Overview

Cisco Intercloud Fabric

Cisco Intercloud Fabric offers two product configurations that address the following business needs:

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

This document describes how to install, configure, and start working with Cisco Intercloud Fabric for Providers. For information about Cisco Intercloud Fabric for Business, see the *Cisco Intercloud Fabric Getting Started Guide*.

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. Cisco Intercloud Fabric provides services for the following types of providers:

- Providers who offer managed services
- Providers who specialize in Intercloud Fabric hybrid workloads

For providers who offer managed services, Cisco Intercloud Fabric for Providers consists of the following components:

- Cisco Intercloud Fabric Provider Platform

- Cisco Intercloud Fabric Director
- Cisco Intercloud Fabric Extender

For providers who specialize in Intercloud Fabric hybrid workloads, Cisco Intercloud Fabric for Providers consists of the Cisco Intercloud Fabric Provider Platform component only.

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 enables cloud API support for service providers who currently do not have API support. Cisco ICFPP provides an extensible adapter framework that allows integration with a variety of provider cloud infrastructure management platforms, such as OpenStack, CloudStack, VMware vCloud Director, and any other API that can be integrated through an software development kit (SDK) provided by Cisco.

Currently, service providers have their own proprietary cloud APIs—such as Amazon EC2 and Windows Azure—that give customers limited choices and provide no easy method for moving from one provider to another. Cisco ICFPP abstracts this complexity and translates Cisco Intercloud Fabric cloud API calls to cloud platform APIs of different provider infrastructure platforms, giving customers the option of moving 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 manager's SDK or API, such as vCenter or System Center, which exposes the provider environment and is not a preferred option for service providers due to security concerns. Cisco ICFPP, as the first point of authentication for the customer cloud so that it can consume provider cloud resources, enforces highly secure access to the provider environment. In addition, it 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 customer cloud environments and provider clouds (public and virtual private clouds), Cisco ICFPP provides the following benefits:

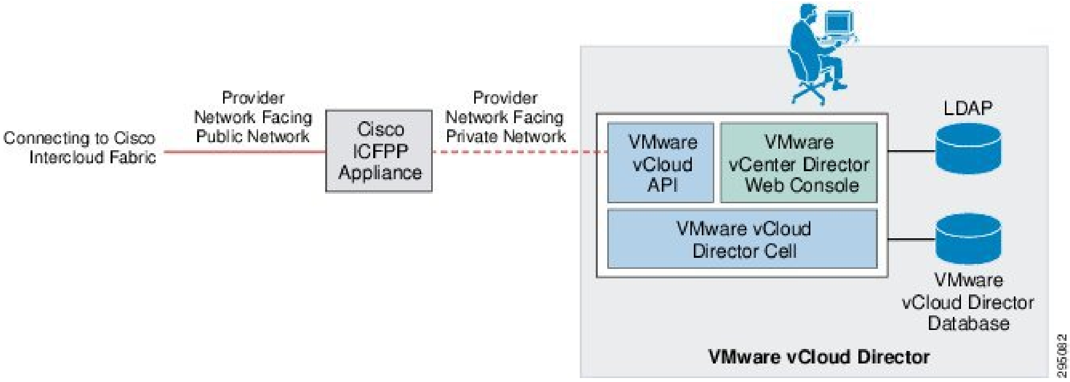
- Standardizes and brings uniformity to cloud APIs, making it easier for Cisco Intercloud Fabric to consume cloud services from service providers that are part of the Cisco Intercloud Fabric ecosystem.
- Helps secure access to a service provider's underlying cloud platform.
- Limits the utilization rate per customer or tenant environment.
- Provides northbound APIs for service providers for integration with existing management platforms.
- Supports multitenancy.
- Monitors resource usage per tenant.
- Meters resource usage per tenant.

Cisco ICFPP Deployment Topology

To access a service provider's cloud resources, Cisco Intercloud Fabric must access the Cisco ICFPP virtual appliance from the public network. To do this, the network interface of the appliance must be deployed on a provider network that is exposed to the service provider's edge router. The network interface of the appliance must also connect to the private provider network that accesses the service provider cloud platform, such as OpenStack or CloudStack.

The Cisco ICFPP deployment topology varies for different service providers and cloud platforms. The following figure shows a standalone deployment with a VMware vCloud Director environment in the service provider. For deployment in a multiple-node cluster, a load balancer in the service provider environment is required to support the cluster configuration.

Figure 1: Cisco ICFPP Appliance Deployment Topology


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

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

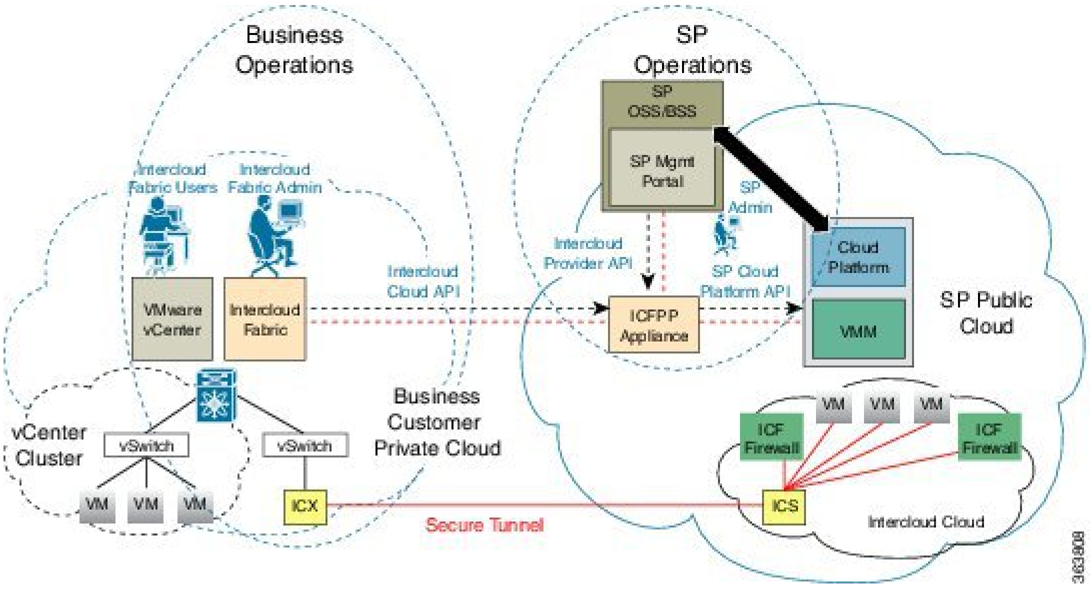
Cisco ICFPP Operational Model

The Cisco ICFPP operational model consists of two main operational stages:

- Service provider operations—Operations performed in the service provider data center by a service provider administrator. These operations primarily involve installing and configuring Cisco ICFPP and provisioning tenant-related information to Cisco ICFPP.
- Business operations—Operations performed in a private data center environment by a Cisco Intercloud Fabric administrator and end users of the Cisco Intercloud Fabric solution. These operations are usually performed after Cisco ICFPP has been deployed and activated in the service provider data center. For example, queries related to metering and usage are are considered part of business operations.

The following figure illustrates the Cisco ICFPP operational model and stages.

Figure 2: Cisco ICFPP Operational Model and Stages



The following sections summarize the operations that constitute these two stages.

Service Provider Operation—Deployment and Initialization

The Cisco ICFPP virtual appliance is deployed in the service provider data center as part of the service provider cloud platform. The service provider administrator configures the virtual appliance with the following information:

- Appliance IP addresses
- SSL server and client configurations
- Initial administrator user credentials and privileges

Next, the service provider administrator adds instances of the cloud platform with which Cisco ICFPP will interface. These cloud platform instances can be assigned to tenants during tenant on-boarding. The following information is required for each cloud platform instance:

- Cloud platform type, such as Cisco Cloud Services
- Cloud platform endpoint IP address and port number
- Service provider administrator or tenant credentials for sign-on with a cloud platform

Service Provider Operation—Tenant On-Boarding

Cisco ICFPP supports multiple tenants concurrently. To enable a tenant on Cisco ICFPP, the service provider administrator must provide the following tenant-specific information on the virtual appliance:

- The cloud platform instance that is assigned to the tenant
- The *resources domain* (a predefined set of resources) that is assigned to the tenant

- Tenant credentials, such as the API key, which is used by Cisco ICFPP to sign a tenant onto the service provider cloud platform. Tenant credentials can be generated by the service provider management portal when the tenant is registered to a cloud account.
- Tenant account username, which is used to identify the tenant-specific record

The same process is used for both adding new tenants and updating existing tenants on Cisco ICFPP. After the Cisco ICFPP virtual appliance is deployed and tenants are provisioned, the service provider administrator must ensure that the Cisco ICFPP virtual appliance DNS information is published to the enterprise customer's portal so that the tenants can reach Cisco ICFPP through the Internet.

Business Operation—Cisco Intercloud Fabric Director Sign-On with the Cisco Intercloud Fabric Provider Platform

With the Cisco ICFPP virtual appliance DNS information and tenant credentials, the Cisco Intercloud Fabric Director (ICFD) administrator can sign on with Cisco ICFPP to start an ICFD-ICFPP management session. Before an ICFD end user can use the ICFD self-service portal, the ICFD administrator must set up the Secure Cloud Extension to extend tenant on-premises networks to the service provider cloud.

Business Operation—Setting Up the Secure Cloud Extension

With an established ICFD-ICFPP management session, the ICFD administrator can issue Intercloud Cloud Orchestration APIs to set up the Secure Cloud Extension for extending the tenant's enterprise network and demanded service appliances, such as virtual firewall and virtual routing services. The Secure Cloud Extension provides ICFD end users with a hybrid infrastructure, which allows the preservation of workload network identities and ensures that the workload security policy is persisted across private and public clouds.

The Secure Cloud Extension has several virtual appliance components that run in the provider cloud. These components consist of the Intercloud Fabric Switch (ICS), ICF Router (CSR), and Intercloud Fabric Firewall (also known as Virtual Security Gateway). As a part of the Secure Cloud Extension deployment, ICFD works with Cisco ICFPP to upload the appliance images to the public cloud, instantiate appliance instances, and bring up the entire ICF infrastructure.

Business Operation—Cloud Provisioning and Virtual Machine Life-Cycle Management

When a Secure Cloud Extension instance is established, ICFD provides different portals for ICFD administrators and end users. Administrators and users can use their respective portals to provision or migrate workloads to public clouds and manage workloads with virtual machine life-cycle management interfaces that are provided by the portals.

In addition to supporting cloud orchestration API requests that are issued by ICFD, Cisco ICFPP meters tenant resource usage and monitors tenant resources so that service providers can manage hybrid cloud services.

For more information, see the available data sheets and white papers on cisco.com at http://www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/white-paper-listing.html.