5G Cloud-Native Infrastructure

F5's 5G Infrastructure solution combines powerful tools for managing traffic into and within containerized networks, providing the tools service providers need to manage next-generation networks.

KEY BENEFITS

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

Security
Enabling security controls that are applied at multiple points in the network and across multiple layers.

Visibility
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 is a crucial first step in deploying a standalone (SA) 5G Core network. A critical inflection point is occurring as service providers implement SBA thus entering an application-centric world where workloads can be dynamically scaled in real time to meet the 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. 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. 5G cloud-native infrastructure is the catalyst that merges traditional service provider "IT" and "network" groups creating an IT-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. This drives the need to prioritize the following requirements when designing and deploying 5G cloud-native infrastructure:

- **Visibility:** Network traffic visibility is vital in any mobile network and even more so in a 5G network. Kubernetes inherently does not provide ingress or egress traffic visibility into the Kubernetes nodes and clusters.
- **Security:** Security controls need to be applied at multiple points in the network and across multiple layers. Enabling packet capture and the ability to implement security at container ingress is critical in ensuring that bad traffic stays out of a service provider's network. Enabling encryption is also fundamental in a 5G network security offering.
- **Control:** Policy management and analytics enable network control and are essential in automating an already complex 5G network.

What You Should Do

Service providers migrating to a 5G cloud-native environment will have a combination of physical network functions (PNFs), virtual network functions (VNFs), and cloud-native network functions (CNFs). 4G LTE networks are still experiencing much growth and will need to be supported alongside 5G non-standalone NR and 5G Core.

Cloud-native 5G architecture along with containers are critical in enabling diversified service requirements. A container is a software package with the entire toolset needed to run an application. Containers are lightweight and efficient for quick development time and they provide security as there are no software dependencies outside of the container. Container workloads are managed with Kubernetes which automates and scales applications based on the network requirements. Containers are critical in 5G because with their dynamic nature, they can easily adapt to the needs of the network, allowing for the proper placement of the application and its workloads within a network, enabling agility, speed, and efficiency.

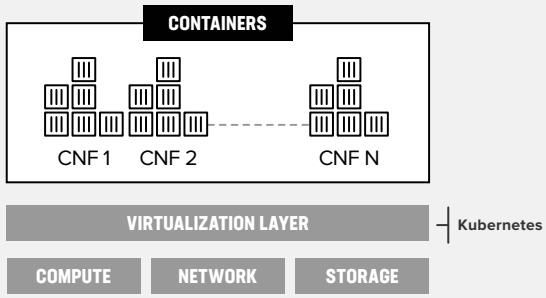

Figure 1: Cloud-native containerization

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 Service Proxy for Kubernetes (SPK)
- Aspen Mesh

BIG-IP SERVICE PROXY FOR KUBERNETES (SPK)

BIG-IP 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.

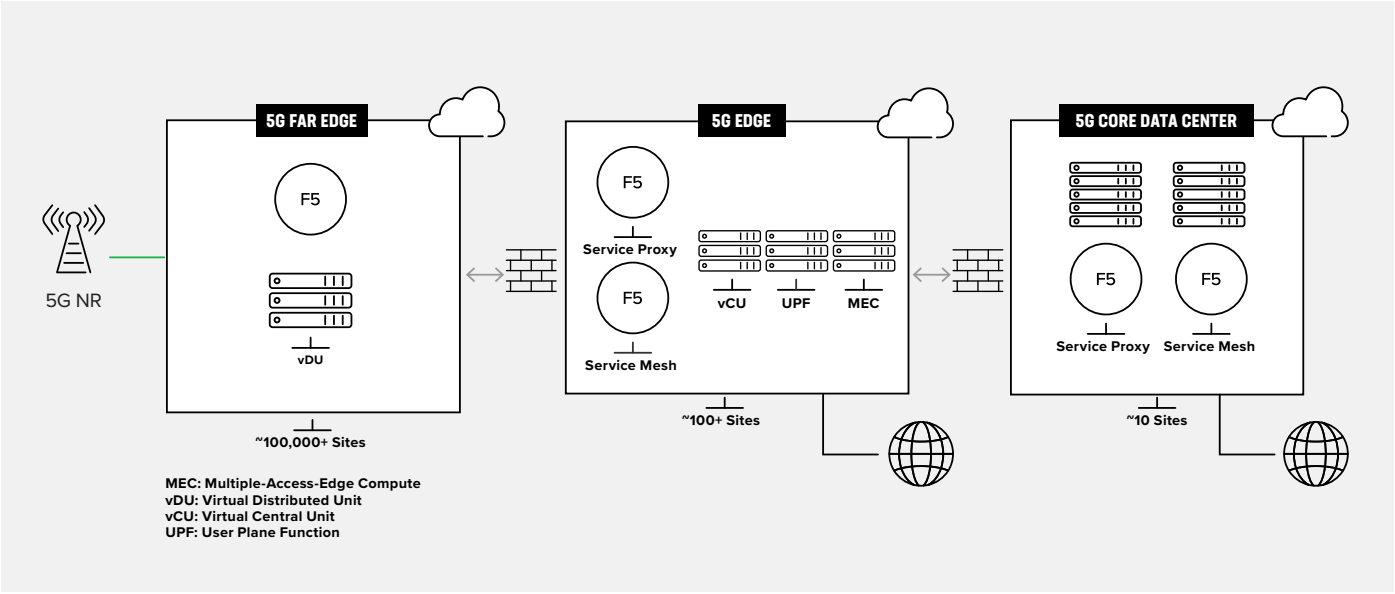

Figure 2: F5 infrastructure solution scaling capability

- **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.

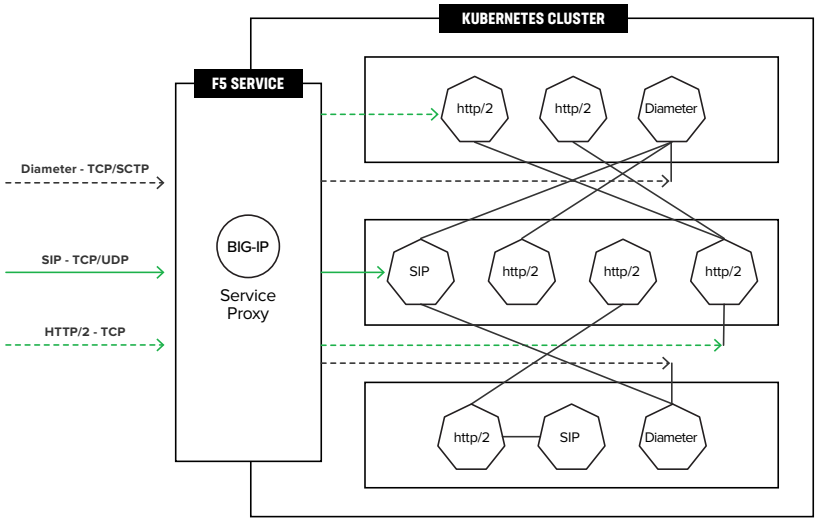

Figure 3: F5's Service Proxy for Kubernetes provides visibility into a service providers network.

- **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**: Providing a signaling firewall at traffic ingress prevents compromised traffic from entering the Kubernetes clusters.
- **mTLS encryption**: Provides 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 providing optimized 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.

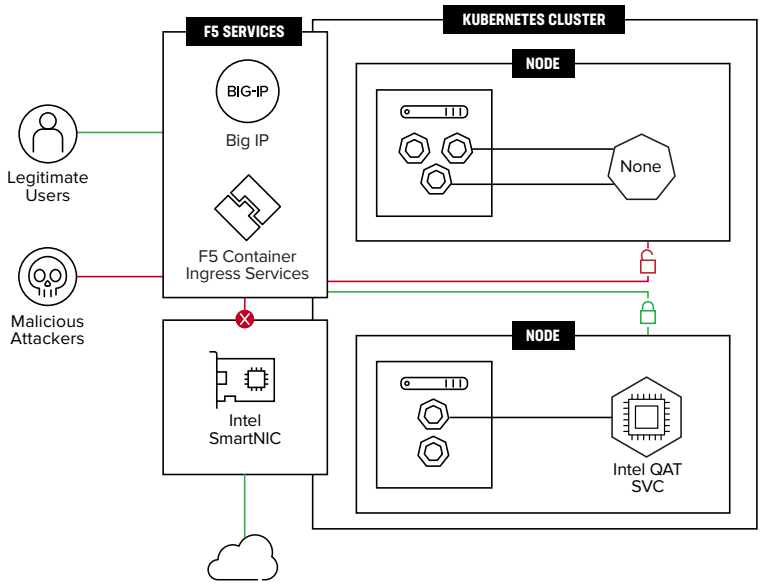

Figure 4: SmartNIC security benefits

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.

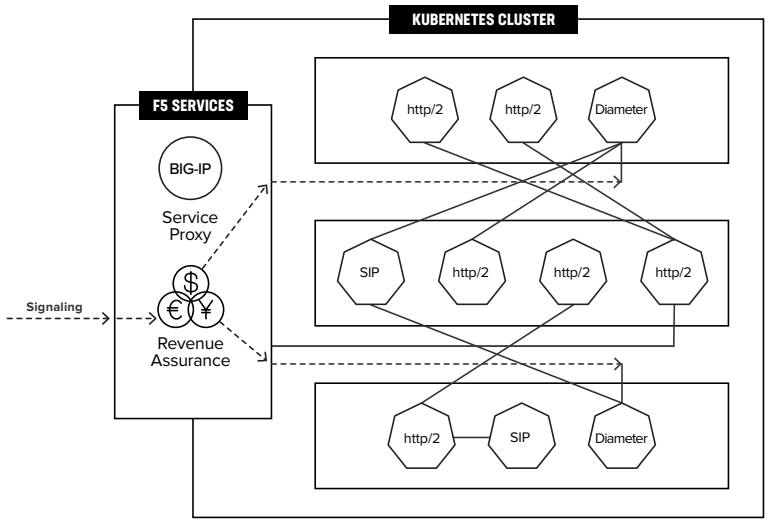

Figure 5: F5's Service Proxy for Kubernetes provides revenue assurance by enabling visibility into a service provider's network.

ASPEN MESH

F5's service mesh delivers a configurable and low-latency infrastructure layer designed to handle a high volume of communication among services using APIs and provides critical capabilities including:

- 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 certs and policy

KEY FUNCTIONALITIES OF SPK AND CARRIER-GRADE SERVICE 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
- Encrypt/Decrypt
- Topology hiding
- Encryption via mutual TLS (mTLS)
- L7 policy management
- Simple insertion point for provider-owned certs and policy

Visibility

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

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.

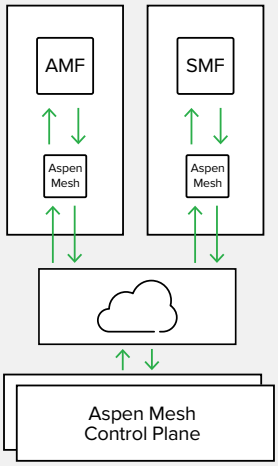

Figure 6: Aspen Mesh sidecar view

Conclusion

F5's Cloud-Native Infrastructure solution is essential for all top tier service providers, providing 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 from the core, edge, and far edge.

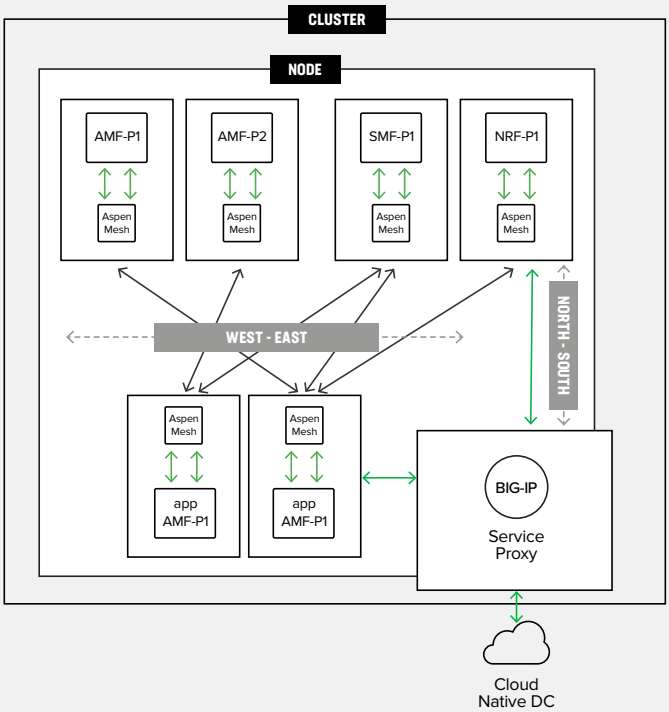

Figure 7: F5 Service Proxy for Kubernetes and Aspen Mesh deployment option.

To learn more, contact your F5 representative.