BIG-IP Service Proxy for Kubernetes (BIG-IP SPK)

Provided by F5 Networks

BIG-IP SPK gives multi-protocol ingress/egress signaling control, security, and visibility for cloud-native 5G, supporting the transition from 4G.

Vendor validated.

Overview | Features & benefits | Documentation | Deploy & use | Get support

Overview

Kubernetes is not designed specifically for service providers and lacks the ability to natively support some network protocols. F5's solution, BIG-IP SPK, brings critical carrier-grade capabilities to a Kubernetes environment. It enables service providers to create a bridge from their existing 4G networks to a cloud-native 5G core network. BIG-IP SPK provides 4G signaling traffic management, visibility, and security at container ingress (North/South) into the 5G core Kubernetes clusters. Running on Red Hat OpenShift, it can also proxy service provider-specific protocols, such as 5G HTTP/2-REST, Diameter, SIP, GTP, and SCTP.

Certification standards

- Runs on OpenShift
- Vendor validated
- Fully containerized
- Collaborative support

Category

Networking

Terms of use

License agreement
Privacy policy

Features & benefits

5G cloud-native infrastructure

Service providers can create an SBA using a microservices-based, cloud-native solution. A cloudnative solution is an evolution of a virtualized, VM-based network. A cloud-native solution provides much more granular provisioning of capacity. This is critical for 5G because it allows providers to provision to average rather than peak capacity for optimal efficiency. Cloud-native network functions (CNFs) have the speed and flexibility to enable this solution, and, as a cloud-native solution, will mitigate vendor lock-in by the big mobile network equipment providers and allow the selection of vendors based on best-of-breed functionality and price.

Visibility and control for MEC deployments

F5 offers a robust toolset of solutions to power your MEC platform, regardless of how you're choosing to augment or build it. Not only can you accelerate your rollout of 5G by bridging from your 4G core to 5G, you can reduce CapEx and OpEx up to 60% with our consolidated S/Gi-LAN on your path to massive scale. Our hardware and virtual solutions provide a wide range of distributed, virtualized network functions and applications, plus automated, zero-touch, and app-centric service delivery.

Multi-protocol 4G and 5G signaling

Service providers must ensure that their new 5G infrastructure is interoperable with existing 4G networks. This will require the implementation of a secure, cloud-native, and service-based architecture from core to edge that can operate at scale.

Critical cloud security

Service providers require robust security for ingress traffic—that is, traffic coming into clusters—to establish the first line of defense against threats. The infrastructure must provide distributed denial-of-service (DDoS) attack protection, signaling firewalls, and web application firewalls at the ingress point to prevent malicious traffic from entering the cluster and impacting 5G core network functions and customer applications.

Documentation

DOCUMENTATION

Multi-Protocol Solution Enables Service Based Architecture with Red Hat

As today's carriers transition to 5G technology, F5 offers a unique solution– including ingress/egress signaling control, security, and visibility–for supporting containerized infrastructures. The multi-protocol F5 solution integrates 4G protocols and infrastructure with a Kubernetes 5G standalone core. This enables service providers who are transitioning to 5G to reduce risk by maintaining their existing 4G services, customers, and billing systems.

Read more →

ARTICLE

BIG-IP Service Proxy for Kubernetes (BIG-IP SPK)

BIG-IP SPK is unique in bringing critical network capabilities to a Kubernetes environment, meeting the demands of a service provider network. It supports ingress/egress control for 4G and 5G signaling, while adding needed security and visibility.

Read more →

DOCUMENTATION

F5 5G E-Book

As more service providers move toward 5G, they need a scalable, secure, cloud-native infrastructure that they, and their customers, can rely on. The standalone 5G Core eliminates the hardware-centric, centralized architectures of the past and embraces a cloud-native, distributed infrastructure for building and operating networks. The approach uses microservices, running on a service-based, containerized architecture that enables service delivery all the way to the far edge of the network. This creates the faster, more reliable network performance that customers demand.

Read more →

Deploy & use

Learn how to install and use this product on your Red Hat platform

> Quick start and configuration

Get support

SUPPORT: https://support.f5.com/csp/my-support/service-request

Details on online support and knowledgebase may be found here: https://support.f5.com/csp/home

https://Support.f5.com
1-888-882-7535 or 1-855-834-0367 Outside North America: +800 11 ASK 4 F5 (800 1127 5 435)