BUSINESS PAPER

Streamline PCI Compliance with the Aruba CX 10000 Distributed Services Switch

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Aruba CX 10000 Distributed Services Switch with embedded AMD Pensando DPUs offers organizations an option to implement effective network segmentation by applying stateful firewall inspection policies at the switch port level, without having to route traffic to an external firewall for inspection. The Aruba CX 10000 is designed for securing East-West traffic and providing effective isolation for individual hosts or groups of hosts in the same rack even when those hosts are in the same L2 broadcast domain. This capability can be leveraged for minimizing the scope of Payment Card Industry Data Security Standard (PCI DSS) compliance as well as for meeting multiple PCI DSS requirements. The ability to implement segmentation at the port or host level ultimately reduces the cost and operational burden required to achieve and maintain PCI compliance, as well as validate compliance annually.

To evaluate features and functionality of the Aruba CX 10000 and determine PCI compliance benefits of this solution, Protiviti, a global consulting firm and one of the world's leading Payment Card Industry Qualified Security Assessors, was provided product documentation as well as a demo and a detailed walk through of the switch by an AMD Pensando product specialist.

This document is intended to provide high-level guidance about the features of the Aruba CX 10000 and its benefits for achieving PCI DSS compliance. Functionality that is valuable and important from a network operations perspective, but does not impact PCI compliance, is not analyzed in this paper. This document also provides information about specific PCI DSS 4.0 requirements that are supported or could be met directly by the Aruba CX 10000. The guidance and opinions expressed in this document are not intended to be comprehensive, and organizations leveraging the AMD/Aruba solution for achieving PCI compliance objectives should seek guidance from their QSA (Qualified Security Assessor) to confirm applicability in the context of their environment.

HOW SCOPE AND SEGMENTATION ARE CONSIDERED IN THE PCI DATA SECURITY STANDARD (DSS)

Per the PCI DSS version 4.0 specification, the scope of requirements applicable to an entity has been defined as the Cardholder Data Environment (CDE), which includes,

"– System components, people, and processes that ***store, process, and transmit cardholder data*** *and/or sensitive authentication data, and,*

– System components that may not store, process, or transmit CHD/SAD but* ***have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.***

- AND system components, people, and processes that ***could impact the security of the CDE****."*[1]

**CHD – Cardholder Data*
SAD – Sensitive Authentication Data (CVV, etc.)

Furthermore, the PCI Security Standards Council (SSC) Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation published in May 2017 clarifies that the CDE also extends to systems on the same network segment as systems that store, process, or transmit cardholder data.

Additionally, the PCI DSS explains, "Without adequate segmentation (sometimes called a "flat network"), the entire network is in scope for the PCI DSS assessment."[2] The detrimental impact is obvious: you quickly find yourself required to secure systems to PCI DSS requirements that have nothing to do with your acceptance of payments or supporting payment transactions.

"To be considered out of scope for PCI DSS, a system component must be properly segmented (isolated) from the CDE, such that the out-of-scope system component could not impact the security of the CDE, even if that component was compromised."[3] To confirm effectiveness of segmentation (isolation), PCI DSS includes a requirement for penetration testing of segmentation (PCI DSS requirement 11.4.5 and 11.4.6).

Given this understanding of how scope can quickly encompass an entire organization, segmentation can be an effective means of reducing the scope, complexity, and cost of maintaining compliance. It is important to note that segmentation as a control is not explicitly required per the PCI DSS. It is, however, often the single most effective method outside of outsourcing or process re-engineering for reducing the scope of PCI DSS compliance obligations in an environment.

Achieving effective network segmentation can be a significant challenge. As noted in the May 2017 Guidance document, out-of-scope systems components must not:

- Be in the same network segment or subnet as systems that store, process, or transmit cardholder data;
- Connect to or access any system in the cardholder data environment;

[1] Payment Card Industry Data Security Standard, v4.0, Payment Card Industry Security Standards Council, March 2022, pg 9.

[2] Payment Card Industry Data Security Standard, v4.0, Payment Card Industry Security Standards Council, March 2022, pg 12.

[3] Payment Card Industry Data Security Standard, v4.0, Payment Card Industry Security Standards Council, March 2022, pg 12.

- Gain access to the cardholder data environment nor impact a security control for cardholder data environment via an in-scope system;
- Meet the criteria of a connected-to or security-impacting system.

The prospect of achieving segmentation that meets this criterion can be very difficult and expensive for both merchants and service providers. This often involves extensive network architecture changes, potential duplication of systems and/or services (in order to create isolation), and capital expenditures on networking infrastructure, etc.

ARUBA CX 10000 DISTRIBUTED SERVICES SWITCH OVERVIEW

The Aruba CX 10000 Distributed Services Switch leverages Aruba switch hardware combined with an AMD Pensando software stack to deliver firewall functionality on every port of the switch. This feature set enables organizations to segment and isolate individual systems without redesigning their network. Security scales organically at the leaf-switch port-level rather than unsustainably by routing traffic to discrete physical or virtual firewalls. Stateful firewall enforcement is enabled in the network fabric itself and scales with it.

The firewall policy management required for achieving all PCI compliance benefits of the solution is provided by another AMD Pensando component, the Policy and Services Manager (PSM). The PSM is deployed on-premises on a virtual machine and represents the management plane for AMD Pensando-enabled switches. The combination of Distributed Services Switches and the PSM introduces host-based segmentation, a commonly available cloud feature, into the on-premises environment without requiring the installation of agents or other host-based software. The solution also provides the flexibility of adding new physical hosts that will be subject to PCI DSS compliance, without significant network design implications or risk of undue expansion of the scope of the CDE. The Aruba CX 10000 is designed for East-West network segmentation and provides hardware based L3/L4 firewall functionality on each access port. The solution includes the following features that are important for support of PCI DSS compliance:

- Stateful inspection and implicit deny for all traffic not explicitly allowed
- Segmentation at the port or host level, reducing the cost and operational burden required to achieve and maintain PCI compliance, as well as validate compliance annually
- Logging of all traffic and device audit logs with ability to send logs to external SIEM, XDR, or other Machine Learning solutions for analysis and alerting
- Support for separate ingress and egress policy for each VLAN and each VRF, allowing for flexible and granular traffic filtering
- Support for TACACS and RADIUS integration via access controls for the Distributed Service Switches and the PSM, leveraging existing access control solutions and Single Sign-On (SSO) functionality
- An API enabling a broad ecosystem across the breadth of integrations with management and monitoring software
- Network Dependency Mapping, providing visibility into current traffic flow and facilitating identification of traffic requirements
- Support for descriptive naming of policies and rules within policies, groups of network ports required for various applications, as well as support for detailed descriptions for each rule within a policy. This feature not only provides for easier manageability but makes configurations easier to understand and review for compliance by PCI QSAs

PCI DATA SECURITY STANDARD 4.0 CONTROL MAPPING SUMMARY

Analysis of PCI DSS 4.0 requirements supported by the CX 10000 switch is summarized in this section. Organizations should consult with their QSA regarding applicability of the guidance presented in this document to the specifics of their environment.

The table below summarizes PCI requirements directly met or supported by the Aruba CX 10000.

PCI DSS Requirement	Met Directly	Supported
1. Install and Maintain Network Security Controls	1.3.1, 1.3.2, 1.3.3, 1.4.1, 1.4.2, 1.4.4	1.2.2, 1.2.3, 1.2.5, 1.2.6, 1.2.7, 1.2.8
2. Apply Secure Configurations to All System Components		2.2.4, 2.2.5, 2.2.7
6. Develop and Maintain Secure Systems and Software		6.5.3
10. Log and Monitor All Access to System Components and Cardholder Data		10.2.1, 10.7.2

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

AMD PENSANDO

Built on the same technology that the hyperscalers use, the heart of the AMD Pensando platform is our fully programmable P4 Data Processing Unit (DPU). Optimized to execute a software stack delivering cloud, compute, network, storage, and security services at cloud scale – with minimal latency, jitter, and power requirements.

The next evolution of switching architecture. The Aruba CX 10000 provides 800G of distributed stateful firewall for east-west traffic, zero trust segmentation, and pervasive telemetry.

BP_ArubaCX10000_RVK_120822

Contact us at www.arubanetworks.com/contact