Preface

The Payment Card Industry (PCI) Data Security Standard (DSS) version 1.2 was released October 2008. This document addresses the updated standard and reflects the removal of specified compensating controls. The document was successfully validated by the QSA auditor on January 27, 2009. The Cisco Secure Store PCI Retail Solution roadmap continues to evolve to address the evolving standard, market changes and ongoing threats to data security to protect sensitive financial information based on compliance and security best practices.

To validate specific Cisco networking products for the Cisco PCI Solution for Retail, a lab environment was built using Cisco Connected Retail architectures. Assessment was made by a Payment Card Industry (PCI) Qualified Security Assessor (QSA). The initial range of products (router, switch, wireless, and associated management tools as specified by the Solution Development team) was scoped to address specific PCI Data Security Specification (DSS) Version 1.2 sub-requirements and was successfully validated by the QSA auditor.

Document Purpose

This document describes the required design and configuration details that address PCI requirements and provide the foundation for Cisco Connected Retail design principles. This document is intended to augment the *Cisco Enterprise Branch Security Design Guide* available at http://www.cisco.com/go/designzone and does not replace that document.

Intended Audience

This document is intended for Cisco system engineers, solution engineers, and partner engineers who are planning to build a retail store network that addresses PCI DSS 1.2 requirements.

About the Cisco PCI Retail Solution

The Cisco PCI Solution for Retail consists of many Cisco components that work together to provide a comprehensive solution that addresses many of the requirements in the *PCI 1.2 Data Security Standards* document. The solution supplies the configurations that are optimized to help a retailer address many of the elements included in a PCI audit.

Every Cisco solution component authenticates against the Active Directory via Cisco Secure Access Control System (CS-ACS). One servers is an exceptions to this, and the solution addressed this by implementing compensating controls by putting each server on to its own network segment behind a firewall.

Cisco continues to demonstrate its commitment to retailers helping companies simplify the PCI audit process by adding features to its product line to remove the need for the following compensating controls:

- Wireless Control System (WCS)—In Release 4.1, Cisco added TACACS+ and RADIUS authentication.