Cisco Nexus 1000V InterCloud

Deployment Guide (Draft)

June 2013

Contents

Overview

The industry is rapidly moving towards a cloud era. Private clouds are widely deployed and organizations are looking towards public clouds to expand their infrastructure to take advantage of the elasticity and cost advantage provided by a public cloud. To gain from the benefits of a public cloud but retain the security, management and control of a private cloud, customers are moving towards a hybrid cloud model.

Although the public cloud offers several advantages like reduced operational and infrastructures costs, rapid application provisioning and abundant resource availability it poses some challenges that are preventing enterprises from fully harnessing the power of the public cloud. Some of the main concerns slowing adoption of hybrid clouds are:

- Security concerns for applications running in a public provider environment – lack of enterprise control and monitoring
- Rearchitecting applications to migrate them from a private or hosted data center to a provider cloud
- Redesigning services and policies to utilize the services offered by the provider
- Inconsistent operational models and tools across cloud providers
- Inability to move workloads between cloud providers leading to vendor lock-in

Nexus 1000V InterCloud provides a hybrid cloud solution that aims to solve these challenges and accelerate the adoption of hybid clouds. Using Nexus 1000V InterCloud an enterprise can securely extend their data center into the public cloud. A secure Layer 2 extension enables data center center applications and services to be run in a public cloud environment as if they were on the private enterprise data center network. All data traversing the system is cryptographically isolated and secured using keys that are generated and managed within the enterprise.

This document provides guidelines for deploying Nexus 1000V InterCloud. Common use cases and deployment scenarios for Nexus 1000V InterCloud will be covered.

For detailed configuration documentation, please refer to the respective Cisco® product configuration guides found on http://www.cisco.com. You will find links to the product configuration guides and other related deployment guides in the "For More Information" section of this document.

Audience

This document is intended for network architects, network engineers and cloud administrators interested in deploying a hybrid cloud solution using Nexus 1000V InterCloud.

Background

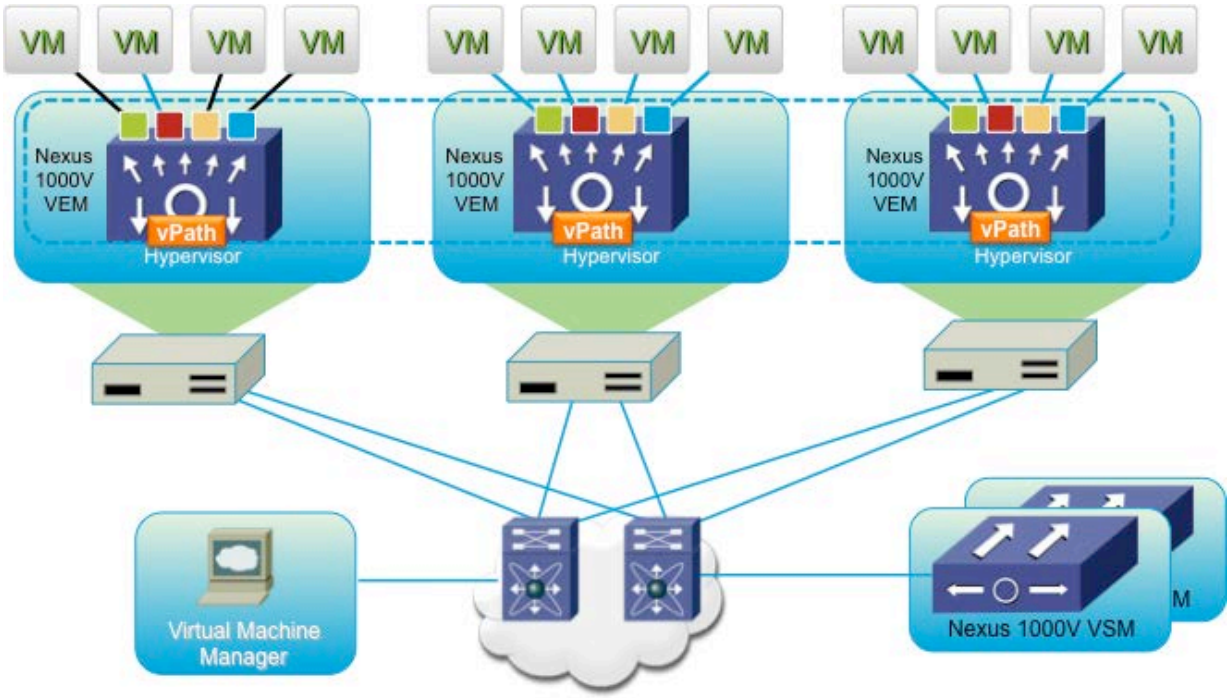
Cisco Nexus 1000V Series Networking

The Cisco Nexus 1000V Series provides Layer 2 switching, advanced networking functions, and a common network management model in a virtualized server environment by replacing the virtual switch within a hypervisor. As Figure 1 shows, the Cisco Nexus 1000V Series Switches manage a data center. Each server in the data center is represented as a line card in the Cisco Nexus 1000V Series Switch and can be managed as if it were a line card in a physical Cisco switch.

The Cisco Nexus 1000V Series implementation has two main components:

- Virtual Supervisor Module (VSM)
- Virtual Ethernet module (VEM)

Figure 1. Cisco Nexus 1000V Series Switch Architecture



Virtual Supervisor Module (VSM)

The VSM provides the management plane functions for the Cisco Nexus 1000V Series. Unlike a traditional Cisco switch, in which the management plane is integrated into the hardware, on the Cisco Nexus 1000V Series, the VSM is deployed as either a virtual appliance on a hypervisor or as a virtual service blade on the Cisco Nexus Cloud Services Platform. The VSM is usually deployed in a high-availability pair, with one VSM functioning as the primary and the other VSM functioning as the secondary supervisor. When the primary VSM fails the secondary VSM will take over as primary.

Virtual Ethernet Module (VEM)

The VEM provides the Cisco Nexus 1000V Series with network connectivity and forwarding capabilities much like a line card in a modular switching platform. Unlike multiple line cards in a single chassis, each VEM acts as an independent switch from a forwarding perspective. The VEM is tightly integrated with the hypervisor it is running on. A pair of VSMs managing one or more VEMs comprise a single Nexus 1000V switch instance.

The communication between the VSM and VEM can be in Layer 2 mode where the VSM and VEMs are in the same Layer 2 domain or in Layer 3 mode. Layer 3 mode is the recommended mode for VSM to VEM communication.

Overview of Cisco Nexus 1000V InterCloud

Nexus 1000V InterCloud is built on the proven infrastructure of the Nexus 1000V Distributed Virtual Switch. It is managed and operated by the Cisco Prime Network Services Controller which is also used to manage virtualized services deployed with Nexus 1000V.

Nexus 1000V InterCloud 1.0 provides the following capabilities:

- Secure network extension from a private data center network to Amazon AWS
- Integration with VMware vCenter version 5.0 and 5.1 to view enterprise Virtual Machine inventory and migrate enterprise applications and templates into Amazon AWS
- Single pane of management for all VMs within InterCloud including VM creation, deletion and cloning
- Advanced Nexus 1000V switching features such as ACL and IGMP for applications running in the public cloud

Nexus 1000V InterCloud comprises of the following infrastructure components:

1 – Cisco Prime Network Services Controller – Single pane of glass for management of Nexus 1000V InterCloud

2 – InterCloud Virtual Switch – Distributed Virtual Switch that spans across enterprise and provider clouds

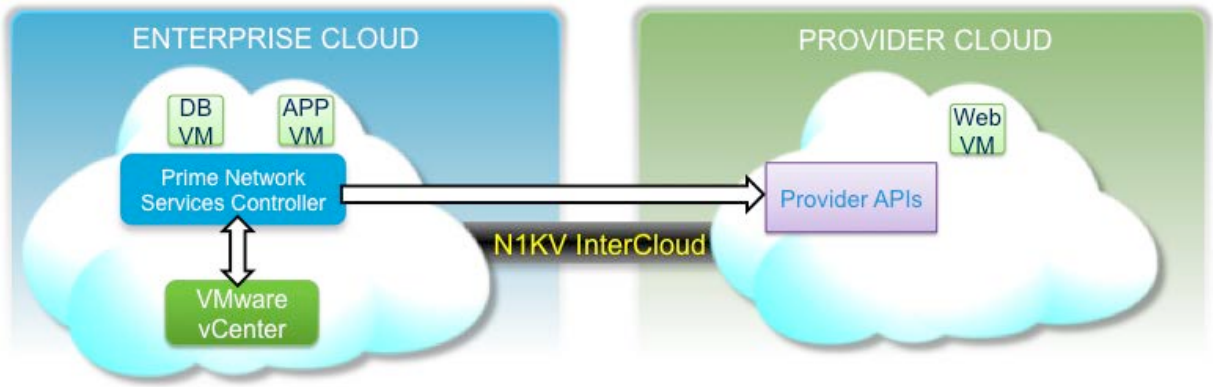
3 – InterCloud Agent – Runs on every cloud Virtual Machine to provide multi-NIC support and encryption support

Cisco Prime Network Services Controller

The Cisco Prime Network Services Controller is the single pane of glass to manage Nexus 1000V InterCloud. It integrates with the Virtual Machine Manager on the enterprise, and is also integrated with the cloud provider through well-known APIs. Cisco Prime Network Services Controller is deployed as an OVA file within vCenter.

In the first release of InterCloud the Cisco Prime Network Services Controller will integrate with VMware vCenter version 5.0 or 5.1 on the enterprise and with Amazon Web Services (AWS) on the provider side. Future releases will add support for additional Virtual Machine Managers and providers.

Figure 2. Cisco Prime Network Services Controller



InterCloud Virtual Switch

The InterCloud Virtual Switch is made up of a Virtual Supervisor Module (VSM) and an InterCloud Link. The InterCloud Link refers to a secure tunnel that is formed between a pair of Virtual Machines – the InterCloud Extender running in the enterprise and the InterCloud Switch running in AWS.

InterCloud Virtual Supervisor Module (VSM)

The InterCloud VSM is similar to the Nexus 1000V VSM, but is only used to configure networking and services for Virtual Machines in the provider cloud. The enterprise data center can run Nexus 1000V or any other virtual switch or Distributed Virtual Switch (DVS). The Nexus 1000V InterCloud software package includes the image for the VSM to be used with InterCloud. The InterCloud VSM image is currently different from the Nexus 1000V VSM image.

InterCloud Link

The InterCloud Link comprises of the InterCloud Extender (ICX) virtual machine, InterCloud Switch (ICS) virtual machine and the secure tunnel that connects the InterCloud Extender and InterCloud Switch. An InterCloud Link is configured through the Cisco Prime Network Services Controller web interface. This configuration automatically triggers the creation of the InterCloud Extender (ICX) and InterCloud Switch (ICS) virtual machines and the establishment of a secure tunnel between them. The InterCloud Extender and InterCloud Switch register with the InterCloud VSM as service modules and are managed like VEMs. A single VSM can manage up to 8 InterCloud Links deployed in a high-availability configuration.

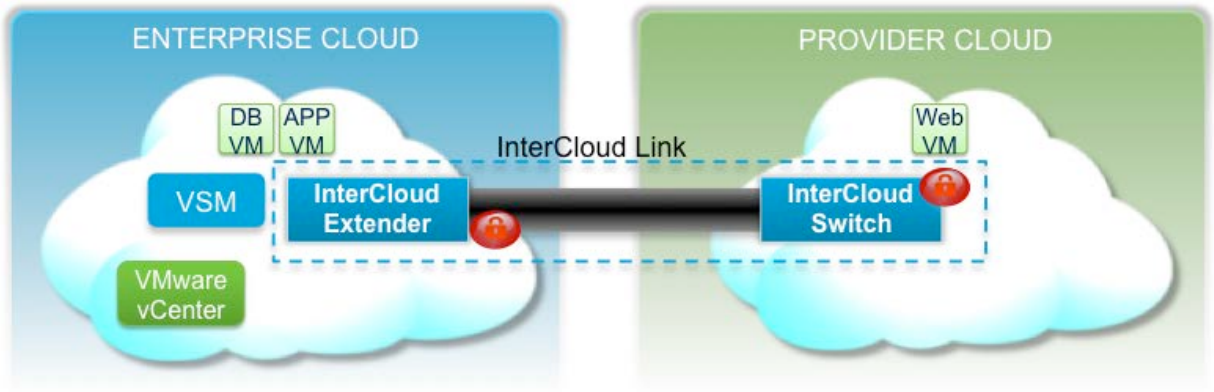
InterCloud Extender (ICX)

The InterCloud Extender (ICX) is deployed as a Virtual Machine within vCenter. The InterCloud Extender can be deployed manually or automatically through the Cisco Prime Network Controller while creating an InterCloud Link. It is recommended to always deploy the InterCloud Extender automatically through the Cisco Prime Network Services Controller. The InterCloud Extender is the endpoint for the secure tunnel from the provider to the enterprise. Additionally it is the entity that provides for the extension of the enterprise network to the public cloud.

InterCloud Switch (ICS)

The InterCloud Switch (ICS) is deployed as a Virtual Machine within the provider environment. When Amazon is used as the provider, the InterCloud Switch image is an AMI image that is uploaded to AWS and deployed through the Cisco Prime Network Services Controller while creating an InterCloud Link. The InterCloud Switch is the endpoint for the secure tunnel on the provider side. In addition it is also the secure tunnel endpoint for the Virtual Machines running in the cloud. All traffic that is sent, both from the enterprise to the provider and between Virtual Machines in the public cloud will go through the InterCloud Switch.

Figure 3. Cisco Nexus 1000V InterCloud Virtual Switch



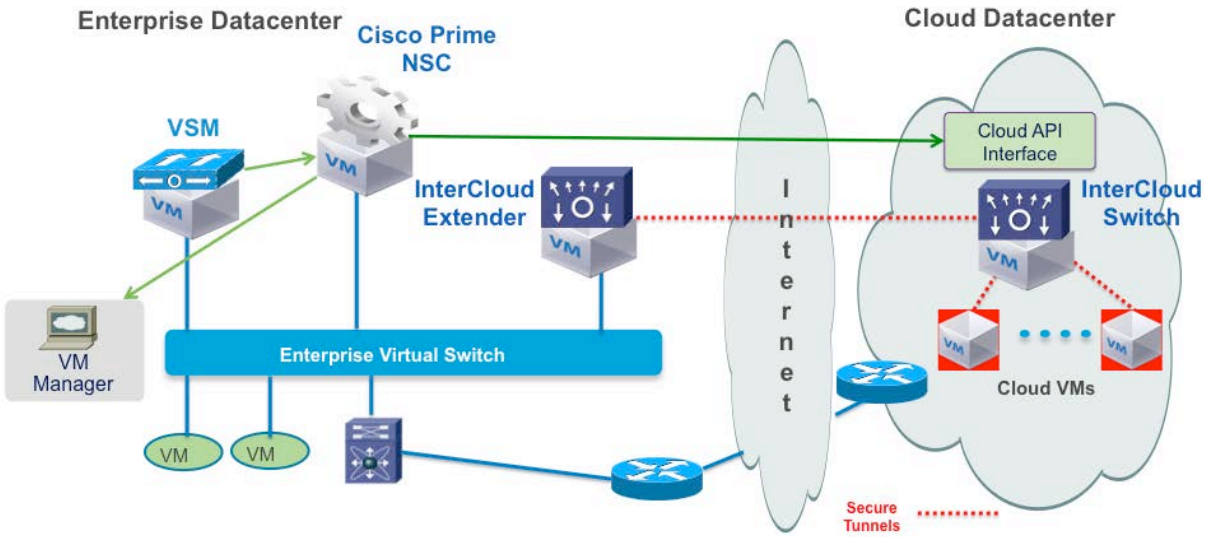
InterCloud Agent (ICA)

The Virtual Machines in the provider cloud are required to run an InterCloud Agent image in order to be part of the InterCloud solution. When a Virtual Machine is migrated from the enterprise or a template is copied from the enterprise to the provider cloud, Cisco Prime Network Services Controller automatically adds the InterCloud Agent image to the Virtual Machine. The ICA is dependent on the Operating System (OS) and version of the Virtual Machine. The supported OS types are:

- RedHat Enterprise Linux Version 6.0/6.1/6.2/6.3 (64-bit and 32-bit versions)
- CentOS 6.3 (64-bit and 32-bit versions)
- Win 2008 R2 (Service Pack1) AMI and VMDK template

Nexus 1000V InterCloud Component Interfaces

Figure 4 shows the main components of the InterCloud solution architecture. There are specific communication needs between each of the components and the following sections will detail the interfaces on each component and how they are used for communication with other interfaces in the system.



Cisco Prime Network Services Controller

The Cisco Prime Network Services controller has a single management interface that is used for web and SSH access. The management interface must have a connection to the public Internet in order to reach the provider. Specifically, the management interface is used for communication with the following components:

- Virtual Supervisor Module
- VMware vCenter
- InterCloud Extender
- InterCloud Switch
- Amazon AWS (Requires public IP through NAT/PAT)
- Cloud Virtual Machines (Requires public IP through NAT/PAT)

Virtual Supervisor Module (VSM)

The Virtual Supervisor Module runs the control plane for the InterCloud Virtual Switch, similar to the Nexus 1000V VSM. The VSM for InterCloud is always run in L3 control mode. The InterCloud Extender and InterCloud Switch register as service modules in this VSM and are displayed in the “show module” output.

The VSM has the same three interfaces – control, packet and management as the Nexus 1000V VSM.

Control Interface –

- Used for communication between active and standby VSM

Management Interface –

- Used to connect to the CLI of InterCloud VSM using SSH
- Used for communication with Cisco Prime Network Services Controller
- This interface is always used as the source interface for L3 control communication with the InterCloud Extender and InterCloud Switch

Packet Interface –

- Not used since only Layer 3 communication is supported for InterCloud VSM

InterCloud Extender

The InterCloud Extender is the endpoint for the secure tunnel from the provider to the enterprise and provides the network extension for VLANs in the enterprise. The InterCloud Extender has three external interfaces and two internal interfaces that perform the following functions:

Data Trunk Interface –

- Trunk interface carrying all the VLANs that need to be extended to the public cloud. This interface is configured with a port-profile on the Enterprise VSM or with a VMware port-group. The VLANs carried in this VLAN must match the VLANs configured on the Internal Tunnel Trunk and Internal Enterprise Trunk interface.

- The trunk interface operates in promiscusous mode. All broadcast/multicast and unknow unicast traffic is sent over the secure tunnel to reach the Virtual Machines in the public cloud

Management Interface –

- Used to connect to the CLI of InterCloud Extender using SSH
- Cisco Prime Network Services Controller uses this interface to configure the InterCloud Extender
- Used as the source interface for L3 control communication with the VSM
- Can be used as the tunnel endpoint for the secure tunnel with the InterCloud Switch. If the management interface is used as the tunnel endpoint it must have a public IP.

Tunnel Interface –

- Optional interface to be used as the tunnel endpoint for secure tunnel with InterCloud Switch
- Used to keep management network private, the tunnel interface will need to have access to the Internet either through NAT/PAT or a direct public IP address.

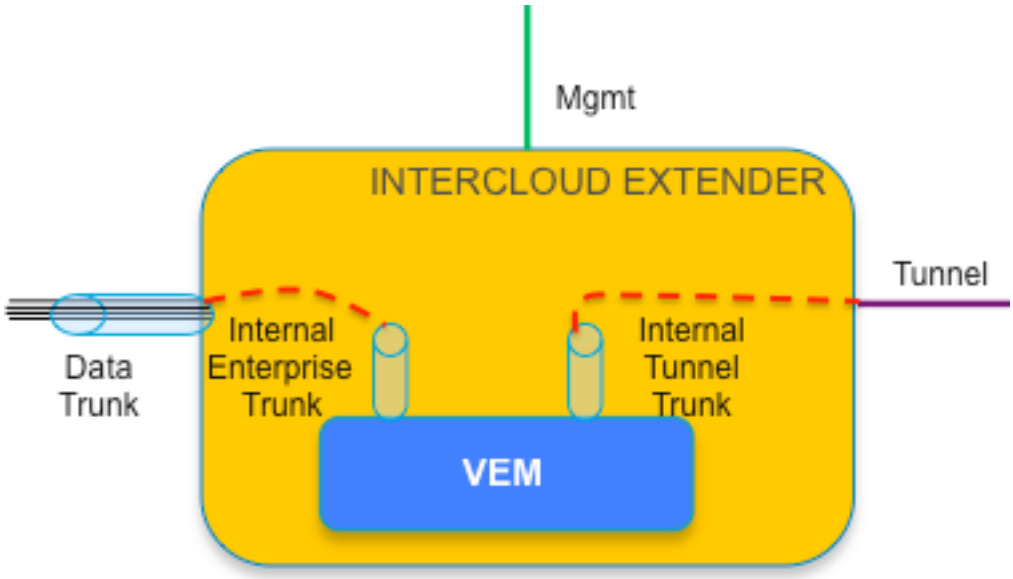
Internal Enterprise Trunk Interface -

- This interface is used to trunk the VLANs on the Data Trunk interface to the embedded VEM in the InterCloud Extender.
- By default this interface is assigned the port-profile **N1K_Cloud_Default_Trunk** which has been pre-configured on the InterCloud VSM.
- The port-profile can be changed by selecting a different port-profile in Cisco Prime Network Services Controller during creation of InterCloud Link. Different port-profiles are generally needed if the same VSM is supporting multiple InterCloud Links extending different sets of VLANs.

Internal Tunnel Trunk Interface -

- This interface is used to trunk the VLANs from the embedded VEM in the InterCloud Extender to to the VEM on the InterCloud Switch through the site-to-site tunnel. Figure 4 shows the Tunnel interface used as the tunnel endpoint.
- By default this interface is assigned the port-profile **N1K_Cloud_Default_Trunk** which has been pre-configured on the InterCloud VSM.
- The port-profile can be changed by selecting a different port-profile in Cisco Prime Network Services Controller during creation of InterCloud Link. Different port-profiles are generally needed if the same VSM is supporting multiple InterCloud Links extending different sets of VLANs.

Figure 4. InterCloud Extender Interfaces



InterCloud Switch

The InterCloud Switch is a Virtual Machine deployed within a provider environment and will be configured with an IP address that is assigned by the provider. The InterCloud Switch also has an embedded Virtual Ethernet Module that provides secure switching for Virtual Machines in the public cloud. The interfaces associated with an InterCloud Switch are:

Management Interface –

- The management interface is an internal interface that is configured with an enterprise address
- Used as the source interface for L3 control communication with InterCloud VSM

Internal Tunnel Trunk Interface -

- This interface is used to trunk the VLANs from the embedded VEM in the InterCloud Switch to to the VEM on the InterCloud Extender through the site-to-site tunnel. Packets sent on the Internal Tunnel Trunk interface are encrypted and sent out on the provider public interface and vice versa.
- By default this interface is assigned the port-profile **N1K_Cloud_Default_Trunk** which has been pre-configured on the InterCloud VSM.
- The port-profile can be changed by selecting a different port-profile in Cisco Prime Network Services Controller during creation of InterCloud Link. Different port-profiles are generally needed if the same VSM is supporting multiple InterCloud Links extending different sets of VLANs.

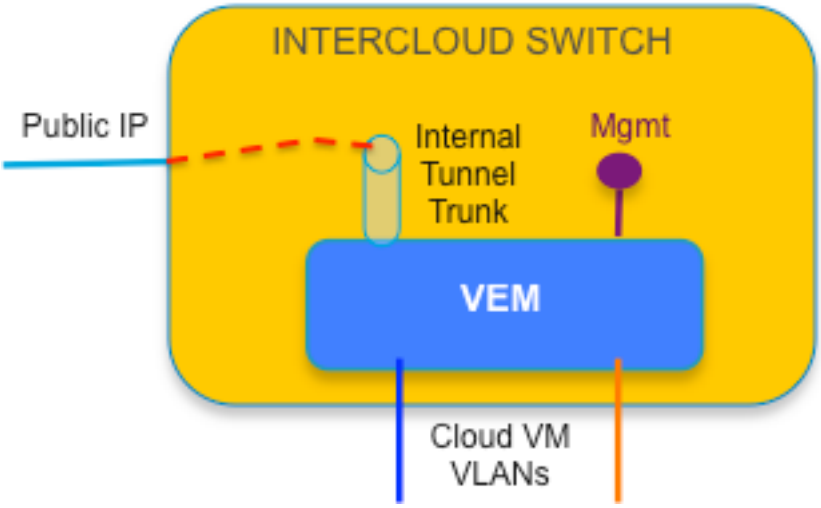
Cloud Virtual Machine Interfaces –

- These interfaces are the secure tunnel endpoints on the InterCloud Switch to Virtual Machines in the public cloud
- The Virtual Machine interfaces connected to these interfaces are configured with port-profiles on the InterCloud VSM (and will also show up as vEth interfaces)

Provider Public Interface –

- Cisco Prime Network Services Controller uses this interface to configure the InterCloud Switch
- Used as the endpoint for the secure tunnel with InterCloud Extender
- This is the only interface accessible over the public Internet
- Used as the tunnel endpoint for the secure tunnel to Virtual Machines in the public cloud

Figure 5. InterCloud Switch Interfaces



Cloud Virtual Machines

The cloud virtual machines are modified versions of the enterprise Virtual Machines that include an InterCloud Agent. The InterCloud Agent provides multi-NIC support as well as support for the secure tunneling between the cloud VM and the InterCloud Switch. The interfaces for the cloud VM are as follows:

Cloud Virtual Machine Provider Public Interface –

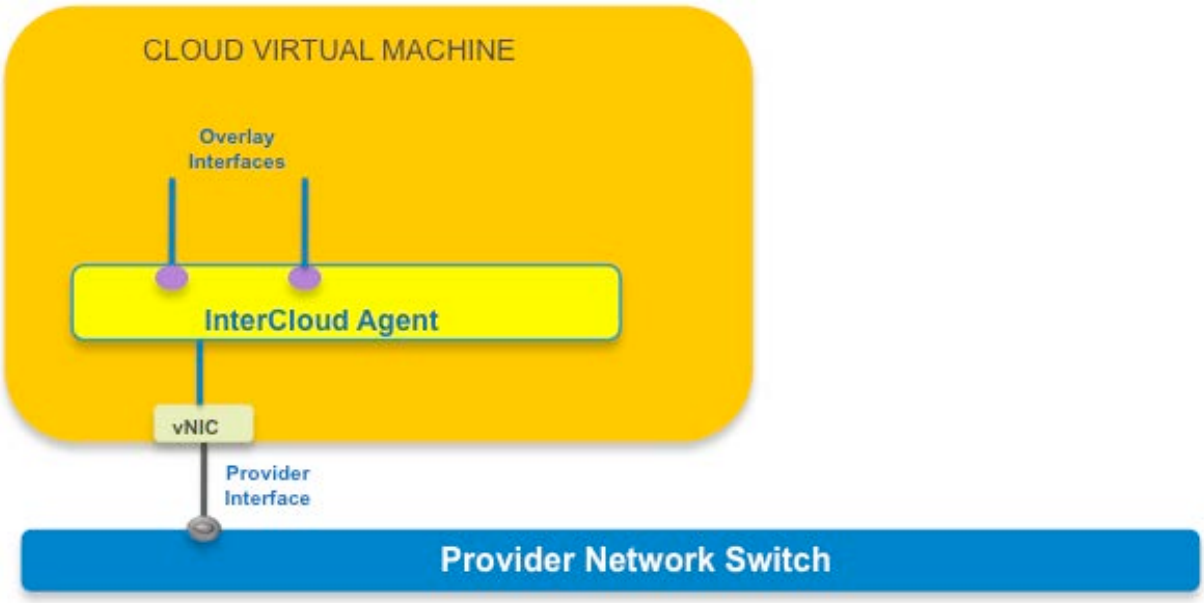
- Cisco Prime Network Services Controller uses this interface to configure the cloud VM
- The access to the provider interface is restricted to prevent an unauthorized user from logging in directly.

Cloud Virtual Machine Overlay Interfaces –

- These interfaces are used to connect the Virtual Machines in the public cloud to the InterCloud Switch through secure tunnels.
- These interfaces are configured with port-profiles on the InterCloud VSM
- A maximum of 8 vNICs are supported for a cloud VM

- These interfaces can be configured through Cisco Prime Network Service Controller to change the port-profile, IP address configuration or DNS information.

Figure 6. InterCloud Switch Interfaces



Security in Nexus 1000V InterCloud

All data in motion is cryptographically isolated and encrypted within the InterCloud solution. This includes traffic exchanged between the InterCloud Extender and InterCloud Switch as well as traffic between the InterCloud Switch and cloud Virtual Machines. A DTLS tunnel is created between these endpoints in order to securely transmit this data, DTLS is a UDP-based secure transmission protocol. The InterCloud Extender always initiates the DTLS tunnel creation.

If there is a firewall protecting access to the internal network the UDP port 6644 must be opened in the outbound direction in order to send DTLS traffic from the InterCloud Extender to InterCloud Switch. If a ACLs are used instead of a firewall, both outbound access with a source port of 6644 must be permitted as well as inbound access with a destination port of 6644 must be permitted.

The keys used for the tunnel between InterCloud Extender and the InterCloud Switch and the tunnel between the InterCloud Switch and cloud Virtual Machines are generated and maintained by the Cisco Prime Network Services Controller. The encryption algorithm used is configurable, with the ability to select different encryption strengths for each tunnel based on the level of security desired.

The supported encryption algorithms are:

- AES-128-GCM
- AES-128-CBC
- AES-256-GCM (Suite B)

- AES-256-CBC
- None

The supported hashing algorithms are:

- SHA-1
- SHA-256
- SHA-384

A default tunnel profile is pre-created in Cisco Prime Network Services Controller with AES-128-CBC as the encryption algorithm and SHA-1 as the hash function. A user can create a new tunnel profile to use a different encryption algorithm or hash. It is not recommended to modify the default tunnel profile.

It is also possible to set a rekey period through the Cisco Prime Network Services Controller to refresh the encryption keys.

Nexus 1000V InterCloud High Availability

High Availability in Nexus 1000V InterCloud is implemented for each component of the InterCloud Infrastructure.

High Availability for Cisco Prime Network Services Controller

The Cisco Prime Network Services Controller is deployed as a Virtual Machine with vCenter and utilizes the High Availability mechanism provided within vCenter.

High Availability for InterCloud VSM

The behavior of the InterCloud VSM deployed as a highly available pair is identical to the HA behavior of Nexus 1000V VSM which leverages the HA mechanism provided by NX-OS. For more details on Nexus 1000V High Availability please refer to the High Availability Configuration Guide at: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_2_2_1/high_availability/b_Cisco_Nexus_1000V_High_Availability_and_Redundancy_Configuration_Guide_2_2_1.html.

High Availability for InterCloud Link

The InterCloud Link comprising of the InterCloud Extender, InterCloud Switch and the tunnel between them is considered as a single unit for the purpose of high availability. When an InterCloud Link is created in HA mode, two pairs of InterCloud Extender and InterCloud Switch VMs are created. These VMs are configured with their own individual IP addresses and are required to be able to communicate with the Cisco Prime Network Services Controller.

Upon instantiation of the Virtual Machines the HA role is pushed by the Cisco Prime Network Services Controller to both deployed InterCloud Extender VMs. The Active InterCloud Extender and InterCloud Switch establish a secure tunnel between them, and the active InterCloud Switch establishes the secure tunnel with the cloud Virtual machines. The Standby InterCloud Extender and InterCloud Switch also establish a secure tunnel between them.

When a failure is detected in the active InterCloud Switch or Extender, the entire HA entity comprising of the endpoints and the secure tunnels is brought down. The standby InterCloud Extender and InterCloud Switch become active and replace the failed pair. In addition, the newly active InterCloud Switch will establish secure access tunnels with the cloud VMs. The failed InterCloud Extender and InterCloud Switch are rebooted to ensure they come up in a standby role.

Nexus 1000V InterCloud Scalability

The scalability numbers for InterCloud can be found in the following document:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/InterCloud/sw/5_2_1_I_C_1_1_1/verified_scalability/reference/InterCloud_Verified_Scalability.html

Nexus 1000V InterCloud Deployment Pre-requisites

The following pre-requisites must be met to begin deploying Nexus 1000V InterCloud:

- The first release will support VMware vSphere Version 5.0 or 5.1 as the Enterprise Virtual Machine Manager. Enterprise Plus license is not required for InterCloud.
- The cloud provider supported is Amazon Web Services. An Amazon account is required to be set up and the access credentials available.
- Internet Router/Firewall must allow outbound/inbound traffic originating from enterprise network to the range of AWS IP addresses for the following protocols and ports:

  IP address range: https://forums.aws.amazon.com/ann.jspa?annID=1701

  Ports:

  TCP 80 – HTTP access from Cisco Prime Network Services Controller to call provider APIs and communicate with InterCloud VMs in provider cloud

  TCP 443 – HTTPS access from Cisco Prime Network Services Controller for AWS calls and communicating with InterCloud VMs in provider cloud

  TCP 22 – SSH from Cisco Prime Network Services Controller to InterCloud VMs in provider cloud

  UDP 6644 – DTLS data tunnel

  TCP 6644 – DTLS control tunnel

  If the ports required for communication are not opened, the command **test intercloud ics-reachability** can be run on the InterCloud Extender CLI to verify reachability.
- After installation of Cisco Prime Network Services Controller NTP configuration is required to ensure the time is in sync with that of AWS.

Nexus 1000V InterCloud Common Deployment Scenarios

Nexus 1000V InterCloud requires access from the enterprise to the public Internet in order to access the public provider cloud. This leads to some specific considerations while planning to deploy InterCloud within an enterprise. Fundamentally, the security requirements for the enterprise management network will determine the following two choices:

- Choosing between the management interface or tunnel interface on the InterCloud Extender as the source for the DTLS tunnel to the InterCloud Switch in the provider.
- Choosing the VLAN that will be extended to the provider cloud for InterCloud Switch Management. The InterCloud Switch management interface must be reachable by the VSM in the enterprise.

The following table lists the communication requirements and IP addresses needed to deploy Nexus 1000V InterCloud. Based on the deployment scenarios some IP addresses may not be required.

Component	Interface	Connectivity Requirements
Cisco Prime Network Services Controller	Management	• VMware vCenter Server • InterCloud Extender Management • InterCloud Switch Management • Cloud VMs Provider Public IP
InterCloud VSM	Management	• InterCloud Extender Management • InterCloud Switch Management
InterCloud Extender	Management	• InterCloud VSM Management • InterCloud Switch Provider Public IP (if tunnel source) • Cisco Prime Network Services Controller Management
	Tunnel	• InterCloud Switch Provider Public IP (if tunnel source)
InterCloud Switch	Management	• InterCloud VSM Management • InterCloud Extender Management/Tunnel (tunnel source) • Cisco Prime Network Services Controller Management
	Provider Public IP (assigned by provider)	• Cisco Prime Network Services Controller Management • Cloud VMs Provider Public IP
Cloud VM	Provider Public IP (assigned by provider)	• Cisco Prime Network Services Controller Management • InterCloud Switch Provider Public IP
	Overlay Interfaces	• Cloud VMs Overlay Interfaces • Enterprise VMs

Tunnel Interface as Tunnel Endpoint and Enterprise Management Network extended to Cloud

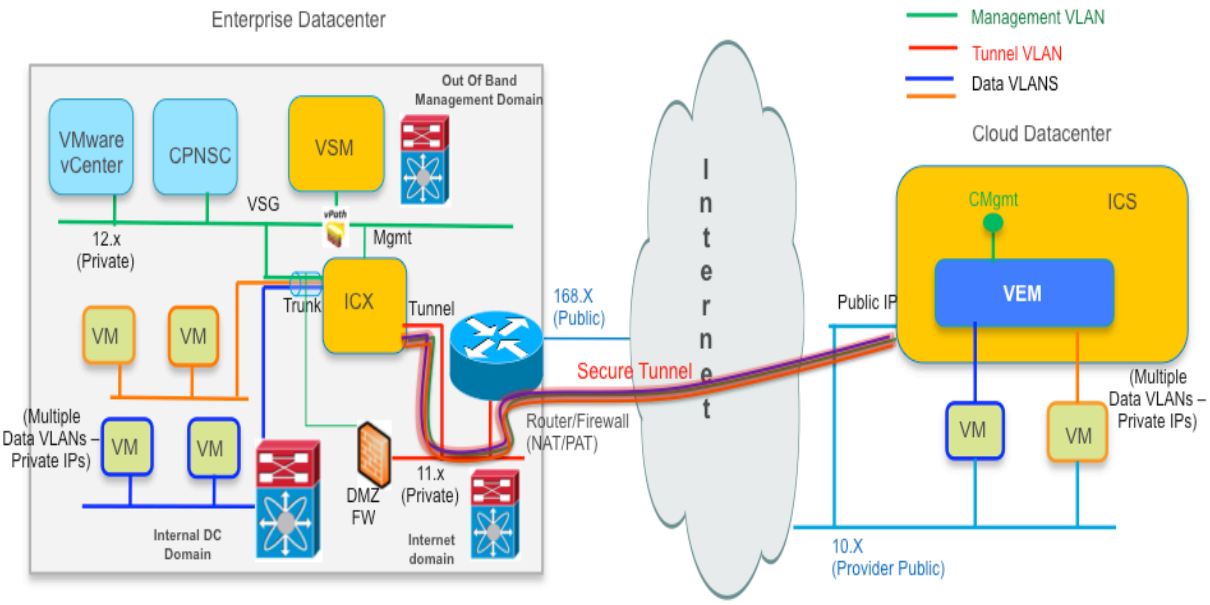
Figure 7 shows a typical enterprise data center design where there are three typical domains. The management domain is only used for out-of-band management and has no connection to the public Internet. The data domain is for the workloads within the data center and the Internet domain has a private network going through a router/firewall providing NAT/PAT to access the public Internet. These domains are typically isolated from each other using a combination of Virtual Security Gateways and firewalls providing a DMZ area for external facing components.

In this scenario, the typical deployment of the InterCloud components is as follows:

- VMware vCenter, Cisco Prime Network Services Controller, VSM for InterCloud, InterCloud Extender and InterCloud Switch are on the same management VLAN.
- The management network is extended to the provider cloud for InterCloud Switch management

- The tunnel interface is used as the tunnel source and will be in a DMZ with external access
- The Cisco Prime Network Services Controller requires external access and will go through a DMZ firewall to be connected to the public domain

Figure 7. Tunnel Interface as Tunnel Endpoint and ICS on Enterprise Management Network

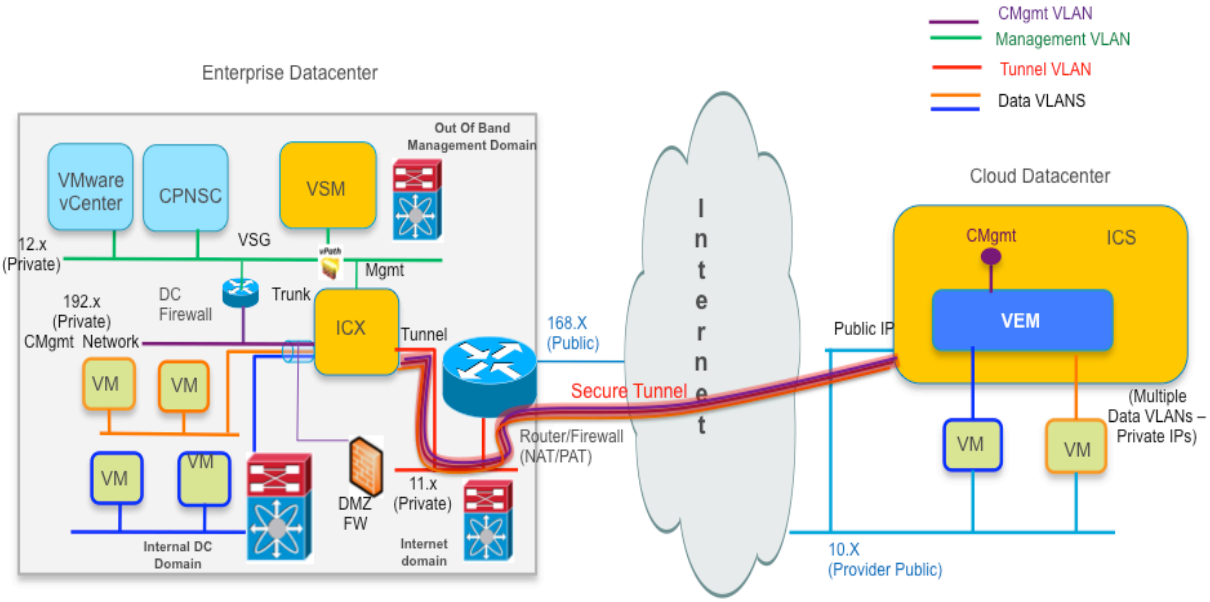


Tunnel Interface as Tunnel Endpoint and Separate Management Network for InterCloud Switch

For deployments where the security rules or regulations disallow extending the private management network on the enterprise to the public domain, the InterCloud Switch management can be placed on a separate VLAN that is extended from the enterprise.

Figure 8 shows a typical deployment in this scenario. The only difference between this deployment example and the one is Figure 7 is the requirement to allocate a VLAN separate from the management VLAN to extend to the cloud, and a mechanism to route between this VLAN and the management VLAN for the InterCloud Switch to communicate with the VSM.

Figure 8. Tunnel Interface as Tunnel Endpoint and ICS on separate Management Network

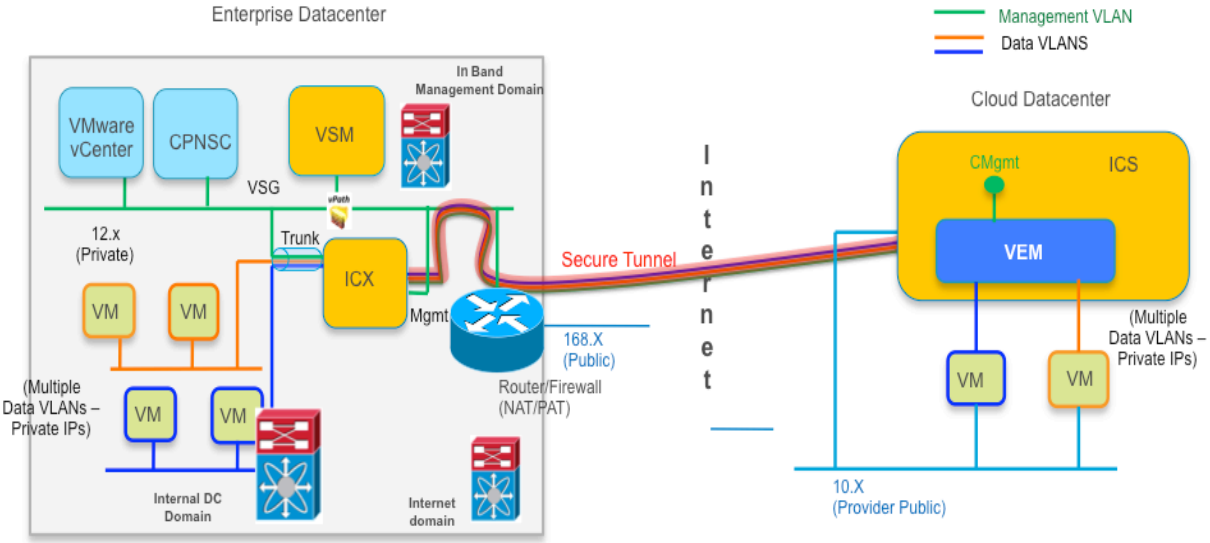


Management Interface as Tunnel Endpoint and Enterprise Management Network extended to Cloud

It is also possible to use the management interface on the InterCloud Extender as the tunnel source. This is considered a less likely scenario in customer environments, but is supported. This scenario may be likely in a lab environment.

Figure 9 shows a typical deployment with the management interface used as the tunnel endpoint. In this case the tunnel interface and VLAN are no longer required and do not need to be configured.

Figure 9. Management Interface as Tunnel Endpoint and ICS on Enterprise Management Network

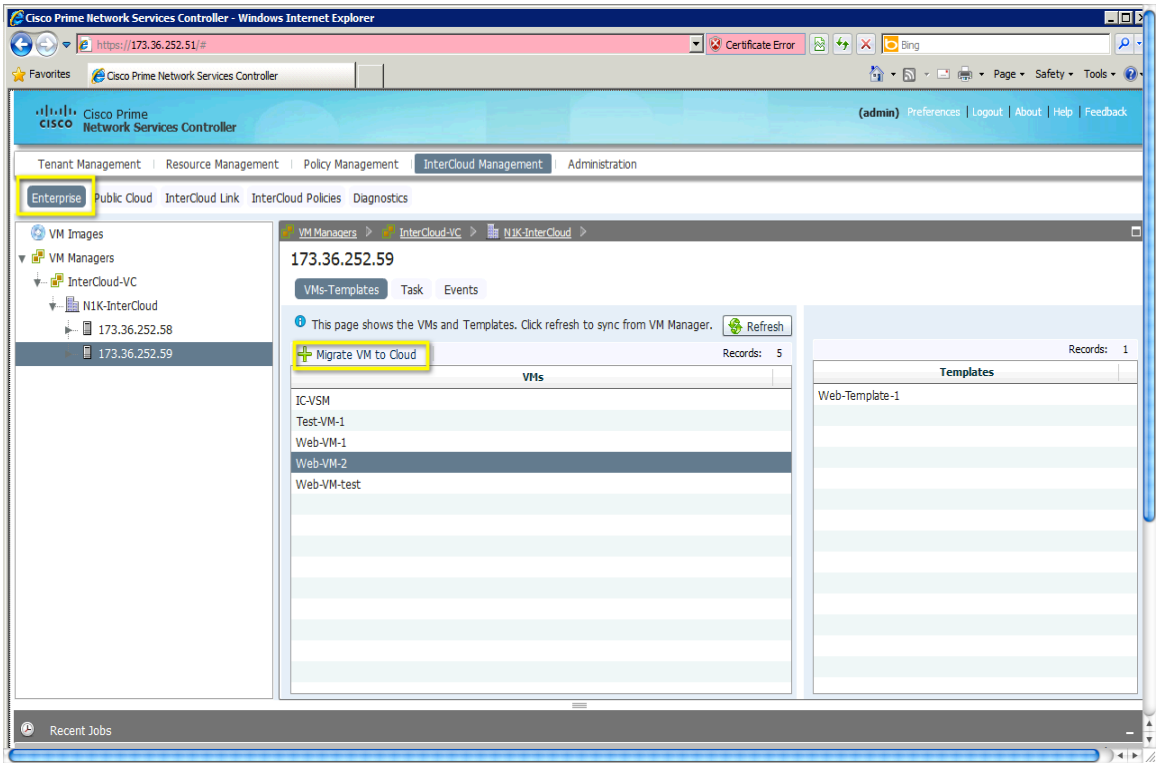


Nexus 1000V InterCloud Use Cases

Use Case 1 – Migrate workloads to the public cloud

Once a network extension has been created by means of an InterCloud Link, Virtual Machines in the enterprise vCenter can be migrated to the public cloud through the **Enterprise** tab on the Cisco Prime Network Services Controller. The migration is a cold migration; the Virtual Machine is shut down at the start of the procedure, migrated and started in the cloud. The Virtual Machine in the enterprise will remain powered off.

Figure 10. Migrating a VM through Cisco Prime Network Services Controller



For a user, the process of migrating a workload is a matter of a few clicks. The most important configuration performed is the assignment of a port-profile on the InterCloud VSM for the Virtual Machine to use after it is migrated. Behind the scenes the Cisco Prime Network Services Controller will read the vmdk file for the Virtual Machine, convert it to an Amazon Machine Image (AMI) format, add the InterCloud Agent and copy the final image to the provider using provider API calls. The Virtual machine is then brought up on the provider side and can be viewed through the **Public Cloud** tab in the Cisco Prime Network Services Controller web UI.

All Virtual Machines in the public cloud can only have locally attached storage. If a Virtual Machine in the enterprise is migrated, all its associated storage is also migrated to AWS. This is an important consideration; as the disk size will directly affect the time take for VM migration.

Use Case 2 – Create Virtual Machines from templates

For users who may not have a completely virtualized infrastructure or are running in a multi-hypervisor environment it is also possible to upload an image into Cisco Prime Network Services Controller and create a template of that image in the public cloud. The template in the cloud can then be used to create Virtual Machines. The Virtual machine attributes such as disk and memory, and network properties such as VLAN and IP address can be

modified during the creation of the Virtual Machine. In this way it is easy to rapidly provision new workloads when there is a requirement.

Use Case 3 – Apply features on Virtual Machine Traffic

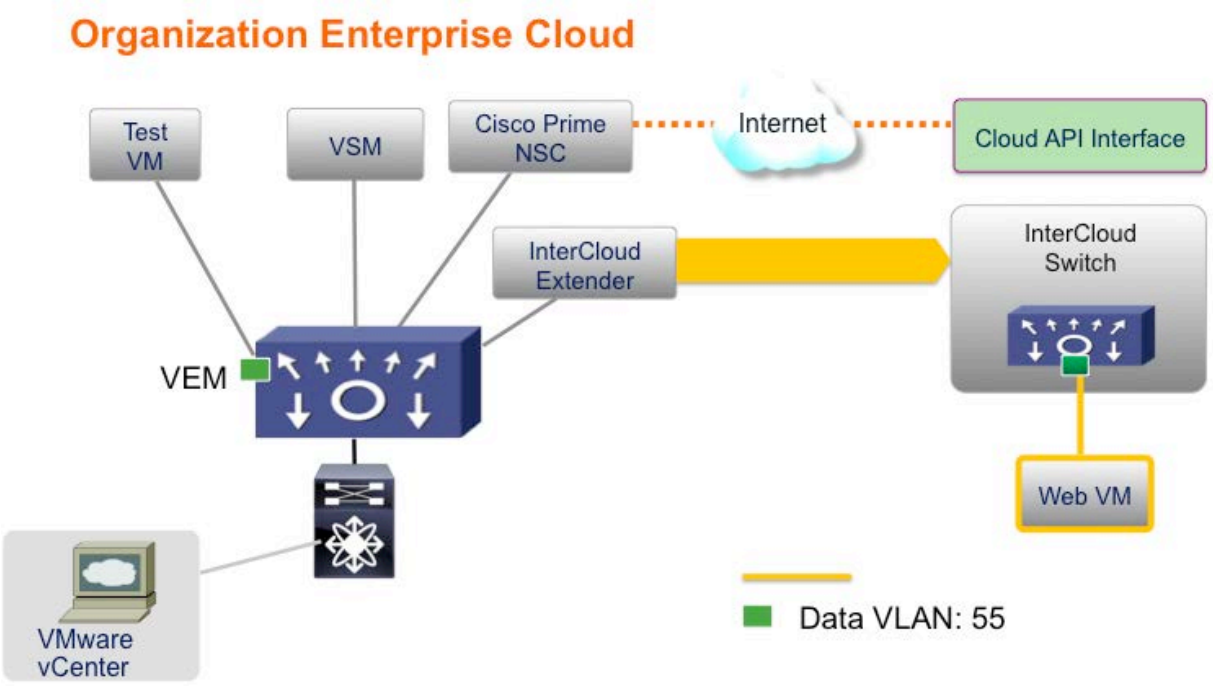
The first release of Nexus 1000V InterCloud includes support for ACL and multicast traffic for Virtual Machines running in the public cloud. These features are configured on the port-profiles in the InterCloud VSM, and applied on the InterCloud Switch.

Deployment Example – Two-tier Web Application

In this use case an organization ABC is trying to migrate a Dev/Test workload to Amazon Web Services. The web server that needs to be tested is going to be moved to AWS and the client machine accessing it will continue to reside in the enterprise data center. The client and web server Virtual Machines are both on VLAN 55 in the enterprise and after migrating the web server it should continue to be on VLAN 55 and accessible at the same IP address as before.

The deployment scenario we are considering is the simple lab deployment scenario in Figure 9, where the management interface is used as the tunnel endpoint and the management VLAN is extended to the public cloud.

Figure 11. Migrating Web Tier in a Two-Tier Web Development vApp



Note: This document does not discuss the installation and basic setup of Cisco Prime Network Services Controller or the Nexus 1000V InterCloud Virtual Supervisor Module (VSM). For details on this please refer to the following installation guides:

Cisco Nexus 1000V InterCloud Installation Guide, Release 5.2(1)IC1(1.1)

Cisco Prime Network Services Controller 3.0 Quick Start Guide

Extending the Network to Cloud

This example assumes the enterprise is running Nexus 1000V as the virtual switch. VMware vSwitch and DVS are also supported but not covered in this document.

Step 1. Configure port-profiles on the enterprise Nexus 1000V for the InterCloud Extender

The InterCloud Extender has three interfaces – management, tunnel and trunk. In this example we will be using the management interface as the tunnel source. Cisco Prime Network Services Manager will configure the management and tunnel interface on the InterCloud Extender VM with the same port-profile, but the tunnel interface is not used. The management VLAN is **252** and the data VLANs being extended are **51 - 60.** Ensure that this VLAN configuration is present on the VSM and upstream switches.

```
port-profile type vethernet ICX-Trunk
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 51-60,252
  no shutdown
  description ICX Trunk port-profile
  state enabled
port-profile type vethernet Access-252
  vmware port-group
  switchport mode access
  switchport access vlan 252
  no shutdown
  description ICX Management port-profile
  state enabled
```

Step 2. Configure port-profiles on the InterCloud VSM

The InterCloud Switch and the Virtual Machines running in the cloud are configured with port-profiles from the InterCloud Nexus 1000V. These are configured as access port-profiles. In addition, the InterCloud VSM is pre-configured with a **N1K_Cloud_Default_Trunk** port-profile. This port-profile needs to be set up to allow the VLANs being extended and with system VLAN configuration for the ICS Management VLAN.

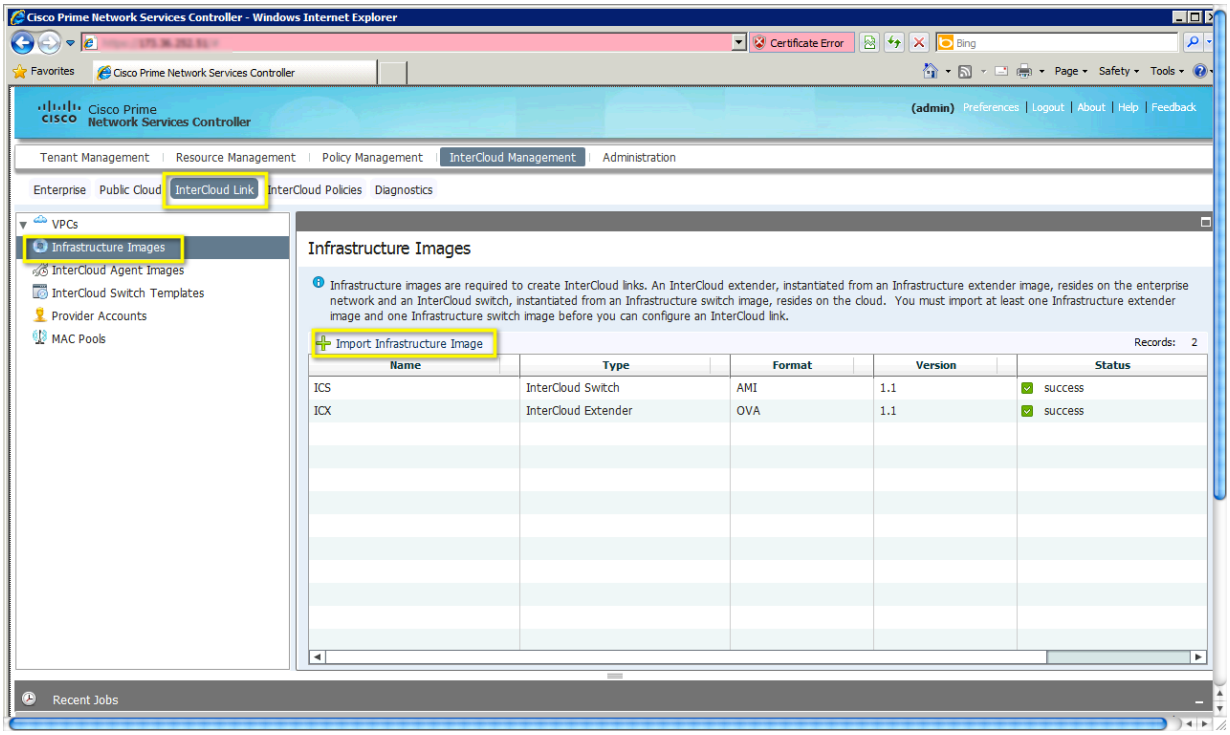
```
port-profile type vethernet N1K_Cloud_Default_Trunk
  switchport mode trunk
  switchport trunk allowed vlan 51-60,252
  no shutdown
  publish port-profile
  max-ports 64
  system vlan 252
  state enabled
port-profile type vethernet ICS-Mgmt
  switchport mode access
```

```
  switchport access vlan 252
  no shutdown
  publish port-profile
  system vlan 252
  state enabled
port-profile type vethernet Cloud-VM-55
  switchport mode access
  switchport access vlan 55
  no shutdown
  publish port-profile
  state enabled
```

Step 3. Upload Infrastructure Images to Cisco Prime Network Services Controller

In order to deploy an InterCloud Link the InterCloud Extender and InterCloud Switch images must be uploaded to Cisco Prime Network Services Controller. Multiple infrastructure images can be uploaded and are distinguished by a configurable version number. During deployment the InterCloud Extender and InterCloud Switch image chosen must have the same version. Clicking on **+Import Infrastructure Image** uploads the Infrastructure images**.**

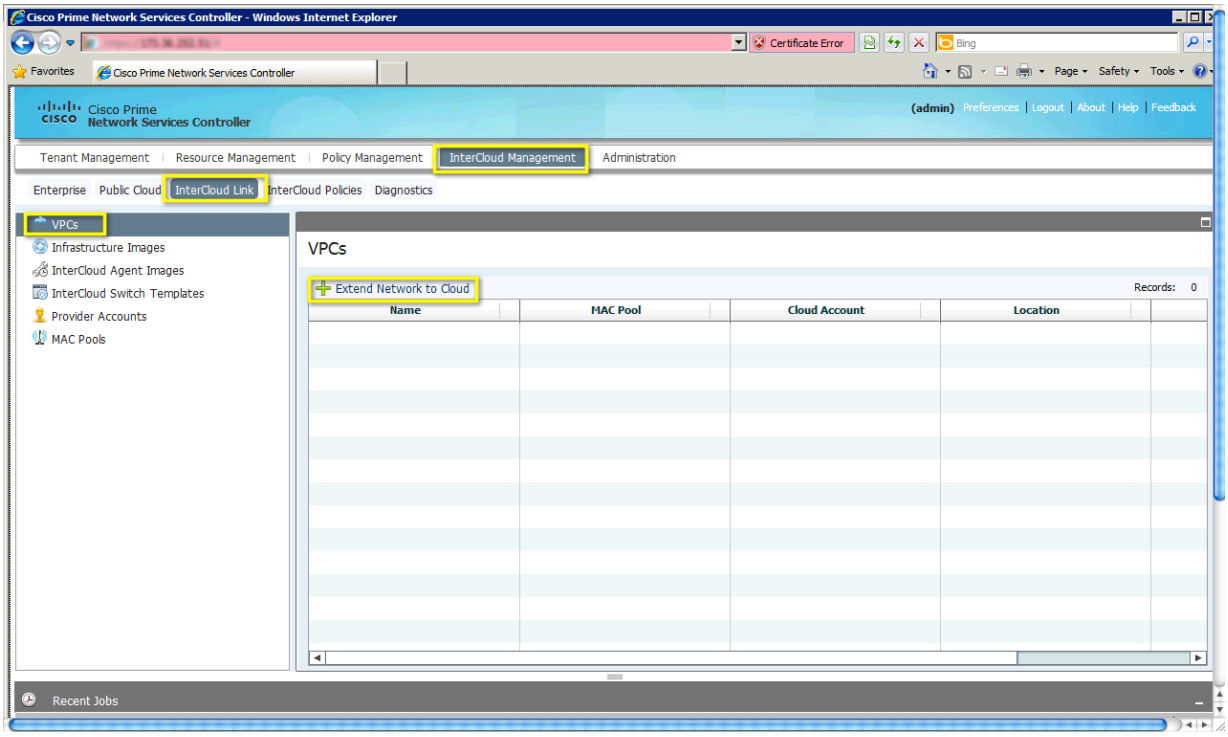
Figure 12. Import Infrastructure Images



Step 4. Extend Network to Cloud

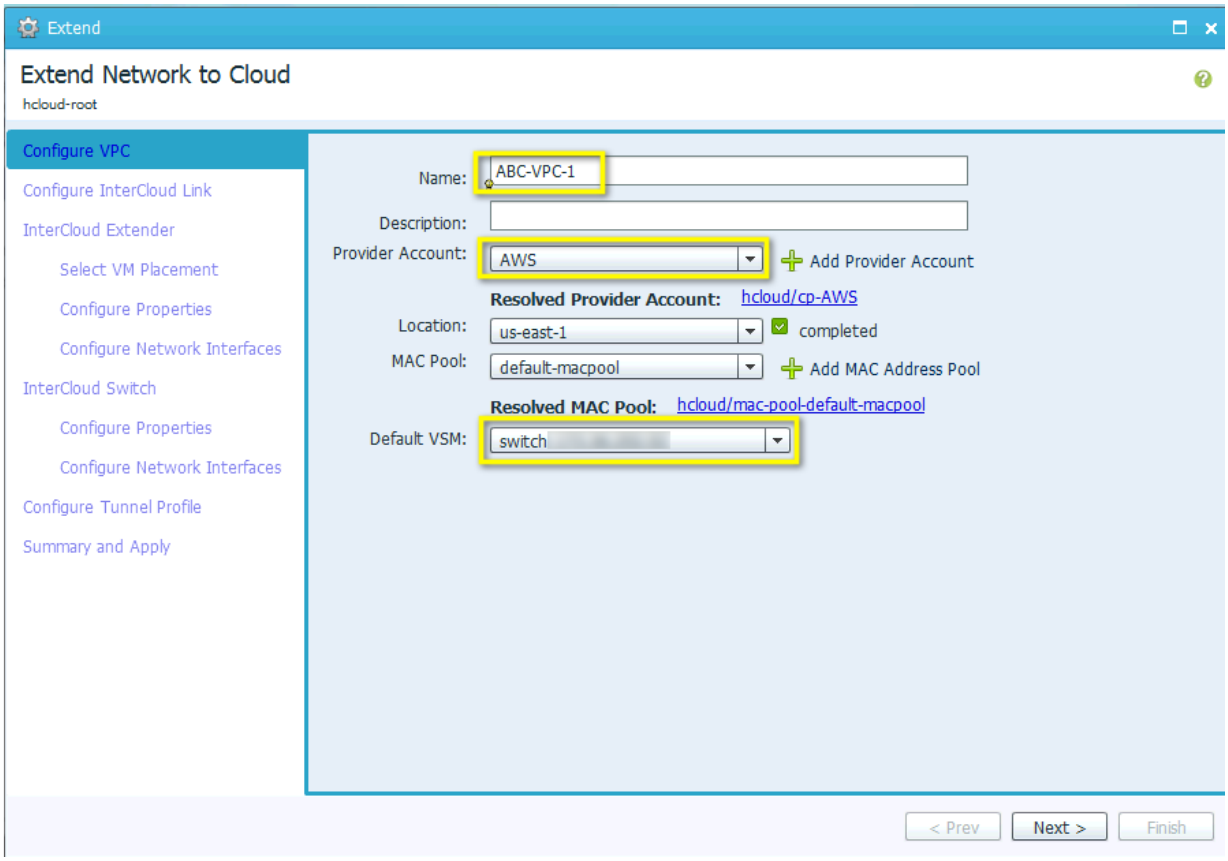
In order to extend network to cloud, navigate to **InterCloud Management > InterCloud Link > VPCs** and click on **+Extend Network to Cloud**. This will open up a dialog box to configure a VPC and InterCloud Link.

Figure 13. Extend Network to Cloud



A dialog box will open to enter the configuration details of the VPC and InterCloud Link

Figure 14. Configure VPC



To configure the VPC, do the following:

a. In the Name field, enter a name for the Virtual Private Cloud

b. In the description field enter an optional description

c. Select an existing provider account from drop down menu or create a new provider account. This example assumes a provider account has been created

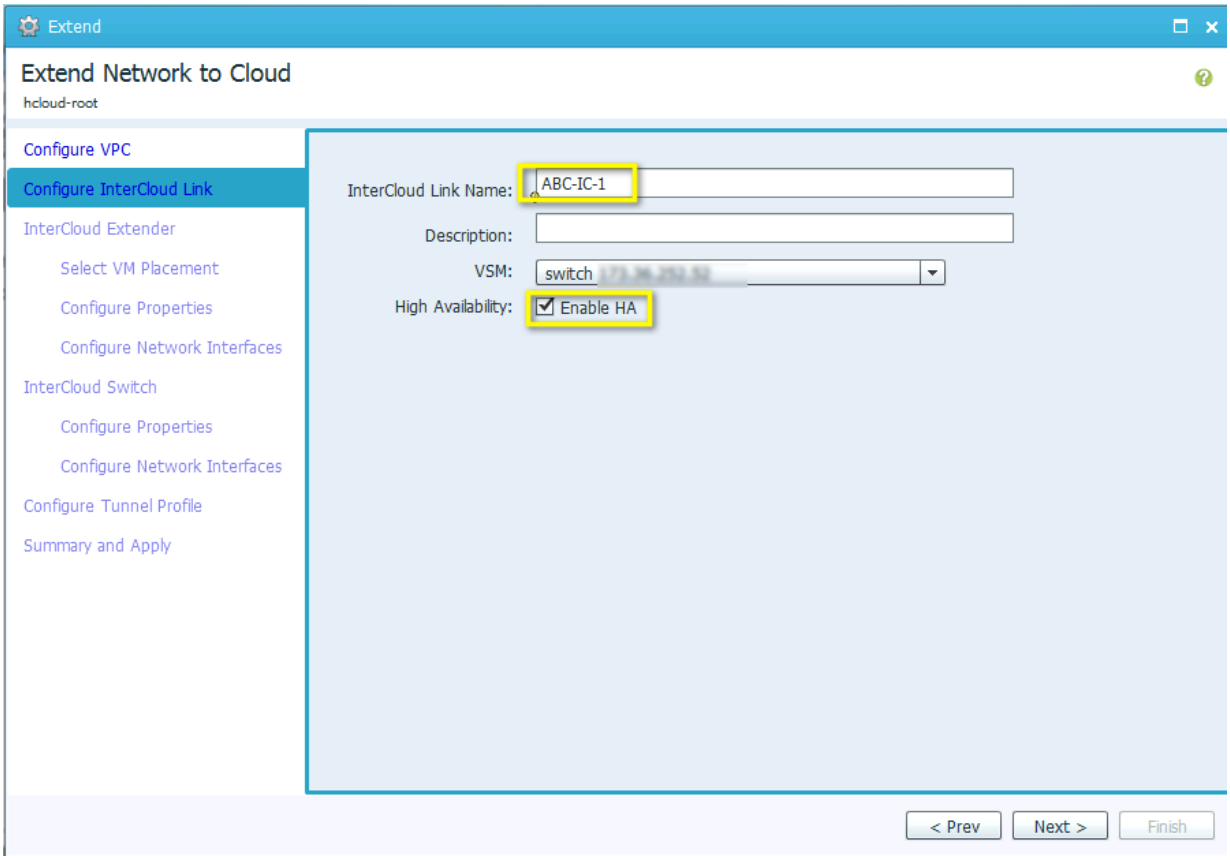
d. Select the region for the VPC. By default the default region for the provider is displayed.

e. Select an existing MAC Pool from drop down menu or create a new MAC Pool. The MAC address for Virtual Machines in the VPC will be assigned MAC addresses from this pool.

f. Select a VSM instance for providing the distributed switch for the VPC.

Click **Next** to add an InterCloud Link.

Figure 15. Configure InterCloud Link



In the **Configure InterCloud Link** screen, do the following:

a. In the Name field, enter a name for the InterCloud Link

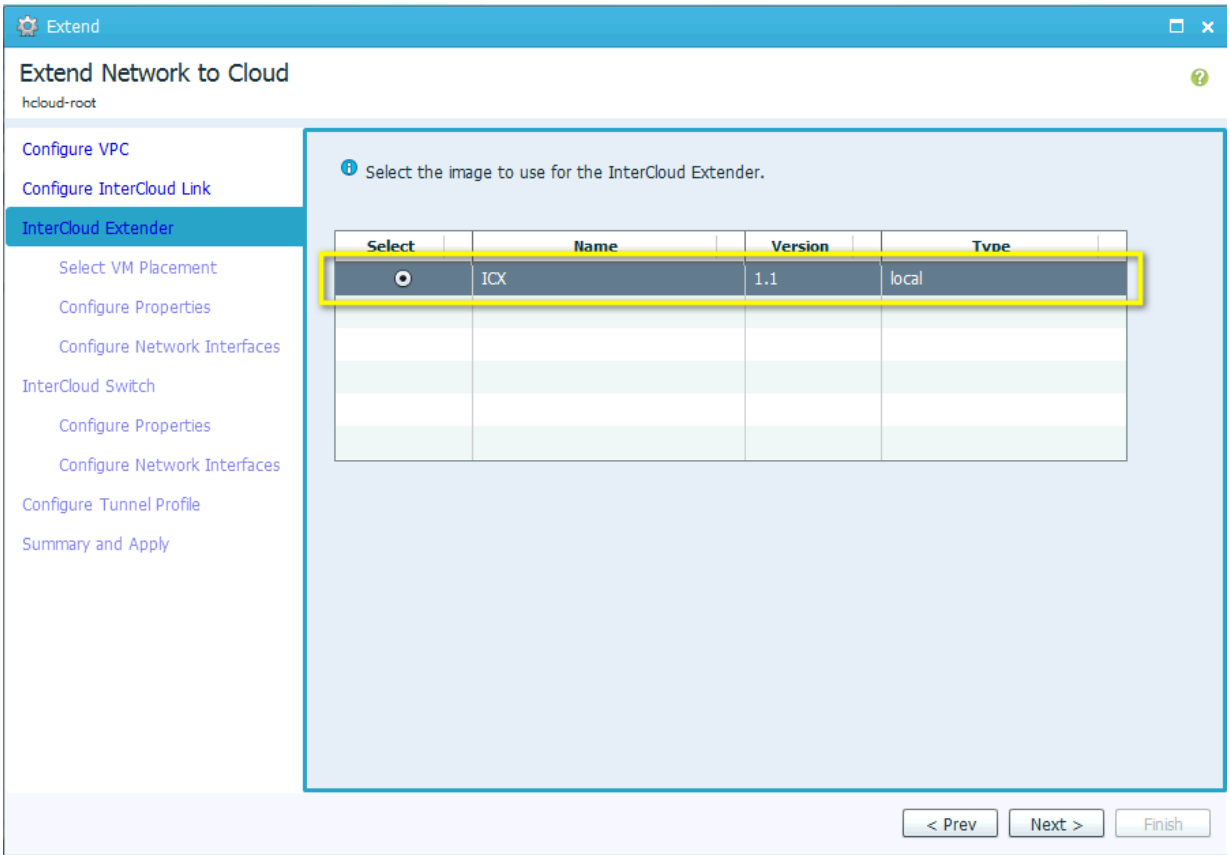
b. In the description field enter an optional description

c. Select a VSM for the InterCloud Link

d. If HA is desired check the box marked **Enable HA.** In this example we will enable HA

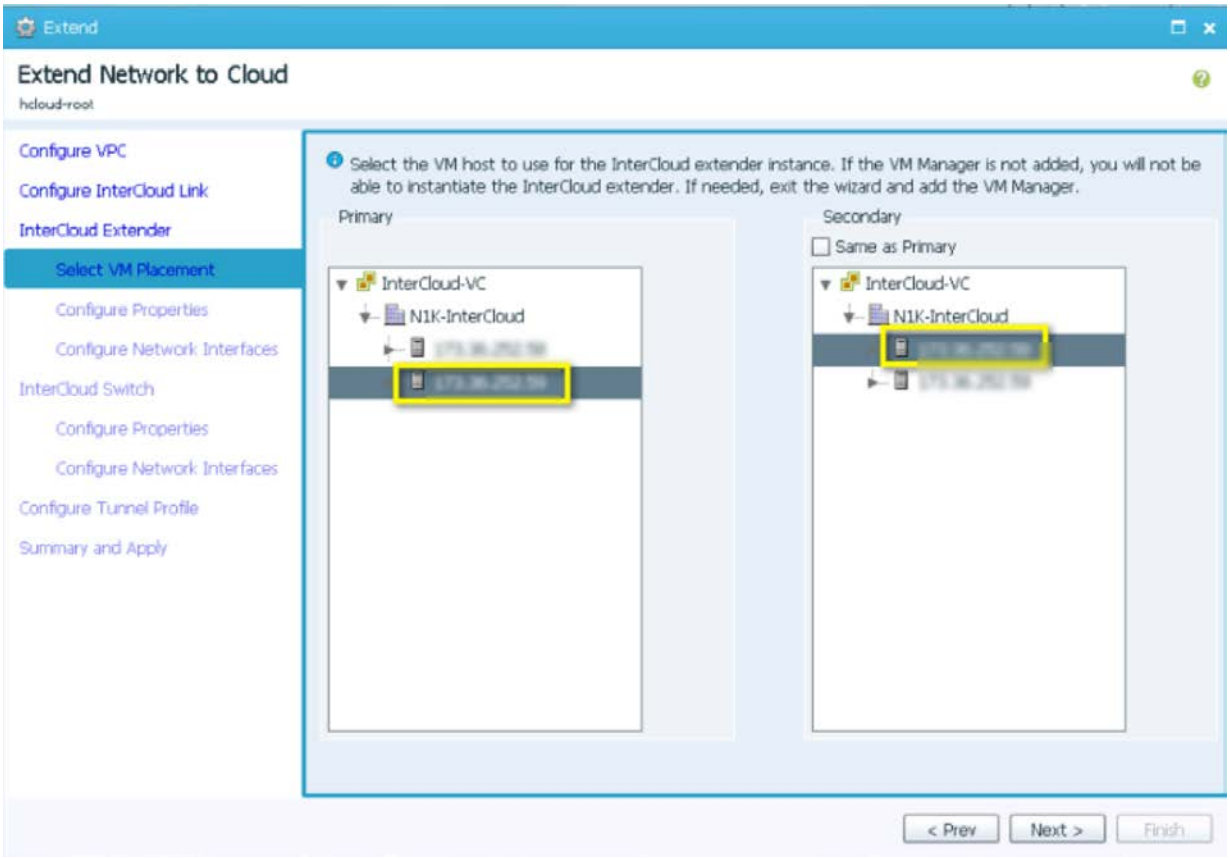
Click **Next**.

Figure 16. Configure InterCloud Extender - Select Image



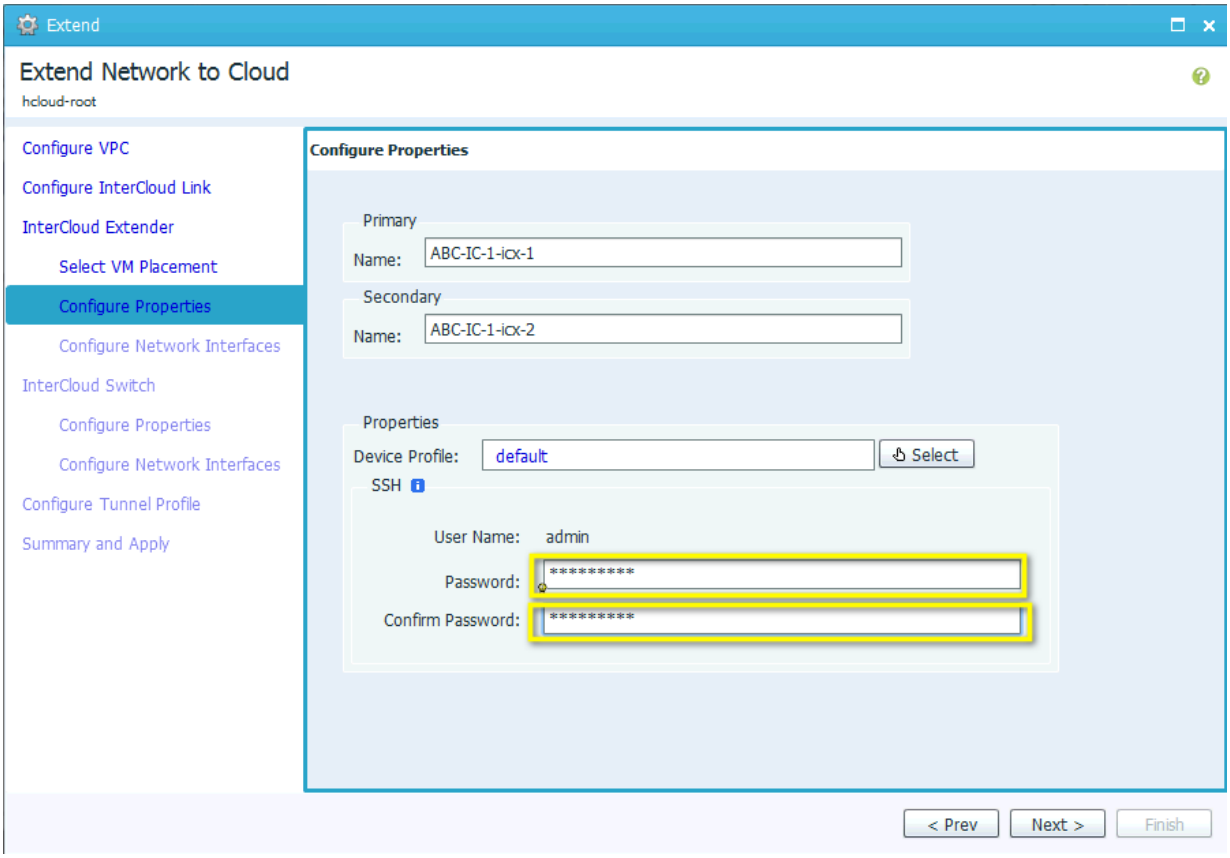
Select an image from the list of Infrastructure images available and click **Next**

Figure 17. Configure InterCloud Extender - Select VM Placement



Select a host from the enterprise vCenter inventory to deploy the primary and secondary InterCloud Extender. It is recommended to select a different host for the secondary, but also possible to select the same host. Click **Next**

Figure 18. Configure InterCloud Extender - Configure Properties



Configure the password for the InterCloud Extender and modify the Device Profile if required. The Device Profile allows a user to configure properties like DNS, NTP and syslog server information for the InterCloud Extender. In addition the log file location can be modified. In this example we use the default Device Profile shown in Figure 20. Click **Next**

Figure 19. Default Device Profile

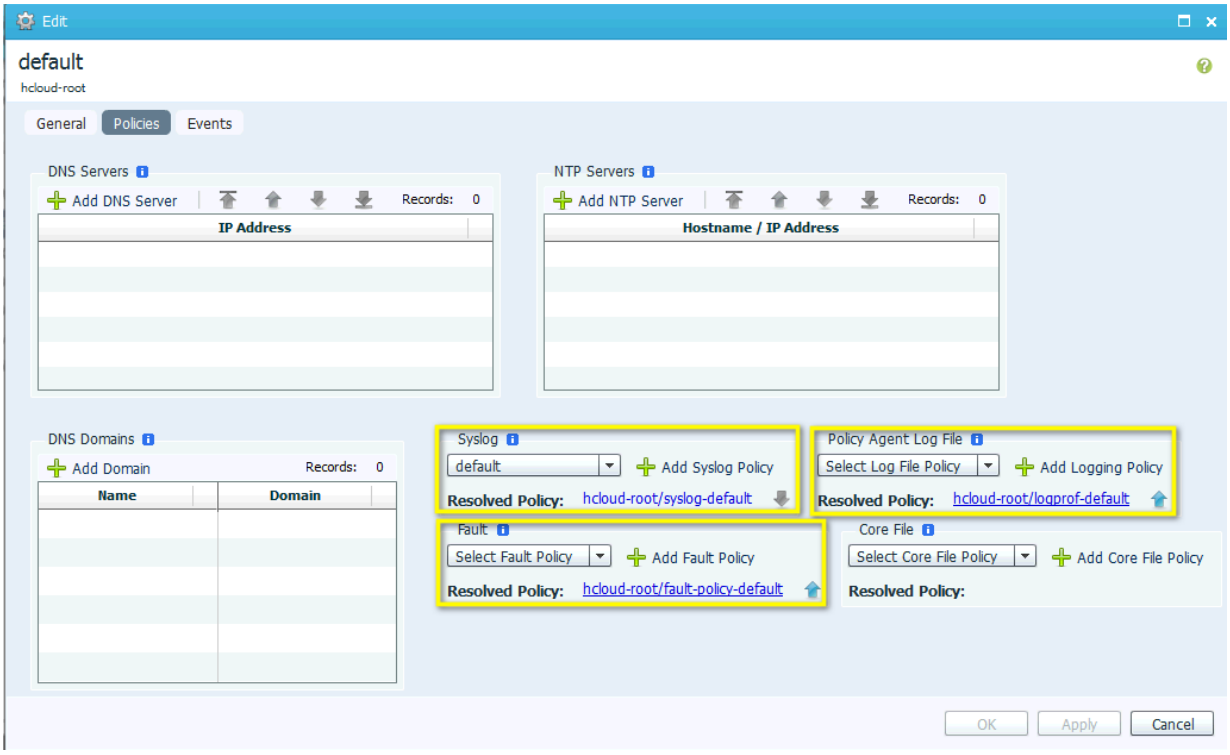
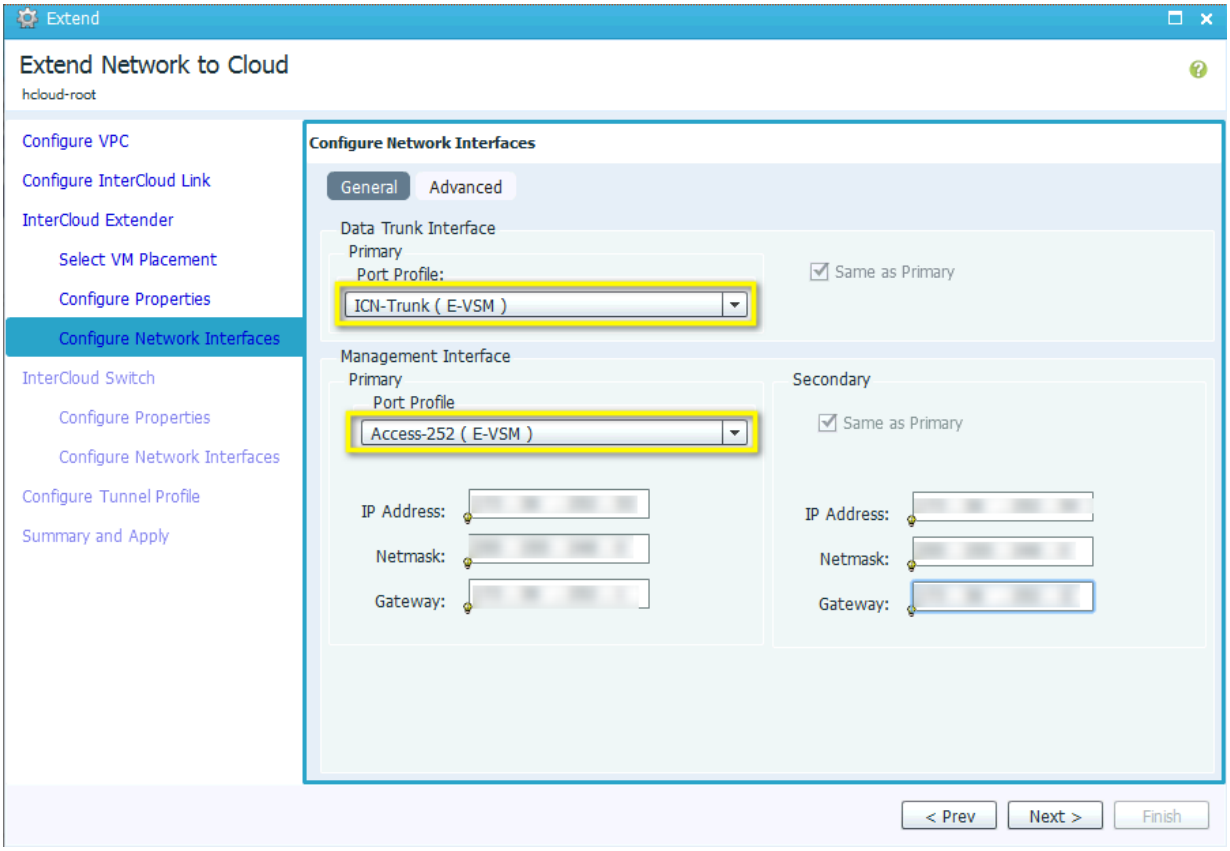


Figure 20. InterCloud Extender - Configure Network Interfaces



In the **Configure Network Interfaces** screen, do the following:

a. Select a port-profile for the Data Trunk interface. The drop-down list is populated with all the port-groups and port-profiles configured for the host selected to deploy the InterCloud Extender in vCenter. In this example we will use the **ICN-Trunk** port-profile configured earlier on the enterprise VSM

b. Select a port-profile for the Management interface. The drop-down list is populated with all the port-groups and port-profiles configured for the host selected to deploy the InterCloud Extender in vCenter In this example we will use the **Access-252** port-profile configured earlier.

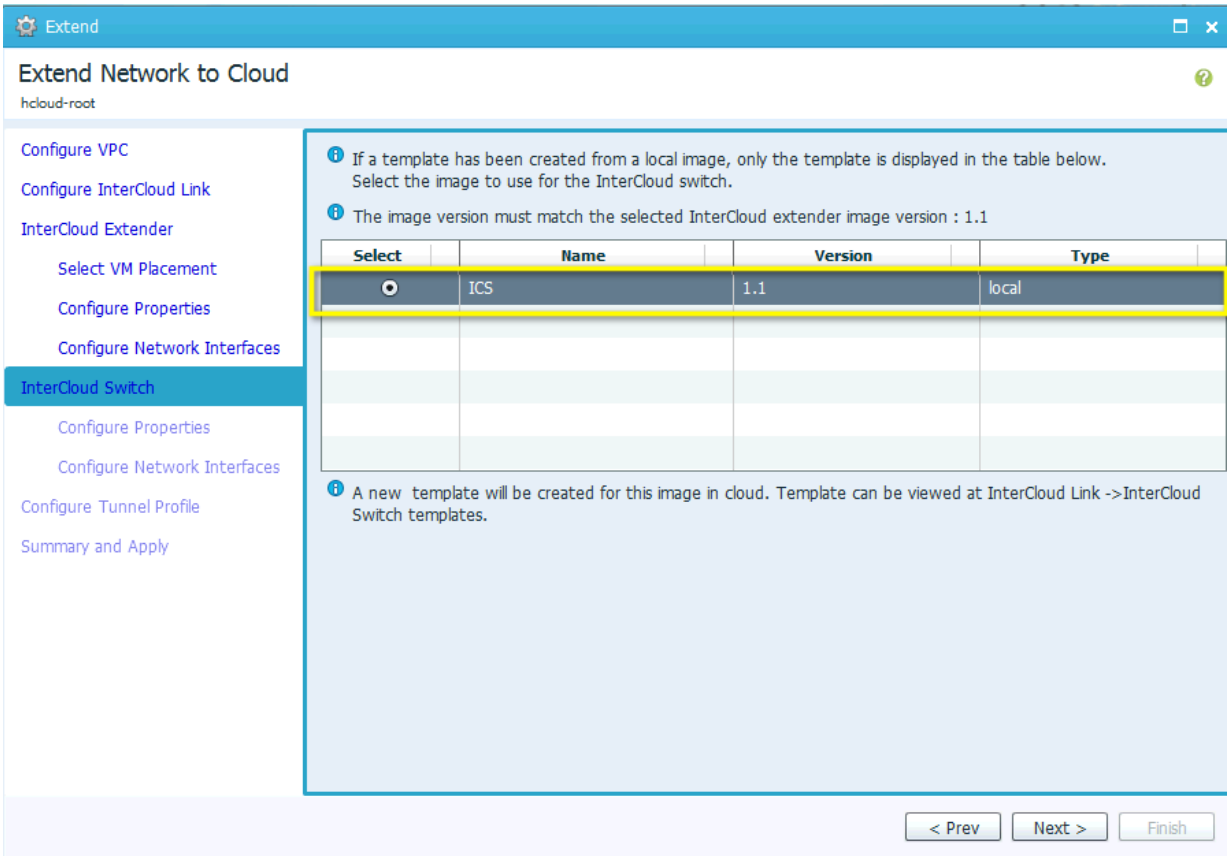
c. If the port-profiles for the secondary are different from the primary, enter this information. In this example we use the same port-profiles for both.

d. If the tunnel interface is going to be used as the tunnel source click on the **Advanced** tab to configure it. In this example we are using the management interface.

e. Configure the IP address, Netmask and Gateway for the primary and secondary InterCloud Extender

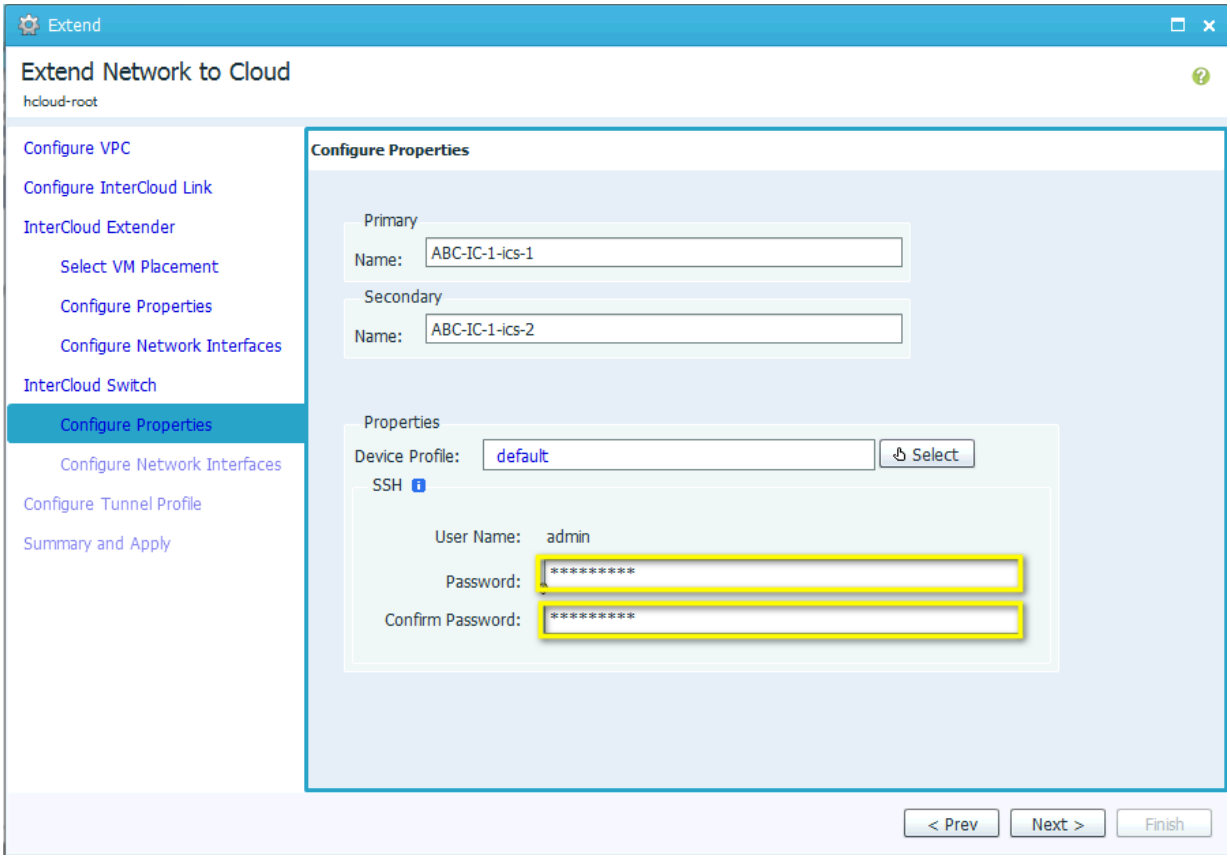
Click **Next**.

Figure 21. Configure InterCloud Switch – Select Image



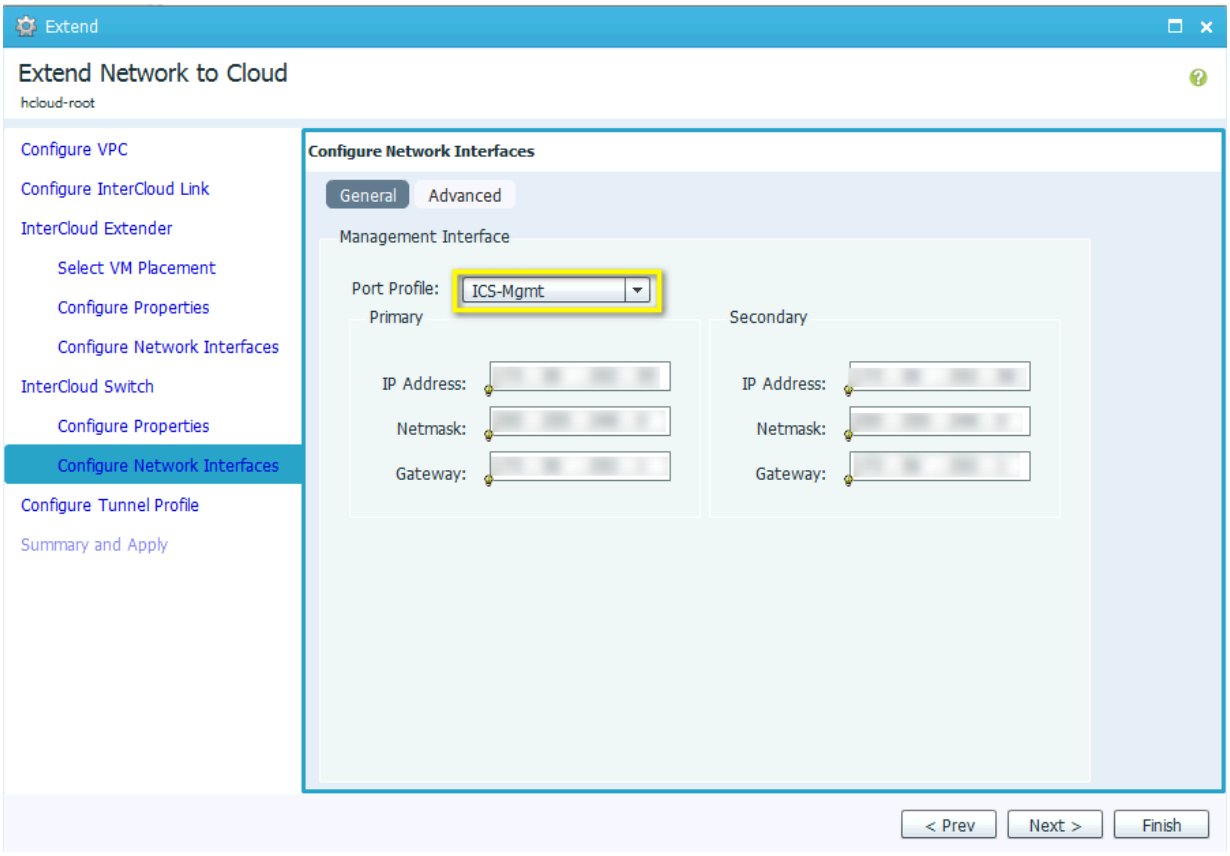
Select an image from the list of Infrastructure images available and click **Next**

Figure 22. Configure InterCloud Switch – Configure Properties



Configure the password for the InterCloud Switch and modify the Device Profile if required. The Device Profile allows a user to configure properties like DNS, NTP and syslog server information for the InterCloud Switch. In addition the log file location can be modified. In this example we use the default Device Profile shown in Figure 20. Click **Next**

Figure 23. InterCloud Switch - Configure Network Interfaces



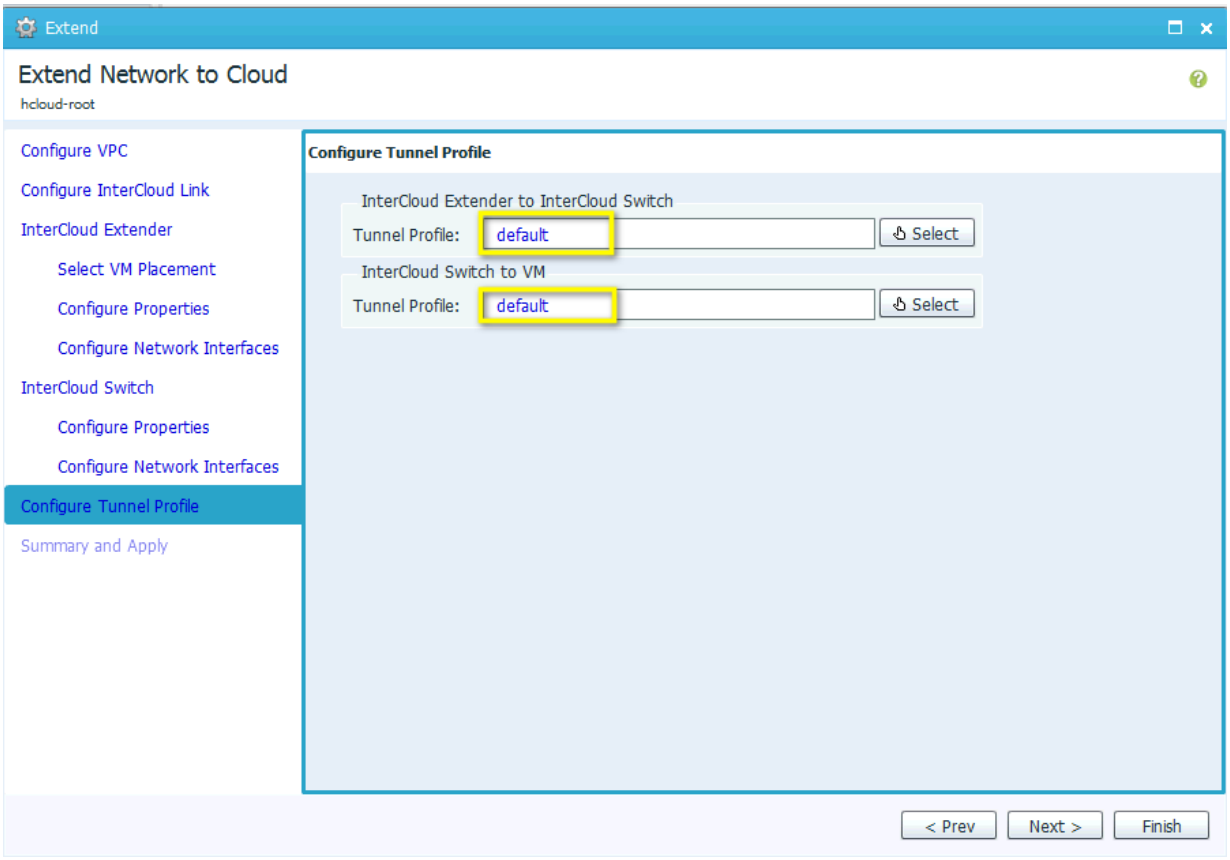
In the **Configure Network Interfaces** screen, do the following:

a. Select a port-profile for the Management interface. The drop-down list is populated with all the port-profiles configured in the InterCloud VSM. In this example we will use the **ICS-Mgmt** port-profile configured earlier.

b. Configure the IP address, Netmask and Gateway for the primary and secondary InterCloud Switch

Click **Next**.

Figure 24. InterCloud Switch - Configure Tunnel Profile



In the **Configure Tunnel Profile** screen, do the following:

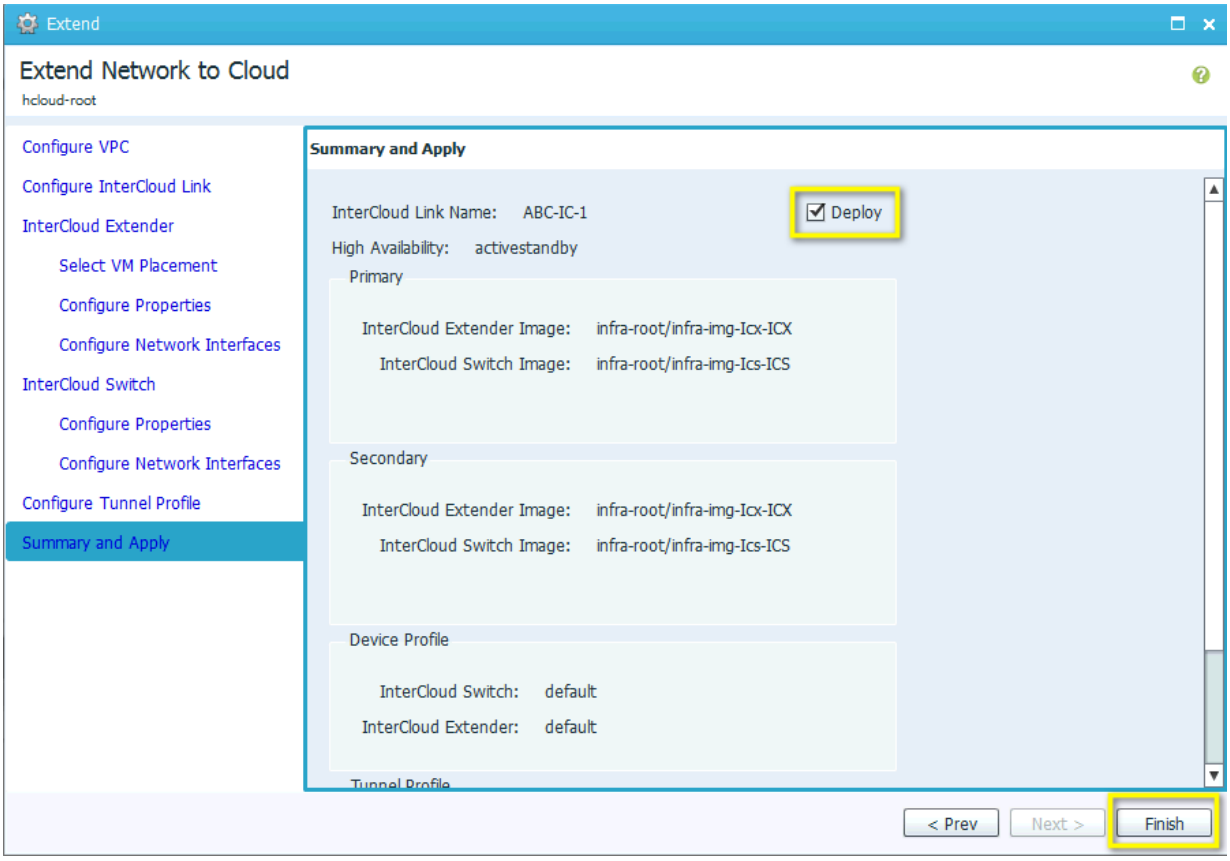
a. In the InterCloud Extender to InterCloud Switch Tunnel Profile field select the default tunnel profile or select a different pre-configured tunnel-profile. This tunnel profile determines the encryption methodology and key parameters for the connection between the InterCloud Extender and InterCloud Switch.

b. In the InterCloud Switch to VM Tunnel Profile field select the default tunnel profile or select a different pre-configured tunnel-profile. This tunnel profile determines the encryption methodology and key parameters for the connection between the InterCloud Switch and the virtual machine in the public cloud.

The default tunnel profile uses AES-128-CBC as the encryption algorithm and SHA-1 as the hash function.

Click **Next**

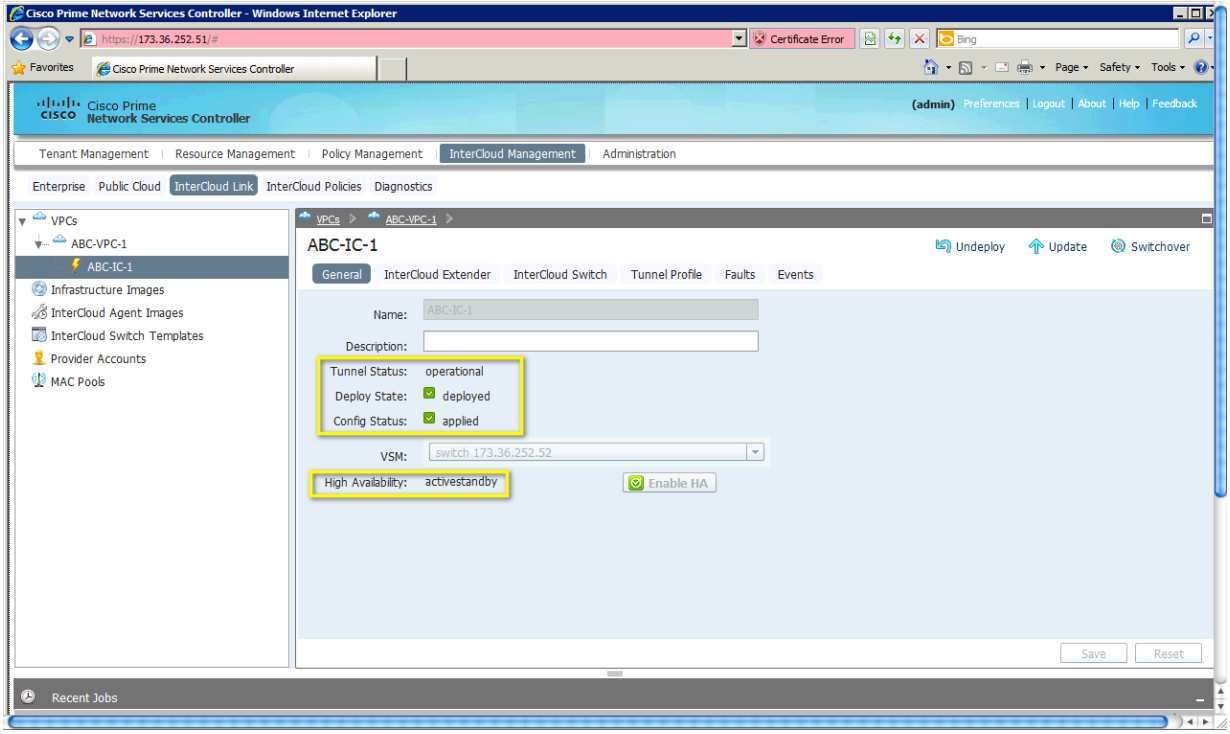
Figure 25. InterCloud Switch – Summary and Apply



Click on **Finish** to deploy the InterCloud Link

Step 5. Verify InterCloud Link

Go to **InterCloud Management > InterCloud Link > VPCs > VPC name > IC Name.** Once the deployment is complete the InterCloud Link will show up as **deployed** with the config state as **applied**. The tunnel status should be **operational** and the HA status will show **activestandby**



The InterCloud Extender and InterCloud Switch images will be registered with the InterCloud VSM as service modules. This can be verified on the VSM using the CLI command:

```
switch# show  module service intercloud
Mod Type                 Name                       Peer Tunnel   IP
--- ------------------ ------------------------  --- -------  ---------------
3   IC Extender        ABC-IC-1-icx-1             6    Up       xxx.xxx.xxx.xxx
4   IC Extender        ABC-IC-1-icx-2             5    Up       xxx.xxx.xxx.xxx
5   IC Switch          ABC-IC-1-ics-2             4    Up       xxx.xxx.xxx.xxx
6   IC Switch          ABC-IC-1-ics-1             3    Up       xxx.xxx.xxx.xxx
switch#
```

The tunnel status can be verified on the InterCloud Extender using the following CLI command:

```
ABC-IC-1-icx-1# show intercloud clink status
ICS:
-------------------------------------------------------------------------------
Name                Peer Ip         Config    Control     Tunnel      Tunnel
                                    State     Connection  Connection  Id
-------------------------------------------------------------------------------
ABC-IC-1-ics-1      54.224.91.81    OK        Up          Up          1
-------------------------------------------------------------------------------
```

If the tunnel is status does not show **Up**, the ports required for communication may not be opened. Use the command **test intercloud ics-reachability**. If all ports are reachable the output is as follows:

```
ABC-IC-1-icx-1# intercloud test ics-reachability
PORT STATE SERVICE REASON
```

```
6644/tcp open ctrl-channel success
6644/udp open data-tunnel success
22/tcp open ssh success
80/tcp open http success
443/tcp open https success
```

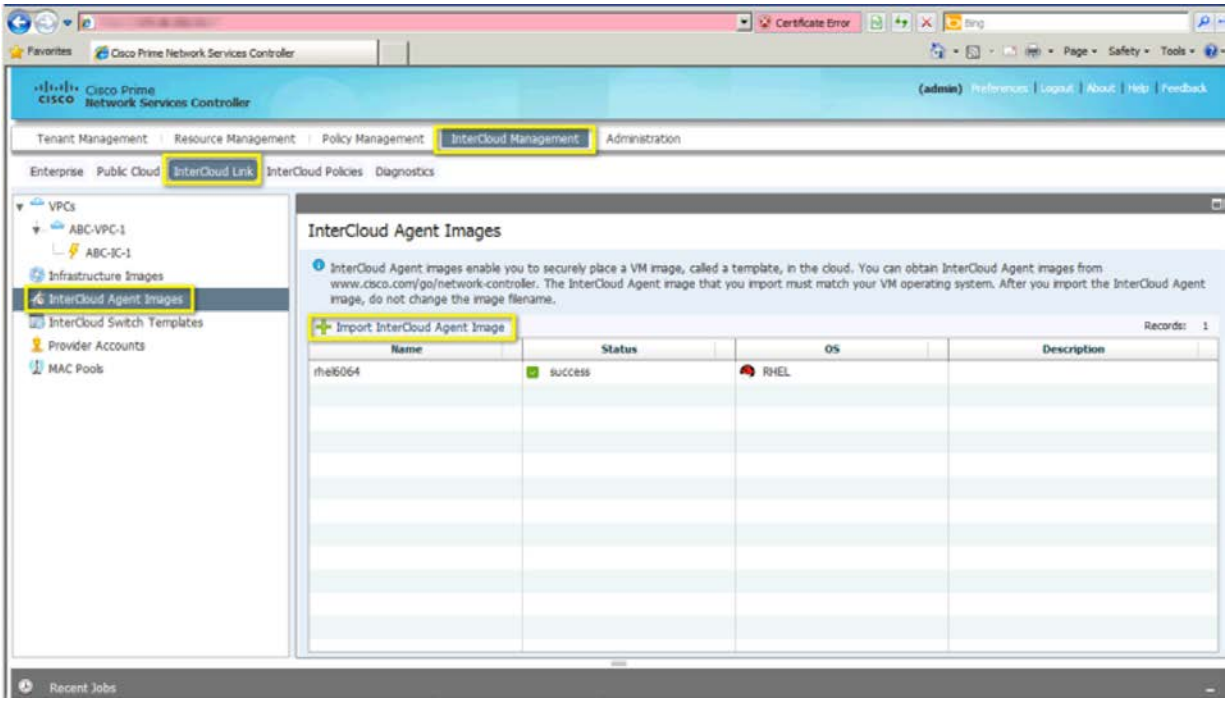
Migrate Web Server to Cloud

The web server and client VM are configured with IP addresses in the 192.168.1.x subnet on VLAN 55 within the enterprise data center. The web server IP address is **192.168.1.5** and the client IP address is **192.168.1.1**. The web server VM is migrated to AWS and retains the same VLAN and IP address configuration.

Step 1. Upload InterCloud Agent Image

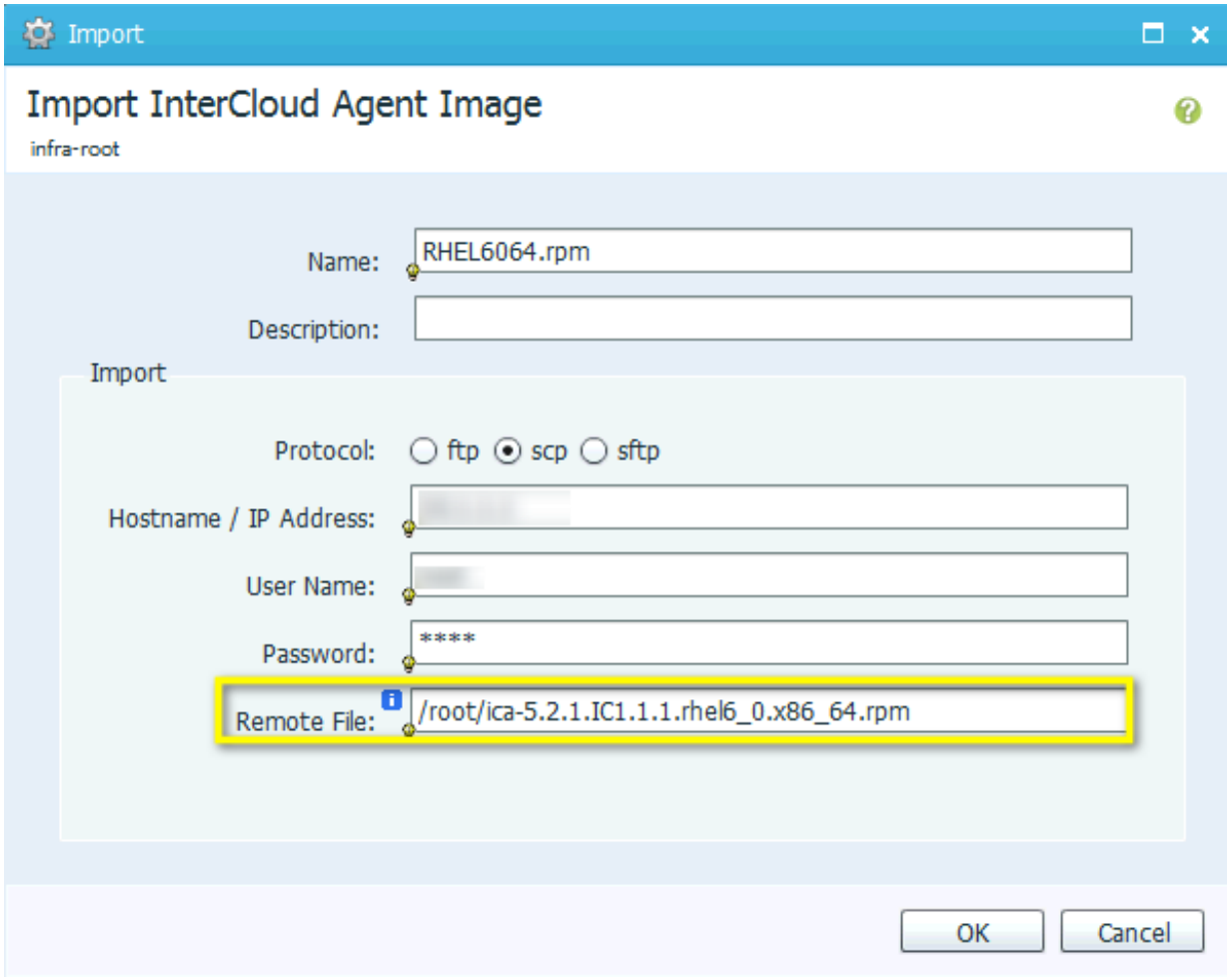
The web server being migrated in this example is running a 64-bit RHEL 6.0 Operating System. The corresponding InterCloud Agent image needs to be uploaded to the Cisco Prime Network Services Controller before we can migrate the VM. Go to **InterCloud Management > InterCloud Link > InterCloud Agent Images** and click on **+Import InterCloud Agent Image**

Figure 26. Import InterCloud Agent Image



This will open up a dialog box to import the image.

Figure 27. Import InterCloud Agent Image Dialog Box



In the Import Driver Image dialog box, do the following:

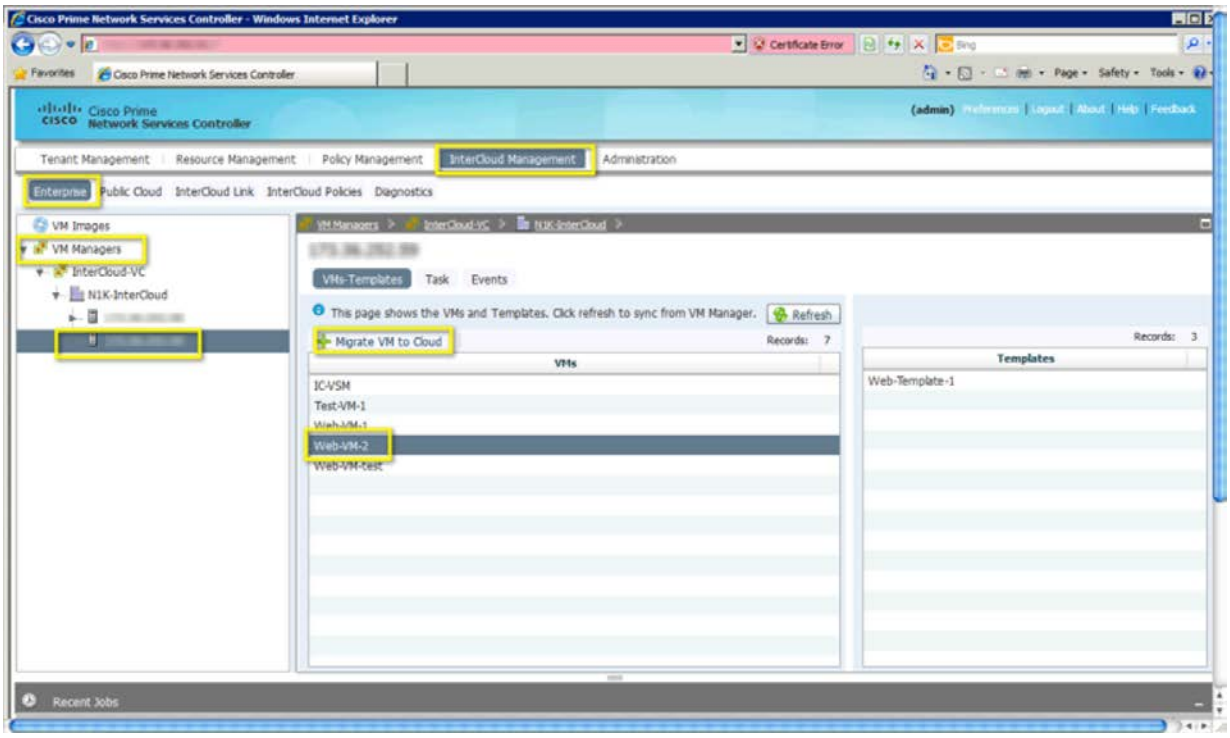
- **a.** In the Name field, enter a name for the image (no spaces allowed).
- **b.** In the description field enter an optional description
- **c.** Select the protocol to use for the file transfer. In this example we are using scp.
- **d.** In the Hostname/IP Address field enter the hostname or IP address for the SCP server
- **e.** In the User Name and Password fields enter the credentials to log in to the server
- **f.** In the Remote File field provide the complete path from the root to the driver image file

Click **OK**.

Step 2. Migrate the Virtual Machine

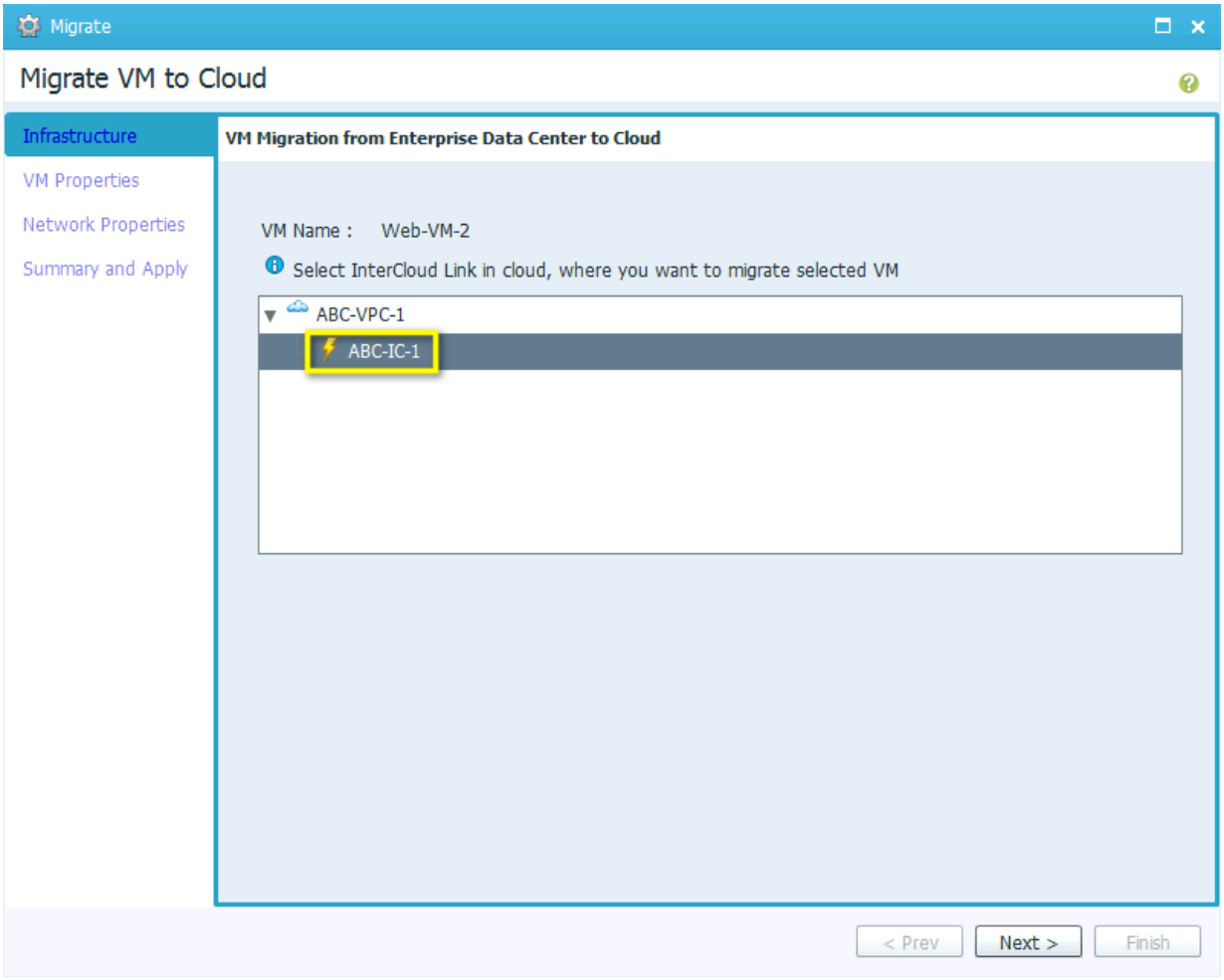
Go to **InterCloud Management > Enterprise > VM Managers > VCenter > Datacenter > Cluster > Host.** Select the Virtual Machine **Web-VM-2.** When the VM is selected **+Migrate VM to Cloud** will appear. Click on this to start the migration.

Figure 28. Select VM to Migrate



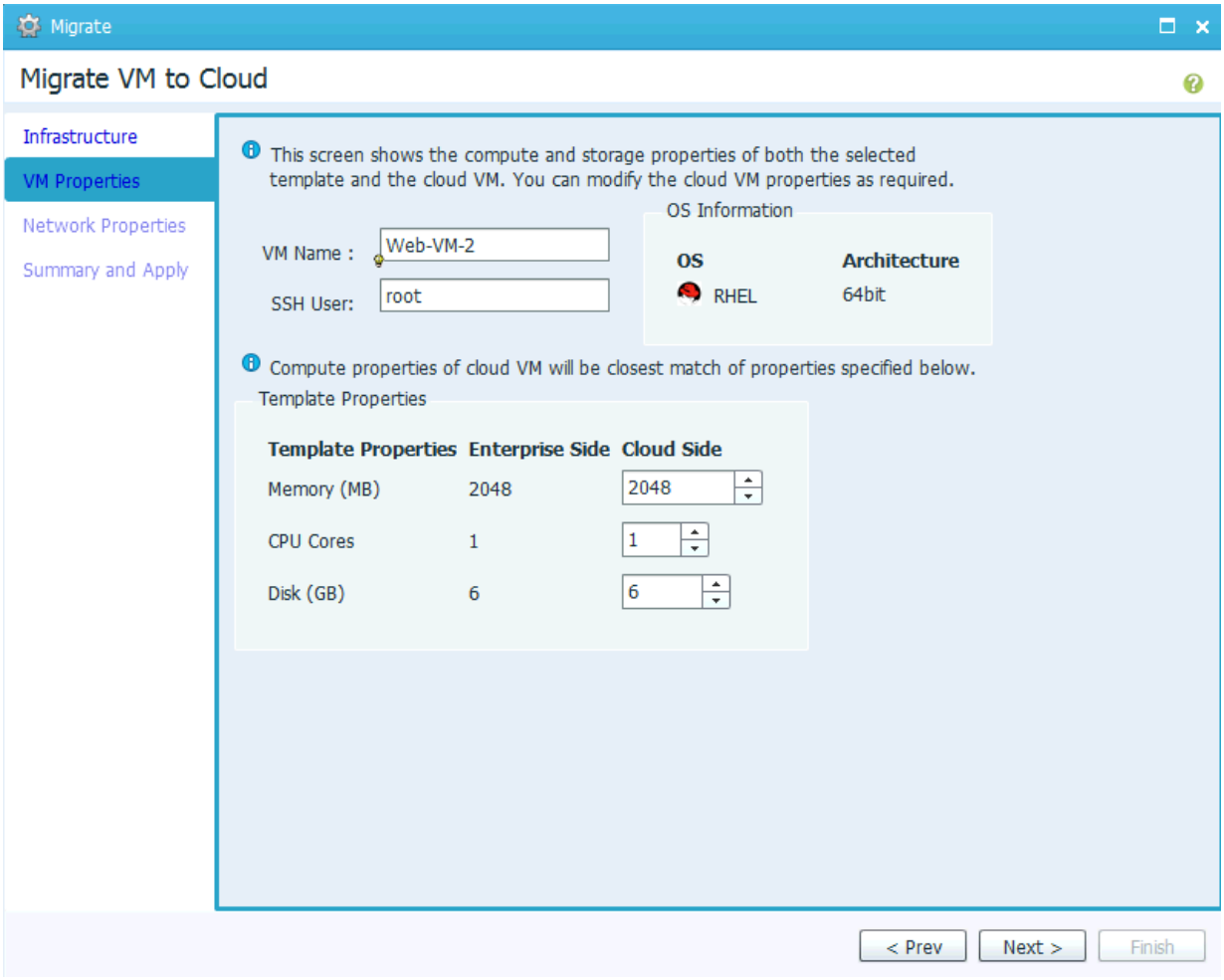
This will open up the dialog box for VM Migration.

Figure 29. Migrate VM – Select VPC and InterCloud Link



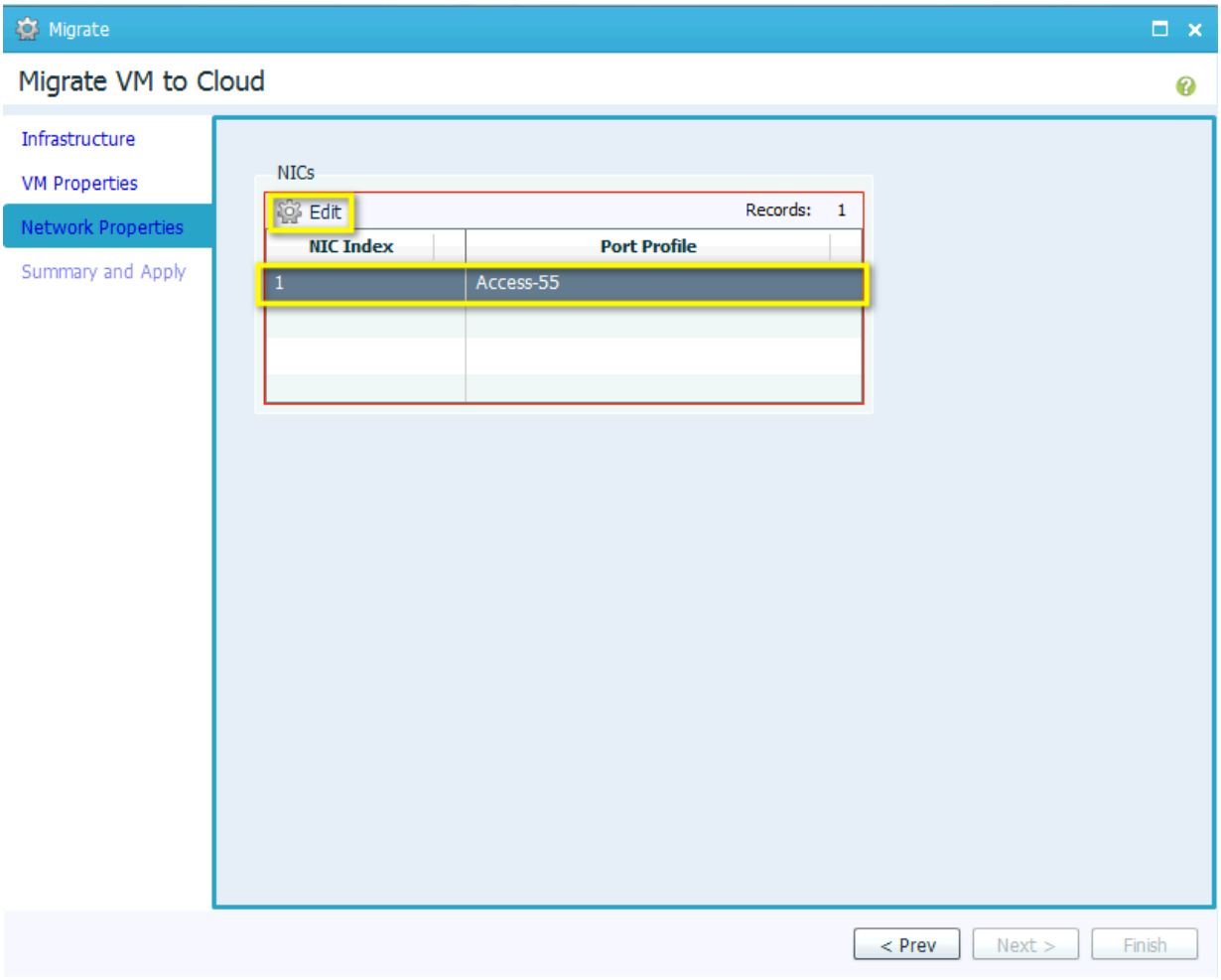
Select the VPC and InterCloud Link where the VM will be migrated. Click **Next**

Figure 30. Migrate VM – VM Properties



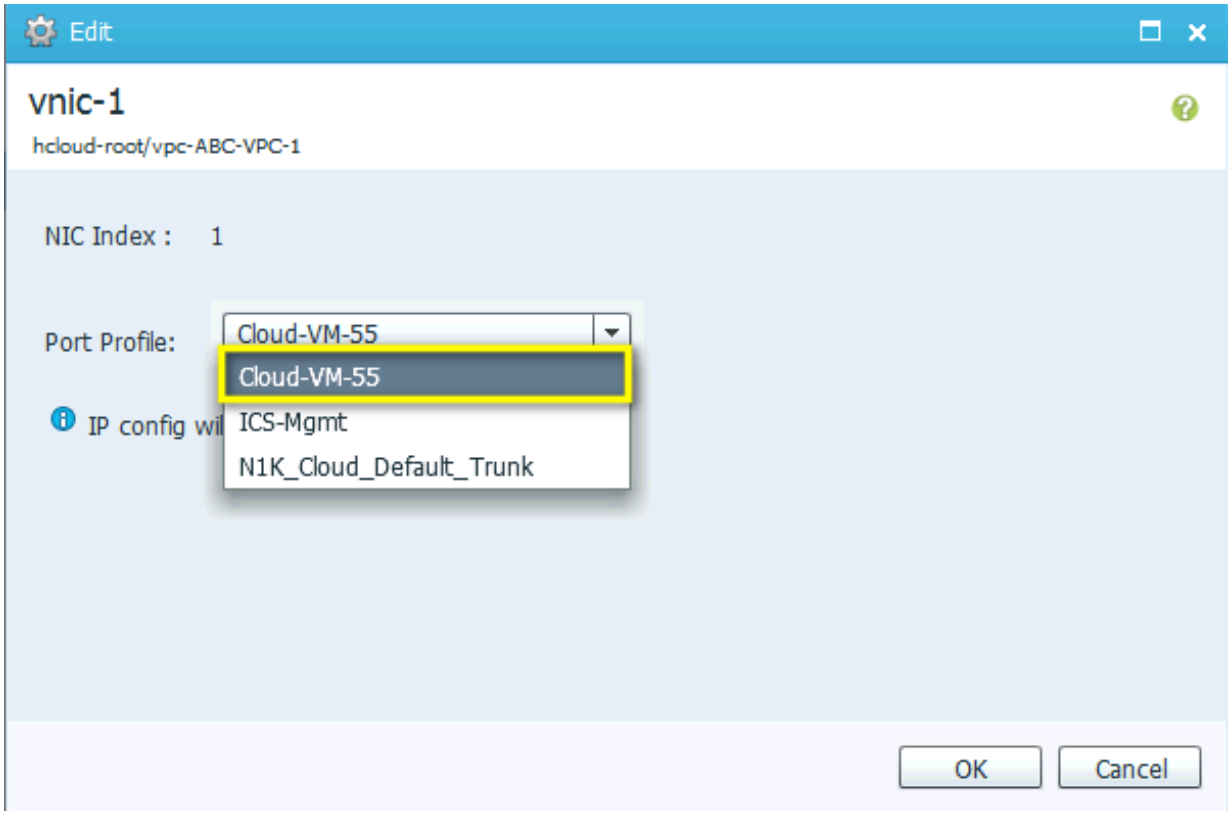
Change the VM properties if desired and click **Next.** Note that the time for migration will depend on the size of the disk being migrated and the latency of the link between the provider and enterprise cloud.

Figure 31. Migrate VM – Network Properties



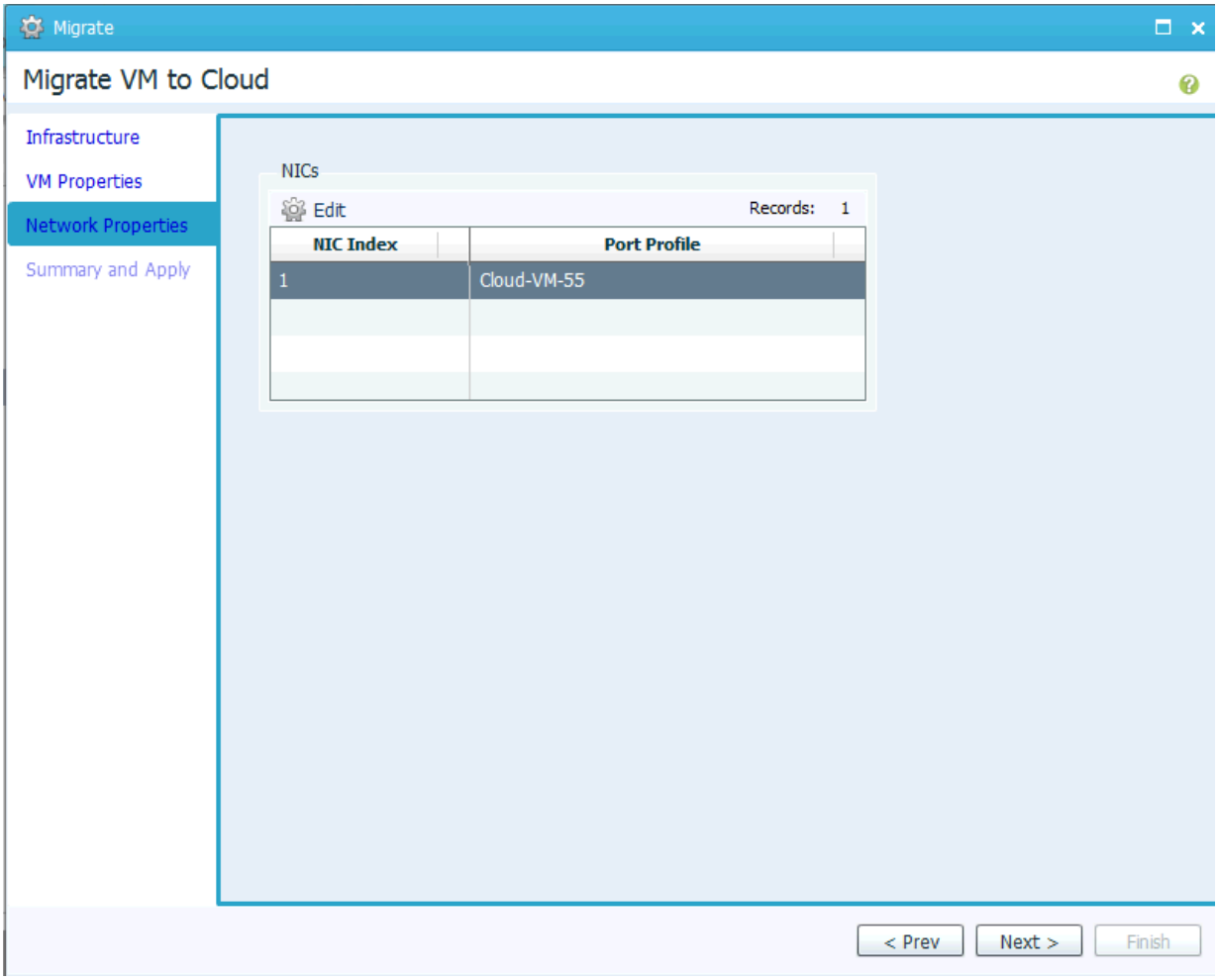
In the **Network Properties** select the NIC and click Edit to edit the Networking properties. This will bring up the Edit window. If the VM has multiple NICs, edit each NIC and configure networking properties.

Figure 32. Migrate VM – Edit Network Properties



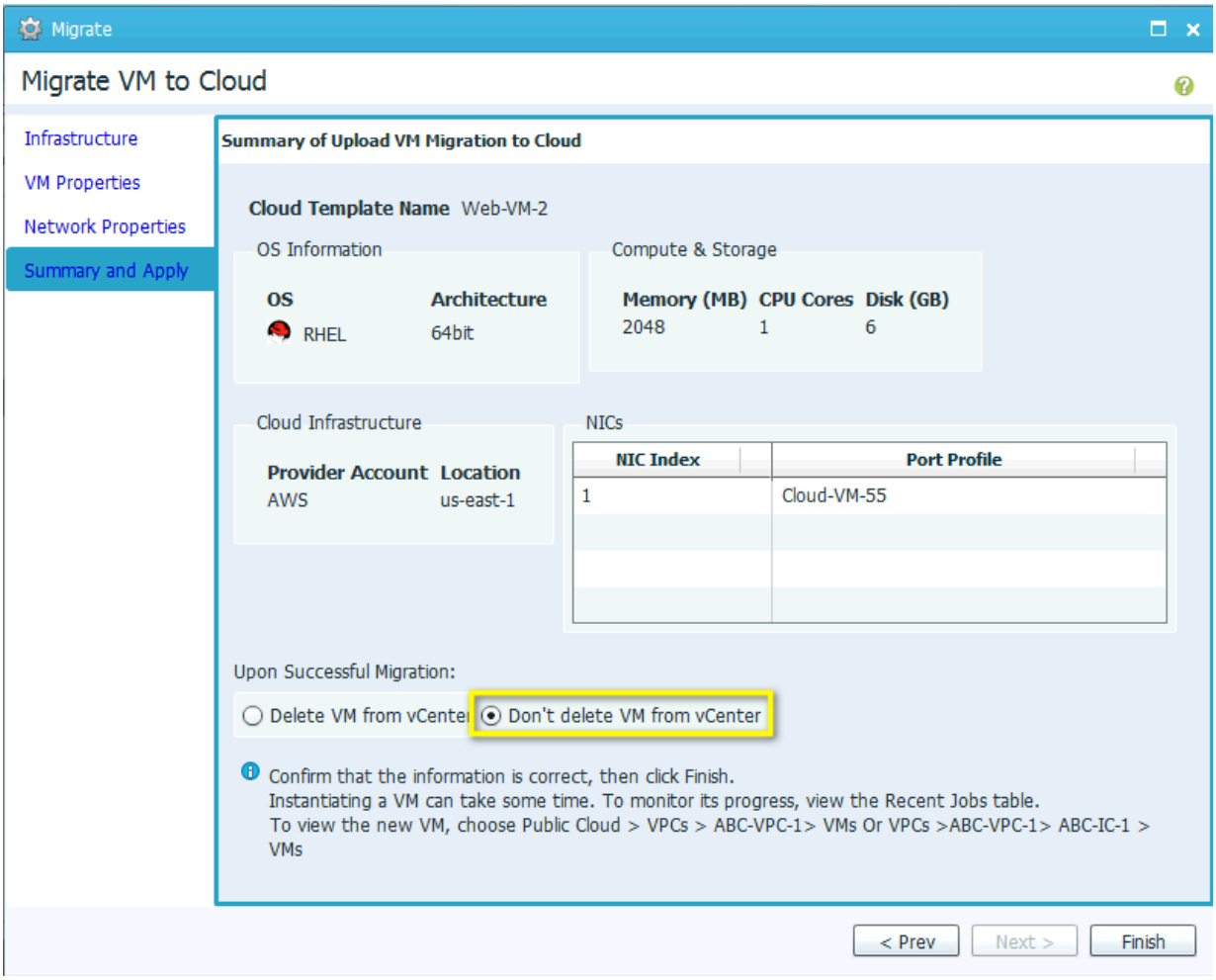
Select the port-profile from the drop-down list. The web server needs to be on VLAN 55 in this example and the port-profile used will be **Cloud-VM-55**. Click **OK**. The IP address configuration will be derived from the Virtual Machine configuration.

Figure 33. Migrate VM – Accept Network Properties



Click **Next.**

Figure 34. Migrate VM – Summary and Apply



In this example we will not delete the VM from vCenter. Click **Finish** to start the Migration.

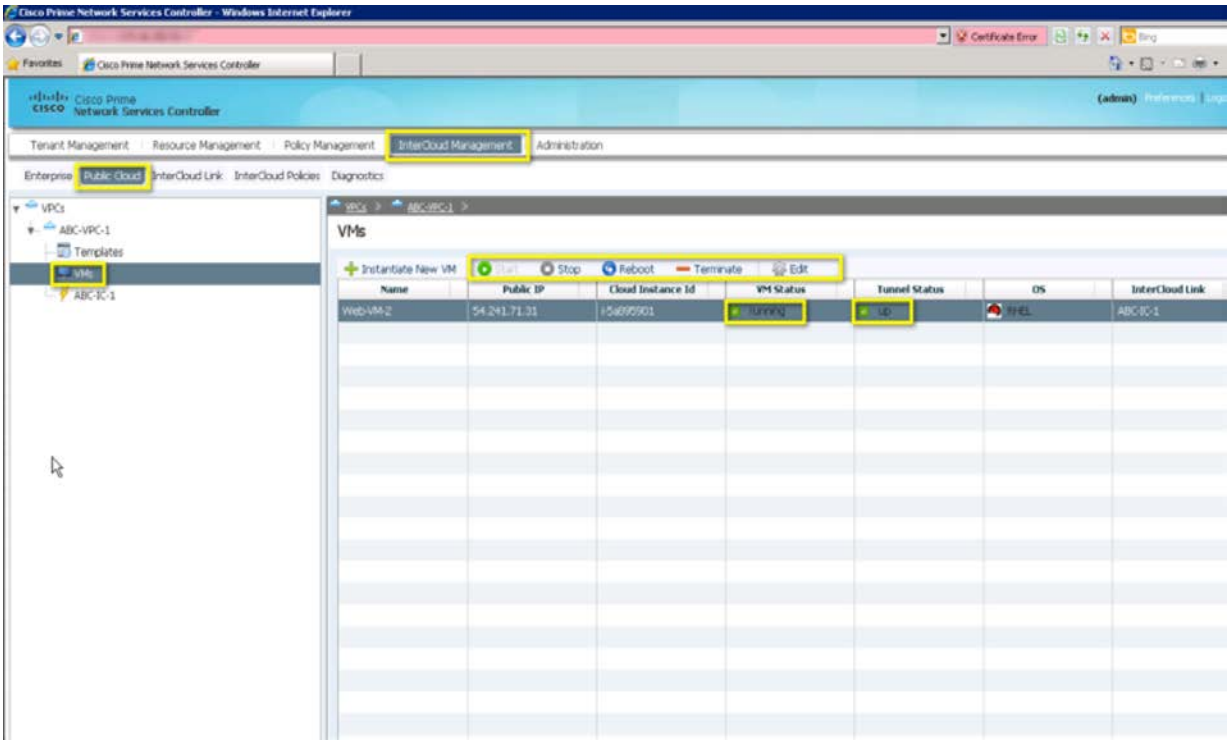
Verifying traffic between client VM and Web Server in cloud

When the Virtual Machine is migrated it can be viewed by going to **InterCloud Management > Public Cloud > VMs**

Step 1. Verify the VM is present in the public cloud

The Virtual Machine once migrated will be running in the public cloud. It can be stopped, rebooted, terminated and configured from the Cisco Prime Network Controller.

Figure 35. View VM in Public Cloud



Step 2. Verify the Virtual Machine is assigned a vEthernet interface on the VSM

The following CLI command will show the vEthernet interface assigned to the web server in the cloud:

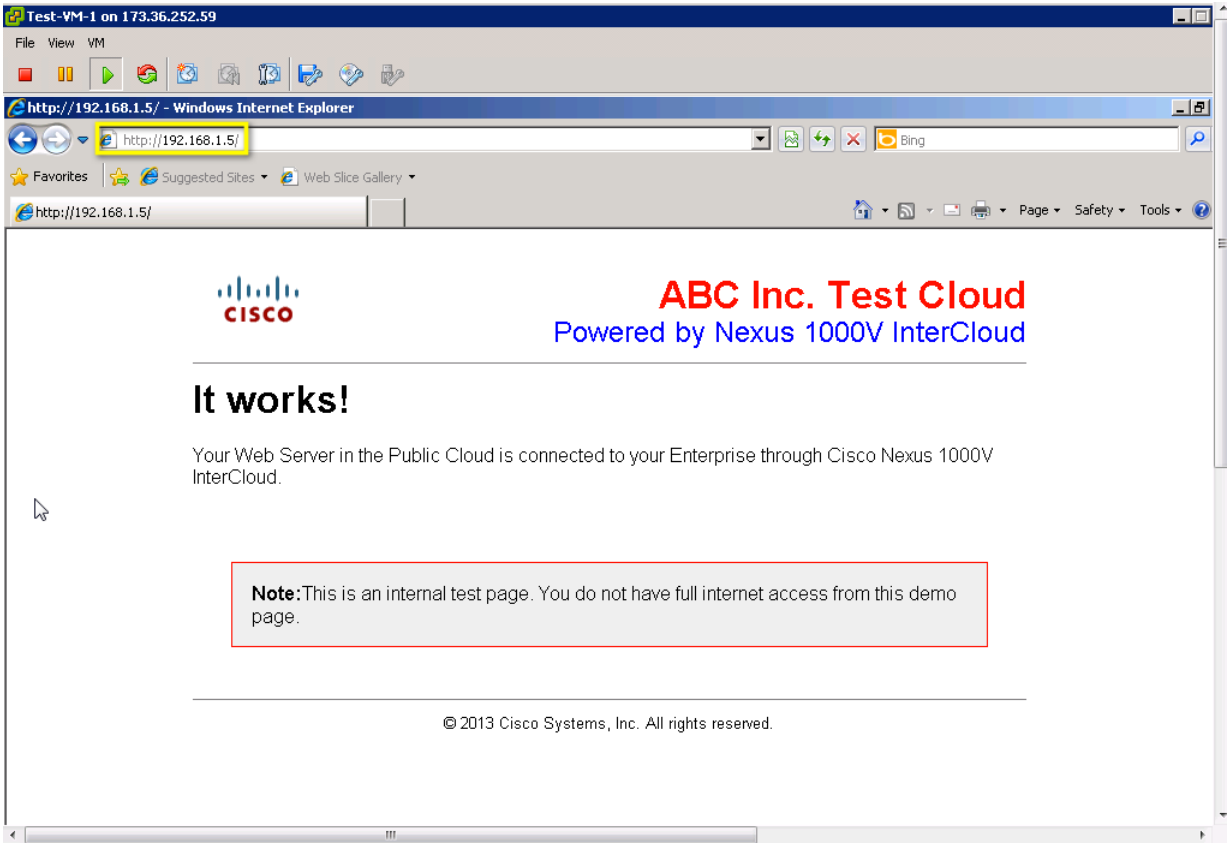
```
switch# show inter virtual

------------------------------------------------------------------------------
Port        Adapter        Owner                     Mod Host
------------------------------------------------------------------------------
Veth1       eth2                                     4   ABC-IC-1-icx-2
Veth2       eth2                                     3   ABC-IC-1-icx-1
Veth4       veth1-0                                  5   ABC-IC-1-ics-2
Veth5       eth1                                     5   ABC-IC-1-ics-2
Veth7       veth1-0                                  6   ABC-IC-1-ics-1
Veth8       eth1                                     6   ABC-IC-1-ics-1
Veth9       veth2-0        Web-VM-2                  6   ABC-IC-1-ics-1
```

Step 3. Verify Web Server Connectivity

From the console of the client Virtual Machine try to access the web page using the address **192.168.1.5.** If the web server was migrated successfully the web page should be displayed.

Figure 36. Web Server Connectivity



Conclusion

Nexus 1000V InterCloud is used to securely extend an enterprise data center to a provider public cloud. By implementing Nexus 1000V InterCloud an organization can run enterprise applications and services in a public shared provider environment without having to re-architect applications, services or security policies. A secure Layer 2 extension connects the Virtual Machines in the cloud to the enterprise Virtual Machines, and the Cisco Prime Network Services Controller provides a single point of management for setting up the extension and managing applications that are migrated to the public cloud.

This guide covered the features and capabilities of Nexus 1000V InterCloud. We saw some options for configuring the enterprise network to prepare for InterCloud deployment and some best practices for extending the enterprise network. We also demonstrated how to deploy Nexus 1000V InterCloud to address a simple Dev/Test use case involving a 2-tier web application.

Glossary

Cisco Prime Network Services Controller

The Cisco Prime Network Services Controller is used to configure and manage Nexus 1000V InterCloud. The Prime Network Services Controller interfaces with the Virtual Machine Manager on the enterprise and provider APIs to provide a single pane of glass for all Virtual Machines that are part of the InterCloud solution.

VPC

A VPC refers to a Virtual Private Cloud. This is a logical container for InterCloud Links that represents a secure and isolated private cloud within the provider environment. A VPC is restricted to a single region within AWS.

InterCloud Link

The InterCloud Link refers to the InterCloud Extender and InterCloud Switch and the secure extension between them. A VPC within InterCloud can have up to 4 InterCloud Links configured in it. Each InterCloud Link is configured with it's own encryption keys.

InterCloud Extender

The InterCloud Extender is a Virtual Machine that is part of the base InterCloud Infrastructure. It is instantiated automatically by the Cisco Prime Network Services Controller in the enterprise vCenter when an InterCloud Link is created. It provides extension capabilities and is the secure tunnel endpoint on the enterprise.

InterCloud Switch

The InterCloud Agent is a Virtual Machine that is part of the base InterCloud Infrastructure. It is instantiated automatically by the Cisco Prime Network Services Controller in the provider cloud when an InterCloud Link is created. It provides secure switching for Virtual Machines in the cloud and is the secure tunnel endpoint on the provider side.

InterCloud Agent

The InterCloud Agent provides secure encryption capabilities and multi-NIC support for Virtual Machines running in the provider cloud. Cisco Prime Network Services Controller inserts it automatically before instantiating a VM in the cloud.

Nexus 1000V Series Switches

Cisco Nexus 1000V Series VSM The Cisco Nexus 1000V Series VSM controls multiple VEMs as one logical modular switch. Instead of physical line-card modules, the VSM supports multiple VEMs running in software inside the physical servers

Cisco Nexus 1000V Series Virtual Ethernet Module

The Cisco Nexus 1000V Series VEM runs as part of the VMware ESX or ESXi kernel and replaces the VMware virtual switch feature

For More Information

For more information about the Cisco Nexus 1000V Series, please refer to the following URLs:

- Cisco Nexus 1000V InterCloud product information: http://www.cisco.com/go/intercloud
- Cisco Nexus 1000V Series product information: http://www.cisco.com/go/1000v
- Cisco Nexus 1000V Series technical documentation: http://www.cisco.com/go/1000vdocs
- Cisco Nexus 1000V community: http://www.cisco.com/go/1000vcommunity
- Deployment guide for Cisco Nexus 1000V Series Switches: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-703595-00 06/12