SOLUTION BRIEF

Fortinet and Tigera Security Solution

Extending Enterprise Security into Kubernetes Environments

Executive Summary

Fortinet FortiGate Next-Generation Firewalls (NGFWs) provide industry-leading threat protection and decryption at scale with a custom ASIC architecture. They also deliver Secure Networking with integrated features like SD-WAN, switching and wireless, and 5G. FortiGate firewalls establish a secure perimeter around applications, effectively managing inbound and outbound traffic for the organization. Firewalls primarily rely on IP addresses for implementing allow-deny policies.

Most enterprises that adopt microservices and Kubernetes-based applications operate in a hybrid environment where legacy applications reside on-premises or in the cloud. These applications rely on perimeter-based NGFWs, such as the FortiGate, with appropriate network security rules to govern traffic flows and extend it to their Kubernetes environment. Fortinet and Tigera have partnered to build integrations with FortiGate and FortiManager to enforce end-to-end security policies, address visibility into north-south and east-west traffic as well as compliance enablement and advanced threat-intelligence capabilities for Kubernetes clusters.

Security Challenges in Kubernetes

IP addresses are effective for non-cloud-native applications, where static IP addresses serve as definitive network identifiers. However, in a Kubernetes environment, workloads have dynamic IP addresses that change whenever they are restarted or scaled to different nodes. This dynamic nature poses challenges requiring continuous updates to firewall rules and the opening of large CIDR ranges for node-based access. This deployment introduces security and compliance risks as workloads running on these CIDR ranges could gain unrestricted access to external or public services.

Maintaining two separate security platforms, one for perimeter network security and one for Kubernetes security, that do not have integration hinders visibility into routing and connectivity within and between Kubernetes clusters and external endpoints. Maintaining, syncing, and operating two different security policy-enforcement platforms manually can be inefficient and prone to errors for containers and Kubernetes and creates security and compliance risks. Kubernetes deployments must fulfill organizational and regulatory security requirements like any on-premises or cloud-based services. If compliance teams cannot trace the incidents across the entire infrastructure, they cannot adequately satisfy audits into Kubernetes clusters.

Solution Components

- Fortinet FortiGate
- Fortinet FortiManager
- Fortinet FortiSIEM
- Tigera Calico Kubernetes Controller

Solution Benefits

- **Security posture continuity:** Extend approved corporate network security policies to Kubernetes
- **Full visibility into Kubernetes clusters:** Pinpoint specific sources of errors and risk
- **Security-driven DevOps:** Shift Kubernetes security to an earlier stage in application development
- **Collaborative security culture:** Ensure security success is jointly owned by platform, security, compliance, networking, and DevOps teams

FORTINET FABRIC-READY

Integrating Calico Enterprise and the Fortinet Security Fabric

To extend traditional perimeter network security to the Kubernetes cluster at the workload level and vice-versa, it becomes crucial to identify workloads that necessitate access to external resources and assign them fixed IP addresses for utilization in FortiGate firewall rules. The integration of Calico with FortiGate firewalls and FortiManager offers an elegant and effective solution, enabling the use of FortiGate firewalls while retaining existing controls and adapting current tools to the Kubernetes environment. This integration provides two options for seamless operation:

FortiGate Calico Kubernetes Controller automatically updates FortiGate firewalls with Kubernetes pod IPs to control pod egress access, minimize firewall change orders, and eliminate error-prone manual processes. Using the Fortinet-Calico Enterprise integration, security teams can retain firewall responsibility and secure traffic using the Calico Enterprise network security policy, which frees up time for network, platform, DevOps, and SRE teams.

FortiManager Calico Kubernetes Controller enables Kubernetes cluster management from the FortiManager centralized management platform. This Fabric Connector translates FortiManager policies into granular Kubernetes network policies, pushing them to the individual clusters in all Kubernetes environments. Thus, the Kubernetes environment becomes integral to the Fortinet Security Fabric and can be seen and controlled from the FortiManager console.

FortiGuard Labs threat feed integration enriches the Calico threat database with global real-time threat intelligence from FortiGuard Labs. Calico Enterprise users gain broader protection from malicious traffic at the source in the Kubernetes cluster. For FortiGuard subscribers, this integration ensures that the most robust protection will cover their Kubernetes environment at no additional cost.

The Calico-FortiSIEM plug-in event correlation and risk management solution delivers the telemetry (metadata) that Calico creates, including DNS logs, flow logs, and audit logs, into the Fortinet security information and event management (SIEM) environment. This helps security operations teams leverage FortiSIEM to better design and automate their workflows for incident response.

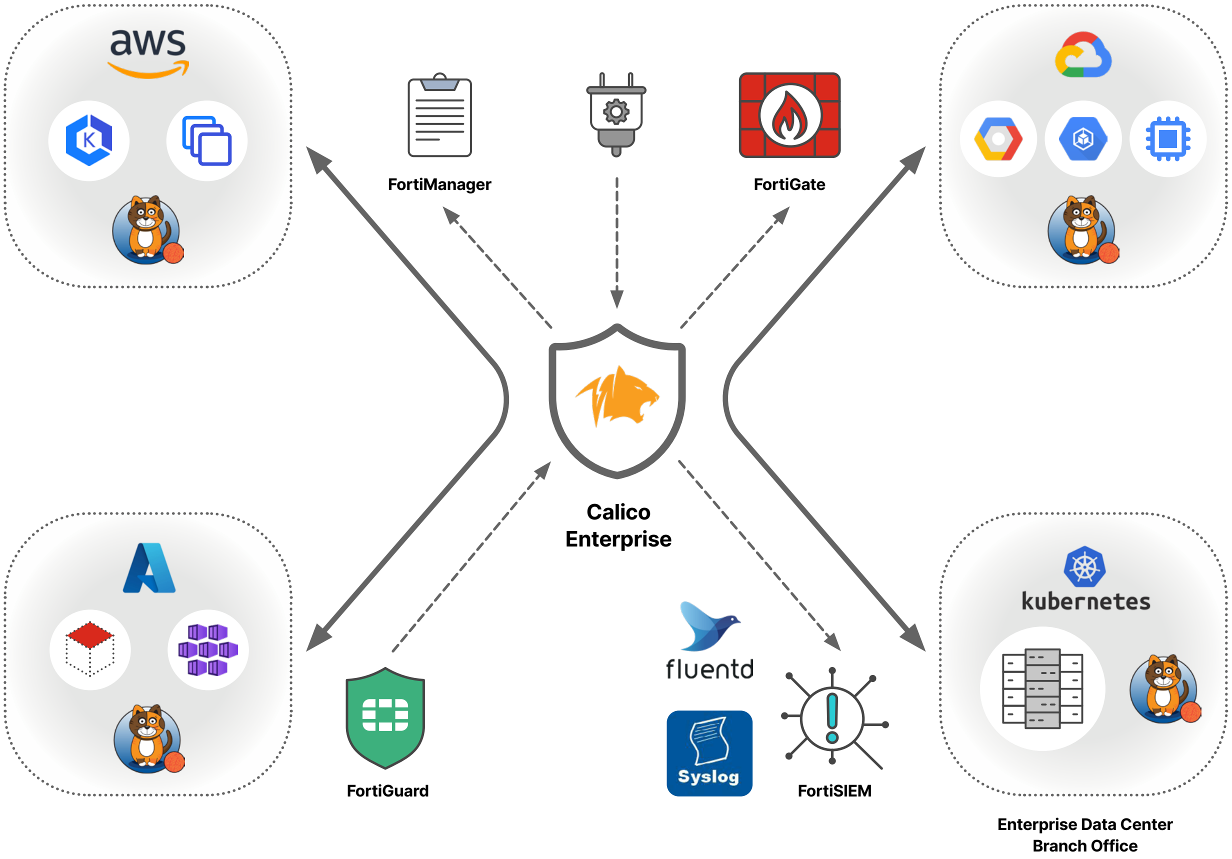

Figure 1: Calico for Fortinet solutions leverage Calico's Kubernetes expertise and broad installed base to benefit Fortinet Security Fabric customers.

Benefits for Customers

The Calico integration with Fortinet FortiGate and FortiManager solutions extends the firewall capability to Kubernetes. The joint solution brings Kubernetes deployments into the fold of the Fortinet Security Fabric. This ensures that organizations migrating to Kubernetes architectures maintain their security posture and ensure the successful adoption of the Kubernetes platform throughout the enterprise. On an operational level, integration between Fortinet and Tigera technologies provides the comprehensive insight needed to speed up troubleshooting, reducing mean time to resolution. These integrated technologies also reduce operational complexity, which reduces staff and training costs and minimizes configuration errors that can add significant attack risk to the organization. Security architects can also demonstrate the reduced risk in a timely fashion to comply with internal and external data-protection rules.

About Tigera

Tigera delivers the industry's only active security platform with full-stack observability for containers and Kubernetes. Tigera's platform, delivered as a fully managed SaaS or self-managed service, prevents, detects, troubleshoots, and automatically mitigates exposure risks of security breaches.

www.fortinet.com

February 22, 2024 4:05 PM

2572906-0-0-EN