



PCI Solution for Retail 2.0 Design and Implementation Guide

February 8, 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-13453-01

IMPORTANT !

THE CONTENTS OF THIS DESIGN AND IMPLEMENTATION GUIDE ARE PROVIDED "AS IS," WITHOUT WARRANTY OR REPRESENTATION OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

PCI COMPLIANCE REQUIRES TRAINING, SERVICES, POLICIES AND OTHER FACTORS OUTSIDE OF CISCO CONTROL. PCI COMPLIANCE MAY ALSO REQUIRE THE GOODS OR SERVICES OF THIRD PARTIES. CISCO CANNOT GUARANTEE OR ENSURE PCI COMPLIANCE FOR ANY CUSTOMER.

THIS DESIGN AND IMPLEMENTATION GUIDE DOES NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING ANY DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

FOR MORE INFORMATION, PLEASE CONSULT WITH A PCI QUALIFIED SECURITY ASSESSOR. A LIST OF ASSESSORS AND MORE INFORMATION ABOUT THE PCI DATA SECURITY STANDARD, CAN BE FOUND AT: [HTTP://WWW.PCISECURITYSTANDARD.ORG](http://www.pcisecuritystandard.org) OR VISIT CISCO RETAIL AT [WWW.CISCO.COM/GO/RETAIL](http://www.cisco.com/go/retail)

THE DESIGNS, SPECIFICATIONS AND INFORMATION IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)



CONTENTS

Preface i-xi

Document Purpose	i-xi
Intended Audience	i-xi
About the PCI Retail Solution	i-xi

CHAPTER 1

Solution Overview 1-1

Executive Summary	1-1
Solution Justification	1-2
Target Market	1-2
Applications and Services Supported by the Solution	1-3
Solution Benefits	1-3
Solution Features and Component Highlights	1-4
Network Systems	1-4
Hosts and Servers	1-5
Monitoring and Management	1-5
Encryption	1-6
Data at Rest Encryption	1-6
Data in Motion Encryption	1-6
Authentication	1-7
Policy	1-7
Other Applications and Services	1-7
Scope of the Solution	1-9
Architecture	1-9
PCI Compliance	1-9
Solution Results	1-10

CHAPTER 2

Solution Architecture 2-1

Applications and Partner Services	2-2
Application Networking Services	2-2
Infrastructure Services	2-2
Network Systems Layer	2-3
Retail Store Network Designs	2-4

- Small Store 2-4
 - Primary Design Requirements 2-4
 - Overview and Description 2-5
 - Advantages 2-6
 - Limitations 2-6
- Medium Store 2-6
 - Primary Design Requirements 2-6
 - Overview and Description 2-7
 - Advantages 2-8
 - Limitations 2-8
- Large Store 2-8
 - Primary Design Requirements 2-8
 - Overview and Description 2-9
 - Advantages 2-10
 - Limitations 2-10
- Data Center 2-11
 - Primary Design Requirements 2-11
 - Overview and Description 2-12
 - WAN Aggregation 2-12
 - Core 2-13
 - Services (Edge) Aggregation 2-14
 - Server Access Layer 2-16
 - Storage 2-16
 - Advantages 2-17
 - Limitations 2-17
 - Internet Edge 2-18
 - Primary Design Requirements 2-19
 - Overview and Description 2-19

CHAPTER 3

Solution Components—Best Practices and PCI 3-1

- Network Systems 3-2
 - Cisco Integrated Services Router 3-2
 - General Notes/Best Practices 3-2
 - PCI Sub-Requirements Satisfied by Solution Component (Router) 3-3
 - PCI Sub-Requirements that Require Compensating Controls (Router) 3-10
 - Mid-Range Routers (WAN Aggregation)/Edge Routers (Internet Edge) 3-10
 - General Notes/Best Practices 3-10
 - Cisco Catalyst Ethernet Switch and Network Switch Module 3-15
 - General Notes/Best Practices 3-15

PCI Sub-Requirements Satisfied by Solution Component (Switches)	3-15
PCI Sub-Requirements that Require Compensating Controls (Switches)	3-18
Cisco Firewall Services Module (FWSM)	3-18
General Notes/Best Practices	3-18
PCI Sub-Requirements Satisfied by Solution Component (Cisco FWSM)	3-19
PCI Sub-Requirements that Require Compensating Controls (FWSM)	3-23
Cisco Intrusion Detection System Services Module (IDSM2)	3-24
General Notes/Best Practices	3-24
PCI Sub-Requirements Satisfied by Solution Component (Cisco IDSM2)	3-24
PCI Sub-Requirements that Require Compensating Controls (Cisco IDSM2)	3-26
Cisco Application Control Engine (ACE) Module	3-26
PCI Sub-Requirements Satisfied by Solution Component (ACE)	3-27
Application Control Engine (ACE) XML Gateway	3-29
General Notes/Best Practices	3-29
PCI Sub-Requirements Satisfied by Solution Component (Cisco ACE XML Gateway)	3-30
Wireless Access Points and Controllers	3-32
General Notes/ Best Practices	3-32
PCI Sub-Requirements Satisfied by Solution Component (Unified Wireless: Wireless Access Points, Wireless Controller and Wireless Control System)	3-32
PCI Sub-Requirements that Require Compensating Controls (Wireless Control System)	3-38
PCI Sub-Requirements that Require Compensating Controls (Wireless Controllers)	3-39
Adaptive Security Appliance (ASA)	3-39
General Notes/Best Practices	3-39
PCI Sub-Requirements Satisfied by Solution Component (Adaptive Security Appliance)	3-40
VPN Tunnel Configuration on Adaptive Security Appliance (ASA) for Remote Access with Two-Factor RSA SecurID Authentication	3-53
System Management	3-53
CiscoWorks LAN Management System	3-53
General Notes/Best Practices	3-53
PCI Sub-Requirements Satisfied by Solution Component (C-LMS)	3-56
PCI Sub-Requirements that Require Compensating Controls (C-LMS)	3-60
Cisco Security Manager	3-61
General Notes/Best Practices	3-61
PCI Sub-Requirements Satisfied by Solution Component (CS-M)	3-61
PCI Sub-Requirements that Require Compensating Controls (CS-M)	3-63
CSA Manager	3-64
General Notes/Best Practices	3-64
PCI Sub-Requirements Satisfied by Solution Component (CSA Manager)	3-64
PCI Sub-Requirements that Require Compensating Controls (CSA Manager)	3-68
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	3-69

General Notes/Best Practices	3-69
PCI Sub-Requirements Satisfied by Solution Component (CS-MARS)	3-69
PCI Sub-Requirements that Require Compensating Controls (CS-MARS)	3-72
CiscoSecure Access Control Server (CS-ACS)	3-73
General Notes/Best Practices	3-73
PCI Sub-Requirements Satisfied by Solution Component (CS-ACS)	3-73
PCI Sub-Requirements that Require Compensating Controls (CS-ACS)	3-75
PCI Sub-Requirements that Require Compensating Controls (RSA enVision)	3-76
Compliance Management	3-76
CiscoWorks Network Compliance Manager (C-NCM)	3-76
General Notes/Best Practices	3-76
Clients and Servers	3-80
Point-of-Sale (POS)	3-80
General Notes/Best Practices	3-80
Servers	3-81
General Notes/Best Practices	3-81
PCI Sub-Requirements Satisfied by Solution Component (NCR POS Systems)	3-81
Wired and Wireless Clients	3-84
General Notes/Best Practices	3-84
Encryption and Key Management	3-84
RSA Key Manager	3-84
General Notes/Best Practices	3-84
PCI Sub-Requirements Satisfied by Solution Component (RSA Key Manager)	3-86
PCI Sub-Requirements that Require Compensating Controls (RSA key Manager)	3-88
RSA Access Manager	3-88
General Notes/Best Practices	3-88
PCI Sub-Requirements Satisfied by Solution Component (RSA Access Manager)	3-88
PCI Sub-Requirements that Require Compensating Controls (RSA Access Manager)	3-90
RSA File Security Manager	3-90
General Notes/Best Practices	3-90
PCI Sub-Requirements Satisfied by Solution Component (RSA File Security Manager)	3-90
PCI Sub-Requirements that Require Compensating Controls (RSA File Security Manager)	3-91
RSA® Authentication Manager, RSA SecurID® and RSA enVision	3-92
General Notes/Best Practices	3-92
PCI Sub-Requirements Satisfied by Solution Component (RSA Authentication Manager, RSA SecurID and RSA enVision)	3-92
PCI Sub-Requirements that Require Compensating Controls	3-93
Solution Component Summary	3-94

CHAPTER 4**Implementing and Configuring the Solution 4-1**

Implementation	4-1
Overview	4-1
Network Topology	4-2
What was Implemented	4-4
What Was Not Implemented	4-13
Audit Findings	4-13
Testing	4-14
Functional Testing	4-14
PCI Audit Testing	4-14
Configuration Tasks	4-14
Routing and Switching	4-14
Unified Wireless	4-15
Adaptive Security Appliance	4-16
Storage Area Networks	4-18
Management	4-19
CiscoWorks LAN Management System (C-LMS)	4-19
Cisco Security Manager (CS-M)	4-20
Cisco Security Agent (CSA)	4-20
Data Center Services	4-21
CiscoSecure CS-MARS Event Monitoring and Alerting	4-21
CiscoSecure Access Control Server (CS-ACS) Authentication	4-21
CiscoWorks Network Compliance Manager (C-NCM)	4-22
Internet Edge	4-22
Cisco Firewall Service Module (FWSM)	4-22
Cisco Intrusion Detection System Services Module (IDSM2)	4-23
Cisco ACE XML Gateway	4-23
Additional Elements	4-24
Application Servers Point-of-Sale (POS)	4-25
NCR	4-25
MS-RMS	4-29
Wincor-Nixdorf	4-29
Microsoft Windows Servers	4-30
Payment Devices	4-32
Mx Series	4-32
Vx Series	4-33
Encryption and Key Management	4-33
RSA Key Manager	4-33
RSA Access Manager	4-38

RSA File Security Manager 4-39
 Remote Access 4-40
 Troubleshooting Configuration 4-41
 Results and Conclusions 4-41

APPENDIX A Bill Of Materials of Devices for Branch Stores A-1

Small Store A-1
 Medium Store A-2
 Large Store A-2
 Partner A-4

APPENDIX B Data Center/Internet Edge Components and Versions B-1

APPENDIX C Application Protocols C-1

APPENDIX D Detailed Implementation and Configuration Steps D-1

Wireless Configuration D-1
 Small Store (HREAP + Controller Architecture) D-1
 Medium Store (Controller-Based) D-2
 Large Store (Controller-Based) D-2
 Section 2.1 of PCI Requirements D-2
 PCI Section 2.3 D-3
 PCI Section 4.1.1 D-4
 PCI Section 9.1.3 D-5
 PCI Section 10.4 D-5
 PCI Section 10.5.4 D-5
 PCI Section 11 D-7
 Point-of-Sale Application Systems D-7
 Wincor-Nixdorf TP.net and PCI D-7
 Cisco Secure Access Control Server D-8
 Cisco Security Manager D-18
 Firewall Use Methodology D-18
 Global CS-M Access Policy (Mandatory) D-19
 Store Policy (Mandatory) D-20
 Store Policy (Default) D-22
 Data Center WAN Access Policy (Mandatory) D-23
 CSA Manager D-23
 Cisco Security Agent (CSA) Custom Policy for RSA Products D-30

Cisco Security Agent (CSA) Custom Policy for NCR	D-34
RSA Key Manager	D-39
RSA Key Manager Administration Console	D-39
Starting and Stopping the Key Manager Server	D-39
RSA Key Manager Server and Client Deployment	D-40
RSA Key Manager Logging	D-42
RSA File Security Manager	D-44
Detailed System Architecture	D-44
Detailed Configuration Steps	D-46
PCI Section 6.5	D-49
Open Web Application Security Project (OWASP)	D-50
PCI 6.5.4 Cross-Site Scripting (XSS) Attacks	D-50
Cisco ACE XML Gateway Blocking XSS Attack	D-51

APPENDIX E**Device Configurations E-1**

Branch Configurations	E-2
Large Store Router #1	E-2
Large Store Router #2	E-15
Medium Store Router #1	E-28
Medium Store Router #2	E-41
Small Store Router #1	E-52
Data Center WAN Router #1	E-65
Data Center WAN Router #2	E-70
Large Store Switch #1	E-76
Large Store Switch #2	E-83
Large Store Switch #3	E-90
Large Store Switch #4	E-96
Medium Store Switch #1	E-103
Medium Store Switch #2	E-109
Large Store Wireless Controller	E-115
Medium Store Wireless Controller	E-132
Small Store Wireless controller in the Data Center	E-147
Large Store Access Point	E-162
Medium Store Access Point	E-163
Small Store Access Point	E-164
Internet Edge Configurations	E-165
Cisco Firewall Service Module	E-165
Cisco Catalyst 3750	E-171
Cisco Catalyst 6500	E-176

Cisco 7200 Edge Router E-186
Cisco Application Control Engine E-192
Data Center Configurations E-195
Cisco Catalyst 3750 E-195
Cisco Catalyst 6500 E-198
Cisco 7206 VXR Router E-200
Cisco Adaptive Security Appliance E-205

APPENDIX F

Report on Compliance (ROC) F-1

GLOSSARY



Preface

To validate specific Cisco networking products for the Cisco PCI Solution for Retail, a lab environment was built using the Cisco Intelligent Retail Network (IRN) 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 1.1 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 IRN design principles. This document is intended to augment the *Cisco Enterprise Branch Security Design Guide* available at <http://www.cisco.com/go/srnd> 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 1.1 requirements.

About the PCI Retail Solution

The 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 1.1 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 solution component authenticates against the Active Directory via Cisco Secure Access Control System (CS-ACS). Four servers are exceptions to this, and the solution addressed them by implementing compensating controls by putting each server on to its own network segment behind a firewall.

Cisco continues to demonstrate its commitment to helping retailers 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.

- Cisco Security Monitoring, Analysis, and Response System (CS-MARS)—Cisco added RADIUS authentication to v 4.3.
- Cisco Security Access Control System (ACS)—Cisco plans to add RADIUS authentication. This feature is scheduled to be available May 2008.
- Cisco Security Agent Manager Server—This server did not require compensating controls because it was able to externally authenticate to Active Directory directly.



CHAPTER 1

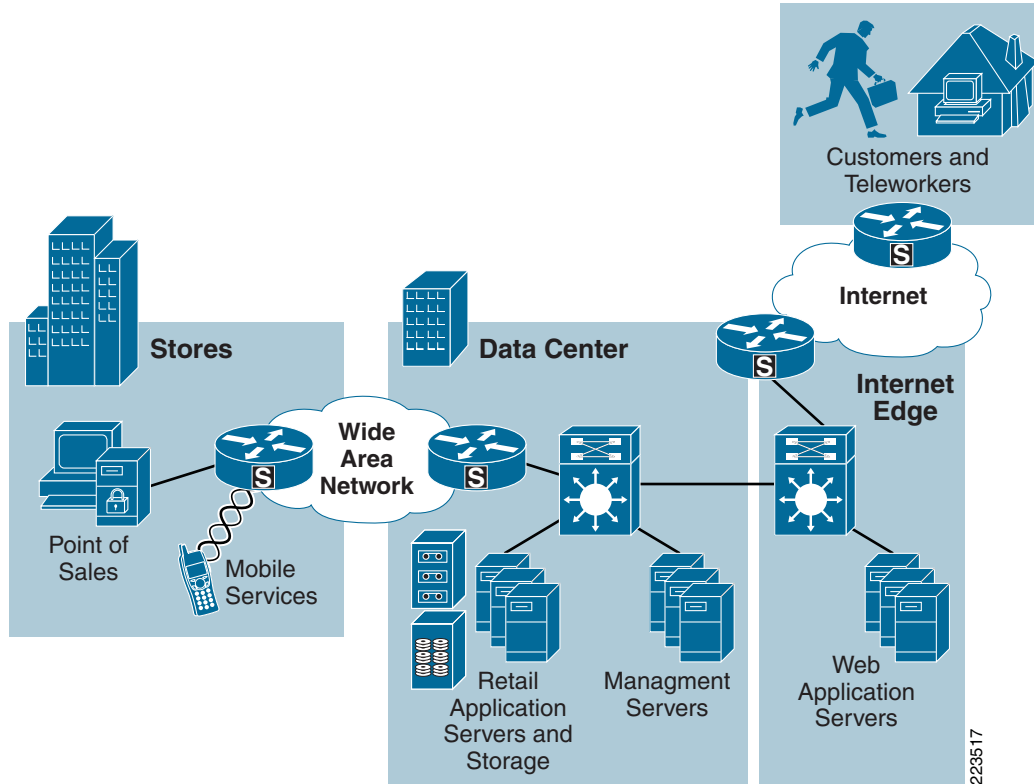
Solution Overview

Executive Summary

The PCI Solution for Retail is a set of configurations and recommendations for data at rest and data in motion on wired and wireless networks. The solution is designed to conform to the Payment Card Industry (PCI) Data Security Specification (DSS) 1.1. The solution was built and tested using point-of-sale (POS) systems, payment devices, wireless client devices, data encryption software, Cisco network infrastructure, and validated by a PCI Qualified Security Assessor (QSA) audit partner. The result is a set retail store, data center and Internet edge designs that simplify the process of a retailer becoming PCI compliant.

To pass PCI compliance, a retail company must address its procedures, security policies, and technical infrastructure so that it can demonstrate adherence to the PCI v1.1 specification sub-requirements. A QSA must perform an audit of the company to verify that each applicable sub-requirement is either addressed or deemed not applicable to that specific company. Once a company becomes compliant, there are ongoing requirements to maintain compliance. The PCI solution for Retail demonstrates how to build the infrastructure, secure data in transit and at rest, and how to monitor and maintain the configurations. [Figure 1-1](#) show the PCI for Retail solution conceptual architecture.

Figure 1-1 PCI Solution for Retail 2.0 Conceptual Architecture



Solution Justification

The PCI DSS version 1.1 affects all retailers that process, store, or transmit credit or debit card information over their networks. Cisco customers have asked for a comprehensive recommendation on how to design, manage, monitor, and remediate a store network that has been audited and meets QSA audit guidelines.

Target Market

Retailers globally who process payment transactions are required to meet PCI DSS guidelines. Typical mid-market and enterprise retailers process 100,000 or more payment card transactions per year and are therefore part of the target market. By modeling retail store networks, data center and the Internet edge infrastructures, the solution is adaptable to many different retail deployments. [Table 1-1](#) lists and describes the different PCI merchant levels (source Visa USA).

Table 1-1 PCI Merchant Levels

Merchant Level	Description
1	<ul style="list-style-type: none"> Any merchant, regardless of acceptance channel, processing over 6,000,000 VISA transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant that VISA, at its sole discretion, determines should meet the level 1 merchant requirements to minimize risk to the VISA system. Any merchant identified by any other payment card brand as level 1.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 VISA transactions per year.
3	Any merchant processing 20,000 to 1,000,000 VISA e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 VISA e-commerce transactions per year, and all other merchants, regardless of acceptance channel, processing up to 1,000,000 VISA transactions per year.

Applications and Services Supported by the Solution

The primary applications that are supported by the PCI Solution for Retail include:

- Highly secure transport of payment card information across the wired and wireless network.
- Highly secure storage of data at rest, at the electronic cash register, on an in-store server, or in the data center.
- The solution includes network and systems management, monitoring and remediation services.

Solution Benefits

The solution demonstrates how to create retail networks that conform to PCI DSS 1.1 guidelines. Customers can simplify the process of becoming PCI compliant by building a similar network with the recommended configurations and best practices.

In addition, the solution provides the following benefits:

- Insight into the Cisco Intelligent Retail Network architecture based on global best practices
- A scalable set of reference designs that can be used as a reference during the PCI compliance process.
- A detailed analysis and mapping of Cisco, and partner components and their relationship with PCI DSS sub-requirements.
- Insight into compensating controls and best practices to harden retail network and data systems.
- A centralized management "tool kit" that provides operational efficiency compared to managing the distributed endpoints individually.

- Insight into the PCI audit process by providing a lab model and associated Report on Compliance (ROC) from Verizon Business (QSA).

Solution Features and Component Highlights

The solution features and components consists of the following:

- [Network Systems](#)
- [Hosts and Servers](#)
- [Monitoring and Management](#)
- [Encryption](#)
- [Authentication](#)
- [Policy](#)
- [Other Applications and Services](#)

Network Systems

- **Routing**—Cisco Integrated Services Router (ISR), mid-range routers and Catalyst 6500 Supervisor's provide routing services across the architecture. Each retail store uses either a single or pair of ISRs to consolidate WAN services, routing, identity, and security services into a single platform with local and centralized management services. The same platform can also serve as the hub for network quality-of-service (QoS), voice call control, and other application services. The WAN aggregation and Internet Edge routers are Cisco 7206VXR routers that support a wide variety of WAN interfaces and allow specific types of traffic into the data center.
- **Switching**—Cisco Catalyst Ethernet switches connect the IP endpoints to the routed services. Catalyst switches support LAN speeds from 10Mbps to 10Gbps. They can also integrate Power over Ethernet (PoE) services over the same cable to power wireless access points, IP telephones, and other 802.3AF-based devices. Catalyst switches use VLANs, access control and quality-of-service to segments LAN traffic based on security or business requirements.
- **Wireless**—Cisco Unified Wireless network provides centrally managed wireless connectivity to mobile computers and phones. The same wireless infrastructure includes integrated wireless intrusion detection, highly secure connectivity, and central management through the Wireless Control System (WCS). Each retail store network shares the same dual-radio infrastructure design regardless of the size of the store. This permits adequate network capacity for high-bandwidth retail applications such as streaming media to mobile kiosks or digital signs. It also provides adequate path isolation and segmentation to ensure that payment data is separately encrypted from the other types of retail business data. The Unified Wireless network can operate as distributed access points with local management, or as a centrally managed wireless-controller-based system.

Specific Cisco Unified Wireless network systems used in this solution include:

- Cisco 1100-series and 1200-series access points simultaneously support 2.4Ghz and 5Ghz 802.11 network connectivity, advanced security services, and central management control.
- Cisco Unified Wireless Controllers include the Wireless LAN Control Module for the ISR platform and the 4000 Series controller used in the large store. The small store features the Hybrid-Remote-Edge-Access-Point (H-REAP) protocol with centralized controller modules. This design supports local authentication in the event that the store loses connection to the central controller.

- Services Aggregation
 - Cisco Catalyst 6500's provide the high-performance, highly scalable and highly available platform to transport payment traffic from the Store-WAN routers, across the core switches and down to the Server Access Layer.
 - Firewall Services Modules (FWSM) are used to allow or block traffic, based on a central policy.
 - Intrusion Detection Module 2 (IDS2) is used to monitor and enforce policy sent from central management system. Cisco Application Control Engines filter content and balance traffic loads based on central policy.
 - Wireless controllers, part of the Cisco Unified Wireless architecture, centralize the control and management of wireless infrastructure installed across the network.
 - These systems work together to segment payment and POS transaction log traffic based on central policy.
 - Cisco Adaptive Security Appliances can also be used to deliver Firewall, IDS, and VPN services.
- Storage—Electronic cash registers, POS servers, and other PCs are used to recreate a typical retail environment. Storage Area Network director class switches connected to EMC storage disks recreate a typical data center storage environment. Other servers and hosts connected to the inside of the Internet edge simulate web application servers.

Hosts and Servers

- Point-of-Sale—NCR POS terminals and SurePOS servers running the NCR Advanced Checkout System software were used to recreate a typical retail environment. Earlier version of the solution used IBM and Wincor-Nixdorf POS devices. These devices use a combination of RSA data security applications to encrypt access to critical payment or administrative data on the system. CSA delivers application firewall, file integrity, and host intrusion prevention services. It can be configured to specifically allow retail business application functions within each device, and greatly limits the requirements for anti-virus software at the retail store level. It can stop "day zero" attacks and be customized to meet the wide-ranging requirements of retail business computing at the cash register, desktop, kiosk, or server level.
- Payment Devices—VeriFone and IBM payment devices were used to simulate a retail payment environment. These devices must meet PCI Payment Encryption Device specifications to be used in the solution.
- Host and Server Security—CSA is a combination of software installed on the each Windows or Linux-based POS device in the store including payment devices, POS registers, and POS servers. CSA is also installed on each of the solution management servers in the data center. CSA can also be installed on store manager PCs and any other desktop or server installed at the retail location.
- Centralized Cisco management services manage, monitor, provision, analyze, remediate, and report on all elements of the distributed system. These services can also create reports for audit and forensic requirements.

Monitoring and Management

The suite of Cisco management applications used in this solution includes:

- Cisco Security Manager (CS-M)—The operational control platform for the security services distributed across ISR routers and security appliances. It can design, provision, and report on firewall, IDS/IPS, and VPN services throughout the retail store networks.
- Cisco Security Monitoring, Analysis and Response System (CS-MARS)—Central log monitoring, correlation, and reporting platform for Cisco network device security alerts (e.g., ASA/FWSM/ISR firewall logs and IDS/IPS alerts) within the large, medium, and small retail environments, as well as the data center environment. In addition, Cisco Security Agent alerts are forwarded to CS-MARS.
- Cisco Security Agent Management Center (CSAMC)—The central management, provisioning, and reporting system for the CSA software installed on POS and store operation devices in each retail store network.
- Wireless Control System (WCS)—The central manager of the Unified Wireless network infrastructure and services installed in each retail store network.
- CiscoWorks LAN Management System (C-LMS)—Supports the central control and collection of running and startup configurations from a wide array of Cisco network devices. C-LMS uses Cisco Discovery Protocol, SNMPv3, and other management protocols to securely communicate from the data center to the retail store network.
- CiscoWorks Network Compliance Manager (C-NCM)—Tracks and regulates configuration and software changes throughout the network infrastructure. IT provides superior visibility into network changes and can track compliance based on PCI guidelines and company policy.

Encryption

Two forms of encryption are used to meet PCI guidelines: data at rest and data in motion.

Data at Rest Encryption

- RSA File Security Manager—File level encryption system used to encrypted sensitive data in the stores or data center.
- RSA Key Manager—Enterprise class key management system used to manage the secure delivery and use of encryption keys throughout the enterprise.
- RSA enVision—A log management and analysis application that is used to manage the RSA SecurID tokens that are part of the authentication component provided below.

Data in Motion Encryption

- Cisco Virtual Private Network (VPN) software—Used to encrypt payment data as it is transmitted across any public network segments. VPNs typically use IPsec with either 3DES (triple DES) or 256-bit AES encryption.
- Secure Socket Layer (SSL) services—Used to encrypt traffic from Internet-based web applications and when remotely administering infrastructure devices (SSHv2).
- Wi-Fi Protected Access version 2 (WPA2)—Used between wireless clients and Cisco access points uses AES encryption for POS and payment data transmitted across the in-store wireless LAN (WLAN).

Authentication

Accounting, Authorization and Authentication (AAA) services used to determine identity and authorize access to systems, devices or services within a components. Highlights of authentication:

- Cisco Secure Access Control Server (CS-ACS)—The central AAA service broker of the infrastructure and remote access elements of the solution CS-ACS is used to enforce the management and control policy for operational access to the network devices and services running on the network. CS-ACS provides access control for network, host, and servers used throughout the solution.
- RSA Access Manager—The access control system required for the RSA applications in the solution.
- RSA Authentication Manager software—Works with RSA Authentication Agents to enhance security with strong, two-factor user authentication provided by the time synchronous-based RSA SecurID tokens. This solution was required of remote users accessing retail applications or VPN-based connections to the Internet edge.

Policy

Two ways to look at policy within this solution include the management of policy and the creation of policy:

- Cisco Security Manager is the operational control platform for the security services distributed across Cisco routers and security appliances. It can design, provision, and report on firewall, IDS/IPS, and VPN services throughout the retail store networks.
- Cisco Security Agent (CSA) can also enforce host and server level policy by limiting access to specific files, folders, and services . CSA is managed through CSA management console which maintains the central policy and can quickly ensure that new devices meet a baseline-level of requirements through its behavioral approach threat deterrence.

Other Applications and Services

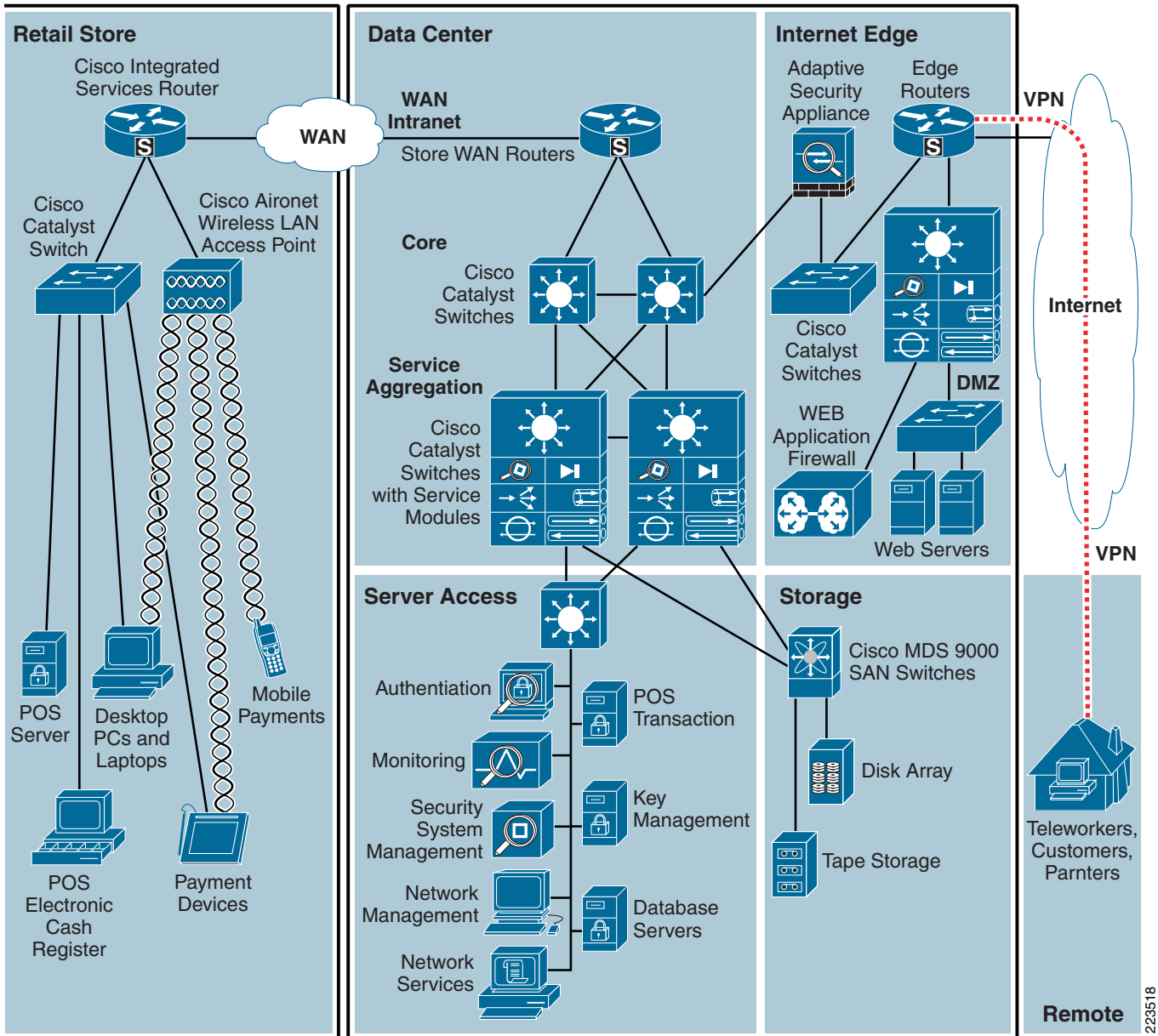
The following application services and partner products were required to create the operational environment and meet the PCI requirements but are not specifically part of the overall solution set:

- Microsoft Active Directory
- Microsoft DNS/DHCP server
- Microsoft Exchange server for alert notification services
- Microsoft Retail Management Server POS software
- Intermec wireless handhelds
- Network Time Protocol server for central time management
- Wincor-Nixdorf POS hardware
- IBM POS hardware

These are covered in more detail in [Chapter 4, “Implementing and Configuring the Solution,”](#) and the appendices.

Figure 1-2 shows a conceptual view of the PCI solution for Retail.

Figure 1-2 PCI Solution for Retail—Conceptual View



223518

Scope of the Solution

Architecture

Cisco and its solution partners have a wide range of products portfolio that could potentially be used to address the PCI specification. The products selected for this solution were chosen for their immediate relevance to a retail company network and data security environment, while allowing auditing and lab testing within the project timelines.

This solution guide includes store reference designs that connect to a central data center over a wide-area network. It also includes Internet edge reference designs that transport Internet-based users to the Extranet or De-Militarized Zone (DMZ). The solution includes and assumes centralized management, but does not include central connection to an actual retail payment or adjudication service.

This release of the PCI Solution for Retail can be used as a foundation to build upon additional products and location reference designs in the future. This solution includes the following:

- Reference store designs that connect to a central data center over a private wide-area network.
- Data center design and centralized management servers that assist a retailer in satisfying PCI requirements.
- An Internet edge design that connects Internet-based consumers, workers, and partners to data center or DMZ-based applications.

The solution does *not* include the following:

- Data center connections to the actual payment service provider, acquiring bank or other merchant services.
- Actual e-commerce architecture, systems and applications.

PCI Compliance

Most of the PCI standards (for example, PCI DSS 1.1, <https://www.pcisecuritystandards.org/index.htm>) are focused on policy and procedure within a retail company. However, specific sub-requirements of the PCI standard address technical infrastructure and its configuration. The PCI Solution for Retail provides Cisco networking equipment, partner software applications, reference architecture, and configurations to satisfy this technical infrastructure aspect of the PCI compliance process. Although this solution does provide related guidance to some of the policy-based sub-requirements, companies seeking to become PCI compliant should contact a security service provider for assistance with their security policy and company procedures.

The Cisco and partner products used in this solution successfully addressed the PCI specification within this specific set of configurations. Retail companies purchasing these products to address PCI should consult a QSA for their own particular environment because elements within it may differ from this solution.

Solution Results

These results are applicable to the specific solution that was created and audited in the Cisco lab. For detailed notes on each solution feature and the audit findings, strengths, and weaknesses, see [Chapter 3, “Solution Components—Best Practices and PCI.”](#) Specific implementation and configuration details are provide in [Chapter 4, “Implementing and Configuring the Solution.”](#) Finally, for a complete audit report by Cybertrust on this specific lab, see [Appendix F, “Report on Compliance \(ROC\).”](#)

[Table 1-2](#) summarizes the solution features per PCI requirement.

Table 1-2 *PCI Requirements Satisfied by PCI Solution for Retail*

Solution Feature	PCI Value
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	
Cisco Firewall Service Module (FWSM), Cisco Adaptive Security Appliance (ASA)	Network security (firewall segmentation/filtering), stateful filtering
CiscoWorks (LMS and NCM), C-SM	Configuration management/secure configurations
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	
ISRs, FWSM, ASA, switches, wireless devices, WCS, CS-ACS, CiscoWorks (LMS and NCM), Cisco Security Agent (CSA), CS-M	Vendor defaults changed
WCS/wireless controllers	Wireless security (WPA/WPA2, SSID broadcast disabled)
ISRs, FWSM, ASA, switches, wireless controllers (CSA Manager, CS-M, CiscoWorks (LMS))	Best practice security parameters enabled
ISRs, FWSM, ASA, switches, wireless controllers (CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS)	Non-console encrypted administrative access
Requirement 3: Protect stored cardholder data	
NCR Advanced Checkout Solution (NCR-ACS) software and terminals	Certified to PCI PIN entry device standard requirements
Verifone VX and MX payment devices	Certified to PCI PIN entry device standard requirements
RSA File Security Manager and Key Manager application	Encrypt access to secure data stored on POS devices and servers
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
Wireless controllers	WPA wireless security
ISRs, Cisco 7200VXR -series routers, ASA	Provide IPsec VPN encryption for data across the retailers' wide area network or Internet-based network circuits.
Requirement 5: Use and regularly update anti-virus software or programs	
CSA	Anti-virus protection, malware/spyware protection, alerting
Requirement 6: Develop and maintain secure systems and applications	
CiscoWorks (LMS and NCM), CS-M (Workflow mode)	Change control and enforcement of compliance configurations
Cisco ACE XML Gateway	Web application protection from OWASP attacks.
Requirement 7: Restrict access to cardholder data by business need-to-know basis	

Table 1-2 PCI Requirements Satisfied by PCI Solution for Retail (continued)

ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Least-privilege, role-based access
Requirement 8: Assign a unique ID to each person with computer access	
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Unique user IDs, authenticated access, encrypted passwords, no group/shared IDs/passwords
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Password strength requirements
ISRs, Cisco 7200VXR, FWSM, ASA, switches, wireless controllers, CSA Manager, CS-M, CiscoWorks (LMS), CS-MARS, CS-ACS, WCS, RSA applications and NCR-ACS	Account lockout requirements
Requirements 9: Restrict physical access to cardholder data	
No products were tested or audited for this requirement at this time.	See note below ¹
Requirement 10: Track and monitor all access to network resources and cardholder data	
ISRs, Cisco 7200VXR, switches, wireless devices, WCS, CS-ACS, CiscoWorks (LMS) CSA, RSA applications, NCR applications	Audit trails, time synchronization
NCR-ACS terminals, RSA File Security Manager, RSA Key Manager, Cisco CSA	Audit access to actual cardholder data and audit trail data
Ciscoworks (LMS and NCM)	Centrally archive audit log records
Requirement 11: Regularly test security systems and processes	
Wireless controllers	Rogue wireless AP/device detection
ISRs, ASA, IDSM2 (sensor), CS-M (policy, signature updates)	Network IDS
CSA	Host-based IDS
CSA	File integrity
Requirement 12: Maintain a policy that addresses information security for employees and contractors	
Verizon Business, Cisco Advanced Services	Creation and maintenance of security policy

1. Cisco video surveillance and monitoring systems can be implemented to meet this requirement, but this was out of scope of this phase's solution testing effort.



CHAPTER 2

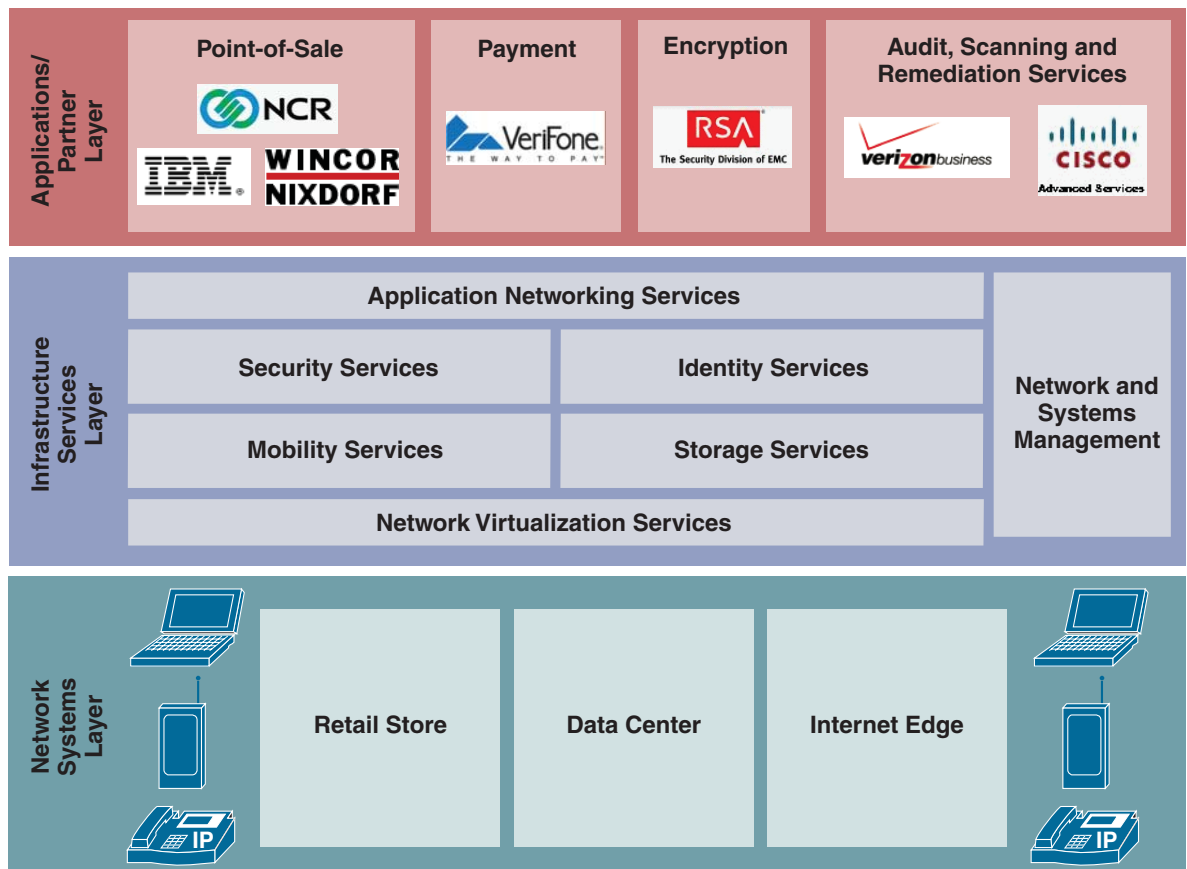
Solution Architecture

The architecture for the PCI Solution for Retail is based on Cisco's Intelligent Retail Network (IRN). IRN is a Service-Oriented Network Architecture (SONA). For more information on SONA and IRN, refer to the following URL:

<http://www.cisco.com/go/retail>

The Cisco IRN reference designs serve as the foundation of the network systems layer. These network designs exhibit best practices for small, medium, and large retail store networks as well as data center and Internet networks. (See [Figure 2-1](#).)

Figure 2-1 PCI Solution for Retail SONA Framework



223519

Applications and Partner Services

The top layer of the SONA framework includes the retail applications and services that are part of the PCI Solution for Retail. These include point-of-sale, payment, and encryption applications. Some of these applications use popular middleware services based on J2EE, .NET, or other systems. The IRN and the shared network services approach allow these various Service-Oriented Architecture (SOA) environments to share the same infrastructure services across multiple retail network topologies. Finally, the right side of the Application Layer includes the professional services that retailers must employ as part of the PCI process. Annual audits, network scans, and remediation services are necessary services that complete the PCI Solution for Retail framework.

Application Networking Services

Application services are the connection from the business applications to the shared services of the infrastructure services layer. This is where filtering, caching, load balancing and protocol optimization interact with applications or application middleware services to optimize the performance from the source of data to the end user.

Application delivery services in this solution include server load-balancing and content filtering features that Cisco IOS routers or Cisco Application Control Engines (ACEs) perform.

Infrastructure Services

Process control is simplified by using common infrastructure services for security, mobility and identity, and management. These are key advantages that aid in operational reporting and the policy requirements of achieving PCI compliance. Fewer services that are shared across more intelligent devices increases the operational efficiency of the whole system.

- **Security services** are used extensively in the PCI Solution for Retail architectures. These services are a combination of security features shared across multiple physical devices, central management in the data center, and virtual access to the security control plane from anywhere in the retail network.
- **Firewall services** are used in the ISR, Firewall Service Module (FWSM) and Adaptive Security Appliance (ASA) securing both application and interface services.
- **Intrusion Detection and Prevention systems (IDS/IPS)** are used across the Cisco ISR, ASA, Intrusion Detection System Services Module 2 (IDSM2), Unified Wireless Network (UWN), and Cisco Security Agent (CSA) at the point-of-sale (POS) host and server levels. The combination of these systems is centrally managed through the Cisco management applications in the data center. Again, distributed access to the IDS/IPS control plane of the system is available from anywhere on the retail network.
- **Monitoring, Analysis and Remediation data** is correlated by the centralized event correlation applications in the data center. The Cisco Security Monitoring, Analysis, and Response System (CS-MARS) not only does correlation and monitoring, but it can also remediate network attacks dynamically or through reactive alarm notifications. The CiscoWorks Network Compliance Manager (C-NCM) can enforce PCI policy on devices it monitors.
- **Mobility services** are another important area in the solution Retailers are demanding support for mobile POS and inventory applications operating on handheld computers or mobile POS kiosks. The Cisco UWN supports a very scalable set of wireless LAN (WLAN) systems ranging from single

access points to systems connecting thousands of access points as a single, centrally managed domain. The retail store networks use various WLAN systems, depending on the requirements of the store category.

- **Identity services** are used to help ensure that authenticated and authorized users are allowed access to retail network systems. The Cisco Secure Access Control Server (CS-ACS) provides the central management of the RADIUS and TACACS+ systems configured on each network device throughout the architecture. A central LDAP-based directory service enhances CS-ACS in helping it meet the requirements of PCI. The use of a distributed network time service helps to ensure consistent synchronization of network and application events, and allows better correlation of events.
- **Management Systems** are used across all the devices, applications, and services throughout the architecture. Network systems are managed with the LAN Management System (C-LMS) (configurations and administrative elements). The Cisco Security Manager (CS-M) manages the security elements of the devices so that a security department has independent control that is outside of the IT network systems team. The CiscoWorks Network Compliance Manager (C-NCM) can work with C-LMS to report on which devices are within compliance guidelines and which ones are not. For the ones that are not meeting guidelines, C-NCM can restore configurations and permit users to enforce configuration mandates.

Wireless systems are managed with the Cisco Wireless Control System (WCS). These systems include configurations, administrative elements, and security services.

RSA data security applications use specific management tools in this architecture. RSA file security manager manages file encryption services on hosts and servers with payment data. RSA enVision is used to monitor and log events associated with RSA SecurID-based two-factor authentication in this solution.

Network Systems Layer

Network virtualization services are built into the architecture. For example, the Cisco ISR in each store network design virtualizes the security, routing, and identity services that many separate network appliances perform in legacy retail network architectures. Virtualization is also a key feature of the Cisco Unified Wireless systems in each store topology that manage the wireless infrastructure holistically rather than at each access point. The wireless system dynamically tunes and heals itself based on inputs from the central management system. The combined group of network systems in each store reference design is also feeding data to the central network and security monitoring system. This virtualization of the entire enterprise allows the central correlation of events to drive proactive and adaptive techniques to make the overall retail environment more secure.

- **Path Isolation** is a key component of network virtualization. The PCI Solution isolates point-of-sale and network control traffic from other types of network traffic using VLANs, multiple WLAN SSID domains, and a private Frame Relay network from the stores to the data center centralized management. Other techniques can also be used to isolate sensitive traffic and are covered in detail in the Enterprise Network Virtualization design guides that can be found at the following URL:
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor7
- **Services Edge** is where the IRN infrastructure services connect to the physical world of the network infrastructure. In this area, firewall, policy enforcement, and policy management services are constructed to control service access between the store POS domain, other in-store LAN domains, and the WAN connection to remote services. The Data center and Internet edge each use services edge to aggregate integrated infrastructure services and affect all traffic coming through these parts of the designs.

Retail Store Network Designs

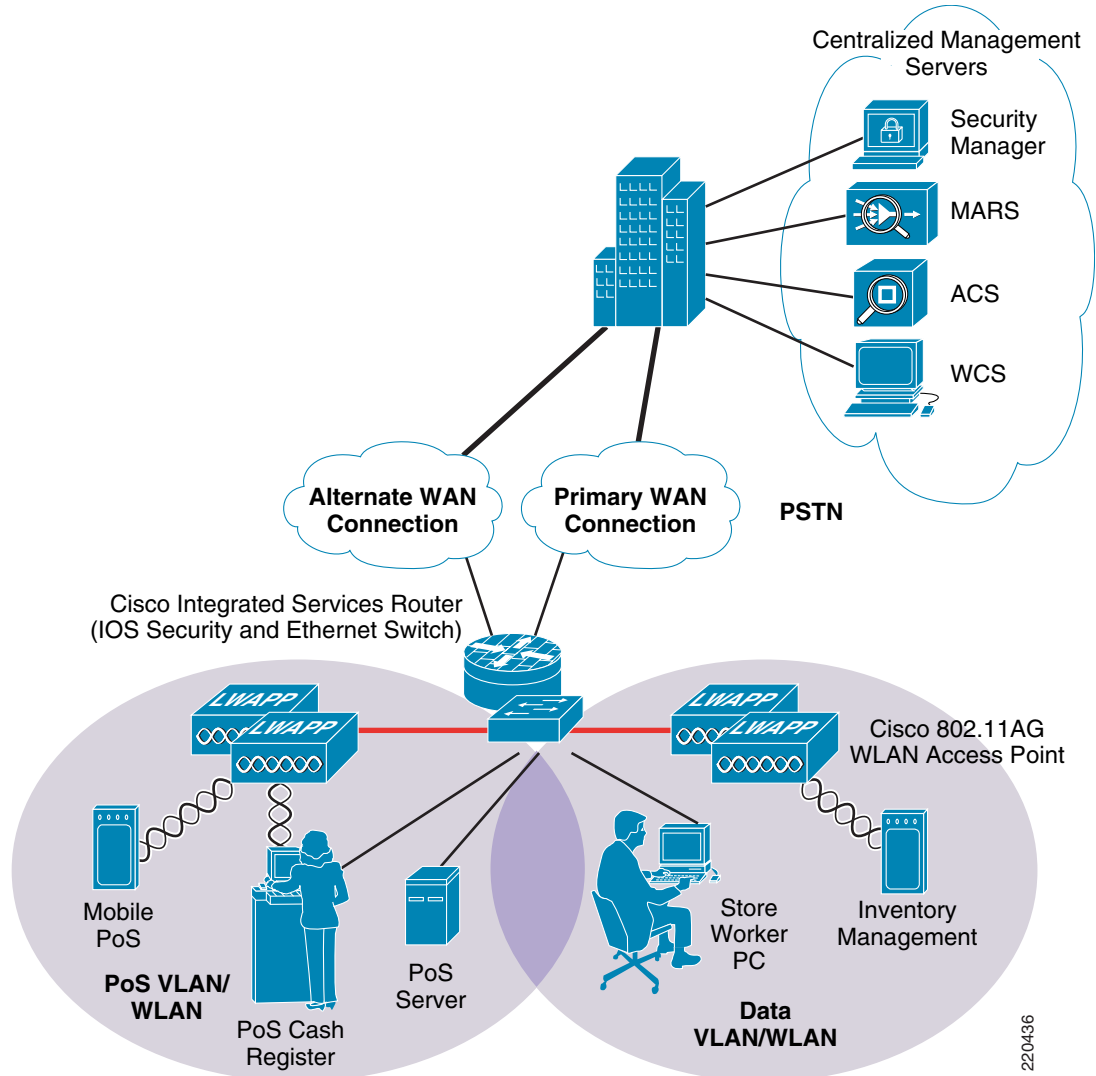
Small Store

The small store network scenario, shown in [Figure 2-2](#), meets the following design requirements.

Primary Design Requirements

- Store size averages between 2000–6000 square feet
- Fewer than 25 devices requiring network connectivity
- Single router and integrated Ethernet switch
- Preference for integrated services within fewer network components because of physical space requirements
- Wireless connectivity

Figure 2-2 PCI Solution for Retail—Small Store Network Design



Overview and Description

The small store reference architecture is a powerful platform for running an enterprise retail business that requires simplicity and a compact form factor. This combination appeals to many different retail formats that can include the following:

- Mall-based retail stores
- Quick-serve restaurants
- Convenience stores
- Fuel stations
- Specialty shops
- Discount retailers who prefer network simplicity over other factors

This network architecture is widely used and consolidates many services into fewer infrastructure components. The small store also supports a variety of retail business application models because an integrated Ethernet switch supports high-speed LAN services. In addition, an integrated Content Engine supports centralized application optimization requirements such as Web Cache Communications Protocol (WCCP)-based caching, pre-positioning of data, local media streaming, and other application velocity services.

Advantages

- Lower cost per store
- Fewer parts to spare
- Fewer software images to maintain
- Lower equipment maintenance costs

Limitations

- Decreased levels of network resilience
- Greater potential downtime because of single points of failure

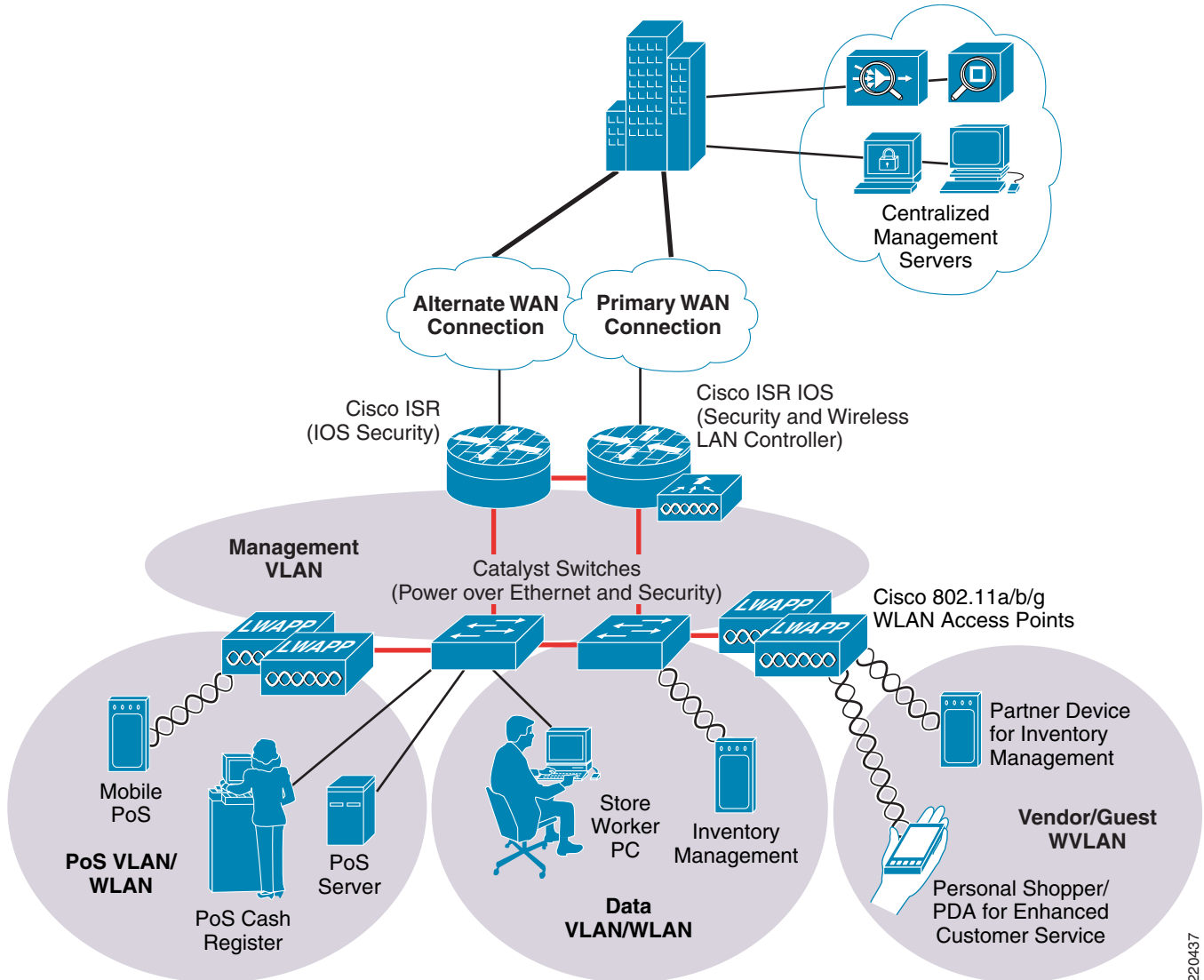
Medium Store

The medium store network scenario, shown in [Figure 2-3](#), meets the following design requirements.

Primary Design Requirements

- Store size averages between 6,000–18,000 square feet
- Physical size of store is smaller than a large store so a distribution layer of network switches is not required
- Number of devices connecting to the network averages 25–100 devices
- Redundant LAN and WAN infrastructures
- Wireless connectivity

Figure 2-3 PCI Solution for Retail—Medium Store Network Design



Overview and Description

The medium retail store reference architecture is designed for enterprise retailers that require network resilience and increased levels of application availability over the small store architecture and its single-threaded, simple approach. As more mission-critical applications and services converge onto the IP infrastructure, network uptime and application availability are more important. The dual-router and dual-LAN switch design of the medium store supports these requirements. Each of the ISR routers can run IOS security services and other store communication services simultaneously. Each of the ISR routers is connected to a dedicated WAN connection. Hot-Standby Routing Protocol (HSRP) is used to ensure network resilience in the event that the network connection fails.

The access layer of the network offers enhanced levels of flexibility and more access ports compared to the small store. Up to 12 wireless access points can be installed in the store (supported by the WCS controller as tested and without adding more controllers). The distributed Cisco Catalyst switches can support a combination of larger physical buildings or a larger number of endpoints than the small store.

Advantages

- More adaptive access layer with support for a greater number of endpoints and more diverse building requirements (multiple floors, sub-areas, and so on)
- Improved network resilience through parallel device design
- Improved network and application availability through parallel paths

Limitations

- No distribution layer between core layer (the ISR) and the access layer switches
- Single WCS Controller decreases in-store resilience of the wireless network; the recommendation is to have store APs fallback to central WCS controller if local WCS controller fails, or install dual-local WCS controllers.

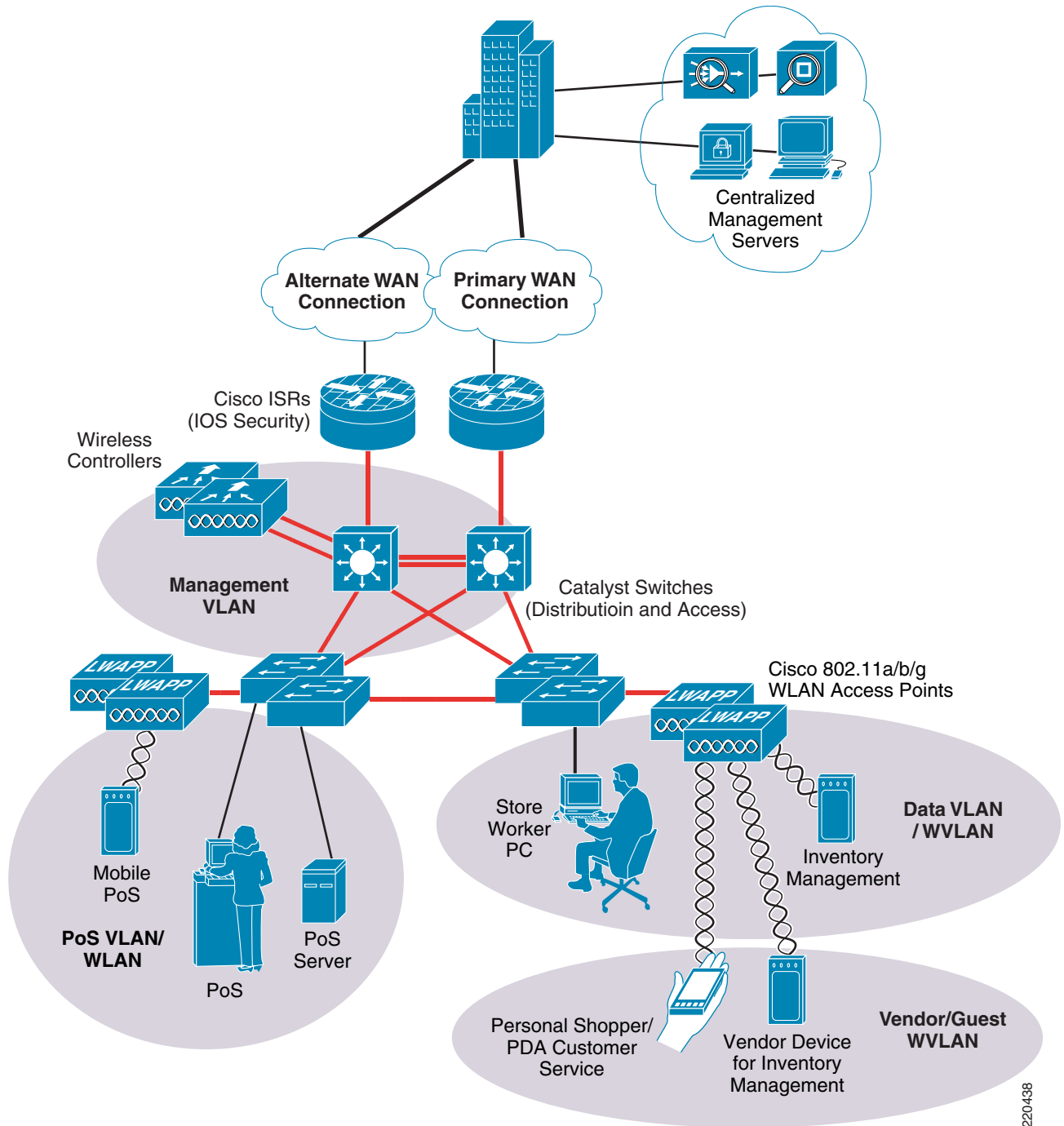
Large Store

The large store network scenario, shown in [Figure 2-4](#), meets the following design requirements.

Primary Design Requirements

- Store size averages between 15,000–150,000 square feet
- More than 100 devices per store requiring network connectivity
- Multiple routers for primary and backup network requirements
- Preference for a combination of network services distributed within the store to meet resilience and application availability requirements
- Tiered network architecture within the store; distribution layer switches are employed between the central network services core and the access layer connecting to the network endpoints (POS, wireless APs, servers)

Figure 2-4 PCI Solution for Retail—Large Store Network Design



Overview and Description

The large retail store reference architecture takes some of the elements of Cisco campus network architecture recommendations and adapts them to a large retail store environment. Network traffic can be better segmented (logically and physically) to meet business requirements. The distribution layer of the large store architecture can greatly improve LAN performance while offering enhanced physical

media connections (that is, fiber and copper for connection to remote access layer switches and wireless access points). A larger number of endpoints can be added to the network to meet business requirements. This type of architecture is widely used by large format retailers globally. Dual routers and distribution layer media flexibility greatly improve network serviceability because the network is highly available and scales to support the large retail store requirements. Routine maintenance and upgrades can be scheduled and performed more frequently or during normal business hours because of parallel path design.

Advantages

- Highest network resilience based on highly available design
- Port density and fiber density for large retail locations
- Increase segmentation of traffic
- Scalable to accommodate shifting requirements in large retail stores

Limitations

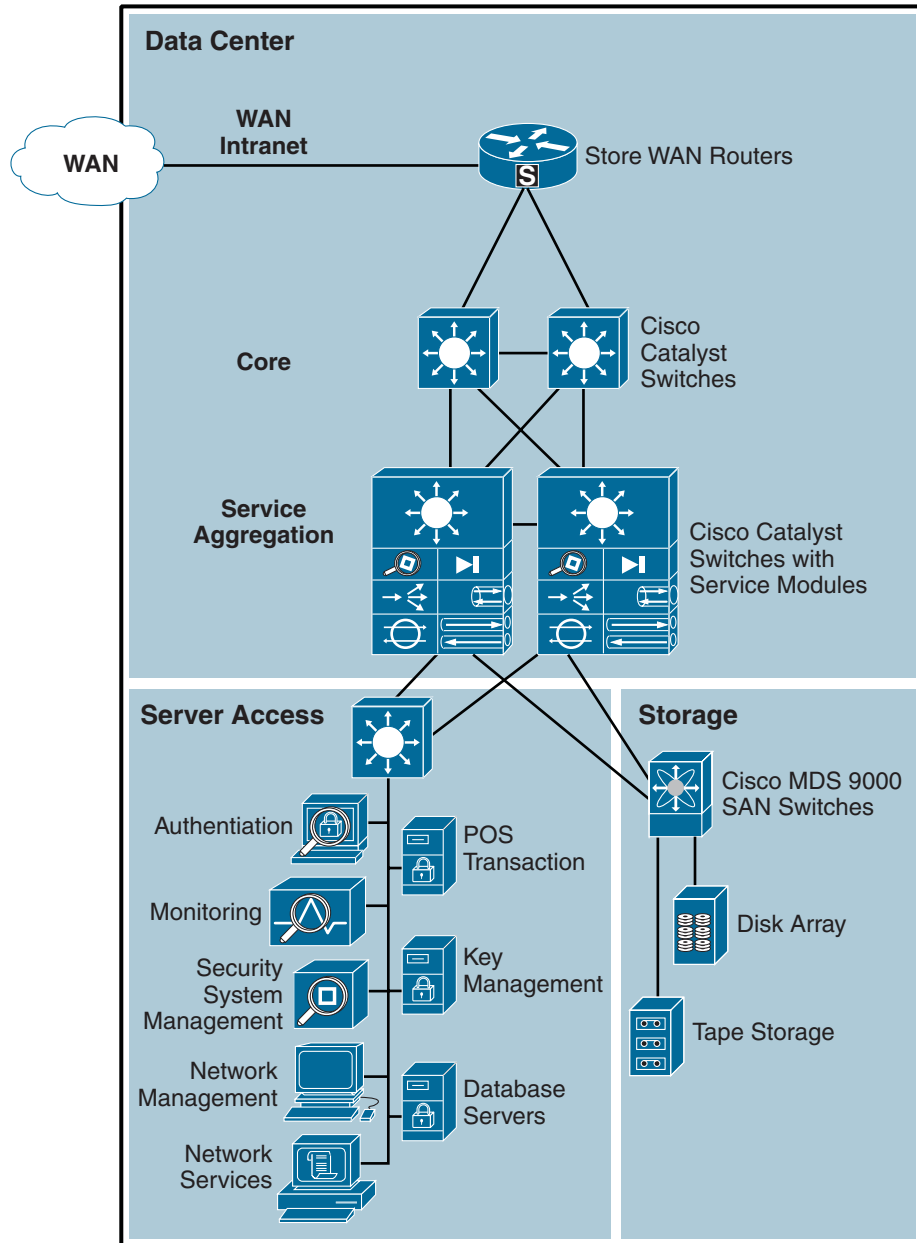
- Higher cost because of network resilience based on highly available design

These retail store network designs are capable of helping a retailer achieve PCI compliance, and also serve as the scalable platform for new services and applications that embody the Cisco Intelligent Retail Network.

Data Center

Figure 2-5 shows the data center solution design.

Figure 2-5 Typical Retail Data Center Design



Primary Design Requirements

- A scalable, highly available repository of business application data and compute servers.
- WAN aggregation layer that securely connects store networks via public or private networks.

- IPSec encryption is required for store networks connected via public networks.
- A high performance core network between WAN aggregation and the service aggregation layer.
- Aggregated network services between the core and server access layer.
- A server access layer that securely connects business and solution management servers to other data center resources.
- A storage area network layer that securely connects storage resources to other resources in the data center.

Overview and Description

For the purpose of this document, the data center is split into five areas: WAN aggregation, core, services aggregation, server access, and storage. The core, services aggregation, and server access tiers of the multi-tier data center architecture was based on the design documented in the *Cisco Data Center Infrastructure Design Guide 2.5*, which can be found at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netso/ns107/c649/ccmigration_09186a008073377d.pdf

The WAN aggregation architecture is based on the *Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0*, which can be found at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration_09186a0080759487.pdf

WAN Aggregation

The WAN aggregation layer is a transit network that aggregates the connections from the retail stores, and enterprise branch office LANs via a private or public service provider network. The WAN aggregation layer does not directly connect end users in the HQ, campus or regional branches; rather, it provides connectivity for the store LANs to connect to the data center core network and its resources.

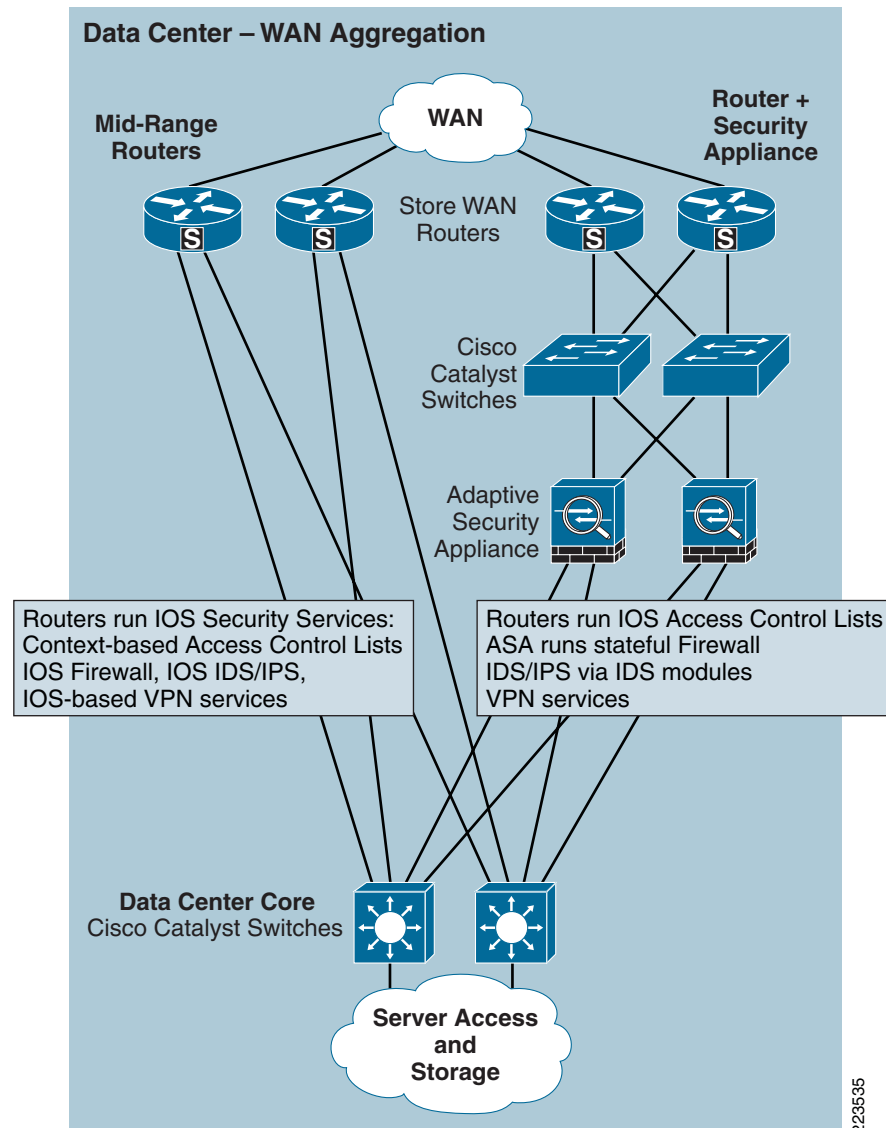
The WAN edge devices are Cisco routers which should not also be used as the Internet gateways for the data center network. This recommendation is based on segmentation and typical throughput requirements for the store WAN. If VoIP is transported between the stores and enterprise network, voice quality issues related to the ability to guarantee bandwidth to store connectivity is another concern. Additionally, redundancy, store-backup networks, and overall network security-related concerns would limit the scope of the WAN aggregation to the function of connecting the store networks to the data center.

At the WAN aggregation layer, interior to the WAN edge routers, a dedicated firewall appliance is used to secure incoming WAN traffic and to terminate store VPN connections. This design provides the highest scalability. Many Cisco routers also support the IOS security software option which includes a firewall feature. Cisco recommends the use of the Cisco IOS Security feature set in stores, branches and teleworker deployments, because of a much lower number of users and connection rates than at the store WAN aggregation headend location.

There are two typical WAN speeds categories for a WAN aggregation network: less than and up to OC3 (155 Mbps) and OC12 (622 Mbps) and above. The choice of these two network speeds determines the platform set to select from Cisco. In addition, this design creates two profiles for each WAN speed. These profiles are designed to provide guidance when designing a WAN edge network regardless of which enterprise WAN architecture is selected. The profiles for each WAN speed investigate integrated versus

dedicated chassis for each functionality component as highlighted in the previous section. Some customers prefer a highly integrated solution where most, if not all, of the WAN edge functions described in this document reside on a single or very few network devices. Other customers prefer the granularity and scalability of these same functions separated across multiple network devices.

Figure 2-6 Data Center – WAN Aggregation Alternatives



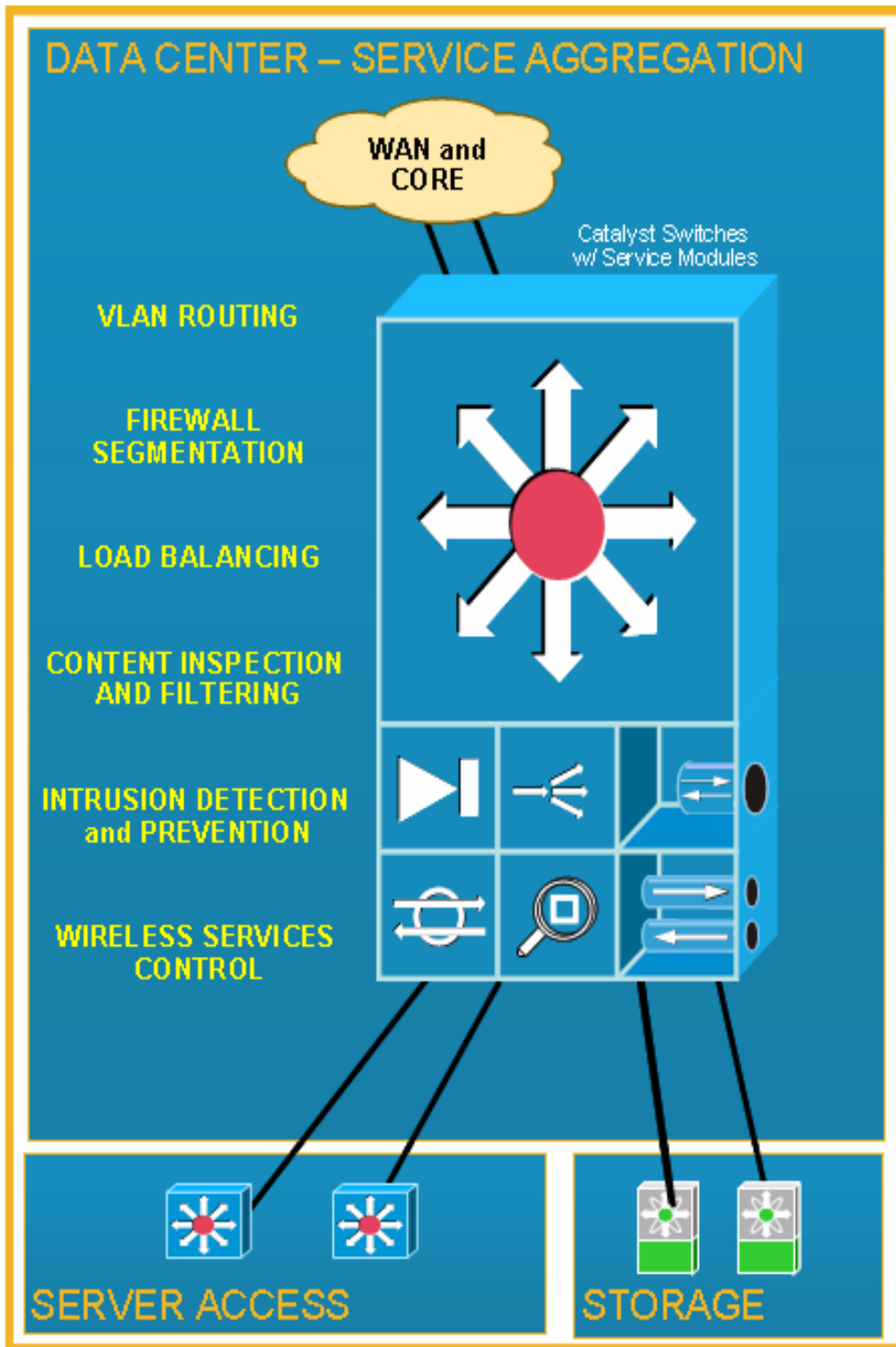
Core

The core layer provides the high-speed packet switching backplane for all flows going in and out of the data center. The core layer provides connectivity to multiple aggregation modules and provides a resilient Layer 3 routed fabric with no single point of failure. The core layer runs an interior routing protocol, such as Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), and load balances traffic between the campus core and aggregation layers using the Cisco Express Forwarding (CEF)-based hashing algorithms.

Services (Edge) Aggregation

The services aggregation layer modules provide important functions, such as service module integration, Layer 2 domain definitions, spanning tree processing, and default gateway redundancy. Server-to-server multi-tier traffic flows through the aggregation layer and can use services, such as firewall and server load balancing, to optimize and secure applications. The service modules provide services, such as content switching, firewall, SSL offload, intrusion detection, network analysis, and more. [Figure 2-7](#) illustrates a characterized view of the service aggregation layer.

Figure 2-7 Conceptual Service Aggregation Layer



This is a conceptual example of a single Cisco Catalyst 6500 switch and service modules. Cisco's data center reference architectures recommend pairs of service aggregation switches to meet typical high-availability requirements of the server access or storage layers.

Server Access Layer

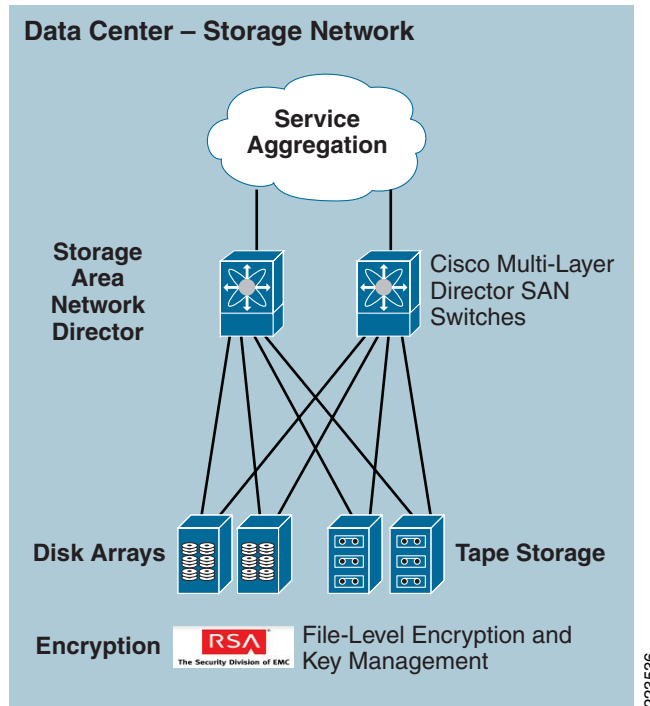
The server access layer is where the servers physically attach to the network. In typical data centers, the server components consist of 1RU servers, blade servers with integral switches, blade servers with pass-through cabling, clustered servers, and mainframes with OSA adapters. The access layer network infrastructure consists of modular switches, fixed configuration 1 or 2RU switches, and integral blade server switches. Switches provide both Layer 2 and Layer 3 topologies, fulfilling the various server broadcast domain or administrative requirements.

The solution management servers connect to the network in this layer. This way they are centralized, segmented from other business application servers, and protected by firewall services from the service aggregation layer above. Business servers, consisting of POS transaction log servers, database, and data warehouse servers would also exist at this layer but would be segmented via separate VLANs and firewall policy.

Storage

A combination of the file encryption provided by the RSA File Security Manager product, fiber-channel zoning, and Logical Unit (LUN) masking/zoning as provided by the Cisco family of multi-layer director switches (MDS) were used in the storage implementation of this solution to deliver encryption and restricted access to cardholder data at rest in the datacenter. By deploying zoning within a Fibre Channel fabric, device access is limited to devices within the zone. This allows the user to segregate devices based on access to a particular storage device (disk array). This is generally an absolute requirement when dealing with a datacenter environment in which multiple file servers in the datacenter server farm are connected to the same SAN fabric and access to cardholder data must be restricted to a subset of servers. LUN masking takes zoning beyond the fiber-channel, switch port level by allowing for the restricted access to specific logical units on a given disk array such that only specific devices belonging to the LUN zone will be able to access those sections of the disk.

Figure 2-8 Data Center Storage Area Networking



Advantages

- Standardized equipment and software images, deployed in a modular, layered approach, simplifies configuration management and increases the systems availability.
- Highly available data center design permits highly resilient access from stores to core data and storage services.
- WAN aggregation alternatives allow flexible selection of service provider network offerings.
- Service aggregation design allows for a modular approach to adding new access layers and managing shared network services (FW, IDS, application networking, wireless management, etc.).
- Firewall, IDS and application networking services are available at all layers of the data center.
- Scalable to accommodate shifting requirements in data center compute and storage requirements.
- Centralized solution management support all aspects of network, security and systems management and supports remote access from anywhere on the network.

Limitations

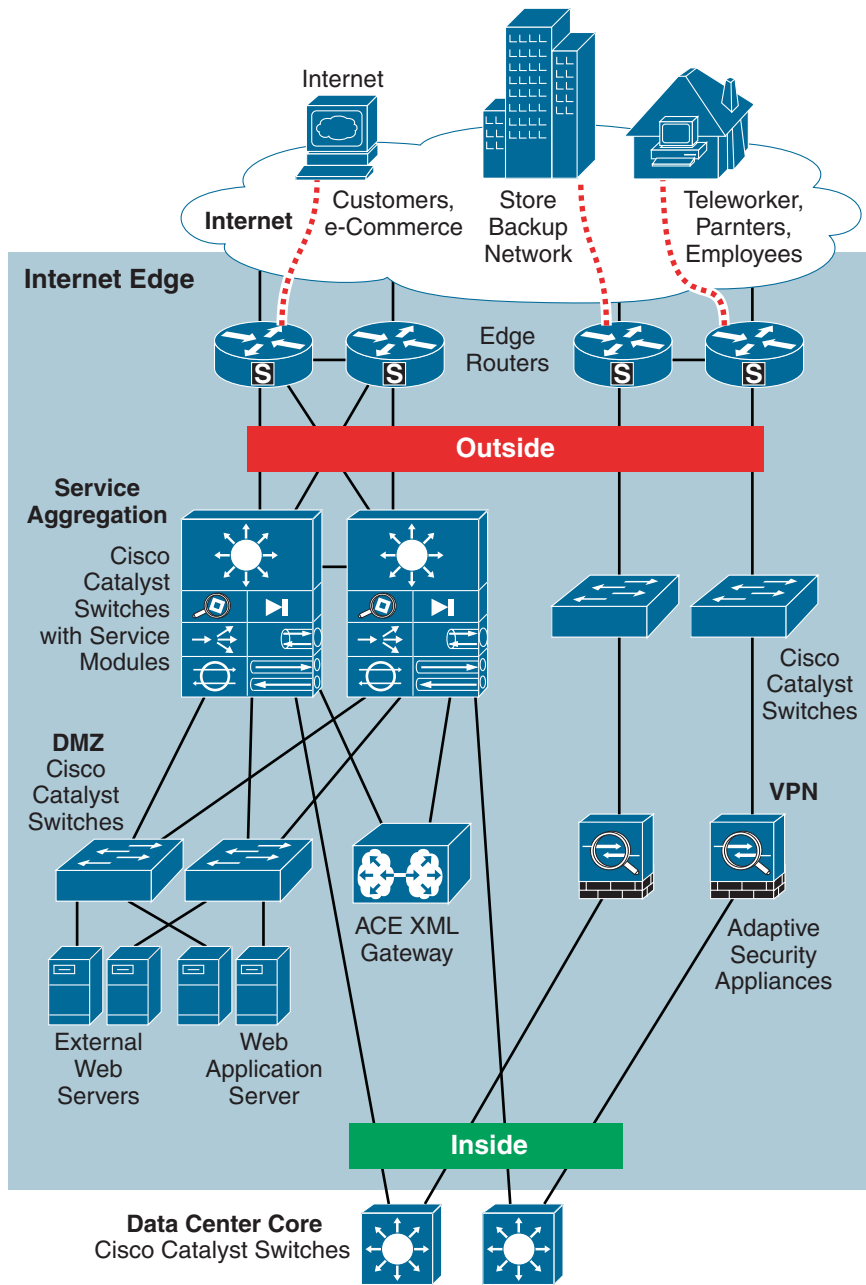
- WAN access speeds are typically the limiting factor between the store network systems and the WAN aggregation layer.
- It is typical for retailers to over-subscribe the WAN circuits between the stores and the WAN edge aggregation router. Over-subscription can cause inconsistent results and packet loss of payment card information in the event that more traffic enters the WAN circuit simultaneously. QoS guidelines to classify payment card traffic as critical are recommended.

- Backup network connections from store networks to the data center are recommended when payment card information is transported via the WAN. These options are not covered in this design guide as they are not a requirement to meet PCI guidelines.

Internet Edge

The Internet edge solution architecture is listed in [Figure 2-9](#).

Figure 2-9 Typical Internet Edge Architecture



Primary Design Requirements

- An enterprise connection to Internet.
- Securing the Internet edge design using Cisco firewall and intrusion detection systems.
- Protecting enterprise network against web attacks.
- Dual-threaded design for network resiliency.
- Collapsed Internet edge and extranet network for a highly centralized and integrated edge network.
- Remote VPN access to enterprise users/telecommuters.

Overview and Description

The solution uses a collapsed Internet edge and extranet network to support Internet connectivity and business partner connectivity. This design takes into account best practices from the in *Data Center Networking: Internet Edge Design Architecture Design Guide* (<http://www.cisco.com/go/srnd/>) and customizes these recommendations for a Retail Internet edge and extranet network. The edges connects Internet services to the complete enterprise environment(i.e., from headquarters to Internet service providers (ISP), branch office connections that use Cisco secure VPN to connect to headquarters. The collapsed design provides highly centralized and integrated edge networks and transports the aggregated traffic through different service modules (Cisco ACE, Cisco FWSM and Cisco IDSM2) within a pair of Cisco Catalyst 6500 switch chassis. The design provides protection and defense against XML threats using the Cisco ACE AXL Gateway. The Internet edge provides the following security functions:

- Secure configurations and management.
- IP anti-spoofing.
- Access Control Lists (ACLs) provide explicitly permitted and/or denied IP traffic that may traverse between inside, outside, and Demilitarized Zone (DMZ).
- Stateful inspection—Provide the ability to establish and monitor session states of traffic permitted to flow across the Internet edge and deny that traffic which fails to match the expected state of an existing or allowed sessions.
- Intrusion detection using Cisco IDSM2—Provides ability to promiscuously monitor traffic across discrete points within the Internet edge and alarm and/or take action detecting suspect behavior that may threaten the enterprise network.
- Demilitarized Zone (DMZ)—Applications servers that need to be directly accessed from the Internet are placed in a quasi-trusted secure area between the Internet and the internal enterprise network. This allows internal hosts and Internet hosts to communicate with servers in the DMZ .

Advantage

- Collapsed architecture
- Highly available design
- Firewall and intrusion detection capabilities in a single chassis

Disadvantage

- Complexity in configuration.

Chapter 3, “Solution Components—Best Practices and PCI,” provides the mapping between specific Cisco solution components and the required PCI elements to meet QSA audit requirements.



CHAPTER 3

Solution Components—Best Practices and PCI

The information in this chapter applies equally to the small, medium, large store, data center, and Internet edge architectures. Each solution component is presented with the following:

- General notes/best practices

This section provides guiding principles for each technology within a retail environment. The notes are Cisco recommendations but do not necessarily fall within the framework of PCI. Some notes exceed the PCI specification and are additional security features of that respective product.

- PCI sub-requirements satisfied by solution component

This section delineates which PCI sub-requirements were successfully audited and validated by the respective technology. Note that this result is directly correlated to the implementation built in the Cisco lab and presented in [Chapter 4, “Implementing and Configuring the Solution.”](#) The results of an audit may vary depending on the implementation within a retail company.

- PCI sub-requirements that require compensating controls

This section delineates which PCI sub-requirements needed additional compensating controls to successfully pass the PCI audit. These technologies required additional configuration or products to pass compliance. The results of an audit may vary depending on the implementation within a retail company.

For detailed configurations, refer to [Chapter 4, “Implementing and Configuring the Solution.”](#)

Network Systems

Cisco Integrated Services Router

The Cisco Integrated Services Router (ISR) consolidates data, network, and security into a single platform with local and centralized management services.

General Notes/Best Practices

- The security features of the ISR routers in the small, medium, and large architectures are configured using Cisco Security Manager. When adopting this as the primary method of router configuration, Cisco does not recommend making changes directly to the command-line interface (CLI) of the router. Unpredictable results can occur when central and local management are used concurrently.
- The general configuration of the ISR routers in the small, medium, and large architectures are maintained with CiscoWorks Resource Manager Essentials (a component of C-LMS).
- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.
- Ensure that inspection rules are enabled on the ISR router so that the firewall maintains state (none are enabled by default).
- Access into a store router from the WAN needs to be protected by a store-located firewall filter if the WAN technology is considered public. In the Retail PCI Solution lab, filtering of the store WAN traffic occurs on the outbound data center side of the Frame Relay connection to preserve bandwidth. Frame Relay is considered a private network.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, AUX, VTY, and line interfaces on the router.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the Cisco Secure Access Control Server (CS-ACS). Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or CS-ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.

PCI Sub-Requirements Satisfied by Solution Component (Router)

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2**—*Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.*

Each of the routers in the PCI Solution for Retail uses firewall feature set capabilities to satisfy this requirement.

The solution allowed the following business-related communication:

- Management protocols for Cisco Security Manager (CS-M) and CiscoWorks (C-LMS)
- Monitoring, analysis, and response system (CS-MARS)
- Authentication, authorization, and accounting (AAA) to access control server (CS-ACS) via TACACS
- Internet Control Message Protocol (ICMP) for network troubleshooting
- Network Time Protocol (NTP) for time stamp synchronization
- System logging access for network events
- Simple Network Management Protocol (SNMP)
- Secure Socket Layer (SSL)
- High availability via Hot Standby Routing Protocol (HSRP)
- Dynamic Host Configuration Protocol (DHCP)
- Everything else was denied and logged

See [Appendix C, “Application Protocols,”](#) for a complete listing of the communications used in this solution.

The following is a sample configuration from the large store architecture:

```
RLRG-1#
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.1000
 remark Allow CSM-Server to access device through the Serial (external) Interface
 permit icmp host 192.168.42.133 host 10.10.62.1 log
 permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
 remark ---- permit ntp ----
 permit udp any host 192.168.62.161 eq ntp
 permit udp any host 192.168.62.162 eq ntp
 permit udp any host 192.168.42.130 eq ntp
 remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
 permit tcp any host 192.168.42.134 eq 69 log
 permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
 remark ---- Ciscoworks so Managed Devices ----
 permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
 permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
 remark ---- System messages to MARS ----
 permit tcp any host 192.168.42.121 eq 2055 log
 permit udp any host 192.168.42.121 eq snmp syslog log
 remark ---- Allow network devices to use the ACS server ----
 permit tcp any host 192.168.42.131 eq tacacs log
 permit udp any host 192.168.42.131 eq 1812 log
 remark ---- ping to Datacenter ----
 permit icmp any 192.168.42.0 0.0.0.255 log
 remark ---- HSRP health information ----
 permit udp any host 224.0.0.2 eq 1985 log
 remark ---- Ping Gateway ----
```

```

permit icmp 10.10.63.0 0.0.0.255 10.10.63.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
!
interface GigabitEthernet0/0.1000
ip access-group CSM_FW_ACL_GigabitEthernet0/0.1000 in
!

```

- **PCI 1.3.3**—*Implementing stateful inspection, also known as dynamic packet filtering (that is, only “established” connections are allowed into the network).*

The stateful inspection in the solution is the Cisco-recommended configuration. The statements inspect the protocol for anomalies on their default ports and maintain the established dynamic connection table for each session.

The following is a sample configuration:

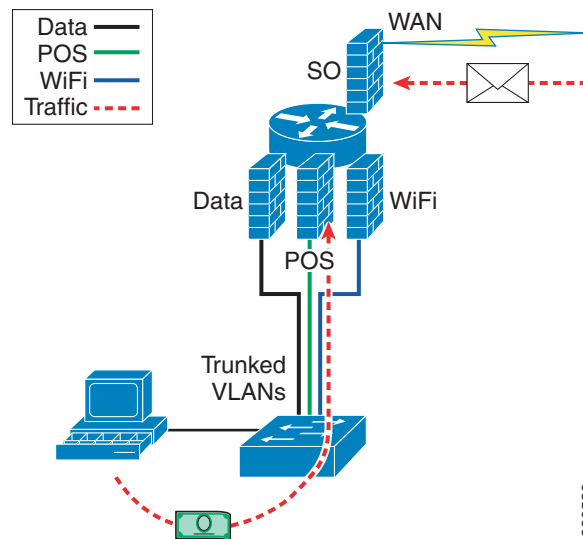
```

RLRG-1#
!
ip inspect name CSM_INSPECT_1 http alert on audit-trail on
ip inspect name CSM_INSPECT_1 dns alert on audit-trail on
ip inspect name CSM_INSPECT_1 radius alert on audit-trail on
ip inspect name CSM_INSPECT_1 tacacs alert on audit-trail on
ip inspect name CSM_INSPECT_1 ssh alert on audit-trail on
ip inspect name CSM_INSPECT_1 ftp alert on audit-trail on
ip inspect name CSM_INSPECT_1 ldap alert on audit-trail on
ip inspect name CSM_INSPECT_1 snmp alert on audit-trail on
ip inspect name CSM_INSPECT_1 icmp alert on audit-trail on
ip inspect name CSM_INSPECT_1 tcp alert on audit-trail on
ip inspect name CSM_INSPECT_1 udp alert on audit-trail on
!
interface GigabitEthernet0/0.1000
ip inspect CSM_INSPECT_1 in
!

```

- **PCI 1.3.5**—*Restricting outbound traffic to that which is necessary for the cardholder data environment.*

The routers are configured to filter and inspect all traffic inbound from each network segment. Through extensive interview and discussion with the QSA, filtering all inbound network traffic to the router was determined to be an acceptable implementation. This effectively restricts the outbound traffic, and is a common practice in many retailer networks. (See [Figure 3-1](#).)

Figure 3-1 Restricting Outbound Traffic

The following is a sample configuration:

```
RLRG-1#
!
interface GigabitEthernet0/0.11
description POINT OF SALE NETWORK
ip access-group CSM_FW_ACL_GigabitEthernet0/0.11 in
ip inspect CSM_INSPECT_1 in
!
```

- **PCI 1.3.7**—Denying all other inbound and outbound traffic not specifically allowed.

Deny and log all traffic not explicitly allowed within each firewall rule set. Logging all denied traffic may cause a significant performance impact depending on the retail environment.

The following is a sample configuration:

```
RLRG-1#
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.1000
< deleted for brevity>
remark Drop anything not explicitly allowed
deny ip any any log
```

- **PCI 1.3.8**—Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes).

The point-of-sale network and the wireless network is segmented by VLANs and secured by the Cisco IOS firewall that is integrated in the router. (See [Figure 3-1](#).)

The following is a sample configuration:

```
RLRG-1#
!
interface GigabitEthernet0/0.14
description WIRELESS
<excerpted for brevity>
ip address 10.10.51.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.14 in
!
interface GigabitEthernet0/0.11
description POINT OF SALE
```

```

<excerpted for brevity>
ip address 10.10.48.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.11 in
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.51.0 0.0.0.255 10.10.51.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.48.0 0.0.0.255 10.10.48.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
!

```

- **PCI 1.5**—*Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).*

The stores in this solution are configured using private addressing that are not routable across the Internet. NAT or PAT must be used in the data center to convert these addresses into public available address space.

Following is an example of a large store addressing plan:

```
10.10.48.0 255.255.240.0 Summarized store addressing block

10.10.48.0 /24- VLAN11 (POS)
10.10.49.0 /24- VLAN12 (Data)
10.10.50.0 /24- VLAN13 (Voice)
10.10.51.0 /24- VLAN14 (Wireless)
10.10.52.0 /24- VLAN15 (Wireless POS)
10.10.53.0 /24- VLAN16 (Partner)
10.10.54.0 /24- VLAN17 (Wireless Guest)
10.10.55.0 /24- VLAN18 (LWAP Control)
10.10.56.0 ~10.10.61.0 - (Future)
10.10.62.0 /24- Other- (Misc)
10.10.62.1 /32- LRG-1 Loop 0
10.10.62.2 /32- LRG-2 Loop 0
10.10.62.16 /30- LRG-1 Serial 0
10.10.62.20 /30- LRG-2 Serial 0
10.10.62.24 /30- VLAN101 (Router Link)
10.10.62.28 /30- VLAN102 (Router Link)
10.10.63.0 /24- VLAN1000 (Management)
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function)*
- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

Disable services such as pad, finger, and small servers. Depending on the Cisco IOS release, these will be enabled or disabled by default and may not be displayed in the running configuration.

Only encrypted management communication was enabled. All other services were disabled.

The following is a sample configuration:

```
no service pad
no ip finger
!
no ip http server
ip http secure-server
```

```
!
line vty 0 4
  transport input ssh
!
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements for Requirements 7 and 8:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords*
- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Compliance of the sub-requirements in this section was achieved within the solution by implementing the Cisco Secure Access Control Server (CS-ACS) and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the router. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.*

Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, AUX, VTY, and line interfaces on the router.

Following is a sample configuration:

```
!
line con 0
  session-timeout 15 output
  exec-timeout 15 0
!
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS for Authentication, Authorization and Accounting (AAA) services.

The Cisco ISR router was not configured or audited for AAA features without the use of ACS.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

Following is a sample configuration:

```
!
aaa new-model
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
```

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
- **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization*
- **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]*

- **PCI 10.4.c**—Verify that the Network Time Protocol (NTP) is running the most recent version
- **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.

Following is a sample configuration:

```
RLRG-1#
!
ntp clock-period 17179470
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
```

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4.a**—Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored.
- **PCI 11.4.c**—Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

The sub-requirements in this section are satisfied through the IPS feature set of the Cisco ISR router combined with monitoring and alerting capability of CS-MARS.

The Cisco Security Manager (C-SM) is used to configure and deploy the IDS/IPS event definitions and signatures to the Cisco ISR routers.

Following is a sample configuration:

```
ip ips sdf location
https://192.168.42.133:443/ids-config/servlet/com.cisco.nm.mdc.ids.config.iosids.servlet.S
DFServlet/11/sdF-complete.xml
ip ips notify SDEE
ip ips name sdm_ips_rule
!
```

PCI Sub-Requirements that Require Compensating Controls (Router)

The Cisco ISR routers within this solution complied with all relevant PCI sub-requirements and did not require any compensating controls.

Mid-Range Routers (WAN Aggregation)/Edge Routers (Internet Edge)

General Notes/Best Practices

- Configuration was done manually on the router CLI and backing-up of configuration and monitoring of configuration for changes and non-compliance were done through the CiscoWorks Network Compliance Manager (C-NCM).
- Firewall rule sets must adhere to a "least amount of access necessary" policy. Where possible, rules must be defined by specific source/destination addressing and TCP/UDP ports required for the cardholder data environment on the point-of-sale networks.

- The perimeter firewall between the data center was provided by the Adaptive Security Appliance. As a result, the Cisco 7206VXR was not evaluated according to the set of 1.x requirements for firewalls.
- Disable the HTTP server service on the router and enable the HTTP secure server.
- Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, AUX, VTY, and line interfaces on the router.
- Configure appropriate banner messages on login, incoming, and exec modes of the router. The login banner warning should not reveal the identity of the company that owns or manages the router. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the router to be directed to the CS-ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the router itself in the event of a WAN or CS-ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the router.
- Change default passwords and community strings to appropriate complexity.
- Enable anti-spoofing on all interfaces.
- For the Internet edge routers, use the following access-list on the interface that is facing the Internet. This access-list explicitly filters traffic destined for infrastructure address space. Deployment of edge infrastructure access-lists requires that you clearly define your infrastructure space and the required/authorized protocols that access this space. The access-list is applied at ingress to your network on all externally facing connections, such as peering connections, customer connections, and so forth.

Following is a sample configuration:

```

!
!
access-list 110 remark Deny special-use address sources
access-list 110 remark Refer to RFC 3330 for additional special use addresses
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
access-list 110 remark Filter RFC 1918 space
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 remark deny your space as source from entering your AS.
access-list 110 remark To be deployed only at the AS edge.
access-list 110 deny ip <YOUR_CIDR_BLOCK> any
access-list 110 permit tcp any host <public web server> eq www log
access-list 110 permit tcp any host <public web server> eq 443 log
access-list 110 remark Permit legitimate business traffic.
access-list 110 permit tcp any <Internet-routable subnet> established
access-list 110 deny ip any any log
!
!

```



Note The **log** keyword can be used to provide additional detail about source and destinations for a given protocol. Although this keyword provides valuable insight into the details of access-lists hits, excessive hits to an access-list entry that uses the **log** keyword increase CPU utilization. The performance impact associated with logging varies by platform.

The service provider network in the solution represented an MPLS network. At the writing of this document, MPLS is considered a private network and secure tunneling across the WAN is not required. However, for best practices, Cisco recommends Virtual Private Network (VPN) tunneling be implemented. For further information on implementing an IPsec VPN, refer to the *IPsec VPN Direct Encapsulation Design Guide* at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netso/ns171/c649/ccmigration_09186a0080739e7c.pdf.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts. See [Appendix E, “Device Configurations.”](#)

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).*
- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

Disable services such as pad, finger, and small servers. Depending on the Cisco IOS release, these will be enabled or disabled by default and may not be displayed in the running configuration.

Only encrypted management communication was enabled. All other services were disabled.

The following is a sample configuration:

```
no service pad
no ip finger
!
no ip http server
ip http secure-server
!
line vty 0 4
  transport input ssh
!
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements for Requirements 7 and 8:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components.*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Compliance of the sub-requirements in this section is achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the router. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.*

Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console, aux, VTY, and line interfaces on the router.

Following is a sample configuration:

```
!
line con 0
 session-timeout 15 output
 exec-timeout 15 0
!
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS for Authentication, Authorization and Accounting (AAA) services.

The Cisco ISR router was not configured or audited for AAA features without the use of CS-ACS.

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

Following is a sample configuration:

```
!
aaa new-model
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
```

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verifying the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals. Time signals are sent directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT). The time servers peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*

Following is a sample configuration:

```
RWAN-10#  
!  
ntp clock-period 17179470  
ntp source Loopback0  
ntp server 192.168.62.162  
ntp server 192.168.62.161 prefer
```

Cisco Catalyst Ethernet Switch and Network Switch Module

The Cisco Catalyst Ethernet switch provides connectivity for the IP endpoints to the routed networks and WAN services.

General Notes/Best Practices

- The general configuration of the Cisco Catalyst switches and Network Switch Module in the small, medium, and large architectures are maintained with the CiscoWorks Resource Manager Essentials (a component of C-LMS).
- The use of VLANs on the Cisco Catalyst switch enables the retailer to provide same-box wired access to its devices while maintaining segregated addressing schemes.
- Disable the HTTP server on the switch and enable the HTTP secure server.
- Set the **session** and **exec timeout** commands to 15 minutes or less.
- Configure appropriate banner messages on login, incoming, and exec modes of the switch. The login banner warning should not reveal the identity of the company that owns or manages the switch. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the switch to be directed to the CS-ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the switch itself in the event of a WAN or CS-ACS failure.
- Use the **no service password-recovery** command in conjunction with the **service password encryption** command to prevent password theft by physical compromise of the switch.
- Change default passwords and community strings to appropriate complexity.

PCI Sub-Requirements Satisfied by Solution Component (Switches)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function).*

- **PCI 2.2.3.c**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.
- **PCI 2.2.4**—Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- **PCI 2.3**—Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Disable services such as pad, finger, and small servers. Depending on the Cisco IOS release, these may be enabled or disabled by default and may not be displayed in the running configuration.

Only encrypted management communication was enabled. All other services were disabled.

Following is a sample configuration:

```
no service pad
no ip finger
!
no ip http server
ip http secure-server
!
line vty 0 4
  transport input ssh
!
```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the router. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 7.2**—Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
- **PCI 8.1**—Identify all users with a unique user name before allowing them to access system components or cardholder data.
- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters

- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

Configure the **session-timeout** and **exec-timeout** commands to 15 minutes or less on the console and VTY interfaces on the switch.

Following is a sample configuration:

```
!
line con 0
 session-timeout 15 output
 exec-timeout 15 0
!
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of these sub-requirements was achieved within the solution by implementing the CS-ACS for Authentication, Authorization and Accounting (AAA) services.

The Catalyst Switches were not configured or audited for AAA features without the use of CS-ACS.

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

Following is a sample configuration:

```
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
```

- **PCI 10.4**—Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points.

Verify the following is included in the process and implemented:

- **PCI 10.4.a**—Verify that NTP or similar technology is used for time synchronization.
- **PCI 10.4.b**—Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.
- **PCI 10.4.c**—Verify that the Network Time Protocol (NTP) is running the most recent version.
- **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.

Following is a sample configuration:

```
SMED-2#
!
ntp clock-period 17179470
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
```

PCI Sub-Requirements that Require Compensating Controls (Switches)

The Cisco Catalyst switches within this solution did not require any compensating controls to pass respective PCI sub-requirements.

Cisco Firewall Services Module (FWSM)

The Cisco FWSM is an integrated module installed inside a Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. The FWSM allows any port on the Cisco Catalyst switch to operate as a firewall port and integrates firewall security inside the network infrastructure.

General Notes/Best Practices

- Firewall rule sets must adhere to a “least amount of access necessary” policy. Rules must be defined by specific source/destination addressing and TCP/UDP ports
- For Internet edge, disable ICMP permit on the outside interface of FWSM. If users need to access servers in the DMZ segment then make sure that external users can reach the servers using very specific protocol and ports.
- Configure the **ip verify reverse path** command on all interfaces to provide anti-spoofing functionality.
- Configure the **console timeout** commands to 15 minutes or less on the console of the FWSM.

- Configure appropriate banner messages on login, incoming, and exec modes of the FWSM. The login banner warning should not reveal the identity of the company that owns or manages the FWSM. The incoming and executive banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Configure the primary login authentication of the FWSM to be directed to the CS-ACS. Individual user account profiles need to be created. Configure secondary or tertiary authentication local to the FWSM itself in the event of connectivity or CS-ACS failure.
- Change default passwords and community strings to appropriate complexity.
- Allow only SSHv2 (and not Telnet or SSHv1) connection from network management station to Cisco FWSM.

PCI Sub-Requirements Satisfied by Solution Component (Cisco FWSM)

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2**—Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.

The Cisco FWSM in Internet edge is used to meet the PCI requirement.

The solution allowed the following business-related communication:

- Monitoring, analysis, and response system (CS-MARS).
- CiscoWorks Network Compliance Manager (C-NCM).
- Authentication, authorization, and accounting to CS-ACS via TACACS.
- Network Time Protocol (NTP) for time stamp synchronization.
- System logging access for network events.
- Simple Network Management Protocol (SNMP)
- Everything else is implicitly denied.

The following is a sample configuration of an outside interface (facing the Internet) of an Internet edge Cisco FWSM.

```
FWSM
!
access-list ECOM_OUT remark ---- permit ntp ----
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.62.130 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.62.130 eq ntp
access-list ECOM_OUT remark ---- System messages to MARS ----
access-list ECOM_OUT extended permit tcp host 192.168.21.4 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.121 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.121 eq syslog log
access-list ECOM_OUT extended permit tcp host 192.168.21.5 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.121 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.121 eq syslog log
access-list ECOM_OUT remark ---- Allow network devices to use the ACS server ----
access-list ECOM_OUT extended permit tcp host 192.168.21.4 host 192.168.42.131 eq tacacs log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT extended permit tcp host 192.168.21.5 host 192.168.42.131 eq tacacs log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT remark ---- Permit snmp to Network Compliance Manager ----
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.118 eq syslog log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.118 eq syslog log
!
```

- **PCI 1.3.3**—*Implementing stateful inspection, also known as dynamic packet filtering (that is, only “established” connections are allowed into the network).*

The stateful inspection in the solution is the Cisco-recommended configuration. The statements inspect the protocol for anomalies on their default ports and maintain the established dynamic connection table for each session. It is a good practice to disable inspection for protocols that are not used.

The following is a sample configuration:

```
FWSM1#
FWSM1# sh run | b policy
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect netbios
    inspect smtp
    inspect icmp
    inspect http
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:51ff3afd13deafb682c969655a835b71
: end
!!
```

- **PCI 1.3.7**—*Denying all other inbound and outbound traffic not specifically allowed.*

In the Cisco FWSM, every access-list ends with an implicit deny **ip any any**.



Note When you enter a new access-list entry, it is always appended to the bottom of the access-list. Since access-list are evaluated in sequential order, the correct order of the access-list entry is important.

- **PCI 1.5**—*Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as Port Address Translation (PAT) or Network Address Translation (NAT).*

The PCI solution in the lab is configured to use private addressing that are not routable across the Internet. NAT is used to convert these addresses into public available address space. To simulate a real environment, we used IP address 192.168.80.25 as public IP address for testing purpose.

```
FWSM>
nat-control
global (ECOM_OUTSIDE) 1 interface
nat (ECOM_DMZ) 1 0.0.0.0 0.0.0.0
nat (DMZ_MGMT) 1 192.168.21.16 255.255.255.240
static (ECOM_DMZ,ECOM_OUTSIDE) 192.168.80.25 192.168.20.1 netmask 255.255.255.255
FWSM>
```

Following is an example of a large store addressing plan:

```
10.10.48.0 255.255.240.0 Summarized store addressing block
```

```
10.10.48.0 /24- VLAN11 (POS)
10.10.49.0 /24- VLAN12 (Data)
10.10.50.0 /24- VLAN13 (Voice)
10.10.51.0 /24- VLAN14 (Wireless)
10.10.52.0 /24- VLAN15 (Wireless POS)
10.10.53.0 /24- VLAN16 (Partner)
```

```

10.10.54.0 /24- VLAN17 (Wireless Guest)
10.10.55.0 /24- VLAN18 (LWAP Control)
10.10.56.0 ~10.10.61.0 - (Future)
10.10.62.0 /24- Other- (Misc)
10.10.62.1 /32- LRG-1 Loop 0
10.10.62.2 /32- LRG-2 Loop 0
10.10.62.16 /30- LRG-1 Serial 0
10.10.62.20 /30- LRG-2 Serial 0
10.10.62.24 /30- VLAN101 (Router Link)
10.10.62.28 /30- VLAN102 (Router Link)
10.10.63.0 /24- VLAN1000 (Management)

```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

PCI 2.2—Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function)
- **PCI 2.2.3.b**—Verify that common security parameter settings are included in the system configuration standards
- **PCI 2.2.3.c**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.
- **PCI 2.2.4**—Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- **PCI 2.3**—Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Disable unwanted services on the Cisco FWSM module.

Only encrypted management communication was enabled. All other services were disabled.

The following is a sample configuration:

```

no ftp mode passive

ssh 192.168.42.131 255.255.255.255 inside
ssh 192.168.42.121 255.255.255.255 inside
ssh 192.168.42.118 255.255.255.255 inside
ssh timeout 5
ssh version 2

```

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And

Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements for Requirements 7 and 8:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords*
- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the Cisco FWSM. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*

Configure the console timeout with the following command:

```
console timeout 15
```

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS for AAA services.

The Cisco ISR router was not configured or audited for AAA features without the use of CS-ACS.

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

Following is a sample configuration:

```
!
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL host 192.168.42.131
  key <removed>
aaa authentication ssh console RETAIL LOCAL
aaa authorization include ssh inside 192.168.11.2 255.255.255.255 192.168.42.131
255.255.255.255 RETAIL
aaa accounting command RETAIL
```

- **PCI 10.4**—Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:
 - **PCI 10.4.a**—Verify that NTP or similar technology is used for time synchronization
 - **PCI 10.4.b**—Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]
 - **PCI 10.4.c**—Verify that the Network Time Protocol (NTP) is running the most recent version
 - **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.

The FWSM does not have a standalone clock, and it does not support NTP. It relies on the switch clock for time.

PCI Sub-Requirements that Require Compensating Controls (FWSM)

The Cisco FWSM within this solution complied with all relevant PCI sub-requirements and did not require any compensating controls.

Cisco Intrusion Detection System Services Module (IDSM2)

The Cisco® Catalyst® 6500 Series Intrusion Detection System Services Module 2 (IDSM2) is an important intrusion prevention system (IPS) solution that protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows the user to monitor traffic directly off the switch backplane.

General Notes/Best Practices

- Configure IDSM2 to lock accounts so that users cannot keep trying to login after a certain number of failed attempts.
- Allow secure management of IDSM2 only from a specific host/hosts.
- Configure appropriate banner messages on login. The login banner warning should not reveal the identity of the company that owns or manages the IDSM2. The banners should state that these areas are considered private and that unauthorized access will result in prosecution to the full extent of the law.
- Change default passwords and community strings to appropriate complexity.

PCI Sub-Requirements Satisfied by Solution Component (Cisco IDSM2)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- Currently, in IDSM2, there are no current password character class requirements. The sensor uses the PAM cracklib to ensure a harder password.
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*

Account lockout is disabled by default on IDSM2. Account lockout is enabled to a configurable number of failed login attempts starting with 1:

```
! -----
service authentication
attemptLimit 4
exit
! -----
```

- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID
- Lockout duration is not configurable in IDSM2. The user account is locked until an administrator resets it by resetting the user's password.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.4—Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:**
 - **PCI 10.4.a**—Verify that NTP or similar technology is used for time synchronization.
 - **PCI 10.4.b**—Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals (directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)), peer with each other to keep accurate time, and share the time with other internal servers.
 - **PCI 10.4.c**—Verify that the Network Time Protocol (NTP) is running the most recent version.
 - **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>

The following is sample configuration:

QSA recommends that IDSM2 should have NTP configuration independent of the parent router or switch.

```
IDSM2(config-hos)# ntp-option ?
disabled  Disable synchronization of the sensor's clock to an NTP time
server.  Appliance sensors will use their internal hardware clock. Sensor modules will use the
clock of the module's parent router or switch.

enabled   Enable synchronization of the sensor's clock to a NTP (Network Time Protocol) time
server.
```

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4.a**—*Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored.*
- **PCI 11.4.c**—*Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection*

```
!
intrusion-detection module 2 management-port access-vlan 97
intrusion-detection module 2 data-port 1 autostate include

!
!
monitor session 10 source vlan 82 , 97
```

The sub-requirements in this section are satisfied through the IDSM2 configuration on a Catalyst switch combined with monitoring and alerting capability of CS-MARS and Cisco IPS Device Manager (IDM). The IDSM2 is configured in the promiscuous mode in the lab to monitor VLAN 82 (DMZ) and VLAN 97 (inside interface of FWSM).

Cisco Security Manager is used update signatures on the IDSM2.

PCI Sub-Requirements that Require Compensating Controls (Cisco IDSM2)

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
QSA recommends a combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
QSA recommends a combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*
QSA recommends screensaver timeouts can be used as a compensating control, when idle session timeouts are not available or impact application/business operations (e.g. backup jobs).

Cisco Application Control Engine (ACE) Module

The Cisco ACE Module is primarily used for maximizing the availability, acceleration and protection on data center and Internet edge applications. The Cisco ACE Module is not documented in the Auditor's Report of Compliance (ROC) as it was mainly used to load balance ACE XML Gateway appliance but still the ACE Module is treated as a networking device and will have the same recommendations as any other Cisco networking device that have been part of the audit.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data**PCI Sub-Requirements Satisfied by Solution Component (ACE)**

- **PCI 1.3.7**—*Denying all other inbound and outbound traffic not specifically allowed.*

Deny all traffic that are not explicitly allowed.

The following is a sample configuration:

```
ACE2/PCI#
access-list allow2server line 20 extended permit ip any host 192.168.20.3
access-list allow2server line 21 extended permit tcp host 192.168.20.44 host
192.168.42.130 eq ldap
access-list allow2server line 22 extended deny ip any any
access-list in2out line 10 extended permit ip host 192.168.20.3 any
access-list in2out line 15 extended deny ip any any
access-list out2in line 10 extended permit tcp any host 192.168.20.1 eq www
access-list out2in line 15 extended deny ip any any
ACE2/PCI#
```

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)*
- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.2.4**—*Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And**Requirement 8: Assign a Unique ID to each Person with Computer Access**

The text following this list refers to the following sub-requirements for Requirements 7 and 8:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords*
- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the router. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*

Configure the **terminal session-timeout** and **login timeout** commands to 15 minutes or less in Cisco ACE.

Following is a sample configuration:

```
ACE2/PCI# terminal session-timeout 15
ACE2/PCI#
ACE2/PCI# show terminal

TTY: /dev/pts/0 Type: "vt100"
Length: 24 lines, Width: 80 columns
Session Timeout: 15 minutes
ACE2/PCI#
```

```
ACE2/PCI#
!
login timeout 15
!
```



Note

The **login timeout** command setting overrides the **terminal session-timeout** command setting.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS for AAA services.

The Cisco ISR router was not configured or audited for AAA features without the use of CS-ACS.

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

```
ACE2/PCI#
tacacs-server host 192.168.42.131 key 7 <removed>
aaa group server tacacs+ RETAIL
    server 192.168.42.131
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local
```

Application Control Engine (ACE) XML Gateway

The ACE XML Gateway delivers an integrated XML firewall. It ensures that XML messages securely and efficiently reach their intended targets. It provides the critical protection needed at each service perimeter—between un-trusted and trusted zones with a comprehensive XML threat defense system.

General Notes/Best Practices

- While configuring a listening port on Cisco ACE XML Gateway, avoid using ports reserved for non-service traffic. These include ports in the range of 8200 through 8299 or 514, which are used for administrative traffic between system components.
- It is highly recommended to change the default SNMP string *reactivity*. The default SNMP string can be changed by logging to Cisco ACE XML Gateway via command line.
 - [root@AXG1 root]# vi /etc/snmp/snmp.conf
 - [root@AXG1 root]# vi /etc/snmp/snmpd.conf
 - # REACTIVITY 2.0-1
 - com2sec theUser default reactivity

PCI Sub-Requirements Satisfied by Solution Component (Cisco ACE XML Gateway)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)*
- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.5**—*Develop all web applications based on secure coding guidelines, such as the Open Web Application Security Project Guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:*
 - **PCI 6.5.1**—*Unvalidated input*
 - **PCI 6.5.4**—*Cross-site scripting (XSS) attacks*
 - **PCI 6.5.5**—*Buffer overflows*
 - **PCI 6.5.6**—*Injection flaws (for example, structured query language (SQL) injection)*
 - **PCI 6.5.7**—*Improper error handling*
 - **PCI 6.5.9**—*Denial of service*
 - **PCI 6.5.10**—*Insecure configuration management*

For detailed configurations, refer to [Appendix D, “Detailed Implementation and Configuration Steps.”](#)

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to “deny all” unless specifically allowed.*

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data*

This requirement was achieved using LDAP connecting to Microsoft Active Directory. Users are authenticated using LDAP as shown in [Figure 3-2](#).

Figure 3-2 User Authentication

System Management > ACE XML Manager Advanced Settings > LDAP Authentication

LDAP SERVER

Host: 192.168.42.130

Port: 389 Use SSL
(usually 389, or 636 for SSL)

Options: Attempt memberOf-style queries to check group membership (faster, but not supported by all LDAP servers)
 Perform group membership queries with the "Setup Query" user (may be required for some LDAP systems, such as Tivoli)

SETUP QUERY

Bind with DN: CN=Administrator,CN=Users,DC=cisco-irm,DC=com

Password: *****

Base DN: CN=Users,DC=cisco-irm,DC=com

Username Attribute: sAMAccountName (e.g., for Active Directory, use sAMAccountName)

SUB-POLICY-TO-GROUP MAPPING

Sub-policies that are not assigned to LDAP group DNs will only be accessible by Administrator users.

ACE XML Manager Sub-Policies	LDAP Group
Shared	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com

ROLE-TO-GROUP MAPPING

ACE XML Manager Role	LDAP Group
Administrator	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
Policy View	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
Access Control	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
Routing	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
Operations	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
Message Traffic Log	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com
External Developer	CN=Administrators,CN=Builtin,DC=cisco-irm,DC=com

NOTE: External developers logging in via LDAP will only be able to see public handlers

223-837

- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges

- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

PCI Sub-Requirements that Require Compensating Controls (Cisco ACE XML Gateway)

The Cisco ACE XML Gateway within this solution complies with all relevant PCI sub-requirements and did not require any compensating controls.

Wireless Access Points and Controllers

General Notes/ Best Practices

Cisco recommends using the LWAPP architecture for retail wireless deployments because of the Cisco ongoing wireless strategy. The autonomous IOS access points are not being enhanced. Future security and user enhancements will be developed on the LWAPP architecture.

The WCS server version used during this solution audit lacks the capability for external authentication. However, version 4.1 and later supports external authentication via TACACS or RADIUS. For versions prior to 4.1, Cisco recommends a combination of documented password policies, manual audit procedures, and firewall segmentation for WCS servers within the data center.

- Configure unique SSID
- Disable broadcast of the SSID
- Change default passwords and community strings
- Enable WPA technology

PCI Sub-Requirements Satisfied by Solution Component (Unified Wireless: Wireless Access Points, Wireless Controller and Wireless Control System)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

- **PCI 2.1.1**—*For wireless environments, change wireless vendor defaults, including but not limited to, WEP keys, default SSID, passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.*

- Step 1** Verify that the Cisco Controller is configured by default for administrative restriction and AAA authentication for administrative users.
- Step 2** There is no default SSID in the Unified Wireless Architecture. The initial SSID is configured through the controller setup wizard.
- Step 3** Disable/remove default SNMP strings of “public/private”.
- Step 4** Create new community strings:
- ```

config snmp community create <string>
config snmp community mode enable <string>
config snmp community accessmode <ro/rw> <string>

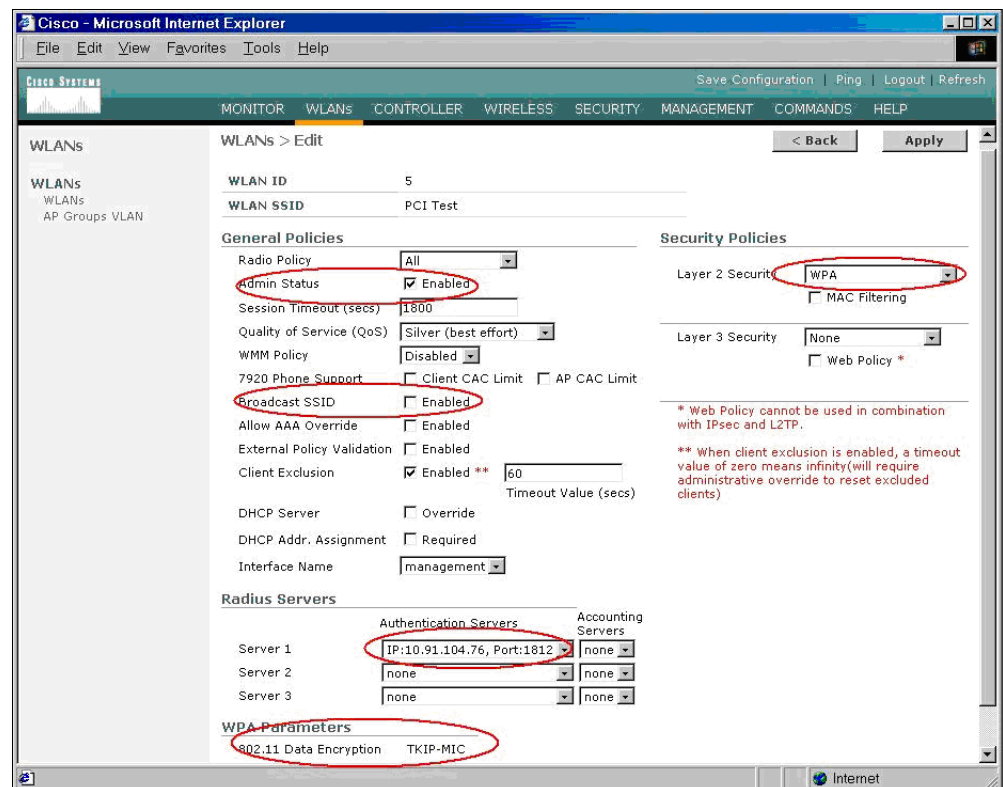
```
- Step 5** Verify that default community strings are no longer accessible.
- Step 6** Configure administrative user either via initial controller setup script or via CLI:
- ```

config mgmtuser add <username> <password> read-write/read-only

```
- Step 7** Configure wireless system for WPA authentication.

Note that SSID Broadcast is enabled by default, but may be disabled. Figure 3-3 shows configuration of WLAN on the Cisco Controller for WPA security using RADIUS client authentication.

Figure 3-3 Configuring Wireless System for WPA Authentication



- Step 8** Verify that WLAN security configuration (SSID broadcast disabled, WEP/WPA in use) is enabled.
- **PCI 2.2.2**—Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).

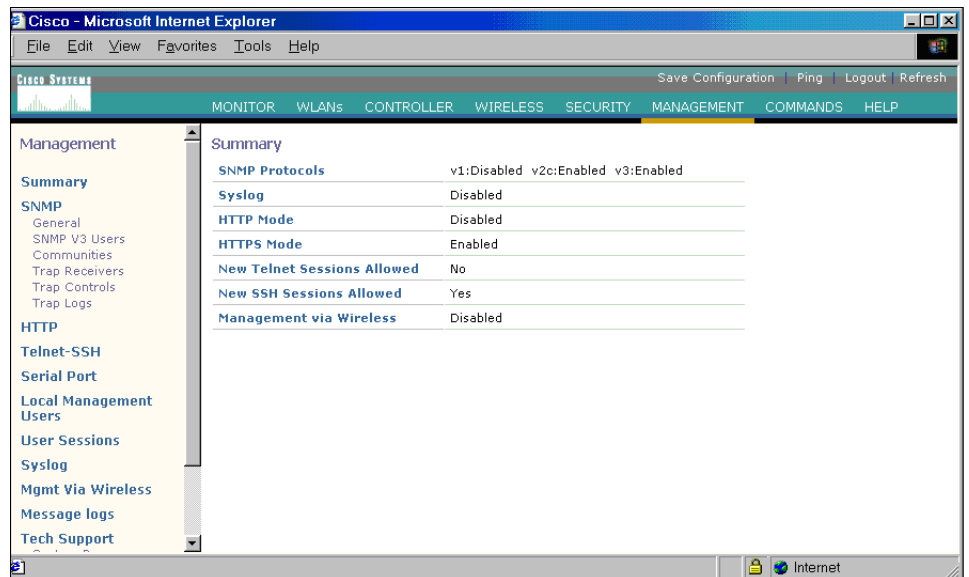
- **PCI 2.2.3**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.
- **PCI 2.2.4**—Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- **PCI 2.3**—Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

Following is a sample configuration:

- Step 1** Verify that the Controller is enabled only for secure management protocols- i.e. HTTPS (SSL) only, Telnet disabled, SNMP v1 disabled, SSH permitted).

Figure 3-4 shows an output from controller “Management> Summary” that shows the controller default settings, which include HTTP disabled, Telnet disabled, and HTTPS (SSL)/ SSH enabled.

Figure 3-4 Controller Default Settings



- Step 2** Verify that administrative access is denied to users accessing over unpermitted interfaces/addresses that are not permitted. Verify that only encrypted protocols are permitted.

- Access points—Configuration to the access point is via the controller with the exception of the console port. Role-based configuration of the console port is defined via the controller.
- Controller—Central management of the controller is the recommended configuration method via WCS. Local management of the controller is configured to authenticate via CS-ACS.
- WCS—The WCS is capable of defining role-based administrator account locally.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

- **PCI 4.1**—Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).

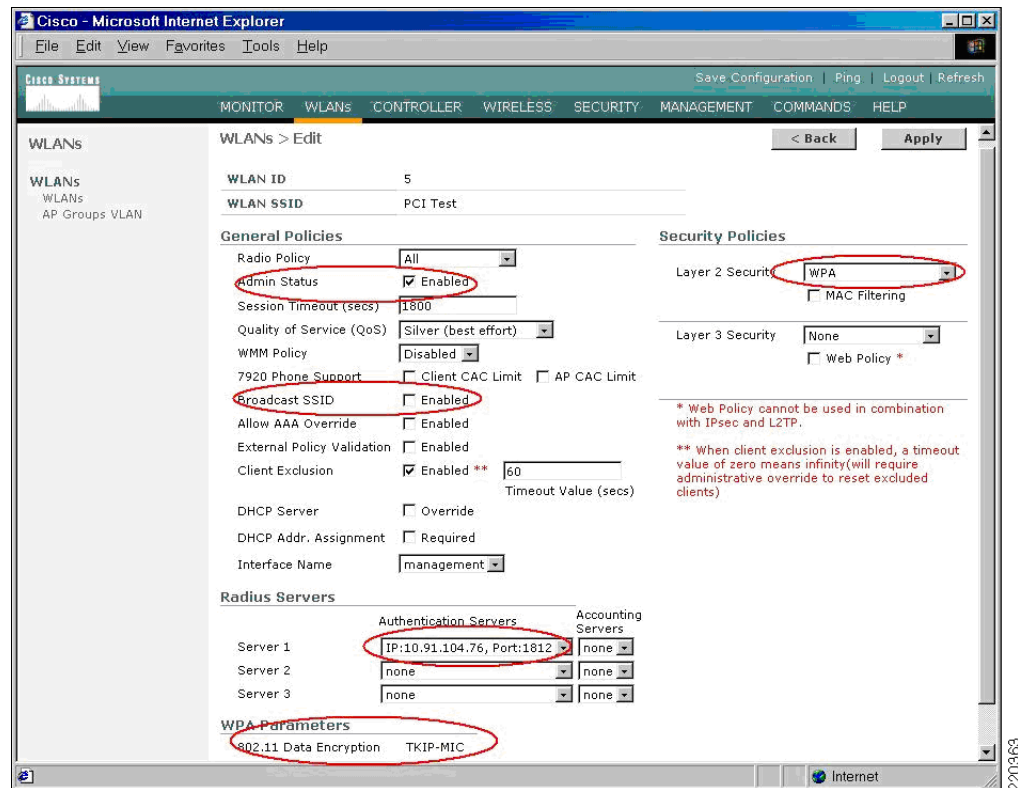
- **PCI 4.1.1**—For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.

If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
 - Use **ONLY** in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
 - Rotate shared WEP keys quarterly (or automatically if the technology permits)
 - Rotate shared WEP keys whenever there are changes in personnel with access to keys
 - Restrict access based on media access code (MAC) address

Step 1 Configure wireless equipment for WPA authentication and encryption. (See [Figure 3-5](#).)

Figure 3-5 Configuring WPA Authentication and Encryption



**Note**

WLAN security data (that is, Pairwise Master Key (PMK used in WPA or WEP key used with 802.1X dynamic WEP) is stored/cached on WLAN controller and only transferred to AP upon client association. Control and configuration traffic between controller and AP is authenticated and encrypted. AES encryption is used on this link.

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

**Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And
Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components.*
- **PCI 8.5.1.b**—*Verify that only administrators have access to management consoles for wireless networks.*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Access points satisfied this requirement because all operation is handled by the controller. Access point console access is configured at the wireless controller.

Controllers satisfied this requirement by using administrator user authentication via RADIUS through CS-ACS.

Wireless clients use RADIUS authentication via CS-ACS prior to enabling encrypted wireless communication.

Wireless Control System (WCS) satisfied requirements PCI 7.2–PCI 8.5.8 by configuring unique user name and passwords on the WCS server itself. WCS did not satisfy 8.5.9–8.5.15 because it does not have a session timeout setting and was not able to take advantage of the CS-ACS via RADIUS. See [PCI Sub-Requirements that Require Compensating Controls \(Wireless Control System\)](#), page 3-38.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

Compliance of the following sub-requirements for access points and controllers was achieved within the solution by implementing the CS-ACS for AAA services.

WCS satisfied these requirements by use of a local user database and corresponding user authentication policy.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*
- **PCI 10.2.3**—*Access to all audit trails*
- **PCI 10.2.6**—*Initialization of the audit logs*

WCS satisfied these requirements by implementation of the CSA client on the WCS server for protection of the local audit trail.

Controllers are configured to use the two NTP servers to satisfy the requirements in this section.

The WCS server satisfied these requirements by configuring the operating system of the WCS server to use NTP.

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
- **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization*
- **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]*
- **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version*

- **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.

The CSA client was applied to the WCS server and configured to monitor the logs and audit trails, to satisfy the following requirements:

- **PCI 10.5.1**—Limit viewing of audit trails to those with a job-related need
- **PCI 10.5.2**—Protect audit trail files from unauthorized modifications
WCS only
- **PCI 10.5.4**—Copy logs for wireless networks onto a log server on the internal LAN.

The controllers are configured to send Syslogs to the CS-MARS appliance.



Note

There is no documented standard for wireless events at this time.

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.1.b**—Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.

The LWAPP unified wireless system has the wireless analyzer capability. Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.

The following is a sample configuration (CLI of Controller):

```
Untrusted AP Policy
Rogue Location Discovery Protocol..... Disabled
  RLDP Action..... Alarm Only
Rogue APs
  Rogues AP advertising my SSID..... Alarm Only
  Detect and report Ad-Hoc Networks..... Enabled
```

PCI Sub-Requirements that Require Compensating Controls (Wireless Control System)

Requirement 8: Assign a Unique ID to each Person with Computer Access

This section applies to WCS server only and not to the wireless controllers or access points.

- **PCI 8.5.9**—Change user passwords at least every 90 days.
- **PCI 8.5.10**—Require a minimum password length of at least seven characters.
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters.
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts.
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

**Caution**

WCS does not support external authentication methods. It was not able to take advantage of the Active Directory, CS-ACS, or other authentication solutions. WCS does not have local individual user password duration enforcement, password complexity, password history or automated failed lockout capability.

Compensating Control for Compliance

The QSA recommends a combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and firewall segmentation for WCS servers within the data center. These would be reasonable compensating controls for password setting limitations within these applications.

The sub-requirements were not met in this lab environment because the data center infrastructure and company policies are not within the scope of the audit, prohibiting deploying the QSA-recommended compensating controls.

PCI Sub-Requirements that Require Compensating Controls (Wireless Controllers)**Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*

**Caution**

The web-based interface of the controllers does not support a 15 minute timeout. The SSH terminal interface of the controller does support the 15 minute timeout.

Compensating Control for Compliance

Cisco recommends disabling the local web-based management of the Wireless Controller. The central WCS server should be used for configuration management of the Wireless Controller.

Adaptive Security Appliance (ASA)**General Notes/Best Practices**

- The ASA is a multi-purpose security appliance that combines firewall, intrusion prevention, and intrusion detection services in small, medium, and large sizes and throughput levels.
- Some retailers use the ASA at the store level because they have an untrusted WAN connection (i.e., Internet or from a managed service provider).
- Many retailers use the ASA in the data center because the larger appliances support very high throughput levels (greater than 1 Gbps). This may be to terminate VPN connections from the store WAN, or from Internet-based VPN connections.
- When using an ASA in the data center or Internet edge, it is recommended that there be separation between the store WAN (and payment traffic) and the Internet direct traffic. In most cases, these are completely separate physical implementations.

- The ASA can be configured easily using the Adaptive Security Appliance Device Manager (ASDM). This graphical interface was used to configure the ASA in this solution. All configuration snapshots are given using the ASDM.
- The Intrusion Protection Service (IPS) v5.1 module on the ASA was managed via the Intrusion Device Manager (IDM) graphical software. All configuration snapshots are given using the IDM interface.

PCI Sub-Requirements Satisfied by Solution Component (Adaptive Security Appliance)

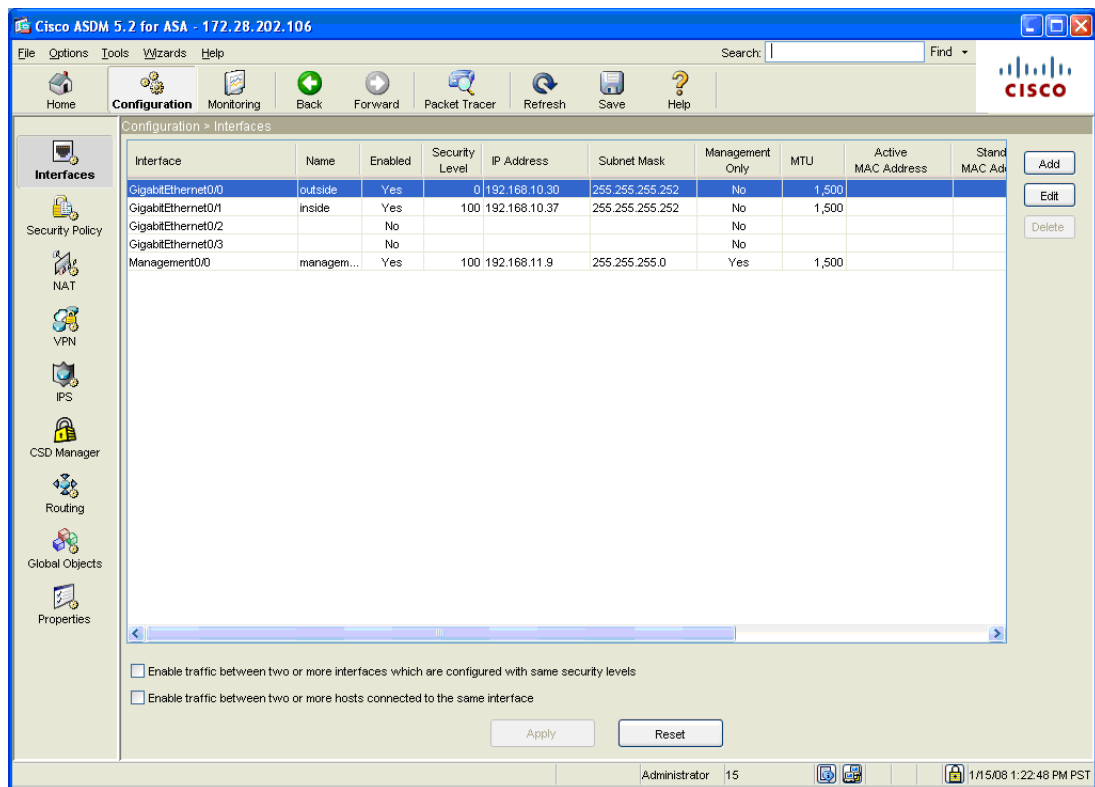
Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.2**—*Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.*

The interfaces on the ASA were configured (see [Figure 3-6](#)) such that the inside interface (LAN-side) had a higher security level than the outside. In this case, the values chosen were 0 and 100, although the values have meaning only relative to each other.

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. The outside network connected to the Internet can be level 0. Other networks, such as DMZs can have values in between. You can assign interfaces to the same security level.

Figure 3-6 ASA Interface Configuration

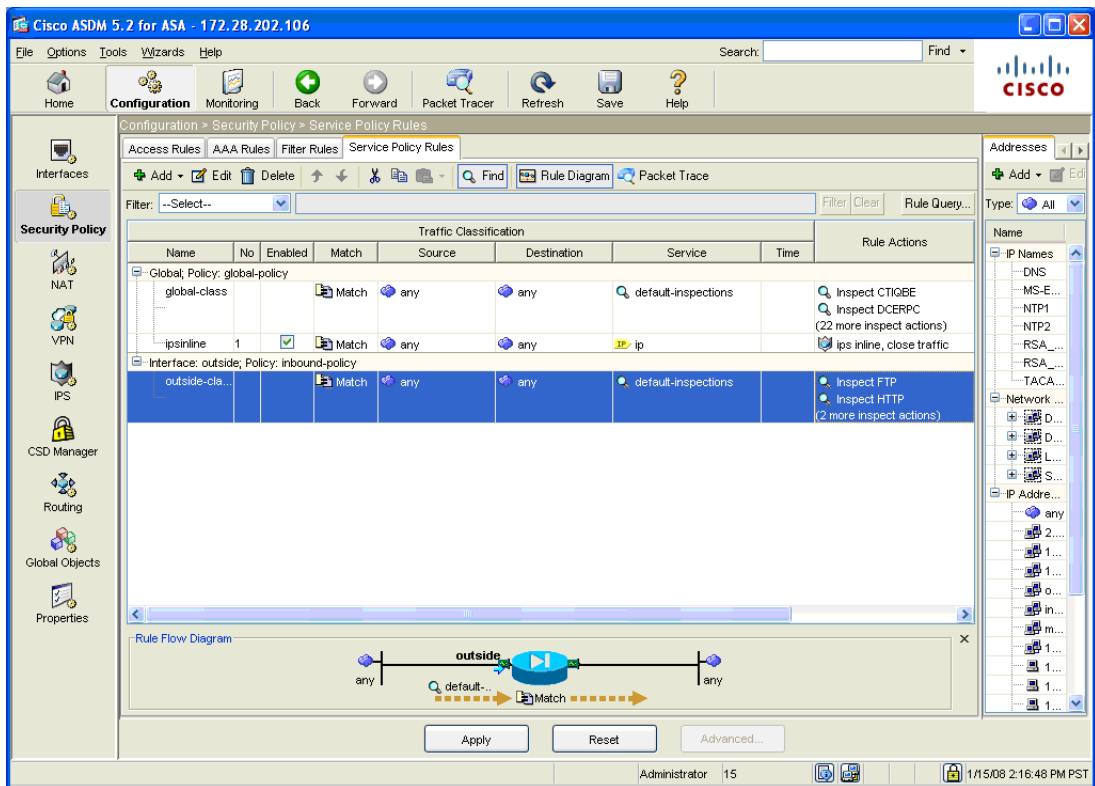


The ASA was configured to allow only the following business-related communication between the large store and the datacenter:

- Management protocols for CiscoWorks Network Compliance Manager (NCM), Cisco Security Manager (CS-M), and CiscoWorks (C-LMS)
- Monitoring, analysis, and response system (CS-MARS)
- Authentication, authorization, and accounting to CS-ACS via TACACS
- Network troubleshooting protocols (ICMP)
- Network Time Protocol (NTP) for time stamp synchronization
- System logging access for network events
- Simple Network Management Protocol (SNMP)
- SSL for secure management access to routers sitting on the outside of the ASA in the WAN aggregation segment of the datacenter as well as the routers and the RSA Key Manager clients sitting in the large store network.
- Dynamic Host Configuration Protocol (DHCP)
- Communication between RSA File Security Manager server and File Security Manager client (TCP ports 19978, 5766)
- Communication between NCR POS systems in the large store and the data center: FTP and SSH.
- **PCI 1.3.3**—*Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network).*
- **PCI 1.3.5**—*Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment.*

The ASA was configured to filter and inspect all traffic inbound from the store branch network (see [Figure 3-7](#)). Through extensive interview and discussion with the QSA, filtering all inbound network traffic was determined to be an acceptable implementation. This effectively restricts the outbound traffic

Figure 3-7 Inspection Rules on ASA Appliance



- **PCI 1.3.7**—Denying all other inbound and outbound traffic not specifically allowed. Deny and log all traffic not explicitly allowed within each firewall rule set.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and other Security Parameters

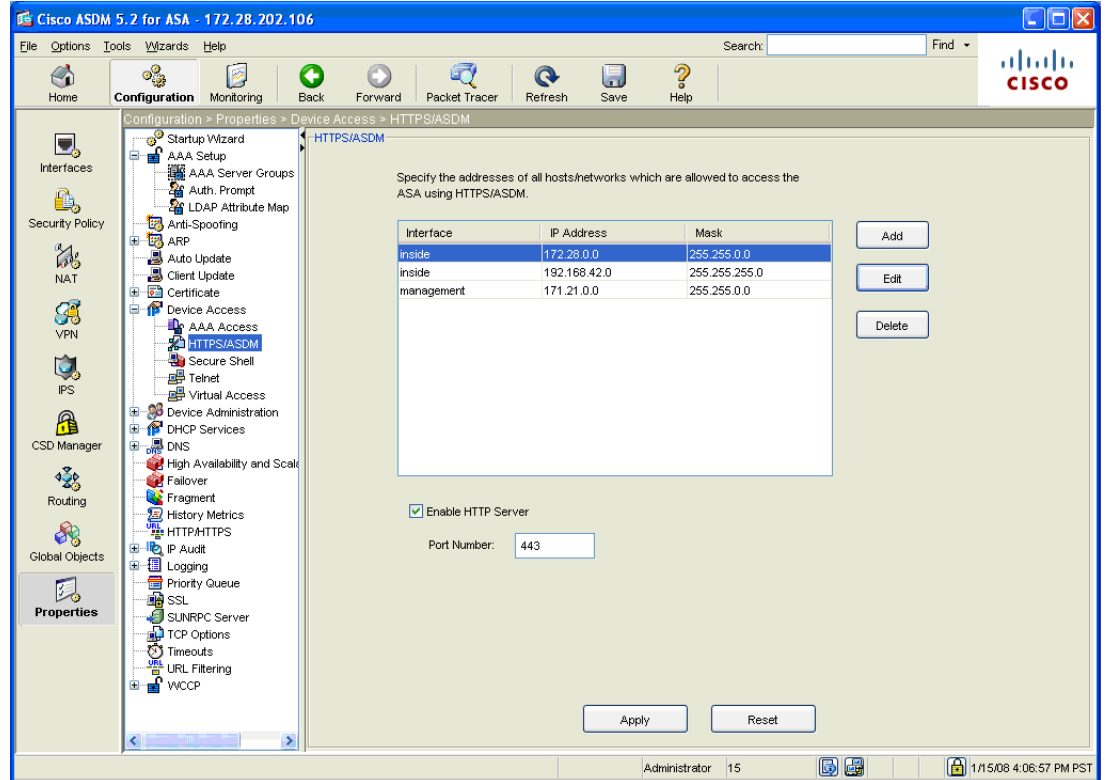
Configure passwords with required complexity and length for local accounts.

The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices’ specified function)
- **PCI 2.3**—Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

HTTPS was enabled on the ASA so all web access to the ASA, including access through the Adaptive Security Device Manager (ASDM) was secure over SSL. With this setting, HTTP access was disabled. SSH access to the ASA was enabled and Telnet access disabled as a result. See Figure 3-8.

Figure 3-8 HTTP and HTTPS Settings on ASA



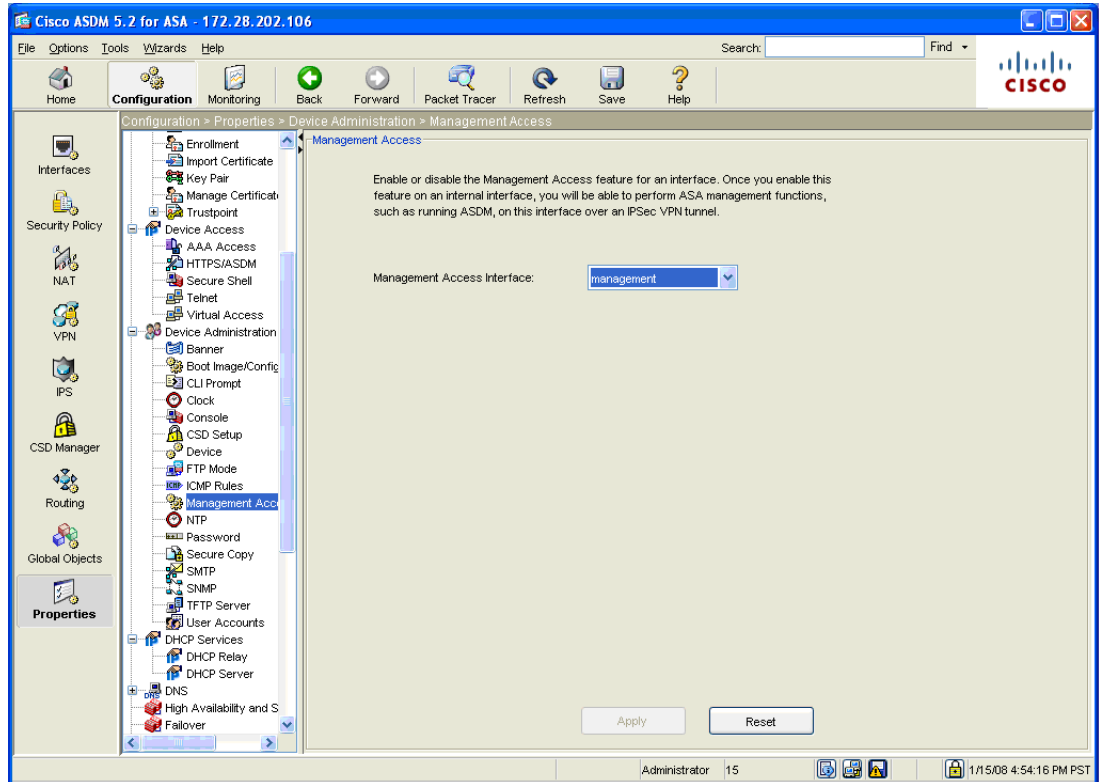
- **PCI 2.2.3.b**—Verify that common security parameter settings are included in the system configuration standards
- **PCI 2.2.3.c**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.

223541

The ASA was configured according to security best practice standards. The following were configured to ensure secure access to the device itself and to harden security for traffic cross the ASA.

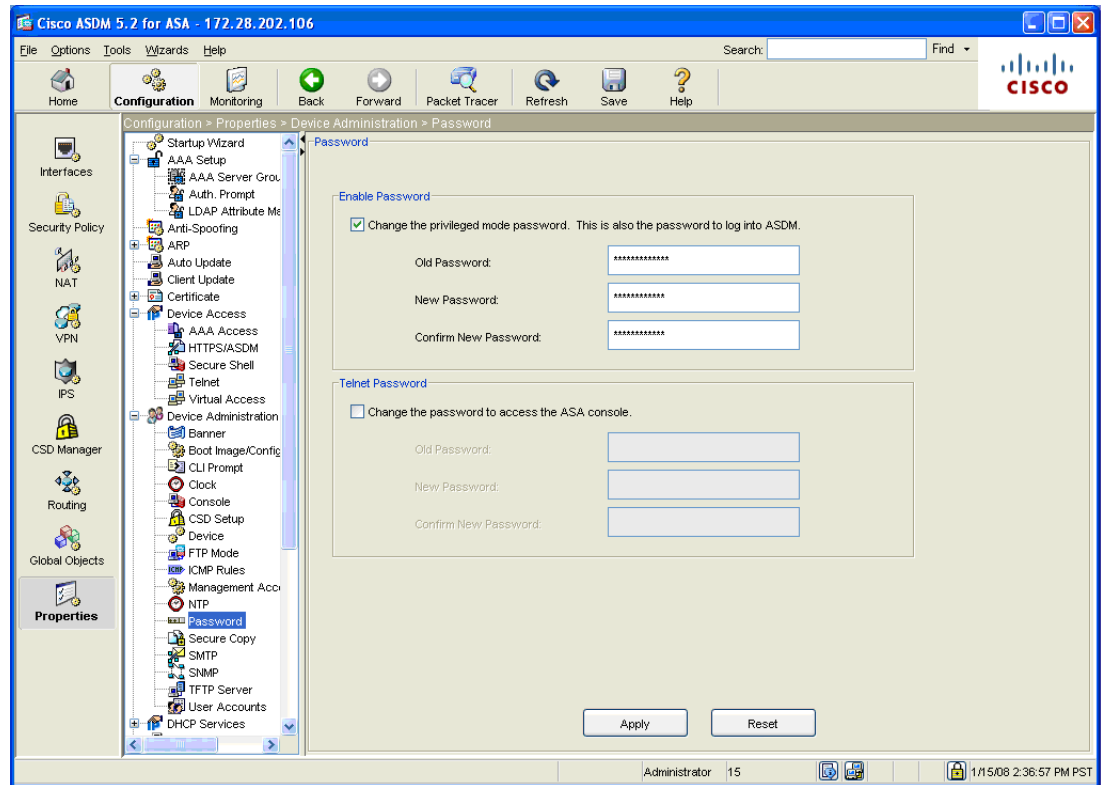
- Anti-spoofing on each interface (Figure 3-9).

Figure 3-9 Anti-Spoofing Configuration on ASA



- Management access limited to the out-of-band management port (see Figure 3-10).

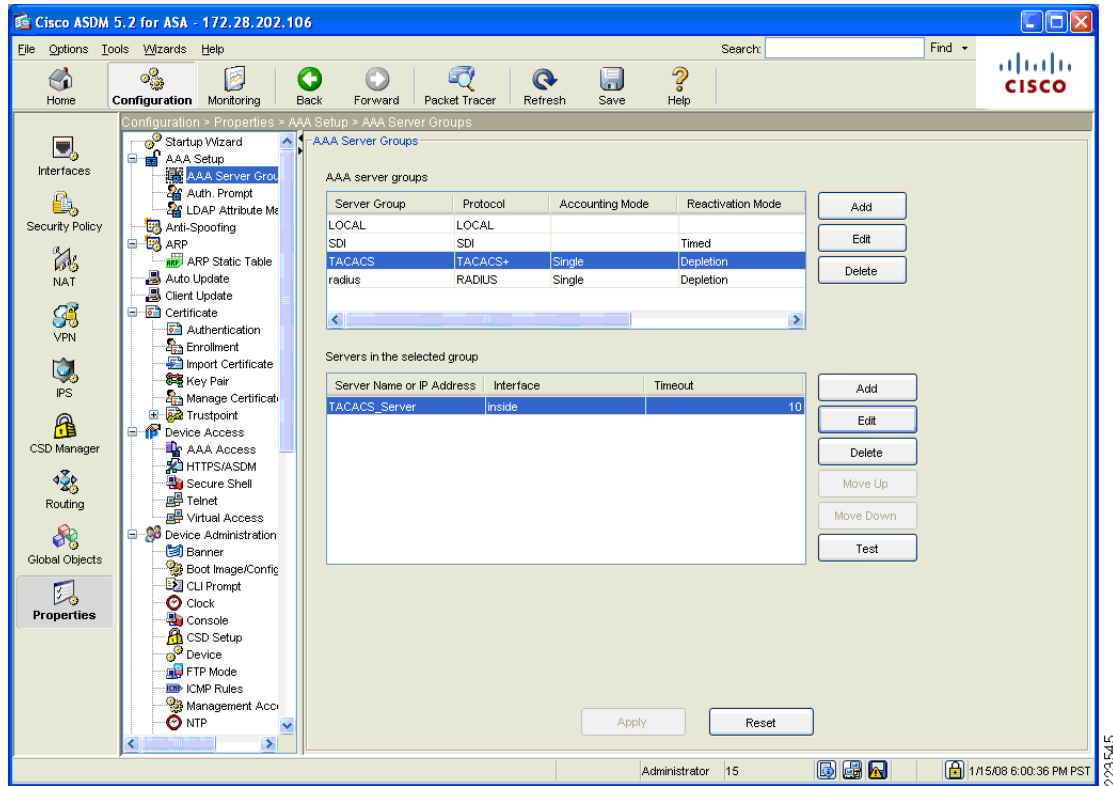
Figure 3-10 Out-of-band Management Setting on ASA



223544

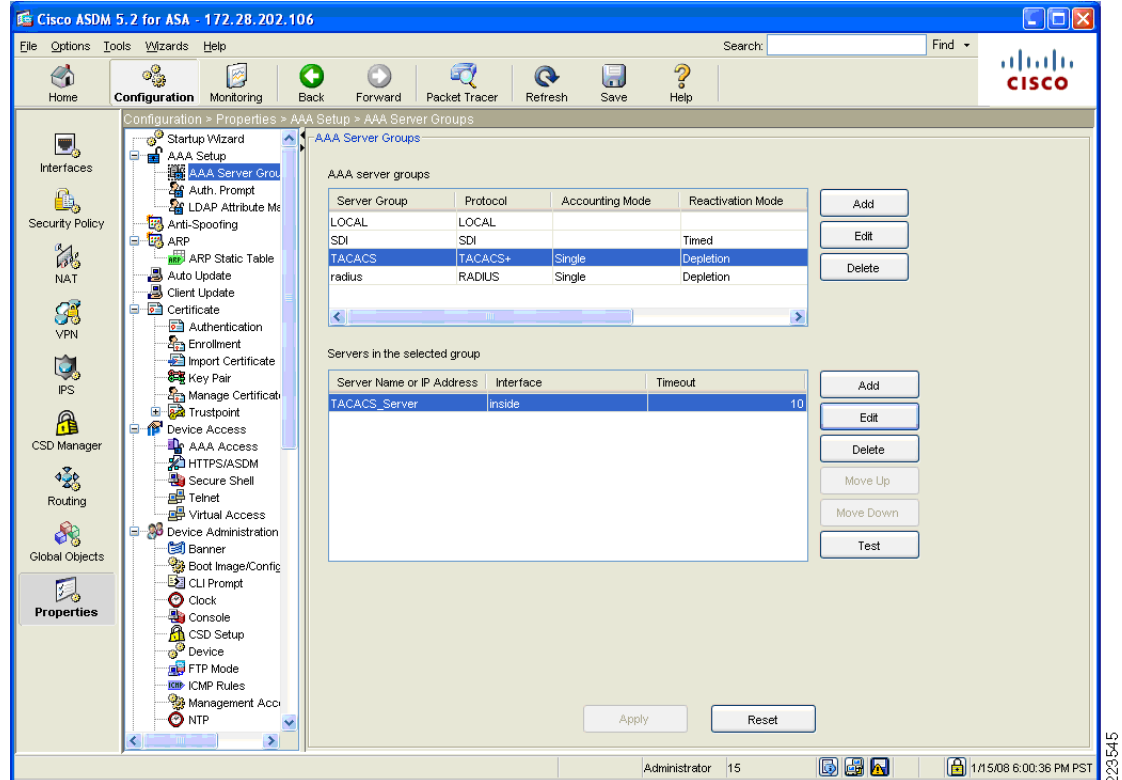
- Default passwords such as enable passwords set to non-default (Figure 3-11).

Figure 3-11 Default Password Configuration on ASA



223545

Figure 3-12 External TACACS Authentication for Requirement 7.2



Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements for Requirements 7 and 8:

- **PCI 7.2**—Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
- **PCI 8.1**—Identify all users with a unique user name before allowing them to access system components or cardholder data.
- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters

- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the ASA. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

Only SSH, Telnet, and console access to the ASA can be configured with a session timeout. In the case, of managing the ASA with ASDM, the workstation on which the ASDM is installed can be configured with a password-protected screensaver set to appear after 15 minutes of idle time. Because of Requirement 2, Telnet should not be used for device management. [Figure 3-13](#) and [Figure 3-14](#) show snapshots of where the timeouts are set via the ASDM for SSH and console session timeouts.

Figure 3-13 Session Timeout for SSH

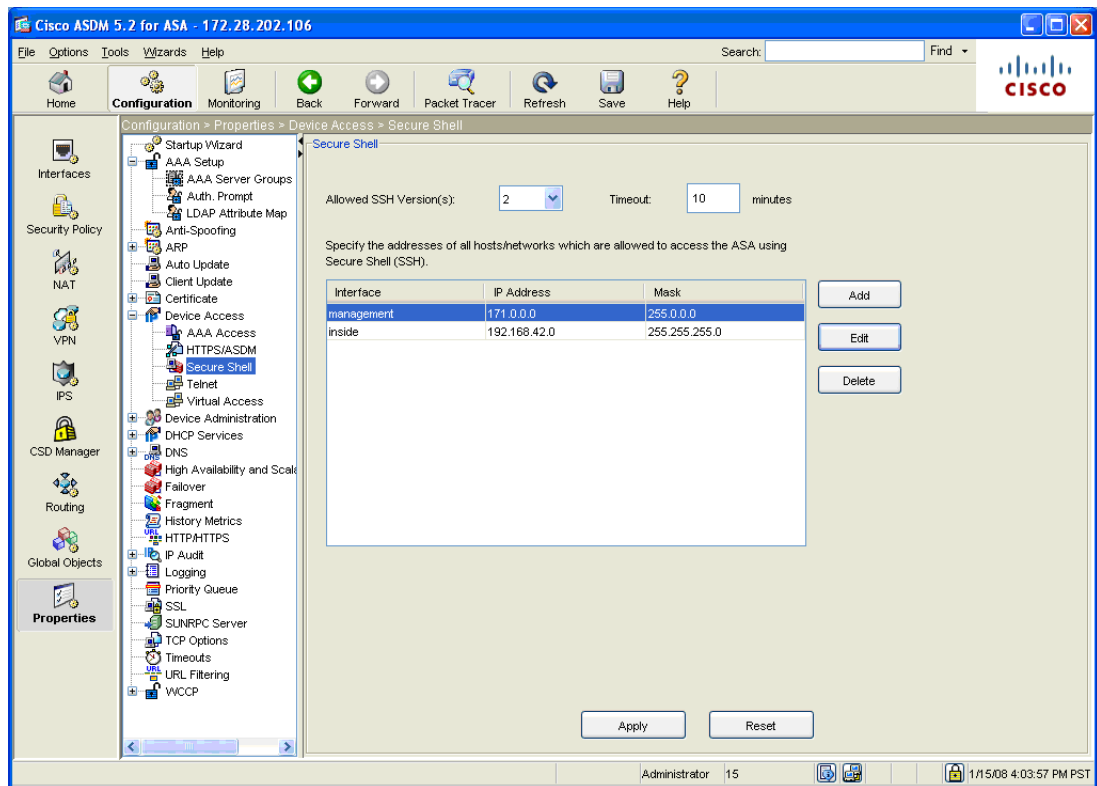
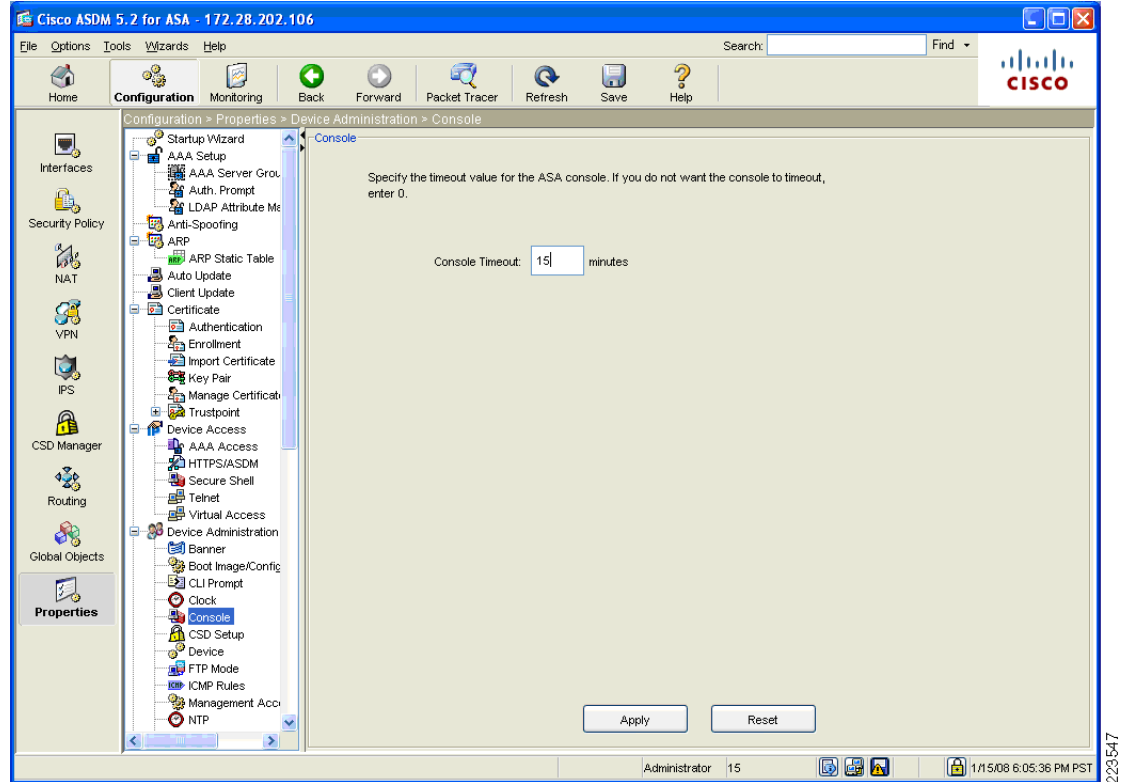


Figure 3-14 Configuring Session Timeout for Console



Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS for AAA services. Time synchronization was configured with central NTP servers and syslogs were configured to be sent to the central CS-MARS server. See Figure 3-15, Figure 3-16, and Figure 3-17 below.

The ASA firewall was not configured or audited for AAA features without the use of CS-ACS.

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

- **PCI 10.4**—Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:
- **PCI 10.4.a**—Verify that NTP or similar technology is used for time synchronization
- **PCI 10.4.b**—Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]
- **PCI 10.4.c**—Verify that the Network Time Protocol (NTP) is running the most recent version
- **PCI 10.4.d**—Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>

Figure 3-15 NTP Server Configured for Requirement 10.4.a.

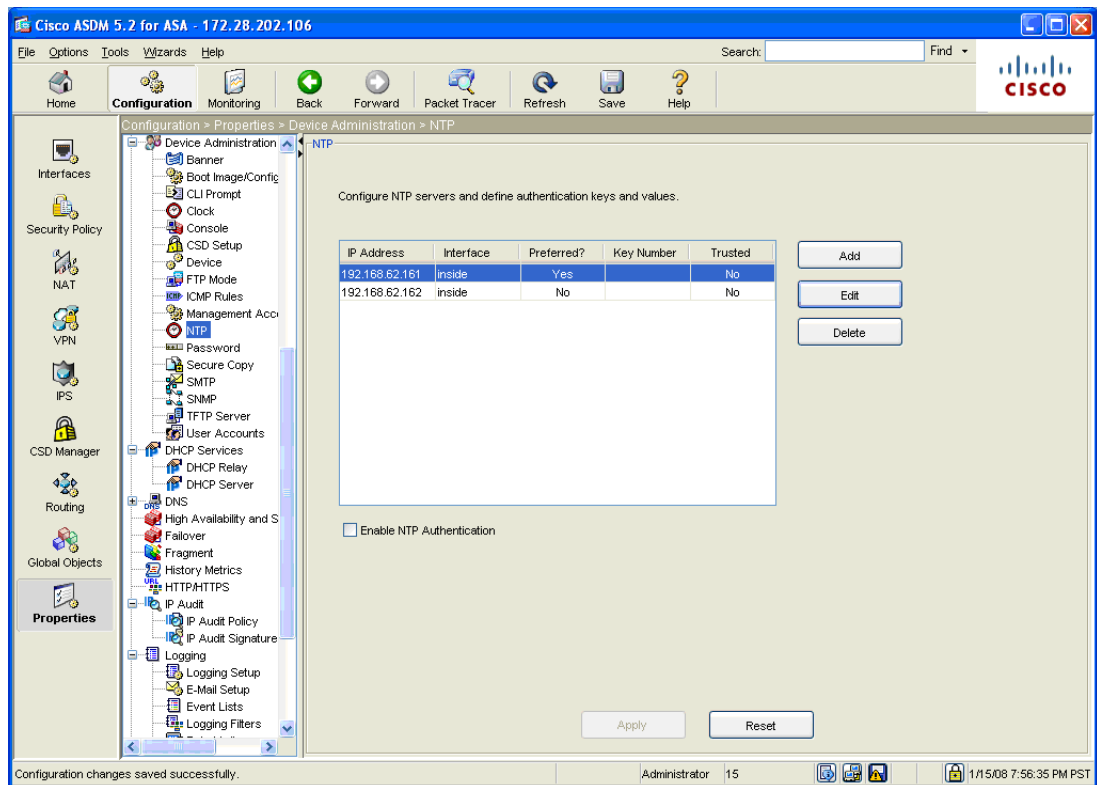


Figure 3-16 Syslog Server Configured to Point at CS-MARS Server

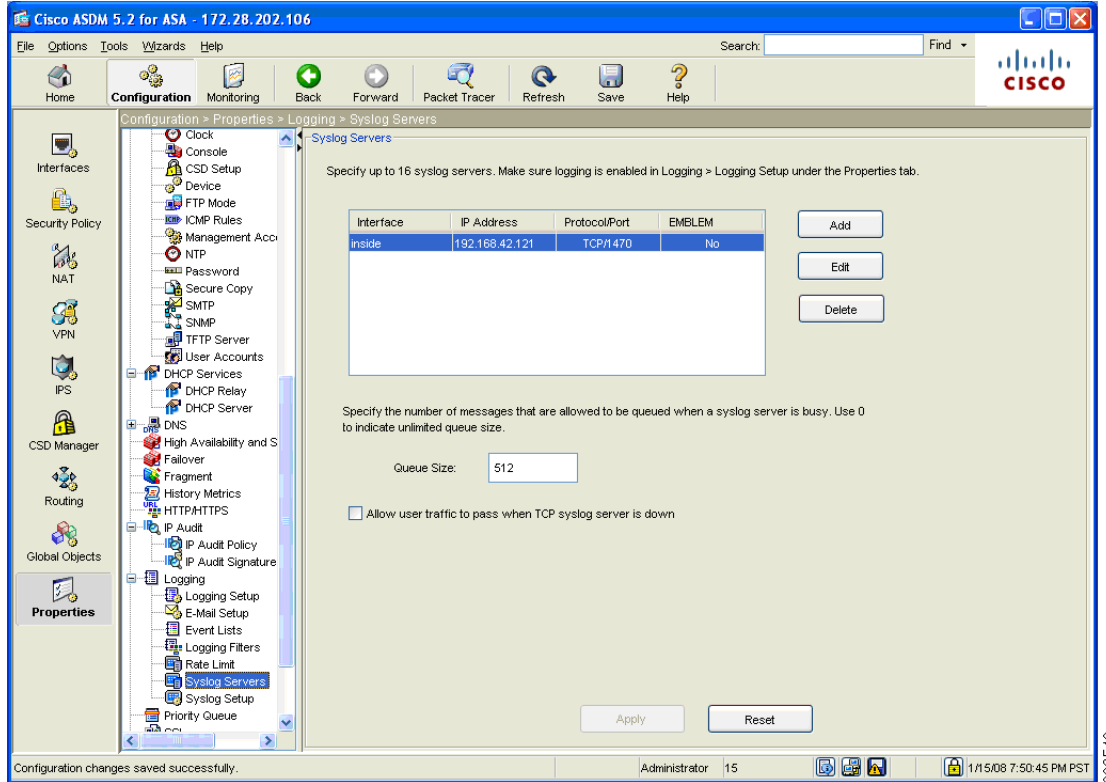
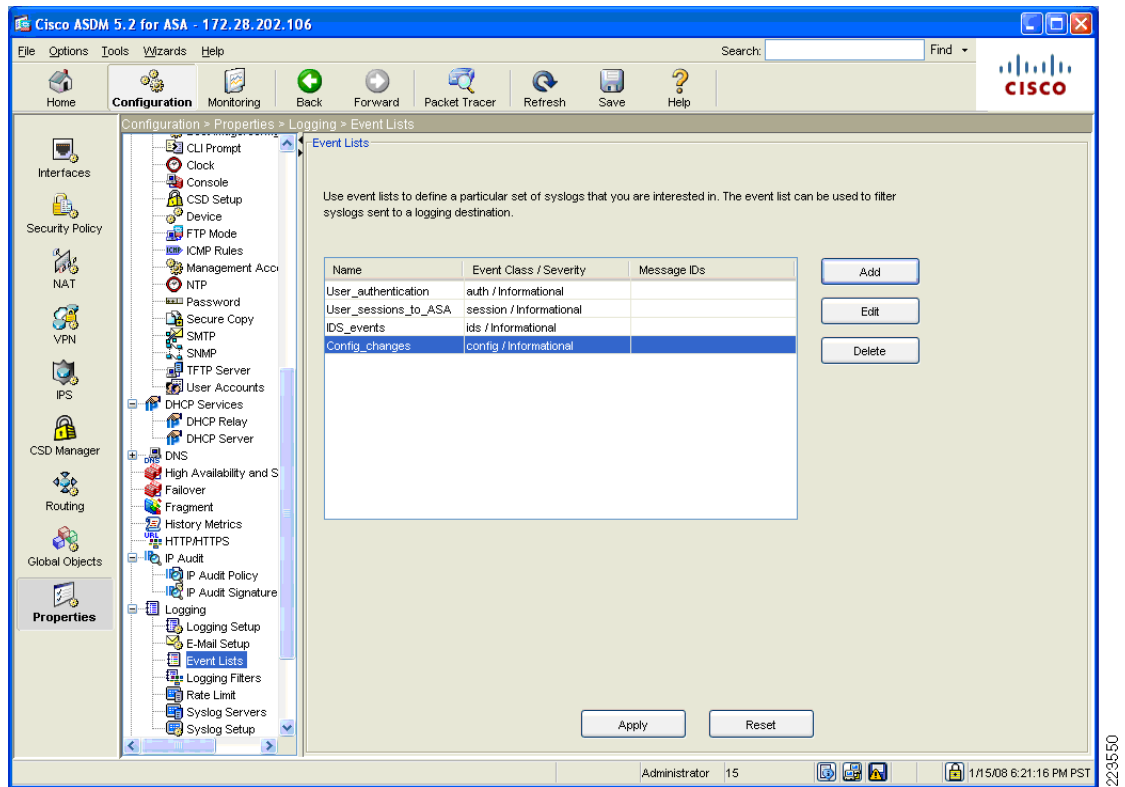


Figure 3-17 Syslog Events Configured for Logging to CS-MARS



- **PC 11.4**—Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

The AIP-SSM-20 module with IPS v5.1 was used for IDS/IPS services on the ASA for traffic between the store branches and the data center. In evaluating the strength of the IDS/IPS system, the QSA considers the following parameters:

- Number of pre-defined signatures available. Typically, the QSA looks at the number as an order of magnitude. In this solution, more than 2000 signatures were available and considered satisfactory.
- Since the IPS module has its own management interface (through the IPS Device Manager), the set of 2.X and 8.X requirements are applied. The following is a listing of the requirements and how the IPS module satisfies them. See [Cisco Intrusion Detection System Services Module \(IDSM2\)](#), page 3-24 for details of how the Device Manager features is mapped to PCI requirements.

VPN Tunnel Configuration on Adaptive Security Appliance (ASA) for Remote Access with Two-Factor RSA SecurID Authentication

General Notes

The ASA in the WAN Aggregation layer was used as the termination point for remote access IPSec VPN tunnels. A Windows client installed with the Cisco VPN client v. 4.0.5 was used as the remote client.

For details on configuring VPN tunnel groups and policies for remote access configurations, refer to the *Cisco ASA 5500 Series Getting Started Guide*, Version 7.2 at the following URL:

http://www.cisco.com/en/US/docs/security/asa/asa72/getting_started/asa5500/quick/guide/remvpn_b.html

System Management

CiscoWorks LAN Management System

The CiscoWorks LAN Management System (C-LMS) provides a network management function that addresses specific PCI 1.1 requirements.

General Notes/Best Practices

C-LMS was installed using the following modules:

- Common services (CS)

CS provides an operating foundation that allows CiscoWorks applications to share data and system resources. It also provides a common desktop for launching CiscoWorks applications and centralizes login, user role definitions, and access privileges.

- CiscoView

CiscoWorks CiscoView is a web-based device management application that provides dynamic status, monitoring, and configuration for a broad range of Cisco devices. CiscoWorks CiscoView aids network management by graphically displaying physical views of Cisco devices, with color-coded modules and ports for at-a-glance performance and status monitoring. Configuration capabilities allow comprehensive changes to devices, when requisite security privileges are granted. CiscoWorks CiscoView offers the following advantages:

- Viewing real-time front and back panel display of Cisco devices
- Monitoring device performance, device environmental status, and mini-Remote Monitoring (mini-RMON)
- Making direct device-configuration changes
- Taking advantage of CiscoWorks LAN Management Solution common device inventory
- Defining granular CS-ACS-authenticated multiple-user access rules

- Campus Manager

CiscoWorks Campus Manager provides powerful tools for configuring, managing, and understanding complex physical and logical Layer 2 infrastructures. CiscoWorks Campus Manager includes the following tools:

- User tracking (and end-host tracking)
- Discrepancy reporting
- Topology services
- VLAN, private VLAN (PVLAN), and VLAN Trunking Protocol (VTP) management
- Spanning-tree management and visualization
- Path analysis
- Data-extraction engine

- Resource Manager Essentials (RME)

CiscoWorks RME provides lifecycle management of Cisco network devices. Designed to reduce human error and eliminate many of the manual tasks associated with maintaining a network, RME helps make Cisco networks the most manageable and available in the world. The RME suite includes the following tools for simplifying the administration of a Cisco network:

- Inventory management
- Device configuration management
- Software image management
- Change audit services
- Syslog analysis

- Device Fault Manager (DFM)

CiscoWorks DFM performs real-time fault analysis of Cisco devices. Through a variety of data collection and analysis techniques, CiscoWorks DFM generates intelligent traps, which can be forwarded to other event management systems installed in the network, sent to e-mail/pager gateways, or displayed in the DFM alarm window. DFM features include the following:

- Problem-focused fault analysis
- Integration with the CiscoWorks desktop and server
- Integration with enterprise management systems
- Support for Layer 2 and Layer 3 Cisco devices
- Incremental device support

CiscoWorks Common Services was configured with Server > Security Browser_server_security_mode enabled. In addition, CS-ACS AAA mode is selected as the authentication option.

Figure 3-18 shows a sample configuration.

Figure 3-18 Common Services Configuration

The screenshot displays the CiscoWorks Common Services interface in Microsoft Internet Explorer. The browser window title is "Security Settings - Microsoft Internet Explorer". The address bar shows the URL "https://ciscoworks/cwhp/classic.SecuritySettings.do". The page header includes the Cisco Systems logo and the text "Common Services". Below the header, there are navigation tabs for "Home", "Server", "Software Center", "Device and Credentials", and "Groups". The "Server" tab is selected, and the "Security" sub-tab is active. The breadcrumb trail reads "You Are Here > Server > Security".

The main content area is titled "Security Settings". On the left, there is a "TOC" (Table of Contents) menu with the following items:

- > Single-Server Management
 - Browser-Server Security Mode Setup
 - Local User Setup
 - Certificate Setup
- > Multi-Server Trust Management
 - Peer Server Account Setup
 - System Identity Setup
 - Peer Server Certificate Setup
 - Single Sign-On Setup
 - AAA Mode Setup
- > Cisco.com Connection Management
 - Cisco.com User Account Setup
 - Proxy Server Setup

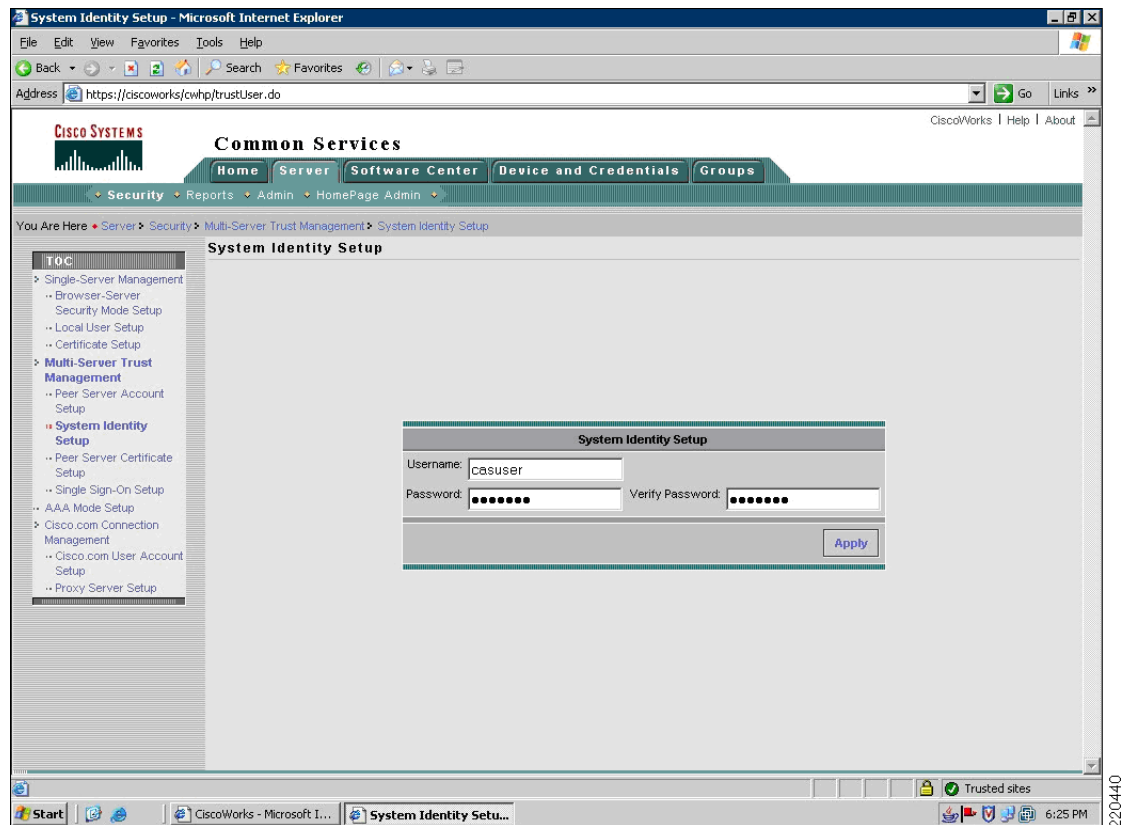
The main content area displays a table titled "Current Settings" with the following information:

Current Settings	
Browser-Server Security Mode:	Enabled
AAA Mode Setup:	TACACS+
Single Sign-On:	Standalone
Proxy Server:	Server not configured
Self Signed Certificate:	Found and Valid

The Windows taskbar at the bottom shows the Start button, several open applications including "CiscoWorks - Microsoft I..." and "Security Settings - Mi...", and the system tray with the time "6:24 PM" and date "22/04/08".

Change the system identity user as shown in Figure 3-19.

Figure 3-19 System Identity Username Configuration



CiscoWorks can be used to update routers and switches to meet required timelines for PCI 6.1.

PCI Sub-Requirements Satisfied by Solution Component (C-LMS)

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

- **PCI 1.3.6**—*Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted), should have the same, secure configuration.*

C-LMS maintains a database of configuration files in a highly secure manner. The suite is capable of alerting administrators of configuration file synchronization issues. The system is also able to correct synchronization inconsistencies (RME). Cisco provides additional value because the switches are capable of this feature as well as the routers.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.*

The management console was configured to support HTTPS access, with HTTP access disabled. CiscoWorks is configured to use SSL as a highly secure management portal technology, and uses SSH and SNMPv3 as primary configuration protocols.

Role-based administration was configured for administrative tasks.


Note

Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

- **PCI 6.2 (6.2b)**—*Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.*

C-LMS can aid in the execution of a configuration change process by maintaining a history of system configuration changes of routers and switches and alerting operators when changes are made. C-LMS also has the capability of defining exception periods during which no configuration changes are made. Exceptions will be noted in the exception report.

C-LMS can also ensure baseline configuration information is consistent and static. Using baseline templates (RME > Archive Management), configuration templates can be developed to enforce mandatory configuration aspects. Changes to these mandatory items can result in the triggered assertion of the selected template, updating the device configuration to include the mandatory items.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And

Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*

- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID

Compliance of these sub-requirements was achieved within the solution by implementation of CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the C-LMS console. These fallback accounts should be rotated based on a QSA-recommended policy.

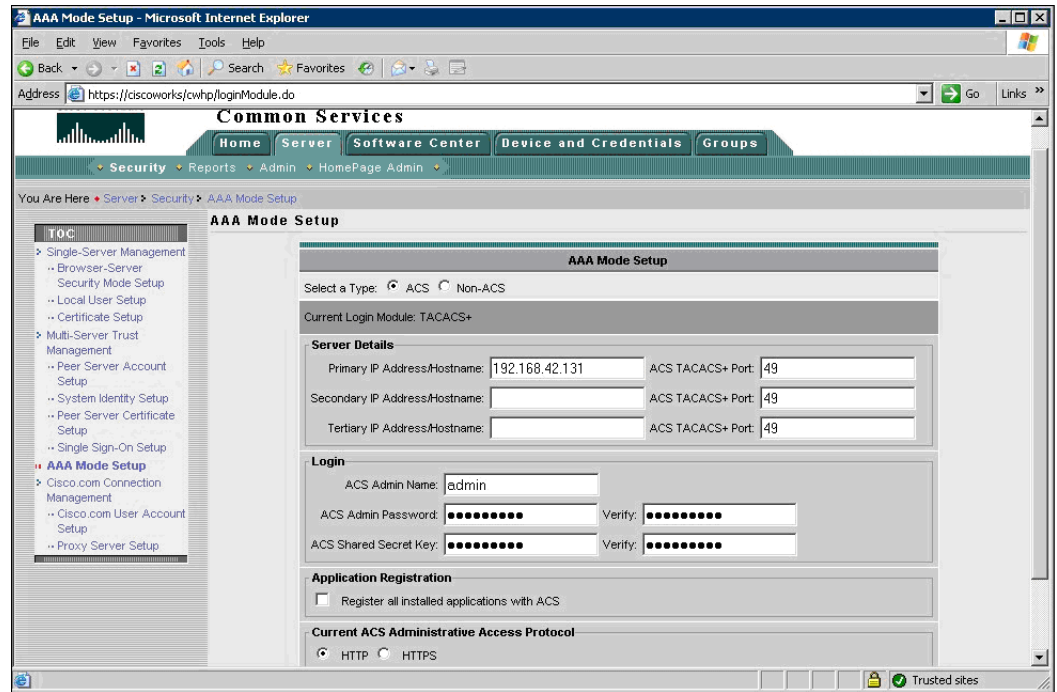
Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

The text following this list refers to the following sub-requirements:

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

Compliance of these sub-requirements was achieved within the solution by implementing the CS-ACS for AAA services. (See [Figure 3-20](#).)

Figure 3-20 AAA Mode Setup



Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.*

C-LMS has the capability of a local 15-minute timeout to satisfy this requirement.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

Compliance of these sub-requirements was achieved within the solution by implementing the CS-ACS for AAA services. (See [Figure 3-18](#).)

- **PCI 10.2.3**—*Access to all audit trails*
- **PCI 10.2.6**—*Initialization of the audit logs*

C-LMS satisfied these requirements by implementation of the CSA client on the C-LMS server for protection of the local audit trail.

The following requirements were satisfied by configuring the operating system of the C-LMS server to use NTP:

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization.*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

The CSA client was installed on the C-LMS server and configured to monitor the logs and audit trails to satisfy this requirement.

PCI Sub-Requirements that Require Compensating Controls (C-LMS)

The C-LMS did not require any compensating controls to pass respective PCI sub-requirements.

Cisco Security Manager

The Cisco Security Manager is a powerful yet easy-to-use solution for configuring firewall, VPN, and IPS policies on Cisco security appliances, firewalls, routers, and switch modules.

General Notes/Best Practices

- Use descriptive notes for each rule set. These are displayed as remarks in the running configuration.
- Virtualize firewall rule set deployment by using a consistent interface naming standard.
- Apply the anti-spoofing feature to all interfaces using FlexConfig.

Following is a sample configuration:

```
## Iterate on the interface names and for each give the following template to prevent DoS
attacks
#if($SYS_INTERFACE_NAME_LIST != [])
  #foreach ($int in $SYS_INTERFACE_NAME_LIST)
    #if (($int != "Tunnel0") && ($int != "Tunnel1") && ($int != "Loopback0"))
      interface $int
        no ip directed-broadcast
        no ip mask-reply
        ip verify unicast source reachable-via rx
      exit
    #end
  #end
#end
```

PCI Sub-Requirements Satisfied by Solution Component (CS-M)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, SNMP community strings, and elimination of unnecessary accounts).

Configure passwords with required complexity and length for local accounts.

See [Appendix E, “Device Configurations.”](#)

- **PCI 2.2.3.c**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.
- **PCI 2.3**—Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

The management console was configured to support HTTPS access, with HTTP access disabled. CS-M is configured to use SSL as a highly secure management portal technology, and uses SSH and SNMPv3 as primary configuration protocols.

Role-based administration was configured for administrative tasks.



Note

Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - *Password*
 - *Token devices (for example, SecureID, certificates, or public key)*
 - *Biometrics*
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords*
- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID*

Compliance of these sub-requirements was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to the C-LMS console. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*

CS-M has the capability of a 15-minute timeout to satisfy this requirement.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.4**—*Invalid logical access attempts*

- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.7**—*Creation and deletion of system-level objects*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

Compliance of these sub-requirements was achieved within the solution by implementing the CS-ACS for AAA services.

- **PCI 10.2.3**—*Access to all audit trails*
- **PCI 10.2.6**—*Initialization of the audit logs*

CS-M satisfied these requirements by implementation of the CSA client on the CS-M server for protection of the local audit trail.

The following requirements were satisfied by configuring the operating system of the CS-M server to use NTP:

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization.*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

The CSA client was installed on the CS-M server and configured to monitor the logs and audit trails to satisfy this requirement

PCI Sub-Requirements that Require Compensating Controls (CS-M)

The Cisco Security Manager did not require any compensating controls to pass respective PCI sub-requirements.

CSA Manager

The Cisco Security Agent (CSA) Manager manages the CSA that delivers application firewall, file integrity, and host intrusion prevention services.

General Notes/Best Practices

- Install the CSA client on all servers and workstations for supported operating systems
- Configure policies to monitor audit trails and logs of respective servers

PCI Sub-Requirements Satisfied by Solution Component (CSA Manager)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts. (See [Appendix E, “Device Configurations.”](#))

- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.*

The management console was configured to support HTTPS access, with HTTP access disabled. CSA Manager is configured to use SSL as a highly secure management portal technology, and uses SSH and SNMPv3 as primary configuration protocols.

Role-based administration was configured for administrative tasks.



Note

Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

Requirement 5: Use and Regularly Update Anti-virus Software or Programs

- **PCI 5.1**—*Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers).*



Note

Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.

- **PCI 5.1.1**—*Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.*
- **PCI 5.2**—*Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.*

A/V software was installed on Windows systems. The assessment focus for PCI A/V requirements depended on Cisco Security Agent software and its ability to meet the intent of A/V requirements. Cisco Security Agent software is installed on all system components commonly affected by viruses, including the following:

- CS-ACS console
- WCS console
- C-LMS console
- CSA console
- CS-M console

Although Verizon Business recommends anti-virus software be installed on the above system components, CSA software can be used, in conjunction with additional compensating controls, to mitigate the majority of common anti-virus risks.

Verizon Business reviewed vendor documentation and observed a demo of the capabilities of CSA to provide layered security through multiple security controls. The PCI Solution for Retail environment implementation addresses the following AV requirements:

- A central (master) console for CSA exists in the PCI Solution for Retail environment, which centrally manages all CSA client policies.
- Log generation is enabled and alerts/logs are centrally stored within CSA and CS-MARS. The retention period is determined by the merchant/service provider. However, because such alerts can be vital for audit trail construction, Verizon Business recommends retaining CSA alerts for at least one year, commensurate with PCI audit trail requirements.



Note

Because POS environments vary with each vendor, a full assessment of the POS environment, Internet/e-mail connectivity to the POS environment, corporate connectivity to the POS environment, and all compensating controls need to be made for each merchant, to make an “In Place/Not in Place” assessment (if CSA software is used as a compensating control for anti-virus software).

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements:

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - *Password*

- Token devices (for example, SecureID, certificates, or public key)
- Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID

Compliance of these sub-requirements was achieved within the solution by implementing the LDAP authentication to Microsoft Active Directory for user account services.

Fallback authentication: In the event of LDAP authentication failure, CSA Manager was configured with local role-based accounts. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

CSA Manager has the capability to support a 15-minute timeout.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.3**—Access to all audit trails
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.2.6**—Initialization of the audit logs
- **PCI 10.2.7**—Creation and deletion of system-level objects
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

Compliance of these sub-requirements was achieved within the solution by implementation of the following:

- Active Directory (AD) authentication logs (authentication requests sent directly to AD).
- All CSA logs, alerts/events sent to CSA Manager.

- Local audit trail for CSA management.
- CSA Manager has the CSA client installed.
- CSA is configured to monitor access to all files containing cardholder data.

The following requirements were satisfied by configuring the operating system of the CSA Manager server to use NTP:

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization.*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*
- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.5**—*Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).*

CSA software is used to monitor and protect access to audit trail files, and alert on unauthorized attempts to modify the audit trail (only application services responsible for writing log data can write/modify/delete the audit trail). Cisco has created an additional backup script to copy the audit trail to a central backup server, where CSA protection has been applied to eliminate all access, modification, and deletion, except for the account responsible for backing up the audit trail.

- **PCI 10.6.a**—*Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.*
- **PCI 10.6.b**—*Through observation and interviews, verify that regular log reviews are performed for all system components.*

CSA performs correlation and analysis of system events, and is configured to alert on those events, warranting immediate action.



Note

Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions (responsibility of the merchant/service provider).

Requirement 11: Regularly Test Security Systems and Processes

- **PCI 11.4.a**—*Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored.*
- **PCI 11.4.b**—*Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises.*
- **PCI 11.4.c**—*Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.*

Cisco CSA (host-based IDS/IPS) is installed on management consoles (for example, CS-M, C-LMS, CSA console, CS-ACS, and WCS console).

CSA is configured to monitor and alert personnel of suspected compromise.

CSA (host-based IDS/IPS) does not rely on signatures, but is behavior-based, eliminating the need to update signatures.

- **PCI 11.5**—*Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.*

Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).

Application of the CSA client to each of the management consoles (C-LMS, CS-M, CSA Manager, WCS, Active Directory) satisfied this requirement for those servers. CSA logs and alerts on attempted access, regardless of whether it is allowed or denied. CSA also logs and alerts on critical file modification.

PCI Sub-Requirements that Require Compensating Controls (CSA Manager)

CSA Manager did not require any compensating controls to pass respective PCI sub-requirements.

Cisco Security Monitoring, Analysis and Response System (CS-MARS)

CS-MARS is an appliance-based, all-inclusive solution that allows network and security administrators to monitor, identify, isolate, and counter security threats.

General Notes/Best Practices

- The PADMIN account cannot be deleted from the CS-MARS appliance. This account should be configured with appropriate password security and distributed only to authorized staff. It should not be used for configuration.
- The version of CS-MARS appliance used during the audit lacks the capability for external authentication; however, v 4.3 and later of CS-MARS supports external authentication via RADIUS. Cisco recommends a combination of documented password policies, manual audit procedures and firewall segmentation within the datacenter for the version of CS-MARS used for this solution audit and for prior versions not supporting RADIUS authentication.
- CS-MARS should be configured to store its audit logs and database to an external NFS server storage facility.
- CS-MARS does not enforce adequate password strength and complexity. A security policy needs to be enforced when developing management passwords.

PCI Sub-Requirements Satisfied by Solution Component (CS-MARS)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts.

- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.*

CS-MARS supports secured communication only through HTTPS and SSH.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And**Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*
- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - *Password*
 - *Token devices (for example, SecureID, certificates, or public key)*
 - *Biometrics*
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components.*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords.*

CS-MARS allows the configuration of unique users and passwords. However, the PNADMIN account is a general administrator account that cannot be deleted. The default password must be changed on this account and stored in a secure location to prohibit the use of a general account.

CS-MARS does not allow alternative or external authentication methods. It cannot be configured to authenticate to CS-ACS or Active Directory.

CS-MARS uses AES encryption method for its passwords.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.2.3**—*Access to all audit trails*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.2.6**—*Initialization of the audit logs*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

Individual role-based user authentication logs are local (no CS-ACS or AD authentication available).

CS-MARS receives CSA logging/alerts, CS-M security events, ISR firewall logs, and IDS/IPS alerts.

There is a local audit trail for CS-MARS.

Audit log files backed up daily to an NFS backup server are monitored by CSA, and all processes and users (except the application processes responsible for writing data to the NFS server) are prohibited from modifying or deleting files from this directory.

CSA alerts are generated, sent to the CS-MARS central server, and an e-mail alert is sent to the administrator e-mail account.

The following requirements were satisfied by configuring the CS-MARS appliance to use NTP:

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization.*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*

Following is a sample configuration:

```
[pnadmin]$ ntp ?

Usage : ntp server [ntp server1] [ntp server2]

        ntp sync

        ntp disable

[pnadmin]$ ntp server ntp1.retailpcilab.local ntp2.retailpcilab.local

Thu Jan 11 12:54:41 PST 2007

[pnadmin]$
```

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*
- **PCI 10.5.3**—*Promptly back up audit trail files to a centralized log server or media that is difficult to alter.*

CS-MARS has centrally stored audit logs.

CS-MARS logs are archived once an hour and sent to a central NFS server running CSA software.

- **PCI 10.5.4**—*Copy logs for wireless networks onto a log server on the internal LAN.*

Wireless Syslogs are sent to CS-MARS central servers from the Wireless Controllers. CS-MARS does not have predefined event triggers for wireless logs. They need to be manually defined based on customer requirements.

- **PCI 10.6.a**—*Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required.*
- **PCI 10.6.b**—*Through observation and interviews, verify that regular log reviews are performed for all system components.*

CS-MARS performs correlation and analysis of system events, and alerts on those warranting immediate action.

**Note**

Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions (the responsibility of the merchant/service provider).

PCI Sub-Requirements that Require Compensating Controls (CS-MARS)

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.*

**Caution**

CS-MARS does not have individual user password duration enforcement, password complexity, password history, or automated failed lockout capability. CS-MARS does not support external authentication methods. It was not able to take advantage of the Active Directory, CS-ACS, or other authentication solutions.

Compensating Control for Compliance

The QSA recommends a combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and firewall segmentation for CS-MARS servers within the data center. These would be reasonable compensating controls for password setting limitations within these applications.

The sub-requirement was not met in this lab environment because the data center infrastructure and company policies are not within the scope of the audit, prohibiting deploying the QSA-recommended compensating controls.

CiscoSecure Access Control Server (CS-ACS)

The CS-ACS provides secured authentication service for ISRs, switches, wireless APs, wireless controllers, C-LMS, and CS-M.

General Notes/Best Practices

- CS-ACS has been configured to authenticate individual users using Active Directory (AD). This is accomplished by creating user groups in AD and mapping them to role-based groups in CS-ACS. This provides the granularity of secure authentication needed to address the PCI specification.
- The solution used the windows versions of CS-ACS. CSA client was installed to protect and alert on unauthorized access of the log and audit trail.
- Remove the default accounts for administration.
- Enable HTTPS and disable HTTP.

PCI Sub-Requirements Satisfied by Solution Component (CS-ACS)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

- **PCI 2.1**—*Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).*

Configure passwords with required complexity and length for local accounts. (See [Appendix E, “Device Configurations.”](#))

- **PCI 2.2.3.c**—*For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.*
- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.*

The management console was configured to support HTTPS access, with HTTP access disabled. CS-ACS is configured to use SSL as a highly secure management portal technology.

CS-ACS employs port hopping to a random high port for secured communication transport.

Role-based administration is configured for administrative tasks.



Note

Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant/service provider.

Requirement 6: Develop and Maintain Secure Systems and Applications

- **PCI 6.1**—*Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.*

Smartnet services enable Cisco customers to have the ability to keep current with the latest versions of code, including security patches and bug fixes.

**Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And
Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 7.2**—Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to “deny all” unless specifically allowed.
- **PCI 8.1**—Identify all users with a unique user name before allowing them to access system components or cardholder data.
- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components.
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords.

Role-based privilege assignment is configured on CS-ACS for all management functions.

Access Control Server allows the configuration of unique users and passwords. CS-ACS administrative accounts do not allow alternative or external authentication methods. It cannot be configured to authenticate to Active Directory for management functions of the server itself. (See [Figure D-8](#).)

- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

CS-ACS is configured to a 15-minute timeout. (See [Figure D-10](#).)

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges.
- **PCI 10.2.3**—Access to all audit trails.
- **PCI 10.2.4**—Invalid logical access attempts.
- **PCI 10.2.5**—Use of identification and authentication mechanisms.
- **PCI 10.2.6**—Initialization of the audit logs.
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource

Individual role-based user authentication logs are local (no AD authentication available).

There is a local audit trail for CS-ACS.

Audit log files backed up daily to a log backup server are monitored by CSA and all processes and users (except the application processes responsible for writing data to the log server) are prohibited from modifying or deleting files from this directory.

CSA alerts are generated, sent to the CS-MARS central server, and an e-mail alert is sent to the administrator e-mail account.

The following requirements were satisfied by configuring the operating system of the CSA Manager server to use NTP:

- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization.*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. Two or three central time servers within the organization receive external time signals directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT), peer with each other to keep accurate time, and share the time with other internal servers.*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version.*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*

These requirements were satisfied by configuring the operating system of the Access Control Server to use NTP.

- **PCI 10.5.1**—*Limit viewing of audit trails to those with a job-related need.*
- **PCI 10.5.2**—*Protect audit trail files from unauthorized modifications.*

Cisco Security Agent (CSA) software is used to monitor and protect access to audit trail files, and to alert on unauthorized attempts to modify the audit trail (only application services responsible for writing log data can write/modify/delete the audit trail). Cisco has created an additional backup script to copy the audit trail to a central backup server, where CSA protection has been applied to eliminate all access, modification, and deletion, except for the account responsible for backing up the audit trail.

PCI Sub-Requirements that Require Compensating Controls (CS-ACS)

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

**Caution**

CS-ACS does not have individual user password duration enforcement, password complexity, password history or automated failed lockout capability for administration of the server itself. CS-ACS administration does not support external authentication methods. It was not able to take advantage of the Active Directory or other authentication solutions.

Compensating Control for Compliance

Cisco recommends a combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90 days, and firewall segmentation for CS-ACS servers within the data center. These would be reasonable compensating controls for password setting limitations within these applications.

The sub-requirement was not met in this lab environment because the data center infrastructure and company policies are not within the scope of the audit, prohibiting deploying the QSA-recommended compensating controls.

PCI Sub-Requirements that Require Compensating Controls (RSA enVision)

RSA enVision did not require any compensating controls to pass respective PCI sub-requirements.

Compliance Management

CiscoWorks Network Compliance Manager (C-NCM)

General Notes/Best Practices

The C-NCM can be used to prepare for a PCI audit by leveraging the following capabilities:

- Maintain comprehensive config change history archive for security audits.
- Monitor and enforce compliance with security standards such as Visa CISP/PCI for credit card transactions.
- Create security compliance policies (regex pattern match on firewall configurations) and check if firewall configurations are in compliance with applied security policies.
- Provide role-based access control and lockdown to devices and their configurations.
- Provision configuration changes on firewall devices.
- Maintain audit trail of changes made on firewall devices.
- Maintain a history of changes made to ACLs.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and other Security Parameters

Configure passwords with required complexity and length for local accounts.

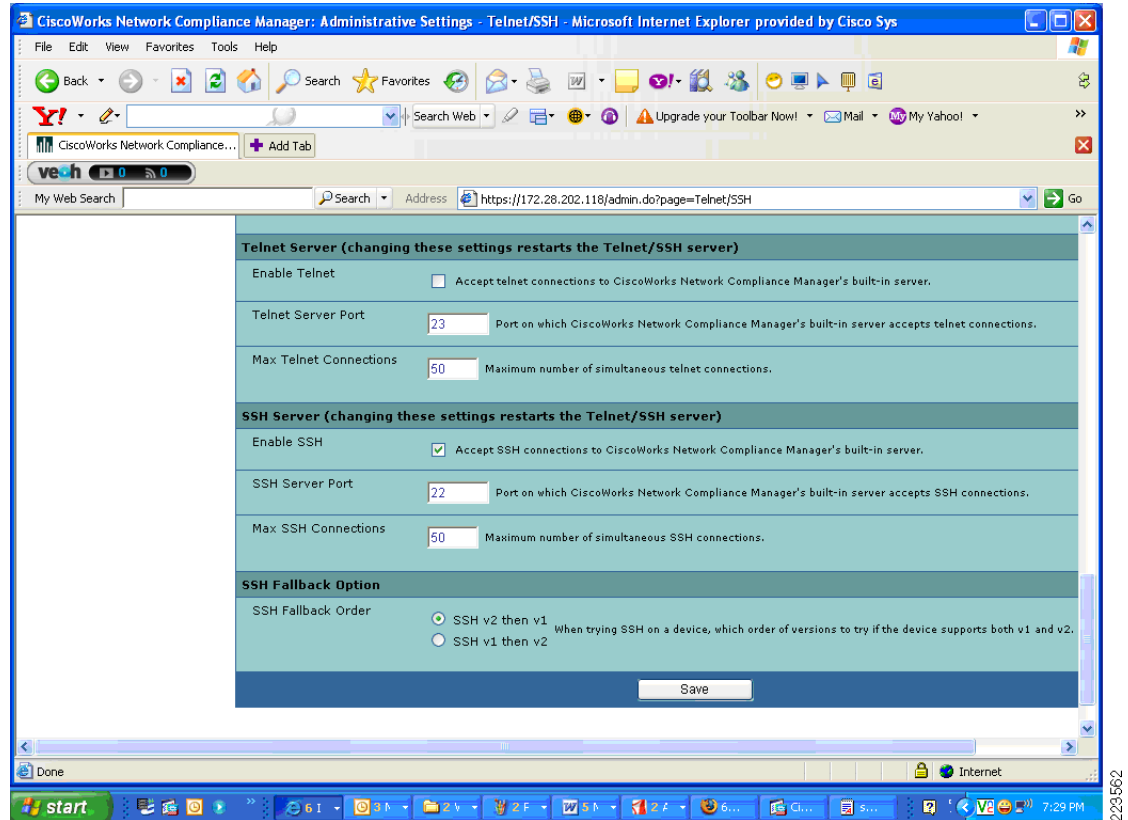
The text following this list refers to the following sub-requirements:

- **PCI 2.2.2**—*Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function).*

- **PCI 2.3**—*Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*

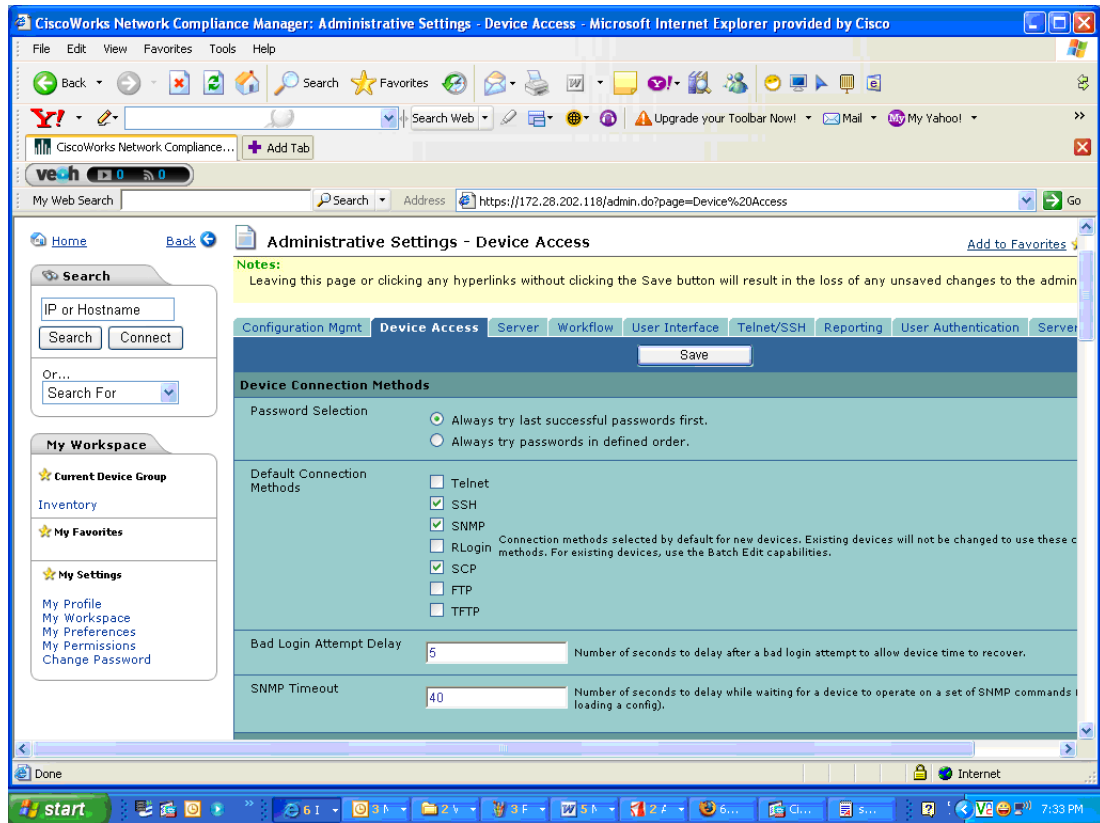
Unsecure access to CS-NCM via HTTP and Telnet were disabled while HTTPS and SSH were configured. See [Figure 3-21](#).

Figure 3-21 Configure CS-NCM to Accept SSH Connections, Disabling Telnet



Services such as Telnet, FTP, and TFTP were not selected for the connection methods to the network devices. CS-NCM was managed according to PCI requirements for services running on CS-NCM as well as services that should be running on the managed network devices. See [Figure 3-22](#).

Figure 3-22 Device Access settings on CS-NCM for Secure Connection Methods to Network Devices



- **PCI 2.2.3.b**—Verify that common security parameter settings are included in the system configuration standards.
- **PCI 2.2.3.c**—For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And Requirement 8: Assign a Unique ID to each Person with Computer Access

The text following this list refers to the following sub-requirements for requirements 7 and 8:

- **PCI 7.2**—Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
- **PCI 8.1**—Identify all users with a unique user name before allowing them to access system components or cardholder data.
- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords

- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Compliance of the sub-requirements in this section was achieved within the solution by implementing the CS-ACS and Microsoft Active Directory for user account services.

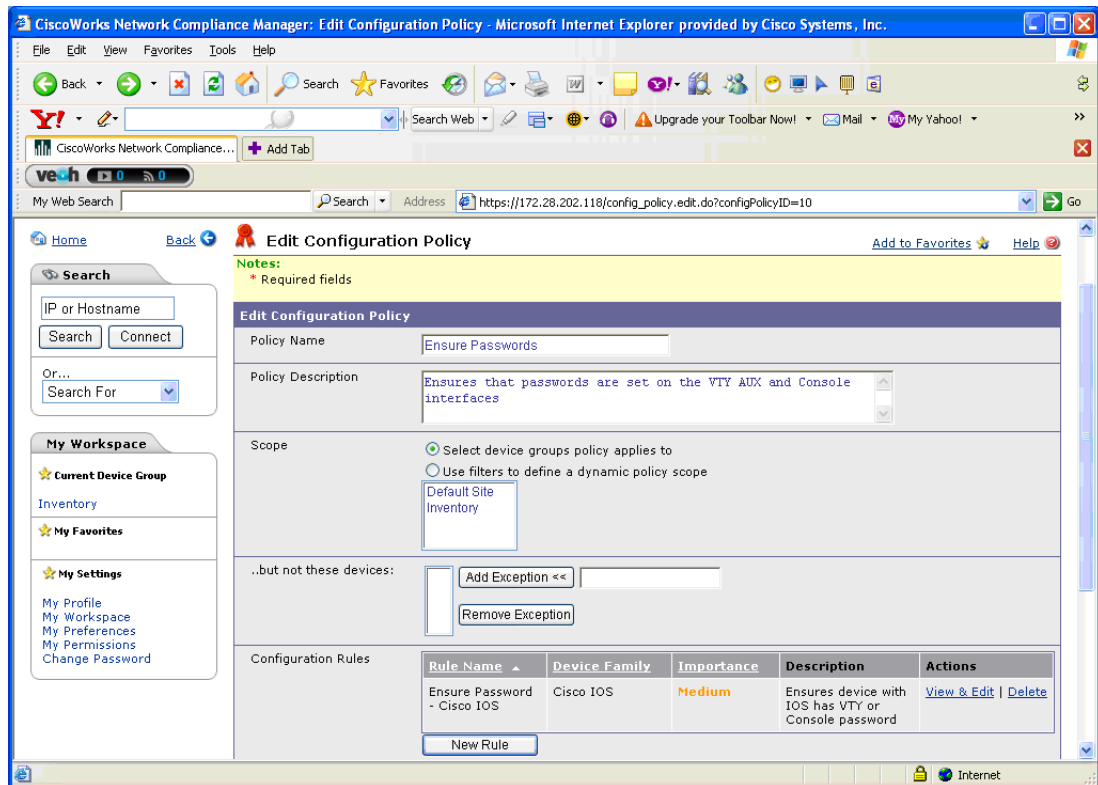
Fallback authentication, in the event of the CS-ACS not being reachable, was configured local to CS-NCM. These fallback accounts should be rotated based on a QSA-recommended policy.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*
- **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*
- **PCI 10.3.1**—*User identification*
- **PCI 10.3.2**—*Type of event*
- **PCI 10.3.3**—*Date and time*
- **PCI 10.3.4**—*Success or failure indication*
- **PCI 10.3.5**—*Origination of event*
- **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*
- **PCI 10.4**—*Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:*
 - **PCI 10.4.a**—*Verify that NTP or similar technology is used for time synchronization*
 - **PCI 10.4.b**—*Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]*
 - **PCI 10.4.c**—*Verify that the Network Time Protocol (NTP) is running the most recent version*
 - **PCI 10.4.d**—*Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). For more information, see <http://www.ntp.org>.*
- **PCI 11.1**—*Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.*

The above requirements were met by the CS-NCM as they pertain to configuration change events on the network devices.

CS-NCM was used to capture configuration snapshots of the ASA, routers, and Catalyst switches in the datacenter. It was used to check whether a device had the proper commands configured in order to satisfy PCI requirements. Configuration changes were monitored and tracked, with the ability to determine which user made what changes on what device. Figure 3-23 shows an example of CS-NCM configured with a rule to check that devices are configured with passwords for console access according to industry standards and best-practices for securing access to routers and such devices.

Figure 3-23 Requirement 2.2-2



Clients and Servers

Point-of-Sale (POS)

General Notes/Best Practices

The NCR Advanced Checkout Solution Point -of-Sale system was audited for PCI compliance. They were installed to provide the necessary transaction traffic to validate the security of the retail infrastructure. The QSA audited the POS system by analyzing different files of NCR's CS-ACS software. Few of files were Database transaction files, user access logs, EFT Journal Report, EFT Offline Report, EFY Rejection Report, Electronic Journal Report, TRMOFF (FOH offline transaction file) and EFTOFF (back office offline transaction file)

Retail companies are recommended to consult Visas cardholder information security program for payment applications:
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html.

The retail company should consult with a QSA or security services company for their specific implementation.

The QSA Verizon Business found that POS servers installed with the CSA client provide tremendous value to a retail company seeking PCI compliance.

Servers

General Notes/Best Practices

NCR provided the point-of-sale (POS) client work station and servers. One of the servers was loaded with NCRs Advanced Checkout Solution (NCR-ACS) and other server was loaded with NCRs Advanced Store Workbench (ASW) client software. The client station is NCR RealPOS80c system running Windows embedded XP version 2.

NCR-ACS Software (version 6.01.04.16) is a highly customizable group of applications that provide the retail environment with a complete store system solution. NCR-ACS includes the application software that runs on the back office computer and at the front-end POS workstations used to check out customers.

- NCR advises its customers to store cardholder data according to CISP Implementation Documentation. Since NCR-ACS is a POS system, NCR advises its customers not to store or place any systems with cardholder data facing the Internet.
- NCR recommends customers implementing the application with any network configuration use only securely encrypted communications.

Advanced Store Workbench (ASW) is the main NCR-ACS software. installed on the backoffice computer system. From ASW, one can access back office reports and applications.

Retail companies are recommended to refer to <http://www.CISecurity.com> for guidance on securing their servers to pass compliance. The retail company should consult with a QSA or security services company for their specific implementation.

QSA found that the NCR-CSA client installed on POS systems would provide tremendous value to a retail company seeking PCI compliance.

PCI Sub-Requirements Satisfied by Solution Component (NCR POS Systems)

Requirement 3: Protect stored cardholder data

- **PCI 3.2**—Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following requirements 3.2.1 through 3.2.3. It is the responsibility of the merchant to ensure the POS systems used do not store sensitive authentication data (e.g., full track data, CVV2, and PIN/PIN block) post authorization (even if encrypted). A major step to ensure POS systems meet PCI requirements is to work with the POS vendors who have certified their POS application/s according to PABP standards.
 - **PCI 3.2.1**—*Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data*

- PCI 3.2.2—Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.
- PCI 3.2.3—Do not store the personal identification number (PIN) or the encrypted PIN block
- PCI 3.3—Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).

Figure 3-24 Masked PAN Information

```

C:\AC5\Server\Bin\bgmenu.exe
12/31/07 Electronic Journal Report Page 16:34:24
TerminalNum=2 TransNum=39 OperatorNum=1 09/27/2007 14:49:30 Signoff
Operator Signed Off. Reason = SignOff

-----
TerminalNum=2 TransNum=1 OperatorNum=1 09/27/2007 14:49:36 Signon
Operator Signed On. Reason = ValidSignon

-----
TerminalNum=2 TransNum=2 OperatorNum=1 09/27/2007 14:51:14 Normal

SubTotal 11.01
Tax Due .00
Total 11.01
401288*****1881 DEBIT TENDER 11.01
Number of Items 2

-----
F2 Print F3 Quit F7 Jump Backward F8 Jump Forward
  
```

- PCI 3.4—Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:
 - Strong one-way hash functions (hashed indexes)
 - Truncation
 - Index tokens and pads (pads must be securely stored)
 - Strong cryptography with associated key management processes and procedures

The minimum account information that must be rendered unreadable is the PAN.

- PCI 3.5—Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:
 - PCI 3.5.1—Restrict access to keys to the fewest number of custodians necessary
 - PCI 3.5.2—Store keys securely in the fewest possible locations and forms
- PCI 3.6.1—Generation of strong keys
- PCI 3.6.2—Secure key distribution
- PCI 3.6.3—Secure key storage
- PCI 3.6.4—Periodic key changes
 - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically
 - At least annually

**Note**

NCR-ACS application—There was no reasonable way to rotate encryption keys, without manually decrypting all data and re-encrypting with a new key. NCR-ACS application allows multiple keys (up to 255) to be used to limit the amount of data encrypted with a single key.

- **PCI 3.6.5**—*Destruction of old keys.*
- **PCI 3.6.6**—*Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key).*
- **PCI 3.6.7**—*Prevention of unauthorized substitution of keys*
- **PCI 3.6.8**—*Replacement of known or suspected compromised keys*

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components.*
- **PCI 8.5.8**—*Do not use group, shared, or generic accounts and passwords.*
- **PCI 8.5.9**—*Change user passwords at least every 90 days.*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters.*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters.*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.*
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts.*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID.*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data.

- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.*

**Note**

NCR-ACS application:NCR-CSA was used to monitor and log access to use of NCR-ACS application binaries and access to NCR application log files.

- **PCI 10.2**—*Implement automated audit trails for all system components to reconstruct the following events:*
 - **PCI 10.2.1**—*All individual accesses to cardholder data*
 - **PCI 10.2.2**—*All actions taken by any individual with root or administrative privileges*

**Note**

NCR-ACS application—Any actions taken by any individual administrative privileges is logged to NCR-ACS **EFT log file** and in the **Transaction LOG**.

- **PCI 10.2.3**—*Access to all audit trails.*

**Note**

NCR-ACS application—Unauthorized access to audit log files and application log directories triggered CSA events, which were logged at CSA Management console.

- **PCI 10.2.6**—*Initialization of the audit logs*

**Note**

NCR-ACS application—CSA protection for audit trail access applies to initialization of audit trail.

- **PCI 10.3**—Record at least the following audit trail entries for all system components for each event:
 - **PCI 10.3.1**—*User identification*
 - **PCI 10.3.2**—*Type of event*
 - **PCI 10.3.3**—*Date and time*
 - **PCI 10.3.4**—*Success or failure indication*
 - **PCI 10.3.5**—*Origination of event*
 - **PCI 10.3.6**—*Identity or name of affected data, system component, or resource*

PCI Sub-Requirements that Require Compensating Controls (NCR POS System)

NCR POS system did not require any compensating controls to pass respective PCI sub-requirements.

Wired and Wireless Clients

General Notes/Best Practices

Configure all wired and wireless endpoints to prompt for user identification and password. Do not statically configure these properties as retail wireless units such as inventory scanners may not be physically secure.

Encryption and Key Management

RSA Key Manager

General Notes/Best Practices

Public Key Infrastructure (PKI) is a key requisite for installing RSA Key Manager Server (based on RSA Key Manager version 2.1.1).

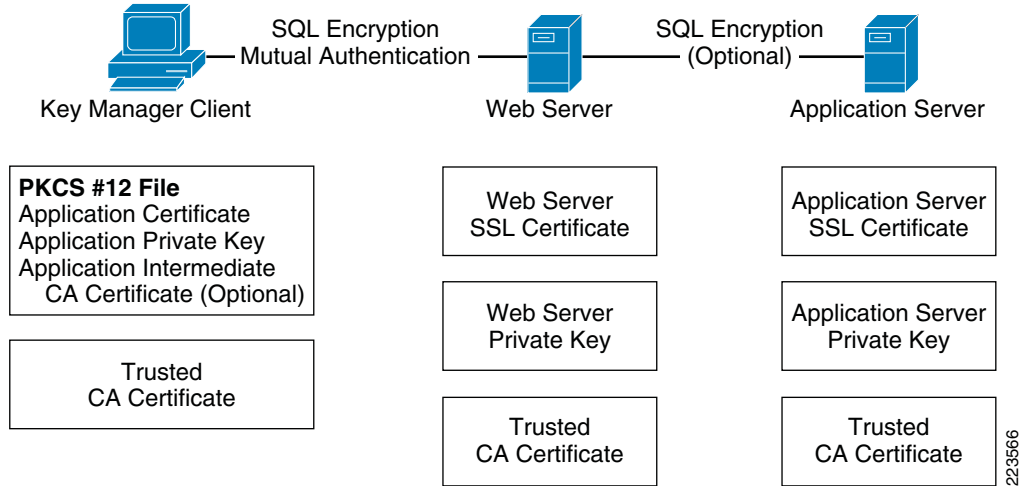
Public Key Infrastructure (PKI) Requirements

In an RSA Key Manager deployment, a PKI needs to be set up to enable highly secure communication and authentication between entities. In an RSA Key Manager PKI trust model, SSL communications is used for the following purposes:

- Highly secure communications between network entities in the RSA Key Manager deployment.
- Mutual authentication between RSA Key Manager Clients and the web server.
- Highly secure communication for delivery of application certificates to the RSA Key Manager Server.

Figure 3-25 illustrates RSA Key Manager PKI requirements.

Figure 3-25 RSA Key Manager PKI Requirements



The certificates and credentials that need to be prepared include:

- Key Manager Client PKCS#12 credentials.
 - Contains the application certificate, application private key, and optionally, the middle Certificate Authority (CA) certificate chain if the application certificate is not signed directly by the web server’s trusted CA certificate.
- Web server SSL certificate and private key.
 - Used by RSA Key Manager Clients to authenticate the server.
- Application server SSL certificate and private key (optional).
 - Used by the web server to authenticate the application server. Recommended to encrypt communications between the web server and the application server, especially if the servers are running on different machines.
- Trusted CA certificate.
 - Installed on each network entity in a RSA Key Manager deployment to verify the signature of certificates sent by a peer. For example, a RSA Key Manager Client has a trusted CA certificate to verify the signature of the web server certificate.
- Middle CA certificate (optional).
 - If a certificate is not signed directly by a trusted CA certificate, a middle CA certificate should be installed and sent during SSL connection to verify the certificate chain.

Security Recommendation

Because of vulnerabilities with RSA signatures with a small public exponent, especially 3, RSA recommends that an exponent of F4 (216+1) be used.

Security Best Practices

A RSA Key Manager Server deployment securely stores security objects, generates and stores cryptographic keys, manages cryptographic policies, and brokers access to security objects by RSA Key Manager Clients. It is crucial that you implement best practice security measures to secure and limit access to this functionality. These measures include, but are not limited to:

- Placing all RSA Key Manager components within a highly secure zone, protected by firewalls and by user authentication and authorization (using RSA Access Manager, for example).
- Highly secure communication between entities in a RSA Key Manager deployment via SSL.
- As much as possible, keeping your RSA Key Manager entities separate from the rest of your organizational systems.
- Suppressing logging of plain text keys in log files on the web server.
- Prevention of memory modification and direct access to data on disk.
- Highly secure database backup procedures.

A RSA Key Manager Server deployment brings together other third-party products (such as web server, application server, and database server products) to provide a complete cryptographic key management solution.

For the latest information on how to configure and secure Microsoft SQL Server in a RSA Key Manager deployment, refer to the following URLs:

- 10 steps to help secure SQL Server
<http://www.microsoft.com/sql/prodinfo/previousversions/securingsqlserver.mspx>
- SQL Server security considerations
<http://msdn2.microsoft.com/en-us/library/ms161948.aspx>.
- Backing up and restoring databases in SQL Server
<http://msdn2.microsoft.com/en-us/library/ms187048.aspx>.

PCI Sub-Requirements Satisfied by Solution Component (RSA Key Manager)

Requirement 3: Protect Stored Cardholder Data

- **PCI 3.5.1**—*Restrict access to keys to the fewest number of custodians necessary*
- **PCI 3.5.2**—*Store keys securely in the fewest possible location and forms*
- **PCI 3.6.1**—*Generation of strong keys*
- **PCI 3.6.2**—*Secure key distribution*
- **PCI 3.6.3**—*Secure key storage*
- **PCI 3.6.4**—*Periodic key changes*
- **PCI 3.6.5**—*Destruction of old keys*
- **PCI 3.6.6**—*Split knowledge and establishment of dual control of keys*
- **PCI 3.6.7**—*Prevention of unauthorized substitution of keys*
- **PCI 3.6.8**—*Replacement of known or suspected compromised keys*

**Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And
Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on user's need to know and is set to "deny all" unless specifically allowed*
- **PCI 8.1**—*Identify all user with a unique user name before allowing them to access system components or cardholder data*

In the lab, RSA Access Manager was used to provide the above function for RSA Key Manager.

- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices
 - Biometrics
- **PCI 8.4**—*Encrypt all passwords during transmission and storage on all system components.*
For RSA key Manager, authentication through RSA Access Manager is hashed and also local authentication is hashed.
- **PCI 8.5.8**—*Do not use group, shared or generic accounts and passwords*
- **PCI 8.5.9**—*Change user passwords at least every 90 days*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager (8 characters)
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager (alpha-numeric+dictionary check).
- **PCI 8.5.12**—*Do not allow individual to submit a new password that is the same as any of the last four passwords he or she has used*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager (last 10 passwords).
- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager (3 invalid attempts in one day)
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID*
For RSA Key Manager, this requirement is satisfied using RSA Access Manager (admin must reset)
- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal*

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user

For RSA Key Manager, in addition to local audit trails, CSA was used to monitor and log access to RSA Key Manager binaries.

- **PCI 10.2.1**—All individual accesses to cardholder data
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.3**—Access to all audit trails

For RSA Key Manager, unauthorized access to audit log files and application log directories triggered CSA events which were logged at CSA Management console.

- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.3.1 through 10.3.6**—Record audit trail entries for user identification, type of event, date and time, success or failure indication and origination of event

PCI Sub-Requirements that Require Compensating Controls (RSA key Manager)

RSA Key Manager did not require any compensating controls to pass respective PCI sub-requirements.

RSA Access Manager

General Notes/Best Practices

RSA Access Manager is used within the lab environment to protect administrative access to RSA Key Manager. See [Figure 3-26](#) for sample configuration.

PCI Sub-Requirements Satisfied by Solution Component (RSA Access Manager)

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 7.2**—Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to “deny all” unless specifically allowed.
- **PCI 8.1**—Identify all user with a unique user name before allowing them to access system components or cardholder data
- **PCI 8.2**—In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password
 - Token devices
 - Biometrics
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components.
- **PCI 8.5.8**—Do not use group, shared or generic accounts and passwords.

- **PCI 8.5.9**—Change user passwords at least every 90 days.
- **PCI 8.5.10**—Require a minimum password length of at least seven characters.
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts.
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

Figure 3-26 RSA Access Manager – Password Policy

Password Policy Basics

Policy Name: Default Password Policy
 Description: Default Password Policy

Lifetime: 60 Days
 History: Users cannot re-use their previous 0 Passwords
 Minimum Lifetime: 0 Seconds
 Default Policy: Make this the default password policy

Password Characters

Minimum length: 8
 Maximum length: 32
 Excluded Characters: ^&*(
 Excluded Words File: words.txt
 Non-alpha Required: Require at least one non-alphabetic character

Policy Lockout

Lock Out: Users can enter an unlimited number of incorrect passwords without being locked out.
 Lock out a user after 3 incorrect password entries in 1 Days

Unlock: Require an administrator to unlock users who have been locked out.
 Automatically unlock users after 10 Minutes

Notification E-mail: [Empty field]

223567

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.3**—Access to all audit trails
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms

- **PCI 10.3.1 through 10.3.6**—*Record audit trail entries for user identification, type of event, date and time, success or failure indication and origination of event*

PCI Sub-Requirements that Require Compensating Controls (RSA Access Manager)

RSA Access Manager did not require any compensating controls to pass respective PCI sub-requirements.

RSA File Security Manager

General Notes/Best Practices

RSA File Security Manager is a software-based security solution that provides transparent encryption of files/folders in conjunction with role-based access control on heterogeneous platforms.

RSA File Security Manager comprises of two integrated components:

- Adapter Manager—Defines the access control rules for network/domain users & applications
- Adapters—Enforces the access control rules at the host/server level

The following are best practices for deploying RSA File Security Manager product:

- Ensure that your systems meet and exceed the minimum system requirements for the adapter and adapter manager console before installation. This information is available in the adapter and adapter manager console installation guides.
- Ensure that the adapter manager console host is able to reach the host on which the file security adapter is installed.
- The adapter and adapter manager console require the use of a control port and audit port to interoperate fully. Ensure that the required firewall ports (default TCP 5766 and 19978) are open to bi-directional traffic to enable full communication between the adapter and adapter manager. Note that the actual port numbers are user configurable.
- Ensure that you frequently backup the policy database at the adapter manager. It is highly recommended that you perform a backup after every significant change to the system.
- By default, the file security adapter generates an audit log for all types of access to the protected folder. The audit log data is stored in “day files” on the protected host.
 - Monitor the file security adapter for the amount of audit log data being generated and plan for appropriate storage.
 - Disable the actions for which you do not want the adapter to create an audit trail.
 - Ensure that you have a backup strategy for the audit log data files generated at the file security adapters. At the end of every 24 hours, the file security adapters switch over to a new audit log file (day file). We recommend that you backup the old audit log day files to a central server and delete the original copy on the file security adapter to best optimize your storage.

PCI Sub-Requirements Satisfied by Solution Component (RSA File Security Manager)

Requirement 3: Protect Stored Cardholder Data

- **PCI 3.5.1**—*Restrict access to keys to the fewest number of custodians necessary*

- **PCI 3.5.2**—*Store keys securely in the fewest possible location and forms*
- **PCI 3.6.1**—*Generation of strong keys*
- **PCI 3.6.2**—*Secure key distribution*
- **PCI 3.6.3**—*Secure key storage*
- **PCI 3.6.4**—*Periodic key changes*
- **PCI 3.6.5**—*Destruction of old keys*
- **PCI 3.6.6**—*Split knowledge and establishment of dual control of keys*
- **PCI 3.6.7**—*Prevention of unauthorized substitution of keys*
- **PCI 3.6.8**—*Replacement of known or suspected compromised keys*

**Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know And
Requirement 8: Assign a Unique ID to each Person with Computer Access**

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed*
- **PCI 10.1**—*Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user*
- **PCI 10.2.1**—*All individual accesses to cardholder data*
- **PCI 10.2.3**—*Access to all audit trails*
- **PCI 10.2.4**—*Invalid logical access attempts*
- **PCI 10.2.5**—*Use of identification and authentication mechanisms*
- **PCI 10.3.1 through 10.3.6**—*Record audit trail entries for user identification, type of event, date and time, success or failure indication and origination of event*

PCI Sub-Requirements that Require Compensating Controls (RSA File Security Manager)

- **PCI 8.5.9**—*Change user passwords at least every 90 days*
- **PCI 8.5.10**—*Require a minimum password length of at least seven characters*
- **PCI 8.5.11**—*Use passwords containing both numeric and alphabetic characters*
- **PCI 8.5.12**—*Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used*

For 8.5.9 through 8.5.12, QSA recommends a combination of documented password policies, manual audit procedures to ensure strong password generation, using periodic dictionary attacks against passwords, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.

- **PCI 8.5.13**—*Limit repeated access attempts by locking out the user ID after not more than six attempts*
- **PCI 8.5.14**—*Set the lockout duration to thirty minutes or until administrator enables the user ID*

For 8.5.13 through 8.5.14, QSA recommends using CSA or other monitoring software to alert on continuous invalid logon attempts, combined with internal firewall segmentation of these components, would be reasonable compensating controls for account lockout setting limitations within these applications.

- **PCI 8.5.15**—*If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.*

QSA recommends screensaver timeouts can be used as a compensating control, when idle session timeouts are not available or impact application/business operations (e.g., backup jobs).

**Note**

Sub-requirements from 8.5.9 through 8.5.15 is addressed in roadmap of RSA File Security Manager in version 2.2 to be released in Q12008.

RSA® Authentication Manager, RSA SecurID® and RSA enVision

The RSA Authentication Manager works with RSA Authentication Agents to enhance security with strong, two-factor user authentication provided by time synchronous-based RSA SecurID tokens.

RSA® Authentication Manager software is the management component of the RSA SecurID® solution, used to verify authentication requests and centrally administer user authentication policies for access to enterprise networks. Working in conjunction with RSA SecurID authenticators and RSA® Authentication Agent software, the solution provides two-factor user authentication that protects access to more VPNs, wireless networks, web applications, business applications, and operating environments.

RSA enVision is an appliance-based information management security platform that captures and stores hundreds of thousands of data events per second, providing an enterprise view of activity from any number of sources, including perimeter and network devices, operating systems and even proprietary applications

General Notes/Best Practices

RSA Authentication Manager should be installed first before installing any of its components like RSA Authentication client and RSA SecurID seeds.

PCI Sub-Requirements Satisfied by Solution Component (RSA Authentication Manager, RSA SecurID and RSA enVision)

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

- **PCI 7.2**—*Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*

Requirement 8: Assign a Unique ID to each Person with Computer Access

- **PCI 8.1**—*Identify all users with a unique user name before allowing them to access system components or cardholder data.*
- **PCI 8.2**—*In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:*
 - Password
 - Token devices (for example, SecureID, certificates, or public key)
 - Biometrics

- **PCI 8.3**—Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
- **PCI 8.4**—Encrypt all passwords during transmission and storage on all system components
- **PCI 8.5.8**—Do not use group, shared, or generic accounts and passwords
- **PCI 8.5.9**—Change user passwords at least every 90 days
- **PCI 8.5.10**—Require a minimum password length of at least seven characters
- **PCI 8.5.11**—Use passwords containing both numeric and alphabetic characters
- **PCI 8.5.12**—Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- **PCI 8.5.13**—Limit repeated access attempts by locking out the user ID after not more than six attempts
- **PCI 8.5.14**—Set the lockout duration to thirty minutes or until administrator enables the user ID.
- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data

- **PCI 10.1**—Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
- **PCI 10.2.2**—All actions taken by any individual with root or administrative privileges
- **PCI 10.2.4**—Invalid logical access attempts
- **PCI 10.2.5**—Use of identification and authentication mechanisms
- **PCI 10.3.1**—User identification
- **PCI 10.3.2**—Type of event
- **PCI 10.3.3**—Date and time
- **PCI 10.3.4**—Success or failure indication
- **PCI 10.3.5**—Origination of event
- **PCI 10.3.6**—Identity or name of affected data, system component, or resource
- **PCI 10.5.1**—Limit viewing of audit trails to those with a job related need
- **PCI 10.5.2**—Protect audit trail files from unauthorized modifications
- **PCI 10.5.3**—Promptly back up trail files to a centralized log server or media that is difficult to alter
- **PCI 10.5.5**—Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)

PCI Sub-Requirements that Require Compensating Controls

RSA Authentication Manager:

- **PCI 8.5.15**—If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

QSA recommends screensaver timeouts can be used as a compensating control, when idle session timeouts are not available or impact application/business operations (e.g., backup jobs).

RSA enVision did not require any compensating controls to pass respective PCI sub-requirements.

**Note**

Cisco security advisories and notice are published for significant security issues that directly involve Cisco products and require an upgrade, fix, or other customer action. Security Advisories are posted on Cisco.com and sent to the cust-security-announce@cisco.com as well as various public mailing lists and newsgroups. The cust-security-announce@cisco.com mailing list is an external list that allows anyone interested to subscribe and receive Cisco security announcements. It is highly recommended that customers should also visit the Cisco Security Advisories and Notices website (http://www.cisco.com/en/US/products/products_security_advisories_listing.html#advisory) to get details and information about the most recent security vulnerabilities and issues.

Solution Component Summary

Table 3-1 shows how the varied solution components are deployed for the respective compliance themes.

Table 3-1 Solution Component Summary

Solution Component Functions			
Technology	Authentication	Configuration Management	Audit Trail
Network Systems			
ISR Router	CS-ACS + AD	C-LMS/General (CS-M/Security)	Syslog to C-LMS and CS-MARS
Mid-range/ WAN Aggregation Router	CS-ACS + AD	Local, C-NCM	Syslog to CS-MARS
Catalyst switch	CS-ACS + AD	C-LMS	Syslog to C-LMS and CS-MARS
Adaptive Security Appliance (ASA)	CS-ACS + AD	Local, C-NCM	Syslog to CS-MARS
Wireless Access Points	Local	WCS	LWAPP to controller
Wireless Controller Administration	CS-ACS + AD	WCS	Syslog to CS-MARS, SNMP to WCS
Edge Router (Cisco 7200)	CS-ACS + AD	General/C-NCM	Syslog to CS-MARS
Cisco Firewall Services Module	CS-ACS + AD	General/ASDM	Syslog to CS-MARS
Cisco Intrusion Detection System	Local	IDM/General	Attacks to CS-MARS, Syslog to local flat files
Cisco ACE XML Gateway (AXG)	AD	AXG Manager	Local flat files
System Management			
C-LMS	CS-ACS + AD	Local	Local flat files
WCS	Local	Local	Local flat files
CS-M	CS-ACS + AD	Local	Local flat files
CSA Manager	AD	Local	Local database

Table 3-1 Solution Component Summary (continued)

Solution Component Functions			
Compliance Management			
C-NCM	CS-ACS + AD	Local	Local database
Monitoring			
CS-MARS	Local	Local	Local database/external NFS share
WCS	Local	Local	Local flat files
Authentication			
CS-ACS	Local	Local	Local flat files
Clients			
Wired users	None	NA	NA
Wireless users	ACS + AD	NA	NA
CSA client	CSA Manager	CSA Manager	NA
Third-Party Products			
RSA Key Manager Server	RSA Access Manager	RSA Key Manager	local flat files
RSA File Security Manager	RSA File Security Manager	RSA File Security Manager console	local flat files
NCR POS Servers	AD	Advanced Checkout Solution configuration tool	local flat files
RSA Authentication Manager/RSA SecureID	RSA Authentication Manager/RSA SecureID	RSA Authentication Manager/RSA SecureID	RSA enVision—log files are stored in proprietary database.



CHAPTER 4

Implementing and Configuring the Solution

Implementation

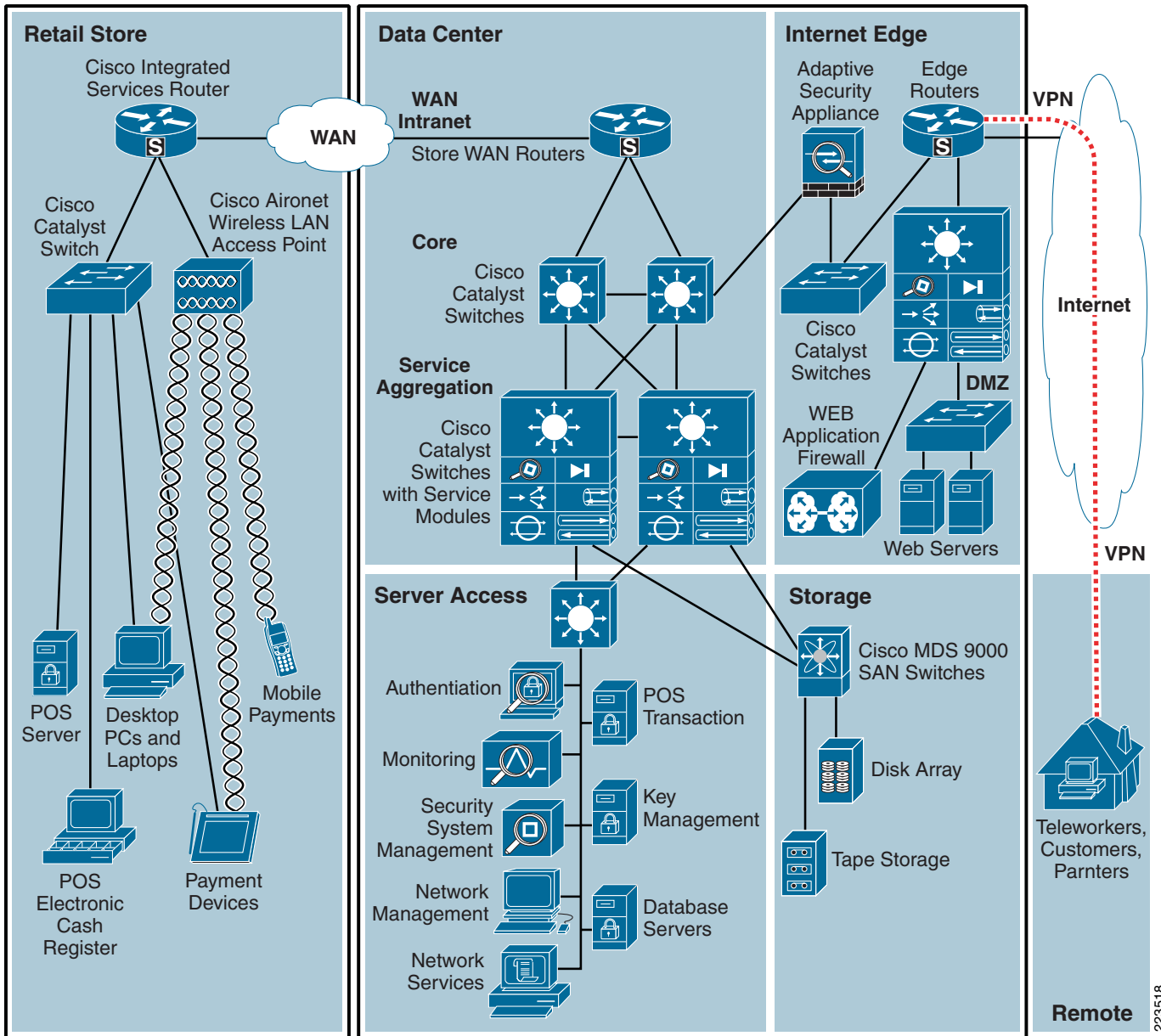
Overview

The PCI solution for Retail was validated in Cisco's Retail lab in San Jose, California. The store, data center, Internet service provider, WAN and Internet edge network infrastructures and security management were installed first. Next, partner point-of sale (POS), payment, encryption, mobile computing devices, and POS application servers were installed to create a simulated enterprise retail environment. Cisco subject matter experts from product business units, Customer Advocacy Advanced Services, Enterprise Solution Engineering, Field Systems Engineering all contributed to the best practices contained in this implementation. Subject matter experts from our partners RSA, EMC, NCR, VeriFone, Wincor-Nixdorf, IBM and NCR also assisted in creating a realistic set of retail POS and payment applications, and creating the secure configurations based on PCI requirements. Finally, Verizon Business provided their on-site and remote auditors who reviewed the designs and configurations, provided input on how to make things more secure, and finally produced the detailed report of compliance found in [Appendix F, "Report on Compliance \(ROC\)."](#)

To validate the Retail Store portion of the PCI Solution for Retail, three retail store designs were used from the Cisco Intelligent Retail Network (IRN) reference architecture. The reference designs include wireless hand-held devices as well as POS systems to ensure functionality of common retail applications and services. The data center design is based on best practices from the *Cisco Data Center Assurance Program 2.5* architecture. The Internet edge is a collapsed architecture based on the Internet edge reference designs and incorporates new technologies in the area of Web application security. The corresponding network, data, and security management systems are documented to demonstrate how to manage and monitor all aspects of the solution.

[Figure 4-1](#) illustrates a high-level architecture showing the connections between the retail stores, data center, and Internet edge.

Figure 4-1 End-to-End Physical Solution Architecture

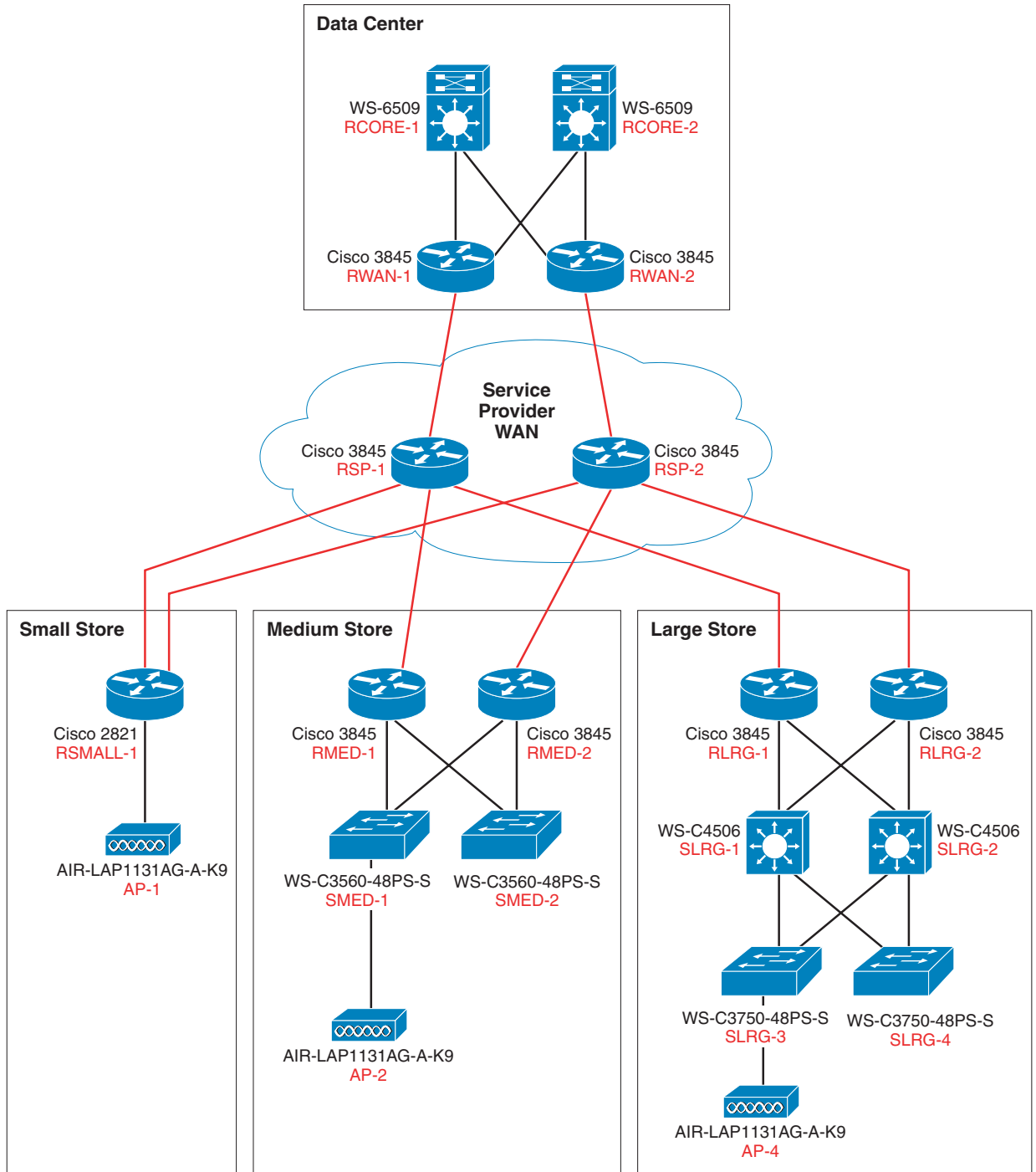


223518

Network Topology

The network topology shown in Figure 4-2 is a private routed network representative of an MPLS WAN with dual service providers connecting the three branch networks to a single data center. The WAN is implemented as *active* on service provider 1 (RSP-1) and *standby* for service provider 2 (RSP-2). Deployments of services in the data center are assumed to be appropriately segregated and secured.

Figure 4-2 Lab Network Overview



All three locations use T-1 circuits for WAN connectivity to the service providers and Ethernet for the LAN segments:

- The small store location consists of a single router with integrated switching module for network devices that have a single wireless access point.

- The medium store uses a dual router infrastructure and redundant LAN switching design, with a single wireless access point, although typical implementation would include up to six.
- The large store uses a redundant router WAN, a redundant switching distribution layer with high capacity fiber, fiber-connected access layer switches distributed throughout the location as needed (typical for a large store big box retailer), and a single wireless access point, although typical implementation would include up to 25.

What was Implemented

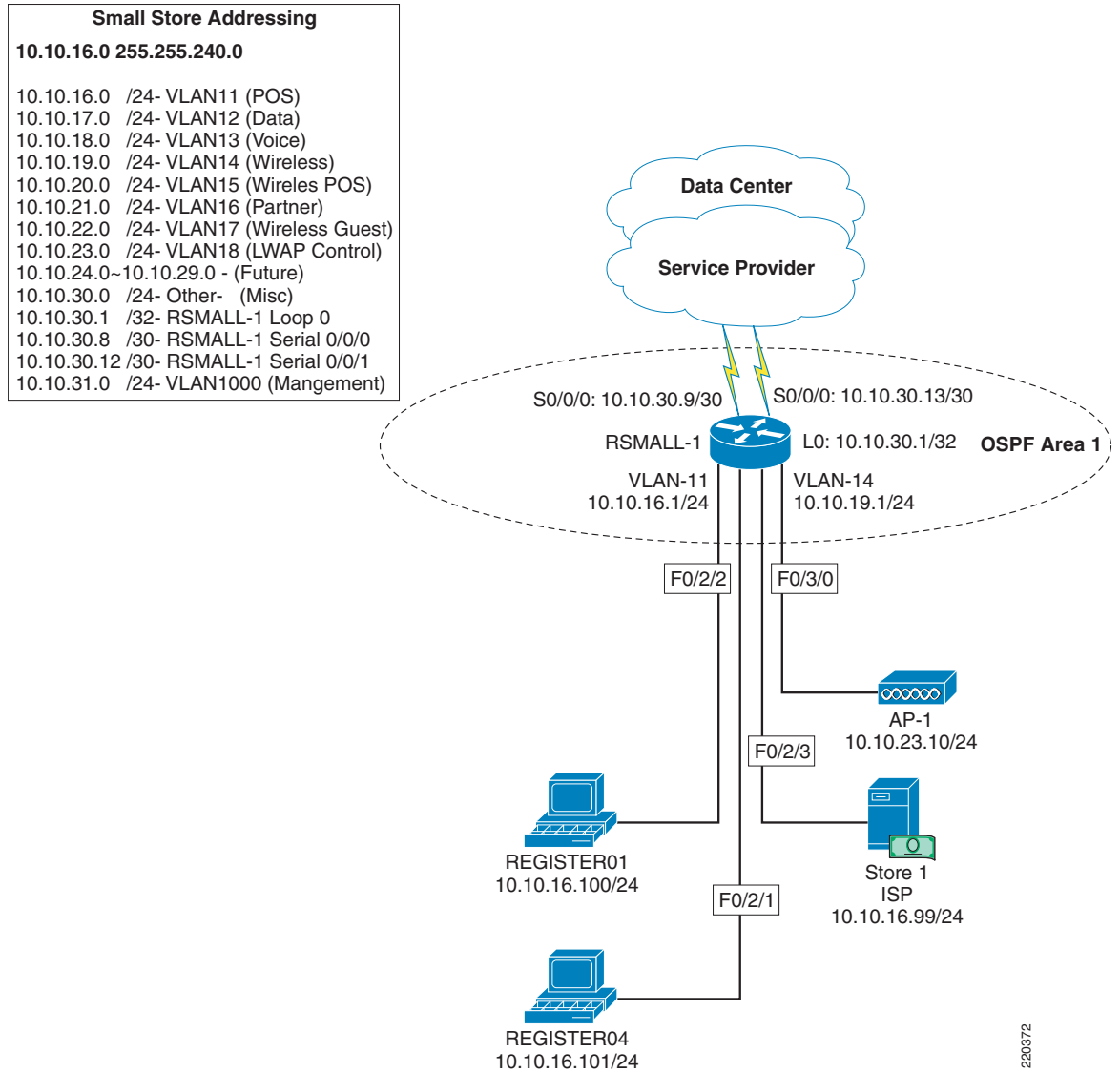
Key features and services implemented include:

- Cisco IOS Firewall stateful inspection
- Cisco IOS Firewall IPS intrusion detection
- Cisco IOS access lists
- Network segmentation using VLANs
- Secure management communications for SSH, HTTPS, and SNMPv3
- AAA to a central authority (CS-ACS and Active Directory)
- Wireless security (WPA with 802.1x)
- Centralized logging and audit tracking
- Redundant NTP time synchronization
- High encryption for server Remote Desktop Protocol (RDP) access
- CSA for client/server desktop security
- Anti-virus for infestation mitigation and removal
- Update services for clients and servers for patch management
- E-mail services for alerts and notifications of real-time events
- Cash registers provided by NCR, IBM, Wincor-Nixdorf
- Mobile Retail Manager (MRM) software from NCR
- Wireless handhelds provided by Intermec and Verifone
- Payment devices provided by VeriFone
- Single thread of WAN aggregation layer and core, service aggregation, and access layer of the data center
- Validated single thread of Internet edge

Detailed listings of all products are available in [Appendix A, “Bill Of Materials of Devices for Branch Stores.”](#)

[Figure 4-3](#) shows the small store IRN solution.

Figure 4-3 Small Store IRN Solution



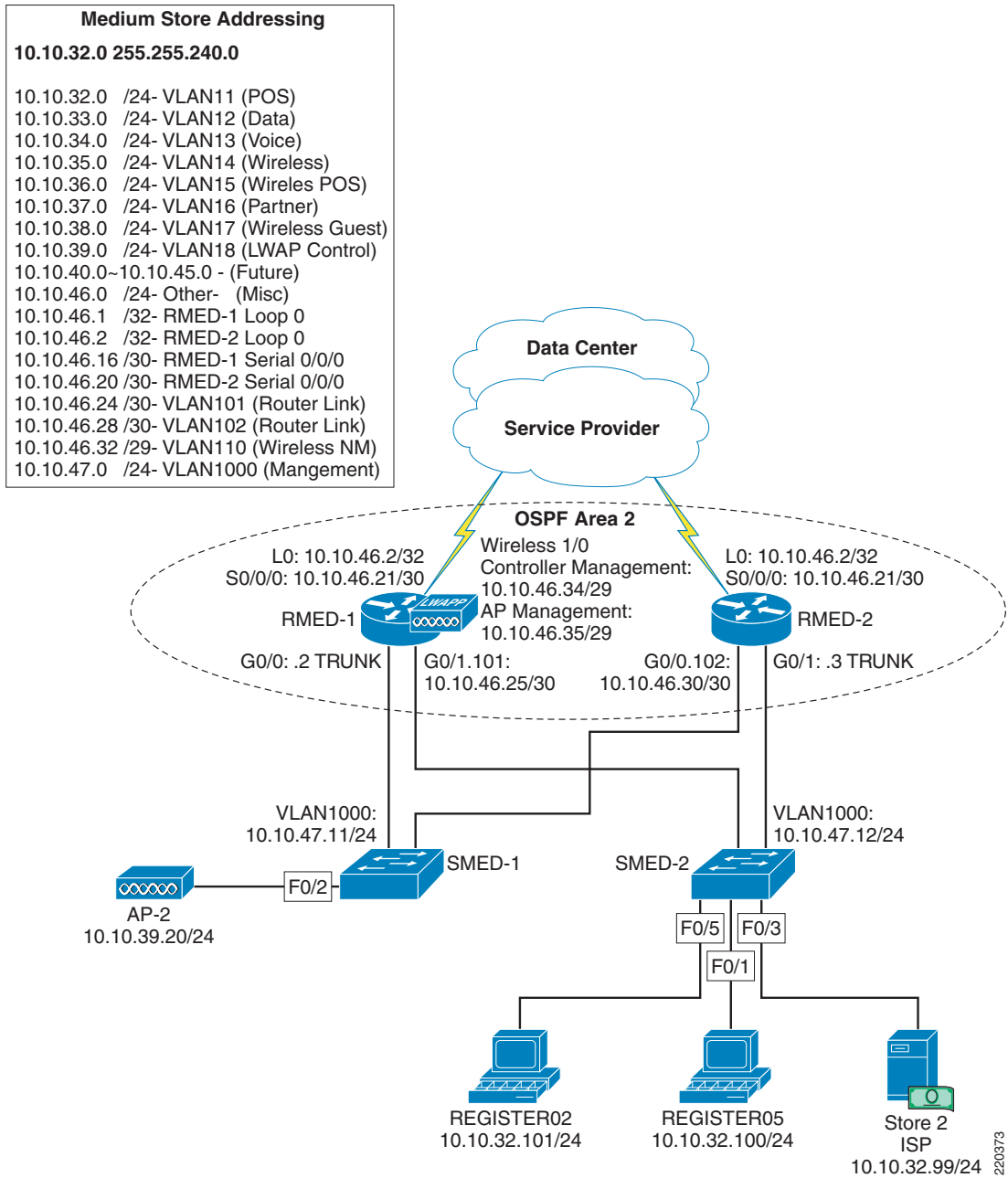
The small store implementation includes the following:

- Cisco 2821 ISR router with integrated switch
- 1131 AG LWAPP access point
- Wincor-Nixdorf Beetle MII register
- IBM 4851 register
- Windows server running Wincor TP.Net software and Cisco CSA software

Figure 4-4 shows the medium store IRN solution.

220372

Figure 4-4 Medium Store IRN Solution

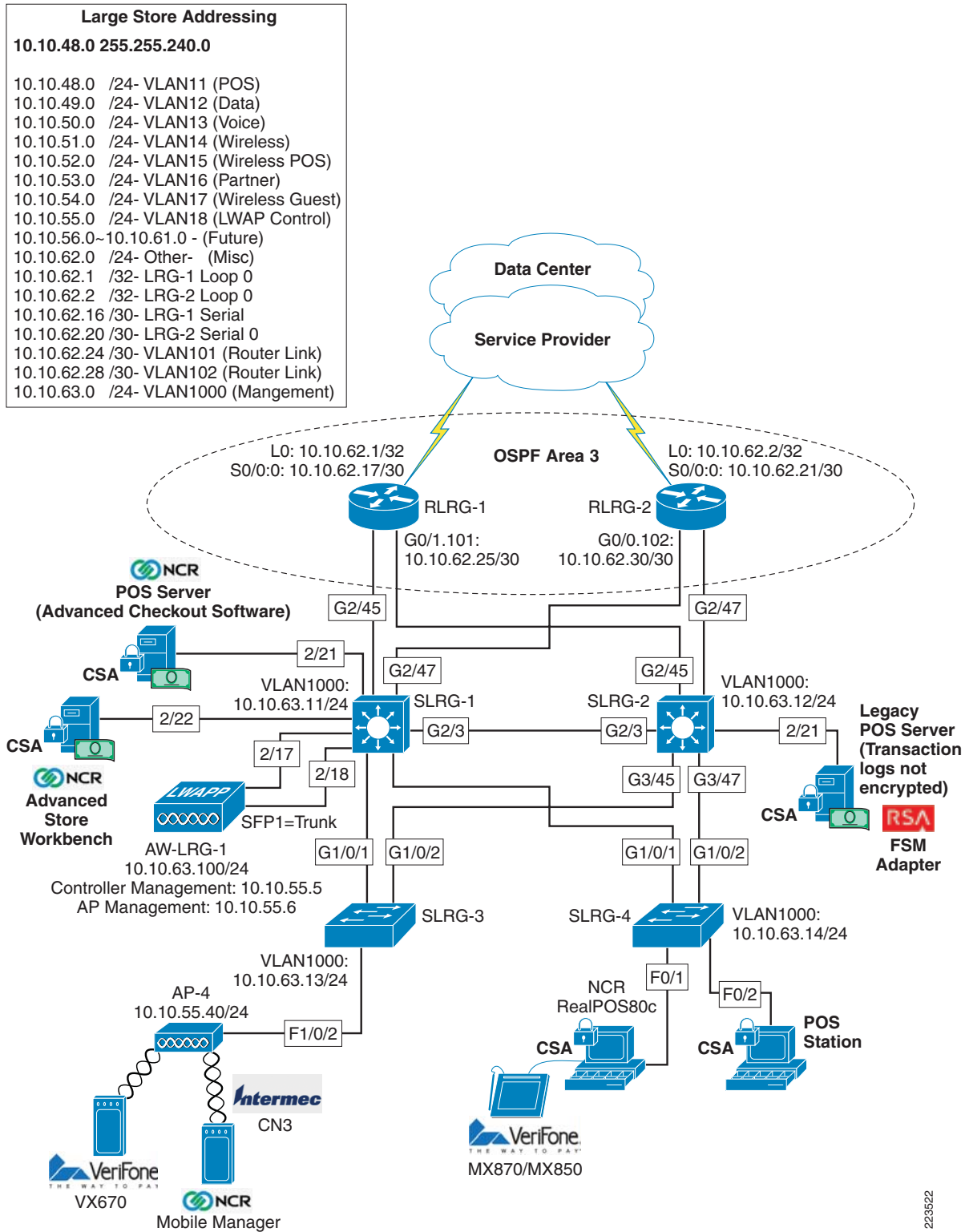


The medium store implementation includes the following:

- Cisco 3845 ISR routers
- Catalyst 3560 Switches
- Wireless NM Controller module
- Cisco 1131 AG LWAPP access point
- Wincor-Nixdorf Beetle S II register
- IBM 4810 Register
- Windows server running Wincor POS and Cisco CSA software

Figure 4-5 shows the large store IRN solution.

Figure 4-5 Large Store IRN Solution



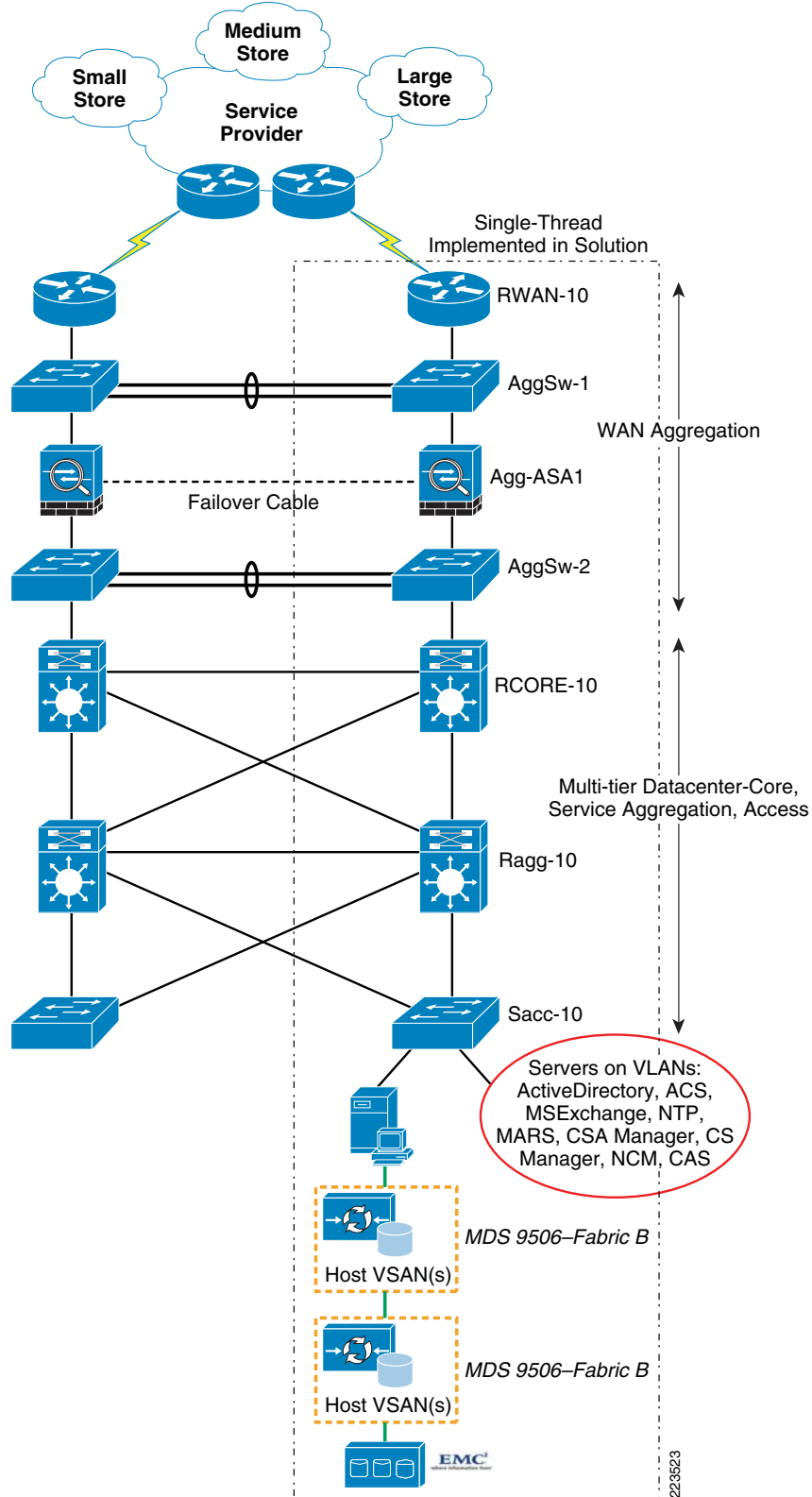
223522

The large store implementation includes the following:

- Cisco 3845 ISR routers
- Cisco Catalyst 3750 and 4500 switches
- Cisco 1131 AG and AP1242 AG LWAPP access point
- Cisco 4402 Wireless Controller
- NCR RealPOS 80c Electronic Cash Register with Advanced Checkout System software and Cisco CSA software
- NCR server running NCR-ACS software, RSA File Security agent and Cisco CSA
- IPsec VPN to data center via ASA in the WAN aggregation layer.

Figure 4-6 shows the data center location.

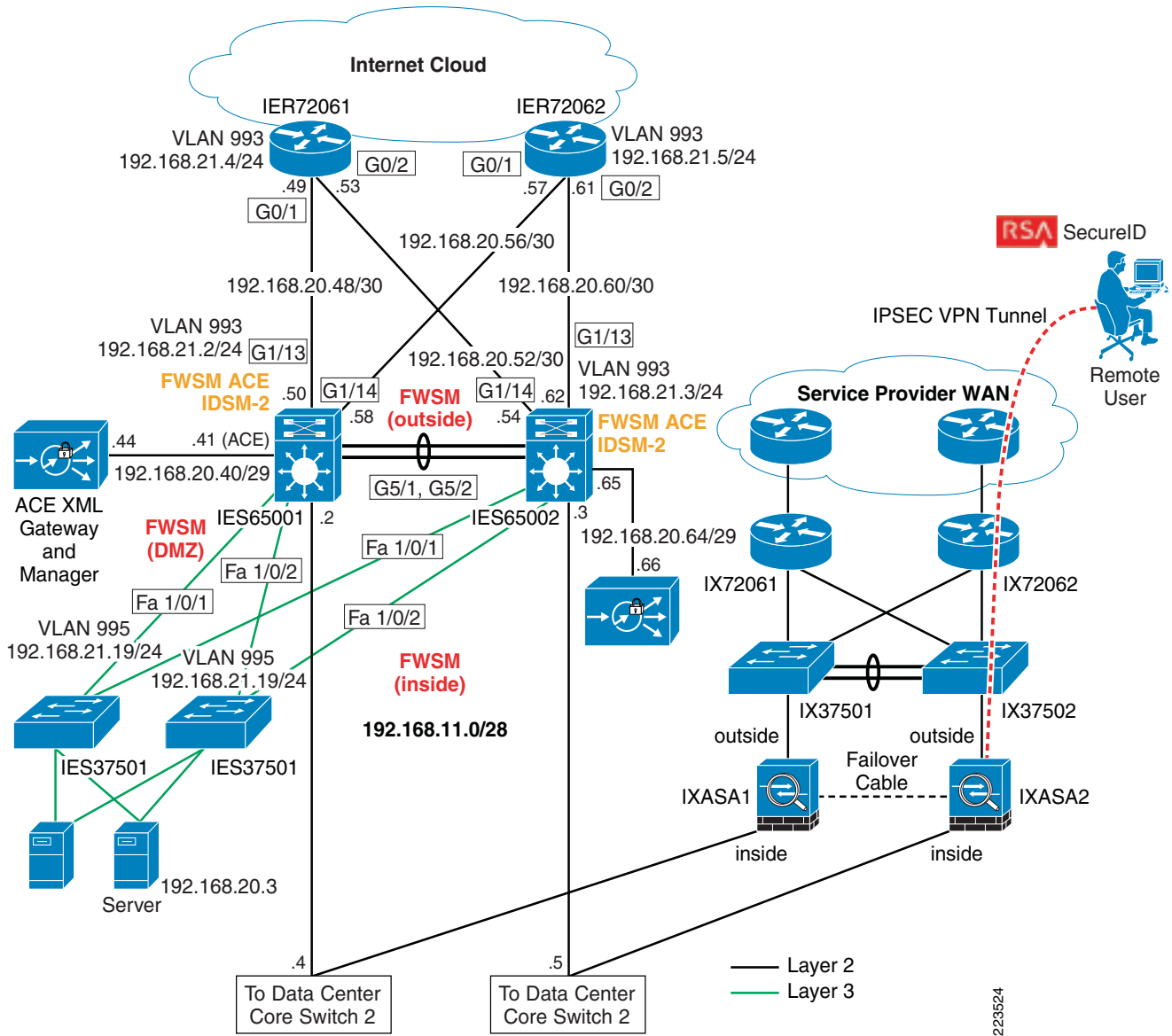
Figure 4-6 Data Center Location



The products implemented in the data center include the following:

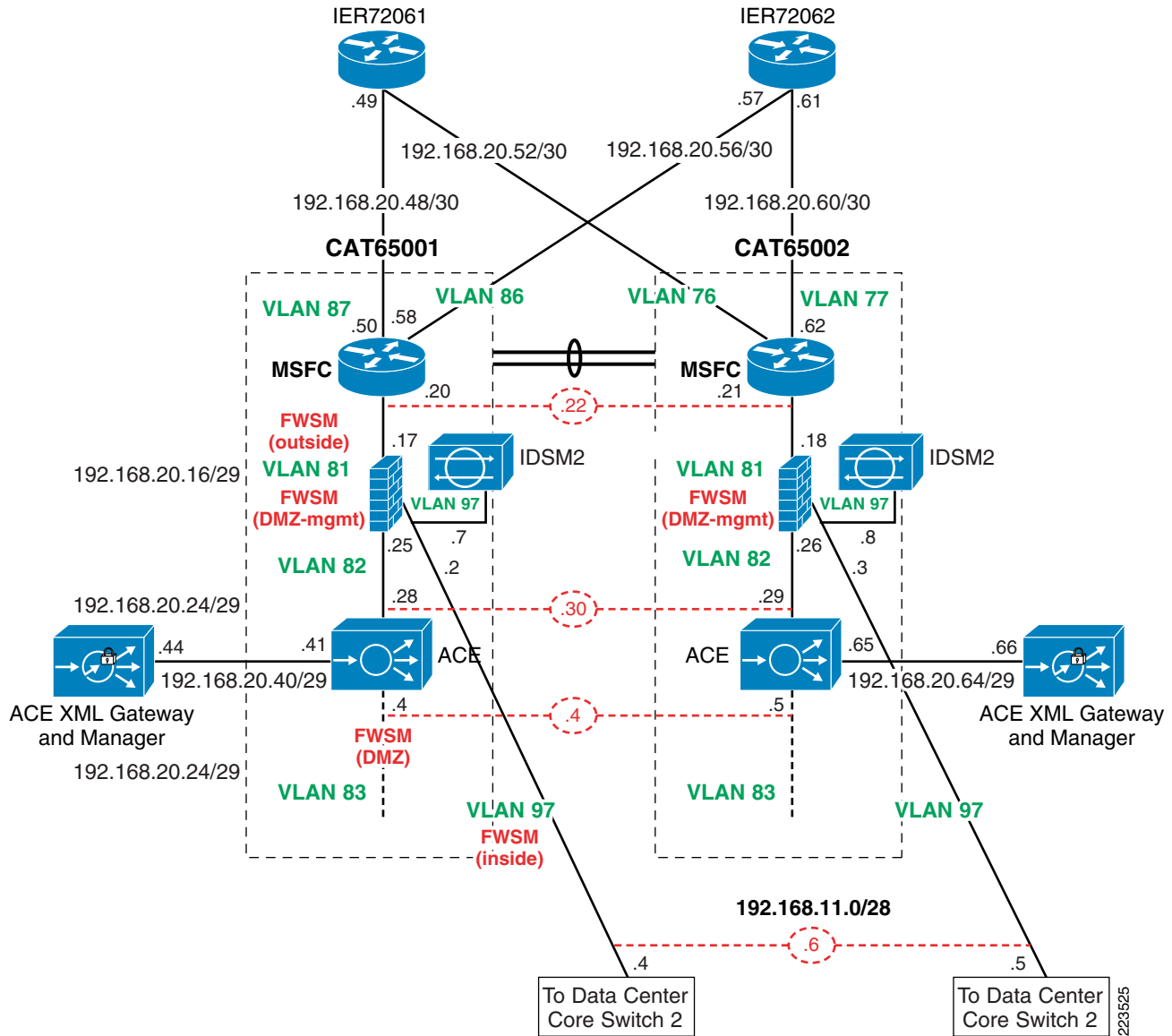
- Cisco Secure Access Control Server (CS-ACS)
- Cisco Security Agent Management Center (CSA-MC)
- Cisco Security Manager (CS-M)
- CiscoWorks LMS (C-LMS) and Resource Manager Essentials modules
- Wireless Control Server Manager (WCS)
- Wireless controller for small store locations (Type 2000 for this lab)
- Cisco Security Monitoring, Analysis and Response System (CS-MARS)
- Microsoft Active Directory Services on Windows 2003 R2 Server
- Microsoft Exchange Server 2003
- Microsoft Windows Server Update Services (WSUS)
- NTP (Network Time Protocol) Appliance (vmWare appliance)
- Windows 2003 R2 Server with NFS file services for UNIX
- Wincor-Nixdorf TP.Net Point of Sale v3.1
- Microsoft Retail Management System Store Operations
- RSA Key Manager
- RSA File Security Manager
- RSA Access Manager
- RSA enVision
- RSA Authentication Manager/RSA SecureID

Figure 4-7 Internet Edge IRN Solution



223524

Figure 4-8 Internet Edge IRN Solution – Catalyst Switch Module Details



The Internet edge implementation includes the following:

- Cisco 7200VXR
- Cisco Catalyst 3750 and 6500 switches
- Cisco Intrusion Detection System Service Module (IDSM2)
- Cisco Firewall Services Module (FWSM)
- Cisco Application Control Engine (ACE)
- Cisco ACE XML Gateway
- Cisco Adaptive Security Appliances (ASA)
- RSA SecureID
- Foundstone's Hacme Bank application

What Was Not Implemented

- E-commerce
- Other locations in a typical enterprise network (headquarter campus, distribution center, etc)
- Redundancy and high availability in WAN aggregation and data center

Audit Findings

The audit process with the QSA from Verizon Business revealed important points that determined the scope of the solution, and what was and was not implemented. In addition, as of the publication of this design guide, the findings are useful for enterprises that need to understand what may be expected of them during the audit process so that they may be able to streamline the process with their QSA.

- PCI auditors currently do not examine the Storage Area Network when conducting a PCI audit. The findings in this solution are based on the QSA's best estimation of what the PCI requirements may evolve to address storage networking sometime in the future.
- Given that a dual-threaded data center has fully redundant devices, the QSA applies the same checks and requirements to both devices. The existence of high availability or redundancy does not change the audit process. As a result, this solution limited implementation to a single thread to save on time and resources. In production data center environments, redundancy and high availability are highly recommended and referenced in other Cisco design guides.
- Some of the PCI requirements can only be met by deploying a specific feature set or product on the network. As an example, Requirement 1 requires that a firewall be deployed on the enterprise edge. A product with the firewall features set, such as the Cisco ISR 3845 with the Cisco IOS Firewall feature set, could be deployed to meet this requirement. It is critical to note that in addition to Requirement 1 being applied to the ISR 3845, an additional set of requirements will be applied. These requirements pertain to any network device that is deployed and they are as follows:
 - Requirement 2—Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).
 - Requirement 7—Restrict access to cardholder data by business need-to-know.
 - Requirement 8—Assign a Unique ID to each Person with Computer AccessRequirements 7 and 8 pertain to implementing external Authentication, Authorization, and Accounting (AAA) on the network device so that different levels of privileged access can be given to different user accounts based on business roles and policies. In addition, each user account is mapped to a specific individual so that any actions can be traced back to a specific individual and not to a group or generic user.
 - Requirement 10—Track and monitor all access to network resources and cardholder data. This set of requirements pertains to audit trails and logging of events on the network device such that configuration changes and network activity involving the network device can be logged and used at a later date for network forensics.
- QSA recommended the use of secure automated or manual process (e.g., secure FTP) for moving the Tlogs (payment card data) from store to data center headquarter (HQ) even though the Tlogs files were encrypted and transferred over a Cisco secure VPN solution.
- The QSA recommended that security vulnerabilities for network devices should be checked against the national vulnerabilities database in preparation for an audit. For more information, refer to <http://nvd.nist.gov/nvd.cfm>.

Testing

These architectures were not tested to meet any specific traffic throughput or capacity levels. Scaling considerations for hosts in the store reference designs are based on typical retail store design best practices. The use of these designs for other types of locations outside of the specific design objectives, could result in less than desired performance levels. The goal of the testing was to determine best practice security recommendations based on PCI DSS requirements.

Functional Testing

- Functionality of the designs were tested by performing remote management and configuration tasks, client transactions for POS, e-mail messaging and alerting, Windows update services, and NTP time synchronization.
- ICMP tools such as Ping and Traceroute were used to validate that network devices and system hosts were reachable between the various locations.
- WildPackets OmniPeek Personal network analyzer was used to capture network traffic for both wired and wireless troubleshooting.

PCI Audit Testing

- [Appendix F, “Report on Compliance \(ROC\),”](#) details the steps performed by Cybertrust as the QSA auditors of the PCI Solution for Retail.
- In addition to reviewing device configurations and network diagrams, Cybertrust performed extensive interviews over several weeks with each of the technology experts that built and configured the devices and management platforms. Cybertrust also performed a vulnerability assessment scan on the network while connected in the data center location. This scan used nCircle software and evaluated all servers, clients and devices in the network. The results of this initial scan are available in [Appendix C, “Application Protocols.”](#) The scan identified several items that were later corrected. No follow-up scan was performed.

Configuration Tasks

Routing and Switching

- The routers and switches were configured using common best practices and router hardening techniques.
- The only network protocol implemented was IPv4, with each location being assigned a summarizable block of hierarchical defined RFC 1918 addresses. Each store LAN was divided into several VLAN segments to appropriately segregate traffic for data, voice, POS, management and wireless needs.
- Unnecessary and insecure services were disabled such as PAD, TCP and UDP small servers and finger. Depending on your version of IOS these settings may not be visible in the config, they may already be off by default.

- Service password-encryption was enabled, and service password recovery was disabled to prevent configurations from being disclosed if hardware was removed from the site.
- AAA Authentication was configured and pointed to the CS-ACS, a local user name and password were configured to authorize access in the event CS-ACS was not reachable. This local account password should be changed quarterly.
- NTP was configured to synchronize time and log events. The time zone was configured to PST, and Service timestamps set.
- The local security certificates were created using the **crypto key generate rsa** command; the key length set to 1024 bits.
- The secure HTTPS server was enabled and the non-secure HTTP server disabled. Additionally, the VTY interfaces were set to allow only SSH connections.
- Logging was configured to send Syslog events to both CiscoWorks and CS-MARS.
- SNMP was configured using V3 user and password. This account should also be changed quarterly.
- The auxiliary and unused line interfaces were disabled by setting **no exec**.
- Loopback interfaces were created on the routers and used for sourcing logs, traps, authentication and time requests.
- All interface IP addresses were defined in DNS.
- Router interfaces under the OSPF process were set to passive as a default, then explicitly permitted on desired interfaces such as serial WAN links and LAN interconnects. This was necessary to control the flow of traffic through appropriate interfaces, because all contained ACLs.

Complete configurations of the routers and switches are available in [Appendix E, “Device Configurations.”](#)

For more information, see the following references:

- Enterprise Branch Security Design Guide:
http://www.cisco.com/univercd/cc/td/doc/solution/e_b_sdc1.pdf
- Business Ready Branch Solutions for Enterprise and Small Offices—Reference Design Guide:
http://www.cisco.com/application/pdf/en/us/guest/netso/ns656/c649/cdcont_0900aecd80488134.pdf
- Enterprise Architecture Solutions:
http://www.cisco.com/en/US/netso/ns477/networking_solutions_packages_list.html

Unified Wireless

Wireless was implemented using Lightweight Access Point Protocol (LWAPP) controllers. The medium and large store locations each had their own local controllers. The small store operated from a centralized LWAPP controller in the data center. The AP in the small store was configured to operate in hybrid REAP mode in the event of a WAN failure. Each of these controllers were centrally managed and configured via WCS Manager. The controllers sent Syslog messages to CS-MARS.

To best meet the PCI requirements regarding wireless security, WPA was deployed using 802.1x requiring user authentication for wireless access. Several wireless segments were configured using different SSIDs mapped back to separate VLANs. This provided segregation of POS traffic from other wireless traffic. Each user needing access the wireless network was assigned a unique user ID and password. This authentication occurred against the Active Directory user database via the CS-ACS server using the RADIUS protocol. The Intermec wireless handheld used a Funk client to access and

authenticate. A Cisco wireless laptop with Odyssey client was also used to access the wireless network. Both of these clients support saving of the user ID and password locally, though saving of the password is not permitted under PCI guidelines.

When authenticated onto the network, IP address and DNS options were provided via DHCP for each wireless segment.

For more information, see the Installation Guide for Cisco WCS Manager at the following URL: http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a00806b57ec.html

Adaptive Security Appliance

The Adaptive Security Appliance (ASA) was used as a firewall at the WAN aggregation layer and Internet-edge Extranet segment. ASA was configured with access control lists, stateful packet inspection, and security levels at the interfaces.

All traffic that goes through the ASA is by default inspected using the Adaptive Security Algorithm and either allowed through or dropped.

If the ASA sees a new connection, it has to check the packet against access lists and perform other tasks to determine if the packet is allowed or denied. To perform this check, the first packet of the session goes through the *session management path*, and depending on the type of traffic, it might also pass through the *control plane path*.

The session management path is responsible for the following tasks:

- Performing the access list checks
- Performing route lookups
- Allocating NAT translations (xlates)
- Establishing sessions in the *fast path*



Note

The *session management path* and the *fast path* make up the *accelerated security path*.

Some packets that require Layer 7 inspection (the packet payload must be inspected or altered) are passed on to the control plane path. Layer 7 inspection engines are required for protocols that have two or more channels:

- A data channel, which uses well-known port numbers.
- A control channel, which uses different port numbers for each session.

These protocols include FTP, H.323, and SNMP.

Q. Is this an established connection?

A. If the connection is already established, the security appliance does not need to recheck packets; most matching packets can go through the *fast path* in both directions. The *fast path* is responsible for the following tasks:

- IP checksum verification
- Session lookup
- TCP sequence number check
- NAT translations based on existing sessions

- Layer 3 and Layer 4 header adjustments

For UDP or other connectionless protocols, the security appliance creates connection state information so that it can also use the *fast path*. Data packets for protocols that require Layer 7 inspection can also go through the *fast path*.

Some established session packets must continue to go through the session management path or the control plane path. Packets that go through the session management path include HTTP packets that require inspection or content filtering. Packets that go through the *control plane path* include the control packets for protocols that require Layer 7 inspection.

The interface security levels affect different ASA functions as described below. The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface. For some security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.
- Inspection engines—Some application inspection engines are dependent on the security level. For some security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level). For some security interfaces, you can filter traffic in either direction.
- Network address translation control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside). Without NAT control, or for some security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.
- Established command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For the same security interfaces, you can configure established commands for both directions. For more information on configuring the ASA, refer to the following documents:

- *Cisco ASA 5500 Configuration Examples and Tech Notes*
http://www.cisco.com/en/US/products/ps6120/prod_configuration_examples_list.html
- *Configuring the ASA 5500 Command Line Reference Guide 8.0*
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/conf_gd.html

Storage Area Networks

The solution involved connecting the data center's storage access layer to a VSAN environment that included EMC DMX 1000 storage arrays and Cisco MDS 9509 switches.

- The EMC storage arrays (DMX 9000) were not audited by the QSA. Per the QSA, PCI auditors currently do not examine the SAN when conducting a PCI audit. The findings in this solution are based on the QSA's best estimation of what the PCI requirements may evolve to address storage networking sometime in the future.
- The MDS 9500s were audited as far as the zoning and LUN masking configured on them to secure the logical partitioning of disk used for storing cardholder data. Only host machines in the data center that require access to that logical disk partition were allowed access. Restriction of user access to that set of host machines were outside the scope of this solution.

In order to pass an audit, the MDS switches must minimally meet the 2.x set of requirements for non-default passwords and system parameters, the 7.x requirements for strong access control, and the 8.x requirements for strong password configurations.

Below is a snapshot of the zoning configuration. **PCI-Retail-HBA1** zone was created to allow a specific file server in the data center, installed with a fiber host bus adapter and connected directly to this MDS switch, to access VSAN 900, LUN 0090, which were created specifically on the EMC storage array for the cardholder data file server.

```
MDS9509-2# sh zoneset act
zoneset name VSAN900 vsan 900
  zone name ECC2-local vsan 900
    * fcid 0xe20000 [pwwn 50:06:04:82:ca:fe:66:03] [DMX1320-FA4AA]
    * fcid 0xe20100 [pwwn 21:00:00:e0:8b:01:c3:e5]

  zone name Cluster2-local vsan 900
    * fcid 0xe20000 [pwwn 50:06:04:82:ca:fe:66:03] [DMX1320-FA4AA]
      pwwn 10:00:00:00:c9:2c:13:71

  zone name Z_PCI-RETAIL-HBA1 vsan 900
    * fcid 0xe20000 [pwwn 50:06:04:82:ca:fe:66:03] [DMX1320-FA4AA]
    * fcid 0x960001 [pwwn 10:00:00:00:c9:5d:28:d9]

MDS9509-2# sh ver
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html

Software
  BIOS:          version 1.1.0
  loader:        version 1.2(2)
  kickstart:    version 3.1(3a)
  system:       version 3.1(3a)

  BIOS compile time:      10/24/03
  kickstart image file is: bootflash:/m9500-sf1ek9-kickstart-mz.3.1.3a.bin
  kickstart compile time: 5/22/2007 17:00:00 [06/16/2007 15:36:31]
  system image file is:   bootflash:/m9500-sf1ek9-mz.3.1.3a.bin
  system compile time:    5/22/2007 17:00:00 [06/16/2007 15:54:18]
```

```
Symmetrix ID          : 000187431320
Database Type         : Type5
Last updated at      : 05:33:37 PM on Tue Nov 20,2007
```

```
Director Identification : FA-3A
Director Port          : 0
```

Identifier	Type	User-generated		Devices
		Node Name	Port Name	
210000e08b01c3e5	Fibre	210000e08b01c3e5	210000e08b01c3e5	010B 0142:0143
1000000c92c10d4	Fibre	targethost1	1000000c92c10d4	None
1000000c92c13de	Fibre	1000000c92c13de	1000000c92c13de	None
210000e08b01bfe5	Fibre	ecc	210000e08b01bfe5	0184
1000000c92c0f2e	Fibre	1000000c92c0f2e	1000000c92c0f2e	0029:002A 014A:014F 015D:0161 0164
1000000c92c142e	Fibre	1000000c92c142e	1000000c92c142e	None
1000000c92c1371	Fibre	node3	1000000c92c1371	00B9:00BA

```
Director Identification : FA-4A
Director Port          : 0
```

Identifier	Type	User-generated		Devices
		Node Name	Port Name	
210000e08b01bfe5	Fibre	ecc	210000e08b01bfe5	0162:0163
210000e08b01c3e5	Fibre	210000e08b01c3e5	210000e08b01c3e5	None
1000000c95d28d9	Fibre	PCI-RETAIL	HBA1	0090

For more information zoning and Logical Unit (LUN) masking, see the following:

- *Using VSANs and Zoning with the Cisco MDS 9000 Family* whitepaper:
<http://www.cisco.com/go/storagenetworking>
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, Release 3.x:
http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080662d35.html

Management

CiscoWorks LAN Management System (C-LMS)

Each router and switch was configured for SNMPv3 and Syslog, allowing CiscoWorks to track and manage them centrally. Router and switch configurations were polled and archived daily. These configurations were then automatically reviewed for key PCI compliance configuration items (that is, **no ip http server**, **transport input ssh**, and so on). If the configuration of an item changes, an alert e-mail is generated and sent to appropriate accounts. RME is used to deploy configuration updates as well as software updates to devices in the network. CiscoWorks provides process management for change design, approval, and deployment. Wireless controller syslogs were not able to be sent to CiscoWorks because of current product limitations.

For more information, see the following:

- Installation Guide for CiscoWorks Common Services with LMS Version 2.5.1:
http://www.cisco.com/en/US/products/sw/cscowork/ps3996/products_installation_guide_book09186a00805305cb.html
- Installation Guide for Cisco RME 4.0.3 with LMS 2.5.1:
http://www.cisco.com/en/US/products/sw/cscowork/ps2073/products_installation_guide_book09186a008050faf6.html

Cisco Security Manager (CS-M)

CS-M was configured to deploy access lists and inspect statements to the router interfaces via HTTPS and SNMPv3. Application traffic flows for all devices and applications were mapped out using network traces, logging ACLs, and extensive research in product documentation. These flows were placed in a table (see [Appendix C, “Application Protocols.”](#)) This information was then used to create the refined ACLs for implementation on all network interfaces inbound to the routers in conjunction with firewall inspect statements. After deployment of these comprehensive access lists, POS and network application functionality were validated.

CS-M automatically adds the command **ip verify unicast source reachable-via rx** to all interfaces, which verifies inbound traffic is not being spoofed on the interfaces.

IPS was also configured and implemented via CS-M using the standard SDF rules and sending SDEE alerts to CS-MARS.

For more information, see the following:

- Cisco Security Manager Installation Guide:
http://www.cisco.com/en/US/products/ps6498/products_installation_guide_book09186a008063d58b.html
- Guide for IPS Manager:
http://www.cisco.com/en/US/products/ps6498/products_user_guide_book09186a008064065d.html

Cisco Security Agent (CSA)

CSA was deployed on all servers and workstations to provide host-based security. CSA provides host-based intrusion prevention, application execution protection, and operating system lockdown. The policy for the clients is centrally managed and deployed from the CSA Manager Center (see [Figure 4-9](#)). Alerts and events are sent back to the CSA-MC, which was configured to interoperate with CS-MARS for centralized monitoring and analysis. The CSA client on the NFS backup server provides file integrity monitoring of the archived syslogs and other events in accordance with PCI Requirement 10.5.5.

Authentication of administrators accessing the CSA-MC is performed by defining users locally and forwarding the authentication requests to Active Directory via LDAP. Users need to enter their full user name (not their User ID) when logging in (that is, login using the name "Bart McGlothin" instead of the userid in AD of "bmcgloth"). The locally defined user names can also be configured with a local password for fallback authentication if for some reason Active Directory or other LDAP servers were not available. This local authentication capability should not be used as the primary method of authentication because alone it does not meet the necessary password complexity and history requirements mandated in the PCI specifications. CSA-MC was configured with role-based users for performing the various administrative tasks.

Additionally, a PCI compliance policy can be imported into the CSA-MC and can be used to enforce or monitor PCI compliance.

Figure 4-9 CSA Management

Name	Filter: PCI	OK	Version	<All>	Rule Modules	Description	Filter: <none>	OK
<input type="checkbox"/> A PCI LAR Policy					1 module			
<input type="checkbox"/> PCI 11.5 NCR ACS directories and files monitoring					1 module	PCI 11.5 NCR ACS directories and files monitoring		
<input type="checkbox"/> PCI Requirement 1.x Compliance					9 modules	Satisfies PCI requirements 1.3.5 and 1.3.9		
<input type="checkbox"/> PCI Requirement 10.x Compliance					12 modules	Satisfies PCI requirements 10.2.1 - 10.2.4, 10.5.1 - 10.5.5		
<input type="checkbox"/> PCI Requirement 11.x Compliance					6 modules	Satisfies PCI requirements 11.4 and 11.5		
<input type="checkbox"/> PCI Requirement 12.x Compliance					12 modules	Satisfies PCI requirements 12.3.10 and 12.5.5		
<input type="checkbox"/> PCI Requirement 2.x Compliance					6 modules	Satisfies PCI requirements 2.1.1 and 2.2.2		
<input type="checkbox"/> PCI Requirement 3.x Compliance					3 modules	Satisfies PCI requirement 3.0		
<input type="checkbox"/> PCI Requirement 4.x Compliance					2 modules	Satisfies PCI requirements 4.1 and 4.1.1 (Windows only)		
<input type="checkbox"/> PCI Requirement 5.x Compliance					3 modules	Satisfies PCI requirements 5.1.1 and 5.2 (Windows only)		
<input type="checkbox"/> PCI Requirement 6.x Compliance					6 modules	Satisfies PCI requirements 6.0 and 6.5		
<input type="checkbox"/> PCI Requirement 7.x Compliance					9 modules	Satisfies PCI requirement 7.0		
<input type="checkbox"/> PCI_Auditors_request					2 modules	PCI_Auditors_request		

For more information, refer to the following:

- Installation Guide for CSA Version 5.1:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_book09186a008067b78a.html

Data Center Services

CiscoSecure CS-MARS Event Monitoring and Alerting

CS-MARS was deployed as the central monitoring and alerting tool for events received from CSA clients, routers, switches, and authentication events from CS-ACS. To demonstrate event alerting, CS-MARS was configured to send e-mail alerts when it received a specific CSA event (that is, unauthorized writing to a CS-ACS event log). CS-MARS was deployed with role-based management, but supports only local user accounts and passwords. Because these local identities do not sufficiently enforce password complexity and history requirements mandated by PCI specifications, this console should be segregated from other general services in the data center and protected by an additional authentication resource. A compensating control of this type is not yet implemented in this design.

For more information, refer to the following:

- http://www.cisco.com/en/US/products/ps6241/products_installation_and_configuration_guide_book09186a00806bbf91.html

CiscoSecure Access Control Server (CS-ACS) Authentication

Individual user accounts were created in Active Directory and placed in groups based on typical enterprise individual roles. These groups were mapped to authentication groups in the CS-ACS, and assigned appropriate rights and permissions per group. This method of authentication was used to ensure appropriate password complexity, history and inactivity requirements. The CS-ACS product alone does not meet these requirements as a standalone authentication product.

For more information, refer to the following:

- Cisco Secure ACS Installation Guide version 4.1:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_guide_book09186a008070a5ff.html
- Cisco Secure ACS Configuration Guide version 4.1:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_configuration_guide_book09186a0080721d25.html

CiscoWorks Network Compliance Manager (C-NCM)

C-NCM was used to enforce compliance policy as established across validated devices. If a device were to have its configuration changed, outside of corporate policy, C-NCM can dynamically restore the configuration of the devices it manages. C-NCM supports a large number of multi-vendor products.

For more information, refer to the following:

- CiscoWorks NCM Installation Guides:
http://www.cisco.com/en/US/partner/products/ps6923/tsd_products_support_install_and_upgrade.html
- CiscoWorks NCM End User Guides:
http://www.cisco.com/en/US/partner/products/ps6923/products_user_guide_list.html

Internet Edge

Cisco Firewall Service Module (FWSM)

Cisco FWSM was configured based on common best practices and recommendations:

- Insecure services such as FTP mode passive were disabled from the configuration.
 - AAA Authentication was configured and pointed to the CS-ACS, a local user name and password were configured to authorize access in the event ACS was not reachable. This local account password should be changed quarterly.
- Access-list configured on FWSM were very specific (i.e., allowed only specific protocols and ports) needed for communication.
- Allowed management session to FWSM only from specific host using SSH version 2
 - The local security certificates were created using the **crypto key generate rsa** command; the key length set to 1024 bits.
- Logging was configured to send syslog events to CS-MARS.
- The FWSM configurations were backed up using C-NCM.

For more information, refer to the following:

Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide, 3.1

http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg.html

Service Module Design with ACE and FWSM

www.cisco.com/univercd/cc/td/doc/solution/ace_fwsm.pdf

Cisco Intrusion Detection System Services Module (IDSM2)

Cisco IDSM2 was configured based on common best practices and recommendations:

- IDSM2 was configured to lock accounts so that users cannot keep trying to log in after a certain number of failed attempts.
- Allowed management of IDSM2 only from a very specific host using Cisco IPS Device Manager with SSL connection.
- The attack information provided by IPS software was sent to CS-MARS for event correlation.
- Login banner was configured to notify users about the private system and device they are accessing.
- IDSM2 was configured to monitor VLANs in DMZ zone.

For more information, refer to the following:

Configuring the Cisco Intrusion Prevention System Sensor 6.0

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids13/cliguide/index.htm>

Cisco ACE XML Gateway

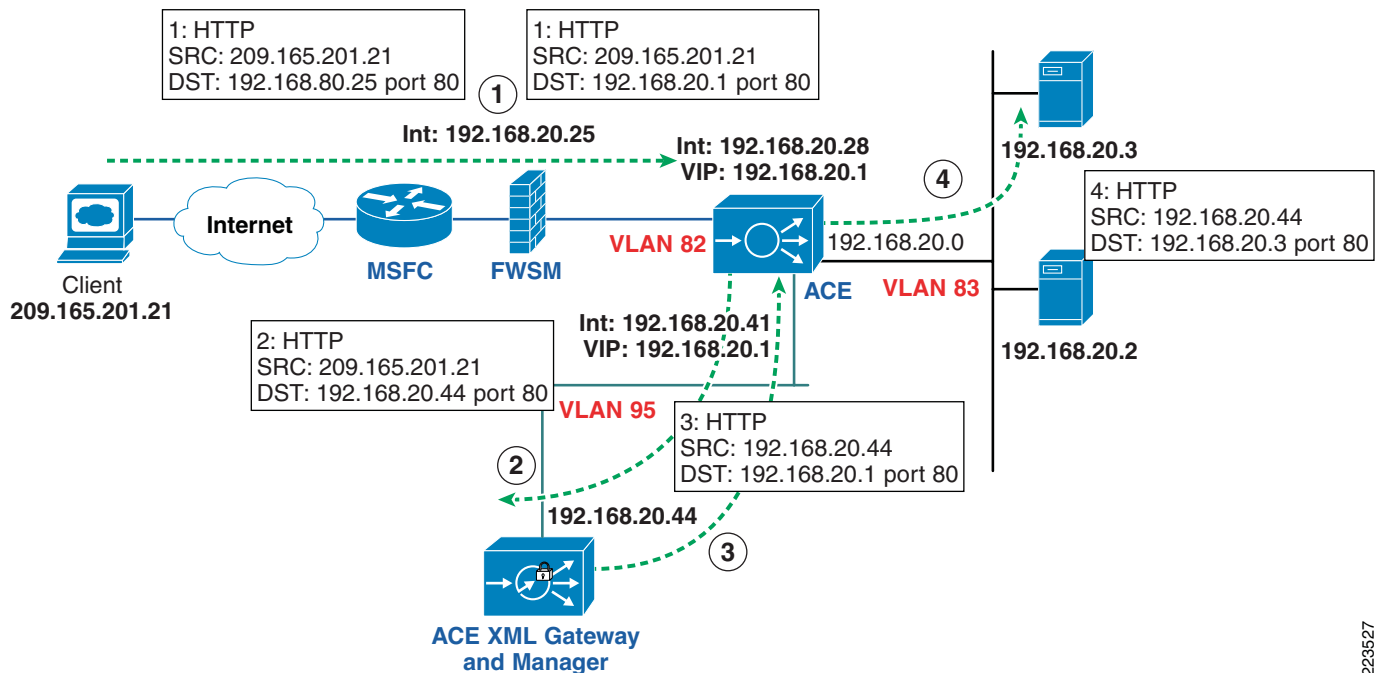
The Cisco ACE XML Gateway delivers firewall capabilities and provides the critical protection needed at each service perimeter, between different trust zones. In addition to working with transport and session layers of network traffic, the Cisco ACE XML Gateway differs from network firewalls in that it focuses primarily on the application layer and works with the payload of the XML message. In the perimeter defense role, the Cisco ACE XML Gateway performs a broad range of security services, such as guarding against malicious XML payloads, structurally invalid XML messages, and XML denial-of-service (XDoS) attacks, and performs other security functions such as non-repudiation; message encryption and integrity; and privacy.

In the lab environment, Cisco ACE XML Gateway and Cisco ACE XML Manager were configured on the the same appliance. The administration server for Cisco ACE XML Gateway implementation is the Cisco ACE XML Manager. The Cisco ACE XML Manager acts as the development and monitoring point for the system. It serves as a web console, which is the web services interface for configuring and monitoring the system. The web application servers in the Internet edge DMZ are running an online banking application and other web applications. The Cisco ACE XML Gateway tests were primarily focused on mitigating attacks on well know web-application security flaws mentioned in PCI 6.5 requirement.

In the scenario illustrated in [Figure 4-10](#), the clients generate a HTTP request to the NATed virtual IP address (VIP) on the Cisco Application Control Engine (ACE) module. This request is then forwarded to Cisco ACE XML gateway which performs its threat defense against application layer attacks and multiplexes HTTP 1.1 request back to the servers. Here, the Cisco ACE XML Gateway acts as reverse proxy appliance that dispatches the inbound HTTP traffic to a set of servers. Cisco ACE XML Gateway can be configured for server pooling of servers in DMZ. This provides improvement in the scalability and reliability of the services provided by the backend servers that are exposed through the Cisco ACE XML Gateway.

Cisco ACE XML Gateway currently does not support any box-to-box redundancy. Multiple Cisco ACE XML Gateways are added as part of Cisco ACE system design, thereby providing redundancy. The Cisco ACE makes a load-balancing decision about which Cisco ACE XML Gateway to forward the incoming request to on the basis of configured policies and state of individual Cisco ACE XML Gateways.

Figure 4-10 Clients-to-Server HTTP Traffic Flow



223527

For more information, refer to the following:

- Cisco ACE XML Gateway and ACE XML Manager implementation and configuration:
http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html
- Cisco ACE Module configuration, administration, and security configuration:
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_installation_and_configuration_guides_list.html
- Service Module Design with Cisco ACE and FWSM:
www.cisco.com/univercd/cc/td/doc/solution/ace_fwsn.pdf

Additional Elements

Time synchronization plays a critical role in event and audit log correlation. For this reason, the PCI requirement is to deploy redundant NTP servers that are synchronized against several reliable time sources. Two VMware-based NTP appliances were deployed to provide this service. These appliances were based on Mandriva Linux 2006 and use ntpd 4.2.0@1.1161-r. This appliance pulls random IP addresses from pool.ntp.org (13 + time.nist.gov). It then synchronizes the virtual machine clock and starts the NTP server service. All network devices and servers point to these appliances to maintain time synchronization.

Application Servers Point-of-Sale (POS)

NCR

NCR provided the POS client work station and servers. One of the servers was loaded with NCRs Advanced Checkout Solution (NCR-ACS) and other server was loaded with NCRs Advanced Store Workbench (ASW) software. The client station is NCR RealPOS80c system running Windows embedded XP version 2. NCR-ACS application is used primarily by high-volume retailers.

Advanced Checkout Solution (NCR-ACS)

The NCR-ACS platform is made up of several modules and services including Transaction Management Services (TMS) and Cooperative Services. These software components, combined with industry-standard operating systems, provide the additional functionality and security necessary for retail transactions. The POS server controls data between the POS terminals and server and ASW clients with TMS service. See [Figure 4-11](#).

The TMS layer of NCR-ACS is a key component of the NCR-ACS architecture. These services consist of server and workstation components that support store sales and office applications by providing straightforward access to data files and peripherals. TSM also assists in managing store POS system complexities of redundancy, communications, reaction to error conditions, and recovery. NCR-ACS TMS's are integrated with underlying client-server operating systems, LANs, and WANs.

All transactions are written to the NCR-ACS Transaction Log (TLOG). After a POS application writes a transaction to the TLOG file, the NCR-ACS Asynchronous Update Process (AUP) program on the server reads the file, processes TLOG data, and updates the store accounting files. NCR-ACS also offers the option of outputting in the IXRetail POSLog format.

Dependent Applications

The NCR-ACS application is dependent on the following third-party applications and software development:

- Microsoft Visual Studio.Net
- Microsoft's Managed Extensions for C++

Database Software

Microsoft SQL Server relational database system is used as data storage for the NCR-ACS application.

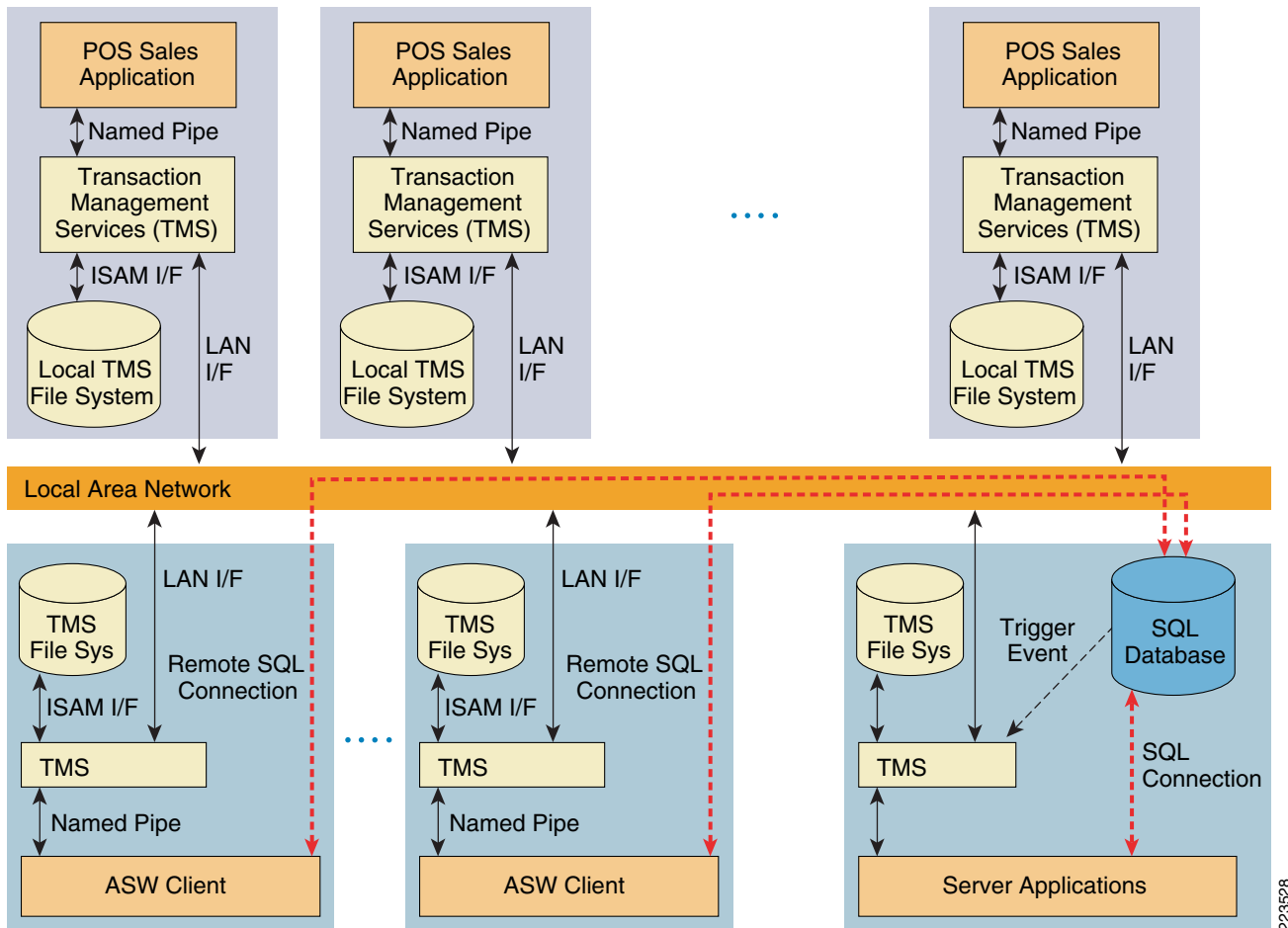
Advanced Store Workbench (ASW)

The ASW provides a graphical user interface that runs on a PC with Microsoft Windows Operating System, but presents a simple, easy-to-use, tabular-based back office user interface to store operations' personnel. The tabular form and tool boxes with standard tools in them, provides an easy-to-use navigational tool for accessing store applications.

The ASW takes full advantage of the open nature of NCR-ACS' architecture shown in [Figure 4-11](#). It takes a standard off-the-shelf PC, an industry standard Ethernet card and TCP/IP communications protocol stack, and integrates those pieces with the transaction management services LAN and ODBC driver interface.

ODBC is a Microsoft standard for open database connectivity which gives the user a sequel-like interface into a file system. In this particular instance, the ODBC driver takes SQL commands on one side and translates them into file system commands for the Advanced Checkout Solution file system. This information is then fed into the ASW using the appropriate Microsoft Office application to display the data in a meaningful way.

Figure 4-11 NCR ACS Single Server Architecture



TMS is the primary proprietary interface for file and LAN between clients and server. POS clients do not access SQL Server. The Database applications reside on the ASW client and server and access one store database. When the database has been modified, the SQL server triggers notification to TMS.

Mobile Retail Manager (MRM)

MRMs are applications that run on hand-held devices. Any device that supports Windows customer edge (CE) device can support these applications to do the store inventory. In the lab, MRM was installed on Intermec CN3 wireless hand-helds running Windows Mobile version 5.0 for checking store inventory. There are ten base functions supported by MRM:

- Store sales summary report
- Reset password

- PLU maintenance
- Item movement report
- Department summary report
- Change merchandising message
- Cash drawer position report
- Add operator
- Terminal Productivity
- Operator Productivity

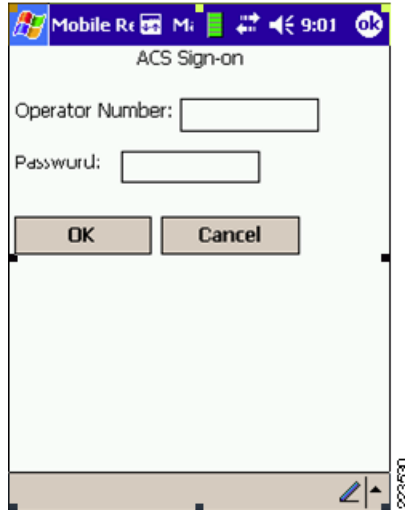
MRM can be executed from the Start Menu of Intermecc CN3 devices running Window Mobile version 5. The program displays a list of available reports. To run a report, simply select the report's name in the main list, and then select the **Run Report** button. See [Figure 4-12](#).

Figure 4-12 **MRM**



When the **Run Report** button is selected, an NCR-ACS sign-on screen is displayed (see [Figure 4-13](#)).

Figure 4-13 MRM Sign-on Screen



The main purpose of MRM is to keep the supervisor/manager on the floor so the manager does not have to go look at reports or do other store related functions. They can look at them on the device and they can be on the floor to interact with customers and address store issues.

NCRs HOME/HOUSE Package

The *HOME/HOUSE* package is required to access and work with the various types of files created and maintained by NCR-ACS. The file of interest is Transaction Detail Log (TLOG), which is the detail transaction file created and maintained by NCR-ACS. This file is normally kept in a binary type format with headers, leaders, and other special control records used to define the segments and the data elements within them. The *HOME/HOUSE* package is used to translate this binary file into an ASCII type file. Selectable options include; defining the separation character, the termination character, and whether or not header and/or trailer records are required. This activity can be tailored to run at specific times during the day and "trickle" the data to host, or it can be triggered during end-of-day (EoD) processing. If triggered as an EoD process, a single file for a day's transactions would be created.

The *HOME/HOUSE* package is usually executed on a host level box (primary in the data center) running either Windows or a version of UNIX. The method of sending the data files to host level is the responsibility of the user. This usually consists of a FTP file to the host machine. This process can be automated both at the store and host levels. The *HOME/HOUSE* package can be tailored to create data files that are ready to be processed by a database engine.

In the Cisco lab environment, the NCR-ACS Server, ASW client and RealPOS 80c systems were pre-configured by NCR with appropriate software before it was shipped to Cisco. The servers and clients were configured to received DHCP IP address from a Windows DHCP server located in data center. The HOME script installed in NCR-ACS server is executed by store closing using ASW client software. The script converts the binary TLOG file located under `ACS\server\data` directory into ASCII format. This ASCII file is stored under a directory `C:\acs\Server\Data\host\dc\070913`, where the last directory is the date (in this case it is September 13, 2007). The directory "070913" is created on the fly when the store closing is initiated using ASW client. If store closing is triggered as EoD processing, a single file (for example, `dc.xxx`) is created under `070913` directory.

The HOUSE scripts was not used in the Cisco lab environment. The TLOG ASCII file was securely FTPed manually through a secure Cisco IPSEC Virtual Private Network (VPN) from store ACS server to a EMC storage environment.

CSA was used in Cisco lab environment to monitor and log access to use of NCR-ACS application binaries and access to NCR application log files, protect NCR RealPOS80c system, and protect ASW server. Anti-virus was also loaded on the NCR-ACS Server, NCR ASW Server, and RealPOS 80c system.

For more information on NCR RealPOS 80c POS workstation, refer to the following URL:

http://www.ncr.com/products_and_services/point_of_sale/pos_workstations/ncr_realpos_80c_.jsp?lang=EN

For more information on NCRs Advanced Checkout Solution (CS-ACS), refer to the following URL:

http://www.ncr.com/products_and_services/point_of_sale/software/food/advanced_checkout_solution.jsp?lang=EN

MS-RMS

The Microsoft Retail Management Solution (MS-RMS) was a free trial download that was implemented to test modern POS systems within the architecture. This was deployed in a non-standard fashion with the Backstore database installed centrally in the data center site. The handhelds and POS registers connected back to the database using SQL port TCP 1433. If for some reason the WAN connection were not available, the systems used a local database to store the transactions. Microsoft has an additional product called System Headquarters that is intended to manage a distributed architecture such as this, but was not available for use in the Cisco lab.

The MS-RMS POS application was installed on two registers provided by IBM, and a General MCS 7825 server in the data center. The registers were also configured with CSA clients and anti-virus software.

For the mobile Handhelds, MobiSuite 4 was installed. This application supports connectivity to MS-RMS and can perform line busting POS transactions, as well as inventory management using the Intermec devices.

Because no payment system was available at time of the audit, the MS-RMS systems and IBM registers were not included in the PCI audit by the QSA.

Installation of MS-RMS was very straight forward with the included documentation:

<http://www.microsoft.com/businesssolutions/retailmanagementsystem/default.msp>

Wincor-Nixdorf

Wincor-Nixdorf provided their TP.Net POS product along with three Beetle registers. One register was installed in each location (small, medium, and large) with their back-of-store SQL database, and transaction server installed on an MCS 7825 server in each store. This represents the recommended client/server Type 2 architecture installation that can support 50 terminals per store. Other configurations can support up to 200 terminals per store.

The TP.net POS application interacts with payments applications through a standards-based Open Payment Initiative (OPI.) interface that is the Wincor-Nixdorf standard interface for card payment systems. The interface is based on TCP/IP communication between the sale system and the card payment system. The protocol is XML-based. The TCP/IP communication occurs generally within a company internal network, mostly on one single sale system via local host. The protocol data is not stored on any system, except that the participating systems (sale system, card payment system) are storing that data for logging purposes. The logging should be deactivated in productive environments.

O.P.I. does not store any cardholder information. The O.PI interface is responsible for the interchange of the cardholder information between the TP.net sale system and the card payment system. The storage of the cardholder information is the responsibility of the sales system and the card payment system. In TP.net, the retention time of the transaction data is configurable to set the storage of the cardholder information to a minimum.

As no payment system was available at time of the audit, the Wincor-Nixdorf systems and registers were not included in the PCI audit by the QSA.

For more information, see the following:

- <http://www.wincor-nixdorf.com/internet/com/Products/Software/Retail/StoreSolutions/TPnet/Main,templateId=blob.jsp,property=DetailPaper.pdf>

Microsoft Windows Servers

Each of the Microsoft Windows servers were hardened using published best practices (see <http://www.CISecurity.com>). Because retailer needs regarding server hardening differ greatly, this aspect of the management platforms was not directly audited by the QSA.

Following are the steps used for server building/hardening:

- Image server hardware using OS imaging software and file
- Re-name server and change SID
- Change administrator password for local account
- Join server to domain
- Downloaded and installed all critical and security updates
- Install anti-virus client and update AV definitions
- Install CSA Client and verify registered to CSA manager
- Set RDP to high encryption (verify Group Policy)
- Install appropriate application(s) for server
- Use Microsoft Security configuration wizard to disable all unused services, and tighten windows firewall
- Run MBSA tool; remediate any additional items on server
- Verify desktop policy to logout/lock desktop after 15 minutes of inactivity

PCI requirements are that servers are hardened per current industry best practice standards. NIS, SANS, CISecurity and ARF are several resources with current guides regarding server hardening.

Microsoft's Active Directory account policies support the configuration of several critical mechanisms regarding user authentications and passwords allowing it to conform to PCI requirements right out of the box. The password policies in AD are defined in the domain security settings policy. These were the default settings from a clean installation of Microsoft Windows 2003 server R2. These default settings exceed PCI requirements, but should be verified in any installation. [Figure 4-14](#) shows the password policy screen.

Figure 4-14 Password Policy

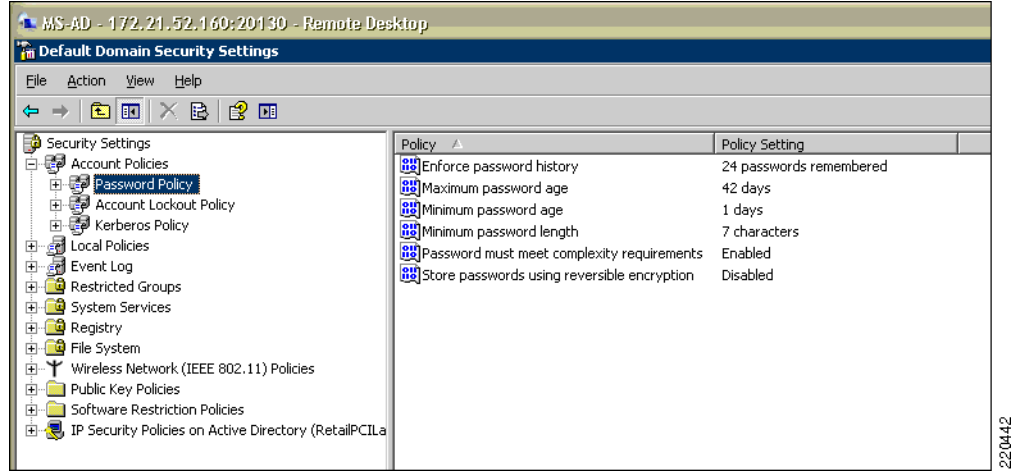
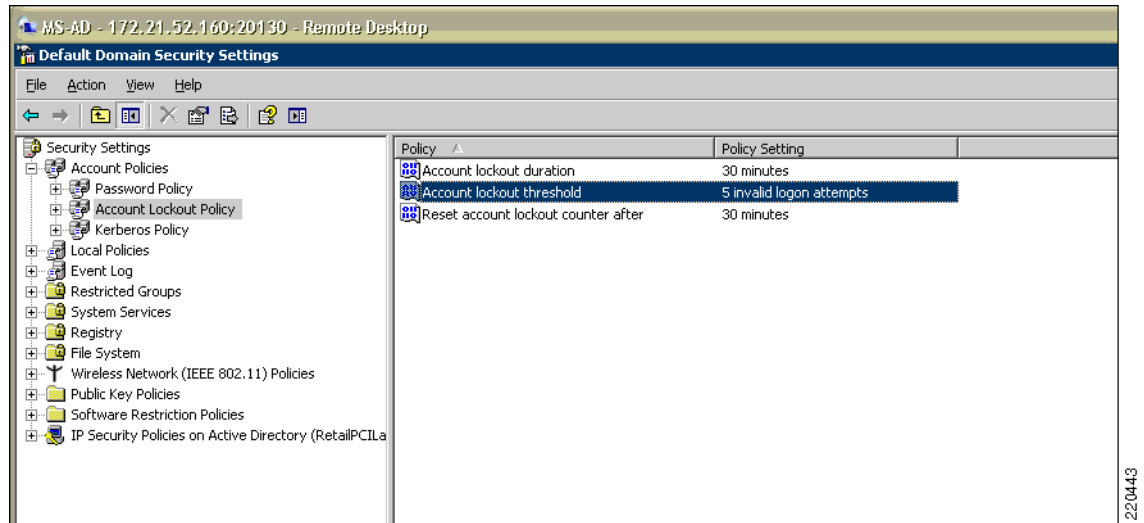


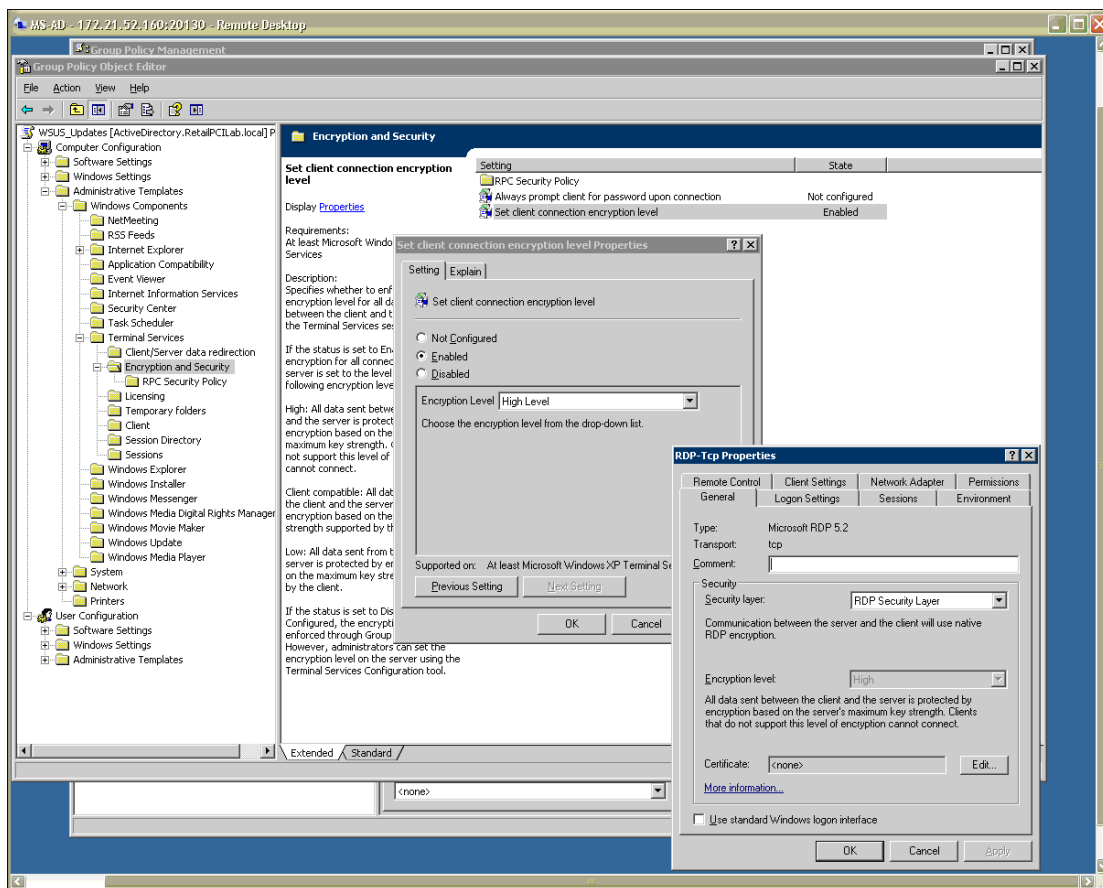
Figure 4-15 shows the Account Lockout Policy screen.

Figure 4-15 Account Lockout Policies



The Remote Desktop Protocol, that is used for remote server management of Microsoft Windows servers, supports various levels of security. To meet PCI requirements, this setting should be set to “High Encryption” for all devices. To achieve this, a change was made to the Domain Group Security Policy, as shown in Figure 4-16.

Figure 4-16 Domain Group Security Policy



This domain group policy was also edited to enforce the requirement of a 15-minute session timeout. This was accomplished by locking the desktops of all servers and workstations after 15 minutes with a password-protected screen saver.

Payment Devices

Mx Series

VeriFone MX870 and MX850 were used as payment devices in the lab, connected to NCR RealPOS80c system. MX800 Series systems support Smart Card and magnetic stripe payments while complying with the latest payment security standards.

Both Mx870 and Mx850 series PIN pads are Payment Card Industry PIN Entry Device (PCI PED) approved (online and offline) for PIN entry and EMV (European Visa/MasterCard) levels 1 and 2 certified.

For more information on VeriFone MX Series, refer to the following URL:

<http://www.verifone.com/products/devices/mx/index.html>

Vx Series

The wireless Vx 670 PIN pad was used in the lab, connecting to the Cisco Unified Wireless infrastructure. The Vx670 PIN pad is PCI PED approved. At the time of testing, Vx670 supported only Wi-Fi Protected Access (WPA). There was no WPA2 support.

**Note**

The scope of Vx670 did not include any payment processing as it required a payment processing gateway for testing. The scope was limited to testing Vx670 and it was able to securely connect (using WPA) to Cisco Unified Wireless Infrastructure.

For more information on Verifone Vx 670, refer to the following URL:

<http://www.verifone.com/products/devices/vx/vx670.html>

Encryption and Key Management

Effective, persistent security for payment card information requires encryption controls that can secure every layer of the IT stack. The section below, covers two RSA encryption and key management products—RSA Key Manager and RSA File Security Manager, which were used in the PCI Solution for Retail's validation process in the lab.

RSA Key Manager

Figure 4-17 shows the RSA Key Management deployment. RSA Key Manager provides enterprise-wide, centralized encryption management allowing enforcement of policy across various encryption usage points. It provides centralized provisioning and lifecycle management for encryption keys and other security objects to reduce the complexity in deployment and ongoing management of encryption controls.

Key management, especially in large connected and distributed enterprises, is difficult to perform correctly. Keys need to be generated carefully and then securely transferred to multiple client applications with guaranteed integrity. A very secure and reliable storage mechanism is required because the loss of a critical key can result in the loss of the critical data it protects. Any outage of the key management system can prevent the business from functioning. Mechanisms need to be provided to enforce security policies for keys such as key rollover, auditing and revocation. A key management system should also be easy to use by those implementing encryption

RSA Key Manager is designed to address all of these concerns to help reduce complexity in encryption deployments. RSA Key Manager software provides policy-based, centralized cryptographic key administration for enterprises that implement encryption-based data protection.

RSA Key Manager consists of three main components:

- RSA Key Manager Clients distributed within an organization's business applications.
- A centralized RSA Key Manager Server.
- An administration console that provides administrator access to the RSA Key Manager Server.

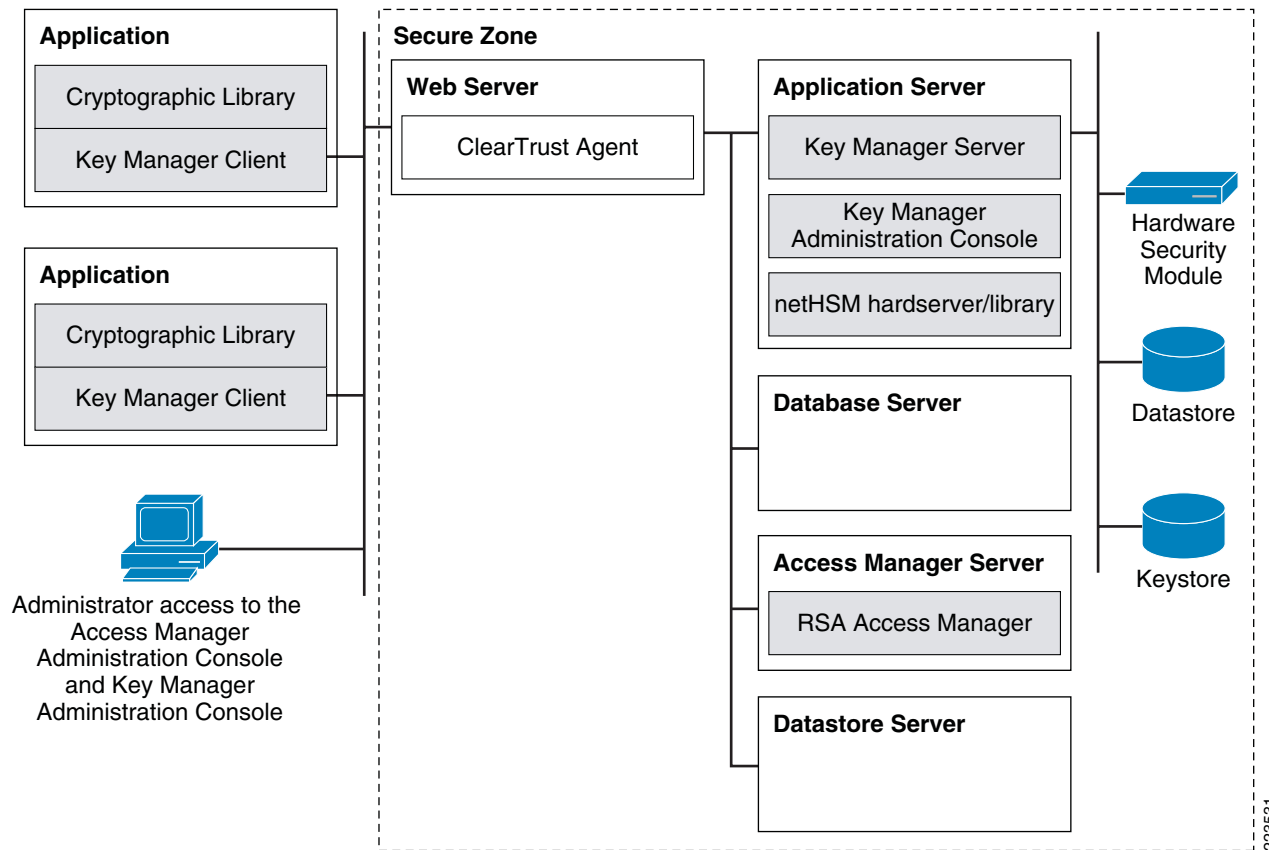
The fundamental services provided by a Key Manager deployment include:

- Key management
 - Key generation—Keys are optionally generated automatically as they expire, providing hands off continuity of operation for expired keys.

- Key storage—Keys are stored centrally, using standard database technologies.
- Key retrieval—Keys are retrieved quickly, easily and securely using client server capabilities.
- Key policy definition—Key properties are aligned with corporate data.
- Classification policies:
 - Key expiration—Keys expire automatically based on policies.
- Cryptographic services for applications:
 - Strong authentication for Key Manager Clients. Public Key Infrastructure (PKI)-based authentication required for cryptographic key access.
 - The Key Manager Client library supports C applications only.
- Continuous operations provided by configurable key caching on the client.

Clients can keep local copies of keys in persistent and non-persistent cache, providing standalone operations during network outages.

Figure 4-17 RSA Key Manager Server Deployment



Deployment Components

In the lab, following components were deployed for successful working of RSA Key Manager:

Web Server

The web server accepts requests via HTTPS from Key Manager Clients and administrators and forwards them to the application server. The Web server is the entry point into the secure zone within which all access is secured by user authentication, user authorization and firewalls. In this environment Microsoft Internet Information Services (IIS) 6.0 is used.

Application Server

The application server accepts requests from the Web server to invoke Key Manager Server or Key Manager Administration Console functionality. In this environment Apache Tomcat (5.5.20) is used.

Database Server

The database server stores the RSA Key Manager Server database. In this environment Microsoft SQL Server 2005 is used.

RSA Access Manager Server

The RSA Access Manager Server runs access management software, which performs authentication and authorization services for the Key Manager Server deployment (refer to [RSA Access Manager, page 4-38](#)).

In order to provide a reference for this solution in the Cisco lab environment, RSA and Cisco created an environment that demonstrates the solution in action. Keys from the RSA Key Manager are generated via a command-line utility on a PC running windows XP that leverages the RSA Key Manager Client (a sample program) application programming interface (API). This is a valid proof-of-concept, but true use cases would rely on customers or third-party partner products leveraging this API to embed the client code directly into the POS software; thus, creating a truly repeatable solution that is fully supported.

Figure 4-18 Typical Application Leveraging RKM Client

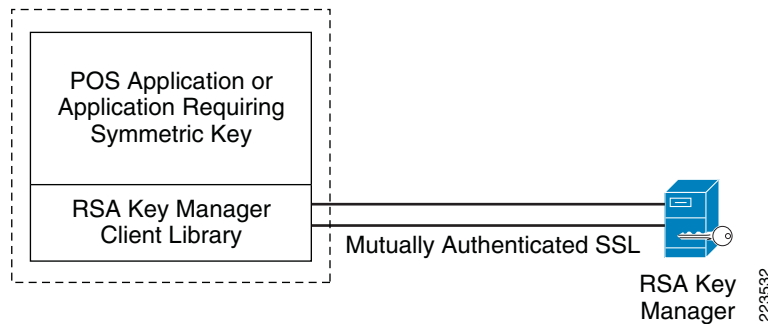


Table 4-1 RSA Key Manager Functionality

RSA Key Manager Server	RSA Key Manager Client
Secure retrieval and provision of keys to Key Manager Clients.	Provision of an API for operational users.

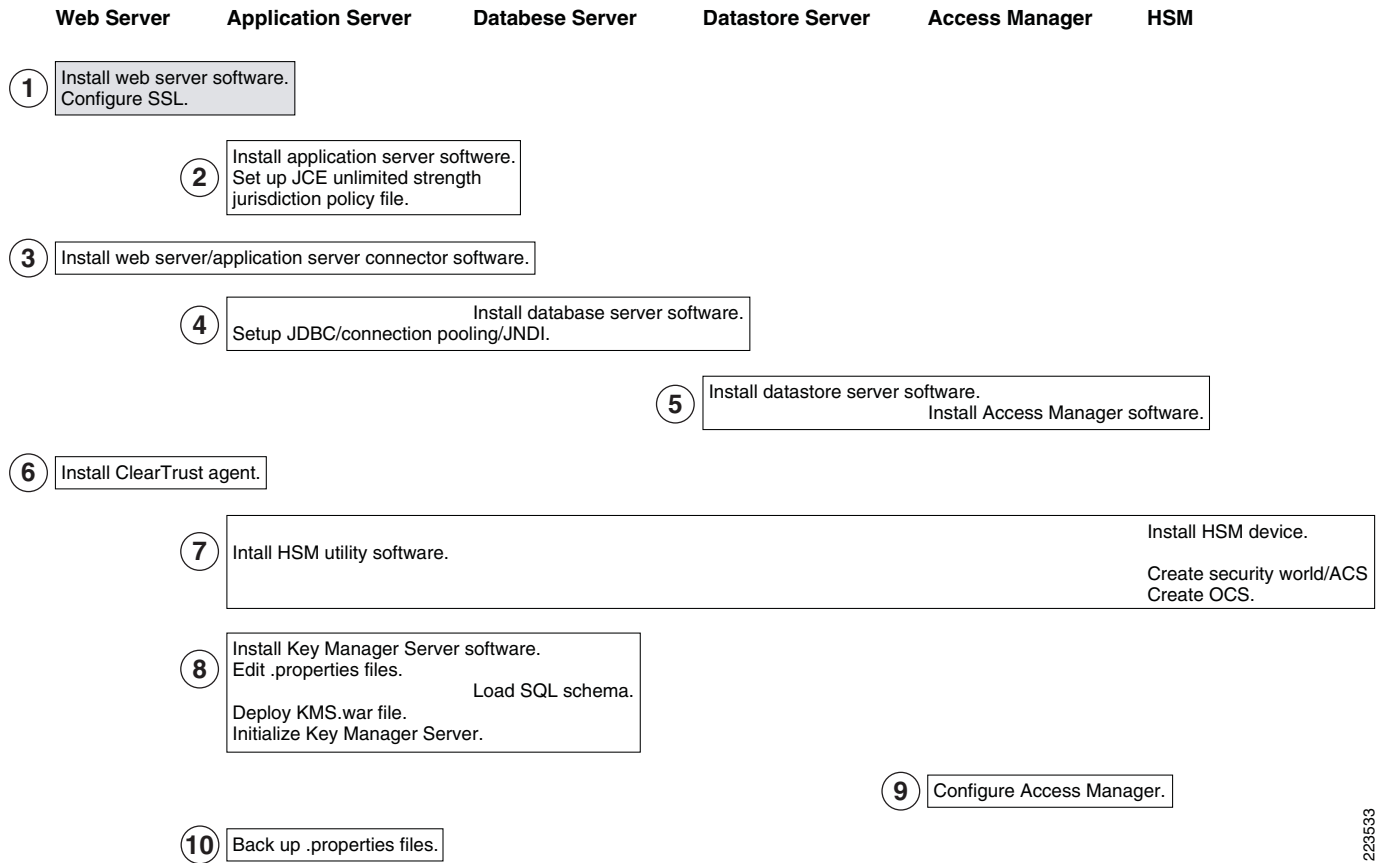
Table 4-1 RSA Key Manager Functionality (continued)

Secure, centralized cryptographic key storage.	Retrieval of cryptographic keys to perform encryption, decryption, MAC, and MAC verification operations.
Generation of strong cryptographic keys.	Ability to store cryptographic keys on the Key Manager Server.
Management of cryptographic key life cycles.	Configurable local caching of cryptographic keys. Cryptographic operations can proceed when connection to a Key Manager Server is lost.
Centralized key, key policy, and key user administration.	Ability to manually maintain key life cycles.
Application level authentication and authorization of key users.	Ability to retrieve and update key and key policy information.
Storage of external data associated with a collection of keys or an individual key.	Limited access to Key Manager Server administration functions for administrative users.
Logging of all key management operations.	Configurable logging of all key operations.

Configuration

This guide does not include every step to install the server but instead provides an overview of the configured lab environment and comments on best practices for deployments. Complete installation instructions can be found in the RSA Key Manager product documentation or for experienced help contact RSA Professional Services (<http://rsa.com/node.aspx?id=1310>).

Figure 4-19 High Level Process of Installing a Key Manager Server Deployment



223533



Note

In this lab environment a Hardware Security Module (HSM) was not used in the solution validation.

Web Server Installation

The IIS web server requires communication via an SSL session. RKM client certificates presented to the web server must be issued by the same root of the SSL certificate on the web server or be trusted by the IIS web server via the IIS certificate trust list. Details regarding this SSL and certificate trust list configuration can be found in your Microsoft IIS documentation.

Tomcat Application Server and Jakarta Connector Installation

Apache Tomcat is used as the engine for the RKM Server and is deployed by copying the KM S. WAR file to the <Tomcat install folder>\webapps directory or through the use of the Tomcat Web Application Manager.

Once the Jakarta connector is installed and configured it is a good idea to ensure that SSL web requests (typically port 443) are forwarded to the application server. For example, do the following:

1. Create Tomcat install folder>\webapps\test\test.html
2. Then place the URL /test/* in <Tomcat install folder>\conf\workers2.properties file.
3. When you hit https://localhost/test/test.html, the request should be forwarded and display that page.

Instructions for the above are in the installation guide but are commonly overlooked. If you can not forward requests to the application server, do not continue with the installation.

Another common practice is to secure the connection between the web server and the application server, especially if the components reside on different hosts. This is done through the Tomcat and is accomplished by creating or importing a certificate for the Tomcat application server.

Detailed instructions for doing this can be found at the following URL:

<http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>

Database Installation and SQL ODBC Connector

The out of the box install steps are very clear on these installation items and should be followed exactly. The inability to contact the keystore located in the SQL server will cause your web application deployment to fail.



Note

In the lab environment, the solution did not use a native PKI Infrastructure, but instead the RSA Key Manager client certificate, web server SSL certificate, and application server certificates were created using RSA's PKI infrastructure and the certificates were manually imported to RSA Key Manager client and server.

CSA was used to monitor and log access to use of RSA Key Manager's application binaries and access to RSA Key Manager's log files.

RSA Access Manager

The RSA Access Manager, formerly known as RSA ClearTrust, web access management solution enables organizations to cost-effectively provide secure access to web applications within intranets, extranets, portals and exchange infrastructures. See [Figure 4-20](#).

RSA Access Manager software is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs.

Figure 4-20 RSA Access Manager Protecting the RSA Key Management Servers Web Interface

rchakkin: Default Administrative Group/Default Administrative Role

Home Define Resources Authorize Access Manage Users Delegate Administration Help Options Log Out

Define Resources > Applications:

Resources in Application

This page lists all the resources in this application. By adding a resource to an application, you can then authorize access to it using entitlements or Smart Rules. To add additional resources to this application, click **Add New**.

Filter resource list by type: All

Add New Resources in Application: KMS Webservice Display 10 records per page

Showing 1-2. <Back | Next>

Actions	Resource	Type	Server	Description	Delete
Actions...	KMS Webservice	Application			<input type="checkbox"/>
Actions...	/kms/*	URL	KMS Webservice		<input type="checkbox"/>

Showing 1-2. <Back | Next>

Done

How To... Hide

- Understand Applications
- Understand Resources

203634

RSA File Security Manager

The RSA File Security Manager is a software-based security solution that provides transparent encryption of files/folders in conjunction with role-based access control on heterogeneous platforms.

RSA File Security Manager does not require the user to modify applications and does not have any specialized hardware needs. It offers centralized management of role-based access control to files/folders and helps achieve separation of duties between system and security administration. All activity in the secured folder is logged securely for audit purposes.

In the lab environment, one copy of the RSA File Security Manager Adapter software was installed on the NCR POS server (the NCR-ACS POS system did not encrypt transaction logs) and another copy on a server located in data center connected to SAN-based storage. This represents the recommended architecture. At the store server, RSA File Security Manager secures the folder that contains the transaction logs generated by the POS registers. Access to the transaction log folder is restricted to only authorized users and fingerprinted local applications. The authorized applications that have access to the secured folder are the POS application and the SFTP client that transfers the transaction logs securely to the server in data center. Administrators and other super users are unable to access the transaction log folder unless they are provided access by the File Security Manager security officer.

Further lab activities included aggregating the the transaction logs onto a server mapped to a storage drive in the data center. Storage layer. The server aggregates the transaction log files from each store server and stores them locally for reconciliation. RSA File Security Manager is installed on this server in the data center as well. The RSA File Security Manager Adapter software CSA software secures the server repository from both accidental and malicious access. Only the server's executable and specific users and applications authorized by the File Security Manager security officer would be configured for plaintext access to the data in the folders. By default, File Security Manager reduces all file/folder access to a least privileges model.

For more information on RSA File Security Manager, see the following URL:

<http://www.rsa.com/node.aspx?id=3228>

Remote Access

RSA Authentication Manager/RSA SecureID and RSA enVision

RSA SecurID® solution includes:

- RSA Authentication Manager—Used for administration, user authentication, password integration, and auditing.
- RSA Authentication Agent—Installed on local computers and servers.

Using RSA Authentication Manager software and RSA Authentication Agent 6.1, RSA SecurID can enable two-factor user authentication. RSA SecurID two-factor authentication is based on something you know (a password or PIN) and something you have (an RSA SecurID authenticator), providing a much more reliable level of user authentication.

On systems protected by RSA SecurID technology, the RSA Authentication Agent prompts users for their logon name and passcode. This passcode is a combination of a one-time 6-digit RSA SecurID token code, which changes every 60 seconds, plus a unique Personal Identification Number (PIN). RSA Authentication Agent then requests authentication services from RSA Authentication Manager, and, based on RSA Authentication Manager responses, enables or prevents logging on to the protected system.

In the lab environment, RSA SecurID technology and RSA Authentication Manager software were used primarily to meet the two-factor authentication requirement stated in PCI DSS document for remote access to networks by employees and third parties. The RSA Authentication agent 6.1 was installed on a Cisco Secure Access Control Server (CS-ACS). To facilitate communication between the CS-ACS and the RSA Authentication Manager/RSA SecurID, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the CS-ACS within its database and contains information about communication and encryption. The communication between Cisco Secure CS-ACS and RSA Authentication Manager uses native RSA SecurID authentication protocol.

The remote user uses Cisco VPN client to establish end-to-end, encrypted VPN tunnels for secure connectivity. The secure VPN connection is terminated on Cisco Adaptive Security Appliance (ASA) Firewall. When the remote user connects to network using Cisco VPN, the remote user is prompted for username and passcode (the combination of the RSA SecurID tokencode and the user PIN). This information is sent to CS-ACS and then forwarded to RSA Authentication Manager for user authentication verification.

To monitor RSA Authentication Manager audit logs, a pre-configured RSA enVision appliance was used in the lab. To securely collect the audit logging information from RSA Authentication Manager, a "NICsftpagent" was installed on RSA Authentication Manager. The audit logs were securely FTPed to RSA enVision every 60 minutes for reporting, alerting, and long-term storage. The logs are stored in a proprietary database in RSA enVision.

For more information refer to the following:

- RSA SecureID configuration
http://www.rsa.com/rsasecured/results.asp?product_program=107&page=3
- RSA Authentication Manager
<http://www.rsa.com/node.aspx?id=1166>
- RSA enVision
<http://www.rsa.com/node.aspx?id=3170>

Troubleshooting Configuration

Several common mistakes that were made, including the following:

- In the initial deployment of switches, the provided IOS code did not support secure HTTP or SSH management. After the IOS upgrade, non-secure protocols still need to be disabled: **no ip http-server**, **ip http secure-server**, and for VTY interfaces, **transport input SSH**.
- With the use of CS-M, access lists in routers should not be modified locally in the routers. This causes potential problems when re-deploying access list updates via CS-M.
- With the use of the command **ip verify unicast source reachable-via rx** on each interface, the local LAN interfaces of the router could not be pinged because this feature would fail authorization because of anti-spoofing. Ping from the data center or a local client.
- In the installation of RSA Key Manager software, skipping minute details (e.g., correct Java version software code) documented in RSA Key Manager installation guide could cause issues in proper working of RSA Key Manager server or client

Recommended troubleshooting tips are as follows:

- While working on authentication for wireless clients, it was very useful to use a WildPackets OmniPeek Personal network analyzer on the wireless controller VLAN (via a switch span port) to monitor the progress of a user logging into the network.
- When diagnosing Syslog events being sent to the C-LMS server, Cisco used a WildPackets OmniPeek Personal network analyzer to verify that the wireless controllers were transmitting the logs even though Cisco works did not report them as the wireless controller device type is not recognized. The OmniPeek Personal analyzer is available as a free download, with the option to pay for support, at the following URL: http://www.omnipeek.com/omnipeek_personal.php
- Cisco found that the medium wireless controller would periodically stop responding. To restore proper operation, the router interface was pinged (**wireless-controller1/0**, **ip address 10.10.46.33**) from the exec prompt.

Results and Conclusions

This solution passed the QSA audit performed by Verizon Business. The network designs required only a few compensating controls for Device management and file integrity monitoring. Products that Verizon Business found most useful included CSA Manager and the CSA clients on the various management servers and the comprehensive network architecture. The detailed results of the audit can be found in [Appendix F, “Report on Compliance \(ROC\).”](#)



APPENDIX A

Bill Of Materials of Devices for Branch Stores

Small Store

Product	Description	Quantity
CISCO2821	2821 w/ AC Pwr,2GE,4HWIC,3PVDM,1NME-X,2AIM,IP BASE,64F/256D	1
S28NAISK9-12409T	Cisco 2800 ADVANCED IP SERVICES	1
MEM2821-256U512D	256 to 512MB DDR DRAM factory upgrade for the Cisco 2821	1
MEM2800-64U128CF	64 to 128 MB CF Factory Upgrade for Cisco 2800 Series	1
NM-CE-BP-40G-K9	Content Engine NM-Basic Perf-40GB	1
SF-ACNS-5.3-K9	ACNS Software v5.3	1
EVM-HD-8FXS/DID	High density voice/fax extension module - 8 FXS/DID	1
EM-HDA-6FXO	6-port voice/fax expansion module - FXO	1
PVDM2-32	32-Channel Packet Voice/Fax DSP Module	1
HWIC-4ESW-POE	4-Port Ethernet Switch HWIC with Power Over Ethernet	1
HWIC-4ESW-POE	4-Port Ethernet Switch HWIC with Power Over Ethernet	1
VWIC-2MFT-T1-DI	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert	1
WIC-1ADSL	1-port ADSL WAN Interface Card	1
AIM-CUE	Unity Express AIM -price includes 12 mailbox	1
SCUE-2.2	Cisco Unity Express base release	1
SCUE-LIC-25CME	Unity Express License 25 Voice Mailbox-Auto Attendant-CCME	1
CUE-LANG-ENG	Cisco Unity Express - British English	1
FL-CCME-SMALL	Cisco Call Manager Express Feat License For Up To 24 Users	1
CAB-AC	Power Cord,110V	1
PWR-2821-51-AC-IP	Cisco 2821/51 AC/IP power supply	1
AIR-LAP1131AG-A-K9	802.11ag LWAPP AP Integrated Antennas FCC Cnfg	1
S113RK9W-12307JX	Cisco 1130 Series IOS WIRELESS LAN LWAPP RECOVERY	1

Medium Store

Product	Description	Quantity
CISCO3845	3845 w/AC PWR,2GE,1SFP,4NME,4HWIC, IP Base, 64F/256D	2
S384AISK9-12409T	Cisco 3845 ADVANCED IP SERVICES	2
MEM3800-256U512D	256 to 512MB DDR DRAM factory upgrade for the Cisco 3800	2
MEM3800-64U128CF	64 to 128 MB CF Factory Upgrade for Cisco 3800 Series	2
CAB-AC	Power Cord,110V	2
NM-AIR-WLC6-K9	WLAN controller NM for 28/38xx ISR	1
NM-CE-BP-40G-K9	Content Engine NM-Basic Perf-40GB	1
SF-ACNS-5.3-K9	ACNS Software v5.3	1
SWLC6K9-11	WLAN Controller NM Software image	1
VIC-4FXS/DID	4 port FXS or DID VIC	1
VIC2-4FXO	Four-port Voice Interface Card - FXO (Universal)	1
VWIC-2MFT-T1-DI	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert	2
WIC-1ADSL	1-port ADSL WAN Interface Card	1
PVDM2-32	32-Channel Packet Voice/Fax DSP Module	2
AIM-CUE	Unity Express AIM -price includes 12 mailbox	1
SCUE-2.3	Cisco Unity Express base release - 2.3	1
SCUE-LIC-50CME	Unity Express License 50 Voice Mailbox-Auto Attendant-CCME	1
FL-CCME-MEDIUM	Cisco Call Manager Express Feat License For Up To 48 Users	2
CUE-LANG-ENU	Cisco Unity Express - North American English	1
PWR-3825-AC	Cisco 3825 AC power supply	2
WS-C3560-48PS-S	Catalyst 3560 48 10/100 PoE + 4 SFP Standard Image	2
CAB-AC	Power Cord,110V	2
GLC-T=	1000BASE-T SFP	4
CAB-SFP-50CM=	Catalyst 3560 SFP Interconnect Cable, 50cm	1
AIR-LAP1131AG-A-K9	802.11ag LWAPP AP Integrated Antennas FCC Cnfg	1
S113RK9W-12307JX	Cisco 1130 Series IOS WIRELESS LAN LWAPP RECOVERY	1

Large Store

Product	Description	Quantity
CISCO3845	3845 w/AC PWR,2GE,1SFP,4NME,4HWIC, IP Base, 64F/256D	2

S384AISK9-12409T	Cisco 3845 ADVANCED IP SERVICES	2
MEM3800-256U512D	256 to 512MB DDR DRAM factory upgrade for the Cisco 3800	2
MEM3800-64U128CF	64 to 128 MB CF Factory Upgrade for Cisco 3800 Series	2
VIC-4FXS/DID	4 port FXS or DID VIC	1
VIC2-4FXO	Four-port Voice Interface Card - FXO (Universal)	1
VWIC-2MFT-T1-DI	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert	2
WIC-1ADSL	1-port ADSL WAN Interface Card	1
PVDM2-64	64-Channel Packet Voice/Fax DSP Module	2
PVDM2-64	64-Channel Packet Voice/Fax DSP Module	2
AIM-CUE	Unity Express AIM -price includes 12 mailbox	1
SCUE-2.3	Cisco Unity Express base release - 2.3	1
SCUE-LIC-200CME	Unity Express License 200 Voice Mailbox-Auto Attendant-CCME	1
PWR-3845-AC/2	Cisco3845 redundant AC power supply	2
CAB-AC	Power Cord,110V	4
FL-CCME-192	Cisco CallManager Express Feat License Up To 192 Phones	2
CUE-LANG-ENU	Cisco Unity Express - North American English	1
PWR-3845-AC	Cisco 3845 AC power supply	2
WS-C4506	Catalyst 4500 Chassis (6-Slot),fan, no p/s	2
PWR-C45-2800ACV	Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
PWR-C45-2800ACV/2	Catalyst 4500 2800W AC Power Supply (Data and PoE)	2
CAB-AC-2800W-TWL K	U.S. Power Cord, Twist Lock, NEMA 6-20 Plug	4
WS-X4013+	Catalyst 4500 Supervisor II-Plus (IOS), 2GE,Console(RJ-45)	2
S45IPBK9-12231SG	Cisco CAT4500 IOS IP BASE SSH	2
MEM-C4K-FLD128M	Cat 4500 IOS-based Supervisor, Compact Flash, 128MB Option	2
WS-X4448-GB-SFP	Catalyst 4500 Gigabit Ethernet Module, 48-Ports 1000X (SFP)	2
WS-X4548-GB-RJ45V	Catalyst 4500 PoE 802.3af 10/100/1000, 48-Ports (RJ45)	2
GLC-SX-MM	GE SFP, LC connector SX transceiver	8
WS-C3750-48PS-S	Catalyst 3750 48 10/100 PoE + 4 SFP Standard Image	2
CAB-STACK-3M-NH	Cisco StackWise 3M Non-Halogen Lead Free Stacking Cable	1
GLC-SX-MM	GE SFP, LC connector SX transceiver	4
CAB-AC	Power Cord,110V	2
AIR-WLC4402-25-K9	4400 Series WLAN Controller for up to 25 Lightweight APs	1
AIR-PWR-CORD-NA	AIR Line Cord North America	1
GLC-T=	1000BASE-T SFP	1
AIR-LAP1131AG-A-K 9	802.11ag LWAPP AP Integrated Antennas FCC Cnfg	1
S113RK9W-12307JX	Cisco 1130 Series IOS WIRELESS LAN LWAPP RECOVERY	1

Partner

Point of Sale Terminals

IBM 4851 (Small Store)
Windows Embedded for Point of Service Version 1.0 (xp-sp2)
1.2Ghz Via, 512MB SDRAM, 40GB Harddrive
IBM 4810-320 (Medium Store)
Windows XP Pro - Version 2002 Service Pack 1 Build 2600
Wincor-Nixdorf Beetle MII system (Small Store)
Windows XP Pro - Version 2002 Service Pack 2 Build 2600
Intel-M P4 2.22Ghz, 1GB RAM, 74GB harddrive
Wincor-Nixdorf Beetle S II System (Medium Store)
Windows XP Pro - Version 2002 Service Pack 2 Build 2600
Intel Celeron 2.4Ghz, 512MB RAM, 37GB Harddrive
Wincor-Nixdorf Beetle S II System (Large Store)
Windows XP Pro - Version 2002 Service Pack 2 Build 2600
Intel Celeron 2.4Ghz, 512MB RAM, 37GB Harddrive
NCR RealPOS 80c (Large Store)
NCR Advanced Checkout Solution v6.01.04.16 (Large Store)
Verifone MX870, MX850 (wireless)

Wireless Handhelds

Verifone Vx670 (wireless) (Large Store)
Intermec Mobile POS CN3 (wireless) (Large Store)
Intermec CN2BA, L Img, WM03 WWE
Microsoft Pocket PC Version 4.20.0 (Build 14053)
802.11b radio
Intermec CN3B2A, Num AImg, 804, WM5 WWE
Windows Mobile Version 5.0 OS 5.1.342 (Build 15096.3.0.0)
108MB RAM, 40MB Flash, 13MB Storage card
802.11b radio

Software

Wincor-Nixdorf TP.Net V3.01
Wincor Nixdorf JavaPOS version 3



APPENDIX **B**

Data Center/Internet Edge Components and Versions

Component	Brand(s) Used	Version
Firewall	Cisco Integrated Services Router (FWSM Firewall), Cisco ASA	<ul style="list-style-type: none"> FWSM v3.1(3) ASA 7.2.(2)
Network IDS	Cisco Integrated Services Router (integrated IDS/IPS), IDSM2	IOS v12.3(11r)T2, 12.4(1r), IDSM 6.0.(2)E1
Router	Cisco Integrated Services Router (IOS Firewall), Cisco 7206VXR	IOS v12.2(18)SXF10a, v12.3(11r)T2, 12.4(1r), 12.4(11)T3 (VXR)
Wireless AP	Cisco 1131AG, 1242AG	
Wireless Controller	AIR-LAP1131AG-A-K9, AIR-LAP1242AG-A-K9	IOS 12.3(11)JA
Windows Server	Windows Server 2003	SP1, SP2
ECOM Web Server (demo server)	Foundstone Hackme Bank	v2.0
Database	N/A – Not reviewed/Not in scope	
Windows Server Anti-Virus	McAfee VirusScan Enterprise + Anti-spyware Module	8.0.0
Firewall, Router, Switch, IDS/IPS Management	Cisco Security Manager (CS-M), Cisco ASDM, Cisco IDM	CS-M v3.0.1, ASDM v5.2.(2), IDM v6.0.2
Router, Switch management	CiscoWorks (LMS), CiscoWorks (C-NCM)	LMS v2.6, NCM v1.2.1
Desktop/Server Firewall (Host-based firewall)	Cisco Security Agent (CSA)	v5.1.0.69, v5.2.0.210
Central Logging / Correlation /Analysis	CS-MAR	CS-MARS (v4.3.1)
Wireless Management	Wireless Control System (WCS)	v4.1
AAA (TACACS+) authentication	CS-ACS	v4.0(1) Build 27
Web Services (application) firewall	Cisco ACE XML Gateway	V5
Load Balancer	Cisco ACE Load Balancer	V3.0(0)A1(4a)

Two-factor Authentication	RSA SecurID (RSA Authentication Manager)	V6.1(300)
RSA Key Manager Authentication	RSA Access Manager	v6.0
Desktop E-mail Encryption	N/A – not in scope	
File Integrity	Cisco Security Agent (CSA)	v5.1
Cardholder Storage Encryption	<ul style="list-style-type: none"> • NCR-ACS (128-bit 3DES) • RSA Key Manager (192-bit 3DES, 128-bit, 192-bit, 256-bit AES) • RSA File Security Manager (192-bit 3DES, 256-bit AES) • RSA enVision 	<ul style="list-style-type: none"> • NCR-ACS v6.01.04.16 • RSA Key Manager v2.1.1 • RSA File Security Manager v2.1.0.9 • enVision (v3.5.1)



APPENDIX C

Application Protocols

This appendix lists important protocols. For details about these protocols and the Application Flow, refer to the Excel Spreadsheet EDCS-572796.

Table C-1 Application Protocols

HTTP	80/TCP HTTP (HyperText Transfer Protocol—Used for transferring web pages
HTTPS	443/TCP,UDP HTTPS—HTTP Protocol over TLS/SSL (encrypted transmission)
FTP	20/TCP,UDP FTP—Data port Official
FTP	21/TCP,UDP FTP—Control (command) port
SSH	22/TCP,UDP SSH (Secure Shell) —Used for secure logins, file transfers (SCP, SFTP) and port forwarding
Telnet	23/TCP,UDP Telnet Protocol—Unencrypted text communications
DNS	53/TCP,UDP DNS (Domain Name System)
CSA-Client	For Agents to CSAMC, the following are needed: 5401/TCP 5402/TCP 443/TCP 80/TCP
CSA-Server	5401/UDP for CSAMC to Agents
TACACS	49/TCP,UDP TACACS Login Host protocol
RADIUS	1812/UDP radius, RADIUS authentication protocol
RADIUS	1813/UDP radacct, RADIUS accounting protocol
DHCP	67/UDP BOOTP (BootStrap Protocol) server; also used by DHCP (Dynamic Host Configuration Protocol) Official
DHCP	68/UDP BOOTP client; also used by DHCP Official
TFTP	69/UDP TFTP (Trivial File Transfer Protocol)
NTP	123/UDP NTP (Network Time Protocol) - used for time synchronization Official
NetBIOS	137/TCP,UDP NetBIOS NetBIOS Name Service Official
NetBIOS	138/TCP,UDP NetBIOS NetBIOS Datagram Service Official
NetBIOS	139/TCP,UDP NetBIOS NetBIOS Session Service

Table C-1 Application Protocols (continued)

RPC	135/TCP, Windows RPC
MSDS	445/TCP Microsoft-DS (Active Directory, Windows shares, Sasser worm, Agobot, Zobotworm)
MSDS	445/UDP Microsoft-DS SMB file sharing
RDP	3389/tcp Microsoft Terminal Server (RDP) officially registered as Windows Based Terminal (WBT)
SNMP	161/TCP,UDP SNMP (Simple Network Management Protocol) Official
SNMP	162/TCP,UDP SNMPTRAP
HSRP	1985/UDP Cisco HSRP
SQL	1433/tcp, udp Microsoft SQL database system Official
SQL	1434/tcp, udp Microsoft SQL Monitor
SYSLOG	514/UDP syslog protocol - used for system logging
AV	82/tcp McAfee Antivirus Update
ICMP	ALL ICMP
NetFlow	2055/TCP Cisco NetFlow
LDAP	636/TCP,UDP LDAP over SSL (encrypted transmission)
LDAP	389/TCP,UDP LDAP (Lightweight Directory Access Protocol)
KERBEROS	464/TCP,UDP Kerberos Change/Set password
KERBEROS	543/TCP klogin, Kerberos login
KERBEROS	544/TCP kshell, Kerberos Remote shell
KERBEROS	88/TCP Kerberos—Authenticating agent
KERBEROS	88/UDP Kerberos—Authenticating agent
GC	TCP Port 3268—Global Catalog Server Local Security Authority
GC	TCP Port 3269—Global Catalog Server Local Security Authority
ASP	TCP Port 42424—ASP.Net Session State ASP.NET State Service
LWAPP-S	UDP/12223 IS used for controller source UDP port to AP "LWAPP control"
LWAPP	UDP/12222 used for controller source UDP port to AP "LWAPP data"
RSA File Security Manager	<p>TCP/19978 and TCP/5766</p> <ul style="list-style-type: none"> • Audit Port: <ul style="list-style-type: none"> – Default listening port is TCP/19978 – The audit service is listening for requests initiated by the adapter manager (console) • Configuration Port: <ul style="list-style-type: none"> – Default listening port is TCP/5766 – The configuration service is listening for requests from the adapter manager (console)
RSA Key Manager	443/TCP,UDP HTTPS—HTTP Protocol over TLS/SSL (encrypted transmission)



APPENDIX **D**

Detailed Implementation and Configuration Steps

This appendix includes the implementation and configuration steps for the following:

- [Wireless Configuration, page D-1](#)
- [Point-of-Sale Application Systems, page D-7](#)
- [Cisco Secure Access Control Server, page D-8](#)
- [Cisco Security Manager, page D-18](#)
- [CSA Manager, page D-23](#)
- [Cisco Security Agent \(CSA\) Custom Policy for RSA Products, page D-30](#)
- [Cisco Security Agent \(CSA\) Custom Policy for NCR, page D-34](#)
- [RSA Key Manager, page D-39](#)
- [RSA File Security Manager, page D-44](#)
- [PCI Section 6.5, page D-49](#)

Wireless Configuration

Small Store (HREAP + Controller Architecture)

In this configuration, the AP is remotely located from the WLAN controller (WLC). In this architecture, the AP communicates with the WLC to obtain its configuration and via the UDP-based Lightweight Access Point Protocol (LWAPP) for control data, but bridges its traffic locally. This is referred to as “hybrid REAP” (H-REAP) operation. Initial configuration requirements are as follows:

- The small store employs an AP1130 in H-REAP mode at the store and WLAN controller located in the data center or large store
- AP is configured for static IP address and controller address
- AP is configured in controller for H-REAP operation
- WLAN is configured for local switching of VLANs
- [Appendix E, “Device Configurations,”](#) details the specific configurations of the small store AP.

Medium Store (Controller-Based)

In this configuration, the AP is connected on a network local to the ISR and employs the controller for both configuration/control data and bridging of traffic. Thus, all AP/wireless data is sourced from the WLC. This is referred to as “local” AP operation. Initial configuration requirements are as follows:

- The medium store employs an ISR with a WLAN Controller Network Module (also known as WLCM/ NM-AIR-WLC6) and “local mode” AP1130.
- ISR must be configured for multiple “wlan-controller” interfaces to support WLAN-client-supporting VLANs.
- ISR must use an L3 interface for the connection of the WLC management interface. Thus, the WLC in this medium store configuration employs a unique WLAN management VLAN.
- According to WLAN best practices deployment, the AP-to-WLC communication employs a VLAN separate from any user data. Because of the L3 connectivity of the ISR WLCM, two VLANs are used: one for WLC communication, and one for AP communication. The ISR accomplishes routing between these two subnets.
- [Appendix E, “Device Configurations,”](#) details the specific interfaces that should be created on the ISR.

Large Store (Controller-Based)

In this configuration, the WLC is a standalone appliance (WLC-4402) with APs connected on a common subnet with the WLC “management” interface. The management interface is employed for both configuration and maintenance of the WLC as well as communication with the APs for configuration and wireless payload. Note that the wireless user traffic is encapsulated in the LWAPP protocol as it flows from AP to controller, and is bridged to its respective VLAN only upon termination/decapsulation at the WLC. Initial configuration requirements are as follows:

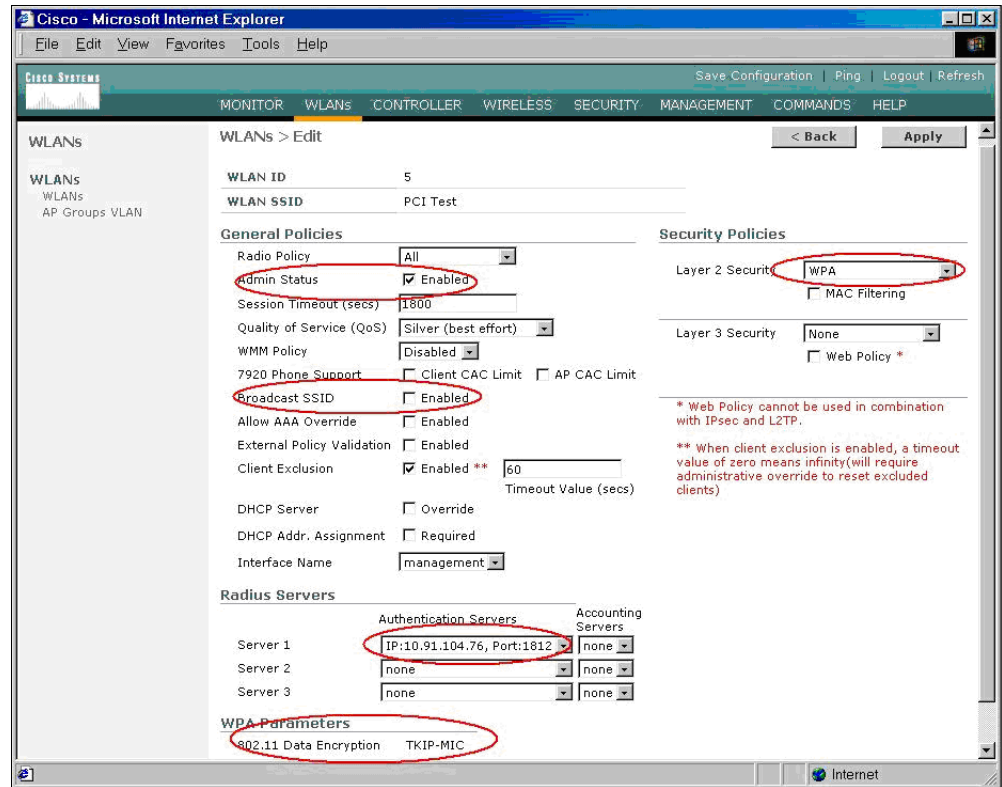
- The large store employs a standalone 4400 series controller and “local mode” APs.
- Controller and switchport are configured for wireless VLANs. Note that VLAN 18 is used for “management” or LWAPP control traffic; that is, all traffic between AP and controller, including keying, configuration, and wireless payload, encapsulated in LWAPP (UDP) tunnel.
- In the 4400 WLC, it is possible to connect the WLC and APs on the same subnet.
- [Appendix E, “Device Configurations,”](#) details the configuration for the WLC4402.

Section 2.1 of PCI Requirements

- Verify that the Cisco Controller is, by default, configured for administrative restriction and AAA authentication for administrative users.
- Verify that no default SSID is enabled on the WLC.
- Disable/remove default SNMP strings of “public/private”.
- Create new community strings:
 - “config snmp community create <string>”
 - “config snmp community mode enable <string>”
 - “config snmp community accessmode <ro/rw> <string>”

- Verify that default community strings are no longer accessible.
- Configure administrative user either via initial controller setup script or via CLI:
“config mgmtuser add <username> <password> read-write/read-only”. If using Wireless Control System (WCS), change default username and password via GUI (PCI Section 2.1.1)
- Configure wireless system for WPA authentication. Note that SSID Broadcast is enabled by default, but may be disabled. [Figure D-1](#) shows the configuration of the WLAN on the Cisco Controller for WPA security using RADIUS client authentication.

Figure D-1 WLAN Configuration

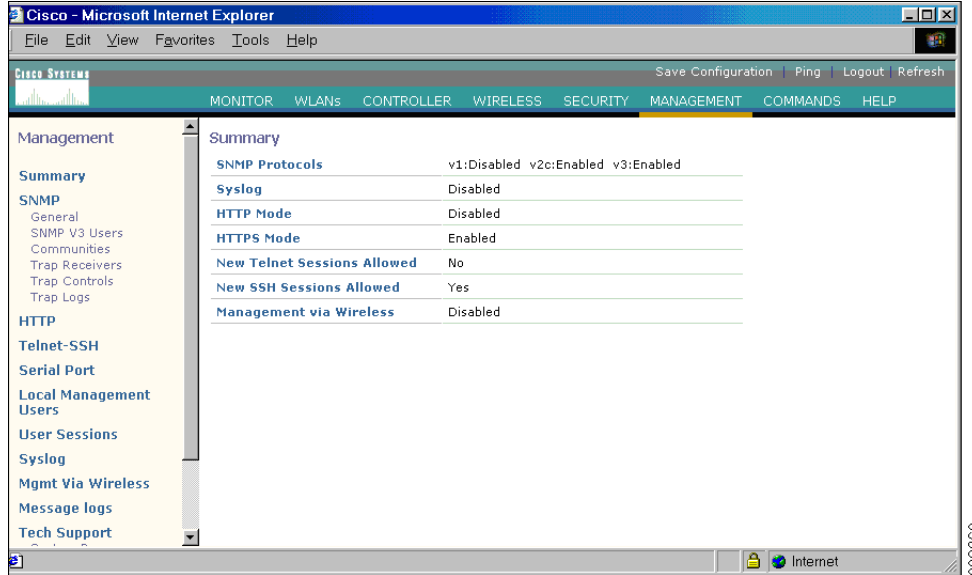


- Verify that WLAN security configuration (SSID broadcast disabled, WEP/ WPA in use) is enabled. (PCI Section 2.1.1)

PCI Section 2.3

- Verify that the controller is enabled only for secure management protocols; that is, HTTPS (SSL) only, Telnet disabled, SNMPv1 disabled, SSH permitted. [Figure D-2](#) shows an output from controller “Management> Summary” that shows the controller default settings, which include HTTP disabled, Telnet disabled, and HTTPS (SSL)/ SSH enabled.

Figure D-2 Management > Summary Controller Output



- Verify that administrative access is denied to users accessing over unpermitted interfaces/addresses and verify that only encrypted protocols are permitted. (PCI Section 2.3)

PCI Section 4.1.1

- Configure wireless equipment for WPA authentication and encryption. (See [Figure D-3](#).)

Figure D-3 WPA Authentication and Encryption Configuration

The screenshot shows the Cisco WLAN configuration page for WLAN ID 5, named 'PCI Test'. The configuration is divided into several sections:

- General Policies:** Radio Policy is set to 'All'. Admin Status is checked and set to 'Enabled'. Session Timeout is 1800 seconds. Quality of Service (QoS) is 'Silver (best effort)'. WMM Policy is 'Disabled'. 7920 Phone Support is unchecked. Broadcast SSID is checked and set to 'Enabled'. Allow AAA Override, External Policy Validation, and Client Exclusion are all checked. Client Exclusion Timeout Value is 60 seconds. DHCP Server is unchecked. DHCP Addr. Assignment is unchecked. Interface Name is 'management'.
- Security Policies:** Layer 2 Security is set to 'WPA'. Layer 3 Security is set to 'None'. Web Policy is unchecked.
- Radius Servers:** Server 1 is configured with IP: 10.91.104.76, Port: 1812. Servers 2 and 3 are set to 'none'.
- WPA Parameters:** 802.11 Data Encryption is set to 'TKIP-MIC'.

Red circles highlight the Admin Status, Broadcast SSID, Layer 2 Security, and WPA Parameters sections.

**Note**

WLAN security data (that is, Pairwise Master Key [PMK] used in WPA or WEP key used with 802.1X dynamic WEP) is stored/cached on the WLAN controller and is transferred to the AP only upon client association. Control and configuration traffic between controller and AP is authenticated and encrypted. AES encryption is used on this link.

PCI Section 9.1.3

Note that console access to wireless APs used with the Cisco Controller does not provide access to any configuration or system information. Note that user access to the console port on the controller may be authenticated via user database or RADIUS.

- Verify that non-authorized access to network components is not permitted.

PCI Section 10.4

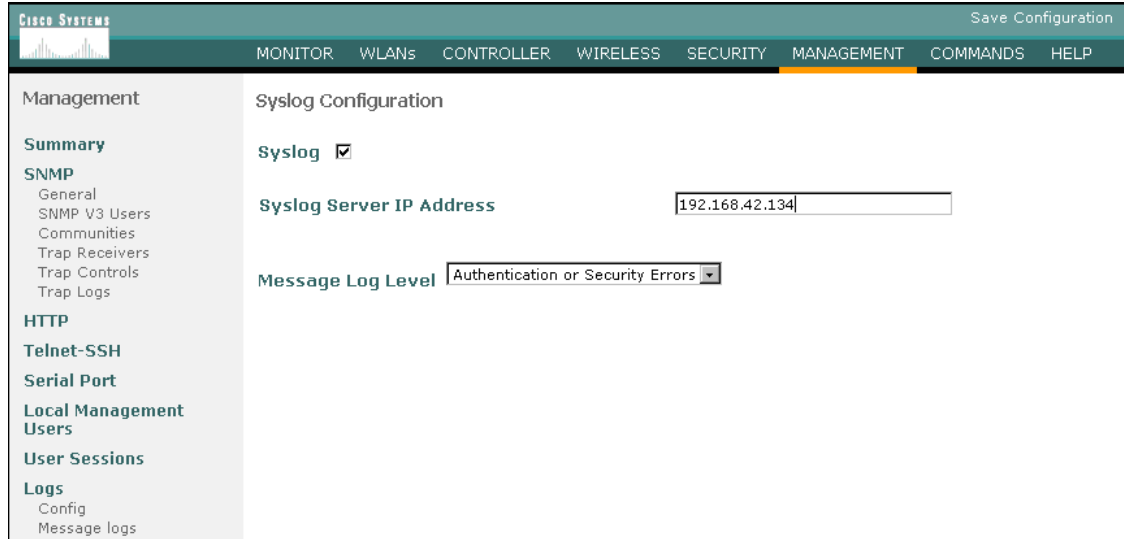
- Enable NTP on the controller to synchronize system clock and messages.

PCI Section 10.5.4

- Enable Syslog on the WLAN Controller. (see [Figure D-4.](#))

- Configure the Syslog server address.
“config syslog <ip address of syslog destination>”

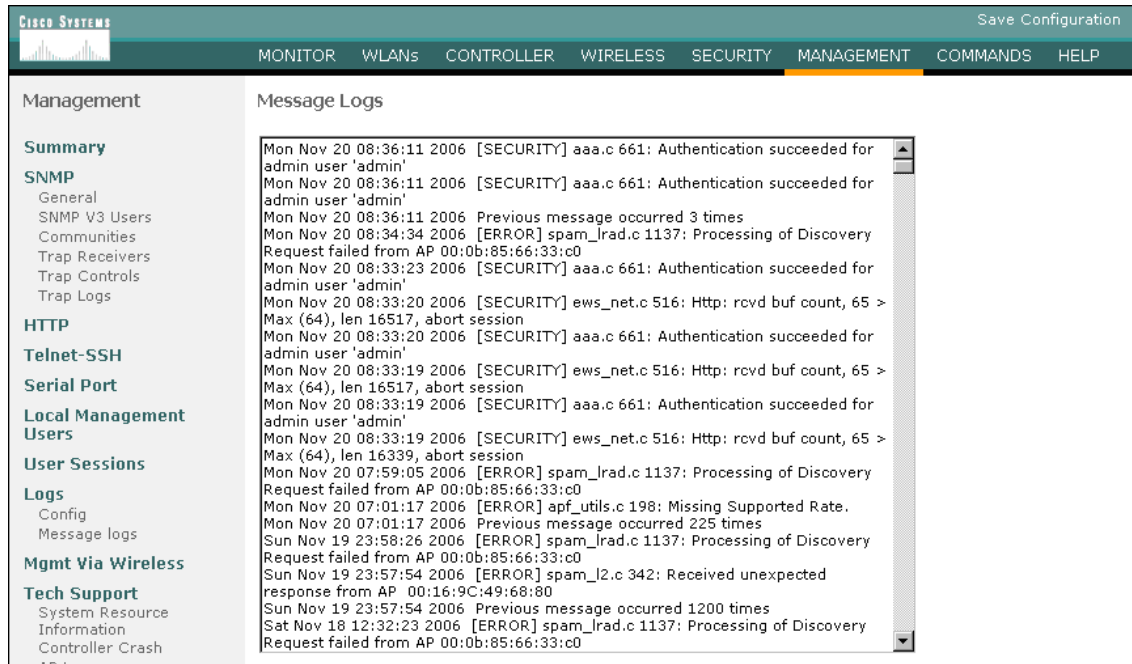
Figure D-4 Enabling Syslog



220369

- Verify syslog logging of information from the controller. (See [Figure D-5](#).)

Figure D-5 Verifying Syslog Logging



220370

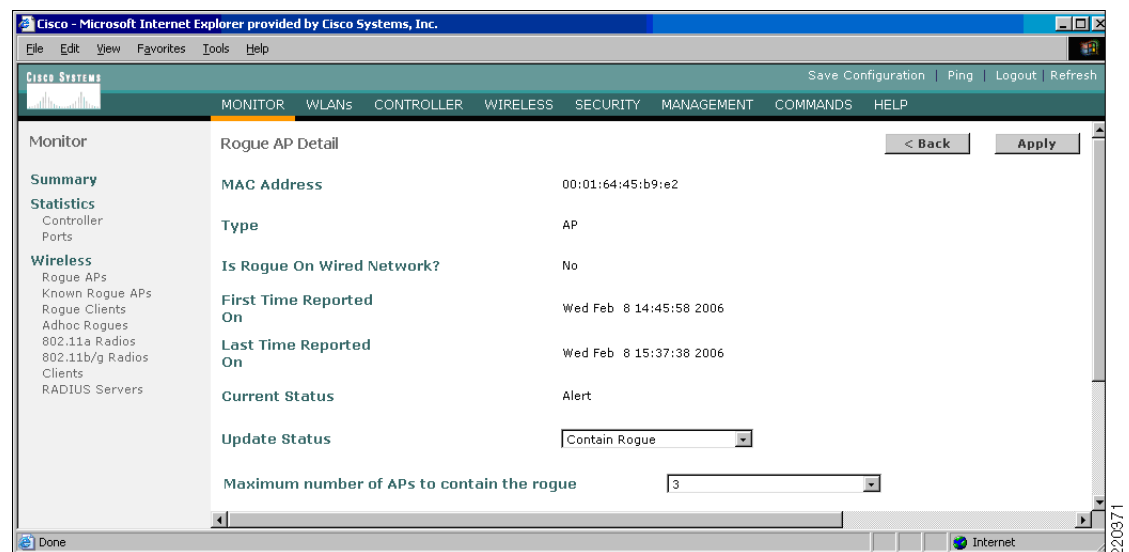
PCI Section 11

Note that WLC is enabled for IDS/rogue AP detection by default. When WLC is performing rogue AP/wireless IDS operation, it periodically scans all active WLAN frequencies to detect any unauthorized or malicious WLAN traffic (Section 11.1).

Verify via the Cisco Controller GUI or via WCS that rogue WLAN devices on the network are detected by the WLC. (See [Figure D-6](#).)

When a rogue AP is detected, the Cisco Controller may invoke a “containment” event, as directed by administrative control. A WLAN containment event is an active mechanism that dis-associates all WLAN clients from a WLAN rogue device.

Figure D-6 Detecting a Rogue AP



Verify that the rogue AP may be detected and contained using the Cisco Controller or WCS user interface. (Section 11.4).

Point-of-Sale Application Systems

Wincor-Nixdorf TP.net and PCI

The Wincor-Nixdorf application was not audited by the QSA. The Wincor product does not directly process credit card payments and therefore is not directly affected by PCI. Following is a summarization of their product in regards to PCI guidelines and its interface to payment system applications. Wincor uses an open standards-based interface called the Open Payment Initiative (O.P.I).

- The primary account number (PAN) and the expiration date are optional elements of the O.P.I. interface specification. These elements are included in the response of a card payment request. To prevent the misuse of these elements, the card payment system should not provide these elements. If the business requirements of the retailer need these elements, the sale system is responsible to fulfill the PCI DSS requirements. The service code and the cardholder name are not elements of the O.P.I. interface specification.

- For the O.P.I. interface, the track content is an optional element in the response of a card payment request. PCI DSS-compliant card payment systems should not provide this element. In TP.net, there is no storage of the full content of a track from the magnetic stripe.
- The card validation code and the PIN verification value are not elements of the O.P.I. interface specification; therefore, no storage is possible.
- Within the O.P.I. interface, the displaying and printing of the account number is the responsibility of the card payment system. For this reason, PCI DSS-compliant card payment systems should mask this element, within the requests for the display and print devices. The TP.net system is not responsible for the contents of the provided print information or display information of the card payment system unless the TP.net sales system formats the print layout by itself, using the elements from the response of the card payment request. It must be ensured that the sale system is using the masked account number for the customer receipt.
- The “unmasked” account number is an optional element of the O.P.I. interface specification. When this element is provided by the card payment system, the TP.net sale system should render this element, when storing it on the system. TP.net V3.x has controls that can be switched on or off to securely render-sensitive card holder data unreadable anywhere it is stored.
- TP.net is developed by using standard system development processes. The development environment is based on the actual Microsoft .NET framework containing all current software patches. Additionally, TP.net has an extensive user management to ensure that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Cisco Secure Access Control Server

CS-ACS was installed on a Windows MCS 7825 server running Windows 2003 server R2. A typical default installation was performed of the CS-ACS product. No individual user accounts were added. Several groups were defined based on typical enterprise roles such as the following:

- Network engineering
- Security engineering
- Wireless engineering
- Wireless handheld users
- Network management
- Network administrator approver
- Network administrator help desk

The system interface was then configured for only HTTPS/SSL-encrypted communications by installing an appropriate certificate. (See [Figure D-7](#).)

Figure D-7 Cisco Secure ACS—Certificate

The screenshot shows the Cisco Secure ACS web interface in Microsoft Internet Explorer. The main content area is titled "System Configuration" and "Install ACS Certificate". It displays the following "Installed Certificate Information":

Issued to:	TACACS
Issued by:	ACTIVE DIRECTORY
Valid from:	November 15 2006 at 16:13:56
Valid to:	November 14 2008 at 16:13:56
Validity:	OK

Below the table are buttons for "Install New Certificate", "Cancel", and "Back to Help". The right-hand "Help" section contains the following text:

Read certificate from file
[Read certificate from file](#)
[Certificate file](#)
[Use certificate from storage](#)
[Certificate CN](#)
[Private key file](#)
[Private key password](#)

You can use this page to perform certificate enrollment to support EAP-TLS and PEAP authentication and HTTPS for access to the ACS web interface. ACS supports the X.509 v3 digital certificate standard. Certificate and CA files must be either in Base64-encoded X.509 format or DER-encoded binary X.509 format.

Note: Whenever you install a new certificate, you must configure the [Certificate Trust List](#). Replacing an existing certificate configuration with a new certificate configuration automatically erases the previous configuration of the [Certificate Trust List](#).

Read certificate from file
 To install a certificate from a file, select this option.
[Back to Top](#)

Certificate file
 If the "Read certificate from file" option is selected, you must type the full path and file name of the certificate in the "Certificate file" box.
[Back to Top](#)

Use certificate from storage
 To have ACS enroll using a certificate from Windows certificate storage on the local machine, select this option.
[Back to Top](#)

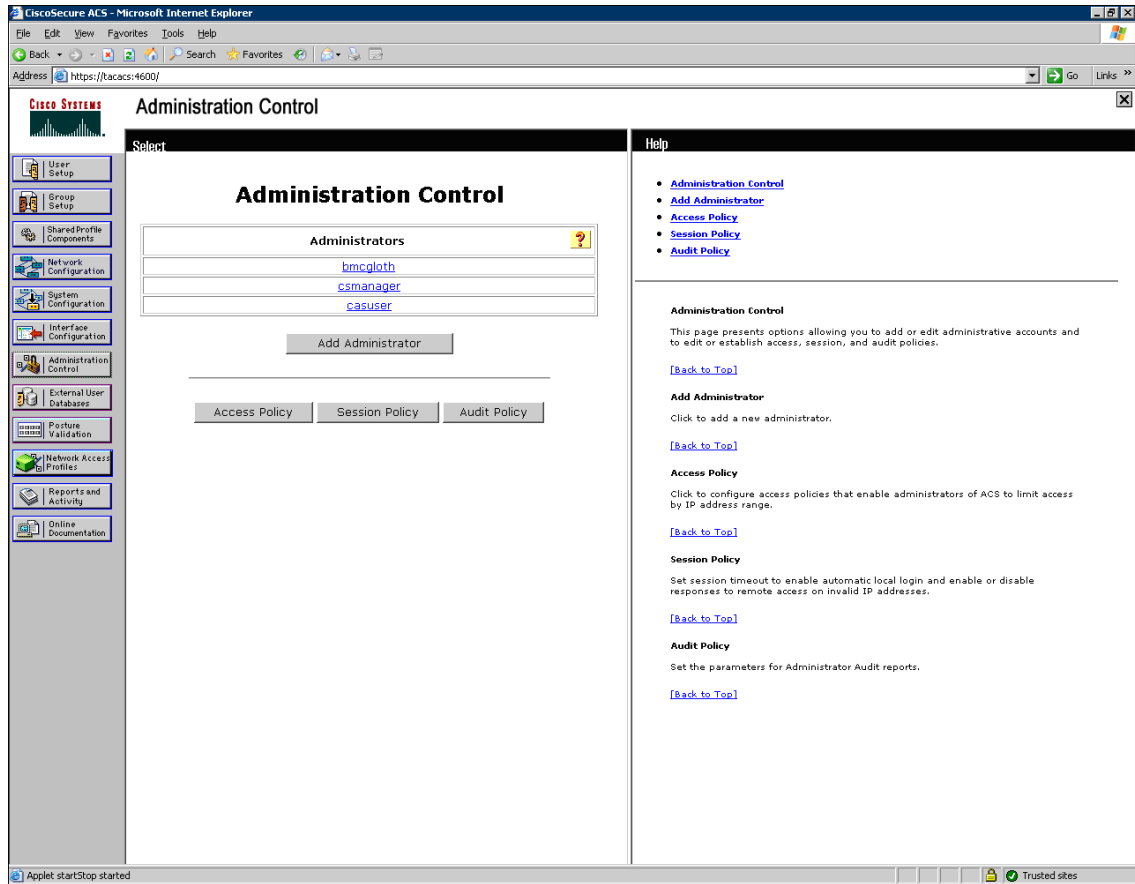
Certificate CN
 If the "Use certificate from storage" option is selected, you must type the common name (CN) of the certificate in the Certificate CN box. For example, if the CN in the certificate is CN=ACS11, then type ACS11 in the Certificate CN box.
[Back to Top](#)

Private key file
 Type the full path and file name of the private key file in the "Private key file" box.
[Back to Top](#)

Private key password

Additional local administrator accounts were added for specific individuals and systems, and the generic Admin account was removed. (See [Figure D-8](#).)

Figure D-8 Administration Control Configuration



CS-ACS does not meet PCI requirements for user administration password complexity and history; it requires only a four-character password, with no complexity, and no history maintained.

As a compensating control, restrict access to the administration interface and leverage an additional authentication method such as Windows login. In the Cisco lab, the configuration of the CS-ACS was allowed only from the server desktop, and remote web access was only allowed from the two management platforms that required it (CiscoWorks LMS and CS Manager).

Connectivity was further restricted to allow only HTTPS connections. (See [Figure D-9](#).)

Figure D-9 Access Policy Setup

Access Policy Setup

IP Address Filtering

Allow all IP addresses to connect
 Allow only listed IP addresses to connect
 Reject connections from listed IP addresses

IP Address Ranges

	Start IP Address	End IP Address
1	192.168.42.131	192.168.42.131
2	192.168.42.133	192.168.42.134
3		
4		
5		
6		
7		
8		
9		
10		

HTTP Configuration

HTTP Port Allocation

Allow any TCP ports to be used for Administration HTTP Access
 Restrict Administration Sessions to the following port range From Port 1024 to Port 65535

Secure Socket Layer Setup

Use HTTPS Transport for Administration Access

Submit Cancel

Help

- [IP Address Filtering](#)
- [IP Address Ranges](#)
- [HTTP Configuration](#)

IP Address Filtering

Click one of the following options:

- Allow all IP addresses to connect.** (default) No filtering on any IP address is performed when an administrator is accessing ACS remotely.
- Allow only listed IP addresses to connect.** Click to allow remote administration from only those workstations whose IP addresses fall within the range specified in IP Address Ranges. Workstations whose IP addresses are not within the specified range will not be able to access ACS remotely.
- Reject connections from listed IP addresses.** Click to filter out remote administration from the IP addresses specified in IP Address Ranges. Remote administration from workstations whose IP addresses do not fall within the specified range will be permitted.

Notes: IP filtering operates upon the IP address received in the HTTP request from a remote administrator's web browser. If the browser is configured to use an HTTP proxy server or if the browser is run on a workstation behind a network device performing network address translation, IP filtering applies only to the IP address of the HTTP proxy server or the NAT device, respectively.

[Back to Top](#)

IP Address Ranges

Specify the IP address range in Class C format from which to permit or deny access.

[Back to Top](#)

HTTP Configuration

Under HTTP Port Allocation, you can specify whether ACS can use any TCP port to grant administrative access to the web interface or ACS uses only a configured range of TCP ports to grant administrative access. Choose one of the following two options:

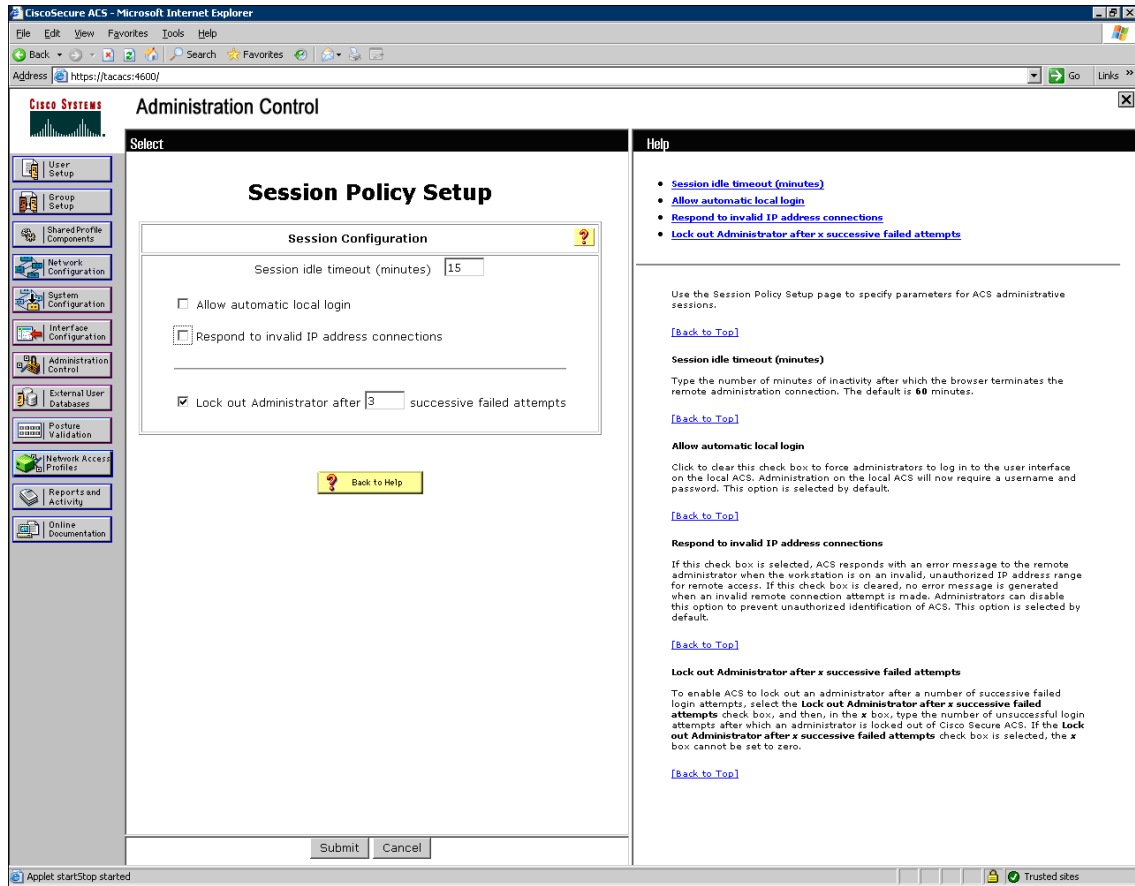
- Allow any TCP ports to be used for Administration HTTP Access.** To allow TCP ports to be used for remote administrative sessions, click this option.
- Restrict Administration Sessions to the following port range From Port X to Port Y.** To restrict TCP ports used for remote administrative sessions to a specific range, click this option and complete the following fields:
 X: Type the port number for the bottom end of the TCP port range.
 Y: Type the port number for the top end of the TCP port range.

Under Secure Socket Layer Setup, you can specify whether ACS uses secure socket layer and HTTPS to encrypt communication between ACS and a web browser used by an administrator. To enable SSL-encrypted administrative access, select the Use

Sessions were restricted to 15 minutes, and admin accounts disabled after three successive failed attempts. The automatic local login was removed. (See [Figure D-10](#).)

220449

Figure D-10 Session Policy Setup



PEAP authentication was configured for support of 802.1x when authenticating wireless or LAN users. (See [Figure D-11](#).)

Figure D-11 Global Authentication Setup

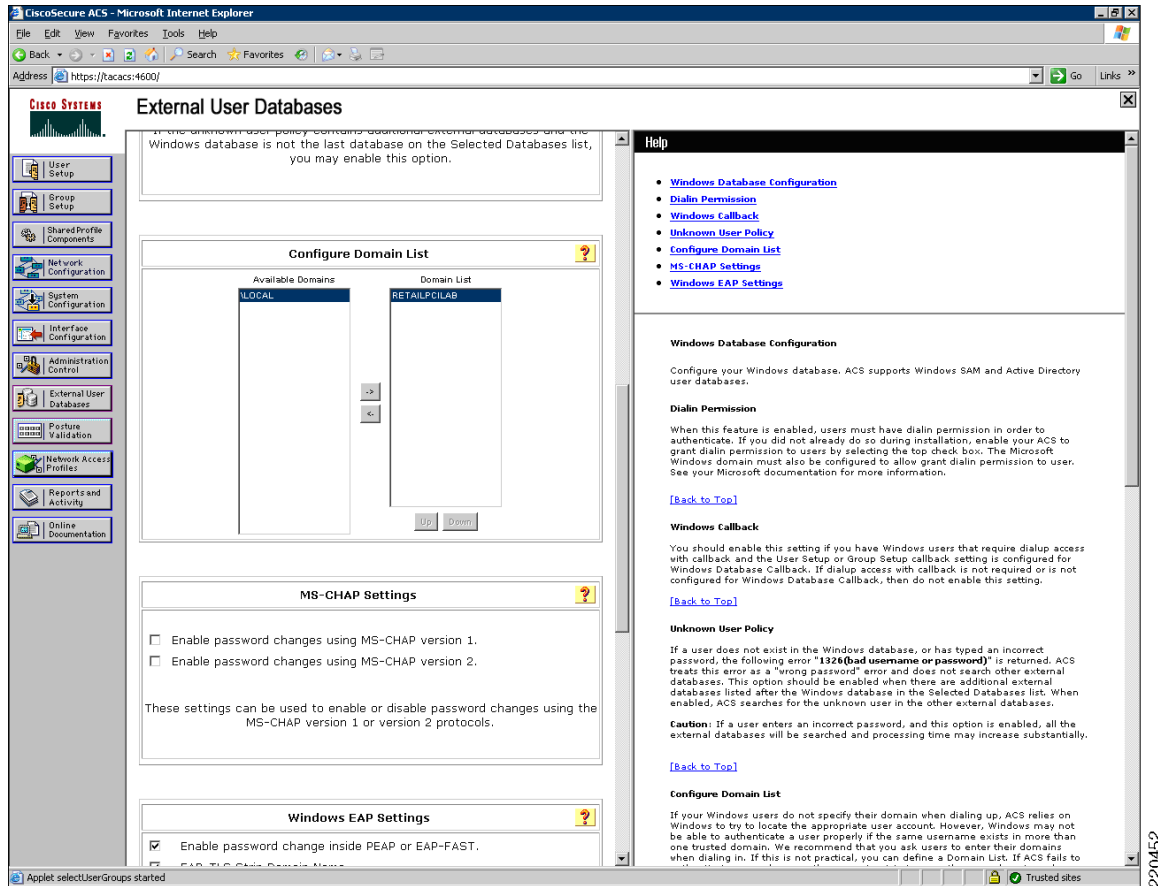
The screenshot shows the Cisco Secure Access Control Server (ACS) configuration interface for Global Authentication Setup. The browser window displays the URL <https://nacacs:4600/>. The configuration page is titled "System Configuration Global Authentication Setup" and is organized into several sections:

- EAP Configuration:**
 - Allow EAP-MSCHAPv2
 - Allow EAP-GTC
 - Allow Posture Validation
 - Cisco client initial message:
 - PEAP session timeout (minutes):
 - Enable Fast Reconnect:
- EAP-FAST Configuration:**
 - [EAP-FAST Configuration](#)
- EAP-TLS Configuration:**
 - Allow EAP-TLS
 - Select one or more of the following options:
 - Certificate SAN comparison
 - Certificate CN comparison
 - Certificate Binary comparison
 - EAP-TLS session timeout (minutes):
- LEAP Configuration:**
 - Allow LEAP (For Aironet only)
- EAP-MD5 Configuration:**
 - Allow EAP-MD5
- AP EAP request timeout (seconds):**
- MS-CHAP Configuration:**
 - Allow MS-CHAP Version 1 Authentication
 - Allow MS-CHAP Version 2 Authentication

At the bottom of the configuration area are buttons for "Submit", "Submit + Restart", and "Cancel". A help window is open on the right side of the browser, displaying the "Global Authentication Setup" help page. The help page includes a list of links for various authentication protocols and detailed descriptions for EAP, PEAP, and MS-CHAPv2.

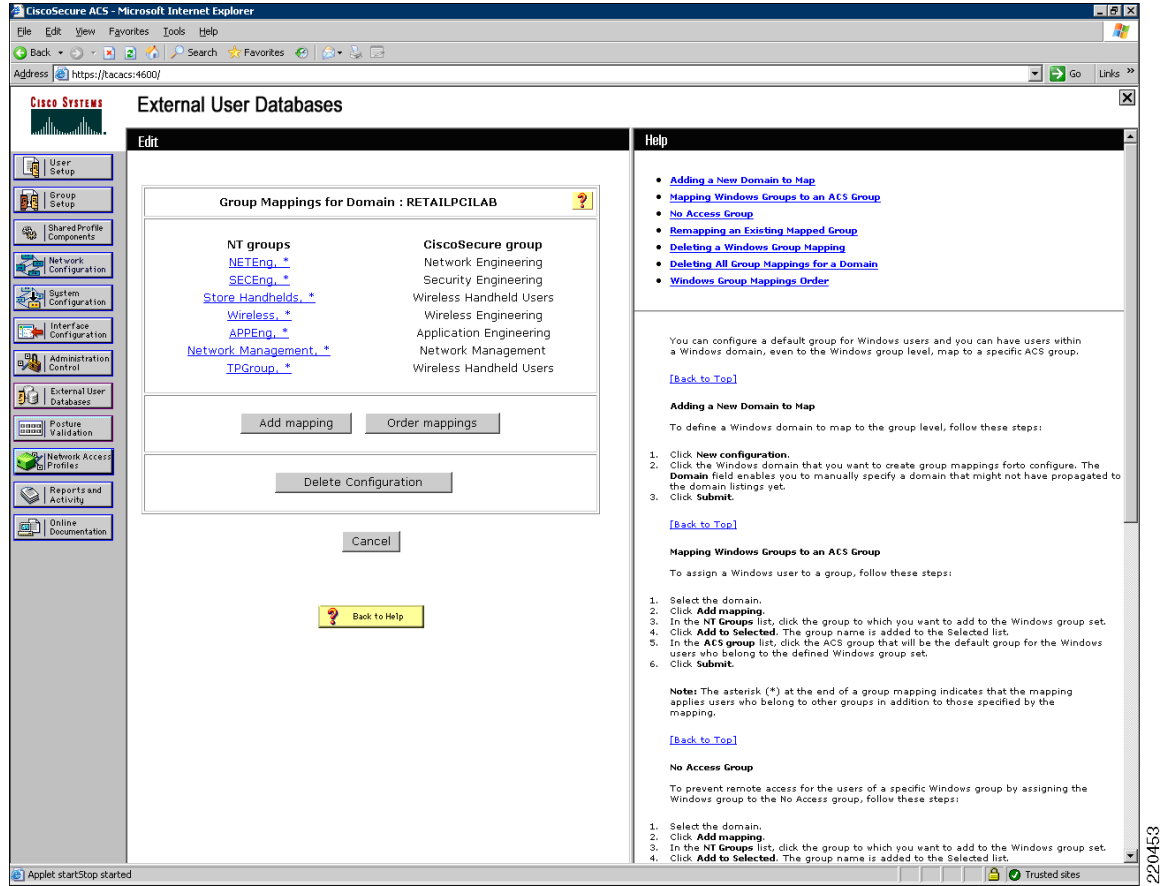
Domains were configured against which to authenticate. (See [Figure D-12](#).)

Figure D-12 Configure Domain List



The local CS-ACS groups were then mapped to similar Microsoft Active Directory user groups. (See [Figure D-13](#).)

Figure D-13 Group Mappings for Domain



Local user mapping is performed dynamically between groups. No local user accounts exist directly in CS-ACS because of the limited password strength enforcement capabilities with regard to meeting PCI requirements. (See Table D-1.)

Table D-1 Local User Mapping

User	Status	Group	Network Access Profile
bmcgloth	Enabled	Dynamic mapping [Currently: Application Engineering (1 users)].	(Default)
csm-user	Enabled	Dynamic mapping [Currently: Security Engineering (1 users)].	(Default)

Logging was set to rotate authentication and system logs daily.

The best practice is to set the log file management to generate a new file daily, and have CS-ACS manage the directory to delete files older than 366 days or per your own security policy. This version of CS-ACS has a bug in that the manage directory feature is stuck on the seven-day default. To overcome this limitation, until an update is available, the manage directory was disabled for all logging. Removal of old logs is performed manually and an audit maintained via the CSA events for the log directory on CS-ACS.

As an additional measure, all log files are also copied daily to the Log backup server via a scheduled batch file. (See [Figure D-14](#).)

Figure D-14 Log File Management

The screenshot shows the Cisco Secure Access Control Server (ACS) System Configuration page in a Microsoft Internet Explorer browser. The page is titled "System Configuration" and is divided into two main sections: "Select Columns To Log" and "Log File Management".

Select Columns To Log: This section allows users to choose which attributes to log. It features two columns: "Attributes" and "Logged Attributes". The "Attributes" column lists various fields such as Proxy IP Address, ExtDB Info, Source-NAS, Device Command S, Global Message Id, Logged Remotely, Outbound Class, Shared RAC, Downloadable ACL, System-Profile-Take, Application-Posture, Real Name, Description, User Field 3, User Field 4, User Field 5, and Cisco-av-pair. The "Logged Attributes" column lists fields like Message Type, User Name, Group Name, Caller ID, Network Access Profi, Authen-Failure-Code, Authen-Failure-Code, Author-Data, NAS-Port, NAS-IP-Address, Filter Information, PEAP/EAP-FAST-Cl, EAP Type, EAP Type Name, Reason, and Access Device. Arrows between the columns allow for moving attributes from one list to the other.

Log File Management: This section provides options for generating and managing log files. It includes a "Generate New File" section with radio buttons for "Every day", "Every week", "Every month", and "When size is greater than 2048 KB". Below this is a "Directory" section with a text input field containing "C:\Program Files\CiscoSecure ACS v4.0\Log". There is a checkbox for "Manage Directory" and two radio button options: "Keep only the last 7 files" and "Delete files older than 7 days". A "Back to Help" button is located at the bottom of this section.

On the right side of the page, there is a help text area with the following content:

This option enables you to change the layout of the log files that you can view under Reports and Activities. Select the **Log to reportname Report** check box, and then configure the following parameters.

[Back to Top]

Select Columns to Log

In the **Attributes** column, click the attribute to be logged and click -> to move it into the **Logged Attributes** column. Click **Up** or **Down** to move the column for this attribute to the desired position in the log. Repeat until all the desired attributes are in the desired position in the Logged Attributes column.

[Back to Top]

Log File Management

The options in this section control the parameters for the Service log file and directory.

[Back to Top]

Generate new file

Click one of the following options to configure when the new log file is generated.

Note: To make sure your system is set to your local time, click **Start: Settings: Control Panel: Regional Settings**.

- **Every Day.** Click this option to have ACS generate a new log file at 12:01 am local time every day.
- **Every Week.** Click this option to have ACS generate a new log file at 12:01 am local time every Sunday.
- **Every Month.** Click this option to have ACS generate a new log file at 12:01 am on the first day of every month.
- **When Size is Greater than X KB.** Click this option and type the number of kilobytes after which to have ACS generate the new log file. The default is 2048 KB.

[Back to Top]

Directory

Type the name of the directory in which to place the log files.

[Back to Top]

Manage Directory

To configure parameters for the directory for the log files, click **Manage Directory** and one of the following options:

- **Keep only the last X files.** Click this option and type the maximum number of log files to keep in the log directory. The default is 7 files.
- **Delete files older than X days.** Click this option and type the maximum number of days to keep the log files in the log directory. The default is 7 days.

[Back to Top]

The browser's address bar shows "https://racacs:4600/". The status bar at the bottom indicates "Applet: ColumnSelection started".

Each network device that is authenticating against the CS-ACS was defined individually, but all were given the same key. Different keys can be used for different groups of devices, and Cisco recommends rotating the keys quarterly. (See [Figure D-15](#).)

Figure D-15 AAA Client Authentication

The screenshot shows the Cisco Secure Access Control Server (ACS) Network Configuration page. The main content is a table titled "(Not Assigned) AAA Clients". The table has three columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. The clients are listed in a table with various hostnames and IP addresses, and their authentication methods are specified as TACACS+ (Cisco IOS) or RADIUS (Cisco Airespace).

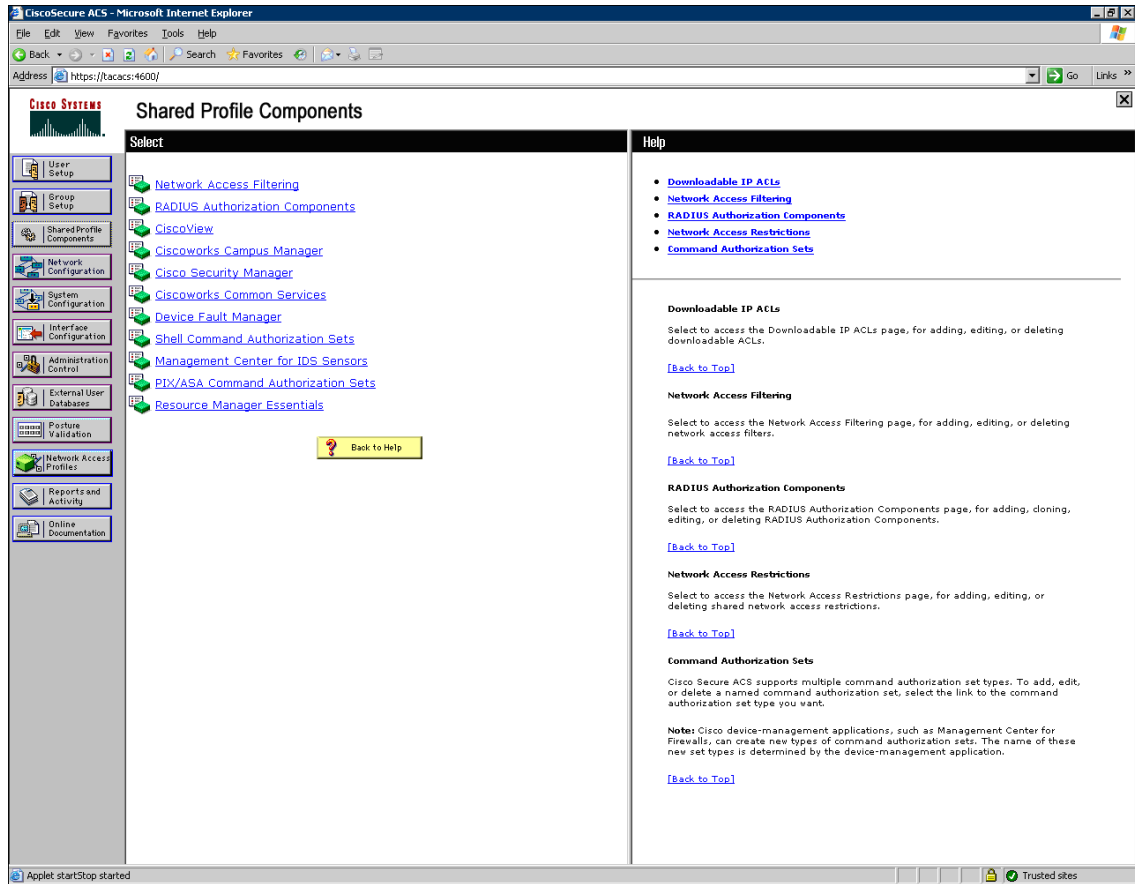
AAA Client Hostname	AAA Client IP Address	Authenticate Using
AL-DC-1	192.168.42.111	TACACS+ (Cisco IOS)
AL-LRG-1	10.10.51.60	TACACS+ (Cisco IOS)
AL-MED-1	10.10.35.10	TACACS+ (Cisco IOS)
AP-1	10.10.19.10	TACACS+ (Cisco IOS)
AP-2	10.10.35.20	TACACS+ (Cisco IOS)
AP-4	10.10.51.40	TACACS+ (Cisco IOS)
AW-DC-1	192.168.42.112	RADIUS (Cisco Airespace)
AW-LRG-1	10.10.55.5	RADIUS (Cisco Airespace)
AW-MED-1	10.10.46.34	RADIUS (Cisco Airespace)
CE-DC-1	192.168.42.110	TACACS+ (Cisco IOS)
CE-LRG-1	10.10.49.99	TACACS+ (Cisco IOS)
CISWORKS	192.168.42.134	TACACS+ (Cisco IOS)
CSAMANAGER	192.168.42.132	TACACS+ (Cisco IOS)
CSMANAGER	192.168.42.133	TACACS+ (Cisco IOS)
MARS-DC-1	192.168.42.121	TACACS+ (Cisco IOS)
RCORE-1	192.168.1.10	TACACS+ (Cisco IOS)
RCORE-2	192.168.1.20	TACACS+ (Cisco IOS)
RLRG-1	10.10.62.1	TACACS+ (Cisco IOS)
RLRG-2	10.10.62.2	TACACS+ (Cisco IOS)
RMED-1	10.10.46.1	TACACS+ (Cisco IOS)
RMED-2	10.10.46.2	TACACS+ (Cisco IOS)
RSMALL-1	10.10.30.1	TACACS+ (Cisco IOS)
RWAN-1	192.168.1.1	TACACS+ (Cisco IOS)
RWAN-2	192.168.1.2	TACACS+ (Cisco IOS)

The page also includes a navigation sidebar on the left with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. A help panel on the right provides instructions on how to manage Network Device Groups (NDGs), including adding, editing, and deleting entries.

With the installation of CiscoWorks components and Cisco Security Manager, several shared profile components were added that allow greater refinement in role-based access to these products when authenticating to CS-ACS. (See Figure D-16.)

220455

Figure D-16 Shared Profile Components



220456

Cisco Security Manager

This section describes the firewall rules in place for the Cisco Retail Store PCI Certification Lab. This section also contains firewall use methodology as well as explanation for the rules used within the firewall for ease of explanation during audit.

Firewall Use Methodology

The firewalls used within the PCI Retail design are based on Cisco IOS running on specialized Cisco router hardware at the branch, FWSM on the Internet Edge, and the Adaptive Security Appliance at the datacenter WAN aggregation layer. Throughout this document, references to firewalls or routers are synonymous because the devices provide both functions. The firewall policy can be applied to particular interfaces in an inbound and/or outbound methodology. The management of the firewall configuration is achieved by either Cisco Security Manager (CS-M), a centralized, GUI-based management product, or by the GUI-based local device management software such as the Adaptive Security Device Manager (ASDM) for the Adaptive Security Appliance. Based on the belief that there will be many similarly deployed store implementations, the baseline for devices is divided into small, medium, and large store

deployments. The use of Cisco Security Manager detailed here is designed to achieve the proper level of security to each store while keeping the complexity of management to a minimum to reduce errors and oversight.

The management paradigm is based on the following five principles:

1. Firewalling is applied at the interface where the traffic originates. This can be a physical interface (such as GigabitEthernet0/1) or a virtual interface (VLAN 14). Because traffic has firewall at its source, it is trusted on the egress side of the connection. To that end, traffic is trusted as it flows across the Frame Relay network (also referred to as the WAN).
2. All traffic on the network uses legitimate IP addresses. This is enforced using unicast Reverse Path Forwarding (uRPF) on each device. Any packet that is received on an interface with a source address that is not able to have its return traffic routed back through the same interface is dropped. This is called anti-spoofing.
3. Each network serves a particular function. Each logical network segment (IP subnet or VLAN) has a specific purpose with a specific type of device that provides segmentation of duties between devices on the same network as well as providing a more straightforward means of configuring the firewall.
4. Interface roles are used to define the purpose of the network that drives policy. This allows firewall rules to be applied based on access from a specific network to another device or network. This allows the management utility (Cisco Security Manager) to define a single policy that is relevant at each store where that network exists.
5. Any exceptions to Principle #4 are handled using object overrides for information locally relevant to the firewall. For example, assume that the APs need access to another particular network at the store where their controllers reside. The firewall policy does not easily define this behavior using Principle #3, so objects used to represent both sides of the connection (source and destination) are used to define the flow.

Firewall rules are applied in a single-match, top-down, one-at-a-time manner. All firewalls at the store sites have the same policy, which is detailed below. The following four tables signify the different pieces of a hierarchical policy. All of them are combined together to form a single security policy.

Global CS-M Access Policy (Mandatory)

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Description
1	permit	CS-M server	Local router	SSH HTTPS ICMP	WAN interfaces	in	Log (IOS)	Allows CS-M server to access device through the serial (external) interface

Store Policy (Mandatory)

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Description
1	permit	any	any	IP	WAN interfaces	in	Log (IOS)	All ACLs for data center to remote are handled at the data center <i>before</i> being put into the WAN
2	permit	any	any	IP	Trusted interconnect	in	Log (IOS)	Trusted ports for passing traffic in failure scenarios
3	permit	any	192.168.62.1 61 192.168.62.1 62 192.168.42.1 30	NTP-UDP	LAN interfaces	in		permit NTP
4	permit	any	CiscoWorks Server	TFTP SNMP Syslog SNMP-Trap	Wireless AP network management interface	in	Log (IOS)	Send logs to their management utilities through the management VLAN
5	permit	CiscoWorks Server	any	SNMP SNMP-Trap Syslog SSH Telnet HTTP HTTPS	Management interface	in	Log (IOS)	CiscoWorks managed devices
6	permit	any	CS-MARS	SNMP Syslog NetFlow	Management interface wireless AP network	in	Log (IOS)	System messages to CS-MARS
7	permit	any	CS-ACS	RADIUS TACACS+	Management interface	in	Log (IOS)	Allow network devices to use the CS-ACS
8	permit	any	Data center network	ICMP	Management interface	in	Log (IOS)	Ping to data center
9	permit	Wireless Controllers	CS-ACS	RADIUS	Wireless AP network	in	Log (IOS)	Authenticate wireless users
10	permit	any	Exchange server	SMTP HTTP HTTPS	Wireless POS network general data interface wireless data network POS network	in	Log (IOS)	E-mail

11	permit	any	224.0.0.2	HSRP	Wireless POS network Partner network Wireless AP network Wireless guest network Voice network General data interface Wireless management network Wireless data network Management interface POS network	in	Log (IOS)	HSRP health information
12	permit	Wireless POS network	Wireless POS network	ICMP	Wireless POS network	in	Log (IOS)	Ping gateway
13	permit	Wireless AP network	Wireless AP network	ICMP	Wireless AP network	in	Log (IOS)	Ping gateway
14	permit	Partner network	Partner network	ICMP	Partner network	in	Log (IOS)	Ping gateway
15	permit	Wireless guest network	Wireless guest network	ICMP	Wireless guest network	in	Log (IOS)	Ping gateway
16	permit	Voice network	Voice network	ICMP	Voice network	in	Log (IOS)	Ping gateway
17	permit	General data interface	General data interface	ICMP	General data interface	in	Log (IOS)	Ping gateway
18	permit	POS network	POS network	ICMP	POS network	in	Log (IOS)	Ping gateway
19	permit	Management Interface	Management Interface	ICMP	Management Interface	in	Log (IOS)	Ping gateway
20	permit	Wireless data network	Wireless data network	ICMP	Wireless data network	in	Log (IOS)	Ping gateway
21	permit	Wireless management network	Wireless management network	ICMP	Wireless management network	in	Log (IOS)	Ping gateway
22	permit	Wireless management network	Wireless AP network	LWAPP-source ICMP	Wireless management network	in	Log (IOS)	Allows controllers to talk to APs

23	permit	Wireless AP network	Wireless management network	LWAPP ICMP	Wireless AP network	in	Log (IOS)	Allow wireless APs to talk to controllers
24	permit	Wireless AP network small	Wireless data center controller	LWAPP ICMP	Wireless AP network	in	Log (IOS)	Small stores to data center controller HREAP
25	permit	Wireless controllers	Wireless management	TFTP SNMP SNMP-Trap ICMP	Wireless management network	in	Log (IOS)	Controllers to WCS Server

Store Policy (Default)

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Description
1	permit	any	Active Directory	ILS DNS-UDP ICMP NTP HTTP Alternate-HTTP HTTPS Boots Nbsession Kerberos High-Ports-TCP tcp/1028 udp/135 tcp/445 udp/389 tcp/135	POS network Wireless POS network	in	Log (IOS)	Clients to Active Directory server
2	permit	any	Wincor-Nixdorf	Microsoft-ds MS-SQL-Server Nbdatagram Nbsession ICMP tcp/4064 MS-RDP HTTP HTTPS	POS network Wireless POS network	in	Log (IOS)	POS devices talking to Wincor
3	permit	any	MS-RMS	MS-SQL-Monitor MS-SQL-Server HTTP HTTPS	POS network Wireless POS network	in	Log (IOS)	POS to MSRMS server

4	permit	any	CSA-MC	tcp/5401 tcp/5402 HTTPS HTTP	General Data Interface POS network Wireless Data network Wireless POS network	in	Log (IOS)	Clients to CSA Manager
5	permit	any	Windows Update server	HTTP HTTPS	Wireless POS network General data interface Wireless data network POS network	in	Log (IOS)	Required for devices to perform windows updates
6	permit	any	255.255.255.255 5 Active Directory	DHCP-Relay	General data interface Management interface POS network Wireless Guest network Wireless management network Wireless data network Wireless POS network	in	Log (IOS)	Allow DHCP to work

Data Center WAN Access Policy (Mandatory)

No.	Permit	Source	Destination	Service	Interface	Dir.	Options	Description
1	deny	any	any	IP	All-Interfaces	in	Log (IOS)	Drop anything that is not explicitly allowed

CSA Manager

CSA was installed using the typical installation steps available in the published documentation. After CSA manager was installed, a policy was created to use CSA to protect the various logs on the CS-ACS server. This is similar to the process used to protect the logs on the other management servers.

First a new policy was created and named “A_PCI LAB Policy”. Then a Windows Rule Module was created called “A_PCI Sensitive LAB Data”, and associated with the policy “A_PCI LAB Policy”. (See [Figure D-17.](#))

The Rule module initially contained two combined policy rules. The first was to monitor and alert on the log files for all management servers (CSA, CS-ACS, CS-M, C-LMS, WCS and the Mars logs on the NFS backup server). The second was to protect the CS-ACS logs from access by any user or process other than the application processes via the web interface.

Figure D-17 Policy Configuration

The screenshot displays the 'Management Center for Cisco Security Agents V5.1' web interface. The main content area is titled 'Configuration > Policies > A_PCI LAB Policy'. It features a 'Quick links' box with links to 'Modify group associations', 'Modify rule module associations', 'Explain rules', and 'View change history'. Below this, the 'Name' field is set to 'A_PCI LAB Policy'. The 'Description' field is empty. Under 'Target Architectures', 'Windows' is selected with 1 module and 2 rules. The 'Attached Rule Modules' section shows one item: 'A_PCI Sensitive LAB Data' for Windows. The 'Combined Policy Rules' section is divided into 'Enforce rules' and 'Detect rules'. The 'Enforce rules' table has one entry: ID 913, Type 'File_access control', Status 'Enabled', Action 'Deny', Log 'Yes', Description 'A_ACS Protect logs', and Rule Module 'A_PCI Sensitive LAB Data'. The 'Detect rules' table has one entry: ID 904, Type 'File_access control', Status 'Enabled', Action 'Alert', Log 'No', Description 'A_Monitor Log files in LAB', and Rule Module 'A_PCI Sensitive LAB Data'. At the bottom, there are 'Save' and 'Delete' buttons, a status bar indicating '3 rule changes pending', and a 'Generate rules' button. The user is logged in as 'bart mcglothlin'.

The file access control rule with the description “A_ACS Protect logs” takes the action of denying and logging access to any files in the identified CS-ACS log directories except for the CS-ACS application processes.

The directories monitored include the following:

- C:\Program Files\CiscoSecure ACS v4.0\CSLog\Log
- C:\Program Files\CiscoSecure ACS v4.0\CSAdmin\Log
- C:\Program Files\CiscoSecure ACS v4.0\CSAuth\Log
- C:\Program Files\CiscoSecure ACS v4.0\CSDBSync\Log

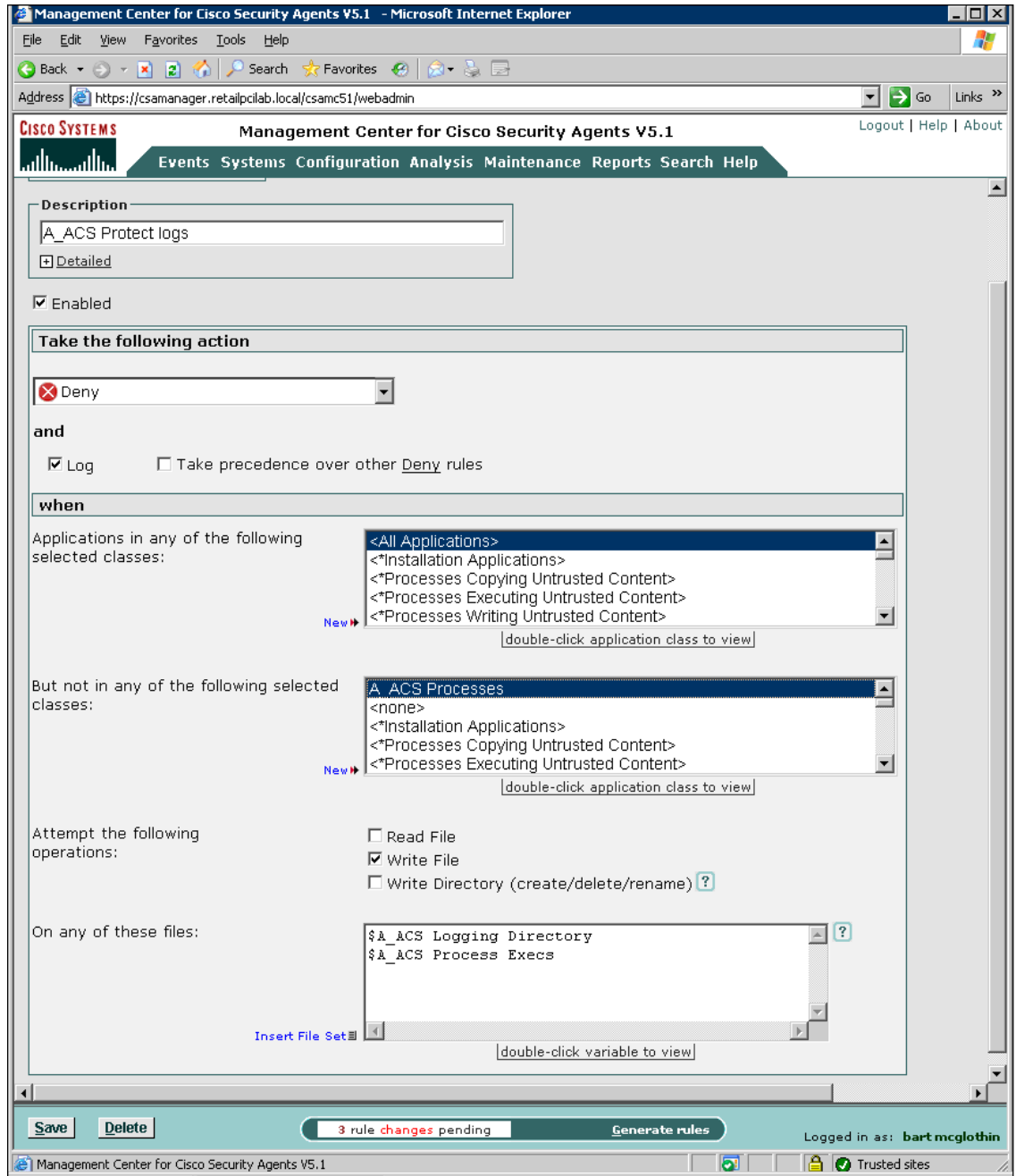
- C:\Program Files\CiscoSecure ACS v4.0\CSMon\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSRADIUS\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSTacacs\Logs
- C:\Program Files\CiscoSecure ACS v4.0\Logs* (* includes sub folders)

The permitted processes are identified as follows:

- CSAdmin.exe
- CSAuth.exe
- CSDBSync.exe
- CSLog.exe
- CSMon.exe
- CSRADIUS.exe
- CSSupport.exe
- CSSupportCL.exe
- CSTacacs.exe
- CSUpdate.exe
- CSUtil.exe

These were located in the “C:\Program Files\CiscoSecure ACS v4.0\bin” directory. (See [Figure D-18.](#))

Figure D-18 Management Center for CSA

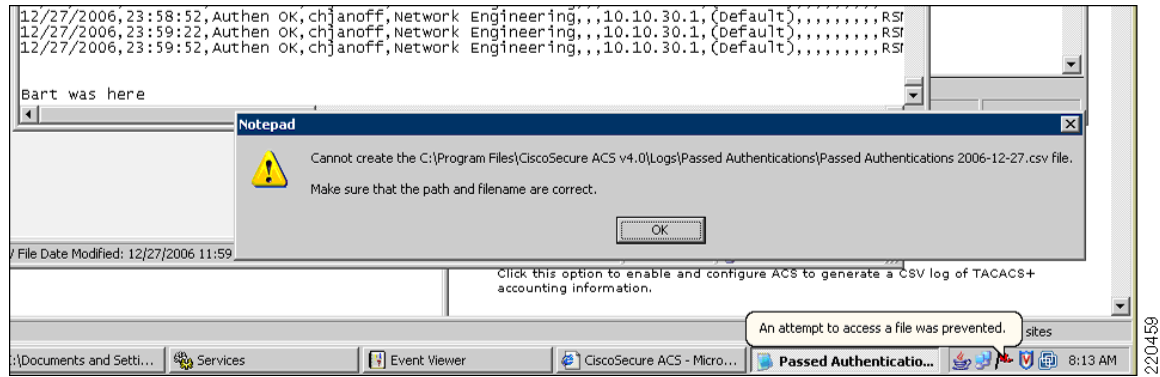


These rules use the CSA agent to enforce blocking of a user or other process from making any direct changes to the files in the prescribed folders.

When a user attempts to save a change, they receive the error message shown in Figure D-19.

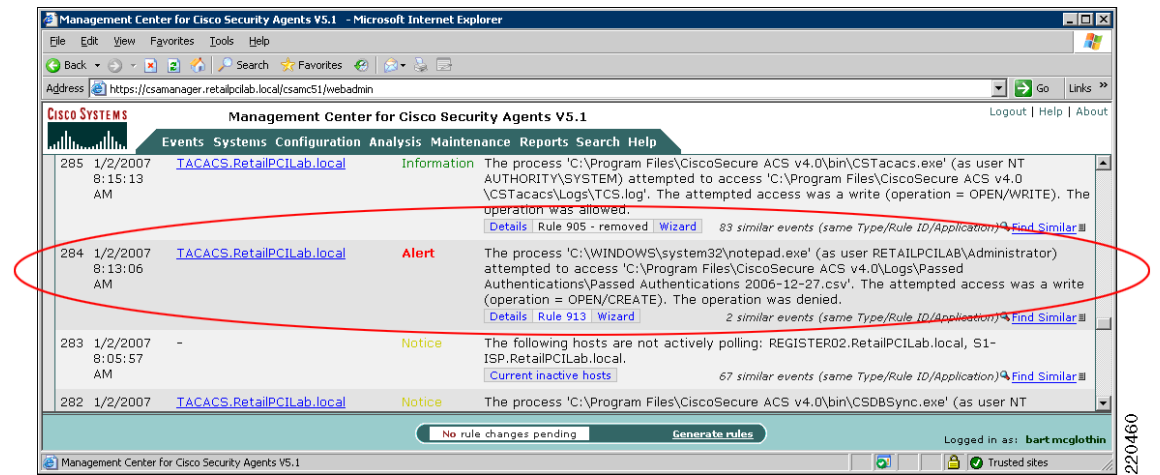
220458

Figure D-19 Error Message



This created an Event in the CSA Manager Event Log (see Figure D-20.)

Figure D-20 CSA Manager Event Log



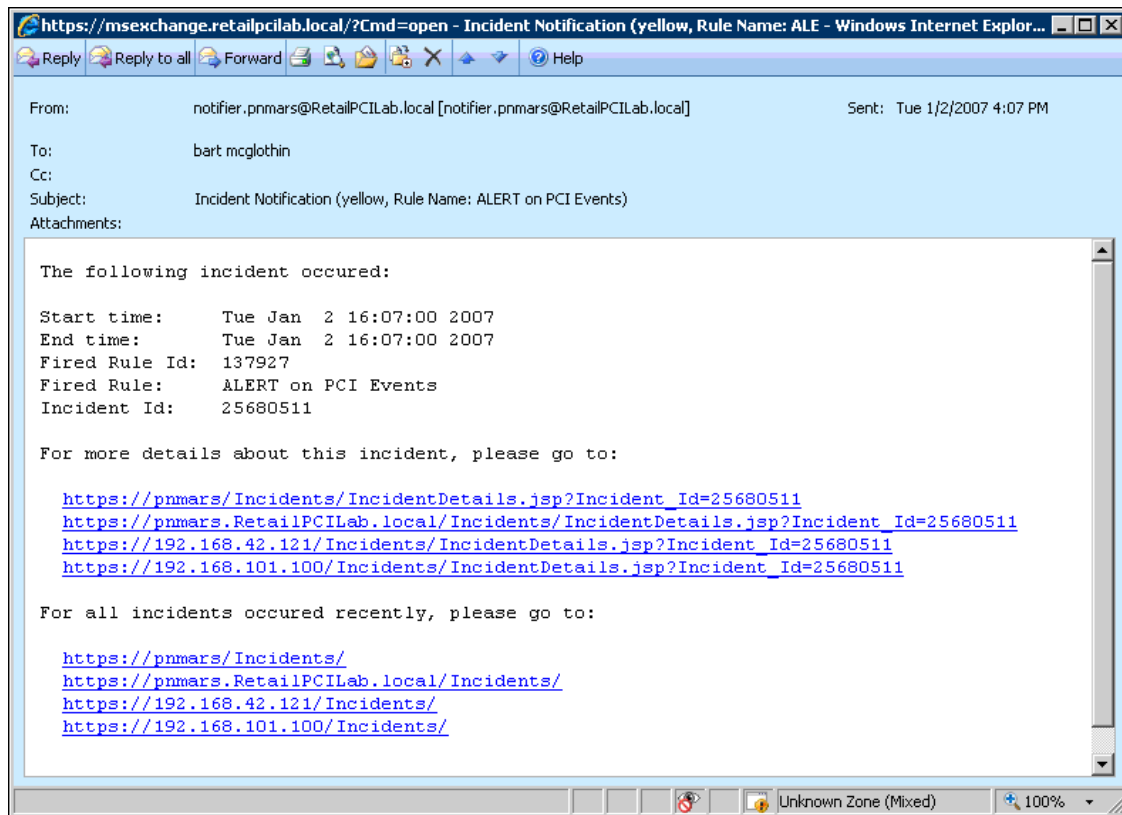
An event in the CS-MARS log was created as well (see Figure D-21.)

Figure D-21 CS-MARS Log

ID	Access	Date	Location	IP	Event Code	Process Name	File Name	Rule ID	Event Time	Status
S:28027447	Access Control	2007 8:20:26 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	22115	2007-01-02 08:20:08.736	False Positive
E:28027448	CSA File Access Control	2007 8:20:26 AM PST	TACACS.RetailPCILab.local	192.168.42.131	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	904	2007-01-02 08:20:08.736	False Positive
S:28027450	Access Control	2007 8:20:26 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	22117	2007-01-02 08:20:08.736	False Positive
E:28027433	CSA File Access Control	2007 8:20:24 AM PST	TACACS.RetailPCILab.local	192.168.42.131	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	913	2007-01-02 08:20:08.157	False Positive
S:28027434	Access Control	2007 8:20:24 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	22111	2007-01-02 08:20:08.157	False Positive
E:28027414	CSA File Access Control	2007 8:20:19 AM PST	TACACS.RetailPCILab.local	192.168.42.131	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	904	2007-01-02 08:20:04.690	False Positive
S:28027415	Access Control	2007 8:20:19 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	22109	2007-01-02 08:20:04.690	False Positive
E:28026660	CSA File Access Control	2007 8:17:05 AM PST	TACACS.RetailPCILab.local	192.168.42.131	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	904	2007-01-02 08:16:49.169	False Positive
S:28026661	Access Control	2007 8:17:05 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\WINDOWS\explorer.exe	TACACS+ Accounting	22104	2007-01-02 08:16:49.169	False Positive
E:28026326	CSA File Access Control	2007 8:15:29 AM PST	TACACS.RetailPCILab.local	192.168.42.131	468	C:\Program Files\CiscoSecure ACS v4.0\bin\ICSTacacs.exe	TCS.log	904	2007-01-02 08:15:13.450	False Positive
S:28026326	Access Control	2007 8:15:29 AM PST	TACACS.RetailPCILab.local	0.0.0.0	468	C:\Program Files\CiscoSecure ACS v4.0\bin\ICSTacacs.exe	TCS.log	22102	2007-01-02 08:15:13.450	False Positive

The CS-MARS log can be configured to send an e-mail alert, as shown in Figure D-22.

Figure D-22 E-mail Alert

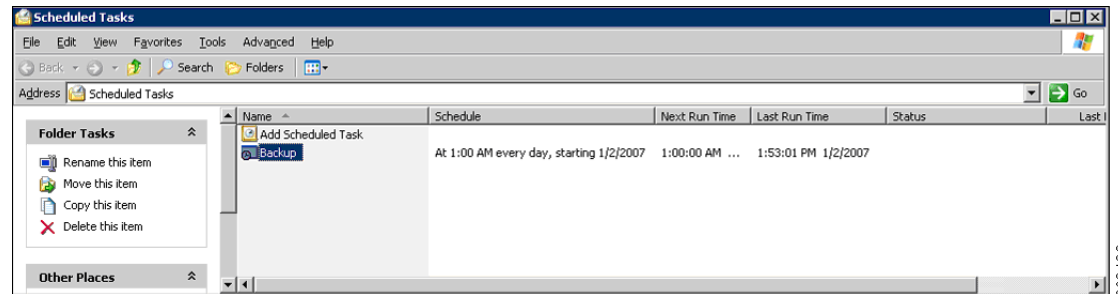


The application is still able to exercise full control over all the files in the protected directories to manage the logs and perform log switches daily.

An attempt was made to prevent the application from being able to delete historical logs by setting the directory privileges for the system account to prevent file deletion. This was not successful because it also prevented the log switch/roll event that occurs daily. The recommended practice to ensure the integrity and availability of historical logs is to switch out the logs at least daily, and then copy or backup those logs to a protected storage location.

A batch file was created to copy the logs daily to the Log backup server, where CSA was then used to restrict access and protect these files. (See [Figure D-23](#).)

Figure D-23 Batch File for Copying Logs



Following is an example of the batch file created to archive the log files off the various management servers:

```
REM===Backup ACS Server LOGS=====
REM===Map a drive letter to the admin share=====
net use x: \\TACACS\C$
E:
cd \ACS
FOR /f "tokens=2-4 delims=/ " %%a in ('DATE/T') do SET /a oldyear=%c-1
FOR /f "tokens=2-4 delims=/ " %%a in ('DATE/T') do SET /a oldmonth=%a-1
If %oldmonth% EQU 0 set /a oldyear=%oldyear%-1
If %oldmonth% EQU 0 set oldmonth=12
If %oldmonth% LEQ 9 set oldmonth=0%oldmonth%
REM===Remove Logs older than 1 year=====
FOR /F " " %%k in ('dir /a:d /o:-N /b %oldyear%-%%oldmonth%*') do rd /s /q %%k
REM===Make new folder for today's daily backup=====
FOR /f "tokens=2-4 delims=/ " %%a in ('DATE/T') do SET date=%c-%%a-%%b
md %date%
cd %date%
REM===Copy Log Files to Server=====
md logs
cd logs
xcopy "x:\Program Files\CiscoSecure ACS v4.0\Log\*" /e /h /o
cd \ACS\%date%
MD CSAdmin
cd CSAdmin
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSAdmin\Log\*" /e /h /o
cd \ACS\%date%
MD CSAAuth
cd CSAAuth
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSAuth\Log\*" /e /h /o
cd \ACS\%date%
MD CSDBSync
cd CSDBSync
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSDBSync\Log\*" /e /h /o
cd \ACS\%date%
MD CSLog
cd CSLog
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSLog\Log\*" /e /h /o
cd \ACS\%date%
```

```

MD CSMon
cd CSMon
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSMon\Logs*.*" /e /h /o
cd \ACS\%date%
MD CSRadius
cd CSRadius
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSRadius\Logs*.*" /e /h /o
cd \ACS\%date%
MD CSTacacs
cd CSTacacs
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSTacacs\Logs*.*" /e /h /o
cd \ACS\%date%
md TACACS-Backup
cd TACACS-Backup
xcopy "x:\TACACS-Backup\*.*" /e /h /o
e:
cd \
REM===Remove Share drive=====
net use x: /delete
REM===Sample Schedule Statement=====
rem at 01:00:00 /every:m,t,w,th,f,s,su "e:\backupacs.cmd"

```

Cisco Security Agent (CSA) Custom Policy for RSA Products

Based on QSA's request, a new custom policy "PCI_auditors_request" was created. This new policy is associated with two new window custom rule modules, which are as follows:

- RSA_File_Security_Manager-8.1_8.5.8—A rule to protect the RSA File Security Manager audit logs and to protect unauthorized access of RSA File Security Manager critical application files and directories.
- The file access control rule with the description "Deny access to RSA File security Manager executables" takes the action of denying and logging access to files identified in the RSA File Security Manager directories as shown below (see [Figure D-24](#)):

C:\Program Files\RSA File Security Manager

- HHActiveX.dll
- RSA File Security Manager.exe
- VDSFEncrypt.dll
- VDSFileRole.dll
- VDSFileService.dll
- VDSFWinCom.dll
- VDSHost.dll
- VKSSecureFSUI.dll

C:\Program Files\RSA Adapter Manager Common

- RSA DBSM-FSM Evaluation License.exe
- SecureDB.CFG
- UniBox10.ocx
- UniBox210.ocx

- UniBoxVB12.ocx
- UniGrid210.ocx
- VDSCAudAgentU.dll
- VDSCKM.dll
- VDSUTFAdapter.dll
- VDSUTFConsole.dll
- VDSUTFConsoleRole.dll

C:\Program Files\RSA File Security Windows Adapter

- FSAdapter.ini
- VDSFWinCEngine.dll
- VDSFWinCrypto.dll
- VDSFWinPCService.exe
- VDSFWinPEngine.dll

Figure D-24 CSA Manager Event Log—RSA File Security Manager

The screenshot shows the Cisco Management Center interface for Cisco Security Agents V5.2. The main navigation bar includes 'Events', 'Systems', 'Configuration', 'Analysis', 'Maintenance', 'Reports', 'Search', and 'Help'. The 'Events' section is active, displaying '31 events' with a 'change filter' button. The event log generation time is 1/5/2008 5:08:58 PM. The event details are as follows:

#	Date	Host	Severity	Event
31	1/5/2008 5:08:51 PM	RSAFSM.cisco-irn.com	Alert	TESTMODE: The process 'C:\WINDOWS\system32\notepad.exe' (as user CISCO-IRN\Administrator) attempted to access 'C:\Program Files\RSA File Security Manager\VDSFWinCom.dll'. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details Rule 1211 Wizard

Additional filters shown: Filter out similar events: Yes (filtered out ~90% of 296 events). A 'Find Similar' button is also present.

The file access control rule with description “Monitor RSA File Security Manager audit logs” monitors attempts to read or write files matching the file sets listed below (see [Figure D-25](#)) in the RSA File Security Manager by all applications, if the attempt causes the process to be terminated or is denied. An event is logged when the rule is triggered.

The directories monitored include the following:

- RSA File Security Manager adapter generated audit files
C:\Program Files\RSA File Security Windows Adapter\AuditLog
- RSA File Security Manager Management Console generated audit files
C:\Program Files\RSA File Security Manager\AuditLog

223729

Figure D-25 CSA Manager Event Log — RSA File Security Manager Audit Logs

Management Center for Cisco Security Agents V5.2 Logout | Help | Abc

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

30 events [change filter](#)

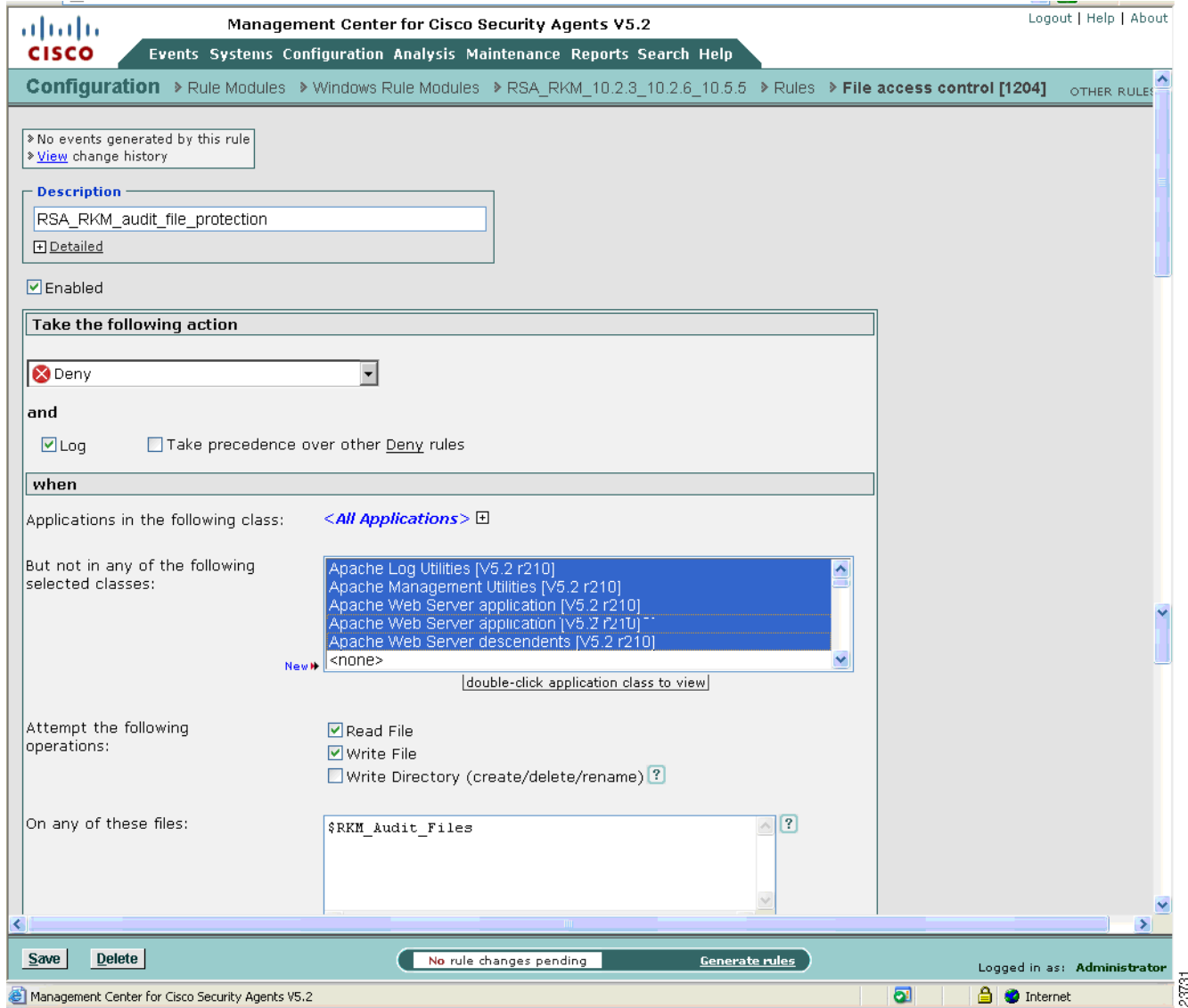
Event log generation time: 1/5/2008 4:56:23 PM
 Severity: Alert
 Host: All
 Rule Module: All
 Events per page: 50
 Sort by: Order received
 Filter out similar events: Yes (filtered out ~90% of 294 events)

#	Date	Host	Severity	Event
30	1/5/2008 4:56:14 PM	pci-ncr1.cisco-irn.com	Alert	TESTMODE: The process 'C:\WINDOWS\system32\notepad.exe' (as user CISCO-IRN\Administrator) attempted to access 'C:\Program Files\RSA File Security Windows Adapter\AuditLog\12062007Audit.log'. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details Rule 1214 Wizard 14 similar events (same Type/Rule ID/Application) Find Similar

223730

- RSA_RKM_10.2.3_10.2.6_10.5.5—A rule to protect the RSA Key Manager audit log files from unauthorized access and allow Apache Web services authorized access to these audit logs (see Figure D-26).

Figure D-26 RSA_RKM_10.2.3_10.2.6_10.5.5 File Access Control Rule



The file access control rule with description “RSA_RKM_audit_file_protection” denies unauthorized applications access to the RSA Key Manager log files .

In the example shown in Figure D-27, notepad (the unauthorized application), is denied access to the RSA Key Manager log files. An event is logged when the rule is triggered.

The directories monitored include the following:

- RSA Key Manager server:
 - C:\WINDOWS\system32\LogFiles\W3SVC1
 - C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs

Figure D-27 CSA Manager Event Log—RSA Key Manager Tomcat Logs

Management Center for Cisco Security Agents V5.2

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

30 events [change filter](#)

Event log generation time: 1/5/2008 4:53:26 PM
 Severity: Alert
 Host: All
 Rule Module: All
 Events per page: 50
 Sort by: Order received
 Filter out similar events: Yes (filtered out ~90% of 291 events)

#	Date	Host	Severity	Event
30	1/5/2008 4:53:10 PM	rkm-1.cisco-irn.com	Alert	TESTMODE: The process 'C:\WINDOWS\system32\notepad.exe' (as user CISCO-IRN\Administrator) attempted to access 'C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs\key-manager.log'. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details Rule 1214 Wizard 13 similar events (same Type/Rule ID/Application) Find Similar

Cisco Security Agent (CSA) Custom Policy for NCR

The following were created:

1. A new policy called “PCI 11.5 NCR-ACS directories and files monitoring”.
2. A Windows Rule Module called “PCI-11.5 NCR Advanced Checkout Solution” and assigned to the newly created policy above. (See [Figure D-28](#).)

The Rule Module initially contained two combined policy rules. The first protects the files and executables in the NCR-ACS directory from unauthorized access. The second protects the NCR-ACS authorized applications from being overwritten.

Figure D-28 NCR Policy Configuration

The screenshot shows the Management Center for Cisco Security Agents V5.2 web interface. The main configuration area is titled "Management Center for Cisco Security Agents V5.2" and includes a navigation menu with options like Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The configuration details for a policy named "PCI 11.5 NCR ACS directories and files monitoring" are displayed. The Name and Description fields both contain the policy name. Under Target Architectures, the "Windows" checkbox is checked, indicating 1 module and 2 rules. The Attached Rule Modules section shows one item: "PCI - 11.5 NCR Advanced Checkout Solution" with a description of "PCI - 11.5 NCR Advanced Checkout Solution" and a target OS of "All Windows". The Combined Policy Rules section for Windows shows two rules:

ID	Type	Status	Action	Log	Description	Rule Module	Events
1205	File access control	Enabled	Deny	Yes	PCI 11.5 NCR ACS Directories and files	PCI - 11.5 NCR Advanced Checkout Solution	113
1212	File access control	Enabled	Deny	Yes	Protect NCR Executables from being overwritten	PCI - 11.5 NCR Advanced Checkout Solution	0

At the bottom of the interface, there are buttons for "Save" and "Delete", a status bar indicating "No rule changes pending", and a "Generate rules" button. The user is logged in as "Administrator".

The “NCR Advanced Checkout Solution” rule module protects the NCR-ACS directory and the executables associated with these applications from unauthorized access. The file access control rule with the description “ PCI 11.5 NCR ACS directories and files” takes the action of denying unauthorized access to all the files and executables contained in the NCR-ACS directories. An event is logged when the rule is triggered.

The NCR-ACS directories include the following:

- @fixed \ACS*.*

where @fixed can be any local drive where the \ACS directory is located.

The authorized NCR applications are:

Directories matching

- *.*\ACS**
- *.***\Microsoft SQL Server**
- *.***\Framework**

Files matching

- *.exe
- csc.exe

See [Figure D-29](#).

Figure D-29 PCI-11.5 NCR ACS Directories and File, File Access Control Rule

The screenshot shows the Management Center for Cisco Security Agents V5.2. The breadcrumb navigation is: Configuration > Rule Modules > Windows Rule Modules > PCI - 11.5 NCR Advanced Checkout Solution > Rules > File access control [1205].

At the top left, it indicates that 113 events were generated by this rule, with a link to view the change history.

Description: PCI 11.5 NCR ACS Directories and files. A "Detailed" view button is available.

Enabled: A checked checkbox indicates the rule is enabled.

Take the following action: A dropdown menu is set to "Deny".

and:

- Log
- Take precedence over other Deny rules

when:

- Applications in the following class: **<All Applications>**
- But not in any of the following selected classes:
 - Command Shell [V5.2 r210]
 - PCI NCR Applications
 - <none>
 - <*Installation Applications>
 - <*Processes Copying Untrusted Content>

Attempt the following operations:

- Read File
- Write File
- Write Directory (create/delete/rename) ?

On any of these files:

- \$PCI 11.5 NCR ACS directories and files

At the bottom right of the configuration area, there is a vertical timestamp: 22:37:04.

The file access control rule with the description “PCI 11.5 NCR ACS directories and files” takes the action of denying unauthorized access to the PCI 11.5 NCR ACS directories and files. In the example shown in Figure D-30, the unauthorized application (explorer.exe) is trying to access the NCR POS system’s NCR-ACS directory.

Figure D-30 CSA Manager Event Log – Accessing NCR POS System’s ACS Directory

The screenshot shows the Cisco Management Center for Cisco Security Agents V5.2 interface. The top navigation bar includes 'Events Systems Configuration Analysis Maintenance Reports Search Help'. The main content area is titled 'Events > Event Log' and displays 31 events. A filter is applied, showing 1 event. The event details are as follows:

#	Date	Host	Severity	Event
31	1/5/2008 6:20:43 PM	pci-ncr1.cisco-irn.com	Alert	TESTMODE: The process 'C:\WINDOWS\explorer.exe' (as user CISCO-IRN\Administrator) attempted to access 'C:\ACS\Clients\Win32\Config\webcid4.cfg'. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details Rule 1205 Wizard

Additional information shown in the screenshot includes: Event log generation time: 1/5/2008 6:21:03 PM; Severity: Alert; Host: All; Rule Module: All; Events per page: 50; Sort by: Order received; Filter out similar events: Yes (filtered out ~90% of 306 events). A vertical text '223735' is visible on the right side of the screenshot.

The file access control rule with the description “Protect NCR Executables from being overwritten” takes the action of preventing the authorized PCI 11 NCR Applications from being overwritten. See Figure D-31.

Figure D-31 Protect NCR Executables from Being Overwritten , File Access Rule

The screenshot displays the configuration page for a File Access Rule in the Cisco Management Center. The breadcrumb navigation shows the path: Configuration > Rule Modules > Windows Rule Modules > PCI - 11.5 NCR Advanced Checkout Solution > Rules > File access control [1212].

Configuration Details:

- Description:** Protect NCR Executables from being overwritten. A checkbox for "Detailed" is present.
- Enabled:** Enabled
- Take the following action:**
 - Action: Deny
 - and**
 - Log
 - Take precedence over other Deny rules
- when**
 - Applications in the following class: <All Applications>
 - But not in the following class: <none>
 - Attempt the following operations:
 - Read File
 - Write File
 - Write Directory (create/delete/rename) ?
 - On any of these files: \$PCI 11 NCR Applications

Additional information: A message box states "No events generated by this rule" with a link to "View change history". The page footer includes the number 223796.

RSA Key Manager

RSA Key Manager Administration Console

This section describes the main use cases and configuration for Key Manager Administration console.

Starting and Stopping the Key Manager Server

The RSA Key Manager requires a startup key that can be stored on an HSM, entered manually at startup (in the form of a password) or cached locally to be replayed during a server restart. The Cisco Retail lab configuration replays the cached password whenever the server is restarted. This enables no user interaction during restart. If this option is not selected, user intervention is required (see [Figure D-32](#)). If an HSM is used, the policies dictated by the deployment (possibly *m of n*) are invoked. If the key material is not presented, no key requests is serviced.

At installation time, the Key Manager Server can be configured to either start automatically (unattended restart) or, for added security, require a master password to be entered. The Enable Unattended Restart option, selected during installation, specifies that the Key Manager Server can service Key Manager Client requests immediately after a start or restart. If this option is not selected, then after a start or restart, Key Manager Client requests are ignored, and any attempt to access the Key Manager Administration Console is redirected to a Key Manager Startup page where an administrator must enter the master password that is set during the Key Manager Server installation.

Figure D-32 Key Manager Startup Page

RSA Key Manager

Key Manager Startup

Enter the master password for the Key Manager Server keysto.e.

Password:

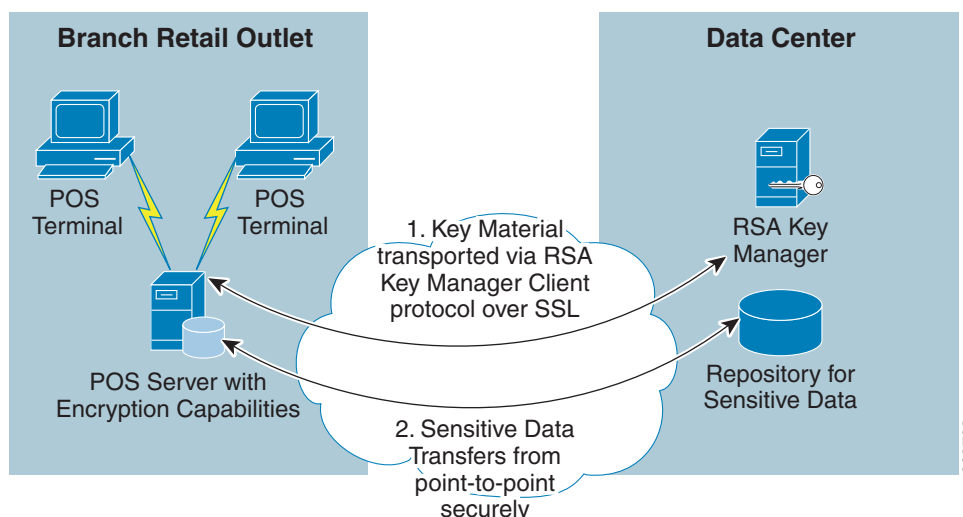
223737

Apache Tomcat was used in the lab environment. Whenever this Tomcat instance is stopped, the RSA Key Manager server stops taking requests. Upon restart the key material in the form of a password is presented automatically. The Key Manager Server is stopped via the application server for your deployment. In this case, we used Tomcat Apache as application server and the Key Manager was stopped by stopping the Tomcat Apache service.

RSA Key Manager Server and Client Deployment

Typical branch architecture could include the transmission of customer credit card data that could be exposed during transmission if encryption mechanisms are not employed. Figure D-33 shows a typical deployment scenario whereby customer credit card information is processed in the branch and encrypted for storage in the point-of-sale server. During the process key material is requested from the RSA Key Manager located in the data center. The key material is then used to encrypt the credit card data and may be transported over any secure point-to-point VPN tunnel (e.g., Cisco VPN) to be stored in the data center repository. This model provides security for both data at rest and data in transit.

Figure D-33 Typical Branch Deployment



In this scenario, the POS server becomes a client to the RSA Key Manager and requests keys based on the client’s ability to establish a mutually authenticated SSL session with the RSA Key Manager and policy dictated by the security officer. In the lab environment, RSA Key Manager sample program was installed on a Windows XP PC (which acted as client to RSA Key Manager). Keys from the RSA Key Manager are requested via a command-line utility running on the RSA Key Manager Client’s PC running Windows XP that leverages the RSA Key Manager Client (a sample program) application programming interface (API).

Successful key generation from a sample RSA Key Manager Client program running on Windows XP PC:

- C:\rkm\samples\2.1>test
- C:\rkm\samples\2.1>set install_dir=c:\rkm
- C:\rkm\samples\2.1>SET LIBRARY_DIR=c:\rkm\library\lib
- C:\rkm\samples\2.1>SET KM_SUPPORT_LIBRARY=kmsvcshlib.dll
- C:\rkm\samples\2.1>SET KM_SUPPORT_LIB_PATH=c:\rkm\library\lib\kmsvcshlib.dll
- C:\rkm\samples\2.1>SET KM_CRYPTOLIB_PATH=c:\rkm\library\lib\kmcryptolib.dll
- C:\rkm\samples\2.1>SET KM_CRYPTOLIB_LIBRARY=kmcryptolib.dll
- C:\rkm\samples\2.1>SET R_SHLIB_LD_LIBRARY_PATH=c:\rkm\library\lib
- C:\rkm\samples\2.1>SET KM_CRYPTOLIB_PATH=c:\rkm\library\lib\kmcryptolib.dll
- C:\rkm\samples\2.1>get_key -init_file init.cfg -svc_file svc.cfg -key_class keyclass1

Demonstrating Get Key Operation

```

Getting key by Key Class keyclass1...
Key ID: 1508515971
UUID:      b8 36 ca b1 5a b8 46 46 80 2f b2 1b ac b5 a2 69      [.6..Z.FF./.....i]
Aliases:
Key class: KeyClass1
Key Data:
          71 a5 17 97 2f a8 e4 a4 d1 83 4b 3a 01 60 35 c6      [q.../.....K:.`5.]
          7a 4a 03 60 d0 b8 1f c2 68 89 63 74 ba 97 2f 2d      [zJ.`....h.ct../-]
Integrity check:
          54 0a bb 5e 25 22 e3 2f 05 85 4a e9 87 c5 fa b6      [T..^%"/..J.....]
          bf 01 81 8c 04 63 c2 8d bd 46 f2 2b a7 61 a6 8f      [.....c...F.+a..]
Attributes:
Key algorithm: AES_256_CBC
Not before: 1199314224893
Not after: 1199400624893
Create date: 1199314224893
Not Before Generalized Time: 20080102225024Z
Not After Generalized Time: 20080103225024Z
Create Date Generalized Time: 20080102225024Z
Key version: 2.1
Key type: UNKNOWN
Key Format: RAW
Exportable: TRUE
Key state: ACTIVATED
Key sub_state: PROTECT_AND_PROCESS
Key state description: Internal creation.

Key bytes (32 bytes):
          71 a5 17 97 2f a8 e4 a4 d1 83 4b 3a 01 60 35 c6      [q.../.....K:.`5.]
          7a 4a 03 60 d0 b8 1f c2 68 89 63 74 ba 97 2f 2d      [zJ.`....h.ct../-]

```

Demonstrating Key Sync Operation

```

Key ID: 1508515971
UUID:      b8 36 ca b1 5a b8 46 46 80 2f b2 1b ac b5 a2 69      [.6..Z.FF./.....i]
Aliases:
Key class: KeyClass1
Key Data:
          71 a5 17 97 2f a8 e4 a4 d1 83 4b 3a 01 60 35 c6      [q.../.....K:.`5.]
          7a 4a 03 60 d0 b8 1f c2 68 89 63 74 ba 97 2f 2d      [zJ.`....h.ct../-]
Integrity check:
          54 0a bb 5e 25 22 e3 2f 05 85 4a e9 87 c5 fa b6      [T..^%"/..J.....]
          bf 01 81 8c 04 63 c2 8d bd 46 f2 2b a7 61 a6 8f      [.....c...F.+a..]
Attributes:
Key algorithm: AES_256_CBC
Not before: 1199314224893
Not after: 1199400624893
Create date: 1199314224893
Not Before Generalized Time: 20080102225024Z
Not After Generalized Time: 20080103225024Z
Create Date Generalized Time: 20080102225024Z
Key version: 2.1
Key type: UNKNOWN
Key Format: RAW
Exportable: TRUE
Key state: ACTIVATED
Key sub_state: PROTECT_AND_PROCESS
Key state description: Internal creation.

```

Get Key Successful

C:\rkm\samples\2.1

RSA Key Manager Logging

The Key Manager Server provides logging of runtime operations to a log file, for audit purposes. All log messages include the time and date, the full class name of the file where the log message was generated, the level of the log message and context information from the application.

Logging Levels

The Key Manager Server provides the following levels of logging:

- Debug

Debug messages are produced to allow diagnostic and application management of the Key Manager Server.

- Information

Information messages are produced when:

- An administrator Identity initiates or terminates access to the Key Manager Administration Console. The administrator user name is logged.
- The Key Manager Server generates a key. The identity group, key class, user name of the administrator who initiated the key generation, key start date, and other context information is logged.
- The Key Manager Server adds or updates an identity. The name of the Identity, user name of the administrator who added or updated the application and other context information is logged.
- The Key Manager Server adds or updates an identity group. The name of the identity group, user name of the administrator who added or updated the identity group and other context information is logged.
- The Key Manager Server adds a new security class or key class. The name of the class, user name of the administrator who added the class and other context information is logged.
- The Key Manager Server adds a new crypto policy. The name of the crypto policy, user name of the administrator who added the crypto policy and other context information is logged.

- Error

Error messages are produced to report on all error conditions that arise in the Key Manager Server at run time. An error condition is any abnormal state of the system that stops the Key Manager Server from executing a business process (for example, the inability to access system resources such as memory or disk space).

The system administrator specifies the logging level, and the Key Manager Server outputs log messages that are greater than or equal to the specified logging level. [Table D-1](#) shows the types of messages that are logged at each logging level.

Table D-2 Messages Logged at Logging levels

	Debug Messages	Information Messages	Error Messages
Debug Level	Yes	Yes	Yes
Information Level	No	No	Yes
Error Level	No	No	Yes
All Levels	Yes	Yes	Yes
Logging Off	No	No	No

[Figure D-34](#) shows the RSA Key Manager logging in the lab environment (C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs).

Figure D-34 RSA Key Manager Logs

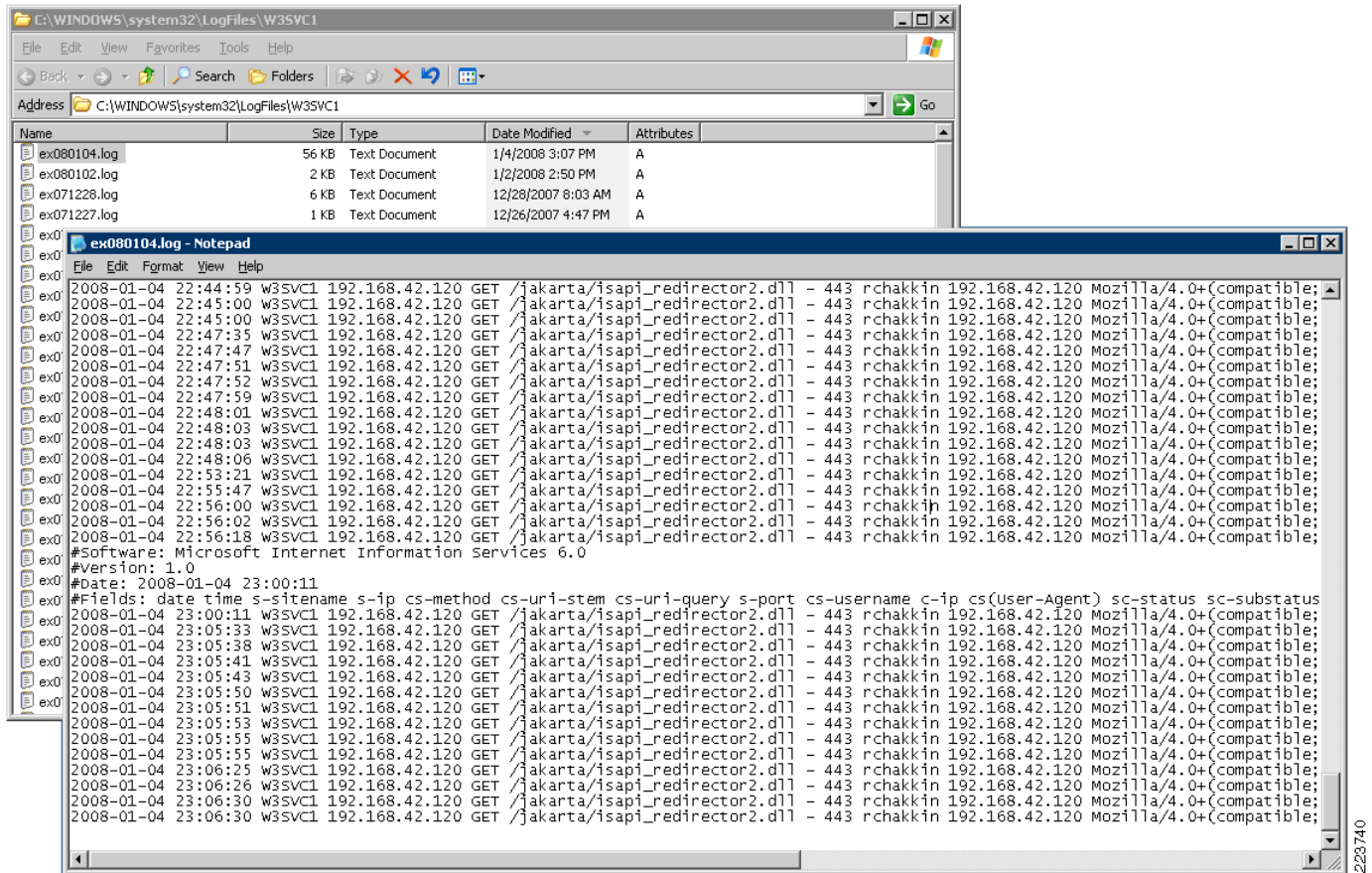
```

at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.a(KeyManager:44)
at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.filter(KeyManager:34)
at com.rsa.keymanager.transport.core.filter.EdgifierFilter.doFilter(KeyManager:21)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:202)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:173)
at com.rsa.edge.javax.servlet.DefaultFilterChain.doFilter(KeyManager:19)
at com.rsa.keymanager.transport.core.filter.TimeFilter.doFilter(KeyManager:15)
at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.a(KeyManager:44)
at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.filter(KeyManager:34)
at com.rsa.keymanager.transport.core.filter.EdgifierFilter.doFilter(KeyManager:21)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:202)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:173)
at com.rsa.edge.javax.servlet.DefaultFilterChain.doFilter(KeyManager:19)
at com.rsa.keymanager.transport.core.filter.ServerAccessibilityFilter.doFilter(KeyManager:19)
at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.a(KeyManager:44)
at com.rsa.keymanager.transport.core.filter.DefaultFilterAdaptor.filter(KeyManager:34)
at com.rsa.keymanager.transport.core.filter.EdgifierFilter.doFilter(KeyManager:21)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:202)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:173)
at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
at org.apache.jk.server.JkCoyoteHandler.invoke(JkCoyoteHandler.java:199)
at org.apache.jk.common.HandlerRequest.invoke(HandlerRequest.java:282)
at org.apache.jk.common.ChannelSocket.invoke(ChannelSocket.java:767)
at org.apache.jk.common.ChannelSocket.processConnection(ChannelSocket.java:697)
at org.apache.jk.common.ChannelSocket$SocketConnection.runIt(ChannelSocket.java:889)
at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
at java.lang.Thread.run(Thread.java:595)
2008-01-04 13:52:06,585 INFO TP-Processor8 com.rsa.keymanager.transport.core.action.LogoutAction - Logged out: kmsrchakkin (1)
2008-01-04 13:52:21,739 INFO TP-Processor8 com.rsa.keymanager.transport.core.action.LogoutAction - Logged out: kmsrchakkin (1)
2008-01-04 14:30:59,299 INFO TP-Processor8 com.rsa.keymanager.transport.core.action.LogoutAction - Logged out: kmsrchakkin (1)

```

Figure D-35 shows the RSA WebServer logging (Microsoft IIS 6.0).

Figure D-35 Web Server Logging



RSA File Security Manager

Detailed System Architecture

Figure D-36 illustrates a typical store architecture. In this architecture, the stores have a POS server that aggregates the transaction logs at each store before transmitting them to the central repository at the data center. To comply with PCI-DSS requirements, merchants are required to secure the transaction log data stored at each POS server and the central repository.

In this specific example, the transaction log data is stored in files, in a folder called “D:\TLOG”. These files are then replicated across to the server attached to EMC storage in Cisco data center for transaction log repository when possible. The TLOG repository stores the files in a folder called “X:\TLOG”. Due to significant sizing and performance requirements, this server’s file system resides on an EMC Symmetrix based Storage Area Network (SAN).

Before RSA File Security Manager is used to secure data at rest on the payment systems, the sensitive data in the files stored on the POS Server and the TLOG repository are subject to a variety of internal and external threats.

Figure D-36 POS System and TLOG repository without RSA File Security Manager

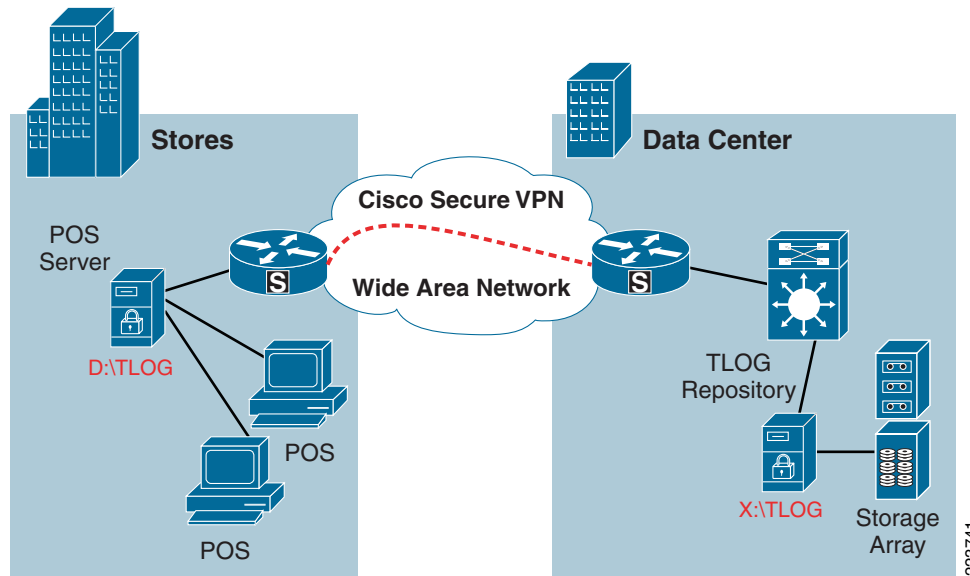
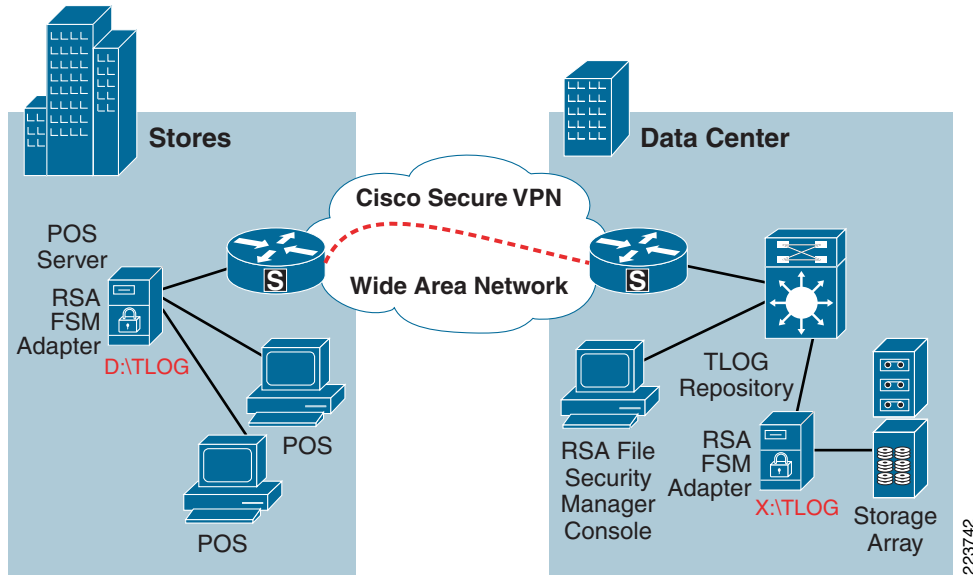


Figure D-37 illustrates the same store infrastructure as Figure D-36, after the RSA File Security Manager components are incorporated into it. RSA File Security Manager does not impose or require and specialized or additional hardware requirements.

The RSA File Security Manager “file system adapters” are installed on each POS server and the central TLOG repository server. In this scenario, these servers run a general purpose operating system such as Windows 2003 Server. The file security adapters are managed and administered from the central data center via the RSA File Security Manager management console (aka “the adapter manager”).

Figure D-37 POS system and TLOG repository with RSA File Security Manager



Detailed Configuration Steps



Note

Only the critical configuration steps are illustrated below.

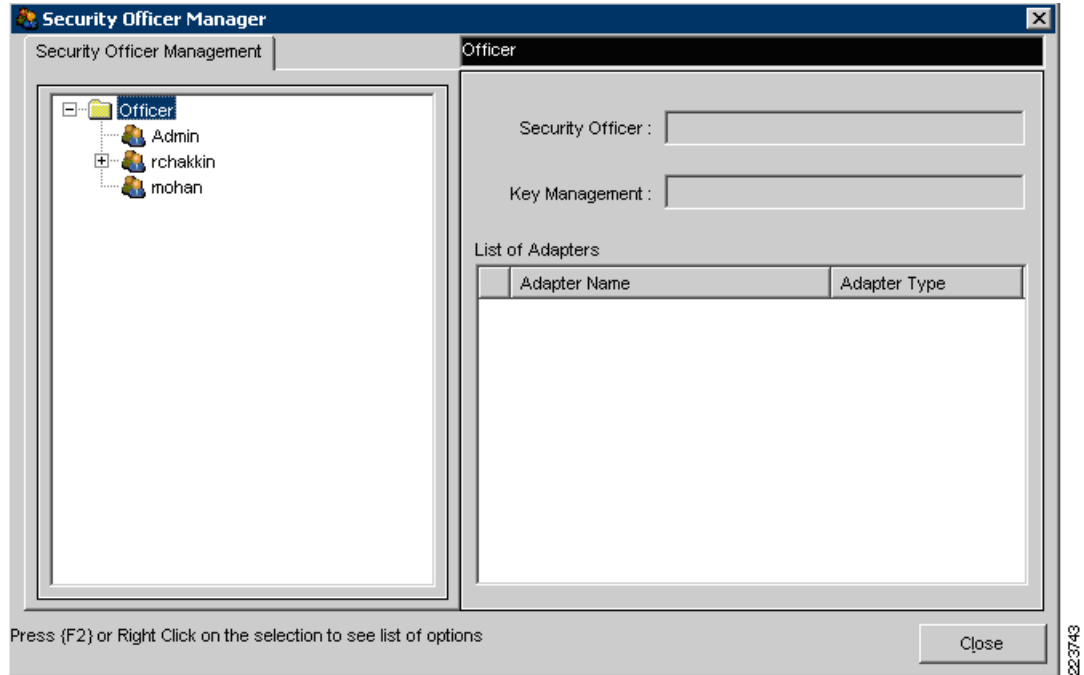
There are two types of security custodians who manage RSA File Security Manager. The Security Administrator (SA) is at the top of the hierarchy. The SA’s duty is to manage the lifecycle of Security Officers (SO). The SA has no visibility into the servers or the files/folders that are secured by the file security adapters.

The SO’s role is to manage the security policy for the servers/systems that have the file security adapters installed. The SO has visibility into references to encryption keys and high-level file system structure. But, note that the SO has no visibility into the actual data in the protected file system.

RSA File Security Manager implements this security model to ensure that we can achieve separation of duties between system administration, actual usage, and security administration. When RSA File Security Manager uses with your server infrastructure, you can ensure that there is no single entity/person who can compromise the security of your system either by accident or malice.

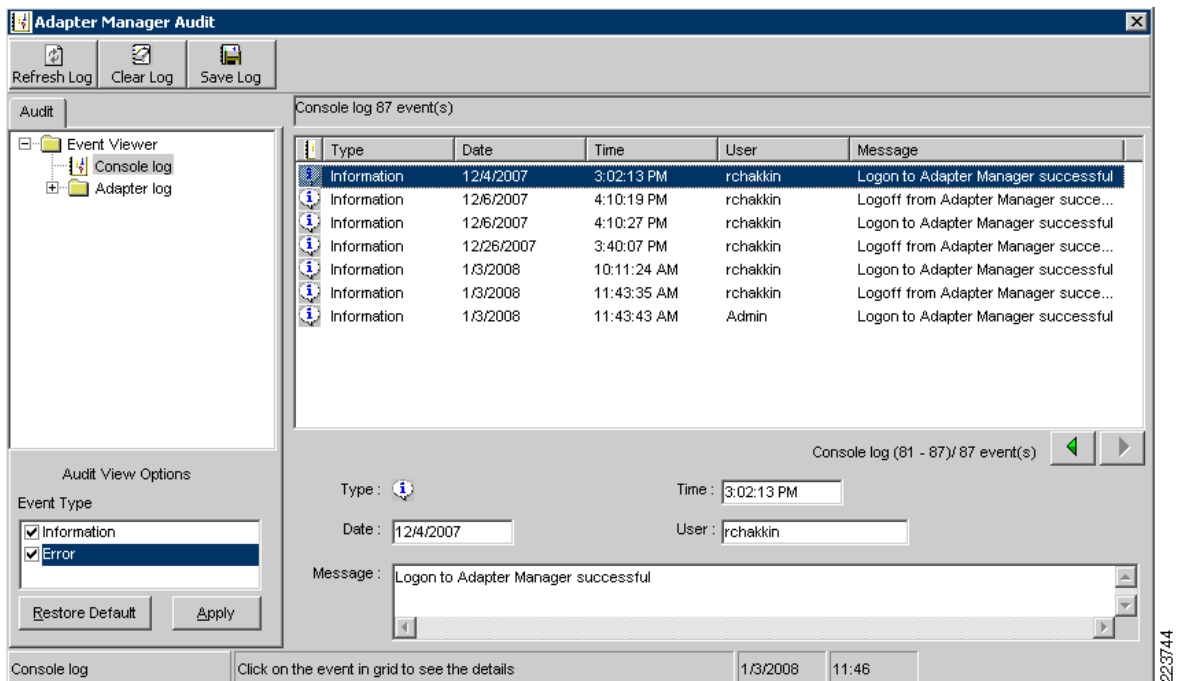
Figure D-38 illustrates the workflow involved with the management of SOs. This is what the SA sees on the RSA File Security Manager graphical management console after a successful login.

Figure D-38 SO Management Screen



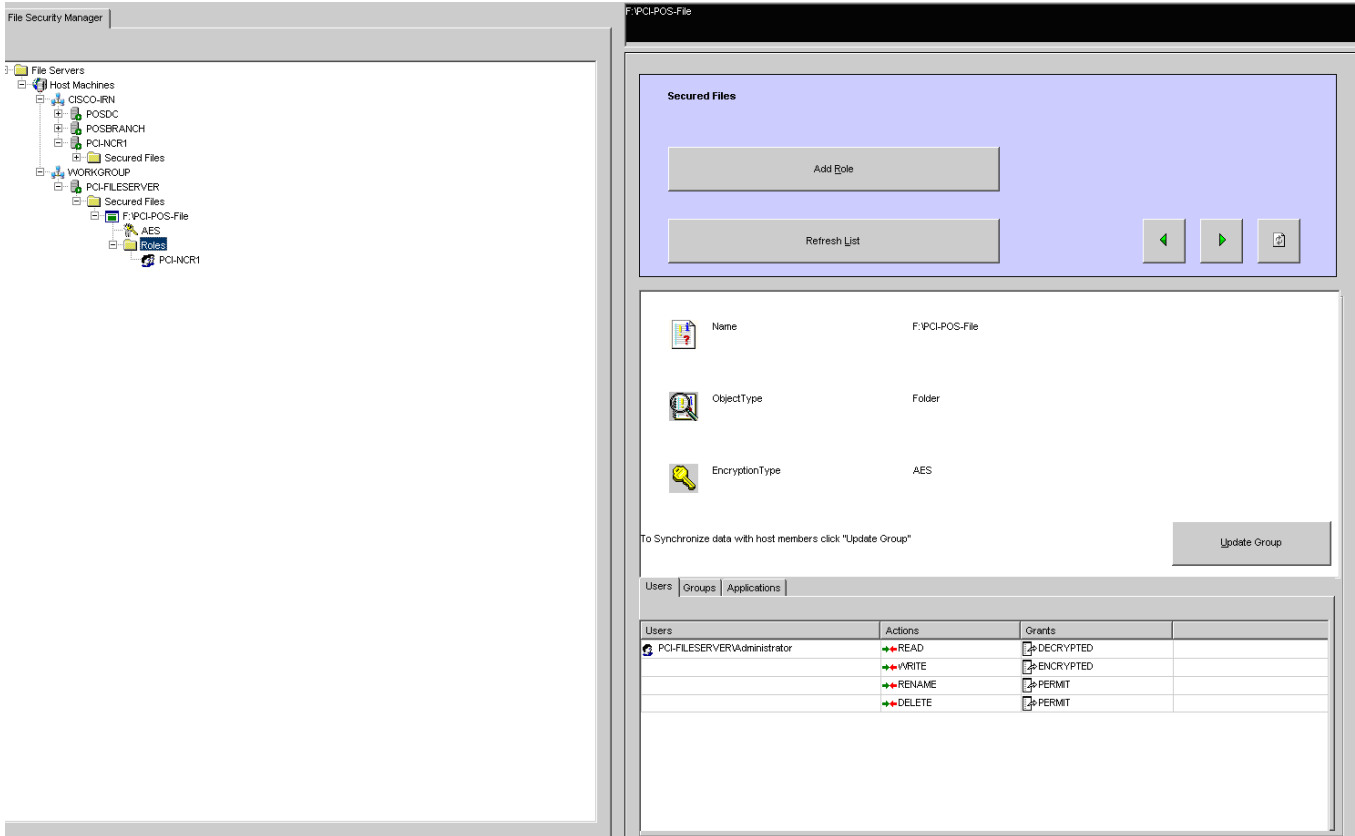
To ensure that events and actions associated with security administration as well as access to secured folders are non-repudiable, RSA File Security Manager captures a detailed audit trail of all events and actions. Figure D-39 illustrates the audit log, which is visible to the security administrator.

Figure D-39 SA Access to Audit Log



The SO's management console looks very different from that of the SA's. A sample GUI is shown in [Figure D-40](#). All security administration is performed by a simple, graphical workflow.

Figure D-40 SO GUI

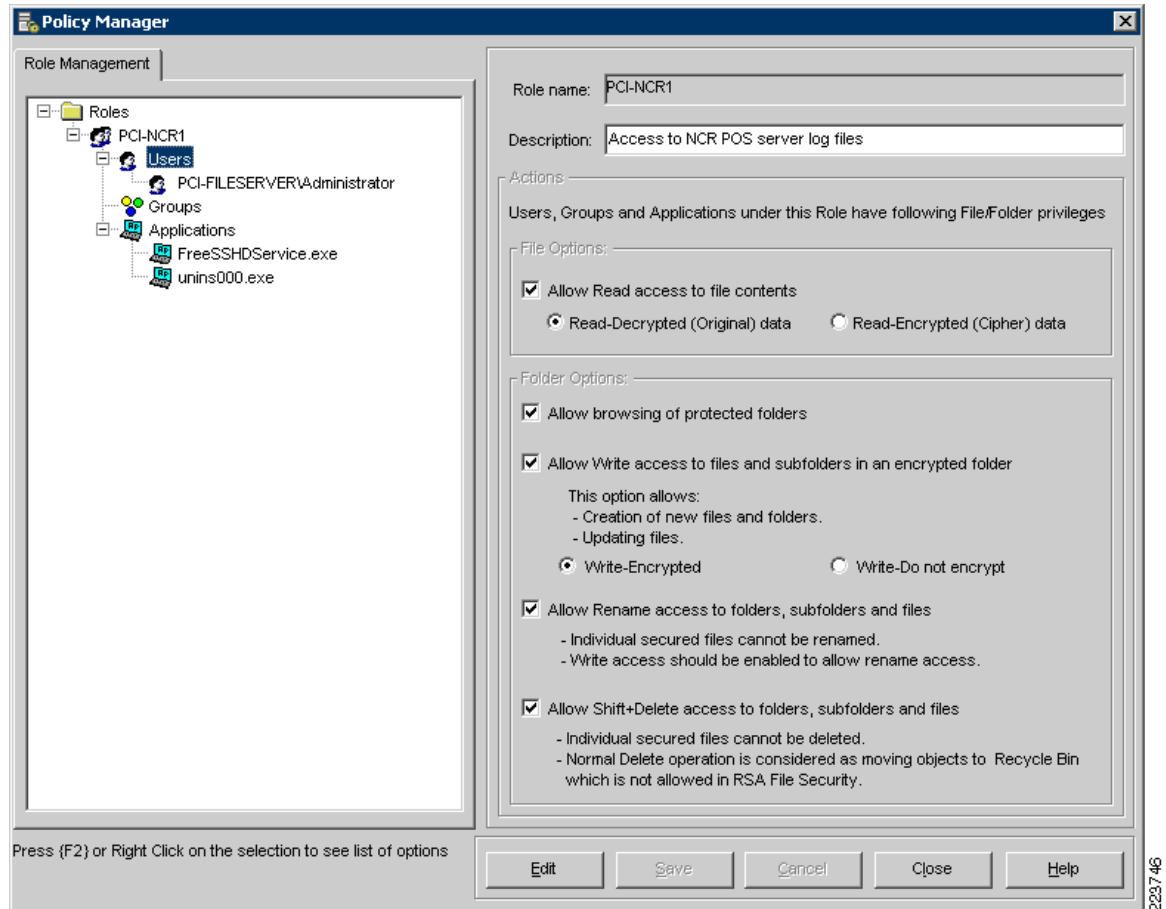


223745

RSA File Security Manager implements a role-based access control methodology. First, the security officer has to define a role and specify what type of access members the role has. Next, the security officer has to specify members of the role, which can either be local or domain users and fingerprinted applications.

For authorized users and applications, the file security adapter's default policy transparently "encrypts" file data when data is written and transparently "decrypts" file data when data is read. An example of a role is illustrated in [Figure D-41](#).

Figure D-41 A Sample Role Screen



PCI Section 6.5

The requirement for PCI 6.5 section was met using Cisco ACE XML Gateway product. Verizon Business observed the use of Cisco's ACE XML Gateway to protect against common web vulnerabilities identified under PCI section 6.5.1 to 6.5.10.

Open Web Application Security Project (OWASP)

The OWASP top ten provides information and awareness about web application security. The OWASP top ten focuses on a broad agreement about what the most critical web application security flaws are. The primary aim of the OWASP top ten is to educate developers, designers, architects, and organizations about the consequence of the most common web application security vulnerabilities. For more information, visit – <http://www.owasp.org>.

PCI 6.5.4 Cross-Site Scripting (XSS) Attacks

Cross site scripting, better know as XSS, is a subset of HTML injection. XSS is the most prevalent and pernicious web application security issue. XSS flaws occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

XSS allows attackers to execute scripts in the victims browser, which can hijack user sessions, deface websites, insert hostile content, conduct phishing attacks, and take over the user’s browser using scripting malware.

Environments Affected

All web application framework are vulnerable to cross scripting.

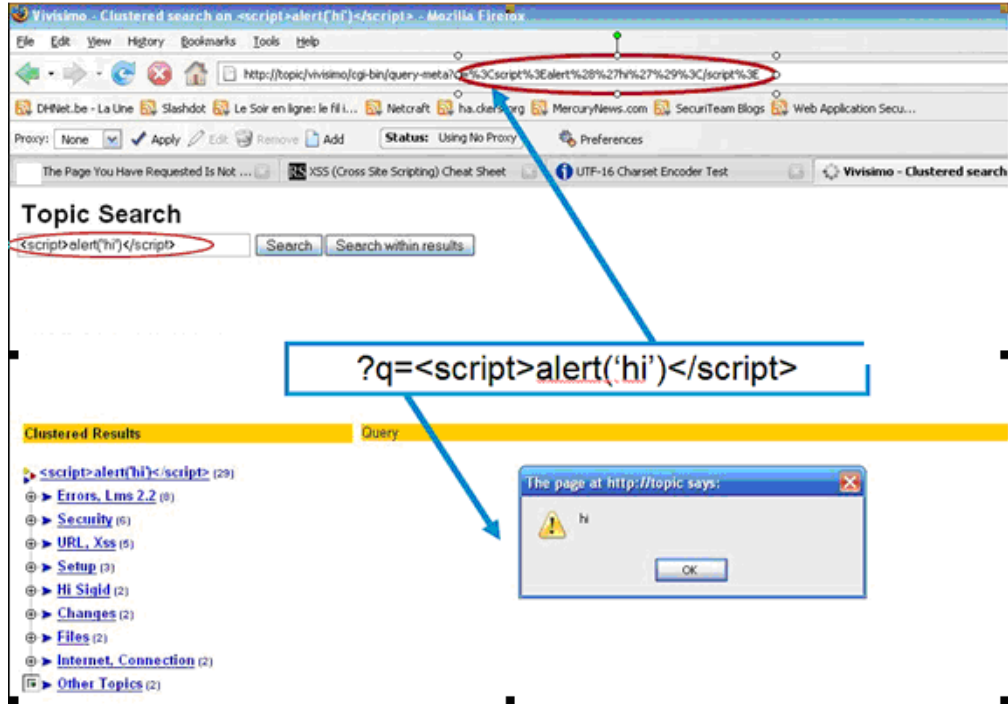
Implications

- Website defacement
- Session IDs stolen (cookies exported to hacker’s site)
- Browser security compromised—control given to hacker
- All data sent between client and server potentially hijacked

Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML-based XSS attacks. For example, ACE XML Gateway can prevent submission of XML and HTML tags to the web server (required for XSS attacks). All XSS attacks were manual and required custom configuration of the ACE XML Gateway application.

In the PCI lab environment, a malicious script is echoed back in an HTML format returned from a trusted website. The script is locally executed on the client PC.

Figure D-42 XSS Example



Mitigation

The Cisco ACE XML Gateway offers the following two ways of protecting a site from XSS:

- Blacklist approach—XSS pattern detection and recognition
- Whitelist approach—The AXG is configured with the legitimate values of the URL/POST query parameters. The Cisco ACE XML Gateway blocks out what falls outside the remaining range.

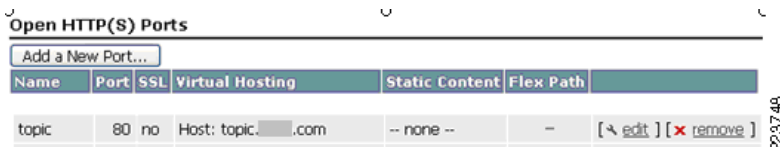
In the lab environment, whitelist approach was used to show how the Cisco ACE XML Gateway can block XSS attack.

Cisco ACE XML Gateway Blocking XSS Attack

The following are the steps for setting XSS attack blocks in the Cisco ACE XML Gateway.

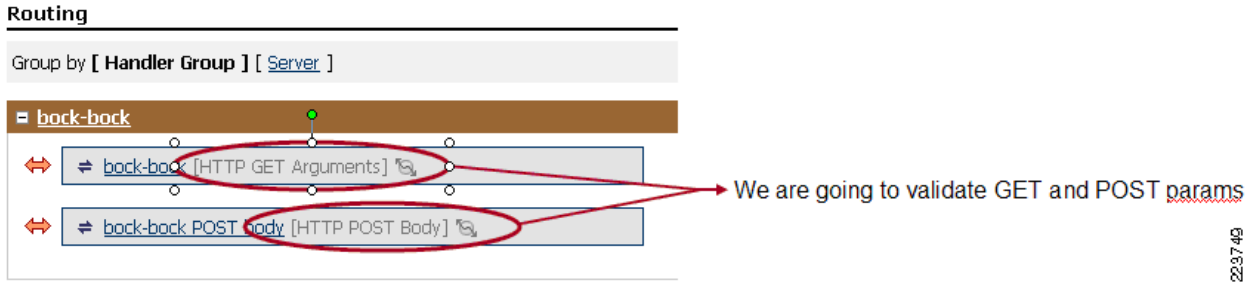
- Step 1** Define the hosts that need to be protected. See [Figure D-43](#).

Figure D-43 Defining Which Hosts Need to Protected



Step 2 Define the policy for each host. See [Figure D-44](#).

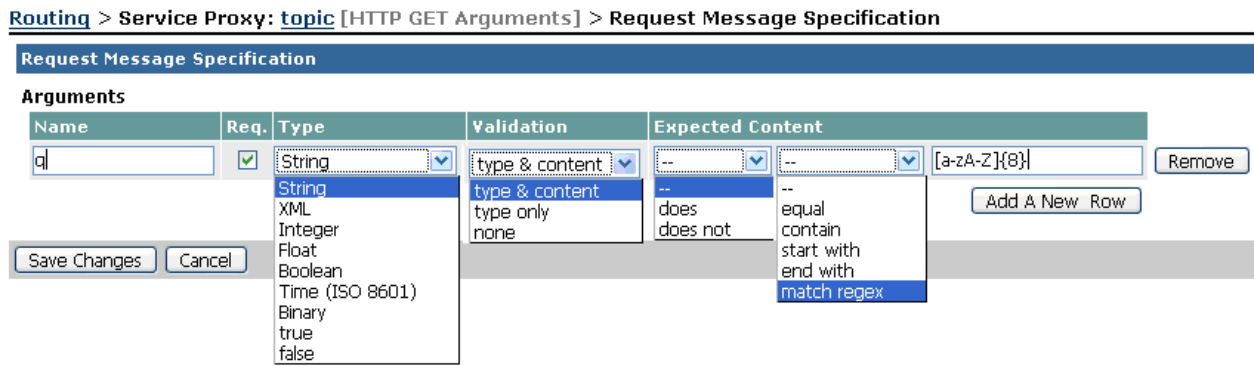
Figure D-44 Defining Policies Per Host



223749

Step 3 Define the acceptable range for each GET or POST query parameter. See [Figure D-45](#)

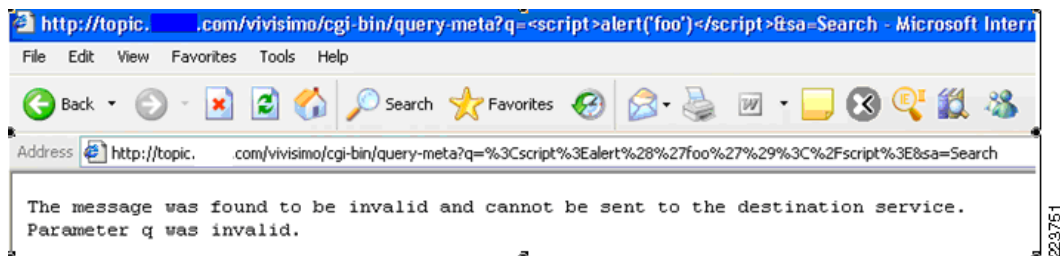
Figure D-45 Defining GET and POST Query Parameter



223750

Step 4 When the Cisco ACE XML Gateway receives a request, it can validate the message to ensure that only messages in the expected format reach the backend server. See [Figure D-46](#).

Figure D-46 Detection of Attack and Blocking



223751

Event log can be found under Reports and Tools section of the Cisco ACE XML Gateway (see Figure D-47).

Figure D-47 Event Log—Invalid Message

Event Log Viewer

Current Manager Event Logging alert, error, warning, notice, info, debug [edit]

Current ACE XML Gateway Event Logging alert, error, warning, notice, info, debug [edit]

During last hour

search events logged on -- all hosts -- for events of type alert, error, warning, notice

with message GUID

category (e.g., /policy/access)

component (e.g., core or console)

description

Display a maximum of 500 events per page [Update]

EVENT LOG SEARCH RESULTS AT JAN 10 2008 01:50:16 AM PST

First < Prev Displaying events 1 - 33 Next > (more recent events are shown at the top)

Time (PST)	Description	Message GUID	Host	Component	Category
Jan 10 2008 01:50:06.994 AM	w Exception during processing of message HTTP GET request for /vivismo/cgi-bin/query-meta from 171.69.141.65; problem type 'Invalid message', problem message 'Parameter q was invalid.'	45ABED2D00000C53C9FC720D44FFB8E7	dhcp-171-69-45-236	core	/policy/error

For more information on request message specification and configuration in the *Cisco ACE XML Gateway Configuration Guide* (v5.1), refer to the following URL:

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 6.5.6 Injection Flaws Injection)

Injection flaws, particularly structured query language (SQL) injection, are common in web applications. There are many types of injections: SQL, LDAP, Xpath, HTML, and XML. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. Attackers trick the interpreter into executing unintended commands via supplying specially crafted data. Injection flaws allow attackers to create, read, update, or delete any arbitrary data available to the application. In the worst case scenario, these flaws allow an attacker to completely compromise the applications and the underlying systems.

Environments Affected

All web application framework that use interpreters or invoke other processes are vulnerable to injection attacks. In the PCI lab environment, the attacker injects a “single quote” in a application (see Figure D-48). The user supplied data is interpreted by the application code as command and query or data. The application error message reveals the database structure as shown in Figure D-48.

Figure D-48 Injection Flaw Example

Report Selection

Search Conditions

Employee Name: ' (Single Quote)

Expense Report ID

Expense Report Date

Expense Submit Date

[Search]

Figure D-49 Application Error Message

```
SQL: [SELECT mex.expense_id, mex.expense_number, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag,
mr.random_review_flag, mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, decode(mex.expense_status, 'T', 1, 'P', 2, 'S', 3, 'A', 4, 'R', 5, 'X', 6, 7)
sortorder1, mr.receipt_status, sum(mrp.payment_amount), mc.currency_code FROM met_expenses mex, met_reviews mr, met_trips mt, met_payments mp,
met_countries mc WHERE mex.expense_id = mr.expense_id(+) AND mex.employee_id = 4700 AND mex.expense_id = mp.expense_id(+) AND
mex.effective_country_code = mc.country_code AND mex.trip_id = mt.trip_id(+) AND mex.expense_number = '' GROUP BY mex.expense_number,
mex.expense_id, mex.expense_status, mex.submit_date, mr.review_status, mt.trip_number, mr.policy_review_flag, mr.random_review_flag,
mr.review_list_review_flag, mex.receipt_status, mr.add_info_status, mr.receipt_status, mc.currency_code ORDER BY sortorder1, mex.submit_date DESC,
mex.expense_number DESC]
```

223754

Database Error.

Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications from XML and HTML-based SQL injection attacks. Limiting input to specific criteria, including restricting required characters/strings for SQL attacks, was demonstrated to prevent such attacks. All SQL injection attacks were manual and required custom configuration of the Cisco ACE XML Gateway application.

For more information on the Cisco ACE XML Gateway configuration (v5.1), refer to the following URL:
http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 6.5.7 Improper Error Handling

Applications can unintentionally leak information about their configurations, internal workings or violate privacy through a variety of application problems (see Figure D-50, for example). Applications can also leak internal state via how long they take to process certain operations or via different responses to different inputs, such as displaying the same error text with different error numbers. Web applications often leaks information about their internal state through detailed or debug error messages. Often, this information can be used to launch or even automate more powerful attacks.

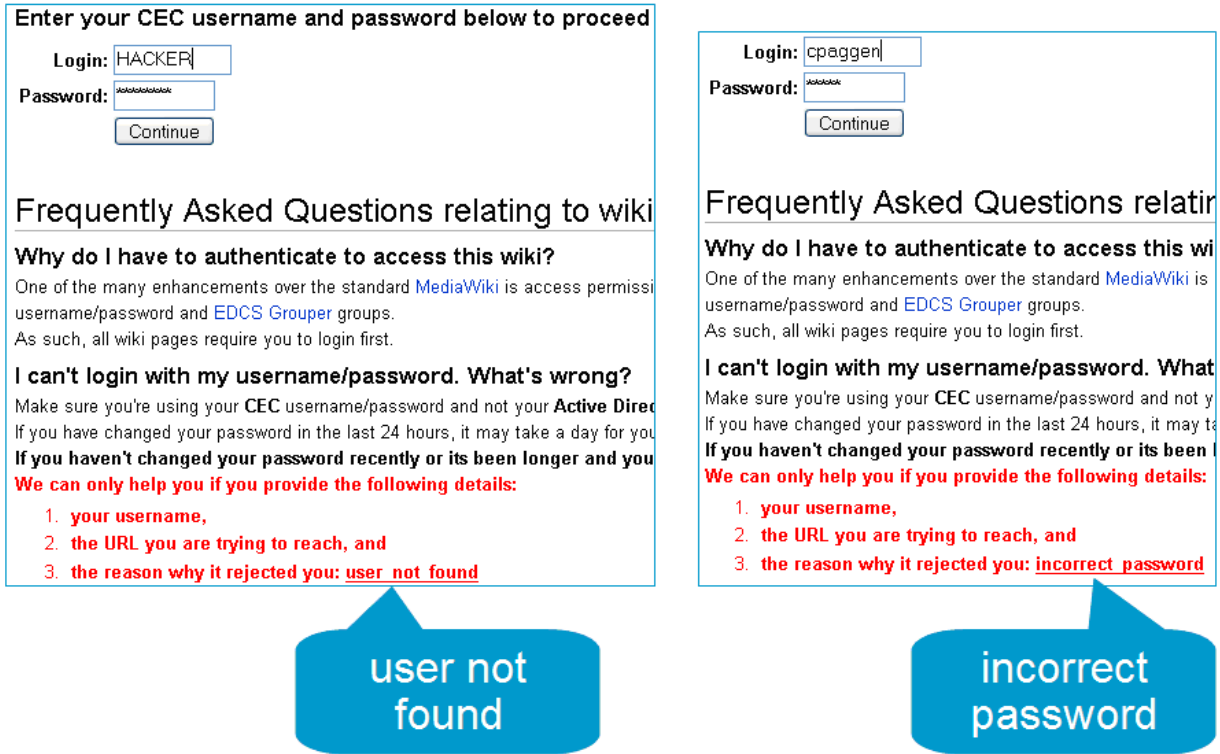
Environments Affected

All web applications framework are vulnerable to information leakage and improper error handling.

Implications

- Provides valuable information to hackers that enable them to launch an attack
- Divulges internal information

Figure D-50 Improper Handling Example



Mitigation

In the lab environment, Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications from XML and HTML-based error handling vulnerabilities. HTML/XML errors from the web server can be intercepted by the Cisco ACE XML Gateway and rewritten as a generic, non-descriptive error message. This was demonstrated during the review. All error handling attacks were manual and required custom configuration of the Cisco ACE XML Gateway application to prevent improper error handling.

223755

The AXG can return customized messages or page instead of standard HTTP return codes as shown in Figure D-51.

Figure D-51 Customized Message Configuration

Exception Mapping Defaults > Authentication or authorization failure

ACCESS ERROR: AUTHENTICATION OR AUTHORIZATION FAILURE

Map To Response Code: 403

Send With Content Type: text/html

Reason Phrase: That's not going to be possible

Message Body: I don't think I can let you do that, you know ...

In this message body, the ACE XML Gateway will replace any occurrences of %s with the internal error description.

Save Changes Cancel

223756

For improper error handling, the AXG can offer full regular expression-based search and replace functions for request and response. Figure D-52 shows how the response message was replaced with new string.

Figure D-52 Improper Error Handling Request

Address http://i.com/vivisimo/cgi-bin/query-meta?q=chakkingal&searchmode=basic

Topic Search

chakkingal Search Search within results

223757

A content screening rule is a regular expression that defines the content to be matched in the outgoing or incoming messages. The custom content screening rule can be accessed from policy portion of navigation menu (see [Figure D-53](#)).

Figure D-53 Custom Content Screening Rule

Content Screening Management > Custom Content Screening Rule

DESCRIPTION

Rule Name:

Description:

REGULAR EXPRESSION

Any messages that match this (POSIX-style) regular expression will immediately be **rejected**.

Regular Expression:

Use case-insensitive regular expression matching

RULE ACTIONS

Run this rule on requests responses HTTP headers

When a message contains one or more matches for this rule's regular expression:

Log this warning event:


Allow the message to continue being processed

Replace any matching string with

223758

Here the the string “Topic Search” was replaced with string “General Query” in the response message as shown in [Figure D-54](#).

Figure D-54 Improper Error Handling Response

Address  http://.../vivisimo/cgi-bin/query-meta?q=chakkingal&btnG=Search&searchmode=basic&searchmode=basic

General Query

223759

The associated event log generated by the replacement of “Topic Search” with string “General Query” is shown in [Figure D-55](#). The replacement activity was configured as “searchreplace” in the custom content screening rule.

Figure D-55 Event Log Search and Replace

Event Log Viewer

Current Manager Event Logging alert, error, warning, notice, info, debug [[edit](#)]

Current ACE XML Gateway Event Logging alert, error, warning, notice, info, debug [[edit](#)]

During time period: 2:18 AM 1/10/08 to 2:38 AM 1/10/08

search events logged on -- all hosts -- for events of type alert, error, warning, notice, info, debug

with message GUID 45ABED2D00000FAF633E0534753388F9|45ABED2D0000583EC4EEEE04952E

category (e.g., /policy/access)

component (e.g., core or console)

description

Display a maximum of 500 events per page [[Update](#)]

EVENT LOG SEARCH RESULTS AT JAN 10 2008 02:30:24 AM PST

[First] [< Prev] Displaying events 1 - 62 [Next >] (more recent events are shown at the top)

Time (PST)	Description	Message GUID
Jan 10 2008 02:28:08.301 AM	I Returning response 200 for request message to client; 59645 bytes	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.161 AM	D Received response for request message	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.158 AM	I Logging message at log level LOG_BRIEF_DEBUG [view logged message]	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.158 AM	D Added message to statistics	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.157 AM	D Sending HTTP response back to HTTP server	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.157 AM	D Regex 'Topic Search' failed on ' <HTML> <HEAD> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <TITLE>Vivisimo - Clustered search on chakkingal</TITLE> <style><!-- .expandstr {FONT-SIZE:smaller;} .expandword {FONT-SIZE:smaller} .s {FONT-SIZE:12px} body, td {FONT-FAMILY:Arial, Sans-serif;} a:link {COLOR:#0000EE;} a:hover, a:visited:hover {COLOR:#CC0000} a:visited {COLOR:#000099;} .tbody {BACKGROUND-COLOR:white; MARGIN: 3 0 0 2;} .treeintro {BACKGROUND:gold; COLOR:black; FONT-WEIGHT:bold;} .foldernum {COLOR:#0000EE; FONT-WEIGHT:bold; FONT-SIZE:smaller} .foldertd {PADDING:0 0 6 0} .folder {FONT-WEIGHT:bold;} a.treemore:link, a.treemore:visited {COLOR:orange;} .listbody {BACKGROUND-COLOR:white; MARGIN:3 0 0 2;} a:link {COLOR:#0000EE;} a:hover, a:visited:hover {COLOR:#CC0000} a:visited {COLOR:#000099;} .introquery, .introsources, .intronum, .intropath {FO	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.156 AM	I searchreplace	45ABED2D0000583EC4EEEE049528F159E
Jan 10 2008 02:28:08.156 AM	D Pattern found, replacing with 'General Query'	45ABED2D0000583EC4EEEE049528F159E

22:36:99

Event Log Viewer

Current Manager Event Logging alert, error, warning, notice, info, debug [edit]

Current ACE XML Gateway Event Logging alert, error, warning, notice, info, debug [edit]

During time period: 2:18 AM 1/10/08 to 2:38 AM 1/10/08

search events logged on -- all hosts -- for events of type alert, error, warning, notice, info, debug

with message GUID 45ABED2D00000FAF633E0534753388F9|45ABED2D00000583EC4EEE04952E

category (e.g., /policy/access)

component (e.g., core or console)

description

Display a maximum of 500 events per page [Update]

EVENT LOG SEARCH RESULTS AT JAN 10 2008 02:30:24 AM PST

First < Prev Displaying events 1 - 62 Next > (more recent events are shown at the top)

Time (PST)	Description	Message GUID
Jan 10 2008 02:28:08.301 AM	I Returning response 200 for request message to client; 59645 bytes	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.161 AM	D Received response for request message	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.158 AM	I Logging message at log level LOG_BRIEF_DEBUG [view logged message]	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.158 AM	D Added message to statistics	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.157 AM	D Sending HTTP response back to HTTP server	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.157 AM	D Regexp "Topic Search" failed on ' <HTML> <HEAD> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <TITLE> Vivismo - Clustered search on chakkingal</TITLE> <style> <!-- .expandstr {FONT-SIZE:smaller;} .expandword {FONT-SIZE:smaller} .s {FONT-SIZE:12px} body, td {FONT-FAMILY:Arial, Sans-serif;} a:link {COLOR:#0000EE;} a:hover, a:visited:hover {COLOR:#CC0000} a:visited {COLOR:#000099;} .treebody {BACKGROUND-COLOR:white; MARGIN: 3 0 0 2;} .treeintro {BACKGROUND:gold; COLOR:black; FONT-WEIGHT:bold;} .foldernum {COLOR:#0000EE; FONT-WEIGHT:bold; FONT-SIZE:smaller} .foldertd {PADDING:0 0 6 0} .folder {FONT-WEIGHT:bold;} a.treemore:link, a.treemore:visited {COLOR:orange;} .listbody {BACKGROUND-COLOR:white; MARGIN:3 0 0 2;} a:link {COLOR:#0000EE;} a:hover, a:visited:hover {COLOR:#CC0000} a:visited {COLOR:#000099;} .introquery, .introsources, .intronum, .intropath {FO	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.156 AM	I searchreplace	45ABED2D00000583EC4EEE04952BF159E
Jan 10 2008 02:28:08.156 AM	D Pattern found, replacing with 'General Query'	45ABED2D00000583EC4EEE04952BF159E

223760

For more information on Custom Content Screening Rule configuration, refer to the *Cisco ACE XML Gateway Configuration Guide (v5.1)* at the following URL:

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 6.5.9 Denial-of-Service

A denial-of-service attack (DoS attack) is an attempt to overwhelm a computer resource (possibly with malicious requests) with the goal of making that resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways and even DNS root servers.

Environments Affected

All web applications framework are vulnerable to information leakage and improper error handling.

Implications

- Service interruption
- Downtime
- Effect on brand reputation
- Lost revenue

Mitigation

In the lab environment, Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications against web-based DoS attacks. Limitations can be placed on sessions (e.g., session timeouts, number of concurrent sessions, etc) to reduce exposure to DoS attacks. The DoS protection can be

configured in AXG under ‘Global Security’ and “request throttling” can be configured under HTTP Servers (see Figure D-56 and Figure D-57).

Figure D-56 Denial-of-Service Attacks Protection

Denial-Of-Service Protection Settings

Enable Denial-of-Service Protection

ATTACK DETECTION THRESHOLDS

These settings describe the traffic allowed from any one IP address before that IP address is considered to be attacking the ACE XML Gateway.

Traffic/Attack Type	Detect Messages That:	Maximum Allowed Rate*	Maximum Allowed Burst
Overall Request Rate	n/a -- all requests are counted	60 requests/min	10 requests
Authentication Failures	n/a -- all failures are counted	12 failures/min	3 failures
CPU Usage	use > 250 ms CPU time	30 "detected" messages/min	5 "detected" messages
Internal Errors	n/a -- all errors are counted	30 errors/min	5 errors
Service Latency	cause > 1 sec of latency	30 "detected" messages/min	5 "detected" messages
Service Errors	n/a -- all errors are counted	30 errors/min	5 errors

*Maximum Allowed Rate of "0" disables detection for that attack

Note: Any attack detected will log an event at "warning" level, regardless of the "Attack Protection" setting below.

ATTACK PROTECTION

When an attack is detected, block the attacking IP address for at least 5 seconds
(actual time could be longer and is calculated based on the intensity of the attack)

Note: Changes will not take effect until the next time the policy is deployed.

223761

Figure D-57 Request Throttling

HTTP Servers > Example: Edit Request Throttling

REQUEST THROTTLING

Throttle the rate of requests to this server based on these upper bounds:

Request rate: 50 requests/second
Request burst: 15 requests at one time
Average request size: 1024 KB (larger sizes count as multiple requests)
Average latency: 30 seconds (larger latencies count as multiple requests)

Never send any request that is larger than 10240 KB

If the server returns code 503 (Server Busy), wait at least 60 seconds before sending another request.

223762

For more information on DoS attack protection, refer to “Working with HTTP Servers” in the *ACE XML Configuration Guide* (v5.1) at the following URL:

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

6.5.10 Insecure Configuration Management

Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications. Encryption (usually SSL) must be used for all authenticated connections, especially internet-accessible web pages, but backend connections as well. Otherwise, the application exposes an authentication or session token. In addition, encryption should be used whenever sensitive data, such as credit card is transmitted.

Environment s Affected

All web applications framework are vulnerable to information leakage and improper error handling.

Implications

- Eavesdropping
- Data manipulation
- Non-repudiation possible

Mitigation

In the lab environment, Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications against the following insecure configuration management area:

Required SSL (HTTPS) web sessions: ACE XML Gateway can be configured to force HTTPS sessions to prevent HTTP sessions that could contain sensitive information, including administrative credentials. [Figure D-58](#) shows snapshot of the SSL configuration.

Figure D-58 SSL Configuration

[HTTP Servers](#) > HacmeBank: Edit General Settings

GENERAL

Name:

Host:

Port: (usually 80 for HTTP, or 443 for HTTPS)

SSL: Encrypt connections with SSL

If requested, use client public/private keypair:

Require remote server certificate signed by this CA certificate:
(Choosing a CA certificate other than "none" will also require that the server hostname matches the subject CN of the server certificate.)

Require a certificate from the remote server that is identical to this certificate:

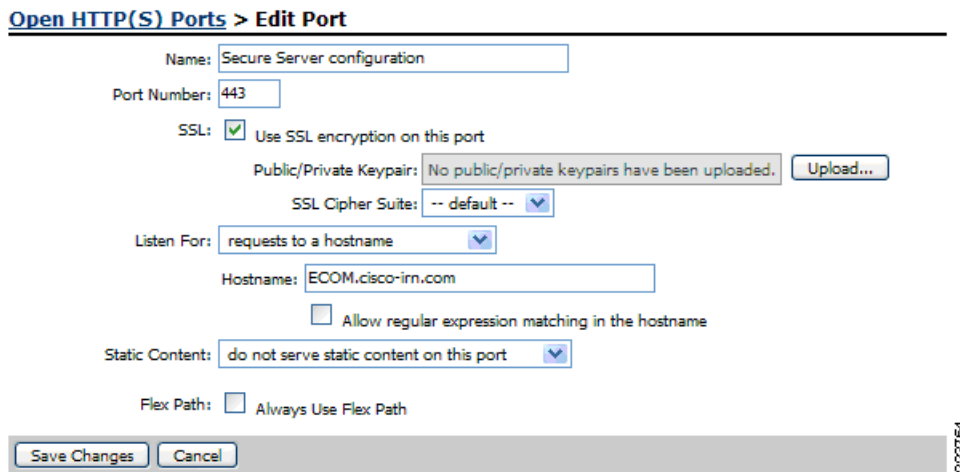
SSL Cipher Suite:

Flex Path: Always Use Flex Path

03/23/22

Figure D-59 shows snapshot of the SSL port configuration.

Figure D-59 SSL Port Configuration



PCI 6.5.5 Buffer Overflows

Attackers use buffer overflows to corrupt the execution stack of a web application. By sending carefully crafted input to a web application, an attacker can cause the web application to execute arbitrary code, effectively taking over the machine. Attackers have managed to identify buffer overflows in a staggering array of products and components. Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site, or the web application itself. Buffer overflows found in widely used server products are likely to become widely known and can pose a significant risk to users of these products. When web applications use libraries, such as a graphics library to generate images, they open themselves to potential buffer overflow attacks.

Environments Affected

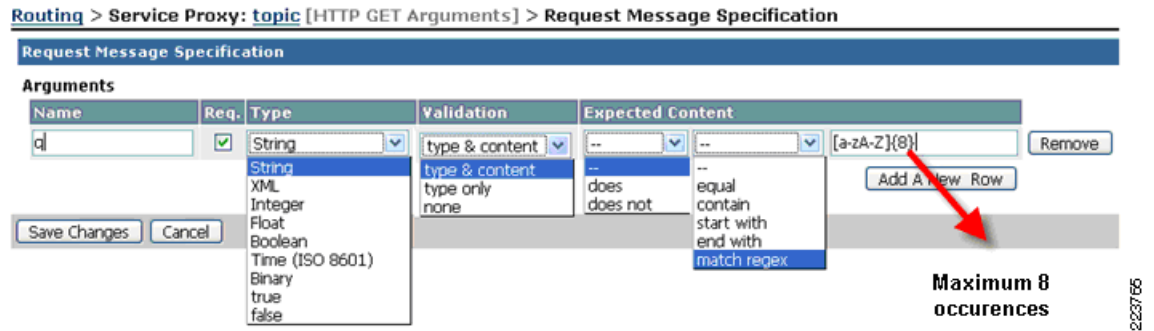
All web servers, application servers, and web applications are susceptible to buffer overflow.

Implications

- Access to operating systems
- Theft of files and passwords
- Ability to propagate viruses and worms in the operating systems

In the lab environment, Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications from XML and HTML-based buffer overflow attacks. URI handling (e.g., limit URI submission), field input validation, etc, was observed to prevent such attacks. All buffer overflow attacks were manual and required custom configuration of the Cisco ACE XML Gateway application. Figure D-60 shows imposing a length restrictions on the parameters prevents buffer overflow.

Figure D-60 Buffer Overflow—Length Restriction



PCI 6.5.1 Unvalidated Input

Web applications use input from HTTP requests (and occasionally files) to determine how to respond. Attackers can tamper with any part of an HTTP request, including the URL, query string, headers, cookies, form fields, and hidden fields, to try to bypass the site’s security mechanisms. Common names for common input tampering attacks include: forced browsing, command insertion, cross site scripting, buffer overflows, format string attacks, SQL injection, cookie poisoning, and hidden field manipulation. A surprising number of web applications use only client-side mechanisms to validate input. Client-side validation mechanisms are easily bypassed, leaving the web application without any protection against malicious parameters. Attackers can generate their own HTTP requests using tools as simple as Telnet. Server-side checks are required to defend against parameter manipulation attacks. Once these are in place, client side checking can also be included to enhance the user experience for legitimate users and/or reduce the amount of invalid traffic to the server.

Environments Affected

All web servers, application servers, and web applications are susceptible to parameter tampering.

In the lab environment, Verizon Business observed the use of the Cisco ACE XML Gateway to protect web applications from XML and HTML-based input validation attacks. All input validation attacks were manual and required custom configuration of the Cisco ACE XML Gateway application.

For unvalidated input examples, refer to cross-site scripting (PCI 6.5.4), buffer overflow (PCI 6.5.5) and Injection flaw (PCI 6.5.6) examples.

2/23/15



Device Configurations

This appendix includes the following device configurations:

- [Branch Configurations](#)
 - [Large Store Router #1, page E-2](#)
 - [Large Store Router #2, page E-15](#)
 - [Medium Store Router #1, page E-28](#)
 - [Medium Store Router #2, page E-41](#)
 - [Small Store Router #1, page E-52](#)
 - [Data Center WAN Router #1, page E-65](#)
 - [Data Center WAN Router #2, page E-70](#)
 - [Large Store Switch #1, page E-76](#)
 - [Large Store Switch #2, page E-83](#)
 - [Large Store Switch #3, page E-90](#)
 - [Large Store Switch #4, page E-96](#)
 - [Medium Store Switch #1, page E-103](#)
 - [Medium Store Switch #2, page E-109](#)
 - [Large Store Wireless Controller, page E-115](#)
 - [Medium Store Wireless Controller, page E-132](#)
 - [Small Store Wireless controller in the Data Center, page E-147](#)
 - [Large Store Access Point, page E-162](#)
 - [Medium Store Access Point, page E-163](#)
 - [Small Store Access Point, page E-164](#)
- [Internet Edge Configurations](#)
 - [Cisco Firewall Service Module, page E-165](#)
 - [Cisco Catalyst 3750, page E-171](#)
 - [Cisco Catalyst 6500, page E-176](#)
 - [Cisco 7200 Edge Router, page E-186](#)
 - [Cisco Application Control Engine, page E-192](#)
- [Data Center Configurations, page E-195](#)

- Cisco Catalyst 3750, page E-195
- Cisco Catalyst 6500, page E-198
- Cisco 7206 VXR Router, page E-200
- Cisco Adaptive Security Appliance, page E-205

Branch Configurations

Large Store Router #1

```
----- show version -----

Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 17-Jun-06 00:59 by prod_rel_team

ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)

RLRG-1 uptime is 11 weeks, 4 days, 3 hours, 7 minutes
System returned to ROM by reload at 18:34:08 UTC Mon Sep 25 2006
System restarted at 11:32:41 PST DST Mon Sep 25 2006
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 3845 (revision 1.0) with 484352K/39936K bytes of memory.
Processor board ID FTX1027A34V
 2 Gigabit Ethernet interfaces
 2 Serial interfaces
 1 terminal line
 2 Channelized T1/PRI ports
 1 Virtual Private Network (VPN) Module
 4 Voice FXO interfaces
 4 Voice FXS interfaces
 1 cisco service engine(s)
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
250880K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102
```

```
----- show running-config -----

Building configuration...

Current configuration : 28349 bytes
!
! Last configuration change at 15:59:42 PST Wed Dec 13 2006 by csm-user
! NVRAM config last updated at 14:27:43 PST Wed Dec 13 2006 by csm-user
!
version 12.4
no service pad
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RLRG-1
!
boot-start-marker
boot system flash flash:c3845-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
card type t1 0 0
logging buffered 8000000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PSTDST recurring
no network-clock-participate wic 0
!
!
ip cef
!
!
no ip bootp server
ip domain name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
ip inspect name CSM_INSPECT_1 http alert on audit-trail on
ip inspect name CSM_INSPECT_1 dns alert on audit-trail on
ip inspect name CSM_INSPECT_1 radius alert on audit-trail on
ip inspect name CSM_INSPECT_1 tacacs alert on audit-trail on
ip inspect name CSM_INSPECT_1 ssh alert on audit-trail on
ip inspect name CSM_INSPECT_1 ftp alert on audit-trail on
```



```

quit
crypto pki certificate chain IDSMDC_CSMANAGER
certificate ca 00CE88ED0F069AE8F5
 30820209 30820172 020900CE 88ED0F06 9AE8F530 0D06092A 864886F7 0D010104
05003049 31123010 06035504 0B13096D 6963726F 736F6674 31123010 06035504
03130943 534D616E 61676572 311F301D 06092A86 4886F70D 01090116 1061646D
696E4064 6F6D6169 6E2E636F 6D301E17 0D303630 39323330 31303235 345A170D
31313039 32333031 30323534 5A304931 12301006 0355040B 13096D69 63726F73
6F667431 12301006 03550403 13094353 4D616E61 67657231 1F301D06 092A8648
86F70D01 09011610 61646D69 6E40646F 6D61696E 2E636F6D 30819F30 0D06092A
864886F7 0D010101 05000381 8D003081 89028181 00BE596C 97AD25EC 35D71F77
598DDDB B8D30AAF 67B268D5 334EAB58 F7418364 664B920A E0011931 4EDF28D1
285B7C45 934EE887 00036A4A C0280132 88C48718 EF48F77E C9EBB27B 6FA11534
03B3B9CB 3DCEFCDC A1339BA4 22C8BFAD 47F50E51 AC04CD7A 03E81331 96BF4ACA
9A1CC2AD 3452AAEB FF84503C A571FB93 EC509A03 8B020301 0001300D 06092A86
4886F70D 01010405 00038181 003A2C37 FC8B0EF1 54E0B963 4D94C234 5EF94288
F6B0B46D 4EFECB7A D15991DE 05FE484E C9DB2AB8 A919DD2F 103545C4 EF7D9269
27975BAD 02CBDDA7 6492EC76 56845082 220A73D7 F9F60FA0 8E9EDDE8 5147E5EB
FB5A00E0 25872141 AA35FAC6 BEF300D9 97343B16 0600B102 F5D555F9 B8AA4D90
26E026CB 6F46B573 700207C8 71
quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 framing esf
 linecode b8zs
!
!
!
!
!
!
interface Tunnel1
 no ip address
 ip access-group CSM_FW_ACL_Group-Async0 in
!
interface Loopback0
 ip address 10.10.62.1 255.255.255.255
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip virtual-reassembly
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SLRG-1
 no ip address
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.48.2 255.255.255.0
 ip access-group CSM_FW_ACL_GigabitEthernet0/0.11 in
 ip verify unicast source reachable-via rx
 ip helper-address 192.168.42.130
 ip inspect CSM_INSPECT_1 in

```

```

ip virtual-reassembly
standby 11 ip 10.10.48.1
standby 11 priority 101
standby 11 preempt
!
interface GigabitEthernet0/0.12
description DATA
encapsulation dot1Q 12
ip address 10.10.49.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.12 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 12 ip 10.10.49.1
standby 12 priority 101
standby 12 preempt
!
interface GigabitEthernet0/0.13
description VOICE
encapsulation dot1Q 13
ip address 10.10.50.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.13 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 13 ip 10.10.50.1
standby 13 priority 101
standby 13 preempt
!
interface GigabitEthernet0/0.14
description WIRELESS
encapsulation dot1Q 14
ip address 10.10.51.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.14 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 14 ip 10.10.51.1
standby 14 priority 101
standby 14 preempt
!
interface GigabitEthernet0/0.15
description WIRELESS POS
encapsulation dot1Q 15
ip address 10.10.52.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.15 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 15 ip 10.10.52.1
standby 15 priority 101
standby 15 preempt
!
interface GigabitEthernet0/0.16
description PARTNER
encapsulation dot1Q 16
ip address 10.10.53.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.16 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130

```



```
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 16 ip 10.10.53.1
standby 16 priority 101
standby 16 preempt
!
interface GigabitEthernet0/0.17
description WIRELESS GUEST
encapsulation dot1Q 17
ip address 10.10.54.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.17 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 17 ip 10.10.54.1
standby 17 priority 101
standby 17 preempt
!
interface GigabitEthernet0/0.18
description LWAP CONTROL
encapsulation dot1Q 18
ip address 10.10.55.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.18 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 18 ip 10.10.55.1
standby 18 priority 101
standby 18 preempt
!
interface GigabitEthernet0/0.102
description ROUTER LINK TO RLRG-2 VIA SLRG-2
encapsulation dot1Q 102
ip address 10.10.62.29 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface GigabitEthernet0/0.1000
description MANAGEMENT
encapsulation dot1Q 1000
ip address 10.10.63.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.1000 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 100 ip 10.10.63.1
standby 100 priority 101
standby 100 preempt
!
interface Service-Engine0/1
no ip address
ip access-group CSM_FW_ACL_Group-Async0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
shutdown
!
interface GigabitEthernet0/1
description ROUTER LINK TO SLRG-2
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
```

```

ip verify unicast source reachable-via rx
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RLRG-2 VIA SLRG-2
encapsulation dot1Q 101
ip address 10.10.62.25 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Serial0/0/0:0
description RLRG-1 to RSP-1
no ip address
ip access-group CSM_FW_ACL_Group-Async0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface Serial0/0/0:0.1 point-to-point
ip address 10.10.62.17 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
frame-relay interface-dlci 103
!
interface Group-Async0
physical-layer async
no ip address
ip access-group CSM_FW_ACL_Group-Async0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation slip
no group-range
!
router ospf 5
router-id 10.10.62.1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0.102
no passive-interface GigabitEthernet0/1.101
no passive-interface Serial0/0/0:0.1
network 10.10.48.0 0.0.15.255 area 3
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp

```

```

permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.1000
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- Ciscoworks so Managed Devices ----
permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Allow network devices to use the ACS server ----
permit tcp any host 192.168.42.131 eq tacacs log
permit udp any host 192.168.42.131 eq 1812 log
remark ---- ping to Datacenter ----
permit icmp any 192.168.42.0 0.0.0.255 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.63.0 0.0.0.255 10.10.63.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.102
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- Trusted ports for passing traffic in failure scenarios ----
permit ip any any log
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark Drop anything not explicitly allowed
deny ip any any log
remark ---- permit ntp ----
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.48.0 0.0.0.255 10.10.48.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log

```

```

permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.12
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.49.0 0.0.0.255 10.10.49.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.13
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.50.0 0.0.0.255 10.10.50.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp

```

```

remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.51.0 0.0.0.255 10.10.51.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.15
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.52.0 0.0.0.255 10.10.52.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.16
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.53.0 0.0.0.255 10.10.53.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log

```

```

ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.17
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.54.0 0.0.0.255 10.10.54.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.18
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Authenticate Wireless users ----
permit udp host 10.10.55.5 host 192.168.42.131 eq 1812 log
permit udp host 10.10.55.6 host 192.168.42.131 eq 1812 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.55.0 0.0.0.255 10.10.55.0 0.0.0.255 log
remark ---- Ping Gateway ----
remark ---- Allow controllers to talk to AP's ----
permit udp 10.10.55.0 0.0.0.255 eq 12222 12223 10.10.55.0 0.0.0.255 log
remark ---- Allow Wireless APs to talk to Controllers ----
permit udp 10.10.55.0 0.0.0.255 10.10.55.0 0.0.0.255 eq 12222 12223 log
remark ---- Controllers to WCS Server ----
permit icmp host 10.10.55.5 host 192.168.42.135 log
permit tcp host 10.10.55.5 host 192.168.42.135 eq 69 log
permit udp host 10.10.55.5 host 192.168.42.135 eq tftp snmp snmptrap log
permit icmp host 10.10.55.6 host 192.168.42.135 log
permit tcp host 10.10.55.6 host 192.168.42.135 eq 69 log
permit udp host 10.10.55.6 host 192.168.42.135 eq tftp snmp snmptrap log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Group-Async0
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0.1
remark ---- All ACLs for DC to Remote will be handled at the Data Center *before* it gets
put into the WAN

```

```

permit ip any any log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.1 log
permit tcp host 192.168.42.133 host 10.10.62.1 eq 22 443 log
remark Drop anything not explicitly allowed
deny ip any any log
!
logging source-interface Loopback0
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact bob
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.134 <removed>
!
!
!
!
!
tacacs-server host 192.168.42.131
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
control-plane
!
!
!
voice-port 0/1/0
!
voice-port 0/1/1
!
voice-port 0/1/2
!
voice-port 0/1/3
!
voice-port 0/2/0
!
voice-port 0/2/1
!
voice-port 0/2/2
!
voice-port 0/2/3
!
!
!

```

```

!
!
!
!
!
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO INC.****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO INC.****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  session-timeout 15  output
  exec-timeout 15 0
  privilege level 15
  login authentication RLOCAL
  stopbits 1
line aux 0
  session-timeout 15  output
  no exec
  stopbits 1
line 386
  session-timeout 15  output
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL

```



```
transport input ssh
line vty 5 15
  session-timeout 15 output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179470
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
End
```

Large Store Router #2

----- show version -----

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 17-Jun-06 00:59 by prod_rel_team
```

```
ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)
```

```
RLRG-2 uptime is 4 weeks, 2 days, 20 hours, 34 minutes
System returned to ROM by error - a Software forced crash, PC 0x60D718F0 at 17:04:41 PST
Tue Nov 14 2006
System restarted at 17:12:53 PST Tue Nov 14 2006
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco 3845 (revision 1.0) with 484352K/39936K bytes of memory.
Processor board ID FTX1027A34T
2 Gigabit Ethernet interfaces
2 Serial interfaces
1 ATM interface
1 terminal line
2 Channelized T1/PRI ports
1 Virtual Private Network (VPN) Module
1 cisco service engine(s)
DRAM configuration is 64 bits wide with parity enabled.
```

479K bytes of NVRAM.
 250880K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102

----- show running-config -----

Building configuration...

```

Current configuration : 27883 bytes
!
! Last configuration change at 16:06:29 PST Wed Dec 13 2006 by csm-user
! NVRAM config last updated at 14:34:40 PST Wed Dec 13 2006 by csm-user
!
version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RLRG-2
!
boot-start-marker
boot system flash flash:c3845-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
card type t1 0 0
logging buffered 8000000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PSTDST recurring
no network-clock-participate wic 0
!
!
ip cef
!
!
ip domain name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
ip inspect name CSM_INSPECT_1 http alert on audit-trail on
ip inspect name CSM_INSPECT_1 dns alert on audit-trail on
ip inspect name CSM_INSPECT_1 radius alert on audit-trail on
    
```



```

BC721185 3F47BB2D 71957001 C062AC30 EB9D523A 4FC7AE6F 55D18936 2076B539
DB88FADD 452D03C9 EFC6E22D 43494798 E840AA7C 2C60DCDD EB03954C 79B7DE7C
A6F522AA DFEEFA51 10C2D3CE 9190FA15 0F4A8C06 9C
quit
crypto pki certificate chain IDSMDC_CSMANAGER
certificate ca 00CE88ED0F069AE8F5
 30820209 30820172 020900CE 88ED0F06 9AE8F530 0D06092A 864886F7 0D010104
05003049 31123010 06035504 0B13096D 6963726F 736F6674 31123010 06035504
03130943 534D616E 61676572 311F301D 06092A86 4886F70D 01090116 1061646D
696E4064 6F6D6169 6E2E636F 6D301E17 0D303630 39323330 31303235 345A170D
31313039 32333031 30323534 5A304931 12301006 0355040B 13096D69 63726F73
6F667431 12301006 03550403 13094353 4D616E61 67657231 1F301D06 092A8648
86F70D01 09011610 61646D69 6E40646F 6D61696E 2E636F6D 30819F30 0D06092A
864886F7 0D010101 05000381 8D003081 89028181 00BE596C 97AD25EC 35D71F77
598DDDD8 B8D30AAF 67B268D5 334EAB58 F7418364 664B920A E0011931 4EDF28D1
285B7C45 934EE887 00036A4A C0280132 88C48718 EF48F77E C9EBB27B 6FA11534
03B3B9CB 3DCEFCDC A1339BA4 22C8BFAD 47F50E51 AC04CD7A 03E81331 96BF4ACA
9A1CC2AD 3452AAEB FF84503C A571FB93 EC509A03 8B020301 0001300D 06092A86
4886F70D 01010405 00038181 003A2C37 FC8B0EF1 54E0B963 4D94C234 5EF94288
F6B0B46D 4EFECB7A D15991DE 05FE484E C9DB2AB8 A919DD2F 103545C4 EF7D9269
27975BAD 02CBDDA7 6492EC76 56845082 220A73D7 F9F60FA0 8E9EDDE8 5147E5EB
FB5A00E0 25872141 AA35FAC6 BEF300D9 97343B16 0600B102 F5D555F9 B8AA4D90
26E026CB 6F46B573 700207C8 71
quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 framing esf
 linecode b8zs
!
!
!
!
!
interface Loopback0
 ip address 10.10.62.2 255.255.255.255
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip inspect CSM_INSPECT_1 in
 ip virtual-reassembly
!
interface GigabitEthernet0/0
 description ROUTER LINK TO SLRG-1
 no ip address
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.102
 description ROUTER LINK TO RLRG-1 VIA SLRG-1
 encapsulation dot1Q 102
 ip address 10.10.62.30 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
 ip verify unicast source reachable-via rx
 ip inspect CSM_INSPECT_1 in
 ip virtual-reassembly

```

```
!  
interface Service-Engine0/1  
  no ip address  
  ip access-group CSM_FW_ACL_Serial0/0/0:0 in  
  ip verify unicast source reachable-via rx  
  ip virtual-reassembly  
  shutdown  
!  
interface GigabitEthernet0/1  
  description ROUTER LINK TO SLRG-2  
  no ip address  
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in  
  ip verify unicast source reachable-via rx  
  duplex auto  
  speed auto  
  media-type rj45  
!  
interface GigabitEthernet0/1.11  
  description POS  
  encapsulation dot1Q 11  
  ip address 10.10.48.3 255.255.255.0  
  ip access-group CSM_FW_ACL_GigabitEthernet0/1.11 in  
  ip verify unicast source reachable-via rx  
  ip helper-address 192.168.42.130  
  ip inspect CSM_INSPECT_1 in  
  ip virtual-reassembly  
  standby 11 ip 10.10.48.1  
  standby 11 priority 95  
  standby 11 preempt  
!  
interface GigabitEthernet0/1.12  
  description DATA  
  encapsulation dot1Q 12  
  ip address 10.10.49.3 255.255.255.0  
  ip access-group CSM_FW_ACL_GigabitEthernet0/1.12 in  
  ip verify unicast source reachable-via rx  
  ip helper-address 192.168.42.130  
  ip inspect CSM_INSPECT_1 in  
  ip virtual-reassembly  
  standby 12 ip 10.10.49.1  
  standby 12 priority 95  
  standby 12 preempt  
!  
interface GigabitEthernet0/1.13  
  description VOICE  
  encapsulation dot1Q 13  
  ip address 10.10.50.3 255.255.255.0  
  ip access-group CSM_FW_ACL_GigabitEthernet0/1.13 in  
  ip verify unicast source reachable-via rx  
  ip helper-address 192.168.42.130  
  ip inspect CSM_INSPECT_1 in  
  ip virtual-reassembly  
  standby 13 ip 10.10.50.1  
  standby 13 priority 95  
  standby 13 preempt  
!  
interface GigabitEthernet0/1.14  
  description WIRELESS  
  encapsulation dot1Q 14  
  ip address 10.10.51.3 255.255.255.0  
  ip access-group CSM_FW_ACL_GigabitEthernet0/1.14 in  
  ip verify unicast source reachable-via rx  
  ip helper-address 192.168.42.130  
  ip inspect CSM_INSPECT_1 in
```

```

ip virtual-reassembly
standby 14 ip 10.10.51.1
standby 14 priority 95
standby 14 preempt
!
interface GigabitEthernet0/1.15
description WIRELESS POS
encapsulation dot1Q 15
ip address 10.10.52.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.15 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 15 ip 10.10.52.1
standby 15 priority 95
standby 15 preempt
!
interface GigabitEthernet0/1.16
description PARTNER
encapsulation dot1Q 16
ip address 10.10.53.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.16 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 16 ip 10.10.53.1
standby 16 priority 95
standby 16 preempt
!
interface GigabitEthernet0/1.17
description WIRELESS GUEST
encapsulation dot1Q 17
ip address 10.10.54.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.17 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 17 ip 10.10.54.1
standby 17 priority 95
standby 17 preempt
!
interface GigabitEthernet0/1.18
description LWAP CONTROL
encapsulation dot1Q 18
ip address 10.10.55.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.18 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 18 ip 10.10.55.1
standby 18 priority 95
standby 18 preempt
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RLRG-1 VIA SLRG-1
encapsulation dot1Q 101
ip address 10.10.62.26 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in

```

```

ip virtual-reassembly
!
interface GigabitEthernet0/1.1000
description MANAGEMENT
encapsulation dot1Q 1000
ip address 10.10.63.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.1000 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 100 ip 10.10.63.1
standby 100 priority 95
standby 100 preempt
!
interface Serial0/0/0:0
description RLRG-2 to RSP-2
no ip address
ip access-group CSM_FW_ACL_Serial0/0/0:0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface Serial0/0/0:0.1 point-to-point
ip address 10.10.62.21 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
ip ospf cost 5000
frame-relay interface-dlci 203
!
interface ATM0/1/0
no ip address
shutdown
no atm ilmi-keepalive
dsl operating-mode auto
!
router ospf 5
router-id 10.10.62.2
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0.102
no passive-interface GigabitEthernet0/1.101
no passive-interface Serial0/0/0:0.1
network 10.10.48.0 0.0.15.255 area 3
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp

```

```

remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.102
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- Trusted ports for passing traffic in failure scenarios ----
permit ip any any log
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark Drop anything not explicitly allowed
deny ip any any log
remark ---- permit ntp ----
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.1000
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- Ciscoworks so Managed Devices ----
permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Allow network devices to use the ACS server ----
permit tcp any host 192.168.42.131 eq tacacs log
permit udp any host 192.168.42.131 eq 1812 log
remark ---- ping to Datacenter ----
permit icmp any 192.168.42.0 0.0.0.255 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.63.0 0.0.0.255 10.10.63.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.48.0 0.0.0.255 10.10.48.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log

```



```

permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.12
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.49.0 0.0.0.255 10.10.49.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.13
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.50.0 0.0.0.255 10.10.50.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log

```

```

remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.51.0 0.0.0.255 10.10.51.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.15
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.52.0 0.0.0.255 10.10.52.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.16
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.53.0 0.0.0.255 10.10.53.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.17
remark Allow CSM-Server to access device through the Serial (external) Interface

```

```

permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.54.0 0.0.0.255 10.10.54.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.18
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Authenticate Wireless users ----
permit udp host 10.10.55.5 host 192.168.42.131 eq 1812 log
permit udp host 10.10.55.6 host 192.168.42.131 eq 1812 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.55.0 0.0.0.255 10.10.55.0 0.0.0.255 log
remark ---- Ping Gateway ----
remark ---- Allow controllers to talk to AP's ----
permit udp 10.10.55.0 0.0.0.255 eq 12222 12223 10.10.55.0 0.0.0.255 log
remark ---- Allow Wireless APs to talk to Controllers ----
permit udp 10.10.55.0 0.0.0.255 10.10.55.0 0.0.0.255 eq 12222 12223 log
remark ---- Controllers to WCS Server ----
permit icmp host 10.10.55.5 host 192.168.42.135 log
permit tcp host 10.10.55.5 host 192.168.42.135 eq 69 log
permit udp host 10.10.55.5 host 192.168.42.135 eq tftp snmp snmptrap log
permit icmp host 10.10.55.6 host 192.168.42.135 log
permit tcp host 10.10.55.6 host 192.168.42.135 eq 69 log
permit udp host 10.10.55.6 host 192.168.42.135 eq tftp snmp snmptrap log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.62.2 log
permit tcp host 192.168.42.133 host 10.10.62.2 eq 22 443 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0.1
remark ---- All ACLs for DC to Remote will be handled at the Data Center *before* it gets
put into the WAN
permit ip any any log
remark Allow CSM-Server to access device through the Serial (external) Interface

```



```
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO INC.****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
    session-timeout 15  output
    exec-timeout 15 0
    privilege level 15
    login authentication RLOCAL
    stopbits 1
line aux 0
    session-timeout 15  output
    no exec
    stopbits 1
line 386
    session-timeout 15  output
    no activation-character
    no exec
    transport preferred none
    transport input all
    transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
    session-timeout 15  output
    exec-timeout 15 0
    logging synchronous
    login authentication RETAIL
    transport input ssh
line vty 5 15
    session-timeout 15  output
    exec-timeout 15 0
    logging synchronous
    login authentication RETAIL
    transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179777
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
End
```

Medium Store Router #1

```
----- show version -----  
  
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE  
SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Sat 17-Jun-06 00:59 by prod_rel_team
```

```
ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)
```

```
RMED-1 uptime is 1 week, 3 days, 21 hours, 17 minutes  
System returned to ROM by reload at 16:25:12 PST Mon Dec 4 2006  
System restarted at 16:25:54 PST Mon Dec 4 2006  
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco 3845 (revision 1.0) with 485376K/38912K bytes of memory.  
Processor board ID FTX1027A08Q  
2 Gigabit Ethernet interfaces  
4 Serial interfaces  
2 terminal lines  
2 Channelized T1/PRI ports  
1 Virtual Private Network (VPN) Module  
4 Voice FXO interfaces  
2 Voice FXS interfaces  
1 cisco content engine(s)  
1 cisco Wireless LAN Controller(s)  
DRAM configuration is 64 bits wide with parity enabled.  
479K bytes of NVRAM.  
125440K bytes of ATA System CompactFlash (Read/Write)
```

```
Configuration register is 0x2102
```

```
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 29725 bytes  
!  
! Last configuration change at 16:06:34 PST Wed Dec 13 2006 by csm-user  
! NVRAM config last updated at 14:34:35 PST Wed Dec 13 2006 by csm-user  
!  
version 12.4  
no service pad
```

```

service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RMED-1
!
boot-start-marker
boot system flash flash:c3845-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
logging buffered 8000000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PSTDST recurring
no network-clock-participate wic 0
!
!
ip cef
!
!
ip domain name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
ip inspect name CSM_INSPECT_1 http alert on audit-trail on
ip inspect name CSM_INSPECT_1 dns alert on audit-trail on
ip inspect name CSM_INSPECT_1 radius alert on audit-trail on
ip inspect name CSM_INSPECT_1 tacacs alert on audit-trail on
ip inspect name CSM_INSPECT_1 ssh alert on audit-trail on
ip inspect name CSM_INSPECT_1 ftp alert on audit-trail on
ip inspect name CSM_INSPECT_1 ldap alert on audit-trail on
ip inspect name CSM_INSPECT_1 snmp alert on audit-trail on
ip inspect name CSM_INSPECT_1 icmp alert on audit-trail on
ip inspect name CSM_INSPECT_1 tcp alert on audit-trail on
ip inspect name CSM_INSPECT_1 udp alert on audit-trail on
ip ips sdf location
https://192.168.42.133:443/ids-config/servlet/com.cisco.nm.mdc.ids.config.iosids.servlet.S
DFServlet/7/sdf-complete.xml
ip ips notify SDEE
ip ips name MediumStore list 23
ip ips name sdm_ips_rule
!
!
voice-card 0
no dspfarm
!

```



```

4886F70D 01010405 00038181 003A2C37 FC8B0EF1 54E0B963 4D94C234 5EF94288
F6B0B46D 4EFECB7A D15991DE 05FE484E C9DB2AB8 A919DD2F 103545C4 EF7D9269
27975BAD 02CBDDA7 6492EC76 56845082 220A73D7 F9F60FA0 8E9EDDE8 5147E5EB
FB5A00E0 25872141 AA35FAC6 BEF300D9 97343B16 0600B102 F5D555F9 B8AA4D90
26E026CB 6F46B573 700207C8 71
quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
!
!
!
!
!
interface Tunnel1
 no ip address
 ip access-group CSM_FW_ACL_Content-Engine3/0 in
!
interface Loopback0
 ip address 10.10.46.1 255.255.255.255
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip inspect CSM_INSPECT_1 in
 ip virtual-reassembly
!
interface GigabitEthernet0/0
 no ip address
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.11
 description POS
 encapsulation dot1Q 11
 ip address 10.10.32.2 255.255.255.0
 ip access-group CSM_FW_ACL_GigabitEthernet0/0.11 in
 ip verify unicast source reachable-via rx
 ip helper-address 192.168.42.130
 ip inspect CSM_INSPECT_1 in
 standby 11 ip 10.10.32.1
 standby 11 priority 101
 standby 11 preempt
!
interface GigabitEthernet0/0.12
 description DATA
 encapsulation dot1Q 12
 ip address 10.10.33.2 255.255.255.0
 ip access-group CSM_FW_ACL_GigabitEthernet0/0.12 in
 ip verify unicast source reachable-via rx
 ip helper-address 192.168.42.130
 ip inspect CSM_INSPECT_1 in
 ip virtual-reassembly
 standby 12 ip 10.10.33.1

```

```

standby 12 priority 101
standby 12 preempt
!
interface GigabitEthernet0/0.13
description VOICE
encapsulation dot1Q 13
ip address 10.10.34.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.13 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 13 ip 10.10.34.1
standby 13 priority 101
standby 13 preempt
!
interface GigabitEthernet0/0.14
description WIRELESS
ip address 10.10.35.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.14 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
shutdown
!
interface GigabitEthernet0/0.15
description WIRELESS POS
ip address 10.10.36.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.15 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
shutdown
!
interface GigabitEthernet0/0.16
description PARTNER
encapsulation dot1Q 16
ip address 10.10.37.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.16 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 16 ip 10.10.37.1
standby 16 priority 101
standby 16 preempt
!
interface GigabitEthernet0/0.17
description WIRELESS GUEST
ip address 10.10.38.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.17 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
shutdown
!
interface GigabitEthernet0/0.18
description LWAP CONTROL
encapsulation dot1Q 18
ip address 10.10.39.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.18 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in

```

```
ip virtual-reassembly
standby 18 ip 10.10.39.1
standby 18 priority 101
standby 18 preempt
!
interface GigabitEthernet0/0.102
description ROUTER LINK TO RMED2 VIA SMED2
encapsulation dot1Q 102
ip address 10.10.46.29 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface GigabitEthernet0/0.1000
description MANAGEMENT
encapsulation dot1Q 1000
ip address 10.10.47.2 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.1000 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 100 ip 10.10.47.1
standby 100 priority 101
standby 100 preempt
!
interface GigabitEthernet0/1
description ROUTER LINK TO SMED-2
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RMED-2
encapsulation dot1Q 101
ip address 10.10.46.25 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
ip ospf cost 200
!
interface Serial0/0/0:0
description RMED-1 to RSP-1
no ip address
ip access-group CSM_FW_ACL_Content-Engine3/0 in
ip verify unicast source reachable-via rx
encapsulation frame-relay IETF
!
interface Serial0/0/0:0.1 point-to-point
description CONNECTION TO RWAN-1
ip address 10.10.46.17 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
frame-relay interface-dlci 102
!
interface Serial0/0/1:0
no ip address
```

```

ip access-group CSM_FW_ACL_Content-Engine3/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface wlan-controller1/0
ip address 10.10.46.33 255.255.255.248
ip access-group CSM_FW_ACL_wlan-controller1/0 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface wlan-controller1/0.14
encapsulation dot1Q 14
ip address 10.10.35.1 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.14 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface wlan-controller1/0.15
encapsulation dot1Q 15
ip address 10.10.36.1 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.15 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface wlan-controller1/0.17
encapsulation dot1Q 17
ip address 10.10.38.1 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/0.17 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Content-Engine3/0
no ip address
ip access-group CSM_FW_ACL_Content-Engine3/0 in
ip verify unicast source reachable-via rx
shutdown
!
interface Group-Async0
physical-layer async
no ip address
ip access-group CSM_FW_ACL_Content-Engine3/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation slip
no group-range
!
router ospf 5
router-id 10.10.46.1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0.102
no passive-interface GigabitEthernet0/1.101
no passive-interface Serial0/0/0:0.1
network 10.10.32.0 0.0.15.255 area 2
!
!
!
no ip http server
ip http access-class 23

```

```

ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_Content-Engine3/0
 remark Allow CSM-Server to access device through the Serial (external) Interface
 permit icmp host 192.168.42.133 host 10.10.46.1 log
 permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
 remark Drop anything not explicitly allowed
 deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
 remark Allow CSM-Server to access device through the Serial (external) Interface
 permit icmp host 192.168.42.133 host 10.10.46.1 log
 permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
 remark ---- permit ntp ----
 permit udp any host 192.168.62.161 eq ntp
 permit udp any host 192.168.62.162 eq ntp
 permit udp any host 192.168.42.130 eq ntp
 remark Drop anything not explicitly allowed
 deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.1000
 remark Allow CSM-Server to access device through the Serial (external) Interface
 permit icmp host 192.168.42.133 host 10.10.46.1 log
 permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
 remark ---- permit ntp ----
 permit udp any host 192.168.62.161 eq ntp
 permit udp any host 192.168.62.162 eq ntp
 permit udp any host 192.168.42.130 eq ntp
 remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
 permit tcp any host 192.168.42.134 eq 69 log
 permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
 remark ---- Ciscoworks so Managed Devices ----
 permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
 permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
 remark ---- System messages to MARS ----
 permit tcp any host 192.168.42.121 eq 2055 log
 permit udp any host 192.168.42.121 eq snmp syslog log
 remark ---- Allow network devices to use the ACS server ----
 permit tcp any host 192.168.42.131 eq tacacs log
 permit udp any host 192.168.42.131 eq 1812 log
 remark ---- ping to Datacenter ----
 permit icmp any 192.168.42.0 0.0.0.255 log
 remark ---- HSRP health information ----
 permit udp any host 224.0.0.2 eq 1985 log
 remark ---- Ping Gateway ----
 permit icmp 10.10.47.0 0.0.0.255 10.10.47.0 0.0.0.255 log
 remark ---- Allow DHCP to work ----
 permit udp any host 255.255.255.255 eq bootps log
 permit udp any host 192.168.42.130 eq bootps log
 remark Drop anything not explicitly allowed
 deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.102
 remark ---- permit ntp ----
 permit udp any host 192.168.62.161 eq ntp
 remark Allow CSM-Server to access device through the Serial (external) Interface
 permit icmp host 192.168.42.133 host 10.10.46.1 log
 permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
 remark ---- Trusted ports for passing traffic in failure scenarios ----
 permit ip any any log
 permit udp any host 192.168.62.162 eq ntp
 permit udp any host 192.168.42.130 eq ntp
 remark Drop anything not explicitly allowed
 deny ip any any log

```

```

remark ---- permit ntp ----
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.32.0 0.0.0.255 10.10.32.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.12
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.33.0 0.0.0.255 10.10.33.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.13
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----

```

```

permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.34.0 0.0.0.255 10.10.34.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.35.0 0.0.0.255 10.10.35.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.15
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.36.0 0.0.0.255 10.10.36.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log

```

```

permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.16
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.37.0 0.0.0.255 10.10.37.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.17
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.38.0 0.0.0.255 10.10.38.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.18
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Authenticate Wireless users ----
permit udp host 10.10.46.34 host 192.168.42.131 eq 1812 log
permit udp host 10.10.46.35 host 192.168.42.131 eq 1812 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.39.0 0.0.0.255 10.10.39.0 0.0.0.255 log
remark ---- Allow Wireless APs to talk to Controllers ----
permit icmp 10.10.39.0 0.0.0.255 10.10.46.32 0.0.0.7 log
permit udp 10.10.39.0 0.0.0.255 10.10.46.32 0.0.0.7 eq 12222 12223 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0.1
remark ---- All ACLs for DC to Remote will be handled at the Data Center *before* it gets
put into the WAN
permit ip any any log

```



```

remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_wlan-controller1/0
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.1 log
permit tcp host 192.168.42.133 host 10.10.46.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.46.32 0.0.0.7 10.10.46.32 0.0.0.7 log
remark ---- Allow controllers to talk to AP's ----
permit icmp 10.10.46.32 0.0.0.7 10.10.39.0 0.0.0.255 log
permit udp 10.10.46.32 0.0.0.7 eq 12222 12223 10.10.39.0 0.0.0.255 log
remark ---- Controllers to WCS Server ----
permit icmp host 10.10.46.34 host 192.168.42.135 log
permit tcp host 10.10.46.34 host 192.168.42.135 eq 69 log
permit udp host 10.10.46.34 host 192.168.42.135 eq tftp snmp snmptrap log
permit icmp host 10.10.46.35 host 192.168.42.135 log
permit tcp host 10.10.46.35 host 192.168.42.135 eq 69 log
permit udp host 10.10.46.35 host 192.168.42.135 eq tftp snmp snmptrap log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
!
logging source-interface Loopback0
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 priv notify *tv.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF.FFFFFFFFF7F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.134 <removed>
!
!
!
!
!

```

```

tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
control-plane
!
!
!
!
!
!
!
!
!
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO INC.****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO INC.****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15 output
 exec-timeout 15 0
 privilege level 15
 login authentication RLOCAL
 stopbits 1
line aux 0
 session-timeout 15 output
 stopbits 1
line 66
 session-timeout 15 output
 no activation-character
 no exec

```

```

transport preferred none
transport input all
transport output all
line 194
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
line vty 5 15
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179777
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
End

```

Medium Store Router #2

```

----- show version -----
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 17-Jun-06 00:59 by prod_rel_team

ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)

RMED-2 uptime is 4 weeks, 1 day, 3 hours, 30 minutes
System returned to ROM by reload at 10:06:01 PST Thu Nov 16 2006
System restarted at 10:14:14 PST Thu Nov 16 2006
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 3845 (revision 1.0) with 484352K/39936K bytes of memory.
 Processor board ID FTX1027A08S
 2 Gigabit Ethernet interfaces
 2 Serial interfaces
 1 ATM interface
 2 Channelized T1/PRI ports
 1 Virtual Private Network (VPN) Module
 DRAM configuration is 64 bits wide with parity enabled.
 479K bytes of NVRAM.
 125440K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102

----- show running-config -----

Building configuration...

```

Current configuration : 23490 bytes
!
! Last configuration change at 16:06:27 PST Wed Dec 13 2006 by csm-user
! NVRAM config last updated at 14:34:32 PST Wed Dec 13 2006 by csm-user
!
version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RMED-2
!
boot-start-marker
boot system flash flash:c3845-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
logging buffered 8000000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
clock summer-time PSTDST recurring
    
```



```

30353738 3930819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100D023 AC4B285B EFBA5F1F 4637FFAD F6FFACEF BAD3B4EF 87A0F9D8 28009E96
1B1F42D2 6590D209 0D46EC87 CC734C6D 9B2F0C6F 91D31B7B 7F420DE2 AFBC88B8
358F4767 0B94C561 50A4D940 83F46B37 1E7EF961 93CB7765 EC6CDDD3 4DF63826
C02C2F27 037F7E00 247D8716 7C37A38E B40EFECC DE796ECD E7C8AA1E C0444DE0
70070203 010001A3 79307730 0F060355 1D130101 FF040530 030101FF 30240603
551D1104 1D301B82 19524D45 442D322E 52455441 494C5043 494C4142 2E4C4F43
414C301F 0603551D 23041830 168014CE 2E180114 EF70DB98 023EA37B 744FC6DE
0FD58930 1D060355 1D0E0416 0414CE2E 180114EF 70DB9802 3EA37B74 4FC6DE0F
D589300D 06092A86 4886F70D 01010405 00038181 00983485 2D1A2DAC 6674792D
72380397 0FBC86BE 52C86B36 6DE04340 86114976 DD274346 326160C1 569004A8
DE49FA7E 1EB18FAD 45528440 07AF1F12 4AD2875D 62252701 3C58623A DADDA43
33164777 895B5FB1 3F41CB3D 281DBE08 5FB49106 36F35EBF 727FD526 2723CFCC
8BE3F6FB D9458586 9D757ABC 7BDE959E 278F0685 12
quit
crypto pki certificate chain IDSMDC_CSMANAGER
certificate ca 00CE88ED0F069AE8F5
30820209 30820172 020900CE 88ED0F06 9AE8F530 0D06092A 864886F7 0D010104
05003049 31123010 06035504 0B13096D 6963726F 736F6674 31123010 06035504
03130943 534D616E 61676572 311F301D 06092A86 4886F70D 01090116 1061646D
696E4064 6F6D6169 6E2E636F 6D301E17 0D303630 39323330 31303235 345A170D
31313039 32333031 30323534 5A304931 12301006 0355040B 13096D69 63726F73
6F667431 12301006 03550403 13094353 4D616E61 67657231 1F301D06 092A8648
86F70D01 09011610 61646D69 6E40646F 6D61696E 2E636F6D 30819F30 0D06092A
864886F7 0D010101 05000381 8D003081 89028181 00BE596C 97AD25EC 35D71F77
598DDDD8 B8D30AAF 67B268D5 334EAB58 F7418364 664B920A E0011931 4EDF28D1
285B7C45 934EE887 00036A4A C0280132 88C48718 EF48F77E C9EBB27B 6FA11534
03B3B9CB 3DCEFCDC A1339BA4 22C8BFAD 47F50E51 AC04CD7A 03E81331 96BF4ACA
9A1CC2AD 3452AAEB FF84503C A571FB93 EC509A03 8B020301 0001300D 06092A86
4886F70D 01010405 00038181 003A2C37 FC8B0EF1 54E0B963 4D94C234 5EF94288
F6B0B46D 4EFECB7A D15991DE 05FE484E C9DB2AB8 A919DD2F 103545C4 EF7D9269
27975BAD 02CBDDA7 6492EC76 56845082 220A73D7 F9F60FA0 8E9EDDE8 5147E5EB
FB5A00E0 25872141 AA35FAC6 BEF300D9 97343B16 0600B102 F5D555F9 B8AA4D90
26E026CB 6F46B573 700207C8 71
quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 0/0/0
framing esf
linecode b8zs
channel-group 0 timeslots 1-24
!
controller T1 0/0/1
framing esf
linecode b8zs
!
!
!
!
!
!
interface Tunnell
no ip address
ip access-group CSM_FW_ACL_ATM0/1/0 in
!
interface Loopback0
ip address 10.10.46.2 255.255.255.255
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface GigabitEthernet0/0
no ip address

```

```
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/0.102
description ROUTER LINK TO RMED1 VIA SMED1
encapsulation dot1Q 102
ip address 10.10.46.30 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface GigabitEthernet0/1
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
duplex auto
speed auto
media-type rj45
!
interface GigabitEthernet0/1.11
description POS
encapsulation dot1Q 11
ip address 10.10.32.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.11 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 11 ip 10.10.32.1
standby 11 priority 95
standby 11 preempt
!
interface GigabitEthernet0/1.12
description DATA
encapsulation dot1Q 12
ip address 10.10.33.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.12 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 12 ip 10.10.33.1
standby 12 priority 95
standby 12 preempt
!
interface GigabitEthernet0/1.13
description VOICE
encapsulation dot1Q 13
ip address 10.10.34.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.13 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 13 ip 10.10.34.1
standby 13 priority 95
standby 13 preempt
!
interface GigabitEthernet0/1.16
description PARTNER
```

```

encapsulation dot1Q 16
ip address 10.10.37.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.16 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 16 ip 10.10.37.1
standby 16 priority 95
standby 16 preempt
!
interface GigabitEthernet0/1.18
description LWAP CONTROL
encapsulation dot1Q 18
ip address 10.10.39.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.18 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 18 ip 10.10.39.1
standby 18 priority 95
standby 18 preempt
!
interface GigabitEthernet0/1.101
description ROUTER LINK TO RMED1 VIA SMED2
encapsulation dot1Q 101
ip address 10.10.46.26 255.255.255.252
ip access-group CSM_FW_ACL_GigabitEthernet0/0.102 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
ip ospf cost 200
!
interface GigabitEthernet0/1.1000
description MANAGEMENT
encapsulation dot1Q 1000
ip address 10.10.47.3 255.255.255.0
ip access-group CSM_FW_ACL_GigabitEthernet0/1.1000 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
standby 100 ip 10.10.47.1
standby 100 priority 95
standby 100 preempt
!
interface Serial0/0/0:0
description RMED2 TO SP
no ip address
ip access-group CSM_FW_ACL_ATM0/1/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface Serial0/0/0:0.1 point-to-point
ip address 10.10.46.21 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
ip ospf cost 5000
frame-relay interface-dlci 202
!

```



```

interface ATM0/1/0
  no ip address
  ip access-group CSM_FW_ACL_ATM0/1/0 in
  ip verify unicast source reachable-via rx
  shutdown
  no atm ilmi-keepalive
  dsl operating-mode auto
!
interface Group-Async0
  physical-layer async
  no ip address
  ip access-group CSM_FW_ACL_ATM0/1/0 in
  ip verify unicast source reachable-via rx
  ip virtual-reassembly
  encapsulation slip
  no group-range
!
router ospf 5
  router-id 10.10.46.2
  log-adjacency-changes
  passive-interface default
  no passive-interface GigabitEthernet0/0.102
  no passive-interface GigabitEthernet0/1.101
  no passive-interface Serial0/0/0:0.1
  network 10.10.32.0 0.0.15.255 area 2
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_ATM0/1/0
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.46.2 log
  permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
  remark Drop anything not explicitly allowed
  deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.46.2 log
  permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
  remark ---- permit ntp ----
  permit udp any host 192.168.62.161 eq ntp
  permit udp any host 192.168.62.162 eq ntp
  permit udp any host 192.168.42.130 eq ntp
  remark Drop anything not explicitly allowed
  deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0.102
  remark ---- permit ntp ----
  permit udp any host 192.168.62.161 eq ntp
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.46.2 log
  permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
  remark ---- Trusted ports for passing traffic in failure scenarios ----
  permit ip any any log
  permit udp any host 192.168.62.162 eq ntp
  permit udp any host 192.168.42.130 eq ntp
  remark Drop anything not explicitly allowed
  deny ip any any log
  remark ---- permit ntp ----

```

```

ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.1000
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- Ciscoworks so Managed Devices ----
permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Allow network devices to use the ACS server ----
permit tcp any host 192.168.42.131 eq tacacs log
permit udp any host 192.168.42.131 eq 1812 log
remark ---- ping to Datacenter ----
permit icmp any 192.168.42.0 0.0.0.255 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.47.0 0.0.0.255 10.10.47.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.32.0 0.0.0.255 10.10.32.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log

```

```

remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.12
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.33.0 0.0.0.255 10.10.33.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.13
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.34.0 0.0.0.255 10.10.34.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.16
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log

```

```

remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.37.0 0.0.0.255 10.10.37.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/1.18
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
permit udp any host 192.168.42.121 eq snmp syslog log
remark ---- Authenticate Wireless users ----
permit udp host 10.10.46.34 host 192.168.42.131 eq 1812 log
permit udp host 10.10.46.35 host 192.168.42.131 eq 1812 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.39.0 0.0.0.255 10.10.39.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0.1
remark ---- All ACLs for DC to Remote will be handled at the Data Center *before* it gets
put into the WAN
permit ip any any log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.46.2 log
permit tcp host 192.168.42.133 host 10.10.46.2 eq 22 443 log
remark Drop anything not explicitly allowed
deny ip any any log
!
logging source-interface Loopback0
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay

```



```

privilege level 15
login authentication RLOCAL
stopbits 1
line aux 0
session-timeout 15 output
no exec
stopbits 1
line vty 0 4
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
line vty 5 15
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179933
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
End

```

Small Store Router #1

```

----- show version -----

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 16-Jun-06 22:22 by prod_rel_team

ROM: System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE SOFTWARE (fc1)

RSMALL-1 uptime is 2 days, 4 hours, 28 minutes
System returned to ROM by power-on
System restarted at 09:14:34 PST Wed Dec 13 2006
System image file is "flash:c2800nm-advipservicesk9-mz.124-9.T.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to

```

export@cisco.com.

Cisco 2821 (revision 53.51) with 1034240K/14336K bytes of memory.
Processor board ID FTX1032A0JQ
8 FastEthernet interfaces
2 Gigabit Ethernet interfaces
2 Serial interfaces
1 ATM interface
1 terminal line
2 Channelized T1/PRI ports
1 Virtual Private Network (VPN) Module
4 Voice FXO interfaces
11 Voice FXS interfaces
1 cisco content engine(s)
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
250880K bytes of ATA CompactFlash (Read/Write)

```

```

Configuration register is 0x2102

```

```

----- show running-config -----

```

```

Building configuration...

```

```

Current configuration : 26527 bytes
!
! Last configuration change at 15:59:25 PST Thu Dec 14 2006 by bmcgloth
! NVRAM config last updated at 14:34:37 PST Wed Dec 13 2006 by csm-user
!
version 12.4
no service pad
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RSMALL-1
!
boot-start-marker
boot system flash flash:c2800nm-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
card type t1 0 0
logging buffered 8000000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
enable password 7 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!

```



```

crypto pki certificate chain TP-self-signed-1524690245
certificate self-signed 01
 30820253 308201BC A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
 69666963 6174652D 31353234 36393032 3435301E 170D3036 31303137 32313533
 33345A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 35323436
 39303234 3530819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
 8100BEF1 94154F84 B0BC3FDC 8C7757CC FA2953C5 699E4FF1 885641AD 5FE26685
 60DC967E E82F35E2 2EB4388B 5432FD19 5D4B7A62 4A2CD316 AE0C0B78 C0E89275
 0F35D1FB 2364BE07 5DBA3396 3A597625 8A4B84DC 6EE962C9 81789889 F155E645
 0323299C 7EA536B4 8C9FC9ED E6077ED2 BD8A6564 A2850505 DE507792 4A9C416C
 FE410203 010001A3 7B307930 0F060355 1D130101 FF040530 030101FF 30260603
 551D1104 1F301D82 1B52534D 414C4C2D 312E5245 5441494C 5043494C 41422E4C
 4F43414C 301F0603 551D2304 18301680 14AC03A4 7A5F1002 496E26D1 6B00D687
 4F5C4A44 CD301D06 03551D0E 04160414 AC03A47A 5F100249 6E26D16B 00D6874F
 5C4A44CD 300D0609 2A864886 F70D0101 04050003 8181007E 53B50747 9D0D80D2
 35A35EFF F5DFB5C1 3544A8F9 5FFE4558 AB69DF97 EEE71406 88A99303 16ACEA73
 C1B9207E 2261FD1B 24AD5726 95AEF225 FFBE4677 0A5F2472 692FF153 687A0A44
 497C1D93 C5521ADF 62D87929 C9A3C9C1 5A6583BC 05E5B526 CD2B628F 16211592
 94111AC3 E7029550 BB206736 AB508719 7D7FFB4A 4D7669
quit
crypto pki certificate chain IDSMDC_CSMANAGER
certificate ca 00CE88ED0F069AE8F5
 30820209 30820172 020900CE 88ED0F06 9AE8F530 0D06092A 864886F7 0D010104
 05003049 31123010 06035504 0B13096D 6963726F 736F6674 31123010 06035504
 03130943 534D616E 61676572 311F301D 06092A86 4886F70D 01090116 1061646D
 696E4064 6F6D6169 6E2E636F 6D301E17 0D303630 39323330 31303235 345A170D
 31313039 32333031 30323534 5A304931 12301006 0355040B 13096D69 63726F73
 6F667431 12301006 03550403 13094353 4D616E61 67657231 1F301D06 092A8648
 86F70D01 09011610 61646D69 6E40646F 6D61696E 2E636F6D 30819F30 0D06092A
 864886F7 0D010101 05000381 8D003081 89028181 00BE596C 97AD25EC 35D71F77
 598DDDB B8D30AAF 67B268D5 334EAB58 F7418364 664B920A E0011931 4EDF28D1
 285B7C45 934EE887 00036A4A C0280132 88C48718 EF48F77E C9EBB27B 6FA11534
 03B3B9CB 3DCEFCDC A1339BA4 22C8BFAD 47F50E51 AC04CD7A 03E81331 96BF4ACA
 9A1CC2AD 3452AAEB FF84503C A571FB93 EC509A03 8B020301 0001300D 06092A86
 4886F70D 01010405 00038181 003A2C37 FC8B0EF1 54E0B963 4D94C234 5EF94288
 F6B0B46D 4EFECB7A D15991DE 05FE484E C9DB2AB8 A919DD2F 103545C4 EF7D9269
 27975BAD 02CBDDA7 6492EC76 56845082 220A73D7 F9F60FA0 8E9EDDE8 5147E5EB
 FB5A00E0 25872141 AA35FAC6 BEF300D9 97343B16 0600B102 F5D555F9 B8AA4D90
 26E026CB 6F46B573 700207C8 71
quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 0/0/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 0/0/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.30.1 255.255.255.255
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip inspect CSM_INSPECT_1 in

```

```

ip virtual-reassembly
!
interface GigabitEthernet0/0
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
shutdown
duplex auto
speed auto
!
interface FastEthernet0/2/0
switchport trunk native vlan 18
switchport mode trunk
spanning-tree portfast
!
interface FastEthernet0/2/1
switchport access vlan 11
spanning-tree portfast
!
interface FastEthernet0/2/2
switchport access vlan 11
spanning-tree portfast
!
interface FastEthernet0/2/3
switchport access vlan 11
spanning-tree portfast
!
interface FastEthernet0/3/0
switchport access vlan 18
!
interface FastEthernet0/3/1
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface Serial0/0/0:0
description RSMALL-1 CONNECTION RSP-1
no ip address
ip access-group CSM_FW_ACL_Content-Engine1/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface Serial0/0/0:0.1 point-to-point
ip address 10.10.30.9 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
frame-relay interface-dlci 101
!
interface Serial0/0/0:0.2 point-to-point
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx

```

```
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Serial0/0/1:0
description RSMALL-1 CONNECTION RSP-2
no ip address
ip access-group CSM_FW_ACL_Content-Engine1/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation frame-relay IETF
!
interface Serial0/0/1:0.1 point-to-point
ip address 10.10.30.13 255.255.255.252
ip access-group CSM_FW_ACL_Serial0/0/0:0.1 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip ips sdm_ips_rule in
ip virtual-reassembly
ip ospf cost 1000
frame-relay interface-dlci 201
!
interface ATM0/1/0
no ip address
shutdown
no atm ilmi-keepalive
dsl operating-mode auto
!
interface Content-Engine1/0
no ip address
ip access-group CSM_FW_ACL_Content-Engine1/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
shutdown
!
interface Vlan1
no ip address
ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
ip verify unicast source reachable-via rx
!
interface Vlan11
description POS
ip address 10.10.16.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan11 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan12
description DATA
ip address 10.10.17.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan12 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan13
description VOICE
ip address 10.10.18.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan13 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
```

```

ip virtual-reassembly
!
interface Vlan14
description WIRELESS
ip address 10.10.19.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan14 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan15
description WIRELESS POS
ip address 10.10.20.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan15 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan16
description PARTNER
ip address 10.10.21.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan16 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan17
description WIRELESS GUEST
ip address 10.10.22.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan17 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan18
description LWAP CONTROL
ip address 10.10.23.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan18 in
ip verify unicast source reachable-via rx
ip helper-address 192.168.42.130
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Vlan1000
description MANAGEMENT
ip address 10.10.31.1 255.255.255.0
ip access-group CSM_FW_ACL_Vlan1000 in
ip verify unicast source reachable-via rx
ip inspect CSM_INSPECT_1 in
ip virtual-reassembly
!
interface Group-Async0
physical-layer async
no ip address
ip access-group CSM_FW_ACL_Content-Engine1/0 in
ip verify unicast source reachable-via rx
ip virtual-reassembly
encapsulation slip
no group-range
!

```

```

router ospf 5
  router-id 10.10.30.1
  log-adjacency-changes
  passive-interface default
  no passive-interface Serial0/0/0:0.1
  no passive-interface Serial0/0/1:0.1
  network 10.10.16.0 0.0.15.255 area 1
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_Content-Engine1/0
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.30.1 log
  permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
  remark Drop anything not explicitly allowed
  deny ip any any log
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.30.1 log
  permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
  remark ---- permit ntp ----
  permit udp any host 192.168.62.161 eq ntp
  permit udp any host 192.168.62.162 eq ntp
  permit udp any host 192.168.42.130 eq ntp
  remark Drop anything not explicitly allowed
  deny ip any any log
ip access-list extended CSM_FW_ACL_Serial0/0/0:0.1
  remark ---- All ACLs for DC to Remote will be handled at the Data Center *before* it gets
  put into the WAN
  permit ip any any log
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.30.1 log
  permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
  remark Drop anything not explicitly allowed
  deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan1000
  remark Allow CSM-Server to access device through the Serial (external) Interface
  permit icmp host 192.168.42.133 host 10.10.30.1 log
  permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
  remark ---- permit ntp ----
  permit udp any host 192.168.62.161 eq ntp
  permit udp any host 192.168.62.162 eq ntp
  permit udp any host 192.168.42.130 eq ntp
  remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
  permit tcp any host 192.168.42.134 eq 69 log
  permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
  remark ---- Ciscoworks so Managed Devices ----
  permit tcp host 192.168.42.134 any eq 22 telnet www 443 log
  permit udp host 192.168.42.134 any eq snmp snmptrap syslog log
  remark ---- System messages to MARS ----
  permit tcp any host 192.168.42.121 eq 2055 log
  permit udp any host 192.168.42.121 eq snmp syslog log
  remark ---- Allow network devices to use the ACS server ----
  permit tcp any host 192.168.42.131 eq tacacs log
  permit udp any host 192.168.42.131 eq 1812 log
  remark ---- ping to Datacenter ----
  permit icmp any 192.168.42.0 0.0.0.255 log

```

```

remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.31.0 0.0.0.255 10.10.31.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan11
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.16.0 0.0.0.255 10.10.16.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
permit udp any host 192.168.52.99 eq 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan12
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.17.0 0.0.0.255 10.10.17.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log

```

```

permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan13
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.18.0 0.0.0.255 10.10.18.0 0.0.0.255 log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan14
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.19.0 0.0.0.255 10.10.19.0 0.0.0.255 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan15
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark ---- E-mail ----
permit tcp any host 192.168.42.140 eq smtp www 443 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.20.0 0.0.0.255 10.10.20.0 0.0.0.255 log
remark ---- Clients to ActiveDirectory Server ----
permit icmp any host 192.168.42.130 log
remark ---- POS Devices talking to Wincor ----
permit icmp any host 192.168.52.98 log
remark ---- POS to MSRMS Server ----
permit tcp any host 192.168.52.99 eq www 443 1433 1434 log
remark ---- Clients to CSA Manager ----
permit tcp any host 192.168.42.132 eq www 443 5401 5402 log
remark ---- Required for devices to perform windows updates ----
permit tcp any host 192.168.42.150 eq www 443 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log

```

```

permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
permit tcp any host 192.168.42.130 range 1024 65535 log
permit tcp any host 192.168.42.130 eq www 88 123 135 139 389 443 445 1028 log
permit udp any host 192.168.42.130 eq domain bootps 88 ntp 135 389 log
permit tcp any host 192.168.52.98 eq www 139 443 445 1433 3389 4064 log
permit udp any host 192.168.52.98 eq netbios-ns 445 1433 log
permit udp any host 192.168.52.99 eq 1433 1434 log
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan16
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.21.0 0.0.0.255 10.10.21.0 0.0.0.255 log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan17
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.22.0 0.0.0.255 10.10.22.0 0.0.0.255 log
remark ---- Allow DHCP to work ----
permit udp any host 255.255.255.255 eq bootps log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
permit udp any host 192.168.42.130 eq bootps log
remark Drop anything not explicitly allowed
deny ip any any log
ip access-list extended CSM_FW_ACL_Vlan18
remark ---- permit ntp ----
permit udp any host 192.168.62.161 eq ntp
remark ---- Send logs to their mgmt utilities through the mgmt VLAN ----
permit tcp any host 192.168.42.134 eq 69 log
remark ---- System messages to MARS ----
permit tcp any host 192.168.42.121 eq 2055 log
remark ---- Authenticate Wireless users ----
permit udp host 192.168.42.112 host 192.168.42.131 eq 1812 log
remark ---- HSRP health information ----
permit udp any host 224.0.0.2 eq 1985 log
remark ---- Ping Gateway ----
permit icmp 10.10.23.0 0.0.0.255 10.10.23.0 0.0.0.255 log
remark ---- Small stores to Datacenter controller HREAP ----
permit icmp 10.10.23.0 0.0.0.255 host 192.168.42.112 log
remark Allow CSM-Server to access device through the Serial (external) Interface
permit icmp host 192.168.42.133 host 10.10.30.1 log
permit tcp host 192.168.42.133 host 10.10.30.1 eq 22 443 log
permit udp any host 192.168.62.162 eq ntp
permit udp any host 192.168.42.130 eq ntp
permit udp any host 192.168.42.134 eq tftp snmp snmptrap syslog log
permit udp any host 192.168.42.121 eq snmp syslog log

```



```

ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  session-timeout 15  output
  exec-timeout 15  0
  privilege level 15
  login authentication RLOCAL
line aux 0
  session-timeout 15  output
  no exec
  transport output none
line 66
  session-timeout 15  output
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output all
line vty 0 4
  session-timeout 15  output
  access-class 23 in
  password 7 <removed>
  logging synchronous
  login authentication RETAIL
  transport input ssh
line vty 5 15
  session-timeout 15  output
  access-class 23 in
  privilege level 15
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179512
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end

```

Data Center WAN Router #1

```
----- show version -----  
  
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE  
SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Sat 17-Jun-06 00:59 by prod_rel_team  
  
ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)  
  
RWAN-1 uptime is 2 weeks, 7 hours, 24 minutes  
System returned to ROM by power-on  
System restarted at 06:27:40 PST Fri Dec 1 2006  
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco 3845 (revision 1.0) with 481280K/43008K bytes of memory.  
Processor board ID FTX1025A0XR  
2 Gigabit Ethernet interfaces  
1 Serial interface  
2 Channelized T1/PRI ports  
1 Virtual Private Network (VPN) Module  
DRAM configuration is 64 bits wide with parity enabled.  
479K bytes of NVRAM.  
250880K bytes of ATA System CompactFlash (Read/Write)
```

```
Configuration register is 0x2102
```

```
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 8302 bytes  
!  
! Last configuration change at 13:51:02 PST Fri Dec 15 2006 by bmcgloth  
! NVRAM config last updated at 13:51:03 PST Fri Dec 15 2006 by bmcgloth  
!  
version 12.4  
no service pad  
service tcp-keepalives-in  
service timestamps debug datetime localtime show-timezone  
service timestamps log datetime localtime show-timezone  
service password-encryption  
no service password-recovery
```



```

!
crypto pki trustpoint TP-self-signed-4205664985
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-4205664985
  revocation-check none
  rsakeypair TP-self-signed-4205664985
!
!
crypto pki certificate chain TP-self-signed-4205664985
  certificate self-signed 01
    3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 34323035 36363439 3835301E 170D3036 31313130 32303137
    34355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
    4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 32303536
    36343938 3530819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
    8100DA07 17320D41 480EDFBE B0BDE611 978E9DDA 860FD32B EDA058E7 7F7748D0
    7BFF7A86 3EF3C0A0 934217AA 312115A3 0D8403E2 0FBBBAB2 82A7C962 B81B3F1A
    4DB3DCB3 BCF9C3A6 BC0913AF 6715BD4C 35122021 6FDE1850 AF4B13F6 5E47C503
    D10CAAEE 14179D0B EAF30728 BAB50CD8 8A338A13 ED91E981 A6783D1B F4A8E016
    73CF0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
    551D1104 19301782 15525741 4E2D312E 796F7572 646F6D61 696E2E63 6F6D301F
    0603551D 23041830 168014A6 680C11F4 A53599AC 2918BC64 A61399DF FDB94B30
    1D060355 1D0E0416 0414A668 0C11F4A5 3599AC29 18BC64A6 1399DFFD B94B300D
    06092A86 4886F70D 01010405 00038181 0015B6FA EC166804 BE5CE9C1 6971C6A1
    33102351 2A873C23 8C443474 A1DA985C 6437BA1F 22C59CDF F3A3A813 64B92291
    47DF74D4 52C0C623 C9854D5B B599A7DF DEFCBEA1 17B7720B 2E800EBD 61997FD6
    AA16B4FB E358FC73 B7BF44C9 3C05DBBC 00EB8F33 6FD33218 98D9E254 66C92E80
    5E822DF4 DECEFF57 B342635B E5B122E4 29
  quit
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 1/0
  framing esf
  linecode b8zs
  channel-group 0 timeslots 1-24
!
controller T1 1/1
  framing esf
  linecode b8zs
!
!
!
!
!
!
interface Loopback0
  ip address 192.168.1.1 255.255.255.255
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
!
interface GigabitEthernet0/0
  ip address 192.168.10.13 255.255.255.252
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  duplex auto
  speed auto
  media-type rj45
!
interface GigabitEthernet0/1
  ip address 192.168.10.17 255.255.255.252
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  duplex auto
  speed auto
  media-type rj45

```

```

!
interface Serial1/0:0
  no ip address
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  encapsulation frame-relay IETF
!
interface Serial1/0:0.1 point-to-point
  ip address 10.10.30.10 255.255.255.252
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  frame-relay interface-dlci 1001
!
interface Serial1/0:0.2 point-to-point
  ip address 10.10.46.18 255.255.255.252
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  frame-relay interface-dlci 1002
!
interface Serial1/0:0.3 point-to-point
  ip address 10.10.62.18 255.255.255.252
  ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
  frame-relay interface-dlci 1003
!
router ospf 5
  router-id 192.168.1.1
  log-adjacency-changes
  network 10.10.30.8 0.0.0.3 area 1
  network 10.10.46.16 0.0.0.3 area 2
  network 10.10.62.16 0.0.0.3 area 3
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.10.12 0.0.0.3 area 0
  network 192.168.10.16 0.0.0.3 area 0
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
  remark implicit trust model between DCs and Remotes
  permit ip any any log
!
logging source-interface Loopback0
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Loopback0
snmp-server packet-size 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch

```

```
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.134 <removed>
!
!
!
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
control-plane
!
!
!
!
!
!
!
!
!
!
!
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
          **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
          **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
```

```

session-timeout 15
exec-timeout 15 0
privilege level 15
logging synchronous
login authentication RLOCAL
stopbits 1
line aux 0
no exec
stopbits 1
line vty 0 4
session-timeout 15
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
line vty 5 15
session-timeout 15
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179581
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
End

```

Data Center WAN Router #2

```

----- show version -----

Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.4(9)T, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 17-Jun-06 00:59 by prod_rel_team

ROM: System Bootstrap, Version 12.3(11r)T2, RELEASE SOFTWARE (fc1)

RWAN-2 uptime is 2 weeks, 7 hours, 27 minutes
System returned to ROM by power-on
System restarted at 06:27:39 PST Fri Dec 1 2006
System image file is "flash:c3845-advipservicesk9-mz.124-9.T.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 3845 (revision 1.0) with 481280K/43008K bytes of memory.
Processor board ID FTX1025A0WS
2 Gigabit Ethernet interfaces
2 Serial interfaces
2 Channelized T1/PRI ports
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity enabled.
479K bytes of NVRAM.
250880K bytes of ATA System CompactFlash (Read/Write)

Configuration register is 0x2102

----- show running-config -----

Building configuration...

```
Current configuration : 8562 bytes
!
! Last configuration change at 13:53:29 PST Fri Dec 15 2006 by bmcgloth
! NVRAM config last updated at 13:53:32 PST Fri Dec 15 2006 by bmcgloth
!
version 12.4
no service pad
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service password-recovery
!
hostname RWAN-2
!
boot-start-marker
boot system flash flash:c3845-advipservicesk9-mz.124-9.T.bin
boot-end-marker
!
card type t1 1 1
logging buffered 800000 informational
no logging rate-limit
no logging console
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
resource policy
!
clock timezone PST -8
```



```
username cisco privilege 15 secret 5 <removed>
!
!
controller T1 1/0
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
controller T1 1/1
 framing esf
 linecode b8zs
 channel-group 0 timeslots 1-24
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.1.2 255.255.255.255
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
!
interface GigabitEthernet0/0
 ip address 192.168.10.21 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip ospf cost 5000
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 192.168.10.25 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip ospf cost 5000
 duplex auto
 speed auto
 media-type rj45
!
interface Serial1/0:0
 no ip address
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 encapsulation frame-relay IETF
!
interface Serial1/0:0.1 point-to-point
 ip address 10.10.30.14 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip ospf cost 5000
 frame-relay interface-dlci 1004
!
interface Serial1/0:0.2 point-to-point
 ip address 10.10.46.22 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip ospf cost 5000
 frame-relay interface-dlci 1005
!
interface Serial1/0:0.3 point-to-point
 ip address 10.10.62.22 255.255.255.252
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
 ip ospf cost 5000
 frame-relay interface-dlci 1006
!
interface Serial1/1:0
 no ip address
 ip access-group CSM_FW_ACL_GigabitEthernet0/0 in
```

```

!
router ospf 5
  router-id 192.168.1.2
  log-adjacency-changes
  network 10.10.30.12 0.0.0.3 area 1
  network 10.10.46.20 0.0.0.3 area 2
  network 10.10.62.20 0.0.0.3 area 3
  network 192.168.1.2 0.0.0.0 area 0
  network 192.168.10.20 0.0.0.3 area 0
  network 192.168.10.24 0.0.0.3 area 0
!
!
!
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Loopback0
!
ip access-list extended CSM_FW_ACL_GigabitEthernet0/0
  remark implicit trust model between DCs and Remotes
  permit ip any any log
!
logging source-interface Loopback0
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 10.10.10.0 0.0.0.7
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.134 <removed>
!
!
!
!
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server domain-stripping
tacacs-server key 7 <removed>
!
control-plane
!
!

```



```

logging synchronous
login authentication RETAIL
transport input ssh
!
scheduler allocate 20000 1000
ntp clock-period 17179531
ntp source Loopback0
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
!
end
    
```

Large Store Switch #1

```

----- show version -----

Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9K91S-M), Version 12.2(20)EW3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 07-Sep-05 11:30 by pwade
Image text-base: 0x00000000, data-base: 0x012B374C

ROM: 12.2(20r)EW1
Dagobah Revision 226, Swamp Revision 34

SLRG-1 uptime is 2 weeks, 7 hours, 20 minutes
System returned to ROM by reload
System restarted at 06:27:26 PST Fri Dec 1 2006
System image file is "bootflash:"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C4506 (MPC8245) processor (revision 10) with 262144K bytes of memory.
Processor board ID FOX101600HF
MPC8245 CPU at 266Mhz, Supervisor II+
Last reset from Reload
12 Virtual Ethernet/IEEE 802.3 interface(s)
98 Gigabit Ethernet/IEEE 802.3 interface(s)
511K bytes of non-volatile configuration memory.

Configuration register is 0x2101

----- show running-config -----
    
```

```
Building configuration...

Current configuration : 8992 bytes
!
! Last configuration change at 19:32:54 PST Mon Dec 11 2006 by casuser
! NVRAM config last updated at 19:27:23 PST Mon Dec 11 2006 by casuser
!
version 12.2
no service pad
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service compress-config
!
hostname SLRG-1
!
logging buffered 51200 debugging
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>
clock timezone PST -8
clock summer-time PSTDST recurring
vtp domain ''
vtp mode transparent
ip subnet-zero
ip domain-name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
!
no ip bootp server
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 11-18,101-102,1000
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet2/1
!
interface GigabitEthernet2/2
!
interface GigabitEthernet2/3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1-100,103-4094
  switchport mode trunk
!
```

```
interface GigabitEthernet2/4
!
interface GigabitEthernet2/5
  switchport access vlan 11
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet2/6
!
interface GigabitEthernet2/7
!
interface GigabitEthernet2/8
!
interface GigabitEthernet2/9
!
interface GigabitEthernet2/10
!
interface GigabitEthernet2/11
!
interface GigabitEthernet2/12
!
interface GigabitEthernet2/13
!
interface GigabitEthernet2/14
!
interface GigabitEthernet2/15
!
interface GigabitEthernet2/16
!
interface GigabitEthernet2/17
  switchport access vlan 1000
!
interface GigabitEthernet2/18
  switchport trunk encapsulation dot1q
  switchport mode trunk
  switchport nonegotiate
  no cdp enable
  spanning-tree portfast trunk
!
interface GigabitEthernet2/19
!
interface GigabitEthernet2/20
!
interface GigabitEthernet2/21
!
interface GigabitEthernet2/22
!
interface GigabitEthernet2/23
!
interface GigabitEthernet2/24
!
interface GigabitEthernet2/25
!
interface GigabitEthernet2/26
!
interface GigabitEthernet2/27
!
interface GigabitEthernet2/28
!
interface GigabitEthernet2/29
!
interface GigabitEthernet2/30
!
interface GigabitEthernet2/31
```



```
!  
interface GigabitEthernet2/32  
!  
interface GigabitEthernet2/33  
!  
interface GigabitEthernet2/34  
!  
interface GigabitEthernet2/35  
!  
interface GigabitEthernet2/36  
!  
interface GigabitEthernet2/37  
!  
interface GigabitEthernet2/38  
!  
interface GigabitEthernet2/39  
!  
interface GigabitEthernet2/40  
!  
interface GigabitEthernet2/41  
!  
interface GigabitEthernet2/42  
!  
interface GigabitEthernet2/43  
!  
interface GigabitEthernet2/44  
!  
interface GigabitEthernet2/45  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet2/46  
!  
interface GigabitEthernet2/47  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet2/48  
!  
interface GigabitEthernet3/1  
!  
interface GigabitEthernet3/2  
!  
interface GigabitEthernet3/3  
!  
interface GigabitEthernet3/4  
!  
interface GigabitEthernet3/5  
!  
interface GigabitEthernet3/6  
!  
interface GigabitEthernet3/7  
!  
interface GigabitEthernet3/8  
!  
interface GigabitEthernet3/9  
!  
interface GigabitEthernet3/10  
!  
interface GigabitEthernet3/11  
!  
interface GigabitEthernet3/12  
!  
interface GigabitEthernet3/13
```

```
!  
interface GigabitEthernet3/14  
!  
interface GigabitEthernet3/15  
!  
interface GigabitEthernet3/16  
!  
interface GigabitEthernet3/17  
!  
interface GigabitEthernet3/18  
!  
interface GigabitEthernet3/19  
!  
interface GigabitEthernet3/20  
!  
interface GigabitEthernet3/21  
!  
interface GigabitEthernet3/22  
!  
interface GigabitEthernet3/23  
!  
interface GigabitEthernet3/24  
!  
interface GigabitEthernet3/25  
!  
interface GigabitEthernet3/26  
!  
interface GigabitEthernet3/27  
!  
interface GigabitEthernet3/28  
!  
interface GigabitEthernet3/29  
!  
interface GigabitEthernet3/30  
!  
interface GigabitEthernet3/31  
!  
interface GigabitEthernet3/32  
!  
interface GigabitEthernet3/33  
!  
interface GigabitEthernet3/34  
!  
interface GigabitEthernet3/35  
!  
interface GigabitEthernet3/36  
!  
interface GigabitEthernet3/37  
!  
interface GigabitEthernet3/38  
!  
interface GigabitEthernet3/39  
!  
interface GigabitEthernet3/40  
!  
interface GigabitEthernet3/41  
!  
interface GigabitEthernet3/42  
!  
interface GigabitEthernet3/43  
!  
interface GigabitEthernet3/44  
!  
interface GigabitEthernet3/45
```

```
    switchport trunk encapsulation dot1q
    switchport mode trunk
    !
interface GigabitEthernet3/46
    !
interface GigabitEthernet3/47
    switchport trunk encapsulation dot1q
    switchport mode trunk
    !
interface GigabitEthernet3/48
    !
interface Vlan1
    no ip address
    !
interface Vlan11
    description POS
    no ip address
    !
interface Vlan12
    description DATA
    no ip address
    !
interface Vlan13
    description VOICE
    no ip address
    !
interface Vlan14
    description WIRELESS
    no ip address
    !
interface Vlan15
    description WIRELESS POS
    no ip address
    !
interface Vlan16
    description PARTNER
    no ip address
    !
interface Vlan17
    description WIRELESS GUEST
    no ip address
    !
interface Vlan18
    description LWAP
    no ip address
    !
interface Vlan101
    description INTER ROUTER LINK
    no ip address
    !
interface Vlan102
    description INTER ROUTER LINK
    no ip address
    !
interface Vlan1000
    description MANAGEMENT
    ip address 10.10.63.11 255.255.255.0
    !
ip default-gateway 10.10.63.1
ip route 0.0.0.0 0.0.0.0 10.10.63.1
ip tacacs source-interface Vlan1000
no ip http server
ip http access-class 23
ip http authentication aaa
```

```

!
!
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
!
!
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.0000000F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps rtr
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!

```

```

line con 0
  session-timeout 15 output
  exec-timeout 15 0
  privilege level 15
  login authentication RLOCAL
  stopbits 1
line vty 0 4
  session-timeout 15 output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
line vty 5 15
  session-timeout 15 output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
ntp clock-period 17179073
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Large Store Switch #2

```
----- show version -----
```

```

Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9K91S-M), Version 12.2(20)EW3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 07-Sep-05 11:30 by pwade
Image text-base: 0x00000000, data-base: 0x012B374C

ROM: 12.2(20r)EW1
Dagobah Revision 226, Swamp Revision 34

SLRG-2 uptime is 2 weeks, 7 hours, 21 minutes
System returned to ROM by reload
System restarted at 06:27:25 PST Fri Dec 1 2006
System image file is "bootflash:"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to

```
export@cisco.com.

cisco WS-C4506 (MPC8245) processor (revision 10) with 262144K bytes of memory.
Processor board ID FOX101600HE
MPC8245 CPU at 266Mhz, Supervisor II+
Last reset from Reload
12 Virtual Ethernet/IEEE 802.3 interface(s)
98 Gigabit Ethernet/IEEE 802.3 interface(s)
511K bytes of non-volatile configuration memory.
```

```
Configuration register is 0x2101
```

```
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 8751 bytes
!
! Last configuration change at 17:31:49 PST Tue Dec 12 2006 by bmcgloth
! NVRAM config last updated at 17:31:50 PST Tue Dec 12 2006 by bmcgloth
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service compress-config
!
hostname SLRG-2
!
logging buffered 51200 debugging
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>
clock timezone PST -8
clock summer-time PSTDST recurring
vtp domain ''
vtp mode transparent
ip subnet-zero
ip domain-name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
power redundancy-mode redundant
!
!
!
vlan internal allocation policy ascending
!
vlan 11-18,101-102,1000
!
```

```
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet2/1
!
interface GigabitEthernet2/2
!
interface GigabitEthernet2/3
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1-100,103-4094
  switchport mode trunk
!
interface GigabitEthernet2/4
!
interface GigabitEthernet2/5
!
interface GigabitEthernet2/6
!
interface GigabitEthernet2/7
  switchport access vlan 1000
  spanning-tree portfast
!
interface GigabitEthernet2/8
!
interface GigabitEthernet2/9
!
interface GigabitEthernet2/10
!
interface GigabitEthernet2/11
!
interface GigabitEthernet2/12
!
interface GigabitEthernet2/13
!
interface GigabitEthernet2/14
!
interface GigabitEthernet2/15
!
interface GigabitEthernet2/16
!
interface GigabitEthernet2/17
!
interface GigabitEthernet2/18
!
interface GigabitEthernet2/19
!
interface GigabitEthernet2/20
!
interface GigabitEthernet2/21
!
interface GigabitEthernet2/22
!
interface GigabitEthernet2/23
!
interface GigabitEthernet2/24
!
interface GigabitEthernet2/25
!
interface GigabitEthernet2/26
!
interface GigabitEthernet2/27
!
interface GigabitEthernet2/28
```

```
!  
interface GigabitEthernet2/29  
!  
interface GigabitEthernet2/30  
!  
interface GigabitEthernet2/31  
!  
interface GigabitEthernet2/32  
!  
interface GigabitEthernet2/33  
!  
interface GigabitEthernet2/34  
!  
interface GigabitEthernet2/35  
!  
interface GigabitEthernet2/36  
!  
interface GigabitEthernet2/37  
!  
interface GigabitEthernet2/38  
!  
interface GigabitEthernet2/39  
!  
interface GigabitEthernet2/40  
!  
interface GigabitEthernet2/41  
!  
interface GigabitEthernet2/42  
!  
interface GigabitEthernet2/43  
!  
interface GigabitEthernet2/44  
!  
interface GigabitEthernet2/45  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet2/46  
!  
interface GigabitEthernet2/47  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet2/48  
!  
interface GigabitEthernet3/1  
!  
interface GigabitEthernet3/2  
!  
interface GigabitEthernet3/3  
!  
interface GigabitEthernet3/4  
!  
interface GigabitEthernet3/5  
!  
interface GigabitEthernet3/6  
!  
interface GigabitEthernet3/7  
!  
interface GigabitEthernet3/8  
!  
interface GigabitEthernet3/9  
!  
interface GigabitEthernet3/10
```



```
!  
interface GigabitEthernet3/11  
!  
interface GigabitEthernet3/12  
!  
interface GigabitEthernet3/13  
!  
interface GigabitEthernet3/14  
!  
interface GigabitEthernet3/15  
!  
interface GigabitEthernet3/16  
!  
interface GigabitEthernet3/17  
!  
interface GigabitEthernet3/18  
!  
interface GigabitEthernet3/19  
!  
interface GigabitEthernet3/20  
!  
interface GigabitEthernet3/21  
!  
interface GigabitEthernet3/22  
!  
interface GigabitEthernet3/23  
!  
interface GigabitEthernet3/24  
!  
interface GigabitEthernet3/25  
!  
interface GigabitEthernet3/26  
!  
interface GigabitEthernet3/27  
!  
interface GigabitEthernet3/28  
!  
interface GigabitEthernet3/29  
!  
interface GigabitEthernet3/30  
!  
interface GigabitEthernet3/31  
!  
interface GigabitEthernet3/32  
!  
interface GigabitEthernet3/33  
!  
interface GigabitEthernet3/34  
!  
interface GigabitEthernet3/35  
!  
interface GigabitEthernet3/36  
!  
interface GigabitEthernet3/37  
!  
interface GigabitEthernet3/38  
!  
interface GigabitEthernet3/39  
!  
interface GigabitEthernet3/40  
!  
interface GigabitEthernet3/41  
!  
interface GigabitEthernet3/42
```

```

!
interface GigabitEthernet3/43
!
interface GigabitEthernet3/44
!
interface GigabitEthernet3/45
!
interface GigabitEthernet3/46
!
interface GigabitEthernet3/47
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet3/48
!
interface Vlan1
  no ip address
!
interface Vlan11
  description POS
  no ip address
!
interface Vlan12
  description DATA
  no ip address
!
interface Vlan13
  description VOICE
  no ip address
!
interface Vlan14
  description WIRELESS
  no ip address
!
interface Vlan15
  description WIRELESS POS
  no ip address
!
interface Vlan16
  description PARTNER
  no ip address
!
interface Vlan17
  description WIRELESS GUEST
  no ip address
!
interface Vlan18
  description LWAP
  no ip address
!
interface Vlan101
  description INTER ROUTER LINK
  no ip address
!
interface Vlan102
  description INTER ROUTER LINK
  no ip address
!
interface Vlan1000
  description MANAGEMENT
  ip address 10.10.63.12 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.10.63.1
ip tacacs source-interface Vlan1000

```

```

no ip http server
ip http access-class 23
ip http authentication aaa
!
!
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
!
!
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.0000000F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 priv <removed>
snmp-server host 192.168.42.134 <removed>
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C

```

```

banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15 output
 exec-timeout 15 0
 privilege level 15
 login authentication RLOCAL
 stopbits 1
line vty 0 4
 session-timeout 15 output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
line vty 5 15
 session-timeout 15 output
 access-class 23 in
 exec-timeout 15 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
!
ntp clock-period 17179115
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Large Store Switch #3

```
----- show version -----
```

```

Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 12:55 by yenanh
Image text-base: 0x00003000, data-base: 0x010272D8

```

```

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)

```

```

SLRG-3 uptime is 2 days, 23 hours, 1 minute
System returned to ROM by power-on
System restarted at 14:46:47 PST Tue Dec 12 2006
System image file is "flash:/c3750-ipbasek9-mz.122-25.SEE2.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco WS-C3750-48P (PowerPC405) processor (revision J0) with 118784K/12280K bytes of memory.

Processor board ID CAT1025ZM98
 Last reset from power-on
 10 Virtual Ethernet interfaces
 48 FastEthernet interfaces
 4 Gigabit Ethernet interfaces
 The password-recovery mechanism is disabled.

512K bytes of flash-simulated non-volatile configuration memory.

Base ethernet MAC Address : 00:0A:B8:29:5E:80
 Motherboard assembly number : 73-9675-11
 Power supply part number : 341-0029-05
 Motherboard serial number : CAT10251KHD
 Power supply serial number : DTH1022DMJA
 Model revision number : J0
 Motherboard revision number : A0
 Model number : WS-C3750-48PS-S
 System serial number : CAT1025ZM98
 SFP Module assembly part number : 73-7757-03
 SFP Module revision Number : A0
 SFP Module serial number : CAT10251H19
 Top Assembly Part Number : 800-25858-03
 Top Assembly Revision Number : G0
 Version ID : V05
 CLEI Code Number : COM1W00ARB
 Hardware Board Revision Number : 0x01

Switch	Ports	Model	SW Version	SW Image
*	1 52	WS-C3750-48P	12.2 (25)SEE2	C3750-IPBASEK9-M

Configuration register is 0xF

----- show running-config -----

Building configuration...

Current configuration : 8823 bytes

```

!
! Last configuration change at 14:55:23 PST Tue Dec 12 2006 by bmcgloth
! NVRAM config last updated at 14:55:49 PST Tue Dec 12 2006 by bmcgloth
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname SLRG-3
!
logging buffered 51200 debugging
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>

```

```

aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c3750-48p
ip subnet-zero
ip domain-name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
!
!
!
crypto pki trustpoint TP-self-signed-3089718912
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3089718912
  revocation-check none
  rsakeypair TP-self-signed-3089718912
!
!
crypto ca certificate chain TP-self-signed-3089718912
certificate self-signed 01
  308202A5 3082020E A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  5B312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303839 37313839 31323128 30260609 2A864886 F70D0109
  02161953 4C52472D 332E5245 5441494C 5043494C 41422E4C 4F43414C 301E170D
  30363132 31323232 35313134 5A170D32 30303130 31303030 3030305A 305B312F
  302D0603 55040313 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669
  63617465 2D333038 39373138 39313231 28302606 092A8648 86F70D01 09021619
  534C5247 2D332E52 45544149 4C504349 4C41422E 4C4F4341 4C30819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100C984 0E5B27D3 4AB3773D
  5814DE27 DDFD860B 67C7FF91 DE8EF12D 369A5AD3 E117A219 945036EF 7A1A8CA1
  44CEADD8 30E5D782 D36638C0 7AAEAC59 292BEA5E ED86C4B9 EBD618BF 06191EA8
  1CB35A56 248F36CB D5724BA2 BCA7C83A A3786760 D3F05C43 C02139C9 91D436A7
  CA009BB9 57338561 A1A9B23A 5FD3BE5E B2CB80EE 9AB10203 010001A3 79307730
  0F060355 1D130101 FF040530 030101FF 30240603 551D1104 1D301B82 19534C52
  472D332E 52455441 494C5043 494C4142 2E4C4F43 414C301F 0603551D 23041830
  1680142F F35934F0 44195D7B 2C4B2994 7CD99325 AC50F630 1D060355 1D0E0416
  04142FF3 5934F044 195D7B2C 4B29947C D99325AC 50F6300D 06092A86 4886F70D
  01010405 00038181 009E71CF 28ECD80C 0F7A16D7 52CC07AB E3284006 69B8EC60
  2FBD493C E45263FB 516927E8 FA9F79DE 2D3DB52F 07BF24BF 32E6E6F0 605B5C7D
  1241EC98 593514A5 0E595C13 3CF657E7 00408BF1 75FE832B 8E18BDB8 8275D63A
  228EA7E2 B29768AC A5092210 CB68C355 1EADBD99 F0243DE9 4DD3A6F7 208CB3CA
  243744CA 14085427 1A
quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet1/0/1
!
interface FastEthernet1/0/2
  switchport access vlan 18

```

```
    switchport mode access
    !
interface FastEthernet1/0/3
    !
interface FastEthernet1/0/4
    !
interface FastEthernet1/0/5
    !
interface FastEthernet1/0/6
    !
interface FastEthernet1/0/7
    !
interface FastEthernet1/0/8
    !
interface FastEthernet1/0/9
    !
interface FastEthernet1/0/10
    !
interface FastEthernet1/0/11
    !
interface FastEthernet1/0/12
    !
interface FastEthernet1/0/13
    !
interface FastEthernet1/0/14
    !
interface FastEthernet1/0/15
    !
interface FastEthernet1/0/16
    !
interface FastEthernet1/0/17
    !
interface FastEthernet1/0/18
    !
interface FastEthernet1/0/19
    !
interface FastEthernet1/0/20
    !
interface FastEthernet1/0/21
    !
interface FastEthernet1/0/22
    !
interface FastEthernet1/0/23
    !
interface FastEthernet1/0/24
    !
interface FastEthernet1/0/25
    !
interface FastEthernet1/0/26
    !
interface FastEthernet1/0/27
    !
interface FastEthernet1/0/28
    !
interface FastEthernet1/0/29
    !
interface FastEthernet1/0/30
    !
interface FastEthernet1/0/31
    !
interface FastEthernet1/0/32
    !
interface FastEthernet1/0/33
    !
```

```
interface FastEthernet1/0/34
!
interface FastEthernet1/0/35
!
interface FastEthernet1/0/36
!
interface FastEthernet1/0/37
!
interface FastEthernet1/0/38
!
interface FastEthernet1/0/39
!
interface FastEthernet1/0/40
!
interface FastEthernet1/0/41
!
interface FastEthernet1/0/42
!
interface FastEthernet1/0/43
!
interface FastEthernet1/0/44
!
interface FastEthernet1/0/45
!
interface FastEthernet1/0/46
!
interface FastEthernet1/0/47
!
interface FastEthernet1/0/48
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/4
!
interface Vlan1
 no ip address
!
interface Vlan11
 description POS
 no ip address
!
interface Vlan12
 description DATA
 no ip address
!
interface Vlan13
 description VOICE
 no ip address
!
interface Vlan14
 description WIRELESS
 no ip address
!
interface Vlan15
 description WIRELESS POS
 no ip address
```



```

!
interface Vlan16
  description PARTNER
  no ip address
!
interface Vlan17
  description WIRELESS GUEST
  no ip address
!
interface Vlan18
  description LWAP
  no ip address
!
interface Vlan1000
  description MANAGEMENT
  ip address 10.10.63.14 255.255.255.0
!
ip default-gateway 10.10.63.1
ip classless
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

```

```

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****
    
```

```

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
    
```

```

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  session-timeout 15  output
  exec-timeout 15 0
  privilege level 15
  login authentication RLOCAL
line vty 0 4
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
line vty 5 15
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
!
monitor session 1 source interface Fa1/0/2
monitor session 1 destination interface Fa1/0/1
ntp clock-period 36028347
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end
    
```

Large Store Switch #4

```

----- show version -----

Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 12:55 by yenanh
Image text-base: 0x00003000, data-base: 0x010272D8
    
```

```
ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)
```

```
SLRG-4 uptime is 2 days, 22 hours, 40 minutes
System returned to ROM by power-on
System restarted at 15:07:50 PST Tue Dec 12 2006
System image file is "flash:/c3750-ipbasek9-mz.122-25.SEE2.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
cisco WS-C3750-48P (PowerPC405) processor (revision J0) with 118784K/12280K bytes of
memory.
Processor board ID CAT1025ZM8X
Last reset from power-on
10 Virtual Ethernet interfaces
48 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is disabled.
```

```
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:0A:B8:29:06:00
Motherboard assembly number    : 73-9675-11
Power supply part number       : 341-0029-05
Motherboard serial number      : CAT10251K93
Power supply serial number     : DTH1022DML4
Model revision number          : J0
Motherboard revision number    : A0
Model number                   : WS-C3750-48PS-S
System serial number           : CAT1025ZM8X
SFP Module assembly part number : 73-7757-03
SFP Module revision Number     : A0
SFP Module serial number       : CAT10250R2A
Top Assembly Part Number       : 800-25858-03
Top Assembly Revision Number   : G0
Version ID                     : V05
CLEI Code Number               : COM1W00ARB
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image
* 1	52	WS-C3750-48P	12.2(25)SEE2	C3750-IPBASEK9-M

Configuration register is 0xF

```
----- show running-config -----
```

```

Building configuration...

Current configuration : 8956 bytes
!
! Last configuration change at 15:11:07 PST Tue Dec 12 2006 by cisco
! NVRAM config last updated at 15:11:58 PST Tue Dec 12 2006 by cisco
!
version 12.2
no service pad
service tcp-keepalives-in
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname SLRG-4
!
logging buffered 51200 debugging
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c3750-48p
ip subnet-zero
ip domain-name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
!
!
!
crypto pki trustpoint TP-self-signed-3089696256
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3089696256
  revocation-check none
  rsakeypair TP-self-signed-3089696256
!
!
crypto ca certificate chain TP-self-signed-3089696256
certificate self-signed 01
  308202A5 3082020E A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  5B312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303839 36393632 35363128 30260609 2A864886 F70D0109
  02161953 4C52472D 342E5245 5441494C 5043494C 41422E4C 4F43414C 301E170D
  39333033 30313030 30323234 5A170D32 30303130 31303030 3030305A 305B312F
  302D0603 55040313 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669
  63617465 2D333038 39363936 32353631 28302606 092A8648 86F70D01 09021619
  534C5247 2D342E52 45544149 4C504349 4C41422E 4C4F4341 4C30819F 300D0609
  2A864886 F70D0101 01050003 818D0030 81890281 8100C03D BD51676B 56EE906A
  4AF90A49 3190F2C3 366B8D2D 79D6CD7E 02E348CC B46EC0DB F239755F EE57DC12
  3B34DCA1 CEADBDFD D7DCA766 C357F7DD D9A81041 D633AA1A 4C75B9BE 04FA33D2
  0F24730E A9B76671 9855A914 E630294A 4BB22598 3C6A651B B5EABA14 3B6CC944
  038ED5B3 8980AEDB 766E8BDD AE3E31DF 7F7818E4 865D0203 010001A3 79307730
  0F060355 1D130101 FF040530 030101FF 30240603 551D1104 1D301B82 19534C52

```

```
472D342E 52455441 494C5043 494C4142 2E4C4F43 414C301F 0603551D 23041830
16801440 3220ED8A C85D6A32 1D06862A B6F7A5E0 33015230 1D060355 1D0E0416
04144032 20ED8AC8 5D6A321D 06862AB6 F7A5E033 0152300D 06092A86 4886F70D
01010405 00038181 002A495D 56F25AB6 EDA4AA1F 0D105306 AC225A9B 37367F32
9668C17F AC44CA02 AA080774 E8F8BCA5 656556E6 7275CD94 FCF39ADA 94D093C4
AE9C814B 1EEF6444 E2860D8E 79712D20 BD95E2E5 B911B288 5603F256 A1815408
AC11E72A D8410797 75FA904E F2171A4E 15BD4405 00A7A969 5D51A0B5 638EC88C
2196934C 8429FEED 9B
quit
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet1/0/1
description Wincor POS
switchport access vlan 11
!
interface FastEthernet1/0/2
!
interface FastEthernet1/0/3
!
interface FastEthernet1/0/4
!
interface FastEthernet1/0/5
!
interface FastEthernet1/0/6
!
interface FastEthernet1/0/7
!
interface FastEthernet1/0/8
!
interface FastEthernet1/0/9
!
interface FastEthernet1/0/10
!
interface FastEthernet1/0/11
!
interface FastEthernet1/0/12
!
interface FastEthernet1/0/13
!
interface FastEthernet1/0/14
!
interface FastEthernet1/0/15
!
interface FastEthernet1/0/16
!
interface FastEthernet1/0/17
!
interface FastEthernet1/0/18
!
interface FastEthernet1/0/19
!
interface FastEthernet1/0/20
!
interface FastEthernet1/0/21
!
interface FastEthernet1/0/22
!
interface FastEthernet1/0/23
```

```
!  
interface FastEthernet1/0/24  
!  
interface FastEthernet1/0/25  
!  
interface FastEthernet1/0/26  
!  
interface FastEthernet1/0/27  
!  
interface FastEthernet1/0/28  
!  
interface FastEthernet1/0/29  
!  
interface FastEthernet1/0/30  
!  
interface FastEthernet1/0/31  
!  
interface FastEthernet1/0/32  
!  
interface FastEthernet1/0/33  
!  
interface FastEthernet1/0/34  
!  
interface FastEthernet1/0/35  
!  
interface FastEthernet1/0/36  
!  
interface FastEthernet1/0/37  
!  
interface FastEthernet1/0/38  
!  
interface FastEthernet1/0/39  
!  
interface FastEthernet1/0/40  
!  
interface FastEthernet1/0/41  
!  
interface FastEthernet1/0/42  
!  
interface FastEthernet1/0/43  
!  
interface FastEthernet1/0/44  
!  
interface FastEthernet1/0/45  
!  
interface FastEthernet1/0/46  
!  
interface FastEthernet1/0/47  
!  
interface FastEthernet1/0/48  
!  
interface GigabitEthernet1/0/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
!  
interface GigabitEthernet1/0/2  
!  
interface GigabitEthernet1/0/3  
  description shut because of errors bart  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  shutdown  
!  
interface GigabitEthernet1/0/4
```

```

!
interface Vlan1
  no ip address
!
interface Vlan11
  description POS
  no ip address
!
interface Vlan12
  description DATA
  no ip address
!
interface Vlan13
  description VOICE
  no ip address
!
interface Vlan14
  description WIRELESS
  no ip address
!
interface Vlan15
  description WIRELESS POS
  no ip address
!
interface Vlan16
  description PARTNER
  no ip address
!
interface Vlan17
  description WIRELESS GUEST
  no ip address
!
interface Vlan18
  description LWAP
  no ip address
!
interface Vlan1000
  description MANAGEMENT
  ip address 10.10.63.13 255.255.255.0
!
ip classless
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group causer v3 auth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart

```

```

snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server host 192.168.42.134 version 3 auth <removed>
snmp-server host 192.168.42.134 <removed>
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  session-timeout 15  output
  exec-timeout 15 0
  privilege level 15
  login authentication RLOCAL
line vty 0 4
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
line vty 5 15
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0

```



```

logging synchronous
login authentication RETAIL
transport input ssh
!
ntp clock-period 36028315
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Medium Store Switch #1

```
----- show clock -----
```

```
13:44:49.223 PST Fri Dec 15 2006
```

```
----- show version -----
```

```

Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 12:34 by yenanh
Image text-base: 0x00003000, data-base: 0x00FF4334

ROM: Bootstrap program is C3560 boot loader
BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)

SMED-1 uptime is 3 weeks, 6 days, 19 hours, 30 minutes
System returned to ROM by power-on
System restarted at 18:15:17 PST Fri Nov 17 2006
System image file is "flash:c3560-ipbasek9-mz.122-25.SEE2.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```

cisco WS-C3560-48PS (PowerPC405) processor (revision M0) with 118784K/12280K bytes of
memory.
Processor board ID CAT1027RHBS
Last reset from power-on
12 Virtual Ethernet interfaces
48 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is disabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:0A:B8:C8:D8:80
Motherboard assembly number    : 73-9676-12

```

```

Power supply part number      : 341-0029-05
Motherboard serial number    : CAT10267XEW
Power supply serial number   : LIT102406MP
Model revision number        : M0
Motherboard revision number  : A0
Model number                  : WS-C3560-48PS-S
System serial number         : CAT1027RHBS
SFP Module assembly part number : 73-7757-03
SFP Module revision Number   : A0
SFP Module serial number     : CAT102681GX
Top Assembly Part Number     : 800-25859-03
Top Assembly Revision Number : G0
Version ID                    : V04
CLEI Code Number             : CNMV3N0CRC
Hardware Board Revision Number : 0x01

```

Switch	Ports	Model	SW Version	SW Image	
*	1	52	WS-C3560-48PS	12.2(25)SEE2	C3560-IPBASEK9-M

Configuration register is 0xF

----- show running-config -----

Building configuration...

Current configuration : 7190 bytes

```

!
! Last configuration change at 17:33:42 PST Tue Dec 12 2006 by bmcgloth
! NVRAM config last updated at 17:33:43 PST Tue Dec 12 2006 by bmcgloth
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname SMED-1
!
logging buffered 51200 debugging
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name retailpcilab.local
!
!

```

```
!  
!  
!  
!  
no file verify auto  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
interface Loopback0  
  no ip address  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
  switchport access vlan 18  
  switchport mode access  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
  switchport access vlan 18  
  switchport mode access  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24
```

```
!  
interface FastEthernet0/25  
!  
interface FastEthernet0/26  
!  
interface FastEthernet0/27  
!  
interface FastEthernet0/28  
!  
interface FastEthernet0/29  
!  
interface FastEthernet0/30  
!  
interface FastEthernet0/31  
!  
interface FastEthernet0/32  
!  
interface FastEthernet0/33  
!  
interface FastEthernet0/34  
!  
interface FastEthernet0/35  
!  
interface FastEthernet0/36  
!  
interface FastEthernet0/37  
!  
interface FastEthernet0/38  
!  
interface FastEthernet0/39  
!  
interface FastEthernet0/40  
!  
interface FastEthernet0/41  
!  
interface FastEthernet0/42  
!  
interface FastEthernet0/43  
!  
interface FastEthernet0/44  
!  
interface FastEthernet0/45  
!  
interface FastEthernet0/46  
!  
interface FastEthernet0/47  
!  
interface FastEthernet0/48  
!  
interface GigabitEthernet0/1  
description CONNECTION TO RMED1  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface GigabitEthernet0/2  
description CONNECTION TO SMED-2  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!  
interface GigabitEthernet0/3  
description CONNECTION TO RMED2  
switchport trunk encapsulation dot1q  
switchport mode trunk  
!
```

```
interface GigabitEthernet0/4
!
interface Vlan1
  no ip address
!
interface Vlan11
  description POS
  no ip address
!
interface Vlan12
  description DATA
  no ip address
!
interface Vlan13
  description VOICE
  no ip address
!
interface Vlan14
  description WIRELESS
  no ip address
!
interface Vlan15
  description WIRELESS POS
  no ip address
!
interface Vlan16
  description PARTNER
  no ip address
!
interface Vlan17
  description WIRELESS GUEST
  no ip address
!
interface Vlan18
  description LWAP
  no ip address
!
interface Vlan101
  description INTER ROUTER LINK
  no ip address
!
interface Vlan102
  description INTER ROUTER LINK
  no ip address
!
interface Vlan1000
  description MANAGEMENT
  ip address 10.10.47.11 255.255.255.0
!
ip default-gateway 10.10.47.1
ip classless
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
ip http authentication aaa exec-authorization RETAIL
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
```

```

access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps stpx root-inconsistency loop-inconsistency
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
 session-timeout 15 output
 exec-timeout 15 0
 privilege level 15
 login authentication RLOCAL
line vty 0 4
 session-timeout 15 output

```

```

access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
line vty 5 15
session-timeout 15 output
access-class 23 in
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport input ssh
!
ntp clock-period 36028255
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Medium Store Switch #2

```
----- show version -----
```

```

Cisco IOS Software, C3560 Software (C3560-IPBASEK9-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 12:34 by yenanh
Image text-base: 0x00003000, data-base: 0x00FF4334

ROM: Bootstrap program is C3560 boot loader
BOOTLDR: C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SE1, RELEASE SOFTWARE (fc)

SMED-2 uptime is 3 weeks, 6 days, 19 hours, 22 minutes
System returned to ROM by power-on
System restarted at 18:23:52 PST Fri Nov 17 2006
System image file is "flash:c3560-ipbasek9-mz.122-25.SEE2.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```

cisco WS-C3560G-48PS (PowerPC405) processor (revision C0) with 118784K/12280K bytes of
memory.
Processor board ID FOC0929U1UJ
Last reset from power-on
12 Virtual Ethernet interfaces
52 Gigabit Ethernet interfaces

```

The password-recovery mechanism is disabled.

```

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:14:A9:37:CA:00
Motherboard assembly number   : 73-9705-04
Power supply part number      : 341-0108-02
Motherboard serial number     : FOC092923N3
Power supply serial number    : DCA09240HNC
Model revision number        : C0
Motherboard revision number   : A0
Model number                  : WS-C3560G-48PS-E
System serial number         : FOC0929U1UJ
SFP Module assembly part number : 73-7757-03
SFP Module revision Number   : A0
SFP Module serial number     : CAT092512MV
Top Assembly Part Number     : 800-26346-02
Top Assembly Revision Number : A0
Version ID                   : 02
CLEI Code Number             : CNMWV00ARB
Hardware Board Revision Number : 0x05

```

Switch	Ports	Model	SW Version	SW Image
* 1	52	WS-C3560G-48PS	12.2 (25)SEE2	C3560-IPBASEK9-M

Configuration register is 0xF

----- show running-config -----

Building configuration...

```

Current configuration : 7483 bytes
!
! Last configuration change at 17:34:41 PST Tue Dec 12 2006 by bmcgloth
! NVRAM config last updated at 17:34:42 PST Tue Dec 12 2006 by bmcgloth
!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname SMED-2
!
logging buffered 51200 debugging
enable secret 5 <removed>
!
username cisco privilege 15 secret 5 <removed>
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone PST -8

```



```
clock summer-time PSTDST recurring
ip subnet-zero
ip domain-name RETAILPCILAB.LOCAL
ip name-server 192.168.42.130
!
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface GigabitEthernet0/1
  switchport access vlan 11
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet0/2
  switchport access vlan 11
!
interface GigabitEthernet0/3
  switchport access vlan 11
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
  switchport access vlan 11
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
```

```
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface GigabitEthernet0/25
!
interface GigabitEthernet0/26
!
interface GigabitEthernet0/27
!
interface GigabitEthernet0/28
!
interface GigabitEthernet0/29
!
interface GigabitEthernet0/30
!
interface GigabitEthernet0/31
!
interface GigabitEthernet0/32
!
interface GigabitEthernet0/33
!
interface GigabitEthernet0/34
!
interface GigabitEthernet0/35
!
interface GigabitEthernet0/36
!
interface GigabitEthernet0/37
!
interface GigabitEthernet0/38
!
interface GigabitEthernet0/39
!
interface GigabitEthernet0/40
!
interface GigabitEthernet0/41
!
interface GigabitEthernet0/42
!
interface GigabitEthernet0/43
!
interface GigabitEthernet0/44
!
interface GigabitEthernet0/45
!
interface GigabitEthernet0/46
!
interface GigabitEthernet0/47
!
interface GigabitEthernet0/48
!
interface GigabitEthernet0/49
description CONNECTION TO RMED-1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/50
```

```
description CONNECTION TO SMED-1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/51
description CONNECTION TO RMED-2
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/52
!
interface Vlan1
no ip address
shutdown
!
interface Vlan11
description POS
no ip address
!
interface Vlan12
description DATA
no ip address
!
interface Vlan13
description VOICE
no ip address
!
interface Vlan14
description WIRELESS
no ip address
!
interface Vlan15
description WIRELESS POS
no ip address
!
interface Vlan16
description PARTNER
no ip address
!
interface Vlan17
description WIRELESS GUEST
no ip address
!
interface Vlan18
description LWAP
no ip address
!
interface Vlan101
description INTER ROUTER LINK
no ip address
!
interface Vlan102
description INTER ROUTER LINK
no ip address
!
interface Vlan1000
description MANAGEMENT
ip address 10.10.47.12 255.255.255.0
!
ip default-gateway 10.10.47.1
ip classless
no ip http server
ip http access-class 23
ip http authentication aaa login-authentication RETAIL
```

```

ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip tacacs source-interface Vlan1000
!
logging source-interface Vlan1000
logging 192.168.42.134
logging 192.168.42.121
access-list 23 permit 192.168.42.0 0.0.0.255
access-list 23 deny any log
access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server trap-source Vlan1000
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server enable traps stpx root-inconsistency loop-inconsistency
snmp-server host 192.168.42.134 <removed>
tacacs-server host 192.168.42.131
no tacacs-server directed-request
tacacs-server key 7 <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:

```

```

THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  session-timeout 15  output
  exec-timeout 15 0
  privilege level 15
  login authentication RLOCAL
line vty 0 4
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
line vty 5 15
  session-timeout 15  output
  access-class 23 in
  exec-timeout 15 0
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
ntp clock-period 36028353
ntp source Vlan1000
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Large Store Wireless Controller

```
(AW-LRG-1_Controller) >show run-config
```

```
Press Enter to continue...
```

```

System Inventory
Burned-in MAC Address..... 00:18:73:36:A0:00
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK

```

```
Press Enter to continue Or <Ctl Z> to abort
```

```

System Information
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.0.179.11
RTOS Version..... 4.0.179.11
Bootloader Version..... 4.0.179.11
Build Type..... DATA + WPS

System Name..... AW-LRG-1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.10.55.5
System Up Time..... 0 days 3 hrs 44 mins 38 secs

Configured Country..... United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +39 C

```

```

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 3
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 2
Burned-in MAC Address..... 00:18:73:36:A0:00
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK

```

Press Enter to continue Or <Ctl Z> to abort

```

Switch Configuration
802.3x Flow Control Mode..... Disable
Current LWAPP Transport Mode..... Layer 3
LWAPP Transport Mode after next switch reboot.... Layer 3
FIPS prerequisite features..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort

```

Network Information
RF-Network Name..... PCI_Large
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Disable
Ethernet Multicast Mode..... Disable Mode: Ucast
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge AP Zero Config..... Enable
Bridge Shared Secret..... youshouldsetme
Allow Old Bridging Aps To Authenticate..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
Apple Talk ..... Disable
AP Fallback ..... Enable
Web Auth Redirect Ports ..... 80
Fast SSID Change ..... Disabled
802.3 Bridging ..... Disable

```

Press Enter to continue Or <Ctl Z> to abort

```

Port Summary

```

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	Mcast Appliance	POE
1	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	Enable	N/A
2	Normal	Disa	Enable	Auto	1000 Full	Down	Enable	Enable	N/A

Press Enter to continue Or <Ctl Z> to abort

```

AP Summary

```

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP000a.b812.3182	2	AIR-LAP1131AG-A-K9	00:0a:b8:12:31:82	default location	1

Press Enter to continue Or <Ctl Z> to abort

```

AP Config
Cisco AP Identifier..... 0
Cisco AP Name..... AP000a.b812.3182
AP Regulatory Domain..... -A
Switch Port Number ..... 1

```

```

MAC Address..... 00:0a:b8:12:31:82
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.55.40
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.55.1
Cisco AP Location..... default location
Cisco AP Group Name..... none
Primary Cisco Switch..... AW-LRG-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA
Reset Button..... Enabled
AP Serial Number..... FTX1027T1X1
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

```

Attributes for Slot 0

```

Radio Type..... RADIO_TYPE_80211g
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

```

Station Configuration

```

Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:17:df:7e:5f:70
Operation Rate Set
  1000 Kilo Bits..... MANDATORY
  2000 Kilo Bits..... MANDATORY
  5500 Kilo Bits..... MANDATORY
  11000 Kilo Bits..... MANDATORY
  6000 Kilo Bits..... SUPPORTED
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... SUPPORTED
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... SUPPORTED
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

```

```

Multi Domain Capability
  Configuration ..... AUTOMATIC
  First Chan Num ..... 1
  Number Of Channels ..... 11

MAC Operation Parameters
  Configuration ..... AUTOMATIC
  RTS Threshold ..... 2347
  Short Retry Limit ..... 7
  Long Retry Limit ..... 4
  Fragmentation Threshold ..... 2346
  Maximum Tx MSDU Life Time ..... 512
  Maximum Rx Life Time ..... 512

Tx Power
  Num Of Supported Power Levels ..... 8
  Tx Power Level 1 ..... 20 dBm
  Tx Power Level 2 ..... 17 dBm
  Tx Power Level 3 ..... 14 dBm
  Tx Power Level 4 ..... 11 dBm
  Tx Power Level 5 ..... 8 dBm
  Tx Power Level 6 ..... 5 dBm
  Tx Power Level 7 ..... 2 dBm
  Tx Power Level 8 ..... -1 dBm
  Tx Power Configuration ..... AUTOMATIC
  Current Tx Power Level ..... 1

Phy OFDM parameters
  Configuration ..... AUTOMATIC
  Current Channel ..... 11
  TI Threshold ..... -50
  Antenna Type..... INTERNAL_ANTENNA
  Internal Antenna Gain (in .5 dBm units).... 8
  Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters
  Configuration ..... AUTOMATIC
  Interference threshold..... 10 %
  Noise threshold..... -70 dBm
  RF utilization threshold..... 80 %
  Data-rate threshold..... 1000000 bps
  Client threshold..... 12 clients
  Coverage SNR threshold..... 12 dB
  Coverage exception level..... 25 %
  Client minimum exception level..... 3 clients
Rogue Containment Information
  Containment Count..... 0

Cisco AP Identifier..... 0
Cisco AP Name..... AP000a.b812.3182
AP Regulatory Domain..... -A
Switch Port Number ..... 1
MAC Address..... 00:0a:b8:12:31:82
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.55.40
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.55.1
Cisco AP Location..... default location
Cisco AP Group Name..... none
Primary Cisco Switch..... AW-LRG-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED

```



```

Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA
Reset Button..... Enabled
AP Serial Number..... FTX1027T1X1
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

```

Attributes for Slot 1

```

Radio Type..... RADIO_TYPE_80211a
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

```

Station Configuration

```

Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:17:df:7e:5f:70
Operation Rate Set
  6000 Kilo Bits..... MANDATORY
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... MANDATORY
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... MANDATORY
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

```

Multi Domain Capability

```

Configuration ..... AUTOMATIC
First Chan Num ..... 36
Number Of Channels ..... 4

```

MAC Operation Parameters

```

Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

```

Tx Power

```

Num Of Supported Power Levels ..... 8

```

```

Tx Power Level 1 ..... 17 dBm
Tx Power Level 2 ..... 15 dBm
Tx Power Level 3 ..... 14 dBm
Tx Power Level 4 ..... 11 dBm
Tx Power Level 5 ..... 8 dBm
Tx Power Level 6 ..... 5 dBm
Tx Power Level 7 ..... 2 dBm
Tx Power Level 8 ..... -1 dBm
Tx Power Configuration ..... AUTOMATIC
Current Tx Power Level ..... 1

Phy OFDM parameters
Configuration ..... AUTOMATIC
Current Channel ..... 64
TI Threshold ..... -50
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units)... 8
Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters
Configuration ..... AUTOMATIC
Interference threshold..... 10 %
Noise threshold..... -70 dBm
RF utilization threshold..... 80 %
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 16 dB
Coverage exception level..... 25 %
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

Press Enter to continue Or <Ctl Z> to abort
AP Airewave Director Configuration
Number Of Slots..... 2
AP Name..... AP000a.b812.3182
MAC Address..... 00:0a:b8:12:31:82
Radio Type..... RADIO_TYPE_80211b/g
Noise Information
Noise Profile..... PASSED
Channel 1..... -90 dBm
Channel 2..... -86 dBm
Channel 3..... -90 dBm
Channel 4..... -88 dBm
Channel 5..... -87 dBm
Channel 6..... -86 dBm
Channel 7..... -88 dBm
Channel 8..... -87 dBm
Channel 9..... -89 dBm
Channel 10..... -88 dBm
Channel 11..... -86 dBm
Interference Information
Interference Profile..... PASSED
Channel 1..... -51 dBm @ 6 % busy
Channel 2..... -39 dBm @ 1 % busy
Channel 3..... -128 dBm @ 0 % busy
Channel 4..... -128 dBm @ 0 % busy
Channel 5..... -52 dBm @ 4 % busy
Channel 6..... -49 dBm @ 12 % busy
Channel 7..... -44 dBm @ 1 % busy
Channel 8..... -52 dBm @ 1 % busy
Channel 9..... -60 dBm @ 1 % busy
Channel 10..... -128 dBm @ 0 % busy

```

```

Channel 11..... -128 dBm @ 0 % busy
Load Information
Load Profile..... PASSED
Receive Utilization..... 3 %
Transmit Utilization..... 2 %
Channel Utilization..... 0 %
Attached Clients..... 2 clients
Coverage Information
Coverage Profile..... PASSED
Failed Clients..... 0 clients
Client Signal Strengths
RSSI -100 dbm..... 0 clients
RSSI -92 dbm..... 0 clients
RSSI -84 dbm..... 0 clients
RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 2 clients
Client Signal To Noise Ratios
SNR 0 dbm..... 0 clients
SNR 5 dbm..... 0 clients
SNR 10 dbm..... 0 clients
SNR 15 dbm..... 0 clients
SNR 20 dbm..... 0 clients
SNR 25 dbm..... 0 clients
SNR 30 dbm..... 0 clients
SNR 35 dbm..... 0 clients
SNR 40 dbm..... 0 clients
SNR 45 dbm..... 2 clients
Nearby APs
Radar Information
Channel Assignment Information
Current Channel Average Energy..... unknown
Previous Channel Average Energy..... unknown
Channel Change Count..... 0
Last Channel Change Time..... Fri Dec 15 18:16:27 2006
Recommendd Best Channel..... 11
RF Parameter Recommendations
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0
Number Of Slots..... 2
AP Name..... AP000a.b812.3182
MAC Address..... 00:0a:b8:12:31:82
Radio Type..... RADIO_TYPE_80211a
Noise Information
Noise Profile..... PASSED
Channel 36..... -91 dBm
Channel 40..... -92 dBm
Channel 44..... -92 dBm
Channel 48..... -93 dBm
Channel 52..... -93 dBm
Channel 56..... -94 dBm
Channel 60..... -89 dBm
Channel 64..... -94 dBm
Channel 149..... -91 dBm
Channel 153..... -94 dBm
Channel 157..... -94 dBm
Channel 161..... -94 dBm
Channel 165..... -93 dBm
Channel 190..... -98 dBm
Interference Information
Interference Profile..... PASSED

```

```

Channel 36..... -128 dBm @ 0 % busy
Channel 40..... -128 dBm @ 0 % busy
Channel 44..... -128 dBm @ 0 % busy
Channel 48..... -128 dBm @ 0 % busy
Channel 52..... -128 dBm @ 0 % busy
Channel 56..... -128 dBm @ 0 % busy
Channel 60..... -128 dBm @ 0 % busy
Channel 64..... -128 dBm @ 0 % busy
Channel 149..... -128 dBm @ 0 % busy
Channel 153..... -128 dBm @ 0 % busy
Channel 157..... -128 dBm @ 0 % busy
Channel 161..... -128 dBm @ 0 % busy
Channel 165..... -128 dBm @ 0 % busy
Channel 190..... -128 dBm @ 0 % busy
Load Information
Load Profile..... PASSED
Receive Utilization..... 0 %
Transmit Utilization..... 0 %
Channel Utilization..... 0 %
Attached Clients..... 0 clients
Coverage Information
Coverage Profile..... PASSED
Failed Clients..... 0 clients
Client Signal Strengths
RSSI -100 dbm..... 0 clients
RSSI -92 dbm..... 0 clients
RSSI -84 dbm..... 0 clients
RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
SNR 0 dbm..... 0 clients
SNR 5 dbm..... 0 clients
SNR 10 dbm..... 0 clients
SNR 15 dbm..... 0 clients
SNR 20 dbm..... 0 clients
SNR 25 dbm..... 0 clients
SNR 30 dbm..... 0 clients
SNR 35 dbm..... 0 clients
SNR 40 dbm..... 0 clients
SNR 45 dbm..... 0 clients
Nearby APs
Radar Information
Channel Assignment Information
Current Channel Average Energy..... unknown
Previous Channel Average Energy..... unknown
Channel Change Count..... 0
Last Channel Change Time..... Fri Dec 15 18:16:27 2006
Recommendd Best Channel..... 64
RF Parameter Recommendations
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0

Press Enter to continue Or <Ctl Z> to abort
802.11A Configuration
802.11a Network..... Enabled
    802.11a Low Band..... Enabled
    802.11a Mid Band..... Enabled
    802.11a High Band..... Enabled
802.11a Operational Rates
    802.11a 6M Rate..... Mandatory
    
```

```

802.11a 9M Rate..... Supported
802.11a 12M Rate..... Mandatory
802.11a 18M Rate..... Supported
802.11a 24M Rate..... Mandatory
802.11a 36M Rate..... Supported
802.11a 48M Rate..... Supported
802.11a 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mandatory..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 36
Default Tx Power Level..... 1
DTPC Status..... Enabled
DTIM Period..... 1
Fragmentation Threshold..... 2346
Long Retry Limit..... 4
Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
Pico-Cell Status..... Disabled
RTS Threshold..... 2347
Short Retry Limit..... 7
TI Threshold..... -50
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

```

Press Enter to continue Or <Ctl Z> to abort

802.11A Advanced Configuration

AP Name	Channel	TxPower Level
AP000a.b812.3182	64*	1*

Press Enter to continue Or <Ctl Z> to abort

802.11A Airewave Director Configuration

RF Event and Performance Logging

```

Channel Update Logging..... Off
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
TxPower Update Logging..... Off

```

Default 802.11a AP performance profiles

```

802.11a Global Interference threshold..... 10 %
802.11a Global noise threshold..... -70 dBm
802.11a Global RF utilization threshold..... 80 %
802.11a Global throughput threshold..... 1000000 bps
802.11a Global clients threshold..... 12 clients
802.11a Global coverage threshold..... 16 dB
802.11a Global coverage exception level..... 25 %
802.11a Global client minimum exception lev.... 3 clients

```

Default 802.11a AP monitoring

```

802.11a Monitor Mode..... enable
802.11a Monitor Channels..... Country channels
802.11a AP Coverage Interval..... 180 seconds
802.11a AP Load Interval..... 60 seconds

```

```

802.11a AP Noise Interval..... 180 seconds
802.11a AP Signal Strength Interval..... 60 seconds
Automatic Transmit Power Assignment
Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:18:73:36:a0:00
Last Run..... 165 seconds ago
Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:18:73:36:a0:00
Last Run..... 165 seconds ago
Channel Energy Levels
Minimum..... unknown
Average..... unknown
Maximum..... unknown
Channel Dwell Times
Minimum..... 0 days, 03 h 43 m 46 s
Average..... 0 days, 03 h 43 m 46 s
Maximum..... 0 days, 03 h 43 m 46 s
Allowed Channel List..... 36,40,44,48,52,56,60,64,149,
..... 153,157,161
Radio RF Grouping
802.11a Group Mode..... AUTO
802.11a Group Update Interval..... 600 seconds
802.11a Group Leader..... 00:18:73:36:a0:00
802.11a Group Member..... 00:18:73:36:a0:00
802.11a Last Run..... 165 seconds ago

Press Enter to continue Or <Ctl Z> to abort
802.11B Configuration
802.11b Network..... Enabled
11gSupport..... Enabled
802.11b/g Operational Rates
802.11b/g 1M Rate..... Mandatory
802.11b/g 2M Rate..... Mandatory
802.11b/g 5.5M Rate..... Mandatory
802.11b/g 11M Rate..... Mandatory
802.11g 6M Rate..... Supported
802.11g 9M Rate..... Supported
802.11g 12M Rate..... Supported
802.11g 18M Rate..... Supported
802.11g 24M Rate..... Supported
802.11g 36M Rate..... Supported
802.11g 48M Rate..... Supported
802.11g 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mode..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 1
Default Tx Power Level..... 1
DTPC Status..... Enabled
Call Admission Limit ..... 105
G711 CU Quantum ..... 15
DTIM Period..... 1
ED Threshold..... -50
Fragmentation Threshold..... 2346
Long Retry Limit..... 4

```

```

Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
PBCC mandatory..... Disabled
Pico-Cell Status..... Disabled
RTS Threshold..... 2347
Short Preamble mandatory..... Enabled
Short Retry Limit..... 7
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

```

Press Enter to continue Or <Ctl Z> to abort

802.11B Advanced Configuration

AP Name	Channel	TxPower Level
AP000a.b812.3182	11*	1*

Press Enter to continue Or <Ctl Z> to abort

802.11B Airewave Director Configuration

RF Event and Performance Logging

```

Channel Update Logging..... Off
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
Transmit Power Update Logging..... Off

```

Default 802.11b AP performance profiles

```

802.11b Global Interference threshold..... 10 %
802.11b Global noise threshold..... -70 dBm
802.11b Global RF utilization threshold..... 80 %
802.11b Global throughput threshold..... 1000000 bps
802.11b Global clients threshold..... 12 clients
802.11b Global coverage threshold..... 12 dB
802.11b Global coverage exception level..... 25 %
802.11b Global client minimum exception lev... 3 clients

```

Default 802.11b AP monitoring

```

802.11b Monitor Mode..... enable
802.11b Monitor Channels..... Country channels
802.11b AP Coverage Interval..... 180 seconds
802.11b AP Load Interval..... 60 seconds
802.11b AP Noise Interval..... 180 seconds
802.11b AP Signal Strength Interval..... 60 seconds

```

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:18:73:36:a0:00
Last Run..... 156 seconds ago

```

Automatic Channel Assignment

```

Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:18:73:36:a0:00
Last Run..... 156 seconds ago
Channel Energy Levels

```

```

Minimum..... unknown
Average..... unknown
Maximum..... unknown
Channel Dwell Times
Minimum..... 0 days, 03 h 43 m 46 s
Average..... 0 days, 03 h 43 m 46 s
Maximum..... 0 days, 03 h 43 m 46 s
Allowed Channel List..... 1,6,11
Radio RF Grouping
802.11b Group Mode..... AUTO
802.11b Group Update Interval..... 600 seconds
802.11b Group Leader..... 00:18:73:36:a0:00
802.11b Group Member..... 00:18:73:36:a0:00
802.11b Last Run..... 156 seconds ago

```

```

Press Enter to continue Or <Ctl Z> to abort
Mobility Configuration
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... PCI_Large
Mobility Group members configured..... 1

```

```

Switches configured in the Mobility Group
MAC Address      IP Address      Group Name
00:18:73:36:a0:00  10.10.55.5      <local>

```

```

Press Enter to continue Or <Ctl Z> to abort
Interface Configuration
Interface Name..... ap-manager
IP Address..... 10.10.55.6
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.55.1
VLAN..... 18
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... Yes

```

```

Interface Name..... management
MAC Address..... 00:18:73:36:a0:00
IP Address..... 10.10.55.5
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.55.1
VLAN..... 18
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```

```

Interface Name..... service-port
MAC Address..... 00:18:73:36:a0:01
IP Address..... 10.10.63.100
IP Netmask..... 255.255.255.0
DHCP Option 82..... Disabled
DHCP Protocol..... Disabled
AP Manager..... No

```



```

Interface Name..... virtual
IP Address..... 1.1.1.1
DHCP Option 82..... Disabled
Virtual DNS Host Name..... Disabled
AP Manager..... No

Interface Name..... wireless
IP Address..... 10.10.51.5
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.51.1
VLAN..... 14
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

Interface Name..... wirelessguest
IP Address..... 10.10.54.5
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.54.1
VLAN..... 17
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

Interface Name..... wirelesspos
IP Address..... 10.10.52.5
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.52.1
VLAN..... 15
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```

Press Enter to continue Or <Ctl Z> to abort
WLAN Configuration

```

WLAN Identifier..... 1
Network Name (SSID)..... Wireless
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds

```

```

Session Timeout..... Infinity
Interface..... wireless
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Enabled
      AES Cipher..... Disabled
    WPA2 (RSN IE)..... Disabled
    Auth Key Management
      802.1x..... Enabled
      PSK..... Disabled
      CCKM..... Disabled
  CKIP ..... Disabled
  IP Security..... Disabled
  IP Security Passthru..... Disabled
  L2TP..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  Cranite Passthru..... Disabled
  Fortress Passthru..... Disabled
  H-REAP Local Switching..... Disabled
  Management Frame Protection..... Enabled (Global MFP Disabled)

WLAN Identifier..... 2
Network Name (SSID)..... WirelessPOS
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 2
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wirelesspos
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers

```

```

Authentication..... 192.168.42.131 1812
Security

    802.11 Authentication:..... Open System
    Static WEP Keys..... Disabled
    802.1X..... Disabled
    Wi-Fi Protected Access (WPA/WPA2)..... Enabled
        WPA (SSN IE)..... Enabled
            TKIP Cipher..... Enabled
            AES Cipher..... Disabled
        WPA2 (RSN IE)..... Disabled
    Auth Key Management
        802.1x..... Enabled
        PSK..... Disabled
        CCKM..... Disabled
    CKIP ..... Disabled
    IP Security..... Disabled
    IP Security Passthru..... Disabled
    L2TP..... Disabled
    Web Based Authentication..... Disabled
    Web-Passthrough..... Disabled
    Auto Anchor..... Disabled
    Cranite Passthru..... Disabled
    Fortress Passthru..... Disabled
    H-REAP Local Switching..... Enabled
    Management Frame Protection..... Enabled (Global MFP Disabled)

WLAN Identifier..... 3
Network Name (SSID)..... WirelessGuest
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wirelessguest
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Security

    802.11 Authentication:..... Open System
    Static WEP Keys..... Disabled
    802.1X..... Disabled
    Wi-Fi Protected Access (WPA/WPA2)..... Enabled
        WPA (SSN IE)..... Enabled
            TKIP Cipher..... Enabled
            AES Cipher..... Disabled
        WPA2 (RSN IE)..... Disabled
    Auth Key Management
        802.1x..... Enabled
        PSK..... Disabled
        CCKM..... Disabled
    CKIP ..... Disabled

```

```

IP Security..... Disabled
IP Security Passthru..... Disabled
L2TP..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Auto Anchor..... Disabled
Cranite Passthru..... Disabled
Fortress Passthru..... Disabled
H-REAP Local Switching..... Disabled
Management Frame Protection..... Enabled (Global MFP Disabled)

```

Press Enter to continue Or <Ctl Z> to abort
 ACL Configuration

Press Enter to continue Or <Ctl Z> to abort
 CPU ACL Configuration

```

CPU Acl Name..... NOT CONFIGURED
Wireless Traffic..... Disabled
Wired Traffic..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort

```

RADIUS Configuration
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled

```

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	RFC3576	IPSec
AuthMode/Phase1/Group/Lifetime/Auth/Encr							
1	NM	192.168.42.131	1812	Enabled	2	Disabled	Disabled
none/unknown/group-0/0 none/none							

Accounting Servers

Index	Type	Server Address	Port	State	Tout	RFC-3576	IPSec
AuthMode/Phase1/Group/Lifetime/Auth/Encr							

Press Enter to continue Or <Ctl Z> to abort

Route Info
 Number of Routes..... 0

Destination Network	Genmask	Gateway

Press Enter to continue Or <Ctl Z> to abort

```

Qos Queue Length Info
Platinum queue length..... 100
Gold queue length..... 75
Silver queue length..... 50
Bronze queue length..... 25

```

Press Enter to continue Or <Ctl Z> to abort

Mac Filter Info

```

Press Enter to continue Or <Ctl Z> to abort
Load Balancing Info
Aggressive Load Balancing..... Enabled
Aggressive Load Balancing Window..... 0 clients

Press Enter to continue Or <Ctl Z> to abort
Dhcp Scope Info

Press Enter to continue Or <Ctl Z> to abort
Exclusion List ConfigurationUnable to retrieve exclusion-list entry

Press Enter to continue Or <Ctl Z> to abort
CDP Configuration

Press Enter to continue Or <Ctl Z> to abort
WPS Configuration Summary

Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled

Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
  Enforced encryption policy..... none
  Enforced preamble policy..... none
  Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120

Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
  RLDP Action..... Alarm Only
  Rogue APs
    Rogues AP advertising my SSID..... Alarm Only
    Detect and report Ad-Hoc Networks..... Enabled
  Rogue Clients
    Validate rogue clients against AAA..... Disabled
    Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1200

Signature Policy
  Signature Processing..... Enabled

Press Enter to continue Or <Ctl Z> to abort
Spanning Tree Switch Configuration

STP Specification..... IEEE 802.1D
STP Base MAC Address..... 00:18:73:36:A0:00
Spanning Tree Algorithm..... Disable
STP Bridge Priority..... 32768
STP Bridge Max. Age (seconds)..... 20
STP Bridge Hello Time (seconds)..... 2
STP Bridge Forward Delay (seconds)..... 15

```

```

Press Enter to continue Or <Ctl Z> to abort
Spanning Tree Port Configuration

STP Port ID..... 8001
STP Port State..... Forwarding
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 4
STP Port Path Cost Mode..... Auto

STP Port ID..... 8002
STP Port State..... Disabled
STP Port Administrative Mode..... 802.1D
STP Port Priority..... 128
STP Port Path Cost..... 4
STP Port Path Cost Mode..... Auto

(AW-LRG-1_Controller) >

```

Medium Store Wireless Controller

```

(AW-MED-1_Controller) >show run-config

Press Enter to continue...
System Inventory
Burned-in MAC Address..... 00:15:2C:E8:74:60

Press Enter to continue Or <Ctl Z> to abort
System Information
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.0.179.11
RTOS Version..... 4.0.179.11
Bootloader Version..... 4.0.179.11
Build Type..... DATA + WPS

System Name..... AW-MED-1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.5
IP Address..... 10.10.46.34
System Up Time..... 7 days 6 hrs 40 mins 2 secs

Configured Country..... United States

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 3
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 0
Burned-in MAC Address..... 00:15:2C:E8:74:60

Press Enter to continue Or <Ctl Z> to abort
Switch Configuration
802.3x Flow Control Mode..... Disable
Current LWAPP Transport Mode..... Layer 3
LWAPP Transport Mode after next switch reboot.... Layer 3
FIPS prerequisite features..... Disabled

```

```

Press Enter to continue Or <Ctl Z> to abort
Network Information
RF-Network Name..... PCI_medium
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Disable
Ethernet Multicast Mode..... Disable   Mode: Ucast
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge AP Zero Config..... Enable
Bridge Shared Secret..... youshouldsetme
Allow Old Bridging Aps To Authenticate..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
AP Fallback ..... Enable
Web Auth Redirect Ports ..... 80
Fast SSID Change ..... Disabled
802.3 Bridging ..... Disable

```

Press Enter to continue Or <Ctl Z> to abort

Port Summary

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap
1	Normal	Forw	Enable	Auto	100 Full	Up	Enable

Press Enter to continue Or <Ctl Z> to abort

AP Summary

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP000a.b812.2cda	2	AIR-LAP1131AG-A-K9	00:0a:b8:12:2c:da	default location	1

Press Enter to continue Or <Ctl Z> to abort

AP Config

```

Cisco AP Identifier..... 3
Cisco AP Name..... AP000a.b812.2cda
AP Regulatory Domain..... -A
Switch Port Number ..... 1
MAC Address..... 00:0a:b8:12:2c:da
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.39.20
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.39.1
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch.....
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled

```

```

PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA
Reset Button..... Enabled
AP Serial Number..... FTX1027T1X2
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

```

Attributes for Slot 0

```

Radio Type..... RADIO_TYPE_80211g
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

```

Station Configuration

```

Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:17:df:7e:3a:30
Operation Rate Set
  1000 Kilo Bits..... MANDATORY
  2000 Kilo Bits..... MANDATORY
  5500 Kilo Bits..... MANDATORY
  11000 Kilo Bits..... MANDATORY
  6000 Kilo Bits..... SUPPORTED
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... SUPPORTED
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... SUPPORTED
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

```

Multi Domain Capability

```

Configuration ..... AUTOMATIC
First Chan Num ..... 1
Number Of Channels ..... 11

```

MAC Operation Parameters

```

Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

```

Tx Power

```

Num Of Supported Power Levels ..... 8
Tx Power Level 1 ..... 20 dBm
Tx Power Level 2 ..... 17 dBm
Tx Power Level 3 ..... 14 dBm
Tx Power Level 4 ..... 11 dBm

```



```

Tx Power Level 5 ..... 8 dBm
Tx Power Level 6 ..... 5 dBm
Tx Power Level 7 ..... 2 dBm
Tx Power Level 8 ..... -1 dBm
Tx Power Configuration ..... AUTOMATIC
Current Tx Power Level ..... 1

Phy OFDM parameters
Configuration ..... AUTOMATIC
Current Channel ..... 1
TI Threshold ..... -50
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units).... 8
Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters
Configuration ..... AUTOMATIC
Interference threshold..... 10 %
Noise threshold..... -70 dBm
RF utilization threshold..... 80 %
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 12 dB
Coverage exception level..... 25 %
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

Cisco AP Identifier..... 3
Cisco AP Name..... AP000a.b812.2cda
AP Regulatory Domain..... -A
Switch Port Number ..... 1
MAC Address..... 00:0a:b8:12:2c:da
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.39.20
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.39.1
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch.....
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA
Reset Button..... Enabled
AP Serial Number..... FTX1027T1X2
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

Attributes for Slot 1
Radio Type..... RADIO_TYPE_80211a

```

```

Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

Station Configuration
Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:17:df:7e:3a:30
Operation Rate Set
  6000 Kilo Bits..... MANDATORY
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... MANDATORY
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... MANDATORY
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

Multi Domain Capability
Configuration ..... AUTOMATIC
First Chan Num ..... 36
Number Of Channels ..... 4

MAC Operation Parameters
Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

Tx Power
Num Of Supported Power Levels ..... 8
Tx Power Level 1 ..... 17 dBm
Tx Power Level 2 ..... 15 dBm
Tx Power Level 3 ..... 14 dBm
Tx Power Level 4 ..... 11 dBm
Tx Power Level 5 ..... 8 dBm
Tx Power Level 6 ..... 5 dBm
Tx Power Level 7 ..... 2 dBm
Tx Power Level 8 ..... -1 dBm
Tx Power Configuration ..... AUTOMATIC
Current Tx Power Level ..... 1

Phy OFDM parameters
Configuration ..... AUTOMATIC
Current Channel ..... 149
TI Threshold ..... -50
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units).... 8
Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters

```

```

Configuration ..... AUTOMATIC
Interference threshold..... 10 %
Noise threshold..... -70 dBm
RF utilization threshold..... 80 %
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 16 dB
Coverage exception level..... 25 %
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

```

Press Enter to continue Or <Ctl Z> to abort

AP Airewave Director Configuration

```

Number Of Slots..... 2
AP Name..... AP000a.b812.2cda
MAC Address..... 00:0a:b8:12:2c:da
Radio Type..... RADIO_TYPE_80211b/g
Noise Information
  Noise Profile..... PASSED
Interference Information
  Interference Profile..... PASSED
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0 %
  Transmit Utilization..... 0 %
  Channel Utilization..... 0 %
  Attached Clients..... 0 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dbm..... 0 clients
  RSSI -92 dbm..... 0 clients
  RSSI -84 dbm..... 0 clients
  RSSI -76 dbm..... 0 clients
  RSSI -68 dbm..... 0 clients
  RSSI -60 dbm..... 0 clients
  RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
  SNR 0 dbm..... 0 clients
  SNR 5 dbm..... 0 clients
  SNR 10 dbm..... 0 clients
  SNR 15 dbm..... 0 clients
  SNR 20 dbm..... 0 clients
  SNR 25 dbm..... 0 clients
  SNR 30 dbm..... 0 clients
  SNR 35 dbm..... 0 clients
  SNR 40 dbm..... 0 clients
  SNR 45 dbm..... 0 clients
Nearby APs
Radar Information
Channel Assignment Information
  Current Channel Average Energy..... unknown
  Previous Channel Average Energy..... unknown
  Channel Change Count..... 0
  Last Channel Change Time..... Fri Dec 15 22:03:36 2006
  Recommndd Best Channel..... 1
RF Parameter Recommendations
  Power Level..... 1
  RTS/CTS Threshold..... 2347
  Fragmentation Threshold..... 2346
  Antenna Pattern..... 0

```

```

Number Of Slots..... 2
AP Name..... AP000a.b812.2cda
MAC Address..... 00:0a:b8:12:2c:da
Radio Type..... RADIO_TYPE_80211a
Noise Information
  Noise Profile..... PASSED
Interference Information
  Interference Profile..... PASSED
Load Information
  Load Profile..... PASSED
  Receive Utilization..... 0 %
  Transmit Utilization..... 0 %
  Channel Utilization..... 0 %
  Attached Clients..... 0 clients
Coverage Information
  Coverage Profile..... PASSED
  Failed Clients..... 0 clients
Client Signal Strengths
  RSSI -100 dbm..... 0 clients
  RSSI -92 dbm..... 0 clients
  RSSI -84 dbm..... 0 clients
  RSSI -76 dbm..... 0 clients
  RSSI -68 dbm..... 0 clients
  RSSI -60 dbm..... 0 clients
  RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
  SNR 0 dbm..... 0 clients
  SNR 5 dbm..... 0 clients
  SNR 10 dbm..... 0 clients
  SNR 15 dbm..... 0 clients
  SNR 20 dbm..... 0 clients
  SNR 25 dbm..... 0 clients
  SNR 30 dbm..... 0 clients
  SNR 35 dbm..... 0 clients
  SNR 40 dbm..... 0 clients
  SNR 45 dbm..... 0 clients
Nearby APs
Radar Information
Channel Assignment Information
  Current Channel Average Energy..... unknown
  Previous Channel Average Energy..... unknown
  Channel Change Count..... 0
  Last Channel Change Time..... Fri Dec 15 22:03:36 2006
  Recommendd Best Channel..... 149
RF Parameter Recommendations
  Power Level..... 1
  RTS/CTS Threshold..... 2347
  Fragmentation Threshold..... 2346
  Antenna Pattern..... 0

Press Enter to continue Or <Ctl Z> to abort
802.11A Configuration
802.11a Network..... Enabled
  802.11a Low Band..... Enabled
  802.11a Mid Band..... Enabled
  802.11a High Band..... Enabled
802.11a Operational Rates
  802.11a 6M Rate..... Mandatory
  802.11a 9M Rate..... Supported
  802.11a 12M Rate..... Mandatory
  802.11a 18M Rate..... Supported
  802.11a 24M Rate..... Mandatory
  802.11a 36M Rate..... Supported
  802.11a 48M Rate..... Supported

```

```

      802.11a 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mandatory..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 36
Default Tx Power Level..... 1
DTPC Status..... Enabled
DTIM Period..... 1
Fragmentation Threshold..... 2346
Long Retry Limit..... 4
Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
Pico-Cell Status..... Disabled
RTS Threshold..... 2347
Short Retry Limit..... 7
TI Threshold..... -50
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

Press Enter to continue Or <Ctl Z> to abort
802.11A Advanced Configuration
AP Name                               Channel    TxPower Level
-----
AP000a.b812.2cda                       149*      1*

Press Enter to continue Or <Ctl Z> to abort
802.11A Airewave Director Configuration
RF Event and Performance Logging
  Channel Update Logging..... Off
  Coverage Profile Logging..... Off
  Foreign Profile Logging..... Off
  Load Profile Logging..... Off
  Noise Profile Logging..... Off
  Performance Profile Logging..... Off
  TxPower Update Logging..... Off
Default 802.11a AP performance profiles
  802.11a Global Interference threshold..... 10 %
  802.11a Global noise threshold..... -70 dBm
  802.11a Global RF utilization threshold..... 80 %
  802.11a Global throughput threshold..... 1000000 bps
  802.11a Global clients threshold..... 12 clients
  802.11a Global coverage threshold..... 16 dB
  802.11a Global coverage exception level..... 25 %
  802.11a Global client minimum exception lev... 3 clients
Default 802.11a AP monitoring
  802.11a Monitor Mode..... enable
  802.11a Monitor Channels..... Country channels
  802.11a AP Coverage Interval..... 180 seconds
  802.11a AP Load Interval..... 60 seconds
  802.11a AP Noise Interval..... 180 seconds
  802.11a AP Signal Strength Interval..... 60 seconds
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode..... AUTO
  Transmit Power Update Interval..... 600 seconds
  Transmit Power Threshold..... -65 dBm

```

```

Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:15:2c:e8:74:60
Last Run..... 565 seconds ago
Automatic Channel Assignment
Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:15:2c:e8:74:60
Last Run..... 565 seconds ago
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... 0 days, 00 h 00 m 31 s
  Average..... 0 days, 00 h 00 m 31 s
  Maximum..... 0 days, 00 h 00 m 31 s
Allowed Channel List..... 36,40,44,48,52,56,60,64,149,
..... 153,157,161
Radio RF Grouping
802.11a Group Mode..... AUTO
802.11a Group Update Interval..... 600 seconds
802.11a Group Leader..... 00:15:2c:e8:74:60
  802.11a Group Member..... 00:15:2c:e8:74:60
802.11a Last Run..... 565 seconds ago

Press Enter to continue Or <Ctl Z> to abort
802.11B Configuration
802.11b Network..... Enabled
11gSupport..... Enabled
802.11b/g Operational Rates
  802.11b/g 1M Rate..... Mandatory
  802.11b/g 2M Rate..... Mandatory
  802.11b/g 5.5M Rate..... Mandatory
  802.11b/g 11M Rate..... Mandatory
  802.11g 6M Rate..... Supported
  802.11g 9M Rate..... Supported
  802.11g 12M Rate..... Supported
  802.11g 18M Rate..... Supported
  802.11g 24M Rate..... Supported
  802.11g 36M Rate..... Supported
  802.11g 48M Rate..... Supported
  802.11g 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mode..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 1
Default Tx Power Level..... 1
DTPC Status..... Enabled
Call Admission Limit ..... 105
G711 CU Quantum ..... 15
DTIM Period..... 1
ED Threshold..... -50
Fragmentation Threshold..... 2346
Long Retry Limit..... 4
Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
PBCC mandatory..... Disabled
Pico-Cell Status..... Disabled
RTS Threshold..... 2347

```

```

Short Preamble mandatory..... Enabled
Short Retry Limit..... 7
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

```

Press Enter to continue Or <Ctl Z> to abort

802.11B Advanced Configuration

AP Name	Channel	TxPower Level
AP000a.b812.2cda	1*	1*

Press Enter to continue Or <Ctl Z> to abort

802.11B Airewave Director Configuration

RF Event and Performance Logging

```

Channel Update Logging..... Off
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
Transmit Power Update Logging..... Off

```

Default 802.11b AP performance profiles

```

802.11b Global Interference threshold..... 10 %
802.11b Global noise threshold..... -70 dBm
802.11b Global RF utilization threshold..... 80 %
802.11b Global throughput threshold..... 1000000 bps
802.11b Global clients threshold..... 12 clients
802.11b Global coverage threshold..... 12 dB
802.11b Global coverage exception level..... 25 %
802.11b Global client minimum exception lev... 3 clients

```

Default 802.11b AP monitoring

```

802.11b Monitor Mode..... enable
802.11b Monitor Channels..... Country channels
802.11b AP Coverage Interval..... 180 seconds
802.11b AP Load Interval..... 60 seconds
802.11b AP Noise Interval..... 180 seconds
802.11b AP Signal Strength Interval..... 60 seconds

```

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:15:2c:e8:74:60
Last Run..... 565 seconds ago

```

Automatic Channel Assignment

```

Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:15:2c:e8:74:60
Last Run..... 565 seconds ago

```

Channel Energy Levels

```

Minimum..... unknown
Average..... unknown
Maximum..... unknown

```

Channel Dwell Times

```

Minimum..... 0 days, 00 h 00 m 31 s
Average..... 0 days, 00 h 00 m 31 s

```

```

Maximum..... 0 days, 00 h 00 m 31 s
Allowed Channel List..... 1,6,11
Radio RF Grouping
802.11b Group Mode..... AUTO
802.11b Group Update Interval..... 600 seconds
802.11b Group Leader..... 00:15:2c:e8:74:60
802.11b Group Member..... 00:15:2c:e8:74:60
802.11b Last Run..... 565 seconds ago

```

Press Enter to continue Or <Ctl Z> to abort

```

Mobility Configuration
Mobility Protocol Port..... 16666
Default Mobility Domain..... PCI_medium
Mobility Group members configured..... 1

```

Switches configured in the Mobility Group

MAC Address	IP Address	Group Name
00:15:2c:e8:74:60	10.10.46.34	<local>

Press Enter to continue Or <Ctl Z> to abort

```

Interface Configuration
Interface Name..... ap-manager
IP Address..... 10.10.46.35
IP Netmask..... 255.255.255.248
IP Gateway..... 10.10.46.33
VLAN..... untagged
Physical Port..... 1
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... Yes

```

```

Interface Name..... management
MAC Address..... 00:15:2c:e8:74:60
IP Address..... 10.10.46.34
IP Netmask..... 255.255.255.248
IP Gateway..... 10.10.46.33
VLAN..... untagged
Physical Port..... 1
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```

```

Interface Name..... virtual
IP Address..... 1.1.1.1
DHCP Option 82..... Disabled
Virtual DNS Host Name..... Disabled
AP Manager..... No

```

```

Interface Name..... wireless
IP Address..... 10.10.35.110
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.35.1
VLAN..... 14
Quarantine-vlan..... no
Physical Port..... 1
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```



```

Interface Name..... wirelessguest
IP Address..... 10.10.38.110
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.38.1
VLAN..... 17
Quarantine-vlan..... no
Physical Port..... 1
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```

```

Interface Name..... wirelesspos
IP Address..... 10.10.36.110
IP Netmask..... 255.255.255.0
IP Gateway..... 10.10.36.1
VLAN..... 15
Quarantine-vlan..... no
Physical Port..... 1
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

```

Press Enter to continue Or <Ctl Z> to abort

WLAN Configuration

```

WLAN Identifier..... 4
Network Name (SSID)..... Wireless-M
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wireless
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Enabled
      AES Cipher..... Disabled
    WPA2 (RSN IE)..... Disabled

```

```

Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
CKIP ..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Auto Anchor..... Disabled
H-REAP Local Switching..... Disabled
Management Frame Protection..... Disabled

WLAN Identifier..... 5
Network Name (SSID)..... WirelessPOS-M
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wirelesspos
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

802.11 Authentication:..... Open System
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
  WPA (SSN IE)..... Enabled
    TKIP Cipher..... Enabled
    AES Cipher..... Disabled
  WPA2 (RSN IE)..... Disabled
  Auth Key Management
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Disabled
  CKIP ..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  H-REAP Local Switching..... Disabled
  Management Frame Protection..... Disabled

WLAN Identifier..... 6
Network Name (SSID)..... WirelessGuest-M
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled

```

```

AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... wirelessguest
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Enabled
      AES Cipher..... Disabled
    WPA2 (RSN IE)..... Disabled
  Auth Key Management
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Disabled
  CKIP ..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  H-REAP Local Switching..... Disabled
  Management Frame Protection..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort
ACL Configuration

Press Enter to continue Or <Ctl Z> to abort
CPU ACL Configuration

```

CPU Acl Name..... NOT CONFIGURED
Wireless Traffic..... Disabled
Wired Traffic..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort

```

RADIUS Configuration
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
Aggressive Failover..... Disabled
Keywrap..... Disabled

```

Authentication Servers

```

Idx  Type  Server Address  Port  State  Tout  RFC3576  IPsec -
AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----
1    NM    192.168.42.131  1812  Enabled  2     Disabled  Disabled -
none/unknown/group-0/0 none/none

```

Accounting Servers

```

Index Type  Server Address  Port  State  Tout  RFC-3576  IPsec -
AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----

```

```

Press Enter to continue Or <Ctl Z> to abort
Route Info
Number of Routes..... 0

```

```

Destination Network          Genmask          Gateway
-----

```

```

Press Enter to continue Or <Ctl Z> to abort
Qos Queue Length Info
Platinum queue length..... 100
Gold queue length..... 75
Silver queue length..... 50
Bronze queue length..... 25

```

```

Press Enter to continue Or <Ctl Z> to abort
Mac Filter Info

```

```

Press Enter to continue Or <Ctl Z> to abort
Load Balancing Info
Aggressive Load Balancing..... Enabled
Aggressive Load Balancing Window..... 0 clients

```

```

Press Enter to continue Or <Ctl Z> to abort
Dhcp Scope Info

```

```

Press Enter to continue Or <Ctl Z> to abort
Exclusion List ConfigurationUnable to retrieve exclusion-list entry

```

```

Press Enter to continue Or <Ctl Z> to abort
CDP Configuration
cdp..... disabled

```

```

Press Enter to continue Or <Ctl Z> to abort
WPS Configuration Summary

```

```

Client Exclusion Policy
Excessive 802.11-association failures..... Enabled
Excessive 802.11-authentication failures..... Enabled
Excessive 802.1x-authentication..... Enabled
IP-theft..... Enabled
Excessive Web authentication failure..... Enabled

```

```

Trusted AP Policy
Management Frame Protection..... Disabled
Mis-configured AP Action..... Alarm Only
Enforced encryption policy..... none
Enforced preamble policy..... none
Enforced radio type policy..... none

```

```

    Validate SSID..... Disabled
    Alert if Trusted AP is missing..... Disabled
    Trusted AP timeout..... 120

Untrusted AP Policy
    Rogue Location Discovery Protocol..... Disabled
    RLDP Action..... Alarm Only
--More-- or (q)uit
Rogue APs
    Rogues AP advertising my SSID..... Alarm Only
    Detect and report Ad-Hoc Networks..... Enabled
Rogue Clients
    Validate rogue clients against AAA..... Disabled
    Detect trusted clients on rogue APs..... Alarm Only
    Rogue AP timeout..... 1200

Signature Policy
    Signature Processing..... Enabled

(AW-MED-1_Controller) >

```

Small Store Wireless controller in the Data Center

```

(AW-SML-1_Controller) >show run-config

Press Enter to continue...
System Inventory
Burned-in MAC Address..... 00:0B:85:33:B7:E0

Press Enter to continue Or <Ctl Z> to abort
System Information
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.0.179.11
RTOS Version..... 4.0.179.11
Bootloader Version..... 4.0.179.11
Build Type..... DATA + WPS
Compact Flash Size..... 256 MB

System Name..... AW-SML-1
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.2
IP Address..... 192.168.42.112
System Up Time..... 0 days 5 hrs 1 mins 57 secs

Configured Country..... United States

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 3
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 0
Burned-in MAC Address..... 00:0B:85:33:B7:E0

Press Enter to continue Or <Ctl Z> to abort
Switch Configuration
802.3x Flow Control Mode..... Disable

```

```

Current LWAPP Transport Mode..... Layer 3
LWAPP Transport Mode after next switch reboot.... Layer 3
FIPS prerequisite features..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort

Network Information

```

RF-Network Name..... PCI_Small
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Disable
Ethernet Multicast Mode..... Disable Mode: Ucast
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge AP Zero Config..... Enable
Bridge Shared Secret..... youshouldsetme
Allow Old Bridging Aps To Authenticate..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
AP Fallback ..... Enable
Web Auth Redirect Ports ..... 80
Fast SSID Change ..... Disabled
802.3 Bridging ..... Disable

```

Press Enter to continue Or <Ctl Z> to abort

Port Summary

Pr	Type	STP Stat	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap
1	Normal	Disa	Enable	Auto	Auto	Down	Enable
2	Normal	Disa	Enable	Auto	Auto	Down	Enable
3	Normal	Disa	Enable	Auto	Auto	Down	Enable
4	Normal	Forw	Enable	Auto	100 Full	Up	Enable

Press Enter to continue Or <Ctl Z> to abort

AP Summary

AP Name	Slots	AP Model	Ethernet MAC	Location	Port
AP0019.5521.13c0	2	AIR-LAP1131AG-A-K9	00:19:55:21:13:c0	default location	4

Press Enter to continue Or <Ctl Z> to abort

AP Config

```

Cisco AP Identifier..... 0
Cisco AP Name..... AP0019.5521.13c0
AP Regulatory Domain..... -A
Switch Port Number ..... 4
MAC Address..... 00:19:55:21:13:c0
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.23.10
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.23.1
Cisco AP Location..... default location
Cisco AP Group Name..... none
Primary Cisco Switch..... AW-SML-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... H-Reap

```

```

Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.8.0
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA
Reset Button..... Enabled
AP Serial Number..... FTX1038T101
AP Certificate Type..... Manufacture Installed
H-REAP Vlan mode :..... Disabled
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

```

Attributes for Slot 0

```

Radio Type..... RADIO_TYPE_80211g
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

```

Station Configuration

```

Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:19:07:35:58:c0
Operation Rate Set
  1000 Kilo Bits..... MANDATORY
  2000 Kilo Bits..... MANDATORY
  5500 Kilo Bits..... MANDATORY
  11000 Kilo Bits..... MANDATORY
  6000 Kilo Bits..... SUPPORTED
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... SUPPORTED
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... SUPPORTED
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

```

Multi Domain Capability

```

Configuration ..... AUTOMATIC
First Chan Num ..... 1
Number Of Channels ..... 11

```

MAC Operation Parameters

```

Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

```

```

Tx Power
  Num Of Supported Power Levels ..... 8
  Tx Power Level 1 ..... 20 dBm
  Tx Power Level 2 ..... 17 dBm
  Tx Power Level 3 ..... 14 dBm
  Tx Power Level 4 ..... 11 dBm
  Tx Power Level 5 ..... 8 dBm
  Tx Power Level 6 ..... 5 dBm
  Tx Power Level 7 ..... 2 dBm
  Tx Power Level 8 ..... -1 dBm
  Tx Power Configuration ..... AUTOMATIC
  Current Tx Power Level ..... 1

Phy OFDM parameters
  Configuration ..... AUTOMATIC
  Current Channel ..... 1
  TI Threshold ..... -50
  Antenna Type..... INTERNAL_ANTENNA
  Internal Antenna Gain (in .5 dBm units).... 8
  Diversity..... DIVERSITY_ENABLED

Performance Profile Parameters
  Configuration ..... AUTOMATIC
  Interference threshold..... 10 %
  Noise threshold..... -70 dBm
  RF utilization threshold..... 80 %
  Data-rate threshold..... 1000000 bps
  Client threshold..... 12 clients
  Coverage SNR threshold..... 12 dB
  Coverage exception level..... 25 %
  Client minimum exception level..... 3 clients
Rogue Containment Information
  Containment Count..... 0

Cisco AP Identifier..... 0
Cisco AP Name..... AP0019.5521.13c0
AP Regulatory Domain..... -A
Switch Port Number ..... 4
MAC Address..... 00:19:55:21:13:c0
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.23.10
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.23.1
Cisco AP Location..... default location
Cisco AP Group Name..... none
Primary Cisco Switch..... AW-SML-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... H-Reap
Remote AP Debug ..... Disabled
S/W Version ..... 4.0.179.11
Boot Version ..... 12.3.8.0
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1131AG-A-K9
IOS Version..... 12.3(11)JA

```



```

Reset Button..... Enabled
AP Serial Number..... FTX1038T101
AP Certificate Type..... Manufacture Installed
H-REAP Vlan mode :..... Disabled
Management Frame Protection Validation..... Enabled (Global MFP Disabled)

```

Attributes for Slot 1

```

Radio Type..... RADIO_TYPE_80211a
Administrative State ..... ADMIN_ENABLED
Operation State ..... UP
WLAN Override ..... Disabled
CellId ..... 0

```

Station Configuration

```

Configuration ..... AUTOMATIC
Number Of WLANs ..... 3
Medium Occupancy Limit ..... 100
CFP Period ..... 4
CFP MaxDuration ..... 60
BSSID ..... 00:19:07:35:58:c0
Operation Rate Set
  6000 Kilo Bits..... MANDATORY
  9000 Kilo Bits..... SUPPORTED
  12000 Kilo Bits..... MANDATORY
  18000 Kilo Bits..... SUPPORTED
  24000 Kilo Bits..... MANDATORY
  36000 Kilo Bits..... SUPPORTED
  48000 Kilo Bits..... SUPPORTED
  54000 Kilo Bits..... SUPPORTED
Beacon Period ..... 100
DTIM Period ..... 1
Fragmentation Threshold ..... 2346
Multi Domain Capability Implemented ..... TRUE
Multi Domain Capability Enabled ..... TRUE
Country String ..... US

```

Multi Domain Capability

```

Configuration ..... AUTOMATIC
First Chan Num ..... 36
Number Of Channels ..... 4

```

MAC Operation Parameters

```

Configuration ..... AUTOMATIC
RTS Threshold ..... 2347
Short Retry Limit ..... 7
Long Retry Limit ..... 4
Fragmentation Threshold ..... 2346
Maximum Tx MSDU Life Time ..... 512
Maximum Rx Life Time ..... 512

```

Tx Power

```

Num Of Supported Power Levels ..... 8
Tx Power Level 1 ..... 17 dBm
Tx Power Level 2 ..... 15 dBm
Tx Power Level 3 ..... 14 dBm
Tx Power Level 4 ..... 11 dBm
Tx Power Level 5 ..... 8 dBm
Tx Power Level 6 ..... 5 dBm
Tx Power Level 7 ..... 2 dBm
Tx Power Level 8 ..... -1 dBm
Tx Power Configuration ..... AUTOMATIC
Current Tx Power Level ..... 1

```

Phy OFDM parameters

```

Configuration ..... AUTOMATIC
Current Channel ..... 64
TI Threshold ..... -50
Antenna Type..... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBm units)... 8
Diversity..... DIVERSITY_ENABLED

```

```

Performance Profile Parameters
Configuration ..... AUTOMATIC
Interference threshold..... 10 %
Noise threshold..... -70 dBm
RF utilization threshold..... 80 %
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 16 dB
Coverage exception level..... 25 %
Client minimum exception level..... 3 clients
Rogue Containment Information
Containment Count..... 0

```

Press Enter to continue Or <Ctl Z> to abort

AP Airwave Director Configuration

```

Number Of Slots..... 2
AP Name..... AP0019.5521.13c0
MAC Address..... 00:19:55:21:13:c0
Radio Type..... RADIO_TYPE_80211b/g

```

Noise Information

```

Noise Profile..... PASSED
Channel 1..... -88 dBm
Channel 2..... -87 dBm
Channel 3..... -91 dBm
Channel 4..... -88 dBm
Channel 5..... -83 dBm
Channel 6..... -84 dBm
Channel 7..... -87 dBm
Channel 8..... -89 dBm
Channel 9..... -91 dBm
Channel 10..... -89 dBm
Channel 11..... -86 dBm

```

Interference Information

```

Interference Profile..... PASSED
Channel 1..... -61 dBm @ 2 % busy
Channel 2..... -66 dBm @ 1 % busy
Channel 3..... -68 dBm @ 1 % busy
Channel 4..... -54 dBm @ 1 % busy
Channel 5..... -48 dBm @ 4 % busy
Channel 6..... -53 dBm @ 12 % busy
Channel 7..... -41 dBm @ 1 % busy
Channel 8..... -128 dBm @ 0 % busy
Channel 9..... -128 dBm @ 0 % busy
Channel 10..... -35 dBm @ 3 % busy
Channel 11..... -61 dBm @ 2 % busy

```

Load Information

```

Load Profile..... PASSED
Receive Utilization..... 4 %
Transmit Utilization..... 2 %
Channel Utilization..... 2 %
Attached Clients..... 0 clients

```

Coverage Information

```

Coverage Profile..... PASSED
Failed Clients..... 0 clients

```

Client Signal Strengths

```

RSSI -100 dbm..... 0 clients

```

```

RSSI -92 dbm..... 0 clients
RSSI -84 dbm..... 0 clients
RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
SNR 0 dbm..... 0 clients
SNR 5 dbm..... 0 clients
SNR 10 dbm..... 0 clients
SNR 15 dbm..... 0 clients
SNR 20 dbm..... 0 clients
SNR 25 dbm..... 0 clients
SNR 30 dbm..... 0 clients
SNR 35 dbm..... 0 clients
SNR 40 dbm..... 0 clients
SNR 45 dbm..... 0 clients
Nearby APs
Radar Information
Channel Assignment Information
Current Channel Average Energy..... -68 dBm
Previous Channel Average Energy..... -49 dBm
Channel Change Count..... 1
Last Channel Change Time..... Fri Dec 15 17:10:15 2006
Recommndd Best Channel..... 1
RF Parameter Recommendations
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0
Number Of Slots..... 2
AP Name..... AP0019.5521.13c0
MAC Address..... 00:19:55:21:13:c0
Radio Type..... RADIO_TYPE_80211a
Noise Information
Noise Profile..... PASSED
Channel 36..... -93 dBm
Channel 40..... -94 dBm
Channel 44..... -93 dBm
Channel 48..... -93 dBm
Channel 52..... -94 dBm
Channel 56..... -95 dBm
Channel 60..... -95 dBm
Channel 64..... -89 dBm
Channel 149..... -92 dBm
Channel 153..... -89 dBm
Channel 157..... -93 dBm
Channel 161..... -84 dBm
Channel 165..... -90 dBm
Channel 190..... -96 dBm
Interference Information
Interference Profile..... PASSED
Channel 36..... -128 dBm @ 0 % busy
Channel 40..... -128 dBm @ 0 % busy
Channel 44..... -128 dBm @ 0 % busy
Channel 48..... -128 dBm @ 0 % busy
Channel 52..... -128 dBm @ 0 % busy
Channel 56..... -128 dBm @ 0 % busy
Channel 60..... -128 dBm @ 0 % busy
Channel 64..... -128 dBm @ 0 % busy
Channel 149..... -128 dBm @ 0 % busy
Channel 153..... -128 dBm @ 0 % busy
Channel 157..... -128 dBm @ 0 % busy
Channel 161..... -128 dBm @ 0 % busy

```

```

Channel 165..... -128 dBm @ 0 % busy
Channel 190..... -128 dBm @ 0 % busy
Load Information
Load Profile..... PASSED
Receive Utilization..... 0 %
Transmit Utilization..... 0 %
Channel Utilization..... 0 %
Attached Clients..... 0 clients
Coverage Information
Coverage Profile..... PASSED
Failed Clients..... 0 clients
Client Signal Strengths
RSSI -100 dbm..... 0 clients
RSSI -92 dbm..... 0 clients
RSSI -84 dbm..... 0 clients
RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
SNR 0 dbm..... 0 clients
SNR 5 dbm..... 0 clients
SNR 10 dbm..... 0 clients
SNR 15 dbm..... 0 clients
SNR 20 dbm..... 0 clients
SNR 25 dbm..... 0 clients
SNR 30 dbm..... 0 clients
SNR 35 dbm..... 0 clients
SNR 40 dbm..... 0 clients
SNR 45 dbm..... 0 clients
Nearby APs
Radar Information
Channel Assignment Information
Current Channel Average Energy..... unknown
Previous Channel Average Energy..... unknown
Channel Change Count..... 0
Last Channel Change Time..... Fri Dec 15 17:00:57 2006
Recommendd Best Channel..... 64
RF Parameter Recommendations
Power Level..... 1
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0

Press Enter to continue Or <Ctl Z> to abort
802.11A Configuration
802.11a Network..... Enabled
802.11a Low Band..... Enabled
802.11a Mid Band..... Enabled
802.11a High Band..... Enabled
802.11a Operational Rates
802.11a 6M Rate..... Mandatory
802.11a 9M Rate..... Supported
802.11a 12M Rate..... Mandatory
802.11a 18M Rate..... Supported
802.11a 24M Rate..... Mandatory
802.11a 36M Rate..... Supported
802.11a 48M Rate..... Supported
802.11a 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mandatory..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60

```

```

Default Channel..... 36
Default Tx Power Level..... 1
DTPC Status..... Enabled
DTIM Period..... 1
Fragmentation Threshold..... 2346
Long Retry Limit..... 4
Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
Pico-Cell Status..... Disabled
RTS Threshold..... 2347
Short Retry Limit..... 7
TI Threshold..... -50
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75
  Voice reserved roaming bandwidth..... 6
  Video AC - Admission control (ACM)..... Disabled
  Video max RF bandwidth..... Infinite
  Video reserved roaming bandwidth..... 0

Press Enter to continue Or <Ctl Z> to abort
802.11A Advanced Configuration
AP Name                               Channel    TxPower Level
-----
AP0019.5521.13c0                       64*       1*

Press Enter to continue Or <Ctl Z> to abort
802.11A Airewave Director Configuration
RF Event and Performance Logging
  Channel Update Logging..... Off
  Coverage Profile Logging..... Off
  Foreign Profile Logging..... Off
  Load Profile Logging..... Off
  Noise Profile Logging..... Off
  Performance Profile Logging..... Off
  TxPower Update Logging..... Off
Default 802.11a AP performance profiles
  802.11a Global Interference threshold..... 10 %
  802.11a Global noise threshold..... -70 dBm
  802.11a Global RF utilization threshold..... 80 %
  802.11a Global throughput threshold..... 1000000 bps
  802.11a Global clients threshold..... 12 clients
  802.11a Global coverage threshold..... 16 dB
  802.11a Global coverage exception level..... 25 %
  802.11a Global client minimum exception lev... 3 clients
Default 802.11a AP monitoring
  802.11a Monitor Mode..... enable
  802.11a Monitor Channels..... Country channels
  802.11a AP Coverage Interval..... 180 seconds
  802.11a AP Load Interval..... 60 seconds
  802.11a AP Noise Interval..... 180 seconds
  802.11a AP Signal Strength Interval..... 60 seconds
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode..... AUTO
  Transmit Power Update Interval..... 600 seconds
  Transmit Power Threshold..... -65 dBm
  Transmit Power Neighbor Count..... 3 APs
  Transmit Power Update Contribution..... SNI.
  Transmit Power Assignment Leader..... 00:0b:85:33:b7:e0
  Last Run..... 591 seconds ago
Automatic Channel Assignment
  Channel Assignment Mode..... AUTO
    
```

```

Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:0b:85:33:b7:e0
Last Run..... 591 seconds ago
Channel Energy Levels
  Minimum..... unknown
  Average..... unknown
  Maximum..... unknown
Channel Dwell Times
  Minimum..... 0 days, 05 h 00 m 58 s
  Average..... 0 days, 05 h 00 m 58 s
  Maximum..... 0 days, 05 h 00 m 58 s
Allowed Channel List..... 36,40,44,48,52,56,60,64,149,
..... 153,157,161
Radio RF Grouping
  802.11a Group Mode..... AUTO
  802.11a Group Update Interval..... 600 seconds
  802.11a Group Leader..... 00:0b:85:33:b7:e0
    802.11a Group Member..... 00:0b:85:33:b7:e0
  802.11a Last Run..... 591 seconds ago

Press Enter to continue Or <Ctl Z> to abort
802.11B Configuration
802.11b Network..... Enabled
11gSupport..... Enabled
802.11b/g Operational Rates
  802.11b/g 1M Rate..... Mandatory
  802.11b/g 2M Rate..... Mandatory
  802.11b/g 5.5M Rate..... Mandatory
  802.11b/g 11M Rate..... Mandatory
  802.11g 6M Rate..... Supported
  802.11g 9M Rate..... Supported
  802.11g 12M Rate..... Supported
  802.11g 18M Rate..... Supported
  802.11g 24M Rate..... Supported
  802.11g 36M Rate..... Supported
  802.11g 48M Rate..... Supported
  802.11g 54M Rate..... Supported
Beacon Interval..... 100
CF Pollable mode..... Disabled
CF Poll Request mandatory..... Disabled
CFP Period..... 4
CFP Maximum Duration..... 60
Default Channel..... 1
Default Tx Power Level..... 1
DTPC Status..... Enabled
Call Admission Limit ..... 105
G711 CU Quantum ..... 15
DTIM Period..... 1
ED Threshold..... -50
Fragmentation Threshold..... 2346
Long Retry Limit..... 4
Maximum Rx Life Time..... 512
Max Tx MSDU Life Time..... 512
Medium Occupancy Limit..... 100
PBCC mandatory..... Disabled
Pico-Cell Status..... Disabled
RTS Threshold..... 2347
Short Preamble mandatory..... Enabled
Short Retry Limit..... 7
Traffic Stream Metrics Status..... Disabled
Call Admission Control (CAC) configuration
  Voice AC - Admission control (ACM)..... Disabled
  Voice max RF bandwidth..... 75

```

```

Voice reserved roaming bandwidth..... 6
Video AC - Admission control (ACM)..... Disabled
Video max RF bandwidth..... Infinite
Video reserved roaming bandwidth..... 0

```

Press Enter to continue Or <Ctl Z> to abort

802.11B Advanced Configuration

```

AP Name                               Channel    TxPower Level
-----
AP0019.5521.13c0                      1*        1*

```

Press Enter to continue Or <Ctl Z> to abort

802.11B Airewave Director Configuration

RF Event and Performance Logging

```

Channel Update Logging..... Off
Coverage Profile Logging..... Off
Foreign Profile Logging..... Off
Load Profile Logging..... Off
Noise Profile Logging..... Off
Performance Profile Logging..... Off
Transmit Power Update Logging..... Off

```

Default 802.11b AP performance profiles

```

802.11b Global Interference threshold..... 10 %
802.11b Global noise threshold..... -70 dBm
802.11b Global RF utilization threshold..... 80 %
802.11b Global throughput threshold..... 1000000 bps
802.11b Global clients threshold..... 12 clients
802.11b Global coverage threshold..... 12 dB
802.11b Global coverage exception level..... 25 %
802.11b Global client minimum exception lev... 3 clients

```

Default 802.11b AP monitoring

```

802.11b Monitor Mode..... enable
802.11b Monitor Channels..... Country channels
802.11b AP Coverage Interval..... 180 seconds
802.11b AP Load Interval..... 60 seconds
802.11b AP Noise Interval..... 180 seconds
802.11b AP Signal Strength Interval..... 60 seconds

```

Automatic Transmit Power Assignment

```

Transmit Power Assignment Mode..... AUTO
Transmit Power Update Interval..... 600 seconds
Transmit Power Threshold..... -65 dBm
Transmit Power Neighbor Count..... 3 APs
Transmit Power Update Contribution..... SNI.
Transmit Power Assignment Leader..... 00:0b:85:33:b7:e0
Last Run..... 591 seconds ago

```

Automatic Channel Assignment

```

Channel Assignment Mode..... AUTO
Channel Update Interval..... 600 seconds
Channel Update Contribution..... SNI.
Channel Assignment Leader..... 00:0b:85:33:b7:e0
Last Run..... 591 seconds ago

```

Channel Energy Levels

```

Minimum..... -68 dBm
Average..... -68 dBm
Maximum..... -68 dBm

```

Channel Dwell Times

```

Minimum..... 0 days, 04 h 51 m 40 s
Average..... 0 days, 04 h 51 m 40 s
Maximum..... 0 days, 04 h 51 m 40 s

```

Allowed Channel List..... 1,6,11

Radio RF Grouping

```

802.11b Group Mode..... AUTO
802.11b Group Update Interval..... 600 seconds
802.11b Group Leader..... 00:0b:85:33:b7:e0

```

802.11b Group Member..... 00:0b:85:33:b7:e0
802.11b Last Run..... 591 seconds ago

Press Enter to continue Or <Ctl Z> to abort

Mobility Configuration
Mobility Protocol Port..... 16666
Default Mobility Domain..... PCI_Small
Mobility Group members configured..... 1

Switches configured in the Mobility Group

MAC Address IP Address Group Name
00:0b:85:33:b7:e0 192.168.42.112 <local>

Press Enter to continue Or <Ctl Z> to abort

Interface Configuration
Interface Name..... ap-manager
IP Address..... 192.168.42.113
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.42.1
VLAN..... untagged
Physical Port..... 4
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... Yes

Interface Name..... management
MAC Address..... 00:0b:85:33:b7:e0
IP Address..... 192.168.42.112
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.42.1
VLAN..... untagged
Physical Port..... 4
Primary DHCP Server..... 192.168.42.130
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No

Interface Name..... virtual
IP Address..... 1.1.1.1
DHCP Option 82..... Disabled
Virtual DNS Host Name..... Disabled
AP Manager..... No

Press Enter to continue Or <Ctl Z> to abort

WLAN Configuration

WLAN Identifier..... 2
Network Name (SSID)..... Wireless-S
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)


```

WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Enabled
      AES Cipher..... Disabled
    WPA2 (RSN IE)..... Disabled
  Auth Key Management
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Disabled
  CKIP ..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  H-REAP Local Switching..... Enabled
  Management Frame Protection..... Disabled

WLAN Identifier..... 3
Network Name (SSID)..... WirelessPOS-S
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1X..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Enabled
      TKIP Cipher..... Enabled
      AES Cipher..... Disabled

```

```

WPA2 (RSN IE)..... Disabled
Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
CKIP ..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Auto Anchor..... Disabled
H-REAP Local Switching..... Enabled
Management Frame Protection..... Disabled

WLAN Identifier..... 4
Network Name (SSID)..... WirelessGuest-S
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Disabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Radio Policy..... All
Radius Servers
  Authentication..... 192.168.42.131 1812
Security

802.11 Authentication:..... Open System
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
  WPA (SSN IE)..... Enabled
    TKIP Cipher..... Enabled
    AES Cipher..... Disabled
  WPA2 (RSN IE)..... Disabled
  Auth Key Management
    802.1x..... Enabled
    PSK..... Disabled
    CCKM..... Disabled
  CKIP ..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Auto Anchor..... Disabled
  H-REAP Local Switching..... Enabled
  Management Frame Protection..... Disabled

```

Press Enter to continue Or <Ctl Z> to abort
ACL Configuration

Press Enter to continue Or <Ctl Z> to abort

CPU ACL Configuration

```
CPU Acl Name..... NOT CONFIGURED
Wireless Traffic..... Disabled
Wired Traffic..... Disabled
```

Press Enter to continue Or <Ctl Z> to abort

RADIUS Configuration

```
Vendor Id Backward Compatibility..... Disabled
Credentials Caching..... Disabled
Call Station Id Type..... IP Address
Administrative Authentication via RADIUS..... Enabled
Aggressive Failover..... Enabled
Keywrap..... Disabled
```

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	RFC3576	IPSec	-
AuthMode/Phase1/Group/Lifetime/Auth/Encr								
1	NM	192.168.42.131	1812	Enabled	2	Disabled	Disabled	-
none/unknown/group-0/0 none/none								

Accounting Servers

Index	Type	Server Address	Port	State	Tout	RFC-3576	IPSec	-
AuthMode/Phase1/Group/Lifetime/Auth/Encr								

Press Enter to continue Or <Ctl Z> to abort

Route Info

Number of Routes..... 0

Destination Network	Genmask	Gateway

Press Enter to continue Or <Ctl Z> to abort

Qos Queue Length Info

```
Platinum queue length..... 100
Gold queue length..... 75
Silver queue length..... 50
Bronze queue length..... 25
```

Press Enter to continue Or <Ctl Z> to abort

Mac Filter Info

Press Enter to continue Or <Ctl Z> to abort

Load Balancing Info

```
Aggressive Load Balancing..... Enabled
Aggressive Load Balancing Window..... 0 clients
```

Press Enter to continue Or <Ctl Z> to abort

Dhcp Scope Info

Press Enter to continue Or <Ctl Z> to abort

Exclusion List ConfigurationUnable to retrieve exclusion-list entry

Press Enter to continue Or <Ctl Z> to abort

CDP Configuration

```

Press Enter to continue Or <Ctl Z> to abort
WPS Configuration Summary

Client Exclusion Policy
  Excessive 802.11-association failures..... Enabled
  Excessive 802.11-authentication failures..... Enabled
  Excessive 802.1x-authentication..... Enabled
  IP-theft..... Enabled
  Excessive Web authentication failure..... Enabled

Trusted AP Policy
  Management Frame Protection..... Disabled
  Mis-configured AP Action..... Alarm Only
    Enforced encryption policy..... none
    Enforced preamble policy..... none
    Enforced radio type policy..... none
  Validate SSID..... Disabled
  Alert if Trusted AP is missing..... Disabled
  Trusted AP timeout..... 120

Untrusted AP Policy
  Rogue Location Discovery Protocol..... Disabled
  RLDLP Action..... Alarm Only
--More-- or (q)uit
Rogue APs
  Rogues AP advertising my SSID..... Alarm Only
  Detect and report Ad-Hoc Networks..... Enabled
Rogue Clients
  Validate rogue clients against AAA..... Disabled
  Detect trusted clients on rogue APs..... Alarm Only
  Rogue AP timeout..... 1200

Signature Policy
  Signature Processing..... Enabled

(AW-SML-1_Controller) >
    
```

Large Store Access Point

1. Use interfaces VLAN1000 & VLAN 11-18 for Controller connectivity.
2. Tag all other dynamic interfaces (VLAN 11-18) on controller
3. Note that VLAN 1000 is used for WLAN "service-port" connectivity. Service port is not routeable and does not support VLAN.

Below is the suggested configuration for Large Store controller.

```

Controller Config Script:
Enter User Name (or 'Recover-Config' this one-time only to reset configuration )

User: wifiguy
Password:lnorfid!

(Cisco Controller) >config prompt AW-LRG-1_Controller
(AW-LRG-1_Controller) >config interface create Wireless 14
(AW-LRG-1_Controller) >config interface create WirelessPOS 15
(AW-LRG-1_Controller) >config interface create WirelessGuest 17
(AW-LRG-1_Controller) >config interface address Wireless 10.10.51.5 255.255.255.0
10.10.51.1
    
```

```
(AW-LRG-1_Controller) >config interface address WirelessPOS 10.10.52.5 255.255.255.0
10.10.55.1
(AW-LRG-1_Controller) >config interface address WirelessGuest 10.10.54.5 255.255.255.0
10.10.54.1
(AW-LRG-1_Controller)>config port WirelessGuest 1
(AW-LRG-1_Controller)>config port WirelessPOS 1
(AW-LRG-1_Controller)>config port Wireless 1

(AW-LRG-1_Controller) >show interface summary
Interface Name                Port  Vlan Id  IP Address      Type      Ap Mgr
-----
ap-manager                    1     18       10.10.55.61    Static    Yes
management                   1     18       10.10.55.60    Static    No
service-port                  N/A   N/A      10.10.63.100   Static    No
virtual                       N/A   N/A      1.1.1.1        Static    No
wireless                      -     14       10.10.51.5     Dynamic   No
wirelesspos                   -     15       10.10.52.5     Dynamic   No
wirelessguest                 -     17       10.10.54.5     Dynamic   No
```

Medium Store Access Point

Below is the suggested configuration in the ISR for integration of the NM-AIR-WLC6 controller

```
!
interface wlan-controller1/0
description WLAN Controller Mgmt interface
ip address 10.10.46.33 255.255.255.248
no snmp trap link-status
!
interface wlan-controller1/0.14
encap dot1q 14
ip address 10.10.35.1 255.255.255.0
no snmp trap link-status
!
interface wlan-controller1/0.15
encap dot1q 15
ip address 10.10.36.1 255.255.255.0
no snmp trap link-status
!
interface wlan-controller1/0.17
encap dot1q 17
ip address 10.10.38.1 255.255.255.0
no snmp trap link-status
!
Medium Store Controller Config Script:
Enter Administrative User Name (24 characters max): wifiguy
Enter Administrative Password (24 characters max): *****

Management Interface IP Address: 10.10.46.34
Management Interface Netmask: 255.255.255.248
Management Interface Default Router: 10.10.46.33
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1]:
Management Interface DHCP Server IP Address: 192.168.42.130

AP Manager Interface IP Address: 10.10.46.35

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.42.130):

Virtual Gateway IP Address: 1.1.1.1
```

```

Mobility/RF Group Name: PCI_Medium

Network Name (SSID): Wireless
Allow Static IP Addresses [YES][no]:

Configure a RADIUS Server now? [YES][no]:
Enter the RADIUS Server's Address: 192.168.42.131
Enter the RADIUS Server's Port [1812]:
Enter the RADIUS Server's Secret: retailpci

Enter Country Code (enter 'help' for a list of countries) [US]:

Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:

Configure a NTP server now? [YES][no]:
Enter the NTP server's IP address: 192.168.42.130
Enter a polling interval between 3600 and 604800 secs: 3600

```

```
(AW-MED-1) >show interface summary
```

Interface Name	Port	Vlan Id	IP Address	Type	Ap Mgr
ap-manager	1	untagged	10.10.46.35	Static	Yes
management	1	untagged	10.10.46.34	Static	No
virtual	N/A	N/A	1.1.1.1	Static	No
wireless	1	14	10.10.35.110	Dynamic	No
wirelessguest	1	17	10.10.38.110	Dynamic	No
wirelesspos	1	15	10.10.36.110	Dynamic	No

Small Store Access Point

1. Use f0/3/0 interface on ISR for HREAP connectivity, VLAN 18 for LWAPP/management traffic.
2. With HREAP, should use trunk port on f0/3/0 to provide access for VLAN11-17 locally.
3. All WLAN security configuration for HREAP set via controller.
4. HREAP configured for local traffic bridging on all WLAN
5. Configure secure username & password at AP (via controller commands)
6. Configure AP for static address and static controller address.

Below is the suggested configuration for the ISR for integration of the HREAP with central controller.

```

!
interface FastEthernet0/3/0
description AP connection for HREAP
switch encap dot1q
switch mode trunk
switchport trunk native vlan 18
!
The following is the configuration for CLI configuration of HREAP AP:
!
ap# lwapp ap ip address 10.10.23.10 255.255.255.0
ap# lwapp ip default-gateway 10.10.23.1
ap# lwapp controller ip address 10.10.55.5
ap# lwapp ap hostname AP-1

```

After AP joins WLC, go to controller to set AP "enable" password.

```

Controller> config ap username <wifiguy> password <lnorfid!> "AP-name"

```

Internet Edge Configurations

Cisco Firewall Service Module

```
----- show version -----

FWSM1# sh ver

FWSM Firewall Version 3.1(3)
Device Manager Version 5.0(1)F

Compiled on Thu 06-Jul-06 12:44 by dalecki

FWSM1 up 30 days 4 hours

Hardware: WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash SMART CF @ 0xc321, 20MB

0: Int: Not licensed      : irq 5
1: Int: Not licensed      : irq 7
2: Int: Not licensed      : irq 11
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Maximum Interfaces       : 256
Inside Hosts            : Unlimited
Failover                 : Active/Active
VPN-DES                  : Enabled
VPN-3DES-AES            : Enabled
Cut-through Proxy       : Enabled
Guards                   : Enabled
URL Filtering           : Enabled
Security Contexts       : 2
GTP/GPRS                 : Disabled
VPN Peers                : Unlimited

Serial Number: SAD11140154
Running Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
Configuration last modified by enable_15 at 00:52:52.300 PDT Sat Jan 26 2008
FWSM1#

----- show running-config -----
:FWSM1# sh run
: Saved
:
FWSM Version 3.1(3)
!
hostname FWSM1
domain-name cisco-irn.com
enable password <removed> encrypted
names
!
interface Vlan81
 nameif ECOM_OUTSIDE
```

```

security-level 0
ip address 192.168.20.17 255.255.255.248 standby 192.168.20.18
!
interface Vlan82
nameif ECOM_DMZ
security-level 50
ip address 192.168.20.25 255.255.255.248 standby 192.168.20.26
!
interface Vlan91
description LAN Failover Interface
!
interface Vlan92
description STATE Failover Interface
!
interface Vlan97
nameif inside
security-level 100
ip address 192.168.11.2 255.255.255.240 standby 192.168.11.3
!
interface Vlan995
nameif DMZ_MGMT
security-level 75
ip address 192.168.21.17 255.255.255.240 standby 192.168.21.18
!
passwd <removed> encrypted
banner exec WARNING:
banner exec      **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
banner exec      **** AUTHORIZED USERS ONLY! ****
banner exec ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner exec TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner exec TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
banner exec REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner exec FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner exec CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner exec ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
banner exec UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS.
banner login WARNING:
banner login      **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
banner login      **** AUTHORIZED USERS ONLY! ****
banner login ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
banner login TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE
NECESSARY
banner login TO IDENTIFY ANY UNAUTHORIZED USER.  THE SYSTEM ADMINISTRATOR OR OTHER
banner login REPRESENTATIVES OF THE SYSTEM OWNER  MAY MONITOR SYSTEM USE AT ANY TIME
WITHOUT
banner login FURTHER NOTICE OR CONSENT.  UNAUTHORIZED USE OF  THIS SYSTEM AND ANY OTHER
banner login CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
banner login ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.
banner login UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL
LAWS.
no ftp mode passive
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit tcp host 192.168.21.4 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.121 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.121 eq syslog
log
access-list ECOM_OUT extended permit tcp host 192.168.21.5 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.121 eq snmp log

```



```

access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.121 eq syslog
log
access-list ECOM_OUT extended permit tcp host 192.168.21.4 host 192.168.42.131 eq tacacs
log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT extended permit tcp host 192.168.21.5 host 192.168.42.131 eq tacacs
log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.118 eq syslog
log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.118 eq syslog
log
access-list ECOM_OUT extended permit tcp any host <removed - Internet routable IP address>
eq www log
access-list ECOM_OUT extended permit tcp any host <removed - Internet routable IP address>
eq https log
access-list ECOM_OUT extended permit udp host 192.168.21.4 host 192.168.42.130 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.5 host 192.168.42.130 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit tcp host 192.168.21.2 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.121 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.121 eq syslog
log
access-list ECOM_OUT extended permit tcp host 192.168.21.2 host 192.168.42.131 eq tacacs
log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.118 eq syslog
log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.62.161 eq ntp
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.62.162 eq ntp
access-list ECOM_OUT extended permit tcp host 192.168.21.3 host 192.168.42.121 eq 2055 log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.121 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.121 eq syslog
log
access-list ECOM_OUT extended permit tcp host 192.168.21.3 host 192.168.42.131 eq tacacs
log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.131 eq 1812 log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.118 eq snmp log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.118 eq syslog
log
access-list ECOM_OUT extended permit udp host 192.168.21.2 host 192.168.42.130 eq ntp log
access-list ECOM_OUT extended permit udp host 192.168.21.3 host 192.168.42.130 eq ntp log
access-list ECOM_DMZ extended permit tcp 192.168.20.40 255.255.255.248 host 192.168.42.130
eq ldap log
access-list ECOM_DMZ extended permit tcp 192.168.20.24 255.255.255.248 host 192.168.42.131
eq tacacs log
access-list ECOM_DMZ extended permit udp 192.168.20.24 255.255.255.248 host 192.168.42.131
eq 1812 log
access-list ECOM_DMZ extended permit udp 192.168.20.24 255.255.255.248 host 192.168.42.130
eq ntp log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.11.2 eq ssh
access-list inside extended permit tcp host 192.168.42.130 host 192.168.11.7 eq https log
access-list inside extended permit tcp host 192.168.42.131 host 192.168.11.7 eq https log
access-list inside extended permit icmp any any echo log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.4 eq ssh log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.5 eq ssh log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.2 eq ssh log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.3 eq ssh log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.19 eq ssh log
access-list inside extended permit tcp host 192.168.42.121 host 192.168.21.20 eq ssh log

```



```

access-list DMZ_MGMT extended permit udp host 192.168.21.19 host 192.168.62.161 eq ntp log
access-list DMZ_MGMT extended permit udp host 192.168.21.19 host 192.168.62.162 eq ntp log
access-list DMZ_MGMT extended permit udp host 192.168.21.20 host 192.168.62.161 eq ntp log
access-list DMZ_MGMT extended permit udp host 192.168.21.20 host 192.168.62.162 eq ntp log
pager lines 24
logging enable
logging timestamp
logging buffered critical
logging device-id hostname
logging host inside 192.168.42.118
logging host inside 192.168.42.121
mtu ECOM_OUTSIDE 1500
mtu ECOM_DMZ 1500
mtu inside 1500
mtu DMZ_MGMT 1500
ip verify reverse-path interface ECOM_OUTSIDE
ip verify reverse-path interface ECOM_DMZ
ip verify reverse-path interface inside
failover
failover lan unit primary
failover lan interface failover Vlan91
failover link statelink Vlan92
failover interface ip failover 192.168.20.13 255.255.255.252 standby 192.168.20.14
failover interface ip statelink 192.168.20.33 255.255.255.252 standby 192.168.20.34
monitor-interface ECOM_OUTSIDE
monitor-interface ECOM_DMZ
monitor-interface inside
icmp permit any ECOM_DMZ
icmp permit any inside
icmp permit any DMZ_MGMT
no asdm history enable
arp timeout 14400
nat-control
global (ECOM_OUTSIDE) 1 interface
nat (ECOM_DMZ) 1 0.0.0.0 0.0.0.0
nat (DMZ_MGMT) 1 192.168.21.16 255.255.255.240
static (ECOM_DMZ,ECOM_OUTSIDE) 192.168.80.25 192.168.20.1 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.42.131 192.168.42.131 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.42.118 192.168.42.118 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.42.121 192.168.42.121 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.62.161 192.168.62.161 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.42.130 192.168.42.130 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.42.130 192.168.42.130 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.42.131 192.168.42.131 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.42.118 192.168.42.118 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.42.121 192.168.42.121 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.62.161 192.168.62.161 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.42.130 192.168.42.130 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.42.131 192.168.42.131 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.42.118 192.168.42.118 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.42.121 192.168.42.121 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.62.161 192.168.62.161 netmask 255.255.255.255
static (inside,ECOM_OUTSIDE) 192.168.62.162 192.168.62.162 netmask 255.255.255.255
static (inside,ECOM_DMZ) 192.168.62.162 192.168.62.162 netmask 255.255.255.255
static (inside,DMZ_MGMT) 192.168.62.162 192.168.62.162 netmask 255.255.255.255
access-group ECOM_OUT in interface ECOM_OUTSIDE
access-group ECOM_DMZ in interface ECOM_DMZ
access-group inside in interface inside
access-group DMZ_MGMT in interface DMZ_MGMT
route ECOM_OUTSIDE 0.0.0.0 0.0.0.0 192.168.20.22 1
route ECOM_DMZ 192.168.20.0 255.255.255.248 192.168.20.30 1
route ECOM_DMZ 192.168.20.40 255.255.255.248 192.168.20.30 2
route inside 192.168.10.0 255.255.255.0 192.168.11.4 1
route inside 192.168.42.0 255.255.255.0 192.168.11.4 1

```

```

route inside 192.168.43.0 255.255.255.0 192.168.11.4 1
route inside 192.168.44.0 255.255.255.0 192.168.11.4 1
route inside 192.168.46.0 255.255.255.0 192.168.11.4 1
route inside 192.168.52.0 255.255.255.0 192.168.11.4 1
route inside 192.168.62.0 255.255.255.0 192.168.11.4 1
route inside 192.168.72.0 255.255.255.0 192.168.11.4 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server RETAIL protocol tacacs+
aaa-server RETAIL host 192.168.42.131
  key <removed>
aaa-server RETAIL host 192.18.42.131
username <removed> password <removed> encrypted privilege 15
aaa authentication ssh console RETAIL LOCAL
aaa authorization include ssh inside 192.168.11.2 255.255.255.255 192.168.42.131
255.255.255.255 RETAIL
aaa accounting command RETAIL
snmp-server host inside 192.168.42.118 community ciscoprivate
snmp-server location IE
snmp-server contact RETAIL-TEAM
snmp-server community ciscoprivate
snmp-server enable traps snmp authentication linkup linkdown coldstart
snmp-server enable traps syslog
snmp-server enable traps ipsec start stop
snmp-server enable traps entity config-change fru-insert fru-remove
snmp-server enable traps remote-access session-threshold-exceeded
telnet timeout 5
ssh 192.168.42.131 255.255.255.255 inside
ssh 192.168.42.121 255.255.255.255 inside
ssh 192.168.42.118 255.255.255.255 inside
ssh timeout 5
ssh version 2
console timeout 15
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect netbios
    inspect smtp
    inspect icmp
    inspect http
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:dc5fdcc45267cc88b5d091d70a18991b
: end
FWSM1#

```

Cisco Catalyst 3750

----- show version -----

```
IES37501#sh ver
Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 12.2(25)SEE4, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 16-Jul-07 03:24 by myl
Image text-base: 0x00003000, data-base: 0x01040000

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)

IES37501 uptime is 8 weeks, 8 hours, 59 minutes
System returned to ROM by power-on
System image file is "flash:/c3750-ipbasek9-mz.122-25.SEE4.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
cisco WS-C3750-48P (PowerPC405) processor (revision J0) with 118784K/12280K bytes of
memory.
Processor board ID CAT1108NJMX
Last reset from power-on
2 Virtual Ethernet interfaces
48 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

```
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:1B:2B:12:19:00
Motherboard assembly number    : 73-9675-11
Power supply part number       : 341-0029-05
Motherboard serial number      : CAT110853HF
Power supply serial number     : LIT110504LF
Model revision number          : J0
Motherboard revision number    : A0
Model number                   : WS-C3750-48PS-S
System serial number           : CAT1108NJMX
SFP Module assembly part number : 73-7757-03
SFP Module revision Number     : A0
SFP Module serial number       : CAT11075JGM
Top Assembly Part Number       : 800-25858-03
Top Assembly Revision Number   : G0
Version ID                     : V05
CLEI Code Number               : COM1W00ARB
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	52	WS-C3750-48P	12.2(25)SEE4	C3750-IPBASEK9-M

Configuration register is 0xF

----- show running-config -----

IES37501#**sh running-config**

Building configuration...

Current configuration : 6764 bytes

```

!
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname IES37501
!
enable secret 5 <removed>.
!
aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
--More--
*Apr 26 02:01:08 PSTDST: %IP_SNMP-4-NOTRAPIP: SNMP trap source Vlan993 has no ipaaa
session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
switch 1 provision ws-c3750-48p
vtp mode transparent
ip subnet-zero
ip routing
ip domain-name <removed>
ip name-server 192.168.42.130
!
ip ssh version 2
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 42
!
vlan 83
 name ACE_inside
!
vlan 729,993,995

```

```
!  
interface FastEthernet1/0/1  
  description VLAN_2_Catalyst6500  
  switchport access vlan 83  
  switchport mode access  
!  
interface FastEthernet1/0/2  
  description VLAN_2_Catalyst6500  
  switchport access vlan 83  
  switchport mode access  
!  
interface FastEthernet1/0/3  
!  
interface FastEthernet1/0/4  
!  
interface FastEthernet1/0/5  
!  
interface FastEthernet1/0/6  
!  
interface FastEthernet1/0/7  
!  
interface FastEthernet1/0/8  
!  
interface FastEthernet1/0/9  
!  
interface FastEthernet1/0/10  
!  
interface FastEthernet1/0/11  
!  
interface FastEthernet1/0/12  
!  
interface FastEthernet1/0/13  
!  
interface FastEthernet1/0/14  
!  
interface FastEthernet1/0/15  
!  
interface FastEthernet1/0/16  
!  
interface FastEthernet1/0/17  
!  
interface FastEthernet1/0/18  
!  
interface FastEthernet1/0/19  
!  
interface FastEthernet1/0/20  
!  
interface FastEthernet1/0/21  
!  
interface FastEthernet1/0/22  
!  
interface FastEthernet1/0/23  
!  
interface FastEthernet1/0/24  
!  
interface FastEthernet1/0/25  
!  
interface FastEthernet1/0/26  
!  
interface FastEthernet1/0/27  
!  
interface FastEthernet1/0/28  
!  
interface FastEthernet1/0/29
```

```
!  
interface FastEthernet1/0/30  
!  
interface FastEthernet1/0/31  
!  
interface FastEthernet1/0/32  
!  
interface FastEthernet1/0/33  
  description HACKME CLIENT OUTSIDE VLAN  
  switchport access vlan 729  
  switchport mode access  
!  
interface FastEthernet1/0/34  
  description HACKME CLIENT OUTSIDE VLAN  
  switchport access vlan 729  
  switchport mode access  
!  
interface FastEthernet1/0/35  
!  
interface FastEthernet1/0/36  
!  
interface FastEthernet1/0/37  
!  
interface FastEthernet1/0/38  
!  
interface FastEthernet1/0/39  
!  
interface FastEthernet1/0/40  
!  
interface FastEthernet1/0/41  
!  
interface FastEthernet1/0/42  
!  
interface FastEthernet1/0/43  
!  
interface FastEthernet1/0/44  
!  
interface FastEthernet1/0/45  
!  
interface FastEthernet1/0/46  
  description MANAGEMENT_VLAN  
  switchport access vlan 995  
  switchport mode access  
!  
interface FastEthernet1/0/47  
  switchport access vlan 83  
  switchport mode access  
!  
interface FastEthernet1/0/48  
  description MANAGEMENT_VLAN  
  switchport access vlan 995  
  switchport mode access  
!  
interface GigabitEthernet1/0/1  
!  
interface GigabitEthernet1/0/2  
!  
interface GigabitEthernet1/0/3  
!  
interface GigabitEthernet1/0/4  
!  
interface Vlan1  
  no ip address  
  shutdown
```



```

!
interface Vlan995
  description MANAGEMENT VLAN
  ip address 192.168.21.19 255.255.255.240
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.21.17
no ip http server
no ip http secure-server
ip tacacs source-interface Vlan995
!
logging source-interface Vlan995
logging 192.168.42.121
logging 192.168.42.118
logging 192.168.44.121
!
access-list 23 permit 192.168.42.118
access-list 23 permit 192.168.42.121
access-list 23 permit 192.168.42.130
access-list 23 permit 192.168.42.131
access-list 23 deny any log
!
snmp-server group causer v3 auth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server group casuser v3 auth access 88
snmp-server community <removed> RW 88
snmp-server community <removed> RO 88
snmp-server packetsize 8192
snmp-server location Internet edge
snmp-server contact Internet edge
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr
snmp-server host 192.168.42.118 version 3 priv causer
snmp-server host 192.168.42.118 retaillab
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key <removed>
radius-server source-ports 1645-1646
!
control-plane
!
banner exec ^CCC
WARNING:
    **** THIS SYST IS PRIVATE PROPERTY FOR THE USE OF CMO Re`il ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESEATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TOAW
ENFORCEMENT OFFICIALS AND PROSECUTION TN THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

```

```

ANY USE OF T
IS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUBH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FUR@HER NOTICE OR CONSENT. UNAUTHORIZED USE OD THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DILOSURE TO LAW S
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION D STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CCC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED SERS ONLY!
^C
banner motd ^CCncom^C
!
line con 0
 session-timeout 15 output
 exec-timeout 60 0
 privilege level 15
 login authentication RLOCAL
line vty 0 4
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
line vty 5 15
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
!
ntp clock-period 36029253
ntp source Vlan995
ntp server 192.168.42.130
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Cisco Catalyst 6500

```

----- show version -----
IES65001#sh ver
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF10a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Wed 19-Sep-07 17:06 by kellythw
Image text-base: 0x40101040, data-base: 0x42DBF630

ROM: System Bootstrap, Version 12.2(17r)S4, RELEASE SOFTWARE (fc1)
BOOTLDR: s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF10a,
RELEASE SOFTWARE (fc1)

```

```

IES65001 uptime is 3 weeks, 4 days, 12 hours, 22 minutes
Time since IES65001 switched to active is 3 weeks, 4 days, 12 hours, 22 minutes
System returned to ROM by reload (SP by reload)
System restarted at 13:36:17 PDT Mon Dec 31 2007
System image file is "disk0:s72033-advipservicesk9_wan-mz.122-18.SXF10a.bin"

```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```

cisco WS-C6509-E (R7000) processor (revision 1.2) with 983008K/65536K bytes of memory.
Processor board ID SMG1014NDXW
SR71000 CPU at 600Mhz, Implementation 0x504, Rev 1.2, 512KB L2 Cache
Last reset from s/w reset
SuperLAT software (copyright 1990 by Meridian Technology Corp).
X.25 software, Version 3.0.0.
Bridging software.
TN3270 Emulation software.
5 Virtual Ethernet/IEEE 802.3 interfaces
64 Gigabit Ethernet/IEEE 802.3 interfaces
1 Ten Gigabit Ethernet/IEEE 802.3 interface
1917K bytes of non-volatile configuration memory.
8192K bytes of packet buffer memory.

```

```

65536K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102

```

```

IES65001#
----- show running-config -----

```

```

IES65001#sh run
Building configuration...

```

```

Current configuration : 12466 bytes
!
! Last configuration change at 01:52:30 PDT Sat Jan 26 2008 by <removed>
! NVRAM config last updated at 01:54:23 PDT Sat Jan 26 2008 by <removed>
!
upgrade fpd auto
version 12.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
service internal
service counters max age 5
!
hostname IES65001
!
boot system flash disk0:s72033-advipservicesk9_wan-mz.122-18.SXF10a.bin
enable secret 5 <removed>
!

```



```
vlan 83
  name ace_inside
!
vlan 85
  name ft_ace
!
vlan 86
!
vlan 87
  name To_Internet_edge_router
!
vlan 91
  name fwsn_failover
!
vlan 92
  name fwsn_statelink
!
vlan 95
  name ACE_XML_gateway
!
vlan 97
  name fw_inside
!
vlan 171
  name back_2_DC_Core
!
vlan 993
  name Management
!
vlan 994
!
vlan 995
  name DMZ_Management
!
!
!
!
interface Loopback0
  ip address 192.168.20.211 255.255.255.255
!
interface Port-channel10
  description ACE-FWSM-Failover Channel
  switchport
  switchport trunk encapsulation dot1q
  switchport mode trunk
  no ip address
!
interface GigabitEthernet1/1
  description connected to IES37501
  switchport
  switchport access vlan 83
  switchport mode access
  no ip address
  logging event link-status
!
interface GigabitEthernet1/2
  description connected to IES37502
  switchport
  switchport access vlan 83
  switchport mode access
  no ip address
  logging event link-status
!
interface GigabitEthernet1/3
```

```

no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/4
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/5
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/6
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/7
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/8
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/9
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/10
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/11
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/12
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/13
description To_IES72061_Internet_Edge_Router
switchport
switchport access vlan 87
switchport mode access
no ip address
logging event link-status
!
interface GigabitEthernet1/14
switchport
switchport access vlan 86
switchport mode access
no ip address
logging event link-status
!

```

```
interface GigabitEthernet1/15
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/16
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/17
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/18
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/19
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/20
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/21
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/22
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/23
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/24
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/25
  description To_ACE_XML_GATEWAY
  switchport
  switchport access vlan 95
  switchport mode access
  no ip address
  logging event link-status
!
interface GigabitEthernet1/26
  no ip address
  logging event link-status
  shutdown
!
interface GigabitEthernet1/27
```

```
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/28
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/29
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/30
description FWSM inside
switchport
switchport access vlan 97
switchport mode access
no ip address
logging event link-status
!
interface GigabitEthernet1/31
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/32
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/33
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/34
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/35
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/36
no ip address
logging event link-status
shutdown
!
interface GigabitEthernet1/37
description To_ACE_XML_GATEWAY
switchport
switchport access vlan 95
switchport mode access
no ip address
logging event link-status
!
interface GigabitEthernet1/38
no ip address
logging event link-status
shutdown
```



```
!  
interface GigabitEthernet1/39  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/40  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/41  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/42  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/43  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/44  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/45  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/46  
  no ip address  
  logging event link-status  
  shutdown  
!  
interface GigabitEthernet1/47  
  switchport  
  switchport access vlan 995  
  switchport mode access  
  no ip address  
  logging event link-status  
!  
interface GigabitEthernet1/48  
  switchport  
  switchport access vlan 995  
  switchport mode access  
  no ip address  
  logging event link-status  
!  
interface GigabitEthernet5/1  
  description port channel-all vlans  
  switchport  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
  no ip address  
  channel-group 10 mode desirable  
!  
interface GigabitEthernet5/2
```

```

description port channel-all vlans
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
no ip address
channel-group 10 mode desirable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan81
description MSFC 81 Vlan
ip address 192.168.20.20 255.255.255.248
ip verify unicast source reachable-via rx
standby 81 ip 192.168.20.22
standby 81 priority 110
standby 81 preempt
!
!
interface Vlan86
ip address 192.168.20.58 255.255.255.252
ip verify unicast source reachable-via rx
end
!
!
interface Vlan87
description TO_IES72061_EDGE_ROUTER
ip address 192.168.20.50 255.255.255.252
ip verify unicast source reachable-via rx
ip cef accounting non-recursive external
!
!
interface Vlan993
description management
ip address 192.168.21.2 255.255.255.0
ip verify unicast source reachable-via rx
!
router ospf 80
router-id 192.168.20.211
log-adjacency-changes
redistribute connected subnets
redistribute static subnets
passive-interface default
no passive-interface Vlan81
no passive-interface Vlan86
no passive-interface Vlan87
no passive-interface Vlan993
network 192.168.20.0 0.0.0.255 area 0
network 192.168.21.0 0.0.0.255 area 0
!
ip classless
ip route 192.168.11.0 255.255.255.0 192.168.20.17
ip route 192.168.20.0 255.255.255.248 192.168.20.17
ip route 192.168.20.24 255.255.255.248 192.168.20.17
ip route 192.168.21.16 255.255.255.240 192.168.20.17
ip route 192.168.30.0 255.255.255.0 192.168.20.49
ip route 192.168.42.0 255.255.255.0 192.168.20.17
ip route 192.168.80.16 255.255.255.248 192.168.20.49
ip route 192.168.80.25 255.255.255.255 192.168.20.17
!
no ip http server
ip tacacs source-interface Loopback0
!

```

```

logging source-interface Loopback0
logging 192.168.42.121
logging 192.168.42.118
logging 192.168.44.121
!
access-list 23 permit 192.168.42.118
access-list 23 permit 192.168.42.121
access-list 23 permit 192.168.42.130
access-list 23 permit 192.168.42.131
access-list 23 deny any log
!
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.0000000F
snmp-server community <removed> RO 88
snmp-server community <removed> RW 88
snmp-server location Internet edge
snmp-server contact Internet edge
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps entity
snmp-server host 192.168.42.118 version 3 priv <removed>
snmp-server host 192.168.42.118 <removed>
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key <removed>
!
radius-server source-ports 1645-1646
!
control-plane
!
!
!
dial-peer cor custom
!
!
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

```

```

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^CC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
alias exec ace3 sess slot 3 proc 0
alias exec fw4 sess slot 4 proc 1
alias exec isdml sess slo 2 proc 1
!
line con 0
 session-timeout 15 output
 exec-timeout 60 0
 login authentication RLOCAL
line vty 0 4
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
line vty 5 15
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
!
!
monitor session 10 source vlan 82 , 97
scheduler runtime netinput 300
scheduler allocate 19998 1000
ntp clock-period 17180178
ntp source Loopback0
ntp server 192.168.42.130
ntp server 192.168.62.161 prefer
no cns aaa enable
end

```

Cisco 7200 Edge Router

```

----- show version -----

IER72061#sh ver
Cisco IOS Software, 7200 Software (C7200P-ADVIPSERVICESK9-M), Version 12.4(11)T3, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 12-Jul-07 00:44 by prod_rel_team

ROM: System Bootstrap, Version 12.4(12.2r)T, RELEASE SOFTWARE (fc1)
BOOTLDR: Cisco IOS Software, 7200 Software (C7200P-KBOOT-M), Version 12.4(4)XD5, RELEASE
SOFTWARE (fc1)

IER72061 uptime is 8 weeks, 5 days, 7 hours, 4 minutes
System returned to ROM by power-on
System image file is "bootflash:c7200p-advipservicesk9-mz.124-11.T3.bin"

This product contains cryptographic features and is subject to United

```

States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 7206VXR (NPE-G2) processor (revision A) with 1966080K/65536K bytes of memory.
 Processor board ID 26800067
 MPC7448 CPU at 1666Mhz, Implementation 0, Rev 2.2
 6 slot VXR midplane, Version 2.6

Last reset from power-on

PCI bus mb1 (Slots 1, 3 and 5) has a capacity of 600 bandwidth points.
 Current configuration on bus mb1 has a total of 400 bandwidth points.
 This configuration is within the PCI bus capacity and is supported.

PCI bus mb2 (Slots 2, 4 and 6) has a capacity of 600 bandwidth points.
 Current configuration on bus mb2 has a total of 0 bandwidth points.
 This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port Adaptor Hardware Configuration Guidelines" on Cisco.com <<http://www.cisco.com>> for c7200 bandwidth points oversubscription and usage guidelines.

1 FastEthernet interface
 4 Gigabit Ethernet interfaces
 4 Serial interfaces
 2045K bytes of NVRAM.

250880K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
 65536K bytes of Flash internal SIMM (Sector size 512K).
 Configuration register is 0x2102
 IER72061#

----- show running-config -----

IER72061#**sh run**
 Building configuration...

```
Current configuration : 7003 bytes
!
upgrade fpd auto
version 12.4
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname IER72061
!
boot-start-marker
boot system flash bootflash:c7200p-advipservicesk9-mz.124-11.T3.bin
boot-end-marker
```

```

!
logging buffered 51200
enable secret 5 <removed>
!
aaa new-model
!
!
aaa authentication login RLOCAL local group tacacs+
aaa authentication login RETAIL group tacacs+ local
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
aaa session-id common
clock timezone PST -8
clock summer-time PSTDST recurring
no ip source-route
ip cef
!
!
!
no ip bootp server
ip domain name <removed>
ip ssh version 2
!
multilink bundle-name authenticated
!
!
!
!
!
username <removed> privilege 15 secret 5 <removed>
!
!
!
!
!
!
interface Loopback0
 ip address 192.168.20.210 255.255.255.255
!
interface Loopback1
 ip address 192.168.21.4 255.255.255.255
!
interface GigabitEthernet0/1
 description TO_Catalyst_6500_1_INTERNAL
 ip address 192.168.20.49 255.255.255.252
 ip verify unicast source reachable-via rx
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
!
interface FastEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto

```

```
!  
interface GigabitEthernet0/2  
  description TO_Catalyst_6500_2_INTERNAL  
  ip address 192.168.20.53 255.255.255.252  
  ip verify unicast source reachable-via rx  
  duplex auto  
  speed auto  
  media-type rj45  
  negotiation auto  
!  
interface GigabitEthernet0/3  
  description TO_INTERNET  
  ip address 192.168.80.18 255.255.255.248  
  ip access-group 110 in  
  ip verify unicast source reachable-via rx  
  ip cef accounting non-recursive external  
  duplex auto  
  speed auto  
  media-type rj45  
  negotiation auto  
!  
interface GigabitEthernet1/0  
  no ip address  
  negotiation auto  
!  
interface Serial3/0  
  no ip address  
  shutdown  
  no fair-queue  
  serial restart-delay 0  
!  
interface Serial3/1  
  no ip address  
  shutdown  
  serial restart-delay 0  
!  
interface Serial3/2  
  no ip address  
  shutdown  
  serial restart-delay 0  
!  
interface Serial3/3  
  no ip address  
  shutdown  
  serial restart-delay 0  
!  
router ospf 80  
  router-id 192.168.20.210  
  log-adjacency-changes  
  passive-interface default  
  no passive-interface GigabitEthernet0/1  
  no passive-interface GigabitEthernet0/2  
  network 192.168.20.48 0.0.0.15 area 0  
  network 192.168.21.0 0.0.0.255 area 0  
!  
no ip http server  
no ip http secure-server  
!  
!  
ip tacacs source-interface Loopback1  
!  
logging alarm informational  
logging source-interface Loopback1  
logging 192.168.42.118
```

```

logging 192.168.44.121
access-list 23 permit 192.168.42.118
access-list 23 permit 192.168.42.121
access-list 23 permit 192.168.42.130
access-list 23 permit 192.168.42.131
access-list 23 deny any log
access-list 110 remark Deny special-use address sources
access-list 110 remark Refer to RFC 3330 for additional special use addresses
access-list 110 deny ip host 0.0.0.0 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 224.0.0.0 31.255.255.255 any
access-list 110 remark Filter RFC 1918 space
access-list 110 deny ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny ip 192.168.0.0 0.0.255.255 any log
access-list 110 remark deny your space as source from entering your AS.
access-list 110 remark To be deploy only at the AS edge.
access-list 110 deny ip <YOUR_CIDR_BLOCK> any
access-list 110 permit tcp any host <public web server> eq www log
access-list 110 permit tcp any host <public web server> eq 443 log
access-list 110 remark Permit legitimate business traffic.
access-list 110 permit tcp any <Internet-routable subnet> established
access-list 110 deny ip any any log
snmp-server group causer v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server community <removed> RW 88
snmp-server community <removed> RO 88
snmp-server chassis-id IER72061
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps casa
snmp-server enable traps tty
snmp-server enable traps srp
snmp-server enable traps bgp
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps dial
snmp-server enable traps entity
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps rsvp
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps voice poor-qov
snmp-server host 192.168.42.118 version 3 priv <removed>
snmp-server host 192.168.42.118 <removed>
!
!
!
!
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key <removed>
radius-server source-ports extended
!
control-plane
!
!
!
```



```
!
!
!
gatekeeper
 shutdown
!
banner exec ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^C
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner login ^C
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!
^C
!
line con 0
  exec-timeout 15 0
  privilege level 15
  password 7 0822455D0A16
  logging synchronous
  login authentication RLOCAL
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  access-class 23 in
  exec-timeout 15 0
  password 7 121A0C041104
  logging synchronous
  login authentication RETAIL
  transport input ssh
!
scheduler allocate 4000 200
ntp clock-period 17179833
ntp source Loopback1
ntp server 192.168.42.130 prefer
ntp server 192.168.42.162
ntp server 192.168.42.161
```

```
!
end

IER72061#
```

Cisco Application Control Engine

Note: The following configurations have not been audited by QSA as ACE was primarily used only to loadbalance ACE XML Gateway. This product is not documented in the Report of Compliance (ROC) prepared by VerizonBusiness.

```
----- show version -----
```

```
ACE1/PCI# sh ver
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
```

```
Software
 loader:      Version 12.2[120]
 system:      Version 3.0(0)A1(4a) [build 3.0(0)A1(4a) adbuild_20:11:06-2007/02/0
6_/auto/adbu-rel/ws/REL_3_0_0_A1_4A]
 system image file: [LCP] disk0:c6ace-t1k9-mz.3.0.0_A1_4a.bin
 installed license: no feature license is installed
```

```
Hardware
Cisco ACE (slot: 3)
cpu info:
 number of cpu(s): 2
 cpu type: SiByte
 cpu: 0, model: SiByte SB1 V0.2, speed: 700 MHz
 cpu: 1, model: SiByte SB1 V0.2, speed: 700 MHz
memory info:
 total: 958004 kB, free: 354284 kB
 shared: 0 kB, buffers: 1892 kB, cached 0 kB
cf info:
 filesystem: /dev/cf
 total: 1000512 kB, used: 360720 kB, available: 639792 kB
```

```
last boot reason: SUP request
configuration register: 0x1
ACE1 kernel uptime is 9 days 5 hours 42 minute(s) 17 second(s)
```

```
----- show running-config -----
```

```
ACE1/Admin# sh run
Generating configuration....

logging enable
logging buffered 7
```

```
hostname ACE1
boot system image:c6ace-t1k9-mz.3.0.0_A1_4a.bin

class-map type management match-any remote-mgmt
  10 match protocol ssh source-address 192.168.42.131 255.255.255.255
  30 match protocol icmp any

policy-map type management first-match remote-access
  class remote-mgmt
    permit

ft interface vlan 85
  ip address 192.168.20.9 255.255.255.252
  peer ip address 192.168.20.10 255.255.255.252
  no shutdown

ft peer 1
  heartbeat interval 300
  heartbeat count 10
  ft-interface vlan 85

ft group 11
  peer 1
  no preempt
  priority 110
  peer priority 105
  associate-context Admin
  inservice

domain <removed>

ip route 0.0.0.0 0.0.0.0 192.168.20.25

context PCI
  allocate-interface vlan 82-83
  allocate-interface vlan 95

ft group 10
  peer 1
  no preempt
  priority 110
  peer priority 105
  associate-context PCI
  inservice
username <removed> password 5 <removed>/ role Admin domain default-domain
username <removed> password 5 <removed> role Admin domain <removed>
ssh key rsa 1024 force

ACE1/Admin#

ACE1/PCI# sh run
Generating configuration...

logging enable
logging timestamp
logging buffered 7
logging monitor 7
logging device-id context-name
logging host <syslog server> udp/514
logging rate-limit 1 120 message 302027
```

```
login timeout 15

tacacs-server host 192.168.42.131 key 7 <removed>
aaa group server tacacs+ RETAIL
    server 192.168.42.131
aaa authentication login default group RETAIL local
aaa authentication login console group RETAIL local
aaa accounting default group RETAIL local

access-list allow2server line 20 extended permit ip any host 192.168.20.3
access-list allow2server line 21 extended permit tcp host 192.168.20.44 host
192.168.42.130 eq ldap
access-list allow2server line 22 extended deny ip any any
access-list in2out line 10 extended permit ip host 192.168.20.3 any
access-list in2out line 15 extended deny ip any any
access-list out2in line 10 extended permit tcp any host 192.168.20.1 eq www
access-list out2in line 15 extended deny ip any any

probe icmp ICMP
    interval 2
    faildetect 2
    passdetect interval 60
    passdetect count 2

rserver host ECOM
    ip address 192.168.20.44
    inservice

serverfarm host PCI-ECOM
    predictor leastconns
    probe ICMP
    rserver ECOM
    inservice

class-map match-any ECOMVIP
    11 match virtual-address 192.168.20.1 any
class-map type management match-any remote-mgmt
    10 match protocol ssh source-address 192.168.42.131 255.255.255.0
    30 match protocol icmp any

policy-map type management first-match remote-access
    class remote-mgmt
        permit
policy-map type loadbalance first-match ECOMPOLICY
    class class-default
        serverfarm PCI-ECOM
policy-map multi-match ECOM_MATCH
    class ECOMVIP
        loadbalance vip inservice
        loadbalance policy ECOMPOLICY

service-policy input remote-access

interface vlan 82
    description ACE_outside
    ip address 192.168.20.28 255.255.255.248
    ip verify reverse-path
    alias 192.168.20.30 255.255.255.248
    peer ip address 192.168.20.29 255.255.255.248
    access-group input out2in
    service-policy input ECOM_MATCH
    no shutdown
```

```
interface vlan 83
  description ACE_inside
  ip address 192.168.20.4 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.6 255.255.255.248
  peer ip address 192.168.20.5 255.255.255.248
  access-group input in2out
  no shutdown
interface vlan 95
  description ACE_inside_xml_gateway
  ip address 192.168.20.41 255.255.255.248
  ip verify reverse-path
  alias 192.168.20.43 255.255.255.248
  peer ip address 192.168.20.42 255.255.255.248
  access-group input allow2server
  no shutdown

domain cisco-irn.com

ip route 0.0.0.0 0.0.0.0 192.168.20.25
username <removed> password 5 <removed> role Admin domain default-domain

snmp-server contact "CISCO_IRN"
snmp-server location "IE"
snmp-server community <removed> group Network-Monitor
snmp-server community <removed> group Network-Monitor

snmp-server host <snmp Manager> traps version 1 <removed>
snmp-server enable traps slb vserver
snmp-server enable traps slb real
snmp-server enable traps syslog
snmp-server enable traps snmp authentication
snmp-server enable traps snmp linkup
snmp-server enable traps snmp linkdown

ACE1/PCI#
```

Data Center Configurations

Cisco Catalyst 3750

```
AggSw-1#show ver
Cisco IOS Software, C3750 Software (C3750-IPBASE-M), Version 12.2(25)SEE2, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 08:46 by yenanh
Image text-base: 0x00003000, data-base: 0x00EE3E54

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: C3750 Boot Loader (C3750-HBOOT-M) Version 12.2(25r)SEC, RELEASE SOFTWARE (fc4)

AggSw-1 uptime is 21 weeks, 5 days, 3 hours, 8 minutes
System returned to ROM by power-on
System image file is "flash:c3750-ipbase-mz.122-25.SEE2/c3750-ipbase-mz.122-25.SEE2.bin"

cisco WS-C3750-48P (PowerPC405) processor (revision J0) with 118784K/12280K bytes of
memory.
Processor board ID CAT1108NJLP
```

```
Last reset from power-on
1 Virtual Ethernet interface
48 FastEthernet interfaces
4 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
```

```
512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address      : 00:1B:2B:10:58:80
Motherboard assembly number    : 73-9675-11
Power supply part number       : 341-0029-05
Motherboard serial number      : CAT110850H9
Power supply serial number     : LIT110504EW
Model revision number          : J0
Motherboard revision number    : A0
Model number                   : WS-C3750-48PS-S
System serial number           : CAT1108NJLP
SFP Module assembly part number : 73-7757-03
SFP Module revision Number     : A0
SFP Module serial number       : CAT11075H68
Top Assembly Part Number       : 800-25858-03
Top Assembly Revision Number   : G0
Version ID                     : V05
CLEI Code Number               : COM1W00ARB
Hardware Board Revision Number : 0x01
```

Switch	Ports	Model	SW Version	SW Image	
*	1	52	WS-C3750-48P	12.2(25)SEE2	C3750-IPBASE-M

Configuration register is 0xF

AggSw-1#

```
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname AggSw-1
!
***Configure enable secret instead of enable password***

enable secret 5 <removed>.
!
*** External TACACS authentication used; defaults to local user authentication
if TACACS unavailable***

aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
***SSH v2 preferred over v1 because of stronger encryption and key exchange***
ip ssh version 2

***SNMP version 3 used; encryption of SNMP data supported***
```

```

access-list 88 permit 192.168.42.0 0.0.0.255
access-list 88 deny any log

snmp-server group PCI v3 noauth notify FFFFFFFFFFFFFFFF
snmp-server group PCI v3 auth access 88
snmp-server group priv v3 auth notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF0F
snmp-server location DC
snmp-server host 192.168.42.118 version 3 auth <removed>
snmp-server host 192.168.42.134 version 3 auth <removed>
snmp-server community <removed> RW 88
snmp-server community <removed> RO 88
snmp-server packetsize 8192
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps rtr

*** Disable insecure remote access to the switch, such as unencrypted HTTP ***
no ip http server
ip http secure-server

ip tacacs source-interface Vlan999
!
logging source-interface Vlan995
logging 192.168.42.121
logging 192.168.42.118
logging 192.168.44.121
!
!

control-plane
!
banner exec ^CCC
WARNING:
    **** THIS SYST IS PRIVATE PROPERTY FOR THE USE OF CMO Re`il ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESEATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TOAW
ENFORCEMENT OFFICIALS AND PROSECUTION TN THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C
banner incoming ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
        **** AUTHORIZED USERS ONLY! ****

ANY USE OF T
IS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUBH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FUR@HER NOTICE OR CONSENT. UNAUTHORIZED USE OD THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DILOSURE TO LAW S
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION D STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.
^C

```

```

banner login ^CCC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED SERS ONLY!
^C
banner motd ^CCncom^C
!
line con 0
 session-timeout 15 output
 exec-timeout 60 0
 privilege level 15
 login authentication RLOCAL
line vty 0 4
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
line vty 5 15
 session-timeout 15 output
 access-class 23 in
 exec-timeout 60 0
 logging synchronous
 login authentication RETAIL
 transport input ssh
!
ntp clock-period 36029253
ntp source Vlan995
ntp server 192.168.42.130
ntp server 192.168.62.162
ntp server 192.168.62.161 prefer
end

```

Cisco Catalyst 6500

** 6500 at the DC Core **

```

RCORE-10#show version
Cisco Internetwork Operating System Software
IOS (tm) s72033_rp Software (s72033_rp-IPSERVICES_WAN-VM), Version 12.2(18)SXF7, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by cisco Systems, Inc.
Compiled Thu 23-Nov-06 07:41 by kellythw
Image text-base: 0x01020150, data-base: 0x01021000

ROM: System Bootstrap, Version 12.2(17r)S4, RELEASE SOFTWARE (fc1)
BOOTLDR:
RCORE-10 uptime is 4 weeks, 2 days, 24 minutes
Time since RCORE-10 switched to active is 4 weeks, 2 days, 24 minutes
System returned to ROM by power cycle (SP by power on)
System image file is "sup-bootdisk:s72033-ipserVICES_wan-vz.122-18.SXF7.bin"

cisco WS-C6509-E (R7000) processor (revision 1.3) with 1015808K/32768K bytes of memory.
Processor board ID SMG1104N1GN
SR71000 CPU at 600Mhz, Implementation 1284, Rev 1.2, 512KB L2 Cache
Last reset from s/w reset
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
TN3270 Emulation software.
2 Virtual Ethernet/IEEE 802.3 interfaces

```



```

68 Gigabit Ethernet/IEEE 802.3 interfaces
9 Ten Gigabit Ethernet/IEEE 802.3 interfaces
1917K bytes of non-volatile configuration memory.

65536K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102

service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption

***External authentication used by default; else use local accounts***

aaa new-model
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL local group tacacs+
aaa authentication login TEST group tacacs+
aaa authentication enable default group tacacs+ enable line
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common

***Disable insecure methods of access like unencrypted HTTP***

no ip http server

***syslogging to CS MARS and NCM servers*****
logging 192.168.42.118
logging 192.168.44.121

***SNMP version 3 chosen for data encryption support*****
snmp-server engineID local 0123456789
snmp-server group group1 v3 auth read group1read
snmp-server trap-source Loopback0
snmp-server packetsize 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps entity
snmp-server enable traps rtr
snmp-server enable traps rsvp
snmp-server enable traps hsrp
snmp-server enable traps frame-relay
snmp-server enable traps config
snmp-server host 192.168.42.134 retaillab

***External authentication via TACACS*****
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key 7 03165E1F07062D5C4D00
ip tacacs source-interface GigabitEthernet1/37

!
radius-server source-ports 1645-1646

***Requiring local authentication on console session and external
Authentication on SSH; restricting remote access to SSH and not telnet***

line con 0
exec-timeout 15 0

```

```

privilege level 15
password 7 044B080F1D24584F0015
logging synchronous
login authentication RLOCAL
transport input ssh
line vty 0 4
exec-timeout 15 0
password 7 02050D480809
logging synchronous
login authentication RETAIL
transport input ssh
line vty 5 15
exec-timeout 60 0
password 7 121A0C041104
logging synchronous
login authentication RETAIL
transport input ssh

```

Cisco 7206 VXR Router

```

===== PuTTY log 2008.02.06 16:13:34 =====
show version
Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.4(16a), RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 10-Sep-07 18:13 by prod_rel_team

ROM: System Bootstrap, Version 12.3(4r)T3, RELEASE SOFTWARE (fc1)
BOOTLDR:

RWAN-10 uptime is 9 weeks, 5 days, 1 hour, 32 minutes
System returned to ROM by power-on
System image file is "disk2:c7200-jk9s-mz.124-16a.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

--More--          A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 7206VXR (NPE-G1) processor (revision B) with 983040K/65536K bytes of memory.
Processor board ID 34978783
SB-1 CPU at 700MHz, Implementation 1025, Rev 0.2, 512KB L2 Cache
6 slot VXR midplane, Version 2.11

Last reset from power-on

PCI bus mb1 (Slots 1, 3 and 5) has a capacity of 600 bandwidth points.
Current configuration on bus mb1 has a total of 600 bandwidth points.
This configuration is within the PCI bus capacity and is supported.

```

PCI bus mb2 (Slots 2, 4 and 6) has a capacity of 600 bandwidth points.
 Current configuration on bus mb2 has a total of 0 bandwidth points.
 This configuration is within the PCI bus capacity and is supported.

Please refer to the following document "Cisco 7200 Series Port Adaptor
 --More-- Hardware Configuration Guidelines" on Cisco.com <<http://www.cisco.com>>
 for c7200 bandwidth points oversubscription and usage guidelines.

3 Gigabit Ethernet interfaces
 1 Virtual Private Network (VPN) Module
 509K bytes of NVRAM.

251904K bytes of ATA PCMCIA card at slot 2 (Sector size 512 bytes).
 16384K bytes of Flash internal SIMM (Sector size 256K).
 Configuration register is 0x2102

```
RWAN-10#
RWAN-10#show run
Building configuration...
```

```
Current configuration : 6417 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RWAN-10
!
boot-start-marker
boot system flash disk2:c7200-jk9s-mz.124-16a.bin
boot-end-marker
!
enable secret 5 $1$cM8m$gKKyxChLyhdQMqbJUBeM1.
!
aaa new-model
!
!
aaa authentication login RETAIL group tacacs+ local
aaa authentication login RLOCAL local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization exec default group tacacs+ if-authenticated
--More--      aaa accounting update newinfo
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
!
!
ip cef
ip domain name cisco-irn.com
!
!
!
!
!
!
!
!
!
```

```

!
!
!
--More--
!
!
crypto pki trustpoint TP-self-signed-34978783
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-34978783
  revocation-check none
  rsakeypair TP-self-signed-34978783
!
crypto pki trustpoint TP-self-signed-1
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1
  revocation-check none
  rsakeypair TP-self-signed-1
!
!
crypto pki certificate chain TP-self-signed-34978783
  certificate self-signed 01
    30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
    2F312D30 2B060355 04031324 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 33343937 38373833 301E170D 30323037 30333033 32363031
    5A170D32 30303130 31303030 3030305A 302F312D 302B0603 55040313 24494F53
    2D53656C 662D5369 676E6564 2D436572 74696669 63617465 2D333439 37383738
    3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100D724
    --More--          264845C3 D19C3236 4E194C24 956B01E1 E3079BC3 D83FBD68 43383CE1
918F3A69
    6046A3D9 999CCFC3 55846A63 09300596 1AB98F32 BB8B92AF 284A5313 58C03EBD
    3C383D98 FE07E155 E7FA0632 FCFBF124 6952E5A4 E7390DFB 8B11DE1B 7B3FD607
    CB64A853 15A0405E 88A21642 7F577D4E 4501C053 9A1C18A8 9D0A8831 0E130203
    010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603 551D1104
    19301782 15525741 4E2D3130 2E636973 636F2D69 726E2E63 6F6D301F 0603551D
    23041830 16801448 AF0217A7 5D7D0C19 61E93E4B A2E6AE3E 6665B830 1D060355
    1D0E0416 041448AF 0217A75D 7D0C1961 E93E4BA2 E6AE3E66 65B8300D 06092A86
    4886F70D 01010405 00038181 000B9A38 C00A1722 FB11196C 0DF270A3 F8C9E17E
    C2F0F65B E1803898 410698B6 2644581F 3324BA4E 9F41477D BA111077 CEED03A6
    B8C768F7 85A4E1D3 D4375477 DEBB5F1B 0FE89F41 5F54621C EC29900A 4746CEA1
    756FE59F D734B107 3D162616 3E76C301 3F287011 80D15D71 D90D3DBC 588BC42D
    30EC2A1F FD414749 75CA4EDB F0
  quit
crypto pki certificate chain TP-self-signed-1
  username administrator privilege 15 secret 5 $1$McmC$gb30qCt8c8r01bZQsBZec0
!
!
!
controller ISA 1/1
!
!
!
crypto isakmp policy 1
  --More--
  encr 3des
!
!
crypto ipsec transform-set PCI esp-3des
!
crypto map toLarge 1 ipsec-isakmp
  set peer 10.10.62.2
  set transform-set PCI
  match address 101
!
!
!

```

```
!  
interface Loopback0  
  ip address 192.168.1.11 255.255.255.255  
!  
interface GigabitEthernet0/1  
  ip address 192.168.10.29 255.255.255.252  
  duplex auto  
  speed auto  
  media-type rj45  
  no negotiation auto  
!  
  --More--  
interface GigabitEthernet0/2  
  ip address 192.168.12.1 255.255.255.0  
  duplex half  
  speed auto  
  media-type rj45  
  no negotiation auto  
!  
interface GigabitEthernet0/3  
  description temporary connection to VLAN 42 for TFTP server  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
  media-type rj45  
  no negotiation auto  
!  
ip route 0.0.0.0 0.0.0.0 192.168.10.30  
ip route 192.168.0.0 255.255.255.0 192.168.10.30  
ip route 192.168.10.20 255.255.255.252 192.168.10.30  
ip route 192.168.10.24 255.255.255.252 192.168.10.30  
ip route 192.168.10.36 255.255.255.252 192.168.10.30  
ip route 192.168.10.40 255.255.255.252 192.168.10.30  
ip route 192.168.42.0 255.255.255.0 192.168.10.30  
  --More--      ip route 192.168.44.0 255.255.255.0 192.168.10.30  
!  
no ip http server  
ip http secure-server  
!  
!  
logging source-interface Loopback0  
logging 192.168.42.118  
logging 192.168.44.121  
logging 192.168.10.22  
logging 192.168.42.121  
access-list 101 permit ip 10.10.0.0 0.0.255.255 192.168.0.0 0.0.255.255  
snmp-server community pciretail RW  
snmp-server chassis-id RWAN-10  
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart  
snmp-server enable traps tty  
snmp-server enable traps casa  
snmp-server enable traps srp  
snmp-server enable traps hsrp  
snmp-server enable traps config  
snmp-server enable traps entity  
snmp-server enable traps config-copy  
snmp-server enable traps bgp  
  --More--      snmp-server enable traps pim neighbor-change rp-mapping-change  
invalid-pim-message  
snmp-server enable traps ipmulticast  
snmp-server enable traps msdp  
snmp-server enable traps rsvp  
snmp-server enable traps frame-relay
```

```

snmp-server enable traps frame-relay subif
snmp-server enable traps syslog
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps voice poor-gov
!
!
tacacs-server host 192.168.42.131
tacacs-server directed-request
tacacs-server key retailpci
!
!
control-plane
!
!
!
--More--
!
!
!
gatekeeper
shutdown
!
banner exec ^CC
WARNING:
    **** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CMO Retail ****
    **** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT
TO MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY
TO IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER
REPRESENTATIVES OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW
ENFORCEMENT OFFICIALS AND PROSECUTION TO THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL, CIVIL AND CRIMINAL LAWS.
^C
!
line con 0
--More--
exec-timeout 15 0
logging synchronous
transport output all
stopbits 1
line aux 0
transport output all
stopbits 1
line vty 0 4
exec-timeout 15 0
logging synchronous
login authentication RETAIL
transport preferred ssh
transport input ssh
transport output ssh
line vty 5 15
exec-timeout 15 0
login authentication RETAIL
transport preferred ssh
transport input telnet
transport output all
!
ntp clock-period 17179833

```

```
ntp source Loopback0
--More--
ntp server 192.168.42.130 prefer
ntp server 192.168.42.162
ntp server 192.168.42.161
!
end

RWAN-10#
```

Cisco Adaptive Security Appliance

```
** ASA5540 configured with AIP-SSM, VPN tunnel for remote users **

** show run **

: Saved

:

ASA Version 7.2(2)

!

hostname AggAsa-1

domain-name cisco-irn.com

enable password RME3c/DSNu0rCc3V encrypted

names

name 192.168.42.130 DNS

name 192.168.42.140 MS-Exchange

name 192.168.62.161 NTP1

name 192.168.62.162 NTP2

name 192.168.42.131 TACACS_Server

name 192.168.42.72 RSA_FSM1

name 192.168.42.113 RSA_FSM2

!

interface GigabitEthernet0/0

 nameif outside

 security-level 0

 ip address 192.168.10.30 255.255.255.252

!

interface GigabitEthernet0/1

 nameif inside
```

```
security-level 100

ip address 192.168.10.37 255.255.255.252

<--- More --->

!

interface GigabitEthernet0/2

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet0/3

shutdown

no nameif

no security-level

no ip address

!

interface Management0/0

description Mgmt connected to RCORE-1.

nameif management

security-level 100

ip address 192.168.11.9 255.255.255.0

management-only

!

passwd NoXXysFNqSeoLcJe encrypted

!

time-range time1

absolute start 00:14 03 October 2007 end 20:14 03 October 2007

<--- More --->

periodic daily 0:00 to 23:59

!

banner login This is for Authorized use of personnel from ACME Inc. only. All other acces
is strictly prohibited.

boot system disk0:/asa722-k8.bin
```



```
no ftp mode passive

clock timezone PST -8

clock summer-time PDT recurring

dns server-group DefaultDNS
  domain-name cisco-irn.com

object-group service udpser udp
  port-object eq domain
  port-object eq netbios-dgm
  port-object eq netbios-ns
  port-object eq tftp

object-group network DC-Network-Services
  network-object host DNS
  network-object host 192.168.42.132
  network-object host MS-Exchange
  network-object host NTP1
  network-object host NTP2

object-group network SysLog-Servers
  description MARS, NCM, CAS
  network-object host 192.168.42.118
  network-object host 192.168.42.119
  network-object host 192.168.42.121

object-group network DC-Partner
  network-object 192.168.42.0 255.255.255.0
  network-object 192.168.46.0 255.255.255.0
  network-object 192.168.52.0 255.255.255.0

object-group network Large-Store-Partner
  network-object 10.10.48.0 255.255.255.0
  network-object 10.10.49.0 255.255.255.0

object-group service Ports-for-POS tcp
  port-object eq 19978
  port-object range ftp-data ftp
  port-object eq 5014
```

```

port-object eq 5015

port-object eq 5766

port-object eq https

access-list inside_access_in extended permit ip any any

access-list TEST_splitTunnelAcl standard permit 2.0.0.0 255.0.0.0

access-list outside extended permit ip any any

access-list outside remark NCR POS to TACACS, RSA FSM, POS-DC

access-list outside remark Large store routers with TACACS server

access-list outside remark Large store routers with TACACs server

access-list outside remark Large store LAN routers with TACACS

access-list outside remark Large store LAN routers to TACACS

access-list outside remark Wireless infrastructure from large store to TACACS.

access-list outside remark HTTPS from any large store device to any DC device.

access-list outside remark Large store wireless infrastructure to TACACS

access-list outside remark CSA on POS clients to CSA Manager

access-list outside remark POS Clients from Large store to CS Manager

access-list outside remark Open unsecured HTTP between large store and DC only for POS
clients to specific CSA Manager server

access-list outside remark Large store Partner machines to Network services (DNS, SMTP,
TACACS, NTP) in datacenter

access-list outside remark Large store infrastructure devices with MARS, NCM, and CAS

access-list outside remark Large Store Infrastructure devices with MARS, CAS, NCM

access-list outside remark DC infrastructure with MARS, CAS, NCM

access-list outside remark DC Infrastructure devices with Network Services

access-list outside remark Ports needed for Partner apps in Large store

access-list outside remark NCR POS to TACACS, RSA FSM, POS-DC

access-list outside remark Large store routers with TACACS server

access-list outside remark Large store routers with TACACs server

access-list outside remark Large store LAN routers with TACACS

access-list outside remark Large store LAN routers to TACACS

access-list outside remark Wireless infrastructure from large store to TACACS.

access-list outside remark HTTPS from any large store device to any DC device.

access-list outside remark Large store wireless infrastructure to TACACS

```

```
access-list outside remark CSA on POS clients to CSA Manager

access-list outside remark POS Clients from Large store to CS Manager

access-list outside remark Open unsecured HTTP between large store and DC only for POS
clients to specific CSA Manager server

access-list outside remark Large store Partner machines to Network services (DNS, SMTP,
TACACS, NTP) in datacenter

access-list outside remark Large store infrastructure devices with MARS, NCM, and CAS

access-list outside remark Large Store Infrastructure devices with MARS, CAS, NCM

access-list outside remark DC infrastructure with MARS, CAS, NCM

access-list outside remark DC Infrastructure devices with Network Services

access-list outside remark Ports needed for Partner apps in Large store

access-list inside extended permit ip any any

access-list outside_access_out extended permit ip any any

access-list IPS extended permit ip any any

pager lines 24

logging enable

logging emblem

logging list IDS_events level informational class ids

logging list User_authentication level informational class auth

logging list User_sessions_to_ASA level informational class session

logging list Config_changes level informational class config

logging buffer-size 8192

logging buffered debugging

logging trap warnings

logging asdm informational

logging host inside 192.168.42.121 6/1470

logging class session trap informational

mtu management 1500

mtu inside 1500

mtu outside 1500

ip local pool ippool 1.1.1.100-1.1.1.200 mask 255.255.255.0

ip local pool Retail-pool 192.168.55.2-192.168.55.253 mask 255.255.255.0

ip local pool INSIDEPOOL 192.168.10.38-192.168.10.39 mask 255.255.255.248
```

```
ip verify reverse-path interface management
ip verify reverse-path interface inside
ip verify reverse-path interface outside
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
asdm history enable
arp timeout 14400
access-group inside_access_in in interface inside
access-group inside out interface inside
access-group outside in interface outside
access-group outside_access_out out interface outside
route management 171.0.0.0 255.0.0.0 192.168.11.1 1
route inside 192.168.10.24 255.255.255.252 192.168.10.38 1
route inside 192.168.10.40 255.255.255.252 192.168.10.38 1
route inside 192.168.42.0 255.255.255.0 192.168.10.38 1
route inside 192.168.10.20 255.255.255.252 192.168.10.38 1
route inside 0.0.0.0 0.0.0.0 192.168.0.2 1
route inside 192.168.62.0 255.255.255.0 192.168.10.38 1
route inside 192.168.44.0 255.255.255.0 192.168.10.38 1
route inside 192.168.0.0 255.255.0.0 192.168.10.38 1
route outside 192.168.12.0 255.255.255.0 192.168.10.29 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
aaa-server radius protocol radius
aaa-server radius host TACACS_Server
key cisco1
radius-common-pw cisco1
aaa-server TACACS protocol tacacs+
```

```
aaa-server TACACS host TACACS_Server

key retailpci

aaa-server SDI protocol sdi

reactivation-mode timed

aaa-server SDI host 192.168.42.136

retry-interval 3

timeout 13

group-policy TEST internal

group-policy TEST attributes

vpn-tunnel-protocol IPSec

split-tunnel-policy tunnelspecified

split-tunnel-network-list value TEST_splitTunnelAcl

group-policy Retail-Remote-Group internal

group-policy Retail-Remote-Group attributes

<--- More --->

dns-server value 192.168.42.130

vpn-tunnel-protocol IPSec

default-domain value cisco-irn.com

username Administrator password 7yuj1JlcXnFvivy7G encrypted privilege 15

username karechan password czJlQkYZuQdSxKOj encrypted privilege 15

username karechan attributes

vpn-group-policy Retail-Remote-Group

username Karen password 5EaxIssboAKknou7 encrypted privilege 15

aaa authentication http console TACACS LOCAL

aaa authentication ssh console TACACS LOCAL

aaa authentication serial console TACACS LOCAL

aaa authentication enable console TACACS LOCAL

http server enable

http 192.168.42.0 255.255.255.0 inside

http 0.0.0.0 0.0.0.0 inside

snmp-server host inside 192.168.42.118 community pciretail version 2c

snmp-server location AggASA-1
```

```
no snmp-server contact

snmp-server community pciretail

snmp-server enable traps snmp authentication linkup linkdown coldstart

sysopt noproxyarp management

sysopt noproxyarp inside

auth-prompt prompt Login to TACACs

auth-prompt accept Logged in.

<--- More --->

auth-prompt reject Can't log in.

service internal

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac

crypto dynamic-map outside_dyn_map 20 set pfs

crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-SHA

crypto dynamic-map outside_dyn_map 40 set pfs

crypto dynamic-map outside_dyn_map 40 set transform-set ESP-3DES-SHA

crypto dynamic-map outside_dyn_map 60 set pfs

crypto dynamic-map outside_dyn_map 60 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside

crypto isakmp enable outside

crypto isakmp policy 10

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

tunnel-group TEST type ipsec-ra

tunnel-group TEST general-attributes

address-pool ippool

authentication-server-group radius

default-group-policy TEST

tunnel-group TEST ipsec-attributes
```

```
pre-shared-key *
tunnel-group Retail-Remote-Group type ipsec-ra
tunnel-group Retail-Remote-Group general-attributes
address-pool Retail-pool
authentication-server-group TACACS
default-group-policy Retail-Remote-Group
tunnel-group Retail-Remote-Group ipsec-attributes
pre-shared-key *
tunnel-group PCIVPN type ipsec-ra
tunnel-group PCIVPN general-attributes
address-pool Retail-pool
authentication-server-group TACACS
tunnel-group PCIVPN ipsec-attributes
pre-shared-key *
telnet timeout 5
ssh scopy enable
ssh 0.0.0.0 0.0.0.0 management
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 5
ssh version 2
console timeout 5
management-access management
!
class-map global-class
<--- More --->
match default-inspection-traffic
class-map ipsinline
match access-list IPS
!
!
policy-map global-policy
class global-class
```

```
inspect ctiqbe
inspect dcerpc
inspect dns
inspect esmtp
inspect ftp
inspect h323 h225
inspect h323 ras
inspect http
inspect icmp
inspect icmp error
inspect ils
inspect ipsec-pass-thru
inspect mgcp
inspect netbios
inspect pptp
inspect rsh
inspect rtsp
<--- More --->
inspect sip
inspect skinny
inspect snmp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect xdmcp
class ipsinline
ips inline fail-close
!
service-policy global-policy global
ntp server NTP2 source inside
ntp server NTP1 source inside prefer
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 rc4-md5
```



```
privilege cmd level 3 mode exec command perfmon
privilege cmd level 3 mode exec command ping
privilege cmd level 3 mode exec command who
privilege cmd level 3 mode exec command logging
privilege cmd level 3 mode exec command failover
privilege show level 5 mode exec command running-config
privilege show level 3 mode exec command reload
privilege show level 3 mode exec command mode
privilege show level 3 mode exec command firewall
privilege show level 3 mode exec command interface
privilege show level 3 mode exec command clock
privilege show level 3 mode exec command dns-hosts
privilege show level 3 mode exec command access-list
privilege show level 3 mode exec command logging
privilege show level 3 mode exec command ip
privilege show level 3 mode exec command failover
privilege show level 3 mode exec command asdm
privilege show level 3 mode exec command arp
privilege show level 3 mode exec command route
privilege show level 3 mode exec command ospf
privilege show level 3 mode exec command aaa-server
privilege show level 3 mode exec command aaa
privilege show level 3 mode exec command crypto
privilege show level 3 mode exec command vpn-sessiondb
privilege show level 3 mode exec command ssh
privilege show level 3 mode exec command dhcpcd
privilege show level 3 mode exec command vpn
privilege show level 3 mode exec command blocks
privilege show level 3 mode exec command uauth
privilege show level 3 mode configure command interface
privilege show level 3 mode configure command clock
privilege show level 3 mode configure command access-list
```

```
privilege show level 3 mode configure command logging
privilege show level 3 mode configure command ip
privilege show level 3 mode configure command failover
privilege show level 5 mode configure command asdm
privilege show level 3 mode configure command arp
privilege show level 3 mode configure command route
privilege show level 3 mode configure command aaa-server
privilege show level 3 mode configure command aaa
privilege show level 3 mode configure command crypto
privilege show level 3 mode configure command ssh
privilege show level 3 mode configure command dhcpd
privilege show level 5 mode configure command privilege
privilege clear level 3 mode exec command dns-hosts
privilege clear level 3 mode exec command logging
privilege clear level 3 mode exec command arp
privilege clear level 3 mode exec command aaa-server
privilege clear level 3 mode exec command crypto
privilege cmd level 3 mode configure command failover
privilege clear level 3 mode configure command logging
privilege clear level 3 mode configure command arp
privilege clear level 3 mode configure command crypto
privilege clear level 3 mode configure command aaa-server
prompt hostname context

Cryptochecksum:c1ee72c1ed9928a7bc78c62c1d4758e2

: end

AggAsa-1#
```



APPENDIX **F**

Report on Compliance (ROC)

The following document is the Report on Compliance (ROC), prepared by Cybertrust, that was performed on the PCI for Retail Solution lab that was built in San Jose, California.



Note

Cisco Systems is not responsible for the content of the following Cybertrust document. It is only provided as a reference. Cybertrust is solely responsible for the following content.



Security Solutions powered by Cybertrust

Verizon Business Assessment: Cisco PCI Solution for Retail

Security Audit Procedures

PCI DSS - Version 1.1

Release: September 2006

Report Date: 02/08/2008

Table of Contents

Security Audit Procedures	1
PCI DSS - Version 1.1	1
Table of Contents	2
Contact Information.....	3
Executive Summary	4
Description of Scope and Methodology	6
Version of the Security Audit Procedures	6
Timeframe.....	6
Scope.....	6
Exclusions.....	9
Overall Description	10
Individuals interviewed.....	11
Documentation Reviewed.....	13
Key Technology	14
Quarterly Scan Results	15
Build and Maintain a Secure Network.....	16
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.....	16
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....	22
Protect Cardholder Data	31
Requirement 3: Protect stored cardholder data	31
Requirement 4: Encrypt transmission of cardholder data across open, public networks.....	48
Maintain a Vulnerability Management Program.....	51
Requirement 5: Use and regularly update anti-virus software or programs.....	51
Requirement 6: Develop and maintain secure systems and applications.....	54
Implement Strong Access Control Measures	64
Requirement 7: Restrict access to cardholder data by business need-to-know	64
Requirement 8: Assign a unique ID to each person with computer access.....	67
Requirement 9: Restrict physical access to cardholder data	79
Regularly Monitor and Test Networks.....	84
Requirement 11: Regularly test security systems and processes.....	101
Maintain an Information Security Policy.....	104
Requirement 12: Maintain a policy that addresses information security for employees and contractors.....	104

Contact Information

VERIZON BUSINESS, INC.

Aaron Reynolds

Senior Security Consultant

Tel: 425-609-7859 (office)

Email: aaron.reynolds@verizonbusiness.com

Cisco Systems, Inc.

Karen Chan, Technical Marketing Engineer

Rupesh Chakkingal, Vertical Application Architect/TME

Executive Summary

Assessment Description

Cisco has engaged Verizon Business to conduct a PCI assessment of their “PCI Solution for Retail” architecture, based on the PCI DSS v1.1 standard. Cisco will market their solution to retail customers looking to meet PCI requirements, specifically within their retail environment and within their back-end data center infrastructure. Cisco has used findings from the assessment to ensure configurations within their solution meet PCI requirements specific to their solution, and plan to provide the results of the assessment to Cisco Sales Engineers interfacing with retail customers.

Verizon Business’ assessment covered three PCI retail architectures (see “Scope” section), targeted to small, medium, and large retail environments. Verizon Business found the three solution architectures to directly address several technical PCI requirements, and can address other requirements either as a compensating control, or in conjunction with compensating controls. The retail architectures are designed to be deployed within a POS retail location, with central management/logging components deployed in a data center environment.

As Cisco’s PCI Solution for Retail architecture only addresses some aspects of a merchant’s overall PCI compliance responsibility, several areas of PCI compliance are left to the merchant to obtain full compliance. The overall approach to the assessment was to focus validation efforts on components which are core to Cisco’s PCI Solution for Retail environment. System components outside of the Cisco PCI Solution for Retail environment (e.g. corporate email, corporate Internet/DMZ firewalls, central cardholder databases, mainframes, and corporate networks) were not included in the scope of the assessment.

Service Providers with Access to Cardholder Data

N/A – not applicable for this assessment

Processors Used

N/A – not applicable for this assessment

Connections to Payment Card Companies

N/A – not applicable for this assessment

POS Products Used (Merchants only; delete if N/A)

NCR Advanced Checkout Solution (ACS) POS software was used within the Cisco Solution for Retail environment. NCR ACS software has been successfully certified through the Payment Application Best Practice (PABP) certification process. NCR ACS software handles both

online and offline cardholder transactions, including debit and credit transactions. NCR ACS software protects “at rest” cardholder data through 3DES encryption, truncation, and masking, including for offline transactions.

Wireless LANs and/or wireless POS terminals connected to the cardholder environment

Wireless networks within the PCI Solution for Retail environment have been configured to use WPA-TKIP w/PEAP authentication, for secure wireless networking. All wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the PCI Solution for Retail network. Additionally, best practice security parameters have been applied to wireless networks, including: https access for wireless management, SSID broadcast disabled, default SSID has been changed, SNMPv3 used (default strings changed), and http access has been disabled.

Wholly-owned Entities

N/A – not applicable for this assessment

International Entities

N/A – not applicable for this assessment

Description of Scope and Methodology

Version of the Security Audit Procedures

The assessment was based on the PCI DSS v1.1 standard.

Timeframe

The assessment took place through several remote interviews, onsite and remote validation during the following two phases:

Phase 1: 11/16/2006 – 12/29/2006

Phase 2: 8/24/2007 – 12/12/2007

Scope

The assessment included the following “in scope” components:

- Large Retail environment
 - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity): Managed by CSA Manager from Data Center environment.
 - Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
 - Cisco switches – (4 – 2 layer 3 switches (Catalyst 4506), 2 layer 2 access switches (Catalyst 3750))
 - Wireless controllers – (1): Used to monitor and update wireless APs.
 - Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - Intermec POS: Wireless POS handheld.
 - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.
 - RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.

- Medium Retail environment
 - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
 - Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
 - Cisco 3560 layer 2 switches – (2)
 - Wireless APs – (1) : Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - Intermec POS: Wireless POS handheld.
 - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.
 - RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.
- Small Retail environment
 - Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
 - Cisco 2821 Integrated Services Router (ISR) – (1) – ISR is configured with Firewall and IDS/IPS feature set.
 - Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - Intermec POS: Wireless POS handheld.
 - RSA Key Manager Client – Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information.

- RSA File Security Manager Client – Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server.
- Data Center environment
 - Cisco Wireless Control System (WCS): Central platform for wireless configuration, management, and monitoring.
 - Cisco Security Monitoring, Analysis and Response System (CS-MARS): Central log monitoring, correlation, and reporting platform for Cisco network device security alerts (e.g. ASA/FWSM/ISR firewall logs and IDS/IPS alerts) within the Large, Medium, and Small retail environments, as well as the data center environment. In addition, Cisco Security Agent alerts are forwarded to CS-MARS.
 - CiscoWorks LAN Management Solution (LMS): Network device configuration management (e.g. routing and switching)
 - CiscoWorks Network Compliance Manager (NCM): CiscoWorks NCM tracks and regulates configuration and software changes across network infrastructure within the retail store and data center environments. Changes to network device configurations (e.g. enabling telnet, disabling exec timeout, enabling default usernames) are audited and reported through CiscoWorks NCM.
 - Cisco Security Manager (CSM): Central provisioning of device configuration and security policies, including: ASAs, FWSMs, IDS/IPS, ISRs and switches (e.g. firewall policy, IDS/IPS configuration and signature management, https access).
 - Cisco Security Agent (CSA) Manager – CSA software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
 - Cisco Secure Access Control Server (ACS) – AAA server
 - Cisco Application Control Engine (ACE – XML Gateway): Although initially designed for XML and SOAP-based web services, ACE XML Gateway demonstrated capabilities to provide application layer defense against html-based web vulnerabilities and attacks. ACE XML Gateway was deployed in the Internet Edge (DMZ) segment of the data center environment.
 - Cisco Adaptive Security Device Manager (ASDM): Secure, web-based configuration management of ASA firewalls.
 - Cisco IPS Device Manager (IDM): IDS/IPS configuration management.
 - Cisco Security Device Manager (SDM): Secure, web-based configuration management of 7206VXR routers.
 - Cisco 7206 VXR router (2 at Internet Edge, 2 at WAN aggregation): Access lists, routing, IPsec VPN termination.
 - Cisco Catalyst 3750 switch (6 – 2 Internet Edge, 4 WAN aggregation): Layer 3 switch (routing and access lists).
 - Cisco Catalyst 6509 Switch (8 – 2 Internet Edge, 2 core datacenter switch, 2 service aggregation switch, 2 access switch): Internet Edge – Routing, FWSM, IDSM2, and Application Control Engine (ACE – load balancer) modules, Core datacenter – layer 3 switch (routing and access lists), core service aggregation – layer 3 switch (routing, access lists, and IDSM module)
 - Cisco Catalyst 4948 Switch (2): Layer 2 access switch.

- Cisco Adaptive Security Appliance (ASA) 5540 (2): Stateful firewall filtering and integrated IDS/IPS @ data center boundary.
- RSA File Security Manager: Used to demonstrate secure storage of centralized data within datacenter environment. SFTP process transparently decrypts data on the POS server (within retail store environment) and sends to a central file server within the data center. The data is re-encrypted (AES-256) using RSA File Security Manager (FSM) before being written to the file system on the central file server. This was a small demonstration of RSA File Security Manager's capabilities to transparently encrypt/decrypt data using strong AES and/or 3DES encryption. The configuration of RSA File Security Manager within the assessed environment was found to meet all key management requirements under PCI DSS v1.1.
- RSA Key Manager: Used for cardholder data encryption (AES-256) within the NCR ACS server. RSA Key Manager provides application development libraries that support a wide range of development languages and can simplify the integration of encryption into point-of-sale, payment, and other applications that create or process cardholder information. RSA Key Manager is the central platform to manage security policies for encryption and decryption of data. The configuration of RSA Key Manager within the assessed environment was found to meet all key management requirements under PCI DSS v1.1.
- RSA Access Manager: Used for central authentication/logging for access to RSA Key Manager within the assessed environment.
- RSA Authentication Manager: Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
- RSA enVision: RSA's solution for compliance and security information management. RSA enVision was used to centrally collect RSA SecurID authentication logs on the RSA Authentication Manager server, using a batch process that runs several times a day.

Exclusions

Due to the nature of this assessment, several areas of a normal PCI assessment were excluded, including:

- Central cardholder data storage (limited to central storage on secure file repository, using RSA File Security Manager for data encryption)
- Authorization / Settlement processes
- Policies, procedures, and standards
- Assessment of "in transit" cardholder data (limited to transmission of test files between large store and data center using SCP to securely transmit file from back-office POS system (NCR ACS server) to secure file repository in data center environment)
- OS security for WCS, CS-MARS, CiscoWorks (LMS), CSM, CSA Manager, Cisco ACS, RSA enVision, RSA Key Manager, RSA File Security Manager, NCR Advanced Checkout Solution (ACS), RSA Authentication Manager, RSA Access Manager, Cisco Network Compliance Manager (NCM),
- Physical Security

- SDLC policies and procedures
- Live cardholder transactions (A fully functional POS environment, which includes authorization responses, was not available during the assessment)

Overall Description

Network Description

Cisco has designed three network architectures for small, medium, and large retail environments. Cisco has chosen Cisco Integrated Services Routers (ISRs) to provide firewall, IDS/IPS, and routing functionality. Extremely explicit access-lists are applied through CSM firewall policies, which are pushed to the ISRs in each architecture. Access-lists implicitly deny all inbound and outbound traffic to the PCI Solution for Retail; all traffic approved within each design is explicitly allowed to the port level. Additionally, Cisco has incorporated wireless into the design, using WPA-TKIP w/PEAP authentication, for secure wireless networking. All wireless traffic must pass through the ISRs and IOS firewall access-lists to traverse any part of the PCI Solution for Retail network.

The data center environment is segmented into multiple VLANs, including Internet Edge, WAN aggregation, and Core service aggregation. Multiple layers of network security are included in all data center segments, including FWSM and ASA stateful firewall filtering, IDS/IPS and integrated IDS/IPS detection/prevention, access lists, secure VPN (WAN aggregation and remote VPN), and two-factor authentication using RSA SecurID tokens.

All network devices within the PCI Solution for Retail are centrally managed through the following:

- Cisco Security Manager (CSM) - (Central security management for ISRs and switches (e.g. firewall policy, IDS/IPS signatures))
- CiscoWorks LAN Management Solution (LMS) – (Central configuration management for ISRs and switches (e.g. routing, switching, VLANs))
- CiscoWorks Network Compliance Manager (NCM) – (Central platform for auditing changes and enforcing configuration standards across network devices within the environment.)
- Cisco Wireless Control System (WCS) – (Central wireless management)
- Cisco Security Agent (CSA) Manager – (Central CSA software manager: HIDS, Host-based firewall, file monitoring / Access Control, Malware protection, zero-day, behavioral A/V protection)
- Cisco ACS – (Central TACACS+ (central authentication) server for ASA firewall, FWSM, ISR, 7206 VXR router, switch, wireless controller, CiscoWorks (LMS and NCM), CS-MARS, WCS, and CSM).
- CS-MARS – (Central logging / Correlation / Analysis / Alerting server. Alerts from IDS/IPS alerts, CSA alerts, firewall logs)
- Cisco ASDM – (Central configuration for ASA firewalls).
- Cisco IPS Device Manager (IDM): IDS/IPS configuration management.
- Cisco Security Device Manager (SDM): Secure, web-based configuration management of 7206VXR routers.
-

Application Description

NCR Advanced Checkout Solution (ACS) POS software was used within the Cisco Solution for Retail environment. NCR ACS software has been successfully certified through the Payment Application Best Practice (PABP) certification process. NCR ACS software handles both online and offline cardholder transactions, including debit and credit transactions. NCR ACS software protects “at rest” cardholder data through 3DES encryption, truncation, and masking, including for offline transactions.

Individuals interviewed

The following staff was interviewed:

Interviewee(s)	Topic	Date
Christian Janoff, Bart Mcglothin, Chris Tobkin, Stephan, Christina Hausman, Josh Huston	Environment Overview, Cisco PCI designs (CS-MARS, CSA, CSM, CiscoWorks (LMS), ACS, WCS)	11/16/06
Christian Janoff, Bart Mcglothin, Chris Tobkin, Stephan, Christina Hausman, Josh Huston	Environment Overview, Cisco PCI designs (CS-MARS, CSA, CSM, CiscoWorks (LMS), ACS, WCS)	11/17/06
Christian Janoff, Bart Mcglothin	Network architecture, firewalls, routers, switches, wireless, IDS/IPS	12/04/06
Christian Janoff, Bart Mcglothin	Audit Logging	12/04/06
Christian Janoff, Bart Mcglothin	Access Control / Authentication	12/04/06
Christian Janoff, Bart Mcglothin	CSA	12/04/06
Christian Janoff, Bart Mcglothin	MARS	12/04/06
Christian Janoff, Bart Mcglothin	CSM	12/04/06
Christian Janoff, Bart Mcglothin	Wireless	12/04/06
Christian Janoff, Bart Mcglothin	CiscoWorks (LMS)	12/06/06
Christian Janoff, Bart Mcglothin, Eric	MARS	12/13/06
Christian Janoff, Bart Mcglothin	Remediation items	12/20/06
Christian Janoff, Bart Mcglothin, Paul Jones	Assessment Results – Messaging	12/21/06
Christian Janoff, Bart Mcglothin, Christina Hausman, Josh Huston	CSA validation	12/22/06
Christian Janoff, Bart Mcglothin	IRoC review, remediation, and clarifications	12/27/06

Rupesh Chakkingal, Karen Chan	Cisco Retail Solution (Phase II overview)	9/13/07
Karen Chan, Sam Rao	CiscoWorks NCM	9/21/07
Karen Chan	Datacenter topology (WAN aggregation, DMZ, Internet Edge)	10/2/07
Karen Chan, Edmond Lam	7206VXR configuration review	10/4/07
Rupesh Chakkingal, Prakash Sinha	ACE XML Gateway	10/9/07
Rupesh Chakkingal, Scot Delancey (NCR)	NCR ACS Server	10/9/07
Rupesh Chakkingal, Ken Moore (Verifone), Marco (Verifone), Dave (Verifone)	Verifone MX/VX Series Pin Pads	10/9/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager	10/10/07
Rupesh Chakkingal, Mohan Atreya (RSA)	RSA File Security Manager	10/10/07
Karen Chan, Don Lanoue, Mark King, Scott Seal	Cisco Configuration Assurance Solution (CAS)	10/11/07
Karen Chan	Cisco Network Compliance Manager (NCM)	10/15/07
Karen Chan	Data Center Network review	10/15/07
Rupesh Chakkingal, Mohan Atreya (RSA)	RSA File Security Manager	10/15/07
Karen Chan	Cisco router secure configuration reviews	10/16/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager	10/16/07
Karen Chan, Pete Davis, Sridharan Srinivasan	Cisco ASA – Secure configuration reviews	10/17/07
Rupesh Chakkingal, Bryan Finch (NCR), Scot Delancey (NCR)	NCR ACS Server (Encryption/Key Management, Retention, password/lockout security, least-privilege access)	10/17/07
Rupesh Chakkingal, Chris Paggen	Cisco ACE XML Gateway (Web application security)	10/17/07
Karen Chan	VSAN Storage (EMC Storage) security – Zoning/LUN Masking	11/19/07
Rupesh Chakkingal, Josh Huston, John Eppich	Cisco Security Agent	11/19/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA File Security Manager	11/19/07

Rupesh Chakkingal, Joe Vittorioso (RSA), Duke Corey (RSA)	RSA enVision	12/6/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Authentication Manager, RSA SecurID	12/6/07
Rupesh Chakkingal, Martin Pueblas	Cisco IDSM review	12/6/07
Rupesh Chakkingal, Joe Vittorioso (RSA)	RSA Key Manager, RSA Access Manager, RSA Authentication Manager	12/7/07
Rupesh Chakkingal, David Paschich	Cisco ACE XML Gateway (web application security)	12/7/07
Karen Chan	VSAN Storage – Security review	12/7/07

Documentation Reviewed

The following documentation was interviewed:

Document	Date / Version
LAB Servers and PC's V12 2006-12-27.doc	12/26/07 / v13
NTPVMapp_FAQ.txt	12/27/06
PCI Lab Application Flows v6 2006-12-27.xls	12/27/06
PCI LAB DOC DIAGRAMS 2006-12.01.vsd	12/01/06
Cisco Retail PCI Lab 11.20.06.doc	11/20/06
Cisco Security Agent v5.1 Test Guide.pdf	2006
CSA for corporate clients.pdf	
CSA deployment best practices.pdf	
Firewall Documentation.doc	11/16/06
PCI DIG v3. 12.19.06.doc	12/19/06

Key Technology

Critical hardware and software in the environment includes:

Component	Brand(s) Used	Version
Firewall	<ul style="list-style-type: none"> ▪ Cisco Integrated Services Router (FWSM Firewall), Cisco ASA 	<ul style="list-style-type: none"> ▪ FWSM v3.1(3) ▪ ASA 7.2.(2)
Network IDS	Cisco Integrated Services Router (integrated IDS/IPS), IDSM2	IOS v12.3(11r)T2, 12.4(1r), IDSM 6.0.(2)E1
Router	Cisco Integrated Services Router (IOS Firewall), Cisco 7206VXR	IOS v12.2(18)SXF10a, v12.3(11r)T2, 12.4(1r), 12.4(11)T3 (VXR)
Wireless AP	Cisco 1131AG, 1242AG	
Wireless Controller	AIR-LAP1131AG-A-K9, AIR-LAP1242AG-A-K9	IOS 12.3(11)JA
POS Software	NCR ACS, NCR RealPOS	ACS v6.01.04.16
POS Devices	NCR, Verifone, Intermec	NCR RealPOS 80c, Verifone MX870, MX850, Vx670 (wireless), and Intermec Mobile POS CN3 (wireless)
Windows Server	Windows Server 2003	SP1, SP2
ECOM Web Server (demo server)	Foundstone Hackme Bank	v2.0
Database	N/A – Not reviewed/Not in scope	
Windows Server Anti-Virus	McAfee VirusScan Enterprise + Anti-spyware Module	8.0.0
Firewall, Router, Switch, IDS/IPS	Cisco Security Manager (CSM), Cisco	CSM v3.0.1, ASDM

Management	ASDM, Cisco IDM	v5.2.(2), IDM v6.0.2
Router, Switch management	CiscoWorks (LMS), CiscoWorks (NCM)	LMS v2.6, NCM v1.2.1
Desktop/Server Firewall (Host-based firewall)	Cisco Security Agent (CSA)	v5.1.0.69, v5.2.0.210
Central Logging / Correlation /Analysis	CS-MARS, RSA enVision	CS-MARS (v4.3.1), enVision (v3.5.1)
Wireless Management	Wireless Control System (WCS)	v4.1
AAA (TACACS+) authentication	Cisco ACS	v4.0(1) Build 27
Web Services (application) firewall	Cisco ACE XML Gateway	V5
Load Balancer	Cisco ACE Load Balancer	V3.0(0)A1(4a)
Two-factor Authentication	RSA SecurID (RSA Authentication Manager)	V6.1(300)
RSA Key Manager Authentication	RSA Access Manager	v6.0
Desktop E-mail Encryption	N/A – not in scope	
File Integrity	Cisco Security Agent (CSA)	v5.1
Cardholder Storage Encryption	<ul style="list-style-type: none"> ▪ NCR ACS (128-bit 3DES) ▪ RSA Key Manager (192-bit 3DES, 128-bit, 192-bit, 256-bit AES) ▪ RSA File Security Manager (192-bit 3DES, 256-bit AES) 	<ul style="list-style-type: none"> ▪ ACS v6.01.04.16 ▪ RSA Key Manager v2.1.1 ▪ RSA File Security Manager v2.1.0.9

Quarterly Scan Results

N/A - Quarterly scanning (internal and external) is the responsibility of the merchant / service provider, and was not part of the assessment.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
1.1 Establish firewall configuration standards that include the following:	1.1 Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	1.1.1 Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration	N/A – Firewall/Router configuration standards (documentation).		Responsibility of merchant / service provider.
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	1.1.2.a Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks	Cisco provided a current network diagram, which documents all connections to the cardholder data, applicable to the reference architecture environment, including wireless networks.		
	1.1.2.b. Verify that the diagram is kept current	Current diagrams were provided for each PCI Solution for Retail environment (e.g. Small, medium, and large POS environments, and		Note: Since each network environment will be unique to the merchant or service

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		data center environment).		provider, updating network diagrams remains the responsibility of each merchant / service provider.
<p>1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</p>	<p>1.1.3 Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the Intranet. Verify that the current network diagram is consistent with the firewall configuration standards.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>
<p>1.1.4 Description of groups, roles, and responsibilities for logical management of network components</p>	<p>1.1.4 Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components.</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p> <p>Note: Verizon Business confirmed role-based groups were created within Cisco ACS for logical management of network devices (e.g. Administrator, System Monitoring, and Config Manager groups).</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>
<p>1.1.5 Documented list of services and ports necessary for business</p>	<p>1.1.5 Verify that firewall configuration standards include a documented list of services/ports necessary for business</p>	<p>N/A – Firewall/Router configuration standards (documentation)</p> <p>Note: Verizon Business reviewed access-lists, in addition to a documented list of required services/protocols for the PCI Solution for Retail environment, and confirmed traffic is limited to that which is required for the environment.</p>		<p>Responsibility of merchant / service provider to document in configuration standards.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	1.1.6 Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider to document in configuration standards.
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	1.1.7.a Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol, and security features implemented	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider to document in configuration standards.
	1.1.7.b Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider to document in configuration standards.
1.1.8 Quarterly review of firewall and router rule sets	1.1.8.a Verify that firewall configuration standards require quarterly review of firewall and router rule sets	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider.
	1.1.8.b Verify that the rule sets are reviewed each quarter	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider. Note: Requirement to review rule sets is to identify and remove stale, unnecessary rules, as well as audit rule set for soundness against current network design.
1.1.9 Configuration standards for routers	1.1.9 Verify that firewall configuration standards exist for both firewalls and routers	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider to document in configuration

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
				<p>standards.</p> <p>Note: Configuration templates exist within CiscoWorks (LMS, NCM), which can aid merchants / service providers to enforce configuration standards. CiscoWorks NCM can also be configured to regularly audit network device configurations to ensure compliance with industry-accepted standards.</p>
<p>1.2 Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.</p>	<p>1.2 Select a sample of firewalls/routers 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. The sample should include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment</p>	<p>Verizon Business confirmed that inbound traffic to and outbound traffic from the PCI Solution for Retail environment is limited to protocols necessary for the environment. ASA firewalls, FWSM firewalls, Integrated Services Routers (ISRs), and router access-lists are configured with “default-deny” rules and explicitly allow traffic to the service/port level.</p>		<p>Configurations for perimeter firewalls/routers outside the PCI Solution for Retail environment are the responsibility of merchant / service provider.</p>
<p>1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:</p>	<p>1.3 Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:</p>			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
1.3.1 Restricting inbound Internet traffic to internet protocol (IP) addresses within the DMZ (ingress filters)	1.3.1 Verify that inbound Internet traffic is limited to IP addresses within the DMZ	Verizon Business reviewed access-lists for inbound Internet traffic and confirmed traffic is limited to IP addresses within the DMZ and restricted to only those services/protocols necessary.		Perimeter firewall/router configurations and rule sets are the responsibility of the merchant / service provider.
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ	1.3.2 Verify that internal addresses cannot pass from the Internet into the DMZ	Verizon Business reviewed access-lists on the Internet edge router and confirmed that Internet sourced RFC-1918 addresses were explicitly denied.		
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	1.3.3 Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run NMAP on all TCP ports with "syn reset" or "syn ack" bits set – a response means packets are allowed through even if they are not part of a previously established session)]	Verizon Business confirmed the PCI Solution for Retail environment configurations for the Cisco ASA firewalls, FWSMs, and ISRs were configured to perform stateful packet inspections.		
1.3.4 Placing the database in an internal network zone, segregated from the DMZ	1.3.4 Verify that the database is on an internal network zone, segregated from the DMZ	All databases within the PCI Solution for Retail environment are on an internal segment, segregated from the DMZ.		
1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	1.3.5 Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder environment, and that the restrictions are documented	Verizon Business confirmed that inbound and outbound traffic is limited to that which is necessary for the cardholder environment.		Note: Documentation of allowed services/protocols is the responsibility of the merchant / service provider.
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration	1.3.6 Verify that router configuration files are secure and synchronized [for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations]	Verizon Business confirmed Cisco ISR and Cisco router device configurations are stored locally and within CiscoWorks (LMS, NCM), which has been implemented with least privilege access. CiscoWorks (LMS, NCM) can be configured to log and alert on configuration		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
files (when machines are re-booted) should have the same secure configuration		inconsistencies between active (running) and startup configurations.		
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	1.3.7 Verify that all other inbound and outbound traffic not covered in 1.2 and 1.3 above is specifically denied	Verizon Business confirmed that all inbound and outbound traffic not necessary for the PCI Solution for Retail environment is specifically denied.		
1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	1.3.8 Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data	Verizon Business confirmed the PCI Solution for Retail environment architecture was designed and segmented to require all wireless traffic destined for any wired host (e.g. POS system, WCS Manager, etc.) to pass through ISR firewall access-lists before being permitted.		
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	1.3.9 Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee	N/A – Security Policy (Remote Access – Desktop firewalls) Note: Remote access to the PCI Solution for Retail environment was assessed for two-factor authentication (requirement 8.3) only.		Installation of personal firewall software for any mobile and employee-owned computers with direct Internet connectivity, and which are used to access the merchant / service provider network, is the responsibility of the merchant / service provider.
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	1.4 To determine that direct access between external public networks and system components storing cardholder data are prohibited, perform the following, <i>specifically</i> for the firewall/router configuration implemented between the DMZ and the internal network:			
1.4.1 Implement a DMZ to	1.4.1 Examine firewall/router	Verizon Business reviewed network		Merchant / Service

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic	configurations and verify there is no direct route inbound or outbound for Internet traffic	diagrams, configurations from network infrastructure system components, including wireless APs, to confirm there are no direct routes inbound or outbound for Internet traffic to/from the retail reference architecture.		Provider would be responsible for ensuring POS devices and other servers in the retail (POS) environment are not configured to communicate directly with the Internet.
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	1.4.2 Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ	Verizon Business reviewed outbound access-lists from the PCI Solution for Retail environment and confirmed that all outbound traffic is destined for "data center" systems. There is no outbound Internet access from the PCI Solution for Retail environment.		
1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	1.5 For the sample of firewall/router components above, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading)	Verizon Business confirmed RFC 1918 addresses were used within the PCI Solution for Retail environment		

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
2.1 Always change vendor-supplied defaults before installing a system on the	2.1 Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with	Verizon Business observed administrators during the login process, while attempting to logon		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	with default accounts and passwords. Verizon Business confirmed all default passwords, including passwords for interactive administrator accounts and SNMP community strings have been changed. Verizon Business confirmed all default administrator accounts have been removed, where possible. Some default administrator accounts cannot be removed from the system, due to application dependencies; however, unique administrator accounts have been created, in order to eliminate the need to use all default administrator accounts.		
<p>2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.</p>	<p>2.1.1 Verify the following regarding vendor default settings for wireless environments:</p> <ul style="list-style-type: none"> • WEP keys were changed from default at installation, and are changed anytime any one with knowledge of the keys leaves the company or changes positions • Default SSID was changed • Broadcast of the SSID was disabled • Default SNMP community strings on access points were changed • Default passwords on access points were changed • WPA or WPA2 technology is enabled if the wireless system is WPA-capable • Other security-related wireless vendor defaults, if applicable 	<p>Verizon Business reviewed wireless settings within the PCI Solution for Retail environment and verified the following:</p> <ul style="list-style-type: none"> - Although default configurations support WEP, WEP keys had been disabled and were not used within the wireless environment. WPA/TKIP (w/PEAP authentication) is used for all wireless security. - No Default SSID exists. This must be entered at initial installation, and is recommended by Cisco to be unique. - SSID broadcast was disabled. - Default SNMP community strings have been changed and (SNMPv3 is being used). - No default passwords exist within the wireless environment. These are entered at initial login. Only unique, non-default accounts exist for interactive administration within the wireless environment. - WPA technology is enabled 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		(WPA/TKIP w/PEAP authentication). - Wireless management and web mode is disabled.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).</p>	<p>2.2.a Examine the organization's system configuration standards for network components, critical servers, and wireless access points, and verify the system configuration standards are consistent with industry-accepted hardening standards as defined, for example, by SANS, NIST, and CIS</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Note: Verizon Business reviewed configurations across all ASA/FWASM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards. CiscoWorks NCM can be used to further support best practice standards across network devices. Network device templates can be created to standardize secure configurations across network devices. Additionally, NCM can be used to periodically (e.g. once a day) audit network configurations to ensure secure configurations are being used and have not been altered contrary to best-practice standards.</p> <p>Note: Host Operating Systems were not included in the secure configuration review, as the OS chosen for management applications could vary with each merchant/service provider. Secure configuration for chosen OS platforms would be performed by the merchant/service provider. Verizon Business reviewed administrative accounts (default username/passwords, password/lockout settings, audit log settings, and secure channels for administration of applications and systems.</p>		<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<p>2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4)</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Note: Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards.</p>		<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>
	<p>2.2.c Verify that system configuration standards are applied when new systems are configured</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Note: Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were configured according to best practice standards. Verizon Business also confirmed all management consoles were configured to support https access, and that http access had been disabled.</p>		<p>Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.</p>
<p>2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)</p>	<p>2.2.1 For a sample of system components, critical servers, and wireless access points, verify that only one primary function is implemented per server</p>	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Within the PCI Solution for Retail environment Cisco has used Virtual (VMware) servers to logically segment system functionality within a single hardware device (e.g. CSA Manager and CSM (Cisco Security Manager) running under separate VMware servers on a single system.</p>		<p>Note: Logical system partitioning (e.g. lpars (IBM mainframe), VMware servers) is an acceptable means to separate server functions within a single server platform.</p>
<p>2.2.2 Disable all</p>	<p>2.2.2 For a sample of system</p>	<p>Verizon Business reviewed</p>		<p>Host OS hardening for</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	components, critical servers, and wireless access points, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service (for example, FTP is not used, or is encrypted via SSH or other technology)	<p>configurations for ASA/FWSM firewalls, ISR routers, switches, and wireless devices and found insecure services and protocols to be disabled.</p> <p>Note: Although Cisco followed a configuration standard to harden the OS for management consoles and POS servers (e.g. WCS, ACS, CSM, CSA, CiscoWorks (LMS, NCM), ACE XML Gateway, RSA File Security Manager, RSA Key Manager, RSA Access Manager, RSA Authentication Manager, and RSA enVision), Verizon Business did not review those configurations beyond secure administrative access (e.g. https, SSH), audit logging, and password/lockout settings. OS hardening is the responsibility of the merchant / service provider, and would vary significantly, depending on OS platform and POS applications deployed.</p>		POS applications, Management servers (e.g. Cisco CSM, RSA Authentication Manager, etc) is the responsibility of the merchant/service provider.
2.2.3 Configure system security parameters to prevent misuse	2.2.3.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for their operating systems, database servers, Web servers, and wireless systems	Verizon Business interviewed administrators, architects, and SMEs from business units to determine they have knowledge of common security parameters for the ASA firewalls, FWSMs, ISRs, routers, switches, wireless components, and management platforms within the PCI Solution for Retail environment.		Interviews to be conducted within respective administrator/security groups for each merchant / service provider.
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards	<p>N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards).</p> <p>Note: Verizon Business reviewed configurations across ASA/FWSM firewalls, ISR routers, switches, and</p>		Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>wireless devices and confirmed they were based on best practice standards. Verizon Business also confirmed all management consoles were configured to support secure access (e.g. SSH, https, High-Encryption RDP), and that http, Telnet, and other insecure protocols commonly used for administrative access had been disabled.</p>		
	<p>2.2.3.c For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately</p>	<p>Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were based on best practice standards, and that common security parameters were set appropriately. Verizon Business also confirmed all management consoles were configured to support secure access (e.g. SSH, https, High-Encryption RDP), and that http, Telnet, and other insecure protocols commonly used for administrative access had been disabled. Additionally, role-based administration was configured for administration of network devices (e.g. ASA/FWSM firewalls, ISRs, routers, switches, wireless controllers) and for management of WCS, CSA, CiscoWorks (LMS, NCM), CSM, CS-MARS, and ACS, ACE XML Gateway, NCR ACS server, RSA File Security Manager, RSA Key Manager, RSA enVision, RSA Authentication Manager, and RSA Access Manager.</p>		<p>Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.</p>
<p>2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file</p>	<p>2.2.4 For a sample of system components, critical servers, and wireless access points, verify that all unnecessary functionality (for</p>	<p>Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were based on best practice</p>		<p>Server hardening, including appropriate security settings for all system components, is the responsibility of the</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
systems, and unnecessary web servers.	example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented, support secure configuration, and that only documented functionality is present on the sampled machines	standards, and that all unnecessary functionality was disabled.		merchant / service provider.
<p>2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.</p>	<p>2.3 For a sample of system components, critical servers, and wireless access points, verify that non-console administrative access is encrypted by:</p> <ul style="list-style-type: none"> • Observing an administrator log on to each system to verify that SSH (or other encryption method) is invoked before the administrator's password is requested • Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally • Verifying that administrator access to the wireless management interface is encrypted with SSL/TLS. Alternatively, verify that administrators cannot connect remotely to the wireless management interface (all management of wireless environments is only from the console) 	<p>Verizon Business reviewed non-console administrative access for ASA firewalls, FWSM firewalls, ISR routers, switches, wireless devices, and the following management consoles: CSA Manager, ACS (TACACS+ server for all network device authentication), CSM, CiscoWorks (LMS,NCM), WCS (wireless console), and ACE XML Gateway, CS-MARS, NCR ACS Server, RSA File Security Manager, RSA Key Manager, RSA enVision, RSA Authentication Manager, and RSA Access Manager . Verizon Business confirmed the following methods were used:</p> <ul style="list-style-type: none"> - ssh (CLI access for ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2 modules, ACE XML Gateway, CS-MARS, and wireless controllers) - RDP (High Encryption) enabled. This forces RDP clients to used 128-bit encryption. RDP access is used to for OS access for the following: NCR ACS server, all Windows-based Cisco management consoles (e.g. CiscoWorks (LMS, NCM), WCS, CSA, ACS, etc), RSA File Security Manager, RSA Key Manager, RSA Authentication Manager, RSA Access Manager, RSA enVision. - 128-bit SSL (https) or SSL encrypted thick-client access for 		<p>Note: Verification of telnet presence within the management consoles (Windows Server 2003) was not performed. This is the responsibility of the merchant / service provider, as part of secure configuration standard processes.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		management console access, including wireless console access (WCS). - Http access has been disabled on all management consoles, ASA/FWSM firewalls, ISRs, routers, switches, and wireless controllers.		
2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."	2.4 Perform testing procedures A.1.1 through A.1.4 detailed in Appendix A, "PCI DSS Applicability for Hosting Providers (with Testing Procedures)" for PCI audits of Shared Hosting Providers , to verify that Shared Hosting Providers protect their entities' (merchants and service providers) hosted environment and data.	N/A – Hosting provider (testing procedures) requirement		This requirement is specific to hosting providers.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.</p>	<p>3.1 Obtain and examine the company policies and procedures for data retention and disposal, and perform the following</p> <ul style="list-style-type: none"> • Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) • Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data • Verify that policies and procedures include coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers • Verify that policies and procedures 	<p>N/A – Data retention / Data disposal policy and procedures.</p>		<p>Data retention / Data disposal policies and procedures are the responsibility of the merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<p>include a programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for an audit, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements</p>			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:</p>	<p>3.2 If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable For each item of sensitive authentication data below, perform the following steps:</p>	<p>VzB observed test transactions and “at rest” data within the NCR POS terminal and NCR ACS application. Verizon Business also reviewed NCR’s PABP assessment results and confirmed that NCR ACS software used within Cisco’s PCI Solution for Retail environment is PABP certified. As a result of the review, Verizon Business has confirmed that sensitive authentication data is not stored subsequent to authorization. Like other POS applications, the NCR ACS software does retain full track data in 128-bit 3DES encrypted format, only in an offline scenario (link to authorizer is down), and is purged at the point the connection is available and the transaction is sent for authorization.</p>		<p>It is the responsibility of the merchant to ensure POS systems used do not store sensitive authentication data (e.g. full track data, CVV2, PIN/PIN block) post authorization (even if encrypted). A large step to ensure POS systems meet PCI requirements is to work with POS vendors that have certified their POS application/s according to PABP standards.</p>
<p>3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data <i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder’s name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the</i></p>	<p>3.2.1 For a sample of system components, critical servers, and wireless access points, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents 	<p>See 3.2 above. Verizon Business confirmed that full track data is not written to disk, other than temporarily in an offline scenario. During this temporary period the track data is encrypted using 128-bit 3DES encryption, and is immediately purged at the point an authorization response is obtained. Verizon Business reviewed the following:</p> <ul style="list-style-type: none"> • Database transaction files • User access log • EFT Journal Report • EFT Offline Report • EFY Rejection Report • Electronic Journal Report • TRMOFF (FOH offline transaction file) • EFTOFF (back office offline 		<p>See 3.2 above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>card verification code or value or PIN verification value data elements.</p> <p>Note: See "Glossary" for additional information.</p>		transaction file)		
<p>3.2.2 Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions</p> <p>Note: See "Glossary" for additional information.</p>	<p>3.2.2 For a sample of system components, critical servers, and wireless access points, examine the following and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents 	<p>See 3.2 above. Verizon Business observed that CVV2/CVC2 data was not received at POS swipe. Verizon Business reviewed the following to confirm CVV/CVC2 data is not present:</p> <ul style="list-style-type: none"> • Database transaction files • User access log • EFT Journal Report • EFT Offline Report • EFY Rejection Report • Electronic Journal Report • TRMOFF (FOH offline transaction file) • EFTOFF (back office offline transaction file) 		<p>See 3.2 above</p>
<p>3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.</p>	<p>3.2.3 For a sample of system components, critical servers, and wireless access points, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance:</p> <ul style="list-style-type: none"> • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents 	<p>See 3.2 above. Verizon Business observed that PIN/PIN block data was not required at POS swipe. Verizon Business reviewed NCR's PABP assessment results and the following to confirm CVV/CVC2 data is not present:</p> <ul style="list-style-type: none"> • Database transaction files • User access log • EFT Journal Report • EFT Offline Report • EFY Rejection Report • Electronic Journal Report • TRMOFF (FOH offline transaction file) • EFTOFF (back office offline 		<p>See 3.2 above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). <i>Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).</i></p>	<p>3.3 Obtain and examine written policies and examine online displays of credit card data to verify that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers</p>	<p>transaction file) Verizon Business reviewed NCR's ACS application and confirmed that only masked data is accessible through the application, even for administrators.</p>		<p>Data control / Data classification policies and procedures, including masking PAN data, except for those with a specific need to see full PAN data, is the responsibility of the merchant.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p> <ul style="list-style-type: none"> • Strong one-way hash functions (hashed indexes) • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures <p>The MINIMUM account information that must be rendered unreadable is the PAN.</p> <p><i>If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls."</i></p>	<p>3.4.a Obtain and examine documentation about the system used to protect stored data, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that data is rendered unreadable using one of the following methods:</p> <ul style="list-style-type: none"> • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures 	<p>Verizon Business reviewed vendor documentation regarding NCR's ACS POS server and observed application files (see 3.2.x comments for application files reviewed) to determine that the following methods are used to render cardholder data unreadable within the POS environment:</p> <ul style="list-style-type: none"> - 128-bit 3DES encryption - Truncation <p>Additionally, Verizon Business reviewed RSA File Security Manager and RSA Key Manager applications, related to protecting sensitive data (including cardholder data) within Cisco's PCI Solution for Retail environment. Verizon Business confirmed the following methods can be used to render cardholder data unreadable:</p> <ul style="list-style-type: none"> - RSA File Security Manager – 192-bit 3DES or 256-bit AES encryption. - RSA Key Manager – 192-bit 3DES or 128-bit, 192-bit, or 256-bit AES encryption. 		<p>Ensuring PAN data, at a minimum, is unreadable anywhere it is stored, is the responsibility of the merchant / service provider. At least one of the following methods must be used:</p> <ul style="list-style-type: none"> • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures
	<p>3.4.b Examine several tables from a sample of database servers to verify the data is rendered unreadable (that is, not stored in plain text)</p>	<p>Verizon Business reviewed NCR's ACS POS server and POS register and confirmed that cardholder data was truncated or encrypted in all locations. Verizon Business also reviewed encryption capabilities for RSA File Security Manager and RSA Key Manager products. Verizon Business confirmed that all test files used during the review were successfully rendered unreadable using strong encryption.</p>		<p>See 3.4 above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that cardholder data is rendered unreadable	N/A – Tape backups were not included in the scope of the review.		See 3.4 above
	3.4.d Examine a sample of audit logs to confirm that cardholder data is sanitized or removed from the logs	Verizon Business reviewed NCR's ACS POS server and POS register and confirmed that cardholder data was truncated or encrypted in all locations. Verizon Business also reviewed encryption capabilities for RSA File Security Manager and RSA Key Manager products. Verizon Business confirmed that all test files used during the review were successfully rendered unreadable using strong encryption.		See 3.4 above
	3.4.e Verify that cardholder data received from wireless networks is rendered unreadable wherever stored	N/A – Cardholder transactions were not tested over wireless networks.		See 3.4 above
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.	3.4.1.a If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local or Active Directory accounts)	N/A – Disk encryption was not used in the environment.		See 3.4 above
	3.4.1.b Verify that decryption keys are not stored on the local system (for example, store keys on floppy disk, CD-ROM, etc. that can be secured and retrieved only when needed)	N/A – Disk encryption was not used in the environment.		Encryption / Key Management policies and procedures, including technical controls is the responsibility of the merchant / service provider.
	3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media)	N/A – Disk encryption was not used in the environment.		See 3.4 above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:</p>	<p>3.5 Verify processes to protect encryption keys used for encryption of cardholder data against disclosure and misuse by performing the following:</p>			
<p>3.5.1 Restrict access to keys to the fewest number of custodians necessary</p>	<p>3.5.1 Examine user access lists to verify that access to cryptographic keys is restricted to very few custodians</p>	<p>Verizon Business confirmed that restricted access to encryption keys is as follows:</p> <ul style="list-style-type: none"> - NCR ACS: Encryption keys are generated using the “Interactive Key Maintenance” tool. Only administrators have access to this tool. The encryption key is stored in an encrypted format within a binary file and is not disclosed to the key administrator at key generation time or at any other time. - RSA File Security Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys. - RSA Key Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported to a key administrator. RSA Key Manager security policies require public key authentication to access key material for encryption/decryption purposes. 		<p>Protection of encryption keys is the responsibility of the merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.5.2 Store keys securely in the fewest possible locations and forms</p>	<p>3.5.2 Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys</p>	<p>Verizon Business reviewed protection/storage for encryption keys and confirmed the following:</p> <ul style="list-style-type: none"> - NCR ACS: Data encryption keys are stored in an encrypted format within the ENCKEY binary file. The key-encrypting key is statically compiled into the application. - RSA File Security Manager: The data encryption key is protected using a private RSA 1024-bit role key. The role key is encrypted using a unique access key. The access key is not stored on the system in its entirety, but is derived by seeding the PRNG with a SID (unique) and additional salt, resulting in unique key material for each user and process configured within FSM. - RSA Key Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. 		<p>See 3.5.1 above</p>
<p>3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:</p>	<p>3.6.a Verify the existence of key management procedures for keys used for encryption of cardholder data</p>	<p>N/A – Key Management policy and procedures</p>		<p>Key Management policies and procedures is the responsibility of the merchant / service provider.</p>
	<p>3.6.b For Service Providers only: If the Service Provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and service provider)</p>	<p>N/A – Key Management policy and procedures</p>		<p>See 3.6.a above</p>
	<p>3.6.c Examine the key management procedures and perform the following:</p>			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
3.6.1 Generation of strong keys	3.6.1 Verify that key management procedures require the generation of strong keys	Verizon Business confirmed that generation of strong keys is included for the following: - NCR ACS: 128-bit 3DES keys - RSA File Security Manager: 192-bit 3DES or 256-bit AES keys - RSA Key Manager: 192-bit 3DES or 128-bit/192-bit/256-bit AES keys		See 3.6.a above
3.6.2 Secure key distribution	3.6.2 Verify that key management procedures require secure key distribution	Verizon Business confirmed that secure distribution of keys is included for the following: - NCR ACS: Encryption keys are generated locally, using the Interactive Key Maintenance tool and imported into the ENCKEY binary file. - RSA File Security Manager: Encryption keys are stored centrally on the RSA File Security Manager server and sent in encrypted format to the client system requiring encryption/decryption functions. - RSA Key Manager: All key transfers are done over SSLv3/TLSv1 connections between Key Manager server and Key Manager Clients.		See 3.6.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.6.3 Secure key storage</p>	<p>3.6.3 Verify that key management procedures require secure key storage</p>	<p>Verizon Business confirmed that secure key storage is included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: Encryption keys are encrypted using a 128-bit 3DES key-encryption key. - RSA File Security Manager: The data encryption key is protected using a private RSA 1024-bit role key. The role key is encrypted using a unique access key (256-bit AES encryption). The access key is not persistently stored on the client system in its entirety, but is derived by seeding the PRNG with a SID (unique) and additional salt, resulting in unique key material for each user and process configured within FSM. - RSA Key Manager: Key encryption key is stored in memory and data encryption keys are stored in encrypted format within Oracle or MS SQL database. 		<p>See 3.6.a above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.6.4 Periodic key changes</p> <ul style="list-style-type: none"> As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically At least annually 	<p>3.6.4 Verify that key management procedures require periodic key changes. Verify that key change procedures are carried out at least annually</p>	<p>Verizon Business confirmed that key rotation capabilities are included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: New keys can be generated using the Interactive Key Maintenance tool. Data encrypted with a particular key is stored with a key index, so that multiple keys can be used for data encryption. - RSA File Security Manager: Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters decrypt “at rest” data and re-encrypt with new key. - RSA Key Manager: RSA Key Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Encryption keys can be assigned different key states, depending on known state of key. Examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised). 		<p>See 3.6.a above</p> <p>Note: NCR ACS application. There was no reasonable way to rotate encryption keys, without manually decrypting all data and re-encrypting with a new key. NCR ACS application allows multiple keys (up to 255) to be used to limit the amount of data encrypted with a single key.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.6.5 Destruction of old keys.</p>	<p>3.6.5 Verify that key management procedures require the destruction of old keys</p>	<p>Verizon Business confirmed that destruction of keys is included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: New keys can be generated using the Interactive Key Maintenance tool. Old keys can be removed from use or overwritten through the Interactive Key Maintenance tool. - RSA File Security Manager: Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters decrypt “at rest” data and re-encrypt with new key. - RSA Key Manager: RSA Key Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined, or delete, when necessary. States are assigned to encryption keys to limit transition use of key. Examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised). 		<p>See 3.6.a above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)</p>	<p>3.6.6 Verify that key management procedures require split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)</p>	<p>Verizon Business confirmed that split knowledge/dual control of keys is included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: Encryption keys are generated using the “Interactive Key Maintenance” tool. Only administrators have access to this tool. The encryption key is stored in an encrypted format within a binary file and is not disclosed to the key administrator at key generation time. - RSA File Security Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys. Additional roles exist within RSA File Security Manager to further segregate key management capabilities between “Security Admin” (responsible for management of security officers and has no visibility into encryption keys or security policies) and “Security Officers” (creates security policies, assigns encryption keys, but has no visibility into data being protected). - RSA Key Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. 		<p>See 3.6.a above</p>
<p>3.6.7 Prevention of unauthorized substitution of keys</p>	<p>3.6.7 Verify that key management procedures require the prevention of unauthorized substitution of keys</p>	<p>Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: Encryption keys are generated using the “Interactive Key Maintenance” tool. Only 		<p>See 3.6.a above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>administrators have access to this tool. CSA has also been installed on the ACS server and further restricts access, monitors access, and logs access to tools necessary for key replacement.</p> <p>- RSA File Security Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. RSA File Security Manager security policies provide access keys to use encryption keys, but not view or export encryption keys. Additional roles exist within RSA File Security Manager to further segregate key management capabilities between "Security Admin" (responsible for management of security officers and has no visibility into encryption keys or security policies) and "Security Officers" (creates security policies, assigns encryption keys, but has no visibility into data being protected). Security Officers can only conduct key administration functions, they cannot access decrypted data, assuming separation of duties has been implemented on the client OS (e.g. key administrators are not users on the client system that uses encryption functions).</p> <p>- RSA Key Manager: Data encryption keys are never disclosed to the key administrators and cannot be exported at any time in clear-text format. Key administration functions can only be access through the Key Manager server, via access controls (authentication) through the RSA Access Manager server.</p>		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>Additionally, Verizon Business confirmed that firewall segmentation and granular firewall access lists exist to further restrict access to POS systems and encryption key management servers.</p>		
<p>3.6.8 Replacement of known or suspected compromised keys</p>	<p>3.6.8 Verify that key management procedures require the replacement of known or suspected compromised keys</p>	<p>Verizon Business confirmed that replacement of known or suspected compromised keys is included for the following:</p> <ul style="list-style-type: none"> - NCR ACS: Compromised keys can be removed or destroyed using the Interactive Key Maintenance tool. - RSA File Security Manager: Client adapters can rotate encryption keys as defined by RSA File Security Manager policies, or manually, in the event of a key compromise. Client adapters transparently decrypt “at rest” data and re-encrypt with new key. - RSA Key Manager: RSA Key Manager assigns lifetimes for key use, and policies can be created to rotate (generate and use new key) as frequently as defined. Different states can be assigned to encryption keys in the event of a suspected or known key compromise. Key state examples include: Active, deactivated, destroyed, compromised, or destroyed-compromised). 		<p>See 3.6.a above</p>
<p>3.6.9 Revocation of old or invalid keys</p>	<p>3.6.9 Verify that key management procedures require the revocation of old or invalid keys (mainly for RSA keys)</p>	<p>N/A – Public keys are not used for data encryption, within the PCI Solution for Retail environment.</p>		<p>See 3.6.a above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	3.6.10 Verify that key management procedures require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities	N/A – Key custodian lists are the responsibility of the merchant/service provider.		See 3.6.a above

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i></p>	<p>4.1.a Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks</p> <ul style="list-style-type: none"> • Verify that strong encryption is used during data transmission • For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL • Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit • Verify that only trusted SSL/TLS keys/certificates are accepted • Verify that the proper encryption strength is implemented for the encryption methodology in use (Check vendor recommendations/best practices) 	<p>4.1.a Verizon Business reviewed the following configurations to confirm that secure transmission of cardholder data would be accomplished:</p> <ul style="list-style-type: none"> - The wireless network within the large, medium, and small store environment (WPA (128-bit RC4 encryption)) - 128-bit SSL (Secure FTP (SFTP) of cardholder data from store environment to PCI file server within data center). Cisco's PCI solution would allow for both transmission of data over private circuit to the WAN edge of the data center, or over IPsec VPN back to data center. - Verizon Business confirmed that the proper encryption strength (128-bit RC4) has been implemented for all wireless traffic within the PCI Solution for Retail environment. Verizon business also confirmed the SFTP sever was configured with strong encryption. <p>Note: Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic.</p>		<p>Note: Verizon Business observed test cardholder transactions within the PCI Solution for Retail environment, however, test transactions did not transmit data beyond the POS environment. Test transactions were at the wired POS and did not include wireless POS transactions; however, Verizon Business did review wireless and SFTP settings and confirmed they were configured appropriately.</p> <p>If cardholder data does not traverse the wireless network, wireless networks would be out of scope for requirement 4.1.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.</p> <p>If WEP is used, do the following:</p> <ul style="list-style-type: none"> • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address 	<p>4.1.1.a For wireless networks transmitting cardholder data or connected to cardholder environments, verify that appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS</p>	<p>Verizon Business reviewed wireless settings within the PCI Solution for Retail environment to confirm WPA (128-bit RC4) encryption has been implemented for all wireless traffic.</p>		
	<p>4.1.1.b If WEP is used, verify</p> <ul style="list-style-type: none"> • it is used with a minimum 104-bit encryption key and 24 bit-initialization value • it is used only in conjunction with Wi-Fi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS • shared WEP keys are rotated at least quarterly (or automatically if the technology is capable) • shared WEP keys are rotated whenever there are changes in personnel with access to keys • access is restricted based on MAC address 	<p>Verizon Business reviewed wireless implementations within the PCI Solution for Retail environment and confirmed WEP (supported by default) had been disabled. Only WPA technology is used within the PCI Solution for Retail environment wireless networks.</p>		
<p>4.2 Never send unencrypted PANs by e-mail.</p>	<p>4.2.a Verify that an email encryption solution is used whenever cardholder data is sent via email</p>	<p>N/A – Data Control / Encryption policy and procedures</p>		<p>Responsibility of merchant / service provider.</p>
	<p>4.2.b Verify the existence of a policy stating that unencrypted PAN is not to be sent via email</p>	<p>N/A – Data Control / Encryption policy and procedures</p>		<p>Responsibility of merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	4.2.c Interview 3-5 employees to verify that email encryption software is required for emails containing PANs	N/A – Data Control / Encryption procedures		Responsibility of merchant / service provider.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
----------------------	--------------------	----------	--------------	------------------------

<p>5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)</p> <p><i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i></p>	<p>5.1 For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed</p>	<p>Verizon Business confirmed A/V software was installed on Windows systems within the PCI Solution for Retail environment; however, the assessment focus for PCI A/V requirements was placed on Cisco Security Agent software, and its ability to meet the intent of A/V requirements. Cisco Security Agent software is installed on the following Windows system components within the environment:</p> <ul style="list-style-type: none"> • Cisco ACS console • WCS console • CiscoWorks (LMS, NCM) consoles • CSA console • CSM console • RSA Authentication Manager • RSA Access Manager • RSA File Security Manager • RSA Key Manager • NCR ACS Server <p>Although Verizon Business recommends installing Anti-Virus software on the above system components, CSA software could be used, in conjunction with existing firewall segmentation and restricted Internet access, in order to mitigate the majority of common anti-virus risks (see comments).</p> <p>Important: Because POS environments vary with each vendor, a full assessment of the POS environment, Internet/email connectivity to the POS environment, corporate connectivity to the POS environment, CSA configuration, and all compensating controls would need to be made for each merchant, in order to make an “In Place/Not in Place” assessment (If CSA software is used as a compensating control for Anti-Virus software).</p>		<p>Note: CSA can be configured to protect against the following virus and malware threats:</p> <ul style="list-style-type: none"> • Virus propagation prevention through intrusion detection/prevention and port blocking • Unauthorized/malicious application execution • Application hijacking • Buffer overflows • Instant Messaging (IM can be configured through CSA policy to prohibit downloading files) <p>Important: Any attempt to use CSA as a compensating control for A/V would be subject to examination of the environment, the configuration of CSA and its ability to mitigate risks from virus threats, and the opinion of the individual assessor.</p>
--	---	---	--	--

<p>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.</p>	<p>5.1.1 For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware</p>	<p>See 5.1 above</p>		<p>See 5.1 above</p>
<p>5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>5.2 Verify that anti-virus software is current, actively running, and capable of generating logs</p> <ul style="list-style-type: none"> • Obtain and examine the policy and verify that it contains requirements for updating anti-virus software and definitions • Verify that the master installation of the software is enabled for automatic updates and periodic scans, and that a sample of system components, critical servers, and wireless access points servers have these features enabled • Verify that log generation is enabled and that logs are retained in accordance with company retention policy 	<p>Verizon Business observed A/V software installed on Windows components within the PCI Solution for Retail environment. Verizon Business also reviewed vendor documentation and observed a demo of CSA's capabilities to provide layered security through multiple security controls. The PCI Solution for Retail environment implementation addresses the following AV requirements (2nd and 3rd bullet items):</p> <ul style="list-style-type: none"> - N/A – A/V policy is the responsibility of the merchant / service provider. - A central (master) console for CSA exists in the PCI Solution for Retail environment, which centrally manages all CSA client policies. - Log generation is enabled and alerts/logs are centrally stored within CSA and MARS. Retention period would be determined by merchant / service provider; however, as such alerts could be vital for audit trail construction, Verizon Business recommends retaining CSA alerts for at least one year, commensurate with PCI audit trail requirements. <p>Note: Verizon Business recommends A/V software be installed on all system components commonly affected by viruses, as was found in Cisco's PCI Solution for Retail environment.</p>		<p>Note: (First bullet item for 5.2) - AV policy and procedure documentation is the responsibility of the merchant / service provider.</p> <p>Important: Any attempt to use CSA as a compensating control for A/V would be subject to examination of the environment, the configuration of CSA and its ability to mitigate risks from virus threats, and the opinion of the individual assessor.</p>

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	6.1.a For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed	Verizon Business reviewed configurations for the PCI Solution for Retail environment components, including management consoles for components within the PCI Solution for Retail environment and confirmed they are running current software releases and contain current vendor patches.		
	6.1.b Examine policies related to security patch installation to verify they require installation of all relevant new security patches within 30 days	N/A – Patch management policy and procedures		Patch management policies and procedures is the responsibility of the merchant / service provider.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	6.2.a Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities	N/A – Patch / Risk management policy and procedures		Patch / Risk management procedures are the responsibility of the merchant / service provider.
	6.2.b Verify that processes to identify new security vulnerabilities include use of outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2 as new vulnerability issues are found	Verizon Business reviewed vendor documentation for CiscoWorks (LMS) and confirmed its ability to generate upgrade reports for active devices under CiscoWorks configuration management.		Overall Patch / Risk management procedures are the responsibility of the merchant / service provider. Verizon Business recommends using multiple outside sources (e.g. SANS, CERT, SecurityFocus,

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
				vendor websites, etc) to identify new vulnerability issues within the environment.
<p>6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.</p>	<p>6.3 Obtain and examine written software development processes to verify that they are based on industry standards and that security is included throughout the life cycle</p> <p>From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:</p>	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
<p>6.3.1 Testing of all security patches and system and software configuration changes before deployment</p>	<p>6.3.1 All changes (including patches) are tested before being deployed into production</p>	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
6.3.2 Separate development, test, and production environments	6.3.2 The test/development environments are separate from the production environment, with access control in place to enforce the separation	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.3 Separation of duties between development, test, and production environments	6.3.3 There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.4 Production data (live PANs) are not used for testing or development	6.3.4 Production data (live PANs) are not used for testing and development, or are sanitized before use	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.5 Removal of test data and accounts before production systems become active	6.3.5 Test data and accounts are removed before a production system becomes active	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers	6.3.6 Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	6.3.7.a Obtain and review any written or other policies to confirm that code reviews are required and must be performed by individuals other than originating code author	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
	6.3.7.b Verify code reviews are conducted for new code and after code changes <i>Note: This requirement applies to code reviews for custom software development, as part of the System Development Life Cycle (SDLC) – these reviews can be conducted by internal</i>	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<i>personnel. Custom code for web-facing applications will be subject to additional controls as of June 30, 2008 – see PCI DSS requirement 6.6 for details.</i>			
6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:	6.4.a Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below			
	6.4.b For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.1 Documentation of impact	6.4.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.2 Management sign-off by appropriate parties	6.4.2 Verify that management sign-off by appropriate parties is present for each sampled change	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.3 Testing of operational functionality	6.4.3 Verify that operational functionality testing was performed for each sampled change	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service provider.
6.4.4 Back-out procedures	6.4.4 Verify that back-out procedures are prepared for each sampled change	N/A – Security Policy/Procedures (Change Control)		Change control policies and procedures is the responsibility of the merchant / service

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>6.5 Develop all web applications based on secure coding guidelines, such as the <i>Open Web Application Security Project Guidelines</i>. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:</p>	<p>6.5.a Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the <i>OWASP Guidelines</i> (http://www.owasp.org)</p>	<p>N/A – Web-based application development (secure coding) not in scope for assessment</p>		<p>provider.</p> <p>Web-based software development processes, including secure coding practices, are the responsibility of the merchant / service provider. In scope web-based applications include external and internal applications which process or transmit cardholder data.</p> <p>Cisco installed Foundstone's "Hacme Bank" application. Hacme Bank simulates a "real-world" online banking application, which has been built with a number of known and common vulnerabilities such as SQL injection and cross-site scripting. This allows users to attempt real exploits against a web application, and thus learn the specifics of the issue and how best to fix it. In addition, external websites were used to demonstrate Cisco XML Gateway's capabilities. Verizon Business observed the use of Cisco's ACE XML Gateway to</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
				protect against common web vulnerabilities and web based attacks identified under 6.5.1 – 6.5.10.
	6.5.b For any web-based applications, verify that processes are in place to confirm that web applications are not vulnerable to the following			
6.5.1 Unvalidated input	6.5.1 Unvalidated input	Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based input validation attacks. All input validation attacks were manual and required custom configuration of the ACE XML Gateway application.		See 6.5.a above
6.5.2 Broken access control (for example, malicious use of user IDs)	6.5.2 Malicious use of User IDs			See 6.5.a above Examples of broken access control prevention were not demonstrated. Such prevention could be demonstrated through secure web-coding and clean results from vulnerability scanning/penetration testing for such vulnerabilities. Additionally, Cisco is working to address additional XML and HTML based web-vulnerabilities in future releases of the product.
6.5.3 Broken authentication and session management (use of account credentials and session)	6.5.3 Malicious use of account credentials and session cookies			See 6.5.a above Examples of broken authentication and

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
cookies)				session management prevention were not demonstrated. Such prevention could be demonstrated through secure web-coding and clean results from vulnerability scanning/penetration testing for such vulnerabilities. Additionally, Cisco is working to address additional XML and HTML based web-vulnerabilities in future releases of the product.
6.5.4 Cross-site scripting (XSS) attacks	6.5.4 Cross-site scripting	Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based XSS attacks. For example, ACE XML Gateway can prevent submission of XML and HTML tags to the web server (required for XSS attacks). All XSS attacks were manual and required custom configuration of the ACE XML Gateway application.		See 6.5.a above
6.5.5 Buffer overflows	6.5.5 Buffer overflows due to unvalidated input and other causes	Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based buffer overflow attacks. URI handling (e.g. limit URI submission), field input validation, etc, was observed to prevent such attacks. All buffer overflow attacks were manual and required custom configuration of the ACE XML Gateway application.		See 6.5.a above
6.5.6 Injection flaws (for example, structured query language (SQL) injection)	6.5.6 SQL injection and other command injection flaws	Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML		See 6.5.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>based SQL injection attacks. Limiting input to specific criteria, including restricting required characters/strings for SQL attacks, was demonstrated to prevent such attacks. All SQL injection attacks were manual and required custom configuration of the ACE XML Gateway application.</p>		
<p>6.5.7 Improper error handling</p>	<p>6.5.7 Error handling flaws</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web applications from XML and HTML based error handling vulnerabilities. HTML/XML errors from the web server can be intercepted by the ACE XML Gateway and re-written as a generic, non-descript error message. This was demonstrated during the review. All error handling attacks were manual and required custom configuration of the ACE XML Gateway application to prevent improper error handling.</p>		<p>See 6.5.a above</p>
<p>6.5.8 Insecure storage</p>	<p>6.5.8 Insecure storage</p>			<p>See 6.5.a above</p> <p>Insecure storage is not designed to be prevented by the ACE XML Gateway. Secure storage should be addressed through secure coding and secure web application architecture, which includes implementation of best-practice encryption/key management for storage of sensitive data.</p>
<p>6.5.9 Denial of service</p>	<p>6.5.9 Denial of service</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web</p>		<p>See 6.5.a above</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>applications against web-based denial of service attacks. Limitations can be placed on sessions (e.g. session timeouts, number of concurrent sessions, etc) to reduce exposure to denial of service attacks.</p>		<p>Due to the nature of the lab environment and available resources, full DoS attacks were not launched. In addition to TCP (HTTP/S) session management, DoS attacks should be prevented through secure coding, and through timely application/OS patch management.</p>
<p>6.5.10 Insecure configuration management</p>	<p>6.5.10 Insecure configuration management</p>	<p>Verizon Business observed the use of ACE XML Gateway to protect web applications against the following insecure configuration management area:</p> <ul style="list-style-type: none"> - Required SSL (HTTPS) web sessions: ACE XML Gateway can be configured to force HTTPS sessions, to prevent HTTP sessions that could contain sensitive information, including administrative credentials. 		<p>See 6.5.a above</p> <p>Secure configuration management goes far beyond SSL encryption for web-application access. Disabling configuration management over insecure networks, enabling web-application security parameters, and disabling default, insecure configurations are all part of secure configuration management.</p>
<p>6.6 Ensure that all web-facing applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> • Having all custom application code reviewed for common vulnerabilities by an organization that 	<p>6.6 For web-based applications, ensure that one of the following methods are in place as follows:</p> <ul style="list-style-type: none"> • Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections 	<p>N/A – This was not included in the scope of the assessment, and is currently not a mandatory requirement for level 1 merchants and service providers.</p>		<p>Note: This will become a required practice as of June 30, 2008.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>specializes in application security</p> <ul style="list-style-type: none"> Installing an application-layer firewall in front of web-facing applications <p><i>Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.</i></p>	<ul style="list-style-type: none"> Verify that an application-layer firewall is in place in front of web-facing applications to detect and prevent web-based attacks 			

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement ensures critical data can only be accessed by authorized personnel.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.</p>	<p>7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following:</p> <ul style="list-style-type: none"> • Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities • Assignment of privileges is based on individual personnel's job classification and function • Requirement for an authorization form signed by management that specifies required privileges • Implementation of an automated access control system 	<p>N/A – Security Policy (Data Control / Data Classification)</p>		<p>Documentation for data classification / data control, including: least privilege access, role based access, authorization forms for all access, and requirements for automated access control systems, is the requirement of the merchant / service provider.</p>
<p>7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.</p>	<p>7.2 Examine system settings and vendor documentation to verify that an access control system is implemented and that it includes the following</p> <ul style="list-style-type: none"> • Coverage of all system components • Assignment of privileges to individuals based on job classification and function • Default "deny-all" setting (some access control systems are set by default to "allow-all" thereby permitting access unless/until a rule is written to specifically deny it) 	<p>Verizon Business reviewed system settings , EMC SAN storage (zoning and LUN masking configuration), vendor documentation, and interviewed SMEs for platforms within the PCI Solution for Retail environment to confirm access control systems within the environment include the following:</p> <ul style="list-style-type: none"> - Coverage of all system components within the PCI Solution for Retail environment: <ul style="list-style-type: none"> • WCS (wireless console) • Cisco ACS (authentication for all network components (e.g. ISRs, routers, switches, and 		

		<p>wireless controllers)</p> <ul style="list-style-type: none"> • CiscoWorks (LMS, NCM) • CSM (Cisco Security Manager) • CSA Manager • CS-MARS • ACE XML Gateway (direct SSH or https – auth forwards to ACS -> AD) • ASA and FWSM firewalls (direct SSH or ASDM – forwards to ACS -> AD) • ISRs (direct SSH or SDM – auth forwards to ACS -> AD) • Routers and switches (direct ssh access forwards authentication to ACS -> AD) • Wireless controllers (direct ssh access forwards authentication to ACS -> AD) • Cisco IDSM-2 modules (direct SSH or IDM – local auth) • RSA Authentication Manager • RSA Access Manager • RSA File Security Manager • RSA Key Manager • RSA enVision • NCR ACS Server • CSA client software provides additional access control protection at the OS level for POS systems and all management consoles running on Windows. CSA can be configured to restrict, monitor, and alert on access to OS/application binaries, configuration and log files, <p>- Role-based privilege assignment for</p>		
--	--	---	--	--

		<p>all management consoles (e.g. WCS, ACS, CSA, CiscoWorks (LMS, NCM), CSM, CS-MARS, ACE XML Gateway, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, RSA enVision, and NCR ACS Server)</p> <p>- Default "deny-all" settings on all management consoles and network devices. ASA firewalls, FWSMs, and ISRs contain "default-deny" access lists with explicit "permit" rules defined to the port level.</p>		
--	--	---	--	--

Requirement 8: Assign a unique ID to each person with computer access.

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.</p>	<p>8.1 For a sample of user IDs, review user ID listings and verify that <u>all</u> users have a unique username for access to system components or cardholder data</p>	<p>Verizon Business reviewed access lists for the following, to confirm all users have a unique username for access to components within the PCI Solution for Retail environment:</p> <ul style="list-style-type: none"> - CS-MARS - WCS central wireless server - Cisco ACS - Cisco Security Agent (CSA) Manager - CSM (Cisco Security Manager) - CiscoWorks (LMS) - Cisco ASDM - All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts. - Cisco ACE XML Gateway - CiscoWorks NCM - Cisco IDM - RSA enVision - RSA Key Manager - RSA Access Manager - RSA Authentication Manager (unique PIN + tokencode) - RSA File Security Manager – RSA File Security Manager does not support renaming the default Security Admin “SA” account. Only one SA account is allowed, so this generic account must be used for all SA 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>functions within RSA File Security Manager. In the Cisco lab environment the RSA File Security Manager system is accessed over RDP. This would allow unique AD credentials to be captured for system access. Additionally, Cisco leveraged CSA software to further restrict, monitor, and log access to the RSA File Security Manager executable.</p> <ul style="list-style-type: none"> - NCR ACS Server (unique AD credentials) 		
<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> • Password • Token devices (for example, SecureID, certificates, or public key) • Biometrics 	<p>8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder environment, perform the following:</p> <ul style="list-style-type: none"> • Obtain and examine documentation describing the authentication method(s) used • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s) 	<p>Verizon Business reviewed authentication methods, including observation of live login attempts to confirm a unique ID and password was required for each authentication attempt to the following:</p> <ul style="list-style-type: none"> - CS-MARS - WCS central wireless server - Cisco ACS - Cisco Security Agent (CSA) Manager - CSM (Cisco Security Manager) - CiscoWorks (LMS) - Cisco ASDM - All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts. - Cisco ACE XML Gateway - CiscoWorks NCM - Cisco IDM - RSA enVision - RSA Key Manager - RSA Access Manager - RSA Authentication Manager 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		(unique PIN + tokencode) - RSA File Security Manager (see 8.1 above) - NCR ACS Server (AD auth)		
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	8.3 To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (Smart card, token PIN) are required.	Verizon Business confirmed the use of two-factor authentication, using RSA SecurID PINs + tokencode for all remote authentication into the data center environment.		Two-factor authentication for all remote access, including for employees, contractors, and third parties, is the responsibility of the merchant / service provider.
8.4 Encrypt all passwords during transmission and storage on all system components.	8.4.a For a sample of system components, critical servers, and wireless access points, examine password files to verify that passwords are unreadable	Verizon Business confirmed local ISR and switch passwords are rendered unreadable, per review of configurations. All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which renders passwords unreadable. Authentication to CSA Manager is forwarded directly to Active Directory. Verizon Business also confirmed the following render local authentication credentials unreadable: - WCS (hashed) - CS-MARS (hashed) - Cisco ACE XML Gateway (hashed) - Cisco IDM (hashed) - CiscoWorks NCM (hashed) - RSA enVision (encrypted hash)		- RSA Authentication Manager (???)

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> - RSA Key Manager (Auth through RSA Access Manager (hashed), local auth (hashed)) - RSA Access Manager (hashed) - RSA File Security Manager (hashed) - NCR ACS (AD auth – passwords unreadable) 		
	<p>8.4.b For Service Providers only, observe password files to verify that customer passwords are encrypted</p>	<p>N/A – Service Provider requirement</p>		<p>Responsibility of service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:</p>	<p>8.5 Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:</p>			
<p>8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects</p>	<p>8.5.1.a Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following:</p> <ul style="list-style-type: none"> • Obtain and examine an authorization form for each ID • Verify that the sampled User IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained,.) by tracing information from the authorization form to the system <p>8.5.1.b Verify that only administrators have access to management consoles for wireless networks</p>	<p>N/A – Security policy and procedures (ID / Account Management)</p>		<p>Creation of access request (authorization) forms for access to PCI “in scope” systems, including: firewalls, routers, switches, VPNs, AD domain access, servers, databases, and applications, is the responsibility of the merchant / service provider.</p>
<p>8.5.2 Verify user identity before performing password resets</p>	<p>8.5.2 Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, email, web, or other non-face-to-face method, the user’s identity is verified before the password is reset</p>	<p>N/A – Security policy and procedures (ID / Account Management)</p>		<p>Account management / password reset procedures are the responsibility of the merchant / service provider.</p>
<p>8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use</p>	<p>8.5.3 Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use</p>	<p>N/A – Security policy and procedures (ID / Account Management)</p>		<p>Account management / password reset procedures are the responsibility of the merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
8.5.4 Immediately revoke access for any terminated users	8.5.4 Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been inactivated or removed	N/A – Not assessed, due to the nature of the PCI Solution for Retail environment.		
8.5.5 Remove inactive user accounts at least every 90 days	8.5.5 For a sample of user IDs, verify that there are no inactive accounts over 90 days old	N/A – Manual audit procedure or third party ID management tool.		Note: Because most authentication systems, including Active Directory, do not have built-in audit tools to easily identify inactive user accounts, manual procedures or third party tools are necessary to identify and remove inactive accounts.
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	8.5.6 Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used	N/A – No external vendor accounts were identified during the assessment.		
8.5.7 Communicate password procedures and policies to all users who have access to cardholder data	8.5.7 Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies	N/A – Security Policy (Security Awareness)		For each merchant / service provider - Individual interviews to be conducted with a sample of users to confirm security awareness for password procedures is in place.
8.5.8 Do not use group, shared, or generic accounts and passwords	8.5.8.a For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following <ul style="list-style-type: none"> Generic User IDs and accounts are disabled or removed Shared User IDs for system administration activities and other 	Verizon Business reviewed user ID lists for the following components within the PCI Solution for Retail environment to confirm generic and shared IDs are disabled or removed, or that unique administrative accounts are used in place of default accounts that cannot be renamed or removed:		Note: “pnadmin” account on CS-MARS cannot be deleted, due to application dependencies. This account is not used interactively. All administrative accounts are unique.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<p>critical functions do not exist</p> <ul style="list-style-type: none"> Shared and generic User IDs are not used to administer wireless LANs and devices 	<ul style="list-style-type: none"> - CS-MARS - WCS central wireless server - Cisco ACS - Cisco Security Agent (CSA) Manager - CSM (Cisco Security Manager) - CiscoWorks (LMS) - Cisco ASDM - All access to ASA firewalls, FWSMs, ISR routers, switches, and wireless controllers (authentication through Cisco ACS (which is configured to forward to Active Directory), using unique accounts. - Cisco ACE XML Gateway - CiscoWorks NCM - Cisco IDM - RSA enVision - RSA Key Manager - RSA Access Manager - RSA Authentication Manager - NCR ACS 		<p>Additionally, RSA File Security Manager "SA" account cannot be deleted, and is the only Security Admin account on the system. See 8.1 for compensating controls used to restrict RSA File Security Manager access and capture unique credentials for RSA File Security Manager access.</p>
	<p>8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited</p>	N/A – Security Policy (Password policy/procedures)		<p>Password policy/procedures are the responsibility of each merchant / service provider.</p>
	<p>8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested</p>	N/A – Security Policy (Password policy/procedures)		<p>Password policy/procedures are the responsibility of each merchant / service provider.</p>
<p>8.5.9 Change user passwords at least every 90 days</p>	<p>8.5.9 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless 	<p>The following do not currently support password expiration, and do not currently support external authentication (e.g.</p>	<p>Note: A combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<p>passwords at least every 90 days</p> <p>For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change</p>	<p>controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which is set to expire passwords after 42 days.</p> <ul style="list-style-type: none"> - CSA Manager (AD auth = 42 days) - Cisco ACE XML Gateway (ACS or AD auth = 42 days) - CS-MARS (AD auth through Cisco ACS = 42 days) - WCS (AD auth through Cisco ACS = 42 days) - CiscoWorks NCM (ACS or AD auth) - RSA enVision (ACS or AD auth = 42 days) - RSA Key Manager (RSA Access Manager auth = 60 days) - RSA Access Manager (60 days) - RSA Authentication Manager (tokencode changes every 60 seconds) - NCR ACS (AD auth = 42 days) 	<p>TACACS or AD):</p> <ul style="list-style-type: none"> - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>days, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>
<p>8.5.10 Require a minimum password length of at least seven characters</p>	<p>8.5.10 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long</p> <p>For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSPs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces passwords to contain a minimum of 7 characters. - CSA Manager (AD Auth = min 7 chars) - Cisco ACE XML Gateway (ACS or AD auth = min 7 chars, local auth= 8 characters) - CS-MARS (AD auth through Cisco ACS = min 7 chars) 	<p>The following do not currently enforce password complexity (e.g. length, alphanumeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>Note: A combination of documented password policies, manual audit procedures to ensure strong password generation, using periodic dictionary attacks against passwords, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> - WCS (AD auth through Cisco ACS = min 7 chars) - CiscoWorks NCM (ACS or AD auth, local auth= 8 characters) - RSA enVision (ACS or AD auth = min 7 chars) - RSA Key Manager (RSA Access Manager auth = 8 characters) - RSA Access Manager (8 characters) - RSA Authentication Manager (PIN + tokencode = min 10, max 16) - NCR ACS (AD auth = min 7 chars) 		
<p>8.5.11 Use passwords containing both numeric and alphabetic characters</p>	<p>8.5.11 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters</p> <p>For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), and CSM) are forwarded to Active Directory, which enforces alpha-numeric passwords. - CSA Manager (AD Auth = alpha-numeric) - Cisco ACE XML Gateway (ACS or AD auth = alpha-numeric) - CS-MARS (AD auth through Cisco ACS = alpha-numeric) - WCS (AD auth through Cisco ACS = alpha-numeric) - CiscoWorks NCM (ACS or AD auth = alpha-numeric, local auth requires upper/lower case + at least 1 special character or digit) - RSA enVision (ACS or AD auth = alpha-numeric) - RSA Key Manager (RSA Access Manager auth = alpha-numeric + 	<p>The following do not currently enforce password complexity (e.g. length, alpha-numeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>Note: A combination of documented password policies, manual audit procedures to ensure strong password generation, using periodic dictionary attacks against passwords, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		dictionary check) - RSA Access Manager (alpha-numeric + dictionary check) - RSA Authentication Manager (supports alpha-numeric) - NCR ACS (AD auth = alpha-numeric)		
<p>8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used</p>	<p>8.5.12 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords</p> <p>For Service Providers only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSPs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces password history for the last 24 passwords. - CSA Manager (AD Auth = last 24 passwords) - Cisco ACE XML Gateway (ACS or AD auth = last 24 passwords) - CS-MARS (AD auth through Cisco ACS = last 24 passwords) - WCS (AD auth through Cisco ACS = last 24 passwords) - CiscoWorks NCM (ACS or AD auth = last 24 passwords) - RSA enVision (ACS or AD auth = last 24 passwords) - RSA Key Manager (RSA Access Manager auth = last 10 passwords) - RSA Access Manager (last 10 passwords) - RSA Authentication Manager (tokencode changes to random value every 60 seconds) - NCR ACS (AD auth = last 24 passwords) 	<p>The following do not currently enforce password complexity (e.g. length, alpha-numeric, history, etc), and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> - Cisco IDM (will be addressed in Cisco IDM v6.1 release) - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>Note: A combination of documented password policies and internal firewall segmentation of these components within the data center would be reasonable compensating controls for password setting limitations within these applications.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts</p>	<p>8.5.13 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts</p> <p>For Service Providers only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts</p>	<p>Verizon Business reviewed system settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces account lockouts after 5 invalid logon attempts. - CSA Manager (AD Auth = 5 invalid attempts) - Cisco ACE XML Gateway (ACS or AD auth = 5 invalid attempts, local auth= 3 invalid attempts) - CS-MARS (AD auth through Cisco ACS = 5 invalid attempts) - WCS (AD auth through Cisco ACS = 5 invalid attempts) - CiscoWorks NCM (ACS or AD auth = 5 invalid attempts, local auth= 6 invalid attempts) - Cisco IDM (5 invalid attempts) - RSA enVision (ACS or AD auth = 5 invalid attempts) - RSA Key Manager (RSA Access Manager auth = 3 invalid attempts in one day) - RSA Access Manager (3 invalid attempts in one day) - RSA Authentication Manager (3 invalid passcodes forces "next token" mode, which requires two consecutive token codes to be entered. 6 failed attempts disables token use) - NCR ACS (AD auth = 5 invalid attempts) 	<p>The following do not currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>Note: Using CSA or other monitoring software to alert on continuous invalid logon attempts, combined with internal firewall segmentation of these components, would be reasonable compensating controls for account lockout setting limitations within these applications.</p>
<p>8.5.14 Set the lockout</p>	<p>8.5.14 For a sample of system</p>	<p>Verizon Business reviewed system</p>	<p>The following do not</p>	<p>Note: Using CSA or</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>duration to thirty minutes or until administrator enables the user ID</p>	<p>components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account</p>	<p>settings for authentication methods to confirm the following:</p> <ul style="list-style-type: none"> - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which enforces account lockouts for 30 minutes. - CSA Manager (AD Auth = 30 min lockout) - Cisco ACE XML Gateway (ACS or AD auth = 30 min lockout, local auth= admin must reset) - CS-MARS (AD auth through Cisco ACS = 30 min lockout) - WCS (AD auth through Cisco ACS = 30 min lockout) - CiscoWorks NCM (ACS or AD auth = 30 min lockout, local auth= admin must reset) - Cisco IDM (Admin must reset) - RSA enVision (ACS or AD auth = 30 min lockout) - RSA Key Manager (RSA Access Manager auth = admin must reset) - RSA Access Manager (admin must reset) - RSA Authentication Manager (admin must reset) - NCR ACS (AD auth = 30 min lockout) 	<p>currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD):</p> <ul style="list-style-type: none"> - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release) 	<p>other monitoring software to alert on continuous invalid logon attempts, combined with internal firewall segmentation of these components, would be reasonable compensating controls for account lockout setting limitations within these applications.</p>
<p>8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal</p>	<p>8.5.15 For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less</p>	<p>Verizon Business confirmed the following components within the PCI Solution for Retail environment have sufficient idle timeout settings:</p> <ul style="list-style-type: none"> - ISRs and switches: (15 minute session-timeout and 15 minute exec-timeout) 	<p>The following do not support idle session timeouts (15 minutes or less) for administrative connections:</p> <ul style="list-style-type: none"> - WCS - IDM 	<p>Note: Screensaver timeouts can be used as a compensating control, when idle session timeouts are not available or impact application/business operations (e.g. backup</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> - ASA firewalls (15 minutes – ssh) - Wireless controllers (15 minutes – ssh) - CiscoWorks (LMS): (15 minutes) - CS-MARS: (15 minutes) - CSM Manager: (15 minutes) - ACS: (15 minutes) - CSA Manager: (15 minutes) - Cisco ACE XML Gateway (15 minutes) - CiscoWorks NCM (15 minutes) - RSA enVision (10 minutes) - RSA Key Manager (15 minutes) - RSA Access Manager (10 minutes) - NCR ACS (configurable to 1 minute) 	<ul style="list-style-type: none"> - wireless controllers (web interface) - ASDM - IDM - RSA File Security Manager (to be addressed in FSM v2.2 release) - RSA Authentication Manager 	<p>jobs).</p>
<p>8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users</p>	<p>8.5.16.a Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators</p>	<p>N/A – Database security not part of the PCI Solution for Retail environment assessment.</p>		<p>Note: Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.</p>
	<p>8.5.16.b Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts. Direct SQL queries should be limited to database administrators)</p>	<p>N/A – Database security not part of the PCI Solution for Retail environment assessment.</p>		<p>Note: Database security, including prohibiting direct SQL queries to the database is the responsibility of the merchant / service provider. Database login accounts should be limited to application accounts and very few dba accounts.</p>

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.</p>	<p>9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data</p> <ul style="list-style-type: none"> • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use 	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p>9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.</p>	<p>9.1.1 Verify that video cameras monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Verify that cameras are monitored and that data from cameras is stored for at least three months</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p>9.1.2 Restrict physical access to publicly accessible network jacks</p>	<p>9.1.2 Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>
<p>9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices</p>	<p>9.1.3 Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted</p>	<p>N/A – Security Policy/Procedures (Physical Security)</p>		<p>Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. <i>“Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>	9.2.a Review processes and procedures for assigning badges to employees, contractors, and visitors, and verify these processes include the following: <ul style="list-style-type: none"> Procedures in place for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges Limited access to badge system 	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
	9.2.b Observe people within the facility to verify that it is easy to distinguish between employees and visitors	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.3 Make sure all visitors are handled as follows:	9.3 Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	9.3.1 Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	9.3.2 Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outside and that visitor badges expire	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	9.3.3 Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.4 Use a visitor log to	9.4.a Verify that a visitor log is in use to	N/A – Security Policy/Procedures		Physical security

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.	record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted	(Physical Security)		(policies, procedures, and controls) is the responsibility of the merchant / service provider.
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility.	9.5 Verify that the storage location for media backups is secure. Verify that offsite storage is visited periodically to determine that backup media storage is physically secure and fireproof	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data	9.6 Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media in computer rooms and data centers (including paper receipts, paper reports, faxes, CDs, and disks in employee desks and open workspaces, and PC hard drives)	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: including the following	9.7 Verify that a policy exists to control distribution of media containing cardholder data, that the policy covers all distributed media including that distributed to individuals	N/A – Security Policy/Procedures (Physical Security/Data Classification)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.7.1 Classify the media so it can be identified as confidential	9.7.1 Verify that all media is classified so that it can be identified as "confidential"	N/A – Security Policy (Data Classification)		Physical security/Data Classification (policies, procedures, and controls) is the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	9.7.2 Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery mechanism that can be tracked	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	9.8 Select a recent sample of several days of offsite media tracking logs, and verify the presence in the logs of tracking details and proper management authorization	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	9.9 Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.9.1 Properly inventory all media and make sure it is securely stored.	9.9.1.a Obtain and review the media inventory log to verify that periodic media inventories are performed 9.9.1.b Review processes to verify that media is securely stored	9.9.1.a N/A – Security Policy/Procedures (Physical Security) 9.9.1.b N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows	9.10 Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials	9.10.1.a Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped, in accordance with ISO 9564-1 or ISO 11568-3e	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured.	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	For example, verify that a “to-be-shredded” container has a lock preventing access to its contents			responsibility of the merchant / service provider.
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed	9.10.2 Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	10.1 Verify through observation and interviewing the system administrator, that audit trails are enabled and active, including for any connected wireless networks.	Verizon Business confirmed through interviews and review of configured log settings, as well as review of the audit trail, that audit trails are enabled and active for the following components within the PCI Solution for Retail environment: - ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (direct ssh access) <ul style="list-style-type: none"> AD auth logs (Cisco ACS auth requests forwarded to AD). CiscoWorks (LMS) – for configuration management (non-security related) – (wireless logs not 		Note: WCS audit trail exists for authentication and administrative access; however, the audit trail is difficult to follow and could require significant time, including experienced Cisco support to fully understand and piece together the audit trail.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>sent to LMS)</p> <ul style="list-style-type: none"> • CSM (security alerts (e.g. firewall logs, IDS alerts, etc) sent from devices to CSM are forwarded to CS-MARS) • CiscoWorks NCM (configuration changes, policy/standards violations) <p>- Cisco ACS</p> <ul style="list-style-type: none"> • Local and AD authentication logs (auth requests forwarded to AD) • Local audit trail for ACS management <p>- CSM (Cisco Security Manager)</p> <ul style="list-style-type: none"> • AD auth logs (Cisco ACS auth requests forwarded to AD). • Local audit trail for CSM management <p>- CSA (Cisco Security Agent) Manager</p> <ul style="list-style-type: none"> • AD authentication logs (authentication requests sent directly to AD). • All CSA logs, alerts/events sent to CSA manager • Local audit trail for CSA management <p>- CS-MARS</p> <ul style="list-style-type: none"> • Local authentication logs (no ACS or AD authentication available) • CSA logging/alerts, CSM security events (firewall logs (ASAs and ISRs), IDS/IPS alerts) • Local audit trail for CS-MARS <p>- WCS (Wireless Console Server)</p> <ul style="list-style-type: none"> • Local authentication 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> • Local audit trail for WCS management and wireless configuration changes - CiscoWorks (LMS) <ul style="list-style-type: none"> • AD auth logs (Cisco ACS auth requests forwarded to AD). • ISR (router) and switch configuration management logs • Local audit trail for LMS management - CiscoWorks NCM <ul style="list-style-type: none"> • AD auth logs (Cisco ACS auth requests forwarded to AD). • Audit trail of network device configuration changes (date and time of change, who made the change, and lines of configuration changed). • Local audit trail for NCM management - Cisco ASDM <ul style="list-style-type: none"> • AD auth logs (Cisco ACS auth requests forwarded to AD). • ASA firewall configuration changes and IDS/IPS alerts sent to CS-MARS. - Cisco IDM <ul style="list-style-type: none"> • IDM local auth logs and local configuration changes. - Cisco ACE XML Gateway <ul style="list-style-type: none"> • AD auth logs (Cisco ACS auth requests forwarded to AD). • Local audit trail for ACE XML Gateway management. - RSA SecurID <ul style="list-style-type: none"> • RSA SecurID access logged through RSA Authentication Manager. 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> • RSA SecurID logs captured by RSA enVision for reporting, alerting, and long-term storage. - RSA Authentication Manager <ul style="list-style-type: none"> • RSA SecurID authentication attempts • Local audit trail for RSA Authentication Manager administrative access/mgmt. • Audit log SFTP'd to RSA enVision every 60 minutes for reporting, alerting, and long-term storage. - RSA Access Manager <ul style="list-style-type: none"> • RSA Key Manager authentication logs • Local audit trail for RSA Access Manager access/management. - RSA File Security Manager (RSA File Security Manager) <ul style="list-style-type: none"> • Local/AD auth logs (access to server) • CSA (Monitors and logs RSA File Security Manager binary use) • Access to RSA File Security Manager protected resources (e.g. access to cardholder data) • Local audit trail for RSA File Security Manager access/management. - RSA Key Manager <ul style="list-style-type: none"> • Local/AD auth logs (access to server) • CSA (Monitors and logs Key Manager binary use) • Key Material requests 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> • Local audit trail for Key Manager access/management. - RSA enVision <ul style="list-style-type: none"> • RSA local/AD auth logs • Local audit trail for RSA enVision access/management. • Local audit trail for RSA enVision log repository access. • RSA SecurID access logs (SFTP'd from RSA Authentication Manager every 60 minutes). - NCR ACS Server <ul style="list-style-type: none"> • Local/AD logs for server access • CSA (Monitors and logs NCR ACS binary use and access to NCR ACS application log files) • Local audit trail for NCR ACS access/management. 		
<p>10.2 Implement automated audit trails for all system components to reconstruct the following events:</p>	<p>10.2 Verify through interviews, examination of audit logs, and examination of audit log settings, that the following events are logged into system activity logs:</p>			
<p>10.2.1 All individual accesses to cardholder data</p>	<p>10.2.1 All individual access to cardholder data</p>	<p>Verizon Business confirmed the following log access to cardholder data within the Cisco's PCI Solution for Retail environment:</p> <ul style="list-style-type: none"> - NCR ACS (logs to EFT log file and Transaction Log) - RSA File Security Manager (logs access to cardholder data protected by RSA File Security Manager) - RSA Key Manager (logs key material requests (necessary for decryption of cardholder data)) - Cisco CSA (installed on all Windows servers within the PCI Solution for 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		Retail environment and configured to monitor and log use of NCR ACS application binaries and log files. Only encrypted cardholder data is accessible within NCR application log files. These files have been configured through Cisco CSA to only allow necessary process and administrative accounts access. Only masked data is accessible through the NCR ACS application.)		
<p>10.2.2 All actions taken by any individual with root or administrative privileges</p>	<p>10.2.2 Actions taken by any individual with root or administrative privileges</p>	<p>Verizon Business reviewed audit log configurations to confirm administrative actions are logged for the following:</p> <ul style="list-style-type: none"> - Management of ASA firewalls, FWSMs, ISRs, routers, IDSM2, switches (ASDM, SDM, CSM, or SSH (forwarded to CS-MARS), CiscoWorks (LMS)) - CS-MARS administration (CS-MARS audit trail) - ACS administration (CSA and local ACS audit trail) - CSA administration (CSA and local CSA audit trail) - CiscoWorks administration (LMS) (CSA and local LMS audit trail) - Wireless controllers (WCS logs) - WCS (CSA and local WCS audit trail – Administrative changes to WCS are logged to the audit trail, but difficult to determine the details of the change) - CSM administration (CSA and local CSM audit trail) - NCM administration (CSA and NCM audit trail) - Cisco ACE XML Gateway (local ACE XML Gateway audit trail) 	<p>The following have limited audit trails, related to administrative actions:</p> <ul style="list-style-type: none"> - RSA File Security Manager (not all administrative actions are logged - to be addressed in FSM v2.2 release) 	<p>Note: Wireless audit trail exists for authentication and administrative access; however, the audit trail is difficult to follow and could require significant time, including experienced Cisco support to fully understand and piece together the audit trail.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> - Cisco IDM (local IDM audit trail) - RSA Authentication Manager (CSA, local RSA Authentication Manager audit trail, RSA enVision (SFTP'd from RSA Authentication Manager every 60 minutes)) - RSA Access Manager (CSA, local RSA Access Manager audit trail) - RSA Key Manager (local audit trail for Key Manager administration) - RSA enVision (local audit trail for enVision administration) - NCR ACS Server (local EFT and Transaction Log files) <p>Note: Reference to CSA is for administrative changes on Windows host OS for each application running on Windows.</p>		
<p>10.2.3 Access to all audit trails</p>	<p>10.2.3 Access to all audit trails</p>	<p>Verizon Business observed CSA Manager policies, log directories and log files monitored by CSA, and CSA event logs generated upon unauthorized access of audit log files and directories, to determine access to the following audit trails is being logged:</p> <ul style="list-style-type: none"> - ACS, CiscoWorks (LMS, NCM), CSA Manager, CSM, WCS Manager, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, NCR ACS: <ul style="list-style-type: none"> • Live log directory and files (CSA is configured to allow application services to write/delete/modify files in the live log directory and rotate (archive) log files to an archive directory. All other users and processes are 		<p>Note: Management consoles reviewed did not log access to audit trails, without CSA monitoring of audit logs. Cisco used a custom archive/backup method to copy the audit trail to a central backup server. Cisco has inserted the script within the Appendix of their implementation guide.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>restricted from accessing, modifying, or deleting files within the live log directories. This prevents users from accessing the audit trail outside of the application (ACS, CiscoWorks (LMS, NCM), WCS, CSM, CSA console, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, NCR ACS). Cisco created a custom archive script which is run from a central backup server and copies all audit logs to a central backup server, where additional CSA protection can be applied. The archive directories are monitored to protect all processes and users from deleting or modifying files written to the archive directory, other than the backup user account which copies files to this directory (necessary to copy files and delete files older than 1 year).</p> <p>- CS-MARS (appliance server, which does not support CSA)</p> <ul style="list-style-type: none"> • Audit log files backed up daily to an NFS backup server are monitored by CSA and all processes and users (except the application processes responsible for writing data to the NFS server) are prohibited from modifying or deleting files from this directory. <p>- RSA enVision (not monitored by CSA, because log files are stored within a proprietary database)</p> <ul style="list-style-type: none"> • Access to application is restricted to least privilege, role-based accounts, and logged • Details on reports 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>run/viewed is logged</p> <p>Verizon Business observed unauthorized attempts to access the audit trail, outside the application. CSA alerts were generated, sent to the CS-MARS central server, and an email alert was sent to the administrator.</p>		
<p>10.2.4 Invalid logical access attempts</p>	<p>10.2.4 Invalid logical access attempts</p>	<p>Verizon Business confirmed that invalid logical access attempts are logged for the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers - Access to CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, CSM, and ACE XML Gateway, IDM - Access to RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager - NCR ACS Server 		
<p>10.2.5 Use of identification and authentication mechanisms</p>	<p>10.2.5 Use of identification and authentication mechanisms</p>	<p>Verizon Business confirmed that userID for authentication is logged for authentication to the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, CSM, ACE XML Gateway, IDM - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager - NCR ACS Server 		
<p>10.2.6 Initialization of the</p>	<p>10.2.6 Initialization of audit logs</p>	<p>Verizon Business confirmed that RSA</p>		<p>See 10.2.3 (CSA</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
audit logs		enVision does not provide capabilities to delete the audit trail through the application. See 10.2.3 (CSA protection for audit trail access applies to initialization of audit trail)		protection for audit trail access applies to initialization of audit trail)
10.2.7 Creation and deletion of system-level objects	10.2.7 Creation and deletion of system level objects	Verizon Business confirmed CSA is installed on all Windows servers within the PCI Solution for Retail environment and is configured to capture deletion of system level objects. Additionally, CiscoWorks (LMS, NCM), and CSM capture all administrative actions for ASA firewalls, FWSMs, ISRs, IDSM2 and switches.		
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Verify through interviews and observation, for each auditable event (from 10.2), that the audit trail captures the following:			
10.3.1 User identification	10.3.1 User identification	Verizon Business confirmed userID is captured in the audit trail for the following: - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM. - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager - NCR ACS Server		
10.3.2 Type of event	10.3.2 Type of event	Verizon Business confirmed event type is captured in the audit trail for the following: - All ASA firewalls, FWSMs, ISRs,		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<p>routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes)</p> <ul style="list-style-type: none"> - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (contained within local audit trails) - CSA generated logs and alerts contain event type within each record. - ACS and AD contain event type within each authentication record. - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records) - NCR ACS Server (contained within EFT and Transaction Log files) 		
<p>10.3.3 Date and time</p>	<p>10.3.3 Date and time stamp</p>	<p>Verizon Business confirmed date and time stamp is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes) - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (date and time stamp contained within local audit trail records) - CSA generated logs and alerts contain a date and time stamp within each record. - ACS and AD contain date and time stamp for each authentication record. 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		<ul style="list-style-type: none"> - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records) - NCR ACS Server (contained within EFT and Transaction Log files) 		
<p>10.3.4 Success or failure indication</p>	<p>10.3.4 Success or failure indication, including those for wireless connections</p>	<p>Verizon Business confirmed “success or failure” indication is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – audit events would indicate a successful change to the configuration. Failed actions based on insufficient permissions would be logged in the ACS audit trail.) - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (success or failure is evident based on event type and/or event detail). - “Success” or “Failure” indication is evident within CSA generated logs and alerts based on the event type. - ACS and AD logs contain success or failure indication for each authentication record. - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (evident based on details within audit trail records) - NCR ACS Server (evident based on details within audit trail records) 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>10.3.5 Origination of event</p>	<p>10.3.5 Origination of event</p>	<p>Verizon Business confirmed “origination of event” is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – security and syslog messages indicate originating device.) - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (local audit trail indicates whether event is locally generated or sent from managed device). - CSA generated logs and alerts indicate originating host. - ACS and AD logs contain originating system for each authentication record. - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (contained within local audit trail records) - NCR ACS Server (all records are local to system) 		
<p>10.3.6 Identity or name of affected data, system component, or resource</p>	<p>10.3.6 Identity or name of affected data, system component, or resources</p>	<p>Verizon Business confirmed “name of affected data, system component, or resource” is captured in the audit trail for the following:</p> <ul style="list-style-type: none"> - All ASA firewalls, FWSMs, ISRs, routers, switches, IDSM2, and wireless controllers (LMS, NCM, and CSM contain detailed audit trail records for security and device configuration changes – security and syslog messages indicate specific 		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		configuration changes being made.) - CS-MARS, CSA Manager, Cisco ACS, CiscoWorks (LMS, NCM), WCS, ACE XML Gateway, IDM, and CSM (local audit trail indicates affected data or resource through event type). - CSA generated logs and alerts indicate detailed information on affected data. - RSA enVision, RSA Key Manager, RSA File Security Manager, RSA Authentication Manager, and RSA Access Manager (evident based on details within audit trail records) - NCR ACS Server (evident based on details within audit trail records)		
10.4 Synchronize all critical system clocks and times	10.4 Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:	Verizon Business reviewed device configurations to confirm management consoles, ACE XML Gateway, ASA firewalls, FWSMs, IDSM2, ISR routers, switches, and wireless devices synchronize system clocks as follows:		
	10.4.a Verify that NTP or similar technology is used for time synchronization	NTP is used for all time synchronization.		
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]	Verizon Business reviewed network device configurations and Windows registry settings to confirm all servers and network devices within the PCI Solution for Retail environment point to at least two internal NTP servers.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	<p>10.4.c Verify that the Network Time Protocol (NTP) is running the most recent version</p> <p>10.4.d Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information</p>	<p>Verizon Business confirmed NTP version 4.2.0 is used for internal time synchronization. Latest stable release is 4.2.2, however, this is a hardened appliance used for time synchronization. No major security bugs have been identified for NTP between the 4.2.0 and 4.2.2 releases.</p> <p>Verizon Business reviewed vendor documentation for the NTP appliances. Internal NTP appliances point to a pool of IP addresses under pool.ntp.org and time.nist.gov. Internal NTP servers do not receive NTP updates, but poll external servers for time updates.</p>		
<p>10.5 Secure audit trails so they cannot be altered</p>	<p>10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:</p>			
<p>10.5.1 Limit viewing of audit trails to those with a job-related need</p>	<p>10.5.1 Verify that only individuals who have a job-related need can view audit trail files</p>	<p>Verizon Business confirmed CS-MARS and RSA enVision, as well as all back-end management consoles, are segmented behind multiple firewalls within the data center environment. All firewalls have been configured to only allow necessary inbound and outbound traffic.</p> <p>See 10.2.3 for additional audit trail access details.</p>		<p>See 10.2.3</p>
<p>10.5.2 Protect audit trail files from unauthorized modifications</p>	<p>10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation,</p>	<p>See 10.2.3/10.5.1 above</p>		<p>See 10.2.3</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	and/or network segregation			
<p>10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.</p>	<p>10.5.3 Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter</p>	<p>Verizon Business confirmed centrally stored audit logs within CS-MARS are archived once an hour and sent to a central NFS server running CSA software.</p> <p>CiscoWorks (LMS) is archiving audit trail once a day. (See 10.2.3 for additional details of audit trail archiving)</p> <p>RSA enVision centrally stores RSA SecurID log records (sent every 60 minutes from RSA Authentication Manager).</p>		<p>See 10.2.3</p>
<p>10.5.4 Copy logs for wireless networks onto a log server on the internal LAN</p>	<p>10.5.4 Verify that logs for wireless networks are offloaded or copied onto a centralized internal log server or media that is difficult to alter</p>	<p>Verizon Business confirmed wireless logs are sent to WCS and CS-MARS central servers.</p>		
<p>10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)</p>	<p>10.5.5 Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities</p>	<p>Cisco Security Agent (CSA) software is used to monitor and protect access to audit trail files, and alert on unauthorized attempts to modify the audit trail (only application services responsible for writing log data can write/modify/delete the audit trail).</p> <p>Cisco has created an additional backup script to copy the audit trail to a central backup server, where CSA protection has been applied to eliminate all access, modification, and deletion, except for the account responsible for backing up the audit trail (see 10.2.3 for additional details).</p> <p>RSA enVision's proprietary database uses 32-bit checksums for log record integrity, in addition to its write-once, read-many design. Audit records cannot be modified through the application.</p>		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).</p> <p><i>Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6</i></p>	<p>10.6.a Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required</p>	<p>Verizon Business confirmed the use of CS-MARS, RSA enVision, and CSA software, which perform correlation and analysis of system events, and alert on those warranting immediate action.</p> <p>Note: Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions (responsibility of merchant / service provider)</p>		<p>Note: Although manual log review, escalation, and follow-up procedures would be the responsibility of the merchant / service provider, automated log correlation, analysis, and alerting is the most efficient way to stay on top of copious amounts of log data.</p>
	<p>10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components</p>	<p>See 10.6.a above.</p>		<p>Interviews to be conducted with each merchant / service provider.</p>
<p>10.7 Retain audit trail history for at least one year, with a minimum of three months available online.</p>	<p>10.7.a Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year</p>	<p>N/A – Security Policy (Data Retention)</p>		<p>Retention policy and procedure documentation is the responsibility of the merchant / service provider.</p>
	<p>10.7.b Verify that audit logs are available online or on tape for at least one year</p>	<p>Verizon Business reviewed online logs and audit trail archive methods within the PCI Solution for Retail environment to confirm audit trails can be retained for at least one year, with at least three months available online.</p>		<p>Note: Due to the nature of the lab environment reviewed, and the recent addition to some components within the environment, archive logs were not available for the full 90 days, for all components; however, sufficient disk space is available to accommodate this logging. Additionally, log retention is directly dependant on the amount of logging within the environment.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
				Proper sizing, based on expected traffic patterns, is critical to ensuring sufficient space is available for online logs.

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	11.1.a Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.	Verizon Business observed CiscoWorks NCM used to audit network security configurations within the environment (e.g. test for Telnet running on all network devices, test for default user accounts, default SNMP community strings, etc). Although such testing is only one example of overall security controls testing expected for PCI compliance, Verizon Business determined it is an effective method for such testing across network components.		Continually testing security controls and application code is the responsibility of merchant / service provider.
	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.	Verizon Business confirmed that wireless controllers are configured to continually scan and detect rogue APs and wireless devices.		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new	11.2.a Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment	N/A – Internal quarterly scanning		Responsibility of merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>system component installations, changes in network topology, firewall rule modifications, product upgrades).</p> <p><i>Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.</i></p>	<p>occurs. Verify that the scan process includes rescans until "clean" results are obtained</p> <p>11.2.b To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify that</p> <ul style="list-style-type: none"> • Four quarterly scans occurred in the most recent 12-month period • The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures 			
<p>11.3 Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following</p>	<p>11.3 Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that any noted vulnerabilities were corrected. Verify that the penetration tests include:</p>	<p>N/A – Penetration Testing (at least annually)</p>		<p>Responsibility of merchant / service provider.</p> <p>Note: Penetration testing needs to be conducted on internal and external system components (network devices, applications, and servers), which are "in scope" for PCI.</p>
<p>11.3.1 Network-layer penetration tests</p>	<p>11.3.1 Network-layer penetration tests</p>	<p>N/A – Penetration Testing (at least annually)</p>		<p>Responsibility of merchant / service provider.</p>
<p>11.3.2 Application-layer penetration tests</p>	<p>11.3.2 Application-layer penetration tests</p>	<p>N/A – Penetration Testing (at least annually)</p>		<p>Responsibility of merchant / service provider.</p>

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.</p>	<p>11.4.a Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored</p>	<p>Verizon Business reviewed the PCI Solution for Retail environment, including device configurations and confirmed Cisco ASA firewalls (with integrated IDS/IPS), ISRs (with integrated IOS IDS), and IDSM-2 modules were configured with full IDS functionality. Verizon Business reviewed IDS placement within the retail and datacenter (Internet Edge, WAN edge, and core data center segments) networks, and confirmed that all critical traffic to, from, and within the PCI Solution for Retail environment would be subject to IDS monitoring. Cisco CSA (host-based IDS/IPS) is also used on critical POS servers and management consoles (e.g. CSM, CiscoWorks (LMS, NCM), CSA console, ACS, and WCS console).</p>		
	<p>11.4.b Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises</p>	<p>Verizon Business confirmed IDS/IPS is in place and can be configured to monitor and alert personnel of suspected compromise.</p>		
	<p>11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection</p>	<p>Verizon Business confirmed ASA firewalls, FWSMs, ISRs, and IDSM-2 versions are running updated releases, and are configured to automatically update IDS/IPS signatures. CSA (host-based IDS/IPS) does not rely on signatures, but is behavioral based, eliminating the need to update signatures.</p>		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
<p>11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.</p> <p><i>Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider)</i></p>	<p>11.5 Verify the use of file integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities</p>	<p>Verizon Business reviewed vendor documentation and observed Cisco Security Agent software in the PCI Solution for Retail environment. In addition to logging and alerting on critical file modification, CSA can also log and alert on attempted access, allowed or denied. Since the initial phase I review of CSA, CSA has been updated with new PCI rules, complete with critical OS files.</p>		

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners)	N/A – Security Policy Note: Verizon Business has assisted numerous merchants and service providers to create new and augment existing policies and procedures to meet PCI requirements.		Responsibility of merchant / service provider.
12.1.1 Addresses all requirements in this specification	12.1.1 Verify that the policy addresses all requirements in this specification.	N/A – Security Policy		Responsibility of merchant / service provider.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	12.1.2 Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment	N/A – Security Policy		Responsibility of merchant / service provider.
12.1.3 Includes a review at least once a year and updates when the environment changes	12.1.3 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment	N/A – Security Policy		Responsibility of merchant / service provider.
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	12.2.a Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements	N/A – Security Policy and Procedures		Responsibility of merchant / service provider.
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	12.3 Obtain and examine the policy for critical employee-facing technologies and verify the policy contains the following:			
12.3.1 Explicit management	12.3.1 Verify that the usage policies	N/A – Acceptable Use Policy		Responsibility of merchant / service

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
approval	require explicit management approval to use the devices			provider.
12.3.2 Authentication for use of the technology	12.3.2 Verify that the usage policies require that all device use is authenticated with username and password or other authentication item (for example, token)	N/A – Acceptable Use Policy		Responsibility of merchant / service provider.
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies require a list of all devices and personnel authorized to use the devices	N/A – Acceptable Use Policy / Asset List		Responsibility of merchant / service provider.
12.3.4 Labeling of devices with owner, contact information, and purpose	12.3.4 Verify that the usage policies require labeling of devices with owner, contact information, and purpose	N/A – Acceptable Use Policy / Asset List		Responsibility of merchant / service provider.
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies require acceptable uses for the technology	N/A – Acceptable Use Policy		Responsibility of merchant / service provider.
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies require acceptable network locations for the technology	N/A – Acceptable Use Policy		Responsibility of merchant / service provider.
12.3.7 List of company-approved products	12.3.7 Verify that the usage policies require a list of company-approved products	N/A – Acceptable Use Policy		Responsibility of merchant / service provider.
12.3.8 Automatic disconnect of modem sessions after a specific period of inactivity	12.3.8 Verify that the usage policies require automatic disconnect of modem sessions after a specific period of inactivity	N/A – Acceptable Use / Remote Access Policy		Responsibility of merchant / service provider.
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use	12.3.9 Verify that the usage policies require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use	N/A – Acceptable Use / Remote Access Policy		Responsibility of merchant / service provider.
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy	12.3.10 Verify that the usage policies prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem. Verify	N/A – Acceptable Use Policy / Remote Access Policy		Responsibility of merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
disks, or other external media. Prohibition of cut-and-paste and print functions during remote access	that the policies prohibit cut-and-paste and print functions during remote access			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	12.4 Verify that information security policies clearly define information security responsibilities for both employees and contractors	N/A – Security Policy		Responsibility of merchant / service provider.
12.5 Assign to an individual or team the following information security management responsibilities:	12.5 Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:	N/A – Security Policy		Responsibility of merchant / service provider.
12.5.1 Establish, document, and distribute security policies and procedures	12.5.1 Verify that responsibility for creating and distributing security policies and procedures is formally assigned	N/A – Security Policy		Responsibility of merchant / service provider.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel	12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned	N/A – Security Policy (Risk / Vulnerability management)		Responsibility of merchant / service provider.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	12.5.3 Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned	N/A – Security Policy (Incident Response)		Responsibility of merchant / service provider.
12.5.4 Administer user accounts, including additions, deletions, and modifications	12.5.4 Verify that responsibility for administering user account and authentication management is formally assigned	N/A – Security Policy (ID / Account management)		Responsibility of merchant / service provider.
12.5.5 Monitor and control	12.5.5 Verify that responsibility for	N/A – Security Policy (Data Control /		Responsibility of

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
all access to data	monitoring and controlling all access to data is formally assigned	Monitoring)		merchant / service provider.
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:	12.6.a Verify the existence of a formal security awareness program for all employees	N/A – Security Policy (Security Awareness)		Responsibility of merchant / service provider.
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)	N/A – Security Policy (Security Awareness)		Responsibility of merchant / service provider.
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually	N/A – Security Policy (Security Awareness)		Responsibility of merchant / service provider.
12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures	12.6.2 Verify that the security awareness program requires employees to acknowledge in writing that they have read and understand the company's information security policy	N/A – Security Policy (Security Awareness)		Responsibility of merchant / service provider.
12.7 Screen potential employees to minimize the risk of attacks from internal sources. <i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	12.7 Inquire of Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential employees who will have access to cardholder data or the cardholder data environment. (Examples of background checks include pre-employment, criminal, credit history, and reference checks)	N/A – Security Policy (Background Checks)		Responsibility of merchant / service provider.
12.8 If cardholder data is shared with service providers, then contractually the following is required:	12.8 If the audited entity shares cardholder data with another company, obtain and examine contracts between the organization and any third parties that handle cardholder data (for example,			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes). Perform the following:			
12.8.1 Service providers must adhere to the PCI DSS requirements	12.8.1 Verify that the contract contains provisions requiring adherence to the PCI DSS requirements	N/A – Third party contracts		Responsibility of merchant / service provider.
12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses	12.8.2 Verify that the contract contains provisions for acknowledgement by the third party of their responsibility for securing cardholder data	N/A – Third party contracts		Responsibility of merchant / service provider.
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.9 Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)	12.9.1 Verify that the Incident Response Plan and related procedures include <ul style="list-style-type: none"> • roles, responsibilities, and communication strategies in the event of a compromise • coverage and responses for all critical system components • notification, at a minimum, of credit card associations and acquirers • strategy for business continuity post compromise • reference or inclusion of incident response procedures from card associations • analysis of legal requirements for 	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	reporting compromises (for example, per California bill 1386, notification of affected consumers is a requirement in the event of an actual or suspected compromise, for any business with California residents in their database)			
12.9.2 Test the plan at least annually	12.9.2 Verify that the plan is tested at least annually	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts	12.9.3 Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.
12.9.4 Provide appropriate training to staff with security breach response responsibilities	12.9.4 Verify through observation and review of policies that staff with security breach responsibilities are periodically trained	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	12.9.5 Verify through observation and review of processes that monitoring and responding to alerts from security systems are included in the Incident Response Plan	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	12.9.6 Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	N/A – Incident Response policy and procedures		Responsibility of merchant / service provider.
12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following	12.10 Verify through observation, review of policies and procedures, and review of supporting documentation that there is a process to manage connected entities by performing the following:	N/A – Incident Response policy and procedures		Responsibility of processor / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
12.10.1 Maintain list of connected entities	12.10.1 Verify that a list of connected entities is maintained	N/A – Incident Response policy and procedures		Responsibility of processor / service provider.
12.10.2 Ensure proper due diligence is conducted prior to connecting an entity	12.10.2 Verify that procedures ensure that proper due diligence is conducted prior to connecting an entity	N/A – Incident Response policy and procedures		Responsibility of processor / service provider.
12.10.3 Ensure the entity is PCI DSS compliant	12.10.3 Verify that procedures ensure that the entity is PCI DSS compliant	N/A – Incident Response policy and procedures		Responsibility of processor / service provider.
12.10.4 Connect and disconnect entities by following an established process	12.10.4 Verify that connecting and disconnecting entities occurs following an established process	N/A – Incident Response policy and procedures		Responsibility of processor / service provider.



GLOSSARY

A

AAA	Authentication, Authorization, and Accounting
ACE	Application Control Engine
ACS	Cisco Access Control Server.
AES	Advanced Encryption Standard.
AP	Access point.
ASA	Adaptive Security Appliance

B

BSSID	Basic Service Set Identifier
--------------	------------------------------

C

CS-ACS	Cisco Secure Access Control Server
C-LMS	CiscoWorks LAN Management System
CS-M	Cisco Security Manager
CS-MARS	Cisco Security Monitoring, Analysis, and Response System
C-NCM	CiscoWorks Network Compliance Manager
CSA	Cisco Security Agent.
ASDM	Adaptive Security Device Manager

D

DFM	Device Fault Manager
------------	----------------------

DHCP Dynamic Host Configuration Protocol

DoS Denial of service.

E

EIGRP Enhanced Interior Gateway Routing Protocol.

F

FWSM Firewall Services Module.

H

HSRP Hot-Standby Routing Protocol

I

ICMP Internet Control Message Protocol

IDS Intrusion Detection System Services Module 2

IDSM2 Intrusion detection system. Intrusion Detection System Services Module 2 (IDSM2)

IPS Intrusion prevention system.

IRN Intelligent Retail Network

ISR Integrated Services Router

L

LAP LWAPP Access Point.

LBS	Location-based service
LWAPP	Lightweight Access Point Protocol

N

NCR-ACS	NCR Advanced Checkout Solution
NAT	Network Address Translation
NTP	Network Time Protocol

O

OSPF	Open Shortest Path First
-------------	--------------------------

P

PAT	Port Address Translation
PCI	Payment Card Industry
POS	Point of Sale

Q

QSA	Qualified Security Assessor
------------	-----------------------------

R

ROC	Report on Compliance
REAP	Remote-Edge Access Point

S

- SLL** Secure Socket Layer
- SNMP** Simple Network Management Protocol
- SNR** Signal-to-noise ratio.
- SOA** Service-Oriented Architecture.
- SONA** Service-Oriented Network Architecture.
- SSH** Secure Shell
- SSID** Service Set Identifier

T

- TLS** Transport Layer Security

W

- WCS** Wireless Control System

- Wi-Fi** Wi-Fi is the brand of the Wi-Fi Alliance, which certifies interoperability of products and services based on IEEE 802.11 technology.
- WPA** Wi-Fi Protected Access