ワイヤレスとネットワークのセキュリティ統合ソリューション デザイン ガイド

Cisco Validated Design

November 24, 2008

Text Part Number: OL-18316-01-J

Cisco Validated Design

Cisco Validated Design Program は、お客様による、より迅速で、信頼性の高い、予測可能な展開を実現するために、設計、テスト、および文書化されたシステムとソリューションから構成されています。詳細については、www.cisco.com/go/validateddesigns を参照してください。

このマニュアルに記載されている設計、仕様、表現、情報、および推奨事項（ひとまとめにして「設計」）はすべて、現状のままで提供されています。シスコおよびその代理店は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、一切の保証の責任を負わないものとします。いかなる場合においても、シスコおよびその代理店は、設計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。

設計は予告なしに変更されることがあります。ユーザは設計の適用に対して全責任を負うものとします。設計はシスコおよびその代理店またはパートナーの技術的または専門的なアドバイスを受けたことを意味するものではありません。ユーザは設計を導入する前に、自社のテクニカル アドバイザに相談する必要があります。シスコによってテストされていない要因により、異なる結果が生まれることがあります。

CONTENTS

CHAPTER 8

はじめに

このマニュアルでは、Cisco Unified Wireless ソリューションのセキュリティ機能、およびそれらの機能と Cisco Self Defending Network の統合について説明しています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	説明
第 1 章「ソリューションの概要」	Cisco Secure Wireless ソリューションの概要について説明します。
第 2 章「ソリューションのアーキテクチャ」	Secure Wireless ソリューション アーキテクチャの概要を説明します。
第 3 章「802.11 セキュリティの概要」	802.11 規格のセキュリティ機能について説明します。
第 4 章「Cisco Unified Wireless Network アーキテクチャ：基本的なセキュリティ機能」	Cisco Unified Wireless ソリューションのセキュリティ機能について説明します。
第 5 章「無線 NAC アプライアンスの統合」	Cisco NAC アプライアンスについて説明します。また、Cisco Unified Wireless ソリューションでの Cisco NAC アプライアンスの展開についても説明します。
第 6 章「Secure Wireless ファイアウォールの統合」	Cisco Unified Wireless ソリューションとシスコ ファイアウォール ソリューションの統合について説明します。
第 7 章「モバイル クライアント セキュリティのための CSA」	CSA v5.2 WLAN のセキュリティ機能について説明します。
第 8 章「シスコの無線 IDS/IPS とネットワーク IDS/IPS の統合」	Cisco Unified Wireless ソリューションと Cisco IPS ソリューションの統合について説明します。
第 9 章「Cisco Unified Wireless 用の CS-MARS 統合」	CS-MARS と Cisco Unified Wireless Network を統合して、ネットワークをまたがる異常検出と関連性の特定を WLAN にまで拡張する方法について説明します。
用語集	このマニュアルで使用する主な用語をリストして定義します。

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、Service Request ツールの使用方法、および追加情報の収集方法については、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。『*What's New in Cisco Product Documentation*』には、シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Really Simple Syndication（RSS）フィードとして『*What's New in Cisco Product Documentation*』に登録し、リーダ アプリケーションを使用して、コンテンツがデスクトップに直接配信されるように設定します。RSS フィードは無料サービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

  http://www.cisco.com/go/services

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

CHAPTER 1

ソリューションの概要

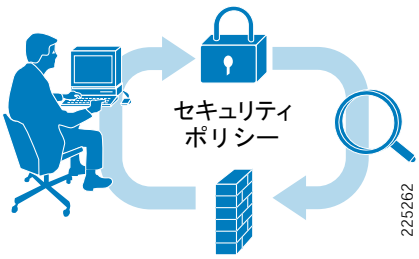
設計の概要

このデザイン ガイドは、ネットワーク セキュリティ テクノロジーと Cisco Unified Wireless Network の統合およびコラボレーションについて説明することを目的としています。Cisco Unified Wireless Network は、包括的な無線セキュリティ機能を特徴としています。ただし、このソリューションの目的は、有線側のネットワーク セキュリティが無線固有のセキュリティ機能をどのように補完するか、および有線側のネットワーク セキュリティをネットワーク全体のセキュリティ計画にどのように統合できるかを明らかにすることです。これにより、企業は、有線と無線の両方のネットワーク アクセス方式を含む共通のネットワーク セキュリティ ポリシーを適用できるようになります。

ネットワーク セキュリティ

ネットワーク セキュリティとは、セキュリティ ポリシーを定義し、予防的なセキュリティ対策を講じてセキュリティ ポリシーを適用し、ネットワークを監視してアクティビティを認識できるようにし、異常を識別して関連性を特定し、脅威を軽減し、セキュリティ ポスチャの修正や改善のために何が発生したかを確認する、継続的なプロセスです。図 1-1 を参照してください。

図 1-1　　セキュリティ プロセス



Cisco Unified Wireless Network は、セキュリティ ツールとセキュリティ テクノロジーの包括的なアーキテクチャを特徴とし、WLAN 環境、クライアント、およびインフラストラクチャをセキュリティで保護します。これらについては、第 4 章「Cisco Unified Wireless Network アーキテクチャ：基本的なセキュリティ機能」にまとめられています。Cisco Unified Wireless Network は、包括的な階層型セキュリティ ソリューションの一部として、無線アクセスのセキュリティ保護という重要な役割を担います。また、Cisco Unified Wireless Network と他のネットワーク インフラストラクチャを組合せて、階層型ネットワーク セキュリティを包含するケースを考えることもできます。

無線ネットワークへの攻撃は、数多く存在するネットワーク攻撃の 1 つの手法に過ぎません。もちろん、WLAN ネットワークは、セキュリティ保護される必要があります。しかしながら、WLAN 関連の攻撃だけに特化したセキュリティ ソリューションは、危険でアンバランスであると言えます。モバイル ネットワーク クライアントは、すべてのロケーションのすべてのインターフェイスで保護される必要があり、企業ネットワークは、すべての境界で保護される必要があります。また、ネットワーク トラフィックの発信元に関係なく、モニタリングと異常検出が必要です。理想としては、同種のインターフェイスには同じツールセットを使用して、これらのベースライン セキュリティ機能を提供することが望ましいです。これにより、運用コストが削減され、設定ミスのリスクが減り、簡単にバイパスされてしまうようなアンバランスなセキュリティ アーキテクチャになることを回避できます。

表 1-1 に、Cisco Unified Wireless Network セキュリティの役割、およびネットワーク セキュリティ アーキテクチャ内の他のコンポーネントの役割を示します。Cisco Unified Wireless Network は、ソリューション、WLAN 規格ベースの予防的なセキュリティと運用上のセキュリティ、および Cisco Security Agent（CSA）、Cisco Network Access Control（NAC）アプライアンス、Cisco Intrusion Prevention System（IPS）、Cisco Security Monitoring, Analysis and Response System（CS-MARS）などのコンポーネントを提供します。シスコ ファイアウォールは、これに基づいて、全体的なネットワーク セキュリティ アーキテクチャを実現します。これにより、階層型セキュリティ システムが提供されます。このシステムでは、Cisco Unified Wireless Network が、アクセス レイヤ テクノロジーに特有のセキュリティ、および全体的なネットワーク セキュリティ システムへの統合を実現します。

表 1-1　WLAN セキュリティ要素と一般的なネットワーク セキュリティ要素

予防的なセキュリティ	WLAN 固有の要素	一般的なネット ワーク セキュリティ 要素
ネットワーク インフラストラクチャの堅牢化	Cisco Unified Wireless Network、LWAPP、管理フレーム保護、802.1X	インフラストラクチャの堅牢化
エンドポイントの保護	Wi-Fi Protected Access/Wi-Fi Protected Access2	CSA および Cisco Secure Services Client
ポリシーの識別およびユーザに対する適用	Wi-Fi Protected Access/Wi-Fi Protected Access2、無線 LAN コントローラ上のクライアント除外	CSA、Cisco Secure Services Client、NAC、およびシスコ ファイアウォール
安全な通信	Wi-Fi Protected Access/Wi-Fi Protected Access2	
アクセス コントロール	無線 LAN コントローラ上のアクセス コントロール リスト	シスコ ファイアウォール
運用上のセキュリティ		
ネットワークの監視	無線 LAN コントローラ、Wireless Control System、Adaptive Wireless IPS	AAA、SNMP、プラットフォーム管理、および CS-MARS
異常検出と関連性の特定、脅威の軽減	無線 LAN コントローラ、Wireless Control System、Adaptive Wireless IPS	CS-MARS、CSA、および IPS

ソリューション コンポーネント

Secure Wireless アーキテクチャは、ブランチ ネットワークとキャンパス ネットワークに向けた中核的なシスコ アーキテクチャ上に構築されます。Secure Wireless アーキテクチャは、シスコ セキュリティ ソリューションと Cisco Unified Wireless Network の統合およびコラボレーションを示し、クライアント アクセス メカニズムに関係なく、ネットワークに共通のセキュリティ フレームワークを提供します。Secure Wireless アーキテクチャのコア コンポーネントは、次のとおりです。

- Cisco Unified Wireless Network
  - 無線侵入防御
  - 不正の検出および軽減
  - アクセス コントロール
  - トラフィック暗号化
  - ユーザ認証
  - RF 干渉および DoS のモニタリング
  - 無線セキュリティ脆弱性のモニタリングおよび監査
  - インフラストラクチャの堅牢化：MFP、インフラストラクチャ デバイス認証
- CSA
- Cisco NAC アプライアンス
- シスコ ファイアウォール
- Cisco IPS
- CS-MARS

Cisco Unified Wireless Network

Cisco Unified Wireless Network は、統合された無線ネットワーク ソリューションであり、企業が直面している無線ネットワークのセキュリティ、展開、管理、および制御の問題に、コスト効率の優れた方法で対応します。このソリューションは、無線ネットワークの利点を統合することにより、総所有コストを低く抑えながら、安全で拡張性のある無線ネットワークを提供します。

Cisco Unified Wireless Network は、安全性、拡張性、およびコスト効率の優れたソリューションの自由性と柔軟性を通じて、競争優位性を維持するために役立ちます。無線ネットワークには、次のような利点があります。

- いつでも、どこからでも情報にアクセスできるので、社員同士、ビジネス パートナー、およびお客様とのコラボレーションが促進されます。
- インスタント メッセージング、E メール、およびネットワーク リソースへのリアルタイム アクセスにより、生産性が向上し、業務上の迅速な意思決定が可能になります。
- 音声、ゲスト アクセス、高度なセキュリティ、ロケーションなどのモビリティ サービスにより、業務に変化をもたらすことができます。
- 屋内および屋外ロケーション用の 802.11n、802.11a/b/g、および企業無線メッシュをサポートするモジュラ アーキテクチャを提供しながら、将来のテクノロジーとサービスへの円滑な移行パスを確保します。

Cisco Security Agent（CSA）

CSA は、アップデート不要の攻撃保護機能、データ損失防止機能、およびシグニチャベースのアンチウイルス機能を 1 つのエージェントに統合した、最初のエンドポイント セキュリティ ソリューションです。これらの機能を独自の手法で組み合せることで、サーバやデスクトップを高度な Day Zero 攻撃から保護し、シンプルな管理インフラストラクチャの中で、利用規定と準拠ポリシーを適用します。

CSA は、次のようなさまざまな利点を備えています。

- アップデート不要の保護機能により、脆弱性が公開されるたびに急いでパッチを適用する必要がなくなるため、パッチに関連するダウンタイムと IT 費用を最小限に抑えることができます。
- 機密データの可視性と制御により、ユーザの操作や、ターゲットを絞ったマルウェアによって引き起こされるデータ損失を防止します。
- シグニチャベースのアンチウイルス保護機能により、既知のマルウェアを識別して削除します。
- 事前に定義された準拠ポリシーと利用規定を使用して、アクティビティの効率的な管理、レポーティング、および監査を行うことができます。
- Cisco NAC、シスコ ネットワーク IPS デバイス、CS-MARS など、先進のネットワーク セキュリティとエンドポイント セキュリティの統合およびコラボレーションを実現します。
- 中央集中型ポリシー管理により、動作ポリシー、データ損失防止、およびアンチウイルス保護の各機能がすべて、1 つの設定およびレポーティング インターフェイスに統合されます。

Cisco NAC アプライアンス

Cisco Network Admission Control（NAC）アプライアンスは、使いやすく強力なアドミッション制御 / 準拠強制ソリューションです。Cisco NAC は、包括的なセキュリティ機能を提供します。

- インバンドまたはアウトオブバンドの導入オプション
- ユーザ認証ツール
- 帯域およびトラフィックのフィルタリング制御
- 脆弱性の評価および修復（ポスチャ評価とも呼ばれる）

Cisco NAC アプライアンスは、ネットワークの集中アクセス管理ポイントとして、セキュリティ ポリシー、アクセス ポリシー、および準拠ポリシーを一箇所で管理できるので、ネットワークを通じて多くのデバイスにポリシーを伝播する必要はありません。また、リモート システムやローカル システムの検査によって、指定条件を満たしていないユーザ デバイスは、ネットワークにアクセスできないようにします。

これらの同じ Cisco NAC アプライアンス機能を Cisco Unified Wireless Network と統合することで、有線と無線の両方のネットワークに一貫してポリシーを適用できます。

シスコ ファイアウォール

ファイアウォールは、外部と内部の両方で、攻撃および不正アクセスからネットワークを保護します。ファイアウォールは、他のネットワーク（有線と無線の両方）からの不正アクセスから無線ネットワークを保護します。また、ユーザが許可なく無線ネットワークにアクセスする

ことを禁止します。シスコは、ファイアウォールをいくつかの製品ラインに統合しています。たとえば、ASA 5500 シリーズ、IOS セキュア ルータ、Catalyst 6500 シリーズ スイッチのサービス モジュールなどです。

Cisco IPS

Cisco IPS は、ネットワークベースのプラットフォームであり、ワーム、スパイウェア、アドウェア、ネットワーク ウイルス、偵察、アプリケーションの不正使用、ポリシー違反といった悪意のあるトラフィックを正確に識別、分類、および阻止するために設計されています。これは、レイヤ 2 ～ 7 での詳細なトラフィック検査によって実現されます。

シスコは、Cisco IPS 4200 シリーズ専用のアプライアンスと IOS IPS の他にも、Cisco ASA 5500 シリーズ、Cisco Integrated Security Router（ISR）、および Catalyst 6500 シリーズ用の統合モジュールなど、さまざまなネットワーク IPS プラットフォームを提供しています。

CS-MARS

CS-MARS は、ネットワーク デバイスやホスト アプリケーション、有線と無線、シスコや他のベンダーなど、ネットワーク全体にわたるセキュリティ モニタリングを提供します。CS-MARS は、ネットワーク、脅威識別、関連性の特定、および集約のエンドツーエンドのトポロジ ビューを提供し、重大なアラートを識別することで、false positive を大幅に減らします。また、軽減応答オプションを作成し、強力な犯罪分析機能を提供し、インシデント応答および準拠規制に関するレポートを作成します。

CHAPTER 2

ソリューションのアーキテクチャ

概要

Secure Wireless ソリューション アーキテクチャの目的は、無線ユーザと有線ユーザにネットワーク全体にわたる共通のセキュリティ サービスを提供し、階層型セキュリティ アーキテクチャに向けた無線セキュリティ インフラストラクチャとネットワーク セキュリティ インフラストラクチャのコラボレーションを可能にすることです。このアーキテクチャは、キャンパス展開とブランチ展開の両方に同様に適用できます。このアーキテクチャのコア コンポーネントは、次のとおりです。

- Cisco Unified Wireless Network アーキテクチャ
- シスコ キャンパス アーキテクチャ
- シスコ ブランチ アーキテクチャ

Cisco Unified Wireless Network アーキテクチャは、無線環境をセキュリティで保護するコア モビリティ サービス プラットフォームを提供し、さらに無線展開自体のセキュリティ保護に必要なすべての機能を提供します。基礎となるキャンパス アーキテクチャとブランチ アーキテクチャは、モビリティ サービス向けの、安全性、性能、およびアベイラビリティの高いネットワーク プラットフォームを提供します。これにより、セキュリティ サービス統合用の共通の有線 / 無線プラットフォームが提供され、すべてのネットワーク クライアントとトラフィック タイプに向けた共通のセキュリティ アーキテクチャを開発できます。

Cisco Unified Wireless Network

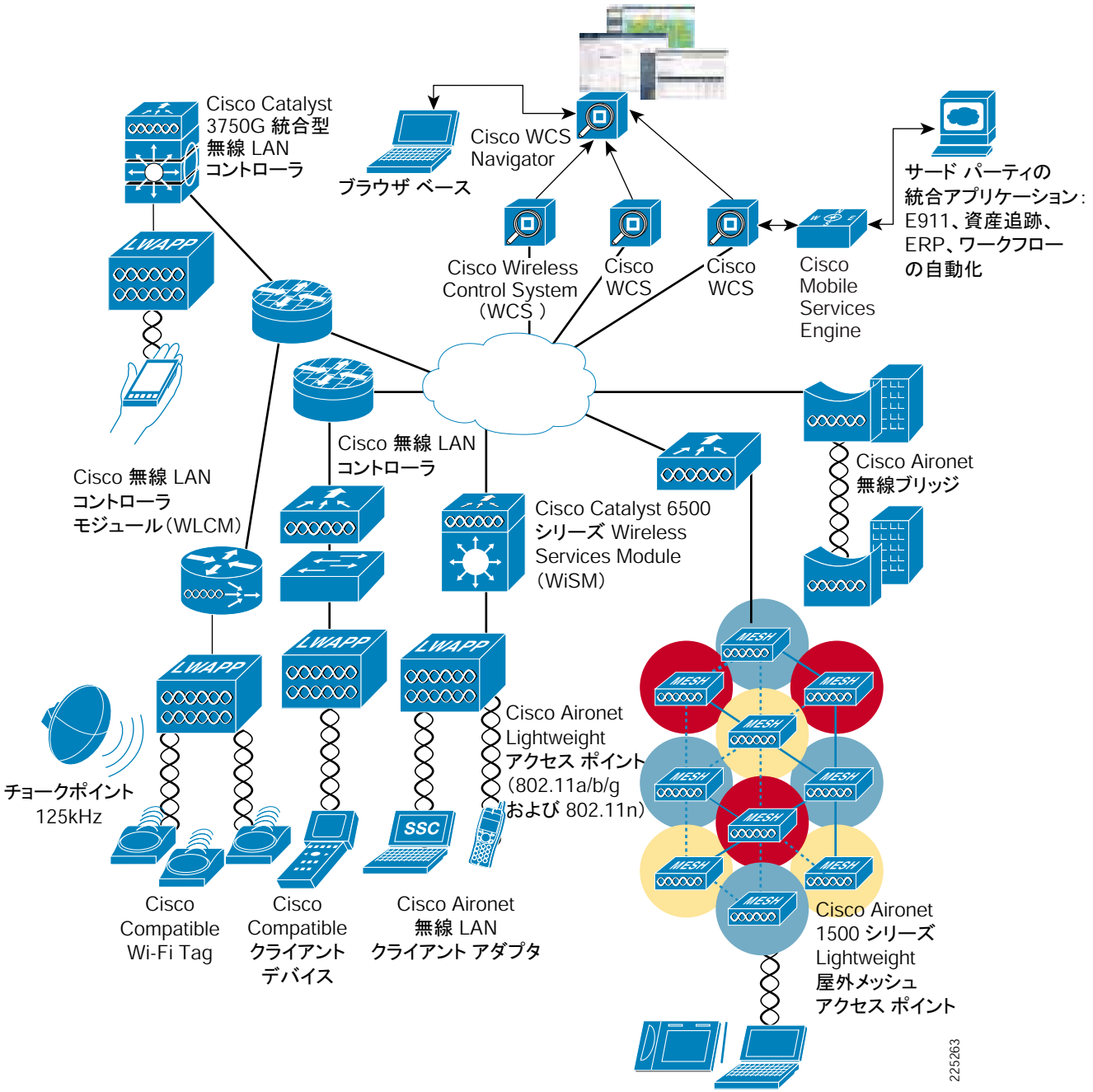
企業の WLAN は、ネットワーク接続に最も効果的な手段の 1 つとなっています。Cisco Unified Wireless Network は、有線と無線を統合したネットワーク ソリューションであり、無線ネットワークを展開する上での無線ネットワークのセキュリティ、展開、管理、および制御の側面に対応します。Cisco Unified Wireless Network は、無線ネットワークと有線ネットワークの利点を統合することにより、総所有コストを低く抑えながら、安全で拡張性のある無線ネットワークを提供します。図 2-1 に、Cisco Unified Wireless Network の要素を示します。

次の 5 つの相互に接続された要素が連携して、統一された企業向け無線ソリューションを提供します。

- クライアント デバイス
- アクセス ポイント
- 無線コントローラ
- ネットワーク管理

- モビリティ サービス

図 2-1　　Cisco Unified Wireless アーキテクチャの概要



クライアント デバイスを基にして、各要素は、ネットワークのニーズの進化および成長に応じて機能を追加し、包括的でセキュリティで保護された WLAN ソリューションを作成します。Cisco Unified Wireless Network は、費用対効果の高い、WLAN のセキュリティ保護、展開、管理の方法を提供し、企業が直面している問題を管理します。このフレームワークは、有線および無線ネットワークを統合して拡張し、総所有コストを低く抑えながら、拡張性、管理容易性、安全性に優れた WLAN を提供します。Cisco Unified Wireless Network は、有線 LAN に期待されるレベルと同等のセキュリティ、信頼性、展開のしやすさ、管理性を無線 LAN に対して提供します。

Cisco Unified Wireless Network 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/unifiedwireless

Cisco Unified Wireless Network インフラストラクチャには、無線ネットワークの安全な展開および運用に必要なコンポーネントが組み込まれています。無線 LAN コントローラを利用して、アクセス ポイントと無線管理システムが包括的な無線セキュリティを確保し、セキュリティ操作を合理化しながら機器コストを削減します。シスコは、無線 LAN 製品とネットワーク セキュリティ製品の両方を一社で提供しています。これにより、高度なネットワーク セキュリティ技術をベースとした、無線ネットワークのセキュリティ保護を実現しています。ネットワーク セキュリティ製品の機能を利用することで、無線ネットワーク、ユーザ、およびそのトラフィックを強力に制御できます。その上、無線セキュリティを有線ネットワーク セキュリティで補完することにより、階層型防御が実現します。階層型防御は、IT 部門のネットワーク運用チームとセキュリティ運用チームの正確さと操作効率を向上させながら、徹底的な保護を提供します。

無線は地上波伝送であるため、特有のセキュリティ要件があります。無線ネットワークに関するセキュリティ上の主な問題は、次のとおりです。

- 企業のネットワークへのバックドア アクセスを可能にする不正なアクセス ポイントおよびクライアント。
- ネットワーク プロファイリングや機密情報の盗用のためにユーザをおびき寄せて接続させようと試みる、ハッカーのアクセス ポイント（悪魔の双子やハニーポットなど）。
- 無線ネットワークを混乱させたり使用不可にしたりするサービス拒絶。
- 地上波ネットワークの偵察、傍受、およびトラフィック クラッキング。現在、これは主にレガシーな問題となっています。無線業界が 802.11i と WPA によるユーザ認証とトラフィック暗号化の標準的なアプローチを作成したためです。
- 無線ユーザが接続するネットワークの制御。特に、無線ユーザがオフィスの外にいる場合。
- ゲスト ユーザの無線セキュリティ。

これらすべての機能に関するセキュリティ イベント管理とレポーティングは、ネットワーク上でセキュリティ イベントが発生した物理的な場所の追跡と共に、堅牢な無線セキュリティ ソリューションの鍵となっています。

これらすべての問題は、Cisco Unified Wireless Network インフラストラクチャを構成する無線コントローラ、アクセス ポイント、および WCS 管理システムに組み込まれている、セキュリティ テクノロジーによって対応されます。ユーザに接続性を提供する無線機器も、展開全体にわたるセキュリティを提供します。組み込みの無線侵入防御システムは、不正なアクセス ポイントとクライアント、DoS 攻撃、ハッカーのアクセス ポイント、ネットワークの偵察、傍受、試行される認証と暗号化のクラッキングを検出および軽減します。さらに、シスコは、ユーザ トラフィックにサービスを提供するアクセス ポイントから無線 IPS モニタリングを提供でき、フルタイムの専用無線 IPS モニタリングも提供できます。両方のアプローチを提供することで、ネットワーク セキュリティ ポリシーに基づくサイト固有の柔軟性を実現できます。これにより、スタンドアロンの無線侵入防御システムに関連する、高いインフラストラクチャ コストが削減されます。

シスコでは、ネットワークは自己防衛的であるべきだと考えています。被害を受けてから単に攻撃を検出するよりも、攻撃を受け付けない堅牢なネットワーク コアを提供する方が賢明です。この目的を達成するために、シスコの管理フレーム保護は、無線侵入防御システムに加えて、攻撃防止の予防的なレイヤを提供し、ほとんどの無線攻撃を無効にします。

Cisco Unified Wireless Network インフラストラクチャには安全なゲスト アクセス管理も統合されており、キャプティブ ゲスト ユーザ ポータル、ネットワーク セグメンテーション、および完全なゲスト管理機能を提供します。最後に、これをすべて包み込んだものが WCS 管理システムであり、前述のすべての組み込みセキュリティ ソリューション対して、完全な設定管理、セキュリティ イベント集約、およびセキュリティ レポーティングを提供します。

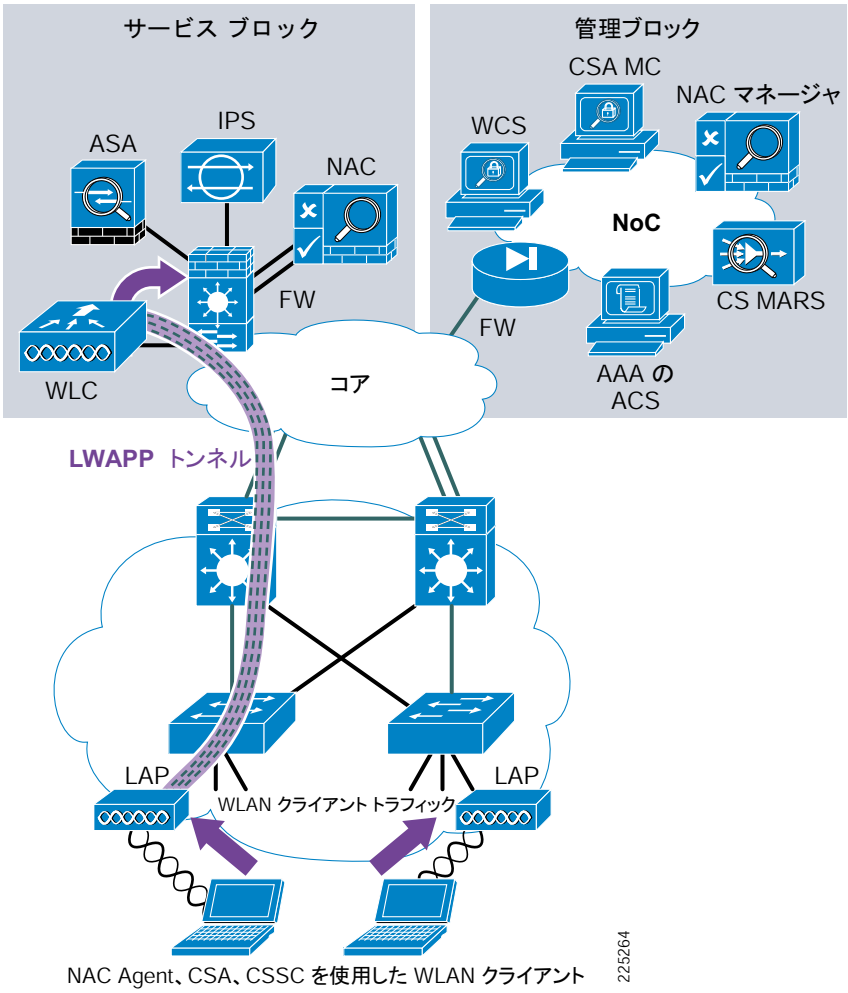
前述のように、シスコは、組み込みの無線セキュリティをシスコ ネットワーク セキュリティ製品からのテクノロジーでさらに補完することにより、無線セキュリティへの階層型アプローチを提供できます。高度なクライアント セキュリティのために、シスコ有線侵入防御、Network Admission Control アプライアンス、Cisco MARS セキュリティ情報管理システム、Cisco Security Agent などのネットワーク セキュリティ プラットフォームを利用することで、有線と無線のセキュリティ コラボレーションが実現します。このコラボレーションにより、ワームやウイルスなどのマルウェアに対するネットワーク保護が強化および拡張され、クライアント セキュリティ ポスチャが適用され、ネットワーク全体のセキュリティ イベント集約、分析、およびレポーティングが提供されます。

Secure Wireless アーキテクチャ

Secure Wireless ソリューション アーキテクチャは、1 つの WLAN セキュリティ コンポーネントと複数のネットワーク セキュリティ コンポーネントで構成されます。Cisco Unified Wireless Network は、WLAN セキュリティ コアを提供します。このコアは、他のシスコ ネットワーク セキュリティ コンポーネントと統合して、完全なソリューションを実現します。Cisco Unified Wireless Network アーキテクチャは、キャンパス サービス ブロック内の無線 LAN コントローラへのクライアント トラフィックをトンネルするメカニズムを提供します。このサービス ブロックは、NAC、IPS、ファイアウォールなどのネットワーク セキュリティ サービスおよびポリシーを適用するための中央の場所を提供します。サービス ブロック内のネットワークを保護するコンポーネントに加えて、Cisco Security Agent が追加の保護ネットワークを提供すると同時に、モバイル クライアントを保護します。

シスコでは、有線と無線のコラボレーションは、単により多くのボックスをネットワークに配置することを意味するのではありません。このコラボレーションは、シスコの有線と無線のセキュリティ テクノロジーの間に構築された専用リンケージであり、セキュリティ機能および保護のスーパーセットを提供します。

図 2-2　Secure Wireless アーキテクチャの概要

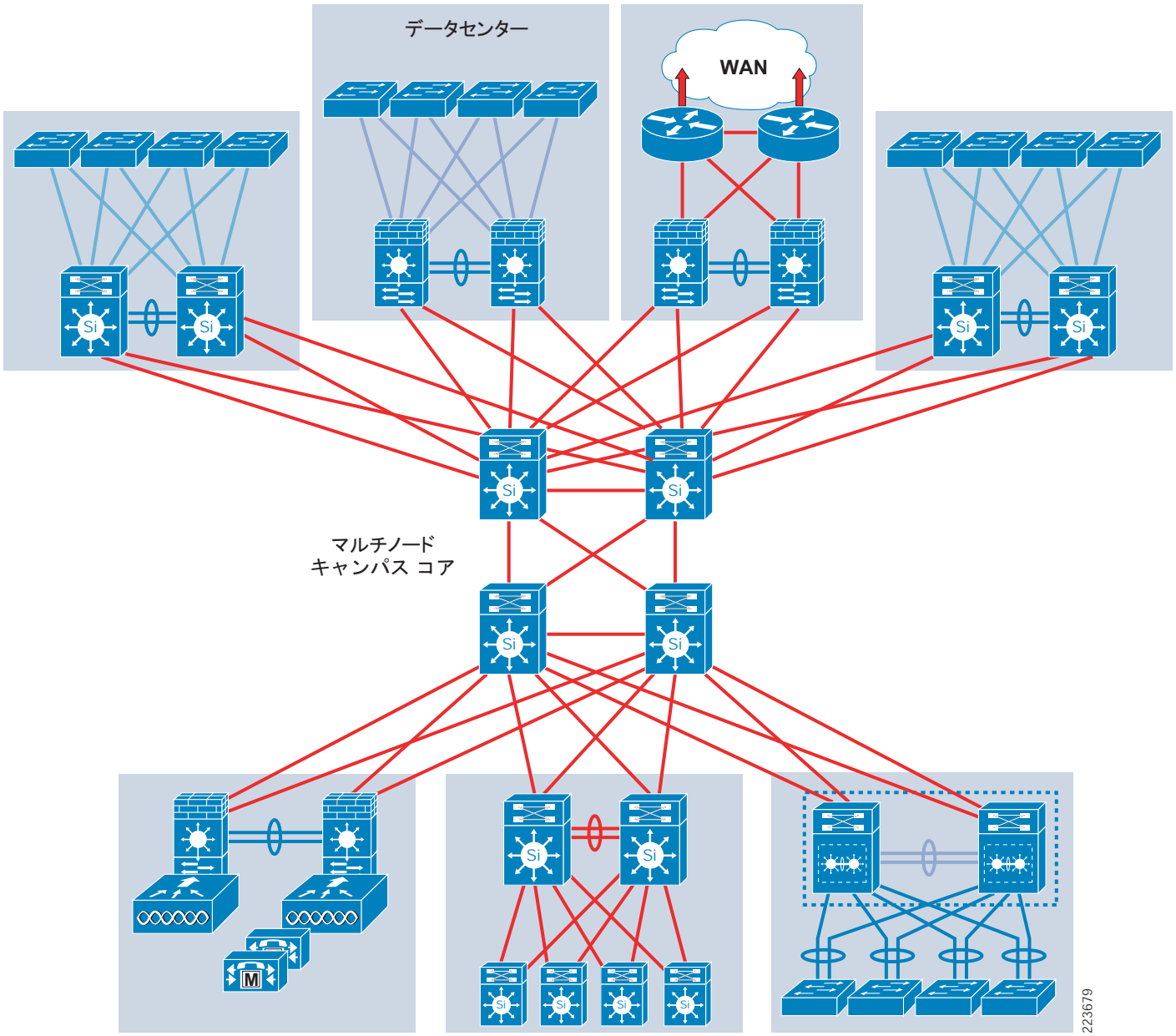


キャンパス アーキテクチャ

全体的なキャンパス アーキテクチャ（図 2-3 を参照）は、基本的な階層型ルータ / スイッチ設計を超えています。アクセス、分散、コアなどの階層は、キャンパス ネットワークの設計方法と構築方法の基盤となりますが、キャンパス ネットワークが何を実行するかに関する根本的な問題に対応しません。キャンパス ネットワークは、Secure Wireless ソリューションの構築に使用されるサービスを提供します。次のようなサービスが、Secure Wireless ソリューションの基礎となります。

- ハイ アベイラビリティ
- アクセス サービス
- アプリケーションの最適化および保護のサービス
- バーチャライゼーション サービス
- セキュリティ サービス
- 運用および管理のサービス

図 2-3　　キャンパス アーキテクチャ



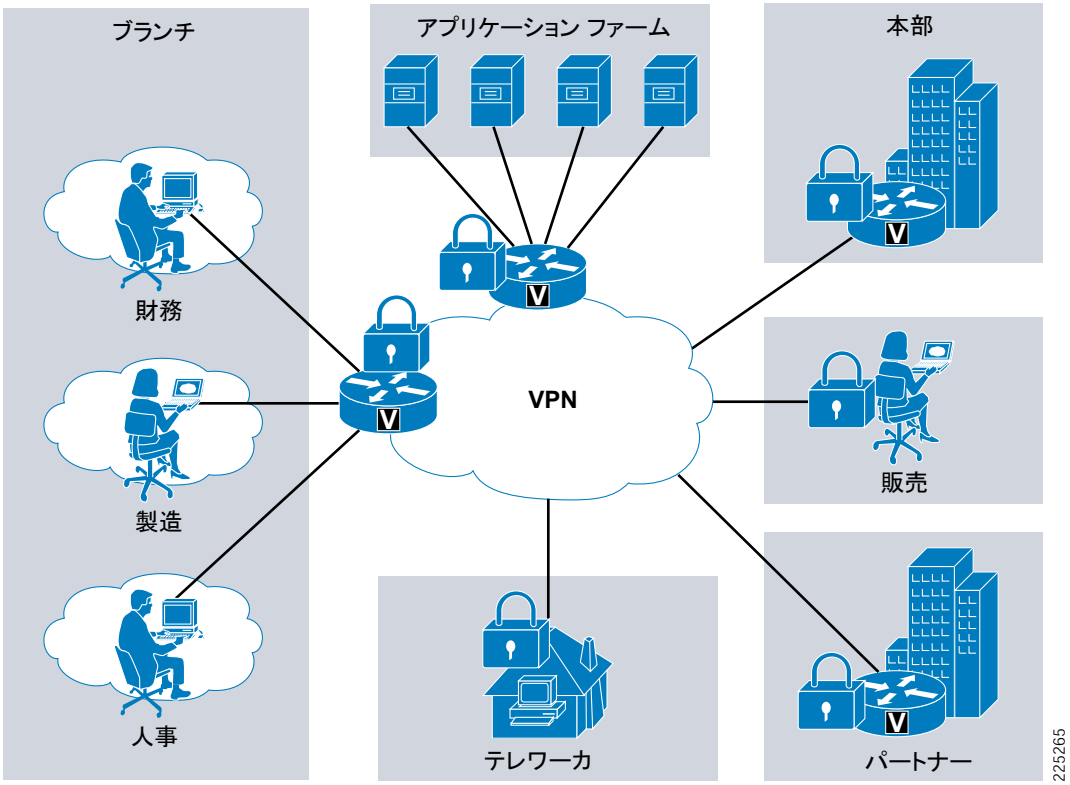
ブランチ アーキテクチャ

フル サービス ブランチは、キャンパスで使用できるものと同じソリューションとサービスをブランチに提供します。これには、セキュリティと無線が含まれ、Secure Wireless ソリューションは、キャンパスと同様にブランチ展開にも適用できます。

ブランチには、WLAN、ファイアウォール、および NAC のオプションが数多く存在します。たとえば、H-REAP、WLAN Controller Module（WLCM; WLAN コントローラ モジュール）、21XX WLC、またはより大きな WLC にするか、ASA、IOS のいずれのファイアウォールにするか、NAC アプライアンスと NAC モジュールのいずれにするか、IPS アプライアンスにする

か IPS モジュールにするかなどのオプションがあります。このデザイン ガイドで、このようなさまざまな組み合せをすべて説明することはできません。そのため、このブランチ設計では、ブランチ展開で一般的な製品、およびキャンパスの例とは大幅に異なる展開および製品を使用することに重点を置いています。したがって、このデザイン ガイドでは、H-REAP と 2106 WLC、IOS ファイアウォール、および IPS モジュールと NAC モジュールを使用しています。図 2-4 に、アーキテクチャの概略図を示します。

図 2-4　　ブランチ アーキテクチャ



CHAPTER 3

802.11 セキュリティの概要

この章では、現在企業の無線 LAN（WLAN）展開を検討しているお客様のために 802.11 セキュリティについて説明します。この章では、802.11 無線ネットワークで使用できる、企業向けの最新のセキュリティ機能について説明します。たとえば、このガイドでは、Wi-Fi Protected Access（WPA）や WPA2 などの方式を中心に説明し、Wired Equivalent Privacy（WEP）についてはほとんど紙面を割いていません。

規制、規格、および業界認定

ほとんどのネットワーク システムと同様に、さまざま規格が適用されます。これらの規格のほとんどは、2 つの標準化団体 Institute of Electrical and Electronics Engineers（IEEE; 電気電子学会）および Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）のいずれかによって策定されたものです。IEEE が定めた 802.11 規格と、IETF が定めた Extensible Authentication Protocol（EAP）方式は、安全な WLAN 展開のサポートで導入される 2 つの中心的な規格です。

IEEE

IEEE は、一連の 802.11 規格を定めています。最初の 802.11 規格は 1999 年に発表され、その後さまざまな修正が加えられてきました。これらの修正では、物理レイヤの実装が追加され、より高いビット レート（802.11b、802.11a、および 802.11g）、QoS の拡張（802.11e）、およびセキュリティの強化（802.11i）が実現されました。このガイドでは、802.11i のセキュリティ強化を中心に説明します。

IEEE は、ポート セキュリティのための 802.1X 規格も定めています。これは、802.11i において WLAN クライアントの認証に使用されます。

IETF

802.11 に関連する IETF の主な RFC および草案は、EAP に基づいています。EAP の利点は、認証プロトコルをその転送から切り離すことです。EAP は、802.1X フレーム、PPP フレーム、UDP パケット、または RADIUS セッションで伝送できます。

802.11 ネットワークでは、EAP は WLAN 上では 802.1X フレームで転送され、Wireless LAN Controller（WLC; 無線 LAN コントローラ）から Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバへは RADIUS プロトコルで転送されます。これにより、WLAN クライアントと AAA サーバの間のエンドツーエンドの EAP 認証が提供されます。これについては、このガイドの後半で詳しく説明します。

Wi-Fi Alliance

コア ネットワークでは同じベンダーの複数のプラットフォームを使用するのが一般的で、その統合は、主に、ベンダーによる製品テストの一環として実施されています。ただし、さまざまなベンダーのプラットフォームが統合されている場合、他のベンダーのデバイスとの相互運用性に関して各デバイスの機能を理解することは、通常、ネットワーク エンジニアとネットワーク管理者の責任となります。

WLAN などのように、システムがクライアント デバイスを含む場合、相互運用性を認定するための業界団体が設立されるのが一般的です。規格にはベンダーによる解釈の余地が残されることが多く、ベンダーがオプションの機能を指定することもあるためです。基本的なデバイス動作を認定することにより、ベンダーの異なる 2 つのデバイスが相互運用可能であるという適度な保証がお客様に提供されます。

Wi-Fi Alliance（http://www.wi-fi.org）は、Wi-Fi、Wi-Fi Protected Access（WPA）、Wi-Fi Protected Access 2（WPA2）、および Wi-Fi Multimedia（WMM）認定プログラムを通じて、WLAN デバイスの相互運用性を認定する業界団体です。

WPA 規格は、WEP 暗号化プロセスの弱点に対応するために開発されたもので、802.11i ワーク グループの規格が承認される前に存在していました。WPA 開発の主な目的の 1 つは、WEP ベースのハードウェアとの下位互換性を確保することでした。この目的を達成するために、WPA 規格は WEB で使用される基本的な RC4 暗号化方式を使用していますが、WEP の弱点に対応するためにキー生成の改良とメッセージ完全性チェックの改善を加えています。

WPA2 は、批准された 802.11i 規格に基づいており、そのコアで Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol（AES CCMP）暗号化を使用します。WPA2 には、新しいクライアントおよび AP ハードウェアが必要です。ラップトップや他のクライアント デバイスの現在のアップグレード サイクルを考えると、WPA 環境と WPA2 環境の混在はしばらく続くと思われます。完全に新規の構築の場合では、お客様は最初から WPA2 デバイスを展開すると予想されます。

Cisco Compatible Extensions

Cisco Compatible Extensions（CCX）プログラムは、Cisco WLAN インフラストラクチャで利用できるクライアント デバイスの普及を促進し、シスコ独自の最新機能を活用して、セキュリティ、モビリティ、QoS（Quality of Service）、およびネットワーク管理を向上することを目的としています。

図 3-1 に示すように、CCX は 802.11 規格、IETF 規格、および Wi-Fi Alliance 認定に基づいており、WLAN 機能のスーパーセットを構成しています。Cisco Unified Wireless Network の導入を計画していない場合でも、CCX 互換のカードを使用すれば、WLAN クライアント デバイスが対応している規格や認定を簡単に追跡できます。

図 3-1　　CCX の構造

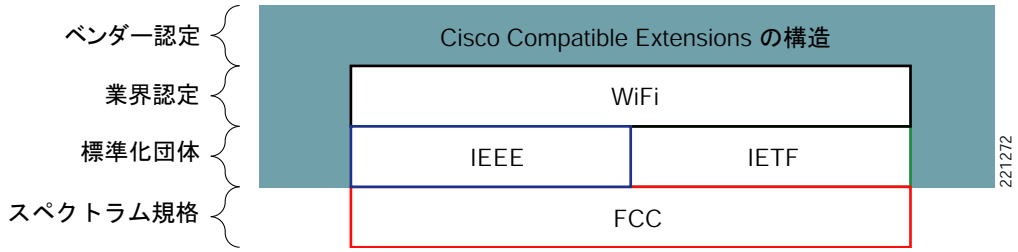


表 3-1 は、CCX のセキュリティ機能を認定レベルごとにまとめたものです。CCX 認定は、該当する Wi-Fi 認定だけでなく、CCX 認定の一環としてすでにテストされている EAP サプリカントも指定します。

CCX のバージョン一覧は、http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html で参照できます。

表 3-1　　CCX のセキュリティ機能の例

セキュリティ	v1	v2	v3	v4	ASD
WEP	x	x	x	x	
IEEE 802.1X	x	x	x	x	x
LEAP	x	x	x	x	x
PEAP と EAP-GTC（PEAP-GTC）		x	x	x	オプション
EAP-FAST			x	x	x
PEAP と EAP-MSCHAPv2（PEAP-MSCHAP）				x	
EAP-TLS ASD には、LEAP、EAP-Fast、または EAP-TLS が必要				x	x
Cisco TKIP（暗号化）	x				
WiFi Protected Access（WPA）: 802.1X + WPA TKIP		x	x	x	
LEAP を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）		x	x	x	x
PEAP-GTC を使用		x	x	x	
EAP-FAST を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）			x	x	x
PEAP-MSCHAP を使用				x	
EAP-TLS を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）				x	x
IEEE 802.11i–WPA2: 802.1X + AES			x	x	
LEAP を使用			x	x	
PEAP-GTC を使用			x	x	
EAP-FAST を使用			x	x	
PEAP-MSCHAP および EAP-TLS を使用				x	
Network Admission Control（NAC）				x	

221405

CCX v5 には、クライアント側での Management Frame Protection（MFP; 管理フレーム保護）など、新しいセキュリティ機能が追加されています。P.4-18 の「管理フレーム保護」を参照してください。

連邦無線セキュリティ ポリシーと FIPS 認定

United States Department of Defense（DoD; 米国国防総省）のミッションクリティカルな性質により、DoD では無線セキュリティの厳しい規格が必要となります。DoD セキュリティ ポリシーは、連邦と民間の展開の全体的なベンチマークを確立し、民間企業向け市場で採用されるセキュリティ方針に影響を及ぼします。このような厳しい DoD 無線セキュリティ要件は、DoD Directive 8100.2「Use of Commercial WLAN Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)」（2006 年 6 月）に概説されています。

この文書の抜粋を次に示します。

> (1) WLAN の認証と暗号化。2007 年度から、すべての新規獲得物について、DoD のコンポーネントが実装する WLAN ソリューションは、IEEE 802.11i に準拠し、WPA2 Enterprise 認定を受け、EAP-TLS 相互認証を含む 802.1X アクセス コントロールを実装し、FIPS 140-2 minimum overall Level 1 で検証された Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code Protocol（AES-CCMP）通信の排他的な使用を保証する設定を実装しなければならない。パラグラフ 3.c.(2) に従って、このポリシー規約施行後 180 日以内に、FIPS 140-2 で検証された暗号化モジュールを含む Wi-Fi Alliance WPA2 認定の 802.11i 実装をサポートしないレガシー WLAN システムの移行計画を DoD CIO に報告しなければならない。

指令 8100.2 は、DoD ネットワーク内のすべての商用 WLAN インストレーションに必須の 4 つの主なポリシー分野に言及しています。

- 規格ベースの IEEE 802.11i セキュリティ（WPA2）
- 相互運用可能な Wi-Fi 認定製品
- ロケーション検知を含む無線侵入検知
- Federal Information Processing Standard（FIPS; 連邦情報処理標準）140-2 および共通基準認定

FIPS 140-2 認定は、連邦（民生および DoD）にて購入する全ての WLAN 獲得製品に必要です。Cisco Unified Wireless LAN コントローラおよびアクセス ポイントは、IEEE 802.11i WLAN セキュリティ規格への準拠について、National Institute of Standards and Technology（NIST; 国立標準技術研究所）FIPS 140-2 level 2 認定を受けています。FIPS 認定は、所定の暗号モジュール内のすべての暗号化機能および暗号化動作が正しく実装されていることを保証します。802.11i（WPA2）セキュリティの場合、これには、強力な無線暗号化のための AES-CCMP の正しい実装と使用が含まれます。

また、Cisco Unified Wireless Network ソリューションは、DoD 無線ポリシーによって指示されている共通基準検証の実行中です。共通基準は、エンドツーエンドの WLAN システム全体の Information Assurance（IA; 情報保証）面を検証します。これには、システムを通過する、およびシステムに格納されるすべての情報のデータ保護、認証とアクセスの強力な制御、侵入検知、およびシステム モニタリングが含まれます。シスコ共通基準ソリューションには、次のような重要な WLAN コンポーネントがすべて含まれます。

- WLAN コントローラ
- Aironet アクセス ポイント
- Wireless Control System（WCS）
- Access Control Server（ACS）
- Wireless Location Appliance

この DoD ポリシーの文書には、強力な認証の要件、およびロケーション検知を含む無線侵入検知の要件も記載されています。これらについては、このガイドの後半、および脅威の阻止と制御に関する後続の文書で説明されています。

要約：

- Cisco Unified Wireless は、米国政府の厳しい無線セキュリティ要件を満たすと認定されています。
- Cisco Unified Wireless は、メインライン ソフトウェアと工場出荷時のハードウェアに FIPS と共通基準が組み込まれる形で出荷されます。
- Cisco Unified Wireless は、DoD のエンドツーエンド セキュリティ要件に準拠しています（信頼できるネットワーク デバイス）。

- Cisco Unified Wireless は、有線ネットワークと無線ネットワークに対して「ロケーション追跡を含む継続的な無線 IDS モニタリング」の DoD 要件を満たします。
- Cisco ACS 4.1 については、現在 FIPS 認定プロセスが進行中です。

米国連邦通信委員会

Federal Communications Commission（FCC; 米国連邦通信委員会）は、米国で WLAN によって使用される Radio Frequency（RF; 無線周波）帯を制御する規制機関です。FCC は、WLAN スペクトラムの無線電力およびアンテナ ゲインに関する規則を定めるだけでなく、その規定違反を起訴できます。例として、関連する FCC 規制の抜粋を次に示します。

- 15.5 項：一般的な動作条件

  (a) 意図的な（電波放射を目的とする）または非意図的な（電波放射を目的としない）ラジエータを操作する者は、機器の以前の登録または認定に基づく、あるいは電力線搬送方式については、この条の 90.63(g) 項に準ずる以前の利用届出に基づく、所定の周波数の継続使用に対する既得のまたは認識可能な権利を有すると見なされないものとする。[90.35(g) 項を参照。]

  (b) 意図的、非意図的、または付随的なラジエータの動作は、有害な干渉が引き起こされないという条件、および認可された無線局の動作、別の意図的または非意図的なラジエータ、Industrial, Scientific, and Medical（ISM; 工業用、科学用、および医療用）機器、あるいは付随的なラジエータによって引き起こされる可能性のある干渉が受け入れられなければならないという条件に従う。

  (c) 無線周波デバイスのオペレータは、デバイスが有害な干渉を引き起こしているという通知を委員会の代表から受け取り次第、デバイスの動作を停止する必要があるものとする。有害な干渉を引き起こしている条件が修正されるまで、動作を再開させないものとする。

- 15.9 項：傍受の禁止

  法的権限の下で行われる法執行官の操作を除き、他人の個人的な会話を盗み聞きまたは録音する目的で、この部の条項に準じて動作するデバイスを直接的または間接的に使用しないものとする。ただし、そのような使用が、会話の当事者すべてに許可されている場合を除く。

したがって、802.11 無線スペクトラムは無許可ですが、規制されており、スペクトラムの不正使用や違法な行為が発生した場合は、法的手段を講じることができます。

802.11 の基本的なセキュリティ機能

ここでは、802.11 無線ネットワークで現在使用できる企業向けセキュリティ機能について説明します。

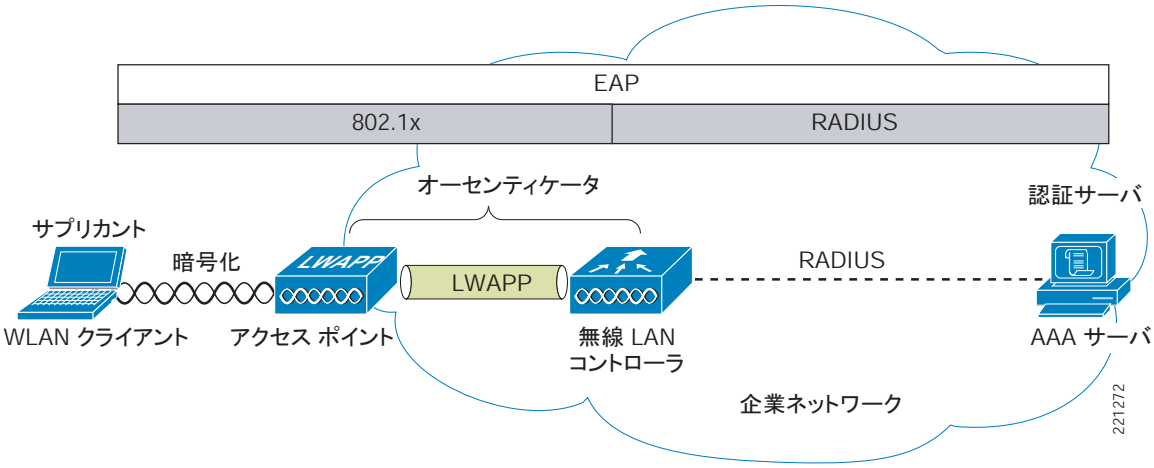
当初の 802.11 プロトコルは脆弱なセキュリティが問題視されていました。データ漏洩に関するこうした問題を解消するため、その後新しく登場したのが 802.11i 規格です。この規格では、強力な認証方式と暗号化方式を採用することで無線通信の機密性要件を実現しています。

このガイドの後半では、WLAN のその他のセキュリティ問題を取り上げます。現在、各標準化機関がこれらの問題の改善に努めています。また、Cisco Unified Wireless Network ソリューションにも対応策が取り入れられています。

用語

このガイドで使用されている一般的な用語を図 3-2 に示します。

図 3-2　　安全な無線トポロジ



このソリューションの基本的な物理構成要素は次のとおりです。

- WLAN クライアント
- アクセス ポイント（AP）
- 無線 LAN コントローラ（WLC）
- AAA サーバ

さらに図 3-2 は、802.1X 認証プロセスで使用する基本的な役割とそれらの関係を示しています。

- 802.1X サプリカントは WLAN クライアント上に配置されます。
- AP と WLC（スプリット MAC アーキテクチャを使用）は 802.1X オーセンティケータとして動作します。
- AAA サーバは認証サーバです。

図 3-2 は、クライアントと認証サーバ間で EAP パケットを伝送する際の 802.1X および RADIUS プロトコルの役割も示しています。802.1X と EAP については、この章の後半で詳しく説明します。

802.11 の基本

802.11 WLAN は、複数の要素と動作から構成されています。これらが、802.11 プロトコルの基礎を築きます。このプロトコルのキーとなる部分が、適切な WLAN を検出し、その WLAN との接続を確立します。このプロセスの主要コンポーネントは、次のとおりです。

- ビーコン：WLAN ネットワークがその存在をアドバタイズするために使用します。
- プローブ：WLAN クライアントがネットワークを見つけるために使用します。

- 認証：元々 802.11 規格に含まれているものです。
- アソシエーション：AP と WLAN クライアントの間のデータ リンクを確立します。

ビーコンは AP によって定期的にブロードキャストされますが、プローブ、認証、およびアソシエーションの各フレームは、通常、アソシエーションと再アソシエーションのプロセス中に限り使用されます。

802.11 ビーコン

次の例は、*wpa1* という WLAN ネットワークの WLAN ビーコン デコードの一部を示しています。このビーコンでは、その WLAN のサービス セット識別子（ネットワーク名）、サポートされているビット レート、およびセキュリティ実装を確認できます。

ビーコンの主な目的は、WLAN クライアントが所定の領域で使用できるネットワークおよび AP を認識できるようにすることです。これにより、WLAN クライアントは、使用するネットワークおよび AP を選択できます。

（注） 多くの WLAN セキュリティ文書では、Service Set Identifier（SSID; サービス セット識別子）を含めずにビーコンを送信することが、WLAN ネットワークの SSID をハッカーに知られないようにするためのセキュリティ上のベスト プラクティスであるとしています。すべての企業 WLAN ソリューションは、これをオプションとして提供しています。ただし、SSID はアソシエーション フェーズで WLAN クライアントをスニフィングしている間に簡単に検出できるため、このオプションにはセキュリティ上の価値がほとんどありません。動作上の問題やクライアント サポートの問題に対応するため、SSID のブロードキャストを許可した方がよい場合が多くあります。選択する SSID は、企業のアイデンティティや WLAN の目的を識別しにくい、比較的あいまいなものである必要がありますが、同時に、できる限りユニークなものである必要があります。WLAN の目的や所有者を明かすような SSID を選択しないでください。SSID として、長いランダムな文字列を作成することはお勧めできません。それによって操作やメンテナンスのオーバーヘッドが増えるだけで、セキュリティはあまり向上しないためです。簡単な単語を使用することをお勧めします。SSID の偶発的または意図的な重複を避けるためのプロセスや規格が存在しないため、一般的な WLAN 関連の単語を使用しないでください。

次に、802.11 ビーコンの例を示します。

```
Type/Subtype: Beacon frame (8)
…
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    …
    Sequence number: 2577IEEE 802.11 wireless LAN management frame
    …
        SSID parameter set: "wpa1"
            Tag Number: 0 (SSID parameter set)
            Tag length: 4
            Tag interpretation: wpa1
        Supported Rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
…
        Vendor Specific: WPA
            Tag Number: 221 (Vendor Specific)
            Tag length: 28
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 2
```

```
                Tag interpretation: Unicast cipher suite 1: TKIP
                Tag interpretation: # of auth key management suites: 1
                Tag interpretation: auth key management suite 1: WPA
                Tag interpretation: Not interpreted
…
```

802.11 接続プロセス（アソシエーション）

802.11 クライアントは、WLAN ネットワーク経由でデータを送信する前に（高速ローミングはこのプロセスの例外ですが、このガイドでは説明しません）、次の 3 段階のプロセスを踏みます。

- 802.11 プロービング：802.11 ネットワークはさまざまなオプションを利用しますが、企業での展開の場合、特定のネットワークの検索で、ネットワーク名（SSID）とビット レートを指定するプローブ要求を複数のチャネルで送出する必要があります。
- 802.11 認証：802.11 は、本来 2 つの認証メカニズムで開発されました。「オープン認証」と呼ばれる最初のメカニズムは、基本的にヌル認証であり、クライアントが「私を認証して」と言うと、AP が「はい」と答えます。これは、ほとんどすべての 802.11 展開で使用されるメカニズムです。

  もう 1 つの認証メカニズムは共有 WEP キーに基づきますが、この認証方式の本来の実装には不備があります。全体的な規格準拠のためにこの方式を実装する必要がありますが、この方式は使用されず、推奨もされません。

  企業の WLAN 展開で使用される方式は、オープン認証だけです。前述のように、オープン認証は基本的にヌル認証であるため、「実際の認証」は 802.1X/EAP 認証メカニズムを使用して行われます。
- 802.11 アソシエーション：この段階で、セキュリティとビット レートのオプションを確定し、WLAN クライアントと AP の間でデータ リンクを確立します。

一般的な安全な企業 WLAN AP は、802.1X 認証が成功するまで、WLAN クライアント トラフィックを AP でブロックします。

クライアントがネットワークに接続し、ある AP からネットワーク内の別の AP にローミングする場合、そのアソシエーションは再アソシエーションと呼ばれます。アソシエーションと再アソシエーション イベントの主な違いは、再アソシエーション フレームが再アソシエーション要求で以前の AP の MAC アドレス（BSSID）を送信し、拡張 WLAN ネットワークにローミング情報を提供することです。

プローブ要求とプローブ応答

一般的な WLAN クライアント サプリカントには、必要な WLAN ネットワークが設定されています。つまり、WLAN クライアントからのプローブ要求には、必要な WLAN ネットワークの SSID が含まれています。この要求は、すべてのアソシエーション メッセージと同様に「暗号化しない状態で」送信されます。そのため、WLAN スニファは、ある領域でどの SSID がアクティブであるかを比較的容易に識別できます。

WLAN クライアントは、単に、利用可能な WLAN ネットワークを検出しようとしている場合、SSID を含めずにプローブ要求を送出できます。その場合、このタイプのクエリーに応答するよう設定されているすべての AP が応答します。

（注） ブロードキャスト SSID が有効になっていない WLAN は、応答しません。

次に、サンプル プローブ要求のセグメントを示します。ここでは、WLAN クライアントが特定の SSID（*wpa1*）で要求を送出しています。

```
IEEE 802.11 wireless LAN management frame
    Tagged parameters (31 bytes)
        SSID parameter set: "wpa1"
            ...
        Supported Rates: 1.0(B) 2.0(B) 5.5 11.0 6.0 9.0 12.0 18.0
```

```
            ...
        Extended Supported Rates: 24.0 36.0 48.0 54.0
            ...
```

次に、サンプル プローブ応答の一部を示します。ここでは、指定された SSID を使用する AP が、その WLAN SSID でサポートされているレートおよびセキュリティ プロパティで応答しています。

```
…
IEEE 802.11 wireless LAN management frame
…
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
   …
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 1
            Tag interpretation: Unicast cipher suite 1: TKIP
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: WPA
            Tag interpretation: Not interpreted
…
```

認証

次の例は、それぞれ「オープン」認証の要求および応答のフレームを示しています。デコードからわかるように、認証データは転送されていません。

- WLAN クライアントの認証要求：

```
…
    Type/Subtype: Authentication (11)
…
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Authentication Algorithm: Open System (0)
        Authentication SEQ: 0x0001
        Status code: Successful (0x0000)
```

- AP の認証応答：

```
…
    Type/Subtype: Authentication (11)
   …
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Authentication Algorithm: Open System (0)
        Authentication SEQ: 0x0002
        Status code: Successful (0x0000)
```

認証フレームに関連するもう 1 つのフレーム タイプは、認証解除フレームです。このフレームが WLAN クライアントに送信されると、そのクライアントは現在接続されている AP から切断されます。これにより、WLAN クライアントは、もう一度プローブ要求プロセス全体をやり直すか、または少なくとも認証 / アソシエーション プロセスをやり直すことになります。認証解除フレームをブロードキャスト MAC アドレスに送信し、そのフレームを送信している AP に関連付けられているすべてのクライアントを切断することができます。ただし、現在の WLAN クライアントの多くは、マルチキャスト認証解除フレームを無視して、このタイプの攻撃の潜在的な規模を縮小しています。

認証解除フレームはスプーフィングできるため、攻撃者はこのフレームを使用して、AP に対する DoS 攻撃（サービス拒絶攻撃）を作成したり、クライアントに再アソシエートを強制して、既知の状態でクライアントに対する攻撃を発生させたりできます。これが、CCX 機能セットの一部としてシスコが Management Frame Protection（MFP; 管理フレーム保護）を開発した理由の 1 つです。MFP については、P.4-18 の「管理フレーム保護」で詳しく説明します。

アソシエーション

次の各トレースでは、アソシエーションの要求フレームと応答フレームで、最終的なビットレートおよびセキュリティ パラメータが同意されています。これが正常に完了すると、WLAN クライアントと WLAN AP の間で 802.11 データ フレームを送信できます。企業の WLAN 展開では、802.1X/EAP 認証が完了して成功するまで、このデータ フレームは、WLAN クライアントと AP の間の 802.1X フレームに限定されます。

- WLAN クライアントのアソシエーション要求：

```
…
    Type/Subtype: Association Request (0)
    Frame Control: 0x0000 (Normal)
    Duration: 314
    Destination address: Airespac_52:42:d9 (00:0b:85:52:42:d9)
    Source address: IntelCor_7c:a3:47 (00:12:f0:7c:a3:47)
    BSS Id: Airespac_52:42:d9 (00:0b:85:52:42:d9)
    Fragment number: 0
    Sequence number: 90
    Frame check sequence: 0x1f17420d [correct]
IEEE 802.11 wireless LAN management frame
    Fixed parameters (4 bytes)
        Capability Information: 0x0431
        Listen Interval: 0x000a
    Tagged parameters (48 bytes)
        SSID parameter set: "wpa1"
            Tag Number: 0 (SSID parameter set)
            Tag length: 4
            Tag interpretation: wpa1
        Supported Rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
        Vendor Specific: WPA
            Tag Number: 221 (Vendor Specific)
            Tag length: 24
            Tag interpretation: WPA IE, type 1, version 1
            Tag interpretation: Multicast cipher suite: TKIP
            Tag interpretation: # of unicast cipher suites: 1
            Tag interpretation: Unicast cipher suite 1: TKIP
            Tag interpretation: # of auth key management suites: 1
            Tag interpretation: auth key management suite 1: WPA
            Tag interpretation: Not interpreted
        Extended Supported Rates: 24.0 36.0 48.0 54.0
            Tag Number: 50 (Extended Supported Rates)
            Tag length: 4
            Tag interpretation: Supported rates: 24.0 36.0 48.0 54.0  [Mbit/sec]
```

- AP のアソシエーション応答：

```
…
    Type/Subtype: Association Response (1)
    Frame Control: 0x0010 (Normal)
```

```
    Duration: 213
    Destination address: IntelCor_7c:a3:47 (00:12:f0:7c:a3:47)
    Source address: Airespac_52:42:d9 (00:0b:85:52:42:d9)
    BSS Id: Airespac_52:42:d9 (00:0b:85:52:42:d9)
    Fragment number: 0
    Sequence number: 1001
    Frame check sequence: 0x759406b6 [correct]
IEEE 802.11 wireless LAN management frame
    Fixed parameters (6 bytes)
        Capability Information: 0x0431
        Status code: Successful (0x0000)
        Association ID: 0x0001
    Tagged parameters (47 bytes)
        Supported Rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0(B) 6.0 9.0 12.0 18.0
[Mbit/sec]
        Extended Supported Rates: 24.0 36.0 48.0 54.0
            Tag Number: 50 (Extended Supported Rates)
            Tag length: 4
            Tag interpretation: Supported rates: 24.0 36.0 48.0 54.0  [Mbit/sec]
        Vendor Specific: Aironet Unknown
            Tag Number: 221 (Vendor Specific)
            Tag length: 29
            Aironet IE type: Unknown (12)
            Aironet IE data: 02C1257CF1AA1E0D010000A80200000000494C9788132233...
```

このアソシエーション プロセスには、関連するアソシエーション解除フレームもあります。このフレームは、WLAN クライアントを AP から切断するために使用できます。アソシエーション解除フレームは、必ずユニキャスト フレームです。そのため、このフレームが DoS 攻撃で使用される可能性は低くなりますが、このフレームによってクライアントの再アソシエートを引き起こすことができるため、既知の状態でクライアントに対する DoS 攻撃または攻撃を開始できます。

802.1X

802.1X はポート単位でアクセスを制御するための IEEE 規格です。認証されたユーザにのみ WLAN ネットワークへのアクセスを許可する手段として、802.11i セキュリティ ワークグループによって採用されました。

- 802.11 アソシエーション プロセスでは、各 WLAN クライアントの「仮想」ポートが AP に作成されます。
- AP は、802.1X ベース トラフィック以外のすべてのデータ フレームをブロックします。
- 802.1X フレームは EAP 認証パケットを伝送します。この認証パケットは、AP によって AAA サーバへ渡されます。
- EAP 認証に成功すると、AAA サーバは EAP 成功メッセージを AP へ送信します。このメッセージを受け取った AP は、該当する WLAN クライアントから仮想ポートへのデータ トラフィックを許可します。
- 仮想ポートを開く前に、認証された WLAN クライアントと AP 間のデータ リンクが暗号化されます。これは、特定のクライアントのために開いたポートへ他の WLAN クライアントがアクセスできないようにするためです。

Extensible Authentication Protocol

Extensible Authentication Protocol（EAP）は、認証プロトコルとそれを伝送するトランスポート プロトコルとの分離を定めている IETF RFC です。これらを分離することにより、EAP プロトコル自体を変更しなくても、802.1X、UDP、RADIUS などのトランスポート プロトコルを使用してこの認証プロトコルを伝送できます。

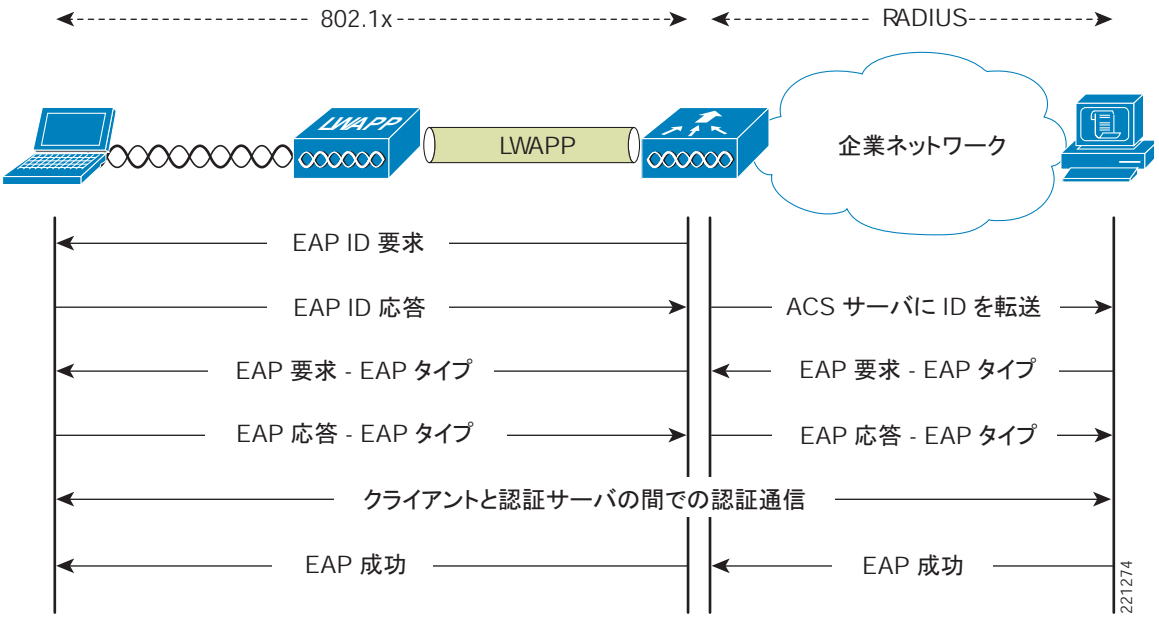
基本的な EAP プロトコルは比較的シンプルであり、次の 4 種類のパケットで構成されます。

- EAP 要求：要求パケットはオーセンティケータからサプリカントへ送信されます。要求パケットにはそれぞれ、要求内容（サプリカントの ID や使用する EAP タイプなど）を示すタイプ フィールドがあります。さらに、シーケンス番号を付けることで、オーセンティケータとピアは、各 EAP 要求に対応する EAP 応答を判別できます。
- EAP 応答：応答パケットはサプリカントからオーセンティケータへ送信されます。その際、どの EAP 要求に対する応答であるかを示すシーケンス番号が付与されます。否定応答（NAK）でない限り、通常、EAP 応答は EAP 要求に対応しています。
- EAP 成功：認証に成功すると、オーセンティケータからサプリカントへ成功パケットが送信されます。
- EAP 失敗：認証に成功しなかったときは、オーセンティケータからサプリカントへ失敗パケットが送信されます。

802.11i 準拠のシステムで EAP を使用すると、AP は EAP パススルー モードで動作します。つまり、コード フィールド、ID フィールド、長さフィールドをチェックした上で、クライアント サプリカントから受け取った EAP パケットを AAA へ転送します。同様に、オーセンティケータ（AP）は、AAA サーバから受け取った EAP パケットをサプリカントへ転送します。

図 3-3 は、EAP プロトコル フロー例を示しています。

図 3-3　　EAP プロトコル フロー



認証

それぞれの要求に応じて、PEAP、EAP-TLS、EAP-FAST などさまざまな認証プロトコルを使用して安全な無線展開を構築できます。どの認証プロトコルも、現在、基盤のトランスポートとして 802.1X、EAP、および RADIUS を使用しています。これらのプロトコルでは、認証に成功した WLAN クライアントだけがネットワークにアクセスできます。また、WLAN ネットワークをユーザが認証することも可能です。

このソリューションでは、RADIUS プロトコルで伝達されるポリシーに従ってアクセス権を付与したり、RADIUS アカウンティング処理を行うこともできます。

認証を実行するために使用する EAP タイプについては、この後で詳しく説明します。EAP プロトコルの選択に影響を与える主要因は、現在使用している認証システム（AAA）です。理想的なのは、新しい認証システムを導入するのではなく、既存の認証システムを利用して安全な WLAN 展開を構築することです。

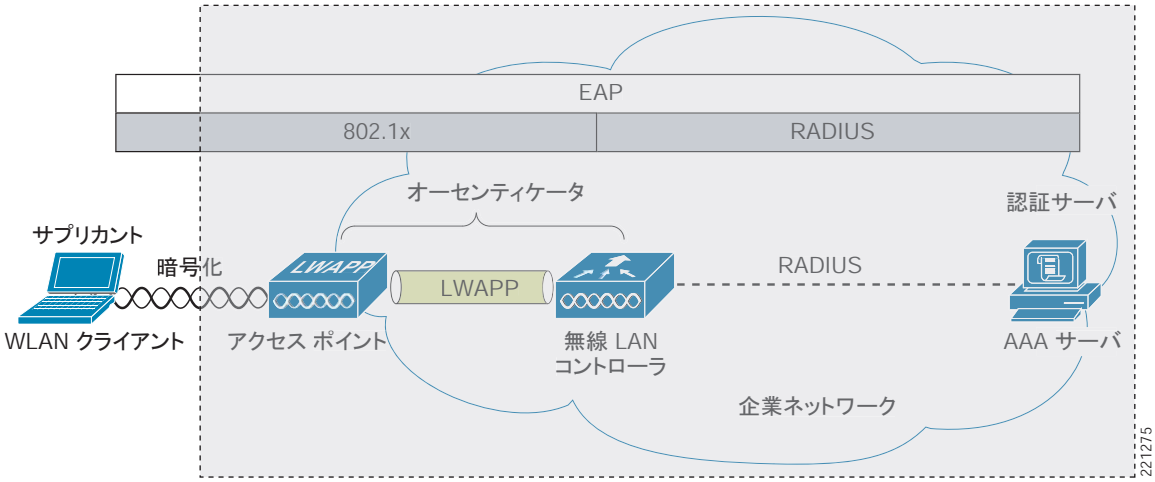
サプリカント

802.1X では、WLAN 認証で使用するクライアント ソフトウェアを「サプリカント」と呼んでいます。Cisco Secure Services Client（CSSC）5.1 は有線ネットワークと無線ネットワークをサポートしており、一般的なすべての EAP に対応しているサプリカントです。WLAN NIC メーカーがサプリカントを提供する場合や、オペレーティング システムにサプリカントが組み込まれている場合もあります。たとえば、Windows XP は PEAP MSCHAPV2 と EAP-TLS をサポートしています。

CSSC の詳細については、
http://www.cisco.com/en/US/prod/collateral/wireless/ps6442/ps7034/product_data_sheet0900aecd805081a7.html を参照してください。

図 3-4 は、認証アーキテクチャ全体におけるサプリカントの位置付けを示しています。サプリカントの役割は、アップストリームのオーセンティケータ（この場合は WLC）に対して、EAP および 802.1X を使用したエンド ユーザ認証を中継することです。サプリカントから EAP メッセージを受け取ったオーセンティケータは、RADIUS を使用して、それらのメッセージを AAA サーバへ転送します。

図 3-4　WLAN クライアント サプリカント



現在、各種の認証ソリューションや顧客のプライオリティを反映したさまざまな EAP サプリカントが市販されています。

表 3-2 は、一般的な EAP サプリカントの機能をまとめたものです。

- PEAP MSCHAPv2：Protected EAP MSCHAPv2。Transport Layer Security（TLS）トンネル（SSL の IETF 標準）を使用して、WLAN クライアントと認証サーバ間のカプセル化 MSCHAPv2 交換を保護します。
- PEAP GTC：Protected EAP Generic Token Card（GTC）。TLS トンネルを使用して、汎用トークン カード交換（ワンタイム パスワードや LDAP 認証など）を保護します。
- EAP-FAST：EAP-Flexible Authentication via Secured Tunnel。PEAP の場合と同様のトンネルを使用します。ただし、PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）は必要ありません。
- EAP-TLS：EAP Transport Layer Security。PKI を使用して、WLAN ネットワークと WLAN クライアントの両方を認証します。クライアント証明書と認証サーバ証明書が必要です。

表 3-2　一般的な各種サプリカントの比較

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
シングル サインオン（MSFT AD のみ）	あり	あり	あり[1]	あり
ログイン スクリプト（MSFT AD のみ）	あり	あり	一部	あり[2]
パスワード変更（MSFT AD）	あり	あり	あり	N/A
Microsoft AD データベースのサポート	あり	あり	あり	あり
ACS ローカル データベースのサポート	あり	あり	あり	あり
LDAP データベースのサポート	あり[3]	なし	あり	あり
OTP 認証のサポート	あり[4]	なし	あり	なし
RADIUS サーバ証明書の必要性	なし[5]	あり	あり	あり
クライアント証明書の必要性	なし[6]	なし	なし	あり
匿名性	あり	あり[7]	あり[8]	なし

1. サプリカントによって異なります。
2. このスクリプトをサポートするには、マシン アカウントとマシン認証が必要です。
3. LDAP データベースを使用する場合は自動プロビジョニングがサポートされません。
4. サプリカントによって異なります。
5. EAP-FAST によってサポートされており、フェーズ 0 のプロビジョニング脆弱性に対応します。
6. EAP-FAST によってサポートされており、フェーズ 0 のプロビジョニング脆弱性に対応します。
7. サプリカントによって異なります。
8. サプリカントによって異なります。

オーセンティケータ

Cisco Secure Wireless ソリューションの場合、オーセンティケータは無線 LAN コントローラ（WLC）です。この WLC は、802.1X ベース サプリカントと RADIUS 認証サーバ間でやり取りされる EAP メッセージのリレーとして動作します。

認証に成功すると、WLC は次の情報を受け取ります。

- EAP 成功メッセージが含まれている RADIUS パケット
- EAP 認証時に認証サーバによって生成された暗号キー
- 通信ポリシーに関する RADIUS Vendor-Specific Attribute（VSA; ベンダー固有属性）

図 3-5 は、認証アーキテクチャ全体における「オーセンティケータ」の論理的位置付けを示しています。オーセンティケータは 802.1X プロトコルを使用してネットワーク アクセスを制御し、サプリカントと認証サーバ間で EAP メッセージを中継します。

図 3-5　　オーセンティケータの位置付け

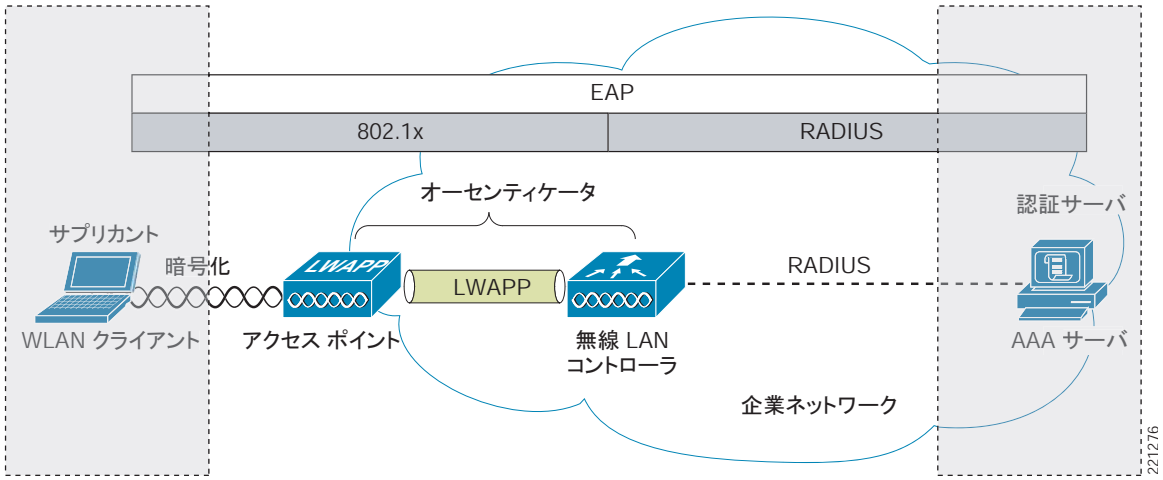


表 3-3 に、EAP-TLS 認証のデコード例を示します。左側の 4 列は無線 802.1X デコードです。右側の 3 列は、同じ EAP-TLS 認証の RADIUS トランザクションを表しています。

EAP 交換シーケンスは次のとおりです。

- AP がクライアントに対して、クライアント ID を要求するパケット #1 を送信します。これによって EAP 交換が開始されます。
- パケット #2 はクライアント ID です。このパケットは RADIUS サーバへ転送されます。この ID に基づいて、RADIUS サーバは EAP 認証を続行するかどうかを判断します。
- パケット #3 を送信し、RADIUS サーバは、認証の EAP 方式として PEAP を使用することを要求します。実際の要求は、RADIUS サーバで設定されている EAP の種類によって異なります。クライアントが PEAP 要求を拒否した場合、RADIUS サーバは他の種類の EAP を提案します。
- パケット #4 ～ 8 は PEAP の TLS トンネル セットアップです。
- パケット #9 ～ 16 は PEAP 内での認証交換です。
- パケット #17 は、認証に成功したことを知らせる EAP メッセージです。

  認証が成功したことをサプリカントとオーセンティケータに通知する以外に、パケット #17 は暗号キーと認証情報をオーセンティケータに伝送します。

表 3-3　　EAP トランザクション

#	送信元	送信先	プロトコル	情報	送信元	送信先	RADIUS 情報
1	AP	クライアント	EAP	要求、ID			
2	クライアント	AP	EAP	応答、ID	WLC	AAA	Access-Request(1)（id=114、l=174）
3	AP	クライアント	EAP	要求、PEAP	AAA	WLC	Access-challenge(11)（id=115、l=76）

表 3-3　EAP トランザクション （続き）

4	クライアント	AP	TLS[1]	Client Hello	WLC	AAA	Access-Request(1)（id=116、l=296）
5	AP	クライアント	TLS	Server Hello、証明書	AAA	WLC	Access-challenge(11)（id=116、l=968）
6	クライアント	AP	TLS	Client Key Exchange、Change Cipher Spec、暗号化されたハンドシェイク メッセージ	WLC	AAA	Access-Request(1)（id=117、l=528）
7	AP	クライアント	TLS	Change Cipher Spec、暗号化されたハンドシェイク メッセージ	AAA	WLC	Access-challenge(11)（id=117、l=145）
8	クライアント	AP	EAP	応答、PEAP	WLC	AAA	Access-Request(1)（id=118、l=196）
9	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-challenge(11)（id=118、l=135）
10	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Request(1)（id=119、l=270）
11	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-challenge(11)（id=119、l=151）
12	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Request(1)（id=120、l=334）
13	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-challenge(11)（id=120、l=162）
14	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Request(1)（id=121、l=265）
15	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-challenge(11)（id=121、l=114）
16	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Request(1)（id=122、l=265）
17	AP	クライアント	EAP	成功	AAA	WLC	Access-Accept(2)（id=122、l=196）

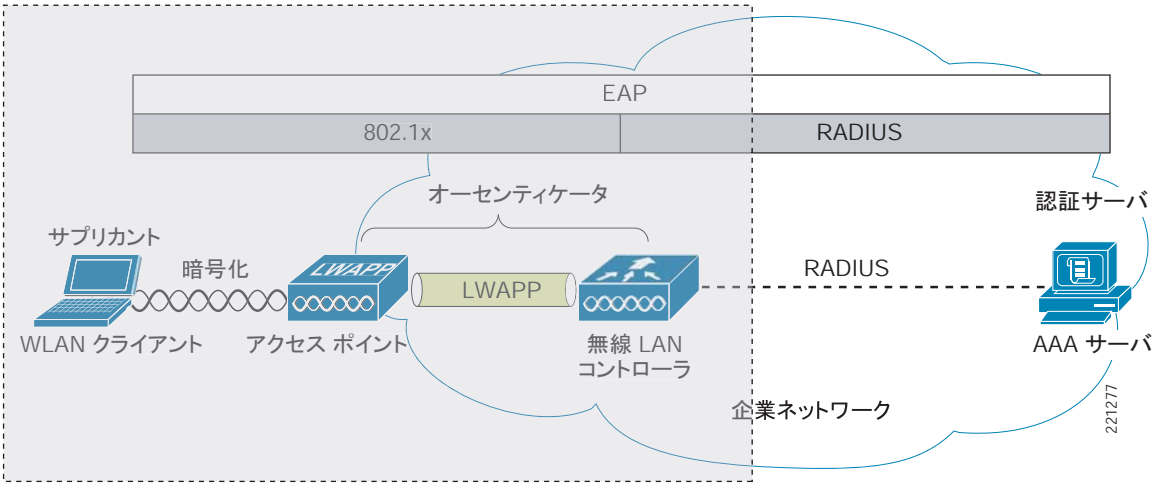
1. TLS トランザクションは EAP パケットとして伝送されます。

認証サーバ

Cisco Secure Wireless ソリューションで使用する認証サーバは Cisco Access Control Server（ACS）です。Cisco ACS は、Windows 2000 サーバまたは Windows 2003 サーバにソフトウェアとしてインストールされている場合と、アプライアンスとして提供される場合があります。また、特定の WLAN インフラストラクチャ デバイスに認証サーバ機能を実装することもできます。たとえば、IOS AP にローカル認証サービスを追加する、WLC でローカル EAP 認証をサポートする、AAA サーバで必要なタイプの EAP をサポートするなどの方法があります。

図 3-6 は、無線認証アーキテクチャ全体における認証サーバの論理的位置付けを示しています。この場合、認証サーバは、RADIUS トンネル経由で EAP 認証を実行します。

図 3-6　　認証サーバの位置付け



EAP 認証に成功すると、認証サーバは EAP 成功メッセージをオーセンティケータへ送信します。このメッセージは EAP 認証プロセスが成功したことをオーセンティケータに通知し、同時に Pairwise Master Key（PMK）をオーセンティケータに渡します。WLAN クライアントと AP 間のその後の通信では、この PMK を基にして暗号化ストリームが作成されます。次に、RADIUS での EAP 成功メッセージのデコード例を示します。

```
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7a (122)
    Length: 196
    Authenticator: 1AAAD5ECBC487012B753B2C1627E493A
    Attribute Value Pairs
        AVP: l=6  t=Framed-IP-Address(8): Negotiated
        AVP: l=6  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Success (3)
                Id: 12
                Length: 4
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=6  t=User-Name(1): xxxxxxx
        AVP: l=24  t=Class(25): 434143533A302F313938662F63306138336330322F31
        AVP: l=18  t=Message-Authenticator(80): 7C34BA45A95F3E55425FDAC301DA1AD7
```

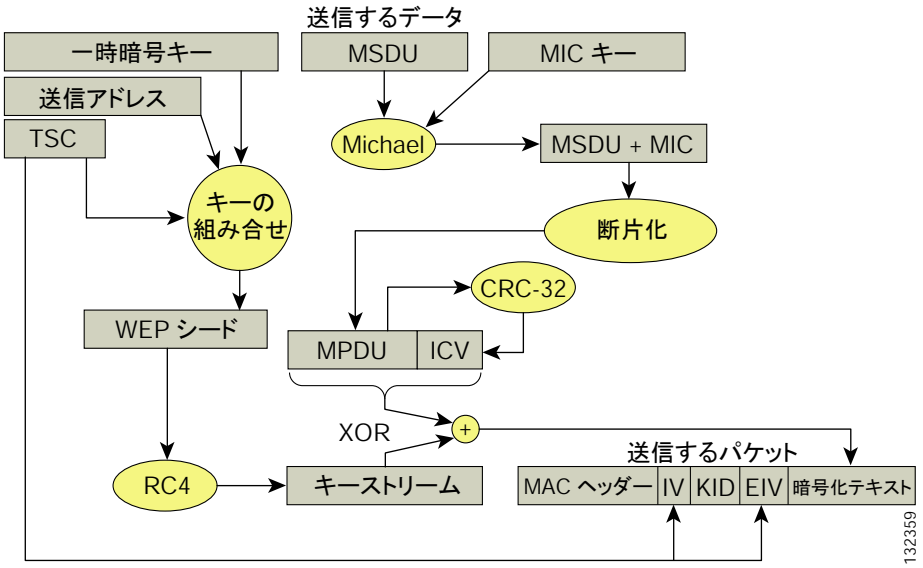
暗号化

802.11i では企業レベルの 2 つの暗号メカニズム Temporal Key Integrity Protocol（TKIP）と Advanced Encryption Standard（AES）が規定されており、これらは Wi-Fi Alliance によって WPA および WPA2 として認定されています。

TKIP は、WPA として認定されている暗号方式です。これまで指摘されていた 802.11 WEP 暗号方式の脆弱性が改善されており、従来と同じ RC4 コア暗号化アルゴリズムを採用しているので、既存の WLAN 装置にも対応しています。WEP の既知の弱点をすべて克服しており、さらに WLAN クライアント デバイスを新しくする必要がないことから、しばらくは TKIP（WPA）が主流となることでしょう。ただし、WPA2 の AES 暗号の方が、IT 業界の規格や基準により柔軟に対応できます。

図 3-7 は TKIP の基本フロー図です。

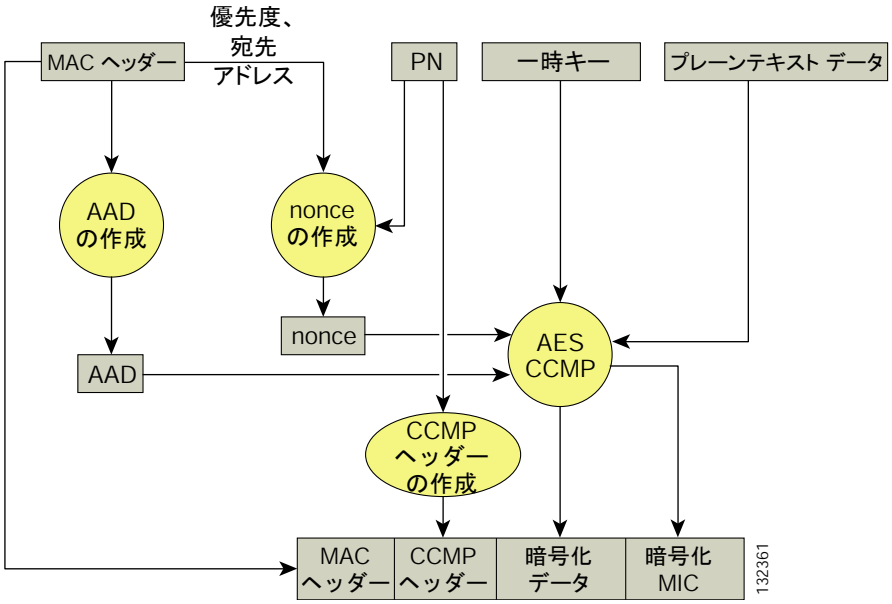
図 3-7　　WPA TKIP



TKIP には 2 つの大きな役割があります。1 つは、MAC Service Data Unit（MSDU; MAC サービス データ ユニット）の RC4 暗号を使用してパケットごとにキーを生成すること。もう 1 つは、暗号化されたパケットの Message Integrity Check（MIC; メッセージ完全性チェック）を実行することです。パケットごとのキーは、送信アドレス、初期化ベクトル（IV）、および暗号キーのハッシュです。フレーム送信のたびに IV が変わるので、RC4 暗号で使用されるキーはフレームごとに異なります。Michael アルゴリムを使用して MIC キーとユーザ データが結合され、MIC が生成されます。Michael は、演算オーバーヘッドが小さく、高いパフォーマンスを得られるアルゴリズムですが、攻撃を受けやすいという欠点もあります。そのため WPA では、WLAN クライアントを一時的に切断し、60 秒間は新しいキー ネゴシエーションを行えなくする予防措置がとられています。ただし、この動作自体が一種の DoS 攻撃となる可能性があります。多くの WLAN 実装は、必要に応じて、この対抗機能を無効できるようになっています。

図 3-8 は、基本的な AES counter mode/CBC MAC Protocol（CCMP）のフロー図です。CCMP は AES 暗号モードの 1 つであり、カウンタ モードは機密性を実現し、CBC MAC はメッセージの完全性を維持します。

図 3-8　WPA2 AES CCMP



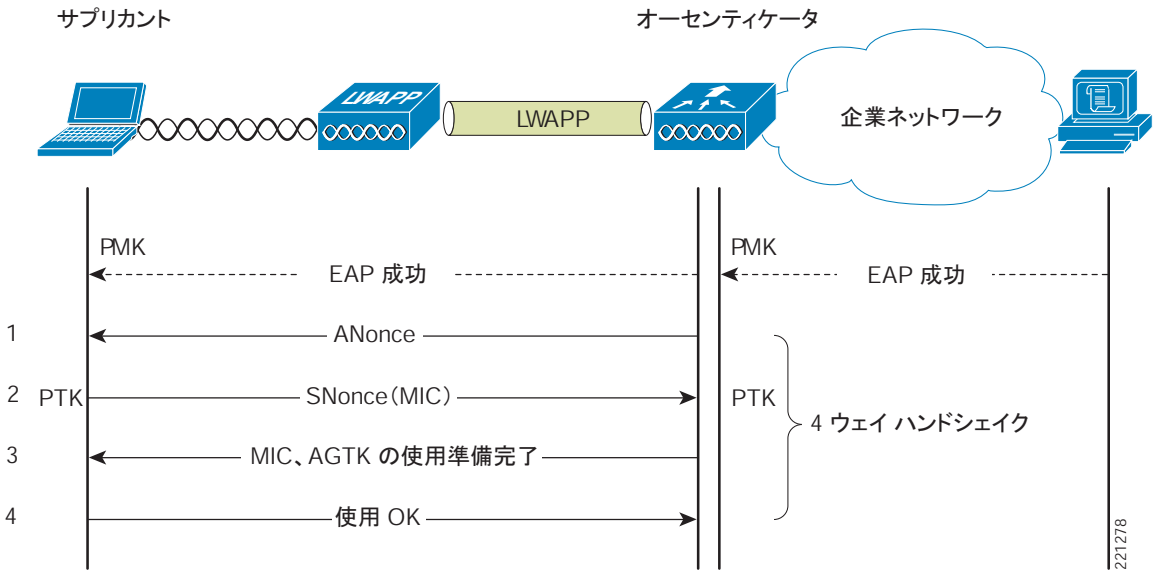
CCMP 手順では、追加の認証データ（AAD）が MAC ヘッダーから取得され、CCM 暗号化プロセスに組み込まれます。これによってフレームが保護され、フレーム内の非暗号化部分の改ざんを防ぎます。

リプレイ アタックを防ぐため、連続したパケット番号（PN）が CCMP ヘッダーに追加されます。この PN と MAC ヘッダーの各部を使用してナンスが生成され、さらにこのナンスが CCM 暗号化プロセスで使用されます。

4 ウェイ ハンドシェイク

4 ウェイ ハンドシェイクは、無線データ フレームの暗号化で必要となる暗号キーを生成するための方式です。図 3-9 は、暗号キー生成時のフレーム交換を示しています。これらのキーを「一時キー」といいます。

図 3-9　　4 ウェイ ハンドシェイク



暗号化に必要なキーは、EAP 認証セクションで生成した PMK に基づいて作成されます。この PMK は EAP 成功メッセージとしてオーセンティケータに送信されますが、サプリカントには転送されません。サプリカントは PMK を独自に生成するためです。

1. オーセンティケータは、Authenticator Nonce（ANounce; オーセンティケータ ナンス）を含む EAPOL-Key フレームを送信します。ANonce は、オーセンティケータにより生成される乱数です。
   a. サプリカントは、ANonce および SNonce（サプリカント ナンス。クライアントおよびサプリカントにより生成される乱数）から Pairwise Temporal Key（PTK）を生成します。
2. サプリカントは、SNonce、（再）アソシエーション要求フレームの RSN 情報エレメント、および MIC を含む EAPOL-Key フレームを送信します。
   a. オーセンティケータは ANonce と SNonce を基にして PTK を生成し、EAPOL-Key フレームの MIC を検証します。
3. オーセンティケータは、ANonce（ビーコンまたはプローブ応答メッセージから取得した RSN 情報エレメント）、MIC（一時キーをインストールするかどうかを決定）、およびカプセル化されたグループ一時キー（GTK）（マルチキャスト暗号キー）を含む EAPOL-Key フレームを送信します。
4. サプリカントは EAPOL-Key フレームを送信して、一時キーがインストールされているかどうかを確認します。

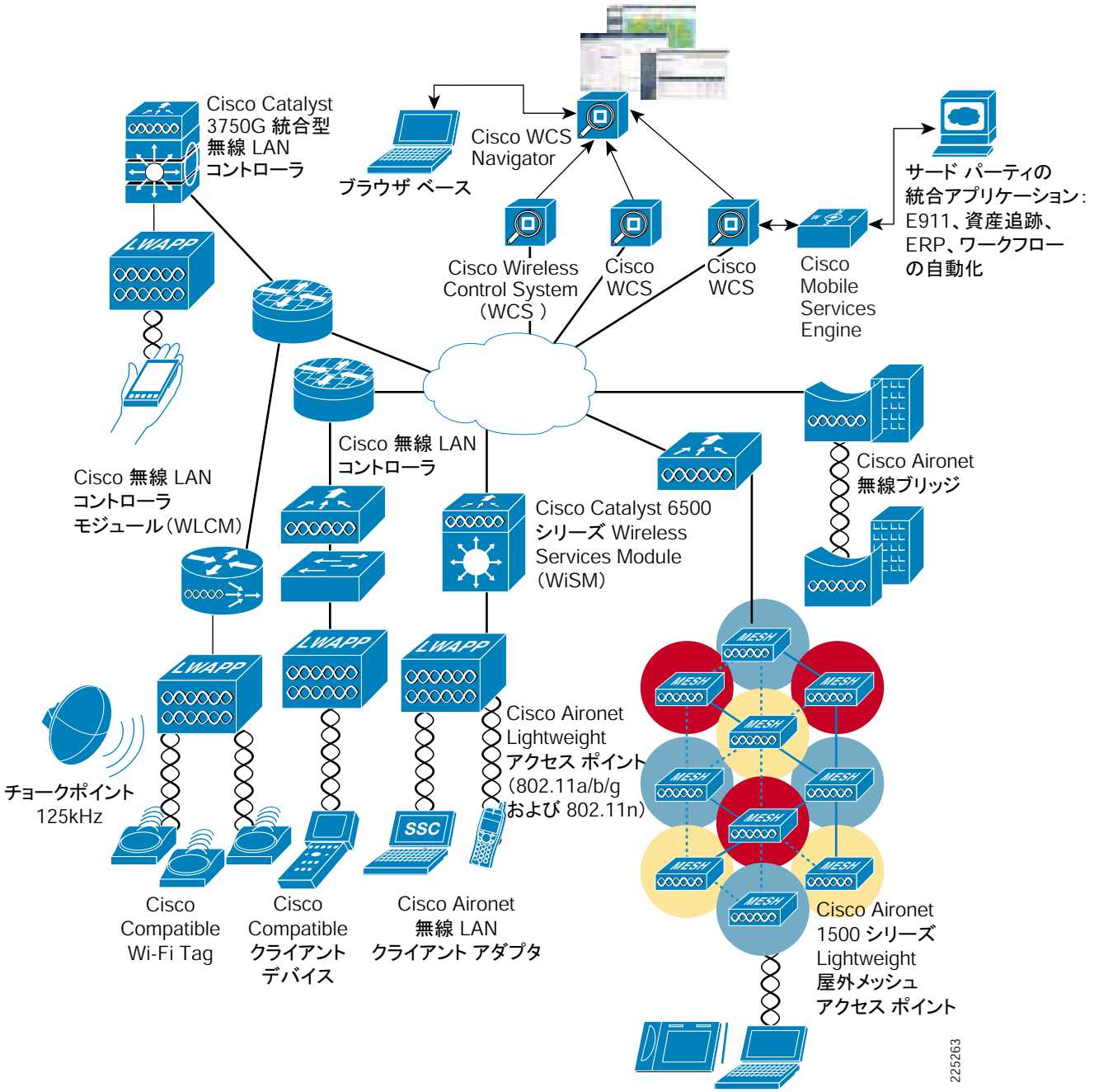
CHAPTER 4

Cisco Unified Wireless Network アーキテクチャ：基本的なセキュリティ機能

Cisco Unified Wireless Network ソリューションは 802.11 のセキュリティ機能を基に設計されており、RF、802.11、およびネットワークベースのセキュリティ機能を強化することで全体的なセキュリティ強化を図っています。802.11 規格には無線媒体のセキュリティが盛り込まれていますが、さらに、Cisco Unified Wireless Network ソリューションではシステム全体のエンドツーエンド セキュリティを実現するため、アーキテクチャと製品のセキュリティ機能を利用し、WLAN エンドポイント、WLAN インフラストラクチャ、クライアント通信、基幹有線ネットワークを保護します。

図 4-1 は Cisco Unified Wireless Network アーキテクチャ構成の概略図です。このアーキテクチャは、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）アクセス ポイント（LAP）、メッシュ LWAPP AP（MAP）、Wireless Control System（WCS）、および Wireless LAN Controller（WLC; 無線 LAN コントローラ）で構成されています。Wireless LAN Controller Module（WLCM; 無線 LAN コントローラ モジュール）または Wireless Services Module（WiSM）で WLC プラットフォームを構成することもできます。さらに、Cisco Access Control Server（ACS）とその Authentication/Authorization/Accounting（AAA; 認証、認可、アカウンティング）機能によって、無線ユーザの認証と認可を行う RADIUS サービスを提供します。

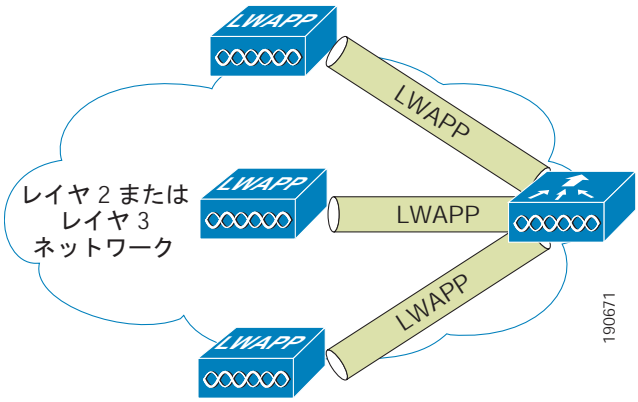
図 4-1　Cisco Unified Wireless Network アーキテクチャ



Cisco Unified Wireless Network アーキテクチャ

図 4-2 はこのアーキテクチャの主要機能です。Lightweight アクセス ポイント プロトコル（LWAPP）アクセス ポイント（LAP）が、LWAPP プロトコルを使用して WLC と通信し、トラフィックをトンネル処理する仕組みを示しています。

図 4-2　　LAP と WLC の接続



LWAPP には 3 つの主要機能があります。

- LAP を制御および管理する
- WLAN クライアント トラフィックを WLC へトンネリングする
- Cisco Unified Wireless System の管理に必要な 802.11 データを収集する

LWAPP の機能

システムの展開と管理が簡単であるほど、そのシステムのセキュリティ管理も容易になります。「重い」AP（Autonomous AP またはインテリジェント AP）を使用していた初期の WLAN システムの場合、AP の導入と設定は、何百ものファイアウォールをそれぞれ個別に設置し、管理することを意味していました。最新のファームウェアがインストールされているか、設定は適切か、セキュリティ対策に問題はないかを常に気にしていなければならなかったのです。さらに、AP は物理的に安全でない領域に設置されることが多く、AP が盗まれ、その情報が漏れると、また別の不正行為に発展する可能性があります。

LWAPP は、展開、設定、および物理的セキュリティの問題に次のように対処します。

- AP の操作と管理はユーザが直接行いません。LWAPP 接続を介して WLC が AP を管理します。これにより、設定機能とファームウェア機能が WLC に移行し、WCS による集中管理が可能になります。
- AP は自身の設定を WLC からダウンロードします。また、WLC で設定が変更されたときは、AP が自動的に更新されます。
- AP のファームウェアを WLC と同期させ、常に適切なバージョンのファームウェアが実行されるようにします。
- 重要な設定データを WLC に保存し、AP には IP アドレス情報のみを保存します。AP に物理的問題が発生した場合でも、NVRAM には設定情報が保存されていないので、悪用される心配がありません。
- LAP と WLC は互いに認証し、AES によって LWAPP 制御チャネルを暗号化します。

LWAPP によって提供される物理的なセキュリティ、ファームウェア、および設定管理の強化点に加え、LWAPP ベース アーキテクチャにおける WLAN トラフィックのトンネリングにより、ソリューション全体のセキュリティを損なうことなく、より簡単な導入が実現されます。アクセス スイッチで dot1q トランキングを設定したり、クライアント サブネットを追加したりしなくても、複数の WLAN VLAN をサポートする LAP をアクセス レイヤ スイッチに配備できます。すべての WLAN クライアント トラフィックはトンネル経由で（WLC が配置されている）中央サイトへ送信されるので、WLAN のアクセスとセキュリティに関するポリシーを企業レベルで容易に導入できます。

Cisco Unified Wireless のセキュリティ機能

802.11 のセキュリティ機能に物理的なセキュリティを追加し、展開の容易な LWAPP アーキテクチャを採用すれば、WLAN 展開のセキュリティ全体が向上します。上記で説明した LWAPP プロトコル自体のセキュリティ機能に加え、Cisco Unified Wireless ソリューションには次のセキュリティ機能が備わっています。

- 機能強化された WLAN セキュリティ オプション
- ACL 機能とファイアウォール機能
- Dynamic Host Configuration Protocol（DHCP）と Address Resolution Protocol（ARP; アドレス解決プロトコル）による保護
- ピアツーピア ブロッキング
- 無線 Intrusion Detection System（IDS; 侵入検知システム）
- クライアントの除外
- 不正 AP 検出
- 管理フレーム保護
- 動的な無線周波数管理
- アーキテクチャ統合
- IDS 統合

機能強化された WLAN セキュリティ オプション

Cisco Unified Wireless Network ソリューションはさまざまな WLAN セキュリティ オプションをサポートしています。たとえば、WLC で複数の WLAN を作成し、従来のプラットフォームではオープン ゲスト WLAN ネットワークや WEP ネットワークを使用して、それ以外では WPA と WPA2 セキュリティ設定を組み合せるなど、それぞれ異なる WLAN セキュリティ設定を使用できます。

各 WLAN SSID は、WLC 上の同じ dot1q インターフェイスまたは異なる dot1q インターフェイスに割り当てることができます。また、モビリティ アンカー接続を介して、別のコントローラへ Ethernet over IP（EoIP）トンネルで伝送できます。

WLAN クライアントが 802.1X で認証される場合、WLC に渡される RADIUS アトリビュートによって dot1q VLAN 割り当てを制御できます。

図 4-3 と図 4-4 は、Unified Wireless WLAN 設定画面の一部を示しています。このサンプル画面には、次の 3 つの設定項目が表示されています。

- WLAN SSID

- WLAN がマップされている WLC インターフェイス
- セキュリティ方式（その他の WPA オプションと WPA2 オプションも選択できますが、この図には表示されていません）

図 4-3　WLAN General タブ

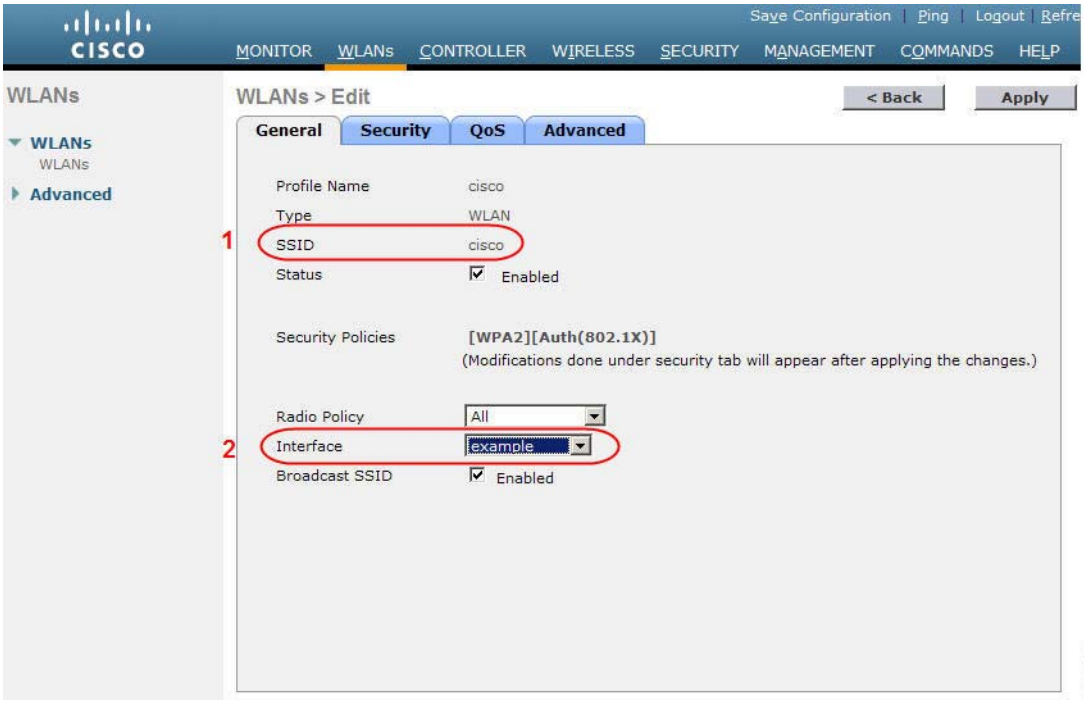
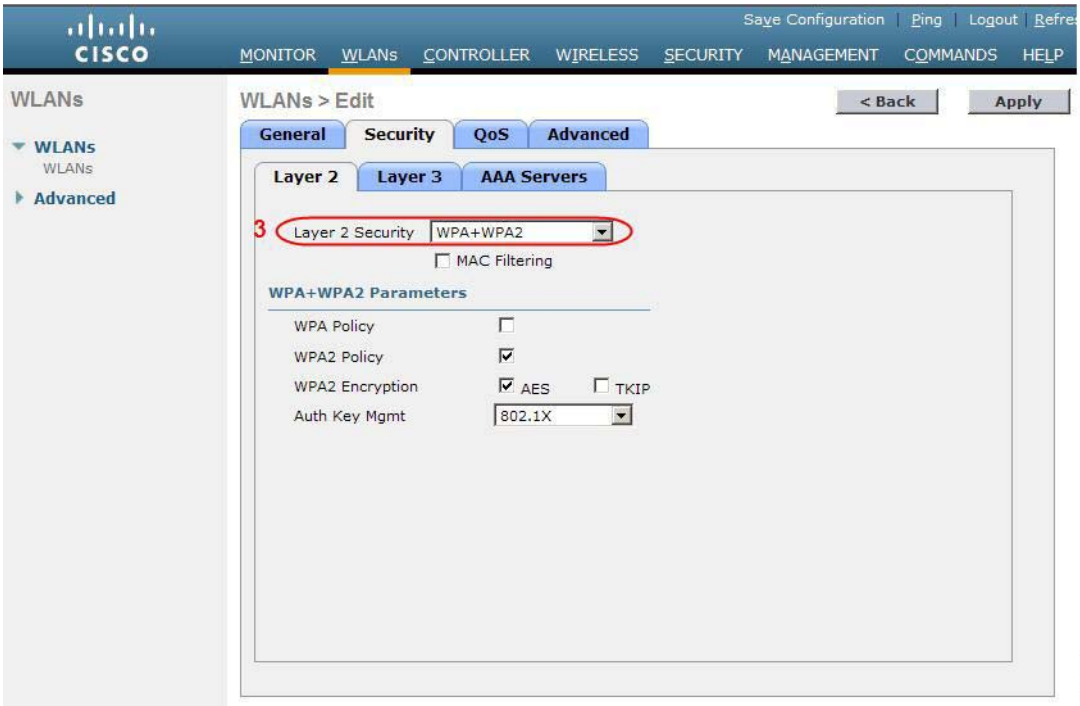


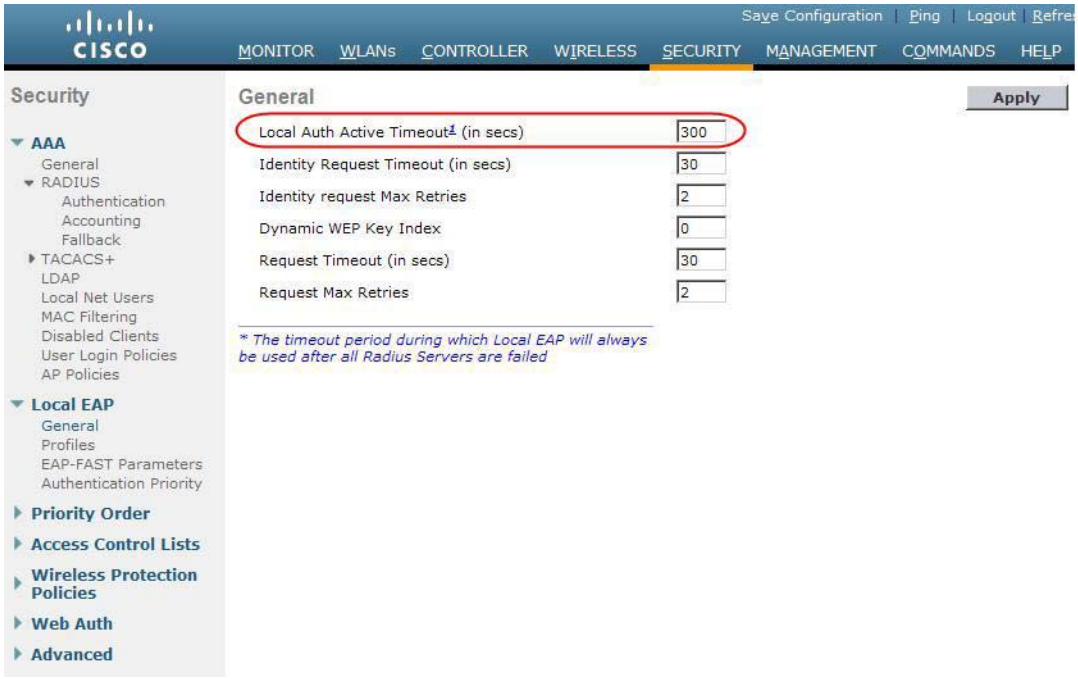
図 4-4　　WLAN Layer 2 Security タブ



ローカル EAP 認証

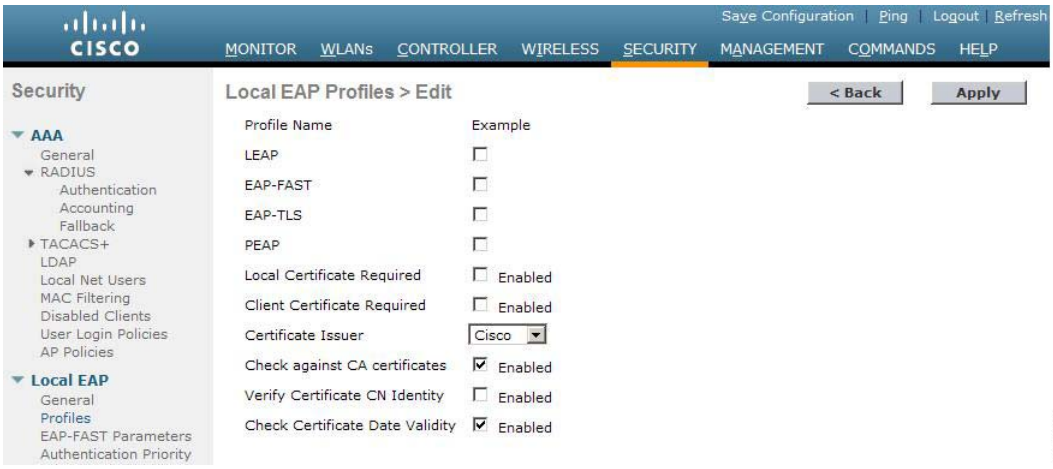
WLC コード リリース 5.0 にはローカル EAP 認証機能が備わっており、外部 RADIUS サーバが用意されていない場合や利用できなくなった場合に、この機能が役立ちます。図 4-5 に示すように、ローカル認証に切り替えるまでの遅延時間を指定できます。RADIUS サーバの機能が回復すると、ローカル認証から RADIUS サーバ認証へ自動的に切り替わります。

図 4-5　ローカル認証タイムアウト



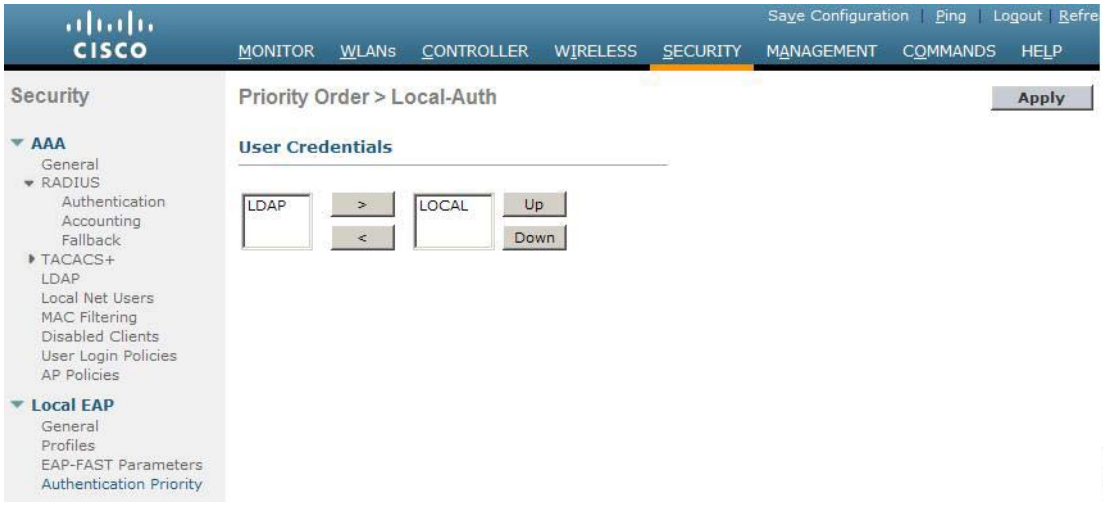
WLC でローカルにサポートされている EAP の種類は、LEAP、EAP-FAST、および EAP-TLS です。ローカル EAP のプロファイル例を図 4-6 に示します。

図 4-6　ローカル EAP のプロファイル



WLC は、ローカル データベースを使用してデータを認証できます。また、LDAP ディレクトリにアクセスして、EAP-FAST 認証または EAP-TLS 認証に必要なデータを取得することもできます。図 4-7 に示すように、LDAP サーバがローカル ネット ユーザのローカル認証データベースに対して持つプライオリティを設定できます。

図 4-7　　ローカル EAP の優先順位



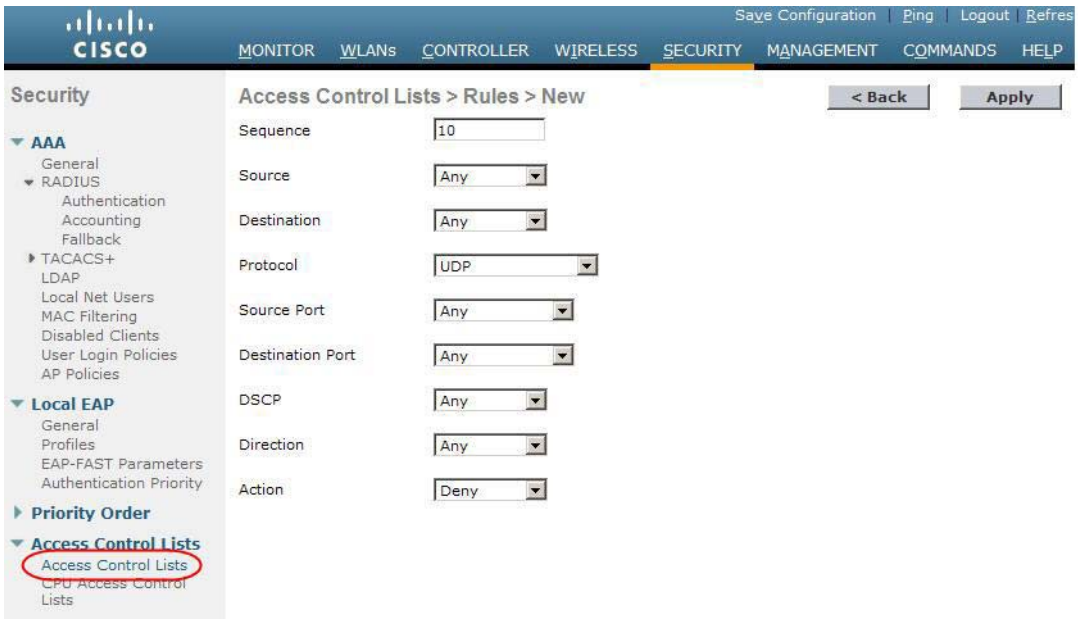
ACL 機能とファイアウォール機能

各 WLC で設定されているインターフェイスに対して、または WLC の CPU 自体に対して、Access Control List（ACL; アクセス コントロール リスト）を定義できます。これらの ACL を使用して特定の WLAN にポリシーを適用し、指定したアドレスやプロトコルへのアクセスを制限したり、WLC 自体の保護を強化したりできます。

インターフェイス ACL は、その ACL の適用対象となるインターフェイス経由でやり取りされる WLAN クライアント トラフィックを制御します。CPU ACL は、WLC 上のインターフェイスとは関係なく、WLC システムがやり取りするすべてのトラフィックに適用されます。

図 4-8 は ACL 設定ページを示しています。ACL では、転送元と転送先のアドレス範囲、プロトコル、転送元と転送先のポート、Differentiated Services Code Point（DSCP）、および ACL の適用方向を指定できます。さまざまな規則に基づいて ACL を作成できます。

図 4-8　　ACL の設定ページ



DHCP および ARP の保護

WLC は、WLAN クライアント DHCP 要求のリレー エージェントとして機能します。その際、WLC は、DHCP インフラストラクチャを保護するためのいくつかのチェックを実行します。中でも重要なのは、DHCP 要求に含まれている MAC アドレスが、その要求の送信元 WLAN クライアントの MAC アドレスと一致するかどうかを検証することです。これによって、それぞれのインターフェイスで、WLAN クライアントが 1 つの IP アドレスだけを要求できるため、DHCP 消耗攻撃を受けないようになります。WLC のデフォルト設定では、WLAN クライアントからのブロードキャスト メッセージを同じ WLAN に返送しないようになっています。これは、WLAN クライアントが DHCP サーバになりすまし、DHCP 情報を悪用するのを防ぐためです。

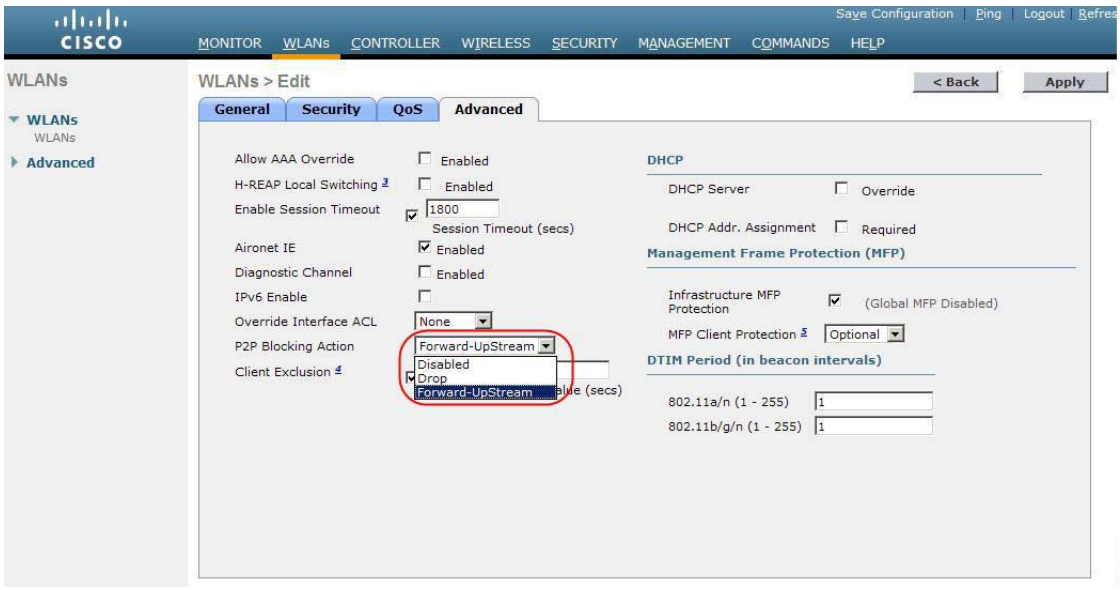
MAC アドレスと IP アドレスとの関連付けを管理する WLC は、WLAN クライアントの ARP プロキシとして機能します。したがって WLC は、重複する IP アドレスや ARP スプーフィング攻撃を阻止できます。WLC は、WLAN クライアント間の直接的な ARP 通信を許可しません。これもまた、WLAN クライアント デバイスを狙った ARP スプーフィング攻撃の防止に役立ちます。

ピアツーピア ブロッキング

WLC は、同じ WLAN 上でのクライアント間通信をブロックするように設定できます。その場合、必ずルータ経由で通信が行われるので、同じサブネット上でのクライアント間攻撃を防止できます。図 4-9 は、WLAN でのピアツーピア ブロッキングの設定を示しています。

（注）　これは、以前のコード リリースからの変更点です。以前のコード リリースでは、ピアツーピア ブロッキングは WLC のグローバル設定でした。

図 4-9　　ピアツーピア ブロッキング



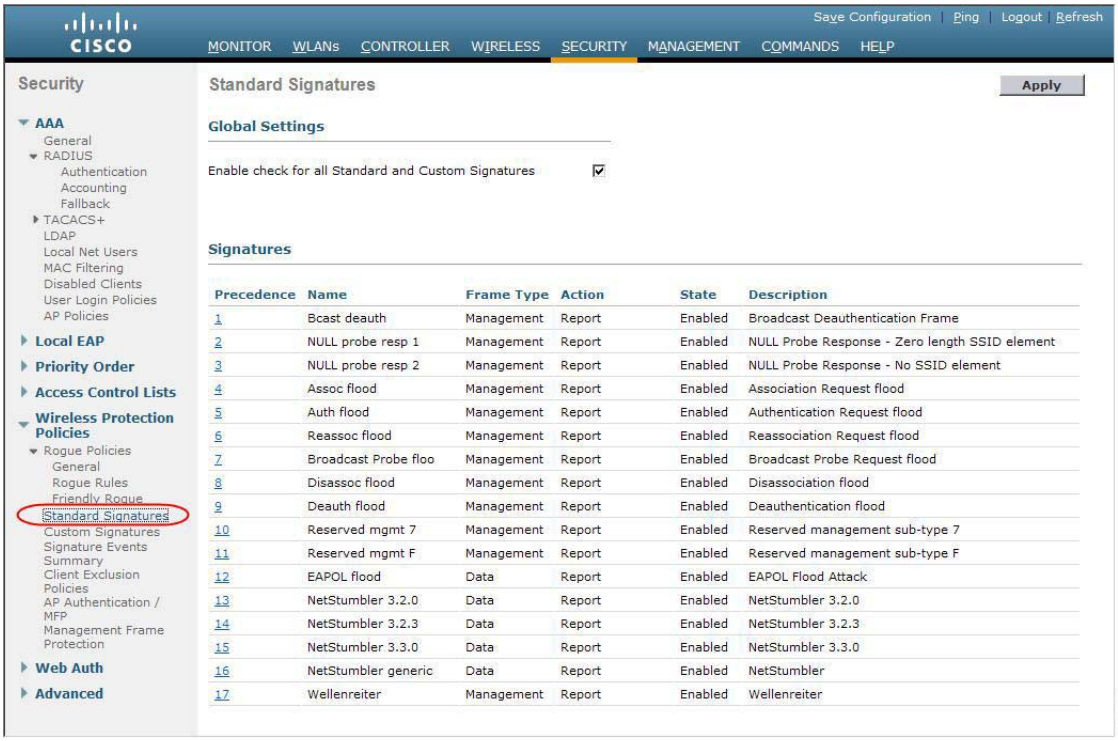
無線 IDS

WLC は、接続されているすべての AP を使用して WLAN IDS 分析を実行し、検出された攻撃を WLC および WCS に報告します。無線 IDS 解析は、有線ネットワーク IDS システムで一般的に実行される解析を補うための機能です。WLC に備わっている無線 IDS 機能は、有線ネットワーク IDS システムの対象とならない 802.11 および WLC 関連の情報を解析します。

WLC で使用されるシグニチャ ファイルは、WLC ソフトウェア リリースに含まれていますが、別のシグニチャ ファイルを使用して単独で更新される場合があります。カスタム シグニチャは、Custom Signatures ウィンドウに表示されます。

図 4-10 は、WLC の Standards Signatures ウィンドウを示しています。

図 4-10　　標準の WLAN IDS シグニチャ



モビリティ サービス エンジン

シスコ モビリティ サービス エンジンは、ソフトウェア スイートとしてプラットフォームに読み込まれる各種サービスをサポートするように設計されたプラットフォームです。

MSE で提供できるサービスは数多くありますが、例として、Context Aware ソフトウェア、Adaptive Wireless IPS、Mobile Intelligent Roaming、Secure Client Manager が挙げられます。これらの各サービスは、特定のアプリケーションの最適化のためにネットワークからのインテリジェンスを提供するよう設計されています。

表 4-1 は、これらのサービスの主な定義と機能をまとめたものです。

表 4-1　　モビリティ サービス ソフトウェア スイートの概要

	Context Aware	Adaptive Wireless IPS	Mobile Intelligent Roaming	Secure Client Manager
説明	ビジネス プロセスをコンテキスト（ロケーション、テレメトリなど）で最適化します。	統合された侵入防御により、無線の脅威を軽減します。	パブリック ネットワークとプライベート ネットワークの区別なく、モビリティ アプリケーションを提供します。	次々と登場する新しいモバイル デバイスに対応できるよう、デバイスのプロビジョニングと管理を簡略化します。

表 4-1 モビリティ サービス ソフトウェア スイートの概要 （続き）

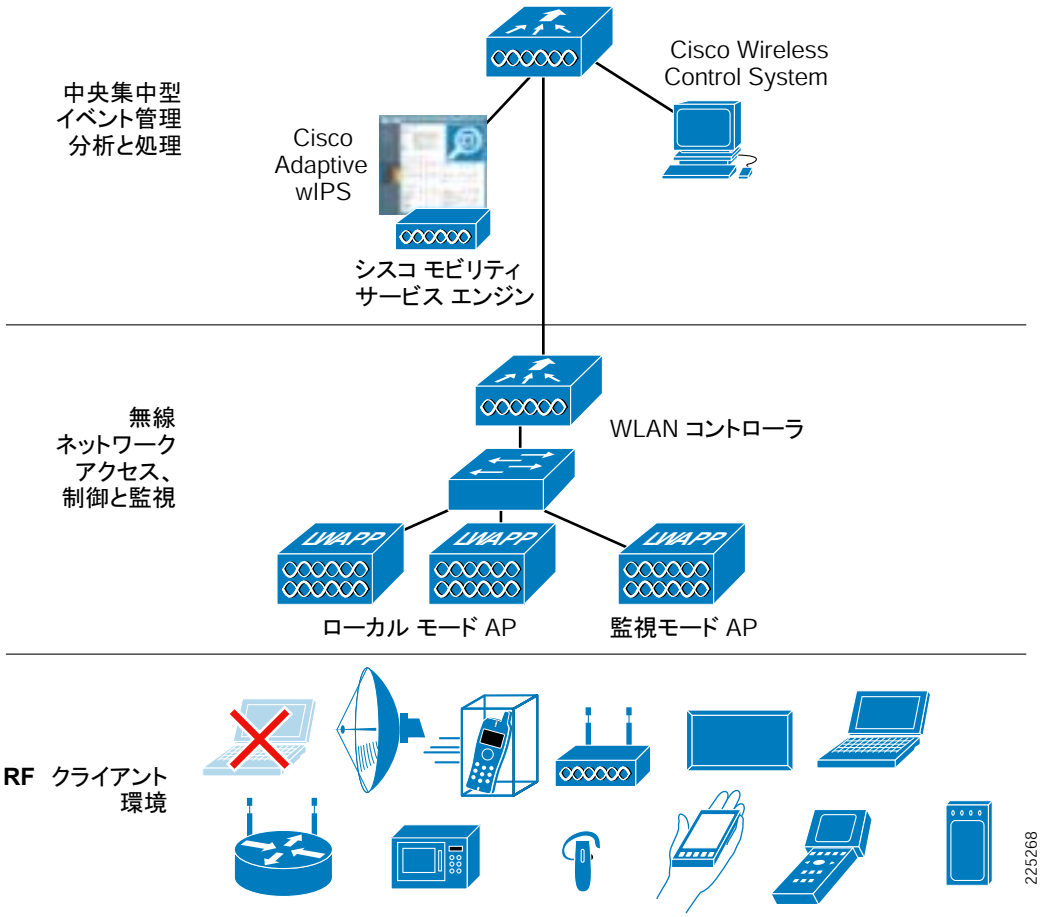
	Context Aware	Adaptive Wireless IPS	Mobile Intelligent Roaming	Secure Client Manager
アプリケーション	資産追跡 状態のモニタリング	適合認定：PCI、HIPAA、SOX	デュアル モードの音声およびデータ アプリケーション	安全な接続
主な業種	医療 製造	小売 金融サービス 医療	企業 医療 教育	小売 医療 企業

Adaptive Wireless IPS

Adaptive Wireless IPS は、モビリティ サービス エンジンの能力と位置を利用して、WLC Wireless IPS を超える保護を提供し、Cisco Unified Wireless Network 内のすべての発信元からの WLAN データを分析します。

シスコ モビリティ サービス エンジンは、分析処理のパフォーマンスとスケーラビリティ、履歴レポートとフォレンジックデータの保管機能、および場所 / 接続ベースの資産追跡やクライアント セキュリティ管理などのサービスの統合機能を備えています。モバイル ビジネス ネットワークの拡張に伴って、Cisco Adaptive Wireless IPS ソリューションは、増え続ける新しいデバイスとスペクトラムの用途を監視および分析し、重要な業務情報の継続的な保護を保証します。図 4-11 は、Cisco Adaptive Wireless IPS ソリューションを構成するコンポーネントを示しています。

図 4-11　Cisco Adaptive Wireless IPS ソリューションのコンポーネント

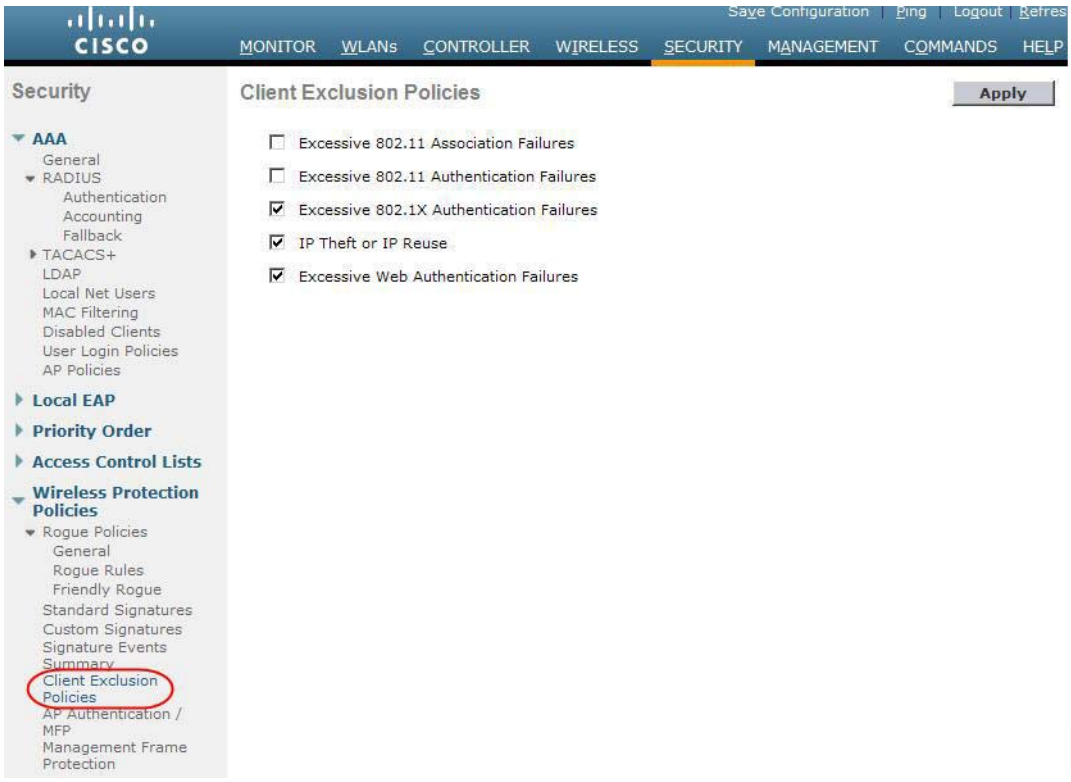


クライアントの除外

WLC には、無線 IDS 以外にも、WLAN インフラストラクチャと WLAN クライアントを保護するための機能が備わっています。WLC には、動作が不審な WLAN クライアントを除外するポリシーを実装できます。図 4-12 は Exclusion Policies ウィンドウを示しています。このウィンドウでは、現在サポートされている次のクライアント除外ポリシーを指定できます。

- Excessive 802.11 Association Failures：不審なクライアントまたは DoS 攻撃
- Excessive 802.11 Authentication Failures：不審なクライアントまたは DoS 攻撃
- Excessive 802.1X Authentication Failures：不審なクライアントまたは DoS 攻撃
- External Policy Server Failures：ネットワークベースの IPS サーバが除外するクライアントを特定
- IP Theft or IP Reuse：不審なクライアントまたは DoS 攻撃
- Excessive Web Authentication Failures：DoS 攻撃またはパスワードクラッキング攻撃

図 4-12　　クライアントの除外ポリシー

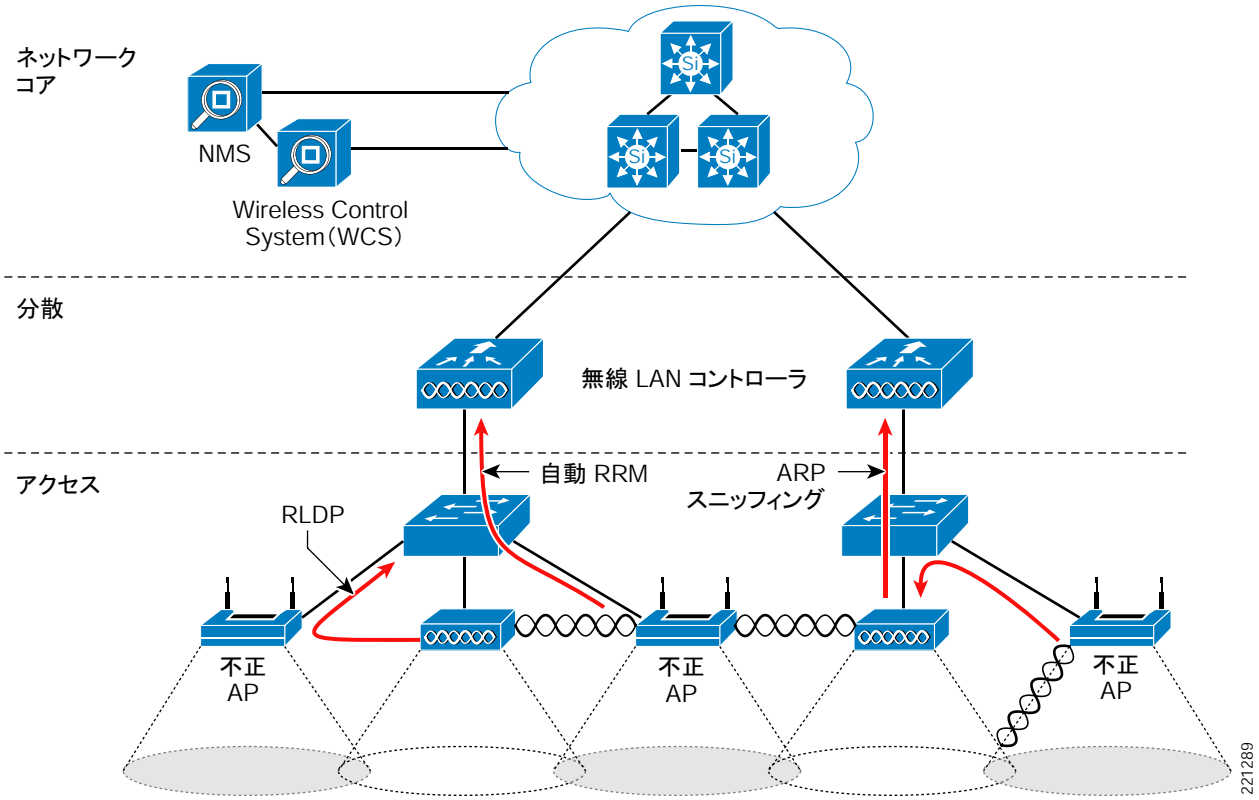


不正 AP

図 4-13 に示すように、Cisco Unified Wireless Networking ソリューションには徹底した不正 AP 対策が設けられています。具体的な機能は次のとおりです。

- 電波 /RF 検出：ビーコンおよび 802.11 プローブ応答を観測または傍受することによって、不正デバイスを検出します。
- 不正 AP の特定：検出された RF 特性および管理対象 RF ネットワークの既知のプロパティに基づいて、不正デバイスの所在を突き止めます。
- 有線検出：不正デバイスを追跡し、有線ネットワークとの関連性を特定します。
- 不正 AP の切り離し：不正 AP へのクライアント接続を阻止します。

図 4-13　不正な無線 AP の検出



電波 /RF 検出

AP RF 検出には、次の 2 つのモデルがあります。

- 標準の AP 配置
- 監視モード AP 配置

どちらの配置モデルも RF 検出をサポートしており、不正 AP だけでなく、アドホック クライアントと不正クライアント（不正 AP のユーザ）の検出に関する情報も収集できます。監視モードの AP は、RF チャネルのスキャン専用で、クライアント データを伝送しません。

不正 AP を探す場合、Unified Wireless AP はチャネルを 50 ms 間停止して不正クライアントの有無を調べ、ノイズとチャネル干渉を監視します（どのチャネルをスキャンするかは、802.11a および 802.11b/g のグローバル WLAN ネットワーク パラメータで設定します）。不正なクライアントやアクセス ポイントが検出されると、その情報がコントローラに送信されます。コントローラが収集する情報は次のとおりです。

- 不正 AP の MAC アドレス
- 不正 AP の名前
- 不正接続しているクライアントの MAC アドレス
- フレームが WPA または WEP で保護されているかどうか
- プリアンブル
- 信号対雑音比（SNR）

- 受信信号強度表示（RSSI）

不正情報を受け取った WLC は、問題のクライアントまたは AP をすぐには不正と見なさず、他の AP からも同様の報告があるか、次のサイクルが完了するまで様子を見ます。同じ AP が再度同じチャネルに移動して、不正アクセス ポイント、不正クライアント、ノイズ、および干渉を監視します。同じクライアントまたはアクセス ポイントが検出された場合、WLC はそれらを不正としてリストします。WLC は次に、この不正がローカル ネットワークに接続されているものか、あるいは単なる隣接 AP であるかを調べます。いずれの場合も、管理対象のローカル WLAN に含まれていない AP は、不正であると見なされます。

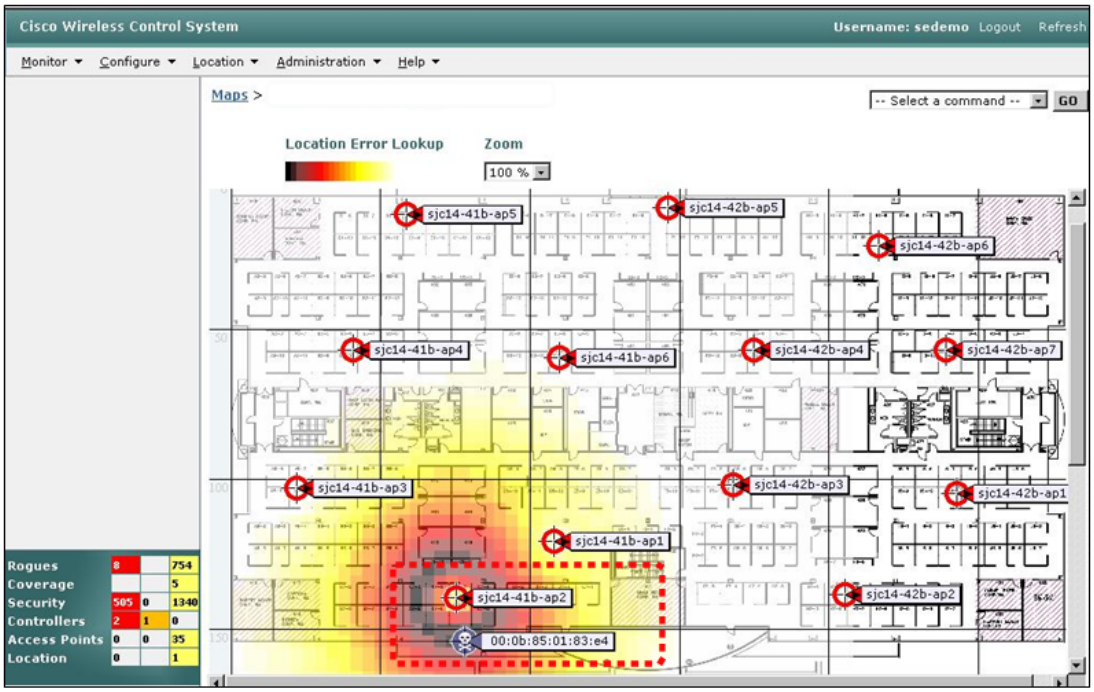
監視モードの AP はユーザ トラフィックを伝送せず、チャネル スキャン専用となります。ある特定の領域について WLAN サービスをサポートせず、不正 AP と不正クライアントの監視のみを行う場合は、通常、この配置モードを使用します。

位置特定

WCS の位置特定機能を使用すれば、不正 AP のおおよその位置を示すフロア図面を作成できます。この例を図 4-14 に示します。このフロア図面には、正規 AP の位置がすべて示されています。また、不正 AP の位置がどくろアイコンで強調表示されています。

Cisco Unified Wireless Location 機能の詳細については、
http://www.cisco.com/en/US/products/ps6386/index.html を参照してください。

図 4-14　　不正 AP マッピング



有線検出

AP が数台しかない支社のように、上記で説明した WCS 不正位置検出機能を利用できない場合もあれば、正確なフロア図面を入手できない場合もあります。そのような場合に備え、Cisco Unified Wireless ソリューションには、「有線」ベースの検出オプションも 2 つ用意されています。

- 不正検出用 AP
- Rogue Location Discovery Protocol（RLDP; 不正ロケーション検出プロトコル）

AP が不正検出用として構成されている場合は、無線機能がオフになり、有線ネットワーク上で、不正 AP にアソシエートされているクライアント（つまり不正クライアント）の MAC アドレスをリッスンするという役割が与えられます。不正検出用 AP は、これらの不正クライアントの MAC アドレスが含まれている ARP パケットをリッスンします。いずれかの ARP を検出すると、それを WLC に報告し、不正 AP が Cisco Unified Wireless Network と同じネットワークに接続されているかどうかを検証します。ARP 情報をすみやかに収集するには、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）ポートを使用して、不正検出用 AP をすべてのブロードキャスト ドメインに接続しておく必要があります。複数の不正検出用 AP を設置することで、一般的なネットワーク上に存在するさまざまなブロードキャスト ドメインに接続できます。

不正クライアントが無線ルータ（一般的な家庭用 WLAN デバイス）の背後に設置されている場合、有線ネットワークではそれらの ARP 要求を確認できません。したがって、不正検出用 AP に代わる方法が必要になります。さらに、（メイン キャンパス ネットワークのように）多数のブロードキャスト ドメインが存在する環境では、不正検出用 AP は実用的な対処方法とはいえません。

このようなときは RLDP オプションが役立ちます。この場合、不正 AP を検出するために、標準 LAP はクライアントとして不正 AP にアソシエートし、テスト パケットをコントローラに送信します。つまり、AP はアクティブな AP であることをやめ、クライアント モードに切り替わります。これによって、問題の不正 AP が実際にネットワーク上に配置されているかどうかを確認すると共に、ネットワーク上での不正 AP の論理的位置を示す IP アドレス情報を通知します。支社では位置データを確立するのが難しいこと、また不正 AP が雑居ビルに設置されている可能性があることを考えると、不正検出用 AP と RLDP は、ロケーションベースの不正 AP 検出を補強する有益な手段といえます。

不正 AP の封じ込め

不正 AP に接続しているクライアント、または不正なアドホック接続クライアントを阻止するには、ローカルの AP が 802.11 認証解除パケットを送信します。ただし、隣接 WLAN の正規 AP に認証解除パケットを送信するのは違法なので、その AP が本当に不正 AP であることを確認してからこの処理を行う必要があります。Cisco Unified Wireless Network ソリューションから不正 AP の自動阻止機能が削除されているのはそのためです。

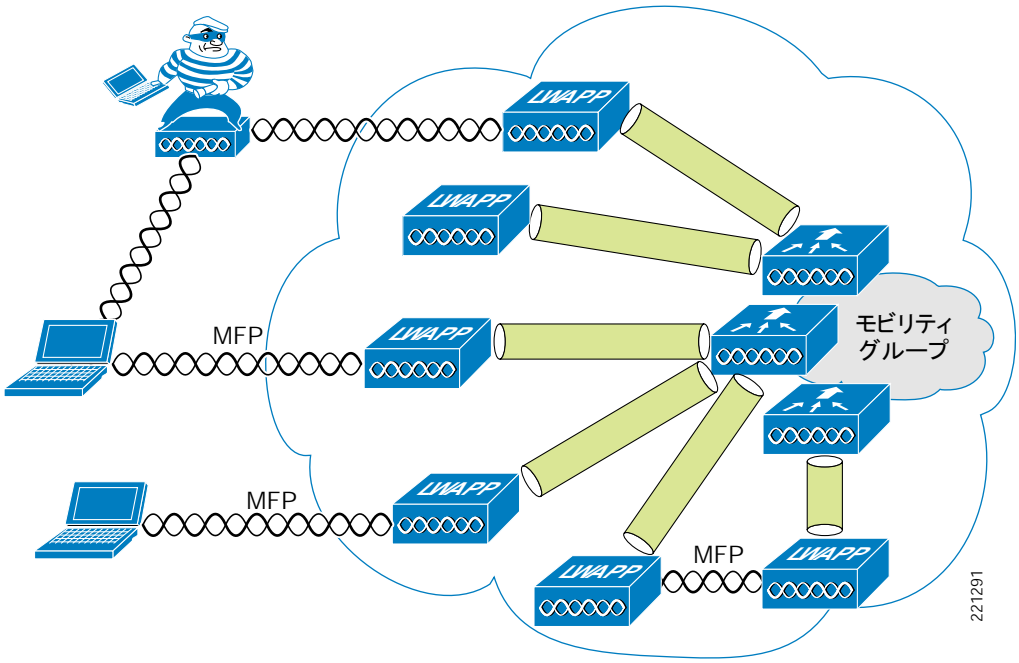
不正 AP クライアントがその企業の WLAN クライアントがどうかを確認するには、問題のクライアントの MAC アドレスと、802.1X 認証時に AAA が収集した MAC アドレスとを比較します。これによって、攻撃を受けている可能性のある WLAN クライアント、またはセキュリティ ポリシーに従っていないユーザを特定できます。

管理フレーム保護

802.11 の問題点の 1 つは、暗号化しない状態で管理フレームが送信され、メッセージ完全性チェックも実施されないので、スプーフィング攻撃を受けやすいということです。WLAN 管理フレームのスプーフィングは、WLAN ネットワーク攻撃で利用される危険性があります。この問題に対処するため、シスコは、802.11 管理フレームに Message Integrity Check（MIC; メッセージ完全性チェック）を挿入するデジタル シグニチャ メカニズムを開発しました。これによって、WLAN 展開の正規メンバを識別することができ、有効な MIC がないことから、不正インフラストラクチャおよびスプーフィングされたフレームを突き止めることができます。

管理フレーム保護（MFP）で使用される MIC は、メッセージの単純な CRC ハッシュではありません。この MIC にはデジタル シグニチャ コンポーネントも含まれています。MFP の MIC コンポーネントはフレームが改ざんされていないことを保証し、デジタル シグニチャ コンポーネントは、MIC が WLAN ドメインの有効なメンバによってのみ生成されることを保証します。MFP で使用されるデジタル シグニチャ キーは、モビリティ グループ内のすべてのコントローラで共有され、グループごとに固有のキーが割り当てられます。したがって、同じモビリティ グループ内の各 WLC で、すべての WLAN 管理フレームを検証することができます（図 4-15 を参照）。

図 4-15　　管理フレーム保護



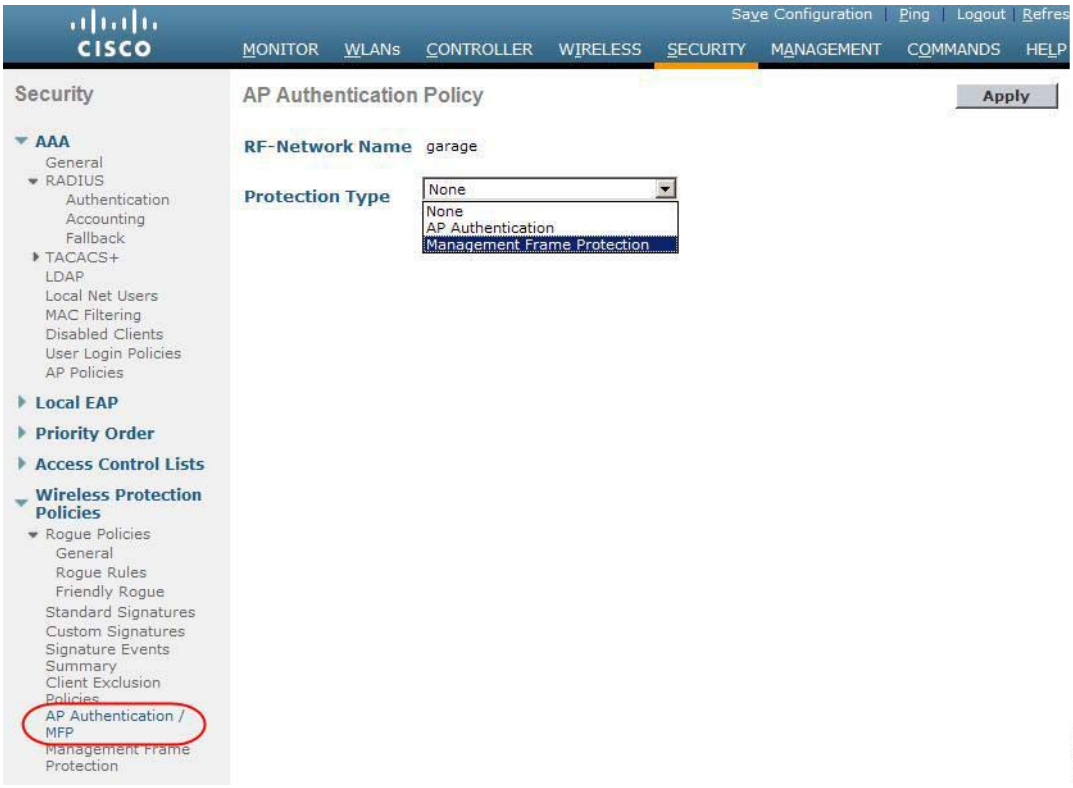
現在、インフラストラクチャ側とクライアントの両方で MFP が可能ですが、クライアントがモビリティ グループ MFP キーを判別し、無効なフレームを検出して拒否できるようにするには、CCXv5 WLAN クライアントが必要です。MFP には次のような利点があります。

- WLAN ネットワーク インフラストラクチャによって生成された 802.11 管理フレームを認証する。
- 正規 AP の MAC または SSID をスプーフィングし、不正行為や Man-In-the-Middle 攻撃の発覚を免れようとする悪質な AP を検出できる。
- 不正 AP および WLAN IDS シグニチャをより効率的に検出できる。
- CCX v5 と併用することで、クライアント デバイスも保護できる。

MFP を有効にするには、次の 2 つの手順があります。

- WLC 上で MFP を有効にします（図 4-16 を参照）。
- モビリティ グループ内の WLAN で MFP を有効にします（図 4-17 を参照）。

図 4-16　コントローラでの MFP の有効化

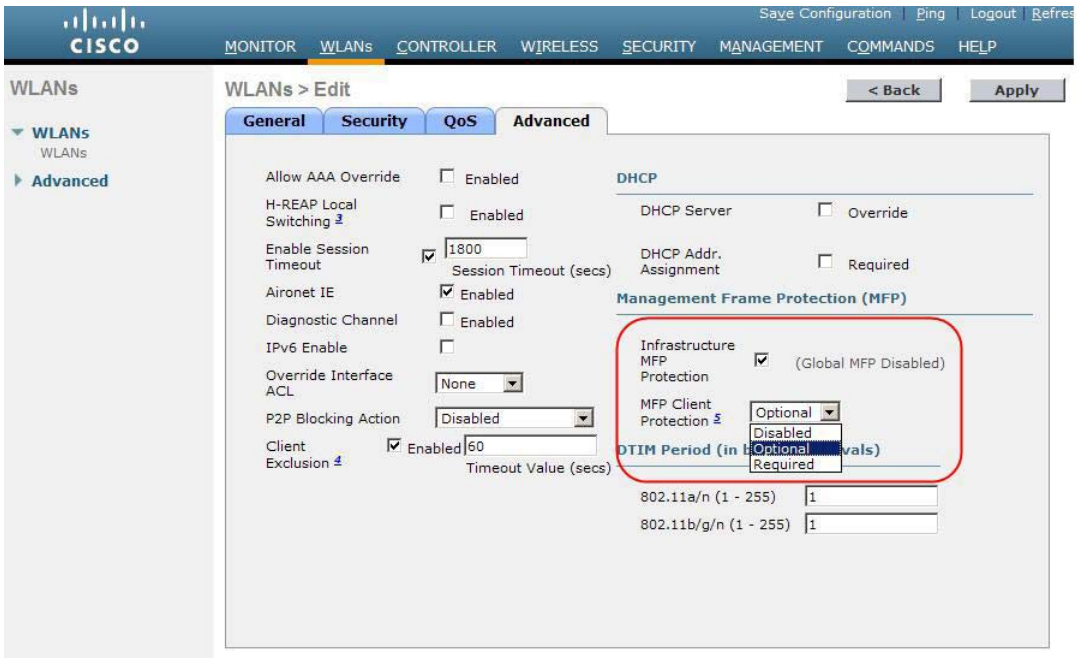


クライアントの管理フレーム保護

CCXv5 WLAN クライアントは MFP をサポートします。図 4-17 に示すように、WLAN ごとに MFP を有効化できます。

WLAN クライアントに MFP を適用する方法は、基本的には AP の場合と同じです。つまり、管理フレームで MIC を使用します。これによって、信頼できる管理フレームをクライアントが識別できるようになります。WPA2 認証プロセスの一部として、MIC の暗号キーが WLAN クライアントに渡されます。クライアント MFP は WPA2 でのみ使用できます。WPA クライアントと WPA2 クライアントが同じ WLAN を共有している場合は、クライアント MFP を Optional に設定する必要があります。

図 4-17　　WLAN ごとの MFP の有効化

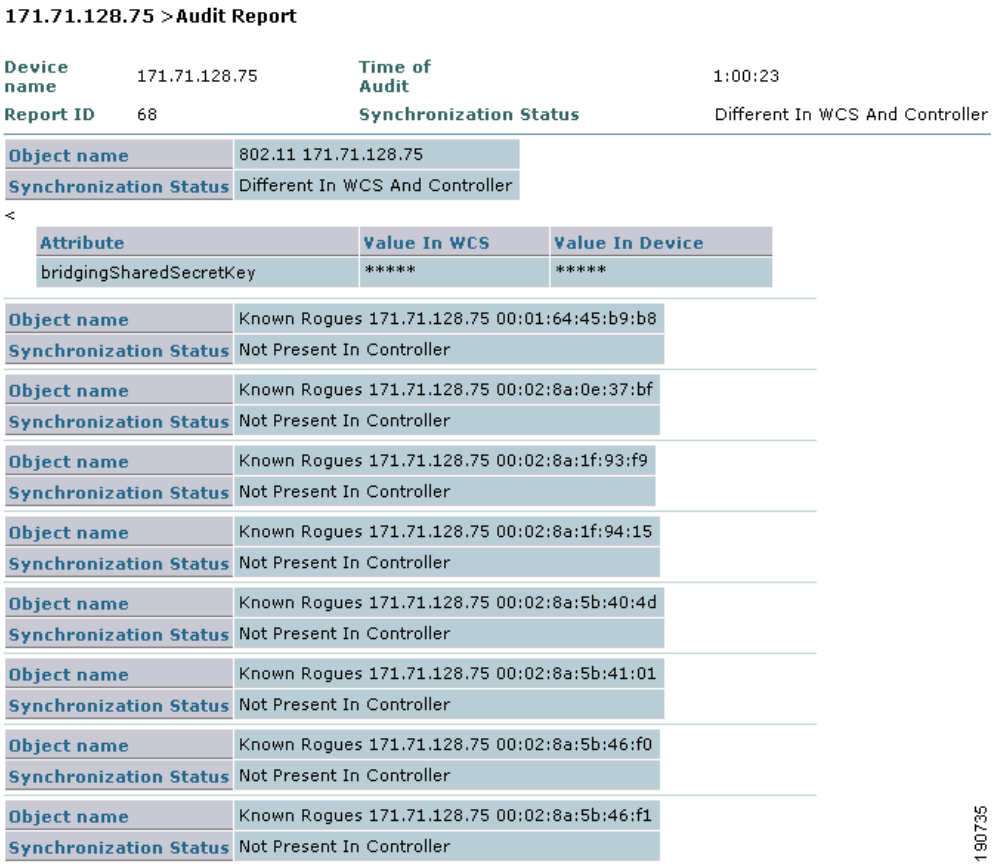


WCS のセキュリティ機能

設定検証

WCS では、必要に応じて、または定期的に、設定監査レポートを生成できます。このレポートでは、現在の WLC 設定および登録済みアクセスポイントの全てを、WCS データベースに保存されている既知の有効な設定と、比較します。現在実行されている設定と、データベースに保存されている設定の間に相違が見つかった場合は、画面レポートとしてネットワーク管理者に通知されます（図 4-18 を参照）。

図 4-18　監査レポートの例



171.71.128.75 >Audit Report

Device name	171.71.128.75	Time of Audit	1:00:23
Report ID	68	Synchronization Status	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

190735

アラーム

WLC で直接生成され、企業のネットワーク管理システム（NMS）に送信されるアラームとは別に、WCS もアラーム通知を送信することができます。コンポーネントによって送信されるアラームの種類が異なるのはもちろんですが、これらアラーム通知方式の違いはそれだけではありません。WLC は Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを使用してアラームを送信します。一方、WCS は Simple Mail Transfer Protocol（SMTP; 簡易メール転送プロトコル）E メールを使用してアラーム メッセージを送信します。これを E メール システムに対する DoS 攻撃として使用できないようにするために、E メール サーバを保護するための標準的な処理を実行する必要があります。

アーキテクチャ統合

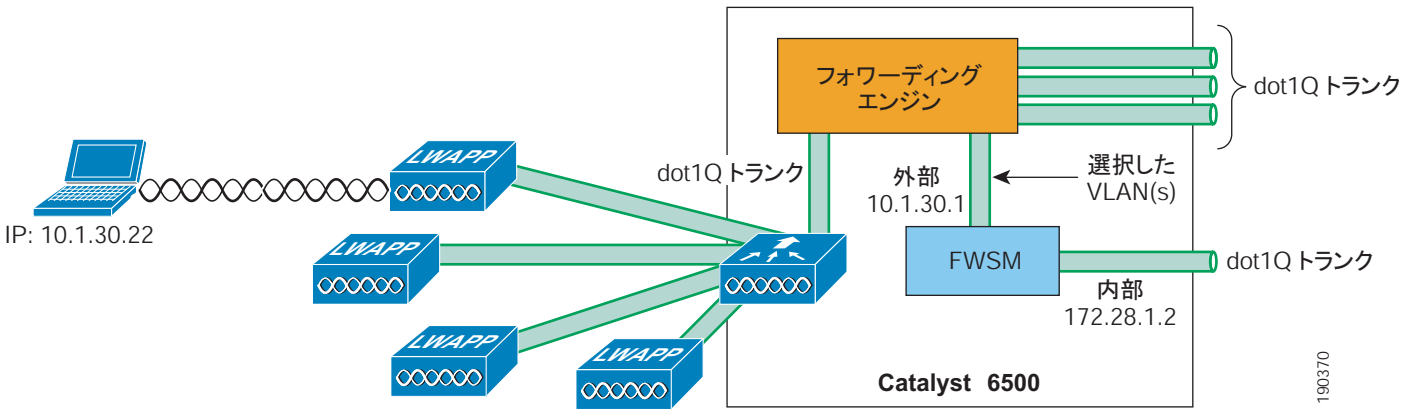
Cisco IOS、シスコのサービス モジュール、およびネットワーク モジュールには、さまざまな種類のセキュリティ サービスが統合されています。また、スタンドアロン アプライアンスとしてもセキュリティサービスを提供しています。Cisco Unified Wireless Network アーキテクチャは、WLAN クライアントと上流有線ネットワークをまたがるレイヤ 2 接続をサポートしているので、これらのセキュリティ サービスをソリューションへ簡単に統合できます。これは、クライアント トラフィックと直列にすることで動作するアプライアンスまたはモジュールを、WLAN クライアントとコア ネットワークの間に簡単に挿入できるということです。たとえば、

Cisco Wireless LAN Services Module（WLSM）ベースの展開では、WLAN クライアント トラフィックを Cisco Firewall Service Module（FWSM）経由でやり取りできるようにするには、Cisco 6500 上に VRF-Lite を実装する必要があります。一方、Wireless Services Module（WiSM）を使用する Cisco Unified WLAN 展開では、（WLAN）クライアントの VLAN を直接 FWSM にマップできます。Cisco Unified Wireless 製品で、物理的なインターフェイスにレイヤ 2 の WLAN トラフィックを直接マップできない WLAN コントローラは、ISR ベースの WLC モジュールだけです。ISR WLAN モジュールは、ISR で利用可能なすべての IOS および IPS 機能にアクセスできてしまうため、WLAN クライアントからの IP トラフィックは、ルータの IOS VRF 機能を使用して、特定の ISR インターフェイスを経由するように誘導する必要があります。

図 4-19 は、WiSM と FWSM モジュールのアーキテクチャ統合例を示しています。この例では、WLAN クライアントは、外部ファイアウォール インターフェイスと同じサブネットに配置されています。ルーティング ポリシーや VRF 設定を使用しなくても、WLAN クライアントの両方向のトラフィックをファイアウォール経由で送受信できます。

WLAN 展開に Cisco Network Admission Control（NAC; ネットワーク アドミッション制御）アプライアンスを取り入れれば、ネットワーク上のエンド デバイスが企業ポリシーに準拠しているかどうかを確認し、最新のセキュリティ ソフトウェア要件を満たしており、必要なシステム パッチを適用しているデバイスのみに接続を許可することができます。上記で説明した FWSM モジュールと同様、Cisco NAC アプライアンス（以前の Cisco Clean Access）も Unified Wireless アーキテクチャにレイヤ 2 で統合できます。したがって、NAC ポリシーの適用対象となる無線ユーザ VLAN を厳密に制御できます。

図 4-19　　ファイアウォール モジュール統合の例



ネットワーク レイヤでの Cisco Unified Wireless Network の統合に加え、Cisco Security ソリューションの管理レイヤおよび制御レイヤにおいて、他の統合が提供されます。Cisco Unified Wireless Network と次のものを統合できます。

- Cisco NAC アプライアンス
- Cisco IPS
- Cisco CS MARS

これらの統合についてはすべて、このデザイン ガイドの後続の章と、シスコ ファイアウォール ソリューションおよび Cisco Security Agent の統合について説明している章で詳しく述べています。

参照資料

- Deploying Cisco 440X Series Wireless LAN Controllers：
  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
- Cisco Wireless LAN Controller Configuration Guide, Release 5.0：
  http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/ccg50.html
- Cisco Wireless Control System Configuration Guide, Release 5.0：
  http://www.cisco.com/en/US/docs/wireless/wcs/5.0/configuration/guide/wcs50cg.html

CHAPTER 5

無線 NAC アプライアンスの統合

この章では、Cisco Network Admission Control（NAC; ネットワーク アドミッション制御）アプライアンスのエンドポイント セキュリティを Cisco Unified Wireless Network 展開に導入するための設計ガイダンスを示します。ベスト プラクティスとなるこれらの推奨事項では、Cisco Unified Wireless Network を『*Enterprise Mobility Design Guide 4.1*』のガイドラインに従って展開したことを前提としています。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

この章では、Cisco NAC アプライアンス（以前の Cisco Clean Access）を信頼性のあるスケーラブルな形式で Cisco Unified Wireless アーキテクチャに組み込む方法について説明します。この章は、Cisco NAC アプライアンス ソリューション自体に関する包括的なガイドを目的としたものではありません。この章では、Cisco Clean Access および Cisco Unified Wireless のエンド ユーザ ガイドで扱っていない実装の詳細を中心に説明します。

概要

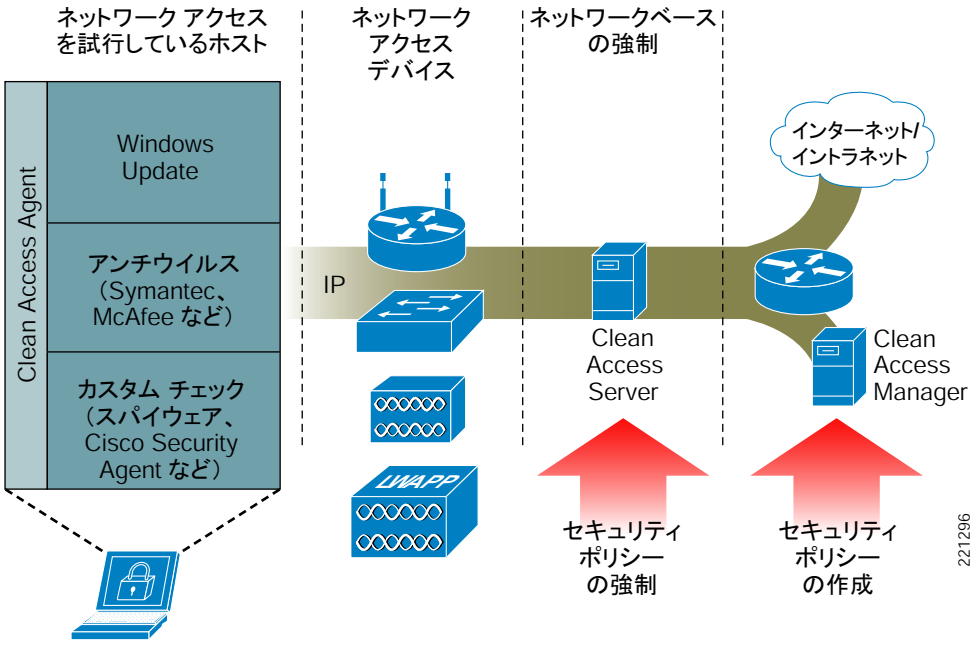
Cisco NAC アプライアンスは、展開の容易な NAC 製品です。ネットワーク コンピューティング リソースにアクセスしようとするすべてのデバイスに対して、ネットワーク インフラストラクチャを使用して、セキュリティ ポリシーへの準拠を強制します。Cisco NAC アプライアンスを展開すると、ネットワークにアクセスしようとする有線、無線、およびリモートのユーザやマシンをネットワーク管理者が事前に認証、認可、評価、および修復できます。Cisco NAC アプライアンスは、ラップトップ、IP Phone、ゲーム コンソールなどのネットワーク接続デバイスがネットワークのセキュリティ ポリシーに準拠しているかどうかを識別し、脆弱性を除去してからネットワークへのアクセスを許可します。

Cisco NAC アプライアンスを展開することにより、次の利点があります。

- ネットワーク内のユーザ、ユーザのデバイス、およびユーザのロールを認識する。この最初の手順は、悪意のあるコードによって被害を受ける可能性が生じる前に、認証の時点で発生します。
- マシンがセキュリティ ポリシーに準拠しているかどうかを評価する。セキュリティ ポリシーには、特定のアンチウイルス ソフトウェアやアンチスパイウェア ソフトウェア、オペレーティング システム（OS）のアップデート、またはパッチを含めることができます。Cisco NAC アプライアンスでは、ユーザのタイプ、デバイスのタイプ、またはオペレーティング システムに応じて異なるポリシーを使用できます。
- 基準に準拠していないマシンをブロック、隔離、および修復して、セキュリティ ポリシーを適用する。

基準に準拠していないマシンは、検疫ネットワークにリダイレクトされ、管理者の判断によって修復が実行されます。図 5-1 に、NAC アプライアンスの一般的なトポロジを示します。

図 5-1　無線アクセス機能を備えたインバンドの Clean Access トポロジ



Clean Access Server および Clean Access Manager の包括的な概要については、次の URL にあるマニュアルを参照してください。

- *Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*
- *Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*

  http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

NAC アプライアンスと WLAN 802.1x/EAP

企業の無線 LAN 展開では、Cisco NAC アプライアンス ソリューションを 802.1x/EAP ベースの認証実装の代替と考えないでください。NAC アプライアンス ソリューションによって提供されるアクセス制御および修復のサービスは、補完的なものであり、802.1x/EAP 自体によって提供されるアクセス制御に追加するための付加的なセキュリティを提供します。

ネットワークに対するすべてのアクセスおよび認証について、NAC アプライアンスを共通の制御ポイントとして使用することもできますが、アプライアンスでは無線データのプライバシーを提供できません。このため、データのプライバシーを保証し、無線セキュリティに対する他の脅威を軽減するには、802.1x/EAP とともに WPA/WPA2 が必要です。

無線ユーザが認証され、ネットワークの無線部分へのアクセス権を付与された後も、NAC アプライアンスは重ねて別のセキュリティを適用します。次の条件が満たされるまでは、ネットワークの有線部分へのアクセスを制限します。

- エンド ユーザが検証または認証される。これは、有線ネットワークでは有用ですが、無線ネットワークの場合、802.1x/EAP 認証によってすでに実行された処理を繰り返すことになるため、冗長な機能になります。

- エンド ユーザのデバイス（コンピュータ）が、セキュリティ ポリシーへの準拠確認に合格する（例：無線ユーザのラップトップで、アンチウイルス ソフトウェアの最新バージョンが実行されている）。

したがって、NAC のサービスを Unified Wireless 展開に導入する場合に課題の 1 つとなるのは、「二重の」認証という問題に対処することです。このトピックについては、P.5-12 の「Unified Wireless 展開での Cisco Clean Access 認証」で詳しく取り上げます。

Unified Wireless Network での NAC アプライアンスのモードおよび配置

動作モード

NAC アプライアンスは、次の 4 つの動作モードで動作できます。

- アウトオブバンド バーチャル ゲートウェイ
- アウトオブバンド IP ゲートウェイ
- インバンド バーチャル ゲートウェイ
- インバンド Real-IP ゲートウェイ

詳細については、P.5-3 の「アウトオブバンド モード」および P.5-4 の「インバンド モード」を参照してください。

各モードの詳細については、サーバ アプライアンスのインストール マニュアルを参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html で入手できます。

アウトオブバンド モード

レイヤ 2 モード（バーチャル ゲートウェイ）またはレイヤ 3 モード（Real-IP ゲートウェイ）のいずれかのアウトオブバンド展開の場合、ユーザ トラフィックが NAC アプライアンスを通過する必要があるのは、認証、ポスチャ評価、および修復の実行中のみです。ユーザが認証され、すべてのポリシー確認に合格した場合、そのユーザのトラフィックは、ネットワークを通じて通常どおりにスイッチされ、アプライアンスを迂回します。Cisco Unified Wireless での NAC アウトオブバンド ゲートウェイのサポートは、ソフトウェア リリース 5.1.151.0 で追加されました。このデザイン ガイドで使用された Unified Wireless ソフトウェア リリースは、NAC アプライアンスのアウトオブバンド ゲートウェイを使用する場合は展開できません。これは、WLAN から VLAN への WLC 上のマッピングを CAM で動的に変更する方法が存在しないためです。この点は、Wireless LAN Controller ソフトウェア リリース 5.1.151.0 で対処されました。Cisco Unified Wireless Network でのアウトオブバンド NAC 機能の詳細については、次の URL を参照してください。

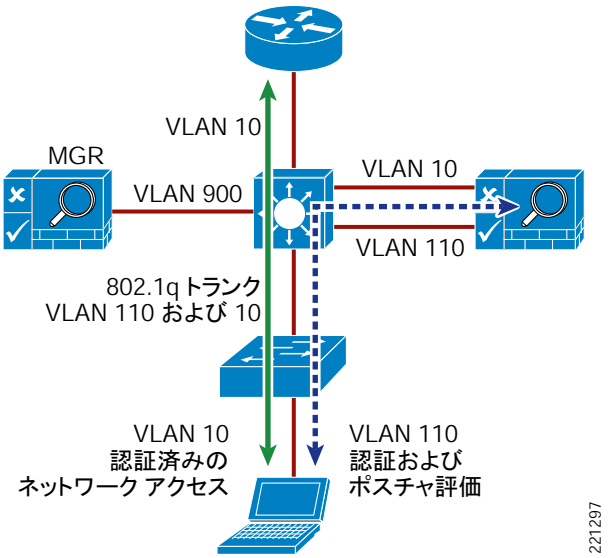
http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a0080a138cc.shtml

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 4 章を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html で入手できます。

図 5-2 に、レイヤ 2 アウトオブバンド トポロジの例を示します。

図 5-2　　レイヤ 2 アウトオブバンド トポロジ



NAC アプライアンスをこの方法で展開するには、クライアント デバイスが Catalyst スイッチのポート経由でネットワークに直接接続されている必要があります。ユーザが認証されてポスチャ評価に合格すると、Clean Access Manager（CAM）は、（ユーザ トラフィックが NAC にスイッチまたはルーティングされる）未認証の VLAN から、完全なアクセス特権を提供する認証済み（認可済み）の VLAN にユーザ ポートをマップするようスイッチに指示します。

インバンド モード

NAC アプライアンスをインバンドで展開する場合は、すべてのユーザ トラフィック（未認証と認証済みの両方）が NAC アプライアンスを通過します。NAC アプライアンスは、エンドユーザと保護対象ネットワーク（複数可）の間に論理的または物理的に配置できます。論理インバンド トポロジの例については図 5-3、物理インバンド トポロジの例については図 5-4 を参照してください。

図 5-3　インバンド バーチャル ゲートウェイ トポロジ

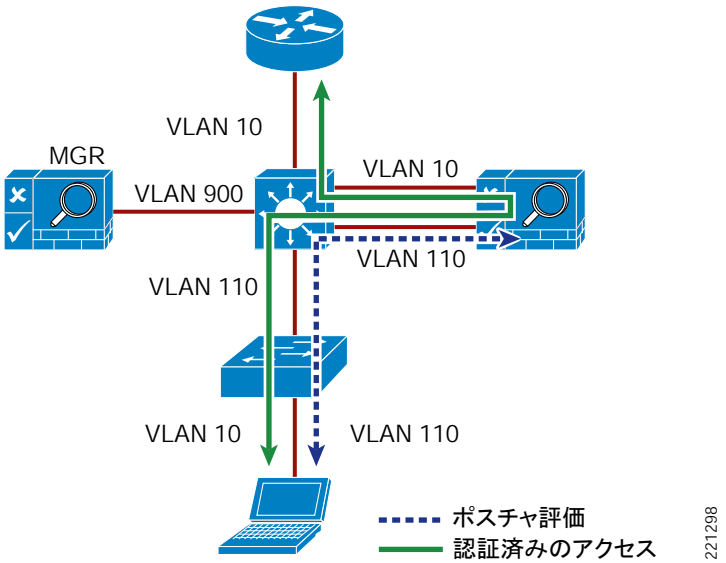
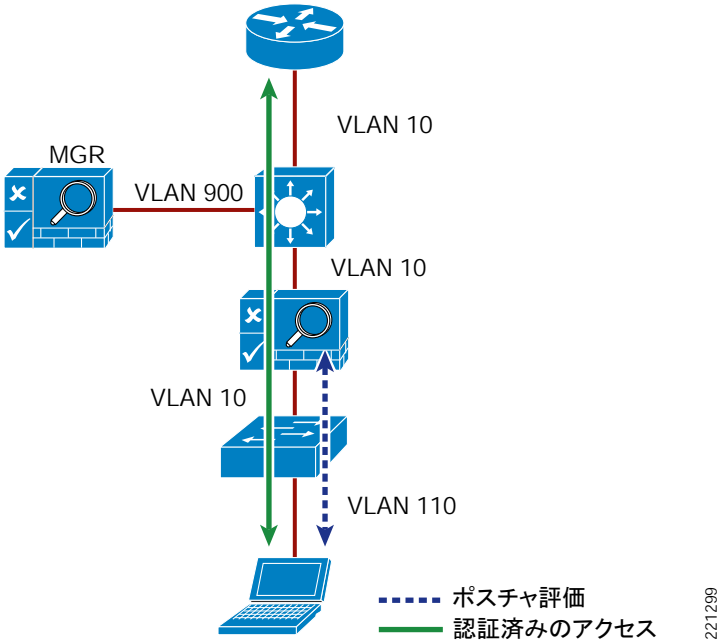


図 5-4　物理インバンド トポロジ



インバンド モードは、このデザイン ガイドで使用されている Cisco Unified Wireless Network ソフトウェアで現在使用できる唯一の方式です。ただし、ソフトウェア リリース 5.1 以降ではアウトオブバンドがサポートされています。P.5-3 の「動作モード」で説明したように、NAC アプライアンスは、バーチャル ゲートウェイと Real-IP ゲートウェイのいずれかとして動作できます。どちらのゲートウェイ方式も Unified Wireless 展開と互換性があり、このガイドで説明します。

インバンド バーチャル ゲートウェイ

NAC アプライアンスをバーチャル ゲートウェイとして設定した場合、アプライアンスは、エンド ユーザとデフォルト ゲートウェイ（ルータ）の間で管理対象クライアント サブネットのブリッジとして機能します。NAC アプライアンスでは、次の 2 つのブリッジ オプションがサポートされています。

- トランスペアレント：所定のクライアント VLAN について、NAC アプライアンスは自身の Untrusted インターフェイスから Trusted インターフェイスにトラフィックをブリッジします。アプライアンスは「より上位のレイヤのプロトコル」を認識するため、デフォルトでは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フレーム（スパニング ツリー）および「unauthorized」ロールで明示的に許可されているプロトコル（DNS や DHCP など）を除いて、トラフィックをすべてブロックします。言い換えると、ネットワークへの接続、認証、ポスチャ評価の取得、および修復のためにクライアントで必要となるプロトコルは許可します。このオプションが有用となるのは、エンド ユーザと保護対象アップストリーム ネットワークの間で、NAC アプライアンスが物理的にインバンドで配置されている場合です（図 5-4 を参照）。
- VLAN マッピング：動作はトランスペアレント方式と類似していますが、アプライアンスの信頼できない側から信頼できる側に同一の VLAN をブリッジするのではなく、2 つの VLAN を使用する点が異なります。たとえば、Wireless LAN Controller（WLC; 無線 LAN コントローラ）と NAC アプライアンスの Untrusted インターフェイスの間に、クライアント VLAN 131 が定義されているとします。VLAN 131 には、ルーテッド インターフェイスまたは Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）は関連付けられていません。NAC アプライアンスの Trusted インターフェイスと、クライアント サブネットのネクスト ホップ ルータ インターフェイス /SVI の間には、VLAN 31 が設定されています。NAC アプライアンスでは、VLAN タグ情報をスワップすることで、VLAN 131 に到着するパケットを VLAN 31 に転送するマッピング ルールが作成されます。クライアントに返されるパケットについては、逆のプロセスが発生します。このモードでは、信頼できない側の VLAN から信頼できる側の VLAN に BPDU が渡されないことに注意してください。

VLAN マッピング オプションを選択するのは、通常、クライアントと保護対象ネットワークの間で NAC アプライアンスを論理的にインバンドで配置する場合です。これは、Unified Wireless 展開にバーチャル ゲートウェイ モードで NAC アプライアンスを展開する場合に使用されるブリッジング オプションです。

（注）　NAC アプライアンス（VLAN マッピングを使用してインバンド バーチャル ゲートウェイとして設定）をハイ アベイラビリティ設定で展開する場合は、十分に注意する必要があります。設定が不適切な場合、特定の隔離された状況ではレイヤ 2 ループ トポロジが形成される可能性があります。この点については、P.5-30 の「ハイ アベイラビリティ フェールオーバーに関する考慮事項」および P.5-42 の「NAC アプライアンスの設定に関する考慮事項」で詳しく説明します。

インバンド Real-IP ゲートウェイ

NAC アプライアンスが「実際の」IP ゲートウェイとして設定されている場合、アプライアンスはルータと同様に動作し、自身のインターフェイス間でパケットを転送します。このシナリオでは、Untrusted インターフェイスの背後に、1 つまたはそれ以上のクライアント VLAN/ サブネットが存在します。NAC アプライアンスは、これらのネットワークに存在するすべてのクライアントのデフォルト ゲートウェイとして機能します。一方、Trusted インターフェイス上には、保護対象のアップストリーム ネットワーク（複数の場合あり）へのパスを表す単一の VLAN/ サブネットが定義されます。

クライアント認証およびポスチャ評価が正常に完了すると、NAC アプライアンスは、デフォルトではトラフィックを信頼できないネットワークから Trusted インターフェイスにルーティングします。このトラフィックは、ネットワークのルーティング トポロジに基づいて転送されます。

NAC アプライアンスは、現時点ではダイナミック ルーティング プロトコルをサポートできません。このため、Untrusted インターフェイスで終端するか、Untrusted インターフェイスの背後に存在しているクライアント サブネットごとに、レイヤ 3 ネットワークの信頼できる側にスタティック ルートを設定する必要があります。これらのスタティック ルートでは、NAC の Trusted インターフェイスの IP アドレスをネクスト ホップとして参照する必要があります。

信頼できない NAC インターフェイスとエンド クライアント サブネットの間に、1 つまたはそれ以上のレイヤ 3 ホップが存在する場合は、NAC アプライアンスでクライアント ネットワークへのスタティック ルートを設定する必要があります。同様に、（信頼できない NAC インターフェイスの IP アドレスを参照する）ダウンストリーム レイヤ 3 ネットワーク内にスタティック デフォルト ルート（0/0）を設定して、クライアント ネットワークから NAC アプライアンスへのデフォルト ルーティング処理を準備する必要があります。

トポロジによっては、NAC アプライアンスを送受信先とするルーティングを準備する方法は複数あります（スタティック ルート、VRF-Lite、MPLS VPN、その他のセグメンテーション技術など）。このデザイン ガイドの対象外となるため、使用可能な方法をすべて取り上げることはしません。

Unified Wireless 展開で使用するゲートウェイ方式

ここまでに説明したように、どちらのゲートウェイ方式も Cisco Unified Wireless 展開との互換性があります。どちらのゲートウェイ方式を選択した場合も、実装可能なサービス オプションおよび機能に関しては、もう一方の方式と比較して大きな不都合はありません。ただし、展開全般にわたって次の事項を考慮すると、いずれかのゲートウェイ方式が有利になります。

- Real-IP ゲートウェイは、マルチキャスト サービスを*サポートしていません*。無線ネットワークでマルチキャストのサポートが必要になる場合は、バーチャル ゲートウェイ モードを使用する必要があります。
- Quality Of Service（QoS; サービス品質）については、Real-IP ゲートウェイ モードとバーチャル ゲートウェイ モードのどちらでも、Type of Service（ToS; タイプ オブ サービス）/Diffrentiated Services Code Point（DSCP; DiffServ コード ポイント）値が透過的に転送されます。所定の QoS 値が変更されることや、QoS 値に基づいて処理が実行されることはありません。
- Real-IP ゲートウェイ モードでは、NAC アプライアンスのアップストリーム側にスタティック ルートを設定して、信頼できないクライアント サブネットへの適切なルーティングをサポートする必要があります。NAC アプライアンスのダウンストリーム側（信頼できない側）のトポロジによっては、追加のスタティック ルート設定が必要になります。
- Real-IP ゲートウェイ モードで中央集中型の DHCP サービスをサポートするには、この他の設定も必要です。具体的には、中央のサーバに DHCP リレーのメッセージを供給する WLC 動的インターフェイスごとに、NAC アプライアンスでフィルタを定義する必要があります。また、DHCP サービスを NAC アプライアンス自体または WLC でホスティングする方法もあります。ただし、通常、この方法は大規模な展開ではお勧めしません。
- Real-IP ゲートウェイ モードの場合、信頼できる側の VLAN/ サブネットは、ユーザ トラフィックのサポート以外に CAM との管理通信にも使用されます。

Unified Wireless 展開での NAC アプライアンスの配置

Cisco NAC アプライアンス ソリューションは、中央集中型とエッジという 2 つの展開モデルをサポートしています。Cisco Unified Wireless 展開では、NAC アプライアンスが無線ユーザとアップストリーム ネットワークの間に論理的にインバンドで配置されている限り、どちらのロケーションも使用できます。

エッジ配置

キャンパス ネットワークの設計では、現在のシスコ ベスト プラクティスとして、レイヤ 3 アクセス / ディストリビューション モデルをお勧めします。WLAN コントローラがディストリビューション レイヤに配置されている場合は、NAC アプライアンスもディストリビューション レイヤに配置する必要があります。

NAC アプライアンスは、バーチャル ゲートウェイと Real-IP ゲートウェイのどちらにも設定できます。ただし、いずれの場合も、NAC アプライアンスを WLC のレイヤ 2 隣接ノードにして、両者間にレイヤ 3 ホップが存在しない状態にすることを強くお勧めします。このように配置すると、NAC アプライアンスと WLC の間に 802.1q トランキングを確立することにより、NAC アプライアンスにどの WLC インターフェイスをマップするかを管理者が制御できます。NAC アプライアンスはユーザ トラフィックにインバンドで介在する必要があるため、目標となるのは、すべてのコントローラ トラフィック（RADIUS、SNMP、LWAPP 制御 / データ、モビリティ トンネルなど）ではなく、信頼できない無線ユーザ トラフィックのみをアプライアンス経由で転送することです。

ディストリビューション レイヤ スイッチ ブロックを high availability（HA; ハイ アベイラビリティ）用に設計し、HA 構成に NAC アプライアンスも展開する場合は、ディストリビューション スイッチ間に 802.1q トランキングを確立する必要があります（図 5-5 および図 5-6 を参照）。

図 5-5　　分散型 WLC/NAC の展開

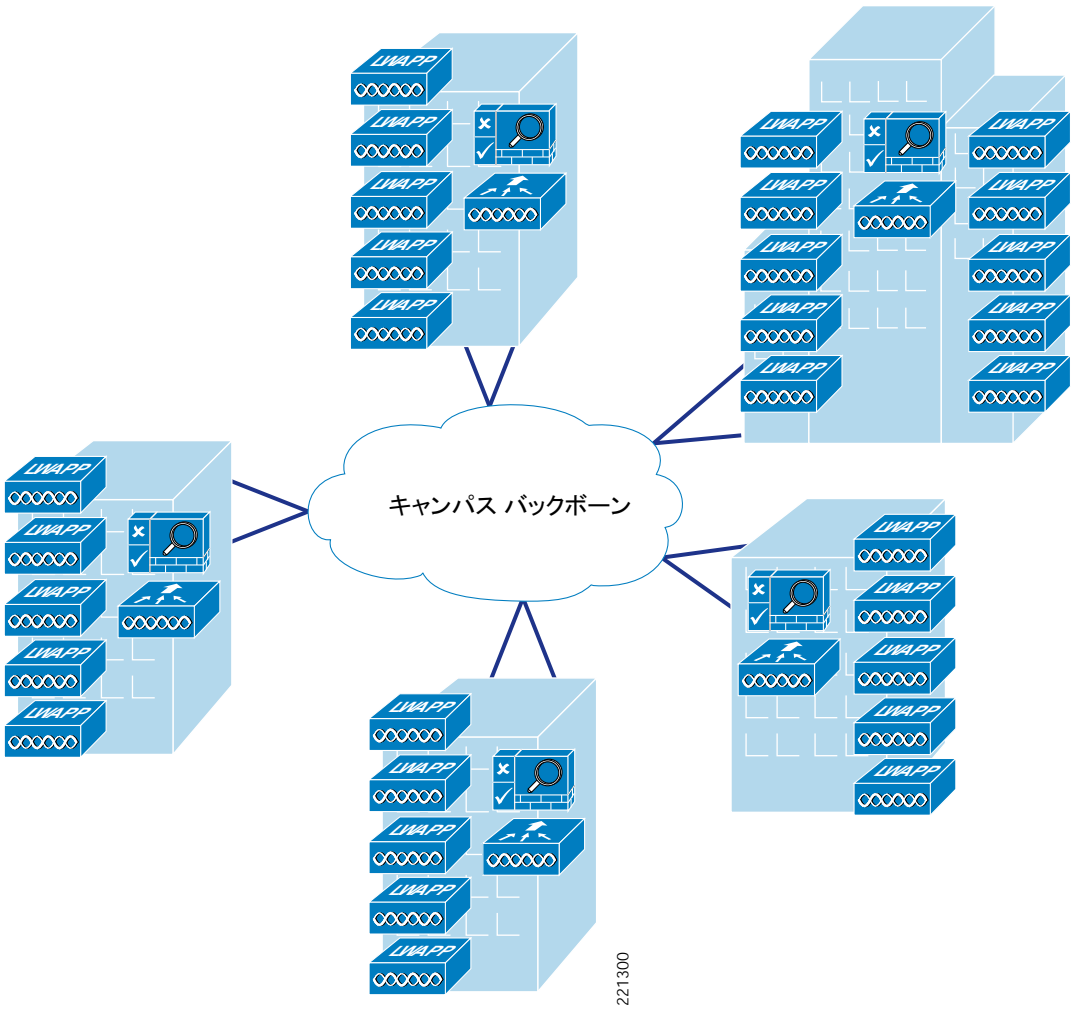
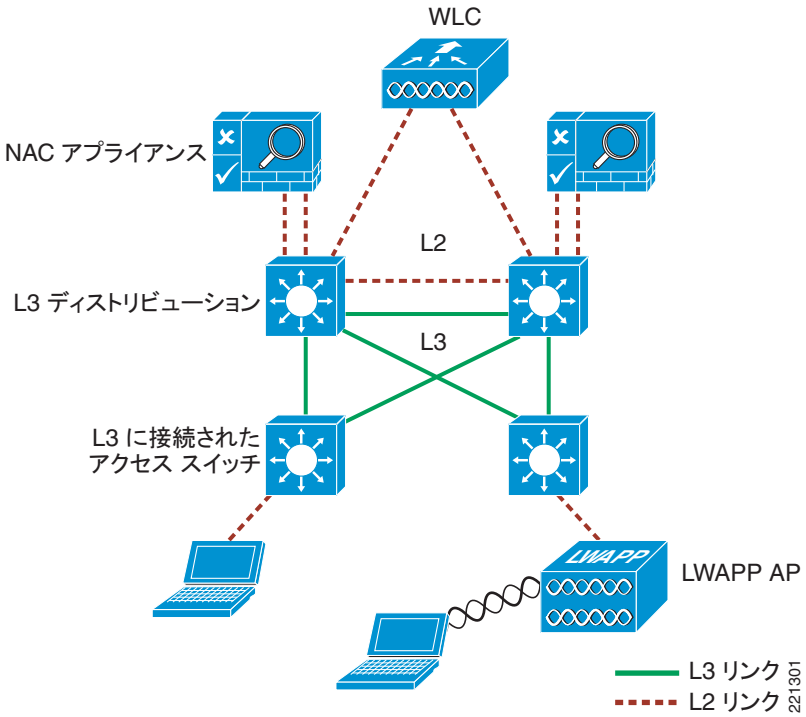


図 5-6　Unified Wireless および NAC アプライアンスを導入したレイヤ 3 アクセス / ディストリビューション



上で説明したように、ディストリビューション レイヤに NAC のサービスを導入する場合、簡潔なレイヤ 3 アクセス / ディストリビューションの設計にレイヤ 2 の複雑さが加わる可能性があります。また、WLAN コントローラ（複数可）のあるディストリビューション レイヤに NAC アプライアンスを配置するアプローチでは、複数のロケーションが関係する場合、またはファイアウォールや IDS/IPS サービスなど、他の一般的なサービスを展開する場合には、最大の経済効果が得られないことがあります。

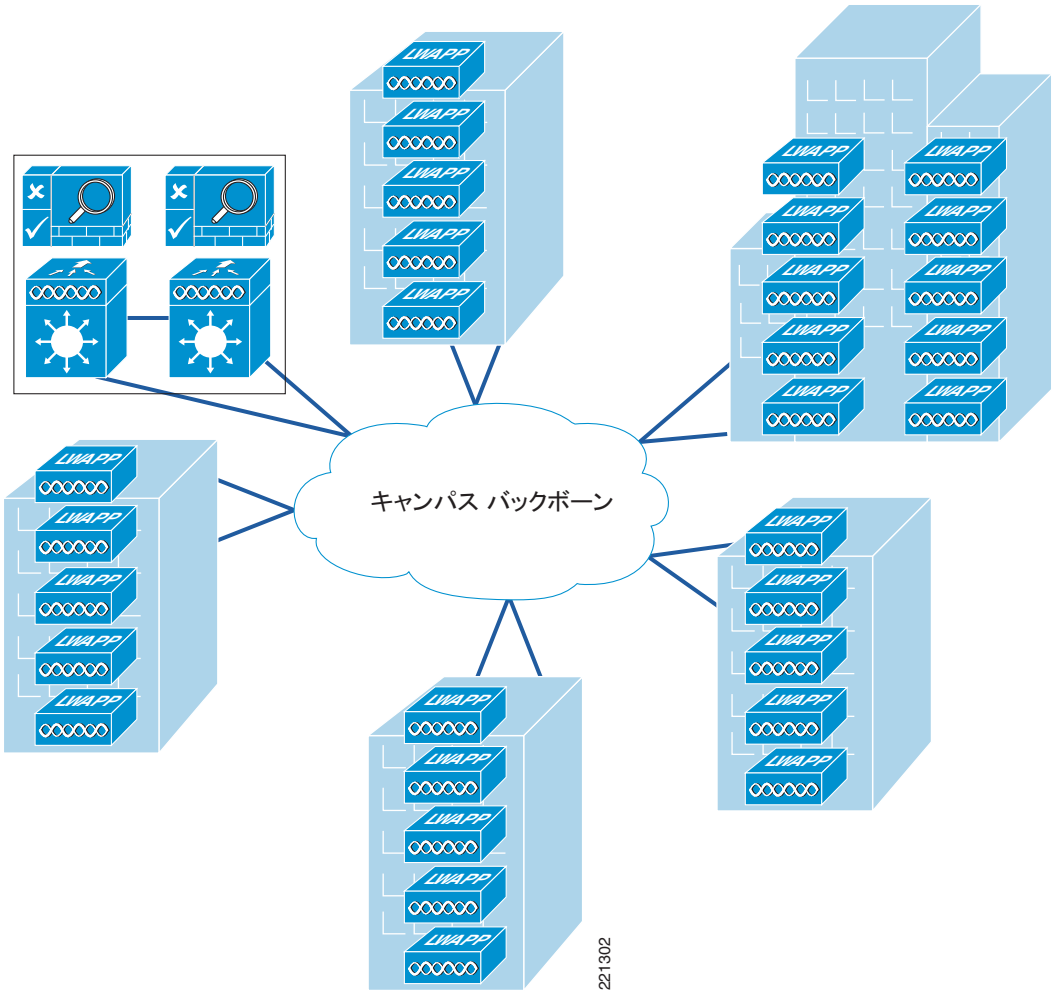
（注） NAC アプライアンスの実装時に、NAC アプライアンスと WLAN コントローラの間に 1 つまたはそれ以上のレイヤ 3 ホップを配置することもできますが、これはお勧めしません。このような構成にする場合は、（基盤となっているネットワークに応じて）複雑なものとなる可能性があるセグメンテーションやポリシー ルーティングの技術を導入し、信頼性のある予測可能な手段によって、信頼できないクライアントのトラフィックを NAC アプライアンスに伝送できるようにする必要があります。RADIUS、LWAPP、モビリティ トンネルなど、ユーザ トラフィック以外のコントローラベース トラフィックを適切に処理しようとする場合の複雑さも考慮する必要があります。

中央集中型の展開

Cisco Unified Wireless での現在のベスト プラクティスとしては、WLAN コントローラをキャンパスの *中央に*配置することをお勧めします。たとえば、データ センターと並置するか、サービス モジュールとして装着します。したがって、WLC と NAC アプライアンスによって独自のスイッチ ブロックを構成し、データ センター内の WLC と NAC アプライアンスの間にレイヤ 2 隣接関係を確立して、データ センター サーバのスイッチ基盤と分離することをお勧めします（図 5-7 を参照）。詳細については、『*Enterprise Mobility 4.1 Design Guide*』の第 2 章を参照して

ください。このマニュアルは、
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
で入手できます。

図 5-7　　中央集中型の WLC/NAC 展開



まとめ

NAC アプライアンスでは、複数の展開オプションおよび動作モードが提供されます。ただし、キャンパスおよびモビリティに関する現時点でのベスト プラクティスを考慮した場合、NAC アプライアンスは、インバンド ゲートウェイとして WLAN コントローラとともに中央に展開することをお勧めします。このトポロジについては、P.5-23 の「Unified Wireless での NAC アプライアンス ハイ アベイラビリティの実装」で詳しく取り上げます。

Unified Wireless 展開での Cisco Clean Access 認証

P.5-3 の「Unified Wireless Network での NAC アプライアンスのモードおよび配置」で説明したように、NAC アプライアンスの主な機能の 1 つはユーザの識別と認証です。NAC ユーザ認証は必須のものであるため、課題となるのは、802.1x/EAP を使用してすでに認証されている企業無線ユーザの認証です。現時点では、無線ユーザの認証状態を NAC アプライアンスで直接認識する方法、および NAC アプライアンスを無線認証の RADIUS プロキシとして運用する方法はありません。このような機能に代わって、NAC では次の認証オプションが用意されています。

- Web 認証
- Clean Access Agent
- Clean Access Agent を通じて次の機能を利用する Single Sign-On（SSO; シングル サインオン）
  - VPN RADIUS アカウンティング
  - Active Directory

Web 認証

Web 認証の場合、無線ユーザは NAC アプライアンスの Web ポータルを使用して認証を受ける必要があります。この方法は、企業ユーザには適しません。ユーザは、Web ブラウザを開いて、認証ページにリダイレクトされてからクレデンシャルを入力する必要があるためです。問題となるのは、次の点です。

- 既存クレデンシャルと新規クレデンシャルのどちらを使用するか。
- ローカル NAC データベースと外部データベースのどちらを使用するか。

一方、Web 認証が有用かつ最適なものになるのは、WLAN が別の方法で「開放」され、ポータル認証を使用した Web リダイレクトなど、汎用的なアクセス手段を使用してアクセスを制御できるゲスト アクセス展開シナリオです。

Clean Access Agent

ユーザは、Clean Access Agent のユーザ インターフェイスを使用して認証を受けます。このシナリオでは、無線クライアント コンピュータは Cisco Clean Access Agent ソフトウェアを実行します。エージェントは、Clean Access で保護されているネットワークを自動的に検出し、ユーザにクレデンシャルの入力を要求します。この方法は、上の Web 方式よりも幾分優れています。ただし、PC に Clean Access Agent ソフトウェアをインストールする必要があります。また、ユーザによる手動でのクレデンシャル入力が必要な点は変わりません。

シングル サインオン VPN

シングル サインオン（SSO）VPN は、ユーザによる操作を必要とせず、実装も比較的容易なオプションです。NAC ソリューションの VPN SSO 機能と併せて、クライアント PC 上で動作する Clean Access Agent ソフトウェアを使用します。VPN SSO では、RADIUS アカウンティング レコードを使用して、ネットワークに接続している認証済みのリモート アクセス ユーザを

NAC アプライアンスに通知します。同様に、この機能を WLAN コントローラと連動することで、ネットワークに接続している認証済みの無線クライアントを NAC サーバに自動的に通知できます。

SSO 認証、ポスチャ評価、修復、およびネットワーク アクセスを NAC アプライアンス経由で実行する無線クライアントの例については、図 5-8 ～図 5-12 を参照してください。

図 5-8　無線 VPN SSO：無線認証 / アソシエーション

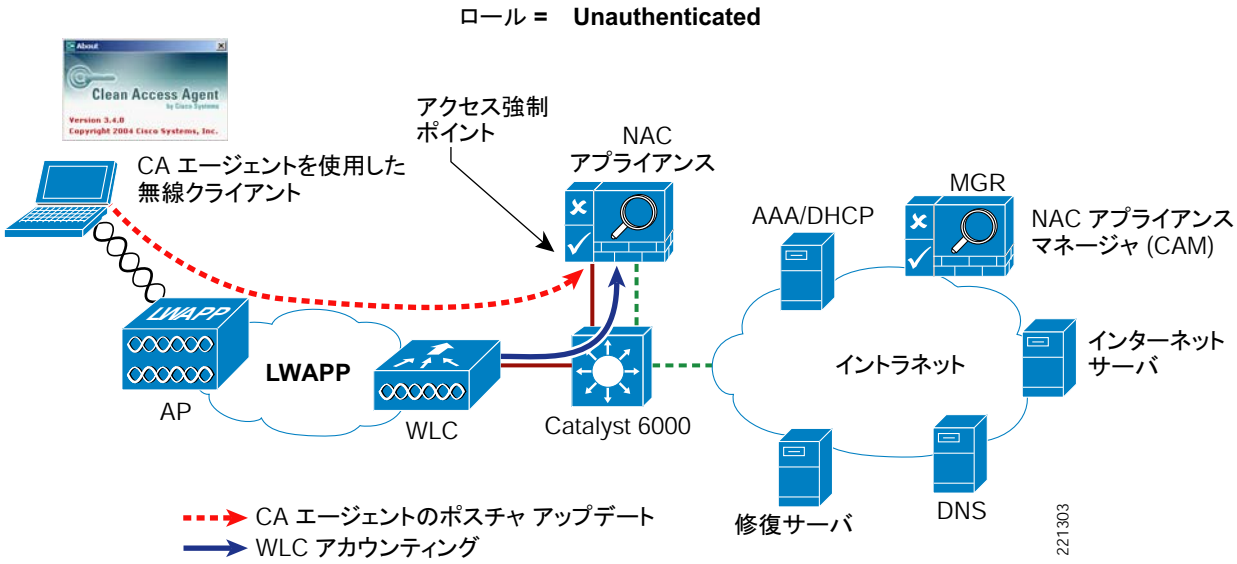


図 5-8 に示すシーケンスは、次のとおりです。

ステップ 1無線ユーザは、WLAN コントローラを通じて、アップストリーム AAA サーバへの 802.1x/EAP 認証を実行します。

ステップ 2クライアントは、AAA サーバまたは DHCP サーバから IP アドレスを取得します。

ステップ 3クライアントが IP アドレスを受信すると、WLC は RADIUS アカウンティング（start）レコードを NAC アプライアンスに転送します。このレコードには、無線クライアントの IP アドレスが含まれています。

（注） WLC コントローラは、802.1x クライアントの認証および IP アドレス割り当てに単一の RADIUS アカウンティング レコード（start）を使用します。一方、Cisco Catalyst スイッチはアカウンティング レコードを 2 つ送信します。802.1x クライアント認証が完了すると accounting start が送信され、クライアントが IP アドレスを割り当てられた後は interim update が送信されます。

ステップ 4 Clean Access Agent は、ネットワーク接続を検出した後、CAM に接続しようとします。トラフィックは NAC アプライアンスによって代行受信され、アプライアンスは、ユーザがオンライン ユーザ リストに記載されているかどうかを CAM に照会して特定します。オンライン ユーザ リストに記載されるのは、認証済みのクライアントに限られます。上の例では、ステップ 3 の RADIUS 更新の結果、この条件に該当します。

ステップ 5 Clean Access Agent は、クライアント マシンのセキュリティ ポスチャおよびリスク ポスチャをローカルで評価し、この評価をネットワーク アドミッション決定のために NAC アプライアンスに転送します。

シングル サインオン Active Directory

シングル サインオン（SSO）Active Directory は、ユーザによる操作を必要とせず、実装も比較的容易なオプションです。Active Directory ドメインに対する Window クライアント認証を利用し、NAC ソリューションの機能を使用して対象ドメインに照会します。併せて、クライアント PC 上で動作する Clean Access Agent ソフトウェアを使用します。Active Directory SSO では、ネットワークに接続されている認証済みの Windows ユーザを Active Directory データベース レコードを使用して NAC アプライアンスに通知します。

SSO 認証、ポスチャ評価、修復、およびネットワーク アクセスを NAC アプライアンス経由で実行する無線クライアントの例については、図 5-9 ～図 5-12 を参照してください。

図 5-9　無線 AD SSO：無線認証 / アソシエーション

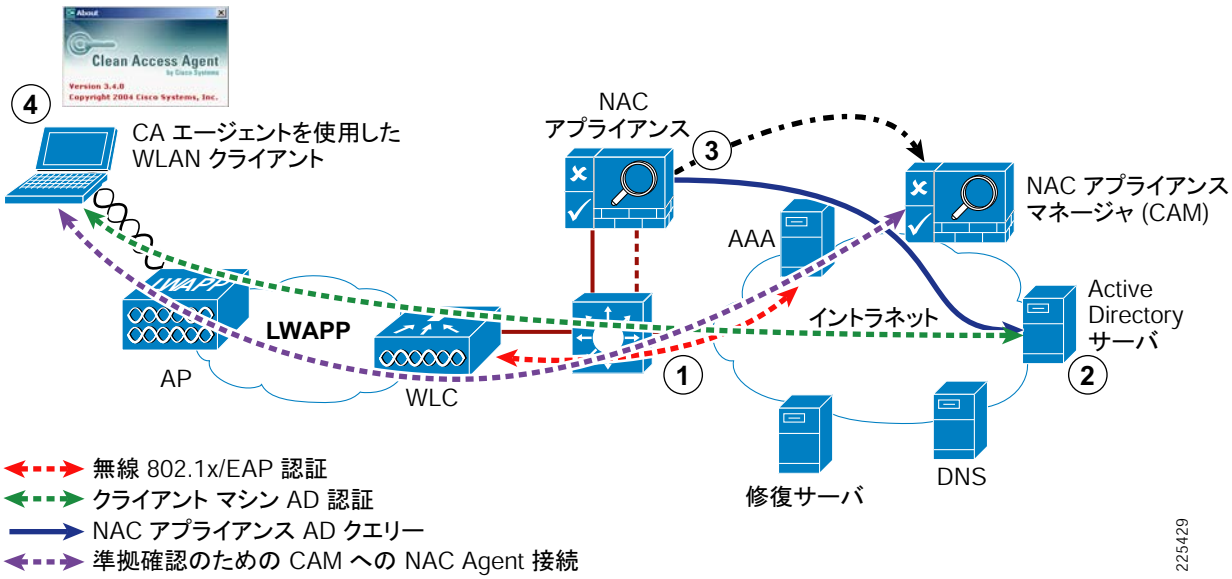


図 5-9 に示すシーケンスは、次のとおりです。

ステップ 1無線ユーザは、WLAN コントローラを通じて、アップストリーム AAA サーバへの 802.1x/EAP 認証を実行します。

ステップ 2クライアントは、AAA サーバまたは DHCP サーバから IP アドレスを取得します。

ステップ 3クライアントが IP アドレスを受信した後、Windows クライアントは、Active Directory ドメインを使用してホスト（マシン）およびクライアントを認証しようとします。

（注）　WLAN クライアント サプリカントは、キャッシュされているクレデンシャルを使用するのではなく、Windows クライアント認証および Active Directory ドメインを許可するように設定する必要があります。ネイティブ Windows サプリカントおよび Cisco Secure Services Client（CSSC）などのサードパーティ サプリカントは、この機能をサポートしています。Clean Access Agent は、ネットワーク接続を検出した後、CAM に接続しようとします。トラフィックは NAC アプライアンスによって代行受信され、アプライアンスは、ユーザが Active Directory で認証されているかどうかを Active Directory に照会して特定します。オンライン ユーザ リストに記載されるのは、認証済みのクライアントに限られます。NAC アプライアンスが CAM を更新します。

ステップ 4 Clean Access Agent は、クライアント マシンのセキュリティ ポスチャおよびリスク ポスチャをローカルで評価し、この評価をネットワーク アドミッション決定のために NAC アプライアンスに転送します。

ポスチャ評価と修復

図 5-10　　無線 SSO：ポスチャ評価

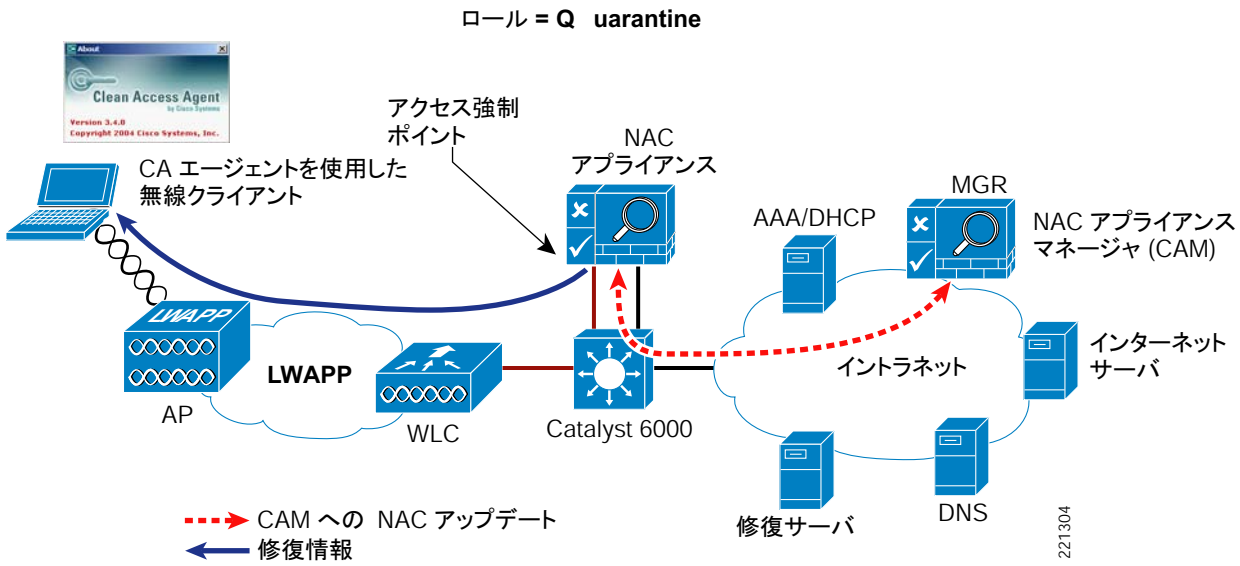


図 5-10 では、次のような動作が行われます。

ステップ 1NAC アプライアンスが、エージェントの評価を NAC アプライアンス マネージャ（CAM）に転送します。

ステップ 2この例では、CAM はクライアントが要件を満たしていないことを特定し、ユーザを Quarantine ロールに移行するよう NAC アプライアンスに指示します。

ステップ 3NAC アプライアンスは、クライアントのエージェントに修復情報を送信します。

図 5-11　無線 SSO：修復

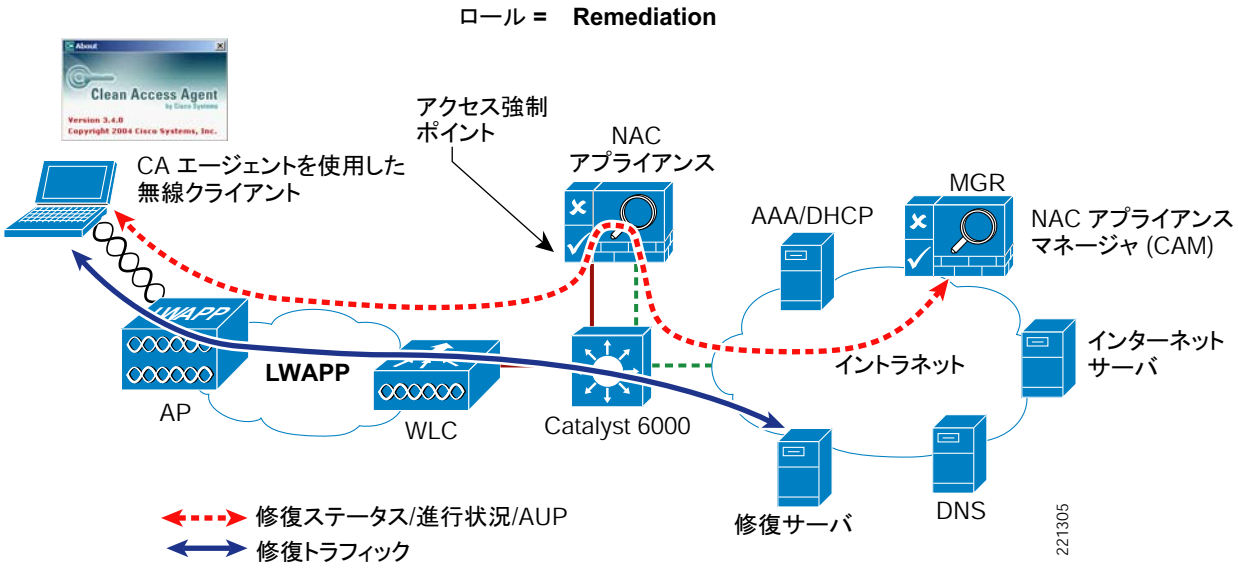


図 5-11 では、次のような動作が行われます。

ステップ 1 Client Agent は、修復が完了するまでの残り時間を表示します。

ステップ 2エージェントは、アンチウイルス定義ファイルの更新など、修復のプロセスを順序に従ってユーザに案内します。

ステップ 3修復が完了すると、エージェントは NAC アプライアンスを更新します。

ステップ 4CAM は、ユーザに Acceptable Use Policy（AUP）ステートメントを表示します。

（注） AUP はオプションであり、ユーザ ロールごとに設定できます。

図 5-12　無線 SSO：ネットワーク アクセス

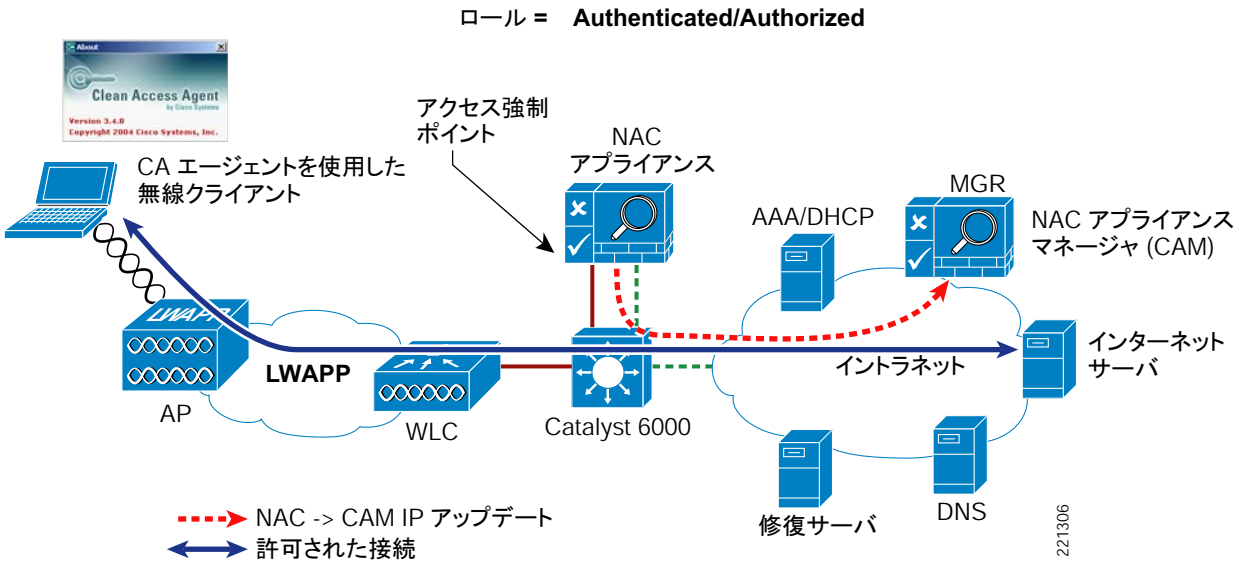


図 5-12 では、次のような動作が行われます。

ステップ 1AUP を受け入れると、NAC アプライアンスはユーザをオンラインの（認可済み）ロールに切り替えます。

ステップ 2SSO 機能によって、オンライン ユーザ リストにクライアントの IP アドレスが入力されます。修復が完了すると、ホストのエントリが証明済みリストに追加されます。これらのテーブルは、（検出済みクライアントのテーブルとともに）いずれも CAM によって管理されます。

ステップ 3エンド ユーザは、ネットワーク経由で通信できるようになります。

上で説明したように、無線ユーザ認証を導入する場合に透過性が最も高いのは、NAC アプライアンス上で SSO 認証を有効にする方法です。

（注） クライアント PC に Clean Access Agent がインストールされていない状態で VPN-SSO 認証を有効にした場合でも、ユーザは自動的に認証されます。ただし、ユーザが Web ブラウザを開いて接続を試行するまでは、NAC アプライアンスを通じてユーザが自動的に接続されることはありません。この場合、ユーザが Web ブラウザを開くと、「エージェントレス」のポスチャ評価フェーズが進行している間、ユーザは一時的にリダイレクトされます（ログイン プロンプトは表示されません）。合格したクライアントは、最初に要求した URL に接続されます。合格しないクライアントは、修復のための必要なリンクまたはサイトに転送されます。前述の動作で前提となるのは、非エージェントベースの PC がこの方法でネットワークに接続することについて、ネットワークの管理者が NAC アプライアンスの設定で許可することです（P.5-18 の「脆弱性の評価と修復」を参照）。

脆弱性の評価と修復

Cisco NAC アプライアンス ソリューションの中心となる機能は、ユーザにネットワークへのアクセスを許可する前に、クライアント デバイスの脆弱性を検出して修正することです。脆弱性評価と修復ポリシーの設定については、『Cisco *NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 9 章と第 10 章を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html で入手できます。

簡単に要約すると、クライアントの脆弱性を確認する方法には次の 2 つがあります。

- ネットワーク スキャン：ネットワークベースの脆弱性評価と Web ベースの修復を提供します。これは、NAC アプライアンスが備えているネットワーク スキャナ機能であり、実際のスキャンや、特定のホストに多い既知のポート脆弱性のチェックを実行します。脆弱性が発見されると、CAM に設定されている Web ページがユーザに表示され、Web サイトへのリンクまたはシステムの修正方法に関する情報が提示されます。
- Clean Access Agent：脆弱性評価と修復に、常駐型でマシンベースのソフトウェア エージェントを使用します。ユーザは Cisco Clean Access Agent をダウンロードしてインストールする必要があります。これによって、管理者は、ホスト レジストリ、プロセス、インストール済みアプリケーション、およびシステム サービスを簡単に表示できるようになります。このエージェントを使用すると、ユーザがシステムを修正できるように、アンチウイルス / アンチスパイウェア定義の更新、Clean Access Manager（CAM）にアップロードされたファイルの配布、または Web サイトへのリンクの配布を実行できます。

Unified Wireless ネットワークでどの方法を使用できるかについては、制約はありません。展開によっては、両方の方法を同時に使用することもできます。ただし、採用可能な 2 つのオプションの中では、可能な限りエージェントベースの評価と修復を導入することをお勧めします。理由は次のとおりです。

- 認証に関して、無線クライアントにとって最も良好なユーザ エクスペリエンスが提供されます。
- 脆弱性の評価と修復は、クライアント PC 上でローカルに実行されます。NAC アプライアンスおよび NAC マネージャでは実行されないため、ソリューション全体のパフォーマンスが向上します。

ローミングに関する考慮事項

詳細については、『*Enterprise Mobility 4.1 Design Guide*』の第 2 章の「Roaming」の項を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

Cisco Unified Wireless ソリューションは、次のローミング シナリオをサポートしています。

1. 同一の WLC に接続されている 2 つの AP 間でのレイヤ 2 クライアント ローミング。
2. 別の WLC に接続されている 2 つの AP 間でのレイヤ 2 クライアント ローミング。
3. 別の WLC に接続されている 2 つの AP 間でのレイヤ 3 クライアント ローミング。各 WLC は、WLAN をそれぞれ別の VLAN またはサブネットにマップします。

P.5-3 の「Unified Wireless Network での NAC アプライアンスのモードおよび配置」で簡単に説明したように、NAC アプライアンスはインバンドで配置し、WLC のレイヤ 2 隣接ノードにする必要があります。つまり、所定のユーザ WLAN に関連付けられている VLAN およびサブ

ネットは、NAC アプライアンスの Untrusted インターフェイスに直接トランキングされます。以降で説明するローミング動作は、NAC アプライアンスでバーチャル ゲートウェイと Real-IP ゲートウェイのどちらの機能が設定されている場合でも同一です。

NAC アプライアンスを使用したレイヤ 2 ローミング

上のシナリオ 1 と 2 では、クライアントが AP 間でローミングした場合、ユーザのトラフィックは同一の VLAN またはサブネット上に維持されるため、同一の VLAN を経由して NAC アプライアンスに転送されます。したがって、上のシナリオ 1 と 2 の両方でローミングがサポートされます。シナリオ 2 に基づいたクライアント ローミングの例については、図 5-13 および図 5-14 を参照してください。

図 5-13　　WLC レイヤ 2 間ローミング：クライアント /NAC の初期接続

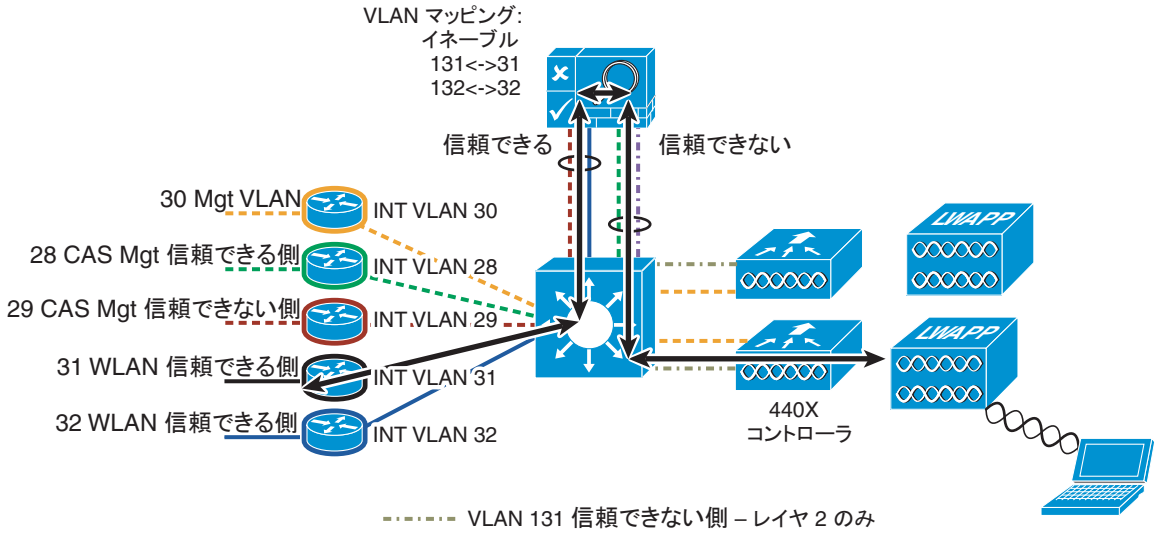


図 5-12 では、クライアントは WLAN に対して認証とアソシエーションを実行し、VPN SSO および Clean Access Agent クライアント ソフトウェアによって NAC を経由して自動接続されます。無線 SSO の詳細については、P.5-64 の「無線シングル サインオンの有効化」を参照してください。

図 5-14　WLC レイヤ 2 間ローミング：クライアントのローミング

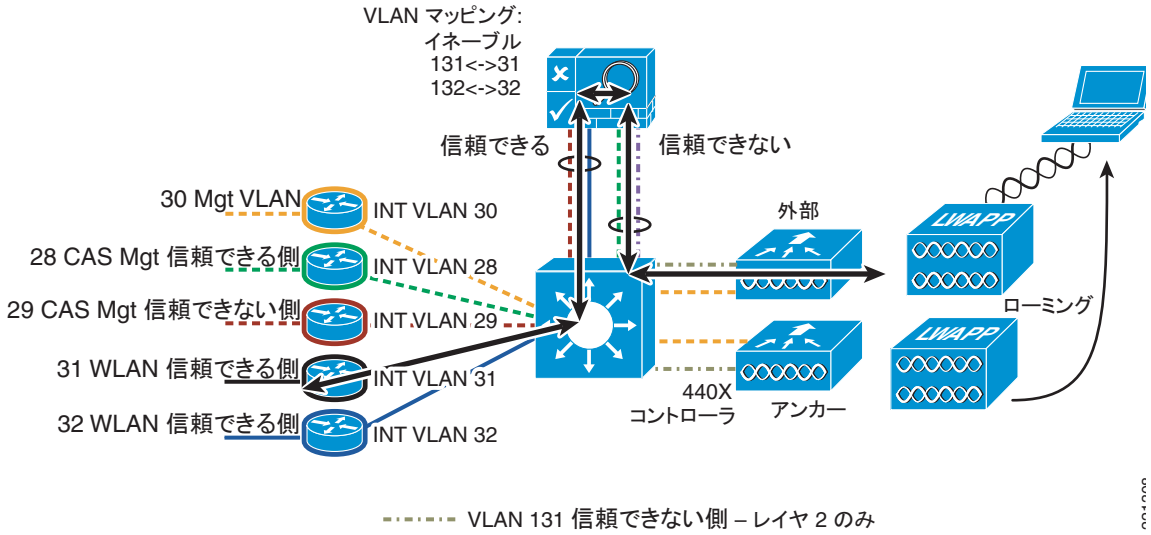


図 5-14 のクライアントが、別の WLC に接続されている AP にローミングした場合、外部コントローラ上の WLAN は同一の（信頼できない）VLAN にアンカー WLC としてマップされているため、接続は維持されます。

NAC アプライアンスを使用したレイヤ 3 ローミング：WLC イメージ 4.0 以前

上のシナリオ 3 に基づいたローミングでは、コントローラ間にある 2 つ以上の VLAN またはサブネットが WLAN をサポートしている場合に問題が生じます。問題は、別のサブネットが使用されているということではなく、モビリティ トンネルのアシンメトリック動作にあります。無線クライアントが認証を受けて NAC アプライアンス経由で接続すると、トラフィックは、アンカー（ホーム）コントローラで WLAN のマップ先となっている VLAN 上で、NAC アプライアンスの Untrusted インターフェイスに到達します。クライアントがローミングしたとき、NAC アプライアンスでのクライアントのステータスは、VPN SSO および Clean Access Agent が使用されている限り、認証済みのままです。

シナリオ 3 の場合、（コントローラ間のローミングを容易にするために）コントローラ間で確立されたモビリティ トンネルは影響を受けません。（モビリティ トンネルの確立に利用される）管理 VLAN は、NAC アプライアンスの Untrusted インターフェイスにトランキングされないためです。クライアントが外部（ローミング先）コントローラへのローミングを完了すると、WLAN からのクライアント トラフィックは、別の VLAN またはサブネットを経由して NAC アプライアンスの Untrusted インターフェイスに転送されるようになります。ローミング イベントは、Unified Wireless ネットワークという観点からは成功していますが、NAC アプライアンスはクライアント トラフィックをブロックします。アプライアンスは、2 つの異なる信頼できない VLAN またはサブネットを同時に経由する場合はユーザのトラフィックをスイッチしないためです。

NAC アプライアンスがユーザ トラフィックをスイッチするのは、ユーザが認証を受けた当初の VLAN を経由する場合のみです。レイヤ 3 境界を越えてローミングを試行するクライアントの例については、図 5-15 および図 5-16 を参照してください。

図 5-15　WLC レイヤ 3 間ローミング：WLAN/NAC の初期接続

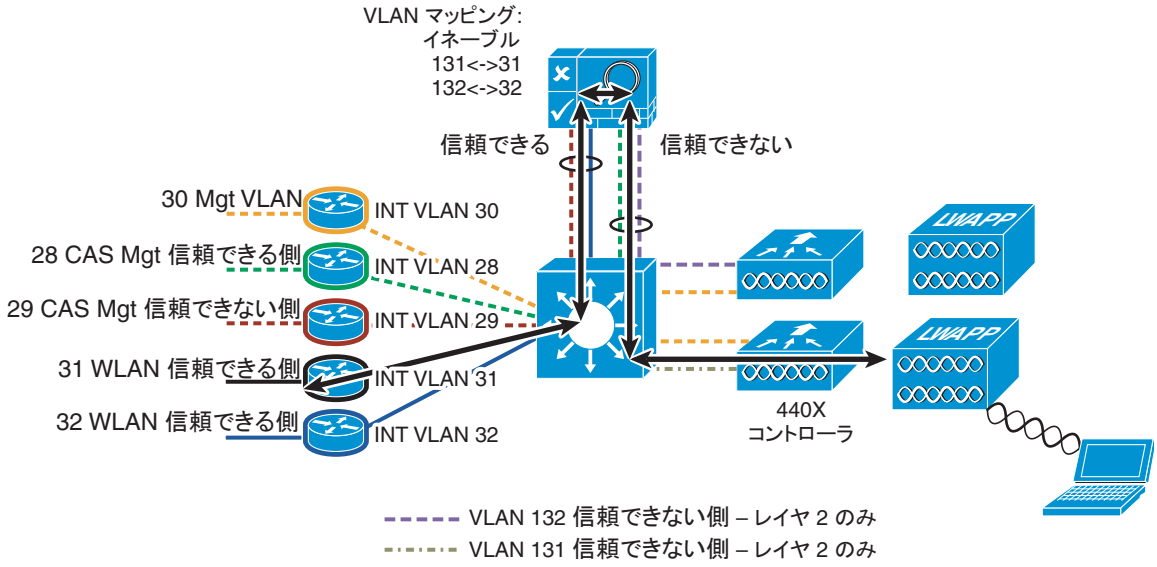


図 5-15 では、クライアントは WLAN に対して認証とアソシエーションを実行し、VPN SSO および Clean Access Agent クライアント ソフトウェアによって NAC を経由して自動接続されます。この他のコントローラは、別の VLAN（132）を使用していることに注意してください。

図 5-16　WLC レイヤ 3 間ローミング：クライアントのローミング

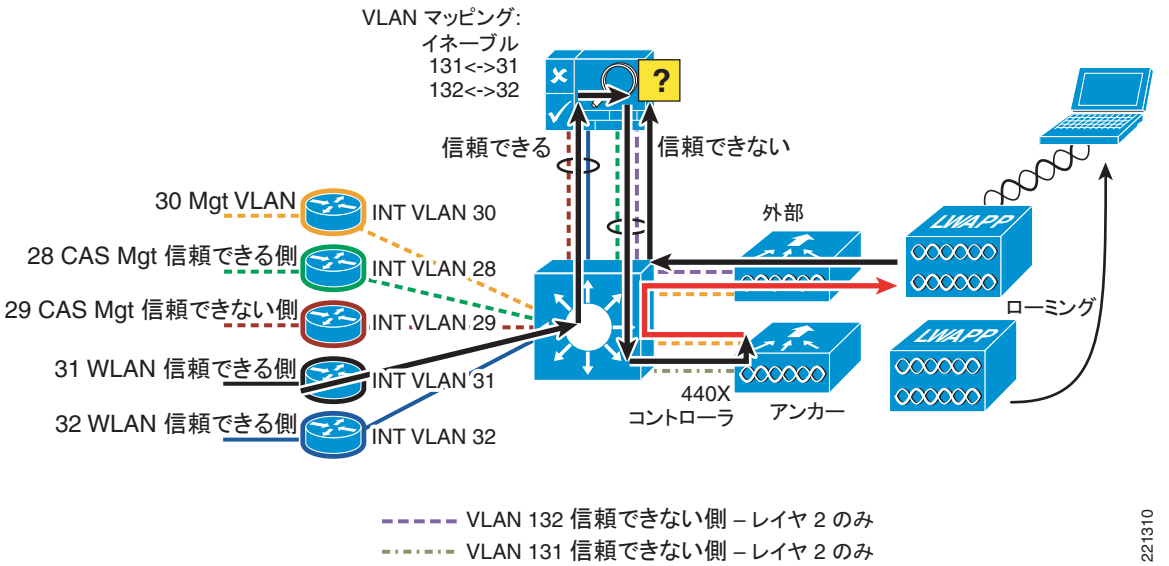


図 5-16 のクライアントが他のコントローラ上の AP にローミングした場合、接続は中断されます。外部（ローミング先）のコントローラは、トラフィックを別の信頼できない VLAN 経由で NAC アプライアンスに転送するためです。

リリース 4.0 以前のコントローラを使用している場合、NAC のサービスを使用したレイヤ 3 ローミングを導入するための対応策はありません。

NAC アプライアンスを使用したレイヤ 3 ローミング：WLC イメージ 4.1 以降

WLC モビリティ トンネルのアシンメトリック動作は、NAC アプライアンス展開で問題となるだけでなく、Cisco Firewall Service Module（FWSM; ファイアウォール サービス モジュール）を Unified Wireless 展開と併せて使用する展開、およびユニキャスト Reverse Path Forwarding（uRPF）確認がルータ インターフェイスまたは SVI 上で有効になっている展開でも問題が発生します。WLC リリース 4.1 以降では、シンメトリックに動作するようモビリティ トンネルを設定できるため、アンカー コントローラを経由して、クライアント トラフィックを双方向で転送できます。クライアントのトラフィックは、WLAN が外部（ローミング先）コントローラ上の別の VLAN またはサブネットにマップされているかどうかにかかわらず、ユーザが認証を受けた当初の VLAN またはサブネット上に維持されます（図 5-17 を参照）。

図 5-17　シンメトリック モビリティ トンネルを使用した WLC レイヤ 3 間ローミング

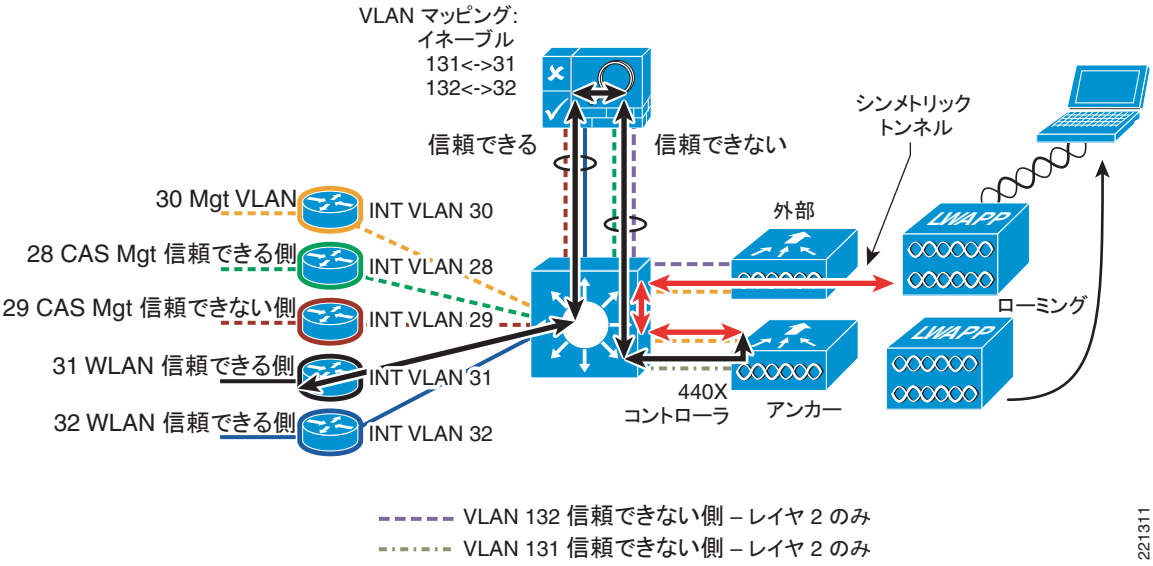


図 5-17 のクライアントがレイヤ 3 ローミングとなる場合は、シンメトリック モビリティ トンネルにより、返信のトラフィックがアンカー コントローラに転送されます。アンカー コントローラは、ユーザが認証を受けた当初の NAC VLAN 上にユーザ トラフィックを維持します。NAC アプライアンスを通じたクライアント接続が維持されます。このシンメトリック トンネリング動作は、ソフトウェア リリース 5.2 以降ではデフォルトになります。

NAC アプライアンスと AP グループを使用したローミング

典型的な展開では、WLAN は WLC ごとに単一の動的なインターフェイスにマップされます。しかし、ここで、最大 100 台までの AP をサポートする 4404-100 WLC が使用される展開シナリオを考えてみてください。各 AP に 25 ユーザがアソシエートされているとします。この結果、2,500 人のユーザが 1 つの VLAN を共有することになります。パフォーマンス上の理由により、お客様の設計によっては、サブネットのサイズを非常に小さくすることが要求される場合もあります。このような要求に対処するには、WLAN を複数のセグメントに分割するのも 1 つの方法です。WLC の AP グループ機能により、コントローラ上の複数の動的インターフェイ

ス（VLAN）で 1 つの WLAN をサポートできるようになります。そのためには、AP のグループを特定の動的インターフェイスにマップします。AP は、従業員のワークグループや物理的な設置場所に基づいて、論理的にグループ化することができます。

WLAN の SSID は複数の AP グループにわたって実装可能であり、AP グループはそれぞれ異なる VLAN またはサブネットにマップされます。したがって、ユーザは WLAN の内部で AP グループの境界を越えてローミングする場合があります。考えられるシナリオは、次のとおりです。

- 異なる AP グループに所属するが、同一のコントローラに接続されている 2 つの AP 間でクライアントがローミングする場合。このローミング シナリオは、NAC アプライアンスが Unified Wireless トポロジを使用して実装されている場合は影響を受けません。クライアントは、別の AP グループの AP にローミングした場合も、当初の接続に使用した同じ動的インターフェイス（VLAN）上に維持されます。このローミング動作は、P.5-19 の「NAC アプライアンスを使用したレイヤ 2 ローミング」で説明したレイヤ 2 ローミングと変わりません。
- 次に、それぞれ異なる AP グループに所属する別個のコントローラに接続された、2 つの AP 間でクライアントがローミングする場合。このシナリオは、P.5-18 の「ローミングに関する考慮事項」のシナリオ 3 と類似しています。複数のコントローラを展開してそれぞれ別の動的インターフェイス（VLAN またはサブネット）を使用することで、キャンパス展開全体にわたって一般的な WLAN をサポートします。唯一異なる点は、WLC 上で AP グループが設定されないことです。上の例に基づいてローミング イベントが発生した場合、P.5-22 の「NAC アプライアンスを使用したレイヤ 3 ローミング：WLC イメージ 4.1 以降」で説明したレイヤ 3 ローミング イベントと同一の結果になります。クライアントが当初に認証を受けたアンカー コントローラ上の AP グループ VLAN ではなく、別の AP グループ VLAN を通じて外部コントローラがクライアント トラフィックを転送しようとすると、クライアントは NAC で停止します。

（注）　WLAN コントローラのシンメトリック モビリティ トンネル機能が使用されている場合（P.5-22 の「NAC アプライアンスを使用したレイヤ 3 ローミング：WLC イメージ 4.1 以降」を参照）、AP グループ境界を越えるローミングがサポートされます。

Unified Wireless での NAC アプライアンス ハイ アベイラビリティの実装

ハイ アベイラビリティを必要とする展開では、NAC アプライアンスを 1:1 のホット スタンバイ構成で展開できます。このシナリオでは、一方の NAC アプライアンスがアクティブになり、もう一方はスタンバイ モードになります。2 つのサーバは、インバンドまたはアウトオブバンドの通信を使用して互いに通信します。各サーバの状態の特定には、アプライアンス間の通信「リンク」が使用されます。NAC アプライアンスの設定が変更された場合は、CAM がアクティブ アプライアンスとスタンバイ アプライアンスの両方に同時に変更内容をプッシュします。アクティブ サーバからスタンバイ サーバへのフェールオーバーは、ステートフルです。詳細については、『*Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*』の第 13 章を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html で入手できます。

また、NAC アプライアンス ハイ アベイラビリティを導入した概略的 Unified Wireless トポロジの例については、図 5-18 を参照してください。

図 5-18　NAC アプライアンス ハイ アベイラビリティを導入した Unified Wireless 展開

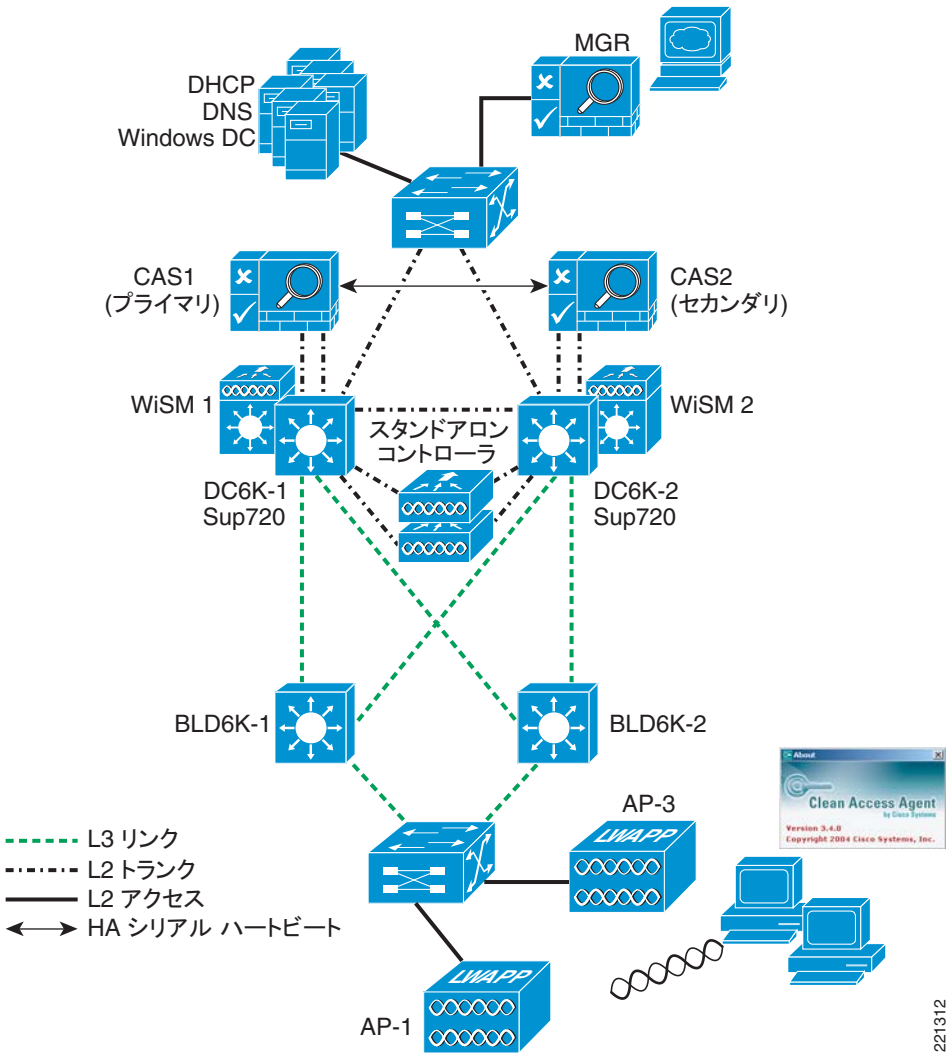


図 5-18 に、アクティブ / スタンバイの NAC アプライアンスを導入した、完全に冗長的なキャンパス トポロジを示します。

P.5-4 の「インバンド モード」で説明したように、NAC アプライアンスはバーチャル ゲートウェイまたは Real-IP ゲートウェイのいずれかとして設定できます。アプライアンスと WLAN コントローラ間の物理的な相互接続は、ゲートウェイの方式にかかわらず同一です。論理上の設定の違いについては、以降の該当する項で説明します。

ハイ アベイラビリティ NAC アプライアンス /WLC の基盤

図 5-19 および図 5-20 に、データ センターの全体的なスイッチ ブロックに組み込まれた WLC と NAC アプライアンスの相互接続について、詳細なダイヤグラムを示します。次のスイッチ ブロックの例は、既存のデータ センター サーバ ファームのスイッチ ブロックに組み込まず、スタンドアロンにする必要があります。

図 5-19　ハイ アベイラビリティ NAC/WLC スイッチ ブロック：バーチャル ゲートウェイ モード

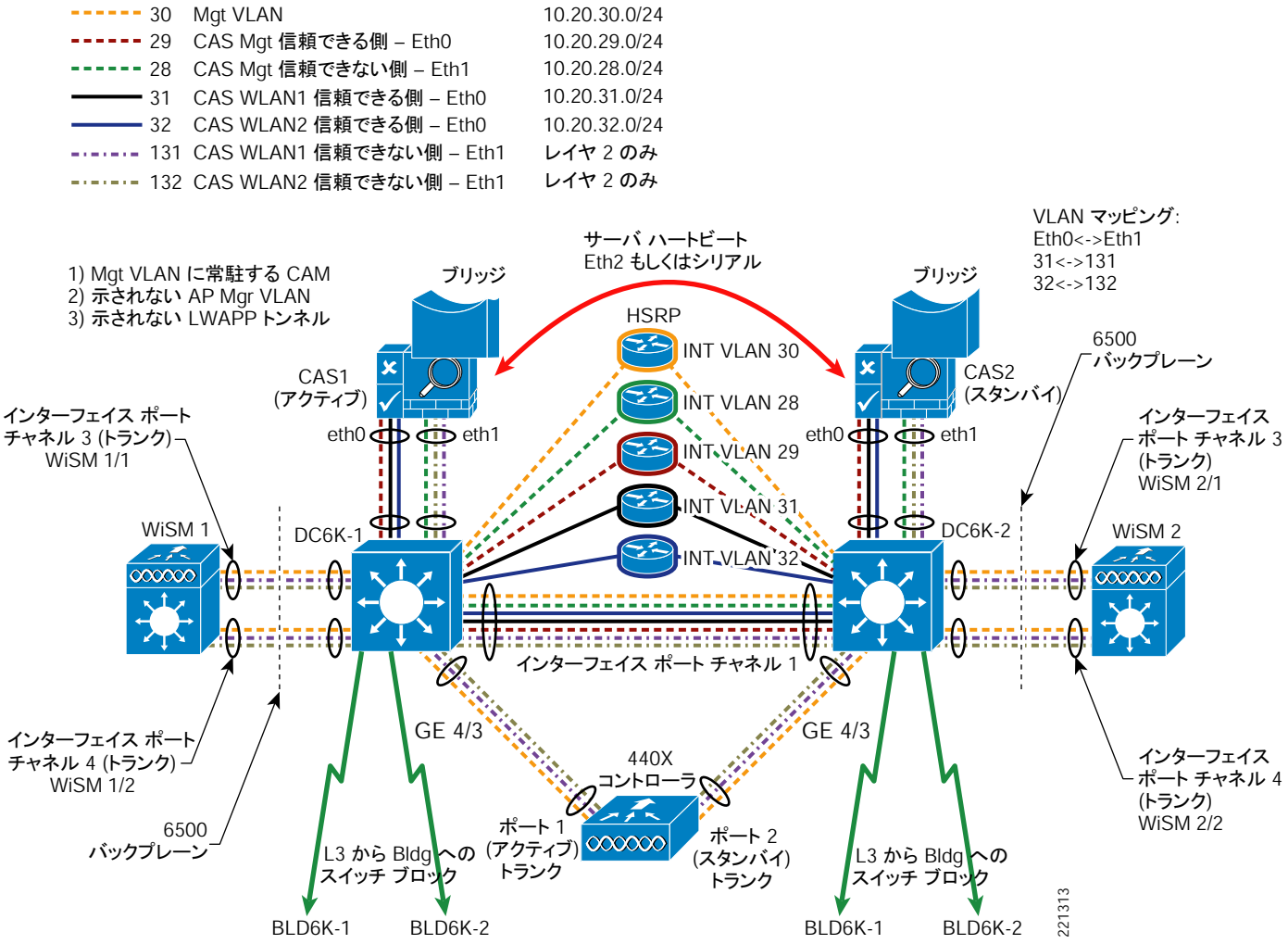
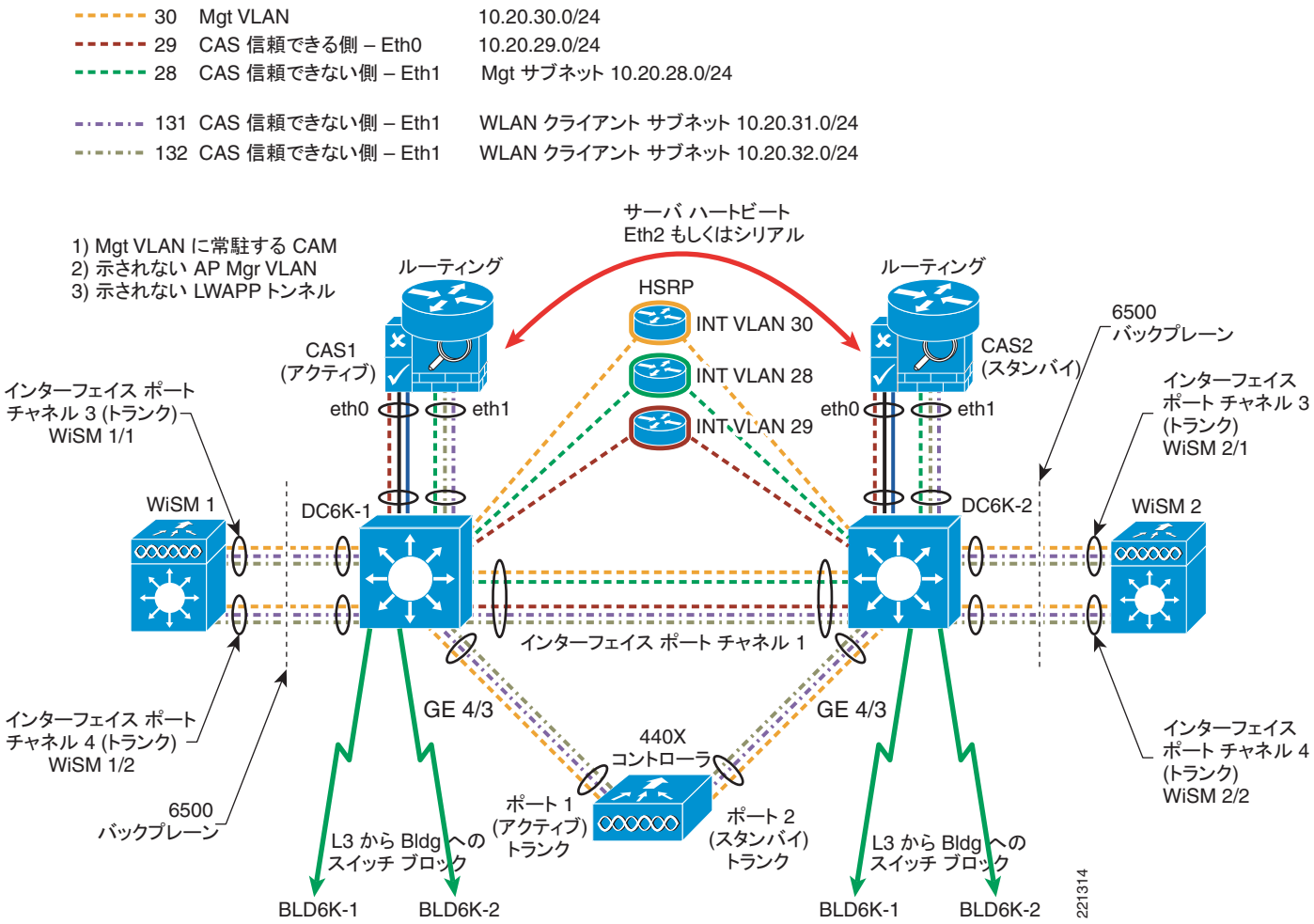


図 5-20　ハイ アベイラビリティ NAC/WLC スイッチ ブロック：Real-IP ゲートウェイ モード



この 2 つのトポロジ例の主な違いは、無線ユーザ VLAN の終端となる地点です。バーチャル ゲートウェイの例では、各ユーザ VLAN が（VLAN マッピングを使用して）NAC アプライアンス経由でブリッジされ、Catalyst スイッチ上の VLAN 固有の SVI が終端となります。Real-IP ゲートウェイの例では、ユーザ VLAN は NAC アプライアンスの Untrusted インターフェイス上が終端となります。次に、Trusted インターフェイス Eth0（VLAN 29）を経由して、アプライアンスがトラフィックをネットワークに転送（ルーティング）します。図 5-21 および図 5-22 は、図 5-19 および図 5-20 を簡略化したものです。

図 5-21　バーチャル ゲートウェイ トポロジの例（簡略図）

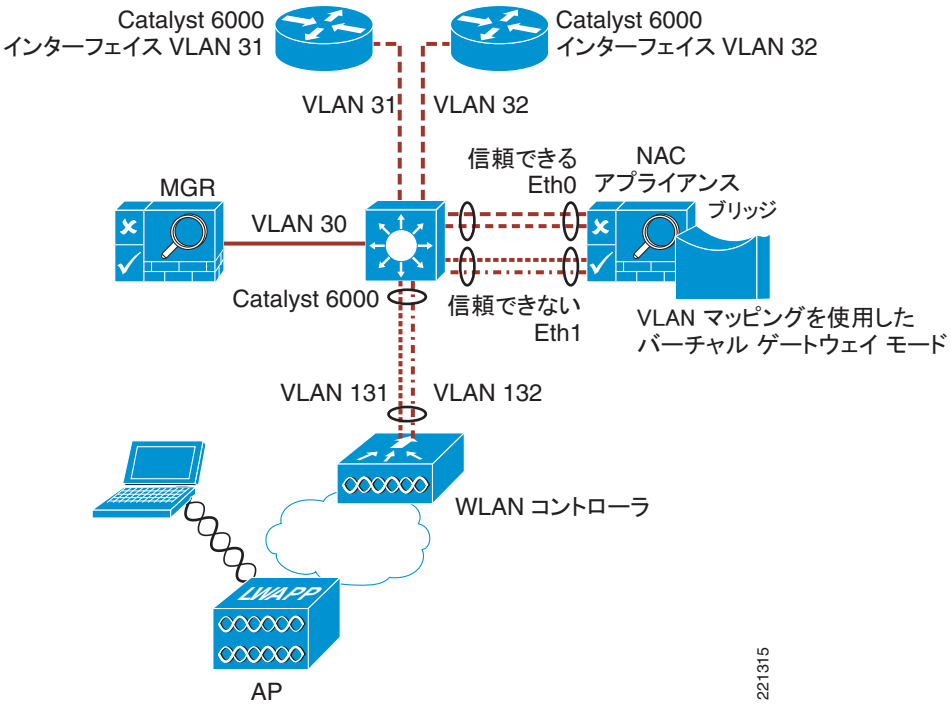
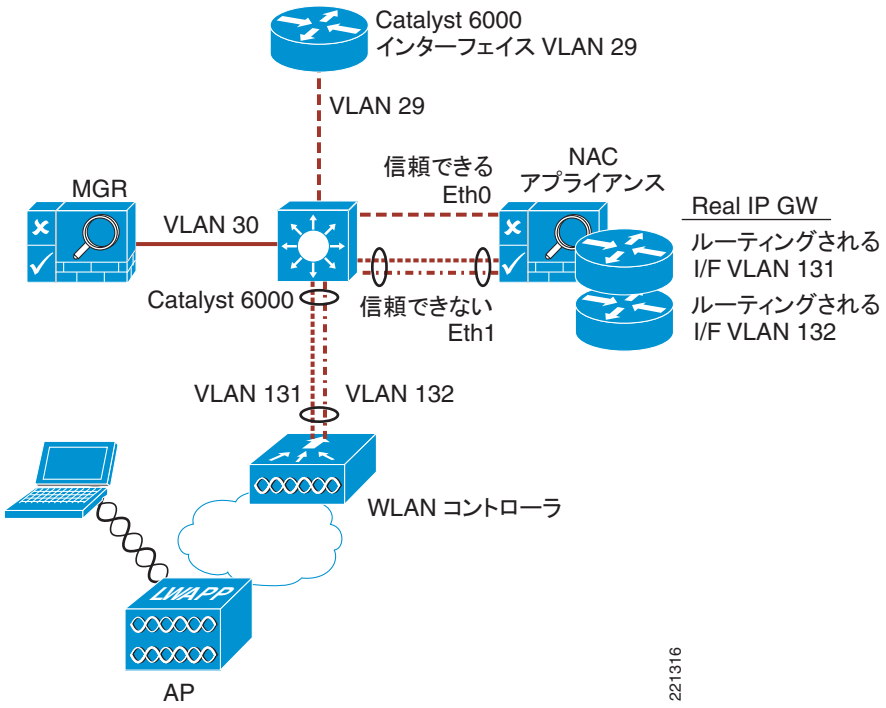


図 5-22　Real-IP ゲートウェイ トポロジの例（簡略図）



WLC 接続

各 WLC（スタンドアロンまたは WiSM モジュール）は、802.1q トランク（複数可）経由でスイッチ ブロックに接続されます。WLC 管理インターフェイスおよび AP 管理インターフェイスの VLAN は、NAC アプライアンスにトランキングされません。これらの VLAN は、Catalyst 6000 上で HSRP 動作用に設定された SVI に直接マップされる必要があります。このように設定することで、管理、RADIUS、LWAPP、およびモビリティ トンネルのトラフィックが NAC アプライアンスを経由せずに済みます。

WLC 動的インターフェイス VLAN

NAC アプライアンスのゲートウェイ方式にかかわらず、NAC のサービスを必要とする WLAN に関連付けられている動的インターフェイス（VLAN）は、NAC アプライアンスの Untrusted インターフェイス（Eth1）に直接トランキングされる必要があります。これらの VLAN については、対応する SVI を Catalyst 6000 上に設定しないでください。

NAC アプライアンスの接続

各 NAC アプライアンスは、802.1q トランクを通じてスイッチ ブロックに接続されます。

NAC 管理 VLAN

Eth0（Trusted）インターフェイスおよび Eth1（Untrusted）インターフェイスは、管理目的の専用 VLAN を使用します。Eth0 管理 VLAN は、CAM/NAC の通信に加えて、HA 動作のリンク ステータス認識にも使用されます。Eth1 管理 VLAN は、NAC アプライアンスが HA トポロジに展開された場合のリンク ステータス認識のみに使用されます。

Eth0 と Eth1 管理 VLAN の両方を、Catalyst 6000 上で HSRP 動作用に設定された SVI にマップする必要があります。信頼できる側の管理 VLAN（Eth0）は、CAM とは異なるサブネットに配置する必要があります。NAC アプライアンスを HA トポロジに展開しない場合は、信頼できない側の管理 VLAN/ インターフェイス（Eth1）を Eth0 管理インターフェイスと同一の IP アドレスで設定できます。

NAC 無線ユーザ VLAN

Unified Wireless LAN 展開では、エンド ユーザの VLAN は WLC の動的インターフェイスに関連付けられている VLAN です。これらの VLAN は、WLC から NAC アプライアンスの Untrusted インターフェイス（Eth1）に直接トランキングされる必要があります。

バーチャル ゲートウェイ モード

NAC アプライアンスの Untrusted インターフェイスにトランキングされるエンド ユーザ VLAN ごとに、アプライアンスの Trusted インターフェイス（Eth0）上に、関連付けられた VLAN が存在している必要があります（P.5-6 の「インバンド バーチャル ゲートウェイ」を参照）。所定の WLAN では、信頼できる VLAN と信頼できない VLAN の間に 1:1 の関係が存在します。信頼できる側の各 VLAN は、Catalyst 6000 上で HSRP 動作用に設定された SVI にマップされます。

Real-IP ゲートウェイ モード

Real-IP ゲートウェイ モードでは、NAC アプライアンスはルータとして機能します。したがって、各エンド ユーザ VLAN は、NAC アプライアンスの Untrusted インターフェイス（Eth1）上のルーテッド サブインターフェイスとして終端します。

スイッチ間の接続

ハイ アベイラビリティ トポロジを正常に運用するには、基盤となる 2 台の Catalyst 6000 の間に 802.1q トランクを確立する必要があります。WLC/NAC 管理（信頼できないトラフィックおよび信頼できるトラフィック）に関連付けられているすべての VLAN が、トランクの通過を許可される必要があります。

（注）　スイッチ間のトランクは、インターフェイス ポート チャネル（スイッチ間の複数の物理リンク）で構成することを強くお勧めします。これは、パフォーマンス上の理由だけでなく、NAC アプライアンス間のハートビート リンクの信頼性と弾力性を確保するためです（P.5-29 の「NAC アプライアンス間の接続」を参照）。

NAC アプライアンス間の接続

ステートフルなフェールオーバーを実現するには、2 つのアプライアンス間でインバンドまたはアウトオブバンドのリンクを確立する必要があります。このリンクは、ステータス、設定、および同期化の情報を 2 つのプラットフォーム間で転送するために使用されます。

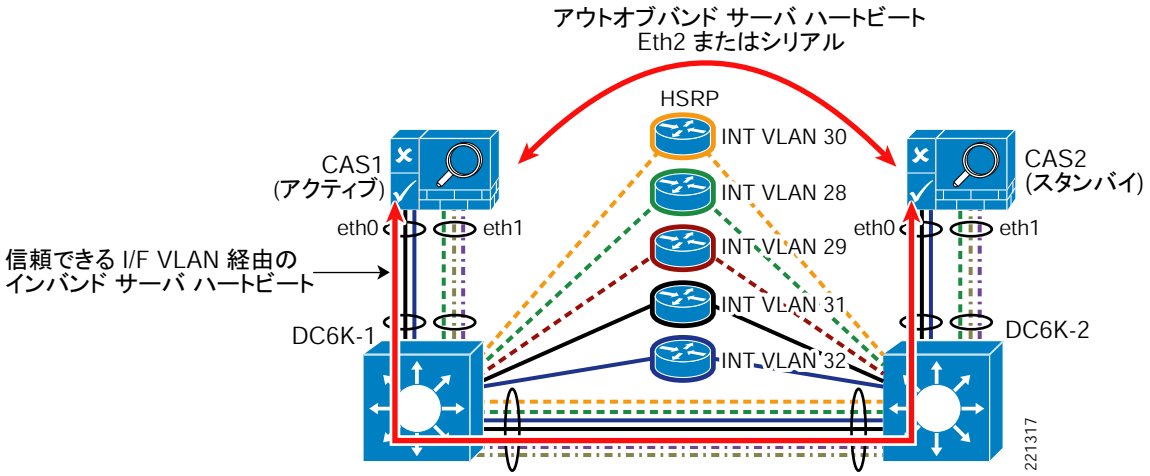
アウトオブバンドには、次の 2 つのオプションがあります。

- 各 NAC アプライアンスのコンソール ポートまたはセカンダリ シリアル ポートを使用したポイントツーポイント シリアル接続
- 各 NAC アプライアンスの 3 番目のイーサネット インターフェイスを使用したポイントツーポイント クロスオーバー イーサネット接続

また、各 NAC アプライアンス上の信頼できる管理（VLAN）インターフェイスを経由して、レイヤ 2 インバンド接続を確立する方法もあります。

（注）　ループ トポロジの形成を予防するため、インバンド サーバ ハートビート方式を使用することを*強くお勧めします*。P.5-30 の「ループ トポロジの防止：バーチャル ゲートウェイ モード」を参照してください。

図 5-23　NAC アプライアンス サーバ ハートビート リンク



ループ トポロジの防止：バーチャル ゲートウェイ モード

アプライアンス間の通信にアウトオブバンド リンクを使用していて、そのリンクが何らかの理由で切断された場合、各 NAC アプライアンスはアクティブなオンライン状態と見なされます。これにより、ユーザ VLAN にわたるレイヤ 2 ループ トポロジが作成されます。これは、VLAN マッピング方式を使用して NAC アプライアンスがブリッジされている場合、Per VLAN Spanning-Tree（PVST）BPDU が転送されないためです。1 つまたはそれ以上の信頼できないクライアント VLAN を発信元とするブロードキャストが、NAC を経由して信頼できる側の VLAN に転送されます。同様に、逆方向の転送も発生します。したがって、両方の NAC アプライアンスが同時にアクティブになった場合、ブロードキャスト ストームが発生します。

このため、インバンドのハートビート方式を使用する必要があります。この場合は、Trusted 管理インターフェイスを通じて、サーバ間に論理 IP/UDP 接続が確立されます。トポロジの内部で障害が発生してサーバ間の論理リンクが切断された場合、両方の NAC アプライアンスが同時にアクティブ状態になった場合に形成されるループも切断されます。

つまり、インバンドとアウトオブバンドの両方のリンクを使用することで、プライマリ NAC アプライアンスが非アクティブになってから再度アクティブになった場合の元の状態に戻らない動作が保証されます。バックアップ NAC アプライアンスが（スケジュールに従って、または不定期に）シャットダウンされるか、そのアプライアンスの Trusted インターフェイスまたは Untrusted インターフェイス上で障害が検出されるまで、ユーザ セッションはバックアップ NAC アプライアンス上に維持されます。

（注）　上の「ループ トポロジ」の脆弱性は、NAC アプライアンスを Real-IP ゲートウェイとして展開する場合は発生しません。ただし、Real-IP ゲートウェイ展開についても、上で説明したものと同一のアプライアンス間通信方式を使用することをお勧めします。

ハイ アベイラビリティ フェールオーバーに関する考慮事項

次のいずれかに該当する場合は、アクティブなアプライアンスからスタンバイ アプライアンスへのステートフル フェールオーバーが発生します。

- アクティブなアプライアンスがリブートされた。
- アクティブなアプライアンスが、スタンバイ アプライアンスのハートビート メッセージに応答しなかった（アプリケーションの障害）。
- アクティブなアプライアンス：Trusted インターフェイス（Eth0）の物理リンクがダウンした。
- アクティブなアプライアンス：Trusted インターフェイス（Eth0）の論理リンク ハートビート（ping）が失敗した。
- アクティブなアプライアンス：Untrusted インターフェイス（Eth1）の物理リンクがダウンした。
- アクティブなアプライアンス：Untrusted インターフェイス（Eth1）の論理リンク ハートビート（ping）が失敗した。

上のいずれかに該当した場合は、スタンバイの NAC アプライアンスが約 30 秒以内にアクティブになります。WLAN コントローラ SSO（VPN-SSO）が設定され、クライアント マシンで Clean Access Agent ソフトウェアが動作している場合、エンド ユーザのセッションはバックアップ NAC アプライアンスを使用して自動的に復元されます。ソリューションが上のいずれかの状態から回復するまでの所要時間は、設定可能な次の 2 つのタイマーに基づいて決まります。

- リンク ハートビート タイマー：Trusted インターフェイスと Untrusted インターフェイスのリンク ステータスを監視します。推奨設定は 25 秒以上です。
- サーバ ハートビート タイマー：インバンドまたはアウトオブバンドのサーバ ハートビート リンクを監視します。推奨設定は 15 秒以上です。

NAC アプライアンスが Real-IP ゲートウェイとして設定されている場合、上のシナリオ 3 または 4 に基づいた障害が発生すると、NAC アプライアンスは正常にフェールオーバーしますが、クライアントは停止します。この問題の回避策は次のとおりです。

- クライアントの ARP キャッシュを手動で消去する（Windows のコマンドラインから **arp -d** を実行）。
- クライアントの WLAN アダプタを一時的に無効にし、有効にする。
- クライアントのデフォルト ゲートウェイ ARP キャッシュ エントリがタイムアウトして更新されるまで、待機する。
- バーチャル ゲートウェイ動作用の NAC アプライアンス ペアを設定する。

Unified Wireless での非冗長 NAC の実装

P.5-23 の「Unified Wireless での NAC アプライアンス ハイ アベイラビリティの実装」で説明したガイドラインは、NAC アプライアンスを 1 つのみインストールする実装の場合も、ほぼすべて有効です。スタンドアロンで動作するように設定された単一の NAC アプライアンスを、単一または冗長のマルチレイヤ スイッチで構成されるトポロジに統合できます。

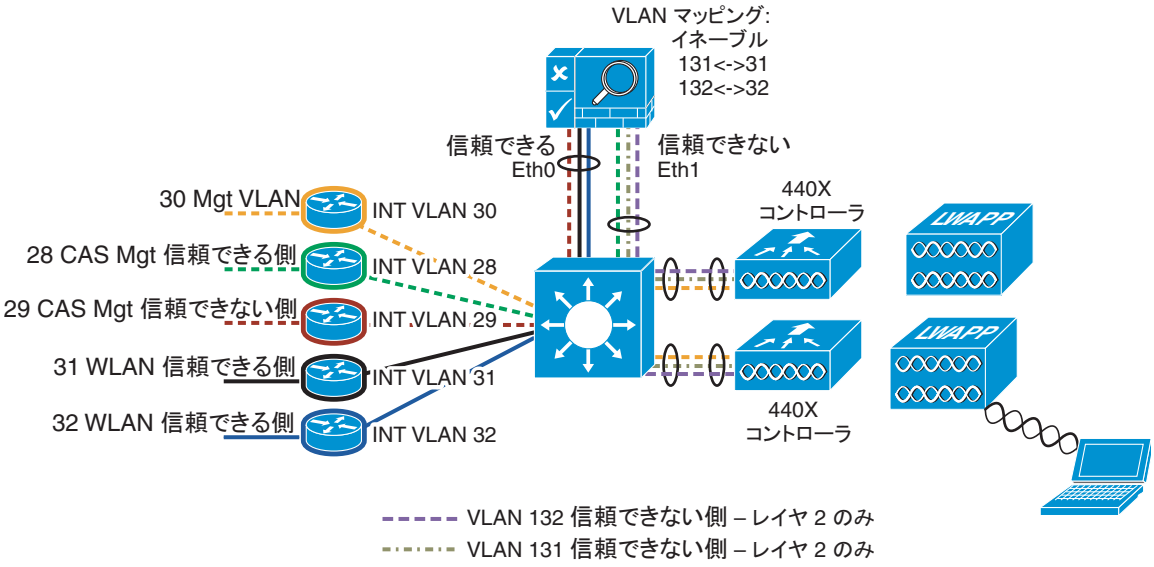
- 単一の NAC アプライアンスを冗長マルチレイヤ スイッチ トポロジの一部として展開する場合は、NAC アプライアンス間の接続に関するガイドラインを除いて、上のすべての展開ガイドラインが有効になります。このアプローチはトポロジ内のシングル ポイント障害の原因となるため、特にお勧めしません。ただし、将来にハイ アベイラビリティを実装する目的で、既存の Unified Wireless 展開に NAC のサービスを導入しようとする場合は有効です。
- 単一の NAC アプライアンスを単一のマルチレイヤ スイッチと組み合せて展開する場合は、次の項目を除くすべての展開ガイドラインが有効です。

– スイッチ間のガイドライン（P.5-29 の「スイッチ間の接続」を参照）。
– NAC 間のガイドライン（P.5-29 の「NAC アプライアンス間の接続」を参照）。

管理 VLAN およびエンド ユーザ VLAN（バーチャル ゲートウェイ モード）に関連付けられているすべての SVI は、HSRP が実装されない状態で設定されます。

図 5-24 に、単一の NAC およびマルチレイヤ スイッチによるトポロジの例を示します。

図 5-24　冗長性のない NAC 実装：バーチャル ゲートウェイ



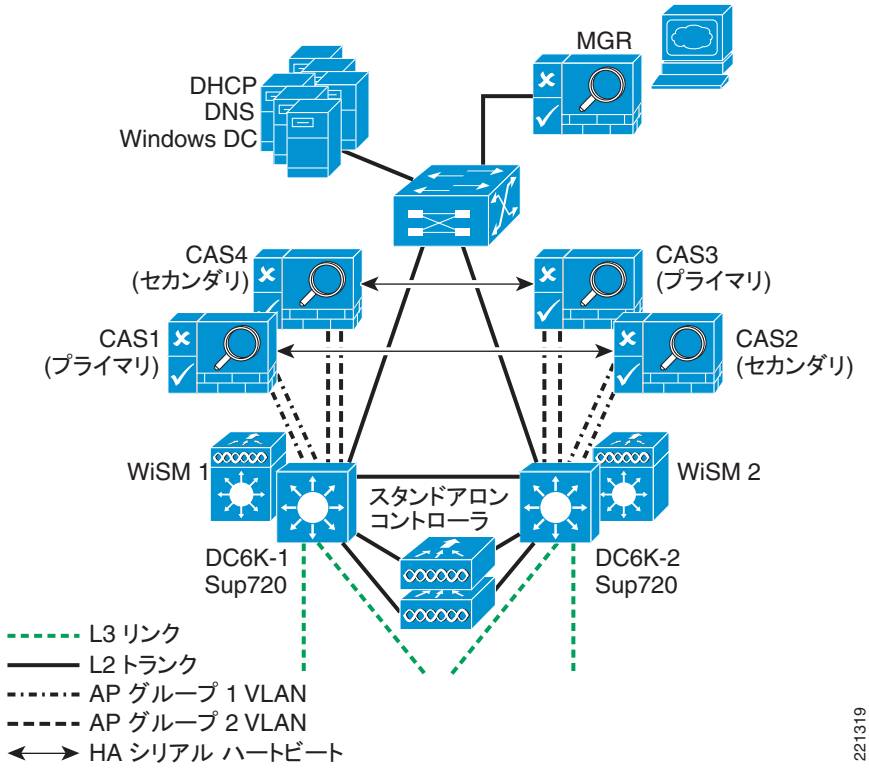
CAM ハイ アベイラビリティの実装

CAM をハイ アベイラビリティ構成に実装する方法については、このデザイン ガイドの対象外です。詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 16 章を参照してください。このマニュアルは、http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html で入手できます。

スケーリングに関する考慮事項

シスコの指定ハードウェア（HP DL350 または同等品）を使用した展開を前提とする場合、単一の NAC アプライアンスによって、現時点では最大 2,500 人の同時ユーザをサポートできます。企業の同時使用ユーザが 2,500 人を超える可能性がある場合や、パフォーマンス上の理由から管理者が複数の NAC アプライアンスにユーザを分散する場合は、追加の NAC アプライアンスをスイッチ基盤に配置して、既存の展開で利用します。図 5-25 に、完全な冗長性を備えた複数 NAC 展開によるトポロジの概略的な例を示します。

図 5-25　Unified Wireless 展開での NAC アプライアンスのスケーリング



このデザイン ガイドで説明されている推奨事項に基づいた展開を前提とすると、無線ユーザを 2 つ以上のアクティブな NAC アプライアンスにわたって分散する場合、最も有効な方法は、複数の動的インターフェイスを WLC AP グループ化機能と組み合せて使用することです（P.5-22 の「NAC アプライアンスと AP グループを使用したローミング」を参照）。この方法では、単一の WLAN を企業の展開全体にわたって実装すると同時に、802.1q トランクを通じて、ユーザのトラフィックを（AP グループまたは VLAN の関係に基づいて）特定の NAC アプライアンスに分散することができます。この技術は、動作モードがバーチャル ゲートウェイと Real-IP ゲートウェイのどちらの場合でも適用できます。

AP グループの関係を定義するときは、クライアントがローミングした場合に、2 つの WLC の間で AP グループ境界を越える状態とならないように注意してください（P.5-22 の「NAC アプライアンスと AP グループを使用したローミング」を参照）。

有線 / 無線統合型 NAC アプライアンスの展開

シスコの WLAN コントローラと Catalyst スイッチではアーキテクチャが異なるため、有線と無線の統合展開をサポートするには、NAC アプライアンスをそれぞれ別に実装する必要があります。ただし、単一の CAM または HA CAM ペアを使用することで、両方のネットワークの NAC アプライアンスを管理できます。

Voice over WLAN 展開での NAC アプライアンス

このデザイン ガイドでは、NAC アプライアンスがすべてのユーザ トラフィックに対して「インライン」で介在しているため、Voice over WLAN（VoWLAN）アプリケーションのサポートに使用される WLAN は、NAC アプライアンス経由でスイッチされないようにする必要があります。理由は次のとおりです。

- NAC アプライアンスは、VoWLAN トラフィックを、遅延の影響を受けにくい他のトラフィックよりも（QoS を利用して）優先的に処理することができません。
- NAC アプライアンスが Real-IP ゲートウェイとして設定されている場合は、マルチキャストベースの IP テレフォニー アプリケーションをサポートできません。
- 現在の VoWLAN 端末のほとんどは、何らかの形でアクセス制御に EAP 認証を使用しています。したがって、NAC が提供する認証サービスおよびアクセス制御サービスを必要としません。また、ほとんどの場合、VoWLAN デバイスは、エンドポイント セキュリティを必要とするその他の無線コンピューティング デバイスと同一の脅威にさらされることがありません。

このため、VoWLAN アプリケーション専用の個別 WLAN および VLAN を展開すること、および所定の VoWLAN に関連付けられている VLAN が NAC アプライアンス経由でトランキングされないようにすることをお勧めします。

マルチレイヤ スイッチ基盤に関する考慮事項

この項では、Cisco Unified Wireless ソリューションへの Cisco NAC アプライアンスの実装に関係する、詳細な実装について説明します。ここでは、ソリューションの個々の項目を設定する手順については示しません。この項の内容は、この章で以前に説明した情報に加えて、Cisco Clean Access NAC アプライアンス ソリューションおよび Cisco Unified Wireless ソリューションについての深い知識を持つ読者を対象としています。

次の設定ガイドラインは、図 5-18 および図 5-19 に示したハイ アベイラビリティ NAC/Unified Wireless トポロジに基づいています。ハイ アベイラビリティ トポロジの例が使用されている理由は、推奨する展開シナリオであるためです。「Unified Wireless 展開で使用するゲートウェイ方式」に示した注意事項が存在するため、アプライアンスを Real-IP ゲートウェイとして展開する代わりに、バーチャル ゲートウェイ方式を使用することを強くお勧めします。単一の NAC アプライアンスを展開する場合も、特に言及した場合を除いて、基本的にすべての面で同一です。

設定例およびスクリーンショットは、Cisco Unified Wireless WLAN コントローラのバージョン 5.0.148.2 ファームウェア イメージおよび Cisco NAC アプライアンス / マネージャのバージョン 4.1.3.1 ソフトウェアに基づいています。以降の設定の項は、レイヤ 1 およびレイヤ 2 のデバイス相互接続からレイヤ 3 デバイスの設定まで、論理上の進行に基づいて構成されています。

図 5-26 に、マルチレイヤ スイッチ ブロックの例を示します。

図 5-26　マルチレイヤ スイッチ ブロック

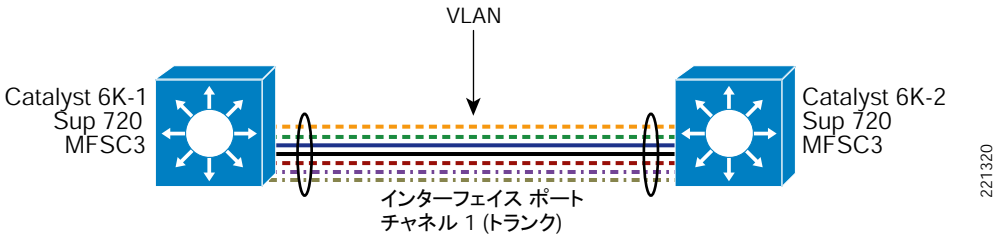


図 5-26 の冗長スイッチ ブロックは、ファイバおよび銅線のギガビット ポート モジュールに加えて Sup720/MSFC3 モジュールを搭載した 2 台の Catalyst 6500 で構成されています。

次の点に注意してください。

- 銅線 GigE モジュールは、NAC アプライアンス サーバへの接続をサポートするために使用されます。
- ファイバ GigE モジュールは、スタンドアロン コントローラの接続に使用されます。Cisco Wireless Services Module（WiSM）のみが展開されている場合、ファイバ モジュールはオプションです。
- ファイバまたは銅線 GigE モジュールのどちらもスイッチ間トランクに使用できます。

スイッチ間トランクの設定

P.5-29 の「スイッチ間の接続」で説明したように、スイッチ間のトランクは、ポート チャネルとしてまとめた 2 つ以上の物理リンクで構成することを強くお勧めします。また、これらのリンクは、各スイッチで複数のインターフェイス モジュールを使用して確立することをお勧めします。これにより、ポート モジュール全体で障害が発生した場合に、NAC アプライアンス間のトランクおよび従属するハートビート リンクが維持されます。

各 Catalyst 6000 上で、次のようなポート チャネル設定を定義します。

```
interface Port-channel1

 description Channel Between C6Ks

 switchport

 switchport trunk encapsulation dot1q

 switchport trunk allowed VLAN 1-156

 switchport mode trunk

 no ip address

 !

----------------------------------snip--------------------------------

!

interface GigabitEthernet5/1

 description To DC-6K-2
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 1-156
 switchport mode trunk
 no ip address
 channel-group 1 mode desirable
!
interface GigabitEthernet6/2
 description to DC-6K-2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 1-156
 no ip address
 channel-group 1 mode desirable
```

上の例では、ポート チャネルが 2 つの別個のモジュール上の 2 つのポートで構成されていることに注意してください。トランク上で VLAN を制限する場合は、NAC の展開に関係する VLAN をすべて許可する必要があります。次の VLAN を含みますが、これらに限定されません。

- WLC 管理 VLAN
- WLC AP 管理 VLAN（複数の場合あり）
- NAC の Trusted インターフェイスの管理 VLAN
- NAC の Untrusted インターフェイスの管理 VLAN
- 1 つまたはそれ以上の NAC の信頼できない側のクライアント VLAN
- 1 つまたはそれ以上の NAC の信頼できる側のクライアント VLAN（バーチャル ゲートウェイ モードのみ）

（注）　上のポート チャネル設定は、アプライアンスを 1 つだけ展開する場合は必要ありません。ただし、アプライアンスが既存の冗長スイッチ ブロックの一部として設定されている場合は必要です。

VLAN の設定

上のリストに示した VLAN は、各 Catalyst 6000 上で設定する必要があります。WLC 管理 VLAN および AP マネージャ VLAN は、既存の Unified Wireless 展開の一部としてすでに設定されている場合もあります。

次に、VLAN の設定例を示します。

```
VLAN 9
```

```
 name ap-mgt !This supports AP-to-WLC LWAPP Tunnels!
!
VLAN 28
 name cas-mgt-untrust
!
VLAN 29
 name CAS-mgt-trusted
!
VLAN 30
 name DC-Mgt !This is the datacenter wide mgt VLAN - includes WLCs!
!
VLAN 31
 name client-VLAN1 !WLAN1 Client VLAN on trusted side of NAC!
!
VLAN 32
 name client-VLAN2 !WLAN2 Client VLAN on trusted side of NAC!
!
VLAN 131
 name WLAN1-CAS-Untrust !This VLAN exists between WLC's and NAC Untrusted i/f!
!
VLAN 132
 name WLAN2-CAS-Untrust !This VLAN exists between WLC's and NAC untrusted i/f!
!
```

上の VLAN 31 および 32 は、NAC アプライアンスが VLAN マッピングを使用してバーチャル ゲートウェイとして設定されている場合、それぞれ VLAN 131 および 132 にマップされる信頼できる側の VLAN を表します。

SVI の設定

展開の前に、各 Catalyst 6000 上のスイッチ仮想インターフェイス（SVI）の設定で必要となるサブネットおよびアドレス方式について、ネットワーク管理者が確認済みであることを前提とします（図 5-27 を参照）。

図 5-27　スイッチ ブロック：SVI

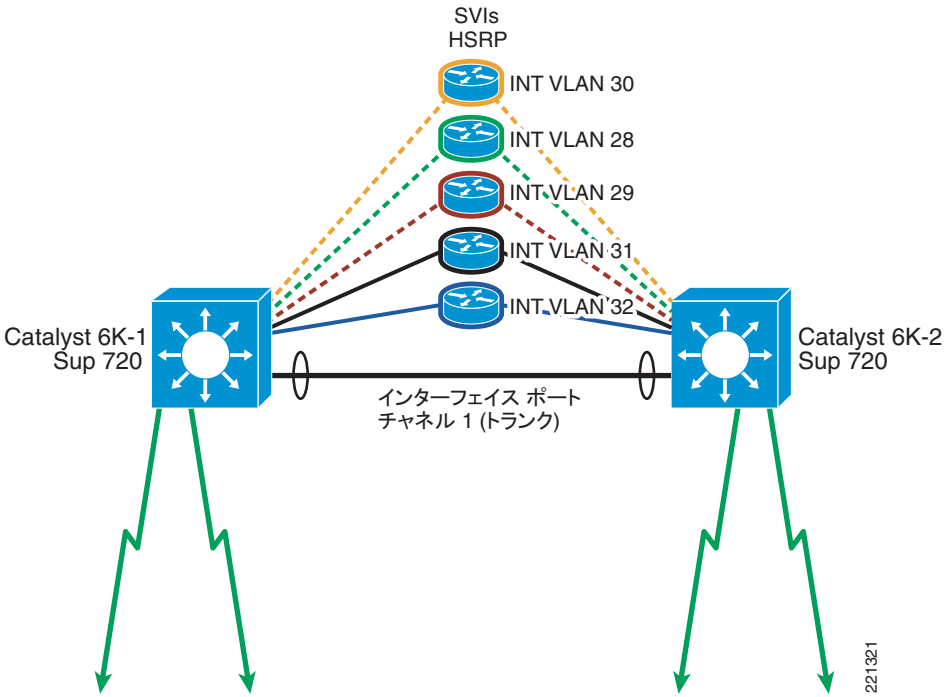


図 5-27 は、キャンパス展開に実際に存在する可能性がある SVI の一部のみを表しています。これらの SVI は、ハイ アベイラビリティ（HA）NAC 展開のサポートに必要となるものの例です。

（注）　図 5-27 には、AP マネージャの SVI は示していません。

ここでは、次の項目に関する SVI の設定例を示します。

- AP 管理 VLAN 9
- データ センター管理 VLAN 30
- NAC の信頼できる管理 VLAN 29
- NAC の信頼できない管理 VLAN 28
- WLAN1 クライアントの信頼できる VLAN 31（バーチャル ゲートウェイ モードのみ）
- WLAN2 クライアントの信頼できる VLAN 32（バーチャル ゲートウェイ モードのみ）

```
interface VLAN9

 description Datacenter Controller AP Management VLAN

 ip address 10.15.9.2 255.255.255.0
```

```
 standby 121 ip 10.15.9.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN28
 description CAS-MGT-Untrust
 ip address 10.20.28.253 255.255.255.0
 standby 121 ip 10.20.28.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN29
 description CAS-MGT-Trust
 ip address 10.20.29.253 255.255.255.0
 standby 121 ip 10.20.29.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN30
 description DC Management Subnet
 ip address 10.20.30.4 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.30.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN31
 description WLAN1 Client Subnet
```

```
 ip address 10.20.31.2 255.255.255.0
 standby 121 ip 10.20.31.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
!
interface VLAN32
 description WLAN2 Client Subnet
 ip address 10.20.32.2 255.255.255.0
 standby 121 ip 10.20.32.1
 standby 121 timers msec 250 msec 750
 standby 121 priority 105
 standby 121 preempt delay minimum 180
```

次に、Cat6K-2 での相互補完的な設定を示します。

```
interface VLAN9
 description Datacenter Controller AP Management VLAN
 ip address 10.15.9.3 255.255.255.0
 standby 121 ip 10.15.9.1
 standby 121 timers msec 250 msec 750
!
interface VLAN28
 description CAS-MGT-Untrust
 ip address 10.20.28.254 255.255.255.0
 standby 121 ip 10.20.28.1
 standby 121 timers msec 250 msec 750
!
interface VLAN29
 description CAS-MGT-Trust
 ip address 10.20.29.254 255.255.255.0
 standby 121 ip 10.20.29.1
 standby 121 timers msec 250 msec 750
!
```

```
interface VLAN30
 description DC Management Subnet
 ip address 10.20.30.5 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.30.1
 standby 121 timers msec 250 msec 750
!
interface VLAN31
 description WLAN1 Client VLAN
 ip address 10.20.31.3 255.255.255.0
 standby 121 ip 10.20.31.1
 standby 121 timers msec 250 msec 750
!
interface VLAN32
 description WLAN2 Client VLAN
 ip address 10.20.32.3 255.255.255.0
 standby 121 ip 10.20.32.1
 standby 121 timers msec 250 msec 750
```

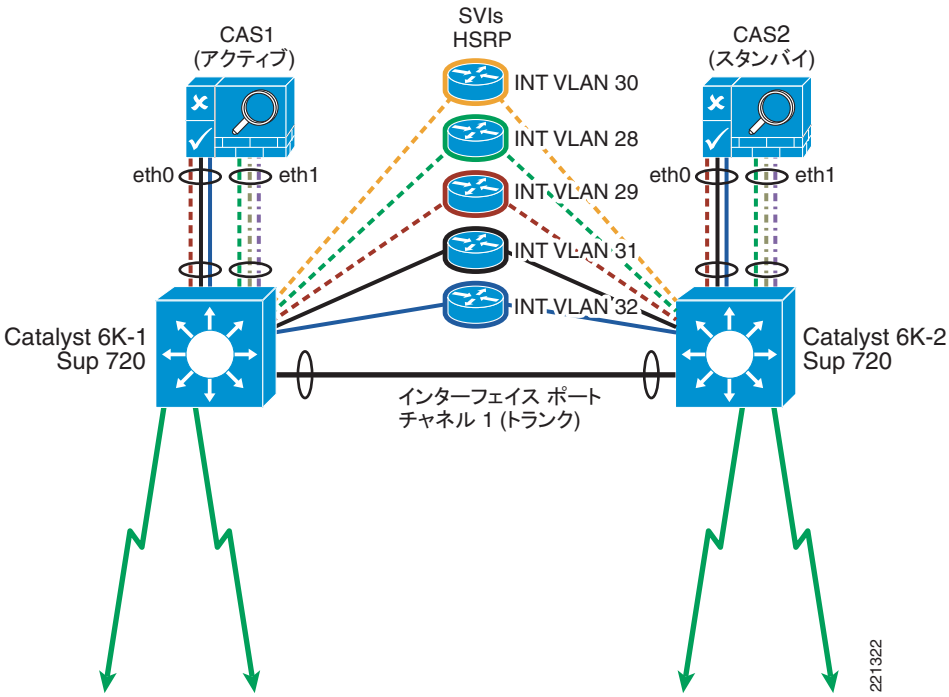
（注） 信頼できないクライアント VLAN（131 および 132）については、SVI は作成されません。

（注） NAC アプライアンス展開に冗長性がない場合も、スイッチ ブロックが冗長構成である場合は HSRP が必要です。一方、スイッチ ブロックに冗長性がない場合、HSRP 設定パラメータは必要ありません。

NAC アプライアンスの設定に関する考慮事項

NAC アプライアンスをハイ アベイラビリティ（HA）ペアとして展開する場合は、設定が完了するまで、Untrusted インターフェイスをネットワークに接続しないことを強くお勧めします（図 5-28 を参照）。これは、設定プロセスの実行中、トポロジでのループの形成を防止するためです。

図 5-28　NAC アプライアンスの HA ペア



NAC アプライアンスの初期設定

初期設定のガイドラインについては、『*Cisco NAC Appliance—Clean Access Server Installation and Administration Guide*』の第 4 章を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

特に重要となるのは、NAC アプライアンス設定スクリプト ユーティリティです。案内される手順に従って、各アプライアンスの Trusted インターフェイスおよび Untrusted インターフェイスを設定します。次の点に注意してください。

- 各アプライアンスの Trusted インターフェイス Eth0 に使用される管理 IP アドレスは、NAC アプライアンス マネージャ（CAM）の IP アドレスとは別のサブネット上に配置する必要があります。
- NAC アプライアンスを HA 構成で展開する場合は、Untrusted インターフェイス Eth1 の管理 IP アドレスを（別のサブネット上に）設定する必要があります。展開する NAC アプライアンスが 1 つのみの場合は、Eth1 の IP アドレスを Eth0 と同一にできます。

- いずれかの管理インターフェイスが特定の VLAN ID に関連付けられている場合は、（設定スクリプト プロセスの実行中、プロンプトが表示されたときに）管理 VLAN タギングを有効にし、設定スクリプト プロセスで VLAN ID を設定する必要があります。このように設定しない場合、Web インターフェイスまたは CAM を使用してアプライアンスにアクセスできなくなります。
- NAC アプライアンスを HA 構成で展開する場合は、HA ペアを単一の論理アプライアンスとして表現するためのサービス アドレス（バーチャル IP）を設定します。ネットワーク管理者は、展開のアドレスを計画する段階で、NAC アプライアンス間の Trusted インターフェイス ペア用に 3 つの IP アドレスが必要であることに注意してください。Untrusted インターフェイス ペアについても 3 つの IP アドレスが必要です。サービス IP は、アプライアンスがネットワークに接続された後に設定します。
- CAM と NAC アプライアンスの間では、共有秘密を使用して通信が保護されます。共有秘密は、完全に同一のものを設定する必要があります。一致しない場合は、CAM がアプライアンスと通信できません。
- 信頼できる IP アドレス（Eth0）または Eth0 のホスト名に基づいて、一時的な証明書を作成する必要があります。この証明書は、後で HA ペアのサービス IP アドレスまたはホスト名を表すものに変更します。

NAC アプライアンスのスイッチ接続

初期設定が完了した後は、アプライアンスをスイッチ ブロックに接続できます。NAC アプライアンスの設定がすべて完了するまでは、Eth0（Trusted インターフェイス）のみを接続してください。
アプライアンスを接続するスイッチ ポートは、トランク ポートとして設定する必要があります。次に、アプライアンスの Eth0 インターフェイスおよび Eth1 インターフェイスに使用するスイッチ ポートの設定例を示します。どちらのスイッチにも適用されます。

```
interface FastEthernet1/1
 description CAS-Trusted
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native VLAN 999
 switchport trunk allowed VLAN 29,31,32
 switchport mode trunk
 no ip address
!
interface FastEthernet1/2
 description CAS-Untrusted
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native VLAN 998
```

```
switchport trunk allowed VLAN 28,131,132

switchport mode trunk

no ip address
```

上の設定で、各トランクは NAC 展開のサポートに必要となる VLAN のみを許可するように設定されています。FastEthernet 1/1 は、NAC アプライアンスの Trusted インターフェイス（管理 VLAN を含む）と 2 つの信頼できる側のクライアント VLAN をサポートします（P.5-36 の「VLAN の設定」を参照）。FastEthernet 1/2 は、NAC アプライアンスの信頼できない管理 VLAN とともに、2 つの信頼できない側のクライアント VLAN をサポートします。

（注） 上の例は FastEthernet インターフェイスですが、実際の NAC アプライアンス展開では、ギガビット イーサネット インターフェイスになります。

NAC アプライアンスの HA サーバの設定

アプライアンスが接続された後は、Web ブラウザを開いて各サーバの Web 管理インターフェイスに直接接続することにより、HA 展開のサポートに必要となる高度なオプションを設定できます。Trusted 管理インターフェイスへの論理接続が存在することが前提です。

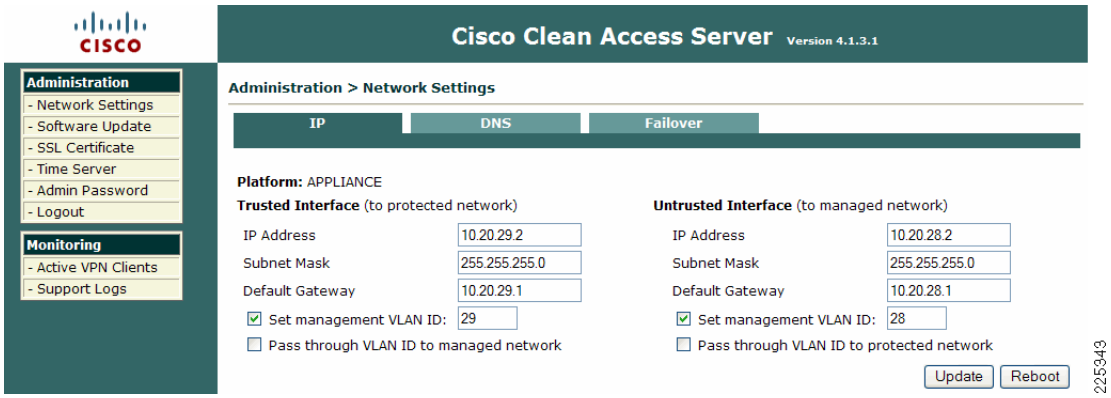
（注） 単一アプライアンス展開の場合、次の手順は必要ありません。

ステップ 1 Web ブラウザを開いて、Trusted インターフェイスの管理 IP またはホスト名を次のように入力し、アプライアンスに接続します。

```
https://<trusted mgt IP>/admin/
```

図 5-29 に示した Network Settings 画面が表示され、アプライアンスのインターフェイス設定の概要が示されます。

図 5-29　NAC アプライアンスのネットワーク設定

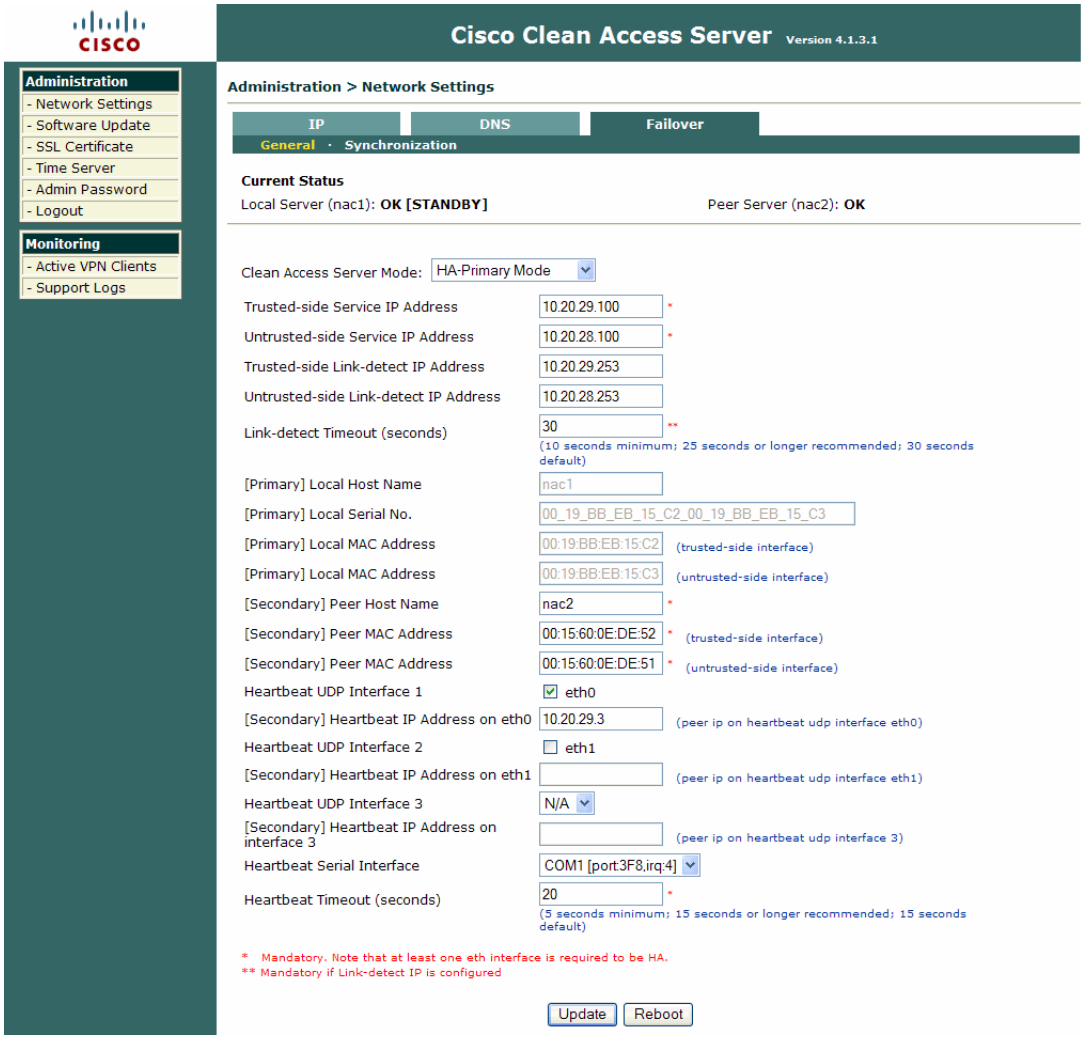


ステップ 2 **Failover** タブをクリックして、アプライアンスの HA 設定に移動します。アプライアンスは、当初はスタンドアロン モードで起動します。

ステップ 3 **HA Primary Mode** を選択し、**Update** をクリックして、**Reboot** をクリックします。

ステップ 4 アプライアンスがリブートした後、再度接続して **Failover** タブに移動すると、HA のコンフィギュレーション設定が表示されます（図 5-30 を参照）。

図 5-30　NAC アプライアンスの HA：プライマリのコンフィギュレーション設定



ステップ 5上の手順を繰り返して、もう一方の NAC アプライアンスを HA セカンダリ モードに設定します。図 5-30 は、NAC アプライアンス間で HA フェールオーバーを有効にするための設定パラメータのリストを示しています。次に、HA を設定する場合のパラメータおよび考慮事項について、概要を示します。

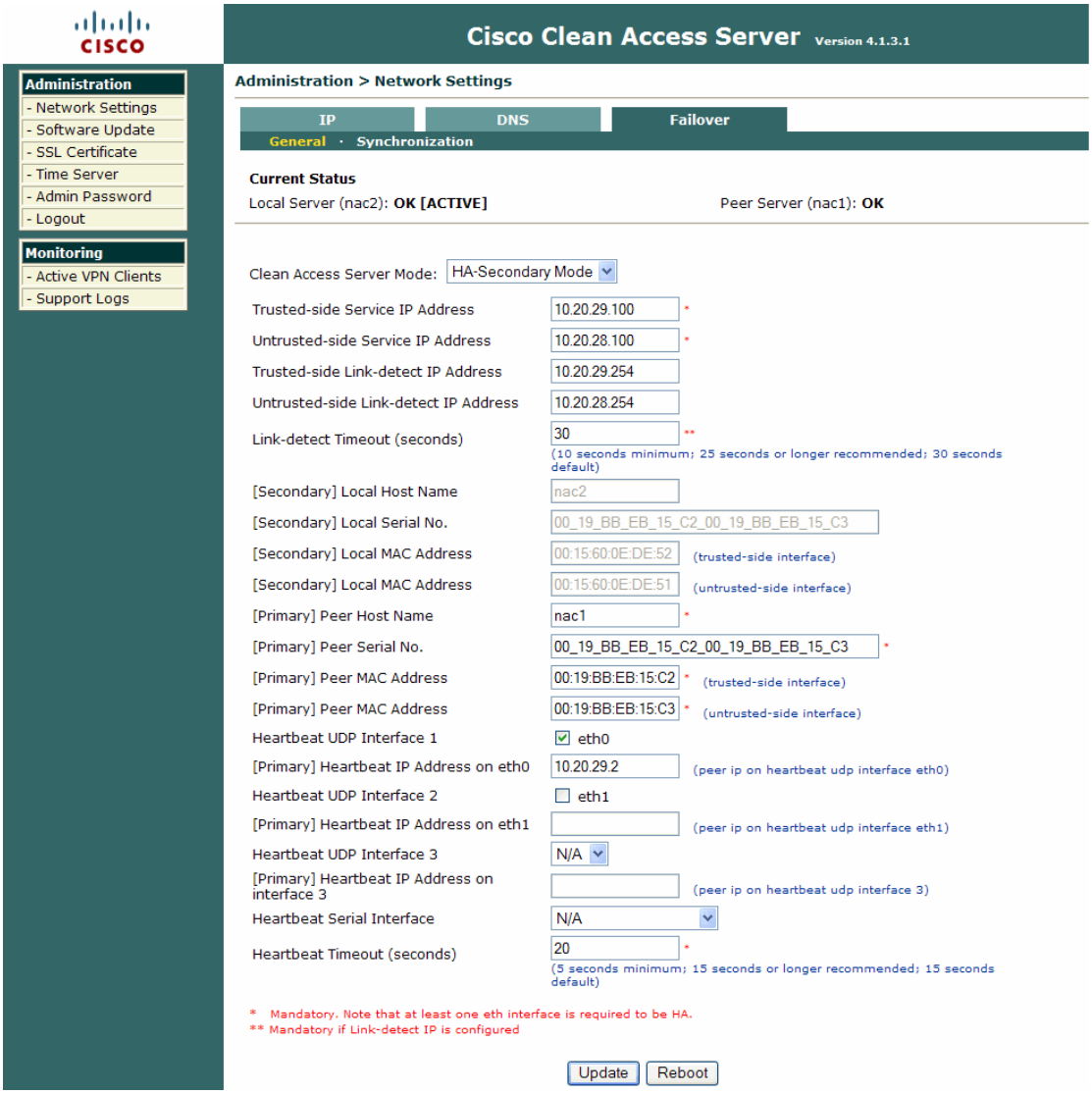
- Server Mode：1 つのサーバを HA プライマリ モードに設定し、もう一方を HA セカンダリ モードに設定します。
- Trusted-side Service IP Address：HA モードで動作する場合に、論理 NAC ペアを表すバーチャル IP アドレス。これは、HSRP 設定のスタンバイ IP と類似しています。
- Untrusted-side Service IP Address：アプライアンスの信頼できない側の論理 NAC ペアを表すバーチャル IP アドレス。
- Trusted-side Link-detect IP Address：信頼できるポートのリンク ステータスを確認するために、アプライアンスで ping の実行対象となる IP アドレス。使用する IP アドレスは、信頼できる管理サブネットの HSRP スタンバイ IP アドレスにする必要があります。P.5-38 の「SVI の設定」のインターフェイス VLAN 29 の設定を参照してください。

- Untrusted-side Link-detect IP Address：信頼できないポートのリンク ステータスを確認するために、アプライアンスで ping の実行対象となる IP アドレス。使用する IP アドレスは、信頼できない管理サブネットの HSRP スタンバイ IP アドレスにする必要があります。P.5-38 の「SVI の設定」のインターフェイス VLAN 28 の設定を参照してください。
- Link-detect Timeout
- [Primary] Local Host Name、Local Serial No.、Local MAC Address (untrusted-side interface)、および Local MAC Address (trusted-side interface)：これらのフィールドは、あらかじめ入力されています。
- [Secondary] Peer Host Name、Peer Serial Number、Peer MAC Address (untrusted-side interface)、および Peer MAC Address (trusted-side interface)：この情報は、もう一方の NAC アプライアンスの HA セカンダリ モード コンフィギュレーション設定から取得できます。
- Heartbeat UDP Interface：アプライアンスが、ピア サーバのステータスと状態の確認に使用するインターフェイス。この値は Eth0（Trusted インターフェイス）に設定することを強くお勧めします。
- [Secondary] Heartbeat IP Address：ピア アプライアンスの Trusted 管理インターフェイス（サービス IP 以外）の IP アドレス。
- Heartbeat Serial Interface：このインターフェイスは、ハートビート UDP インターフェイスとともに使用し、単独では使用しないでください。各アプライアンスの該当するシリアル インターフェイスには、クロス（ヌル）モデム ケーブルを接続します。
- Heartbeat Timeout

ステップ 6すべての設定を入力した後、**Update** をクリックし、次に **Reboot** をクリックします。

ステップ 7セカンダリ（スタンバイ）サーバとして機能する NAC アプライアンスについて、上の設定を繰り返します。セカンダリの NAC アプライアンスで使用される相互補完的な HA 設定の例については、図 5-31 を参照してください。

図 5-31　　NAC アプライアンスの HA セカンダリの設定



HA 展開での自己署名証明書

NAC アプライアンスを初めて設定するときは、一時的な自己署名証明書を作成するかどうかについて、インストール スクリプトで確認を求められます。作成する場合、通常は、Trusted インターフェイス Eth0 の IP アドレスまたはホスト名を使用して証明書が作成されます。この自己署名証明書は、認証およびポスチャ評価のために NAC アプライアンスへの HTTP リダイレクトを実行するとき、および Clean Access デスクトップ エージェントが認証およびポリシー評価のためにアプライアンスに接続するときに、エンド ユーザとの SSL セッションを確立するために使用されます。インポートした証明書をアプライアンス（複数可）にインストールすることもできます。

HA 展開のために NAC アプライアンスのペアを設定する場合は、アプライアンス ペアのサービス IP アドレスを反映するために、一時的証明書の再生成が必要になることがあります。また、ホスト名を使用している場合は、サービス IP アドレスを反映するために、DNS の更新が必要になることがあります。

証明書で IP アドレスが使用されている場合は、NAC アプライアンスの Web 管理 GUI の左側のメニュー バーにある SSL Certificate を選択することで、サービス IP に基づいて新しい一時的証明書を生成できます（図 5-32 を参照）。

もう一方のアプライアンスについて、このプロセスを繰り返します。同一のホスト名またはサービス IP アドレスを使用する必要があります。

図 5-32　一時的な SSL 証明書の生成

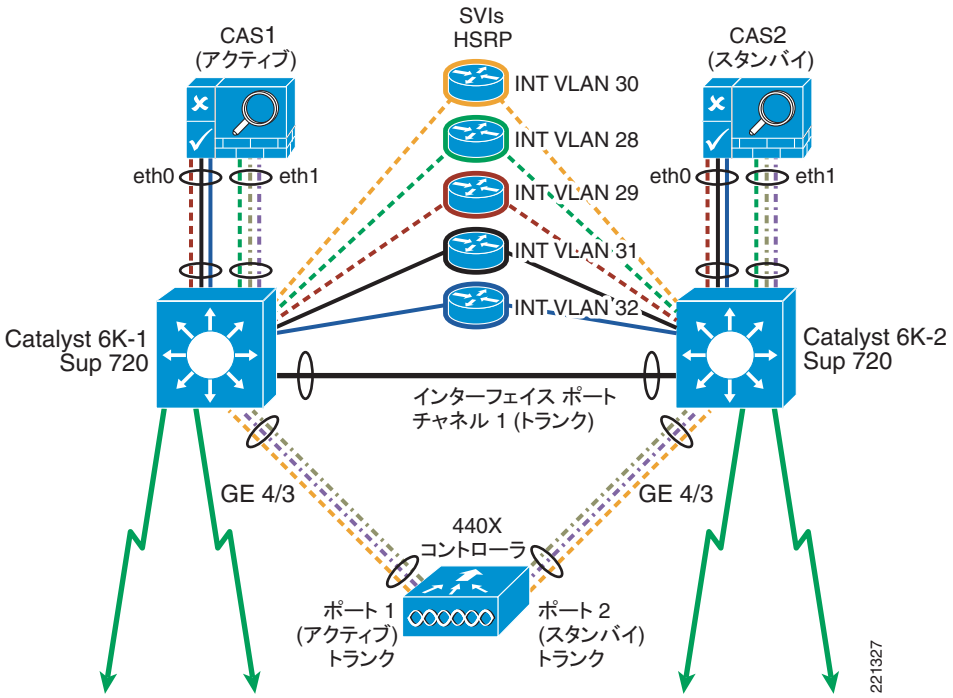
図 5-32 の SSL 証明書のドメインは、図 5-30 の HA 設定に含まれている信頼できる側のサービス IP アドレスであることに注意してください。

NAC アプライアンスを使用するスタンドアロン WLAN コントローラの展開

Cisco 4400 シリーズ WLAN コントローラの詳細な設定ガイドラインについては、http://www.cisco.com/en/US/partner/products/ps6366/products_configuration_guide_book09186a00806b0077.html のマニュアルを参照してください。

スタンドアロンの WLC をスイッチ ブロックに展開する場合は、2 つのオプションがあります（図 5-33 を参照）。

図 5-33　スタンドアロン WLC/ スイッチ ブロック



Cisco 4402 シリーズの WLC はギガビット イーサネット ポートを 2 つ搭載し、4404 シリーズの WLC は 4 つのギガビット イーサネット ポートを搭載しています。使用可能なオプションは、次のとおりです。

- 単一のスイッチを使用したディストリビューション レイヤでは、4402/04 を設置するときに、すべてのポートを 1 台のスイッチに接続し、WLC のポートを Link Aggregation（LAG; リンク集約）モードに設定して、関連する Catalyst スイッチのポートをポート チャネルとして設定します。このオプションは、WLC/NAC のスイッチ ブロックに含まれている Catalyst スイッチが 1 台のみの場合に最適です。
- 推奨の冗長スイッチを使用したディストリビューション レイヤでは、デュアルホーム シナリオの場合、4402/04 を設置するときに、一方のポート（4404 の場合はポートのペア）を 1 台のスイッチに接続し、もう一方のポート（4404 の場合はポートのペア）を他のスイッチ ブロックに接続します。この方法を選択する場合は、WLC 上に設定される管理インターフェイスおよび動的インターフェイスについて、プライマリおよびバックアップのポートを指定できます。

図 5-33 に示したコントローラは、冗長スイッチ ブロックにデュアルホーム接続された 4402 を表しています。次に、各 Catalyst 6000 でのスイッチ ポートの設定例を示します。

```
Cat6K-1

interface GigabitEthernet4/3

 description To WLC#3 Port 1

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk
```

```
 no ip address
DC6K-2

interface GigabitEthernet4/3

 description To WLC#3 Port 2

 switchport

 switchport trunk encapsulation dot1q

 switchport mode trunk

 no ip address
```

WLC のポートおよびインターフェイスの設定

WLC の物理ポートがデュアルホーム接続されている場合、関連する管理インターフェイスおよび動的インターフェイスは、どちらのポートにマップしてもかまいません。物理ポートを両方ともアクティブにすると、動的インターフェイスをサポートすると同時に、別の動的インターフェイスまたは管理インターフェイスのバックアップ ポートとして運用できます。図 5-34 に、WLC のポートのステータスを示します。

図 5-34　　WLC のポートの概要

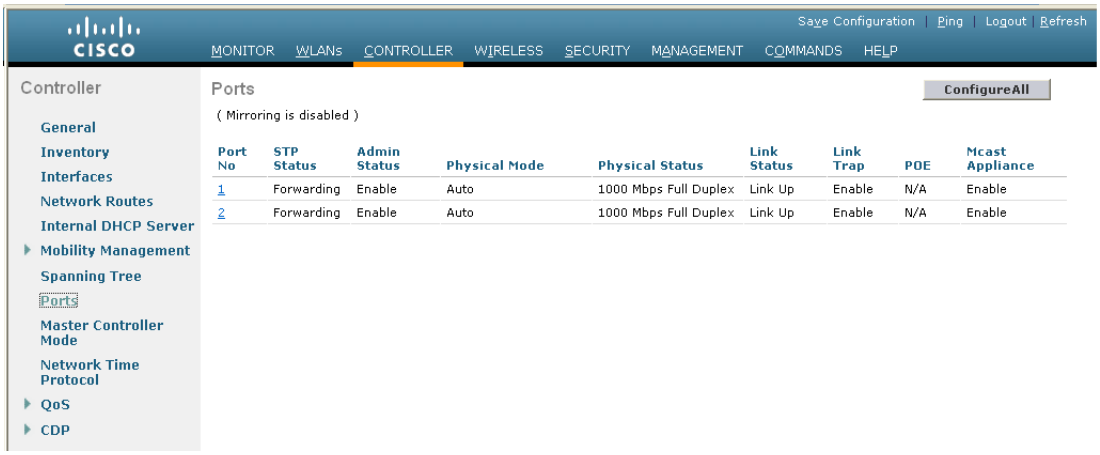


図 5-35 に、WLC 上で設定されている管理インターフェイスおよび動的インターフェイスの概要を示します。

図 5-35　　WLC のインターフェイスの概要

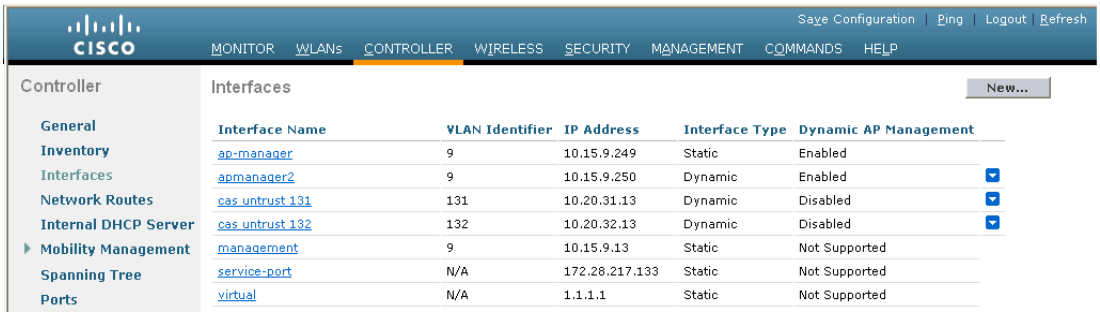


図 5-35 では、AP マネージャ インターフェイスが 2 つ存在していることに注意してください。1 つは静的、もう 1 つは動的です。静的な AP マネージャ インターフェイスは、デフォルトの AP マネージャ インターフェイスを表しています。削除することはできず、Unified Wireless ソリューションの適切な動作に不可欠です。

AP マネージャ インターフェイス

静的な AP マネージャ インターフェイスは、1 つのポートにのみ割り当てることができます。バックアップ ポートを割り当てることはできません。したがって、静的 AP マネージャ インターフェイスをサポートする WLC ポートまたは Catalyst スイッチ インターフェイスがダウンした場合、そのコントローラに接続していたすべての AP は、コントローラの優先順位設定に基づいて別のコントローラに再接続します。

この動作を回避するには、AP 管理をサポートする 2 番目の動的インターフェイスを設定して、他の物理 WLC ポートに割り当てます。WLC は、各物理ポートに AP 管理インターフェイスが割り当てられた状態になります。1 つのポートで障害が発生した場合も、AP マネージャ インターフェイスを引き続き使用できます（図 5-36 および図 5-37 を参照）。

図 5-36　　静的 AP マネージャ インターフェイスの設定

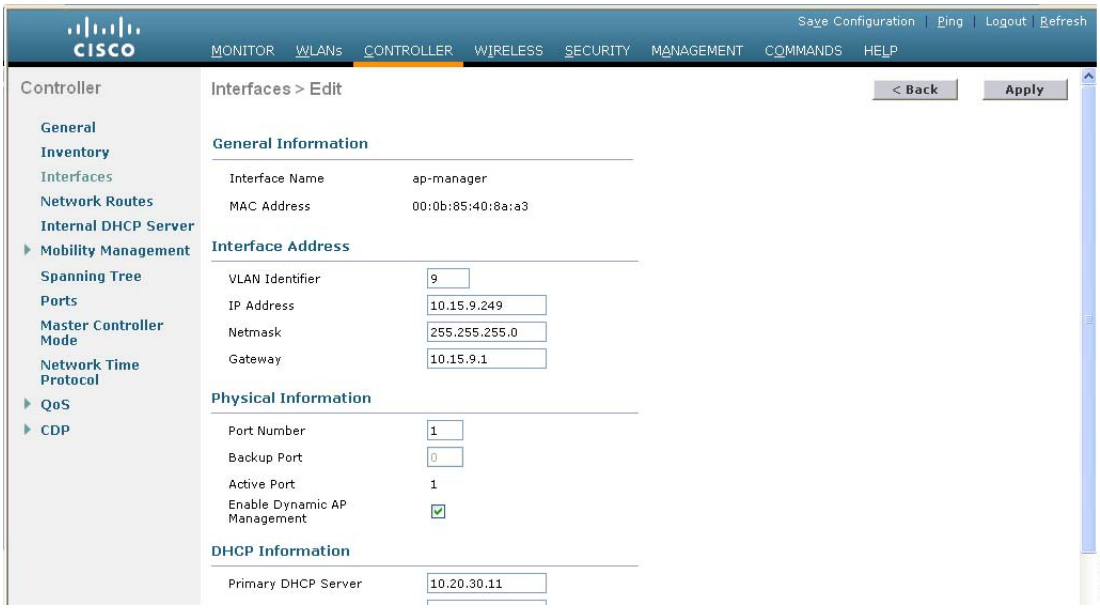
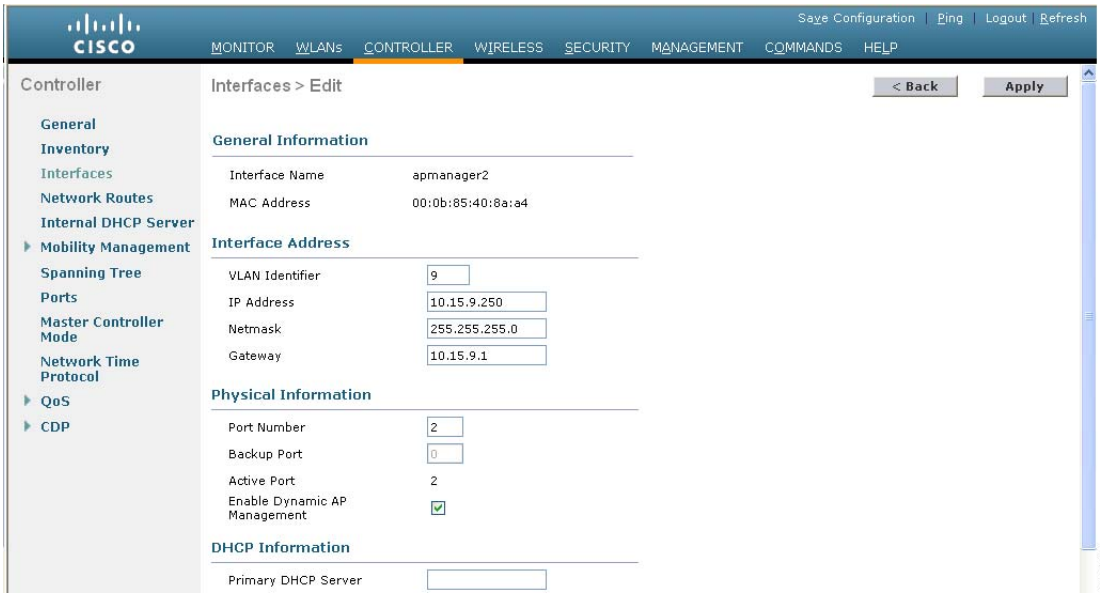


図 5-37　　動的 AP マネージャ インターフェイスの設定



WLAN クライアント インターフェイス

WLAN クライアントをサポートする動的インターフェイス /VLAN は、WLC 上のいずれかの物理ポートに割り当てることができます。また、これらのインターフェイスにバックアップ ポートを割り当てることもできます。

図 5-35 では、次の 2 つの WLAN クライアント インターフェイスが設定されています。

- cas untrust 131
- cas untrust 132

図 5-38 および図 5-39 に、それぞれの動的インターフェイスの設定例を示します。

図 5-38　「cas untrust 131」動的インターフェイスの設定

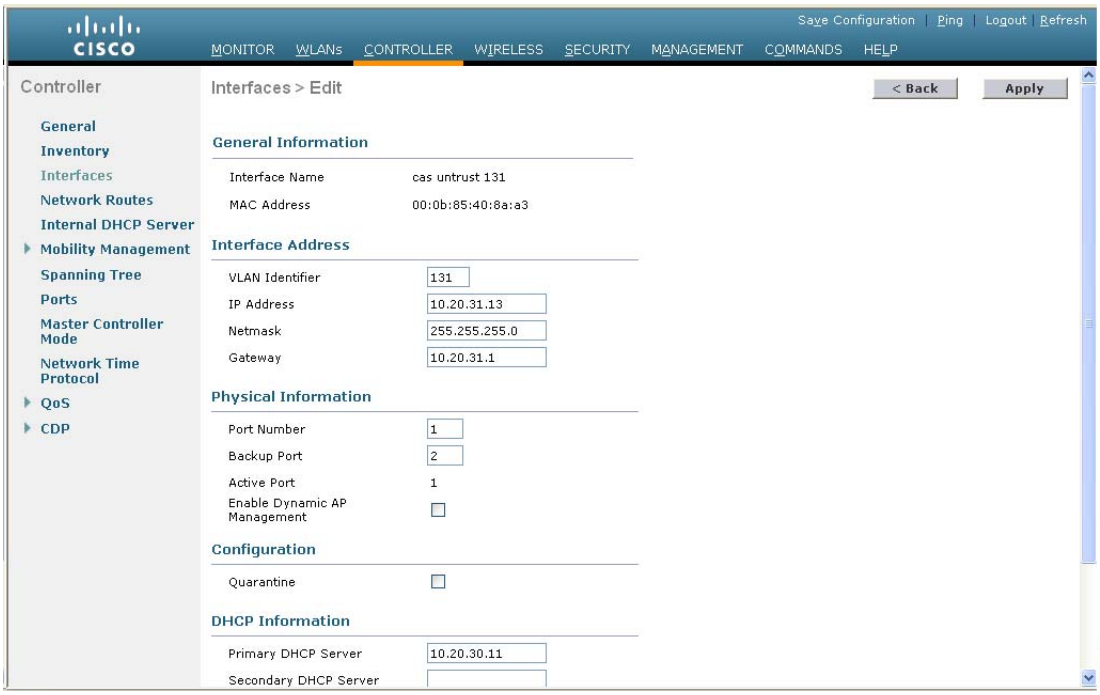


図 5-39　「cas untrust 132」動的インターフェイスの設定

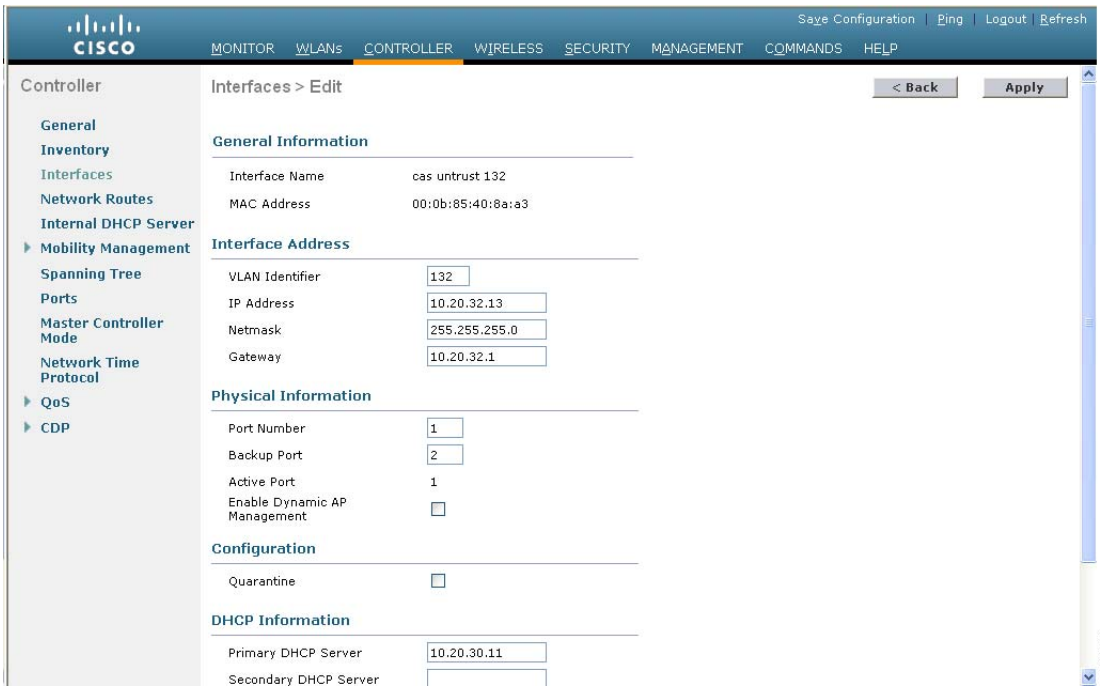


図 5-38 および図 5-39 に示した WLAN クライアント インターフェイスの設定では、次の点に注意してください。

- 各インターフェイスは、異なる物理ポートに割り当てられます。また、各インターフェイスには、もう一方の物理ポートがバックアップとして割り当てられます。
- 設定される IP アドレス、サブネット、およびゲートウェイ パラメータは、NAC アプライアンスの信頼できる側にリンクされます。具体的には、スイッチ ブロックの VLAN 31 と 32、SVI 31 と 32 です。
- クライアントの WLAN トラフィックは、VLAN 131 および 132 からスイッチされ、NAC アプライアンスの信頼できない側にトランキングされます。

信頼できない WLC インターフェイスへの WLAN のマッピング

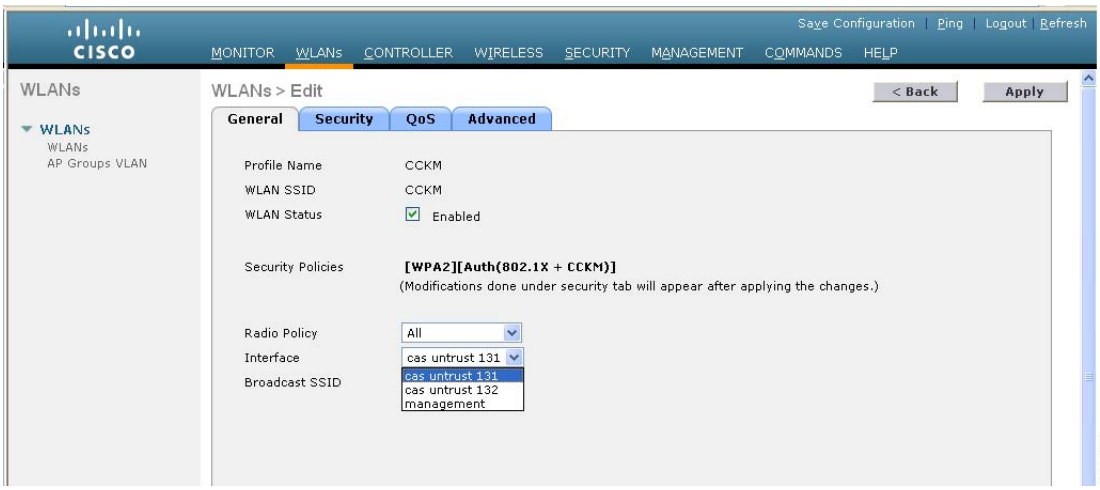
P.5-52 の「WLAN クライアント インターフェイス」に示すように、2 つの動的インターフェイスが作成され、NAC アプライアンスの Untrusted インターフェイス（Eth1）にトランキングされる VLAN に割り当てられます。インターフェイス名は次のとおりです。

- cas untrust 131
- cas untrust 132

NAC アプライアンスにトランキングされるコントローラ インターフェイスに対して（NAC のサービスを必要とする）キャンパス WLAN を割り当てるのは、簡単なプロセスです。

図 5-40 では、**cas untrust 131** という名前のインターフェイスに WLAN CCKM が割り当てられています。この WLAN の認証を受ける（または WLAN とのアソシエーションを確立する）すべてのクライアントは、認証、ポリシーまたはポスチャ評価、および修復のために、必要に応じて NAC アプライアンス経由でスイッチされます。

図 5-40　　WLAN：動的インターフェイスの割り当て



NAC アプライアンスを使用する場合の WiSM の展開

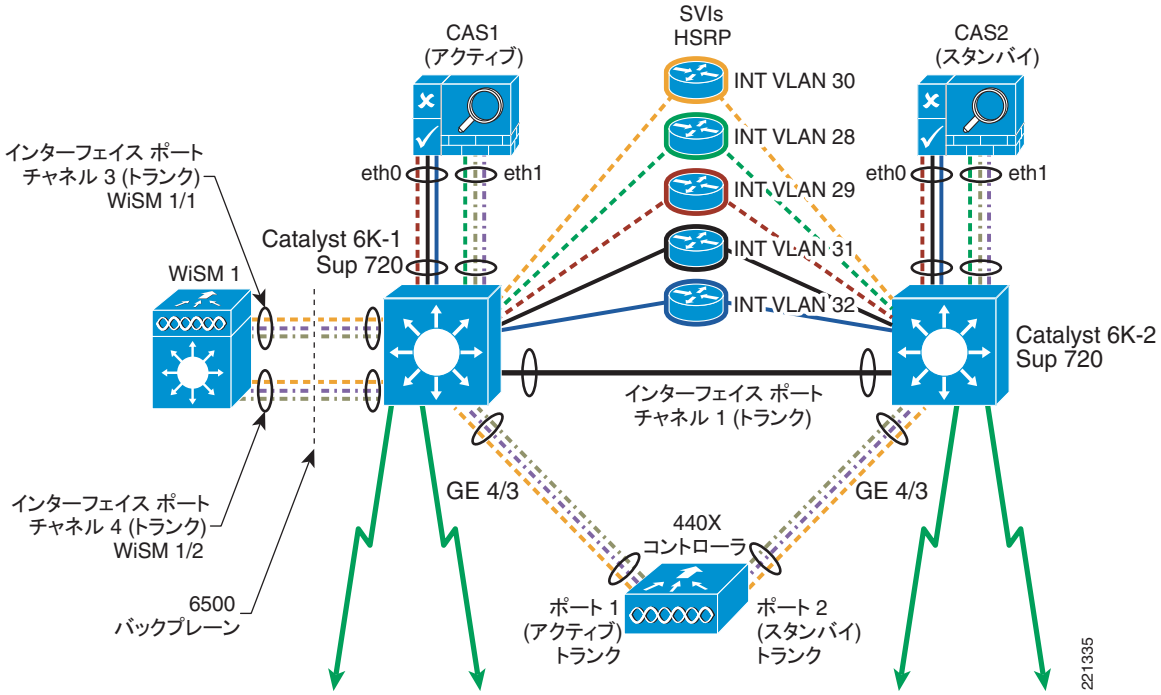
WiSM のインストールおよび設定に関する詳細なガイドラインについては、次の URL を参照してください。

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

WiSM モジュールは Catalyst 6500 に直接装着されるため、モジュールの展開に関する唯一のオプションは、モジュールの装着先となるスイッチです。このガイドで示した設計上の推奨事項に従うと、WiSM は NAC アプライアンスのレイヤ 2 隣接ノードになります。したがって、どちらの NAC アプライアンスがアクティブになっているかにかかわらず、どちらのスイッチにも配置できます（冗長スイッチは、スイッチ ブロックを形成しているものとします）。これは、スタンドアロン コントローラ実装の場合も同様です。

図 5-41　　WiSM モジュールの統合



WiSM バックプレーン スイッチの接続

WiSM モジュールは、6500 のバックプレーンに直接接続します。このモジュールは 2 つの WLAN コントローラを搭載しており、各コントローラは 4 つのギガビット イーサネットと同等のバックプレーンへの接続機能を備えています。4 つのギガビット接続が、それぞれ 1 組としてポート チャネルにグループ化されます。次の Cat6K-1 の設定例を参照してください。

```
:

interface Port-channel3
```

```
 description To WiSM 3/1 10.20.30.50
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
!
interface Port-channel4
 description To WiSM 3/2 10.20.30.52
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast

interface GigabitEthernet3/1
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 3 mode on
!
interface GigabitEthernet3/2
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
```

```
 mls qos trust dscp
 spanning-tree portfast
 channel-group 3 mode on
!
interface GigabitEthernet3/3
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 3 mode on
!
interface GigabitEthernet3/4
 description To WiSM 3/1
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 3 mode on

interface GigabitEthernet3/5
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
```

```
 channel-group 4 mode on
!
interface GigabitEthernet3/6
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
!
interface GigabitEthernet3/7
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
!
interface GigabitEthernet3/8
 description To WiSM 3/2
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust dscp
 spanning-tree portfast
 channel-group 4 mode on
```

WiSM インターフェイスの設定

WiSM は、スタンドアロンのコントローラと同様に設定し、運用します。したがって、WiSM の管理インターフェイスおよび動的インターフェイスの設定は、「WLAN クライアント インターフェイス」の項で示したスタンドアロン コントローラの設定と類似しています。異なる点は次のとおりです。

- WiSM コントローラは、セカンダリ AP マネージャ インターフェイスを必要としません。
- クライアント WLAN に割り当てられる動的インターフェイスは、バックアップ ポートをサポートしません。これは、コントローラのバックプレーン接続が LAG モードで動作するためです。

WiSM WLAN インターフェイスの割り当て

WLAN/ インターフェイスの設定は、P.5-54 の「信頼できない WLC インターフェイスへの WLAN のマッピング」で説明したものと同一です。

Clean Access Manager および NAC アプライアンスの設定ガイドライン

この項では、Cisco Unified Wireless ソリューションとの相互運用に関係する Clean Access ソリューションの設定について説明します。ポリシー、ポスチャ評価技術、および修復方法については、この項の対象外です。詳細な設定ガイドラインについては、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

以降の項では、CAM を物理的に設置して初期設定を完了し、適切なアプライアンス ライセンスをインストール済みで、NAC アプライアンスへの論理接続が存在していることを前提とします。

CAM への HA NAC ペアの追加

NAC アプライアンスを HA ペアとして設定した場合、CAM では 1 つの論理 NAC アプライアンスとして認識されます。HA ペアを初めて追加するときは、ペアの信頼できる側のサービス IP アドレスを使用して追加します。新しいアプライアンスの追加については、図 5-42 および 図 5-43 を参照してください。

図 5-42　　CAM への HA サーバ ペアの追加

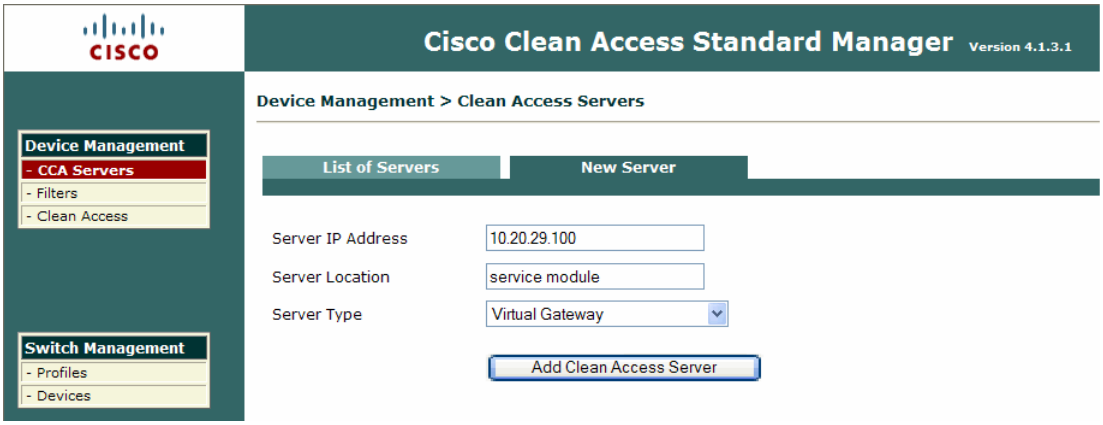


図 5-43 では、Server Type がバーチャル ゲートウェイに設定されていることに注意してください。

図 5-43　　サーバの追加の完了

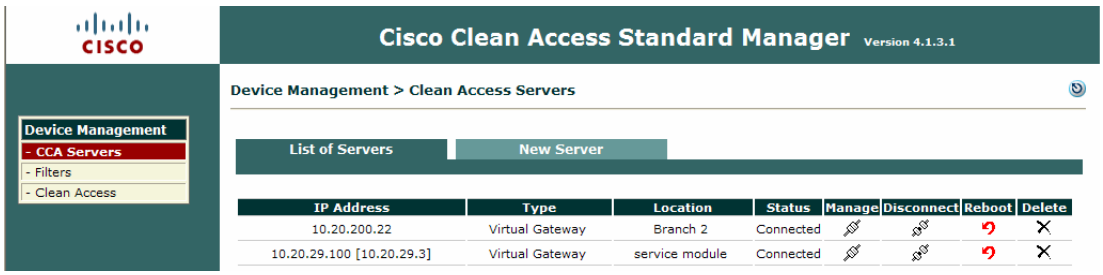


図 5-43 の IP Address フィールドに注目してください。2 つの IP アドレスが表示されています。最初のアドレスは、アプライアンス ペアのサービス IP アドレスです。2 番目のアドレス（角カッコで囲まれているもの）は、アクティブになっている実際のアプライアンスを表します。HA ペアを追加できない場合は、次の作業を行います。

- CAM と NAC アプライアンス インターフェイス間の接続を確認する。サービス IP アドレスに加えて、Trusted 管理インターフェイスのアドレスに対しても ping が成功することを確認します。
- 有効なアプライアンス ライセンス（複数の場合あり）を CAM に確実にインストールする。
- P.5-44 の「NAC アプライアンスの HA サーバの設定」の説明に従って、アプライアンスの Web 管理インターフェイスを使用して各アプライアンスに直接接続し、アプライアンスの HA ステータスを確認する。**Failover** タブをクリックして、アプライアンスのステータスを確認します。1 つのアプライアンスがアクティブで、もう一方のアプライアンスは非アクティブになっている必要があります。

図 5-44　　アクティブ サーバ

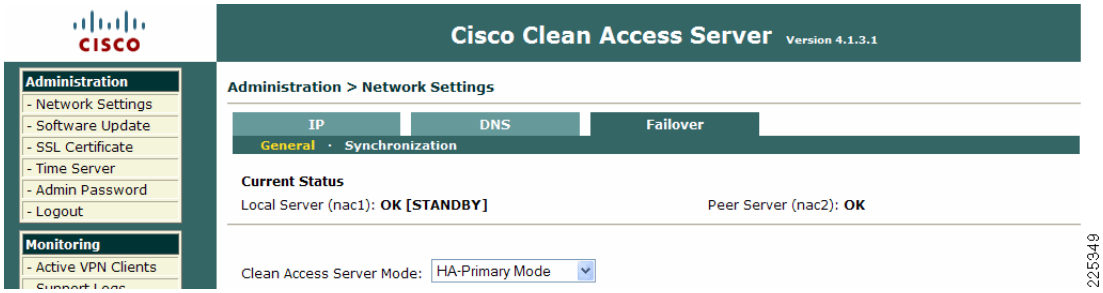
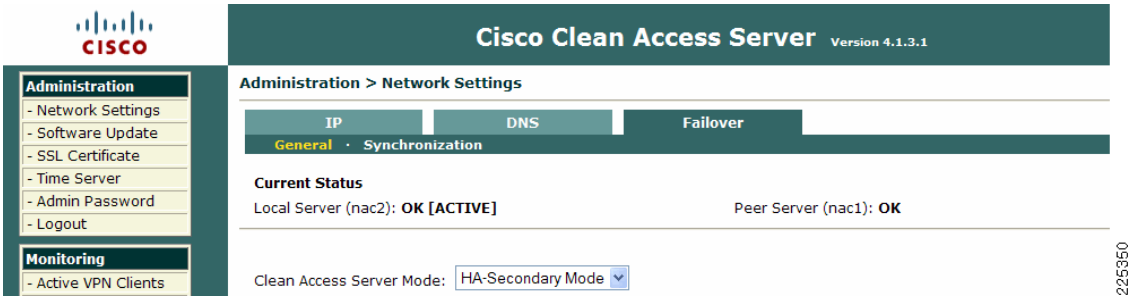


図 5-45　　非アクティブ サーバ



CAM への単一の NAC アプライアンスの追加

このプロセスは P.5-59 の「CAM への HA NAC ペアの追加」と同一です。ただし、アプライアンスの Trusted 管理インターフェイスが保持している実際の IP アドレスを使用する点が異なります。

Untrusted インターフェイスの接続（HA 設定）

NAC アプライアンス（複数可）を CAM にバーチャル ゲートウェイとして追加した後、HA ペアのフェールオーバー ステータスを参照して、一方のアプライアンスがアクティブ、もう一方が非アクティブになっている場合は（図 5-20 および図 5-21 を参照）、各アプライアンス上の信頼できないポートをスイッチ ブロックに接続できます。

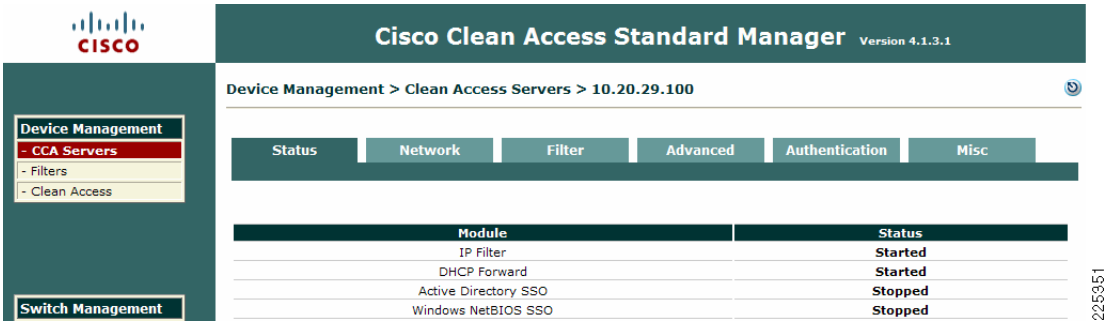
管理対象ネットワークの追加

CAM には、NAC のサービスを必要とするサブネットが設定されている必要があります。このマニュアルの NAC/Unified Wireless 設計の例を使用した場合、管理の対象となるネットワークは、VLAN 31、32、およびそれぞれの SVI に関連付けられている信頼できる側のサブネットです（P.5-35 の「スイッチ間トランクの設定」および P.5-38 の「SVI の設定」を参照）。

ステップ 1CAM の Server List ページで、**Manage** をクリックします。図 5-46 に示すように、サーバのステータスが表示されます。

（注）　以降に示す設定の追加と更新は、すべて、アクティブと非アクティブの両方の NAC アプライアンスに対して行います。

図 5-46　サーバのステータス



ステップ 2　**Advanced** タブをクリックします。図 5-47 に示すように、Managed Subnet サブメニューが表示されます。

図 5-47　Managed Subnet 設定サブメニュー

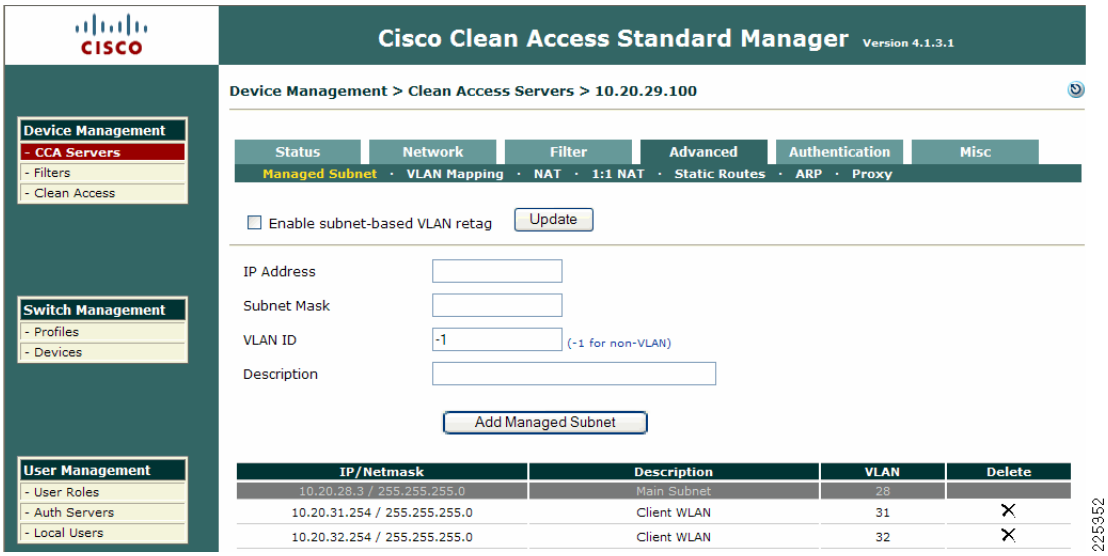


図 5-47 の設定では、2 つのクライアント サブネットが設定されています。これらのネットワークは、P.5-35 の「スイッチ間トランクの設定」および P.5-38 の「SVI の設定」で設定した信頼できる側の VLAN/ サブネットを表しています。また、これらは WLC の動的インターフェイス設定で設定したものと同一のサブネットです。P.5-52 の「WLAN クライアント インターフェイス」を参照してください。上の設定では、次の点に注意してください。

- サブネットベースの VLAN 再タグ付けを有効にしないでください。
- 管理対象サブネットにある IP アドレスも、NAC アプライアンスに割り当てる必要があります。したがって、WLAN コントローラと NAC による HA トポロジに含まれている所定の管理対象クライアント サブネットについては、次のアドレスを予約する必要があります。

  - Cat6K-1 SVI
  - Cat6K-2 SVI
  - HSRP スタンバイ IP
  - VLAN またはサブネットの動的インターフェイスを持つ各 WLAN コントローラ
  - NAC アプライアンスの管理対象サブネット IP（上記）
- この展開で使用される IP アドレス方式の計画について考慮する必要があります。エンド クライアント用のアドレスを十分に確保するには、VLSM マスキングが必要になることがあります。

上の管理対象サブネットの設定に関連する VLAN は、信頼できる側の VLAN 31 および 32 です。一方、WLAN コントローラの設定では、それぞれ VLAN 131 および 132 を使用します。P.5-52 の「WLAN クライアント インターフェイス」を参照してください。この点については、P.5-63 の「VLAN マッピング」で詳しく説明します。

VLAN マッピング

VLAN マッピングは、信頼できない側の VLAN を信頼できる側の VLAN にブリッジして、実質的に単一の VLAN を形成するものです。VLAN マッピングの概念については、P.5-4 の「インバンド モード」で説明しています。

Managed Subnet サブメニューで、VLAN Mapping サブメニューをクリックします。VLAN マッピングの設定例については、図 5-48 を参照してください。

図 5-48　　VLAN Mapping サブメニュー

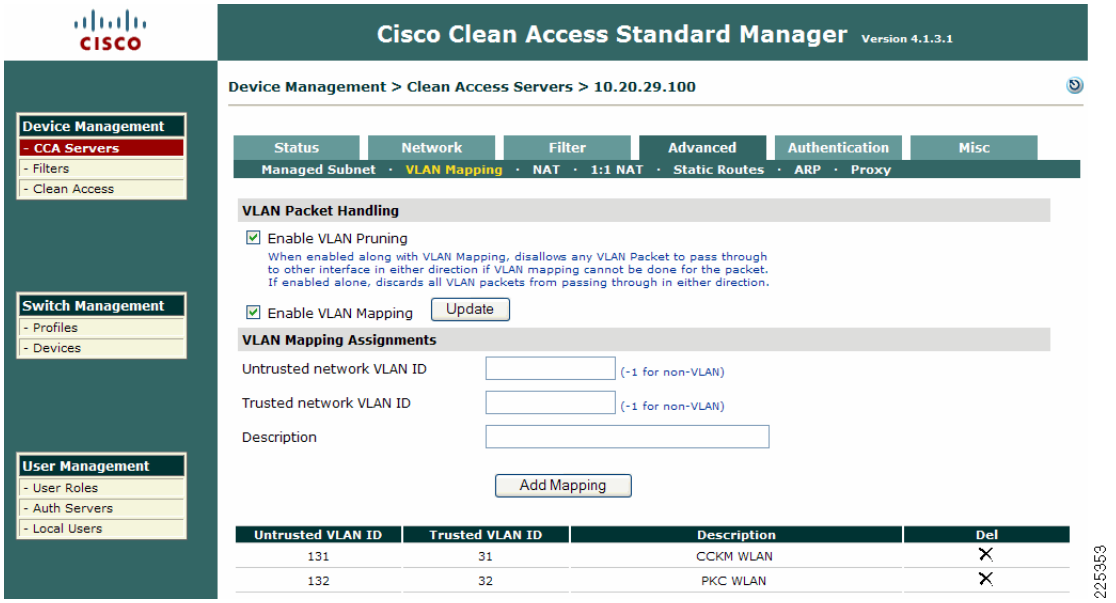


図 5-48 の設定では、2 つの VLAN マッピング ペアがあります。クライアントが（WLC から）信頼できない側の VLAN に到達した場合、要約すると次の処理が発生します。

- 認証を受けるように要求されます。
- ポリシーに準拠しているかどうかが確認されます。

- 認証を完了し、ポリシーへの準拠確認に合格したクライアントは、信頼できる側の VLAN にスイッチされます。

DHCP パススルー

NAC アプライアンスは、ユーザが認証されてポスチャ評価に合格するまで、デフォルトでは、信頼できない側の VLAN と信頼できる側の VLAN 間のトラフィックをすべてブロックします。例外となるのは、次の場合です。

- Filters サブメニューの設定で設定済みのデバイスまたはサブネット
- DNS パケット（Unauthenticated ロールでは、デフォルトで許可されています）
- DHCP パケット

NAC アプライアンスがバーチャル ゲートウェイとして設定されている場合は、DHCP パススルーを有効にして、クライアント デバイスが IP アドレスを取得できるようにする必要があります。これは、DHCP サーバが中央集中型であり、NAC アプライアンスの信頼できる側に配置されていることが前提になります。WLAN コントローラが DHCP サーバとして動作している場合、DHCP パススルーは必要ありません。ただし、規模の大きいキャンパス展開では、この構成はお勧めしません。

ステップ 1CAM の左側にあるメニューで、**Devices** の下の **CCA Servers** を選択し、P.5-59 の「CAM への HA NAC ペアの追加」で設定した NAC アプライアンスの **Manage** アイコンをクリックします。

ステップ 2サーバ ステータスのページで、**Network** タブを選択し、DHCP サブメニューを選択します。図 5-49 に示すように、DHCP 設定のページが表示されます。

図 5-49　NAC アプライアンス：バーチャル ゲートウェイ /DHCP の設定

ステップ 3図 5-49 に示したドロップダウン メニューから、**DHCP Passthrough** を選択します。

ステップ 4**Select DHCP Type** ボタンをクリックして、アプライアンス上でパススルー モードを確立します。

（注） 上の変更を行った後は、アプライアンスのリブートが必要になることがあります。この場合、アプライアンスは自動的にリブートします。

無線シングル サインオンの有効化

無線シングル サインオン（SSO）は、WLAN NAC 展開の重要なコンポーネントです。これは、ほぼすべての企業レベルの WLAN 展開において、WLAN セキュリティ ソリューションの一部として 802.1X/EAP 認証が実装されるためです。この認証は NAC アプライアンスの動作よりも

前に発生しますが、認証および認可は、NAC フレームワークの重要なコンポーネントです。したがって、クライアントを NAC で認証および認可できるメカニズムを導入して、WLAN ユーザが認証を 2 回受けずに済むようにする必要があります。

NAC アプライアンスは、次の 2 つの SSO メカニズムをサポートしています。

- VPN SSO
- Active Directory SSO

無線 VPN SSO での認証の設定

無線 SSO を有効にするには、次の作業が必要です。

- NAC アプライアンス上で VPN 認証を有効にする：802.1x/EAP WLAN が設定され、NAC の評価に従う各 WLC は、NAC アプライアンスで「VPN コンセントレータ」として定義する必要があります。
- WLC 上で RADIUS アカウンティングを有効にする：NAC アプライアンスで定義される各コントローラは、NAC で管理対象サブネットとなる各 802.1x/EAP WLAN についての RADIUS アカウンティング レコードを、NAC アプライアンスに送信するよう設定する必要があります。

ステップ 1CAM の左側にあるメニューで、Devices の下の CCA Servers を選択し、P.5-59 の「CAM への HA NAC ペアの追加」で設定した NAC アプライアンスの **Manage** アイコンをクリックします。

ステップ 2サーバ ステータスのページで、**Authentication** タブを選択し、**VPN Auth** サブメニューを選択します。

図 5-50 に示すように、VPN 認証の一般的な設定のページが表示されます。

図 5-50　　VPN 認証：一般的な設定

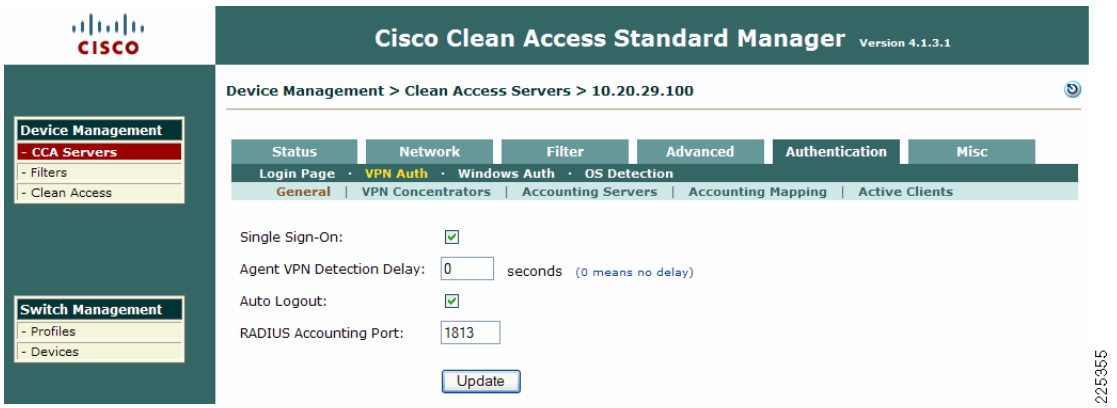


図 5-50 は、VPN 認証についてのグローバル設定オプションを示しています。SSO のチェックボックスをオンにし、WLAN コントローラ上で設定された番号と一致する RADIUS Accounting Port 番号も設定する必要があります。オプションで、**Auto Logout** チェックボックスをオンにすることもできます。これは、accounting stop を受信した後に、NAC アプライアンスでユーザ セッションを自動的にログアウトする機能です。

ステップ 3VPN Auth の General 設定サブメニューで、**VPN Concentrators** をクリックします。図 5-51 を参照してください。

図 5-51　VPN 認証：VPN コンセントレータの設定

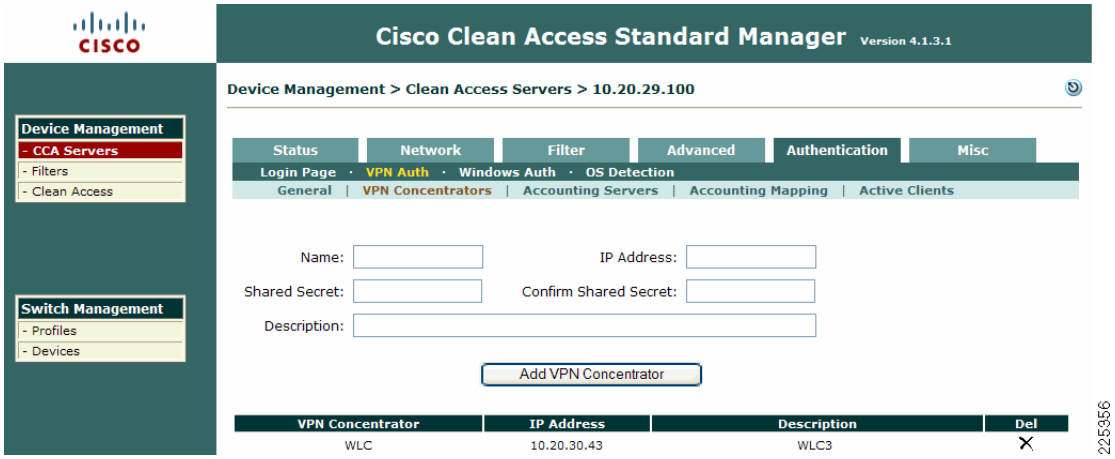


図 5-51 に示した設定画面では、WLAN コントローラを設定します。NAC アプライアンスの管理対象 802.1x/EAP ベース WLAN を保持している WLC ごとに、エントリを作成する必要があります。上のフィールドは、すべて説明不要の単純なものです。

（注） 上の VPN コンセントレータのエントリで使用する IP アドレスは、WLAN コントローラの管理 IP アドレスにする必要があります。

RADIUS プロキシ アカウンティング（オプション）

キャンパス展開において、RADIUS アカウンティング レコードをアップストリームの AAA サーバ（複数可）に転送する必要がある場合は、WLC で受信されたアカウンティング レコードをプロキシ処理して転送するように NAC アプライアンスを設定できます。

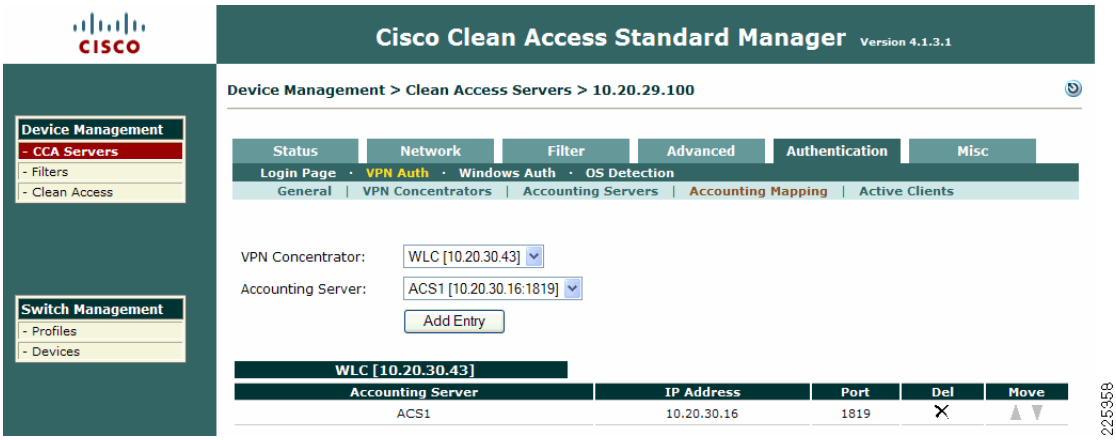
ステップ 1VPN Auth サブメニューで、**Accounting Servers** を選択します（図 5-52 を参照）。

図 5-52　アカウンティング サーバの設定

図 5-52 に示したアカウンティング サーバの設定ページには、NAC アプライアンスでプロキシ処理の対象となる適格なアップストリーム AAA サーバ（アカウンティング サーバ）が表示されます。次の手順は、WLAN コントローラとアップストリーム アカウンティング サーバの間にプロキシ関係を作成することです。

ステップ 2VPN Auth サブメニューで、**Accounting Mapping** を選択します（図 5-53 を参照）。

図 5-53　アカウンティングのマッピング



ステップ 1図 5-53 に示したプルダウン メニューを使用して、WLAN コントローラとアップストリーム アカウンティング サーバの間に、NAC アプライアンスを経由するマッピング（プロキシ）関係を確立します。

WLAN コントローラ：無線 VPN SSO のための RADIUS アカウンティングの設定

無線 SSO の設定に必要な最後の手順は、WLAN コントローラ上で RADIUS アカウンティングを有効にすることです。NAC アプライアンスでの管理対象の 802.1x/EAP WLAN を保持しているコントローラごとに、次の作業を行う必要があります。

ステップ 1コントローラのメイン設定ページで、最上部のメニュー バーにある **Security** を選択し、左側のメニューの **RADIUS Accounting** を選択します。図 5-54 を参照してください。

図 5-54　　WLAN コントローラの RADIUS アカウンティングの設定

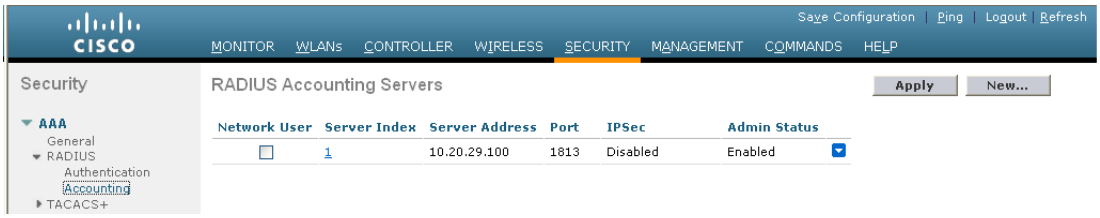


図 5-54 は、NAC アプライアンスの RADIUS アカウンティング サーバ エントリを示しています。次の点に注意してください。

- アカウンティング サーバの IP アドレスは、NAC アプライアンスの Trusted 管理インターフェイスの「サービス IP アドレス」にする必要があります。
- このサーバ エントリは、デフォルトでは設定済みのすべての WLAN で使用されるため、**Network User** チェックボックスはオンにしないでください。ただし、次の場合は除きます。
  - WLAN の RADIUS サーバ設定で、アカウンティングが明示的に無効になっている（WLC の 4.0.206.0 MR2 以降のイメージのみ）。
  - WLAN の RADIUS サーバ設定で、別のアカウンティング サーバが選択されている。
- 上の条件に該当しない場合、チェックボックスをオンにすると、NAC の管理対象になっていない WLAN のアカウンティング レコードを NAC アプライアンスが受信する可能性があります。

ステップ 2最後の手順は、NAC の管理対象となる 802.1x/EAP WLAN ごとに、アカウンティングを有効にすることです。コントローラのメイン メニューで、**WLANs** タブを選択します。

ステップ 3設定する WLAN をリストで確認し、**Edit** をクリックします（図 5-55 を参照）。

図 5-55　　WLAN の設定画面

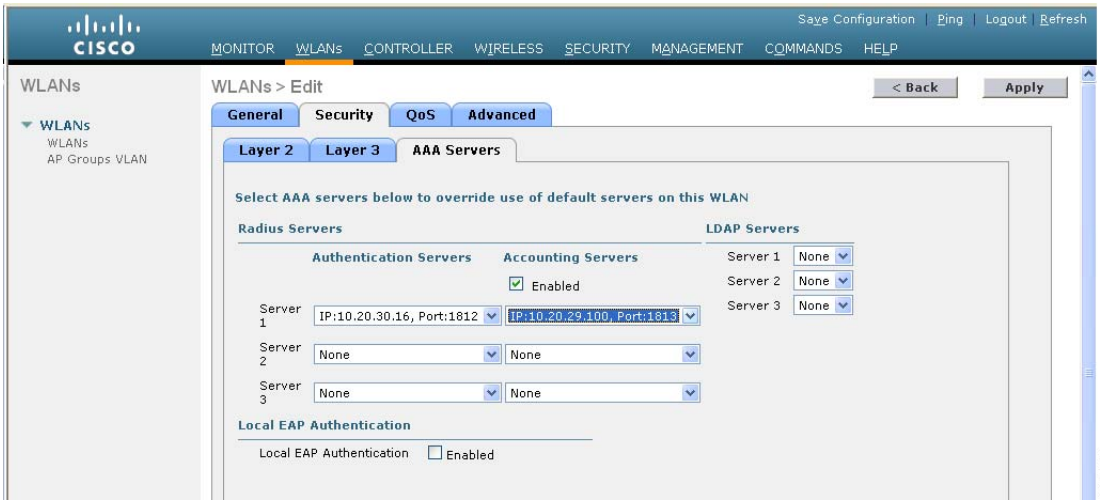
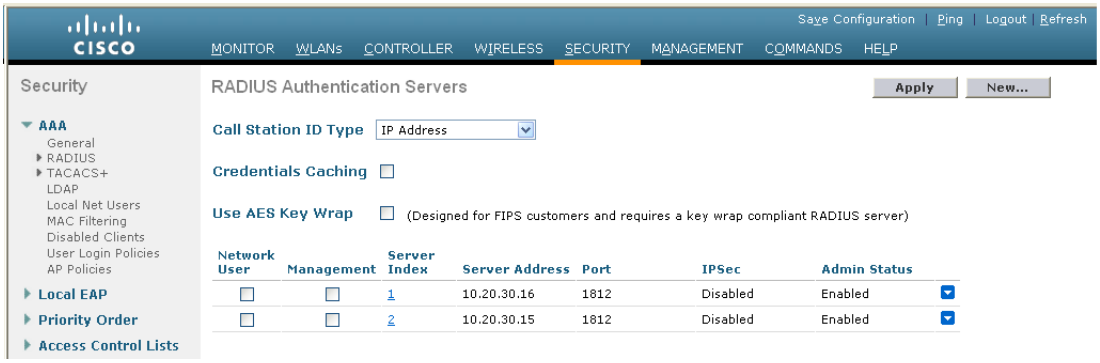


図 5-55 では、WLAN でアカウンティングが有効になっていて、図 5-54 で設定した NAC アプライアンス エントリが RADIUS アカウンティング サーバとして選択されています。

（注） 上で設定されているアカウンティング サーバ（NAC）エントリでは、NAC HA ペアのサービス IP を使用しています。このため、NAC で障害が発生した場合も引き続き無線 SSO を利用できます。

（注） WLC リリース 4.0 以前の場合、無線 SSO が正常に機能するには、RADIUS 認証サーバの設定で Call Station ID Type を **IP Address** に設定する必要があります（図 5-56 を参照）。リリース 4.1 以降の場合、Call Station ID の設定は重要な意味を持ちません。これは、RADIUS アカウンティング メッセージにレコードの標準アトリビュートとして Framed-IP-Address が含まれているためです。

図 5-56　　Call Station ID Type の設定



無線 Active Directory SSO での認証の設定

ステップ 1CAM の左側にあるメニューで、Devices の下の CCA Servers を選択し、P.5-59 の「CAM への HA NAC ペアの追加」で設定した NAC アプライアンスの **Manage** アイコンをクリックします。

ステップ 2サーバ ステータスのページで、**Authentication** タブを選択し、**Windows Auth** サブメニューを選択します。

ステップ 3サブメニューを使用して、この NAC アプライアンスの Active Directory サーバ名、Directory ドメイン名、およびアカウント詳細情報を設定します。アカウントは NAC アプライアンスごとに作成する必要があります。

図 5-57 に例を示しています。

図 5-57　Windows 認証：一般的な設定

（注） NAC のユーザ パスワードに DES 暗号化を強制的に使用するには、Active Directory サーバ（またはドメイン）上で、**ktpass** コマンドを使用する必要があります。このコマンドを使用しない場合、Windows は Linux でサポートされない RC4 を使用します。たとえば、*ktpass.exe -princ <casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM> -mapuser <casuser> -pass <Cisco123> -out <c:\casuser.keytab> -ptype KRB5_NT_PRINCIPAL -target <cca-eng-domain.cisco.com> +DesOnly* と入力します。NAC のマニュアルでは、-target アトリビュートの使用が指定されていません。このアトリビュートは、**ktpass** コマンドの動作に必要となる場合があります。この場合は、AD サーバの完全修飾ドメイン名を指定します。

ステップ 4CAM の左側にあるメニューで、**Auth Servers** を選択し、**Auth Servers** の下の **New** を選択して、サブメニューの内容を図 5-58 に示したように入力します。プロバイダー名は、Active Directory SSO の Auth Server の名前と同一です。

図 5-58　　認証サーバの設定

ステップ 5 Active Directory に対する Windows クライアント認証を確実に実行するには、未認証のクライアントが Windows クライアント トラフィックの転送のために NAC アプライアンスをパススルーすることについて、NAC アプライアンスで許可する必要があります（図 5-59 を参照）。

図 5-59　　Active Directory 認証トラフィックの許可

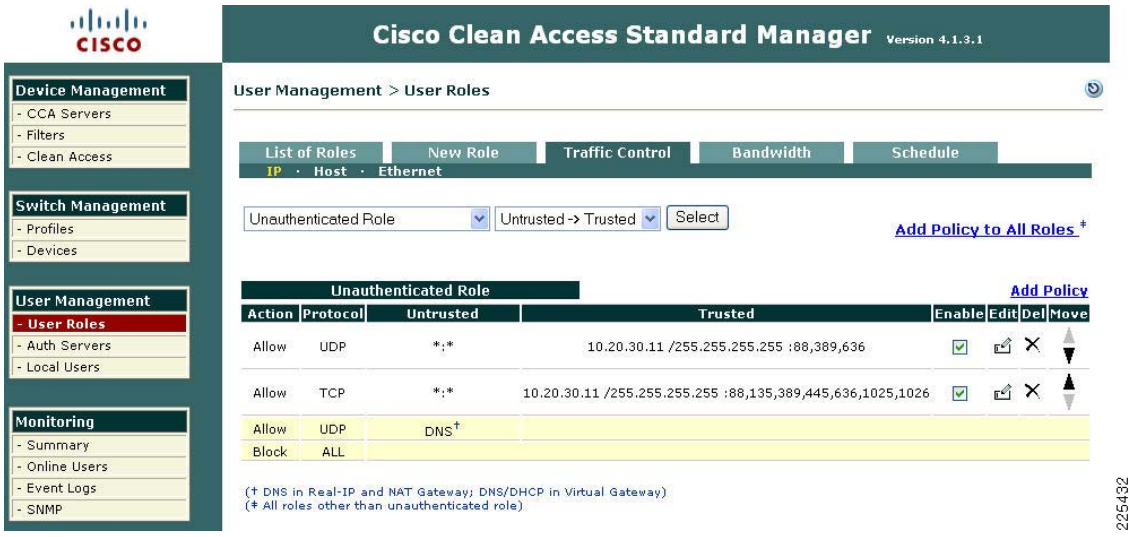
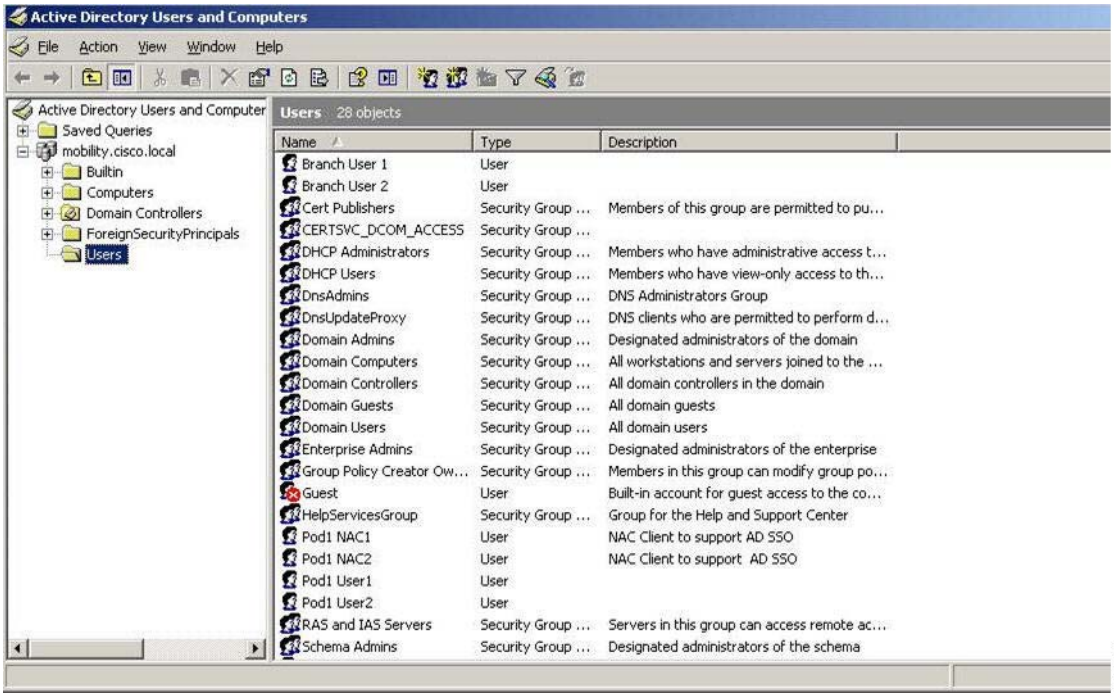


図 5-60 に、NAC アプライアンスから Active Directory に照会できるようにするために、Active Directory 内に作成された NAC アプライアンス アカウントの例を示します（Pod1 NAC1 および Pod1 NAC2）。

図 5-60　　AD のクライアントとしての NAC アプライアンス



無線ユーザのロールの作成

この項で以降に示すユーザ定義ページの設定例は、NAC アプライアンスを使用して無線 SSO 接続をサポートするための必要最小限の設定です。以降の項の内容は、他の認証方式、ポスチャ評価ポリシー、または修復技術を利用可能にするための包括的なガイドではありません。また、一般的な企業展開に導入できるオプションを網羅したものではありません。これらの高度なトピックに関する詳細なガイダンスについては、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

初期インストールが完了した後、NAC マネージャ（CAM）には次の 3 つのデフォルト ユーザ ロールが存在します。

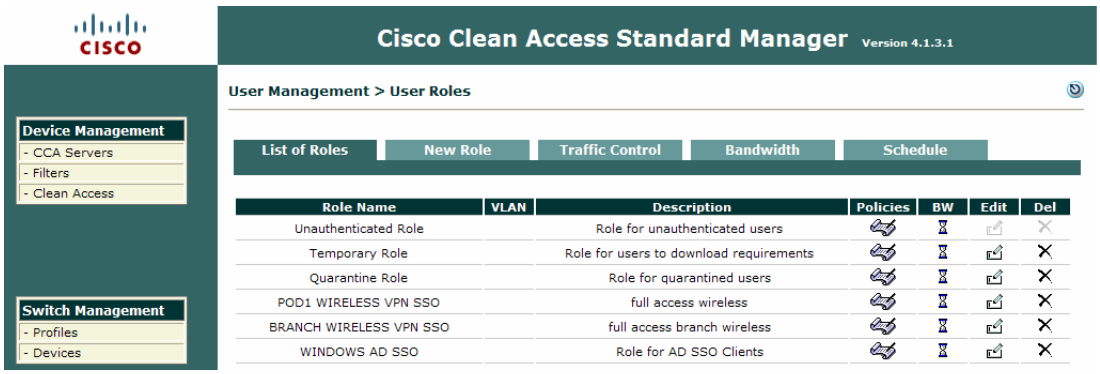
- Quarantine
- Unauthenticated
- Temporary

管理対象サブネット上のユーザが NAC アプライアンスの認証を受けていない場合、デフォルトでは Unauthenticated ロールを割り当てられます。Temporary ロールおよび Quarantine ロールは、システム管理者によって定義されたポリシー要件を満たしていない、修復の必要なユーザのために予約されています。

認証を完了し、すべてのポリシー確認に合格したユーザは、ユーザのログイン ロールに割り当てられます。ユーザのログイン ロールは、ユーザやグループに応じて異なるものにできます。したがって、無線ユーザ用のユーザ ロールを設定する必要があります。

ステップ 1CAM 画面の左側にあるメニュー カラムで、User Management の下の **User Roles** をクリックします。図 5-61 は、3 つのデフォルト ロールを示しています。

図 5-61　User Roles 画面



ステップ 2この画面で、**New Role** タブをクリックします。図 5-62 に示すように、新しいロールの設定画面が表示されます。

図 5-62　新しいユーザ ロールの設定

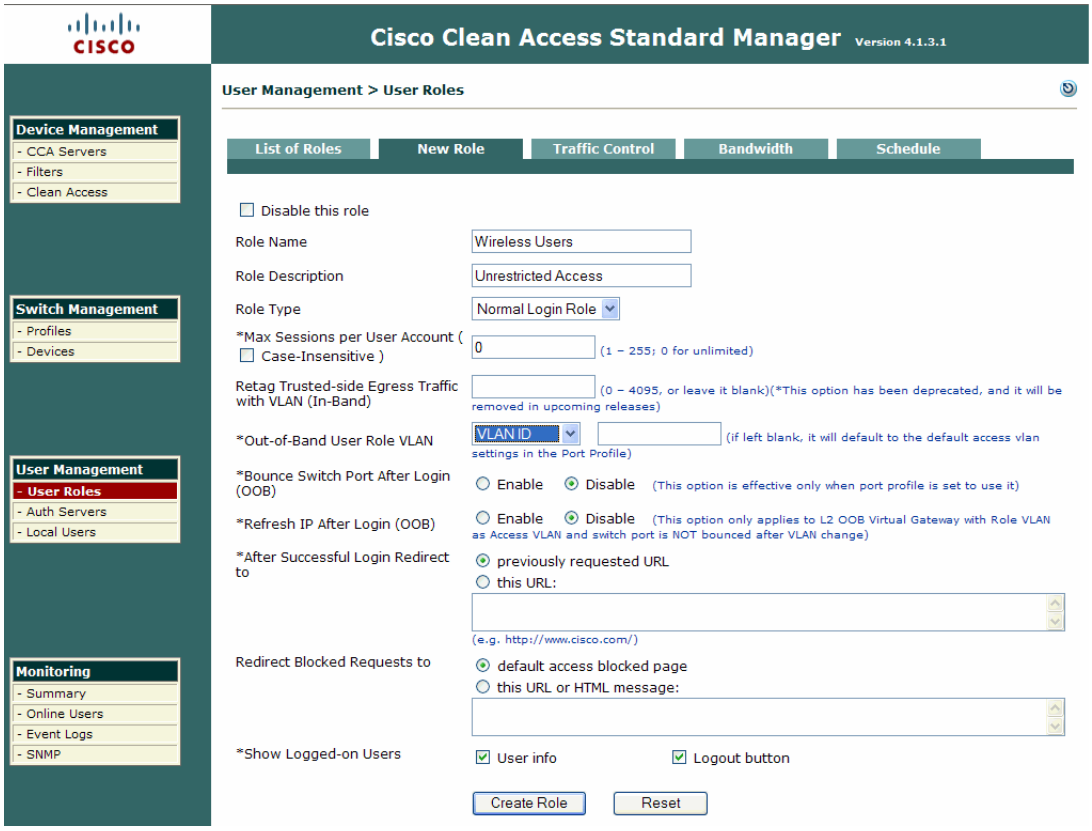


図 5-63 に示すように、ロールの名前と説明を入力します。表示されているその他のオプションは、すべてデフォルト値です。**Role Type** が Normal Login Role であることに注意してください。

ステップ 3 **Create Role** をクリックします。ユーザ ロールのリストが更新され、新しいロールが含まれた状態になります。

ステップ 4 Wireless Users ロールに関連付けられている **Policies** アイコンをクリックして、トラフィック ポリシーを設定します（図 5-63 を参照）。

図 5-63　新しい無線ユーザ ロール

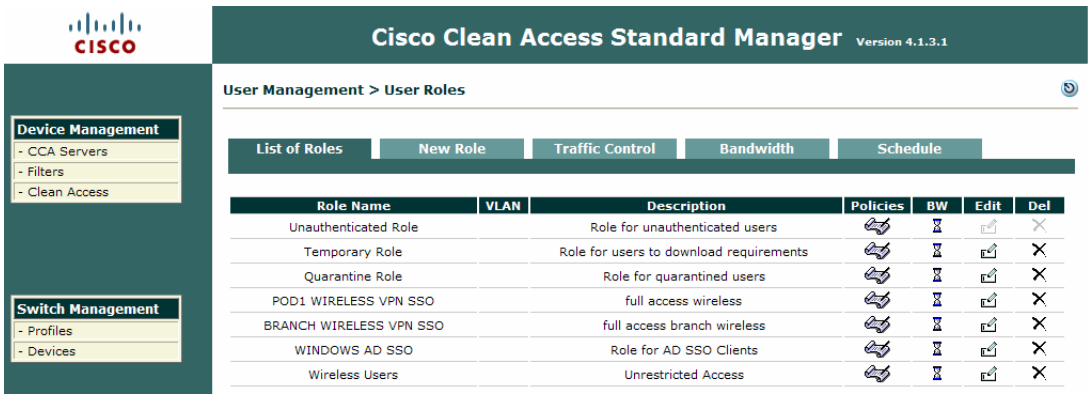
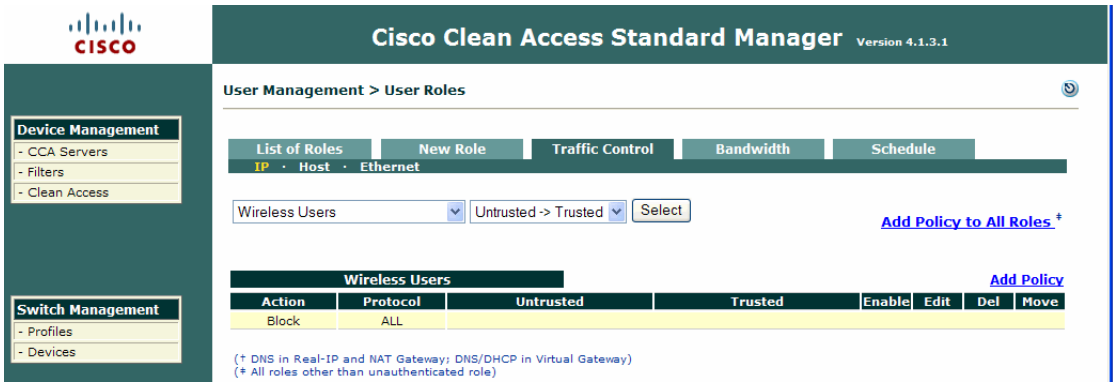


図 5-64 に、無線ユーザ ロールでのトラフィック制御設定の詳細を示します。デフォルトのポリシーでは、すべてのトラフィックがブロックされます。

図 5-64　　無線ユーザ ロールでのトラフィック制御



ステップ 5 Add Policy をクリックして、デフォルトのポリシーを修正します。

図 5-65 に示すように、新しいポリシーの設定画面が表示されます。

図 5-65　　新しいポリシーの設定

ステップ 6図 5-65 に示した Category プルダウン メニューで、**ALL TRAFFIC** を選択して、Untrusted インターフェイスから Trusted インターフェイスへのトラフィックをすべて許可し、Add Policy をクリックします（図 5-66 を参照）。

図 5-66　更新された無線ユーザ トラフィック ポリシー

正常に認証され、ポスチャ評価に合格した無線ユーザは、図 5-62 に示した更新済みのポリシーに基づいて、権限のあるリソースに無制限にアクセスできます。所定のユーザ ロールに対して、さらに多くのポリシー オプションを適用することもできます。

ここで示した例は、NAC アプライアンスを通じて無線クライアントのネットワーク アクセスをサポートするための必要最小限の設定に過ぎません。ユーザ ロールの設定の詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 6 章を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

無線ユーザ ロールの認証サーバの定義

ユーザのログイン ロールごとに、認証サーバを定義する必要があります。NAC アプライアンスでエンド ユーザの認証に使用される方法は、ログイン ロールによって決まります。次のような種類の認証タイプおよび認証方法がサポートされています。

- Kerberos
- Windows NT
- RADIUS
- LDAP
- シングル サインオン Active Directory
- シングル サインオン VPN

P.5-12 の「シングル サインオン VPN」、P.5-14 の「シングル サインオン Active Directory」、および P.5-64 の「無線シングル サインオンの有効化」で説明したように、無線ユーザの SSO は、NAC アプライアンスの VPN SSO 機能または SSO Active Directory 機能を使用することでサポートされます。次の設定手順では、図 5-55 で行った NAC アプライアンスの VPN 認証設定を、図 5-67 で定義した新規作成の無線ユーザ ロールにマップします。

ステップ 1CAM 画面の左側にあるメニュー カラムで、User Management の下の **Auth Servers** をクリックします。

図 5-67　　認証サーバの設定

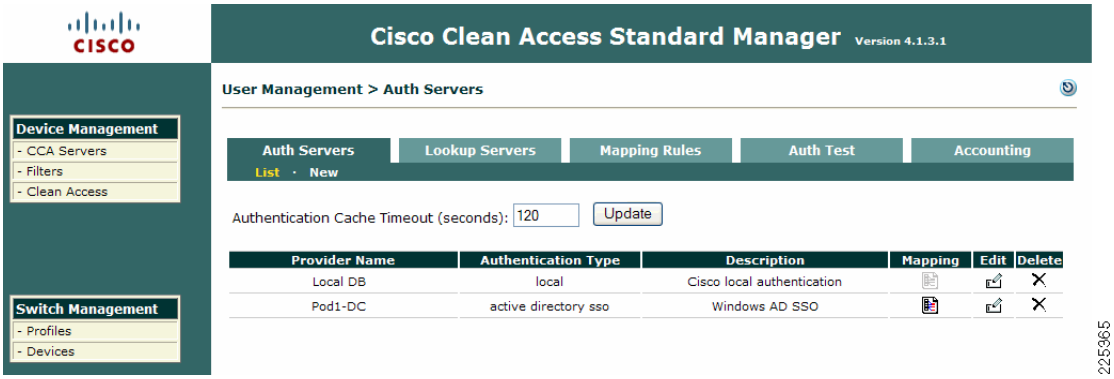


図 5-67 に示したように、CAM 上のローカル データベースを使用するデフォルトの認証サーバ ゲストが定義されています。この認証サーバは、ゲスト アクセス サービスに使用できます。

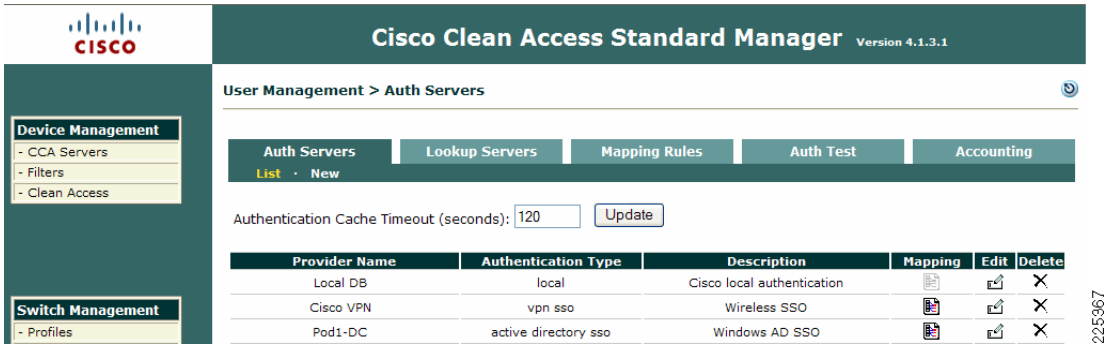
ステップ 2 Auth Servers サブメニューの New ボタンをクリックします（図 5-68 を参照）。

図 5-68　　新しい認証サーバの設定

図 5-68 では、Authentication Type が「Cisco VPN SSO」に設定され、Default Role は「無線ユーザのロールの作成」で設定した Wireless Users に設定されています（選択したメカニズムが Active Directory の場合は Active Directory SSO）。

ステップ 3説明を追加し、**Add Server** をクリックして設定を完了します。図 5-69 に示すように、新しいエントリが追加されます。

図 5-69　無線 SSO 用の VPN SSO 認証サーバ



無線 SSO については、内部または外部の認証サーバは設定されません。代わりに、無線ユーザがネットワークとのアソシエーションを確立してネットワークに接続しようとした場合、NAC アプライアンスがクライアントの MAC アドレスおよび IP を確認し、WLAN コントローラから受信したアカウンティング レコードの情報と照合します。一致が確認された場合、無線ユーザは自動的に NAC に認証されます。上の例では、認証サーバ「vpn sso」を使用して認証された無線ユーザすべてを無線ユーザのロールにマップしています。認証サーバ マッピング機能を使用することで、無線ユーザごと、または無線ユーザ グループごとに独自のロールを作成できます。この場合、有線ユーザまたはグループの割り当て先となる NAC アプライアンス ロールは、RADIUS VSA を使用して制御できます。詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 7 章を参照してください。このマニュアルは、次の URL で入手できます。

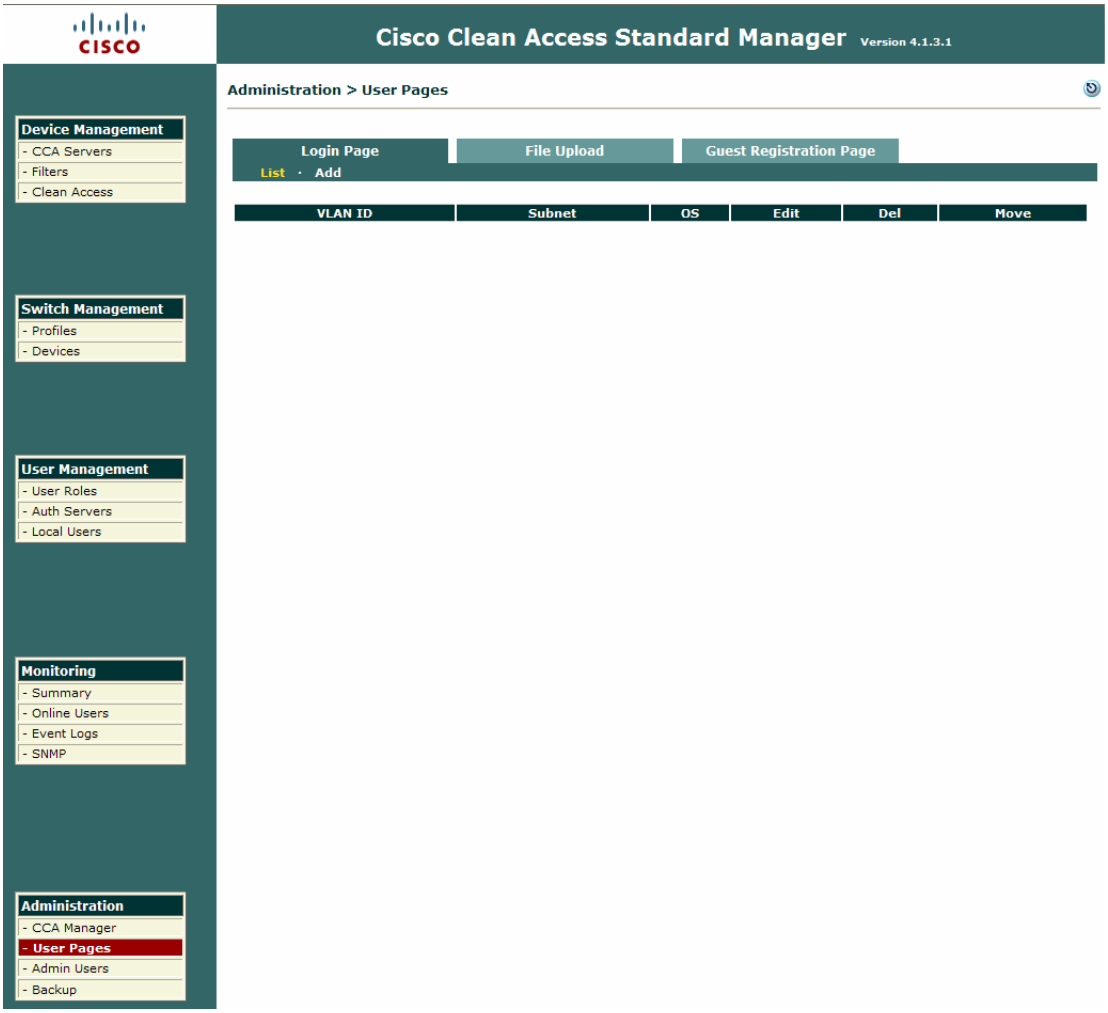
http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

ユーザ ページの定義

ユーザ ページは、認証、ポスチャ評価、修復を目的としてエンド ユーザが接続したとき、およびリダイレクトされたときに最初に表示されるページです。ユーザは、付与されたユーザ ロールで設定されている Clean Access 方式（ポスチャおよびポリシーの評価方式）によっては、Clean Access Agent の使用が必須となる場合があります。それ以外の場合は、NAC アプライアンスが備えるネットワーク スキャン機能を使用してポリシー評価とポスチャ評価を実行できます。クライアント マシンに Agent がインストールされている場合、基本的には、ユーザはユーザ ページにリダイレクトされなくなります。ただし、Agent がインストールされていないユーザも、ポリシーの要件に応じて、再認証および継続的なポスチャ評価のためにユーザ ページでの操作が定期的に必要になることがあります。

ステップ 1CAM 画面の左側にあるメニュー カラムで、Administration の下の **User Pages** をクリックします（図 5-70 を参照）。

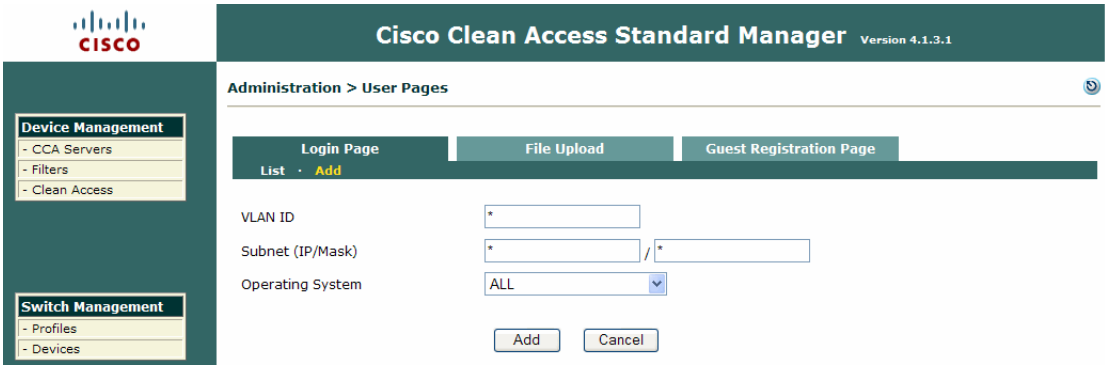
図 5-70　ユーザ ログイン ページのリスト



ステップ 2 Login Page タブの下の **Add** をクリックします。

新しいログイン ページのネットワークおよびオペレーティング システムに関する設定オプションについては、図 5-71 を参照してください。

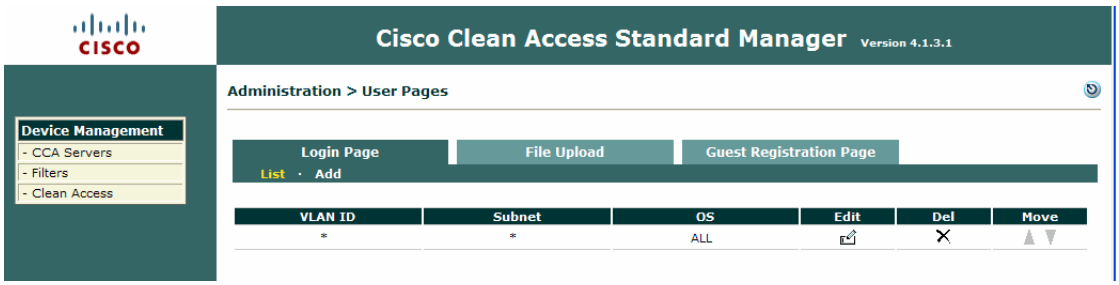
図 5-71　ログイン ページ：ネットワークおよびオペレーティング システムの設定



複数のログイン ページを設定して、さまざまなタイプのユーザやユーザ グループに対応することができます。ユーザ ページを最もすばやく作成する方法は、**Add** をクリックして、図 5-44 に示したデフォルトを受け入れることです。複数のページを設定する必要がある場合は、VLAN およびサブネットの情報を定義することにより、ユーザに表示されるページを指定できます。

（このガイドで提示した）無線展開で VLAN の情報を定義する場合は、信頼できる側の VLAN ID ではなく、信頼できない側の VLAN ID を使用します（P.5-54 の「信頼できない WLC インターフェイスへの WLAN のマッピング」を参照）。図 5-72 に、上のデフォルト値を使用したログイン ページを示します。

図 5-72　新規作成されたログイン ページ



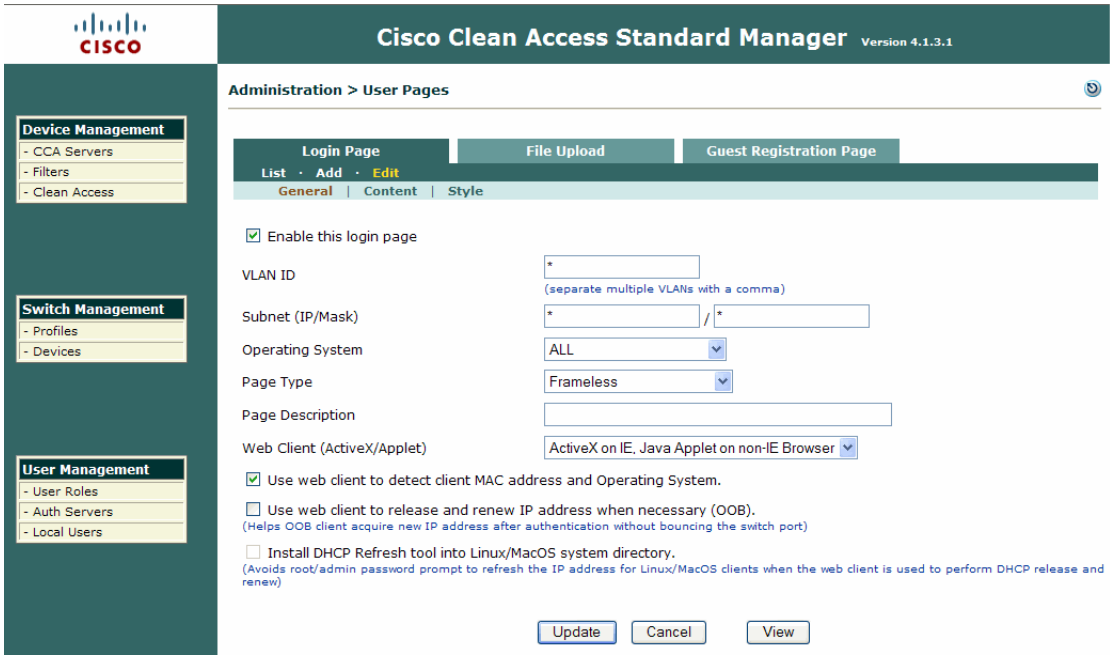
ステップ 3　**Edit** ボタンをクリックして、次の作業に進みます。

図 5-73 に示すように、一般的なログイン ページ設定オプションが表示されます。

このページで設定できるオプションの詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

図 5-73　　ログイン ページ：一般的な設定

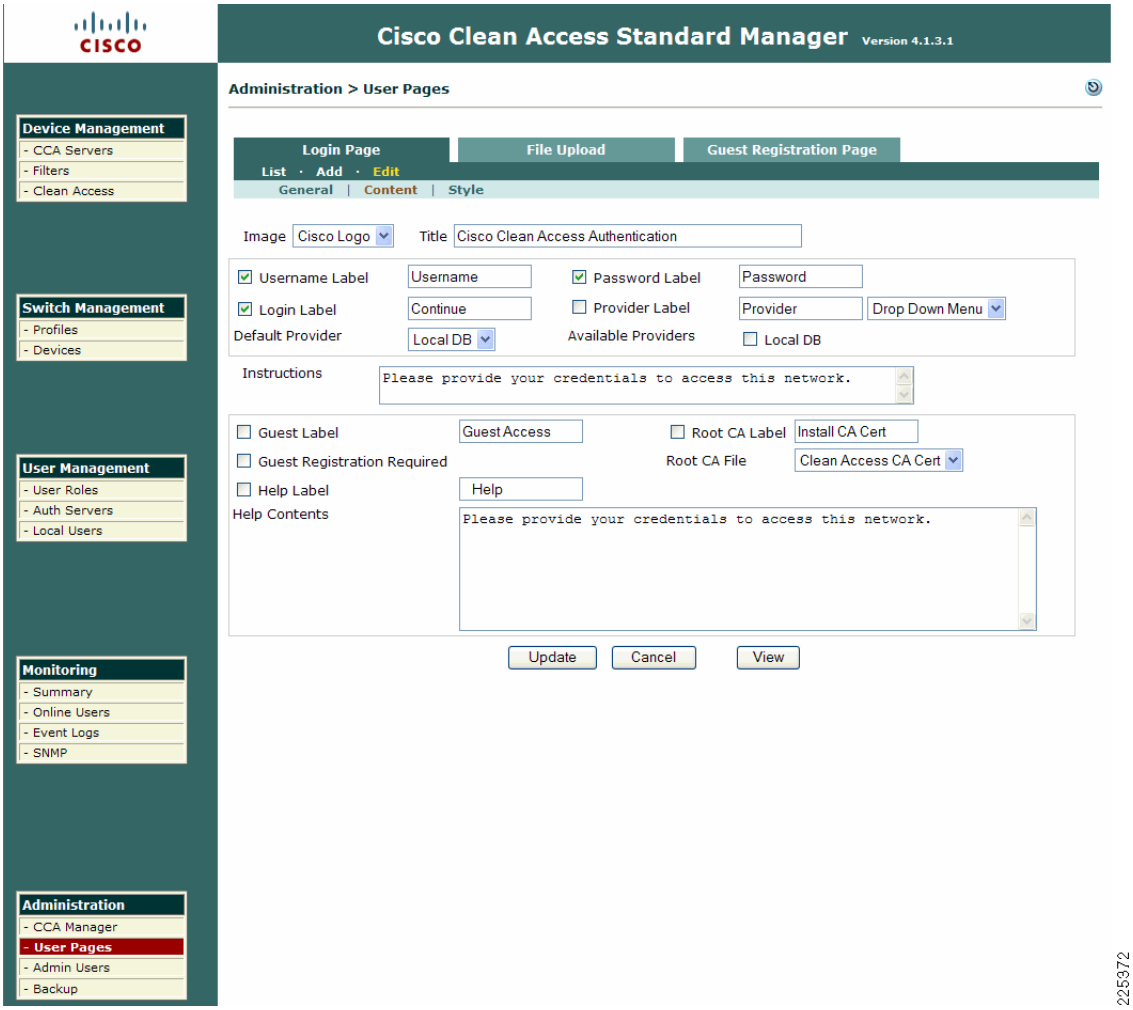


ステップ 4図 5-73 の **Enable this login page** チェックボックスがオンになっていることを確認してください。この展開での必要性に応じて、他の任意のオプションを設定し、**Update** をクリックします。

ページが更新された後、Login Page サブメニューの **Content** をクリックします。

ステップ 5ネットワークの管理者は、図 5-74 に示したコンテンツ設定ページを使用することで、ユーザに表示されるページをカスタマイズできます。

図 5-74　　ログイン ページのコンテンツに関する設定可能な項目



エージェントベースの無線 SSO の場合、設定は特に必要ありません。詳細については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 5 章を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

Clean Access の方式およびポリシーの設定

最後の設定手順は、所定のユーザ ロールで使用されるポスチャ評価方式を選択することです。ここまでの手順によって、ソリューションは無線ユーザ SSO をサポートするように設定されています。すでに説明したように、Clean Access Agent を（P.5-64 の「無線シングル サインオンの有効化」で設定した）VPN SSO と組み合せた場合に最も良好なエンド ユーザ エクスペリエンスが提供され、より包括的なポスチャ評価およびポリシー適用が行われます。

ステップ 1CAM 画面の左側にあるメニュー カラムで、Device Management の下の **Clean Access** をクリックします（図 5-75 を参照）。

図 5-75　Clean Access Certified List

図 5-75 のリストは、「クリーン」であることが証明されているすべてのデバイスを示しています。

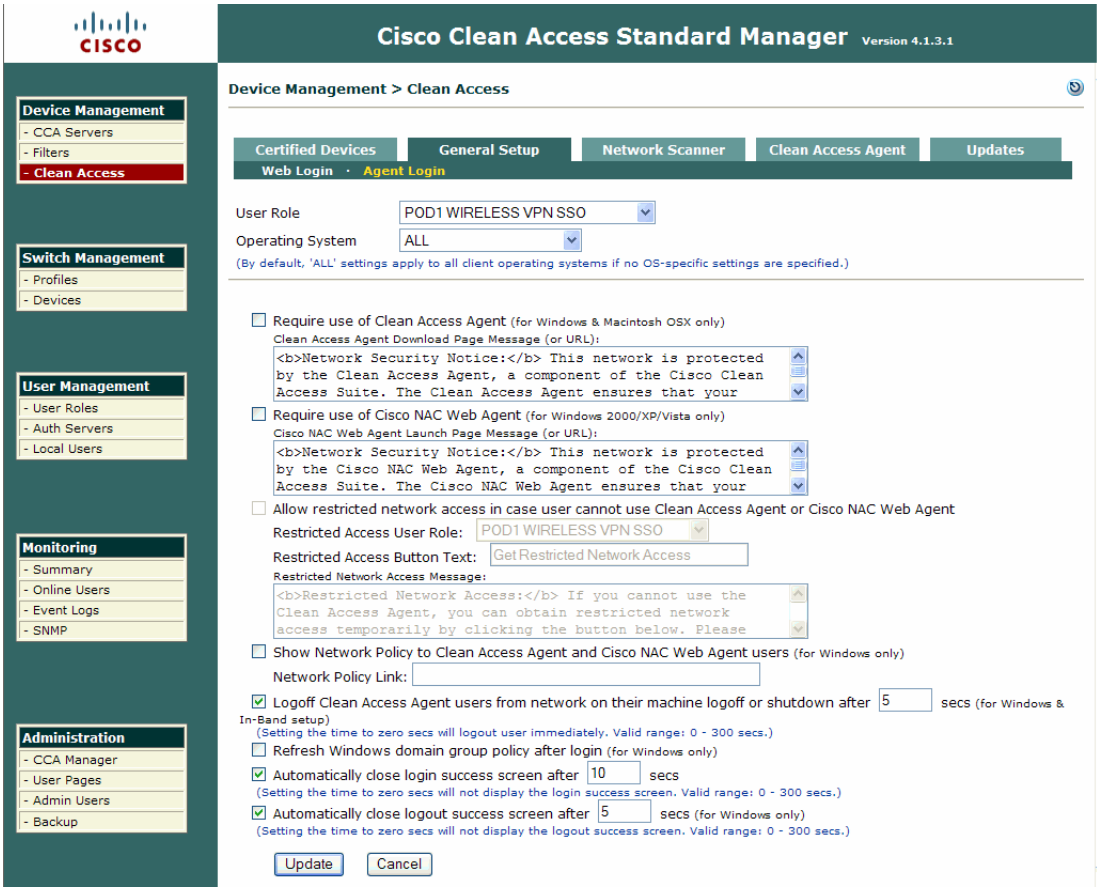
ステップ 2この画面で、**General Setup** タブをクリックします。

図 5-76 に、Web ログインを使用して認証を実行し、ネットワーク スキャナ方式を使用してポスチャ評価を受けるユーザに対して実行されるアクションの概要を示します。

図 5-76　Web ログインのネットワーク スキャンのパラメータ

ステップ 3図 5-76 の **General Setup** タブの下にある **Agent Login** オプションをクリックします。図 5-77 に、認証ユーザのログインで Clean Access Agent を使用する場合に関係する設定パラメータを示します。

図 5-77　Clean Access Agent のログイン パラメータ



ステップ 4図 5-77 の User Role で、**Wireless Users** を選択します。**Require use of Clean Access Agent** チェックボックスをオンにする必要があります。

このページの他のオプションの詳細および使用方法については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

ステップ 5完了したら、**Update** をクリックします。これで、NAC エンドポイント セキュリティを導入した Unified Wireless 展開をサポートするために必要となる、最小限の設定手順が完了しました。このガイドで説明した設定を使用することで、無線ユーザは、Clean Access Agent を通じて NAC アプライアンス経由で自動的に接続できます。特定のポスチャ評価アクションやポリシー適用アクションを受ける必要はありません。

ポスチャ評価、検疫、および修復のためのポリシーを作成するには、さらに設定が必要です。これらのトピックについては、このマニュアルの対象外です。Clean Access Agent のルール、要件、およびロール要件の設定については、『*Cisco NAC Appliance—Clean Access Manager Installation and Administration Guide*』の第 12 章を参照してください。このマニュアルは、次の URL で入手できます。

http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

エンド ユーザの例：無線シングル サインオン

図 5-78 ～図 5-86 に、Cisco NAC アプライアンスのエンドポイント セキュリティを導入した無線ユーザ SSO の例を示します。

図 5-78　CSSC サプリカントを備えた無線クライアント

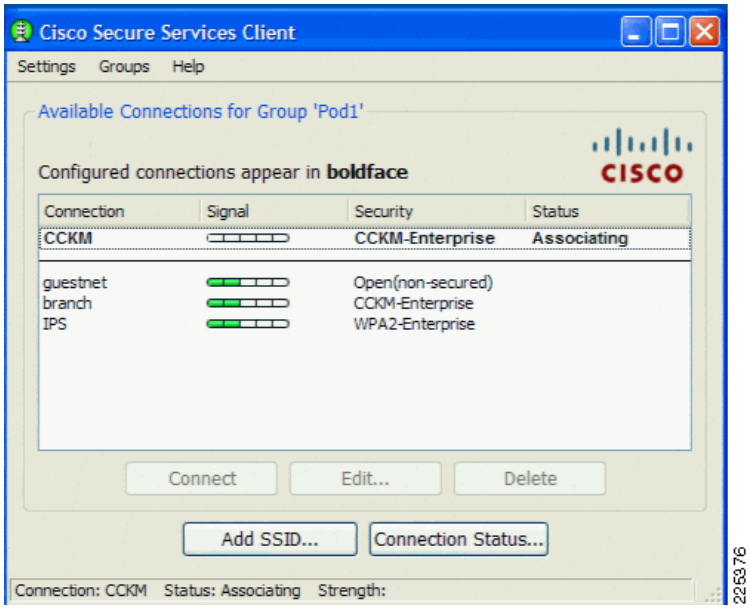


図 5-79　802.1x/PEAP 認証およびアソシエーションの完了

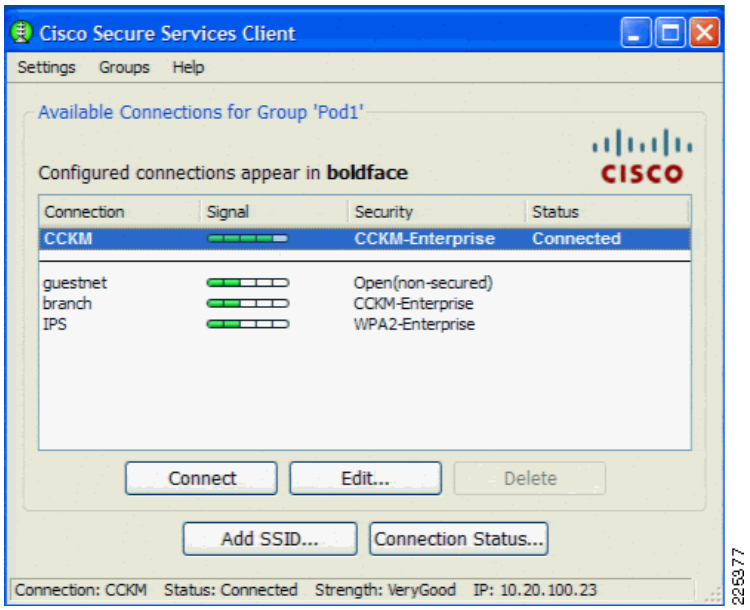


図 5-80　NAC Appliance アプライアンスのユーザ ページへのブラウザ リダイレクト

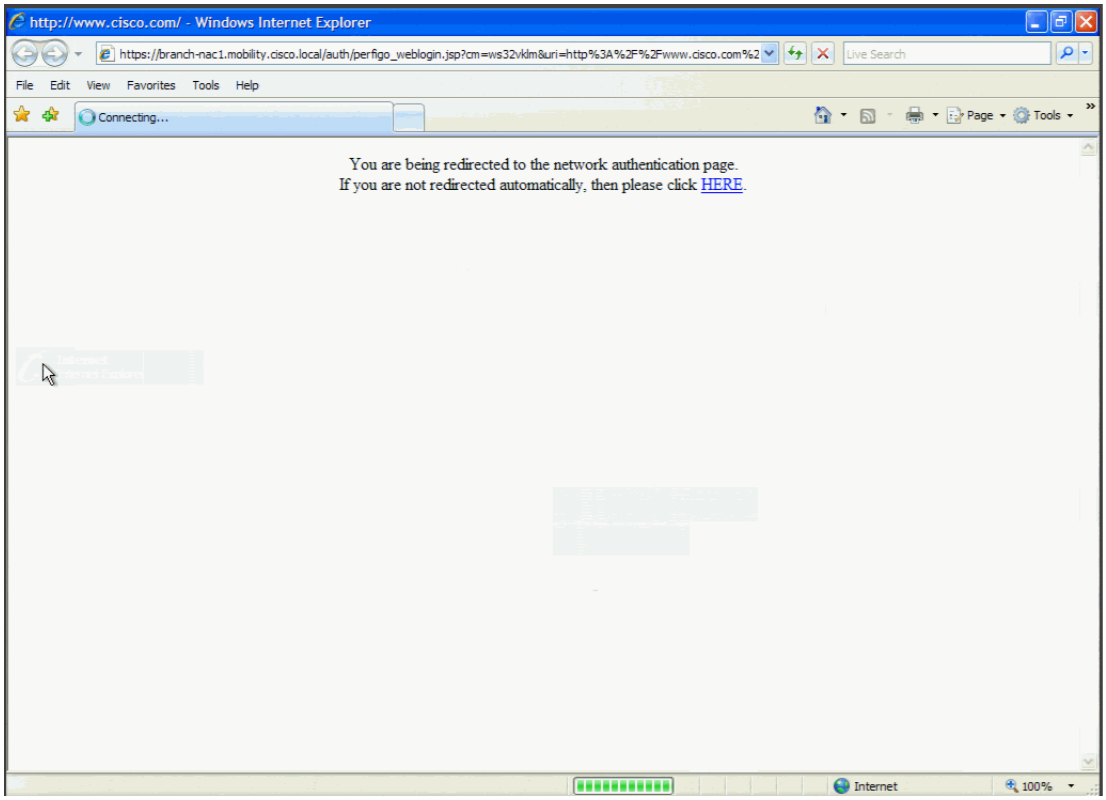


図 5-81　Clean Access Agent を使用するための必須ポリシー

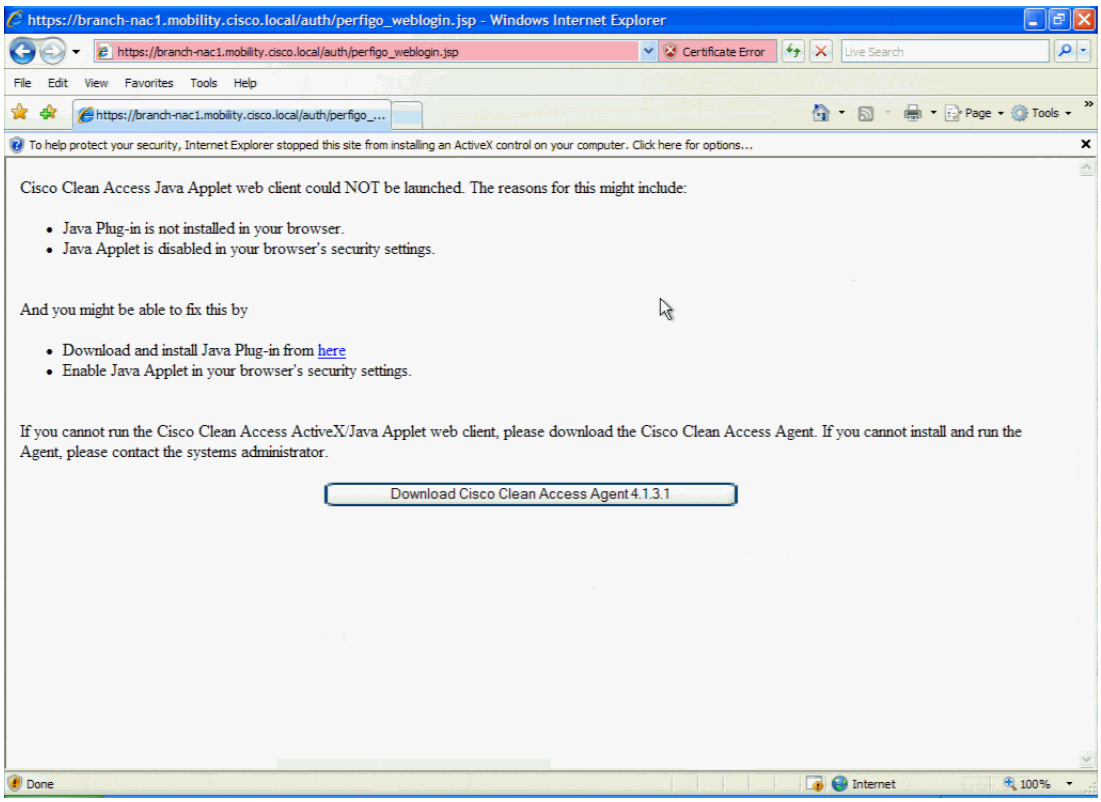


図 5-82　Clean Access Agent インストーラのダウンロード

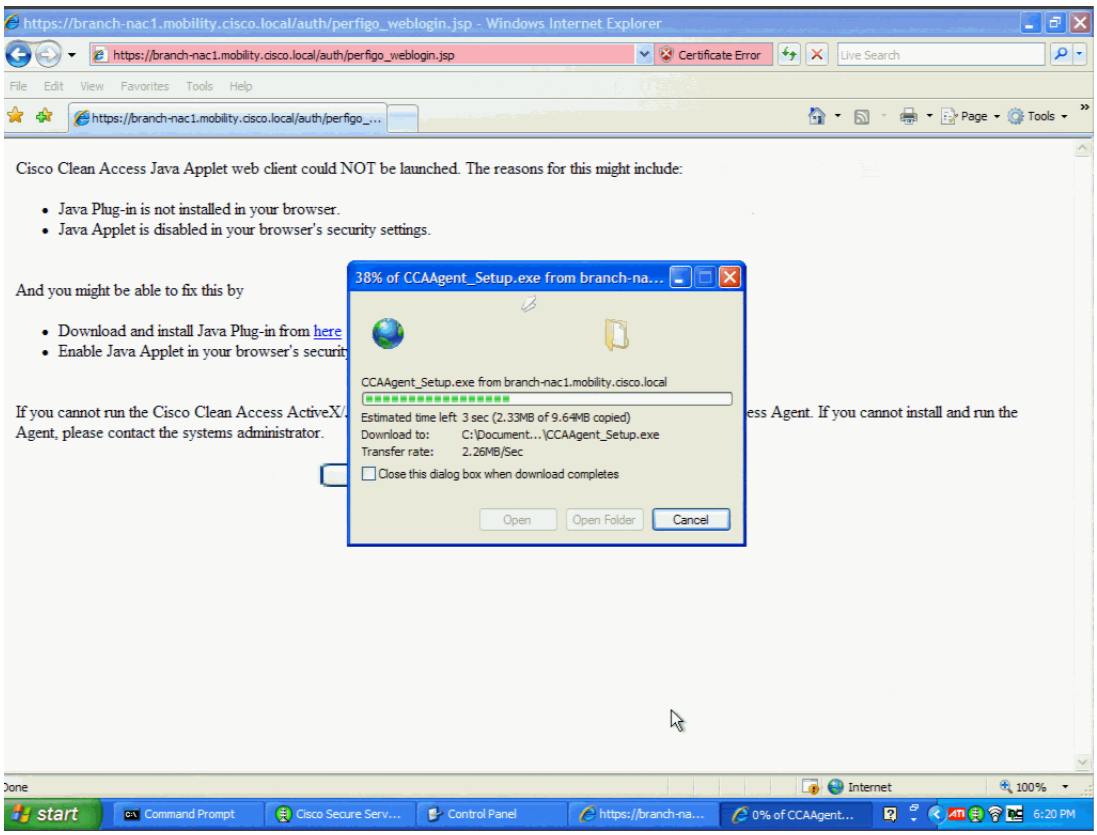


図 5-83　Clean Access Agent の自動インストール

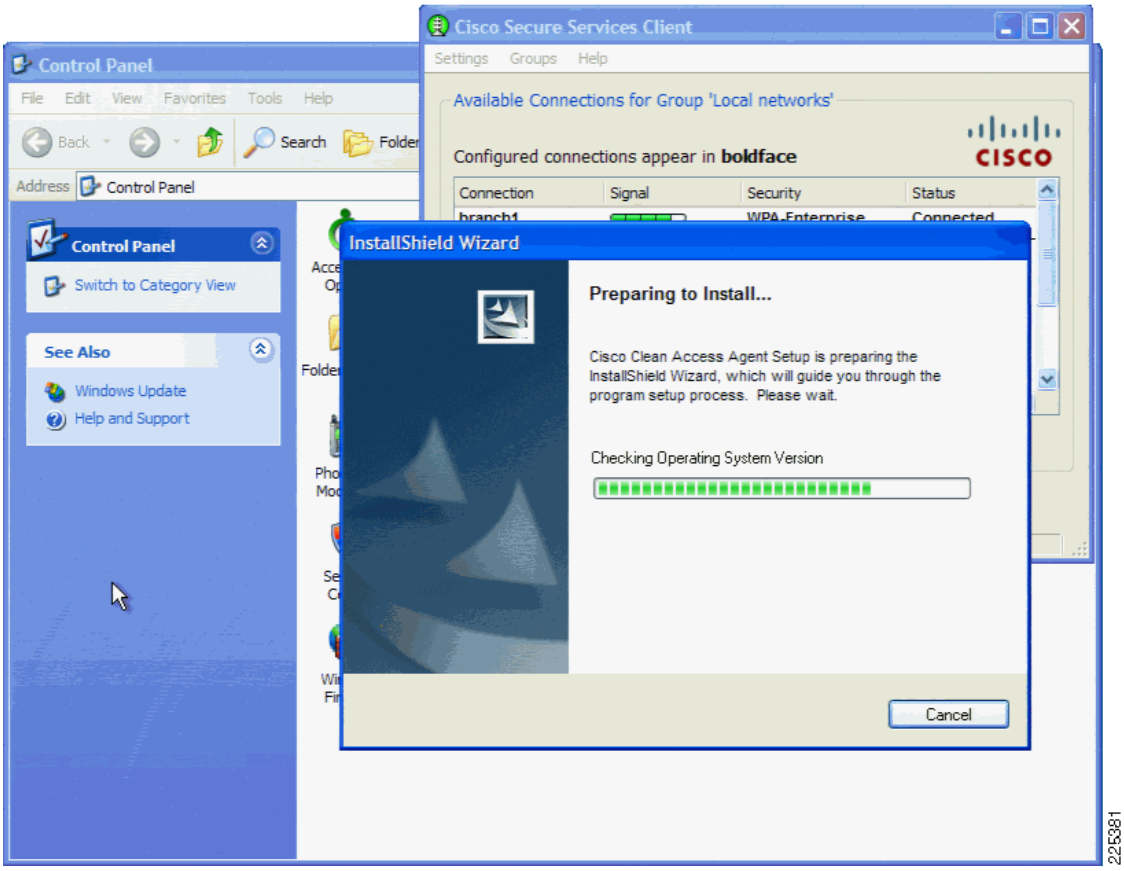


図 5-84　進行中の Clean Access Agent インストール

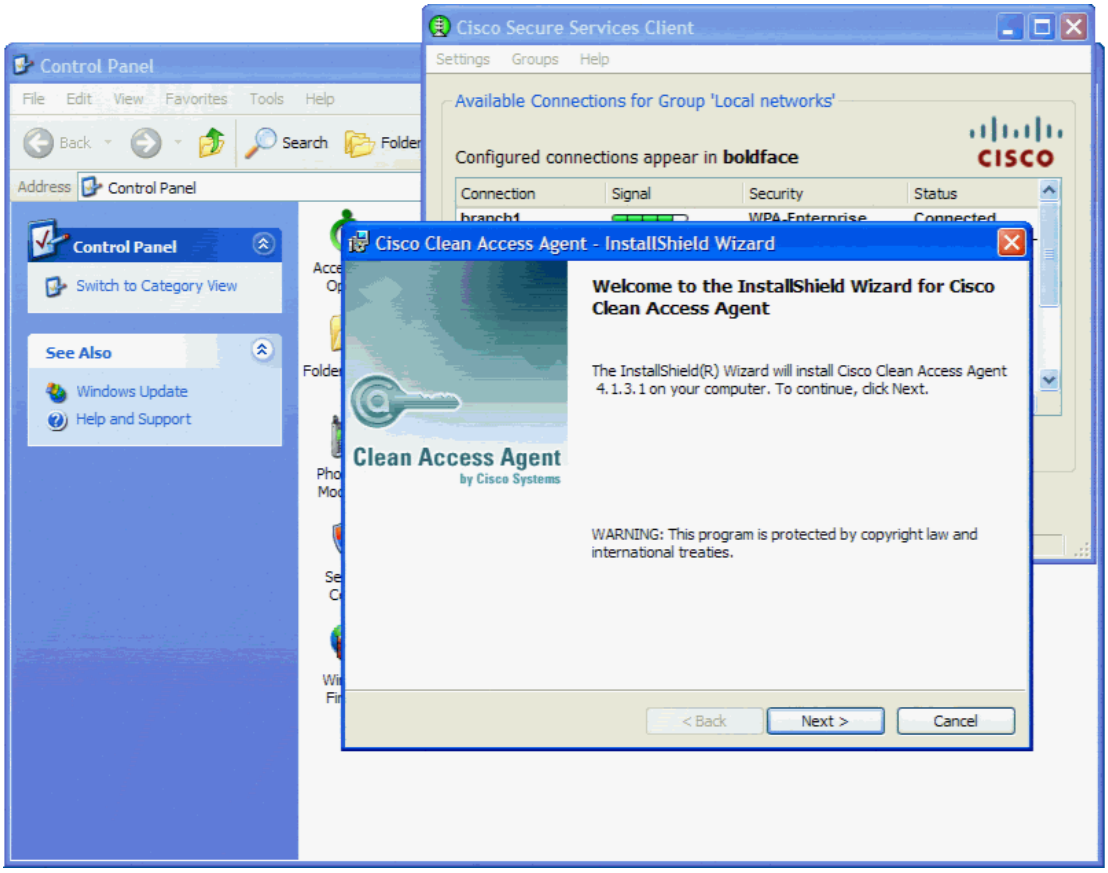


図 5-85　　Agent を通じた NAC アプライアンスへの自動ログイン

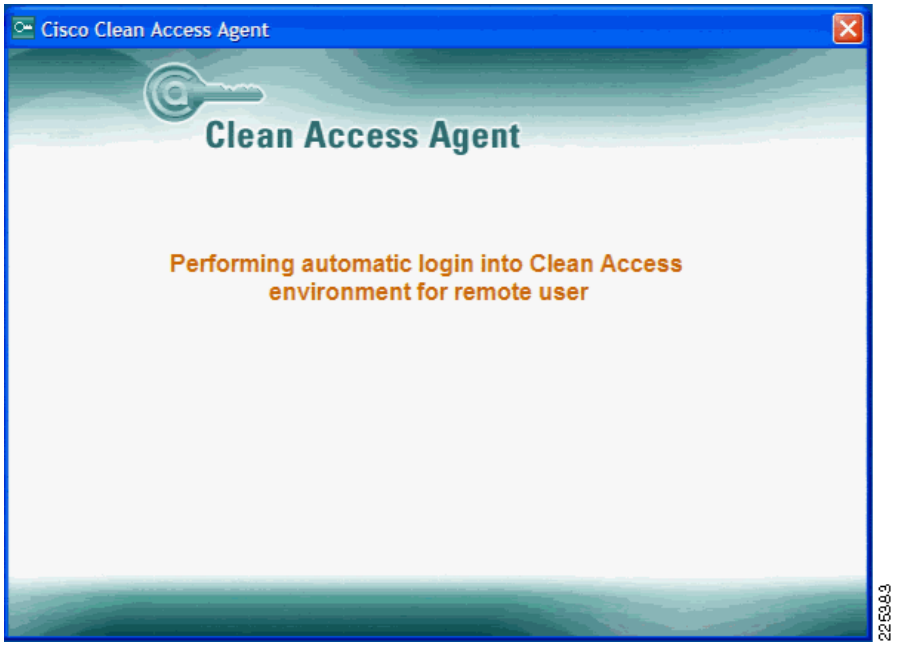
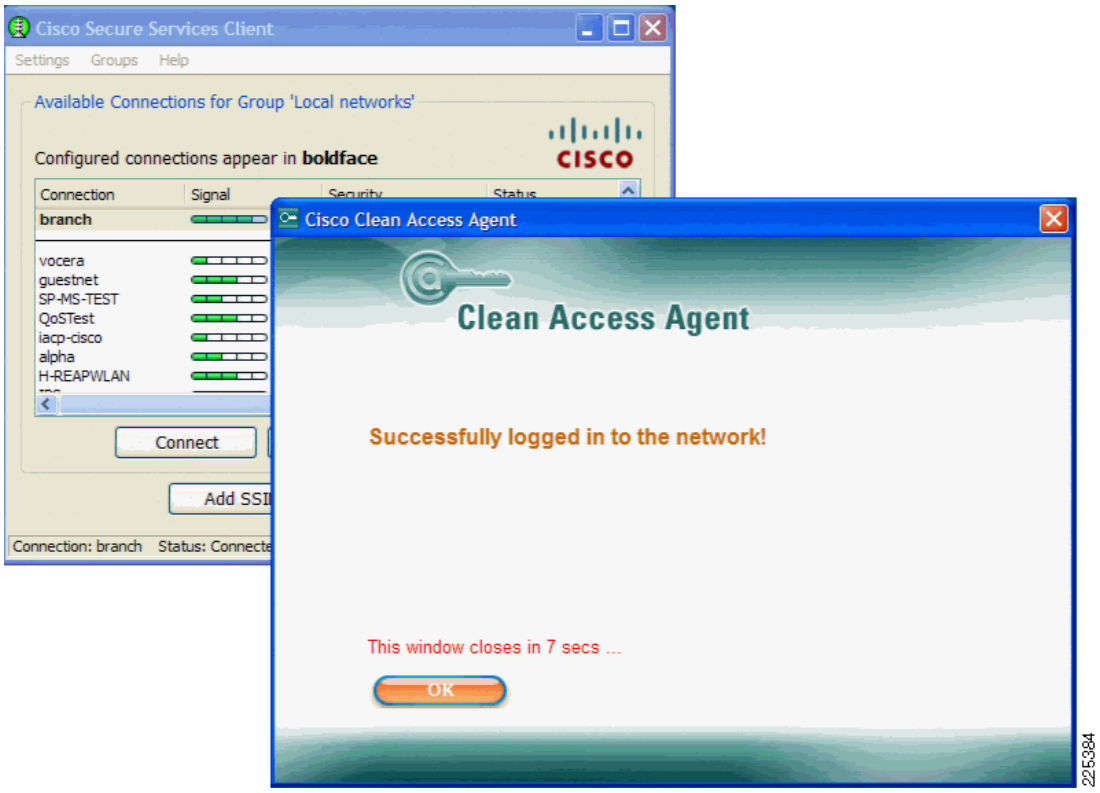


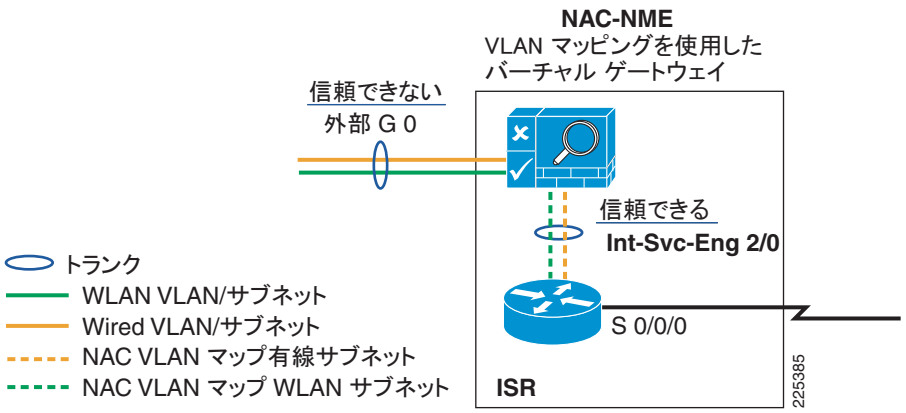
図 5-86　　NAC 認証の完了



ブランチ展開および NAC ネットワーク モジュール（NME）

ネットワーク モジュール スロットを搭載し、モジュールに対応する Integrated Services Router（ISR; サービス統合型ルータ）では、Cisco NAC ネットワーク モジュールがサポートされています（Cisco 2811、2821、2851、3825、および 3845 プラットフォーム）。ISR 用の Cisco NAC ネットワーク モジュール（NME-NAC-K9）は、製品の Cisco NAC アプライアンス ポートフォリオを小規模なロケーションまで延長し、本部からブランチ オフィスまでの Network Admission Control（NAC; ネットワーク アドミッション制御）機能の導入を支援します。NAC アプライアンス サーバ機能が ISR 用のネットワーク モジュールに統合されることで、データ、音声、およびセキュリティ上の要件について、ネットワーク管理者がブランチ オフィス内の単一デバイスを管理できるようになり、ネットワークの複雑さ、IT スタッフに対するトレーニングの必要性、予備的な装置の必要性、および保守コストを低減できます。ブランチ オフィスに展開されたサービス統合型ルータ用の Cisco NAC ネットワーク モジュールは、潜在的な脅威が WAN を経由してネットワークに悪影響を及ぼす前に、ローカルで脅威に対処します。図 5-87 に、NAC-NME、および NME の ISR への統合の概略図を示します。NAC-NME は、標準の NAC アプライアンスと同一の論理インターフェイス（Trusted インターフェイスと Untrusted インターフェイス）を提供します。Untrusted インターフェイスは NAC-NME 上の物理 RJ-45 コネクタであり、Trusted インターフェイスは ISR バックプレーンが終端となります。

図 5-87　NAC-NME と ISR の接続



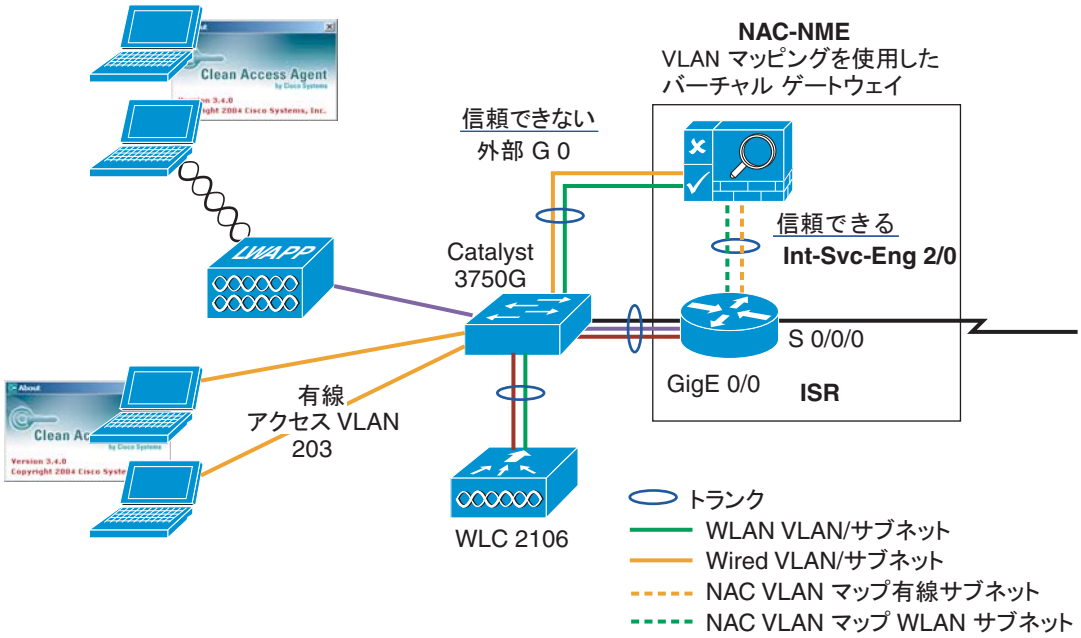
NAC-NME は、NAC アプライアンスと同一のインターフェイスを使用して管理され、アプライアンスと同一の機能セットを備えています。ただし、NAC アプライアンスのハイ アベイラビリティおよびスケーリングに関する機能は除きます。NAC-NME は NAC アプライアンスと同一の管理インターフェイスを使用して設定し、機能も同一のものが使用されるため、設定についてはここで繰り返しません。ここでは、図 5-88 に示したネットワーク設定例のみを中心に説明します。

ハイ アベイラビリティに関する考慮事項

この NAC ブランチ ソリューションでは、中央集中型の Clean Access Manager との通信が必要です。したがって、この設計はハイ アベイラビリティ WAN 接続を前提としています。このハイ アベイラビリティ WAN 接続では、802.1X/RADIUS 認証も前提条件になります。ブランチ

WLC では、ローカルの EAP 認証機能をローカル認証に使用することもできますが、これらの認証は RADIUS アカウンティング情報を生成しないため、VPN シングル サインオン実装での使用には適しません。

図 5-88　NAC-NME とブランチ接続の例



次の設定は、NAC-NME の Trusted インターフェイスが ISR 上でどのように終端するかを示しています。この設定に示したように、NAC-NME の Trusted インターフェイスは、**interface Integrated-Service-Engine2/0** コマンドによってトランク インターフェイスとして終端します。NAC-NME の管理インターフェイスはネイティブ インターフェイスであり、クライアント トラフィックは別のサブインターフェイス上に設定されます。

```
!
interface Integrated-Service-Engine2/0
 ip address 10.20.200.17 255.255.255.252
 service-module ip address 10.20.200.18 255.255.255.252
 no keepalive
!
interface Integrated-Service-Engine2/0.4
 description WLAN 204 Clients
 encapsulation dot1Q 4
 ip address 10.20.204.1 255.255.255.0
 ip helper-address 10.20.30.11
!
interface Integrated-Service-Engine2/0.6
 description Wired Clients
 encapsulation dot1Q 6
 ip address 10.20.206.1 255.255.255.0
 ip helper-address 10.20.30.11
```

ブランチ NAC と SSO

SSO は、キャンパスの場合と同様に、ブランチでも重要なものになります。ブランチ展開では、通常、NAC NME を有線クライアントと WLAN クライアントの両方に使用します。有線クライアントがブランチ スイッチで 802.1X 認証を受ける場合、VPN SSO が有効なソリューションになることもありますが、有線 NAC クライアントが 802.1X/EAP 認証を使用していない場合は、Active Directory SSO がブランチでの最善の SSO ソリューションです。

WLCM と NAC-NME

このバージョンのデザイン ガイドでは、ブランチ テストについて、WLC 2106 を使用した設計および設計テストを中心に説明しました。ただし、Cisco Unified Wireless Network のブランチ展開には Wireless LAN Controller Module（WLCM; 無線 LAN コントローラ モジュール）が含まれている場合もあるため、NAC-NME の実装では、この設計についても検討しました。Cisco Unified Wireless Network および NAC の基本的な設定は、WLC 2106 と WLCM のどちらについても同一です。WLC 2106 展開と WLCM 展開の主な違いは、ISR 上で終端する WLCM によってもたらされます。つまり、WLAN クライアント トラフィックは NAC-NME にルーティングされる必要があり、アウトバウンドトラフィックが NAC-NME を経由することを強制するポリシー ルートが必要です。この様子を図 5-89 に示します。ポリシー ルートによって、アウトバウンドトラフィックが NAC-NME を経由することを強制できますが、WLAN クライアントのサブネットは ISR に直接接続されているため、インバウンドトラフィックを NAC-NME 経由で転送することはできません。この様子を図 5-90 に示します。WLCM クライアント トラフィックが双方向で NAC-NME を経由することを強制するメカニズムとしては、Integrated Routing and Bridging（IRB）または VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）を実装することによって、ルータ内でブリッジングを提供するか、レイヤ 3 転送パスを分割する方法が適しています。ただし、このデザイン ガイドではテストされていません。

図 5-89　　WLCM とポリシー ルーティングのアウトバウンドトラフィック

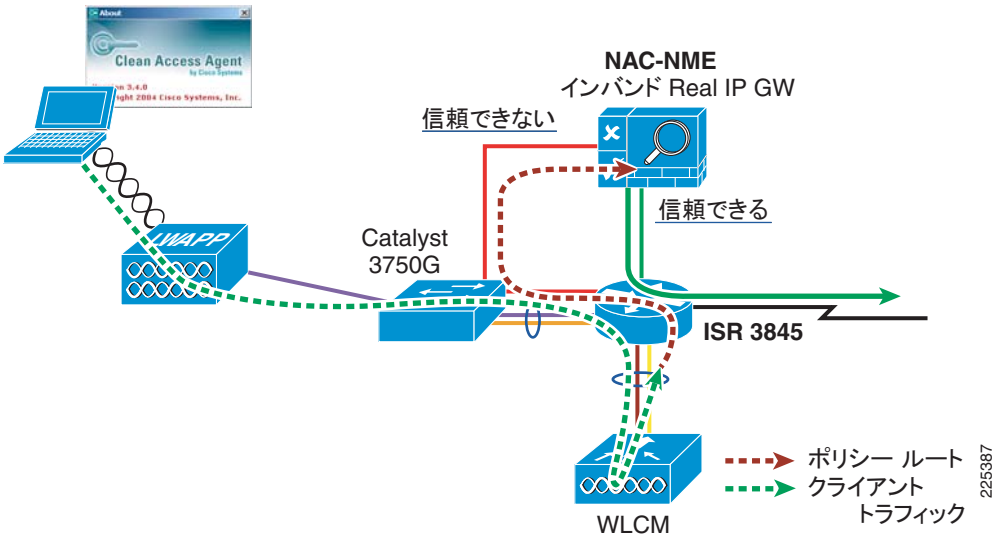
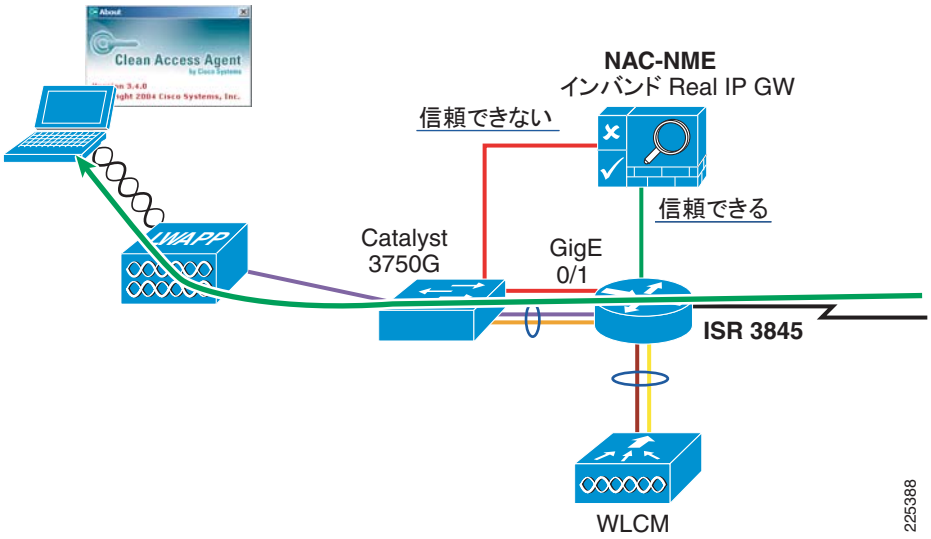


図 5-90　　WLCM とインバウンド トラフィック

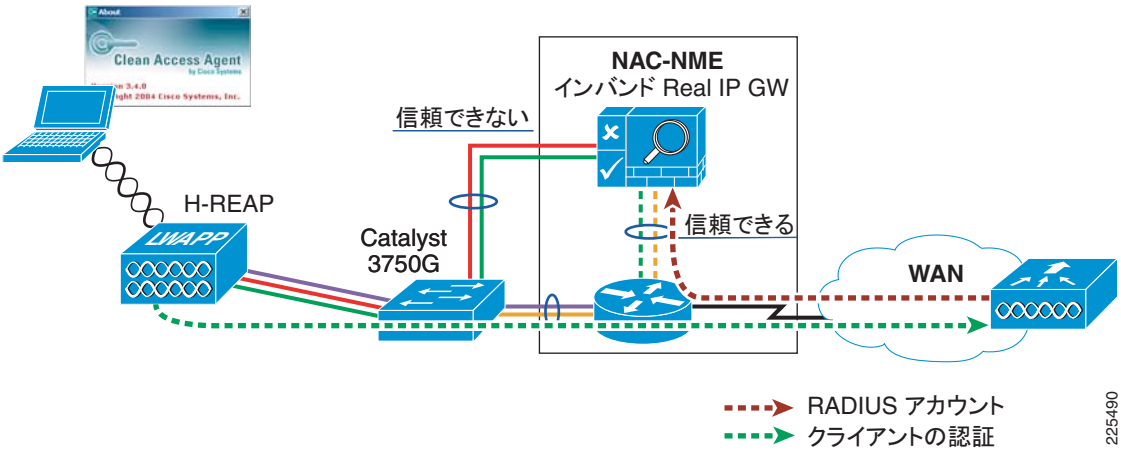


H-REAP と NAC-NME

Cisco Unified Wireless Network ブランチ展開のもう 1 つのオプションは、H-REAP を使用することです。この場合、WLC が H-REAP 管理を提供しますが、図 5-91 に示すように、WLAN クライアント トラフィックは H-REAP インターフェイスで終端できます。H-REAP の dot1q トランクは、ブランチ スイッチ上で終端できます。これらの VLAN は、NAC-NME の Untrusted インターフェイスにマップできます。これにより、H-REAP クライアント トラフィックのパスは WLC 2106 と同一になります。

このモードの H-REAP を使用する場合、ローカル ブランチの NAC アプライアンスと中央の WLC 認証 SSO VPN という構成はお勧めしません。異なるブランチ ロケーションにある複数の H-REAP を管理する中央の WLC は、RADIUS アカウンティング メッセージの送信先となる適切な NAC-NME を特定するメカニズムを備えていないためです。たとえば、複数のブランチが存在し、いずれも H-REAP と NAC-NME を導入している場合、中央の WLC には、通常、異なるブランチのすべての H-REAP に対して同一の WLAN が設定され、RADIUS 認証は中央の WLC によって実行されます。NAC-NME が複数存在している場合も、中央の WLC の WLAN 設定では、すべての WLAN クライアントに対して 1 つの優先 RADIUS アカウンティング アドレスしか保持されていません。

図 5-91　H-REAP と NAC-NME



CHAPTER 6

Secure Wireless ファイアウォールの統合

今日の企業では、ネットワーク アクセスを必要とするさまざまなタイプの従業員が存在し、数多くの手段によってネットワークへのアクセスを差別化しています。Cisco Unified Wireless ソリューションは、複数の Service Set Identifier（SSID; サービス セット識別子）、ユーザまたは ID ベースの Virtual LAN（VLAN; バーチャル LAN）、ユーザまたは ID ベースの Quality Of Service（QoS）割り当て、ゲスト アクセス サービス、および WLC フィルタリング機能を実装することにより、このニーズに直接応えます。他のシスコ製品を次のような方法で Cisco Unified Wireless ソリューションに統合することにより、必要に応じてアクセスをさらにカスタマイズできます。

- ステートフルなパケット検査が必要となる場合は、ファイアウォールに加えて、Wireless LAN Controller（WLC; 無線 LAN コントローラ）上で使用可能なフィルタ、およびアップストリームのルータ Access Control List（ACL; アクセス コントロール リスト）を使用できます。
- ポスチャ評価が必須となる場合は、ソリューションに NAC アプライアンスを追加する必要があります。
- WLAN クライアントが別の IT 部門（パートナーおよび請負業者のクライアント）によって管理される場合は、ソリューションにゲスト アクセスを追加できます。

ファイアウォールの役割

ファイアウォールは、長期にわたって、ネットワークのセキュリティ インフラストラクチャにおける最初の防衛線となっています。ファイアウォールは、アクセス試行および接続が行われるたびに、ユーザのネットワーク アクセス権に関する企業ポリシーを接続情報と比較することでこれを達成しています。ユーザ ポリシーと接続情報は一致している必要があり、一致しない場合、ファイアウォールはネットワーク リソースへのアクセスを許可しません。これにより、不正な侵入を防止します。

近年では、ファイアウォールの展開先として、企業のプライベート ネットワークが公共のインターネットと接する従来のネットワーク境界だけでなく、ブランチ オフィス ネットワークの WAN エッジのほか、企業内の重要なロケーションでは企業ネットワーク全体も対象にすることがベスト プラクティスとして広まってきています。この分散型のファイアウォール戦略は、内部の脅威からの保護に役立ちます。このような脅威は、Computer Security Institute（CSI）が実施している年次調査によると、サイバー損失において以前から大きな割合を占めています。

内部の脅威の増大をもたらしているのは、企業 LAN の内部で新たに形成されたネットワーク境界です。これらの境界（信頼境界）の例としては、スイッチとバックエンド サーバの間、さまざまな部署の間、無線 LAN が有線ネットワークと接する地点などがあります。ファイアウォールは、これらの重要なネットワーク合流点でのアクセス侵犯を防止します。たとえば、営業担当者がコミッション追跡経理システムにアクセスできないようにします。

ファイアウォールを複数のネットワーク セグメントに配置することは、企業および業界の統制に関する最新法令に企業が準拠する上でも役立ちます。Sarbanes-Oxley Act（SOX 法 ; サーベンス - オクスリー法）、Gramm-Leach-Bliley Act（GLB Act; グラム - リーチ - ブライリー法）、Health Insurance Portability and Accountability Act（HIPAA; 医療保険の相互運用性と説明責任に関する法律）、Payment Card Industry (PCI) Data Security Standard（PCI DSS; 決済カード業界データセキュリティ基準）には、情報セキュリティの監査と追跡に関する要件が含まれています。

ファイアウォールは、約 10 年前に広く普及して以来、企業ネットワーク内の展開箇所が増加しているほか、機能もさらに洗練されています。アプリケーションやプロトコルの検査など、不正防止のための機能が追加されており、オペレーティング システムおよびアプリケーションの脆弱性を利用した不正使用の阻止を支援します。

ファイアウォールは、アプリケーション検査の機能など、追加の不正防止機能によって強化されています。この検査機能は、アプリケーションのタイプを調査、識別、および検証する機能のほか、単純な接続情報を超える各種の項目を基準として、詳細なポリシーに従ってトラフィックを処理する機能を提供します。これは、オープンなポートを使用してネットワークに不正にアクセスしようとするトラフィックやユーザを識別し、ブロックする場合に役立ちます。

たとえば、Web データや Web サービスの転送には HTTP が使用されています。現在ではネットワーク トラフィックの約 75 % を占めており、通常はアプリケーション ポート 80 を使用します。ほとんどのファイアウォールでは、ポート 80 は常に開放されているため、ポート 80 を宛先とするトラフィックはすべて許可されます。ハッカー、ワーム、およびウイルスは、このピンホールを使用して Web アプリケーションを攻撃し、可能であれば機密データへのアクセスを取得しようとします。

この行為からシステムを保護するには、アプリケーション フィルタリングによって詳細なパケット検査を実行し、どの HTTP アプリケーション トラフィックがネットワークに進入しようとしているかを正確に特定します。ネットワークへの進入を許可する必要のある HTTP アプリケーションも数多く存在しますが、ブロックすることが望ましいものも存在します。アプリケーション ファイアウォールは、この場合も詳細なパケット検査を使用して、アプリケーション プロトコル（ここでは HTTP）が標準以外の方法で動作していないかどうかを特定します。

たとえば、ポリシーを設定することで、異常に長い HTTP ヘッダーや、バイナリ データを含むヘッダーを識別してブロックできます。このようなヘッダーは、攻撃である可能性があります。管理者は、サーバに対する 1 分間あたりの要求を一定数に制限するポリシーを設定することにより、Denial of Service（DoS; サービス拒絶）攻撃を回避できます。

ファイアウォールは、IP フラグメント、セッション レイヤ、およびアプリケーションの弱点を利用した攻撃から保護できるため、単純な ACL よりも強力な保護機能を提供します。シスコのステートフル ファイアウォール技術では、選択されたプロトコルの上位レイヤの動作を分析することにより、攻撃者がそのレイヤを攻撃できないようにし、単純なファイアウォールを上回る保護を実現します。効率的なものにするには、使用されるアドレスおよびプロトコルを固定し、明確に定義する必要があります。このようにしない場合、ファイアウォール ポリシーの範囲が広すぎて非効率になります。つまり、効率的でセキュアなものにするには、膨大な量の追加、移動、および変更が必要になります。このため、企業通信が明確に定義されている企業インターネット エッジにはファイアウォールが展開され、一方、プロトコルとピアの関係があまり明確に定義されていない企業ネットワーク自体の内部にはファイアウォールが展開されないのが一般的です。

企業の WLAN 展開では、多くの場合、WLAN クライアント接続は有線クライアント接続よりもセキュリティが強化されていますが、企業の WLAN 展開にはファイアウォールを含めることをお勧めします。理由のいくつかを次に示します。

- 目標となるのは、特定のアプリケーションに対するすべてのクライアント アクセスにファイアウォールを適用することであり、WLAN は、単にこのポリシーの適用対象となる最初の地点に過ぎません。
- 企業内で使用される複数の WLAN では、部署の区分、従業員のタイプ、またはビジネス パートナーからの要望に対応するため、さまざまなセキュリティ レベルが必要です。
- 法令に従うには、ネットワークをファイアウォールで保護する必要があります。一般には、法令でテクノロジーが指定されることはありませんが、法令の要件に基づいたセキュリティ ポリシーによっては、ファイアウォールの使用が必須となる場合があります。

アクセス エッジ ファイアウォールの代替手段

多くの企業では、ネットワークのセグメンテーションが WLAN のセキュリティ目標の 1 つとなります。セグメンテーションが必要となる場合に、セグメンテーション目標を達成するための柔軟な手段を提供するのは ACL です。企業は、セキュリティに関する投資を他の領域に向けることができます。

（注）　ACL とファイアウォールのどちらを採用するかは、セグメンテーションの対象となるユーザ集団について脅威を見積もることで決まります。たとえば、企業ネットワークをインターネットから分離する場合はファイアウォールが必要ですが、部署 1A を部署 2C から分離するときは不要な場合があります。

ほとんどの企業ネットワークでは、その性質上、ネットワーク アドレス（宛先）およびプロトコルについて、アクセスを許可するクライアントと許可しないクライアントを決定することは非常に困難です。したがって、ファイアウォールはアプリケーション サーバの近辺に配置することをお勧めします。これらのサーバでは、アプリケーション用および管理用のプロトコルとアドレスが、アクセス エッジの場合よりも明確に定義されています。データセンターでのファイアウォール展開に関するガイダンスについては、次の URL を参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns376/c649/ccmigration_09186a008078de90.pdf

ウイルスおよびワームからの保護

ウイルスやワームの攻撃を受ける可能性がある場合、ファイアウォールでは限定的な保護機能しか提供できません。ファイアウォールは、通常、多くの攻撃によって不正利用されているアプリケーションの弱点を認識できず、防御できるのがプロトコル攻撃に限られるためです。クライアント ウイルスやワームに対処する場合に、最も一般的な戦略を表す言葉は「信頼するが、検証および監視する」というものです。この戦略では、クライアント デバイスはネットワークへのアクセス権を付与されますが、アクセス権が付与される前に、クライアントのオペレーティング システムおよび保護ソフトウェアのステータスが検証されます。クライアントの動作は監視され、疑わしい動作が識別されます。

たとえば、企業の WLAN クライアントが認証を受けてネットワークへのアクセス権を取得し、クライアントからネットワークへの接続は攻撃から保護されているとします。この場合に必要となるのは、WLAN クライアントがウイルスまたはワームをホストしていないこと、および WLAN クライアントが不適切に動作していないことを保証するタスクです。これらのタスクは、Network Admission Control（NAC; ネットワーク アドミッション制御）および Intrusion Prevention System（IPS; 侵入防御システム）を使用して実行できます。これには、アンチウイルス ソフトウェアの最新バージョンがインストールされていること、パッチ レベルが最新状態に維持されていることを保証する CSA などのホストベース IPS システムが含まれます。

Cisco NAC アプライアンスは、認証およびポリシー適用を実行するほか、クライアント ソフトウェアのポスチャ評価を実行することにより、クライアントが適切なレベルのソフトウェアおよびパッチを実行していることを保証し、必要に応じて修復手順をクライアントに案内します。

IPS は、クライアントの動作を監視して、疑わしい動作がある場合はアラームおよびアラートを送信し、サービスへのアクセスをブロックし、クライアントのネットワーク アクセスをブロックして対処できます。

ゲスト アクセス ポリシーの適用

アクセス エッジでファイアウォールを適用してゲスト アクセスを制御する方法では、効果は限定的です。ファイアウォールの主な動作は、内部 IP アドレスへのアクセスをブロックする単純なアクセス リストとなるためです。企業ネットワークを越えてインターネット エッジに転送されるゲスト クライアント トラフィックについては、ファイアウォールは対処しません。より効果的なソリューションは、専用のゲスト アクセス WLAN またはサービスを実装することです。この機能は、Cisco Unified Wireless ソリューションでネイティブにサポートされています。

詳細については、『*Enterprise Mobility 4.1 Design Guide*』の第 12 章を参照してください。このマニュアルは、
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html
で入手できます。

ACL をアクセス レイヤに配置し、ファイアウォールをインターネット エッジに配置することで、ゲスト アクセス展開であっても ACL およびファイアウォールは優れたコンポーネントになります。

ファイアウォールの統合

シスコのさまざまな WLC およびファイアウォール製品を使用すると、数多くの WLC とファイアウォールの組み合せが可能になります。この章では、次の 3 つのファイアウォール統合の例を中心に説明します。

- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）と Cisco Firewall Services Module（FWSM）の統合
- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）と Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の統合
- 210X WLC と ISR ルータの Cisco IOS Firewall の統合

ただし、この章で示す設計原則および設定例は、他の製品の設定にも適用できます。

シスコのセキュリティ製品の詳細については、
http://www.cisco.com/en/US/products/hw/vpndevc/index.html を参照してください。

このガイドで使用されている FWSM ソフトウェアは、バージョン 3.1(4) です。ADSM のバージョンは 5.0(2)F です。

FWSM、ASA、および IOS Firewall

シスコの FWSM および ASA は、業界最高水準の 1 秒あたり接続数、スループット、およびモジュールまたはアプライアンスごとの同時接続数を実現しています。静的な VLAN 設定または Cisco IOS ソフトウェアのポリシーベース ルーティングを使用して、トラフィックを複数の FWSM または ASA に転送することにより、これらの FWSM または ASA をクラスタ化できます。同一のシャーシに FWSM を 4 つまで展開し、合計で 20 Gbps のスループットを得ることができます。お客様のキャパシティ要件に合せて、さまざまな ASA アプライアンスを使用できます。これらのアプライアンスは、150Mpbs ～ 5Gbps の範囲のファイアウォール スループットを提供します。

単一の FWSM では、最大で 1,000（コンテキストごとに 256）の仮想インターフェイスをサポートできます。単一のシャーシを最大 4,000 の VLAN にまで拡張できます。また、Cisco Catalyst 6500 シリーズのシャーシで 2 つの Cisco Application Control Engine（ACE; アプリケーション制御エンジン）を使用することにより、3 つの FWSM で 15 Gbps を超えるファイアウォール スループットをロード バランスできます。スイッチ バックプレーンに完全なファイアウォール保護を適用する一方で、遅延は最小限の値に抑えます（小さなフレームの場合は 30 ms）。シスコの FWSM は、高いパフォーマンスを提供しながら、汎用 CPU の持つ柔軟性も備えた高速なネットワーク プロセッサを基盤としています。

FWSM の詳細については、
http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_book09186a0080579a1e.html を参照してください。

使用可能な各種の ASA モデルの詳細については、http://www.cisco.com/en/US/partner/products/ps6120/prod_models_comparison.html を参照してください。

Cisco IOS Firewall は IOS 統合型のソリューションであり、ネットワーク レイヤおよびアプリケーション レイヤに対する攻撃、ウイルス、およびワームからネットワーク インフラストラクチャを保護することで、ネットワークのアベイラビリティと企業リソースのセキュリティの確保を支援します。また、Session Initiation Protocol（SIP）エンドポイントおよびコール制御リソースを保護することにより、統合通信を保護します。Cisco IOS Firewall は、共通基準（EAL4）の認定を取得したステートフルなファイアウォール ソリューションです。Cisco IOS Firewall は、ブランチ オフィス、中小規模の企業環境、およびマネージド サービスに適しており、ネットワーク上のアプリケーション トラフィックを効率的に制御します。Cisco Integrated Threat Control フレームワークの基本部分であり、Cisco IOS Intrusion Prevention System（IPS）、IOS Content Filtering、および IOS Network Address Translation（NAT）を含む他の Cisco IOS セキュリティ機能と連携して、ブランチ オフィス境界のための完全に統合されたセキュリティ ソリューションを構築します。

このマニュアルのいくつかの設定例を考察する前に、ファイアウォール ソリューションの特性について考慮する必要があります。FWSM および ASA では、アーキテクチャとファイアウォール設定オプションが互いに非常によく似ており、一括して説明できます。IOS Firewall のアーキテクチャと設定オプションはこれらと異なるため、この章の以降の個別の項で説明します。

FWSM および ASA の動作モード

次に、考慮する必要のある FWSM および ASA の動作モードを示します。

- ルーテッド モードとトランスペアレント モード
- シングル コンテキスト モードとマルチ コンテキスト モード

ルーテッドとトランスペアレント

ファイアウォールは、ルーテッドまたはトランスペアレントのいずれかのモードで動作できます。ルーテッド モードの場合、ファイアウォールは、トラフィック、トラフィック フローを制御するためのルート設定に加えて、ファイアウォール上に設定されているポリシーのレイヤ 3 インターフェイスとして機能します（図 6-1 および図 6-2 を参照）。

図 6-1 FWSM のルーテッド モード

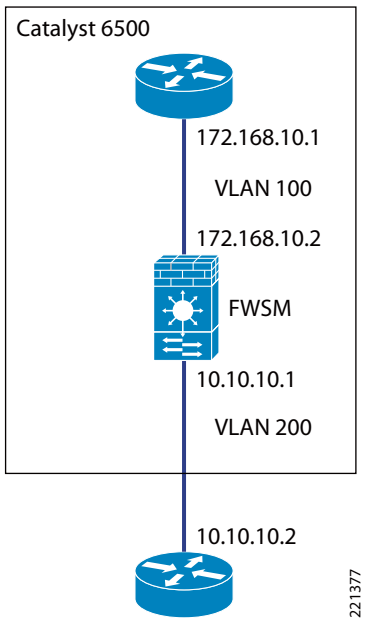
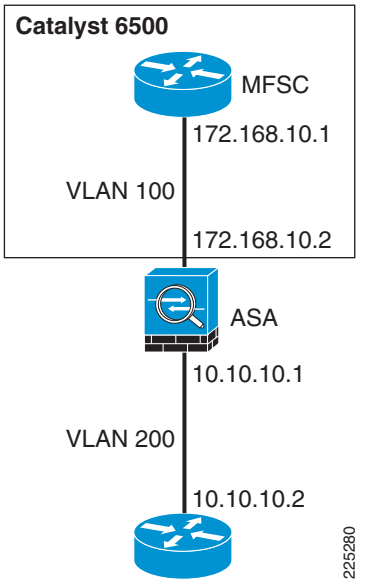


図 6-2 ASA のルーテッド モード



トランスペアレント モードの場合、ファイアウォールは「bump-in-the-wire」として機能し、レイヤ 2 でポリシーを適用します。ファイアウォールの内側と外側は、同一のサブネットにあります（図 6-3 および図 6-4 を参照）。

図 6-3　FWSM のトランスペアレント モード

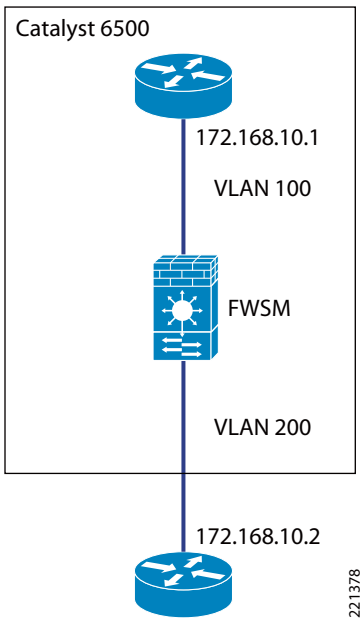
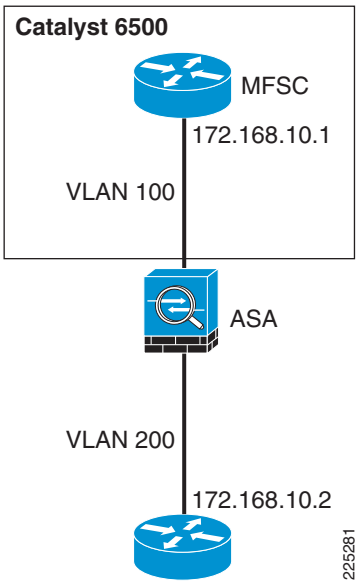


図 6-4　ASA のトランスペアレント モード



この章の例では、ルータをトランスペアレント モードで使用しています。このモードでは、WLAN のアドレス方式を変更したり、ルーティング方式に追加したりせずにファイアウォール機能を挿入できるためです。ファイアウォールのモードの詳細については、http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/intro.html#wp1047294 を参照してください。

シングル コンテキストとマルチ コンテキスト

FWSM または ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスに分割できます。各コンテキストは、それぞれ独自のセキュリティ ポリシー、インターフェイス、および管理者を保持します。マルチ コンテキストは、スタンドアロンのデバイスが複数ある状態と似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、管理機能を含むほとんどの機能がサポートされます。ダイナミック ルーティング プロトコルなど、一部の機能はサポートされません。

マルチ コンテキスト モードでは、FWSM または ASA はコンテキストごとに設定を保持します。この設定では、スタンドアロン デバイスに対して設定可能なセキュリティ ポリシー、インターフェイス、およびほぼすべてのオプションが指定されています。

システム管理者は、システム コンフィギュレーションでコンテキストを設定することによって、コンテキストを追加または管理します。このコンフィギュレーションは、シングル モード設定の場合と同様に、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、FWSM または ASA の基本的な設定値を指定したものです。システム コンフィギュレーションには、システム自体のネットワーク インターフェイスおよびネットワークの設定値は含まれていません。システムがネットワーク リソースにアクセスする必要がある場合（サーバから設定をダウンロードするなど）、システムは「admin」コンテキストとして指定されたいずれかのコンテキストを使用します。

ダイナミック ルーティングおよびマルチキャストが不要な場合は、複数の仮想デバイスを設定することにより、数多くの利点があります。次に、このガイドで使用されている例での主な利点を示します。

- FWSM または ASA 間でのロード シェアリングをサポートし、提案されている WLAN トポロジに沿ったアクティブ / アクティブ フェールオーバー モデルのサポート。
- 複数のファイアウォール ポリシーの個別管理のサポート。この機能は、部署別の WLAN ファイアウォール ポリシーを実装している場合は必須となることがあります。
- 大きなキャパシティのサポート。シングル コンテキスト モードの場合、サポートされる VLAN ペアは 8 つのみです。このマニュアルで言及しているファイアウォール /WLAN トポロジの例では十分なものですが、マルチ コンテキスト モードにすると、コンテキストごとに 8 つの VLAN がサポートされます。

シングル コンテキストとマルチ コンテキストの機能の違いの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg.html

基本的なトポロジ

図 6-5 および図 6-6 に、ファイアウォール /WLAN トポロジの例で使用されている基本的なモジュール設定を示します。FWSM または ASA はトランスペアレント モードに設定され、WiSM クライアント VLAN と 6500 Multi-Feature Switch Card（MFSC）のルーティング エンジンの間でファイアウォールが適用されます。このため、WLAN クライアント トラフィックがサブネットのデフォルト ゲートウェイに到達するには、FWSM または ASA を経由する必要があります。

この例では、WLAN ごとに 2 つの VLAN が定義されています。WiSM から FWSM または ASA までの 15x VLAN、および FWSM と MFSC の間の 5x VLAN です。これらの VLAN が存在するため、WLAN クライアントのトラフィックは、デフォルト ゲートウェイに到達するまでに必ず FWSM を経由します。

ASA と FWSM の設定上の主な違いは、単に、ASA が 6500 スイッチ バックプレーンに直接接続されないこと、信頼できる VLAN と信頼できない VLAN がスイッチ ポートに割り当てられる必要があること、これらのポートが ASA にケーブル接続されることです。

図 6-5　FWSM の基本設定

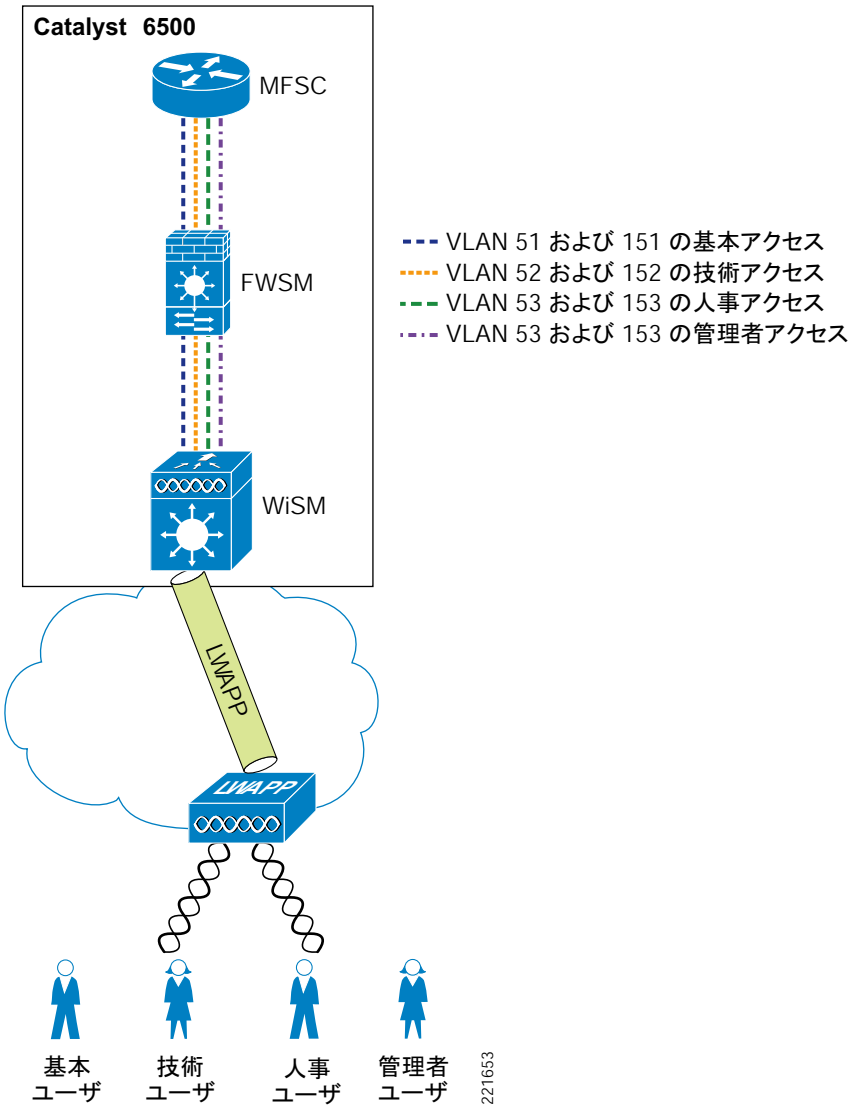
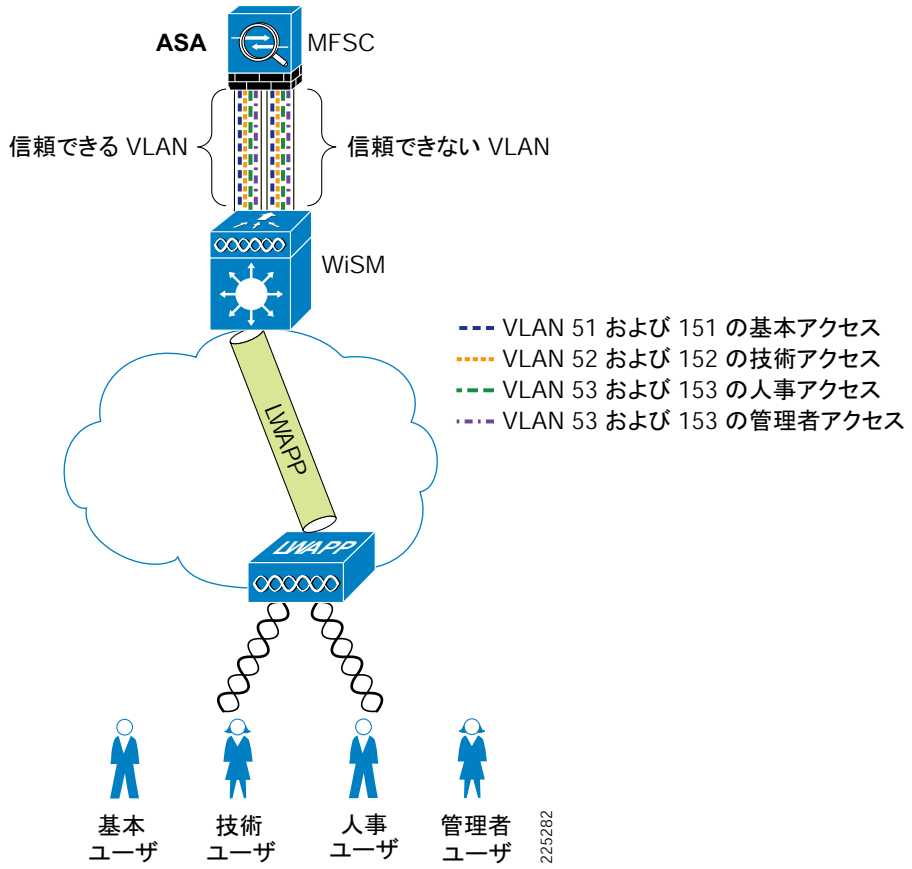


図 6-6　ASA の基本設定



シナリオの例

部署の分割

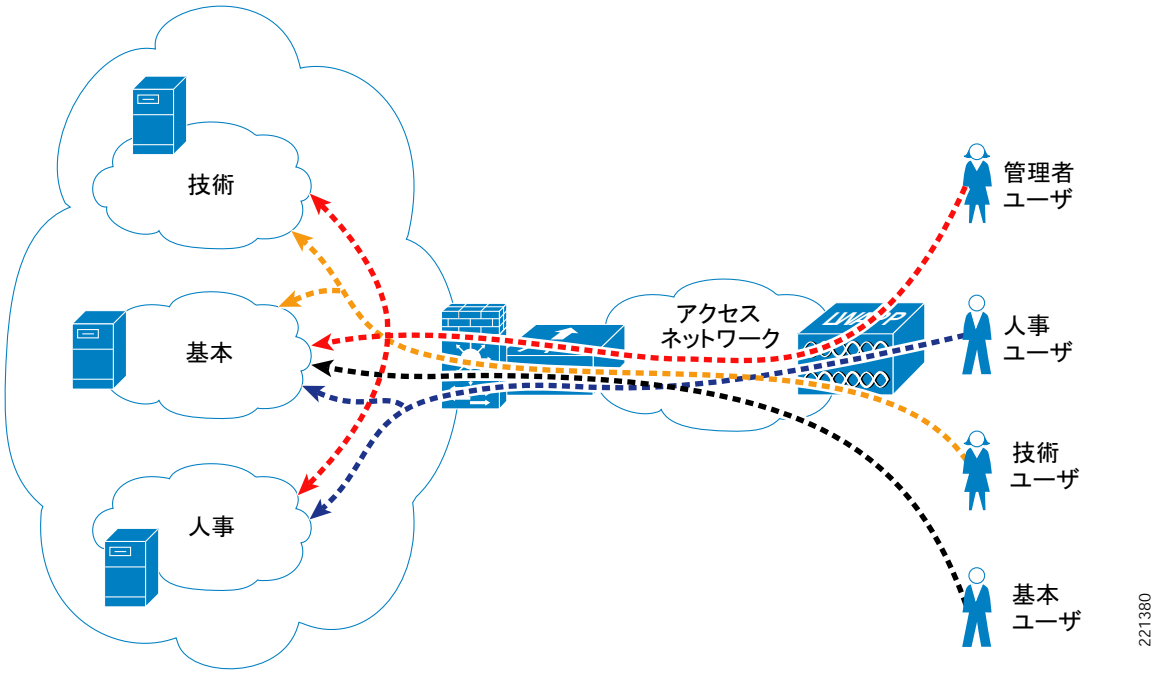
このシナリオでは、企業はアプリケーションへのアクセスを部署のメンバシップに基づいて制御します。この例では、次の 4 つのアクセス レベル シナリオについて説明します。

1. 基本レベル アクセス
   - E メールへのアクセス：SMTP、POP
   - イントラネットへのアクセス：HTTP および HTTPS
2. 人事（HR）アクセス
   - 基本レベル アクセス
   - HR サーバへのアクセス：HTTPS
3. 技術アクセス
   - 基本レベル アクセス
   - 技術サーバへのアクセス
4. 管理者アクセス
   - 無制限アクセス

（注）　通常の企業では、さらに複雑なポリシーが必要になる場合もありますが、このガイドの目的は、ファイアウォール ポリシーの設定ではなく Cisco Secure Wireless の機能を例示することです。たとえば、Microsoft Active Directory などの Network Operating System（NOS; ネットワーク オペレーティング システム）をサポートして、ドメイン認証、ファイル転送、および印刷を実行できるようにするには、ポリシーの作成が必要になる場合があります。

1 つの共通 WLAN SSID が使用され、VLAN はユーザ ID とグループ メンバシップに基づいて割り当てられます。この方法は、グループごとに異なる SSID を使用する方法よりも優れています。これは、クライアントのグループ メンバシップを変更する場合、およびグループの追加と削減を行う場合に、クライアントに対する変更が不要なためです。図 6-7 に、さまざまなユーザが WLAN インフラストラクチャを共有する一方で、ネットワーク アドレス、ネットワーク リソース、およびプロトコルへのアクセスが各自のロールのみに基づいて許可される場合の概念を示します。

図 6-7　　ユーザのネットワーク トラフィック アクセス



WLAN ユーザのアクセスは、次の手順になります。

1. WLAN クライアントが、共通の WLAN SSID とのアソシエーションを確立します。
2. 標準の 802.1X 認証メカニズムを通じて、ユーザが EAP を使用して AAA サーバとの認証を完了します。
3. AAA サーバによって送信される EAP 成功メッセージの一部として、ユーザのグループ メンバシップに基づいた VLAN メンバシップ情報が WLC に転送されます。
4. WLC は、この WLAN クライアント接続を AAA サーバの指定した VLAN にマップします。
5. WLAN クライアントが送受信するトラフィックに対して、各自のグループに関連付けられている FWSM ポリシーが適用されます。

ACS RADIUS の設定

ACS サーバは、認証が完了したユーザのグループ メンバシップに基づいて、追加の情報を RADIUS プロトコルを使用して RADIUS クライアントに送信します。ACS でのグループ メンバシップは、ACS サーバ内のローカル設定をもとにすることも、ユーザの外部認証データベースに保持されているメンバシップ基準をもとにすることもできます。説明を簡潔にするため、この例では、次のユーザ タイプのユーザ グループ メンバシップには ACS のローカル グループ設定情報を使用しています。

- Userbasic
- UserEng
- UserHR
- UserAdmin

割り当てられる ACS グループは、次のとおりです。

- BasicUser

- EngUser
- HRUser
- AdminUser

図 6-8 に、各ユーザの VLAN 割り当てなど、この設定に関連するグループ設定の例を示します。これらの割り当ては、グループの IETF RADIUS オプションの一部です。図 6-8 に示した例は、*BasicUser* グループのものです。*Tunnel Type* および *Tunnel Medium Type* は、VLAN 情報が渡されることを定義します。*Tunnel-Private-Group-ID* は VLAN 番号を渡します。*BasicUser*、*EngUser*、*HRUser*、および *AdminUser* グループの VLAN 割り当ては、それぞれ 151、152、153、および 154 です。

（注）　これらの IETF オプションはデフォルトでは含まれていないため、ACS の Interface Configuration メニューを使用して追加する必要があります。

図 6-8　　グループの VLAN の設定

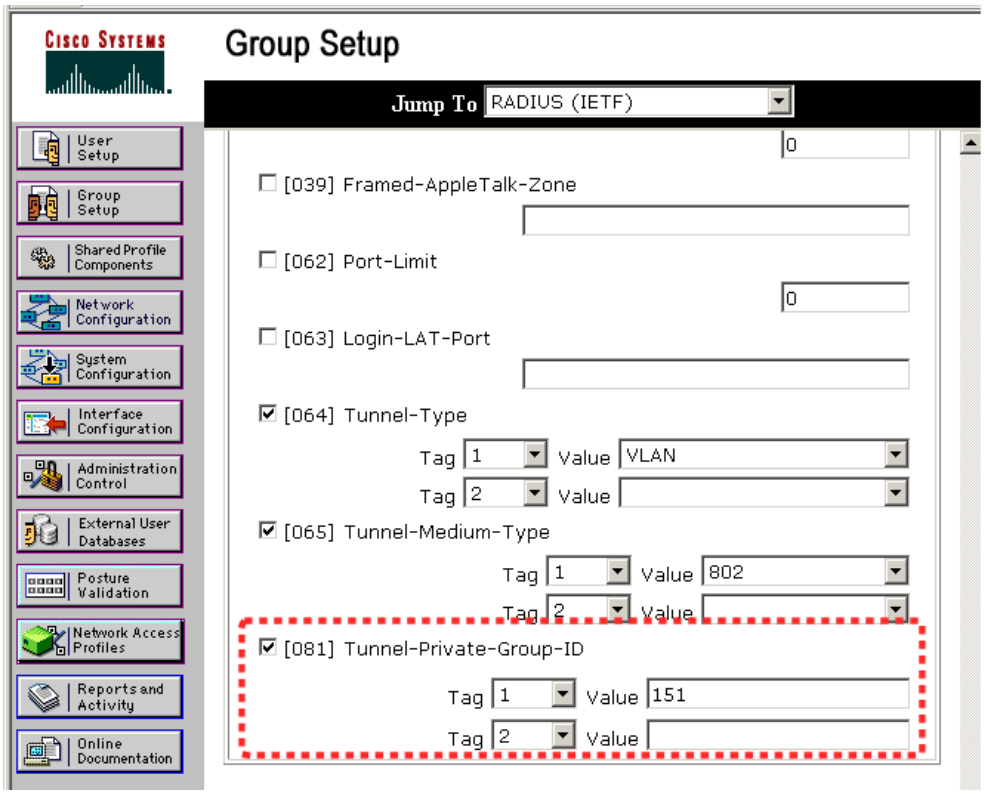
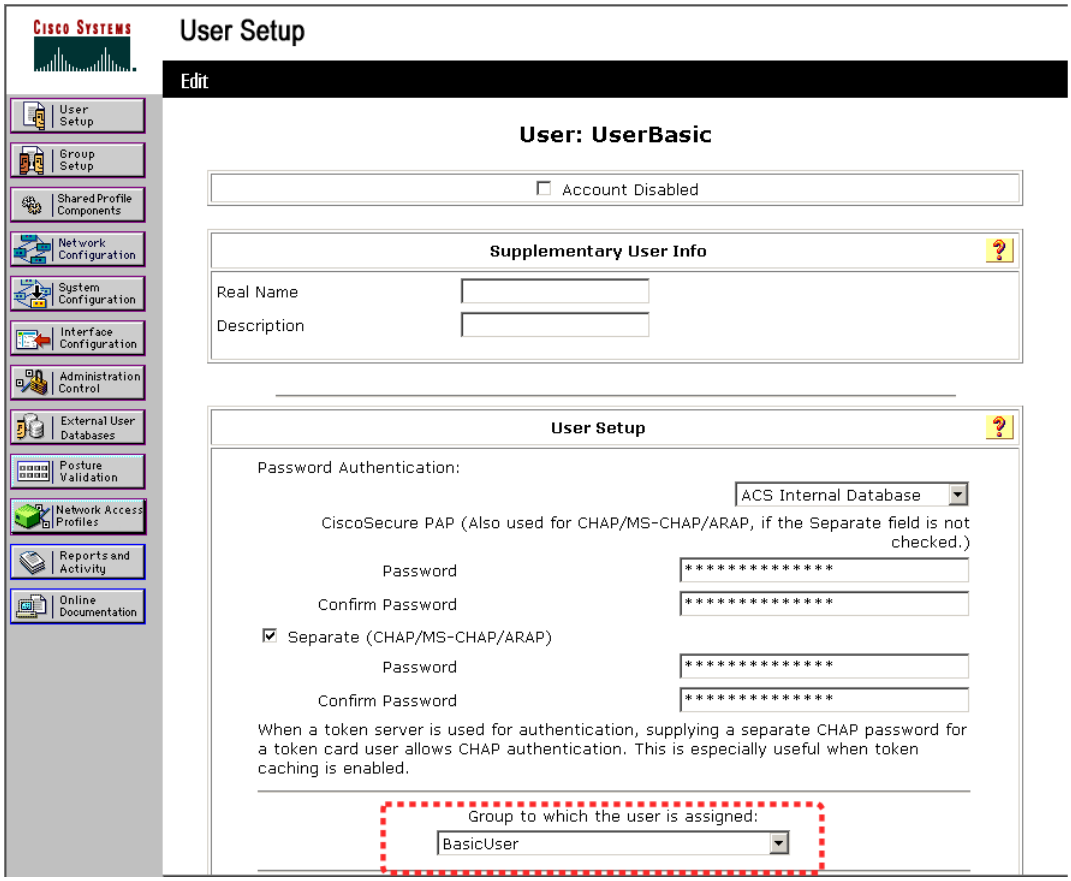


図 6-9 に、ACS で行ったユーザからグループへのマッピングの例を示します。ユーザ *UserBasic* が *BasicUser* グループにマップされています。

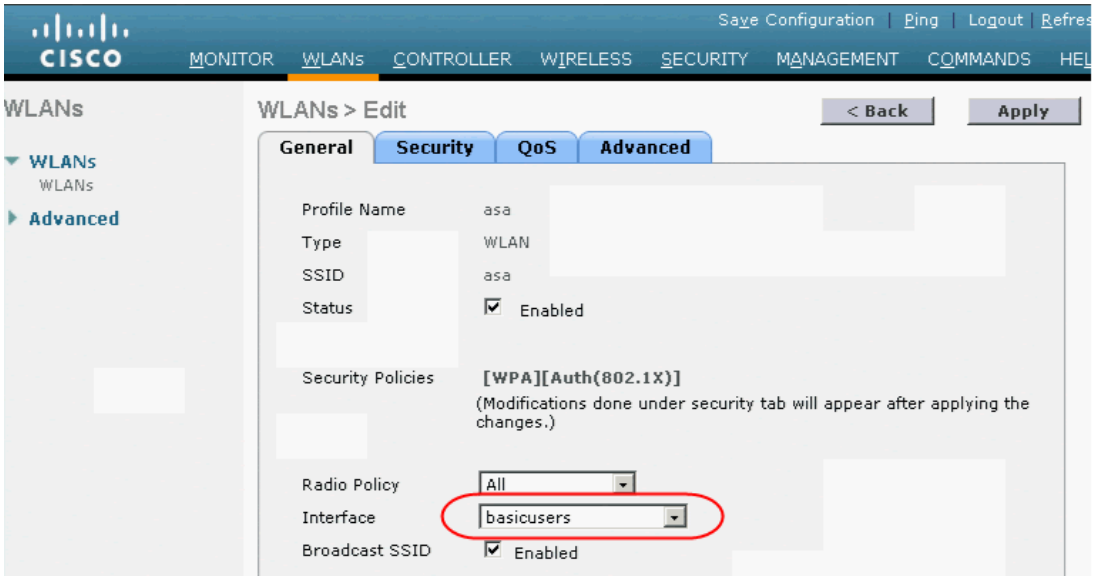
図 6-9　　ユーザのグループの設定



WLC の設定

この例の主な WLC 詳細設定は、WLAN の設定および WLC インターフェイスの設定です。図 6-10 に、WLAN の設定の例を示します。802.1X 認証を WLAN セキュリティの基盤にして、VLAN マッピング情報を転送できるようにしているほか、最も重要な詳細設定は、WLAN のマップ先となる WLC インターフェイスです。

図 6-10　WLC の WLAN の設定



この例でのマッピング先は、FWSM 経由でのアクセス レベルが最も低い *basicusers* インターフェイスです。RADIUS の accept パケットで送信される VLAN 情報が、WLC 上の対応する動的インターフェイスと一致していない場合、WLAN クライアントの接続先は、WLAN の設定で指定されている（デフォルトの）インターフェイスになります。WLAN の VLAN マッピングを AAA サーバが変更できるようにするには、図 6-11 に示すように、その WLAN について AAA オーバーライドを設定する必要があります。

図 6-11　AAA オーバーライド

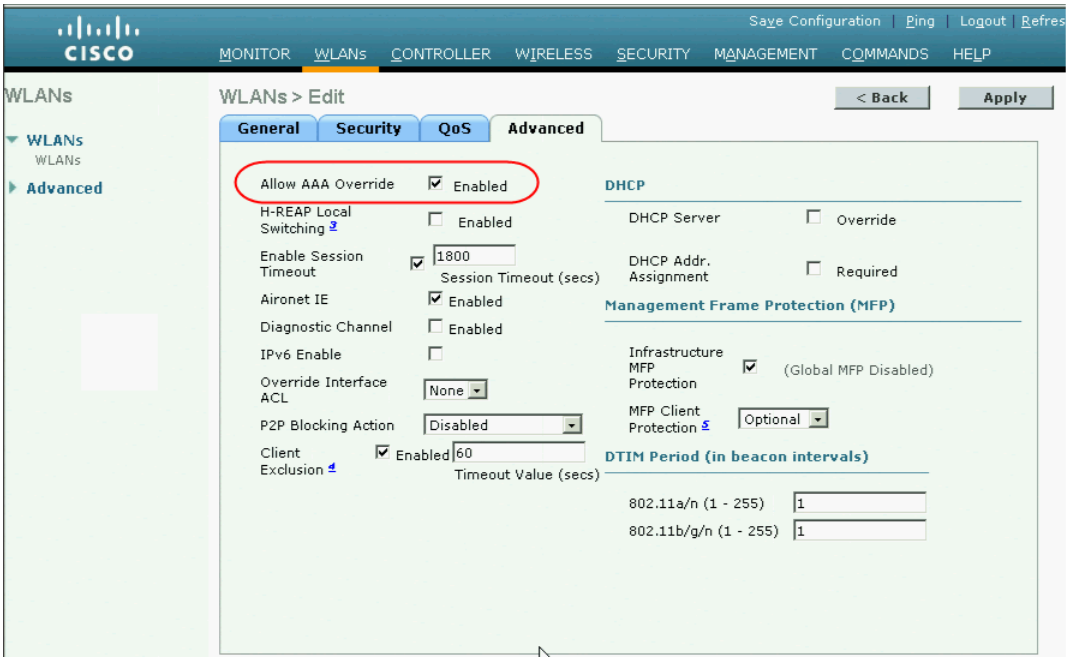
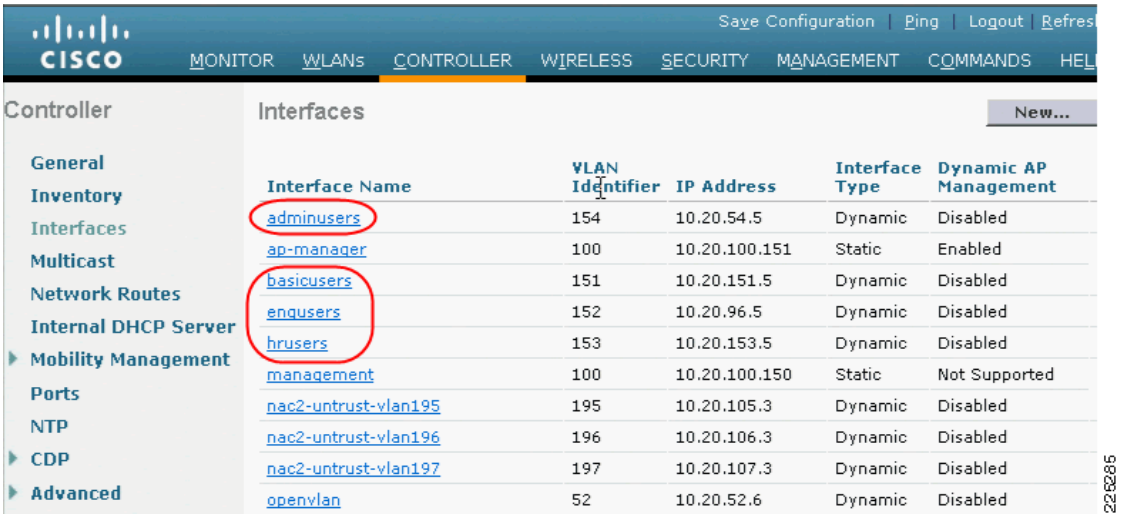


図 6-12 に、使用可能な各 FWSM VLAN が動的インターフェイスとして定義されている WLC インターフェイス設定を示します。ただし、図 6-10 の WLAN 設定で *basicuser* がデフォルト インターフェイスとして選択されていることに注意してください。インターフェイス *adminusers*、*engusers*、および *hrusers* は WLAN に関連付けられておらず、使用されるのは、正常な 802.1X/EAP 認証の一部として VLAN アトリビュートが渡されるときに限られます。

図 6-12　　WLC インターフェイスの設定



FWSM または ASA の設定

ASA および FWSM のファイアウォール設定の構文は、ファイアウォール ポリシーを実装する場合、基本的には同一であり、主な違いは 6500 への接続です。ASA は、6500 バックプレーンに接続する FWSM で使用される VLAN インターフェイスではなく、スイッチ モジュールに接続されている物理インターフェイスを使用します。設定上の違いがある場合は、それらについて指摘します。同様に、設定が共通する場合も指摘しています。FWSM を設定する前に、6500 上で必須となる設定があります。

次の設定例は、FWSM または ASA の展開をサポートするために必要となる 6500 の VLAN 設定を示しています。VLAN 50 は、FWSM の管理インターフェイスとして使用されます。VLAN 51 ～ 54 は、各種のユーザ グループ用の信頼できる VLAN、VLAN 151 ～ 154 は信頼できない VLAN です。IP アドレスを使用してインターフェイスが設定されているのは、VLAN 50 ～ 54 のみであることに注意してください。

VLAN 55 と 56 は、2 つの FWSM または ASA をハイ アベイラビリティ設定で展開する、以降の設計例で使用されます。

VLAN 57 と VLAN 58 は、FWSM または ASA のセキュリティ コンテキストの個別管理インターフェイス用に定義されています。

```
vlan 50
 name FWSM-admin
!
vlan 51
 name FWSM-Trusted-BasicGroup
!
vlan 52
 name FWSM-Trusted-EngGroup
!
vlan 53
 name FWSM-Trusted-HRGroup
!
vlan 54
 name FWSM-Trusted-AdminGroup
!
vlan 55
 name Failover-VLAN
!
vlan 56
 name State-VLAN
!
vlan 57
 name FWSM-EngineeringContext-admin
!
vlan 58
 name FWSM-StaffContext-admin
!
vlan 151
 name FWSM-Untrusted-BasicGroup
!
vlan 152
 name FWSM-Untrusted-EngGroup
!
vlan 153
 name FWSM-Untrusted-HRGroup
!
vlan 154
 name FWSM-Untrusted-AdminGroup
!
!
interface Vlan50
```

```
 description FWSM Admin
 ip address 10.20.50.2 255.255.255.0
 standby 121 ip 10.20.50.1
 standby 121 preempt
!
interface Vlan51
 description BasicUsers
 ip address 10.20.51.2 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.51.1
 standby 121 preempt
!
interface Vlan52
 description EngUsers
 ip address 10.20.52.2 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.52.1
!
interface Vlan53
 description HRUsers
 ip address 10.20.53.2 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.53.1
 standby 121 preempt
!
interface Vlan54
 description AdminUsers
 ip address 10.20.54.2 255.255.255.0
 ip helper-address 10.20.30.11
 standby 121 ip 10.20.54.1
 standby 121 preempt
!
interface Vlan57
 description EngineeringContext Admin
 ip address 10.20.57.2 255.255.255.0
 standby 121 ip 10.20.57.1
 standby 121 preempt
!
interface Vlan58
 description StaffContext Admin
 ip address 10.20.58.2 255.255.255.0
 standby 121 ip 10.20.58.1
 standby 121 preempt
```

次の設定例は、FWSM で使用されるインターフェイスを指定するための 6500 の設定コマンドを示しています。FWSM にマップされるルーティング可能インターフェイスの数に基づいて、**firewall multiple-vlan-interfaces** は必須となることに注意してください。

（注） ASA については、6500 固有の設定コマンドは必要ありません。

```
firewall multiple-vlan-interfaces
firewall module 2 vlan-group 50
firewall vlan-group 50  50-58,150-155
```

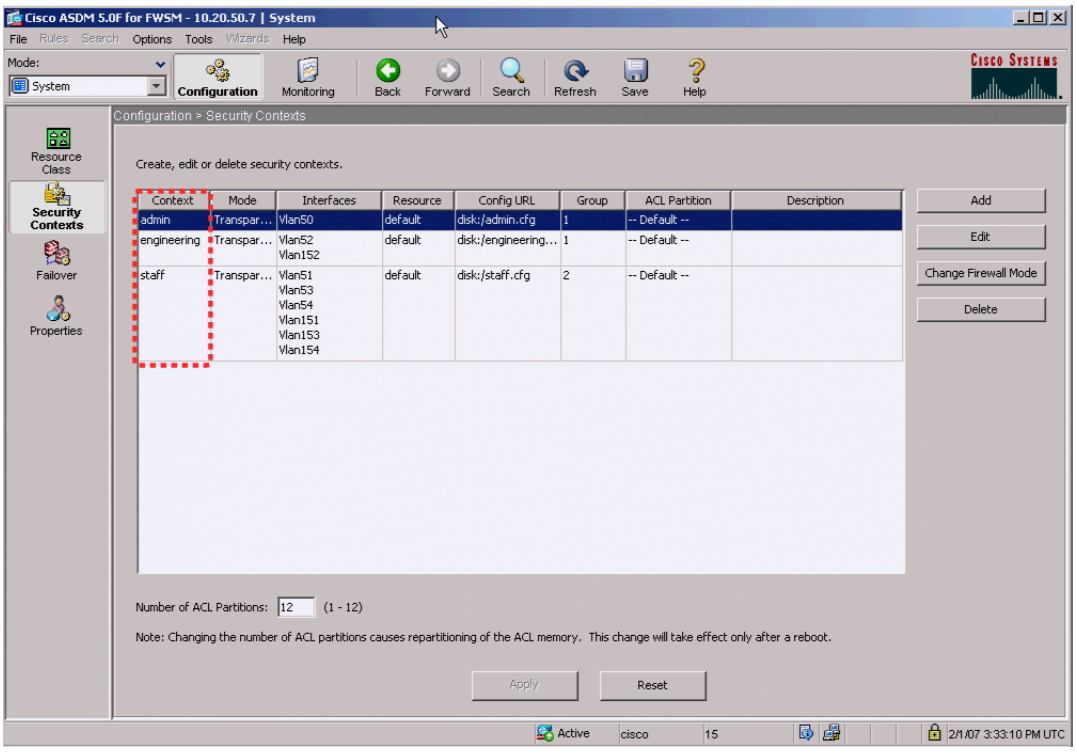
FWSM の設定

図 6-13 に、Cisco Adaptive Security Device Manager（ASDM）の FWSM（または ASA）の設定画面を示します。ここでは、FWSM に対するさまざまなセキュリティ コンテキストを定義し、各コンテキストに割り当てる VLAN を指定します。この例では、基本ユーザ、HR ユーザ、および管理者ユーザを同一の運用グループがサポートします。したがって、これらのユーザの VLAN ペアは *staff* という同一コンテキストに配置できます。技術グループの運用サポートは、別の運用グループによって実行されます。これらのユーザの VLAN ペアは、*engineering* という個別コンテキストに配置されています。

FWSM を管理するための個別コンテキスト *admin* も作成されています。このコンテキストは、ネットワークの信頼できる側に接続される VLAN を 1 つ保持しています。

（注）　ADSM は、Cisco FWSM、PIX、および適応型セキュリティ アプライアンス（ASA）用の GUI 設定ツールであり、Java アプリケーションまたはダウンロード可能アプリケーションのいずれかの形式で使用できます。以前に説明したように、マルチ コンテキストによって WLAN 展開にもたらされる利点および柔軟性を得るために、複数のコンテキストが設定されています。このシナリオ例では、企業の技術部門で、通常の IT 展開に対する別個の管理機能が必要になると仮定しています。したがって、*staff* と *engineering* という 2 つのコンテキストが作成されます。FWSM を管理するための追加コンテキスト *admin* も自動的に作成されます。FWSM は CLI または ASDM のどちらを使用しても設定できますが、通常は設定メカニズムを組み合せて使用しないことをお勧めします。

図 6-13　　ASDM FWSM セキュリティ コンテキスト



システム設定の例を以下に示します。これは、6500 から **session** コマンドを使用して FWSM と通信する場合に表示される情報です。この設定で注目する重要な点は、複数のコンテキストの作成、コンテキストへの VLAN の割り当て、およびコンテキスト設定を保存するファイルの命名です。

特定のコンテキストを表示および設定するには、**changeto context** *name* 構文を使用します。

```
FWSM Version 3.1(6) <system>
!
resource acl-partition 12
hostname FWSM-1
domain-name srnd3.net
console timeout 0


admin-context admin
context admin
  allocate-interface Vlan50
  config-url disk:/admin.cfg
!


context engineering
  allocate-interface Vlan152
  allocate-interface Vlan52
  allocate-interface Vlan57
  config-url disk:/engineering.cfg
!


context staff
  allocate-interface Vlan151
  allocate-interface Vlan153
  allocate-interface Vlan154
  allocate-interface Vlan51
  allocate-interface Vlan53
  allocate-interface Vlan54
  allocate-interface Vlan58
  config-url disk:/staff.cfg
```

admin コンテキストに変更するためのコマンド構文は、**changeto context** *admin* です。次の例は、*admin* コンテキストからの設定の例を示しています。ここでは、使用される VLAN、VLAN の信頼レベル、および Bridge group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）のインターフェイスを定義しています。コンテキストはトランスペアレントモードになっているため、ブリッジとして動作します。BVI が使用されることで、IP アドレスの指定が可能になっています。また、ASDM のサポートを有効にして、ASDM クライアントで使用される IP アドレスを定義するための **http** コマンドにも注目してください。

```
FWSM Version 3.1(4) <context>
!
firewall transparent
hostname admin
interface Vlan50
 nameif inside
 bridge-group 1
 security-level 100
!
interface BVI1
 ip address 10.20.50.7 255.255.255.0 standby 10.20.50.8


...!
route inside 0.0.0.0 0.0.0.0 10.20.50.1 1
```

```
...
http server enable
http 10.20.30.0 255.255.255.0 inside
```

図 6-14 に、*admin* コンテキストの FWSM ASDM インターフェイスの表示を示します。ここでは、VLAN および BVI インターフェイスが設定されています。

図 6-14　　FWSM ASDM の admin コンテキストのインターフェイス

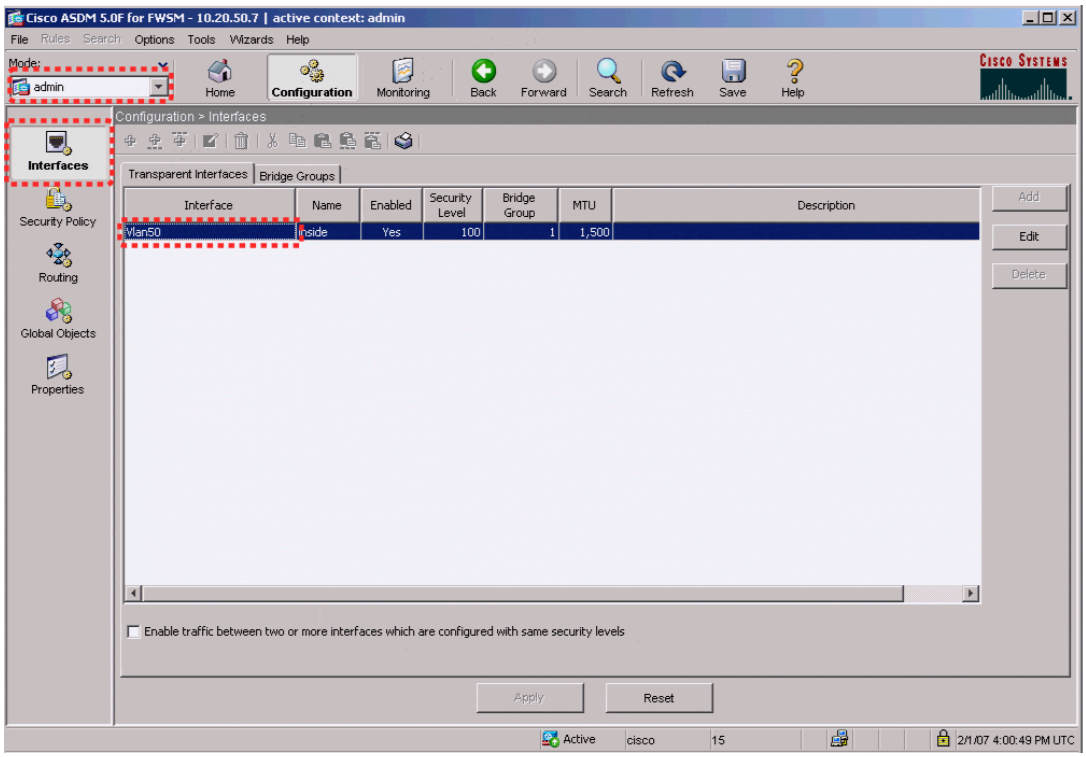


図 6-15 に、FWSM の *engineering* コンテキストを示します。ここでは、VLAN および BVI インターフェイスの BVI 情報が設定されています。

図 6-15　FWSM ASDM の engineering インターフェイス

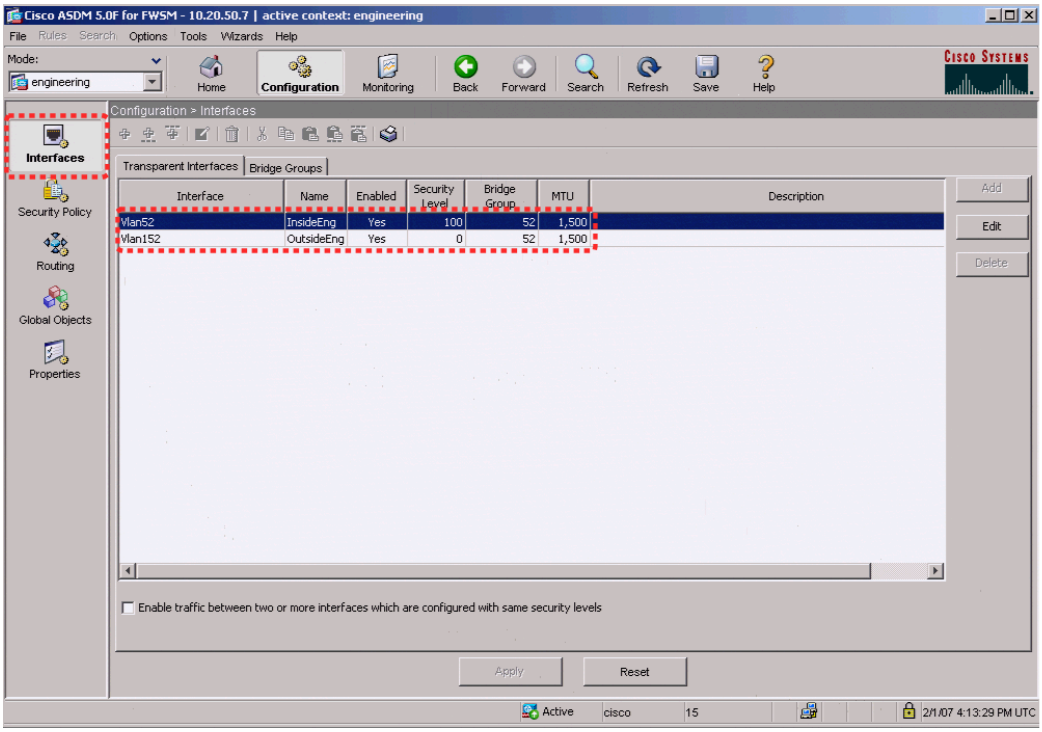


図 6-16 に、ASDM の *engineering* コンテキストの Security Policy 設定ページを示します。

図 6-16　　ASDM の engineering のセキュリティ ポリシー

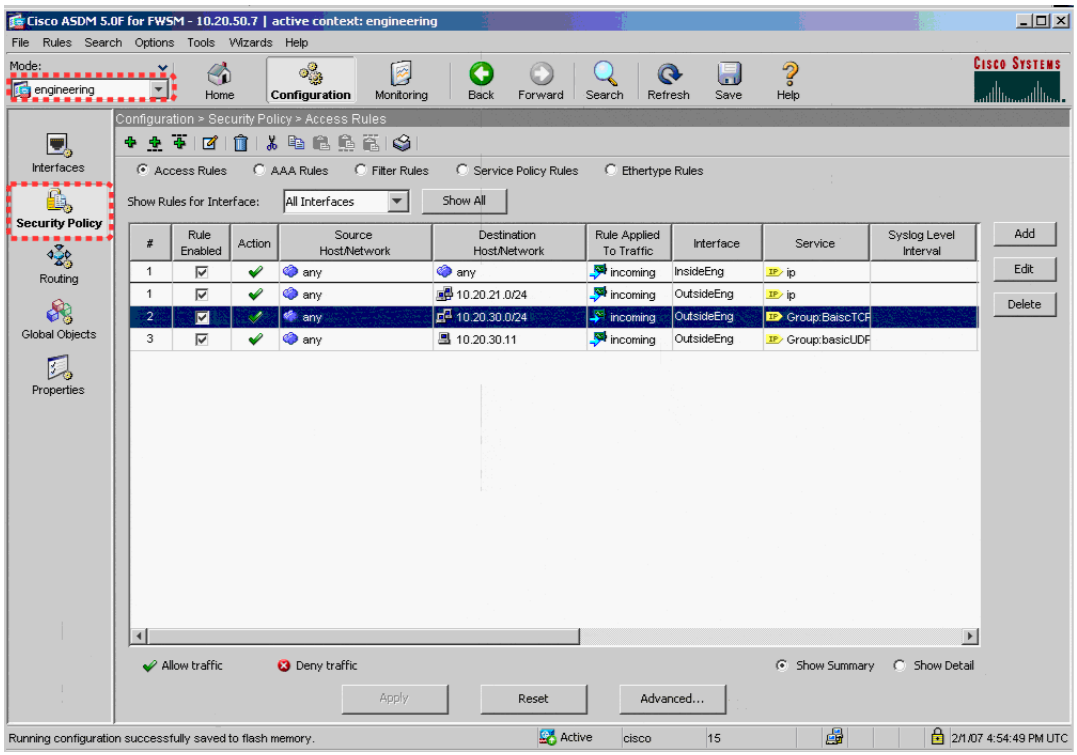


図 6-17 および図 6-18 に、このポリシー ページで適用可能なルールの例を示します。この例では、送信元インターフェイス *OutsideEngineering* は、サービス グループ *BasicUDP* で定義された UDP プロトコル グループを使用して、*InsideEngineering* を通じてホスト 10.20.30.11 にアクセスすることを許可されています。図 6-18 は、サービス グループ *BasicUDP* がサーバへの DHCP 要求および DNS 要求を許可していることを示しています。これは、ユーザに対する基本的な DHCP アドレス指定および DNS アドレス指定を許可するためです。

図 6-17　　FWSM ASDM のアクセス ルール

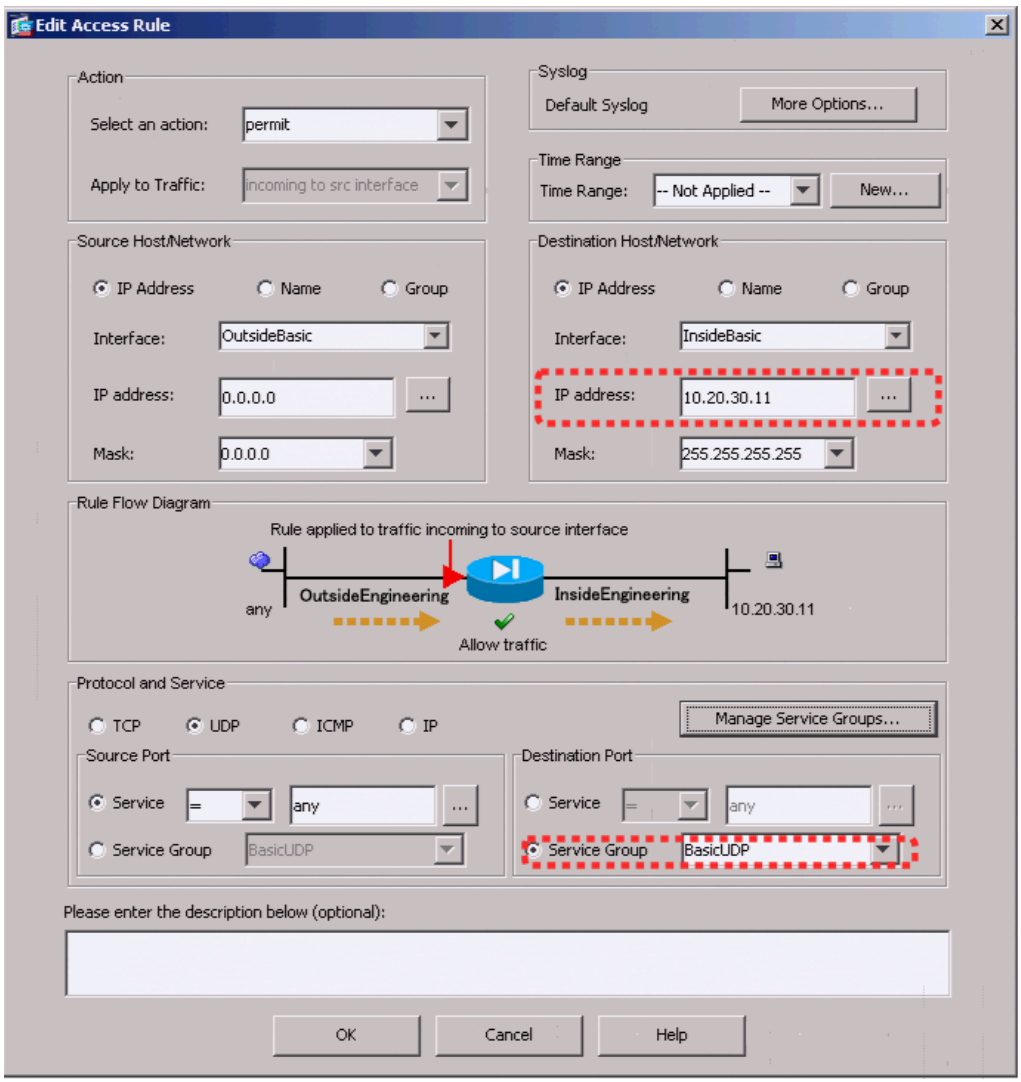
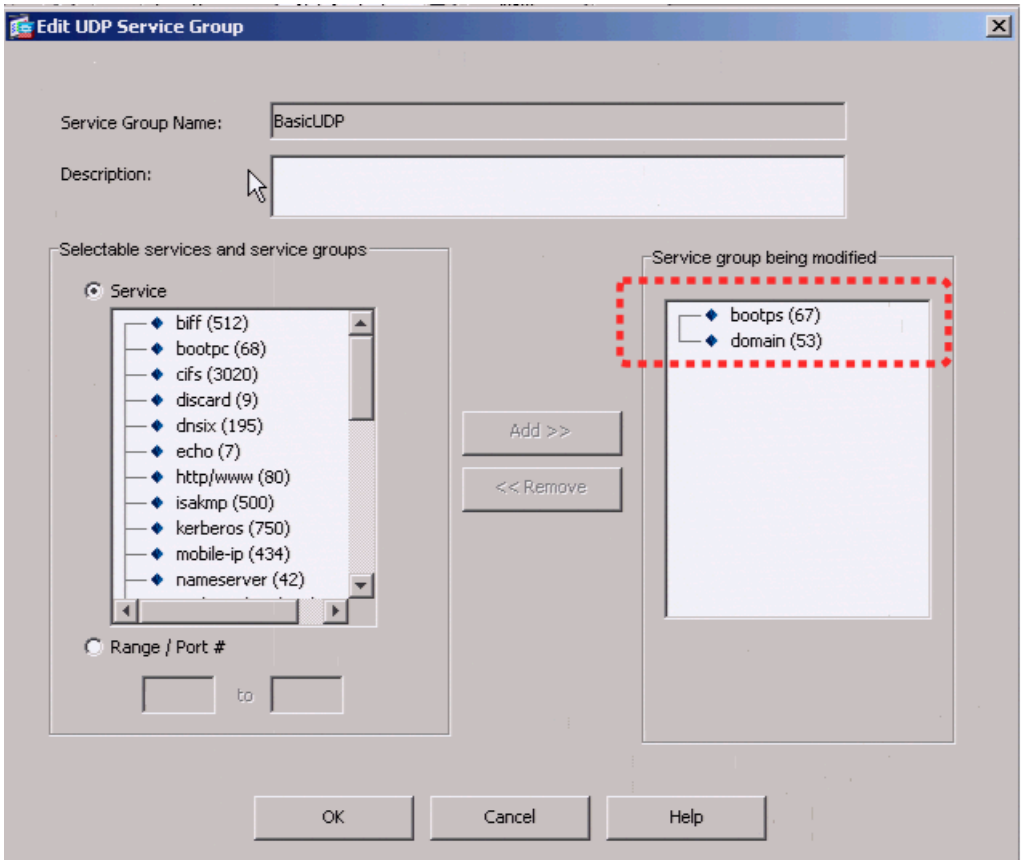


図 6-18　FWSM の UDP サービス グループ



次の設定例に、このコンテキストに関係する関連 CLI コマンドを示します。ここでは、セキュリティ ポリシーも追加して、10.20.30.0/24 サブネット上のその他の基本的なサービス、および 10.20.21.0/24 サブネット上の技術サービスへのアクセスを許可しています。

（注） BPDU の設定は、ハイ アベイラビリティについての以降のトピックに関連するものです。

```
FWSM Version 3.1(4) <context>
!
firewall transparent
hostname engineering
!
interface Vlan152
 nameif OutsideEng
 bridge-group 52
 security-level 0
!
interface Vlan52
 nameif InsideEng
 bridge-group 52
 security-level 100
!
interface Vlan57
 nameif EngineeringAdmin
 bridge-group 57
 security-level 100
!
```

```
interface BVI57
 ip address 10.20.57.7 255.255.255.0 standby 10.20.57.8
!
object-group service basicUDP udp
 port-object eq bootps
 port-object eq domain
object-group service BasicTCP tcp
 port-object eq www
 port-object eq imap4
 port-object eq https
 port-object eq pop3
 port-object eq smtp
access-list OutsideEng_access_in remark access to engineering network
access-list OutsideEng_access_in extended permit ip any 10.20.21.0 255.255.255.0
access-list OutsideEng_access_in extended permit tcp any 10.20.30.0 255.255.255.0
object-group BaiscTCP
access-list OutsideEng_access_in extended permit udp any host 10.20.30.11 object-group
basicUDP
access-list InsideEng_access_in extended permit ip any any
access-list BPDU ethertype permit bpdu


monitor-interface InsideEng
...
access-group BPDU in interface InsideEng
access-group InsideEng_access_in in interface InsideEng
access-group BPDU in interface OutsideEng
access-group OutsideEng_access_in in interface OutsideEng
route EngineeringAdmin 0.0.0.0 0.0.0.0 10.20.57.1 1
...
http server enable
http 10.20.30.0 255.255.255.0 EngineeringAdmin
```

図 6-19 に、*staff* コンテキストを示します。ここでは、VLAN および BVI インターフェイスの BVI 情報が設定されています。

図 6-19　　ASDM の staff のインターフェイス

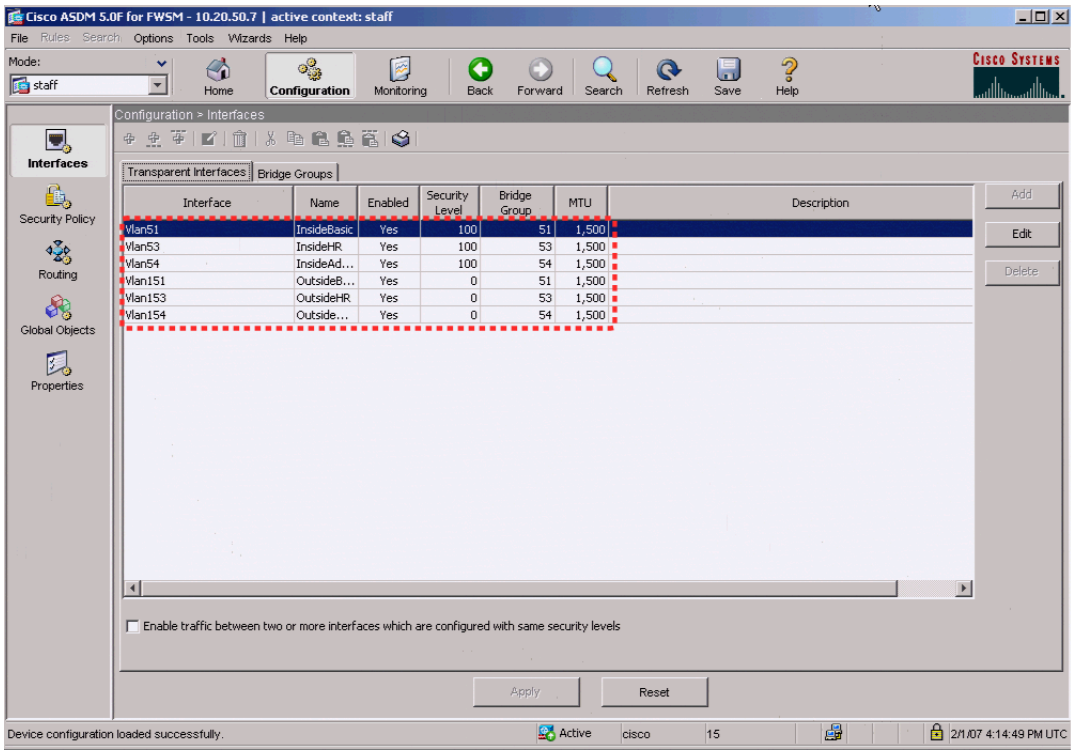
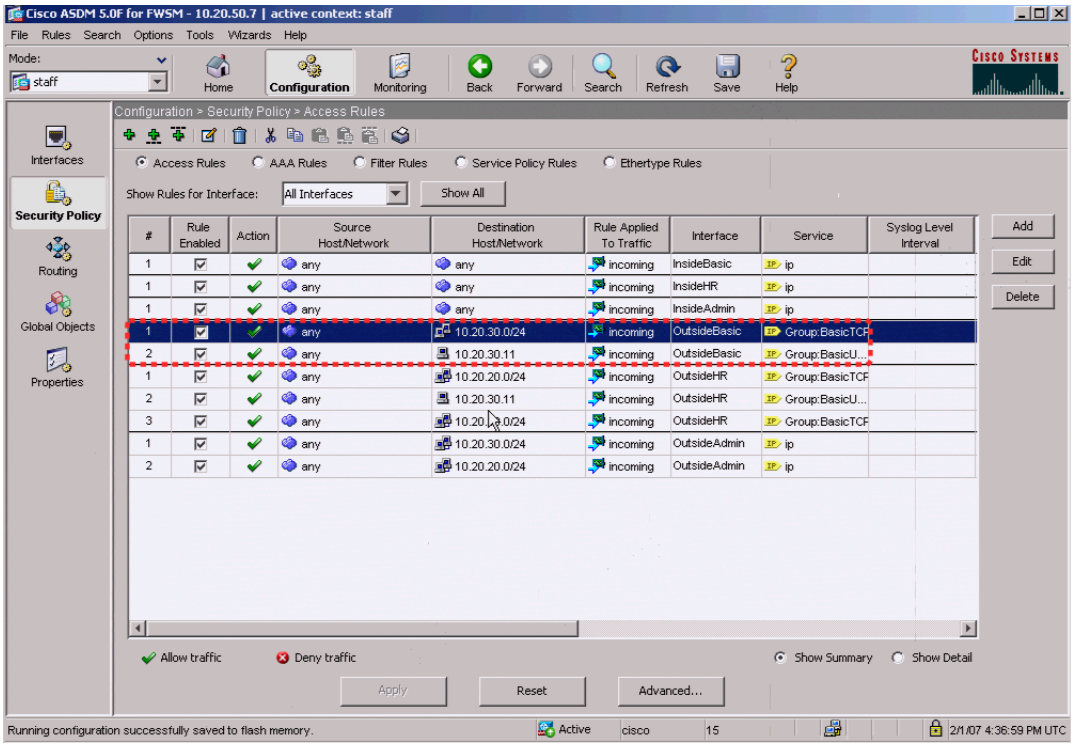


図 6-20 に、ASDM の *staff* コンテキストの Security Policy 設定ページを示します。

図 6-20　ASDM の staff のセキュリティ ポリシー



staff コンテキストの設定は、次のとおりです。

```
firewall transparent
hostname staff
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan151
 nameif OutsideBasic
 bridge-group 51
 security-level 0
!
interface Vlan153
 nameif OutsideHR
 bridge-group 53
 security-level 0
!
interface Vlan154
 nameif OutsideAdmin
 bridge-group 54
 security-level 0
!
interface Vlan51
 nameif InsideBasic
 bridge-group 51
 security-level 100
!
interface Vlan53
 nameif InsideHR
```

```
 bridge-group 53
 security-level 100
!
interface Vlan54
 nameif InsideAdmin
 bridge-group 54
 security-level 100
!
interface Vlan58
 nameif StaffAdmin
 bridge-group 58
 security-level 100
!
interface BVI58
 ip address 10.20.58.7 255.255.255.0
!
...
object-group service BasicUDP udp
 port-object eq bootps
 port-object eq domain
object-group service BasicTCP tcp
 port-object eq www
 port-object eq https
 port-object eq imap4
 port-object eq pop3
 port-object eq smtp
object-group service HRTCP tcp
 port-object eq https
access-list InsideBasic_access_in extended permit ip any any
access-list InsideHR_access_in extended permit ip any any
access-list InsideAdmin_access_in extended permit ip any any
access-list OutsideAdmin_access_in extended permit ip any 10.20.30.0 255.255.255.0
access-list OutsideAdmin_access_in extended permit ip any 10.20.20.0 255.255.255.0
access-list OutsideHR_access_in extended permit tcp any 10.20.20.0 255.255.255.0
object-group BasicTCP
access-list OutsideHR_access_in extended permit udp any host 10.20.30.11 object-group
BasicUDP
access-list OutsideHR_access_in extended permit tcp any 10.20.30.0 255.255.255.0
object-group BasicTCP
access-list OutsideBasic_access_in extended permit tcp any 10.20.30.0 255.255.255.0
object-group BasicTCP
access-list OutsideBasic_access_in extended permit udp any host 10.20.30.11 object-group
BasicUDP
access-list BPDU ethertype permit bpdu
...
monitor-interface InsideBasic
monitor-interface InsideHR
monitor-interface InsideAdmin
no asdm history enable
arp timeout 14400
access-group BPDU in interface InsideBasic
access-group InsideBasic_access_in in interface InsideBasic
access-group BPDU in interface InsideHR
access-group InsideHR_access_in in interface InsideHR
access-group BPDU in interface InsideAdmin
access-group InsideAdmin_access_in in interface InsideAdmin
access-group BPDU in interface OutsideAdmin
access-group OutsideAdmin_access_in in interface OutsideAdmin
access-group BPDU in interface OutsideBasic
access-group OutsideBasic_access_in in interface OutsideBasic
access-group BPDU in interface OutsideHR
access-group OutsideHR_access_in in interface OutsideHR
route StaffAdmin 0.0.0.0 0.0.0.0 10.20.58.1 1
...
```

```
http server enable
http 10.20.30.0 255.255.255.0 StaffAdmin
```

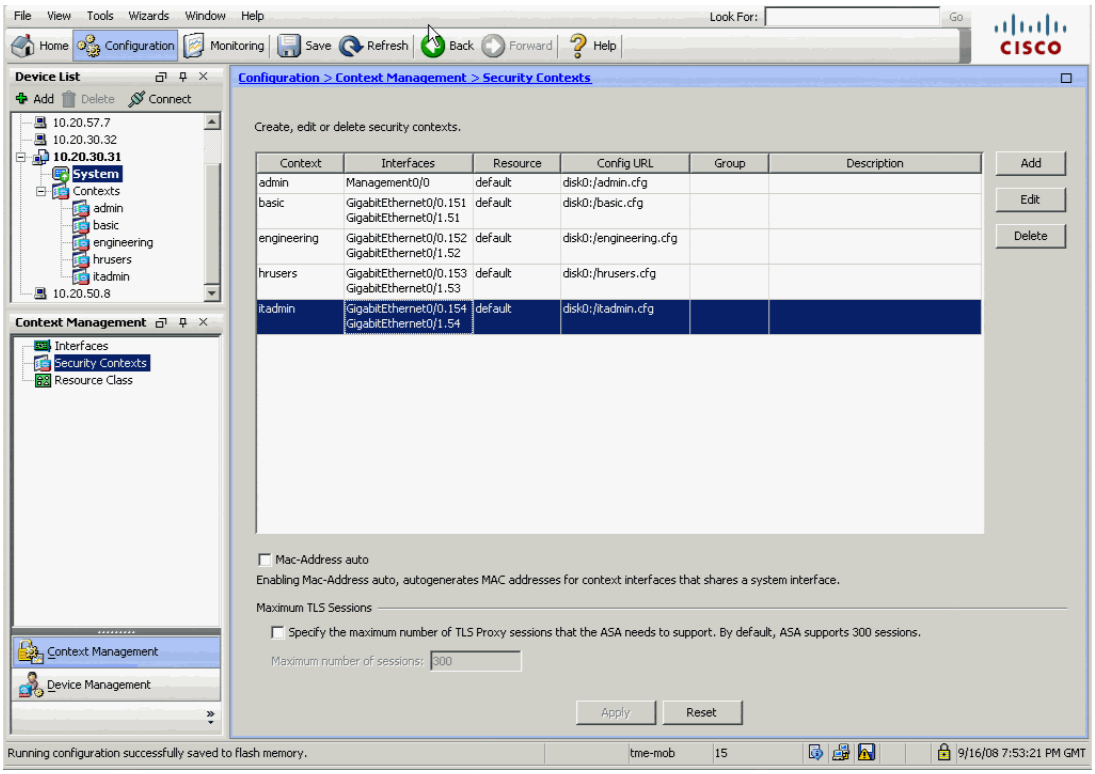
ASA の設定

ASA およびセキュリティ コンテキスト

FWSM ソフトウェアのバージョンと ASA ソフトウェアのバージョンが異なるため、ASA の設定に使用される ASDM のバージョンは、FWSM に使用されるものとは別のバージョンでした。同一の ASDM インターフェイスを使用できる FWSM および ASA のバージョンも存在しますが、この設計では、Cisco Safe Harbor プログラムに沿った FWSM バージョンを使用することを選択したため、使用されていません。

ASDM インターフェイスの違いを除くと、主な違いはコンテキストの設定です。FWSM では、コンテキストごとに複数のインターフェイスを使用できます。一方、ASA ではコンテキストごとに 2 つのインターフェイスを使用できます。つまり、信頼できる VLAN と信頼できない VLAN のペアごとに、セキュリティ コンテキストを作成する必要があります。図 6-21 に、この追加のコンテキストを示します。

図 6-21　　ASDM ASA のセキュリティ コンテキストの設定



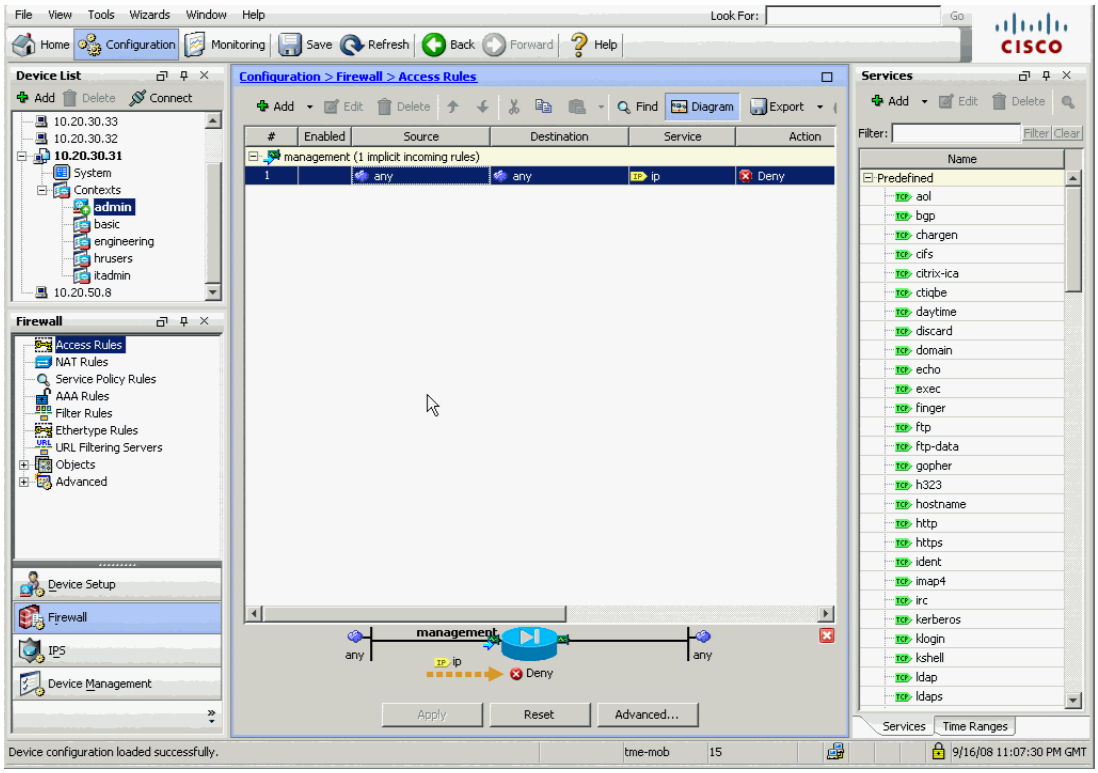
ASA の CLI コンテキスト設定

```
ASA Version 8.0(3) <system>
!
firewall transparent
```

```
hostname asa-1
!

admin-context admin
context admin
  allocate-interface Management0/0
  config-url disk0:/admin.cfg
!

context engineering
  allocate-interface GigabitEthernet0/0.152
  allocate-interface GigabitEthernet0/1.52
  config-url disk0:/engineering.cfg
!

context basic
  allocate-interface GigabitEthernet0/0.151
  allocate-interface GigabitEthernet0/1.51
  config-url disk0:/basic.cfg
!

context hrusers
  allocate-interface GigabitEthernet0/0.153
  allocate-interface GigabitEthernet0/1.53
  config-url disk0:/hrusers.cfg
!

context itadmin
  allocate-interface GigabitEthernet0/0.154
  allocate-interface GigabitEthernet0/1.54
  config-url disk0:/itadmin.cfg
```

図 6-22 に、admin コンテキストの ASA ASDM インターフェイスの表示を示します。ここでは、VLAN および BVI インターフェイスが設定されています。

図 6-22　ASA ASDM の admin コンテキストのインターフェイス



ASA には、admin セキュリティ コンテキストに配置された専用の管理インターフェイスがあります。関連する設定を次に示します。

ASA の admin コンテキストの設定

```
firewall transparent
hostname ciscoasa
enable password 8oedxwIWpACbU1CP encrypted
names
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.20.30.31 255.255.255.0
 management-only
!
...

!
route management 0.0.0.0 0.0.0.0 10.20.30.1 1
http server enable
http 10.20.30.0 255.255.255.0 management
...
```

サービス グループおよび Windows ドメイン認証

FWSM の例では、サポートしようとする基本的な UDP プロトコルおよび TCP プロトコルについて、サービス グループを作成しました。ASA についても、同じタイプのサービス グループを作成できます。この ASA の例では、テストに関連する 2 つのグループを追加しました。これらのグループ AD-UDP（図 6-23）および AD-TCP（図 6-24）を使用すると、Microsoft Active Directory で認証を受けるためにクライアントが必要とするトラフィックの転送を許可できます。このタイプのトラフィックは、通常、多くのお客様の環境で許可する必要があります。また、この章で以降に説明するように、ASA と NAC アプライアンスを組み合せる場合は必須条件となります。

図 6-23　AD-UDP サービス グループ

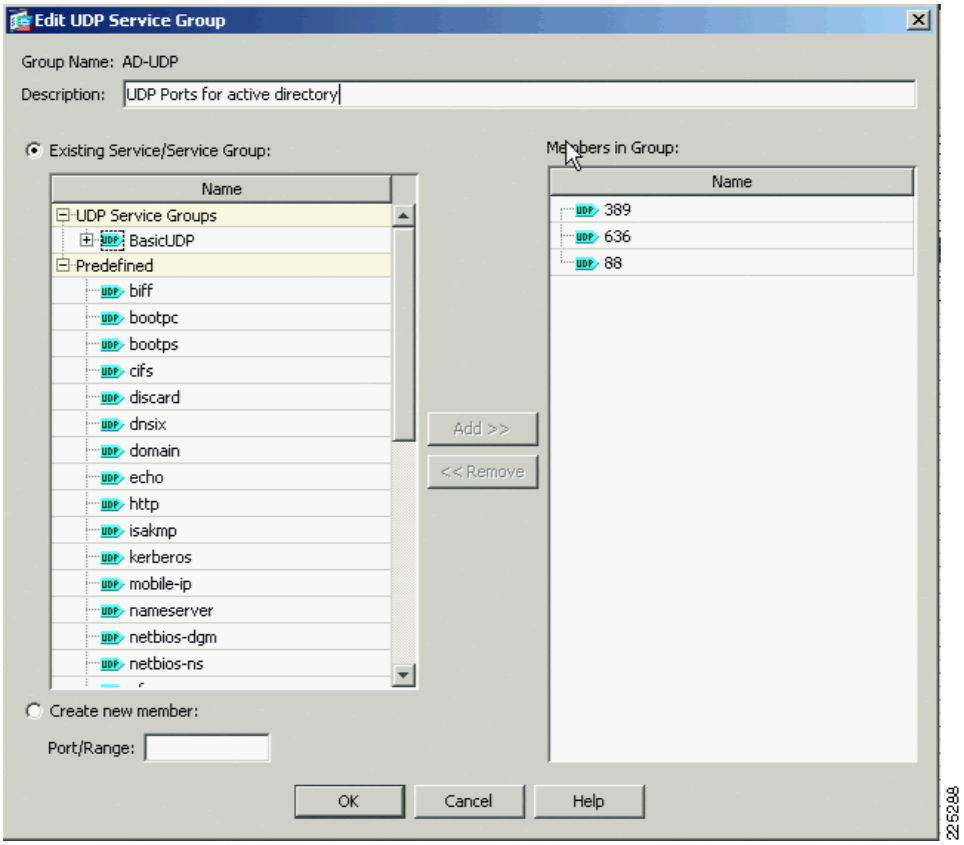
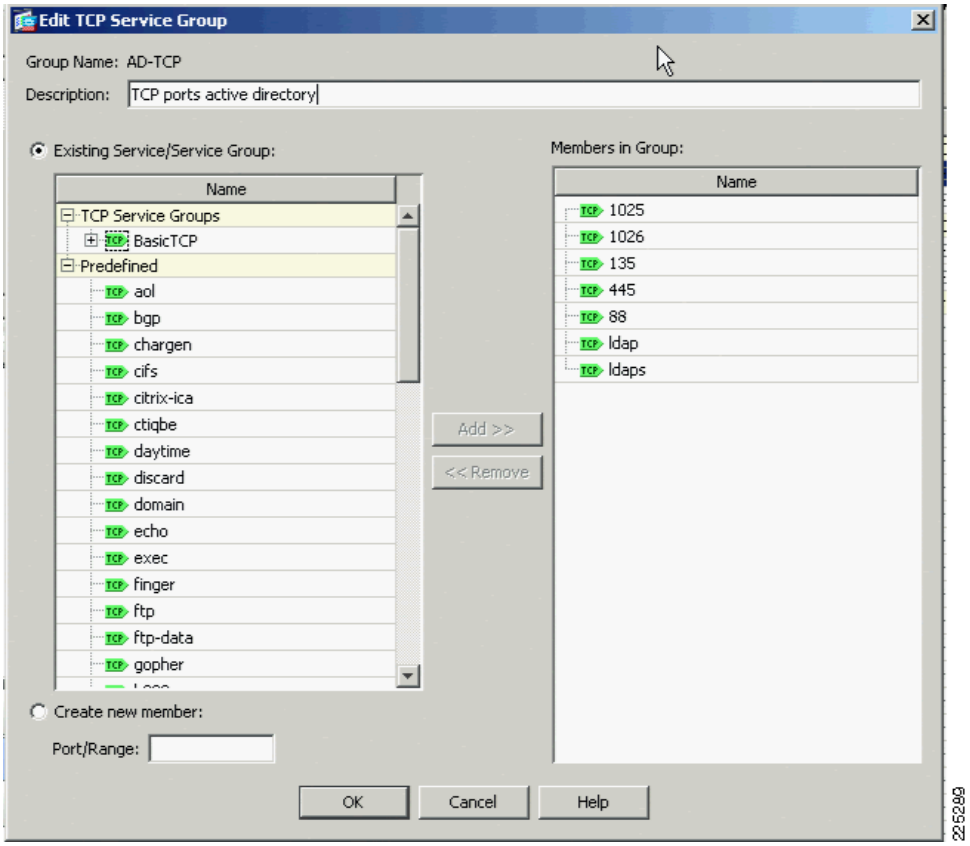


図 6-24　AD-TCP サービス グループ

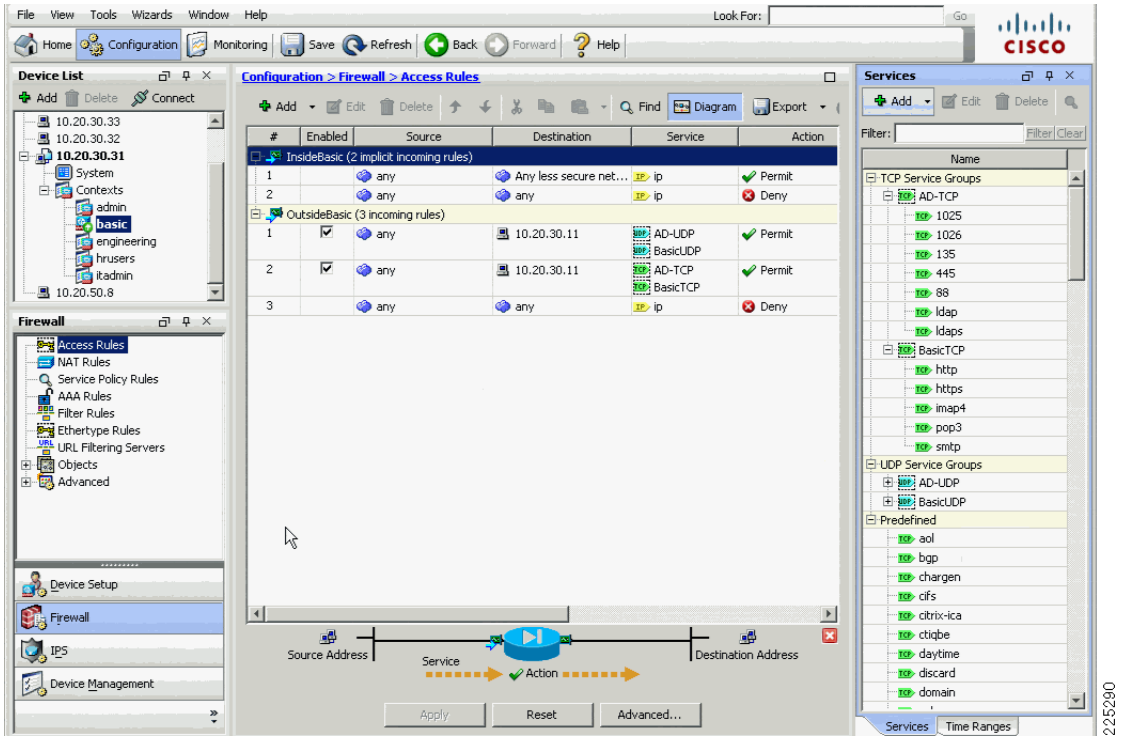


サービス グループの設定

```
object-group service BasicUDP udp
 port-object eq bootps
 port-object eq domain
object-group service BasicTCP tcp
 port-object eq www
 port-object eq imap4
 port-object eq https
 port-object eq pop3
 port-object eq smtp
object-group service AD-TCP tcp
 description TCP ports active directory
 port-object eq 1025
 port-object eq 1026
 port-object eq 135
 port-object eq 445
 port-object eq 88
 port-object eq ldap
 port-object eq ldaps
object-group service AD-UDP udp
 description UDP Ports for active directory
 port-object eq 389
 port-object eq 636
 port-object eq 88
object-group service DM_INLINE_TCP_1 tcp
 group-object AD-TCP
```

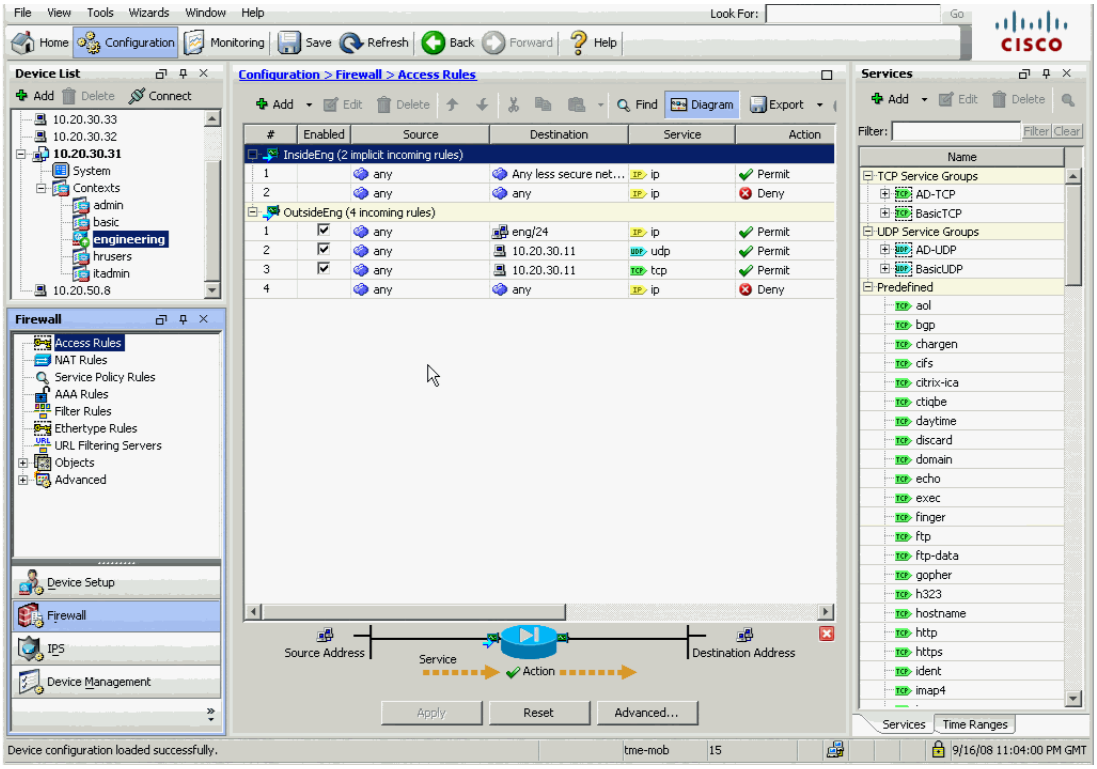
```
 group-object BasicTCP
object-group service DM_INLINE_UDP_1 udp
 group-object AD-UDP
 group-object BasicUDP
```

図 6-25　　basic の設定



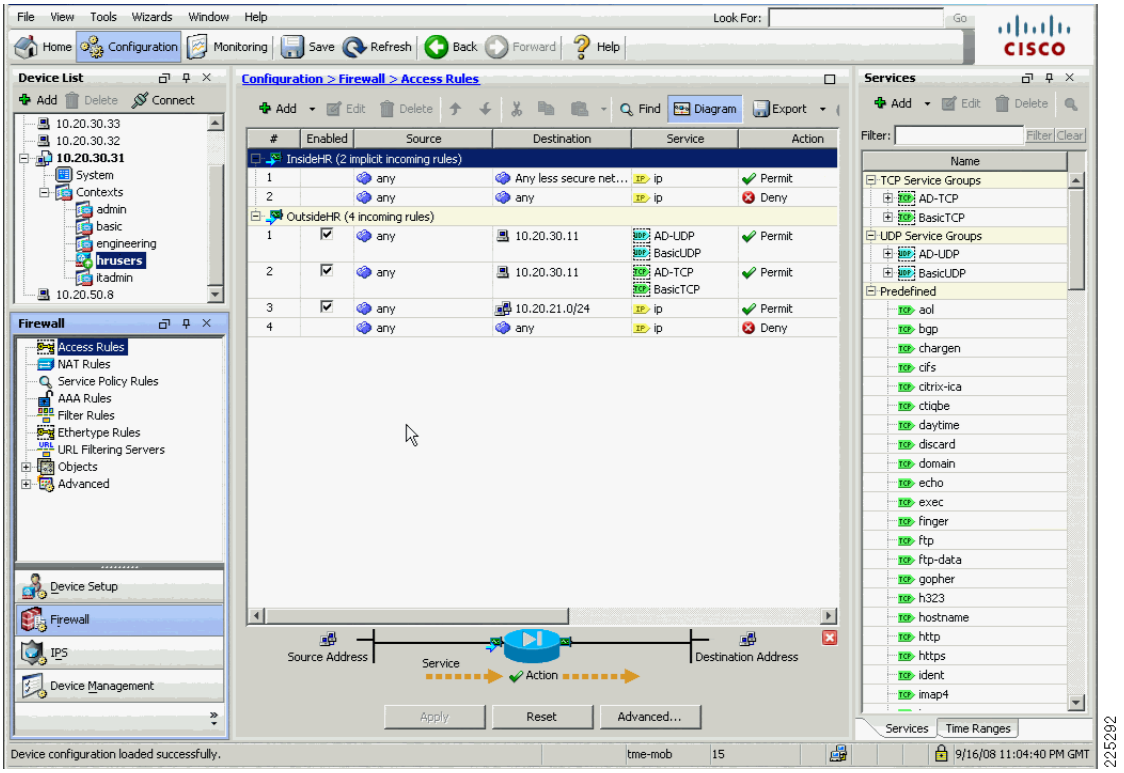

```
firewall transparent
hostname basic
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0.151
 nameif OutsideBasic
 security-level 0
!
interface GigabitEthernet0/1.51
 nameif InsideBasic
 security-level 100
!
...
access-list OutsideBasic_access_in extended permit udp any host 10.20.30.11 object-group
DM_INLINE_UDP_1
access-list OutsideBasic_access_in extended permit tcp any host 10.20.30.11 object-group
DM_INLINE_TCP_1
pager lines 24


...
access-group OutsideBasic_access_in in interface OutsideBasic
```

図 6-26　engineering の設定



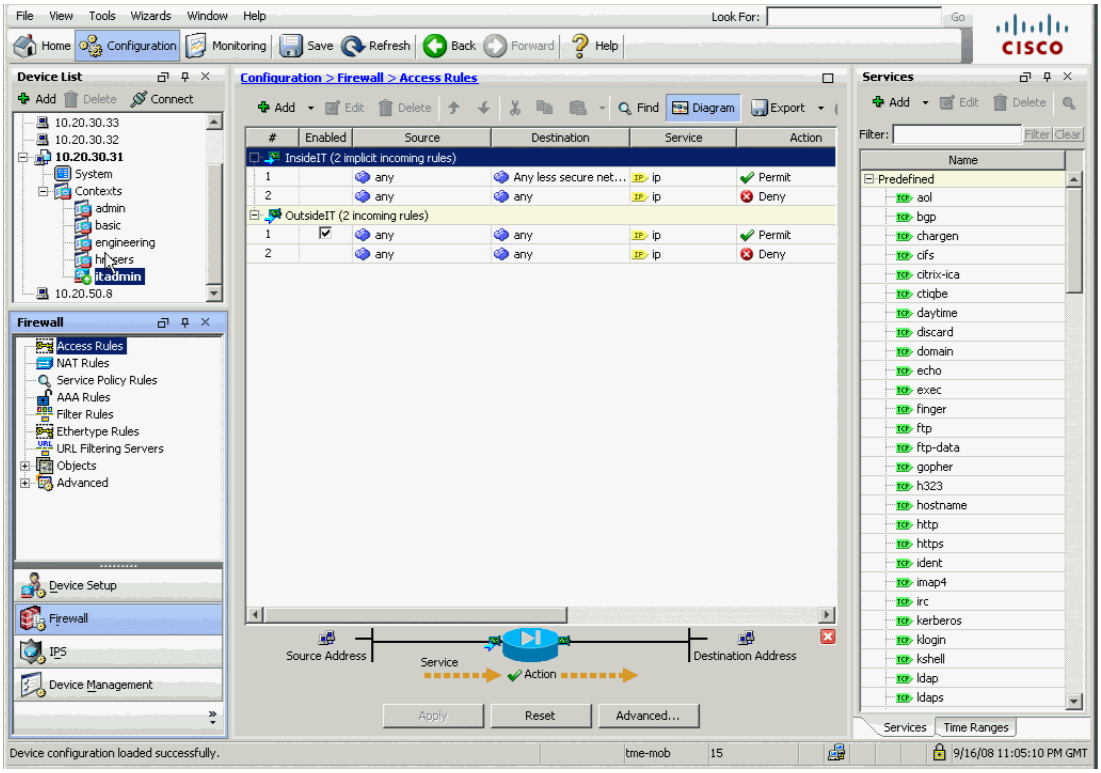

```
firewall transparent
hostname engineering

...
!
interface GigabitEthernet0/0.152
 nameif OutsideEng
 security-level 0
!
interface GigabitEthernet0/1.52
 nameif InsideEng
 security-level 100
!
...


object-group service DM_INLINE_TCP_1 tcp
 group-object AD-TCP
 group-object BasicTCP
object-group service DM_INLINE_UDP_1 udp
 group-object AD-UDP
 group-object BasicUDP
access-list InsideEng_access_in_1 extended permit ip any eng 255.255.255.0
access-list OutsideEng_access_in_1 extended permit ip any eng 255.255.255.0
access-list OutsideEng_access_in_1 extended permit udp any object-group DM_INLINE_UDP_1
host 10.20.30.11
access-list OutsideEng_access_in_1 extended permit tcp any object-group DM_INLINE_TCP_1
host 10.20.30.11
...

access-group OutsideEng_access_in_1 in interface OutsideEng
```

図 6-27　　hrusers コンテキストの設定




```
firewall transparent
hostname hrusers


...!
interface GigabitEthernet0/0.153
 nameif OutsideHR
 security-level 0
!
interface GigabitEthernet0/1.53
 nameif InsideHR
 security-level 100
!
 ...
object-group service DM_INLINE_TCP_1 tcp
 group-object AD-TCP
 group-object BasicTCP
object-group service DM_INLINE_UDP_1 udp
 group-object AD-UDP
 group-object BasicUDP
access-list OutsideHR_access_in extended permit udp any host 10.20.30.11 object-group
DM_INLINE_UDP_1
access-list OutsideHR_access_in extended permit tcp any host 10.20.30.11 object-group
DM_INLINE_TCP_1
access-list OutsideHR_access_in extended permit ip any 10.20.21.0 255.255.255.0
...

access-group OutsideHR_access_in in interface OutsideHR
```

図 6-28　itadmin セキュリティ コンテキストの設定



ハイ アベイラビリティ

このマニュアルで以前に説明した FWSM の設定は、スタンドアロンの FWSM/WiSM の組み合せに対応したものです。多くの実稼働環境では、保守または障害発生によって FWSM が使用不能になった場合でも運用を確実に継続できるように、ハイ アベイラビリティ設定が必要となります。図 6-29 に、ハイ アベイラビリティの例について概略図を示します。ここでは、2 台の 6500 にそれぞれ WiSM が装着され、FWSM は、2 台の 6500 間で FWSM VLAN をブリッジするトランクを通じて接続されています。

ASA のハイ アベイラビリティ設定の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807dac5f.shtml

図 6-29　FWSM のハイ アベイラビリティ

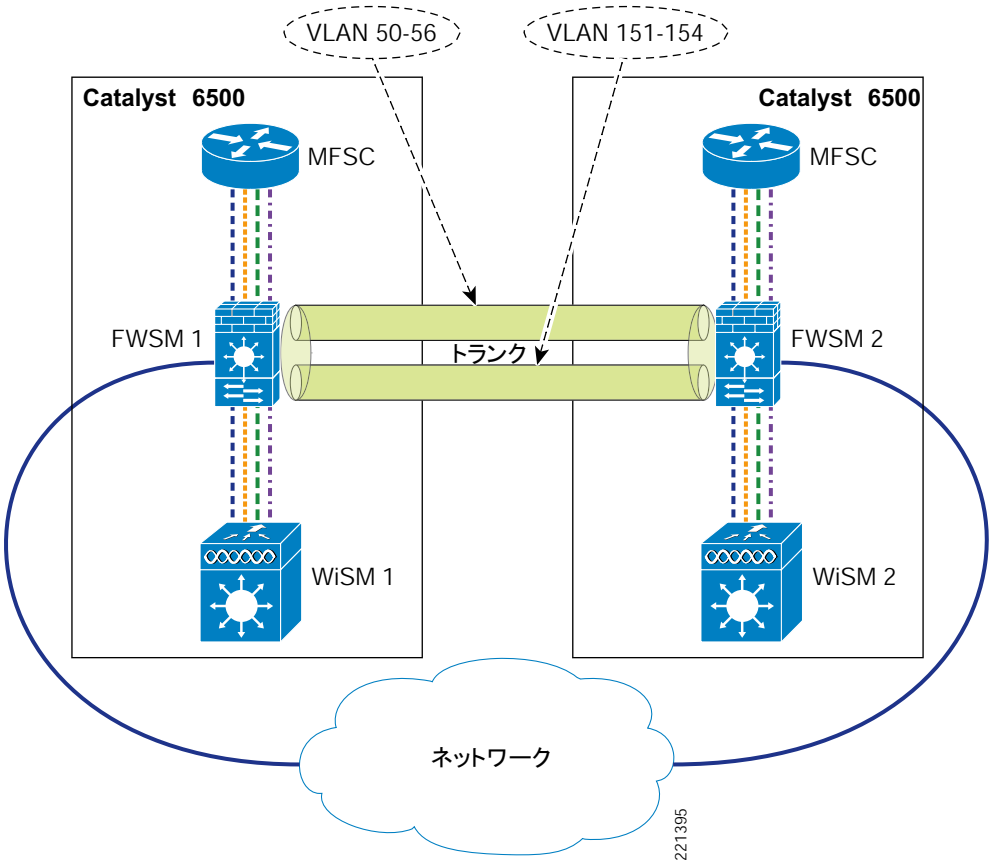
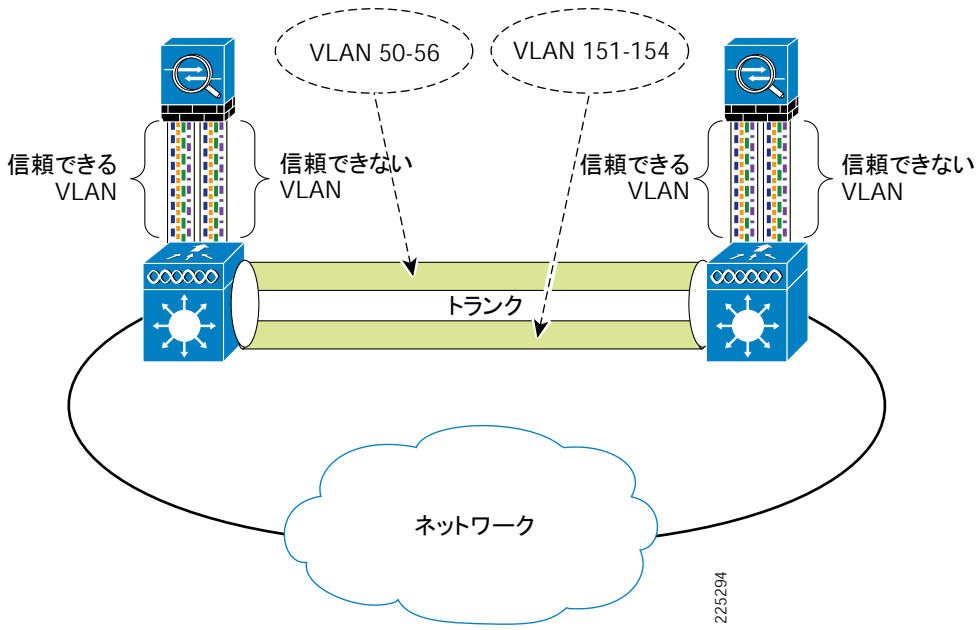


図 6-30　ASA のハイ アベイラビリティ



スパニング ツリーおよび BPDU

図 6-29 に示したようなネットワーク構成では、信頼できない VLAN と信頼できる VLAN を FWSM または ASA が同時にブリッジする場合、2 台の 6500 間でループが作成される可能性があります。

FWSM または ASA のフェールオーバー機能を使用すると、HA ペア間で 1 つの FWSM または ASA セキュリティ コンテキストのみがトラフィックを転送することが保証され、このレイヤ 2 ループの発生は防止されます。

FWSM または ASA フェールオーバーの設定に誤りがあった場合に備えて、これらのループを防止するための追加の手順を実行し、ファイアウォールによってスパニング ツリー BPDU が確実に渡されるようにします。デフォルトの FWSM または ASA アクセス ポリシーでは、スパニング ツリー BPDU がブロックされます。このため、6500 のスパニング ツリー設定ではループから保護されません。FWSM または ASA の各セキュリティ コンテキストに含まれている各 VLAN 設定で、スパニング ツリー BPDU が渡されるようにアクセス リストを設定する必要があります。これらについては、P.6-19 の「FWSM または ASA の設定」の設定例に含まれています。

BPDU が FWSM または ASA をパススルーすることを許可すると、状況によってはセキュリティ上の危険性が生じます。ただし、このトポロジでは、（他の WLC に加えて）WiSM が WLAN クライアントからのスパニング ツリー Ethertype を渡さないため、スパニング ツリー BPDU が FWSM または ASA を通過することを許可しても、セキュリティ上の悪影響はありません。実装が適切である場合、通常の FWSM フェールオーバー動作ではレイヤ 2 ループは発生しないため、BPDU のパススルーは必須ではありません。

（注）　HA 展開の場合、FWSM フェールオーバー機能の使用は重要です。この機能によって、ペアごとに 1 つの FWSM セキュリティ コンテキストのみがトラフィックを転送し、FWSM 間でファイアウォール クライアントの状態情報が転送されることが保証されるためです。

WLAN クライアントのローミングおよびファイアウォールの状態

FWSM モジュールまたは ASA については、レイヤ 2 ループに関する考慮事項以外に、ファイアウォールを通過するすべてのトラフィック フローに関して保持されるプロトコル状態情報を考慮する必要があります。HA 設定の場合、FWSM または ASA は、クライアントのトラフィックが同一の FWSM または ASA を通じて転送され、フェールオーバー FWSM のプロトコル状態データが最新の状態に維持されることを保証する必要があります。これは、FWSM または ASA をフェールオーバー設定にすることで達成されます。

FWSM には、次の 2 つのフェールオーバー オプションがあります。

- アクティブ / スタンバイ：1 つの FWSM または ASA がアクティブ状態になります。スタンバイの FWSM または ASA は、アクティブなファイアウォールの設定および状態を追跡しますが、トラフィックを転送しません。
- アクティブ / アクティブ：アクティブなセキュリティ コンテキストを FWSM または ASA 間で分散できます。また、それぞれの状態を互いに追跡し、各 FWSM または ASA で他方のトラフィック フローを確実に引き継ぐことができます。アクティブなセキュリティ コンテキストをこの方法で共有することにより、負荷を FWSM または ASA にわたって分散できます。

負荷が FWSM または ASA にわたって共有され、クライアントのモビリティにも影響しないため、この場合はアクティブ / アクティブが最適な方法です。

次の設定例は、FWSM 1 の追加のフェールオーバー設定パラメータを示しています。FWSM 2 の設定も同一ですが、**failover LAN unit primary** を **failover LAN unit secondary** に変更する点が異なります。FWSM のモードは、シングル コンテキストまたはマルチ コンテキストのいずれかに設定する必要があります。フェールオーバー システムは、この点を除いて FWSM 1 の設定を FWSM 2 にコピーし、設定の同期を維持します。

（注） 各セキュリティ コンテキストの定義では、コンテキストの参加先となるフェールオーバー グループを指定します。したがって、そのコンテキストでどの FWSM がトラフィックを転送するかを定義します。

```
interface Vlan55
 description LAN Failover Interface
!
interface Vlan56
 descriptionSTATE Failover Interface
!
.....
failover
failover lan unit primary
failover lan interface failover Vlan55
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover replication http
failover link STATE Vlan56
failover interface ip failover 12.20.200.1 255.255.255.0 standby 12.20.200.2
failover interface ip STATE 12.20.201.1 255.255.255.0 standby 12.20.201.2


failover group 1
  preempt
failover group 2
  secondary
  preempt 5


admin-context admin
context admin
  allocate-interface Vlan50
  config-url disk:/admin.cfg
  join-failover-group 1
!


context engineering
  allocate-interface Vlan152
  allocate-interface Vlan52
  allocate-interface Vlan57
  config-url disk:/engineering.cfg
  join-failover-group 2
!


context staff
  allocate-interface Vlan151
  allocate-interface Vlan153
  allocate-interface Vlan154
  allocate-interface Vlan51
  allocate-interface Vlan53
  allocate-interface Vlan54
  allocate-interface Vlan58
```

```
config-url disk:/staff.cfg
join-failover-group 1
```

設定する FWSM コンテキストごとに、次の例のようにスタンバイ アドレスと監視インターフェイスを設定する必要があります。

- フェールオーバーの *engineering* コンテキスト

```
interface BVI57
 ip address 10.20.57.7 255.255.255.0 standby 10.20.57.8
 …
monitor-interface InsideEng
```

- フェールオーバーの *staff* コンテキスト

```
interface BVI58
 ip address 10.20.58.7 255.255.255.0 0 standby 10.20.58.8
…
monitor-interface InsideBasic
monitor-interface InsideHR
monitor-interface InsideAdmin
```

レイヤ 2 およびレイヤ 3 のローミング

4.1 コード リリースよりも前の WLC ファームウェアの場合、異なるサブネットにわたる WLAN クライアント ローミングは、WLAN クライアントに対しては透過的ですが、その結果として、アシンメトリックなクライアント トラフィック フローが発生しました。WLAN クライアントを宛先とするトラフィックは、クライアントの「アンカー」WLC に送信され、この WLC で EoIP トンネルを通じて外部の WLC にトンネリングされました。しかし、図 6-31 および図 6-32 に示すように、WLAN クライアントによって送信されるトラフィックは、外部 WLC によってネットワークに直接転送されていました。

図 6-31　アシンメトリックなレイヤ 3 ローミング

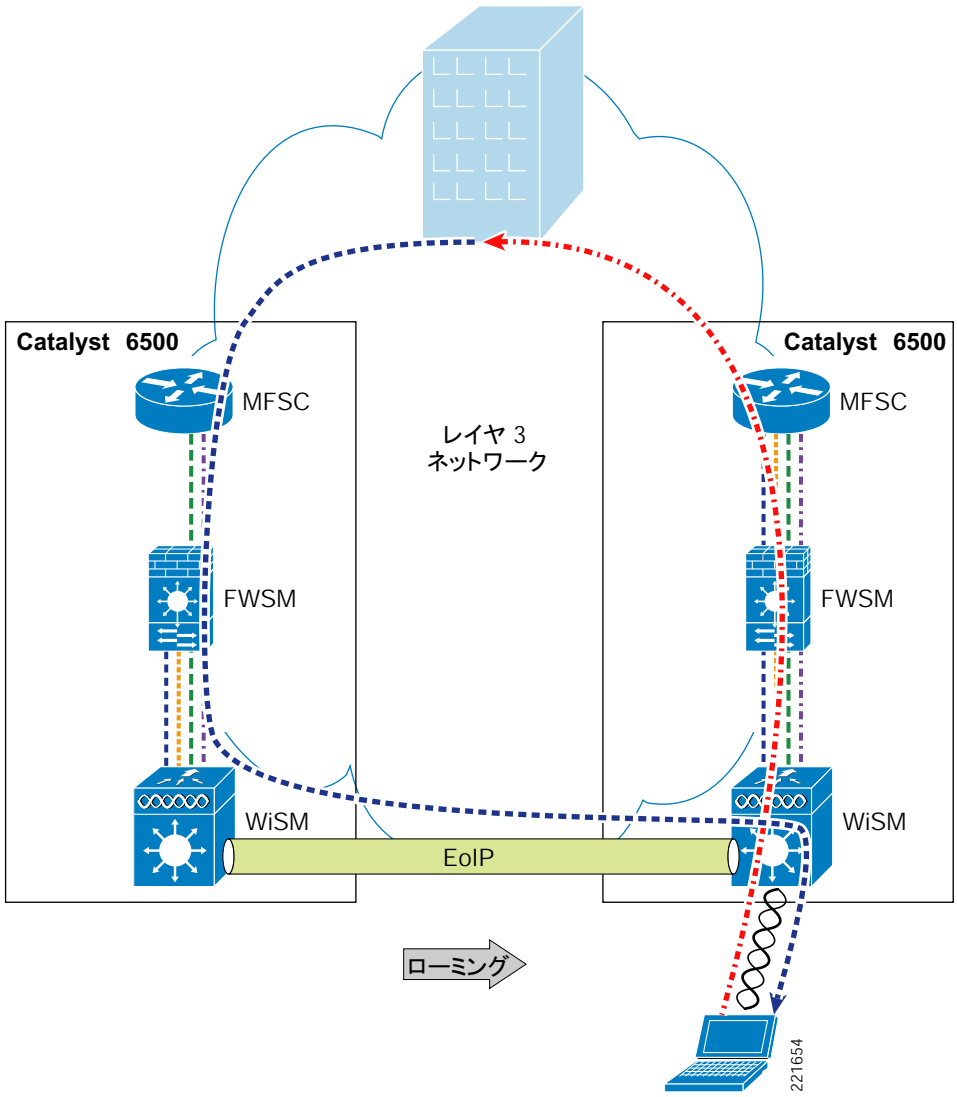
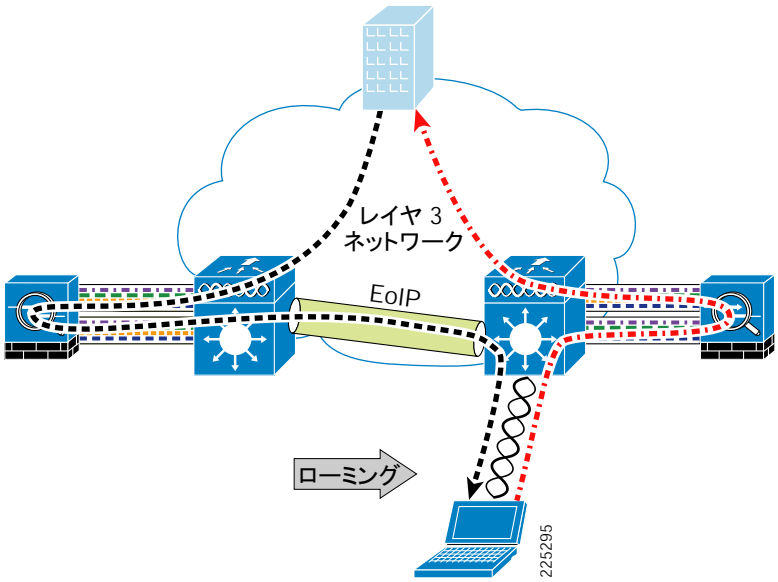


図 6-32　　ASA のアシンメトリックなレイヤ 3 ローミング



4.1 コード リリースには、レイヤ 3 ローミングを図 6-33 に示したシンメトリックにするためのオプションがあります（デフォルトではオフ）。これにより、WLAN クライアントのローミングがレイヤ 2 に限られるという要件は緩和されています。リリース 5.2 では、シンメトリック トンネリングがデフォルトのトンネリング モードです。

図 6-33　FWSM のシンメトリックなレイヤ 3 ローミング

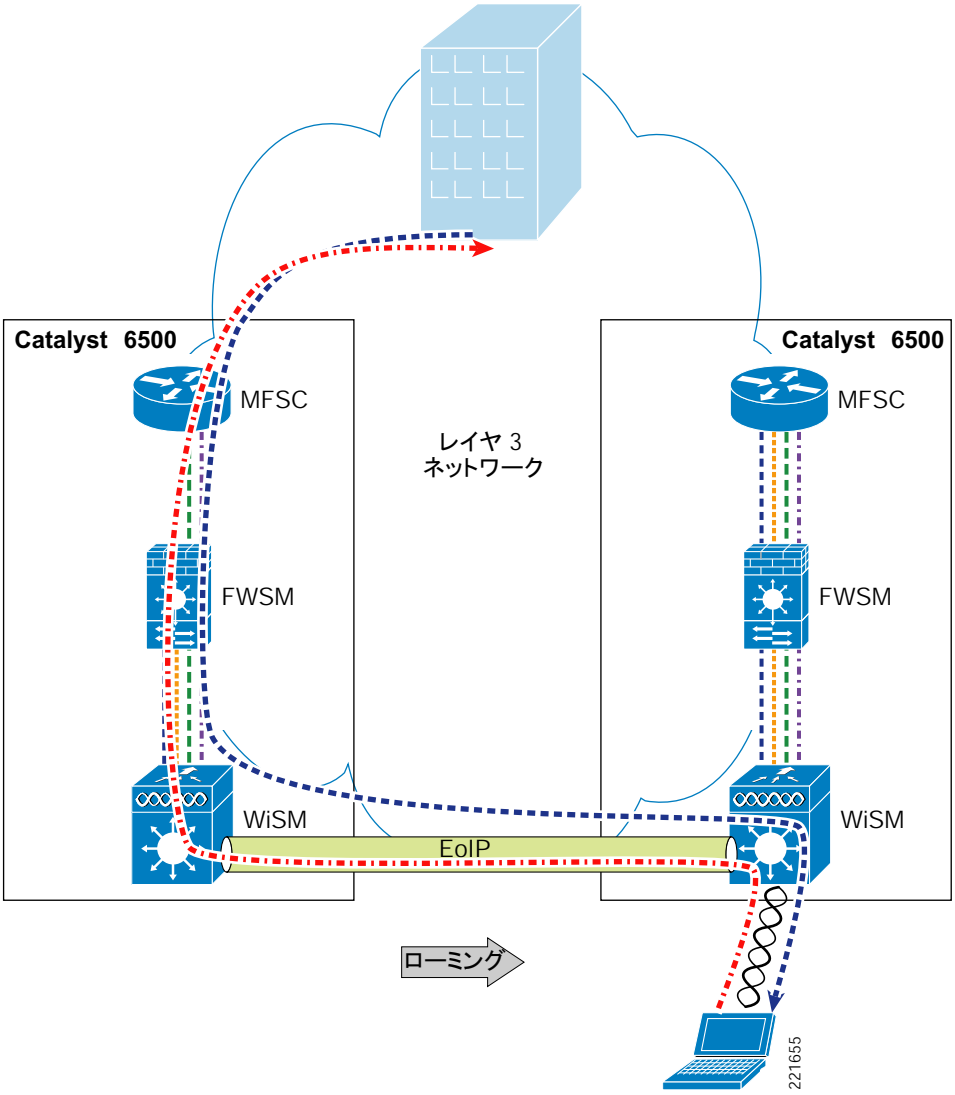
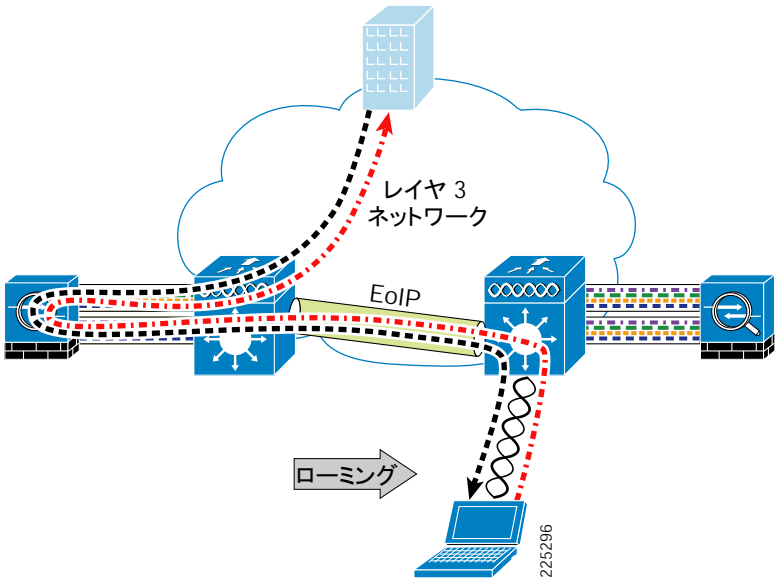


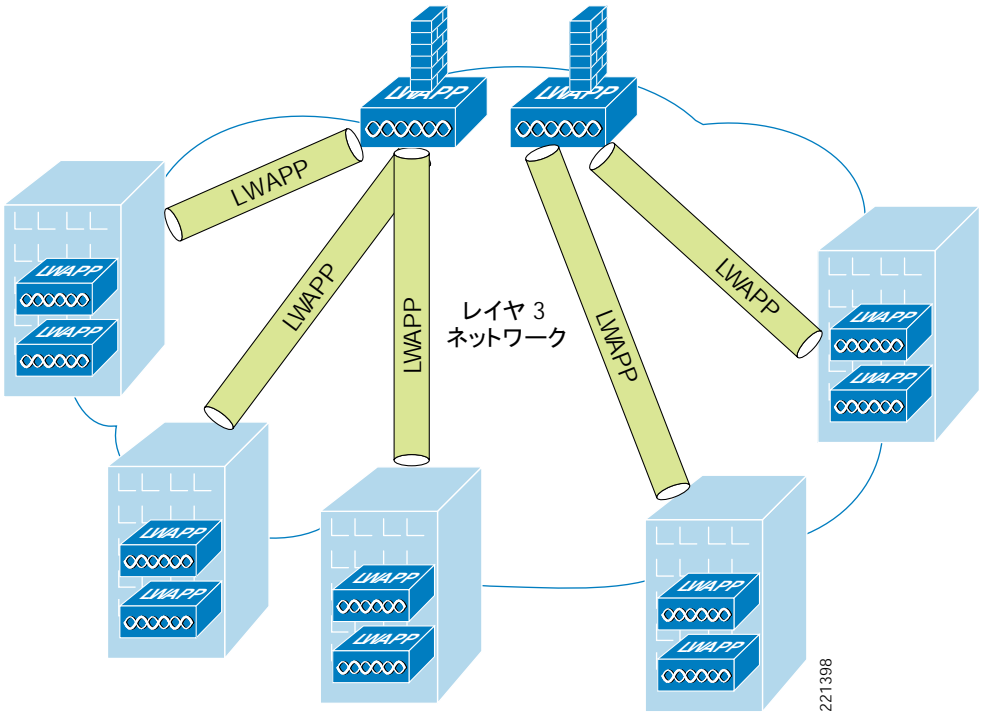
図 6-34　　ASA のシンメトリックなレイヤ3 ローミング



シンメトリックなレイヤ 3 によるアーキテクチャへの影響

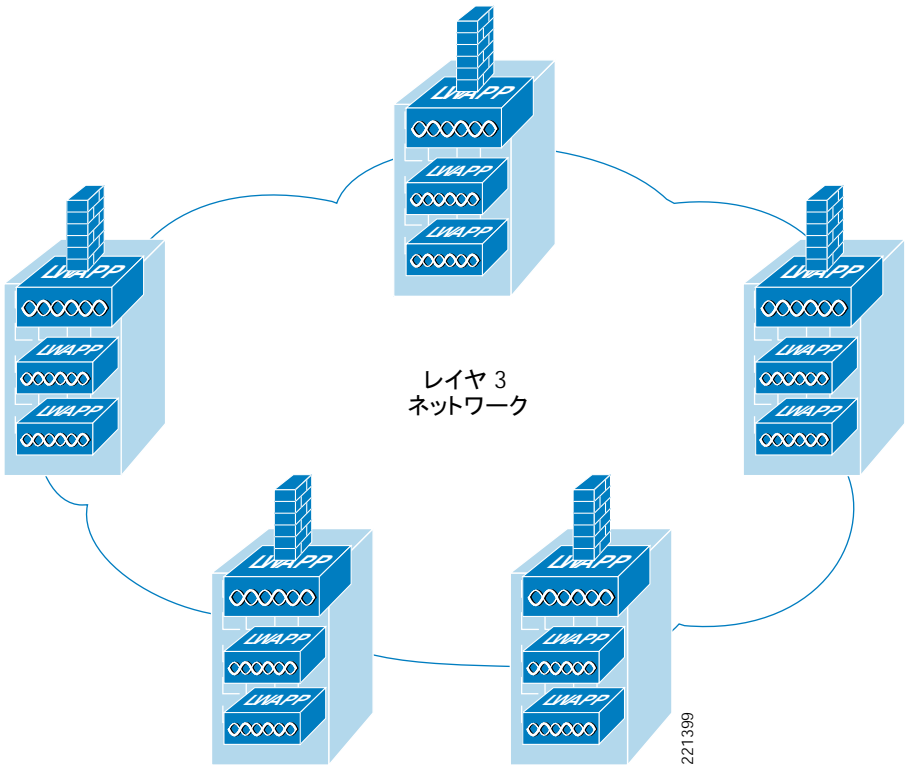
シンメトリックなレイヤ 3 ローミングが使用可能になる以前、ファイアウォールが適用されている WLAN では、クライアントを同一の VLAN 上に維持して、WLAN クライアント トラフィックが同一のファイアウォールを通過する状態を保つ必要がありました。このため、WLC のファイアウォール ソリューションは、WLAN クライアントがレイヤ 3 ローミングを実行しないことが保証されている場合を除いて、図 6-35 に示した中央集中型の展開に限定されていました。

図 6-35　　中央集中型の展開



シンメトリックなレイヤ 3 ローミングでは、WLC のファイアウォール ソリューションを図 6-36 に示した分散型にして、さらにレイヤ 3 ローミングをサポートすることができます。

図 6-36　　分散型の展開



シンメトリックなレイヤ 3 ローミングでの設定の変更

このマニュアルで示した設定例では、図 6-36 の分散型 WLC モデルを採用する場合、設定上の基本的な変更点はありません。これは、適切なサブネット変更を行った複数ロケーションの設定と同一になるためです。WLC 上でシンメトリックなレイヤ 3 ローミングを有効にするには、**config mobility symmetric-tunneling enable** コマンドを使用します。

（注）　このコマンドは、モビリティ グループに含まれているすべての WLC 上で入力する必要があります。変更を有効にするには、WLC をリブートする必要があります。

レイヤ 3 ローミングはモバイル IP ではない

レイヤ 3 ローミングを利用する展開について検討するときは、レイヤ 3 ローミングがモバイル IP と同一ではないことを理解するのが重要です。重要な点は、レイヤ 3 ローミングでクライアントが同一の IP アドレスを維持できるのは、クライアントが Unified Wireless 展開のモビリティ グループ内で別のサブネットに移動した場合に限られるということです。

モバイル IP では、クライアントに静的な IP アドレスを割り当てて、クライアントのモバイル IP ホーム エージェントに接続されるあらゆるネットワーク（WLAN やセルラー WAN などのネットワーク）内で、その IP アドレスを使用して接続を維持できます。レイヤ 3 ローミングでは、WLAN クライアントはホーム サブネット上でアドレスを取得し、WLAN ローミングによって別のサブネットに移動する場合もその接続を維持できます。モバイル IP のアドレス

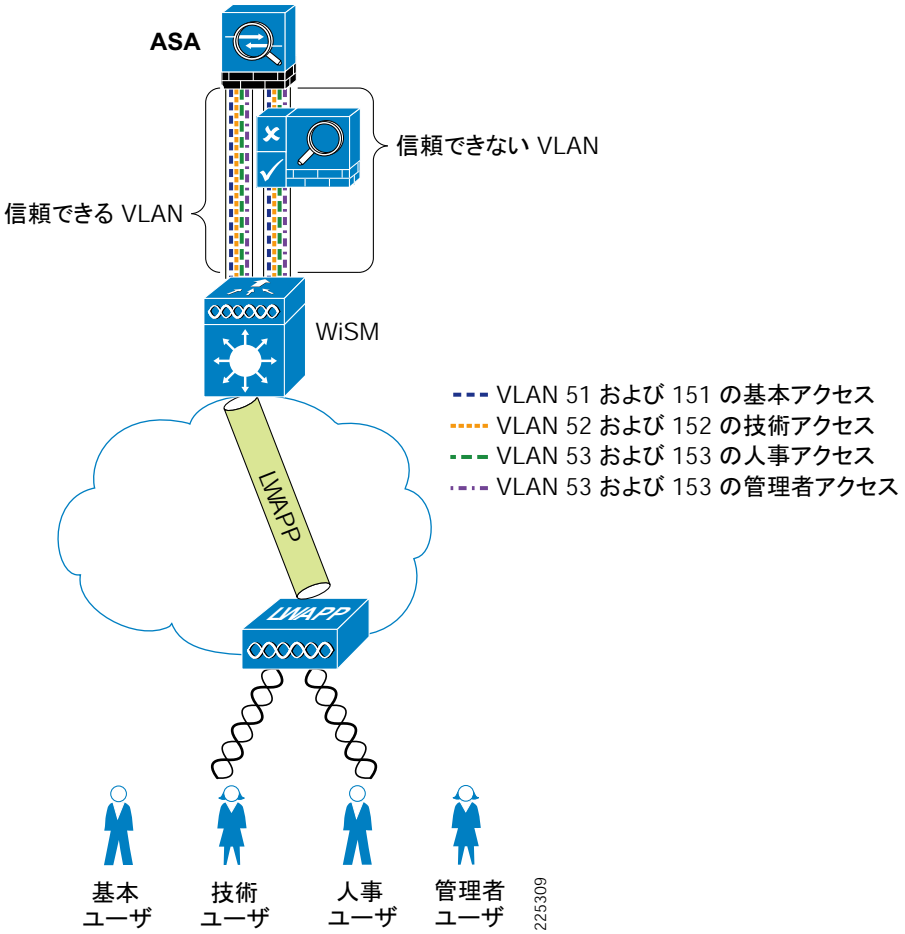
マッピングは静的な設定ですが、レイヤ 3 ローミングは動的なものであり、その基盤となるのは、クライアントが WLAN とのアソシエーションを確立したときの IP アドレスおよびサブネットをラーニングした WLC モビリティ グループです。

NAC とファイアウォールの結合

この章では、設計テストの一環として、ASA ファイアウォールと NAC アプライアンスを組み合せて使用するための要件について検討しました。バーチャル ゲートウェイ モードの NAC アプライアンスと、透過型ファイアウォールとして機能する ASA を使用する場合は、ケーブル配線と VLAN 割り当てという比較的単純なプロセスになります。図 6-37 に概略図を示します。

WiSM からの VLAN は、NAC アプライアンスの Untrusted インターフェイスにマップされ、ポスチャ評価が実行されます。クライアント デバイスは、自身のポスチャ評価を渡します。クライアント デバイスのトラフィックは、ASA の信頼できない VLAN インターフェイスに渡され、適切なポリシーが適用されます。NAC アプライアンスで RADIUS SSO が使用されている場合、ASA のファイアウォール ポリシーを変更する必要はありません。ただし、NAC で Active Directory SSO が使用されている場合は、この章で以前に説明したように、ASA ファイアウォール ポリシーで特定の TCP ポートおよび UDP ポートを許可する必要があります。Microsoft Active Directory クライアントをサポートするように設計されたファイアウォール実装では、ほとんどの場合、これらのポートはすでに許可されています。

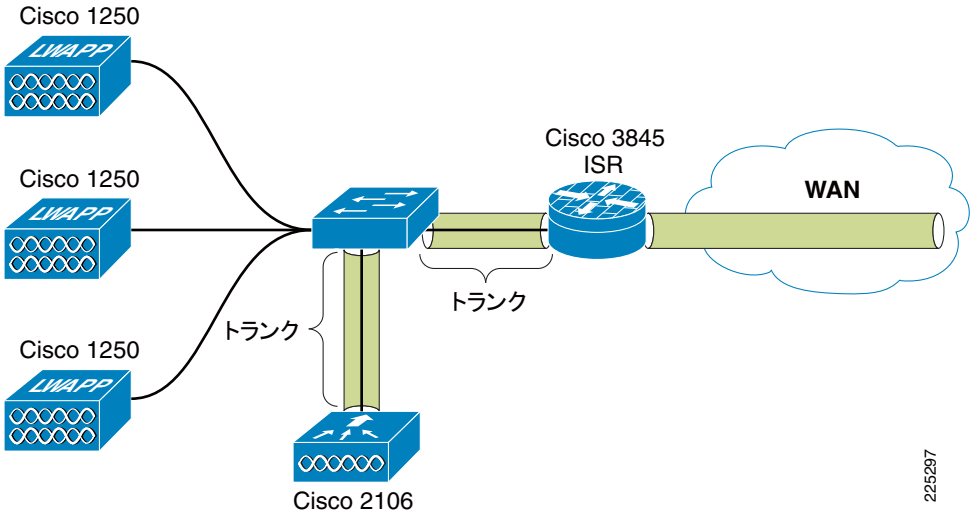
図 6-37　直列配置の ASA と NAC アプライアンス



ブランチ WLC 展開と IOS Firewall

図 6-38 に、ブランチ ネットワークをテストするための基本的なネットワーク設定の概略図を示します。このネットワークは、背後のキャンパス コアに IPSec VPN 経由で接続される Cisco 3845 ISR で構成されています。ブランチのローカル ネットワークは、dot1q トランク経由で ISR ルータに接続される 3750G スイッチで構成されています。3750G は、トランク接続を使用して 2106 WLC に接続されるほか、ローカル ネットワークに通じる 1250 AP にも接続されます。このシンプルなトポロジでは、この他のシスコ ISR、LAN スイッチ、および 2100 ファミリ WLC も同様に適用できます。

図 6-38　　ブランチのトポロジ

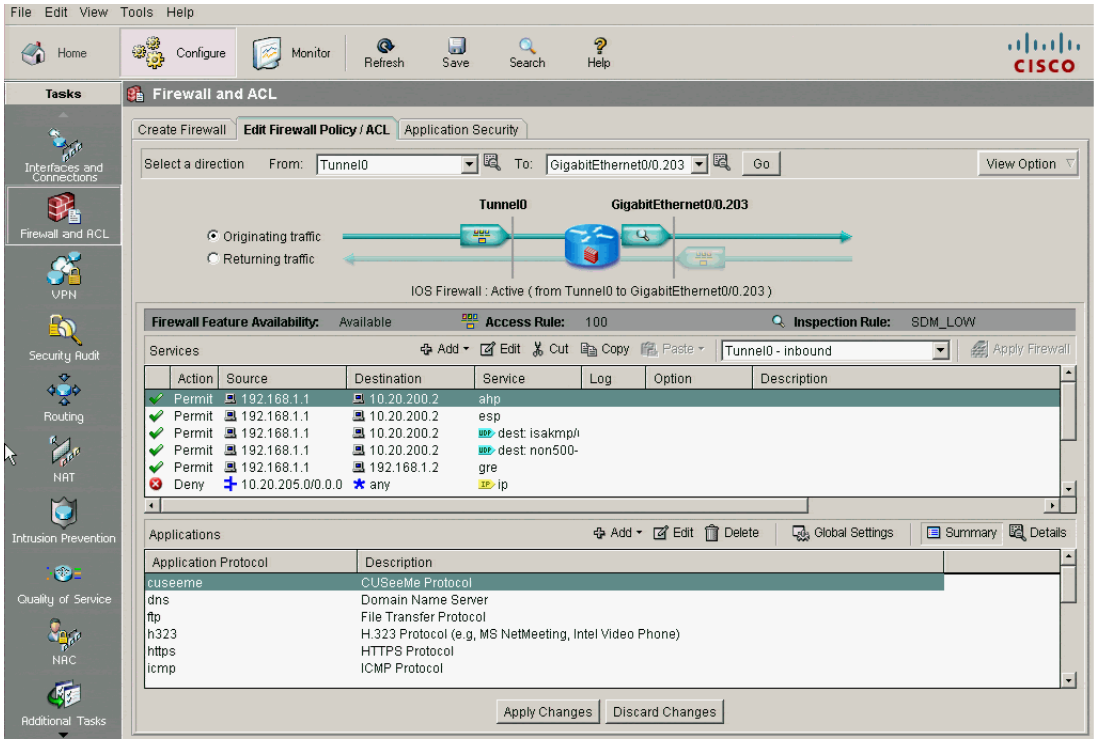


EAP 認証プロセスの一環として ID ベースで VLAN が割り当てられているブランチに対しても、キャンパス展開で説明した基本原則および WLC 設定を同様に適用できます。このブランチ例での相違点は、FWSM または ASA の代わりに IOS Firewall を使用することです。この例では IOS Firewall が使用されていますが、ASA を使用することもできます。

SDM

ASA および FWSM の場合と同様に、ISR の設定では、ファイアウォール設定を含めて設定用の GUI を利用できます。ISR の GUI インターフェイスは、Security Device Manager（SDM）と呼ばれます。図 6-39 に例を示します。

図 6-39　　SDM でのファイアウォールおよび ACL の設定



このブランチの例では、キャンパス展開を簡略化して、2 つの異なるポリシーを実装したものを使用しています。1 つのホストへの限定的な HTTPS アクセスに使用される基本のポリシーと、オープン アクセスに使用される別のポリシーがあります。

これらの設定の作成には、SDM が使用されています。関連する CLI 設定を次に示します。

一般的な IOS Firewall 検査ステートメント

```
ip inspect name SDM_LOW cuseeme
ip inspect name SDM_LOW dns
ip inspect name SDM_LOW ftp
ip inspect name SDM_LOW h323
ip inspect name SDM_LOW https
ip inspect name SDM_LOW icmp
ip inspect name SDM_LOW netshow
ip inspect name SDM_LOW rcmd
ip inspect name SDM_LOW realaudio
ip inspect name SDM_LOW rtsp
ip inspect name SDM_LOW sqlnet
ip inspect name SDM_LOW streamworks
ip inspect name SDM_LOW tftp
ip inspect name SDM_LOW tcp
ip inspect name SDM_LOW udp
ip inspect name SDM_LOW vdolive
ip inspect name SDM_LOW http
```

基本ポリシー

```
access-list 101 remark auto generated by SDM firewall configuration
access-list 101 remark SDM_ACL Category=1
```

```
access-list 101 deny   ip 10.20.200.0 0.0.0.3 any
access-list 101 permit icmp any 10.20.0.0 0.0.255.255 echo-reply
access-list 101 permit icmp any 10.20.0.0 0.0.255.255 time-exceeded
access-list 101 permit icmp any 10.20.0.0 0.0.255.255 unreachable
access-list 101 permit udp any eq bootps host 10.20.30.11 eq bootps
access-list 101 permit udp any host 10.20.30.11 eq domain
access-list 101 permit tcp any host 10.20.30.14 eq 443
access-list 101 deny   ip 10.0.0.0 0.255.255.255 any
access-list 101 deny   ip 172.16.0.0 0.15.255.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 deny   ip host 255.255.255.255 any
access-list 101 deny   ip host 0.0.0.0 any
access-list 101 deny   ip any any log


interface GigabitEthernet0/0.203
 description wlan203 subnet$FW_OUTSIDE$
 encapsulation dot1Q 203
 ip address 10.20.203.5 255.255.255.0
 ip access-group 101 in
 ip verify unicast reverse-path
 ip helper-address 10.20.30.11
 ip inspect SDM_LOW out
 snmp trap ip verify drop-rate
 standby 103 ip 10.20.203.1
 standby 103 preempt
 standby 103 track Serial0/0/0
```

オープン アクセス ポリシー

```
access-list 102 remark auto generated by SDM firewall configuration
access-list 102 remark SDM_ACL Category=1
access-list 102 deny   ip 10.20.200.0 0.0.0.3 any
access-list 102 permit icmp any 10.20.0.0 0.0.255.255 echo-reply
access-list 102 permit icmp any 10.20.0.0 0.0.255.255 time-exceeded
access-list 102 permit icmp any 10.20.0.0 0.0.255.255 unreachable
access-list 102 permit udp any eq bootps host 10.20.30.11 eq bootps log
access-list 102 permit ip 10.20.205.0 0.0.0.255 any
access-list 102 deny   ip 172.16.0.0 0.15.255.255 any
access-list 102 deny   ip 192.168.0.0 0.0.255.255 any
access-list 102 deny   ip 127.0.0.0 0.255.255.255 any
access-list 102 deny   ip host 255.255.255.255 any
access-list 102 deny   ip host 0.0.0.0 any
access-list 102 deny   ip any any log
interface GigabitEthernet0/0.205
 description wlan205 subnet$FW_OUTSIDE$
 encapsulation dot1Q 205
 ip address 10.20.205.5 255.255.255.0
 ip access-group 102 in
 ip verify unicast reverse-path
 ip helper-address 10.20.30.11
 ip inspect SDM_LOW out
 snmp trap ip verify drop-rate
 standby 105 ip 10.20.205.1
 standby 105 priority 110
 standby 105 preempt
 standby 105 track Serial0/0/0
```

H-REAP

ブランチ展開によっては、H-REAP AP を使用できる場合があります。基本的な設定原則は同一です。H-REAP での重要な注意点として、H-REAP は、現時点で ID ベースの VLAN 割り当てをサポートしていないことがあります。したがって、H-REAP の展開では、複数の SSID で異なるポリシーを実装するか、すべてのユーザに共通のファイアウォール ポリシーを使用する必要があります。

WLCM

Wireless LAN Controller Module（WLCM; 無線 LAN コントローラ モジュール）は、Cisco ISR ルータ用の統合型無線 LAN コントローラであり、ブランチ展開で有効となるもう 1 つの設計オプションです。WLCM と 21XX サービス コントローラの機能セットおよびキャパシティは、互いに類似しています。この章のブランチ テストでは 2106 を中心に説明していますが、設計および設定は、WLCM の展開にも同様に適用できます。

ハイ アベイラビリティ

2016 WLC では、物理的な冗長インターフェイスは提供されません。これらは 4400 シリーズのコントローラで提供されます。

ブランチ展開での主な WLAN ハイ アベイラビリティ機能には、次の 2 つがあります。

- ローカル EAP RADIUS 認証：認証アカウントをローカル アカウントとしてローカル WLC 上で提供し、中央の AAA サーバへの接続が失われた場合に EAP 認証を実行できます。
- AP フェールオーバー：ブランチにあるローカル WLC で障害が発生した場合に、AP を中央の WLC にフェールオーバーできます。効率的なソリューションにするには、ローカルで主に終端するトラフィックも含めて、クライアント トラフィックを伝送するための WAN キャパシティが十分に存在している必要があります。ブランチの AP と中央の WLC の間では、ラウンドトリップ時間が 100 ms 以内である必要があります。

テスト時のソフトウェア バージョン

デバイス	テストされたソフトウェア バージョン
Cisco Catalyst 6500	12.2(18)SXF8
Cisco WiSM	5.0.148.2
Cisco FWSM	3.1(4)
Cisco ASA	8.0(3)
Cisco ACS	4.2(1)
2106	5.0.148.2

CHAPTER 7

モバイル クライアント セキュリティのための CSA

有線アクセスと無線アクセスの機能を備えた安全なユニファイド ネットワークでは、セキュリティに対する統合型の多層防御アプローチが必要です。これには、脅威の効率的な検出および軽減に不可欠となる包括的なエンドポイント セキュリティ、およびポリシーの適用を含みます。

この章では、モバイル クライアントのエンドポイント セキュリティにおける Cisco Security Agent（CSA）の役割について概説します。また、エンドポイントが遭遇した脅威に対処し、ロケーションに基づいてポリシーを適用するための CSA のセキュリティ機能について概要を示します。さらに、これらの機能の設計および展開に役立つ実装ガイドラインについても説明します。

この章で言及しているソフトウェア実装、スクリーンショット、および動作は、P.7-58 の「テスト環境のハードウェアおよびソフトウェア」に示したリリースに基づいています。読者は、すでに CSA に精通していることを前提とします。

（注） この章では、CSA のモバイル クライアント セキュリティに関係する機能のみを取り上げます。

CSA の概要

CSA は、アップデート不要の攻撃保護機能、データ損失防止機能、およびシグニチャベースのアンチウイルス機能を 1 つのエージェントに統合した、最初のエンドポイント セキュリティ ソリューションです。これらの機能を独自の手法で組み合せることで、サーバやデスクトップを高度な Day Zero 攻撃から保護し、シンプルな管理インフラストラクチャの中で、利用規定と準拠ポリシーを適用します。

CSA は、次のようなさまざまな利点を備えています。

- アップデート不要の保護機能により、脆弱性が公開されるたびに急いでパッチを適用する必要がなくなるため、パッチに関連するダウンタイムと IT 費用を最小限に抑えることができます。
- 機密データの可視性と制御により、ユーザの操作や、ターゲットを絞ったマルウェアによって引き起こされるデータ損失を防止します。
- シグニチャベースのアンチウイルス保護機能により、既知のマルウェアを識別して削除します。

- 事前に定義された準拠ポリシーと利用規定を使用して、アクティビティの効率的な管理、レポーティング、および監査を行うことができます。
- Cisco Network Admission Control（NAC）、シスコ ネットワーク IPS デバイス、Cisco Security Monitoring, Analysis, and Response System（CS-MARS）など、先進のネットワーク セキュリティとエンドポイント セキュリティの統合およびコラボレーションを実現します。
- 中央集中型ポリシー管理により、動作ポリシー、データ損失防止、およびアンチウイルス保護の各機能がすべて、1 つの設定およびレポーティング インターフェイスに統合されます。

CSA ソリューションのコンポーネント

CSA ソリューションは、次のコンポーネントで構成されます。

- Cisco Management Center for Cisco Security Agents（CSA MC）

  Management Center は、すべての Cisco Security Agent の設定、管理、およびレポート生成を中央で一元的に行うためのスタンドアロン アプリケーションとして動作します。

- Cisco Security Agent

  デスクトップおよびサーバに展開され、定義済みのセキュリティ ポリシーおよび一般的な使用ポリシーを適用するホストベース エージェントです。これらのエージェントは CSA Management Center（MC）で管理され、CSA MC にレポートを送信しますが、各エージェントは自律的に動作し、CSA MC と通信できない場合でもセキュリティ ポリシーを適用します。これらのエージェントは、さまざまなデスクトップ / サーバ プラットフォームおよびオペレーティング システムでサポートされています。

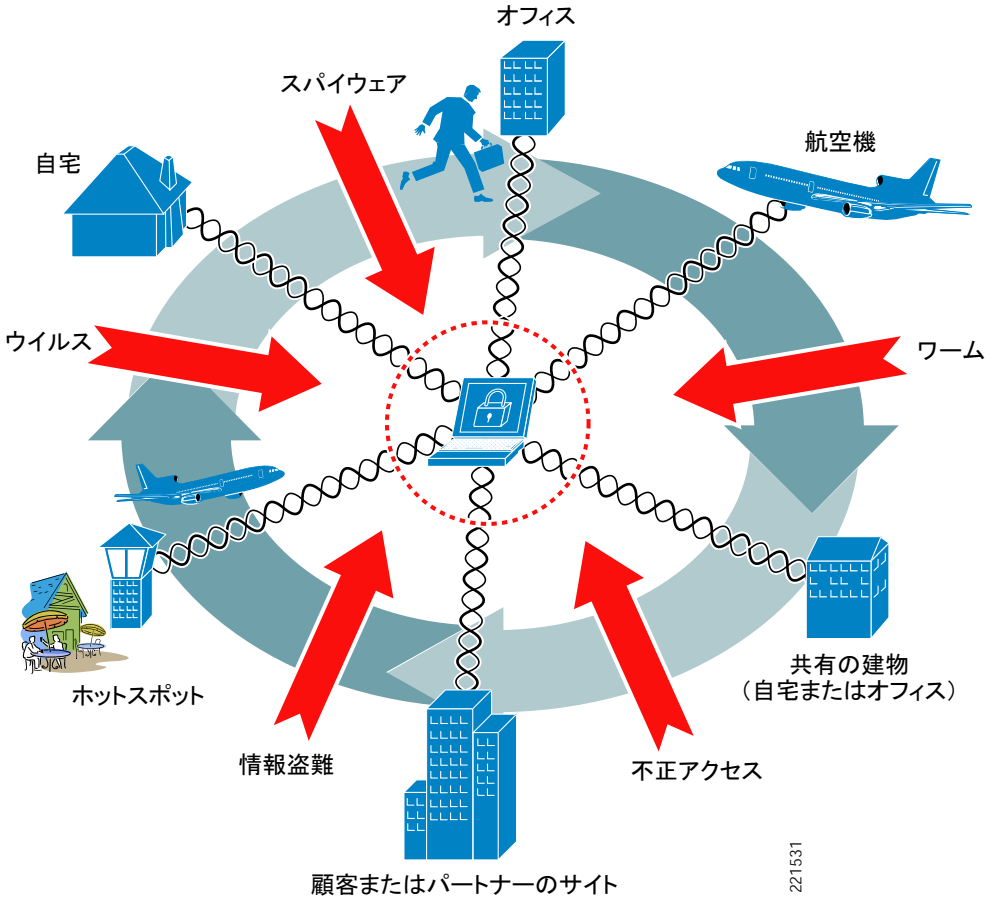
CSA の製品、プラットフォーム、および機能の詳細については、P.7-58 の「参考資料」に示した製品ページを参照してください。

モバイル クライアント セキュリティのための CSA の概要

一般的なクライアント保護のための CSA

モバイル クライアントと固定クライアント、およびサーバは、いずれもセキュリティ上のさまざまな脅威にさらされています。これには、ウイルス、ワーム、ボットネット、スパイウェア、情報盗難、および不正アクセスが含まれます。CSA は、アップデート不要の攻撃保護機能、データ損失防止機能、およびシグニチャベースのアンチウイルス機能を単一のエージェントで提供するほか、利用規定および準拠ポリシーを適用する機能を提供することにより、クライアントとサーバをこれらの攻撃から防御するための包括的なエンドポイント セキュリティを実現します（図 7-1 を参照）。

図 7-1　クライアントおよびサーバが遭遇するセキュリティ上の一般的な脅威

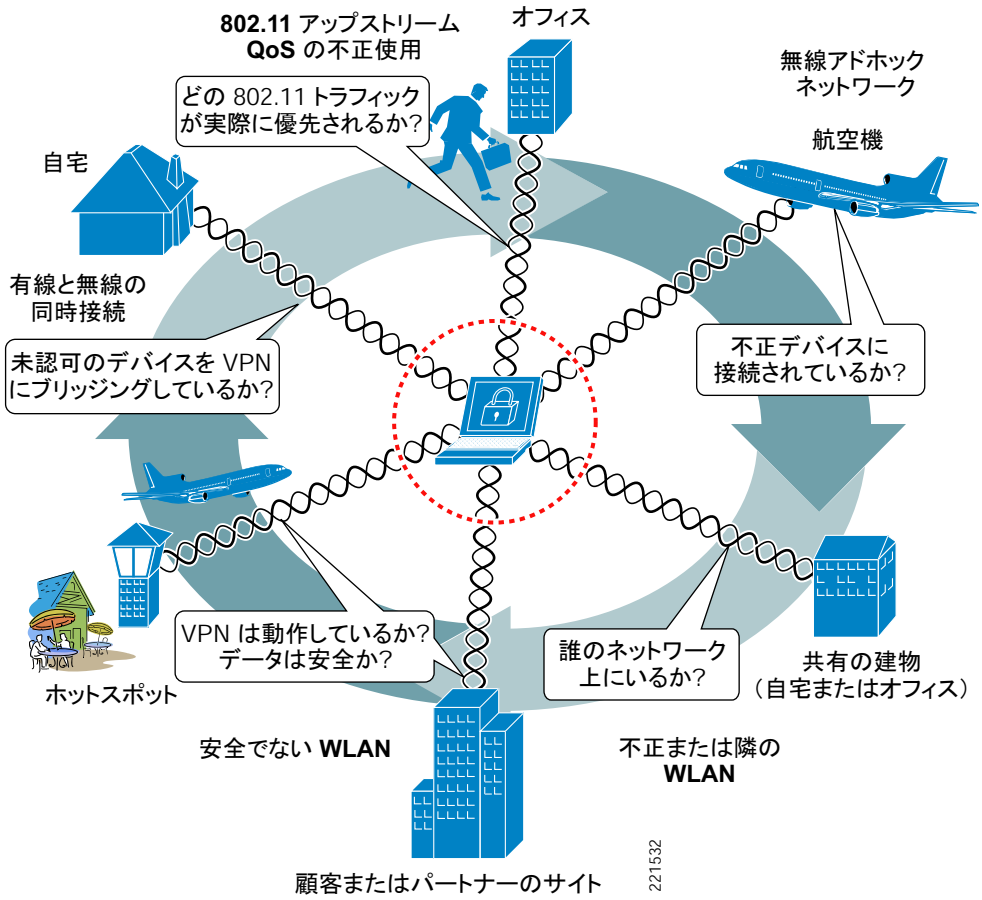


エンドポイントのセキュリティは、クライアントとサーバ自体、および接続先となる企業ネットワークを保護するもので、セキュリティに対する統合型の多層防御アプローチでは重要な要素です。

モバイル クライアント保護のための CSA

多くのモバイル クライアントは、意識的または無意識に、有線または無線の各種ネットワークとのアソシエーションを確立します。この対象には、企業ネットワーク、ホットスポット、ホーム ネットワーク、パートナーのネットワーク、無線アドホック ネットワーク、不正なネットワークなどがあります。このため、さらに多くのセキュリティ上の脅威にさらされます（図 7-2 を参照）。

図 7-2　モバイル クライアントが遭遇する追加的なセキュリティ上の脅威



CSA は、一般的なエンドポイント保護を拡張して、モバイル クライアントが遭遇する一般的な脅威に対処し、適用されているセキュリティ ポリシーを現在のロケーションに応じて調整する機能を提供します。

表 7-1 に、モバイル クライアントが遭遇するセキュリティ上の一般的な脅威と追加的な脅威、それらの脅威がもたらすリスク、および脅威を軽減するために使用できる CSA 機能の概要を示します。これらの各領域については、以降の項でさらに詳しく説明します。

表 7-1　モバイル クライアントに関係するセキュリティ上の一般的な脅威および CSA の軽減機能

モバイル クライアントに関係するセキュリティ上の脅威	セキュリティ上の懸念事項	CSA の機能
無線アドホック接続	• 通常、セキュリティで保護されず、認証されず、暗号化されない接続 • 権限のないデバイスや不正デバイスに接続されるリスクが高い	• 事前定義の無線アドホック ルール モジュール[1] • 無線アドホック トラフィックの制限

表 7-1　モバイル クライアントに関係するセキュリティ上の一般的な脅威および CSA の軽減機能

有線と無線の同時接続	• セキュリティで保護されていない無線ネットワークまたは不正デバイスから、有線ネットワークにトラフィックがブリッジされるリスク • 標準のネットワーク セキュリティ処理の迂回	• 事前定義の有線と無線の同時接続ルール モジュール[1] • イーサネットがアクティブな場合に無線トラフィックを制限する
企業以外のネットワーク、セキュリティで保護されていないネットワーク、未認可ネットワーク、不正ネットワーク、または不適切なネットワークへの接続	• 認証または暗号化が使用されていないか、使用されていても強力なものでない • スニッフィング、MITM、不正なネットワーク接続などのリスク • 情報盗難リスクの増大	• ローミング時に VPN の使用を強制する事前定義ルール モジュール[1] • 企業以外のネットワーク上で厳密な制御を適用するためのロケーション認識型ポリシーの適用[1]
802.11 アップストリーム QoS の不正使用および未サポート	• トラフィック QoS マーキングへの違反が、DoS 攻撃(サービス拒絶攻撃)、帯域幅の占有、プライオリティ キューのジャンピングなどを試行するために不正使用される恐れがある • 多くのレガシー デバイスおよびアプリケーションでは、QoS マーキングがサポートされていない	• Trusted QoS Marking[2] • クライアントから送信されるパケットに対する DiffServ 設定のマーキングまたは再マーキングによる、アップストリーム QoS ポリシーの適用

1. CSA v5.2 では、CSA のロケーション認識型ポリシー適用機能が導入されました。無線アドホック接続、および有線と無線の同時接続に対処する事前定義のルール モジュールにより、ローミング時に VPN の使用を強制するほか、クライアントの接続先 SSID を限する機能を備えています。
2. CSA v5.0 では、CSA Trusted QoS Marking 機能が導入されました。

(注) モバイル クライアント用の CSA ポリシーは、全般的な CSA セキュリティ ポリシーを補完および拡張するために使用します。前の項で説明したように、固定クライアントとモバイル クライアントの両方、およびサーバに対して、一般的なエンドポイント保護を提供する全般的なポリシーがすでに適用されている必要があります。

CSA および補完的なシスコ セキュリティ機能

Cisco Unified Wireless およびシスコ セキュリティ ポートフォリオは、セキュリティに対する統合型の多層防御アプローチをサポートするための補完的なセキュリティ機能を数多く備えています。たとえば、以降で説明するように、CSA によって対処されるモバイル クライアント セキュリティ上の 2 つの脅威については、補完機能や代替機能で検出して軽減できます。

無線アドホック接続

CSA は、無線アドホック接続がもたらす脅威に対して、クライアント エンドポイントの観点から対処し、このタイプの接続をホストするクライアントがどのロケーションに存在していても、常にクライアントを保護します。

この機能を補完するには、無線アドホック ネットワークおよび不正ネットワークの脅威を Cisco WLAN Controller（WLC; WLAN コントローラ）の IDS/IPS 機能で検出して軽減することにより、この脅威にネットワーク側から対処します。

これらの機能を両方とも利用することで、セキュリティに対するさらに包括的なアプローチが実現します。CSA は、すべての環境でクライアントを保護します。WLC は、企業ネットワーク上のこのようなアクティビティを可視化して、制御する機能を提供します。

Cisco WLC の無線 IDS/IPS 機能の詳細については、P.7-58 の「参考資料」を参照してください。

有線と無線の同時接続

CSA は、イーサネット ポートがアクティブになっている場合は無線ネットワーク上のトラフィックを制限し、有線と無線の同時接続によってもたらされる脅威に対処します。

シスコでは、この脅威に Cisco Secure Services Client（CSSC）を使用して対処する、クライアントベースの代替アプローチを提供しています。CSSC は、有線および無線のネットワークへのセキュア アクセスで必要となる、ユーザ ID、デバイス ID、およびネットワーク アクセス プロトコルを管理するためのソフトウェア クライアントです。機能の 1 つに、有線ポートがアクティブな場合は無線アクセスをブロックする機能があります。ただし、主な役割は、有線および無線ネットワーク用の 802.1X サプリカントを提供して、ローカル ネットワーク アクセス プロファイルを中央で管理できるようにすることです。これらのプロファイルによって、適切な認証パラメータおよび暗号化パラメータの使用を強制します。

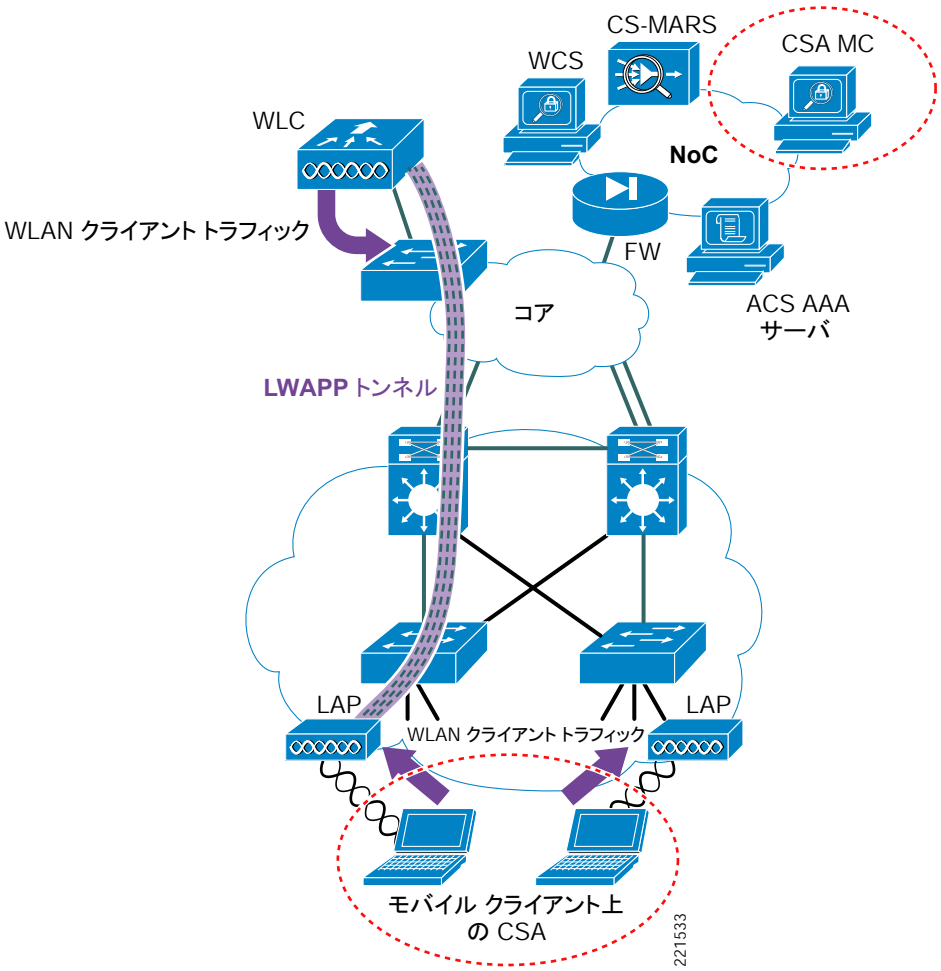
これらの 2 つの製品は、いずれも有線と無線の同時接続に対処する機能を備えていますが、各製品の完全な機能セットおよび役割は大幅に異なり、ネットワーク セキュリティ上は互いを補完する役割を担っています。CSA は、充実したエンドポイント保護、データ損失防止、およびアンチウイルスの機能を提供します。CSSC は、セキュア アクセスのための強力な認証フレームワークを提供します。

CSSC の詳細については、P.7-58 の「参考資料」を参照してください。

CSA と Cisco Unified Wireless Network の統合

Cisco Unified Wireless Network アーキテクチャに CSA を統合するには、クライアントに CSA を展開し、Cisco Management Center for Cisco Security Agents（CSA MC）を展開します（図 7-3 を参照）。

図 7-3　Cisco Unified Wireless Network アーキテクチャでの CSA の統合

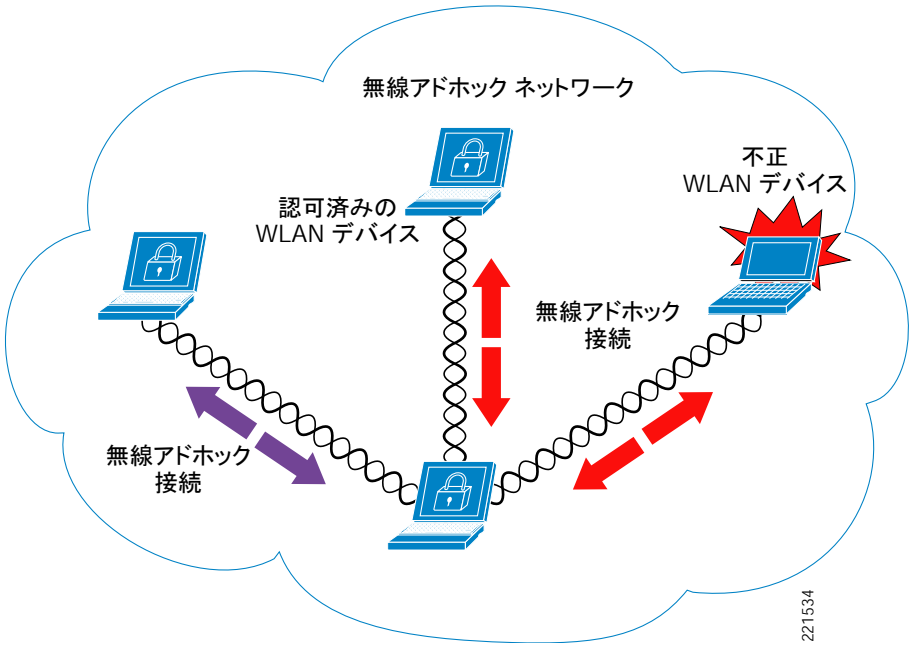


無線アドホック接続

無線アドホック ネットワークとは、2 つ以上の無線ノードがピアツーピアで直接通信し、無線ネットワークのインフラストラクチャが存在しない状態です。これは、Independent Basic Service Set（IBSS; 独立型基本サービス セット）と呼ばれる場合もあります。

無線アドホック ネットワークは、ホスト間で通信を迅速に確立することを目的として、通常は一時的に形成されます。たとえば、自然発生的な会議の開催中に、または自宅内のホスト間で、ファイルを交換する場合などです（図 7-4 を参照）。

図 7-4　　無線アドホック ネットワークの例



無線アドホック ネットワークに関するセキュリティ上の懸念事項

無線アドホック接続は、一般的にはセキュリティ リスクと見なされます。その理由は次のとおりです。

- 通常、セキュリティが不足しているか、まったくない

  無線アドホック接続は、通常、セキュリティをほとんど導入しない状態で実装されています。認証、アクセス コントロール、暗号化などは実行されません。結果として、許可されたデバイス間であってもセキュリティ リスクが発生します。クライアント自体だけでなく、転送されるデータ、接続先となるクライアントおよびネットワークもリスクの対象です。

- エンドポイントが不正デバイスに接続されるリスクが非常に高い

  無線アドホック接続ではセキュリティが存在しないことが多いため、エンドポイントは不正デバイスに接続される恐れがあります。

- 許可されたデバイスを使用していても、エンドポイントが安全でない接続を経由するリスクが非常に高い

  無線アドホック接続ではセキュリティが存在しないことが多いため、これはこの接続に特有のリスクとなります。

- 不正な無線アドホック デバイスがセキュアな有線ネットワークにブリッジされるリスク

  無線アドホック接続と有線接続を同時に使用する場合、不正なデバイスが有線ネットワークにブリッジされる恐れがあります。

- Microsoft Windows のネイティブ WLAN クライアントの脆弱性

  無線アドホック プロファイルが設定されている場合、Microsoft Wireless Auto Configuration のデフォルト動作は、不正デバイスに接続される恐れのある重大なリスクとなります。具体的には、ユーザは 802.11 無線が有効になっていることすら認識していない場合があるた

めです。Microsoft Wireless Auto Configuration 機能とは、Windows Server 2003 の場合は Wireless Configuration サービス、Windows XP の場合は Wireless Zero Configuration サービスを指します。

この脆弱性および不正利用の手口の詳細については、P.7-58 の「参考資料」を参照してください。

CSA の事前定義の無線アドホック ルール モジュール

CSA v5.2 では、無線アドホック接続に対処するために、**Prevent Wireless Adhoc communications** と呼ばれる事前定義の Windows ルール モジュールが導入されました。

このルール モジュールを適用することにより、無線アドホック接続でエンドポイントを脅威から保護できます。

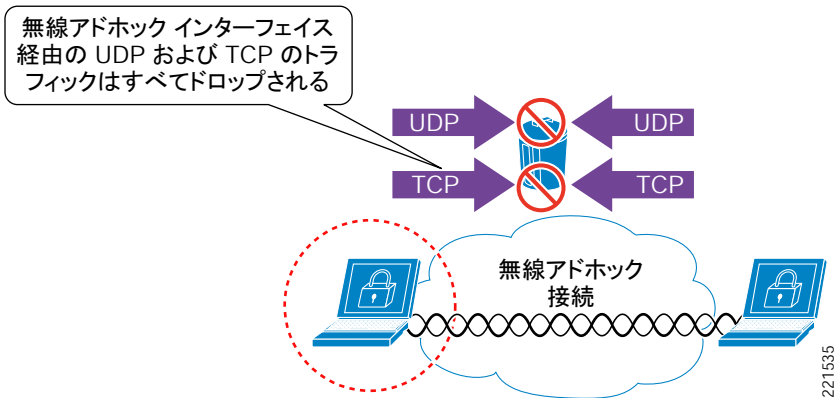
事前定義ルール モジュールの動作

次に、事前定義の無線アドホック Windows ルール モジュールのデフォルト動作について概要を示します。

無線アドホック接続がアクティブになっている場合、アクティブな無線アドホック接続上の UDP および TCP のトラフィックは、アプリケーションおよび IP アドレスとは無関係にすべて拒否されます。

図 7-5 を参照してください。

図 7-5　CSA の事前定義の無線アドホック Windows ルール モジュールの動作



次に、事前定義の無線アドホック Windows ルール モジュールのデフォルト動作を示します。

- アクティブな無線アドホック接続上で UDP または TCP のトラフィックが検出された場合、ルール モジュールが呼び出されます。これは、他のネットワーク接続がアクティブになっているかどうかは関係しません。
- 無線アドホック接続でルーティングされる UDP および TCP のトラフィックは、すべてドロップされます。
- 無線アドホック以外の接続上にあるトラフィックは、このルール モジュールの影響を受けません。
- ユーザ クエリーは実行されません。
- メッセージがログに記録されます。

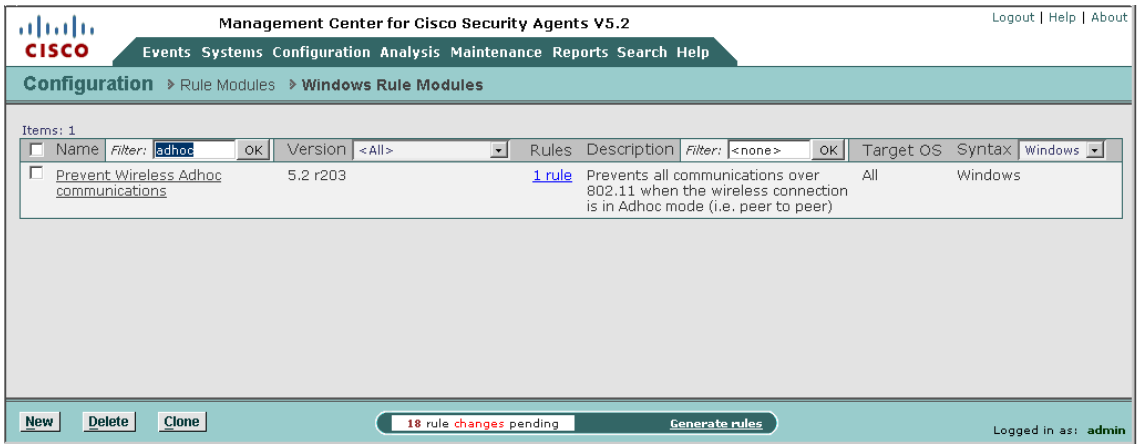
- アクティブな無線アドホック接続が存在しない場合、ルール モジュールは失効します。
- ルール モジュールの失効後は、ロギングが発生しません。

事前定義ルール モジュールの設定

事前定義の無線アドホック ルール モジュールは、**Prevent Wireless Adhoc communications** という名前の Windows ルール モジュールです。

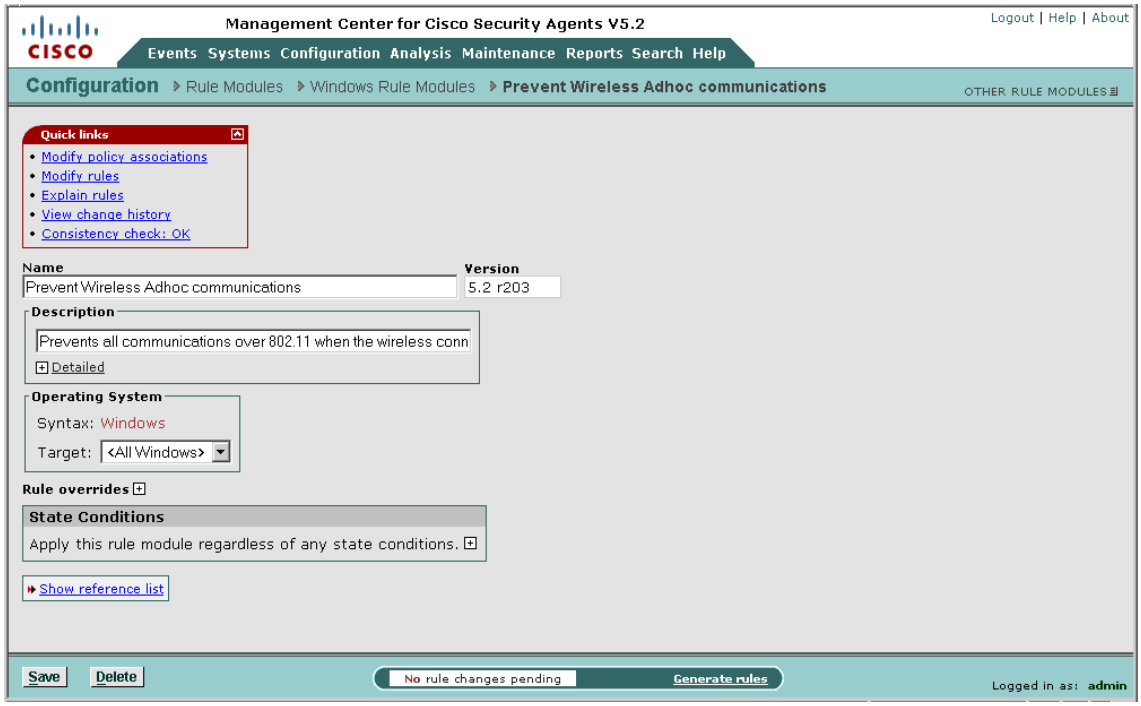
CSA MC で **Configuration -> Rule Modules -> Rule Modules [Windows]** を参照すると、見つけることができます。すばやく検索するには、**adhoc** という名前でフィルタを定義します（図 7-6 を参照）。

図 7-6　事前定義の無線アドホック Windows ルール モジュールのリスト



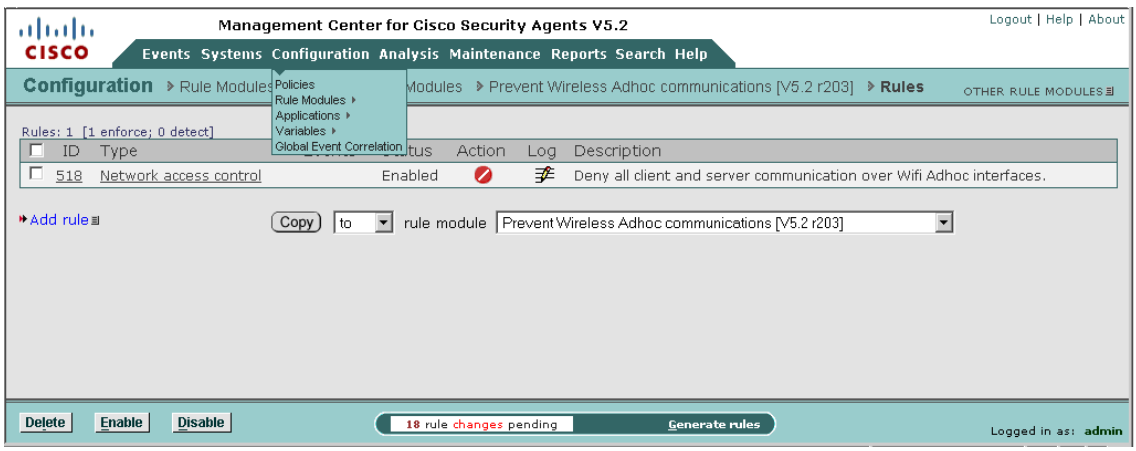
ルール モジュールの名前をクリックすると、このルール モジュールの説明、オペレーティング システム、および状態条件が表示されます（図 7-7 を参照）。

図 7-7　事前定義の無線アドホック Windows ルール モジュールの定義



Modify rules リンクをクリックすると、関連付けられているルールが表示されます（図 7-8 を参照）。ルール モジュールのリストで **1 rule** リンクをクリックして、このルールに直接アクセスすることもできます。

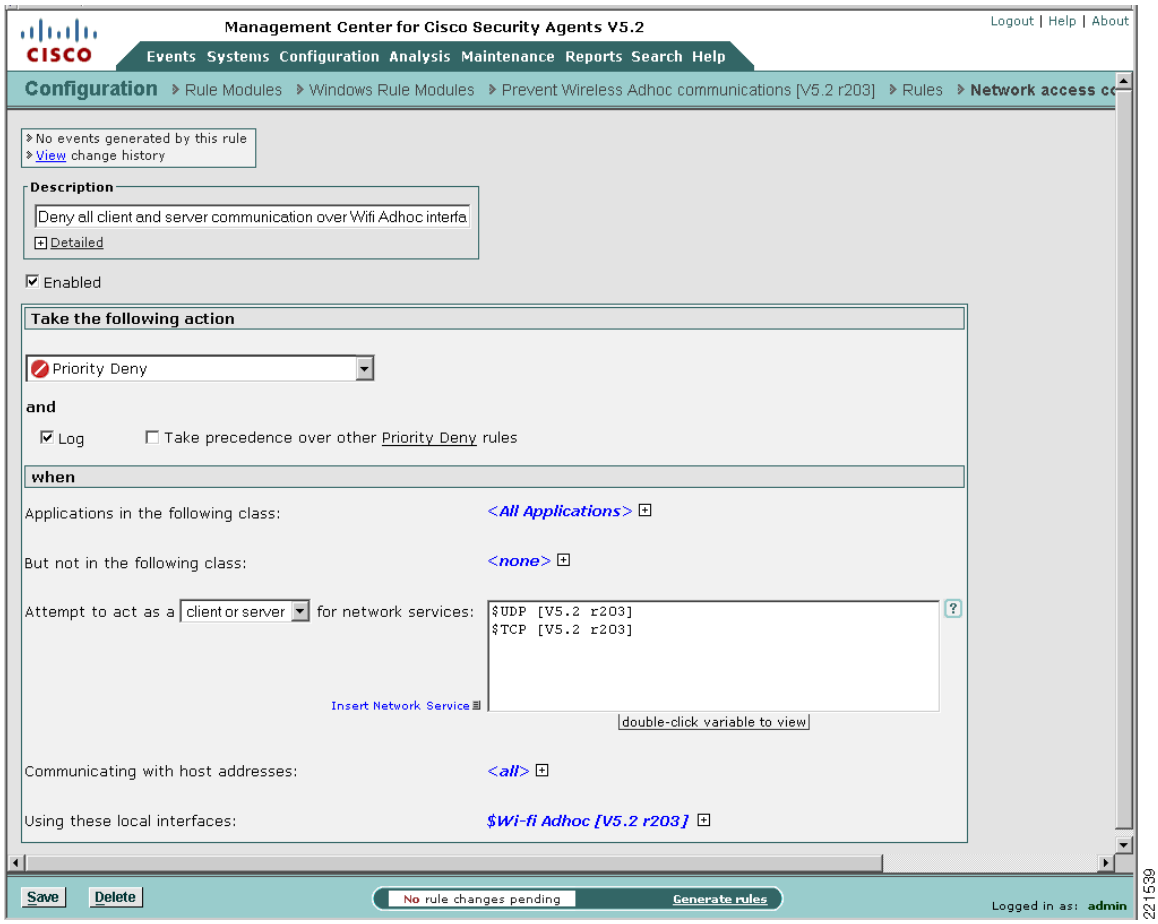
図 7-8　事前定義の無線アドホック Windows ルール モジュールに関連付けられているルール



（注）　ルールの番号は、使用されている個々のシステムに応じて異なります。

ルール名をクリックすると、ルールの詳細設定が表示されます（図 7-9 を参照）。

図 7-9　事前定義の無線アドホック ルールの設定



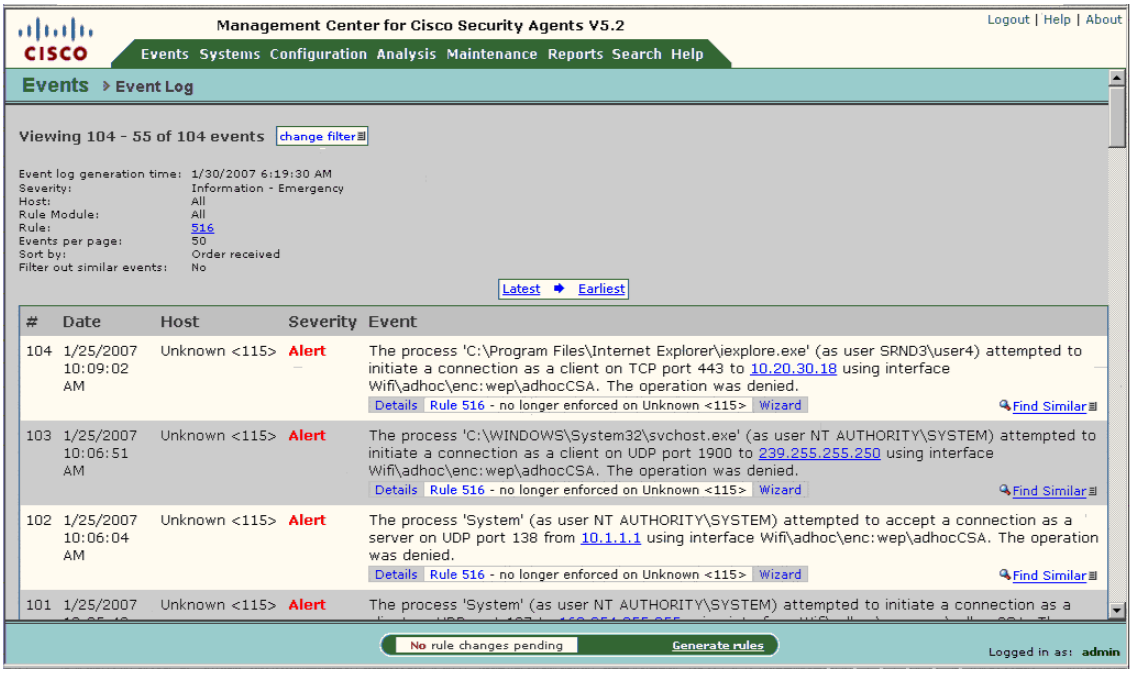
これは、無線アドホック接続上の UDP および TCP のトラフィックを、アプリケーションおよび IP アドレスとは無関係にすべて拒否するルールの詳細設定を示しています。

事前定義ルール モジュールのロギング

事前定義の無線アドホック Windows ルール モジュールでは、イベント ロギングがデフォルトで有効になっています。

ルール モジュールがトリガーされる一意インスタンスごとに、アラートが生成されます。デフォルトでは、同一のシナリオについてイベント ログ エントリが作成されるのは、1 時間ごとに 1 回のみです。図 7-10 に、ログ エントリの例を示します。

図 7-10　事前定義の無線アドホック Windows ルール モジュールによって生成される CSA MC イベント ログ



無線アドホック ルールのカスタマイズ

無線アドホック ポリシーの適用機能を実装しようとするお客様は、次のオプションによってカスタマイズした無線アドホック ルール モジュールを導入することを検討してください。

- ルールのアクションとしてカスタマイズしたユーザ クエリー：ユーザ クエリーを提示する独自の無線アドホック ルール モジュールを開発して、無線アドホック接続に伴うリスクをエンド ユーザに通知することにより、セキュリティ リスクに関する知識をユーザに伝達できます。
- テスト モードのカスタマイズしたルール モジュール：カスタマイズした無線アドホック ルール モジュールをテスト モードで展開すると、管理者は、エンド ユーザ側の操作性を変更しないまま、無線アドホック接続のイベントを表示できるようになります。

独自のルール モジュールの開発例については、P.7-49 の「独自のルール モジュールの開発例」に示します。

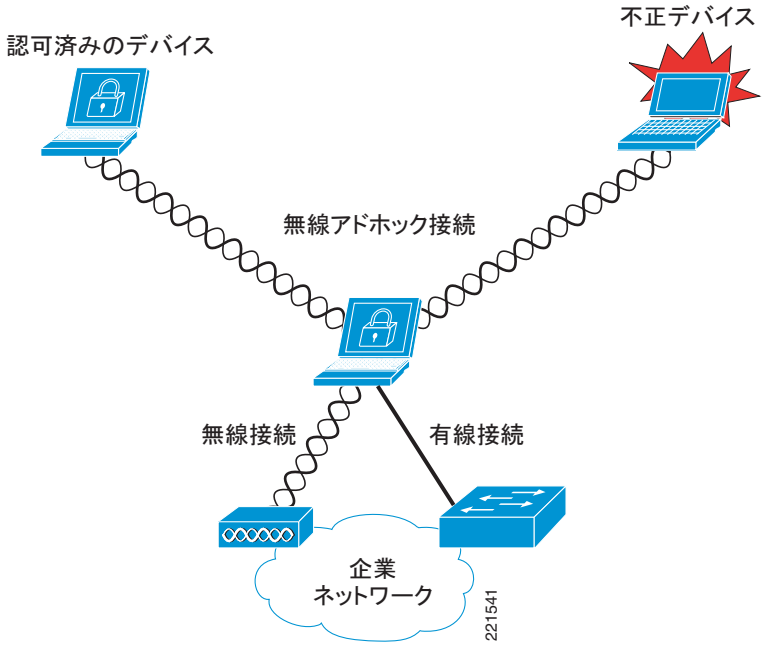
（注） 業務上の要件およびセキュリティ ポリシーはお客様ごとに異なるため、事例ごとに再確認した上で適用し、展開する必要があります。

有線と無線の同時接続

有線と無線の同時接続が発生するのは、クライアントが有線ネットワーク上（通常はイーサネット）でアクティブな接続を保持すると同時に、オープン WLAN、セキュア WLAN、無線アドホック ネットワークなどへのアクティブな無線接続も保持している場合です（図 7-11 を参照）。

この状況が発生するのは、通常、ユーザが会議中に WLAN に接続した後、自分のデスクに戻ってドッキング ステーションに接続し直した場合です。

図 7-11　有線と無線の同時接続



有線と無線の同時接続に関するセキュリティ上の懸念事項

有線と無線の同時接続は、一般にはセキュリティ リスクと見なされます。その理由は次のとおりです。

- 不正なデバイスがセキュアな有線ネットワークにブリッジされるリスク

  有線と無線の接続を同時に使用する場合は、不正なデバイスが有線ネットワークにブリッジされる恐れがあります。

- 許可されたデバイスが有線ネットワークにブリッジされるリスク

  有線と無線の接続を同時に使用する場合は、許可されたデバイスが有線ネットワークにブリッジされ、ネットワークのセキュリティ処理およびポリシーを迂回する恐れがあります。

- エンド ユーザの認識の欠如

  ユーザは、各自の 802.11 無線を有効にしたまま、不用意に放置することが多くあります。この行為は、クライアント上に設定されている無線プロファイルによっては、不正なデバイスがクライアントに無線で接続し、セキュリティ保護のない（無線アドホック）プロファイルを使用して有線ネットワークにブリッジする機会を与える恐れがあります。この状況が発生するのは、通常、公共のホットスポット、未認証のホーム WLAN、セキュリティ保護のないパートナー サイトなど、企業以外の WLAN をユーザが使用し、しばらく経ってから企業 LAN などの有線ネットワークに接続する場合です。

CSA の事前定義の有線と無線の同時接続ルール モジュール

CSA v5.2 では、有線と無線の同時接続に対処するために、**Prevent Wireless if Ethernet active** と呼ばれる事前定義のルール モジュールが導入されました。この事前定義のルール モジュールは、802.11 a/b/g/n、オープン、アドホック、およびセキュア 802.11 無線接続を含むすべての 802.11 無線接続を対象としています。3G ネットワークへの接続など、802.11 以外の無線接続は含まれていませんが、独自のルールを作成することで対象にできます。

このルール モジュールを適用すると、全般的なネットワーク ポリシーが適用され、ネットワークのインフラストラクチャおよびリソースに加えて、クライアント自体も保護できます。

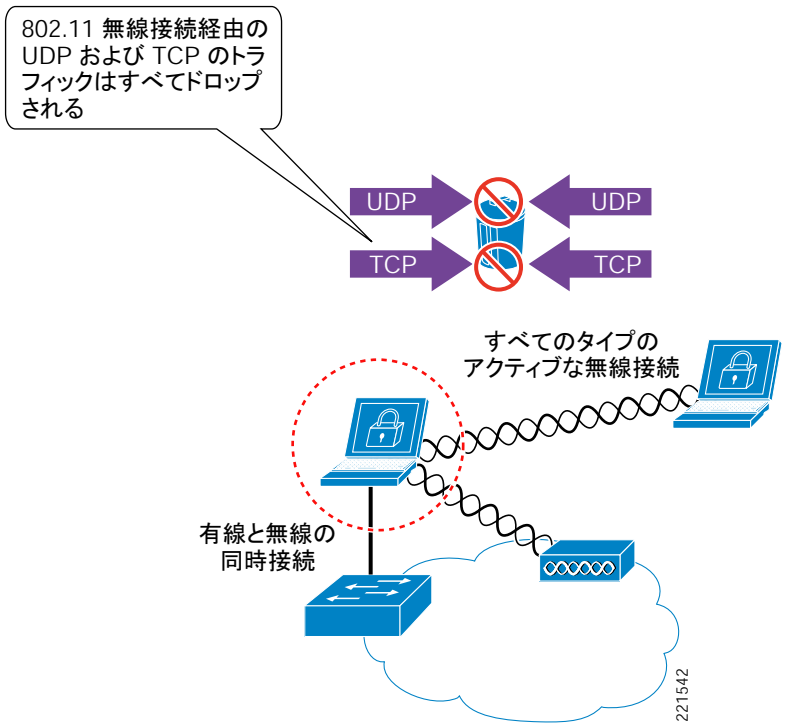
エンドポイントに CSSC が展開されている場合は、この脅威を阻止するための代替手段として、このクライアントの有線と無線の同時接続機能を利用できます。

事前定義ルール モジュールの動作

次に、事前定義の有線と無線の同時接続 Windows ルール モジュール（図 7-12 を参照）のデフォルト動作について概要を示します。

イーサネット接続がアクティブになっている場合、アクティブな 802.11 無線接続上の UDP および TCP のトラフィックは、アプリケーションおよび IP アドレスとは無関係にすべて拒否されます。

図 7-12　CSA の事前定義の有線と無線の同時接続 Windows ルール モジュールの動作



事前定義の有線と無線の同時接続 Windows ルール モジュールは、次の要素を含んでいます。

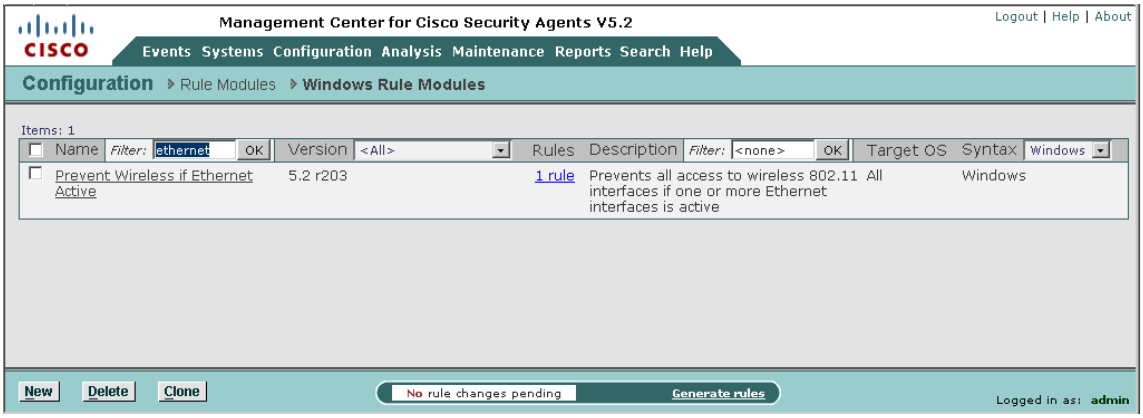
- イーサネット接続がアクティブになっていて、任意のアクティブな 802.11 無線接続上で UDP または TCP のトラフィックが検出された場合、ルール モジュールが呼び出されます。これは、オープン、アドホック、セキュア無線接続など、802.11 接続のタイプは関係しません。
- 802.11 無線接続でルーティングされる UDP および TCP のトラフィックは、すべてドロップされます。
- 802.11 無線以外の接続上にあるトラフィックは、このルール モジュールの影響を受けません。
- ユーザ クエリーは実行されません。
- メッセージがログに記録されます。
- アクティブなイーサネット接続が存在しない場合、ルール モジュールは失効します。
- ルール モジュールの失効後は、ロギングが発生しません。

事前定義ルール モジュールの設定

事前定義の有線と無線の同時接続ルール モジュールは、**Prevent Wireless if Ethernet active** という名前の Windows ルール モジュールです。

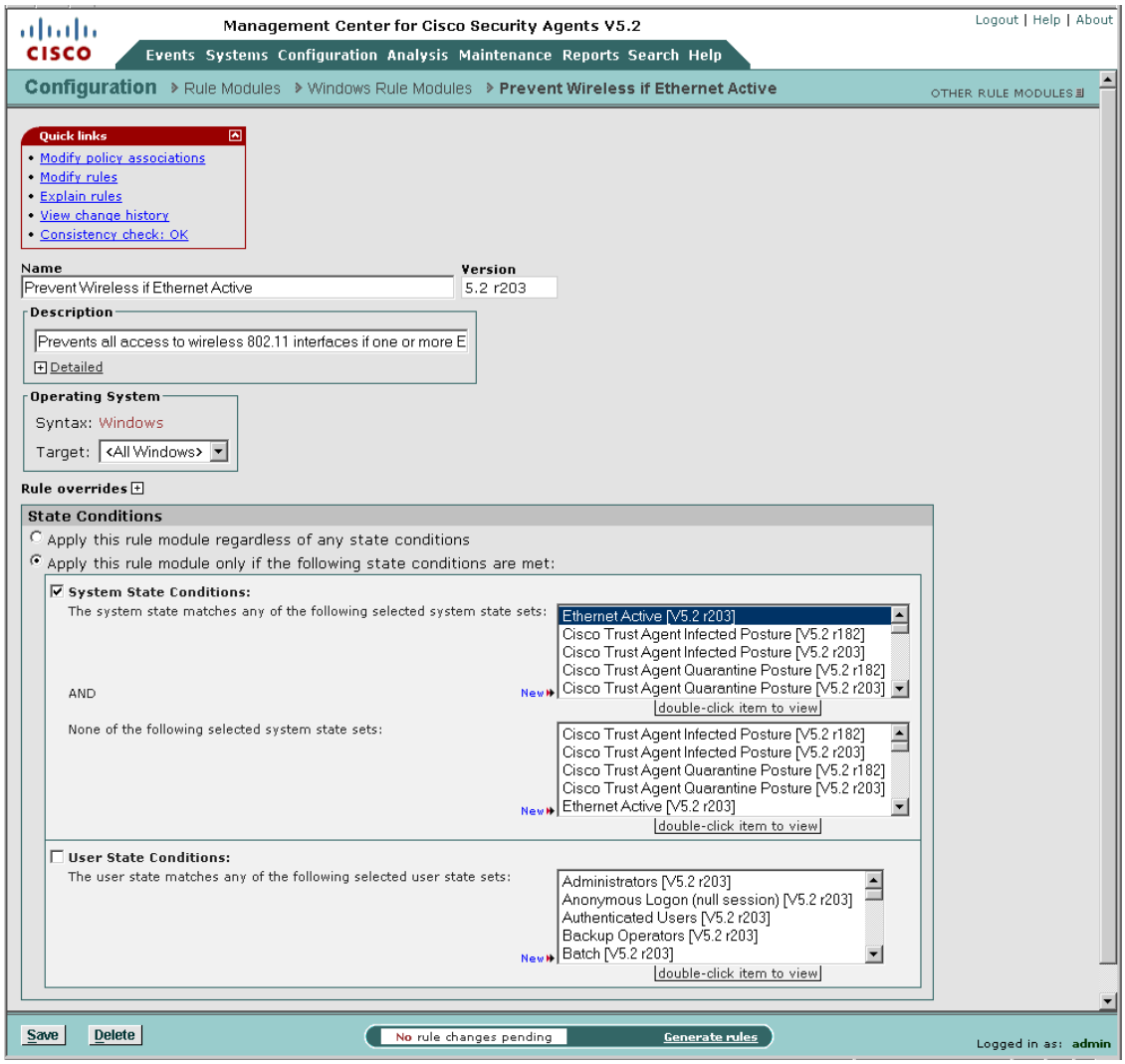
CSA MC で **Configuration -> Rule Modules -> Rule Modules [Windows]** を参照すると、見つけることができます（図 7-13 を参照）。すばやく検索するには、**ethernet** という名前でフィルタを定義します。

図 7-13　事前定義の有線と無線の同時接続 Windows ルール モジュールのリスト



ルール モジュールの名前をクリックすると、このルール モジュールの説明、オペレーティング システム、および状態条件が表示されます（図 7-14 を参照）。

図 7-14　事前定義の有線と無線の同時接続 Windows ルール モジュールの設定

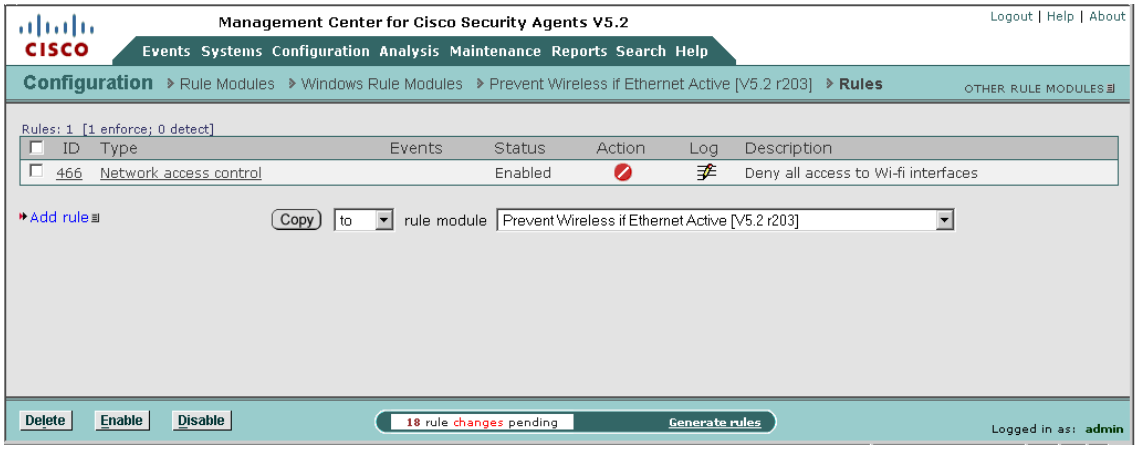


これは、このルールに存在する状態条件を示しています。この場合、ルールが呼び出されるにはイーサネット インターフェイスがアクティブになっている必要があります。

Modify rules リンクをクリックすると、ルールの概要が表示されます（図 7-15 を参照）。

ルール モジュールのリストで **1 rule** リンクをクリックして、このルールに直接アクセスすることもできます（図 7-13 を参照）。

図 7-15　事前定義の有線と無線の同時接続 Windows ルール モジュールに関連付けられているルール



（注）　ルールの番号は、使用されている個々のシステムに応じて異なります。

ルール名をクリックすると、ルールの詳細設定が表示されます（図 7-16 を参照）。

図 7-16　事前定義の有線と無線の同時接続ルールの設定

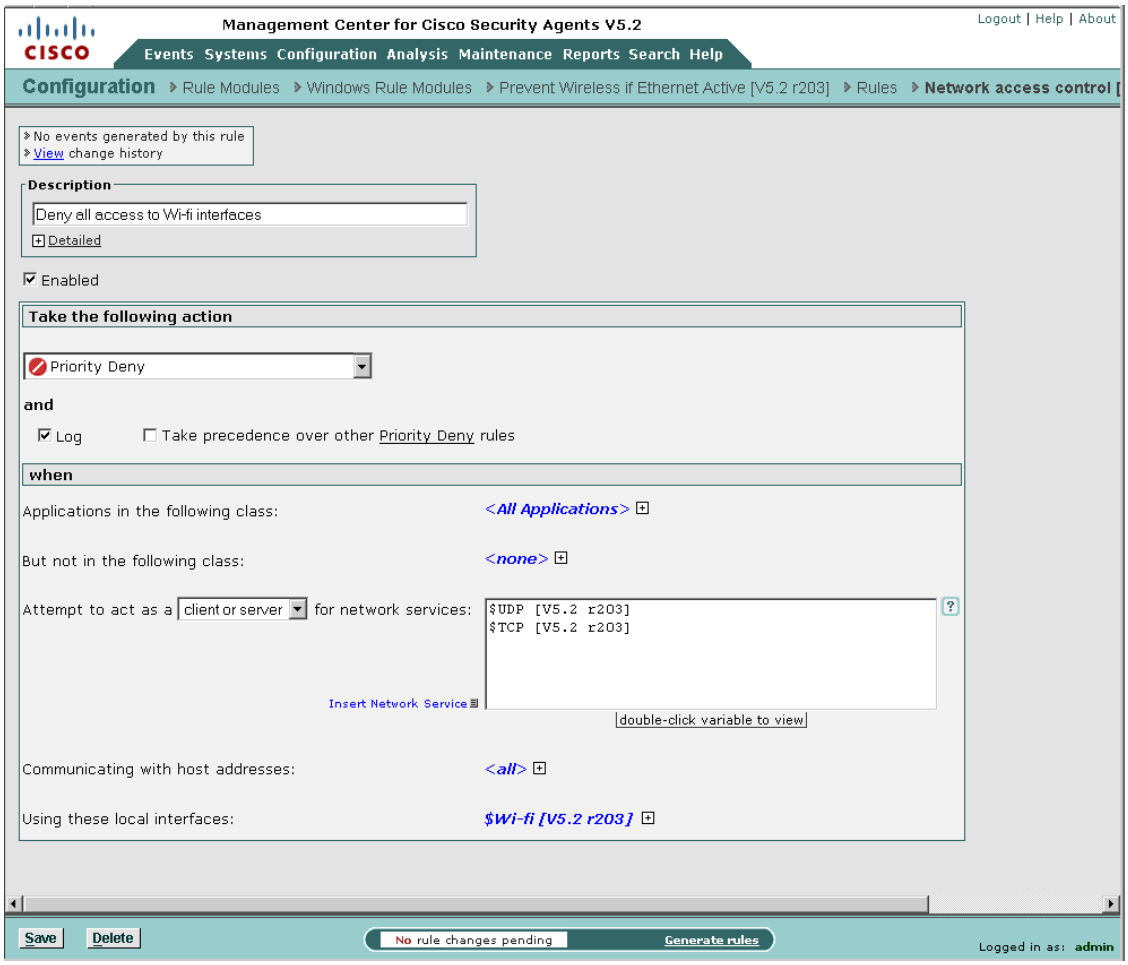


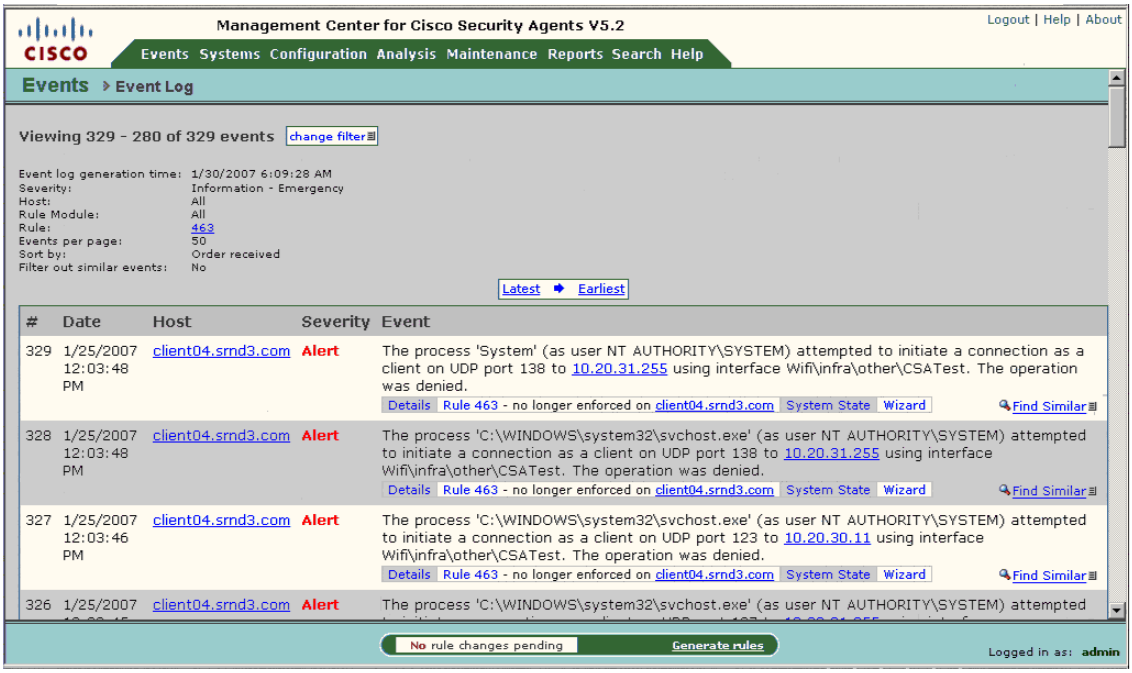
図 7-16 は、イーサネット接続がアクティブになっている場合、アプリケーションおよび IP アドレスとは無関係に、アクティブな 802.11 無線接続上の UDP および TCP のトラフィックをすべて拒否するルールの詳細設定を示しています。

事前定義ルール モジュールのロギング

事前定義の有線と無線の同時接続 Windows ルール モジュールでは、イベント ロギングがデフォルトで有効になっています。

ルール モジュールがトリガーされる一意インスタンスごとに、アラートが生成されます。デフォルトでは、同一のシナリオについてイベント ログ エントリが作成されるのは、1 時間ごとに 1 回のみです。図 7-17 に、ログ エントリの例を示します。

図 7-17　事前定義の有線と無線の同時接続ルール モジュールによって生成される CSA MC イベント ログ



有線と無線の同時接続ルールのカスタマイズ

有線と無線の同時接続ポリシーの適用機能を実装しようとするお客様は、次のオプションによってカスタマイズした有線と無線の同時接続ルール モジュールを導入することを検討してください。

- ルールのアクションとしてカスタマイズしたユーザ クエリー：ユーザ クエリーを提示する独自の有線と無線の同時接続ルール モジュールを開発して、有線と無線の同時接続に伴うリスクをエンド ユーザに通知することにより、セキュリティ リスクに関する知識をユーザに伝達できます。
- ロケーションに基づいてカスタマイズしたルール モジュール：有線と無線の同時接続に関する独自のルール モジュールを開発すると、802.11 無線接続が企業 WLAN 宛ての場合は有線と無線の同時接続を許可し、他の WLAN へのトラフィックは拒否することが可能になります。このトピックの詳細については、P.7-22 の「ロケーション認識型ポリシーの適用」を参照してください。
- テスト モードのカスタマイズしたルール モジュール：カスタマイズした有線と無線の同時接続ルール モジュールをテスト モードで展開すると、管理者は、エンド ユーザ側の操作性を変更しないまま、有線と無線の同時接続のイベントを表示できるようになります。

独自のルール モジュールの開発例については、P.7-49 の「独自のルール モジュールの開発例」に示します。

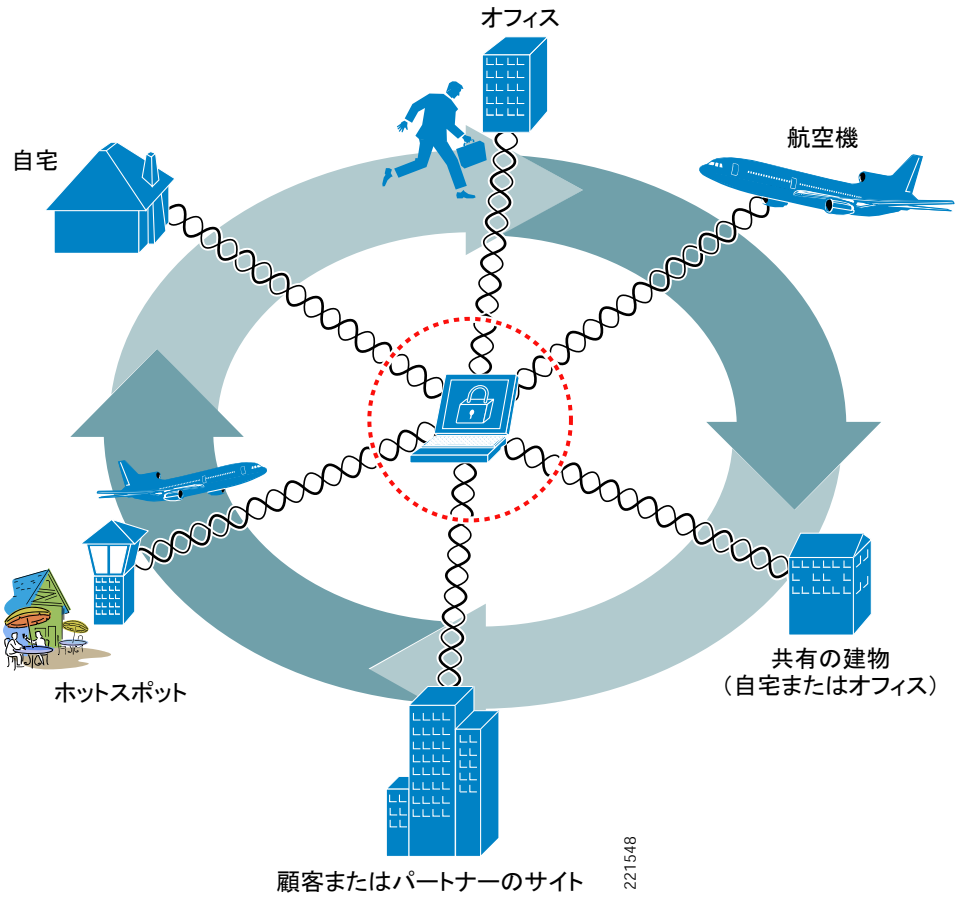
（注） 業務上の要件およびセキュリティ ポリシーはお客様ごとに異なるため、事例ごとに再確認した上で適用し、展開する必要があります。

ロケーション認識型ポリシーの適用

ロケーション認識型ポリシーの適用とは、モバイル クライアントの接続先となるネットワークに応じて、それらのロケーションに関係する既知のセキュリティ リスクに基づいて、異なるセキュリティ ポリシーや追加のセキュリティ ポリシーを適用する機能です（図 7-18 を参照）。モバイル クライアントは、次のネットワークを含めて、さまざまな範囲のネットワークに接続する可能性があります。

- 企業オフィス
- 自宅
- ホットスポット
- 顧客またはパートナーのサイト

図 7-18　モバイル クライアントの接続先となる可能性があるロケーションおよびネットワーク



セキュリティ上の脅威に対するモバイル クライアントの露出

モバイル クライアントは、複数のロケーションで異なるネットワークに接続するため、次のような理由により、さらに多くのセキュリティ リスクにさらされます（図 7-19 を参照）

- セキュリティや保護のレベルが異なるネットワークへの露出

  ロケーションが異なると、必然的にセキュリティ リスクも異なります。たとえば、オープンな公共ホットスポットへの無線接続に伴うセキュリティ リスクは、セキュアな企業ネットワークへの有線または無線による接続のセキュリティ リスクと比較した場合、非常に大きくなります。

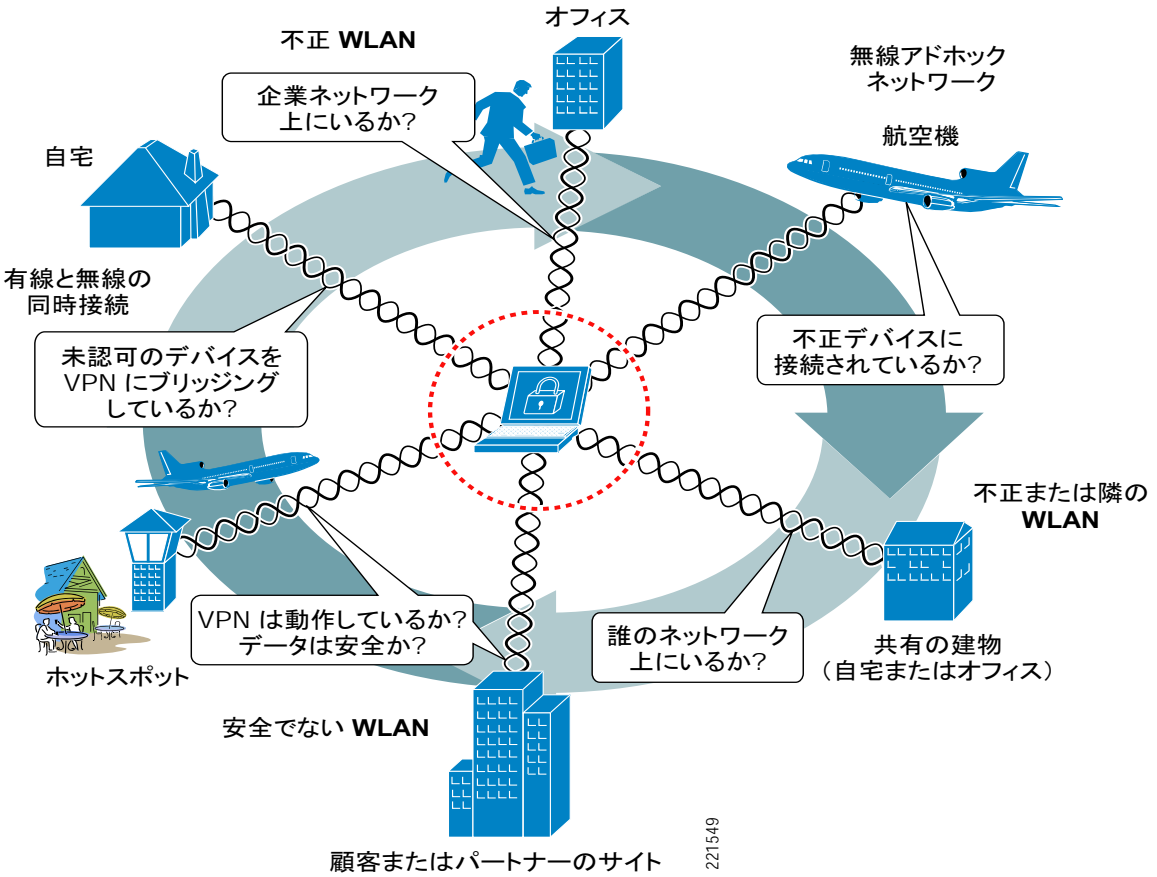
- アクティブな WLAN 接続に関するユーザの認識の欠如

  複数の WLAN プロファイルを持つモバイル クライアントのエンド ユーザは、WLAN 環境がある場合でも、接続先の WLAN を必ずしも把握していません。このため、故意または無意識に、不正なネットワークに接続する恐れがあります。

  たとえば、航空機を利用するユーザは、搭乗前にホットスポットまたはホーム ネットワークを使用した後、VPN からは切断する一方で、802.11 無線を無効にしない場合があります。このユーザが機内でラップトップを使用した場合、同乗者が運営し、ホットスポットやホーム ネットワークをスプーフィングする不正なネットワークに無意識に接続する恐れがあります。

  同様に、共用の建物内にいるユーザは、自分が企業 WLAN に接続されていると考えていても、実際には隣の WLAN に接続されている場合があります。

図 7-19　複数のロケーションへの接続に伴うセキュリティ上の懸念事項



CSA のロケーション認識型ポリシーの適用

CSA は、モバイル クライアントのロケーションに基づいて、異なるセキュリティ ポリシーを適用する機能を備えています。したがって、セキュリティ保護の処理を個々のロケーションのリスクに応じて調整し、適切なセキュリティ ポリシーを適用することができます。たとえば、モバイル クライアントが企業以外のネットワークに接続されている場合は、比較的厳格な制御を行ってホストをロックダウンし、ユーザが企業サイトに戻るときに VPN 接続の開始を強制できます。

CSA v5.2 では、「Roaming - Force VPN」と呼ばれる事前定義のロケーション認識型 Windows ルール モジュールも導入されました。このルール モジュールは、システムの状態条件とインターフェイス セットを利用して、クライアントがオフィスの外部にいる場合は VPN の使用を強制するルールを適用します。詳細については、P.7-32 の「ローミング時に VPN の使用を強制する CSA の事前定義ルール モジュール」を参照してください。

CSA の展開を補完するには、CSSC の導入を検討する必要があります。CSSC によって、許可される各ネットワーク プロファイルに対して必須の認証パラメータおよび暗号化パラメータを適用するとともに、必要に応じて VPN の自動アクティベーションを有効にします。CSSC の詳細については、製品マニュアルを参照してください（P.7-58 の「参考資料」を参照）。

ロケーション認識型ポリシー適用機能の動作

現時点では、CSA は次の基準に基づいてモバイル クライアントのロケーションを特定できます。

- システムの状態条件（次の項目を含む）：
  - イーサネットがアクティブ
  - CSA MC の到達可能性
  - Cisco Trust Agent のポスチャ
  - ネットワーク インターフェイス セット
  - DNS サーバのサフィックス（cisco.com など）
  - システムのセキュリティ レベル
- ネットワーク インターフェイス セットの特性（次の項目を含む）：
  - ネットワーク接続のタイプ（有線、Wi-Fi、Bluetooth、PPP など）
  - WLAN のモード（インフラストラクチャまたはアドホック）
  - 無線の SSID
  - 無線の暗号化タイプ（AES、WEP、TKIP など）
  - ネットワーク アドレスの範囲

CSA がクライアントのロケーションを識別した後は、関連付けられている CSA ポリシー ルールによって、そのロケーションで適用される特定のセキュリティ ポリシーが決定されます。CSA のロケーション認識型ポリシーは、CSA の標準の機能を利用し、事前定義または独自のルールを使用することにより、クライアントの現在の接続先となっているロケーションやネットワークに関係するセキュリティ リスクに応じて、クライアントに適用されるセキュリティ処理を調整します。

ロケーション認識型ポリシーの適用機能の設定

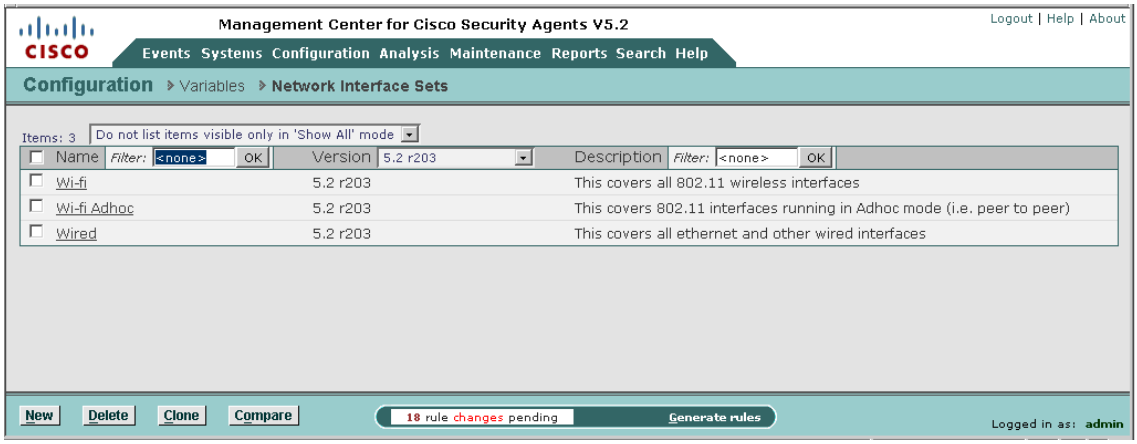
ロケーションごとにロケーション認識型のポリシーを作成する一般的な手順は、次のとおりです。

- 識別基準となるネットワーク インターフェイス セットを定義します。
- 識別基準となるシステム状態条件を定義します。
- ロケーション固有のルール モジュールを定義します。
- ロケーション固有のルールを定義し、関連付けます。
- ロケーション固有のルール モジュールを既存または新規のポリシーに関連付けます。
- ロケーション固有のポリシーの適用対象となるホストを、ロケーション固有のポリシーが含まれているグループのメンバにする必要があります。

ネットワーク インターフェイス セットの表示および定義

CSA MC ページで事前定義のネットワーク インターフェイス セットにアクセスし、新しいネットワーク インターフェイス セットを作成するには、**Configuration -> Variables -> Network Interface Sets** を参照します（図 7-20 を参照）。

図 7-20　事前定義のネットワーク インターフェイス セット



ネットワーク インターフェイス セットの名前をクリックすると、説明および関連付けられている設定パラメータが表示されます（図 7-21 を参照）。

図 7-21　事前定義の Wi-Fi ネットワーク インターフェイス セット

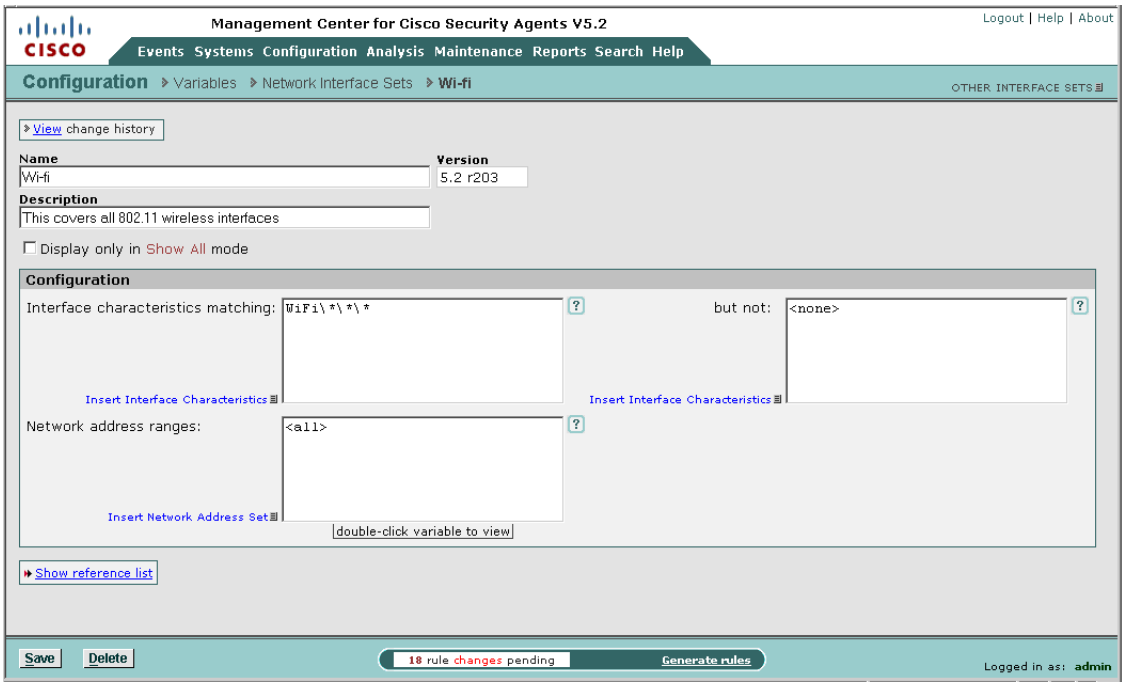


図 7-21 は、事前定義の Wi-Fi ネットワーク インターフェイス セットを示しています。インターフェイス特性定義の「WiFi***」にあるワイルドカードが示すように、モード、暗号化、または SSID にかかわらず、すべての無線接続が対象になります。

ネットワーク インターフェイス セットでは、接続のタイプに応じて数多くのパラメータを定義できます。たとえば、WLAN については次のようなパラメータがあります（図 7-22 を参照）。

- モード：インフラストラクチャまたはアドホック
- 暗号化：AES、WEP、TKIP など
- SSID

図 7-22　設定可能な Wi-Fi パラメータおよび企業 WLAN の定義例

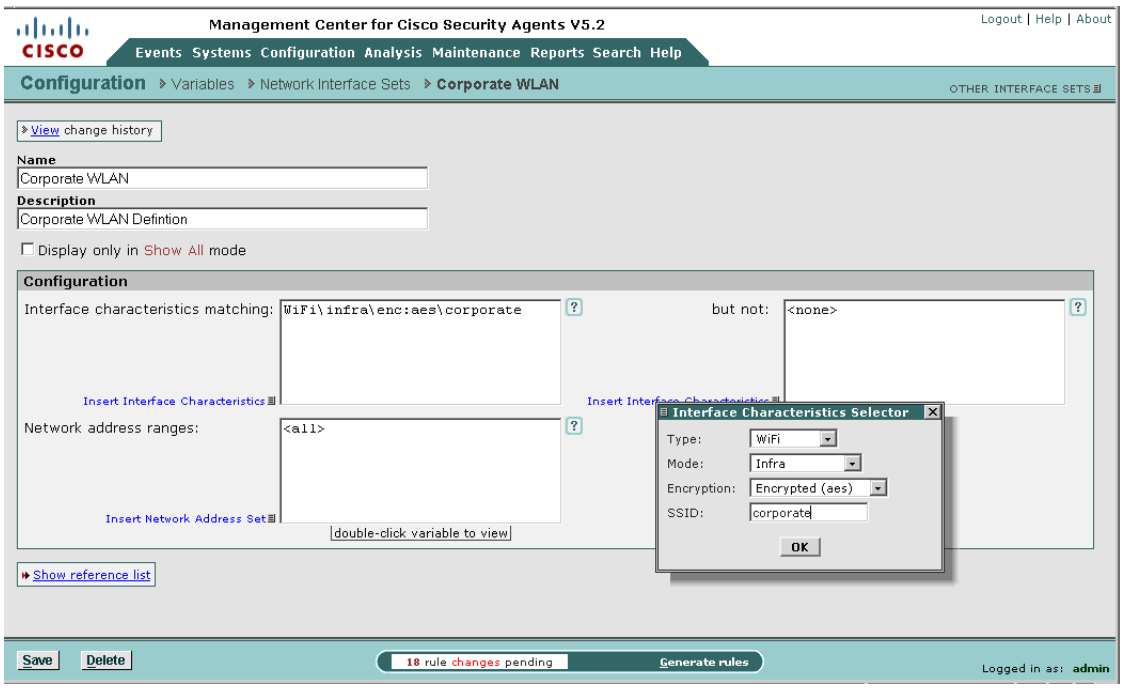
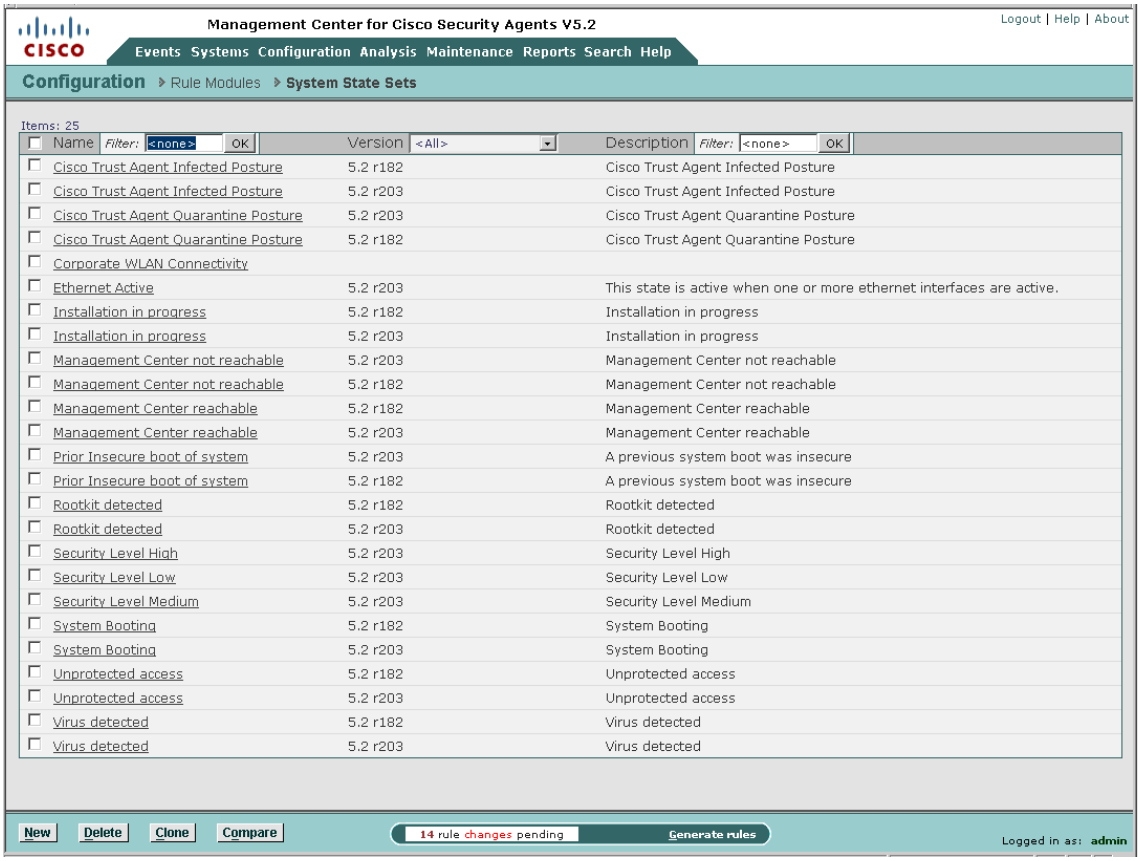


図 7-22 は、モード、暗号化、SSID など、無線接続について定義できるネットワーク インターフェイス特性を示しています。また、企業 WLAN を定義する方法についても図 7-22 に示しています。

システム状態セットの表示および定義

CSA MC で事前定義のシステム状態セットにアクセスし、新しいシステム状態セットを作成するには、**Configuration -> Rule Modules -> System State Sets** を参照します（図 7-23 を参照）。

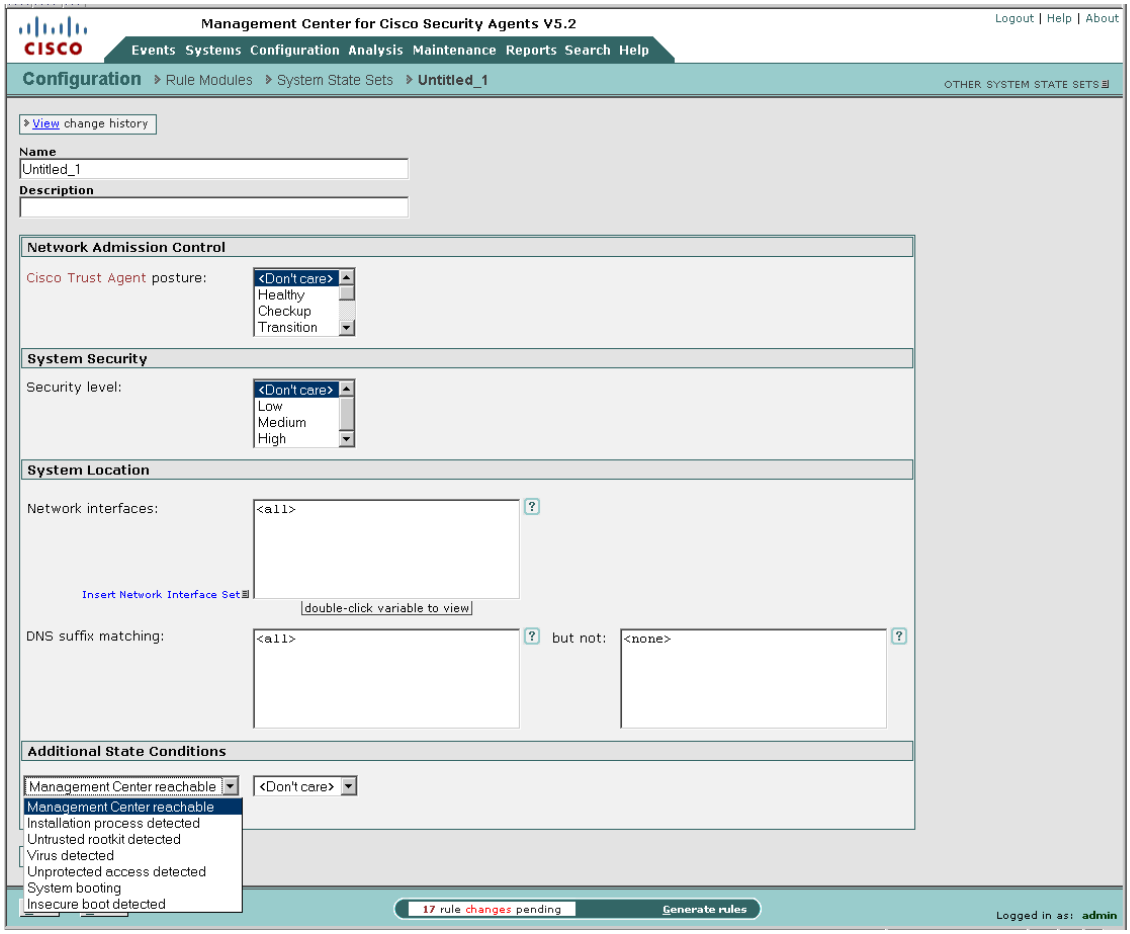
図 7-23　事前定義のシステム状態セット



次のような数多くのパラメータに基づいて、新しいシステム状態セットを作成できます（図 7-24 を参照）。

- Cisco Trust Agent のポスチャ
- システムのセキュリティ レベル
- システムのロケーション（次の項目が基準）
  - ネットワーク インターフェイス セット
  - DNS サフィックス
- Management Center の到達可能性など、追加の状態条件

図 7-24　　独自のシステム状態セットで設定できるパラメータ

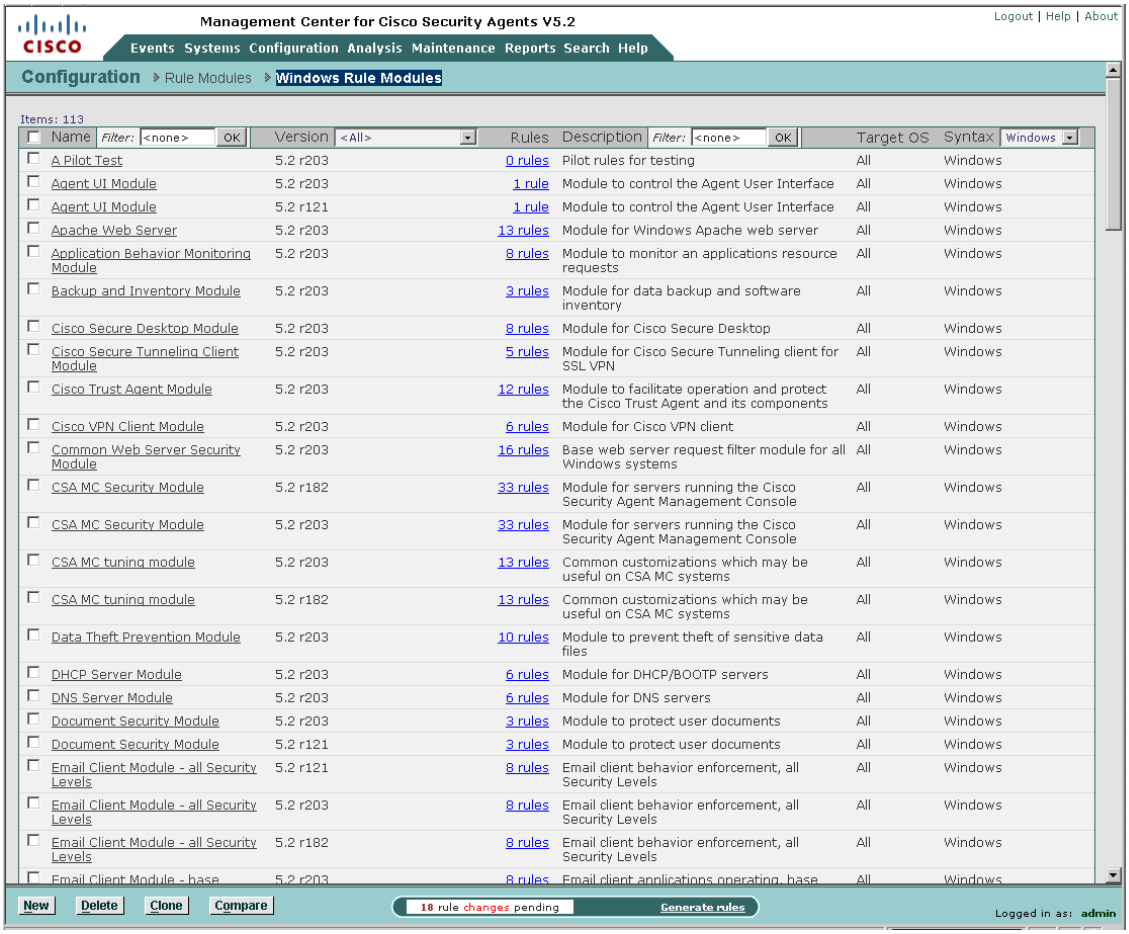


ロケーション認識型ルール モジュールの表示および定義

識別基準となるネットワーク インターフェイス セットおよびシステム状態セットを定義した後は、これらのセットを利用してロケーション認識型のルール モジュールを作成し、ロケーションに基づいて個々のルールを適用できます。

CSA MC ページで事前定義の Windows ルール モジュールにアクセスし、新しい Windows ルール モジュールを作成するには、**Configuration -> Rule Modules -> Windows Rule Modules** を参照します（図 7-25 を参照）。

図 7-25　事前定義の Windows ルール モジュール



事前定義の Roaming - Force VPN Windows ルール モジュールは、ロケーション認識型ポリシーの適用機能を展開する方法の例となります。詳細については、P.7-32 の「ローミング時に VPN の使用を強制する CSA の事前定義ルール モジュール」を参照してください。

ロケーション認識型ポリシーの適用機能の設定に関する全般的な注意事項

ロケーション認識型ポリシーの適用機能の設定に関する全般的な注意事項としては、次のものがあります。

- ネットワーク インターフェイス セットの定義では、一致条件として使用する特性を範囲の広いものにすることも、非常に限定的なものにすることもできます。たとえば、範囲の広いネットワーク インターフェイス セットでは、すべての無線接続を含めることができます。限定的なネットワーク インターフェイス セットでは、特定の SSID および暗号化タイプを持つ特定の WLAN プロファイルのみを含めます。
- ネットワーク インターフェイス セットには、特定の WLAN プロファイルなど、例外を含めることができます。
- 単一のネットワーク インターフェイス セットに複数の接続タイプ特性を含めることができます。たとえば、企業のネットワーク インターフェイス セットは、有線と WLAN の特性を使用して定義できます。

- 特定のネットワーク インターフェイス セットに関連付けられるルールを適用する場合、システム状態条件は必須ではありません。
- システム状態条件が定義されている場合、ルール モジュールが呼び出されるのは、システム状態条件を満たした場合のみになります。
- 識別基準となるシステム状態条件は、複数定義できます。たとえば、イーサネットがアクティブかつManagement Center が到達不能などです。
- ポリシーがホストに適用されるようにするには、CSA 実装に関する全般的な要件に従って、ホストを、適用するポリシーが含まれているグループのメンバにする必要があります。
- CSA グループのメンバシップは加法的なものであるため、ホストは複数のグループのメンバになることができます。

ローミング時に VPN の使用を強制する CSA の事前定義ルール モジュール

CSA v5.2 では、ネットワーク接続がアクティブな場合、企業ネットワークへの接続を強制する事前定義の Windows ルール モジュールが導入されました。このルール モジュールは、**Roaming - Force VPN** と呼ばれます。

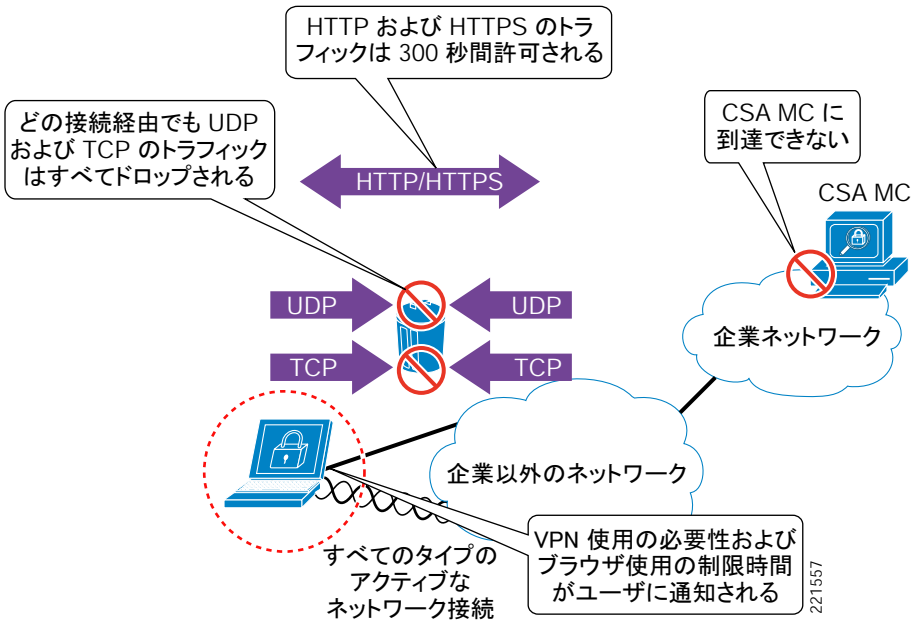
ローミング シナリオでは、このルール モジュールを適用することにより、セキュリティ ポリシーを適用して、企業以外の安全でないネットワーク上にあるクライアント自体、ローカルのデータ、および転送中のデータを保護できます。

事前定義ルール モジュールの動作

次に、ローミング時に VPN の使用を強制する事前定義の Windows ルール モジュール（図 7-26 を参照）のデフォルト動作について概要を示します。

CSA MC が到達不能でネットワーク インターフェイスがアクティブな場合、アクティブなインターフェイス上の UDP および TCP のトラフィックは、アプリケーションおよび IP アドレスとは無関係にすべて拒否されます。例外となるのは Web トラフィックで、300 秒間許可されます。

図 7-26　ローミング時に VPN の使用を強制する CSA の事前定義 Windows ルール モジュールの動作



ローミング時に VPN の使用を強制する事前定義の Windows ルール モジュールは、次の要素を含んでいます。

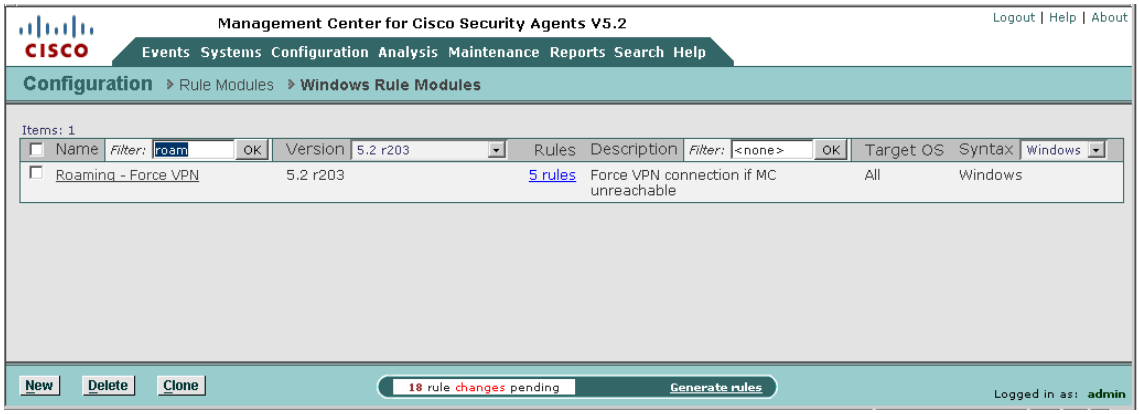
- CSA MC が到達不能でシステムがブートしていない場合、いずれかのアクティブな接続で UDP または TCP のトラフィックが発生すると、ルール モジュールが呼び出されます。これは、使用されている接続のタイプは関係しません。
- あらゆる接続でルーティングされている UDP および TCP のトラフィックが、HTTP および HTTPS のトラフィックを除いてすべてドロップされます。
- HTTP および HTTPS のトラフィックは、300 秒間許可されます。
- ユーザ クエリーが提示され、ユーザに対して、ユーザが企業ネットワークに接続されていないこと、アクセスするには VPN クライアントを使用する必要があること、ブラウザを使用してホットスポットに接続する時間の長さは制限されていることが通知されます。
- メッセージがログに記録されます。
- 300 秒が経過した後も CSA MC が到達不能のままである場合は、HTTP および HTTPS を含むすべての UDP および TCP のトラフィックがドロップされます。
- CSA MC が到達可能になると、ルール モジュールは失効します。
- ルール モジュールの失効後は、ロギングが発生しません。

事前定義ルール モジュールの設定

企業ネットワークへの接続を強制する事前定義の Windows ルール モジュールは、**Roaming - Force VPN** と呼ばれます。

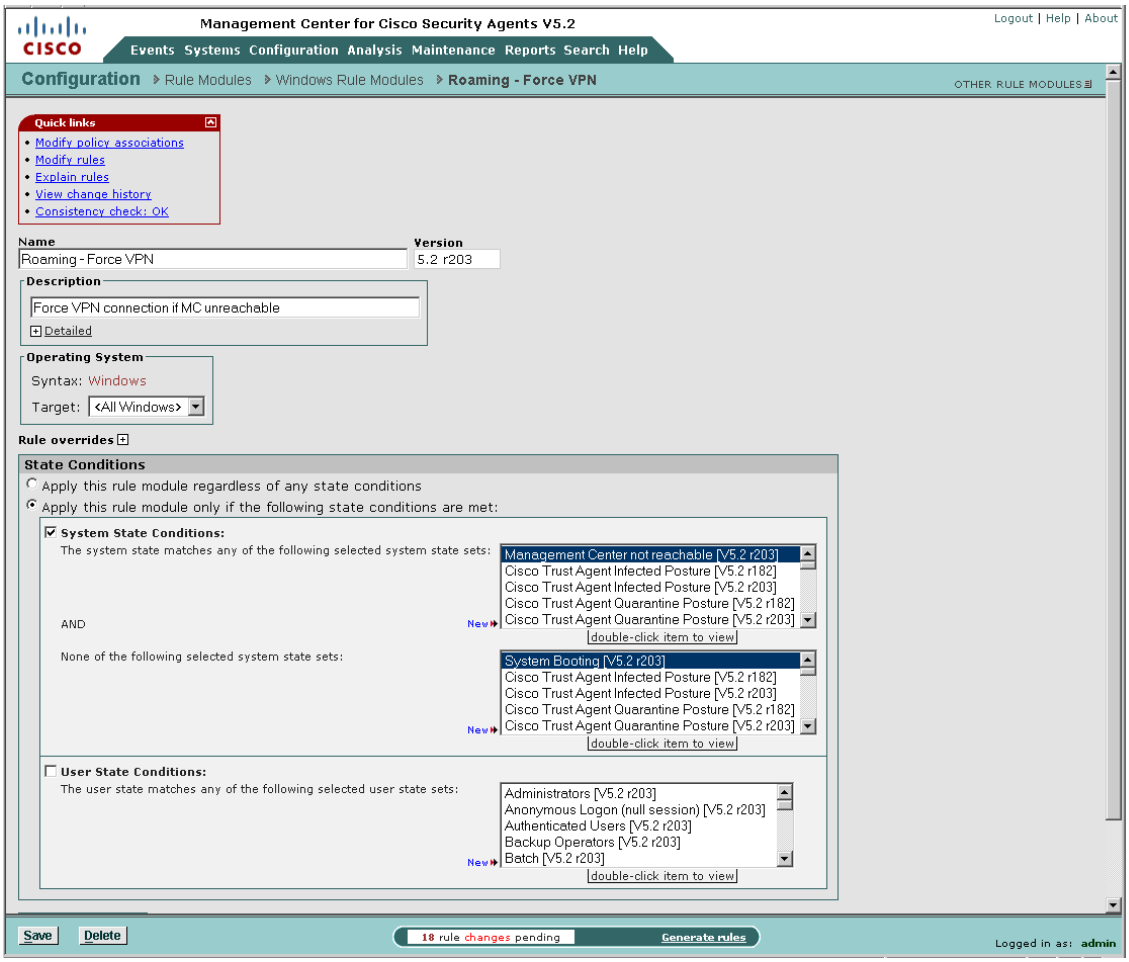
CSA MC で **Configuration -> Rule Modules -> Rule Modules [Windows]** を参照すると、見つけることができます（図 7-27 を参照）。すばやく検索するには、**roam** という名前でフィルタを定義します。

図 7-27　ローミング時に VPN の使用を強制する事前定義 Windows ルール モジュールのリスト



ルール モジュールの名前をクリックすると、このルール モジュールの説明、オペレーティング システム、および状態条件が表示されます（図 7-28 を参照）。

図 7-28　ローミング時に VPN の使用を強制する事前定義 Windows ルール モジュールの定義

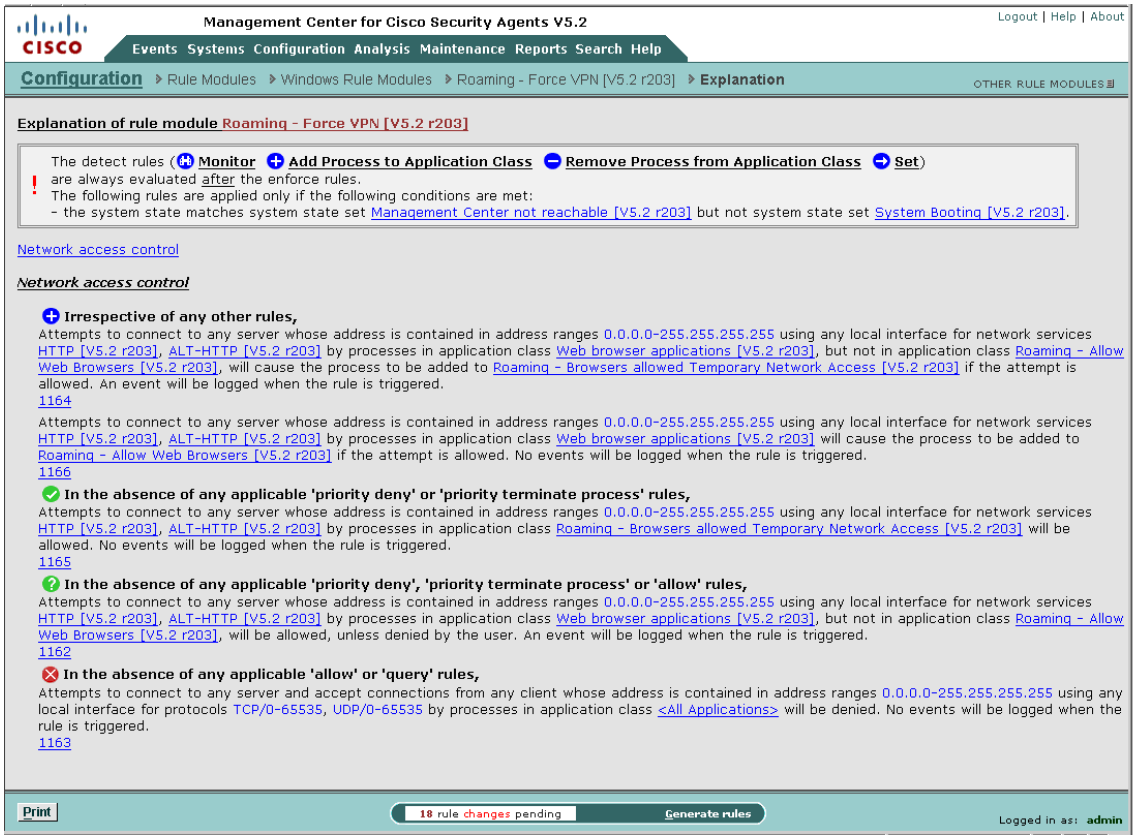


この事前定義ルール モジュールの状態条件では、ルールが呼び出されるには、次の条件を満たすことが要件になっています。

- Management Center が到達不能
- システムがブートしていない

Explain rules リンクをクリックすると、ルールの説明および関連付けられているアクションが表示されます（図 7-29 を参照）。

図 7-29　ローミング時に VPN の使用を強制する Windows ルール モジュールに関連付けられているルールの説明

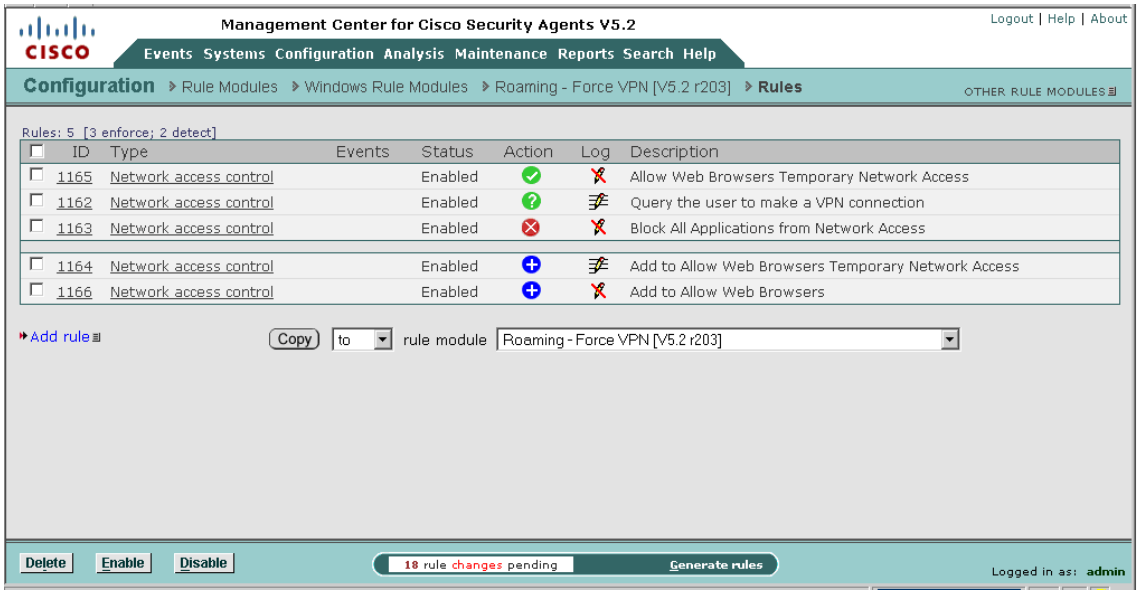


また、ルール モジュールの定義画面で Modify rules リンクをクリックした場合も、関連付けられているルールが一覧表示されます（図 7-30 を参照）。

ルール モジュールのリストで **5 rules** リンクをクリックして、ルールに直接アクセスすることもできます（図 7-27 を参照）。

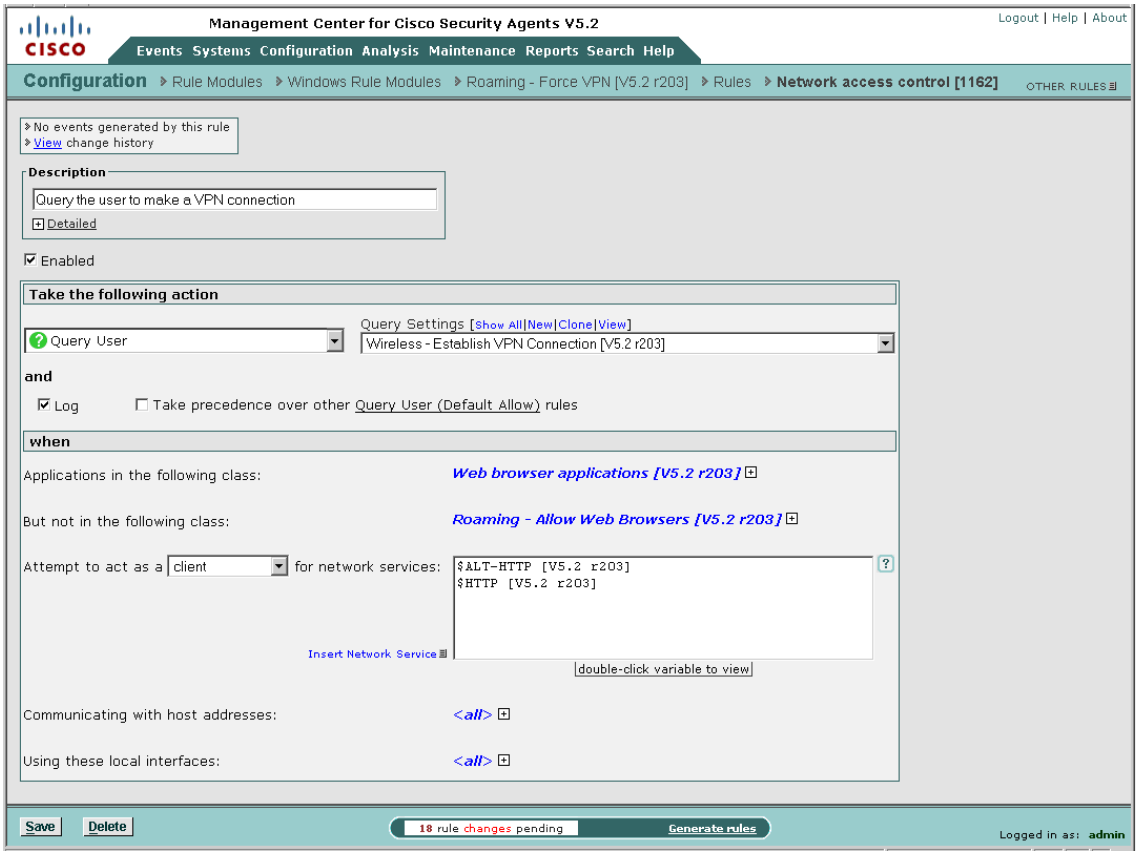
（注） ルールの番号は、使用されている個々のシステムに応じて異なります。

図 7-30　ローミング時に VPN の使用を強制する Windows ルール モジュールに関連付けられているルール



特定のルール名をクリックすると、そのルールの詳細な設定が表示されます（図 7-31 を参照）。

図 7-31　VPN 接続を確立するユーザにクエリーを提示する事前定義のネットワーク アクセス コントロール ルール



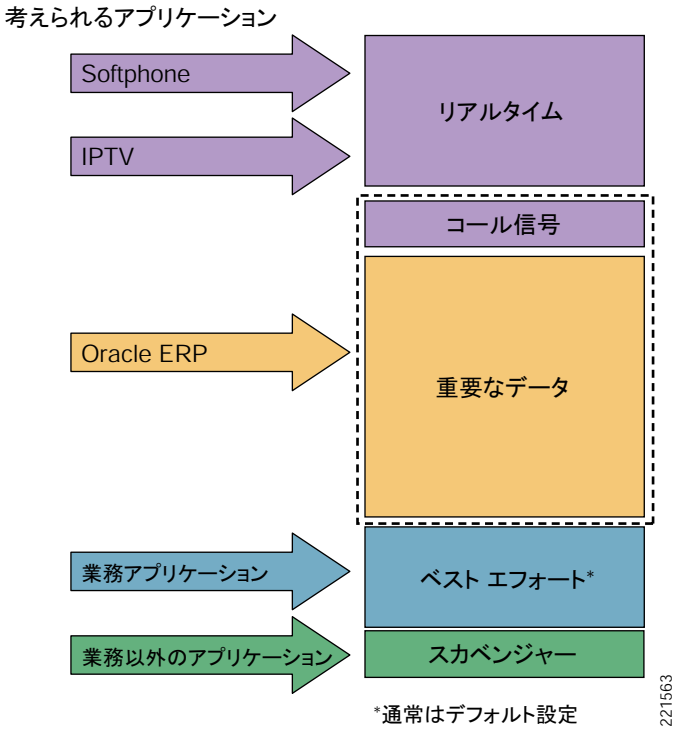
アップストリーム QoS マーキング ポリシーの適用

QoS マーキング ポリシーの適用とは、ホストを発信元とするアプリケーション フローの QoS パラメータを設定または再マーキングする機能です。ネットワーク内のアップストリーム デバイスは、これらのマーキングを使用することにより、パケットを分類して適切な QoS サービス ポリシーを適用できます。

QoS マーキングの目的は、アプリケーション フローを複数のサービス クラスに分割して、個々のネットワークの要件および業務上の優先順位に従って処理できるようにすることです。一般的なサービス クラスには、次のものがあります（図 7-32 を参照）。

- Voice over IP（VoIP）など、遅延の影響を受けやすいアプリケーション
- ネットワーク コントロール トラフィック
- 基幹業務アプリケーション
- 一般的なユーザ トラフィック（E メールや Web など）
- 業務以外のトラフィック

図 7-32　　4 ～ 5 クラスの QoS モデルで構成されるアプリケーションの例



このモデルを適用できるのは、DiffServ アーキテクチャを実装している企業ネットワークまたはキャンパス ネットワークです。

アップストリーム QoS マーキングの利点

全般的なネットワーキングの観点から見ると、アップストリーム QoS マーキングの主な利点は、次の 2 つになります。

- ネットワークとサービスのアベイラビリティ：ネットワークとサービスのアベイラビリティを確保することは、ネットワークのセキュリティ上、特に遅延の影響を受けやすい VoIP などの業務アプリケーションでは重要な要素です。VoIP は、データ損失、遅延、およびジッタの影響を受けやすくなっています。この点が特に重要となるのは、輻輳のあるリンクや帯域幅が限られているリンク上のほか、一般的な障害、DoS 攻撃、ワームの発生によってリンクやサイトが停止した場合など、ネットワークで問題が発生している場合です。

  QoS マーキングを使用して、業務でのニーズに応じて複数のサービス クラスに優先順位を設定することにより、重要な業務アプリケーションをどのようなネットワーク状態でも維持し、優先的に処理することができます。

- 運用コストの管理：QoS マーキングを使用することにより、特に WAN リンクなど、高コストで帯域幅が限定的なリンクにおいて、必要な帯域幅のみが展開されることも保証されます。これは、ポリシーに応じて複数のサービス クラスを処理し、運用コストを最小限に抑えることで実現します。

WLAN でのアップストリーム QoS マーキングの利点

WLAN で QoS マーキングを使用することには、大きな利点があります。802.11 の帯域幅は共有媒体であり、コンテンションが頻繁に発生するためです。

WLAN エンドポイント上でアップストリーム QoS マーキングを使用すると、アプリケーションのニーズに応じて 802.11 トラフィックが分類され、優先順位が設定されます。アプリケーションが混在する環境では、遅延の影響を受けやすい VoIP アプリケーションなど、優先順位が高いアプリケーションの 802.11 媒体へのアクセス優先順位を高くすることにより、サービスのアベイラビリティを維持できます。

WLAN でのアップストリーム QoS マーキングの課題

アップストリーム QoS マーキングは WLAN に大きな利点をもたらしますが、QoS を有効にすることで、次のような課題も発生します。

- QoS マーキングの不正使用または誤用

  802.11e および Wi-Fi Multimedia（WMM）対応のデバイスは、アップストリーム パケットに QoS 分類をマーキングする機能を備えていますが、これらの自己査定マーキングは、意図しないまま高評価のマーキングが行われたり、セキュリティが侵害されたホストなどによって意図的に不正使用されたりすることがあるため、必ずしも信頼できず、不正使用されやすいものです。したがって、これらの設定を使用する場合、プライオリティ キューのジャンピングなどの一般的な QoS マーキング不正使用だけでなく、802.11 RF 媒体とネットワーク インフラストラクチャの両方に対する DoS 攻撃が試みられる恐れもあります。

- レガシー デバイスでの QoS の未サポート

  802.11e および WMM に対応しないレガシー デバイスは、アップストリーム QoS マーキングをサポートしていません。したがって、これらのデバイスからのトラフィックは分類も優先順位の設定も行われず、WLAN では、通常はベスト エフォート方式で処理されます。

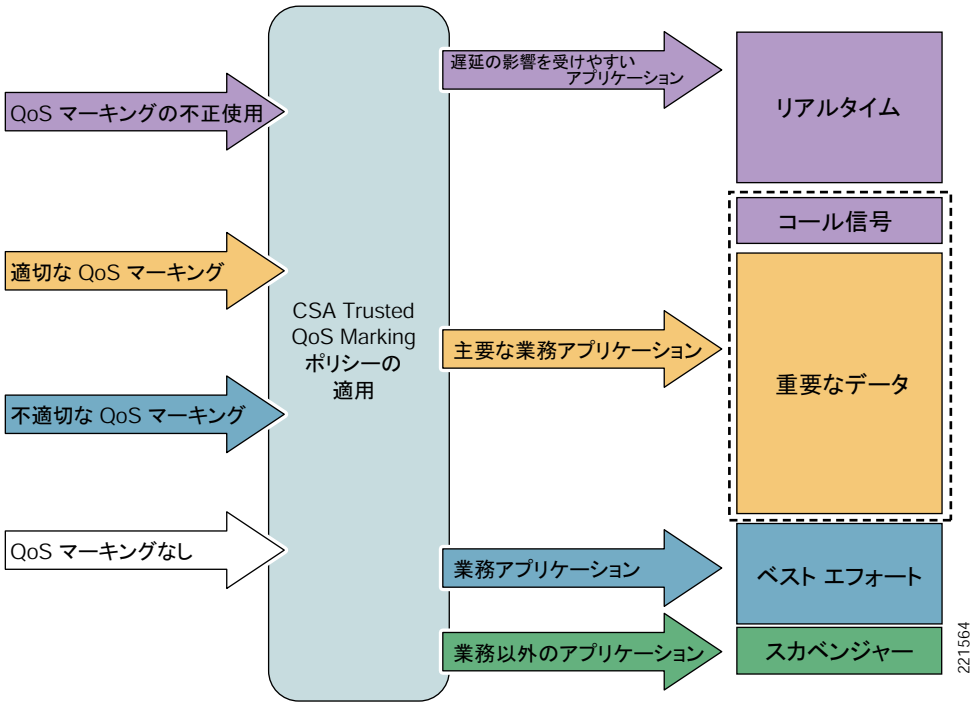
- レガシー アプリケーションでの QoS の未サポート

  アプリケーションの多くは、QoS 機能をサポートしていません。したがって、これらのアプリケーションからのトラフィックは分類も優先順位の設定も行われず、WLAN では、通常はベスト エフォート方式で処理されます。

CSA Trusted QoS Marking

CSA v5.0 では、エンドポイント上のホスト アプリケーション フローにアップストリーム QoS マーキングを適用する機能が導入されました。したがって、CSA を使用することにより、ホストを発信元とするすべてのアップストリーム トラフィックに対して、ネットワーク ポリシーに応じた QoS マーキングを確実に設定できます（図 7-33 を参照）。

図 7-33　　ポリシー適用のための CSA Trusted QoS Marking



CSA によって設定される QoS マーキングは、Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値であり、CSA のポリシー ルールとして定義されます。このため、管理者は、次に示す精密な制御を一元的に定義できます。

- プロトコルごと
- ポート範囲ごと
- アプリケーション、ポート、およびプロトコルごと

DSCP 値は、802.11 RF 媒体での転送のためにレイヤ 2 Class of Service（CoS; サービス クラス）値にマップされます。このマッピングは、クライアントが実行します。

また、Cisco NAC を展開すると、クライアントに CSA を確実にインストールして実行できます。これにより、エンドポイント上で QoS マーキングが適切に設定され、検証されることが保証されます。

CSA Trusted QoS 機能の詳細については、P.7-58 の「参考資料」の CSA の項に示したマニュアルを参照してください。

WLAN クライアントでの CSA Trusted QoS Marking の利点

CSA Trusted QoS Marking では、表 7-2 に示すように、802.11 ネットワークにアップストリーム QoS を実装することで生じる一般的な課題に対処できます。

表 7-2　QoS の一般的な課題

WLAN 上での QoS の一般的な課題	CSA Trusted QoS Marking の適用
QoS マーキングの不正使用または誤用	適切に定義されていないアップストリーム QoS マーキングを上書きする
レガシー デバイスでの QoS の未サポート	QoS をサポートしないレガシー デバイス上でアップストリーム QoS マーキングを使用できるようにする
レガシー アプリケーションでの QoS の未サポート	QoS をサポートしないレガシー アプリケーション上でアップストリーム QoS マーキングを使用できるようにする

このように、CSA Trusted QoS Markings を適用することにより、クライアントから送信されるすべてのパケットに QoS マーキングが適用され、これらのマーキングがネットワーク ポリシーに適合するよう設定されることが保証されます。したがって、アプリケーションを正確に分類し、優先順位を設定できるようになります。この点は、複数のアプリケーションやさまざまなエンドポイントおよびプラットフォームで構成される混成環境の場合、特に重要です。

WLC の背後にあるアクセス スイッチでパケットを再分類および再マーキングして、この処理を補完することにより、あらゆる異常を確実に修正できます。

CSA Trusted QoS Marking の展開に関する基本ガイドライン

クライアントを発信元とするパケットすべてにアップストリーム QoS マーキングを適用するには、すべてのクライアントに CSA Trusted QoS Marking を展開することをお勧めします。これは、次の 2 つの段階によって展開できます。

1. デフォルトの QoS ルール モジュールを定義して、すべてのトラフィックをベスト エフォートとしてマーキングします。
2. 追加のルール モジュールを定義し、VoIP などの識別されたミッションクリティカル アプリケーションに対して、適切な QoS マーキングを適用します。

CSA Trusted QoS 機能の実装については、このマニュアルでは詳しく取り扱いません。この機能を実装する方法の詳細については、P.7-58 の「参考資料」の CSA の項に示したマニュアルを参照してください。

CSA 無線セキュリティ ポリシーのレポート

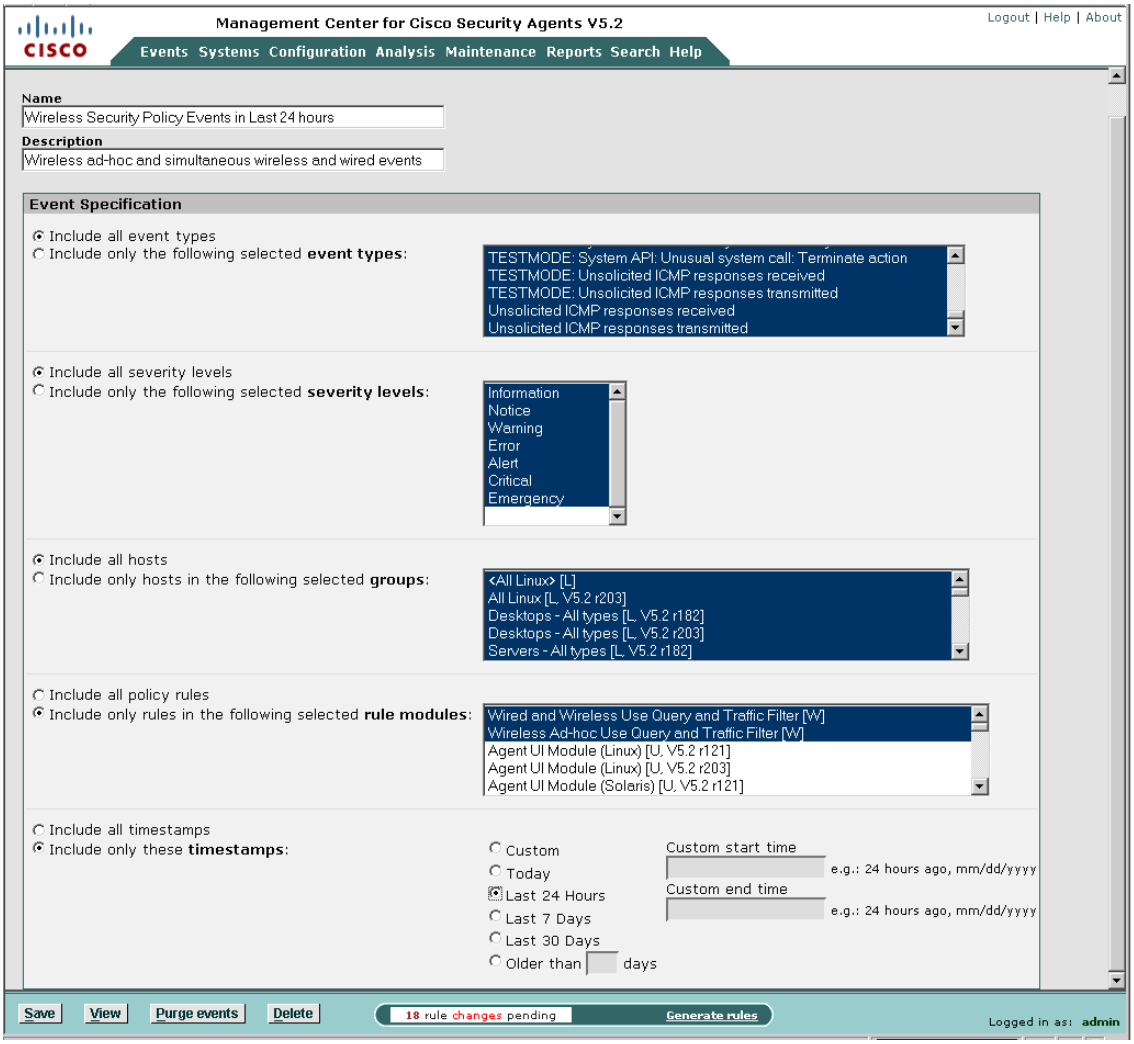
CSA Management Center のレポート

CSA MC に組み込まれているレポート生成機能を使用すると、重大度、グループ、ホスト、またはポリシーに基づいてイベントを表示できます。

無線固有の便利なレポートの 1 つに、一定期間中に発生した無線ポリシー違反イベントのリストがあります。1 つまたはそれ以上の WLAN ポリシーで無線ルールが設定されている場合は、次の手順に従って、このタイプのレポートを簡単に生成できます。

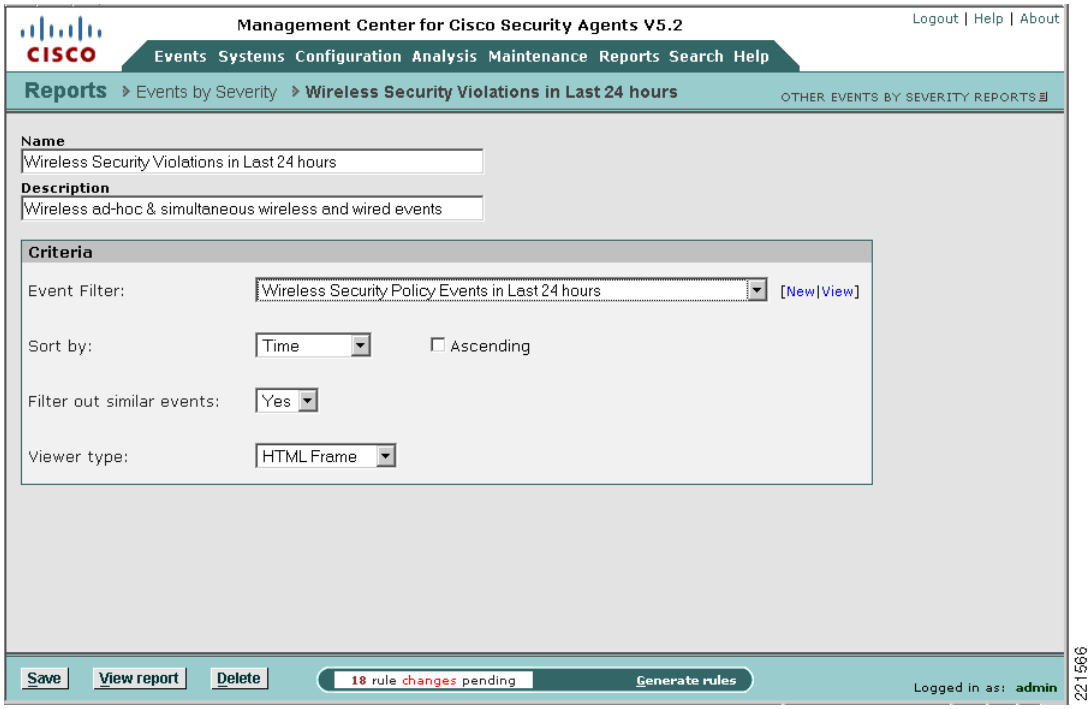
ステップ 1対象となる無線固有のポリシーのイベント セット、および必要な期間を定義します。**Events -> Event Sets** を参照し、無線固有のルール モジュールのみを含む新しいイベント セットを作成して、タイムスタンプ（最近 24 時間など）を設定します（図 7-34 を参照）。

図 7-34　　無線固有のポリシーに基づいた無線固有のイベント セットの作成



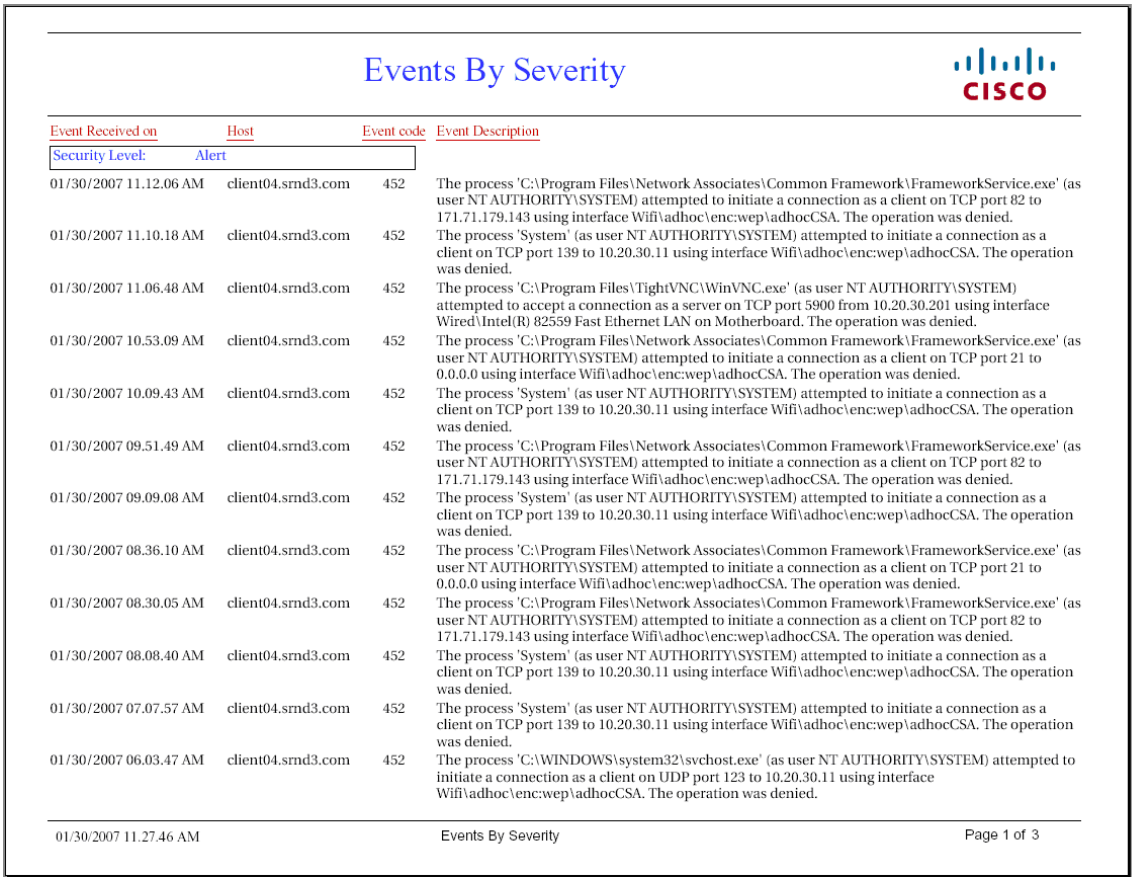
ステップ 2新しく定義したイベント セットをイベント フィルタとして使用し、必要となる形式に応じて、重大度別またはグループ別のイベント レポートを作成および定義します。**Reports -> Event Severity** を参照し、新しく作成した無線固有のイベント セットをイベント フィルタに設定して、新しいレポートを作成します（図 7-35 を参照）。

図 7-35　重大度別の無線ポリシー イベント レポートの定義例



（注） 重大度別のイベント レポートでは、イベントをホスト別にソートできます（図 7-36 を参照）。これは、問題が発生した場合の追跡に便利です。

図 7-36　　重大度別の無線ポリシー イベント レポートの例



Events By Severity

Event Received on	Host	Event code	Event Description
Security Level: Alert			
01/30/2007 11.12.06 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 11.10.18 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 11.06.48 AM	client04.srnd3.com	452	The process 'C:\Program Files\TightVNC\WinVNC.exe' (as user NT AUTHORITY\SYSTEM) attempted to accept a connection as a server on TCP port 5900 from 10.20.30.201 using interface Wired\Intel(R) 82559 Fast Ethernet LAN on Motherboard. The operation was denied.
01/30/2007 10.53.09 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 21 to 0.0.0.0 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 10.09.43 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 09.51.49 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 09.09.08 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.36.10 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 21 to 0.0.0.0 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.30.05 AM	client04.srnd3.com	452	The process 'C:\Program Files\Network Associates\Common Framework\FrameworkService.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 82 to 171.71.179.143 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 08.08.40 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 07.07.57 AM	client04.srnd3.com	452	The process 'System' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on TCP port 139 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.
01/30/2007 06.03.47 AM	client04.srnd3.com	452	The process 'C:\WINDOWS\system32\svchost.exe' (as user NT AUTHORITY\SYSTEM) attempted to initiate a connection as a client on UDP port 123 to 10.20.30.11 using interface Wifi\adhoc\enc:wep\adhocCSA. The operation was denied.

01/30/2007 11.27.46 AM　　Events By Severity　　Page 1 of 3

221567

サードパーティの統合

CSA MC では、内蔵のレポート機能を使用するほかに、次の方法でサードパーティ アプリケーションを統合できます。

- CSA MC イベント データベースに対する SQL サーバ ビュー アクセス
- アラートの SNMP 配信
- フラット ファイルへのアラートのロギング
- アラートの E メール配信

CSA と CS-MARS プラットフォームとの統合は、CSA によって SNMP アラートを CS-MARS に配信することでサポートされます。ホストベースの IDS デバイスおよび IPS デバイスの設定については、P.7-58 の「参考資料」に示した CS-MARS ユーザ ガイドを参照してください。

（注） アラートを E メールで配信する場合は、十分に注意して、E メール サーバに対する DoS 攻撃の発生を防止する必要があります。

CSA でのモバイル クライアント セキュリティに関する一般的なガイドライン

モバイル クライアント セキュリティのために CSA を統合する場合の全般的な展開ガイドラインは、次のとおりです。

- 一般的なクライアント エンドポイント保護のために CSA を展開します。
- モバイル クライアントが遭遇する脅威に対処するため、次のような CSA ポリシーの追加を検討します。
  - 無線アドホックポリシーの適用
  - 有線と無線の同時接続に関するポリシーの適用
  - ロケーション認識型ポリシーの適用
  - アップストリーム QoS マーキング
  - 少なくとも、デフォルトの QoS ルール モジュールを定義して、すべてのトラフィックをベスト エフォートとしてマーキングする
- Cisco Secure Services Client（CSSC）を使用して、セキュリティ ポリシーに応じてネットワーク アクセス プロファイルを適用することを検討します。これには、WLAN プロファイルおよび認証と暗号化のパラメータが含まれます。

次の作業を行うことをお勧めします。

- 定義済みの企業セキュリティ ポリシーを適用するための独自の CSA ポリシーを開発する。
- ここまでに説明した運用上の考慮事項をルール モジュールごとに個々の環境と照らし合せて、十分に再確認した上で展開する。
- WLAN ポリシー違反イベントを定期的に監視し、全般的なセキュリティ ポリシーの一環として再確認する。

その他の情報

CSA の事前定義ルール モジュールの運用上の考慮事項

無線アドホック接続

無線アドホック ポリシー適用機能の実装を検討している場合は、CSA の事前定義無線アドホック ルール モジュールの運用面について、次の点を考慮することをお勧めします。

- 無線アドホック接続のステータス
  - 無線アドホック接続は、継続的に新しいものが開始され、受け入れられます。
  - 確立された無線アドホック接続は、アクティブで接続された状態を持続し、セキュリティ リスクとなります。
  - エンド ユーザには、無線アドホック接続はアクティブで接続された状態を持続しているように見えます。
- トラフィックのフィルタリング

- ドロップされるのは、無線アドホック接続上の UDP および TCP のトラフィックに限られます。この他の CSA セキュリティ処理を導入して、UDP および TCP 以外の攻撃からクライアントを保護する必要があります。
- 無線アドホック接続で確立されている UDP または TCP ベースのセッションは、ルール モジュールが呼び出されると機能を停止します。これは、リターン IP アドレスが無線アドホック接続をホストする無線アダプタのものであり、フィルタリングされるためです。無線アドホック以外の接続を通じて、セッションを再確立する必要があります。
- 無線アドホック接続でルーティングされる ICMP ping は、デフォルトではこのルール モジュールによってフィルタリングされず、脅威は残ったままになります。着信 ICMP パケットは、CSA Network Shield ルール モジュールを適用することでフィルタリングできます。
- 発信 ICMP は、CSA Network Shield ルール モジュールが適用されている場合でも、無線アドホック接続で引き続き機能します。無線アドホック接続はアクティブで接続済みであり、ICMP ping は引き続き機能しますが、接続が「正常に機能していない」ように見えるため、エンド ユーザの混乱を招く場合があります。運用スタッフは、ルール モジュールが適用されている場合でも、クライアントからの発信 ICMP ping は引き続き機能することを認識している必要があります。

- クライアントのルーティング テーブル
  - ルール モジュールが適用された後、無線アドホック接続はすべて接続済みでアクティブなままであるため、ルーティング テーブルは更新されません。
  - 特定の宛先ホスト IP またはネットワークについて無線アドホック接続に優先ルートが設定されている場合は、ルール モジュールが呼び出されると、この宛先にルーティングされるか、この宛先を経由する UDP および TCP のトランザクションはすべて機能を停止します。この宛先へのトラフィックは、無線アドホック以外の代替接続上に代替のルートが存在していても、すべてドロップされます。
  - 運用スタッフは、ポリシーの適用対象となる無線接続上に優先ルートが存在している場合、（UDP および TCP ベースの）一部のアプリケーションで処理が失敗する可能性があることを認識している必要があります。
- 補完機能
  - 無線アドホック接続および不正アクセス ポイントに対するクライアント側の軽減機能は、ネットワーク側での検出と軽減によって補完し、多層防御を展開する必要があります。これは、WLC の不正 AP セキュリティ機能を使用する Cisco Unified Wireless Network で実現できます。詳細については、WLC のマニュアルを参照してください（P.7-58 の「参考資料」を参照）。

有線と無線の同時接続

有線と無線の同時接続ポリシー適用機能の実装を検討している場合は、事前定義の有線と無線の同時接続アドホック ルール モジュールの運用面について、次の点を考慮することをお勧めします。

- 無線接続のステータス
  - イーサネット インターフェイスがアクティブな場合でも、継続的に新しい 802.11 無線接続が開始され、受け入れられます。
  - 確立された 802.11 無線接続は、イーサネット インターフェイスがアクティブな場合でも、アクティブで接続済みのままになります。
  - エンド ユーザには、802.11 無線接続はアクティブで接続された状態を持続しているように見えます。

- トラフィックのフィルタリング
  - ドロップされるのは、802.11 無線接続上の UDP および TCP のトラフィックに限られます。この他の CSA セキュリティ処理を導入して、UDP および TCP 以外の攻撃からクライアントを保護する必要があります。
  - 有線インターフェイスに同時接続する前に 802.11 無線接続で確立されている UDP または TCP ベースのセッションは、ルール モジュールが呼び出されると機能を停止します。これは、リターン IP アドレスが無線アダプタのものであり、フィルタリングされるためです。ルール モジュールを無効にするには、802.11 無線以外の接続を通じてセッションを再確立するか、イーサネット接続を非アクティブにする必要があります。
  - 802.11 無線接続でルーティングされる ICMP ping は、このルール モジュールによってフィルタリングされず、脅威は残ったままになります。着信 ICMP パケットは、CSA Network Shield ルール モジュールを適用することでフィルタリングできます。
  - 発信 ICMP は、CSA Network Shield ルール モジュールが適用されている場合でも、802.11 無線接続で引き続き機能します。無線接続はアクティブで接続済みであり、ICMP ping は引き続き機能しますが、接続が「正常に機能していない」ように見えるため、エンド ユーザの混乱を招く場合があります。運用スタッフは、ルール モジュールが適用されている場合でも、クライアントからの発信 ICMP ping は引き続き機能することを認識している必要があります。
- クライアントのルーティング テーブル
  - ルール モジュールが適用された後、802.11 無線接続はすべて接続済みでアクティブなままであるため、ルーティング テーブルは更新されません。
  - 特定の宛先ホスト IP またはネットワークについて 802.11 無線接続に優先ルートが設定されている場合は、ルール モジュールが呼び出されると、この宛先にルーティングされるか、この宛先を経由する UDP および TCP のトランザクションはすべて機能を停止します。この宛先へのトラフィックは、802.11 無線以外の代替接続上に代替のルートが存在していても、すべてドロップされます。
  - 運用スタッフは、ポリシーの適用対象となる無線接続上に優先ルートが存在している場合、（UDP および TCP ベースの）一部のアプリケーションで処理が失敗する可能性があることを認識している必要があります。
- 802.11 以外の無線インターフェイス
  - 事前定義のルール モジュールは、802.11 a/b/g/n ネットワークを含むすべての 802.11 無線接続に適用されます。事前定義のルール モジュールでは、3G ネットワークへの接続など、802.11 以外の無線接続は対象になりませんが、独自のルールを作成することで対象にできます。
- 代替となる実装
  - CSSC が展開されている場合は、この脅威を阻止するための代替手段として、このクライアントの有線と無線の同時接続機能を利用できます。

ローミング時の VPN の使用の強制

クライアントがアクティブなインターフェイスを持っている場合に、この事前定義ルール モジュールを展開して企業ネットワークへの接続を強制することを検討している場合は、次の点を考慮することをお勧めします。

- 企業以外のネットワークへの接続
  - 企業以外のネットワークへのすべてのアクセスは、企業ネットワークを経由する場合に限り許可されます。

  - 企業以外のネットワークへのローカル クライアントの接続は、このルール モジュールが適用された時点でブロックされます。
- 期間に関する考慮事項
  - デフォルトでは、ユーザが企業以外のネットワークへのローカル接続を確立し、企業ネットワークへの VPN 接続を確立するための時間は 300 秒しかありません。この手順では、ユーザはホットスポットに接続し、認証を受け、登録して課金情報を入力した後、VPN への接続を開始し、確立し、認証を受ける必要があります。
- ネットワーク接続のステータス
  - ネットワーク接続は、ルール モジュールが呼び出されてタイムアウトを過ぎた場合でもアクティブなままですが、トラフィックはドロップされます。
  - ルール モジュールが呼び出されてタイムアウトを過ぎた場合でも、ネットワーク接続は確立済みでアクティブな状態を維持します。
  - エンド ユーザには、ネットワーク接続はアクティブで接続を維持しているように見えますが、UDP および TCP のトラフィックは転送されません。
- トラフィックのフィルタリング
  - ドロップされるのは、UDP および TCP のトラフィックに限られます。この他の CSA セキュリティ処理を導入して、UDP および TCP 以外の攻撃からクライアントを保護する必要があります。
  - ICMP ping は、デフォルトではこのルール モジュールによってフィルタリングされず、脅威は残ったままになります。着信 ICMP パケットは、CSA Network Shield ルール モジュールを適用することでフィルタリングできます。
  - 発信 ICMP は、CSA Network Shield ルール モジュールが適用されている場合でも、引き続き機能します。ネットワーク インターフェイスはアクティブで接続済みであり、ICMP ping は引き続き機能しますが、接続が「正常に機能していない」ように見えるため、エンド ユーザの混乱を招く場合があります。
  - 運用スタッフは、ルール モジュールが適用されている場合でも、クライアントからの発信 ICMP ping は引き続き機能することを認識している必要があります。
- 補完機能
  - CSSC が展開されている場合は、このクライアントの VPN アクティベーション機能を利用してユーザ エクスペリエンスを拡張し、VPN 接続を支援することができます。

独自のルール モジュールの開発例

この項では、独自のルール モジュールを開発する方法を示します。例として、カスタマイズした有線と無線の同時接続ルール モジュールを使用します。カスタマイズしたルール モジュールは、次の処理を実行します。

- 有線と無線の同時接続が検出されると、カスタマイズ済みのユーザ クエリーを発行して、同時接続を許可するか拒否するかのオプションをユーザに提示します。

このカスタマイズを利用して、ユーザ クエリーを発行し、有線と無線の同時接続に伴うセキュリティ リスクをエンド ユーザに通知することによって、これらのセキュリティ リスクをユーザに伝達できます。これにより、セキュリティ ポリシーに関する意識の向上を図ることができるほか、サポート コール数の削減につながります。ユーザに対して、有線と無線の同時接続を許可するか拒否するかのオプションを提示できます。デフォルトのアクションは拒否です。

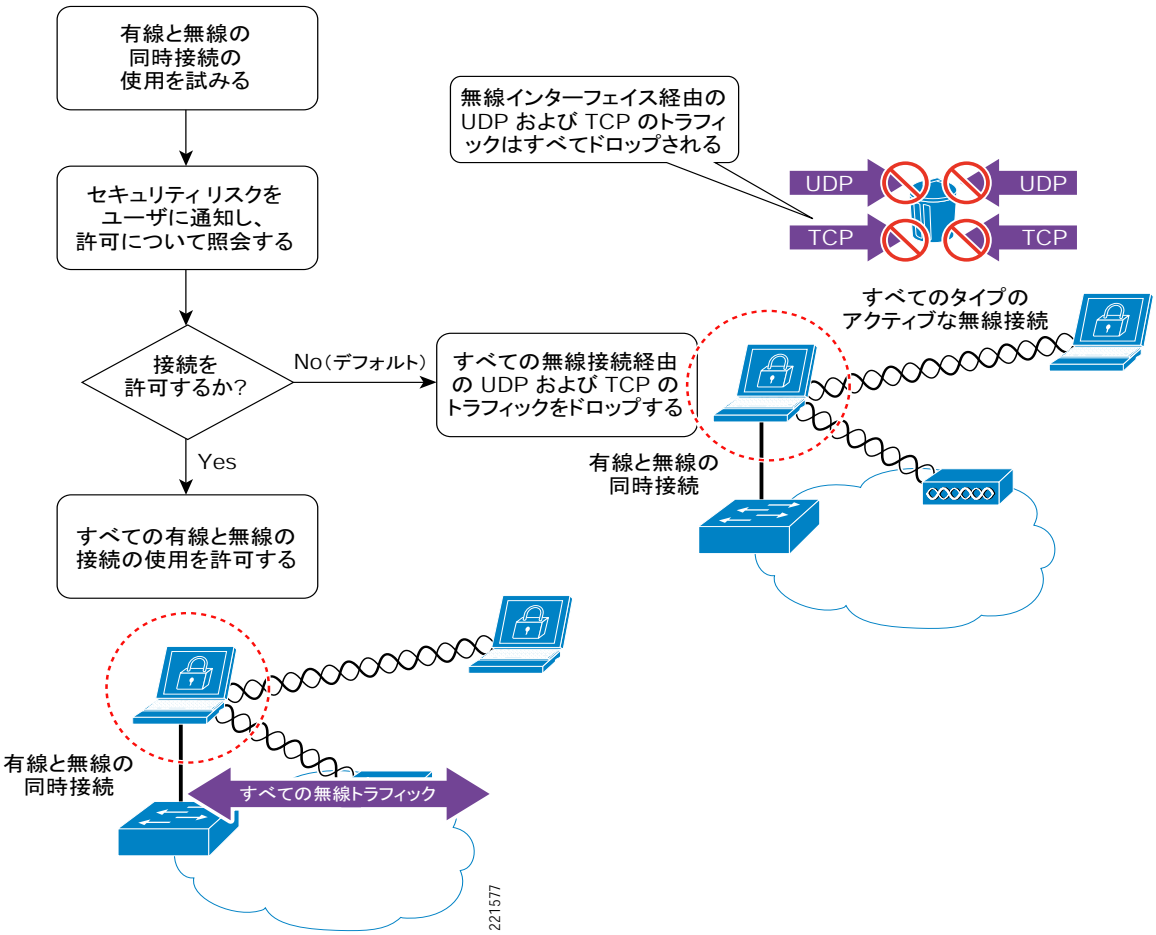
応答のキャッシュを有効にすると、ユーザの作業中断を最小限に抑えることができます。

次に、このカスタマイズした有線と無線の同時接続ルール モジュールを作成する手順の概要を示します。

サンプルのカスタマイズ済みルール モジュールの動作

図 7-37 に、このカスタマイズした有線と無線の同時接続ルール モジュールの動作を示します。

図 7-37　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールの動作



次に、カスタマイズしたサンプル ルール モジュールの動作を示します。

- イーサネット接続がアクティブになっているときに、アクティブな 802.11 無線接続上で UDP または TCP のトラフィックの送信が試行されると、カスタマイズしたルール モジュールが呼び出されます。
- 802.11 無線以外の接続上にあるトラフィックは、このルール モジュールの影響を受けません。
- セキュリティ ポリシーを説明するユーザ クエリーが提示されます。
- ユーザに対して、アクションを許可するか拒否するかのオプションが提示されます。
- デフォルトのアクションは拒否です。
- 802.11 無線接続でルーティングされる UDP および TCP のトラフィックは、すべてドロップされます。

- メッセージがログに記録されます。

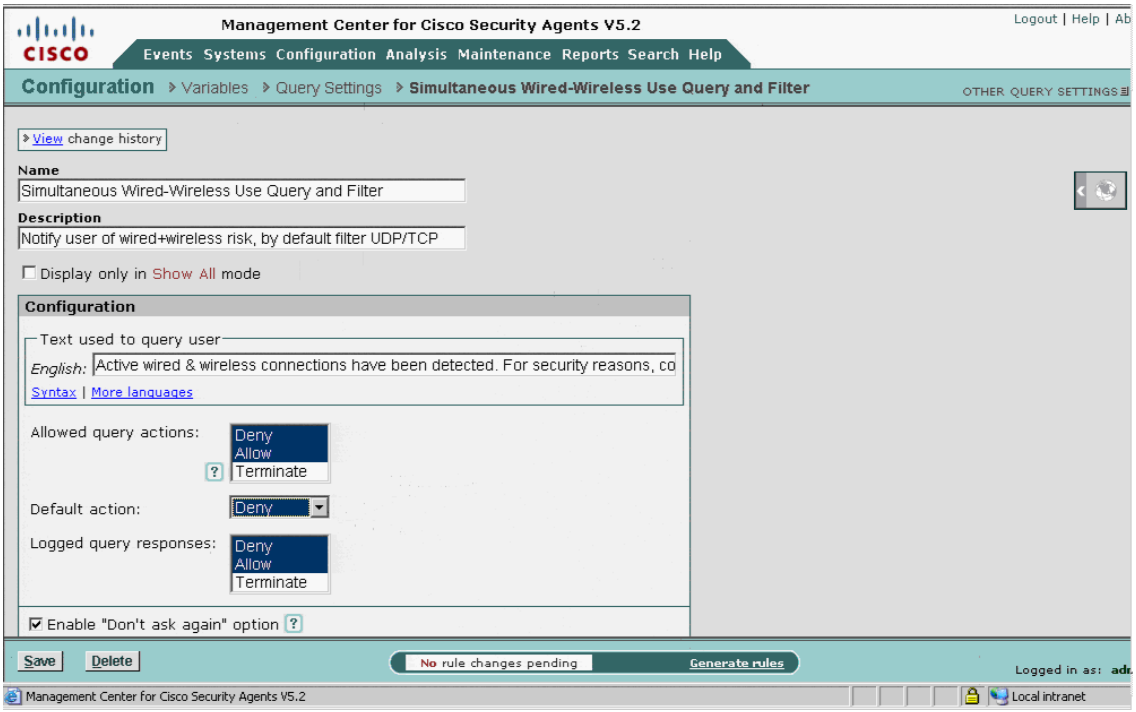
サンプルのカスタマイズ済みルール モジュールの定義

次に、ユーザ クエリーと通知も含めてカスタマイズした、有線と無線の同時接続ルール モジュールを設定する手順を示します。重要な手順については、スクリーンショットの例も示します。

ステップ 1 **Configuration -> Variables -> Query Settings** を使用して、エンド ユーザにイベントを通知するための新しいクエリー設定変数を作成します。ウィンドウ下部の **New** ボタンをクリックします。

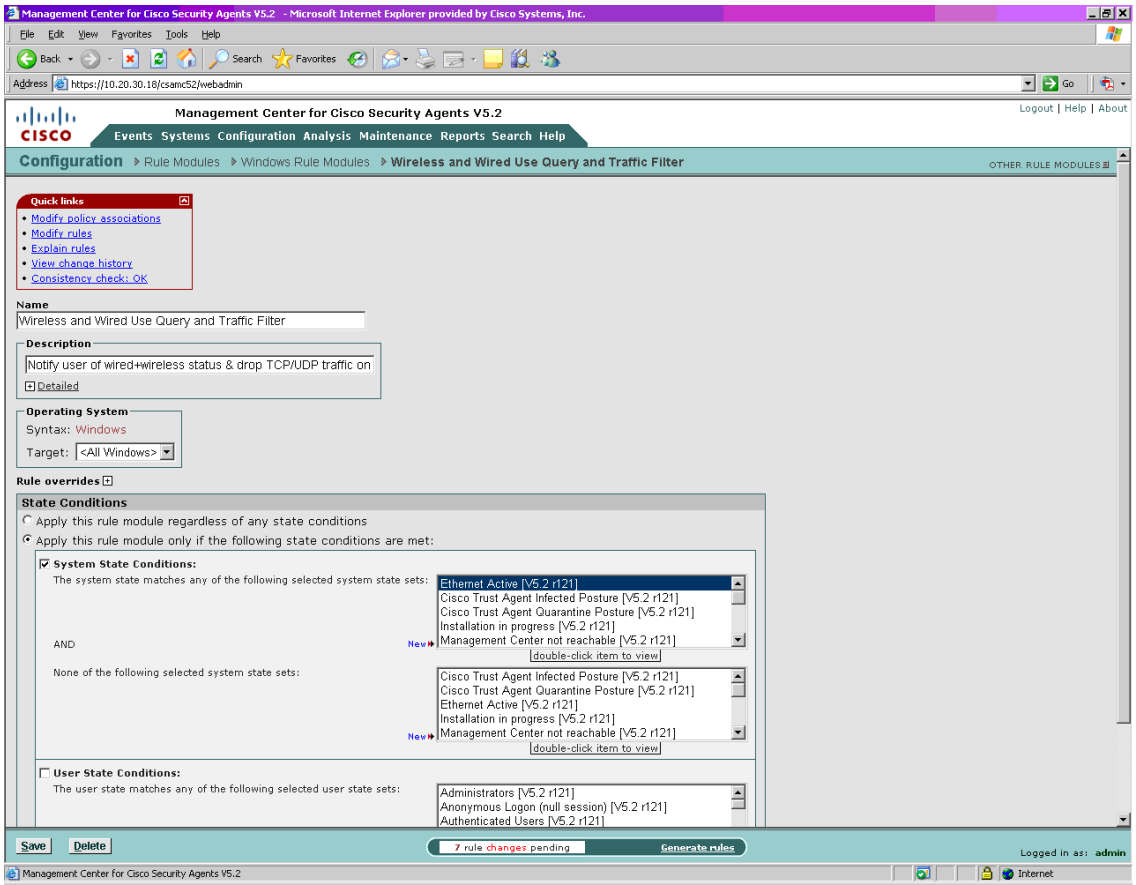
ステップ 2 アクションについての選択肢をユーザに提示するクエリーを設定します。ただし、デフォルトでは拒否アクションを適用します（図 7-38 を参照）。

図 7-38　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールでの新しいクエリー設定変数の定義



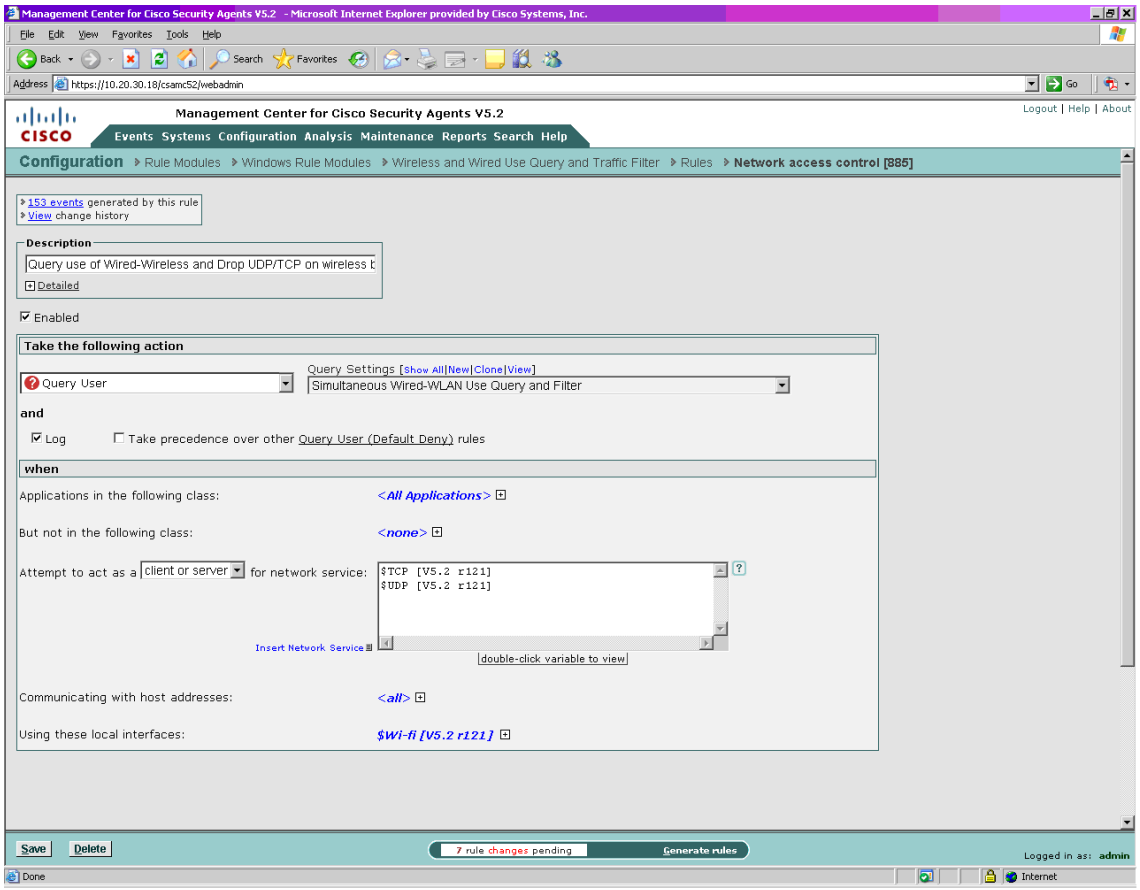
ステップ 3事前定義の有線と無線の同時接続 Windows ルール モジュールを見つけてコピーし、名前を変更します（図 7-39 を参照）。

図 7-39　サンプルの新しいカスタマイズ済み有線と無線の同時接続ルール モジュール



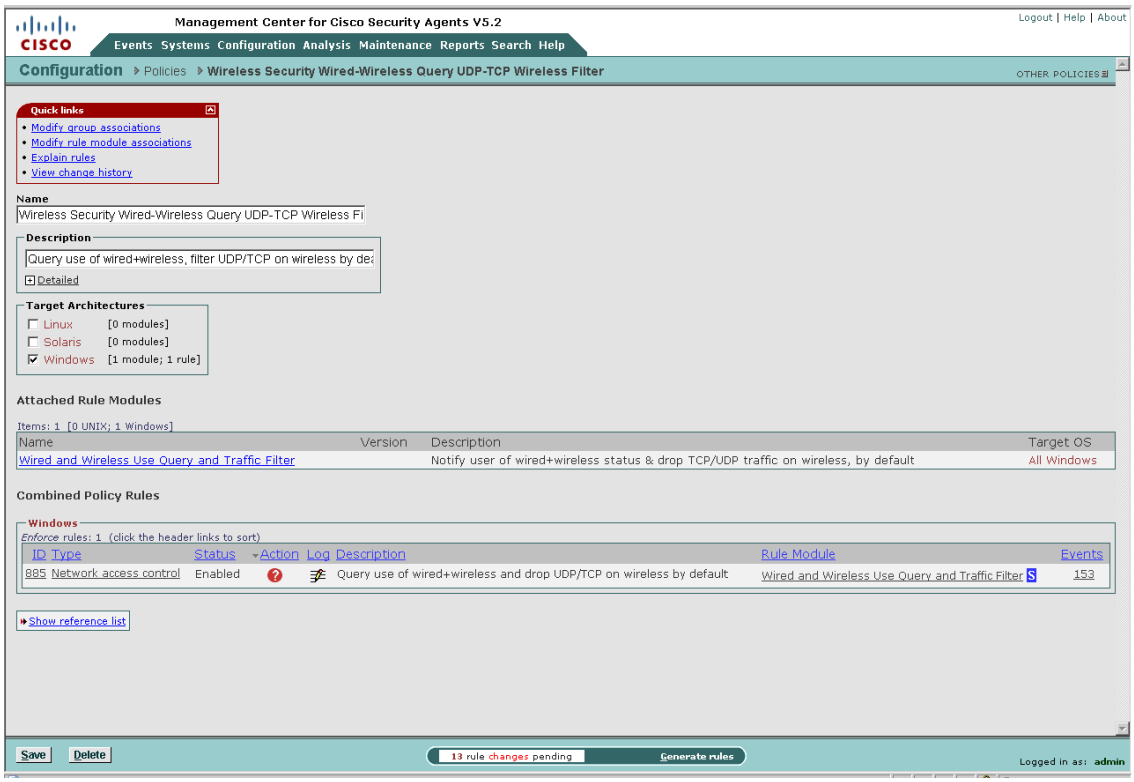
ステップ 4 このカスタマイズした新しい有線と無線の同時接続ルール モジュールに関連付けられているルールを変更して、ユーザにクエリーを提示するようにし、新しいクエリー設定を適用します（図 7-40 を参照）。

図 7-40　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールへの新しいクエリー設定の適用



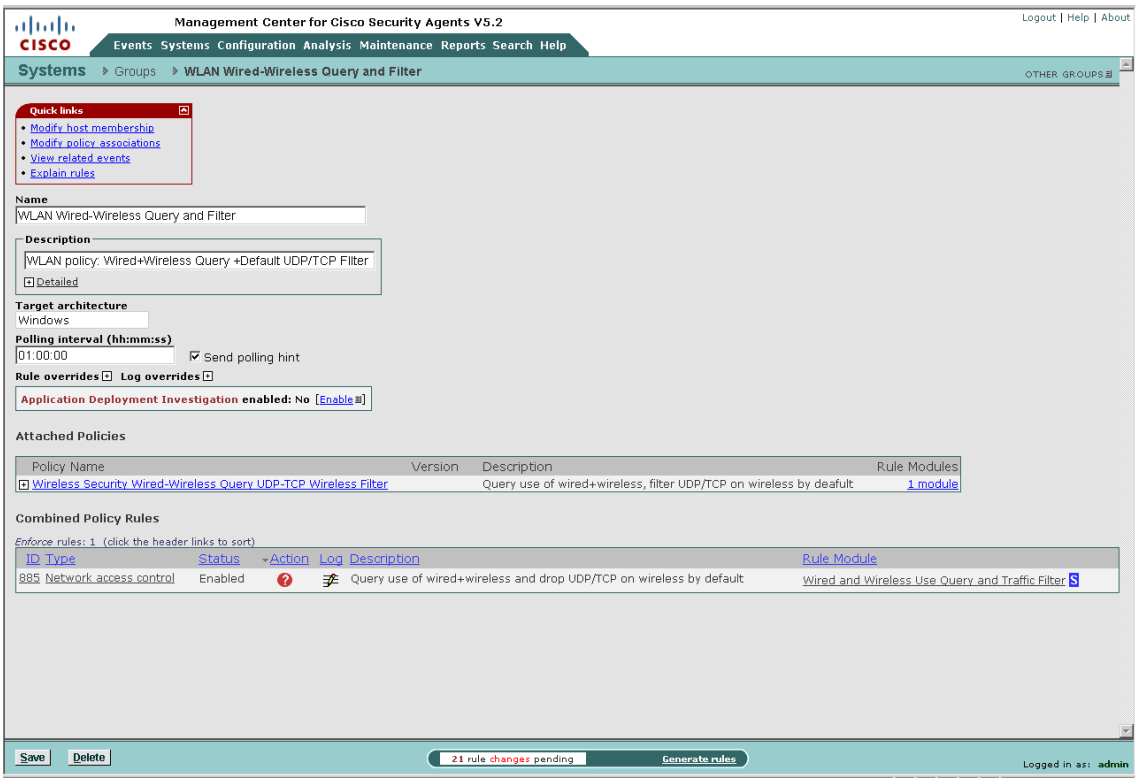
ステップ 5新しいルール モジュールを現在のポリシーに関連付けるか、新しいポリシーを作成します（図 7-41 を参照）。

図 7-41　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールのポリシーへの関連付け



ステップ 6更新したポリシーまたは新しいポリシーを現在のグループに関連付けるか、新しいグループを作成します（図 7-42 を参照）。

図 7-42　サンプルのカスタマイズ済み有線と無線の同時接続ポリシーのグループへの関連付け

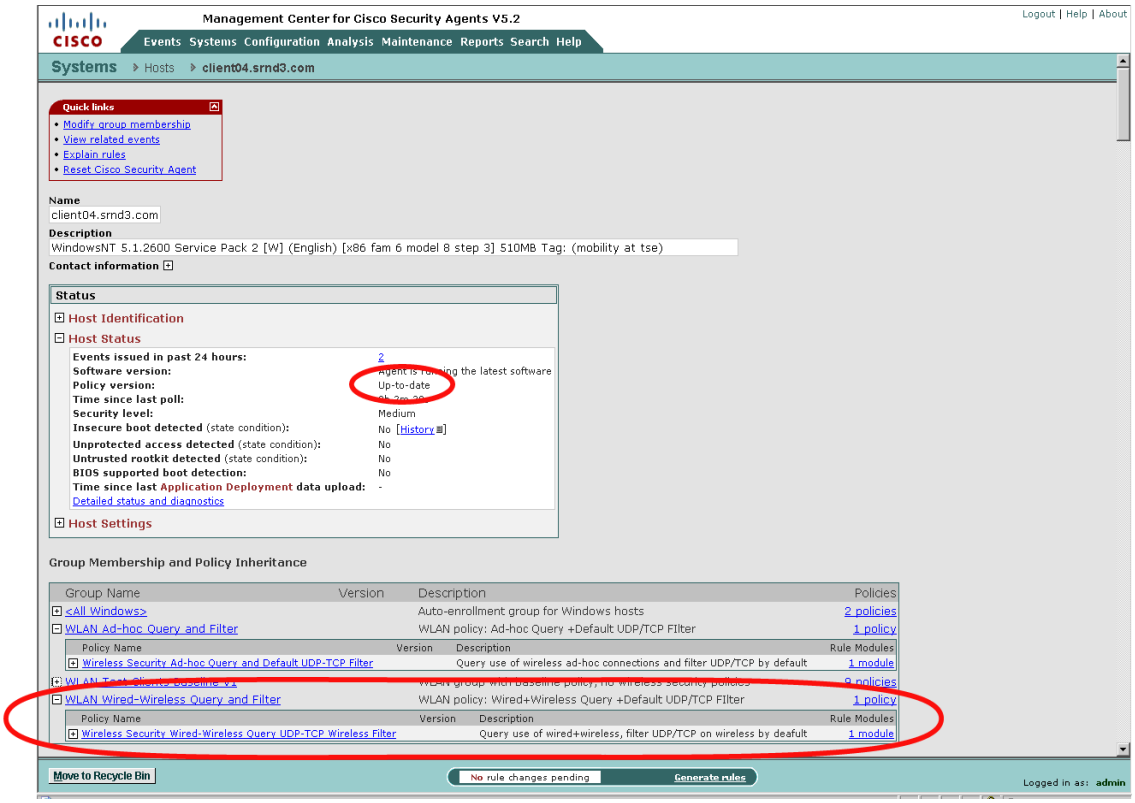


ステップ 7新しいグループを作成した場合は、ホストのメンバシップを必ず更新して、該当するホストにポリシーが適用されるようにします。

ステップ 8ルールを生成して、すべての変更内容を適用します。

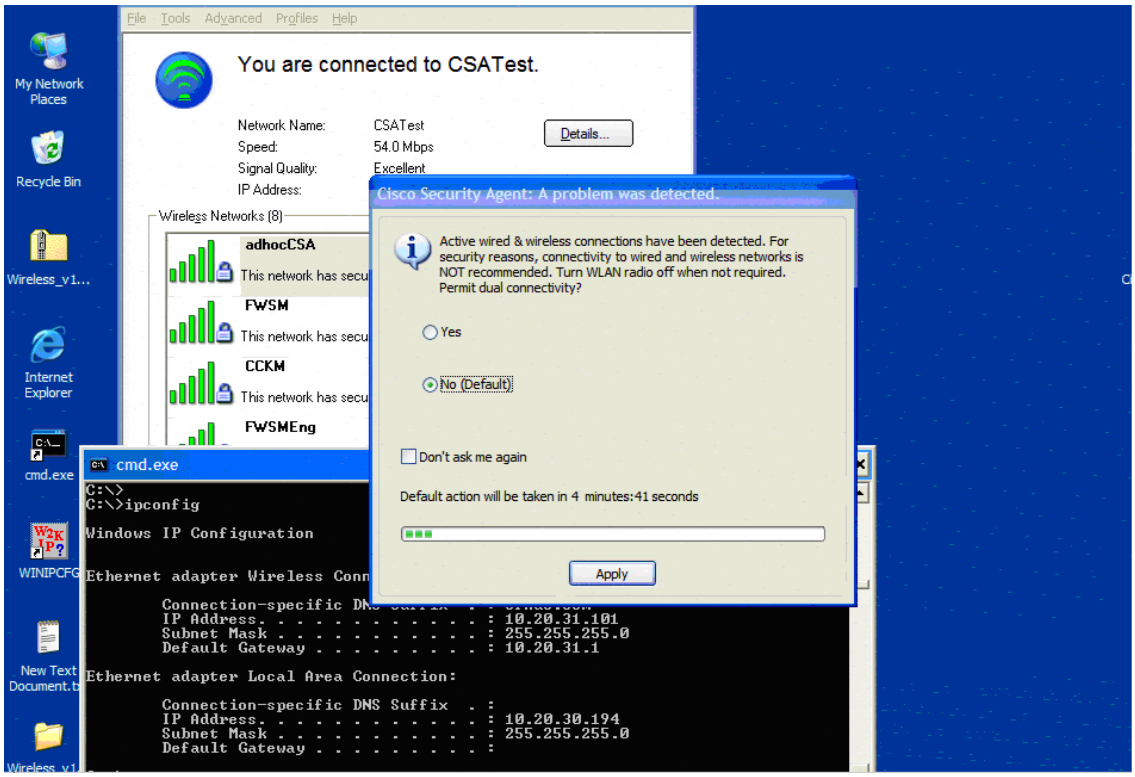
ステップ 9カスタマイズした新しいルール モジュールの動作を確認する前に、ホストが最新のポリシーを実行していることを確認してください（図 7-43 を参照）。

図 7-43　ポリシー ステータスとグループ メンバシップが表示されているホスト詳細情報



ステップ 10イーサネット接続がアクティブになっているホスト上で、802.11 無線接続の使用を試行して、カスタマイズした新しいルール モジュールを確認します（図 7-44 を参照）。

図 7-44　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールを適用した場合のエンド ユーザ通知



サンプルのカスタマイズ済みルール モジュールのロギング

ユーザ クエリー アクションが設定されているカスタマイズ済みルール モジュールでイベント ロギングが有効になっている場合は、ユーザに通知ウィンドウが表示されると Notice イベントが生成されます。

以降の 1 時間以内に、同じ動作によってルール モジュールがトリガーされた場合、そのたびにアラート イベントが生成されます。このアラートでは、ブロックがトリガーされているにもかかわらず、ユーザにクエリーが提示されていないことが示されます。デフォルトでは、**Don't ask again** アクションが有効になっていない場合でも、ユーザ クエリーが実行されるのは、特定のイベント タイプごとに 1 時間に 1 回のみです（図 7-45 を参照）。

図 7-45　サンプルのカスタマイズ済み有線と無線の同時接続ルール モジュールによって生成される CSA MC イベント ログ

テスト環境のハードウェアおよびソフトウェア

表 7-3 に、このマニュアルの記述をサポートするために実施したテストで使用された、主なプラットフォームおよびそのソフトウェア構成を示します。

表 7-3　テスト環境のハードウェアおよびソフトウェア

CSA	ソフトウェア	V5.2.0.203
	CSA MC プラットフォーム	Microsoft Windows 2003 Enterprise Edition Service Pack 1
モバイル クライアント	オペレーティング システム	Microsoft Windows XP Professional Service Pack 2
	無線クライアント	CSSC v5.1.0.39
	無線アダプタ	Intel PRO/Wireless 2915ABG ドライバ バージョン 9.0.4.26

参考資料

Cisco Security Agent（CSA）

- CSA 製品サイト
  http://www.cisco.com/go/csa/
- CSA Trusted QoS
  - Implementing Trusted Endpoint Quality of Service Marking
    http://www.cisco.com/application/pdf/en/us/guest/products/ps6786/c1225/ccmigration_09186a00805b6a81.pdf

Cisco Secure Services Client（CSSC）

- Cisco Secure Services Client（CSSC）
  http://www.cisco.com/en/US/products/ps7034/index.html

Cisco Unified Wireless

- シスコ無線製品
  http://www.cisco.com/en/US/products/hw/wireless/index.html
- 無線ネットワーク セキュリティ
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_package.html
- 不正な AP および無線アドホック接続の監視
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns279/c649/ccmigration_09186a00808d9330.pdf

CS MARS

- CS MARS のユーザ ガイド
  http://www.cisco.com/en/US/products/ps6241/products_user_guide_list.html

無線アドホック接続の脆弱性

- アドホック接続での脆弱性となる Wireless Auto Configuration の動作について説明した Microsoft 記事
  http://technet2.microsoft.com/WindowsServer/en/library/370b019f-711f-4d5a-8b1e-4289db0bcafd1033.mspx?mfr=true
- Windows のアドホック動作が不正利用される場合の手口について説明した Wi-Fi Planet の記事「*The Windows Ad-Hoc Exploit*」
  http://www.wi-fiplanet.com/news/article.php/3578271

CHAPTER 8

シスコの無線 IDS/IPS とネットワーク IDS/IPS の統合

安全な Cisco Unified Network は、有線と無線の両方のアクセスを特徴とし、効果的で一貫性のあるポリシー適用にとって重要なネットワークをまたがる脅威の検出や軽減など、セキュリティに対する統合型の多層防御アプローチを必要とします。無線 IDS/IPS とネットワーク IDS/IPS は両者共、ネットワーク セキュリティの重要な要素であり、脅威の検出および軽減で補完的な役割を果たします。

この章では、無線 Intrusion Detection System/Intrusion Prevention System（IDS/IPS; 侵入検知システム / 侵入防御システム）とネットワーク IDS/IPS の補完的な役割、およびその補完的な役割を Cisco WLAN Controller（WLC; WLAN コントローラ）プラットフォームと Cisco IPS プラットフォームのそれぞれが果たす方法について説明します。また、これら 2 つのシスコ プラットフォームのコラボレーションを有効にすることにより、これらのプラットフォームを使用して、簡単で効果的な自動脅威軽減ツールを提供する方法についても説明します。

Cisco IPS を展開して Cisco Unified Wireless Network と統合するためのガイドラインを示し、自動脅威軽減のために WLC と IPS のコラボレーションを有効にする方法について説明します。

この章で示すソフトウェア実装、スクリーンショット、および動作は、P.8-51 の「テスト ベッドのハードウェアとソフトウェア」に記載のリリースに基づいています。読者は、すでに Cisco Unified Wireless Network と Cisco IPS の両方に精通していることを前提とします。

（注） この章では、Cisco WLC プラットフォームと Cisco IPS プラットフォームに固有の IDS/IPS 統合機能だけを扱います。

WLAN セキュリティにおける無線 IDS/IPS とネットワーク IDS/IPS の役割

Cisco IPS は、ネットワークベースのプラットフォームであり、ワーム、スパイウェア、アドウェア、ネットワーク ウイルス、アプリケーションの不正使用、ポリシー違反といった悪意のあるトラフィックを正確に識別、分類、および阻止するために設計されています。これは、レイヤ 2 ～ 7 での詳細なトラフィック検査によって実現されます。

Cisco WLC の無線 IDS/IPS 機能と Cisco IPS プラットフォームのネットワーク IDS/IPS 機能は、WLAN セキュリティに対する統合型の多層防御アプローチの主要な要素であり、WLAN における脅威の検出と軽減において補完的かつ協力的な役割を果たします。

無線 IDS/IPS とネットワーク IDS/IPS の補完的な役割

無線 IDS/IPS とネットワーク IDS/IPS の補完的な役割により、有線ネットワークで使用されている脅威検出 / 軽減の原理とポリシーを WLAN にまで拡張できます。

無線 IDS/IPS とネットワーク IDS/IPS は、次のように補い合います。

- 無線 IDS/IPS は、802.11 RF メディアに固有の脅威と異常のモニタリング、検出、および軽減にとって重要です。
- ネットワーク IDS/IPS は、クライアント トラフィックの一般的な脅威と異常のモニタリング、検出、および軽減の鍵となり、ネットワーク インフラストラクチャのデバイスおよびサービスの保護にも重要です（図 8-1 を参照）。

図 8-1　WLAN の脅威検出 / 軽減に向けた無線 IDS/IPS とネットワーク IDS/IPS

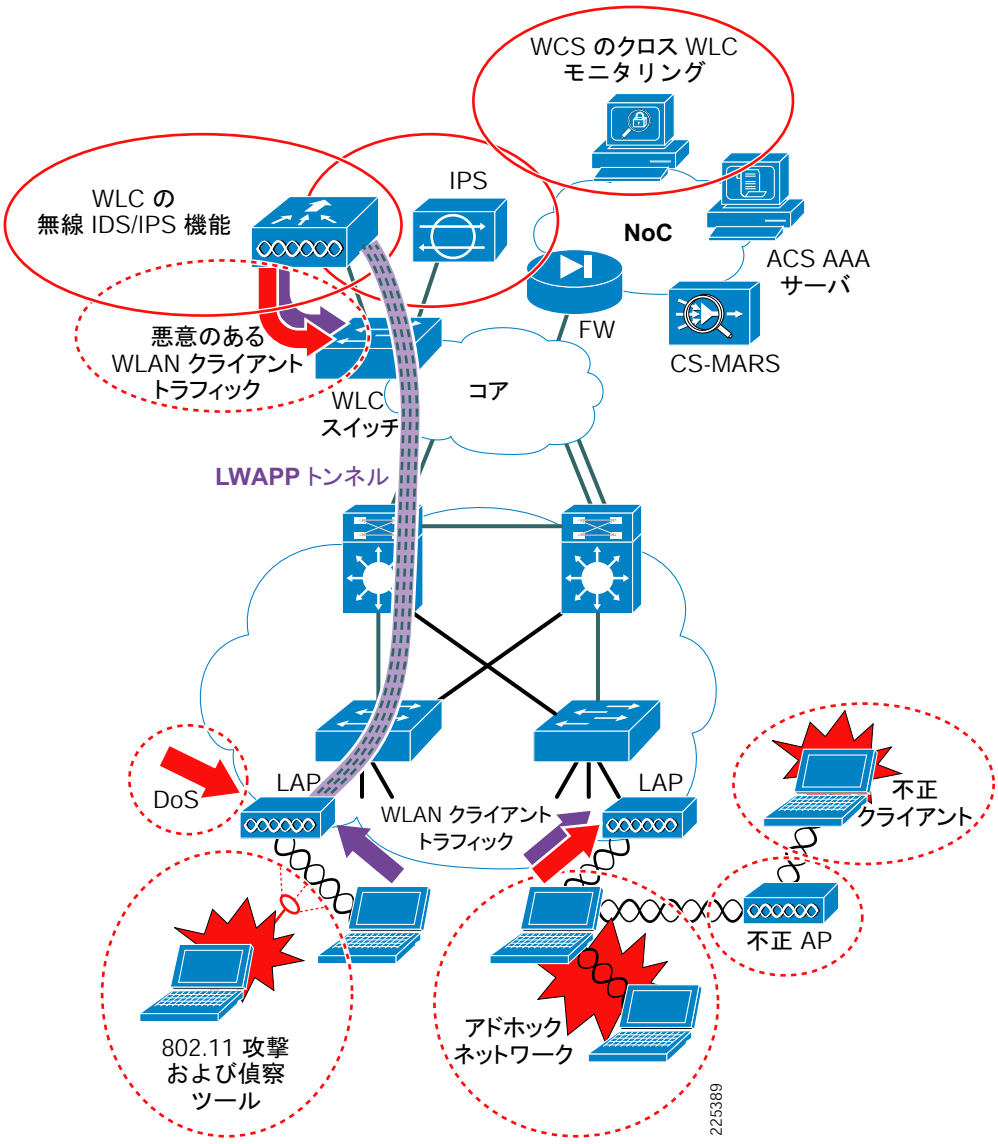


表 8-1 に、WLAN の脅威の検出と軽減における Cisco WLC と Cisco IPS の重要な補完的役割および機能の概要を示します。

表 8-1　WLAN の脅威の検出と軽減における役割

IDS/IPS の要素	WLAN の脅威	WLAN の脅威を検出および軽減するための機能
WLC の無線 IDS/IPS 機能[1]	不正 AP	検出、位置特定、および阻止（有線ネットワーク上のトレースバックを含む）
	不正クライアント	検出および阻止
	無線アドホック ネットワーク	検出および阻止
	802.11 DoS	802.11 DoS 攻撃シグニチャ[2] Cisco Management Frame Protection（MFP; 管理フレーム保護）[3]
	802.11 攻撃ツール	802.11 偵察シグニチャ[2]
	過剰な 802.11 アソシエーションおよび認証	クライアント除外設定による検出、トラッキング、および阻止
	IP の盗難および再使用	検出および阻止
	RF 干渉	動的な無線リソース管理
Cisco IPS プラットフォームのネットワーク IDS/IPS 機能	悪意のある WLAN クライアント トラフィック たとえば、ワーム、ウイルス、アプリケーションの不正使用、スパイウェア、アドウェア、ポリシー違反など[4]	悪意のあるトラフィックの、シグニチャベースの検出、識別、および分類 アラート、SNMP トラップ、パケット ドロップ、接続ブロック、ホスト ブロックなど、使用可能な一連の応答アクション

1. 無線 IDS/IPS 機能は、Cisco WLC によって提供されます。Cisco Mobility Services Engine（MSE; モビリティ サービス エンジン）の Adaptive Wireless IPS 機能については、このガイドでは扱いません。
2. WLC および WCS では、標準のシグニチャが用意されていますが、脅威検出機能を拡張するために開発できるカスタム シグニチャもサポートしています。
3. シスコの管理フレーム保護は、802.11 ベースの DoS 攻撃に対応するためのシグニチャベースの管理フレーム認証を提供するだけでなく、不正 AP の容易な識別も可能にする独自の機能です。管理フレーム保護の詳細については、P.4-18 の「管理フレーム保護」を参照してください。
4. WLAN 環境に展開された Cisco IPS プラットフォームは、WLAN クライアントに対して、有線クライアントに実行するものと同じ、悪意のあるトラフィックのモニタリング、検出、および軽減を実行します。また、通常は、同じポリシーが適用されます。

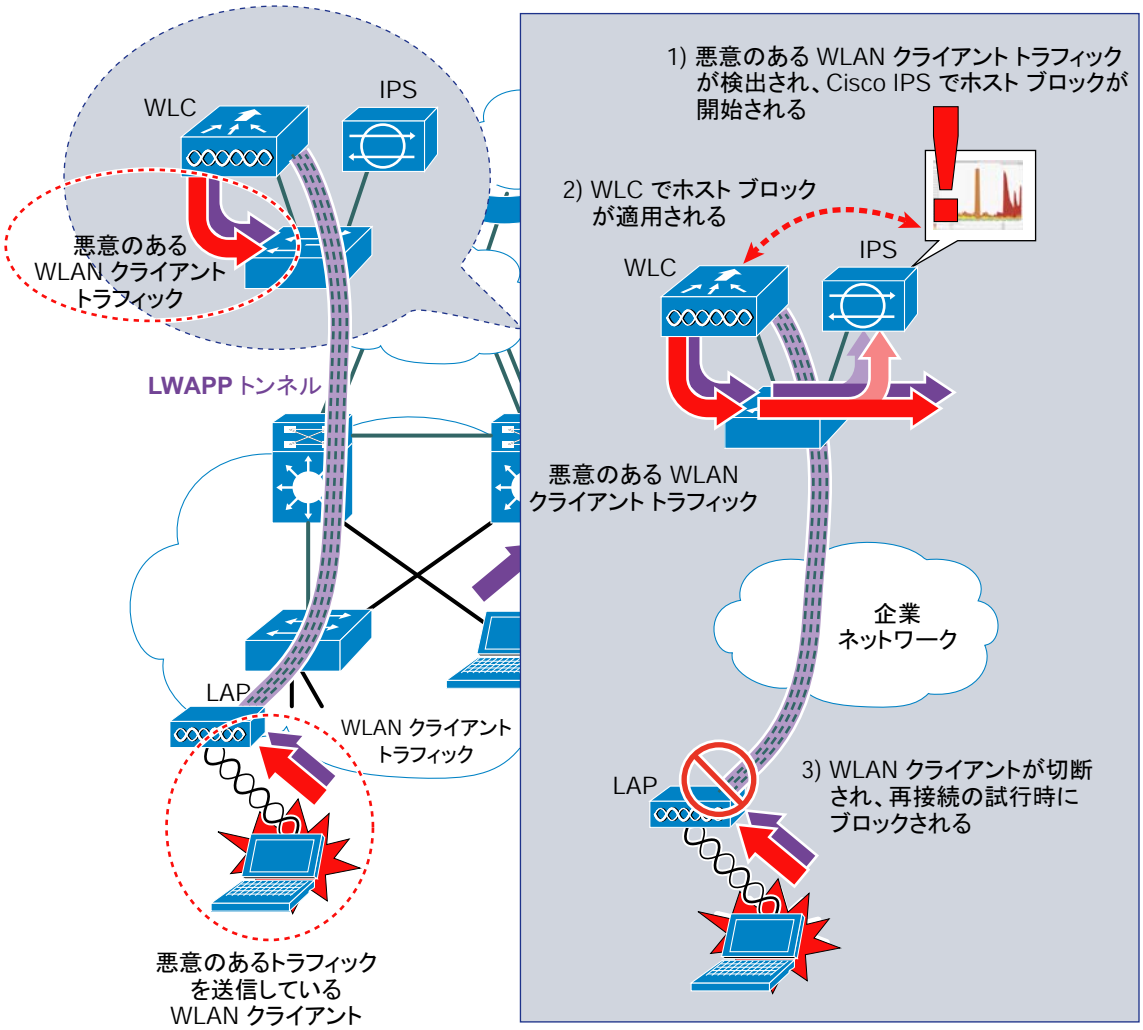
無線 IDS/IPS 機能については、P.4-1 の「Cisco Unified Wireless Network アーキテクチャ：基本的なセキュリティ機能」および P.4-10 の「無線 IDS」で詳しく説明します。

Cisco IPS の詳細については、P.8-52 の「参考資料」を参照してください。

Cisco WLC と Cisco IPS の協力的な役割

Cisco WLC と Cisco IPS のコラボレーションにより、簡単で効果的な自動脅威軽減ツールが提供されます。このツールは、アクセス エッジで、ローカル適用による集中化された制御を実現します。このコラボレーションでは、追加のハードウェアが不要で、設定が非常に簡単であり、これら 2 つのプラットフォームの展開により、脅威の検出と軽減におけるこれらプラットフォームの価値がさらに高まります（図 8-2 を参照）。

図 8-2　自動脅威軽減に向けた Cisco WLC と Cisco IPS の統合



Cisco IPS は、クライアント トラフィックを監視し、脅威や異常を識別すると、ホスト ブロックの作成によってクライアント切断をトリガーします。WLC が Cisco IPS とのコラボレーションにより、WLAN クライアントに対してこの軽減アクションを自動的に適用します。クライアントは、アクセス エッジでネットワークから除外され、ホスト ブロックが削除されるかタイムアウトになるまで再エントリを拒否されます。したがって、Cisco WLC と Cisco IPS のコラボレーションにより、異常な動作の検出時に使用できる追加の自動脅威軽減ツールが運用スタッフに提供されます。

Cisco WLC と Cisco IPS のコラボレーションの仕組み

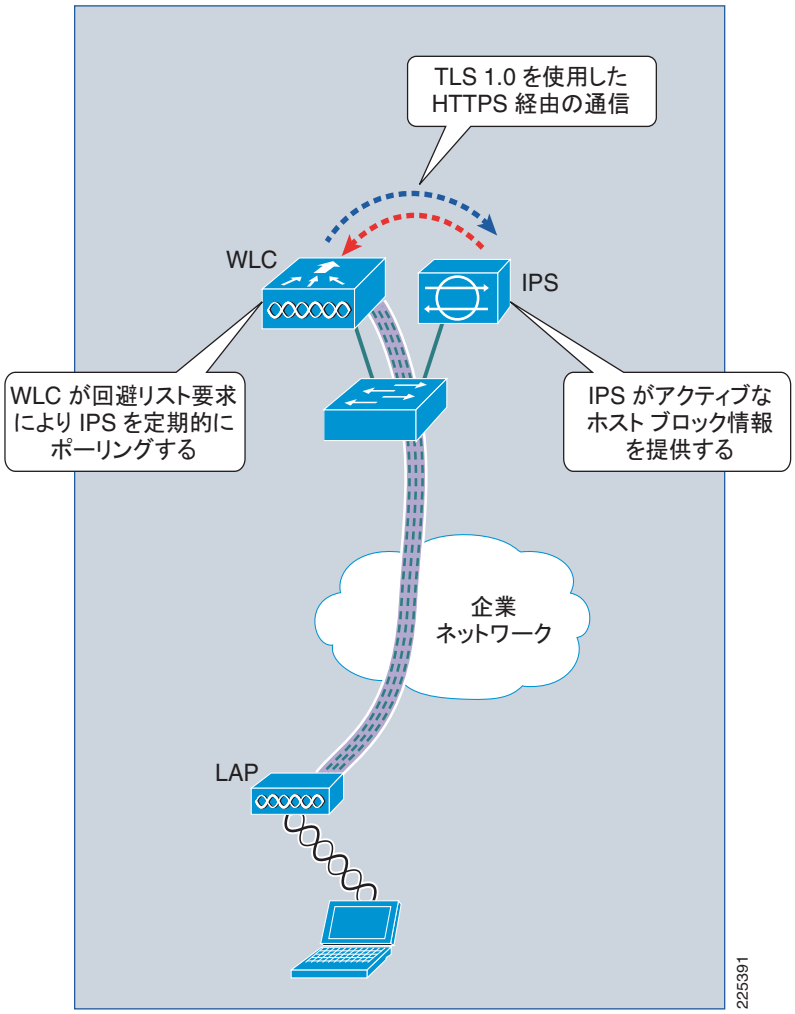
Cisco WLC と Cisco IPS のコラボレーションにより、自動脅威軽減ツールが提供され、IPS 上のホスト ブロック アクティベーションを WLAN で直接適用できるようになります。このコラボレーションには、次の主な動作要素が含まれます。

- Cisco WLC と Cisco IPS の同期化
- WLC による Cisco IPS ホスト ブロックの適用
- Cisco IPS ホスト ブロックの取り消し

Cisco WLC と Cisco IPS の同期化

Cisco WLC と Cisco IPS は、WLC が Shun リスト要求により IPS を定期的にポーリングすることで、アクティブなホスト ブロック情報を同期させます。Cisco IPS は、アクティブなホスト ブロック リストで応答します（図 8-3 を参照）。

図 8-3　Cisco WLC と Cisco IPS の同期化



次の点に注意してください。

- Cisco WLC と Cisco IPS 間の通信は、Transport Layer Security（TLS）1.0 を使用して HTTPS で行われます。これにより、X.509 証明書を使用して IPS の ID が認証されること、およびデータが SHA-1 ハッシュ アルゴリズムで暗号化されることが保証されます。
- IPS とのコラボレートには、モビリティ グループ内の 1 つの WLC だけが必要です。モビリティ グループ内のすべての WLC に、アクティブなホスト ブロック情報が自動的に渡されます。ただし、冗長性を確保するために、モビリティ グループ内の複数の WLC が同じ IPS とコラボレートするように設定できます。
- 1 つの WLC が複数の IPS デバイスとコラボレートできます。

WLC による Cisco IPS ホスト ブロックの適用

Cisco WLC と Cisco IPS のコラボレーションによって、自動脅威軽減が提供されます。これにより、Cisco WLC に Cisco IPS ホスト ブロックが渡され、一致する WLAN クライアントがある場合、Cisco WLC がそのホスト ブロックを適用できるようになります。

クライアント トラフィック内の異常なアクティビティが IPS によって検出された場合、その後の調査により、その異常を生成しているクライアントをブロックするという決定が下されることがあります。このブロックは、Cisco IPS で開始して、IPS で直接適用するか、または WLC などの別のネットワーク デバイスとのコラボレーションによって適用することができます。Cisco IPS での適用は拒否アクションによって行われ、別のネットワーク デバイスでの適用はブロック アクションによってアクティブになります。

Cisco IPS の拒否アクションとブロック アクションの詳細については、P.8-50 の「Cisco IPS のブロック アクションと拒否アクション」を参照してください。

（注）　アクションの実行前に、脅威が正確に識別、分類、およびトレースされていることを確認することが重要です。さらに、異常な動作がホストに対する DoS 試行でないことを確認してください。

WLC などの別のネットワーク デバイスでホスト ブロックを適用できるようにするために、次のいずれかの方法により、Cisco IPS でホスト ブロックをアクティブにできます。

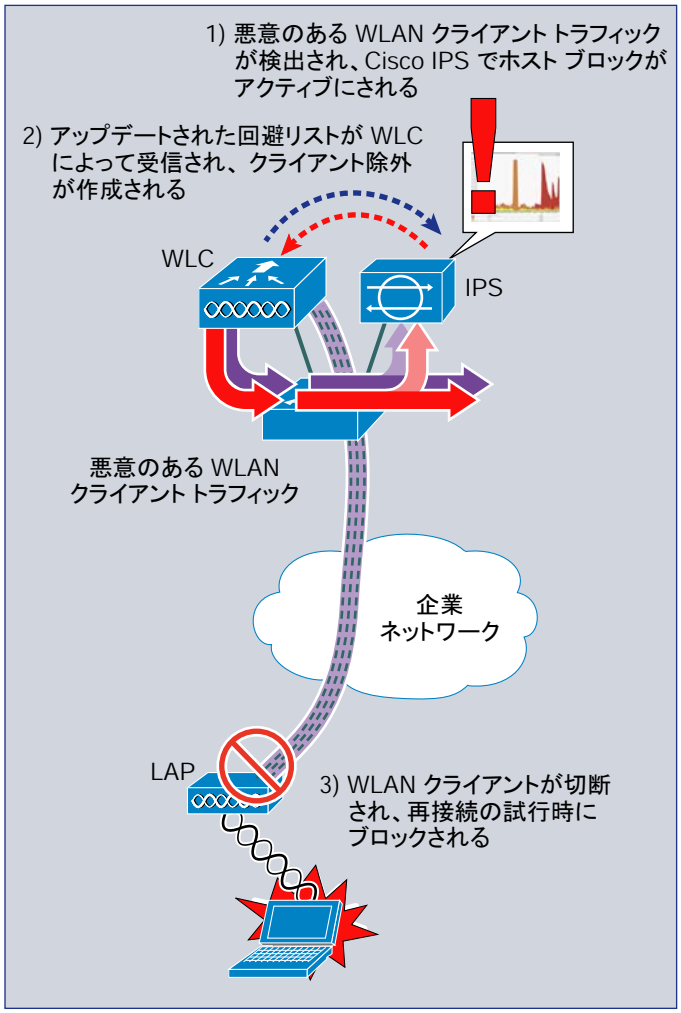
- 手動によるホスト ブロックの作成
- 「Request Block Host」アクションとシグニチャの関連づけによる自動適用
- 「Request Block Host」アクションと、特定の Risk Rating（RR; リスク評価）しきい値に基づくイベント アクション オーバーライドの関連づけによる自動適用

（注）　ブロッキング アクションの自動適用は、IPS の一般的な設計ガイドラインに従って慎重に使用する必要があります。IPS の展開と調整のガイドラインが記載されたマニュアルについては、P.8-52 の「参考資料」を参照してください。

WLC は、次に Shun リスト要求により IPS をポーリングしたときに、IPS ホスト ブロック情報を受信します。そのホスト ブロック情報に一致する WLAN クライアントが WLC にアソシエートされている場合、WLC は、そのホストの WLAN クライアント除外を作成して、そのホスト ブロックを適用します。WLAN クライアントは WLAN から切断され、ホスト ブロック アクションがアクティブである間、再接続をブロックされます。

図 8-4 に、WLC が WLAN クライアントに Cisco IPS ホスト ブロックを適用する様子を示します。

図 8-4　WLC による Cisco IPS ホスト ブロックの適用



次に、WLC が Cisco IPS ホスト ブロックを適用する手順を示します。

ステップ 1ホスト ブロックが Cisco IPS で開始され、ブロックするクライアントの送信元 IP アドレスを定義します。

ステップ 2WLC が、次に Shun リスト要求により IPS をポーリングしたときに、アップデートされたアクティブなホスト ブロック リストを受信します。

ステップ 3WLC が回避クライアント リストをアップデートして、IPS の最新のアクティブ ホスト ブロック情報を反映させます。

ステップ 4WLC が、現在アソシエートされているクライアントの送信元 IP アドレスが回避クライアント リスト内のエントリに一致するかどうかを確認します。

ステップ 5アソシエートされている WLAN クライアントの送信元 IP アドレスが回避クライアントに一致する場合、WLC は、そのクライアントの MAC アドレスに基づいてクライアント除外を作成し、IPS ホスト ブロック アクションを適用します。

ステップ 6ブロック対象の WLAN クライアントが切断されます。

ステップ 7IPS ホスト ブロックが有効である間、除外された MAC アドレスを持つ WLAN クライアントは、アソシエートを試みるたびに WLC によって切断されます。

ステップ 8ホスト ブロックは、期限切れになるか削除されるまで IPS 上でアクティブなままです。

ステップ 9クライアント除外は、タイムアウトになるまで WLC 上でアクティブなままです。クライアント除外のタイムアウトは、WLC で WLAN プロファイルごとに定義されるもので、IPS で定義されるホスト ブロック タイムアウトとは無関係です。

ステップ 10WLC でクライアント除外が期限切れになっても、IPS でホスト ブロックがまだアクティブである場合、ブロック対象の送信元 IP アドレスを持つクライアントが WLC にアソシエートされるか、アソシエートを試みていると、WLC は新しいクライアント除外を作成します。

Cisco IPS ホスト ブロックの取り消し

Cisco IPS ホスト ブロックの取り消しは、次のいずれかのイベントに基づいて行われます。

- ホスト ブロックのタイムアウト
- ホスト ブロックの手動削除

Cisco IPS ホスト ブロックが取り消されると、WLC は、IPS への次回のポーリングで、アップデートされたアクティブなホスト ブロック リストを受信し、回避クライアント リストをアップデートします。

次に、WLAN クライアントの Cisco IP ホスト ブロックの取り消しで WLC が実行する手順を示します。

ステップ 1 Cisco IPS のアクティブなホスト ブロック情報がアップデートされ、以前ブロックされていたホストの送信元 IP アドレスを含まなくなります。

ステップ 2WLC が、次に Shun リスト要求により IPS をポーリングしたときに、アップデートされたアクティブなホスト ブロック リストを受信します。

ステップ 3WLC が回避クライアント リストをアップデートし、IPS の最新のアクティブ ホスト ブロック情報を反映させ、ブロックされなくなったホストをすべて削除します。

ステップ 4以前ブロックされていたホストにアソシエートされているアクティブな WLC クライアント除外は、クライアントが接続されている WLAN プロファイルのクライアント除外タイムアウト値に基づいてタイムアウトになります。

ステップ 5クライアント除外タイムアウトになると、以前ブロックされていたホストがブロックされなくなります。

Cisco Unified Wireless と IPS の統合

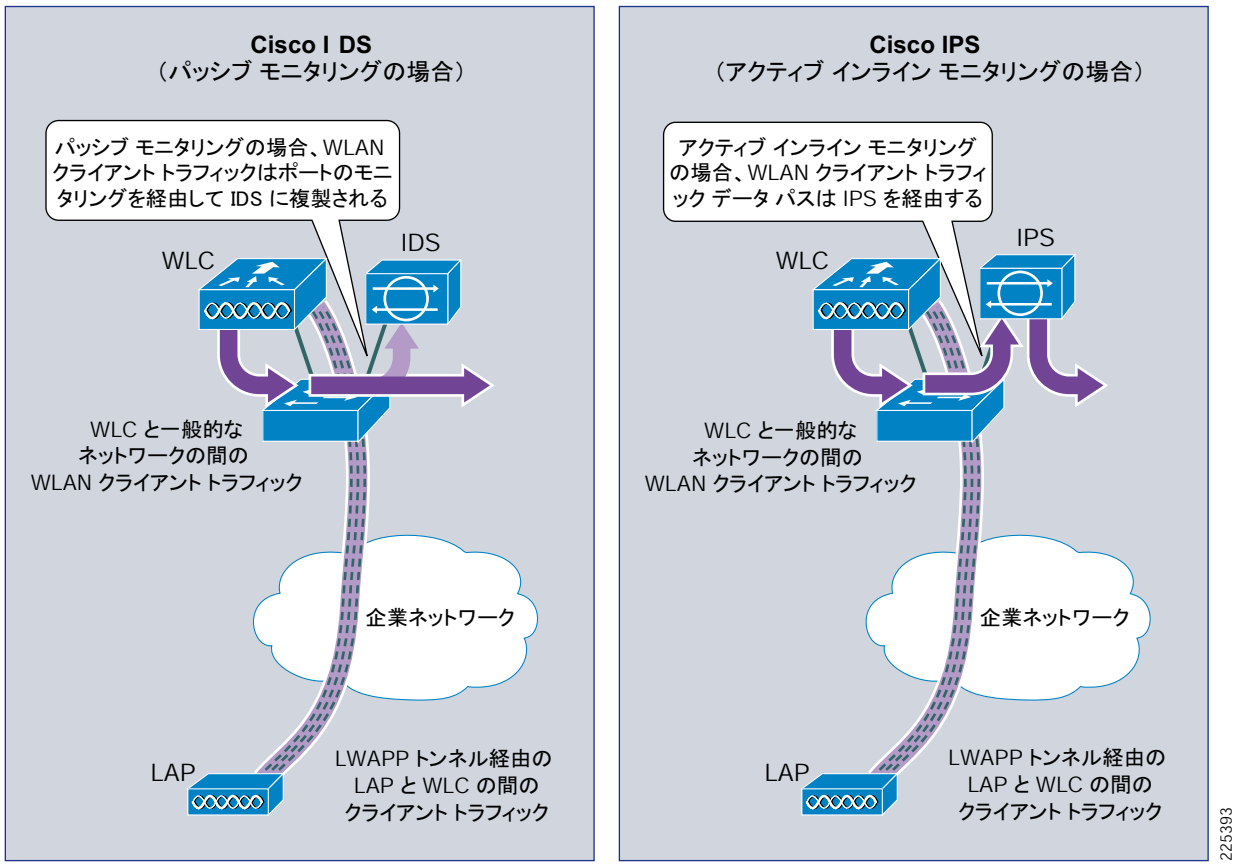
この項では、Cisco IPS と Cisco Unified Wireless Network の統合に必要な手順、および Cisco WLC と Cisco IPS のコラボレーションを有効にして、簡単で効果的な自動脅威軽減ツールを提供する方法について説明します。このコラボレーションは、追加のハードウェアが不要で、設定が非常に簡単です。

Cisco IPS の設定は、Cisco IDS Device Manager（IDM）を使用して示されています。Cisco WLC の設定は、WLC の GUI を使用して示されています。

IPS の展開と統合

Cisco Unified Wireless Network では、すべての WLAN クライアント トラフィックが WLC を介して企業ネットワークに入ります。これにより、このトラフィックに対して脅威の検出と軽減を実行するための最適な場所、および Cisco IPS のための簡単な統合ポイントが提供されます（図 8-5 を参照）。

図 8-5　Cisco Unified Wireless と IPS 展開モード



Cisco IPS を IDS として展開して、Promiscuous（無差別）モードのパッシブ モニタリングを使用するか、または IPS として展開して、インライン モードのアクティブ モニタリングを使用することができます。Cisco WLC とのコラボレーションの目的で、Cisco IPS を IDS モードまたは IPS モードのいずれかで展開できます。IPS ではなく WLC でホスト ブロックが適用されるため、センサーはインラインでなくてもかまいません。したがって、IPS 展開モードの選択は、ネットワーク設計の一般的な選択です。

IPS 展開モードの詳細については、P.8-50 の「Cisco IPS の展開モード」を参照してください。

次の点に注意してください。

- Cisco IPS は、WLAN クライアント トラフィック上で、有線クライアント トラフィック上と同じモニタリングおよび異常検出を実行します。

- Cisco IPS を展開してどのインターフェイス、サブインターフェイス、および VLAN を監視するかを設定できます。したがって、IPS を展開して、WLC 無線 VLAN のすべてまたはサブセットを監視できます。
- IPS は、WLAN トラフィックのモニタリング専用である必要はありません。有線トラフィックと無線トラフィックの両方を監視するために IPS を展開できます。

IPS の詳細な設計ガイダンスについては、P.8-52 の「参考資料」に記載のマニュアルを参照してください。

Cisco WLC と Cisco IPS のコラボレーションの有効化

Cisco WLC と Cisco IPS のコラボレーションでは、次の簡単な手順を実行する必要があります。

- Cisco IPS で WLC のユーザ アカウントを作成する。
- Cisco IPS で WLC を許可ホストとして定義する。
- Cisco WLC で Cisco IPS を CIDS センサーとして定義する。
- WLAN プロファイルでクライアント除外を有効にする。

次に、各手順を実行する方法の詳細を示します。

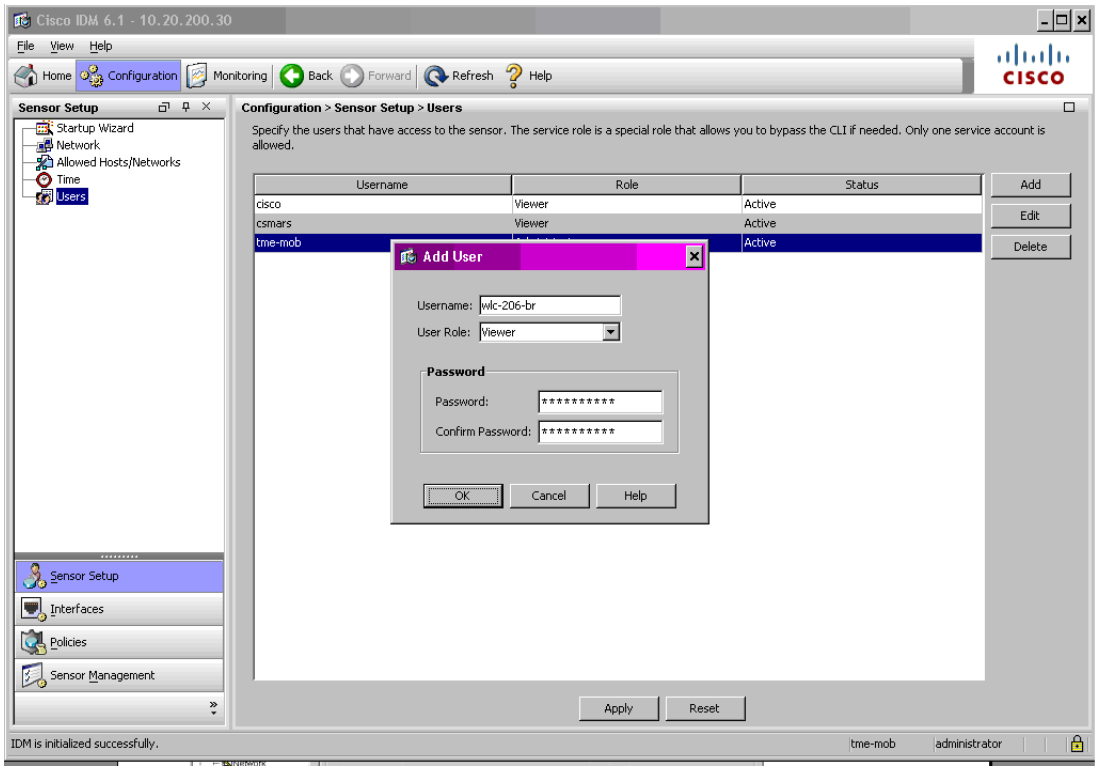
Cisco WLC と Cisco IPS のコラボレーションを有効にするための最初の手順は、WLC が IPS からアクティブなホスト ブロック情報を入手できるようにすることです。

ステップ 1 Cisco IPS で、WLC のユーザ アカウントを作成します。

これにより、WLC が IPS からアクティブなホスト ブロック情報を入手できるようになります。

IDM で、**Configuration -> Sensor Setup -> Users** の順に進みます。ユーザ ロール **Viewer** で新しいユーザを追加し、パスワードを設定します（図 8-6 を参照）。

図 8-6　　Cisco IPS で WLC のユーザ アカウントを作成する



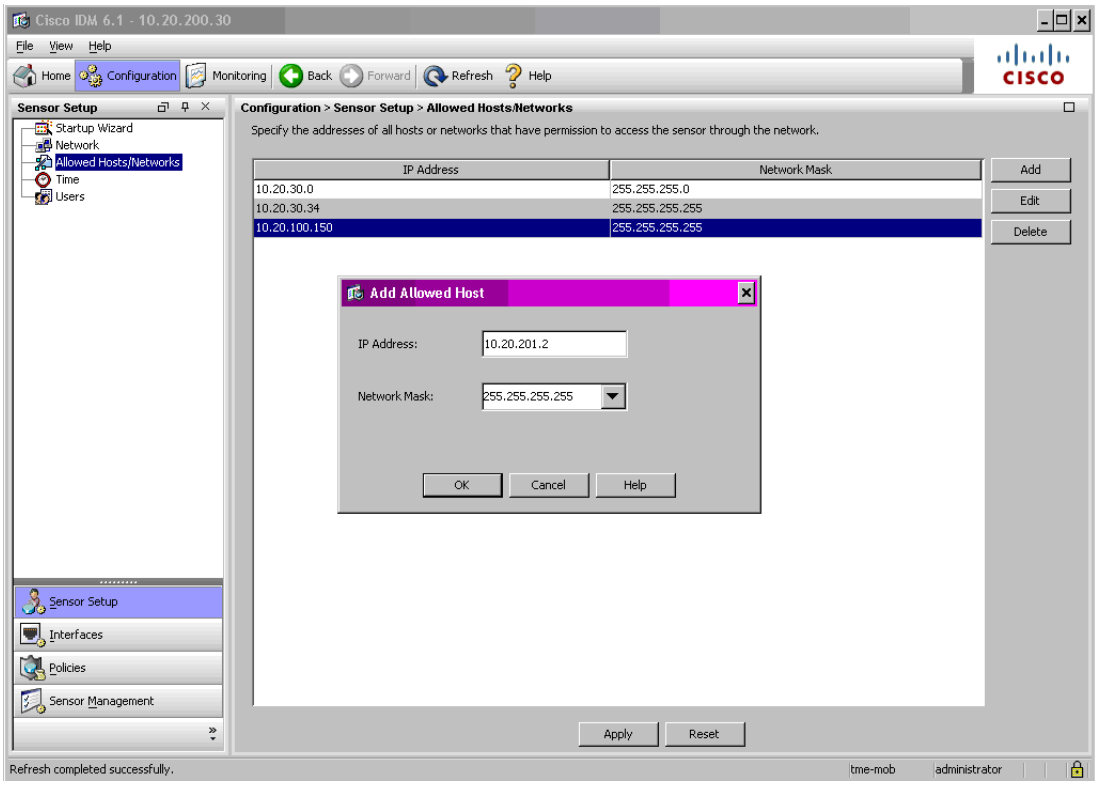
次の点に注意してください。

- WLC ごとに個別のユーザ アカウントを作成することをお勧めします。これにより、トラブルシューティングやモニタリングが容易になります。
- WLC には、ユーザ ロール「Viewer」で提供される表示アクセスだけを許可する必要があります。このアクセスだけが必要です。これにより、セキュリティ ベスト プラクティスとして推奨されているとおり、必要最小限のアクセス権限だけが付与されることが保証されます。
- 強力なパスワード ポリシーが適用されていることを確認します。
- IPS とのコラボレートには、モビリティ グループ内の 1 つの WLC だけが必要です。ただし、冗長性を確保するために、複数の WLC を設定できます。

ステップ 2 Cisco IPS で、WLC を許可ホストとして定義します。これにより、WLC ホストがアクティブなホスト ブロック リストを取得するために IPS と通信できるようになります。

IDM v6.1 で、**Configuration -> Allowed Hosts/Networks** の順に進みます。WLC の送信元 IP アドレスとネットワーク マスクで、許可ホストを追加します（図 8-7 を参照）。

図 8-7　　Cisco IPS で WLC を許可ホストとして定義する



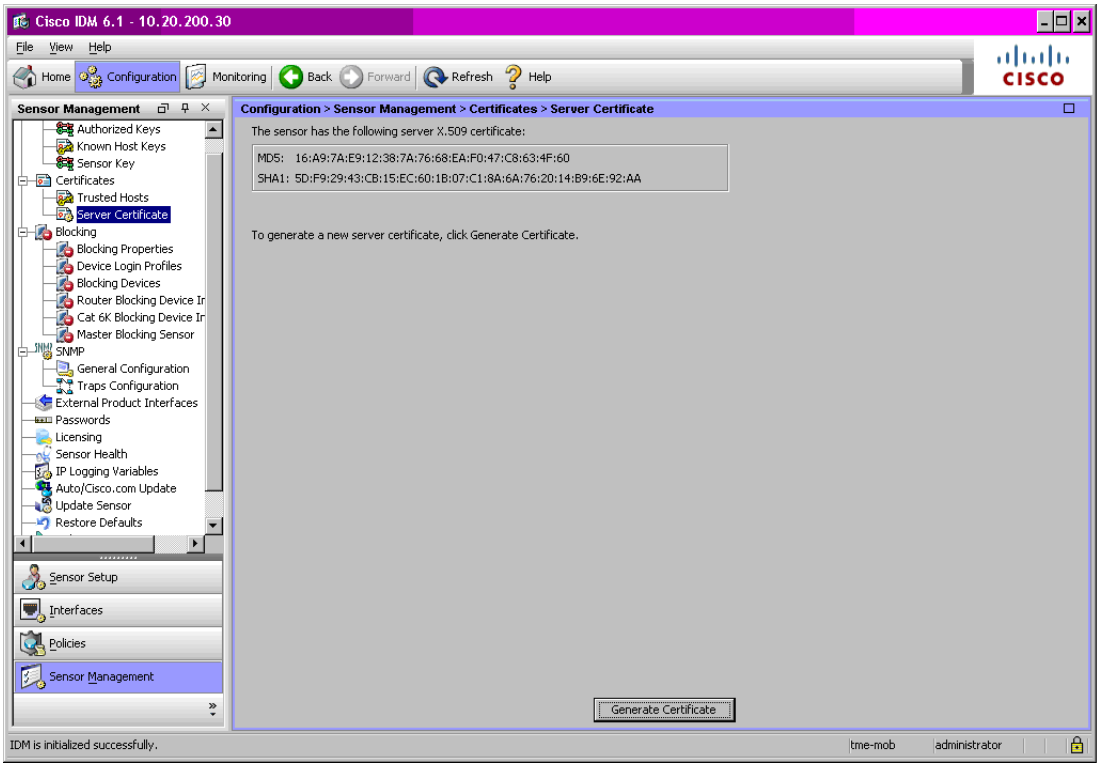
次の点に注意してください。

- 適切なネットワーク マスクを使用して、1 つのホスト IP アドレスまたはネットワーク IP アドレス範囲を定義できます。これは、通常、企業のネットワーク セキュリティ ポリシーによって決まりますが、一般的には管理の容易さとセキュリティ リスクの間のトレードオフです。

ステップ 3 Cisco IPS の TLS フィンガープリントを入手します。

TLS フィンガープリントは、IPS のサーバ側の X.509 証明書です。このフィンガープリントは、サーバを認証するため、および WLC と IPS 間の通信をセキュリティで保護するために TLS 1.0 で使用されます。IDM で、**Configuration -> Sensor Setup -> Certificates -> Server Certificate** の順に進みます（図 8-8 を参照）。

図 8-8　　Cisco IPS の TLS フィンガープリントの例



TLS フィンガープリントは、Cisco IPS の CLI で次のコマンドを入力して取得することもできます。

```
show tls fingerprint
```

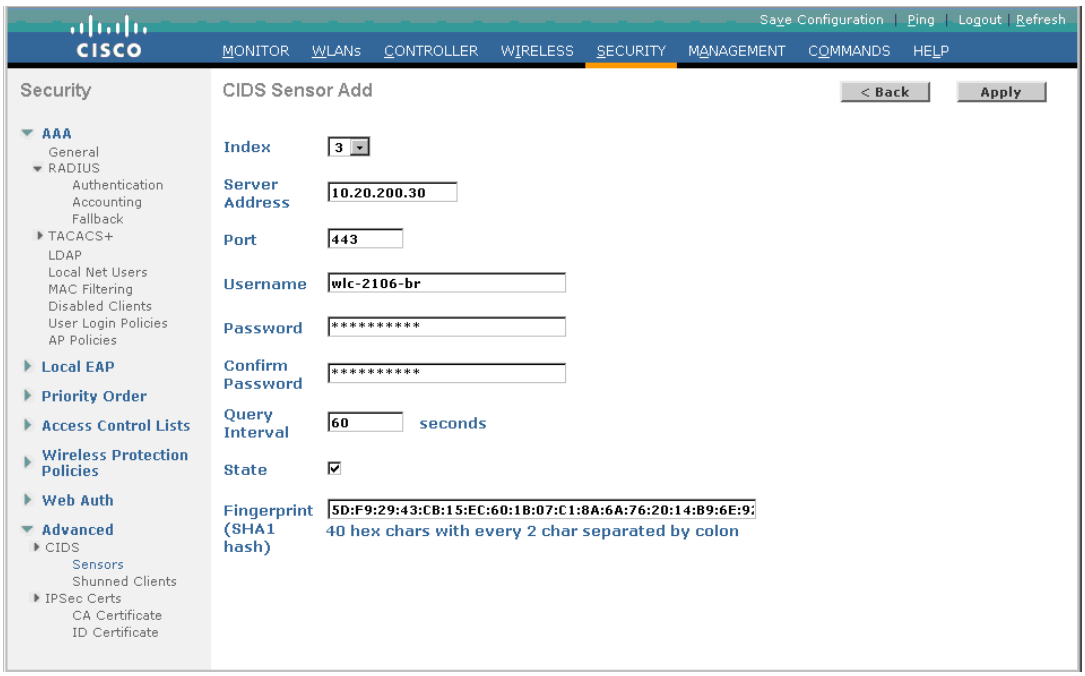
TLS フィンガープリントの例は、次のとおりです。

```
ips-3845-2# show tls fingerprint
MD5: 16:A9:7A:E9:12:38:7A:76:68:EA:F0:47:C8:63:4F:60
SHA1: 5D:F9:29:43:CB:15:EC:60:1B:07:C1:8A:6A:76:20:14:B9:6E:92:AA
```

ステップ 4 Cisco IPS とコラボレートする各 WLC で、IPS を CIDS センサーとして定義します。

WLC で、**Security -> CIDS -> Sensors** の順に進みます。IPS の IP アドレスで、新しい CIDS センサーを追加します。IPS で作成した WLC ユーザ アカウントのユーザ名とパスワード（ステップ 1 で指定）を入力します。**State** ボックスをオンにしてセンサーをアクティブにし、IPS の TLS フィンガープリントを入力して、**Apply** ボタンを選択します（図 8-9 を参照）。

図 8-9　　WLC で IPS を CIDS センサーとして定義する



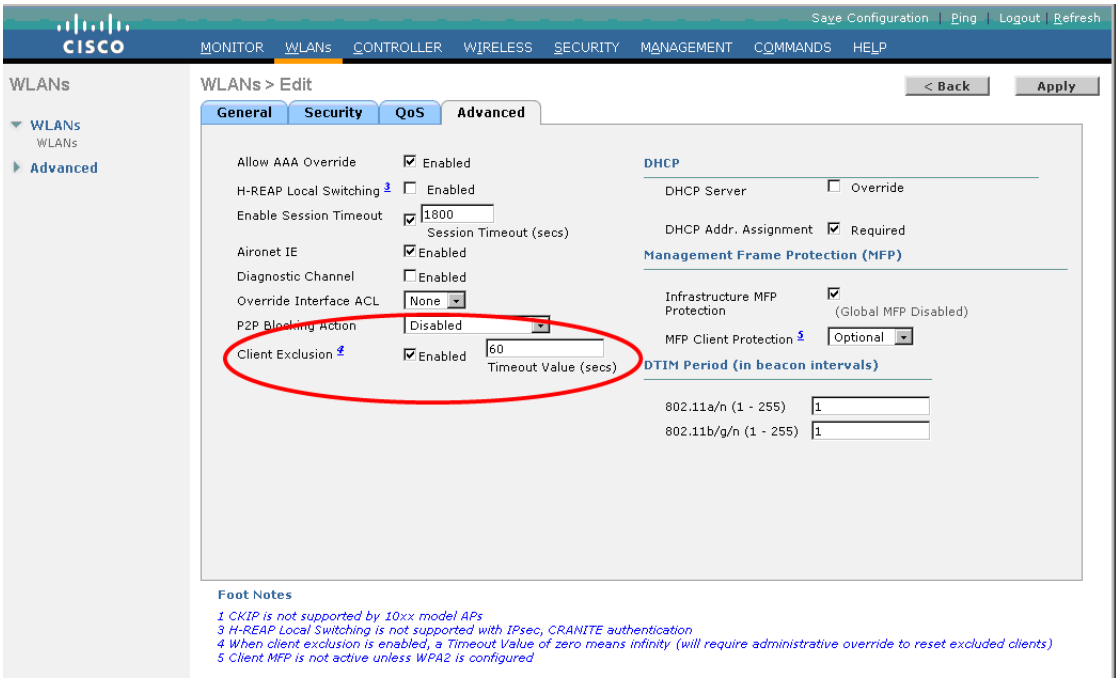
次の点に注意してください。

- クエリー間隔によって、WLC が Shun リスト要求により IPS をポーリングする頻度が決まります。
- デフォルトのクエリー間隔は、60 秒です。
- クエリー間隔は、Cisco IPS でアクティブなホスト ブロックがアクティブになってから WLC で適用されるまでの時間に影響します。また、クエリー間隔とクライアント除外タイムアウトは、Cisco IPS でアクティブなホスト ブロックが取り消されてから WLC でブロックが解除されるまでの時間に影響します。
- IPS とのコラボレートには、モビリティ グループ内の 1 つの WLC だけが必要です。モビリティ グループ内のすべての WLC に、アクティブなホスト ブロック情報が自動的に渡されます。冗長性を確保するために、モビリティ グループ内の複数の WLC が 1 つの Cisco IPS とコラボレートするように設定できます。
- 1 つの WLC が複数の IPS デバイスとコラボレートできます。
- IPS 展開は、多くの場合、その規模とハイ アベイラビリティを実現するため、およびさまざまな論理的ロケーションと地理的ロケーションに対応するために、複数のセンサーを装備します。このネットワーク全体の脅威検出 / 軽減機能を十分に活用するために、1 つの WLC が複数の IPS デバイスとコラボレートできます。

ステップ 5WLAN クライアント ブロッキングの適用をサポートする必要がある WLAN ごとに、WLAN プロファイルでクライアント除外を有効にする必要があります。

WLC で、**WLANs** に進み、WLAN プロファイルにアクセスします。クライアント ブロッキングを有効にする特定の WLAN プロファイルを選択し、**Advanced** タブに進みます。**Client Exclusion** の隣で、**Enabled** チェックボックスがオンであることを確認します（図 8-10 を参照）。

図 8-10　WLAN クライアント ブロッキングの適用をサポートする WLAN ごとにクライアント除外を有効にする



次の点に注意してください。

- WLAN クライアント ブロッキングをサポートする必要がある WLAN プロファイルごとに、クライアント除外を有効にする必要があります。
- 特定の WLAN プロファイルでクライアント除外が有効でない場合、WLC は IPS からアクティブなホスト ブロック情報を受信しますが、その WLAN プロファイルではホスト ブロックが適用されません。
- WLAN プロファイルでクライアント除外が有効である場合は、タイムアウト値を定義する必要があります。このタイムアウトは、その WLAN プロファイルに固有のものです。WLC は、その WLAN プロファイルで適用されるすべてのクライアント除外に対して、このタイムアウトを適用します。
- デフォルトのクライアント除外タイムアウトは 60 秒です。
- クライアント除外が作成されると、クライアント除外タイムアウトによって、WLC でクライアントの MAC アドレスに基づきクライアントがブロックされる期間が決まります。
- Cisco IPS ホスト ブロックの結果として作成されたクライアント除外は、クライアント除外タイムアウトになるまでアクティブなままです。クライアント除外は、Cisco IPS ホスト ブロックの取り消しでは削除されません。

Cisco WLC と Cisco IPS のコラボレーション モニタリングの有効化

ネットワーク アクティビティのモニタリングは、効果的なネットワーク管理にとって重要です。この章では、次の機能を使用して、Cisco WLC と Cisco IPS のコラボレーションのモニタリングを有効にする方法について詳しく説明します。

- WLC ローカル ロギング
- SNMP トラップ
- WCS
- CS-MARS

WLAN クライアント ブロック イベントの WLC ローカル ロギングの有効化

WLC は、WLC GUI または WLC CLI でアクセスできるローカル メッセージ ログを提供します。このメッセージ ログに WLAN クライアント ブロック イベントをロギングするには、WLC のログ レベルを最小重大度 1（**Alerts**）に設定する必要があります。その場合、WLC は、IPS ホスト ブロックの結果として WLAN クライアントをブロックすると、ローカル メッセージ ログ エントリを生成します。このエントリには、IPS から受信した IP アドレス、およびアソシエートされたクライアントの MAC アドレスが含まれます。

クライアント除外によって WLC が拒否したクライアント アソシエーションを表示する必要がある場合は、WLC のログ レベルを最小重大度 4（**Warnings**）に設定する必要があります。ブロックされたクライアントが、その後、その MAC アドレスのアクティブなクライアント除外が存在する間にアソシエートを試みた場合、WLAN クライアント ブロック イベントでこのエントリが生成されます。

表 8-2 に、これらの各ロギング オプションで必要となるロギング レベルの概要を示します。

表 8-2　必要なロギング レベル

イベント	最小重大度	
IPS ホスト ブロック適用の結果としての WLC クライアント回避イベント	Alerts	重大度 1
アクティブなクライアント除外によって拒否されたクライアント アソシエーション要求	Warnings	重大度 4

警告　ログの重大度を「Warnings」にすると、非常に多くのイベントが生成されます。このログ レベルは、慎重に使用する必要があります。

Buffered Log Level と Console Log Level のデフォルトは、**Critical**（重大度 2）です。このデフォルト設定では、Cisco IPS ホスト ブロックの結果として適用された WLAN クライアント ブロック イベントがロギングされます。

ログ レベルを定義するパラメータは、次のとおりです。

- *Buffered Log Level*

  WLC GUI メッセージ ログのログ レベルを定義します。

- *Console Log Level*

WLC CLI ログのログ レベルを定義します。

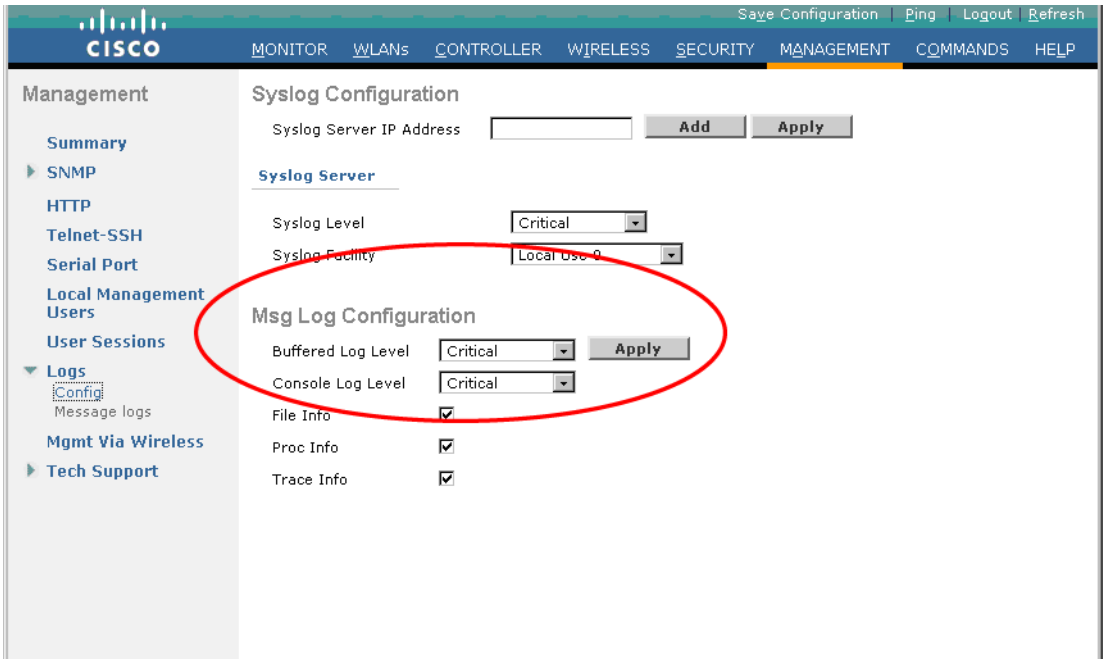
以前のリリースの WLC では、パラメータ *Message Log Level* により GUI と CLI の両方のログ レベルが定義されます。**Significant System events** という設定で、WLAN クライアント ブロック イベントのロギングが有効になります。

次に、WLAN クライアント ブロック イベントを表示できるようにするためのログ レベルの設定手順を示します。

ステップ 1 *Buffered Log Level* と *Console Log Level* のパラメータが重大度 1 に設定されていることを確認します。この例では、ログ レベルを **Critical** に設定します。これは、重大度 2 の設定です。

WLC で、**Management -> Logs -> Config** の順に進みます。Buffered Log Level と Console Log Level の両方のパラメータで、ログ レベルを **Critical** に設定します。**Apply** をクリックして、すべての変更を適用します（図 8-11 を参照）。

図 8-11　WLAN クライアント ブロック イベントを含めるための WLC ローカル ロギング レベル



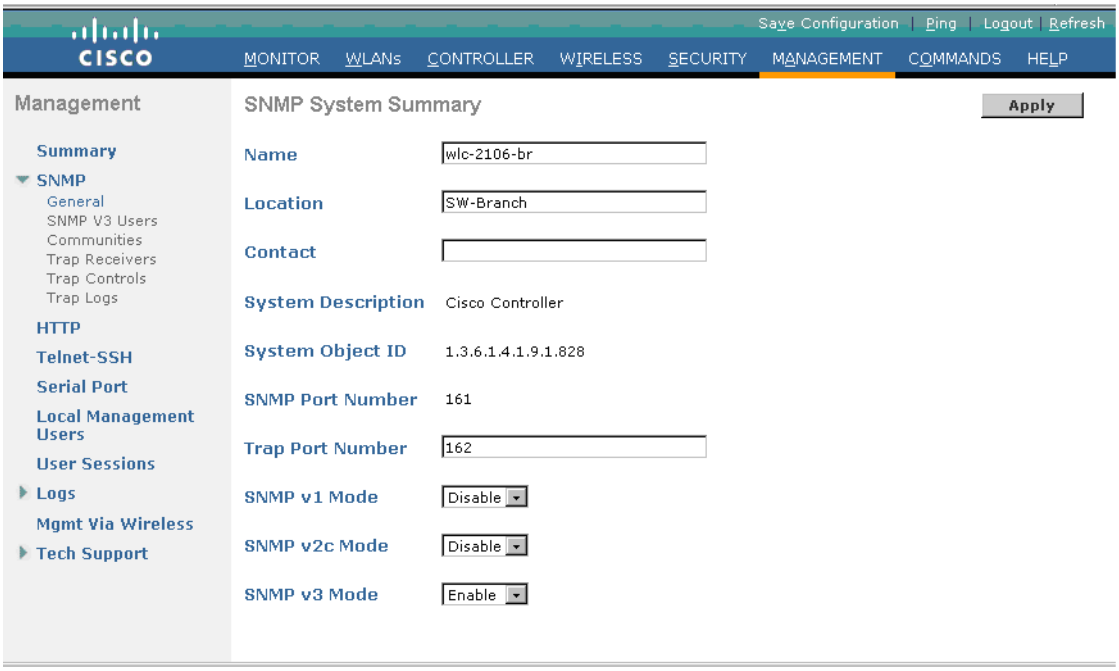
WLAN クライアント ブロック イベントの SNMP トラップの有効化

IPS ホスト ブロックの適用は、クライアント除外の自動作成を通じて WLC によって実行されます。したがって、このイベントの発生時に SNMP トラップを生成するには、WLC でクライアント除外の SNMP トラップを有効にする必要があります。

ステップ 1 WLC の一般的なパラメータが正しく定義されていることを確認します。

WLC で、**Management -> SNMP -> General** の順に進みます。少なくともシステム名と正しいトラップ ポート番号が定義されていることを確認し、不要な SNMP バージョンを無効にします（図 8-12 を参照）。

図 8-12　WLC で一般的な SNMP パラメータを確認する



次の点に注意してください。

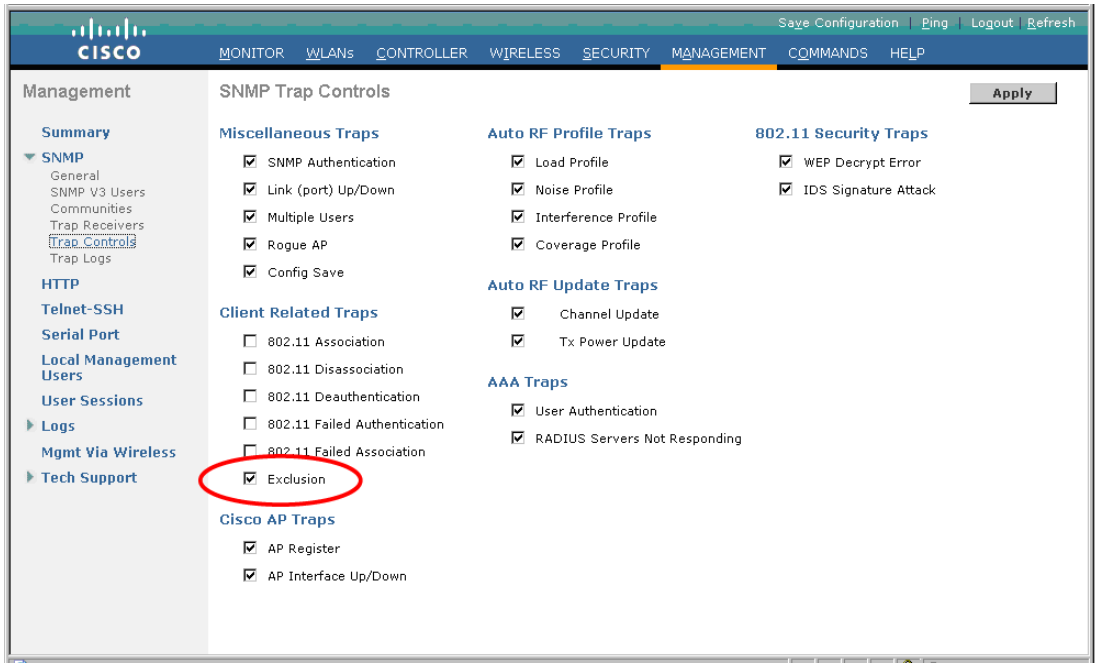
- SNMP v1 と SNMP v2c は、コミュニティ ストリングを含め、すべてのデータをクリア テキストで伝送するため、スニフィングに対して脆弱です。
- SNMP v1 または v2c は、不要な場合は無効にする必要があります。
- SNMP v3 が SNMP の最も安全な実装を提供するため、サポートされている場合は SNMP v3 をお勧めします。
- SNMP v1 または v2c が必要な場合は、デフォルトではない SNMP コミュニティ ストリングが使用されることを確認してください。
- デフォルトのパブリック コミュニティとプライベート コミュニティの定義を削除してください。
- SNMP v1 または v2c が必要な場合は、読み取り専用アクセスだけを許可する必要があります。
- SNMP v1 または v2c が必要な場合は、ACL を使用して、許可された管理プラットフォームだけにアクセスを制限する必要があります。

SNMP アクセスをセキュリティで保護する方法の詳細については、P.8-52 の「参考資料」の「ネットワーク セキュリティ ベースライン」を参照してください。

ステップ 2クライアント除外の WLC SNMP トラップを有効にします。

WLC で、**Management -> SNMP -> Trap Controls** の順に進みます。**Client Related Traps** で、**Exclusion** チェックボックスがオンであることを確認します（図 8-13 を参照）。

図 8-13　　WLC でクライアント除外の SNMP トラップを有効にする



WLC をまたがる WLAN イベントの WCS でのモニタリングの有効化

WCS は、すべての WLC のイベントの統合ビューを提供します。このビューは、Unified Wireless Network 全体にわたるアクティビティの可視性を実現するために非常に重要です。WCS は、各 WLC から送信された SNMP トラップを利用して、このような統合ビューを生成します。したがって、WCS に SNMP トラップを送信するよう各 WLC を設定する必要があります。

すべての WLC のイベントに対する WCS のモニタリングを有効にするには、次の主な要素が必要です。

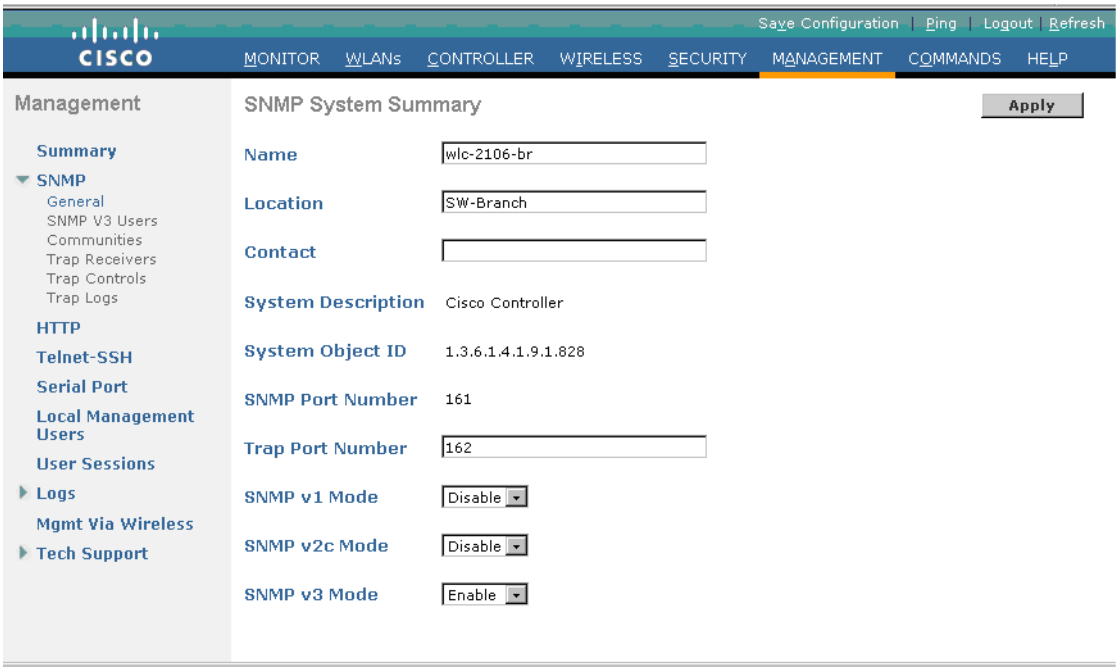
- 各 WLC 上：
  - 一般的な SNMP パラメータを確認する。
  - SNMP トラップ制御を確認する。
  - WCS を SNMP v3 ユーザとして定義する。
  - WCS を SNMP トラップ レシーバとして定義する。
- WCS 上：
  - 各 WLC とその SNMP パラメータを定義する。

次に、これらの各要素を設定する方法の詳細を示します。WCS は SNMP v3 をサポートしているため、SNMP v3 の設定を示します。SNMP v1 と v2c もサポートされていますが、SNMP v3 が SNMP の最も安全な実装であるため、サポートされている場合は SNMP v3 をお勧めします。

ステップ 1各 WLC で、一般的な SNMP パラメータが正しく定義されていることを確認します。

WLC で、**Management -> SNMP -> General** の順に進みます（図 8-14 を参照）。詳細については、P.8-17 の「WLAN クライアント ブロック イベントの SNMP トラップの有効化」を参照してください。

図 8-14　　WLC で一般的な SNMP パラメータを確認する

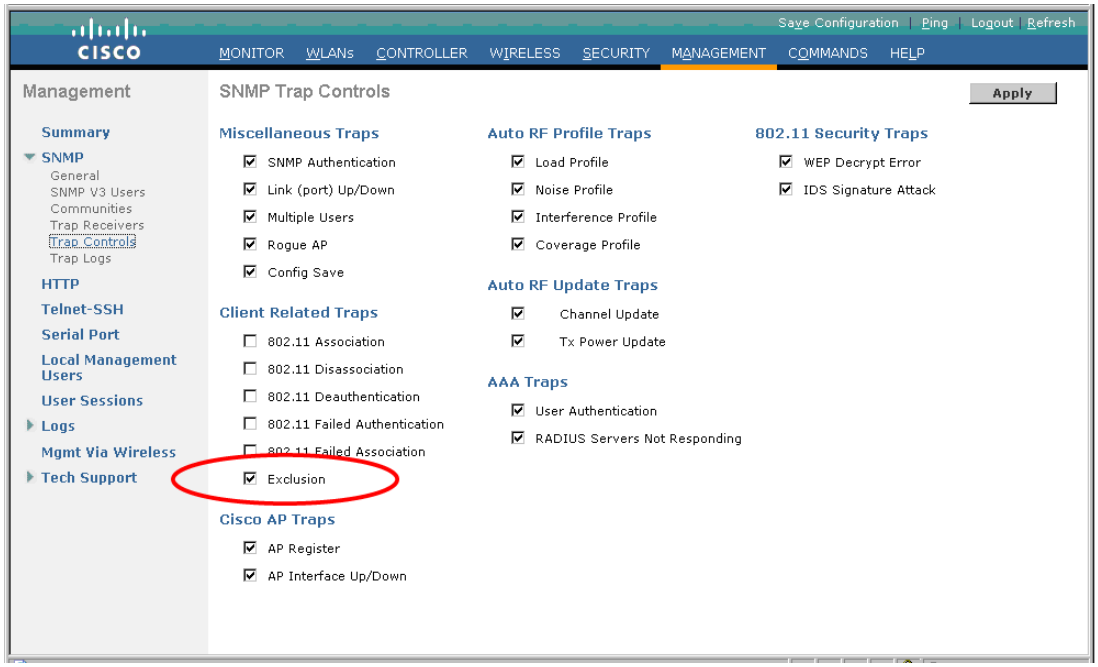


この例では、WCS の SNMP v3 サポートを利用します。したがって、SNMP v3 モードが有効である必要があります。

ステップ 2各 WLC で、必要なすべての SNMP トラップ制御が有効であることを確認します。

WLC で、**Management -> SNMP -> Trap Controls** の順に進みます（図 8-15 を参照）。WLAN クライアントのホスト ブロック イベントで SNMP トラップが生成されるようにするために、除外のトラップが有効であることを確認します。詳細については、P.8-17 の「WLAN クライアント ブロック イベントの SNMP トラップの有効化」を参照してください。

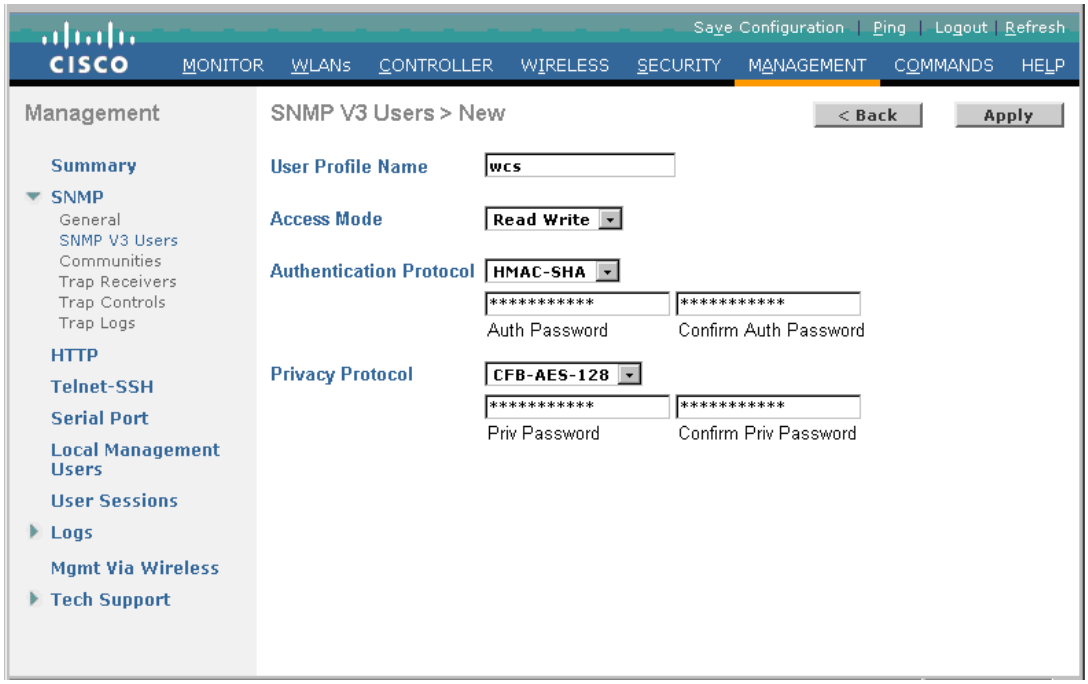
図 8-15　　WLC で SNMP トラップ制御を確認する



ステップ 3各 WLC で、WCS を SNMP v3 ユーザとして定義します。

WLC で、**Management -> SNMP -> SNMP V3 Users** の順に進みます。**New** を選択し、WCS のユーザ プロファイル名を定義します。WCS で WLC の設定を変更できるようにする場合は、Access Mode ドロップダウン ボックスを **Read Write** に設定します。認証パスワードとプライバシー パスワードを定義し、**Apply** をクリックします（図 8-16 を参照）。

図 8-16　　WLC で WCS を SNMPv3 ユーザとして定義する



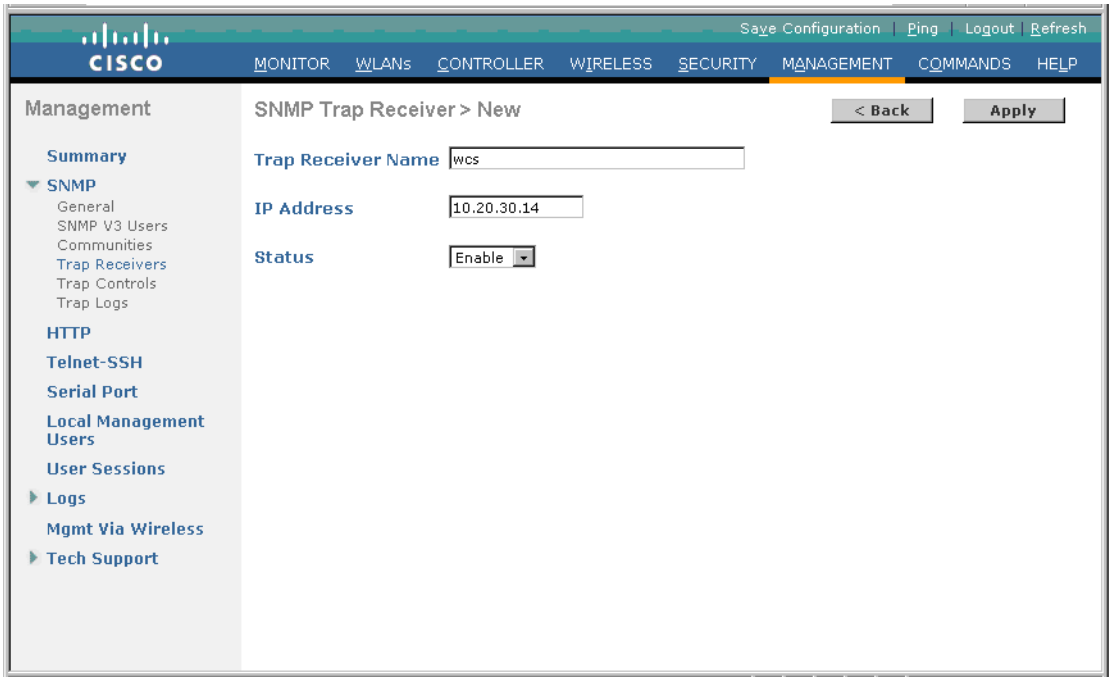
次の点に注意してください。

- WCS で WLC を設定する必要がない場合は、アクセス モードを読み取り専用に設定する必要があります。
- デフォルトの認証プロトコルとプライバシー プロトコルは、最も安全な、推奨される設定です。
- 認証パスワードとプライバシー パスワードの長さは、12 文字以上にする必要があります。

ステップ 4各 WLC で、WCS を SNMP トラップ レシーバとして定義します。

WLC で、**Management -> SNMP -> Trap Receivers** の順に進みます。**New** を選択し、WCS の名前と IP アドレスを定義します。Status ドロップダウン ボックスを **Enable** に設定し、**Apply** をクリックします（図 8-17 を参照）。

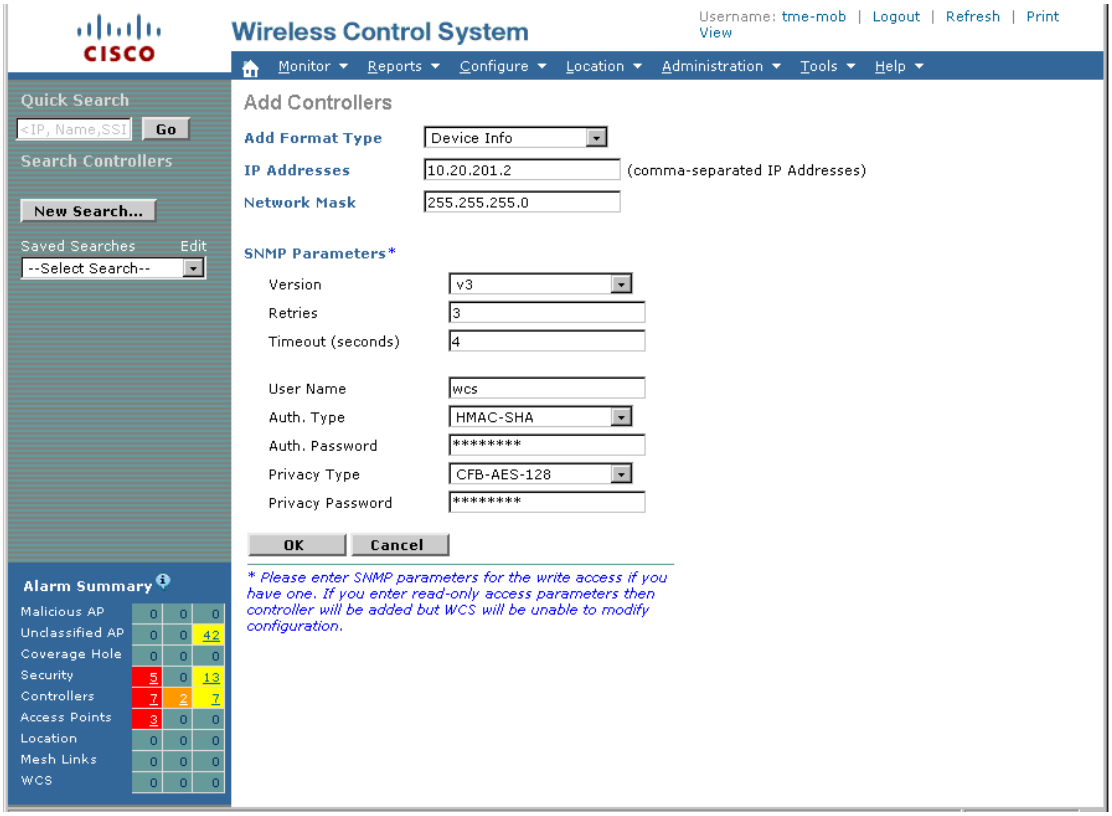
図 8-17　　各 WLC で WCS を SNMP トラップ レシーバとして定義する



ステップ 5WCS で、各 WLC とその SNMP パラメータを定義します。

WCS で、**Configure -> Controllers** の順に進みます。コントローラを追加するか（コントローラが存在しない場合）、またはすでに定義されているコントローラをクリックして SNMP パラメータを変更します。図 8-18 を参照してください。

図 8-18　　WCS で各 WLC とその SNMP パラメータを定義する



OK をクリックします。WCS が、WLC を検出してそのプロパティを取得しようとします。

次の点に注意してください。

- SNMP パラメータは、WCS の SNMP v3 ユーザ プロファイルとして WLC に定義されているものと一致する必要があります。

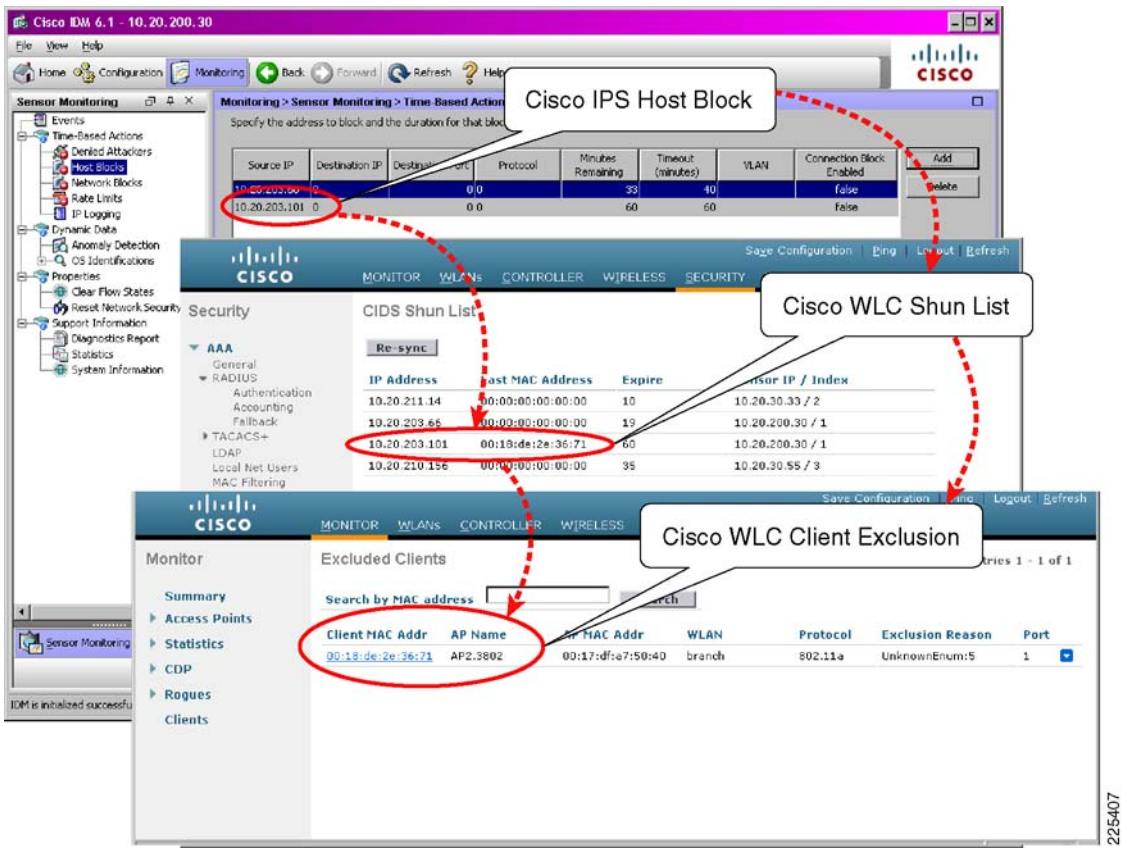
WLAN イベントに対する CS-MARS のモニタリングの有効化

CS-MARS は、脅威の効果的な検出と軽減にとって重要な、ネットワークをまたがる異常を検出し関連性を特定します。CS-MARS を Cisco Unified Wireless Network と統合することにより、この可視性を拡張して WLAN を含めることができます。詳細については、第 9 章「Cisco Unified Wireless 用の CS-MARS 統合」を参照してください。

Cisco IPS ホスト ブロックのアクティブ化と WLC による適用

この項では、WLAN クライアント ブロックが、Cisco IPS で手動ホスト ブロックによってアクティブになり、WLC でクライアント除外によって自動的に適用される様子を示します。図 8-19 に、関連する主な手順を示します。

図 8-19　　Cisco IPS ホスト ブロックのアクティブ化と WLC による適用

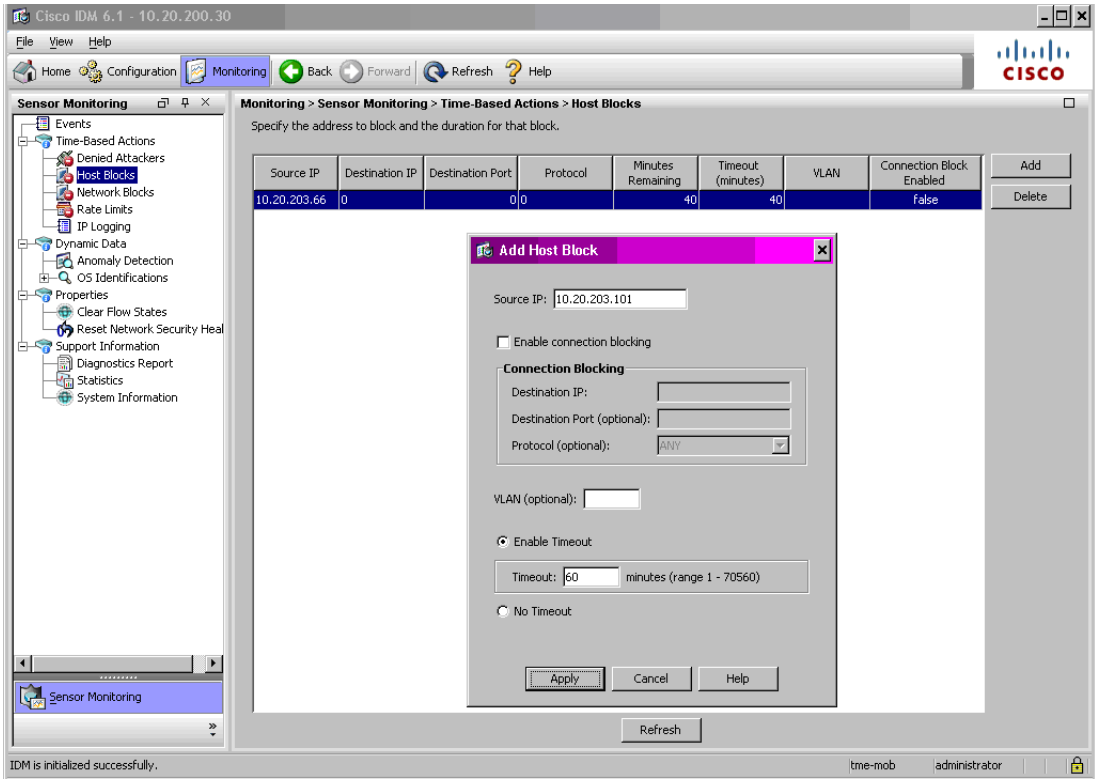


WLAN クライアント ブロックを試行する前に、WLC が Cisco IPS を正常にポーリングし、Shun リスト要求に対する応答を受信できることを確認してください。詳細については、P.8-30 の「Cisco WLC と Cisco IPS の通信ステータスの確認」を参照してください。

ステップ 1IPS で、ホスト ブロックを追加します。

IDM で、**Monitoring -> Time-Based Actions -> Host Blocks** の順に進みます。ブロックする WLAN クライアントの送信元 IP アドレスで新しいホスト ブロックを追加し、タイムアウトを定義します。**Apply** をクリックします（図 8-20 を参照）。

図 8-20　Cisco IPS でのクライアント ブロックの開始

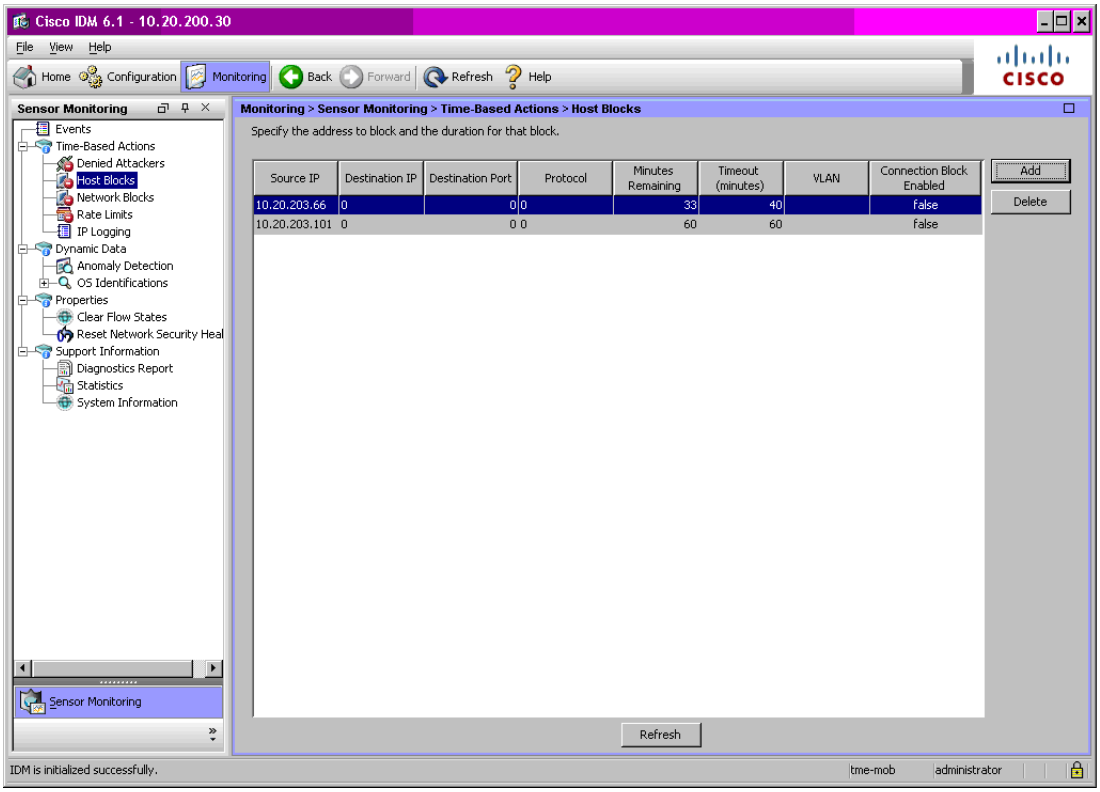


次の点に注意してください。

- アクティブなホスト ブロックのタイムアウトは、デフォルトで 60 分です。

その後、ブロック対象クライアントがその特定の IPS のホスト ブロック リストに表示されます（図 8-21 を参照）。

図 8-21　　Cisco IPS 上のホスト ブロック リストの例

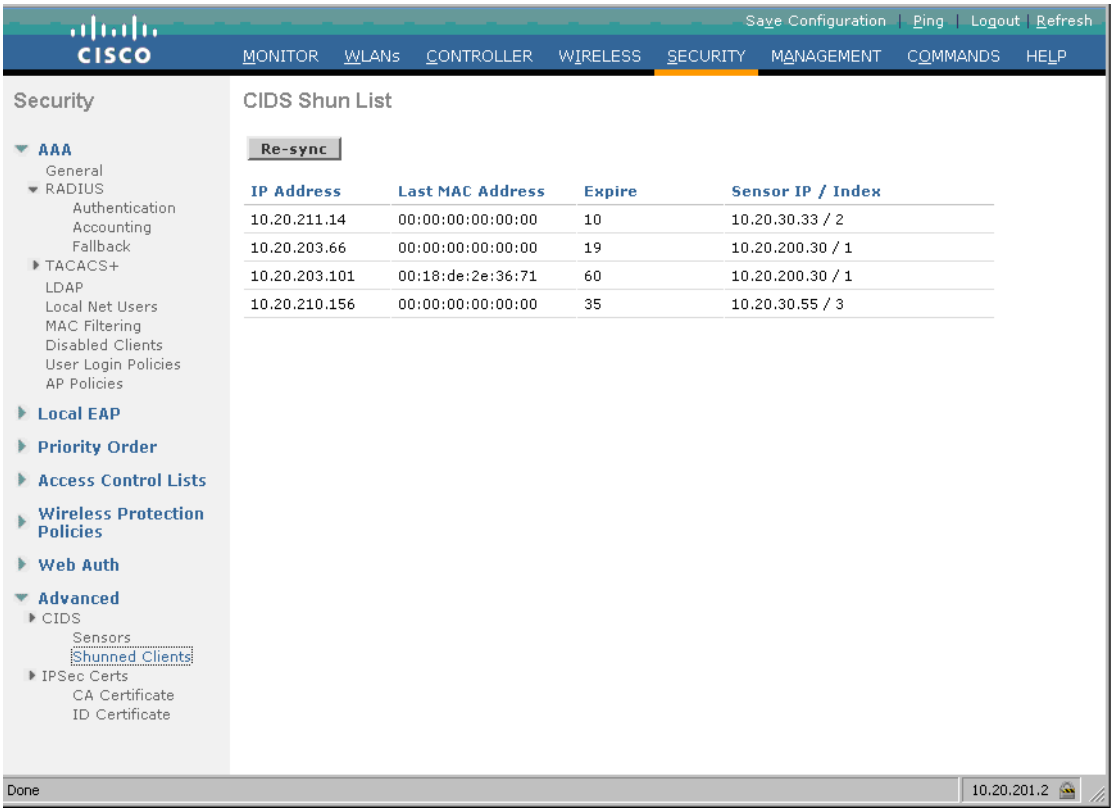


次の点に注意してください。

- ホスト ブロック リストは、WLC によって要求されるクライアント Shun リストとなります。
- 有線クライアントであるか WLAN クライアントであるかに関係なく、すべてのアクティブなホスト ブロックが WLC に渡されます。

ステップ 2WLC が、IPS に対する次回のポーリングで、アップデートされたアクティブなホスト ブロック リストを受信し、Shun リストをアップデートします。これは、WLC の **Security -> CIDS -> Shunned Clients** に反映されます（図 8-22 を参照）。

図 8-22　WLC 上の CIDS Shun リストの例



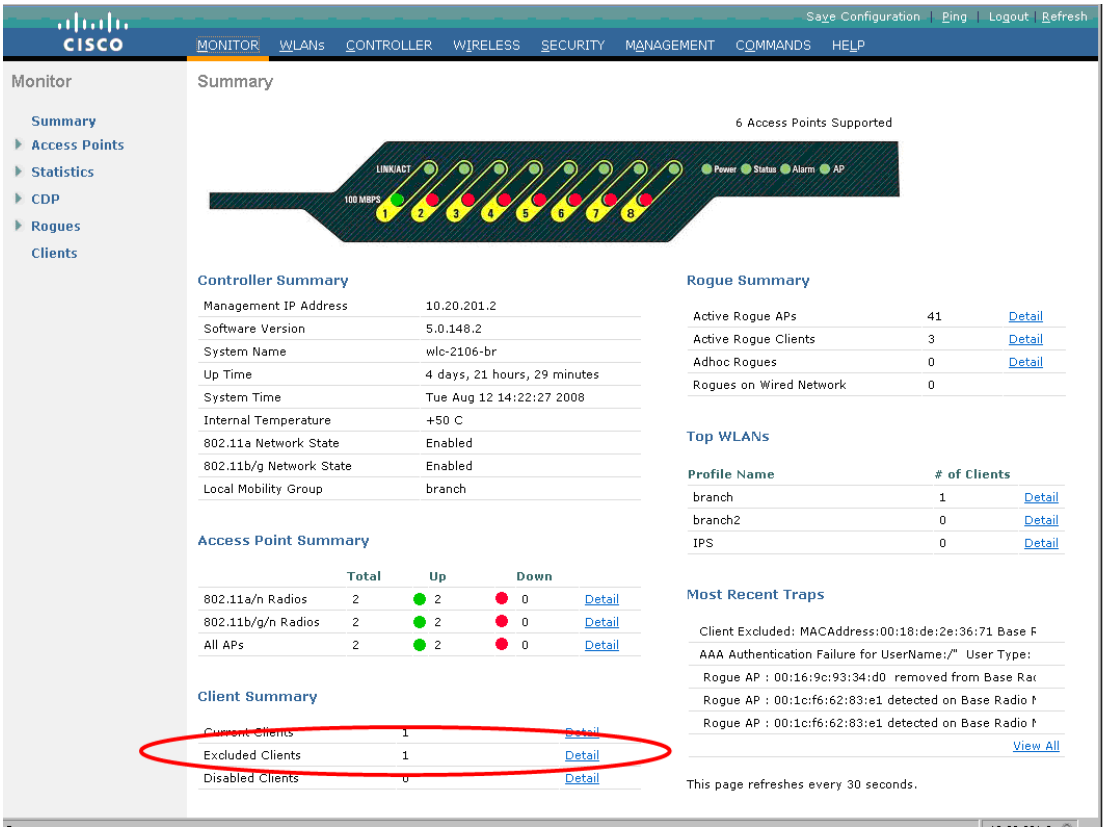
次の点に注意してください。

- CIDS Shun リストには、WLC が通信するすべての Cisco IPS から受信したすべてのホスト ブロックが含まれています。
- Expire カラムには、ホスト ブロックの有効期限までに残されている時間が分単位で表示されます。この有効期限は、Cisco IPS に設定されているタイムアウトによって定義されます。
- WLC がモビリティ グループに含まれている場合、Shun リストはモビリティ グループ内のすべての WLC に自動的に渡されます。

ステップ 3ホスト ブロックの送信元 IP アドレスに一致する WLAN クライアントが現在 WLC にアソシエートされている場合、WLC は自動的にそのクライアントのクライアント除外を作成し、そのクライアントを切断します。

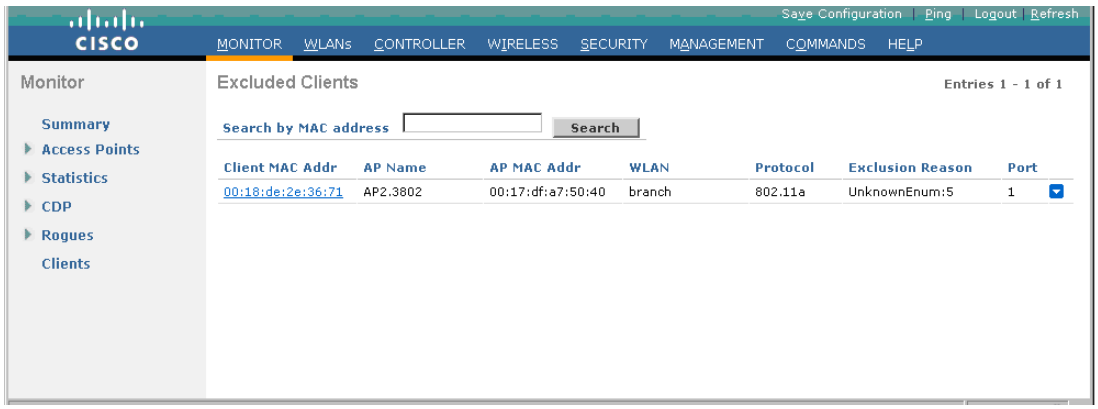
WLC で現在有効なすべてのクライアント除外を表示するには、**Monitor -> Summary** の順に進み、Client Summary セクションで **Excluded Clients** の隣にある **Detail** をクリックします（図 8-23 を参照）。

図 8-23　除外されたクライアントの Detail リンクを含む WLC の Monitor Summary 画面



その後、Excluded Clients リストが表示されます（図 8-24 を参照）。

図 8-24　IPS ホスト ブロックを示す Excluded Clients リストの例



次の点に注意してください。

- IPS ホスト ブロックの結果として作成されたクライアント除外は、除外理由「UnknownEnum:5」で表示されます。
- 除外された WLAN クライアントは、WLC でクライアント除外が有効である間、このサマリー画面に表示されます。

- クライアント除外は、その特定の WLAN プロファイルのクライアント除外タイムアウトに基づいて、有効期限が切れるまでアクティブなままです。
- クライアント除外は、Cisco IPS ホスト ブロックの取り消しでは削除されません。
- 除外されたクライアント エントリは、そのクライアントが WLC に接続されていたが切断されたことを示します。

Cisco WLC と Cisco IPS のコラボレーションのモニタリング

Cisco WLC と Cisco IPS の通信ステータスの確認

Cisco WLC と Cisco IPS の間の正常な通信は、次のどのインターフェイスでも確認できます。

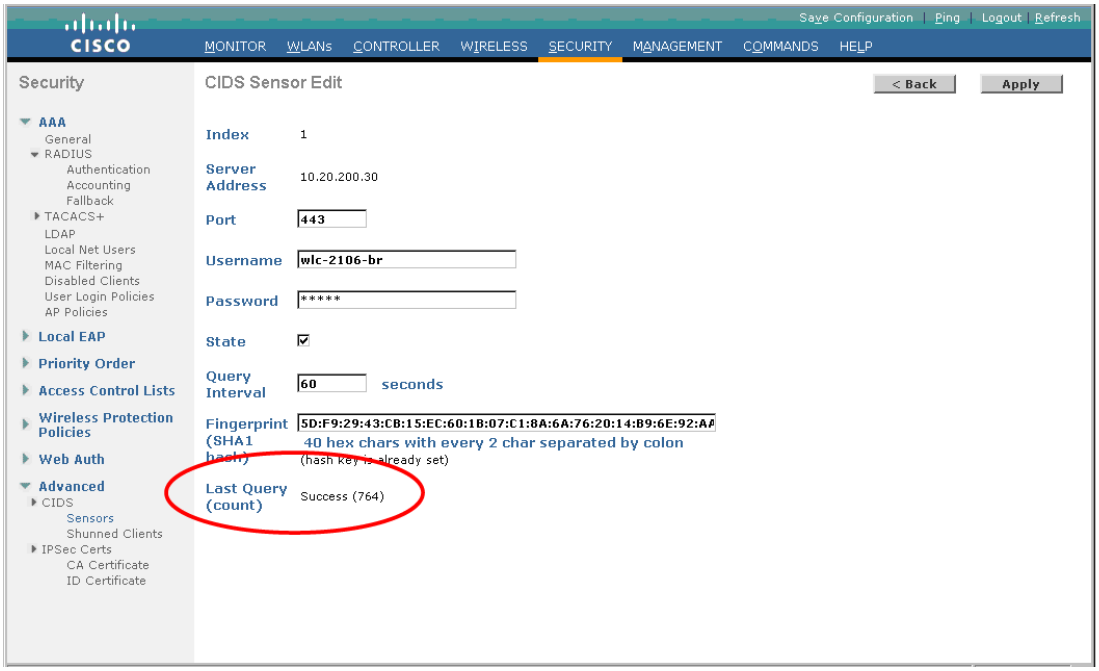
- WLC GUI
- WLC CLI
- IDM GUI
- IPS CLI

Cisco WLC と Cisco IPS の間の正常な通信が確認された場合、運用スタッフは、このコラボレーションで有効になった自動脅威軽減ツールを使用できます。

WLC GUI

WLC GUI では、**Security** -> **Advanced** -> **CIDS** -> **Sensors** の順に進み、特定のセンサーのインデックス番号をクリックすることで、特定の Cisco IPS との通信の現在のステータスを確認できます。WLC と IPS が正常に通信できる場合は、**Last Query** フィールドに「Success」と表示されます（図 8-25 を参照）。

図 8-25　WLC GUI での WLC と Cisco IPS 間の通信ステータスの確認



WLC CLI

WLC CLI では、次の手順を実行して Cisco IPS との通信を確認できます。

ステップ 1 Cisco IPS とコラボレートしている WLC の CLI にログインします。

ステップ 2次のように入力して、WLC-IPS 通信のデバッグを有効にします。

```
debug wps cids enable
```

イベントが発生するとすぐに、デバッグが自動的に画面に表示されます。

次に、WLC が Shun リスト要求により Cisco IPS を正常にポーリングした場合の例を示します。

```
Tue Aug 12 14:21:43 2008: cidsProcessSdeeQuery: ip=10.20.200.30,port=443 state=1
interval=60
Tue Aug 12 14:21:43 2008: cidsQuerySend:
https://10.20.200.30:443/cgi-bin/transaction-server?command=getShunEntryList
Tue Aug 12 14:21:43 2008: curlHandle is bbd422c
Tue Aug 12 14:21:43 2008: Perform on curlHandle bbd422c ...
Tue Aug 12 14:21:43 2008: Response code is 0
Tue Aug 12 14:21:43 2008: xmlDoc buffer freed
Tue Aug 12 14:21:43 2008: Parser cleaned
```

ステップ 3通信を確認した後、デバッグを無効にします。

```
debug wps cids disable
```

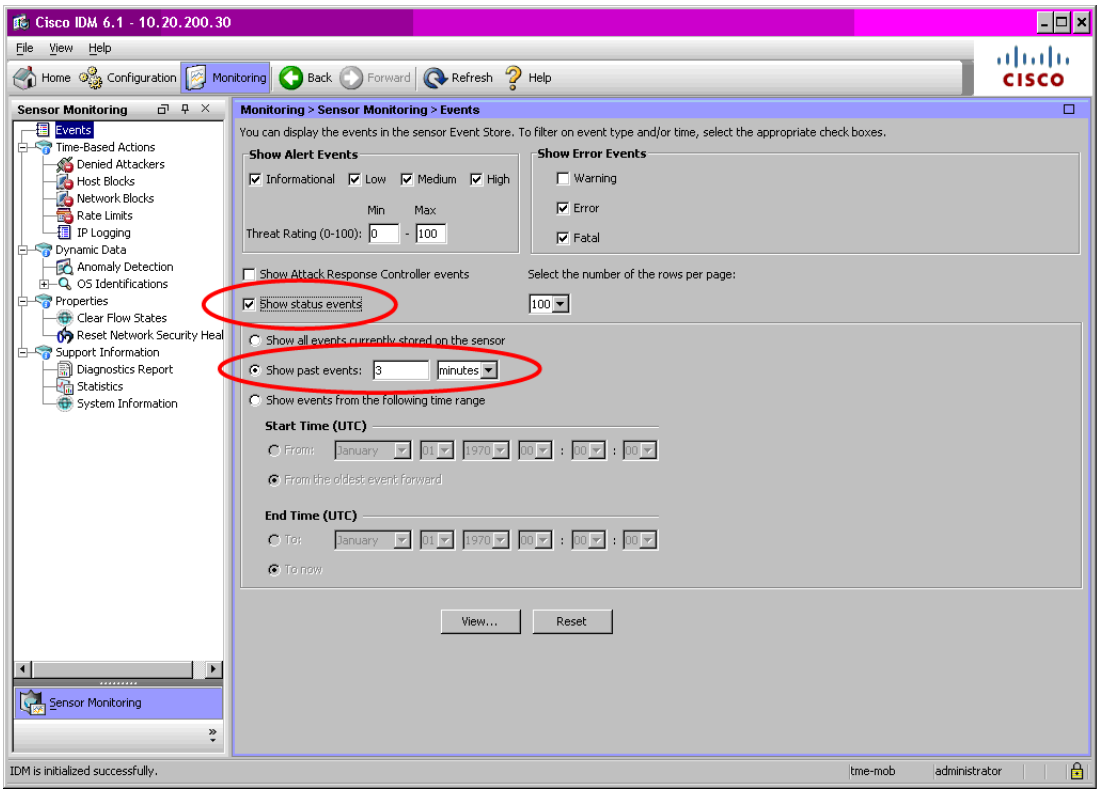
IDM GUI

IDM ツールを使用して、Cisco IPS が Cisco WLC との通信中に生成したイベントを表示できます。

IDM で、**Monitoring -> Events** の順に進みます。

Show status events を有効にし、**Show past events** で短い期間を定義して（図 8-26 では 3 分と表示）、**View** を選択します。

図 8-26　IDM での Cisco WLC と Cisco IPS の通信イベントの表示



IDM Event Viewer 画面では、次に説明するように、IPS ソフトウェア リリースによって、正常な通信の結果として生成される関連イベントが異なります。

- IPS Release 6.1 より前

  2 つの関連エントリが生成されます。1 つはイベント **User logged into HTTP server** に対するエントリで、もう 1 つはイベント **getShunEntryList succeeded** に対するエントリです。

- IPS Release 6.1 以降

  デフォルトでは、イベント **User logged into HTTP server** に対する 1 つのエントリだけが生成されます。**getShunEntryList** イベントを表示して、Shun リスト要求のステータスを確認するには、IPS CLI で制御トランザクションのロギングを有効にする必要があります。詳細については、P.8-34 の「IPS CLI」を参照してください。

どの WLC が IPS にログインしたか、Shun リスト要求が正常に処理されたかどうかなど、詳細を表示するには、イベントをダブルクリックします。図 8-27 および図 8-28 を参照してください。

図 8-27　　IDM での Cisco IPS に対する WLC ログイン イベント

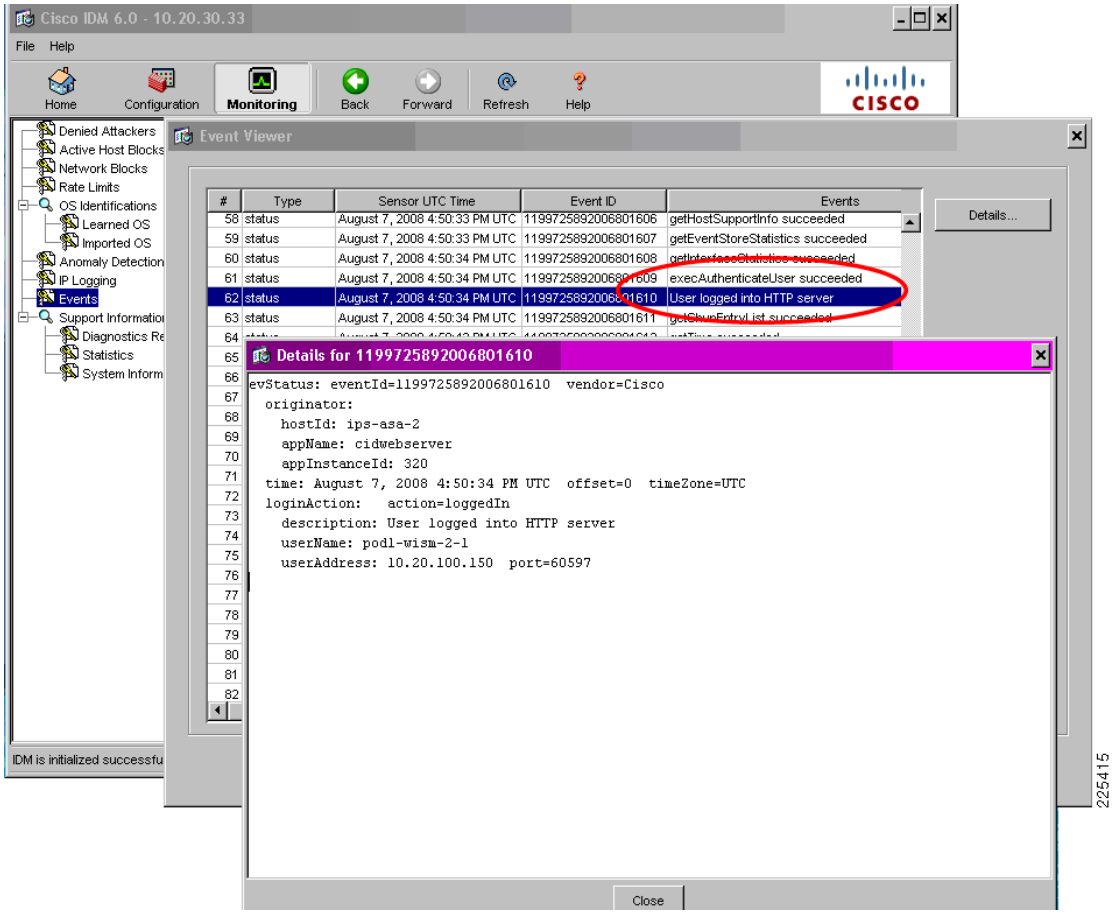
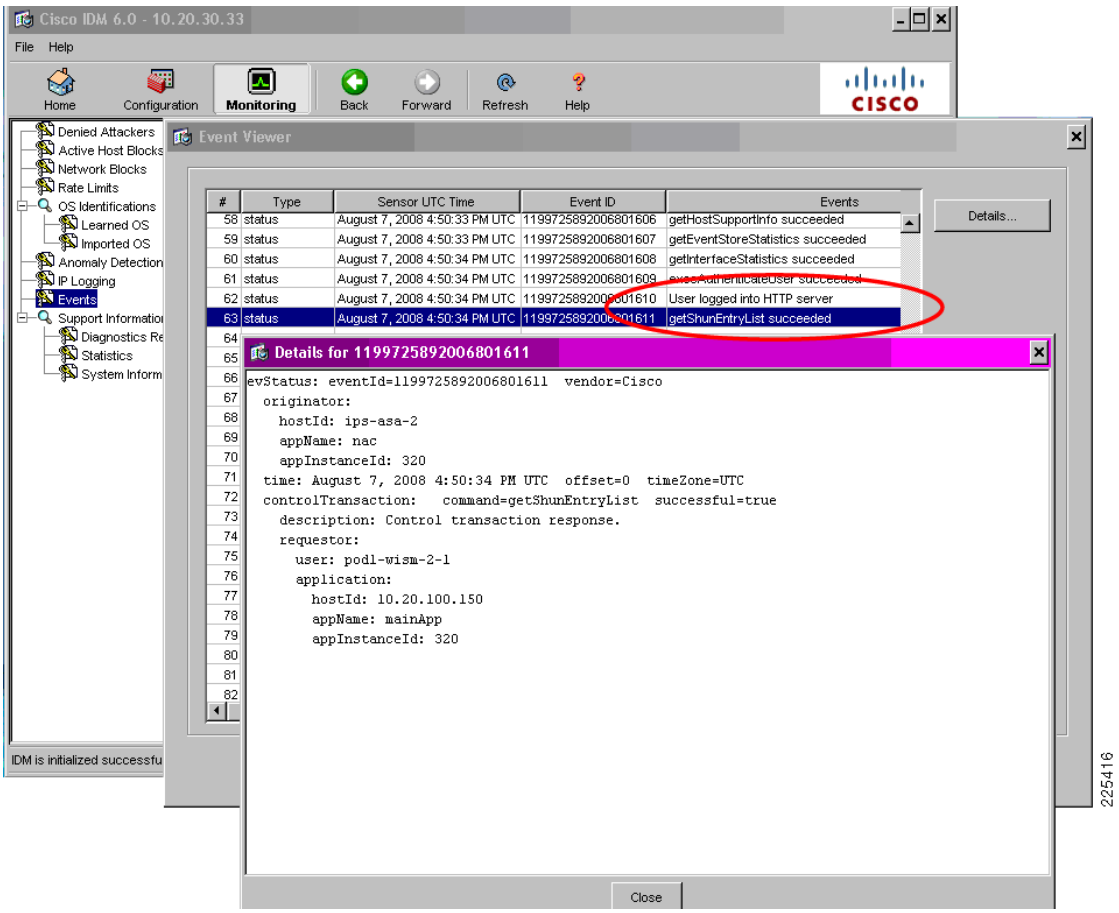


図 8-28　　IDM での WLC による Shun リスト正常取得イベント



IPS CLI

IPS CLI では、次の手順を実行して特定の Cisco WLC との通信を確認できます。

ステップ 1 Cisco WLC とコラボレートしている IPS の CLI にログインします。

ステップ 2次のように入力して、その WLC の最近のイベントを確認します。

```
ips-3845-2# show events past 0:03 | include 10.20.201.2
```

次に、WLC が IPS に正常にログインし、Shun リストを取得した場合の例を示します。

```
evStatus: eventId=1199725892006801610 vendor=Cisco
  originator:
    hostId: ips-asa-2
    appName: cidwebserver
    appInstanceId: 320
  time: 2008/08/07 16:50:34 2008/08/07 16:50:34 UTC
  loginAction: action=loggedIn
    description: User logged into HTTP server
    userName: pod1-wism-2-1
    userAddress: port=60597 10.20.100.150
```

```
evStatus: eventId=1199725892006801611 vendor=Cisco
  originator:
    hostId: ips-asa-2
    appName: nac
    appInstanceId: 320
  time: 2008/08/07 16:50:34 2008/08/07 16:50:34 UTC
  controlTransaction: command=getShunEntryList successful=true
    description: Control transaction response.
    requestor:
      user: pod1-wism-2-1
      application:
        hostId: 10.20.100.150
        appName: mainApp
        appInstanceId: 320
```

（注）　IPS Release 6.1 以降では、デフォルトで、イベント **getShunEntryList succeeded** が生成されません。このイベントおよび Shun リスト要求のステータスを表示するには、次のように入力して、IPS CLI で制御トランザクションのロギングを有効にする必要があります。

```
ips-3845-2(config)# service logger
ips-3845-2(config-log)# event-store
ips-3845-2(config-log-eve)# status-event-logging-categories controlTransaction enabled
true
```

正常な通信を確認した後、特に必要がない限り、次のように入力してこのレベルのロギングを無効にしてください。

```
ips-3845-2(config)# service logger
ips-3845-2(config-log)# event-store
ips-3845-2(config-log-eve)# status-event-logging-categories controlTransaction enabled
false
```

詳細については、IPS のマニュアルを参照してください（P.8-52 の「Cisco IPS」を参照）。

WLAN クライアント ブロック イベントの表示

WLAN クライアント ブロック イベントの WLC ローカル ロギング

WLC でローカル ロギングが最小重大度 1 に設定されている場合、WLC は IPS ホスト ブロックの結果として適用された WLAN クライアント ブロック イベントを記録します。ローカル ロギングを設定する方法の詳細については、P.8-16 の「WLAN クライアント ブロック イベントの WLC ローカル ロギングの有効化」を参照してください。

WLAN クライアント ブロックの WLC ローカル ログ形式

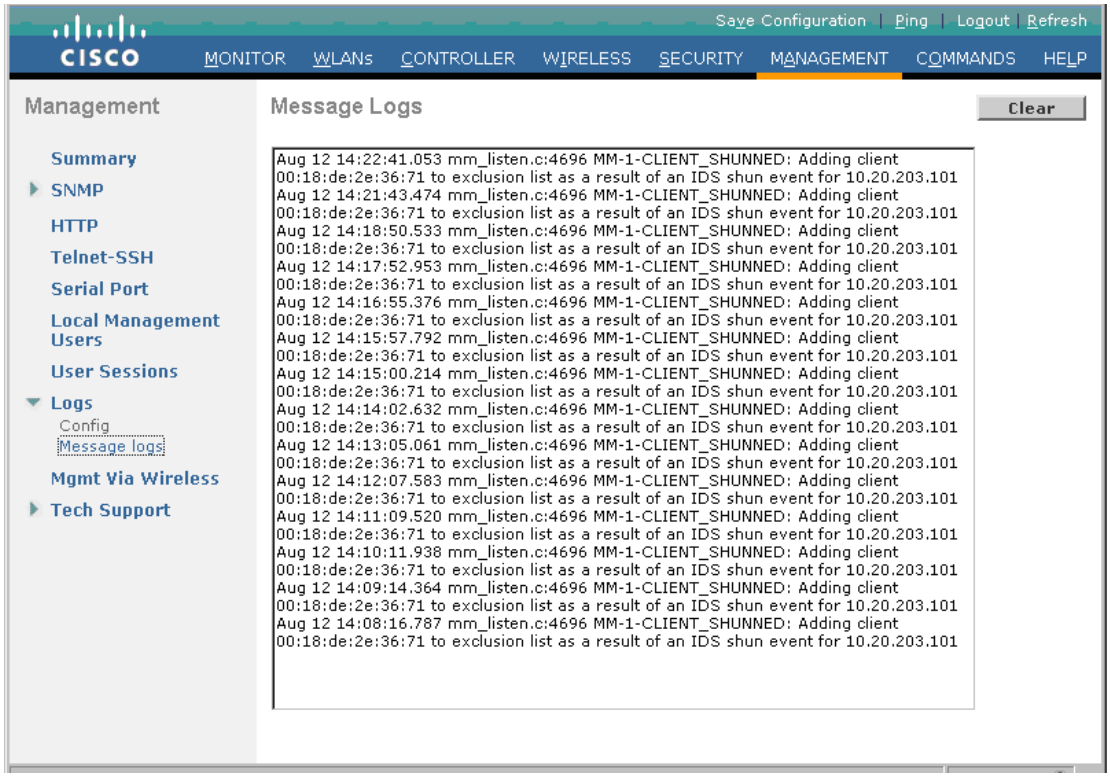
WLAN クライアント ブロックの適用時に WLC によって生成されるローカル メッセージ ログ エントリの一般的な形式は、次のとおりです。

```
mm_listen.c:4696 MM-1-CLIENT_SHUNNED: Adding client 00:18:de:2e:34:ca to exclusion list as
a result of an IDS shun event for 10.20.205.51
```

WLC ローカル ログ

WLC ローカル ログは、**Management -> Logs -> Message Logs** で表示できます（図 8-29 を参照）。

図 8-29　WLAN クライアント ブロック イベントを示す WLC ローカル ログ



次の点に注意してください。

- クライアント IP アドレスのアクティブな IPS ホスト ブロックが存在している間に、WLC クライアント除外が期限切れになると、WLC は、クライアントが WLAN にアソシエートするか、アソシエートを試みるたびに、新しいクライアント除外を自動的に作成します。
- したがって、IPS ホスト ブロックが有効である期間とクライアント除外タイムアウトによっては、複数のクライアント除外イベントが発生し、複数のメッセージ ログ エントリが生成されることがあります。

WLAN クライアント ブロック イベントの SNMP レポーティング

クライアント除外の SNMP トラップが有効である場合は、WLC が WLAN クライアント回避を実装して IPS ホスト ブロックを適用すると、SNMP トラップが生成されます。WLC、WCS、CS-MARS、および一般的な SNMP 管理ステーションが、このような SNMP トラップを使用できます。SNMP を有効にする方法の詳細については、P.8-17 の「WLAN クライアント ブロック イベントの SNMP トラップの有効化」を参照してください。

WLC GUI は、次の 2 つの場所で SNMP トラップを報告します。

- WLC のサマリー画面
- WLC の SNMP トラップ ログ

WLAN クライアント ブロックの SNMP トラップ形式

WLAN クライアント ブロックの適用時に WLC によって生成される SNMP トラップの一般的な形式は、次のとおりです。

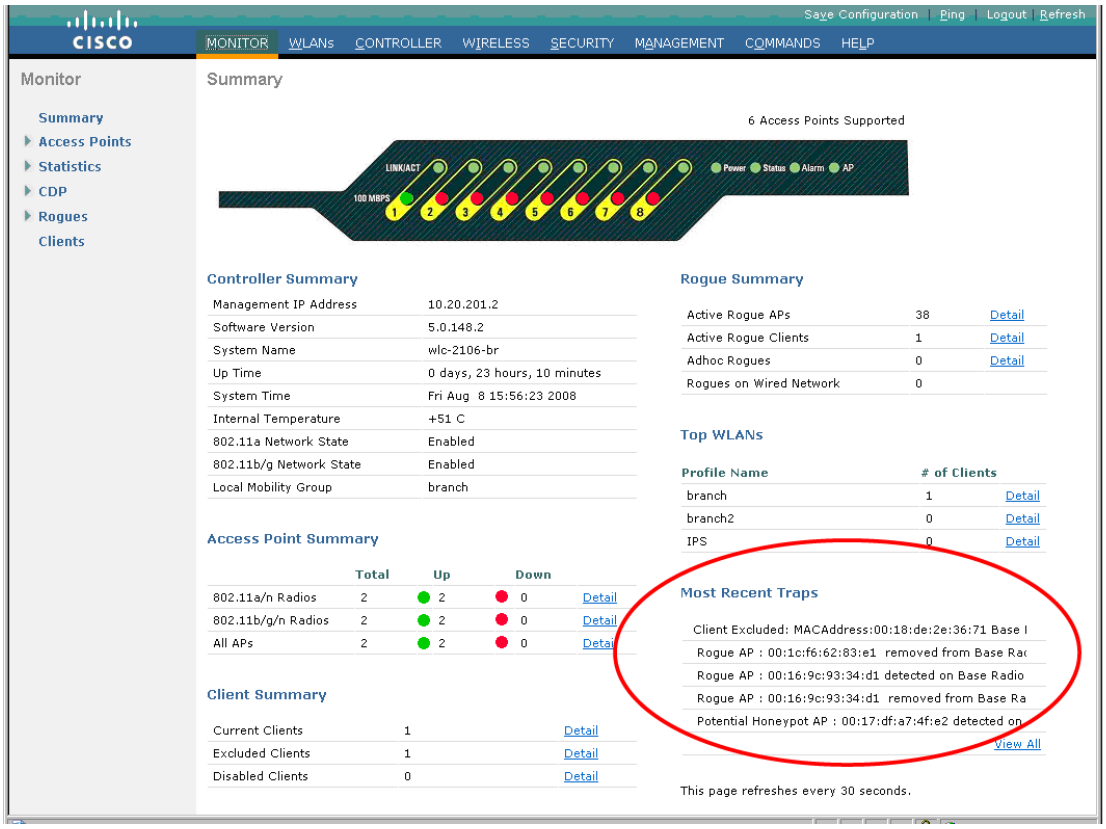
```
Client Excluded: MACAddress:00:18:de:2e:36:71 Base Radio MAC :00:17:df:a7:50:40 Slot: 1
Reason:Unknown ReasonCode: 5
```

この例では、**Reason:Unknown** および **ReasonCode: 5** が、IPS ホスト ブロックの結果として除外イベントが生成されたことを示しています。

WLC のサマリー画面

WLC のサマリー画面にある **Most Recent Traps** セクションに、WLAN クライアント ブロック イベントがクライアント除外イベントとして表示されます。WLC で、**Monitor -> Summary** の順に進みます（図 8-30 を参照）。

図 8-30　　WLAN クライアント ブロック イベントを示す WLC のサマリー画面



WLC の SNMP トラップ ログ

WLC の SNMP トラップ ログには、WLC によって生成された SNMP トラップがすべて含まれています。WLAN クライアント ブロック イベントで生成された SNMP トラップは、クライアント除外イベントとしてログに表示されます。WLC で SNMP トラップ ログを表示するには、**Management -> SNMP -> Trap Logs** の順に進みます（図 8-31 を参照）。

図 8-31　WLAN クライアント ブロックの結果として生成された WLAN クライアント除外トラップ

次の点に注意してください。

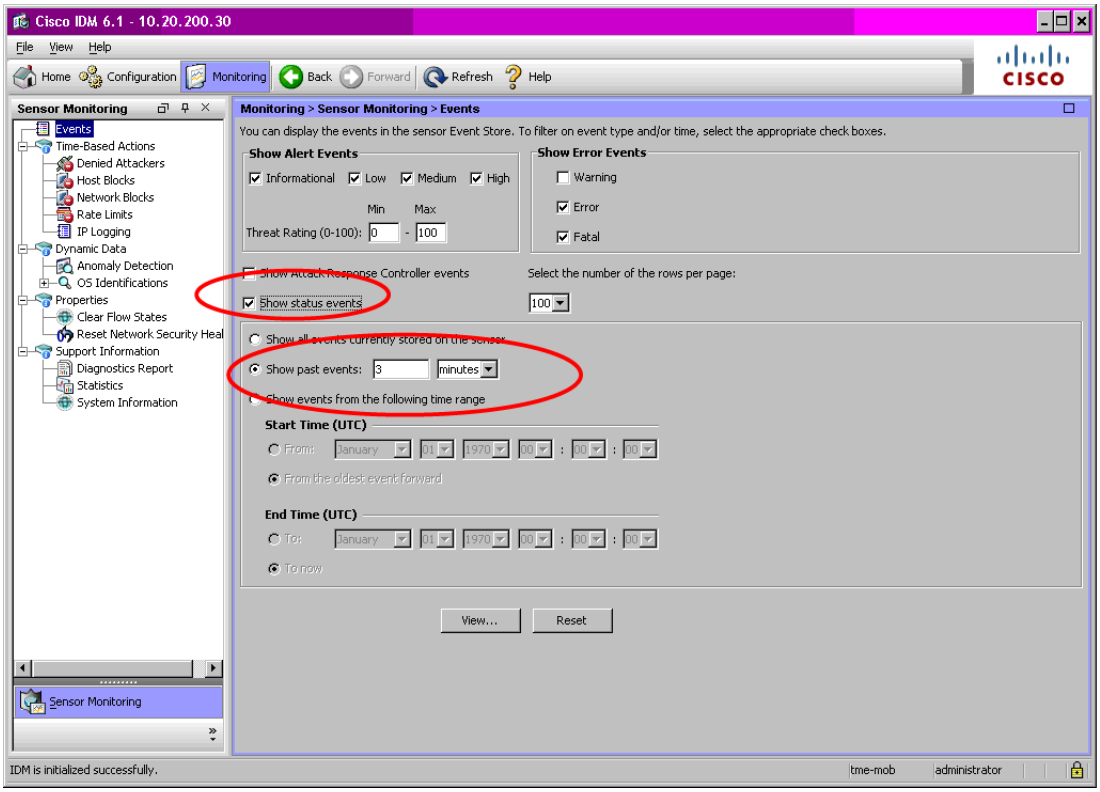
- クライアント IP アドレスのアクティブな IPS ホスト ブロックが存在している間に、WLC クライアント除外が期限切れになると、WLC は、クライアントが WLAN にアソシエートするか、アソシエートを試みるたびに、新しいクライアント除外を自動的に作成します。
- したがって、IPS ホスト ブロックが有効である期間とクライアント除外タイムアウトによっては、複数のクライアント除外イベントが発生し、複数の SNMP トラップが生成されることがあります。

ホスト ブロック イベントに関連する IPS イベント

ホスト ブロックがアクティブになったときに Cisco IPS によって生成されたイベントは、IDM で表示できます。

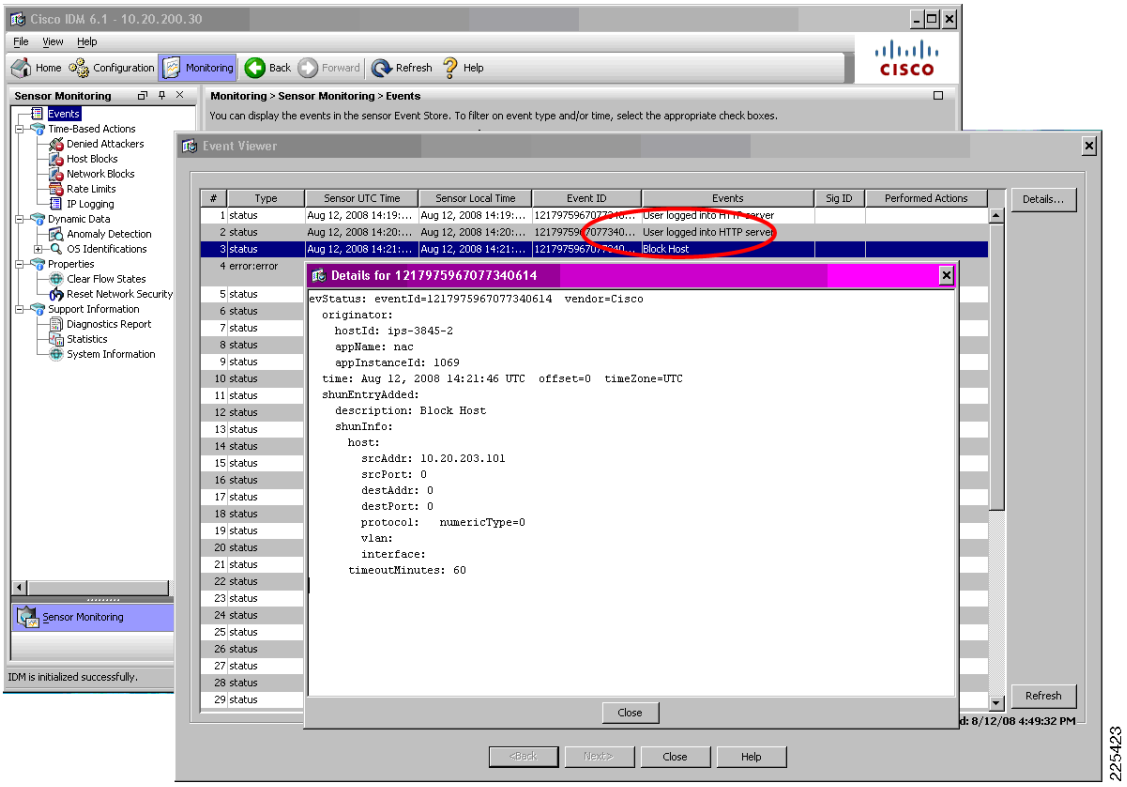
IDM で、**Monitoring -> Events** の順に進みます。**Show status events** を有効にし、**Show past events** で短い期間を定義して（図 8-32 では 3 分と表示）、**View** を選択します。

図 8-32　　IDM でのホスト ブロック イベントの表示



その後、IDM Event Viewer が表示されます。IDM Event Viewer 画面では、アクティブにされたホスト ブロックごとに **Block Host** イベントが生成されます。ブロックされた IP アドレスなどの詳細を表示するには、イベントをダブルクリックします（図 8-33 を参照）。

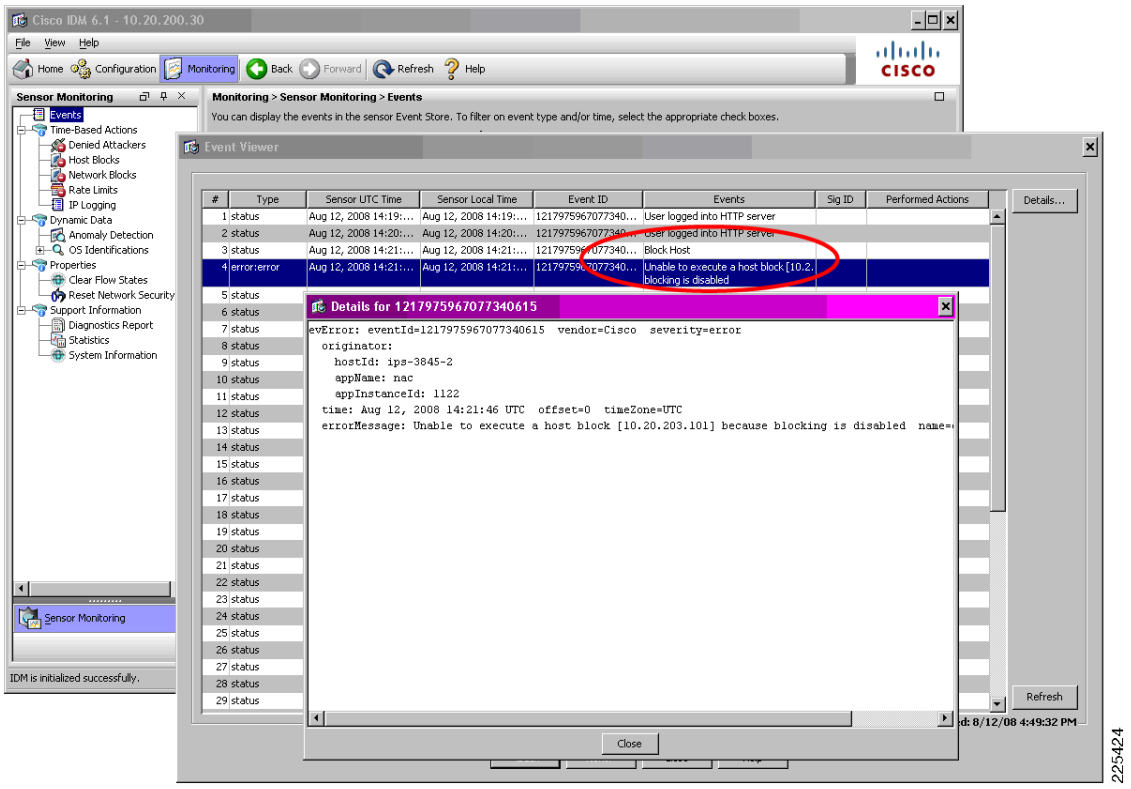
図 8-33　　IDM でのブロック ホスト イベント



（注） IPS でブロッキングが有効でないか、または設定されていない場合、ホスト ブロックを実行できないことを示すエラー イベントが生成されます（図 8-34 を参照）。ただし、アクティブなホスト ブロック リストはそのホスト ブロックで正しくアップデートされ、WLC-IPS コラボレーションによってブロックが正常に適用されます。

このエラー メッセージは、単に、IPS がデバイスにホスト ブロック ポリシーをプッシュできなかったことを示します。WLC-IPS コラボレーションでは、これは正常な動作です。IPS がアクティブにホスト ブロックをプッシュするのではなく、WLC が IPS からアクティブなホスト ブロック リストをプルするためです。このエラーは、Attack Response Controller（ARC）機能のプッシュ特性によるものです。この機能は、ホスト ブロック適用のために、ブロッキングが有効にされ、設定されることを期待します。ARC 機能の詳細については、IPS のマニュアルを参照してください（P.8-52 の「Cisco IPS」を参照）。

図 8-34　　IDM でのホスト ブロック エラー イベント



WLAN クライアント ブロック イベントの WLC CLI レポーティング

WLC CLI を使用して、IPS から受信しているアクティブなホスト ブロック リスト、およびアップデートされている Shun リストを表示できます。

これらのイベントのデバッグを有効にするには、次の手順を実行します。

ステップ 1 Cisco IPS とコラボレートしている WLC の CLI にログインします。

ステップ 2次のように入力して、WLC-IPS 通信のデバッグを有効にします。

```
debug wps cids enable
```

イベントが発生するとすぐに、デバッグが自動的に画面に表示されます。

次に、WLC から Cisco IPS への Shun リスト クエリーの例を示します。この例では、Shun リストに、IP アドレス 10.20.203.101 の新しいホスト ブロックが含まれています。

```
Tue Aug 12 14:21:43 2008: cidsProcessSdeeQuery: ip=10.20.200.30,port=443 state=1
interval=60
Tue Aug 12 14:21:43 2008: cidsQuerySend:
https://10.20.200.30:443/cgi-bin/transaction-server?command=getShunEntryList
Tue Aug 12 14:21:43 2008: curlHandle is bbd422c
Tue Aug 12 14:21:43 2008: Perform on curlHandle bbd422c ...
Tue Aug 12 14:21:43 2008: Response code is 0
Tue Aug 12 14:21:43 2008: Add 10.20.203.101 from local sensor 10.20.200.30 to shun-list
Tue Aug 12 14:21:43 2008: xmlDoc buffer freed
Tue Aug 12 14:21:43 2008: Parser cleaned
```

ステップ 3デバッグの完了後、デバッグを無効にします。

```
debug wps cids disable
```

WLAN クライアント ブロック イベントの IPS CLI レポーティング

次の手順を実行することで、WLC にホスト ブロックが渡されるときに IPS CLI で生成されたイベントを表示できます。

ステップ 1 Cisco WLC とコラボレートしている IPS の CLI にログインします。

ステップ 2次のように入力して、その WLC の最近のイベントを確認します。

```
ips-3845-2# show events past 0:03 | include block
```

次に、Cisco IPS でアクティブにされているホスト ブロックと取得の例を示します。

```
evStatus: eventId=1217975967077340614 vendor=Cisco
  originator:
    hostId: ips-3845-2
    appName: nac
    appInstanceId: 1069
  time: 2008/08/12 14:21:46 2008/08/12 14:21:46 UTC
  shunEntryAdded:
    description: Block Host
    shunInfo:
      host:
        srcAddr: 10.20.203.101
        srcPort: 0
        destAddr: 0
        destPort: 0
        protocol: numericType=0
        vlan:
        interface:
      timeoutMinutes: 60
```

（注） IPS でブロッキングが有効でないか、または設定されていない場合、ホスト ブロックを実行できないことを示すエラー イベントが生成されます（図 8-34 を参照）。ただし、アクティブなホスト ブロック リストはそのホスト ブロックで正しくアップデートされ、WLC-IPS コラボレーションによってブロックが正常に適用されます。

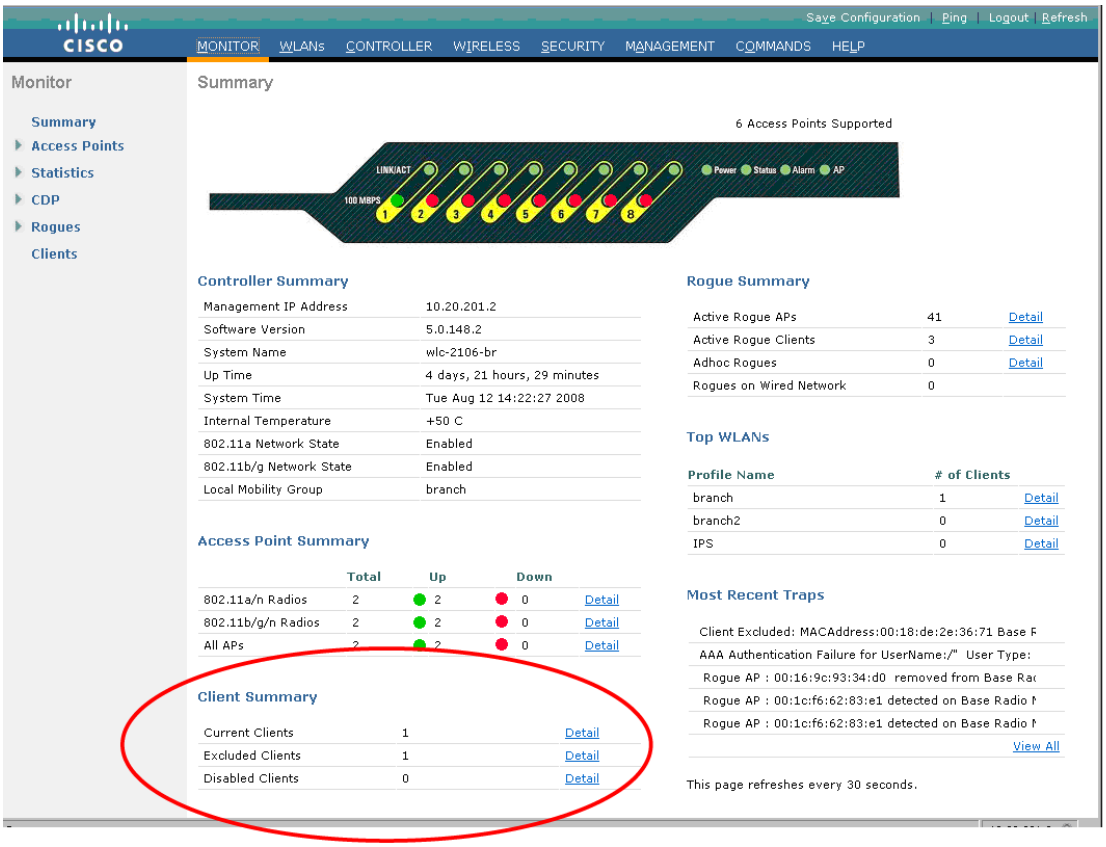
このエラー メッセージは、単に、IPS がデバイスにホスト ブロック ポリシーをプッシュできなかったことを示します。WLC-IPS コラボレーションでは、これは正常な動作です。IPS がアクティブにホスト ブロックをプッシュするのではなく、WLC が IPS からアクティブなホスト ブロック リストをプルするためです。このエラーは、Attack Response Controller（ARC）機能のプッシュ特性によるものです。この機能は、ホスト ブロック適用のために、ブロッキングが有効にされ、設定されることを期待します。ARC 機能の詳細については、IPS のマニュアルを参照してください（P.8-52 の「Cisco IPS」を参照）。

```
evError: eventId=1217975967077340615 severity=error vendor=Cisco
  originator:
    hostId: ips-3845-2
    appName: nac
    appInstanceId: 1122
  time: 2008/08/12 14:21:46 2008/08/12 14:21:46 UTC
  errorMessage: name=errSystemError Unable to execute a host block [10.20.203.101] because
blocking is disabled
```

除外されたクライアントの表示

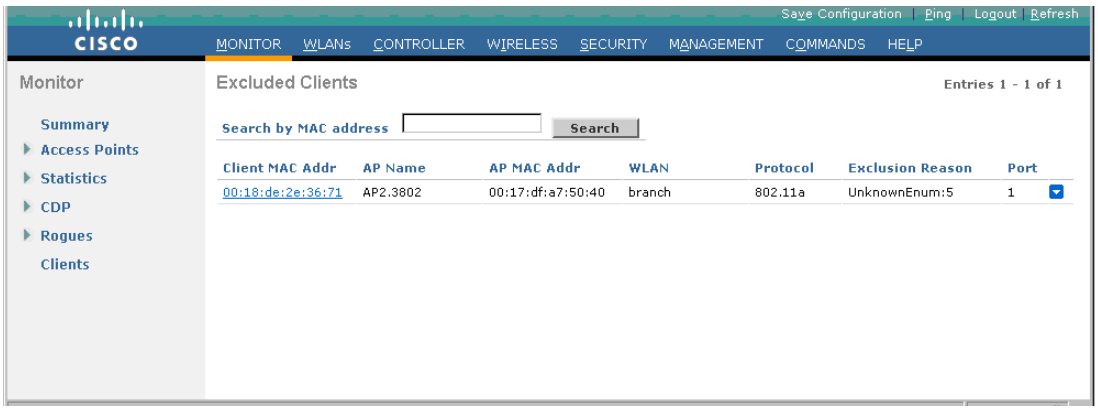
WLC で現在有効なすべてのクライアント除外および除外の理由は、WLC の「Excluded Clients」リストで確認できます。これを表示するには、**Monitor -> Summary** の順に進み、Client Summary セクションで「Excluded Clients」の隣にある **Detail** をクリックします（図 8-35 を参照）。

図 8-35　除外されたクライアントの Detail リンクを含む WLC の Monitor Summary 画面



その後、Excluded Clients リストが表示されます（図 8-36 を参照）。

図 8-36　Excluded Clients リスト



次の点に注意してください。

- IPS ホスト ブロックの結果として作成されたクライアント除外は、除外理由「UnknownEnum:5」で表示されます。
- 除外された WLAN クライアントは、WLC でクライアント除外が有効である間、このサマリー画面に表示されます。
- クライアント除外は、その特定の WLAN プロファイルのクライアント除外タイムアウトに基づいて、有効期限が切れるまでアクティブなままです。
- クライアント除外は、Cisco IPS ホスト ブロックの取り消しでは削除されません。
- 除外されたクライアント エントリは、そのクライアントが WLC に接続されていたが切断されたことを示します。

WLC をまたがる WLAN クライアント ブロック イベントの WCS でのモニタリング

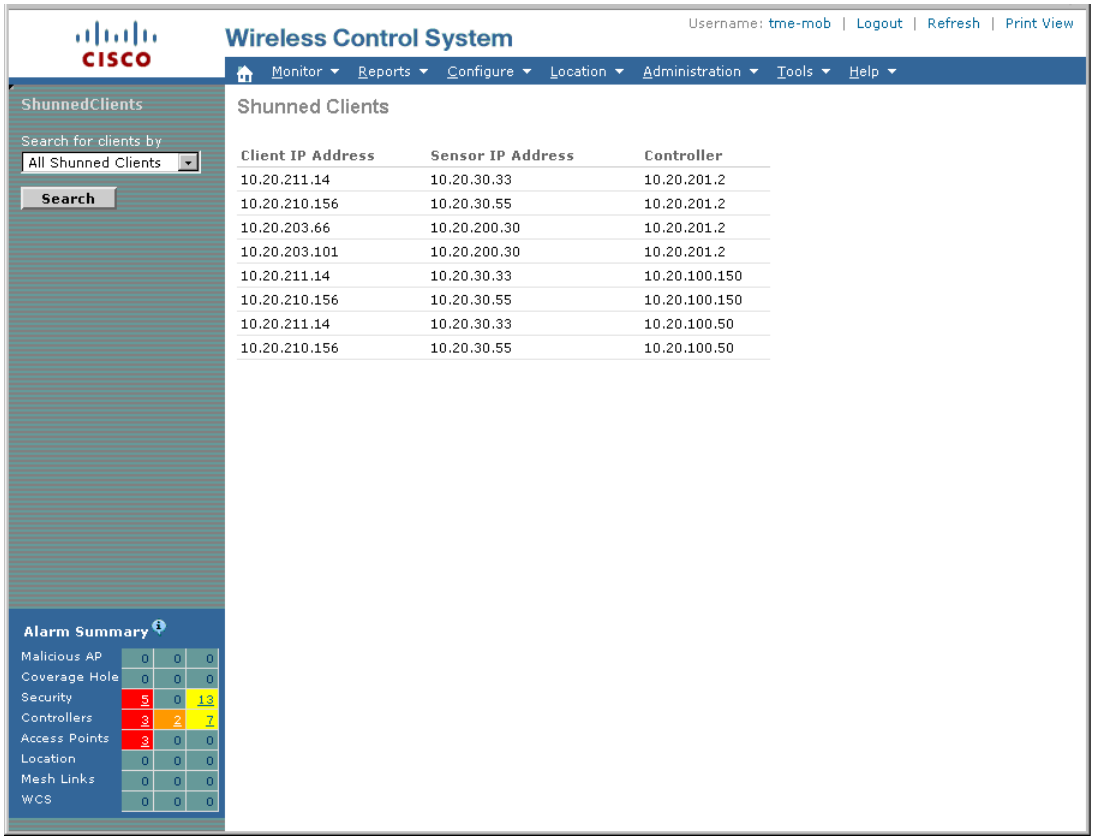
WCS のクロス WLC モニタリングが有効である場合、現在回避されているクライアントおよび現在除外されているクライアントの統合ビューを WCS で表示できます。また、過去のセキュリティ イベントと統計情報も表示できます。WLAN イベントに対する WCS のクロス WLC モニタリングを有効にする方法の詳細については、P.8-19 の「WLC をまたがる WLAN イベントの WCS でのモニタリングの有効化」を参照してください。

回避されたクライアントの統合リスト

WCS は、回避されたクライアントの統合リストを提供します。このリストには、すべての WLC に渡されたすべてのアクティブなホスト ブロックが表示されます。

WCS で、**Monitor -> Security -> Shunned Clients** の順に進みます。ドロップダウン リストから検索オプションを選択します。この検索オプションにより、すべての IP アドレス、コントローラごとの IP アドレス、またはクライアントごとの IP アドレスに基づいて、ブロックされたクライアントのリストを生成できます（図 8-37 を参照）。

図 8-37　回避されたクライアントに関する WCS のクロス WLC ビュー



次の点に注意してください。

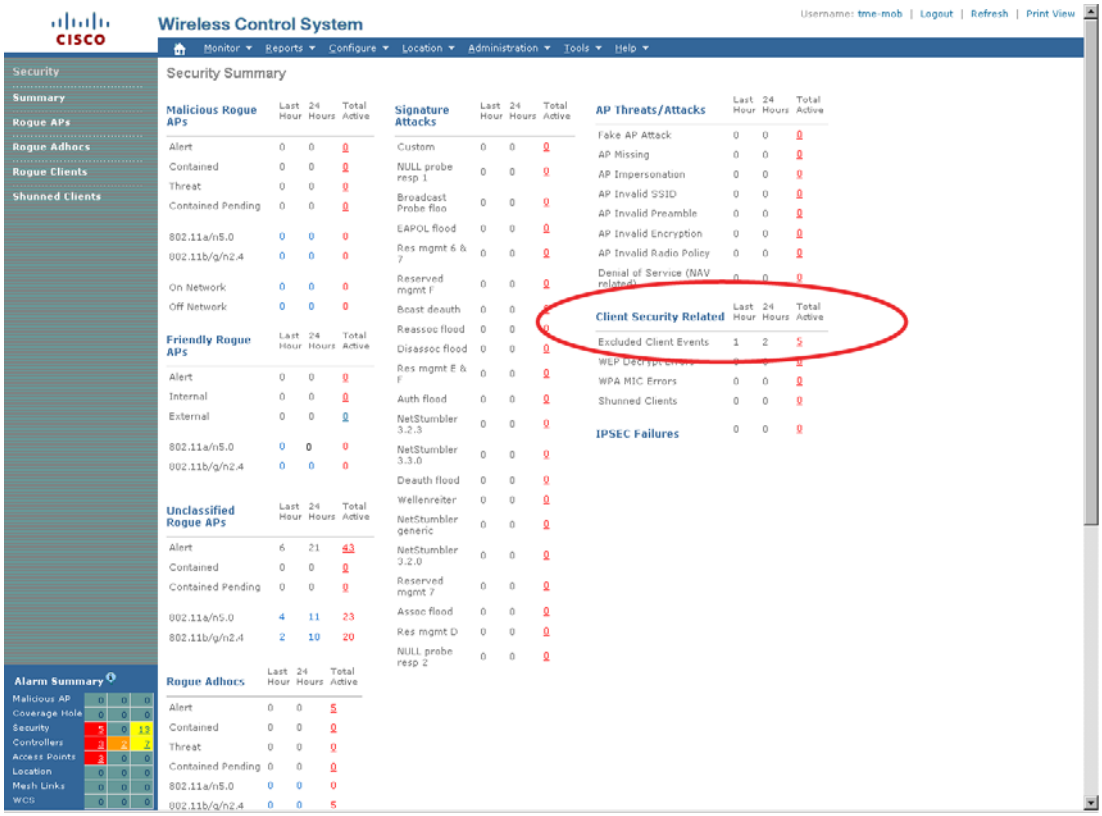
- これは、コラボレートしているすべての Cisco IPS デバイスから WLC に渡された、各 WLC 上の回避クライアント リストの統合ビューです。
- このリストは、WLC によってブロックされるクライアント IP アドレスを示しています。これに一致する IP アドレスを持つクライアントは、WLAN に接続しているとブロックされます。
- このリストは、WLC によって現在除外されているクライアントを表すものではありません。
- 複数の WLC が同じ Cisco IPS とコラボレートする場合は、重複したクライアント IP アドレスが表示されます。

除外クライアント イベントの統合リスト

WCS は、すべての WLC にわたるアクティブなクライアント除外の統合リストを提供します。

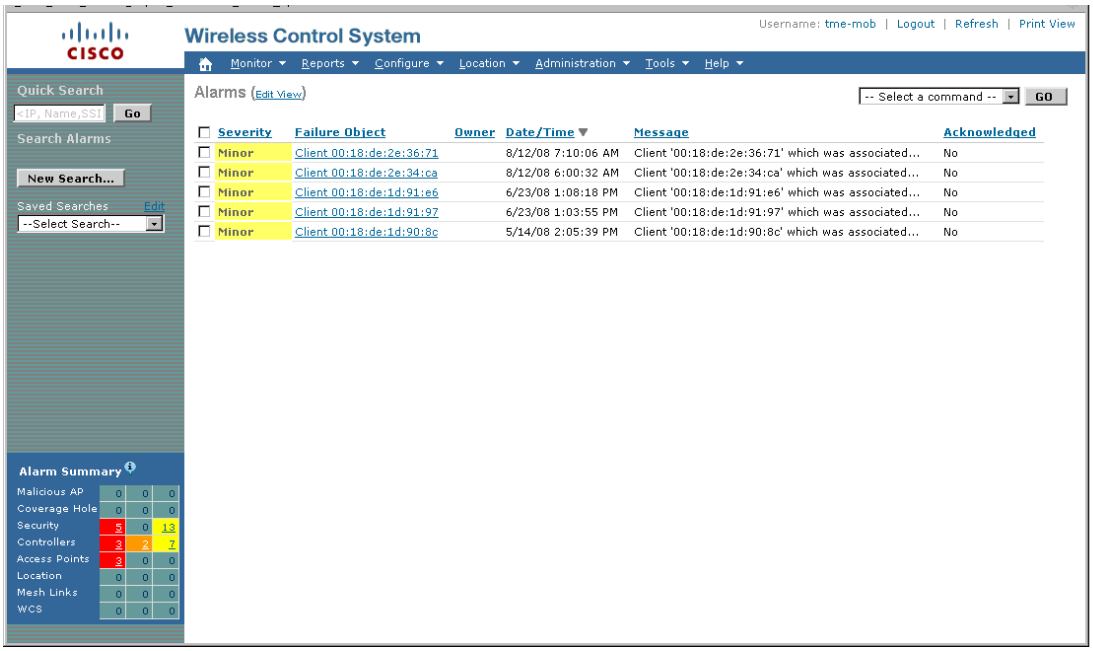
WCS で、**Monitor -> Security -> Summary** の順に進み、**Excluded Client Events** に対応する **Total Active** フィールドをクリックします（図 8-38 を参照）。

図 8-38　WCS の Security Summary 画面の例



その後、すべての WLC にわたるアクティブなクライアント除外が表示されます（図 8-39 を参照）。

図 8-39　アクティブな除外クライアント イベントを示す WCS 画面の例

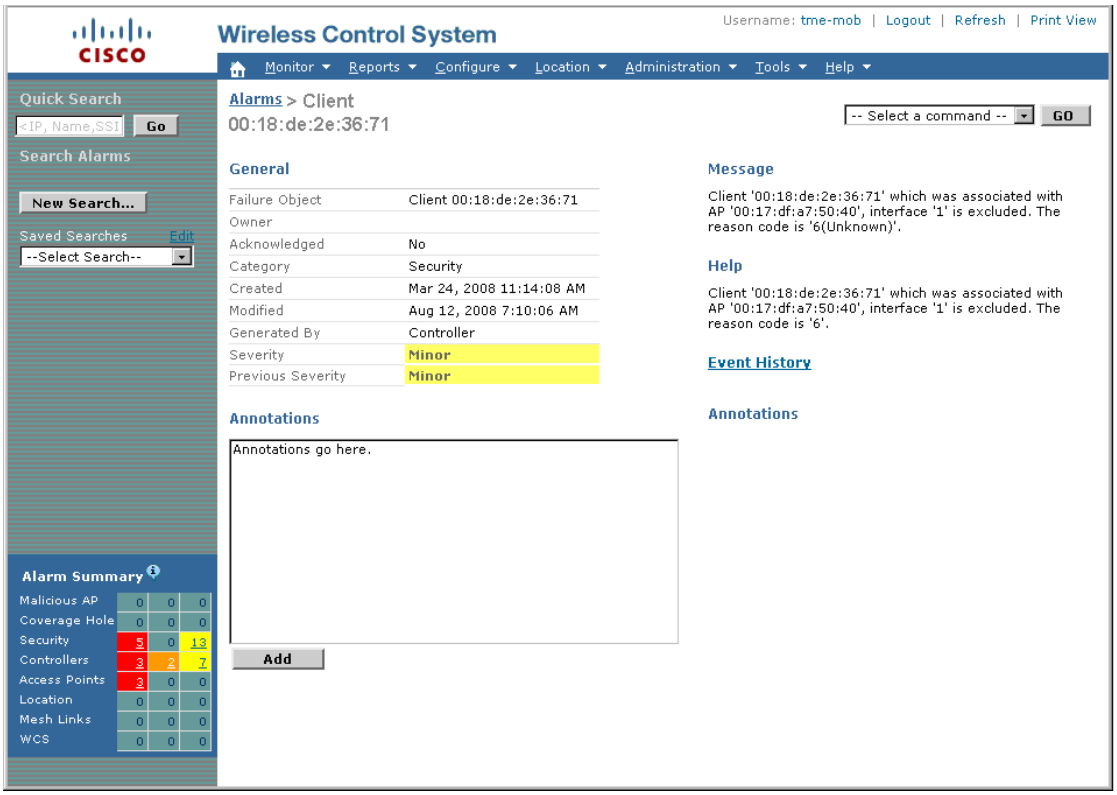


次の点に注意してください。

- WCS は、イベントに関するデータの集約を実行します。したがって、同じイベントがまとめられ、1 つのイベントとして表示されます。この機能の設定は変更できません。ただし、すべてのイベントはロギングされ、任意のイベントのイベント履歴で表示することができます。

クライアントをクリックすることで、任意の除外イベントの詳細情報を表示できます（図 8-40 を参照）。

図 8-40　詳細なクライアント除外イベントを示す WCS 画面



シスコの無線 IDS/IPS とネットワーク IDS/IPS の統合に関する一般的なガイドライン

無線 IDS/IPS とネットワーク IDS/IPS を展開するための一般的なガイドラインは、次のとおりです。

- WLAN 固有の脅威の検出と軽減には、Cisco WLC の無線 IDS/IPS 機能を利用します。
- WLAN クライアントの一般的な脅威の検出と軽減のために、Cisco IPS を展開します。
- Cisco WLC と Cisco IPS の統合を有効にして、簡単で効果的な脅威軽減ツールを運用スタッフに提供し、集中化された制御と適用をアクセス エッジで直接実現します。
- 分散型 IPS 展開を利用して、ネットワークをまたがる脅威の検出と軽減に向けた Cisco WLC と IPS のコラボレーションおよび IPS どうしのコラボレーションを最大限にします。
- ポリシー違反イベントが定期的に監視され、確認されるようにします。

その他の情報

Cisco WLC と Cisco IPS のコラボレーションの運用上の詳細

Cisco WLC と Cisco IPS の統合に関連して運用上の観点から考慮する必要のある一般的な情報は、次のとおりです。

- Cisco IPS ホスト ブロックは、送信元 IP アドレスに基づいて定義されます。
- Cisco IPS ホスト ブロックは、WLC で MAC ベースのクライアント除外として適用されます。
- アクティブなホスト ブロックのタイムアウトは、Cisco IPS で定義します。
- クライアント除外のタイムアウトは、WLAN プロファイルごとに WLC で定義します。
- Cisco IPS ホスト ブロックが有効である間に、ブロックされた WLAN クライアントが WLAN に再アソシエートすると、そのクライアントは引き続き切断されたままです。
- Cisco IPS ホスト ブロックが有効である間に、クライアント除外が期限切れになった場合、WLC は、クライアントが WLAN に接続しようとすると、新しいクライアント除外を作成します。
- ブロック対象クライアントは、その IP アドレスを変更することで、ホスト ブロックをバイパスできます。
- クライアント除外が有効である間は、ブロックされたクライアントが異なる IP アドレスで WLAN に再接続しようとすると、WLC がそのクライアントをブロックします。
- デフォルトでは、ブロックされた WLAN クライアントは再接続を試みます。WLAN から繰り返し切断されたときの WLAN クライアントの正確な動作は、その特定の WLAN クライアントおよび無線のコンフィギュレーション設定によって異なります。一部のクライアントは、特定の回数、接続試行に失敗すると、特定の WLAN への再接続試行を停止することがあります。
- WLC で適用されているアクティブなクライアント除外を表示するには、**Monitor-> Wireless -> Clients** を参照します。このリストには、除外されたクライアントが *Excluded* というステータスで表示されます。ただし、除外されたクライアントは現在接続されていません。
- ホスト ブロックが取り消されても、取り消されたホスト ブロックに対応するアクティブなクライアント除外は有効なままです。クライアント除外は、クライアントの MAC アドレスに基づいて定義されており、その WLAN プロファイルに設定されているクライアント除外タイムアウトになるまで有効なままです。したがって、Cisco IPS でホスト ブロックが有効でなくなっても、クライアント除外がタイムアウトになるまで、以前にブロックされたクライアントは、引き続き WLAN への接続をブロックされます。
- WLAN クライアントが固定 IP アドレスで接続する場合、WLC がそのクライアント IP アドレスを認識するまでに少し時間がかかることがあります（その間、クライアント IP アドレスは 0.0.0.0 と表示されます）。WLC は、クライアント IP アドレスの認識後に限り、ホスト ブロックを適用できます。
- ブロックされた IP アドレスが別のクライアントに再割り当てされるというリスクがあります。
- Cisco IPS から Cisco WLC への自動脅威軽減技術を効果的なものにするために、ネットワーク上で送信元 IP スプーフィング保護を有効にする必要があります。

Cisco IPS の展開モード

この機能を展開するときの設計上の主要な選択の 1 つは、IDS モードにするか IPS モードにするかです。

- IDS モード

  Promiscuous（無差別）モードのパッシブ モニタリング。トラフィックが、モニタリング ポートを通じて分析のために IDS に渡されます。異常な動作が検出されると、管理システムにイベントが通知されます。その後、運用スタッフが、そのインシデントに対して実行するアクションを決定します。

- IPS モード

  インライン モードのアクティブ モニタリング。データ パスに IPS が存在します。検出機能は IDS の場合と同じです。ただし、インライン設定では、悪意のあるトラフィックを IPS デバイス自体でフィルタするオプションが運用スタッフに提供されます。

（注） IPS モードはデータ パスに存在するため、IPS モードがネットワークのパフォーマンスに悪影響を及ぼさないように展開が適切に設計されていることを確認することが重要です。

IPS センサーは、通常、IDS モードまたは IPS モードのいずれかで動作するようにしか設定できません。ただし、設計上、両方のモードを展開する必要が生じることがあります。たとえば、VLAN ごとに、一部のフローではパッシブ モニタリングを提供し、他のフローではアクティブ モニタリングを提供する場合です。このシナリオを実現するために、次の条件で設計することができます。

- 複数の物理プラットフォーム。各プラットフォームを IDS モードまたは IPS モードで展開します。
- 複数の仮想センサーをサポートする 1 つのプラットフォーム。同じプラットフォームで IDS モードと IPS モードの両方を有効にします。これは、一部のセンサーを IDS モードで設定し、他のセンサーを IPS モードで設定することによって実現されます。各仮想センサーは、IDS モードまたは IPS モードのいずれかで動作するようにしか設定できないことに注意してください。

製品、プラットフォーム、機能、展開オプション、および考慮事項の詳細については、製品ページを参照してください。詳細については、P.8-52 の「参考資料」を参照してください。

Cisco IPS のブロック アクションと拒否アクション

Cisco IPS のブロック アクションは、IPS でアクティブにされますが、コラボレートしているデバイスで適用されます。Cisco IPS は、ローカライズされた技術で脅威軽減を適用するために、このコラボレート デバイスに依存します。Cisco Unified Wireless Network では、このシナリオのコラボレート デバイスは Cisco WLC で、ローカルな脅威軽減技術はクライアント除外です。

これに対して、Cisco IPS の拒否アクションは、IPS で作成され適用されます。IPS 自体がトラフィックをフィルタし、攻撃を軽減します。拒否アクションは、WLC での WLAN クライアント ブロックをトリガーしません。

必要な場合は、ブロック アクションと拒否アクションの両方のアクティブ化により、IPS で直接、および別のネットワーク デバイス（Cisco WLC など）とのコラボレーションを通じて、脅威軽減を適用できます。

（注）　Cisco IPS を通過するトラフィックに対して脅威軽減を Cisco IPS が直接実行できるようにするには、Cisco IPS をインライン モードで展開する必要があります。

Cisco IPS と Cisco WLC の統合の依存関係

Cisco IPS と Cisco WLC のコラボレーションは、表 8-3 に示すソフトウェア プラットフォームおよびハードウェア プラットフォームに依存します。

表 8-3　Cisco IPS と Cisco WLC の統合の依存関係

コンポーネント	最小限のソフトウェア	ハードウェア
IPS	IPS センサー ソフトウェア リリース v5.x 以降	• Cisco IPS 4200 シリーズ アプライアンス
		• Catalyst 6500 シリーズ Intrusion Detection System Services Module（IDSM-2）
		• ASA IPS モジュール（AIP-SSM）
		• ISR AIM IPS モジュール（AIM-IPS）
WLC	Cisco Unified Wireless Network v4.0 以降	• すべての Cisco Unified Wireless Network WLAN コントローラおよびアクセス ポイント
LWAPP AP		

Cisco Integrated Services Router（ISR: サービス統合型ルータ）などのルーティング プラットフォーム用の Cisco IOS IPS は、現在、脅威軽減に向けた Cisco WLC との統合をサポートしていないことに注意してください。

テスト ベッドのハードウェアとソフトウェア

表 8-4 に示す IPS と WLC のすべてのプラットフォームおよびソフトウェア リリース間で、統合テストが実施および検証されました。

表 8-4　テスト ベッドのハードウェアとソフトウェア

コンポーネント	ハードウェア	ソフトウェア
IPS	ISR 3845 内の AIM-IPS	6.1(1)E2 IOS v12.4(20)T を実行する ISR
	ASA 5520 内の AIP-SSM-20	6.0(3)E1 8.0(3) を実行する ASA
	IPS 4255	5.1(1)S205.0
WLC	WLC 2106	5.0.148.2
	Cisco Catalyst 6500 シリーズ内の Wireless Services Module（WiSM）	5.0.148.2
WCS		5.0.72.0

- その他のプラットフォームおよびモードがサポートされており、同様の機能を提供します。
- IPS デバイスは、Promiscuous（無差別）モードで設定されました。
- Cisco WLC と Cisco IPS のコラボレーションは、WLC バージョン 4.0.206.0、WCS バージョン 4.0.96.0 と 5.0.56.0、Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）上の WLC バージョン 4.1.171.0、および Cisco IPS 4255 バージョン 5.1(1) で、すでに検証されています。

参考資料

Cisco IPS

- Cisco IPS 製品

  http://www.cisco.com/go/ips
- Cisco IPS 4200 シリーズの設定例およびテクニカル ノート

  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_configuration_examples_list.html
- Cisco IPS 4200 シリーズのコンフィギュレーション ガイド

  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html
- Cisco IPS の調整の概要（CCO へのログインが必要）

  http://www.cisco.com/en/US/partner/prod/collateral/vpndevc/ps5729/ps5713/ps4077/overview_c17-464691.html

シスコ セキュリティ製品

- シスコ セキュリティ製品

  http://www.cisco.com/en/US/products/hw/vpndevc/index.html

Cisco Unified Wireless

- Cisco Wireless Network セキュリティ

  http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns386/networking_solutions_package.html
- シスコ無線製品

  http://www.cisco.com/en/US/products/hw/wireless/index.html
- シスコ無線 LAN コントローラと Cisco IPS の統合ガイド

  http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807360fc.shtml

一般的なネットワーク セキュリティ

- ネットワーク セキュリティ ベースライン

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

CHAPTER 9

Cisco Unified Wireless 用の CS-MARS 統合

安全な Unified Network は、有線と無線の両方のアクセスを特徴とし、効果的な脅威の検出と軽減にとって重要なネットワークをまたがる異常検出や関連性の特定など、セキュリティに対する統合型の多層防御アプローチを必要とします。

この章では、CS-MARS を Cisco Unified Wireless Network と統合して、ネットワークをまたがる異常検出と関連性の特定を WLAN にまで拡張し、ネットワークのすべての要素にわたる可視性をネットワーク セキュリティ スタッフに提供する方法について説明します。

この章で示すソフトウェア実装、スクリーンショット、および動作は、P.9-27 の「テスト ベッドのハードウェアとソフトウェア」に記載のリリースに基づいています。読者は、すでに CS-MARS と Cisco Unified Wireless Network の両方に精通していることを前提とします。

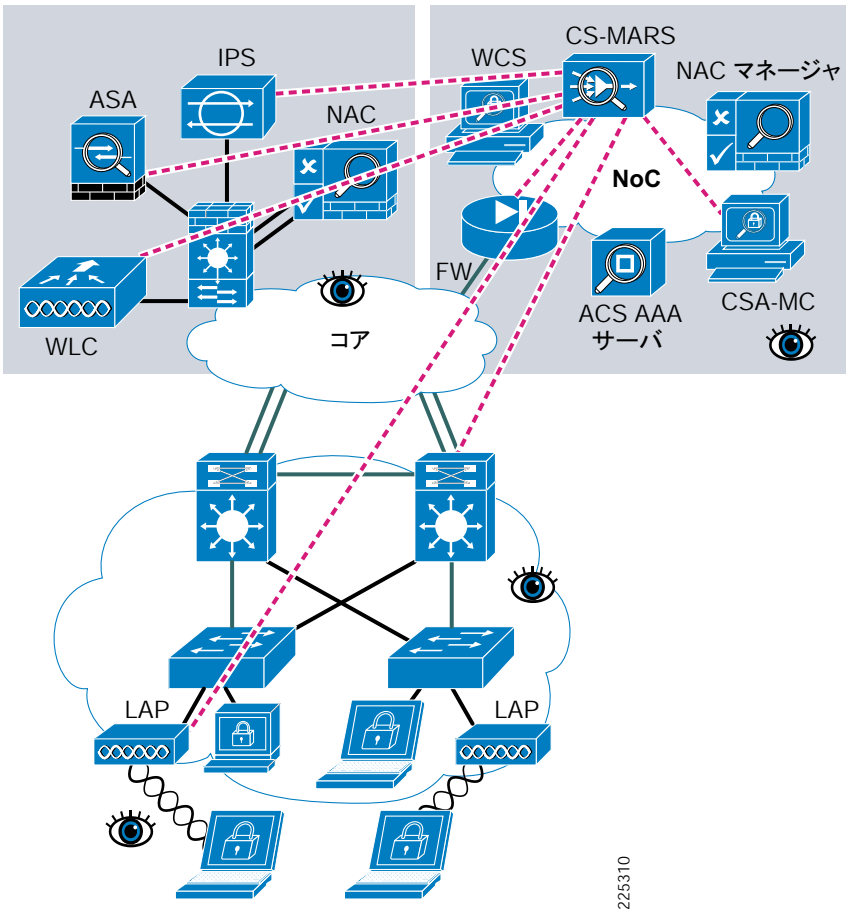
（注） このガイドでは、Cisco Unified Wireless 統合に固有の CS-MARS 機能だけを扱います。

CS-MARS のネットワークをまたがるセキュリティ モニタリング

CS-MARS のセキュリティ モニタリングは、ネットワークをまたがるインテリジェンス、イベントの高度な関連性の特定、および脅威の検証を統合し、ネットワークやアプリケーションの潜在的な脅威を効果的に識別します。

ネットワーク インテリジェンスは、シスコや他のベンダーのネットワーク デバイスやホスト アプリケーションなど、ネットワーク上のデバイスからの大量のネットワーク データとセキュリティ データの効率的な集約および関連性の特定によって得られます。この拡張モニタリングにより、ネットワーク全体のステータス、トラフィック フロー、およびイベントの重要な可視性が提供されます。CS-MARS の詳細については、P.9-27 の「参考資料」を参照してください。

図 9-1　　CS-MARS のネットワークをまたがる異常検出と関連性の特定



Cisco Unified Wireless への CS-MARS 可視性の拡張

CS-MARS Release 5.3.2 は、Cisco Unified Wireless Network デバイスのネイティブ サポートを導入することで可視性を WLAN にまで拡張し、WLAN イベントを CS-MARS の脅威の検出、調査、軽減、およびレポーティング機能に統合しました。

これには、次のような WLAN イベントの可視性が含まれます。

- WLAN DoS 攻撃
- 不正 AP
- 802.11 プローブ
- アドホック ネットワーク
- クライアント除外とブラックリスト
- WLAN の動作ステータス

詳細については、P.9-14 の「Cisco Unified Wireless 用の CS-MARS 機能」を参照してください。

CS-MARS は、Cisco WLC と Wireless Control System（WCS）によって提供される WLAN 固有の異常検出と関連性を特定する機能を補完し、ネットワークをまたがる異常検出と関連性の特定にとって重要なネットワーク全体の統合ビューをネットワーク セキュリティ スタッフに提供します。

WCS の詳細については、P.9-27 の「参考資料」を参照してください。

CS-MARS と Cisco WLC の統合の実装

Cisco WLC の設定

CS-MARS で Cisco Unified Wireless Network 上のイベントを表示できるようにするには、SNMP トラップを CS-MARS に送信するよう各 Cisco WLC を設定する必要があります。

さらに、CS-MARS が各 WLC とそれに接続されている LWAPP AP を検出する必要がある場合は、各 WLC で読み取り専用のコミュニティ ストリングも設定する必要があります。これにより、CS-MARS が WLC に照会して、その情報を入手できます。

CS-MARS と WLC の統合を有効にするために必要な設定手順は、次のとおりです。

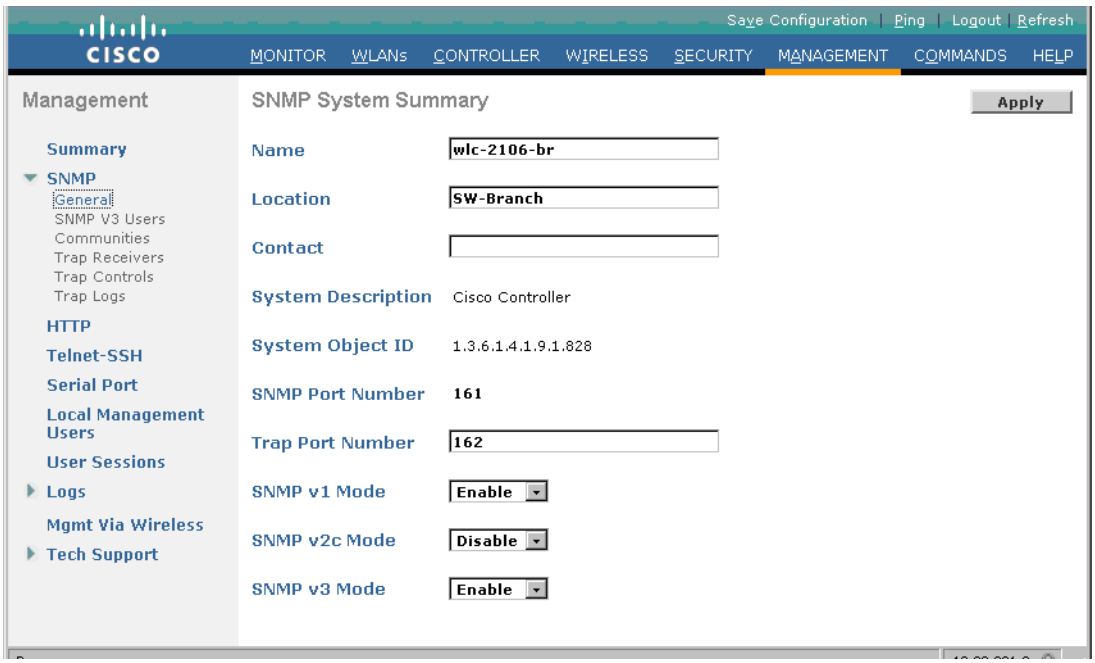
1. SNMP v1 を有効にします（現在、CS-MARS は SNMP v1 だけをサポートしています）。
2. CS-MARS 用のコミュニティ設定を定義します。
3. 必要な SNMP トラップが有効であることを確認します。
4. CS-MARS を SNMP トラップ レシーバとして定義します。

次に、これらの各手順を実行する方法の詳細を示します。

ステップ 1SNMP v1 を有効にします。

WLC で、**Management -> SNMP -> General** の順に進みます。一般的な SNMP パラメータを確認し、SNMP v1 Mode の隣にある状態のボックスを **Enable** に設定して、**Apply** をクリックします（図 9-2 を参照）。

図 9-2 Cisco WLC での SNMP v1 の有効化

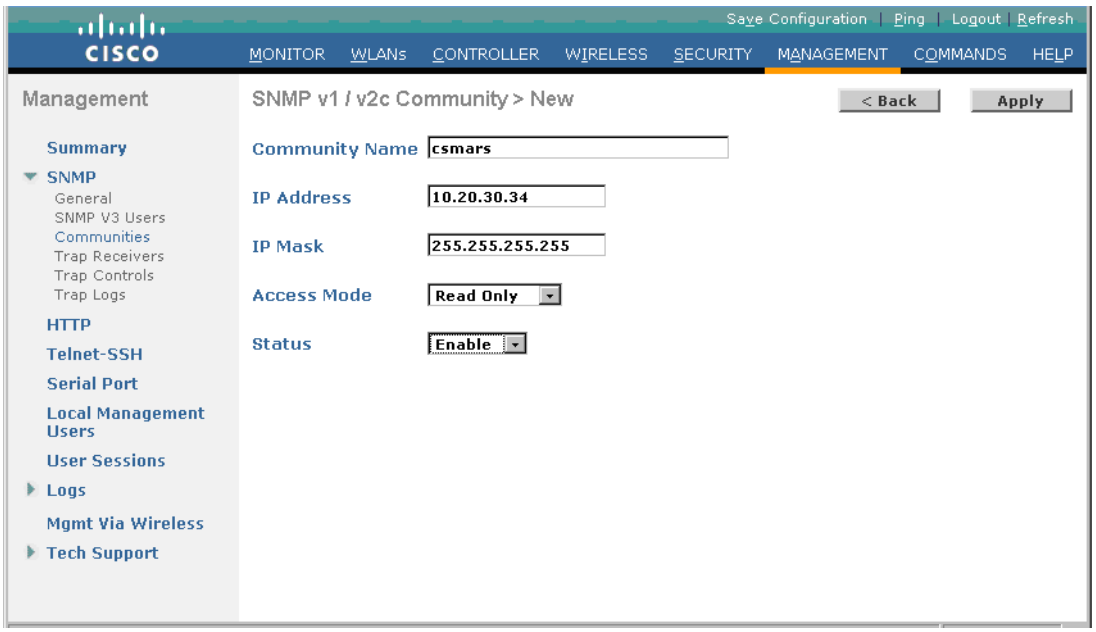


（注） WLC では、デフォルトで SNMP v1 が無効です。

ステップ 2CS-MARS 用のコミュニティ設定を定義します。

WLC で、**Management -> SNMP -> Communities** の順に進みます。CS-MARS 用の読み取り専用コミュニティ ストリング、および CS-MARS 管理ステーションの送信元 IP アドレスとマスクを定義します。Access Mode を **Read Only** に設定し、Status を **Enable** に設定して、**Apply** をクリックします（図 9-3 を参照）。

図 9-3　　CS-MARS 用のコミュニティ設定の定義



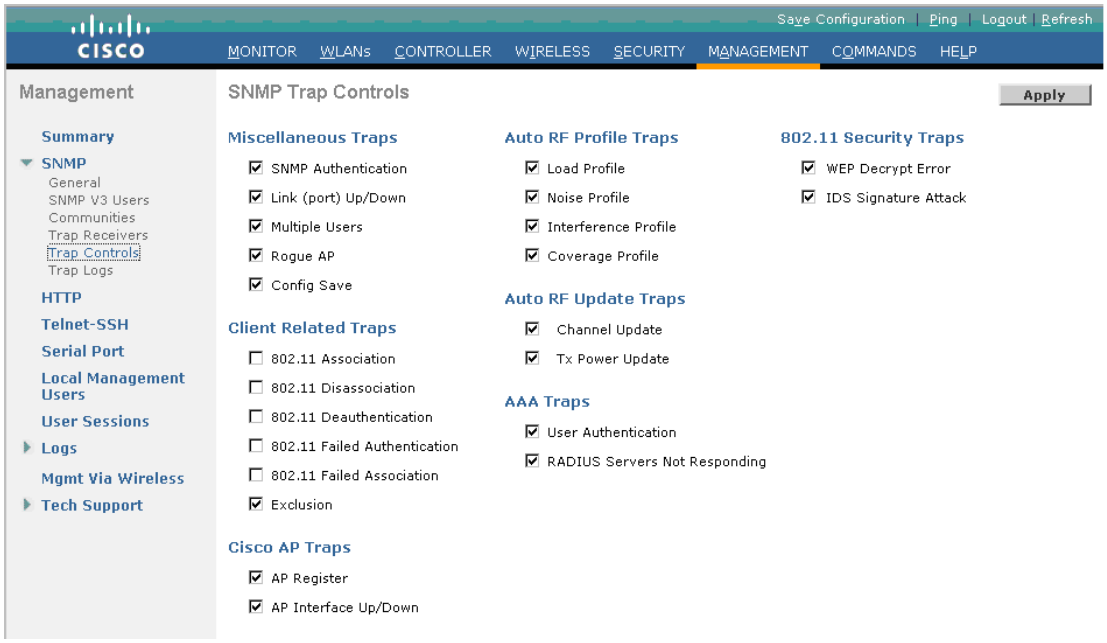
次の点に注意してください。

- IP Address フィールドと IP Mask フィールドがブランクのままである場合、これらのフィールドはデフォルトの 0.0.0.0/0.0.0.0 になり、このコミュニティ ストリングでどの送信元 IP アドレスにも読み取り専用アクセスを許可します。
- 特定のコミュニティ ストリングでのアクセスを、許可された送信元 IP アドレスだけに制限することをお勧めします。
- SNMP v1 は、コミュニティ ストリングを含め、すべてのデータをクリア テキストで伝送するため、スニフィングに対して脆弱です。お客様がセキュリティ ポリシーを確認し、SNMP v1 トランザクションを保護するために IPSec や Out-of-Band（OOB; アウトオブバンド）管理ネットワークなどの追加のセキュリティ技術が必要であるかどうかを判断する必要があります。
- CS-MARS には、読み取り専用のアクセスだけを許可する必要があります。このアクセスだけが必要です。これにより、セキュリティ ベスト プラクティスとして推奨されているとおり、必要最小限のアクセス権限だけが付与されることが保証されます。

ステップ 3必要な SNMP トラップが有効であることを確認します。

WLC で、**Management -> SNMP -> Trap Controls** の順に進みます。チェックボックスがオンになっているすべてのイベントに SNMP トラップが送信されます。モニタリングに必要なトラップ制御を設定し、**Apply** をクリックします（図 9-4 を参照）。

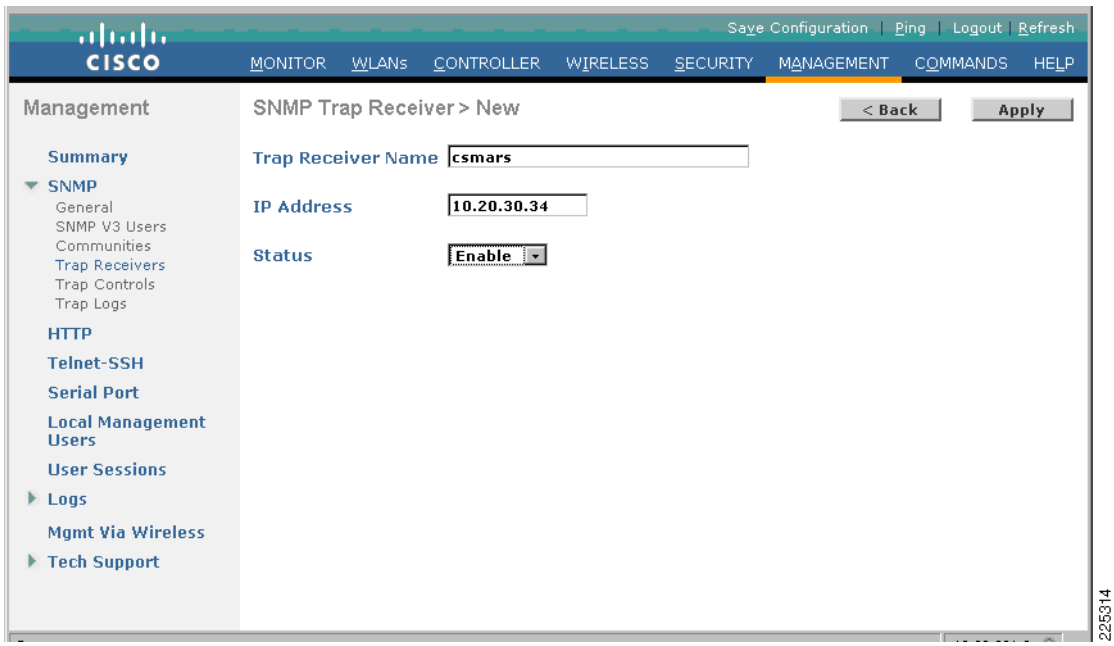
図 9-4 WLC の SNMP トラップ制御の確認



ステップ 4CS-MARS を SNMP トラップ レシーバとして定義します。

WLC で、**Management -> SNMP -> Trap Receivers** の順に進みます。CS-MARS の名前と IP アドレスで、新しい SNMP トラップ レシーバを追加します。Status を **Enable** に設定し、**Apply** をクリックします（図 9-5 を参照）。

図 9-5 SNMP トラップ レシーバとしての CS-MARS の定義



CS-MARS の設定

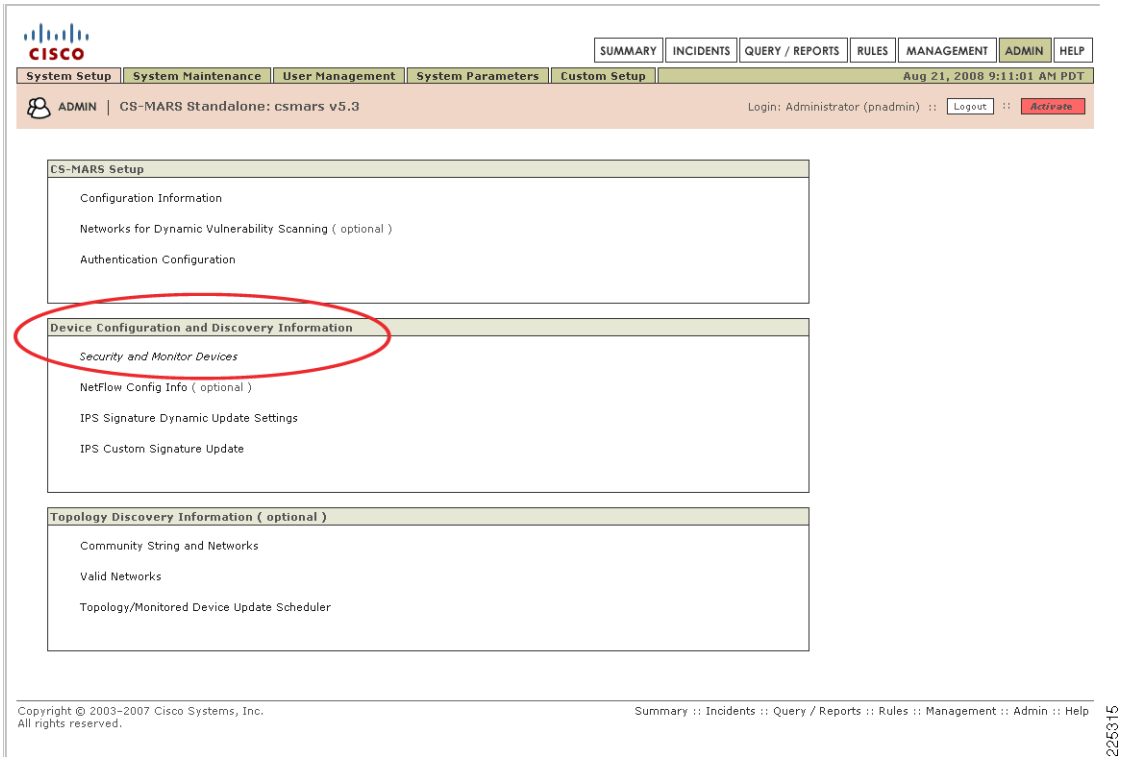
CS-MARS で各 Cisco WLC とそれに接続されている LWAPP AP を検出するには、CS-MARS で各 WLC を定義する必要があります。これにより、WLC デバイスへの SNMP 読み取り専用アクセスが CS-MARS に提供され、CS-MARS がこのデバイスおよび他のデバイスに固有の情報を入手できるようになります。CS-MARS で必要な設定はこれだけです。

Cisco WLC の手動による追加

CS-MARS に Cisco WLC を手動で追加するには、次の手順を実行します。

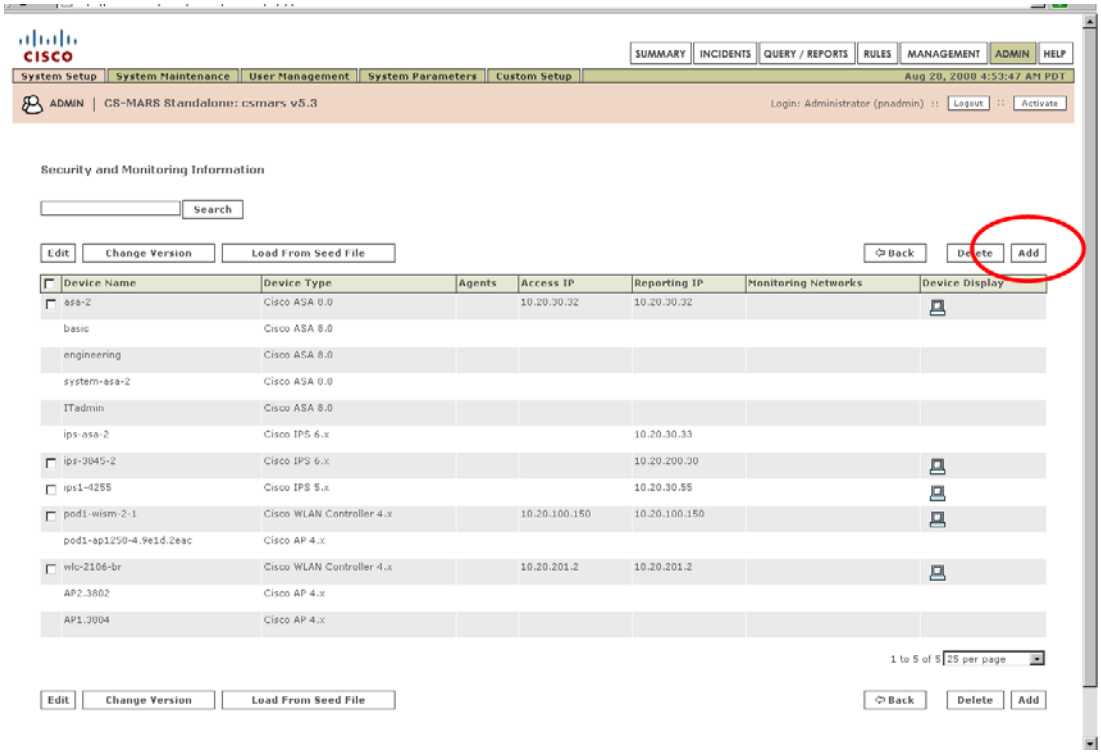
ステップ 1CS-MARS GUI で、**ADMIN -> System Setup** に移動します。中央の **Device Configuration and Discovery Information** というセクションで、**Security and Monitor Devices** を選択します（図 9-6 を参照）。

図 9-6　　CS-MARS の System Setup 画面



ステップ 2 Security and Monitoring Information 画面で、**Add** をクリックします（図 9-7 を参照）。

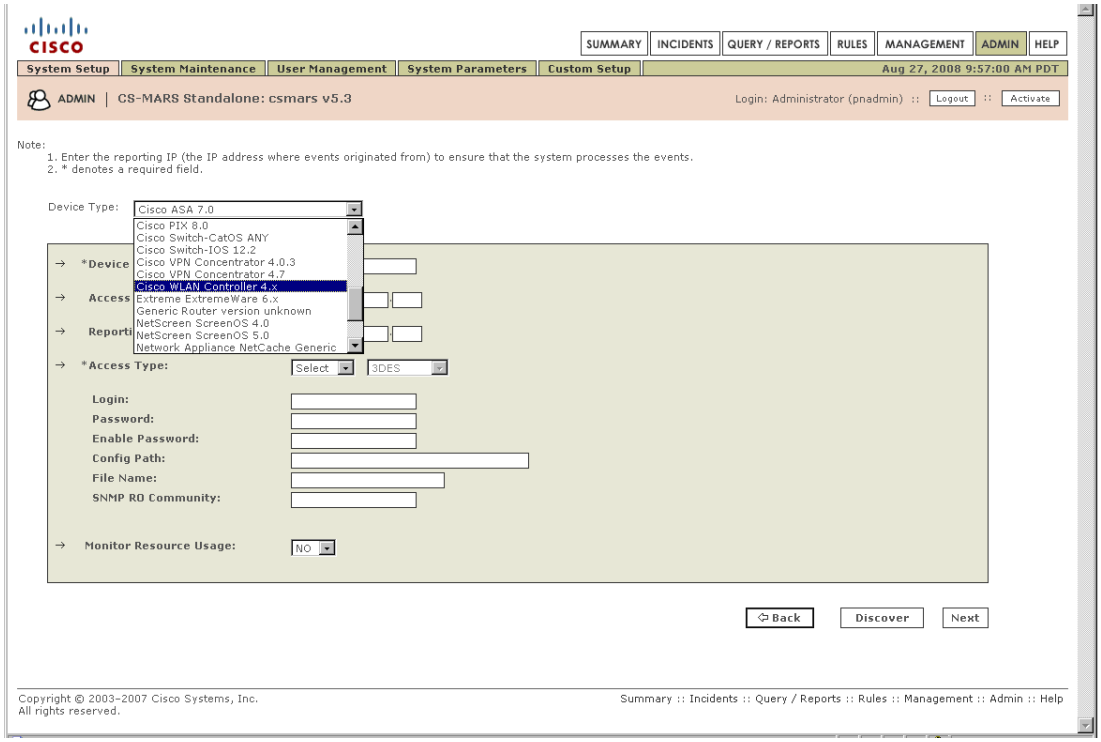
図 9-7　　新しいデバイスを追加するための CS-MARS 画面



ステップ 3 Device Type ドロップダウン ボックスで Cisco WLAN Controller 4.x までスクロールダウンしてそれを選択し、Cisco WLC を追加します。

（注） Cisco Unified Wireless Network Software Release 5.x を実行する WLC がサポートされており、Cisco WLAN Controller 4.x として設定できます（図 9-8 を参照）。

図 9-8　　CS-MARS での Cisco WLC の追加

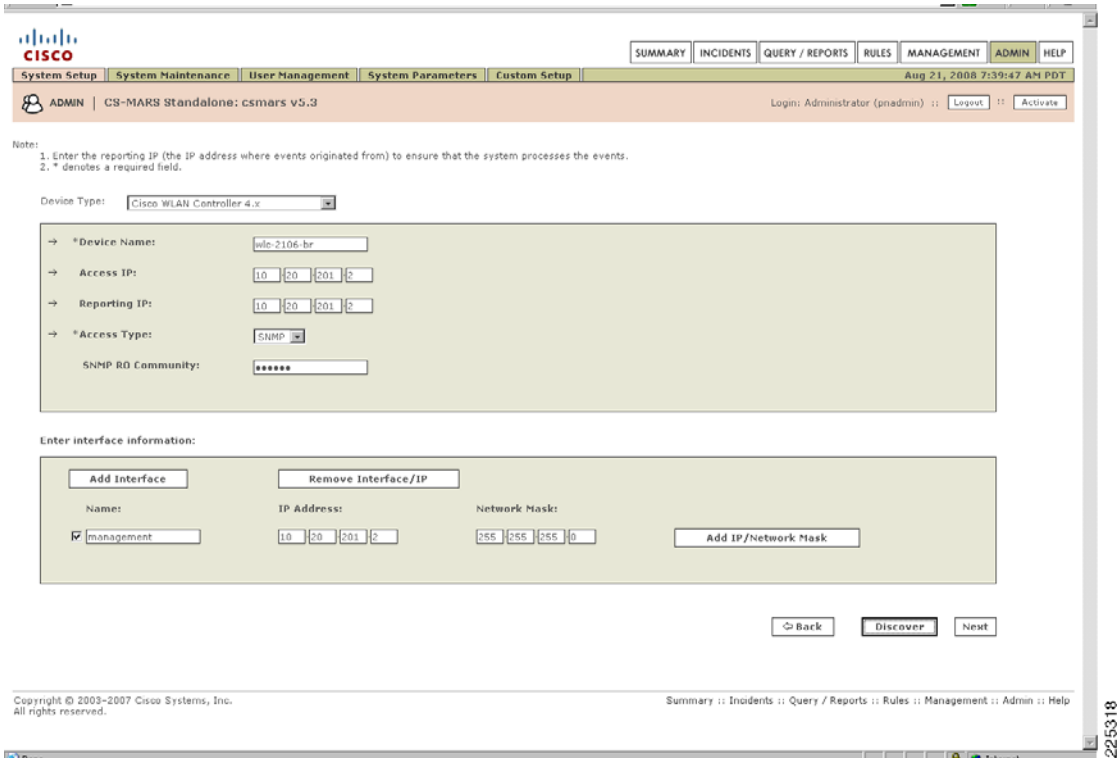


デバイス エントリ フィールドがこのデバイス タイプを反映するように変更されます。また、次の情報を入力して WLC を定義できます。

- Device Name：WLC の名前。
- Access IP：SNMP 読み取り専用アクセスに使用される、WLC の IP アドレス。
- Reporting IP：SNMP トラップの送信元 IP アドレスとして使用される、WLC 管理インターフェイスの IP アドレス。
- Access Type：SNMP（ドロップダウン ボックスで使用可能な唯一のオプション）を選択します。
- SNMP RO Community：WLC で CS-MARS 用に定義されている SNMP コミュニティ名。
- Interface Information：WLC 管理インターフェイスの IP アドレスとネットワーク マスク。

ステップ 4WLC の情報をすべて定義した後、**Discover** をクリックします（図 9-9 を参照）。

図 9-9 CS-MARS での Cisco WLC の定義



次の点に注意してください。

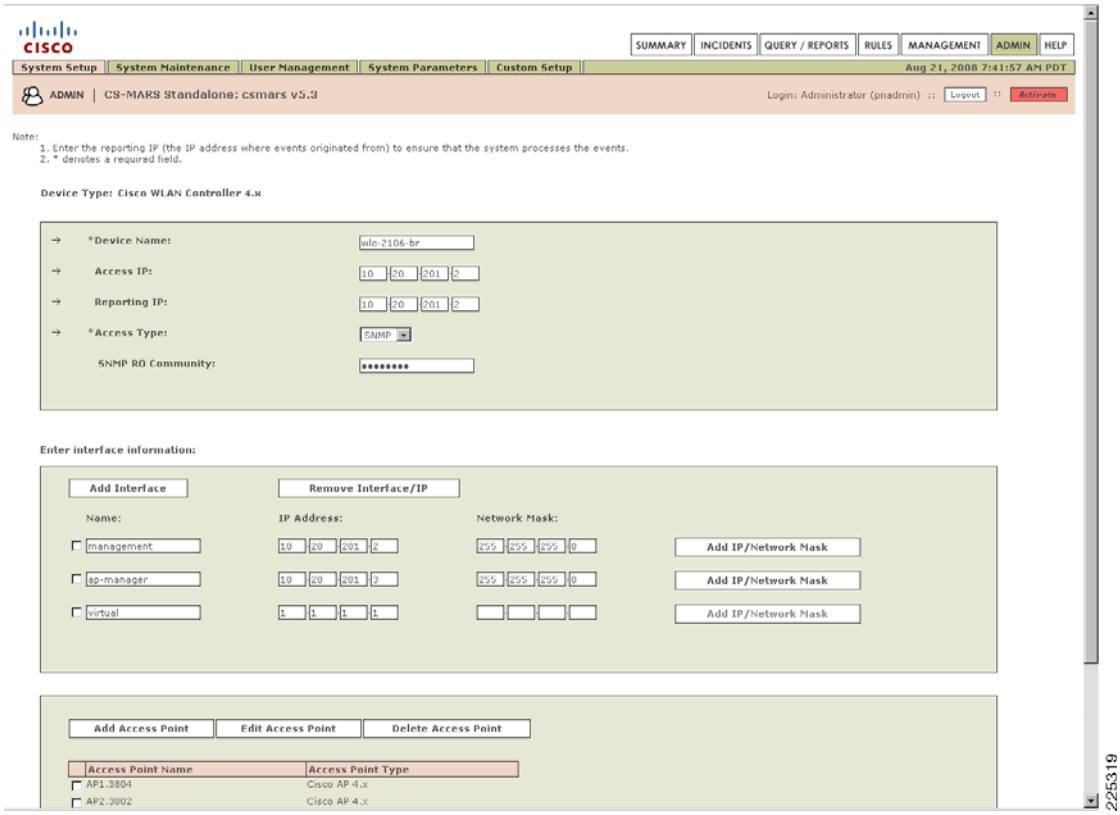
- WLC 管理インターフェイスを定義する必要があります。他のインターフェイスは、このデバイスの検出が成功すると自動的に追加されます。
- 検出に成功するには、WLC で SNMP v1 アクセスがすでに有効である必要があります（P.9-3 の「Cisco WLC の設定」を参照）。

WLC の検出に成功すると、他のインターフェイス、および現在アソシエートされているすべてのアクセス ポイントが検出され、CS-MARS のインターフェイスに読み込まれます（図 9-10 を参照）。

検出が成功しない場合は、次の点を確認してください。

- CS-MARS が WLC に ping を実行できる。
- WLC で SNMP v1 が有効になっている。
- CS-MARS で定義されている SNMP コミュニティ ストリングが、WLC で CS-MARS 用に定義されているものと一致する。
- WLC で CS-MARS 用の SNMP コミュニティ ストリングが有効になっている。
- CS-MARS の送信元 IP アドレスが、WLC で定義されているものと一致する。

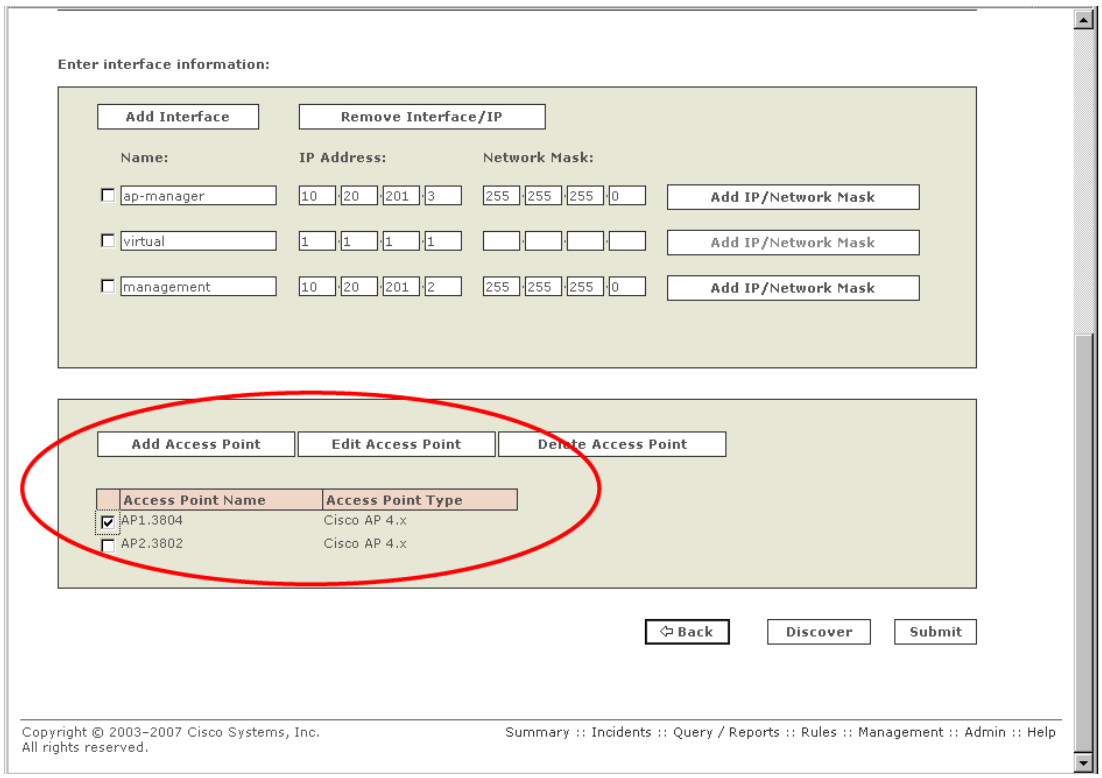
図 9-10　　CS-MARS での Cisco WLC の正常な検出



ステップ 5 Submit を選択し、**Activate** を選択して設定をアクティブにします。

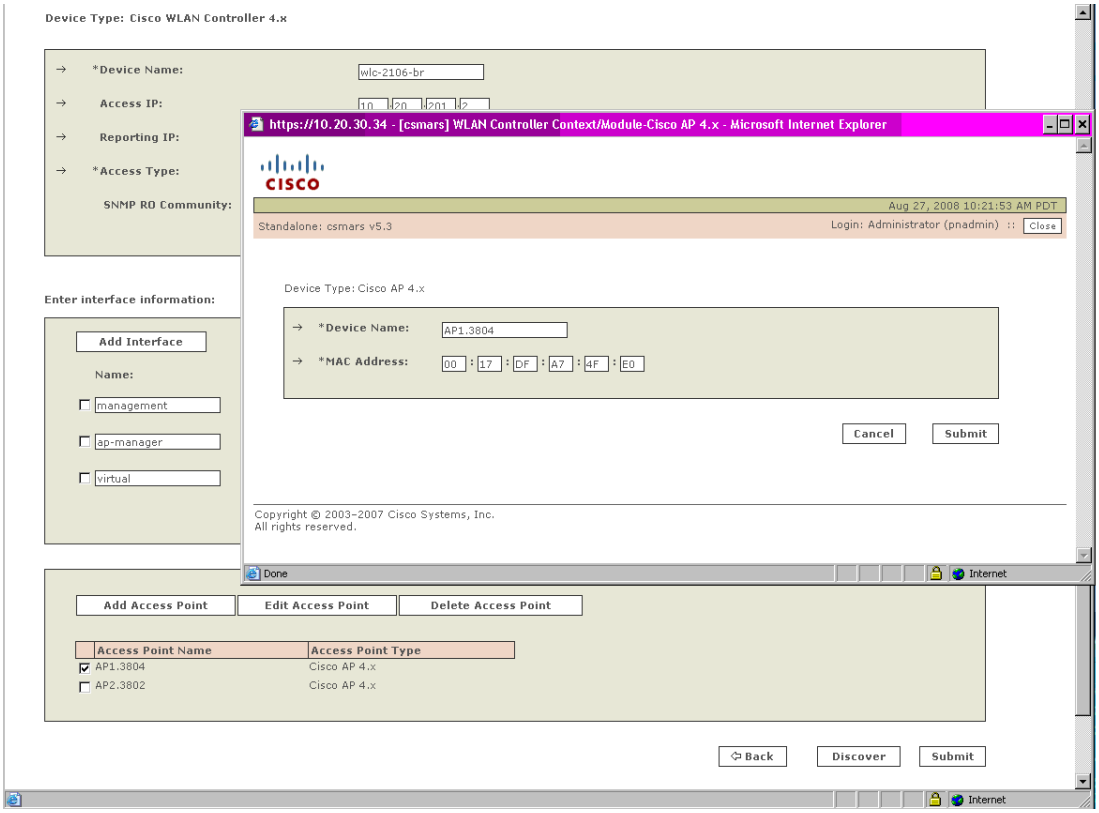
CS-MARS は、一般的な Access IP および Reporting IP ではなく、MAC アドレスに基づいて Access Point（AP; アクセス ポイント）を識別します。特定の AP の MAC アドレスを表示するには、WLC デバイス ページの下部までスクロールし、AP の名前の隣にあるボックスをオンにして、**Edit Access Point** をクリックします（図 9-12 を参照）。

図 9-11 CS-MARS での Cisco LWAPP アクセス ポイントの表示



その後、AP のデバイス名と MAC アドレスが表示されます（図 9-12 を参照）。

図 9-12　CS-MARS 上のデバイスとしての Cisco LWAPP アクセス ポイント



（注） 正確なイベント ロギングを有効にするには、アクセス ポイントの MAC アドレスが一意である必要があります。

CS-MARS が Cisco LWAPP AP からのイベントを解析する方法の詳細については、P.9-25 の「CS-MARS による WLAN AP イベントの解析」を参照してください。

Cisco Unified Wireless 用の CS-MARS 機能

この項では、Cisco Unified Wireless をサポートするための CS-MARS 機能について簡単に概説します。

CS-MARS の無線 LAN 機能の詳細については、『*CS-MARS User Guide*』を参照してください（P.9-27 の「参考資料」を参照）。

WLAN イベント

Cisco Unified Wireless デバイスに対する CS-MARS のサポートには、次のような WLAN イベントの可視性が含まれます。

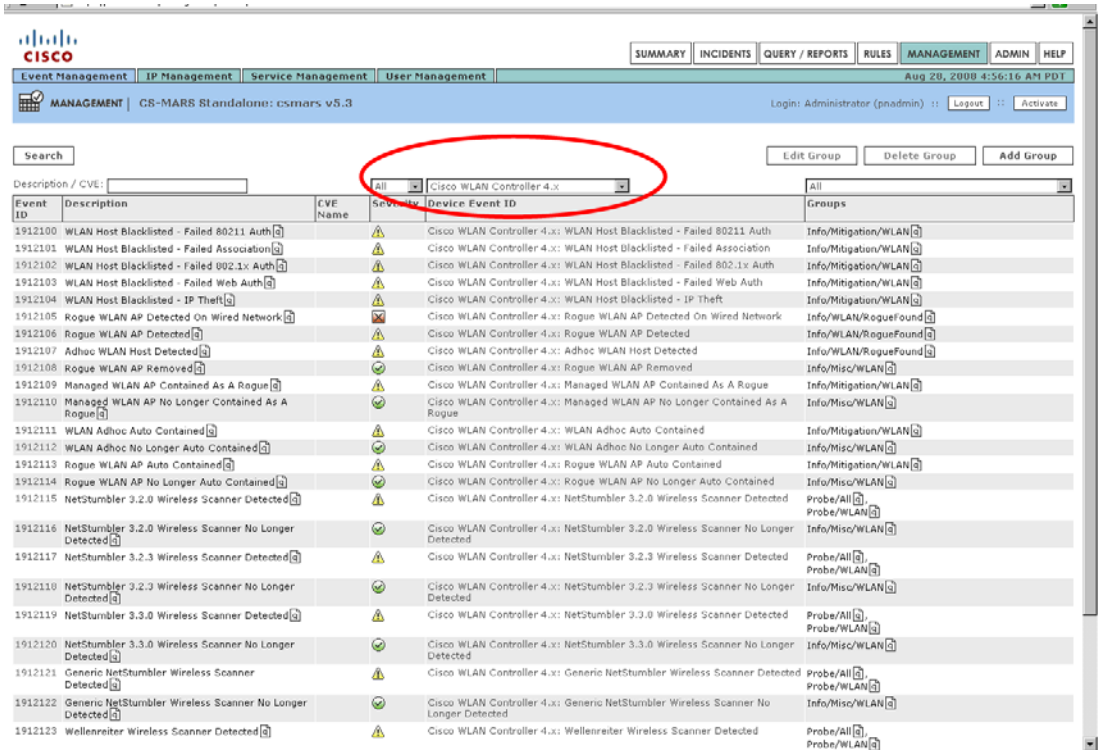
- WLAN DoS 攻撃
- 不正 AP
- 802.11 プローブ
- アドホック ネットワーク
- クライアント除外とブラックリスト
- WLAN の動作ステータス

CS-MARS によって解析されるすべての WLAN イベントを表示するには、次の手順を実行します。

ステップ 1 **MANAGEMENT -> Event Management** に移動します。

ステップ 2 プルダウン メニューから Cisco WLAN Controller 4.x を選択し、すべての WLC イベントを確認します（図 9-13 を参照）。

図 9-13　　CS-MARS WLAN イベントのサブセットの例



この画面には、CS-MARS がネイティブにサポートしている Cisco WLAN コントローラ関連のすべてのイベントが表示されます。

WLAN イベント関連のイベント グループ

CS-MARS は WLAN イベントの関連性を特定し、表 9-1 に示すような WLAN 固有のイベント グループおよび一般的なイベント グループにまとめます。

表 9-1　　イベント グループ

イベント グループのタイプ	イベント グループ
DoS	DoS/All
	DoS/Network/WLAN
情報	Info/High Usage/Network Device
	Info/Misc/WLAN
	Info/Mitigation/WLAN
	Info/WLAN/RogueFound

表 9-1 イベント グループ

イベント グループのタイプ	イベント グループ
動作	OperationalError/WLAN OperationalStatusChange/WLAN
ペネトレーション	Penetrate/All Penetrate/GuessPassword/All Penetrate/GuessPassword/System/Non-root Penetrate/SpoofIdentity/Misc

CS-MARS のクエリーおよびレポートで、イベント グループは「Event Type」として表示されます。

WLAN イベントに基づくルール

CS-MARS には、表 9-2 に示す WLAN 固有の検査ルールが用意されています。

表 9-2 WLAN イベントに基づくルール

CS-MARS のルール	CS-MARS のルール グループ
System Rule: Operational Issue: WLAN	System: Operational Issue
System Rule: Rogue WLAN AP Detected	System: Operational Issue
System Rule: WLAN DoS Attack Detected	System: Network Attacks and DoS

これらのルールはデフォルトで有効であり、既存のルール グループに統合されています。

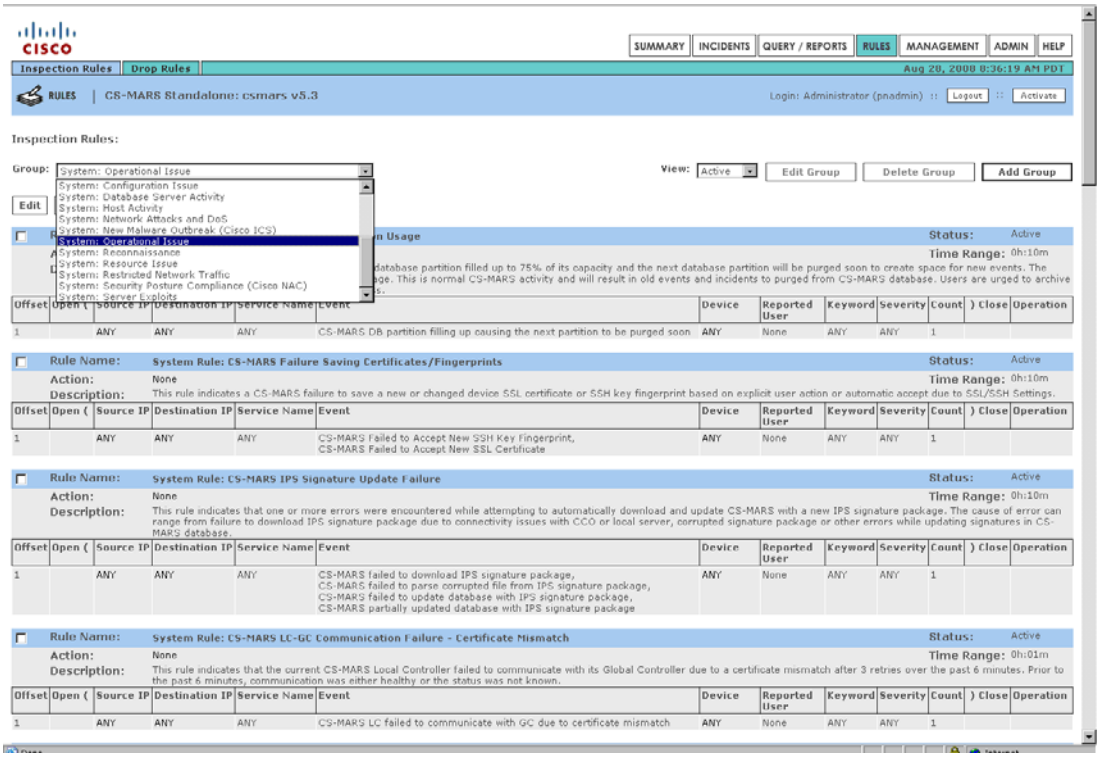
CS-MARS のルールの詳細を表示するには、次の手順を実行します。

ステップ 1 **RULES** に移動します。

ステップ 2 リストをスクロールダウンし、ルールを見つけます。

ルールが所属するルール グループがわかっている場合は、**Group** の隣にあるドロップダウン ボックスで適切なルール グループを選択することにより、リストをフィルタできます（図 9-14 を参照）。

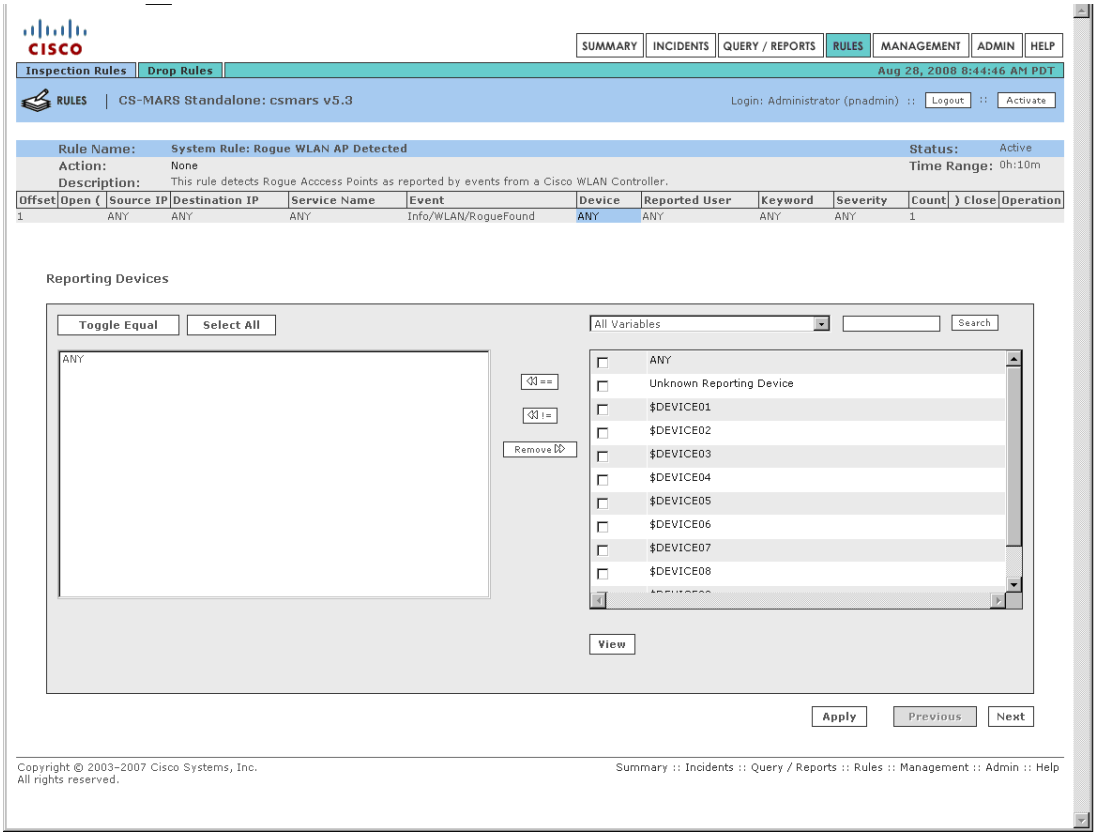
図 9-14　　ルール グループに基づく CS-MARS ルールの表示



特定のルールを選択して **Edit** をクリックすることで、そのルールの詳細を表示できます。

例として、図 9-15 に、ルール **System Rule: Rogue WLAN AP Detected** のデフォルトの詳細を示します。

図 9-15 CS-MARS のルール Rogue WLAN AP Detected



WLAN イベント関連のクエリーとレポート

CS-MARS には、次のような WLAN 固有のクエリーとレポートが用意されています。

- WLAN DoS Attacks Detected
- WLAN Probes Detected
- WLAN Rogue AP or Adhoc Hosts Detected
- WLAN Successful Mitigations

WLAN イベントは、必要に応じて、次のような既存のクエリーおよびレポートにも統合されています。

- Network Attacks and DoS
- Reconnaissance
- Operational Issue

WLAN イベントに関するクエリーの実行

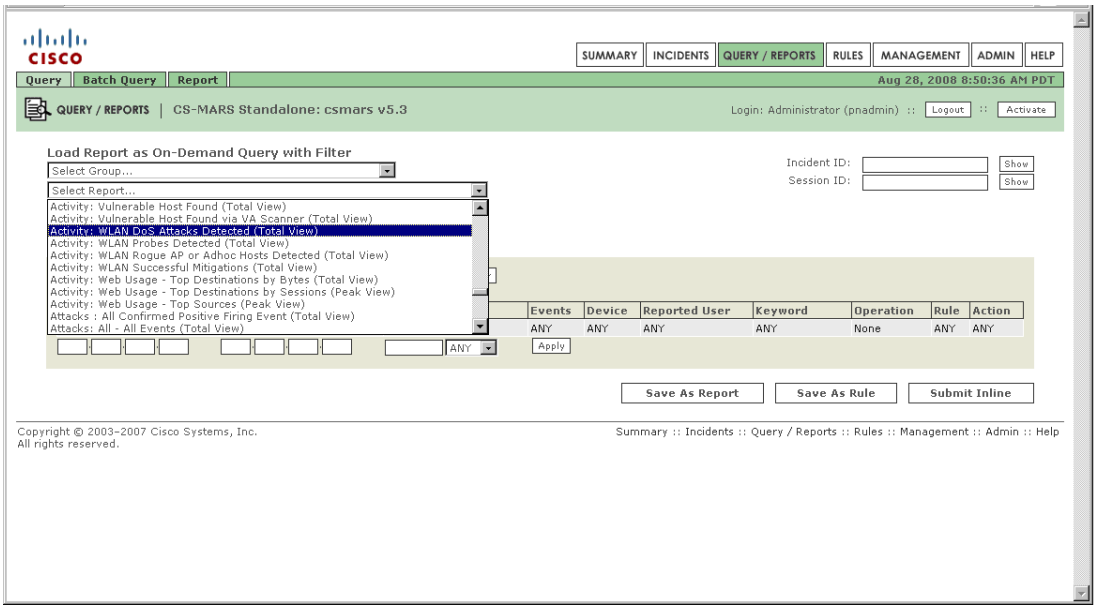
特定の WLAN 固有のイベントに関するクエリーを実行するには、次の手順を実行します。

ステップ 1　**QUERY/REPORTS** に移動します。

ステップ 2　**Select Report…** ドロップダウン ボックスから、必要な WLAN 固有のレポートを選択します。

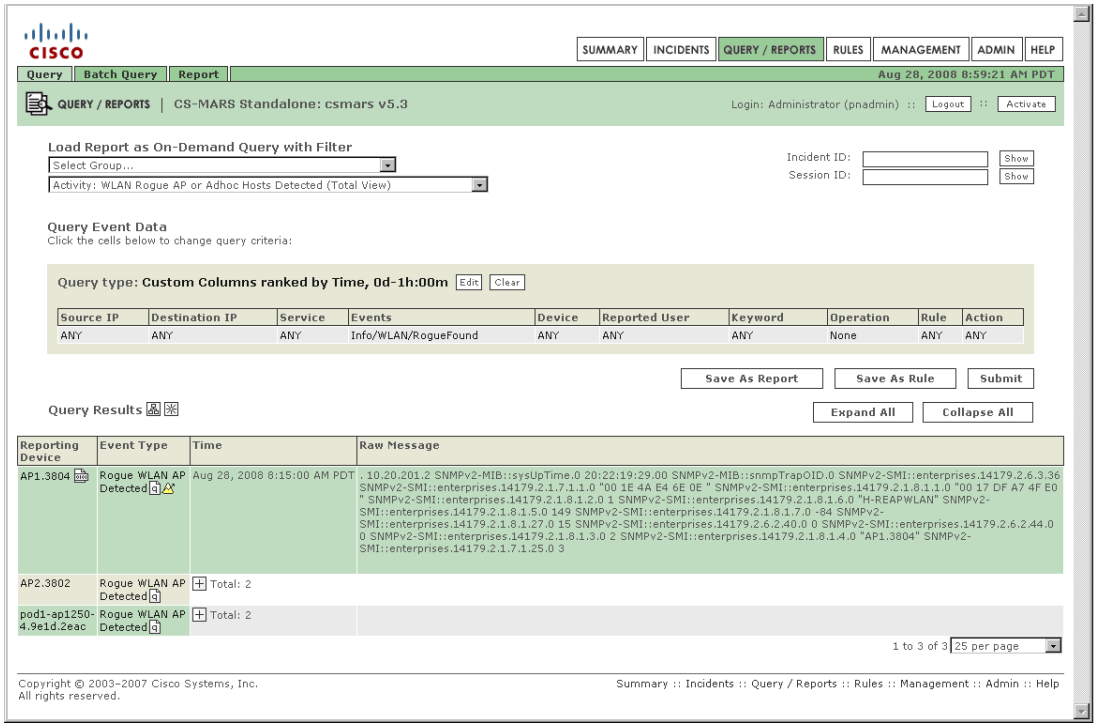
レポートが所属するレポート グループがわかっている場合は、**Select Group…** ドロップダウン ボックスで適切なレポート グループを選択することにより、リストをフィルタできます（図 9-16 を参照）。

図 9-16　CS-MARS の WLAN 固有のレポート



クエリーの期間が適切であることを確認し（ここでは、最後の 1 時間と表示）、**Submit Inline** をクリックします（図 9-17 を参照）。

図 9-17 CS-MARS の Rogue WLAN AP レポートの例



WLAN イベントに関するレポートの生成

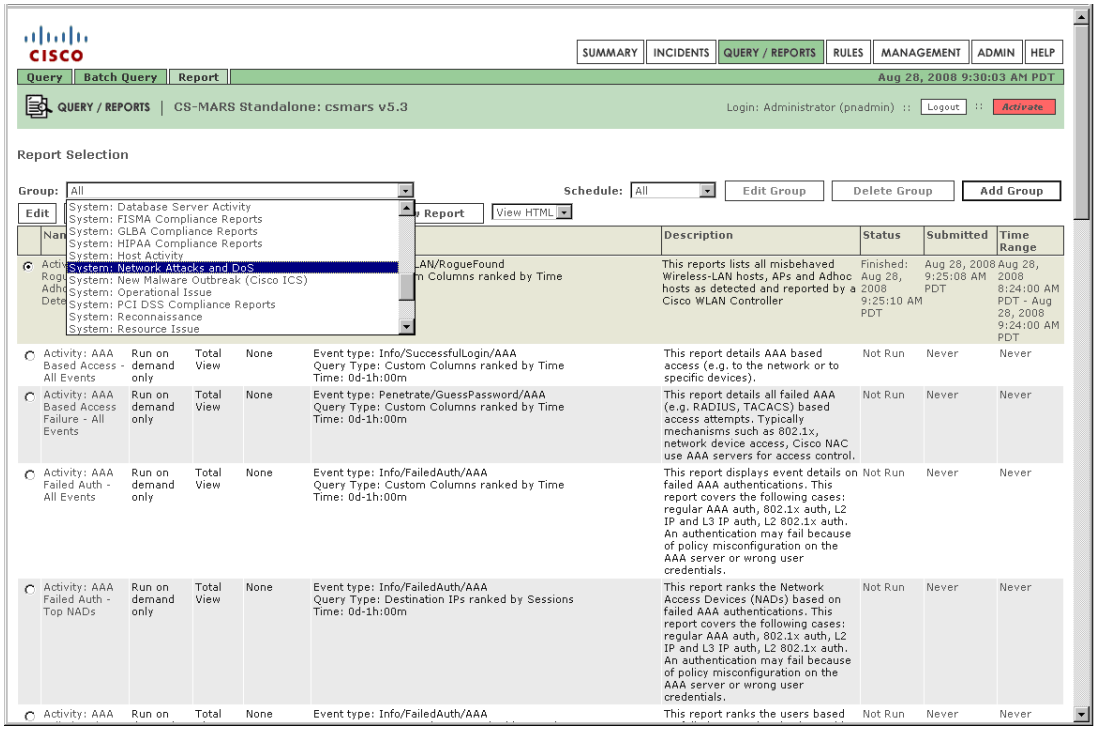
関連性を特定してイベント セットにまとめられたイベントを展開して、個々のイベントおよびそれに関連付けられている生メッセージを表示できます。

特定の WLAN 固有のイベントに関するレポートを生成するには、次の手順を実行します。

ステップ 1QUERY/REPORTS -> Report に移動します。

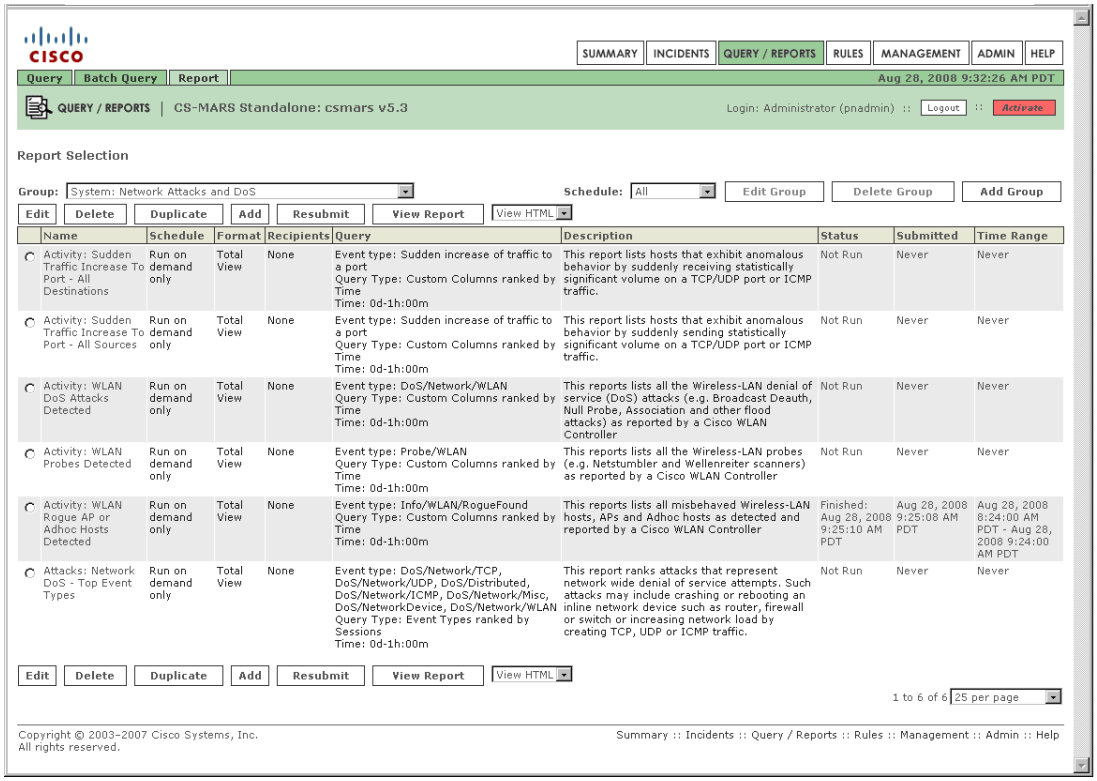
ステップ 2Group --Report Groups - ドロップダウン ボックスから、必要なレポート グループを選択します（図 9-18 を参照）。

図 9-18　　レポート グループ基づく CS-MARS レポートの選択



そのレポート グループ内で使用可能なレポートが表示されます（図 9-19 を参照）。

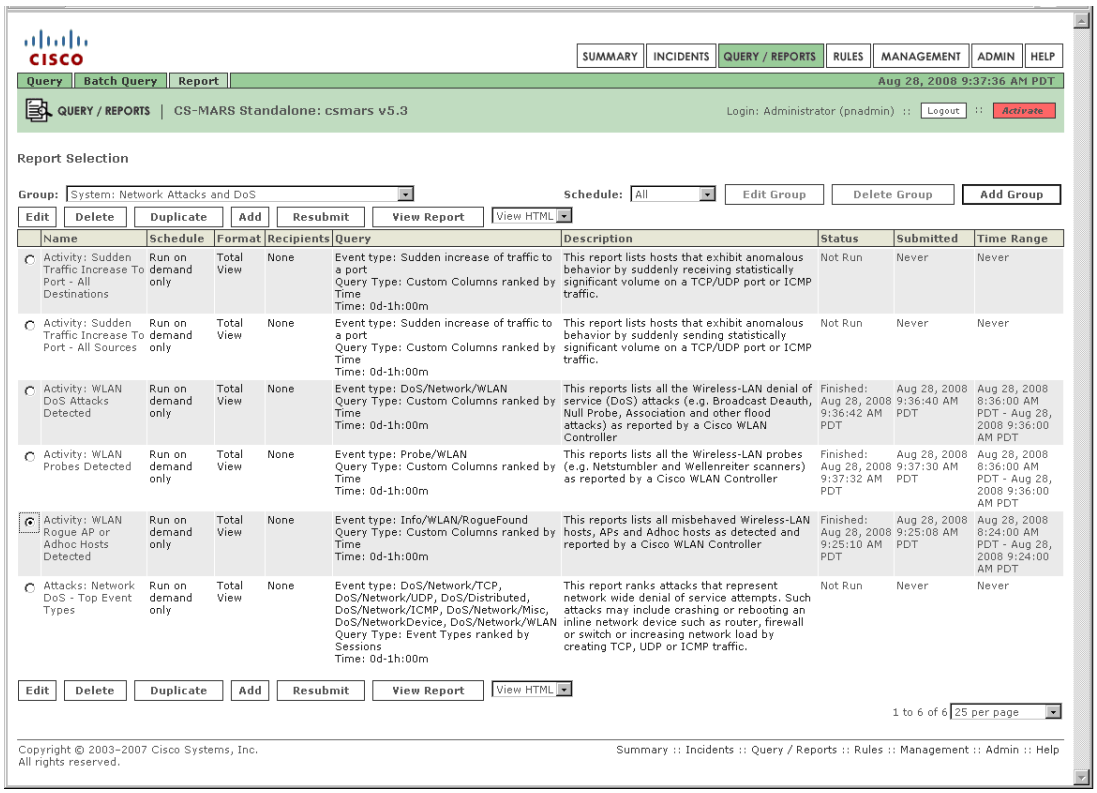
図 9-19 CS-MARS の Network Attacks and DoS レポート グループ



ステップ 3 必要なレポートを選択し、そのレポートが最近生成されていない場合は、**Resubmit** をクリックします。

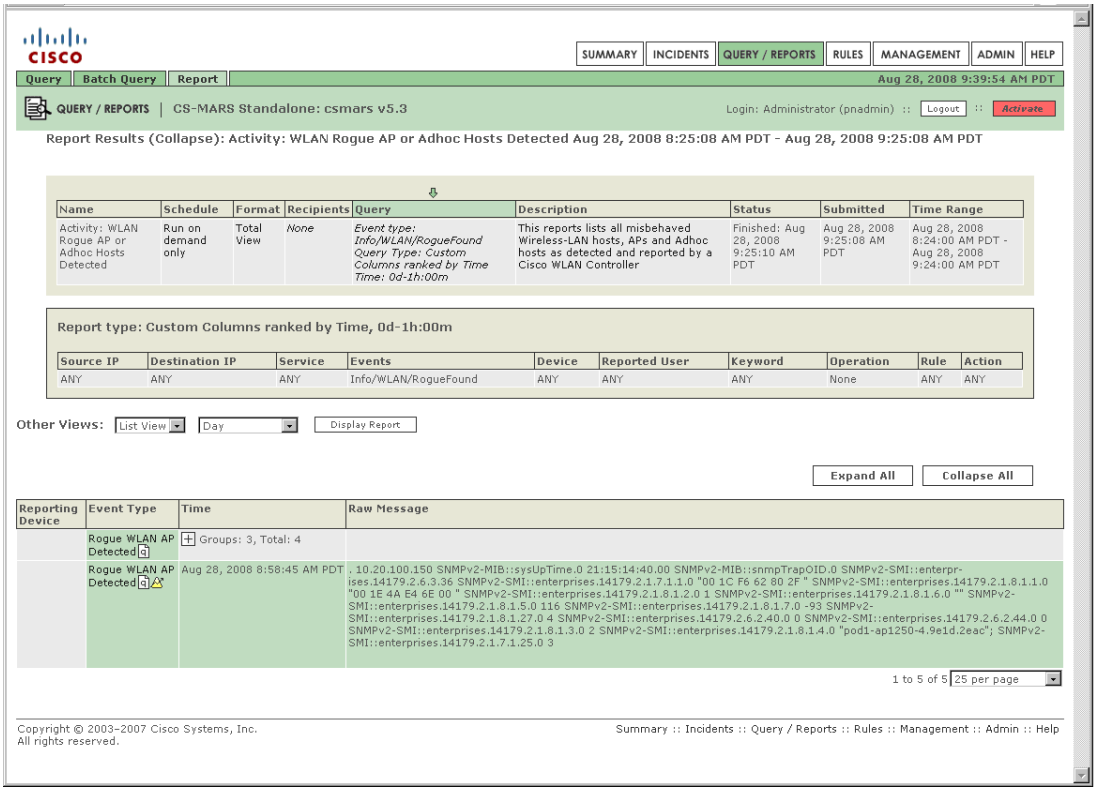
新しく生成されたレポートを表示するには、**View Report** をクリックします（図 9-20 を参照）。

図 9-20 CS-MARS のレポートの生成と表示



レポートが表示されます（図 9-21 を参照）。

図 9-21 CS-MARS の WLAN Rogue AP レポートの例



Cisco Unified Wireless 用の CS-MARS 統合に関する一般的なガイドライン

CS-MARS モニタリングを Cisco Unified Wireless Network にまで拡張するための一般的なガイドラインは、次のとおりです。

- Cisco Unified Wireless Network に対する CS-MARS のモニタリングを有効にして、ネットワークをまたがる可視性を提供します。
- アクセス ポイントの MAC アドレスが一意であることを確認します。
- 豊富にある WLAN イベントを使用するカスタム ルールを作成して、CS-MARS の機能をさらに拡張することを検討します。
- WLAN イベントの詳細な分析と調査には、WCS を使用します。

その他の情報

Cisco Unified Wireless 用の CS-MARS の運用上の考慮事項

この項では、CS-MARS のネットワークをまたがる異常検出と関連性の特定を Cisco Unified Wireless Network にまで拡張する場合の運用上の考慮事項を示します。

- Cisco Unified Wireless イベントのレポーティング デバイスは、イベントを生成した WLC または AP の名前です。
- 多くの場合、WLC および AP は、異常が発生しているデバイスの MAC アドレスに基づいて WLAN 異常を識別して報告するだけです。通常、送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルなどの関連情報は報告されません。この場合、CS-MARS は、送信元 IP アドレスと宛先 IP アドレスを 0.0.0.0、送信元ポートと宛先ポートを 0、プロトコルを N/A として、WLAN イベントを表示します。異常の発生源として識別されたデバイスの MAC アドレスは、生メッセージで参照できます。
- 現在、CS-MARS は、WLAN 異常が発生しているデバイスの MAC アドレスに基づいてイベントの分類も関連性の特定も行いません。WLAN 固有のイベントの詳細な異常検出および関連性の特定では、Cisco WLC および Wireless Control System（WCS）を利用して、CS-MARS で識別された異常をさらに詳しく調査できます。
- CS-MARS の false positive 調整は、送信元 IP アドレスまたは宛先 IP アドレスに基づいて行われます。不正 AP の報告など、多くの WLAN 異常にはクライアントの送信元 IP アドレスも宛先 IP アドレスも含まれないため、現在この調整を行うことはできません。ただし、Cisco Unified Wireless Release 5.0 では、不正デバイス分類用の拡張機能が導入されたため、この機能がインシデント調査に利用されます。この機能の詳細については、P.9-27 の「参考資料」を参照してください。
- カスタム パーサーでは、WLAN イベントに対する CS-MARS のネイティブ解析を拡張して、たとえば WLAN 異常の送信元 MAC アドレスを使用することができます。この CS-MARS 機能の詳細については、P.9-27 の「参考資料」を参照してください。
- 現在、CS-MARS は SNMP v1 だけをサポートしています。SNMP v1 は、コミュニティ ストリングを含め、すべてのデータをクリア テキストで伝送するため、スニフィングに対して脆弱です。お客様がセキュリティ ポリシーを確認し、SNMP v1 トランザクションを保護するために IPSec や Out-of-Band（OOB; アウトオブバンド）管理ネットワークなどの追加のセキュリティ技術が必要であるかどうかを判断することをお勧めします。一般的なベスト プラクティスとしては、わかりにくい強力なコミュニティ ストリングを使用する、デフォルトのコミュニティ ストリングを削除する、許可された発信元だけにアクセスを制限する、読み取り専用アクセスだけを許可するなどがあります。SNMP アクセスをセキュリティで保護する方法の詳細については、P.9-28 の「一般的なネットワーク セキュリティ」の「ネットワーク セキュリティ ベースライン」を参照してください。

CS-MARS による WLAN AP イベントの解析

CS-MARS が Cisco LWAPP アクセス ポイントからのイベントを検出して解析できるようにするには、まず Cisco WLC を CS-MARS のレポーティング デバイスとして定義する必要があります。Cisco WLC を CS-MARS のレポーティング デバイスとして定義するために必要な手順は、この章ですでに詳しく説明しました。

WLC は、WLC が監視する AP からイベントを受信し、そのイベントを SNMP トラップとして転送します。このトラップの送信元 IP アドレスは、常に WLC です。ただし、AP が元のイベントを生成した場合、AP の MAC アドレスが Object Identifier（OID; オブジェクト識別子）として SNMP トラップに埋め込まれています。

CS-MARS は、レポーティング デバイスを正確に識別するために、このような SNMP トラップを解析します。

CS-MARS が WLC から受信した SNMP トラップに、イベント発信元として AP の MAC アドレスが含まれている場合、イベントが解析される方法は、その MAC アドレスを持つ AP が CS-MARS にすでに定義されているかどうかによって異なります。

- AP の MAC アドレスが既知の場合、CS-MARS は AP のデバイス名をレポーティング デバイスとして表示します。
- AP の MAC アドレスが未知の場合、CS-MARS はこの最初のイベントをレポーティング デバイスとして WLC のデバイス名で表示し、この AP を自動的にトラップ送信元の WLC の子エージェントとして定義します。したがって、後続のイベントはレポーティング デバイスとして厳密にその AP に帰属します。これは、その AP がデバイスとして定義されており、MAC アドレスに基づく識別が可能であるためです。

新規、未定義、または以前に未検出の AP に対するこのような漸進的な自動検出により、手動で定義する必要がなくなります。

（注） アクセス ポイントの漸進的な自動検出を行うには、WLC で SNMPv1 読み取りアクセスが有効になっている必要があります。WLC の設定については、P.9-3 の「Cisco WLC の設定」を参照してください。

AP の MAC アドレスが未知であり、自動検出が失敗した場合、そのイベントは WLC に帰属します。

AP の MAC アドレス情報を含まない WLC SNMP トラップは、レポーティング デバイスとして WLC に帰属します。

Cisco Unified Wireless 用の CS-MARS 統合の依存関係

CS-MARS と Cisco WLC の統合は、表 9-3 に示すソフトウェア プラットフォームおよびハードウェア プラットフォームに依存します。

表 9-3 CS-MARS と Cisco WLC の統合の依存関係

コンポーネント	最小限のソフトウェア	その他の情報
CS-MARS	Release 5.3.2 以降	Release 6.0 は、Gen1 と Gen2 の両方のハードウェアをサポートします。 Release 5.3.2 は、Gen2 ハードウェア（110 および 210）だけをサポートします。
Cisco WLC	Cisco Unified Wireless Release 4.x 以降	LWAPP AP のみ
LWAPP AP		

テスト ベッドのハードウェアとソフトウェア

表 9-4 に示す CS-MARS と WLC のプラットフォームおよびソフトウェア リリースを使用して、統合テストが実施および検証されました。

表 9-4 テスト ベッドのハードウェアとソフトウェア

コンポーネント	ハードウェア	ソフトウェア
CS-MARS	MARS 210	5.3.5 (2934)
WLC	WLC 2106	5.0.148.2
	Cisco Catalyst 6500 シリーズ内の Wireless Services Module（WiSM）	5.0.148.2

参考資料

Cisco Unified Wireless

- シスコ無線製品

  http://www.cisco.com/en/US/products/hw/wireless/index.html

- Cisco Wireless Control System（WCS）

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

- 不正デバイスの管理

  Cisco Wireless LAN Controller Configuration Guide, Release 5.0
  http://www.cisco.com/en/US/docs/wireless/controller/5.0/configuration/guide/c5sol.html#wp1345692

CS-MARS

- CS-MARS

  http://www.cisco.com/en/US/products/ps6241/tsd_products_support_series_home.html

- 無線 LAN デバイスの設定

  User Guide for Cisco Security MARS Local Controller, Release 5.3.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgwlan.html

- カスタム デバイスの設定

  User Guide for Cisco Security MARS Local Controller, Release 5.3.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/cfgcustm.html

  User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x
  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/cfgCustm.html

一般的なネットワーク セキュリティ

- ネットワーク セキュリティ ベースライン
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.html

GLOSSARY

A

AAA Authentication、Authorization、Accounting（認証、認可、アカウンティング）

ACS Cisco Access Control Server

AES Advanced Encryption Standard（高度暗号化規格）

AP アクセス ポイント

B

BSSID Basic Service Set Identifier（基本サービス セット識別子）

C

CAM Clean Access Manager

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CCX Cisco Compatible Extensions

CSA Cisco Security Agent

CSSC Cisco Secure Services Client

D

DoS Denial Of Service（サービス拒絶）

E

EAP Extensible Authentication Protocol（拡張認証プロトコル）

EAP-FAST EAP-Flexible Authentication via Secured Tunnel

EAP-TLS EAP-Transport Layer Security

F

FWSM Firewall Services Module（ファイアウォール サービス モジュール）

I

IDS Intrusion Detection System（侵入検知システム）

IPS Intrusion Prevention System（侵入防御システム）

L

LAP LWAPP アクセス ポイント

LWAPP Lightweight Access Point Protocol（Lightweight アクセス ポイント プロトコル）

M

MAP メッシュ AP

MFP Management Frame Protection（管理フレーム保護）

MIC Message Integrity Check（メッセージ完全性チェック）

N

NAC Network Admission Control（ネットワーク アドミッション制御）

P

PEAP GTC Protected EAP Generic Token Card

PEAP MSCHAP Protected EAP Microsoft Challenge Handshake Authentication Protocol

PKI Public Key Infrastructure（公開鍵インフラストラクチャ）

R

RADIUS Remote Authentication Dial-In User Service

RF 無線周波

RLDP	Rogue Location Discovery Protocol（不正ロケーション検出プロトコル）
RSSI	Received Signal Strength Indication（受信信号強度表示）

S

SNR	Signal-to-Noise Ratio（信号対雑音比）
SSID	IEEE Extended Service Set Identifier（IEEE 拡張サービス セット識別子）
SSO	Single Sign-On（シングル サインオン）
SVI	Switched Virtual Interface（スイッチ仮想インターフェイス）

T

TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

W

WCS	Wireless Control System
WEP	Wired Equivalent Privacy
Wi-Fi	Wi-Fi Alliance のブランド。製品とサービスの相互運用性を IEEE 802.11 テクノロジーに基づいて認定
WiSM	Wireless Services Module
WLAN	無線 LAN
WLC	Wireless LAN Controller
WLCM	Wireless LAN Controller Module
WLSM	Wireless LAN Services Module
WMM	Wi-Fi Multimedia（Wi-Fi マルチメディア）
WPA	Wi-Fi Protected Access