May 10, 2018

SECURITY SOLUTION FOR KUBERNETES USING CLOUD-NATIVE VIRTUAL NETWORK FUNCTIONS

Jan Medved
Cisco Systems, Inc.

SECURITY SOLUTION FOR KUBERNETES USING CLOUD-NATIVE VIRTUAL NETWORK FUNCTIONS

AUTHORS:
Jan Medved

CISCO SYSTEMS, INC.

ABSTRACT

A cloud security solution is described herein for Kubernetes-orchestrated clusters using a security cloud-native Virtual Network Function (VNF) deployed on the cluster. One advantage to this solution is that it is built into Kubernetes networking, and is therefore easier to manage/orchestrate. Moreover, it is modular (e.g., can be combined with other solutions via Service Function Chaining (SFC)), and is easier to extend/modify than in other security solutions, which may require changes to the kernel.

DETAILED DESCRIPTION

Existing networking solutions for Kubernetes rely on data path capabilities of the Linux kernel or the Open Virtual Switch (OVS) plugin within the kernel. This limits their functionality to implementations of basic Kubernetes policy with possibly minor extensions. Sophisticated security features, such as Distributed Denial of Service (DDOS) attack detection/mitigation or scrubbing of traffic destined for application pods must be implemented by an external appliance. In particular, there exists no security solution where the capabilities of a sophisticated security device are built into the Kubernetes networking plugin.

The techniques described herein use a cloud-native security Virtual Network Function (VNF) to secure application workloads deployed on a Kubernetes cluster. A cloud-native VNF is a VNF designed for cloud environments: it runs on the Kubernetes cluster, its lifecycle is orchestrated by Kubernetes, and its control/management plane is designed according to the twelve-factor application principles (see https://12factor.net). Cloud-native VNFs must support Development Operations (DevOps) based deployment patterns, including canary and blue-green deployments. The security appliance may be

based on Ligato, which is a framework for implementing cloud-native VNFs (see http://github.com/ligato).

The prerequisite for deployment of cloud-native VNFs on Kubernetes is the use of Contiv-VPP as the Kubernetes Container Networking Interface (CNI) networking plugin (see http://github.com/contiv/vpp). The security appliance is deployed on the Kubernetes cluster as yet another pod. The Contiv-VPP plugin is instructed to redirect traffic destined to a target application pod to the security appliance, where security policies are applied. The Contiv-VPP plugin then routes the application traffic from the security appliance to the target application pod. On the reverse path, the outgoing traffic of the application pod can be routed to the appliance, or directly to the network.

Figure 1 below illustrates an example present mode of operation.

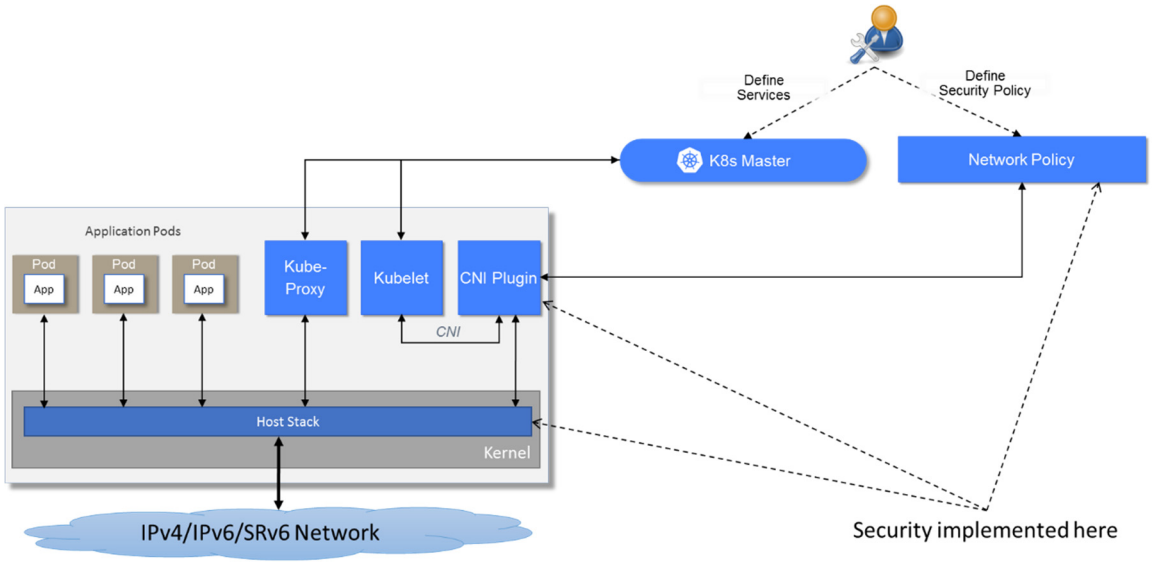

Figure 1

Figure 2 below illustrates an example solution described herein.

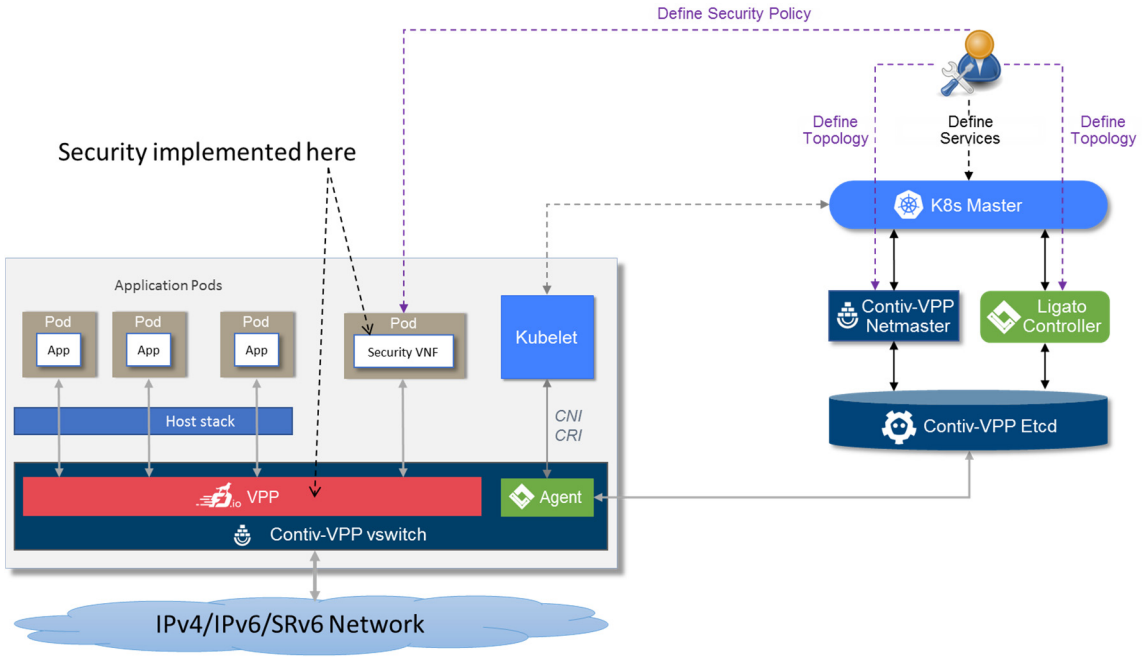

Figure 2

Figure 3 below illustrates an example data path.

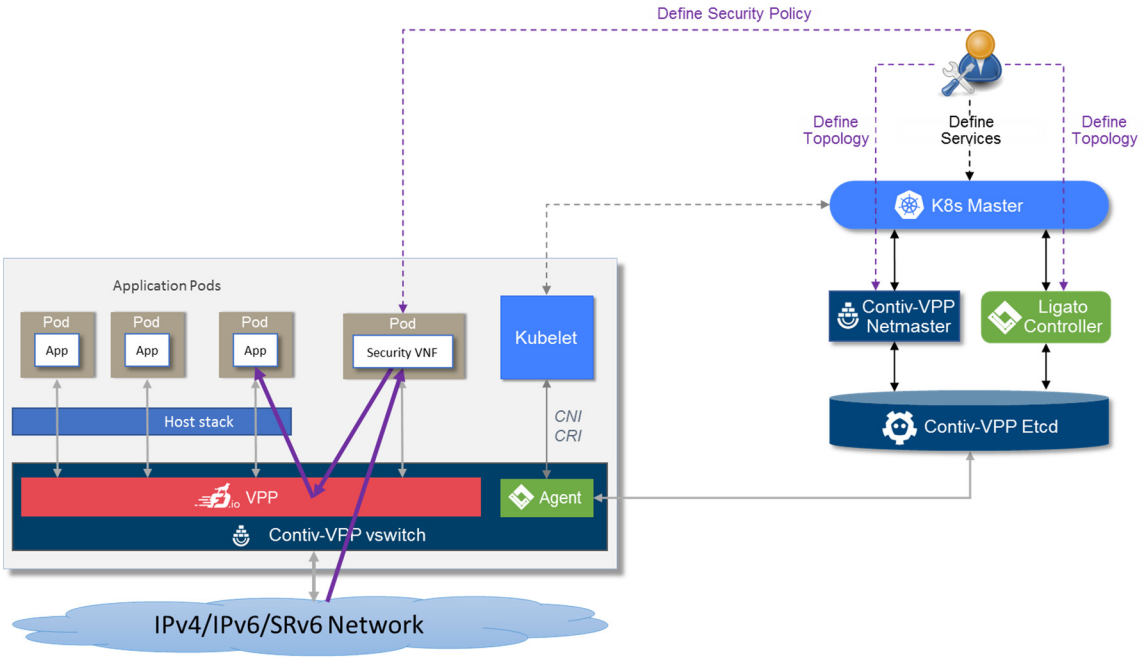

Figure 3

Figure 4 below illustrates an example container application network chain.

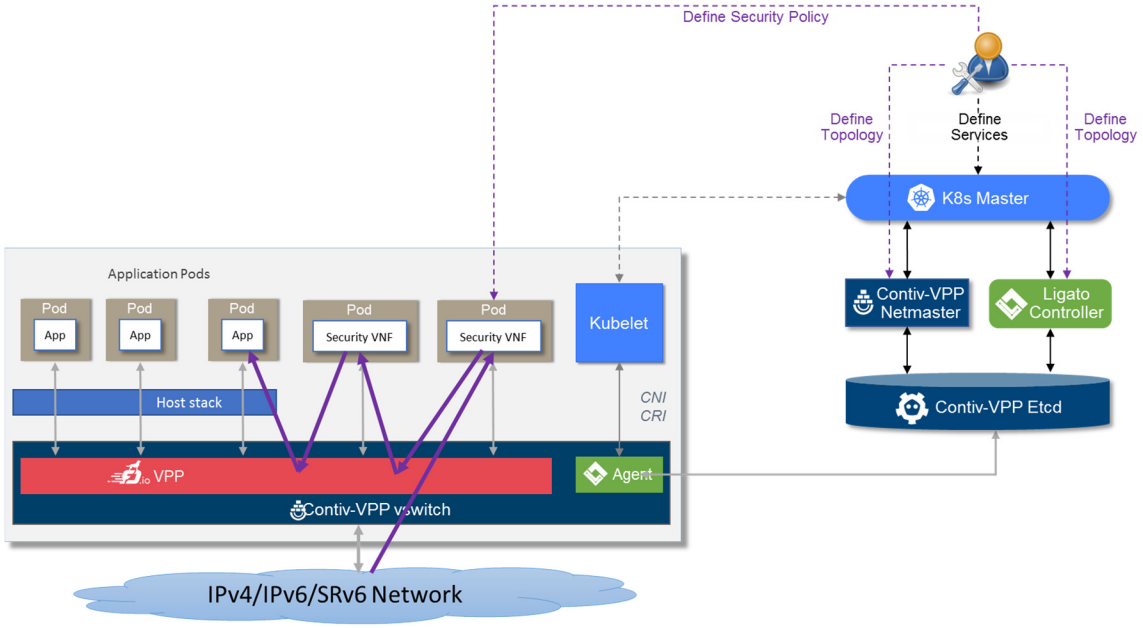

Figure 4

In summary, a cloud security solution is described herein for Kubernetes-orchestrated clusters using a security cloud-native VNF deployed on the cluster. One advantage to this solution is that it is built into Kubernetes networking, and is therefore easier to manage/orchestrate. Moreover, it is modular (e.g., can be combined with other solutions via Service Function Chaining (SFC)), and is easier to extend/modify than in other security solutions, which may require changes to the kernel.