Cisco Intercloud Fabric Security Features: Technical Overview

White Paper

May 2015

Contents

What You Will Learn

This white paper describes the security features of the Cisco Intercloud Fabric™ solution and how it helps users create a secure hybrid cloud infrastructure.

For most organizations, security is a critical concern when using public clouds. Cisco Intercloud Fabric provides users with the same level of security in the public cloud they have in their own data center. The solution lets users build secure hybrid clouds that extend their existing data center infrastructure to public clouds as needed and on demand, take advantage of flexible capacity, and achieve lower costs and faster delivery of resources.

Introduction

Hybrid clouds are quickly becoming the new normal. National Institute of Standards and Technology (NIST) defines hybrid cloud as a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cisco Intercloud Fabric enables customers to build highly secure hybrid clouds and transparently extend their private cloud to public cloud environments, while keeping the same level of security across both environments.

Cisco Intercloud Fabric provides complete end-to-end security between public and private clouds, using the following capabilities:

- Secure site-to-site communication
- Cisco Intercloud Fabric secure shell
    - Trusted cloud VMs
    - Encrypted VM-to-VM communication
    - Controlled cloud VM access through cloud security groups
- Role-based access control (RBAC) on cloud resources.
- Zone-based firewall using Cisco Intercloud Fabric firewall (Cisco® Virtual Security Gateway [VSG])

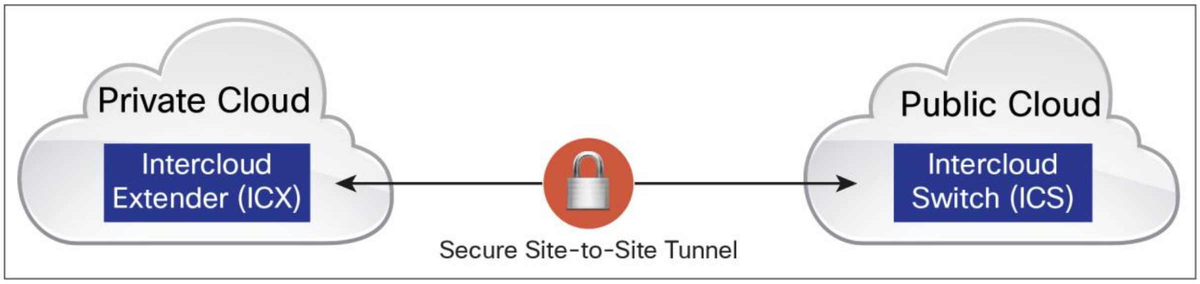
Secure Site-to-Site Communication

Cisco Intercloud Fabric creates a cryptographically isolated and encrypted tunnel to securely communicate between private and public clouds (Figure 1). It uses two VMs, a Cisco Intercloud™ Extender VM in the enterprise cloud, and a Cisco Intercloud Switch VM in the public cloud to create a secure tunnel between the two VMs as endpoints. This helps ensure that all network communications between private and public cloud sites are secure and encrypted.

The tunnel can be configured to be a Datagram Transport Layer Security (DTLS)/Transport Layer Security (TLS)/Hypertext Transport Protocol Secure (HTTPS) tunnel depending on customer choice of UDP/TCP/HTTP as the tunnel data transport protocol.

Key and certificate management is performed by the Cisco Intercloud Fabric Director software running in the private cloud. It is also possible to periodically refresh the keys from the director.

Figure 1. Secure Site-to-Site Tunnel Architecture



The TCP/UDP ports listed in Table 1 are used for the secure tunnel data and control traffic.

Table 1. TCP and UDP Ports

Transport Protocol	Ports
TCP	TCP 6646 (data), TCP 6644 (control)
UDP	UDP 6644 (data), TCP 6644 (control)
HTTPS	TCP 443

If there is a firewall protecting access to the internal network, the ports listed in Table 1 must be opened.

- 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-CBC, AES-256-CBC, AES-128-GCM, and AES-256-GCM (Suite B) (not available with TCP protocol).

The supported hashing algorithms are SHA-1, SHA-256, and SHA-384.

Cisco Intercloud Fabric supports secure and encrypted communications between private and public clouds. Key and certificate management for the site-to-site tunnel is done by the director running in the private cloud. This secure site-to-site tunnel also provides Layer 2 extension of an enterprise network into the public cloud.

Cisco Intercloud Fabric Secure Shell

Cisco Intercloud Fabric creates a secure shell around all public cloud VMs that are a part of the solution. This secure shell is created with multiple levels of security, including preshared Secure Shell (SSH) and tunnel keys, creating encrypted tunnels for VM-to-VM traffic in a public cloud and the ability to limit access to cloud VMs using cloud security groups.

The following sections provide details about the security mechanisms of the secure shell.

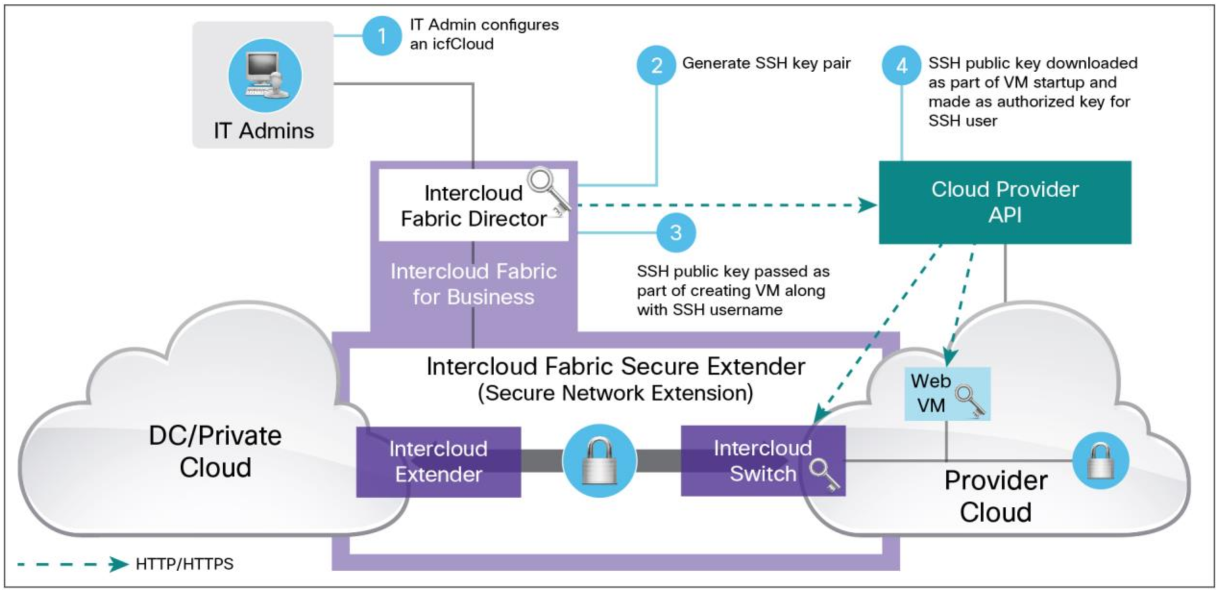
Trusted Cloud VMs

Cisco Intercloud Fabric makes sure that every cloud VM that is a part of the secure shell is trusted. This trust is created via preshared SSH keys (Figure 2).

Each time an IT admin creates an intercloud fabric cloud link, an SSH key pair is generated by the Cisco Intercloud Fabric Director in the private cloud. The SSH public key and the SSH username is passed onto every VM that is deployed or migrated in the public cloud. This makes each cloud VM instantiated or migrated with the director trusted. Only VMs with this SSH key are accessed by the director and can be used to create a secure tunnel with an intercloud switch. Since SSH keys are generated by the director in the enterprise, the enterprise has full control of these keys.

Today, different cloud providers have different ways of generating and managing SSH key pairs for instances running on public clouds. Cisco Intercloud Fabric solves this issue by providing a consistent approach to creating and distributing SSH keys over supported public cloud providers.

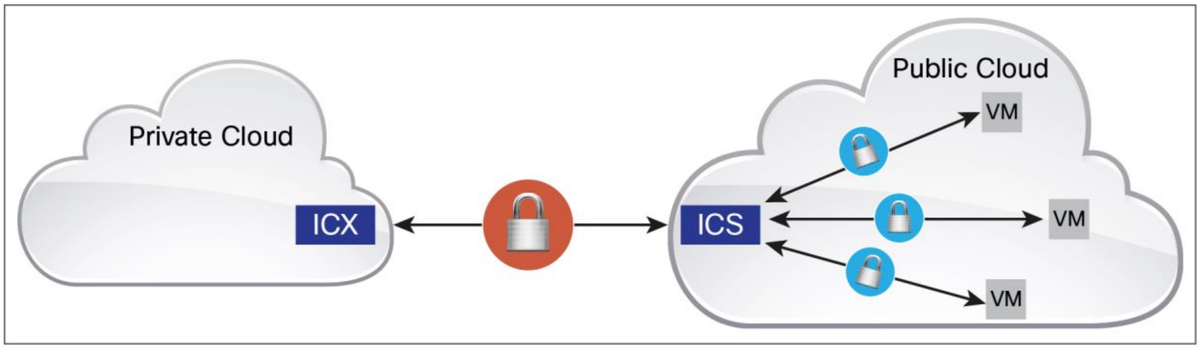
Figure 2. Trusted Cloud VMs


1 IT Admin configures an icfCloud
IT Admins
2 Generate SSH key pair
4 SSH public key downloaded as part of VM startup and made as authorized key for SSH user
Intercloud Fabric Director
Cloud Provider API
3 SSH public key passed as part of creating VM along with SSH username
Intercloud Fabric for Business
Intercloud Fabric Secure Extender (Secure Network Extension)
Web VM
DC/Private Cloud
Intercloud Extender
Intercloud Switch
Provider Cloud
HTTP/HTTPS

Encrypted VM-to-VM Communication

Cisco Intercloud Fabric provides complete security for data in motion on public clouds. Each time a VM is instantiated or migrated in the public cloud, the Cisco Intercloud Fabric Director inserts preshared keys (PSKs) into the cloud VM. These keys are inserted via an SSH connection using SSH keys, as defined in the preceding ◦. Using these PSKs, an intercloud switch and the cloud VM authenticate each other to create a secure and encrypted access tunnel (Figure 3). All data in motion between VMs in the public cloud is carried over these secure and encrypted access tunnels. Since VMs external to the intercloud fabric infrastructure do not have access to these PSKs, they can’t create an access tunnel with the intercloud switch.

Figure 3. Encrypted VM-to-VM Communication



The access tunnel is a Datagram Transport Layer Security (DTLS) tunnel. The encryption algorithm used is configurable, and different encryption strengths can be used depending on the level of security desired.

Support for data-at-rest encryption via third-party vendors is being considered for future releases of Cisco Intercloud Fabric.

Controlled Cloud VM Access through Cloud Security Groups

Cisco Intercloud Fabric cloud security groups have the ability to limit access of cloud VM public interfaces to selected IP addresses defined in the cloud security group, typically in the enterprise public IP space.

Each cloud VM opens only the following inbound ports for end-points with IP addresses in the cloud security group:

- SSH port: TCP 22
- HTTPS port: TCP 443
- RDP port: TCP 3389
- Intercloud fabric tunnel ports: TCP 6644 and 6646
- Intercloud fabric tunnel ports: UDP 6644 and 6646

RBAC on Cloud Resources

The Cisco Intercloud Fabric Director offers role-based access control (RBAC) to limit access to cloud resources based on user role or group. The director provides an end-user portal and an IT admin portal based on the user role. An IT administrator can create different portals for different user groups and restrict the visibility and access of available cloud resources to appropriate users or user groups. The use case that follows shows an example of how to use the RBAC feature provided by the director.

Figure 4 shows a typical software company with multiple product development teams, test teams, finance teams, and more. Without Cisco Intercloud Fabric, administrators would have no control or visibility into the cloud resources used by each team. With Cisco Intercloud Fabric, an IT admin can create different portals for different teams, providing them access to appropriate cloud resources.

In Figure 5, an IT admin has created different portals for different teams. Product A team members get access to AWS for bursting onto public cloud, while the Product B team can create workloads in the Microsoft Azure public cloud. This capability gives IT admins control over the cloud resources available to teams or user groups.

Using Cisco Intercloud Fabric catalogs, IT admins can provide “IT certified” images to specific user groups to maintain control and make it easier for users to acquire certified workloads.

Figure 4. A Software Company with Multiple Teams

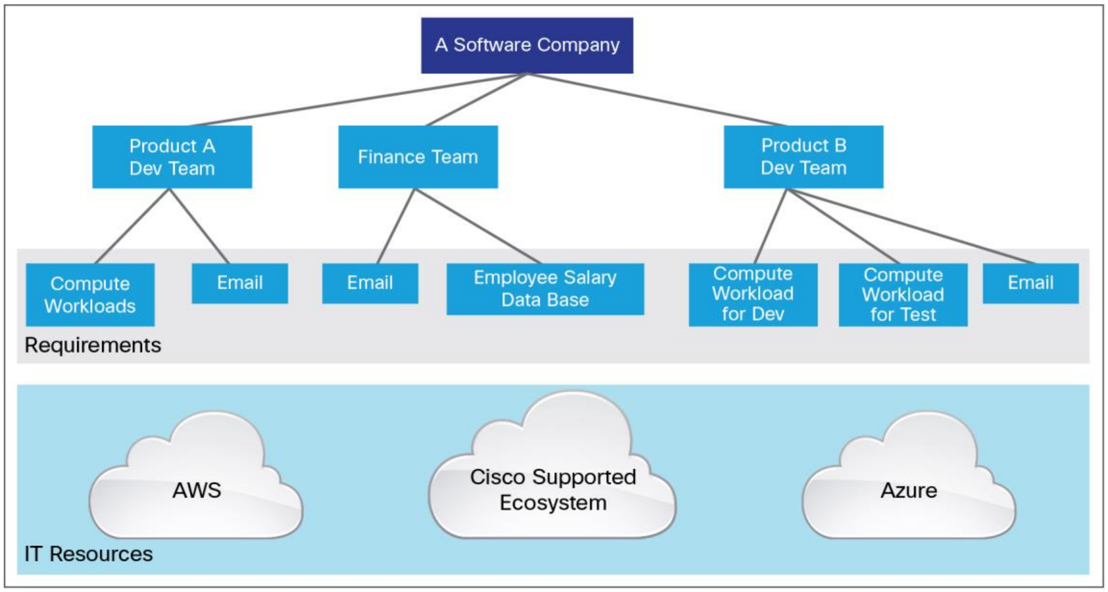
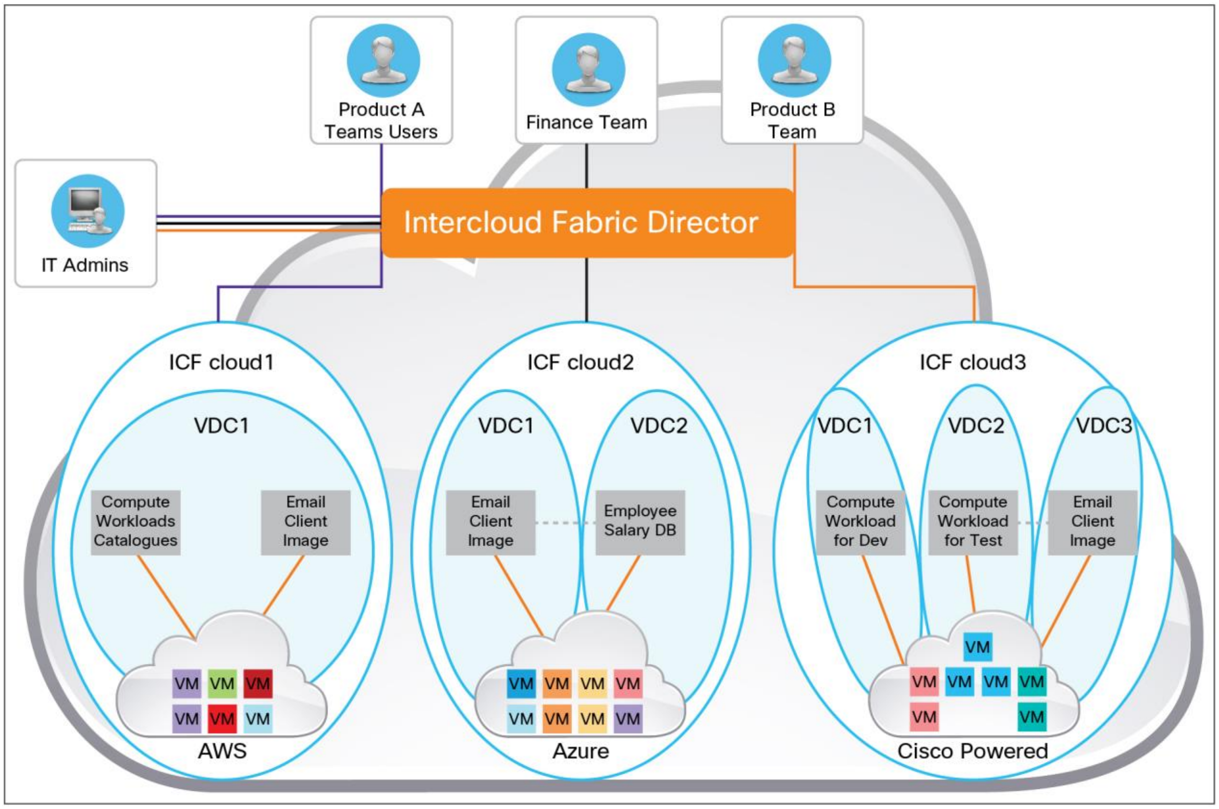


Figure 5. Admin Portal and Different End-User Portals Provided by Cisco Intercloud Fabric Director



Zone-Based Firewall Using Cisco Intercloud Fabric Firewall

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, the Cisco Virtual Security Gateway (VSG), which provides policy enforcement for communication between virtual machines and protects 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 VSG zone-based firewall include:

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

With VSG support in Cisco Intercloud Fabric, customers who use the VSG for the Cisco Nexus® 1000V Series Switch in their enterprise data center can extend the same policies to the VSG instance in the public cloud. This allows them to have consistent firewall policies across their entire hybrid cloud infrastructure.

Conclusion

Cisco Intercloud Fabric provides multiple layers of security for workloads running on public clouds. Encrypted site-to-site tunnels and access tunnels help ensure that all data in motion is secure. Every intercloud fabric cloud VM is secure and trusted through preinserted SSH and PSK keys, and the VSG firewall lets users define zoning and security policies with consistent policies in private and public clouds. With these capabilities, Cisco Intercloud Fabric provides complete end-to-end security for workloads running in a hybrid infrastructure.

For More Information

http://www.cisco.com/c/en/us/products/cloud-systems-management/intercloud-fabric/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-734535-00 05/15