SOLUTION OVERVIEW

Quickly Connect Apps and APIs across Multiple Clusters and Clouds

F5 Distributed Cloud App Connect simplifies and secures multi-site north-south app delivery and multi-cluster east-west app connectivity, dramatically reducing operational complexity and cross-cloud application deployment times.

KEY BENEFITS

Faster deployments and simplified ops
Utilize infrastructure as code to efficiently provision resources and maintain uniform policies across multiple sites with centralized SaaS-based management and a distributed control plane.

Cross-cluster security coverage
Automatically deploy multi-layer security in front of and between clusters using our proxy-based architecture, providing API discovery and control without exposing the underlying network to potential threats.

Increased uptime and reliability
Get end-to-end observability for rapid identification of app performance issues across sites before they become disruptive, reducing mean-time-to-resolution.

Improved developer experience
Connect apps and deliver APIs with service discovery between K8s clusters in disparate networks with retention of metadata such as service advertisements and identity, for end-to-end policy decoupled from location.

Connecting Clusters Between Clouds Using Conventional Tools

As organizations expand their cloud strategies to multi-cloud, they seek solutions to interconnect applications and services hosted in different clusters, not just cross-connect virtual networks. This can include connecting applications to specialized services, external identity and access management sources, or in-house data or services that have been hosted in different clouds.

As application architectures change from “scale up” to “scale out” and network traffic increases between locations, the new east-west traffic paradigm complicates network design and security enforcement. For example, while a human might interact with an application every few seconds, an API call in a core loop might create thousands of interactions. Furthermore, sensitive internal APIs may require greater protection and access limitations, which can be difficult to engineer when the microservices are no longer in the same cluster.

Connecting apps between different clusters presents unique challenges. Within a single cluster, app connectivity and security are straightforward, but different clusters may reuse the same private IP address ranges, and traditional service meshes do not extend between clusters. This makes it difficult to provide shared context for security policy enforcement, and inter-service connections between clusters require a method of exchanging metadata like service advertisements. Traditional VPNs that provide only layer 3 IP connectivity are not enough without an additional control channel to mediate the connections.

Applications are also sensitive to east-west network latency, which is multiplied by the number of request/response pairs or “app turns.” If there are 1,000 API calls in a core loop, each millisecond of latency becomes a full second of application delay as each loop iteration waits for the response from the remote service. To avoid these issues, it is crucial to have visibility and control of the path of east-west connections between different regions or clouds.

Complications like these may explain why it can take multiple weeks or months for enterprises to deliver an application across multiple clouds using conventional tools.

HOW LONG DOES IT TAKE TO DELIVER AN APP USING EXISTING PRODUCTS?

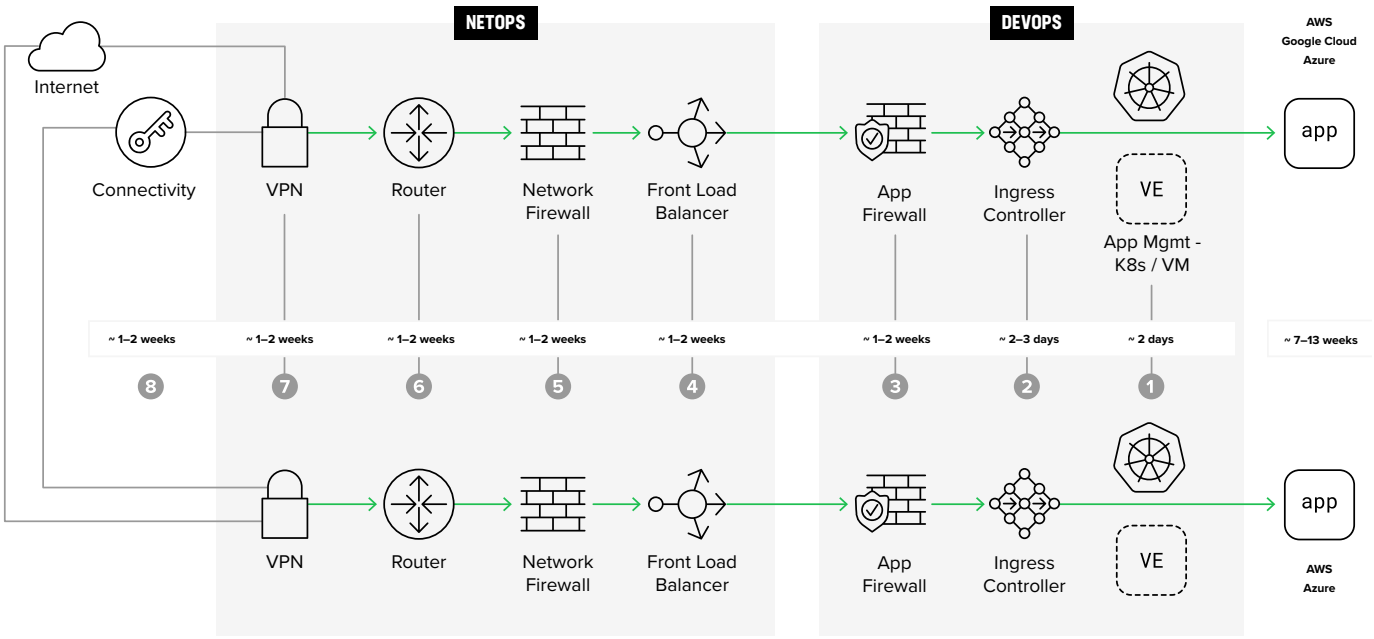

Figure 1: A graphical depiction of the steps involved in delivering an app across multiple clouds using conventional tools and cloud providers.

APP-TO-APP CONNECTIONS HAVE DIFFERENT REQUIREMENTS THAN HUMAN-MACHINE INTERACTIONS. AS APPLICATION ARCHITECTURES ARE CHANGED FROM "SCALE UP" TO "SCALE OUT" AND NETWORK TRAFFIC INCREASES BETWEEN MACHINES, THE NEW EAST-WEST TRAFFIC PARADIGM CREATES CHALLENGES IN NETWORK DESIGN AND SECURITY ENFORCEMENT.

Simplify Cross-Cloud App Deployments

The F5® Distributed Cloud App Connect securely connects and delivers applications across clouds, with setup in minutes rather than days or weeks—a fraction of the time it takes using conventional tools.

Consider the scenario where an organization intends to offer multiple parties private access to an application on a public cloud. This would not only include the organization's cloud account but also its partner's or customer's account, which may be hosted on a different cloud provider where the organization has no control over the end user or configuration.

To ensure fine-grained control over the services delivered to partners and branches, the organization requires control over HTTP methods, routes, and specific APIs.

Traditionally, three IT teams would be responsible for enforcing these controls internally:

- Developers are responsible for building the application.
- DevOps are responsible for deploying the app and related infrastructure.
- NetOps are responsible for setting service-ticket rules in the firewall to allow specific traffic in while blocking all malicious traffic.

KEY FEATURES

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.

Secure ingress and egress
Leverage an ingress-egress controller with advanced network and security services for multiple app clusters.

To deliver the app to the partner, the organization must trust that its partner will undertake similar steps to secure the service being delivered to end-users. The partner may also need to establish a VPN connection, set up routing to the organization's site, and manage any potential IP address overlap issues.

Deploying a multi-cloud app involves time-consuming steps and several challenges. These include changing routing and firewall configurations, controlling access to services and APIs, protecting against threats from unexpected sources, tracking metrics across the company network, and dealing with troubleshooting complexities.

F5 Distributed Cloud App Connect provides an easy solution for connecting clusters across various cloud providers and regions. It offers orchestrated awareness for API endpoints on all connected clusters, allowing cross-cluster service discovery and advertisement for seamless app-to-app communication with fine-grained API control. Connections between sites are self-maintaining, redundant, and fully automated, which reduces the need for administrative tasks such as establishing VPNs and routing.

App Connect provides end-to-end visibility for customers, who can choose their underlying transport, including the F5 Global Network, which is specifically designed for reliable high-speed app-to-app connections. It works with various clusters, including most Kubernetes environments, and can integrate natively to Kubernetes to discover services, advertise specific services to remote clusters across clouds, and coordinate security policies across clouds to protect advertised services. In other cluster environments, App Connect has multiple options for remote service advertisement and delivery, including presenting the remote service with an IP address local to its consumers for easy reachability without routing.

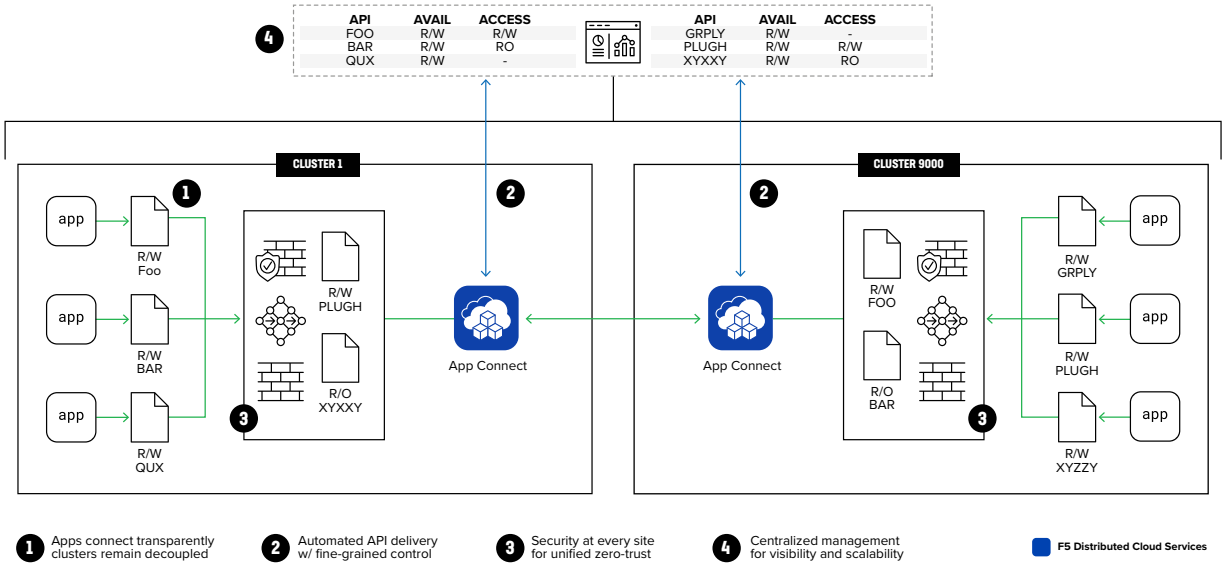

Figure 2: An architectural view of F5 Distributed Cloud App Connect, which reduces the time and complexity in connecting apps across public and private clouds

F5 DISTRIBUTED CLOUD APP CONNECT WORKS WITH A VARIETY OF CLUSTERS, INCLUDING MOST KUBERNETES ENVIRONMENTS.

Conclusion

F5 Distributed Cloud App Connect reduces operational complexity and time spent deploying apps and services across clouds:

1. **Enables app-to-app connectivity.** Accelerates app deployment by reducing issues with IP overlap and routing. Reduces potential security risks associated with exposing the underlying network to facilitate connectivity.
2. **Fine-grained controls for API access.** Intent-driven policies can be distributed to any or all sites instead of relying on IP addresses. You have complete control over what's being advertised and exposed.
3. **Cross-functional observability.** The console simplifies app deployments by allowing app configurations to be network aware. Additionally, the integrated stack architecture provides a centralized location for troubleshooting, offering visibility for all sites and functions along with application context and instrumentation to facilitate modern cross-cloud observability.

Sign up for a free trial or contact your F5 representative for a solution demo and more details.