Falco + Network Policies (Runtime Security)

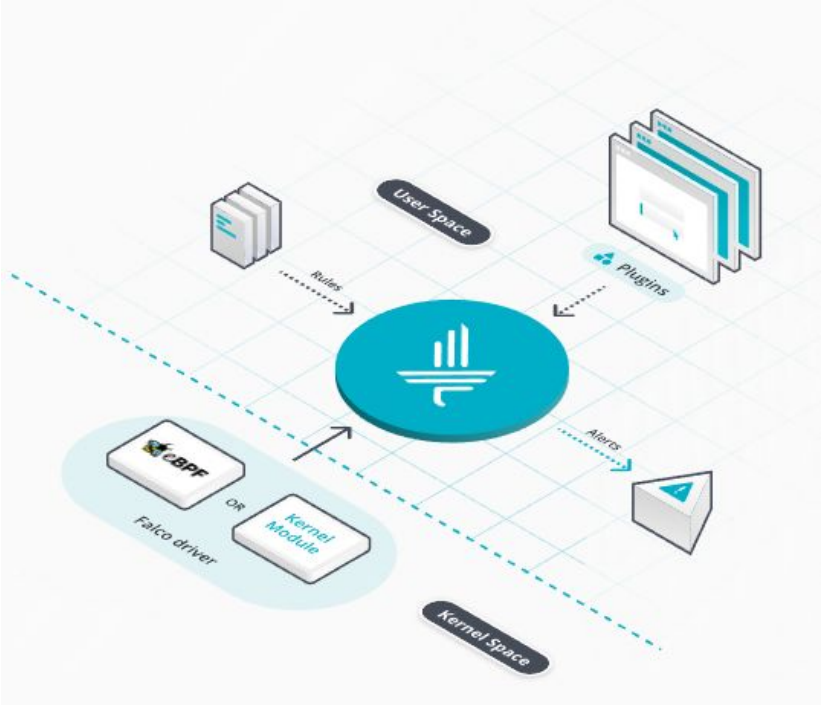
Equipo 4:

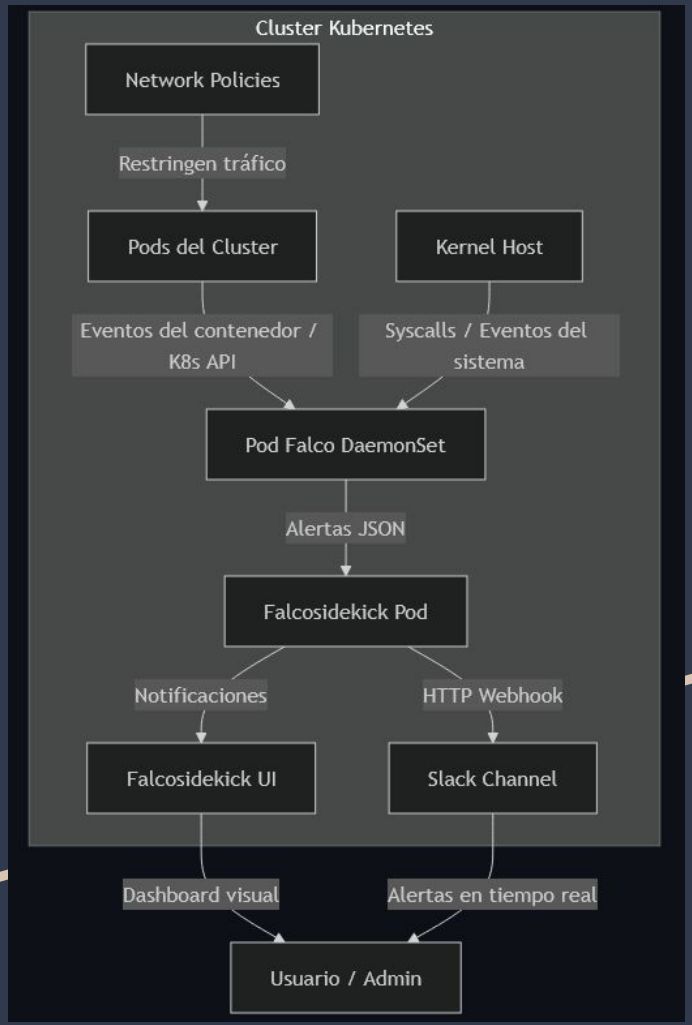
Álvarez Reyes Juan Luis
Martínez Balderas Roberto

¿Qué es Falco?

Falco es una herramienta de seguridad nativa de la nube que proporciona seguridad en tiempo de ejecución en hosts, contenedores, Kubernetes y entornos de nube.

En otras palabras Falco es un **IDS (Intrusion Detection System)** que funciona en tiempo real.





¿Qué lo hace importante?

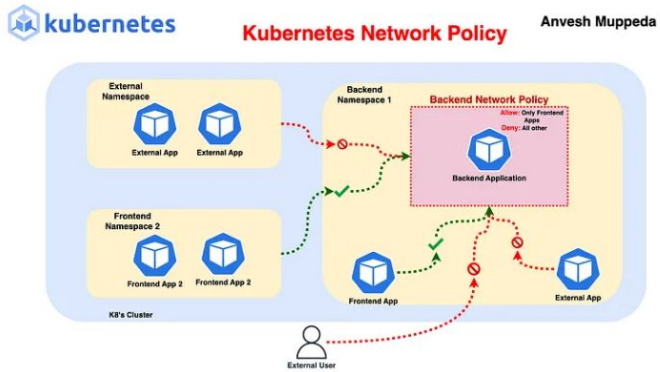
- Revisa eventos del kernel de Linux para poder detectar cualquier comportamiento anómalo.
- Es Flexible ya que permite la utilización de múltiples plugins y personalizar las reglas de detección.
- Permite una integración fácil con más de 50 sistemas.
- Código abierto.

¿Qué son las Network Policies?

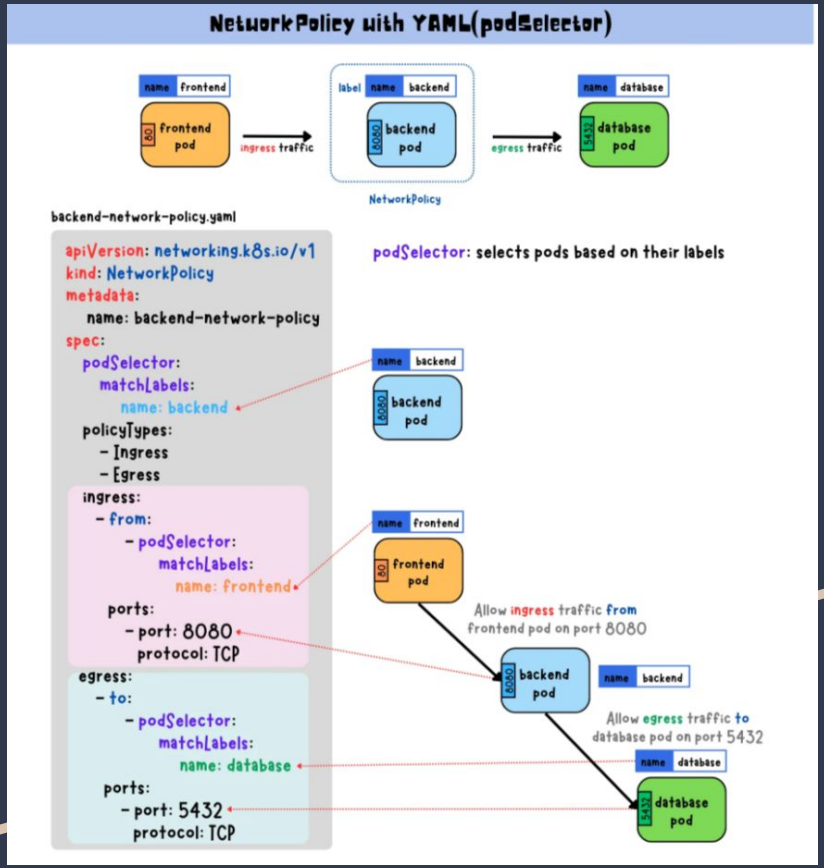
Las Network Policies son una serie de reglas que definen el flujo de tráfico dentro del clúster, así como entre los pods y el exterior.

Se implementan mediante un plugin de red o CNI. Los CNIs que soportan las políticas son:

Antrea, Calico, Cilium, Kube-router, Romana y Weave Net



Documentación oficial en: https://kubernetes.io/docs/concepts/services-networking/network-policies/



Las Network Policies son importantes porque:

- Proporcionan una capa adicional de seguridad al clúster, controlando el flujo de tráfico.
- Permiten el aislamiento de aplicaciones por espacio de nombres (namespace).
- Restringen el tráfico de entrada y salida hacia Pods específicos.
- Limitan o bloquean el acceso a API externas, reduciendo la exposición del clúster a redes no confiables

Demostración

CONCLUSIONES:

- La utilización conjunta de **Falco (IDS)** y **Network Policies** fortalece significativamente la seguridad en **Kubernetes**.
- En conjunto, proporcionan **visibilidad, control y respuesta ante incidentes** tanto a nivel de las **llamadas ejecutadas al kernel en cada pod**, como en el **manejo del tráfico que fluye entre ellos**.
- Permiten una gran flexibilidad al ser **ampliamente configurables** y adaptarse prácticamente a **cualquier esquema de trabajo**.
- Ambas, al estar desarrolladas bajo el respaldo de la **Cloud Native Computing Foundation (CNCF)**, presentan una **gran sinergia** entre sí.

Gracias!!!