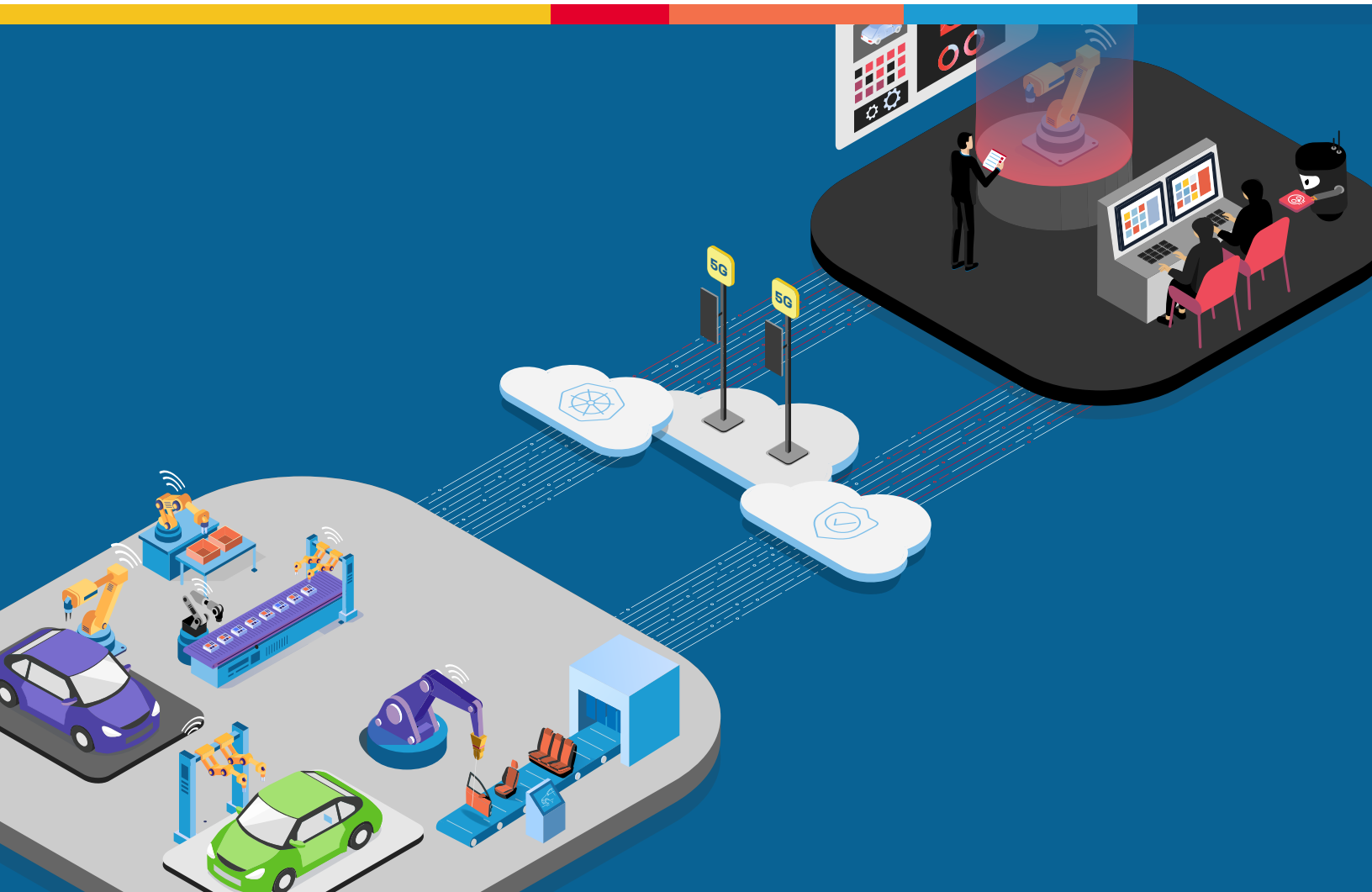
SOLUTION OVERVIEW

5G Cloud-Native Infrastructure

F5's 5G infrastructure solutions combine powerful tools for managing and securing traffic into and within containerized networks, providing the tools service providers need to modernize their network infrastructure.



KEY BENEFITS

Control
Applies policy control and intelligent traffic management over multiple traffic types that are unique to a service provider network.

Security
Provides a single point for network security controls for traffic into and within service provider's cloud-native infrastructure.

Visibility
Supports visibility of traffic flow into and within the infrastructure for greater operational efficiency, more efficient troubleshooting, and flexible revenue controls.

Service-based architecture (SBA) and a cloud-native infrastructure are crucial first steps in deploying a standalone (SA) 5G Core network. A critical inflection point occurs as service providers implement SBA thus entering an application-centric world where workloads can be dynamically scaled in real time to meet ever-changing consumer demands. 5G makes it possible to deploy and manage distributed networks needed to satisfy the growing number of enterprise initiatives from Industry 4.0 and FinTech to autonomous vehicles and smart cities. The evolution to a cloud-native infrastructure for 5G deployments align with service provider's broader digital transformation initiative to implement a distributed cloud from core to edge and leverage the public cloud. Service providers now need to build a multi-cloud network to satisfy the increasing demand for instantaneous access to cloud services from the core, edge, and far-edge of the network. A cloud-native infrastructure is the catalyst that merges traditional service provider "IT" and "network" groups creating an app-centric 5G network.

Why This Is an Issue

Service providers implementing a cloud-native infrastructure are pioneers in their digital transformation journey. The one-size-fits-all approach no longer applies to 5G networks, where multiple cloud deployments are merely a starting point. 5G infrastructure is built on a cloud-native containerized architecture, where container workloads are managed using Kubernetes, which orchestrates applications based on network requirements. However, Kubernetes was not specifically designed for carrier-grade deployments or the business need for service providers to keep complexity and cost to a minimum, while ensuring the infrastructure is secure. As service providers deploy Kubernetes based cloud-native infrastructure, it is important to understand the limitations of standard Kubernetes in a service provider environment:

Kubernetes networking needs to integrate into the broader service provider network

Kubernetes networking does not natively provide a central point for network traffic ingress/egress. Exposing internal Kubernetes networking to the external service provider network will lead to increased operational complexity and cost.

Service provider network functions are different from IT apps

Service provider networks utilize multiple protocols (SIP, GTP, SCTP, etc.) that are not natively supported by Kubernetes but are critical as service providers make the transition from 4G to 5G.

Kubernetes clusters need to be secured and protected

As Kubernetes cloud-native infrastructures are deployed there is a risk of expanding the attack surface because Kubernetes does not provide a single point for networking security control.

THE USE OF A SERVICE PROXY AND SERVICE MESH INTEGRATES WITH KUBERNETES MANAGEMENT AND ORCHESTRATION PROVIDING A COMPLETE SOLUTION THAT CAN MEET THE DEMANDING REQUIREMENTS OF SERVICE PROVIDER USE CASES.

What You Should Do

Kubernetes is the industry solution for building cloud-native infrastructure. However, careful consideration needs to be made in how Kubernetes is integrated into service provider use cases. One approach that has been taken by some is to circumvent Kubernetes design patterns, which can reduce most of the benefits of Kubernetes and cloud-native principles. Additionally, circumventing Kubernetes design patterns will lead to increased operational and networking complexity, plus an increased security attack surface. This has been seen with service providers who are taking a horizontal stack approach with their infrastructure deploying a multiple-vendor CNF or single vendor vertical stack approach.

The alternative approach is to implement a solution that aligns with Kubernetes design patterns where there is a single point for networking control and security for cluster ingress/egress traffic, a “Service Proxy”, plus a “Service Mesh” for visibility, control, and security for traffic within the cluster. The use of a service proxy and service mesh integrates with Kubernetes management and orchestration providing a complete solution that can meet the demanding requirements of service provider use cases. This solution can be integrated with a service provider’s horizontal stack or single-vendor vertical stack. Aligning with Kubernetes design patterns will lead to reduced complexity, lower operational cost, and greater security.

How F5 Can Help

F5 enables the visibility, control, and security needed for 5G cloud-native deployments. F5’s 5G Cloud-Native Infrastructure solution is comprised of two products:

- BIG-IP Next Service Proxy for Kubernetes (SPK)
- Carrier-grade Aspen Mesh

BIG-IP NEXT SERVICE PROXY FOR KUBERNETES (SPK)

BIG-IP Next Service Proxy for Kubernetes (SPK) provides critical carrier-grade capabilities to a Kubernetes environment, enabling extended performance and security for cloud-native 5G deployments. SPK features include:

- **Scale:** F5’s solution can scale to hundreds of thousands of sites.

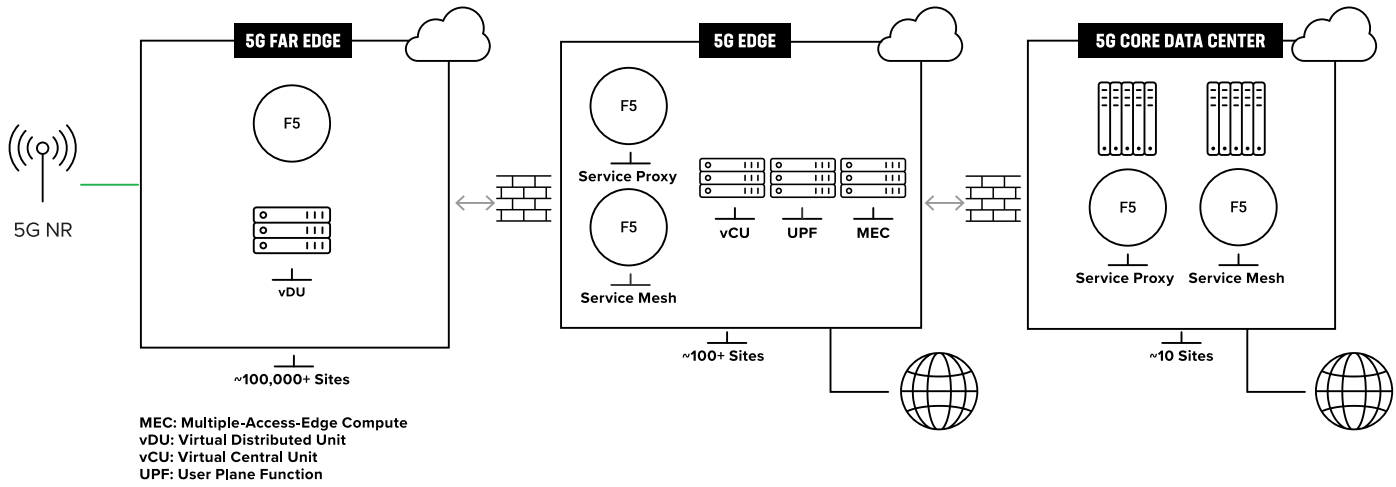


Figure 1: F5 infrastructure solution scaling capability

- **5G Ingress/Egress Control:** Intelligent handling of messaging protocols enabling signaling control for routing and load balancing. An example: Diameter signaling can now be scaled for multiple containers, enabling the interworking of 4G and 5G signaling.

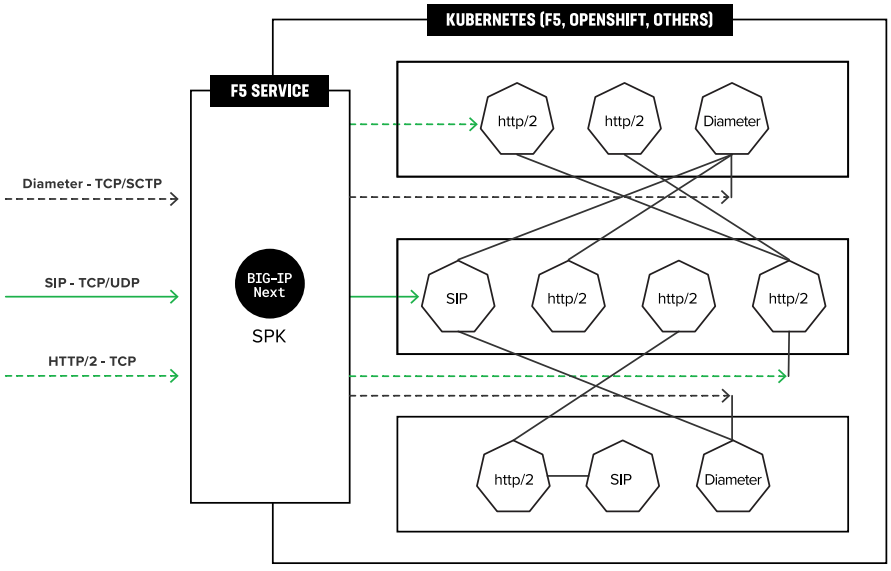


Figure 2: F5's BIG-IP Next Service Proxy for Kubernetes provides visibility into a service provider's network.

KEY FUNCTIONALITIES OF SPK AND CARRIER-GRADE MESH

Ingress/Egress Control

- L4 Load Balancing – TCP, UDP, and SCTP
- L7 Load Balancing – Diameter, SIP, HTTP/2
- GTPcV2 Load Balancing
- Routing
- Rate limiting
- Management across clusters providing load balancing capabilities

Security

- Signaling firewall, DDoS, WAF
- Encryption /Decryption
- Topology hiding
- Encryption via mutual TLS (mTLS)
- L7 policy management
- Simple insertion point for provider-owned and policy

Visibility

- Revenue assurance
- Statistics and analytics
- Packet capture for traceability
- Service discovery

- **Per-subscriber traffic visibility:** Enabling per-subscriber visibility at ingress provides traceability over any event that needs to be tracked for compliance and billing purposes.
- **Load balancing:** Provides load balancing for Layer 4 and Layer 7 (TCP, UDP, SCTP, HTTP/S, HTTP/2/S, Diameter, GTPcV2, and SIP).
- **4G and 5G signaling protocol support:** TCP, UDP, SCTP, HTTP/S, HTTP/2/S, Diameter, GTPcV2, and SIP provide a containerized “proxy” 4G to 5G functionality.
- **Service discovery:** Provides application workload service discovery.
- **Enhanced security:** Employs a signaling firewall at traffic ingress to prevent compromised traffic from entering the Kubernetes clusters.
- **mTLS encryption:** Uses encryption through mTLS to secure service-to-service communication.
- **Topology hiding:** The internal structure of a cloud-native function (CNF) is obscured at traffic ingress.

To touch on a few of the value areas above, security services such as distributed denial-of-service (DDoS) protection, firewall, and web application firewall (WAF) can be applied at ingress to prevent malicious traffic from entering the cluster and impacting the 5G core network functions and customer applications. Additional security is also provided by SmartNIC, in partnership with Intel, which implements a signaling firewall. This firewall provides ingress security, preventing compromised traffic from entering the cluster while optimizing traffic steering, which enables a TCO reduction of 47%. The SmartNIC can be used to offload and optimize specific network services, such as cryptographic security functions and packet processing. This alleviates strain on CPU resources and prevents CPU overload resulting in significant performance improvements.

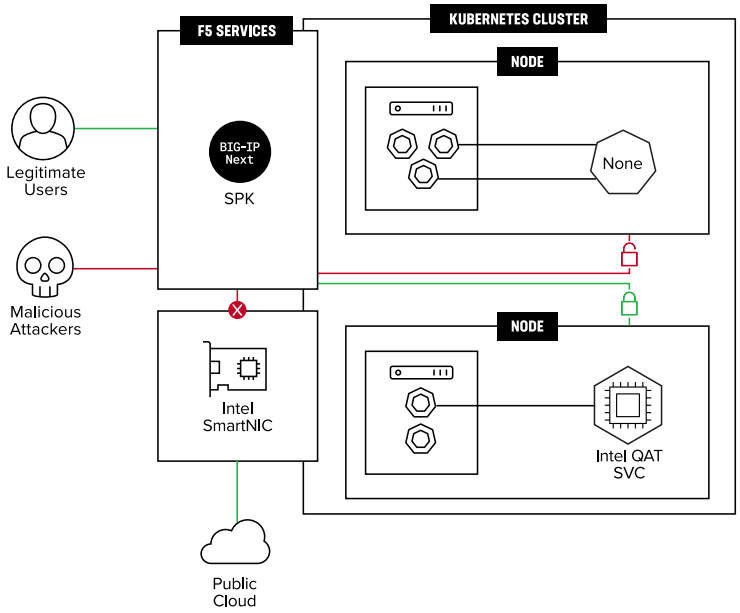


Figure 3: SmartNIC security benefits

BIG-IP NEXT SPK PROVIDES CRITICAL CARRIER-GRADE CAPABILITIES TO A KUBERNETES ENVIRONMENT, ENABLING EXTENDED PERFORMANCE AND SECURITY FOR CLOUD-NATIVE 5G DEPLOYMENTS.

Container visibility is also critical in providing revenue assurance by offering detailed transaction records. The entry point to the Kubernetes cluster is the ideal location to gather information for compliance and billing.

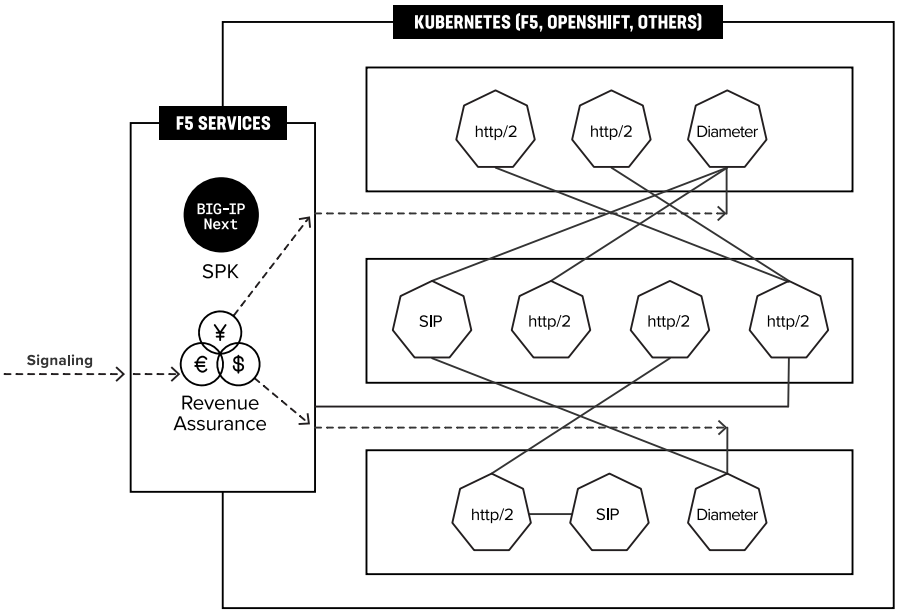


Figure 4: F5's BIG-IP Next Service Proxy for Kubernetes provides revenue assurance by enabling visibility into a service provider's network.

ASPEN MESH

F5's service mesh delivers a configurable, low-latency infrastructure layer designed to handle high volume communication among services using APIs, while providing critical capabilities, such as:

- Service discovery
- Observability
- Encryption via mutual TLS (mTLS)
- Packet capture for traceability
- L7 policy management
- Management across clusters providing load-balancing capabilities
- Simple insertion point for provider-owned certifications and policy

SIDECARS HANDLE INTERSERVICE COMMUNICATIONS, MONITORING, AND SECURITY RELATED CONCERNS, THUS OFFERING AN ABSTRACTION LAYER FOR INDIVIDUAL SERVICES (APPLICATIONS).

The service mesh builds on open source Istio and is implemented by providing a proxy instance, called a sidecar, for each service instance. Sidecars handle interservice communications, monitoring, and security related concerns, thus offering an abstraction layer for individual services (applications). By providing a sidecar data plane at every app (CNF container), F5 Aspen Mesh can intercept all ingress and egress container traffic. This capability enables CNF sidecar traffic capture, including intra-node CNF traffic and pre-encryption tapping, and also reduces SSL load for brokers. The service proxy easily integrates with existing infrastructure, provides full packet visibility, is scalable and extensible, and uses existing packet broker APIs.

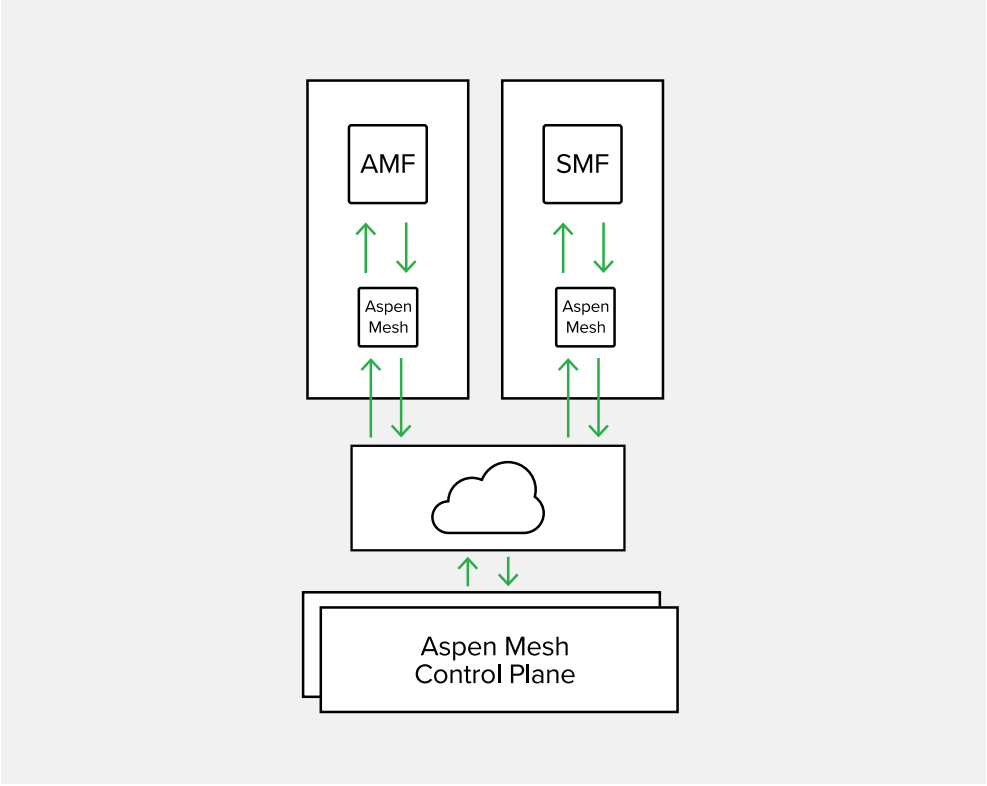


Figure 5: Aspen Mesh sidecar view

Conclusion

F5's cloud-native infrastructure solution is essential for all top-tier service providers delivering visibility, control, security, and scale for 5G network deployments. This solution is pivotal in reducing cost and complexity when deploying and operating a 5G network for the core, edge, and far edge.

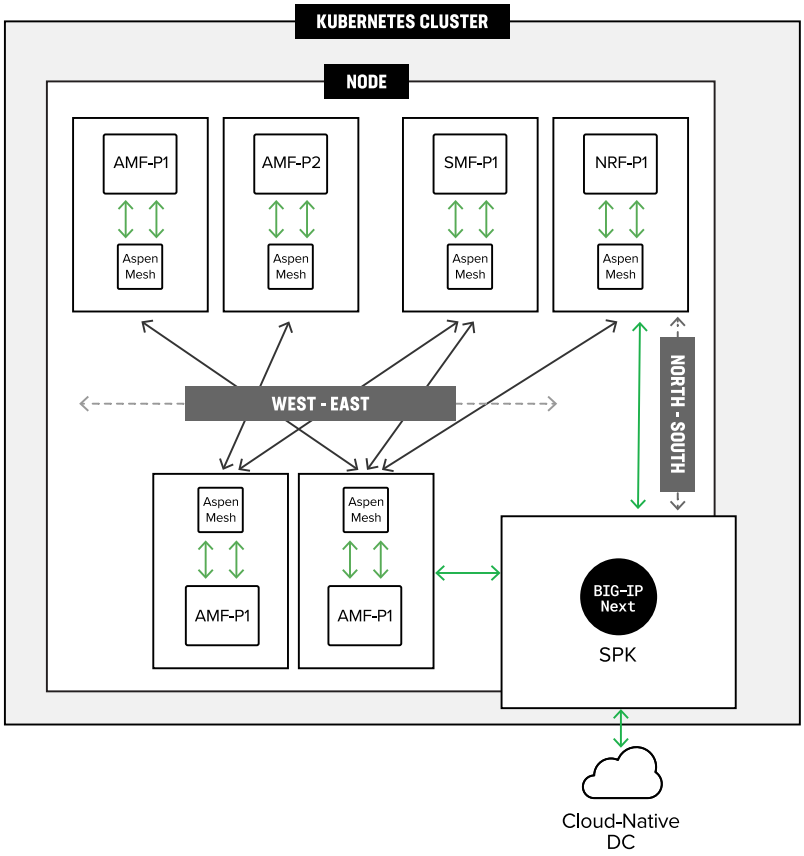


Figure 6: F5 BIG-IP Next Service Proxy for Kubernetes and Aspen Mesh deployment option.

To learn more, contact your F5 representative, or visit F5 Service Provider Solutions.