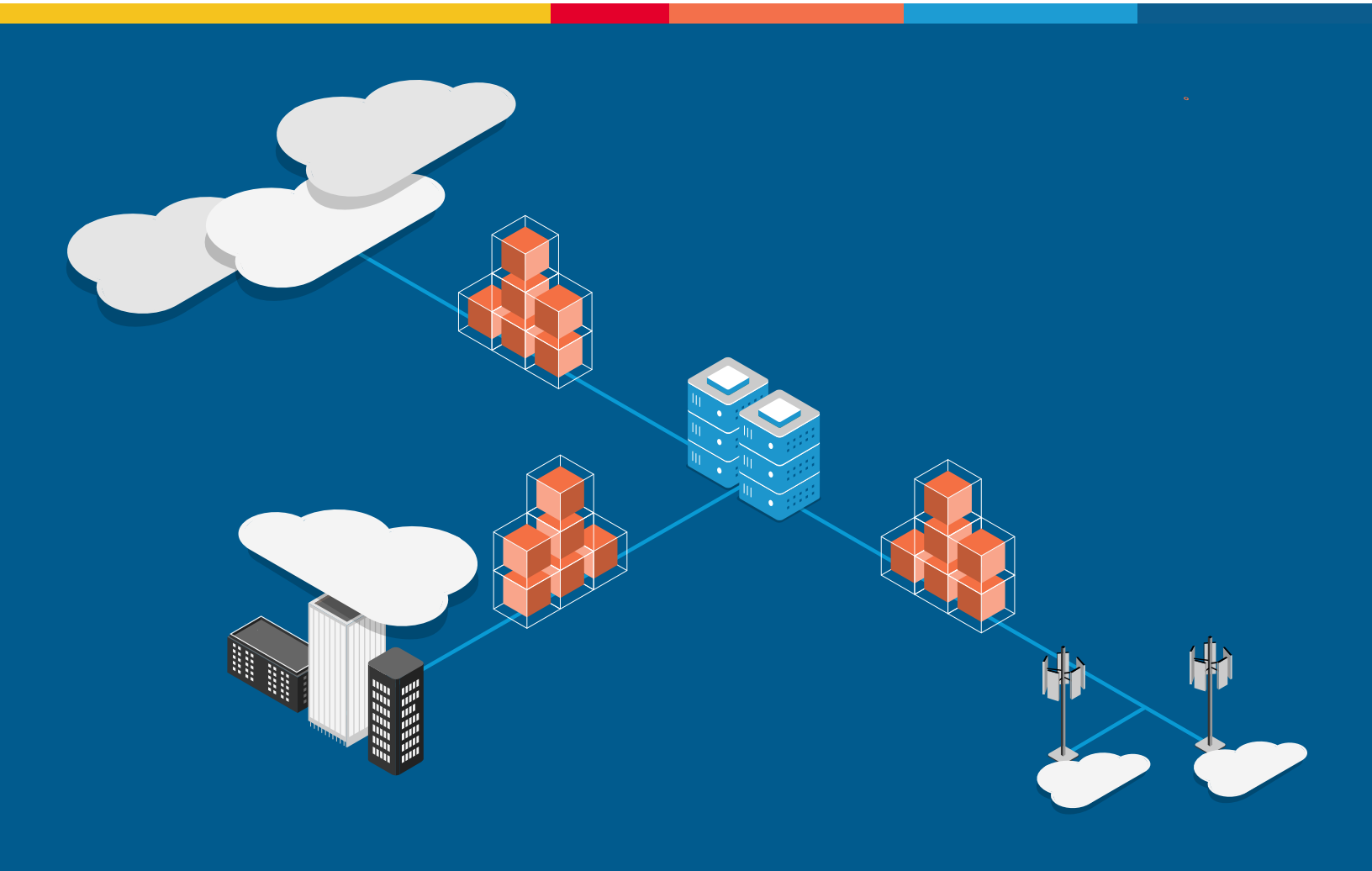
SOLUTION OVERVIEW

# F5 BIG-IP Cloud-Native Network Function Solutions for Service Providers

F5 BIG-IP Cloud-Native Network Function (CNF) solutions leverage cloud-native benefits to reduce cost of ownership. This solution includes Edge Firewall, DNS, CGNAT, and Policy Enforcer CNFs.



KEY BENEFITS

**Minimize operating costs**
Reduce CapEx and OpEx by increasing automation and consolidating data plane functions.

**Improve performance of applications**
Better enable applications by automatically allocating resources where they're needed and when they're needed.

**Protect your network**
Carrier-grade security designed for service providers.

**The telecommunications industry is at an inflection point**, and what we do now will set the stage for the next 10 years. Service providers are building out their 5G networks, which call for a service-based architecture. Cloud-native architectures offer critical benefits, and cloud-native network functions (CNFs) are becoming the main delivery mechanism for the network services that comprise this architecture.

A network function enriches network traffic and typically applies some type of policy, such as carrier-grade network address translation (CGNAT), firewall, DNS caching, routing, and user plane functions (UPF). A CNF consists of microservices that decouple the virtual function control and data plane processes into smaller units, collected in containers. By building APIs between the microservices containers and integrating them into an orchestration system such as Kubernetes, CNFs provide many benefits that were not possible in previous architectures.

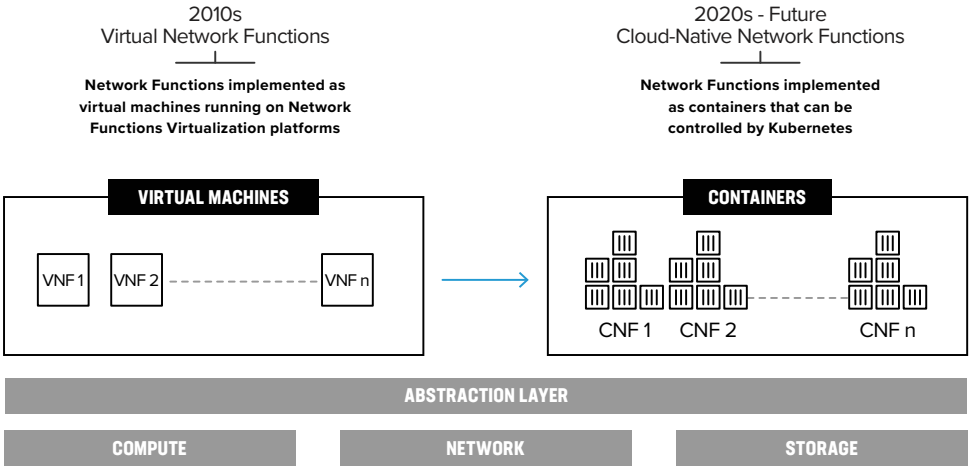



**Figure 1. Cloud-native represents the evolution of network functions delivery.**

### What does cloud-native mean?

A cloud-native application uses a collection of tools that manage and simplify the orchestration of services that make up the application. CNFs bring critical capabilities to the network. They're scalable, automated, resilient, manageable, and observable. Cloud-native applications support dynamic elasticity and scale, occupy a smaller footprint with fast restart, and use continuous deployment and automation principles. Rather than moving each service as a monolithic "heavy brick," microservices can be deployed around the network as "grains of sand" in a far more granular manner. CNFs are an integral component of 5G networks and can be deployed to improve efficiency and reduce costs in 4G networks.

MAINTAINING AND IMPROVING NETWORK SECURITY IS CRITICAL NOT ONLY BECAUSE OF THE INCREASING THREAT SURFACE, BUT ALSO THE LARGER, MORE COMPLEX ATTACKS THAT TARGET THE NETWORK.

**Service providers face unique challenges**

They have multiple pain points to address, and they're looking for solutions that can reduce network costs. CapEx and OpEx continue to rise, especially with the availability of "all you can eat," high-speed bandwidth. End users have always demanded more for less—and with the arrival of 5G, their expectations are even higher. And, of course, service providers are always looking for ways to protect their revenue from new public cloud competitors. Ultimately, service providers need solutions that can reduce network costs.

Service providers need scalable and automated functions. Virtual machines can be automated, but they're monolithic. And while a service provider can run a monolith in the cloud, it can't increase resources for a single part of the monolith. With microservices, the environment can be configured to automatically add and remove virtual server instances as system loads change.

Security is always of paramount importance. Maintaining and improving network security is critical not only because of the increasing threat surface, but also the larger, more complex attacks that target the network. Lack of fixed perimeters, increasing volumes of sensitive personal data, and accelerated app and code release cycles make security more challenging. That's why service providers are looking for more visibility into their network and the health of their revenue-generating services from the data that cloud-native systems can gather.

## F5 BIG-IP Cloud-Native Network Functions–Industry-Leading, Cloud-Native Solutions Designed for Service Providers

F5® BIG-IP® Cloud-Native Network Functions (CNFs) share many characteristics with our F5® BIG-IP® Virtual Edition (VE) and hardware platforms. We've re-architected our existing network functions for deployment in Kubernetes, which means the features and functionality that exist today will become microservices in the new CNF products. Unlike some competing products, these are truly cloud-native CNFs, with all the inherent advantages, including a smaller footprint, rather than a virtual machine in a container "wrapper."

Cloud-native solutions help service providers reduce their total network cost. This Kubernetes-based solution is designed primarily for service providers—it is optimized for highly demanding environments that require flexible resource allocation. BIG-IP CNFs are automatable, scalable, and extremely efficient, allowing them to outperform monolithic virtual machines. With microservices placed in containers, different functional areas of the application can scale at different rates, depending on what that particular application needs.

BIG-IP CNFs PROVIDE SERVICE PROVIDERS WITH A COMPREHENSIVE, CARRIER-GRADE SET OF CLOUD-NATIVE NETWORK FUNCTIONS THAT ALLOW SERVICE PROVIDERS TO PROTECT AND ENRICH THEIR ENTIRE NETWORK.

Microservices also shorten the development, testing, and upgrade cycles for new software. Operational savings come from greater automation. Capabilities such as auto-scale, which adds and removes CNF instances as the load on the system changes, and automated deployments, rather than error-prone manual deployment, significantly increase overall efficiency. Automated deployment pipelines, automated new software rollout, automated management, and automated failover all simplify processes and reduce costs.

BIG-IP CNFs provide service providers with a comprehensive, carrier-grade set of cloud-native network functions that allow service providers to protect and enrich their entire network. Native IPv6 and telco protocol support can integrate with some of the world's most demanding environments and traffic mixes.

BIG-IP CNFs are built on the F5 cloud-native engine, which is a visibility, support, and licensing control infrastructure. A wide range of CNFs will be rolled out over time, beginning with CGNAT, Edge Firewall, DNS, and Policy Enforcer CNFs. The CGNAT CNF uses address translation technology to ease IPv6 migration and improve network scalability with IPv4 address management. The Edge Firewall CNF brings over the firewall, DDoS, and IPS technology from the existing F5 BIG-IP Advanced Firewall Manager (AFM). Its unique, application-centric design effectively guards against targeted, network infrastructure-level attacks.

A DNS CNF will support DNS caching and can reduce DNS latency by up to 80%. The Policy Enforcer CNF supports several advanced policy and traffic management use cases from the F5® BIG-IP® Policy Enforcement Manager™ (PEM). Combining policy enforcer tools—such as traffic classification, TCP optimization, and subscriber awareness—supports strategies to help deliver increased performance, improved subscriber quality of experience , improved average revenue per user, and lowered total cost of ownership.

### A consolidated data plane reduces CapEx and OpEx

F5 is reducing the software footprint and enabling horizontal scaling that can be natively controlled by Kubernetes, as well as making that horizontal scaling more robust. The CNF control plane is fundamentally different from a VNF implementation, as all configuration is performed by interacting with the native Kubernetes API. There is no F5 command line, GUI interface, or F5 API. The native Kubernetes API is extended with custom resource definitions to ensure F5 products can be properly configured.

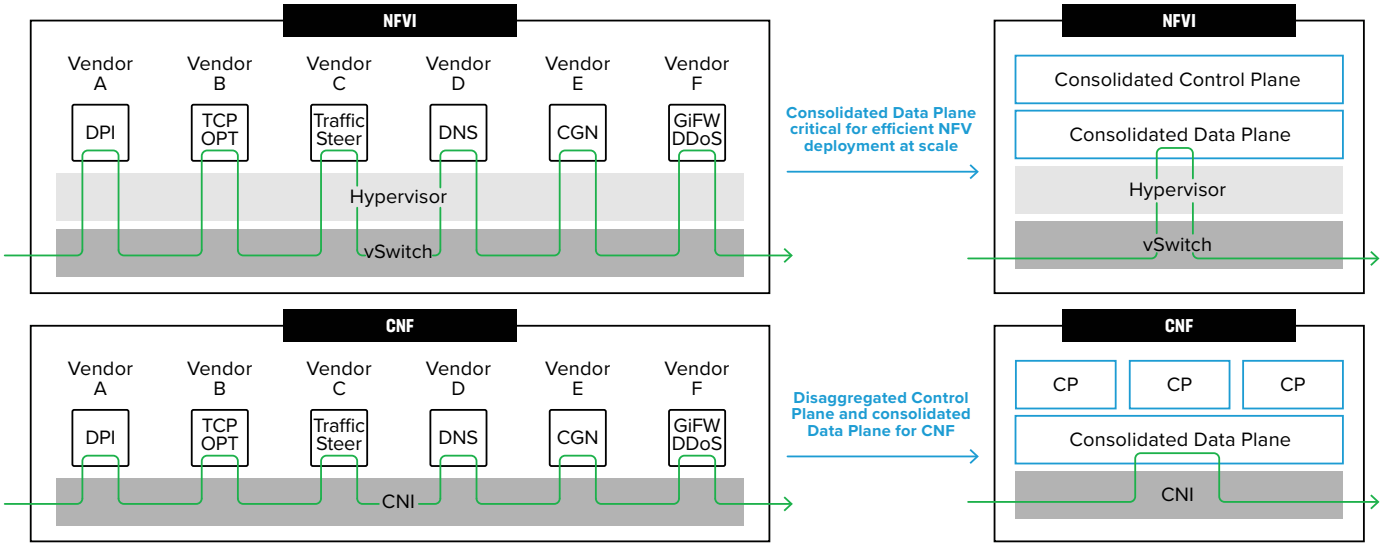



**Figure 2. Control plane and data plane for F5 VNF and CNF.**

The data plane is consolidated for multiple functions and features a zero-copy memory architecture resulting in a significant CPU reduction compared to other SGi-LAN / N6 LAN solution vendors. Traffic traverses the hypervisor just once, creating a "single-hop" architecture that reduces the number of virtual machines required and reduces CPU usage. For CNF deployments, the control plane is disaggregated, so it can scale independently of the data plane in a highly granular manner.

### Hardware acceleration for improved performance

In Kubernetes, and with virtualization in general, performance is always a concern. As the industry adopts CNFs to build systems with containers and pods in Kubernetes, performance concerns do not disappear entirely. F5 provides amplified performance by offloading selected functionality to hardware. This gives service providers the best of both worlds—cloud-native characteristics with the higher performance characteristics of an F5 hardware appliance. Some workloads are still CPU bound, so they can be boosted with field-programmable gate array (FPGA) offload capabilities, such as for L4 services or SSL and compression. And BIG-IP CNFs integrate with SmartNICs with Intel® FPGAs—including the BIG-IP VE for SmartNICs, letting our customers enjoy high-performance solutions that work in Kubernetes.

## Use Cases

An example use case for the BIG-IP CNFs is SGi-LAN / N6 LAN consolidation for mobile service providers. Migrating to 5G drives the need for a high-bandwidth, service-rich, and secure N6 LAN. In a cloud-native architecture, F5 supports the same wide function set that BIG-IP VE and hardware support, so providers can seamlessly migrate to a cloud-native architecture when it makes sense for them to do so.

KEY FEATURES

- Orchestrated by Kubernetes API
- Data plane offload to specialized hardware integrations
- IPv6 and telco protocol support

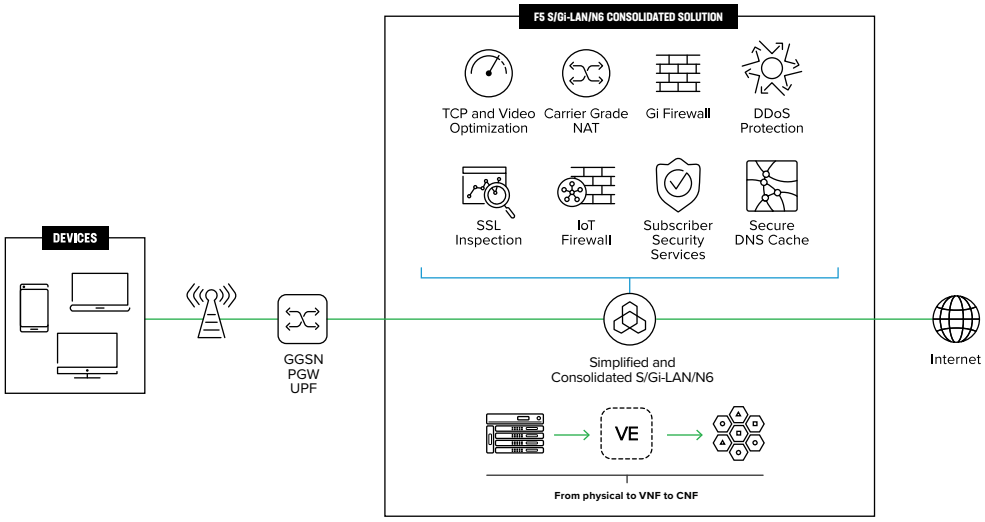



**Figure 3:** Consolidated S/Gi-LAN/N6 architecture for 5G and 4G packet core networks.

CNF solutions are the perfect form factor for those looking to move workloads to a cloud-native architecture. Primarily for mobile service providers implementing 5G, these solutions also support use cases for fixed-line and cable service providers who are deploying data centers and adopting multi-access edge compute solutions. Additionally, large technology companies and enterprises looking to securely deploy revenue-generating apps in a microservices architecture on Kubernetes will benefit from BIG-IP CNFs.

## Conclusion

Service providers, large technology companies, and large enterprises are looking to automate their operations and adopt modern architectures so they can scale their networks, all while reducing costs. BIG-IP CNF solutions leverage cloud-native benefits to deliver reduced cost of ownership from consolidation, code efficiency, and automation—providing a full portfolio of network functions.

**Find out how F5 products and solutions can help you achieve your goals.**

**To learn more, contact your F5 representative.**