Whitepaper

TIGERA

PCI Network Security Compliance for Kubernetes Platforms

Modern architectures require greater attention to network security, especially for applications that handle credit card data. The addition of containers and Kubernetes only creates additional concerns.

Table of Contents

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) requires any entity that stores, processes or transmits cardholder information to meet minimum levels of security to ensure it adequately protects the integrity and confidentiality of payment information. It applies to businesses of all sizes as well as organizations that only transmit card data and service providers whose offerings include handling cardholder data. PCI is a global standard on which most enterprises model their security standards and processes.

PCI DSS covers systems that handle cardholder data, whether at rest or in motion, systems that segregate the cardholder data environment (CDE), and those that control access to the CDE. That might include routers, switches, hypervisors, and application software.

While the PCI standard is extensive, it was designed with traditional infrastructure components in mind. Before Kubernetes, monolithic application components communicated via in-process library function calls. With Kubernetes, modern application components communicate via network-based API calls. This difference means that security can no longer be enforced primarily by libraries and runtime frameworks. Instead, security must be applied at the network level. Traditional security solutions like perimeter security, zone-based security, and static firewalls are not scalable or flexible enough to meet security controls for Kubernetes. Compliance tools designed to provide audit trails also were designed for static applications and environments and won't provide context into microservice traffic in Kubernetes.

Challenges Meeting PCI Compliance Requirements with Traditional Solutions and Approaches

PCI requires that businesses with more than six million credit card transactions per year undergo yearly audits conducted by a qualified auditor. In these modern environments, an audit can ensure only that an organization was in compliance at a certain point in time. Then ten minutes

later a developer might push a new version of code containing a mistake that throws it out of compliance.

PCI compliance requirements apply to applications, infrastructure, and networks yet developers, operations and security teams often don't speak the same language or have the same priorities. Many organizations have compliance teams that also must be part of any plan.

PCI requires network segmentation or isolating the cardholder data environment from the remainder of an entity's network. However, traditional firewalls don't adequately protect dynamic environments that can encompass hundreds of thousands of API calls per second in hybrid and multi-cloud setups. This evolution in architecture is bringing a whole new class of connectivity and security issues. The challenge for organizations running hybrid and cloud environments is how to combine components and services in a scalable, automated and secure manner – and how to ensure consistency and portability.

PCI DSS requires proper monitoring at the network level. The challenge with traditional network monitoring tools is that they generate inaccurate data for Kubernetes. These dated methods only capture 5-tuple information, which does not capture the context required to demonstrate compliance in a dynamic Kubernetes environment.

How Tigera Supports PCI Requirements

Tigera focuses on establishing zero-trust network security, visibility and traceability, and enterprise control and continuous compliance across all environments.

Tigera promotes the concept of continuous compliance using policies based on the characteristics and metadata of a workload rather than IP addresses, which are constantly changing in dynamic environments.

"Policy as code" is part of continuous compliance which enables organizations to create immutable security artifacts. This can be implemented in the CI/CD pipeline and become part of your organization's version control system. Network policies can provide an automated and

scalable way to control traffic and isolate workloads for security and compliance. Furthermore, tiered network policy models help align with organizational needs with separating concerns of different groups in a hierarchical manner. Policy tiers enable businesses to safely delegate policy specification to various teams. By leveraging tiered network policy, teams can plan and meet their compliance objectives in an efficient and autonomous manner.

Continuous compliance means employing a continual audit that shows what traffic was allowed in your infrastructure, what traffic was denied and why, as well as logs of who was trying to change what and whether those changes went into effect.

Continuous compliance gives teams the ability to pinpoint any point in time and say with reasonable surety whether the organization was in compliance – and provide documentation showing why they say so.

Tigera PCI Requirements Mapping

The following table addresses requirements from sections 1,2,4, 5, 6, 7, 10, and 11 of the PCI DSS and Tigera guidance for bringing your systems into compliance with them. Note: Not all the requirements are covered. Some may require more specific information about your environment for you to know how to become fully compliant.

PCI Control #	Requirements	Tigera Guidance
1.1, 1.1.4, 1.1.6, 1.2.1,1.2.2,1.2.3	Install and maintain a firewall configuration to protect cardholder data	• Tigera Secure identifies everything covered by PCI requirements with a well-defined label (for example: PCI=true) • Tigera Secure blocks all traffic between PCI and non-PCI workloads • Tigera Secure whitelists all traffic within PCI workloads
1.1.2, 1.1.3	Current network diagram that identifies all connections between the CDE and other networks and systems	• Leverage Tigera Secure flow log and policy visualization tool to stay current with the network diagram/graph for inscope workloads in Kubernetes environments
1.1.1,1.1.5,1.1.7	A formal process for approving and testing all network connections and changes to the rule sets	• Record and review all network policy changes that affect connectivity between covered components with Tigera Secure
1.3, 1.3.1, 1.3.2, 1.3.3,1.3.4,1.3.5, 1.3.7	Prohibit and/or manage access between internet and CDE	• Tigera Secure whitelists ingress access from public internet only if the endpoint is providing a publicly accessible service • Tigera Secure whitelists egress access to the public internet from all in-covered components • Tigera Secure provides mutual Transport Layer Security (mTLS) to protect against forged source IP addresses

2.2,2.4	Inventory the systems and make sure they meet industry-accepted system-hardening standards	• Tigera Secure helps keep a running inventory of all ephemeral workloads along with their network security controls
4.1	Data-in-transit encryption to safeguard sensitive data	• Tigera Secure enables data-in-transit encryption for all covered workloads
5.1, 5.2, 5.3, 5.4, 10.6, 11.4	Protect all systems against malware with Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS) and network monitoring. Regularly update antivirus software. Review logs for anomalous and suspicious activity.	• Use Tigera Secure anomaly and Threat detection capabilities instead of antivirus software • Leverage Tigera Secure to monitor and analyze the findings • Tigera Secure can automatically quarantine workloads with confirmed compromise • Tigera Secure network flow logs provide insights into statistical and behavioral anomalies
6.5, 6.6	Detect and prevent web attacks	• Use Tigera Enterprise Calico Policy to implement fine-grained access controls for services
7.1,7.2	Restrict access to cardholder data by business need to know	• Use Tigera Zero Trust Network Security features to implement a default-deny model - access to all data services should be specifically allowed, otherwise denied • Follow Tigera Zero Trust Network Security and implement a least-privilege model - all processes must be able to access only information necessary for their legitimate purpose
10.1,10.2.10.3	Implement and record audit trail for all access to system components	• Tigera Secure records all policy changes that impact connectivity to / from in-scope assets

Managing PCI Audits with Tigera Secure

The following table outlines how to prepare for PCI audits sections 1,2,4, 5, 6, 7, 10, and 11 with Tigera. Note: Not all the requirements are covered. Some may require more specific information about your environment for you to know how to become fully compliant.

PCI Control #	Requirements	Tigera Guidance on Evidence Report
1.1, 1.1.4, 1.1.6, 1.2.1,1.2.2,1.2.3	Install and maintain a firewall configuration to protect cardholder data	• Tigera Secure provides evidence of compliance with Inventory Report
1.1.2, 1.1.3	Current network diagram that identifies all connections between the CDE and other networks and systems	• Tigera Secure provides evidence of compliance with Flow Log Visualization
1.1.1,1.1.5,1.1.7	A formal process for approving and testing all network connections and changes to the rule sets	• Tigera Secure provides evidence of compliance with Network Access Report
1.3, 1.3.1, 1.3.2, 1.3.3,1.3.4,1.3.5, 1.3.7	Prohibit and/or manage access between internet and CDE	• Tigera Secure provides evidence of compliance with Network Access Report
2.2,2.4	Inventory the systems and makes sure they are consistent with industry-accepted system-hardening standards	• Available with future Tigera Secure releases
4.1	Data-in-transit encryption to safeguard sensitive data	• Tigera Secure provides evidence of compliance with Network Access Report
5.1, 5.2, 5.3, 5.4, 10.6, 11.4	Protect all systems against malware with Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS) and network monitoring. Regularly update antivirus software. Review logs for anomalous and suspicious activity.	• Tigera Secure provides evidence of compliance with Inventory Report
6.5, 6.6	Detect and prevent against web attacks	• Tigera Secure provides evidence of compliance with Inventory Report
7.1,7.2	Restrict access to cardholder data by business need to know	• Tigera Secure provides evidence of compliance with Inventory Report
10.1,10.2.10.3	Implement and record audit trail for all access to system components	• Tigera Secure provides evidence of compliance with Policy Audit Report

About Tigera

Tigera delivers solutions for secure application connectivity for the cloud native world. Tigera technology is used by the world's largest enterprises and public cloud providers to power connectivity for application development and deployment and to address the connectivity and security challenges that arise in at-scale production. Tigera Secure meets enterprise needs for zero trust network security, multi-cloud and legacy environment support, organizational control and compliance, and operational simplicity. Tigera Secure builds on leading open source projects Kubernetes, Calico, and Istio, which Tigera engineers help maintain and contribute to as active members of the cloud native community.

tigera.io

email: contact@tigera.io

phone: +1.415.612.9546

Tigera, Inc. 58 Maiden Lane, Fifth Floor, San Francisco CA 94018 USA