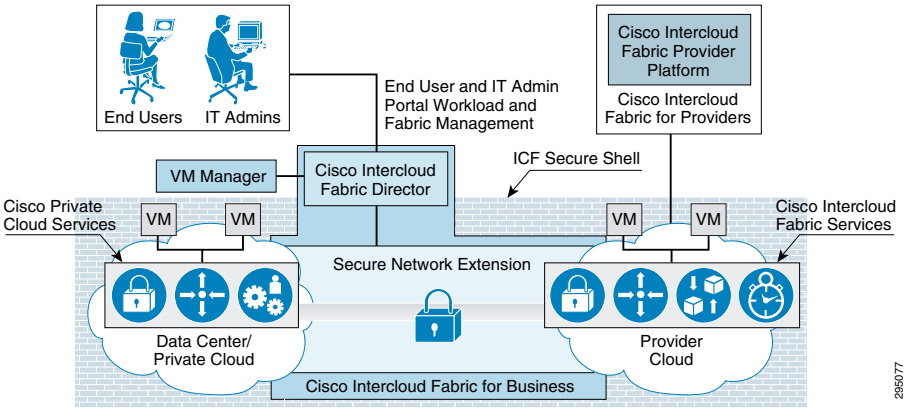
CHAPTER 2

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.

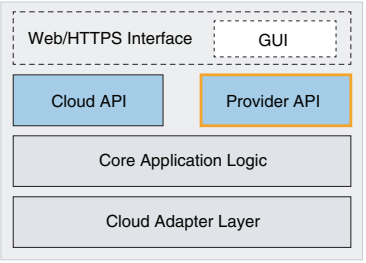
As the interface between the Cisco Intercloud Fabric from customers' cloud environments and provider clouds (public and virtual private clouds), Cisco ICFPP provides a variety of benefits, as described below:

- 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.

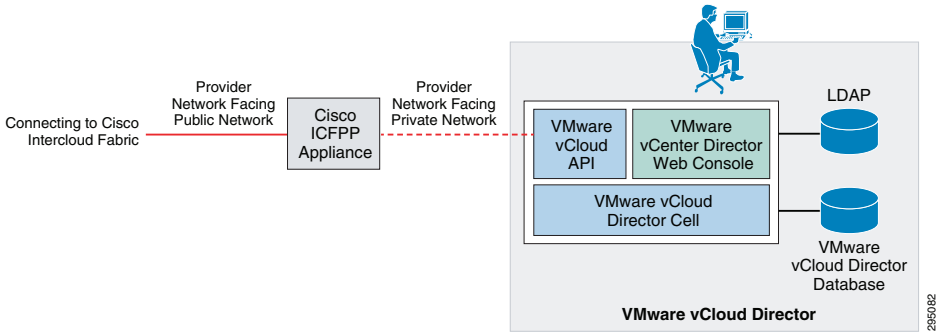
Cisco ICFPP Deployment Topology

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.