



Cisco PCI Solution for Retail 2.0 設計および実装 ガイド

March 19, 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

重要！

この設計および実装ガイドの内容は、「現状のまま」として提供されます。明示的であれ黙示的であれ商品性及び、特定の目的への適合性などについての保証、または一連の取引、使用法、または商習慣などに起因する著作権非侵害の保証を含む、いかなる保証または表明も行いません。

PCI への準拠を実現するには、トレーニング、サービス、ポリシー、その他シスコの管理外のさまざまな要素が必要です。また、サードパーティによる製品やサービスも必要になることがあります。このガイドは、すべての顧客の PCI 準拠の実現を保証するものではありません。

このデザインと実装ガイドは、シスコ、その代理店、またはパートナーの技術的またはその他の専門的アドバイスによるものではありません。デザインを実装する前に、ユーザ企業の技術アドバイザに相談する必要があります。結果はシスコでテストしていない要因によって異なる場合があります。

詳細については、PCI QUALIFIED SECURITY ASSESSOR (QSA) にお問い合わせください。QSA の一覧、および PCI データセキュリティ標準に関する詳細については、次の URL にアクセスください。

HTTP://WWW.PCISECURITYSTANDARD.ORG OR VISIT CISCO RETAIL AT WWW.CISCO.COM/GO/RETAIL

このマニュアルに記載されている設計、仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

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, 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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)



はじめに

Cisco PCI Solution for Retail を構成するシスコの各ネットワーク製品を検証するため、Cisco Intelligent Retail (IRN) を使用して実験環境が構築されました。査定は、Payment Card Industry (PCI) Qualified Security Assessor (QSA) が行いました。初期の製品範囲（ソリューション開発チームによって指定されたルータ、スイッチ、ワイヤレス、関連管理ツール）は、PCI データ セキュリティ仕様バージョン 1.1 の各要件への準拠を目的として決定され、QSA 監査企業の検証を受け合格しました。

本ガイドの目的

このガイドでは、PCI 要件に準拠するために必要な設計と構成の詳細について説明し、Cisco IRN 設計原理の基盤を提供します。このガイドは、<http://www.cisco.com/go/srnd> で公開されている『Cisco Enterprise Branch Security Design Guide』の内容を補足するもので、置換するものではありません。

対象読者

このガイドは、対象読者として、PCI DSS 1.1 の各要件に準拠する小売店舗ネットワークの構築を担当するシスコ システム エンジニア、ソリューション エンジニア、パートナー エンジニアを想定しています。

Cisco PCI Solution for Retail の概要

Cisco PCI Solution for Retail は、『PCI 1.1 Data Security Standards』に記載されている多数の要件を満たす総合的なソリューションを実現するために連携動作する多数のシスコ製コンポーネントで構成されます。このソリューションは、小売業者が、PCI 監査に含まれる多くの要素にスムーズに対応できるように最適化された構成を提供します。

各ソリューション コンポーネントは、Cisco Secure Access Control System (CS-ACS) を介して Active Directory によって認証されます。ただし、4 つのサーバは例外です。このソリューションでは、各サーバをファイアウォールの背後にある自身のネットワーク セグメントに設置するという補完コントロールを実装することにより、この例外に対応しました。

シスコでは、小売業者による PCI 監査プロセスの簡素化に引き続き重点を置いています。具体的には、製品ラインに機能を追加して、次の補完コントロールを使用せずに済むようにします。

- ワイヤレス コントロール システム (WCS) — リリース 4.1 で、TACACS+ および RADIUS を追加しました。

- Cisco Security Monitoring, Analysis, and Response System (CS-MARS) — バージョン 4.3 で、RADIUS 認証を追加しました。
- Cisco Security Access Control System (ACS) — RADIUS 認証を追加する予定です。この機能は、2008 年 3 月より使用可能になる予定です。
- Cisco Security Agent Manager Server — このサーバは外部から直接 Active Directory の認証を受けることができるため、補完コントロールを必要としませんでした。



CHAPTER 1

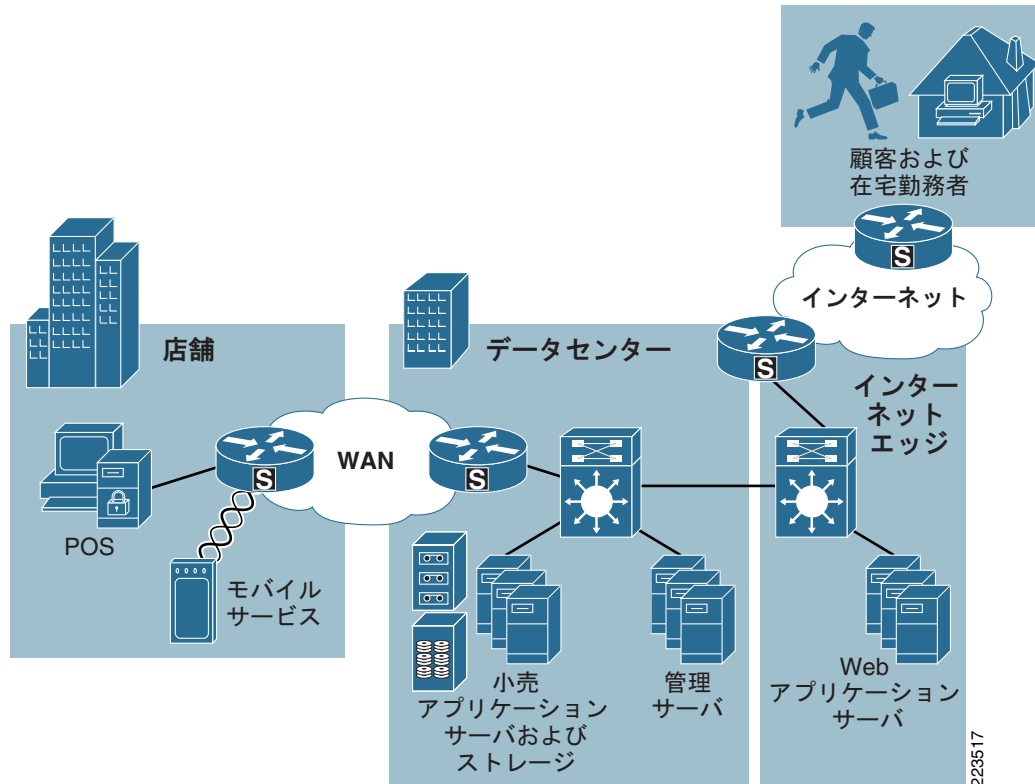
ソリューションの概要

要約

Cisco PCI Solution for Retail は、有線および無線ネットワークにおいて、静止中のデータおよび移動中のデータに適用される設定や推奨事項を規定したものです。このソリューションは、Payment Card Industry (PCI) Data Security Specification (DSS) 1.1 に準拠して設計されています。このソリューションは、Point-of-Sale (POS; 販売時点管理) システム、支払い装置、無線クライアント装置、データ暗号化ソフトウェア、シスコ ネットワーク インフラストラクチャを使用して構築およびテストされており、PCI Qualified Security Assessor (QSA) 監査パートナーによって検証済みです。このソリューションを導入することによって、ブランチ小売店舗、データセンター、インターネット エッジ デザインの集合が形成され、小売業を PCI に準拠させるプロセスが簡素化されます。

PCI 準拠の査定に合格するには、小売業者が、PCI v1.1 の各要件に適合していることを示すことができるように、自社の業務手順、セキュリティ ポリシー、技術基盤を整備する必要があります。QSA は、企業に対して監査を実行して、各該当要件が満たされているか、あるいはその企業には適用されない要件なのかを確認する必要があります。PCI に準拠していると承認されたあとも、企業は、その準拠状態を継続的に維持する必要があります。Cisco PCI Solution for Retail では、インフラストラクチャの構築、静止 / 移動中データの保護方法、設定の監視および維持方法を示します。図 1-1 に、Cisco PCI Solution for Retail アーキテクチャの概念図を示します。

図 1-1 Cisco PCI Solution for Retail 2.0 のアーキテクチャの概念図



ソリューションが必要な理由

PCI DSS バージョン 1.1 の規定は、ネットワーク経由で、クレジットカードまたはデビットカード情報を処理、格納、転送するすべての小売業者に適用されます。シスコのお客様は、QSA 監査ガイドラインを満たすような小売ネットワークの設計、管理、モニタリングを行う方法について、総合的な推奨事項の提示を求めています。

対象市場

支払いトランザクションを処理する小売業者は、PCI DSS ガイドラインの要件を満たす必要があります。典型的な中堅小売業者は、年間の支払いカードトランザクションの処理件数が 10 万件を超えるため、本ソリューションの対象市場に含まれます。本ソリューションは、小売店舗ネットワーク、データセンター、インターネットエッジインフラストラクチャをモデル化することにより、多種多様な小売業に対応できます。表 1-1 に、PCI で規定されている小売業レベルを示します（出典 Visa USA）。

表 1-1 PCI 規定の小売業レベル

小売業レベル	説明
1	- 受注経路を問わず、年間の VISA トランザクション処理件数が 600 万件を超える小売業者。 - ネットワーク上でのハッキングや攻撃による顧客情報の流出被害を被っている小売業者。 - VISA のシステムに対するリスクを最小化するため、レベル 1 の小売業要件を満たす必要があると VISA が独自に判断した小売業者。 - VISA 以外のカード会社によってレベル 1 であると特定された小売業者。
2	受注経路を問わず、年間の VISA トランザクション処理件数が 100 万～600 万件の小売業者。
3	e- コマースによる年間の VISA トランザクション処理件数が、2 万～100 万件の小売業者。
4	e- コマースによる年間の VISA トランザクション処理件数が 2 万件未満の小売業者。また、受注経路を問わず、年間の VISA トランザクション処理件数が 100 万件までの、その他すべての小売業者。

本ソリューションがサポートするアプリケーションとサービス

Cisco PCI Solution for Retail によってサポートされている主要なアプリケーションは次のとおりです。

- 有線および無線ネットワークを介して支払いカード情報を高度にセキュリティ保護された状態で転送
- 電子キャッシュ レジスタ、店舗内サーバ、またはデータセンターの静止中データを高度にセキュリティ保護された状態で保管
- ネットワークおよびシステムの管理、モニタリング、改善サービス

ソリューションの利点

本ソリューションは、PCI DSS 1.1 のガイドラインに準拠した小売業ネットワークを構築する方法を示すものです。顧客は、推奨された構成とベスト プラクティスを用いて同じネットワークを構築することによって、PCI 準拠を実現するプロセスを簡素化できます。

他にも、次のような利点があります。

- グローバルなベストプラクティスに基づく Cisco Intelligent Retail Network アーキテクチャに対する正しくかつ詳細な理解
- PCI 準拠を実現するためのプロセス中に利用できるスケーラブルな参照デザインのセット
- シスコ、およびパートナー コンポーネントと各パートナーの PCI DSS 要件との関連性の詳細な分析とマッピング
- 小売業ネットワークとデータ システムを強化するための管理方法とベストプラクティスの正確かつ詳細な理解
- 分散したエンドポイントを個別に管理するよりも高い運用効率を実現する集中管理方式のための「ツールキット」

- ・ 実験的なモデルとそれに対応する Verizon Business (QSA) からの Report on Compliance (ROC; 準拠性レポート) が提供されるため、PCI 監査プロセスの正確かつ詳細な理解が可能

ソリューションの機能と主要なコンポーネント

本ソリューションは、以下の各機能とコンポーネントで構成されます。

- ・ ネットワーク システム
- ・ ホストとサーバ
- ・ 監視と管理
- ・ 暗号化
- ・ 認証
- ・ ポリシー
- ・ その他のアプリケーションとサービス

ネットワーク システム

- ・ ルーティング — Cisco Integrated Services Router (ISR; サービス統合型ルータ)、中規模ルータ、および Catalyst 6500 スーパーバイザによって、アーキテクチャ全体のルーティング サービスを提供します。各小売店舗では、1 台または 2 台の ISR を設置して、WAN サービス、ルーティング、アイデンティティ管理、セキュリティ サービスを単一のプラットフォームに統合し、各店舗および中央の管理サービスを提供します。同じプラットフォームが、ネットワークの Quality of Service (QoS; サービス品質)、ボイス コール制御、その他のアプリケーション サービスのハブとしても機能します。WAN 集約ルータおよびインターネット エッジルータには Cisco 7206VXR ルータを使用します。これにより、広範な WAN インターフェイスがサポートされ、特定のタイプのトラフィックだけがデータセンターに入ることを許可されます。
- ・ スイッチング — Cisco Catalyst イーサネット スイッチによって、IP エンドポイントを経路選択された各サービスに接続します。Catalyst スイッチは、10 Mbps ~ 10 Gbps のスイッチング速度を実現します。また、Power over Ethernet (PoE) サービスを組み込むことにより、同じケーブルで、無線アクセス ポイント、IP 電話、その他の 802.3AF ベースのデバイスに電源を供給することもできます。Catalyst スイッチは、VLAN、アクセス コントロール、QoS を使用して、セキュリティ要件やビジネス要件に基づき LAN トラフィックを振り分けます。
- ・ 無線 — Cisco Unified Wireless ネットワークによって、モバイル コンピュータおよび携帯電話に対する無線接続の一元管理を実現します。この無線インフラストラクチャには、統合型無線侵入検知、高度なセキュア接続、Wireless Control System (WCS; ワイヤレス制御システム) による集中管理機能も含まれています。各小売店舗ネットワークは、店舗の規模に関係なく、同じデュアル無線インフラストラクチャ設計を共有します。これにより、モバイル型キオスクへのストリーミングやデジタル署名など、高帯域小売業アプリケーション向けに十分なネットワーク容量を確保できます。また、パスの分離および分割によって、支払いデータが、他のタイプの小売ビジネス データとは別に確実に暗号化されます。Unified Wireless ネットワークは、ローカル管理型の分散アクセス ポイントとして、または集中管理型のワイヤレス制御システムとして運用可能です。

本ソリューションで使用する Cisco Unified Wireless ネットワーク システムの構成要素は次のとおりです。

- Cisco 1100 シリーズおよび 1200 シリーズのアクセス ポイントにより、2.4 GHz および 5 GHz の 802.11 ネットワーク接続、高度なセキュリティ サービス、集中型管理制御を同時にサポートします。

- Cisco Unified Wireless Controller には、ISR プラットフォーム向けのワイヤレス LAN コントロール モジュール、および大規模店舗で使用されている 4000 シリーズ コントローラがあります。小規模店舗では、集中型コントローラ モジュールによる Hybrid-Remote-Edge-Access-Point (H-REAP) プロトコルを実装します。この設計により、店舗と中央のコントローラとの接続が失われたとき、店舗側でのローカル認証が可能になります。
- サービスの集約
 - Cisco Catalyst 6500 は、高いパフォーマンスとスケーラビリティおよび可用性を備えたプラットフォームによって、店舗-WAN ルータからコア スイッチを経由してサーバ アクセス レイヤまで、支払いトラフィックを転送します。
 - Firewall Services Modules (FWSM; ファイアウォール サービス モジュール) を使用して、中央のポリシーに基づき、トラフィックを許可または拒否します。
 - Intrusion Detection Module 2 (IDS2; 侵入検知モジュール 2) を使用して、中央の管理システムから送信されたポリシーを監視および実施します。Cisco Application Control Engine によって、コンテンツをフィルタリングし、中央のポリシーに基づいてトラフィック負荷を分散します。
 - Cisco Unified Wireless アーキテクチャの一部であるワイヤレス コントローラは、ネットワーク全体にインストールされたワイヤレス インフラストラクチャを集中的に制御および管理します。
 - これらのシステムは協調動作して、中央のポリシーに基づき、支払いトランザクション ログと POS トランザクション ログのトラフィックを分離します。
 - Cisco 適応型セキュリティ アプライアンスを使用して、ファイアウォール、IDS、VPN の各サービスを実現することもできます。
- ストレージ — 電子キャッシュ レジスタ、POS サーバ、その他の PC を使用して、典型的な小売環境を再構築します。EMC 製ストレージディスクに接続された SAN ダイレクタ クラス スイッチによって、典型的なデータセンター ストレージ環境を構築します。インターネット エッジ内部に接続された他のサーバとホストは、Web アプリケーション サーバをシミュレートします。

ホストとサーバ

- POS — NCR 製 POS 端末と NCR Advanced Checkout System ソフトウェアが稼働する SurePOS サーバを使用して、典型的な小売環境を構築します。旧バージョンでは、IBM および Wincor-Nixdorf 製 POS 端末を使用していました。これらのデバイスは、RSA データ セキュリティ アプリケーションと連係して、システム上の重要な支払いデータや管理データに対するアクセスを暗号化します。CSA は、アプリケーション ファイアウォール、ファイル整合性、ホスト侵入防御サービスを実現します。各デバイス内で小売業ビジネス アプリケーションの機能を個別に許可し、小売店舗レベルで、アンチウイルス ソフトウェアに対する要件を大幅に限定するように構成できます。たとえば、「デイゼロ」攻撃を防いだり、キャッシュ レジスタ、デスクトップ、キオスク、サーバの各レベルで、小売ビジネス コンピューティングの広範な要件を満たすようにカスタマイズしたりできます。
- 支払い用デバイス — VeriFone および IBM 製の支払い用デバイスを使用して、小売業支払い環境をシミュレートします。これらのデバイスを本ソリューションで使用するには、PCI 支払い暗号化デバイス仕様の要件を満たしている必要があります。
- ホストおよびサーバのセキュリティ — CSA は、店舗に設置された、(支払い用デバイス、POS レジスタ、POS サーバなど) Windows または Linux ベースの POS デバイス上にインストールされたソフトウェアの組み合わせです。CSA は、データセンター内の各ソリューション管理サーバ上にもインストールされます。また、店舗の管理用 PC や、小売企業に設置されたその他のデスクトップやサーバにもインストールできます。

- 集中型シスコ管理サービスは、分散システムのすべての要素について、管理、監視、プロビジョニング、分析、改善、レポート作成を実行します。これらのサービスには、監査および裁判用のレポートを作成する機能もあります。

監視と管理

本ソリューションで使用するシスコ管理アプリケーションスイートは次のとおりです。

- Cisco Security Manager (CS-M)** — 各 ISR ルータとセキュリティ アプライアンスに分散されたセキュリティ サービスのための運用管理プラットフォーム。小売店舗ネットワーク全体における、ファイアウォール、IDS/IPS、および VPN サービスの設計、プロビジョニング、レポートの作成を行います。
- Cisco Security Monitoring, Analysis and Response System (CS-MARS)** — 大規模、中規模、小規模の小売業環境、およびデータセンター環境におけるシスコ ネットワーク デバイスセキュリティ警告（例：ASA/FWSM/ISR ファイアウォール ログや IDS/IPS 警告）用の集中型ログ モニタリング、相互関係、レポート作成プラットフォーム。Cisco Security Agent の警告も CS-MARS に転送されます。
- Cisco Security Agent Management Center (CSAMC)** — 各小売店舗ネットワークに設置された POS や店舗運用装置にインストールする CSA ソフトウェアの一元管理、プロビジョニング、レポート作成システム。
- Wireless Control System (WCS)** — 各小売店舗ネットワークにインストールされた Unified Wireless ネットワーク インフラストラクチャおよびサービスを一元管理します。
- CiscoWorks LAN Management System (C-LMS)** — 広範なシスコ ネットワーク デバイスから実行/スタートアップ コンフィギュレーションを集中的に制御および収集します。C-LMS は、Cisco Discovery Protocol (CDP; シスコ検出プロトコル)、SNMPv3、およびその他の管理プロトコルを使用して、データセンターから小売店舗ネットワークへの安全な通信を実現します。
- CiscoWorks Network Compliance Manager (C-NCM)** — ネットワーク インフラストラクチャ全体におけるコンフィギュレーションとソフトウェアの変更を追跡および管理します。IT により、ネットワークの変更を詳細に把握し、PCI ガイドラインと企業のポリシーに準拠しているかどうかを追跡できます。

暗号化

PCI ガイドラインに準拠するには、2 つのタイプの暗号化、すなわち静止中データの暗号化と移動中データの暗号化を使用します。

静止中データの暗号化

- RSA File Security Manager** — 店舗またはデータセンターにおける機密データの暗号化に使用されるファイル レベルの暗号化システム。
- RSA Key Manager** — エンタープライズ環境全体における暗号化鍵の安全な配信と使用を管理するためのエンタープライズクラスの鍵管理システム。
- RSA enVision** — 以下に示す認証コンポーネントの一部である RSA SecurID トークンを管理するためのログ管理 / 分析用アプリケーション。

移動中データの暗号化

- Cisco Virtual Private Network (VPN; バーチャル プライベート ネットワーク)** ソフトウェア — パブリック ネットワーク セグメント上を送信される支払いデータを暗号化します。VPN では通常、3DES (triple DES) または 256 ビット AES 暗号方式による IPSec を使用します。

- Secure Socket Layer (SSL) サービス — インターネット ベースの Web アプリケーションからのトラフィック、およびインフラストラクチャ デバイスをリモート管理するトラフィック (SSHv2) を暗号化します。
- Wi-Fi Protected Access バージョン 2 (WPA2) — ワイヤレス クライアントとシスコ アクセス ポイント間に使用します。店舗内ワイヤレス LAN (WLAN) を越えて転送される POS および支払いデータを AES で暗号化します。

認証

Accounting, Authorization and Authentication (AAA; アカウンティング、許可、認証) サービスを使用して、アイデンティティの確認、およびコンポーネント内のシステム、デバイス、サービスに対するアクセスの許可を行います。認証の主要構成要素は次のとおりです。

- Cisco Secure Access Control Server (CS-ACS) — インフラストラクチャの中央の AAA サービスブローカとソリューションのリモート アクセス要素では、CS-ACS を使用して、ネットワーク デバイスおよびネットワーク上で動作するサービスに対する運用アクセス ポリシーの管理と制御を実施します。CS-ACS は、ソリューションを構成するネットワーク、ホスト、サーバのアクセス制御を実現します。
- RSA Access Manager — ソリューションの RSA アプリケーションに必要なアクセス制御システム。
- RSA Authentication Manager ソフトウェア — RSA 認証エージェントと連係し、時刻同期ベースの RSA SecurID トークンによる強力な 2 ファクタ ユーザ認証を使用して、セキュリティを向上します。このソリューションは、小売アプリケーションまたはインターネット エッジへの VPN ベースの接続にアクセスするリモート ユーザには必須です。

ポリシー

このソリューションでは、ポリシーの管理とポリシーの作成の 2 つの視点からポリシーを把握します。

- Cisco Security Manager は、各 ISR ルータとセキュリティ アプライアンスに分散されたセキュリティ サービスのための運用管理プラットフォームです。小売店舗ネットワーク全体における、ファイアウォール、IDS/IPS、および VPN サービスの設計、プロビジョニング、レポートの作成を行います。
- Cisco Security Agent (CSA) でも、特定のファイル、フォルダ、サービスへのアクセスを制限することで、ホストおよびサーバ レベルのポリシーを実施できます。CSA の管理は CSA 管理コンソールから行います。CSA 管理コンソールは、中央ポリシーを保持しており、動作に基づいて脅威を抑止するアプローチによって、新規のデバイスを迅速かつ確実にベースライン要件を満たす状態に移行させます。

その他のアプリケーションとサービス

運用可能な環境を構築し、PCI 要件を満たすには、以下のアプリケーション サービスとパートナー製品が必要です。ただし、これらはソリューション全体の必須構成要素ではありません。

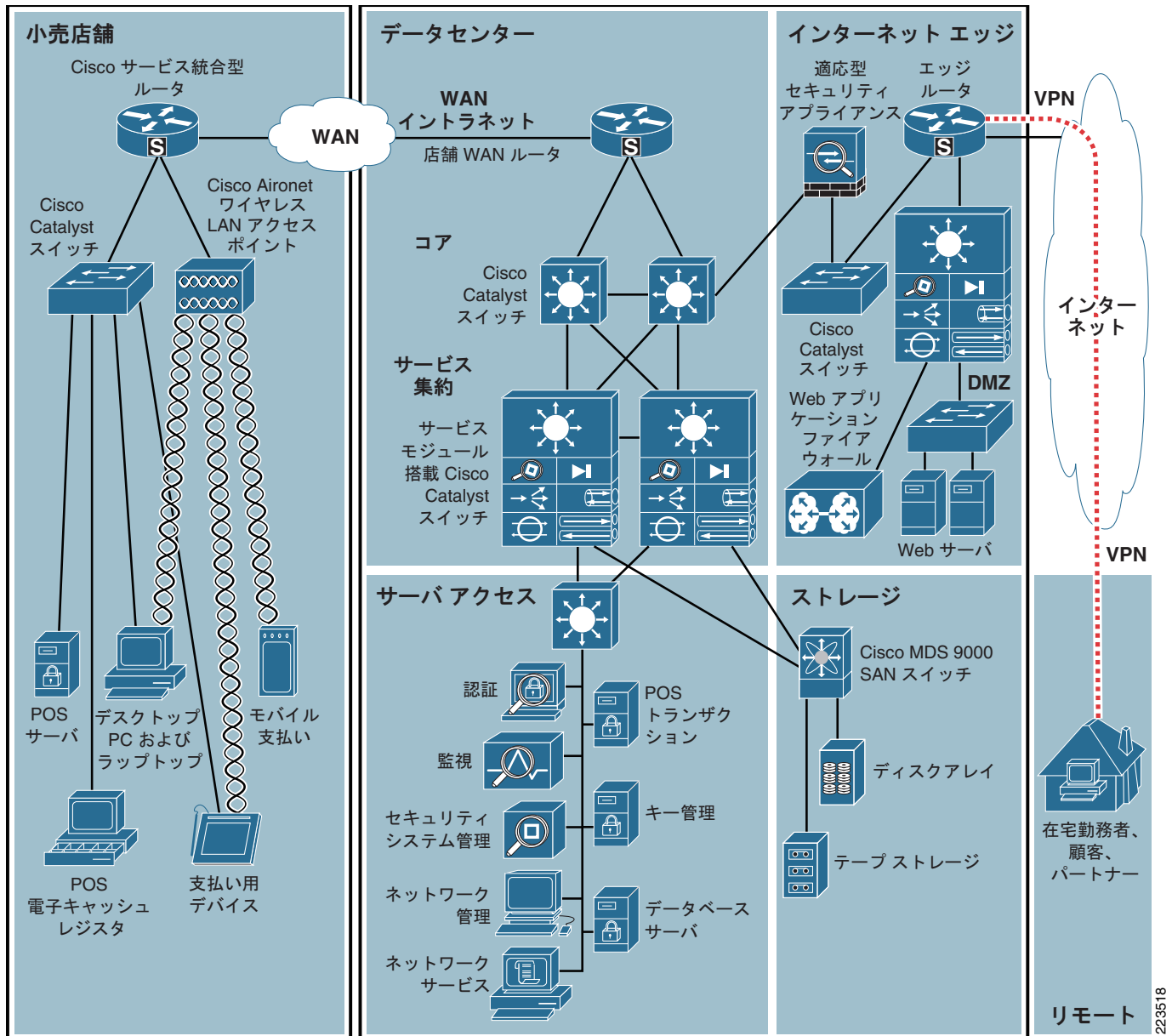
- Microsoft Active Directory
- Microsoft DNS/DHCP サーバ
- Microsoft Exchange サーバ (アラート通知サービス用)
- Microsoft Retail Management Server POS ソフトウェア
- Intermec ワイヤレス ハンドヘルドデバイス
- Network Time Protocol サーバ (中央時刻管理用)

- Wincor-Nixdorf POS ハードウェア
- IBM POS ハードウェア

これらのサービスおよび製品の詳細については、第4章「ソリューションの実装と設定」および付録を参照してください。

図 1-2 に、Cisco PCI Solution for Retail の概念図を示します。

図 1-2 Cisco PCI Solution for Retail — 概念図



ソリューションの範囲

アーキテクチャ

シスコとソリューションパートナーは、PCI 仕様に準拠するために使用可能な広範な製品ポートフォリオを用意しています。本ソリューション用に使用した各製品は、小売企業ネットワークとデータセキュリティ環境に直接関連しており、プロジェクトのスケジュール内に監査とラボでのテストが可能なもの、という基準で選択されました。

本ソリューションガイドには、WAN 経由で中央のデータセンターに接続する店舗参照設計が含まれています。また、インターネットベースのユーザをエクストラネットまたは De-Militarized Zone (DMZ; 非武装地帯) に転送する、インターネットエッジ参照設計も含まれています。本ソリューションでは、集中型管理を想定していますが、実際の小売支払いサービスまたは判定サービスへの集中接続は含まれていません。

Cisco PCI Solution for Retail の現リリースは、将来、製品やロケーション参照設計を追加するための基盤として利用できます。本ソリューションには次の項目が含まれます。

- プライベート WAN 経由で中央のデータセンターに接続する店舗参照設計
- 小売業の PCI 要件への準拠を容易にするデータセンター設計と集中管理サーバ
- インターネットベースの消費者、社員、パートナーをデータセンターまたは DMZ ベースのアプリケーションに接続する、インターネットエッジ設計

本ソリューションには次の項目は含まれません。

- データセンターから実際の支払いサービスプロバイダー、承継銀行、その他の商業サービスへの接続
- 実際の e- コマースを実現するアーキテクチャ、システム、アプリケーション

PCI 準拠

大半の PCI 標準（たとえば、PCI DSS 1.1, <https://www.pcisecuritystandards.org/index.htm> など）は、小売業者内部のポリシーと手順にフォーカスしたものです。しかし、PCI 標準の個々の要件は、技術的なインフラストラクチャとその構成を規定しています。Cisco PCI Solution for Retail は、PCI 準拠プロセスの技術インフラストラクチャ要件を満たすための、シスコ製ネットワーク機器、パートナー社製ソフトウェアアプリケーション、参照アーキテクチャ、およびコンフィギュレーションからなります。このソリューションはポリシーベースの下位要件に関連する指針も提供していますが、PCI 準拠の実現を目指す企業は、セキュリティサービスプロバイダーに、自社のセキュリティポリシーと業務手順の策定支援を依頼する必要があります。

本ソリューションで使用したシスコおよびパートナーの製品は、この一連のコンフィギュレーションの範囲内で PCI 仕様に完全に準拠しています。ただし、各製品の構成要素は本ソリューションとは異なる可能性があるため、PCI に対応するためにこれらの製品を購入する小売企業は、QSA に問い合わせ、自社の環境を確認する必要があります。

ソリューションの結果

以下の結果は、シスコのラボで作成および監査した特定のソリューションにのみ当てはまります。各ソリューションの機能と監査結果、および長所と短所に関する詳細については、[第 3 章「ソリューション コンポーネント — ベスト プラクティスおよび PCI」](#)を参照してください。個々

■ ソリューションの結果

の実装と設定の詳細については、[第4章「ソリューションの実装と設定」](#)を参照してください。
また、この実験について Verizon Business 社が作成した監査レポートについては、[付録F「Report on Compliance \(ROC\)」](#)を参照してください。

表 1-2 に、このソリューションの機能を PCI 要件に従って要約します。

表 1-2 Cisco PCI Solution for Retail が満たしている PCI 要件

ソリューションの機能	PCI 値
要件 1: カード所有者データを保護するためのファイアウォール構成を導入して維持する	
FWSM、Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス)	ネットワーク セキュリティ (ファイアウォール セグメンテーション/フィルタリング)、ステートフル フィルタリング
CiscoWorks (LMS と NCM)、C-SM	構成管理 / 安全性の高い構成
要件 2: システム パスワードおよびその他のセキュリティ パラメータに、ベンダー提供のデフォルト値を使用しない	
ISR、FWSM、ASA、スイッチ、ワイヤレス デバイス、WCS、CS-ACS、CiscoWorks (LMS と NCM)、Cisco Security Agent (CSA)、CS-M	ベンダーのデフォルトが変更された
WCS/ ワイヤレス コントローラ	ワイヤレス セキュリティ (WPA/WPA2、SSID ブロードキャストのディセーブル化)
ISR、FWSM、ASA、スイッチ、ワイヤレス コントローラ (CSA Manager、CS-M、CiscoWorks [LMS])	ベスト プラクティス セキュリティ パラメータのイネーブル化
ISR、FWSM、ASA、スイッチ、ワイヤレス コントローラ (CSA Manager、CS-M、CiscoWorks [LMS]、CS-MARS、CS-ACS、WCS)	非コンソール暗号化管理アクセス
要件 3: 保存されたカード所有者データを保護する	
NCR Advanced Checkout Solution (NCR-ACS) ソフトウェアと端末	PCI PIN 入力デバイス標準要件により認定
Verifone VX/MX 支払いデバイス	PCI PIN 入力デバイス標準要件により認定
RSA File Security Manager および Key Manager アプリケーション	POS デバイスおよびサーバ上に保存されたセキュアなデータへのアクセスを暗号化
要件 4: カード所有者データをオープンまたはパブリック ネットワーク経由で送信する場合は暗号化する	
ワイヤレス コントローラ	WPA ワイヤレス セキュリティ
ISRs、Cisco 7200VXR シリーズ ルータ、ASA	小売業者の WAN またはインターネット ベースのネットワーク回線越しにデータを取得する場合、IPSec VPN で暗号化
要件 5: アンチウイルス ソフトウェアまたはプログラムを導入し、定期的にアップデートする	
CSA	アンチウイルス保護、マルウェア / スパイウェア保護、アラート
要件 6: 安全性の高いシステムおよびアプリケーションを開発 / 保守する	
CiscoWorks (LMS と NCM)、C-SM (ワークフロー モード)	変更管理と準拠構成の実施
Cisco ACE XML Gateway	OWASP 攻撃からの Web アプリケーションの保護
要件 7: カード所有者データへのアクセスを業務上必要な範囲内に制限する	

表 1-2 Cisco PCI Solution for Retail が満たしている PCI 要件（続き）

ISR、Cisco 7200VXR、FWSM、ASA、スイッチ、ワイヤレスコントローラ、CSA Manager、CS-M、CiscoWorks (LMS)、CS-MARS、CS-ACS、WCS、RSA アプリケーション、NCR-ACS	最小特権、ロールベースのアクセス
要件 8：コンピュータにアクセスする利用者ごとに一意な ID を割り当てる	
ISR、Cisco 7200VXR、FWSM、ASA、スイッチ、ワイヤレスコントローラ、CSA Manager、CS-M、CiscoWorks (LMS)、CS-MARS、CS-ACS、WCS、RSA アプリケーション、NCR-ACS	一意なユーザ ID、認証済みアクセス、暗号化パスワード、グループ / 共有 ID / パスワードなし
ISR、Cisco 7200VXR、FWSM、ASA、スイッチ、ワイヤレスコントローラ、CSA Manager、CS-M、CiscoWorks (LMS)、CS-MARS、CS-ACS、WCS、RSA アプリケーション、NCR-ACS	パスワード強化要件
ISR、Cisco 7200VXR、FWSM、ASA、スイッチ、ワイヤレスコントローラ、CSA Manager、CS-M、CiscoWorks (LMS)、CS-MARS、CS-ACS、WCS、RSA アプリケーション、NCR-ACS	アカウント ロックアウト要件
要件 9：カード所有者データに対する物理的なアクセスを制限する	
今回は、この要件をテストまたは監査した製品はありません	注を参照 ¹
要件 10：ネットワーク リソースおよびカード所有者データに対するすべてのアクセスを追跡および監視する	
ISR、Cisco 7200VXR、スイッチ、ワイヤレスデバイス、WCS、CS-ACS、CiscoWorks (LMS) CSA、RSA アプリケーション、NCR アプリケーション	監査証跡、時刻同期
NCR-ACS 端末、RSA File Security Manager、RSA Key Manager、Cisco CSA	実際のカード所有者データと監査証跡データへの監査によるアクセス
CiscoWorks (LMS と NCM)	監査ログ レコードの集中アーカイブ
要件 11：セキュリティ システム / プロセスを定期的にテストする	
ワイヤレス コントローラ	不正ワイヤレス AP / デバイスの検出
ISR、ASA、IDSM2（センサー）、CS-M（ポリシー、シグニチャ更新）	ネットワーク IDS
CSA	ホスト ベース IDS
CSA	ファイル整合性
要件 12：社員と契約業者の情報セキュリティを実現するポリシーを維持する	
Verizon Business 社、Cisco Advanced Services	セキュリティ ポリシーの作成と保守

1. シスコ ビデオ偵察 / 監視システムを実装すればこの要件を満たすことができますが、それは今回のソリューション テストの範囲外です。



CHAPTER 2

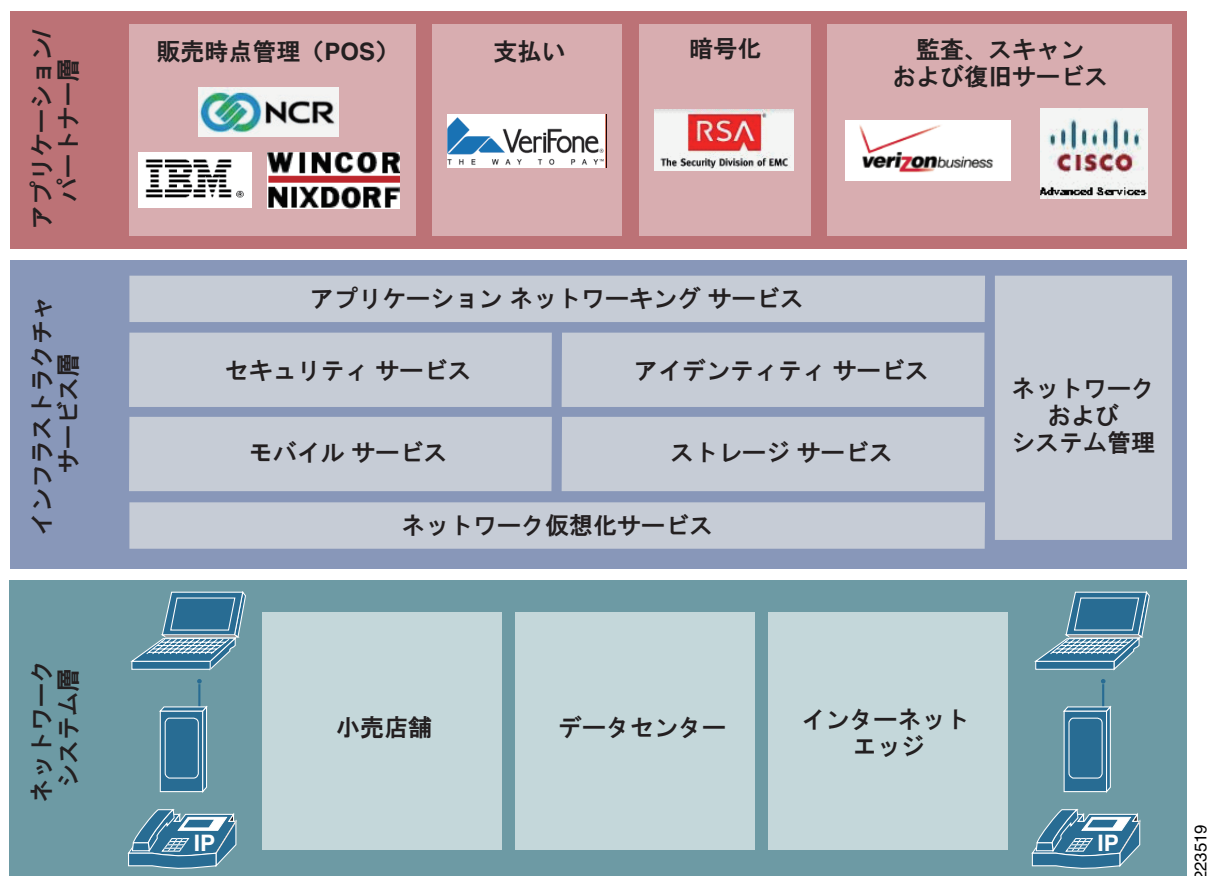
ソリューションアーキテクチャ

Cisco PCI Solution for Retail は、シスコの Intelligent Retail Network (IRN) を基盤としています。IRN は Service-Oriented Network Architecture (SONA; サービス指向型ネットワークアーキテクチャ) です。SONA と IRN の詳細については、次の URL を参照してください。

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

Cisco IRN 参照設計は、ネットワークシステム層の基盤となります。これらのネットワーク設計は、小規模、中規模、および大規模の小売店舗ネットワーク、ならびにデータセンターおよびインターネットネットワークのベストプラクティスを提示するものです (図 2-1 を参照)。

図 2-1 Cisco PCI Solution for Retail の SONA フレームワーク



アプリケーションとパートナー サービス

SONA フレームワークの最上位層には、Cisco PCI Solution for Retail の一部である 小売業向けアプリケーションおよびサービスがあります。具体的には、POS、支払い、暗号化の各アプリケーションです。これらのアプリケーションの一部は、J2EE、.NET、その他のシステムを基盤とする広く使用されているミドルウェア サービスを使用しています。IRN および共有ネットワーク サービス アプローチにより、これら各種の Service-Oriented Architecture (SOA; サービス指向型アーキテクチャ) 環境は、複数の小売業ネットワーク トポロジで同じインフラストラクチャ サービスを共有できます。アプリケーション層の右端にあるのは、小売業者が PCI プロセスの一部として使用する必要があるプロフェッショナル サービスです。年一回の監査、ネットワーク スキャン、および復旧サービスは、Cisco PCI Solution for Retail フレームワークの形成に必要な必須サービスです。

アプリケーション ネットワーキング サービス

アプリケーション サービスは、ビジネス アプリケーションからインフラストラクチャ サービス層の共有サービスへの接続を提供します。このサービスでは、フィルタリング、キャッシング、ロード バランシング、プロトコルの最適化の各処理をアプリケーションまたはアプリケーション ミドルウェアと連携して実行し、データ元からエンド ユーザまでのパフォーマンスを最適化します。

本ソリューションのアプリケーション配布サービスには、Cisco IOS ルータまたは Cisco Application Control Engine (ACE) が実行する、サーバのロード バランシングおよびコンテンツ フィルタリング機能が含まれています。

インフラストラクチャ サービス

セキュリティ、モバイル性、アイデンティティ、管理に共通のインフラストラクチャを使用すると、プロセス制御が簡素化されます。これらは、運用レポートの作成と PCI 準拠を実現するためのポリシー要件の策定において重要な利点となります。多数のインテリジェント デバイス間で多数のサービスを共有することによって、システム全体の運用効率が向上します。

- セキュリティ サービス**は、Cisco PCI Solution for Retail アーキテクチャで広く使用されています。セキュリティ サービスは、複数の物理デバイス間で共有されるセキュリティ機能、データセンターでの一元管理、小売業ネットワーク内の任意の場所からのセキュリティ制御プレーンに対する仮想アクセスを組み合わせたものです。
- ファイアウォール サービス**は、ISR、Firewall Service Module (FWSM; ファイアウォール サービス モジュール) および Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) で使用され、アプリケーションとインターフェイス サービスの両方のセキュリティを保護します。
- 侵入検知/侵入防止システム (IDS/IPS)** は、POS ホストおよびサーバレベルで動作する Cisco ISR、ASA、IDSM2、UWN、CSA で使用されます。これらのシステムの組み合わせは、データセンターのシスコ製管理アプリケーションによって一元管理されます。ここでも、システムの IDS/IPS 制御プレーンには、小売ネットワークのどこからでもアクセス可能です。
- データのモニタリング、分析、復旧**の関連付けは、データセンターで動作するイベント関連付けアプリケーションによって一元的に行われます。Cisco Security Monitoring, Analysis, and Response System (CS-MARS) は関連付けとモニタリングだけでなく、ネットワークに対する攻撃に対して、動的に、またはアラーム通知によって対処的に修復を行います。Cisco Works Network Compliance Manager (C-NCM) は、監視対象のデバイスに対して PCI ポリシーを実施できます。

- **モバイル サービス**は、本ソリューションにおけるもう1つの重要な領域です。小売業者は、モバイル型 POS や、ハンドヘルド コンピュータまたはモバイル型 POS キオスク上で動作する在庫管理アプリケーションのサポートを求めています。Cisco UWN では、単一のアクセスポイントから、一元管理された単一ドメインとしての数千のアクセスポイントに接続するシステムまで、広範なスケーラビリティのワイヤレス LAN (WLAN) システムをサポートします。小売店舗ネットワークでは、店舗が属するカテゴリの要件に応じて、さまざまな WLAN システムを使用します。
- **アイデンティティ サービス**は、認証および許可されたユーザが、小売ネットワークシステムにアクセスできるようにします。Cisco Secure Access Control Server (CS-ACS) は、アーキテクチャ全体の各ネットワークデバイス上に設定された RADIUS および TACACS+ システムを一元管理します。一元管理された LDAP ベースのディレクトリ サービスによって、CS-ACS は、PCI 要件への準拠を容易に実現できます。分散ネットワーク時刻サービスを使用することで、ネットワークおよびアプリケーションイベントが確実に同期化され、イベントの相関関係を強化できます。
- **管理システム**は、アーキテクチャ全体のすべてのデバイス、アプリケーション、サービスで使用されます。ネットワークシステムは、LAN Management System (C-LMS) (構成および管理要素) によって管理されます。Cisco Security Manager (CS-M) は、IT ネットワークシステム部から独立してセキュリティ対策をコントロールできるように、デバイスのセキュリティ要素を管理します。CiscoWorks Network Compliance Manager (C-NCM) は、C-LMS と連携して、PCI ガイドラインに準拠しているデバイスと、準拠していないデバイスについて、レポートを作成します。そして、ガイドラインに準拠していないデバイスについて、構成を復元し、ユーザが必須構成を実施できるようにします。

ワイヤレスシステムは、Cisco Wireless Control System (WCS) によって管理されます。WCS は、構成、管理要素、セキュリティサービスからなります。

本アーキテクチャでは、RSA データセキュリティアプリケーションは固有の管理ツールを使用しています。RSA ファイルセキュリティマネージャは、支払いデータが存在するホストおよびサーバ上におけるファイル暗号化サービスを管理します。また、RSA enVision を使用して、本ソリューションの RSA SecurID ベースの2ファクタ認証に関連するイベントを監視し、ログに記録します。

ネットワークシステム層

本ソリューションでは、アーキテクチャにネットワーク仮想化サービスが組み込まれています。たとえば、各店舗ネットワーク設計において、Cisco ISR は、セキュリティ、ルーティング、アイデンティティなどのサービスを仮想化します。これらのサービスは、レガシーの小売ネットワークアーキテクチャでは、多数の異なるネットワークアプライアンスによって実行されてきました。仮想化は、各店舗トポロジを構成する Cisco Unified Wireless システムの主要な機能でもあります。このシステムは、ワイヤレスインフラストラクチャを、アクセスポイントごとではなく、全体として一元的に管理します。このワイヤレスシステムは、集中管理システムからの入力に基づいて、自身を動的に調整および修復します。中央のネットワークおよびセキュリティ監視システムには、各店舗参照設計におけるネットワークシステムの統合グループからデータが供給されます。このようにエンタープライズ全体の仮想化では、イベントの相関関係を一元管理して予測的または適応的な対処を施すことによって、小売環境全体のセキュリティを高めることができます。

- **パスの分離**は、ネットワーク仮想化の主要コンポーネントです。Cisco PCI ソリューションでは、VLAN、複数の WLAN SSID ドメイン、および店舗とデータセンター間を集中管理するプライベートフレームリレーネットワークを使用して、POS およびネットワーク制御トラフィックを他のタイプのネットワークトラフィックから分離します。機密性の高いトラフィックを分離する技法は他にもあります。詳しくは、次の URL で公開されている『Enterprise Network Virtualization design guide (エンタープライズネットワーク仮想化設計ガイド)』を参照してください。

http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor7

- **サービス エッジ**とは、IRN インフラストラクチャ サービスが物理的なネットワーク インフラストラクチャに接続する場所です。サービス エッジでは、ファイアウォール、ポリシー実施、およびポリシー管理サービスが構築され、店舗 POS ドメイン、その他の店舗内 LAN ドメイン、およびリモート サービスへの WAN 接続の間で実行されるサービス アクセスを制御します。データセンターとインターネット エッジはそれぞれ、サービス エッジを使用して、統合型インフラストラクチャ サービスを集約し、この部分を通してすべてのトラフィックを制御します。

小売店舗ネットワーク設計

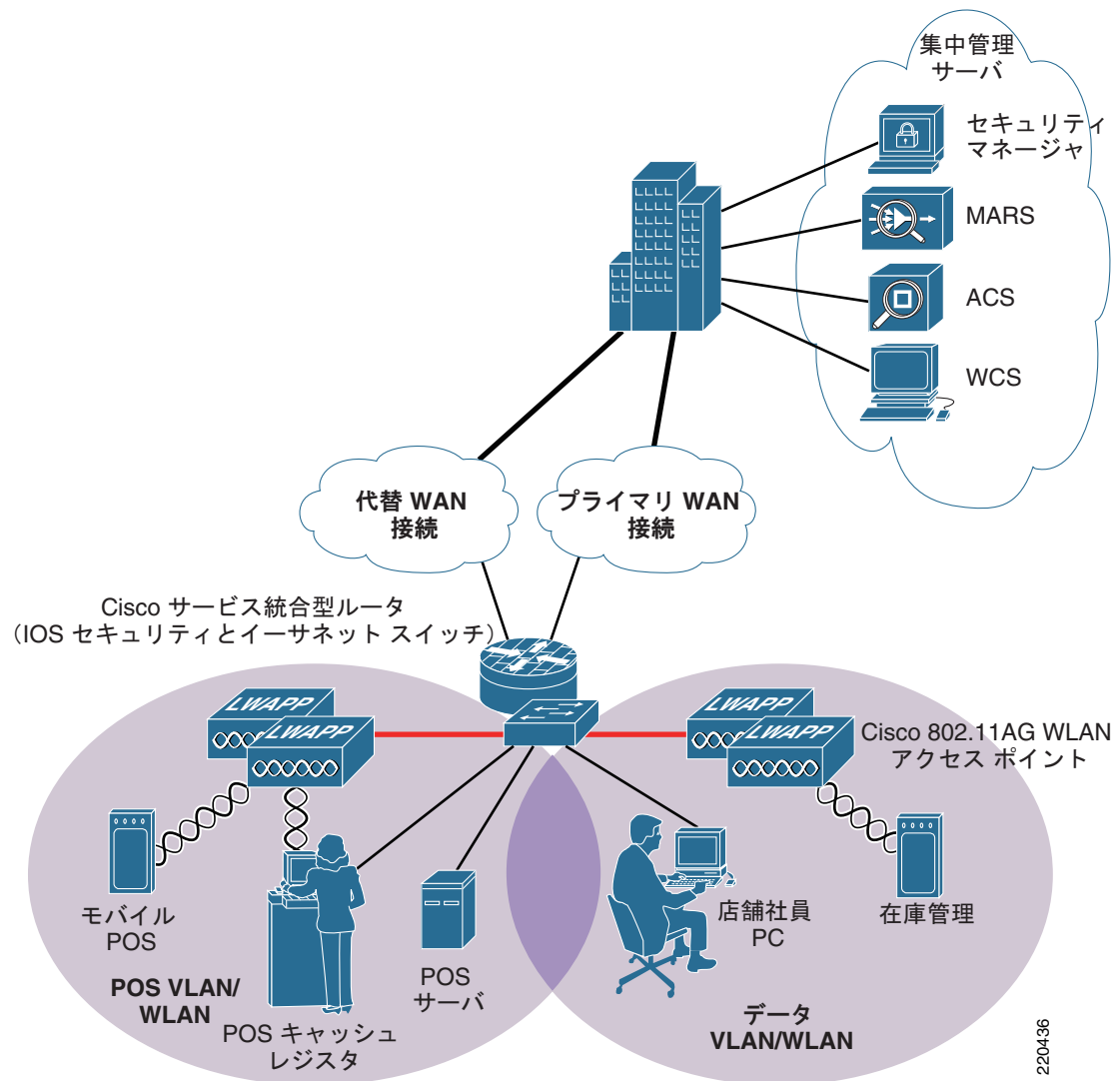
小規模店舗

小規模店舗ネットワークのシナリオでは、次の設計要件を満たす必要があります (図 2-2)。

主要な設計要件

- 店舗面積は平均で 2,000 ～ 6,000 平方フィートであること
- ネットワーク接続が必要な装置が 25 台未満であること
- 単一のルータと統合型イーサネット スイッチ
- 物理スペースが制約されているため、より少ないネットワーク コンポーネントによる統合型サービスが望ましい
- ワイヤレス接続環境

図 2-2 Cisco PCI Solution for Retail — 小規模店舗ネットワーク設計



概要と説明

小規模店舗の参照アーキテクチャは、シンプルで設置面積が小さい小売業を稼働するための強力なプラットフォームです。このアーキテクチャは、以下に示すさまざまな小売形態にも適しています。

- 商店街の小売店舗
- 簡易型レストラン
- コンビニエンスストア
- ガソリンスタンド
- 専門小売店
- シンプルなネットワーク構成を最優先するディスカウントショップ

このネットワークアーキテクチャは広く普及しており、多数のサービスを少数のインフラストラクチャコンポーネントに統合します。小規模店舗では、統合イーサネットスイッチが高速LANサービスをサポートしているため、さまざまな小売ビジネスアプリケーションモデルをサポー

トしています。また、統合コンテンツ エンジン、Web Cache Communications Protocol (WCCP) ベースのキャッシング、データの事前ポジショニング、ローカル メディア ストリーミング、その他のアプリケーション速度サービスなど、中央のアプリケーションの最適化要件を満たしています。

利点

- 店舗あたりのコストの軽減
- 予備パーツの削減
- 維持するソフトウェア イメージ数の削減
- 装置維持コストの軽減

制約

- ネットワーク復元力レベルの低下
- シングル ポイント障害による潜在的ダウンタイムの増加

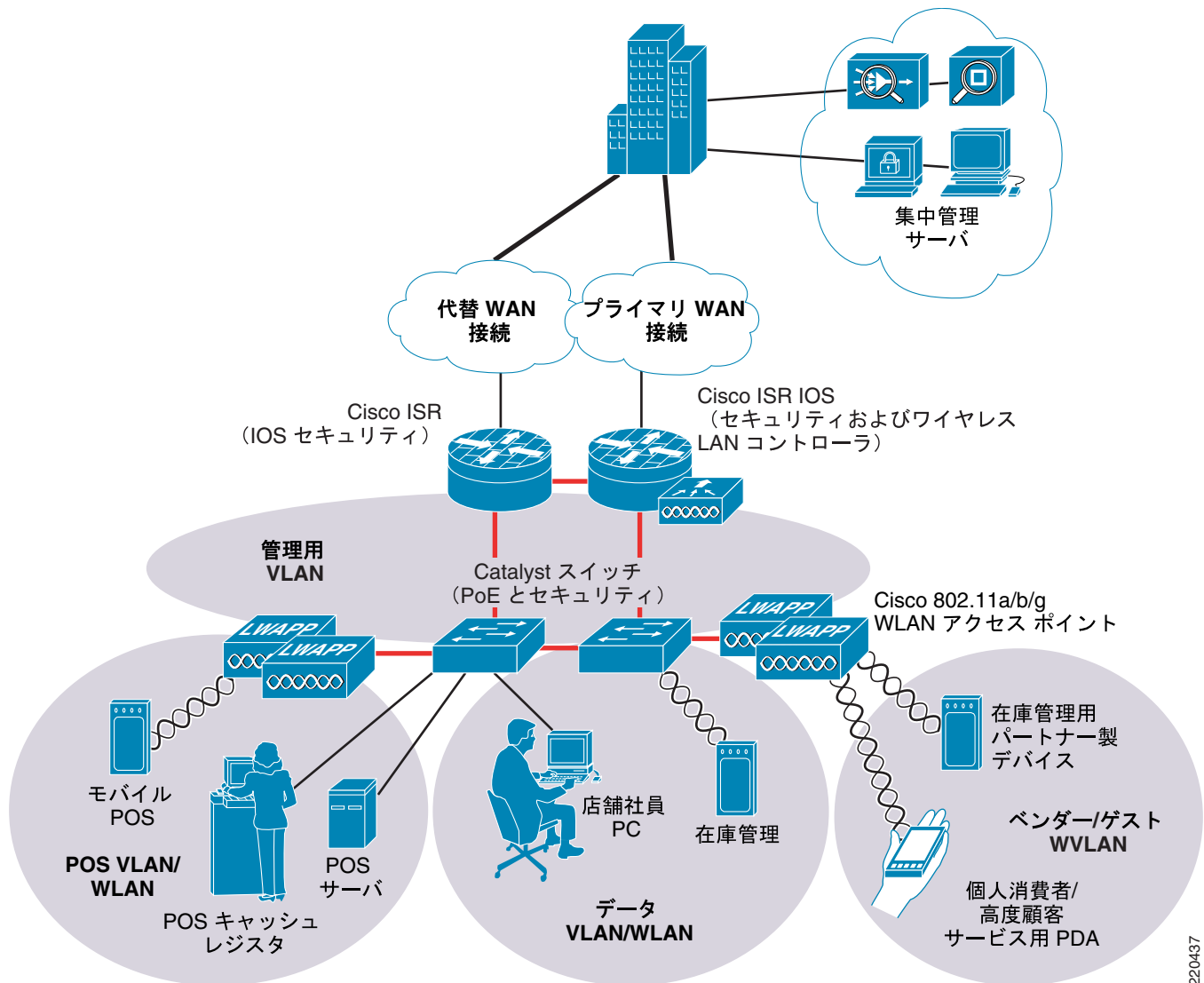
中規模店舗

中規模店舗ネットワークのシナリオでは、次の設計要件を満たす必要があります (図 2-3)。

主要な設計要件

- 店舗面積は平均で 6,000 ～ 18,000 平方フィートであること
- 店舗の物理サイズは大規模店舗よりも小さいため、ネットワーク スイッチのディストリビューション レイヤは不要
- ネットワークに接続する装置の数は平均で 25 ～ 100 台
- 冗長な LAN および WAN インフラストラクチャ
- ワイヤレス接続環境

図 2-3 Cisco PCI Solution for Retail — 中規模店舗ネットワーク設計



概要と説明

中規模小売店舗参照アーキテクチャは、ネットワーク復元力と、小規模店舗アーキテクチャとその単スレッドのシンプルなアプローチでは実現できない高いアプリケーション可用性を必要とする小売業者向けに設計されています。ミッションクリティカル性の高いアプリケーションとサービスが IP インフラストラクチャ上に集中するため、ネットワークのアップタイムとアプリケーション可用性がより重要になりますが、中規模店舗のデュアル ルータおよびデュアル LAN スイッチ設計により、そうした要件も満たされます。各 ISR ルータは、IOS セキュリティ サービスと店舗におけるその他の通信サービスを同時に実行できます。各 ISR ルータは専用の WAN 回線に接続されます。ネットワーク接続障害発生時に確実にネットワークを回復するために、Hot-Standby Routing Protocol (HSRP; ホットスタンバイルーティングプロトコル) を使用します。

ネットワークのアクセス レイヤでは、小規模店舗に比べて、より高い柔軟性とより多くのアクセス ポートを提供しています。店舗内にはワイヤレス アクセス ポイントを 12 個まで設置できます (WCS コントローラによってサポートされるため、コントローラを追加する必要はありません)。分散型 Cisco Catalyst スイッチは小規模店舗よりも大きなビルおよび多くのエンド ポイント数に対応できます。

利点

- より適応性の高いアクセス レイヤにより、多数のエンド ポイントとさまざまなビル要件（複数フロア、サブエリアなど）をサポート
- 並列デバイス設計による高いネットワーク復元力
- 並列パスによるネットワーク / アプリケーション可用性の向上

制約

- コア レイヤ (ISR) スイッチとアクセス レイヤ スイッチ間にディストリビューション レイヤが存在しない
- WCS が 1 台しかないため店舗内ワイヤレス ネットワークの復元力が低下する（このため、各店舗内の WCS コントローラで障害が発生したら、店舗 AP を中央の WCS コントローラにフォールバックさせるか、ローカルの WCS コントローラを 2 台設置することを推奨）

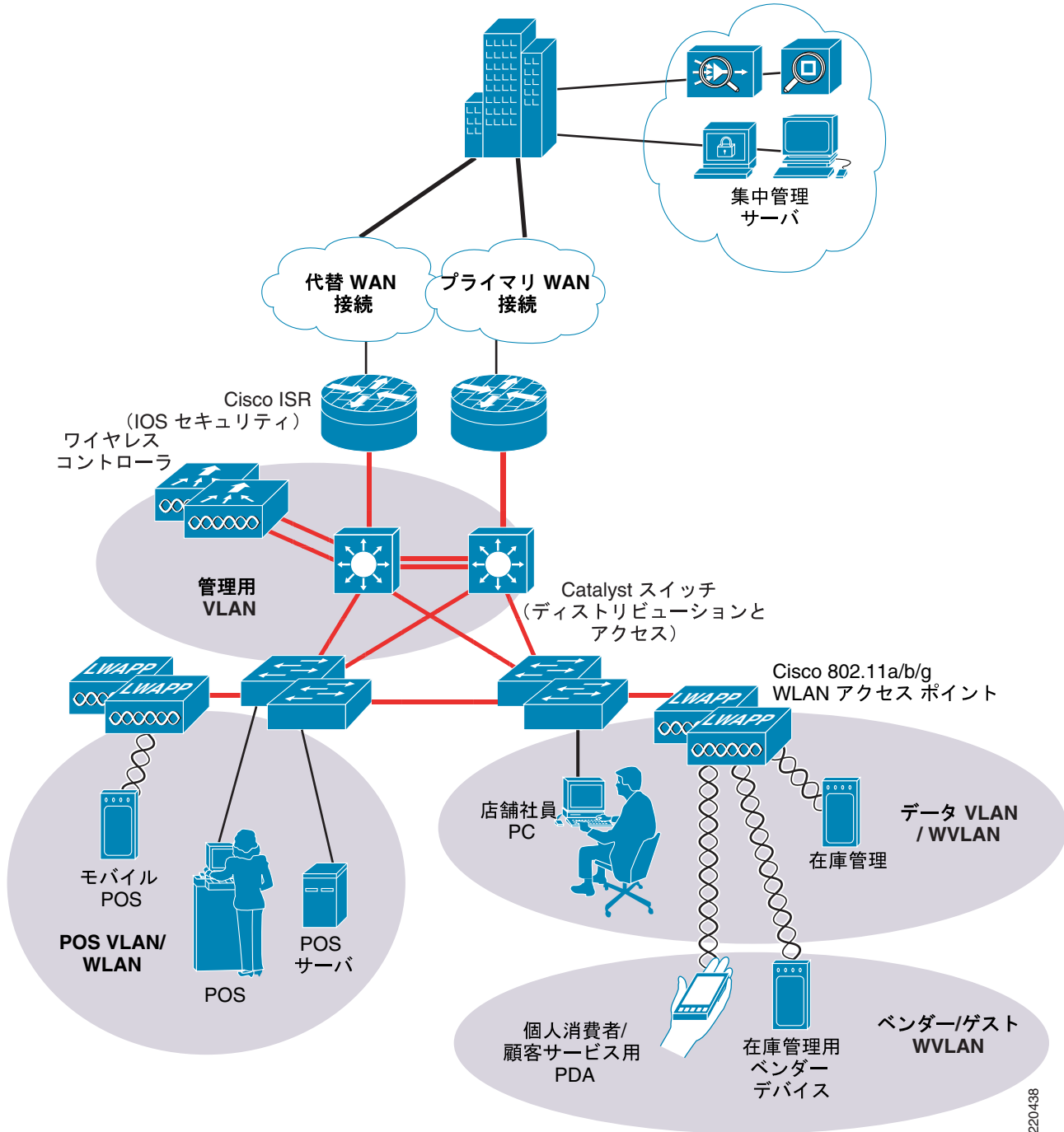
大規模店舗

大規模店舗ブランチ ネットワークのシナリオでは、次の設計要件を満たす必要があります (図 2-4)。

主要な設計要件

- 店舗面積は平均で 15,000 ～ 150,000 平方フィートであること
- 店舗あたり 100 台以上の装置がネットワークに接続する必要がある
- プライマリ / バックアップ ネットワーク用に複数のルータが必要
- 復元力およびアプリケーション可用性要件を満たすために、店舗内に分散されたネットワーク サービスを組み合わせることが望ましい
- 店舗内の階層型ネットワーク アーキテクチャ。中央のネットワーク サービス コアと、ネットワーク エンドポイント (POS、ワイヤレス AP、サーバ) を接続するアクセス レイヤ間にはディストリビューション レイヤ スイッチを使用

図 2-4 Cisco PCI Solution for Retail — 大規模店舗ネットワーク設計



概要と説明

大規模小売店舗参照アーキテクチャは、シスコ キャンパス ネットワーク アーキテクチャ推奨事項の一部の要素を取り入れ、それを大規模小売店舗環境に合わせて変更したものです。このアーキテクチャでは、ネットワーク トラフィックの（物理的かつ論理的な）分割方法をビジネス要件に合わせて改善できます。大規模店舗アーキテクチャのディストリビューション レイヤによって LAN のパフォーマンスが大幅に向上すると同時に、より高速な物理メディアによる接続（すなわち、光ファイバや銅ケーブルによる、リモートのアクセス レイヤ スイッチやワイヤレス アクセス ポイントへの接続）も提供できます。また、ビジネス要件に合わせて多数のエンドポイントを追加することもできます。このタイプのアーキテクチャは、世界中の大規模小売業者によって広く使用されています。デュアル ルータとディストリビューション レイヤ メディアの柔軟性によって、ネットワークの可用性が向上し、大規模小売店舗の要件に対応するスケーラビリティが実現されるため、ネットワークのサービスabilityが大幅に向上します。並列パス設計によって、定期的な保守およびアップグレードを、より高い頻度で、また通常の営業時間内に、スケジューリングし実行できます。

利点

- ・ 高可用性設計に基づく最高レベルのネットワーク復元性
- ・ 大規模小売店舗に対応したポート密度と光ファイバ密度
- ・ トラフィック分割度の向上
- ・ 大規模小売店舗における要件の変化に対応できるスケーラビリティ

制約

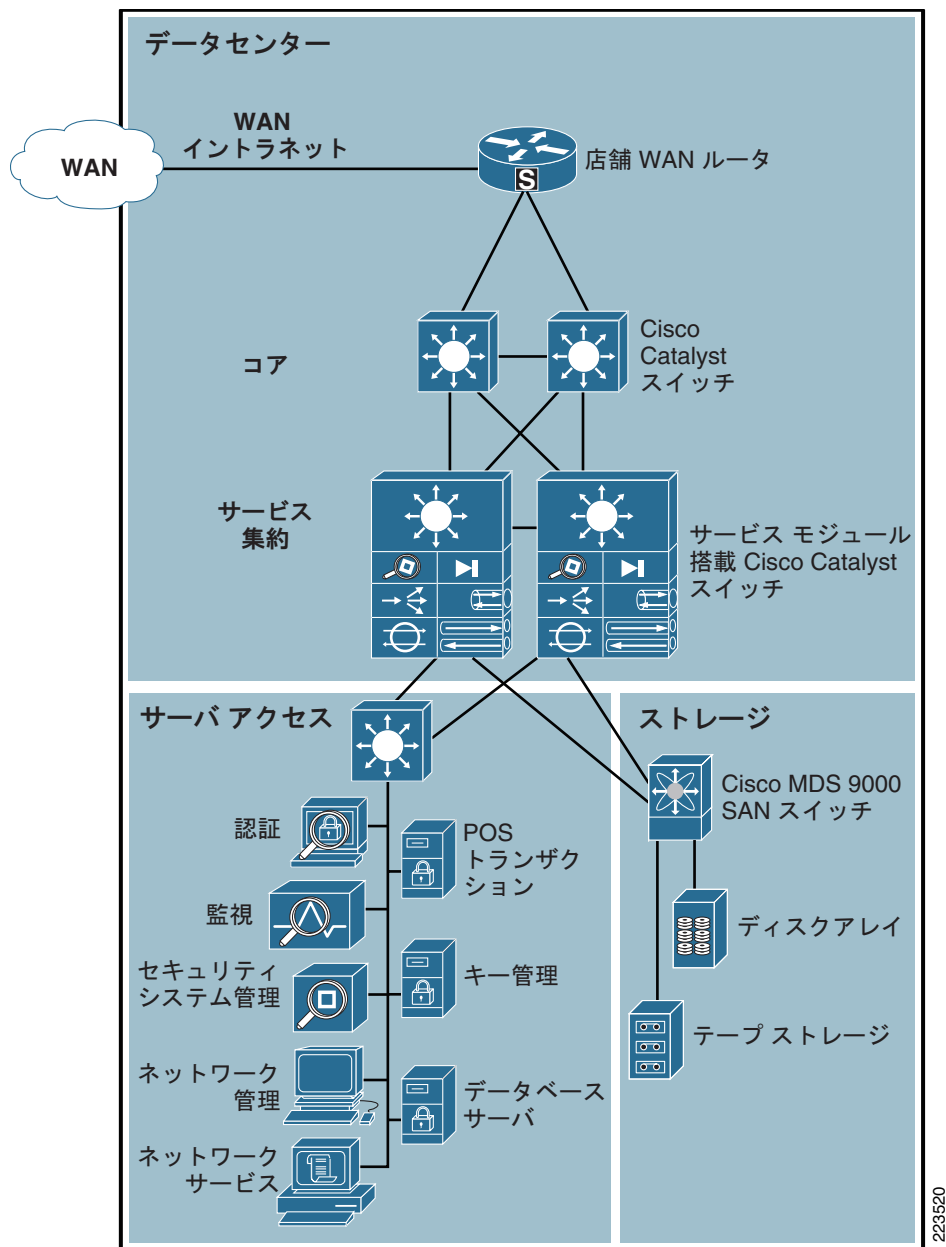
- ・ 高可用性設計に基づくネットワーク復元性を実現するための高いコスト

これらの小売店舗ネットワーク設計は、小売業者が PCI 準拠をスムーズに実現できるようにするだけでなく、Cisco Intelligent Retail Network を形成する新規のサービスやアプリケーションのためのスケーラブルなプラットフォームとしても利用できます。

データセンター

図 2-5 にデータセンター ソリューションの設計を示します。

図 2-5 典型的な小売エンタープライズ データセンター設計



主要な設計要件

- ・ スケーラブルで高い可用性を備えた、ビジネス アプリケーション データのリポジトリと計算サーバ
- ・ パブリック / プライベート ネットワーク経由で店舗ネットワークを確実に接続する WAN 集約レイヤ
- ・ パブリック ネットワーク経由で店舗ネットワークを接続する場合には、IPSec 暗号化が必要
- ・ WAN 集約およびサービス集約レイヤ間の高パフォーマンス コア ネットワーク
- ・ コアとサーバアクセス レイヤ間の集約化ネットワーク サービス
- ・ ビジネスおよびソリューション管理サーバを他のデータセンター リソースに確実に接続するサーバアクセス レイヤ
- ・ ストレージリソースをデータセンター内の他のリソースに確実に接続するストレージエリア ネットワーク レイヤ

概要と説明

本ガイドでは、WAN 集約、コア、サービス集約、サーバアクセス、ストレージの5つのエリアにデータセンターを分割します。この多重階層データセンター アーキテクチャのコア、サービス集約、サーバアクセスの各階層は、『Cisco Data Center Infrastructure Design Guide 2.5』に記述されている設計に基づいています。この設計ガイドは下記の URL で公開されています。

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

WAN 集約アーキテクチャは『Infrastructure Protection and Security Service Integration Design for the Next Generation WAN Edge v 2.0』の記述に基づいています。この設計ガイドは下記の URL で公開されています。

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

WAN 集約

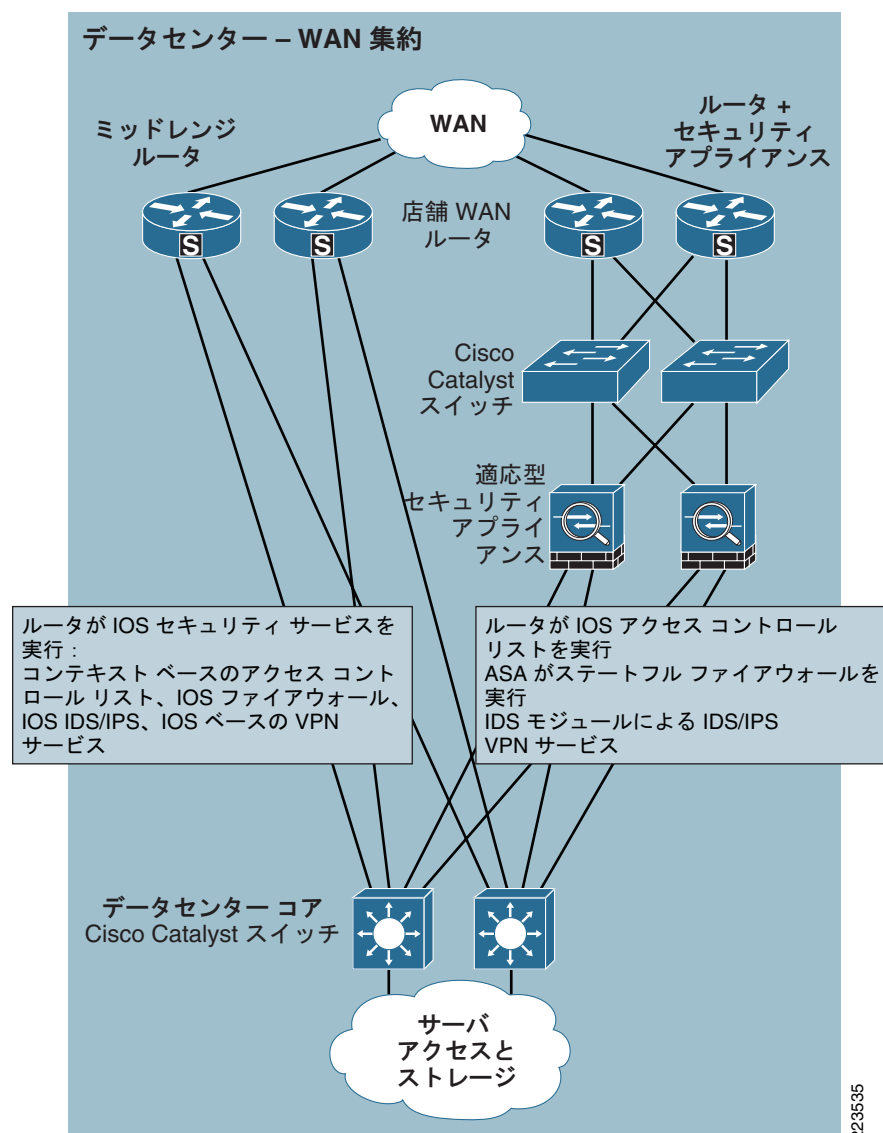
WAN 集約レイヤは、小売店舗からの接続、およびプライベート / パブリック サービス プロバイダー ネットワークを経由した各支店 LAN からの接続を集約する中継ネットワークです。WAN 集約レイヤは、本社、キャンパスまたは地域の支店のエンドユーザに直接接続するのではなく、店舗 LAN からデータセンター コア ネットワークとそのリソースへの接続を提供します。

WAN エッジデバイスはシスコ製ルータですが、データセンター ネットワーク用のインターネット ゲートウェイとして使用されていないことを推奨します。これは、店舗 WAN のセグメンテーションと典型的なスループットによるものです。店舗とエンタープライズ ネットワーク間で VoIP を転送する場合は、音声の品質を維持しながら、店舗への接続帯域幅を保証できるかどうかという問題を検討する必要があります。さらに、冗長性、店舗バックアップ用ネットワーク、ネットワーク全体のセキュリティ問題を考慮すると、WAN 集約の範囲は、店舗ネットワークからデータセンターへの接続機能だけに限定されます。

WAN 集約レイヤの各 WAN エッジルータの内側では、専用のファイアウォール アプライアンスを使用して、着信 WAN トラフィックのセキュリティを保護し、店舗 VPN 接続を終端します。この設計により、最高レベルのスケーラビリティが実現されます。また、大半のシスコルータは、ファイアウォール機能を含む IOS セキュリティ ソフトウェア オプションをサポートしています。店舗、支店、在宅勤務者宅では、ユーザ数と接続使用率が店舗 WAN 集約ヘッドエンドよりもかなり低下するため、シスコでは Cisco IOS セキュリティ機能セットを使用することを推奨しています。

WAN 集約ネットワークには2つの標準的な WAN 速度カテゴリがあります。すなわち、OC3（155 Mbps）未満と OC12（622 Mbps）以上の2つです。どちらのネットワーク速度を選択するかによって、どのシスコ製プラットフォームを選択するかが決まります。また、この設計では、各 WAN 速度について、2つのプロファイルを作成します。これらのプロファイルは、選択したエンタープライズ WAN アーキテクチャに関係なく、WAN エッジネットワークを設計するときの指針となるように設計されています。各 WAN 速度のプロファイルは、統合型シャーシと専用シャーシを調べて、前のセクションで概説した各機能コンポーネントが存在するかどうか確認します。単一または極めて少数のネットワーク デバイス上に本ドキュメントで説明した大半の WAN エッジ機能が集約された高度統合化ソリューションを選択するか、これらの WAN エッジ機能が複数のネットワーク デバイスに分散された粒度とスケーラビリティ重視のソリューションを選択するかは、お客様によって異なります。

図 2-6 データセンター—2つの WAN 集約ソリューション



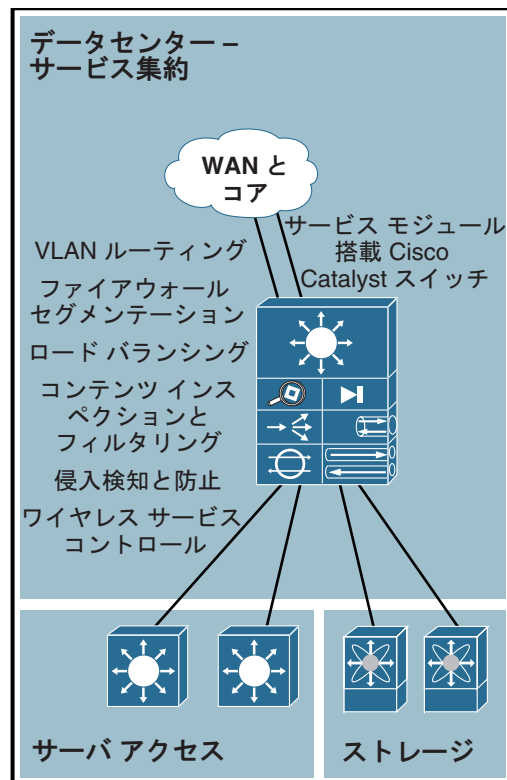
コア

コアレイヤは、データセンターに着信する、またはデータセンターから発信されるすべてのフローに対して高速なパケットスイッチングを行うためのバックプレーンを提供します。複数の集約モジュールに対する接続を提供し、復元力のあるレイヤ3経由のファブリックによりシングルポイント障害をなくします。コアレイヤは、Open Shortest Path First (OSPF) や Enhanced Interior Gateway Routing Protocol (EIGRP) などの内部ルーティングプロトコルを実行し、Cisco Express Forwarding (CEF) ベースのハッシングアルゴリズムを使用して、キャンパスコアと集約レイヤ間のトラフィックのロードバランシングを実施します。

サービス（エッジ）集約

サービス集約レイヤモジュールは、サービスモジュールの統合、レイヤ2ドメインの定義、スパンニングツリー処理、デフォルトゲートウェイの冗長性などの重要な機能を提供します。サーバ間のマルチレイヤトラフィックは集約レイヤを通過し、ファイアウォールやサーバロードバランシングなどのサービスを使用して、アプリケーションの最適化とセキュリティ保護を実行します。これらのサービスモジュールは、コンテンツスイッチング、ファイアウォール、SSLのオフロード、侵入検知、ネットワーク分析などのサービスを提供します。図2-7に、サービス集約レイヤの概念図を示します。

図 2-7 サービス集約レイヤの概念図



この概念図の例は、1 台の Cisco Catalyst 6500 スイッチと各サービスモジュールで構成されています。シスコのデータセンター参照アーキテクチャでは、サーバアクセスやストレージレイヤにおける典型的な高可用性要件を満たすために、2 台のサービス集約スイッチを使用することを推奨しています。

サーバアクセス レイヤ

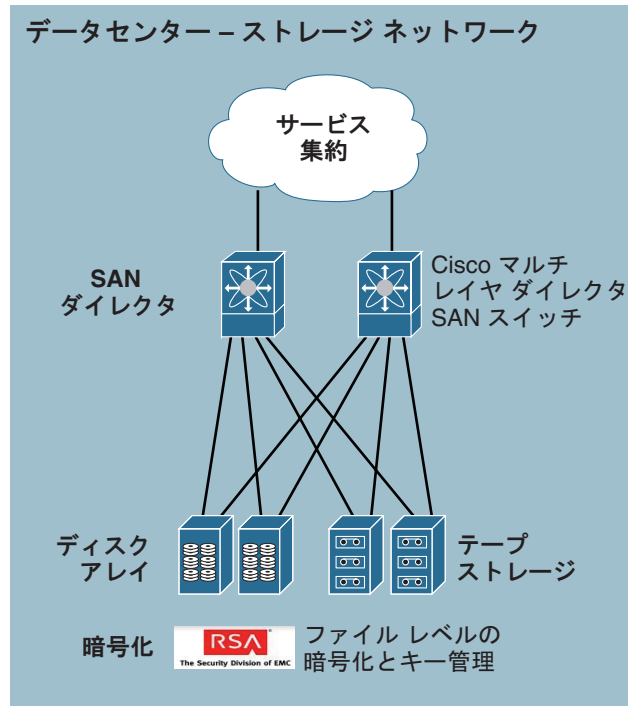
サーバアクセス レイヤは、サーバとネットワークが物理的に接続する場所です。典型的なデータセンターでは、サーバコンポーネントは、1 RU のサーバ、スイッチ内蔵のブレードサーバ、パススルー ケーブル配線を使用したブレードサーバ、クラスタサーバ、OSA アダプタを搭載したメインフレームで構成されます。アクセス レイヤ ネットワーク インフラストラクチャは、モジュラ型スイッチ、コンフィギュレーションが固定された 1 RU または 2 RU スwitch、統合型ブレードサーバスイッチで構成されます。各スイッチは、レイヤ 2 およびレイヤ 3 の両トポロジを実現できるため、さまざまなサーバブロードキャスト ドメインや管理要件を満たすことができます。

ソリューション管理サーバは、このレイヤのネットワークに接続されます。このようにしてサーバは集約化され、他のビジネスアプリケーションサーバから分離されて、ファイアウォールサービスによって上位のサービス集約レイヤから保護されます。ビジネスサーバ（POS トランザクションログサーバ、データベース、データウェアハウスサーバで構成）は、このレイヤに配置されますが、独立した VLAN とファイアウォールポリシーによって分割されます。

ストレージ

このソリューションのストレージ実装では、RSA File Security Manager 製品によるファイル暗号化、ファイバチャネルのゾーン分割機能、シスコのマルチレイヤダイレクタスイッチ（MDS）による LU（論理ユニット）のマスキング/ゾーン分割機能を組み合わせて、データセンターにあるカード所有者の静止データの暗号化とアクセス制限を行います。ファイバチャネルファブリック内でゾーン分割を行うと、ゾーン内のデバイスだけにアクセスが制限されます。ゾーン分割により、ユーザは、特定のストレージデバイス（ディスクアレイ）に対するアクセスに基づいて各デバイスを分割配置できます。データセンター環境を構築する場合に、データセンターサーバファーム内の複数のファイルサーバを同じ SAN ファブリックに接続し、カード所有者データにアクセスできるサーバを一部のサーバだけに制限する必要があるときは、一般に、この分割配置方式が絶対要件となります。LUN マスキングを行うには、ファイバチャネル、スイッチポートレベルを越えたゾーン分割が必要になります。それには、指定したディスクアレイ上の特定の LUN に対する限定アクセスを許可して、その LUN ゾーンに属する特定のデバイスだけが当該ディスクセクションにアクセスできるようにします。

図 2-8 データセンターの SAN



利点

- モジュラおよびレイヤ方式で配置された標準化された機器とソフトウェア イメージによって、構成管理が簡素化され、システムの可用性が向上します。
- 高可用性データセンター設計により、店舗からコアのデータ / ストレージ サービスに対するアクセスにおいて高い復元力を実現できます。
- WAN 集約代替方式により、サービス プロバイダー ネットワーク オファリングの柔軟な選択が可能となります。
- サービス集約設計によって、新規アクセス レイヤの追加や共有ネットワーク サービス (FW、IDS、アプリケーション ネットワーキング、ワイヤレス管理など) の管理にモジュラ方式のアプローチが可能となります。
- ファイアウォール、IDS、およびアプリケーション ネットワーキング サービスは、データセンターのすべてのレイヤで使用できます。
- データセンターにおける処理能力やストレージ要件の変化に対応できるスケーラビリティを備えています。
- ソリューション管理の一元化によって、ネットワークのすべての側面、セキュリティ、システム管理、およびネットワーク上の任意の場所からのリモートアクセスをサポートします。

制約

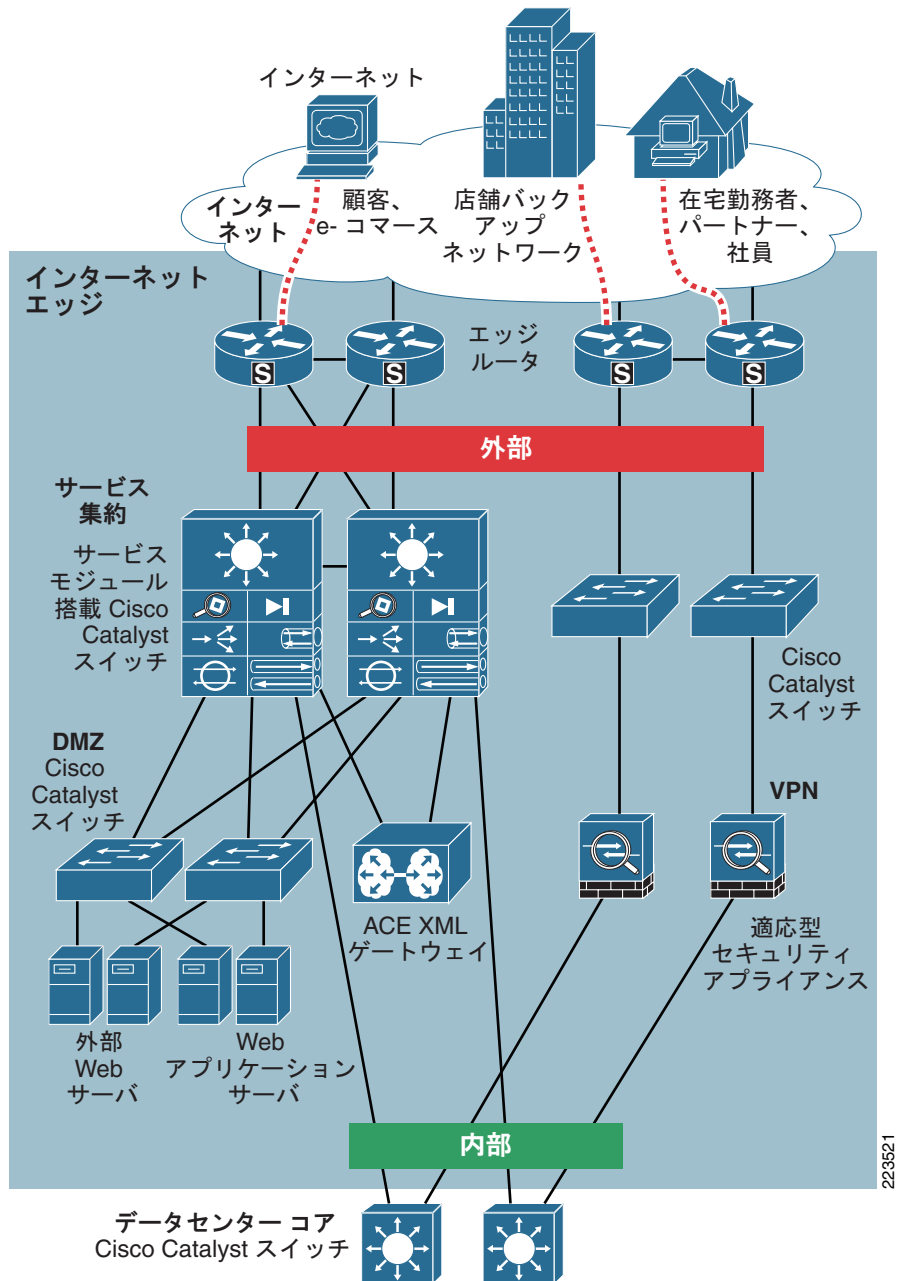
- WAN アクセス速度が、店舗ネットワーク システムと WAN 集約レイヤ間の制限要因になります。

- 小売業者では、店舗と WAN エッジ集約ルータ間の WAN 回線が加入超過状態になることがよくあります。加入超過状態の回線は不安定となり、WAN 回線にトラフィックが同時に流れ込み処理能力を超えると、支払いカード情報のパケットが失われます。このため、支払いカードトラフィックを重要なトラフィックとして分類する QoS ガイドラインが推奨されています。
- 支払いカード情報を WAN 経由で転送するときは、店舗ネットワークからデータセンターへのバックアップ用ネットワーク接続が推奨されています。これらのオプションは、PCI ガイドラインに準拠するために必要ではないため、この設計ガイドでは説明していません。

インターネット エッジ

図 2-9 に、インターネット エッジ ソリューション アーキテクチャの構成を示します。

図 2-9 典型的なインターネット エッジ アーキテクチャ



主要な設計要件

- インターネットへのエンタープライズ接続
- シスコ製ファイアウォールと侵入検知システムを使用したインターネット エッジ設計のセキュリティ保護
- Web 攻撃からエンタープライズ ネットワークを保護
- ネットワーク復元力を実現するためのデュアル スレッド設計
- 高度に集中化および統合化されたエッジ ネットワークを実現するためのコラプスト インター ネット エッジとエクストラネット
- エンタープライズ ユーザ / 在宅勤務者へのリモート VPN アクセス

概要と説明

このソリューションでは、コラプスト インターネット エッジとエクストラネットを使用して、インターネット接続性とビジネス パートナー接続性をサポートします。この設計は、『*Data Center Networking: Internet Edge Design Architecture Design Guide*』 (<http://www.cisco.com/go/srnd/>) に記述されているベスト プラクティスを考慮して、そこに記載されている推奨事項を小売業インターネット エッジ/エクストラネット用にカスタマイズしたものです。エッジは、インターネット サービスを完全なエンタープライズ環境（すなわち、本社から ISP、シスコのセキュア VPN を使用して本社と接続するブランチ オフィス接続）に接続します。コラプスト設計により、高度に集中化および統合化されたエッジ ネットワークを実現し、集約化されたトラフィックを、2 台の Cisco Catalyst 6500 スイッチ シャーシ内のさまざまなサービス モジュール（Cisco ACE、Cisco FWSM、Cisco IDSM2）を介して転送できます。この設計では、Cisco ACE AXL Gateway を使用して、XML の脅威に対する保護と防御を実現しています。インターネット エッジは次のセキュリティ機能を提供します。

- セキュアな構成と管理。
- IP アンチ スプーフィング。
- Access Control List (ACL; アクセス コントロール リスト) により、内部、外部、Demilitarized Zone (DMZ; 非武装地帯) 間を横断する IP トラフィックを明示的に許可および / または拒否できます。
- ステートフル インспекション — インターネット エッジの通過を許可されたトラフィックのセッション ステータスを確認かつ監視し、既存または許可されたセッションで予想されるステータスと一致しないトラフィックを拒否する機能を提供します。
- Cisco IDSM2 を使用した侵入検知 — インターネット エッジ内の個々のポイントを通過するトラフィックを混合モードで監視し、エンタープライズ ネットワークに脅威を与える可能性のある怪しい動作を検出すると、アラームを発信したり対策を講じたりします。
- DMZ — インターネットから直接アクセスする必要のあるアプリケーション サーバを、インターネットと内部エンタープライズ ネットワークの間にある、ある程度信頼できるセキュアなエリアに配置します。これにより、内部ホストとインターネット ホストは、DMZ に設置されたサーバと通信できます。

利点

- コラプスト アーキテクチャ
- 高可用性設計
- 単一シャーシ内のファイアウォールと侵入検知機能

欠点

- 設定が複雑

個々のシスコ ソリューション コンポーネントと QSA 監査要件を満たすために必要な PCI 要素間のマッピングについては、[第 3 章「ソリューション コンポーネント — ベスト プラクティスおよび PCI」](#)を参照してください。



CHAPTER 3

ソリューションコンポーネントーベストプラクティスおよび PCI

この章の情報は、小規模、中規模、大規模の各店舗、データセンター、およびインターネットエッジアーキテクチャに対し、同等に適用されます。各ソリューションコンポーネントは、次のものととも示されます。

- 一般的な注意事項 / ベストプラクティス
ここでは、小売ビジネス環境内の各テクノロジーの手引きとなる原則を示します。注はシスコの推奨事項ですが、必ずしも PCI のフレームワークの範囲内であるとは限りません。一部の注は、PCI 仕様を上回る、該当する製品の追加セキュリティ機能です。
- ソリューションコンポーネントが満たす PCI の下位要件
ここでは、どの PCI 下位要件が、該当する各テクノロジーで監査され、検証されたかを解説します。この結果は、シスコのラボで構築された実装に直接関連しており、[第4章「ソリューションの実装と設定」](#)に記載されています。監査の結果は、小売業者内の実装により異なる場合があります。
- 補完コントロールが必要な PCI 下位要件
ここでは、PCI 監査を問題なく終了するために追加の補完コントロールを必要とした PCI 下位要件について解説します。ここで説明するテクノロジーには、コンプライアンスを認められるために追加の構成および製品が必要でした。監査の結果は、小売業者内での実装により異なる場合があります。

詳細な構成については、[第4章「ソリューションの実装と設定」](#)を参照してください。

ネットワーク システム

Cisco Integrated Services Router

Cisco Integrated Services Router (ISR) は、データ、ネットワーク、セキュリティをローカルおよび中央集中型の 1 つのプラットフォームに統合します。

一般的な注意事項 / ベスト プラクティス

- 小規模、中規模、大規模のアーキテクチャにおける ISR ルータのセキュリティ機能は、Cisco Security Manager を使用して設定します。シスコでは、これをルータ設定の主要方式として採用している場合、ルータの CLI (コマンドライン インターフェイス) へ直接変更することは推奨しません。中央およびローカルの管理機能が同時に使用されると、予期できない結果となる可能性があります。
- 小規模、中規模、大規模のアーキテクチャにおける ISR ルータの一般的な設定は、CiscoWorks Resource Manager Essentials (C-LMS のコンポーネントの 1 つ) により維持されます。
- ファイアウォール ルール セットは、「必要最小限のアクセス量」ポリシーに従う必要があります。ルールは、特定の送信元 / 送信先アドレス設定、および point-of-sale (POS) ネットワークのカード所有者データ環境に必要な TCP/UDP ポートにより定義される必要があります。
- 検査ルールが ISR ルータで有効になっており、ファイアウォールが状態を維持していることを確認してください (デフォルトでは、どのルールも有効になっていません)。
- WAN テクノロジーが公開されていると見なされる場合は、WAN から店舗ルータへのアクセスが、店舗に設置されたファイアウォール フィルタによって保護されている必要があります。Cisco PCI Solution for Retail ラボでは、店舗 WAN トラフィックのフィルタリングは、帯域幅を維持するためにフレーム リレー接続のアウトバウンドデータセンター側で実行されます。フレーム リレーは、プライベート ネットワークと見なされます。
- ルータの HTTP サーバ サービスを無効にして、HTTP セキュア サーバを有効にしてください。
- ルータのコンソール、AUX、VTY の各インターフェイスおよび CLI で、**session-timeout** コマンドと **exec-timeout** コマンドを 15 分以下に設定します。
- ルータのログイン、着信、および EXEC の各モードの適切なバナー メッセージを設定します。ルータを所有または管理している企業をログイン バナー警告からは特定できないようにする必要があります。着信バナーおよび管理バナーには、その領域がプライベートなものと見なされていることと、不正アクセスが法律の及ぶ限りにおいて訴追の対象となることを記述する必要があります。
- ルータの 1 次ログイン認証を、Cisco Secure Access Control Server (CS-ACS) に誘導されるよう設定します。個々のユーザ アカウント プロファイルを作成する必要があります。WAN または CS-ACS での障害に備えて、ルータ自体に対してローカルの 2 次認証または 3 次認証を設定します。
- **no service password-recovery** コマンドを **service password encryption** コマンドとともに使用して、ルータに物理的な侵害によるパスワードの盗難を防ぎます。
- デフォルト パスワードおよびコミュニティ スtring を適度に複雑なものに変更します。

ソリューションコンポーネントが満たすPCIの下位要件（ルータ）

要件1：カード所有者データを保護するよう設定されたファイアウォールを設置および維持する

- **PCI 1.2** — カード所有者データ環境に必要なプロトコルを除き、「非信頼」ネットワークおよびホストからのすべてのトラフィックを拒否するファイアウォール設定を構築する。

PCI Solution Retail の各ルータは、ファイアウォール機能セットを使用して、この要件を満たします。

このソリューションでは、次のビジネス関連の通信機能を使用できました。

- Cisco Security Manager (CS-M) および CiscoWorks (C-LMS) の管理プロトコル
- 監視、分析、および応答システム (CS-MARS)
- アクセスコントロールサーバ (CS-ACS) に対する TACACS を介した authentication, authorization, and accounting (AAA; 認証、認可、アカウンティング)
- Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) によるネットワークトラブルシューティング
- Network Time Protocol (NTP; ネットワークタイムプロトコル) によるタイムスタンプ同期化
- システムロギングアクセスによるネットワークイベント
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)
- Secure Sockets Layer (SSL)
- Hot Standby Routing Protocol (HSRP) によるハイアベイラビリティ
- DHCP
- 上記以外はすべて拒否され、ログに記録

このソリューションで使用される通信機能の全リストについては、[付録C「アプリケーションプロトコル」](#)を参照してください。

次に示すのは、大規模店舗アーキテクチャでの設定例です。

```
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** — ダイナミック パケット フィルタリングとも呼ばれるステートフル インスペクションを実装する（つまり、ネットワークに対して「確立された」接続のみが許可される）。

ソリューションのステートフル インスペクションはシスコの推奨設定です。文のデフォルトポートに異常がないかどうか、文によりプロトコルが検査され、各セッションの確立済みダイナミック接続テーブルが維持されます。

設定例を次に示します。

```

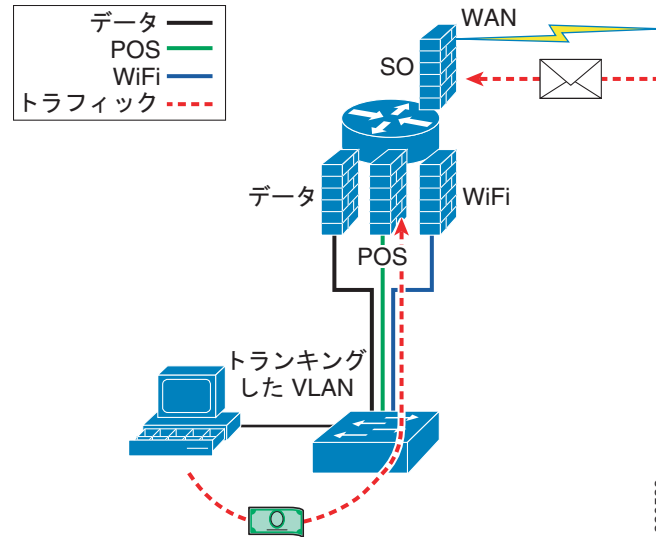
RLRG-1#
!
ip inspect name CSM_INSPECT_1 http alert on audit-trail on
ip inspect name CSM_INSPECT_1 dns alert on audit-trail on
ip inspect name CSM_INSPECT_1 radius alert on audit-trail on
ip inspect name CSM_INSPECT_1 tacacs alert on audit-trail on
ip inspect name CSM_INSPECT_1 ssh alert on audit-trail 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** — カード所有者データ環境に必要なものに限るようにアウトバウンドトラフィックを制限する。

ルータは、各ネットワーク セグメントからのすべてのインバウンドトラフィックをフィルタリングし、検査するよう設定されます。QSA との広範囲にわたる討議の結果、ルータへのすべてのインバウンドネットワークトラフィックのフィルタリングの実装が可能であるという決定が下されました。これは、アウトバウンドトラフィックを効果的に制限するもので、多くの小売業者ネットワークで一般的に実行されています（図 3-1 を参照）。

図 3-1 アウトバウンド トラフィックの制限



設定例を次に示します。

```
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** — 特に許可されているものを除き、すべてのインバウンドおよびアウトバウンドのトラフィックを拒否する。

各ファイアウォールルールセット内で明示的には許可されていないすべてのトラフィックを拒否し、ログに記録します。小売業者の環境によっては、拒否されたすべてのトラフィックのロギングが、パフォーマンスに重大な影響を及ぼす場合があります。

設定例を次に示します。

```
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** — あらゆる無線ネットワークとカード所有者データ環境の間に境界ファイアウォールを設置する。また、無線環境からのあらゆるトラフィックを拒否するように、またはあらゆるトラフィックを制御しないように（このようなトラフィックがビジネス上必要な場合）、これらのファイアウォールを設定する。

POS ネットワークおよび無線ネットワークは、VLAN によりセグメント化され、ルータに統合された Cisco IOS ファイアウォールで保護されます (図 3-1 を参照)。

設定例を次に示します。

```
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** — インターネット上での内部アドレスの変換および解読を防ぐための IP マスカレードを実装する。Port Address Translation (PAT; ポート アドレス変換) や Network Address Translation (NAT; ネットワーク アドレス変換) などの RFC 1918 アドレス空間を実装するテクノロジーを使用する。

このソリューションの店舗は、インターネット上でルーティングできないプライベート アドレッシングで設定されています。データセンターでは、NAT または PAT を使用して、これらのアドレスをパブリックに使用可能なアドレス空間に変換する必要があります。

次に示すのは、大規模店舗のアドレッシングプランの例です。

```
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)
```

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E「[Device Configurations](#)」を参照してください。

このリストのあとの記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル (デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル) をすべて無効にする。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

パッド、フィンガー、およびスモール サーバなどのサービスを無効にします。これらのサービスは、Cisco IOS リリースに応じてデフォルトで有効または無効になり、実行コンフィギュレーションには表示されない場合があります。

暗号化された管理通信のみが有効で、その他のすべてのサービスは無効でした。

設定例を次に示します。

```

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

```

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発および維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このリストのあとの記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、Cisco Secure Access Control Server (CS-ACS)、およびユーザ アカウント サービスの Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、ルータに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

ルータのコンソール、AUX、VTY の各インターフェイスおよび CLI で、**session-timeout** コマンドと **exec-timeout** コマンドを 15 分以下に設定します。

設定例を次に示します。

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

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、ここで説明している下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

Cisco ISR ルータは、ACS を使用しなかった場合は AAA 機能向けに設定されず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

設定例を次に示します。

```
!
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** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
- **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する（組織内の 2、3 台の中央時間サーバは、外部からの時間信号を受信 [特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接] し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する）。

- **PCI 10.4.c** — 最新バージョンの *Network Time Protocol (NTP)* (ネットワーク タイム プロトコル) を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの *NTP* 時間を更新する特定の外部ホストが指定されていることを確認する (攻撃者によるクロックの変更を防ぐため)。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、*NTP* サービスで提供されるようにすることができる (内部時間サーバの不正使用を防ぐため)。詳細については、<http://www.ntp.org> を参照。

設定例を次に示します。

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

要件 11 : セキュリティ システムおよびセキュリティ プロセスを定期的にテストする

- **PCI 11.4.a** — ネットワークでのネットワーク侵入検知システムおよび侵入防御システムのいずれか、または両方を必ず使用する。カード所有者データ環境での重要なネットワーク トラフィックがすべて監視されていることを確認する。
- **PCI 11.4.c** — *IDS/IPS* 設定を調べて、*IDS/IPS* デバイスがベンダーの指示に従って構成、維持、および更新されており、保護機能が最適であることを確認する。

ここで説明した下位要件は、*CS-MARS* の監視および警告機能を組み合わせた *Cisco ISR* ルータの *IPS* 機能セットにより満たされます。

Cisco Security Manager (C-SM) により、*IDS/IPS* イベント定義および *Cisco ISR* ルータへの署名が設定され、導入されます。

設定例を次に示します。

```
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
!
```

補完コントロールが必要な PCI 下位要件 (ルータ)

このソリューション内の *Cisco ISR* ルータは、すべての関連 PCI 下位要件を満たしているため、補完コントロールは不要でした。

ミッドレンジ ルータ (WAN 集約) / エッジ ルータ (インターネット エッジ)

一般的な注意事項 / ベスト プラクティス

- 設定はルータの CLI で手動で行われ、設定のバックアップおよび、設定の変更と非コンプライアンスに対する監視は、*CiscoWorks Network Compliance Manager (C-NCM)* を介して行われました。

- ファイアウォールルールセットは、「必要最小限のアクセス量」ポリシーに従う必要があります。可能な場合は、特定の送信元 / 送信先アドレス設定、および Point-of-Sale (POS) ネットワークのカード所有者データ環境に必要な TCP/UDP ポートによってルールが定義される必要があります。
- データセンターとの間の境界ファイアウォールは、Adaptive Security Appliance により提供されました。その結果、Cisco 7206VXR は、ファイアウォールの 1.x 要件セットに従って評価されてはいません。
- ルータの HTTP サーバ サービスを無効にして、HTTP セキュア サーバを有効にしてください。
- ルータのコンソール、AUX、VTY の各インターフェイスおよび CLI で、**session-timeout** コマンドと **exec-timeout** コマンドを 15 分以下に設定します。
- ルータのログイン、着信、および EXEC の各モードの適切なバナー メッセージを設定します。ルータを所有または管理している企業をログイン バナー警告からは特定できないようにする必要があります。着信バナーおよび管理バナーには、その領域がプライベートなものに見なされていることと、不正アクセスが法律の及ぶ限りにおいて訴追の対象となることを記述する必要があります。
- ルータの 1 次ログイン認証を、CS-ACS に誘導されるよう設定します。個々のユーザ アカウント プロファイルを作成する必要があります。WAN または CS-ACS での障害に備えて、ルータ自体に対してローカルの 2 次認証または 3 次認証を設定します。
- no service password-recovery** コマンドを **service password encryption** コマンドとともに使用して、ルータの物理的な侵害によるパスワードの盗難を防ぎます。
- デフォルト パスワードおよびコミュニティ ストリングを適度に複雑なものに変更します。
- すべてのインターフェイスでアンチスプーフィングを有効にします。
- インターネット エッジルータの場合は、インターネットで接続できるインターフェイスで次のアクセスリストを使用します。このアクセスリストは、インフラストラクチャ アドレス空間宛てのトラフィックを明示的にフィルタリングします。エッジインフラストラクチャ アクセスリストを導入するには、インフラストラクチャ空間と、この空間へのアクセスに必要な認可されたプロトコルを明確に定義する必要があります。アクセスリストは、ピアリング接続やカスタマー接続などのような、外部から接続できるすべての接続でネットワークへの進入時に適用されます。

設定例を次に示します。

```

!
!
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
!
!
```



(注) **log** キーワードを使用すると、任意のプロトコルの送信元および送信先に関する詳細情報を提供できます。このキーワードはアクセスリストの該当項目に対する貴重な情報を提供しますが、**log** キーワードを使用するアクセスリスト項目が多数該当する場合は、CPU 使用率が増大します。ロギングに関連するパフォーマンスへの影響は、プラットフォームにより異なります。

このソリューションのサービス プロバイダー ネットワークは MPLS ネットワークを表しています。このマニュアルの執筆時には、MPLS がプライベート ネットワークと見なされており、WAN 上のセキュア トンネリングは不要でした。ただし、ベスト プラクティスのためには、Virtual Private Network (VPN; バーチャル プライベート ネットワーク) トンネリングを実装することを推奨します。IPSec VPN の実装に関する詳細情報については、次の URL にある『*IPSec VPN Direct Encapsulation Design Guide*』を参照してください。

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

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。付録 E「Device Configurations」を参照してください。

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル (デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル) をすべて無効にする。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

パッド、フィンガー、およびスモール サーバなどのサービスを無効にします。これらのサービスは、Cisco IOS リリースに応じてデフォルトで有効または無効になり、実行コンフィギュレーションには表示されない場合があります。

暗号化された管理通信のみが有効で、その他のすべてのサービスは無効でした。

設定例を次に示します。

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

要件 6：セキュリティで保護されたシステムおよびアプリケーションを開発および維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常にご利用できます。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および**要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる**

このリストの後の記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、CS-ACS および、ユーザ アカウント サービスのための Microsoft Active Directory の実装により満たされています。

CS-ACS に到達できない場合のフォールバック認証は、ルータに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

ルータのコンソール、AUX、VTY の各インターフェイスおよび CLI で、**session-timeout** コマンドと **exec-timeout** コマンドを 15 分以下に設定します。

設定例を次に示します。

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

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、ここで説明している下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

Cisco ISR ルータは、CS-ACS を使用しなかった場合は AAA 機能向けに設定されず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

設定例を次に示します。

```
!
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** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバは、外部からの時間信号を受信します。時間信号は、特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接送信されます。これらの時間サーバは互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有します。
 - **PCI 10.4.c** — 最新バージョンの *Network Time Protocol* (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスで提供されるようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

設定例を次に示します。

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

Cisco Catalyst イーサネット スイッチおよび Network Switch Module

Cisco Catalyst イーサネット スイッチは、ルーティングされたネットワークおよび WAN サービスへの、IP エンドポイントの接続を提供します。

一般的な注意事項 / ベスト プラクティス

- 小規模、中規模、大規模のアーキテクチャにおける Cisco Catalyst スイッチおよび Network Switch Module の一般的な設定は、CiscoWorks Resource Manager Essentials (C-LMS のコンポーネントの 1 つ) により維持されます。
- Cisco Catalyst スイッチで VLAN を使用すると、小売業者は、隔離されたアドレッシング方式を維持しながら、そのデバイスに同ボックス有線アクセスを提供できます。
- スイッチの HTTP サーバを無効にして、HTTP セキュア サーバを有効にしてください。
- **session** コマンドおよび **exec timeout** コマンドを 15 分以下に設定します。
- スイッチのログイン、着信、および EXEC の各モードの適切なバナー メッセージを設定します。スイッチを所有または管理している企業をログイン バナー警告からは特定できないようにする必要があります。着信バナーおよび管理バナーには、その領域がプライベートなものに見なされていることと、不正アクセスが法律の及ぶ限りにおいて訴追の対象となることを記述する必要があります。
- スイッチの 1 次ログイン認証を、CS-ACS に誘導されるよう設定します。個々のユーザアカウント プロファイルを作成する必要があります。WAN または CS-ACS での障害に備えて、スイッチ自体に対してローカルの 2 次認証または 3 次認証を設定します。
- **no service password-recovery** コマンドを **service password encryption** コマンドとともに使用して、スイッチの物理的な侵害によるパスワードの盗難を防ぎます。
- デフォルト パスワードおよびコミュニティ スtring を適度に複雑なものに変更します。

ソリューション コンポーネントが満たす PCI の下位要件（スイッチ）

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する（たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など）。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E「[Device Configurations](#)」を参照してください。

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル（デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル）をすべて無効にする。

- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

パッド、フィンガー、およびスモール サーバなどのサービスを無効にします。これらのサービスは、Cisco IOS リリースに応じてデフォルトで有効または無効になり、実行コンフィギュレーションには表示されない場合があります。

暗号化された管理通信のみが有効で、その他のすべてのサービスは無効でした。

設定例を次に示します。

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

要件 6：セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このソリューションでは、ここで説明している下位要件は、CS-ACS および、ユーザ アカウント サービスのための Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、ルータに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。

- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

スイッチのコンソール インターフェイスおよび VTY インターフェイスで、**session-timeout** コマンドと **exec-timeout** コマンドを 15 分以下に設定します。

設定例を次に示します。

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

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、これらの下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

Catalyst スイッチは、CS-ACS を使用しなかった場合は AAA 機能向けに設定されず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

設定例を次に示します。

```
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** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。

次の事柄がプロセスに含まれ、実装されていることを確認する。

- **PCI 10.4.a** — *NTP* または類似のテクノロジーを時間の同期化に使用していることを確認する。
- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間およびUTC（以前の GMT）に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
- **PCI 10.4.c** — 最新バージョンの *Network Time Protocol (NTP)*（ネットワーク タイム プロトコル）を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの *NTP* 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、*NTP* サービスで提供されるようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

設定例を次に示します。

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

補完コントロールが必要な PCI 下位要件（スイッチ）

このソリューションでは、Cisco Catalyst スイッチには、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

Cisco Firewall Services Module (FWSM)

Cisco FWSM は、Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 インターネット ルータの内部に搭載された統合モジュールです。FWSM を使用すると、Cisco Catalyst スイッチのあらゆるポートがファイアウォール ポートとして動作するため、ネットワーク インフラストラクチャの内部にファイアウォール セキュリティを統合できます。

一般的な注意事項 / ベスト プラクティス

- ファイアウォール ルール セットは、「必要最小限のアクセス量」ポリシーに従う必要があります。ルールは、特定の送信元 / 送信先アドレス設定および TCP/UDP ポートによって定義される必要があります。
- インターネット エッジの場合は、FWSM の外側のインターフェイスの ICMP 許可を無効にします。ユーザが DMZ セグメント内のサーバにアクセスする必要がある場合は、外部ユーザが、特定のプロトコルとポートを使ってサーバに到達できることを確認します。
- すべてのインターフェイス上で、アンチスプーフィング機能を提供するよう **ip verify reverse path** コマンドを設定します。
- FWSM のコンソールで、**console timeout** コマンドを 15 分以下に設定します。

- FWSM のログイン、着信、および EXEC の各モードの適切なバナー メッセージを設定します。FWSM を所有または管理している企業をログイン バナー 警告からは特定できないようにする必要があります。着信バナーおよび管理バナーには、その領域がプライベートなものに見なされていることと、不正アクセスが法律の及ぶ限りにおいて訴追の対象となることを記述する必要があります。
- FWSM の 1 次ログイン認証を、CS-ACS に誘導されるよう設定します。個々のユーザ アカウント プロファイルを作成する必要があります。接続または CS-ACS での障害に備えて、FWSM 自体に対してローカルの 2 次認証または 3 次認証を設定します。
- デフォルト パスワードおよびコミュニティ スtring を適度に複雑なものに変更します。
- ネットワーク 管理ステーションから Cisco FWSM に対しては、SSHv2 (Telnet でも SSHv1 でもない) 接続のみを許可します。

ソリューション コンポーネントが満たす PCI の下位要件 (Cisco FWSM)

要件 1: カード所有者データを保護するよう設定されたファイアウォールを設置および維持する

- **PCI 1.2** — カード所有者データ環境に必要なプロトコルを除き、「非信頼」ネットワークおよびホストからのすべてのトラフィックを拒否するファイアウォール設定を構築する。

この PCI 要件は、インターネット エッジの Cisco FWSM を使用すると満たされます。

このソリューションでは、次のビジネス関連の通信機能を使用できました。

- 監視、分析、および応答システム (CS-MARS)
- CiscoWorks Network Compliance Manager (C-NCM)
- CS-ACS に対する TACACS を介した AAA
- NTP によるタイム スタンプ同期化
- システム ロギング アクセスによるネットワーク イベント
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)
- 上記以外の機能は暗黙的に拒否されます。

インターネット エッジ Cisco FWSM の外部インターフェイス (インターネットで接続できる) の設定例を次に示します。

```
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** — ダイナミック パケット フィルタリングとも呼ばれるステートフル インスペクションを実装する（つまり、ネットワークに対して「確立された」接続のみが許可される）。

ソリューションのステートフル インスペクションはシスコの推奨設定です。文のデフォルトポートに異常がないかどうか、文によりプロトコルが検査され、各セッションの確立済みダイナミック接続テーブルが維持されます。使用されていないプロトコルの検査は無効にすることを推奨します。

設定例を次に示します。

```
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** — 特に許可されているものを除き、すべてのインバウンドおよびアウトバウンドのトラフィックを拒否する。

Cisco FWSM では、すべてのアクセスリストの末尾が暗黙拒否 **ip any any** です。



(注) アクセスリストに新しい項目を入力すると、常にアクセスリストの末尾に付加されます。アクセスリストは順番に評価されるため、その項目の順序が正しいことは重要です。

- **PCI 1.5** — インターネット上での内部アドレスの変換および解読を防ぐための IP マスカレードを実装する。Port Address Translation (PAT; ポート アドレス変換) や Network Address Translation (NAT; ネットワーク アドレス変換) などの RFC 1918 アドレス空間を実装するテクノロジーを使用する。

ラボ内の PCI ソリューションは、インターネット上でルーティングできないプライベート アドレッシングを使用するよう設定されています。これらのアドレスは NAT を使用して、パブリックに使用可能なアドレス空間に変換されます。実稼働環境をシミュレーションするために、シスコでは、テストのためのパブリック IP アドレスとして IP アドレス 192.168.80.25 を使用しました。

```
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>
```

次に示すのは、大規模店舗のアドレッシング プランの例です。

```
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)

```

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E 「[Device Configurations](#)」を参照してください。

PCI 2.2 — すべてのシステム コンポーネントのための設定標準を開発する。これらの標準は、すでに知られているセキュリティの脆弱性に対処し、SysAdmin Audit Network Security Network (SANS)、National Institute of Standards Technology (NIST; 国立標準技術研究所)、および Center for Internet Security (CIS) などで定義されているような、業界で認められたシステム強化標準に準拠しているものにする。

このリストのあとの記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル (デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル) をすべて無効にする。
- **PCI 2.2.3.b** — 一般的なセキュリティ パラメータ設定がシステム設定標準に含まれることを確認する。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

Cisco FWSM モジュール上の不要なサービスを無効にします。

暗号化された管理通信のみが有効で、その他のすべてのサービスは無効でした。

設定例を次に示します。

```

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

```

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発および維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および**要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる**

このリストのあとの記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、CS-ACS および、ユーザ アカウント サービスのための Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、Cisco FWSM に対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

コンソールのタイムアウトを次のコマンドで設定します。

```
console timeout 15
```

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、ここで説明している下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

Cisco ISR ルータは、CS-ACS を使用しなかった場合は AAA 機能向けに設定されず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

設定例を次に示します。

```
!
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** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
- **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する（組織内の2、3 台の中央時間サーバは、外部からの時間信号を受信[特殊なラジオ、GPS 衛星、または、国際原子時間およびUTC（以前の GMT）に基づくその他の外部ソースから直接] し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する）。
- **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスで提供されるようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

FWSM にはスタンドアロンのクロックはありません。また、NTP をサポートしていません。そのため、スイッチのクロックの時間に基づいて動作します。

補完コントロールが必要な PCI 下位要件（FWSM）

このソリューションでは、Cisco FWSM は、すべての関連 PCI 下位要件を満たしているため、補完コントロールは不要でした。

Cisco Intrusion Detection System サービス モジュール (IDSM2)

Cisco® Catalyst® 6500 シリーズ Intrusion Detection System サービス モジュール 2 (IDSM2) は、充実した IPS 機能を、広範に配置された Cisco Catalyst シャーシを介して直接ネットワーク インフラストラクチャに統合し、スイッチド環境を保護する重要な進入防御システム (IPS) ソリューションです。この統合によりユーザは、スイッチ バックプレーンから離れて、トラフィックを直接監視できます。

一般的な注意事項 / ベスト プラクティス

- ユーザが特定の回数以上はログインを試みることができないようにアカウントをロックするよう、IDSM2 を設定します。
- IDSM2 のセキュア管理を特定のホストからのみ実行できるようにします。
- ログイン時の適切なバナー メッセージを設定します。IDSM2 を所有または管理している企業をログイン バナー警告からは特定できないようにする必要があります。バナーには、その領域がプライベートなものに見なされていることと、不正アクセスが法律の及ぶ限りにおいて訴追の対象となることを記述する必要があります。
- デフォルト パスワードおよびコミュニティ スtring を適度に複雑なものに変更します。

ソリューション コンポーネントが満たす PCI の下位要件 (Cisco IDSM2)

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- 現時点の IDSM2 には、現在のパスワード文字クラスに関する要件はありません。センサーは、PAM cracklib を使用してパスワードを強化します。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。

IDSM2 ではデフォルトで、アカウントのロックアウトが無効になっています。アカウントのロックアウトは、1 から始まるログインの失敗回数を設定して有効にします。

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

- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- IDSM2 では、ロックアウトの期間を設定できません。ユーザ アカウントは、管理者がユーザ パスワードをリセットしてアカウントをリセットするまでロックされます。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用して、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバが外部からの時間信号を受信（特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接）し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
 - **PCI 10.4.c** — 最新バージョンの Network Time Protocol（NTP; ネットワーク タイム プロトコル）を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスで提供されるようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

設定例を次に示します。

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.
```

要件 11 : セキュリティ システムおよびセキュリティ プロセスを定期的にテストする

- **PCI 11.4.a** — ネットワークでのネットワーク侵入検知システムおよび侵入防御システムのいずれか、または両方を必ず使用する。カード所有者データ環境での重要なネットワーク トラフィックがすべて監視されていることを確認する。

- **PCI 11.4.c** — IDS/IPS 設定を調べて、IDS/IPS デバイスがベンダーの指示に従って構成、維持、および更新されており、保護機能が最適であることを確認する。

```
!
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
```

ここで述べる下位要件は、CS-MARS および Cisco IPS Device Manager (IDM) の監視および警告機能を組み合わせた Catalyst スイッチでの IDSM2 設定により満たされます。IDSM2 はラボでは、VLAN 82 (DMZ) および VLAN 97 (FWSM のインターフェイス内の) を監視するために無差別モードで設定されます。

IDSM2 では、Cisco Security Manager を使用して署名を更新します。

補完コントロールが必要な PCI 下位要件 (Cisco IDSM2)

- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
QSA では、文書化されたパスワード ポリシーや手動監査手順を組み合わせ、パスワードを必ず 90 日ごとに変更することを推奨しています。また、データセンター内のこれらのコンポーネントの内部ファイアウォールをセグメント化することは、これらのアプリケーション内のパスワード設定の制限に対する合理的な補完コントロールとなります。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
QSA では、文書化されたパスワード ポリシーや手動監査手順を組み合わせ、パスワードを必ず 90 日ごとに変更することを推奨しています。また、データセンター内のこれらのコンポーネントの内部ファイアウォールをセグメント化することは、これらのアプリケーション内のパスワード設定の制限に対する合理的な補完コントロールとなります。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。
QSA では、アイドルセッションのタイムアウトが使用できないか、アプリケーション/ビジネス業務 (バックアップジョブなど) に影響する場合は、スクリーンセーバーのタイムアウトを補完コントロールとして使用することを推奨しています。

Cisco Application Control Engine (ACE) モジュール

Cisco ACE モジュールは主に、データセンターおよびインターネット エッジアプリケーションでのアベイラビリティ、アクセラレーション、および保護を最大化するために使用されます。Cisco ACE モジュールは、オーディタの Report of Compliance (ROC) では文書化されていません。これは、Cisco ACE モジュールが主に ACE XML ゲートウェイ アプライアンスのロードバランシングに使用されていたが、依然としてネットワークング デバイスとして扱われており、監査の一部である他のシスコ ネットワークング デバイスと同じ推奨事項が適用されることになるためです。

要件 1: カード所有者データを保護するよう設定されたファイアウォールを設置し、維持する

ソリューション コンポーネントが満たす PCI の下位要件 (ACE)

- **PCI 1.3.7** — 特に許可されているものを除き、すべてのインバウンドおよびアウトバウンドのトラフィックを拒否する。

明示的に許可されていないすべてのトラフィックを拒否します。

設定例を次に示します。

```
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#
```

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する（たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など）。

必要な複雑さと長さを備えたパスワードをローカルアカウントに設定します。

このリストのあとの記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル（デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル）をすべて無効にする。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

要件 6：セキュリティで保護されたシステムおよびアプリケーションを開発および維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8：コンピュータにアクセスする各ユーザに一意的 ID を割り当てる

このリストのあとの記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意的ユーザ名をつける。
- **PCI 8.2** — 一意的 ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス（SecurID、証明書、または公開キーなど）
 - 生体認証

- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、CS-ACS および、ユーザ アカウント サービスのための Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、ルータに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

Cisco ACE で **terminal session-timeout** コマンドおよび **login timeout** コマンドを 15 分以下に設定します。

設定例を次に示します。

```
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
!
```



(注) **login timeout** コマンドの設定は、**terminal session-timeout** コマンドの設定より優先して使用されます。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、ここで説明している下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

Cisco ISR ルータは、CS-ACS を使用しなかった場合は AAA 機能向けに設定されず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み

- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

```
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 ゲートウェイ

ACE XML ゲートウェイは、統合 XML ファイアウォールを提供します。このゲートウェイにより、XML メッセージがセキュリティで保護され、指定されたターゲットに効率よく到達できるようになります。ACE XML ゲートウェイは包括的な XML 攻撃防御システムにより、非信頼ゾーンと信頼ゾーンの間の各サービス境界で必要とされる不可欠な保護を提供します。

一般的な注意事項 / ベスト プラクティス

- Cisco ACE XML ゲートウェイのリスニング ポートの設定時には、非サービス トラフィックのために予約されたポートを使用しないようにします。これらのポートには、8200 ~ 8299 の範囲内、またはシステム コンポーネント間の管理トラフィックに使用される 514 のポートが含まれます。
- デフォルト SNMP ストリング *reactivity* の変更を強く推奨します。デフォルト SNMP ストリングは、コマンドラインで Cisco ACE XML ゲートウェイにログインして変更できます。
 - [root@AXG1 root]# vi /etc/snmp/snmp.conf
 - [root@AXG1 root]# vi /etc/snmp/snmpd.conf
 - # REACTIVITY 2.0-1
 - com2sec theUser default reactivity

ソリューション コンポーネントが満たす PCI の下位要件 (Cisco ACE XML ゲートウェイ)

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル (デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル) をすべて無効にする。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。

- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

要件 6：セキュリティで保護されたシステムおよびアプリケーションを開発および維持する

- **PCI 6.5** — *Open Web Application Security Project Guidelines* などのセキュア コーディング ガイドラインに基づいて、すべての Web アプリケーションを開発する。カスタム アプリケーションコードを見直して、コーディングの脆弱性を特定する。ソフトウェア開発プロセスでの一般的なコーディングの脆弱性の防止を実行し、次の項目に対処する。
 - **PCI 6.5.1** — 無効な入力
 - **PCI 6.5.4** — クロスサイト スクリプティング (XSS) 攻撃
 - **PCI 6.5.5** — バッファのオーバーフロー
 - **PCI 6.5.6** — インジェクションの欠陥 (*Structured Query Language [SQL; 構造化照会言語]* インジェクションなど)
 - **PCI 6.5.7** — 不適切なエラー処理
 - **PCI 6.5.9** — サービスの拒否
 - **PCI 6.5.10** — セキュアでない設定管理

詳細な構成については、[付録 D「詳細な実装および構成手順」](#)を参照してください。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。

この要件は、Microsoft Active Directory への LDAP 接続の使用により満たされました。ユーザは、[図 3-2](#)に示すように、LDAP を使用して認証されます。

図 3-2 ユーザ認証

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-im,DC=com

Password: *****

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

ROLE-TO-GROUP MAPPING

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

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

223637

- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザ パスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み

- PCI 10.2.5 — 識別および認証のメカニズムの使用
- PCI 10.3.1 — ユーザ ID
- PCI 10.3.2 — イベントのタイプ
- PCI 10.3.3 — 日付と時間
- PCI 10.3.4 — 成功または失敗の表示
- PCI 10.3.5 — イベントの開始
- PCI 10.3.6 — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

補完コントロールが必要な PCI 下位要件 (Cisco ACE XML ゲートウェイ)

このソリューションでは、Cisco ACE XML ゲートウェイは、すべての関連 PCI 下位要件を満たしており、補完コントロールを必要としません。

無線アクセス ポイントおよびコントローラ

一般的な注意事項 / ベスト プラクティス

シスコでは、無線戦略を推進しているため、小売業無線を展開するための LWAPP アーキテクチャの使用を推奨しています。自律 IOS アクセス ポイントの強化は行っていない。今後のセキュリティおよびユーザの機能強化は、LWAPP アーキテクチャ上で開発されます。

このソリューション監査中に使用される WCS サーババージョンには、外部認証の機能がありません。ただし、バージョン 4.1 以降は、TACACS または RADIUS を介して外部認証をサポートしています。4.1 より前のバージョンの場合、シスコでは、データセンター内の WCS サーバについて、文書化されたパスワードポリシー、手動監査手順、およびファイアウォールのセグメント化を組み合わせることを推奨します。

- 一意の SSID を設定する
- SSID のブロードキャストを無効にする
- デフォルトパスワードおよびコミュニティ スtring を変更する
- WPA テクノロジーを有効にする

ソリューション コンポーネントが満たす PCI の下位要件 (Unified Wireless : Wireless Access Points、Wireless Controller、および Wireless Control System)

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- PCI 2.1 — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E 「Device Configurations」を参照してください。

- PCI 2.1.1 — 無線環境の場合は、WEP キー、デフォルト SSID、パスワード、および SNMP コミュニティ スtring などの無線ベンダーのデフォルト値を変更し、SSID ブロードキャストを無効にする。WPA 対応の場合は、暗号化と認証を行う Wi-Fi Protected Access (WPA) テクノロジーを有効にする。

ステップ 1 シスコ コントローラで、管理ユーザのための管理上の制限および AAA 認証がデフォルトで設定されていることを確認します。

- ステップ 2** Unified Wireless アーキテクチャにはデフォルトの SSID はありません。初期 SSID は、コントローラ セットアップ ウィザードによって設定されます。
- ステップ 3** 「public/private」のデフォルト SNMP スtring を無効にするか、削除します。
- ステップ 4** 次のコミュニティ スtring を新規作成します。

```
config snmp community create <string>
```

```
config snmp community create <string>
```

```
config snmp community accessmode <ro/rw> <string>
```

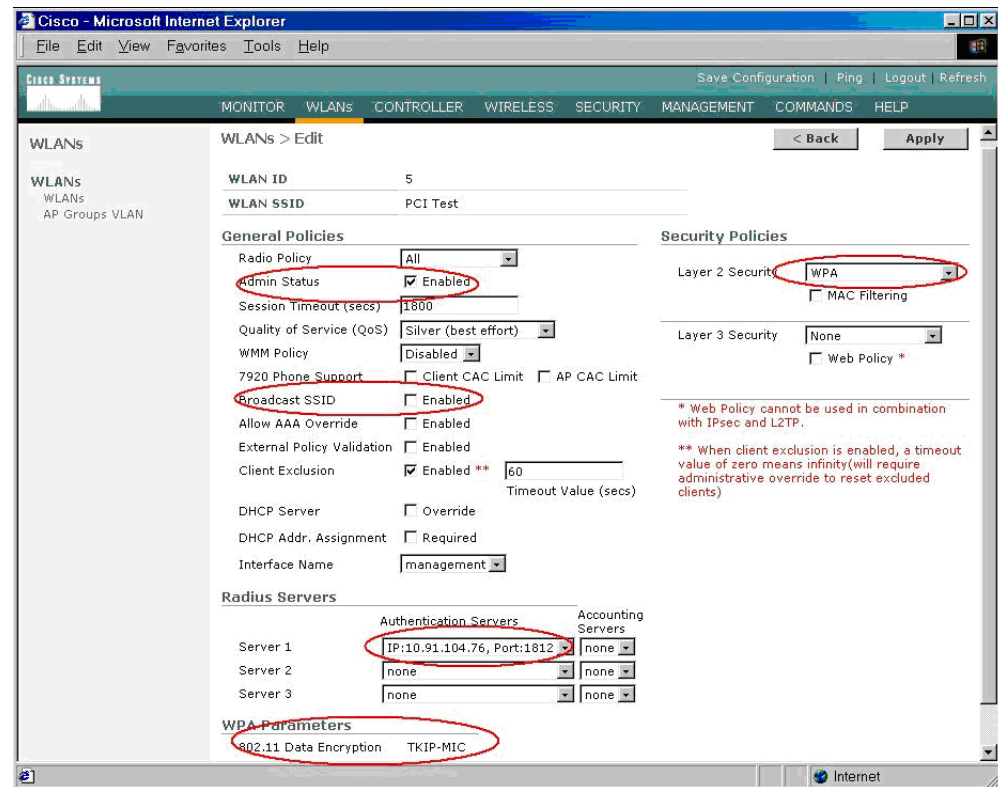
- ステップ 5** デフォルトのコミュニティ スtring にはアクセスできなくなっていることを確認します。
- ステップ 6** 初期コントローラ セットアップ スクリプトまたは CLI で、次のように管理ユーザを設定します。

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

- ステップ 7** WPA 認証のための無線システムを設定します。

SSID ブロードキャストはデフォルトで有効になっていますが、無効にすることができます。RADIUS クライアント認証を使用した、WPA セキュリティ用シスコ コントローラの WLAN の設定を 図 3-3 に示します。

図 3-3 WPA 認証のための無線システムの設定



- ステップ 8** WLAN セキュリティ設定（SSID ブロードキャストが無効、WEP/WPA を使用）が有効であることを確認します。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル（デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル）をすべて無効にする。
- **PCI 2.2.3** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。

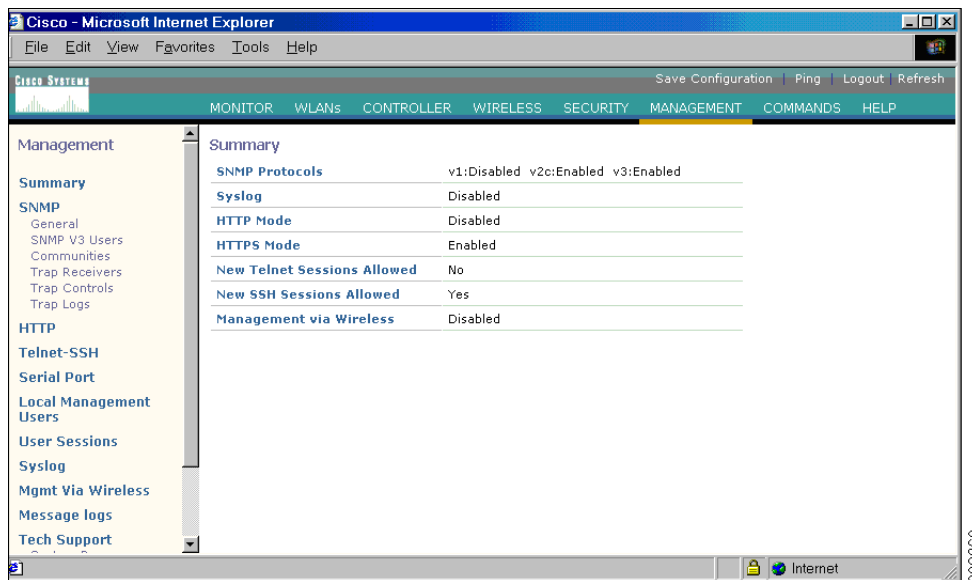
- **PCI 2.2.4** — スクリプト、ドライブ、特性、サブシステム、ファイルシステムなどのすべての不要な機能、および不要なすべての Web サーバを削除する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

設定例を次に示します。

ステップ 1 コントローラがセキュア管理プロトコルに対してのみ有効 (HTTPS [SSL] のみ、Telnet が無効、SNMP v1 が無効、SSH は許可) であることを確認します。

図 3-4 は、コントローラのデフォルト設定を示すコントローラ「Management> Summary」からの出力を示します。この設定では、HTTP が無効、Telnet が無効、および HTTPS (SSL) /SSH が有効となっています。

図 3-4 コントローラのデフォルト設定



ステップ 2 許可されていないインターフェイス / アドレスからアクセスするユーザによる管理者アクセスは拒否されることを確認します。暗号化プロトコルのみが許可されることを確認します。

- アクセス ポイント — アクセス ポイントは、コンソール ポートを除き、コントローラ経由で設定します。コンソール ポートのロールベース設定は、コントローラ経由で定義されます。
- コントローラ — コントローラの集中管理は、推奨される WCS 経由の設定方式です。コントローラのローカル管理は、CS-ACS 経由で認証を行うよう設定されます。
- WCS — WCS では、ローカルでロールベースの管理者アカウントを定義できます。

要件 4 : オープンなパブリック ネットワーク上でのカード所有者データの送信を暗号化する

- **PCI 4.1** — 強力な暗号法と、Secure Sockets Layer (SSL) /Transport Layer Security (TLS) および Internet Protocol Security (IPSEC) などのセキュリティ プロトコルを使用して、オープンなパブリック ネットワーク上での送信中に、機密性の高いカード所有者データを保護する。

PCI DSS の適用範囲内のオープンなパブリック ネットワークには、インターネット、WiFi (IEEE 802.11x)、Global System for Mobile Communications (GSM)、および General Packet Radio Service (GPRS) などがある。

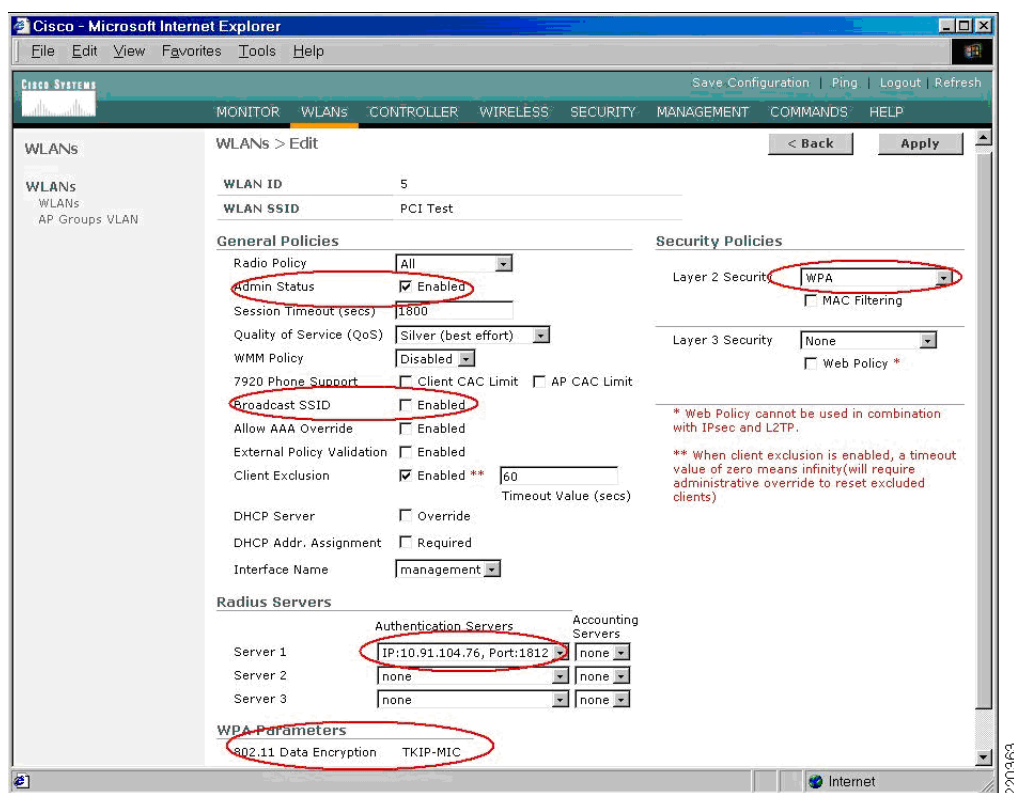
- **PCI 4.1.1** — 無線ネットワークで送信されるカード所有者データの場合は、WiFi Protected Access (WPA または WPA2) テクノロジー、IPSEC VPN、または SSL/TLS を使用して、送信を暗号化する。機密の保護および無線 LAN へのアクセスを、Wired Equivalent Privacy (WEP) のみに依存しない。

WEP を使用する場合は、次のように使用する。

- 最小の 104 ビット暗号キーおよび 24 ビット初期化値で使用する
 - WiFi Protected Access (WPA または WPA2) テクノロジー、VPN、または SSL/TLS との組み合わせでのみ使用する
 - 共有 WEP 鍵を四半期ごとに（または、テクノロジーで可能な場合は自動的に）交代で使用する
 - 鍵にアクセスできる担当者に変更が生じるたびに、共有 WEP 鍵を交代で使用する
 - メディアアクセス制御 (MAC) アドレスに基づいてアクセスを制御する

ステップ 1 WPA 認証および暗号化のための無線機器を構成します（図 3-5 を参照）。

図 3-5 WPA 認証および暗号化の設定



(注)

WLAN セキュリティデータ（つまり、WPA で使用される Pairwise Master Key [PMK; ペアマスター鍵] または 802.1X ダイナミック WEP で使用される WEP 鍵）は、WLAN コントローラに格納/キャッシュされ、クライアントアソシエーションの直後にのみ AP に転送されます。コントローラと AP の間の制御および設定トラフィックは、認証され、暗号化されます。このリンクでは AES 暗号化が使用されます。

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.1.b** — 無線ネットワークの管理コンソールにアクセスできるのは管理者のみであることを確認する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

すべての動作がコントローラにより処理されるため、アクセス ポイントはこの要件を満たしました。アクセス ポイント コンソール アクセスは、無線コントローラで設定されます。

コントローラは、CS-ACS 経由の RADIUS を介した管理ユーザ認証を使用して、この要件を満たしました。

無線クライアントは、暗号化された無線通信を有効にする前に、CS-ACS 経由の RADIUS 認証を使用します。

Wireless Control System (WCS) は、WCS サーバ自体で一意のユーザ名とパスワードを設定することで、要件 PCI 7.2 ~ 8.5.8 を満たしました。WCS は、セッション タイムアウト設定を備えていますが、RADIUS 経由の CS-ACS を利用できなかったため、要件 PCI 8.5.9 ~ 8.5.15 を満たしていませんでした。「[補完コントロールが必要な PCI 下位要件 \(Wireless Control System\)](#)」(p.3-38)を参照してください。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このソリューションでは、次のアクセス ポイントおよびコントローラの下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

WCS は、ローカル ユーザ データベースおよび対応するユーザ認証ポリシーを使用して、これらの要件を満たしました。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前
- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.6** — 監査ログの初期化

WCS は、WCS サーバの CSA クライアントを実装してローカル監査証跡を保護し、この要件を満たしました。

コントローラは、2 台の NTP サーバを使用するよう設定され、ここで説明した要件を満たします。

WCS サーバは、NTP を使用するように WCS サーバのオペレーティング システムを設定し、この要件を満たしました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
- **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する（組織内の 2、3 台の中央時間サーバは、外部からの時間信号を受信 [特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接] し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する）。
- **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスで提供されるようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

CSA クライアントは、次の要件を満たすよう、WCS サーバに適用され、ログと監査証跡を監視するよう設定されました。

- **PCI 10.5.1** — 業務に必要な担当者のみ監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。

WCS のみ

- **PCI 10.5.4** — 内部 LAN のログ サーバに無線ネットワークのログをコピーする。

コントローラは、Syslog を CS-MARS アプライアンスに送信するよう設定されます。



(注) 現時点では、無線イベントに関する文書化された標準はありません。

要件 11：セキュリティ システムおよびセキュリティ プロセスを定期的にテストする

- **PCI 11.1.b** — 少なくとも四半期ごとに、無線アナライザを使用してすべての無線デバイスを識別する。

LWAPP 統合無線システムは無線アナライザ機能を備えています。Verizon Business により、無線コントローラが継続して、不正 AP および無線デバイスをスキャンおよび検出するよう設定されていることが確認されています。

設定例を次に示します（コントローラの CLI）。

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

補完コントロールが必要な PCI 下位要件（Wireless Control System）

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

ここで説明する内容は WCS サーバのみに適用されるもので、無線コントローラにもアクセス ポイントにも適用されません。

- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗したあとはユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。



注意

WCS は外部認証方式をサポートしていません。また、Active Directory、CS-ACS、およびその他の認証ソリューションのいずれも利用できませんでした。WCS は、ローカルの個々のユーザパスワード持続時間実施、パスワード複雑度、パスワード履歴、自動失敗ロックアウト機能のいずれも備えていません。

コンプライアンスのための補完コントロール

QSA では、文書化されたパスワードポリシーや手動監査手順を組み合わせ、パスワードを必ず 90 日ごとに変更すること、およびデータセンター内の WCS サーバのファイアウォールのセグメント化を推奨しています。これは、これらのアプリケーション内のパスワード設定を制限するための合理的な補完コントロールといえます。

下位要件は、このラボ環境では満たされていませんでした。これは、データセンター インフラストラクチャおよび企業のポリシーは監査の適用範囲外で、QSA 推奨の補完コントロールを導入できないためです。

補完コントロールが必要な PCI 下位要件 (Wireless Controller)

要件 8 : コンピュータにアクセスする各ユーザーに一意の ID を割り当てる

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザーに要求する。



注意

コントローラの Web ベース インターフェイスは、15 分のタイムアウトをサポートしていません。コントローラの SSH 端末インターフェイスは、15 分のタイムアウトをサポートしています。

コンプライアンスのための補完コントロール

シスコでは、Wireless Controller のローカル Web ベース管理を無効にすることを推奨しています。Wireless Controller の設定管理には、中央 WCS サーバを使用する必要があります。

Adaptive Security Appliance (ASA)

一般的な注意事項 / ベスト プラクティス

- ASA は、小規模、中規模、大規模のサイズおよびスループット レベルでのファイアウォール、侵入防御、および侵入検知のサービスを組み合わせた多目的セキュリティ アプライアンスです。
- 一部の小売業者は、非信頼 WAN 接続（インターネットまたはマネージド サービス プロバイダーからの接続）を使用するため、ASA を店舗レベルで使用しています。
- 小売業者の多くは、より大規模なアプライアンスで非常に高いスループット レベル（1 Gbps 超）をサポートするため、データセンター内で ASA を使用しています。これは、店舗 WAN からの VPN 接続またはインターネット ベースの VPN 接続を終了するためである場合があります。
- データセンターまたはインターネット エッジで ASA を使用している場合は、店舗 WAN（および支払いトラフィック）とインターネットから直接受信するトラフィックを分離することを推奨します。ほとんどの場合は、物理的に完全に分離した状態で実装されています。
- ASA は、Adaptive Security Appliance Device Manager (ASDM) を使用して簡単に設定できます。このグラフィカル インターフェイスが、このソリューションでの ASA の設定に使用されています。設定のスナップショットはすべて、ASDM を使用して提供されています。
- ASA の Intrusion Protection Service (IPS) v5.1 モジュールは、Intrusion Device Manager (IDM) グラフィック ソフトウェアを介して管理されています。設定のスナップショットはすべて、IDM インターフェイスを使用して提供されています。

ソリューション コンポーネントが満たす PCI の下位要件 (Adaptive Security Appliance)

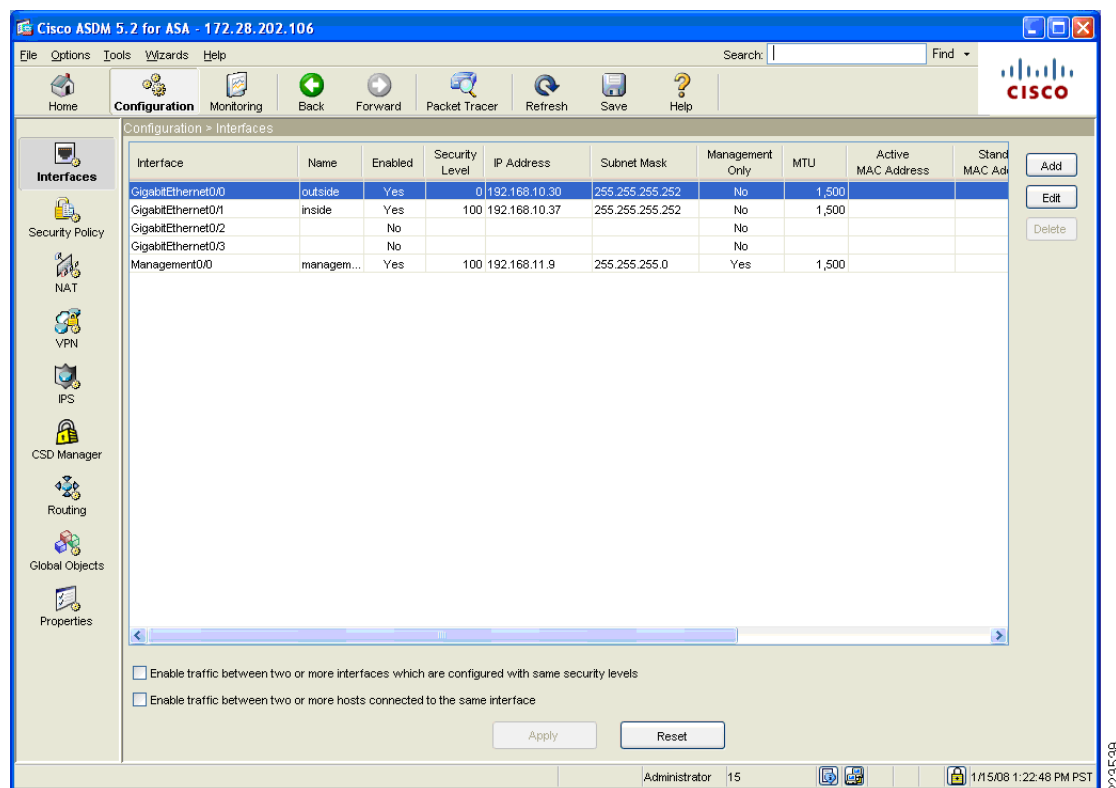
要件 1 : カード所有者データを保護するよう設定されたファイアウォールを設置し、維持する

- **PCI 1.2** — カード所有者データ環境に必要なプロトコルを除き、「非信頼」ネットワークおよびホストからのすべてのトラフィックを拒否するファイアウォール設定を構築する。

ASA のインターフェイスは、内側のインターフェイス（LAN 側）が外側のインターフェイスよりセキュリティが高くなるよう設定されました（図 3-6 を参照）。この場合、選択された値は 0 と 100 でしたが、これらの値には互いに相対的な意味しかありません。

各インターフェイスには、0（最低）～ 100（最高）のいずれかのセキュリティ レベルを割り当てる必要があります。たとえば、内側のホスト ネットワークのような、最もセキュリティの高いネットワークにはレベル 100 を割り当てる必要があります。インターネットに接続された外側のネットワークにはレベル 0 を、DMZ などのその他のネットワークにはその中間のレベルを割り当てることができます。複数のインターフェイスに同じセキュリティ レベルを割り当てられます。

図 3-6 ASA インターフェイスの設定



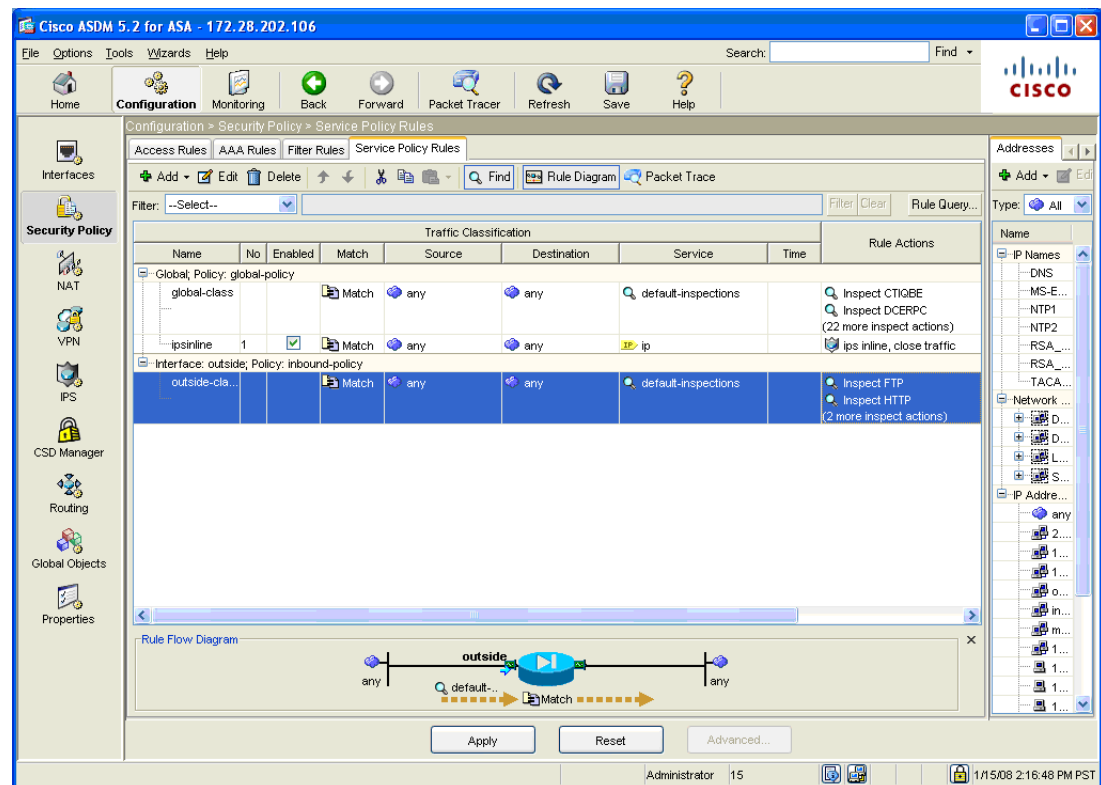
ASA は、大規模店舗とデータセンター間で次のようなビジネス関連の通信のみを許可するように設定されました。

- CiscoWorks Network Compliance Manager (NCM)、Cisco Security Manager (CS-M)、および CiscoWorks (C-LMS) の管理プロトコル
- 監視、分析、および応答システム (CS-MARS)
- CS-ACS に対する TACACS を介した認証、認可、およびアカウントティング
- ネットワーク トラブルシューティング プロトコル (ICMP)
- Network Time Protocol (NTP; ネットワーク タイム プロトコル) によるタイム スタンプ同期化
- ネットワーク イベントのシステム ロギング アクセス
- Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)

- データセンターの WAN 集約セグメントにある ASA の外側に配置されたルータ、および大規模店舗ネットワークに配置されたルータと RSA Key Manager クライアントへのセキュア管理アクセス用 SSL
- DHCP
- RSA File Security Manager サーバと File Security Manager クライアント (TCP ポート 19978、5766) 間の通信
- 大規模店舗とデータセンターに配置された NCR POS システム間の通信 (FTP および SSH)
- PCI 1.3.3** — ダイナミック パケット フィルタリングとも呼ばれるステートフルインスペクションを実装する (つまり、ネットワークに対して「確立された」接続のみが許可される)。
- PCI 1.3.5** — カード所有者データ環境に必要なものに限るようにインバウンドおよびアウトバウンドのトラフィックを制限する。

ASA は、店舗ブランチ ネットワークからのインバウンドトラフィックをすべてフィルタリングおよび検査するよう設定されています (図 3-7 を参照)。QSA との綿密な面談と討議の結果、すべてのインバウンドネットワークトラフィックのフィルタリングを実装してもよいという決定が下されました。これにより、アウトバウンドトラフィックが効率的に制限されます。

図 3-7 ASA アプライアンスのインスペクション ルール



- PCI 1.3.7** — 特に許可されているものを除き、すべてのインバウンドおよびアウトバウンドのトラフィックを拒否する。

各ファイアウォールルールセット内で明示的には許可されていないすべてのトラフィックを拒否し、ログに記録します。

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

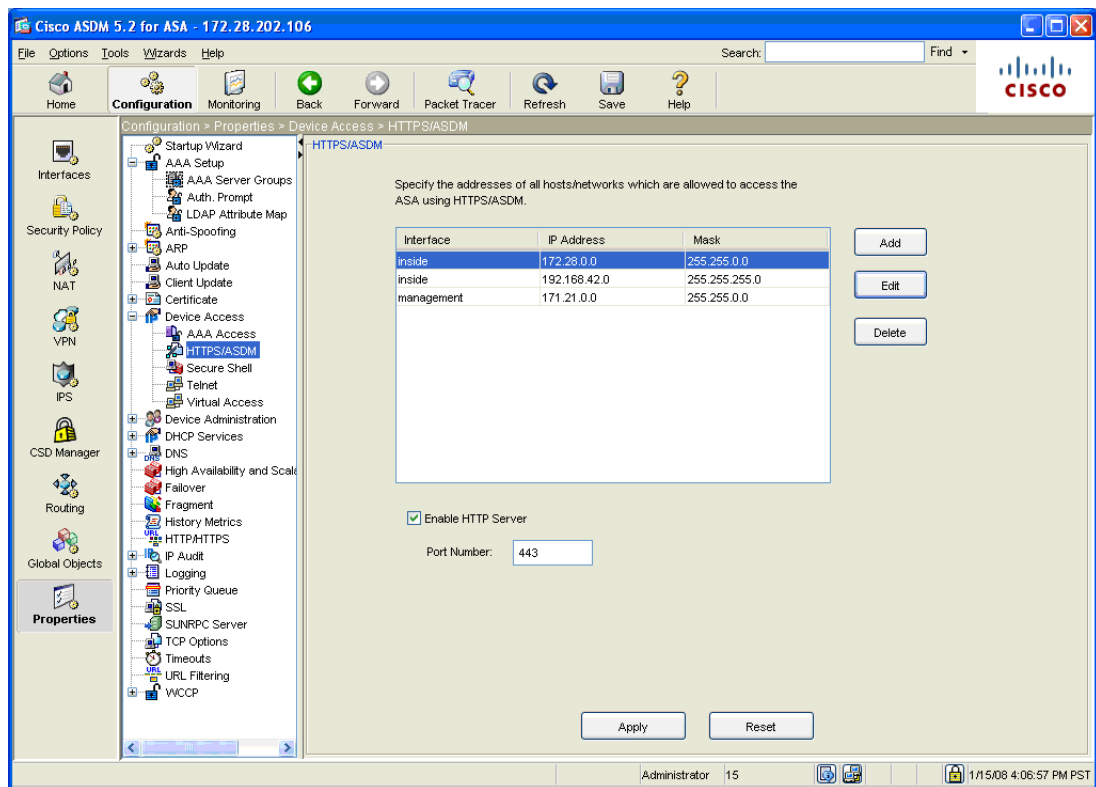
必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル（デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル）をすべて無効にする。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

HTTPS が ASA で有効になっており、Adaptive Security Device Manager (ASDM) 経由のアクセスを含む、ASA へのすべての Web アクセスが SSL により保護されました。この設定では、HTTP アクセスは無効でした。ASA への SSH アクセスは有効で、その結果、Telnet アクセスは無効でした。図 3-8 を参照してください。

図 3-8 ASA の HTTP 設定および HTTPS 設定

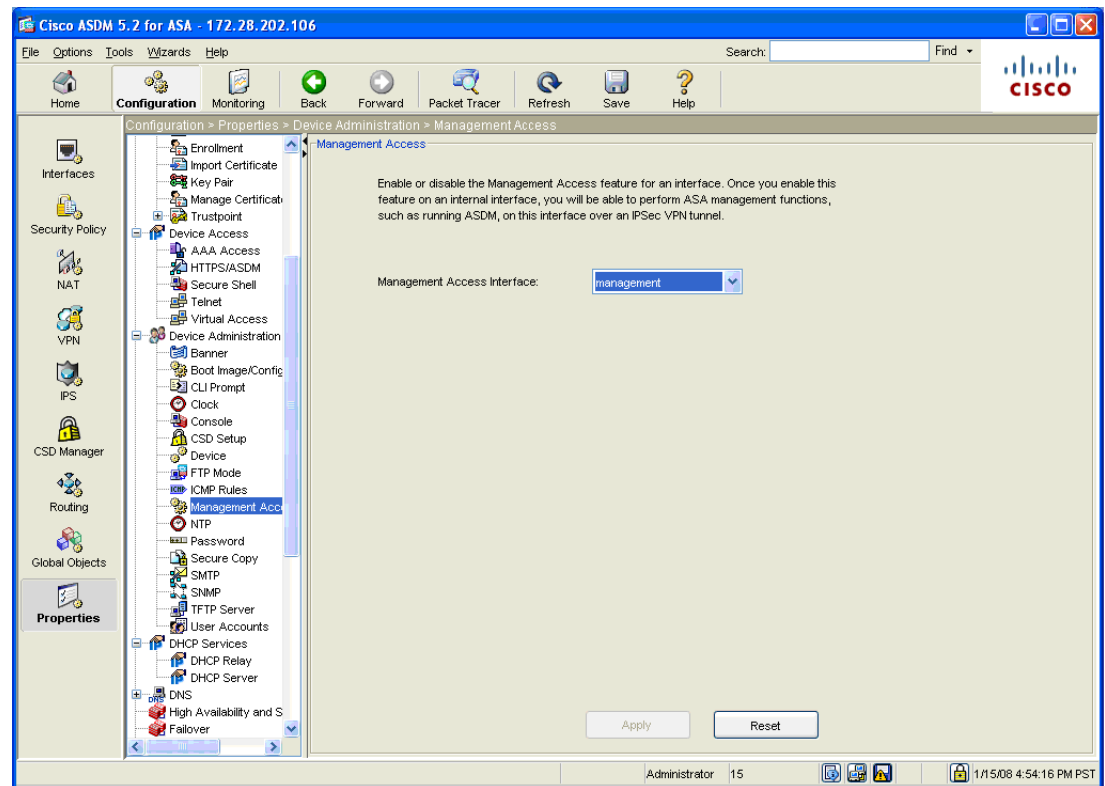


- **PCI 2.2.3.b** — 一般的なセキュリティ パラメータ設定がシステム設定標準に含まれることを確認する。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。

ASA は、セキュリティ ベスト プラクティス 標準に従って設定されました。次の設定により、デバイス自体へのセキュアアクセスが保証され、ASA 全体のトラフィックのセキュリティが強化されました。

- 各インターフェイスのアンチスプーフィング (図 3-9)

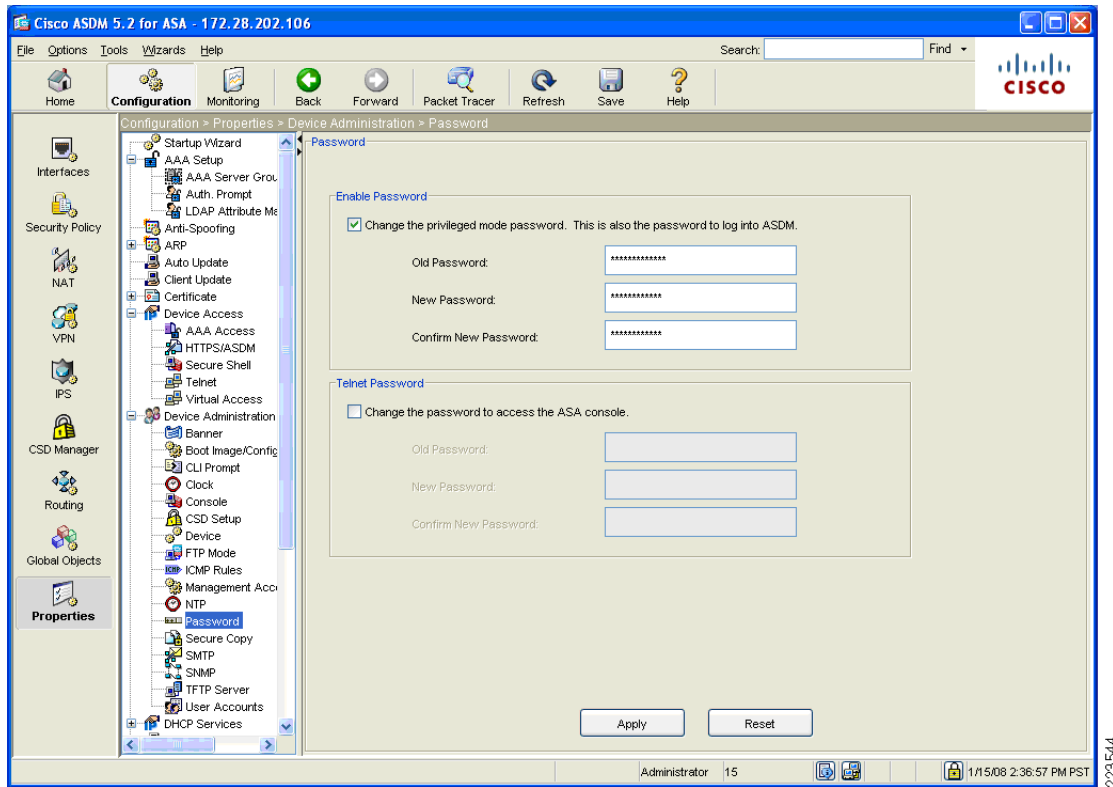
図 3-9 ASA のアンチスプーフィング設定



223543

- ・ 帯域外管理ポートのみに制限された管理アクセス（図 3-10 を参照）

図 3-10 ASA の帯域外管理設定



223544

- ・ イネーブルパスワードなどのデフォルトパスワードをデフォルト以外の値に設定 (図 3-11)

図 3-11 ASA のデフォルトパスワード設定

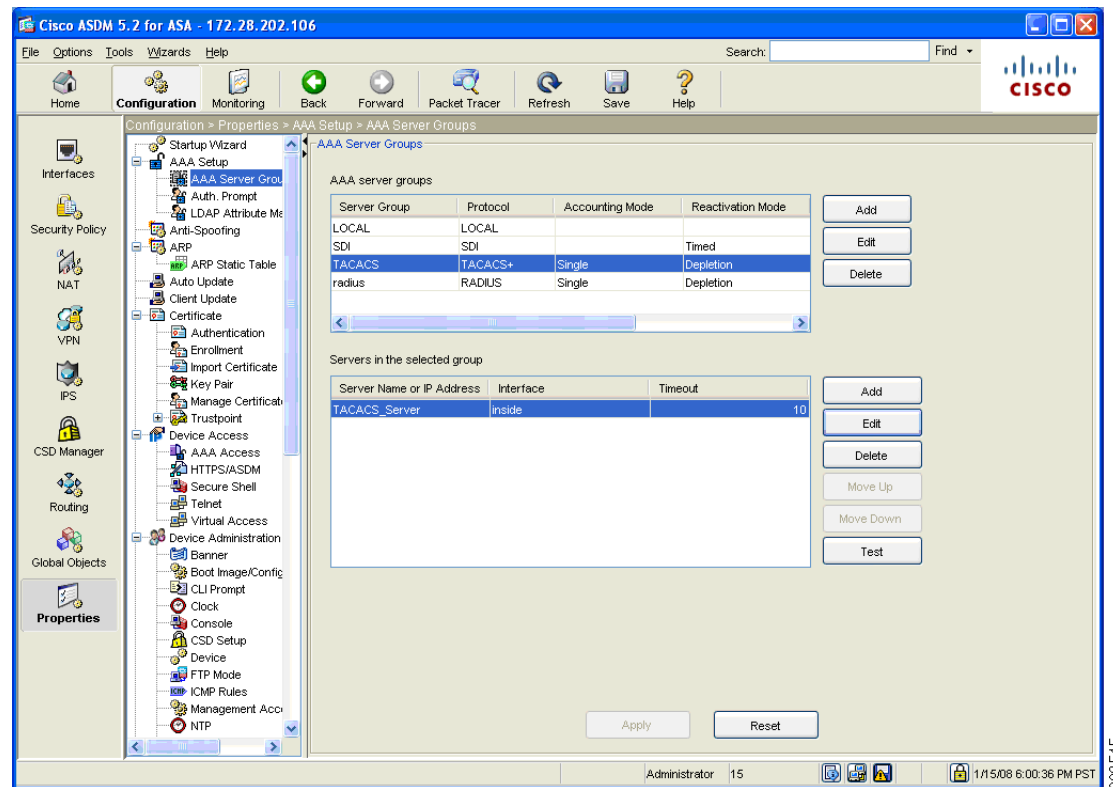
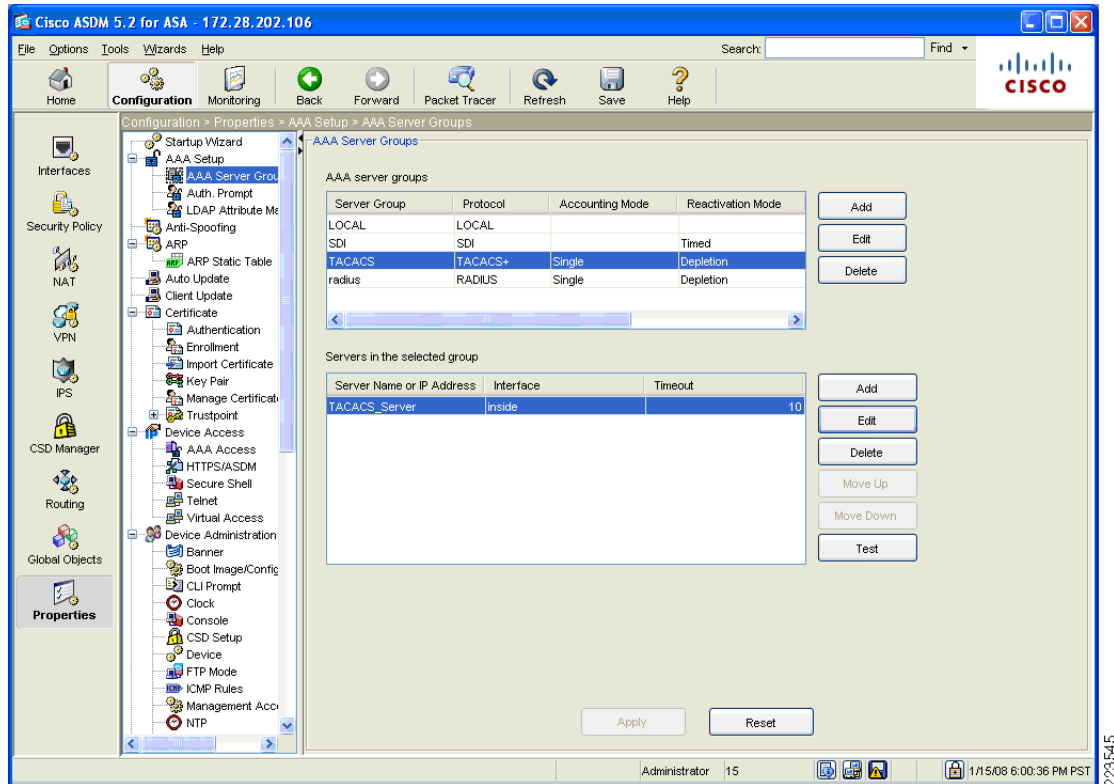


図 3-12 要件 7.2 のための外部 TACACS 認証



要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および
 要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このリストの後の記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークンデバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。

- **PCI 8.5.13** — アクセスを6回試みて失敗した後はユーザIDをロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は30分、または管理者がユーザIDを有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、ユーザアカウントサービスのためのCS-ACSおよびMicrosoft Active Directoryの実装により満たされました。

CS-ACSに到達できない場合のフォールバック認証は、ASAに対してローカルに設定されました。これらのフォールバックアカウントは、QSA推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が15分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

セッションタイムアウトを設定できるのは、ASAへのSSH、Telnet、およびコンソールアクセスのみです。ASDMでASAを管理している場合は、ASDMがインストールされたワークステーションを、アイドル時間が15分間続いた後に、パスワードで保護されたスクリーンセーバーが起動するよう設定できます。要件2により、Telnetを使用したデバイス管理は使用できません。[図 3-13](#) および [図 3-14](#) は、ASDMを介してSSHおよびコンソールのセッションタイムアウトを設定したスナップショットを示しています。

図 3-13 SSHのセッションタイムアウト

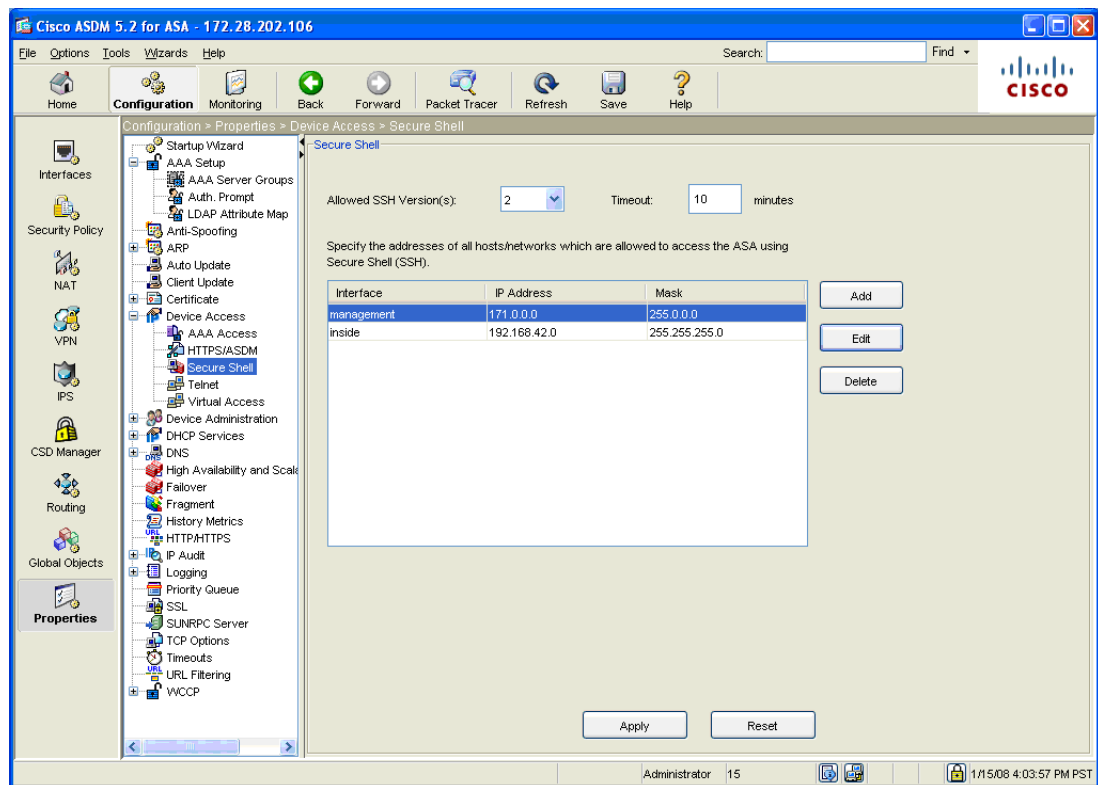
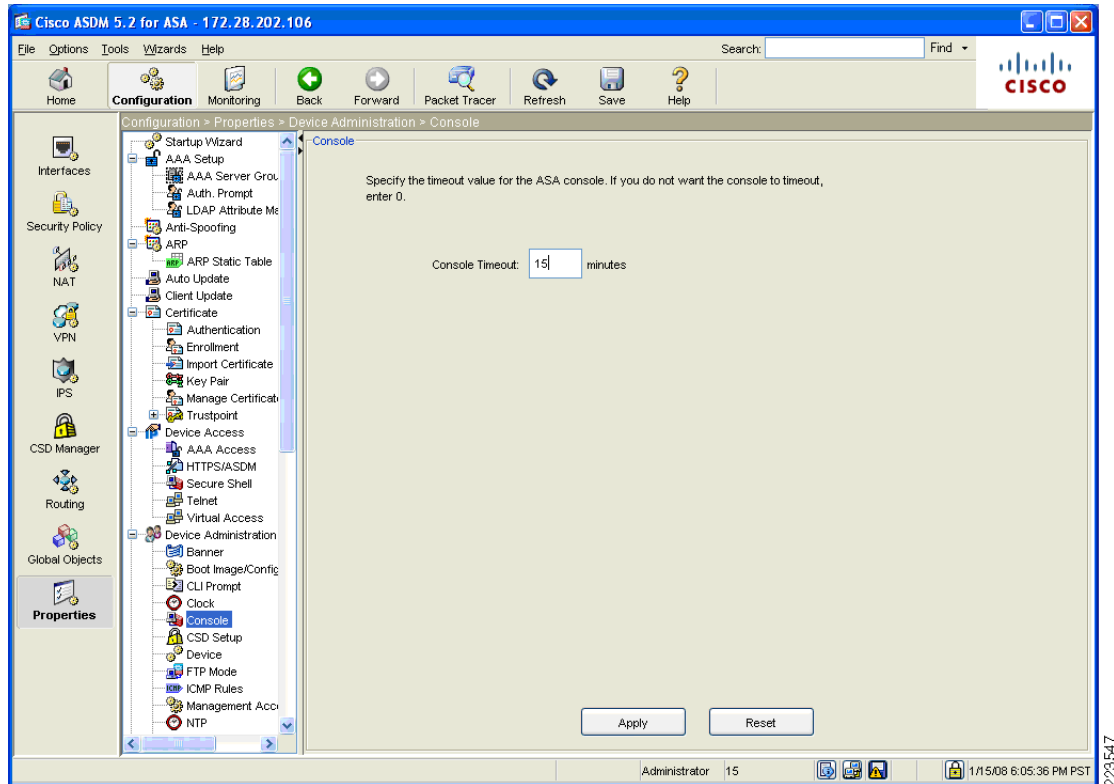


図 3-14 コンソールのセッション タイムアウトの設定



このソリューションでは、ここで説明している下位要件は、AAA サービスのための CS-ACS の実装により満たされました。時間の同期化は中央 NTP サーバで設定され、Syslog は中央 CS-MARS サーバに送信されるよう設定されました。図 3-15、図 3-16、および次の図 3-17 を参照してください。

ASA ファイアウォールは、CS-ACS を使用しなかった場合は AAA 機能向けに設定されておらず、監査も行われませんでした。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前
- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
- **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。

- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する（組織内の2、3 台の中央時間サーバは、外部からの時間信号を[特殊なラジオ、GPS 衛星、または、国際原子時間およびUTC（以前の GMT）に基づくその他の外部ソースから直接] 受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する）。
- **PCI 10.4.c** — 最新バージョンの *Network Time Protocol (NTP; ネットワーク タイム プロトコル)* を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。

図 3-15 要件 10.4.a を満たすよう設定された NTP サーバ

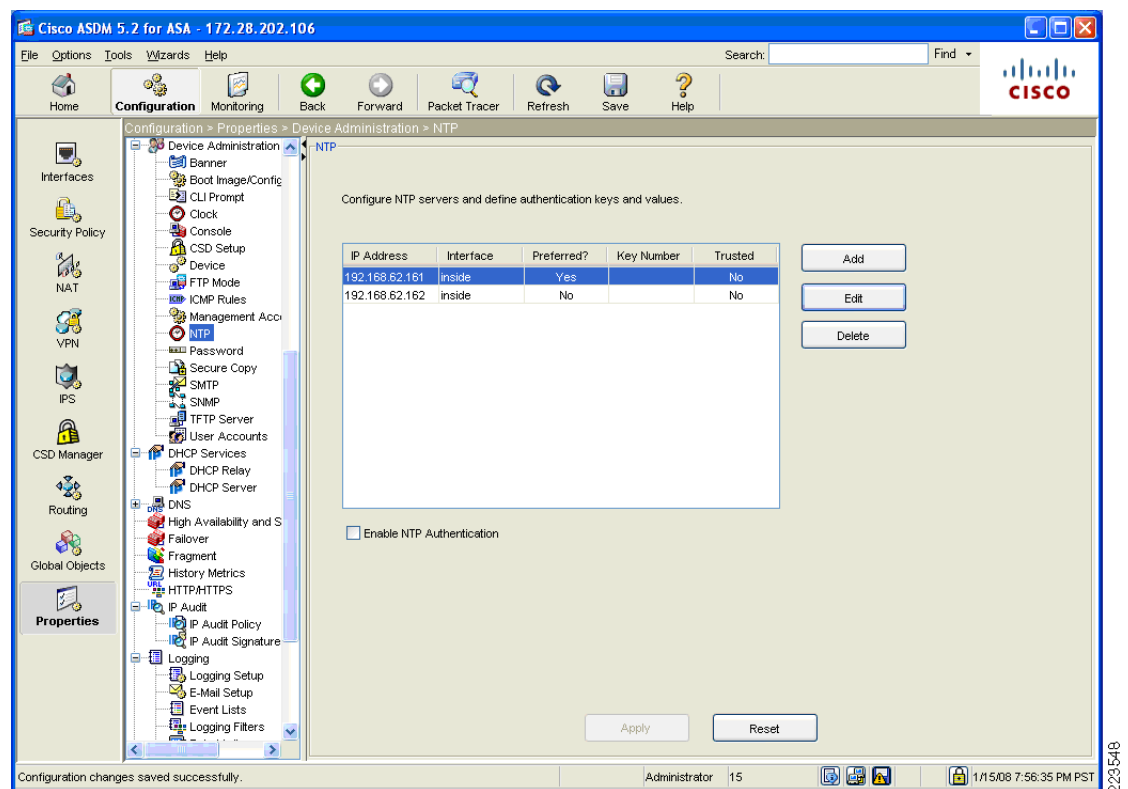
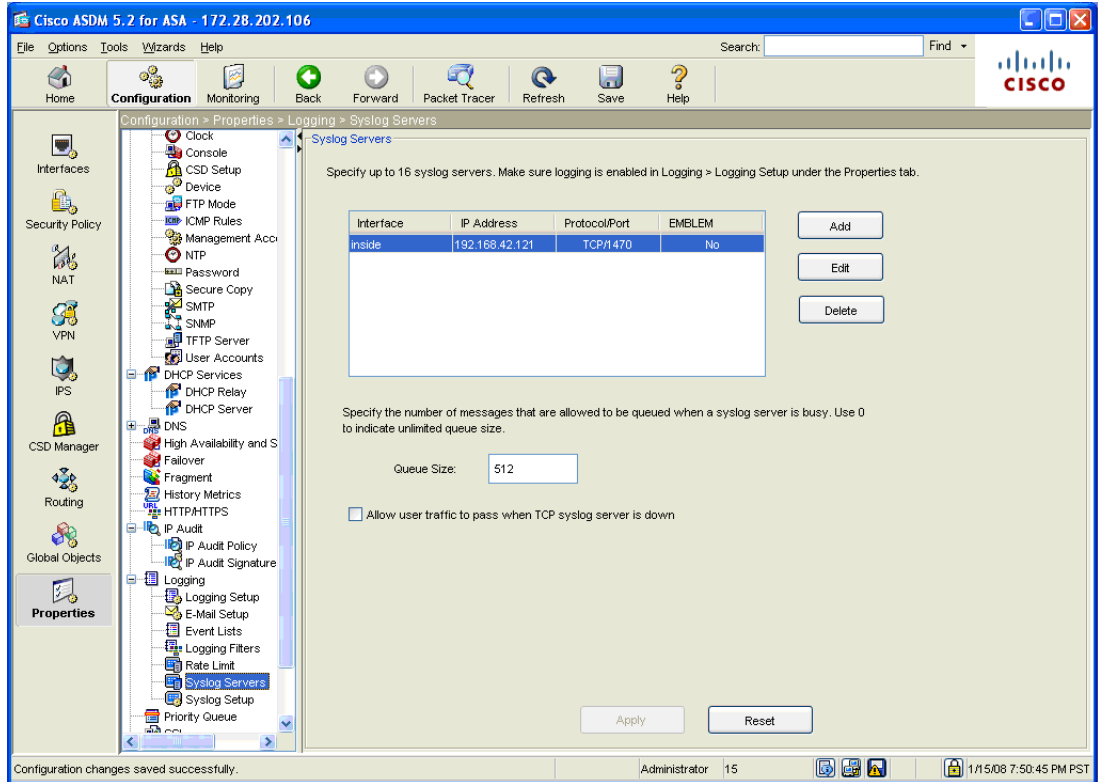
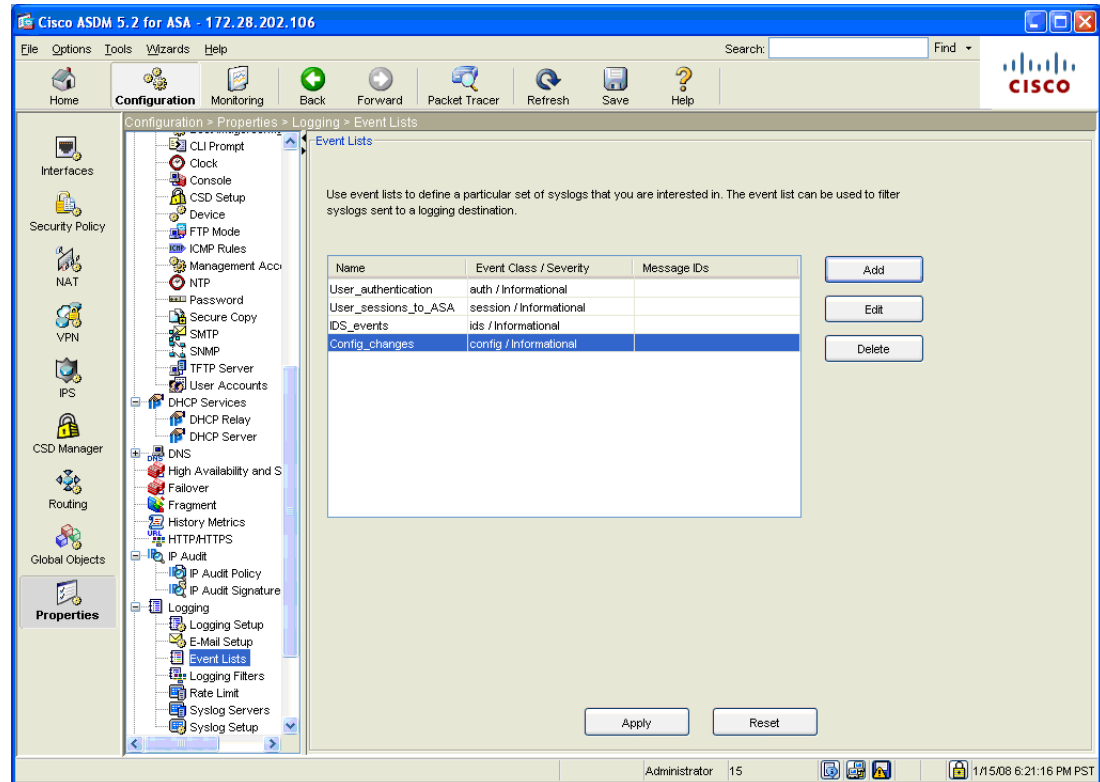


図 3-16 CS-MARS サーバを指すよう設定された Syslog サーバ



223549

図 3-17 CS-MARS へのログを作成するよう設定された Syslog イベント



- **PC 11.4** — ネットワーク侵入検知システム、ホストベースの侵入検知システム、および侵入防御システムを使用して、すべてのネットワークトラフィックを監視し、侵害が疑われる場合は担当者に警告する。すべての侵入検知および侵入防御のエンジンを最新の状態に保つ。

IPS v5.1 を搭載した AIP-SSM-20 モジュールが、店舗ブランチとデータセンター間のトラフィック用の ASA の IDS/IPS サービスに使用されました。IDS/IPS システムの強度を評価する際に、QSA は次のパラメータを考慮します。

- 使用可能な定義済みの署名の数。QSA は一般に、数を指標とみなします。このソリューションでは、2000 個を超える署名が使用可能で、十分であると見なされました。
- IPS モジュールには、それ自体の管理インターフェイス（IPS Device Manager を介した）があるため、2.X および 8.X の要件セットが適用されます。次に、要件のリストと、IPS モジュールがそれらをどのように満たすかを示します。Device Manager 機能と PCI 要件との対応の詳細については、「Cisco Intrusion Detection System サービス モジュール (IDSM2)」(p.3-24) を参照してください。

2 ファクタ認証 RSA SecurID によるリモート アクセス用 Adaptive Security Appliance (ASA) の VPN トンネル設定

一般的な注意事項

WAN 集約レイヤの ASA が、リモート アクセス IPSec VPN トンネルの終端地点として使用されました。Cisco VPN クライアント v. 4.0.5 がインストールされた Windows クライアントが、リモート クライアントとして使用されました。

リモート アクセス設定のための VPN トンネル グループおよびポリシーの詳細な設定については、次の URL にある『Cisco ASA 5500 Series Getting Started Guide, Version 7.2』を参照してください。

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

システム管理

CiscoWorks LAN Management System

CiscoWorks LAN Management System (C-LMS) は、特定の PCI 1.1 要件を満たすためのネットワーク管理機能を提供します。

一般的な注意事項 / ベスト プラクティス

C-LMS は、次のモジュールを使ってインストールされました。

- Common Services (CS)

CS は稼働基盤を提供し、CiscoWorks アプリケーションによるデータおよびシステム リソースの共有を可能にします。また、アプリケーションを起動する共通デスクトップも提供し、ログイン、ユーザ ロール定義、およびアクセス権を集中化します。

- CiscoView

CiscoWorks CiscoView は Web ベースのデバイス管理アプリケーションで、広範囲のシスコ デバイスのダイナミック ステータス、監視、および設定を提供します。CiscoWorks CiscoView は、一目でパフォーマンスとステータスを監視できる色分けされたモジュールおよびポートによって、シスコ デバイスの物理ビューをグラフィカルに表示し、ネットワーク管理に役立ちます。必要なセキュリティ権限が許可される場合は、設定機能により、デバイスを包括的に変更できます。CiscoWorks CiscoView には、次の利点があります。

- シスコ デバイスの前面パネルと背面パネルのリアルタイム表示
- デバイスのパフォーマンス、デバイス環境のステータス、および mini-Remote Monitoring (mini-RMON) の監視
- 直接のデバイス設定変更
- CiscoWorks LAN Management Solution 共通デバイス インベントリの利用
- きめ細かく CS-ACS 認証された複数ユーザ アクセス ルールの定義

- Campus Manager

CiscoWorks Campus Manager は、複雑な物理および論理レイヤ 2 インフラストラクチャを構成して管理し、理解するための強力なツールを提供します。CiscoWorks Campus Manager には、次のツールが含まれます。

- User Tracking (および End-host Tracking)
- Discrepancy Reporting

- Topology Services
- VLAN、プライベート VLAN (PVLAN)、および VLAN Trunking Protocol (VTP) 管理
- スパニングツリーの管理と仮想化
- Path Analysis
- Data-extraction Engine

- Resource Manager Essentials (RME)

CiscoWorks RME は、シスコ ネットワーク デバイスのライフサイクル管理を提供します。人的エラーを削減し、ネットワークの保守に関連する手作業の多くを排除するために設計された RME を使用すると、シスコ ネットワークの管理可能性と可用性を最大限に高めることができます。RME スイートには、シスコ ネットワークの管理を簡素化する次のツールが含まれます。

- Inventory Management
- Device Configuration Management
- Software Image Management
- Change Audit Services
- Syslog Analysis

- Device Fault Manager (DFM)

CiscoWorks DFM は、シスコ デバイスのリアルタイムの障害分析を実行します。さまざまなデータ収集とデータ分析の技術により、CiscoWorks DFM はインテリジェントトラップを生成します。このトラップは、ネットワークに設置された他のイベント管理システムに転送したり、E メール / ポケットベル ゲートウェイに送信したりできます。また、DFM アラームウィンドウに表示することもできます。DFM 機能には、次のものが含まれます。

- 問題焦点型障害分析
- CiscoWorks のデスクトップおよびサーバとの統合
- 企業管理システムとの統合
- レイヤ 2 およびレイヤ 3 シスコ デバイスのサポート
- 差分デバイス サポート

CiscoWorks Common Services は [Server] > [Security] で Browser_server_security_mode を有効にして、設定されました。さらに、CS-ACS AAA モードが認証オプションとして選択されています。

図 3-18 は設定例を示します。

図 3-18 Common Services の設定

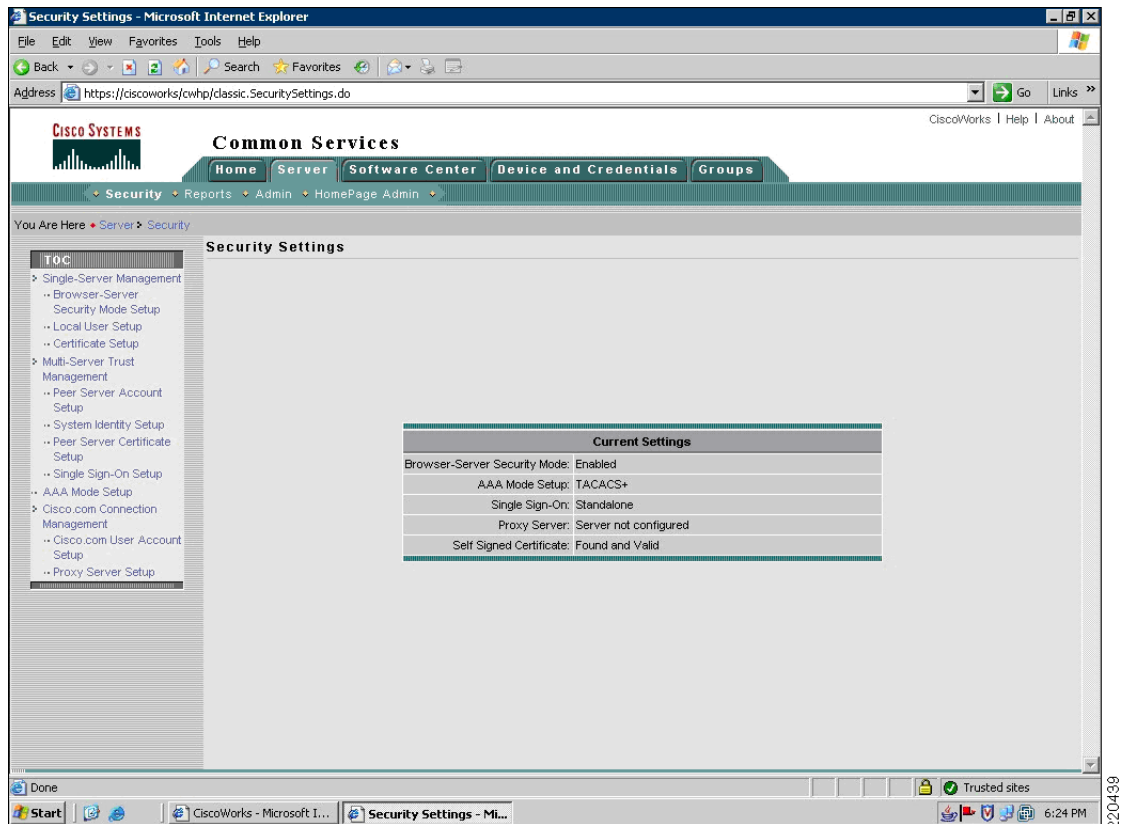
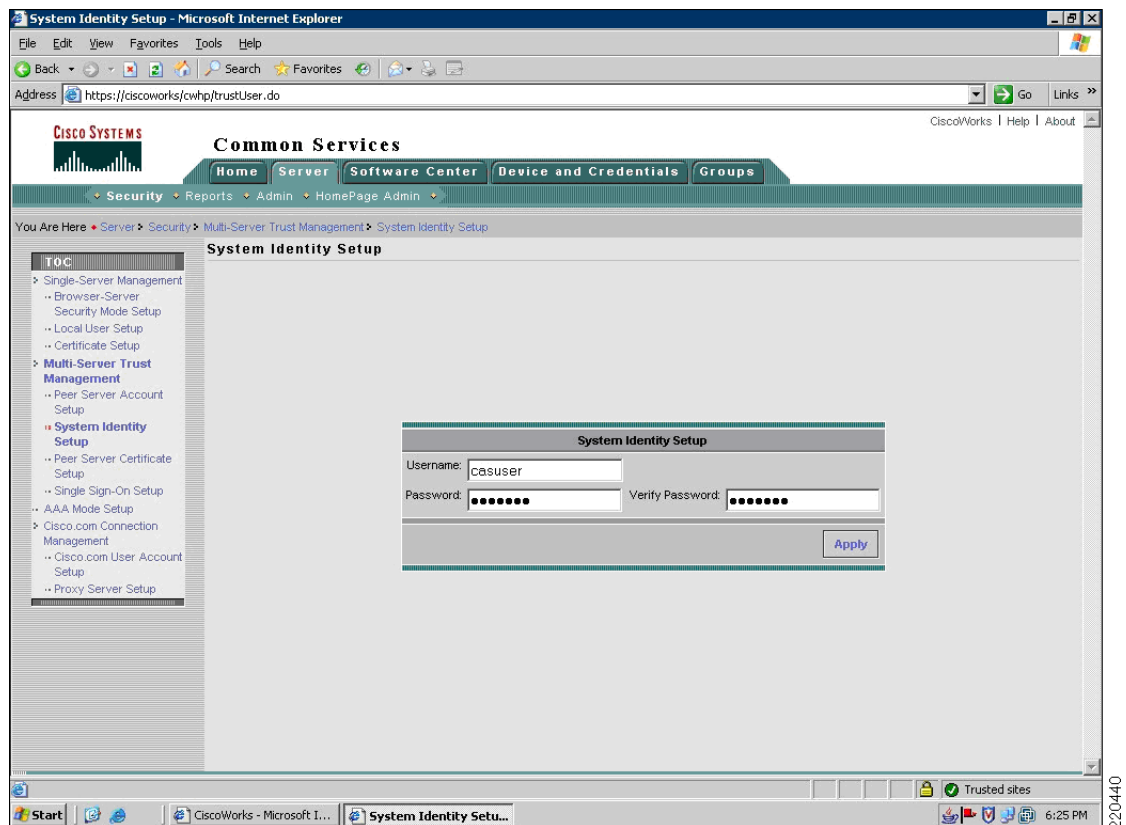


図 3-19 に示すように、システム アイデンティティ ユーザを変更します。

図 3-19 システム アイデンティティ ユーザ名の設定



CiscoWorks を使用して、ルータとスイッチを更新し、PCI 6.1 に必要なスケジュールに合わせるすることができます。

ソリューション コンポーネントが満たす PCI の下位要件（C-LMS）

要件 1：カード所有者データを保護するよう設定されたファイアウォールを設置し、維持する

- **PCI 1.3.6** — ルータのコンフィギュレーションファイルのセキュリティ保護と同期化。たとえば、実行コンフィギュレーションファイル（ルータの通常動作のため）およびスタートアップコンフィギュレーションファイル（マシンのリブート時）は、同一のセキュアな設定でなければならない。

C-LMS は、コンフィギュレーションファイルのデータベースを非常にセキュアな方法で維持します。このスイートには、コンフィギュレーションファイルに同期化の問題が発生すると、管理者に警告する機能があります。また、このシステムには同期化の不整合を修正する機能もあります（RME）。シスコのスイッチはルータ同様に、この機能を備えているため、付加価値があります。

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する（たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など）。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E「Device Configurations」を参照してください。

- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

管理コンソールは、HTTPS アクセスをサポートするよう設定されており、HTTP アクセスは無効でした。CiscoWorks は、高度なセキュア管理ポータルテクノロジーとして SSL を使用するよう設定され、プライマリ設定プロトコルとして SSH および SNMPv3 を使用します。

ロールベース管理は管理タスク用に設定されました。



(注)

すべてのシステム コンポーネントに対する適切なセキュリティ設定を含むサーバ機能強化は、小売業者 / サービス プロバイダーが行う必要があります。

要件 6：セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

- **PCI 6.2 (6.2b)** — 新しく発見されたセキュリティの脆弱性（インターネット上で自由に警告サービスに登録できる、など）を識別するプロセスを確立する。標準を更新して、新しい脆弱性問題に対処する。

C-LMS は、ルータとスイッチのシステム設定変更履歴を維持し、変更された場合はオペレータに警告するため、設定変更プロセスの実行に役立ちます。また、C-LMS には、まったく変更が行われない例外期間を定義する機能もあります。例外は例外レポートに記入されます。

ベースライン設定情報が一貫しており、静的であることも、C-LMS によって保証されます。

ベースライン テンプレート ([RME] > [Archive Management]) を使用すると、必須項目が確実に設定されるよう、設定テンプレートを作成できます。これらの必須項目を変更すると、選択したテンプレートの確認が実行され、必須項目が含まれるようにデバイスの設定が更新されます。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード

- トークン デバイス (SecurID、証明書、または公開キーなど)
- 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、これらの下位要件は、ユーザ アカウント サービスのための CS-ACS および Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、C-LMS コンソールに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

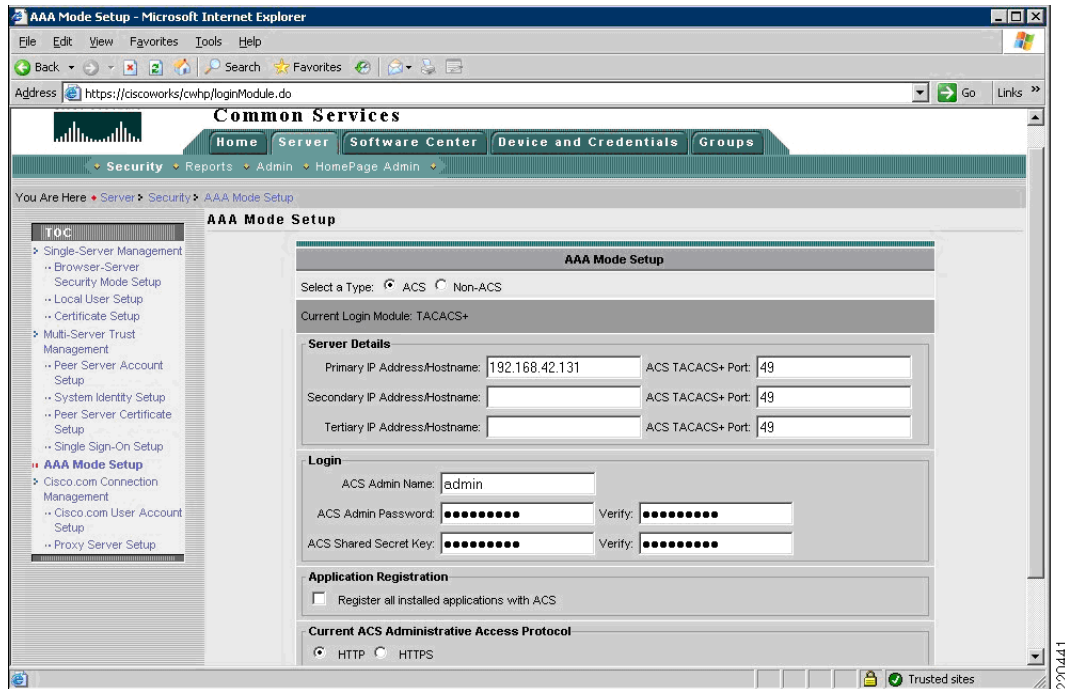
要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

このソリューションでは、これらの下位要件は、AAA サービスのための CS-ACS の実装により満たされました (図 3-20 を参照)。

図 3-20 AAA モードのセットアップ



要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

C-LMS には、この要件を満たす、ローカルでの 15 分のタイムアウト機能があります。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
 - **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
 - **PCI 10.2.4** — 無効な論理アクセスの試み
 - **PCI 10.2.5** — 識別および認証のメカニズムの使用
 - **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
 - **PCI 10.3.1** — ユーザ ID
 - **PCI 10.3.2** — イベントのタイプ
 - **PCI 10.3.3** — 日付と時間
 - **PCI 10.3.4** — 成功または失敗の表示
 - **PCI 10.3.5** — イベントの開始
 - **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前
- このソリューションでは、これらの下位要件は、AAA サービスのための CS-ACS の実装により満たされました（図 3-18 を参照）。
- **PCI 10.2.3** — すべての監査証跡へのアクセス
 - **PCI 10.2.6** — 監査ログの初期化

C-LMS は、C-LMS サーバの CSA クライアントを実装してローカル監査証跡を保護し、この要件を満たしました。

この要件は、C-LMS サーバのオペレーティング システムを、NTP を使用するように設定することで満たされました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
 - **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。
- **PCI 10.5.1** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。
- **PCI 10.5.3** — 監査証跡ファイルは、集中ログ サーバ、または変更が困難なメディアに速やかにバックアップする。

CSA クライアントは、この要件を満たすよう、C-LMS サーバにインストールされ、ログと監査証跡を監視するよう設定されました。

補完コントロールが必要な PCI 下位要件（C-LMS）

C-LMS には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

Cisco Security Manager

Cisco Security Manager は、シスコのセキュリティ アプライアンス、ファイアウォール、ルータ、およびスイッチ モジュール上でファイアウォール、VPN、および IPS ポリシーを設定するための強力な、しかも容易に使用できるソリューションです。

一般的な注意事項 / ベスト プラクティス

- 各ルールセットには、わかりやすい説明を記載します。これらの説明は、実行コンフィギュレーションの備考として表示されます。
- 一貫したインターフェイス ネーミング標準を使用して、ファイアウォール ルールセットの導入を仮想化します。
- FlexConfig を使用して、アンチスプーフィング機能をすべてのインターフェイスに適用します。

設定例を次に示します。

```
## 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
#end
```

ソリューション コンポーネントが満たす PCI の下位要件 (CS-M)

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

付録 E 「Device Configurations」を参照してください。

- PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

管理コンソールは、HTTPS アクセスをサポートするよう設定されており、HTTP アクセスは無効でした。CS-M は、高度なセキュア管理ポータル テクノロジーとして SSL を使用するよう設定され、プライマリ設定プロトコルとして SSH および SNMPv3 を使用します。

ロールベース管理は管理タスク用に設定されました。



(注)

すべてのシステム コンポーネントに対する適切なセキュリティ設定を含むサーバ機能強化は、小売業者 / サービス プロバイダーが行う必要があります。

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および**要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる**

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、これらの下位要件は、ユーザ アカウント サービスのための CS-ACS および Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、C-LMS コンソールに対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

CS-M には、この要件を満たす 15 分のタイムアウト機能があります。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み

- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

このソリューションでは、これらの下位要件は、AAA サービスのための CS-ACS の実装により満たされました。

- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.6** — 監査ログの初期化

CS-M は、CS-M サーバの CSA クライアントを実装してローカル監査証跡を保護し、この要件を満たしました。

この要件は、CS-M サーバのオペレーティング システムを、NTP を使用するように設定することで満たされました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
 - **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。
- **PCI 10.5.1** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。

CSA クライアントは、この要件を満たすよう、CS-M サーバにインストールされ、ログと監査証跡を監視するよう設定されました。

補完コントロールが必要な PCI 下位要件（CS-M）

C-SM には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

CSA Manager

Cisco Security Agent (CSA) Manager は、アプリケーション ファイアウォール、ファイルの整合性、およびホストの侵入防御サービスを提供する CSA を管理します。

一般的な注意事項 / ベスト プラクティス

- CSA クライアントを、サポートされるオペレーティング システムのすべてのサーバとワークステーションにインストールします。
- それぞれのサーバの監査証跡とログを監視するよう、ポリシーを設定します。

ソリューション コンポーネントが満たす PCI の下位要件 (CSA Manager)

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します (付録 E 「Device Configurations」を参照)。

- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

管理コンソールは、HTTPS アクセスをサポートするよう設定されており、HTTP アクセスは無効でした。CSA Manager は、高度なセキュア管理ポータル テクノロジーとして SSL を使用するよう設定され、プライマリ設定プロトコルとして SSH および SNMPv3 を使用します。

ロールベース管理は管理タスク用に設定されました。



(注)

すべてのシステム コンポーネントに対する適切なセキュリティ設定を含むサーバ機能強化は、小売業者 / サービス プロバイダーが行う必要があります。

要件 5 : アンチウイルス ソフトウェアまたはアンチウイルス プログラムを使用し、定期的に更新する

- **PCI 5.1** — ウイルスに感染しやすいすべてのシステム (とくにパーソナル コンピュータおよびサーバ) にアンチウイルス ソフトウェアを導入する。



(注)

通常、ウイルスに感染しやすいシステムには、UNIX ベースのオペレーティング システムやメインフレームは含まれません。

- **PCI 5.1.1** — アンチウイルス プログラムが、スパイウェアおよびアドウェアなどのその他の悪意のあるソフトウェアを検知して削除し、これらのソフトウェアから防御する機能を持つことを確認する。
- **PCI 5.2** — すべてのアンチウイルス メカニズムが最新のものであり、アクティブに実行され、監査ログを作成できることを確認する。

アンチウイルス ソフトウェアは、Windows システムにインストールされています。PCI アンチウイルス要件の評価の焦点は、Cisco Security Agent ソフトウェア、およびこのソフトウェアがアンチウイルス要件の目的にどの程度一致しているかによって異なります。Cisco Security Agent ソフトウェアは、ウイルスに感染しやすいすべてのシステム コンポーネントにインストールされます。次にその例を示します。

- CS-ACS コンソール
- WCS コンソール

- C-LMS コンソール
- CSA コンソール
- CS-M コンソール

Verizon Business では、アンチウイルス ソフトウェアを上記のシステム コンポーネントにインストールすることを推奨していますが、CSA ソフトウェアを他の補完コントロールと併用すると、ほとんどの一般的なウイルス感染のリスクを軽減できます。

Verizon Business は、複数のセキュリティ制御による階層的なセキュリティを提供するために、ベンダーのマニュアルを見直し、CSA の機能のデモンストレーションに出席しています。Cisco PCI Solution for Retail 環境を実装すると、次のアンチウイルス要件に対処できます。

- Cisco PCI Solution for Retail 環境には、CSA の中央（マスター）コンソールがあり、ここですべての CSA クライアント ポリシーを集中的に管理します。
- ログ生成が有効になっており、警告/ログが、CSA および CS-MARS の内部に集中的に格納されます。保持期間は、小売業者/サービス プロバイダーが決定します。ただし、このような警告は監査証跡を構築するために不可欠な場合があるため、Verizon Business では CSA 警告を、PCI 監査証跡要件に相応する 最低 1 年間は保持することを推奨しています。



(注)

POS 環境は各ベンダーによってさまざまであるため、各小売業者に対して、POS 環境、POS 環境へのインターネット/Eメールの接続性、POS 環境への企業接続性、およびすべての補完コントロールの詳細な評価を実施して、「適/不適 (In Place/Not in Place)」評価を実施する必要があります (CSA ソフトウェアがアンチウイルス ソフトウェアの補完コントロールとして使用される場合)。

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および 要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このリストの後の記述は、次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。

- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、これらの下位要件は、ユーザ アカウント サービスのための Microsoft Active Directory への LDAP 認証の実装により満たされました。

フォールバック認証：LDAP 認証に障害が発生した場合は、CSA Manager がローカルのロールベース アカウントで設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

CSA Manager には、15 分間のタイムアウトをサポートする機能があります。

要件 10：ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.6** — 監査ログの初期化
- **PCI 10.2.7** — システムレベル オブジェクトの作成と削除
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

このソリューションでは、これらの下位要件は、以下の実装により満たされました。

- Active Directory (AD) 認証ログ（直接 AD に送信される認証要求）
- すべての CSA ログ、警告 / イベントの CSA Manager への送信
- CSA 管理のローカル監査証跡
- CSA Manager には CSA クライアントをインストール
- CSA は、カード所有者データを含むすべてのファイルへのアクセスを監視するよう設定

この要件は、CSA Manager サーバのオペレーティング システムを、NTP を使用するように設定することで満たされました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。

- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間およびUTC（以前のGMT）に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
- **PCI 10.4.c** — 最新バージョンの *Network Time Protocol* (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアントマシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。
- **PCI 10.5.1** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。
- **PCI 10.5.5** — ファイル整合性の監視機能と変更検出ソフトウェアをログに使用して、既存のログデータを、警告を生成せずには変更できないようにする（ただし、新しいデータを追加する場合は警告が生成されない）。

CSA ソフトウェアは、監査証跡ファイルへのアクセスを監視して保護し、監査証跡を不正に変更しようとした場合に警告を生成するために使用されます（ログデータの書き込みを担当するアプリケーション サービスのみが監査証跡の書き込み / 変更 / 削除を実行できます）。シスコでは、監査証跡を中央のバックアップサーバにコピーする追加のバックアップ スクリプトを作成しています。このバックアップサーバでは、CSA 保護が適用され、監査証跡のバックアップを担当するアカウントを除き、すべてのアクセス、変更、削除が排除されます。

- **PCI 10.6.a** — セキュリティ ポリシーと手順を取得して調査し、1 日に1 回以上はセキュリティ ログを調べる手順が含まれ、例外に対するフォローアップが要求されていることを確認する。
- **PCI 10.6.b** — 監視と面談により、すべてのシステム コンポーネントについて定期的なログの調査が実施されていることを確認する。

CSA は、システム イベントの相関と分析を実行します。また、処置が迅速に行われるように、システム イベントに関する警告を生成するよう設定されています。



(注)

文書化されたセキュリティ ポリシーと手順により、例外に対するフォローアップを含む、セキュリティ ログの毎日の調査（小売業者 / サービス プロバイダーが実行します）が要求されている必要があります。

要件 11 : セキュリティ システムおよびセキュリティ プロセスを定期的にテストする

- **PCI 11.4.a** — ネットワークでのネットワーク侵入検知システムおよび侵入防御システムのいずれか、または両方を必ず使用する。カード所有者データ環境での重要なネットワーク トラフィックがすべて監視されていることを確認する。
- **PCI 11.4.b** — 監視を行い、侵害が疑われる場合は担当者に警告するよう、IDS と IPS のいずれかまたは両方が所定の場所に設置されていることを確認する。
- **PCI 11.4.c** — IDS/IPS 設定を調べて、IDS/IPS デバイスがベンダーの指示に従って構成、維持、および更新されており、保護機能が最適であることを確認する。

Cisco CSA（ホストベース IDS/IPS）は、管理コンソール（CS-M、C-LMS、CSA コンソール、CS-ACS、および WCS コンソールなど）にインストールされます。

CSA は、監視を行い、侵害が疑われる場合は担当者に警告するよう設定されます。

CSA（ホストベース IDS/IPS）は署名に依存しない動作ベースであるため、署名を更新する必要がありません。

- **PCI 11.5** — 重要なシステム ファイルやコンテンツ ファイルの不正な変更が疑われる場合は 担当者が警告を受け取るよう、ファイル整合性監視ソフトウェアを導入し、少なくとも毎週、重要なファイルを比較するよう設定する。

重要なファイルは、カード所有者データを含むファイルだけとは限りません。ファイル整合性を監視する場合の重要なファイルとは、一般に、定期的には変更されないが、システムへの侵入や侵害の可能性が発生した場合に変更される可能性のあるファイルです。ファイル整合性監視製品には通常、関連オペレーティング システムの重要ファイルがあらかじめ設定されています。カスタム アプリケーションのファイルなどのその他の重要ファイルは、ユーザ（つまり、小売業者またはサービス プロバイダー）が評価して定義する必要があります。

管理コンソール（C-LMS、CS-M、CSA Manager、WCS、Active Directory）のそれぞれで CSA クライアントを使用することにより、それらのサーバに対するこの要件が満たされています。CSA は、許可されているかどうかにかかわらず、疑わしいアクセスに関するログと警告を生成します。CSA はまた、重要ファイルが変更された場合にもログと警告を生成します。

補完コントロールが必要な PCI 下位要件（CSA Manager）

CSA Manager には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

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

CS-MARS は、ネットワークとセキュリティの管理者がセキュリティ上の脅威に対する監視、識別、隔離、および対処を行うためのアプライアンスベースの包括的なソリューションです。

一般的な注意事項 / ベスト プラクティス

- PNADMIN アカウントは CS-MARS アプライアンスから削除できません。このアカウントは、適切なパスワードセキュリティを使用して設定し、認可された担当者にのみ配布する必要があります。このアカウントを使用して設定を行わないでください。
- 監査時に使用される CS-MARS アプライアンスの各バージョンには、外部認証の機能がありません。ただし、v 4.3 以降の CS-MARS は、RADIUS を介した外部認証をサポートしています。シスコでは、このソリューションの監査に使用される CS-MARS のバージョン、および RADIUS 認証をサポートしない旧バージョンについては、文書化されたパスワード ポリシー、手動監査手順、およびデータセンター内のファイアウォールのセグメント化を組み合わせて使用することを推奨します。
- CS-MARS は、その監査ログとデータベースを外部 NFS サーバストレージファシリティに格納するよう設定する必要があります。
- CS-MARS では、適切な強度と複雑さによるパスワード保護が実施されません。管理パスワードの開発時には、なんらかのセキュリティ ポリシーを実施する必要があります。

ソリューション コンポーネントが満たす PCI の下位要件（CS-MARS）

要件 2：システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- **PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する（たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など）。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

CS-MARS は、HTTPS と SSH を介してのみ、セキュリティ保護された通信をサポートします。

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。

CS-MARS では、一意のユーザおよびパスワードを設定できます。ただし、PNADMIN アカウントは一般管理者アカウントであり、削除できません。このアカウントのデフォルト パスワードは、変更して、セキュリティ保護された場所に格納し、一般アカウントを使用できないようにする必要があります。

CS-MARS では、代替または外部の認証方式は許可されません。CS-MARS では、CS-ACS または Active Directory に対する認証は設定できません。

CS-MARS は、パスワードに AES 暗号化方式を使用します。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス (特に、root などの管理者権限を使用したアクセス) を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.6** — 監査ログの初期化
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ

- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

個々のロールベース ユーザ認証ログはローカルです (CS-ACS 認証も AD 認証も使用できません)。

CS-MARS は CSA ログイン / 警告、CS-M セキュリティ イベント、ISR ファイアウォール ログ、および IDS/IPS 警告を受信します。

CS-MARS にはローカル監査証跡があります。

NFS バックアップ サーバに毎日バックアップされる監査ログ ファイルは CSA により監視され、すべてのプロセスとユーザ (NFS サーバへのデータの書き込みを担当するアプリケーション プロセスを除く) は、このディレクトリにあるファイルを変更することも削除することもできません。

CSA 警告は、生成されると CS-MARS 中央サーバに送信され、警告 E メールが管理者の E メール アカウントに送信されます。

次の要件は、NTP を使用するよう CS-MARS アプライアンスを設定することで満たされました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間および UTC (以前の GMT) に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
 - **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する (攻撃者によるクロックの変更を防ぐため)。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる (内部時間サーバの不正使用を防ぐため)。詳細については、<http://www.ntp.org> を参照。

設定例を次に示します。

```
[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** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。

- **PCI 10.5.3** — 監査証拠ファイルは、集中ログサーバ、または変更が困難なメディアに速やかにバックアップする。

CS-MARS では、監査ログが中央に保管されています。

CS-MARS ログは1時間おきにアーカイブされ、CSA ソフトウェアを実行する中央 NFS サーバに送信されます。

- **PCI 10.5.4** — 内部 LAN のログサーバに無線ネットワークのログをコピーする。

無線 Syslog は、Wireless Controller から CS-MARS 中央サーバに送信されます。CS-MARS には、無線ログを生成する定義済みイベント トリガーはありません。顧客の要件に基づいて手動で定義する必要があります。

- **PCI 10.6.a** — セキュリティ ポリシーと手順を取得して調査し、1 日に1 回以上はセキュリティ ログを調べる手順が含まれ、例外に対するフォローアップが要求されていることを確認する。
- **PCI 10.6.b** — 監視と面談により、すべてのシステム コンポーネントについて定期的なログの調査が実施されていることを確認する。

CS-MARS は、システム イベントの相関と分析を実行します。また、処置が迅速に行われるように、システム イベントに関する警告を生成します。



(注)

文書化されたセキュリティ ポリシーと手順により、例外に対するフォローアップを含む、セキュリティ ログの毎日の調査（小売業者 / サービス プロバイダーが実行します）が要求されている必要があります。

補完コントロールが必要な PCI 下位要件（CS-MARS）

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。



注意

CS-MARS は、個々のユーザ パスワード持続時間の適用、パスワード複雑度、パスワード履歴、自動失敗ロックアウト機能のいずれも備えていません。CS-MARS は外部認証方式をサポートしていません。Active Directory、CS-ACS、およびその他の認証ソリューションのいずれも利用できませんでした。

コンプライアンスのための補完コントロール

QSA では、文書化されたパスワード ポリシーや手動監査手順を組み合わせ、パスワードを必ず 90 日ごとに変更すること、およびデータセンター内の CS-MARS サーバのファイアウォールのセグメント化を推奨しています。これは、これらのアプリケーション内のパスワード設定の制限に対する合理的な補完コントロールといえます。

下位要件は、このラボ環境では満たされませんでした。これは、データセンター インフラストラクチャおよび企業のポリシーは監査の適用範囲外で、QSA 推奨の補完コントロールを導入できなかったためです。

Cisco Secure Access Control Server (CS-ACS)

CS-ACS は、ISR、スイッチ、無線 AP、無線コントローラ、C-LMS、および CS-M のための、セキュリティ保護された認証サービスを提供します。

一般的な注意事項 / ベスト プラクティス

- CS-ACS は、Active Directory (AD) を使用して、個々のユーザの認証を行うよう設定されています。この機能は、AD にユーザ グループを作成し、それを CS-ACS のロールベース グループにマッピングすることで実現されます。これにより、PCI 仕様に対処するために必要な、きめ細かいセキュアな認証が提供されます。
- このソリューションは CS-ACS の Windows バージョンを使用しています。CSA クライアントがインストールされており、ログと監査証跡を不正なアクセスから保護し、警告を作成します。
- 管理者用デフォルト アカウントを削除します。
- HTTPS を有効にして、HTTP を無効にします。

ソリューション コンポーネントが満たす PCI の下位要件 (CS-ACS)

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

- PCI 2.1** — システムをネットワークにインストールする前に必ず、ベンダーが提供するデフォルト設定を変更する (たとえば、パスワード、SNMP コミュニティ スtring、および不要なアカウントの削除など)。

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します (付録 E 「Device Configurations」を参照)。

- PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。
- PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、または SSL/TLS (Transport Layer Security) などのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

管理コンソールは、HTTPS アクセスをサポートするよう設定されており、HTTP アクセスは無効でした。CS-ACS は、高度なセキュア管理ポータル テクノロジーとして SSL を使用するよう設定されています。

CS-ACS はランダムな高速ポートへのポート ホッピングを使用して、セキュリティ保護された通信転送を実現します。

ロールベース管理は、管理タスク用に設定されています。



(注)

すべてのシステム コンポーネントに対する適切なセキュリティ設定を含むサーバ機能強化は、小売業者 / サービス プロバイダーが行う必要があります。

要件 6 : セキュリティで保護されたシステムおよびアプリケーションを開発し、維持する

- **PCI 6.1** — すべてのシステム コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ パッチがインストールされていることを確認する。リリース後 1 カ月以内の該当セキュリティ パッチをインストールする。

SMARTnet サービスを使用するシスコのお客様は、セキュリティ パッチや不具合修正プログラムなどの最新バージョンのコードを常に利用できます。

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および**要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる**

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。

CS-ACS では、すべての管理機能に対してロールベース権限割り当てが設定されます。

Access Control Server では、一意のユーザおよびパスワードを設定できます。CS-ACS 管理アカウントでは、代替または外部の認証方式は許可されません。このアカウントは、サーバ自体の管理機能のために Active Directory に対する認証を行うようには設定できません (図 D-8 を参照)。

- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

CS-ACS は、15 分間でタイムアウトするよう設定されています (図 D-10 を参照)。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス (特に、root などの管理者権限を使用したアクセス) を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.2.6** — 監査ログの初期化
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

個々のロールベース ユーザ認証ログはローカルです (AD 認証は使用できません)。

CS-ACS にはローカル監査証跡があります。

ログ バックアップ サーバに毎日バックアップされる監査ログ ファイルは CSA により監視され、すべてのプロセスとユーザ (ログ サーバへのデータの書き込みを担当するアプリケーション プロセスを除く) は、このディレクトリにあるファイルを変更することも削除することもできません。

CSA 警告は、生成されると CS-MARS 中央サーバに送信され、警告 E メールが管理者の E メール アカウントに送信されます。

この要件は、CSA Manager サーバのオペレーティング システムを、NTP を使用するように設定することで満たされました。

- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
 - **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
 - **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する。組織内の 2、3 台の中央時間サーバが外部からの時間信号を、特殊なラジオ、GPS 衛星、または、国際原子時間および UTC (以前の GMT) に基づくその他の外部ソースから直接受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する。
 - **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
 - **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する (攻撃者によるクロックの変更を防ぐため)。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる (内部時間サーバの不正使用を防ぐため)。詳細については、<http://www.ntp.org> を参照。

次の要件は、Access Control Server のオペレーティング システムを、NTP を使用するように設定することで満たされました。

- **PCI 10.5.1** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。

CSA ソフトウェアは、監査証跡ファイルへのアクセスを監視して保護し、監査証跡を不正に変更しようとした場合に警告を生成するために使用されます (ログ データの書き込みを担当するアプリケーション サービスのみが監査証跡の書き込み / 変更 / 削除を実行できます)。シスコでは、監査証跡を中央のバックアップ サーバにコピーする追加のバックアップ スクリプトを作成しています。このバックアップ サーバでは、CSA 保護が適用され、監査証跡のバックアップを担当するアカウントを除き、すべてのアクセス、変更、削除が排除されます。

補完コントロールが必要な PCI 下位要件 (CS-ACS)

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.5.9** — ユーザ パスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。

- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

**注意**

CS-ACS は、サーバ自体を管理するための、個々のユーザ パスワード 持続時間の適用、パスワード 複雑度、パスワード 履歴、自動失敗 ロックアウト 機能のいずれも備えていません。CS-ACS 管理は外部認証方式をサポートしていません。Active Directory およびその他の認証ソリューションのいずれも利用できませんでした。

コンプライアンスのための補完コントロール

シスコでは、文書化されたパスワード ポリシーや手動監査手順を組み合わせ、パスワードを必ず 90 日ごとに変更すること、およびデータセンター内の CS-ACS サーバのファイアウォールのセグメント化を推奨しています。これは、これらのアプリケーション内のパスワード設定の制限に対する合理的な補完コントロールといえます。

下位要件は、このラボ環境では満たされませんでした。これは、データセンター インフラストラクチャおよび企業のポリシーは監査の適用範囲外で、QSA 推奨の補完コントロールを導入できなかったためです。

補完コントロールが必要な PCI 下位要件 (RSA enVision)

RSA enVision には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

コンプライアンス管理

CiscoWorks Network Compliance Manager (C-NCM)

一般的な注意事項 / ベスト プラクティス

C-NCM を使用すると、次の機能を活用して、PCI 監査に備えることができます。

- セキュリティ 監査のための包括的な設定変更履歴アーカイブの維持
- クレジット カード取り引きに関する VISA CISP/PCI などのセキュリティ 標準へのコンプライアンスの監視および実施
- セキュリティ コンプライアンス ポリシー (ファイアウォール設定の regex パターン マッチ) の作成、および適用されたセキュリティ ポリシーにファイアウォール設定が準拠していることのチェック
- デバイスとその設定に対するロールベース アクセス コントロールおよびロックダウン
- ファイアウォール デバイスでの設定変更のプロビジョニング
- ファイアウォール デバイスに加えられた変更の監査証跡の維持
- ACL の変更履歴の維持

要件 2 : システム パスワードおよびその他のセキュリティ パラメータとしてベンダーが提供するデフォルト設定を使用しない

必要な複雑さと長さを備えたパスワードをローカル アカウントに設定します。

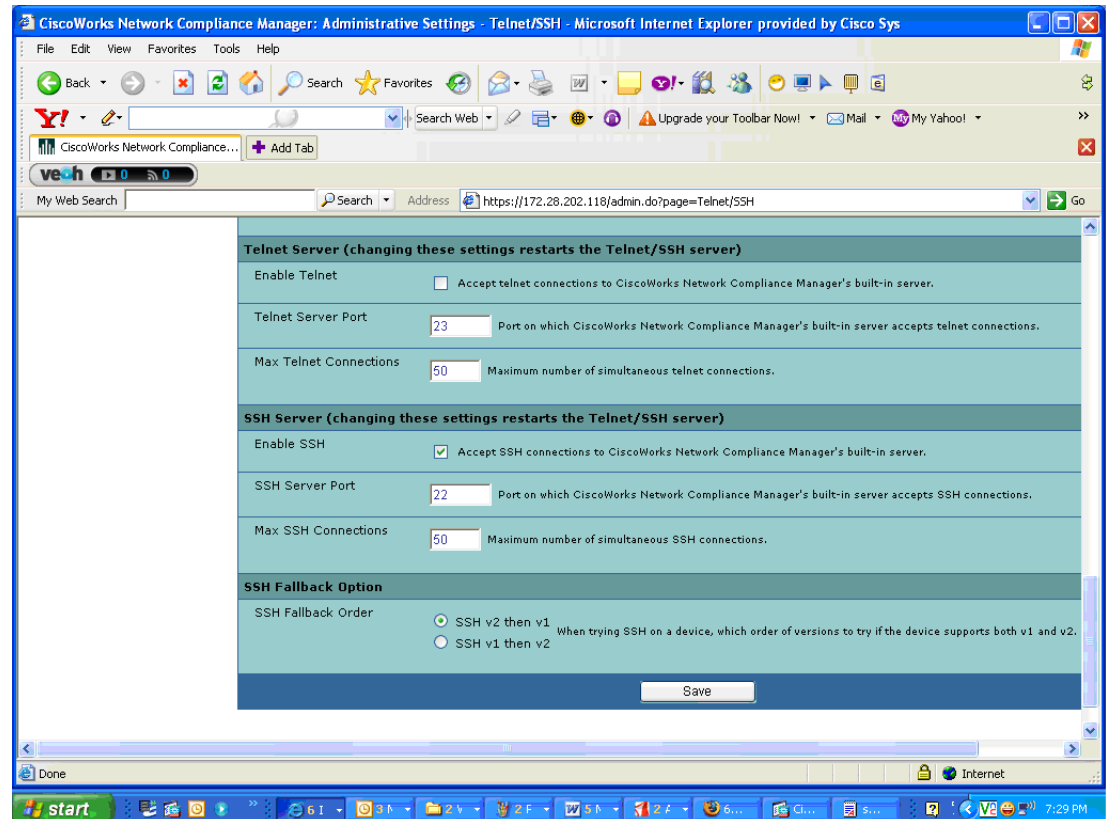
このリストの後の記述は、次の下位要件に関するものです。

- **PCI 2.2.2** — 不要で信頼できないサービスとプロトコル (デバイスの指定機能を実行するために、直接必要ではないサービスとプロトコル) をすべて無効にする。

- **PCI 2.3** — 非コンソール管理者アクセスをすべて暗号化する。SSH、VPN、またはSSL/TLSなどのテクノロジーを、Web ベースの管理、およびその他の非コンソール管理者アクセスに使用する。

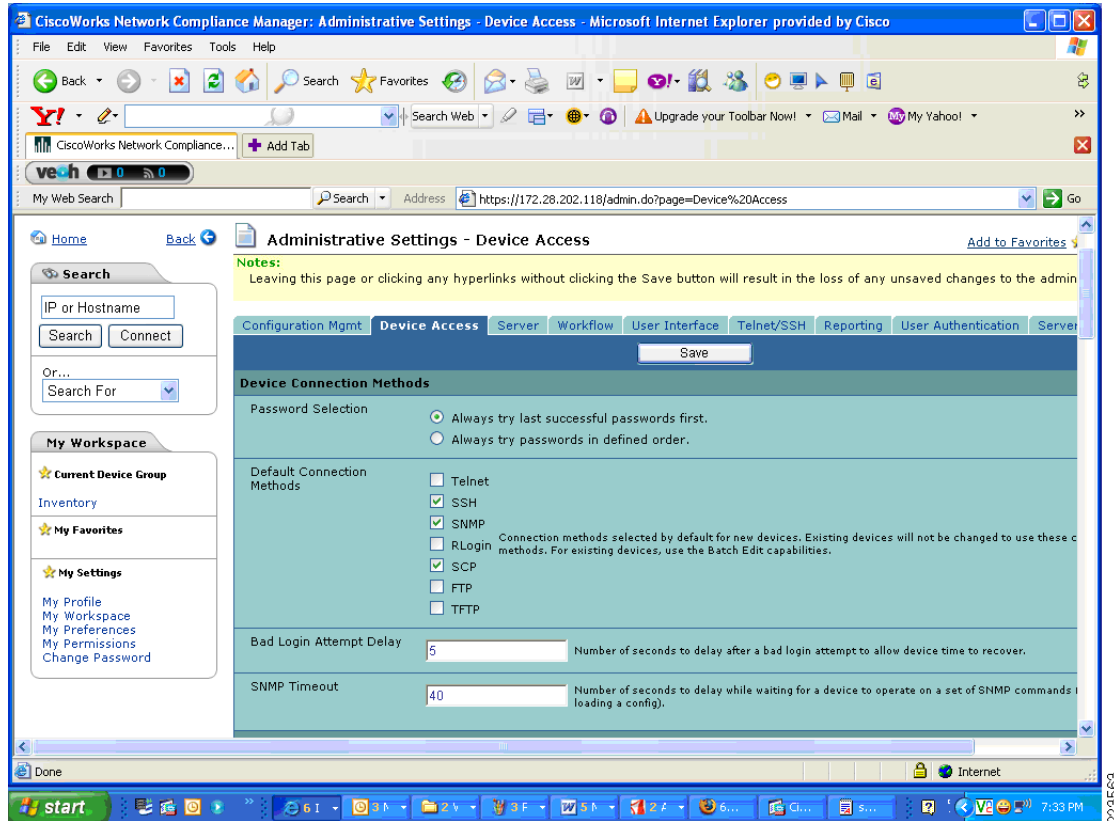
HTTP および Telnet 経由の、CS-NCM へのセキュリティ保護されていないアクセスは、HTTPS と SSH が設定されている間は無効になっています。図 3-21 を参照してください。

図 3-21 Telnet を無効にして SSH 接続を受け入れるための CS-NCM の設定



Telnet、FTP、および TFTP などのサービスは、ネットワーク デバイスへの接続方式として選択されませんでした。CS-NCM は、CS-NCM 上で動作するサービスだけでなく、管理対象のネットワーク デバイス上で動作する必要のあるサービスも対象とした PCI 要件に従って管理を行いました。図 3-22 を参照してください。

図 3-22 ネットワーク デバイスへのセキュアな接続方式のための、CS-NCM のデバイス アクセス設定



- **PCI 2.2.3.b** — 一般的なセキュリティ パラメータ設定がシステム設定標準に含まれることを確認する。
- **PCI 2.2.3.c** — サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントについて、共通のセキュリティ パラメータが適切に設定されていることを確認する。

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

このリストの後の記述は、要件 7 および 8 の次の下位要件に関するものです。

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークンデバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。

- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

このソリューションでは、ここで説明している下位要件は、ユーザ アカウント サービスのための CS-ACS および Microsoft Active Directory の実装により満たされました。

CS-ACS に到達できない場合のフォールバック認証は、CS-NCM に対してローカルに設定されました。これらのフォールバック アカウントは、QSA 推奨ポリシーに基づいて交代で使用する必要があります。

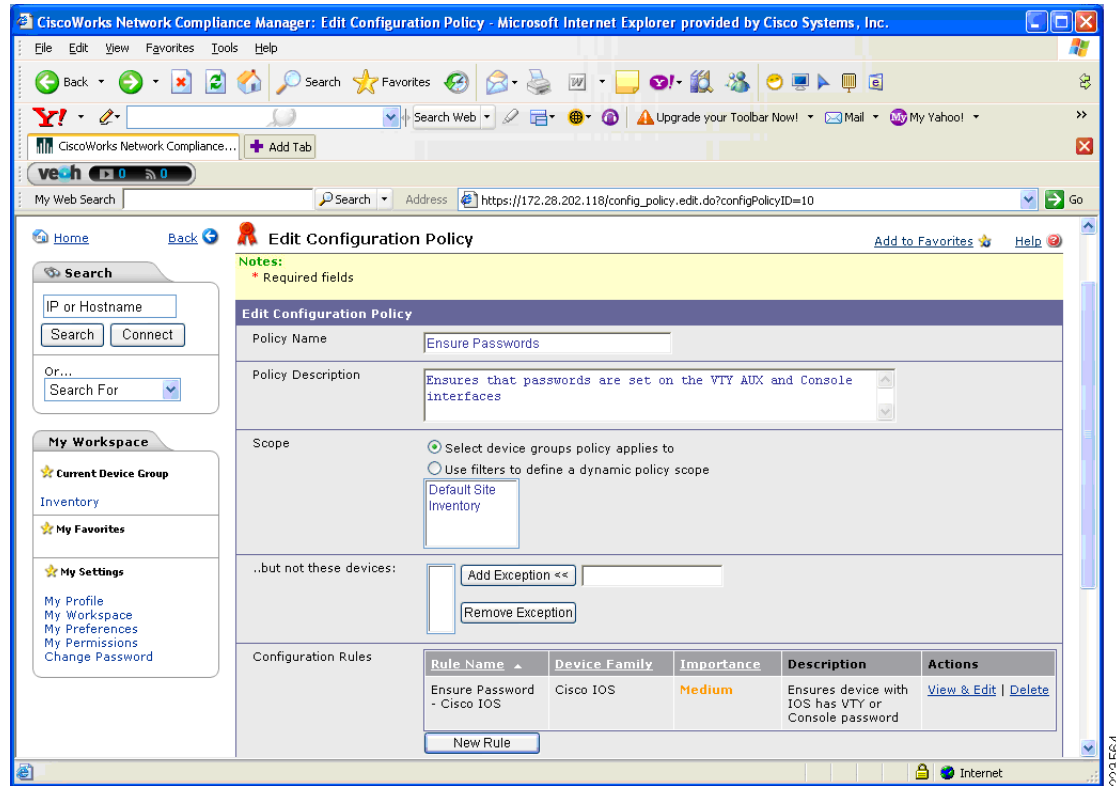
- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.3.1** — ユーザ ID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前
- **PCI 10.4** — 組織内の正確な時間だけでなく、サンプルとなるシステム コンポーネント、重要なサーバ、無線アクセス ポイントの時間関連システム パラメータ設定を入手し、配布するプロセスを採用し、見直す。次の事柄がプロセスに含まれ、実装されていることを確認する。
- **PCI 10.4.a** — NTP または類似のテクノロジーを時間の同期化に使用していることを確認する。
- **PCI 10.4.b** — 内部サーバには、外部ソースからの時間信号を受信していないものがあることを確認する（組織内の 2、3 台の中央時間サーバは、外部からの時間信号を [特殊なラジオ、GPS 衛星、または、国際原子時間および UTC（以前の GMT）に基づくその他の外部ソースから直接] 受信し、互いにピアリングして正確な時間を維持し、他の内部サーバとその時間を共有する）。
- **PCI 10.4.c** — 最新バージョンの Network Time Protocol (NTP; ネットワーク タイム プロトコル) を実行していることを確認する。
- **PCI 10.4.d** — 時間サーバの NTP 時間を更新する特定の外部ホストが指定されていることを確認する（攻撃者によるクロックの変更を防ぐため）。この更新は、対称キーで暗号化することもできる。さらに、アクセス コントロール リストを作成して、クライアント マシンの IP アドレスを指定し、NTP サービスを提供するようにすることができる（内部時間サーバの不正使用を防ぐため）。詳細については、<http://www.ntp.org> を参照。
- **PCI 11.1** — 不正なアクセスのあらゆる試みを適切に識別し、阻止するために、セキュリティの制御、制限、ネットワーク接続、および制約を毎年テストする。

上記の要件は、ネットワーク デバイス上の設定変更イベントに関連するため、CS-NCM により満たされました。

データセンター内の ASA、ルータ、および Catalyst スイッチの設定のスナップショットは、CS-NCM を使用してキャプチャされました。CS-NCM を使用して、PCI 要件を満たすための正しいコマンドがデバイスで設定されているかがチェックされました。設定変更は、どのユーザがどのデバイスをどのように変更したかを特定する機能により監視され、追跡されました。図 3-23

は CS-NCM の例を示しています。この CS-NCM には、ルータとこれらのデバイスへのアクセスのセキュリティ保護に関する業界標準とベスト プラクティスに従って、コンソールアクセス用パスワードがデバイスに設定されていることをチェックする規則が設定されています。

図 3-23 要件 2.2-2



クライアントおよびサーバ

Point-of-Sale (POS)

一般的な注意事項 / ベスト プラクティス

NCR Advanced Checkout Solution Point-of-Sale システムは PCI 準拠について監査されました。このシステムは、必要なトランザクション トラフィックを提供して、小売りインフラストラクチャのセキュリティを確認するためにインストールされました。QSA は、NCR の CS-ACS ソフトウェアのさまざまなファイルを分析して、POS システムを監査しました。分析したファイルは、データベース トランザクションファイル、ユーザ アクセス ログ、EFT ジャーナル レポート、EFT オフライン レポート、EFY 拒否レポート、電子ジャーナル レポート、TRMOFF (FOH オフライン トランザクション ファイル)、および EFTOFF (管理部門用オフライン トランザクション ファイル) などでした。

小売業者に対しては、VISA の支払いアプリケーション向けカード所有者情報セキュリティ プログラムを参考にすることを推奨します。

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html

小売業者ごとの実装の詳細については、QSA またはセキュリティ サービス企業に相談する必要があります。

QSA Verizon Business は、CSA クライアントとともに POS サーバをインストールすると、PCI 準拠を目指す小売業者にとってきわめて有用であるとしています。

サーバ

一般的な注意事項 / ベスト プラクティス

NCR 提供の Point-of-Sale (POS) クライアント ワークステーションおよびサーバが使用されました。サーバの 1 つには、NCR の Advanced Checkout Solution (NCR-ACS) がロードされ、別のサーバには、NCR の Advanced Store Workbench (ASW) クライアント ソフトウェアがロードされました。クライアント ステーションは、Windows XP Embedded バージョン 2 が動作する NCR RealPOS80c システムです。

NCR-ACS ソフトウェア (バージョン 6.01.04.16) は、大幅にカスタマイズ可能なアプリケーションのグループで、小売業環境に完全な店舗システム ソリューションを提供します。NCR-ACS には、管理部門のコンピュータ、および顧客の確認に使用するフロントエンド POS ワークステーションで動作するアプリケーション ソフトウェアが含まれます。

- NCR は顧客に、CISP Implementation Documentation (実装マニュアル) に従ってカード所有者データを保管するよう助言しています。NCR-ACS は POS システムであるため、NCR は顧客に、インターネットで接続できるシステムにはカード所有者データを保管したり、配置したりしないよう助言しています。
- NCR は、任意のネットワーク構成でこのアプリケーションを実装する顧客に対し、確実に暗号化された通信方法のみを使用することを推奨しています。

ASW は、管理部門のコンピュータ システムにインストールされる主要 NCR-ACS ソフトウェアです。ASW からは、管理部門のレポートやアプリケーションにアクセスできます。

小売業者には、<http://www.CISecurity.com> にある、サーバのコンプライアンス認定を取得するためのガイドを参照することを推奨します。小売業者ごとの実装の詳細については、QSA またはセキュリティ サービス企業に相談する必要があります。

QSA は、POS システムに NCR-CSA クライアントをインストールすると、PCI 準拠を目指す小売業者にとってきわめて有用であるとしています。

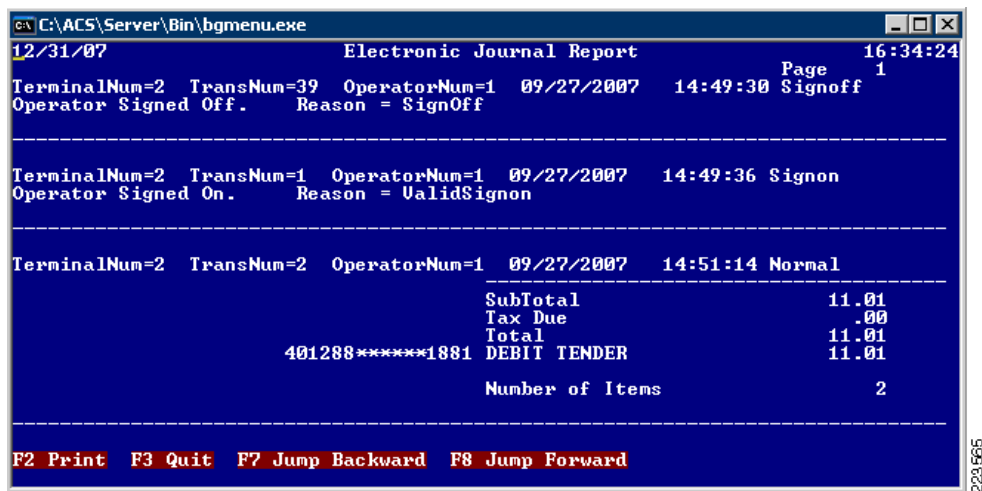
ソリューション コンポーネントが満たす PCI の下位要件 (NCR POS システム)

要件 3 : 保管されたカード所有者データを保護する

- **PCI 3.2** — 認可後のセンシティブ認証データは (暗号化されていたとしても) 保管しない。
センシティブ認証データには、次の要件 3.2.1 ~ 3.2.3 に述べるデータが含まれます。小売業者は責任を持って、認可後のセンシティブ認証データ (完全追跡データ、CVV2、および PIN/PIN ブロックなど) が (暗号化されていても)、使用する POS システムに保管されないようにする必要があります。POS システムが PCI 要件を満たすようにするための重要なポイントは、PABP 標準に従って POS アプリケーションを保証している POS ベンダーを利用することです。
 - **PCI 3.2.1** — 磁気ストライプ (カードの裏面や、チップなどにある) から読み取られた情報の内容全体を保管しない。このデータは、フルトラック、トラック、トラック 1、トラック 2、磁気ストライプデータとも呼ばれる。
 - **PCI 3.2.2** — 非対面取り引きでの確認に使用するカード確認用の値またはコード (支払い用カードの表面または裏面に印刷されている 3 桁または 4 桁の数字) を保管しない。

- PCI 3.2.3 — 個人識別番号 (PIN) または暗号化された PIN ブロックを保管しない。
- PCI 3.3 — PAN が表示される場合はマスクする (表示される最大桁数は先頭の 6 桁と末尾の 4 桁)。

図 3-24 マスクされた PAN の情報



- PCI 3.4 — 少なくとも、保管されているあらゆる場所で、次の手法のいずれかを使用して PAN を判読不能な形式にする (ポータブル デジタル メディア、バックアップ メディア、ログに含まれるデータ、および無線ネットワーク経由で受信または保管されたデータを含む)。
 - 強固な一方向ハッシュ機能 (ハッシュ インデックス)
 - トランケーション
 - インデックス トークンおよびパッド (パッドはセキュリティで保護して保管する必要があります)
 - 関連するキー管理のプロセスおよび手順を伴う強固な暗号化

判読不能な形式にする必要のある最小のアカウント情報は PAN です。

- PCI 3.5 — カード所有者データの暗号化に使用する暗号キーを、開示と濫用の両方から、次のように保護する。
 - PCI 3.5.1 — キーへのアクセス権を、必要最小限の人数の管理者のみに制限
 - PCI 3.5.2 — 最小限の場所および形式で、キーを安全に保管
- PCI 3.6.1 — 強力なキーの生成
- PCI 3.6.2 — セキュリティで保護されたキーの配布
- PCI 3.6.3 — セキュリティで保護されたキーの保管
- PCI 3.6.4 — 定期的なキーの変更
 - 関連アプリケーションで必要とされ推奨される方法 (キーの再作成など) で実行。自動的に行われることが望ましい。
 - 少なくとも毎年



(注)

NCR-ACS アプリケーション — すべてのデータを手動で復号化して新しいキーで暗号化し直す以外に、暗号キーを交代で使用する合理的な方法はありませんでした。NCR-ACS アプリケーションでは、複数のキー (最大 255 個) の使用により、1 つのキーで暗号化されるデータの量を制限できます。

- **PCI 3.6.5** — 以前のキーの破棄
- **PCI 3.6.6** — キーに関する知識の分割、およびキーの二重管理の確立（完全なキーを再構築するには、各自がキーの部分のみを知っている 2、3 人の担当者が必要となる）
- **PCI 3.6.7** — キーの不正な置換の防止
- **PCI 3.6.8** — 解読されたことがわかっている、または疑われるキーの交換

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、*root* などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。



(注)

NCR-ACS アプリケーション : NCR-CSA を使用して、NCR-ACS アプリケーションのバイナリを使用するためのアクセス、および NCR アプリケーションのログ ファイルへのアクセスを監視し、そのログを作成しました。

- **PCI 10.2** — すべてのシステム コンポーネントの自動監査証跡を実装して、次のイベントを再構築する。
 - **PCI 10.2.1** — カード所有者データへのすべての個別アクセス
 - **PCI 10.2.2** — *root* または管理者の権限を持つユーザのいずれかが行ったすべてのアクション



(注)

NCR-ACS アプリケーション — 個別の管理者権限によるアクションはすべて、NCR-ACS の **EFT** ログ ファイルおよび **Transaction LOG** に記録されます。

- **PCI 10.2.3** — すべての監査証跡へのアクセス



(注)

NCR-ACS アプリケーション — 監査ログ ファイルおよびアプリケーション ログ ディレクトリへの不正なアクセスにより CSA イベントがトリガーされ、そのログが CSA 管理コンソールで生成されました。

- **PCI 10.2.6** — 監査ログの初期化



(注)

NCR-ACS アプリケーション — 監査証跡アクセスの CSA 保護が監査証跡の初期化に適用されません。

- **PCI 10.3** — すべてのシステム コンポーネントの各イベントについて、少なくとも次の監査証跡エントリを記録する。
 - **PCI 10.3.1** — ユーザ ID
 - **PCI 10.3.2** — イベントのタイプ
 - **PCI 10.3.3** — 日付と時間
 - **PCI 10.3.4** — 成功または失敗の表示
 - **PCI 10.3.5** — イベントの開始
 - **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースの ID または名前

補完コントロールが必要な PCI 下位要件 (NCR POS システム)

NCR POS システムには、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

有線クライアントおよび無線クライアント

一般的な注意事項 / ベスト プラクティス

ユーザ ID とパスワードの入力を求めるよう、すべての有線エンドポイントおよび無線エンドポイントを設定します。在庫管理用スキャナなどの小売業向け無線ユニットは物理的に保護されていない可能性があるため、これらのプロパティを静的に設定しないでください。

暗号化およびキー管理

RSA Key Manager

一般的な注意事項 / ベスト プラクティス

RSA Key Manager サーバ (RSA Key Manager バージョン 2.1.1 に基づく) をインストールするには、PKI (Public Key Infrastructure; 公開鍵インフラストラクチャ) が必要不可欠です。

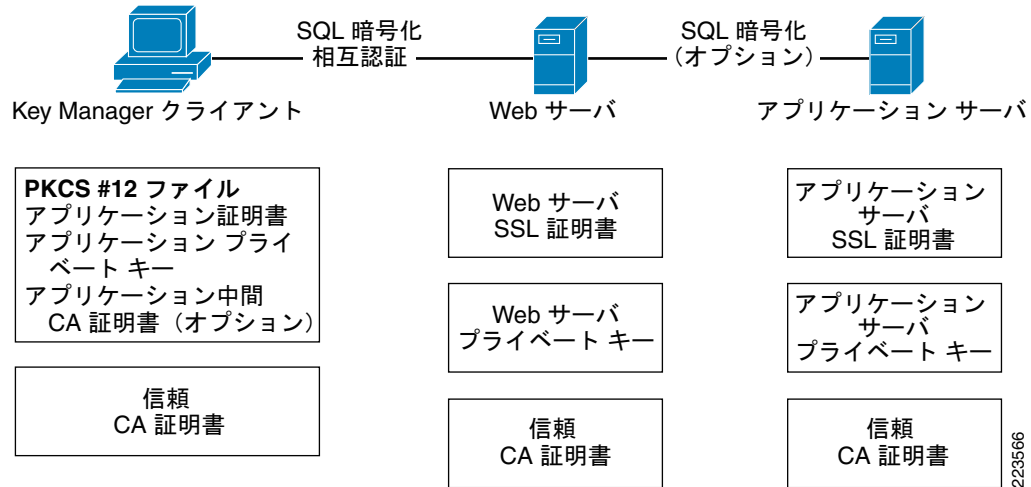
PKI の要件

RSA Key Manager を導入する場合は、PKI がセットアップされ、エンティティ間での高度なセキュア通信とセキュア認証が有効である必要があります。RSA Key Manager PKI 信頼モデルでは、次の目的で SSL 通信が使用されます。

- 導入した RSA Key Manager のネットワーク エンティティ間での高度なセキュア通信
- RSA Key Manager クライアントと Web サーバ間の相互認証
- RSA Key Manager サーバにアプリケーション証明書を配信するための高度なセキュア通信

図 3-25 は、RSA Key Manager の PKI 要件を示します。

図 3-25 RSA Key Manager の PKI 要件



準備する必要がある証明書およびクレデンシャルには、次のものがあります。

- Key Manager クライアント PKCS#12 クレデンシャル
この情報には、アプリケーション証明書、アプリケーション プライベート キー、およびオプションの中間 Certificate Authority (CA; 認証局) 証明書チェーン (アプリケーション証明書が、Web サーバの信頼 CA 証明書で直接署名されていない場合) が含まれます。
- Web サーバ SSL 証明書およびプライベート キー
RSA Key Manager クライアントにより、サーバの認証に使用されます。
- アプリケーション サーバ SSL 証明書およびプライベート キー (オプション)
Web サーバにより、アプリケーション サーバの認証に使用されます。特に複数のサーバが異なるマシンで動作している場合は、Web サーバとアプリケーション サーバ間の通信を暗号化するために推奨されています。
- 信頼 CA 証明書
導入された RSA Key Manager の各ネットワーク エンティティにインストールされ、ピアにより送信された証明書の署名を確認します。たとえば、RSA Key Manager クライアントには、Web サーバ証明書の署名を確認するための信頼 CA 証明書があります。
- 中間 CA 証明書 (オプション)
証明書が信頼 CA 証明書により直接署名されていない場合は、中間 CA 証明書をインストールして SSL 接続中に送信し、証明書チェーンを確認する必要があります。

セキュリティ推奨事項

RSA 署名の公開指数が小さい (3 など) と脆弱性が高くなるため、RSA では F4 (216+1) という指数の使用を推奨しています。

セキュリティのベストプラクティス

RSA Key Manager サーバの導入により、セキュリティ オブジェクトのセキュアな保管、暗号キーの生成と保管、暗号ポリシーの管理、および RSA Key Manager クライアントによるセキュリティ オブジェクトへのアクセスの仲介が実行されます。この機能へのアクセスをセキュリティで保護し、制限するための最善のセキュリティ対策を実装することは非常に重要です。次に示すのは、このような対策のほんの数例です。

- ファイアウォール、およびユーザの認証と認可 (RSA Access Manager などを使用した) で保護された高度なセキュアゾーン内に、すべての RSA Key Manager コンポーネントを配置する

- ・ 導入した RSA Key Manager のエンティティ間の、SSL による高度なセキュア通信
- ・ 可能なかぎり、RSA Key Manager エンティティを残りの組織システムから分離する
- ・ Web サーバのログ ファイルに、キーがプレーン テキストで記述されないようにする
- ・ メモリの変更およびディスク上のデータへの直接アクセスを禁止する
- ・ 高度にセキュアな手順でデータベースをバックアップする

RSA Key Manager サーバを導入すると、その他のサードパーティ製品（Web サーバ、アプリケーション サーバ、およびデータベース サーバの各製品など）が統合され、完全な暗号キー管理ソリューションが提供されます。

RSA Key Manager 導入時の Microsoft SQL Server の設定と保護の方法に関する最新情報については、次の URL を参照してください。

- ・ 10 steps to help secure SQL Server (SQL Server の保護に役立つ 10 のステップ)
<http://www.microsoft.com/sql/prodinfo/previousversions/securingsqlserver.msp>
- ・ SQL Server のセキュリティに関する注意点
[http://msdn.microsoft.com/ja-jp/library/ms161948\(SQL.90\).aspx](http://msdn.microsoft.com/ja-jp/library/ms161948(SQL.90).aspx)
- ・ SQL Server でのデータベースのバックアップおよび復元
[http://msdn.microsoft.com/ja-jp/library/ms187048\(SQL.90\).aspx](http://msdn.microsoft.com/ja-jp/library/ms187048(SQL.90).aspx)

ソリューション コンポーネントが満たす PCI の下位要件 (RSA Key Manager)

要件 3 : 保管されたカード所有者データを保護する

- ・ PCI 3.5.1 — キーへのアクセス権を、必要最小限の人数の管理者のみに制限
- ・ PCI 3.5.2 — 最小限の場所および形式で、キーを安全に保管
- ・ PCI 3.6.1 — 強力なキーの生成
- ・ PCI 3.6.2 — セキュリティで保護されたキーの配布
- ・ PCI 3.6.3 — セキュリティで保護されたキーの保管
- ・ PCI 3.6.4 — 定期的なキーの変更
- ・ PCI 3.6.5 — 以前のキーの破棄
- ・ PCI 3.6.6 — キーに関する知識の分割、およびキーの二重管理の確立
- ・ PCI 3.6.7 — キーの不正な置換の防止
- ・ PCI 3.6.8 — 解読されたことがわかっている、または疑われるキーの交換

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- ・ PCI 7.2 — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- ・ PCI 8.1 — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。

ラボでは、RSA Access Manager を使用して、RSA Key Manager に上記の機能が提供されました。

- ・ PCI 8.2 — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。

- パスワード
- トークン デバイス
- 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
RSA Key Manager の場合は、RSA Access Manager を介した認証がハッシュされ、ローカル認証もハッシュされます。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます (8 文字)。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます (英数字および辞書によるチェック)。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます (最後のパスワード 10 件)。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます (1 日に 3 回のアクセス失敗)。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
RSA Key Manager の場合、この要件は RSA Access Manager により満たされます (管理者によるリセットが必要)。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス (特に、root などの管理者権限を使用したアクセス) を、各ユーザにリンクさせるためのプロセスを確立する。
RSA Key Manager の場合は、ローカル監査証跡に加えて、CSA で RSA Key Manager バイナリへのアクセスが監視され、そのログが生成されました。
 - **PCI 10.2.1** — カード所有者データへのすべての個別アクセス
 - **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
 - **PCI 10.2.3** — すべての監査証跡へのアクセス
 RSA Key Manager の場合は、監査ログ ファイルおよびアプリケーション ログ ディレクトリへの不正なアクセスにより CSA イベントがトリガーされ、そのログが CSA 管理コンソールで生成されました。
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用

- **PCI 10.3.1 ~ 10.3.6** — ユーザ ID、イベントのタイプ、日付と時間、成功または失敗の表示、およびイベントの開始を示す監査証跡エントリを記録する。

補完コントロールが必要な PCI 下位要件 (RSA Key Manager)

RSA Key Manager には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

RSA Access Manager

一般的な注意事項 / ベスト プラクティス

RSA Access Manager はラボ環境で、RSA Key Manager への管理者アクセスを保護するために使用されています。設定例については、[図 3-26](#) を参照してください。

ソリューション コンポーネントが満たす PCI の下位要件 (RSA Access Manager)

要件 7 : カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件 8 : コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス
 - 生体認証
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた 4 つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを 6 回試みて失敗した後はユーザ ID をロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は 30 分、または管理者がユーザ ID を有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が 15 分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

図 3-26 RSA Access Manager — パスワード ポリシー

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:

223.567

要件 10 : ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、root などの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.3** — すべての監査証拠へのアクセス
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.3.1 ~ 10.3.6** — ユーザ ID、イベントのタイプ、日付と時間、成功または失敗の表示、およびイベントの開始を示す監査証拠エントリを記録する。

補完コントロールが必要な PCI 下位要件（RSA Access Manager）

RSA Access Manager には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。

RSA File Security Manager

一般的な注意事項 / ベスト プラクティス

RSA File Security Manager は、異種プラットフォームでのロールベースのアクセス制御を組み合わせ、ファイル / フォルダの透過的な暗号化を提供するソフトウェアベースのセキュリティ ソリューションです。

RSA File Security Manager は、次の 2 つの統合コンポーネントから構成されます。

- アダプタ マネージャ — ネットワーク / ドメインのユーザとアプリケーションのアクセス制御ルールを定義します。
- アダプタ — ホスト / サーバのレベルでアクセス制御ルールを実施します。

RSA File Security Manager 製品の導入のベスト プラクティスは次のとおりです。

- インストールの前に、アダプタおよびアダプタ マネージャ コンソールの最低システム要件をシステムが満たしているか、または超えていることを確認します。この最低要件の情報は、アダプタおよびアダプタ マネージャ コンソールのインストール ガイドに記載されています。
- アダプタ マネージャ コンソール ホストが、ファイルセキュリティ アダプタがインストールされているホストに到達できることを確認します。
- アダプタおよびアダプタ マネージャ コンソールが適切に連携するには、制御ポートおよび監査ポートを使用する必要があります。アダプタとアダプタ マネージャ間で適切な通信が行われるよう、必要なファイアウォール ポート（デフォルトの TCP 5766 および 19978）が双方向トラフィックに使用可能であることを確認します。実際のポート番号は、ユーザが設定可能です。
- アダプタ マネージャでポリシー データベースを頻繁にバックアップするようにします。システムに重大な変更を加えた後は必ず、バックアップを実行することを強く推奨します。
- デフォルトでは、保護されたフォルダへのすべてのタイプのアクセスが、ファイルセキュリティ アダプタにより監査ログに記録されます。監査ログ データは、保護されたホストの「日ファイル」に保管されます。
 - 生成される監査ログ データの量をファイルセキュリティ アダプタで監視し、適切な保管方法を計画します。
 - アダプタによる監査証跡の作成が不要なアクションを無効にします。
 - ファイルセキュリティ アダプタで生成された監査ログ データ ファイルのバックアップ戦略を策定しておきます。24 時間が経過するたびに、ファイルセキュリティ アダプタは新しい監査ログ ファイル（日ファイル）を生成します。以前の監査ログの日ファイルは中央サーバにバックアップし、ファイルセキュリティ アダプタにある元のファイルを削除して、ストレージを最適化することを推奨します。

ソリューション コンポーネントが満たす PCI の下位要件（RSA File Security Manager）

要件 3：保管されたカード所有者データを保護する

- PCI 3.5.1 — キーへのアクセス権を、必要最小限の人数の管理者のみに制限
- PCI 3.5.2 — 最小限の場所および形式で、キーを安全に保管
- PCI 3.6.1 — 強力なキーの生成
- PCI 3.6.2 — セキュリティで保護されたキーの配布
- PCI 3.6.3 — セキュリティで保護されたキーの保管
- PCI 3.6.4 — 定期的なキーの変更
- PCI 3.6.5 — 以前のキーの破棄
- PCI 3.6.6 — キーに関する知識の分割、およびキーの二重管理の確立
- PCI 3.6.7 — キーの不正な置換の防止
- PCI 3.6.8 — 解読されたことがわかっている、または疑われるキーの交換

要件7: カード所有者データへのアクセスを、業務上必要な範囲内に制限する、および

要件8: コンピュータにアクセスする各ユーザに一意のIDを割り当てる

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。
- **PCI 10.1** — システムコンポーネントへのすべてのアクセス（特に、rootなどの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.1** — カード所有者データへのすべての個別アクセス
- **PCI 10.2.3** — すべての監査証跡へのアクセス
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.3.1 ~ 10.3.6** — ユーザID、イベントのタイプ、日付と時間、成功または失敗の表示、およびイベントの開始を示す監査証跡エントリを記録する。

補完コントロールが必要な PCI 下位要件 (RSA File Security Manager)

- **PCI 8.5.9** — ユーザパスワードを、少なくとも90日ごとに変更する。
- **PCI 8.5.10** — 7文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。
- **PCI 8.5.12** — ユーザが直前に使用していた4つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。

8.5.9 ~ 8.5.12 について、QSA では、文書化されたパスワードポリシーや手動監査手順を組み合わせ、パスワードに辞書攻撃を定期的に使用して強力なパスワードを生成すること、およびデータセンター内のこれらのコンポーネントの内部ファイアウォールのセグメント化を推奨しています。これは、これらのアプリケーション内のパスワード設定の制限に対する合理的な補完コントロールとなります。

- **PCI 8.5.13** — アクセスを6回試みて失敗した後はユーザIDをロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は30分、または管理者がユーザIDを有効にするまでに設定する。

8.5.13 ~ 8.5.14 について、QSA では、CSA または他の監視ソフトウェアを使用して、何度も繰り返されるログオン失敗に対する警告を生成すること、およびこれらのコンポーネントの内部ファイアウォールのセグメント化の併用を推奨しています。これは、これらのアプリケーション内のアカウントロックアウト設定の制限に対する合理的な補完コントロールとなります。

- **PCI 8.5.15** — セッションのアイドル状態が15分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

QSA では、アイドルセッションのタイムアウトが使用できないか、アプリケーション/ビジネス業務（バックアップジョブなど）に影響する場合は、スクリーンセーバーのタイムアウトを補完コントロールとして使用することを推奨しています。



(注)

下位要件 8.5.9 ~ 8.5.15 は、Q12008 でリリースされる RSA File Security Manager のバージョン 2.2 のロードマップで対処しています。

RSA® Authentication Manager、RSA SecurID® および RSA enVision

RSA Authentication Manager は RSA Authentication Agent と連携し、時間同期ベース RSA SecurID トークンが提供する強力な 2 ファクタ ユーザ認証によりセキュリティを向上させます。

RSA® Authentication Manager ソフトウェアは RSA SecurID® ソリューションの管理コンポーネントであり、認証要求の検証、および企業ネットワークへのアクセスのユーザ認証ポリシーの集中管理に使用されます。このソリューションは、RSA SecurID 認証ツールおよび RSA® Authentication Agent ソフトウェアと連携して、さらに多くの VPN、無線ネットワーク、Web アプリケーション、ビジネス アプリケーション、および業務環境へのアクセスを保護する 2 ファクタ ユーザ認証を提供します。

RSA enVision は、毎秒数十万件のデータ イベントをキャプチャして保管するアプライアンスベースの情報管理セキュリティ プラットフォームです。周辺デバイスやネットワーク デバイス、オペレーティング システム、さらには専用アプリケーションに至るまでの任意の数のソースから、そのアクティビティの企業ビューを提供します。

一般的な注意事項 / ベスト プラクティス

RSA Authentication Manager は、RSA Authentication クライアントや RSA SecurID シードなどの付属コンポーネントをインストールする前に、最初にインストールする必要があります。

ソリューション コンポーネントが満たす PCI の下位要件（RSA Authentication Manager、RSA SecurID、および RSA enVision）

要件 7：カード所有者データへのアクセスを、業務上必要な範囲内に制限する

- **PCI 7.2** — 複数のユーザを持つシステムに対して、ユーザの必要に基づいてアクセスを制限し、特に許可されていないかぎり、「すべて拒否」に設定するメカニズムを確立する。

要件 8：コンピュータにアクセスする各ユーザに一意の ID を割り当てる

- **PCI 8.1** — システム コンポーネントまたはカード所有者データへのアクセスをユーザに許可する前に、すべてのユーザに一意のユーザ名をつける。
- **PCI 8.2** — 一意の ID を割り当てるとともに、次の方式の少なくとも 1 つを使用して、すべてのユーザの認証を行う。
 - パスワード
 - トークン デバイス (SecurID、証明書、または公開キーなど)
 - 生体認証
- **PCI 8.3** — 従業員、管理者、および第三者によるネットワークへのリモート アクセスの 2 ファクタ認証を実装する。トークンを使用する *Remote Authentication and Dial-In Service (RADIUS)* または *Terminal Access Controller Access Control System (TACACS)*、または個別の証明書を使用する VPN (SSL/TLS または IPSEC に基づく) などのテクノロジーを使用する。
- **PCI 8.4** — すべてのシステム コンポーネント上での送信および保管時に、すべてのパスワードを暗号化する。
- **PCI 8.5.8** — グループ、共有、および汎用アカウントとパスワードのいずれも使用しない。
- **PCI 8.5.9** — ユーザパスワードを、少なくとも 90 日ごとに変更する。
- **PCI 8.5.10** — 7 文字以上の長さのパスワードの使用を要求する。
- **PCI 8.5.11** — 数字とアルファベットの両方を含むパスワードを使用する。

- **PCI 8.5.12** — ユーザが直前に使用していた4つまでのパスワードのいずれかと同じパスワードは、新しいパスワードとして指定できないようにする。
- **PCI 8.5.13** — アクセスを6回試みて失敗した後はユーザIDをロックアウトして、それ以上は試みることができないようにする。
- **PCI 8.5.14** — ロックアウトの期間は30分、または管理者がユーザIDを有効にするまでに設定する。
- **PCI 8.5.15** — セッションのアイドル状態が15分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

要件 10：ネットワーク リソースおよびカード所有者データへのすべてのアクセスを追跡および監視する

- **PCI 10.1** — システム コンポーネントへのすべてのアクセス（特に、rootなどの管理者権限を使用したアクセス）を、各ユーザにリンクさせるためのプロセスを確立する。
- **PCI 10.2.2** — root または管理者の権限を持つユーザのいずれかが行ったすべてのアクション
- **PCI 10.2.4** — 無効な論理アクセスの試み
- **PCI 10.2.5** — 識別および認証のメカニズムの使用
- **PCI 10.3.1** — ユーザID
- **PCI 10.3.2** — イベントのタイプ
- **PCI 10.3.3** — 日付と時間
- **PCI 10.3.4** — 成功または失敗の表示
- **PCI 10.3.5** — イベントの開始
- **PCI 10.3.6** — 影響されるデータ、システム コンポーネント、またはリソースのID または名前
- **PCI 10.5.1** — 業務に必要な担当者のみに監査証跡が表示されるよう制限する。
- **PCI 10.5.2** — 監査証跡ファイルが不正に変更されないよう保護する。
- **PCI 10.5.3** — 監査証跡ファイルは、集中ログ サーバ、または変更が困難なメディアに速やかにバックアップする。
- **PCI 10.5.5** — ファイル整合性の監視機能と変更検出ソフトウェアをログに使用して、既存のログデータを、警告を生成せずには変更できないようにする（ただし、新しいデータを追加する場合は警告が生成されない）。

補完コントロールが必要な PCI 下位要件

RSA Authentication Manager

- **PCI 8.5.15** — セッションのアイドル状態が15分を超えて続いた場合は、端末を再度アクティブにするためにパスワードを再入力するようユーザに要求する。

QSA では、アイドルセッションのタイムアウトが使用できないか、アプリケーション/ビジネス業務（バックアップジョブなど）に影響する場合は、スクリーンセーバーのタイムアウトを補完コントロールとして使用することを推奨しています。

RSA enVision には、それぞれの PCI 下位要件を満たすための補完コントロールは不要でした。



(注)

シスコ製品に直接関連し、お客様による更新や修正などの対処を必要とする重大なセキュリティ問題については、シスコのセキュリティに関する勧告および情報（Cisco Security Advisories and Notice）が公開されています。セキュリティ勧告（Security Advisory）は [Cisco.com](https://www.cisco.com/cust-security-announce) に提示され、cust-security-announce@cisco.com の他に、さまざまな公開メーリングリストおよびニュースグループに送信されます。cust-security-announce@cisco.com メーリングリストは外部リストであり、興味があればどなたでも、シスコのセキュリティに関する情報を購読し、受信することができます。

す。お客様には、Cisco Security Advisories and Notices の Web サイト (http://www.cisco.com/en/US/products/products_security_advisories_listing.html#advisory) を参照し、最新のセキュリティに関する脆弱性および問題の詳細情報を入手することを強く推奨します。

ソリューション コンポーネントのまとめ

表 3-1 は、各コンプライアンスの趣旨に応じて多様なソリューション コンポーネントが導入される様子を示します。

表 3-1 ソリューション コンポーネントのまとめ

ソリューション コンポーネントの機能			
テクノロジー	認証	設定管理	監査証跡
ネットワーク システム			
ISR ルータ	CS-ACS および AD	C-LMS/ 一般 (CS-M/ セキュリティ)	C-LMS および CS-MARS への Syslog
ミッドレンジ /WAN 集約ルータ	CS-ACS および AD	ローカル、C-NCM	CS-MARS への Syslog
Catalyst スイッチ	CS-ACS および AD	C-LMS	C-LMS および CS-MARS への Syslog
Adaptive Security Appliance (ASA)	CS-ACS および AD	ローカル、C-NCM	CS-MARS への Syslog
無線アクセス ポイント	ローカル	WCS	コントローラへの LWAPP
無線コントローラ管理	CS-ACS および AD	WCS	CS-MARS への Syslog、WCS への SNMP
エッジルータ (Cisco 7200)	CS-ACS および AD	一般 /C-NCM	CS-MARS への Syslog
Cisco Firewall Services Module	CS-ACS および AD	一般 /ASDM	CS-MARS への Syslog
Cisco Intrusion Detection System	ローカル	IDM/ 一般	CS-MARS への攻撃、ローカル フラット ファイルへの Syslog
Cisco ACE XML Gateway (AXG)	AD	AXG Manager	ローカル フラット ファイル
システム管理			
C-LMS	CS-ACS および AD	ローカル	ローカル フラット ファイル
WCS	ローカル	ローカル	ローカル フラット ファイル
CS-M	CS-ACS および AD	ローカル	ローカル フラット ファイル
CSA Manager	AD	ローカル	ローカル データベース
コンプライアンス管理			
C-NCM	CS-ACS および AD	ローカル	ローカル データベース
監視			

表 3-1 ソリューション コンポーネントのまとめ（続き）

ソリューション コンポーネントの機能			
CS-MARS	ローカル	ローカル	ローカル データベース / 外部 NFS 共有
WCS	ローカル	ローカル	ローカル フラット ファイル
認証			
CS-ACS	ローカル	ローカル	ローカル フラット ファイル
クライアント			
有線ユーザ	なし	該当せず	該当せず
無線ユーザ	ACS および AD	該当せず	該当せず
CSA クライアント	CSA Manager	CSA Manager	該当せず
サードパーティ製品			
RSA Key Manager サーバ	RSA Access Manager	RSA Key Manager	ローカル フラット ファイル
RSA File Security Manager	RSA File Security Manager	RSA File Security Manager コンソール	ローカル フラット ファイル
NCR POS サーバ	AD	Advanced Checkout Solution 設定ツール	ローカル フラット ファイル
RSA Authentication Manager/RSA SecurID	RSA Authentication Manager/RSA SecurID	RSA Authentication Manager/RSA SecurID	RSA enVision — ログ ファイルは専用データベースに保管

■ ソリューション コンポーネントのまとめ



CHAPTER 4

ソリューションの実装と設定

実装

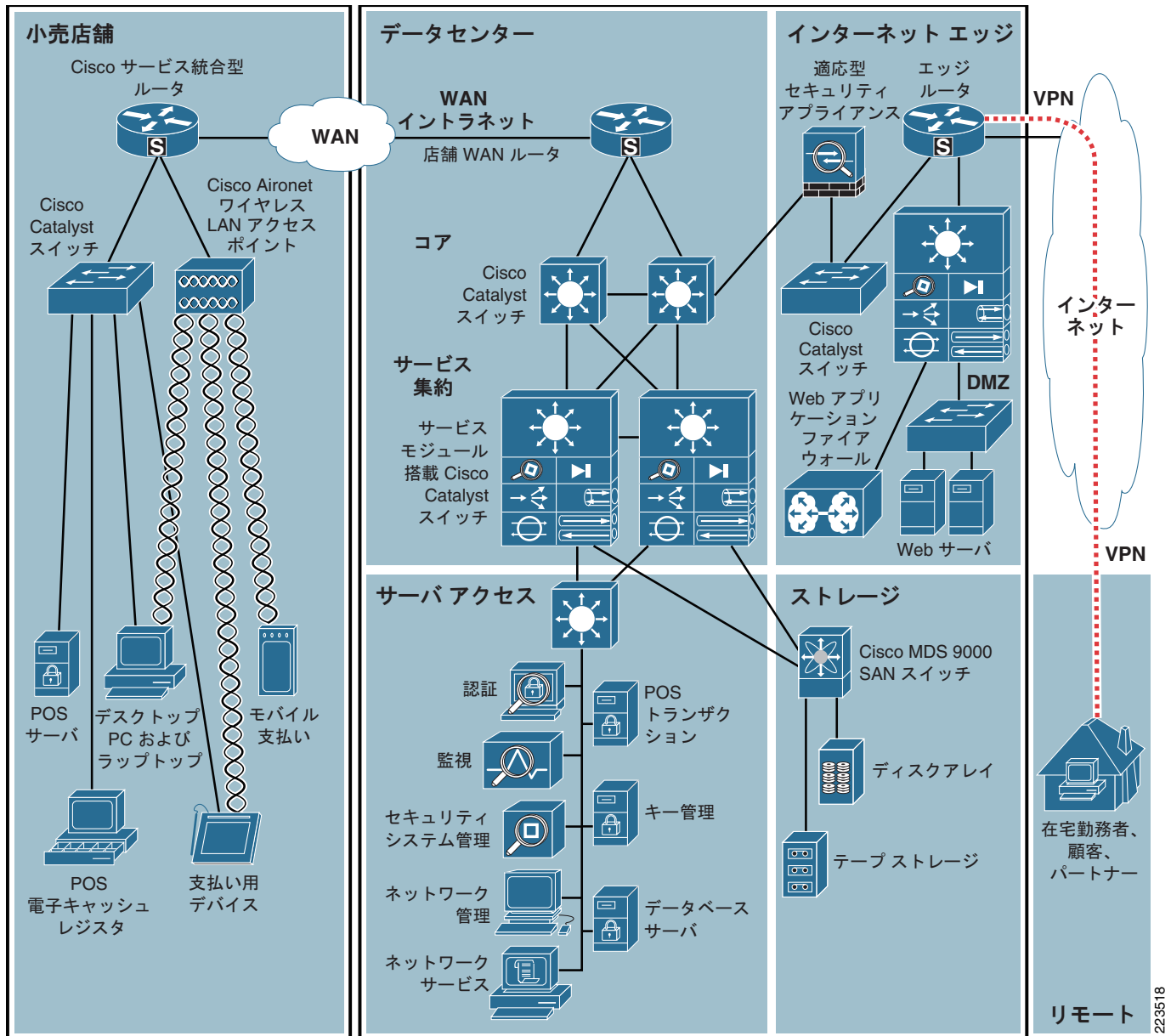
概要

Cisco PCI Solution for Retail は、カリフォルニア州サンノゼにあるシスコの Retail ラボで検証されました。最初に、店舗、データセンター、インターネット サービス プロバイダー、WAN およびインターネット エッジを網羅するネットワーク インフラストラクチャとセキュリティ管理機能がインストールされました。次に、パートナーの point-of-sale (POS; 販売時点管理システム)、支払い、暗号化、モバイル コンピューティング デバイス、および POS アプリケーション サーバがインストールされ、シミュレートされた企業小売環境が構築されました。シスコのプロダクト ビジネス部門、カスタマー アドボカシー アドバンスト サービス部門、エンタープライズ ソリューション エンジニアリング部門、フィールド システム エンジニアリング部門のこの主題の専門家がすべて、この実装におけるベスト プラクティスの確立に尽力しました。また、パートナーである RSA、EMC、NCR、VeriFone、Wincor-Nixdorf、および IBM のこの主題の専門家も、小売業における POS および支払いアプリケーションの現実的なセットの構築と、PCI 要件に基づいた安全な設定の作成に参加しました。最後に、Verizon Business のオンサイトとリモートのオーディタが、設計と設定を検査し、さらに安全にする方法についてアドバイスし、適合性に関する詳細なレポートを作成しました。このレポートは、[付録 F「Report on Compliance \(ROC\)」](#)に掲載されています。

PCI Solution for Retail の小売店を検証するために、Cisco Intelligent Retail Network (IRN) 参照ネットワークで使用されている 3 つの小売店をベースとしました。参照設計には、一般的な小売業向けアプリケーションおよびサービスの機能を確保するために、ワイヤレス ハンドヘルド デバイスと POS システムが含まれています。データセンターの設計は、『*Cisco Data Center Assurance Program 2.5*』に記載されたアーキテクチャのベスト プラクティスに基づいています。インターネット エッジは、インターネット エッジ参照設計に基づいたコラプストアーキテクチャで、Web アプリケーション セキュリティ分野に新しいテクノロジーが組み込まれています。対応するネットワーク、データ、およびセキュリティ管理システムは、ソリューションのすべての側面を管理および監視する方法を明確化するために文書化されています。

図 4-1 は、小売店、データセンター、およびインターネット エッジ間の接続を示す全体的なアーキテクチャを示しています。

図 4-1 エンドツーエンド物理ソリューションのアーキテクチャ

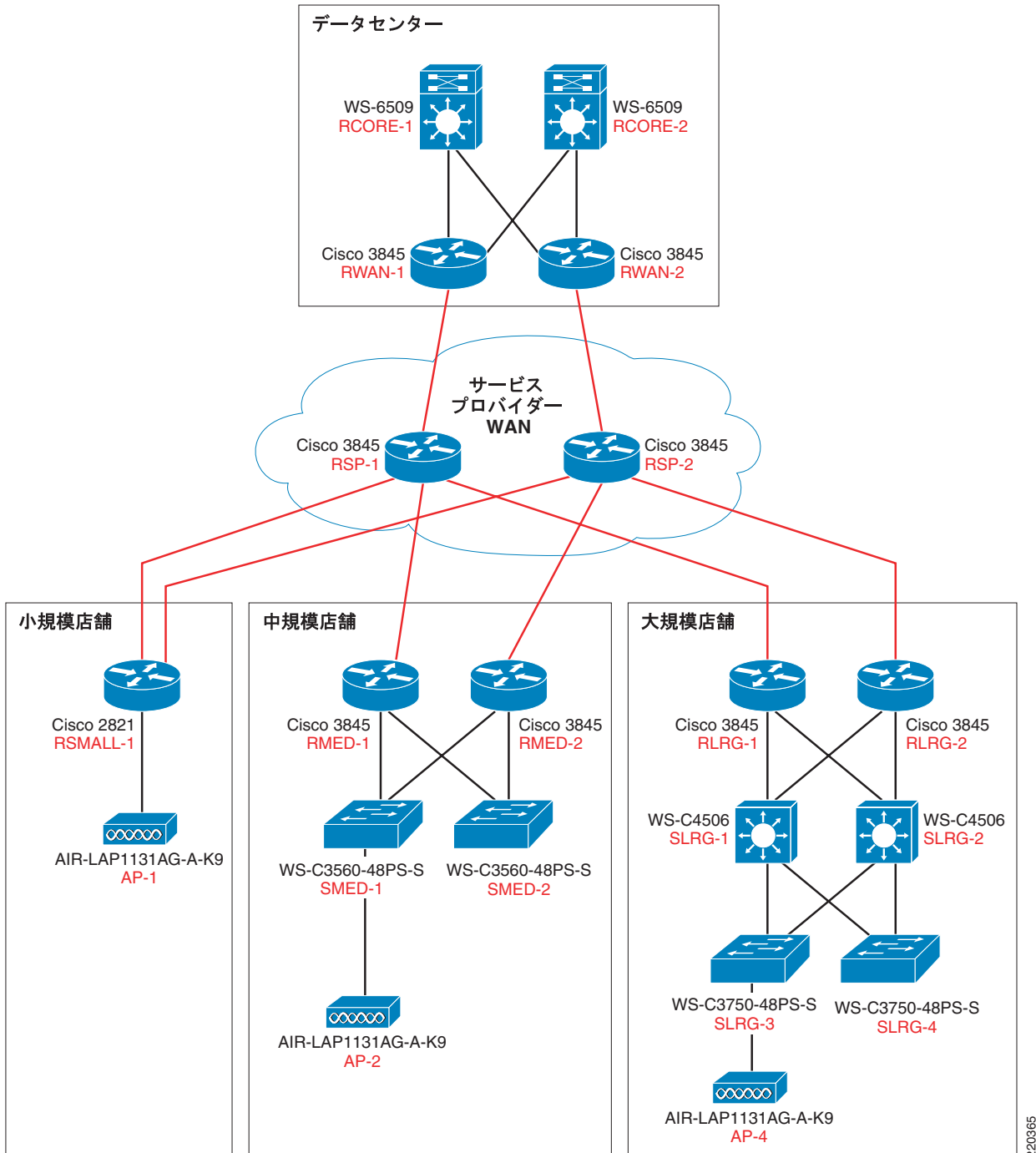


223518

ネットワーク トポロジ

図 4-2 に示すネットワーク トポロジは、プライベートルーテッドネットワークであり、3つのブランチ ネットワークを単一のデータセンターに接続しているデュアル サービス プロバイダーを持つ MPLS WAN を表しています。WAN は、サービス プロバイダー 1 (RSP-1) 上でアクティブとして実装され、サービス プロバイダー 2 (RSP-2) に対してはスタンバイとして実装されています。データセンター内のサービスの導入は、適切に分離され安全性が確保されているものとします。

図 4-2 ラボ ネットワークの概要



3つのロケーションすべてで、サービスプロバイダーへのWAN接続ではT-1回線を使用し、LANセグメントではイーサネットを使用しています。

- 小規模店舗のロケーションは、1台のルータから構成されています。このルータには、単一のワイヤレスアクセスポイントを持つネットワークデバイス用の統合スイッチングモジュールが内蔵されています。
- 中規模店舗では、デュアルルータインフラストラクチャおよび冗長LANスイッチング設計が使用されています。一般的な実装では最大6つのワイヤレスアクセスポイントを装備できますが、ここでは、単一のワイヤレスアクセスポイントが装備されています。
- 大規模店舗は、冗長ルータWAN、大容量光ファイバを備えた冗長スイッチングディストリビューションレイヤ、光ファイバで接続されたアクセスレイヤスイッチ（必要に応じてロケーション全体に分散される。大規模小売店では一般的）、および単一のワイヤレスアクセスポイント（一般的な実装では最大25まで装備可能）を使用しています。

実装されたコンポーネント

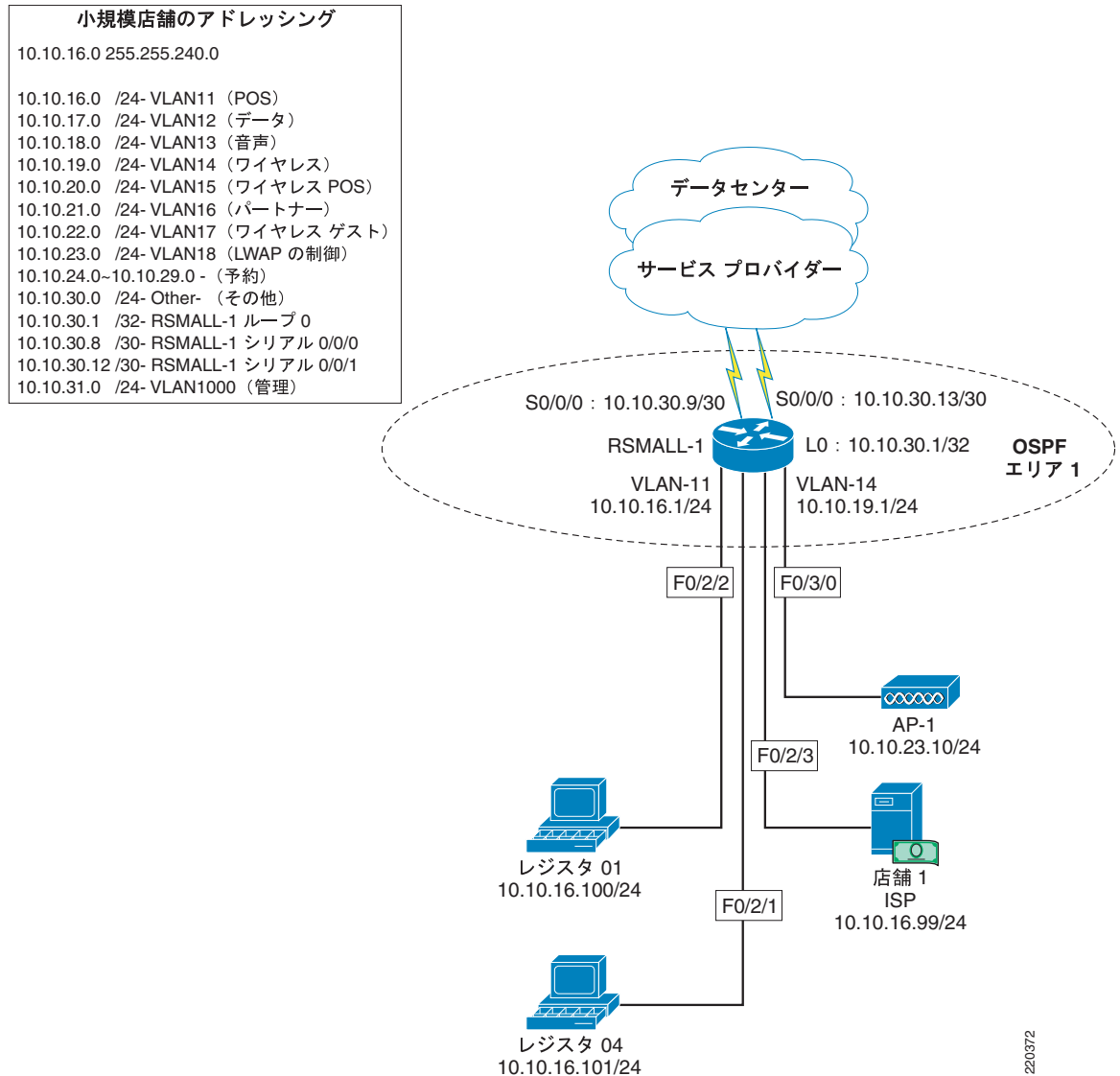
実装された主な機能とサービスは、次のとおりです。

- Cisco IOS Firewall ステートフルインスペクション
- Cisco IOS Firewall IPS 侵入検知
- Cisco IOS アクセスリスト
- VLANを使用したネットワークセグメンテーション
- SSH、HTTPS、およびSNMPv3に対応した安全な管理通信
- 中央の認証機構（CS-ACSおよびActive Directory）に対するAAA
- ワイヤレスセキュリティ（802.1x使用のWPA）
- 集中型のロギングおよび監査追跡
- 冗長NTP時間同期化
- サーバのRemote Desktop Protocol（RDP）アクセス用の強度な暗号化
- クライアント/サーバデスクトップセキュリティ用のCSA
- 感染の軽減と除去のためのアンチウイルス
- クライアントとサーバのパッチ管理のためのアップデートサービス
- リアルタイムイベントのアラートおよび通知を送るEメール
- NCR、IBM、Wincor-Nixdorfにより提供されたキャッシュレジスタ
- NCRのMobile Retail Manager（MRM）ソフトウェア
- IntermecおよびVerifoneにより提供されたワイヤレスハンドヘルド
- VeriFoneにより提供された支払い装置
- データセンターのWAN集約レイヤとコア、サービス集約、およびアクセスレイヤのシングルスレッド
- インターネットエッジの有効なシングルスレッド

すべての製品の詳細なリストは、[付録A「店舗用製品一覧」](#)に記載されています。

[図4-3](#)は、小規模店舗向けIRNソリューションを示しています。

図 4-3 小規模店舗向け IRN ソリューション

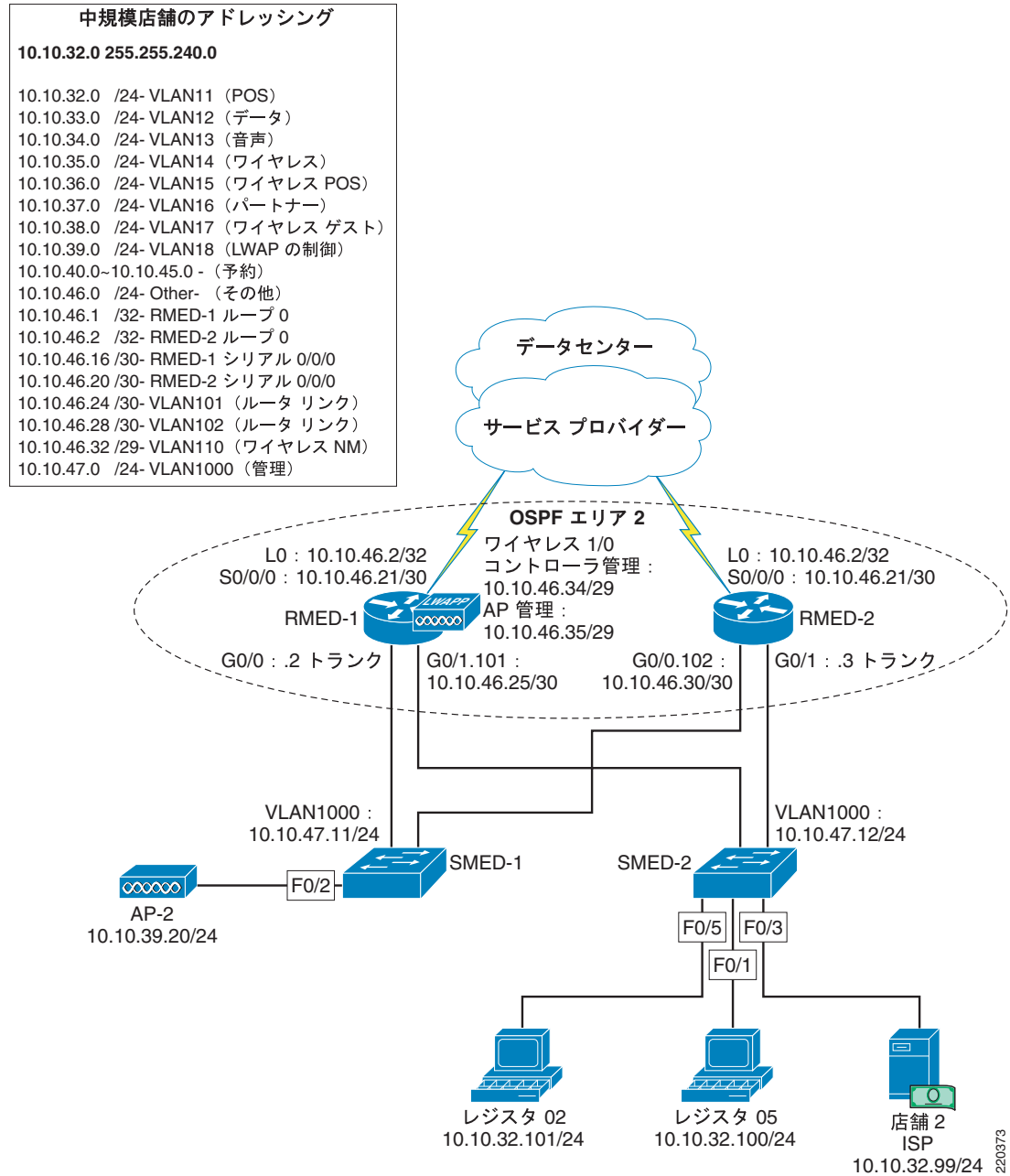


小規模店舗の実装には、次が含まれます。

- Cisco 2821 ISR ルータ (統合スイッチを装備)
- 1131 AG LWAPP アクセス ポイント
- Wincor-Nixdorf Beetle MII レジスタ
- IBM 4851 レジスタ
- Wincor TP.Net ソフトウェアおよび Cisco CSA ソフトウェアを稼働する Windows サーバ

図 4-4 は、中規模店舗向け IRN ソリューションを示しています。

図 4-4 中規模店舗向け IRN

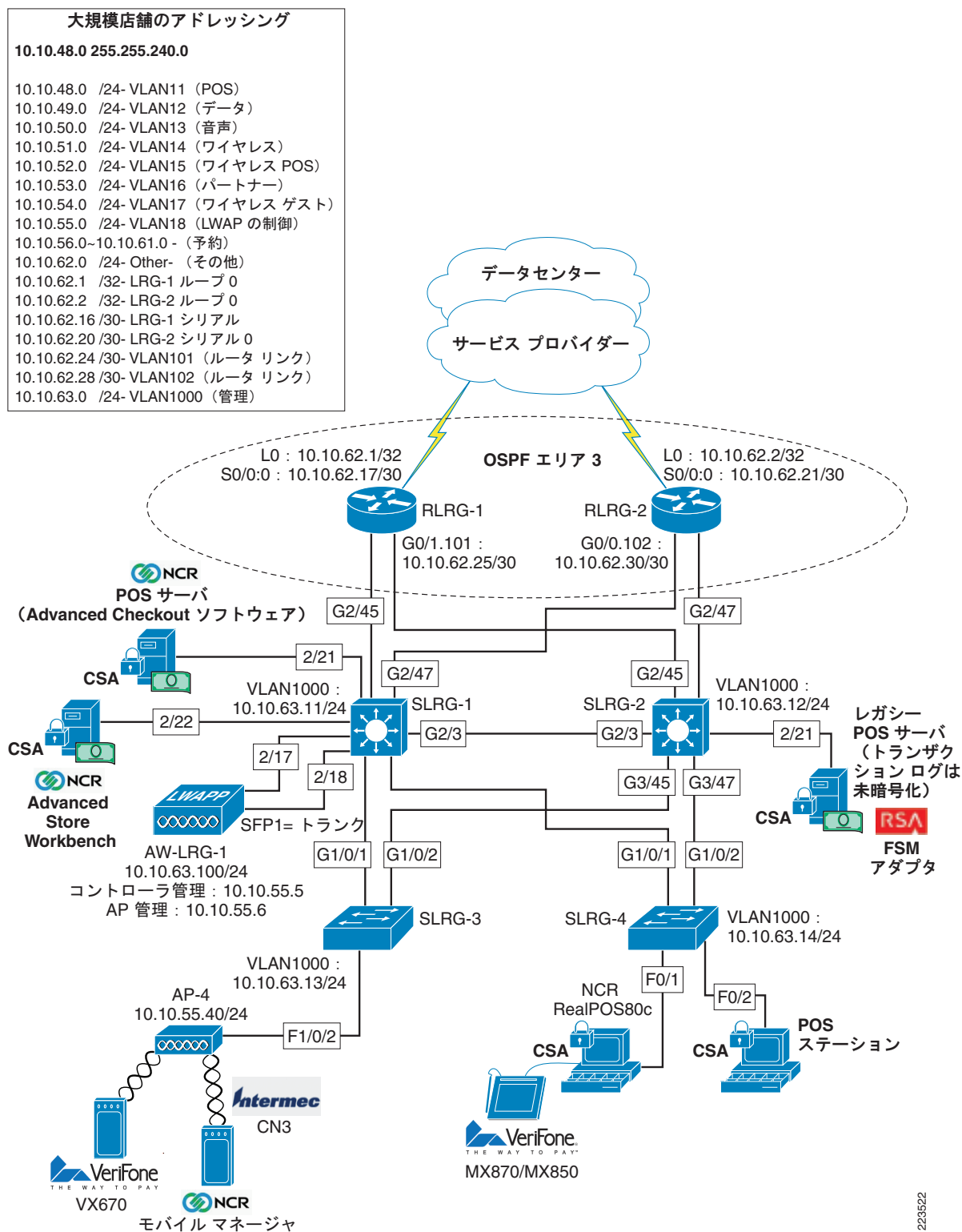


中規模店舗の実装には、次が含まれます。

- Cisco 3845 ISR ルーター
- Catalyst 3560 スイッチ
- Wireless NM Controller モジュール
- Cisco 1131 AG LWAPP アクセス ポイント
- Wincor-Nixdorf Beetle S II レジスタ
- IBM 4810 レジスタ
- Wincor POS ソフトウェアおよび Cisco CSA ソフトウェアを稼働する Windows サーバ

図 4-5 は、大規模店舗向け IRN ソリューションを示しています。

図 4-5 大規模店舗向け IRN ソリューション

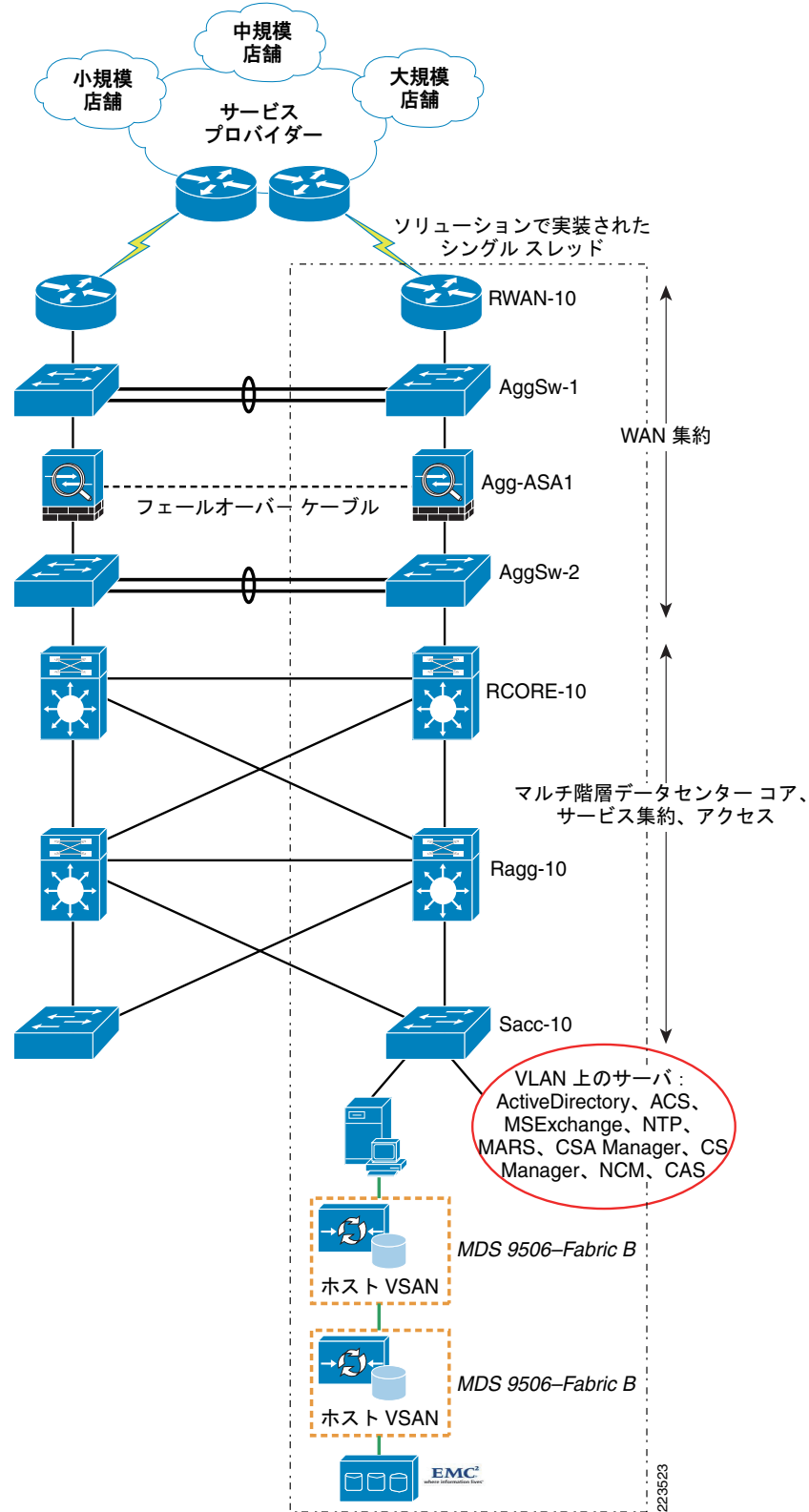


大規模店舗の実装には、次が含まれます。

- Cisco 3845 ISR ルータ
- Cisco Catalyst 3750 および 4500 スイッチ
- Cisco 1131 AG および AP1242 AG LWAPP アクセス ポイント
- Cisco 4402 Wireless Controller
- NCR RealPOS 80c 電子キャッシュ レジスタ (Advanced Checkout System ソフトウェアおよび Cisco CSA ソフトウェアを装備)
- NCR-ACS ソフトウェア、RSA File Security エージェント、および Cisco CSA を稼働する NCR サーバ
- WAN 集約レイヤで ASA 経由でデータセンターに接続する IPSec VPN

図 4-6 は、データセンターのロケーションを示しています。

図 4-6 データセンターのロケーション



データセンターに実装されている製品は、次のとおりです。

- Cisco Secure Access Control Server (CS-ACS)
- Cisco Security Agent Management Center (CSA-MC)
- Cisco Security Manager (CS-M)
- CiscoWorks LMS (C-LMS) および Resource Manager Essentials モジュール
- Wireless Control Server Manager (WCS)
- 小規模店舗ロケーション向けワイヤレス コントローラ (このラボの場合、Type 2000)
- Cisco Security Monitoring, Analysis and Response System (CS-MARS)
- Windows 2003 R2 Server 上の Microsoft Active Directory サービス
- Microsoft Exchange Server 2003
- Microsoft Windows Server Update Services (WSUS)
- Network Time Protocol (NTP; ネットワーク タイム プロトコル) アプライアンス (vmWare アプライアンス)
- Windows 2003 R2 Server (UNIX 対応 NFS ファイル サービス装備)
- 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 SecurID

図 4-7 インターネット エッジ IRN PCI ソリューション

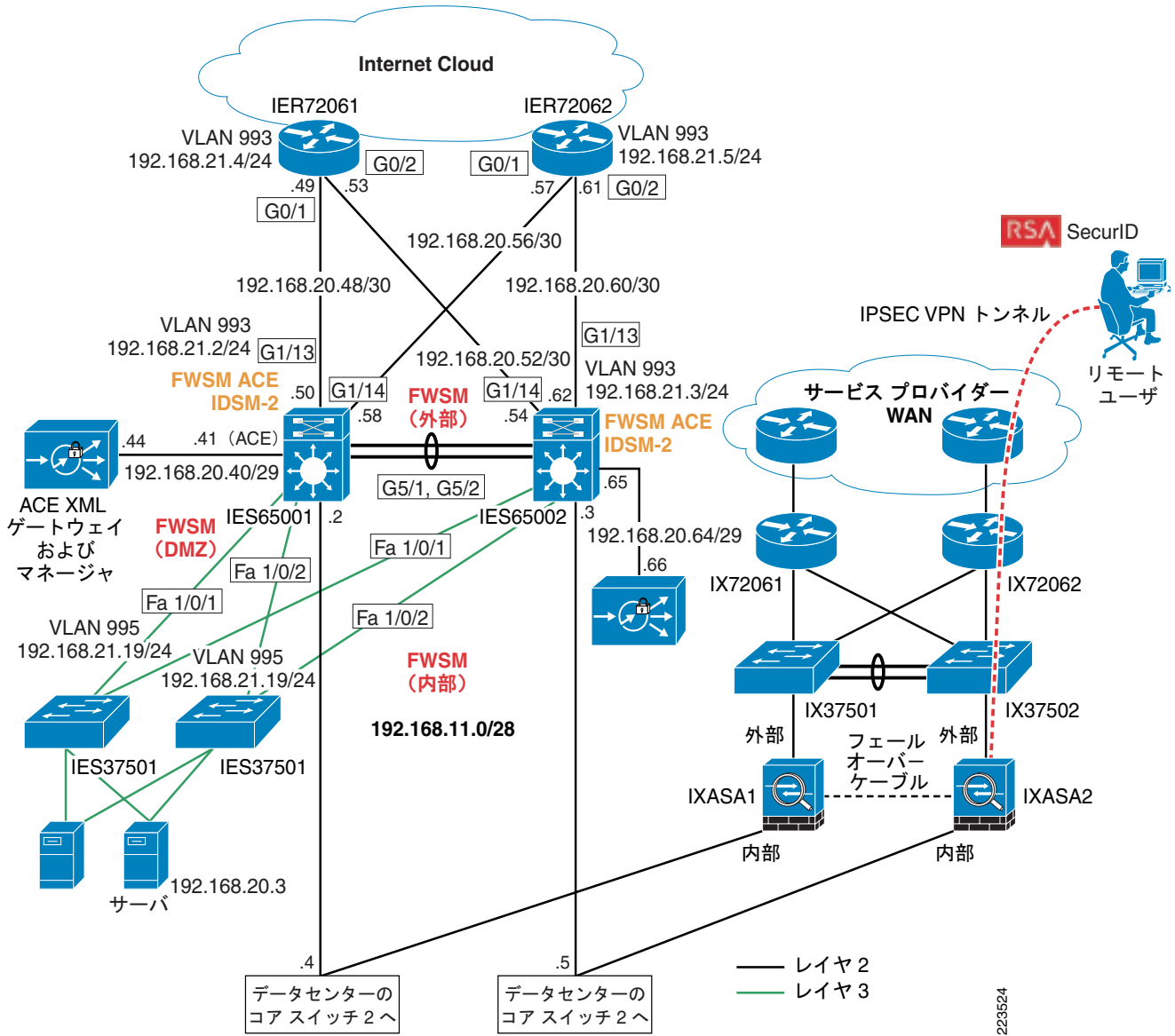
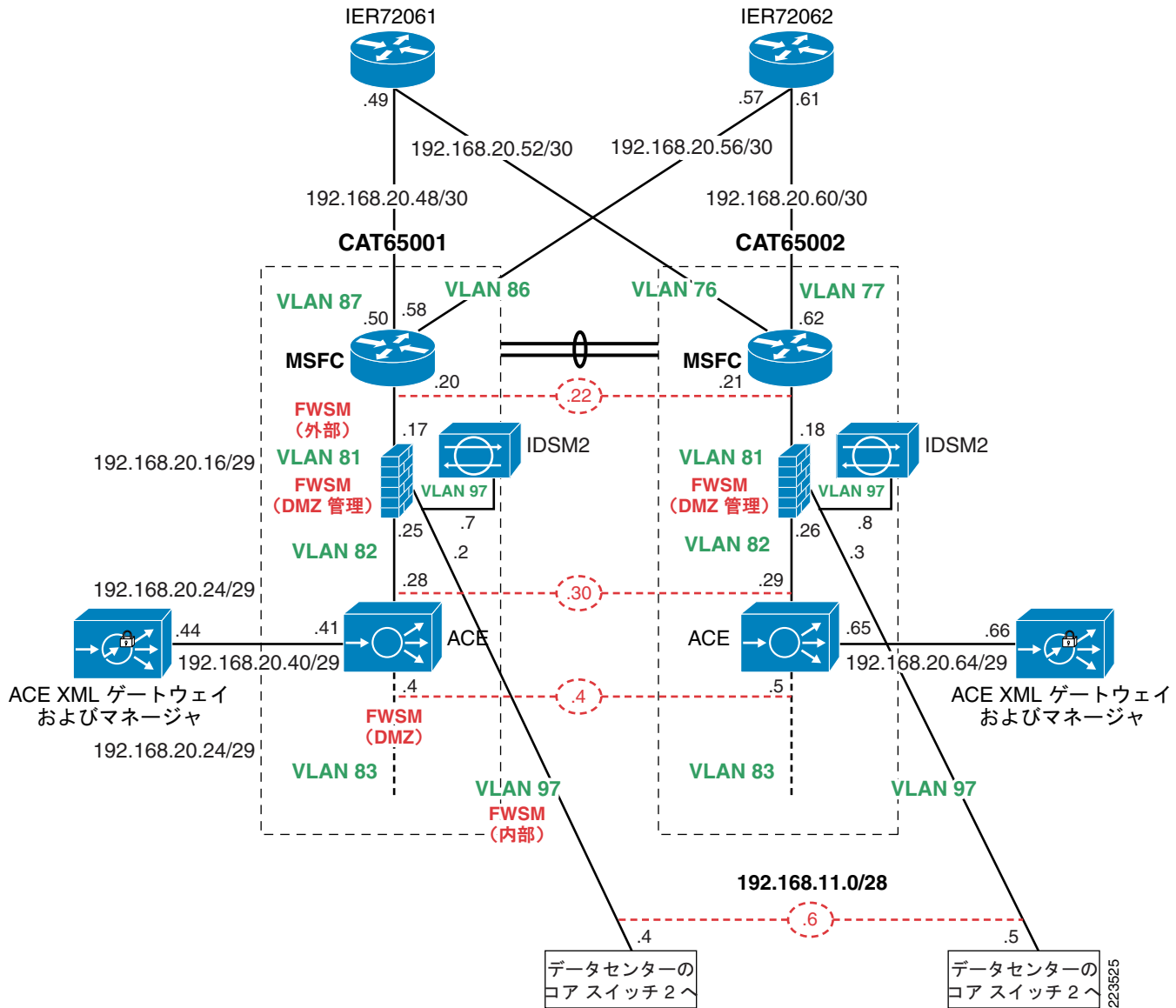


図 4-8 インターネット エッジ IRN PCI ソリューションー Catalyst スイッチ モジュールの詳細



インターネット エッジの実装には、次が含まれます。

- Cisco 7200VXR
- Cisco Catalyst 3750 および 6500 スイッチ
- 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 SecurID
- Foundstone の Hacme Bank アプリケーション

未実装のコンポーネント

- e- コマース
- 一般的な企業ネットワークのその他のロケーション（本社構内、流通センターなど）
- WAN 集約およびデータセンターにおける冗長性とハイ アベイラビリティ

監査結果

Verizon Business の QSA が実施した監査プロセスにより、ソリューションのスコープを決定する重要な点と、何を実装し何を実装しないかが明確になりました。さらに、この設計ガイドの発行以降、QSA による監査プロセスを効率化できるように監査プロセスでどのような結果が予測できるかを把握する必要のある企業にとって、この監査結果は有用な情報となっています。

- PCI オーディタは、現在、PCI 監査の実施時にストレージエリア ネットワークは調査しません。このソリューションの監査結果は、将来的にストレージ ネットワーキングに取り組む際に、どの PCI 要件に関連するかという QSA の最適な見積もりに基づいています。
- デュアルスレッド データセンターが完全冗長デバイスを保持している場合、QSA は両方のデバイスに同じ検査と要件を適用します。ハイ アベイラビリティまたは冗長性が存在しても、監査プロセスは変更されません。そのため、時間とリソースを節約するために、このソリューションの実装はシングルスレッドに限定されています。データセンターの実稼働環境では、他のシスコ設計ガイドで言及されているように、冗長性とハイ アベイラビリティを備えるようにしてください。
- 特定のフィーチャセットまたは製品をネットワークに配置することで満たすことができるのは一部の PCI 要件だけです。たとえば、要件 1 では、ファイアウォールを企業エッジに導入する必要があります。この要件を満たすために、Cisco IOS Firewall フィーチャセット装備の Cisco ISR 3845 など、ファイアウォール フィーチャセットを装備した製品を導入できます。ISR 3845 に適用される要件 1 以外にも、追加の一連の要求が適用される点にも注意が必要です。これらの要件は、配置するネットワーク デバイスに関連しています。それらを次に示します。
 - 要件 2 — ネットワークにシステムをインストールする前に、必ず、ベンダー提供のデフォルト値を変更する（たとえば、パスワード、SNMP [簡易ネットワーク管理プロトコル] コミュニティストリング、不要なアカウントの削除を含む）。
 - 要件 7 — ビジネス上知る必要があるかないかに基づいて、アクセスをカード所有者データに制限する
 - 要件 8 — コンピュータ アクセス権を持つ各人に一意の ID を割り当てる要件 7 および 8 は、ネットワーク デバイスの外部 Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントティング) の実装に関係しています。外部 AAA は、ビジネス上のルールとポリシーに基づいてユーザ アカウントごとに異なる権限レベルのアクセスを付与できるようにします。さらに、グループや汎用ユーザではなく、特定の個人について動作を追跡できるように、各ユーザ アカウントは特定の個人にマッピングされます。
- 要件 10 — ネットワーク リソースとカード所有者データへのすべてのアクセスを追跡および監視する。これらの一連の要件は、監査証跡とネットワークデバイス上のイベントのログギングに関係しています。ネットワーク デバイスに関連する設定を変更したり、ネットワーク アクティビティをログギングして、その後ネットワークの科学捜査で使用できるようにするためです。
- QSA は、Tlog（ペイメント カード データ）ファイルが暗号化されており、シスコのセキュア VPN ソリューションを介して転送される場合でも、店舗から本社（HQ）データセンターへの Tlog ファイルの移動には、安全な自動または手動プロセス（セキュア FTP など）を使用してください。

- また、監査の準備段階で、ネットワーク デバイスのセキュリティの脆弱性を国内脆弱性データベースに照合してチェックしてください。詳細については、<http://nvd.nist.gov/nvd.cfm> を参照してください。

テスト

これらのアーキテクチャでは、特定のトラフィック スループット レベルまたは容量レベルを満たすかどうかについてのテストは行っていません。店舗参照設計におけるホストのスケールリングの考慮事項は、一般的な小売店の ベスト プラクティスに基づいています。特定の設計目的以外の場所でこれらの設計を使用しても、必要なパフォーマンス レベルが得られないことがあります。テストの目的は、PCI DSS 要件に基づいて、ベスト プラクティスと言えるセキュリティの推奨事項を決定することでした。

機能のテスト

- 設計の機能性に関するテストでは、リモートでの管理および設定タスク、POS 対応のクライアント トランザクション、E メールによるメッセージとアラート、Windows アップデート サービス、および NTP 時間同期化を実行しました。
- ネットワーク デバイスとシステム ホストがさまざまなロケーション間で到達可能であることを検証するために、**Ping** コマンドや **Traceroute** コマンドなどの ICMP ツールを使用しました。
- ワイヤードおよびワイヤレスの両方のトラブルシューティングで、ネットワーク トラフィックをキャプチャするために WildPackets OmniPeek Personal ネットワーク アナライザを使用しました。

PCI 監査のテスト

- Cisco PCI Solution for Retail の QSA オーディタとして Cybertrust が実行した手順については、[付録 F「Report on Compliance \(ROC\)」](#) で詳しく説明しています。
- Cybertrust では、デバイスの設定とネットワーク図の検査に加え、数週間に渡って、デバイスと管理プラットフォームを構築および設定した各テクノロジーの専門家に広範囲に及ぶインタビューを実施し、データセンター ロケーションに接続された状態でネットワークの脆弱性評価スキャンを実行しました。このスキャンでは、nCircle ソフトウェアを使用し、ネットワーク内のすべてのサーバ、クライアント、およびデバイスを評価しました。この初期スキャンの結果については、[付録 C「アプリケーション プロトコル」](#) を参照してください。スキャンでは、後から修正されたいくつかの項目が特定されました。それ以降はスキャンは実行されませんでした。

設定作業

ルーティングとスイッチング

- ルータとスイッチは、共通のベスト プラクティスおよびルータ強化技術を使用して設定されました。
- 実装されたネットワーク プロトコルは IPv4 のみで、各ロケーションには、階層型で定義された RFC 1918 アドレスの集約可能なブロックが割り当てられました。各店舗 LAN は、データ、音声、POS、管理、およびワイヤレスの各ニーズに応じてトラフィックを適切に分離するために、複数の VLAN セグメントに分割されました。

- PAD、TCP、および UDP の小型のサーバやフィンガーなど、不要で安全でないサービスは無効化されました。これらの設定項目が設定内に表示されない Cisco IOS バージョンでは、すでにデフォルトでオフになっていることがあります。
- ハードウェアがサイトから除去された場合に設定が開示されるのを防ぐため、サービス パスワード暗号化は有効に、サービス パスワード回復は無効に設定されました。
- AAA 認証が設定され、CS-ACS を記載しました。ローカル ユーザ名とパスワードは、CS-ACS が到達不能な場合にアクセスが許可されるように設定しました。このローカル アカウント パスワードは、四半期ごとに変更する必要があります。
- 時間を同期化し、イベントをログするために、NTP を設定しました。時間帯を PST に設定し、サービス タイムスタンプをセットしました。
- **crypto key generate rsa** コマンドを使用して、ローカル セキュリティ証明書を作成しました。キーの長さは 1024 ビットに設定されました。
- セキュア HTTP サーバは有効化され、非セキュア HTTP サーバは無効化されました。さらに、SSH 接続だけを許可するように、VTY インターフェイスを設定しました。
- CiscoWorks と CS-MARS の両方に Syslog イベントを送信するようにロギングを設定しました。
- V3 ユーザおよびパスワードを使用して SNMP を設定しました。このアカウントも、四半期ごとに変更する必要があります。
- **no exec** を設定することで、補助回線インターフェイスと未使用回線インターフェイスは無効化されました。
- ループバック インターフェイスを作成し、ログ、トラップ、認証要求、および時間要求の送信元として使用しました。
- すべてのインターフェイス IP アドレスが DNS に定義されました。
- OSPF プロセス配下のルータ インターフェイスは、デフォルトとしてパッシブに設定され、その後、シリアル WAN リンクや LAN インターコネクトなどの必要なインターフェイス上で明示的に許可されました。これは、すべて ACL を保持していたため、適切なインターフェイスを通じてトラフィックフローを制御するために必要でした。

ルータとスイッチの詳細な設定は、付録 E「Device Configurations」で参照できます。

詳細については、次の参考資料を参照してください。

- 『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/ns432/c649/cdcont_0900aecd801a8a2d.pdf
- 『Enterprise Architecture Solutions』 :
http://www.cisco.com/en/US/netso/ns477/networking_solutions_packages_list.html

Unified Wireless

ワイヤレスは、Lightweight Access Point Protocol (LWAPP; Lightweight アクセス ポイント プロトコル) コントローラを使用して実装されました。中規模および大規模店舗ロケーションには、それぞれ専用のローカル コントローラが配置されました。小規模店舗は、データセンター内の中央集中型 LWAPP コントローラから操作しました。小規模店舗内の AP は、WAN 障害の発生時に Hybrid REAP モードで動作するように設定しました。これらの各コントローラは、WCS Manager を介して集中的に管理および設定しました。コントローラは、Syslog メッセージを CS-MARS に送信します。

ワイヤレス セキュリティに関する PCI 要件を最適に満たすために、ワイヤレス アクセス時にユーザ認証を要求する 802.1x を使用して WPA を導入しました。個別の VLAN にマッピングされた異なる SSID を使用して、複数のワイヤレス セグメントが設定されました。これにより、POS

トラフィックは、他のワイヤレストラフィックから分離しました。ワイヤレス ネットワークへのアクセスを必要とする各ユーザに、一意のユーザ ID とパスワードを割り当てました。この認証は、RADIUS プロトコルを使用し、CS-ACS サーバを介して、Active Directory ユーザ データベースに対して実行されました。Intermec ワイヤレス ハンドヘルドは、アクセスと認証に Funk クライアントを使用しました。また、ワイヤレス ネットワークへのアクセスには、Cisco ワイヤレス ラップトップと Odyssey クライアントも使用しました。PCI ガイドラインではパスワードの保存は許可されていませんが、これらのクライアントはどちらもローカルでのユーザ ID とパスワードの保存をサポートしています。

ネットワーク上での認証時には、ワイヤレス セグメントごとに DHCP を介して IP アドレスと DNS オプションが提供されました。

詳細については、次の URL にある『*Installation Guide for Cisco WCS Manager*』を参照してください。

http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_book09186a00806b57ec.html

Adaptive Security Appliance

Adaptive Security Appliance (ASA) を、WAN 集約レイヤとインターネットエッジのエクストラ ネット セグメントでファイアウォールとして使用しました。ASA には、アクセス コントロール リスト、ステートフルパケット インスペクション、およびインターフェイスでのセキュリティ レベルを設定しました。

デフォルトでは、ASA を経由するトラフィックはすべて、Adaptive Security Algorithm (アダプティブ セキュリティ アルゴリズム) を使用して検査され、ASA の経由が許可されるか、または廃棄されます。

ASA は、新しい接続を認識した場合、パケットをアクセス リストに照合してチェックし、そのパケットを許可するか拒否するかを決定するための他のタスクを実行しなければなりません。このチェックを実行するため、セッションの最初のパケットはセッション管理パスを通過します。トラフィックのタイプによって、コントロールプレーンパスを通過することもあります。

セッション管理パスは、次のタスクを実行します。

- アクセス リストのチェックの実行
- ルート ルックアップの実行
- NAT 変換 (xlate) の割り当て
- 高速パスでのセッションの確立



(注)

セッション管理パスと高速パスは、加速化されたセキュリティ パスから構成されます。

レイヤ7インスペクションを必要とする (パケット ペイロードを検査または変更する必要がある) 一部のパケットは、コントロールプレーンパスに渡されます。レイヤ7インスペクション エンジンには、次の2つ以上のチャネルを持つプロトコルの場合に必要となります。

- well-known ポート番号を使用するデータ チャネル
- セッションごとに異なるポート番号を使用するコントロール チャネル

このようなプロトコルには、FTP、H.323、SNMP が含まれます。

Q. これは、確立済みの接続ですか。

A. 接続がすでに確立されている場合、セキュリティ アプライアンスはパケットを再度チェックする必要はありません。大半の一致するパケットは、双方向で高速パスを経由できます。高速パスは、次のタスクを実行します。

- IP チェックサムの検証

- セッションルックアップ
- TCP シーケンス番号のチェック
- 既存のセッションに基づく NAT 変換
- レイヤ 3 およびレイヤ 4 ヘッダーの調整

UDP または他のコネクションレス型プロトコルの場合、セキュリティ アプライアンスは、**高速**パスも使用できるように、接続状態情報を作成します。レイヤ 7 インспекションを必要とするプロトコルのデータ パケットも**高速**パスを経由できます。

一部の確立済みセッションのパケットは、セッション管理パスまたはコントロールプレーンパスを継続して経由する必要があります。セッション管理パスを経由するパケットには、インспекションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロールプレーンパスを経由するパケットには、レイヤ 7 インспекションが必要なプロトコルのコントロール パケットが含まれます。

インターフェイスセキュリティ レベルは、さまざまな ASA 機能に影響します。次の動作の制御にレベルを使用します。

- ネットワーク アクセス — デフォルトでは、上位のセキュリティ インターフェイスが下位のセキュリティ インターフェイス（発信）を明示的に許可します。上位のセキュリティ インターフェイスのホストは、下位のセキュリティ インターフェイスの任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することで、アクセスを制限できます。同じセキュリティ インターフェイスの場合、インターフェイスには、同じセキュリティ レベルまたはそれより下のセキュリティ レベルの他のインターフェイスへのアクセスが明示的に許可されます。
- インспекション エンジン — 一部のアプリケーション インспекション エンジンは、セキュリティ レベルに依存しています。同じセキュリティ インターフェイスの場合、インспекション エンジンはどちらの方向にも適用されます。
 - NetBIOS インспекション エンジン — 発信接続にのみ適用されます。
 - SQL*Net インспекション エンジン — SQL*Net（以前の OraServ）ポートの制御接続が 1 ペアのホスト間に存在する場合は、セキュリティ アプライアンスを通じて着信データ接続だけが許可されます。
- フィルタリング — HTTP (S) および FTP フィルタリングは、発信接続（上位レベルから下位レベル）のみに適用されます。同じセキュリティ インターフェイスの場合、どちらの方向のトラフィックもフィルタできます。
- Network Address Translation (NAT; ネットワーク アドレス変換) の制御 — NAT 制御が有効で、上位セキュリティ インターフェイス（内部）上のホストが下位セキュリティ インターフェイス（外部）上のホストにアクセスする場合は、上位セキュリティ インターフェイス上のホストに NAT を設定する必要があります。NAT 制御が使用されていないか、同じセキュリティ インターフェイスの場合は、任意のインターフェイス間で NAT を使用するか、または NAT を使用しないかを選択できます。外部インターフェイスに NAT を設定する際に、特別なキーワードが必要となる場合があること注意してください。
- Established コマンド — このコマンドは、すでに上位レベルのホストから下位レベルのホストへの確立済みの接続がある場合に、下位セキュリティ ホストから上位セキュリティ ホストへの戻り接続を確立できます。

同じセキュリティ インターフェイスの場合は、両方向に **established** コマンドを設定できます。ASA の設定方法の詳細については、次のドキュメントを参照してください。

- 『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

ストレージエリア ネットワーク

ソリューションでは、データセンターのストレージ アクセス レイヤを、EMC DMX 1000 ストレージアレイと Cisco MDS 9509 スイッチが配置された VSAN 環境に接続する必要があります。

- EMC ストレージアレイ (DMX 9000) は、QSA の監査対象外でした。QSA に従い、PCI オーディタは、現在、PCI 監査の実施時に SAN を検査しません。このソリューションの監査結果は、将来的にストレージ ネットワーキングに取り組む際に、どの PCI 要件が関連するかという QSA の最適な見積もりに基づいています。
- MDS 9500 は、カード所有者データを格納するディスクの論理パーティションの安全性を確保するために、それらにゾーン分割と LUN マスクが設定されているかぎり、監査対象となりました。論理ディスク パーティションへアクセスする必要のあるデータセンター内のホストマシンだけにアクセスが許可されました。その一連のホストマシンへのユーザアクセスの制限は、このソリューションの対象外です。

監査に合格するために、MDS スイッチは少なくとも、デフォルト以外のパスワードとシステムパスワードに関する 2.x の要件セット、強力なアクセス コントロールに関する 7.x 要件、および強力なパスワード設定に関する 8.x 要件を満たす必要があります。

次に、ゾーン分割設定のスナップショットを示します。**PCI-Retail-HBA1** ゾーンは、データセンター内の特定のファイル サーバを許可するために作成されました。さらに、光ファイバホストバス アダプタとともにインブートされ、直接この MDS スイッチに接続されました。これにより、特に、カード所有者データ ファイル サーバ用の EMC ストレージアレイで作成された VSAN 900、LUN 0090 へアクセスできるようになりました。

```
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-sflek9-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-sflek9-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

                                User-generated
Identifier      Type      Node Name      Port Name      Devices
-----
210000e08b01c3e5  Fibre  210000e08b01c3e5  210000e08b01c3e5  010B
                                           0142:0143

10000000c92c10d4  Fibre  targethost1      10000000c92c10d4  None
10000000c92c13de  Fibre  10000000c92c13de  10000000c92c13de  None
210000e08b01bfe5  Fibre  ecc               210000e08b01bfe5  0184
10000000c92c0f2e  Fibre  10000000c92c0f2e  10000000c92c0f2e  0029:002A
                                           014A:014F
                                           015D:0161
                                           0164

10000000c92c142e  Fibre  10000000c92c142e  10000000c92c142e  None
10000000c92c1371  Fibre  node3             10000000c92c1371  00B9:00BA

Director Identification : FA-4A
Director Port           : 0

                                User-generated
Identifier      Type      Node Name      Port Name      Devices
-----
210000e08b01bfe5  Fibre  ecc               210000e08b01bfe5  0162:0163
210000e08b01c3e5  Fibre  210000e08b01c3e5  210000e08b01c3e5  None
10000000c95d28d9  Fibre  PCI-RETAIL       HBA1             0090

```

ゾーン分割と LUN（論理ユニット）マスクの詳細については、次を参照してください。

- 『*Using VSANs and Zoning with the Cisco MDS 9000 Family*』 ホワイトペーパー :
<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

管理

CiscoWorks LAN Management System (C-LMS)

各ルータとスイッチは、CiscoWorks が集中的に追跡し管理できるように、SNMPv3 および Syslog 対応として設定されました。ルータとスイッチのコンフィギュレーションは、毎日ポーリングされアーカイブされ、これらのコンフィギュレーションは、主要な PCI 適合性設定項目に関して検査されました（つまり、**no ip http server**、**transport input ssh** など）。項目の設定が変更された場合、アラート E メールが生成され、適切なアカウントに送信されました。コンフィギュレーションアップデートとソフトウェア アップデートをネットワーク内のデバイスに展開するために RME を使用しました。設計、承認、および配置の変化に関するプロセス管理は CiscoWorks で行います。ワイヤレス コントローラの syslog は、製品上の制限のため、CiscoWorks には送信できませんでした。

詳細については、次を参照してください。

- 『*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_book09186a0805305cb.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_book09186a08050faf6.html

Cisco Security Manager (CS-M)

CS-M は、HTTPS および SNMPv3 を介してルータ インターフェイスにアクセス リストと inspect 文を展開するように設定されました。すべてのデバイスとアプリケーションのアプリケーショントラフィック フローは、ネットワーク トレース、ロギング ACL、および製品マニュアルに記載された広範な調査機能を使用して、綿密に計画されました。これらのフローは、表に一覧されました（付録 C「アプリケーション プロトコル」を参照）。その後、この情報を使用して、firewall inspect 文と組み合わせて、ルータに着信するすべてのネットワーク インターフェイス上の実装に合わせた ACL が作成されました。これらの包括的なアクセス リストを導入したあと、POS およびネットワーク アプリケーションの機能性を検証しました。

CS-M は、コマンド **ip verify unicast source reachable-via rx** をすべてのインターフェイスに自動的に追加します。このコマンドは、着信トラフィックがインターフェイス上でスプーフィングされていないことを検証します。

また、標準の SDF ルールを使用し、SDEE アラートを CS-MARS に送信するために、IPS も CS-M 経由で実装されました。

詳細については、次を参照してください。

- 『*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

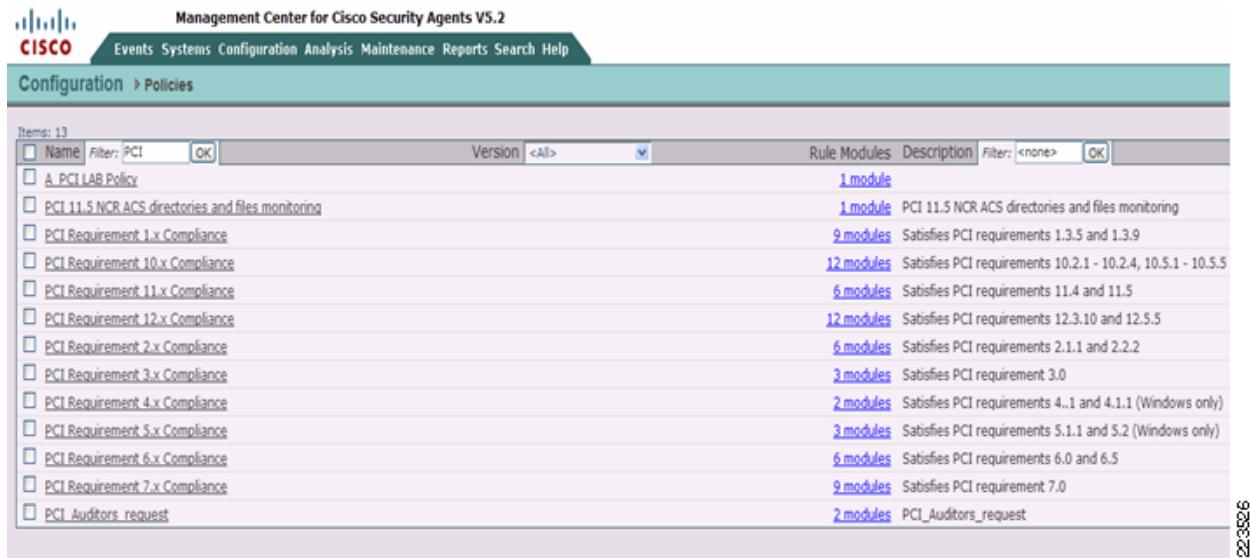
Cisco Security Agent (CSA)

ホストベースのセキュリティを提供するために、すべてのサーバとワークステーションに CSA を配置しました。CSA は、ホストベースの侵入防御、アプリケーション実行保護、およびオペレーティング システムのロックダウンを提供します。クライアントのポリシーは、CSA Manager Center で集中的に管理され展開されます（図 4-9 を参照）。アラートとイベントは、CS-MARS と相互運用するように設定された CSA-MC に送信され集中的に監視および分析されます。NFS バックアップ サーバ上の CSA クライアントが、PCI 要件 10.5.5 に従い、アーカイブされた syslog とその他のイベントのファイルの保全性を監視します。

CSA-MC にアクセスする管理者を認証するには、ユーザをローカルで定義し、認証要求を LDAP を介して Active Directory に転送します。ユーザは、ログイン時には（ユーザ ID ではなく）フルネームを入力する必要があります（つまり、AD のユーザ ID である「bmcgloth」の代わりに、名前「Bart McGlothlin」を使用してログインします）。また、何らかの理由で Active Directory または他の LDAP サーバが使用不能になった場合に備え、フォールバック認証用としてもローカルに定義されたユーザ名とローカルパスワードが設定されます。このローカル認証機能は、単独では、PCI 仕様に必須のパスワードの複雑さと履歴要件を満たしていないため、認証のプライマリ方式として使用するのとは避けてください。CSA-MC には、さまざまな管理タスクを実行するためのロールベースのユーザを設定しました。

さらに、PCI 適合性ポリシーを CSA-MC にインポートできるため、それを使用して、ポリシーを実施したり、PCI 適合性を監視したりできます。

図 4-9 CSA 管理



詳細については、次を参照してください。

- 『Installation Guide for CSA Version 5.1』:
http://www.cisco.com/en/US/products/sw/secursw/ps5057/products_installation_guide_book09186a008067b78a.html

データセンターのサービス

Cisco Secure CS-MARS のイベント モニタリングとアラート

CS-MARS は、CSA クライアント、ルータ、スイッチから受信したイベント、および CS-ACS からの認証イベントに対応する中央のモニタリングおよびアラート ツールとして配置されました。CS-MARS は、特定の CSA イベント（許可されていない CS-ACS イベントログへの書き込み）を受信したときに E メール アラートを送信するように設定され、イベント アラートを実証できるようにしました。CS-MARS には、ロールベースの管理が装備されましたが、ローカル ユーザ アカウントとパスワードのみをサポートします。これらのローカル ID は、PCI 仕様に必須のパスワードの複雑さと履歴要件を十分に備えていないため、このコンソールは、データセンター内の他の汎用サービスから分離し、追加の認証リソースによって保護する必要があります。このタイプの補完コントロールは、この設計ではまだ実装されていません。

詳細については、次を参照してください。

- http://www.cisco.com/en/US/products/ps6241/products_installation_and_configuration_guide_book09186a00806bbf91.html

Cisco Secure Access Control Server (CS-ACS) 認証

個々のユーザ アカウントは、Active Directory 内で作成され、通常の企業における個々のロールに基づいてグループに分類されました。これらのグループは、CS-ACS 内の認証グループにマッピングされ、グループごとに適切な権限とアクセス権が割り当てられました。この認証方式は、適切なパスワードの複雑さ、履歴、および非アクティビティ要件を確実に満たすために使用されました。CS-ACS 製品単独では、スタンドアロン認証製品としてこれらの要件を満たしていません。

詳細については、次を参照してください。

- 『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)

確立済みの適合性ポリシーを有効なデバイス間に適用するために C-NCM を使用しました。デバイスの設定が企業ポリシーに反して変更された場合、C-NCM は管理対象のデバイスの設定を動的に元に戻します。C-NCM は、他数のマルチベンダー製品をサポートしています。

詳細については、次を参照してください。

- 『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

インターネット エッジ

Cisco Firewall Services Module (FWSM)

Cisco FWSM は、共通のベスト プラクティスと推奨事項に基づいて次のように設定されました。

- パッシブな FTP モードなどの安全でないサービスは、設定で無効化されました。
 - AAA 認証が設定され、CS-ACS がポイントされました。ローカル ユーザ名とパスワードは、ACS が到達不能な場合にアクセスが許可されるように設定されました。このローカルアカウントパスワードは、四半期ごとに変更する必要があります。
- FWSM に設定されたアクセスリストは、通信で必要なものはかなり限定されました（つまり、特定のプロトコルとポートのみを許可）。
- SSH バージョン 2 を使用する特定のホストから FWSM への管理セッションだけが許可されました。
 - crypto key generate rsa** コマンドを使用して、ローカル セキュリティ証明書が作成されました。キーの長さは 1024 ビットに設定されました。
- ロギングは、CS-MARS に syslog イベントを送信するように設定しました。
- FWSM の設定は C-NCM を使用してバックアップしました。

詳細については、次を参照してください。

『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 Service Module (IDSM2)

共通のベスト プラクティスと推奨事項に基づいて次のように Cisco IDSM2 を設定しました。

- IDSM2 は、ユーザがログイン試行を継続して実行できないように、一定回数のログイン試行に失敗するとアカウントをロックするように設定されました。
- IDSM2 の管理は、SSL 接続を持つ Cisco IPS Device Manager を使用した特定のホストからの管理だけが許可されました。
- イベントの関連付けのため、IPS ソフトウェアが提供する攻撃情報を CS-MARS に送信しました。
- ユーザがアクセスしているプライベートなシステムとデバイスについて、そのユーザに通知するためにログイン バナーを設定しました。
- IDSM2 を、DMZ ゾーン内の VLAN を監視するように設定しました。

詳細については、次を参照してください。

『*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

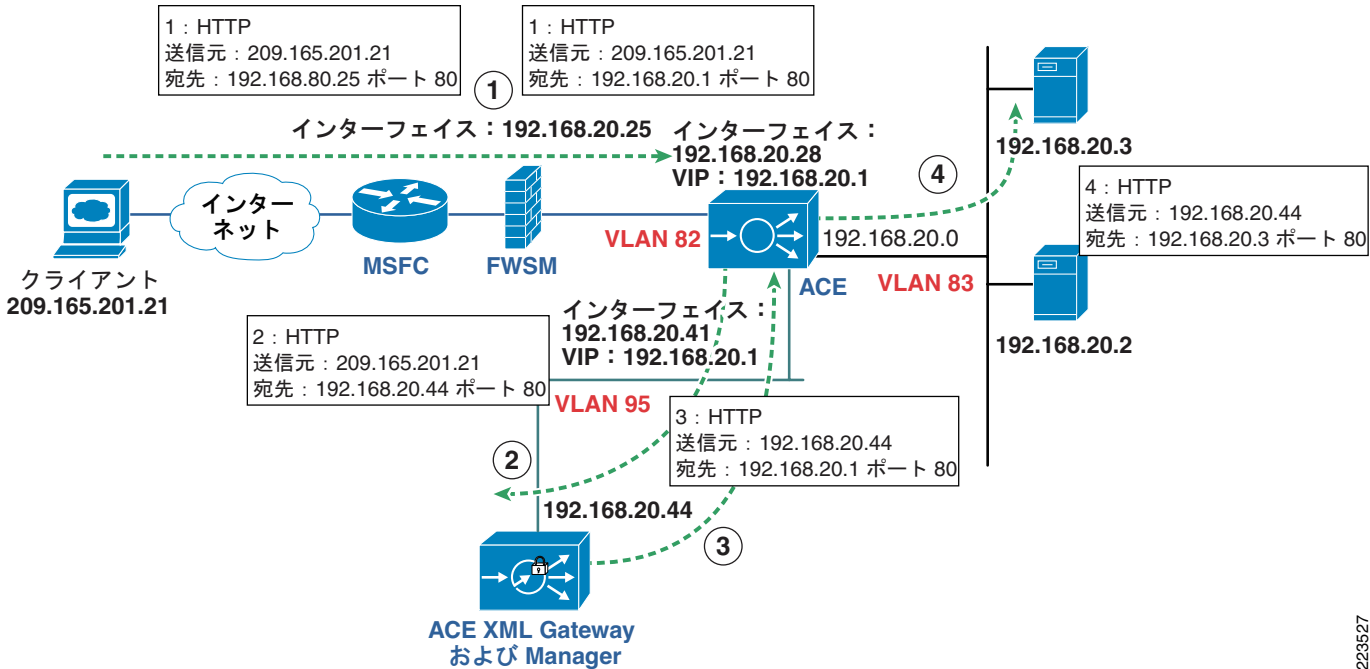
Cisco ACE XML Gateway はファイアウォール機能を備え、異なる信頼ゾーン間の各サービス境界で必要不可欠な保護を提供します。Cisco ACE XML Gateway は、ネットワーク トラフィックのトランスポート レイヤとセッション レイヤで動作する以外に、アプリケーション レイヤに主に重点を置き、XML メッセージのペイロードを処理する点でネットワーク ファイアウォールとは異なっています。境界防御ロールでは、Cisco ACE XML Gateway は、不正な XML ペイロード、構造的に無効な XML メッセージ、および XDoS（XML サービス拒絶）攻撃の防御など広範なセキュリティ サービスを実行するとともに、否認防止、メッセージの暗号化と保水性、プライバシーなどのその他のセキュリティ機能も実行します。

ラボ環境では、Cisco ACE XML Gateway と Cisco ACE XML Manager は同じアプライアンスに設定されました。Cisco ACE XML Gateway の実装の管理サーバは、Cisco ACE XML Manager です。Cisco ACE XML Manager は、システムの開発および監視ポイントとして機能します。Web コンソールとして動作し、システムを設定および監視するための Web サービス インターフェイスとなります。インターネット エッジ DMZ 内の Web アプリケーション サーバは、オンラインバンキング アプリケーションとその他の Web アプリケーションを稼働しています。Cisco ACE XML Gateway のテストでは、PCI 6.5 要件で言及されている、Web アプリケーションのセキュリティの既知の不具合を対象とした攻撃の軽減に重点が置かれました。

図 4-10 に示すシナリオでは、クライアントは、Cisco Application Control Engine (ACE) モジュール上の NAT 変換された Virtual IP Address (VIP; 仮想 IP アドレス) に対する HTTP 要求を生成します。その後、この要求は Cisco ACE XML Gateway に転送され、そこで、アプリケーション レイヤ攻撃に対する攻撃防御が実行され、HTTP 1.1 要求は多重化されてサーバに返送されます。ここでは、Cisco ACE XML Gateway は、着信 HTTP トラフィックを一連のサーバに迅速に送信する逆プロキシアプライアンスとして動作します。Cisco ACE XML Gateway は、DMZ 内のサーバのサーバプールとして設定することができます。これにより、Cisco ACE XML Gateway を通じて露呈されたバックエンドサーバが提供するサービスのスケーラビリティと信頼性を改善できます。

Cisco ACE XML Gateway は、現在、ボックスツーボックス冗長性はサポートしていません。追加された複数の Cisco ACE XML Gateway は、Cisco ACE システム設計の一部として動作するため、冗長性が提供されます。Cisco ACE は、Cisco ACE XML Gateway が着信要求を転送する際に、設定されたポリシーと個々の Cisco ACE XML Gateway の状態に基づいて、ロードバランシングを決定します。

図 4-10 クライアント/サーバ間の HTTP トラフィック フロー



詳細については、次を参照してください。

- Cisco ACE XML Gateway および ACE XML Manager の実装と設定：
http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html
- Cisco ACE Module のコンフィギュレーション、管理、およびセキュリティ設定：
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_installation_and_configuration_guides_list.html
- 『Service Module Design with ACE and FWSM』：
www.cisco.com/univercd/cc/td/doc/solution/ace_fwsm.pdf

その他の要素

時間同期は、イベントと監査ログの相関付けにおいて重要です。このため、PCI 要件として、複数の信頼できる時刻源と同期される冗長 NTP サーバを配置する必要があります。このサービスを提供するため、2 つの VMware ベースの NTP アプライアンスを配置しました。これらのアプライアンスは、Mandriva Linux 2006 に基づき、ntpd 4.2.0@1.1161-r を使用します。このアプライアンスは、pool.ntp.org (13 + time.nist.gov) からランダムに IP アドレスを取得します。その後、仮想マシンクロックを同期し、NTP サーバサービスを開始します。すべてのネットワーク デバイスとサーバは、これらのアプライアンスをポイントし、時間同期を維持します。

アプリケーション サーバの POS

NCR

NCR が POS クライアント ワークステーションとサーバを提供しました。1 台のサーバに NCR Advanced Checkout Solution (NCR-ACS) がロードされ、他のサーバには NCR Advanced Store Workbench (ASW) ソフトウェアがロードされました。クライアントは、XP バージョン 2 が組み込まれた Windows を稼働する NCR RealPOS80c システムです。NCR-ACS アプリケーションは、主に、大量の商品を扱う小売業者によって使用されています。

Advanced Checkout Solution (NCR-ACS)

NCR-ACS プラットフォームは、複数のモジュールと、Transaction Management Service (TMS) や Cooperative Service を含む各種サービスから構成されています。これらのソフトウェア コンポーネントと業界標準のオペレーティングシステムとの組み合わせが、小売業のトランザクションに必要な追加の機能とセキュリティを提供します。POS サーバが、POS 端末とサーバ、および TMS サービスを装備した ASW クライアント間のデータを制御します。[図 4-11](#) を参照してください。

NCR-ACS の TMS レイヤは、NCR-ACS アーキテクチャの重要なコンポーネントです。これらのサービスは、サーバおよびワークステーション コンポーネントから構成され、データ ファイルと周辺装置への直接アクセスを提供することで、店舗の販売およびオフィスアプリケーションをサポートします。また、TSM は、冗長性、通信、エラー状態への対処、および復旧といった店舗向け POS システムの複雑さの管理も支援します。NCR-ACS TMS は、基礎となるクライアント/サーバオペレーティングシステム、LAN、および WAN と統合されています。

すべてのトランザクションは、NCR-ACS Transaction Log (TLOG) に書き込まれます。POS アプリケーションがトランザクションを TLOG ファイルに書き込んだ後、サーバ上の NCR-ACS Asynchronous Update Process (AUP) プログラムがファイルを読み込み、TLOG データを処理して、店舗のアカウントリング ファイルを更新します。また、NCR-ACS には、IXRetail POSLog 形式で出力するオプションもあります。

従属アプリケーション

NCR-ACS アプリケーションは、次のサードパーティ製アプリケーションおよびソフトウェア開発に依存しています。

- Microsoft Visual Studio.Net
- Microsoft の Managed Extensions for C++

データベース ソフトウェア

Microsoft SQL Server リレーショナル データベース システムが、NCR-ACS アプリケーションのデータ ストレージとして使用されています。

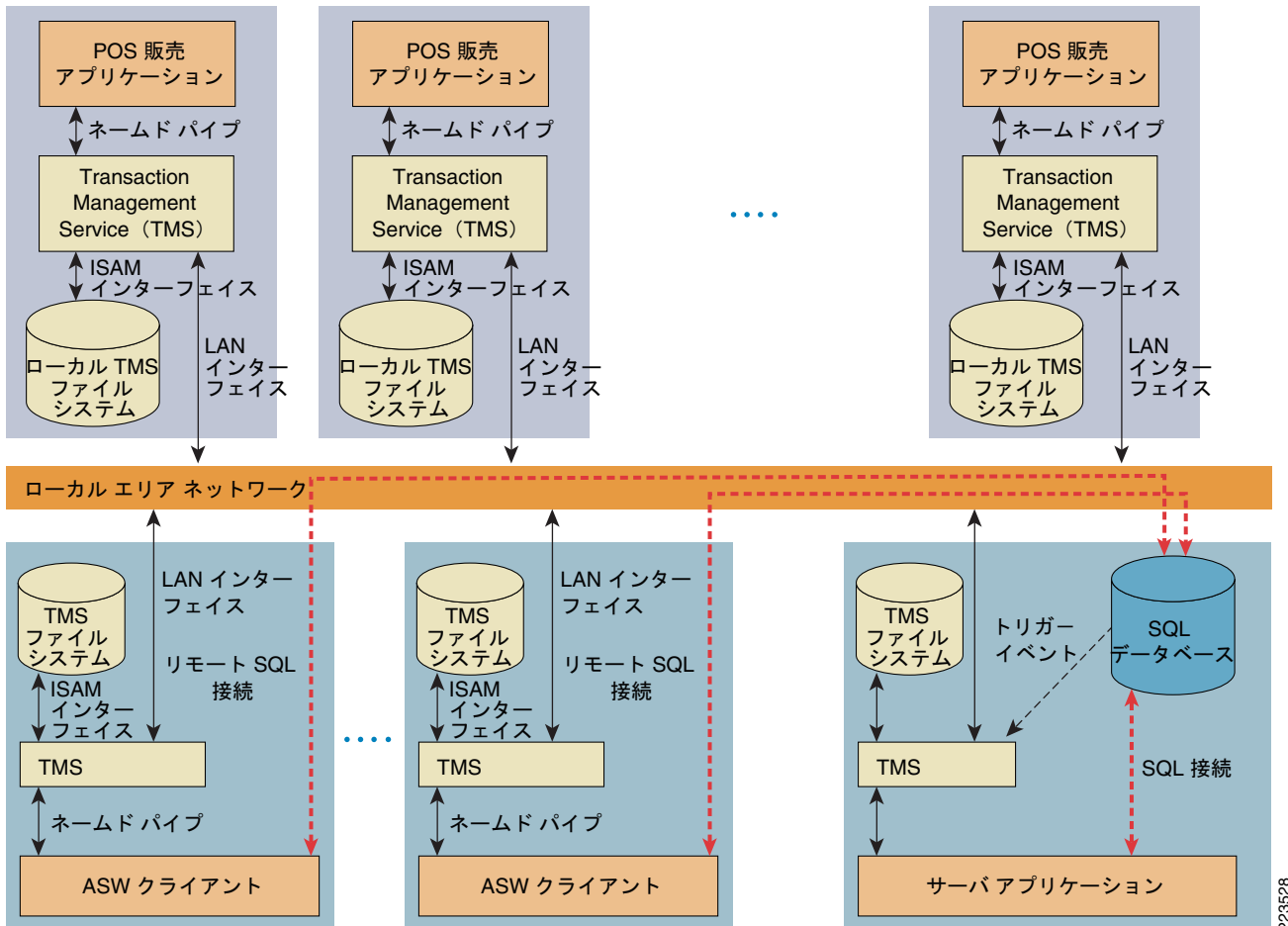
Advanced Store Workbench (ASW)

ASW は、Microsoft Windows オペレーティング システムを実行する PC 上で稼働するグラフィカル ユーザ インターフェイスを提供しますが、店舗のオペレーション担当者に対しては簡素で使いやすい表形式のバックオフィス ユーザ インターフェイスを表示します。表形式のフォームと標準ツールを揃えたフォーム内のツール ボックスが、店舗アプリケーションにアクセスするための使いやすいナビゲーション ツールを提供します。

ASW は、[図 4-11](#) に示す NCR-ACS アーキテクチャのオープンな性質を十分に活用しています。それは、標準の市販の PC、業界標準のイーサネット カードと TCP/IP 通信プロトコル スタックを使用し、それらのコンポーネントをトランザクション管理サービス LAN および ODBC ドライバ インターフェイスと統合しています。

ODBC は、ファイル システムへの SQL に似たインターフェイスをユーザに提供するオープンなデータベース接続用の Microsoft 標準です。この特定の例では、ODBC ドライバは、片側で SQL コマンドを取り、それらを Advanced Checkout Solution ファイル システム用のファイル システム コマンドに変換します。その後、この情報は、適切な Microsoft Office アプリケーションを使用して ASW に渡され、有意義な方法でデータが表示されます。

図 4-11 NCR ACS シングル サーバ アーキテクチャ



TMS は、クライアントとサーバ間のファイルおよび LAN 専用のプライマリ インターフェイスです。POS クライアントは SQL Server にはアクセスしません。データベース アプリケーションは ASW クライアントとサーバに常駐し、1 つの店舗データベースにアクセスします。データベースが変更されると、SQL サーバは TMS への通知をトリガーします。

Mobile Retail Manager (MRM)

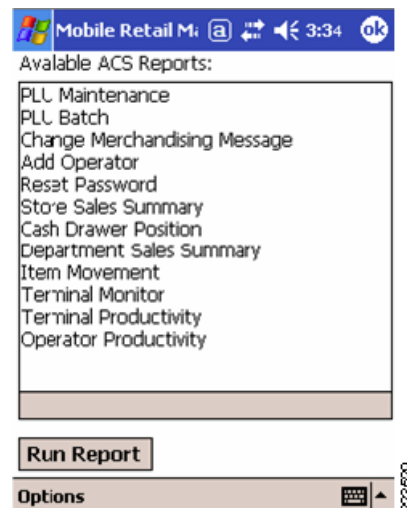
MRM は、ハンドヘルド デバイスで稼働するアプリケーションです。Windows Customer Edge (CE; カスタマー エッジ) デバイスをサポートするデバイスは、これらのアプリケーションをサポートして、店舗の在庫管理を実行できます。ラボでは、MRM は、店舗の在庫リストをチェックするために、Windows Mobile バージョン 5.0 を実行する Intermec CN3 ワイヤレス ハンドヘルドにインストールされました。MRM では、10 種類の基本機能がサポートされています。

- 店舗の販売要約レポート
- リセットパスワード

- PLU メンテナンス
- 品目移動レポート
- 部門要約レポート
- マーチャンダイジング メッセージの変更
- 現金引き出し機の配置レポート
- オペレータの追加
- 端末の生産性
- オペレータの生産性

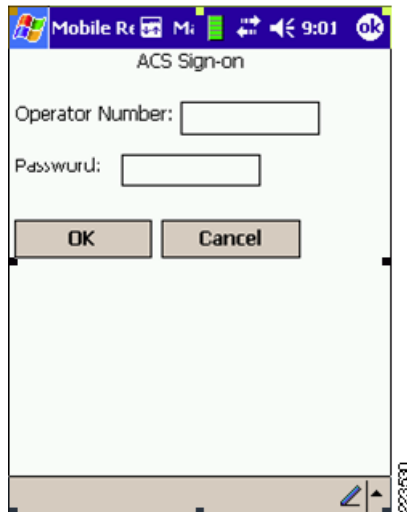
MRM は、Window Mobile バージョン 5.0 を実行する Intermec CN3 デバイスの Start メニューから実行できます。プログラムにより、使用可能なレポートのリストが表示されます。レポートを実行するには、メインリストでレポートの名前を選択し、その後、**Run Report** ボタンを選択します。図 4-12 を参照してください。

図 4-12 MRM



Run Report ボタンを選択すると、NCR-ACS サインオン画面が表示されます（図 4-13 を参照）。

図 4-13 MRM サインオン画面



MRM の主な目的は、監督者や管理者が、レポートを見たり、他の店舗関連の機能を実行したりするためにわざわざ移動するの必要をなくし、フロアに常駐できるようにすることです。MRM を使用すると、デバイス上でレポートを確認し、フロアに居ながら、顧客とやり取りし、店舗の問題を解決できます。

NCR HOME/HOUSE パッケージ

HOME/HOUSE パッケージは、NCR-ACS によって作成され維持されている各種ファイルにアクセスし作業するために必要です。対象となるファイルは、NCR-ACS によって作成され維持されている詳細なトランザクションファイルである **Transaction Detail Log (TLOG)** です。このファイルは、通常、ヘッダー、リーダー、およびその他の特殊制御レコードを持つバイナリタイプの形式で保持され、その中に含まれるセグメントとデータ要素を定義するために使用します。

HOME/HOUSE パッケージを使用して、このバイナリ ファイルを ASCII タイプのファイルに変換できます。選択可能なオプションとして、区切り文字、終了文字、およびヘッダー レコードとトレーラ レコードの一方または両方が必要かどうかを定義できます。このアクティビティは、日中に一定の回数実行し、データを「小分け」にしてホストに送信するように指定することもできれば、**End-of-Day (EoD)** 処理中にトリガーすることもできます。EoD プロセスとしてトリガーされた場合は、1 日のトランザクションの単一のファイルが作成されます。

HOME/HOUSE パッケージは、通常、Windows かあるバージョンの UNIX のどちらかが実行されているホスト レベルのボックス（主にデータセンター内）で実行されます。データ ファイルをホスト レベルへ送信する方式は、ユーザが決定します。通常は、ホスト マシンへの FTP ファイルとして送信されます。このプロセスは、店舗レベルとホスト レベルの両方で自動化できます。*HOME/HOUSE* パッケージは、データベース エンジンが処理可能なデータ ファイルを作成するように指定できます。

シスコのラボ環境における、NCR-ACS Server、ASW クライアント、および RealPOS 80c システムは、シスコに出荷される前に、NCR によって適切なソフトウェアを使用して事前設定されています。サーバとクライアントは、データセンター内の Windows DHCP サーバから受信した DHCP IP アドレスに設定されました。NCR-ACS サーバにインストールされた HOME スクリプトは、ASW クライアントソフトウェアを使用して店舗のクロージング処理時に実行されます。スクリプトは、**ACS\server\data** ディレクトリにあるバイナリ TLOG ファイルを ASCII 形式に変換します。この ASCII ファイルは、**C:\acs\Server\Data\host\dc\070913** ディレクトリに格納されます。最新のディレクトリには、その日の日付が付けられます（この場合は、2007 年 9 月 13 日）。ASW クライアントを使用して店舗のクロージング処理が開始されるとすぐに、「070913」ディレクトリが作成されます。店舗のクロージング処理が EoD 処理としてトリガーされた場合、**070913** ディレクトリには単一のファイル（たとえば、**dc.xxx**）が作成されます。

HOUSE スクリプトは、シスコのラボ環境では使用しませんでした。TLOG ASCII ファイルは、セキュアな Cisco IPSEC Virtual Private Network (VPN; バーチャルプライベートネットワーク) を介して、店舗の ACS サーバから EMC ストレージ環境へ、安全に手動で FTP 転送されました。

シスコのラボ環境では、NCR-ACS アプリケーションバイナリ ファイルを使用するためのアクセスおよび NCR アプリケーション ログ ファイルへのアクセスの監視とログへの記録、NCR RealPOS80c システムの保護、および ASW サーバの保護を実行するために、CSA を使用しました。NCR-ACS Server、NCR ASW サーバ、および RealPOS 80c システムにアンチウイルスもロードしました。

NCR RealPOS 80c POS ワークステーションの詳細については、次の URL を参照してください。

http://www.ncr.com/products_and_services/point_of_sale/pos_workstations/ncr_realpos_80c_.jsp?lang=EN

NCR Advanced Checkout Solution (CS-ACS) の詳細については、次の URL を参照してください。

http://www.ncr.com/products_and_services/point_of_sale/software/food/advanced_checkout_solution.jsp?lang=EN

MS-RMS

Microsoft Retail Management Solution (MS-RMS) は、無償の試用版がダウンロードされ、アーキテクチャ内のモデム POS システムをテストするために実装されました。これは、データセンターサイトに集中的にインストールされた Backstore データベースとともに、非標準的な方法で配置されました。ハンドヘルドと POS レジスタは、SQL ポート TCP 1433 を使用してデータベースに逆接続されました。何かの理由で、WAN 接続が使用できなくなった場合には、システムはローカル データベースを使用してトランザクションを格納しました。Microsoft には、このような分散アーキテクチャの管理を目的とした System Headquarters と呼ばれる追加製品を用意していますが、シスコのラボでは使用できませんでした。

MS-RMS POS アプリケーションを、IBM によって提供された 2 台のレジスタと、データセンター内の General MCS 7825 サーバにインストールしました。レジスタには、CSA クライアントとアンチウイルス ソフトウェアも設定しました。

モバイル ハンドヘルドには、MobiSuite 4 がインストールされました。このアプリケーションは、MS-RMS への接続をサポートし、ラインバスター POS トランザクションと、Intermec デバイスを使用した在庫管理を実行できます。

監査時には支払いシステムが使用できなかったため、MS-RMS システムと IBM レジスタは QSA による PCI 監査には含まれませんでした。

MS-RMS のインストールは付属のマニュアルに従い非常に簡単に実行できました。マニュアルは、次の URL から入手可能です。

<http://www.microsoft.com/businesssolutions/retailmanagementsystem/default.mspx>

Wincor-Nixdorf

Wincor-Nixdorf は、TP.Net POS 製品と 3 台の Beetle レジスタを提供しました。バックストア SQL データベースとともに、ロケーション (小規模、中規模、大規模) ごとに 1 台ずつレジスタが設置され、各店舗の MCS 7825 サーバにトランザクションサーバがインストールされました。これは、店舗あたり 50 台の端末をサポートできる推奨されるクライアント/サーバタイプ 2 アーキテクチャ インストールを表しています。他の構成では、店舗あたり最大 200 台の端末をサポートできます。

TP.net POS アプリケーションは、カード支払いシステム向けの Wincor-Nixdorf 標準インターフェイスである標準ベースの Open Payment Initiative (OPI) インターフェイスを通じて、支払いアプリケーションとやり取りします。インターフェイスは、販売システムとカード支払いシステム間の TCP/IP 通信に基づいています。プロトコルは、XML ベースです。TCP/IP 通信は、一般に社内ネットワーク内で行われ、ほとんどはローカル ホストを介して単一の販売システム上で発生しま

す。プロトコルデータは、関与するシステム（販売システム、カード支払いシステム）がログイン目的でデータを格納する以外は、どのシステムにも格納されません。ログインは、実稼働環境では無効にする必要があります。

O.P.I. はカード所有者情報を格納しません。O.P.I. インターフェイスは、TP.net 販売システムとカード支払いシステム間でカード所有者情報を交換する役割を担っています。カード所有者情報のストレージは、販売システムとカード支払いシステムの役割となります。TP.net では、カード所有者情報のストレージを最小限にするため、トランザクションデータの保存時間を設定できません。

監査時には支払いシステムが使用できなかったため、Wincor-Nixdorf システムとレジスタは QSA による PCI 監査には含みませんでした。

詳細については、次を参照してください。

- <http://www.wincor-nixdorf.com/internet/com/Products/Software/Retail/StoreSolutions/TPnet/Main,templateId=blog.jsp,property=DetailPaper.pdf>

Microsoft Windows Server

各 Microsoft Windows Server は、公開済みのベストプラクティス（<http://www.CISecurity.com> を参照）を使用して強化されました。サーバの強化に関する小売業者のニーズはかなり異なるため、QSA による管理プラットフォームのこの側面の直接的な監査は行いませんでした。

次には、サーバの構築/強化に使用された手順を示します。

- OS イメージングソフトウェアとファイルを使用するイメージサーバハードウェア
- サーバの名前の変更と SID の変更
- ローカルアカウントの管理者パスワードの変更
- サーバのドメインへの加入
- すべての重要なアップデートとセキュリティアップデートのダウンロードとインストール
- アンチウイルスクライアントのインストールと AV 定義のアップデート
- CSA クライアントのインストールと CSA マネージャへの登録の確認
- RDP を強力な暗号化に設定（グループポリシーの確認）
- サーバ用の適切なアプリケーションのインストール
- Microsoft Security 設定ウィザードを使用した、すべての未使用サービスの無効化と、Windows ファイアウォールの厳密化
- MBSA ツールの実行、サーバの追加項目の修正
- 15 分間の非アクティビティ状態の後、デスクトップをログアウト/ロックするためのデスクトップポリシーの確認

PCI 要件として、サーバは現在の業界のベストプラクティス標準に従って強化する必要があります。NIS、SANS、CISecurity、および ARF は、サーバ強化に関連して現在のガイドで取り上げられているリソースです。

Microsoft の Active Directory アカウントディレクトリは、ユーザ認証とパスワードに関するいくつかの重要なメカニズムの設定をサポートしており、細かい設定なしで PCI 要件に準拠できるようになっています。AD のパスワードポリシーは、ドメインセキュリティ設定ポリシー内で定義されます。これらは、Microsoft Windows Server 2003 R2 のクリーンインストールのデフォルト設定でした。これらのデフォルト設定は PCI 要件を上回っていますが、どのインストールでも確認する必要があります。図 4-14 に、パスワードポリシー画面を示します。

図 4-14 パスワード ポリシー

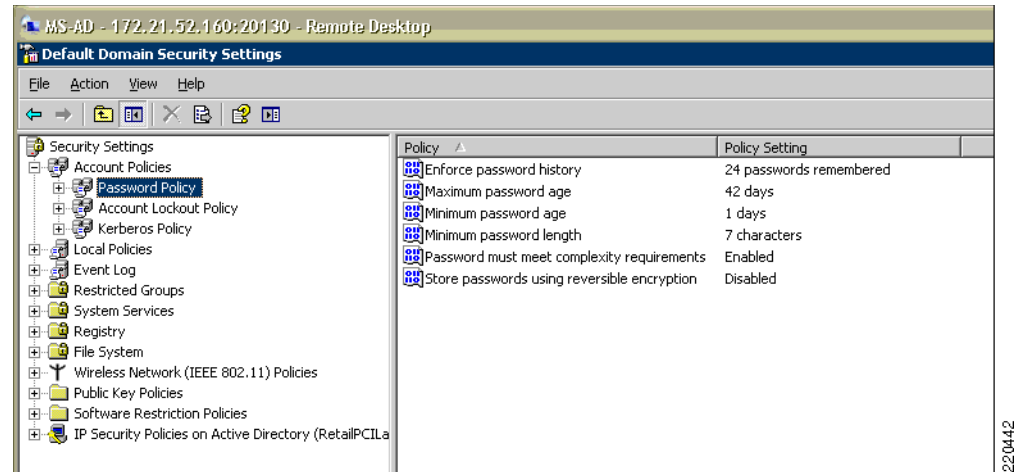
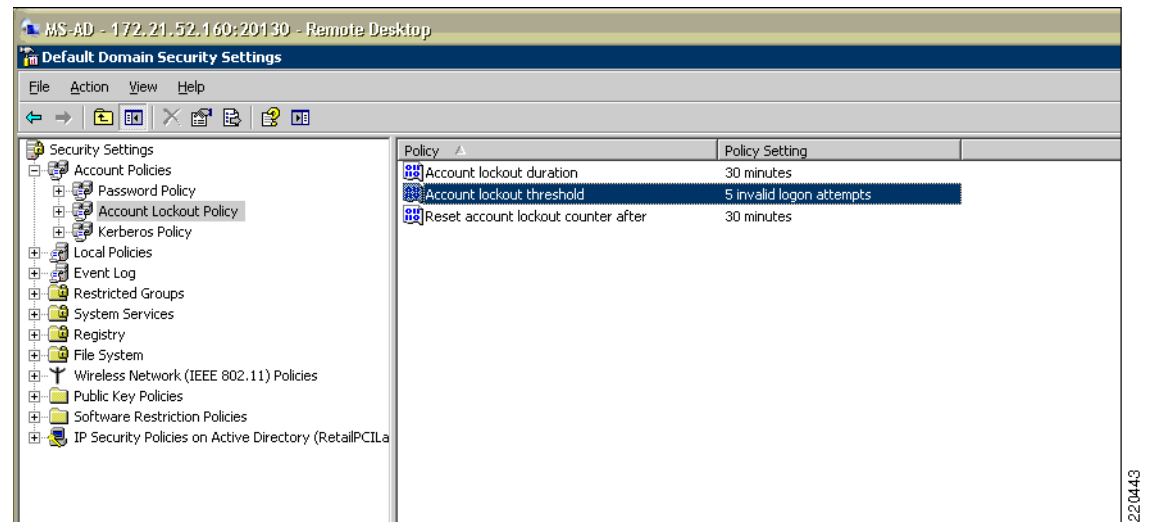


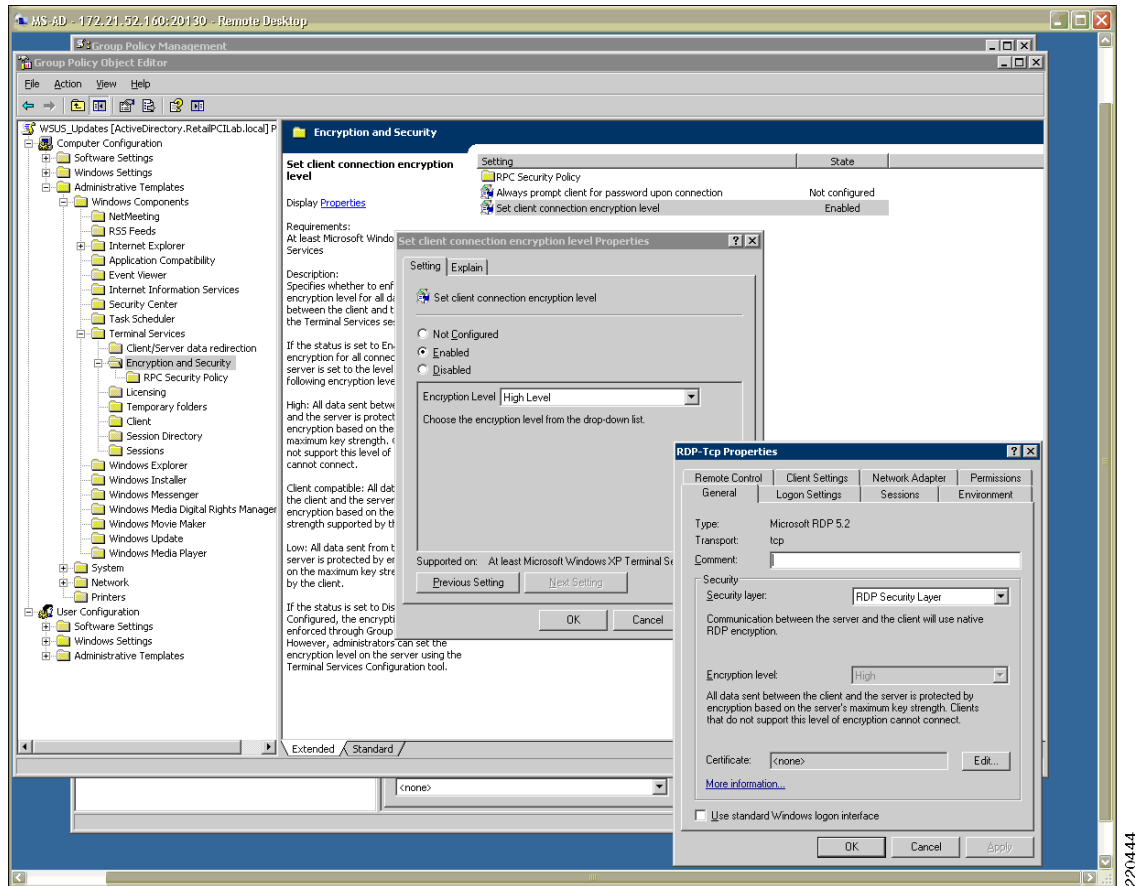
図 4-15 に、アカウント ロックアウト ポリシー画面を示します。

図 4-15 アカウント ロックアウト ポリシー



Microsoft Windows Server のリモート サーバ管理で使用する Remote Desktop Protocol は、さまざまなレベルのセキュリティをサポートしています。PCI 要件を満たすために、すべてのデバイスでこの設定値を「High Encryption（強度な暗号化）」に設定する必要があります。これを行うため、図 4-16 に示すように、ドメイン グループ セキュリティ ポリシーを変更しました。

図 4-16 ドメイン グループ セキュリティ ポリシー



15 分間のセッション タイムアウトの要件を適用するためにこのドメイン グループ ポリシーも編集しました。このため、すべてのサーバとワークステーションのデスクトップをパスワード保護されたスクリーン セーバーで 15 分後にロックしました。

支払いデバイス

Mx シリーズ

VeriFone MX870 および MX850 をラボ内の支払いデバイスとして使用し、NCR RealPOS80c システムに接続しました。MX800 シリーズは、最新の支払いセキュリティ標準に準拠する一方、スマート カードと磁気ストライプを使用した支払いをサポートします。

Mx870 シリーズおよび Mx850 シリーズのどちらの PIN パッドも、PIN 入力（オンラインとオフライン）と EMV（European Visa/MasterCard）レベル 1 および 2 に対して認定された Payment Card Industry PIN Entry Device（PCI PED）です。

VeriFone MX シリーズの詳細については、次の URL を参照してください。

<http://www.verifone.com/products/devices/mx/index.html>

Vx シリーズ

ラボでは、ワイヤレス Vx 670 PIN パッドが使用され、Cisco Unified Wireless インフラストラクチャに接続されました。Vx670 PIN パッドは、PCI PED として認定されています。テスト時には、Vx670 は Wi-Fi Protected Access (WPA) だけをサポートしていました。WPA2 はサポートしていませんでした。



(注)

テストするには支払い処理ゲートウェイが必要だったため、Vx670 のスコープには支払い処理は含まれていませんでした。スコープは Vx670 のテストに限定され、(WPA を使用して) 安全に Cisco Unified Wireless インフラストラクチャに接続できました。

Verifone Vx 670 の詳細については、次の URL を参照してください。

<http://www.verifone.com/products/devices/vx/vx670.html>

暗号化とキー管理

ペイメント カード情報の効果的で持続的なセキュリティを実現するには、IT スタックの各レイヤの安全性を確保する暗号化制御機能が必要です。次のセクションでは、RSA Key Manager と RSA File Security Manager の 2 つの RSA 暗号化およびキー管理製品について説明します。これらは、Cisco PCI Solution for Retail のラボにおける検証プロセスで使用されました。

RSA Key Manager

図 4-17 に、RSA キー管理の構成を示します。RSA Key Manager は、企業全体の中央集中型暗号化管理を提供し、さまざまな暗号化使用ポイントにポリシーを適用できます。また、暗号キーとその他のセキュリティ オブジェクトの中央集中型のプロビジョニングおよびライフサイクル管理を提供し、暗号化制御の構成と継続した管理の複雑さを低減します。

特に大規模な接続および分散された企業におけるキー管理は、適切に実行するのが困難です。キーは、慎重に生成し、その後、完全性が保証された状態で複数のクライアントアプリケーションに安全に転送する必要があります。クリティカルなキーの損失は、それが保護するクリティカルなデータの損失を招くことがあるため、非常に安全で信頼できるストレージメカニズムが必要となります。キー管理システムが停止すると、ビジネスの機能を妨げることがあります。キーのロールオーバー、監査、および廃止などキーに関するセキュリティ ポリシーを適用するためのメカニズムが必要です。また、キー管理システムは、暗号化を実装することで、簡単に使用できなければなりません。

RSA Key Manager は、これらの懸念をすべて解消し、暗号化構成の複雑さを低減できるように設計されています。RSA Key Manager ソフトウェアは、暗号化ベースのデータ保護を実装する企業向けに、ポリシーベースの中央集中型暗号化鍵管理を提供します。

RSA Key Manager は、3 つの主要なコンポーネントから構成されています。

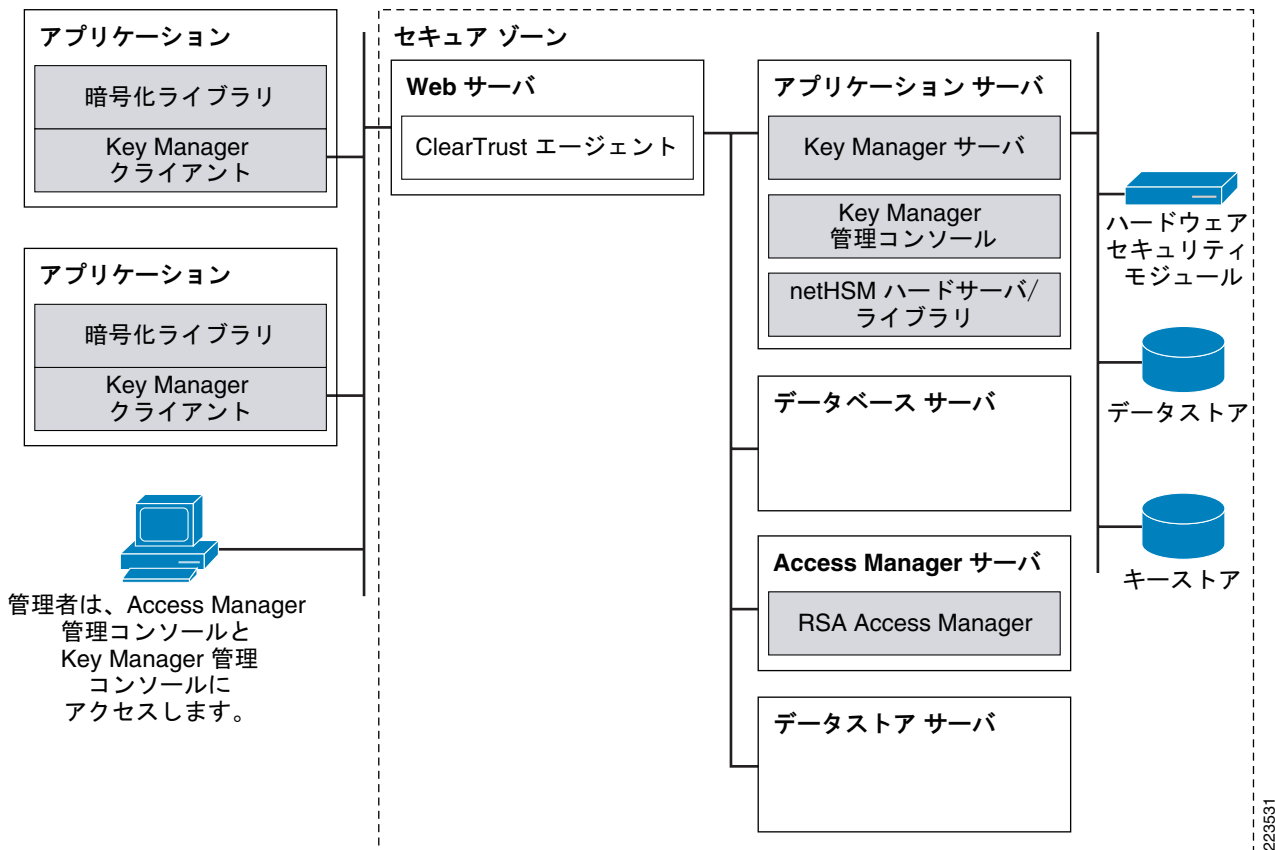
- 組織のビジネス アプリケーション内に分散された RSA Key Manager Client
- 中央集中型 RSA Key Manager Server
- 管理者に RSA Key Manager Server へのアクセスを提供する管理コンソール

Key Manager の構成により提供される基本サービスは、次のとおりです。

- キー管理
 - キー生成 — キーは、オプションで、期限切れになると自動的に生成され、期限切れのキーの動作も自動的に継続されます。
 - キー ストレージ — キーは、標準のデータベース技術を使用して中央に格納されます。

- キー取得 — クライアント / サーバ機能を使用して、迅速、簡単、かつ安全にキーを取得します。
- キーポリシー定義 — キー プロパティは、企業データに適合されます。
- 分類ポリシー :
 - キーの有効期限 — キーは、ポリシーに基づいて自動的に期限切れになります。
- アプリケーションの暗号化サービス :
 - Key Manager Client の強力な認証。暗号鍵アクセスには、Public Key Infrastructure (PKI; 公開鍵インフラストラクチャ) ベースの認証が必要です。
 - Key Manager Client ライブラリは、C アプリケーションのみをサポートします。
- クライアント上の設定可能なキー キャッシングにより提供された連続した動作
 クライアントは、固定的キャッシュおよび非固定的キャッシュで、キーのローカル コピーを保持できるため、ネットワークの停止中もスタンドアロンで動作可能です。

図 4-17 RSA Key Manager Server の構成



構成のコンポーネント

ラボでは、RSA Key Manager を正常に動作させるために、次のコンポーネントが配置されました。

Web サーバ

Web サーバは、HTTPS を介して Key Manager Client と管理者からの要求を受け取り、それらをアプリケーションサーバに転送します。Web サーバは、ユーザ認証、ユーザ許可、およびファイアウォールによってすべてのアクセスの安全性が確保されるセキュアゾーンへのエントリポイントです。この環境では、Microsoft Internet Information Services (IIS) 6.0 が使用されます。

アプリケーションサーバ

アプリケーションサーバは、Web サーバからの要求を受け取り、Key Manager Server または Key Manager 管理コンソール機能を起動します。この環境では、Apache Tomcat (5.5.20) が使用されます。

データベースサーバ

データベースサーバは、RSA Key Manager サーバデータベースを格納します。この環境では、Microsoft SQL Server 2005 が使用されます。

RSA Access Manager Server

RSA Access Manager Server はアクセス管理ソフトウェアを稼働し、Key Manager Server 構成の認証および許可サービスを実行します（「[RSA Access Manager](#)」 [p.4-38] を参照）。

シスコのラボ環境では、このソリューションの基準を提供するために、RSA とシスコが共同で、稼働中のソリューションを実証する環境を構築しました。RSA Key Manager からのキーは、RSA Key Manager Client (サンプルプログラム) Application Programming Interface (API; アプリケーションプログラミングインターフェイス) を使用する Windows XP が稼働された PC 上でコマンドラインユーティリティを使用して生成されます。これは、有効なコンセプト実証手段です。ただし、実際のユースケースでは、この API を利用する顧客またはサードパーティパートナーの製品に依存して、クライアントコードを直接 POS ソフトウェアに組み込みます。したがって、完全にサポートされた真に再現可能なソリューションを作成できます。

図 4-18 RKM Client を利用する一般的なアプリケーション

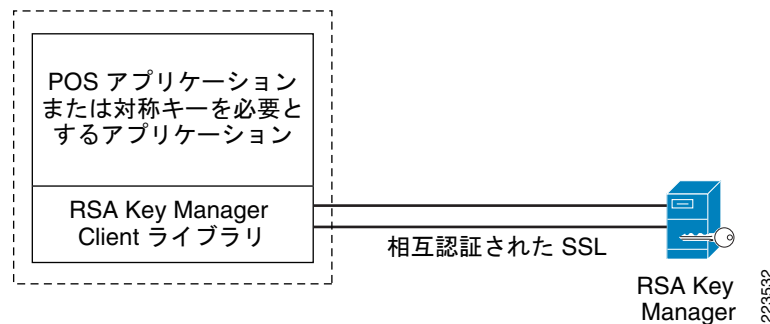


表 4-1 RSA Key Manager の機能

RSA Key Manager Server	RSA Key Manager Client
キーの安全な取得と Key Manager Client へのプロビジョニング	操作可能なユーザ用の API のプロビジョニング
安全な中央集中型の暗号鍵ストレージ	暗号化、復号化、MAC、および MAC 検証操作を実行するための暗号鍵の取得

表 4-1 RSA Key Manager の機能（続き）

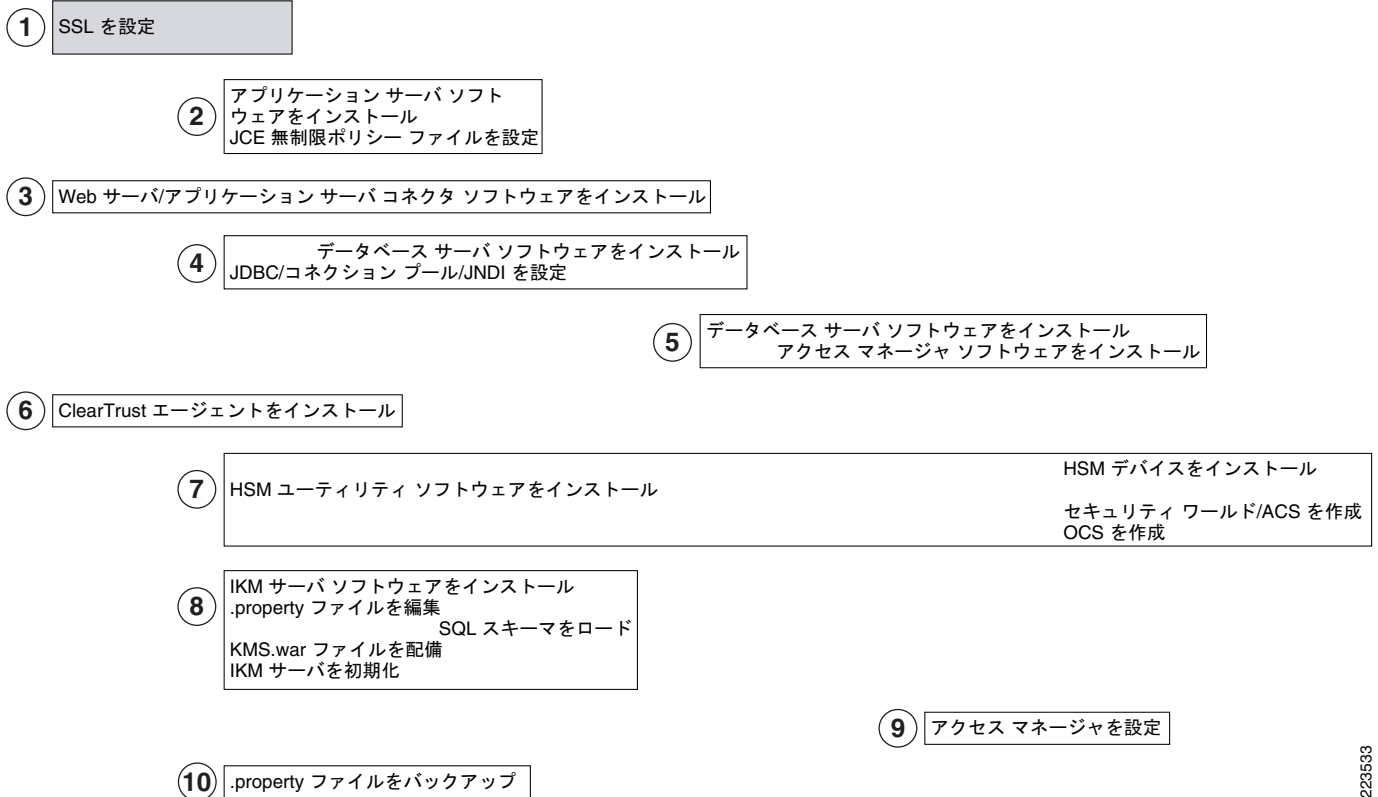
強力な暗号鍵の生成	暗号鍵を Key Manager Server に格納する機能
暗号鍵ライフサイクルの管理	設定可能な暗号鍵のローカル キャッシング。Key Manager Server への接続が失われた場合も暗号化操作を続行できます。
中央集中型のキー、キー ポリシー、およびキー ユーザの管理	キーのライフサイクルを手動で維持する機能
キー ユーザのアプリケーション レベルでの認証および許可	キーおよびキー ポリシー情報の取得とアップデート機能
キーの集合または個々のキーに関連付けられた外部データのストレージ	Key Manager Server 管理機能へのアクセスを管理ユーザに制限
すべてのキー管理操作のロギング	すべてのキー操作の設定可能なロギング

設定

このガイドでは、サーバをインストールするための各手順については説明していませんが、代わりに設定済みのラボ環境の概要と構成のベスト プラクティスについて説明しています。詳細なインストール手順については、RSA Key Manager 製品のマニュアルを参照するか、経験豊富なサポート センターである RSA Professional Services (<http://rsa.com/node.aspx?id=1310>) にお問い合わせください。

図 4-19 Key Manager Server 構成のインストール プロセスの概要

Web サーバ アプリケーション サーバ データベース サーバ データストア サーバ アクセス マネージャ HSM



(注) このラボ環境では、ソリューションの検証に Hardware Security Module (HSM) を使用しませんでした。

Web サーバのインストール

IIS Web サーバには、SSL セッションを介した通信が必要です。Web サーバに提示される RKM クライアント証明書は、Web サーバ上の SSL 証明書と同じ発行元から発行されているか、IIS 証明書信頼リストを介して IIS Web サーバによって信頼されている必要があります。この SSL および証明書信頼リストの設定の詳細については、Microsoft IIS のマニュアルを参照してください。

Tomcat アプリケーション サーバおよび Jakarta コネクタのインストール

Apache Tomcat は、RKM Server 用のエンジンとして使用され、KM S. WAR ファイルを <Tomcat のインストール フォルダ>\webapps ディレクトリにコピーするか、または Tomcat Web Application Manager を使用して配置されます。

Jakarta コネクタがインストールされ設定された後、SSL Web 要求（通常、ポート 443）がアプリケーション サーバに確実に転送されることを確認しておくことを推奨します。たとえば、次の手順を実行します。

1. Tomcat のインストール フォルダ >\webapps\test\test.html を作成します。
2. その後、<Tomcat のインストール フォルダ>\conf\workers2.properties ファイルに、URL /test/* と入力します。

3. <https://localhost/test/test.html> がヒットすると、要求が転送され、そのページが表示されます。上記の手順は、インストールガイドに記載されていますが、通常は見落とされています。要求をアプリケーション サーバに転送できない場合は、インストールを続行しないでください。

もう1つの一般的なプラクティスは、特にコンポーネントが異なるホストに常駐する場合に、Web サーバとアプリケーションサーバ間の接続を確保することです。このためには、Tomcat を通じて Tomcat アプリケーションサーバの証明書を作成またはインポートします。

詳細な手順については、次の URL を参照してください。

<http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>

データベースのインストールおよび SQL ODBC コネクタ

これらのインストールアイテムの独自のインストール手順は非常に明確で、それらに正確に従う必要があります。SQL サーバにあるキーストアにアクセスできない場合、Web アプリケーションは稼働できません。



(注)

ラボ環境では、ソリューションはネイティブの PKI インフラストラクチャは使用しておらず、代わりに RSA Key Manager クライアント証明書、Web サーバ SSL 証明書、およびアプリケーションサーバ証明書を RSA の PKI インフラストラクチャを使用して作成し、証明書を手動で RSA Key Manager Client および Server にインポートしました。

CSA を使用して、RSA Key Manager のアプリケーション バイナリ ファイルを使用するためのアクセスと RSA Key Manager のログ ファイルへのアクセスが監視されログに記録されました。

RSA Access Manager

RSA Access Manager (旧名は RSA ClearTrust) の Web アクセス管理ソリューションを使用することで、組織は、イントラネット、エクストラネット、ポータル、およびエクステンジインフラストラクチャ内で、Web アプリケーションへの安全なアクセスをコスト効率良く提供できます。[図 4-20](#) を参照してください。

RSA Access Manager ソフトウェアは、組織が多数のユーザを管理する一方、適合性を保証し、企業リソースを不正アクセスから保護し、正規のユーザのジョブの実行をより簡単にする中央集中型のセキュリティ ポリシーを適用できるようにすることを目的に設計されています。

図 4-20 RSA Key Management Server Web インターフェイスを保護する RSA Access Manager

rchakkin: Default Administrative Group/Default Administrative Role

Help Options Log Out

Home Define Resources Authorize Access Manage Users Delegate Administration

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:

Add New Resources in Application: **KMS Webserver** Display records per page

Showing 1-2. <Back | Next>

Actions	Resource	Type	Server	Description	Delete
Actions...	KMS Webserver	Application			☐
Actions...	/kms/*	URL	KMS Webserver		☐

Showing 1-2. <Back | Next>

Done

How To... Hide

- Understand Applications
- Understand Resources

223534

RSA File Security Manager

RSA File Security Manager は、異種のプラットフォーム上でファイルやフォルダの透過的な暗号化とともに role-based access control (RBAC; ロールベース アクセス コントロール) を提供するソフトウェアベースのセキュリティ ソリューションです。

RSA File Security Manager では、ユーザがアプリケーションを修正する必要はなく、専用のハードウェアも必要ありません。ファイルやフォルダに対するロールベース アクセス コントロールを中央集中型で管理し、システムとセキュリティ管理の役割の分離を実現できます。セキュアなフォルダ内のすべてのアクティビティは、監査を目的として安全にログに記録されます。

ラボ環境では、RSA File Security Manager アダプタ ソフトウェアが NCR POS サーバにインストールされ (NCR-ACS POS システムはトランザクション ログを暗号化しない)、もう 1 つのコピーが SAN ベースのストレージに接続されたデータセンター内のサーバにインストールされました。これは、推奨アーキテクチャを表しています。店舗サーバでは、RSA File Security Manager は、POS レジスタによって生成されたトランザクション ログを含むフォルダの安全性を確保します。トランザクション ログ フォルダへのアクセスは、許可されたユーザとフィンガープリント付きのローカル アプリケーションのみに制限されます。セキュアなフォルダにアクセス可能な許可されたアプリケーションは、POS アプリケーションと SFTP クライアントです。SFTP クライアントは、トランザクション ログをデータセンター内のサーバに安全に転送します。管理者とその他のスーパーユーザは、File Security Manager セキュリティ オフィサによってアクセス権が付与されない限り、トランザクション ログ フォルダにはアクセスできません。

その他のラボ アクティビティとして、データセンター内のストレージ ドライブにマッピングされたサーバ上でのトランザクション ログの集約があります。ストレージ レイヤ。サーバは、各店舗サーバからのトランザクション ログ ファイルを集約し、調整するために、それらをローカルに格納します。RSA File Security Manager は、データセンター内のこのサーバにもインストールされます。RSA File Security Manager アダプタ ソフトウェアの CSA ソフトウェアが、不測のアクセスと悪質なアクセスの両方からサーバ リポジトリを保護します。File Security Manager セキュリティ オフィサによって許可されたサーバの実行可能で特定のユーザとアプリケーションだけに、フォルダ内のデータへのプレーンテキスト アクセスが設定されます。デフォルトでは、File Security Manager はすべてのファイル/フォルダ アクセスを最小限の権限モデルまで削減します。

RSA File Security Manager の詳細については、次の URL を参照してください。

<http://www.rsa.com/node.aspx?id=3228>

リモート アクセス

RSA Authentication Manager/RSA SecurID および RSA enVision

RSA SecurID® ソリューションには、次の機能が含まれます。

- RSA Authentication Manager — 管理、ユーザ認証、パスワード統合、および監査に使用します。
- RSA Authentication Agent — ローカルのコンピュータとサーバにインストールします。

RSA Authentication Manager ソフトウェアと RSA Authentication Agent 6.1 を使用することで、RSA SecurID は 2 ファクタ ユーザ認証の実行が可能になります。RSA SecurID 2 ファクタ認証は、知っているもの（パスワードまたは PIN）と持っているもの（RSA SecurID オーセンティケータ）に基づき、非常に信頼性の高いユーザ認証を提供します。

RSA SecurID テクノロジーによって保護されたシステムでは、RSA Authentication Agent がユーザにログイン名とパスコードの入力を求めます。このパスコードは、60 秒ごとに変更される 6 桁のワンタイム RSA SecurID トークンコードと、一意の Personal Identification Number (PIN; 個人識別番号) の組み合わせです。その後、RSA Authentication Agent は、RSA Authentication Manager に認証サービスを要求し、RSA Authentication Manager の応答に基づいて、保護されたシステムへのログオンを有効にするか、または無効にします。

ラボ環境では、主に、従業員やサードパーティによるネットワークへのリモートアクセスについて PCI DSS ドキュメントに規定された 2 ファクタ認証の要件を満たすために、RSA SecurID テクノロジーと RSA Authentication Manager ソフトウェアを使用しました。RSA Authentication agent 6.1 が、Cisco Secure Access Control Server (CS-ACS) にインストールされました。CS-ACS と RSA Authentication Manager/RSA SecurID との間の通信を容易にするために、RSA Authentication Manager データベースに Agent Host レコードを追加する必要があります。Agent Host レコードは、データベース内の CS-ACS を識別し、通信と暗号化に関する情報を保持しています。Cisco Secure CS-ACS と RSA Authentication Manager との間の通信では、ネイティブ RSA SecurID 認証プロトコルを使用します。

リモートユーザは、安全な接続を確保するために、Cisco VPN クライアントを使用してエンドツーエンドの暗号化された VPN トンネルを確立します。セキュア VPN 接続は、Cisco Adaptive Security Appliance (ASA) ファイアウォールで終端されます。リモートユーザは、Cisco VPN を使用してネットワークに接続すると、ユーザ名とパスコード（RSA SecurID トークンコードとユーザ PIN の組み合わせ）の入力が求められます。この情報は CS-ACS に送信され、その後、ユーザ認証の確認のために RSA Authentication Manager に転送されます。

RSA Authentication Manager 監査ログを監視するため、ラボでは、事前に設定された RSA enVision アプライアンスが使用されました。監査ロギング情報を RSA Authentication Manager から安全に収集するために、「NICsftpagent」が RSA Authentication Manager にインストールされました。監査ログは、レポート、アラート、および長期の保管のために、60 分ごとに FTP を使用して安全に RSA enVision に転送されました。ログは、RSA enVision の専用データベースに格納されます。

詳細については、次を参照してください。

- RSA SecurID の設定
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>

設定のトラブルシューティング

よくある間違いには、次のようなものがあります。

- スイッチの初期構成時に、提供された IOS コードがセキュア HTTP または SSH 管理をサポートしていませんでした。IOS のアップグレード後も、引き続き安全でないプロトコルを無効にする必要があります。無効にするには、**no ip http-server**、**ip http secure-server**、および VTY インターフェイスの場合は **transport input SSH** を使用します。
- CS-M を使用している場合は、ルータ内のアクセス リストをルータ内でローカルに修正しないでください。これは、CS-M を介してアクセス リストのアップデートが再配置されたときに問題を招くことがあります。
- 各インターフェイスでコマンド **ip verify unicast source reachable-via rx** を使用すると、ルータのローカル LAN インターフェイスに ping できなくなります。これは、アンチスプーフィングが原因で、この機能が許可されないためです。データセンターまたはローカル クライアントから ping を実行してください。
- RSA Key Manager ソフトウェアのインストール時に、RSA Key Manager インストール ガイドに記載された詳細な部分（正しい Java バージョン ソフトウェア コードなど）を省くと、RSA Key Manager Server または Client の正常な動作に問題が生じることがあります。

推奨されるトラブルシューティングのヒントは次のとおりです。

- ワイヤレス クライアントの認証の実行時に、ワイヤレス コントローラ VLAN 上で（スイッチ スパン ポートを通じて）WildPackets OmniPeek Personal ネットワーク アナライザを使用して、ネットワークへのユーザ ログインの経過を監視したことが非常に役立ちました。
- C-LMS サーバに送信されている Syslog イベントの診断中に、シスコは WildPackets OmniPeek Personal ネットワーク アナライザを使用しました。これにより、ワイヤレス コントローラ デバイス タイプが認識されないために CiscoWorks がそれらをレポートしない場合でも、ワイヤレス コントローラがログを送信中であることを確認できました。OmniPeek Personal アナライザは、次の URL から無償ダウンロードとして入手できます。サポートはオプションで有償です。http://www.omnipeek.com/omnipeek_personal.php
- シスコは、ミディアム ワイヤレス コントローラが定期的に応答を中断することを発見しました。正常な動作に戻すため、exec プロンプトからルータ インターフェイスに ping を実行しました（**wireless-controller1/0, ip address 10.10.46.33**）。

結果とまとめ

このソリューションは、Verizon Business によって実施された QSA 監査に合格しました。ネットワーク設計に追加する必要があるのは、デバイス管理とファイル完全性モニタリングのためのいくつかの補完コントロール機能だけでした。Verizon Business がもっとも有用と認めた製品は、さまざまな管理サーバ上の CSA Manager と CSA クライアント、および包括的なネットワーク アーキテクチャでした。監査の詳細な結果は、付録 F「[Report on Compliance \(ROC\)](#)」に掲載されています。



APPENDIX A

店舗用製品一覧

小規模店舗

製品	説明	数量
CISCO2821	2821、AC 入力電源、ギガビット イーサネット ポート (GE) × 2、高速 WAN インターフェイス カード (HWIC) × 4、パケット音声データ モジュール (PVDM) × 3、Network Module Enhanced Extended (NME-X) × 1、Advanced Integration Module (AIM) × 2、IP Base、64F/256D	1
S28NAISK9-12409T	Cisco 2800 ADVANCED IP SERVICES	1
MEM2821-256U512D	Cisco 2821 対応 256 ~ 512 MB DDR DRAM 工場アップグレード	1
MEM2800-64U128CF	Cisco 2800 シリーズ対応 64 ~ 128 MB CF 工場アップグレード	1
NM-CE-BP-40G-K9	Content Engine ネットワーク モジュール (NM)、基本パフォーマンス、40 GB	1
SF-ACNS-5.3-K9	ACNS ソフトウェア v5.3	1
EVM-HD-8FXS/DID	高密度音声 / ファックス拡張モジュール、FXS/DID × 8	1
EM-HDA-6FXO	6 ポート音声 / ファックス拡張モジュール、FXO	1
PVDM2-32	32 チャネルパケット音声 / ファックス DSP モジュール	1
HWIC-4ESW-POE	4 ポートイーサネット スイッチ HWIC、Power Over Ethernet (PoE) 対応	1
HWIC-4ESW-POE	4 ポートイーサネット スイッチ HWIC、PoE 対応	1
VWIC-2MFT-T1-DI	2 ポート RJ-48 マルチフレックス トランク、T1、ドロップアンドインサート	1
WIC-1ADSL	1 ポート ADSL WAN インターフェイス カード	1
AIM-CUE	Unity Express AIM、価格には 12 個のメールボックスが含まれる	1
SCUE-2.2	Cisco Unity Express 基本リリース	1
SCUE-LIC-25CME	Unity Express ライセンス、25 個の音声メールボックス、自動応答、CCME	1
CUE-LANG-ENG	Cisco Unity Express、イギリス英語版	1

FL-CCME-SMALL	Cisco Call Manager Express 機能ライセンス、最大 24 ユーザ	1
CAB-AC	電源コード、110 V	1
PWR-2821-51-AC-IP	Cisco 2821/51 AC/IP 電源装置	1
AIR-LAP1131AG-A-K9	802.11ag LWAPP AP 統合アンテナ FCC 設定	1
S113RK9W-12307JX	Cisco 1130 シリーズ IOS WIRELESS LAN LWAPP RECOVERY	1

中規模店舗

製品	説明	数量
CISCO3845	3845、AC 入力電源、ギガビットイーサネットポート (GE) × 2、SFP ポート × 1、拡張ネットワーク モジュール (NME) × 4、高速 WAN インターフェイス カード (HWIC) × 4、IP Base、64F/256D	2
S384AISK9-12409T	Cisco 3845 ADVANCED IP SERVICES	2
MEM3800-256U512D	Cisco 3800 対応 256 ~ 512 MB DDR DRAM 工場アップグレード	2
MEM3800-64U128CF	Cisco 3800 シリーズ対応 64 ~ 128 MB CF 工場アップグレード	2
CAB-AC	電源コード、110 V	2
NM-AIR-WLC6-K9	ISR 28/38xx 対応 WLAN コントローラ NM	1
NM-CE-BP-40G-K9	Content Engine ネットワーク モジュール (NM)、基本パフォーマンス、40 GB	1
SF-ACNS-5.3-K9	ACNS ソフトウェア v5.3	1
SWLC6K9-11	WLAN コントローラ NM ソフトウェア イメージ	1
VIC-4FXS/DID	4 ポート FXS または DID VIC	1
VIC2-4FXO	4 ポート音声インターフェイス カード、FXO (ユニバーサル)	1
VWIC-2MFT-T1-DI	2 ポート RJ-48 マルチフレックス トランク、T1、ドロップ アンド インサート	2
WIC-1ADSL	1 ポート ADSL WAN インターフェイス カード	1
PVDM2-32	32 チャンネル パケット音声 / ファックス DSP モジュール	2
AIM-CUE	Unity Express AIM、価格には 12 個のメールボックスが含まれる	1
SCUE-2.3	Cisco Unity Express 基本リリース、2.3	1
SCUE-LIC-50CME	Unity Express ライセンス、50 個の音声メールボックス、自動応答、CCME	1
FL-CCME-MEDIUM	Cisco Call Manager Express 機能ライセンス、最大 48 ユーザ	2
CUE-LANG-ENU	Cisco Unity Express、北米英語版	1
PWR-3825-AC	Cisco 3825 AC 電源装置	2

WS-C3560-48PS-S	Catalyst 3560、10/100 ポート×48 (PoE 対応)、SFP ポート×4、標準イメージ	2
CAB-AC	電源コード、110 V	2
GLC-T=	1000BASE-T SFP	4
CAB-SFP-50CM=	Catalyst 3560 SFP 相互接続ケーブル、50 cm	1
AIR-LAP1131AG-A-K9	802.11ag LWAPP AP 統合アンテナ FCC 設定	1
S113RK9W-12307JX	Cisco 1130 シリーズ IOS WIRELESS LAN LWAPP RECOVERY	1

大規模店舗

製品	説明	数量
CISCO3845	3845、AC 入力電源、ギガビット イーサネット ポート (GE) × 2、SFP ポート×1、拡張ネットワーク モジュール (NME) × 4、高速 WAN インターフェイス カード (HWIC) × 4、IP Base、64F/256D	2
S384AISK9-12409T	Cisco 3845 ADVANCED IP SERVICES	2
MEM3800-256U512D	Cisco 3800 対応 256 ~ 512 MB DDR DRAM 工場アップグレード	2
MEM3800-64U128CF	Cisco 3800 シリーズ対応 64 ~ 128 MB CF 工場アップグレード	2
VIC-4FXS/DID	4 ポート FXS または DID VIC	1
VIC2-4FXO	4 ポート 音声インターフェイス カード、FXO (ユニバーサル)	1
VWIC-2MFT-T1-DI	2 ポート RJ-48 マルチフレックス トランク、T1、ドロップ アンド インサート	2
WIC-1ADSL	1 ポート ADSL WAN インターフェイス カード	1
PVDM2-64	64 チャンネル パケット音声 / ファックス DSP モジュール	2
PVDM2-64	64 チャンネル パケット音声 / ファックス DSP モジュール	2
AIM-CUE	Unity Express AIM、価格には 12 個のメールボックスが含まれる	1
SCUE-2.3	Cisco Unity Express 基本リリース、2.3	1
SCUE-LIC-200CME	Unity Express ライセンス、200 個の音声メールボックス、自動応答、CCME	1
PWR-3845-AC/2	Cisco3845 リダンダント AC 電源	2
CAB-AC	電源コード、110 V	4
FL-CCME-192	Cisco CallManager Express 機能ライセンス、最大 192 台の電話機	2
CUE-LANG-ENU	Cisco Unity Express、北米英語版	1
PWR-3845-AC	Cisco 3845 AC 電源装置	2

■ パートナー

WS-C4506	Catalyst 4500 シャーシ (6 スロット)、ファン、電源モジュールなし	2
PWR-C45-2800ACV	Catalyst 4500 2800 W AC 電源装置 (データおよび PoE)	2
PWR-C45-2800ACV/2	Catalyst 4500 2800 W AC 電源装置 (データおよび PoE)	2
CAB-AC-2800W-TWL K	U.S. 電源コード、ツイスト ロック、NEMA 6-20 プラグ	4
WS-X4013+	Catalyst 4500 Supervisor II-Plus (IOS)、ギガビット イーサネット (GE) ポート×2、コンソール (RJ-45)	2
S45IPBK9-12231SG	Cisco CAT4500 IOS IP BASE SSH	2
MEM-C4K-FLD128M	Cat 4500 IOS ベース スーパーバイザ、コンパクト フラッシュ、128 MB オプション	2
WS-X4448-GB-SFP	Catalyst 4500 ギガビット イーサネット モジュール、48 ポート 1000X (SFP)	2
WS-X4548-GB-RJ45V	Catalyst 4500 PoE 802.3af 10/100/1000、48 ポート (RJ45)	2
GLC-SX-MM	GE SFP、LC コネクタ SX トランシーバ	8
WS-C3750-48PS-S	Catalyst 3750、10/100 ポート×48 (PoE 対応)、SFP ポート×4、標準イメージ	2
CAB-STACK-3M-NH	Cisco StackWise 3M ノンハロゲン無鉛スタッキング ケーブル	1
GLC-SX-MM	GE SFP、LC コネクタ SX トランシーバ	4
CAB-AC	電源コード、110 V	2
AIR-WLC4402-25-K9	4400 シリーズ WLAN コントローラ、最大 25 の Lightweight アクセスポイント (AP) に対応	1
AIR-PWR-CORD-NA	無線用ライン コード、北米仕様	1
GLC-T=	1000BASE-T SFP	1
AIR-LAP1131AG-A-K9	802.11ag LWAPP AP 統合アンテナ FCC 設定	1
S113RK9W-12307JX	Cisco 1130 シリーズ IOS WIRELESS LAN LWAPP RECOVERY	1

パートナー

Point of Sale (POS) 端末

IBM 4851 (小規模店舗)
Windows Embedded for Point of Service バージョン 1.0 (xp-sp2)
1.2 GHz Via、512 MB SDRAM、40 GB ハードドライブ
IBM 4810-320 (中規模店舗)
Windows XP Pro バージョン 2002 サービス パック 1 ビルド 2600
Wincor-Nixdorf Beetle MII システム (小規模店舗)
Windows XP Pro バージョン 2002 サービス パック 2 ビルド 2600

Intel-M P4 2.22 GHz、1 GB RAM、74 GB ハードドライブ
Wincor-Nixdorf Beetle S II システム（中規模店舗）
Windows XP Pro バージョン 2002 サービス パック 2 ビルド 2600
Intel Celeron 2.4 GHz、512 MB RAM、37 GB ハードドライブ
Wincor-Nixdorf Beetle S II システム（大規模店舗）
Windows XP Pro バージョン 2002 サービス パック 2 ビルド 2600
Intel Celeron 2.4 GHz、512 MB RAM、37 GB ハードドライブ
NCR RealPOS 80c（大規模店舗）
NCR Advanced Checkout Solution v6.01.04.16（大規模店舗）
Verifone MX870、MX850（ワイヤレス）

ワイヤレス ハンドヘルド

Verifone Vx670（ワイヤレス）（大規模店舗）
Intermec Mobile POS CN3（ワイヤレス）（大規模店舗）
Intermec CN2BA、L Img、WM03 WWE
Microsoft Pocket PC バージョン 4.20.0（ビルド 14053）
802.11b 無線
Intermec CN3B2A、Num AImg、804、WM5 WWE
Windows Mobile バージョン 5.0 OS 5.1.342（ビルド 15096.3.0.0）
108 MB RAM、40 MB フラッシュ、13 MB ストレージ カード
802.11b 無線

ソフトウェア

Wincor-Nixdorf TP.Net V3.01
Wincor Nixdorf JavaPOS バージョン 3



APPENDIX B

データセンター / インターネット エッジの コンポーネントおよびバージョン

コンポーネント	使用している製品	バージョン
ファイアウォール	Cisco Integrated Services Router (FWSM ファイアウォール)、Cisco ASA	- FWSM v3.1(3) - ASA 7.2.(2)
ネットワーク IDS	Cisco Integrated Services Router (IDS/IPS 内蔵)、IDSM2	IOS v12.3(11r)T2、12.4(1r)、IDSM 6.0.(2)E1
ルータ	Cisco Integrated Services Router (IOS ファイアウォール)、Cisco 7206VXR	IOS v12.2(18)SXF10a、v12.3(11r)T2、12.4(1r)、12.4(11)T3 (VXR)
ワイヤレス AP	Cisco 1131AG、1242AG	
ワイヤレス コントローラ	AIR-LAP1131AG-A-K9、AIR-LAP1242AG-A-K9	IOS 12.3(11)JA
Windows サーバ	Windows Server 2003	SP1、SP2
ECOM Web サーバ (デモ サーバ)	Foundstone Hackme Bank	v2.0
データベース	該当せず — 検査なし / 対象外	
Windows サーバ アンチウイルス	McAfee VirusScan Enterprise + Anti-spyware モジュール	8.0.0
ファイアウォール、ルータ、スイッチ、IDS/IPS 管理	Cisco Security Manager (CS-M)、Cisco ASDM、Cisco IDM	CS-M v3.0.1、ASDM v5.2.(2)、IDM v6.0.2
ルータ、スイッチ管理	CiscoWorks (LMS)、CiscoWorks (C-NCM)	LMS v2.6、NCM v1.2.1
デスクトップ / サーバ ファイアウォール (ホストベースのファイアウォール)	Cisco Security Agent (CSA)	v5.1.0.69、v5.2.0.210
中央のロギング / 相関 / 分析	CS-MAR	CS-MARS (v4.3.1)
無線管理	Wireless Control System (WCS)	v4.1
AAA (TACACS+) 認証	CS-ACS	v4.0(1) ビルド 27
Web サービス (アプリケーション) ファイアウォール	Cisco ACE XML Gateway	V5

ロード バランサ	Cisco ACE ロード バランサ	V3.0(0)A1(4a)
2 ファクタ 認証	RSA SecurID (RSA Authentication Manager)	V6.1(300)
RSA Key Manager 認証	RSA Access Manager	v6.0
デスクトップ E メール暗号化	該当せず — 対象外	
ファイルの完全性	Cisco Security Agent (CSA)	v5.1
カード所有者ストレージ暗号化	• NCR-ACS (128 ビット 3DES) • RSA Key Manager (192 ビット 3DES、128 ビット、192 ビット、256 ビット AES) • RSA File Security Manager (192 ビット 3DES、256 ビット AES) • RSA enVision	• 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

アプリケーション プロトコル

この付録では、重要なプロトコルを一覧に示します。これらのプロトコルとアプリケーションフローの詳細については、Excel スプレッドシートの EDCS-572796 を参照してください。

表 C-1 アプリケーション プロトコル

HTTP	80/TCP HTTP (HyperText Transfer Protocol) — Web ページの転送に使用
HTTPS	443/TCP、UDP HTTPS — TLS/SSL を使用した HTTP プロトコル (暗号化伝送)
FTP	20/TCP、UDP FTP — データ ポート (公式)
FTP	21/TCP、UDP FTP — 制御 (コマンド) ポート
SSH	22/TCP、UDP SSH (Secure Shell) — セキュア ログイン、ファイル転送 (SCP、SFTP)、およびポート転送に使用
Telnet	23/TCP、UDP Telnet プロトコル — 非暗号化テキスト通信
DNS	53/TCP、UDP DNS (Domain Name System)
CSA-Client	エージェントから CSAMC への場合は、次が必要です。 5401/TCP 5402/TCP 443/TCP 80/TCP
CSA-Server	CSAMC からエージェントへの場合は、5401/UDP
TACACS	49/TCP、UDP TACACS ログイン ホスト プロトコル
RADIUS	1812/UDP radius、RADIUS 認証プロトコル
RADIUS	1813/UDP radacct、RADIUS アカウンティング プロトコル
DHCP	67/UDP BOOTP (BootStrap Protocol) サーバ。DHCP (Dynamic Host Configuration Protocol) によっても使用 (公式)
DHCP	68/UDP BOOTP クライアント。DHCP によっても使用 (公式)
TFTP	69/UDP TFTP
NTP	123/UDP NTP (Network Time Protocol) — 時間同期に使用 (公式)
NetBIOS	137/TCP、UDP NetBIOS NetBIOS ネーム サービス (公式)
NetBIOS	138/TCP、UDP NetBIOS NetBIOS データグラム サービス (公式)
NetBIOS	139/TCP、UDP NetBIOS NetBIOS セッション サービス
RPC	135/TCP、Windows RPC

表 C-1 アプリケーションプロトコル (続き)

MSDS	445/TCP Microsoft-DS (Active Directory、Windows 共有、Sasser ワーム、Agobot、Zobot ワーム)
MSDS	445/UDP Microsoft-DS SMB ファイル共有
RDP	3389/tcp Microsoft Terminal Server (RDP) は、Windows Based Terminal (WBT) として正式に登録
SNMP	161/TCP、UDP SNMP (Simple Network Management Protocol) (公式)
SNMP	162/TCP、UDP SNMPTRAP
HSRP	1985/UDP Cisco HSRP
SQL	1433/tcp、udp Microsoft SQL データベース システム (公式)
SQL	1434/tcp、udp Microsoft SQL モニタ
SYSLOG	514/UDP Syslog プロトコル — システム ロギングに使用
AV	82/tcp McAfee Antivirus アップデート
ICMP	すべての ICMP
NetFlow	2055/TCP Cisco NetFlow
LDAP	636/TCP、UDP LDAP over SSL (暗号化伝送)
LDAP	389/TCP、UDP LDAP (Lightweight Directory Access Protocol)
KERBEROS	464/TCP、UDP Kerberos パスワードの変更 / 設定
KERBEROS	543/TCP klogin、Kerberos ログイン
KERBEROS	544/TCP kshell、Kerberos リモート シェル
KERBEROS	88/TCP Kerberos — エージェントの認証
KERBEROS	88/UDP Kerberos — エージェントの認証
GC	TCP ポート 3268 — グローバル カタログ サーバ ローカル セキュリティ機関
GC	TCP ポート 3269 — グローバル カタログ サーバ ローカル セキュリティ機関
ASP	TCP ポート 42424 — ASP.Net セッション状態 ASP.NET 状態サービス
LWAPP-S	UDP/12223 IS。AP 「LWAPP 制御」用にコントローラ送信元 UDP ポートで使用
LWAPP	UDP/12222。AP 「LWAPP データ」用にコントローラ送信元 UDP ポートで使用
RSA File Security Manager	TCP/19978 および TCP/5766 - 監査ポート： - デフォルトのリスニング ポートは、TCP/19978 - 監査サービスは、アダプタ マネージャ (コンソール) によって開始される要求を待ち受ける - 設定ポート： - デフォルトのリスニング ポートは、TCP/5766 - 設定サービスは、アダプタ マネージャ (コンソール) からの要求を待ち受ける
RSA Key Manager	443/TCP、UDP HTTPS — TLS/SSL を使用した HTTP プロトコル (暗号化伝送)



APPENDIX **D**

詳細な実装および構成手順

この付録には、以下の各実装および構成手順が記述されています。

- [ワイヤレス構成 \(p.D-1\)](#)
- [POS アプリケーション システム \(p.D-7\)](#)
- [Cisco Secure Access Control Server \(p.D-8\)](#)
- [Cisco Security Manager \(p.D-18\)](#)
- [CSA Manager \(p.D-24\)](#)
- [RSA 製品用の Cisco Security Agent \(CSA\) カスタム ポリシー \(p.D-31\)](#)
- [NCR 用の Cisco Security Agent \(CSA\) カスタム ポリシー \(p.D-35\)](#)
- [RSA Key Manager \(p.D-40\)](#)
- [RSA File Security Manager \(p.D-45\)](#)
- [PCI 第 6.5 項 \(p.D-50\)](#)

ワイヤレス構成

小規模店舗 (HREAP + コントローラ アーキテクチャ)

この構成では、AP が WLAN コントローラ (WLC) から離れた場所にあります。このアーキテクチャでは、AP は WLC と通信してその構成を取得します。制御データの場合は、UDP ベースの Lightweight Access Point Protocol (LWAPP; Lightweight アクセス ポイント プロトコル) を使用しますが、そのトラフィックはローカルでブリッジされます。これを、「Hybrid REAP (H-REAP)」操作と呼びます。初期設定要件は次のとおりです。

- 小規模店舗では、店舗にある H-REAP モードの AP1130 を、データセンターまたは大規模店舗では WLAN コントローラを使用します。
- AP に、固定 IP アドレスとコントローラ アドレスを設定します。
- H-REAP 操作用コントローラに AP を設定します。
- VLAN のローカル スイッチング用に WLAN を設定します。
- 小規模店舗 AP の個々の設定について詳しくは、[付録 E 「Device Configurations」](#) を参照してください。

中規模店舗（コントローラ ベース）

この構成では、ISR が存在するネットワーク上に AP を接続し、構成 / 制御データとトラフィックのブリッジングの両方にコントローラを使用します。したがって、すべての AP/ ワイヤレス データは WLC から発信されます。これを、「ローカル」AP 操作と呼びます。初期設定要件は次のとおりです。

- 中規模店舗では、WLAN Controller Network Module (WLCM/ NM-AIR-WLC6) が搭載された ISR と「ローカル モード」の AP1130 を使用します。
- ISR には、WLAN クライアント サポート VLAN をサポートするために、複数の wlan-controller インターフェイスを設定する必要があります。
- ISR は、WLC 管理インターフェイスへの接続に L3 インターフェイスを使用する必要があります。したがって、この中規模店舗構成の WLC では、一意な WLAN 管理用 VLAN を使用します。
- WLAN のベスト プラクティス構成に従って、AP-WLC 間の通信には、あらゆるユーザ データと分離された VLAN を使用します。ISR WLCM が L3 接続されているため、WLC 通信用と AP 通信用の 2 つの VLAN を使用します。ISR は、この 2 つのサブネット間のルーティングを行います。
- ISR 上に作成する必要がある個々のインターフェイスの詳細については、[付録 E「Device Configurations」](#) を参照してください。

大規模店舗（コントローラ ベース）

この構成では、WLC は、スタンドアロンのアプライアンス (WLC-4402) です。AP は、WLC 管理インターフェイスによって共通のサブネットに接続されます。管理インターフェイスは、WLC の設定と保守の両方、および設定とワイヤレス ペイロードのための AP との通信に使用されます。ワイヤレス ユーザ トラフィックは、AP からコントローラに送信される間は LWAPP でカプセル化されており、WLC で終端 / カプセル開放されるときにはじめて、それぞれの VLAN にブリッジされます。初期設定要件は次のとおりです。

- 大規模店舗では、スタンドアロンの 4400 シリーズ コントローラと「ローカル モード」AP を使用します。
- コントローラとスイッチポートをワイヤレス LAN 用に設定します。VLAN 18 は、「管理」または LWAPP 制御トラフィック、すなわち、LWAPP (UDP) でカプセル化された、AP とコントローラ間のすべてのトラフィック（キーイング、設定、ワイヤレス ペイロードを含む）に使用される点に注意してください。
- 4400 WLC では、WLC と AP を同じサブネット上で接続できます。
- WLC4402 の設定の詳細については、[付録 E「Device Configurations」](#) を参照してください。

PCI 要件の第 2.1 項

- シスコ製コントローラが、デフォルトで、管理制限および管理ユーザの AAA 認証用に設定されていることを確認します。
- デフォルトの SSID が WLC 上でイネーブルされていないことを確認します。
- デフォルトの SNMP コミュニティ スtring public をディセーブルし、private を削除します。
- 次のコミュニティ スtring を新規に作成します。

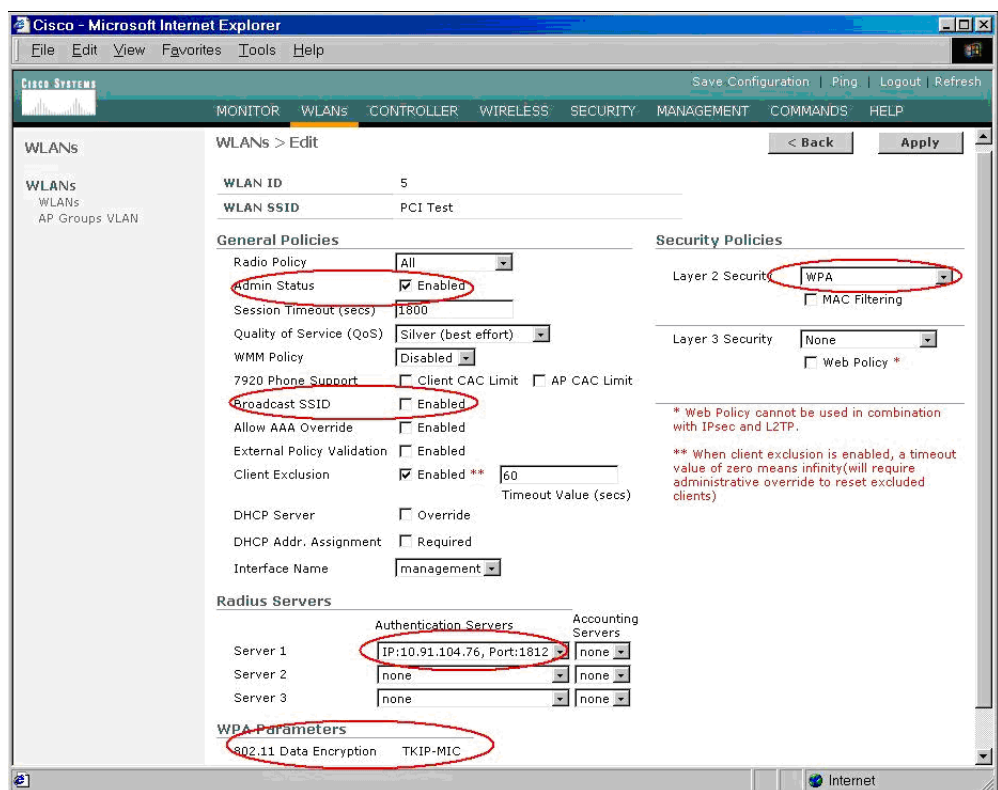
```
“config snmp community create <string>”
“config snmp community mode enable <string>”
“config snmp community accessmode <ro/rw> <string>”
```

- デフォルトのコミュニティストリングがアクセス不能になっていることを確認します。
- 初期コントローラセットアップスクリプトまたは CLI を介して、次のように管理ユーザを設定します

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

Wireless Control System (WCS) を使用する場合は、GUI で、デフォルトのユーザ名とパスワードを変更します (PCI 第 2.1.1 項)。
- ワイヤレスシステムを WPA 認証用に設定します。SSID ブロードキャストはデフォルトではイネーブルになっていますが、ディセーブルにできます。図 D-1 では、シスコ製コントローラ上で、RADIUS クライアント認証を使用した WPA セキュリティ用に WLAN を設定しています。

図 D-1 WLAN の設定

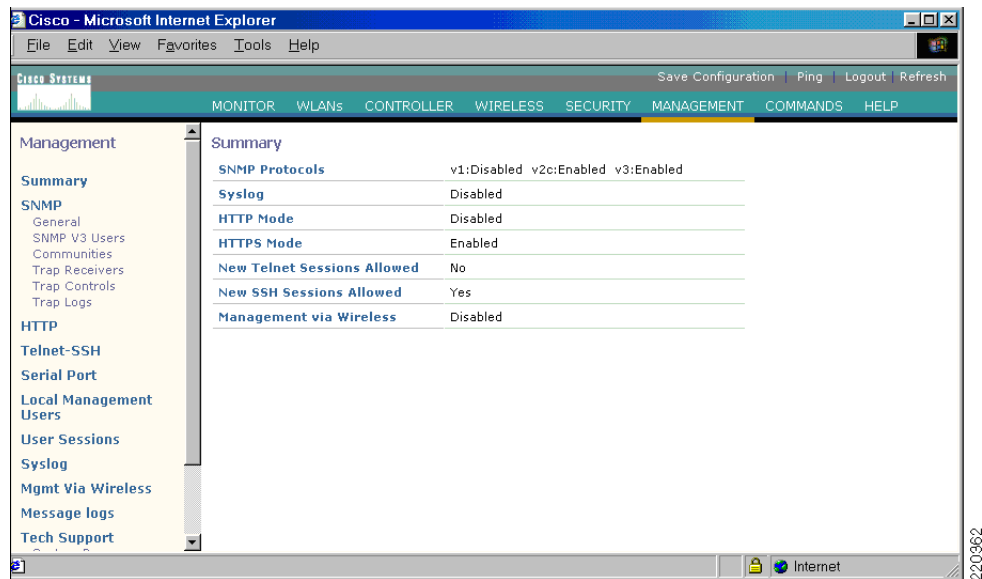


- WLAN セキュリティ設定 (SSID ブロードキャストはディセーブル、WEP/ WPA は使用中) がイネーブルにされていることを確認します (PCI Section 2.1.1)。

PCI 第 2.3 項

- コントローラがセキュア管理プロトコルのみイネーブルにされている (すなわち、HTTPS (SSL) のみ、Telnet ディセーブル、SNMPv1 ディセーブル、SSH 許可) ことを確認します。図 D-2 は、コントローラの [管理]>[サマリー] の出力です。コントローラのデフォルトのストリング (HTTP ディセーブル、Telnet ディセーブル、HTTPS [SSL]/ SSH イネーブル) が表示されています。

図 D-2 コントローラの [管理]>[サマリー] の出力

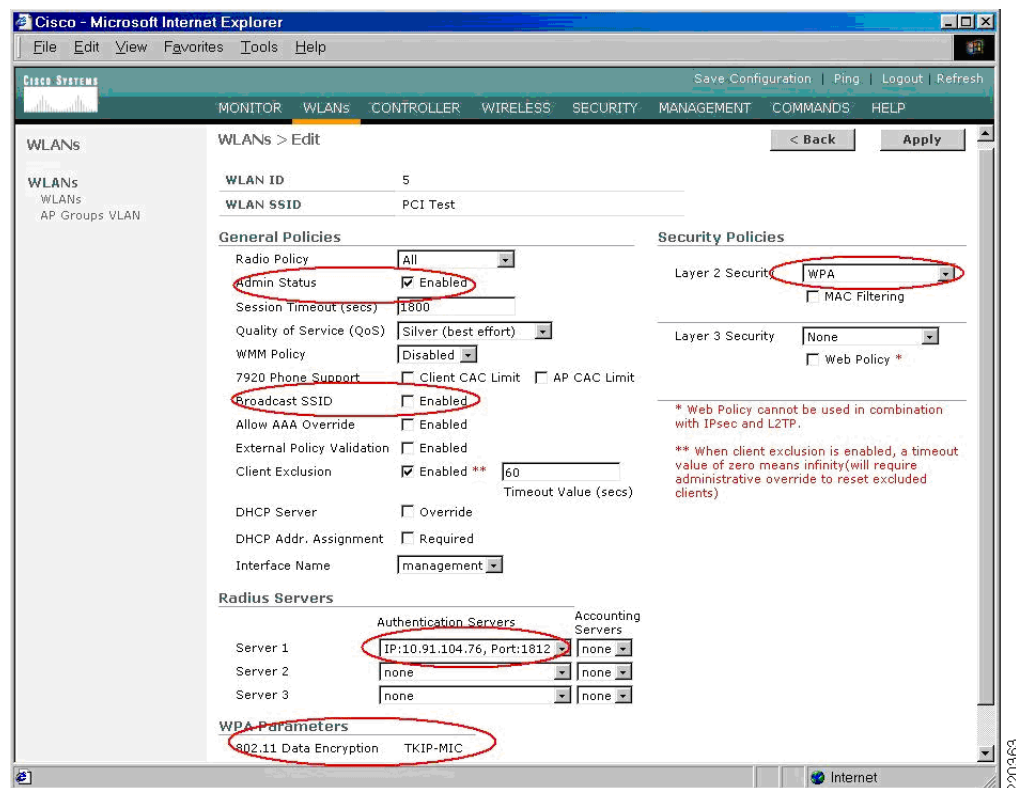


- 許可されていないインターフェイス / アドレスを介してアクセスするユーザに対する管理アクセスが拒否されていること、暗号化プロトコルだけが許可されていることを確認します (PCI 第 2.3 項)。

PCI 第 4.1.1 項

- ワイヤレス機器を WPA 認証および暗号化用に設定します (図 D-3 を参照)。

図 D-3 WPA 認証および暗号化設定



(注)

WLAN セキュリティ データ（すなわち、WPA で使用される Pairwise Master Key [PMK]、または 802.1X ダイナミック WEP で使用される WEP キー）は、WLAN コントローラ上に保存 / キャッシングされ、クライアント アソシエーション時にのみ AP に転送されます。コントローラと AP 間の制御および設定用トラフィックは、認証および暗号化されます。このリンクでは、AES 暗号化が使用されます。

PCI 第 9.1.3 項

シスコ製コントローラで使用するワイヤレス AP にコンソールからアクセスした場合、設定およびシステム情報には一切アクセスできません。コントローラのコンソール ポートに対するユーザアクセスの認証には、ユーザ データベースまたは RADIUS を使用できます。

- ネットワーク コンポーネントに対する未承認のアクセスが許可されないことを確認します。

PCI 第 10.4 項

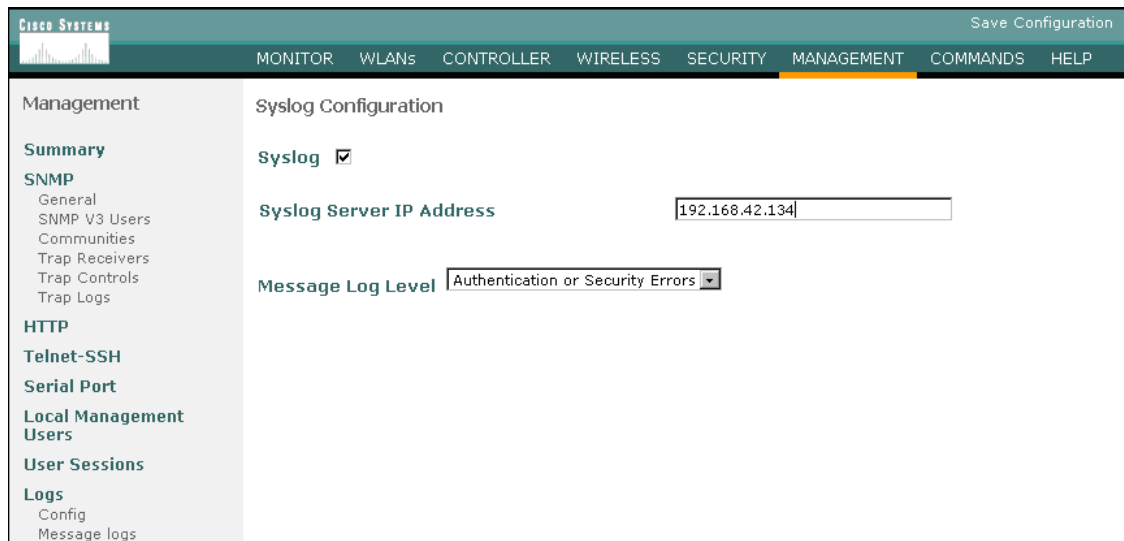
- コントローラ上の NTP をイネーブルにして、システム クロックとメッセージを同期化します。

PCI 第 10.5.4 項

- WLAN コントローラ上の Syslog をイネーブルにします（図 D-4 を参照）。
- Syslog サーバのアドレスを設定します。

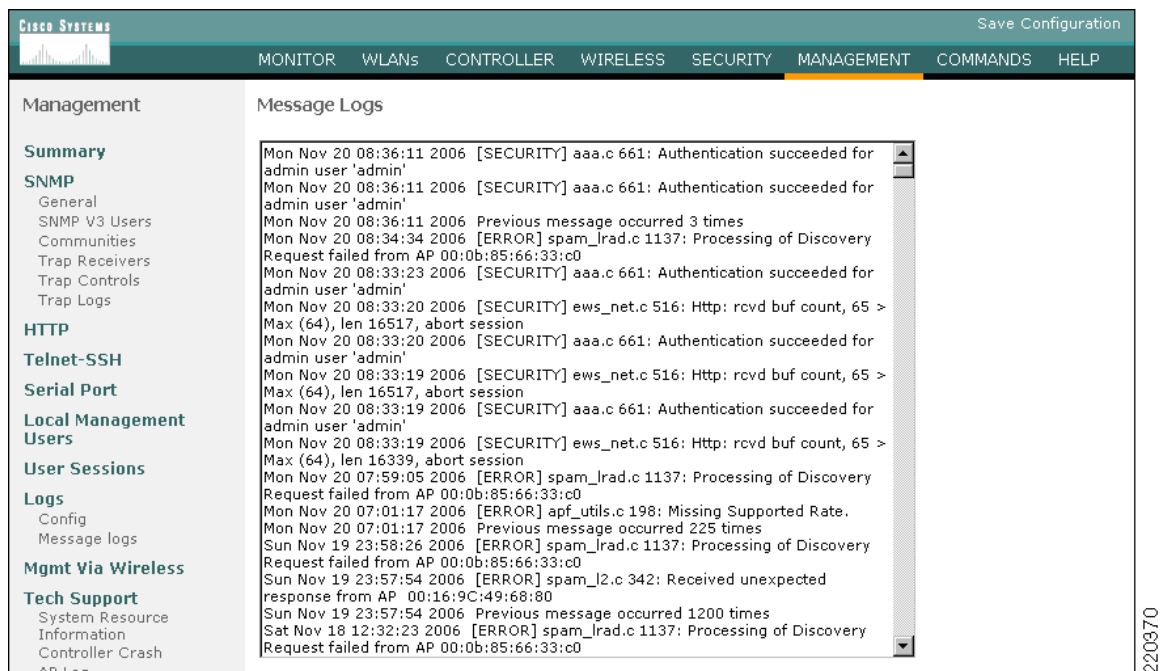
“config syslog <syslog 出力先の ip アドレス>”

図 D-4 Syslog のイネーブル化



- コントローラからの syslog ログ情報を確認します（図 D-5 を参照）。

図 D-5 Syslog ログの確認



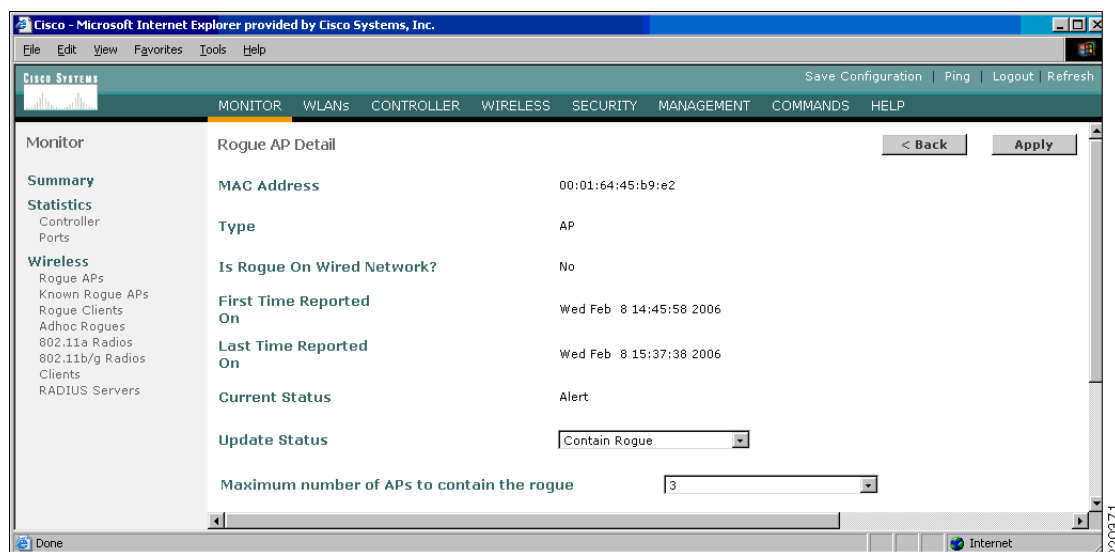
PCI 第 11 項

WLC は、IDS/rogue 不正 AP 検出がデフォルトでイネーブルになっています。WLC は、不正 AP/ワイヤレス IDS 操作を実行するとき、定期的にすべてのアクティブな WLAN の周波数をスキャンして、不正な、または悪意のある WLAN トラフィックを検出します（第 11.1 項）。

Cisco Controller GUI または WCS を介して、ネットワーク上の不正 WLAN 機器が WLC によって検出されることを確認します（図 D-6 を参照）。

不正 AP が検出されると、Cisco Controller は、管理コントロールによって指示されたとおりに、「containment（阻止）」イベントを起動します。WLAN containment イベントは、WLAN 不正デバイスからすべての WLAN クライアントを切断するアクティブなメカニズムです。

図 D-6 不正 AP の検出



不正 AP が検出されること、なおかつ Cisco Controller または WCS ユーザ インターフェイスを使用して阻止できることを確認します（第 11.4 項）。

POS アプリケーション システム

Wincor-Nixdorf TP.net と PCI

Wincor-Nixdorf アプリケーションは、QSA によって監査されませんでした。Wincor 製品はクレジット カードによる支払いを直接処理するわけではないので、PCI によって直接には規制されません。以下に、PCI ガイドラインの観点から見た Wincor 製品と、支払いシステム アプリケーションに対するインターフェイスを要約します。Wincor は、Open Payment Initiative (O.P.I.) と呼ばれるオープンな標準ベースのインターフェイスを使用しています。

- プライマリ アカウント番号 (PAN) と有効期限は、O.P.I. インターフェイス仕様のオプション要素です。これらの要素は、カード支払い要求の応答に含まれます。これらの要素が誤って使用されないように、カード支払いシステムではこれらの要素を開示してはなりません。小売業者のビジネス要件でこれらの要素が必要な場合は、販売システム側で PCI DSS 要件を満たすようにします。サービス コードとカード所有者名は、O.P.I. インターフェイス仕様の要素ではありません。

- O.P.I. インターフェイスの場合、トラックの内容は、カード支払い要求に対する応答のオプション要素です。PCI DSS 準拠のカード支払いシステムでは、この要素を開示してはなりません。TP.net では、磁気ストライプのトラックの全内容を記録する領域はありません。
- カード確認コードと PIN 確認値は O.P.I. インターフェイス仕様の要素ではないため、記録できません。
- O.P.I. インターフェイス内では、アカウント番号の表示と印刷はカード支払いシステムが担当します。このため、PCI DSS 準拠のカード支払いシステムでは、表示および印刷機器へのリクエスト内で、この要素をマスクする必要があります。TP.net システムは、提供された印刷情報またはカード支払いシステムの表示情報の内容には責任を持ちません（ただし、TP.net 販売システムが、カード支払い要求に対する応答に含まれる要素を用いて印刷レイアウトを自身でフォーマットする場合はその限りではありません）。販売システムは、顧客の領収書に、必ずマスクされたアカウント番号を使用する必要があります。
- マスクされていないアカウント番号は、O.P.I. インターフェイス仕様のオプション要素です。この要素が、カード支払いシステムによって提供された場合、TP.net 販売システムは、この要素をシステムに格納するときに表示する必要があります。TP.net V3.x には、格納場所によらず、表示に弱いカード所有者データを確実に読み取り不能にする機能のオン/オフを切り替えるコントロールが用意されています。
- TP.net は、標準のシステム開発プロセスを使用して開発されています。開発環境には、最新の修正プログラムがすべてインストールされた Microsoft .NET フレームワークを使用します。また、TP.net には拡張ユーザ管理機能が用意されているため、重要なデータおよびシステムに対するアクションは、既知のユーザおよび許可されたユーザだけが実行できます（実行トレースの出力先もこれらのユーザに限定されます）。

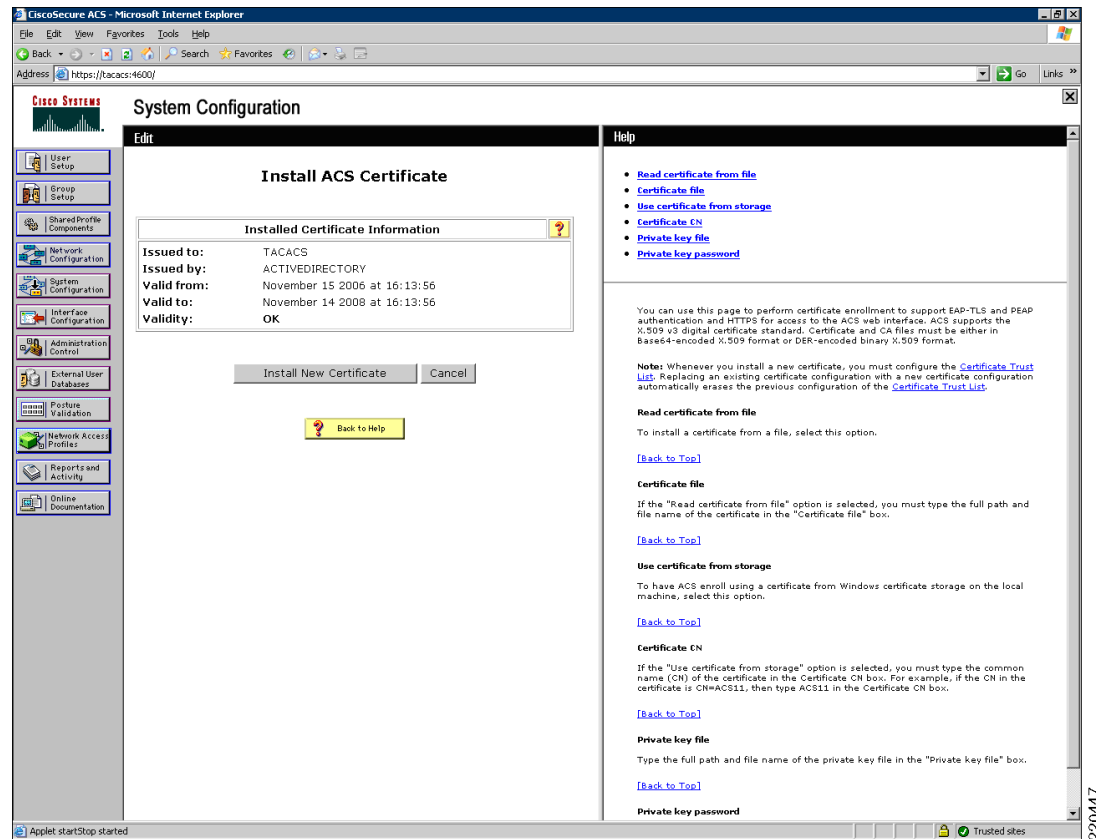
Cisco Secure Access Control Server

CS-ACS を、Windows 2003 サーバ R2 が稼働する Windows MCS 7825 サーバ上にインストールしました。CS-ACS 製品のデフォルトの標準インストールを選択しました。個別のユーザアカウントは追加していません。以下に示す一般的なエンタープライズ ロールに基づいて、複数のグループを定義しています。

- ネットワーク エンジニア
- セキュリティ エンジニア
- ワイヤレス エンジニア
- ワイヤレス ハンドヘルド ユーザ
- ネットワーク管理者
- ネットワーク管理承認者
- ネットワーク管理ヘルプ デスク

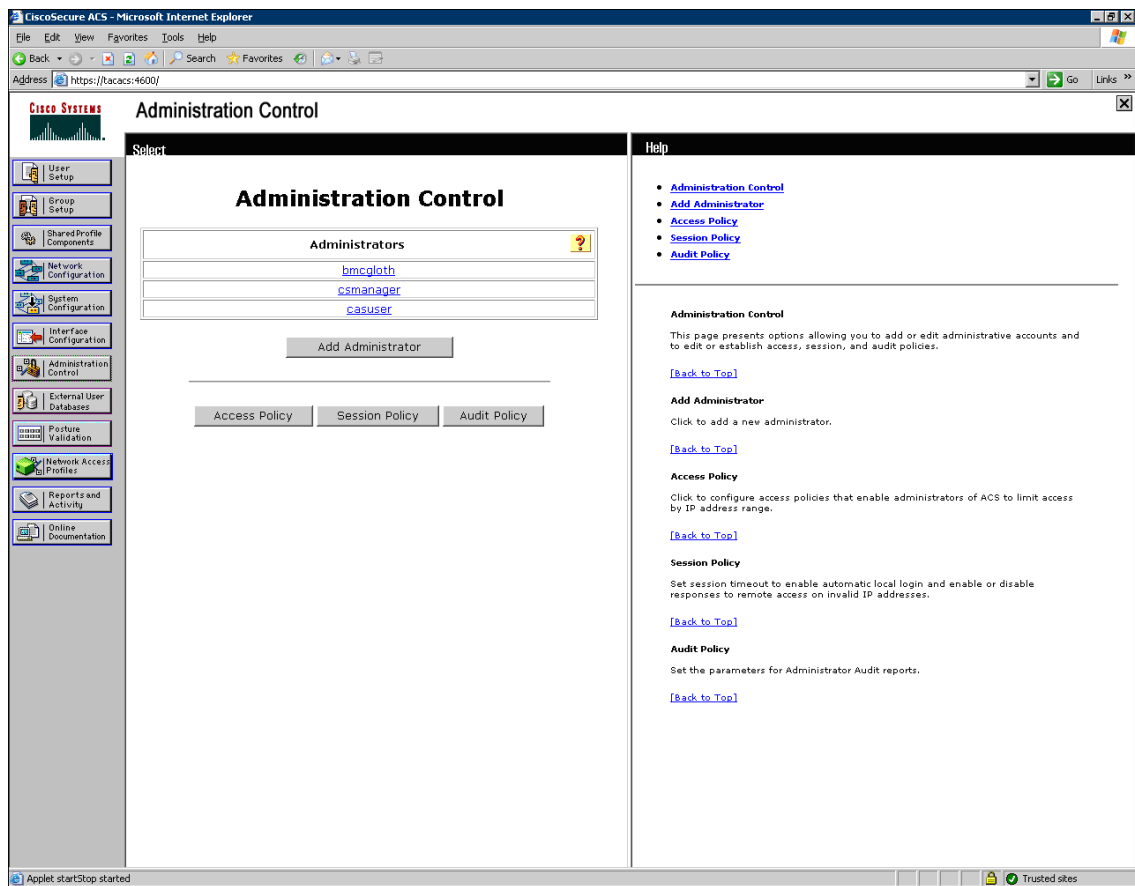
システム インターフェイスは、適切な証明書をインストールすることで、HTTPS/SSL 暗号化された通信専用を設定しました（図 D-7 を参照）。

図 D-7 Cisco Secure ACS — 証明書



特定のユーザとシステム用にローカル管理者アカウントを追加し、汎用の管理者アカウントを削除します（図 D-8 を参照）。

図 D-8 管理者コントロールの設定



CS-ACS は、ユーザ管理者用パスワードの複雑さと履歴という点で、PCI 要件を満たしていません。パスワードは 4 文字でよく、複雑さ（使用しなければならない文字）に関する制限もなく、履歴も保持されません。

これを補うため、管理者インターフェイスに対するアクセスを制限し、Windows ログインなどの追加の認証方式を利用しています。シスコのラボでは、CS-ACS の設定はサーバデスクトップからのみ許可され、リモート Web アクセスは、2 つの管理プラットフォーム（CiscoWorks LMS と CS Manager）からのみ許可されます。

接続はさらに制限され、HTTPS 接続のみ許可されます（図 D-9 を参照）。

図 D-9 アクセス ポリシーの設定

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

セッションは 15 分間に制限しました。3 回以上続けてログインに失敗した場合は、その管理者用アカウントを無効にします。自動のローカルログインは削除しました (図 D-10 を参照)。

図 D-10 セッション ポリシーの設定

Administration Control

Select

Session Policy Setup

Session Configuration

Session idle timeout (minutes) 15

☐ Allow automatic local login

☐ Respond to invalid IP address connections

☒ Lock out Administrator after 3 successive failed attempts

[Back to Help](#)

Help

- [Session idle timeout \(minutes\)](#)
- [Allow automatic local login](#)
- [Respond to invalid IP address connections](#)
- [Lock out Administrator after x successive failed attempts](#)

Use the Session Policy Setup page to specify parameters for ACS administrative sessions.

[\[Back to Top\]](#)

Session idle timeout (minutes)

Type the number of minutes of inactivity after which the browser terminates the remote administration connection. The default is 60 minutes.

[\[Back to Top\]](#)

Allow automatic local login

Click to clear this check box to force administrators to log in to the user interface on the local ACS. Administration on the local ACS will now require a username and password. This option is selected by default.

[\[Back to Top\]](#)

Respond to invalid IP address connections

If this check box is selected, ACS responds with an error message to the remote administrator when the workstation is on an invalid, unauthorized IP address range for remote access. If this check box is cleared, no error message is generated when an invalid remote connection attempt is made. Administrators can disable this option to prevent unauthorized identification of ACS. This option is selected by default.

[\[Back to Top\]](#)

Lock out Administrator after x successive failed attempts

To enable ACS to lock out an administrator after a number of successive failed login attempts, select the **Lock out Administrator after x successive failed attempts** check box, and then, in the **x** box, type the number of unsuccessful login attempts after which an administrator is locked out of Cisco Secure ACS. If the **Lock out Administrator after x successive failed attempts** check box is selected, the **x** box cannot be set to zero.

[\[Back to Top\]](#)

Submit Cancel

Applet start/stop started

Trusted sites

ワイヤレスまたは LAN ユーザを認証するとき、802.1x に対応するように PEAP 認証を設定しました (図 D-11 を参照)。

図 D-11 グローバル認証の設定

System Configuration
Global Authentication Setup

EAP Configuration

PEAP

- ☒ Allow EAP-MSCHAPv2
- ☒ Allow EAP-GTC
- ☒ Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect: ☒

EAP-FAST
[EAP-FAST Configuration](#)

EAP-TLS

- ☐ 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

- ☐ Allow LEAP (For Aironet only)

EAP-MD5

- ☐ Allow EAP-MD5

AP EAP request timeout (seconds):

MS-CHAP Configuration

- ☐ Allow MS-CHAP Version 1 Authentication
- ☒ Allow MS-CHAP Version 2 Authentication

Buttons: Submit, Submit + Restart, Cancel

Help

Global Authentication Setup

This page specifies settings for various authentication protocols.

- [EAP Configuration](#)
- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP Request Timeout](#)
- [MS-CHAP Configuration](#)

EAP Configuration

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

PEAP

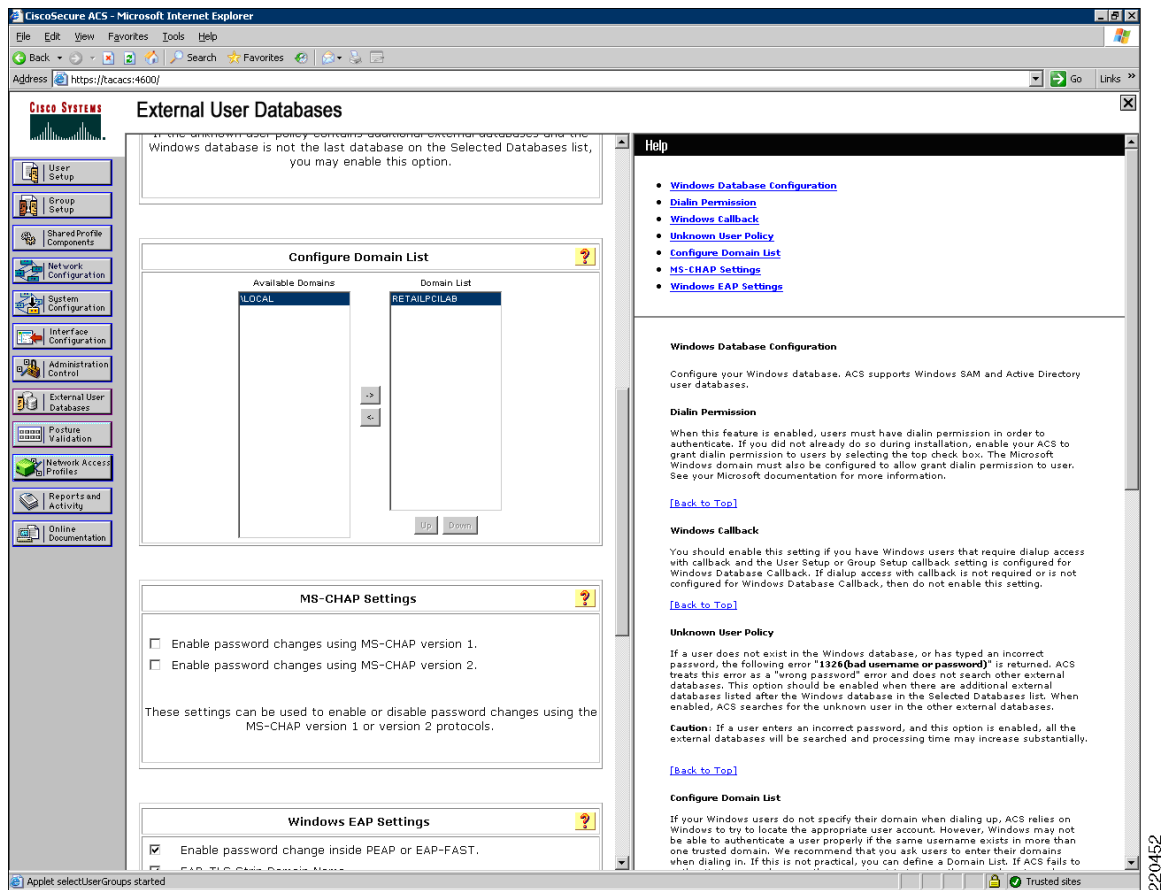
PEAP is the outer layer protocol for the secure tunnel.
Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.

- Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- Allow EAP-GTC** — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- Allow Posture Validation** — Enable this option to use the PEAP (EAP-TLV) protocol for posture validation of Network Admission Control (NAC) clients.
- Cisco client initial message** — To specify a message for users who use a Cisco PEAP client, type the message in this field. The message is limited to 40 characters.
- PEAP session timeout (minutes)** — Enter the amount of time in minutes to define the length of the maximum PEAP session.

ACS supports a fast reconnect feature. When the session resume feature is enabled, the fast reconnect feature causes ACS to allow a PEAP session to resume without checking user credentials. In effect, enabling this feature allows ACS to trust a user based on the cached TLS session from the original PEAP authentication. Because ACS only caches a TLS session when a PEAP session is successful, ACS will not cache a TLS session when a PEAP session fails.

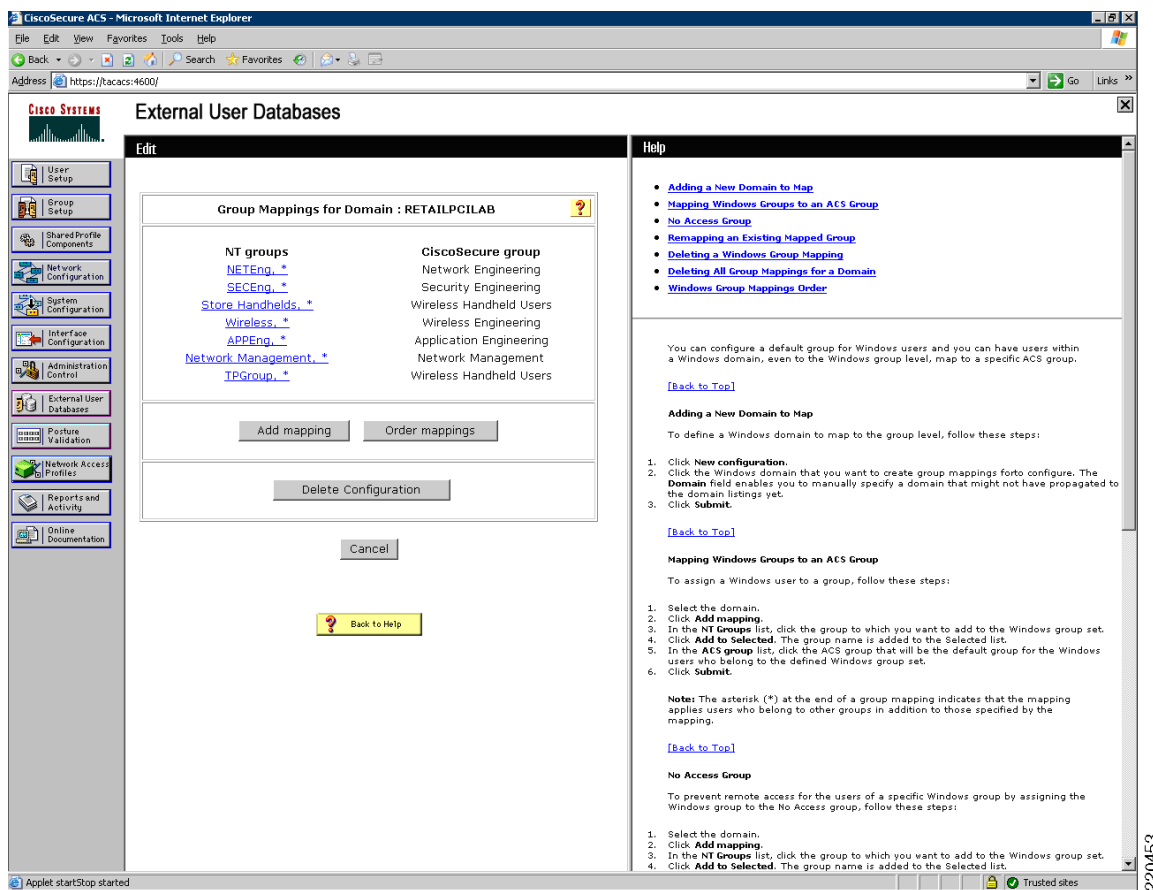
認証対象ドメインを設定します（図 D-12 を参照）。

図 D-12 ドメイン リストの設定



ローカルの CS-ACS グループを、Microsoft Active Directory の対応するユーザ グループにマッピングしました (図 D-13 を参照)。

図 D-13 ドメインのグループ マッピング



ローカル ユーザのマッピングは、グループ間で動的に実行されます。十分に強いパスワードを設定する機能がないため、PCI 要件を満たすという観点から、ローカル ユーザ アカウントは、CS-ACS 上には保存されていません（表 D-1 を参照）。

表 D-1 ローカル ユーザのマッピング

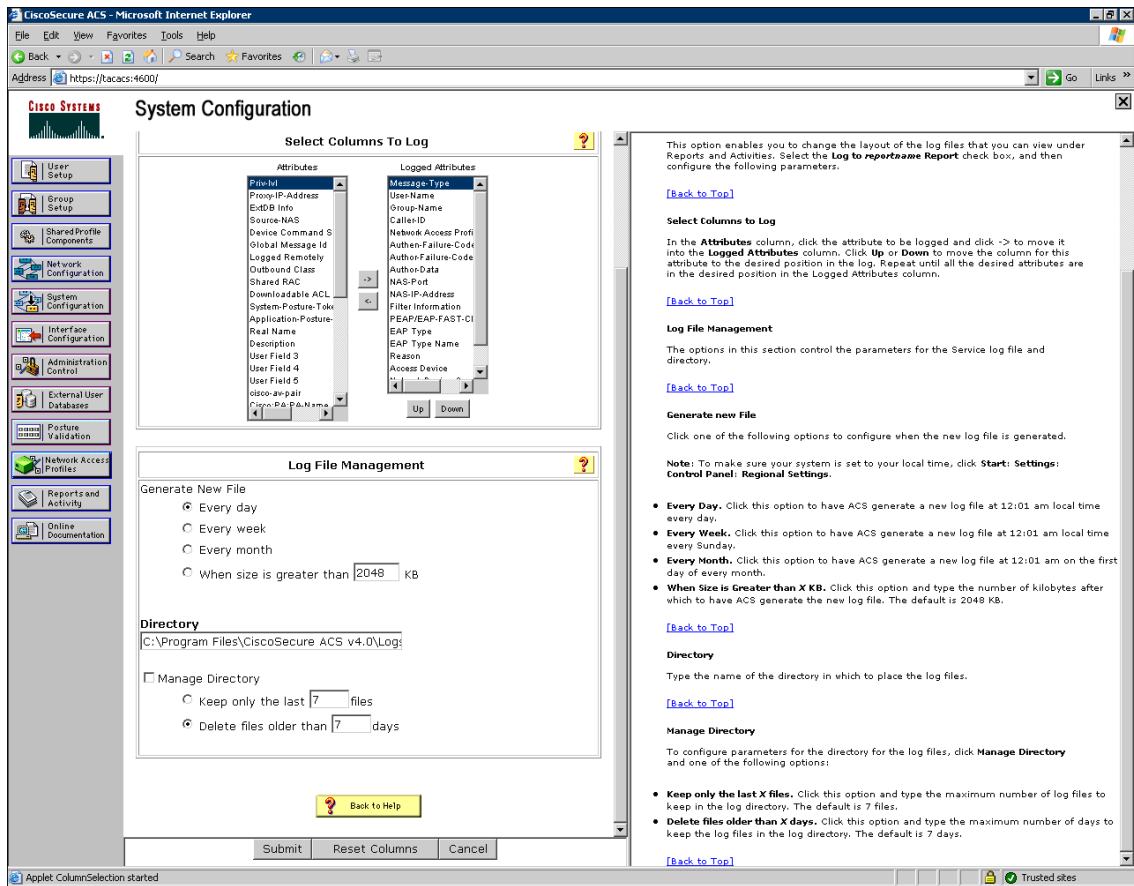
ユーザ	ステータス	グループ	ネットワーク アクセス プロファイル
bmcgloth	イネーブル	動的マッピング [現在 : アプリケーション エンジニア (1 ユーザ)]	(デフォルト)
csm-user	イネーブル	動的マッピング [現在 : セキュリティ エンジニア (1 ユーザ)]	(デフォルト)

ロギングは、認証ログとシステム ログを毎日循環させるように設定しました。

ベスト プラクティスは、毎日新規のファイルを作成するようにログ ファイル管理を設定し、CS-ACS でディレクトリを管理して、366 日以上経過するか、セキュリティ ポリシーに適合しないファイルを削除する方法です。現バージョン CS-ACS にはバグがあるため、ディレクトリ管理機能がデフォルトの 7 日に固定されています。この制限を回避するため、アップデート版が使用可能になるまでの間、すべてのロギングについてディレクトリ管理機能をディセーブルにしました。古いログの削除は手動で行います。また、監査ログは、CS-ACS ログ ディレクトリ用の CSA イベントによって管理されます。

さらなる対策として、すべてのログファイルをスケジュール済みのバッチファイルによってログバックアップサーバに毎日コピーします (図 D-14 を参照)。

図 D-14 ログ ファイルの管理



CS-ACS から認証を受ける各ネットワーク デバイスは個別に定義しますが、すべてのデバイスに同じ認証キーを使用します。デバイス グループごとに異なるキーを使用することもできます。シスコではキーを四半期単位で循環させることを推奨しています (図 D-15 を参照)。

図 D-15 AAA クライアント認証

Network Configuration

(Not Assigned) AAA Clients

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)
CISCOWORKS	192.168.42.134	TACACS+ (Cisco IOS)
CSAMANAGER	192.168.42.132	TACACS+ (Cisco IOS)
CSAMANAGER	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)

Page Down

Add Entry Search Cancel

Applet start/stop started

Help

- Network Device Groups
- Adding a Network Device Group
- Editing a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

Note: This page changes depending your interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appear. If you are not using NDGs, the AAA Clients table and the AAA Servers table appear in place of the Network Device Groups table.

Network Device Groups

Network device groups are collections of AAA clients and AAA servers. You can assign AAA clients and AAA servers to the network device groups you create. AAA clients and AAA servers not assigned to a particular NDG are, by default, assigned to the Not Assigned NDG.

To view the AAA Client and AAA Servers tables for a particular NDG, click the name of the NDG.

[Back to Top](#)

Adding a Network Device Group

To add an NDG to the list, click **Add Entry**, directly under the **Network Device Groups** table.

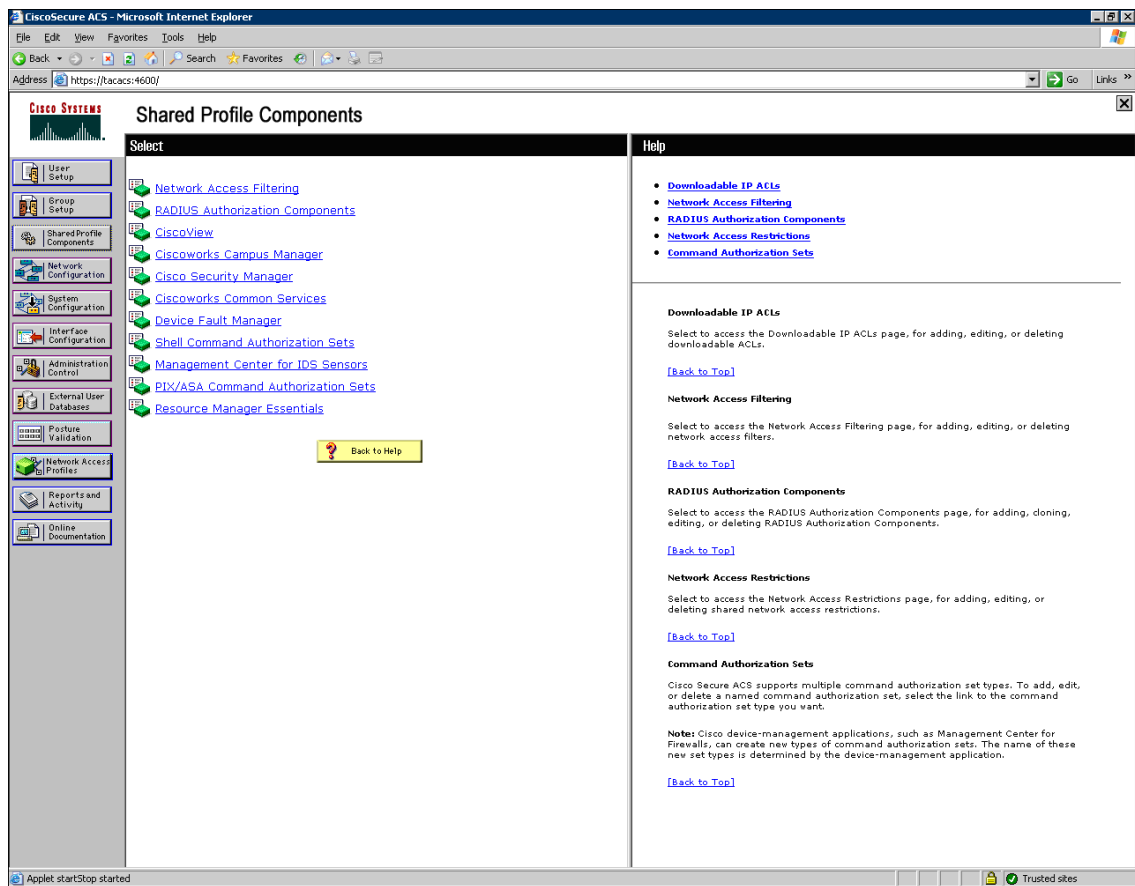
[Back to Top](#)

Editing a Network Device Group

To edit an NDG, you must first access the NDG. To do so, click the name of the NDG in the Network Device Groups table. Click **Edit Properties** at the bottom of the page.

CiscoWorks コンポーネントおよび Cisco Security Manager のインストール時に、複数の共有プロファイル コンポーネントを追加して、CS-ACS の認証を受けるとき、これらの製品に対するロールベースのアクセスのレベルを細かく設定できるようにしました（図 D-16 を参照）。

図 D-16 共有プロファイル コンポーネント



Cisco Security Manager

このセクションでは、Cisco 小売店舗 PCI 認証ラボに設定するファイアウォール構成規則について説明します。また、ファイアウォールの使用方法、および監査中の説明を分かりやすくするため、ファイアウォール内で使用する規則について説明します。

ファイアウォールの使用方法

小売業向け PCI 設計で使用するファイアウォールは、ブランチに設置された特殊なシスコ製ルータ、インターネット エッジ上の FWSM、およびデータセンター WAN 集約レイヤに配置された適応型セキュリティ アプライアンスの各デバイス上で動作する Cisco IOS に基づいています。本ガイドでは、ファイアウォールとルータを同義語とみなします。というのは、これらのデバイスは両方の機能を備えているからです。ファイアウォール ポリシーは、インバウンドおよび（または）アウトバウンド方式で、特定のインターフェイスに適用できます。ファイアウォール設定を管理するには、Cisco Security Manager (CS-M)、一元化された GUI ベースの管理製品、または GUI ベースのローカルのデバイス管理ソフトウェア（たとえば、適応型セキュリティ アプライアンスの場合は Adaptive Security Device Manager [ASDM]）を使用します。店舗の実装には多くの類似点があると思われるため、各デバイスのベースラインを小規模、中規模、および大規模店舗構

成に分類します。ここで詳しく説明する Cisco Security Manager の使用法では、各店舗で適切なレベルのセキュリティを実現すると同時に、管理の複雑さを最小限に抑えて、設定ミスや見落としを減らします。

この管理パラダイムは、次の 5 つの原則に基づいています。

1. ファイアウォールは、トラフィックの発信元インターフェイスに適用します。これは、物理インターフェイス（GigabitEthernet0/1）の場合もあれば、仮想インターフェイス（VLAN 14）の場合もあります。トラフィックは、送信元にファイアウォールが構成されているため、接続の出力側では信頼されます。そのために、トラフィックは、フレームリレー ネットワーク（WAN）経由で転送されるときも信頼されます。
2. ネットワーク上のすべてのトラフィックに正規の IP アドレスを使用します。これは、各デバイス上で **unicast Reverse Path Forwarding**（uRPF; ユニキャスト RPF）を使用して強制的に実施します。ある送信元アドレスを持つインターフェイスでパケットを受信したが、そのリターントラフィックを同じインターフェイスを介して送信元にルーティング（返信）できない場合、受信したパケットはすべて破棄します。これは、アンチ スプーフィングと呼ばれます。
3. 各ネットワークは特定の機能を提供します。各論理ネットワーク セグメント（IP サブネットまたは VLAN）は、特定のタイプのデバイスによって特定の目的を実現します。こうしたデバイス タイプによって、同一ネットワーク上のデバイス間で責任分担できると同時に、ファイアウォールをより単純な方法で設定できます。
4. インターフェイス ロールを使用してネットワークの目的を定義し、ポリシーを推進します。これにより、特定のネットワークから別のデバイスまたはネットワークへのアクセスに基づいて、ファイアウォール規則を適用できます。また、管理用ユーティリティ（Cisco Security Manager）によって、当該ネットワークが存在する各店舗に適切な単一のポリシーを定義できます。
5. 原則 4 の例外は、ファイアウォールのローカルな情報で、オブジェクトの上書きを行って対処します。たとえば、AP が、コントローラが存在する店舗にある、別の特定のネットワークにアクセスする必要があるとします。ファイアウォール ポリシーでは、この動作を原則 3 に従って簡単に確定できないため、接続の両側（送信元と宛先）を表すオブジェクトを使用してフローを定義します。

ファイアウォール規則は、単一マッチで、上から下に向かって、1 回に 1 つずつ適用されます。店舗サイトのファイアウォールはすべて同じポリシーを持ちます（詳細は以下の表を参照）。以下の 4 つの表は、階層型ポリシーの各部分を表しています。これらすべてを組み合わせると、単一のセキュリティ ポリシーが形成されます。

グローバルな CS-M アクセス ポリシー（必須）

No.	許可	送信元	宛先	サービス	インターフェイス	方向	オプション	説明
1	許可	CS-M サーバ	ローカル ルータ	SSH HTTPS ICMP	WAN インターフェイス	入力	ログ (IOS)	CS-M サーバが（外部）シリアル インターフェイス経由でデバイスにアクセスするのを許可する

店舗ポリシー（必須）

No.	許可	送信元	宛先	サービス	インターフェイス	方向	オプション	説明
1	許可	任意	任意	IP	WAN インターフェイス	入力	ログ (IOS)	データセンターからリモートへのすべての ACL をデータセンターで処理してから WAN 上に送出する
2	許可	任意	任意	IP	信頼されたインターコネクト	入力	ログ (IOS)	エラーが発生するシナリオでトラフィックを通過させるための信頼されたポート
3	許可	任意	192.168.62.1 61 192.168.62.1 62 192.168.42.1 30	NTP-UDP	LAN インターフェイス	入力		NTP を許可する
4	許可	任意	CiscoWorks Server	TFTP SNMP Syslog SNMP-Trap	ワイヤレス AP ネットワーク 管理インターフェイス	入力	ログ (IOS)	管理用 VLAN を介して管理ユーティリティをログに送信する
5	許可	CiscoWorks Server	任意	SNMP SNMP-Trap Syslog SSH Telnet HTTP HTTPS	管理インターフェイス	入力	ログ (IOS)	CiscoWorks の管理対象デバイス
6	許可	任意	CS-MARS	SNMP Syslog NetFlow	管理インターフェイス ワイヤレス AP ネットワーク	入力	ログ (IOS)	CS-MARS に対するシステム メッセージ
7	許可	任意	CS-ACS	RADIUS TACACS+	管理インターフェイス	入力	ログ (IOS)	ネットワーク デバイスによる CS-ACS の使用を許可する
8	許可	任意	データセンター ネットワーク	ICMP	管理インターフェイス	入力	ログ (IOS)	データセンターへの ping
9	許可	ワイヤレスコントローラ	CS-ACS	RADIUS	ワイヤレス AP ネットワーク	入力	ログ (IOS)	ワイヤレス ユーザを認証する

10	許可	任意	Exchange サーバ	SMTP HTTP HTTPS	ワイヤレス POS ネット ワーク 汎用データ イ ンターフェイ ス ワイヤレス データ ネット ワーク POS ネット ワーク	入力	ログ (IOS)	E メール
11	許可	任意	224.0.0.2	HSRP	ワイヤレス POS ネット ワーク パートナー ネットワーク ワイヤレス AP ネット ワーク ワイヤレス ゲ スト ネット ワーク 音声ネット ワーク 汎用データ イ ンターフェイ ス ワイヤレス管 理ネットワー ク ワイヤレス データ ネット ワーク 管理インター フェイス POS ネット ワーク	入力	ログ (IOS)	HSRP ヘルス情報
12	許可	ワイヤレス POS ネット ワーク	ワイヤレス POS ネット ワーク	ICMP	ワイヤレス POS ネット ワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
13	許可	ワイヤレス AP ネット ワーク	ワイヤレス AP ネット ワーク	ICMP	ワイヤレス AP ネット ワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
14	許可	パートナー ネットワー ク	パートナー ネットワー ク	ICMP	パートナー ネットワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
15	許可	ワイヤレス ゲスト ネット ワーク	ワイヤレス ゲスト ネット ワーク	ICMP	ワイヤレス ゲ スト ネット ワーク	入力	ログ (IOS)	ゲートウェイに ping を実行

16	許可	音声ネットワーク	音声ネットワーク	ICMP	音声ネットワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
17	許可	汎用データ インターフェイス	汎用データ インターフェイス	ICMP	汎用データ インターフェイス	入力	ログ (IOS)	ゲートウェイに ping を実行
18	許可	POS ネットワーク	POS ネットワーク	ICMP	POS ネットワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
19	許可	管理インターフェイス	管理インターフェイス	ICMP	管理インターフェイス	入力	ログ (IOS)	ゲートウェイに ping を実行
20	許可	ワイヤレス データ ネットワーク	ワイヤレス データ ネットワーク	ICMP	ワイヤレス データ ネットワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
21	許可	ワイヤレス 管理ネットワーク	ワイヤレス 管理ネットワーク	ICMP	ワイヤレス 管理ネットワーク	入力	ログ (IOS)	ゲートウェイに ping を実行
22	許可	ワイヤレス 管理ネットワーク	ワイヤレス AP ネットワーク	LWAPP-source ICMP	ワイヤレス 管理ネットワーク	入力	ログ (IOS)	コントローラによる AP との通信を許可
23	許可	ワイヤレス AP ネットワーク	ワイヤレス 管理ネットワーク	LWAPP ICMP	ワイヤレス AP ネットワーク	入力	ログ (IOS)	ワイヤレス AP による コントローラとの通信を許可
24	許可	ワイヤレス AP ネットワーク 小規模	ワイヤレス データセンター コントローラ	LWAPP ICMP	ワイヤレス AP ネットワーク	入力	ログ (IOS)	小規模店舗から データセンター コントローラ HREAP
25	許可	ワイヤレス コントローラ	ワイヤレス 管理	TFTP SNMP SNMP-Trap ICMP	ワイヤレス 管理ネットワーク	入力	ログ (IOS)	コントローラから WCS サーバ

店舗ポリシー（デフォルト）

No.	許可	送信元	宛先	サービス	インターフェイス	方向	オプション	説明
1	許可	任意	Active Directory	ILS DNS-UDP ICMP NTP HTTP Alternate-HTTP HTTPS Boots Nbssession Kerberos High-Ports-TCP tcp/1028 udp/135 tcp/445 udp/389 tcp/135	POS ネットワーク ワイヤレス POS ネットワーク	入力	ログ (IOS)	クライアントから Active Directory サーバ
2	許可	任意	Wincor-Nixdorf	Microsoft-ds MS-SQL-Server Nbdatagram Nbssession ICMP tcp/4064 MS-RDP HTTP HTTPS	POS ネットワーク ワイヤレス POS ネットワーク	入力	ログ (IOS)	POS デバイスと Wincor との通信
3	許可	任意	MS-RMS	MS-SQL-Monitor MS-SQL-Server HTTP HTTPS	POS ネットワーク ワイヤレス POS ネットワーク	入力	ログ (IOS)	POS から MSRMS サーバ
4	許可	任意	CSA-MC	tcp/5401 tcp/5402 HTTPS HTTP	汎用データ インターフェイス POS ネットワーク ワイヤレス データ ネットワーク ワイヤレス POS ネットワーク	入力	ログ (IOS)	クライアントから CSA マネージャ

5	許可	任意	Windows Update サーバ	HTTP HTTPS	ワイヤレス POS ネット ワーク 汎用データ インターフェ イス ワイヤレス データ ネット ワーク POS ネット ワーク	入力	ログ (IOS)	ウィンドウの更新を実行 するデバイスに必要
6	許可	任意	255.255.255.255 Active Directory	DHCP リレー	汎用データ インターフェ イス 管理インター フェイス POS ネット ワーク ワイヤレス ゲ スト ネット ワーク ワイヤレス管 理ネットワー ク ワイヤレス データ ネット ワーク ワイヤレス POS ネット ワーク	入力	ログ (IOS)	DHCP の動作を許可

データセンター WAN アクセス ポリシー（必須）

No.	許可	送信元	宛先	サービス	インターフェ イス	方向	オプ ション	説明
1	拒否	任意	任意	IP	すべてのイン ターフェイス	入力	ログ (IOS)	明示的に許可されていないもの はすべて拒否

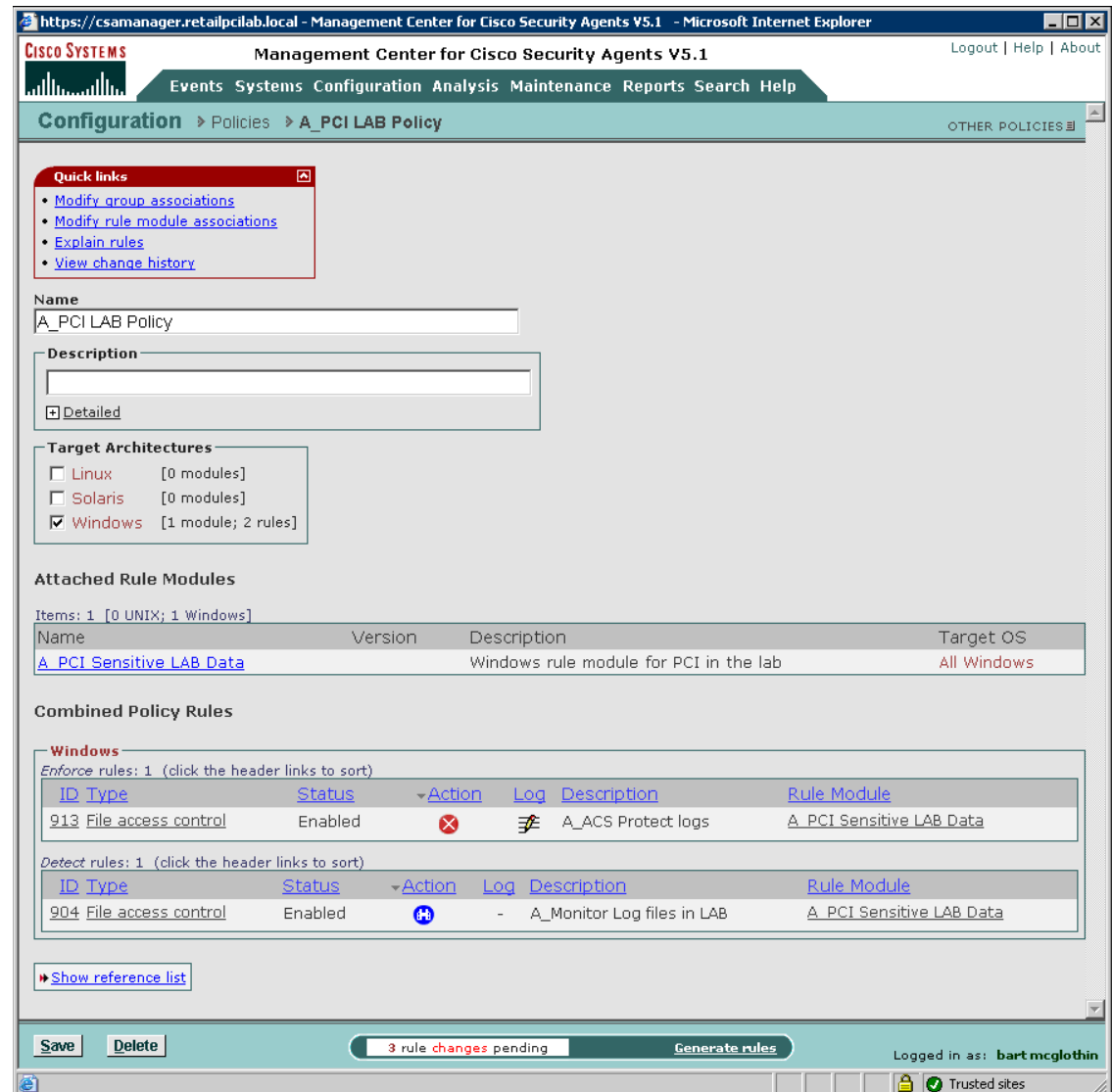
CSA Manager

CSA は、公開されているドキュメントに記載されている典型的なインストール手順を用いてインストールしました。CSA マネージャをインストールした後、CSA を使用して CS-ACS サーバ上のさまざまなログを保護するためのポリシーを作成しました。これは、他の管理サーバ上のログを保護するときに行うプロセスと同じです。

最初に、新規ポリシーを作成して、「A_PCI LAB Policy」と命名しました。次に、「A_PCI Sensitive LAB Data」という名前で Windows Rule Module を作成し、「A_PCI LAB Policy」ポリシーと関連付けました（図 D-17 を参照）。

初期ルール モジュールには、2 つの連結されたポリシー ルールが含まれています。最初のルールは、すべての管理サーバのログ ファイル（NFS バックアップ サーバ上の CSA、CS-ACS、CS-M、C-LMS、WCS、および Mars ログ）を監視し警告するものです。2 番めのルールは、CS-ACS ログを、すべてのユーザまたはプロセス（Web インターフェイス経由のアプリケーションプロセスは除く）によるアクセスから保護するものです。

図 D-17 ポリシーの設定



「A_ACS Protect logs」という説明のファイル アクセス制御ルールは、特定された CS-ACS ログ ディレクトリ内の任意のファイルに対するアクセスを拒否しログに記録するアクションを規定します（CS-ACS アプリケーション プロセスを除く）。

監視されるディレクトリは次のとおりです。

- C:\Program Files\CiscoSecure ACS v4.0\CSLog\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSAdmin\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSAuth\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSDBSync\Logs

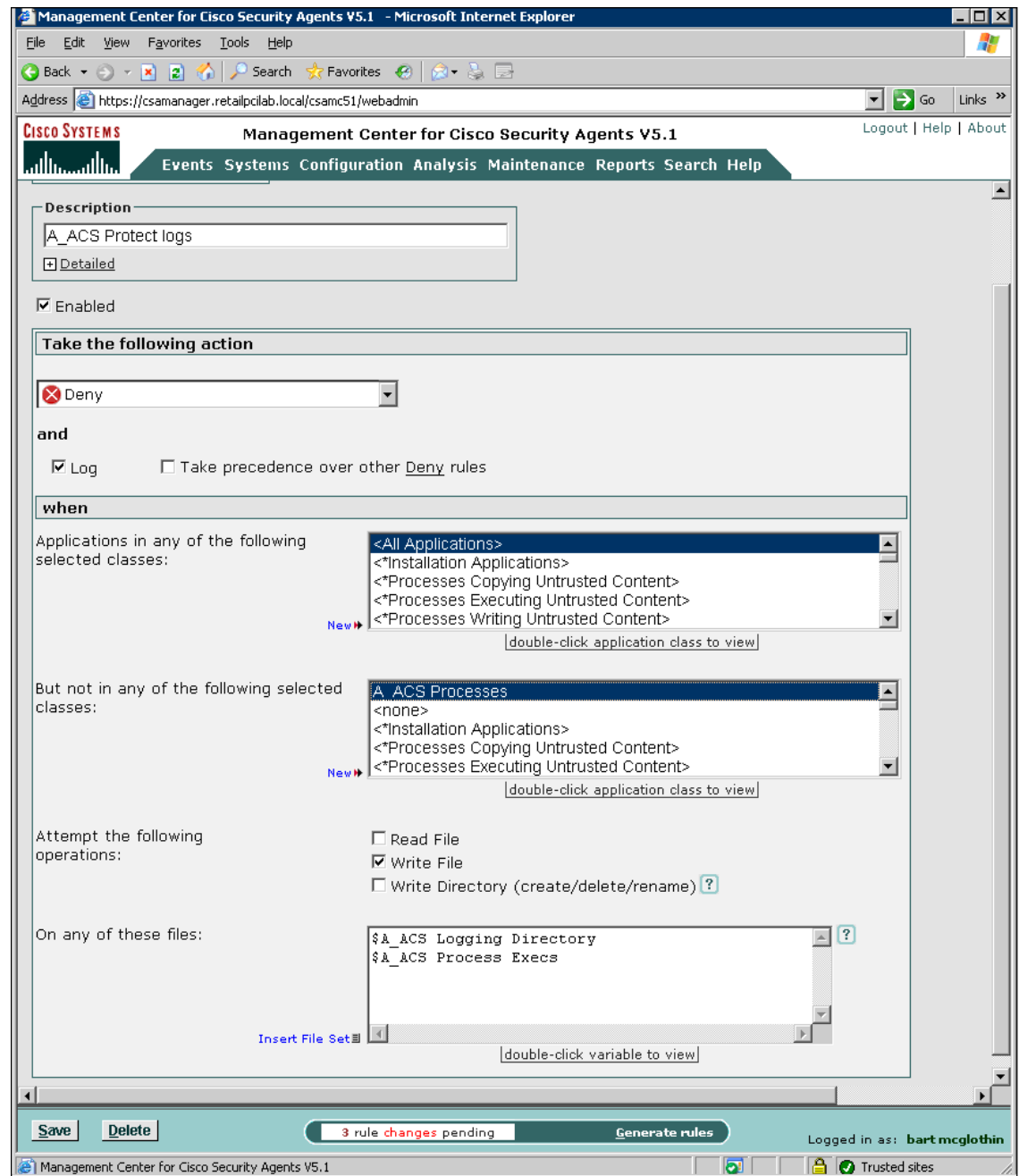
- C:\Program Files\CiscoSecure ACS v4.0\CSMon\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSRADIUS\Logs
- C:\Program Files\CiscoSecure ACS v4.0\CSSTacacs\Logs
- C:\Program Files\CiscoSecure ACS v4.0\Logs* (* はサブフォルダを含む)

許可されたプロセスの名前は次のとおりです。

- CSAdmin.exe
- CSAuth.exe
- CSDBSync.exe
- CSLog.exe
- CSMon.exe
- CSRADIUS.exe
- CSSupport.exe
- CSSupportCL.exe
- CSTacacs.exe
- CSUpdate.exe
- CSUtil.exe

これらのファイルは、“C:\Program Files\CiscoSecure ACS v4.0\bin” ディレクトリにあります (図 D-18 を参照)。

図 D-18 CSA の管理センター

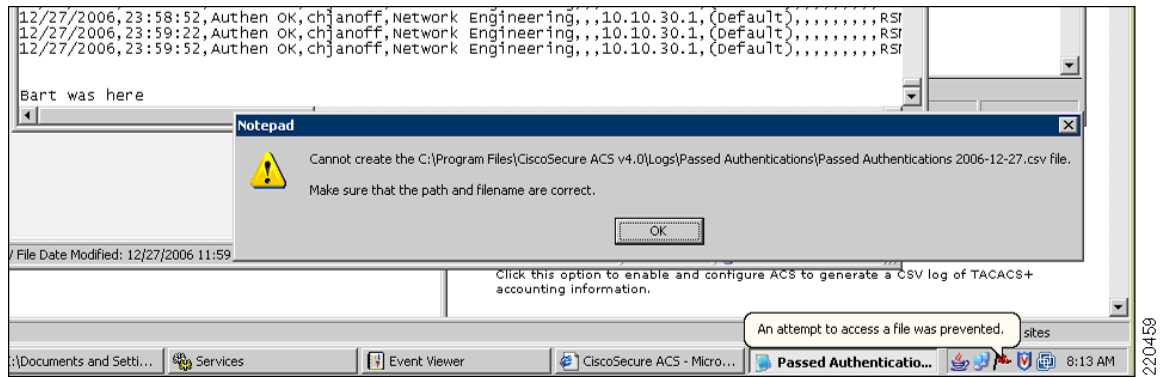


これらのルールは、CSA エージェントを使用して、ユーザおよびその他のプロセスが事前に指定したフォルダ内のファイルを直接変更するのを禁止します。

変更内容を保存しようとする、図 D-19 に示すエラー メッセージが表示されます。

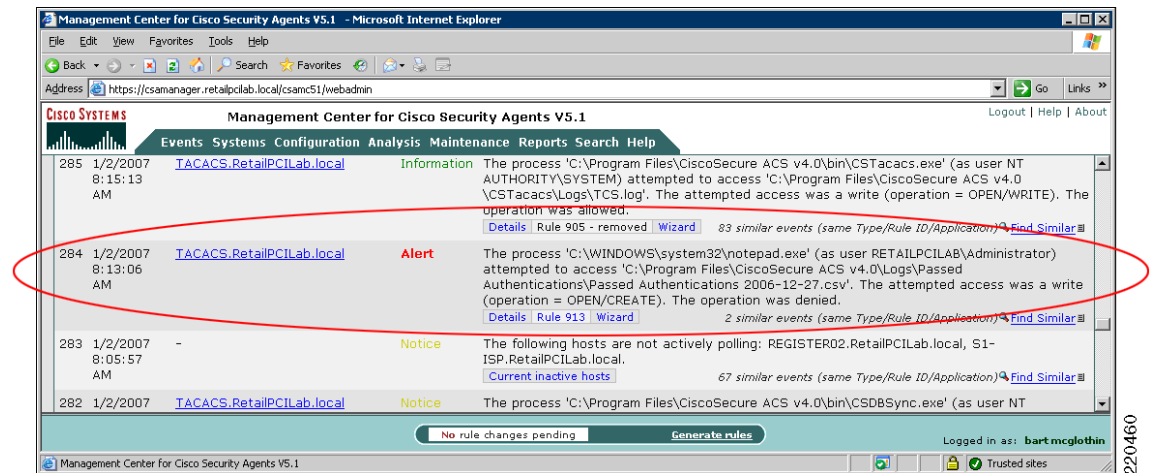
220458

図 D-19 エラー メッセージ



エラーが発生すると、CSA Manager イベント ログ内にイベントが記録されます（図 D-20 を参照）。

図 D-20 CSA Manager のイベント ログ



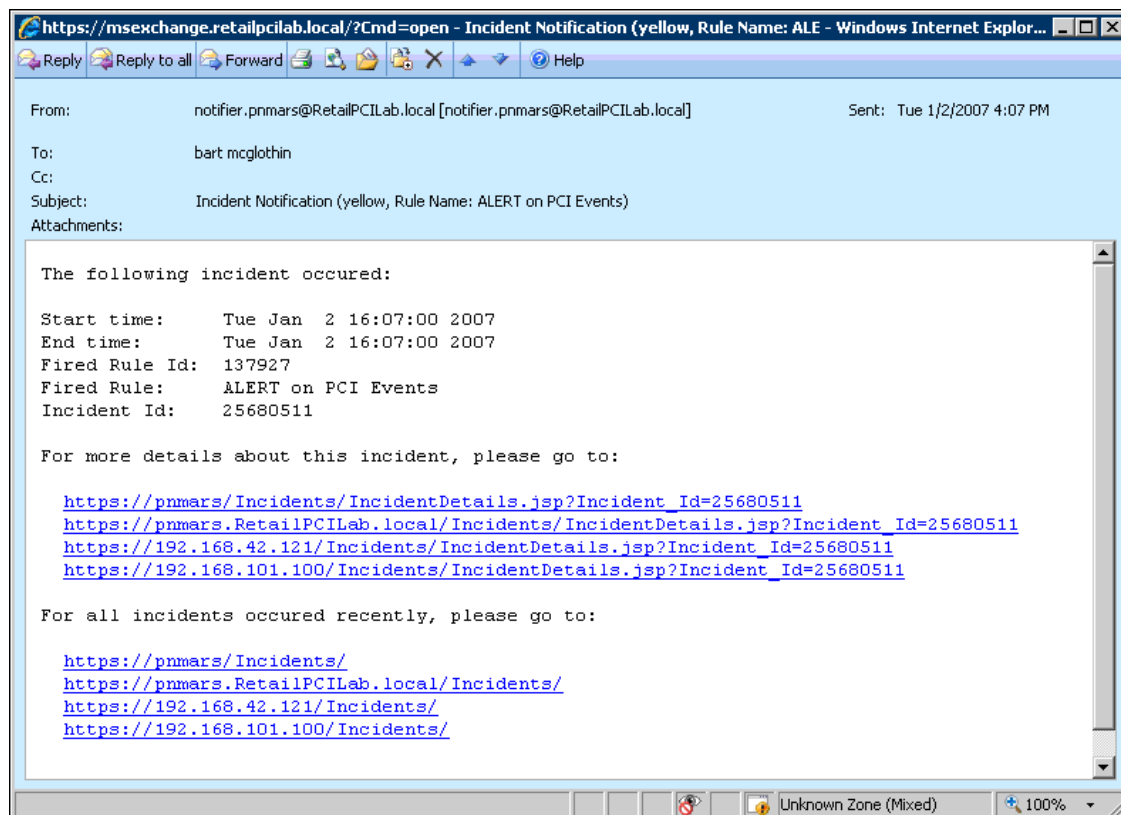
CS-MARS ログにもイベントが記録されます（図 D-21 を参照）。

図 D-21 CS-MARS ログ

Event ID	Source	Time	Process	File Name	Event Code	Event Text	Result
S:28027447	Access Control	2007-01-02 8:20:26 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:08.173	attempted to acc	Positive
E:28027448	CSA File Access Control	2007-01-02 8:20:26 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:08.173	attempted to acc	False Positive
E:28027450	CSA File Access Control	2007-01-02 8:20:26 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:08.173	attempted to acc	False Positive
E:28027433	CSA File Access Control	2007-01-02 8:20:24 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:08.157	attempted to acc	False Positive
E:28027434	CSA File Access Control	2007-01-02 8:20:24 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:08.157	attempted to acc	False Positive
E:28027414	CSA File Access Control	2007-01-02 8:20:19 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:04.690	attempted to acc	False Positive
E:28027415	CSA File Access Control	2007-01-02 8:20:19 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:20:04.690	attempted to acc	False Positive
E:28026660	CSA File Access Control	2007-01-02 8:17:05 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:16:49.169	attempted to acc	False Positive
E:28026661	CSA File Access Control	2007-01-02 8:17:05 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:16:49.169	attempted to acc	False Positive
E:28026326	CSA File Access Control	2007-01-02 8:15:29 AM PST	C:\WINDOWS\explorer.exe	TACACS+ Accounting	08:15:13.480	attempted to acc	False Positive

E メールアラートを送信するように CS-MARS ログを設定することもできます（図 D-22 を参照）。

図 D-22 E メールアラート

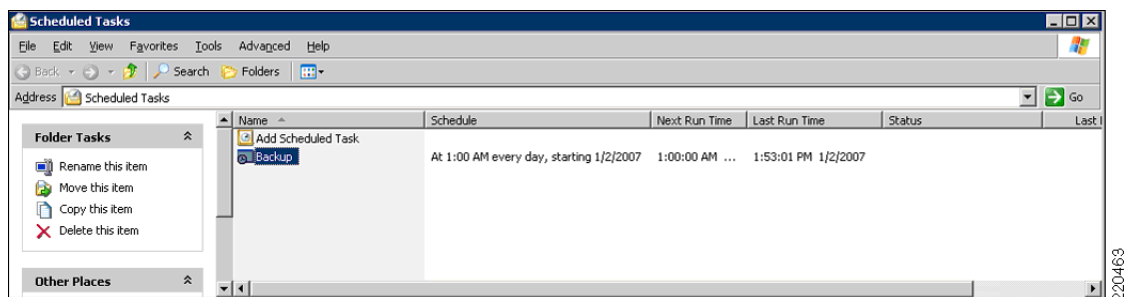


アプリケーションは保護されたディレクトリ内のすべてのファイルに対してフルアクセス権を所有しているため、ログの管理やログスイッチの切り替えなどを日常的に実行できます。

アプリケーションによる履歴ログの削除を禁止するため、システムアカウントによるファイルの削除を禁止するディレクトリ権限を設定しましたが、うまくいきませんでした。というのは、その方法だと、日常的に発生するログの切り替え/ロールイベントも禁止されてしまうからです。履歴ログの整合性と可用性を保証するには、1日最低1回はロギング機能をオフにして、保護された格納場所にログをコピーまたはバックアップする方法を推奨します。

ログバックアップサーバにログを毎日コピーするためのバッチファイルを作成しました。ログバックアップサーバでは、CSAを使用してアクセスを制限し、コピーされたログファイルを保護します（図 D-23 を参照）。

図 D-23 ログコピー用のバッチファイル



以下の例は、ログファイルを各種管理サーバにアーカイブするためのバッチファイルです。

```
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\Logs\*" /e /h /o
cd \ACS\%date%
MD CSAdmin
cd CSAdmin
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSAdmin\Logs\*" /e /h /o
cd \ACS\%date%
MD CSAAuth
cd CSAAuth
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSAuth\Logs\*" /e /h /o
cd \ACS\%date%
MD CSDBSync
cd CSDBSync
xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSDBSync\Logs\*" /e /h /o
cd \ACS\%date%
MD CSLog
cd CSLog
```



```

xcopy "x:\Program Files\CiscoSecure ACS v4.0\CSLog\Logs*.*" /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"

```

RSA 製品用の Cisco Security Agent (CSA) カスタム ポリシー

QSA からの要請に基づき、新規のカスタム ポリシー「PCI_auditors_request」を作成しました。この新規ポリシーは、次の 2 つの新規ウィンドウ カスタム ルール モジュールに関連付けられています。

- RSA_File_Security_Manager-8.1_8.5.8 — RSA File Security Manager 監査ログを保護し、RSA File Security Manager の重要なアプリケーション ファイルおよびディレクトリを不正アクセスから保護するためのルール。
- 「Deny access to RSA File security Manager executables」という説明のファイル アクセス制御ルールは、以下に示す RSA File Security Manager ディレクトリ内の特定のファイルに対するアクセスを拒否しログに記録するアクションを規定します (図 D-24 を参照)。

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

図 D-24 CSA Manager イベント ログ — RSA File Security Manager

Management Center for Cisco Security Agents V5.2

Logout | Help | Abc

Events Systems Configuration Analysis Maintenance Reports Search Help

Events > Event Log

31 events [change filter](#)

Event log generation time: 1/5/2008 5:08:58 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 296 events)

#	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

[Find Similar](#)

「Monitor RSA File Security Manager audit logs (RSA File Security Manager 監査ログの監視)」という説明のファイルアクセス制御ルールは、RSA File Security Manager 内の以下に示すファイルセット (図 D-25 を参照) に一致するファイルに対する、すべてのアプリケーションによる読み取りまたは書き込みアクセス (プロセスが終了させられたか、アクセスが拒否されたか) を監視します。このルールがトリガーされるとイベントがログに記録されます。

監視されるディレクトリは次のとおりです。

- RSA File Security Manager アダプタによって生成された監査ファイル
C:\Program Files\RSA File Security Windows Adapter\AuditLog
- RSA File Security Manager 管理コンソールによって生成された監査ファイル
C:\Program Files\RSA File Security Manager\AuditLog

図 D-25 CSA Manager イベント ログ — RSA File Security Manager 監査ログ

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](#)

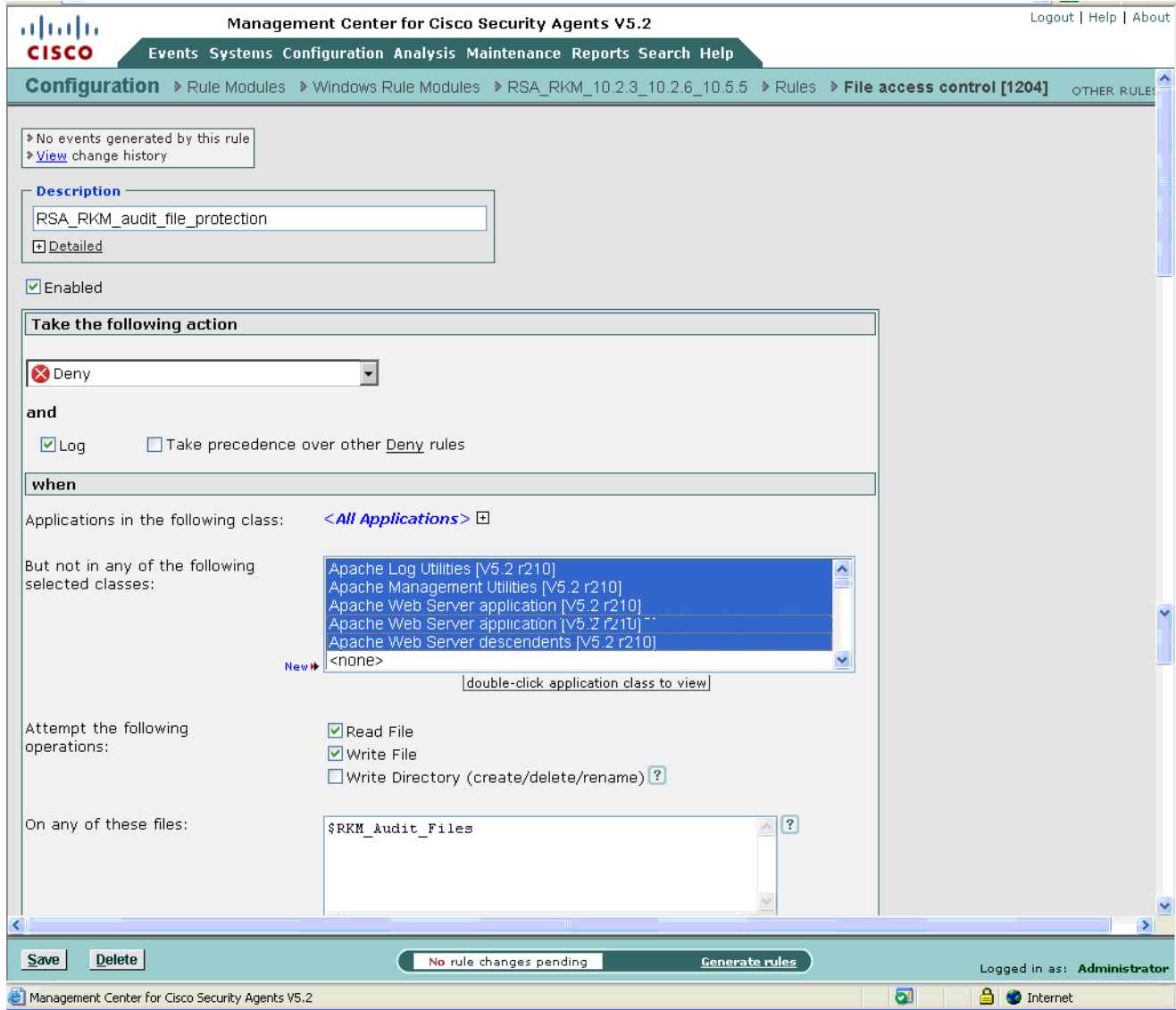
Event log generation time: 1/5/2008 4:56:23 PM
 Severity: Alert
 Host: All
 Rule Module: All
 Events per page: 50
 Sort by: Order received
 Filter out similar events: Yes (filtered out ~90% of 294 events)

#	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](#)

- RSA_RKM_10.2.3_10.2.6_10.5.5 — 不正アクセスから RSA Key Manager 監査ログ ファイルを保護し、同監査ログファイルに対する Apache Web サービスによる承認済みのアクセスを許可します (図 D-26 を参照)。

図 D-26 RSA_RKM_10.2.3_10.2.6_10.5.5 ファイル アクセス制御ルール



「RSA_RKM_audit_file_protection」という説明のファイルアクセス制御ルールは、RSA Key Manager ログファイルに対する未承認アプリケーションによるアクセスを拒否します。

図 D-27 の例では、メモ帳（未承認アプリケーション）による RSA Key Manager ログファイルへのアクセスを拒否しています。このルールがトリガーされるとイベントがログに記録されます。

監視されるディレクトリは次のとおりです。

- RSA Key Manager サーバ :
 - C:\WINDOWS\system32\LogFiles\W3SVC1
 - C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs

図 D-27 CSA Manager イベント ログ — RSA Key Manager Tomcat ログ

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](#)

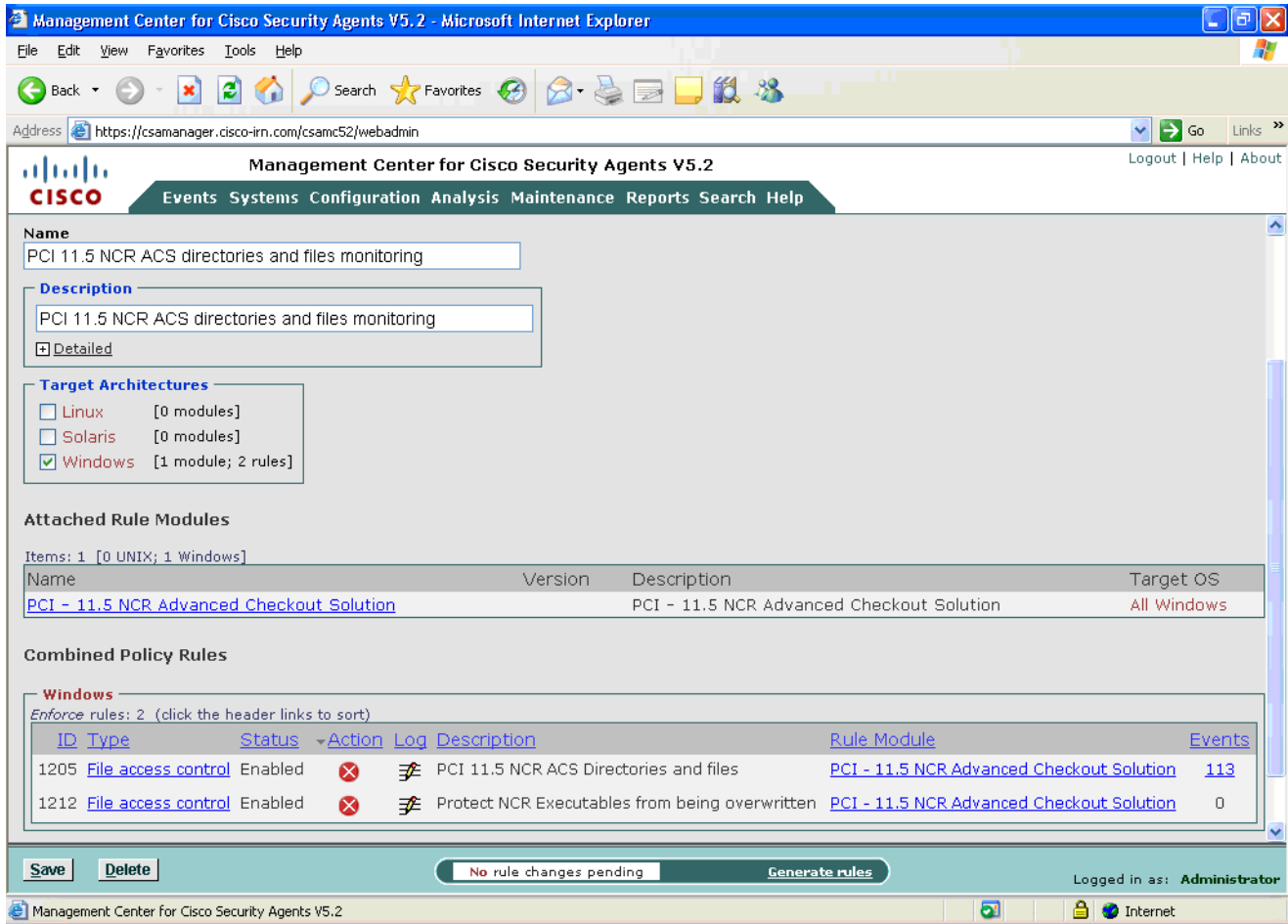
NCR 用の Cisco Security Agent (CSA) カスタム ポリシー

以下を作成しました。

1. 「PCI 11.5 NCR-ACS directories and files monitoring (PCI 11.5 NCR-ACS のディレクトリおよびファイルの監視)」という名前の新規ポリシー
2. 上記の新規作成ポリシーに割り当てられた「PCI-11.5 NCR Advanced Checkout Solution (PCI-11.5 NCR 高度チェックアウト ソリューション)」という名前の Windows Rule Module (図 D-28 を参照)

初期ルール モジュールには、2 つの連結されたポリシー ルールが含まれています。最初のルールは、NCR-ACS ディレクトリ内のファイルと実行可能ファイルを不正アクセスから保護します。2 番目のルールは、NCR-ACS の承認済みアプリケーションが上書きされないように保護します。

図 D-28 NCR ポリシーの設定



「NCR Advanced Checkout Solution」ルールモジュールは、NCR-ACS ディレクトリおよびこれらのアプリケーションに関連する実行ファイルを未許可のアクセスから保護します。「PCI 11.5 NCR ACS directories and files」ファイルアクセス コントロール ルールは、NCR-ACS ディレクトリ内のすべてのファイルおよび実行ファイルへの未許可のアクセスを拒否します。ルールがトリガーされた場合のイベントはロギングされます。

NCR-ACS ディレクトリは次のとおりです。

- @fixed \ACS**

@fixed は、\ACS ディレクトリが存在する任意のローカル ドライブ

承認済み NCR アプリケーション：

ディレクトリ マッチング

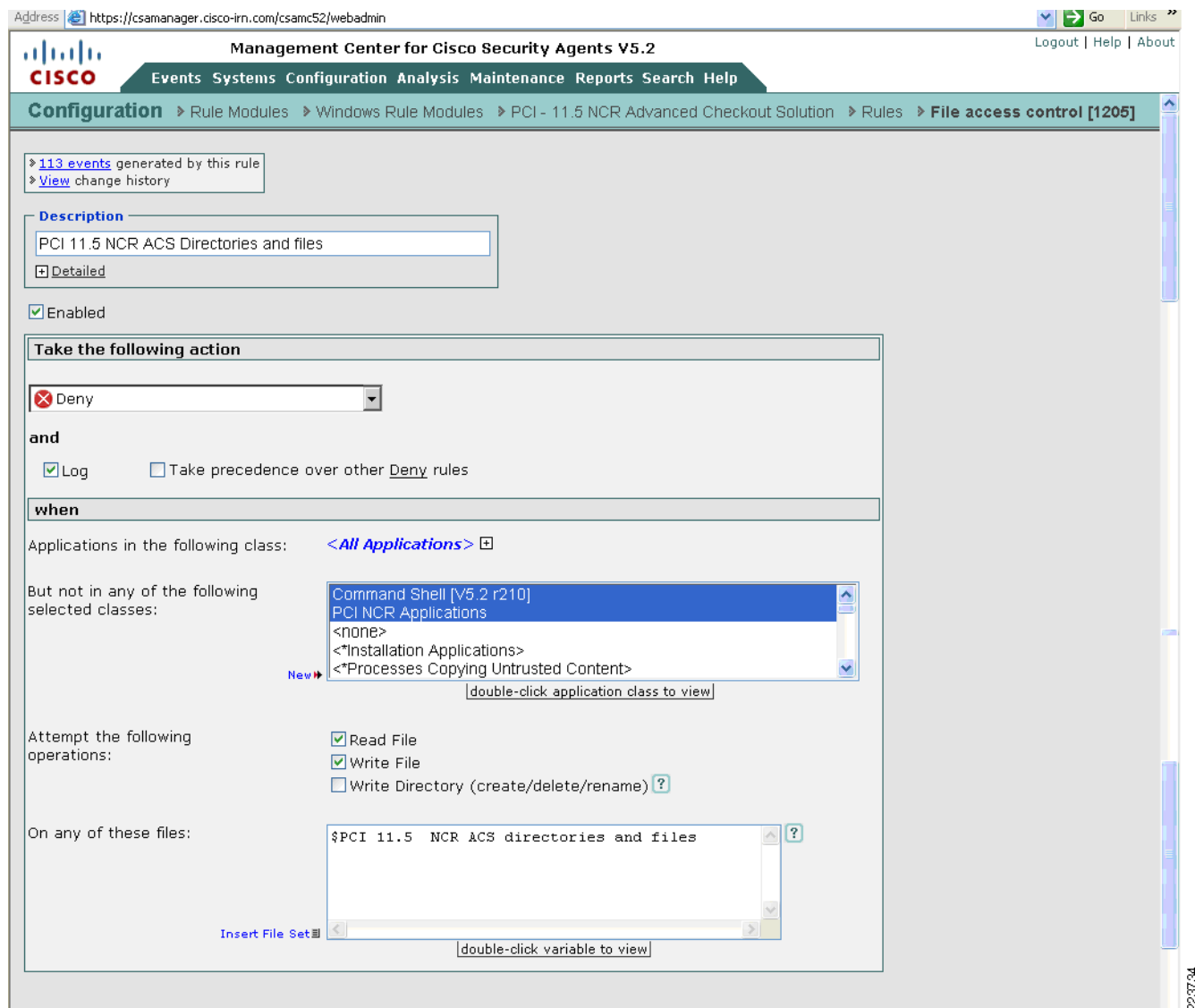
- *.*\ACS**
- *.***\Microsoft SQL Server**
- *.***\Framework**

ファイル マッチング

- *.exe
- csc.exe

図 D-29 を参照してください。

図 D-29 PCI-11.5 NCR ACS ディレクトリ、ファイル、ファイル アクセス制御ルール



「PCI 11.5 NCR ACS directories and files (PCI 11.5 NCR ACS のディレクトリとファイル)」という説明のファイルアクセス制御ルールは、PCI 11.5 NCR ACS のディレクトリとファイルに対する不正アクセスを拒否するアクションを規定します。図 D-30 に示した例では、未承認のアプリケーション (explorer.exe) が NCR POS システムの NCR-ACS ディレクトリにアクセスしようとしています。

図 D-30 CSA Manager イベント ログに NCR POS システムの ACS ディレクトリへのアクセス

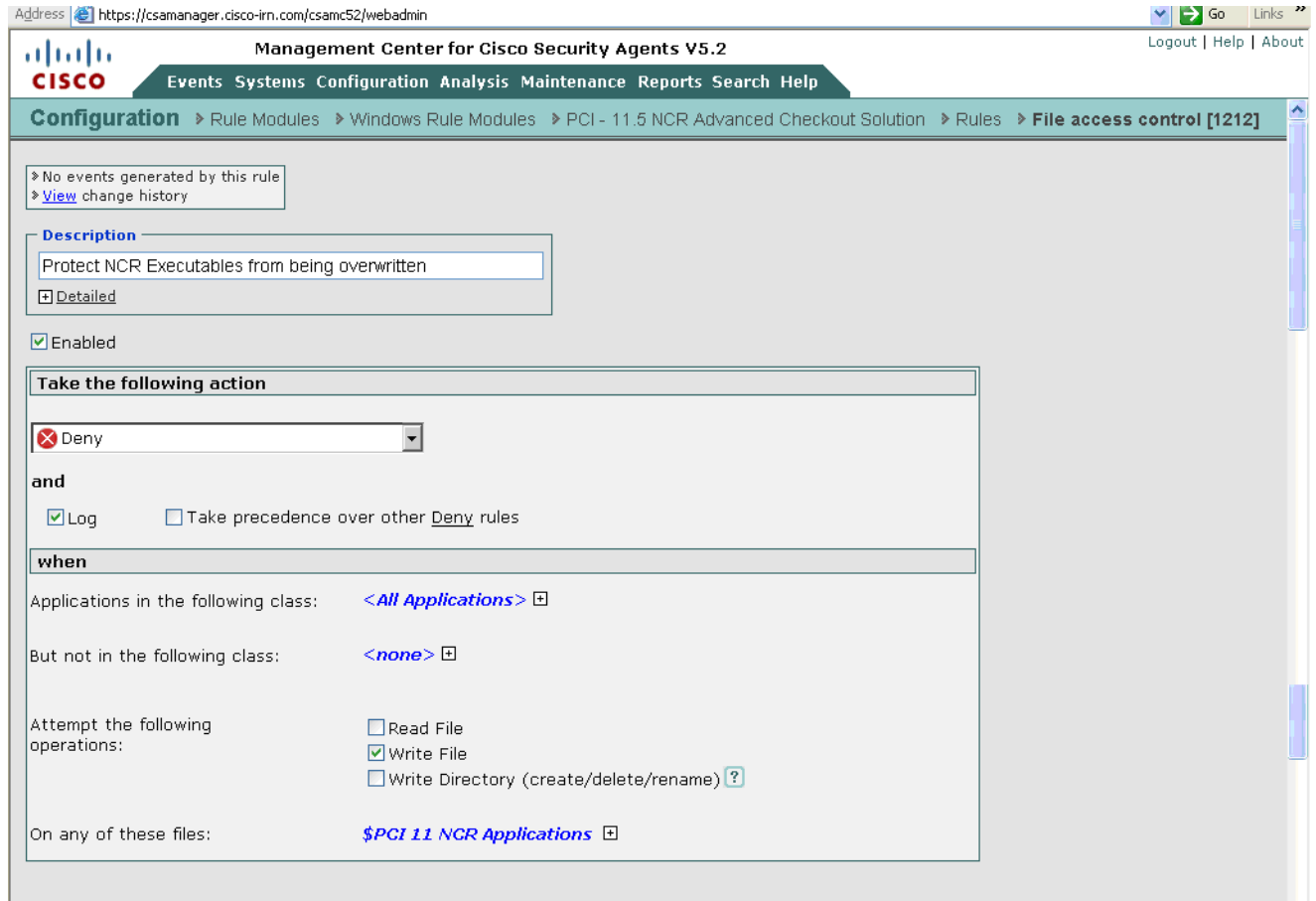
The screenshot shows the Cisco Management Center for Cisco Security Agents V5.2 interface. The top navigation bar includes links for Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. The main content area is titled 'Events > Event Log' and displays 31 events. A filter bar allows users to change filters. The event log shows a single event with the following details:

#	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

Below the event log, it indicates '50 similar events (same Type/Rule ID/Application)' and provides a link to 'Find Similar'. The interface also shows the event log generation time as 1/5/2008 6:21:03 PM and the filter settings as 'Filter out similar events: Yes (filtered out ~90% of 306 events)'.

「Protect NCR Executables from being overwritten (NCR 実行可能ファイルの上書き禁止)」という説明のファイル アクセス制御ルールは、承認済みの PCI 11 NCR アプリケーションが上書きされないように保護するアクションを規定します。図 D-31 を参照してください。

図 D-31 NCR 実行可能ファイルの上書きを禁止するファイル アクセス ルール



RSA Key Manager

RSA Key Manager 管理コンソール

このセクションでは、Key Manager 管理コンソールの主要な使用例と設定について説明します。

Key Manager サーバの起動と停止

RSA Key Manager には起動用のキーが必要です。このキーは、HSM 上に格納しておくこともできますし、起動時にパスワードとして手動で入力することもできます。あるいは、ローカルのキャッシュに格納しておき、サーバの再起動時に再生することもできます。Cisco 小売業向け PCI ラボの設定では、サーバが再起動されるたびにキャッシュに格納されたパスワードを再生します。これにより、再起動時にユーザの介入が不要になります。このオプションを選択しないと、再起動にユーザの介入が必要になります（図 D-32 を参照）。HSM を使用すると、構成によって記述されたポリシー（おそらく m 個のうち n 個）が起動されます。キー データが提示されないと、キー要求は受け付けられません。

Key Manager サーバは、インストール時に、自動で起動するか（無人再起動）、あるいはセキュリティを考慮して、マスター パスワードの入力を求めるようにするかを設定できます。インストール時に [Enable Unattended Restart（無人再起動を行う）] オプションをオンにすると、Key Manager サーバは、起動または再起動の直後に、Key Manager クライアントからの要求を処理できるようになります。このオプションをオフにすると、サーバの起動または再起動後、Key Manager クライアントからの要求は無視され、Key Manager 管理コンソールにアクセスすると Key Manager 起動ページにリダイレクトされるようになります。クライアントからの要求を処理するには、この起動ページで、管理者が、Key Manager サーバのインストール時に設定したマスター パスワードを入力する必要があります。

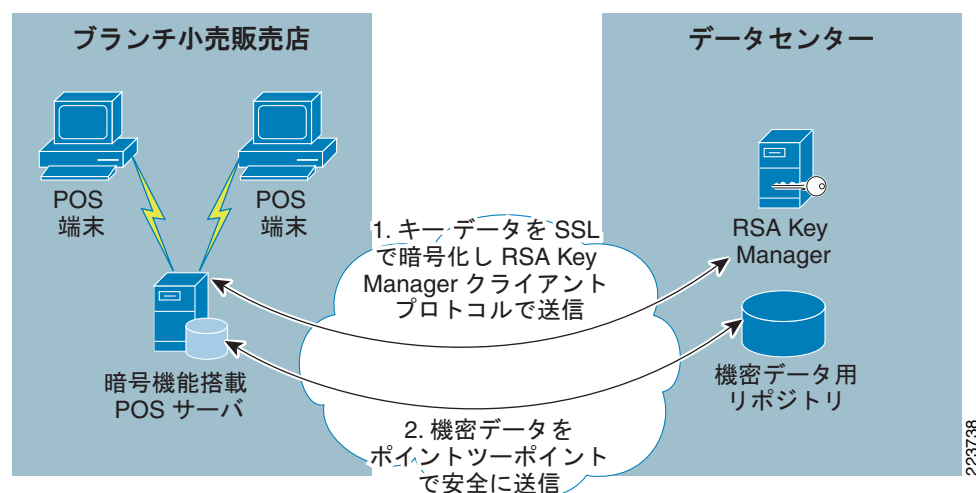
図 D-32 Key Manager 起動ページ

ラボの環境では、Apache Tomcat を使用しました。この Tomcat インスタンスを停止すると、RSA Key Manager サーバは要求の処理を停止します。再起動時には、キー データがパスワードとして自動的に提示されます。Key Manager サーバは、配置したアプリケーション サーバによって停止されます。ここでは、アプリケーション サーバとして Tomcat Apache を使用したため、Key Manager は Tomcat Apache サービスによって停止されます。

RSA Key Manager サーバ/クライアントの配置

一般的なブランチアーキテクチャでは、顧客のクレジットカードデータを送信することも可能ですが、暗号化メカニズムを使用していないと、送信中にカードデータが流出する可能性があります。図 D-33 に典型的な配置シナリオを示します。このシナリオでは、顧客のクレジットカード情報をブランチで処理し、暗号化して、POS サーバに保存しています。この処理では、キーデータを、データセンターに設置されている RSA Key Manager から取得し、そのキーデータを使用してクレジットカードデータを暗号化します。あるいは、セキュアなポイントツーポイント VPN トンネル経由で転送し、データセンターのリポジトリに保存する方法もあります。このモデルでは、静止中 / 移動中の両データのセキュリティ保護を実現できます。

図 D-33 一般的なブランチ構成



このシナリオでは、POS サーバが RSA Key Manager のクライアントになっており、クライアントの機能に基づいてキーを要求し、RSA Key Manager と相互に認証された SSL セッションを確立し、セキュリティ担当者によって指示されたポリシーを設定しています。ラボの環境では、RSA Key Manager のサンプルプログラムを Windows XP PC（RSA Key Manager のクライアントとして動作）にインストールしました。RSA Key Manager からキーを取得するには、RSA Key Manager クライアント PC（Windows XP マシン）上で動作するコマンドラインユーティリティを使用します。このユーティリティは、RSA Key Manager クライアント（サンプルプログラム）のアプリケーションプログラミングインターフェイス（API）を利用したものです。

以下の例では、Windows XP PC 上で動作する RSA Key Manager クライアントのサンプルプログラムからのキーの生成に成功しています。

- 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

キー取得操作のデモ

```

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../-]

```

キー同期操作のデモ

```

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.

```

キー取得に成功

C:\rkm\samples\2.1

RSA Key Manager ロギング

Key Manager サーバは、ランタイム動作をログ ファイルに記録します。このログは監査目的に使用されます。すべてのログ メッセージには、日付と時刻、ログ メッセージが生成されたファイルの完全なクラス名、ログ メッセージのレベル、アプリケーションから取得したコンテキスト情報が含まれます。

ロギング レベル

Key Manager サーバには、次のロギング レベルがあります。

- デバッグ

Key Manager サーバの診断とアプリケーション管理のためのデバッグ メッセージを生成します。

- 情報

次の場合に、情報メッセージを生成します。

- 管理者用アイデンティティによって Key Manager 管理コンソールへのアクセスを開始または終了したとき。管理者のユーザ名がログに記録されます。
- Key Manager サーバがキーを生成したとき。アイデンティティ グループ、キー クラス、キー生成を開始した管理者のユーザ名、キー開始日付、その他のコンテキスト情報がログに記録されます。
- Key Manager サーバがアイデンティティを追加または更新したとき。アイデンティティの名前、アプリケーションを追加または更新した管理者のユーザ名、その他のコンテキスト情報がログに記録されます。
- Key Manager サーバがアイデンティティ グループを追加または更新したとき。アイデンティティ グループの名前、アイデンティティ グループを追加または更新した管理者のユーザ名、その他のコンテキスト情報がログに記録されます。
- Key Manager サーバが新規のセキュリティ クラスまたはキー クラスを追加したとき。クラスの名称、アプリケーションを追加または更新した管理者のユーザ名、その他のコンテキスト情報がログに記録されます。
- Key Manager サーバが新規のクリプト ポリシーを追加したとき。クリプト ポリシーの名称、クリプト ポリシーを追加した管理者のユーザ名、その他のコンテキスト情報がログに記録されます。

- エラー

ランタイム時に Key Manager サーバ内で発生したすべてのエラー 条件を知らせるエラー メッセージを生成します。エラー条件が発生するとシステムが異常状態になり、Key Manager サーバはビジネス プロセスの実行を停止します（たとえば、メモリやディスク スペースなどのシステム リソースにアクセスできなくなります）。

システム管理者がロギング レベルを指定すると、Key Manager サーバは、指定されたロギング レベル以上のログ メッセージを出力します。表 D-1 に、各ロギング レベルで出力されるメッセージの種類を示します。

表 D-2 各ロギング レベルで出力されるメッセージ

	デバッグ メッセージ	情報メッセージ	エラー メッセージ
デバッグ レベル	出力あり	出力あり	出力あり
情報レベル	出力なし	出力なし	出力あり
エラー レベル	出力なし	出力なし	出力あり
すべてのレベル	出力あり	出力あり	出力あり
ロギング オフ	出力なし	出力なし	出力なし

図 D-34 に、ラボ環境での RSA Key Manager のログ出力を示します (C:\Program Files\Apache Software Foundation\Tomcat 5.5\logs)。

図 D-34 RSA Key Manager のログ

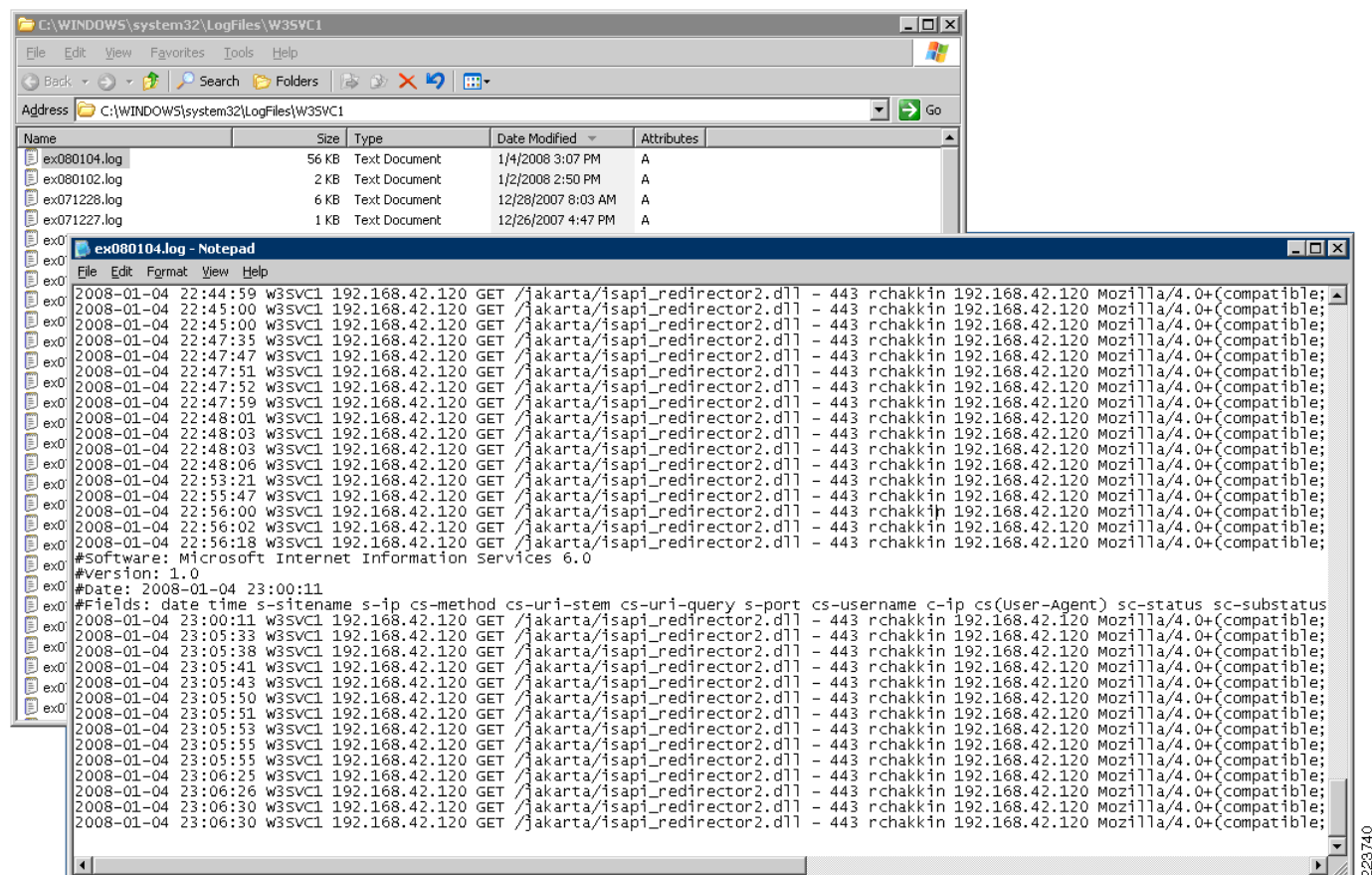
```

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.EdgeFilter.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.EdgeFilter.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.EdgeFilter.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)

```

図 D-35 に RSA Web サーバのログ出力を示します (Microsoft IIS 6.0)。

図 D-35 Web サーバのログ出力



RSA File Security Manager

詳細なシステム アーキテクチャ

図 D-36 に、一般的な店舗アーキテクチャを示します。このアーキテクチャでは、店舗に POS サーバを設置します。この POS サーバが、各店舗でトランザクションログを集約してから、データセンターにある中央のリポジトリに送信します。PCI-DSS 要件に準拠するには、各小売業者が、各 POS サーバおよび中央のリポジトリに格納されたトランザクションログデータのセキュリティを保護する必要があります。

次の例では、“D:\TLOG”ディレクトリ内のファイルにトランザクションログデータを格納し、これらのファイルを、シスコデータセンター内の EMC 製ストレージに接続されたサーバにトランザクションログリポジトリとして複製しています。TLOG リポジトリでは、“X:\TLOG”フォルダ内にファイルを格納します。このサーバのファイルシステムは、大容量のデータ領域と高いパフォーマンスが要求されるため、EMC Symmetrix ベースの SAN 上に存在します。

RSA File Security Manager を使用して支払いシステム上の静止データのセキュリティを保護しない構成では、POS サーバおよび TLOG リポジトリ上に格納されたファイル内の機密データが、社内外のさまざまな脅威にさらされることになります。

図 D-36 POS システムと TLOG リポジトリ (RSA File Security Manager を使用しない場合)

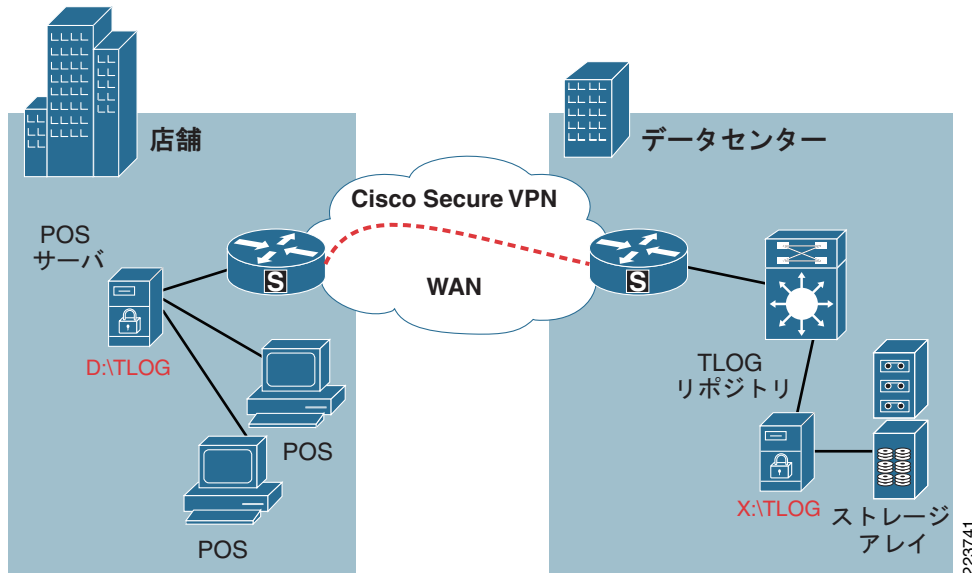
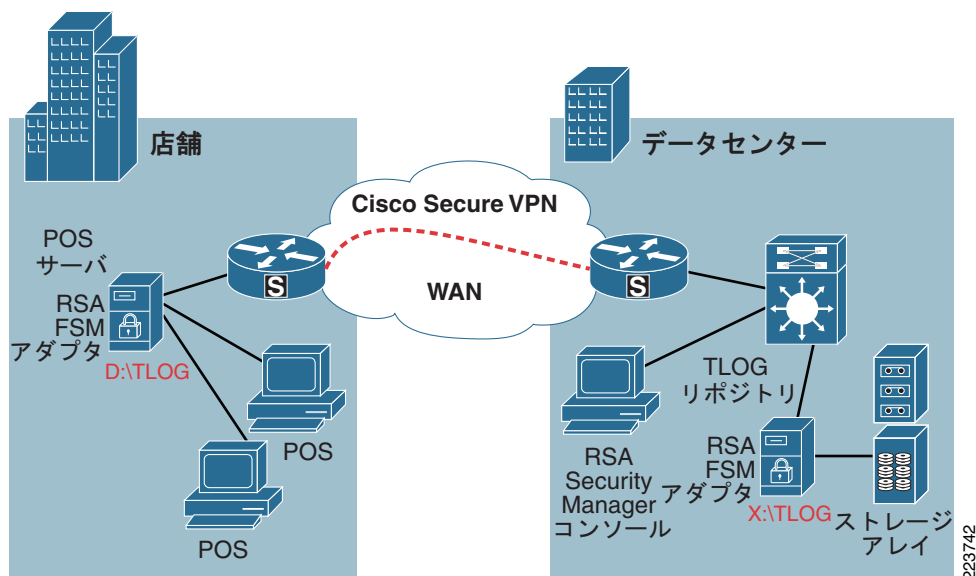


図 D-37 に示した店舗インフラストラクチャは図 D-36 と同じですが、RSA File Security Manager コンポーネントが組み込まれています。RSA File Security Manager は必須ではなく、専用のハードウェアや追加のハードウェアも不要です。

RSA File Security Manager の「ファイル システム アダプタ」は、各 POS サーバと中央の TLOG リポジトリ サーバにインストールします。このシナリオでは、これらのサーバ上で、Windows 2003 Server などの汎用のオペレーティング システムが稼働しています。ファイルセキュリティアダプタは、RSA File Security Manager 管理コンソール (別名「アダプタ マネージャ」) を介して中央のデータセンターから管理されます。

図 D-37 POS システムと TLOG リポジトリ (RSA File Security Manager を使用した場合)



詳細な設定手順



(注) 以下に、重要な設定手順のみを示します。

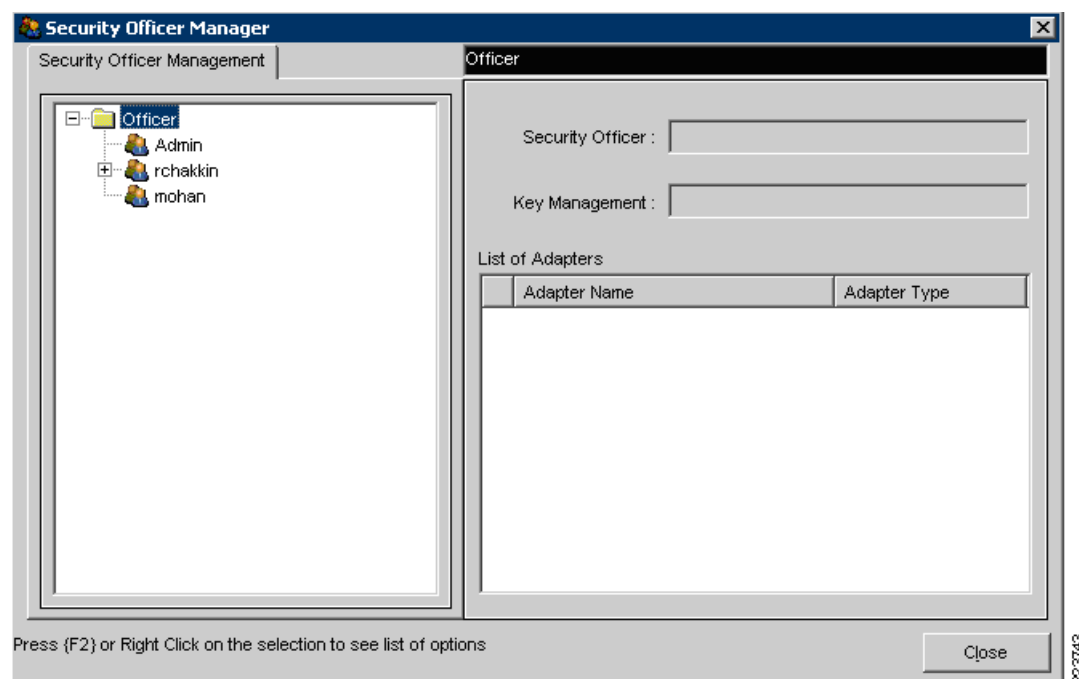
RSA File Security Manager を管理するセキュリティ管理者には、セキュリティ管理者 (SA) とセキュリティ担当者 (SO) の 2 つのタイプがあります。セキュリティ管理者 (SA) は階層の最上位に位置します。SA の義務は、SO のライフサイクルを管理することです。SA は、ファイルセキュリティアダプタによってセキュリティ保護されたサーバやファイル/フォルダの中身を見ることはできません。

SO ロールは、ファイルセキュリティアダプタがインストールされているサーバ/システムのセキュリティポリシーを管理します。SO は、暗号キーや高レベルのファイルシステム構造への参照を見ることができます。ただし、保護されたファイルシステム内の実データを見ることはできません。

RSA File Security Manager は、このセキュリティモデルを実装することで、システム管理、実際の使用、セキュリティ管理の各責任を分担することができます。RSA File Security Manager をサーバインフラストラクチャに組み込めば、エンティティまたはユーザが単独で、故意に、または誤って、システムのセキュリティを損なうことがなくなります。

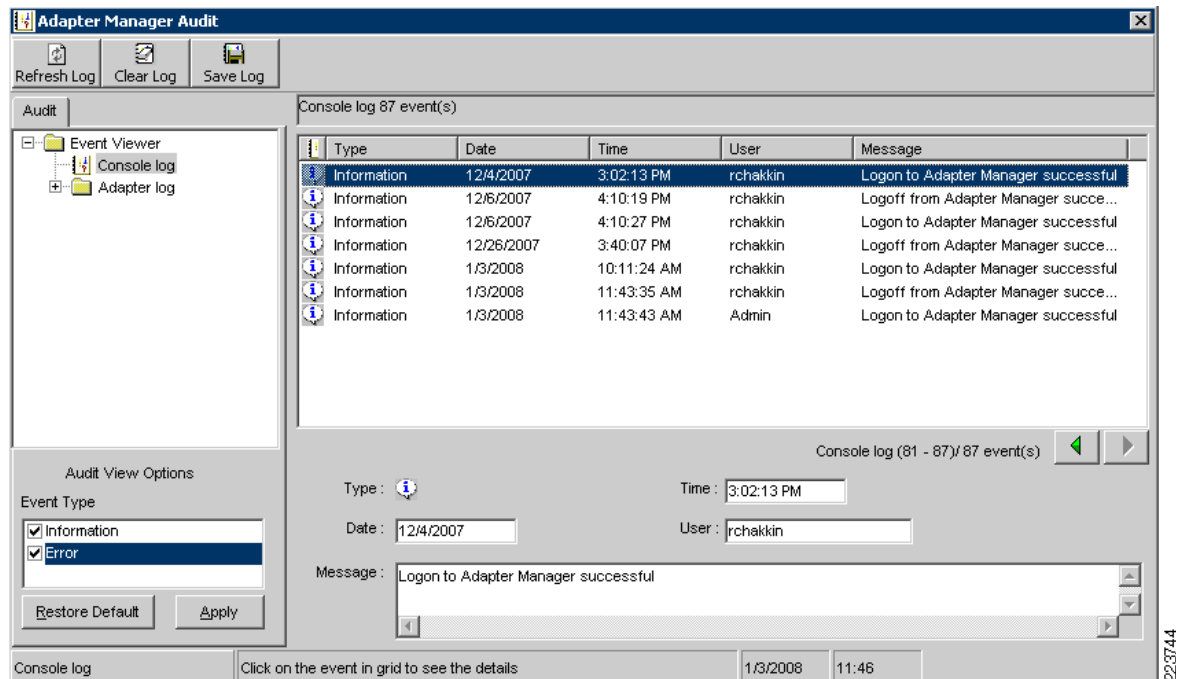
図 D-38 に、SO の管理に必要なワークフローを示します。次の図は、SA が正常にログインしたときに、RSA File Security Manager のグラフィカル管理コンソール上に表示される画面です。

図 D-38 SO 管理画面



セキュリティ管理に関連付けられたイベントとアクション、およびセキュリティ保護されたフォルダに対するアクセスが拒否されないように、RSA File Security Manager は、すべてのイベントとアクションの監査証跡を取り込む必要があります。図 D-39 に、セキュリティ管理者に表示される監査ログを示します。

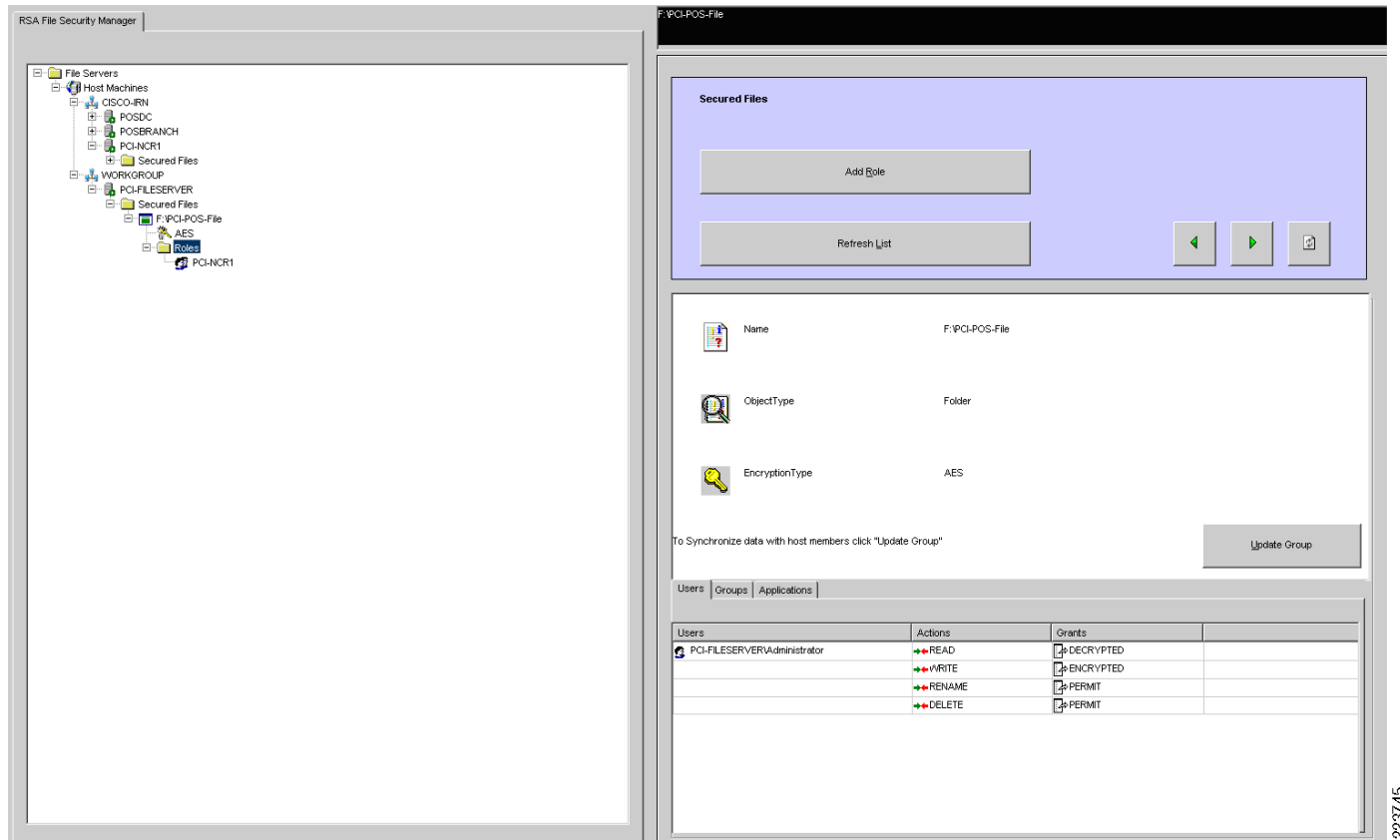
図 D-39 SA による監査ログへのアクセス



22/3744

SO の管理コンソールは、SA の管理コンソールと大きく異なります。図 D-40 に、GUI の例を示します。すべてのセキュリティ管理は、シンプルでグラフィカルなワークフローに従って実行できます。

図 D-40 SO 用 GUI

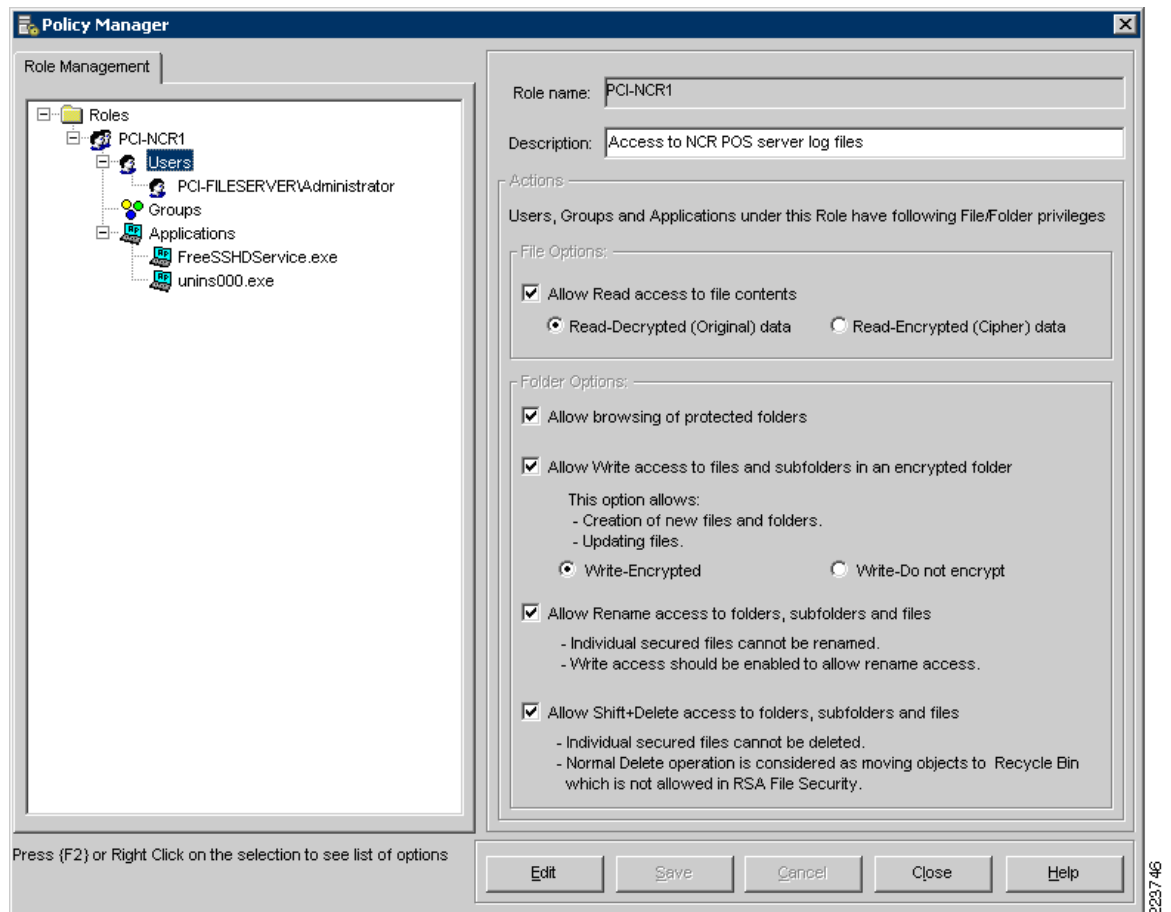


2237/45

RSA File Security Manager は、ロールベースのアクセス制御方式を実装しています。まず、セキュリティ担当者は、ロールを定義し、そのロールに属するアクセスメンバのタイプを指定する必要があります。次に、ロールのメンバを指定します。ロールのメンバには、ローカルまたはドメインユーザおよびフィンガープリント付きアプリケーションを指定できます。

承認済みのユーザおよびアプリケーションの場合は、ファイルセキュリティアダプタのデフォルトのポリシーによって、ファイルデータが、書き込み時に透過的に「暗号化」され、読み取り時に透過的に「復号化」されます。図 D-41 に、ロールの例を示します。

図 D-41 ロール画面の例



PCI 第 6.5 項

PCI 6.5 の要件は、Cisco ACE XML Gateway 製品を使用することによって満たされています。Verizon Business 社により、シスコの ACE XML Gateway を使用して、PCI 第 6.5.1 ～ 6.5.10 項に規定されている Web でよくある脆弱性からの保護を実現できることが確認されました。

Open Web Application Security Project (OWASP)

OWASP Top 10 には、Web アプリケーションのセキュリティに関する情報と注意事項が記載されています。OWASP Top 10 は、Web アプリケーションのセキュリティ上の欠陥のうち最も重大なものに関する共通認識に注目したものです。OWASP Top 10 の第一の目的は、Web アプリケー

ションに、よく知られているセキュリティ上の脆弱性が存在する場合の悪影響を、開発者、デザイナー、アーキテクト、および組織に認識してもらうことです。詳細については、<http://www.owasp.org> を参照してください。

PCI 第 6.5.4 項 クロスサイト スクリプティング (XSS) 攻撃

クロスサイト スクリプティング (XSS) 攻撃は、HTML インジェクション攻撃の一種です。XSS は最も広く蔓延している有害な Web アプリケーションセキュリティ問題です。XSS は、アプリケーションがユーザの入力したデータを受け取り、その内容を検証またはエンコーディングせずにブラウザに送信すると発生します。

XSS を利用すると、攻撃者は、被害者のブラウザ内でスクリプトを実行できます。これにより、ユーザセッションの乗っ取り、Web サイトの体裁の破壊、敵意のあるコンテンツの挿入、フィッシング攻撃の実行、スクリプトで書かれたマルウェアによるユーザブラウザの乗っ取りなどが可能となります。

影響を受ける環境

すべての Web アプリケーション フレームワークは、クロスサイト スクリプティングに対して脆弱です。

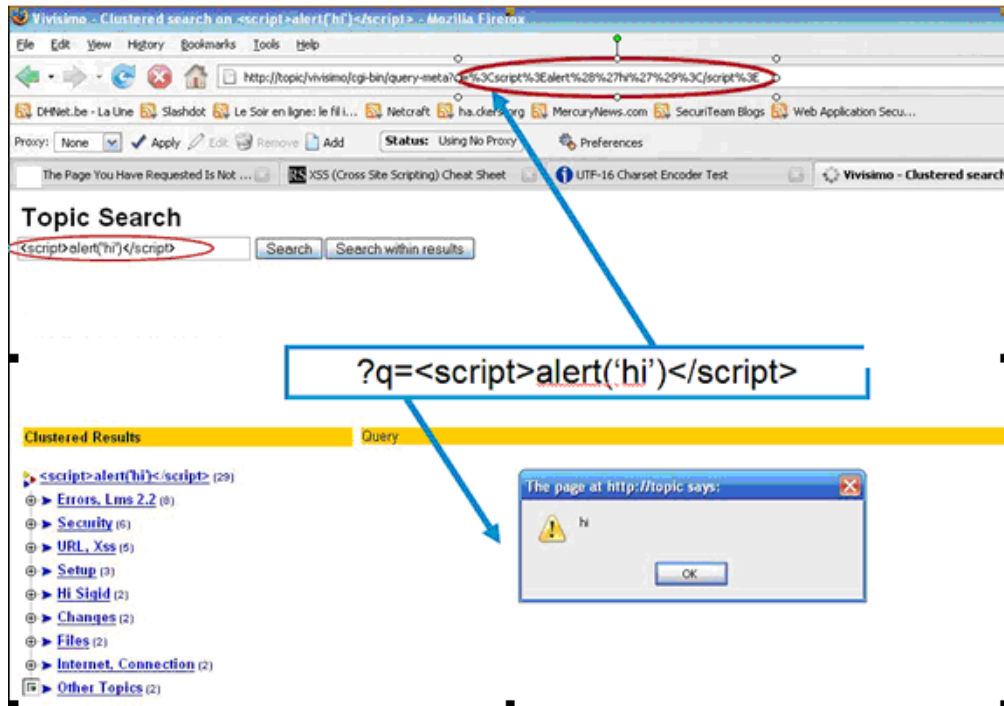
考えられる被害

- Web サイトの体裁の破壊
- セッション ID の不正入手（クッキーをハッカーのサイトにエクスポート）
- ブラウザのセキュリティ脆弱化 — ハッカーにコントロールを奪われる
- クライアントとサーバ間でやりとりされるデータはすべて盗用される可能性がある

Verizon Business 社により、ACE XML Gateway を使用して、XML および HTML ベースの XSS 攻撃から Web アプリケーションを保護する方法が確認されました。たとえば、ACE XML Gateway は、XML/HTML タグの Web サーバへの送信（XSS 攻撃で必要となる）を禁止できます。すべての XSS 攻撃は、手動で行われ、ACE XML Gateway アプリケーションにはカスタムの設定が必要でした。

PCI 用ラボの環境では、悪意のあるスクリプトは、信頼された Web サイトから HTML 形式でエコーバックされます。スクリプトは、クライアント PC 上でローカルに実行されます。

図 D-42 XSS の例



対策

Cisco ACE XML Gateway は、XSS からサイトを保護する方法として、次の 2 つを用意しています。

- ・ ブラック リスト方式 — XSS パターンを検出および認識します。
- ・ ホワイト リスト方式 — AXG を URL/POST クエリー パラメータの正規の値で設定します。
Cisco ACE XML Gateway は、残りの範囲外の値を拒否します。

ラボの環境では、ホワイト リスト方式を使用して、Cisco ACE XML Gateway が XSS 攻撃をブロックする方法を示しました。

Cisco ACE XML Gateway による XSS 攻撃のブロック

以下に、Cisco ACE XML Gateway 内に XSS 攻撃をブロックするための設定を行う手順を示します。

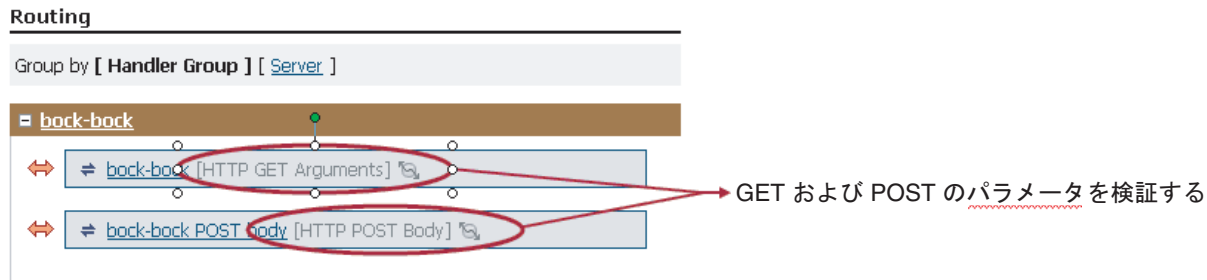
ステップ 1 保護する必要があるホストを決定します。図 D-43 を参照してください。

図 D-43 保護する必要があるホストの決定

Open HTTP(S) Ports					
Add a New Port...					
Name	Port	SSL	Virtual Hosting	Static Content	Flex Path
topic	80	no	Host: topic. .com	-- none --	-
[edit] [remove]					

ステップ 2 各ホストのポリシーを定義します。図 D-44 を参照してください。

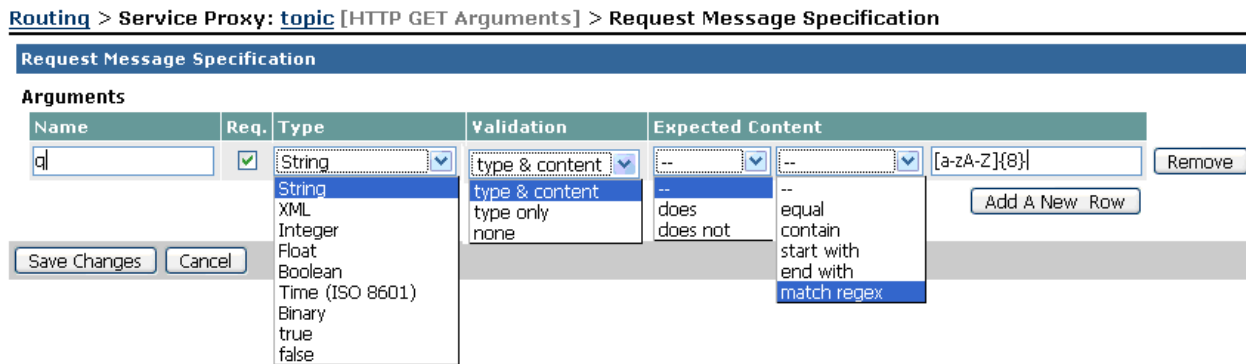
図 D-44 各ホストのポリシーを定義



223749

ステップ 3 各 GET または POST クエリー パラメータについて、受け入れ可能な範囲を決定します。図 D-45 を参照してください。

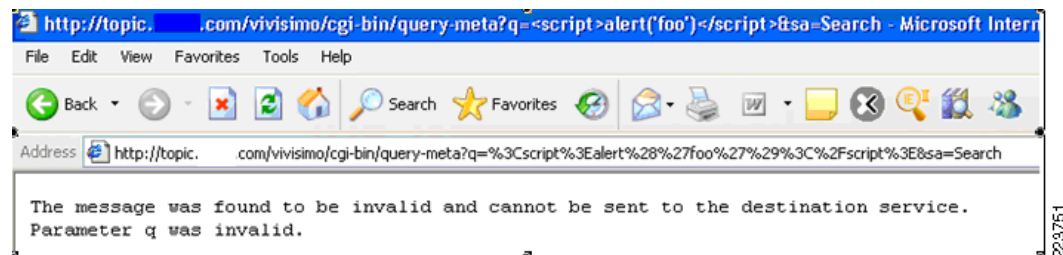
図 D-45 GET および POST のクエリー パラメータを決定



223750

ステップ 4 Cisco ACE XML Gateway は、リクエストを受信すると、メッセージを検証して、期待どおりのフォーマットを持つメッセージだけがバックエンド サーバに到達するようにします。図 D-46 を参照してください。

図 D-46 攻撃の検出とブロック



223751

イベント ログは、Cisco ACE XML Gateway の [Reports and Tools (レポートとツール)] セクションに表示されます (図 D-47 を参照)。

図 D-47 イベント ログ — 無効なメッセージ

The screenshot shows the 'Event Log Viewer' interface. It includes search filters for 'Current Manager Event Logging' and 'Current ACE XML Gateway Event Logging', both set to 'alert, error, warning, notice, info, debug'. Search criteria include 'During: last hour', 'search events logged on: -- all hosts --', 'for events of type: alert, error, warning, notice', and 'Display a maximum of 500 events per page'. The search results are displayed in a table with columns: Time (PST), Description, Message GUID, Host, Component, and Category. The first event is an exception during processing of an HTTP GET request for /vivisimo/cgi-bin/query-meta from 171.69.141.65, with a problem type of 'Invalid message' and a problem message of 'Parameter q was invalid.'.

Time (PST)	Description	Message GUID	Host	Component	Category
Jan 10 2008 01:50:06.994 AM	Exception during processing of message HTTP GET request for /vivisimo/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

要求メッセージの仕様と構成の詳細については、『Cisco ACE XML Gateway Configuration Guide』(v5.1) に記述があります。以下の URL を参照してください。

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 第 6.5.6 項 インジェクション脆弱性

インジェクション脆弱性、とりわけ structured query language (SQL; 構造化照会言語) インジェクション脆弱性は、Web アプリケーションで頻繁に検出されています。インジェクションには、SQL、LDAP、Xpath、HTML、XML などのタイプがあります。インジェクションは、ユーザの入力したデータがコマンドやクエリーの一部としてインタープリタに渡されると発生します。攻撃者は、巧妙に加工されたデータを与えて、想定していないコマンドをインタープリタに実行させます。インジェクション脆弱性を利用すると、アプリケーションが利用可能な任意のデータについて、作成、読み取り、更新、削除を実行できます。最悪のケースでは、アプリケーションや下層のシステムが完全に破壊される可能性もあります。

影響を受ける環境

インタープリタを使用しているか、その他のプロセスを呼び出しているすべての Web アプリケーションフレームワークには、インジェクション攻撃に対する脆弱性があります。PCI ラボの環境では、攻撃者が一重引用符をアプリケーション内に注入しています (図 D-48 を参照)。これにより、ユーザが入力したデータは、アプリケーションコードによって、コマンドやクエリーまたはデータとして解釈されます。アプリケーションのエラーメッセージからデータベースの構造が漏れてしまいます (図 D-48 を参照)。

図 D-48 インジェクション脆弱性の例

223753

図 D-49 アプリケーションのエラー メッセージ

```
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(mp.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]
```

Database Error.

223754

Verizon Business 社により、ACE XML Gateway を使用して、XML および HTML ベースの SQL インジェクション攻撃から Web アプリケーションを保護する方法が確認されました。SQL インジェクション攻撃に必要な文字や文字列を制限するなど、個々の条件の入力を制限することで、こうした攻撃を防ぐ方法が実証されました。すべての SQL インジェクション攻撃は、手動で行われ、ACE XML Gateway アプリケーションにはカスタムの設定が必要でした。

Cisco ACE XML Gateway の設定 (v5.1) の詳細については、以下の URL を参照してください。

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 第 6.5.7 項 不適切なエラー処理

アプリケーションは、さまざまなアプリケーションの欠陥により、意図せずして、設定や内部動作に関する情報を外部に漏らしたり、個人情報の保護に違反したりする可能性があります (図 D-50 を参照)。また、特定の処理に要する時間や、入力を変えたときの応答の変化 (たとえば、エラー番号は異なるのに同じエラーテキストが表示される) などによって、アプリケーションの内部状態が漏れる可能性があります。Web アプリケーションでは、詳細なエラーメッセージまたはデバッグ用のエラーメッセージによって内部状態に関する情報が漏れることがよくあります。多くの場合、こうした情報を利用して、さらに強力な攻撃を起動する、あるいは自動的に実行することができます。

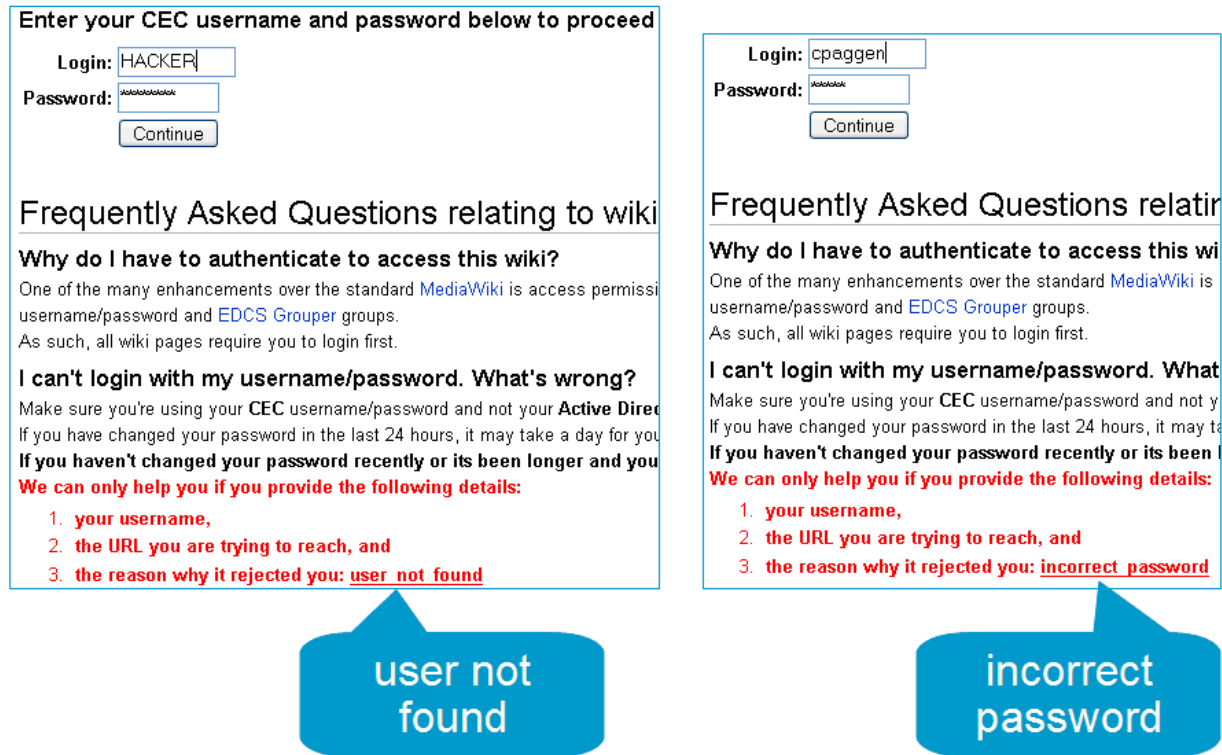
影響を受ける環境

すべての Web アプリケーション フレームワークは、情報の漏洩や不適切なエラー処理を利用した攻撃に対して脆弱です。

考えられる被害

- ・ ハッカーに攻撃を可能にするような有益な情報を提供する
- ・ 内部情報が流出する

図 D-50 不適切な処理の例



対策

ラボの環境では、Verizon Business 社によって、ACE XML Gateway を使用して、XML および HTML ベースのエラー処理脆弱性から Web アプリケーションを保護する方法が確認されました。Web サーバから出力される HTML/XML エラーを Cisco ACE XML Gateway で解釈して、一般的かつ非説明的なエラー メッセージで書き換えることができます。この方法はレビューで実証されました。すべてのエラー処理脆弱性に対する攻撃は、手動で行われ、ACE XML Gateway アプリケーションには不適切なエラー処理を防ぐためのカスタムの設定が必要でした。

AXG では、標準の HTTP 戻りコードの代わりにカスタマイズされたメッセージまたはページを返すことができます (図 D-51 を参照)。

図 D-51 メッセージ設定のカスタマイズ

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

不適切なエラー処理については、AXG は、要求および応答メッセージに対して完全な正規表現による検索と置換を行うことができます。図 D-52 は、応答メッセージを新しい文字列で置き換える方法を示しています。

図 D-52 不適切なエラー処理要求

Address  http://i...com/vivisimo/cgi-bin/query-meta?q=chakkingal&searchmode=basic

Topic Search

chakkingal Search Search within results

コンテンツ スクリーニング ルールは、発信または着信メッセージに対してマッチングするコンテンツを定義する正規表現です。カスタムのコンテンツ スクリーニング ルールには、ナビゲーション メニューのポリシー部分からアクセスできます (図 D-53 を参照)。

図 D-53 カスタムのコンテンツ スクリーニング ルール

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

223759

ここでは、応答メッセージ内の「Topic Search」という文字列を「General Query」という文字列で置換しています (図 D-54 を参照)。

図 D-54 不適切なエラー処理応答

Address http://.../vivisimo/cgi-bin/query-meta?q=chakkingal&btnG=Search&searchmode=basic&searchmode=basic

General Query

223759

「Topic Search」という文字列を「General Query」という文字列で置換することによって生成されるイベントログを [図 D-55](#) に示します。この置換操作は、カスタム コンテンツ スクリーニング ルールに「searchreplace」として設定されています。

図 D-55 イベントログの検索と置換

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 Regex '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, .introrum, .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

PCI 第 6.5 項

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 45ABED2D00000FAF633E0534753388F9J45ABED2D00000583EC4EEE04952E

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 Regex '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, .intrinum, .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

カスタム コンテンツ スクリーニング ルールの設定の詳細については、『Cisco ACE XML Gateway Configuration Guide』(v5.1) に記述があります。以下の URL を参照してください。

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

PCI 第 6.5.9 項 サービス拒否

サービス拒否攻撃 (DoS 攻撃) とは、(悪意のある要求などを発行して) コンピュータのリソースを大量に消費させ、正規のユーザがリソースを利用できなくする攻撃のことです。DoS 攻撃の犯人は通常、銀行、クレジットカード支払いゲートウェイ、さらには DNS ルートサーバといった注目度の高い Web サーバ上でホスティングされているサイトやサービスを標的にします。

影響を受ける環境

すべての Web アプリケーション フレームワークは、情報の漏洩や不適切なエラー処理によって攻撃に対して脆弱です。

考えられる被害

- ・ サービスの中断
- ・ ダウンタイム
- ・ ブランドイメージの損傷
- ・ 収益の低下

対策

ラボの環境では、Verizon Business 社によって、Cisco ACE XML Gateway を使用して、Web ベースの DoS 攻撃から Web アプリケーションを保護する方法が確認されました。セッションに制限 (たとえば、セッションタイムアウト、同時セッション数など) を課すことで、DoS 攻撃を受ける可能性を軽減できます。AXG では、[Global Security] で DoS 攻撃からの保護を、HTTP サーバでリクエスト スロットリングを設定できます (図 D-56 と 図 D-57 を参照)。

図 D-56 サービス拒否攻撃からの保護

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

図 D-57 リクエスト スロットリング

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

DoS 攻撃からの保護の詳細については、『*ACE XML Configuration Guide*』(v5.1) の「Working with HTTP Servers」の章を参照してください。このガイドは次の URL で公開されています。

http://www.cisco.com/en/US/products/ps7314/products_installation_and_configuration_guides_list.html

6.5.10 セキュリティ保護されていない構成管理

機密性の高い通信を保護するためにネットワーク トラフィックの暗号化必要な場合でも、暗号化を行っていないアプリケーションが多く存在します。インターネット上でアクセス可能な Web ページだけでなく、バックエンドの接続も含めた、すべての認証された接続には暗号化（通常は SSL）を使用する必要があります。暗号化を行わないと、アプリケーションは、認証またはセッション用のトークンを公開してしまうことになります。また、クレジットカード情報など、機密性の高いデータの送信にも常に暗号化を使用する必要があります。

影響を受ける環境

すべての Web アプリケーション フレームワークは、情報の漏洩や不適切なエラー処理によって攻撃に対して脆弱です。

考えられる被害

- 盗聴

- データ操作
- 支払い拒絶不能

対策

ラボの環境では、Verizon Business 社によって、Cisco ACE XML Gateway を使用して、次のセキュリティ保護されていない構成管理エリアから Web アプリケーションを保護する方法が確認されました。

必須 SSL (HTTPS) Web セッション：ACE XML Gateway は、HTTPS セッションを強制し、機密情報を含む可能性のある HTTP セッションを禁止させるように設定できます。図 D-58 に、SSL 設定のスナップショットを示します。

図 D-58 SSL の設定

HTTP Servers > HacmeBank: Edit General Settings

GENERAL

Name: ECOM.cisco-irm.com

Host: ECOM.cisco-irm.com

Port: 443 (usually 80 for HTTP, or 443 for HTTPS)

SSL: ☒ Encrypt connections with SSL

If requested, use client public/private keypair: -- none --

☒ Require remote server certificate signed by this CA certificate: -- none --
(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: -- none --

SSL Cipher Suite: -- default --

Flex Path: ☐ Always Use Flex Path

図 D-59 に、SSL ポート設定のスナップショットを示します。

図 D-59 SSL ポート設定

Open HTTP(S) Ports > Edit Port

Name: Secure Server configuration

Port Number: 443

SSL: ☒ Use SSL encryption on this port

Public/Private Keypair: No public/private keypairs have been uploaded.

SSL Cipher Suite: -- default --

Listen For: requests to a hostname

Hostname: ECOM.cisco-irm.com

☐ Allow regular expression matching in the hostname

Static Content: do not serve static content on this port

Flex Path: ☐ Always Use Flex Path

PCI 第 6.5.5 項 バッファ オーバーフロー

攻撃者は、バッファ オーバーフローを利用して、Web アプリケーションの実行スタックを破壊することができます。巧妙に加工された入力を Web アプリケーションに送りつけて、任意のコードを実行させ、事実上マシンを乗っ取ることができます。攻撃者は、膨大な数の製品やコンピュータにバッファ オーバーフロー脆弱性が存在することを特定しています。バッファ オーバーフロー脆弱性は、サイトの静的および動的な処理を行う Web サーバやアプリケーションサーバ製品、あるいは Web アプリケーション自体に存在する可能性があります。広く普及しているサーバ製品にバッファ オーバーフロー脆弱性が見つかり、その事実が広く知られるようになり、そうした製品のユーザに重大なリスクをもたらす可能性があります。画像生成用のグラフィック ライブラリなど、ライブラリを使用している Web アプリケーションは、バッファ オーバーフロー攻撃に対して無防備です。

影響を受ける環境

すべての Web サーバ、アプリケーション サーバ、Web アプリケーションは、バッファ オーバーフロー攻撃に対して脆弱です。

考えられる被害

- ・ オペレーティング システムへのアクセス
- ・ ファイルやパスワードの盗難
- ・ オペレーティング システム内でのウイルスやワームの伝染

ラボの環境では、Verizon Business 社によって、Cisco ACE XML Gateway を使用して、XML および HTML ベースのバッファ オーバーフロー攻撃から Web アプリケーションを保護する方法が確認されました。URI 処理（URI 送信の制限など）やフィールド入力値の検証などによって、こうした攻撃を防げることが確認されました。すべてのバッファ オーバーフロー攻撃は手動で行われ、Cisco ACE XML Gateway アプリケーションにはカスタムの設定が必要でした。図 D-60 は、パラメータ長を制限することでバッファ オーバーフローを防いでいる例です。

図 D-60 バッファ オーバーフロー パラメータ長の制限

Routing > Service Proxy: topic [HTTP GET Arguments] > Request Message Specification

Request Message Specification

Name	Req.	Type	Validation	Expected Content
q1	☒	String	type & content	--
		XML	type & content	--
		Integer	type only	does
		Float	none	does not
		Boolean		equal
		Time (ISO 8601)		contain
		Binary		start with
		true		end with
		false		match regex

Maximum 8 occurrences

PCI 第 6.5.1 項 未検証の入力

Web アプリケーションは、HTTP リクエスト（またはファイル）からの入力に基づいて、応答方法を決定します。攻撃者は、HTTP リクエスト（URL、クエリー文字列、ヘッダー、クッキー、フォーム フィールド、非表示フィールドなど）の一部を改ざんして、サイトのセキュリティ保護メカニズムを迂回しようとします。よくある入力改ざん攻撃として、強制ブラウジング、コマンドインジェクション、クロスサイトスクリプティング、バッファ オーバーフロー、フォーマット文字列攻撃、SQL インジェクション、クッキー ポイズニング、表示フィールド操作などがあります。膨大な数の Web アプリケーションが、クライアント側だけで入力の検証を行っています。クライアント側の入力検証は簡単に迂回できるため、Web アプリケーションは、悪意のあるパラメータに対して無防備な状態になります。攻撃者は、Telnet などの簡単なツールを使用し

て、自前の HTTP リクエストを生成できます。パラメータ操作攻撃に対抗するには、サーバ側でのチェックが必須です。こうした対策を施した上でなら、正規ユーザのユーザ エクスペリエンスが向上し、サーバに送信される未検証のトラフィックの量が軽減されるという点で、クライアント側での入力チェックも有効な手段となります。

影響を受ける環境

すべての Web サーバ、アプリケーション サーバ、Web アプリケーションは、パラメータ改ざん攻撃に対して脆弱です。

ラボの環境では、Verizon Business 社によって、Cisco ACE XML Gateway を使用して、XML および HTML ベースの入力検証攻撃から Web アプリケーションを保護する方法が確認されました。すべての入力検証攻撃は、手動で行われ、ACE XML Gateway アプリケーションにはカスタムの設定が必要でした。

未検証入力の例については、クロスサイト スクリプティング (PCI 第 6.5.4 項)、バッファ オーバーフロー (PCI 第 6.5.5 項)、インジェクション脆弱性 (PCI 第 6.5.6 項) の例を参照してください。



APPENDIX **E**

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
```

PCI Solution for Retail Design and Implementation Guide

```

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 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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
```

PCI Solution for Retail Design and Implementation Guide

```

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 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

```

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
    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
!

```

```

!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-3152768543
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3152768543
  revocation-check none
  rsakeypair TP-self-signed-3152768543
!
crypto pki trustpoint IDSMDC_CSMANAGER
  enrollment url tftp://192.168.42.133/IDSMDC_CSMANAGER
  revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-3152768543
certificate self-signed 01
  30820251 308201BA A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33313532 37363835 3433301E 170D3036 31303137 32333336
  33305A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31353237
  36383534 3330819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100F26B 0F3A8F1A 81236BAE BF0BF7D6 6BC81158 30FF7143 0D5E2A1F 8C5672A1
  2A2E59FC 68120573 C018079D 5CA9A874 C9DF93DD AF6C3494 D5393F73 643F0E0F
  A778CF19 3823DEB2 A06BBCC5 E42DC606 235003C3 CA5135BC 90A34E7D EE16B116
  D504B437 73EB46E8 97BADE2A 0F54D564 03540644 9E3B5A2F 21A6509A 85965A58
  BA7B0203 010001A3 79307730 0F060355 1D130101 FF040530 030101FF 30240603
  551D1104 1D301B82 19524D45 442D312E 52455441 494C5043 494C4142 2E4C4F43
  414C301F 0603551D 23041830 16801401 5366E2FF A2A35080 84F65E4D E0B5925E
  5D5AE130 1D060355 1D0E0416 04140153 66E2FFA2 A3508084 F65E4DE0 B5925E5D
  5AE1300D 06092A86 4886F70D 01010405 00038181 0032411D 3470B6AE D314B70E
  D00137E5 D5BA0261 3D36766D A2B7AA01 99006259 E1E26B8D 25B36E18 6DCE7D9E
  07924127 F618E2A9 F170494D 1B50A1A9 0C54EB06 64B0BF58 97BF3EB3 AAF1005E
  4E0FB668 5310A1C7 0A797201 6E8A06C5 8B7F9B8C F95DB0DC 3A18E38B 65C6486C
  51B6C791 284F2C68 9A6D5EB0 B14CD9CD 076F7236 A7
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
    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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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

PCI Solution for Retail Design and Implementation Guide

```

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 Tunnel1
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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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
!
!
!
!
!
!
!
!
!
!
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 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+
!
```

PCI Solution for Retail Design and Implementation Guide


```

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 FFBEE477 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
 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
 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

```



```

permit udp 10.10.23.0 0.0.0.255 host 192.168.42.112 eq 12222 12223 log
permit icmp 10.10.23.0 0.0.0.255 host 192.168.42.113 log
permit udp 10.10.23.0 0.0.0.255 host 192.168.42.113 eq 12222 12223 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 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 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

E-66

```

!
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
    D10CAAE8 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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/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 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 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
```

PCI Solution for Retail Design and Implementation Guide

```
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 packet-size 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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/ww1/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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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/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 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 CE68C355 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 yenanah
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 packet-size 8192
snmp-server location XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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 yenhnh
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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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
  RLDLP 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 Airewave 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
Recommendd 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

```

PCI Solution for Retail Design and Implementation Guide

```
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
FURTHER NOTICE OR CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER
CRIMINAL CONDUCT REVEALED BY SUCH USE IS SUBJECT TO DISCLOSURE TO LAW S
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 ^CCC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS 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 (fcl)
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 (fcl)
BOOTLDR: S72033_rp Software (S72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF10a,
RELEASE SOFTWARE (fcl)

```

```

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>
!

```

PCI Solution for Retail Design and Implementation Guide

```
vlan 83
  name ace_inside
!
vlan 85
  name ft_ace
!
vlan 86
!
vlan 87
  name To_Internet_edge_router
!
vlan 91
  name fwsf_failover
!
vlan 92
  name fwsf_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-FWSF-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 yenhnh
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-ip-services_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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
snmp-server contact XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
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/wwl/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 $1$qM8m$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 dls
snmp-server enable traps dial
snmp-server enable traps voice poor-qov
!
!
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 7yuj1JlcXnFviy7G 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 Verizon Business, 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 Verizon Business document. It is only provided as a reference. Verizon Business is solely responsible for the following content.

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
 - o 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.
 - o Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
 - o Cisco switches – (4 – 2 layer 3 switches (Catalyst 4506), 2 layer 2 access switches (Catalyst 3750))
 - o Wireless controllers – (1): Used to monitor and update wireless APs.
 - o Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - o NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - o Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - o Intermec POS: Wireless POS handheld.
 - o 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.
 - o 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
 - o Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
 - o Cisco 3845 Integrated Services Router (ISR) – (2): ISRs are configured with Firewall and IDS/IPS feature set.
 - o Cisco 3560 layer 2 switches – (2)
 - o Wireless APs – (1) : Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - o NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - o Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - o Intermec POS: Wireless POS handheld.
 - o 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.
 - o 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
 - o Cisco Security Agent (CSA) software used for HIDS, host-based firewall, malware/spyware protection, behavioral anti-virus protection, file monitoring / access control (file integrity)
 - o Cisco 2821 Integrated Services Router (ISR) – (1) – ISR is configured with Firewall and IDS/IPS feature set.
 - o Wireless APs – (1): Used for wireless POS networks. Wireless APs have been configured with WPA-TKIP security enabled,
 - o NCR Advanced Checkout Solution (ACS) software: Payment Application Best Practice (PABP) certified POS software.
 - o Verifone POS devices: MX/Vx Series (Wired and wireless POS devices). Verifone POS devices have been PCI PED (Pin Entry Device) certified.
 - o Intermec POS: Wireless POS handheld.
 - o 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.

- o 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
 - o Cisco Wireless Control System (WCS): Central platform for wireless configuration, management, and monitoring.
 - o 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.
 - o CiscoWorks LAN Management Solution (LMS): Network device configuration management (e.g. routing and switching)
 - o 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.
 - o 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).
 - o 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)
 - o Cisco Secure Access Control Server (ACS) – AAA server
 - o 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.
 - o Cisco Adaptive Security Device Manager (ASDM): Secure, web-based configuration management of ASA firewalls.
 - o Cisco IPS Device Manager (IDM): IDS/IPS configuration management.
 - o Cisco Security Device Manager (SDM): Secure, web-based configuration management of 7206VXR routers.
 - o Cisco 7206 VXR router (2 at Internet Edge, 2 at WAN aggregation): Access lists, routing, IPsec VPN termination.
 - o Cisco Catalyst 3750 switch (6 – 2 Internet Edge, 4 WAN aggregation): Layer 3 switch (routing and access lists).
 - o 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)
 - o Cisco Catalyst 4948 Switch (2): Layer 2 access switch.

- o Cisco Adaptive Security Appliance (ASA) 5540 (2): Stateful firewall filtering and integrated IDS/IPS @ data center boundary.
- o 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.
- o 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.
- o RSA Access Manager: Used for central authentication/logging for access to RSA Key Manager within the assessed environment.
- o RSA Authentication Manager: Central management/logging of RSA SecurID (two-factor) authentication for remote access into the data center environment.
- o 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 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 McGlothlin, 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 McGlothlin, 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 McGlothlin	Network architecture, firewalls, routers, switches, wireless, IDS/IPS	12/04/06
Christian Janoff, Bart McGlothlin	Audit Logging	12/04/06
Christian Janoff, Bart McGlothlin	Access Control / Authentication	12/04/06
Christian Janoff, Bart McGlothlin	CSA	12/04/06
Christian Janoff, Bart McGlothlin	MARS	12/04/06
Christian Janoff, Bart McGlothlin	CSM	12/04/06
Christian Janoff, Bart McGlothlin	Wireless	12/04/06
Christian Janoff, Bart McGlothlin	CiscoWorks (LMS)	12/06/06
Christian Janoff, Bart McGlothlin, Eric	MARS	12/13/06
Christian Janoff, Bart McGlothlin	Remediation items	12/20/06
Christian Janoff, Bart McGlothlin, Paul Jones	Assessment Results – Messaging	12/21/06
Christian Janoff, Bart McGlothlin, Christina Hausman, Josh Huston	CSA validation	12/22/06
Christian Janoff, Bart McGlothlin	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	▪ Cisco Integrated Services Router (FWSM Firewall), Cisco ASA	▪ 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	▪ 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)	▪ 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.
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	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.	N/A – Firewall/Router configuration standards (documentation)		Responsibility of merchant / service provider to document in configuration standards.
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	1.1.4 Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components.	N/A – Firewall/Router configuration standards (documentation) 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).		Responsibility of merchant / service provider to document in configuration standards.
1.1.5 Documented list of services and ports necessary for business	1.1.5 Verify that firewall configuration standards include a documented list of services/ports necessary for business	N/A – Firewall/Router configuration standards (documentation) 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.		Responsibility of merchant / service provider to document in configuration standards.

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
				standards. 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.
1.2 Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.	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	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.		Configurations for perimeter firewalls/routers outside the PCI Solution for Retail environment are the responsibility of merchant / service provider.
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:	1.3 Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:			

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.		
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.	2.1.1 Verify the following regarding vendor default settings for wireless environments: - 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	Verizon Business reviewed wireless settings within the PCI Solution for Retail environment and verified the following: - 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
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).	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	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards). 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. 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. 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.		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
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4)	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards). 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.		Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.
	2.2.c Verify that system configuration standards are applied when new systems are configured	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards). 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.		Documentation and implementation of system configuration standards is the responsibility of the merchant / service provider.
2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	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	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards). 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.		Note: Logical system partitioning (e.g. lpars (IBM mainframe), VMware servers) is an acceptable means to separate server functions within a single server platform.
2.2.2 Disable all	2.2.2 For a sample of system	Verizon Business reviewed		Host OS hardening for

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)	configurations for ASA/FWSM firewalls, ISR routers, switches, and wireless devices and found insecure services and protocols to be disabled. 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.		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	N/A – System configuration standards (e.g. Firewall/Router standards, server standards, wireless standards). Note: Verizon Business reviewed configurations across ASA/FWSM firewalls, ISR routers, switches, and		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
		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.		
	2.2.3.c For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately	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.		Server hardening, including appropriate security settings for all system components, is the responsibility of the merchant / service provider.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file	2.2.4 For a sample of system components, critical servers, and wireless access points, verify that all unnecessary functionality (for	Verizon Business reviewed configurations across all ASA/FWSM firewalls, ISR routers, switches, and wireless devices and confirmed they were based on best practice		Server hardening, including appropriate security settings for all system components, is the responsibility of the

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.
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.	2.3 For a sample of system components, critical servers, and wireless access points, verify that non-console administrative access is encrypted by: - 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)	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: - 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		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.

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
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.	3.1 Obtain and examine the company policies and procedures for data retention and disposal, and perform the following • 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	N/A – Data retention / Data disposal policy and procedures.		Data retention / Data disposal policies and procedures are the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	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			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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:	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:	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.		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.
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>	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: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents	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: • 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		See 3.2 above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
card verification code or value or PIN verification value data elements. <i>Note: See "Glossary" for additional information.</i>		transaction file)		
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 <i>Note: See "Glossary" for additional information.</i>	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: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents	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: • 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)		See 3.2 above
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	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: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents	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: • 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		See 3.2 above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		transaction file)		
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>	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	Verizon Business reviewed NCR's ACS application and confirmed that only masked data is accessible through the application, even for administrators.		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.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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. <i>If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls."</i>	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: - 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	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: 128-bit 3DES encryption - Truncation 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: - 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.		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: - 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
	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)	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

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
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:	3.5 Verify processes to protect encryption keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to keys to the fewest number of custodians necessary	3.5.1 Examine user access lists to verify that access to cryptographic keys is restricted to very few custodians	Verizon Business confirmed that restricted access to encryption keys is as follows: - 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.		Protection of encryption keys is the responsibility of the merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
3.5.2 Store keys securely in the fewest possible locations and forms	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	Verizon Business reviewed protection/storage for encryption keys and confirmed the following: - 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.		See 3.5.1 above
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:	3.6.a Verify the existence of key management procedures for keys used for encryption of cardholder data	N/A – Key Management policy and procedures		Key Management policies and procedures is the responsibility of the merchant / service provider.
	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)	N/A – Key Management policy and procedures		See 3.6.a above
	3.6.c Examine the key management procedures and perform the following:			

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
3.6.3 Secure key storage	3.6.3 Verify that key management procedures require secure key storage	Verizon Business confirmed that secure key storage is included for the following: - 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.		See 3.6.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
3.6.4 Periodic key changes - As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically - At least annually	3.6.4 Verify that key management procedures require periodic key changes. Verify that key change procedures are carried out at least annually	Verizon Business confirmed that key rotation capabilities are included for the following: - 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).		See 3.6.a above 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 DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
3.6.5 Destruction of old keys.	3.6.5 Verify that key management procedures require the destruction of old keys	Verizon Business confirmed that destruction of keys is included for the following: - 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).		See 3.6.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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)	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)	Verizon Business confirmed that split knowledge/dual control of keys is included for the following: - 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.		See 3.6.a above
3.6.7 Prevention of unauthorized substitution of keys	3.6.7 Verify that key management procedures require the prevention of unauthorized substitution of keys	Verizon Business confirmed that prevention of unauthorized substitution of keys is included for the following: - NCR ACS: Encryption keys are generated using the "Interactive Key Maintenance" tool. Only		See 3.6.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		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. - 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). - 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.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		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.		
3.6.8 Replacement of known or suspected compromised keys	3.6.8 Verify that key management procedures require the replacement of known or suspected compromised keys	Verizon Business confirmed that replacement of known or suspected compromised keys is included for the following: - 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).		See 3.6.a above
3.6.9 Revocation of old or invalid keys	3.6.9 Verify that key management procedures require the revocation of old or invalid keys (mainly for RSA keys)	N/A – Public keys are not used for data encryption, within the PCI Solution for Retail environment.		See 3.6.a above

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
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. <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>	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 • 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)	4.1.a Verizon Business reviewed the following configurations to confirm that secure transmission of cardholder data would be accomplished: - 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. Note: Wireless networks have been configured to provide PCI required security necessary to support cardholder traffic.		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. If cardholder data does not traverse the wireless network, wireless networks would be out of scope for requirement 4.1.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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	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	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.		
	4.1.1.b If WEP is used, verify • 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	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.		
4.2 Never send unencrypted PANs by e-mail.	4.2.a Verify that an email encryption solution is used whenever cardholder data is sent via email	N/A – Data Control / Encryption policy and procedures		Responsibility of merchant / service provider.
	4.2.b Verify the existence of a policy stating that unencrypted PAN is not to be sent via email	N/A – Data Control / Encryption policy and procedures		Responsibility of merchant / service provider.

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

5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) <i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i>	5.1 For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed	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: • 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 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). 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).		Note: CSA can be configured to protect against the following virus and malware threats: • 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) 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.

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.	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	See 5.1 above		See 5.1 above
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	5.2 Verify that anti-virus software is current, actively running, and capable of generating logs • 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	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): - 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. 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.		Note: (First bullet item for 5.2) - AV policy and procedure documentation is the responsibility of the merchant / service provider. 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.

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.
6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.	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 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:	N/A – SDLC policy/procedures		SDLC processes are the responsibility of the merchant / service provider.
6.3.1 Testing of all security patches and system and software configuration changes before deployment	6.3.1 All changes (including patches) are tested before being deployed into production	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
				provider.
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:	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)	N/A – Web-based application development (secure coding) not in scope for assessment		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. 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

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
		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.		
6.5.7 Improper error handling	6.5.7 Error handling flaws	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.		See 6.5.a above
6.5.8 Insecure storage	6.5.8 Insecure storage			See 6.5.a above 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.
6.5.9 Denial of service	6.5.9 Denial of service	Verizon Business observed the use of ACE XML Gateway to protect web		See 6.5.a above

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		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.		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.
6.5.10 Insecure configuration management	6.5.10 Insecure configuration management	Verizon Business observed the use of 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.		See 6.5.a above 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.
6.6 Ensure that all web-facing applications are protected against known attacks by either of the following methods: Having all custom application code reviewed for common vulnerabilities by an organization that	6.6 For web-based applications, ensure that one of the following methods are in place as follows: 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	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.		Note: This will become a required practice as of June 30, 2008.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
specializes in application security Installing an application-layer firewall in front of web-facing applications <i>Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.</i>	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
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	7.1 Obtain and examine written policy for data control, and verify that the policy incorporates the following: - 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	N/A – Security Policy (Data Control / Data Classification)		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.
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.	7.2 Examine system settings and vendor documentation to verify that an access control system is implemented and that it includes the following - 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)	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: - Coverage of all system components within the PCI Solution for Retail environment: - WCS (wireless console) - Cisco ACS (authentication for all network components (e.g. ISRs, routers, switches, and		

		wireless controllers) • 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, - Role-based privilege assignment for		

		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) - 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.		

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
8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.	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	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: - 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
		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. - NCR ACS Server (unique AD credentials)		
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	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: • 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)	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: - 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
		- 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)		
	8.4.b For Service Providers only, observe password files to verify that customer passwords are encrypted	N/A – Service Provider requirement		Responsibility of service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	8.5 Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	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: - 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	N/A – Security policy and procedures (ID / Account Management)		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.
	8.5.1.b Verify that only administrators have access to management consoles for wireless networks	Verizon Business reviewed WCS access lists to confirm very few administrators were allowed access to wireless configuration settings.		
8.5.2 Verify user identity before performing password resets	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	N/A – Security policy and procedures (ID / Account Management)		Account management / password reset procedures are the responsibility of the merchant / service provider.
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	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	N/A – Security policy and procedures (ID / Account Management)		Account management / password reset procedures are the responsibility of the merchant / service provider.

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 - 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
	critical functions do not exist Shared and generic User IDs are not used to administer wireless LANs and devices	- 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		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.
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited	N/A – Security Policy (Password policy/procedures)		Password policy/procedures are the responsibility of each merchant / service provider.
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested	N/A – Security Policy (Password policy/procedures)		Password policy/procedures are the responsibility of each merchant / service provider.
8.5.9 Change user passwords at least every 90 days	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	Verizon Business reviewed system settings for authentication methods to confirm the following: - All authentication through ACS (access to ASA firewalls, FWSMs, ISRs, routers, switches, and wireless	The following do not currently support password expiration, and do not currently support external authentication (e.g.	Note: A combination of documented password policies, manual audit procedures to ensure passwords are being changed every 90

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	passwords at least every 90 days 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	controllers), CiscoWorks (LMS), ASDM, and CSM) are forwarded to Active Directory, which is set to expire passwords after 42 days. - 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)	TACACS or AD): - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release)	days, and internal firewall segmentation of these components within the data center, would be reasonable compensating controls for password setting limitations within these applications.
8.5.10 Require a minimum password length of at least seven characters	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 For Service Providers only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements	Verizon Business reviewed system settings for authentication methods to confirm the following: - 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 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)	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): - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release)	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.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		- 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)		
8.5.11 Use passwords containing both numeric and alphabetic characters	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 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	Verizon Business reviewed system settings for authentication methods to confirm the following: - 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 +	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): - Cisco IDM - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release)	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.

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)		
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	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 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	Verizon Business reviewed system settings for authentication methods to confirm the following: - 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 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)	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): - 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)	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.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	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 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	Verizon Business reviewed system settings for authentication methods to confirm the following: - 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)	The following do not currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD): - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release)	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.
8.5.14 Set the lockout	8.5.14 For a sample of system	Verizon Business reviewed system	The following do not	Note: Using CSA or

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
duration to thirty minutes or until administrator enables the user ID	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	settings for authentication methods to confirm the following: - 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)	currently support account lockouts, and do not currently support external authentication (e.g. TACACS or AD): - ACS (authentication for ACS management) - RSA File Security Manager (to be addressed in FSM v2.2 release)	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.
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	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	Verizon Business confirmed the following components within the PCI Solution for Retail environment have sufficient idle timeout settings: - ISRs and switches: (15 minute session-timeout and 15 minute exec-timeout)	The following do not support idle session timeouts (15 minutes or less) for administrative connections: - WCS - IDM	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

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		- 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)	- wireless controllers (web interface) - ASDM - IDM - RSA File Security Manager (to be addressed in FSM v2.2 release) - RSA Authentication Manager	jobs).
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	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	N/A – Database security not part of the PCI Solution for Retail environment assessment.		Note: Ensuring authentication is enabled on all database components storing cardholder data is the responsibility of the merchant / service provider.
	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)	N/A – Database security not part of the PCI Solution for Retail environment assessment.		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.

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
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	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 • 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	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
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.	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	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.1.2 Restrict physical access to publicly accessible network jacks	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	N/A – Security Policy/Procedures (Physical Security)		Physical security (policies, procedures, and controls) is the responsibility of the merchant / service provider.
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	9.1.3 Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted	N/A – Security Policy/Procedures (Physical Security)		Physical security (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
9.2 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: - 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) • 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
		sent to LMS) • 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) - Cisco ACS • Local and AD authentication logs (auth requests forwarded to AD) • Local audit trail for ACS management - CSM (Cisco Security Manager) • AD auth logs (Cisco ACS auth requests forwarded to AD). • Local audit trail for CSM management - CSA (Cisco Security Agent) Manager • AD authentication logs (authentication requests sent directly to AD). • All CSA logs, alerts/events sent to CSA manager • Local audit trail for CSA management - CS-MARS • 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 - WCS (Wireless Console Server) • Local authentication		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		- Local audit trail for WCS management and wireless configuration changes - CiscoWorks (LMS) - 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 - 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 - AD auth logs (Cisco ACS auth requests forwarded to AD). - ASA firewall configuration changes and IDS/IPS alerts sent to CS-MARS. - Cisco IDM - IDM local auth logs and local configuration changes. - Cisco ACE XML Gateway - AD auth logs (Cisco ACS auth requests forwarded to AD). - Local audit trail for ACE XML Gateway management. - RSA SecurID - RSA SecurID access logged through RSA Authentication Manager.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		• RSA SecurID logs captured by RSA enVision for reporting, alerting, and long-term storage. - RSA Authentication Manager • 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 • RSA Key Manager authentication logs • Local audit trail for RSA Access Manager access/management. - RSA File Security Manager (RSA File Security Manager) • 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 • 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
		- Local audit trail for Key Manager access/management. - RSA enVision - 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 - 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.		
10.2 Implement automated audit trails for all system components to reconstruct the following events:	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:			
10.2.1 All individual accesses to cardholder data	10.2.1 All individual access to cardholder data	Verizon Business confirmed the following log access to cardholder data within the Cisco's PCI Solution for Retail environment: - 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.)		
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Actions taken by any individual with root or administrative privileges	Verizon Business reviewed audit log configurations to confirm administrative actions are logged for the following: - 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)	The following have limited audit trails, related to administrative actions: - RSA File Security Manager (not all administrative actions are logged - to be addressed in FSM v2.2 release)	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.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		- 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) Note: Reference to CSA is for administrative changes on Windows host OS for each application running on Windows.		
10.2.3 Access to all audit trails	10.2.3 Access to all audit trails	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: - ACS, CiscoWorks (LMS, NCM), CSA Manager, CSM, WCS Manager, RSA Authentication Manager, RSA Access Manager, RSA File Security Manager, RSA Key Manager, NCR ACS: • 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		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.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
		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). - CS-MARS (appliance server, which does not support CSA) • 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. - RSA enVision (not monitored by CSA, because log files are stored within a proprietary database) • 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
		run/viewed is logged 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.		
10.2.4 Invalid logical access attempts	10.2.4 Invalid logical access attempts	Verizon Business confirmed that invalid logical access attempts are logged for the following: - 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		
10.2.5 Use of identification and authentication mechanisms	10.2.5 Use of identification and authentication mechanisms	Verizon Business confirmed that userID for authentication is logged for authentication to the following: - 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		
10.2.6 Initialization of the	10.2.6 Initialization of audit logs	Verizon Business confirmed that RSA		See 10.2.3 (CSA

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
		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 (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)		
10.3.3 Date and time	10.3.3 Date and time stamp	Verizon Business confirmed date and time stamp is captured in the audit trail for the following: - 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
		- 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)		
10.3.4 Success or failure indication	10.3.4 Success or failure indication, including those for wireless connections	Verizon Business confirmed “success or failure” indication is captured in the audit trail for the following: - 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
10.3.5 Origination of event	10.3.5 Origination of event	Verizon Business confirmed “origination of event” is captured in the audit trail for the following: - 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)		
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Identity or name of affected data, system component, or resources	Verizon Business confirmed “name of affected data, system component, or resource” is captured in the audit trail for the following: - 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
	10.4.c Verify that the Network Time Protocol (NTP) is running the most recent version	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.		
	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	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.		
10.5 Secure audit trails so they cannot be altered	10.5 Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
10.5.1 Limit viewing of audit trails to those with a job-related need	10.5.1 Verify that only individuals who have a job-related need can view audit trail files	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. See 10.2.3 for additional audit trail access details.		See 10.2.3
10.5.2 Protect audit trail files from unauthorized modifications	10.5.2 Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation,	See 10.2.3/10.5.1 above		See 10.2.3

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
	and/or network segregation			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	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	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. CiscoWorks (LMS) is archiving audit trail once a day. (See 10.2.3 for additional details of audit trail archiving) RSA enVision centrally stores RSA SecurID log records (sent every 60 minutes from RSA Authentication Manager).		See 10.2.3
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN	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	Verizon Business confirmed wireless logs are sent to WCS and CS-MARS central servers.		
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)	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	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). 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). 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.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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). <i>Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6</i>	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	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. Note: Documented security policies and procedures need to require daily review of security logs, including follow-up to exceptions (responsibility of merchant / service provider)		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.
	10.6.b Through observation and interviews, verify that regular log reviews are performed for all system components	See 10.6.a above.		Interviews to be conducted with each merchant / service provider.
10.7 Retain audit trail history for at least one year, with a minimum of three months available online.	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	N/A – Security Policy (Data Retention)		Retention policy and procedure documentation is the responsibility of the merchant / service provider.
	10.7.b Verify that audit logs are available online or on tape for at least one year	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.		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.

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
system component installations, changes in network topology, firewall rule modifications, product upgrades). <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>	occurs. Verify that the scan process includes rescans until "clean" results are obtained			
	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 - 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	N/A – Third party external, quarterly scanning		Responsibility of merchant / service provider.
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	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:	N/A – Penetration Testing (at least annually)		Responsibility of merchant / service provider. Note: Penetration testing needs to be conducted on internal and external system components (network devices, applications, and servers), which are "in scope" for PCI.
11.3.1 Network-layer penetration tests	11.3.1 Network-layer penetration tests	N/A – Penetration Testing (at least annually)		Responsibility of merchant / service provider.
11.3.2 Application-layer penetration tests	11.3.2 Application-layer penetration tests	N/A – Penetration Testing (at least annually)		Responsibility of merchant / service provider.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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.	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	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).		
	11.4.b Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises	Verizon Business confirmed IDS/IPS is in place and can be configured to monitor and alert personnel of suspected compromise.		
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection	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.		

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE / COMMENTS
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. <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>	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	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.		

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 • 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.

