Cloud Integration Point(CIP) と自動無線デバイス分類/検知/防御システム(WIPS)

イントロダクション

今日の企業の無線 LAN ネットワーク環境はあらゆる危険に溢れており、次々出現するセキュリティ上の脅威への対策が必要です。組織の既存のシステムが古くなり、企業内の無線 LAN ネットワークを安全に保護していない場合、無線 LAN 環境を保護する新しい手段の評価、検討が至急必要となります。自社の古い既存システムのセキュリティを確保することは、あらゆる規模の企業にとって非常に大きな労力を必要としますが、既存の無線 LAN システムにおけるセキュリティ確保に関して、ウォッチガードがご提案できるソリューションがあります。ウォッチガードの Cloud Integration Point(CIP) により、WatchGuard Wi-Fi Cloud と以下のような他社製のオンプレミスのワイヤレスコントローラ機器や、イベントログ管理サービスとの統合が可能となります。

- Aruba モビリティコントローラ
- Cisco ワイヤレス LAN コントローラ
- HP マルチサービス モビリティ (MSM) コントローラ
- ArcSight エンタープライズセキュリティ管理 (ESM)
- Syslog server

自動無線デバイス分類 / 自動脅威検知 / 防御

既存の機器はそのまま、ただウォッチガードの WIPS センサを追加するだけ

ウォッチガードの各アクセスポイントは WIPS 専用機器として設置可能です。そしてそれは既存の無線 LAN アクセスポイントに当社の WIPS センサを重ね合わせて稼働できることを意味します。特長として、ウォッチガードの WIPS センサはサードパーティのアクセスポイントに対応し、異なるブランドであっても同時に設置することができます。Cisco、Aruba、HP それぞれのメーカーの AP はウォッチガードの Wi-Fi Cloud と他社の無線 LAN コントローラ機器間との連携によって、より大規模なネットワークをサポートし追加の管理機能の恩恵を受けることができます。

1 台の WIPS センサに 3 台のアクセスポイントを推奨しています。そうすることで、Wi-Fi トラフィックをユーザーに配信するのではなく、ワイヤレススキャンに 100%専念し、ワイヤレスの脅威からビジネスを守る、前例のない WIPS セキュリティによる保護を提供します。

自動無線デバイス分類 / 検知 / 防御システム (WIPS) センサを重ね合わせて展開

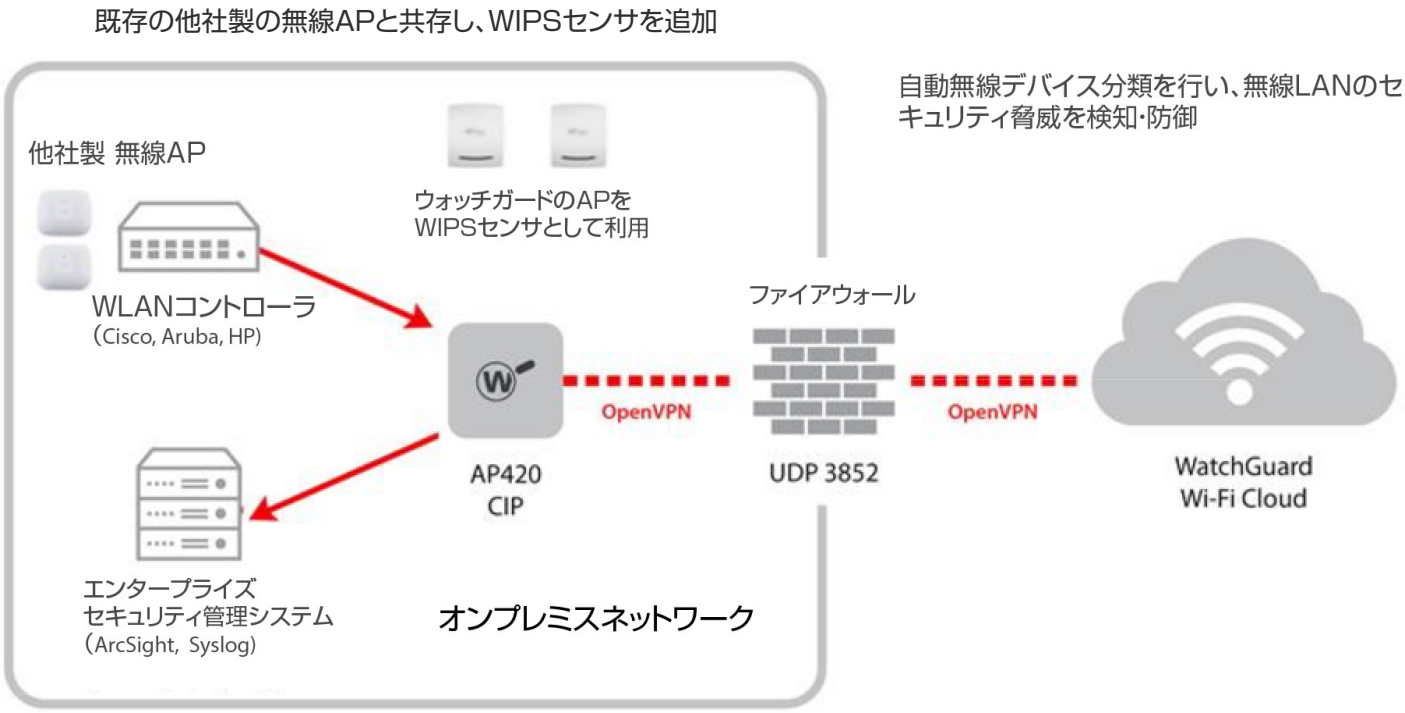
Cloud Integration Point(CIP) 機能による Cisco、Aruba、および HP WLAN コントローラとの統合により、WatchGuard Wi-Fi Cloud がサードパーティのコントローラで管理されているデバイスに関する情報を取得できるようになり、他社製の機器による無線 LAN 環境に重ねて設置されている WIPS センサの管理も容易です。Wi-Fi Cloud は、サードパーティの WLAN コントローラで管理されているデバイス情報を自動無線デバイス分類およびデバイスの位置追跡に使用します。この Cloud Integration Point(CIP) は、アクセスポイント AP420 でサポートされています。

エンタープライズセキュリティ管理（ESM）サーバとの統合により、Wi-Fi Cloud はイベントと監査ログをこれらのサーバに送信できるため、管理者は既存のインフラストラクチャを使用して Wi-Fi Cloud のイベントとログを管理できます。Wi-Fi Cloud とオンプレミスのシステムとの統合により、既存のインフラストラクチャを引き続き使用しながら、Wi-Fi Cloud の次の重要なセキュリティ上の利点を活用できるようになります。

- 他社製 Wi-Fi コントローラの管理下にある承認済みデバイスの WIPS 機能による自動分類
- Wi-Fi クライアントの位置追跡
- トラブル対応に利用できるイベント監視とログ分析に関する統合ビューを得るために、イベントと監査ログを中央のログサーバーに送信します。

Cloud Integration Point(CIP) の機能

Wi-Fi Cloud とオンプレミスのシステムを統合する上での重要な課題は、通常、これらのシステムがファイアウォールの内側にあるプライベートネットワーク上に存在することです。Wi-Fi Cloud を使用してネットワーク内の CIP デバイスを複数の社内システムと統合することができます。これにより、メッセージは機密の扱いとなり、傍受することができなくなります。



Wi-Fi Cloud ソリューションは、社内ネットワークで Cloud Integration Point (CIP) として AP420 を使用します。AP は、CIP モードで設定されている場合、アクセスポイントまたは WIPS センサ機能を実行せず、UDP ポート 3852 で Wi-Fi Cloud への安全な OpenVPN トンネルを作成します。CIP から Wi-Fi Cloud への通信が OpenVPN トンネルの作成を許可するため、このポートはファイアウォール上で開く必要があります。その後の通信はすべてトンネル経由で行われます。CIP と Wi-Fi Cloud 間で送信されるすべてのデータは、OpenVPN トンネルを介して送信され、AES-256-CBC 暗号化で保護されます。CIP にはファイアウォールが含まれており、定義された宛先と CIP 用に設定されたポートにのみトラフィックを転送します。また、CIP は、トンネルから LAN へのトラフィックにネットワークアドレス変換（NAT）を使用します。LAN から Wi-Fi Cloud への接続は確立できません。CIP の要件と設定手順の詳細については、WatchGuard Support Center を参照してください。

全く新しい WIPS（自動無線デバイス分類 / 検知 / 防御システム）

ウォッチガードの WIPS には、特許取得済みの次の検知および防止方法が含まれています。

- 以下を含む一般的な無線 LAN の脅威を検知、防止
  - 中間者攻撃 (MitM)
  - 偽装アクセスポイント
  - 誤設定のアクセスポイント
  - 不正アクセスポイント
  - 不適切かつ違法な使用
  - アクセスポイントの MAC アドレス偽装
  - カルマ攻撃
  - WPA/WPA2 暗号化クラッキング (KRACK)
- スマートフォンやタブレットなどのクライアントや、アクセスポイントの正確かつ自動的な分類を可能にする
  - 承認済み　- ネットワークに接続されている既知のアクセスポイント
  - 外部　- ネットワークに接続されていない近隣のアクセスポイント
  - 不正アクセスポイント　- ネットワークに接続されている未知のアクセスポイント
- 設定変更可能なポリシーによる Wi-Fi クライアント接続の制御
- PCI や一般的な Wi-Fi セキュリティ指針など、既知の規格に対するネットワークの準拠状況をすばやく確認するため詳細なレポートを実行

この高度な検知プロセスは、市場にある他の WIPS 製品には不足しているものです。そしてこの検知プロセスは、隣接の無線 LAN ネットワークを不正に妨害することなく、許容できない接続のみを直ちに遮断することができます。

ウォッチガードの特徴は、安全なネットワークを提供することであり、当社独自の効果的な WIPS ソリューションが最も強力なレベルのセキュリティを提供します。さらに、Wi-Fi Cloud 管理により、ユーザは無線設定や自己修復メッシュなど多彩な機能を容易に最適化でき、ロケーション分析機能や、マーケティングツールにより強力なビジネス上の洞察を得ることができます。

ビジネスの成長を加速させるクラウド管理型セキュア無線 LAN ソリューション、Wi-Fi Cloud に関する詳細は www.watchguard.co.jp/wifi をご覧ください。

WatchGuard について

WatchGuard® Technologies, Inc. は、世界中の 8 万人以上のお客様に、ネットワークセキュリティ、Secure Wi-Fi、ネットワークインテリジェンス製品 / サービスを提供するグローバルリーダーです。当社の使命は、エンタープライズグレードのセキュリティをあらゆる種類、規模の企業がシンプルに利用できるようにすることです。ワシントン州シアトルに本社を置き、北米、ヨーロッパ、アジア太平洋、中南米など世界各国にオフィスを構えています。 詳細については、WatchGuard.com をご覧ください。

ウォッチガード・テクノロジージャパン株式会社
〒106-0041　東京都港区麻布台1-11-9 BPRプレイス神谷町5階　TEL:03.5797.7205　FAX:03.5797.7207
http://www.watchguard.co.jp jpnsales@watchguard.com