Cisco InterCloud: Enable a Hybrid Cloud

January 27, 2014

Cisco InterCloud: Enable a Hybrid Cloud

CONTENTS

CHAPTER 1 **Introduction** 1-1

Hybrid Cloud with Cisco InterCloud 1-1

Cisco InterCloud Use Cases 1-2

Development and Testing 1-2

Capacity Augmentation 1-3

Shadow IT Control 1-3

Disaster Recovery 1-3

Greenfield Deployment 1-4

Brownfield Deployment 1-4

CHAPTER 2 **Cisco InterCloud Architectural Overview** 2-1

Cloud Deployment Models 2-1

Enterprise Managed 2-1

Service Provider Managed 2-2

Cisco InterCloud Solution 2-3

Cisco InterCloud Business Edition 2-3

Cisco InterCloud Provider Edition 2-3

Cisco InterCloud Components 2-4

Cisco InterCloud Director 2-4

Self-Service IT Portal and Service Catalog 2-5

Cisco InterCloud Director and Cisco UCS Director Integration 2-5

Ease of Installation 2-5

Cisco InterCloud Secure Fabric 2-5

Cisco InterCloud Extender 2-6

Cisco InterCloud Switch 2-6

Cisco InterCloud Secure Fabric Security Feature 2-6

Cisco InterCloud Secure Fabric Virtual Zone-Based Firewall Feature 2-7

Cisco InterCloud Secure Fabric Virtual Router Feature 2-7

Cisco InterCloud Provider Enablement Platform 2-7

Cisco ICPEP Architecture 2-8

When to Deploy Cisco ICPEP? 2-9

Cisco ICPEP Deployment Topology 2-9

Cisco ICPEP Operating Model 2-10

Cisco InterCloud Management System 2-10

Example 1: Cisco IAC as the Cisco InterCloud Management System 2-11
Example 2: ServiceMesh Agility Platform as the Cisco InterCloud Management System 2-12
Conclusion 2-12

APPENDIX A **Shadow IT and Cisco Cloud Consumption Professional Services** A-1

CHAPTER 1

Introduction

This document is written for IT decision makers, architects, engineers, and application owners who make architectural decisions for hybrid deployments. The architecture described in this document is for large and medium-sized businesses that are considering hybrid cloud solutions. This document is also useful for service providers that deliver hybrid cloud services to businesses.

Hybrid Cloud with Cisco InterCloud

In December 2012, Cisco commissioned Forrester Consulting to investigate the growing interest in infrastructure as a service (IaaS), and more specifically in the hybrid cloud model. According to Forrester, about half of U.S. and European enterprise IT decision makers report that their companies use cloud IaaS, and Forrester expects enterprises to increasingly adopt IaaS. In many enterprises that are adopting private clouds, on-premises infrastructure cannot always provide the resources needed to address unplanned growth. The hybrid cloud architecture combines private cloud infrastructure with cloud service provider infrastructure to provide users with essentially unlimited resources in the public cloud, with security and control managed in the private cloud.

IT decision makers report that their greatest interest in IaaS in a hybrid cloud is as a complement, rather than a replacement, for on-premises capacity. These decision makers are planning for the resulting impact on network operations and spending. Although a hybrid approach promises cost savings and significant gains in IT and business flexibility, some concerns remain about management and integration of on-premises infrastructure with cloud services in a hybrid cloud architecture.

Forrester asked 69 IT decision makers in the United States, United Kingdom, France, and Germany about their cloud strategies. These decision makers were interested in using, or were already using, a service provider for cloud IaaS. A large majority (76 percent) plan to implement hybrid clouds. In addition, the 2012 Gartner Data Center Summit survey suggests that 70 percent of enterprises will pursue hybrid cloud strategies by 2015. Most hybrid cloud adopters plan to use IaaS as a complement to on-premises servers and storage, but a significant number also look to service providers for peak workload and other use cases.

Forrester also reports that in firms using IaaS, decision makers state that the most valuable benefits of a hybrid cloud strategy are IT flexibility, reduced costs, and faster, more flexible responses to market and business needs. IT decision makers are also clear about their views of the potential challenges associated with a hybrid cloud strategy. Many want consistent security policies and highly secure communications that span the data center and the cloud service provider, and they want to learn how to make existing applications work in both locations. Other important needs include transparent integration with cloud service providers for movement of virtual machines, shared networks with cloud service providers, and consistent application management across the hybrid cloud architecture.

IT decision makers will seek solutions to these challenges using existing tools and skills, or they will explore new offerings that make it easier to address the challenges of hybrid cloud strategies. Evolving solutions that address the most immediate hybrid cloud challenges include:

- Consistent policy enforcement and capabilities for firewalls, security, and application delivery
- Highly secure network connectivity for virtual machine migration
- A common view of workloads and resources across data centers and cloud service providers
- Support for heterogeneous hypervisor environments and infrastructure software

The Cisco® InterCloud solution provides a faster, more flexible response to business needs and addresses the potential challenges of hybrid clouds (Figure 1-1).

- Cisco InterCloud is an open solution that supports multiple hypervisors and multiple clouds with the freedom to place workloads in both private and service provider clouds across heterogeneous environments.
- To protect critical business assets and meet compliance requirements, Cisco InterCloud provides highly secure, scalable connectivity to extend private clouds to service provider clouds.
- Cisco InterCloud provides workload security throughout the resulting hybrid clouds.
- Cisco InterCloud enforces consistent network and workload policies throughout the hybrid cloud.
- To provide consistent operations and workload portability across clouds, Cisco InterCloud delivers unified hybrid cloud management for end users and IT administrators, enabling workload mobility to and from service provider clouds for physical and virtual workloads.

Figure 1-1 Cisco InterCloud Solution

• **Open:** Freedom to place workloads across heterogeneous private and public clouds
• **Consistent Security:** Workloads in public clouds as a secure extention from private clouds
• **Portability:** Unified management and networking to move workloads across clouds

295076

Cisco InterCloud Use Cases

Cisco's industry research shows that the most common use cases for hybrid cloud designs are development and testing, capacity augmentation, and shadow (rogue) IT control. The Cisco InterCloud roadmap adds support for disaster recovery.

Development and Testing

In the development and testing use case, enterprise customers develop workloads in service provider clouds and bring the workload back to their private clouds after the workload is promoted to the production environment. To achieve the economic benefits of the cloud and support faster development, many application developers use service provider clouds for the development and testing environment. However, deployment of production applications in service provider clouds raises critical security and compliance concerns for IT departments. IT decision makers want to provide flexibility to application developers and enable them to use cloud service providers, but they require production workloads to be deployed in private clouds with security and controls to meet compliance requirements such as Payment

Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley mandates. Cisco InterCloud provides this flexibility with its capability both to move workloads into service provider clouds and to bring workloads back into the customers' private clouds and on-premises infrastructure.

Capacity Augmentation

The capacity augmentation use case addresses the need for temporary resources. For example, to meet seasonal demands, an enterprise can rely on the service provider cloud to provide temporary resources; when high-demand processing finishes, the resources are decommissioned. For example, during peak shopping seasons for retailers or tax season for financial services, there are planned and unplanned demands for additional cloud resources for short and long durations. To achieve the economic benefits of a hybrid cloud, customers can flexibly extend to service provider clouds to meet peak demands while benefiting from the security and control of the private cloud. The Cisco InterCloud solution transparently delivers required capacity while providing the security and control of a private cloud.

Shadow IT Control

Many enterprises prefer to deploy development workloads in the public cloud, primarily for convenience and faster deployment. This approach can cause concern for IT administrators, who must control the flow of IT traffic and spending and help ensure the security of data and intellectual property. Without the proper controls, data and intellectual property can escape this oversight. The Cisco InterCloud solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control and placing these resources under Cisco InterCloud control.

Disaster Recovery

To meet growing IT infrastructure needs and to help ensure enterprise continuity during a site-level disaster, enterprises must have live mobility and fully automated, efficient disaster-recovery processes for applications across data centers. Failure to have robust, efficient mobility and fully automated disaster-recovery solutions can result in millions of dollars of lost revenue and employee productivity. The task of establishing efficient disaster-recovery processes and building a disaster-recovery site is both time consuming and costly.

With the emergence of hybrid clouds, enterprises can consider running their production environments in private clouds and their disaster-recovery environments in service provider clouds. The enterprise can replicate data to the service provider cloud while resources in the service provider cloud remain nonoperational until disaster recovery is needed. If a disaster strikes, IT administrators can quickly bring up the applications in the service provider cloud without affecting business needs because the data already resides in the service provider cloud.

This approach results in significant IT cost savings because there is no longer any need to build another data center for disaster recovery. This approach also presents new opportunities for service providers to take advantage of their multitenant clouds to provide disaster recovery as a service (DRaaS).

Greenfield Deployment

The Cisco InterCloud solution can greatly benefit organizations that are in the early stages of adopting the public cloud but have not yet taken that step. The Cisco InterCloud solution can more securely manage workload migration between private and public clouds and support cross-cloud policy consistency.

Brownfield Deployment

Organizations in which developers have already circumvented IT and deployed public cloud solutions can use Cisco Cloud Consumption services to identify public cloud use and restore cooperation between IT and developers. Such organizations can consider the following approach:

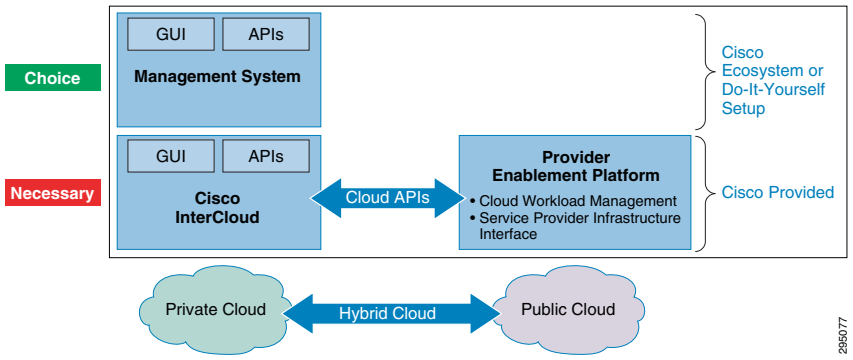
- Use Cisco Cloud Onboarding services to migrate workloads to a service provider that can meet the organization's compliance requirements. These services provide the benefits of bulk purchasing, bringing all IT costs under a common authority, and meet availability and business-continuity requirements.
- Return the workloads to IT management by deploying Cisco InterCloud and integrate the solution with the organization's existing infrastructure and tools; this approach supports a simple, highly secure hybrid cloud integration plan.
- Continue using Cisco Cloud Consumption services to track public cloud use.

CHAPTER 2

Cisco InterCloud Architectural Overview

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

Figure 2-1 Cisco InterCloud Solution Overview



Cloud Deployment Models

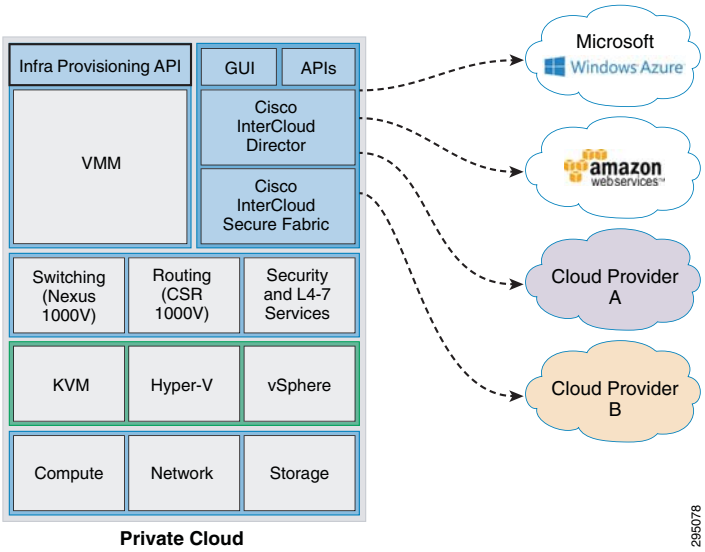
Cisco InterCloud addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.

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



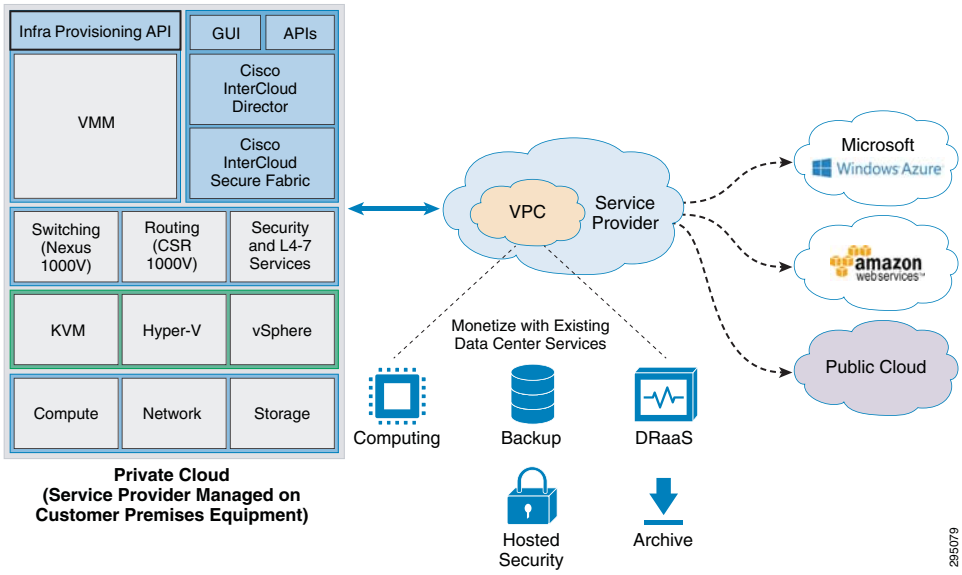
Service Provider Managed

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

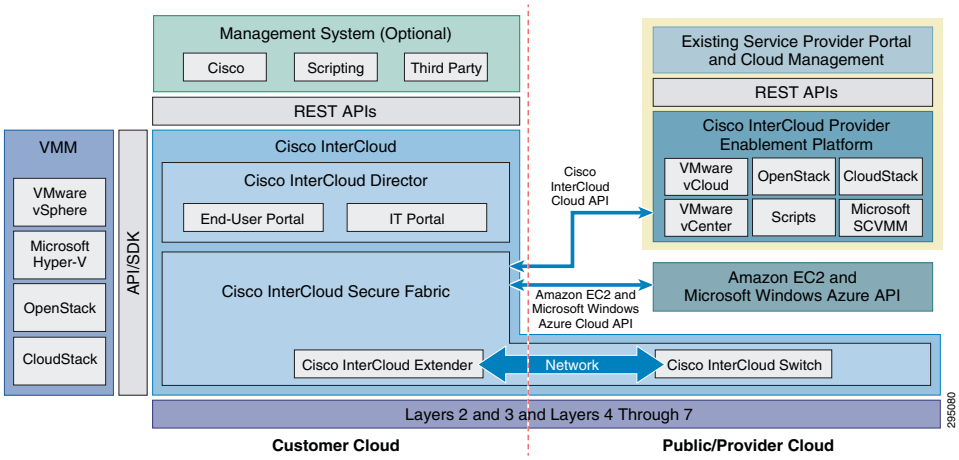
Cisco InterCloud Provider Edition is intended for provider-managed cloud environments, allowing their enterprise customers to transparently extend their private cloud environments into the provider's public cloud, while keeping the same level of security and policy across cloud environments. Cisco InterCloud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



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.

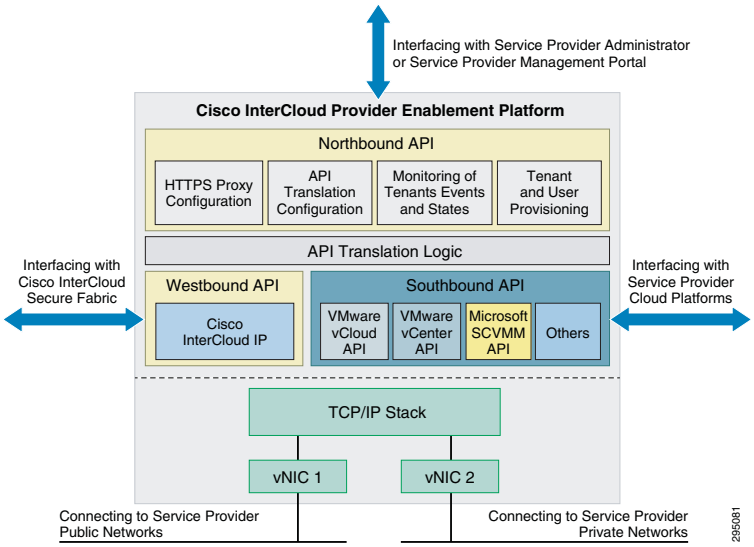
As the interface between the Cisco InterCloud Secure Fabric from customers' cloud environments and provider clouds (public and virtual private clouds), Cisco ICPEP provides a variety of benefits as part of the Cisco InterCloud solution:

- 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



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?

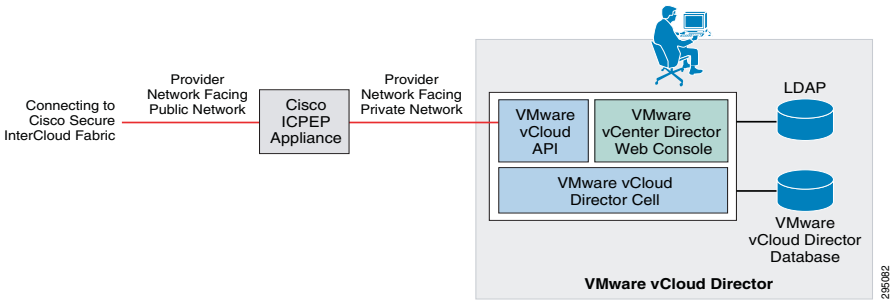
Cisco ICPEP should be implemented for all service providers that interface with Cisco InterCloud Secure Fabric. The only exceptions to this rule are Amazon EC2 and Microsoft Windows Azure, which are available to Cisco InterCloud Secure Fabric through their native public cloud APIs.

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



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.

APPENDIX A

Shadow IT and Cisco Cloud Consumption Professional Services

Rogue cloud applications, or shadow IT, can be identified by deploying the Cisco Cloud Usage Collector in the customer network. NetFlow data is sent from customer routers to the collector to identify the cloud service providers that are being accessed, the number of unique IP addresses being used, and the volume of traffic to these providers. This information together reveals shadow IT consumption.

Cloud computing has dramatically changed the IT landscape. To help lower costs and obtain greater business agility, companies are shifting from a primarily on-premises IT structure to a mix of cloud and on-premises applications. In 2014 an estimated 10 percent of IT budgets will be spent on cloud services, and by 2020 the cloud marketplace is expected to be worth US$159 billion.

The increase in public cloud service adoption has also led to an increase in rogue cloud applications. This shadow IT occurs when a business implements a public cloud that is not managed by or integrated into the company's IT infrastructure. Although many IT teams are aware that shadow IT exists in their enterprises, they are often unaware of the number of cloud applications that have entered the enterprise. Initial assessments with customers reveal that authorized cloud service vendors typically represent only 20 percent of their actual cloud use, and that 5 to 10 times more cloud services are consumed than those IT is aware of.

Industry surveys also support this trend. A recent survey conducted by advisory firm CEB shows that chief information officers (CIOs) of 165 organizations (representing more than US$47 billion in IT spending) estimate shadow IT to be 40 percent beyond the official IT budget. Additionally, Gartner predictions show IT budgets are moving out of the control of IT departments. By 2015, 35 percent of enterprise IT expenditures for most organizations will be managed outside the IT department's budget (Gartner Top Predictions for IT Organizations and Users for 2012 and Beyond).

Shadow IT presents a new set of challenges for business and IT leaders, including how to manage the costs and risks associated with cloud adoption and how to establish effective cloud management processes.

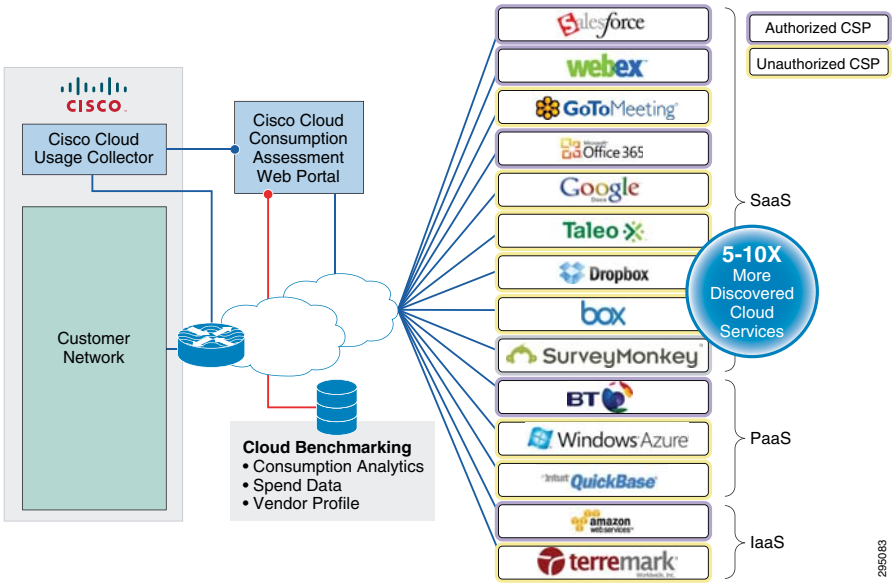
The Cisco Cloud Consumption Professional Services offering was created to help customers gain visibility into cloud services and implement stronger cloud management practices. Cisco Cloud Consumption Professional Services helps customers become more agile, reduce risks, and optimize public cloud costs.

Cisco Cloud Consumption Professional Services uses the network to help customers determine which cloud service providers (CSPs) are being accessed by employees across their entire organization. The services provide customers with full visibility into their organizations’ authorized and unauthorized public cloud use.

By placing data collection tools in the customer network, Cisco can gather enterprisewide cloud service provider usage data to identify redundant cloud services, public cloud spending, potential risks, and cloud usage trends.

Cisco Cloud Consumption Professional Services typically discovers 5 to 10 times more cloud services than those authorized by IT and gives organizations the tools to understand the risks and costs associated with cloud use (Figure A-1).

Figure A-1 Shadow IT Control



For example, despite blocking 90 percent of public Internet traffic and authorizing only 11 cloud providers, the IT department for the Government of New Brunswick, Canada, uncovered more than 220 cloud providers with potential savings of US$750,000 with Cisco Cloud Consumption Assessment Service.

The Cisco Cloud Consumption Professional Services offering is an add-on to the Cisco InterCloud solution through Cisco Advanced Services, but in future releases this offering will be fully incorporated into the product.