appgate

ZERO TRUST FOR KUBERNETES

Extend granular, dynamic secure access for cloud-native workloads

Background

Kubernetes, also known as K8s, is a driving force for DevOps and DevSecOps and cloud-native workloads. All major cloud platforms (Google, AWS and Azure) now offer a Kubernetes service. Built as an open-source platform, it provides the container orchestration engine for microservice-based software architectures. So, while it is safe to say that Kubernetes is driving digital transformation, the corollary is that security must evolve to support these new microservice architectures.

Zero Trust secure access enables the DevSecOps world with technology maturity, the power of scale and disruptive security aligned perfectly to modern software, continuous integration and continuous deployment (CI/CD) pipeline. Appgate SDP, an industry- leading Zero Trust Network Access solution, unifies user-to-service and service-to-service access for all traditional and cloud-native workloads into a single policy model that accelerates digital transformation and provides least privileged access.

The Problem

Kubernetes provides the speed, agility and application performance to help drive enterprise digital transformation but comes with a unique set of security challenges. Broader adoption means container sprawl and increased complexity in how containers are secured. A cloud-native skills shortage and not-fit-for-purpose legacy security tools leave security professionals overwhelmed.

Kubernetes security is an enormous and fluid subject, but at the top level, security professionals are concerned about:

- Maintaining consistent security across traditional and cloud-native workloads
- Increasing complexity created by using multiple security controls
- Lack of support for cloud-native environments from current security solutions
- Protecting a new attack surface and preventing attackers from using Kubernetes as part of a kill chain
- Streamlining DevSecOps to ensure that developers do not get ahead of security policies

The Solution

Enterprises and governments around the world recognize that adopting a Zero Trust security model represents the most efficient way to protect assets in an ever-more dangerous world. It is only logical to extend core Zero Trust principles ensure all resources are accessed securely, regardless of location; adopt a least privilege strategy and strictly enforce access control; and inspect and log all traffic into microservices architectures.

With a comprehensive ZTNA solution, you can use a unified policy model that manages secure access for all users (remote or on-premises), workloads (traditional or cloud-native) in any location (datacenters or in any cloud). Any user, any resource, any location.

BUSINESS BENEFITS OF KUBERNETES SECURED BY APPGATE

Zero Trust secure access for traditional and cloud-native workloads with a unified policy model

Streamline security into DevSecOps pipeline for faster agility and consistent security

Consistent security that adapts and scales with Kubernetes and CI/CD process

Provide secure egress access from containers at the pod level

Eliminate the need for bastion hosts or jump boxes

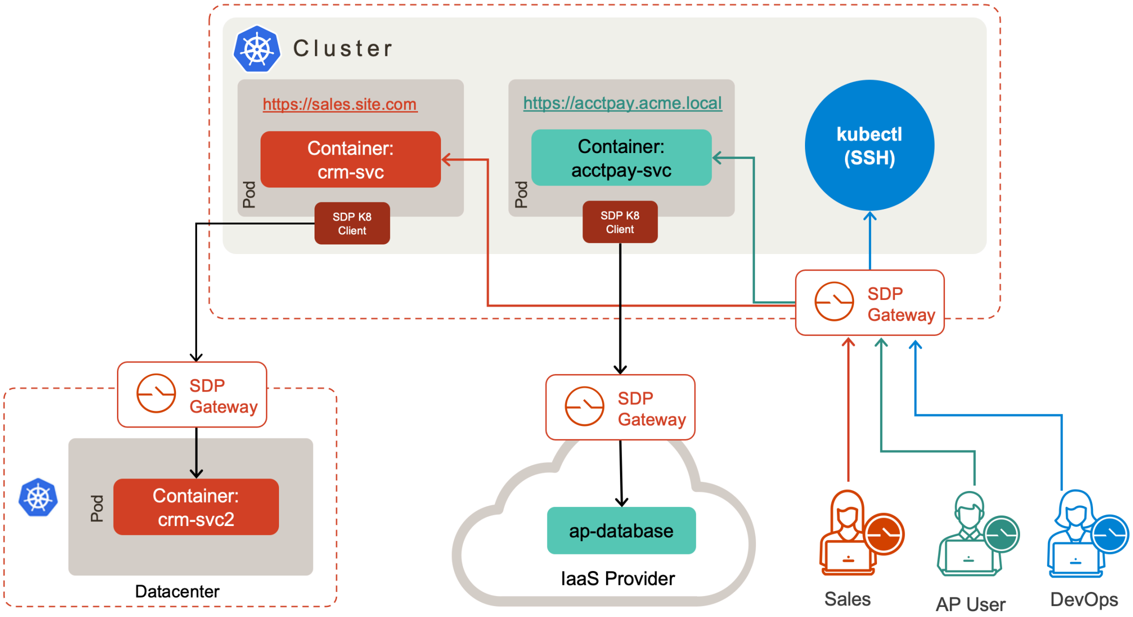
Use Cases

Appgate SDP has a proven track record in providing secure dynamic Zero Trust access to solve complex hybrid enterprise security problems and secure traditional cloud workloads. Appgate extends this model to protect microservices, enforcing granular, secure access to and from Kubernetes environments and building security into CI/CD pipelines.

Appgate SDP enables granular, dynamic secure access for Kubernetes in four areas:

1. **DevOps or admin access to Kubernetes resources like the UI or kubectl CLI:** Seamless granular access to Kubernetes environments and traditional resources for developers and admins
2. **Workforce access to web-based microservice applications:** Eliminate challenges for non-unified security solutions and enable dynamic URL filtering
3. **Pod-level egress access from containers to resources that live outside the cluster:** Securely connect to resources outside of the cluster, such as a database, log server or another microservice in a different cluster or location
4. **Temporary, on-demand access for private air gap Kubernetes deployments for patches, code updates and administration:** Enable a dynamic, just-in-time policy enforcement platform without the need for additional infrastructure like jump boxes

How it Works



This diagram shows three different use cases, all secured by unified policy model: The Blue user represents a developer implementing kubectl commands via SSH; the Green and Orange users need access to specific web-based microservices applications related to their departments; the sidecar client is used to secure egress access to resources outside of the cluster; in this example a database and another microservice.

Why Appgate

As developers continue to take advantage of cloud-native software, demand increases for scalable, container-based software developed with security in mind and protected when deployed with a robust ZTNA solution. Appgate SDP provides Zero Trust access for traditional workloads and cloud-native workloads regardless of location, for user-to-service, and service-to-service with a unified policy model, simplifying security across the enterprise. A Zero Trust access solution needs to solve not only for cloud-native workloads, but also secure traditional workloads in the cloud, on-premises, and in the datacenter.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.