H3Cアクセスコントローラ
WLANセキュリティコンフィギュレーションガイド(WIPS)

内容

WIPSの概要

WIPSについて

Wireless Intrusion Prevention System(WIPS)を使用すると、WLANを監視し、攻撃や不正なデバイスを検出し、対策を講じることができます。WIPSは、WLANセキュリティの完全なソリューションを提供します。

WIPSコンポーネント

WIPSには、ネットワーク管理モジュール、AC、およびセンサー(WIPSでイネーブルになっているAP)が含まれています。

- センサーはWLANを監視し、チャネル情報を収集し、さらに分析するためにその情報をACに報告します。
- ACは、攻撃や不正デバイスを特定し、対策を講じ、アラームをトリガーします。
- ネットワーク管理モジュールを使用すると、WebインターフェイスでWIPSを設定できます。設定管理、レポート生成、およびアラーム管理機能を提供します。

WIPSの機能

WIPSには次の機能があります。

- **攻撃検出**: WIPSは、802.11フレームをリッスンすることで攻撃を検出し、アラームをトリガーして管理者に通知します。
- **シグニチャベースの攻撃検出**: WIPSは、シグニチャベースの攻撃検出を提供します。シグニチャには、パケット識別方法と、一致するパケットに対して実行するアクションが含まれます。
- **デバイス分類**: WIPSは、802.11フレームをリッスンすることでワイヤレスデバイスを識別し、分類規則に基づいてデバイスを分類します。
- **対策**: WIPSを使用すると、不正デバイスに対する対策を実行できます。

攻撃の検出

フラッドアタック検出

APが短期間に多数の同じタイプのフレームを受信した場合、APはフラッド攻撃を受ける可能性があります。APが過負荷にならないように、WIPSは着信パケット統計情報を定期的に調べ、疑わしいフラッド攻撃を検出したときにアラームをトリガーします。WIPSは、次のフラッド攻撃を検出できます。

- **認証要求フラッド攻撃**: 認証要求をAPに送信する多数のクライアントを模倣することにより、APのアソシエーションテーブルをフラッドします。
- **プローブ要求/アソシエーション要求/再アソシエーション要求フラッド攻撃**: プローブ要求、アソシエーション要求、再アソシエーション要求をAPに送信する多数のクライアントを模倣することによって、APのアソシエーションテーブルをフラッドします。
- **EAPOL-startフラッド攻撃**: IEEE 802.1Xで定義されたEAPOL-startフレームをAPに送信する多数のクライアントを模倣することにより、APのリソースを使い果たします。
- **ブロードキャスト/ユニキャスト認証解除フラッド攻撃**: APから関連付けられたクライアントへの認証

解除フレームをスプーフィングして、クライアントとAPの関連付けを解除します。この攻撃により、複数のクライアントへの無線サービスが迅速に終了する可能性があります。

- **ブロードキャスト/ユニキャストアソシエーション解除フラッド攻撃**: APから関連付けられたクライアントへのアソシエーション解除フレームをスプーフィングして、クライアントとAPのアソシエーションを解除します。この攻撃により、複数のクライアントへの無線サービスが迅速に終了する可能性があります。
- **RTS/CTSフラッド攻撃**:RTS/CTSフレームをフラッドしてRFメディアを予約し、RFメディアを共有する他のワイヤレスデバイスに送信を阻止させます。この攻撃では、仮想キャリアメカニズムの脆弱性を利用します。
- **ブロックACKフラッド攻撃**: ブロックACKフレームをAPにフラッディングして、ブロックACKメカニズムの動作を中断します。
- **ヌルデータフラッド攻撃**: クライアントからAPへ、電源管理ビットが1のヌルデータフレームをスプーフィングします。APは、クライアントが省電力モードであると判断し、クライアント用にフレームをバッファします。バッファされたフレームのエージングタイムが期限切れになると、APはフレームを破棄します。これにより、クライアントとAPとの通信が中断されます。
- **ビーコンフラッド攻撃**: 多数の偽のAPを模倣してビーコンフレームをフラッディングし、クライアントアソシエーションを中断します。
- **EAPOL-Logoffフラッド攻撃**: IEEE 802.1X標準では、Extensible Authentication Protocol over LAN(EAPOL)を使用した認証プロトコルが定義されています。クライアントは、APとのセッションを終了するためにEAPOL-Logoffフレームを送信する必要があります。EAPOL-Logoffフレームは認証されず、攻撃者はEAPOL-Logoffフレームをスプーフィングしてクライアントのアソシエーションを解除できます。
- **EAP-success/failureフラッド攻撃**:802.1X認証を使用するWLANでは、APがEAP-successフレームまたはEAP-failureフレームをクライアントに送信して、認証の成功または失敗をクライアントに通知します。攻撃者はAPのMACアドレスをスプーフィングしてEAP-successフレームまたはEAP-failureフレームをクライアントに送信し、認証プロセスを中断させることができます。

不正な形式のパケット検出

WIPSは、フレームが表1に示す基準に一致した場合にフレームが不正であると判断し、アラームとログをトリガーします。

表1不正な形式のフレームの一致基準

検出タイプ	適用フレーム	一致条件
無効なIE長検出	すべての管理フレーム	IEの長さが802.11プロトコルに準拠していません。パケットが解決された後、IEの残りの長さは0ではありません。
重複IEの検出	すべての管理フレーム	重複するIE。このタイプの検出は、ベンダー定義のIEには適用できません。
冗長IE検出	すべての管理フレーム	IEはフレームにとって必要なIEではなく、予約されたIEでもない。
無効なパケット長の検出	すべての管理フレーム	パケットペイロードが解決された後、IEの残りの長さは0ではありません。
IBSS、ESS設定異常検出	• ビーコンフレーム • プローブ応答フレーム	IBSSとESSの両方が1に設定されている。

不正な認証要求フレーム の検出	認証要求フレーム	• 認証アルゴリズム番号が802.11プロトコルに準拠しておらず、3より大きい。 • 認証トランザクションシーケンス番号は1であり、ステータスコードは0ではありません。 • 認証トランザクションシーケンス番号が4より大きくなっています。
不正なアソシエーション要求フレームの検出	アソシエーション要求フレーム	フレーム長は0です。
不正なHT IE検出	• ビーコンフレーム • プローブ応答 • アソシエーションの応答 再関連付け要求	• HT機能IEのSM省電力値は2です。 • HT動作IEのセカンダリチャネルオフセット値は2です。
オーバーサイズ期間の検出	• ユニキャスト管理フレーム • ユニキャストデータフレーム • RTS、CTS、およびACKフレーム	パケット継続時間の値が、指定されたしきい値より大きい。
不正なプローブ応答フレーム検出	プローブ応答フレーム	フレームはメッシュフレームではなく、SSIDの長さが0です。
無効な認証解除コードの検出	フレームの認証解除	理由コードは0、または67～65535の範囲です。
無効なアソシエーション解除コードの検出	関連付けを解除するフレーム	理由コードは0、または67～65535の範囲です。
オーバーサイズのSSID検出	• ビーコンフレーム • プローブ要求 • プローブ応答 • アソシエーション要求フレーム	SSIDの長さが32を超えています。
FATA-Jack検出	認証フレーム	認証アルゴリズム番号の値は2です。
無効な送信元アドレス検出	すべての管理フレーム	• TO DSは1で、クライアントからAPにフレームが送信されたことを示します。 フレームの送信元MACアドレスがマルチキャストアドレスまたはブロードキャストアドレスである。
オーバーサイズのEAPOLキー検出	EAPOL-Keyフレーム	TO DSが1で、キーの長さが0より大きい場合。

スプーフィング攻撃の検出

スプーフィング攻撃では、攻撃者は別のデバイスに代わってフレームを送信し、ネットワークを脅かします。WIPSは、次のスプーフィング攻撃の検出をサポートしています。

- **フレームスプーフィング**: 偽のAPは、許可されたAPをスプーフィングしてビーコンまたはプローブ応答フレームを送信し、クライアントにアソシエートさせます。
- **AP MACアドレススプーフィング**: クライアントが認可されたAPをスプーフィングして、認証解除フレームまたはアソシエーション解除フレームを他のクライアントに送信します。これにより、クライアントがオフラインになり、WLANの正しい動作に影響を与える可能性があります。
- **クライアントMACアドレススプーフィング**: 偽のAPは、認可されたクライアントをスプーフィングして、認可されたAPに関連付けます。

フレームスプーフィング攻撃の検出

WIPSは、フレーム受信時刻とタイムスタンプを使用してAPの起動時間を計算します。計算されたAPの起動時間がWIPSに記録された起動時間と異なる場合、WIPSはこれがスプーフィング攻撃であると判断します。

APのMACアドレススプーフィング攻撃の検出

WIPSは送信者のMACアドレスを検査します。送信者のMACアドレスがAP MACアドレステーブルにすでに存在する場合、WIPSはこれがスプーフィング攻撃であると判断します。

クライアントMACアドレススプーフィング攻撃の検出

WIPSは送信者のMACアドレスを調べます。送信者のMACアドレスがクライアントのMACアドレステーブルにすでに存在する場合、WIPSはこれがスプーフィング攻撃であると判断します。

弱いIV検出

WEPセキュリティプロトコルで使用されるRC4暗号化アルゴリズムで安全でないIVが使用されている場合、WEPキーはクラックされる可能性が高くなります。IVは、最初のバイトが16(10進数)より小さく、2番目のバイトがFFの場合に弱いIVとなります。WIPSは、各WEPパケット内のIVを検出することにより、この種の攻撃を防止します。

オメルタ攻撃検出

Omertaは、802.11プロトコルに基づくDoS攻撃ツールです。クライアントのアソシエーションを解除するために、理由コード0x01のアソシエーション解除フレームを送信します。理由コード0x01は、不明なアソシエーション解除理由を示します。WIPSは、各アソシエーション解除フレームの理由コードを検出することで、Omerta攻撃を検出します。

ブロードキャストアソシエーション解除/認証解除攻撃の検出

攻撃者は、正当なAPをスプーフィングしてブロードキャストアソシエーション解除または認証解除フレームを送信し、APに関連付けられているすべてのクライアントをログオフします。

40 MHz帯域幅モードがディセーブルになっているクライアントでの検出

802.11nデバイスは、20 MHzと40 MHzの両方の帯域幅モードをサポートしています。クライアントで40

MHz帯域幅モードが無効になっている場合、クライアントと同じAPに関連付けられている他のクライアントも20 MHz帯域幅を使用する必要があります。これは、ネットワークのスループットと効率に影響します。

WIPSは、クライアントから送信されたプローブ要求フレームを検出することによって、このようなクライアントを検出します。

省電力攻撃の検出

攻撃者は、クライアントのMACアドレスをスプーフィングして、パワーセーブオンフレームをAPに送信します。APはクライアントのフレームをキャッシュします。攻撃されたクライアントは、クライアントがまだパワーセーブモードであるとAPが判断するため、データフレームを受信できません。キャッシュされたフレームのエージングタイムが期限切れになると、APはフレームを廃棄します。WIPSは、パワーセーブオンフレームとパワーセーブオフフレームの比率を決定することで、パワーセーブ攻撃を検出します。

禁止チャネルの検出

許可チャネルリストを設定し、禁止チャネル検出をイネーブルにすると、WIPSは、許可チャネルリストにないチャネルが禁止チャネルであると判断します。

ソフトAP検出

ソフトAPとは、APとして動作し、無線サービスを提供するクライアントを指します。攻撃者はソフトAPを介して内部ネットワークにアクセスし、さらに攻撃を開始することができます。WIPSは、デバイスがクライアントとAP間で役割を切り替える間隔を検出することで、ソフトAPを検出します。WIPSは、関連付けられていないクライアントではソフトAP検出を実行しません。

Windowsブリッジ検出

有線ネットワークに接続されたワイヤレスクライアントが、有線NICを介してWindowsブリッジを確立する場合、クライアントは外部APと内部ネットワークをブリッジできます。これにより、内部ネットワークにセキュリティ問題が発生する可能性があります。WIPSは、関連付けられたクライアントから送信されたデータフレームを分析することで、Windowsブリッジを検出します。

暗号化されていないデバイスの検出

認可されたAPまたはクライアントが暗号化されていないフレームを送信すると、ネットワークにセキュリティ上の問題が発生する可能性があります。WIPSでは、認可されたAPまたはクライアントから送信されたフレームを分析して、暗号化されていないデバイスを検出します。

ホットスポット攻撃の検出

攻撃者は、ホットスポットと同じSSIDを持つ不正なAPを設定して、クライアントをアソシエートさせます。クライアントが不正なAPにアソシエートした後、攻撃者はさらに攻撃を開始して、クライアント情報を取得します。

WIPSがホットスポット攻撃を検出できるように、ホットスポットファイルを設定できます。

AP偽装攻撃検出

AP偽装攻撃では、正規のAPと同じBSSIDおよびESSIDを持つ悪意のあるAPが、クライアントにアソシエートさせます。この偽装APは、ホットスポット攻撃を開始したり、検出システムを騙したりします。

WIPSは、APがビーコンフレームを送信する間隔を検出することによって、AP偽装攻撃を検出します。

HT-グリーンフィールドAP検出

HT-greenfieldモードで動作しているAPは、802.11a/b/gデバイスと通信できないため、コリジョン、エラー、および再送信が発生する可能性があります。WIPSは、APから送信されたビーコンフレームまたはプローブ応答フレームを分析することによって、HT-greenfield APを検出します。

ハニーポットAP検出

ハニーポットAP攻撃では、攻撃者は悪意のあるAPを設定して、クライアントにアソシエートさせます。悪意のあるAPのSSIDは、正規のAPのSSIDと類似しています。クライアントがハニーポットAPにアソシエートすると、ハニーポットAPはポートスキャンや偽認証などの攻撃をさらに開始して、クライアント情報を取得します。

WIPSは、外部APのSSIDを検出することによってハニーポットAPを検出します。外部APのSSIDと正当なAPのSSIDの類似性が指定されたしきい値に達すると、WIPSはアラームを生成します。

MITM攻撃検出

MITM攻撃では、攻撃者は不正なAPを設定し、クライアントにアソシエートさせます。次に、不正なAPはクライアントのMACアドレスをスプーフィングして、認可されたAPにアソシエートさせます。クライアントと認可されたAPが通信すると、不正なAPはクライアントと認可されたAPの両方からパケットをキャプチャします。不正なAPはフレームを変更し、フレーム情報を取得する場合があります。WIPSは、認可されたAPからアソシエーションを解除され、ハニーポットAPに関連付けられたクライアントを検出することで、MITM攻撃を検出します。WIPSは、ハニーポットAP検出とMITM攻撃検出の両方をイネーブルにしている場合にだけ、MITM攻撃を検出できます。

ワイヤレスブリッジ検出

攻撃者は、ワイヤレスブリッジを介して内部ネットワークに侵入する可能性があります。ワイヤレスブリッジを検出すると、WIPSはアラームを生成します。ワイヤレスブリッジがメッシュネットワーク内にある場合、WIPSはメッシュリンクを記録します。

アソシエーション/再アソシエーションDoS攻撃の検出

アソシエーション/再アソシエーションDoS攻撃は、アソシエーション要求をAPに送信する多数のクライアントを模倣することによって、APのアソシエーションテーブルをフラッディングします。テーブル内のエントリ数が上限に達すると、APは正当なクライアントからの要求を処理できなくなります。

APフラッド攻撃検出

WIPSは、WLAN内のAPの数を検出し、APの数が指定されたしきい値を超えると、APフラッド攻撃のアラームをトリガーします。

デバイス侵入攻撃検出

攻撃者は、無効なパケットをWIPSに送信して処理コストを増加させることができます。WIPSは、学習したデバイスエントリを定期的に調べて、デバイスエントリの学習をレート制限するかどうかを決定します。指定された間隔内に学習されたAPまたはクライアントエントリの数がしきい値を超えると、WIPSはアラ

ームをトリガーし、新しいエントリの学習を停止します。

デバイスエントリには、非アクティビティタイマーとエージングタイマーを設定できます。非アクティビティタイマーが期限切れになる前にワイヤレスデバイスがパケットを送受信しない場合、デバイスは非アクティブステータスになります。エージングタイマーが期限切れになる前にワイヤレスデバイスがパケットを送受信しない場合、デバイスエントリは削除されます。

シグニチャベースの攻撃検出

WIPSは、シグニチャベースの攻撃検出を提供します。シグニチャには、パケット識別方法と、一致するパケットに対して実行するアクションが含まれます。センサーは、検出されたパケットをシグニチャと照合し、パケットがシグニチャと一致する場合はシグニチャで定義されたアクションを実行します。

シグニチャには最大6つのサブシグニチャを含めることができます。サブシグニチャは、フレームタイプ、MACアドレス、シリアルID、SSIDの長さ、SSID、およびフレームパターンに基づいて定義できます。パケットがシグニチャと一致するのは、シグニチャ内のすべてのサブシグニチャと一致する場合だけです。

デバイスの分類

AP分類

APカテゴリ

表2に示すように、WIPSは、事前定義された分類ルールに従って、検出されたAPを分類します。

表2 AP分類

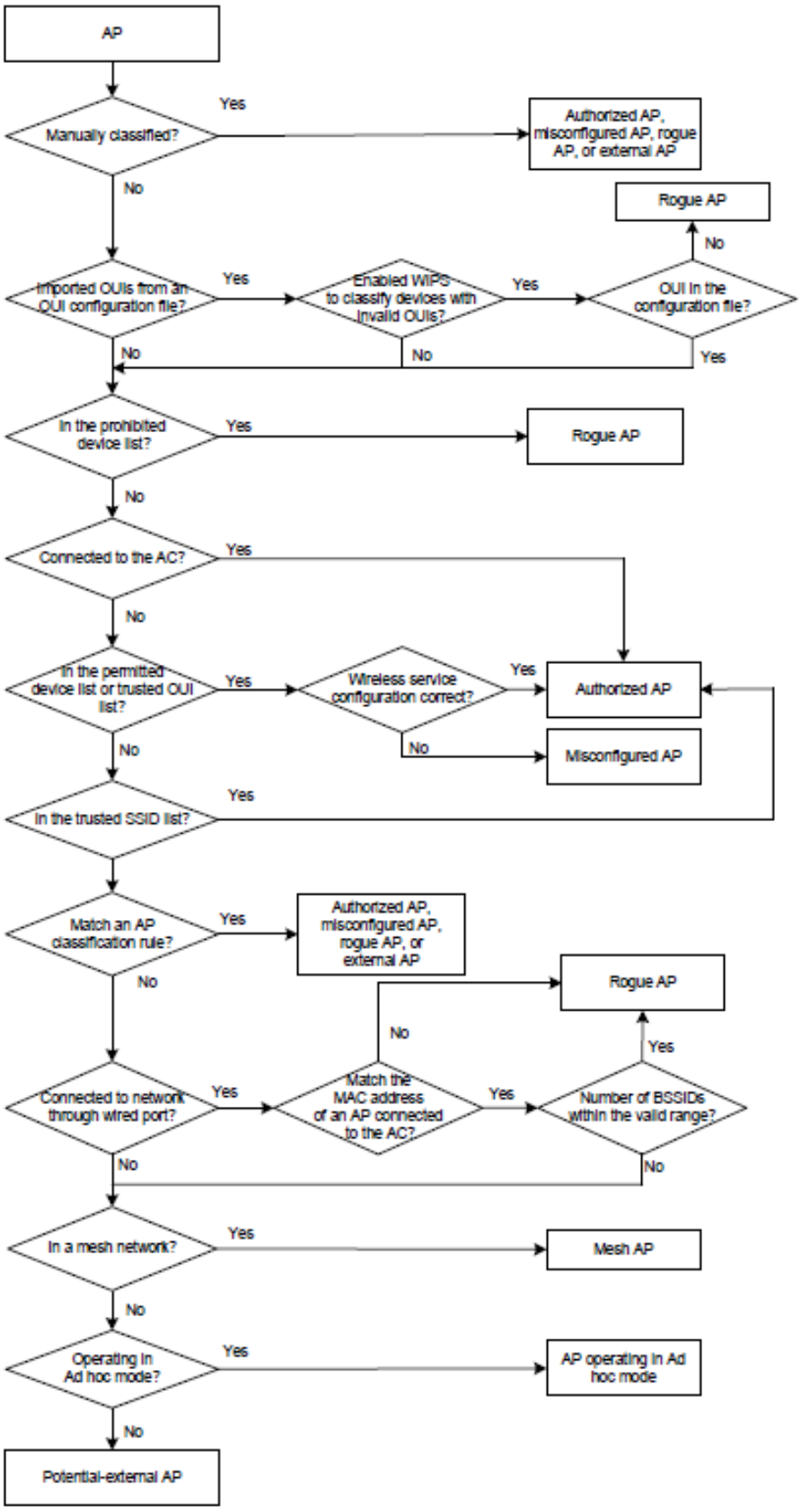
分類	説明	分類規則
認可されたAP	WLANで許可されているAP。	• ACに接続されており、禁止デバイスリストに含まれていない。 • 認可されたAPとして設定されている。 • 許可されたデバイスリスト内。 • ユーザ定義のAP分類規則によって、認可されたAPとして分類されます。
不正なAP	WLANで使用できないAP。	• 禁止されているデバイスリスト内 • OUI構成ファイル内にありません。 • 不正APとして設定されている。 • ユーザ定義のAP分類ルールによって、不正APとして分類されます。 APの有線ポートがネットワークに接続されていて、APがACに接続されていない場合、APは不正なAPである可能性があります。
APの設定ミス	WLANで使用できるが、設定が正しくないAP。	• 誤って設定されたAPとして設定されている。 • ユーザ定義のAP分類ルールによって、誤って設定されたAPとして分類されます。
外部AP	隣接するWLANにあるAP。	• 外部APとして設定されます。 • ユーザ定義のAP分類規則によって外部APとして分類されます。

アドホック	アドホックモードで動作しているAP。 WIPSは、ビーコンフレームをリッスンすることによってアドホックAPを検出します。	該当なし
メッシュAP	WLANメッシュネットワーク内のAP。	WIPSは、ビーコンフレームを使用してメッシュAPを識別します。
潜在的に認可されたAP	認可されている可能性のあるAP。	APは、次のすべての条件を満たす場合に、潜在的に認可されたAPです。 • 許可デバイスリストにありません。 • 禁止デバイスリストにない。 • 信頼されたSSIDリストにない。 • 信頼できるOUIリストに含まれていません。 • ACに接続されています。 • 手動で分類されていません。 • ユーザ定義のAP分類ルールと一致しません。
不正APの可能性	不正なAPである可能性があるAP。	ワイヤレス設定が正しくなく、次のいずれのリストにも含まれていない。 • 許可されたデバイスリスト。 • 禁止されたデバイスリスト • 信頼できるOUIリスト。 APの有線ポートがネットワークに接続されている場合、APは不正なAPです。
可能性-外部AP	外部APである可能性があるAP。	• ワイヤレスサービスの設定が正しくありません。 • ワイヤード(有線)ポートがネットワークに接続されていません。 • 次のリストのいずれにも含まれていない。 ○ 許可されたデバイスリスト。 ○ 禁止されたデバイスリスト ○ 信頼できるOUIリスト。
未分類のAP	カテゴリを判別できないAP。	該当なし

AP分類フロー

WIPSは、図1に示すプロセスに従って、検出されたAPを分類します。

図1 AP分類の流れ



注:

AP分類フローでは、H3Cデバイスだけが有線ネットワーク接続検出をサポートしています。

クライアントの分類

表3に示すように、WIPSは、事前定義された分類ルールに基づいて、検出されたクライアントを分類します。

クライアントカテゴリ

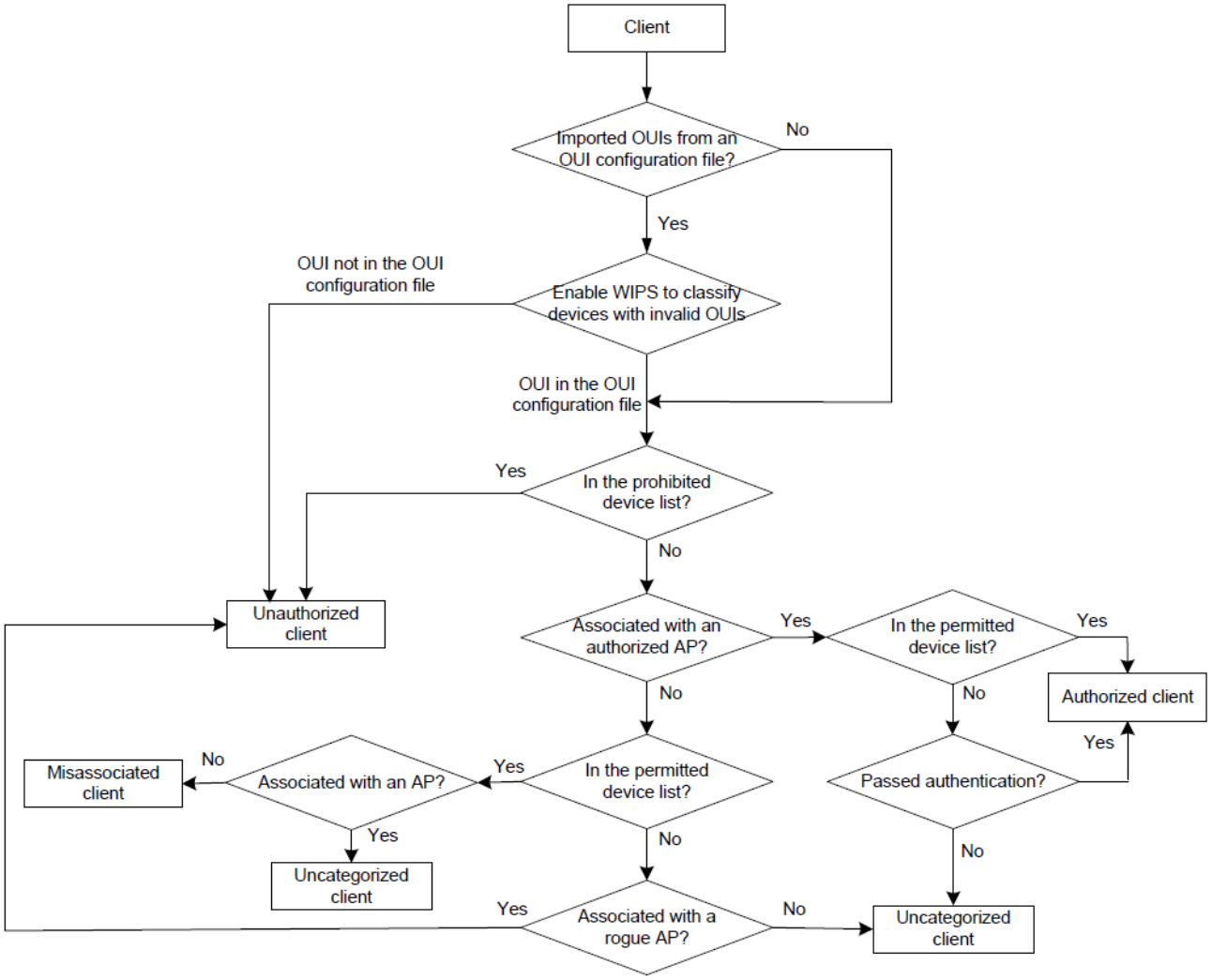
表3 クライアントの分類

分類	説明	分類規則
許可されたクライアント	WLANで許可されているクライアント。	• 禁止デバイスリスト内で、認可されたAPに関連付けられています。 • 認証に合格し、認可されたAPに関連付けられています。
許可されていないクライアント	WLANで使用できないクライアント。	• 禁止されているデバイスリスト内 • 不正なAPに関連付けられている。 • OUI構成ファイル内にありません。
誤って関連付けられたクライアント	不正なAPに関連付けられているクライアント。	許可されたデバイスリスト内にあるが、不正なAPに関連付けられている。誤って関連付けられたクライアントは、ネットワークにセキュリティ上の脅威をもたらす可能性があります。
未分類のクライアント	カテゴリを判別できないクライアント。	該当なし

クライアント分類フロー

WIPSは、図2に示すプロセスに従って、検出されたクライアントを分類します。

図2 クライアント分類のフロー



対策

不正なデバイスは攻撃を受けやすく、WLANにセキュリティ上の問題をもたらす可能性があります。WIPSを使用すると、不正なデバイスに対する対策を講じることができます。

WIPSの設定

WIPSタスクの概要

WIPSを設定するには、次の作業を行います。

1. WIPSのイネーブル化
2. 攻撃検出の設定
   a. 攻撃検出ポリシーの設定
   b. 攻撃検出ポリシーの適用
3. シグニチャベースの攻撃検出の設定
   a. シグニチャの設定
   b. シグニチャポリシーの設定
   c. 署名ポリシーの適用
4. デバイス分類の設定
   a. 自動デバイス分類ポリシーの設定
   b. 手動AP分類ポリシーの設定
   c. 分類ポリシーの適用
5. 対策の設定
   a. 対策ポリシーの設定
   b. 対策方針の適用
   c. 対策パケット送信間隔の設定
   d. 拡張対策モードの有効化
6. 高度なWIPS機能の設定
   - NATが設定されたクライアントの検出
   - アラーム無視機能の設定
   - アクセスサービスを提供しながらWIPSスキャンを実行するようにAPを設定する
   - OUIの設定
   - クライアントアソシエーションエントリの高速学習のイネーブル化

WIPSを有効にする

このタスクについて

ワイヤレスネットワークを複数の仮想セキュリティドメイン(VSD)に分割して、これらのVSDに異なるポリシーを適用できます。

APの無線用にWIPSを設定する前に、APをVSDに追加する必要があります。

手順

1. システムビューを開始します。

   System-view
2. APビューまたはAPグループビューを開始します。
   - APビューを開始します。

wlan ap *ap-name*

- APグループビューを開始します。

  wlan ap-group *group-name*

3. APまたはAPグループをVSDに追加します。

   wips virtual-security-domain *vsd-name*

   デフォルト:

   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、APグループはVSDに追加されません。

4. 無線ビューまたはAPグループの無線ビューを開始します。

   - radio viewを開始します。

     radio *radio-id*

   - 次のコマンドを順番に実行して、APグループの無線ビューを開始します。

     ap-model *ap-model*

     radio *radio-id*

5. WIPSを有効にします。

   wips enable

   デフォルト:

   - 無線ビューでは、無線はAPグループ無線ビューの設定を使用します。
   - APグループの無線ビューでは、WIPSはディセーブルです。

攻撃検出の設定

攻撃検出ポリシーの設定

フラッドアタック検出の設定

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. 攻撃検出ポリシーを作成し、そのビューを開始します。

   detect policy *policy-name*

4. フラッド攻撃検出を設定します。

   - アソシエーション要求フラッド攻撃検出を設定します。

     flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*

     デフォルトでは、アソシエーション要求フラッド攻撃検出はディセーブルです。

   - 認証要求フラッド攻撃検出を設定します。

     flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*

     デフォルトでは、認証要求フラッド攻撃検出はディセーブルです。

   - ビーコンフラッド攻撃検出を設定します。

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*

デフォルトでは、ビーコンフラッド攻撃検出はディセーブルです。

- ブロックACKフラッド攻撃検出を設定します。

  flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、Block Ackフラッド攻撃検出はディセーブルです。

- RTSフラッド攻撃検出を設定します。

  flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、RTSフラッド攻撃検出はディセーブルです。

- CTSフラッド攻撃検出を設定します。

  flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、CTSフラッド攻撃検出はディセーブルです。

- 認証解除フラッド攻撃検出を設定します。

  flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、認証解除フラッド攻撃検出はディセーブルです。

- アソシエーション解除フラッド攻撃検出を設定します。

  flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、アソシエーション解除フラッド攻撃検出はディセーブルです。

- EAPOL-startフラッド攻撃検出を設定します。

  flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、EAPOL-startフラッド攻撃検出はディセーブルです。

- ヌルデータフラッド攻撃検出を設定します。

  flood null data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、ヌルデータフラッド攻撃検出はディセーブルです。

- プローブ要求フラッド攻撃検出を設定します。

  flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、プローブ要求フラッド攻撃検出はディセーブルです。

- 再アソシエーション要求フラッド攻撃検出を設定します。

  flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、再アソシエーション要求フラッド攻撃検出はディセーブルです。

- EAPOL-Logoffフラッド攻撃検出を設定します。

  flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、EAPOL-Logoffフラッド攻撃検出はディセーブルです。

- EAP失敗フラッド攻撃検出を設定します。

  flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、EAP失敗フラッド攻撃検出はディセーブルです。

- EAP-successフラッド攻撃検出を設定します。

  flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、EAP-successフラッド攻撃検出はディセーブルです。

不正な形式のパケット検出の設定

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. 攻撃検出ポリシーを作成し、そのビューを開始します。

   detect policy *policy-name*

4. 不正な形式のパケット検出を設定します。
   - 重複したIE検出を設定します。

     malformed duplicated-ie [**quiet** *quiet-value*]

     デフォルトでは、重複IE検出はディセーブルになっています。
   - FATA-Jack検出を設定します。

     malformed fata-jack [**quiet** *quiet-value*]

     デフォルトでは、FATA-Jack検出はディセーブルになっています。
   - 異常なIBSSまたはESS設定の検出を設定します。

     malformed illegal-ibss-ess [**quiet** *quiet-value*]

     デフォルトでは、異常なIBSSまたはESS設定の検出はディセーブルになっています。
   - 無効な送信元アドレス検出を設定します。

     malformed invalid-address-combination [**quiet** *quiet-value*]

     デフォルトでは、無効な送信元アドレスの検出はディセーブルです。
   - 不正なアソシエーション要求フレーム検出を設定します

     malformed invalid-assoc-req [**quiet** *quiet-value*]

     デフォルトでは、不正なアソシエーション要求フレーム検出はディセーブルになっています。
   - 不正な認証要求フレーム検出を設定します。

     malformed invalid-auth [**quiet** *quiet-value*]

     デフォルトでは、不正な認証要求フレーム検出はディセーブルになっています。
   - 無効な認証解除コード検出を設定します。

     malformed invalid-deauth-code [**quiet** *quiet-value*]

     デフォルトでは、無効な認証解除コードの検出はディセーブルです。
   - 無効なアソシエーション解除コードの検出を設定します。

     malformed invalid-disassoc-code [**quiet** *quiet-value*]

     デフォルトでは、無効なアソシエーション解除コードの検出はディセーブルになっています。
   - 無効なIE長の検出を設定します。

     malformed invalid-ie-length [**quiet** *quiet-value*]

     デフォルトでは、無効なIE長の検出はディセーブルです。
   - 不正なHT IE検出を設定します。

     malformed invalid-ht-ie [**quiet** *quiet-value*]

デフォルトでは、不正なHT IE検出はディセーブルなっています。

- 無効なパケット長検出を設定します。
  malformed invalid-pkt-length [**quiet** *quiet-value*]
  デフォルトでは、無効なパケット長の検出はディセーブルです。
- オーバーサイズ期間の検出を設定します。
  malformed large-duration [**quiet** *quiet-value* | **threshold** *threshold-value*]
  デフォルトでは、オーバーサイズ期間の検出はディセーブルです。
- 不正な形式のプローブ応答フレーム検出を設定します。
  malformed null-probe-resp [**quiet** *quiet-value*]
  デフォルトでは、不正な形式のプローブ応答フレーム検出はディセーブルになっています。
- オーバーサイズのEAPOLキー検出を設定します。
  malformed overflow-eapol-key [**quiet** *quiet-value*]
  デフォルトでは、オーバーサイズのEAPOLキー検出はディセーブルです。
- オーバーサイズSSID検出を設定します。
  malformed overflow-ssid [**quiet** *quiet-value*]
  デフォルトでは、オーバーサイズSSID検出はディセーブルです。
- 冗長IE検出を設定します。
  malformed redundant-ie [**quiet** *quiet-value*]
  デフォルトでは、冗長IE検出はディセーブルです。

その他のタイプの攻撃の検出の設定

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. 攻撃検出ポリシービューを開始します。
   detect policy *policy-name*
4. その他の攻撃検出を設定します。
   - クライアントMACアドレススプーフィング攻撃検出を設定します。
     client-spoofing [**quiet** *quiet-value*]
     デフォルトでは、クライアントMACアドレススプーフィング攻撃検出はディセーブルです。
   - APのMACアドレススプーフィング攻撃検出を設定します。
     ap-spoofing [**quiet** *quiet-value*]
     デフォルトでは、APのMACアドレススプーフィング攻撃検出はディセーブルです。
   - 弱いIV検出を設定します。
     weak-iv [**quiet** *quiet-value*]
     デフォルトでは、弱いIV検出はディセーブルです。
   - Omerta攻撃検出を設定します。
     omerta [**quiet** *quiet-value*]
     デフォルトでは、Omerta攻撃検出はディセーブルです。
   - ブロードキャストアソシエーション解除攻撃検出を設定します。
     disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold**

threshold-value] *

デフォルトでは、ブロードキャストアソシエーション解除攻撃検出はディセーブルになっています。

- スプーフィング認証解除フレーム検出を設定します。

  deauth-spoofing [**quiet** *quiet*]

  デフォルトでは、スプーフィング認証解除フレーム検出はディセーブルです。

- ブロードキャスト認証解除攻撃検出を設定します。

  deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

  デフォルトでは、ブロードキャスト認証解除攻撃検出はディセーブルです。

- 40 MHz帯域幅モードをディセーブルにして、クライアントで検出を設定します。

  ht-40mhz-intolerance [**quiet** *quiet-value*]

  デフォルトでは、40 MHz帯域幅モードがディセーブルになっているクライアントでの検出はディセーブルになっています。

- 省電力攻撃検出を設定します。

  power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

  デフォルトでは、省電力攻撃検出はディセーブルになっています。

- Windowsブリッジ検出を設定します。

  windows-bridge [**quiet** *quiet-value*]

  デフォルトでは、Windowsブリッジ検出はディセーブルです。

- 暗号化されていない認可されたAP検出を設定します。

  unencrypted-authorized-ap [**quiet** *quiet-value*]

  デフォルトでは、暗号化されていない認可されたAP検出はディセーブル。

- 暗号化されていない認可クライアント検出を設定します。

  unencrypted-trust-client [**quiet** *quiet-value*]

  デフォルトでは、暗号化されていない認可クライアント検出はディセーブルになっています。

- ソフトAP検出を設定します。

  soft-ap [**convert-time** *time-value*]

  デフォルトでは、ソフトAP検出はディセーブルです。

- AP偽装攻撃検出を設定します。

  ap-impersonation [**quiet** *quiet-value*]

  デフォルトでは、AP偽装攻撃検出はディセーブルになっています。

- HT-greenfield AP検出を設定します。

  ht-greenfield [**quiet** *quiet-value*]

  デフォルトでは、HT-greenfield AP検出はディセーブルです。

- アソシエーション/再アソシエーションDoS攻撃検出を設定します。

  association-table-overflow [**quiet** *quiet-value*]

  デフォルトでは、アソシエーション/再アソシエーションDoS攻撃検出はディセーブルです。

- ワイヤレスブリッジ検出を設定します。

  wireless-bridge [**quiet** *quiet-value*]

  デフォルトでは、ワイヤレスブリッジ検出はディセーブルです。

- APフラッド攻撃検出を設定します。

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

デフォルトでは、APフラッド攻撃検出はディセーブルです。

- ハニーポットAP検出を設定します。

  honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

  デフォルトでは、ハニーポットAP検出はディセーブルです。

- MITM攻撃検出を設定します。

  man-in-the-middle [**quiet** *quiet-value*]

  デフォルトでは、MITM攻撃検出はディセーブルになっています。

- チャネル変更検出を設定します。

  ap-channel-change [**quiet** *quiet-value*]

  デフォルトでは、チャネル変更検出はディセーブルです。

- ランダムなMACアドレスを使用するApple端末に対してアラームをトリガーしないようにWIPSを設定します。

  random-mac-scan enable

  デフォルトでは、WIPSはランダムMACアドレスを使用するApple端末に対してアラームをトリガーします。

禁止チャネル検出の設定

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. 攻撃検出ポリシーを作成し、そのビューを開始します。

   detect policy *policy-name*

4. 許可チャネルリストを設定します。

   permit-channel *channel-id-list*

   デフォルトでは、許可チャネルリストにチャネルは追加されません。

5. 禁止されたチャネル検出を設定します。

   prohibited-channel [**quiet** *quiet-value*]

デフォルトでは、禁止チャネル検出はディセーブルになっています。

ホットスポット攻撃検出の設定

1. システムビューを開始します。

   system-view

2. WIPSビューを開始します。

   wips

3. 設定ファイルからホットスポット情報をインポートします。

   Import hotspot *file-name*

   デフォルトでは、ホットスポット情報はインポートされません。

4. 攻撃検出ポリシービューを開始します。

   detect policy *policy-name*

5. ホットスポット攻撃検出を設定します。

   hotspot-attack [**quiet** *quiet-value*]

   デフォルトでは、ホットスポット攻撃検出はディセーブルになっています。

デバイスエントリ攻撃検出の設定

1. システムビューを開始します。

   system-view

2. WIPSビューを開始します。

   wips

3. 攻撃検出ポリシービューを開始します。

   detect policy *policy-name*

4. クライアントエントリ攻撃検出パラメータを設定します。
   - レート制限クライアントエントリ学習。

     client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*

     デフォルトでは、統計情報収集間隔は60秒、待機時間は1200秒、クライアントエントリしきい値は1024です。
   - クライアントエントリタイマーを設定します。

     client-timer inactive *inactive-value* **aging** *aging-value*

     デフォルトでは、非アクティブ時間は300秒、エイジング時間は600秒です。

5. APエントリ攻撃検出パラメータを設定します。
   - レート制限APエントリ学習。

     ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*

     デフォルトでは、統計情報収集間隔は60秒、待機時間は1200秒、APエントリのしきい値は512です。
   - APエントリタイマーを設定します。

     ap-timer inactive *inactive-value* **aging** *aging-value*

     デフォルトでは、APの非アクティブ時間は300秒で、エージングタイムは600秒です。

RSSIベースのワイヤレスデバイス検出の設定

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. 攻撃検出ポリシービューを開始します。

   detect policy *policy-name*

4. クライアントまたはAPのRSSIしきい値を設定します。

   rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

   デフォルトでは、クライアントまたはAPに対してRSSIしきい値は設定されていません。

5. ワイヤレスデバイス検出のRSSI差のしきい値を設定します。

   rssi-change-threshold *threshold-value*

   デフォルトでは、RSSI差のしきい値は20です。

関連付けられていないクライアントを検出するためのWIPSのイネーブル化

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

wips

3. 攻撃検出ポリシービューを開始します。
   detect policy *policy-name*
4. WIPSで関連付けられていないクライアントを検出できるようにします。
   detect dissociate-client enable
   デフォルトでは、WIPSは関連付けられていないクライアントを検出しません。

ワイヤレスデバイス情報の報告間隔の設定

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. 攻撃検出ポリシービューを開始します。
   detect policy *policy-name*
4. APが検出されたデバイスに関する情報をレポートする間隔を設定します。
   report-interval *interval*
   デフォルトでは、APは検出されたデバイスに関する情報を30000ミリ秒ごとに報告します。

攻撃検出ポリシーの適用

このタスクについて

VSDに攻撃検出ポリシーを適用すると、VSD内のすべての無線で攻撃検出ポリシーを有効にできます。

手順

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. VSDを作成し、ビューを開始します。
   virtual-security-domain *vsd-name*
4. VSDに攻撃検出ポリシーを適用します。
   apply detect policy *policy-name*
   デフォルトでは、VSDには攻撃検出ポリシーは適用されません。

シグニチャベースの攻撃検出の設定

シグニチャの設定

このタスクについて

複数のシグニチャを設定した場合、WIPSは検出されたパケットを、一致が見つかるまで、IDの昇順で設定されたシグニチャと照合します。

1つのシグニチャに1つまたは複数のサブシグニチャを設定できます。

制約事項とガイドライン

1つのシグニチャに最大6つのサブシグニチャを設定して、パケットのさまざまなアトリビュートを照合できます。

手順

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. 署名を作成し、そのビューを開始します。

   signature rule *rule-id*
4. シグニチャのサブシグニチャを設定します。
   - フレームのフレームタイプと一致するサブシグニチャを設定します。

     frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

     デフォルトでは、フレームのフレームタイプと一致するサブシグニチャは設定されていません。
   - フレームのMACアドレスと一致するサブシグニチャを設定します。

     mac-address { **bssid** | **destination** | **source** } *mac-address*

     デフォルトでは、フレームのMACアドレスと一致するサブシグニチャは設定されていません。
   - フレームのシーケンス番号と一致するサブシグニチャを設定します。

     seq-number *seq-value1* [**to** *seq-value2*]

     デフォルトでは、フレームのシーケンス番号と一致するサブシグニチャは設定されていません。
   - フレームのSSIDの長さと一致するサブシグニチャを設定します。

     ssid-length *length-value1* [**to** *length-value2*]

     デフォルトでは、フレームのSSID長と一致するサブシグニチャは設定されていません。
   - フレームのSSIDと一致するサブシグニチャを設定します。

     ssid [**case-sensitive**] [**not**] { **equal** | **include**} *string*

     デフォルトでは、フレームのSSIDと一致するサブシグニチャは設定されていません。
   - フレームの指定されたビットと一致するサブシグニチャを設定します。

     pattern *pattern-number* **offset** *offset-value* **mask** *hex-value value1* [**to** *value2*] [**from-payload**]

     デフォルトでは、フレームの指定ビットと一致するサブシグニチャは設定されていません。
   - サブシグニチャが論理AND関係になるように設定します。

     match all

     デフォルトでは、サブシグニチャは論理OR関係にあります。パケットは、シグニチャのサブシグニチャのいずれかと一致する場合、シグニチャと一致します。

     このコマンドを設定すると、パケットは、シグニチャのすべてのサブシグニチャと一致する場合にだけシグニチャと一致します。

シグニチャポリシーの設定

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

wips

3. シグニチャポリシービューを開始します。

   signature policy *policy-name*

4. 指定されたシグニチャをシグニチャポリシーにバインドします。

   apply signature rule *rule-id*

   デフォルトでは、シグニチャはシグニチャポリシーにバインドされていません。

5. WIPSでシグニチャと一致するパケットを検出できるようにします。

   detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

   デフォルトでは、シグニチャと一致するパケットの検出はイネーブルになっています。

   統計情報収集インターバルは60秒、待機インターバルは600秒、アラームしきい値は50です。

シグニチャポリシーの適用

このタスクについて

シグニチャポリシーをVSDに適用すると、シグニチャポリシーがVSD内のすべての無線で有効になります。

手順

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. VSDビューを開始します。

   virtual-security-domain *vsd-name*

4. 指定されたシグニチャポリシーをVSDに適用します。

   apply signature policy *policy-name*

   デフォルトでは、シグニチャポリシーはVSDに適用されません。

デバイス分類の設定

デバイス分類について

WIPSでデバイスを分類できるようにするには、次の方法を使用します。

- **自動分類**: WIPSは、MACアドレスを追加することにより、デバイスを自動的に分類します。指定されたリストへのOUI(SS ID)。WIPSでは、ユーザ定義のAP分類規則を使用してAPを分類することもできます。
- **手動分類**: デバイスのカテゴリを手動で指定します。手動分類は、APだけに適用できます。

自動分類と手動分類の両方を設定すると、手動分類が有効になります。

自動デバイス分類ポリシーの設定

自動デバイス分類ポリシーの設定

1. システムビューを開始します。

System-view

2. WIPSビューを開始します。

   wips

3. 分類ポリシーを作成し、そのビューを開始します。

   classification policy *policy-name*

4. 自動デバイス分類を設定します。
   - 無効なOUIを持つデバイスを不正デバイスとして分類するようにWIPSを設定します。

     invalid-oui-classify illegal

     デフォルトでは、WIPSは無効なOUIを持つデバイスを不正デバイスとして分類しません。
   - 許可デバイスリストにMACアドレスを追加します。

     trust mac-address *mac-address*

     デフォルトでは、許可デバイスリストにMACアドレスは存在しません。
   - 信頼できるOUIリストにOUIを追加します。

     trust oui *oui*

     デフォルトでは、信頼できるOUIリストにOUIは存在しません。

     このコマンドは、AP分類だけに適用できます。
   - 信頼できるSSIDリストにSSIDを追加します。

     trust ssid *ssid-name*

     デフォルトでは、信頼できるSSIDリストにSSIDは存在しません。
   - MACアドレスをスタティック禁止デバイスリストに追加します。

     block mac-address *mac-address*

     デフォルトでは、スタティック禁止デバイスリストにはMACアドレスは存在しません。
   - 指定したAP分類ルールを分類ポリシーにバインドします。

     apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

     デフォルトでは、AP分類ルールは分類ポリシーにバインドされていません。

AP分類ルールの設定

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。

   wips

3. AP分類規則を作成し、そのビューを開始します。

   ap-classification rule *rule-id*

4. AP分類規則の基準を設定します。
   - APのRSSIと一致するようにAP分類ルールを設定します。

     rssi *value1* [**to** *value2*]

     デフォルトでは、AP分類ルールはAPのRSSIと一致しません。
   - APの無線サービスのSSIDと一致するようにAP分類ルールを設定します。

     ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

     デフォルトでは、AP分類ルールはAPの無線サービスのSSIDと一致しません。
   - AP分類ルールを設定して、APの実行時間を一致させます。

     up-duration *value1* [**to** *value2*]

デフォルトでは、AP分類ルールはAPの実行時間と一致しません。

- AP分類ルールを設定して、APに関連付けられるAP分類ルールを設定します。

  client-online *value1* [**to** *value2*]

  デフォルトでは、AP分類ルールはAPに関連付けられたクライアントの数と一致しません。
- APを検出するセンサーの数と一致するようにAP分類ルールを設定します。

  discovered-ap *value1* [**to** *value2*]

  デフォルトでは、AP分類ルールは、APを検出するセンサーの数と一致しません。
- APで使用されるセキュリティモードと一致するようにAP分類規則を設定します。

  Security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

  デフォルトでは、AP分類ルールはAPで使用されるセキュリティモードと一致しません。
- APで使用される認証モードと一致するようにAP分類規則を設定します。

  Authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

  デフォルトでは、AP分類ルールはAPで使用される認証モードと一致しません。
- APのOUI情報と一致するようにAP分類規則を設定します。

  oui *oui-info*

  デフォルトでは、AP分類ルールはAPのOUI情報と一致しません。
- AP分類ルール基準が論理AND関係になるように設定します。

  match all

  デフォルトでは、AP分類規則の基準は論理OR関係にあります。AP分類規則のいずれかの基準に一致する場合、APはAP分類規則と一致します。

  このコマンドを設定すると、AP分類ルールのすべての基準に一致する場合にだけ、APはAP分類ルールに一致します。

手動AP分類ポリシーの設定

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. 分類ポリシービューを開始します。

   classification policy *policy-name*
4. 指定したAPのカテゴリを指定します。

   manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

   デフォルトでは、APにカテゴリは指定されていません。

分類ポリシーの適用

このタスクについて

分類ポリシーをVSDに適用すると、VSD内のすべての無線で分類が有効になります。

手順

1. システムビューを開始します。

   System-view

2. WIPSビューを開始します。
   wips
3. VSDビューを開始します。
   virtual-security-domain *vsd-name*
4. 分類ポリシーをVSDに適用します。
   apply classification policy *policy-name*
   デフォルトでは、分類ポリシーはVSDに適用されません。

対策の設定

対策ポリシーの設定

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. 対策ポリシーを作成し、そのビューを開始します。
   countermeasure policy *policy-name*
4. APに対するWIPS対策を設定します。
   - WIPSで外部APに対する対策を実行できるようにします。
     countermeasure external-ap
     デフォルトでは、WIPSは外部APに対する対策を行いません。
   - WIPSで、誤って設定されたAPに対する対策を実行できるようにします。
     countermeasure misconfigured-ap
     デフォルトでは、WIPSは誤って設定されたAPに対する対策を行いません。
   - WIPSで、潜在的に認可されたAPに対する対策を実行できるようにします。
     countermeasure potential-authorized-ap
     デフォルトでは、WIPSは、潜在的に認可されたAPに対する対策を行いません。
   - WIPSで、潜在的な外部APに対する対策を実行できるようにします。
     countermeasure potential-external-ap
     デフォルトでは、WIPSは潜在的な外部APに対する対策を行いません。
   - WIPSで、潜在的な不正APに対する対策を実行できるようにします。
     countermeasure potential-rogue-ap
     デフォルトでは、WIPSは潜在的な不正APに対する対策を実行しません。
   - WIPSで不正なAPに対する対策を実行できるようにします。
     countermeasure rogue-ap
     デフォルトでは、WIPSは不正なAPに対する対策を行いません。
   - 分類されていないAPに対してWIPSが対策を実行できるようにします。
     countermeasure uncategorized-ap
     デフォルトでは、WIPSは分類されていないAPに対して対策を行いません。
5. クライアントに対するWIPS対策を設定します。
   - WIPSで、誤って関連付けられたクライアントに対する対策を実行できるようにします。

countermeasure misassociation-client

デフォルトでは、WIPSは誤ってアソシエートされたクライアントに対する対策を行いません。

- WIPSで不正なクライアントに対する対策を実行できるようにします。

  countermeasure unauthorized-client

  デフォルトでは、WIPSは不正なクライアントに対する対策を行いません。

- 分類されていないクライアントに対してWIPSが対策を実行できるようにします。

  countermeasure uncategorized-ap

  デフォルトでは、WIPSは分類されていないクライアントに対しては対策を行いません。

6. 攻撃者に対するWIPS対策を設定します。

- ブロードキャスト認証解除攻撃を開始するデバイスに対してWIPSが対策を実行できるようにします。

  countermeasure attack deauth-broadcast

  デフォルトでは、WIPSは、ブロードキャスト認証解除攻撃を開始するデバイスに対する対策を行いません。

- ブロードキャストアソシエーション解除攻撃を開始するデバイスに対してWIPSが対策を実行できるようにします。

  countermeasure attack disassoc-broadcast

  デフォルトでは、WIPSはブロードキャストアソシエーション解除攻撃を開始するデバイスに対する対策を行いません。

- WIPSでハニーポットAPに対する対策を実行できるようにします。

  countermeasure attack honeypot-ap

  デフォルトでは、WIPSはハニーポットAPに対する対策を行いません。

- WIPSで、ホットスポット攻撃を開始するデバイスに対する対策を実行できるようにします。

  countermeasure attack hotspot-attack

  デフォルトでは、WIPSは、ホットスポット攻撃を開始するデバイスに対する対策を行いません。

- 40 MHz帯域幅モードがディセーブルになっている802.11nデバイスに対してWIPSが対策を実行できるようにします。

  countermeasure attack ht-40-mhz-intolerance

  デフォルトでは、WIPSは、40 MHz帯域幅モードがディセーブルの802.11nデバイスに対しては対策を行いません。

- 不正な形式のパケットを送信するデバイスに対する対策をWIPSで実行できるようにします。

  countermeasure attack malformed-packet

  デフォルトでは、WIPSは不正な形式のパケットを送信するデバイスに対する対策を行いません。

- WIPSで、MITM攻撃を開始するデバイスに対する対策を実行できるようにします。

  countermeasure attack man-in-the-middle

  デフォルトでは、WIPSは、MITM攻撃を開始するデバイスに対する対策を行いません。

- WIPSで、オメルタ攻撃を開始するデバイスに対する対策を実行できるようにします。

  countermeasure attack omerta

  デフォルトでは、WIPSはOmerta攻撃を開始するデバイスに対する対策を行いません。

- 省電力攻撃を開始するデバイスに対してWIPSが対策を実行できるようにします。

  countermeasure attack power-save

  デフォルトでは、WIPSは省電力攻撃を開始するデバイスに対する対策を行いません。

- WIPSでソフトAPに対する対策を実行できるようにします。

  countermeasure attack soft-ap

  デフォルトでは、WIPSはソフトAPに対する対策を行いません。
- 弱いIVを使用する機器に対して、WIPSが対策できるようにする。

  countermeasure attack weak-iv

  デフォルトでは、WIPSは弱いIVを使用するデバイスに対しては対策を行いません。
- WIPSで、Windowsブリッジ攻撃を開始するデバイスに対する対策を実行できるようにします。

  countermeasure attack windows-bridge

  デフォルトでは、WIPSは、Windowsブリッジ攻撃を開始するデバイスに対する対策を行いません。
- 暗号化されていない認可クライアントに対してWIPSが対策を実行できるようにします。

  countermeasure attack unencrypted-trust-client

  デフォルトでは、WIPSは暗号化されていない認可クライアントに対しては対策を行いません。
- WIPSがすべての攻撃者に対して対策を実行できるようにします。

  countermeasure attack all

  デフォルトでは、WIPSはすべての攻撃者に対して対策を講じません。

7. WIPSでアドホックデバイスに対する対策を実行できるようにします。

   countermeasure adhoc

   デフォルトでは、WIPSはアドホックデバイスに対する対策を行いません。
8. WIPSで、指定されたデバイスに対する対策を実行できるようにします。

   countermeasure mac-address *mac-address*

   デフォルトでは、WIPSはデバイスに対する対策を行いません。
9. 攻撃者を検知したすべてのセンサーが攻撃者に対抗できるようにします。

   Select sensor all

   デフォルトでは、攻撃者を最後に検出したセンサーだけが、攻撃者に対抗します。

対策方針の適用

このタスクについて

VSDに対策ポリシーを適用すると、VSD内のすべての無線で対策ポリシーを有効にできます。

手順

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. VSDビューを開始します。

   virtual-security-domain *vsd-name*
4. VSDに対策ポリシーを適用します。

   apply countermeasure policy *policy-name*

   デフォルトでは、VSDには対策ポリシーは適用されません。

対策パケット送信間隔の設定

このタスクについて

センサーがチャネルで不正なデバイスを検出した場合に、チャネルで対策パケットを送信できるようにするには、次の作業を実行します。センサーは、スキャン期間内にだけ対策パケットをチャネルで送信します。また、センサーが対策パケットを送信する間隔を指定できます。チャネルスキャンの詳細については、『Radio Resources Management Configuration Guide』の「channel scanning configuration」を参照してください。

手順

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. 対策ポリシービューを開始します。
   countermeasure policy *policy-name*
4. センサーが対策パケットを送信する間隔を指定します。
   countermeasure packet-sending-interval *interval*
   デフォルトでは、センサーは30ミリ秒ごとに対策パケットを送信します。

拡張対策モードの有効化

このタスクについて

不正なAP上で同じSSIDを共有する2つの無線間でデュアルバンドクライアントがローミングしないようにするには、次の作業を実行します。

手順

1. システムビューを開始します。
   System-view
2. WIPSビューを開始します。
   wips
3. 対策ポリシービューを開始します。
   countermeasure policy *policy-name*
4. 拡張対策モードをイネーブルにします。
   countermeasure enhance
   デフォルトでは、拡張対策モードはイネーブルになっていません。

NATが設定されたクライアントの検出

このタスクについて

クライアント間のネットワーク共有を防止するようにNATが設定されているクライアントをAPが検出できるようにするには、次の作業を実行します。

手順

1. システムビューを開始します。

System-view

2. APビューまたはAPグループビューを開始します。
   - APビューを開始します。

     wlan ap *ap-name*
   - APグループビューを開始します。

     wlan ap-group *group-name*
3. NATが設定されたクライアントを検出するようにAPをイネーブルにします。

   wlan nat-detect enable

   デフォルト:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、NATが設定されたクライアントでの検出はディセーブルです。
4. NATが設定されたクライアントに対してWIPSが対策を実行できるようにします。

   wlan nat-detect countermeasure

   デフォルト:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、WIPSはNATが設定されたクライアントに対して対策を行いません。

アラーム無視機能の設定

このタスクについて

この機能が設定されている場合、WIPSはアラーム無視デバイスリスト内のワイヤレスデバイスに対してアラームをトリガーしません。

手順

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. アラーム無視デバイスリストにデバイスのMACアドレスを追加します。

   Igonrelist mac-address *mac-address*

   デフォルトでは、アラーム無視デバイスリストにMACアドレスは追加されません。

アクセスサービスを提供しながらWIPSスキャンを実行するようにAPを設定する

このタスクについて

この機能により、WIPS検出および保護機能は強化されますが、アクセスサービス機能は低下します。

手順

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

wips

3. アクセスサービスを提供しながらWIPSスキャンを実行するようにAPを設定します。

   access-scan enable

   デフォルトでは、APはアクセスサービスを提供している間はWIPSスキャンを実行しません。

OUIの設定

このタスクについて

Organizationally Unique Identifier(OUI;組織固有識別子)は、デバイスのMACアドレスの最初の3バイトであり、デバイスのベンダーを識別するために使用されます。

デバイスが起動すると、デフォルトのOUI構成ファイル内のUIがOUIライブラリに自動的にインポートされます。

次のように、OUIライブラリを手動で構成することもできます。

- **import oui**コマンドを使用して、OUIコンフィギュレーションファイルからOUIライブラリにOUIをインポートします。

  インポートされたOUI、更新されたOUI、既存のOUI、およびインポートに失敗したOUIの数が表示されます。
- **export oui**コマンドを使用して、OUIライブラリ内のUIをOUIコンフィギュレーションファイルにエクスポートします。

  正常にエクスポートされたOUIの数と、エクスポートに失敗したOUIの数が表示されます。

OUIのインポート

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. OUI構成ファイルからOUIライブラリにOUIをインポートします。

   import oui *file-name*

OUIのエクスポート

1. システムビューを開始します。

   System-view
2. WIPSビューを開始します。

   wips
3. OUIライブラリ内のUIをOUI構成ファイルにエクスポートします。

   export oui *file-name*

クライアントアソシエーションエントリの高速学習のイネーブル化

このタスクについて

クライアントアソシエーションエントリは、クライアントがAPにアソシエートした後にACに保存されるエントリです。

この機能がイネーブルでない場合、センサーは、クライアントがAPに正常に関連付けられた後にだけ、クライアントアソシエーションエントリを学習できます。この機能がイネーブルになると、センサーは、アソシエーションプロセス中にクライアントアソシエーションエントリを学習できます。

センサーがアソシエーションプロセス中にクライアントアソシエーションエントリを学習した場合、センサーは、APとクライアント間のアソシエーション要求または応答を検出するたびにエントリを更新します。

この機能によりアソシエーションの効率性は向上しますが、アソシエーションの精度は低下します。この機能は、ネットワーク内で高速な攻撃検出と対策が必要な場合にだけイネーブルにすることをお勧めします。

手順

1. システムビューを開始します。
   system-view
2. WIPSビューを開始します。
   wips
3. 攻撃検出ポリシービューを開始します。
   detect policy *policy-name*
4. クライアントアソシエーションエントリの高速学習をイネーブルにします。
   client-association fast-learn enable
   デフォルトでは、クライアントアソシエーションエントリの高速学習はディセーブルです。

WIPSの表示コマンドおよびメンテナンスコマンド

任意のビューでdisplayコマンドを実行し、ユーザビューでコマンドをリセットします。

タスク	コマンド
すべてのセンサーに関する情報を表示します。	**display wips sensor**
センサーから収集されたWALN攻撃検出統計情報を表示します。	**display wips statistics [receive | virtual-security-domain** *vsd-name* **]**
不正デバイスに対してWIPSが実行した対策に関する情報を表示します。	**display wips virtual-security-domain** *vsd-name* **countermeasure record**
VSDで検出されたワイヤレスデバイスに関する情報を表示します。	**display wips virtual-security-domain** *vsd-name* **device [ap [adhoc | authorized | external | mesh | misconfigured | potential-authorized | potential-external | potential-rogue | rogue | uncategorized] | client [[dissociative-client] [authorized | misassociation | unauthorized | uncategorized]] | mac-address** *mac-address* **] [verbose]**
検出されたNAT設定済みクライアントに関する情報を表示します。	**display wlan nat-detect [mac-address** *mac-address* **]**
OUIライブラリ内のすべての埋め込まれたUIを削除します。	**reset wips embedded-oui**
すべてのセンサーから収集されたWALN攻撃検出統計情報をクリアします。	**reset wips statistics**
不正デバイスに対してWIPSが実行した対策に関する明確な情報。	**reset wips virtual-security-domain** *vsd-name* **countermeasure record**
VSDの学習済みAPまたはクライアントエントリをクリアします。	**reset wips virtual-security-domain** *vsd-name* **{ ap { all | mac-address** *mac-address* **} | client { all | mac-address** *mac-address* **} | all }**
検出されたNAT設定クライアントに関する情報をクリアします。	**reset wlan nat-detect**

WIPSの設定例

このドキュメントに記載されているAPモデルおよびシリアル番号は、あくまでも例です。APモデルおよびシリアル番号のサポートは、ACモデルによって異なります。

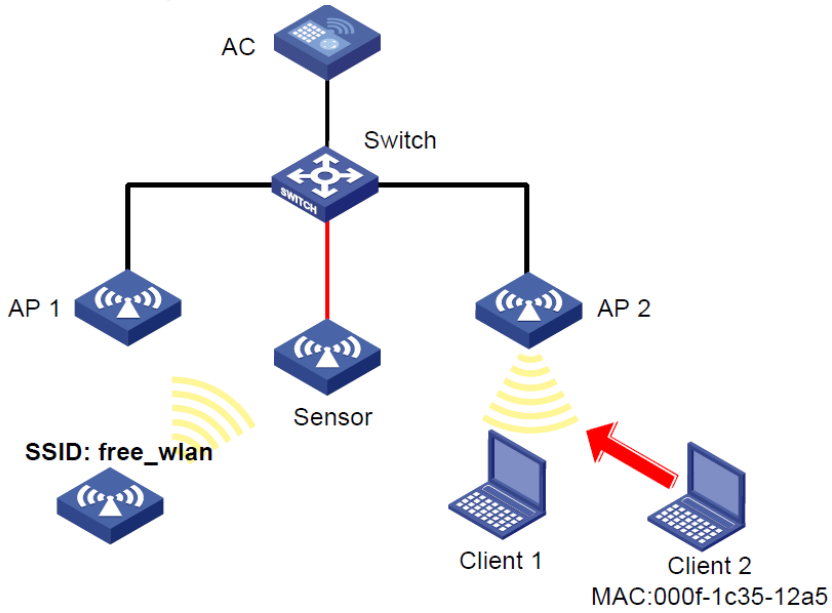
例:デバイス分類と対策の設定

ネットワーク構成

図3に示すように、センサーはスイッチを介してACに接続されています。AP 1およびAP 2は、SSID abcを介してクライアントにワイヤレスサービスを提供します。次のタスクを実行します。

- センサーのWIPSをイネーブルにします。
- ワイヤレスデバイス分類を設定して、MACアドレス000f-1c35-12a5を静的な禁止デバイスリストに追加し、SSID abcを信頼できるSSIDリストに追加します。
- WIPSが潜在的な外部APおよび不正クライアントに対する対策を実行できるように、対策を設定します。

図3 ネットワーク図



手順

ACでワイヤレスサービスを構成します。（詳細は省略）

ワイヤレスサービスの設定の詳細については、「WLANアクセスの設定」を参照してください。

vsd1という名前のVSDを作成します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain vsd1

[AC-wips-vsd-vsd1] quit

[AC-wips] quit

Sensorという名前のAPを作成し、APに対してWIPSを有効にします。

[AC] wlan ap Sensor model WA4320i-ACN

[AC-wlan-ap-Sensor] serial-id 210235A1GQB139000435

[AC-wlan-ap-Sensor] radio 1

[AC-wlan-ap-Sensor-radio-1] radio enable

[AC-wlan-ap-Sensor-radio-1] wips enable

[AC-wlan-ap-Sensor-radio-1] quit

APセンサーをVSDvsd1に追加します。

[AC-wlan-ap-Sensor] wips virtual-security-domain vsd1

[AC-wlan-ap-Sensor] quit

class1という名前の分類ポリシーを作成し、クライアント2のMACアドレスを禁止デバイスリストに

追加し、SSIDabcを信頼できるSSIDリストに追加します。

[AC] wips

[AC-wips] classification policy class1

[AC-wips-cls-class1] block mac-address 000f-1c35-12a5

[AC-wips-cls-class1] trust ssid abc

[AC-wips-cls-class1] quit

分類ポリシーclass1をVSDvsd1に適用します。

[AC-wips] virtual-security-domain vsd1

[AC-wips-vsd-vsd1] apply classification policy class1

[AC-wips-vsd-vsd1] quit

protectという名前の対抗策ポリシーを作成し、WIPSが無許可のクライアントおよび潜在的な外部APに対して対抗策を講じられるようにします。

[AC-wips] countermeasure policy protect

[AC-wips-cms-protect] countermeasure unauthorized-client

[AC-wips-cms-protect] countermeasure potential-external-ap

[AC-wips-cms-protect] quit

対抗策ポリシープロテクトをVSDvsd1に適用します

[AC-wips] virtual-security-domain vsd1

[AC-wips-vsd-vsd1] apply countermeasure policy protect

[AC-wips-vsd-vsd1] quit

[AC-wips] quit

設定の確認

VSDvsd1のワイヤレスデバイス分類情報を表示します。

[AC] display wips virtual-security-domain vsd1 device

Total 3 detected devices in virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
Unauth - unauthorized; Uncate - uncategorized;
(A) - associate; (C) - config; (P) - potential

MAC address Type Class Duration Sensors Channel Status

00e0-fc00-5829 AP Auth 00h 10m 24s 1 149 Active

000f-e228-2528 AP Auth 00h 10m 04s 1 149 Active

000f-e223-1616 AP Ext(P) 00h 10m 46s 1 149 Active

000f-1c35-12a5 Client Unauth 00h 10m 02s 1 149 Active

000f-e201-0102 Client Auth 00h 10m 02s 1 149 Active

出力は、MACアドレス000f-e223-1616のAPが潜在的な外部APとして分類され、MACアドレス000f-1c35-12a5のクライアントが無許可のクライアントとして分類されていることを示しています。

WIPSがデバイスに対して講じた対策に関する情報を表示します。

[AC] display wips virtual-security-domain vsd1 countermeasure record

Total 2 times countermeasure, current 2 countermeasure record in virtual-security-domain vsd1

Reason: Attack; Ass - associated; Black - blacklist;
Class - classification; Manu - manual;

MAC address Type Reason Countermeasure AP Radio ID Time

00e0-fc00-5829 AP Class Sensor 1 2014-06-03/09:30:25

000f-e228-2528 AP Class Sensor 1 2014-06-03/19:31:56

000f-e223-1616 AP Class Sensor 1 2014-06-03/10:30:36

000f-1c35-12a5 Client Class Sensor 1 2014-06-03/09:13:26

000f-e201-0102 Client Class Sensor 1 2014-06-03/09:33:46

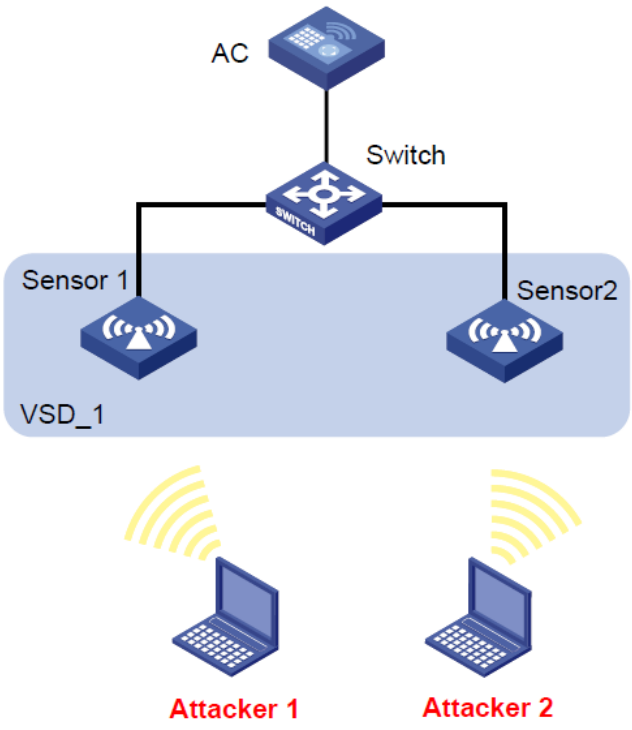
この出力は、WIPSがMACアドレス000f-1c35-12a5の無許可のクライアントおよびMACアドレス000f-e223-1616の潜在的な外部APに対して対策を講じたことを示しています。

例:不正な形式のパケットおよびフラッド攻撃検出の設定

ネットワーク構成

図4に示すように、スイッチを介してACに接続する2つのAPをセンサーとして設定します。VSD VSD_1にSensor 1とSensor 2を追加します。不正な形式のパケット検出とフラッド攻撃検出を設定して、WIPSがビーコンフラッド攻撃または重複したIEを持つ不正な形式のパケットを検出したときにアラームをトリガーできるようにします。

図4 ネットワーク図



手順

```
# ACでワイヤレスサービスを構成します。（詳細は省略）
# ワイヤレスサービスの設定の詳細については、「WLANアクセスの設定」を参照してください。
# Sensor1という名前のAPを作成し、APに対してWIPSを有効にします。
<AC> system-view
[AC] wlan ap sensor1 model WA4320i-ACN
[AC-wlan-ap-sensor1] serial-id 210235A1GQB139000435
[AC-wlan-ap-sensor1] radio 1
[AC-wlan-ap-sensor1-radio-1] radio enable
[AC-wlan-ap-sensor1-radio-1] wips enable
[AC-wlan-ap-sensor1-radio-1] return
#  Sensor2という名前のAPを作成し、APに対してWIPSを有効にします。
<AC> system-view
[AC] wlan ap sensor2 model WA4320i-ACN
[AC-wlan-ap-sensor2] serial-id 210235A1GQB139000436
[AC-wlan-ap-sensor2] radio 1
[AC-wlan-ap-sensor2-radio-1] radio enable
[AC-wlan-ap-sensor2-radio-1] wips enable
[AC-wlan-ap-sensor2-radio-1] quit
[AC-wlan-ap-sensor2] quit
# VSD_1という名前のVSDを作成します。
[AC] wips
[AC-wips] virtual-security-domain VSD_1
[AC-wips-vsd-VSD_1] quit
# dtc1という名前の攻撃検出ポリシーを作成します。
[AC-wips] detect policy dtc1
#  IEが重複している不正な形式のパケットの検出を有効にし、クワイエット時間を50秒に設定します。
[AC-wips-dtc-dtc1] malformed duplicated-ie quiet 50
# ビーコンフラッド攻撃の検出を有効にし、統計間隔、しきい値、および休止時間をそれぞれ100秒、
# 200秒、および50秒に設定します。
[AC-wips-dtc-dtc1] flood beacon interval 100 quiet 50 threshold 200
[AC-wips-dtc-dtc1] quit
# 攻撃検出ポリシーdtc1をVSDVSD_1に適用します。
[AC-wips] virtual-security-domain VSD_1
[AC-wips-vsd-VSD_1] apply detect policy dtc1
[AC-wips-vsd-VSD_1] quit
[AC-wips] quit
# VFDVSD1にセンサーを追加します。
[AC] wlan ap sensor1
[AC-wlan-ap-sensor1] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor1] quit
# APセンサー2をVSDVSD_1に追加します。
[AC] wlan ap sensor2
[AC-wlan-ap-sensor2] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor2] return
```

設定の確認

WIPSがWLANで攻撃を検出しなかった場合に、パケット統計を表示します。出力は、不正な形式の
パケットまたはフラッド攻撃メッセージが存在しないことを示しています。
<AC> display wips statistics receive
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0

Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
WIPSがビーコンフラッド攻撃および重複したIEを含む不正な形式のパケットを検出したときにパケット
統計を表示します。出力は、IEが重複している不正な形式のパケットの場合に検出されたメッセージの
数が28であり、ビーコンフラッド攻撃の場合に検出されたメッセージの数が18であることを示しています。
<AC> display wips statistics receive
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 18
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0

Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 28
Detected fata-jack messages: 0

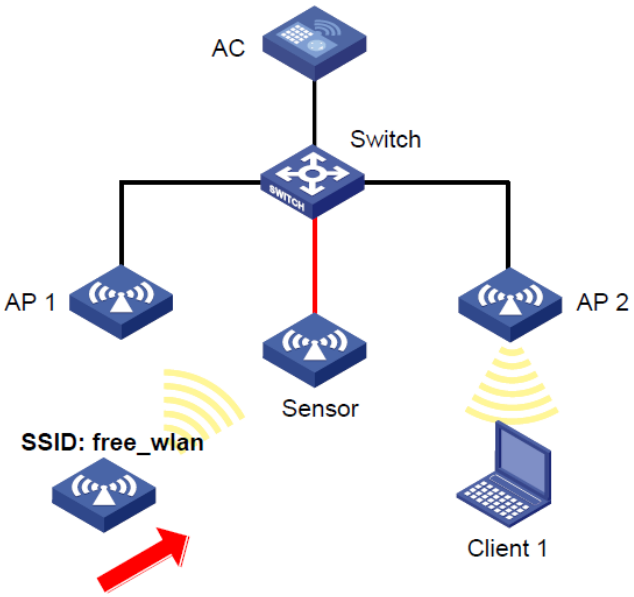
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0

例:シグニチャベースの攻撃検出の設定

ネットワーク構成

図5に示すように、AP 1とAP 2は、SSID abcを介してクライアントに無線サービスを提供します。センサーのWIPSをイネーブルにし、SSIDがabcでないビーコンフレームを検出したときにWIPSがアラームをトリガーできるようにシグニチャを設定します。

図5 ネットワーク図



手順

ACでワイヤレスサービスを構成します。（詳細は省略）

ワイヤレスサービスの設定の詳細については、「WLANアクセスの設定」を参照してください。

Sensor1という名前のAPを作成し、APに対してWIPSを有効にします。

<AC> system-view

[AC] wlan ap sensor1 model WA4320i-ACN

[AC-wlan-ap-sensor1] serial-id 210235A1GQB139000435

[AC-wlan-ap-sensor1] radio 1

[AC-wlan-ap-sensor1-radio-1] radio enable

[AC-wlan-ap-sensor1-radio-1] wips enable

[AC-wlan-ap-sensor1-radio-1] quit

[AC-wlan-ap-sensor1] quit

vsd1という名前のVSDを作成します。

[AC] wips

[AC-wips] virtual-security-domain vsd1

[AC-wips] quit

APセンサー1をVSDvsd1に追加します。

[AC] wlan ap sensor1

[AC-wlan-ap-sensor1] wips virtual-security-domain vsd1

[AC-wlan-ap-sensor1] quit

シグニチャ1を作成し、ビーコンフレームに一致するようにサブシグニチャを設定し、

SSIDがabcではないフレームに一致するようにサブシグニチャを設定します。

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] frame-type management frame-subtype beacon

[AC-wips-sig-rule-1] ssid not equal abc

[AC-wips-sig-rule-1] quit

sig1という名前のシグニチャポリシーを作成し、シグニチャ1をシグニチャポリシーsig1にバインドします。

[AC-wips] signature policy sig1

[AC-wips-sig-sig1] apply signature rule 1

WIPSがシグニチャに一致するパケットを検出できるようにし、統計情報の収集間隔、静止時間、

およびアラームしきい値をそれぞれ5秒、60秒、および60に設定します。

[AC-wips-sig-sig1] detect signature interval 5 quiet 60 threshold 60

[AC-wips-sig-sig1] quit

シグニチャポリシーsig1をVSDvsd1に適用します。

[AC] wips

[AC-wips] virtual-security-domain vsd1

[AC-wips-vsd-vsd1] apply signature policy sig1

[AC-wips-vsd-vsd1] quit

設定の確認

センサーがSSIDfree_wlanを使用してワイヤレスサービスを検出したときに、ACがセンサーから
アラームを受信することを確認します。
WIPS/5/WIPS_SIGNATURE: -VSD=vsd1-RuleID=1; Signature rule matched.
センサーから収集した攻撃検出情報を表示します。出力は、シグニチャに一致するパケットの
検出されたメッセージの数が26であることを示しています。
[AC] display wips statistics receive
Information from sensor
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0

Detected AP spoof ad-hoc messages: 0

Detected ad-hoc spoof AP messages: 0

Detected client spoof AP messages: 0

Detected weak IV messages: 0

Detected excess AP messages: 0

Detected excess client messages: 0

Detected sig rule messages: 26