Designlet: HCX Network Extension on Google Cloud VMware Engine

VMware Cloud Migration

Table of contents

Designlet: HCX Network Extension on Google Cloud VMware Engine

Introduction

HCX Network Extension (NE) provides a Layer 2 VPN (L2VPN) to extend a broadcast domain from a customer site into an Google Cloud VMware Engine private cloud. NE functionality is provided by a dedicated virtual appliance at both sites.

Summary and Considerations

Use Case	NE is used to provide Layer 2 adjacency between VMs at the customer site and VMs that have been migrated to Google Cloud VMware Engine. This provides a stopgap to facilitate communication between VMs in the same VLAN/port group while migrations are occurring. NE is especially useful for customers who are not able to re-IP VMs during the migration process.
Pre-requisites	
General Considerations/Recommendations	
Cost implications	Egress charges will apply to VM traffic on extended networks communicating from Google Cloud VMware Engine to on-premises.
Performance Considerations	An NE appliance is capable of 4-6 Gbps throughput. Additional appliances can be deployed to scale throughput.
Documentation reference	HCX User Guide
Last Updated	July 2021

Planning and Implementation

Planning

HCX Network Extension (NE) provides a Layer 2 VPN between a customer site and an Google Cloud VMware Engine private cloud. This service is fully integrated into HCX and provides functionality similar to the NSX L2 VPN. Using an alternative bridging solution, like NSX L2 VPN, is not supported for use with NE, so you should settle on a single L2 extension technology for your migration or disaster recovery needs.

HCX NE appliances are deployed as a pair, with one running at the source site and the other at the destination site. The encrypted tunnel between NE appliances uses UDP port 4500. If there are any firewalls in the path between appliances, it should be configured to allow communication between the appliances on these ports.

NE is an optional service, and customers should understand the pros and cons involved with using it. There are alternatives to using NE, like assigning new IPs to VMs as they are migrated or moving a network with all attached VMs to the cloud in a single migration event. NE is a valuable tool when neither of these options is feasible. While the NE appliance is designed for reliability and quick boot, it is not highly available (vSphere High Availability can be used to mitigate this concern.) Additionally, HCX 4.0 includes an in-service upgrade option for NE appliances, which significantly reduces the downtime from a software upgrade to a matter of seconds.

Using NE with other HCX services can provide performance benefits and optimizations to traffic flow. HCX Traffic Engineering performs TCP Flow Conditioning, which dynamically adjusts MSS to reduce fragmentation for NE traffic. HCX Mobility Optimized Networking (MON) provides optimized traffic flows for VMs that are attached to an extended network and have been migrated to Google Cloud VMware Engine.

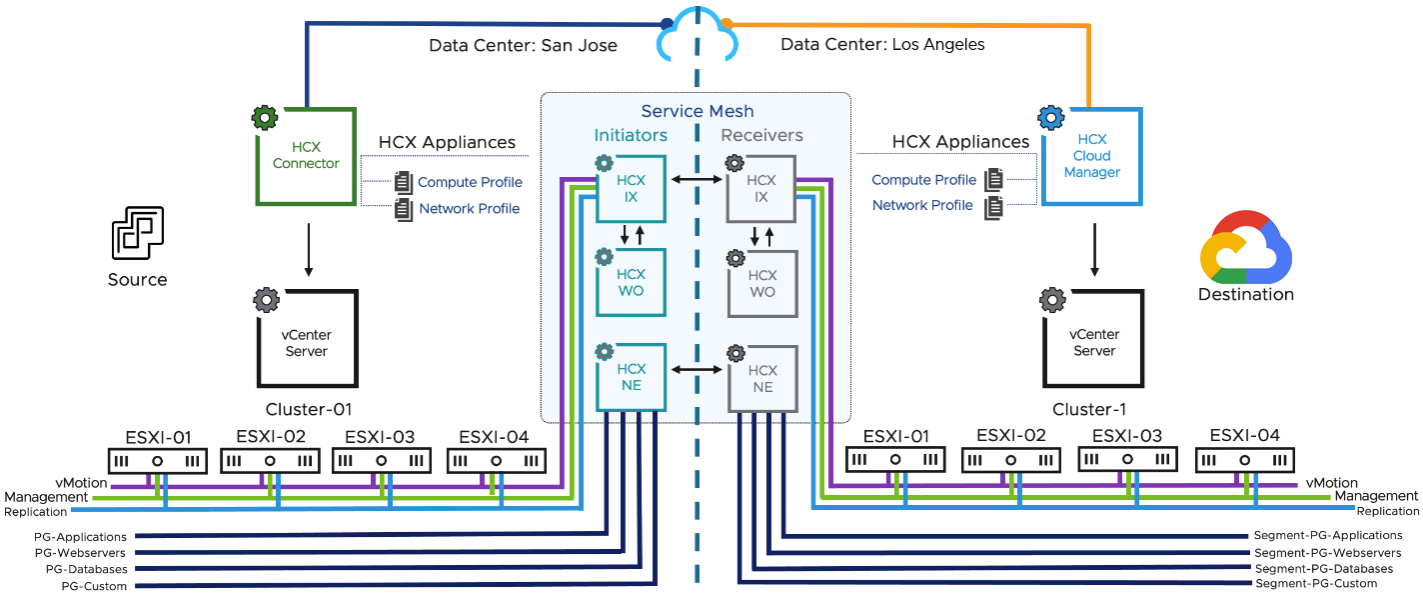

Figure 1 - Example HCX Service Mesh with Network Extension

Implementation

Eligible networks can be extended via the HCX Manager UI. Follow the steps below to extend a network.

To extend a network

- In the HCX Manager UI, navigate to Services > Network Extension. Any existing network extensions are displayed on this screen.
- Select **Extend Networks.**
- If you have multiple service meshes, select the appropriate service mesh from the dropdown list.
- Select the network(s) you want to extend, and click **Next.**
- Using the dropdowns, select the NSX-T tier-1 router that the extended network(s) will be attached to, and the NE appliance

to use.

- Provide the gateway IP address and prefix length in CIDR format (e.g. 192.168.10.1/24), and click **Submit.**

HCX will begin the process of extending the network. A status of **Extension complete** will appear for the network once the network is extended. To verify NE is working, migrate a VM that is connected to an extended network. Once migrated, verify communication is working between the migrated VM and a local VM in the same network. A simple ping should show increased latency to a migrated VM, indicating that the traffic is being transported across the L2VPN tunnel.

You can view information and metrics about extended networks, including local/remote MAC addresses and amount of data transferred.

To view network extension details

1. Navigate to Infrastructure > Interconnect.
2. Under the appropriate service mesh, Click **View Appliances.**
3. Expand the desired network extension appliance, and click **Network Extension details.**
4. To view metrics and information for a specific network, click **Show More Details.**