SOLUTION OVERVIEW

Securely Extend Amazon VPC Lattice Applications to Your Entire Environment with F5

Connect apps and services in AWS with other cloud, edge, and on-premises environments with F5 Distributed Cloud Services. Consistent policies, unified visibility, and automated service discovery empower more reliable apps anywhere.

aws PARTNER

KEY BENEFITS

Simplified networking
Extend your Amazon VPC Lattice to all environments to deliver apps anywhere without needing to modify the underlying networking.

Improved security
Insert consistent security controls and encrypt traffic to defend apps, APIs, and networks against threats.

Increased reliability
Identify app or service performance issues quickly, before they cause an outage, with end-to-end observability and performance metrics.

Painless cross-cloud deployments
Use infrastructure as code to provision resources faster and apply uniform policies to all environments.

Challenges to Connecting Apps and Services

Microservices app architectures have gained popularity for their flexibility and decentralized approach, but discovering and connecting the growing number of services across multiple environments can be a challenge. Building these connections creates network complexity, resulting in routing issues, overlaps, and other problems.

To solve this issue, Amazon Web Services (AWS) built an application networking solution called Amazon VPC Lattice. This connects services at scale across multiple AWS virtual private clouds (VPCs), accounts, and compute services while also adding application layer security, granular traffic controls, and service-to-service visibility.

However, with so many organizations using hybrid or multi-cloud environments and distributed app architectures, they also need a way to extend access and security outside of their AWS environments.

Connect Apps Beyond AWS

F5® Distributed Cloud App Connect allows you to provide systems and users outside of AWS with secure access to your Amazon VPC Lattice. Connect apps, services, or users anywhere and everywhere, whether they're on premises, in other public clouds, at the edge, or delivered as a SaaS application. Multiple infrastructures are supported, including Kubernetes and legacy virtual machines.

You can also extend multi-cloud networking to your own data center or private cloud with F5® Distributed Cloud Customer Edge. It provides routing flexibility across a multi-cloud fabric, manages how client-side and server-side connections are handled, and can inject L4-L7 services into a proxy architecture.

While Distributed Cloud Customer Edge is self-managed within your own environment and Distributed Cloud App Connect is a SaaS offering, both use the same centralized control plane, the F5® Distributed Cloud Console, for configuration management and observability. These solutions can be used together to connect your entire hybrid environment.

KEY FEATURES

Unified management
Get single-pane-of-glass management and observability with the F5 Distributed Cloud Console.

Automated service discovery
Identify services across clusters and clouds with global orchestration for transparent service advertisement and delivery at any other site.

Granular security policies and controls
Manage access privileges and securing settings consistently to protect the underlying network from potential security threats.

Broad compatibility
Connect services in AWS with those in other clouds or on premises as well as modern and legacy infrastructure.

Find and Connect Services

Deploy Distributed Cloud App Connect in an AWS VPC that is part of your lattice network. Once added, you can easily discover and advertise services across clusters and clouds using orchestrated awareness for API endpoints. These connections are self-maintaining, redundant, and fully automated to simplify app to app networking.

Integrate Security

Protect your apps and services by incorporating F5 security solutions into your app networking. F5 Distributed Cloud Services all use a single, unified console, meaning you can connect and secure your apps and networks in one place. Security solutions include:

- **F5® Distributed Cloud API Security** – Discover API endpoints and monitor for anomalous behavior.
- **F5® Distributed Cloud Bot Defense** – Block malicious bot traffic that delivers attacks and disrupts legitimate users.
- **F5® Distributed Cloud DDoS Mitigation** – Prevent application-based and volumetric distributed denial of service attacks.
- **F5® Distributed Cloud Web Application Firewall** – Protect applications with advanced threat detection and AI-powered intelligence.

These security solutions make it easy to deploy comprehensive, consistent, and repeatable protection for apps anywhere. In addition, app segmentation in Distributed Cloud App Connect provides secure access via granular policies to support a zero trust strategy, while end-to-end native TLS encryption protects data in transit.

Troubleshoot Apps

Distributed Cloud App Connect offers full observability through app-level dashboards. These provide performance metrics to assist with troubleshooting, as well as network and security visibility within the same console for better context. Together, you get visibility across your entire network—in AWS or other clouds and on premises.

Secure and Deliver Apps Anywhere

With F5, you can connect your apps on AWS with services or users in other environments without the complexity of traditional networking. Bring applications and services together anywhere, even your own private cloud or data center, for ultimate flexibility. Add a wide variety of security services to protect apps and networking without the need for additional management tools for secure services anywhere they're needed.

Learn more about F5 Distributed Cloud Services at f5.com/cloud.