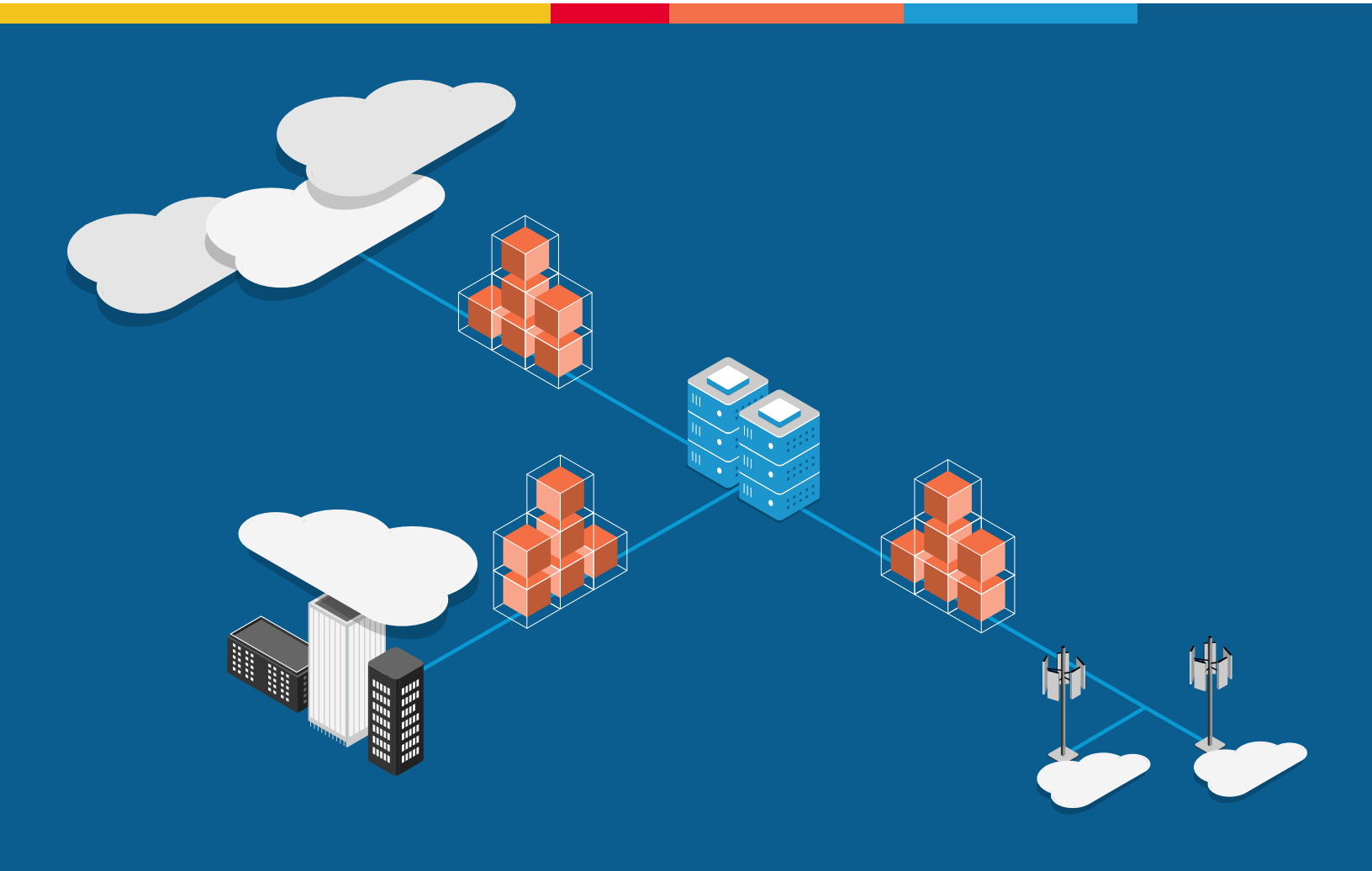
SOLUTION OVERVIEW

F5 BIG-IP Next Cloud-Native Network Function Solutions

F5 BIG-IP Next 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

Automated
Incorporates manual and repetitive tasks.

Agile
Able to identify and respond quickly to the need for change.

Scalable
Highly dynamic and allows applications to scale automatically.

Resilient
Quick to resolve issues and return to normal operation.

The digital transformation has been underway for years. Users now expect to connect from anywhere—for business or pleasure—and have a low latency, reliable, seamless, and secure experience while doing so system loads change.

Companies have embedded technologies across their businesses to drive fundamental change to increase revenues, drive greater business agility and efficiency, and unlock new value for employees, customers, and shareholders. Now cloud-native architectures allow enterprises to further transform the way that they develop and operate those technologies, and how they deliver applications both within their organization and to their customers. A cloud-native architecture brings the ability to continually deploy and update applications, enhancing the user experience while not disrupting it, and enabling revenue generation and cost reduction.

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

Service providers face unique challenges

Service providers 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.

Automated and highly scalable functions will help solve some of the challenges. 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 cloud-native 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 having greater visibility into the network and the health of revenue-generating services, thanks to the data that cloud-native systems can gather, is more important than ever.

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.

The benefits of a cloud-native network

A network function enriches network traffic and typically applies some type of policy. A cloud-native application uses a collection of tools that manage and simplify the orchestration of services that make up that application. A cloud-native network function 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.

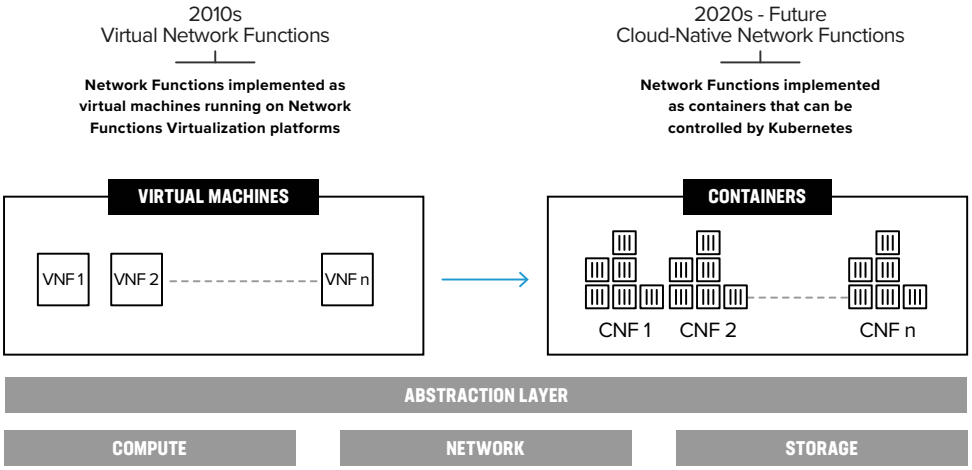


Figure 1: Cloud-native represents the evolution of network functions delivery.

CNFs bring critical capabilities to the network. They are scalable, automated, resilient, manageable, and observable. Cloud-native applications support dynamic elasticity and scale and occupy a smaller footprint with fast restart. 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.

Cloud-native solutions are built on continuous integration/continuous delivery (CI/CD) principles—a software delivery process that automates builds, testing, and deployment, allowing software to move from development systems to live production systems quickly and reliably. With a high-quality CI/CD system, cloud-native applications can be deployed daily, hourly, or even faster. As an automated and faster methodology, improved applications are in production quicker with less resources, resulting in significant OpEx savings.

BIG-IP NEXT 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.

F5 BIG-IP Next Cloud-Native Network Functions–Industry-Leading, Cloud-Native Solutions

F5® BIG-IP® Next 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 reduce total network cost. This Kubernetes-based solution is optimized for highly demanding environments that require flexible resource allocation. BIG-IP Next 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.

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

BIG-IP Next CGNAT, Edge Firewall, DNS, and Policy Enforcer CNF

BIG-IP Next CNFs are built on a common cloud-native architecture, the F5 cloud-native engine, which provides 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 BIG-IP Next CGNAT CNF uses address translation technology to ease IPv6 migration and improve network scalability with IPv4 address management.

The BIG-IP Next Edge Firewall CNF employs the firewall, DDoS, and IPS technology from the industry-leading F5® BIG-IP® Advanced Firewall Manager (AFM) and is certified by the Cloud Native Computing Foundation (CNCF). Its unique, application-centric design provides a full-proxy network security solution that effectively guards against targeted network infrastructure-level attacks. Using DoS profiles, BIG-IP Next Edge Firewall CNF performs a variety of checks and mitigates a multitude of attacks and key DDoS vectors.

The BIG-IP Next DNS CNF enables DNS caching functionality. DNS latency can be reduced by enabling a DNS cache on F5® BIG-IP® DNS and having it respond immediately to client

requests. This consolidates the cache and increases the cache hit rate, reducing DNS latency up to 80 percent. In addition to caching, BIG-IP Next DNS CNF allows the device to do its own DNS resolving without requiring the use of an upstream DNS resolver.

The BIG-IP Next 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 like traffic classification, TCP optimization, and subscriber awareness supports strategies for enhancing performance, subscriber quality of experience, average revenue per user, and reduced total cost of ownership.

BIG-IP Next CNFs include iRules support. The F5 iRules® scripting language—F5's traffic scripting interface—enables programmatic analysis, manipulation, and detection of all aspects of the traffic in your networks. F5 customers routinely implement security mitigation rules, support new protocols, and fix application-related errors in real time. With robust and flexible iRules, customers can easily and rapidly develop solutions that can confidently be deployed across multiple applications.

A consolidated data plane reduces CapEx and OpEx

BIG-IP Next CNFs enable horizontal scaling 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.

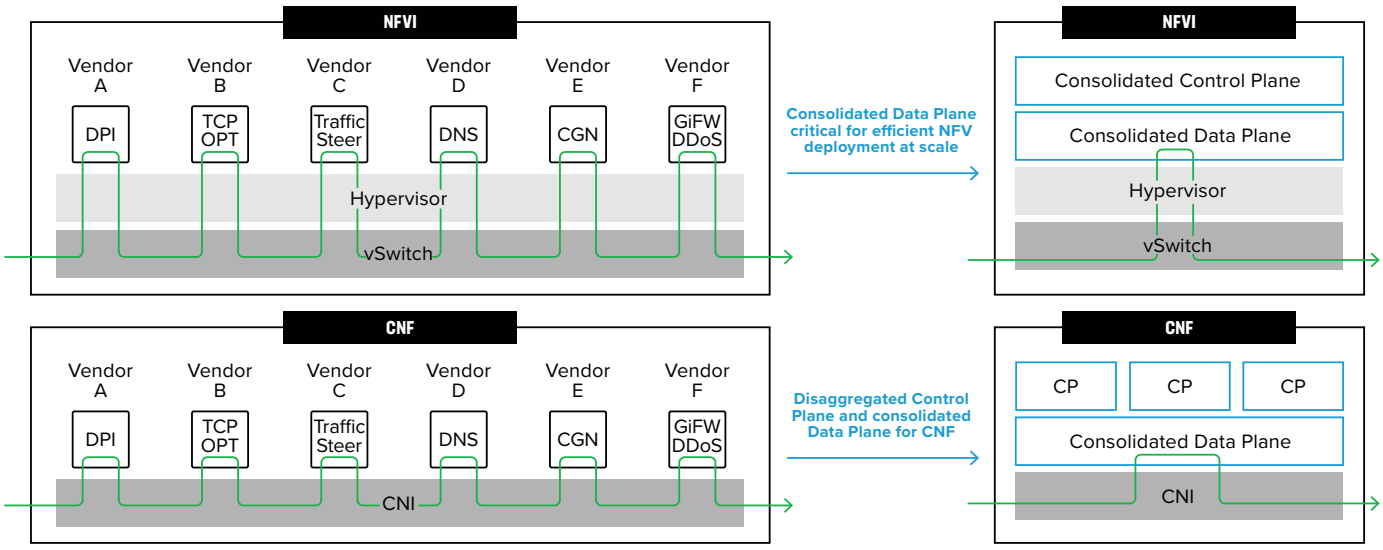


Figure 2: Control plane and data plane for F5 VNF and CNF.

KEY FEATURES

- Consolidated data plane and zero-copy memory architecture for cost savings in the N6 / S/Gi-LAN
- Hardware acceleration for improved performance
- A full-proxy network security solution certified by the Cloud Native Computing Foundation (CNCF)
- Orchestrated by Kubernetes API

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

As the industry adopts CNFs to build systems with containers and pods in Kubernetes, performance concerns do not disappear. 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 Next CNFs integrate with SmartNICs with Intel® FPGAs—letting our customers enjoy high-performance solutions that work in Kubernetes.

Deployments

From retail to financial services to manufacturing, enterprises are looking toward new cloud-native architectures. The Cloud Foundry Foundation provides an example with Home Depot, which leveraged cloud-native architectures and continuous delivery practices to develop more than 2,000 applications, handling over 2 billion service calls a month. This transformation reduced deployment times from six weeks to six hours.[1] The Cloud-Native Computing Foundation (CNCF) also showcases notable cases, such as PNC Bank, which replaced a process of 37 days or more with an automated and instantaneous process, enhancing code deployment security and audit compliance. Additionally, Booking.com in the Netherlands built 500 new services on the platform within the first 8 months, while Spotify realized a threefold improvement in CPU utilization.[2]

For mobile service providers, BIG-IP Next CNFs can be deployed for SGi-LAN / N6 LAN consolidation. 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.

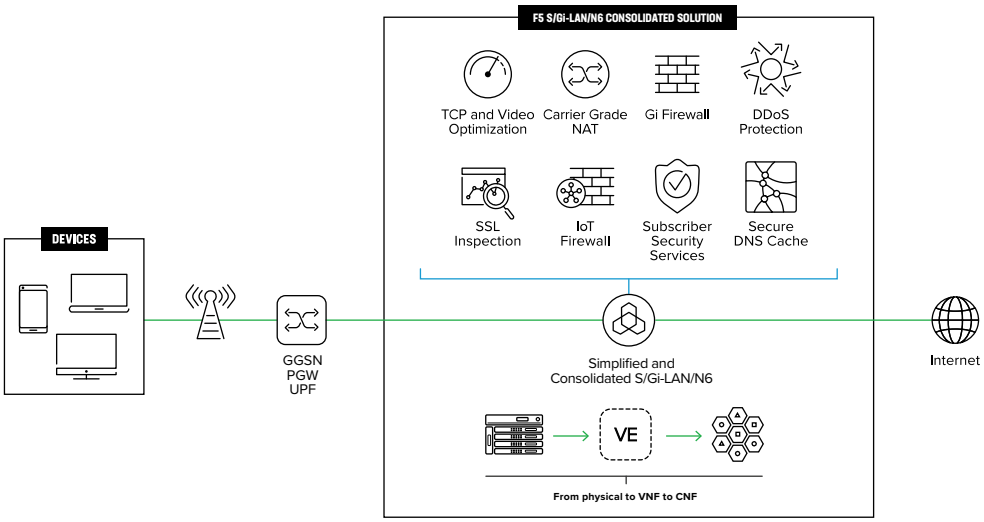


Figure 3: Consolidated S/Gi-LAN / N6 architecture for 5G and 4G packet core networks.

Summary

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

Find out how F5 products and solutions can help you achieve your goals. To learn more, contact your F5 representative, or send us an inquiry at F5 Sales.

[1] TechBeacon, "Cloud-native architectures are reshaping the enterprise," April 2018, , found at https://techbeacon.com/app-dev-testing/cloud-native-architectures-are-reshaping-enterprise

[2] Cloud Native Computing Foundation, Case Studies, found at https://www.cncf.io/case-studies/