Start Small, Scale Huge: Understanding Cilium and eBPF in Today's Kubernetes

By Nesar Kavri

In the rapidly evolving landscape of cloud-native infrastructure, traditional networking and security models often struggle to keep pace with the dynamic nature of Kubernetes. Enter Cilium, an open-source project that has revolutionized how we think about container networking, security, and observability. At its core lies eBPF (Extended Berkeley Packet Filter), a powerful technology that allows us to run sandboxed programs in the Linux kernel without changing kernel source code or loading modules.

Why eBPF matters? Traditionally, networking and security policies were implemented using iptables, which can become a bottleneck at scale due to linear rule processing. eBPF changes the game by enabling efficient, programmable packet processing at the kernel level. This allows Cilium to provide high-performance networking (CNI), transparent load balancing, and deep visibility into API calls without the overhead of sidecar proxies.

Furthermore, observability is no longer an afterthought. With Hubble, built on top of Cilium, engineers gain deep insights into network flows, service dependencies, and security policy enforcement in real-time. By leveraging eBPF, Hubble provides this visibility with minimal performance impact, making it an essential tool for debugging complex microservices architectures.

As organizations scale their Kubernetes footprint, the need for a robust, scalable, and secure networking layer becomes critical. Cilium, powered by eBPF, offers a compelling solution that not only meets these demands but also simplifies the operational complexity of managing large-scale clusters. It's time to move beyond legacy limitations and embrace the future of cloud-native networking.