Cisco Intercloud Fabric: Hybrid Cloud with Choice, Consistency, Control and Compliance

January 8, 2016

Cisco Intercloud Fabric: Hybrid Cloud with Choice, Consistency, Control and Compliance

CONTENTS

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 Landscape and Challenges

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
- Workload mobility and portability

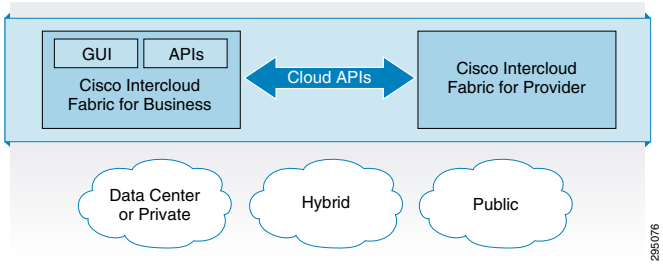
Cisco Intercloud Fabric Overview and Value Proposition

Cisco Intercloud Fabric is a software solution that enables customers to manage and access their workloads across multiple public clouds in a heterogeneous environments, giving customers choice and flexibility to place their workloads where it benefits the most and according to a technical (capacity, security, etc.) or business (compliance, etc.) needs.

With Cisco Intercloud Fabric, customers can choose what networks can be securely extended to the public cloud, and consistent network configuration and security policies can be enforced throughout the hybrid cloud. Intercloud Fabric mechanism to enforce security goes beyond the secure tunnel between private and public clouds, and extends the security all the way to the Virtual Machines (VMs) running in the cloud, so the communication between these VMs in the cloud can be secured as well. This mechanism is explained later in this document.

Figure 1-1 illustrates the solution footprint for enterprise customers, where Cisco Intercloud Fabric for Business can be deployed in the private cloud in heterogeneous environments. This software solution gives IT an admin portal that allows management of workloads, security policies, and network extension to the cloud, and includes northbound API capabilities to allow integration with existing private cloud management solutions. IT customers, including enterprise lines of businesses, can take advantage of Intercloud Fabric for Business embedded self-service catalog to create new workloads in multiple clouds, and manage workload lifecycle and migration through its end-user portal.

Figure 1-1 Cisco Intercloud Fabric Solution



Cisco Intercloud Fabric for Provider is a multi-tenant software appliance that is installed and managed by the cloud providers that are part of the Intercloud Fabric ecosystem. This virtual appliance creates Cloud API uniformity across different cloud providers and abstracts the complexity of supporting heterogeneous Cloud APIs. In the future Intercloud Fabric for Provider will help to build Cisco infrastructure-specific differentiation for all Cisco Powered Cloud Providers.

Cisco Intercloud Fabric gives customers multiple choices of cloud providers, including the ecosystem of Cisco Powered Cloud Providers and the hyper scale public clouds such as Amazon EC2 and Microsoft Azure. Cisco believes that business customers also want choices of hypervisors for their virtualized

environment, so it is important for the solution that enables hybrid cloud to be hypervisor agnostic. The scenario with multiple choices of hypervisors on premises and off premises can make workload mobility and portability difficult, but Cisco Intercloud Fabric resolves this problem and makes this transparent for customers, allowing workloads to be moved to multiple clouds and back to the enterprise.

In summary, Cisco Intercloud Fabric aims to provide a more flexible response to business needs and addresses the potential challenges of hybrid clouds, among other benefits that can be described as follow:

- Workload security throughout the resulting hybrid clouds.
- Consistent operations and workload portability across clouds. Cisco Intercloud Fabric 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.
- To protect critical business assets and meet compliance requirements, Cisco Intercloud Fabric provides highly secure, scalable connectivity to extend private clouds to service provider clouds.

Cisco Intercloud Fabric 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 Fabric 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 Fabric 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 Fabric 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 Fabric solution helps control this shadow IT, discovering resources deployed in the public cloud outside IT control (Appendix A, "Shadow IT and Cisco Cloud Consumption Professional Services") and placing these resources under Cisco Intercloud Fabric control.

Intercloud Fabric Deployment Models

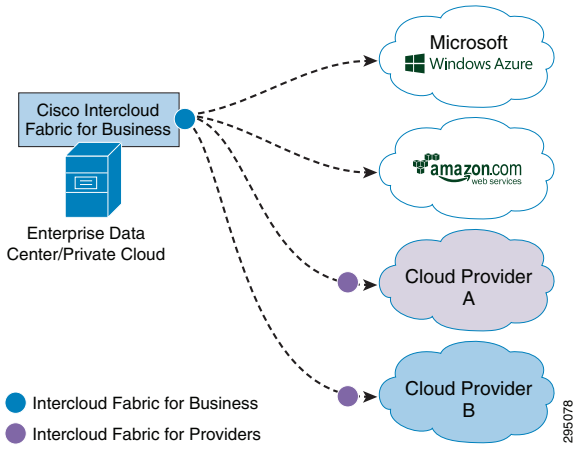
Cisco Intercloud Fabric addresses the cloud deployment requirements appropriate for two hybrid cloud deployment models: Enterprise Managed and Service Provider Managed.

Enterprise Managed

In the enterprise managed hybrid cloud deployment model, an enterprise manages its own cloud environments. Cisco Intercloud Fabric 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 Fabric 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 1-2).

Figure 1-2 Enterprise Managed Hybrid Cloud



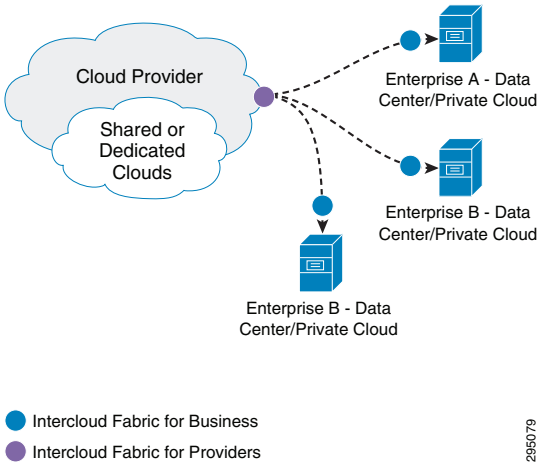
Service Provider Managed

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 Fabric provides transparent and highly secure connectivity between both private cloud environments (typically called virtual private clouds [VPCs]) and a variety of public clouds (Figure 1-3).

Figure 1-3 Service Provider Managed Hybrid Cloud



Greenfield Deployment

The Cisco Intercloud Fabric 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 Fabric 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 (Appendix A, “Shadow IT and Cisco Cloud Consumption Professional 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.

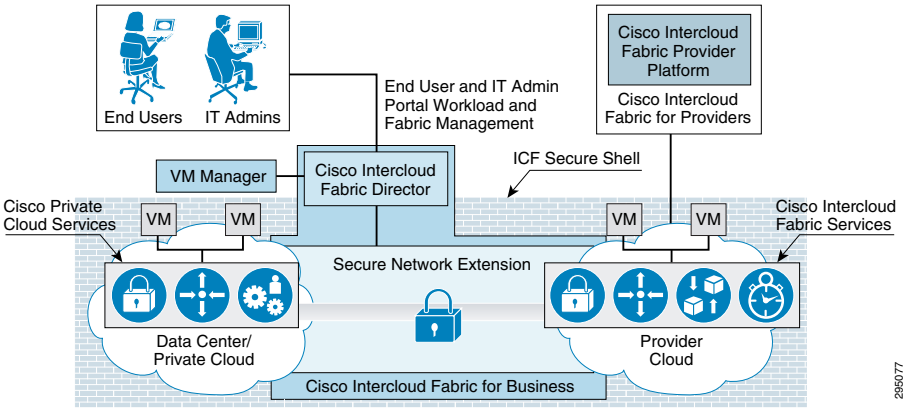
- Return the workloads to IT management by deploying Cisco Intercloud Fabric and integrate the solution with the organization's existing infrastructure and tools; this approach supports a simple, highly secure hybrid cloud integration plan.
- Continue using Cisco Cloud Consumption services to track public cloud use.

CHAPTER 2

Cisco Intercloud Fabric Architectural Overview

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

Figure 2-1 Cisco Intercloud Fabric Solution Overview



The Cisco Intercloud Fabric architecture provides two product configurations to address the following two consumption models:

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers

Cisco Intercloud Fabric for Business

Cisco Intercloud Fabric for Business 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 Fabric for Business consists of the following components:

- Cisco Intercloud Fabric Director
- Cisco Intercloud Fabric Secure Fabric

Cisco Intercloud Fabric 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 Fabric Director (ICFD) provides to the end user and IT administrator a seamless experience to create and manage workloads across multiple clouds, it is the single point of management and consumption for hybrid cloud solutions.

Heterogeneous cloud platforms are supported by Cisco ICFD 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 ICFD provides the required software development kit (SDK) and APIs to integrate with the various cloud infrastructure platforms.

Cisco ICFD 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. We discuss this later in the document.

Future releases of Cisco ICFD will include enhanced services that differentiate the Cisco Intercloud Fabric solution, such as bare-metal workload deployment in a hybrid cloud environment and an enhanced IT administrative portal with options to configure disaster recovery and other services.

Self-Service IT Portal and Service Catalog

The Cisco ICFD 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 ICFD provides a service catalog that combines offers from multiple clouds and a single self-service IT portal for hybrid workloads.

For IT administrators, Cisco ICFD 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; advanced policies are available in the management layer.
- Customize portal branding.
- 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 Fabric Secure Extension management.
- Future capabilities can be added through the end-user or IT administrative portal.

Ease of Installation

Cisco ICFD 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 ICFD also improves Day 1 and Day 2 operations, making it easier to configure provider cloud access and manage the environment.

Cisco Intercloud Fabric Secure Extension

All data in motion is cryptographically isolated and encrypted within the Cisco Intercloud Fabric Secure Extender. This data includes traffic exchanged between the private and public clouds (site to site) and the virtual machines running in the cloud (VM to VM). 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 Fabric 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 Fabric Core Services

Cisco Intercloud Fabric includes a set of services that are crucial for customers to successfully manage their workloads across the hybrid cloud environment. These services are identified as Intercloud Fabric Core Services and can be described as follow:

- **Cloud Security**—security enforcement for site to site and VM to VM communications.
- **Networking**—switching, routing and other advanced network-based capabilities.
- **VM Portability**—VM format conversion and mobility.
- **Management and Visibility**—hybrid cloud monitoring capabilities.
- **Automation**—VM lifecycle management, automated operations and programmatic API.

Future releases of Cisco Intercloud Fabric will include an extended set of services, including support for 3rd party appliances.

Cisco Intercloud Fabric Firewall Services

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 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 Fabric Routing Services

Cisco Intercloud Fabric Secure Extender 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 Fabric 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 the cloud by Intercloud 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 Secure Intercloud Fabric Shell

Cisco Secure Intercloud Fabric Shell (Secure ICF Shell) is a high level construct that identifies a group of VMs and the associated Cloud Profiles, and it is designed to be portable and secure across clouds. A cloud profile includes the following configurations:

- **Workload Policies**—a set of policies that are created by the enterprise IT admin via Intercloud Fabric Director portal to define what networks will be extend, security enforcements to be applied to the workloads in the cloud, and other characteristics such as DNS configuration.
- **Definition of the Site-to-Site and VM to VM Secure Communication**—IT admins can manage, enable, or disable secure tunnel configurations between the private and public clouds and/or between the VMs in the cloud.

- **VM Identity**—Intercloud Fabric creates an identity for all the VMs that it manages to ensure only trusted VMs are allowed to participate of the networks extended to the cloud, communicate to other VMs in the same circle of trust in the public cloud, or to communicate to other VMs in the private cloud.
- **Cloud VM Access Control**—Intercloud Fabric helps to control the access to the cloud VMs via the secure tunnel established between private and public clouds, or directly via the VM public IP defined and managed via Intercloud Fabric.

Cisco Intercloud Fabric for Providers

Cisco Intercloud Fabric for Providers is intended for provider 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. There are two Cisco Intercloud Fabric offers for providers; those who offer managed services, or those who are just targets for Intercloud Fabric hybrid workloads. Cisco Intercloud Fabric for Providers that want to offer managed services consists of the following components:

- Cisco Intercloud Fabric Director
- Cisco Intercloud Fabric Secure Fabric
- Cisco Intercloud Fabric Provider Platform

Cisco Intercloud Fabric for Providers that want to just be a target for Intercloud Fabric hybrid workloads consists of the following component:

- Cisco Intercloud Fabric Provider Platform

Cisco Intercloud Fabric Provider Platform

Cisco Intercloud Fabric Provider Platform (ICFPP) 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 ICFPP provides an extensible adapter framework to allow integration with a variety of provider cloud infrastructure management platforms, such as OpenStack, Cloudstack, VMware vCloud Director and virtually any other APIs that can be integrated through an SDK provided by Cisco.

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 ICFPP abstracts this complexity and translates Cisco Intercloud 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 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 ICFPP, 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 Fabric.

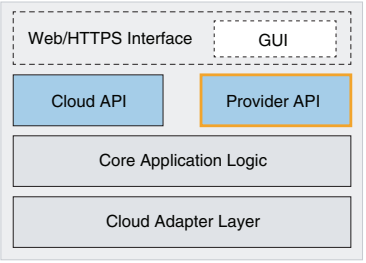
As the interface between the Cisco Intercloud Fabric from customers' cloud environments and provider clouds (public and virtual private clouds), Cisco ICFPP provides a variety of benefits, as described below:

- Brings standardization and uniformity to cloud APIs, making it easier for Cisco Intercloud Fabric to consume cloud services from service providers that are part of the Cisco Intercloud Fabric 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 existing management platforms.
- Supports multitenancy.
- Provides tenant-level resource monitoring.
- In the future, it will help build Cisco infrastructure-specific differentiation.
- In the future, support will be provided for enterprises to deploy bare-metal workloads in the provider cloud.

Cisco ICFPP Architecture

Cisco ICFPP is a virtual appliance deployed in the service provider cloud data center to enable service provider customers to access cloud resources using Cisco Intercloud Fabric APIs. The virtual appliance provides a virtual network interface to allow customers' Cisco Intercloud Fabric to reach the Cisco ICFPP appliance instance from public networks, and to allow the Cisco ICFPP appliance to connect with the service provider cloud platforms. Figure 2-2 shows the Cisco ICFPP appliance architecture.

Figure 2-2 Cisco Intercloud Fabric Provider Platform Architecture



Cisco ICFPP architecture includes four major interface modules:

- **Northbound Cloud API**—This module implements the Cisco Intercloud Fabric cloud API, which is consumed by Cisco Intercloud Fabric (customer cloud) for workload provisioning.
- **Northbound Provider API**—This module implements a set of APIs for the service provider administrator to use to configure the Cisco ICFPP appliance, provision tenants and users, and monitor tenant operations.
- **Core Application Logic**—This module implements translation logic between Cisco Intercloud Fabric cloud APIs and cloud platform-specific APIs.
- **Cloud Adapter Layer**—This module implements the various cloud platform interface adapters, each of which is responsible for interfacing with a specific cloud platform such as OpenStack, Cloudstack, or custom.

When to Deploy Cisco ICFPP?

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

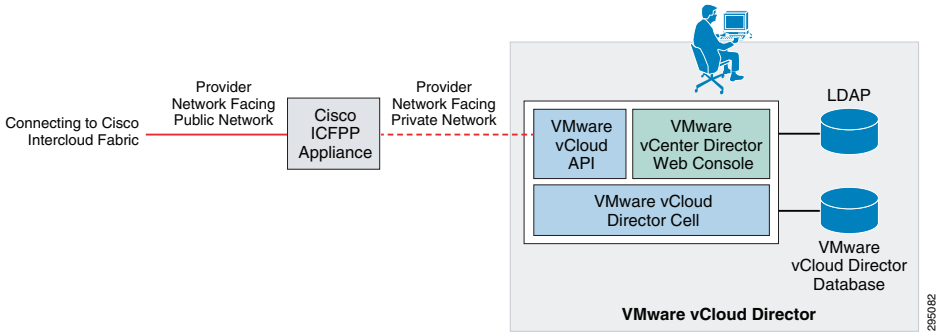
Cisco ICFPP Deployment Topology

To access the service provider's cloud resources, Cisco Intercloud Fabric needs to access the Cisco ICFPP appliance from the public network; therefore, the network interface of the appliance needs to be deployed in a provider network that is exposed to the service provider's edge router. The network interface needs also to connect to the private provider network that accesses the service provider cloud platform (for example, OpenStack or Cloudstack).

The Cisco ICFPP deployment topology varies for different service providers and cloud platforms.

Figure 2-3 shows a deployment with a VMware vCloud Director environment in the service provider.

Figure 2-3 Cisco ICFPP Appliance Deployment Topology



The Cisco ICFPP appliance uses HTTPS connections to communicate with the Cisco Intercloud Fabric and the service provider cloud platform. A firewall is not required in the network path between the Cisco Intercloud Fabric and the Cisco ICFPP appliance, or between the Cisco ICFPP appliance and the cloud platform endpoints, but can be used to reinforce only expected traffic flows to and from ICFPP.

Cisco ICFPP Operating Model

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

Day 0 Operation: Deployment and Initialization

The Cisco ICFPP 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
- 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 ICFPP 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 ICFPP 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 Fabric component can start to access the Cisco ICFPP appliance with a sign-on API request.

Cisco Intercloud Fabric and Cisco Validated Designs

For Cisco Powered Cloud Providers or large enterprise customers that deploy VMDC (Virtualized Multiservice Data Center) validated design, Intercloud Fabric is complementary to it and does not have dependency on specific configuration or version. For cloud providers, Cisco Intercloud Fabric for Provider can integrate with the cloud management platform of choice, and for large enterprise VMDC customers, Intercloud Fabric for Business also integrates with the environment, interfacing with the VM Manager and the cloud management platform of choice, if needed, allowing workload mobility and management across multiple clouds.

For customers that deploy FlexPod or other Cisco Validated Designs in their data centers, and are willing to securely move and manage their workloads across multiple clouds, Intercloud Fabric for Business complements the solution and augment its value with the capabilities discussed previously in this document. Intercloud Fabric for Business interfaces with the VM Manager of the converged infrastructure and provides all the resources needed to manage the workload in hybrid cloud environment.

Cisco Intercloud Fabric and Management Cloud Platforms Integration

The seemingly borderless environment created by Cisco Intercloud Fabric between private and public resources provides numerous features and benefits. To also provide the benefits of automated placement decisions for cloud services, application visibility and orchestration, application blueprints or deployment profiles, enterprises can use a management cloud platform of choice integrated with Cisco Intercloud Fabric through its Northbound APIs.

The management cloud platform connects to Cisco ICFD through the available northbound REST (Representational State Transfer) API, which enables it to perform operations on ICFD resources and to integrate with upstream portal and orchestration systems. As of today, ICFD supports the following API operations:

- Policy Management
- VDC Management
- Catalog Operations
- Charge-Back Management
- Workflow Management
- Auditing Management
- Virtual Machine Operations

Other API operations will be added in future releases of the product. Cisco ICFD REST API is compatible with HTTP and HTTPS protocols, and supports code formatted in JSON and XML. A Java API is also available. The APIs document is available at cisco.com/go/intercloudfabric.

Conclusion

Cisco Intercloud Fabric 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 Fabric allows the creation of workload policies that mirror business needs, with flexibility and enterprise-level security built in. Cisco Intercloud Fabric 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 Fabric 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).

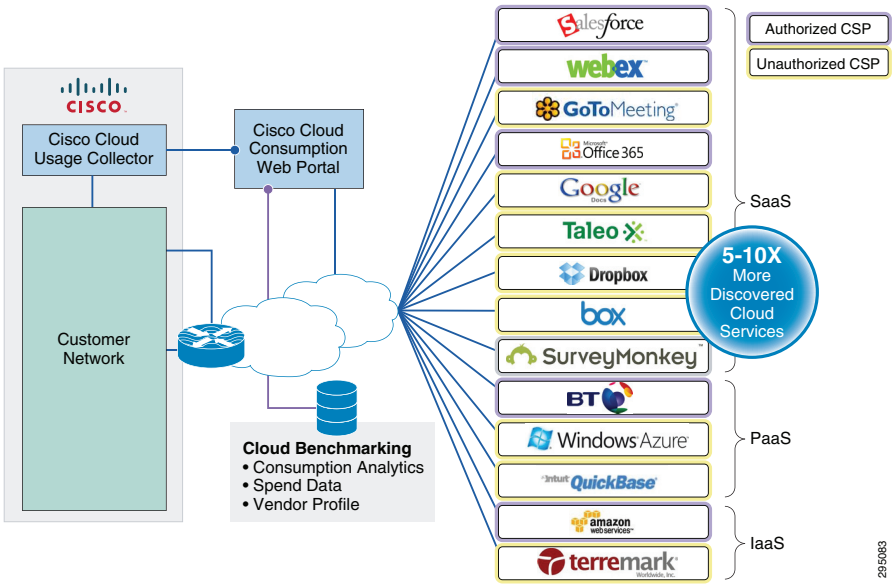
Shadow IT presents a new set of challenges for business and IT leaders, including how to manage the costs and risks associated with cloud adoption and how to establish effective cloud management processes.

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 enterprise-wide 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 Fabric solution through Cisco Advanced Services, but in future releases this offering will be fully incorporated into the product.