White Paper

Securely Connect and Migrate Apps across Any Cloud

Microservices have changed how we think about distributed infrastructure in the cloud.

Applications are changing at a rapid pace, and infrastructure is struggling to keep up. Modern networks are messy and require significant overhead to effectively deploy and scale. Delivery and migration of legacy and modern apps—while ensuring connectivity and security at scale—has become increasingly difficult and is especially challenging with native cloud tooling.

From Docker to Kubernetes, containerization and microservices have changed how enterprises manage their applications. Microservice architectures have introduced an increasing number of APIs and application services to manage, meanwhile AI is about to add a new layer of complexity. Maintaining connectivity and security between app services has become increasingly intricate and time consuming, requiring different tools and skills to maintain particularly in multicloud environments. Microservices have changed how we think about distributed infrastructure in the cloud.

The F5 2024 State of Application Strategy report found that 63% of organizations are deploying applications in three or more environments. A full 38% of orgs are deploying apps in at least six environments. Increasingly, these applications are being containerized, split into microservices, and deployed across distributed environments—while still needing to communicate with monolithic legacy apps like ERP systems.

Deploying applications across distributed environments is a trend that is quickly gaining ground, but traditional networking topologies and tools are at a disadvantage when it comes to deploying modern, distributed apps and services. These tools were built to accommodate on-premises data centers and, at most, a single cloud. While they are necessary at a foundational network layer, they become a bottleneck to deploying applications at today's rapid pace.

When dealing with an ever-growing number of cloud environments, applications, and API endpoints with both public-facing and private security profiles, adding app security to existing network adds even more friction.

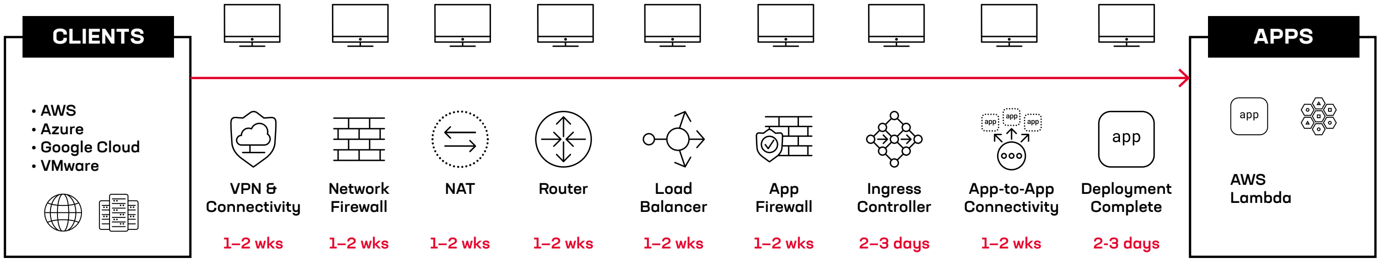


Figure 2: Traditional app deployment can take weeks, even months. Adding environments exponentially increases complexity, and each tool often requires its own console and interface.

The traditional methodology for connecting applications across existing network topologies would include the following:

1. Establish a Network that Connects Multiple Environments

Create a network infrastructure that enables connectivity between various environments, such as on-premises data centers, public clouds, and edge locations using either existing on-premises-based tooling or those provided by a cloud provider. This involves setting up network connectivity between sites, followed by provisioning APIs and configuring load balancing.

Teams responsible for application delivery will need to handle tasks ranging from API routing based on application logic to networking tasks, including DNS provisioning and firewall rule creation. Such coordination ensures that the applications are accessible and function correctly across the integrated network.

2. Configure Wide Area Network for Application Delivery

Once the network is established, the next step is to configure the wide area network (WAN) to support application delivery. This includes setting up virtual private networks (VPNs), fine-tuning routing configurations, and establishing network address translation (NAT) policies. These tasks need to be carefully managed to accommodate both public and private networking requirements, ensuring that applications are delivered efficiently and securely to the end-users, regardless of their location.

3. Implement Cross-Environment Security Measures

Securing applications requires a comprehensive approach that addresses both network and application layer requirements. This involves implementing security measures that can protect disparate hybrid cloud environments, which necessitate collaboration between various teams. Security teams will work together to coordinate firewall rules and NAT policies, while also ensuring that routing and load balancing configurations support secure communication between environments. This collaborative effort is essential to protect the network infrastructure and the applications it supports from potential threats.

4. Collaborate Across Teams for Effective Network Operations

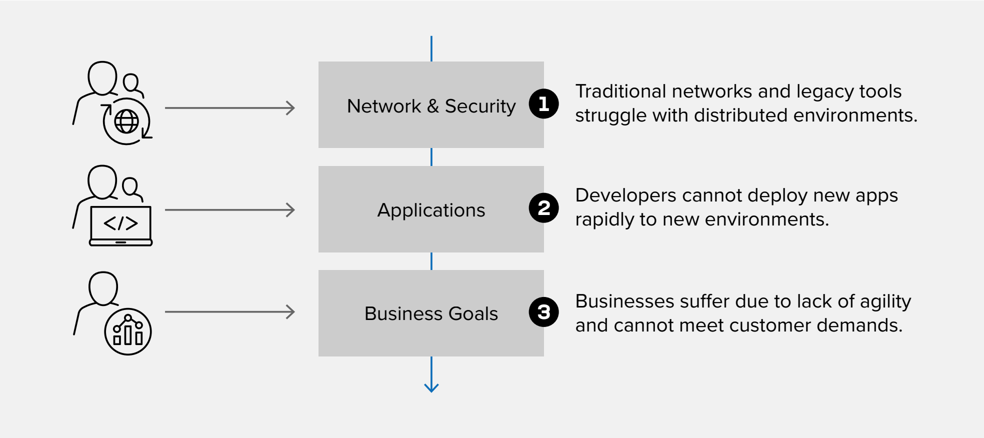
Ensuring the efficient delivery of these application services on the network often demands close collaboration between multiple teams. This involves provisioning configurations for both private and public application delivery, managing certificates, and configuring network settings for content delivery (CDNs) for the public delivery of application assets. Each team brings its expertise to the table, ensuring that all aspects of the network are optimized for performance, security, and reliability.

Existing tools mostly solve for niche use cases and require a patchwork of tools that were never truly designed to work together.

The above steps require multiple disciplines including DevOps, NetOps, SecOps, platform engineers, and even cloud architects when dealing with multiple cloud providers and environments. Existing tools mostly solve for niche use cases, and modern use cases require a patchwork of tools that were never designed to work together.

Meanwhile, some enterprise organizations continue to migrate aging data centers to the cloud. Not all apps and infrastructure can migrate at the same time, but they still need to work together and remain secure. Mergers and acquisitions also introduce entirely new cloud, hybrid, and on-premises environments; new security variables; and complexity that architects and administrators need to resolve across the organization.

When migrating applications between cloud providers there are risks of downtime, service interruptions, configuration management issues, and performance and security issues. Ensuring data integrity and compatibility between different cloud environments can also present several challenges.



1 Traditional networks and legacy tools struggle with distributed environments.

2 Developers cannot deploy new apps rapidly to new environments.

3 Businesses suffer due to lack of agility and cannot meet customer demands.

Figure 3: Traditional organizations often struggle to maintain application speed and business velocity due to the limitations of their networks.

Securely Deliver and Migrate Applications Across Clouds

A streamlined solution to avoid sprawl and complexity in multi-cloud environments.

F5 Distributed Cloud App Connect provides a solution for securely connecting legacy and modern apps across any public cloud and on-premises environments. By automating and simplifying service connectivity between disparate environments, F5 can help enterprises build a modern network that scales multicloud connectivity to any app, enabling secure app migrations across any provider with consistent policy enforcements and security.

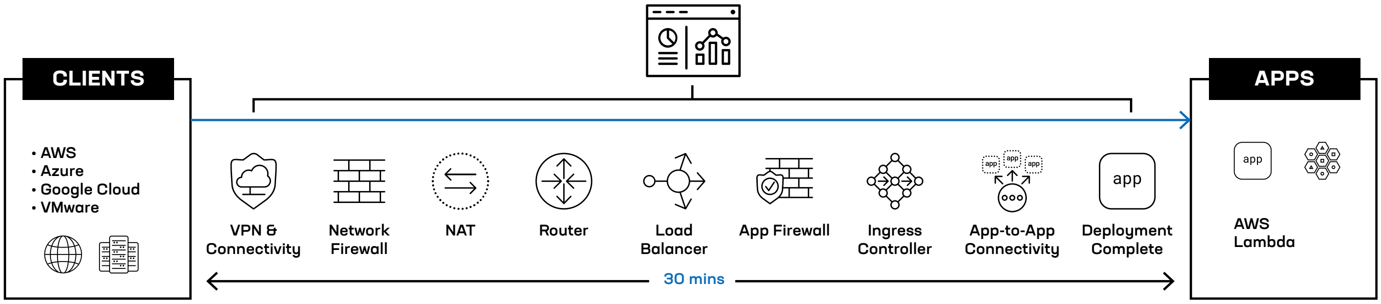


Figure 4: Service networking with F5 Distributed Cloud App Connect allows seamless app-to-app connectivity without the traditional networking overhead.

With Distributed Cloud App Connect, every app can securely communicate with one another wherever they are deployed. Distributed Cloud App Connect works seamlessly with a platform of web application and API protection (WAAP) services that secures apps and APIs against a broad spectrum of threats with robust security policies via an integrated WAF, DDoS protection, bot management, and other security tools. This enables the enforcement of consistent, strong security policies across all apps without needing to configure individual custom policies for each app and environment across the network.

Distributed Cloud App Connect helps enable app migrations and portability in a few clicks, by seamlessly connecting applications, APIs, and Kubernetes clusters across any cloud region or environment.

Distributed Cloud App Connect helps enable app migrations and portability in a few clicks, by seamlessly connecting applications, APIs, and Kubernetes clusters across any cloud region or environment. This makes it easy to re-distribute or allocate traffic between cloud environments during a migration, without disrupting the availability of services during an active migration.

F5 enables hybrid networks that extend on-premises networks to any cloud, with security, deployment flexibility, and networking provisioned from a single platform. Seamlessly operate apps in any cloud or on-premises datacenter in a fraction of the time with existing tools and gain full observability and an abstraction layer to aid orchestration. Easily observe all network traffic, quickly diagnose problems, and maintain high network availability from a centralized console.

How Distributed Cloud App Connect Provides Extensibility across Distributed Sites

As organizations navigate the complexities of modern cloud infrastructure, the need to connect remote, physical edge sites to the cloud marks a pivotal advancement in network architecture. The F5 Distributed Cloud Platform extends services to these environments with lightweight customer edge (CE) software packages that can be deployed as virtual machines (VMs) or containerized services in any physical or cloud environment. These lightweight extensions function as highly available edge gateways. The CE is a fully integrated stack of networking, security, and app management services including API security, application delivery, web application firewall, and routing. They play an instrumental role in extending network capabilities to any site within the network, without needing to provision physical network connectivity.

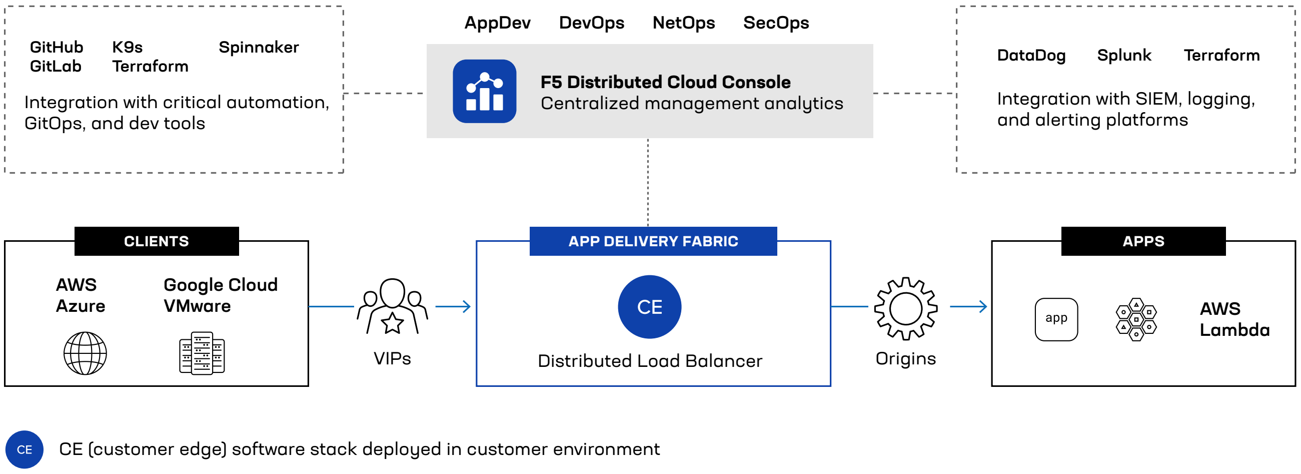
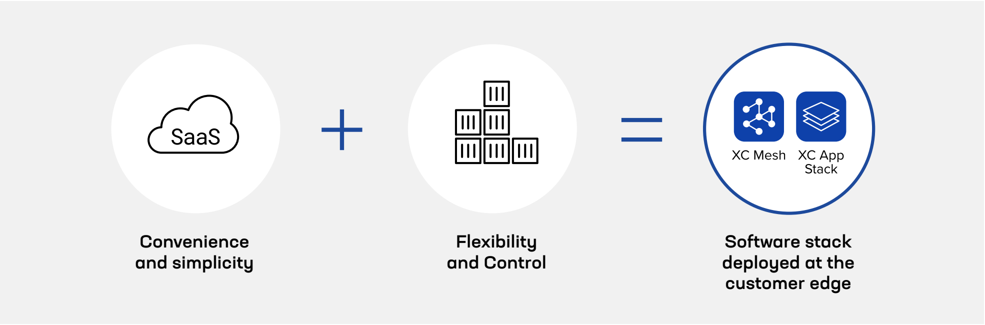

GitHub
GitLab
K9s
Terraform
Spinnaker
Integration with critical automation, GitOps, and dev tools
AppDev
DevOps
NetOps
SecOps
F5 Distributed Cloud Console
Centralized management analytics
DataDog
Splunk
Terraform
Integration with SIEM, logging, and alerting platforms
CLIENTS
AWS
Azure
Google Cloud
VMware
VIPs
APP DELIVERY FABRIC
CE
Distributed Load Balancer
Origins
APPS
app
AWS
Lambda
CE
CE (customer edge) software stack deployed in customer environment

Figure 5: F5 Distributed Cloud Console centralizes management of application delivery, reducing operational complexity.

Distributed Cloud App Connect extends into any on-premises or cloud environment enabling a framework that simplifies and secures app connectivity across diverse environments. These lightweight software extensions enable seamless communication of distributed application services within a multicloud landscape. This interoperability is crucial for organizations pursuing digital transformation, as it allows for increased portability, enhances app security, and taps into the benefits of secure multicloud networking with F5.


SaaS
+
=
XC Mesh
XC App Stack
Convenience and simplicity
Flexibility and Control
Software stack deployed at the customer edge

The need to connect remote, physical edge sites to the cloud marks a pivotal advancement in network architecture.

Additional functionalities include:

- Access to the regional edge (RE) sites on the F5 Global Network.
- Local delivery of security and networking services for internal applications, minimizing security risk by avoiding exposure to the public Internet.
- A managed Kubernetes platform which allows hosting of apps as containers or VMs.

Distributed Cloud App Connect: Simple, Secure, Scalable

In the realm of modern network architecture, businesses strive for solutions that not only streamline operations but also uphold stringent security protocols—all while providing the scalability necessary to grow and adapt in a dynamic marketplace. Distributed Cloud App Connect embodies these principles by offering a simple, secure, and scalable approach to application portability and migrations.

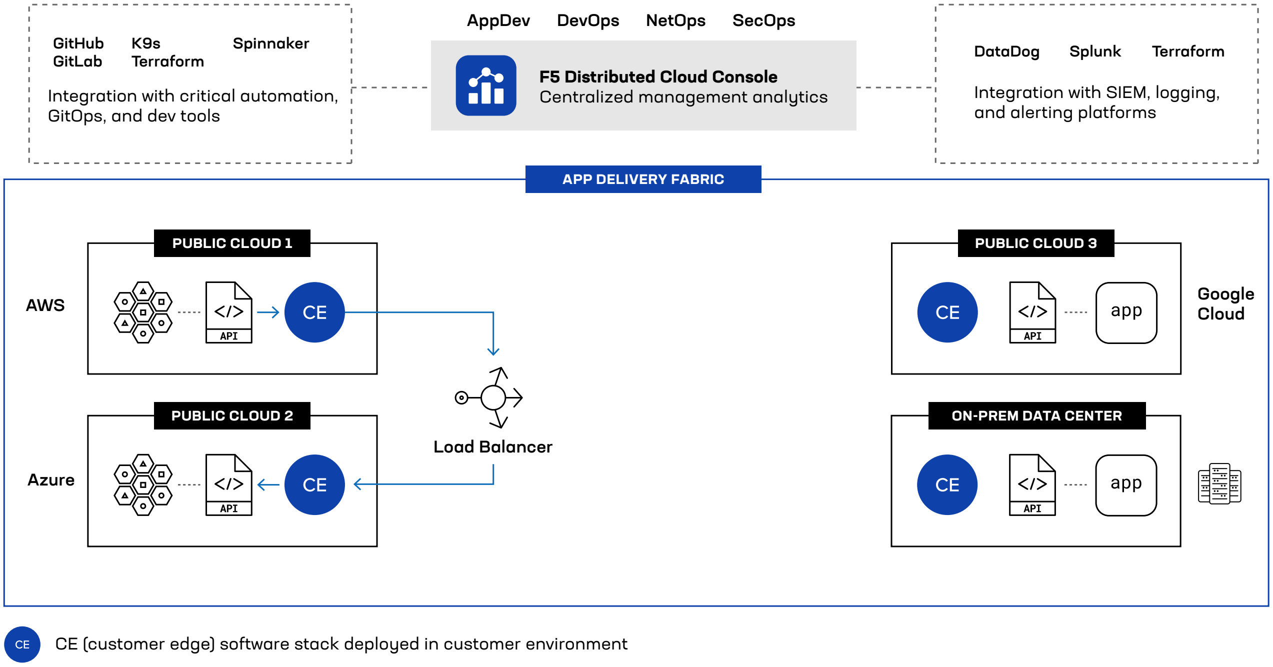

GitHub
GitLab
K9s
Terraform
Spinnaker
Integration with critical automation, GitOps, and dev tools
AppDev
DevOps
NetOps
SecOps
F5 Distributed Cloud Console
Centralized management analytics
DataDog
Splunk
Terraform
Integration with SIEM, logging, and alerting platforms
APP DELIVERY FABRIC
PUBLIC CLOUD 1
AWS
API
CE
PUBLIC CLOUD 2
Azure
API
CE
Load Balancer
PUBLIC CLOUD 3
CE
API
app
Google Cloud
ON-PREM DATA CENTER
CE
API
app
CE
CE (customer edge) software stack deployed in customer environment

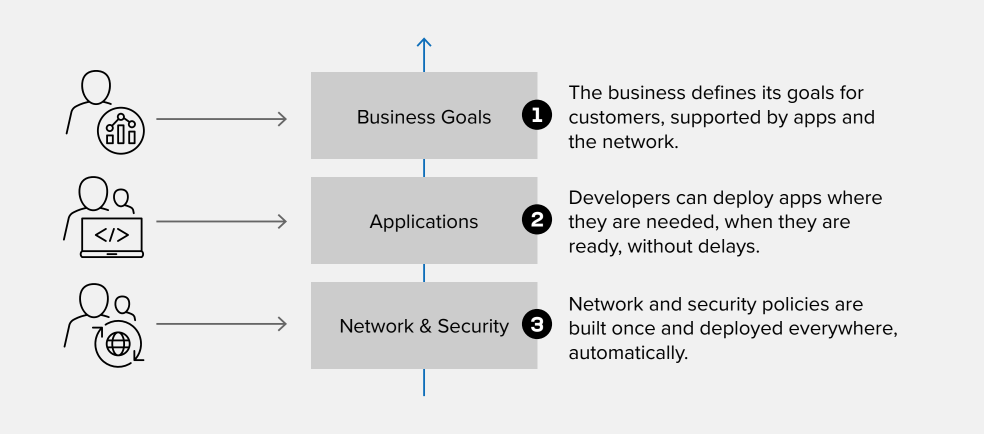
Figure 7: Distributed Cloud App Connect offers a simple, secure, and scalable approach to application portability and migrations.

- **Consistent Operational Model**. Integrate app delivery and security in a single stack, with a consistent operational model everywhere regardless of location. DevOps teams can focus on innovation and development by ensuring a standard deployment and management experience, rather than grappling with the nuances of different cloud environments, reducing operational complexity.

Gain centralized visibility of applications across multiple clouds, enabling NetOps to monitor and manage app performance across their entire network infrastructure and connected sites.

- **Centralized Observability Across All Clouds**. Gain centralized visibility of applications across multiple clouds, enabling NetOps to monitor and manage app performance across their entire network infrastructure and connected sites. It simplifies the complexity associated with multicloud networks by providing clear insights into performance metrics, security posture, and operational statuses across all cloud platforms.
- **Consistent Application Security**. Enforce consistent security policies across applications deployed in any environment, providing end-to-end encryption, access controls, and threat detection. This consistency ensures that security is never compromised during application migrations, thus upholding the integrity of the data and user trust.
- **App Connectivity and Migrations**. Seamlessly connect application service communications across clouds with private, global connectivity, making application migrations and workload portability across clouds a hassle-free experience that can often be achieved with a single click.
- **External Kubernetes Networking**. Simplify networking between Kubernetes clusters on different cloud providers. Gain centralized visibility for workloads deployed across various Kubernetes distributions.

Building a Foundation with F5 Distributed Cloud Services



1 The business defines its goals for customers, supported by apps and the network.

2 Developers can deploy apps where they are needed, when they are ready, without delays.

3 Network and security policies are built once and deployed everywhere, automatically.

Figure 8: Distributed Cloud Services provides a strategic infrastructure foundation that empowers businesses to easily build and deploy network and security policies, effortlessly distribute and connect applications, and drive app velocity.

Distributed Cloud App Connect provides a strategic infrastructure foundation that empowers businesses to effortlessly distribute and connect applications. It negates the need to stitch together multiple traditional network topologies, allowing even those with limited networking expertise to build a robust application distribution system. The visibility offered by Distributed Cloud App Connect enables the easy movement of workloads between environments, ensuring that applications are always optimally positioned for performance and cost effectiveness.

F5 Distributed Cloud Services transcend conventional network boundaries, offering a scalable, secure, and efficient mechanism for managing app connectivity and migrations. Empowering organizations to embrace a multicloud strategy, with increased security and network reliability.

F5 Distributed Cloud Services transcend conventional network boundaries, offering a scalable, secure, and efficient mechanism for managing app connectivity and migrations.

Contact us for more information or to schedule a demo.

DC 07.2024 | WP-GTM-1383966259