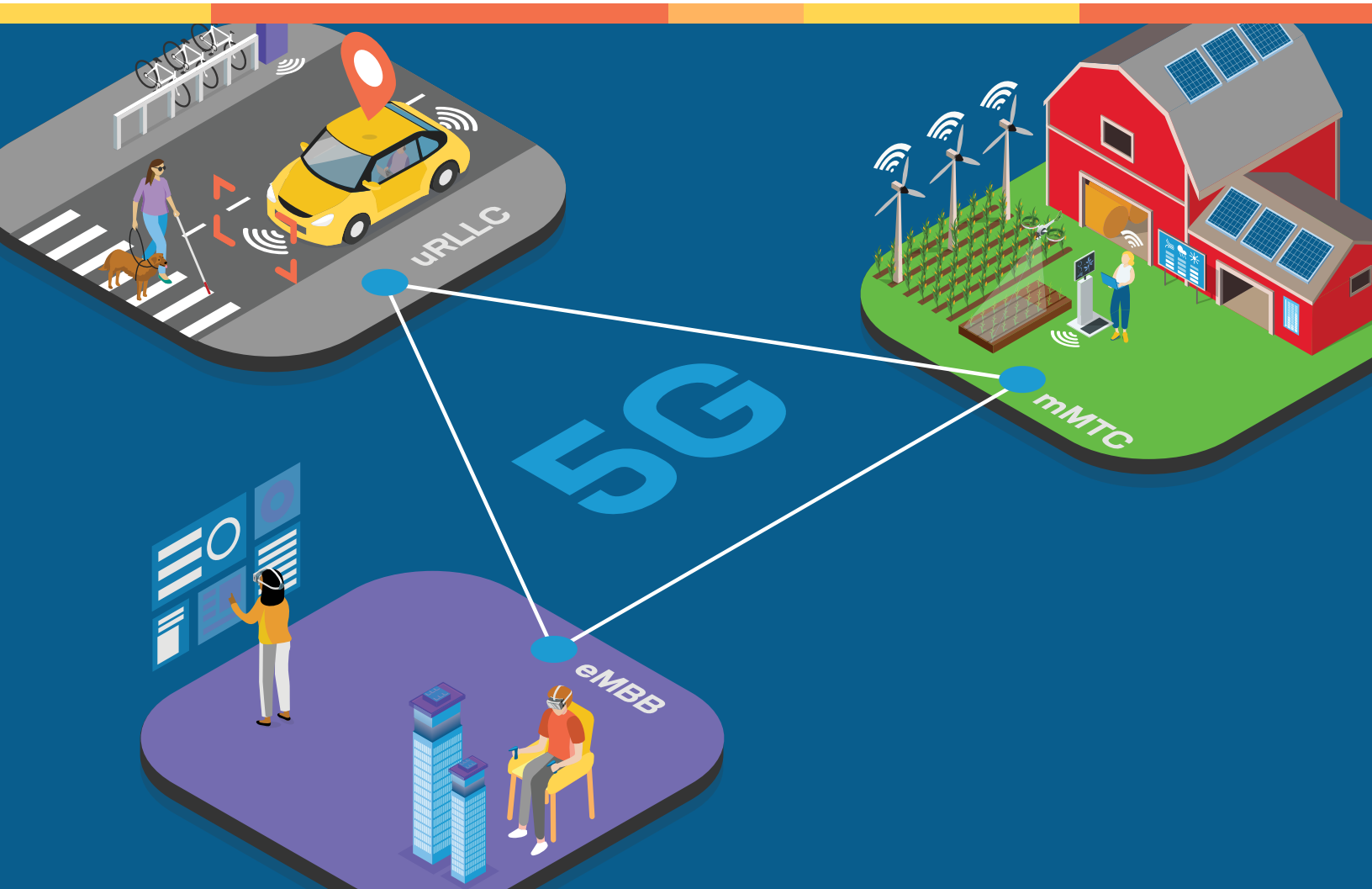
SOLUTION OVERVIEW

The Path from 4G to 5G

Balancing 4G network with 5G rollouts.



KEY BENEFITS

Control Insights
Policy control and intelligent traffic management over multiple traffic types tailored for service provider networks.

Security
Security controls at multiple points and across multiple layers, providing end-to-end network protection.

Visibility
Monitor traffic into and within the infrastructure, improving operational efficiency, easing troubleshooting, and creating flexible revenue controls.

Service providers are in a race against competitors, continuing to monetize their current investment in 4G while rapidly transitioning to 5G to ensure customer retention and competitive advantage. To enable success, it's critical to have interoperable solutions with current infrastructure for the following areas:

- Signaling interworking in the migration from 4G to 5G
- Transitioning to best of suite S/Gi-LAN to N6 service-based interface
- Implementing cloud-native 5G infrastructure

This paper aims to help the reader understand the evolution from 4G to 5G, what it enables, and how to get there.

Background

Migrating to a new mobile technology is far from straightforward and requires strong collaboration to ensure success. 5G is the turning point of innovation, accelerating new opportunities with new technologies. The key differentiator with 5G vis a vis its 4G predecessor is that 5G is designed to leverage 4G LTE technology – the new must work with the existing technology and networks. This makes the complexity and permutations boundless. The key to success for service providers is working with reliable partners that have solved the 4G challenges and continue to solve 5G challenges regardless of where the service providers are in their digital transformation journey.

5G rollouts are moving full speed ahead but what has not been clearly forged is how 4G will coexist with 5G technology. Every service provider must construct their very own unique migration path, leveraging their existing network as they try to monetize their 5G investments. 5G was by no means meant to render any technology obsolete – it was designed with the exact opposite in mind.

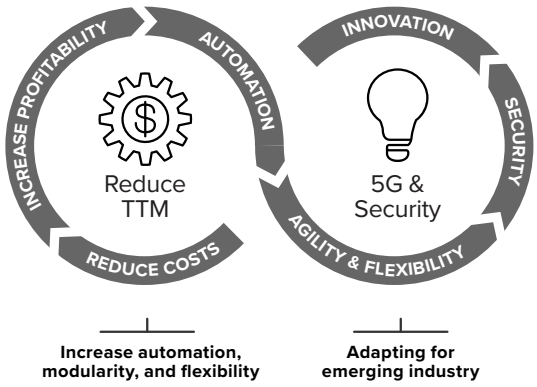


Figure 1: Unique journey from 4G to 5G

The Three Critical Areas to Solve for 5G

SIGNALING INTERWORKING IN THE MIGRATION FROM 4G TO 5G

EVERY SERVICE PROVIDER MUST CONSTRUCT THEIR VERY OWN UNIQUE MIGRATION PATH, LEVERAGING THEIR EXISTING NETWORK AS THEY TRY TO MONETIZE THEIR 5G INVESTMENTS.

Why this is an issue

There are a number of signaling challenges that a service provider must address in 5G network deployments which also exist in 4G networks. As discussed earlier, 4G and 5G networks will need to coexist as standards evolve. Disrupting existing 4G network functions (for instance charging systems) is not an option as service providers are monetizing their existing 5G network.

Signaling is the lifeblood of all cellular networks. There are common signaling challenges that face both 4G and 5G networks such as:

- Overload handling and load balancing.
- The interworking of signaling protocols between 4G and 5G hybrid networks.
- 5G roaming security, protecting interfaces between networks.

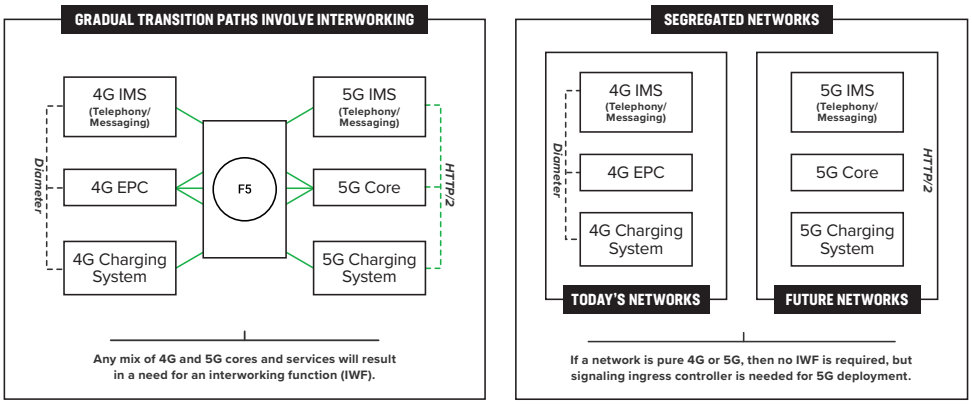


Figure 2: 4G and 5G signaling interworking

What you should do

Service providers need to plan out their signaling migration path from 4G to 5G. Unlimited scalability is critical in a mobile network. Service providers need to manage their 4G control plane traffic and signaling with Diameter session-oriented load balancing technology along with interworking with 5G HTTP/2 signaling. F5 is an industry leader in offering robust 4G signaling solutions for service providers with the BIG-IP load balancer, Diameter Routing Agent (DRA), and a Diameter Edge Agent (DEA). Therefore, transitioning to 5G is made easy by providing an interworking path between 4G and 5G signaling.

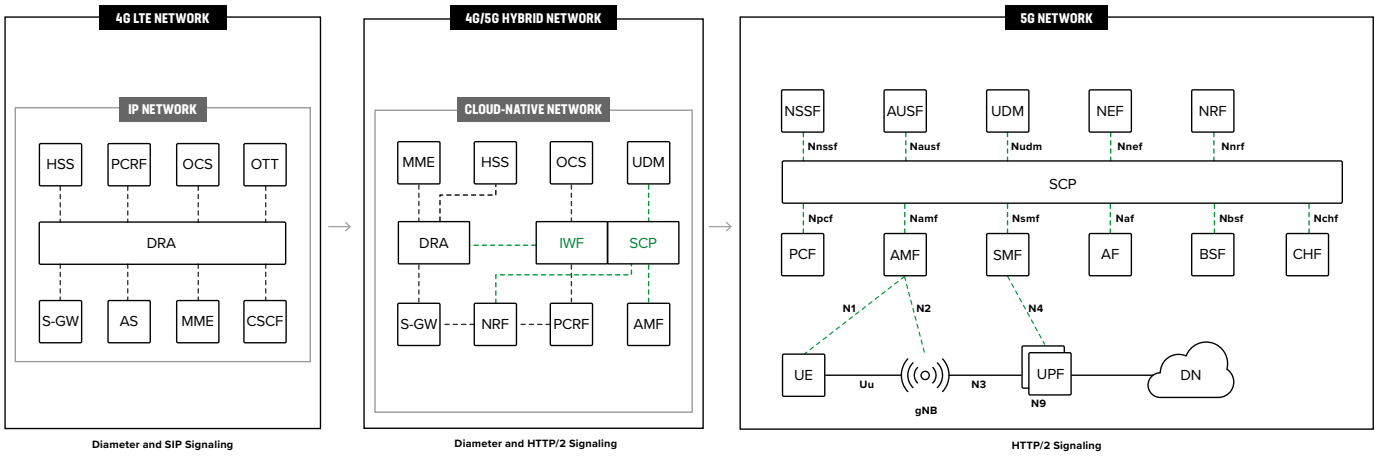


Figure 3: Mobile core signaling evolution

How F5 Can Help

F5 offers critical signaling interworking and signaling translation solutions that can successfully scale and manage 4G control plane traffic and signaling with 5G network signaling functions without compromising traffic, leading to unprecedented quality of experiences (QoE) for consumers. The table below provides insight into some of the permutations possible as service providers migrate to hybrid core mobile networks.

	4G IMS, Charging, Partners Diameter Rx	**Mixed IMS, Charging, Partners** Diameter Rx, HTTP/2 N5	**5G IMS, Charging, Partners** HTTP/2 N5
Pure 4G Packet Core Diameter Gx/Rx	**Diameter ONLY** Session Binding: **DRA**	**Interworking** Translation: N5 ➔ Rx Session Binding: DRA; Gx/N5	**Interworking** Translation: N5 ➔ Rx Session Binding: DRA; Gx/N5
4G/5G Mix Packet Core(s) Diameter Gx/Rx, HTTP/2 N4	**Interworking** Translation: Rx ➔ N5 Session Binding: DRA; N4/Rx	**Interworking** Translation: N5 ➔ Rx; Rx ➔ N5 Session Binding: DRA; Gx/N5; N4/Rx	**Interworking** Translation: N5 ➔ Rx Session Binding: Gx/N5; ; NRF/SBI
Pure 5G Packet Core HTTP/2 N4	**Interworking** Translation: Rx ➔ N5 Session Binding: N4/Rx	**Interworking** Translation: Rx ➔ N5 Session Binding: N4/Rx; NRF/SBI	**HTTP/2 ONLY** Session Binding: **NRF/SCP/SMF**

Figure 4: Hybrid core 4G/5G transition paths use IWF for applications, charging, and intercarrier

Having championed 4G signaling, F5 also provides 5G Core network signaling solutions. The F5 5G Core signaling solution includes Service Communication Proxy (SCP), Binding Session Function (BSF), and Security Edge Protection Proxy (SEPP). Together these 5G Signaling network functions address service providers 5G signaling network challenges by providing:

- Simplified network topology by applying signaling aggregation and routing.
- Load balancing, overload handling and message parameter harmonization.
- Optimization of 5G SBA signaling controls to enable better network visibility and boost network performance by continuously coordinating with other network functions.
- Support for binding session capability for 5G Voice over IMS.
- Support for 5G roaming which provides security and protection of messages exchanged between public land mobile networks (PLMNs).

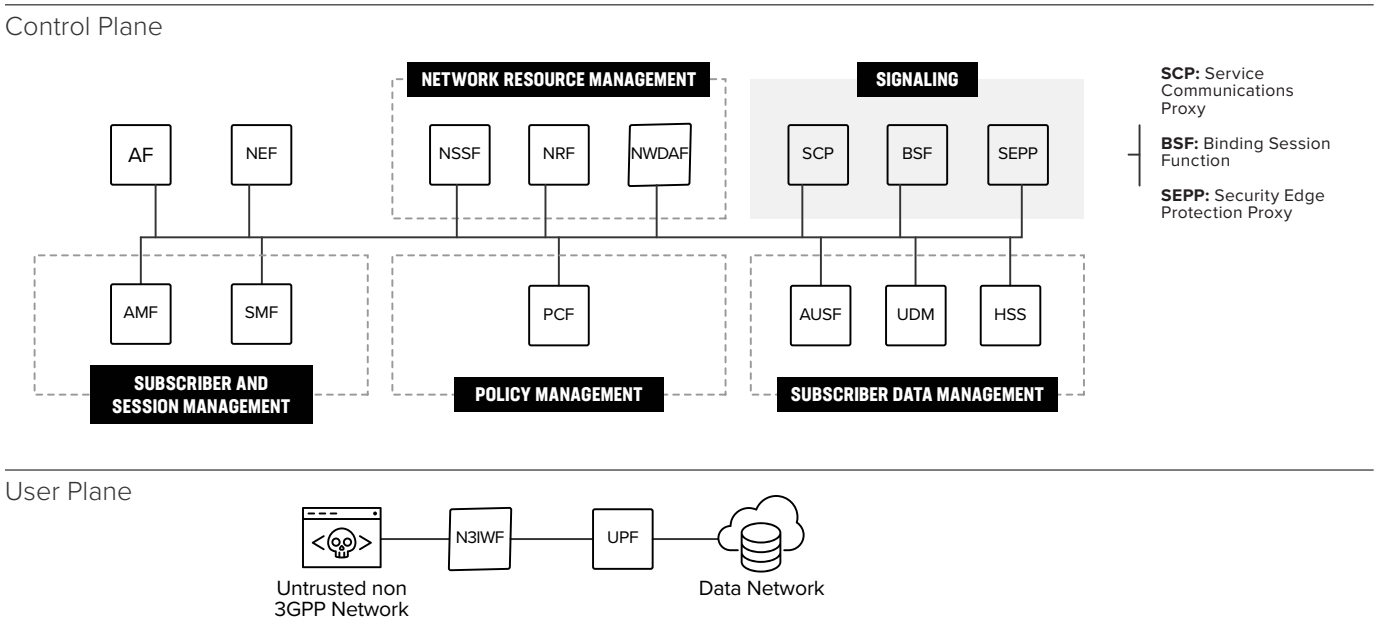


Figure 5: 5G Core signaling functions optimizing 5G signaling traffic.

F5's Service Communication Proxy (SCP) supports the following use cases:

- Simplified 5G cloud-native SBA network mesh connectivity
- Flexible user-based routing selection
- Real time congestion control, load balancing, and overload protection
- End-to-end user experience visibility for multi-vendor environment
- 4G/5G protocol interworking
- Communication security

F5'S SIGNALING SOLUTIONS INCLUDE SERVICE COMMUNICATION PROXY, BINDING SESSION FUNCTION, AND SECURITY EDGE PROTECTION PROXY

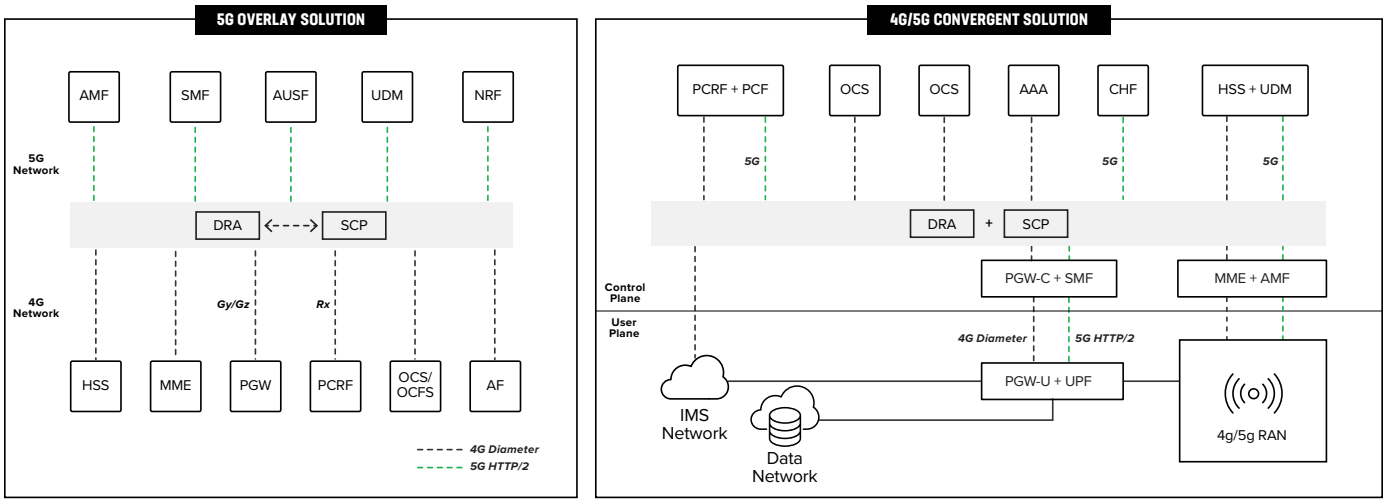


Figure 6: 4G/5G protocol interworking

F5's Binding Session Function (BSF) network function will support:

- Session binding to support scalable policy solution
- Session binding capabilities to support the interworking with IMS (VoLTE) services delivered over NR

F5's Security Edge Protection Proxy (SEPP) will support the following:

- Roaming security: SEPP sits on the edge of the network, protecting the network from threats originating from roaming partners and IPX providers. SEPP includes message filtering and policing on inter-PLMN control plane interfaces, as well as topology hiding.

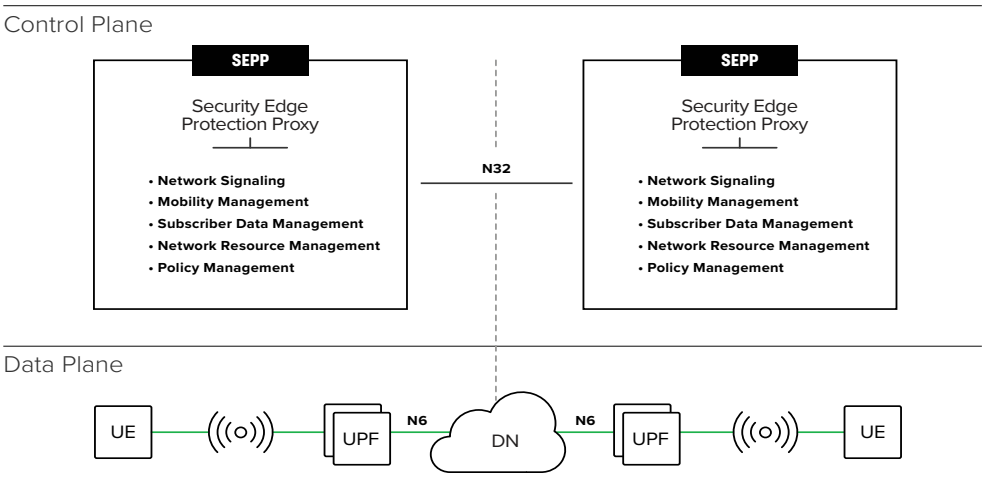


Figure 7: Security Edge Protection Proxy (SEPP)

TRANSITIONING YOUR BEST OF SUITE S/GI-LAN TO N6 SERVICE-BASED INTERFACE

F5'S 5G SIGNALING NETWORK SOLUTIONS WORK IN TANDEM TO ADDRESS 5G NETWORK SIGNALING CHALLENGES

Why this is an issue

Scaling is a number one concern for service providers especially with the explosive demand that 5G is generating. The containerized N6 LAN interface can result in device sprawling as architectures increase in complexity because a multi-vendor environment consists of a best-of-breed rather than best-of-suite. Adopting the best-of-breed approach can dilute the cost benefit associated with virtualizing your network and add additional complexity due to vendor interoperability. The results can increase CapEx and OpEx, introduce additional points of failure into the network, and make it difficult to scale your network. As a result, the delivery of new services to subscribers can involve major delays, leading to loss of new revenue streams and lowered subscriber QoE.

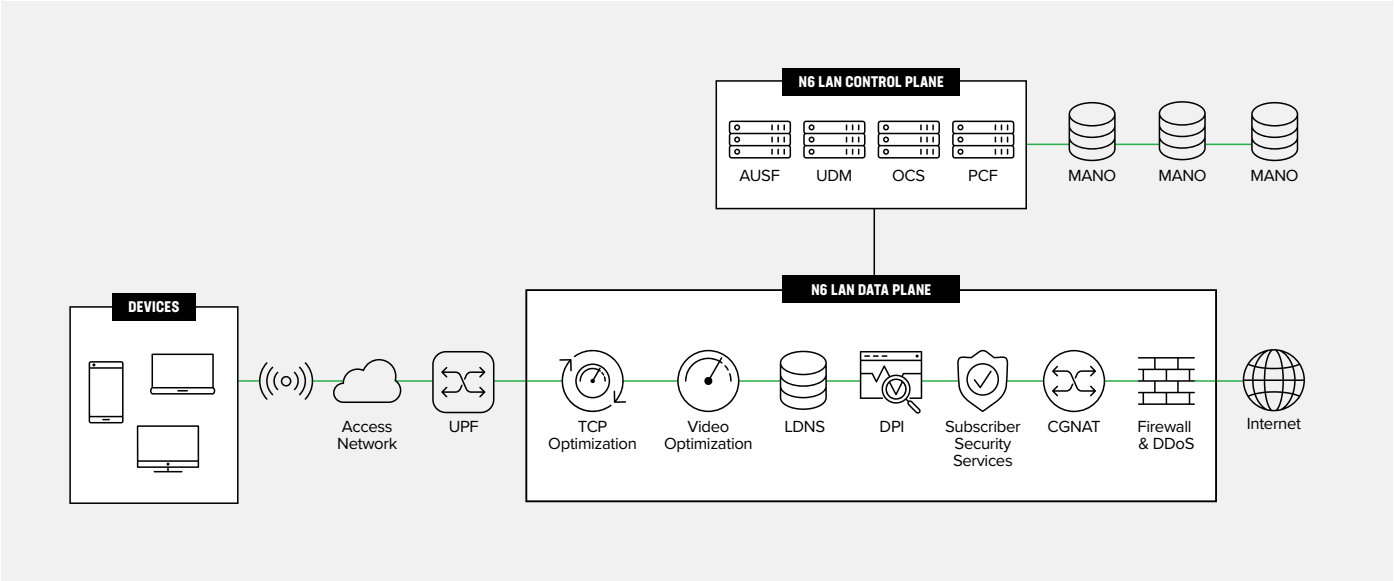


Figure 8: What is N6 LAN? (Before F5)

What you should do

With 5G comes a rapid growth in apps, data and video streaming which will continue to put strain on the mobile network. The S/Gi interface in 3G and 4G is transformed into a Service Based Interface (SBI) with the introduction of the 5G Core. The N6 LAN supports services including network address translation (NAT), firewall, policy management, traffic steering, and URL filtering, as well as TCP and video optimization. You can intelligently steer traffic, including video traffic, to optimization platforms or apply policy management actions based on subscriber and application awareness.

How F5 Helps

A containerized N6 LAN solution from F5 helps you build a cost-effective model, allowing for faster time to market for new services and less network complexity. F5 containerized network functions (CNFs) are a core component within an efficient virtual N6 LAN, providing solutions such as virtual policy enforcement, virtual firewall, and virtual Application Delivery Controller (ADC) services.

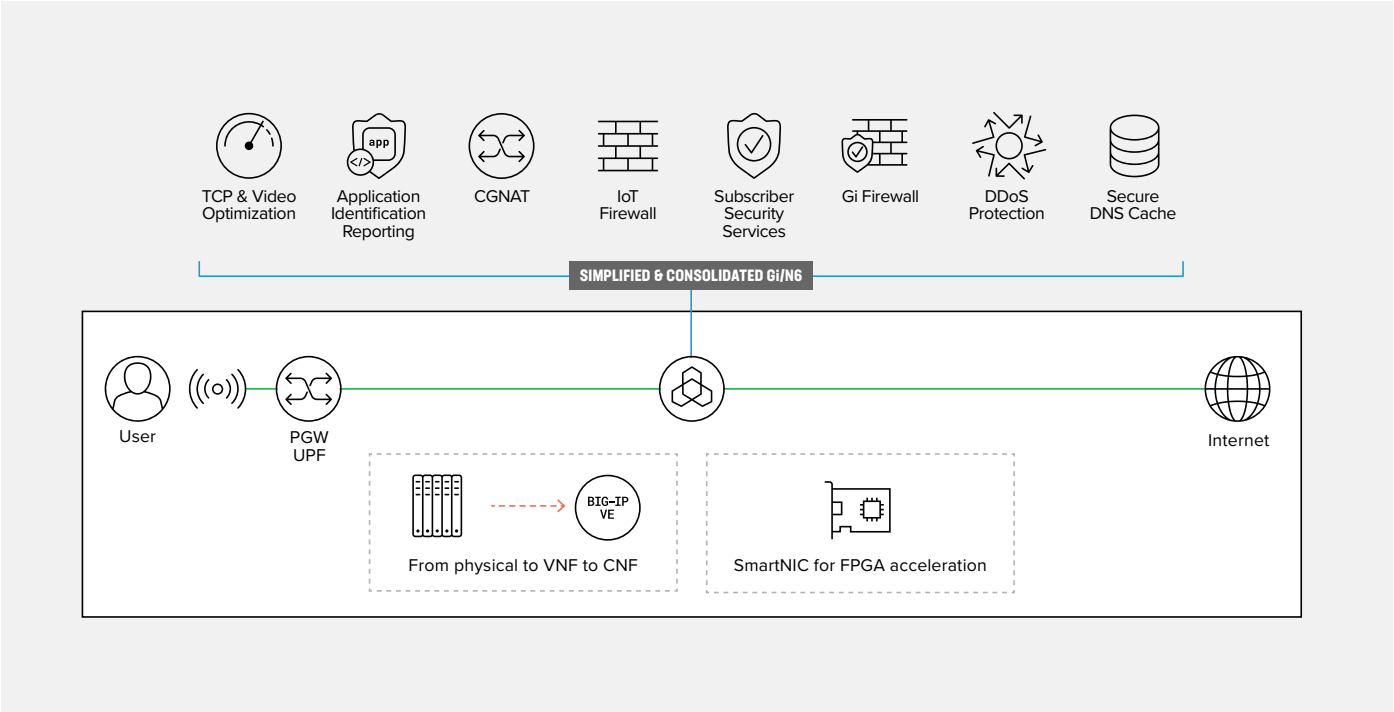
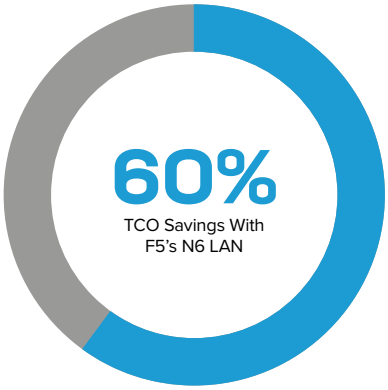


Figure 9: F5's consolidated N6 LAN solution

F5's N6 LAN solution allows dynamic service chaining based on real-time subscriber and application awareness, along with delivering secure N6 LAN. By deploying a common, shared set of commercial, off-the-shelf (COTS) hardware to run various functions, a service provider can reduce hardware costs and deploy multiple services dynamically. This cloud model means you can deliver services based on real-time network conditions and use network resources more efficiently. Because you can launch new services without any network downtime, you also increase service agility. A containerized N6 LAN lets you innovate, improve subscriber QoE, and lower costs resulting in a 60% TCO.

CONSOLIDATION OF SERVICES RESULTED IN A 60% SAVINGS ON TOTAL COST OF OPERATION.



SAVINGS FROM CONSOLIDATING CONTAINERIZED SERVICES

- Lower CPU usage
- Fewer CPU hops, minimizing latency
- "Zero Copy" memory architecture optimizes resource consumption
- Network simplification, easier orchestration and management
- Simplified troubleshooting
- Easier to implement new services, software upgrades

Figure 10: TCO savings with F5's N6 LAN

IMPLEMENTING CONTAINERIZED 5G CLOUD-NATIVE

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. Kubernetes was not specifically designed for carrier grade deployments or the need for service providers to keep complexity and cost to a minimum. This drives the prioritization of 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 implement security at container ingress is critical to 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.

F5'S 5G SOLUTIONS PROVIDE THE VISIBILITY, CONTROL, AND SECURITY SERVICE PROVIDERS NEED FOR A SUCCESSFUL 5G TRANSITION.

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). LTE 4G 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, is 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. Why are containers so critical in 5G? With the dynamic nature of containers, 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 within the network.

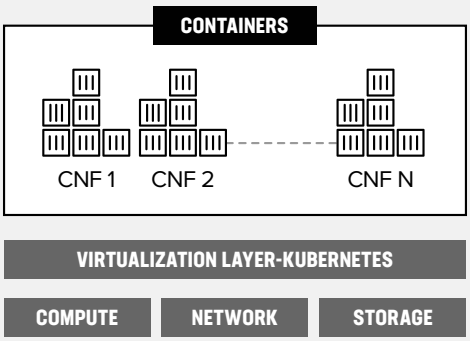


Figure 11: Cloud-native containerization

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.

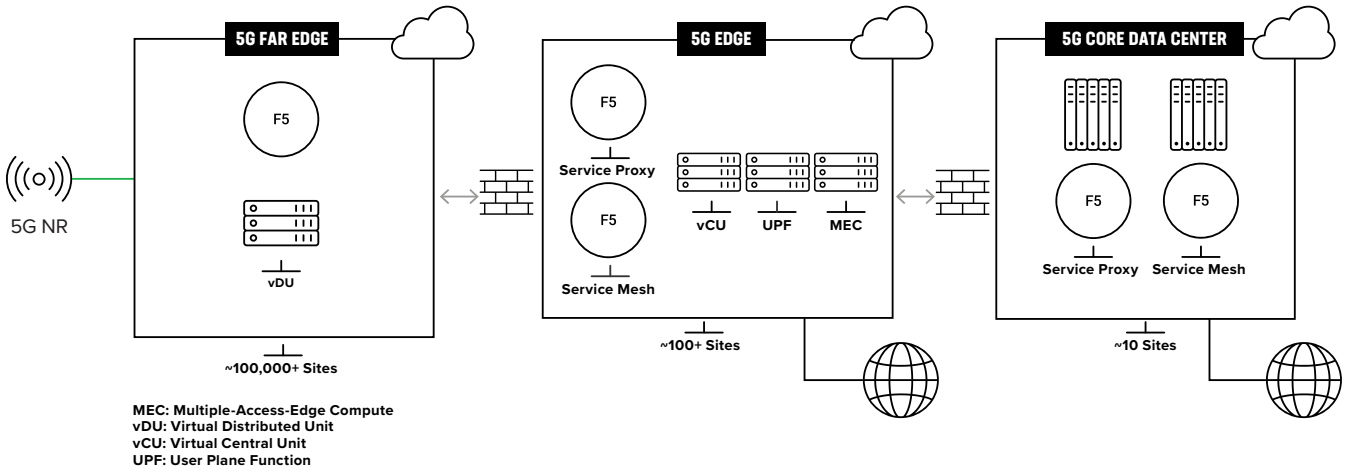


Figure 12: F5 infrastructure solution scaling capability

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

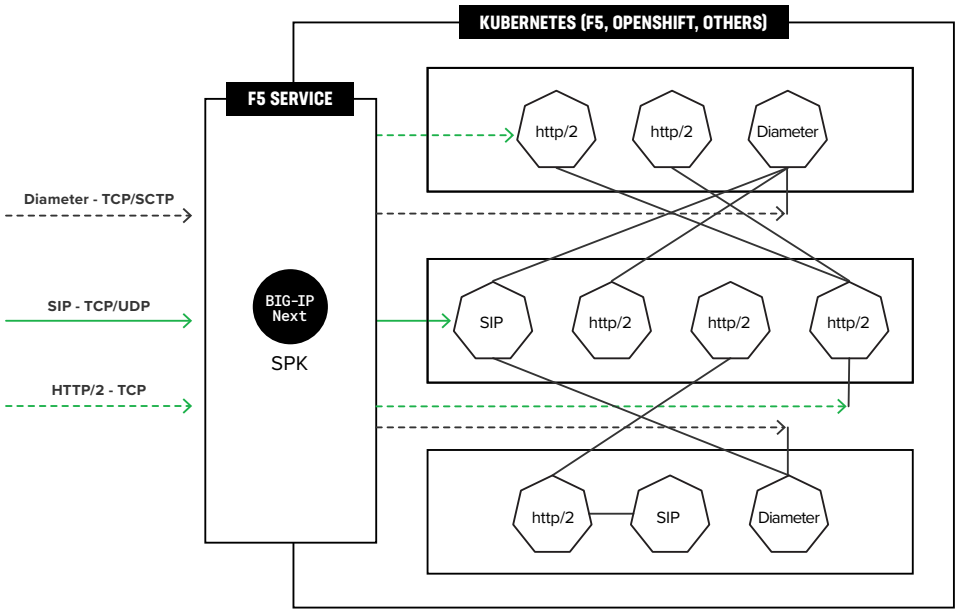


Figure 13: 5G ingress use cases

- **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.

OPTIMIZED TRAFFIC STEERING ENABLES A TCO REDUCTION OF 47%.

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.

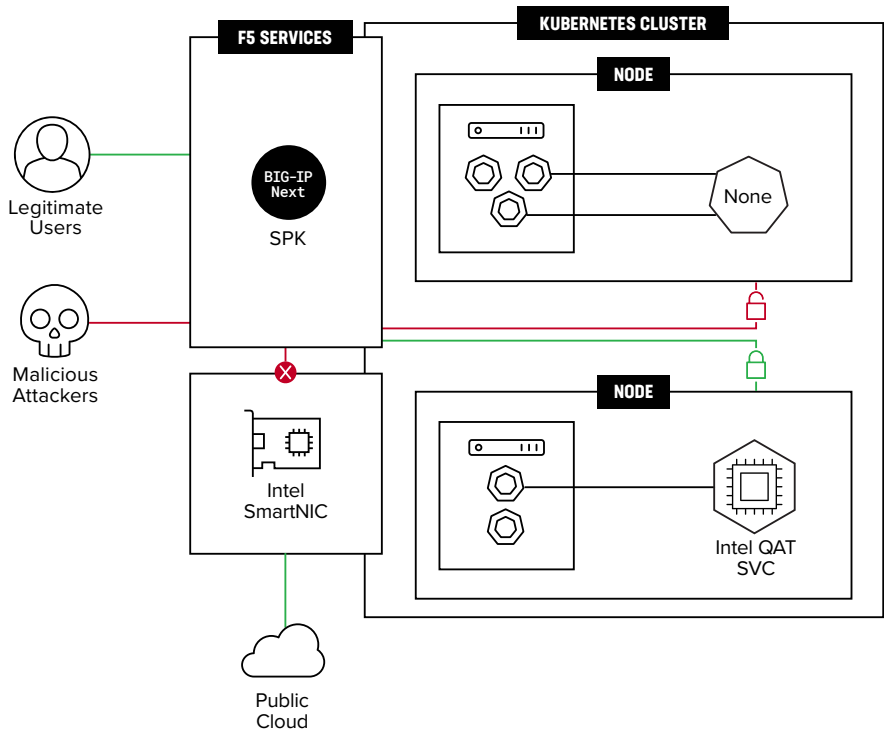


Figure 14: SmartNIC security benefits

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.

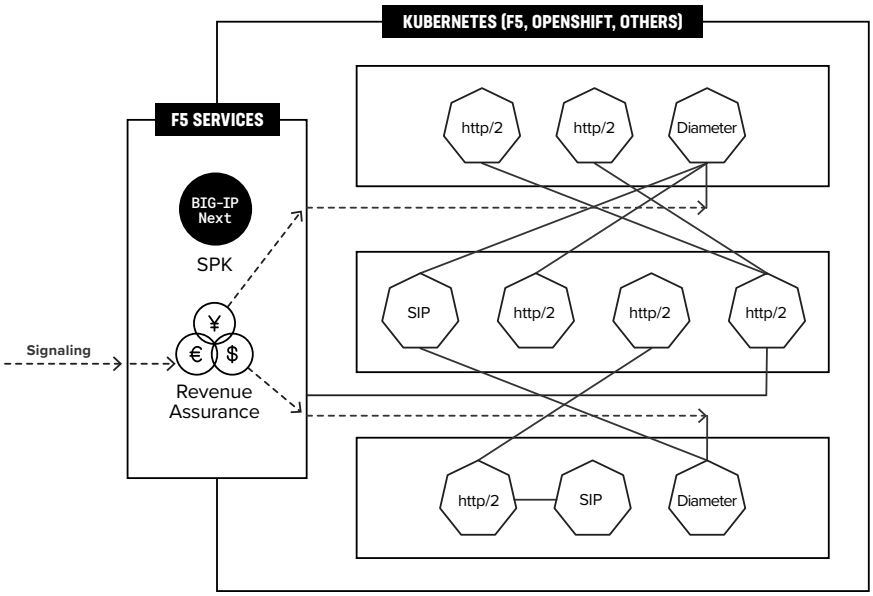


Figure 15: The entry point to the Kubernetes cluster is the ideal location to gather information for compliance and billing.

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

F5 IS COMMITTED UNDERSTANDING AND CONQUERING THE CHALLENGES OF 5G DEPLOYMENT.

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.

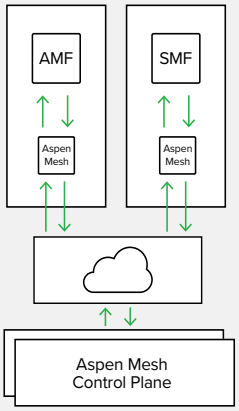


Figure 16: Aspen Mesh sidecar view

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.

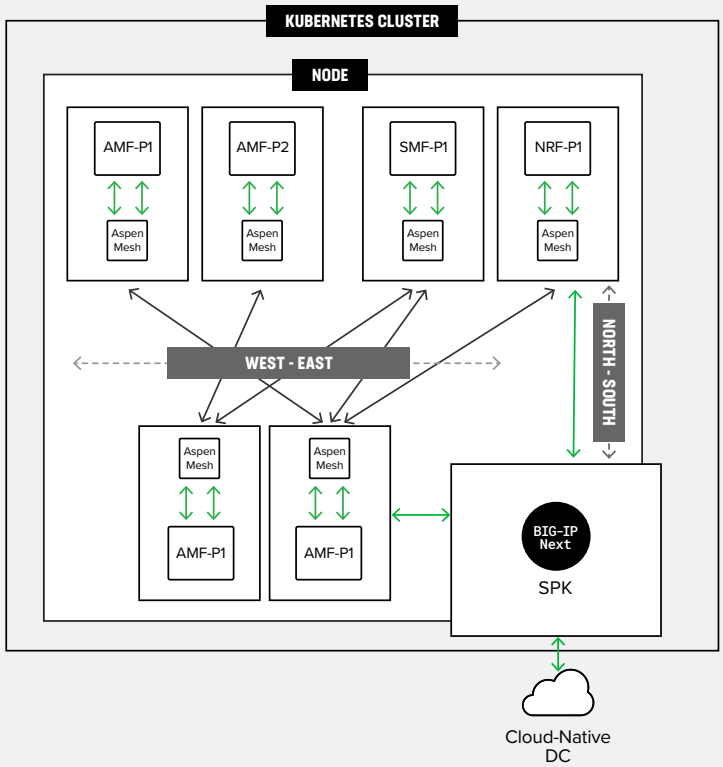


Figure 17: BIG-IP Next Service Proxy for Kubernetes and Aspen Mesh implementation

Conclusion

As 5G keeps on gaining momentum, service providers need to adopt measures to protect their exisiting 4G networks as they monetize new 5G investments. Proper migration and interworking plans need to be executed as multi-cloud, hybrid networks emerge. Migrating to 5G requires critical steps to be taken and F5 offers proven solutions that drive a migration path while maintaining existing 4G network which include:

- Signaling interworking in the migration from 4G to 5G
- Transitioning to best of suite S/Gi-LAN/N6 service-based interface
- Implementing cloud-native 5G infrastructure

The transition journey is unique for every service provider and F5 is committed to understanding and conquering challenges that may arise during the deployment of innovative 5G networks.

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