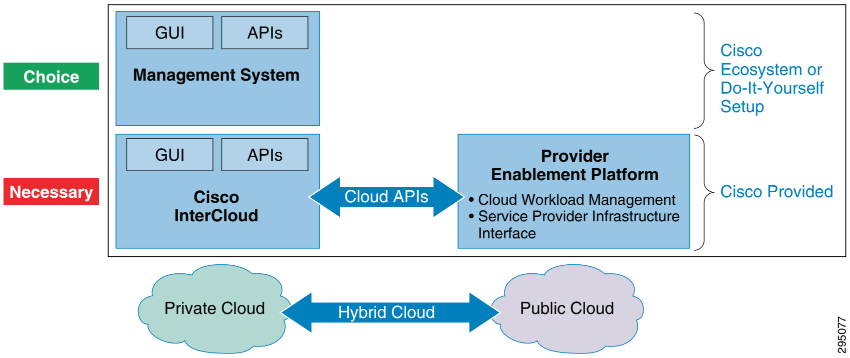
CHAPTER 2

Cisco InterCloud Architectural Overview

Figure 2-1 presents an overview of the Cisco InterCloud architecture.

Figure 2-1 Cisco InterCloud Solution Overview


Choice
Necessary
GUI
APIs
Management System
GUI
APIs
Cisco InterCloud
Cloud APIs
Provider Enablement Platform
• Cloud Workload Management
• Service Provider Infrastructure Interface
Cisco Ecosystem or Do-It-Yourself Setup
Cisco Provided
Private Cloud
Hybrid Cloud
Public Cloud
295077

Cloud Deployment Models

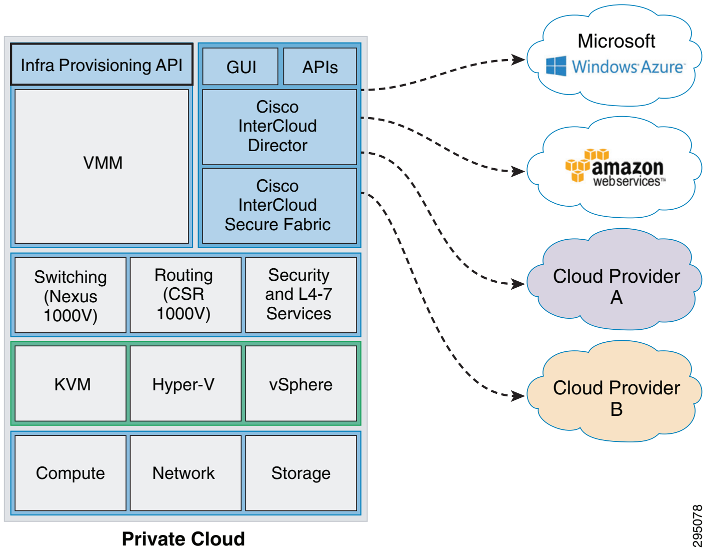
Cisco InterCloud addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.

Enterprise Managed

In the enterprise managed hybrid cloud deployment model, an enterprise manages its own cloud environments. Cisco InterCloud uses hybrid cloud scenarios, extending the private cloud into a public cloud while granting administrative control over both the private and public clouds to the enterprise IT department.

In this hybrid cloud scenario, an enterprise contracts with a service provider, and the service provider provides some cloud resources (computing, storage, and network connectivity) for use by the enterprise. The enterprise, by using the Cisco InterCloud solution, then transparently and securely extends its network into the public cloud, allowing those resources in the public cloud to be treated and handled just as if they were in the on-premises private cloud. All security and policy requirements are applied across the entire hybrid cloud (Figure 2-2).

Figure 2-2 Enterprise Managed Hybrid Cloud



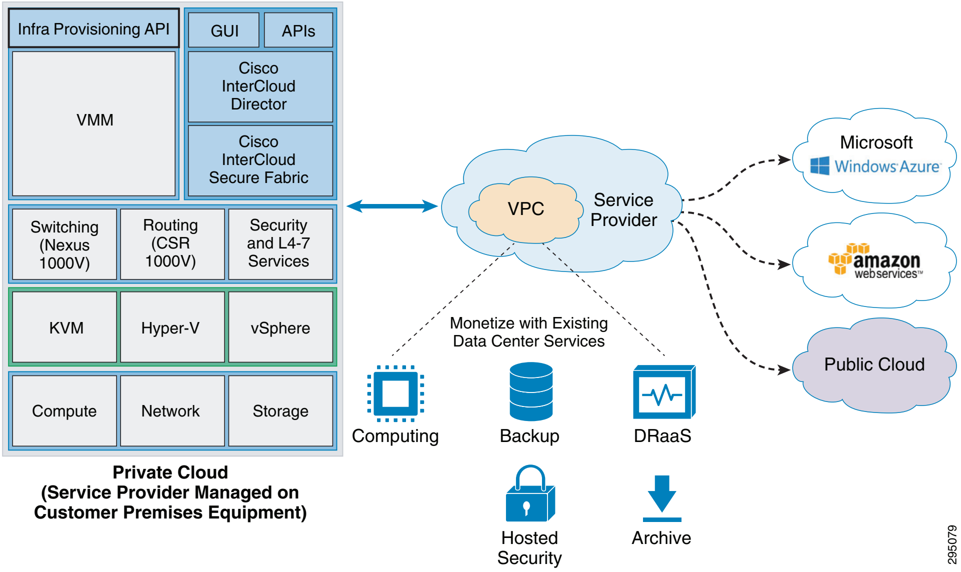
Service Provider Managed

In the service provider managed hybrid cloud scenario, the service provider administers and controls all cloud resources. Customers of the service provider use those resources and deploy their workloads on the service provider managed cloud, but the service provider retains administrative control over the entire cloud environment.

This scenario allows customers to focus on bringing new applications and technology to the marketplace faster, without having to focus on running the data center.

This scenario still allows the creation and use of hybrid clouds. Cisco InterCloud provides transparent and highly secure connectivity between both private cloud environments (typically called virtual private clouds [VPCs]) and a variety of public clouds (Figure 2-3).

Figure 2-3 Service Provider Managed Hybrid Cloud



Cisco InterCloud Solution

The Cisco InterCloud architecture provides two product configurations to address these two consumption models. They are:

- Cisco InterCloud Business Edition
- Cisco InterCloud Provider Edition

Cisco InterCloud Business Edition

Cisco InterCloud Business Edition is intended for enterprise customers who want to be able to transparently extend their private clouds into public cloud environments, while keeping the same level of security and policy across environments. Cisco InterCloud Business Edition consists of the following components:

- Cisco InterCloud Director
- Cisco InterCloud Secure Fabric

Cisco InterCloud Provider Edition

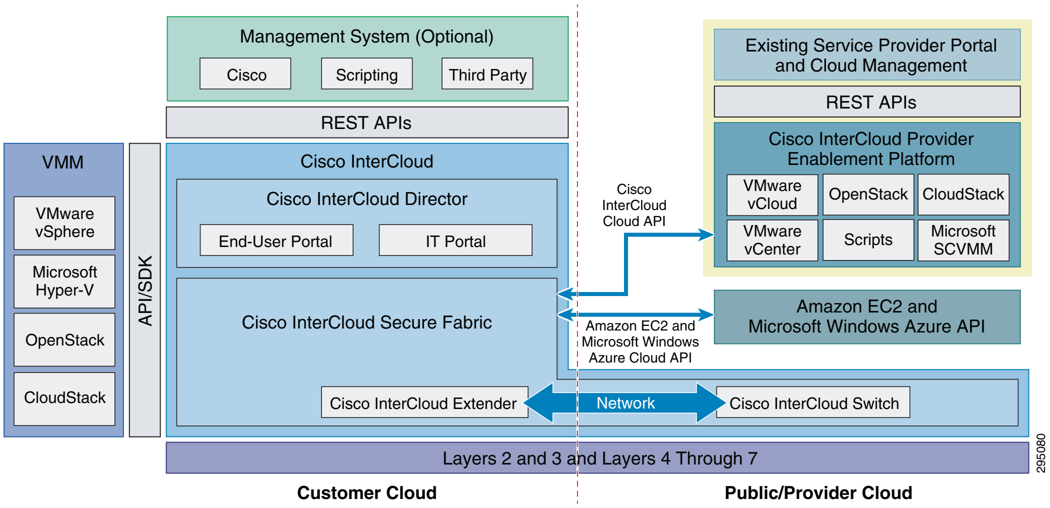
Cisco InterCloud Provider Edition is intended for provider-managed cloud environments, allowing their enterprise customers to transparently extend their private cloud environments into the provider's public cloud, while keeping the same level of security and policy across cloud environments. Cisco InterCloud Provider Edition consists of the following components:

- Cisco InterCloud Director
- Cisco InterCloud Secure Fabric
- Cisco InterCloud Provider Enablement Platform

Cisco InterCloud Components

Figure 2-4 shows the Cisco InterCloud components.

Figure 2-4 Cisco InterCloud Architecture


Management System (Optional)
Cisco
Scripting
Third Party
REST APIs
VMM
VMware vSphere
Microsoft Hyper-V
OpenStack
CloudStack
API/SDK
Cisco InterCloud
Cisco InterCloud Director
End-User Portal
IT Portal
Cisco InterCloud Secure Fabric
Cisco InterCloud Extender
Network
Cisco InterCloud Switch
Cisco InterCloud Cloud API
Amazon EC2 and Microsoft Windows Azure Cloud API
Existing Service Provider Portal and Cloud Management
REST APIs
Cisco InterCloud Provider Enablement Platform
VMware vCloud
OpenStack
CloudStack
VMware vCenter
Scripts
Microsoft SCVMM
Amazon EC2 and Microsoft Windows Azure API
Layers 2 and 3 and Layers 4 Through 7
295080
Customer Cloud
Public/Provider Cloud

Cisco InterCloud Director

Workload management in a hybrid environment goes beyond the capability to create and manage virtual services in a private or public and provider cloud and network extension. Both capabilities are part of the overall hybrid cloud solution, which also needs to provide different types of services, such as policy capabilities (placement, quotas, etc.), capabilities to manage workloads in heterogeneous environments, and other capabilities as discussed here.

Cisco InterCloud Director (ICD) provides to the end user and IT administrator a seamless experience and access to both private and provider clouds, enabling workloads to be placed where they benefit the most and according to technical (capacity, security, etc.) and business (compliance, etc.) needs. Cisco ICD is the single point of management and consumption for hybrid cloud solutions for end users and IT administrators.

Heterogeneous cloud platforms are supported by Cisco ICD in the private cloud, which operationally unifies workload management in a cloud composed of different cloud infrastructure platforms, such as VMware vSphere and vCloud, Microsoft Hyper-V and System Center Virtual Machine Manager (SCVMM), OpenStack, and CloudStack. This unification provides a holistic workload management experience and multiple options for cloud infrastructure platforms for our customers. Cisco ICD provides the required software development kit (SDK) and APIs to integrate with the various cloud infrastructure platforms.

Cisco ICD exposes northbound APIs that allows customers to programmatically manage their workloads in the hybrid cloud environment or to integrate with their management system of choice, which allows more detailed application management that includes policy and governance, application design, and other features.

Future releases of Cisco ICD will include enhanced services that differentiate the Cisco InterCloud solution, such as bare-metal workload deployment in a hybrid cloud environment and an enhanced IT administrative portal with options to configure disaster recovery, backup, virtual desktop infrastructure (VDI), and other services.

Self-Service IT Portal and Service Catalog

The Cisco ICD self-service IT portal makes it easy for IT administrators to manage and consume hybrid cloud offers, and for the end users to consume services. For end users, Cisco ICD provides a service catalog that combines offers from multiple clouds and a single self-service IT portal for private and public clouds.

For IT administrators, Cisco ICD has an IT administrative portal from which administrators can perform the following administrative tasks:

- Configure connection to public and enterprise private clouds
- Configure roles and permissions and enterprise Lightweight Directory Access Protocol (LDAP) integration
- Add and manage tenants
- Configure basic business policies that govern workload placement between the enterprise and public clouds, capacity and quota rules, and lease expiration; advanced policies are available in the management layer
- Set up the workflow for request approval
- Customize portal branding for different tenants and service providers
- Monitor capacity and quota use
- Browse and search the service catalog and initiate requests to provision and manage workloads in the cloud
- View the workload across multiple clouds and migrate workloads as necessary
- Manage user information and preferences
- Configure catalog and image entitlement
- Configure virtual machine template and image import, categorization, and entitlement
- Perform Cisco InterCloud Secure Fabric management

Future capabilities can be added through the end-user or IT administrative portal.

Cisco InterCloud Director and Cisco UCS Director Integration

Cisco ICD does not require Cisco UCS® Director to be installed or configured, but customers with an existing Cisco UCS Director implementation will benefit from the tight integration between both products. Existing Cisco UCS Director installations allow Cisco ICD to be installed as a plug-in.

Ease of Installation

Cisco ICD provides a simplified installation experience, allowing customers to set up the initial environment and connect to a service provider within hours. As a single pane for workload management in the hybrid environment, Cisco ICD also improves Day 1 and Day 2 operations, making it easier to configure provider cloud access and manage the environment.

Cisco InterCloud Secure Fabric

The Cisco InterCloud Secure Fabric forms the basis for the core switching and services infrastructure in the Cisco InterCloud solution. The functions provided by Cisco InterCloud Secure Fabric include:

- Secure Layer 2 network extension from a private data center network to a provider cloud
- Advanced switching features such as access control lists (ACLs) and Internet Group Management Protocol (IGMP) for applications running in the public cloud
- Cisco InterCloud services including zone-based firewalling, VPN, and routing capabilities in the cloud

Cisco InterCloud Secure Fabric consists of several components working together to provide these functions. The enterprise data center is connected to the provider data center through a highly secure tunnel established between a pair of virtual appliances: the Cisco InterCloud Extender running in the enterprise, and the Cisco InterCloud Switch running in the provider cloud. These appliances can be deployed in a high-availability pair to provide redundancy. Virtual services are then deployed within this environment to provide support for firewalling and routing in the cloud.

Cisco InterCloud Extender

The Cisco InterCloud Extender is deployed as a virtual appliance in the enterprise data center. The Cisco InterCloud Extender is the endpoint for the secure tunnel from the provider to the enterprise. Additionally, it is the entity that enables the extension of the enterprise network to the public cloud.

Cisco InterCloud Switch

The Cisco InterCloud Switch is deployed as a virtual appliance in the provider environment. For example, when Amazon is the provider, the Cisco InterCloud Switch image is an Amazon Machine Image (AMI). The Cisco InterCloud Switch is the endpoint for the secure tunnel on the provider side. 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, goes through the Cisco InterCloud Switch. This approach provides the end-to-end security that is a primary feature of Cisco InterCloud.

Cisco InterCloud Secure Fabric Security Feature

All data in motion is cryptographically isolated and encrypted within the Cisco InterCloud Secure Fabric. This data includes traffic exchanged between the Cisco InterCloud Extender and Cisco InterCloud Switch as well as traffic between the Cisco InterCloud Switch and cloud virtual machines. A Datagram Transport Layer Security (DTLS) tunnel is created between these endpoints to more securely transmit this data. DTLS is a User Datagram Protocol (UDP)–based highly secure transmission protocol. The Cisco InterCloud Extender always initiates the creation of a DTLS tunnel.

The encryption algorithm used is configurable, and different encryption strengths can be used depending 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

Cisco InterCloud Secure Fabric Virtual Zone-Based Firewall Feature

In traditional data center deployments, virtualization presents a need to secure traffic between virtual machines; this traffic is generally referred to as east-west traffic. Instead of redirecting this traffic to the edge firewall for lookup, data centers can handle the traffic in the virtual environment by deploying a zone-based firewall. Cisco InterCloud Secure Fabric includes a zone-based firewall that can be deployed to provide policy enforcement for communication between virtual machines and to protect east-west traffic in the provider cloud. The virtual firewall is integrated with Cisco Virtual Path (vPath) technology, which enables intelligent traffic steering and service chaining. The main features of the zone-based firewall include:

Policy definition based on network attributes or virtual machine attributes such the virtual machine name

- Zone-based policy definition, which allows the policy administrator to partition the managed virtual machine space into multiple logical zones and write firewall policies based on these logical zones
- Enhanced performance due to caching of policy decisions on the local Cisco vPath module after the initial flow lookup process

Cisco InterCloud Secure Fabric Virtual Router Feature

Cisco InterCloud Secure Fabric provides a Layer 2 extension from the enterprise data center to the provider cloud. To support Layer 3 functions without requiring traffic to be redirected to the enterprise data center, Cisco InterCloud also includes a virtual router. The virtual router is based on proven Cisco IOS® XE Software and runs as a virtual machine in the provider cloud. The router deployed in Cisco InterCloud Secure Fabric serves as a virtual router and firewall for the workloads running in the provider cloud and works with Cisco routers in the enterprise to deliver end-to-end Cisco optimization and security. The main functions provided by the virtual router include:

- Routing between VLANs in the provider cloud
- Direct access to cloud virtual machines
- Connectivity to enterprise branch offices through a direct VPN tunnel to the service provider’s data center
- Access to native services supported by a service provider: for example, use of Amazon Simple Storage Service (S3) or Elastic Load Balancing services

Cisco InterCloud Provider Enablement Platform

Cisco InterCloud Provider Enablement Platform (ICPEP) simplifies and abstracts the complexity involved in working with a variety of public cloud APIs, and it enables cloud API support for service providers that currently do not have it. Cisco ICPEP provides an extensible adapter framework to allow integration with a variety of provider cloud infrastructure management platforms, such as VMware vCloud, OpenStack, Microsoft System Center, scripts, and other cloud APIs.

Currently, service providers have their own proprietary cloud APIs (Amazon Elastic Compute Cloud [EC2], Microsoft Windows Azure, VMware vCloud Director, OpenStack, etc.), giving customers limited choices and no easy option to move from one provider to another. Cisco ICPEP abstracts this complexity and translates Cisco InterCloud Secure Fabric API calls to different provider infrastructure platforms, giving customers the choice to move their workloads regardless of the cloud API exposed by the service provider.

Many service providers do not provide cloud APIs that Cisco InterCloud Secure Fabric can use to deploy customers' workloads. One option for these providers is to provide direct access to their virtual machine managers' SDKs and APIs (for example, through VMware vCenter or Microsoft System Center), which exposes the provider environment and in many cases is not a preferred option for service providers because of security concerns, for example. Cisco ICPEP, as the first point of authentication for the customer cloud that allows it to consume provider cloud resources, enforces highly secure access to the provider environment and provides the cloud APIs that are required for service providers to be part of the provider ecosystem for Cisco InterCloud.

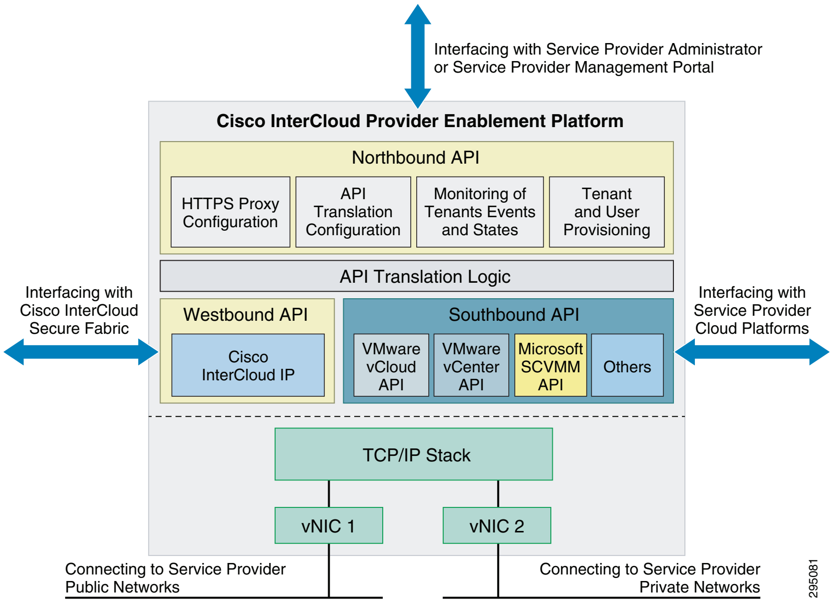
As the interface between the Cisco InterCloud Secure Fabric from customers' cloud environments and provider clouds (public and virtual private clouds), Cisco ICPEP provides a variety of benefits as part of the Cisco InterCloud solution:

- Brings standardization and uniformity to cloud APIs, making it easier for Cisco InterCloud to consume cloud services from service providers that are part of the Cisco InterCloud ecosystem
- Helps secure access to service providers' underlying cloud platforms
- Limits the utilization rate per customer and tenant environment
- Provides northbound APIs for service providers to integrate with their existing management platforms
- Supports multitenancy
- Provides tenant-level resource monitoring
- Offers chargeback features
- In the future, will help build Cisco infrastructure-specific differentiation
- In the future, will provide support for enterprises to deploy bare-metal workloads in the provider cloud

Cisco ICPEP Architecture

Cisco ICPEP is a virtual appliance deployed in the service provider cloud data center to enable service provider customers to access cloud resources using Cisco InterCloud APIs. The virtual appliance provides two virtual network interfaces: one interface allows customers' Cisco InterCloud Secure Fabric to reach the Cisco ICPEP appliance instance from public networks, and the other interface allows the Cisco ICPEP appliance to connect with the service provider cloud platforms. Figure 2-5 shows the Cisco ICPEP appliance architecture.

Figure 2-5 Cisco InterCloud Enablement Platform Architecture


Interfacing with Service Provider Administrator or Service Provider Management Portal
Cisco InterCloud Provider Enablement Platform
Northbound API
HTTPS Proxy Configuration
API Translation Configuration
Monitoring of Tenants Events and States
Tenant and User Provisioning
API Translation Logic
Westbound API
Cisco InterCloud IP
Southbound API
VMware vCloud API
VMware vCenter API
Microsoft SCVMM API
Others
Interfacing with Cisco InterCloud Secure Fabric
Interfacing with Service Provider Cloud Platforms
TCP/IP Stack
vNIC 1
vNIC 2
Connecting to Service Provider Public Networks
Connecting to Service Provider Private Networks
295081

Cisco ICPEP architecture includes four major interface modules:

- **Northbound API**—This module implements a set of APIs for the service provider administrator to use to configure the Cisco ICPEP appliance, provision tenants and users, and monitor tenant operations.
- **Westbound API**—This module implements the Cisco InterCloud cloud API, which is consumed by Cisco InterCloud Secure Fabric (customer cloud) for workload provisioning.
- **Southbound API**—This module implements the various cloud platform interface adapters, each of which is responsible for interfacing with a specific cloud platform such as VMware vCloud Director and Microsoft System Center.
- **API Translation Logic**—This module implements translation logic between Cisco InterCloud cloud APIs and cloud platform–specific APIs.

When to Deploy Cisco ICPEP?

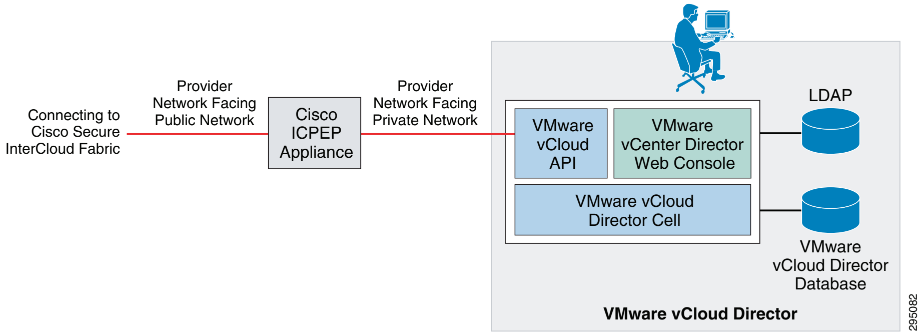
Cisco ICPEP should be implemented for all service providers that interface with Cisco InterCloud Secure Fabric. The only exceptions to this rule are Amazon EC2 and Microsoft Windows Azure, which are available to Cisco InterCloud Secure Fabric through their native public cloud APIs.

Cisco ICPEP Deployment Topology

To access the service provider's cloud resources, Cisco InterCloud Secure Fabric needs to access the Cisco ICPEP appliance from the public network; therefore, the public network interface of the appliance needs to be deployed in a provider network that is exposed to the service provider's edge router. The private network interface for the appliance can connect to the private provider network that accesses the service provider cloud platform (for example, VMware vCloud Director).

The Cisco ICPEP deployment topology varies for different service providers and cloud platforms. Figure 2-6 illustrates a deployment with a VMware vCloud Director environment in the service provider.

Figure 2-6 *Cisco ICPEP Appliance Deployment Topology*


Connecting to Cisco Secure InterCloud Fabric
Provider Network Facing Public Network
Cisco ICPEP Appliance
Provider Network Facing Private Network
VMware vCloud API
VMware vCenter Director Web Console
VMware vCloud Director Cell
LDAP
VMware vCloud Director Database
VMware vCloud Director
295082

The Cisco ICPEP appliance uses HTTPS connections to communicate with the Cisco InterCloud Secure Fabric and the service provider cloud platform. A firewall is not required in the network path between the Cisco InterCloud Secure Fabric and the Cisco ICPEP appliance, or between the Cisco ICPEP appliance and the cloud platform endpoints.

Cisco ICPEP Operating Model

The following example describes Day 0 and Day 1 operations for the Cisco ICPEP appliance.

Day 0 Operation: Deployment and Initialization

The Cisco ICPEP appliance is deployed in the service provider data center as part of the service provider's cloud platform. In Day 0 operation, the service provider administrator deploys the appliance in the provider network and provides the appliance with the following configurations:

- Appliance IP address
- SSL server and client configurations
- Administrator user credentials and privileges
- Cloud platform type and endpoint address

The service provider administrator provisions service provider tenants and users for the appliance. After the Cisco ICPEP appliance is deployed, the service provider administrator publishes the URL of the appliance to the provider's customers so that they can reach it.

Day 1 Operation: Tenant Sign-On and Query

After the Cisco ICPEP appliance is operational in the service provider data center and its URL has been posted publicly, the provider's customers can start to reach the appliance, and the Cisco InterCloud Secure Fabric component can start to access the Cisco ICPEP appliance with a sign-on API request.

Cisco InterCloud Management System

The seemingly borderless environment created by Cisco InterCloud between private and public resources provides numerous features and benefits. To also provide the benefits of automated placement decisions for cloud services, enterprises can use a Cisco InterCloud management system, which makes placement decisions that comply with business needs such as the following:

- **Access Control**—A set of policies that enforce role-based access control (RBAC) for the various virtual machines

- **Compliance**—Support to define policies aligned with the existing compliance requirements such as those for Sarbanes-Oxley, PCI, HIPAA, and Statement on Auditing Standards (SAS) Number 70 (SAS 70)
- **Capacity Utilization—**Capability to define policies that monitor capacity utilization and take actions such as notification or restriction of environment use; eventually, this policy will trigger resizing of the environment
- **Network**—Capability to enforce ACL or firewall rules based on workload requirements, appliance and hardware (Cisco Virtual Security Gateway [VSG]), or operating system level (Microsoft Windows Firewall or iptables)
- **Performance**—Policy definition for performance characteristics of the workload such as memory, CPU, or disk utilization, and the capability to take actions based on this utilization such as resizing of a virtual machine
- **Personalization—**Virtual machine operating system personalization to follow corporate standards for naming conventions, installed software, etc.
- **Placement Eestrictions—**Capability to restrict virtual machine placement based on business requirements: for example, a policy to restrict the placement of virtual machines that have sensitive workloads and cannot run in the public cloud
- **Provisioning—**Capability to establish the number of virtual machines per user or project

With a Cisco InterCloud management system in place, these kinds of decisions, implemented through policies set by the enterprise, allow functions in multiple clouds as a contiguous environment, while implementing consistent business-relevant placement decisions.

The Cisco InterCloud management system connects to Cisco ICD through the available northbound API, integrating upstream portal and orchestration systems with the resources that Cisco InterCloud provides.

Cisco InterCloud will offer two management system options at release: Cisco Intelligent Automation for Cloud (IAC) and ServiceMesh Agility Platform. These options are being augmented in the Cisco InterCloud roadmap to include CloudForms and CloudStack, plus a published API for custom integrations for particular customers' needs.

Example 1: Cisco IAC as the Cisco InterCloud Management System

Cisco IAC enables organizations to deliver a disciplined and structured automation solution for the multitude of applications under their control. The powerful Cisco IAC platform can scale from single-cloud to multicloud to hybrid cloud deployments, while supporting comprehensive application sets ordered by end users on demand. The framework can accommodate complex customer technical and business requirements, offering end users a single interface for requesting a comprehensive array of services.

The Cisco IAC solution is often deployed to complement other Cisco products and services and partner technology solutions for data center, cloud computing, mobility, collaboration, and other end-user IT and workplace-related services.

The addition of Cisco InterCloud management capabilities to Cisco IAC is therefore a natural evolution that allows the platform to transparently migrate workloads between and across clouds. Cisco IAC is tightly integrated with the Cisco InterCloud solution, providing an added layer of capabilities that address the business requirements of a hybrid cloud management solution. The integrated solution simplifies the intelligent placement of computing workloads based on an advanced policy-based engine that automates the entire process, eliminating any human interaction in the decision-making cycle. These policies can incorporate a variety of parameters, such as cost, workload, and location preference, helping ensure an optimized, efficient, and cost-effective business operating model.

Using the Cisco advantage, Cisco IAC InterCloud management development efforts are internally harmonized to align with the evolution of the Cisco InterCloud solution.

Example 2: ServiceMesh Agility Platform as the Cisco InterCloud Management System

ServiceMesh is working with Cisco to make ServiceMesh Agility Platform a fully integrated management system for Cisco InterCloud. ServiceMesh Agility Platform, with its policy and governance of cloud resources, is well established as a cloud management platform. It takes an application-centric view of the IT environment, which adds a vast amount of policy and governance control over the IT development and operations (DevOps) environment.

ServiceMesh Agility Platform brings extensive software-development lifecycle functions to the Cisco InterCloud solution. Applications are characterized as blueprints that can be deployed uniformly among cloud resources. This approach blueprints also presents a framework that can pass development artifacts between development environments, which then can be quickly rolled out with ServiceMesh Agility Platform.

ServiceMesh Agility Platform works with most popular hypervisors, and it has also been integrated with Cisco UCS Director for bare-metal deployment of application resources.

When ServiceMesh Agility Platform is layered on top of Cisco InterCloud, cloud administrators can truly offer complete IT as a service (ITaaS), allowing developers to quickly and consistently deploy their workloads in the proper environment, for the proper amount of time, and according to the IT policies created by the cloud administrator. This amount of flexibility, governance, and control, provided transparently across private and public clouds, with all security and lifecycle policies applied consistently across all environments, dramatically changes the role of IT. It allows IT to be viewed as an enabler to DevOps, rather than as a hurdle, which has been the case in the past.

Conclusion

Cisco InterCloud addresses many of the most common challenges of hybrid cloud adoption. It creates an essentially borderless environment for enterprise customers with hybrid clouds, and it allows service providers to present their public cloud offerings for consumption by their enterprise customers.

Additionally, Cisco InterCloud allows the creation of workload policies that mirror business needs, with flexibility and enterprise-level security built in. Cisco InterCloud can bring consistent policy and security to a multicloud environment, with a single pane for viewing workloads across these clouds and support for a variety of hypervisor and cloud provider resources. Additionally, by bringing rogue, shadow IT deployments into view, Cisco InterCloud helps assure IT stakeholders that their applications are being deployed securely and in the right environment.

This solution is built from the foundation, and is supported by APIs, to offer flexibility of implementation and to help ensure a wide range of independent integration.