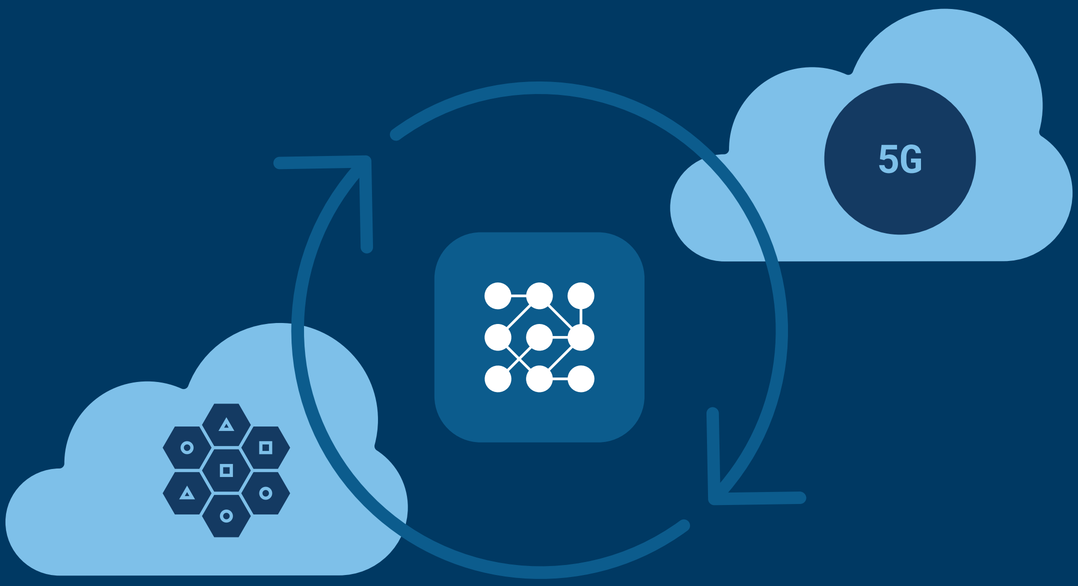
SOLUTION OVERVIEW

Deploy, Manage, and Monitor CNFs at Scale with F5 Aspen Mesh

F5 cloud-native solutions help to simplify 5G standalone deployments, improve security, facilitate multi-vendor CNF management, and decrease outages and performance hits associated with unplanned configuration changes.



KEY BENEFITS

Ideal for deploying a 5G standalone network
Speed up transition from 4G VNFs to 5G CNFs. Evaluate 5G CNFs head-to-head.

Built-in visibility
Aspen Mesh Packet Inspector enables service mesh visibility with traffic capture.

Full-featured
Open source Istio capabilities with traffic control and policy enforcement.

The Challenge of Transitioning to a Cloud-Native Network

The move to a cloud-native approach signifies that service providers are embracing the 5G standalone architecture, which relies on microservices deployed as CNFs within the service-based architecture. This shift enables improved operational efficiency and reduces the overall cost of doing business. It paves the way for new cloud-based services to be brought to the market enabling edge processing, reduced latency, and greater available bandwidth. The move from non-standalone to stand-alone involves the adoption of cutting-edge technology. Preserving or migrating legacy 4G services, as well as allowing network visibility, are essential for monitoring the operation of the network, onboarding new vendors, and evaluating and qualifying new CNF offerings for future deployment.

The benefits of a multi-vendor environment

A multi-vendor CNF deployment environment allows service providers to bring the best applications to market. However, this approach can often give rise to deployment concerns. Operators must maintain control over their CNF deployments and service offerings, ensuring a strict security posture and packet-level visibility into the operation of each CNF, all deployed on a unified platform. Many CNF vendors prefer to deploy on top of a pre-configured environment where the vendor retains control of the CNF configuration, the deployment environment, configurations, and security settings. To optimize CNF security, performance, and operational efficiency, operators need to:

1. Maintain control over each deployment environment.
2. Access security and performance settings for each environment.
3. Install monitoring hooks to assess performance tradeoffs across each platform and CNF.

These three areas are often at loggerheads with each other.

The need for advanced capabilities

Service providers must meet the demands of high availability and disaster recovery scenarios, and ensure that data and service availability comply with government regulations. These requirements align directly with the capabilities of the F5® Aspen Mesh service delivery platform. This means that the service provider can confidently deploy 5G standalone CNF-based services in a fully supported, visible, and secure manner.

OPERATORS MUST MAINTAIN CONTROL OVER THEIR CNF DEPLOYMENTS AND SERVICE OFFERINGS, ENSURING A STRICT SECURITY POSTURE AND PACKET-LEVEL VISIBILITY INTO THE OPERATION OF EACH CNF.

THE F5 ASPEN MESH MICROSERVICE DEPLOYMENT PLATFORM ALLOWS THE TRANSITION FROM VNF TO CNF APPLICATIONS, TO MOVE TO A MULTI-VENDOR ENVIRONMENT AND THE DEPLOYMENT OF CNFS AT SCALE.

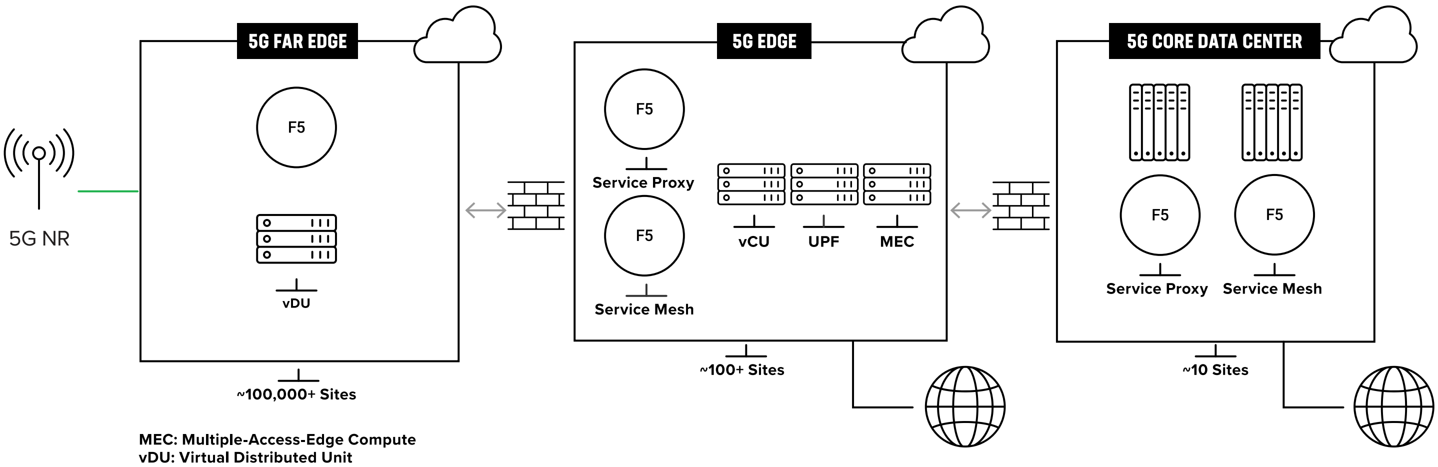
Supporting the transition

Support can be a challenging issue for service providers, especially with open source software. Questions arise about who will provide bug-fixes, feature updates, and resolutions to CVE (Common Vulnerabilities and Exposures) reports. Additionally, who will provide training and in-depth expert knowledge beyond what the service provider possesses in-house? Aspen Mesh is maintained and fully supported with training also available.

F5 Aspen Mesh Solves Many Challenges

Aspen Mesh is a microservice deployment solution that controls service-to-service communication in a microservices architecture, enabling real-time updates of policies and configurations across all data planes within the service mesh. It offers observability, security, and traffic management for east/west traffic flowing within and between Kubernetes clusters, while also providing the tools to ensure network security and visibility.

Aspen Mesh enables the transition from VNF to CNF applications, facilitating a move to a multi-vendor environment and the deployment of CNFs at scale. Simultaneously, it supports back-office IT applications while helping to regain control of the deployment platform and associated security settings.



MEC: Multiple-Access-Edge Compute
vDU: Virtual Distributed Unit
vCU: Virtual Central Unit
UPF: User Plane Function

Figure 1: F5 infrastructure solution scaling capability for service providers

KEY FEATURES

Robust security by default
Configuration provides for strict security capability out of the box.

Fully supported
24x7 white glove support and training.

With Aspen Mesh, operators can:

- Develop, test, fine-tune, and deploy new cloud-native offerings.
- Solve vendor and CNF lifecycle management challenges.
- Ensure compliance with government regulation and internal auditing requirements.
- Deploy large-scale or complex workloads.
- Achieve service visibility to aid fault-finding and configuration verification.
- Enable high availability and disaster recovery scenarios.
- Attain deployment agility and avoid single vendor lock-in.

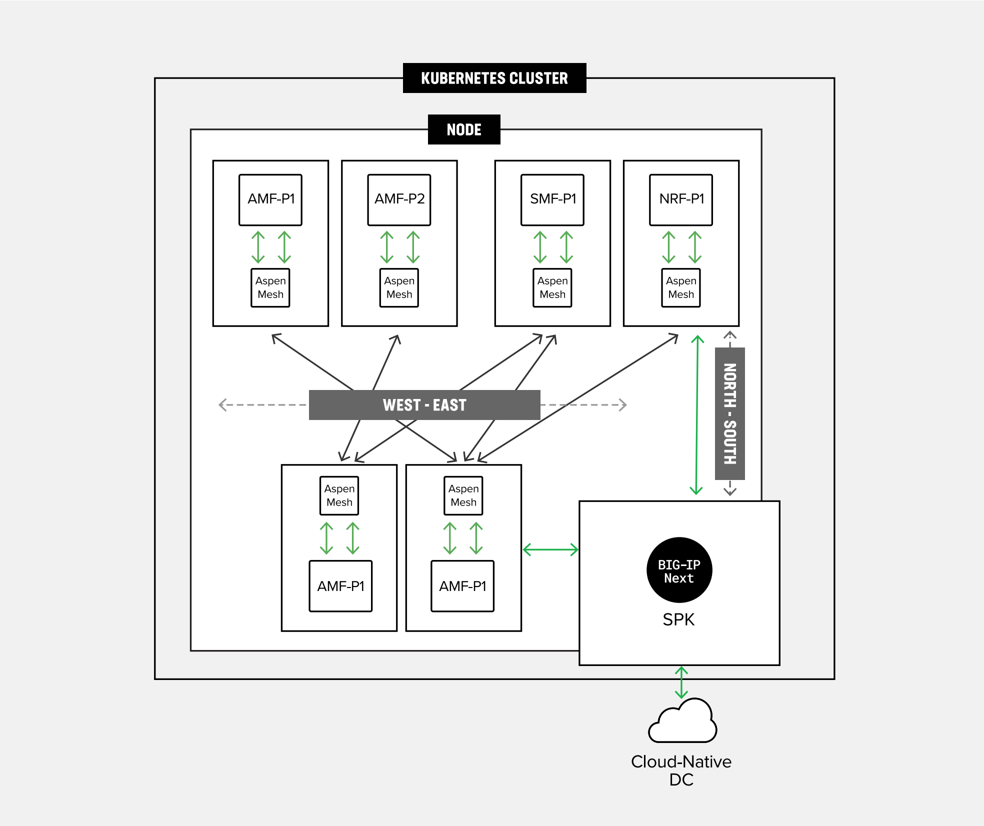


Figure 2: F5 BIG-IP Next Service Proxy for Kubernetes and F5 Aspen Mesh deployment

Aspen Mesh Provides the Power to Deploy CNFs with Confidence

ASPEN MESH PACKET INSPECTOR HELPS TO BRIDGE THE GAP IN VISIBILITY INTO THE SERVICES AND THEIR INTERACTIONS, PRESENTING DATA IN A MANNER EASILY UNDERSTANDABLE TO COMMONLY USED ANALYTIC TOOLS.

Certificate Management

Mutual Transport Layer Security (mTLS) is used for authentication and encryption for all communications in the 5G core network. Managing certificates at scale is complex, and achieving TLS interoperability between vendors can be challenging, with no assurance of consistent security across different vendors. Aspen Mesh resolves the certificate management problem centrally.

Traffic Inspection

Traditionally, physical probes were used to capture traffic for regulatory or operational needs, but this becomes unfeasible in the context of encrypted microservice communications. Aspen Mesh addresses this challenge with Aspen Mesh Packet Inspector. This solution helps to bridge the gap in visibility into the services and their interactions, presenting data in a manner easily understandable to commonly used analytic tools. CNF traffic is captured directly at the sidecar, including intra-node CNF traffic, which reduces SSL decryption load. This integration seamlessly interfaces with the existing service assurance infrastructure, enabling full packet visibility across the service mesh and service-based architecture, which is scalable and extensible with support for existing packet broker APIs. This unique capability sets Aspen Mesh apart and plays a critical role in automating the deployment environment.

Observability

Scale and complexity challenges are common when network functions are implemented as discrete microservices. Keeping track of traffic flows within the cluster can be challenging. Aspen Mesh resolves the observability issue at both layer 4 and layer 7, driving graphical dashboards.

Additionally, Aspen Mesh provides 24/7 support, training, bug fixes, and access to in-depth expert knowledge.

Conclusion

ASPEN MESH ALLOWS CONTROL OVER SECURITY SETTINGS, PREVENTS UNPLANNED CONFIGURATION CHANGES, AND ENSURES THE ISOLATION OF CNFS FROM EACH OTHER AS WELL AS DIFFERENT VENDORS FROM ONE ANOTHER.

Whether you are planning to deploy a 5G standalone service-based architecture for CNFs with built-in security and visibility, transitioning from 4G VNF to 5G CNF-based services to enable a quicker transition to a unified 5G standalone core, or deploying new back-office IT applications leveraging microservices, Aspen Mesh can help you deploy faster, more securely, and with better visibility.

With peace of mind, service providers can now confidently deploy and manage a multi-vendor CNF environment that resolves many common concerns. Aspen Mesh allows control over security settings, prevents unplanned configuration changes, and ensures the isolation of CNFs from each other as well as different vendors from one another. Operators can now easily manage multiple vendors, services, and CNF network elements, all while managing the operating lifecycle for each when deployed on a unified 5G CNF deployment platform.

To learn more, contact your F5 representative, or visit F5.