SOLUTION OVERVIEW

Next-Generation Multi-Cloud Networking

F5 Distributed Cloud's multi-cloud networking solution offers an innovative networking and security service for public and/or private clouds. It relieves NetOps and DevOps teams from the struggle of managing multiple services and provides end-to-end policy and observability.

KEY BENEFITS

Faster deployments
Accelerate cloud migration or adoption of a new cloud provider using a consolidated service that delivers the same API, networking, and security capabilities across any cloud provider.

Productivity gains
Remove the friction from cloud networking with automated Infrastructure as Code, SaaS operations, lifecycle management, and intent-driven policies that empower self-service operations for DevOps and organization control for NetOps/SecOps.

Streamlined infrastructure operations
With cloud-native F5 Distributed Cloud Mesh nodes in your virtual private cloud (VPC) and the optional F5 Global Network, you deliver a secure multi-cloud network without worrying about complex network operations.

Enhanced functionality
NetOps teams can deploy Distributed Cloud Mesh in their services VPC and configure networking and security, while DevOps can configure DNS, load balancing, and API gateway.

Optional managed services
The F5 managed services engineering team can help your NetOps and DevOps teams design, implement, and test the most optimal and secure network within the cloud, multiple clouds, or hybrid clouds.

Organizations are accelerating migration to the public cloud to gain the simplicity and automation efficiencies promised by the cloud. Some enterprises are in the initial phases of adopting the public cloud starting with migrating simple applications. Many more enterprises are further along in their cloud migration journey and are dealing with migrating mission-critical apps to the cloud. Migrating crucial apps comes with its own set of challenges due to myriad enterprise IT requirements.

Still other organizations are in advanced phases where they face having to manage multiple public-cloud environments due to mergers and acquisitions or line of businesses wanting to use a specific cloud for various capabilities. Gartner has reported that 81% of the organizations responding to its 2020 global survey are already using two or more cloud providers.

In all these scenarios, infrastructure and operation teams face significant operational complexity with networking and security in the public cloud.

The infrastructure and operation teams could include multiple personas depending upon the size of the organization: Network Operations (NetOps), Security Operations (SecOps), and Developer Operations (DevOps).

NetOps typically are the site admins and oversee networking-related operations; SecOps manage the organization-wide infrastructure and application security operations, and DevOps handle the application-related networking and security operations. A large infrastructure and operations team might have all three personas, while a smaller team might have individuals performing all these roles at once.

These are pain points felt by NetOps teams:

- **Virtual edition appliances are not cloud-native:** Many enterprises adopted a lift-and-shift approach, using virtual edition (VE) versions of their on-premises networking and security appliances in the cloud. However, they soon realized that the virtual edition versions were not cloud-native and did not provide the automation and cost efficiencies expected from a cloud deployment.
- **Cloud networking skills gaps:** Next, they adopted the public cloud providers' products directly but ran into the problem of skills gaps in cloud networking technologies. Infrastructure and operations teams are used to managing appliances on-premises, with full control of networking and security. However, in the public cloud, they must begin dealing with cloud provider constructs such as transit gateway, VNet peering, availability zones, and more, due to the skills gaps. NetOps require automation and orchestration of cloud-provider constructs because a single cloud provider's networking and security constructs are often quite different from what they are used to on-premises.

KEY FEATURES

App- and API-centric connectivity
Deliver apps and APIs across clouds without exposing their networks.

Consolidated L3-L7 networking and security stack
Get consolidated L3 to L7 networking and security for unified cloud policies.

SaaS-based control plane and operations for lifecycle management
SaaS-based controller and analytics service enables end-to-end lifecycle management.

Global performant and high-capacity, cross-cloud backbone
Global backbone provides deterministic performance across clouds.

Rich observability and analytics
Single-pane-of-glass observability enables efficient monitoring of data and outputs across clouds, sites, and layers.

Extensible external security service insertion
Extensible solution with optional service insertion of F5 BIG-IP and third-party firewalls.

CLOUD NETWORKING IS OPERATIONALLY COMPLEX TO INFRASTRUCTURE AND OPERATIONS TEAMS BECAUSE OF SKILLS GAPS IN CLOUD, DIFFERENCES ACROSS THE CLOUD CONSTRUCTS, DISJOINTED OPERATIONS ACROSS MULTIPLE POINT PRODUCTS, AND FRACTURED VISIBILITY.

- **Lack of advanced networking and security controls:** Meanwhile, enterprises further along in their journey and seeking to migrate mission-critical apps to the cloud face a different problem: They do not have the same level of advanced networking and security controls that they are used to on-premises. For example, granular VPC-VPC traffic segmentation policy is difficult.
- **Operational complexity due to disjointed policies and configurations for multiple point products:** To achieve advanced networking and security, NetOps augment public cloud products with multiple point products for networking/routing and for firewalls. But these point product appliances have different operational models for policy and configurations, resulting in added complexity and inconsistent policies.

The challenges for SecOps include:

- **Complex integration with external security services:** SecOps would like to use the same products for security—such as a network firewall or application firewall—on the public cloud as they use on-premises. However, SecOps struggle with deploying and operating the product on the public cloud because of a lack of expertise with public cloud networking. Specifically, they struggle with:
  - Inserting security services in the traffic flow in a public cloud
  - Granular policies to steer traffic towards the security service for inspection

These are issues that DevOps teams encounter:

- **Siloed operational model:** The application architecture itself is changing from monolithic to microservices. DevOps teams need to operate clusters with back load balancers, API gateway, and service mesh technologies.
- **Hurry up and wait:** DevOps must operate clusters per team, per microservice, and per app, which often result in numerous load balancers and clusters to be managed. They cannot wait on NetOps to provision and connect their clusters, because it could span multiple iterations, negating the service velocity benefits of moving to microservices.
- **Seeking separate self-services:** NetOps and DevOps, therefore, seek self-service capabilities where NetOps teams are only responsible for configuring organization-wide policies (for example, apps in the ‘dev’ environment can’t talk to apps in ‘prod’ environment) while providing DevOps teams the ability to set up app-specific policies on their own.

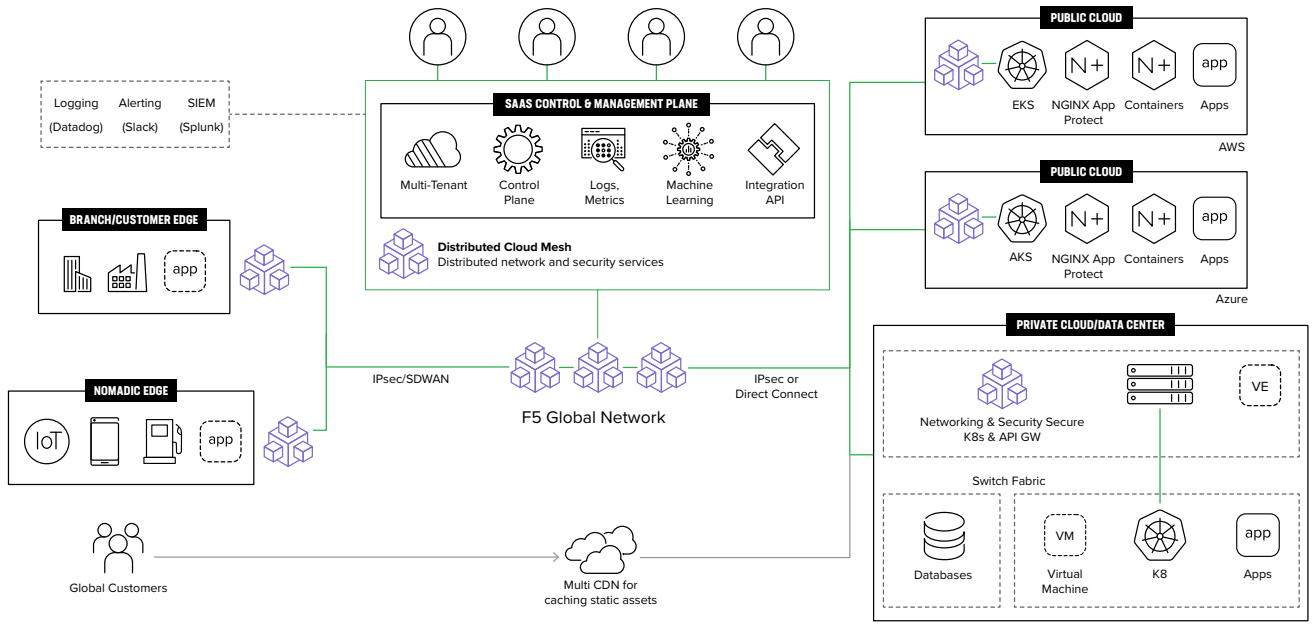
F5 Distributed Cloud Services: Seamless and Secure App-to-App Connectivity Across Clouds

F5® Distributed Cloud Services provide an innovative new multi-cloud networking offering that simplifies the operational complexity for NetOps, SecOps, and DevOps teams that manage multiple networking and security services in one or more clouds. Key features behind this simplification are unified end-to-end policy and granular observability.

F5 Distributed Cloud's multi-cloud networking solution includes:

- **F5® Distributed Cloud Mesh:** Our integrated stack of Layer 3 to Layer 7 networking and security services includes a virtual router, network firewall, distributed load balancer, application firewall, API gateway, and API Security. Distributed Cloud Mesh can be deployed in customers' private or public clouds, edge locations (including branch or retail stores or manufacturing facilities), and on the F5 Global Network.
- **F5® Distributed Cloud Console:** Distributed Cloud Console provides a single-pane-of-glass observability across multiple layers of the stack (L3-L7) as well as across multiple heterogeneous clouds.
- **F5 Global Network:** This high-performance global network provides 10+ Tbps capacity and consists of more than 23 points of presence (POPs), with new PoPs continually added. The multi-Tbps private backbone offers private peering to cloud and SaaS providers.

Figure 1: A reference architecture for F5's Multi-Cloud Networking solution



F5 DISTRIBUTED CLOUD SERVICES PROVIDE AN INNOVATIVE NEW MULTI-CLOUD NETWORKING OFFERING THAT SIMPLIFIES THE OPERATIONAL COMPLEXITY FOR NETOPS, SECOPS, AND DEVOPS TEAMS.

- **SaaS-based F5 Distributed Cloud Platform:** The F5 Distributed Cloud Platform is SaaS-delivered and provides a distributed control and management plane with end-to-end lifecycle management, AI/ML-powered analytics, and rich integrations with the ecosystem via APIs.

Here is how the F5 Distributed Cloud multi-cloud networking solution addresses the challenges faced by NetOps, SecOps, and DevOps teams.

- **Simplified operations with unified policies across clouds:** Distributed Cloud Mesh provides a unified operational model across multiple layers of the stack. The configuration model is the same across all layers of the stack—be it the routing layer, the load balancer layer, network firewall, or app firewall. Distributed Cloud Mesh can be deployed in any cloud providing unified app networking and security policy across clouds. The distributed control plane ensures that policies and configurations are defined once and distributed to all nodes deployed across multiple clouds. Distributed Cloud Console offers granular observability across all stack layers and all clouds, ensuring full visibility for operations teams.
- **Faster deployments via Infrastructure as Code automation and orchestration:** Distributed Cloud Mesh automates and orchestrates the configuration of a cloud provider's networking constructs (such as AWS Transit Gateway, VPC attachments, and VNet peering) by providing Infrastructure as Code, thereby reducing the configuration and management complexity of networking and security in the cloud. The automation and orchestration solve the cloud networking skills gap challenge, resulting in faster deployments. Distributed Cloud Mesh is built from the ground up using cloud-native methodologies leveraging the cloud provider's constructs such as availability zones, security groups, transit gateway, and VPC attachments. Mesh ensures the user is leveraging the best of each cloud, while automating and orchestrating the cloud constructs, simplifying operations, and accelerating deployments.
- **Granular networking and security controls:** Distributed Cloud Mesh provides granular networking and security controls for VPC-to-VPC traffic segmentation, and steering policies that are uniform across clouds. VPC-to-VPC traffic can be segmented per subnet, IP address, and port level instead of only at the VPC level. Distributed Cloud Mesh provides a flexible tagging mechanism (for example, dev, staging, or prod) or business groups (marketing, finance, dev) enabling operations teams to create policies that represent their business imperatives (e.g., apps in the dev environment are not allowed to talk to apps in prod environment).

YOU BENEFIT FROM OUR APP-TO-APP CENTRIC COMMUNICATION ACROSS CLOUDS, WITH UNIFIED POLICIES, SIMPLIFIED OPERATIONS, AND RICH OBSERVABILITY BACKED BY A HIGH-PERFORMANCE, HIGH-CAPACITY, AND PRIVATE CROSS-CLOUD BACKBONE.

- **Simple, flexible insertion of security services for advanced security control:** Distributed Cloud Mesh orchestrates the deployment of external security services across clouds, enabling SecOps and NetOps teams to use their security service of choice in the cloud. Distributed Cloud Mesh provides granular steering policies, at an IP address/port level, to determine which traffic needs to be inspected by the security service. Traffic steering policies can be defined using the flexible tagging mechanism, ensuring the policies are unified and consistent across clouds and represent the business imperative. Distributed Cloud Console offers rich observability across both Distributed Cloud Mesh and the external security service, enhancing visibility for the NetOps and SecOps teams.
- **App-centric architecture with a global multi-cloud backbone enables velocity for DevOps teams:** Distributed Cloud Mesh's proxy-based architecture enables DevOps to advertise apps across clouds without worrying about the underlying networking and routing infrastructure. The app-to-app centric global backbone enables DevOps to easily allow apps to communicate across clouds without requiring NetOps or DevOps to deal with cross-cloud connectivity providers. F5's high-capacity public network makes it effortless for DevOps to advertise applications publicly with a single click, with full network and app security protection on the network. Moreover, the F5 Global Network provides private connectivity across clouds and SaaS providers, enabling regulated enterprises to ensure end-to-end private connectivity for apps, clouds, and SaaS providers.
- **Multi-tenancy and network isolation:** The F5 Distributed Cloud Platform is multi-tenant, enabling NetOps to create workspaces for each DevOps team. So, DevOps can deploy Distributed Cloud Mesh in each of the clusters in self-service fashion without requiring any support from NetOps. Moreover, DevOps teams can manage their application-specific policies in their own workspaces, while NetOps teams still have the full visibility and control to enforce organization-wide policies. Distributed Cloud Mesh provides full network isolation across workspaces, ensuring that DevOps teams' applications are isolated from each other but with the flexibility to allow policies for cross-workspace communication.

In summary, the F5 Distributed Cloud's multi-cloud networking solution offers these differentiators:

- Delivers apps and APIs across clouds without exposing their networks
- Consolidates L3 to L7 networking and security for unified cloud policies
- Features a SaaS-based controller and analytics service for lifecycle management
- Includes a global backbone providing deterministic performance across clouds
- It is extensible, with the service insertion of F5 BIG-IP and third-party firewalls

You benefit from our app-to-app centric communication across clouds, with unified policies, simplified operations, and rich observability backed by a high-performance, high-capacity, and private cross-cloud backbone.

Figure 2: A look at multi-cloud networking features from the F5 Distributed Cloud Platform vs. competing solutions

Features	Other Solutions	Distributed Cloud Mesh
Consolidated L3-L7+ networking + security service	x	✓
Multi-tenancy + self-service for NetOps and DevOps	x	✓
Multi-layer security	x	✓
App-to-App without exposing underlying network	x	✓
Global physical network	x	✓
Security Service Insertion	✓	✓
Automation assistance for NetOps	✓	✓
Observability and analytics	External	✓
Lifecycle management	Controller	SaaS

Use Cases

Four important use cases for multi-cloud networking from F5 Distributed Cloud Services:

1. Multi-Cloud Transit

With its multi-cloud transit capabilities, Distributed Cloud Mesh delivers seamless and secure networking into any cloud. It connects multiple clouds securely with a choice of physical transit: Over the Internet, over your own private backbone, or via the F5 Global Network. F5 Distributed Cloud Console, the control plane of the solution, is a SaaS-based operations and observability portal to manage infrastructure and apps across public and private clouds and edge sites.

The F5 Distributed Cloud Platform provides:

- A SaaS-based control plane to simplify multi-cloud networking
- A highly automated, fast, redundant, secure connections between sites

- Integrated L3-L7 networking and security
- Orchestration and automation of each cloud provider's networking and security constructs
- A single source of truth for network, security, and application health and performance across all clouds
- Multiple connectivity options for greenfield or existing environments, including the F5 global network fiber backbone, customer-provided network, or fully automated site-to-site IPsec/SSL virtual private networks

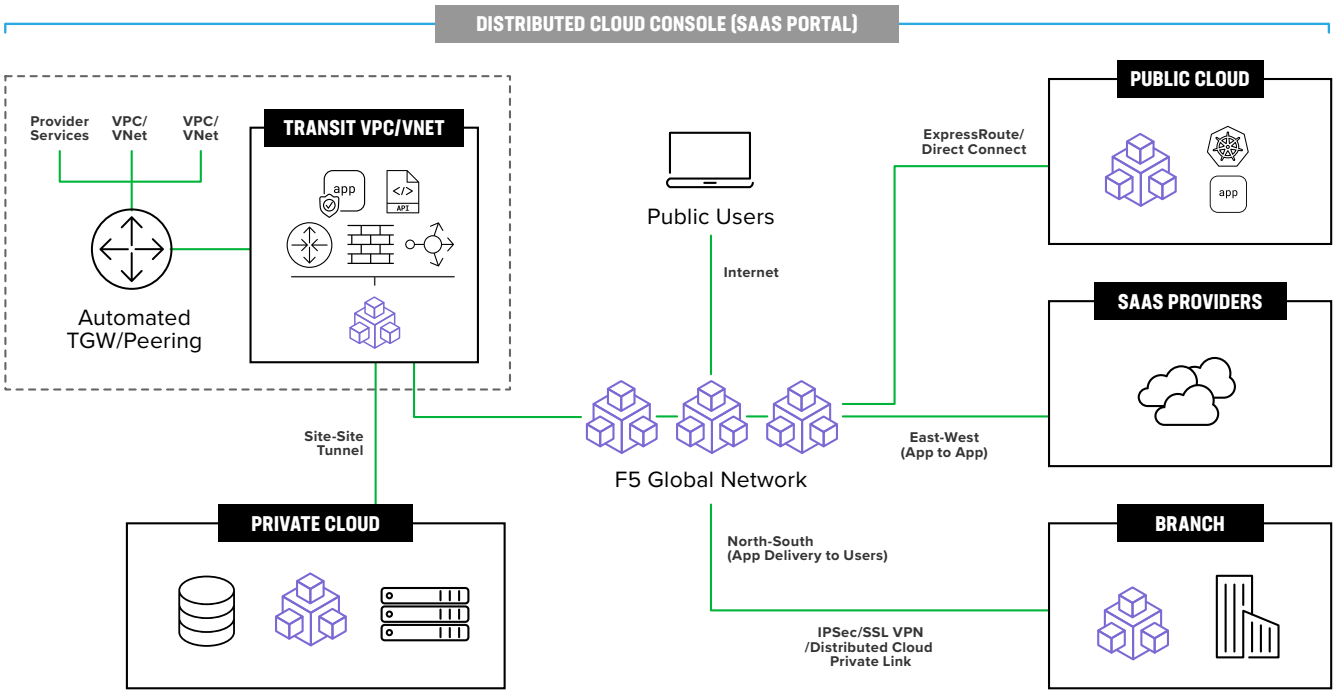


Figure 3: A visual look at how multi-cloud transit works inside Distributed Cloud Mesh

2. Security Service Insertion

With Distributed Cloud Mesh and Distributed Cloud Console, customers have the option of inserting F5® BIG-IP product(s) or other third-party security services, so SecOps teams can extend their security service controls across all private and public clouds—protecting their investment in existing skill sets and policies.

Distributed Cloud Mesh simplifies where and how to apply the security services with cloud-agnostic traffic steering rules, which reroute network traffic from virtual cloud networks through the security service, then to the destination, using the same steering rules across different public and private clouds. Using F5 Distributed Cloud Console, IT pros get granular visibility and single-pane-of-glass traffic management across clouds and networks.

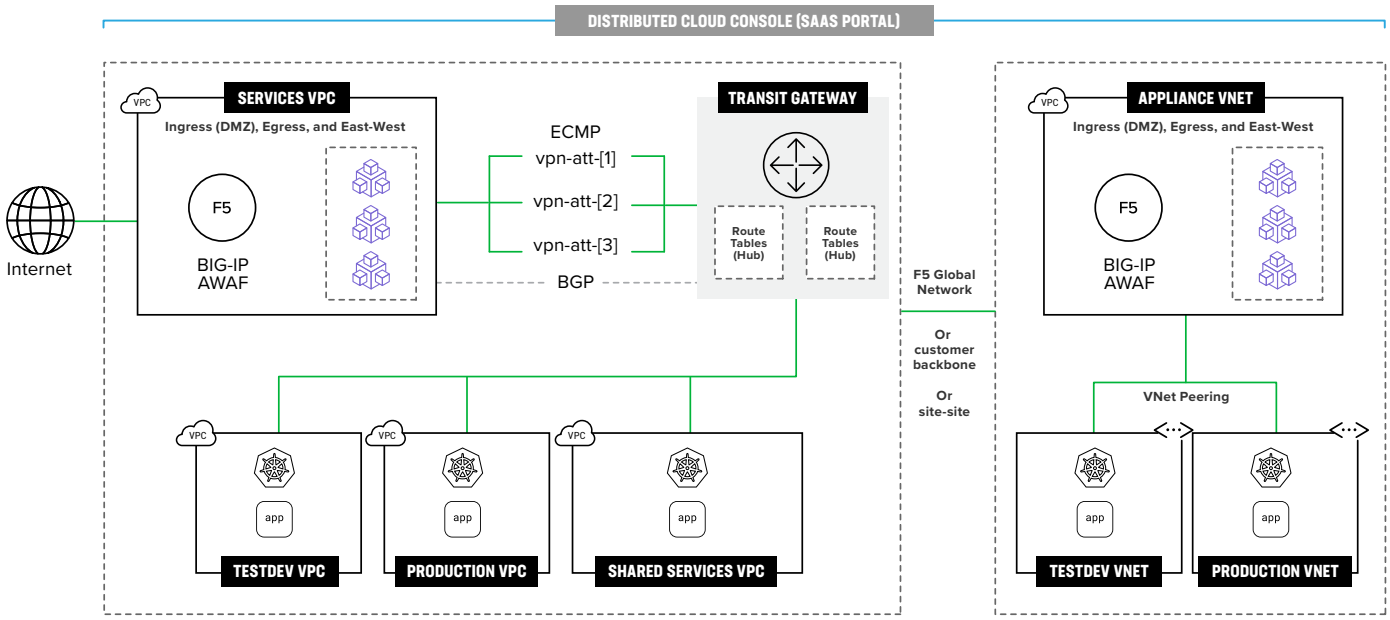


Figure 4: A visual look at the security services insertion use case

3. Multi-Cluster App Mesh

Multi-cluster app mesh enables applications and APIs to be advertised across a customer's public or private clouds and on the F5 Global Network without fine-grained control, and without worrying about the underlying networking and routing. Application services hosted in one cluster can be exported and advertised in other local or remote clusters across clouds, transparently allowing distributed apps to cross-connect. As Distributed Cloud Mesh delivers the services, it also monitors them and applies full-stack advanced security, providing solid assurance that any security holes are eliminated.

This use case applies both to Kubernetes and to traditional virtual machines and container environments. Distributed Cloud Mesh can connect natively to Kubernetes to discover services, advertise specific services to remote clusters across clouds, and distribute security policies across clouds to protect the advertised services.

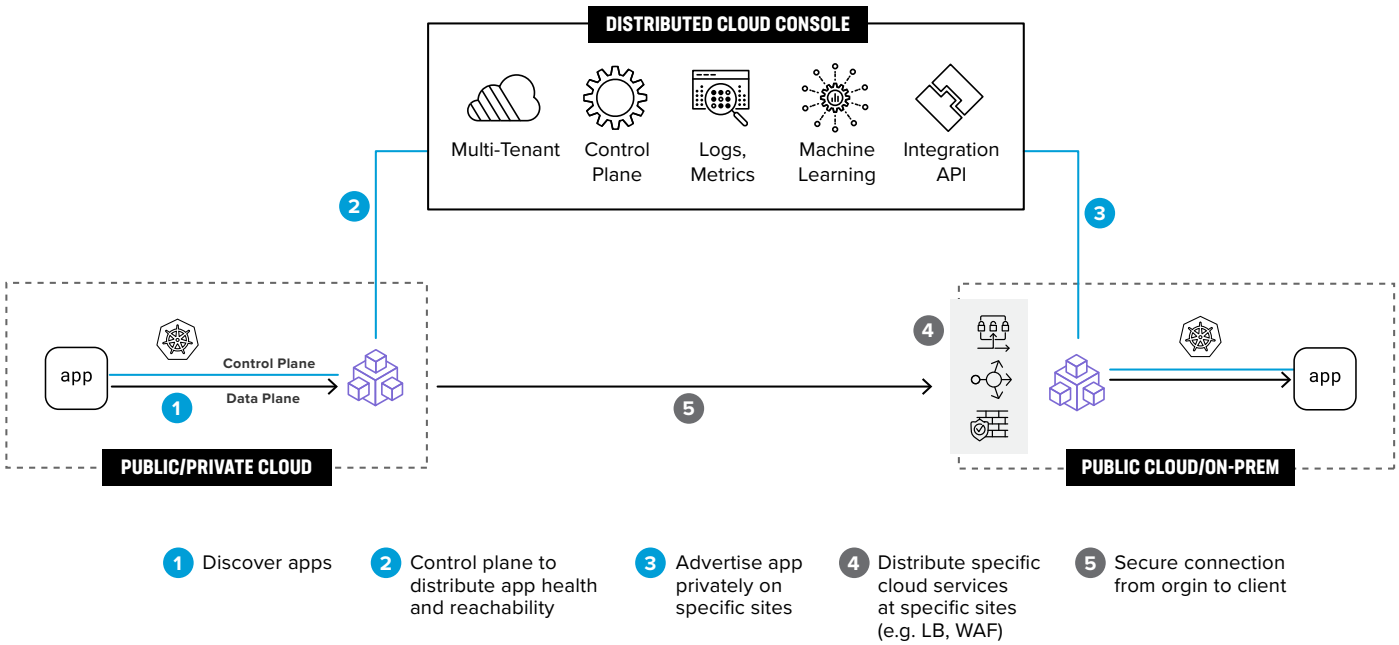


Figure 5: A visual look at multi-cluster app mesh, provided in Distributed Cloud Mesh

4. IP Address Overlap

Distributed Cloud Mesh provides a clean solution to IP overlap because of its proxy-based architecture. Overlap is only an issue when connections strictly on the underlying networks are exposed. Distributed Cloud Mesh enables services to be advertised at Layer 7 across clusters, without relying on the underlying Layer 3 network being exposed. Therefore, the Layer 3 network can have overlapping IPs, but the service can still be advertised across clusters.

Using Distributed Cloud Mesh, it is even possible to deliver a remote service—whatever its real IP address—into a local subnet, with a local IP address. So, there are no network changes required at all: no network address translation (NAT), no firewall pinholes, and no routing changes. Distributed Cloud Mesh provides full control and full visibility without network disruption, for the cleanest possible IP overlap solution.

Test-drive the multi-cloud networking solution for free or check out other options. For more information, visit the Multi-Cloud Networking webpage on F5.com.