FortiOS - Kubernetes Cookbook

Version 6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

October 28, 2020
FortiOS 6.4 Kubernetes Cookbook
01-640-619493-20201028

TABLE OF CONTENTS

About FortiGate-VM and Kubernetes

FortiOS supports automatically updating dynamic addresses for Kubernetes (K8s) using a K8s Fabric connector, enabling FortiOS to manage K8s pods as global address objects, as with other connectors.

In addition, Fortinet has partnered with Tigera for further integration between Calico and FortiGate. Calico and Calico Enterprise provide the networking and security framework to secure K8s networks. The largest public cloud providers have selected Calico to provide network security for their hosted K8s services. Through its Firewall Manager integration, it can offload zone-based security to the FortiGate firewall. This is accomplished by providing dynamic address updates directly to the FortiGate via REST API.

Automatically updating dynamic addresses using a Kubernetes Fabric connector

See *Private Cloud K8s SDN connector*.

Automatically updating dynamic addresses using Calico FortiGate integration

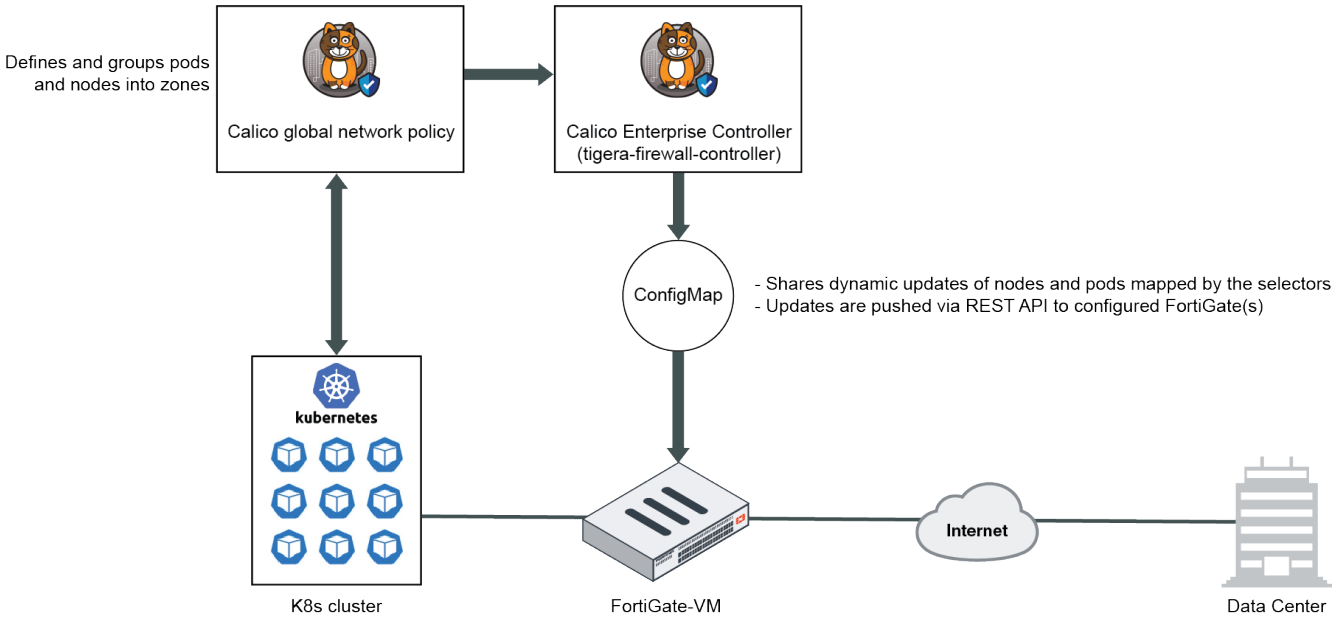
When deploying a Kubernetes (K8s) cluster, you can install a third-party network policy provider. Calico is a popular provider that provides the necessary framework to protect and secure the network. The largest public cloud providers have selected Calico to provide network security for their hosted K8s services (Amazon EKS, Azure AKS, Google GKE, and IBM IKS) running across tens of thousands of clusters.

Through its Firewall Manager integration, Calico can effectively separate network controls and security controls. Operationally, this allows a company to assign security tasks to the Security Operations team using a familiar firewall such as the FortiGate and management tool such as FortiManager.

Nearly every application has dependencies external to K8s that require some level of access control, such as access requirements for database, third-party APIs, and cloud services.

Calico implements zone-based security in order to secure K8s workloads. For example, Internet-facing workloads run in the demilitarized zone, while other workloads for backend business logic may run in the trusted zone. These workloads are dynamic in nature and can be brought up/down and moved across nodes and clusters frequently. Therefore, a Firewall Manager must be informed of each dynamic address change to properly secure the workload.

See Extend FortiGate Firewalls to Kubernetes with Calico Enterprise in Tigera's documentation for the general workflow. Following is a high-level overview of the workflow:



The Calico Enterprise Controller, also called tigera-firewall-controller, shares K8s node and pod addresses with FortiGate. The controller uses a ConfigMap to define the selectors for mapping the workloads to firewall address groups. The ConfigMap also defines the desired FortiGate(s)/FortiManager(s) to communicate with. The controller then pushes dynamic updates to the FortiGate(s) via REST API. Subsequently, traffic from the K8s cluster passes through the FortiGate, and you can administer zone-based security using firewall policies.

To configure automatically updating dynamic addresses using Calico FortiGate integration:

1. Configure Calico assets as Extend FortiGate Firewalls to Kubernetes with Calico Enterprise describes.
2. Configure a REST API administrator in FortiOS:
   a. Go to *System* > *Administrators*, then select *Create New* > *REST API Admin*.
   b. In the *Username* field, enter a username, such as *calico_enterprise_api_user*.
   c. If desired, enter comments.
   d. Creating a new administrator profile with minimal privileges is recommended. Create a new profile:
      i. From the *Administrator Profile* dropdown list, select *Create*.
      ii. In the *Name* field, enter the desired name, such as *tigera_api_user_profile*.
      iii. Under *Access Permissions*, configure the following:
         i. For *Firewall*, select *Custom*.
         ii. For *Address*, select *Read/Write*. The REST API can send read and write requests (HTTP GET/POST/PUT/DELETE) to the resource.
         iii. For all others, leave as *None*.
      iv. Click *OK*.
   e. FortiOS displays an API key. Copy and store the key securely, as it is only shown once.

Once configuration is complete on the FortiGate and Calico, you see address objects being created on the FortiGate. When changes occur on your workloads, the address objects change as well. The address objects are marked with a “Managed by Tigera Calico Enterprise” comment.

With these new dynamic address groups, you can define firewall policies to deploy zone-based security for your K8s network.

Change log

Date	Change Description
2020-03-31	Initial release.
2020-10-28	Added Automatically updating dynamic addresses using Calico FortiGate integration on page 4. Updated About FortiGate-VM and Kubernetes on page 4.