cradlepoint

PCI Compliance

CradlePoint Enablers for PCI Compliant Systems

White Paper

September 8, 2011

Preface

Right of Revision

CradlePoint reserves the right to revise this publication and to make changes in the content thereof without obligation to notify any person or organization of any revisions or changes.

Revision Tracking

Revision	Date	Description	Author
1.0	Sep 8, 2011	Initial Release	Ken Hosac

Intellectual Property

Table of Contents

1. Overview

Business Driver

Point-of-Sale (POS) businesses are paranoid, with good reason, about protecting sensitive customer and company information. Financial institutions require that any company that stores, processes or transmits credit card information complies with the PCI-DSS (Payment Card Industry, Data Security Standards).

Companies that fail to comply are subject to fines, lawsuits, and can even be banned from processing credit cards. Even worse, companies that are breached can find themselves in the news headlines, significantly impacting goodwill with customers, partners and shareholders.

Summary

When properly configured, monitored and maintained, CradlePoint devices meet the requirements of PCI-DSS 2.0. Enabling features include network segmentation (ethernet ports, SSIDs and VLANs), stateful firewall, MAC/IP/URL filtering, authentication/encryption, event logging, event alerts, time synchronization, and configuration/upgrade management from WiPipe Central.

Objective of this Document

CradlePoint specializes in network connectivity solutions for the Retail Point-of-Sale market. Our products are deployed broadly in several Retail POS segments that process credit card transactions, including:

- Retail Stores
- Restaurants & Bars
- Convenience Stores
- Coffee Shops
- Kiosks
- ATMs
- Service Locations
- Entertainment & Recreational Venues
- Special Events
- Temporary Vending Locations

The objective of this White Paper is to help our customers better understand how to create and maintain a PCI Compliant network using CradlePoint devices for network connectivity.

2. PCI Security Standards

Overview

The objective of the Payment Card Industry (PCI) Security Standards is to protect cardholder data. The standards are developed and published by the PCI Security Standards Council (SSC), which consists of hundreds of industry participants who have a vested interested in reducing vulnerabilities in the card-processing ecosystem.

The PCI-SSC was founded by the following five global payment brands:

- American Express
- Discovery Financial Services
- JCB International
- MasterCard Worldwide
- Visa, Inc.

Scope

The PCI SSC publishes the following standards:

- **PCI Data Security Standards (DSS):** Applies to any entity that stores, processes, and/or transmits cardholder data. The standard covers technical and operational components include in or connected to cardholder data. If a business accepts or processes payment cards, it must comply with the PCI DSS.
- **PIN Transaction Security Requirements (PTS):** Applies to manufacturers who develop PIN (personal identification number) entry terminals used for payment card financial transactions.
- **Payment Application Data Security Standards (PA-DSS):** Applies to software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement.

Compliance

Merchants who process credit card transactions are responsible for complying with the PCI-DSS. "PCI Compliance" is achieved when the merchant successfully demonstrates (via external audits or self-certification) that their entire system and process complies with the 12 requirements of the PCI-DSS.

2. PCI Security Standards (continued)

Requirements

Version 2.0 of the PCI-DSS was released in October, 2010. The PCI-DSS provides a baseline of technical and operational requirements designed to protect cardholder data. The PCI-DSS is organized around the following high-level goals and requirements:

Goals	Requirements
Build and Maintain a Secure Network	1) Install and maintain a firewall configuration to protect cardholder data. 2) Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3) Protect stored cardholder data. 4) Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5) Use and regularly update anti-virus software or programs. 6) Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7) Restrict access to cardholder data by business need to know. 8) Assign a unique ID to each person with computer access. 9) Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10) Track and monitor all access to network resources and cardholder data. 11) Regularly test security systems and processes.
Maintain an Information Security Policy	12) Maintain a policy that addresses information security for all personnel.

Certification

While the standards are driven by the PCI SSC, each payment card financial institution has its own program for compliance. In general, compliance can be certified by the merchant through a Self-Assessment Questionnaire (SAQ) or through a Qualified Assessor such as a QSA (Qualified Security Assessor) or ASV (Approved Scanning Vendor).

It is the merchant's responsibility to work with their payment card financial institution to determine what form of certification is required.

3. CradlePoint Recommendations for PCI Compliance

Overview

The PCI SSC does not publish any certification standards for network equipment other than PIN entry terminals. As a result, there is no such thing as a "PCI Compliant Router".

To become "PCI Compliant", the merchant must verify that their entire system (POS devices, network devices, servers, applications, policies, and procedures) complies with the PCI-DSS 2.0. As part of that overall effort, the merchant must verify that their network equipment (including CradlePoint devices) is properly configured and managed to ensure overall compliance with the PCI-DSS.

CradlePoint cannot control how an end user configures and manages a CradlePoint router. Similarly, CradlePoint does not have any control over the other devices, servers and applications that comprise an end-to-end card payment system. As such, PCI compliance can only be obtained by the merchant in the context of their entire system. The merchant is also responsible for obtaining certification of their end-to-end system from a QSA (Qualified Security Assessor) or ASV (Approved Scanning Vendor).

CradlePoint devices are utilized in several PCI-compliant systems. This section provides a summary of CradlePoint features and capabilities that have been used by other customers to help achieve PCI Compliance for their end-to-end systems.

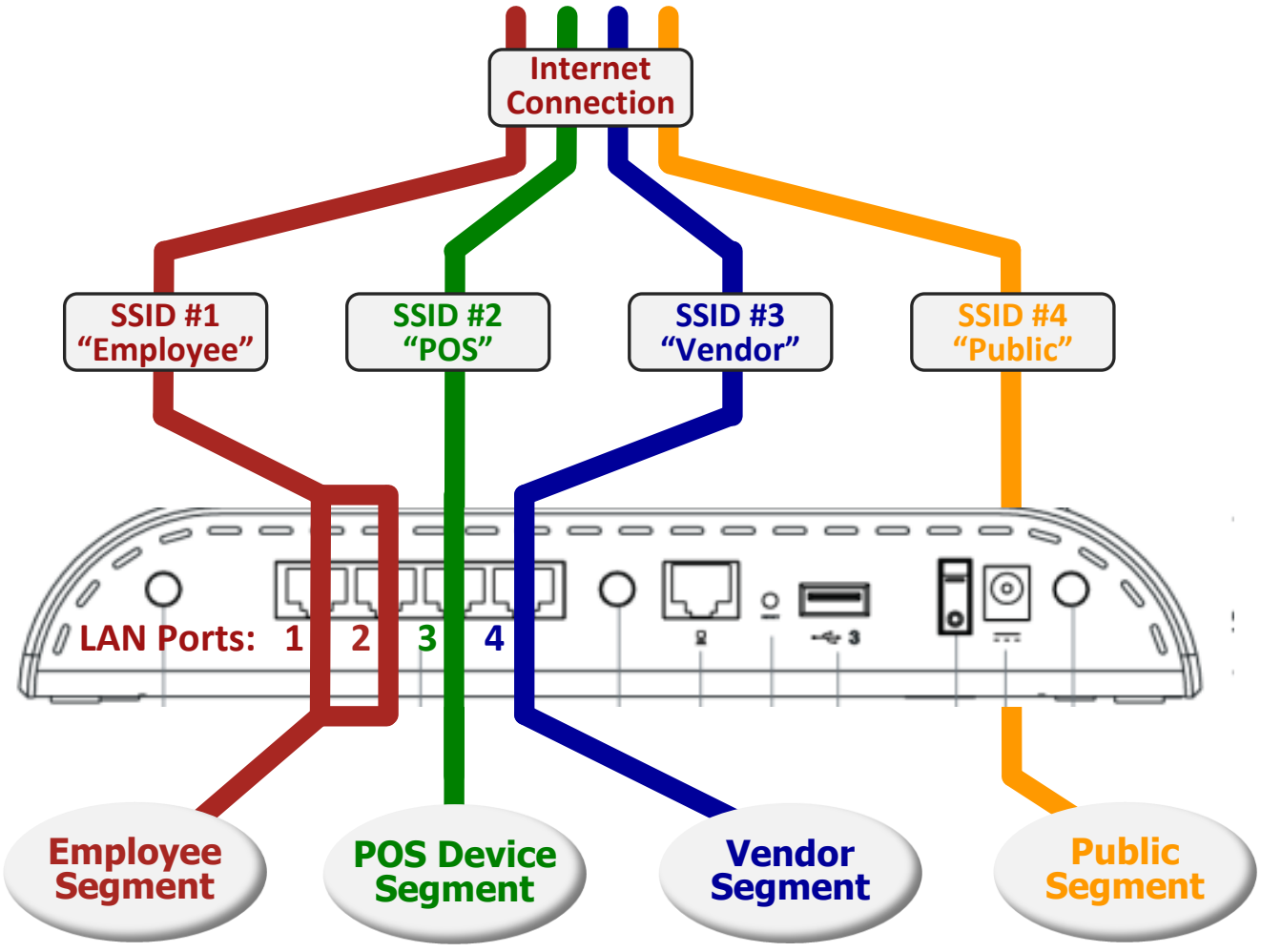
3. CradlePoint Recommendations for PCI Compliance (continued)

Reference Implementation

The following reference implementation represents a reasonably complex topology that includes:

- Ethernet access for POS devices
- Ethernet and WiFi access for employee computers and printers
- Ethernet and WiFi access for 3rd-party vendor
- WiFi access for customers.

We recognize that Retail POS enterprises may only implement certain subsets of this topology. However, the more complete topology is shown to highlight the capabilities provide by CradlePoint to address a wide range of target applications while maintaining PCI Compliance.



3. CradlePoint Recommendations for PCI Compliance (continued)

Recommendations

Step 1: Upgrade the router with the latest firmware

Step 2: Change the default passwords

Step 3: Lock down the router entry points

Step 4: Configure the firewall

Step 5: Segment the network into individual “security zones”

Step 6: Create secure WAN connectivity

Step 7: Configure communication with an external SysLog server

Step 8: Configure communication with an external Time server

Step 9: Lock down the configuration with WiPipe Central

Step 10: Monitor device usage with WiPipe Central

Step 11: Keep device firmware updated with WiPipe Central

3. CradlePoint Recommendations for PCI Compliance (continued)

Key Features

The following describes several of the CradlePoint features and capabilities that are pertinent to PCI Compliance:

- Network Segmentation (Ethernet, SSID and VLAN)
- Ethernet ports (4) that can be individually assigned to specific segments
- WiFi SSIDs (4) that can be individually secured and assigned to specific segments
- Virtual LAN support and tagging (VLAN)
- Stateful Packet Inspection (SPI)
- Network Address Translation (NAT)
- Application Level Gateways (ALG)
- Inbound filtering of IP addresses
- De-Militarized Zone (DMZ)
- Virtual Server
- Ability to disable WAN services (ping, WNMP, web-based mgmt, etc)
- MAC filtering
- Session filtering (non-UDP/TCP/ICMP)
- Layer 2 Tunneling Protocol (L2TP)
- VPN Client with support for up to 20 tunnels (product-specific)
- IPSec
- GRE
- WiFi security (WPA/WPA2 Personal/Enterprise, AES/TKIP)
- RADIUS user authentication on WiFi
- SysLog support
- Alerting
- WiPipe Central managed service – to manage configuration, firmware updates and monitor usage.

Additional Information

For additional information about how CradlePoint can help enable PCI-Compliant card payment systems, please contact CradlePoint directly. Our Professional Services organization can provide consulting services and best practices that can help guide you towards PCI Compliance.