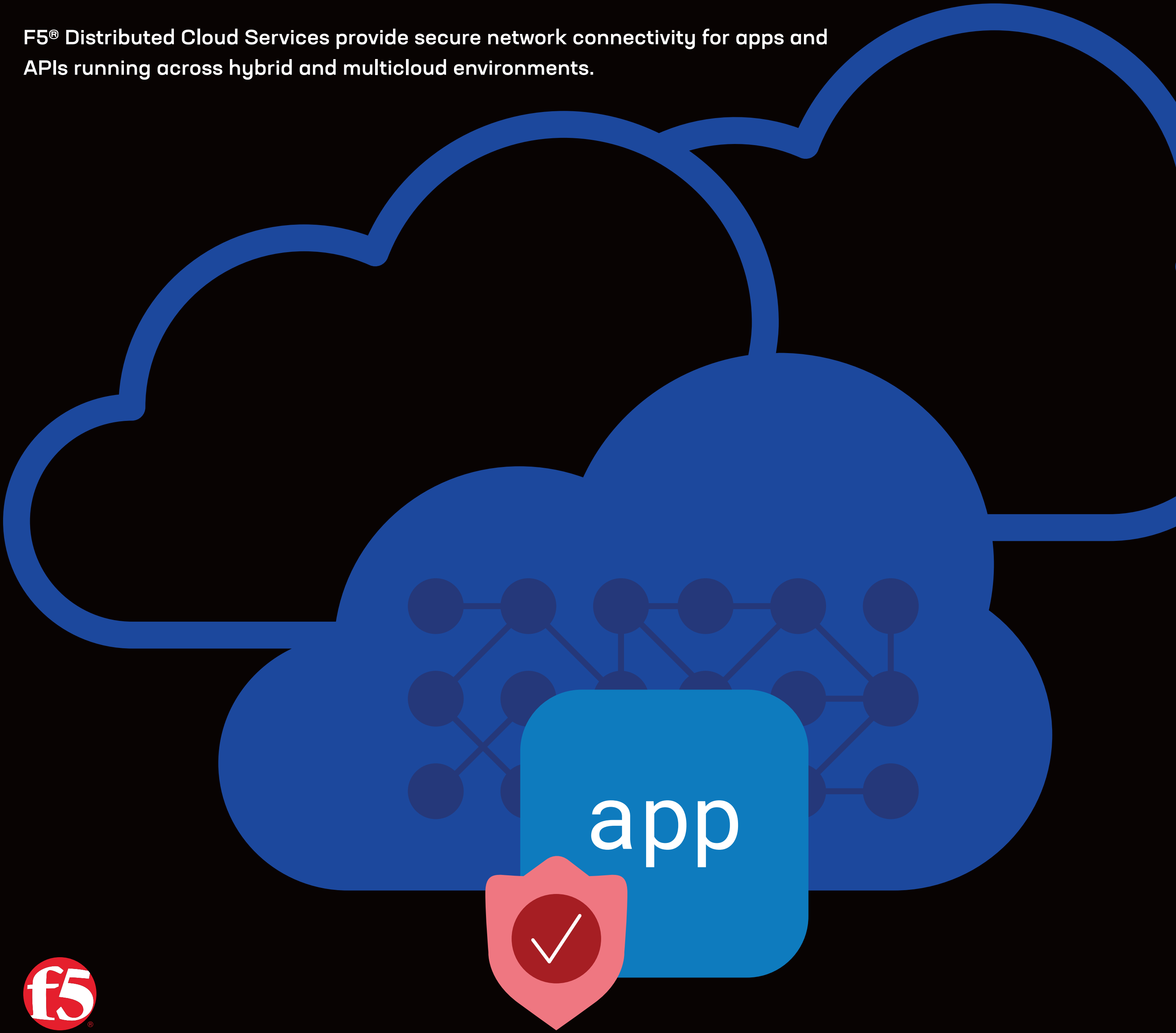
Solution Overview

Secure Multicloud Networking for Hybrid Cloud and Distributed Architectures

F5® Distributed Cloud Services provide secure network connectivity for apps and APIs running across hybrid and multicloud environments.



Key Benefits

Simplify Operations and Reduce Costs
Reduce TCO with SaaS-based networking provisioning across hybrid, multicloud, and edge environments.

Accelerate Application Deployment and Provisioning
Automate network provisioning and orchestration across multiple cloud providers.

Enable Consistent Security for Every Application and API
Deploy consistent security policies for apps in any cloud without having to duplicate policies for individual cloud providers.

Gain End-to-End Visibility Across Distributed Sites
Centralized network visibility across all sites and apps, with specific site drill downs to expedite issue remediation and troubleshooting.

Enable Seamless Hybrid and Multicloud Connectivity.
Connect networks and workloads between public clouds, on-premises data centers and edge sites in a fraction of the time compared to existing network tooling

Modern Apps Introduce New Complexities

According to the 2024 F5 State of Application Strategy report, 63% of modern enterprises are deploying apps to 3 or more environments, and 38% are deploying in as many as 6 distinct environments.

Modern microservices-based apps are easily deployed to any environment; either in the cloud, or on-premises in a data center, branch facility, or remote edge site. This inherent mobility introduces additional complexities for networking and security teams to navigate, as every environment brings unique challenges and requirements to support these apps.

Securing applications across multiple environments is a complex, time-consuming, and labor-intensive process. On top of this, connecting legacy and modern apps at scale using existing network topologies is increasingly difficult. Managing heterogeneous tech stacks deployed across highly distributed sites presents a number of challenges for operational teams.

- Securing both apps and networks is complex, especially when there needs to be consistency across environments. Each environment has unique tooling and requires specific skill sets. As teams are forced to operate with tighter budgets, managing these environments becomes increasingly burdensome.
- Networks and applications have diverse security requirements, and often need multiple tools to ensure they are protected. Cloud-provider security solutions can only go so far, and ensuring consistent security policy enforcement for modern and traditional apps in hybrid and multicloud environments is highly labor-intensive and time-consuming.
- Microservices-based applications that are distributed across multiple clouds and edge environments require overly complex and cumbersome VPNs and network topologies to ensure seamless connectivity. This impedes the speed of app deployments and business agility.
- The increasing complexity of network topologies built using conventional, on-premises-based network tooling and individual public-cloud provider tooling introduces significant overhead and operational burden for overstretched network operations teams.

These challenges create additional friction between networking, application, and security teams, which negatively impact business agility and productivity. Organizations need a solution that can adequately address the needs of these teams while improving collaboration and operational efficiencies.

Key Features

Automate Cloud Network Provisioning

One-click provisioning establishes connectivity and security to any cloud hybrid, or on-premises location.

Enforce Granular Routing and Segmentation Policies

Granular control over traffic and network isolation, both at an individual site level and across multiple sites and clouds.

Establish End-to-End Encryption Across the Network

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

Enable End-to-End Private Connectivity

Establish high-speed private connectivity to public clouds and SaaS providers.

Enable Service Connectivity Across Apps and Clusters .

Establish direct connections with automated provisioning between apps and clusters, reducing the threat surface and enabling local security via CE deployments.

Delivering Secure Multicloud Architectures

Secure multicloud networking extends beyond provisioning secure transit between different clouds. Organizations must account for the specific network and security needs of modern workloads and service-based applications across cloud and edge sites when building a solution. These considerations should account for the following:

Build foundational Layer 3 connectivity: you will need a secure unified network fabric that can connect multiple environments, including multiple public clouds, on-premises data centers, branches, or remote edge sites. This network should extend to, and orchestrate, on-premises networks to any cloud, without additional network complexity. Additionally, you should be able to easily provision routing, NAT, and network firewalls, with centralized observability across your entire network.

Establish connectivity at Layer 7 for application services: You will need to create a delivery fabric that directly connects application services across hybrid and multicloud environments. This creates direct connections between these applications without needing to expose them to the public internet. This network also needs to connect and orchestrate workloads that run in on-premises and edge environments, and account for cloud-native and legacy architectures. Additionally, when new applications are deployed to distributed environments, you need a way to ensure that connectivity and security is consistent and can be provisioned rapidly.

Secure your L3 and L7 Networks and Applications: Finally, you need to ensure that your network and applications are secured against a wide variety of threats. In distributed environments, that security needs to be deployed locally, not only delivered via SaaS. You need protection for both applications and APIs, and account for threats like DDoS and bot attacks. The policies you create must be easy to deploy everywhere your applications run—and need to be enforced consistently. You need to have visibility into every application to respond to threats quickly. Finally, you need a way to ensure only specific applications are exposed publicly, with a DMZ that can scale to meet rapid demand changes and not become too expensive and burdensome to maintain.

F5 Distributed Cloud Secure Multicloud Networking

F5® Distributed Cloud Services simplify the operational complexity of multicloud networking for enterprise teams that operate in one or more clouds. Distributed Cloud Services are cloud-native, SaaS-based services that can deliver networking and security services via traditional SaaS on the F5 global private network, or locally (Hybrid SaaS) in your own cloud or on-premises environments. The hybrid deployment model is enabled by deploying a custom software package, called a CE, that provides networking, security, and app delivery services wherever they are installed. Distributed Cloud Services are all supported by a globally distributed data fabric which leverages AI/ML solutions that analyze network performance and threats, while providing new recommendations.

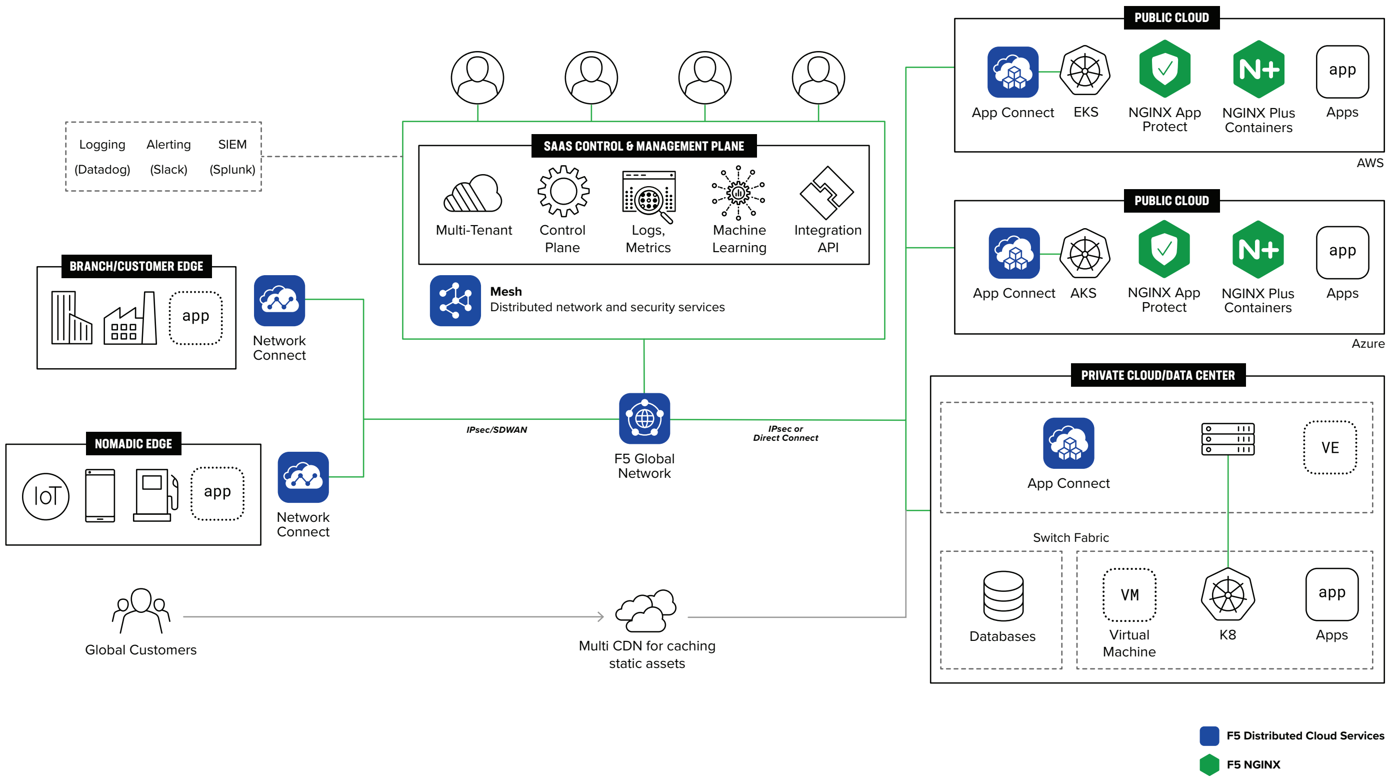


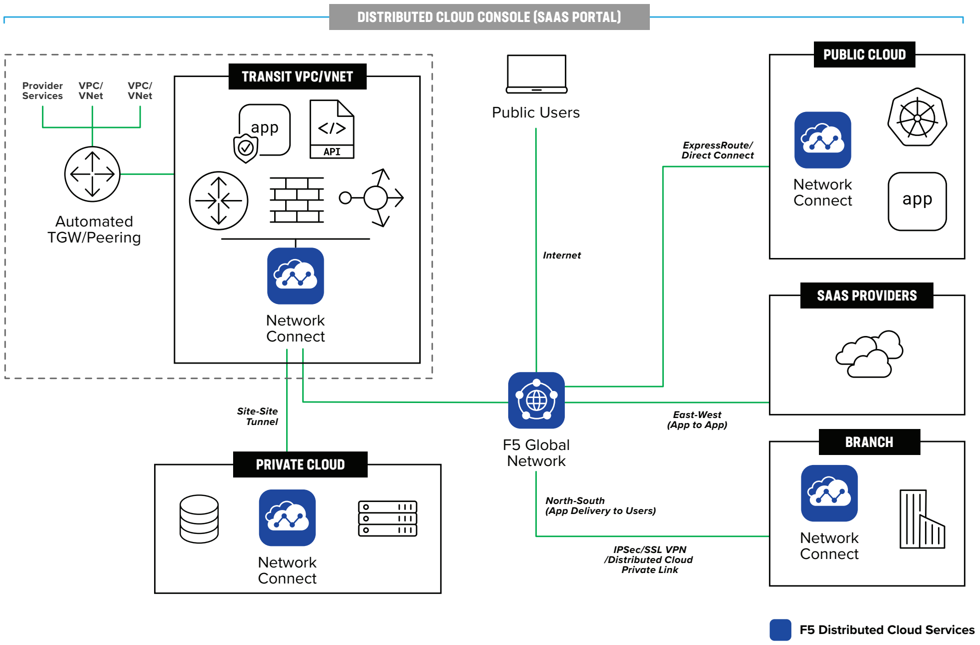
Figure 1: A reference architecture for F5's Multicloud Networking solution

The F5 secure multicloud networking solution includes the following key components:

F5® Distributed Cloud Network Connect lets you build Layer 3 network connectivity across your hybrid and multicloud environment. It includes a virtual router and network firewall with globally orchestrated control for point-and-click connectivity, fully segmented and encrypted in transit, to connect networks across cloud, on-premises, and edge locations.

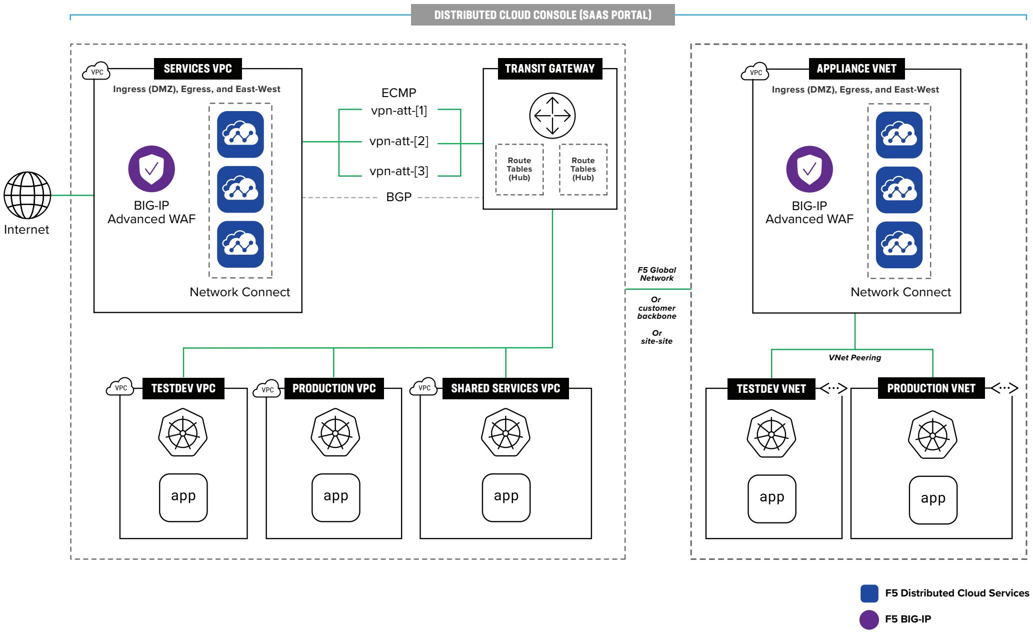
Network Connect provides automated network provisioning and enables end-to-end private connectivity. This creates the secure network fabric that allows you to provision connectivity and security to every site where a CE deployed.

Figure 2: A visual look at how multicloud transit works inside Distributed Cloud Network Connect



Network Connect also supports third party service insertion, allowing you to use existing F5® BIG-IP® or Palo Alto Networks security services.

Figure 3: A visual look at the security services insertion use case



F5® Distributed Cloud App Connect creates app-centric service connectivity between applications. It includes a distributed load balancer, application firewall, API proxy for app-to-app and cross-cluster API delivery, and cross-cluster app and API discovery, as well as native TLS encryption. This provides automatic and scalable orchestration to connect any app on public cloud, in on-premises data centers, in co-location data centers, and edge locations (including retail stores or manufacturing facilities). App Connect enables consistent application security and networking policies to be deployed anywhere a CE is deployed and supporting any type of app—whether it be an AI inference or other modern containerized app, or a monolithic legacy app. App Connect also solves for the IP address overlap problem by enabling you to deliver apps into a local subnet with a local IP address, regardless of its real IP address. That means no network changes need to be made for new apps.

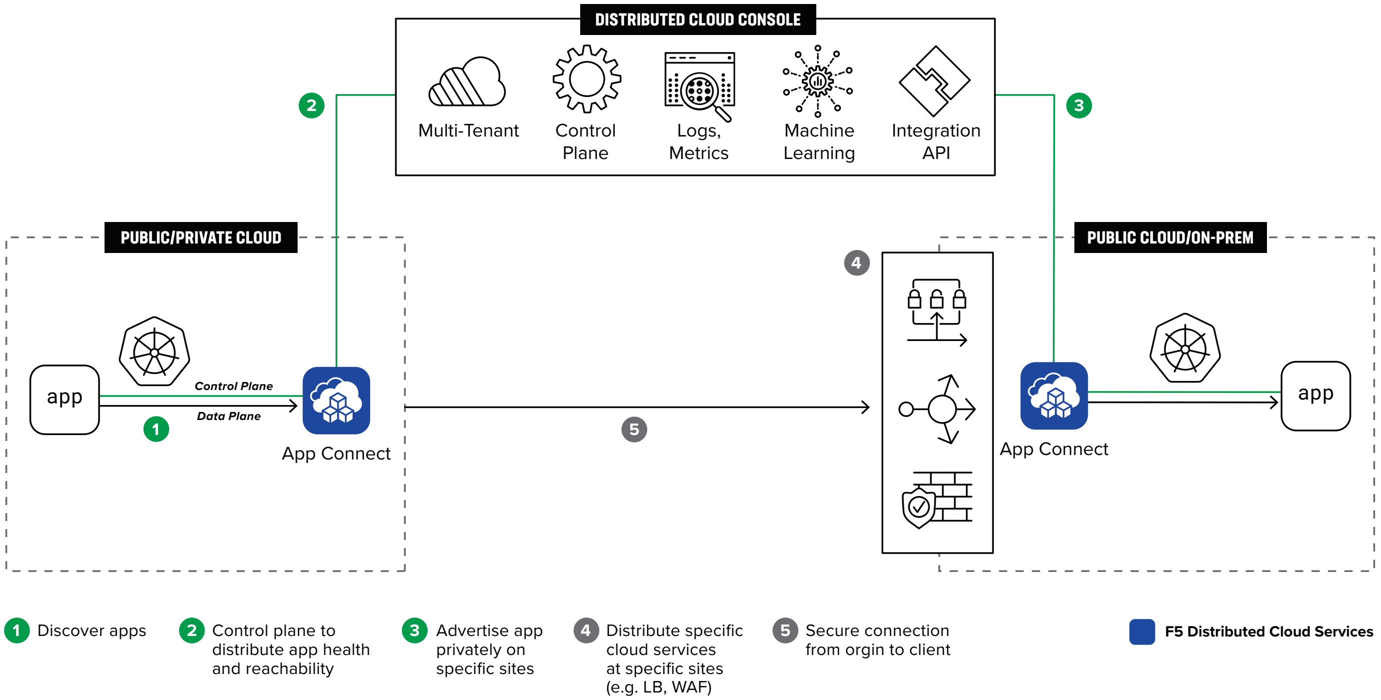

DISTRIBUTED CLOUD CONSOLE
Multi-Tenant
Control Plane
Logs, Metrics
Machine Learning
Integration API
2
3
PUBLIC/PRIVATE CLOUD
app
Control Plane
Data Plane
1
App Connect
5
4
PUBLIC CLOUD/ON-PREM
App Connect
app
1 Discover apps
2 Control plane to distribute app health and reachability
3 Advertise app privately on specific sites
4 Distribute specific cloud services at specific sites (e.g. LB, WAF)
5 Secure connection from orgin to client
F5 Distributed Cloud Services

Figure 4: A visual look at multi-cluster app mesh, provided in Distributed Cloud App Connect

F5® Distributed Cloud Customer Edge (CE) is a software package deployed on a VM or in a container in any environment. It orchestrates the local control plane and data plane components to route, encrypt, and secure traffic. A CE operates as a highly available edge gateway that can be deployed on any site in your network, and extends the network to that site, without needing to establish physical networking. A CE enables access to the regional edge sites on the F5 Global Network and delivers these platform services locally. Multiple CEs can create a service mesh which facilitates app-to-app communication without the need to have any direct L3 connectivity between the environments where apps are located. A CE also enables consistent enforcement and management of security policies across hybrid and multicloud environments. A CE can also provide a managed Kubernetes platform, which allows hosting of apps as containers or VMs. The regular mesh functionality of load balancing and security features are also available for these sites.

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	X	✓
Automation assistance for NetOps	X	✓
Observability and analytics	External	✓
Lifecycle management	Controller	SaaS

Key takeaways for F5 secure multicloud networking:

- Consistent, AI-powered security and protection of both modern and legacy apps. Whether your apps live on-premises, in the cloud, or on edge sites, F5® Distributed Cloud WAAP capabilities provide strong security across the board to defend against a huge array of threats to simplify SecOps.
- Connectivity between legacy and modern apps and APIs across clouds, data centers, and edge locations, using service networking instead of traditional methods, enabling you to provision app connectivity in minutes, instead of months. This lets DevOps teams innovate quickly, confident the network will keep up.
- Seamless network connectivity, segmentation, and security across clouds, on-premises, and edge environments. It abstracts cloud networking complexities with orchestration, to create a seamless network with end-to-end network visibility that can be operated centrally via the F5® Distributed Cloud Console.

Conclusion

As apps are deployed on increasingly distributed environments, you must have a platform that can provide the connectivity and security you need to respond to your customers. Secure multicloud networking from F5® Distributed Cloud Services gives you the tools to connect any cloud, on-premises, and edge site that you operate into a single network.

You can deploy and connect both modern and legacy apps, APIs, and clusters with consistent networking services already provisioned, regardless of where they are deployed. Finally, you can protect your network and apps with consistent security policies that you create once and deploy everywhere through the F5 Distributed Cloud console.

More Information

Ready to get started? Get in touch with F5 to dive into what secure multicloud networking solution from F5® Distributed Cloud Services can do for you.