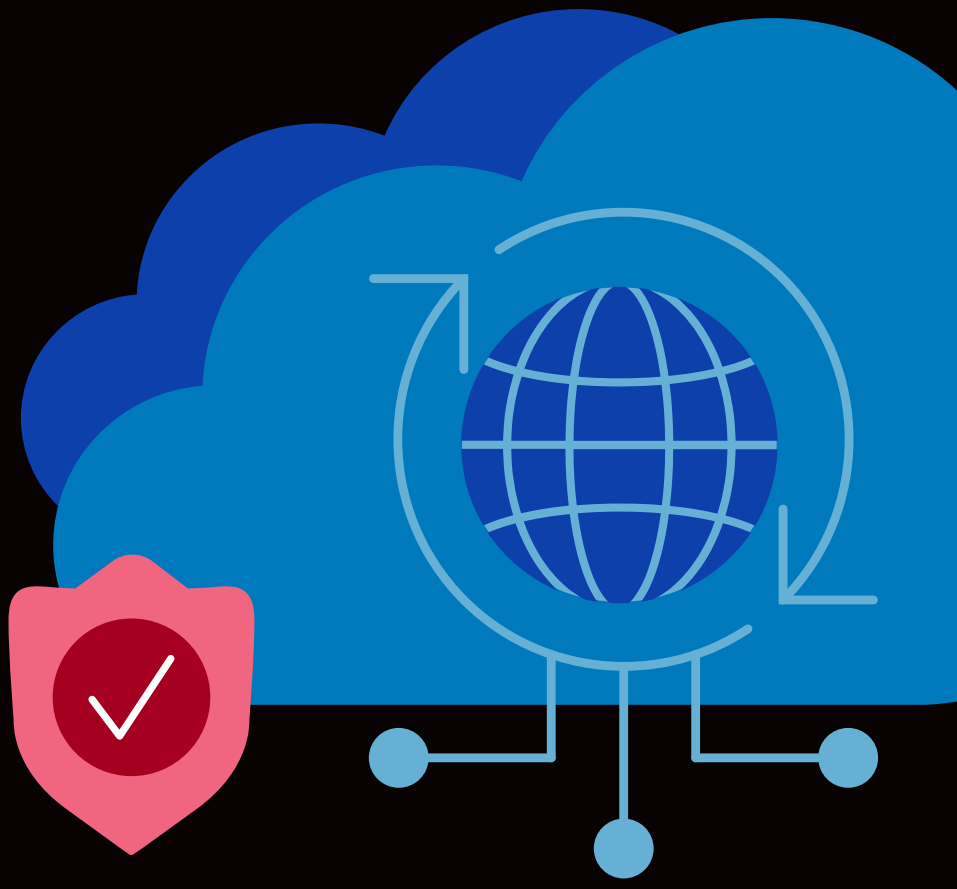
Solution Overview

How to Securely Connect Your Clouds and Networks

F5 Distributed Cloud Network Connect, part of the multi-cloud networking solution from F5 Distributed Cloud Services, delivers high-performance networking and security across public and private clouds.



KEY FEATURES

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

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.

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 selfservice 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.

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

Overcoming Cloud Networking Challenges

Navigating a complex environment for business transformation

Organizations that seek to transform their businesses have directed their IT teams to transition to public clouds, seeking benefits like agility, flexibility, and simplicity. However, as they continue to move their operations into the cloud, they face new challenges that require specific skills in cloud networking to manage connectivity across different products and environments.

To recognize the benefits of the cloud, such as cost savings, efficient IT resource utilization, and scalability, it is essential to address the challenges faced by infrastructure and operations teams in managing networking and security in the cloud. Some of these challenges include:

- **Incompatibilities and delays.** Network Operations (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 expertise with native toolsets across every cloud provider. This makes the skills gap a very real problem for them to solve when attempting to build a solution for secure connectivity between different clouds and/or their on-prem and edge sites.
- **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.
- **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, increasing security risks across their environment.
- **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.

KEY BENEFITS

Automate cloud network provisioning
One-click provisioning for establishing connectivity and security between 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.

Secure network traffic
Enable network capabilities such as BGP, access controls, and security at all sites with other F5 products and third-party services.

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.

Streamline network operations with an AI assistant
Use natural language queries to get real-time AI-powered insights into network traffic posture, detect anomalies, and offers actionable recommendations.

- **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.
- **Security.** Network teams need to maintain a security mindset. Implementing solutions that minimize the friction with SecOps teams will allow them to 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.
- **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 any outages.

Streamline Cloud Networking with F5 Distributed Cloud Network Connect

F5 Distributed Cloud Network Connect is a SaaS-based solution that offers easy, secure, and consolidated connectivity across public and hybrid clouds, data centers, and edge sites. It provides unified policies and single-pane-of-glass management, reducing complexity and increasing efficiency.

Network Connect automates the configuration of native public cloud networking resources in AWS, Microsoft Azure, and Google Cloud Platform, and it seamlessly connects multiple clouds using site-to-site connectivity over a private backbone or the F5 Global Network. The Distributed Cloud platform provides multi-tenancy and segmentation, enabling self-service capabilities for DevOps without compromising network stability or security.

Network Connect differentiates itself from competitors with its centralized management, self-service capabilities, support for commonly used tools, automation, and available private transit using the F5 global backbone.

- Consolidated networking and security services, with unified, cloud-agnostic policies.
- Centralized management plane with distributed control and data plane across cloud, physical sites, and edge.
- Full multi-tenancy/self-service for collaboration across DevOps, NetOps, and SecOps.
- SaaS-based operations with single pane-of-glass for policy, lifecycle management, and end-to-end observability.
- F5's Terraform provider and public APIs that deliver to the automation needs of app teams.

- Support for commonly used tools such as Opsgenie and Slack for alerting and Splunk and Datadog for SIEM, simplifying life for DevOps and SecOps.
- The F5 Global Network a high-capacity global physical backbone that is optionally available with the Distributed Cloud Private Link solution. This is a last-mile physical connection that enables end-to-end private transit between the customer's data centers and public cloud providers.

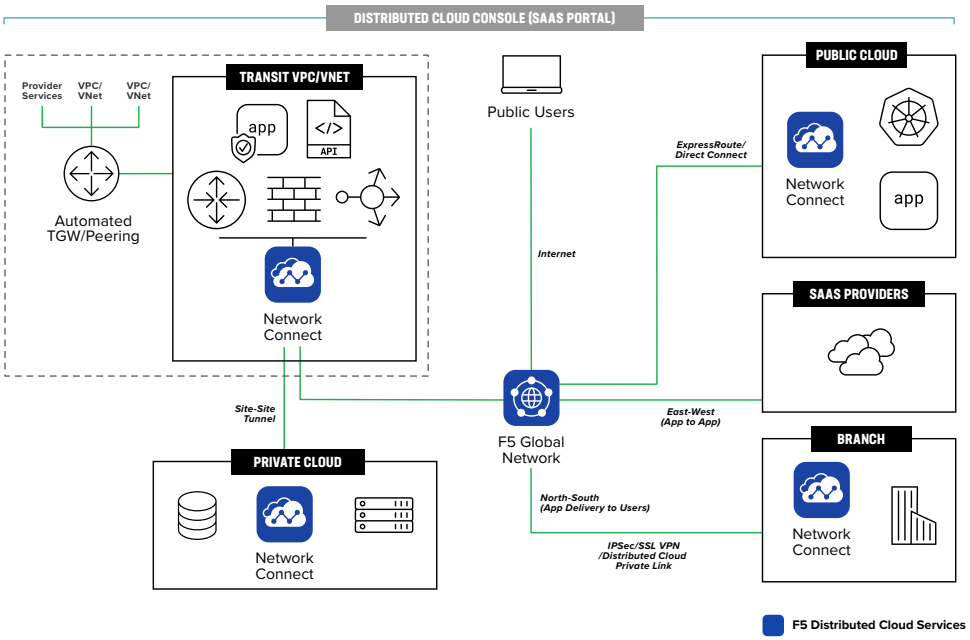


Figure 1: A visual look at how Multicloud Transit works inside Distributed Cloud Network Connect

Conclusion

Multicloud transit is easy using F5 Distributed Cloud Network Connect.

Next Steps

See how F5 Distributed Cloud Network Connect works with a free trial.

Find out how F5 products and solutions can enable you to achieve your goals. Contact F5 today.