VMware vCloud® Architecture Toolkit™
for Service Providers

Customer Onboarding with VMware NSX® L2VPN Service for VMware Cloud Providers™

Version 2.9

January 2018

Harold Simon

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Tables

List of Figures

Introduction

1.1 Overview

The VMware Cloud Provider™ Program is an ecosystem of over 4,000 service providers located in more than 100 countries offering VMware based cloud services. Local providers secure data sovereignty while providing a wide range of cloud services and vertical market expertise through specialized compliance and certifications.

VMware Cloud Providers are uniquely positioned to offer their services to the market and become a seamless extension of existing VMware enterprise customers' on-premises data centers. Having the capability to move workloads in and out of the customer's chosen cloud platform is a key factor for most enterprise customers to help them maintain their existing investments within their on-premises applications, and avoid lock-in to any one vendor or provider.

One of the initial concerns about moving to a hybrid cloud solution is determining the methods that will be used for onboarding into a service provider infrastructure. In many cases, customers have the requirement to migrate systems with changing IP addresses or to be able to deploy new workloads to a service provider's infrastructure while maintaining Layer 2 connectivity with existing on-premises workloads.

1.2 Document Purpose and Scope

This document examines some of the key prerequisites and scenarios in which VMware Cloud Providers can leverage the VMware NSX® L2VPN service to streamline the process for customers who are onboarding to a VMware Cloud Provider Program hybrid cloud solution. Where applicable, VMware Cloud Provider Program partners can enhance the customer onboarding process by offering hybrid network connectivity, seamless migration, and workload mobility services that help customers adopt the hosted cloud platform with less risk and impact to their running applications, and without the need for changing IP addresses after relocating to the VMware Cloud Provider Program hosted environment. This solution can also be leveraged for migrations where only a portion of the workloads are being migrated, but still need Layer 2 access to other systems that remain on the customer premise.

1.3 Definitions, Acronyms, and Abbreviations

L2VPN: Layer 2 Virtual Private Network is a means of stretching logical networks across geographical locations or sites. The connection is secured through SSL encryption.

WAN: A Wide Area Network is a telecommunications network that spans a large geographical area.

VXLAN: Virtual Extensible LAN is an encapsulation protocol for extending Layer 2 networks over Layer 3 networks.

Trunk Port: An interface on the VMware NSX Edge™ device or standalone NSX Edge appliance that is configured to carry all VLAN/VXLAN traffic.

PSC: The VMware Platform Services Controller™ (PSC) refers to the core group of infrastructure services that are essential to the operations of VMware vCenter®. This group of services include VMware vCenter Single Sign-On™, license service, lookup service, and VMware Certificate Authority. For full details of PSC deployment models and configurations, see the VMware vSphere Installation and Setup documentation.

vCenter Single Sign-On: The service that facilitates secure authentication services to VMware vCenter Server® and other software components that make up the VMware vSphere® infrastructure.

Customer Onboarding Overview

This section describes some of the concepts and criteria that are instrumental in planning for onboarding activities. While variations of the solution can be leveraged with VMware Cloud Provider Program public cloud offerings, the focus of this document is on the implementation of VMware NSX L2VPN for migration to VMware Cloud Providers offering the vSphere Hosting solution.

2.1 Key Onboarding Factors

2.1.1 VMware Cloud Provider Infrastructure

The infrastructure recommended for leveraging VMware NSX L2VPN servers for migrations follows the guidelines detailed for the vSphere Hosting service. The VMware Cloud Provider will offer a managed or unmanaged instance of vSphere with VMware NSX, as well as additional product integrations for monitoring and metering of the environment.

2.1.2 Customer On-Premises Infrastructure

So that VMware NSX L2VPN services provide the greatest benefit, the customer will ideally have an existing implementation of vSphere and VMware NSX for spanning VXLAN-VXLAN and VXLAN-VLAN. If the customer has not yet implemented VMware NSX in their environment, the standalone NSX Edge appliance can be deployed in the customer’s environment for the stretching of on-premises VLANs to the hosted service provider.

2.1.3 Hybrid Network Connectivity

The VMware Cloud Provider must implement the necessary hybrid network connectivity between the customer’s on-premises data center and the VMware Cloud Provider hosted data center.

The network connectivity for VMware NSX L2VPN services can be facilitated by a dedicated connected network, such as an MPLS circuit or a leased-line connection, or across the Internet where VPN services from VMware NSX can be used to provide a software approach to connecting hybrid cloud data centers.

See the Architecting a VMware NSX Solution for the VMware Cloud Provider Program document provided with the *VMware vCloud Architecture Toolkit™ for Service Providers (vCAT-SP)* for more information about network connectivity.

2.1.4 Tenancy

This document focuses on leveraging VMware NSX L2VPN services in a VMware Cloud Provider Program Hosting solution as described in the introduction to the vCAT-SP located in the vCAT-SP Documentation Center. The VMware Cloud Provider Program hosted solution is designed to be deployed per tenant. Therefore, the focus of this document is on implementation of VMware NSX L2VPN from a single-tenant perspective.

2.1.5 Users and Roles

L2VPN services are used for onboarding for both managed and unmanaged implementations. With regard to determining who will manage the onboarding activities, the VMware Cloud Provider can manage migrations on the customer’s behalf or allow the customer to perform the migrations in a self-service scenario. In either case, it is important to verify that the personnel have the appropriate level of access to the VMware Cloud Provider Program hosted environment and the on-premises virtual environments to successfully perform the end-to-end task of migrating VMs to the VMware Cloud Provider Program hosted solution. Some details regarding onboarding options are outlined in Section 6, VMware NSX L2VPN Onboarding Scenarios.

2.1.5.1 Service Provider

The service provider will offer the necessary compute, storage, and networking required for the VMware Cloud Provider Program hosted solution. Depending on the customer requirements, the service provider can manage the solution, which includes but is not limited to migration of workloads, or can provide an unmanaged service to the environment for customers who prefer the direct management of workloads in the hosted solution.

2.1.5.2 Customer/Tenant

The customer or tenant will provide the compute, storage, and networking required for the on-premises vSphere infrastructure from which workloads will be migrating.

2.1.5.3 Workload Mobility and Migration Services

The service provider will offer a managed or self-service workload mobility service to their end customers where they facilitate the hybrid network connectivity and VMware Cloud Provider Program virtual infrastructure and processes for workload mobility and migration to streamline customer onboarding.

Conceptual Architecture

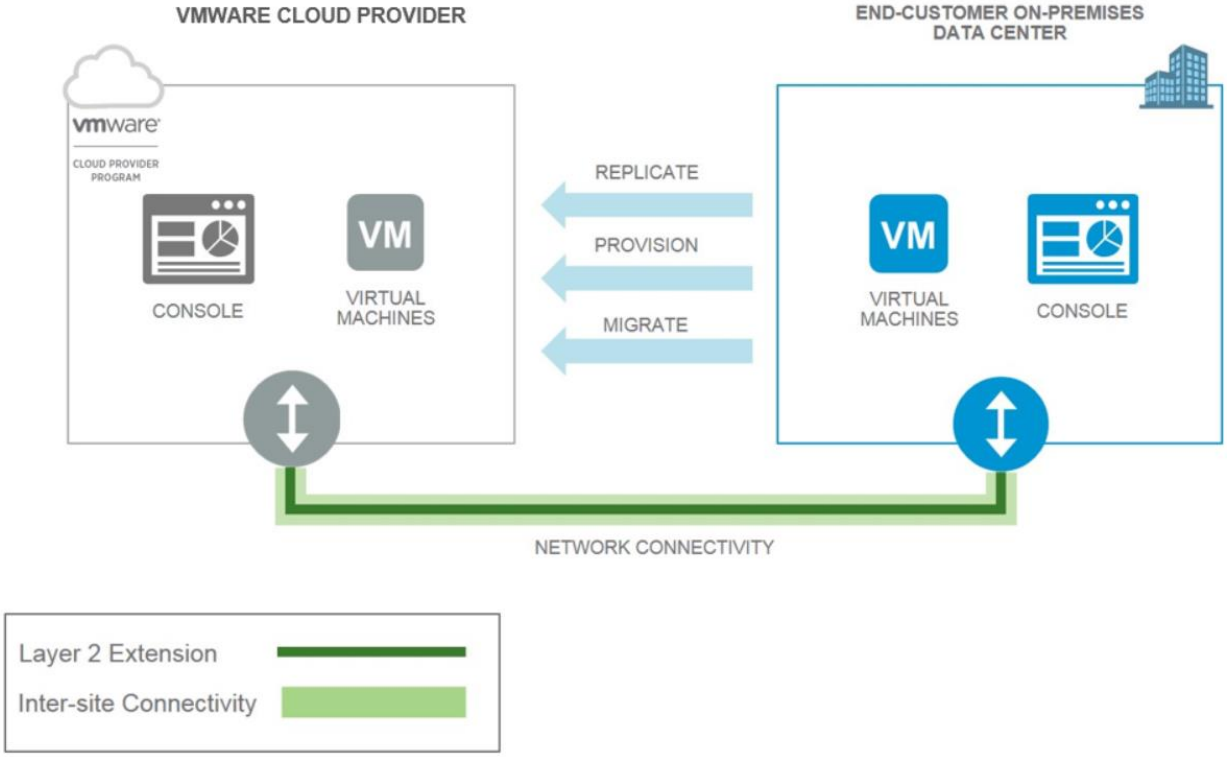
3.1 Business Drivers

The key business drivers for implementing this solution are to provide a simplified approach and enhanced customer onboarding (self-service or managed) between an on-premises data center and a VMware Cloud Provider while reducing the requirements for the procurement and configuration of external networking hardware. With this solution, a VMware Cloud Provider can implement stretched Layer 2 network services for their customers with low risk, speed, and agility.

3.2 Conceptual Architecture Solution Overview

The following figure highlights the conceptual architecture in which the VMware Cloud Provider offers additional services, such as replication, hybrid provisioning, workload mobility, and migration services. This architecture focuses on workload mobility and migration services.

Figure 1. Conceptual Diagram



Designing for VMware NSX L2VPN Service

4.1 VMware NSX L2VPN Deployment Models

With VMware NSX L2VPN services, there are two main deployment models that the service provider must consider when offering these services to the market:

- Stretched L2VPN with VMware NSX on and off premises
- Stretched L2VPN with standalone NSX Edge on premises

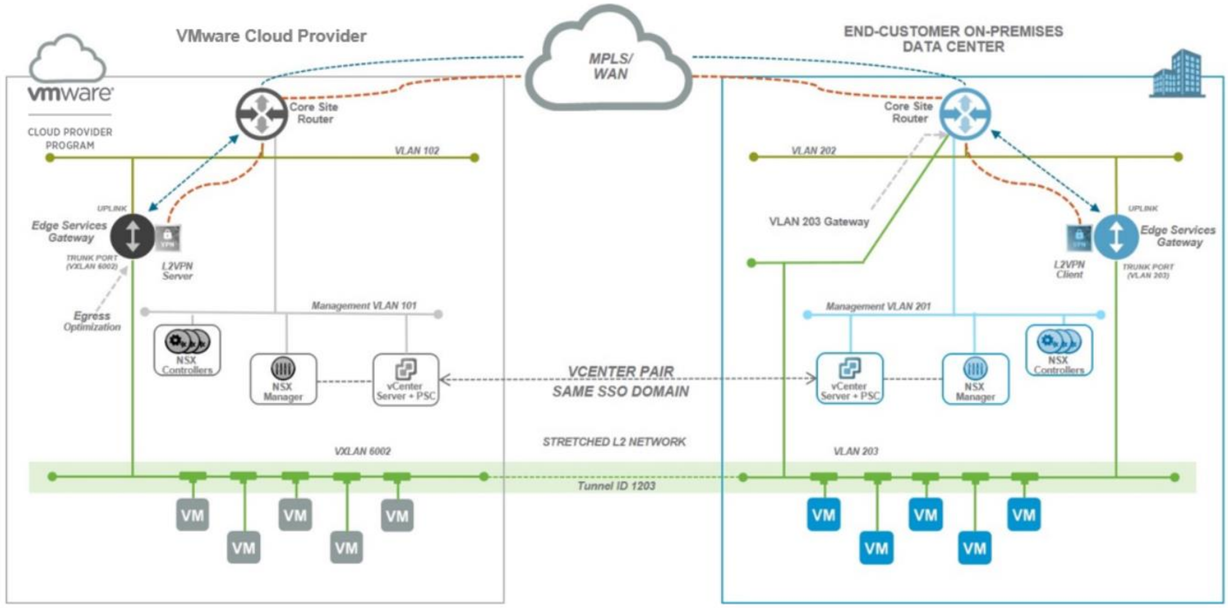
The following section provides an architecture example of both solutions.

4.1.1 Stretched L2VPN with VMware NSX On Premises

In this scenario, VMware NSX L2VPN services are configured with VMware NSX deployed both in the VMware Cloud Provider environment and in the on-premises vSphere implementation at the customer's data center. This scenario provides increased flexibility, because the VMware NSX L2VPN service can extend VXLAN to VXLAN, VLAN to VLAN, and VXLAN to VLAN networks between sites.

In the following figure, VMware NSX is implemented on both sides of the hybrid cloud solution with separate, non-connected instances of VMware NSX. However, for implementations that require simplified management of long-distance VMware vSphere vMotion® migrations from the on-premises site to the VMware Cloud Provider site, the vCenter Server and Platform Services Controller (PSC) instances are joined to the vCenter Single Sign-On domain.

Figure 2. VMware NSX to VMware NSX Stretched L2VPN

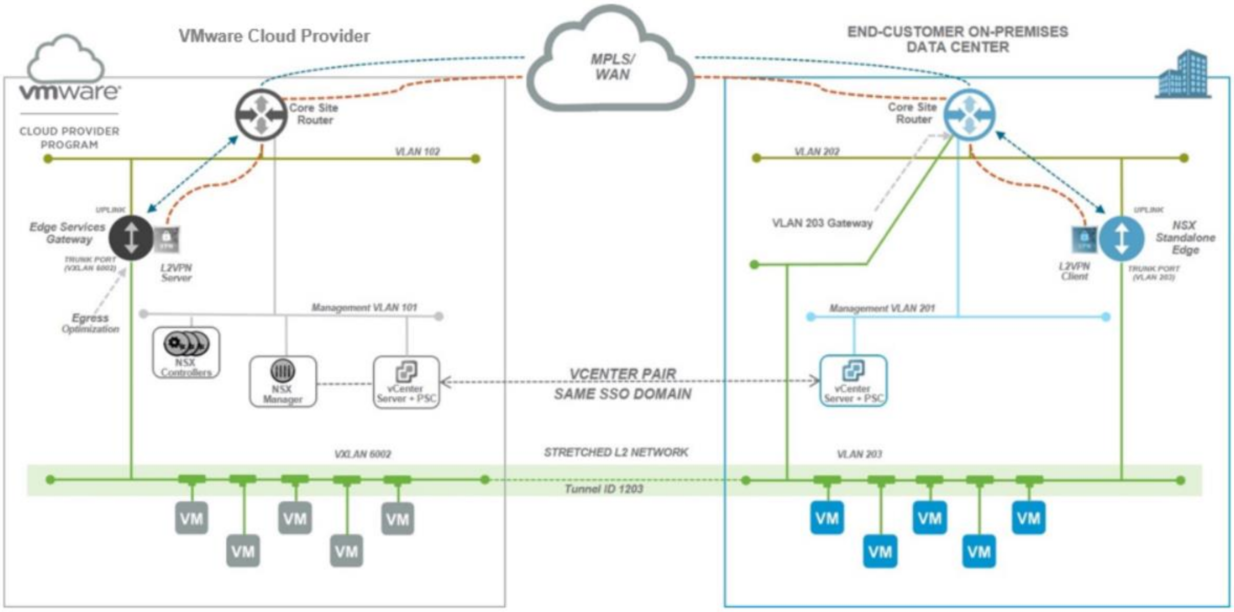


In the illustration, the VMware Cloud Provider (on the left) has an NSX Edge gateway appliance configured as the L2VPN server and the customer (on the right) has an NSX Edge gateway appliance configured as the L2VPN client.

4.1.2 Stretched L2VPN with Standalone NSX Edge

While the VMware NSX to VMware NSX configuration offers more options, it is still possible to extend Layer 2 networks for prospective VMware Cloud Provider Program customers who have not yet implemented VMware NSX in their on-premises infrastructure. You can enable this by deploying the standalone NSX Edge appliance in the customer's data center. With the standalone NSX Edge, VMware Cloud Providers can help customers extend on-premises VLANs to VXLAN-backed networks in the VMware Cloud Provider's hosting environment.

Figure 3. VMware NSX to Non VMware NSX Stretched L2VPN



In this illustration, the VMware Cloud Provide (on the left) has an NSX Edge gateway appliance configured as the L2VPN server and the customer (on the right) has an NSX Edge gateway appliance configured as the L2VPN client.

This document focuses on the option with no VMware NSX on premises because VMware NSX is a relatively new product for enterprise customers.

4.2 Architecture Prerequisites

This section describes the software and networking requirements for successfully implementing stretched Layer 2 VPN with VMware NSX.

4.2.1 VMware Software Product Requirements

Required product versions detailed for this document are as follows:

- VMware vSphere 6.x
- VMware vCenter Server 6.x
- VMware NSX 6.2 (required for the VMware Cloud Provider)
- Standalone NSX Edge appliance (no VMware NSX on premises)

Note The use of VMware vSphere Distributed Switch™ instances requires Enterprise Plus licensing.

4.2.2 Networking Requirements

To facilitate the communication between vCenter Server instances and hosts from VMware Cloud Provider Program to the on-premises network, the VMware Cloud Provider and customer must determine the means by which communication will be realized.

Where applicable, VMware recommends that WAN connectivity be implemented between the customer and VMware Cloud Provider. This enables more flexibility with onboarding options that require direct connectivity for hosts between sites (for example, long-distance vSphere vMotion migration and VMware vSphere Replication™).

For situations in which WAN connectivity cannot be established, the use of public IP addresses at each site is required with NAT services configured for the NSX Edge and standalone NSX Edge.

All networking components must be designed to meet the proper bandwidth and latency requirements for any planned site-to-site and intra-data center network traffic.

Management Components and Feature Design

5.1 vSphere Component Design

To provide L2VPN services through VMware NSX between a VMware Cloud Provider and the on-premises infrastructure of the customer, vSphere must be implemented in both locations. This section reviews some of the key vSphere components and recommended configurations for a successful deployment.

5.1.1 vCenter Server

vCenter Server is a key component of the solution that provides centralized management of VMs in both VMware Cloud Provider and customer locations. Additionally, it is a required component for the use of VMware NSX with vSphere based deployments. While it is possible to have completely separate deployments of vCenter Server with individual PSC and single sign-on (SSO) domains, deploying both vCenter Server instances within the same SSO domain reduces some of the management tasks within the implementation. First, there is the benefit of having a shared view of both vCenter Server instances provided that the user has the required privileges for both. Additional benefits of this configuration are discussed in Section 6, VMware NSX L2VPN Onboarding Scenarios.

With the service provider model, it is common for the end customer to have their own PSC/SSO domains. Where this is the case, the long-distance vSphere vMotion operations must be performed through the API and not through the UI with the federated view of the vCenter Server instances.

5.1.2 vSphere Cluster Design

VMware recommends that clusters within the VMware Cloud Provider environment conform to the guidance established in the Architecting a VMware vSphere Compute Platform for the VMware Cloud Platform Program document. For additional NSX Edge cluster recommendations, see the Architecting a VMware NSX Solution for the VMware Cloud Provider Program document.

5.1.3 Virtual Switches

Virtual switches provide L2VPN connectivity for VMs and NSX Edge appliances. For most VMware NSX L2VPN solutions, the vSphere Distributed Switch is used. However, it is possible to use the standard virtual switch for the configuration of the trunks ports that are used by the NSX Edge appliance. VMware recommends that the vSphere Distributed Switch be used for trunk port configurations because there is less management overhead during configuration of the L2VPN services at both sites. See Section 5.3.4, Trunk Port for more details about the use of trunk ports with VMware NSX L2VPN services.

5.2 VMware NSX Component Design

This section discusses the key components, features, and design considerations that are instrumental to the successful implementation of VMware NSX L2VPN services. For more details on these components and steps to configure VMware NSX L2VPN services, see the VMware NSX 6.2 Administration Guide.

5.2.1 NSX Edge

For this use case, the VMware Cloud Provider NSX Edge appliance acts as the L2VPN server and on the customer side, the standalone NSX Edge appliance acts as the client. For implementations in which the migrated workloads require Internet access, enable egress optimization on the NSX Edge fulfilling the L2VPN server role. This supports the local routing of migrated systems as opposed to sending data across the VPN tunnel. This allows, for example, workloads on the VMware Cloud Provider Program side of the VPN to access the Internet locally.

5.2.2 NSX Edge Considerations

For increased availability, VMware recommends deploying the NSX Edge in a high availability (HA) configuration. In this configuration, the two NSX Edge appliances must be placed on different datastores for increased redundancy. The primary appliance will be active and host all NSX Edge services, while the secondary appliance will be in standby mode. A heartbeat is maintained between the appliances over an internal interface. For a complete description of the failover process for NSX Edge appliances deployed in HA mode, see the VMware NSX 6.2 Administration Guide.

5.2.3 Standalone NSX Edge Appliance

The standalone NSX Edge appliance is a virtual appliance that can be implemented with VMware Cloud Provider Program customers that have not yet adopted VMware NSX in their on-premises data center. There is no additional charge or licensing for the standalone NSX Edge. The standalone NSX Edge appliance is configured during deployment, and is deployed after the configuration of the L2VPN service because it depends on details used during the configuration of the L2VPN server on the NSX Edge at the VMware Cloud Provider’s site.

5.2.4 VMware NSX Logical Switch

When configuring the VMware NSX L2VPN service, logical switches will be leveraged for VM connectivity. Logical switches used for Layer 2 network extensions communicate directly with the L2VPN server through the trunk port interface on the NSX Edge hosting the L2VPN server service. If VXLANs are stretched from the L2VPN client, the logical switches will have a similar configuration and might be connected to a distributed logical router (DLR) for local routing in the on-premises site.

5.2.5 Transport Zones

Verify that transport zones are configured for the appropriate clusters in the VMware Cloud Provider environment so that the required VXLANs / logical switches are present on the desired destination clusters.

5.3 VMware NSX L2VPN Service Components

5.3.1 L2VPN Server

The L2VPN server will be configured on the NSX Edge appliance hosted on the VMware Cloud Provider side of the solution. The L2VPN server contains the important details regarding the configuration of networks that are being extended. Configuration of the L2VPN server is typically facilitated by the VMware Cloud Provider but might require customer input for configuration details.

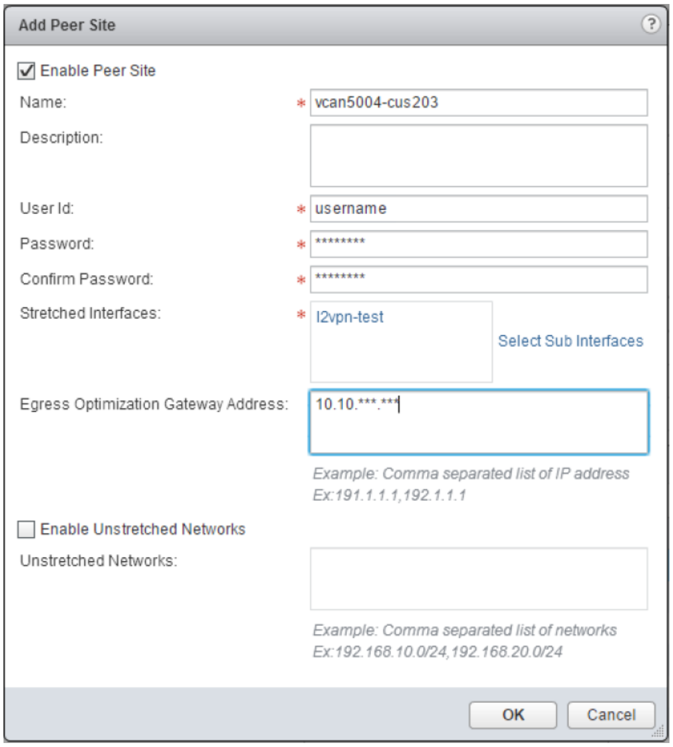
5.3.2 L2VPN Server Global Configuration

This section of the configuration contains details such as the external interface IP address, port number, and encryption algorithm that will be used for L2VPN client connections.

5.3.2.1 L2VPN Server Site Configuration

This section of the L2VPN server configuration page contains details, such as the connection name, user ID and password, the sub-interface that will be extended, egress optimization IP addresses, and specification of non-stretched networks.

Figure 4. L2VPN Server Site Configuration



☑ Enable Peer Site

Name: * vcan5004-cus203

Description:

User Id: * username

Password: * ********

Confirm Password: * ********

Stretched Interfaces: * l2vpn-test

Egress Optimization Gateway Address: 10.10.***.***

Example: Comma separated list of IP address
Ex:191.1.1.1,192.1.1.1

☐ Enable Unstretched Networks

Unstretched Networks:

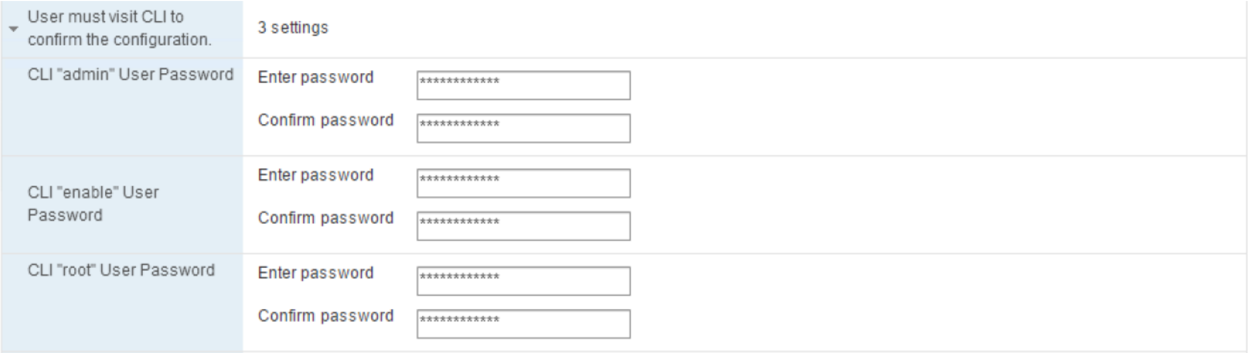
Example: Comma separated list of networks
Ex:192.168.10.0/24,192.168.20.0/24

5.3.3 L2VPN Client

The L2VPN client will be configured on the NSX Edge or standalone NSX Edge that is deployed on the remote (customer) side of the solution. After the L2VPN service is configured on the VMware Cloud Provider Program side, the provider will inform the customer of the details that will be required for the successful pairing of the L2VPN client with the L2VPN server.

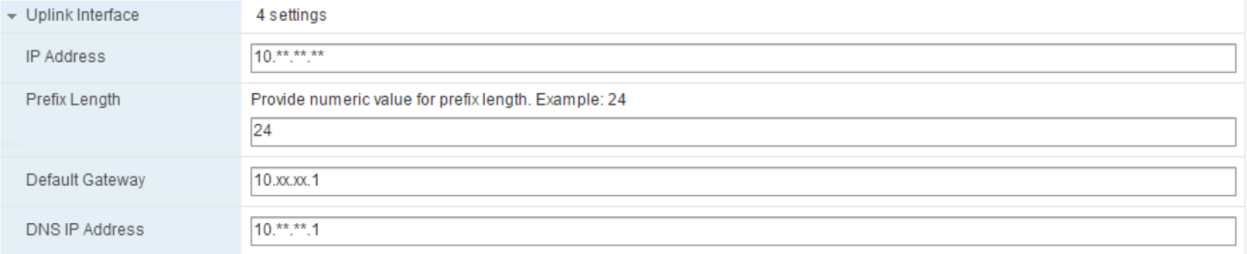
Note The configuration details of the standalone NSX Edge are entered during the deployment of the standalone NSX Edge appliance OVF file in vCenter Server. See the following figures for views related to the standalone NSX Edge L2VPN client menu.

Figure 5. Standalone Edge Credentials



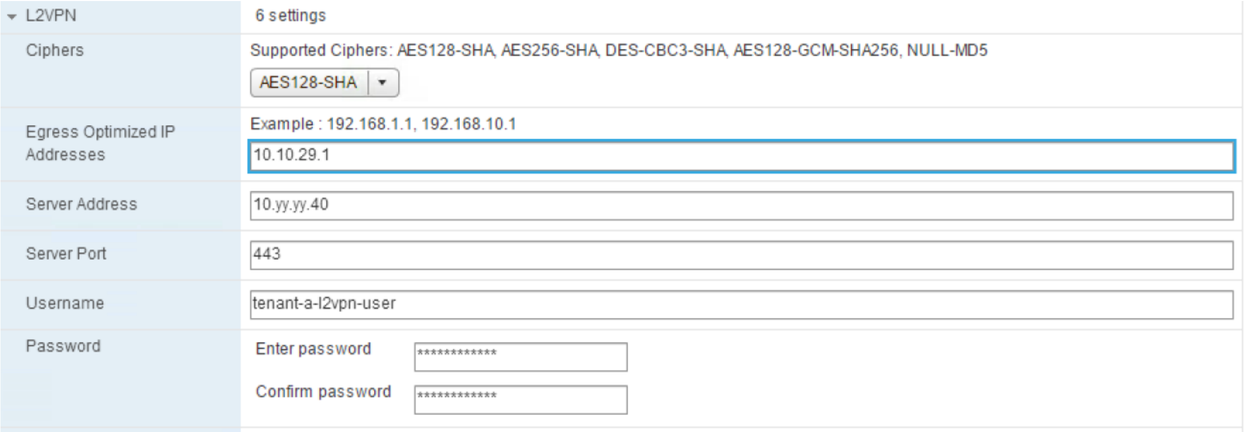
User must visit CLI to confirm the configuration.	3 settings	
CLI "admin" User Password	Enter password	************
	Confirm password	************
CLI "enable" User Password	Enter password	************
	Confirm password	************
CLI "root" User Password	Enter password	************
	Confirm password	************

Figure 6. Standalone Edge Uplink Interface



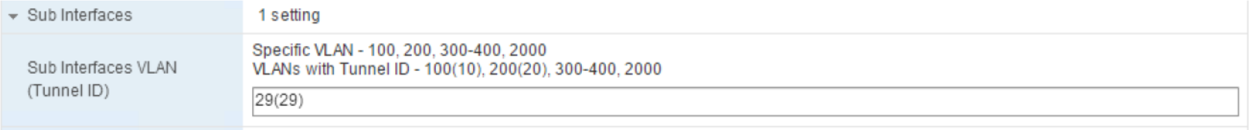
▾ Uplink Interface	4 settings
IP Address	10.**.**.**
Prefix Length	Provide numeric value for prefix length. Example: 24 24
Default Gateway	10.xx.xx.1
DNS IP Address	10.**.**.1

Figure 7. Standalone Edge L2VPN Configuration



▾ L2VPN	6 settings
Ciphers	Supported Ciphers: AES128-SHA, AES256-SHA, DES-CBC3-SHA, AES128-GCM-SHA256, NULL-MD5 AES128-SHA ▾
Egress Optimized IP Addresses	Example : 192.168.1.1, 192.168.10.1 10.10.29.1
Server Address	10.yy.yy.40
Server Port	443
Username	tenant-a-l2vpn-user
Password	Enter password ************ Confirm password ************

Figure 8. Standalone Edge Sub-Interface Configuration



▾ Sub Interfaces	1 setting
Sub Interfaces VLAN (Tunnel ID)	Specific VLAN - 100, 200, 300-400, 2000 VLANs with Tunnel ID - 100(10), 200(20), 300-400, 2000 29(29)

5.3.4 Trunk Port

Both the NSX Edge and the standalone NSX Edge appliance require the configuration of a trunk port interface. This interface is used to connect the NSX Edge appliances to the local VLANs or VXLANs that will be stretched between the on-premises data center and the VMware Cloud Provider. Some of the design considerations to consider with the trunk port configuration on the NSX Edge are as follows:

- Port group security – The port group configured for trunk port usage requires one of the following configurations:
    - VLAN setting of VLAN trunk, with the specified VLANs configured
    - Promiscuous mode and forged transmits

Note When configuring the NSX Edge appliance, port group security settings are configured automatically by VMware NSX.

Considerations when configuring the trunk port configuration for the standalone NSX Edge appliance are as follows:

- Port group security – The port group configured for trunk port usage requires one of the following configurations:
    - VLAN setting of VLAN trunk, with the specified VLANs configured
    - Sink port configuration (recommended) or promiscuous mode enabled
    - Forged transmits

For full details on the configuration of trunk ports for VMware NSX L2VPN services, see the VMware NSX Administration Guide. Also, see the Layer 2 VPN to the Cloud blog post for additional configuration details for the VMware NSX L2VPN service.

5.3.5 Tunnel ID

The Tunnel ID is a construct that is used to map/associate the networks between sites. In Figure 2 and Figure 3, the Tunnel ID 1203 maps the VXLAN 6002 on the L2VPN server side (VMware Cloud Provider) of the VPN tunnel to VLAN 203 on the L2VPN client side (customer) of the VPN tunnel.

5.3.6 Egress Optimization

For implementations that require workloads on the extended segment located within the VMware Cloud Provider to access the Internet, egress optimization can be enabled on the NSX Edge appliances with an egress optimization IP address. Typically, this is the same IP address as the default gateway that is used for the on-premises network being extended to the VMware Cloud Provider. Enabling this feature allows Internet bound traffic on the provider side of the connection to exit (egress) through the local egress optimization gateway instead of sending the traffic back over the extended network link to the Internet and then back across the extended link.

The egress optimization feature is intended to be used to allow extended workloads to access the Internet or other networks within the VMware Cloud Provider's environment.

5.3.7 VMware NSX L2VPN Service Threshold Recommendations

This section provides configuration threshold recommendations to consider when using the VMware NSX L2VPN service. These are guidelines to provide optimal user experience and reliability of the underlying service.

Table 1. VMware NSX L2VPN Server Threshold Recommendations

Description	Recommend Threshold
Number of L2VPN clients per L2VPN server	5
Number of networks per L2VPN server and L2VPN client pair	200

VMware NSX L2VPN Onboarding Scenarios

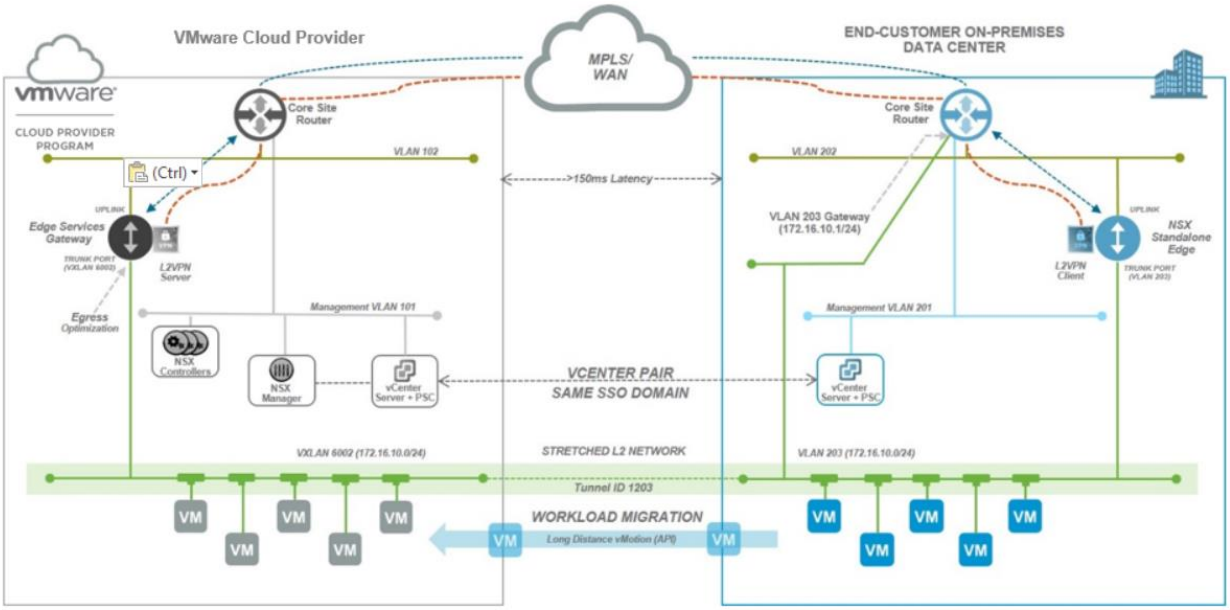
Customer onboarding can encompass several scenarios. Some common onboarding scenarios include the following:

- Migration of live workloads
- Offline data transfer of workloads
- Provisioning of new workloads

This section describes some of the scenarios in which the VMware NSX L2VPN service can be leveraged as a means for onboarding customer workloads to a VMware Cloud Provider.

Long-distance vSphere vMotion migration is an attractive feature to leverage when considering VMware NSX L2VPN services, enabling the live migration of a VM between vCenter Server instances. With one vCenter Server node deployed in each site joined to the same SSO domain, consumers are able to perform vSphere vMotion migration tasks between vCenter Server instances through the VMware vSphere Web Client. Having both vCenter Server instances joined to the same SSO domain is not a requirement, but is recommended for easier management of hybrid cloud environments.

Figure 9. L2VPN with Long-Distance vSphere vMotion Migration



It is important to remember that for successful vSphere vMotion operations to occur, the VMware Cloud Provider Program and on-premises VMware ESXi™ hosts must be able to communicate between sites on the vSphere vMotion VMkernel port. If you are using a dedicated vSphere vMotion IP network, verify that hosts have the vSphere vMotion TCP/IP stack associated with the appropriate vSphere vMotion VMkernel ports. Because vSphere vMotion traffic is unencrypted, you might also consider configuring the appropriate access list and other internal network security standards so that vSphere vMotion traffic is not compromised.

While VMware NSX L2VPN services are best suited for low-latency, high-bandwidth situations, long-distance vSphere vMotion can be a suitable option for implementations where the site-to-site network connectivity meets the recommended requirements for long-distance vSphere vMotion migration.

6.1.1 Long-Distance vSphere vMotion Migration Considerations

Long-distance vSphere vMotion migration requires that the latency between sites is less than 150 ms. VMware also recommends that a bandwidth of 250 Mbps be available for each vSphere vMotion operation. For configurations where the respective vCenter Server instances are in separate SSO domains, migration must be implemented leveraging the VMware vSphere API. An example of how to use PowerShell to execute API-driven long-distance vSphere vMotion operations can be found here.

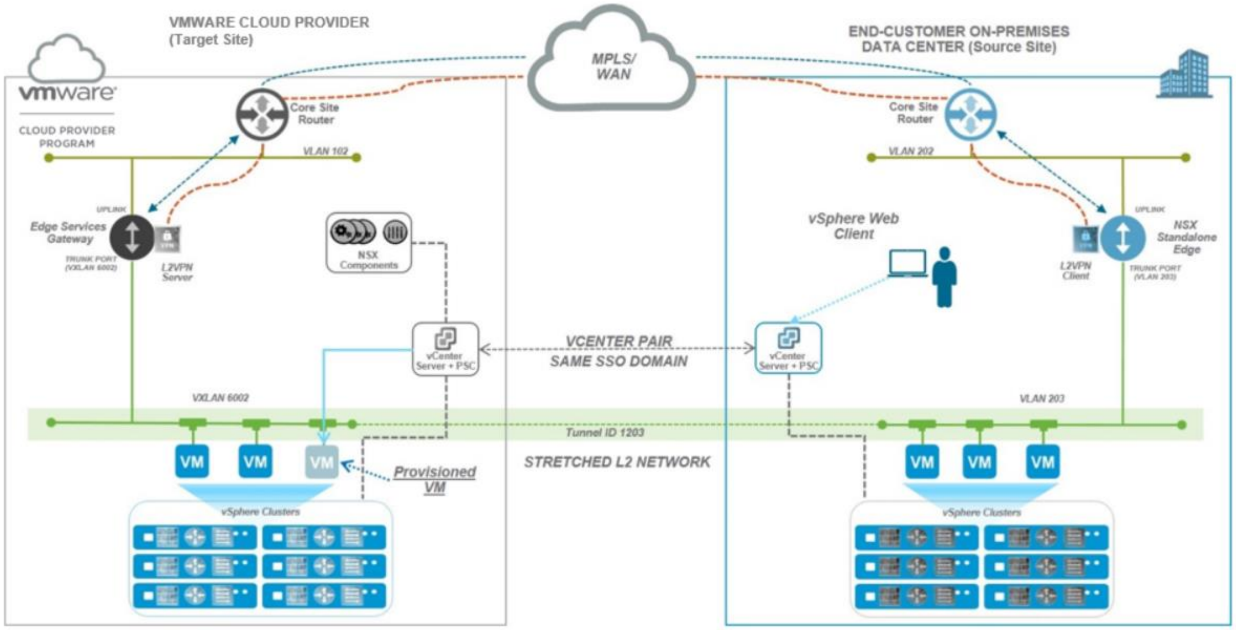
Table 2. Long-Distance vSphere vMotion Bandwidth and Latency

Attribute	Value
Long-distance vSphere vMotion latency minimum	150 ms
Per long-distance vSphere vMotion bandwidth minimum	250 Mbps

6.2 L2VPN and New Workload Provisioning

The following figure depicts a common onboarding scenario in which the customer wants to deploy new workloads onto the VMware Cloud Provider Program hosted service on an extended L2 network. This can be used in instances where an on-premises network must be extended to machines in the cloud, but it is simply more efficient to manually provision the workload to the VMware Cloud Provider Program hosted solution than it would be to migrate the workloads to the VMware Cloud Provider Program environment.

Figure 10. L2VPN New Workload Provisioning

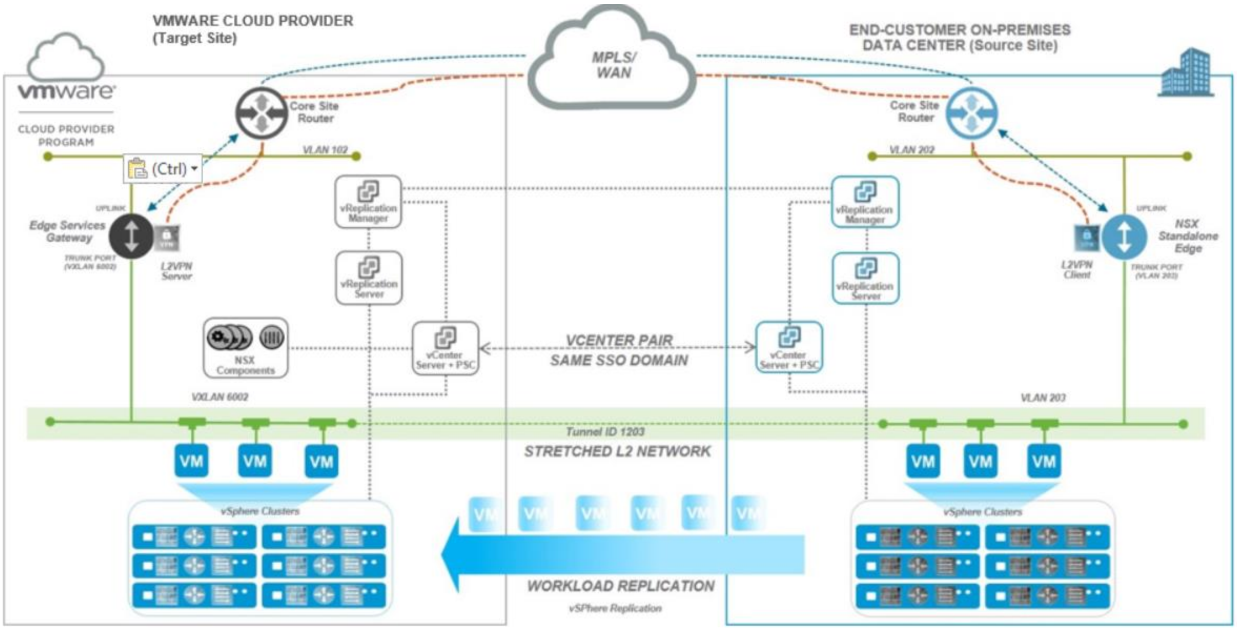


To ease management of both infrastructures, the vCenter Server instances can be paired on the same SSO domain and managed from the same login to the vSphere Web Client. Having both vCenter Server instances joined to the same SSO domain is optional, but is recommended for easier management of the environments.

6.3 L2VPN with vSphere Replication

In this scenario, vSphere Replication is used to migrate workloads from on premises to the VMware Cloud Provider. This scenario can leverage existing plans for vSphere Replication in a disaster recovery as a service (DRaaS) model. Using vSphere Replication as the migration tool is helpful in situations where network connectivity bandwidth and latency does not fit the requirements for long-distance vSphere vMotion operations, but is sufficient for ongoing replication of VM data.

Figure 11. L2VPN with vSphere Replication



Replication can occur while the VMs are active in the on-premises location. After replication is complete, a maintenance window can be scheduled to cut over to the replicated instance of the workloads in the VMware Cloud Provider Program hosted environment. As with the previous scenarios, joining both vCenter Server instances to the same SSO domain is optional, but recommended for easier management of the hybrid cloud environments.

Conclusion

With VMware NSX L2VPN services, VMware Cloud Providers can offer customers a path to onboarding workloads to the hosted VMware Cloud Provider Program solutions. For migration scenarios requiring VMs to maintain an existing IP address, or applications that require L2 access to on-premises workloads, VMware NSX L2VPN services can be deployed with minimal configuration to the underlying network infrastructure.

This document outlines some of the onboarding use cases of a vSphere to vSphere solution. VMware NSX L2VPN services can also be leveraged with VMware Cloud Providers who offer a public cloud (VMware vCloud Director® based pubic cloud). VMware Cloud Provider Program partners can look forward to other VMware Cloud Provider Program use cases with VMware NSX Service at VMware Partner Central.

References

The following table provides additional information pertinent to this document and its topics.

Document Title	Link or URL
VMware vCloud Architecture Toolkit for Service Providers	https://www.vmware.com/cloud-computing/cloud-architecture/vcat-sp.html
vCloud Architecture Toolkit (vCAT) Blog	https://blogs.vmware.com/vcat/
Architecting a VMware vSphere Compute Platform for VMware Cloud Provider Program	http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vcat/architecting-a-vmware-vsphere-compute-platform.pdf
Architecting a VMware NSX Solution for VMware Cloud Provider Program	http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/vcat/vmware-architecting-a-vmware-nsx-solution.pdf
Connecting Remote Sites with VMware NSX VMworld Session NET5352	https://vmworld2015.lanyonevents.com/connect/sessionDetail.ww?SESSION_ID=5352
VMware NSX 6.2 Administrator Guide	http://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/PDF/nsx_62_admin.pdf
vSphere Installation and Setup	http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-602-installation-setup-guide.pdf
Layer 2 VPN to the Cloud	https://fojta.wordpress.com/tag/l2vpn/