ホワイトペーパー

既存の FortiGate が無線 LAN コントローラに、統合された運用管理を提供

FortiGate を活用した無線 LAN 機能の概要

シンアクセスポイント　UTMとの統合　最新のIEEE802.11n準拠

はじめに

ネットワークセキュリティのために開発された専用オペレーティングシステム、FortiOSは、FortiGateプラットフォームの様々なソフトウェア基盤を支えています。その最新バージョンでは、無線LANコントローラ機能を含む様々な機能追加・拡張が実現されています。FortiOSに含まれる無線LANコントローラ機能を活用することで、新たに専用の無線LANコントローラを追加することなく、セキュリティ対策を強化したビジネス規模の無線LANを構築することが可能です。同時に、有線ネットワークと無線ネットワークの管理を一つに統合することも可能となります。FortiGateプラットフォームをベースにした無線ネットワークは、これまでは有線ネットワークで実現されていた統合脅威管理（UTM）機能がもたらす全ての利点を享受することが可能です。よって、FortiGate で実現可能なセキュリティ対策機能を活用し、無線ネットワーク トラフィックが社内LANまたはインターネットの外にルーティングされる前に、全てのネットワーク トラフィックをFortiGateでトンネル化し、よりセキュアな無線LANの構築が可能となります。

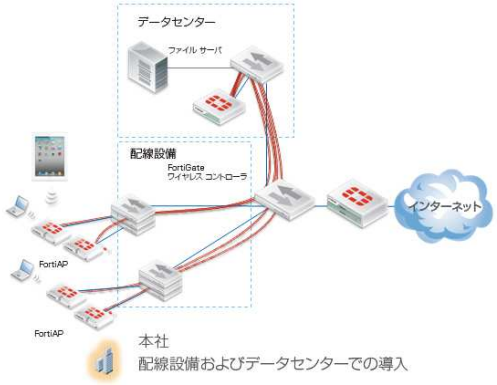
フォーティネットのソリューションは、これまで無線LANのエンタープライズレベルでの導入で問題視されていたセキュリティ機能との統合における課題を解決し、最も厳しいセキュリティ ポリシーで無線ネットワーク接続の統合セキュリティを提供します。

シンアクセスポイント、FortiAP-220B

ネットワークの範囲や収容能力の要件が大規模なサイトでは、集中型のコントローラによるシンアクセスポイント　アーキテクチャの選択が最適です。シンアクセスポイントであるFortiAP-220Bは、RF無線として機能し、CAPWAPトンネルを使用して、全てのトラフィックを無線LANコントローラとして設定されているFortiGateデバイスに直接転送します。FortiAP-220Bは、FortiGateに標準搭載されている無線LANコントローラ下で稼動するシンアクセスポイントです。

FortiAP-220Bの導入

FortiGateコントローラとの接続が確立できれば、FortiAP-220Bは、ネットワーク内のどのポイントにも設置することが可能です。FortiAP-220Bは、ローカルでTKIPまたはAES暗号を実行し、すべての認証、チャネル割当、トランスミッターの出力レベル設定および不正なアクセスポイントの検知や抑制といった複雑な機能を集中型の無線LANコントローラであるFortiGateに任せます。無線LANのセキュリティのために、CAPWAPトンネル内部での無線トラフィックはLANデバイスを迂回し、FortiGateデバイスで終端します。ここで、データ処理とルーティング要求のためにトラフィック転送を許可します。



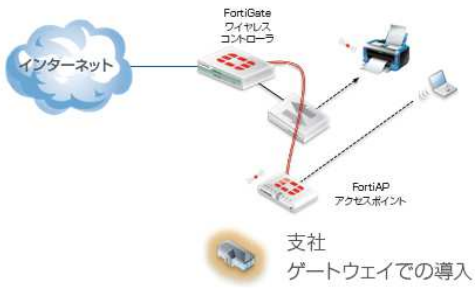
本社
配線設備およびデータセンターでの導入

ネットワーク配線設備／データセンターでの導入

FortiAP-220Bは、エンタープライズレベル、全社レベルでの導入に最適です。複数台のFortiAPが導入され、各FortiAPが、数多くの無線クライアントにサービスを提供します。無線LANコントローラとしてのFortiGateデバイスは、社内ネットワークから無線LANをセグメント化します。これによって、それぞれのFortiAPクライアントに対して別々のポリシーを導入することが可能になります。このセグメント化されたLANからルーティングされたトラフィックはデータセンターで終端します。リソースへのアクセスを許可する前に、別の無線LANコントローラにそれぞれの異なるポリシーを適用します。

ゲートウェイにおける導入

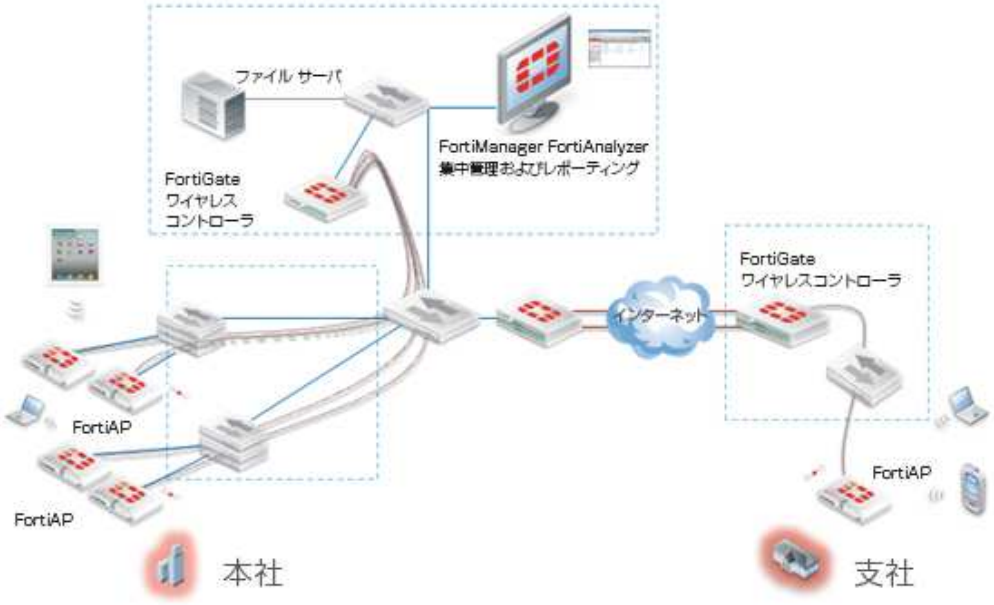
ゲートウェイにおける導入は、ブランチオフィス、サテライトオフィスなどの小規模のリモートロケーションに最適です。このゲートウェイモードでは、全ての無線トラフィックは、インターネットへのゲートウェイ層で無線LANコントローラのFortiGateにより管理されます。データのセキュリティを保護するために文書印刷などのローカルトラフィックは社内LAN内部で処理されます。



支社
ゲートウェイでの導入

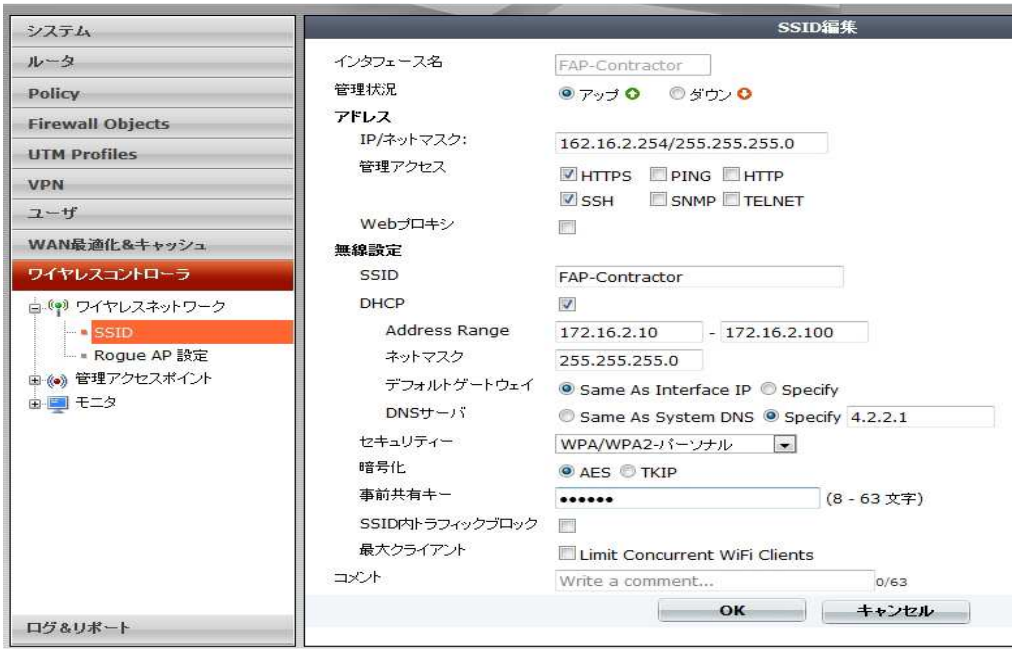
一元化された集中管理、構成設定およびレポーティング

全てのFortiAP及びSSIDは、グローバルに制御される個々のプロファイルによって独立したインタフェースを形成します。無線インフラの分散型導入においてグローバル管理を簡素化するために、FortiManagerとFortiAnalyzerによって、一元化された管理、ログ収集、レポーティングを提供します。



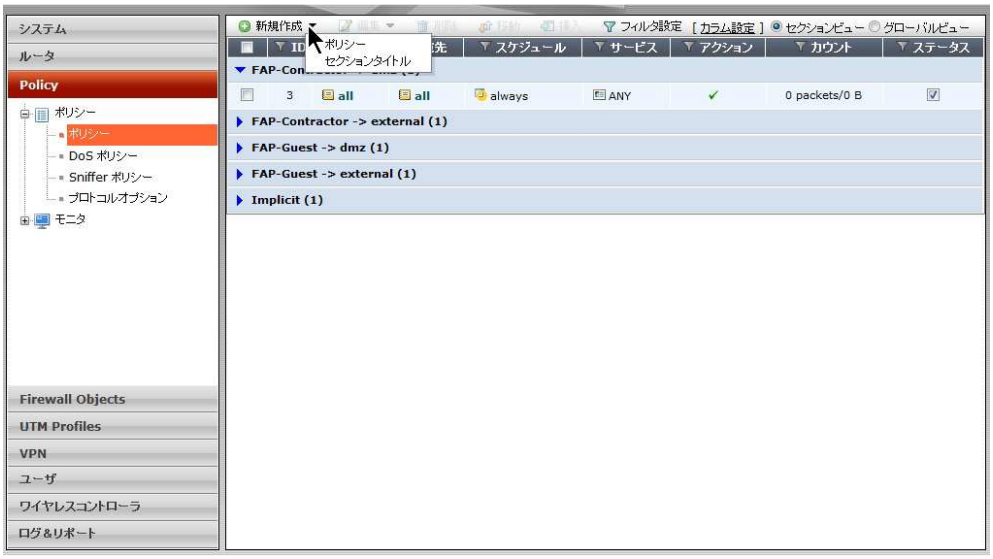
自動プロファイル設定

FortiAPがLANに新たに設置されると、FortiGateはレイヤ2またはレイヤ3ネットワーク間で新設されたアクセスポイントを自動的に検出します。FortiGateの管理GUIを通して、検出したアクセスポイントのSSIDプロファイルを設定しカスタマイズすることができます。こうした設定は、全ての関連したアクセスポイントおよびFortiGateにほぼリアルタイムに反映されます。このような自動プロビジョニングにより運用上の効率性を向上し、管理面での複雑性を軽減します。



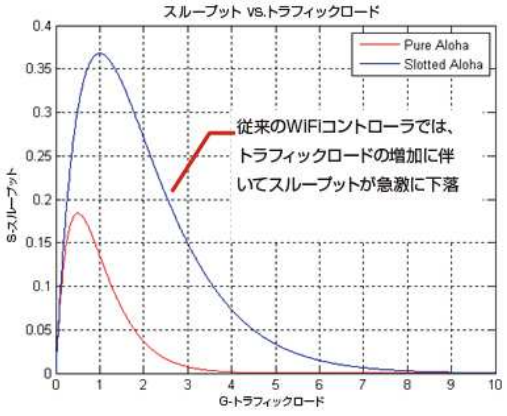
統合された有線および無線トラフィック管理

FortiGateによって、有線トラフィックと無線トラフィックの両方を1つのコンソールに統合することが可能になります。自社ネットワークを、有線、無線を問わず、1つの管理インタフェースから一元管理することを可能にします。さらに、有線LAN内のUTMおよびファイアウォールと同一のポリシーを無線トラフィックに適用することができます。これによって、ユーザがどのようにネットワークにアクセスしているか、またどのようなアプリケーションを使用しているかを完全に可視化することが可能になります。例えば、ファイアウォールタブを使って、ルールベースのポリシーと同時にレイヤ7 DPI（Deep Packet Inspection）を設定することで、ユーザがスパムメールの送信元になることを防止することができます。



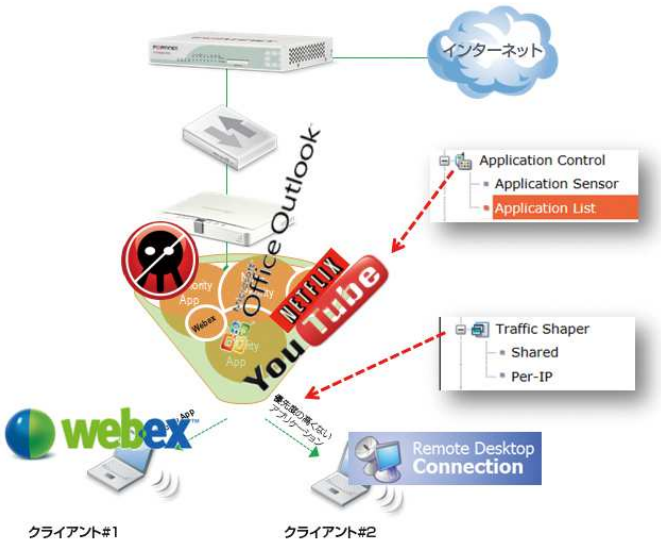
IEEE 802.11eおよびアプリケーションベースのQoS

フォーティネットは IEEE 802.11 WME（Wireless Multimedia Enhancement）をサポートしています。これは音声や画像のストリーミングデータを効率良く伝送し、サービスを区分化するための有益なトラフィック分類手段になります。しかしながら、WME はユーザやアプリケーションを認知するものではありません。FortiOS は、WME を補完し、アプリケーションベースの QoS をサポートすることで、より柔軟性のある QoS モデルを実現しています。FortiOS が提供するポリシーベースの無線 LAN コントローラの WAN 最適化機能は、ビジネス クリティカルな基幹アプリケーションを重要でないアプリケーションより優先的に処理することを可能にします。たとえば、既存の WME ベースの無線 LAN コントローラはデバイスに依存し、無線アクセスポイントに送信される前に自身のパケットをマークします。これによって、アクセスポイントのために QoS ジョブを簡単にします。しかしながら、ラップトップ上で稼動するほとんどのアプリケーション、特に、Web ベースのアプリケーションや SaaS アプリケーションはこの利点を活用することができません。これらのアプリケーションは Web ブラウザ上で本質的に拘束されており、無線上で実行していることを全く意識していません。例えば、Youtube ビデオを見ているユーザは、同じ重要な帯域幅を Web 会議の WebEx プレゼンテーションをお客様に行っているユーザと競合しています。この帯域幅競合は、VNC（Virtual Network Computing）、リモート デスクトップ共有や VMware のシンクライアント使用などといった場合に、マウスポインターをフリーズさせてしまいます。さらに悪いことに、ユーザの数が増えるにつれてネットワークの総スループットが減少し、従来の無線製品は、どれがビジネスクリティカルか全く分からないため、これらのユーザ間で均等に帯域幅を共有します。これらの問題のためにさらに帯域幅を費やすという従来の方法が採用されがちですが、単に帯域を増加させるのは解決にはなりません。



ここに、レイヤ 7 DPI（Deep Packet Inspection）テクノロジとしての次世代の無線ネットワークの意義があります。次世代の無線ネットワークは、クライアントの無線アプリケーションを分類し、ユーザ毎、またはアプリケーションレートリミッタごとに適用し、共有されている帯域幅を効果的に活用することを可能にします。

この WAN エッジで実証済みの ASIC ベースの DPI テクノロジを適用している企業はフォーティネットだけです。FortiOS はアプリケーション検知および無線 LAN コントローラと UTM を活用して、無線通信に対してビジネス規模の QoS を実現します。フォーティネットのソリューションを採用すれば、ユーザは業務アプリケーションやそれらのグループをより優先度が高いクラスに分類するだけで帯域幅の不足から開放され、業務アプリケーションや業務ユーザのためにネットワーク領域を確保できます。



完全な認証および暗号オプション

データ暗号およびユーザ認証設定は、SSID毎に構成することができます。これによって、管理者はユーザグループをベースに、複数のSSIDを構成設定できます。そのユーザグループは、ゲストや従業員、または音声やビデオなどのトラフィック タイプによってそれぞれ、認証オプションやポリシーを適用することができます。FortiOSの認証オプションは、複数の異なるセキュリティ モードをサポートしています。次のリストで、これらの機能や関連した利点のいつくかを説明します。

認証方式	利点
デバイスMACブラックリスト/ホワイトリスト	MACアドレスベース認証によりデバイス毎の制御が可能
Open / WEP64 / WEP128	ゲスト アクセスまたはホットスポットに対してダイレクトなインターネット ルーティングを許可
ゲストのCaptive Portal	SSIDに基づいてログイン画面をカスタマイズ
WPA /WPA2 802.11i PSK (Pre-shared key:事前共有鍵)	事前共有鍵によるパスワード共有
WPA/WPA2 802.11i Enterprise (RADIUSバックエンドを搭載した802.1X)	個々に監視されたセキュアな証明書による堅牢なセキュリティ
暗号（TKIPおよびAES）	最高レベルの暗号プロテクション

認証 –ブラックリスト/ホワイトリスト

FortiOS では、スマートフォンやタブレットなどのデバイスを明示的にホワイトリスト、またはブラックリストへ登録できます。これによって、さらなる認証が必要なくなり、アクセスを高速化されます。MACアドレスを使って、セキュリティ プロビジョニングのためのローカル認証データベースを構築することができます。リスト上に指定されていないユーザに対してのみ、通常の認証シーケンス（例えば、Captive PortalやWPA2）が実行されます。この機能は、CLI（Command Line Interface）を介して利用可能になります。

Open / WEP64 / WEP128

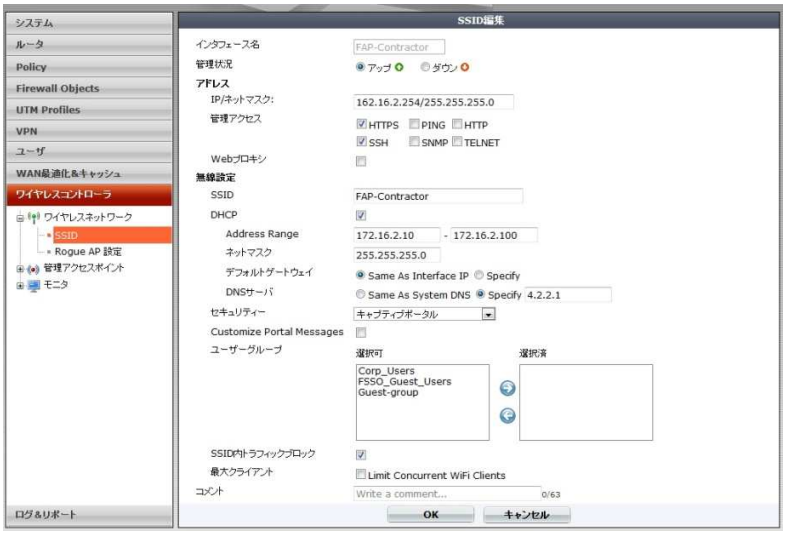
FortiOS は、Open／WEP64／WEP128をサポートしています。しかし、Openオプションは、トラフィックがダイレクトのインターネット ルーティングを必要としているホットスポットやゲストアクセスポイントで主に使用されます。このオプションは認証または暗号を含んでいません。それゆえ、ファイアウォールポリシーは、無線インタフェースおよびWANインタフェース間のトラフィックを許可するだけで、その他すべてのトラフィックはブロックされます。高度なセキュリティが大きな問題になっていない場合や、クライアントがSSLまたはIPSec VPNを使用している場合でのみOpen設定は使用されます。

ゲストのCaptive Portal

ブラウザを起動したら、全てのWebサイトアドレスはFortiGate無線LANコントローラによって一旦受け取られます。Captive Portal認証は、特定の無線SSIDインタフェースに対してIDベースのポリシーを呼び出すことで、有効になります。Captive Portalユーザは、外部またはローカル データベースに対する認証が可能になります。
FortiOS では、複数のCaptive Portalメッセージを SSIDに基づいてカスタマイズされたログイン画面により表示します。これらのSSID設定などの無線設定は効率的に管理されます。

- IP アドレス設定
- DHCP / DNS
- Captive Portal
- ユーザ グループ

ゲストCaptive Portalは、FortiTokenのワンタイム パスワード（OTP）ソリューションを使用することで、二要素認証方式をサポートします。



WPA /WPA2 802.11i PSK(Pre-shared key：(事前共有鍵)

WPA (WiFi Protect Access)は下位互換で利用できますが、すべてのユーザはセキュアなデータ暗号を強化するためにWPA2に移行する必要があります。WAP事前共有鍵によって、すべての無線LANユーザ間でパスワードを共有できます。このタイプのセキュリティはゲストまたはホームアクセスで有益です。しかしながら、企業は、RADIUSによるWPA2を使用してユニークなユーザ名とパスワードの組み合わせを従業員や契約社員に提供することが必要になります。

WPA/WPA2 802.11i Enterprise (RADIUSバックエンドによる802.1X)

このモードでは、ユーザ名およびパスワード情報がユーザから求められ、802.1X認証を使用してバックエンドのRADIUSサーバに対して認証が行われます。これは無線の導入において、最もセキュアな認証方式です。
FortiOSはまた、WPA-Enterprise認証に対して組み込まれたパブリック認証をサポートしています。

暗号（TKIPおよびAES）

802.11i 標準では、TKIP に加えて AES（Advanced Encryption Standard）を指定します。AES はより高度なセキュリティを可能にし、政府機関や大規模な企業での導入に適しています。企業や組織が従来の無線機器をリプレースする場合、AES は WLAN セキュリティにとって一般的に認知された暗号標準になっています。FortiOS は、TKIP および AES 暗号方式の両方に加えて、802.11i/WPA2 で指定された他の規格をサポートしています。

DARRP (Distributed Automatic Radio Resource Provisioning)：自動チャネル プロビジョニング

FortiAPユニットに対して、各デバイスは最適な通信チャネルを自動的かつ周期的に判断します。DARRP機能によって、FortiAPユニットは自動チャネル選択を可能にしています。これによって、大規模な導入ネットワークにおいてアクセスポイント相互のチャネル干渉を防止しています。
DARRP機能は、次のように動作します。

- 各FortiAPユニットは利用できるチャネルを個々にスキャンします。インタフェースおよびチャネルの利用状況を測定し、頻度が最も少ないチャネルを選択し、それから通信利用率が最も低いチャネルを選択します。
- FortiAPユニットは、インタフェースおよびチャネルの利用状況が変更になったかどうかを判断するためにバックグラウンドでこのスキャンを周期的に実行します。
- 何らかの状況が変更になった場合、FortiAPユニットはすべてのクライアントに対して新しく選択されたチャネルに移行するように信号を送ります。

ログメッセージは、チャネルがFortiAPユニットによって変更された時点を確認するために記録されます。加えて、デバッグログもまた、すべての稼動においてDARRPアルゴリズムの判断を反映するために記録されます。複数のチャネルがWebベースのマネージャで選択されている場合、デフォルトでARRPアルゴリズムは自動的に[ON]になります。1つのチャネルが選択された場合は、ARRPアルゴリズムは無効になります。

イントラSSIDプライバシー

複数のユーザがホットスポットで*Guest* SSIDなどの同じSSIDを共有している場合には、各ユーザの通信プライバシーが保証される必要があります。1つのSSID内でトラフィック セグメンテーションを有効にすることで、FortiOSはイントラ内のSSIDプライバシーを提供します。これは同じネットワークを共有している他のクライアントからの潜在的な攻撃から他のクライアントを保護します。

不正アクセスポイント検知/抑制およびオンワイヤの相関付け

不正アクセスポイントは、悪意のあるユーザによってクレジットカード情報などの機密データを盗み取ることを可能にする漏洩ポイントとなるため、社内ネットワークに脅威を与えると言えます。この理由によって、PCI-DSSコンプライアンスでは、不正アクセスポイントに対する積極的なモニタリングを要求し、もし発見された場合、不正アクセスポイントを抑制することを要求しています。FortiGate不正アクセスポイントコントロールエンジンはこのプロセスを自動化することで、無線LANシステム管理者が継続的に未知のAPを監視できるようにし、さらに、不正アクセスポイントがFortiAPネットワーク上にないか、または近接APにないかを判断することを可能にしています。次のリストで、これらの機能や関連した利点を説明します。

不正アクセスポイント制御方式	利点
監視	潜在的な不正アクセスポイントのMACアドレスを収集
オンワイヤ検知	有線・無線ネットワーク間のトラフィックをモニタリングし、不正アクセスポイントを特定
抑制	不正アクセスポイントへの接続を認証解除することで、脅威を排除

監視

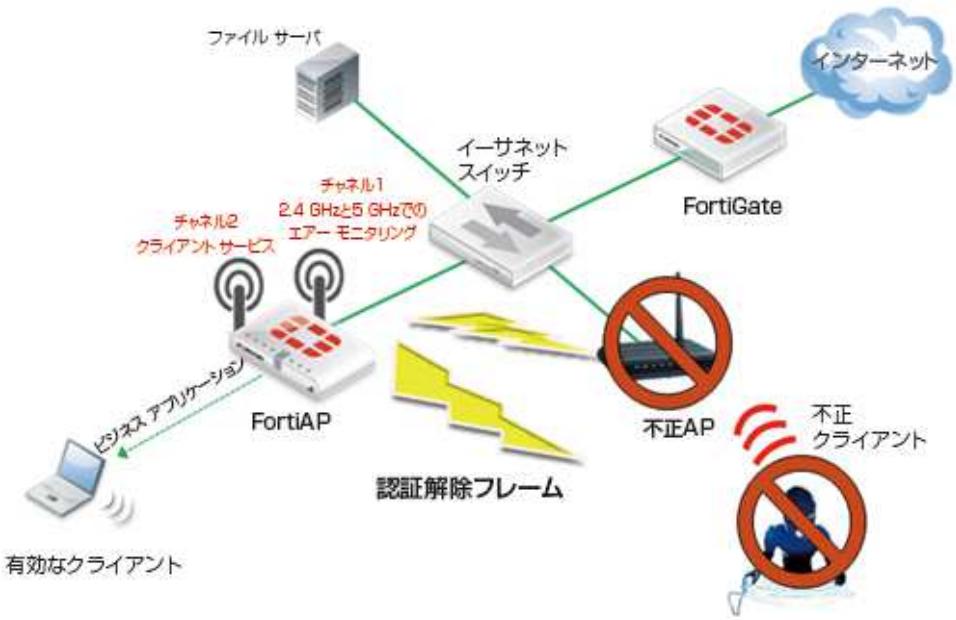
監視フェーズ中は、クライアントとアクセスポイント間、クライアントとクライアント間の通信はモニタリングされ、インフラおよびアドホック無線アクセスポイントの両方を検知します。検知した未知のアクセスポイントのMACアドレスは、潜在的に不正アクセスポイントが存在している可能性があるため、さらに分析するためにコントローラに送信されます。

オンワイヤ検知および相関付け

“オンワイヤ”機能は、迅速な検知を助けるだけではなく、不正アクセスポイントが何らかのテクノロジを使用して実際ネットワークに接続していることをITスタッフに警告することの支援を目的としています。FortiGateおよびFortiAPは連携して稼動することで、フォーティネット デバイスが接続される各VLAN上のネットワーク接続デバイスのMACアドレスを収集します。加えて、FortiAPはクライアントおよびアクセスポイントから無線MACアドレス を収集し、その情報をFortiGateユニットに送信します。収集した無線および有線のMACアドレスを比較します。有線LANおよび無線LAN上に共通のMACアドレスが存在する場合は、クライアントは不正アクセスポイントを通して通信していることを示唆しています。“オンワイヤ”イベントは高優先度のSYSLOGメッセージを生成し、不正アクセスポイントの移行または排除の措置を促す警告をITスタッフに発します。検知したアクセスポイントのMACアドレスを有線MACアドレスと関連付け、これらのMACアドレスが互いに近接しているかどうかを検出します。また、これは、NATモードのアクセスポイントは無線LAN上に存在する可能性があることを示唆します。さらに、こうしたイベントは調査プロセスでITを支援するためにフラグ付けされて注意を喚起します。

抑制

認証解除フレームをクライアント（ステーション）および不正アクセスポイント（サーバ）の両方に送信することで、不正アクセスポイントを抑制し、有益なデータが転送されないように通信を遮断することが可能になります。これによって、機密デ―タの漏洩リスクが低減されます。またー方で、ITが社内ネットワークから好ましくない不正アクセスポイントの抑制を実行することができます。



音声モビリティのための高速なローミングとサポート

音声や動画などの延滞に影響を受けるトラフィックが1つのアクセスポイントから別のアクセスポイントにローミングされる時点で認証が遅れると、QoSに大きな問題をもたらすことになります。PMK（Pairwise Master Key）キャッシングおよび事前認証に基づいた標準ベースの認証キャッシングテクノロジを使用して高速なローミングを組み込むことで、フォーティネットはこの問題に対処してきました。PMKキャッシングは、クライアントがアクセスポイントとアソシエーションを確立することを可能にします。そして、完全なRADIUS認証を実行した時点で、FortiGate無線LANコントローラはその特定のアクセスポイントとネゴシエーションしたマスターキーをキャッシュに格納します。ユーザがそのアクセスポイントから元のアクセスポイントへ再ローミングする場合、クライアントは再認証を必要と

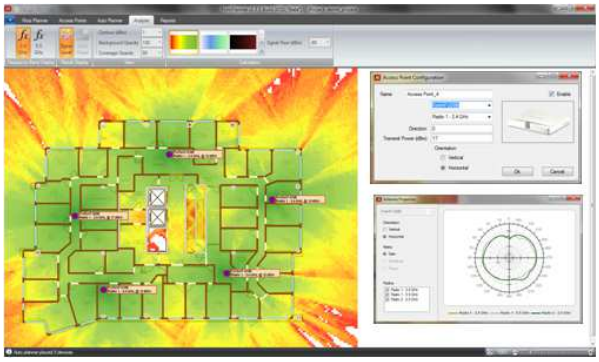
しません。その機能は、事前認証をサポートしている無線クライアントが、接続遅延または接続切れを起こすことなく無線通信を続行することを保証します。

アクセスポイントのスケーラビリティ

FortiGateのモデルによって、1台から何百台ものFortiAPアクセスポイントをネットワークで管理することができます。適切なモデルを選択することで、無線LANの導入を容易にサイジングすることが可能になり、初期投資を削減すると同時に、運用コストを削減します。最新のスケーラビリティ マトリックスに関しては、http://docs.fortinet.comに掲載されたFortiGate Maximum Values Matrixを参照してください。

無線の通信範囲とカバレージの把握

多くの無線アクセスポイントベンダは最高の出力を要求し、出力が強さと通信範囲の広さに関係すると主張しています。しかしながら、これは無線通信がFMラジオの電波塔のように一方向のブロードキャスティングの場合にのみ当てはまります。無線トラフィックは双方向なため、無線の通信範囲はクライアントおよびアクセスポイント両方の性能によって決まります。無線対応のデバイスのほとんどはバッテリー電源であり（例えば、ラップトップやその他のモバイルデバイス）、こうしたデバイスの送信出力を制限することは、バッテリー寿命を高めるとともに、デバイスの大きさを小さくすることにつながります。したがって、クライアントデバイスは双方向の無線通信の到達範囲を決める最も弱いリンクとなります。これは携帯電話で5本バーが立っているのに、電話が繋がらないことを思い出してください。今までに自分の携帯電話でこんなことが起こり、どうしてだろうと不思議に思ったことがあるでしょう。自分の携帯電話は出力の強い基地局から電波を受けることができますが、基地局の範囲に到達するのに携帯電話の出力が不十分であるために基地局に返信できない場合にこの問題が発生します。無線ネットワークは、同じような制限を受けており、最も弱いリンクであることを念頭におくべきです。



FortiAPは、通常、17dBmまたは50mWの出力を提供しています。これによって、無線ネットワーク上でクライアントとの双方向通信リンクを確立するのに必要な出力レベルを満たすか超えるように最適化されています。通常の無線の範囲は、電波障害源や電波妨害源に依存します。最適な出力レベルの把握というニーズに取り組むためにFortiAP用にFortiPlannerアクセスポイントプランニングツールを開発しました。
FortiPlannerは、ビル内に必要なFortiAPの数を計算し、FortiAP設置フロアプランを提供します。

以下のサイトからFortiPlannerの無償版をダウンロードすることができます。
www.fortinet.com/wirelessの[Resources]

備考：FortiPlannerは無償ツールのため、サポート対象外となります。

付録 A

FortiAP-220B機能一覧

無線標準への対応および機能	FortiAP-220B
シンアクセスポイント	✔
Wi-Fiチャネルの数	2
802.11a	✔
802.11b	✔
802.11eおよびWMEマルチメディア拡張	✔
802.11g	✔
802.11h	✔
802.11i (TKIP/AES)	✔
802.11j	✔
802.11n (2x2 MIMO)	✔
802.1X	✔
Power Over Ethernet (PoE)	✔ 802.3af
ハイスループット40Mhzオプション	✔
Short Guard インターバル	✔
最大無線アソシエーション／合計	600 Mbps
チャネルあたりのSSIDの数（チャネルあたり1つは予備SSID）	16
同時クライアント アクセスおよびバックグラウンド スキャン	2.4GHz & 5GHz
同時クライアント アクセスおよびフルタイムの不正アクセスポイント検知	✔
“オンワイヤ”不正アクセスポイント相関および抑制	✔
高速ローミング	✔

付録B

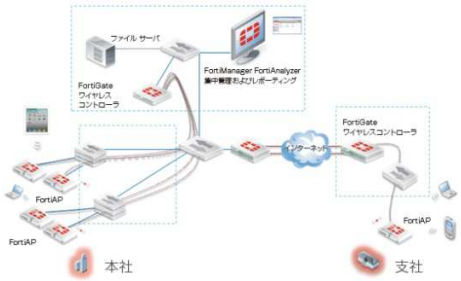
フォーティネットの無線LANソリューション

<table>
<tr>
<td>  </td>
<td>フォーティネットの提供するビジネス規模の無線LANソリューションについて

IEEE 802.11nは、広く採用されるようになってきています。その中でも、モバイルデバイスやアプリケーションは着実に普及してきています。それに伴い、無線環境の導入は複雑になりつつあり、すべての無線ユーザやアプリケーションを同じように扱うにはもはや十分でありません。このような解決方法として、WLANコントロールポリシーを導入し強化する必要性に迫られています。フォーティネットは今日のIT業界においてビジネス規模の無線LANソリューションを提供しており、こうした無数の課題に取り組んでいます。
-ビジネス アプリケーションを特定し、アクセスを制御
-完全なUTMポリシーを有線データおよび無線データの両方に適用
-無線環境の平等な活用を強化し、生産性の向上を実現
- IDベースのポリシー管理により複雑性を排除
-一元管理によってシンプルな運用を可能に
-低いTCOと同時に導入から運用までの柔軟性を実現</td>
</tr>
<tr>
<td>シンプルさ- 無線ネットワークはシンプルに管理できることがに求められます。そのために、有線と無線を1つのネットワーク エレメントとして容易に統合管理される方法が不可欠です。

セキュリティ- 徹底したセキュリティは、マルチメディアの共有や不正無線LANの潜在リスクを考えると、無線LANネットワークにおいては最重要課題です。

スケーラビリティ- ソリューションは、経済的に妥当なコストで適切なレベルの価格／パフォーマンスを提供する必要があります。フォーティネットはアクセスポイントの集中型および分散型の導入をサポートしています。さらに、フォーティネットは、UTMを強化し、無線LANコントローラとして機能させることで、大規模な展開を可能にしています。</td>
<td> 
</td>
</tr>
</table>

<table>
<tr>
<td> 
</td>
<td>集中コントロールでシンプルな導入
フォーティネットはアクセスポイントの集中型および分散型の導入をサポートしています。全てのFortiAPおよびSSIDは、グローバルに制御されるプロファイルとともに、それぞれが独立したインタフェースを形成します。

最高のROIを達成した、有線および無線の統合セキュリティ
無線LANコントローラはすべて有線ネットワークおよび無線ネットワーク間でUTMポリシーを適用しています。レイヤ7アプリケーションレベルでのアプリケーションの優先順位付けと制御とともに、セキュアかつ統合されたコンソールを実現します。
最も少ないTCOを実現したスケーラブルなアーキテクチャ
ニーズが増えるにつれてネットワークを拡大させることができます。機器を総入れ替えすることなく、既存の投資を有効活用できます。</td>
</tr>
<tr>
<td>アクセスポイント／コントローラの広範な選択
製品と専用無線LANコントローラなど、機能が分離したエレメントを管理するには、いくつかのハードルが伴います。フォーティネットのFortiGateは、無線LANコントローラが標準搭載されており容易に無線LAN導入や運用を可能にします。豊富なラインナップの中から最適なモデルを選択頂き、十分なネットワーク 範囲を保証するほか、不正アクセスポイントエレメントの動きを監視したり、容易な管理・運用を提供することができます。</td>
<td>  </td>
</tr>
</table>

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-18-18
住友不動産六本木通ビル 8 階
TEL:03-6434-8531/8533
www.fortinet.co.jp

お問い合わせ