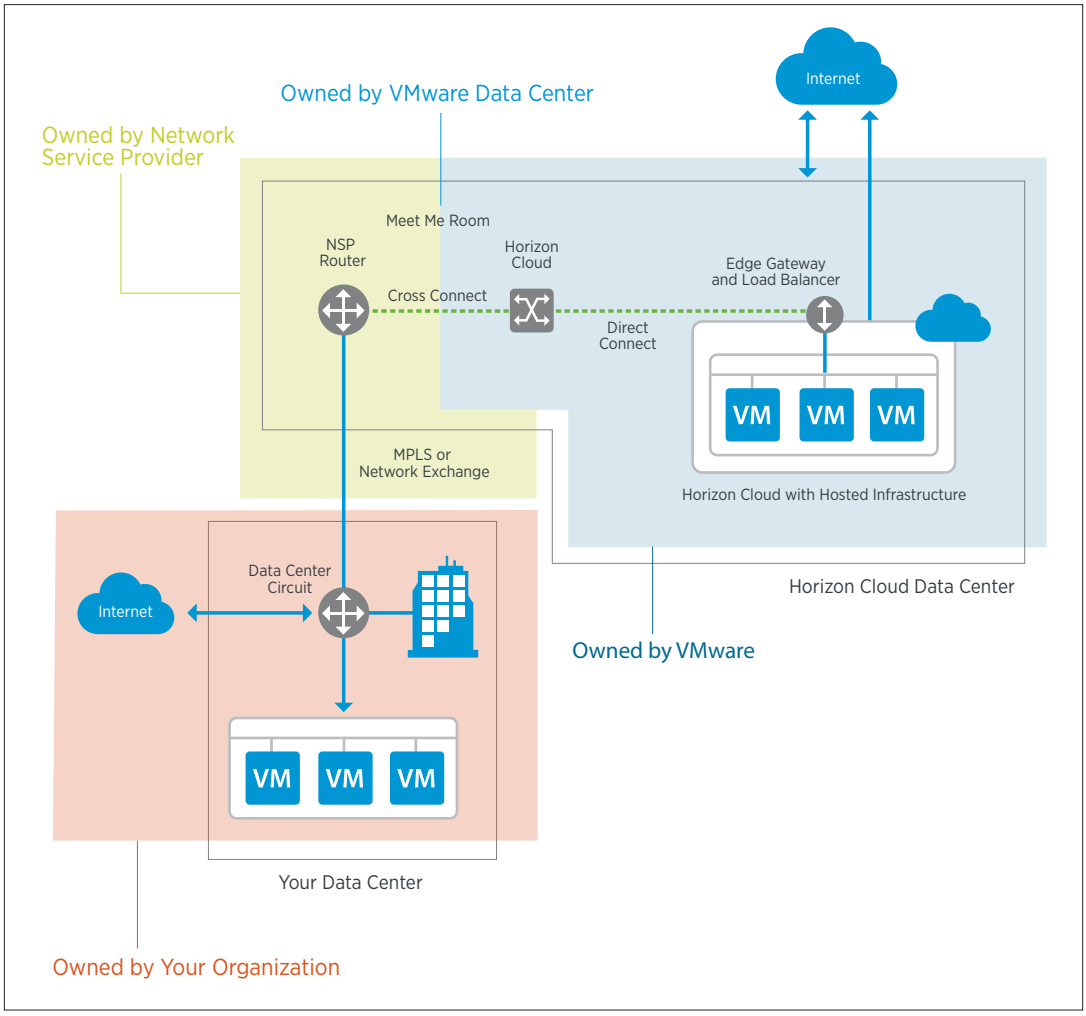

Figure 6: Areas of Ownership

Sending Traffic Through a Dedicated Connection or MPLS Direct Connect VPN

A dedicated connection or MPLS routes traffic within a telecommunications network as data travels from one network node to the next. Building an MPLS Direct Connect VPN tunnel has a higher cost than creating a site-to-site IPsec VPN connection, but provides some advantages. MPLS Direct Connect circuits are not shared with others, as is done with connections routed over the Internet, so they are free of the interruptions that can occur on the public Internet. Direct Connect providers offer committed bandwidth and service-level agreements. The cost of the service depends on the options you choose and the amount of dedicated bandwidth you require.

Sending Traffic Through a Network Exchange

A network exchange, also known as a cloud exchange, is a service that connects your private network using your preferred network service provider with cloud service providers, such as Horizon Cloud, using secure, high-throughput, low-latency connections.

A network exchange usually has a lower cost than creating an MPLS Direct Connect VPN tunnel, and in most cases, can be activated within hours, reducing the overall time it takes to connect Horizon Cloud to your organization's site. Horizon Cloud offers Equinix Cloud Exchange as the network exchange option.

Connecting Your Existing Rack in the Same Data Center

If you already have IT resources and services that are collocated in the same data center as Horizon Cloud, you can connect your existing environment to your Horizon Cloud tenant.

Direct Connect Connectivity Options

You have several Direct Connect connectivity options to choose from, which provide additional bandwidth and control of your organization's corporate and user data flows based on your configuration. Besides bandwidth requirements, a key consideration is choosing how Internet traffic is routed from Horizon Cloud desktops and applications: through an Internet connection provided by Horizon Cloud or over the Direct Connect to your own network. Work with your Horizon Cloud team to choose a Direct Connect option that best matches your organization's needs.

Direct Connect Option 1: Direct Connect Using the Horizon Cloud Internet Connection

Similar to VPN Option 2, this option routes Internet-bound desktop traffic to use the Horizon Cloud gateway and in-guest traffic using Direct Connect. This option is a good choice when you have a significant amount of in-guest application traffic using Direct Connect and you want to take advantage of the VMware Internet bandwidth provided with your tenant.

As shown in Figure 7, all in-guest traffic, such as desktop applications, authentication, DHCP, and DNS, traverses Direct Connect to your organization's network. Desktop and RDSH server traffic destined for the Internet is directed out the Horizon Cloud gateway.

Protocol traffic for external users connecting to the desktops and RDSH servers also passes through the Horizon Cloud gateway to the Unified Access Gateway. The Unified Access Gateway acts as a secure proxy for your connection into the Horizon Cloud environment and proxies Horizon Cloud traffic to and from the Security Zone. Protocol traffic for users connecting from your organization's network can be configured to connect through the Internet or to traverse Direct Connect to reach the desktops and RDSH servers. Internal users also connect through Unified Access Gateways that are located in internal trusted zones.

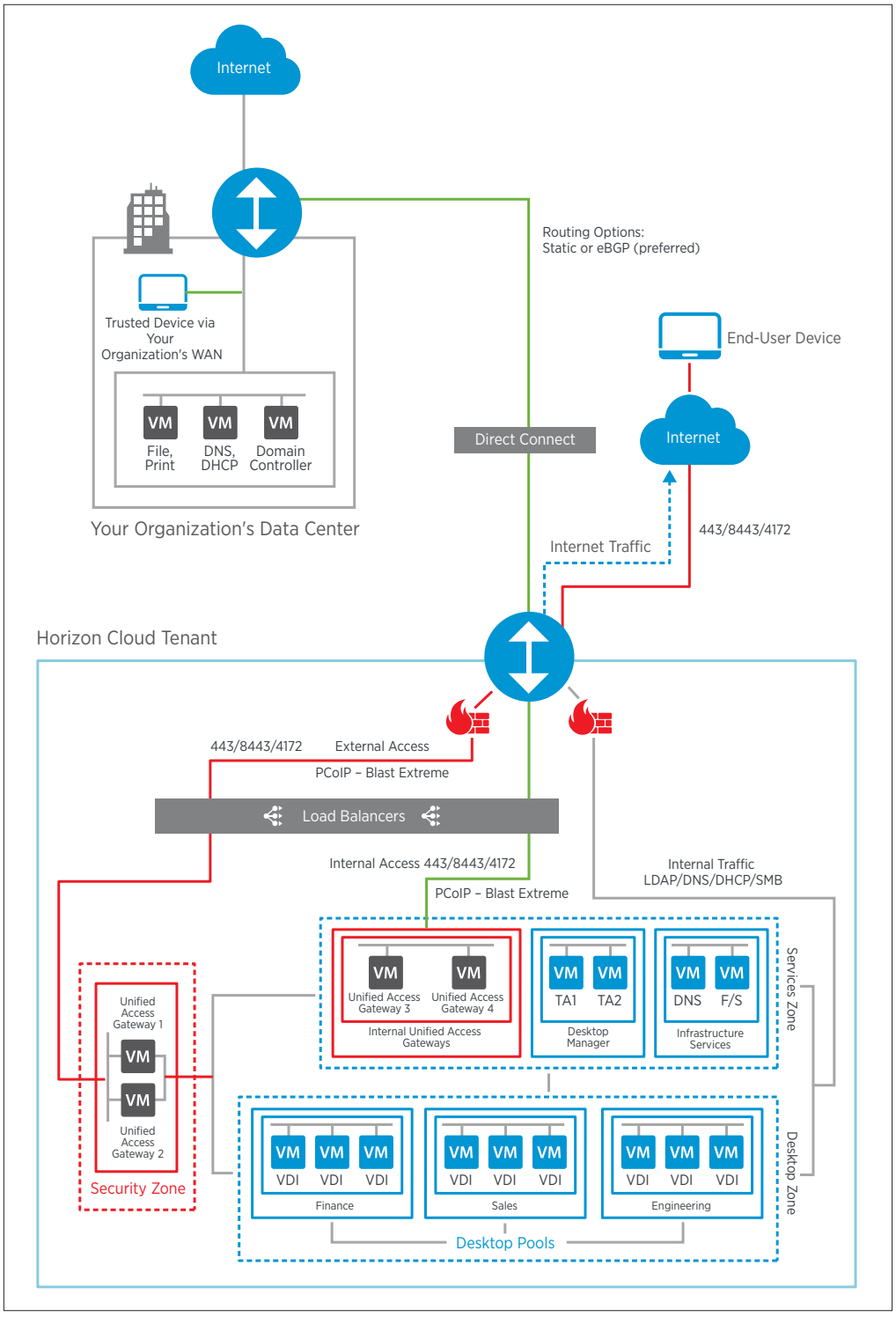

Figure 7: Connectivity Using the Horizon Cloud Internet Connection

Direct Connect Option 2: Direct Connect with Internet over Company-Owned Internet Gateway

This Direct Connect routing configuration is a good choice when you require all in-guest and Internet-bound desktop traffic to traverse Direct Connect through your company-owned Internet gateway, but also require users to be able to connect over the Internet. Desktop traffic destined for the Internet must be managed either using your provided proxy agent or through a group policy configuration because no desktop traffic traverses the VMware gateway.

As shown in Figure 8, external user protocol traffic flows through the Horizon Cloud gateway to provide access to desktops and applications, but all in-guest traffic and Internet-bound desktop traffic traverses Direct Connect to your organization's data center. This option provides the advantage of enabling full visibility and control over user and desktop activity. However, it can pose significant challenges with routing the protocol traffic coming in from the Internet by preventing users from connecting remotely to the environment. If you are considering this option, consult your Horizon Cloud representative to fully understand the considerations.

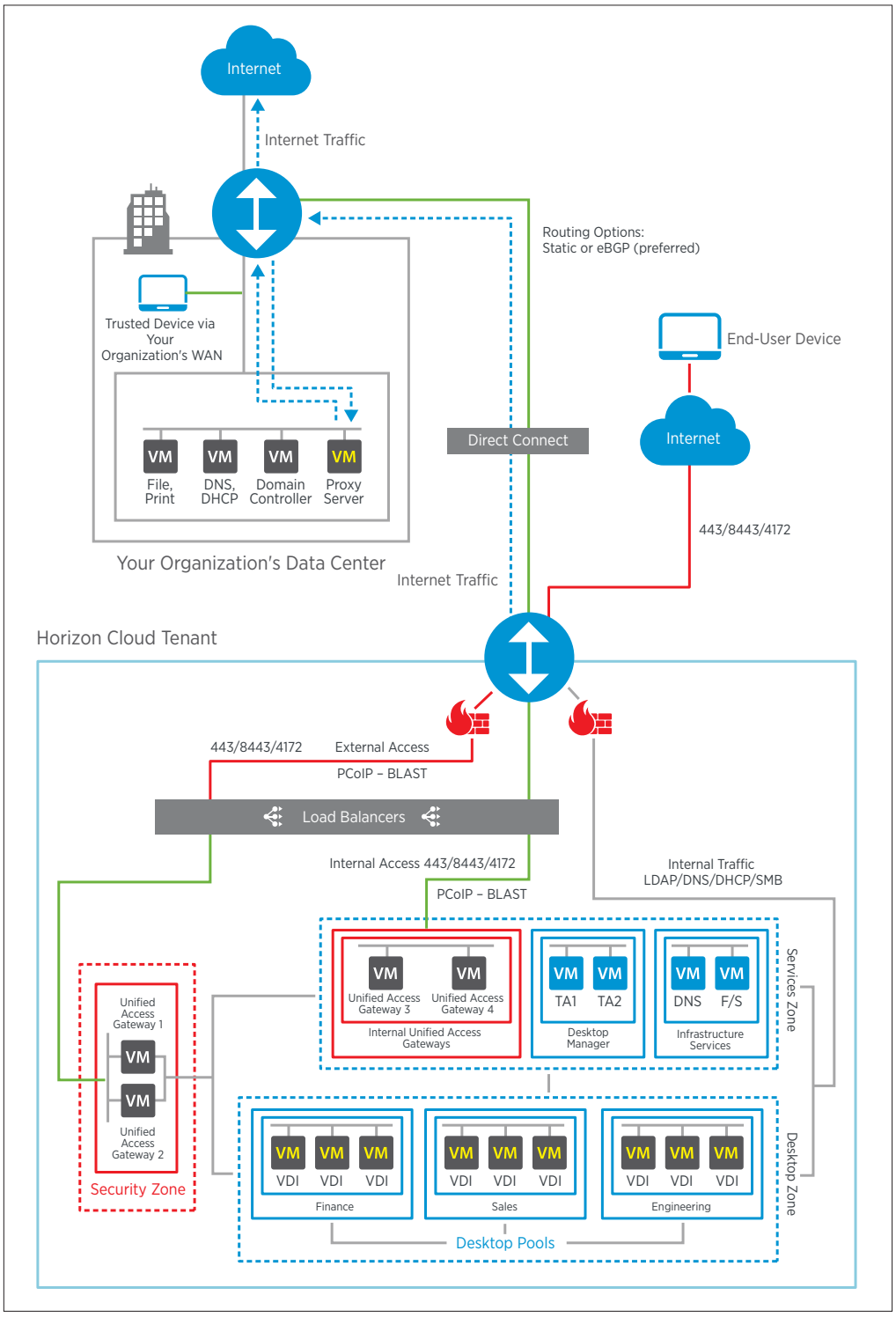

Figure 8: Connectivity Through Your Organization's Internet Gateway

Direct Connect Option 3: No Internet Connectivity Through Horizon Cloud Gateway

In this option, routing is configured so that all connectivity to Horizon Cloud desktops is through Direct Connect, and no Internet connection is through the Horizon Cloud gateway. This option provides the advantage of enabling full visibility and control over all protocol, user, and desktop activity to ensure the highest levels of security and regulatory compliance. This option is suitable when you require all users to connect to Horizon Cloud through your organization's network.

As shown in Figure 9, this option disables the Horizon Cloud gateway, making it technically impossible for users to connect externally to Horizon Cloud through the Internet. All traffic—protocol, in-guest, and Internet-bound desktop traffic—traverses Direct Connect through your company-owned Internet gateway. Users must be on your organization's network or connected remotely through your organization's VPN to connect to Horizon Cloud. End users who are connected through your organization's VPN require the ports in Figure 9 to be open across your organization's VPN. These ports are considered internal connections to Horizon Cloud.

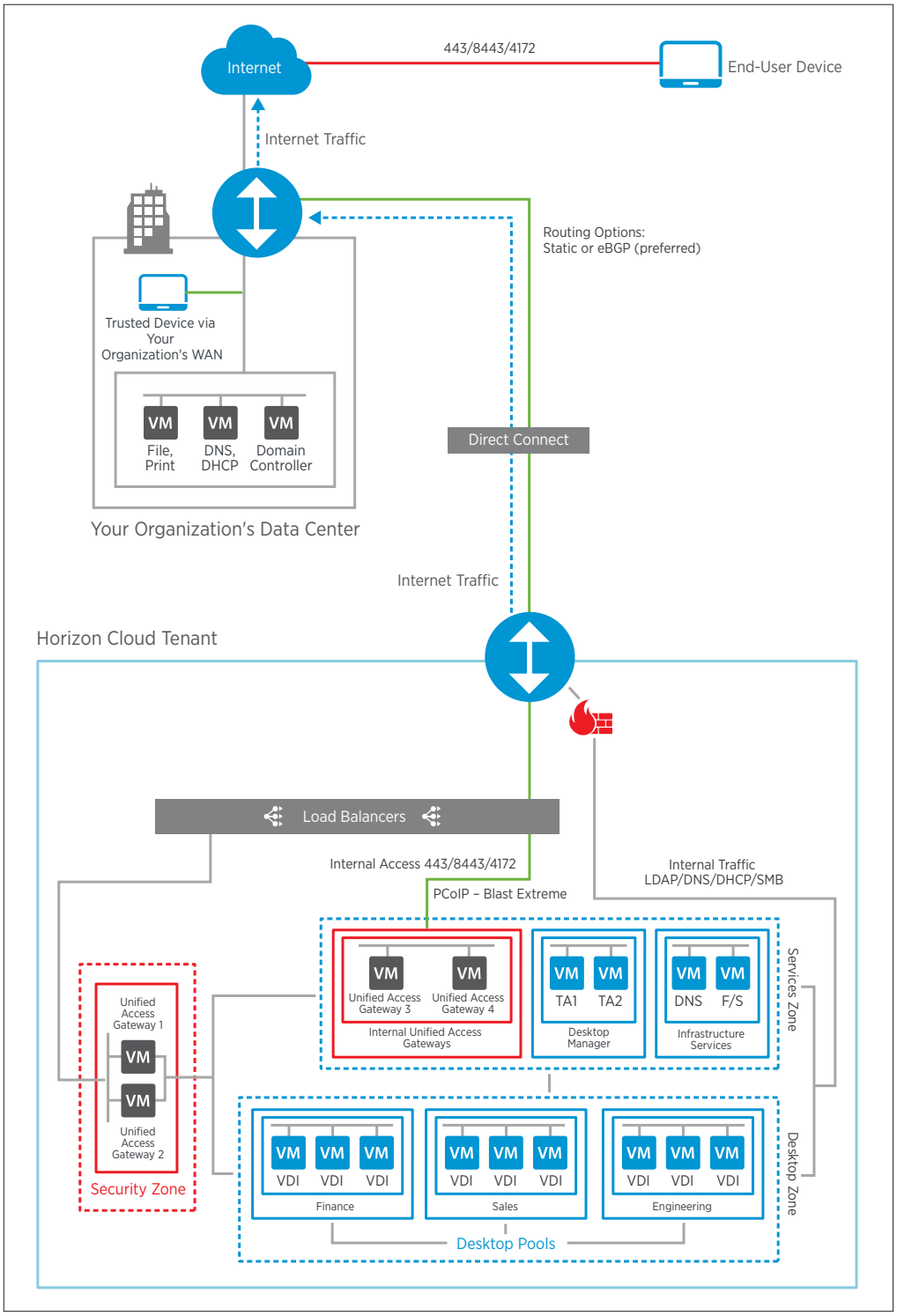

Figure 9: No Internet Connectivity Through Horizon Cloud

Direct Connect Setup

When setting up Direct Connect, work with your telecommunications provider to establish a connection to the Horizon Cloud data center and then connect to your Horizon Cloud tenant by establishing connectivity between the NSP router and your Edge Gateway. The Horizon Cloud team works with you to establish this connection. You must complete the VMware Direct Connect Collection form to establish connectivity. This form requests basic information, such as a network administrator contact, your telecommunications provider, connectivity type, and circuit ID.

When using Direct Connect, you must provide a network subnet with a minimum of two addresses (**/30**) to use between the carrier termination and Horizon Cloud and establish connectivity to your Edge Gateway.

You must also provide a Letter of Authorization – Customer Facility Request (LOA-CFA), which is usually from your telecommunications provider to VMware, to facilitate the connection of the Cross Connect or Network Exchange between the NSP router and the Horizon Cloud environment. The LOA-CFA usually provides the cabinet, patch panel, and a port number.

Horizon Cloud supports multiple Direct Connects, although load balancing the connections is not supported. To deploy redundant connections with direct connects and automatic failover requires implementing the appropriate network routing. For more information, see Network Routing.

Network Routing

Horizon Cloud supports both static routing and dynamic routing, allowing traffic to pass between Horizon Cloud and your internal network segments. Dynamic routing capabilities for Dedicated Connection, MPLS, or Network Exchange–based connections are offered using Border Gateway Protocol (BGP), a standardized exterior protocol for exchanging routing information between systems on the Internet. Dynamic routing via External BGP (eBGP)—a BGP extension used for communication between autonomous systems—allows routing changes to be automatically propagated to Horizon Cloud. When eBGP is used with the proper path attributes, such as local path manipulation using local preference or weight, and a remote path manipulation such as Multi-Exit-Discriminator (MED), you can select which redundant link is active. The protocol also ensures that automatic failover between multiple dedicated connections, MPLS, or Network Exchange connections is supported. You are responsible for assigning the BGP autonomous system number to the Horizon Cloud service router, which is usually a private number in the **65xxx** range. Static routing is available if you cannot support BGP routing.

Split DNS

Split DNS is the preferred method of accessing your Horizon Cloud environment when users are connecting from inside and outside your network. Split DNS enables users on your local network to connect through the internal network to a private IP address, and external users can connect to a public IP address while using the same URL. This method simplifies end-user access by not having to use two URLs, one for internal and the other for external.

When setting up split DNS, create a new host (A Record) that points to the virtual IP of the internal Unified Access Gateways in a specific DNS forward lookup zone on your internal DNS servers. The DNS forward lookup zone is based on your current DNS configuration. If you have the same internal DNS name as you do externally, you create the A Record in the forward lookup zone. If you do not have the same internal DNS name as you do externally, or if you are using the Horizon Cloud URL, you create a DNS stub zone with forward lookup that matches the external fully qualified domain name. Then create the A Record in the forward lookup zone.

Sample Tenant Network Architecture

Figure 10 shows two options for network connectivity to Horizon Cloud: an island tenant with no VPN connectivity, and a tenant with VPN connectivity connecting to your on-premises data center. Figure 10 also introduces the Horizon Cloud tenant appliances and Unified Access Gateway appliances, along with utility servers.

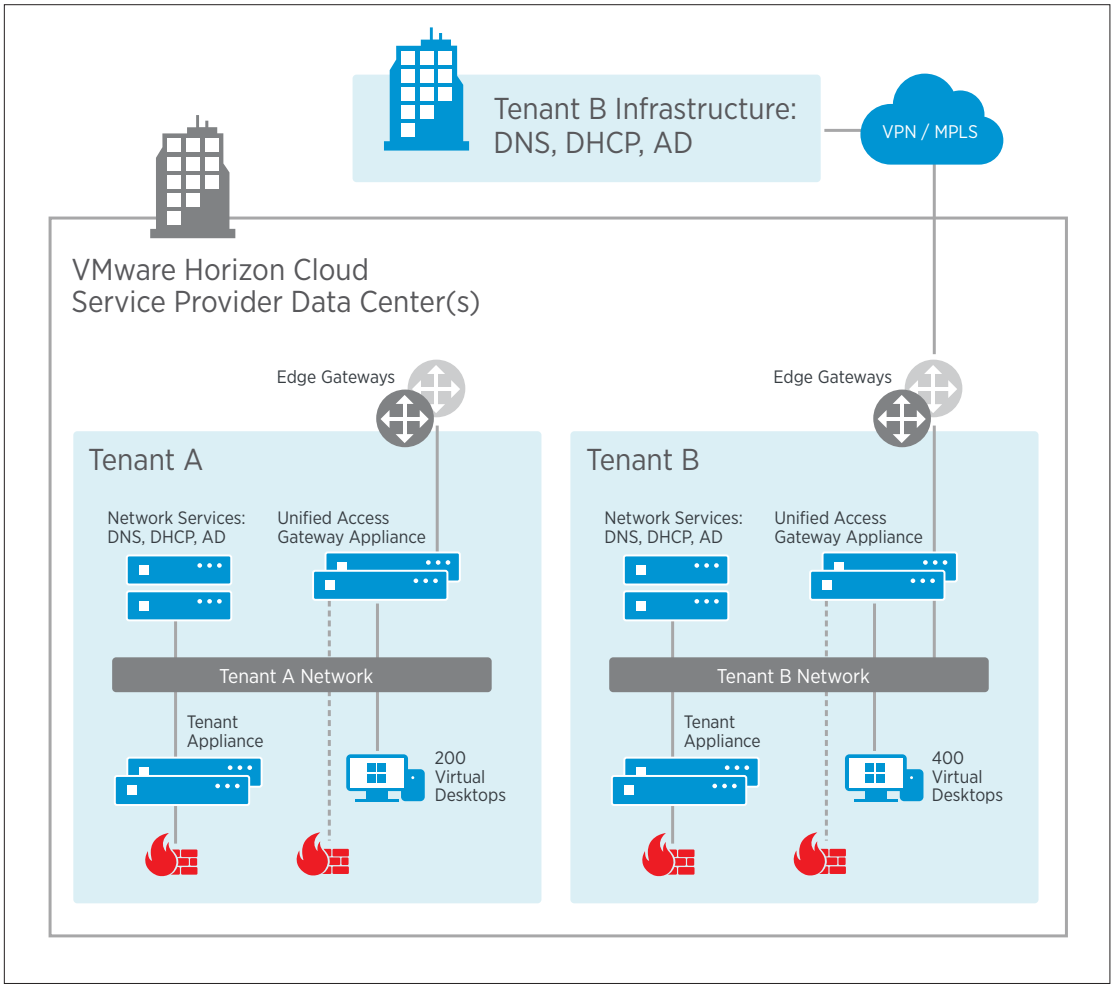

Figure 10: Example of Tenant Network Architecture

Understanding Zones

Horizon Cloud with Hosted Infrastructure establishes zones that segregate the different resources based on their function. Horizon Cloud has three zones. Each zone is unique to each Horizon Cloud deployment and is not shared.

- **Security Zone** – A demilitarized security zone (DMZ) where the external Unified Access Gateway appliances reside. It facilitates secure remote access to the Horizon Cloud tenant environment.
- **Services Zone** – Where Horizon Cloud services are hosted, including tenant appliances, utility servers, and internal Unified Access Gateway appliances
- **Desktop Zone** – Hosts the desktops and RDSH servers

Horizon Cloud Appliances

The tenant appliance contains your Horizon Cloud Administration Console, Horizon Cloud User Portal, account configuration database and desktop mappings, and domain join information. The Unified Access Gateway appliance allows secure access for both internal and external connections to Horizon Cloud virtual desktops and RDSH-hosted applications. For redundancy and high availability, two of each appliance are deployed.

- **Tenant appliance** – A hardened Linux appliance that provides desktop and application brokering, provisioning, and entitlement services. It hosts the end-user and administrative portals, which are part of the Services Zone, and communicates status information to the service provider.
- **Unified Access Gateway** – A hardened Linux appliance that provides secure remote access into the Horizon Cloud environment. It is part of the Security Zone (for external Horizon Cloud access) and the Services Zone (for internal Horizon Cloud access).
- **Utility servers** – By default, one utility server is provided for free and is optional unless noted in the service description. Utility servers can be Active Directory, DNS, DHCP, UEM, or file servers to collocate services in the Horizon Cloud tenant and are connected to your network (Services Zone).
- **Edge Gateway appliance** – A gateway that provides network edge security and gateway services to isolate security zones and virtualized networks along with NAT, DHCP, VPN, and a load balancer.

Network Security

Horizon Cloud uses an Edge Gateway appliance to manage the VPN and Direct Connect connectivity, as well as any management traffic, in and out of the Horizon Cloud tenant where the desktops, RDSH servers, and management appliances reside.

If you want additional buffering between the management appliances and your organization's network environment, consider deploying a corporate-managed firewall policy as long as all required ports are enabled for internal and remote users and any applications or services that those users require.

Understanding Unified Access Gateway

VMware Unified Access Gateway (formerly VMware Access Point) is a hardened Linux virtual appliance that allows secure remote access to the Horizon Cloud environment. If your users use an external connection through the public Internet—whether the traffic is web-based or protocol-based—the traffic is sent to the external Unified Access Gateway. Unified Access Gateway acts as a secure proxy for your connection into the Horizon Cloud environment. The external Unified Access Gateway proxies Horizon Cloud traffic to and from the Security Zone. The Security Zone is a DMZ networking security construct that gives a segment of your organization's network access to the outside but with strict rules regulating access to what is inside your network. For internal users connecting to the Horizon Cloud environment, traffic is sent to the internal Unified Access Gateway appliances located in the Services Zone.

Summary

This white paper describes the main network connectivity options available for a Horizon Cloud with Hosted Infrastructure deployment. It provides an overview of the decisions and responsibilities and the basic requirements for firewall and ports. Networking configuration options are described, and additional tips and best practices for networking are provided. With the information in this white paper, you are ready to obtain approval from your networking stakeholders and proceed with deployment of VMware Horizon Cloud with Hosted Infrastructure. For information about deployment considerations beyond networking, see VMware Horizon Cloud Service with Hosted Infrastructure Deployment Considerations.

Appendix A: Choosing Between Integrated or Isolated Active Directory

Although the Horizon Cloud platform relies on Active Directory, you are not required to integrate Horizon Cloud with your existing Active Directory environment. You can integrate your Active Directory into Horizon Cloud any time you choose. You have the option of using a separate, isolated Active Directory domain that is local to the Horizon Cloud desktops and applications. Choosing an isolated domain is advantageous for the following use cases:

- **Technology proof of concept** – For an organization to engage in a technology proof of concept without directly integrating your organization's infrastructure. In a pilot domain, you can set up everything required to test and validate your use cases within a fully sandboxed environment.
- **Organizations with outsourced users** – For a large organization that offloads development work to other countries and needs to provide employees with desktops without connecting directly into your organization's infrastructure. In a pilot domain, you can set up everything those employees need within a fully sandboxed environment.
- **Organizations with seasonal users** – For an organization that ramps up two or three times a year for a period of time without adding a large number of desktops in your organization's Active Directory structure. You can use a separate pilot domain when you need it and discard it when the season is over.
- **Organizations with limited resources** – For a smaller organization without much infrastructure, you can use a separate isolated domain to save the cost of building a primary directory services infrastructure.

  See license considerations in the Horizon Cloud Service Level Agreement when implementing an island account.

Appendix B: Subnet Considerations

Your Horizon Cloud tenant contains multiple zones. For the Services Zone and the Desktop Zone, you must assign the networks to use. If you are integrating with your existing environment, those networks cannot be in use.

The Services Zone hosts the Horizon Cloud services, including tenant appliances, utility servers, and internal Unified Access Gateway appliances. It is recommended that you use a subnet that provides approximately 30 IP addresses (/27), although you determine if that is the appropriate number based on your requirements. This subnet cannot overlap existing networks in your network infrastructure.

The Desktop Zone is where all your desktops and RDSH servers are located. You define and assign a network to support the total number of desktops and RDSH servers that you need. It is recommended that you maintain extra address capacity in the subnet for desktop refreshes and maintenance. The subnet cannot overlap what is already in use on your network infrastructure.

When using Direct Connect options, you must provide a network with a minimum of two addresses (/30) to use between the carrier termination and VMware. For more information, see Direct Connect. Also see *Connectivity Options* in the VMware Horizon Cloud with Hosted Infrastructure Deployment Considerations white paper.

Protocol, In-Guest, and Internet-Bound Traffic

Understanding traffic flows associated with Horizon Cloud is key when choosing the type of network to implement, and it is an important step before deploying Horizon Cloud. Consider the protocol traffic generated by Horizon Clients and network traffic generated by applications and other services on Horizon Cloud desktops and RDSH servers.

Note: At a minimum, site-to-site VPN, Dedicated Connection, MPLS, or Network Exchange is needed for Active Directory, DNS, DHCP, and NTP, except with island accounts. An island account has no connectivity to the tenant site, so all access into the system is from the public Internet. An island account is an implementation in which Horizon Cloud hosts basic Active Directory, DNS, DHCP, and NTP. When implementing an island account, see the license considerations in the Horizon Cloud Service Level Agreement Terms of Service Documents.

Protocol Traffic

Protocol traffic is the network traffic exchange between the virtual desktop and the endpoint using PCoIP, Blast Extreme, or Blast HTML5 access protocols. Screen images, keyboard and mouse movements, and USB and other device traffic travel between the endpoint and virtual desktop using the desired Horizon protocol. It is important to account for the protocol traffic to properly size your network connection to Horizon Cloud. Protocol traffic could be using the same network connection for other in-guest traffic, potentially impacting the end-user experience.

In-Guest Traffic

In-guest traffic is created when an application makes a network call to another application or IT service from within the virtual desktop or RDSH session. An example is when the browser launches from the desktop and reaches out to an internally hosted corporate website. In-guest traffic bound for internal IT resources is routed to the network connection back to the customer's data center or network. Proper planning for the network connection back to the customer data center is important. In addition to ensuring ample bandwidth, you can specify alternate routes and connections back to data center resources to separate the protocol traffic and in-guest traffic.

Internet-Bound Traffic

A key step in the process is choosing how Internet traffic is routed from Horizon Cloud desktops and applications. You can leverage the Internet connection provided by Horizon Cloud or route all Internet-bound traffic through your own organization's network. Determining how Internet-bound traffic is routed within the VMware data center depends on the routing option you choose for the default route (0.0.0.0/0).

DHCP

Ensure that the desktop subnet includes enough IP addresses to cover the number of desktops and RDSH servers that are provisioned, along with additional buffer for overlap. For example, if you provide the /24 in CIDR format for the subnet, you get exactly 252 addresses. Adding additional subnets up front allows for seamless capacity expansion when it is needed.

Appendix C: Choosing Horizon Cloud User Portal and Administration Console Portal URLs

Users and administrators access the desktops, RDSH servers, and management functions through secured web-based portals:

- **Horizon Cloud User Portal** – A web-based portal offering end users clientless access to Horizon Cloud desktops and applications using HTML5
- **Horizon Cloud Administration Console** – The web-based portal used by IT administrators to provision and manage Horizon Cloud desktops and applications, resource entitlements, and images

Both portals use the same URL, followed with `/horizonadmin`, such as:

- **Horizon Cloud User Portal** – `https://desktop.virtualdesktopaccess.com`
- **Horizon Cloud Administration Console** – `https://desktop.virtualdesktopaccess.com/horizonadmin`

You can define the naming convention used for these portals.

Portal URL Option 1

This option is the most common for pilots because of its simplicity and ease of use. The DNS domain is owned and provided by VMware. You can also set up split DNS for internal access.

- `https://companyname.horizon.vmware.com`
- Uses the VMware `*.horizon.vmwware.com` certificate

Portal URL Option 2

Option 2 includes two choices. It requires the owner of `virtualdesktopaccess.com` to provide an SSL certificate in an Apache2 format and to set up internal and public (if required) DNS records using split DNS.

- `https://desktop.virtualdesktopaccess.com`
- `https://www.virtualdesktopaccess.com`

Choice 1: If you have a site-to-site VPN or Direct Connect, you can choose whether to make the Horizon Cloud Administration Console accessible from the public Internet.

Choice 2: If you have an island tenant without a site-to-site VPN or Direct Connect, the Horizon Cloud User and Administration portals must be accessible from the public Internet via the Unified Access Gateway.

Additional Resources

You can find out more about Horizon Cloud from the following resources:

- SysTrack Desktop Assessment, Part 1: Moving to VDI? Details You Should Know (VMware blog post)
- Technical Introduction to VMware Access Point for Secure Remote Access (VMware blog post)
- Virtual private network (VPN)
- Active Directory and Active Directory Domain Services Port Requirements
- Equinix Cloud Exchange
- Service Description: VMware Horizon Cloud Service with Hosted Infrastructure
- Setting Up Desktop and Application Pools in View – VMware Horizon 7.0
- VMware Horizon Cloud Service with Hosted Infrastructure Terms of Service
- VMware Horizon Air / Horizon Cloud Support Center
- VMware Horizon Cloud – Enterprise Mobility Management – AirWatch
- VMware Horizon Cloud On-Premises Infrastructure
- VMware Horizon Cloud Service with Hosted Infrastructure Deployment Considerations
- VMware Horizon Cloud with Hosted Infrastructure
- VMware Horizon Cloud with On-Premises Infrastructure – Supported Hardware
- VMware NSX 6 Administration Guide
- VMware Unified Access Gateway

About the Authors

This white paper was written by

- Rick Terlep, End-User-Computing Architect, End-User-Computing Technical Marketing, VMware
- Jerrid Cunniff, End-User-Computing Cloud Services Senior Solutions Engineer, VMware
- Daniel Berkowitz, End-User-Computing Cloud Services Senior Solutions Engineer, VMware
- Justin Venezia, End-User-Computing Cloud Services Senior Architect, VMware
- Cindy Heyer Carroll, End-User-Computing Technical Marketing Technical Writer, VMware

Feedback

The purpose of this white paper is to assist you. Your feedback is valuable.
To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.

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