RAFAY

SERVICE BRIEF

Rafay Network Policy Manager

Centrally Manage all Network Policies and Traffic for your Kubernetes Infrastructure

TECHNOLOGY BENEFITS

Centralized Network Policy and Enforcement
Enables a zero-trust security posture by authenticating network traffic for cluster-wide connectivity and namespace isolation

Standardized Installation Profiles
Provides fleet-wide automated deployment and consistent delivery of network security and configuration for inter-pod and container connectivity standards

Fleet-wide Network-Visibility
Network policy dashboards provide connectivity visualization at the network and namespace layer including historical replay for troubleshooting and service validation

BUSINESS BENEFITS

Strengthen Security
Cluster-wide hardening helps reduce lateral movement across your Kubernetes fleet infrastructure

Faster Service Delivery
Simplified automation of network-level policy definition and enforcement accelerates service delivery fleet-wide, including policy updates and full life cycle cluster management

Reduce Service Outages
Consistent network policy and enforcement reduces cluster misconfigurations and non-policy changes making applications more reliable in production environments

Network Policy Manager, one of several services available on Rafay's Kubernetes Operations Platform, provides centralized traffic management and visibility into your pod and namespace communication. This ensures isolation boundaries, enables secure multi-tenancy, and reduces lateral attack surface via zero-trust segmentation.

Figure 1 shows real-time and historical visibility into network traffic flows to validate network connectivity, enforce policies, and troubleshoot applications.

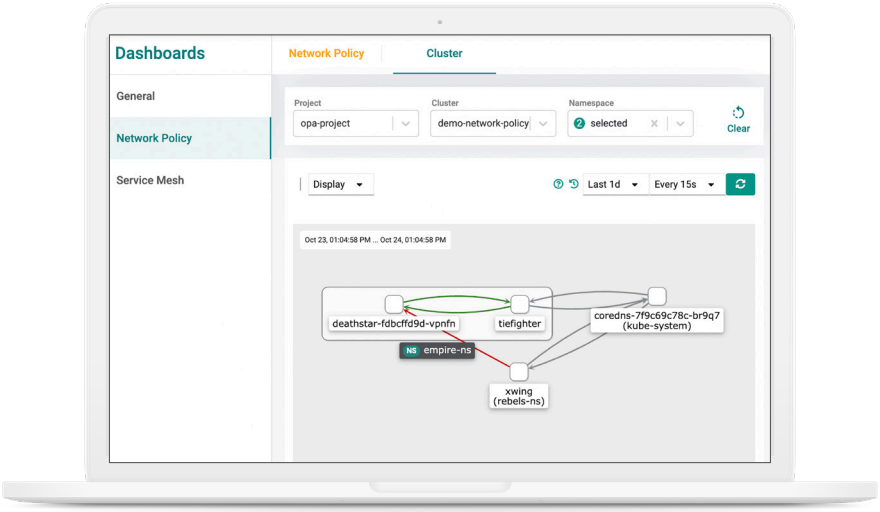

Figure 1 - Dashboard of the Rafay Network Policy Manager

The Challenge

Network security configuration can be error-prone, time-consuming, and add operational overhead to manage and enforce multiple clusters. In addition, without the necessary security policy and enforcement, Kubernetes infrastructure network traffic is open to lateral movement, including ingress/egress and pod connectivity. This is why CISA recommends using network policies to control traffic and enforce segmentation in their Kubernetes Hardening Guide.

Enterprise requirements that solve these challenges include:

- **Secure zero-trust segmentation** to prevent lateral movement and reduce the attack surface, including org/cluster-wide defaults
- **Centralized namespace isolation** to enforce different types of multi-tenancy in shared cluster environments
- **Governance and standardization** for multi-cluster network policy, enforced configuration, and security compliance
- **Real-time and historical visibility** into application traffic flows and reducing time to resolve issues
- **Network Policy Automation** and enforcement of network policy installation, configuration, and upgrades

Key Capabilities of Network Policy Manager

Network Policy Manager, powered by Cilium, is a service that allows platform teams to centralize network security and visibility for fleet-wide Kubernetes environments instantly. This removes the burden and operational overhead of enabling network policy automation, standardization, and governance across your fleet of clusters and applications using disparate DIY tools.

The Network Policy Manager provides:

- **Centralized Network Policy Enforcement**: Zero-trust segmentation, rules configuration, consistent policy for inter-pod network connectivity, namespace isolation, and cluster-wide policies
- **Automated Deployment**: Network Policy Profiles and Rafay Cluster Blueprinting enable automated network security deployment, consistent delivery, and standards enforcement for large scale across any cluster type or cloud provider
- **Built-in Dashboards**: Visualization of real-time and historical traffic flows across your Kubernetes infrastructure with added granular access controls for developer self-service

Platform Teams enable Network Policy Manager for fleet-wide Kubernetes clusters with a simple, centralized enable option via the Rafay Controller shown in Figure 2. Cilium is automatically installed and configured on the target clusters as a chained CNI using Network Policy Profile and Rafay Cluster Blueprints for cluster-wide deployments. Cluster Blueprints allow network policies to be "baked-in" to the target clusters and enforce fleet-wide standardized configuration. A Network Policy installation profile is defined with a policy and associated rules so administrators can configure and enforce declarative network policies scoped to a cluster or namespace.

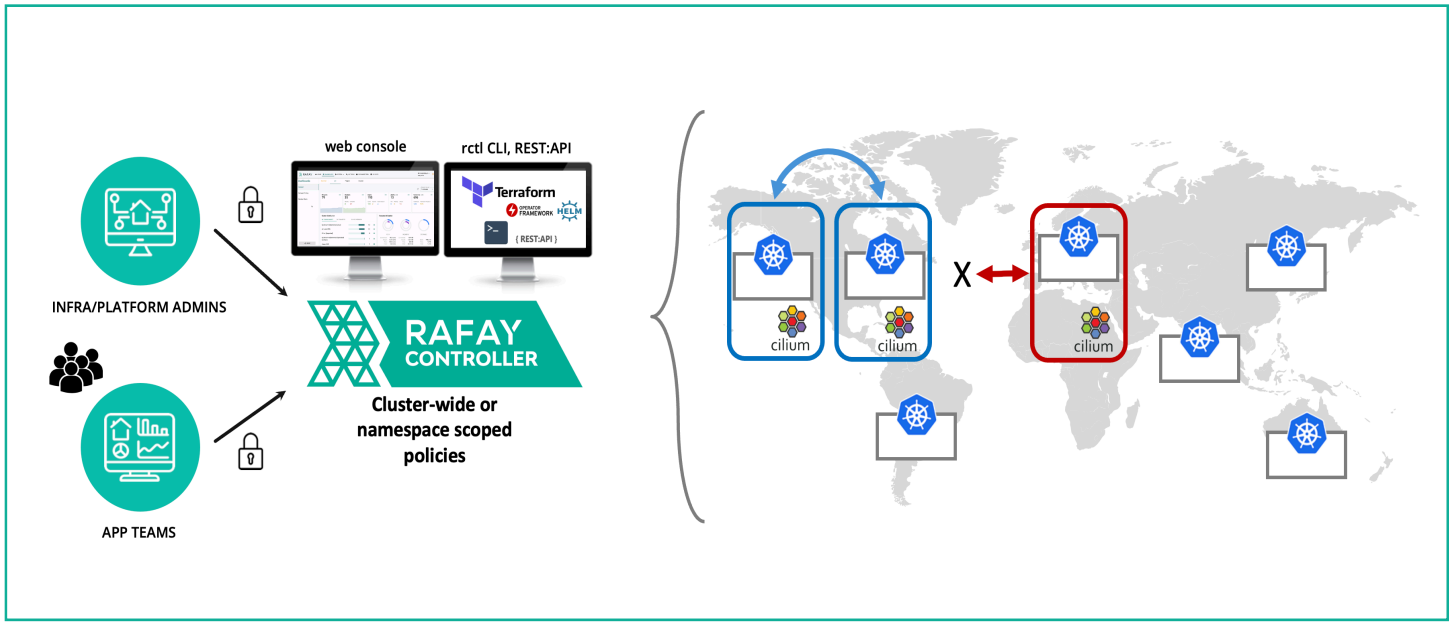

Figure 2 - Rafay Network Policy Manager

A Network Policy rule is a construct that helps define traffic flow patterns that are allowed or denied. Two network policy rules are supported for 1) cluster-wide and 2) namespace policies. In addition, all Network Policy rules are based upon a whitelist model; each rule in the policy allows traffic that matches the rule.

Users have visibility into network flows for their clusters and applications directly via the Rafay Controller web console, rctl CLI, or REST-API. For example, the Network Policy Dashboard (Figure 1) provides visibility and historic replay into network traffic connectivity and flows between pods and namespaces. In addition, it is controlled based on user role, giving platform teams visibility into the entire infrastructure while developers may only get visibility into their specific namespaces and applications. This enables validating namespace isolation, checking default security posture, troubleshooting applications, and comparing and contrasting network traffic flows over time. In addition, the historical replay enables visualization for verification and connectivity over time. This allows platform teams to validate isolation boundaries and cluster-wide defaults while allowing developers to troubleshoot their specific applications. More details can be found in Rafay's online documentation.

Summary

The Rafay Network Policy Manager provides strengthened security, accelerates service delivery, and reduces service outages. Key highlights are:

Centralized Network Policy Enforcement	Provides zero-trust security segmentation to prevent lateral movement and enforce network connectivity across your clusters and namespaces, thus strengthening security.
Standardized Installation Profiles	Provide a set of parameters to set up and install the Network Policy and visibility Add-On (Cilium), providing consistent network policy and configuration enforcement for accelerating service delivery.
Network Policy Dashboards	Provide troubleshooting and visibility into traffic flows across your Kubernetes infrastructure, visualizing which network policies are being enforced across namespace isolation and clusters for reducing service outages.