Cisco Adaptive wIPS リリース 8.0 管理導入ガイド

初版:2008 年 11 月
最終更新日:2017 年 3 月

Cisco ワイヤレス IPS ソリューションの概要

Cisco ワイヤレス IPS ソリューションは、お客様のそれぞれのニーズに応じて、柔軟でスケーラブルなワイヤレス セキュリティ ソリューションを 24 時間 365 日フルタイムで提供します。このドキュメントでは、シスコ ユニファイド ワイヤレス ソリューションの一部として提供されるワイヤレス IPS セキュリティ ソリューションについて説明します。導入形式に応じて、基本となるワイヤレス LAN コントローラ(WLC)を始めとして、WLC と MSE や、WLC、MSE、および CleanAir 対応アクセス ポイントなど、セキュリティのニーズに合わせたソリューションを利用できます。以下で、これら 3 つのソリューションを比較します。

有線ネットワーク攻撃

ワイヤレス IPS 最適化モードのアクセス ポイントは、現在の Cisco Unified Wireless Network 実装と同じロジックを使用して、不正脅威の査定と緩和を行います。これにより、ワイヤレス IPS アクセス ポイントは、不正アクセス ポイントおよびアドホック ネットワークをスキャンし、検出して、封じ込めることができます。不正ワイヤレス デバイスに関するこの情報が発見されると、不正アラーム集約が行われる PI に報告されます。ただし、この機能を使用すると、ワイヤレス IPS モード アクセス ポイントを使用して、攻撃封じ込めが起動された場合、封じ込めの間、系統的な攻撃を狙いとしたチャネル スキャンを実行する機能が中断されます。

機能	BaseWIPS（WLC）	Adaptive WIPS (WLC および MSE)	Adaptive WIPS（WLC、MSE、および CleanAir 対応アクセス ポイント）
不正アクセス ポイントとアドホック不正の検出、分類、ロケーション トラッキング、封じ込め	○	○	○
不正アクセス ポイントの接続先スイッチ ポートのトレースと無効化	○	○	○
管理フレームの偽装検出	○	○	○
WAN のダウン時に不正を封じ込め	○	○	○
内部および外部不正アクセス ポイントの検出と封じ込め時間	○	○	○

Over-the-Air 攻撃

Cisco 適応型ワイヤレス IPS は、強力なワイヤレスの脅威の検出および緩和の機能をワイヤレス ネットワーク インフラストラクチャに組み込むことで、業界で最も包括的で正確な運用効率の高いワイヤレス セキュリティ ソリューションを実現します。Cisco 適応型ワイヤレス IPS ソリューションによって検出される Over-the-Air 攻撃を以下に示します。

機能	BaseWIPS（WLC）	Adaptive WIPS (WLC および MSE)	Adaptive WIPS（WLC、MSE、および CleanAir 対応アクセス ポイント）
スマートフォン テザリングの検出と封じ込め	○	○	○
DoS 攻撃者と、内部アクセス ポイントに関連付けようとしている非認定デバイスのロケーション トラッキングと封じ込め	○	○	○
Wired Equivalent Privacy（WEP）のクラッキング検出	○	○	○
MAC スプーフィング不正の検出と封じ込め	○	○	○
自動 MAC ラーニング	○	○	○
インターネット接続共有（ICS）の検出	○	○	○
企業レベルのアラーム/イベントの相関付け	○	○	○
攻撃シグネチャのしきい値のカスタマイズ	○	○	○
インフラストラクチャに統合された、オフチャネルの不正検出とロケーション	○	○	○
DoS シグネチャの更新	×	○	○
ワイヤレス侵入シグニチャの更新	×	○	○
攻撃フォレンジック（すべてのシグニチャ）	×	○	○

802.11 以外の脅威

Cisco CleanAir® テクノロジーは、ネットワークの RF 状態をモニタおよび管理する有効なツールです。Cisco MSE はこれらの機能を拡張します。以下の図は、Cisco 適応型ワイヤレス IPS ソリューションに CleanAir 対応のアクセス ポイントを導入する利点を示しています。

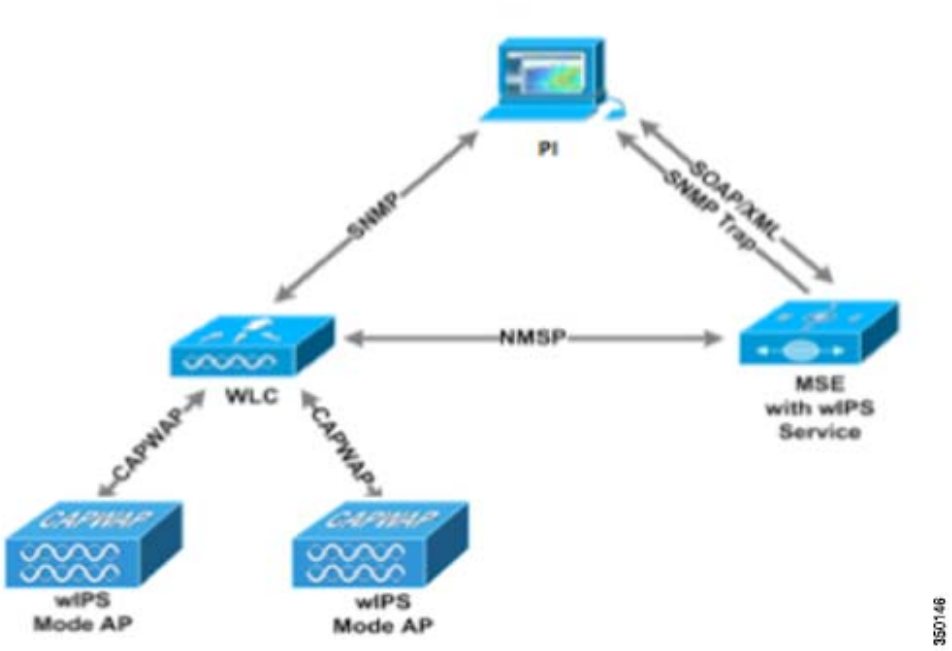
機能	BaseWIPS（WLC）	Adaptive WIPS (WLC および MSE)	Adaptive WIPS（WLC、MSE、および CleanAir 対応アクセス ポイント）
非 Wi-fi トランスミッタの検出とロケーション	×	×	○
非 Wi-fi ブリッジの検出とロケーション	×	×	○
非 Wi-fi アクセス ポイントの検出とロケーション	×	×	○
レイヤ 1 DoS 攻撃のロケーションと検出	×	×	○

Cisco 適応型ワイヤレス IPS の概要

概要には完全な Cisco ワイヤレス IPS ソリューションが含まれていますが、このドキュメントでは ワイヤレス IPS の Over-the-Air 攻撃の検出のすべての側面に焦点を当てます。このドキュメントでは以下の詳細を説明します。

- 適応型ワイヤレス IPS のコンポーネント/アーキテクチャ
- ワイヤレス IPS の導入モード
- wIPS スキャンのオフ チャネルとオン チャネルの比較
- ワイヤレス IPS 通信プロトコル
- ワイヤレス IPS 設定およびプロファイル管理
- ワイヤレス IPS アラーム フロー
- 構成の考慮事項
- フォレンジック
- ライセンシングとサポート
- 手順を追った設定ガイド

Cisco 適応型ワイヤレス IPS システムのアーキテクチャ



このドキュメントでは、Over-the-Air 攻撃に向けたワイヤレス IPS ソリューションを紹介します。Cisco 適応型 ワイヤレス Intrusion Prevention System（wIPS）は、連携して統合セキュリティ モニタリング ソリューションを提供する多数のコンポーネントから構成されています。現在 Cisco Unified Wireless Network ソリューションを構成する WLAN コントローラ、アクセス ポイント、およびプライム インフラストラクチャ コンポーネント に加え、wIPS では 2 つの追加のコンポーネントが導入されています。これらの追加のハードウェア コンポーネントには、wIPS モードのアクセス ポイントおよびワイヤレス IPS サービス ソフトウェアを実行する Mobility Services Engine があります。

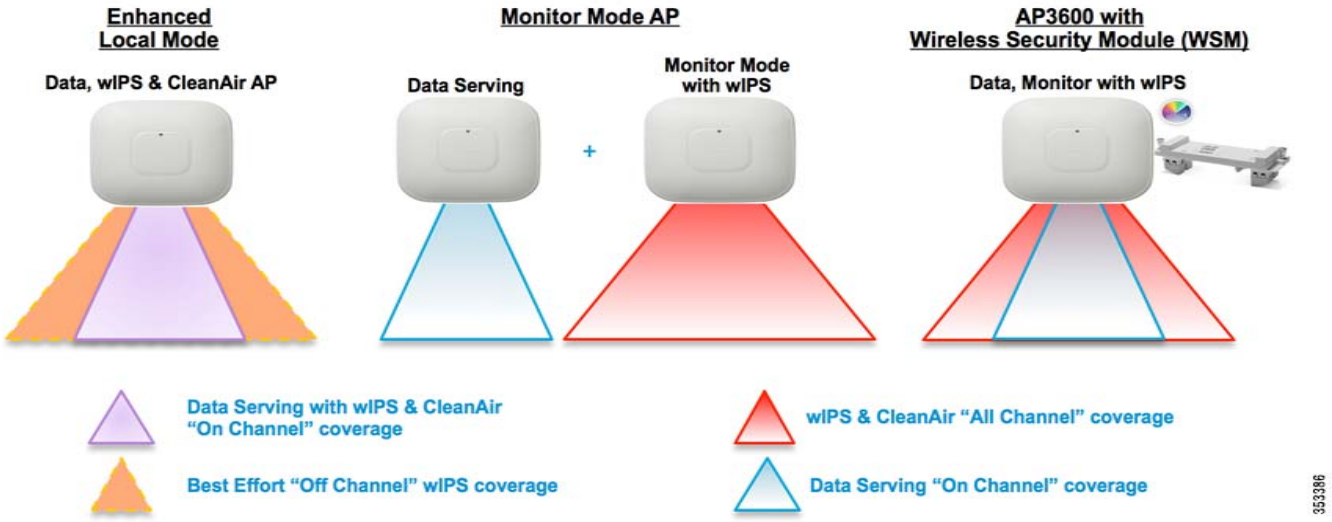
Adaptive ワイヤレス IPS の導入でのコンポーネントの機能

- ワイヤレス IPS モード アクセス ポイント：ワイヤレス IPS モード アクセス ポイントは、モニタ モード、ワイヤレス IPS または WSM モジュールを使用したアクセス ポイントです。この用語は、ワイヤレス IPS 対応のアクセス ポイントをグループ化するために使用されます。
- ワイヤレス IPS モニタ モード アクセス ポイント：定期的なチャネル スキャンと攻撃検出およびフォレンジック（パケット キャプチャ）機能を提供します。
- ローカル モード アクセス ポイント：タイムスライス型不正スキャンに加え、ワイヤレス サービスをクライアントに提供します。
- ワイヤレス IPS を使用したローカル モードのアクセス ポイント：ローカル モードと同様にクライアントにワイヤレス サービスを提供しますが、オフチャネルでスキャンする場合は無線がチャネル上に長時間とどまるため、攻撃検出を強化できます。
- ワイヤレス セキュリティ モジュール（WSM）：Cisco Aironet 3600/3700 シリーズのアクセス ポイントのアドオンで、継続的なスキャンと攻撃の検出および分析機能をモジュールにオフロードすることで、クライアントに向けた無線を解放します。

- Mobility Services Engine（ワイヤレス IPS サービスを実行）：すべてのコントローラとそれらの各ワイヤレス IPS モニタ モード アクセス ポイントからのアラーム集約の中央ポイントです。アラーム情報とフォレンジック ファイルはアーカイブ目的でシステムに保存されます。
- ワイヤレス LAN コントローラ：ワイヤレス IPS モニタ モード アクセス ポイントからの攻撃情報を MSE に転送し、AP に設定パラメータを配布します。
- プライム インフラストラクチャ：管理者が MSE でワイヤレス IPS サービスを設定し、ワイヤレス IPS 設定をコントローラに適用して、アクセス ポイントをワイヤレス IPS モニタ モードに設定する手段を提供します。また、ワイヤレス IPS アラームの表示、フォレンジック、レポート、および attack encyclopedia（攻撃百科事典）のアクセスにも使用します。

wIPS 導入モード

7.4 リリース以降、Cisco 適応型ワイヤレス IPS には ワイヤレス IPS モード アクセス ポイントの 3 つのオプションがあります。ワイヤレス IPS モード アクセス ポイントの違いを詳細に理解するために、各モードについて説明します。



wIPS を使用するローカル モード

wIPS を使用したローカル モードでは、「オンチャネル」での wIPS 検出が可能です。それにより、攻撃者がクライアント用のチャネルで検出されます。他のすべてのチャネルでは、ELM がベストエフォート型の wIPS 検出を提供します。ベストエフォートでの検出では、フレームごとに無線が短時間「オフチャネル」になります。「オフチャネル」の場合、そのチャネルをスキャン中に攻撃が行われると、攻撃が検出されます。

AP3600 の wIPS を使用するローカル モードの例では、2.4 GHz の無線がチャネル 6 で動作しています。AP は継続的にチャネル 6 をモニタし、チャネル 6 の攻撃はすべて検出および報告されます。AP がチャネル 11 を「オフチャネル」でスキャンしている間に攻撃者がチャネル 11 を攻撃すると、攻撃が検出されます。

ELM の機能は次のとおりです。

- チャネル スキャン（2.4 GHz および 5 GHz）に 24 時間 365 日の wIPS セキュリティ スキャンを追加し、ベスト エフォート型のオフチャネル サポートを提供します。
- アクセス ポイントはクライアントに追加サービスを提供し、G2 シリーズのアクセス ポイントではチャネル（2.4 GHz および 5 GHz）に対する CleanAir スペクトラム解析も実行します。

- データを提供するローカルおよび FlexConnect AP での適応型ワイヤレス IPS スキャン
- 個別のオーバーレイ ネットワークを必要としない保護
- ワイヤレス LAN の PCI コンプライアンスをサポート
- フル 802.11 および 802.11 以外の攻撃を検出
- 調査およびレポート機能を追加
- 統合または専用 MM AP を柔軟に設定可能
- AP での事前処理によってデータ バックホールを最小化（つまり、非常に低い帯域幅のリンクでも機能します）
- データ提供への影響を縮小

モニタ モード

モニタ モードでは、「オフチャネル」のワイヤレス IPS 検出が実行されます。アクセス ポイントが各チャネルに長時間留まることによって、すべてのチャネルの攻撃を検出できます。2.4 GHz 無線はすべての 2.4 GHz チャネルをスキャンし、5 GHz チャネルはすべての 5 GHz チャネルをスキャンします。追加のアクセス ポイントをクライアント アクセスのためにインストールする必要があります。

モニタ モード機能の一部は次のとおりです。

- モニタ モード アクセス ポイント（MMAP）はモニタ モード専用で動作し、全チャネル（2.4 GHz および 5 GHz）に対するワイヤレス IPS セキュリティ スキャンを追加できます。
- G2 シリーズのアクセス ポイントでは、全チャネル（2.4 GHz および 5 GHz）で CleanAir スペクトル分析を実行可能です。
- MMAP はクライアントにサービスを提供しません。

ワイヤレス セキュリティ モジュール（WSM）を備えた AP 3600/3700：ワイヤレス セキュリティおよびスペクトラムの進化

WSM モジュールを搭載した Cisco 3600 シリーズ アクセス ポイントは、「オンチャネル」と「オフチャネル」の組み合わせを使用します。これは、AP3600（2.4 GHz および 5 GHz）がクライアントにサービスを提供しているチャネルをスキャンし、WSM モジュールがモニタ モードで動作してすべてのチャネルをスキャンすることを意味します。

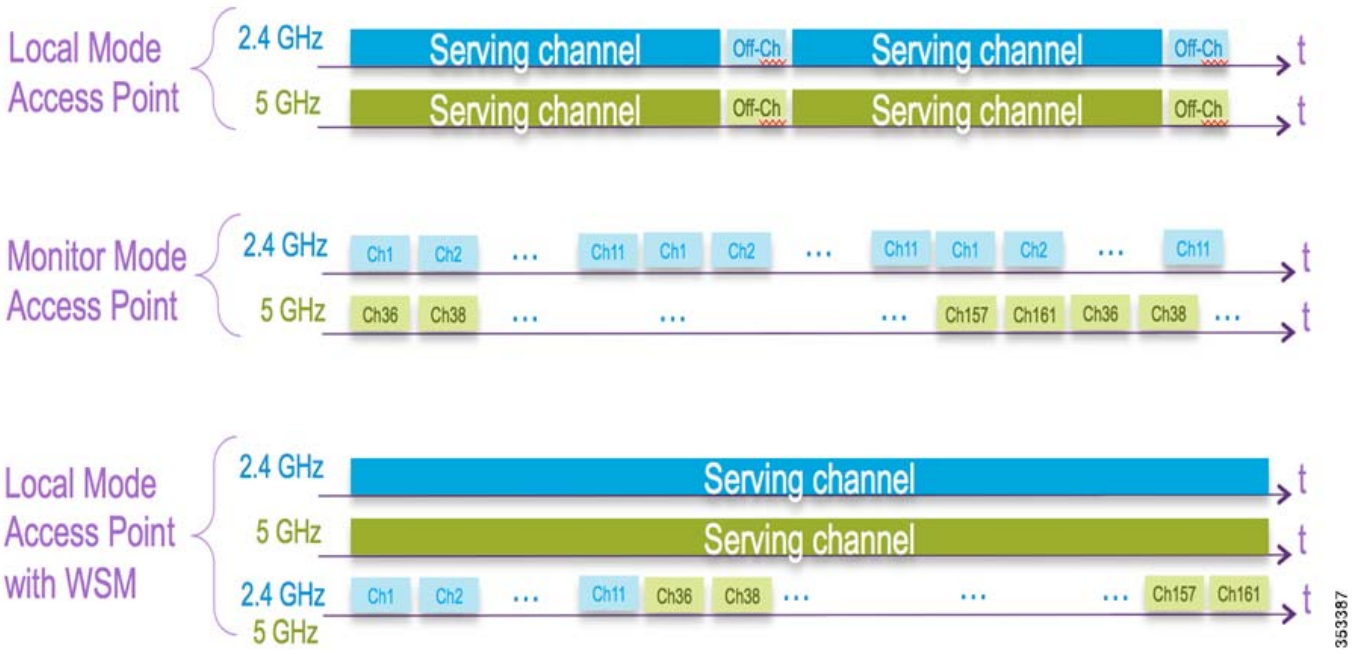
WSM モジュールの機能の一部は次のとおりです。

- クライアントへのサービス提供、ワイヤレス IPS セキュリティ スキャン、CleanAir テクノロジーを使用したスペクトル分析を兼ね備えた業界初のアクセス ポイントです。
- 独自アンテナで 2.4 GHz および 5 GHz の専用無線を提供し、両帯域の全ワイヤレス チャネルに対する 24 時間 365 日のスキャンを実施します。
- 単一のイーサネット インフラストラクチャにより、管理するデバイスを少なくして運用を簡素化し、AP3600 無線インフラストラクチャおよびイーサネット有線インフラストラクチャへの投資回収率を最適化します。

wIPS モードによるスキャンのオン チャネルとオフ チャネルの比較

次の図は、無線の動作を示しています。無線がそのサービス チャネル上にある場合は「オンチャネル」と見なされ、他のチャネルをスキャンしている場合は「オフチャネル」と見なされます。

ローカル モードの AP は通常は「オンチャネル」であるため、「オフチャネル」で攻撃を検出することは困難です。モニタ モードの AP は常に「オフチャネル」ですが、クライアントにサービスを提供できません。WSM モジュールは両方の長所を兼ね備えています。



ワイヤレス IPS 通信プロトコル

各システム コンポーネント間の通信を行うため、多くのプロトコルが使われています。

- CAPWAP（Control and Provisioning of Wireless Access Points）：このプロトコルは、アクセス ポイントとコントローラ間の通信に使用されます。これは、アラーム情報をコントローラに行き来させ、設定情報をアクセス ポイントに適用する双方向トンネルを提供します。CAPWAP 制御メッセージは DTLS で暗号化され、CAPWAP データには DTLS による暗号化のオプションがあります。
- NMSP（Network Mobility Services Protocol）：ワイヤレス LAN コントローラと Mobility Services Engine 間の通信に使われるプロトコル。ワイヤレス IPS 構成の場合、このプロトコルは、アラーム情報をコントローラから MSE へ集約し、ワイヤレス IPS 設定情報をコントローラに適用する経路を提供します。このプロトコルは暗号化されます。
  - コントローラ TCP ポート：16113
- SOAP/XML（Simple Object Access Protocol）：MSE とPI 間の通信方式です。このプロトコルは、MSE で実行するワイヤレス IPS サービスに設定パラメータを配布するために使用します。
  - oMSE TCP ポート：443
- SNMP（Simple Network Management Protocol）：このプロトコルは、Mobility Services Engine からプライム インフラストラクチャにワイヤレス IPS アラーム情報を転送するために使用されます。さらに、ワイヤレス LAN コントローラから Prime Infrastructure に不正アクセス ポイント情報を伝えるためにも使われます。

ワイヤレス IPS 設定およびプロファイル管理

ワイヤレス IPS プロファイルの設定は、プロファイルの表示と変更に使用される PI から始まるチェーン階層を進みます。実際のプロファイルは、MSE で実行するワイヤレス IPS サービス内に保存されます。プロファイルは、MSE 上のワイヤレス IPS サービスから、特定のコントローラに伝播され、次に、その目的のコントローラに関連付けられているワイヤレス IPS モード アクセス ポイントに透過的にこのプロファイルが伝達されます。PI でワイヤレス IPS プロファイルへの設定の変更が行われ、一連の Mobility Services Engine およびコントローラに適用される場合、変更を導入するために次の手順が実行されます。

1. PI で設定プロファイルが変更され、バージョン情報が更新されます。
2. XML ベースのプロファイルが MSE で実行するワイヤレス IPS エンジンに適用されます。この更新は、SOAP/XML プロトコルによって行われます。
3. MSE 上のワイヤレス IPS エンジンは、NMSP を使用して設定プロファイルを適用することによって、そのプロファイルに関連付けられている各コントローラを更新します。

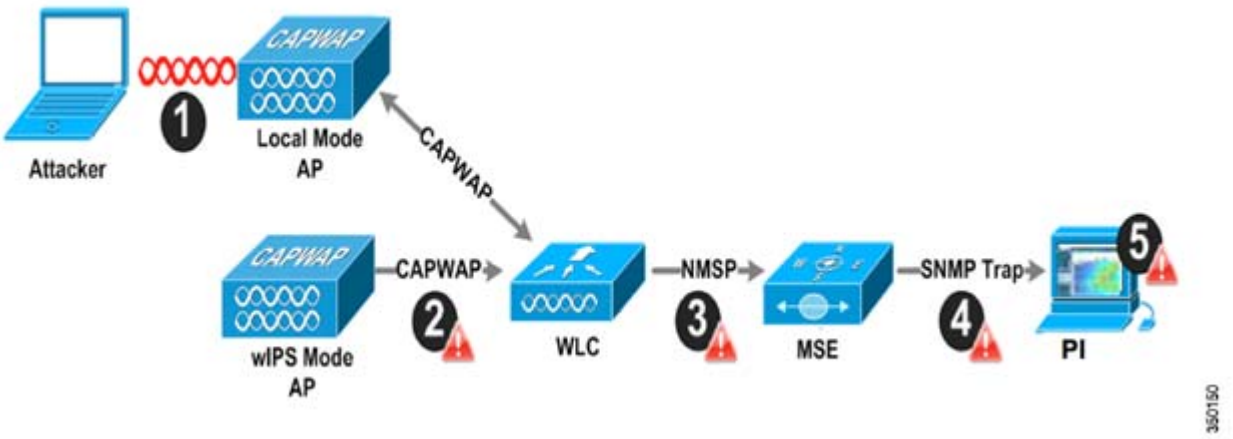
（注）　コントローラは、1 つの設定プロファイルに関連付けられています。設定プロファイルは、コントローラに参加しているすべてのワイヤレス IPS モード アクセス ポイントに対して使用されます。そのため、そのコントローラに接続されているすべてのワイヤレス IPS モード AP は、同じワイヤレス IPS 設定を共有します。

4. ワイヤレス LAN コントローラは更新されたワイヤレス IPS プロファイルを受け取り、それを NVRAM に保存し（以前のすべてのバージョンのプロファイルを置き換える）、CAPWAP 制御メッセージを使用して、更新されたプロファイルをそれに関連付けられたワイヤレス IPS アクセス ポイントに伝播します。
5. ワイヤレス IPS モード アクセス ポイントはコントローラから更新されたプロファイルを受け取り、そのワイヤレス IPS ソフトウェア エンジンに変更を適用します。

Mobility Services Engine は 1 つの Prime Infrastructure からのみ設定できることに注意してください。これは必然的に 1 対 1 の関係になります。つまり、Mobility Services Engine は一度特定の PI に関連付けられたら、別の PI に追加できません。

ワイヤレス IPS アラーム フロー

Adaptive wIPS システムは、通信のリニア チェーンに従って、エアウェーブのスキャンから取得した攻撃情報を Prime Infrastructure のコンソールに伝播します。



1. Cisco 適応型ワイヤレス IPS システムでアラームをトリガーさせるためには、正規のアクセス ポイントまたはクライアントに対して攻撃が仕掛けられる必要があります。正規のアクセス ポイントおよびクライアントは、同じ「RF グループ」名をブロードキャストしているデバイスを「信頼」することによって、Cisco Unified Wireless Network 内で自動的に検出されます。この設定では、ローカルモード アクセス ポイントとそれらに関連付けられたクライアントのリストが動的に管理されます。SSID グループ機能を使用して、SSID によってデバイスを「信頼する」ようにシステムを設定することもできます。WLAN インフラストラクチャに害を及ぼすと見なされた攻撃だけが残りのシステムに伝播されます。
2. ワイヤレス IPS モード アクセス ポイント エンジンによって攻撃が識別されると、アラームの更新がワイヤレス LAN コントローラに送信され、CAPWAP 制御トンネル内にカプセル化されます。

3. ワイヤレス LAN コントローラは、アラームの更新をアクセス ポイントから、Mobility Services Engine を実行するワイヤレス IPS サービスに透過的に転送します。この通信に使用されるプロトコルは NMSP です。
4. Mobility Services Engine 上のワイヤレス IPS サービスによって受け取られたアラームの更新は、アーカイブと攻撃追跡のためにアラーム データベースに追加されます。SNMP トラップが攻撃情報を格納する Prime Infrastructure に転送されます。同じ攻撃を参照する複数の更新が受け取られた（たとえば、複数のアクセス ポイントで同じ攻撃が認識された）場合、1 つの SNMP トラップだけが PI に送信されます。
5. アラーム情報を含む SNMP トラップは PI によって受信され、表示されます。

構成の考慮事項

必要なコンポーネント

Cisco 適応型ワイヤレス IPS システムの基本システム コンポーネントを次の通りです。

- wIPS モニタ モードのアクセス ポイント、wIPS またはワイヤレス セキュリティ モジュールを使用するローカル モードのアクセス ポイント
- ワイヤレス LAN コントローラ
- ワイヤレス IPS サービスを実行する Mobility Services Engine
- Prime Infrastructure

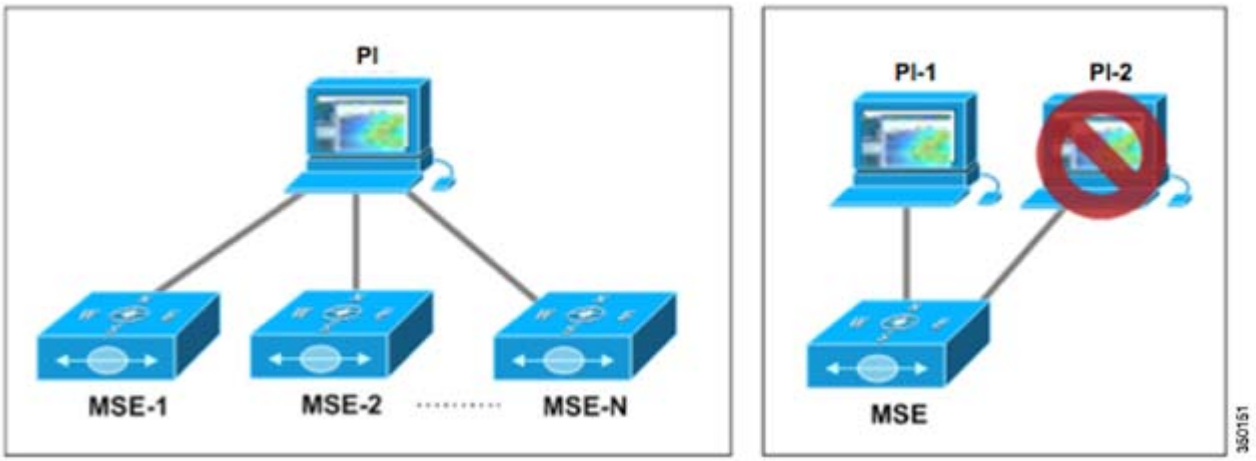
適応型ワイヤレス IPS システムに必要な最小コード バージョン:

- Cisco Mobility Services Engine ソフトウェア リリース 5.2.xxx 以降で使用可能
- Cisco Wireless Control System で 5.2.xxx 以降が必要
- シスコ ワイヤレス LAN コントローラで 5.2.xxx 以降が必要
- リリース 5.2 以降のワイヤレス IPS 機能には、モニタ モードの（クライアントにサービスを提供しない）アクセス ポイントが必要
- リリース 7.1.xxx 以降のワイヤレス IPS 機能には、wIPS を使用するローカル モードの（つまり、クライアントにサービスを提供しない）アクセス ポイントが必要

ワイヤレス セキュリティ モジュール（WSM）に必要な最小コード バージョン:

- ワイヤレス LAN コントローラ：バージョン 7.4.XX 以上
- Cisco Prime Infrastructure：バージョン 1.3.XX 以上
- Mobility Services Engine：バージョン 7.4.XX 以上

システムのスケーラビリティ



Mobility Services Engine（MSE）は、1 つの Prime Infrastructure からのみ管理できます。これには、ネットワークをスケールする際の設計上の意味があります。1 つの Prime Infrastructure から、複数の Mobility Services Engine を管理することも可能です。

システムの設計時には、次のスケーラビリティ項目を考慮してください。

- PI は、ハイエンド サーバで最大 15,000 アクセス ポイントをサポートできます。この 15,000 という制限には、クライアントにサービスを提供するアクセス ポイントと、ワイヤレス IPS モニタ モードのアクセスポイントの両方が含まれます。PI ごとの制限である 15,000 のアクセス ポイントの範囲内で、ワイヤレス IPS AP とデータ AP はさまざまな比率で組み合わせることができます。これらの比率は、環境の RF 条件、既存の WLAN インストールの密度、およびセキュリティ モニタリングの必要なレベルによって異なります。
- 各ワイヤレス IPS モードには、異なる推奨構成密度があります。ワイヤレス IPS を使用したローカル モードの場合は、1:1 の構成密度をお勧めしています。これは、すべての AP をワイヤレス IPS を使用したローカル モードに設定することを意味しています。モニタ モードの AP には 1:5 の構成密度をお勧めしています。また、WSM モジュールを使用した AP 3600 には 2:5 の密度をお勧めしています。以下の表にこれを示します。

さまざまなワイヤレス IPS モードの 15,000 のアクセス ポイントをサポートするための推奨事項

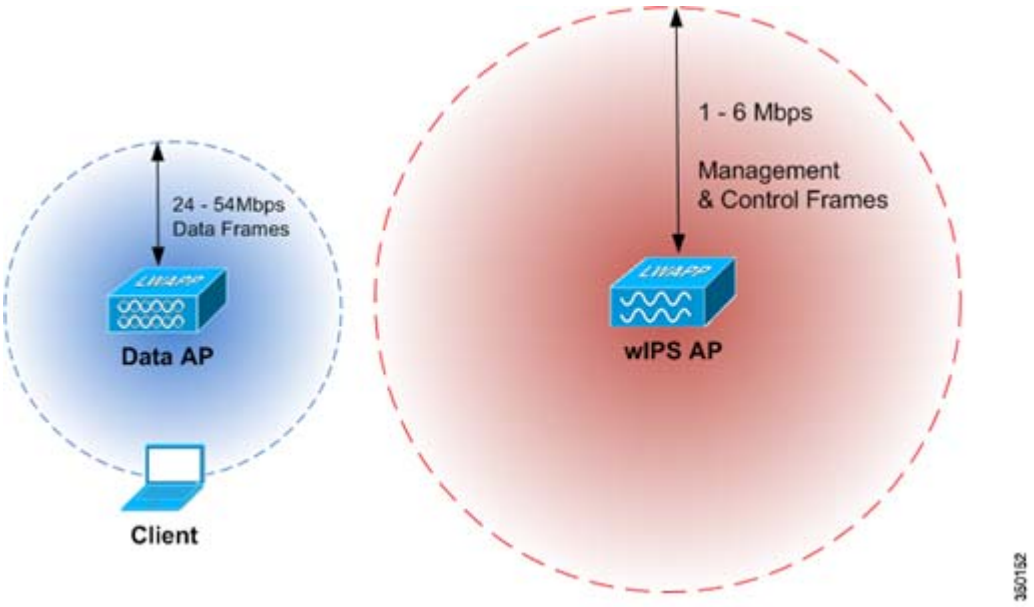
	1:1 の比率	1:5 の比率	2:5 の比率
wIPS MM AP		3000	
ローカル モード データ AP		12000	9000
ELM AP	15000		
AP3600 + WSM			6000
合計 (PI 限定)	15000	15000	15000

（注） モニタ モードのワイヤレス IPS にのみ、データに対して個別のアクセス ポイントが必要です。

- ワイヤレス LAN コントローラが wIPS で実行して、ローカル モード、モニタ モード、ローカル モードをサポートすることができ、ローカル/flex のモードから WSM モジュールのすべて同時に接続します。各アクセス ポイントが AP ライセンスを使用します。

必要な wIPS アクセス ポイント数

適応型ワイヤレス IPS システムを構成する前に、アクセス ポイントのセルの通信範囲が、フレームが受信され、復号化される実際の範囲より小さいことを考慮することが重要です。この相違の理由は、アクセス ポイントの通信範囲が、最弱リンク（一般的な構成では WLAN クライアント）によって制限されるためです。WLAN クライアントの出力がアクセス ポイントの最大出力より本質的に低いため、セルの範囲はクライアントの能力に制限されます。さらに、アクセス ポイントを全出力以下で実行し、ワイヤレス ネットワークに RF 冗長性とロード バランシングを組み込むことをお勧めします。これらの先述の事項とシスコのアクセス ポイントの優れたレシーバ感度の組み合わせによって、適応型ワイヤレス IPS システムは、広範囲の監視を行いながら、クライアントがサービスするインフラストラクチャより少ないアクセス ポイント密度で構成できます。



上の図で示すように、ワイヤレス IPS の構成は、大半の攻撃で障害の発生に使われる 802.11 管理および制御フレームの検知に基づきます。これは、24 Mbps から 54 Mbps の高いスループット データ レートを提供するために調査されるデータ アクセス ポイントと異なります。

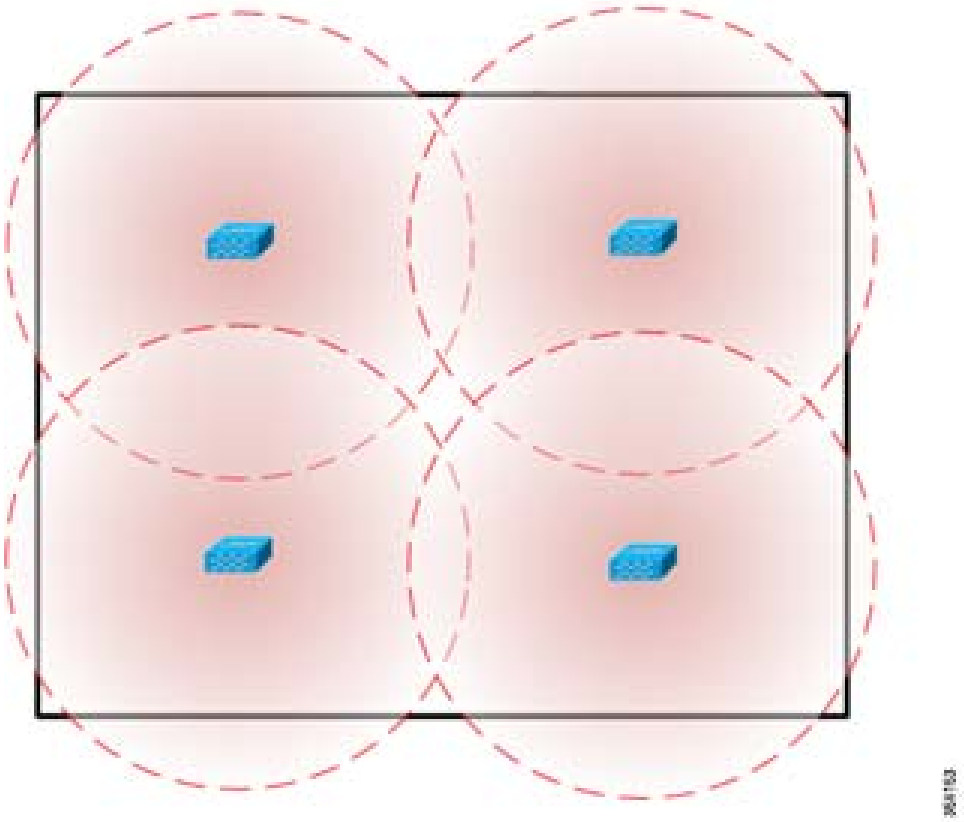
特定の環境に必要なワイヤレス IPS アクセス ポイント数を正確に決定するために、多数の要因があります。目的とする構成のセキュリティ要件と環境条件はそれぞれ異なるため、すべての構成のニーズに対処する確実なルールはありませんが、いくつかの一般的なガイドラインを考慮する必要があります。

必要な wIPS アクセス ポイント数に影響する主な要因を次に示します。

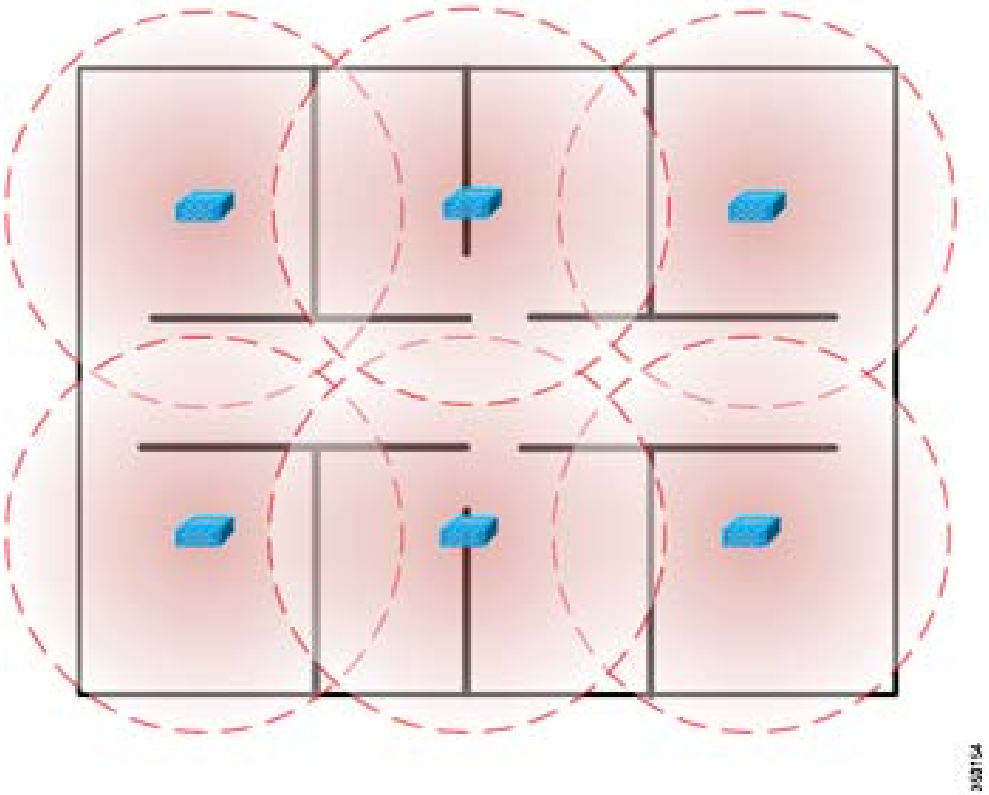
構成の条件

構成は、フロア レイアウトやビルディングの素材などの固有の環境条件に左右されます。ワイヤレス信号の伝播は信号が通過する素材の種類に大きく依存するため、多数の壁のあるオフィス環境では、空の倉庫よりも多くのセンサーが必要になります。このことは、データ サービス アクセス ポイントの構成方法に関する既存の知識と同様です。RF 信号の減衰を引き起こす環境内の障害物が多いほど、ワイヤレス IPS アクセス ポイントを高い密度で構成する必要があります。

下の図では、ワイヤレス信号を妨害したり、弱めたりする壁がなければ、長距離の攻撃を「リッスン」できるワイヤレス IPS アクセス ポイントを構成したオープンな室内環境を示しています。



明確な対比として、下の図では、信号の減衰を引き起こす多数の厚い壁のある室内環境を示しています。この場合、攻撃を検出するために、多くのワイヤレス IPS アクセス ポイントを構成する必要があります。



監視する周波数帯域

2.4 GHz および 5 GHz 帯域の無線周波数伝播特性は、双方の波長の差の結果として異なります。簡単に述べると、2.4 GHz ワイヤレス信号（802.11b/g/n）は、5 GHz（802.11a/n）より長距離を伝送します。目的のインストールに必要なワイヤレス IPS アクセス ポイント数を正確に計算するには、ワイヤレス IPS 構成で監視する必要がある周波数帯域を考慮する必要があります。

ワイヤレス IPS AP（2.4 GHz）あたりの監視範囲

データ レート	壁のある室内	オープンな室内
1 Mbps @ -86 dBm	～ 35,000 平方フィート	～ 85,000 平方フィート
6 Mbps @ -86 dBm	～ 10,668 平方フィート	～ 25,908 平方フィート

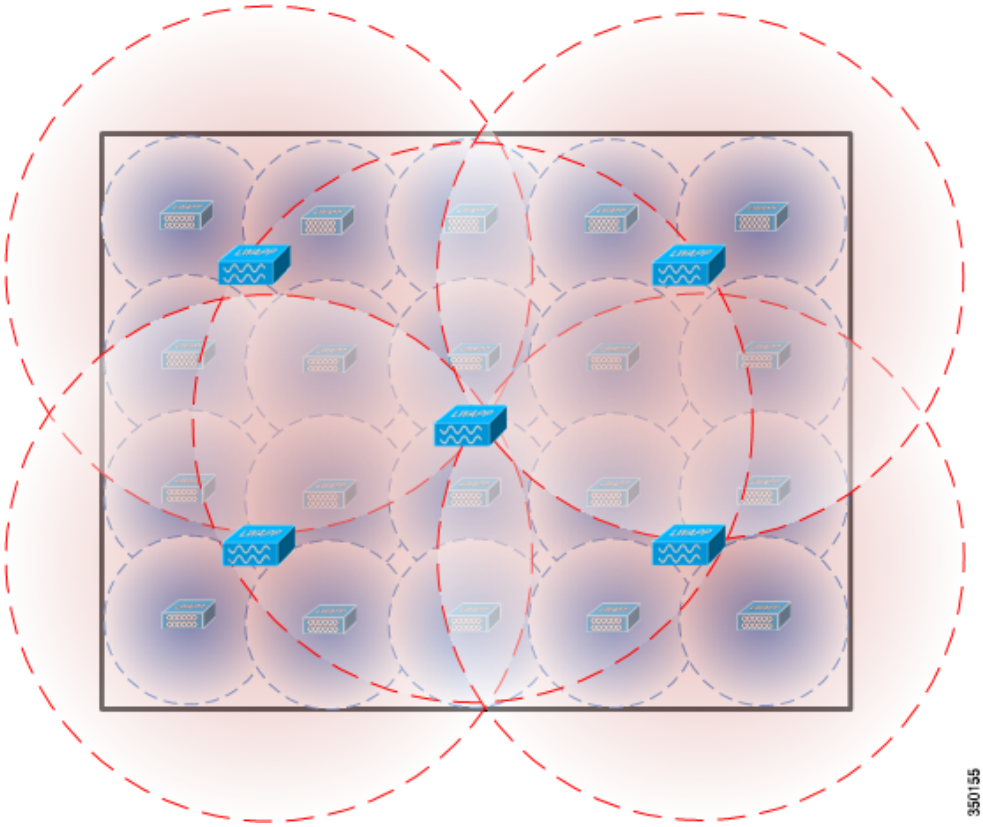
ワイヤレス IPS AP（5 GHz）あたりの監視範囲		
データ レート	壁のある室内	オープンな室内
1 Mbps @ -86 dBm	～ 15,000 平方フィート	～ 85,000 平方フィート
6 Mbps @ -86 dBm	～ 4,572 平方フィート	～ 25,908 平方フィート

上の表は、各周波数および各タイプの環境で、1 つのワイヤレス IPS モード アクセス ポイントでカバーできる円の平方フィートを示しています。これらのメトリックから、特定のフロア領域をカバーするために必要なワイヤレス IPS アクセス ポイント数の基準がわかります。これらの表は MatLab のシミュレーション用ソフトウェアを使用して、攻撃デバイスが 15 dBm の送信電力を出力していると想定して作成されています。この計算で使用しているレシーバ感度は、ワイヤレス IPS をサポートするシスコのアクセス ポイントのライン間の最小公分母を示しています。

ワイヤレス IPS アクセス ポイントの位置

ワイヤレス IPS モード アクセス ポイントの物理構成は、WLAN インフラストラクチャ全体を広く監視するという最終目標に基づいています。このため、ワイヤレス IPS モード AP は、2 つの一般的なガイドラインに従って配置します。まず、ワイヤレス IPS アクセス ポイントを物理的な位置の周辺に配置して、ビルディングの外部から仕掛けられた攻撃を十分に監視します。これは、ワイヤレス IPS モード アクセス ポイントをビルディングの物理的な先端に配置するのではなく、検出範囲が先端に達するように適切に配置する必要があることを意味します。次に、ワイヤレス IPS アクセス ポイントをビルディングの中心全体に配置し、物理的なビルディング内部から仕掛けられた攻撃を検出できるようにします。

ワイヤレス IPS アクセス ポイントの物理的な設置位置は、データ サービス アクセス ポイントを設置する場合と同じベスト プラクティスに基づく必要があります。これらの規則に従って、ワイヤレス IPS アクセス ポイントのアンテナを厚いビルディング素材の陰に設置したり、吊り天井の上に設置したりしないことが重要です。アクセス ポイントを吊り天井の上に配置する場合、固有の外部アンテナを使用して、監視する同じ物理空間にアンテナを引き込む必要があります。



上の構成例では、4 つのワイヤレス IPS アクセス ポイントをビルディングの境界周辺に配置し、物理的なビルディングの周辺全体のセキュリティ モニタリングを実現します。さらに、1 つのワイヤレス IPS アクセス ポイントをビルディングの中心に配置して、ビルディング内部のセキュリティ モニタリングを実行します。

アクセス ポイント密度の推奨事項

上述のように、アクセス ポイントのカバレッジの面積は、周波数と環境に基づいて測定できます。ただし、新しいワイヤレス IPS モードでは、その他の要因もワイヤレス IPS アクセス ポイントの密度に関する推奨事項に関与します。すべてのアクセス ポイント モードは同じ距離をモニタできますが、以下に示す理由により、各モードは異なる密度で展開することを推奨します。

wIPS を使用するローカル モードのアクセス ポイントは、クライアントへのサービス提供を対象としています。wIPS を使用するローカル モードを展開する場合、すべてのアクセス ポイントを wIPS を使用するローカル モードにすることを推奨します。

モニタ モードのアクセス ポイントの場合、ローカル モードとモニタ モードのアクセスポイントの比率を 1:5 にすることを推奨します。

最後に、WSM モジュールには、2.4 GHz および 5 GHz 帯域の両方ですべてのチャネルをモニタする単一の無線があります。無線はスキャンするチャネルを追加するため、検出時間を短縮するために WSM モジュールを 2:5 の密度で展開することを推奨します。

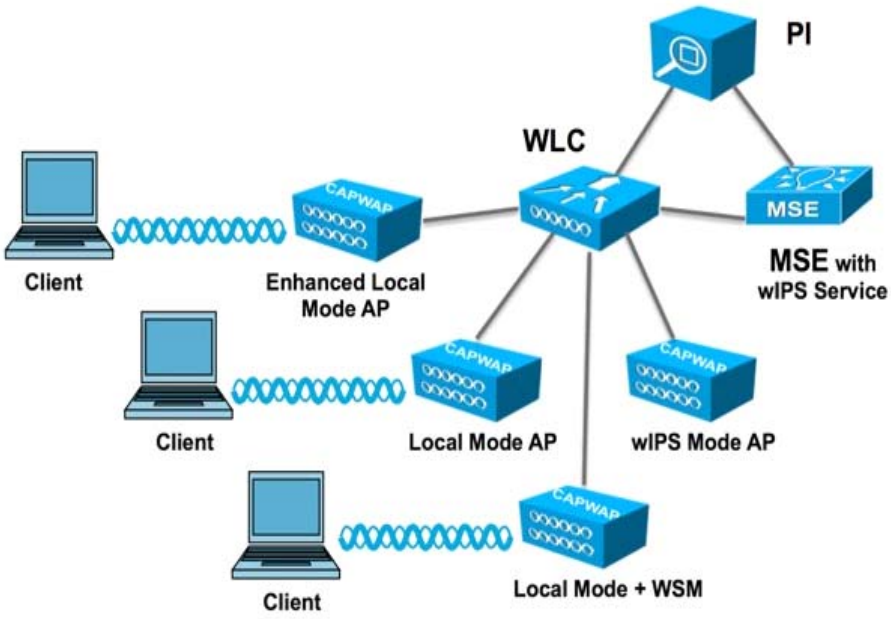
Evolution of Wireless Security & Spectrum

Features	Good Enhanced Local Mode	Better Monitor Mode AP	Best AP3600 with Wireless Security Module (WSM)
Deployment Density (#WSM : #AP)	1:1	1:5	1:5 – CleanAir 2:5 - wIPS
Serving Wireless data clients while Securing and Monitoring	Y	N	Y
Shared Ethernet infrastructure for Wireless Data and Monitoring	Y	N (Requires a separate Ethernet connection for a Data AP and for Monitoring AP)	Y
wIPS Security Scanning	• 7x24 On-channel • Best effort Off-Channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
CleanAir Spectrum Intelligence	• 7x24 On-channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
Feature off-load – eliminating jitter from off channel scanning	N	N	Y

353388

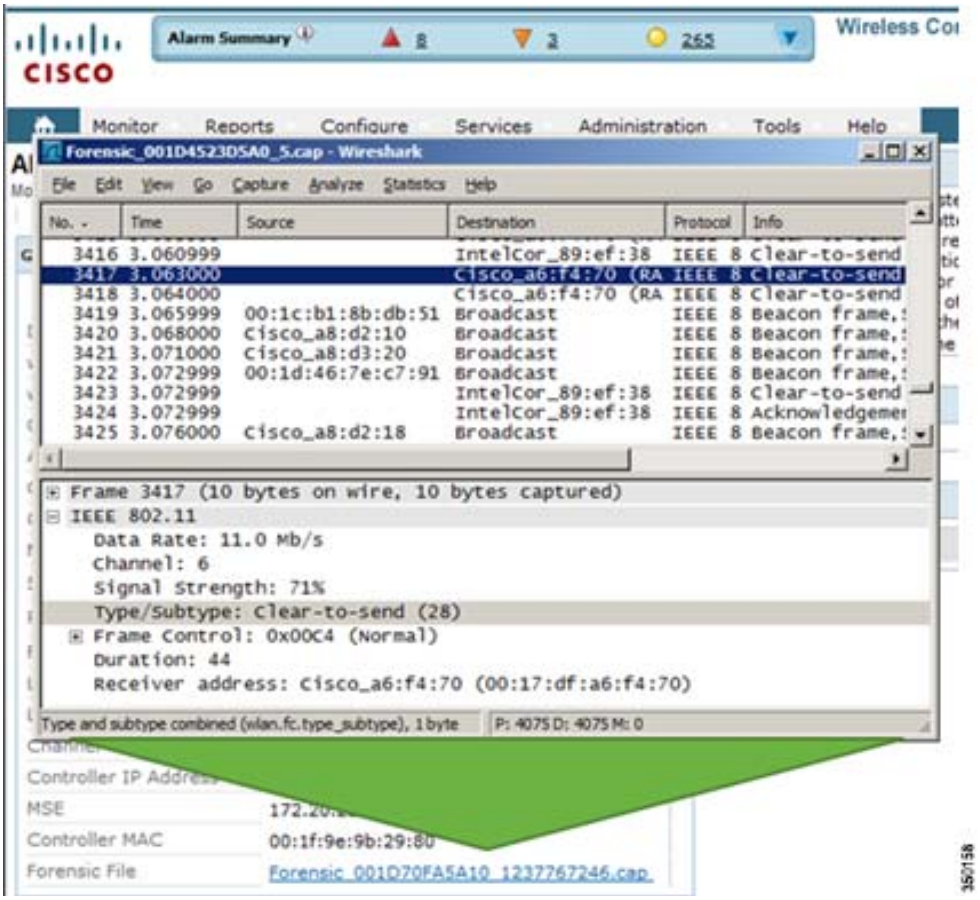
Cisco Unified Wireless Network に統合された wIPS

統合 wIPS 構成は、非 wIPS モードのアクセス ポイントと wIPS モードのアクセス ポイントを同じコントローラ上で混合させ、同じ Prime Infrastructure によって管理するシステム設計です。ローカル モード、FlexConnect モード、wIPS を使用するローカル モード、モニタ モード、および WSM モジュールを備えた 3600 シリーズ アクセス ポイントを組み合わせることができます。wIPS 保護およびデータのオーバーレイによって、コントローラや Prime Infrastructure を含む多くのコンポーネントが共有されるため、インフラストラクチャ コストの重複が削減されます。



フォレンジック

Cisco 適応型ワイヤレス IPS システムは、詳しい調査とトラブルシューティングの目的で、攻撃フォレンジックをキャプチャする機能を備えています。基本レベルで、フォレンジック機能は、一連のワイヤレス フレームをログに記録し、抽出する機能を持つ切り替えベースのパケット キャプチャ ファシリティです。この機能は、PI の wIPS プロファイル設定内から攻撃単位で有効にします。



この機能をイネーブルにすると、エアウェーブに特定の攻撃アラームが見られたら、フォレンジック機能がトリガーされます。元のアラームをトリガーした wIPS モード AP のバッファ内に格納されたパケットに基づいて、フォレンジック ファイルが作成されます。このファイルは CAPWAP によってワイヤレス LAN コントローラに転送され、次に NMSP によって、Mobility Services Engine で実行するワイヤレス IPS サービスに転送されます。このファイルは、ユーザがフォレンジックに設定したディスク容量制限に達するまで、MSE のフォレンジック アーカイブに保存されます。デフォルトでこの制限は 20 ギガバイトで、この制限に達すると、最も古いフォレンジック ファイルが削除されます。フォレンジック ファイルには、フォレンジック ファイルへのハイパーリンクを含むアラームを Prime Infrastructure で開くことでアクセスできます。このファイルは「CAP」ファイル形式で保存されています。この形式のファイルは、WildPacket's Omnipeek、AirMagnet Wi-Fi Analyzer、Wireshark、またはまたはこの形式をサポートするその他のパケット キャプチャ プログラムで開くことができます。Wireshark は、http://www.wireshark.org から入手できます。

(注)　ワイヤレス IPS システムのフォレンジック機能はむやみに使用せず、目的の情報がキャプチャされたら無効にする必要があります。この推奨事項の理由は、アクセス ポイントにかかる負荷が大きく、この機能に必要とするスケジュールされたチャネル スキャンへの割り込みのためです。ワイヤレス IPS アクセス ポイントは、フォレンジック ファイルを生成している同じインスタンスで、チャネル スキャンを同時に実行できません。フォレンジック ファイルがダンプされている間、チャネル スキャンは最大 5 秒間遅延します。

適応型ワイヤレス IPS 設定

Mobility Services Engine の設定

Mobility Services Engine を設定する方法は以下の通りです。

ステップ 1　ログイン:

次の資格情報でログインします:**root/password**

ステップ 2　設定プロセスの開始:

最初の起動時に、MSE からセットアップ スクリプトを起動するように求められます。このプロンプトに [yes] と入力します。

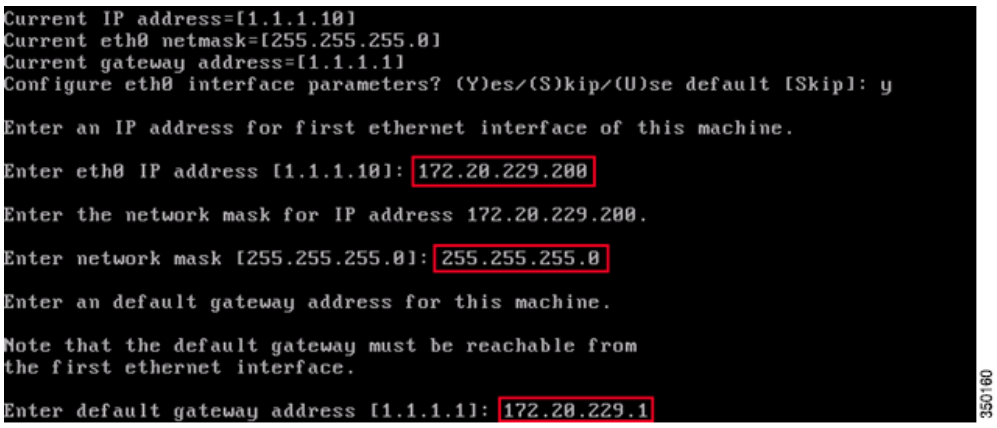
(注)　MSE からセットアップが求められない場合は、次のコマンドを入力します:
/opt/mse/setup/setup.sh

ステップ 3　ホスト名と DNS ドメイン名の設定:

```
Current hostname=[mse]
Configure hostname?  (Y)es/(S)kip/(U)se default [Skip]: y

The host name should be a unique name that can identify
the device on the network. The hostname should start with
a letter, end with a letter or number, and contain only
letters, numbers, and dashes.

Enter a host name [mse]: MSE-1

Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: y

Enter a domain name for the network domain to which this device
belongs.  The domain name should start with a letter, and it should
end with a valid domain name suffix such as ".com".  It must contain
only letters, numbers, dashes, and dots.

Enter a domain name: cisco.com
```

350159

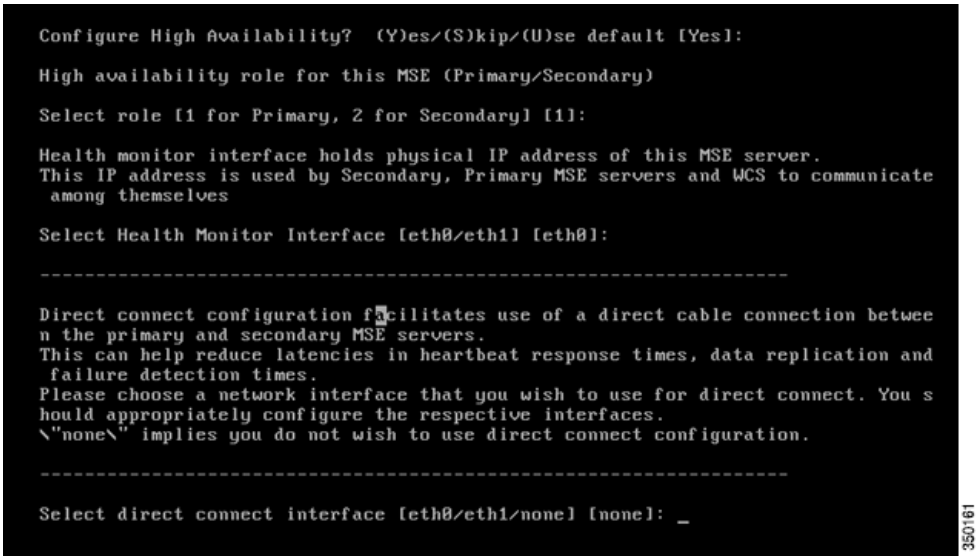
ステップ 4　イーサネット インターフェイス パラメータの設定:



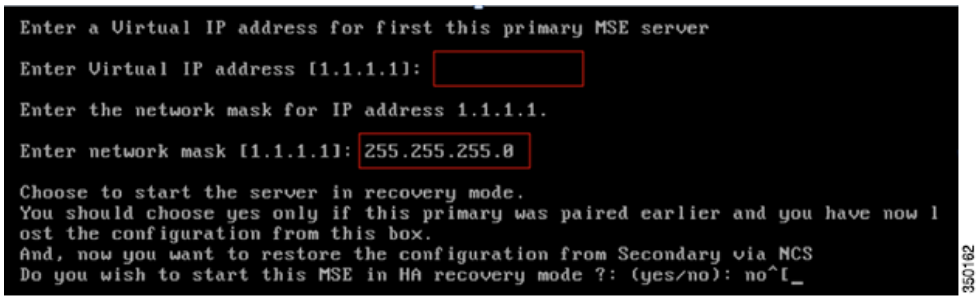
「eth1」インターフェイス パラメータの入力を求められた場合、2 つめの NIC は操作に必要ではないため、[Skip] と入力して次の手順に進みます。

(注)　設定するアドレスは、このアプライアンスで使用する目的のワイヤレス LAN コントローラと PI 管理システムへの IP 接続を提供する必要があります。

ステップ 5　高可用性の設定(オプション):



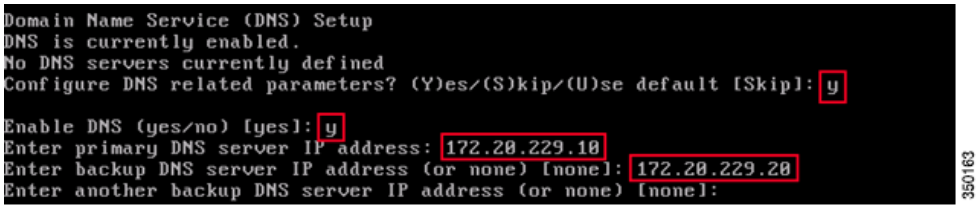
高可用性を有効にし、MSE のロールを選択します。次に、セカンダリの MSE サーバにアクティブにモニタリングされるイーサネット ポートを選択します。直接接続がある場合は、そのイーサネット ポートを選択する必要があります。



次に、この HA ペアの仮想 IP アドレスを指定します。仮想 IP アドレスを指定すると、HA リカバリ モードを開始して HA 交換を開始できます。

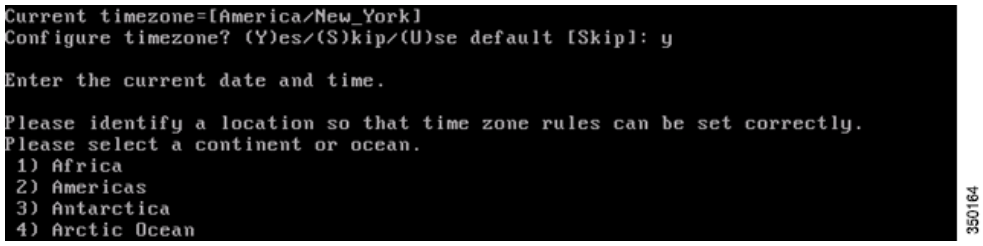
ステップ 6　DNS サーバ情報の入力:

正常なドメイン解決に必要な DNS サーバは 1 つだけですが、復元力のためバックアップ サーバを入力します。

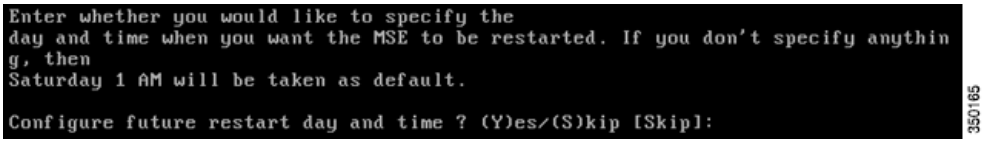


ステップ 7　タイムゾーンの設定:

デフォルトの New York のタイム ゾーンが環境に当てはまらない場合は、[Location] メニューを参照して正しく設定します。

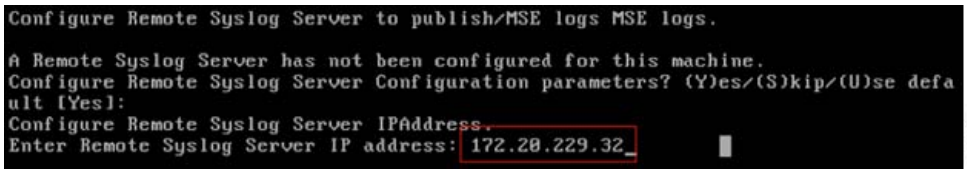


ステップ 8　MSE を再起動する時間の割り当て（任意）:



この手順は省略できます。

ステップ 9　リモート Syslog サーバの設定:

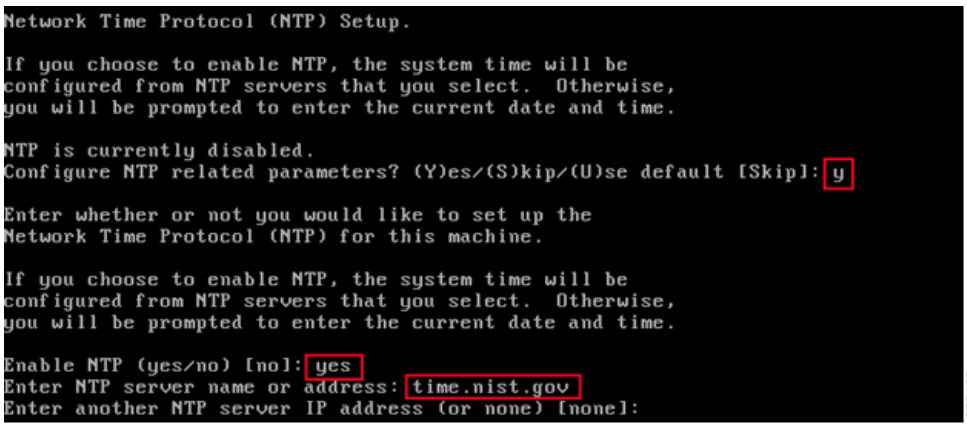


リモート Syslog サーバの IP アドレスを設定します。

次に、ログ メッセージの優先度レベルと機能を指定します。

ステップ 10　NTP またはシステム時間の設定:

NTP はオプションですが、システムで正確なシステム時間が維持できます。「No」を選択した場合、システムの現在の時間を設定するように求められます。



(注)　Mobility Services Engine、ワイヤレス LAN コントローラ、および WCS 管理システムには正しい時間を設定する必要があります。これは、3 つすべてのシステムで同じ NTP サーバをポイントし、それらに正しいタイム ゾーンが設定されるようにすることによって実現できます。

ステップ 11　監査ルールの設定(任意):

```
Audit rules Setup.
Configure audit rules and enable Audit daemon? (Y)es/(S)kip/(U)se default [Yes]:

Enable audit rules (yes/no): no
```

350169

これにより、ユーザは監査デーモンを設定できます。この手順は省略できます。

ステップ 12　ログイン バナーの設定:

ログイン バナーは、ユーザにシステムの使用状況を知らせ、未承認ユーザがシステムにアクセスできないようにするための警告を表示するために使用されます。ログイン バナーは複数行のメッセージの場合があるため、1 つのピリオド(.)でメッセージを終了し、次の手順に進みます。

```
Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [Skip]: yes

Enter text to be displayed as login banner. Enter a single period
on a line to terminate.

Login banner [Cisco Mobility Service Engine]:
MSE-1
Unauthorized Access is not allowed
.
```

350170

ステップ 13　ローカル コンソール ルート ログインの有効化:

このパラメータは、システムへのローカル コンソール アクセスを有効または無効にするために使用します。このパラメータは、ローカル トラブルシューティングを実行できるようにするために有効にする必要があります。

```
System console is not restricted.
Configure system console restrictions? (Y)es/(S)kip/(U)se default [Yes]:

Enter whether or not you would like to restrict
console login to the serial interface.

Restrict system console to serial interface (yes/no) [no]:
```

350171

ステップ 14　SSH(セキュアシェル)ルートログインの有効化:

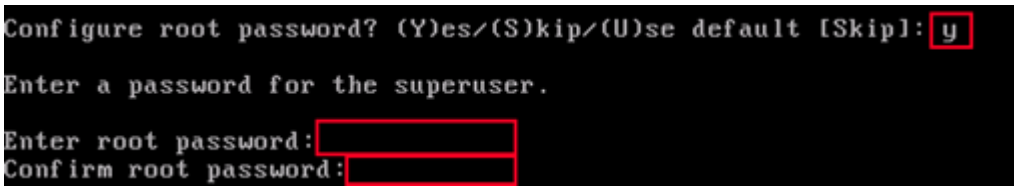
このパラメータは、システムへのリモート コンソール アクセスを有効または無効にするために使用します。このパラメータはリモート トラブルシューティングを実行できるようにするために有効にする必要がありますが、ただし、会社のセキュリティ ポリシーでこのオプションを無効にするように命じられている場合もあります。

```
SH root access is currently disabled.
onfigure ssh access for root (Y)es/(S)kip/(U)se default [Skip]: yes

nter whether or not you would like to enable ssh
oot login. If you disable this option, only console
oot login will be possible.

nable ssh root access (yes/no): yes
```

350172

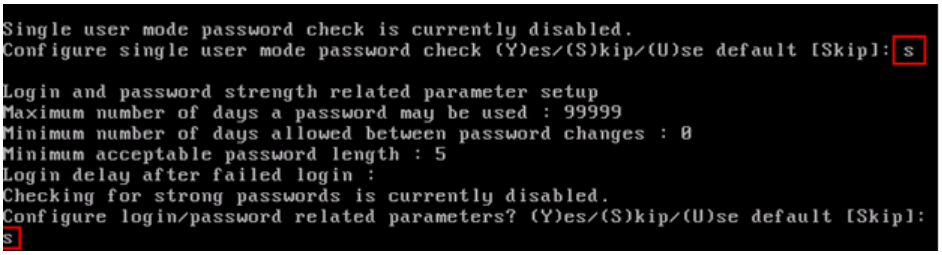
ステップ 15　ルートパスワードの変更:

この手順は、システムのセキュリティを確保するために重要であり、辞書にある単語ではない文字と数字から構成される強力なパスワードを選択してください。パスワードの最小文字数は 8 文字です。



ステップ 16　単一のユーザ モードおよびパスワードの強度の設定:

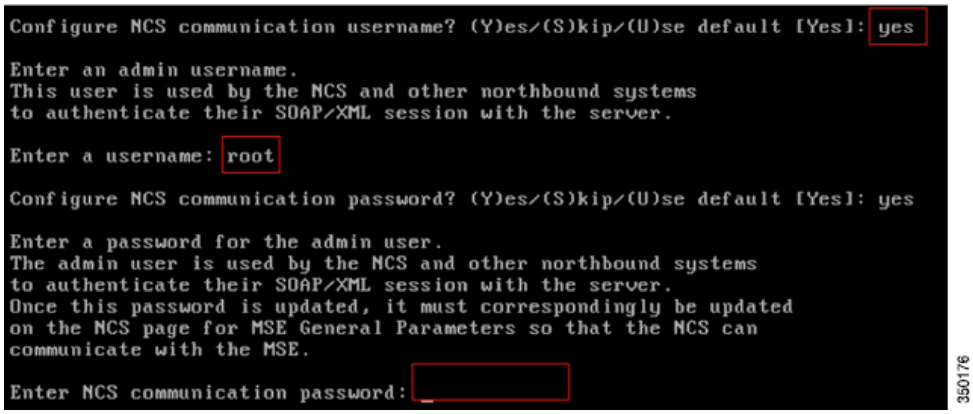
これらの設定パラメータは必須ではなく、デフォルトの設定は「s」を入力してそれらをスキップすることです。



ステップ 17　GRUB パスワードの入力:

この設定パラメータは必須ではなく、デフォルトの設定は「s」を入力してそれをスキップすることです(任意)。

ステップ 18　Prime Infrastructure 通信パスワードの設定:



ステップ 19　変更の保存と再起動:

セットアップ スクリプトが完了し、**プロンプトが表示されたら、変更を保存します**。保存後、**プロンプトに従って MSE を再起動**し、すべての設定が正しく適用されていることを確認します。

ステップ 20　MSE サービスの再起動:

ユーザ名 **root** と**手順 13** で設定したパスワードを使用して、MSE にログインします。コマンド「service msed start」を実行して、MSE サービスを開始します。

```
login as: root
Cisco Mobility Service Engine

root@172.20.226.203's password:
Last login: Wed Jul 23 10:11:58 2008 from dhcp-171-71-123-7.cisco.com
[root@MSE-1 ~]# service msed start
Starting MSE Platform
Cannot find UDI information. Exiting
null
Invalid Platform type. Now Exiting.
Starting MSE Platform, waiting to check the status.
Starting MSE Platform, waiting to check the status.
MSE Platform is up, getting the status
```

350177

ステップ 21　起動時の MSE サービス開始の有効化:

コマンドの実行:「chkconfig msed on」

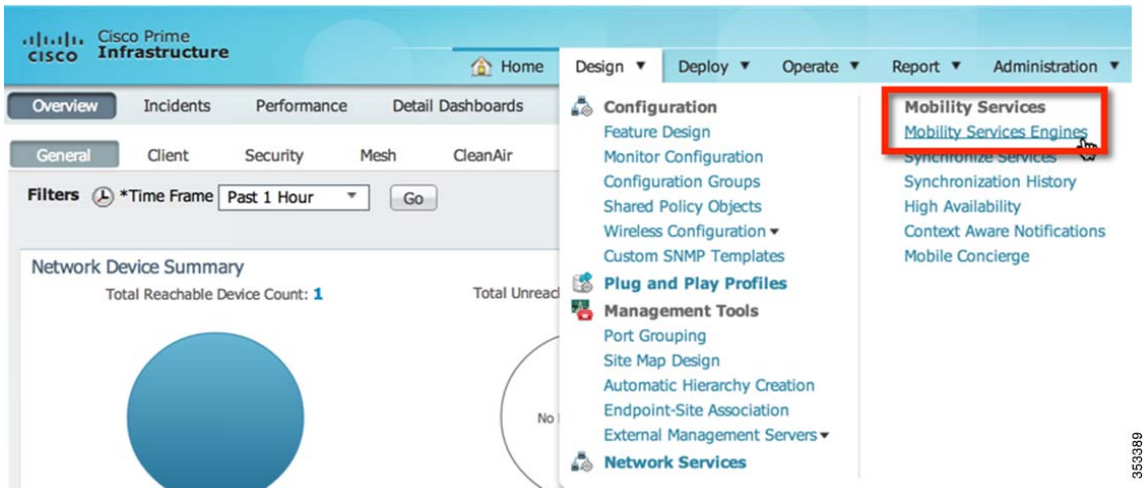
```
[root@MSE-1 ~]#
[root@MSE-1 ~]# chkconfig msed on
[root@MSE-1 ~]#
```

PI への MSE の追加

PI への MSE の追加:

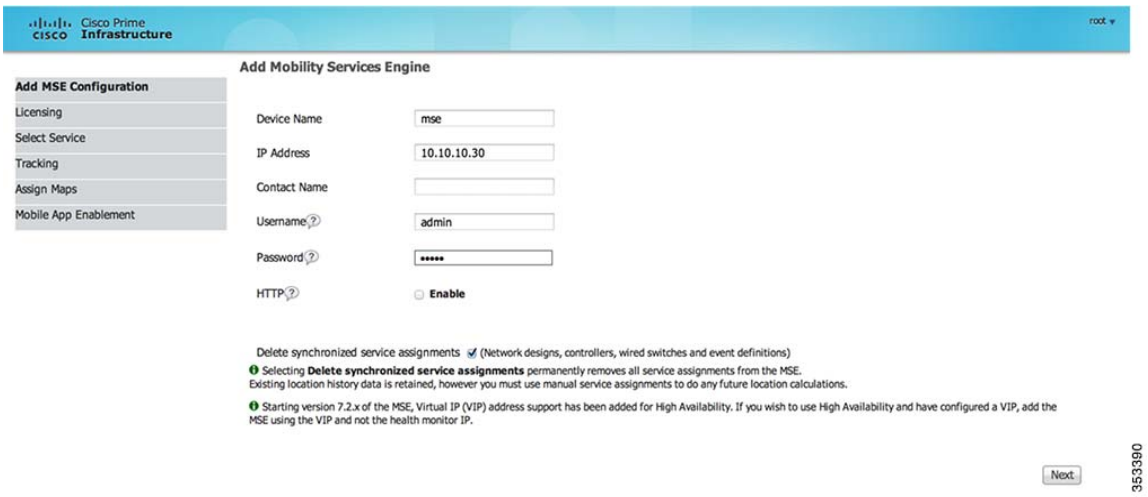
ステップ 1　Mobility Services 設定ページへの移動:

PI にログインし、[Design] ドロップダウン メニューから [Mobility Services Engine] をクリックします。



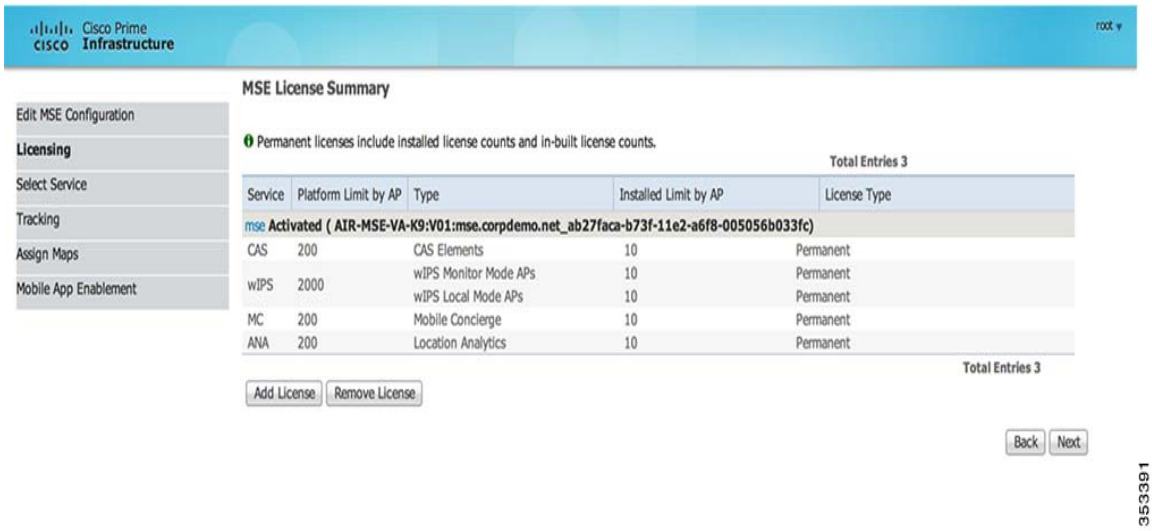
ステップ 2　PI への Mobility Services Engine の追加:

右側のドロップ ダウンから、[Add Mobility Services Engine] を選択し、[Go] をクリックします。



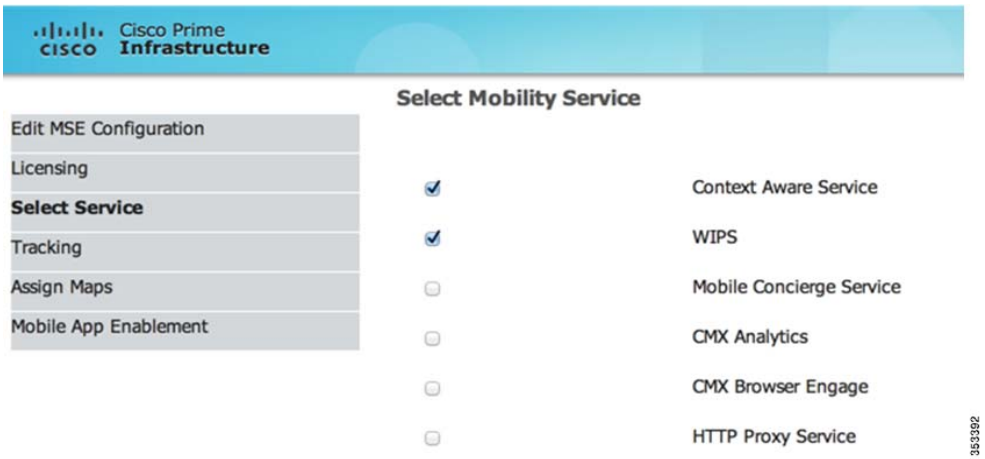
MSE の一意のデバイス名、MSE のセットアップ時に設定した IP アドレス、サポートの連絡先名、MSE のセットアップ時に設定した **PI 通信パスワード**を入力します。ユーザ名をデフォルトの「admin」から変更しないでください。

ステップ 3　MSE ライセンスの追加:

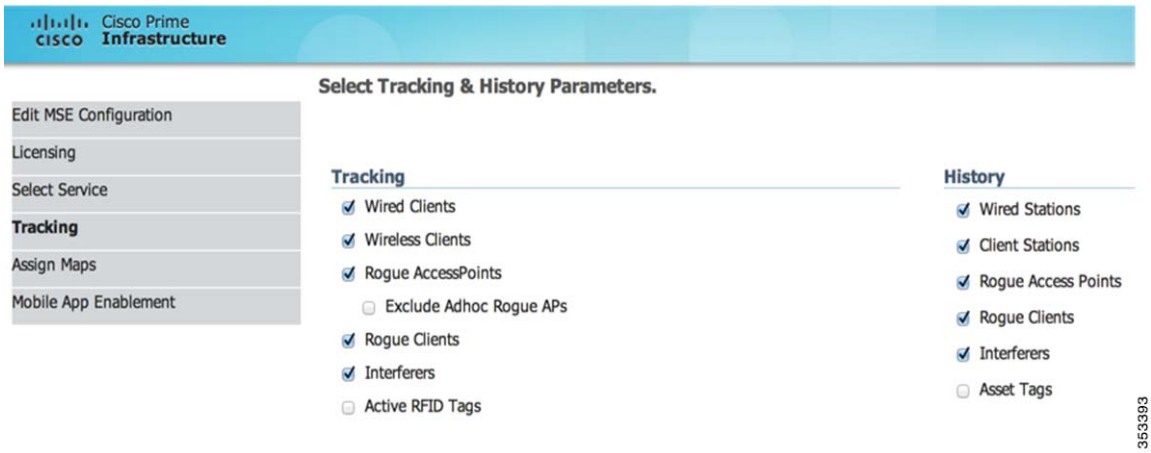


ここで MSE ライセンスを追加します。

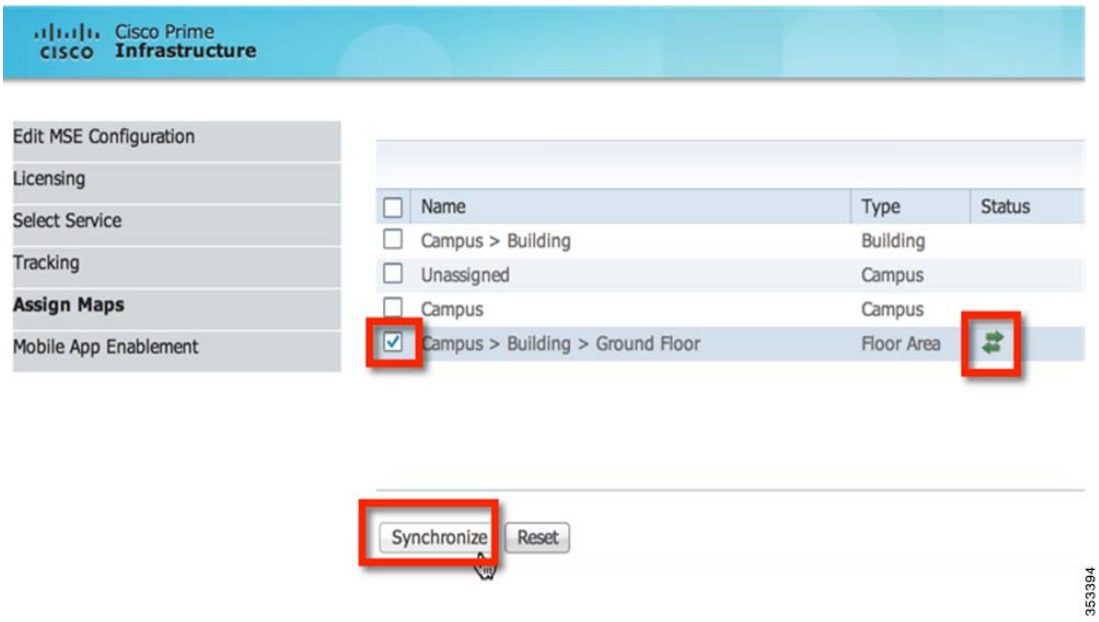
ステップ 4　MSE で実行する WIPS サービスの選択:



ステップ 5　トラッキングと履歴のパラメータの選択:

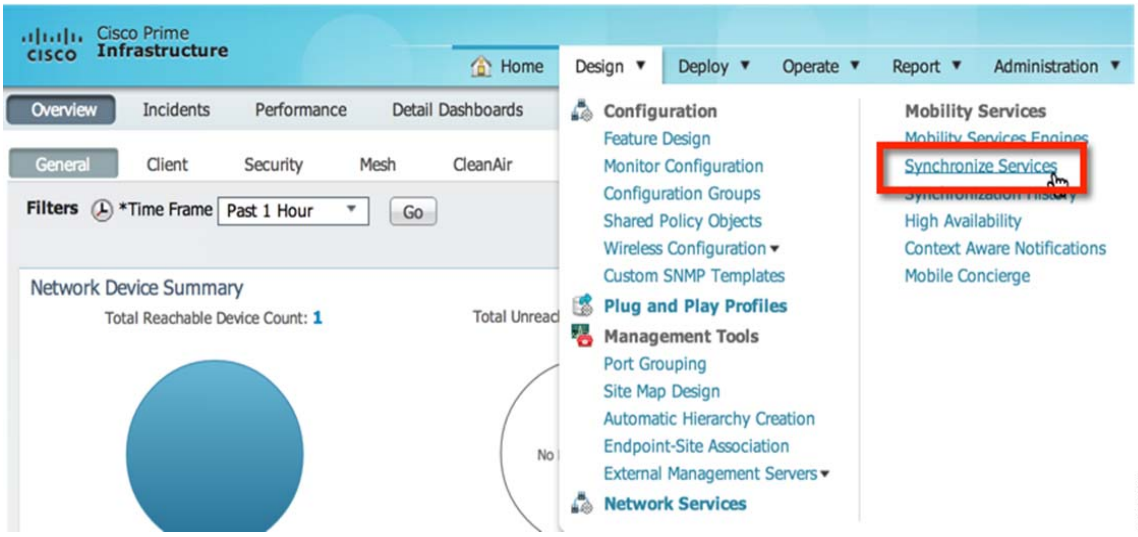


マップを割り当て、ネットワークの設計を同期します。同期すると、以下の図でハイライトするように、ステータスが表示されます。



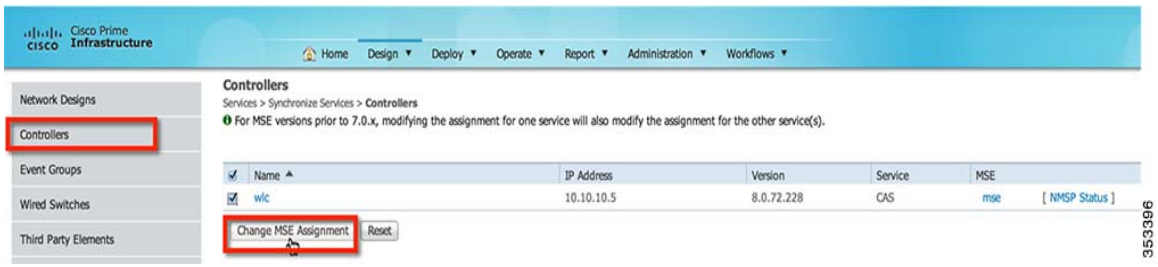
ステップ 6　同期:

[Design] ドロップダウンメニューから、[Synchronize Services] を選択します。

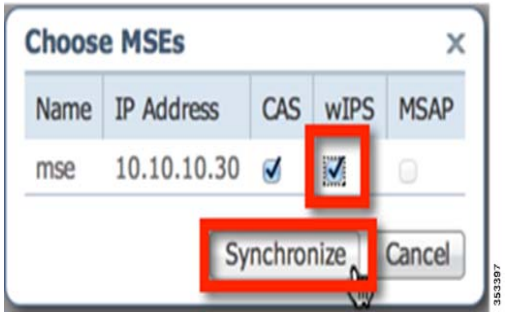


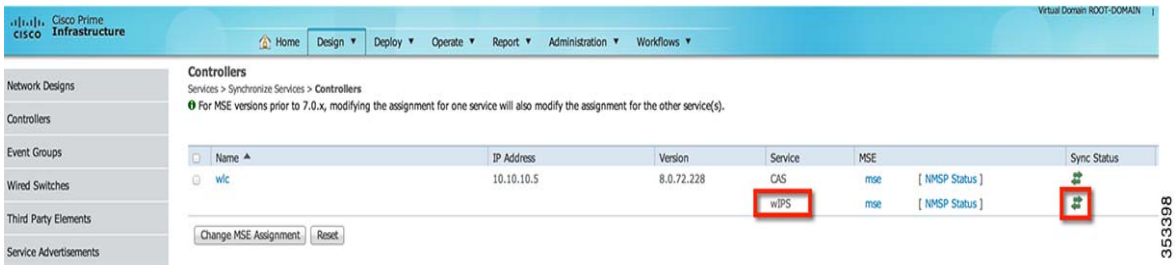
ステップ 7　同期させるコントローラの選択:

コントローラのリストを表示する、[Controllers] タブを選択します。目的のコントローラを選択したら、[Change MSE Assignment] ボタンを押します。



MSE と同期させるコントローラのリストを示すポップアップが表示されます。同期させる希望の機能を選択してクリックします。





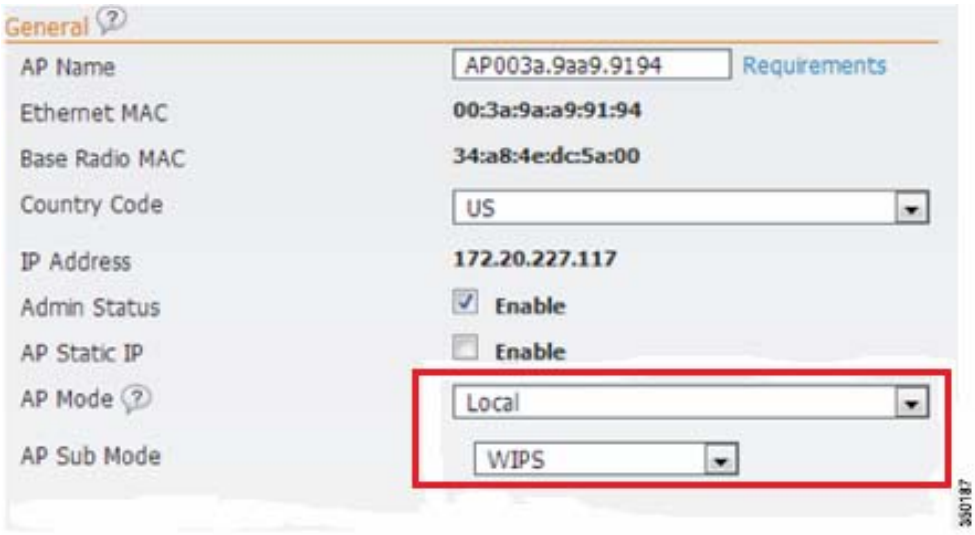
ワイヤレス IPS を使用したローカル モードへのアクセス ポイントの設定

ローカル モードのインドア アクセス ポイント（AP）は、ワイヤレス IPS を使用したローカル モードに設定できます。

WIPS を使ってローカル モード Ap の設定。

ステップ 1　ワイヤレス IPS を使用したローカル モードへの AP の設定:

a. [Operate] > [Device Group] > [Device Type] > [Unified AP] で PI の AP 設定メニューを開き、アクセス ポイントの名前をクリックし、次に [Configuration] をクリックします。



b. [AP Mode] を [Local] に変更します。

c. **WIPS** を **AP サブ モード**を変更します。

d. ページ下部の [Save] をクリックします。

e. AP を再起動するように求められたら、[OK] をクリックします。

ワイヤレス IPS を使用したローカル モードに設定した各 AP でこれを繰り返します。

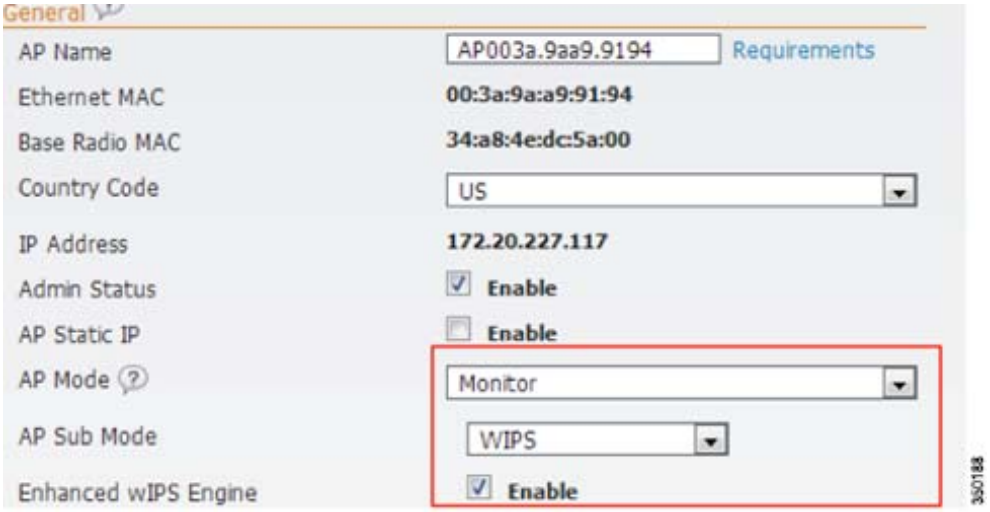
アクセス ポイントのワイヤレス IPS モニタ モードへの設定

任意のインドア アクセス ポイント（AP）をワイヤレス IPS モニタ モードに設定できます。

AP のワイヤレス IPS モニタ モードへの設定：

ステップ 1　アクセス ポイントのモニタ モードへの設定：

a. [Operate] > [Device Group] > [Device Type] > [Unified AP] で PI の AP 設定メニューを開き、アクセス ポイントの名前をクリックし、次に [Configuration] をクリックします。



b. [AP Mode] を [Monitor] に変更します。

c. [Enhanced WIPS Engine] を有効にします。

d. [Monitor Mode Optimization] を [WIPS] に変更します。

e. ページ下部の [Save] をクリックします。

f. AP を再起動するように求められたら、[OK] をクリックします。

ワイヤレス IPS モニタ モードに設定されている各 AP でこれを繰り返します。

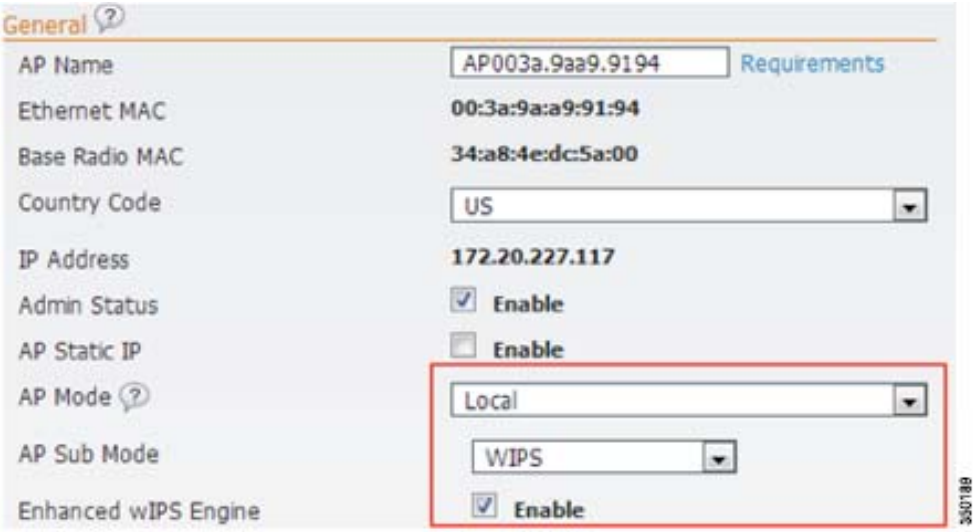
AP3600 ローカル モードおよび WSM モジュールへのアクセス ポイントの設定

このモードは、WSM モジュールをインストールした 3600 シリーズ アクセス ポイント（AP）でのみ利用可能です。

AP の AP3600 と WSM モジュールへの設定:

ステップ 1　AP のローカルモードへの設定:

[Operate] > [Device Group] > [Device Type] > [Unified AP] で PI の AP 設定メニューを開き、アクセス ポイントの名前をクリックし、次に [Configuration] をクリックします。



a. [AP Mode] を [Local] に変更します。

b. [Enhanced WIPS Engine] を有効にします。

c. **WIPS** を **AP サブ モード**を変更します。

d. ページ下部の [Save] をクリックします。

e. AP を再起動するように求められたら、[OK] をクリックします。

ローカル モードに設定した各 AP でこれを繰り返します。

wIPS プロファイルの設定

デフォルトで、MSE と対応するワイヤレス IPS アクセス ポイントは PI からデフォルトのワイヤレス IPS プロファイルを継承します。このプロファイルは、デフォルトで有効にされている大部分の攻撃アラームによってあらかじめ調整されており、ワイヤレス IPS アクセス ポイントと同じ RF グループ内のアクセス ポイントに対する攻撃を監視します。このように、システムは WLAN インフラストラクチャとワイヤレス IPS アクセス ポイントの両方が同じコントローラ上に混合されている統合ソリューションを利用する構成モデルに対する攻撃を監視するようにあらかじめ設定されています。

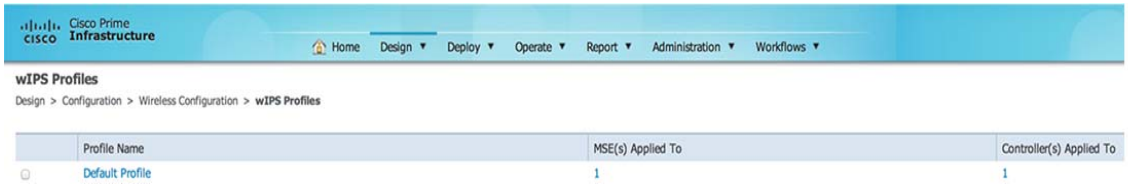
（注） 下の手順の一部はオーバーレイだけとしてマークされており、Autonomous や完全に個別のコントローラベースの WLAN などの既存の WLAN インフラストラクチャを監視するように適応型ワイヤレス IPS ソリューションを構成している場合にだけ実行されます。

ワイヤレス IPS プロファイルの設定:

ステップ 1　ワイヤレス IPS プロファイルへの移動:

最上位の PI メニューから、[Design] > [Configuration] > [Wireless Configuration] > [wIPS Profiles] の順にクリックします。

ステップ 2　新しいプロファイルの作成:

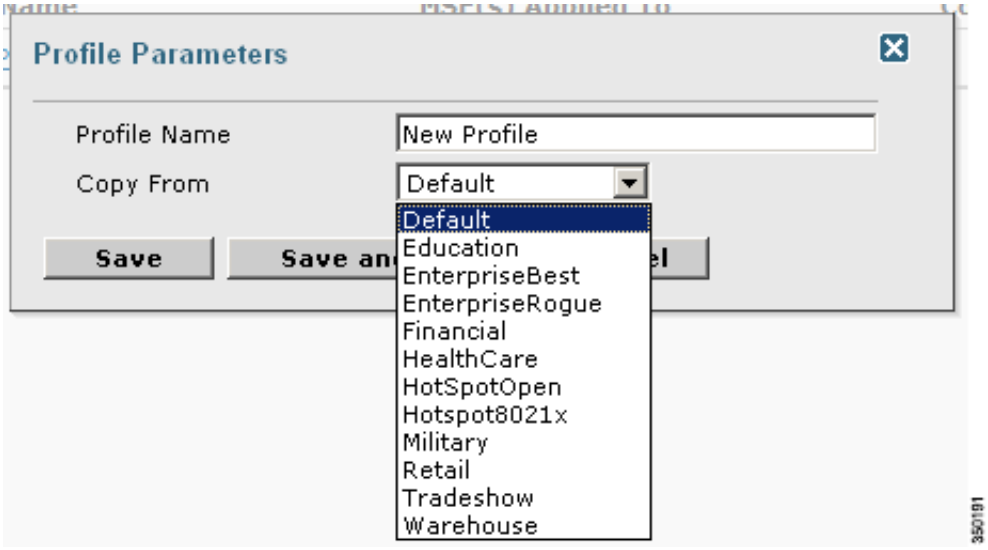


左側の [Profile List] をクリックします。

右上のドロップ ダウン メニューの [Add Profile] を選択します。

ステップ 3　プロファイル テンプレートの選択:

Cisco 適応型ワイヤレス IPS システムには、一連のプロファイル テンプレートがあらかじめ定義されており、お客様はそれらを開始点として使用して、独自のカスタム プロファイルを作成できます。各プロファイル テンプレートは、特定の垂直産業に合わせて作成されており、どの特定のアラームが有効にされているかに関してはさまざまに異なります。

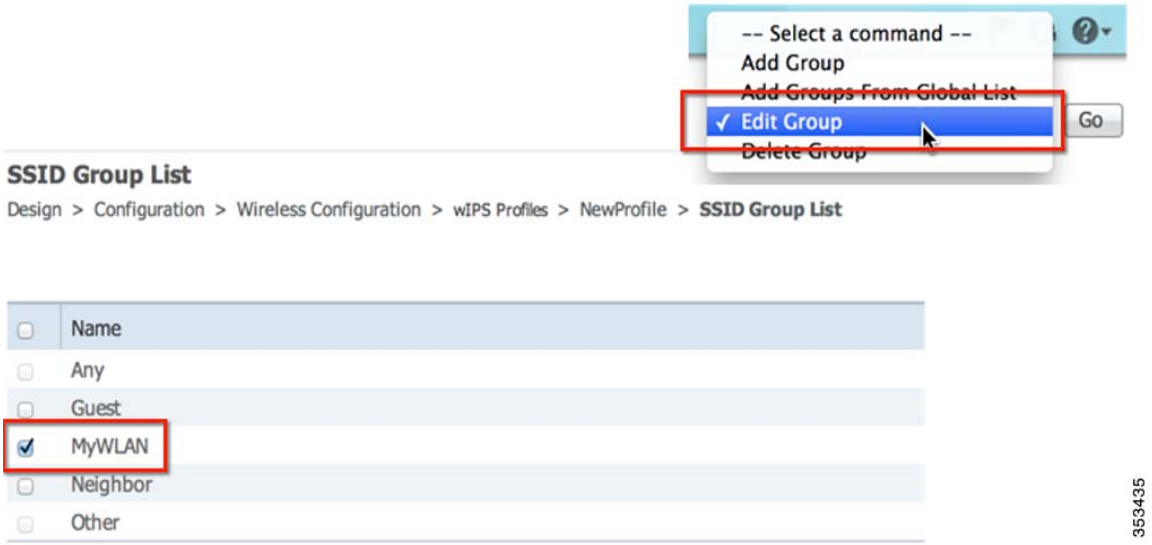


プロファイルを選択し、名前を指定したら、[Save and Edit] をクリックします。

ステップ 4　SSID のモニタへの設定（任意）:

デフォルトで、ローカル ワイヤレス LAN インフラストラクチャ（同じ RF グループ名を持つ AP によって定義された）に対して仕掛けられた攻撃が監視されます。オーバーレイ構成モデルで構成する場合など、他のネットワークに対する攻撃を監視させる必要がある場合は、SSID グループ機能を使用する必要があります。

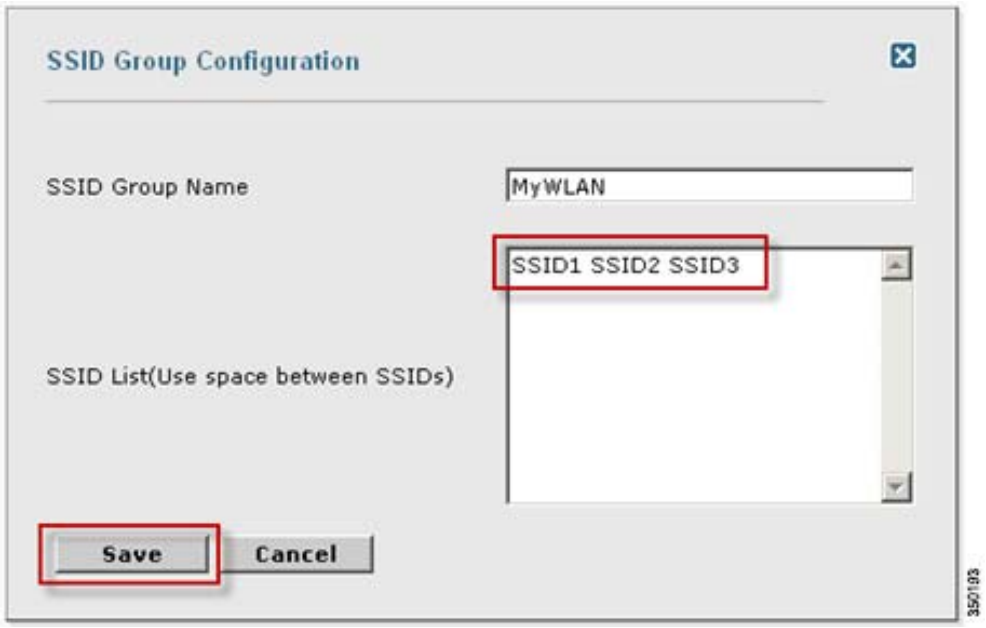
この手順が必要ない場合は、単に [Next] をクリックします。



[MyWLAN] の横のボックスをオンにして、右上隅のドロップ ダウンから [Edit Group] を選択し、[Go] をクリックします。

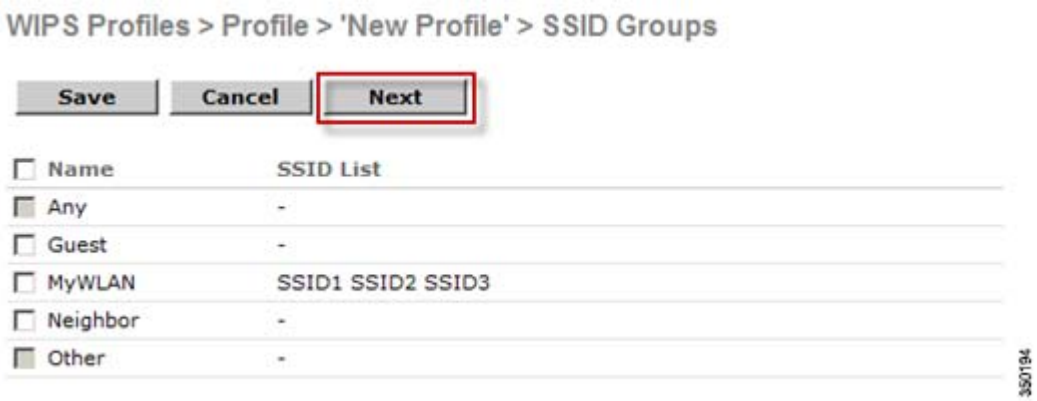
ステップ 5　SSID のモニタへの入力（任意）：

ここでも、この手順は、オーバーレイ構成モデルで一般的な別の WLAN インフラストラクチャに対する攻撃を監視するためにシステムが使用される場合にのみ必要です。



SSID（複数の場合は、1 つのスペースで区切る）を入力し、[Save] をクリックします。

[SSID Groups] ページは次のスクリーン ショットのようになり、SSID が正常に追加されたことを確認します。

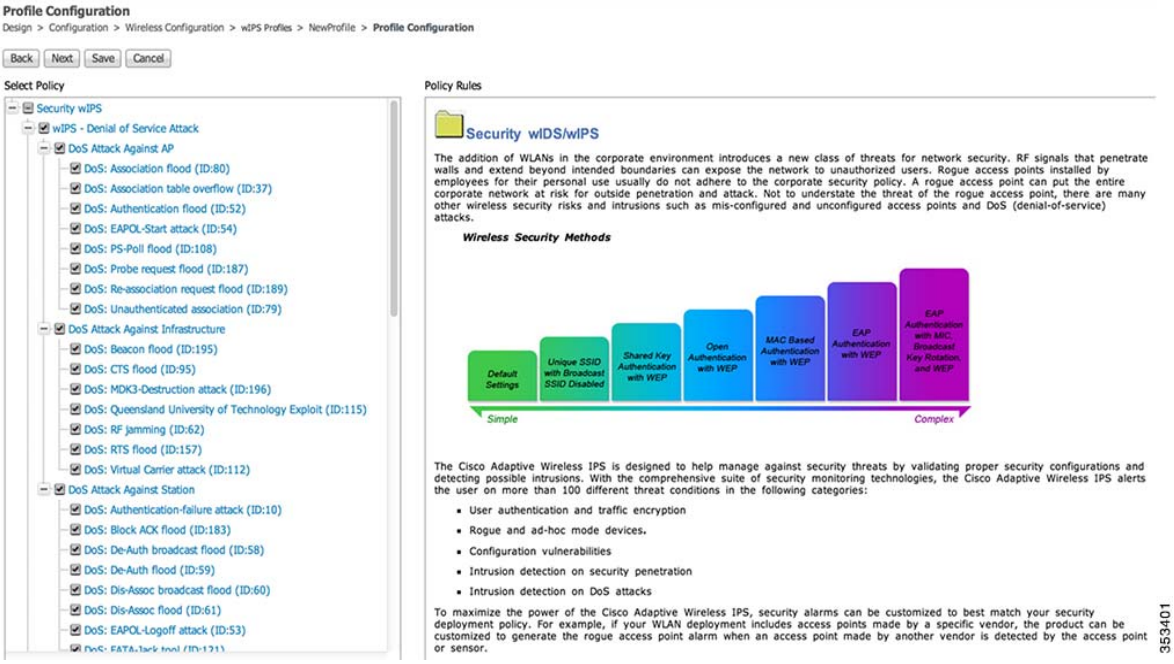


[Next] をクリックします。

ステップ 6　プロファイルの編集:

この設定画面では、特定の攻撃を有効または無効にできます。さらに、管理者は特定のアラームをドリル ダウンし、それらの特定のしきい値を編集したり、フォレンジックを有効にしたりすることもできます。

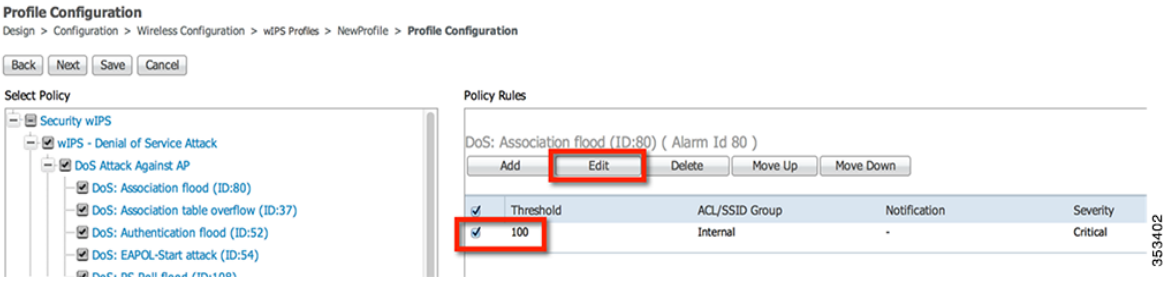
アラームを有効または無効にするには、目的の特定のアラームの横のボックスをクリックするだけです。



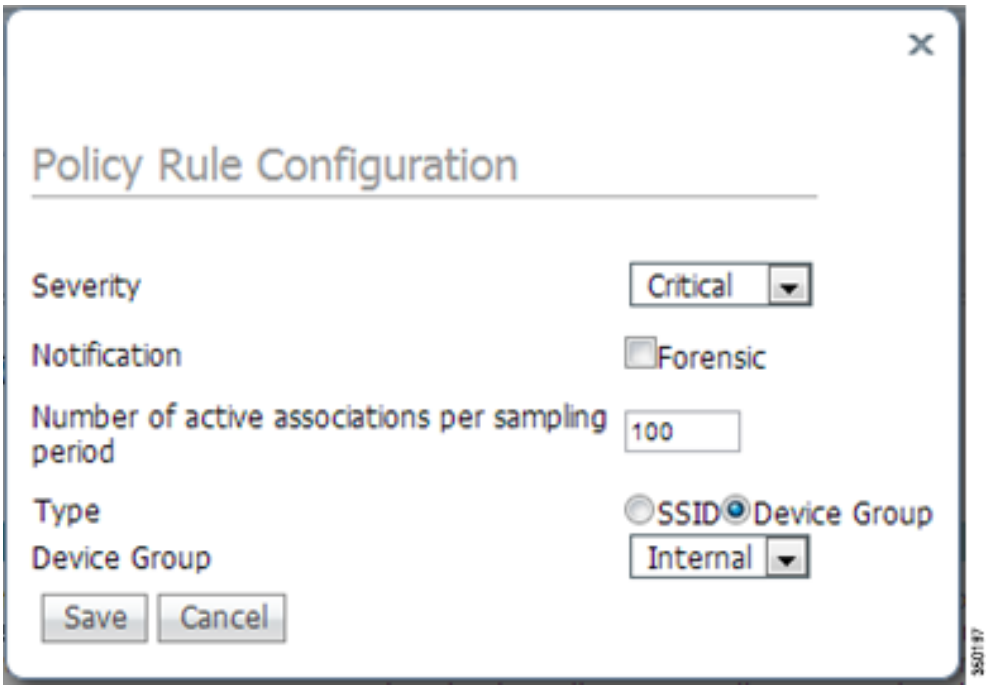
ポリシー パラメータを編集するには、アラームをクリックすると、右側のフレームが変更され、その攻撃のポイント設定が表示されます。

ステップ 7　ポリシー規則の編集:

特定のアラームを選択したら、そのアラームに関連付けられているポリシー ルールを変更できます。



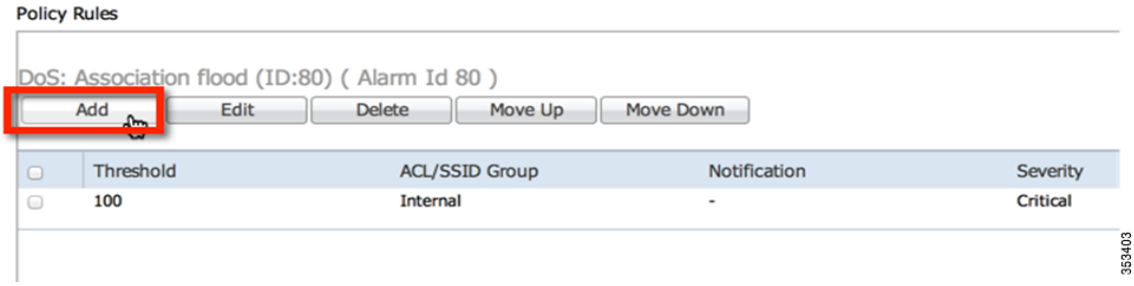
ポリシー ルールを編集するには、ルールの横のボックスをオンにし、[Edit] をクリックします。



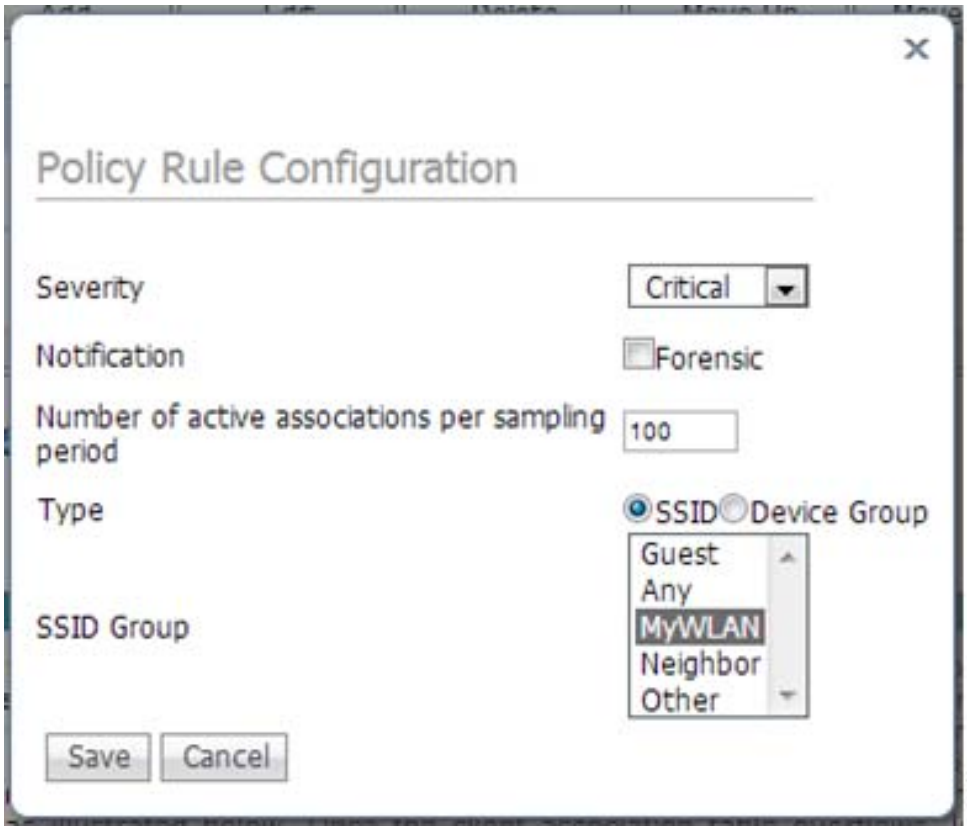
ポリシー ルール ウィンドウでは、多数のその他のパラメータに加え、アラームの重大度を変更できます。通知項目は、この特定のアラームにフォレンジック（パケット キャプチャ）を採用するかどうかを定義するチェックボックスです。さらに、このアラームの特定のしきい値もあり、この例ではアクティブなアソシエーション数として定義されていますが、これはアラームごとに異なります。次に、タイプ パラメータで、システムに攻撃を監視させる WLAN インフラストラクチャを定義します。デフォルトで、これは [Device Group] と [Internal] に設定され、ワイヤレス IPS AP と同じ「RF グループ」名のすべての AP を指定します。タイプを [SSID] に変更すると、オーバーレイ構成に一般的な個別のネットワークを監視させることができます。この構成については後述します。

ステップ 8　ポリシー ルールの追加（任意）：

ポリシー ルールの編集は、一般に、SSID によって別の WLAN インフラストラクチャを監視するように構成されるオーバーレイ構成でだけ必要になります。



ポリシー ルールを追加するには、[Add] をクリックします。

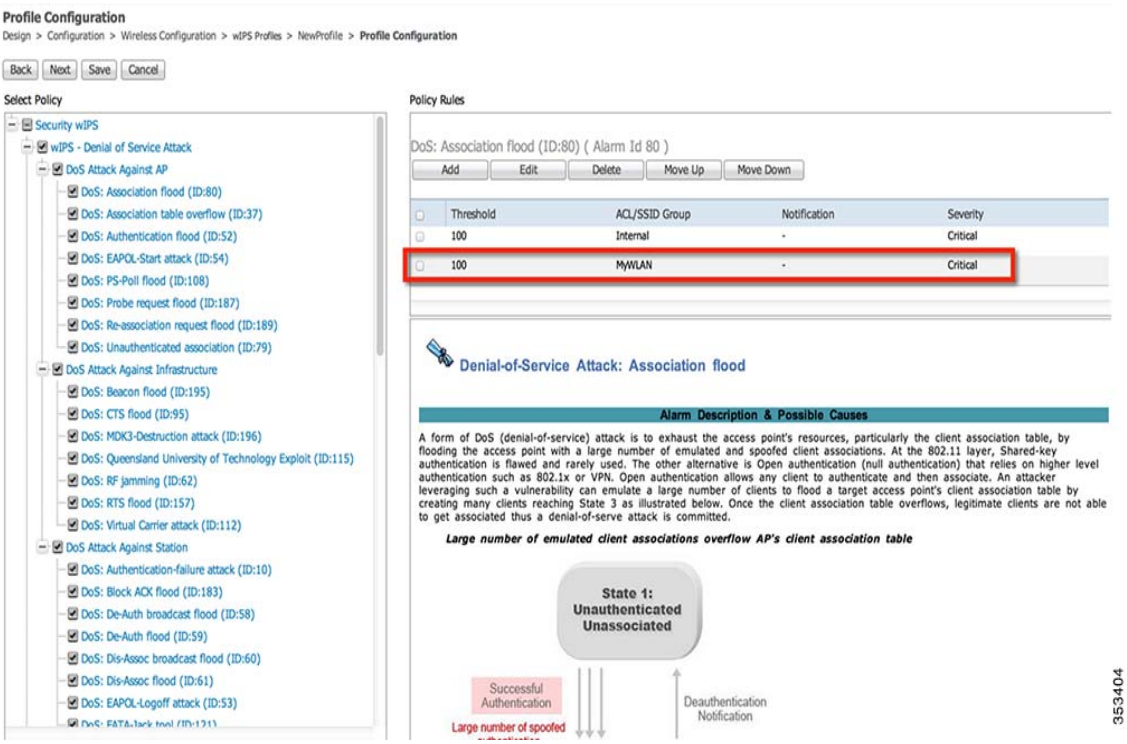


ポリシー ルール ウィンドウでは、多数のその他のパラメータに加え、アラームの重大度を変更できます。通知項目は、この特定のアラームにフォレンジック（パケット キャプチャ）を採用するかどうかを定義するチェックボックスです。さらに、このアラームの特定のしきい値もあり、この例ではアクティブなアソシエーション数として定義されていますが、これはアラームごとに異なります。次に、タイプ パラメータで、システムに監視させる SSID を定義します。タイプを [Device Group] に変更すると、システムは同じ「RF グループ」の AP に対する攻撃のみを監視します。[SSID] を選択している場合、先にセットアップで SSID グループによって定義したとおりに、システムを使用して、個別の WLAN インフラストラクチャに対する攻撃を監視することができます。

変更したら、[Save] をクリックします。

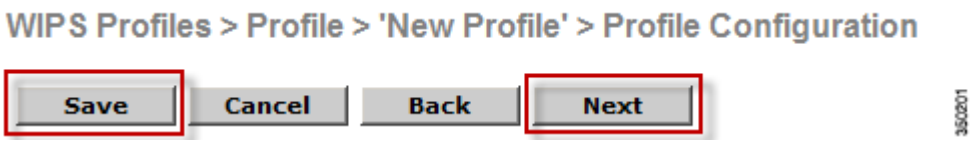
ステップ 9　追加のポリシー ルールの設定(任意):

SSID によって別の WLAN インフラストラクチャを監視するようにシステムを設定した場合、SSID によって監視するように、すべての各ポリシー ルールを変更する必要があります。個別の各アラームに、システムで以前に作成した SSID グループに対する攻撃を監視するように定義したポリシー ルールを作成する必要があります。



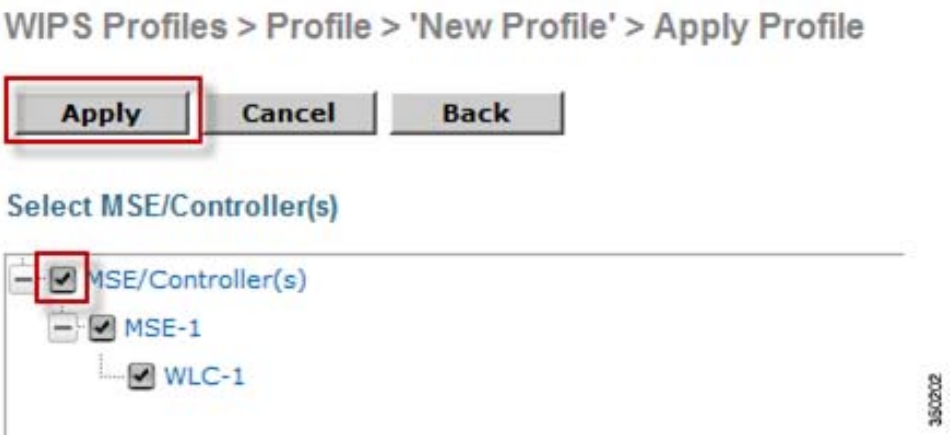
ステップ 10　プロファイルの保存:

変更したら、[Save] をクリックして、Prime Infrastructure のプロファイルを保存し、完了したら [Next] をクリックします。



ステップ 11　プロファイルの適用:

プロファイルを適用する MSE/コントローラの組み合わせを選択して、[Apply] をクリックします。



コントローラベースの IDS を無効にする

システムでワイヤレス IPS が有効化されている場合、IDS は自動的に無効化されます。したがって、ユーザが IDS を有効にする場合は、ワイヤレス IPS のサブモードを無効にする必要があります。

コントローラ ベースの IDS の無効化:

ステップ 1　コントローラにログインします。

ステップ 2　トップレベル コントローラ メニューの [Security] タブをクリックします。

ステップ 3　左側で、[Wireless Protection Policies] > [Standard Signatures] をクリックします。

ステップ 4　以下のスクリーンショットに示すように、標準シグニチャのチェックボックスをオフにします。

適応型ワイヤレス IPS 管理のベスト プラクティス

適応型ワイヤレス IPS のシグネチャについて

CUWN リリース間での aWIPS シグネチャの互換性

WLC および MSE のリリース 7.5 から 8.0 まで、新しい aWIPS シグネチャと、緩和アクションなどの拡張 aWIPS 機能が追加されています。

参照してください MSE、PI、WLC の間の互換性のあるリリースの組み合わせは、次の表最初に、aWIPS シグニチャのサポートに関して。

MSE のリリース	PI のリリース	コントローラのリリース
7.4	1.3、2.0、2.1	7.4
7.5	1.4	7.5
7.6	1.4.1	7.6
8.0	2.2	8.0

aWIPS を適切に調整するためには、最初に利用可能な設定オプションと推奨設定を理解しておく必要があります。

重大度

aWIPS アラームの重大度は、セキュリティ脅威レベルと、ワイヤレスの本番ネットワークに対する運用上の影響に基づいて設定されています。例えば、ほどんどの DoS 攻撃が、ワイヤレス インフラストラクチャに運用上の影響を与える可能性があります。したがって、重大度はデフォルトで [Critical] に設定されています。デフォルトの重大度レベルを変更する必要はありませんが、InfoSec とセキュリティの監視チームの綿密な内部調査とレビューが実施されていれば、臨機応変に変更できます。

オブジェクトのモニタリング

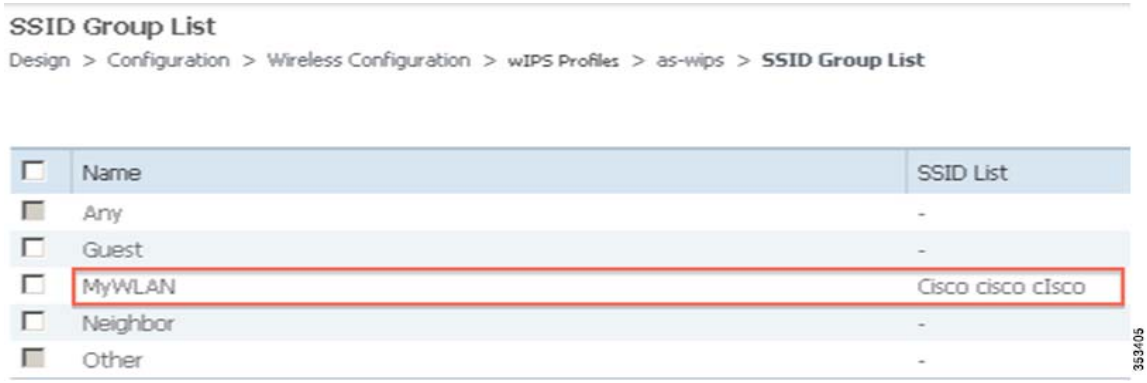
オブジェクトのモニタリングには、SSID グループとデバイス グループの 2 つのタイプがあります。シグネチャに応じて、いずれも設定しないことも、1 つを設定することも、両方を設定することもできます。

デバイス グループは、管理者が aWIPS 攻撃に対して監視する デバイスの MAC アドレスのリストです。AP や関連クライアントなどのインフラストラクチャ デバイスに固有の攻撃の監視として最も効果的なのは、監視対象のデバイス グループとして [Internal] オプションを選択することです。

特定の SSID グループが設定されている場合は、SSID に固有の攻撃に対して SSID のリストが監視されることを意味します。これらのアラームを正確に監視するためには、この SSID のリストを特定の SSID グループ内で設定し、後にシグネチャ設定で参照できるようにすることが重要です。

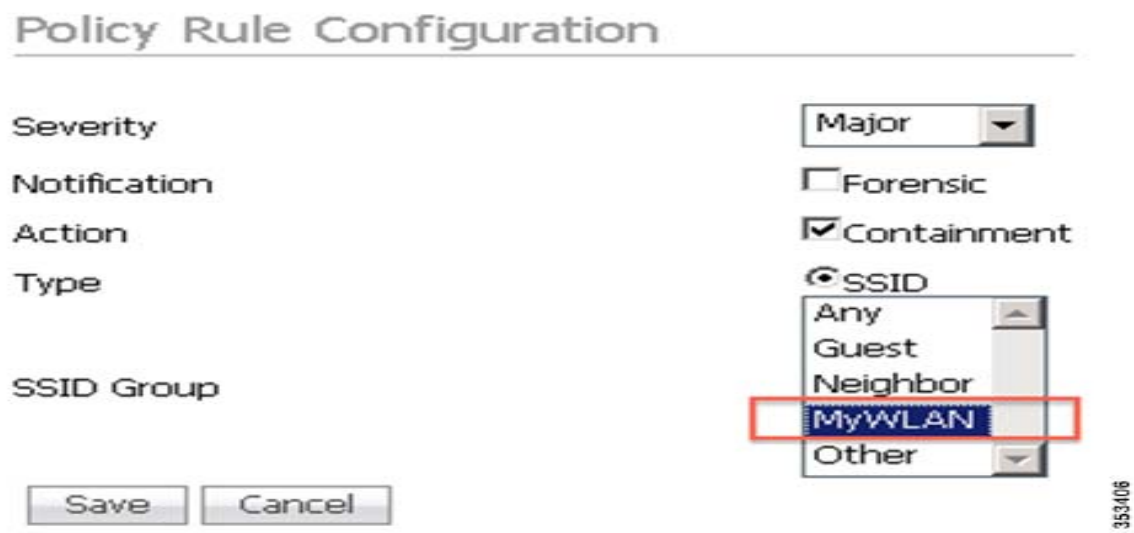
[Honeypot AP detected] シグネチャを設定し、**Cisco**、**cisco**、**cIsco** の SSID が監視されるようにするには、以下の 2 つの手順を実行します。

ステップ 1　指定した SSID である **Cisco**、**cisco**、**cIsco** が、ワイヤレス IPS プロファイルの SSID グループ リストの **MyWLAN** などの SSID グループ内で設定されていることを確認します。



(注)　SSID 名の設定では、まだ正規表現がサポートされていません。

ステップ 2　ワイヤレス IPS プロファイルの [Profile Configuration] ページで、[Honeypot AP detected] シグネチャをハイライトし、以下のスクリーンショットのように [MyWLAN] SSID グループが含まれていることを確認します。



(注)　[Honeypot AP detected] シグネチャ攻撃は、オープンな認証で指定した SSID のみを検出できます。SSID グループに [Any] を選択した場合、設定した SSID または SSID グループのみではなく、すべての SSID によってアラームがトリガーされます。監視する SSID の範囲に影響を与えるため、管理者は慎重に SSID グループを変更する必要があります。

通知

[Forensic] は、アラーム設定の [Notification] の唯一のオプションです。トラブルシューティングおよび分析用 aWIPS アラームをトリガーした無線のパケットをキャプチャすることを意味します。

すべてのアラームに対して [Forensic] を有効にすることは推奨されません。それによって、特に WLC と MSE が別々の場所に配置され、WAN リンクを介して通信している場合は aWIPS アラーム関連のトラフィックのスループットが大幅に増加する可能性があるためです。ただし、[Forensic] オプションは、トラブルシューティングおよびアラームの精度検証の目的で、特定のアラームに対して有効にできます。

キャプチャされたフォレンジック ファイルがトラブルシューティングのための十分でない場合、管理者はサードパーティ製のスニッフィング ツール（AirMagnet Wi-Fi Analyzer や Wireshark AirPcap など）を使用して、より長い期間をキャプチャできます。

スニッフィング ツールを所有していない場合、Cisco TAC はキャプチャに向けて OmniPeek Remote Assistant（ORA）を提供しています。

スニッフィング ツールによってトラフィックをキャプチャするために、管理者は以下の手順を実行できます。

1. トリガーされたアラームからアラームの MAC、レポート AP、最後のレポート時間、また該当する場合はアラーム チャネルを見つけます。
2. 特に繰り返し発生するアラームの場合は、最後のレポート時間に近いサイト訪問時間を計画します。
3. レポート AP のエリアで、または近いエリアでキャプチャを開始します。
4. 以下の 2 つのキャプチャを取得します。
   a. 2.4 GHz と 5 GHz 内のすべてのチャネルを有効にし、最低でも 30 分間キャプチャし、キャプチャを保存します。このキャプチャを実行できないスニッフィング ツールもあることに注意してください。
   b. アラーム チャネルに焦点を当て、最低でも 30 分間キャプチャし、キャプチャを保存します。

十分あトレースを収集したら、詳細な分析のために Cisco TAC にファイルを送信します。

アクション

Action は、攻撃が検出された際に aWIPS によって実行される緩和アクションを指します。現時点では、Cisco aWIPS にはロケーション、自己免疫、ブラックリスト、封じ込めの 4 つの緩和アクションがあります。最後の 3 つのアクションは、WLC および MSE のリリース 7.5 または 7.6、および PI リリース 1.4 または 1.4.1 でのみ利用可能です。

参照先

他のスキームが指定されていない限り、ほとんどの aWIP アラームにとって、ロケーションが引き続き唯一の利用可能な緩和スキームです。この緩和オプションは、明示的に設定可能ではありません。MSE によってホストされる他のサービスを利用し、コンテキストを認識して攻撃者またはアラーム ソースを特定して、後で物理的に除去できるようにします。

自動免疫

一部の DoS 攻撃では、潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するようにワイヤレス IPS を誘導する場合があります。これにより、コントローラは正規のクライアントから切断されます。自己免疫機能は、攻撃者が作成したパケットを無視し、正規のクライアントを切断から保護するために設計されています。現在、自己免疫アクションをサポートしているのは以下の攻撃のみです。

- DOS：再アソシエーション要求フラッド

(注)　ローミング中に通信を中断してしまうため、特に Cisco 792x フォンの展開では自己免疫を有効にすることは推奨されません。

ブラックリスト

自己免疫とは異なり、ブラックリストはより積極的な緩和アクションで、特定した攻撃デバイスが最初に接続された場合はその認証を解除します。これにより、デバイスがブラックリストにある限り、その後のデバイスからのトラフィックをすべて無視します。現在、以下の攻撃でブラックリスト アクションがサポートされています。

- 疑わしい after-hours トラフィックの検出
- 偽の DHCP サーバの検出
- ベンダー リストによる未承認アソシエーション
- DNS トンネルバイパスの検出
- ICMP トンネルバイパスの検出

封じ込め

ワイヤレス IPS 攻撃の封じ込めアクションは、不正な AP の封じ込めに似ています。SSID に関連する攻撃の封じ込めを開始し、正規のクライアントが攻撃者が設定した SSID に接続されることを防ぎます。現在、以下の攻撃で封じ込めアクションがサポートされています。

- ソフト AP またはホスト AP の検出
- Airsnarf 攻撃の検出
- ハニーポット AP の検出
- Hotspotter ツールの検出
- Karma ツールの検出
- デバイス ブロードキャスト XSS SSID

しきい値

一部の aWIPS はしきい値に基づいています。つまり、フレーム/パケットがサンプリング期間のしきい値を超えると、アラームがトリガーされます。Cisco ワイヤレス IPS のサンプリング期間は 1 分間です。これは、ワイヤレス IPS AP の累積滞在時間です。

ワイヤレス IPS を使用したローカル モードの AP は、オフチャネルのスキャンに 50 ミリ秒しか使いません。攻撃がオフチャネルの場合は長い時間がかかります。ELM がオフチャネルの攻撃に対して最善の努力しか提供できないのはこのためです。オフチャネルの攻撃を検出するには、モニタリング モード（MM）の AP を使用することをお勧めします。一方、ELM でチャネル時間のほとんどの動作であるために、MM AP よりも迅速なチャネルの攻撃を検出します。

最善の結果を得るためには、WSM モジュールを搭載した ELM AP が、ワイヤレス IPS 導入に向けた推奨ソリューションです。しきい値に基づいたアラームは、しきい値ベース以外のものと比較して、誤検出が多くなる傾向にあります。ただし、しきい値に基づいた一部のアラームは、アウト オブ シーケンス（OOS）の論理も考慮に入れることで、アラームの精度を向上できます。したがって、これらのアラームは管理者の監視、レビュー、調整対象となります。

忠実度

忠実度は、従来の Cisco aWIPS ドキュメンテーションまたは aWIPS ユーザ インターフェイスに不足していた重要な属性です。これは、シグネチャの精度の信頼度レベルの尺度です。ワイヤレス IPS の忠実度レベルは、以下のように、精度の割合に応じて 5 つのカテゴリに分類できます。

- 非常に高い > 95 %
- 高い > 80 %
- 中程度 > 60 %
- 低い < 50 %
- 非常に低い

忠実度のメトリック値が高ければ高いほど、レポートされるシグネチャ アラームが正確であることを意味します。高い忠実度のシグネチャには固有の検出ロジックのパターンがあり、低い忠実度のシグネチャはさまざまな誤検出条件によってトリガーされる可能性があります。したがって、このメトリックは、管理者がワイヤレス IPS の攻撃の監視または緩和に優先順位を付けるために重要です。

aWIPS の監視および調整

以下は、ワイヤレス IPS のプロファイルに関するいくつかの誤解です。

1. あらゆる組織に最適な万能のワイヤレス IPS プロファイルはありません。各組織のワイヤレス環境は異なるためです。同じ組織でも、ワイヤレス環境は時間とともに変化します。ワイヤレス IPS プロファイルは、ワイヤレス IPS アラームによって環境に合わせてカスタマイズする必要があります。シスコでは、金融、小売り、エンタープライズなど、異なる業種に基づいたワイヤレス IPS のテンプレートを提供しています。ただし、これらは管理者が利用を開始するための基準に過ぎません。
2. 各テンプレートに対してデフォルトで有効化されているシグネチャを除いては、さまざまな業種のワイヤレス IPS テンプレートに違いはありません。各業種のワイヤレス IPS テンプレートのしきい値に基づいたアラームについては、しきい値の設定に違いはありません。

推奨ガイドライン

以下の表には、有効にすることが推奨される aWIPS シグネチャと、忠実度およびデフォルトの重大度設定（ソフトウェア リリース 8.0 に基づく）を記載しています。

アラーム名	アラーム ID	忠実度	アラームの重大度
Airsnarf 攻撃	102	非常に高い（Very high）	Major
不良 EAP-TLS フレーム	181	大きい	警告

アラーム名	アラーム ID	忠実度	アラームの重大度
Broadcom RSN 範囲外攻撃	223	非常に高い（Very high）	Major
クラック可能な WEP IV キーの使用	38	大きい	Major
デバイスのセキュリティ異常による Day-Zero 攻撃	133	大きい	Major
WLAN のセキュリティ異常による Day-Zero 攻撃	135	大きい	Major
デバイス ブロードキャスト XSS SSID（ID：210）	210	非常に高い（Very high）	[Critical]
選択された認証方法によって保護されていないデバイス（ID：261）	261	大きい	Major
DNS トンネルバイパスの検出（ID：216）	216	大きい	Major
DoS：アソシエーション テーブル オーバーフロー	37	非常に高い（Very high）	[Critical]
DoS：認証フラッド	52	Medium	[Critical]
DoS：認証失敗攻撃	10	中規模	[Critical]
DoS：ビーコン DS 設定 DoS	222	大きい	[Critical]
DoS：ビーコン フラッド	195	Medium	警告
DoS：ブロック ACK フラッド	183	大きい	警告
DoS：CTS フラッド	95	Low	[Critical]
DoS：De-Auth ブロードキャスト フラッド	58	Medium	[Critical]
DoS：De-Auth フラッド	59	Medium	[Critical]
DoS：Dis-Assoc ブロードキャスト フラッド	60	Medium	[Critical]
DoS：Dis-Assoc フラッド	61	Medium	[Critical]
DoS：EAPOL-Logoff 攻撃	53	大きい	[Critical]
DoS：EAPOL-Start 攻撃	54	Medium	[Critical]
DoS：FATA-Jack ツール	121	非常に高い（Very high）	[Critical]
DoS：MDK3-Destruction 攻撃（ID：196）	196	非常に高い（Very high）	[Critical]
DoS：Premature EAP-Failure	57	大きい	[Critical]
DoS：Premature EAP-Success	56	大きい	[Critical]
DoS：プローブ要求フラッド	187	Low	警告
DoS：PS-Poll フラッド	108	Medium	[Critical]
DoS：RTS フラッド	157	Low	[Critical]
DoS：仮想キャリア攻撃	112	大きい	[Critical]
802.1x 認証に対する EAP 攻撃	117	大きい	Major
偽の AP の検出	89	Medium	Major

アラーム名	アラーム ID	忠実度	アラームの重大度
ハニーポット AP の検出	118	非常に高い（Very high）	Major
Hotspotter ツールの検出	124	大きい	Major
Identical Send and Receive Address	178	大きい	警告
Improper Broadcast Frames	179	大きい	警告
Karma ツールの検出（ID：197）	197	大きい	Major
Karmetasploit 攻撃の検出（ID：214）	214	大きい	Major
プローブ要求ファジングフレームの検出（ID：219）	219	Medium	Major
プローブ応答ファジングフレームの検出（ID：220）	220	Medium	Major
ソフト AP またはホスト AP の検出	99	Medium	Major
スプーフされた MAC アドレスの検出	35	大きい	Major
WEP IV キーの再利用	2	大きい	Major
WiFiTap ツールの検出（ID：198）	198	大きい	Major

管理者は、以下のように、上記の表を監視と調整の一般的なガイダンスとして参照できます。

1. InfoSec およびセキュリティ インシデント監視チームとの内部レビュー後に、組織で監視する重要なアラームのサブグループを特定し、対応する緩和計画を立てる。
2. [Honeypot AP detected] シグネチャなど、高い重大度（「メジャー」以上）と高い忠実度（「高い」以上）の組み合わせのアラームに焦点を当てる。管理者は、必要に応じて詳細な検証のためにパケット トレースを収集し、これらのアラームに対して緩和を開始する必要があります。
3. 低い重大度（「マイナー」以下）または低い忠実度（「中程度」以下）のアラームに対する選択的努力に焦点を当てる。管理者が優先順位リストを作成するためには、最初にこれらのアラームのセキュリティと運用に対する影響を理解する必要があります。このリストによって、管理者は必要に応じて検証および緩和に優先順位を付けることができます。例えば、**DoS：De-Auth フラッド**アラームはこのようなアラームの 1 つです。しきい値に基づいているため、忠実度レベルは**中程度**です。ただし、この攻撃は正規のクライアントを切断するため、重大度は**クリティカル**です。このようなアラームが発生した場合、管理者はトラブルシューティングを実施して、誤検出かどうかを検証する必要があります。その後、必要に応じて緩和を実施します。
4. 低い重大度（「マイナー」以下）および低い忠実度（「中程度」以下）の組み合わせのアラームを無視する。例えば、**NetStumbler の検出**アラームはこのようなアラームの 1 つです。実際の経験から、多くのプローブ要求を送信する**口数の多い**クライアントによって容易にトリガーされることが想定されます。これはしきい値に基づくアラームです。トリガーされた場合でも、Netstumbler ツールを使用するデバイスが検出されるとは限りません。管理者は、このアラームを無視するかオフにしてもほとんど問題ありません。
5. 必要に応じてしきい値に基づくアラームをオンにする。前述したように、しきい値の基づくアラームによって誤検出がトリガーされる傾向にあります。管理者は、いくつかの誤検出シナリオに対してしきい値を調整する必要があります。例えば、**DoS：CTS フラッド** アラームはこのようなアラームの 1 つです。802.11n と 802.11n 以外のデバイスを組み合わせて展開している場合、802.11n 以外のデバイスに向けた保護スキームの CTS-to-Self フレームは、このアラームに対して誤検出をトリガーする傾向にあります。このような場合、管理者はしきい値を増加し、今後このアラームがトリガーされることを避ける必要があります。

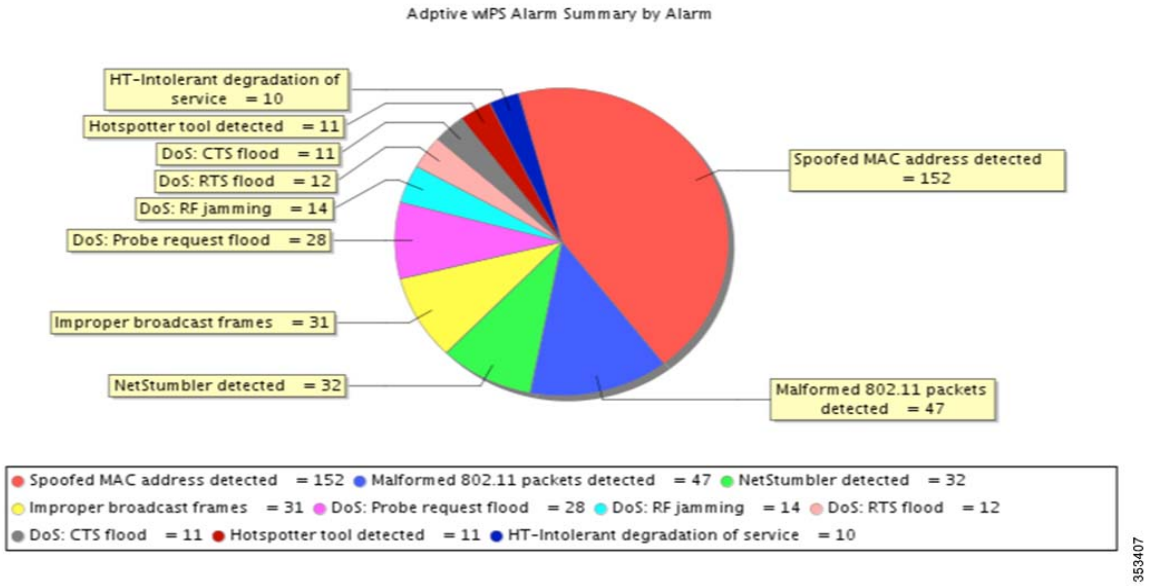
6. 自動の緩和アクションは、高い重大度(「メジャー」以上)と高い忠実度(「高い」以上)の組み合わせに対してのみ実装することをお勧めします。例えば、**ハニーポット AP の検出**アラームをトリガーする、企業 SSID を使用するデバイスに対しては、管理者は緩和を自動化するアクションとして**封じ込め**を実装できます。一方で、**Hotspotter ツールの検出**で重大度が**マイナー**の場合などは、**封じ込め**アクションを実装する必要はありません。
7. ワイヤレス IPS アラームのトレンドと履歴を分析し、基準として「常連のエラー」を特定します。その後、必要に応じてトラブルシューティング、調整、緩和を実施します。

ワイヤレス環境の動的な性質を考慮すると、ワイヤレス IPS の監視と調整は継続的なプロセスです。ワイヤレス IPS のトレンドと履歴を分析するには、以下の 2 つの方法を使用できます。

- ワイヤレス IPS アラームに向けた PI のネイティブ レポート テンプレートを活用する。
- PI のノース バウンド通知レシーバとして、サードパーティ製セキュリティ情報とイベント管理 (SIEM) を使用します。

このドキュメントでは、PI のネイティブ レポート テンプレートを使用してワイヤレス IPS アラームのトレンドと履歴を分析する方法を説明します。

PI では、[Report] > [Report Launch Pad] > [Security] > [Adaptive wIPS Alarm Summary] から、一定期間の aWIPS アラームの概要を生成できます。



上記の図は、シスコのラボ環境の、過去 4 週間の aWIPS アラーム概要のスナップショットです。この環境では、**スプーフされた MAC アドレスの検出**カウントは、合計アラーム数の約 50% です。最初に、これは**高い**忠実度と**メジャー**の重大度のアラームです。上記の一般的なガイドラインの 2 番によれば、管理者はトラブルシューティングを実施し、過去 4 週間で非常に頻繁にトリガーされた理由を見つける必要があります。分析のためのトレースを収集するために、管理者はまずこのアラームの [Forensic]を有効にできます。それでも十分ではない場合、検出された AP とレポートのエリアを特定し、これらの AP に対して**グローバル フォレンジック キャプチャ**を開始して、より多くのトレースを収集する必要があります。また、Cisco TAC と協力してトレースを分析し、トラブルシューティングを実施することもできます。

ヒント

実際の経験とフィードバックに基づいて、管理者は以下のヒントを使用して、このセクションで一部のワイヤレス IPS アラームを調整できます。特に指定されない限り、これらの推奨事項はすべての条件に適用されることに注意してください。

オフにするか無視するアラーム:

- プローブ要求およびしきい値によってトリガーされるアラーム。

  モバイル デバイスはプローブ要求に関して非常に口数が多く、このタイプのアラームが頻繁にトリガーされます。これらのアラームによっては、運用上の影響は発生しません。

  - DoS:プローブ要求フラッド
  - AP のデバイス プローブ
  - NetStumbler の検出
  - NetStumbler 犠牲者の検出

- 特定の暗号化または認証に基づくアラーム。

  WEP 暗号化がワイヤレスの本番環境に実装されていない場合:

  - 暗号化が無効な AP
  - 暗号化が無効なクライアント
  - WEP IV キーの再利用
  - オープン認証を使用するデバイス
  - クラック可能な WEP IV キーの使用
  - 共有キー認証を使用するデバイス
  - 高速 WEP クラック ツールの検出
  - ChopChop 攻撃
  - フラグメンテーション攻撃

  LEAP 認証がワイヤレスの本番環境に実装されていない場合:

  - ASLEAP ツール検出

- スペクトラム分析に基づくものの、Cisco CleanAir ソリューションがあるアラーム

  ワイヤレスの本番環境に Cisco CleanAir 対応の AP がある場合、CleanAir ソリューションによって、きめ細かく正確なスペクトラム レポートおよび分析が提供されます。これは、この目的に向けた推奨ソリューションでもあります。

  - DoS:RF Jamming
  - DoS:Queensland University of Technology Exploit

- 特定の機能または時間に基づくアラーム:

  - 疑わしい営業時間外のトラフィックの検出。

  24 時間稼働の施設の場合は、このアラームを有効にする必要はありません。

  - PSPF 違反の検出

ワイヤレスの本番ネットワークに P2P ブロックが必要ではない場合は、このシグネチャを有効にしてピア ツー ピア通信を検出する必要はありません。

- 旧式の可能性があるアラーム:

  以下のアラームはワイヤレス デバイスにクラッシュを引き起こす可能性がある攻撃を検出するために使用されるため、旧式となっている可能性があります。このタイプの攻撃は、非常に旧式のドライバを搭載するワイヤレス クライアントに対してのみ有効であり、そのようなクライアントは現在のエンタープライズ ワイヤレス ネットワークではほとんど見られません。また、当社の導入経験に基づいても、シスコのワイヤレス デバイスにも影響を与えません。したがって、これらを無効にすることをお勧めします。

  - 不正 802.11 パケットの検出
  - 不正なビーコン
  - ビーコン ファジング フレームの検出
  - プローブ要求ファジング フレームの検出
  - プローブ応答ファジング フレームの検出

- RF 環境に基づき、不要な誤検出を引き起こす可能性のあるアラーム:

  - 未承認アソシエーションの検出

  一般的に、関連するワイヤレス クライアントを管理対象外の SSID に接続することを許可する場合、このアラームは無効にできます。特に小売りおよびパブリック Wi-Fi での導入では、ユーザに Wi-Fi ゲスト サービスを提供する場合、このアラームを有効にしていると頻繁にトリガーされます。ユーザが隣接する Wi-Fi ネットワークに接続する可能性があるためです。

  - Hotspotter ツールの検出

  このアラームは、既知のホットスポット（attwifi など）が検出されると必ずトリガーされます。キャリアまたは小売店による実際のホットスポットの可能性もありますが、ハッカーがワイヤレス クライアントを誘導するために設定した偽のホットスポットの可能性もあります。施設の周辺に実際のホットスポットがある場合、特に小売りやパブリック Wi-Fi での導入では、このアラームを無効にして不要に生成される誤検出を無視できます。

調整が必要なアラーム

- しきい値に基づくアラーム:

  - DoS：CTS フラッド

  802.11n および 802.11n 以外のデバイスが混合で展開されている場合、このアラームが頻繁にトリガーされる可能性があります。実際に DoS 攻撃が発生しているとは限りません。管理者は、環境に基づいてしきい値を増加できます。

  - DoS：RTS フラッド

  CTS フラッドと同様に、このアラームでも誤検出が多くなる可能性があります。しきい値を増加する必要があります。

- SSID に基づくアラーム:

  - ハニーポット AP の検出

  管理者が独自の SSID を使用するデバイスのみを管理する場合、前のセクションの例のように、監視する SSID グループで SSID を設定する必要があります。

  - ソフト AP またはホスト AP の検出

これは、すべての SSID を監視するためのデフォルトのアラームです。最初に、クライアントがワイヤレス インフラストラクチャに関連付けられるとトリガーされ、後で AP モードに切り替わるとトリガーされます。管理者が独自の SSID を使用するデバイスのみを管理する場合、独自の SSID がある特定の SSID グループを変更する必要があります。

ライセンス/オーダー情報

Cisco 適応型 ワイヤレス IPS は、シスコ モビリティ サービス エンジン上のライセンス型ソフトウェア機能セットです。以下の表は、適応型ワイヤレス IPS に利用可能なライセンス レベルを示しています。

表 1-1　Cisco ワイヤレス IPS ソフトウェア ライセンス

ライセンスの SKU	説明
L-WIPS-MM-1AP	1 つのモニタ モードのアクセス ポイントに向けたライセンス
L-WIPS-MM-100AP	100 個のモニタ モードのアクセス ポイントに向けたライセンス
L-WIPS-MM-1000AP	1000 個のモニタ モードのアクセス ポイントに向けたライセンス
L-WIPS-ELM-1AP	1 つのワイヤレス IPS を使用したローカル モードのアクセス ポイントに向けたライセンス
L-WIPS-ELM-100AP	100 個のワイヤレス IPS を使用したローカル モードのアクセス ポイントに向けたライセンス
L-WIPS-ELM-1000AP	1000 個のワイヤレス IPS を使用したローカル モードのアクセス ポイントに向けたライセンス

（注）　WSM モジュールは、L-WIPS-MM を使用します。さらに、ワイヤレス IPS 攻撃のロケーションや、不正なアクセス ポイントまたはクライアントのロケーションが必要な場合は、お客様はこれらのロケーションを計算するための個別の MSE サーバと、これらの AP に対する個別のロケーション ライセンスを購入する必要があります。

MSE 8.0 ライセンス SKU は以下のとおりです。

表 1-2　Cisco MSE でサポートされる SKU

Cisco MSE モデル	SKU	サービス SKU	説明
Cisco MSE 3365 物理アプライアンス	AIR-MSE-3365-K9	CON-SNT-AIRMSE3K	ハードウェアおよびソフトウェアのサポート
Cisco MSE 3355 物理アプライアンス	AIR-MSE-3355-K9	CON-SNT-MSE3355	ハードウェアおよびソフトウェアのサポート
Cisco MSE 仮想アプライアンス	L-MSE-7.0-K9	CON-SAU-LMSE7K	ソフトウェアおよびソフトウェア サポート
Cisco MSE 8.0 基本ライセンス	L-LS-xAP	CON-SAU-LLS1APSW	Cisco MSE 3365 アプライアンスを注文する場合にのみ、ソフトウェアをサポート
Cisco MSE 8.0 CMX ライセンス	L AD LS xAP	CON-SAU-LADLA1AP	Cisco MSE 3365 アプライアンスを注文する場合にのみ、ソフトウェアをサポート

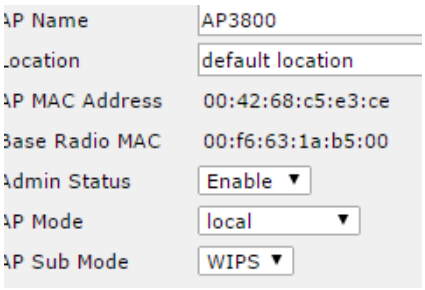
2800、3800、および 1560 AP での WIPS モニタリング

フレキシブル ラジオ アサインメントでは、統合無線の動作ロールを手動で設定することも、利用可能な RF 環境に基づいて AP でインテリジェントに決定することもできます。AP は、ワイヤレス セキュリティ モニタリングおよび 5 GHz ロールで動作できます。このロールでは、一方の無線が 5 GHz クライアントにサービスを提供し、もう一方の無線が 2.4 GHz と 5 GHz の両方をスキャンして wIPS 攻撃者、CleanAir 干渉源、および不正なデバイスを検出します。

無線がそのサービス チャネル上にある場合は「オンチャネル」と見なされ、他のチャネルをスキャンしている場合は「オフチャネル」と見なされます。AP に WIPS スキャンを設定できる展開シナリオは 3 つあります。

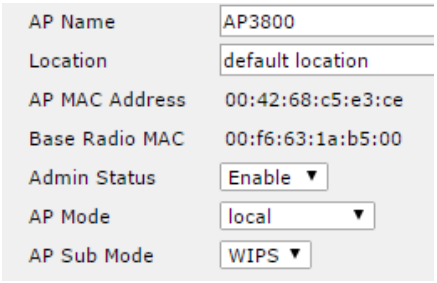
- **ELM がグローバル モードで FRA 無線がクライアント サービス モード**：ベストエフォートのオフチャネル サポートを提供します。

  wIPS を使用したローカル モードでは、「オンチャネル」での wIPS 検出が可能です。それにより、攻撃者がクライアント用のチャネルで検出されます。他のすべてのチャネルでは、ELM がベスト エフォート型の wIPS 検出を提供します。ベストエフォートでの検出では、フレームごとに無線が短時間「オフチャネル」になります。「オフチャネル」の場合、そのチャネルをスキャン中に攻撃が行われると、攻撃が検出されます。ELM クライアント サービス モードの FRA 無線は、引き続きクライアントにサービスを提供できます。

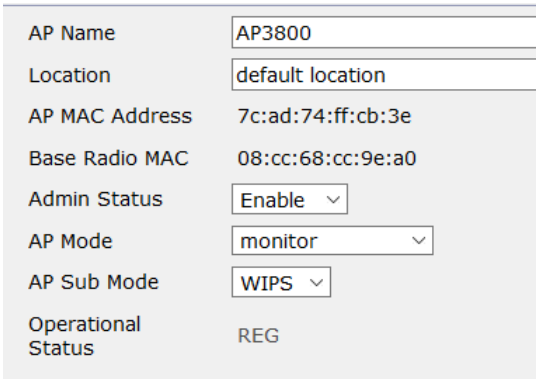


- **ELM がグローバル モードで FRA 無線がモニタ モード。**

  ELM モードでは、無線スロット 1（5 GHz）に対するベストエフォートのスキャンが実施されます。一方、FRA 無線のモニタ モードでは、専用の wIPS 検出が「オフチャネル」で実施されます。つまり、アクセス ポイントが各チャネルに長時間留まり、すべてのチャネルに対する攻撃を検出します。モニタ モードの FRA 無線はクライアントにサービスを提供できません。



- **モニタ モードの AP**：すべてのチャネル（2.4 GHz および 5 GHz）に対して専用の wIPS セキュリティ スキャンを実施し、無線攻撃を検出します。



概要 - 異なる導入モードにおける、ワイヤレス IPS 脅威検出の比較:

WLC でのワイヤレス IPS シグネチャ ネイティブ	コントローラ コードとバンドルされているため、ライセンスの必要なし	Good
FRA での ELM	ライセンスが必要。60 以上のシグネチャを検出	ベター/ベスト エフォート
モニタ モード	ライセンスが必要。100 以上のシグネチャを検出	最高水準

サポートされているアラーム

アラーム ID	アラーム名
0	暗号化が無効な AP
1	暗号化が無効なクライアント
2	WEP IV キーの再利用
7	オープン認証を使用するデバイス
8	AP のデバイス プローブ
9	AP アソシエーションのキャパシティが上限に達しています
10	DoS：認証失敗攻撃
34	チャネル上の過剰なマルチキャスト/ブロードキャスト
35	スプーフされた MAC アドレスの検出
37	DoS：アソシエーション テーブル オーバーフロー
38	クラック可能な WEP IV キーの使用
40	VPN によって保護されていないデバイス
41	802.1x によって保護されていないデバイス
49	ステーションによる AP の過負荷
52	DoS：認証フラッド
53	DoS：EAPOL-Logoff 攻撃
54	DoS：EAPOL-Start 攻撃
56	DoS：Premature EAP-Success
57	DoS：Premature EAP-Failure
58	DoS：De-Auth ブロードキャスト フラッド
59	DoS：De-Auth フラッド
60	DoS：Dis-Assoc ブロードキャスト フラッド
61	DoS：Dis-Assoc フラッド

アラーム ID	アラーム名
62	DoS：RF Jamming
63	EAP メソッドへの辞書攻撃
64	中間者攻撃
65	共有キー認証を使用するデバイス
72	PEAP によって保護されていないデバイス
79	DoS：認証されないアソシエーション
80	DoS：アソシエーション フラッド
89	偽の AP の検出
93	WPA または 802.11i 事前共有キーの使用
99	ソフト AP またはホスト AP の検出
101	未承認アソシエーションの検出
102	Airsnarf 攻撃
103	ASLEAP ツール検出
107	不正 802.11 パケットの検出
113	偽の DHCP サーバの検出
117	802.1x 認証に対する EAP 攻撃
119	NetStumbler の検出
120	Wellenreiter の検出
121	DoS：FATA-Jack ツール
125	802.11i/AES によって保護されていないデバイス
126	高速 WEP クラック ツールの検出
154	高速 WEP クラック ツールの検出
156	フラグメンテーション攻撃
178	Identical Send and Receive Address
179	Improper Broadcast Frames
181	不良 EAP-TLS フレーム
182	HT-Intolerant Degradation of Service
183	DoS：ブロック ACK フラッド
187	DoS：プローブ要求フラッド
188	DoS：プローブ応答フラッド
189	DOS：再アソシエーション要求フラッド
195	DoS：ビーコン フラッド
198	WiFiTap ツールの検出
205	不正なビーコン
213	AirDrop セッションの検出
217	ICMP トンネルバイパスの検出
218	ビーコン ファジング フレームの検出

アラーム ID	アラーム名
219	プローブ要求ファジング フレームの検出
220	プローブ応答ファジング フレームの検出
222	DoS：ビーコン DS 設定 DoS
257	デバイスが EAP-TTLS を使用していません
260	ブルートフォース非表示 SSID
261	選択された認証方法によって保護されていないデバイス

サポートされていないアラーム

ID	アラーム
13	帯域の過剰な使用率
50	使用率による AP の過負荷
51	802.1x キー変更のタイムアウトが長すぎます
68	TKIP によって保護されていないデバイス
87	疑わしい営業時間外のトラフィックの検出
95	DoS：CTS フラッド
105	EAP-FAST によって保護されていないデバイス
108	DoS：PS-Poll フラッド
112	DoS：仮想キャリア攻撃
115	DoS：Queensland University of Technology Exploit
118	ハニーポット AP の検出
124	Hotspotter ツールの検出
133	デバイスのセキュリティ異常による Day-Zero 攻撃
135	WLAN のセキュリティ異常による Day-Zero 攻撃
138	ベンダー リストによる未承認アソシエーション
155	ChopChop 攻撃
157	DoS：RTS フラッド
173	ノード上の過剰なマルチキャスト/ブロードキャスト
186	EAP-TLS によって予測されない AP
193	異常なフラグメンテーション番号
194	不完全なフラグメンテーション番号

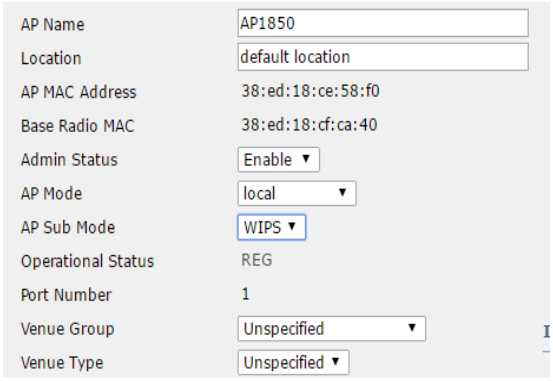
ID	アラーム
196	DoS：MDK3-Destruction 攻撃
197	Karma ツールの検出
207	AirPwn
210	XSS SSID をブロードキャストするデバイス
214	Karmetaspoilt 攻撃の検出
215	DHCP スターベーション攻撃の検出
216	DNS トンネルバイパスの検出
221	WiFi Protected Setup Pin ブルートフォース
223	Broadcom RSN 範囲外攻撃
224	WiFi ダイレクト デバイスの検出
225	WPA 辞書攻撃の検出

1800 AP プラットフォーム（1810、1815、1850、および 1830）での WIPS モニタリング

同様に、1810、1815、1850、および 1830 を含む 1800 Wave 2 アクセス ポイントをネットワークに展開し、wIPS 攻撃者、CleanAir 干渉源、および不正なデバイスを無線でスキャンできます。AP18xx シリーズ プラットフォームは、ローカル モードとモニタ モードのワイヤレス IPS スキャンをサポートしています。AireOS リリース 8.5 に AP18xx シリーズのモニタ モードのサポートが追加されました。

ELM モード – WIPS をサブ モードとして使用するローカル AP モード

wIPS を使用したローカル モードでは、「オンチャネル」での wIPS 検出が可能です。それにより、攻撃者がクライアント用のチャネルで検出されます。他のすべてのチャネルでは、ELM がベストエフォート型の wIPS 検出を提供します。ベストエフォートでの検出では、フレームごとに無線が短時間「オフチャネル」になります。「オフチャネル」の場合、そのチャネルをスキャン中に攻撃が行われると、攻撃が検出されます。ELM クライアント サービス モードの FRA 無線は、引き続きクライアントにサービスを提供できます。



サポートされているアラーム

アラーム ID	アラーム名
7	オープン認証を使用するデバイス
8	AP のデバイス プローブ
9	AP アソシエーションのキャパシティが上限に達しています
10	DoS：認証失敗攻撃
34	チャネル上の過剰なマルチキャスト/ブロードキャスト
35	スプーフされた MAC アドレスの検出
37	DoS：アソシエーション テーブル オーバーフロー
49	ステーションによる AP の過負荷
52	DoS：認証フラッド
58	DoS：De-Auth ブロードキャスト フラッド
59	DoS：De-Auth フラッド
60	DoS：Dis-Assoc ブロードキャスト フラッド
61	DoS：Dis-Assoc フラッド
62	DoS：RF Jamming
65	共有キー認証を使用するデバイス
79	DoS：認証されないアソシエーション
80	DoS：アソシエーション フラッド
89	偽の AP の検出
93	WPA または 802.11i 事前共有キーの使用
99	ソフト AP またはホスト AP の検出
107	不正 802.11 パケットの検出
119	NetStumbler の検出

アラーム ID	アラーム名
120	Wellenreiter の検出
121	DoS：FATA-Jack ツール
178	Identical Send and Receive Address
179	Improper Broadcast Frames
182	HT-Intolerant Degradation of Service
187	DoS：プローブ要求フラッド
188	DoS：プローブ応答フラッド
189	DOS：再アソシエーション要求フラッド
195	DoS：ビーコン フラッド
205	不正なビーコン
213	AirDrop セッションの検出
218	ビーコン ファジング フレームの検出
219	プローブ要求ファジング フレームの検出
220	プローブ応答ファジング フレームの検出
222	DoS：ビーコン DS 設定 DoS
260	ブルートフォース非表示 SSID

サポートされていないアラーム

アラーム ID	アラーム名
0	暗号化が無効な AP
1	暗号化が無効なクライアント
2	WEP IV キーの再利用
13	帯域の過剰な使用率
38	クラック可能な WEP IV キーの使用
40	VPN によって保護されていないデバイス
41	802.1x によって保護されていないデバイス
50	使用率による AP の過負荷
51	802.1x キー変更のタイムアウトが長すぎます
53	DoS：EAPOL-Logoff 攻撃
54	DoS：EAPOL-Start 攻撃
56	DoS：Premature EAP-Success
57	DoS：Premature EAP-Failure
63	EAP メソッドへの辞書攻撃
64	中間者攻撃
68	TKIP によって保護されていないデバイス
72	PEAP によって保護されていないデバイス

アラーム ID	アラーム名
87	疑わしい営業時間外のトラフィックの検出
94	PSPF 違反の検出
95	DoS：CTS フラッド
96	802.1x 暗号化されないブロードキャストまたはマルチキャスト
101	未承認アソシエーションの検出
102	Airsnarf 攻撃
103	ASLEAP ツール検出
105	EAP-FAST によって保護されていないデバイス
108	DoS：PS-Poll フラッド
112	DoS：仮想キャリア攻撃
113	偽の DHCP サーバの検出
115	DoS：Queensland University of Technology Exploit
117	802.1x 認証に対する EAP 攻撃
118	ハニーポット AP の検出
124	Hotspotter ツールの検出
125	802.11i/AES によって保護されていないデバイス
126	高速 WEP クラック ツールの検出
133	デバイスのセキュリティ異常による Day-Zero 攻撃
135	WLAN のセキュリティ異常による Day-Zero 攻撃
138	ベンダー リストによる未承認アソシエーション
154	NetStumbler 犠牲者の検出
155	ChopChop 攻撃
156	フラグメンテーション攻撃
157	DoS：RTS フラッド
173	ノード上の過剰なマルチキャスト/ブロードキャスト
181	不良 EAP-TLS フレーム
183	DoS：ブロック ACK フラッド
186	EAP-TLS によって保護されていない AP
193	異常なフラグメンテーション番号
194	不完全なフラグメンテーション番号
196	DoS：MDK3-Destruction 攻撃
197	Karma ツールの検出

アラーム ID	アラーム名
198	WiFiTap ツールの検出
207	AirPwn
210	XSS SSID をブロードキャストするデバイス
214	Karmetaspoilt 攻撃の検出
215	DHCP スターベーション攻撃の検出
216	DNS トンネルバイパスの検出
217	ICMP トンネルバイパスの検出
221	WiFi Protected Setup Pin ブルートフォース
223	Broadcom RSN 範囲外攻撃
224	WiFi ダイレクト デバイスの検出
225	WPA 辞書攻撃の検出
257	デバイスが EAP-TTLS を使用していません
261	選択された認証方法によって保護されていないデバイス