SOLUTION OVERVIEW

Next-Generation Multi-Cloud Networking

The F5® Distributed Cloud 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

Operational simplification for lower cost and complexity
Reduce effort and lower TCO with centralized management and an integrated service stack for uniform services and policy across all clouds and premises.

Agility for faster provisioning and deployment
Accelerate cloud migration and app deployment with automated provisioning of links and network services, centrally controlled and globally orchestrated for safe self-service within policy.

Integrated security to protect and inspect all networks
Native integration and automation of routing, access, segmentation, and F5 or third-party security services to abstract network complexity and accelerate deployment.

End-to-end visibility across clouds, data centers, and edge
Gain continuous and consistent centralized network visibility with drill down across all sites and cloud providers for faster troubleshooting and issue resolution.

Challenges Faced by Organizations Migrating to the Cloud

Navigating complexity in networking and security

Many organizations are moving to the public cloud to benefit from its simplicity and automation. Some are in the early stages of adoption, starting with migrating simple applications, while others are further along, dealing with migrating mission-critical apps that come with their own set of challenges. Other organizations manage multiple public-cloud environments due to mergers or lines of business using specific clouds. According to Gartner, 81% of organizations in its 2020 global survey already use two or more cloud providers. Regardless of the scenario, infrastructure and operations teams face significant operational complexity with networking and security in the public cloud.

Some of the challenges that NetOps teams experience include:

- **Incompatibilities and delays.** NetOps teams are facing extra work because of the differences between traditional enterprise networking equipment and public cloud networking constructs (e.g., TGW, IAM security groups, network peering, and policies to steer traffic). Cloud networking constructs have a complex mix of features and limitations, with a strict compatibility matrix making them difficult to deploy and manage. These proprietary differences significantly slow down deployments and migrations.
- **Resourcing and expertise.** It is increasingly difficult for businesses to source and retain talent that has the expertise with native toolsets across every cloud provider. This makes the skills gap a very real problem for them to solve for when attempting to build a solution to establish secure connectivity among different clouds and/or their on-prem and edge sites.
- **Network performance and uptime.** Organizations need to ensure reliable, highly performant network connectivity across public/private cloud environments. When application performance falters, the network is often the first to be blamed—especially in distributed architectures. As a result, network teams need to have a holistic view of all cloud and edge sites to easily troubleshoot potential issues.
- **Complexity.** Networking between regions in a single cloud and across multiple cloud providers is complex. Each provider offers disparate toolsets that don't naturally work together. Network teams are forced to cobble together solutions from multiple traditional network vendors using datacenter networking architectures, each with their own portals and dashboards, which make it increasingly difficult to rapidly provision network and/or app connectivity across clouds.

KEY FEATURES

Automate cloud network provisioning
One-click provisioning for establishing connectivity and security among clouds, data centers, and edge locations.

Define granular routing and segmentation policies
Granular control over traffic and network isolation, both at an individual location level and across multiple sites and clouds.

End-to-end encryption and policies
Native TLS encryption from workload-to-workload, with retention of metadata across clusters, sites, and clouds.

Enable end-to-end private connectivity
Provide high-speed private connectivity to public clouds and SaaS providers using existing WAN/cloud provider links or the F5 Global Network.

App layer networking
Proxy-based architecture with granular policy for transparent interconnect and load balancing for TCP, UDP, or HTTP/s, decoupled from the underlying network.

Centralize observability and diagnostics
Gain centralized visibility and insights into network, security, apps, and users, eliminating the need to gather data from multiple sources.

The challenges for SecOps include:

- **Increased risk.** Inconsistent policies and operational models can result in increased security risks. Customers expect the same levels of security and advanced networking in the cloud as they do on-premises. Cloud-native constructs lack the capabilities to provide similar coverage, forcing customers to defer to cloud versions of traditional vendor offerings. This results in multiple configurations and operational models that increase security risks across their environment.
- **Security.** Network teams need to maintain a security mindset. Implementing solutions that minimize the friction with SecOps teams will allow them meet business and compliance requirements while achieving time-to-service commitments. They also need to ensure that whatever platform they introduce doesn't add potential security risks to the business.

These are issues that DevOps teams encounter:

- **Business agility.** Digital business moves at the pace of its developers and applications. Network teams need to keep pace and quickly provision network connectivity and policies to support the needs of developer and DevOps teams. Application teams often need additional tool sets to ensure application performance across distributed cloud environments.
- **Cloud diversity and reliability.** Customers who cannot effectively manage and resource the deployment of applications across multiple clouds are beholden to a single cloud provider which weakens their ability to negotiate and puts them at risk for service disruptions when their provider suffers outages.

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.

The F5 Distributed Cloud multi-cloud networking solution includes:

- **F5® Distributed Cloud Network Connect.** Our secure Layer 3 networking includes a virtual router and network firewall with globally orchestrated control for point and click connectivity, fully segmented and encrypted in transit, to connect customer networks among private or public clouds, campus, and branch locations.

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.

- **F5® Distributed Cloud App Connect.** Our integrated stack of Layer 7 networking and security services includes a distributed load balancer, application firewall, API proxy for app to app and cross-cluster API delivery, and API discovery for stealth API security. This provides automatic and scalable orchestration to connect apps among public clouds, data centers, co-lo facilities, and edge locations (including retail stores or manufacturing facilities).
- **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 heterogenous 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.
- **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.

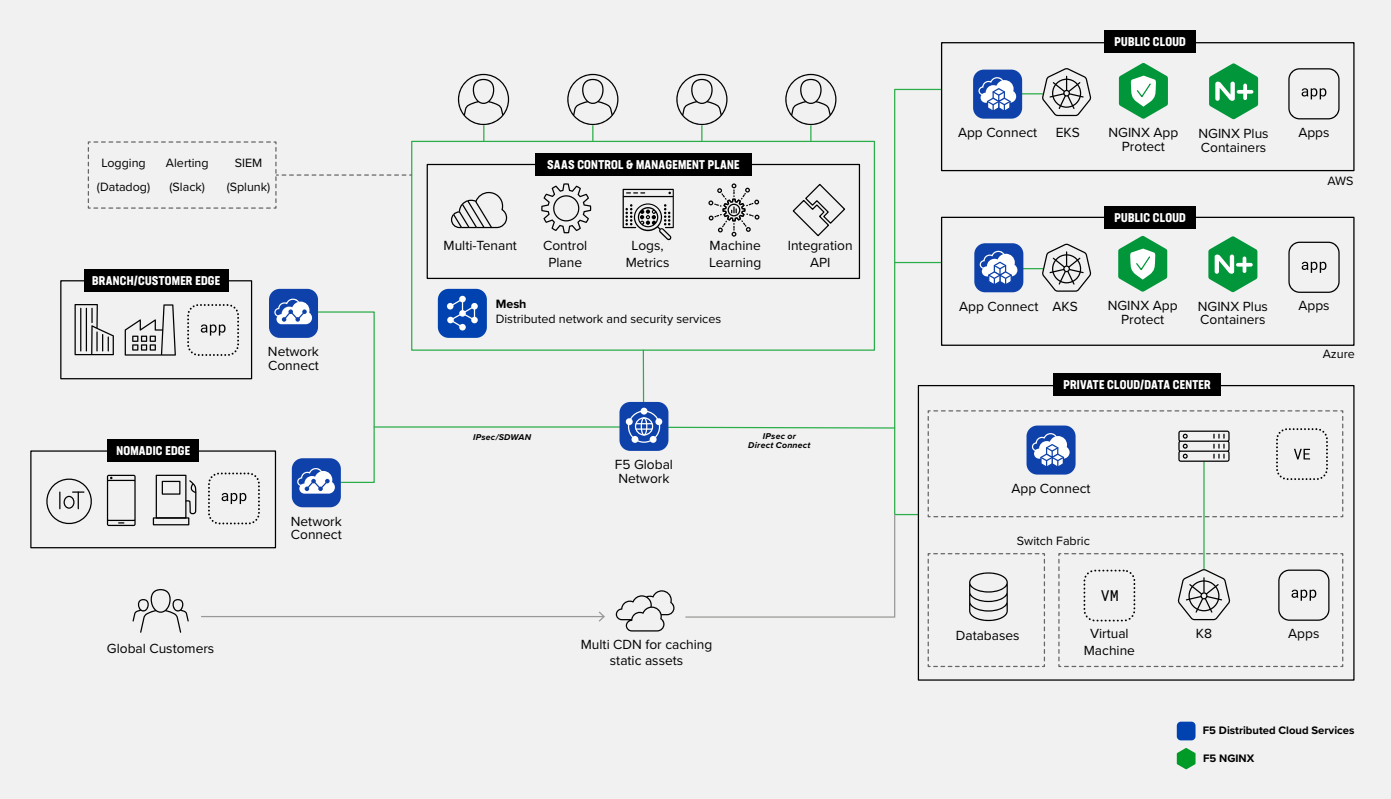


Figure 1: A reference architecture for F5's Multi-Cloud Networking solution

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

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

- **Simplify network and workload connectivity across distributed cloud environments.** Seamlessly integrate with existing cloud-native network constructs and lower TCO by reducing the number of tools needed to support multiple cloud networks.
- **Quickly provision network and workload connectivity for workloads in any cloud at the pace DevOps teams expect.** Self-service portal enables DevOps teams to easily provision connectivity. Shared console for DevOps, NetOps, and SecOps teams reduces multiple consoles and policy enforcement. Seamless support for containers and modern app architectures extends across multiple different providers and environments.
- **Meet compliance requirements with cloud-native security and advanced application networking services.** Seamless integration with F5® Distributed Cloud Web App and API Protection (WAAP) services with global application of intent-based policies. Allows insertion of third-party security services, such as Palo Alto Networks. Offers private transport with the F5 global backbone.
- **Gain valuable observability across all sites to quickly troubleshoot network and app performance issues.** Centralized console that provides visibility across all sites. Easily quantify health and performance across all sites historically and in real-time with synthetic monitoring. Integrate with many third-party analytics tools such as Splunk, Datadog and PagerDuty.

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

- End-to-end private connectivity between public clouds and physical sites such as data centers, co-lo facilities, campus, and branch.
- Automated provisioning of cloud networking constructs.
- Network segmentation with granular policy among apps, sites, and networks.
- Integrated network security or insertion of third-party security services.
- Application-layer networking among different networks, sites, providers, and environments.
- End-to-end policy enforcement with orchestrated retention of metadata between sites.
- End-to-end encryption between workloads.
- Integrated app-layer inspection and security.
- Cross-cluster service discovery, advertisement, and delivery.
- API discovery and control with granular policy for distribution and access.
- Centralized visibility, observability, and analytics for network, security, and app layers at every site.

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

Features	Other Solutions	Distributed Cloud Services
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

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.

Use Cases

Multi-Cloud Transit

Distributed Cloud Network Connect provides easy and secure connectivity into any cloud with multi-cloud transit capabilities. It connects multiple clouds with a choice of transit options: existing WAN/cloud-provider links, over a private backbone, or via the F5 Global Network. The SaaS-based console offers unified management and observability of infrastructure and applications across public and private clouds, as well as edge sites.

- **Automate cloud network provisioning.** One-click provisioning for establishing connectivity and security among clouds, data centers, and edge locations.
- **Enable end-to-end private connectivity.** Provide high-speed private connectivity to public clouds and SaaS providers using existing WAN/cloud provider links or the F5 Global Network.
- **Define granular routing and segmentation policies.** Granular control over traffic and network isolation, both at an individual location level and across multiple sites and clouds.
- **Secure network traffic.** Enable network capabilities such as BGP, access controls, and security at all sites with other F5 products and third-party services.
- **Centralize observability and diagnostics.** Gain centralized visibility and insights into network, security, apps, and users, eliminating the need to gather data from multiple sources.

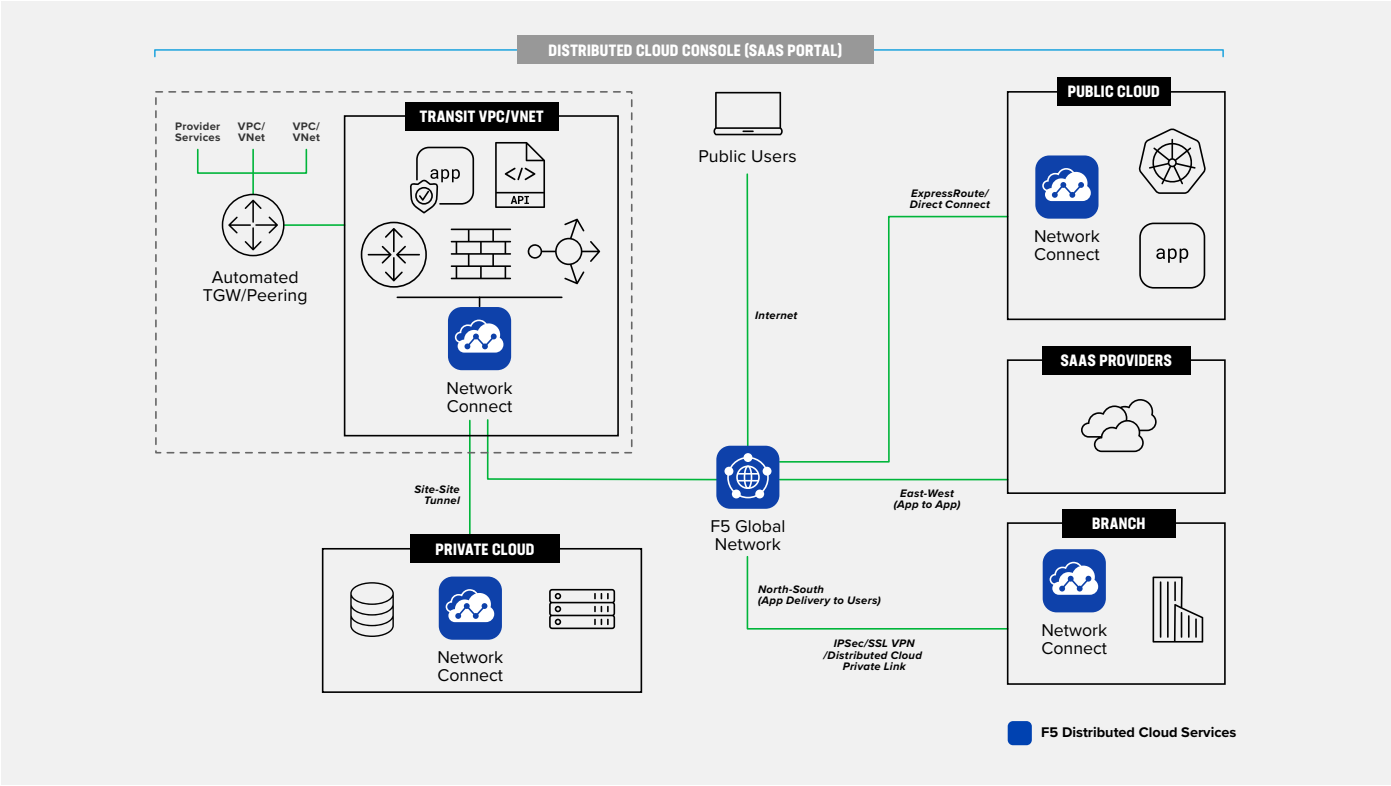


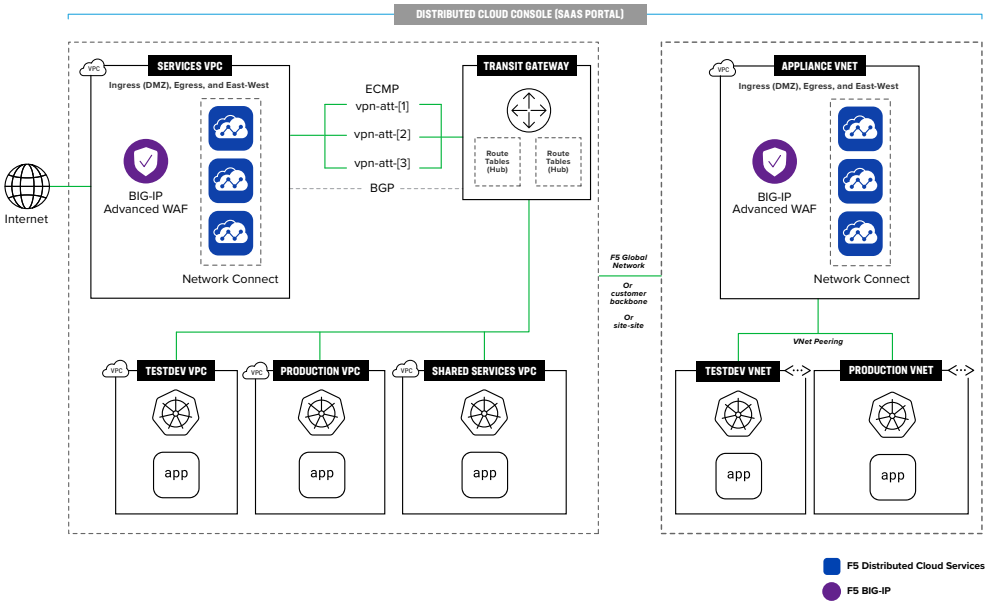
Figure 3: A visual look at how multi-cloud transit works inside Distributed Cloud Network Connect

Security Service Insertion

Distributed Cloud Network Connect offers customers the flexibility to use either F5 BIG-IP services or third-party security services from Palo Alto Networks, allowing SecOps teams to apply security controls consistently across all private and public clouds. This approach preserves their investment in existing skill sets and policies.

Inserting security services is simplified and agnostic to the cloud environment. This is achieved by implementing traffic steering rules that direct network traffic from virtual cloud networks through the security service and on to the destination. The same rules are used across different public and private clouds. Administrators can easily manage and monitor traffic across clouds and networks from a single console with granular visibility.

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



Multi-Cluster App Connectivity

Distributed Cloud App Connect enables customers to advertise applications and APIs across public or private clouds with precise control, without exposing underlying networking or routing. It allows application services and APIs in one cluster to be advertised in other local or remote clusters across clouds, enabling seamless communication between distributed app services. As services are delivered, administrators can apply granular controls over API endpoint read/write privileges.

This use case is applicable to both Kubernetes and traditional virtual machines and container environments. Distributed Cloud App Connect can be deployed as an ingress/egress or as a Kubernetes pod to discover services, advertise specific services to remote clusters across clouds, and distribute security policies across clouds to protect the advertised services.

- **App layer networking.** Proxy-based architecture with granular policy for transparent interconnect and load balancing for TCP, UDP, or HTTP/s, decoupled from the underlying network.
- **End-to-end encryption and policies.** Native TLS encryption from workload-to-workload, with retention of metadata across clusters, sites, and clouds.
- **Cross-cluster service discovery.** Native service discovery at every site, globally orchestrated, for transparent service advertisement and delivery at any other site.
- **Full Observability.** App-level dashboards with performance metrics and visitor analytics, augmented by network and security visibility at every site, in the same SaaS console.

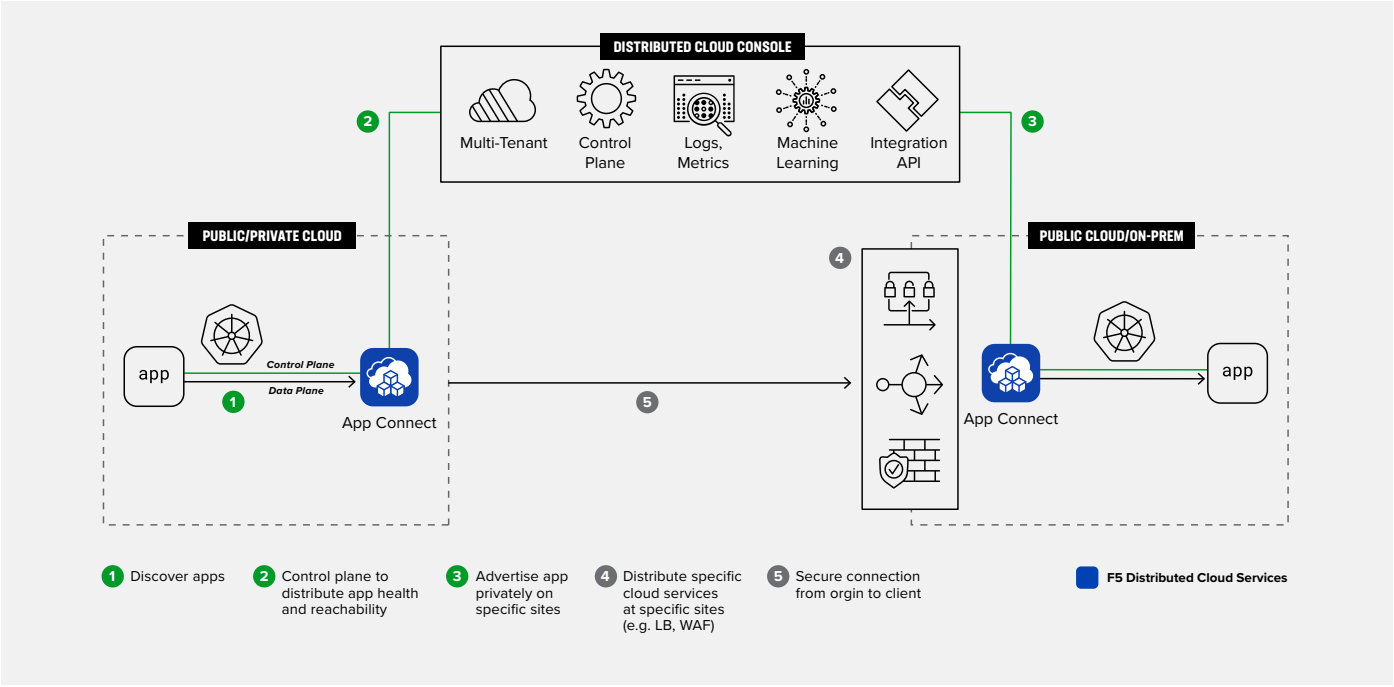


Figure 5: A visual look at multi-cluster app mesh, provided in Distributed Cloud App Connect

IP Address Overlap

The Distributed Cloud App Connect proxy-based architecture provides a simple solution for IP overlap. Overlap only becomes an issue when connections rely strictly on the underlying networks. However, advertising services at Layer 4 or Layer 7 does not depend on the underlying Layer 3 IP address space at either end, so the service can still be advertised even if the Layer 3 network has overlapping IPs.

Using Distributed Cloud App Connect, it is possible to deliver a remote service into a local subnet with a local IP address, regardless of its real IP address. As a result, there are no network changes required, such as NAT, firewall pinholes, or routing changes. Distributed Cloud App Connect offers full control and improved visibility without network disruption, providing the cleanest possible solution for overlapping IP addresses.

Test-drive the multi-cloud networking solution for free or check out other options. For more information, contact F5 sales to schedule a demo.