Cisco Aironet ワイヤレス セキュリティに関する FAQ [英語]

目次

概要

このドキュメントでは、Cisco Aironet ワイヤレス セキュリティに関して最もよく寄せられる質問（FAQ）について説明します。

一般的な FAQ

Q. ワイヤレスセキュリティのための必要とは何か。

A. 有線ネットワークでは、データは端デバイスを接続するケーブルに残ります。 しかし無線ネットワークは外気に RF 場合のブロードキャストによってデータを送受信します。 ブロードキャスト性質が理由で WLAN 使用、アクセスできたりまたはデータを破損する侵入者またはハッカーのより大きい脅威があります。 この問題を軽減するために、すべての WLAN は付加をの必要とします:

1. ネットワーク リソースに不正アクセスを防ぐユーザ認証。
2. 送信されたデータ（別名暗号化）の統合およびプライバシーを保護するデータ 機密性。

Q. ワイヤレス LAN のための 802.11 規格が定義する異なる認証方式とは何か。

A. 802.11 規格は Wireless LAN クライアントの認証のための 2 つのメカニズムを定義します:

1. オープン認証
2. 共有キー認証

同様に 2 つの他の広く使われたメカニズムがあります:

1. SSID ベースの認証
2. MAC アドレス認証

Q. 開いた認証とは何か。

A. 開いた認証は基本的にヌル認証アルゴリズムです、つまりユーザまたはマシンの確認がないこ

とを意味します。 認証を許可します Access Point （AP）に認証要求を置くデバイスを開いて下さい。 クライアントを AP に関連付けることを許可するように認証使用クリアテキスト伝達を開いて下さい。 no encryption が有効に なる場合、WLAN の SSID を知っているどのデバイスでもネットワークにアクセス権を得ることができます。 Wired Equivalent Privacy（WEP）が AP で有効に なる場合、WEPキーはアクセスコントロールの方法になります。 正しい WEPキーを備えていないデバイスは AP によって認証が正常でもデータを送信できません。 どちらも AP が送信 するそのようなデバイス 復号化 データできません。

Q. クライアントが AP と関連付けることができるようにどんなステップが開いた認証含みますか。

1. クライアントは AP にプローブ 要求を送信 します。
2. AP はプローブ応答を返します。
3. クライアントは AP 応答を評価し、推奨 AP を選択します。
4. クライアントは AP に認証要求を送ります。
5. AP は認証を確認し、クライアントを登録します。
6. クライアントは AP にそれから Association 要求を送信 します。
7. AP はアソシエーションを確認し、クライアントを登録します。

Q. open 認証の利点と欠点とは何か。

A. open 認証の利点と欠点はここにあります:

長所: 開いた認証は複雑な認証アルゴリズムをサポートしないワイヤレス デバイスによって使用できる基本認証メカニズムです。 802.11 仕様の認証は接続指向です。 意図的に認証のための必要条件はデバイスがネットワークに迅速 アクセスを得るようにします。 このような場合、開いた認証を使用できます。

欠点: 開いた認証はクライアントが有効なクライアントでハッカー クライアントではないかどうか確認する方法を提供しません。 開いた認証と WEP暗号化を使用しない場合、WLAN の SSID を知っているどのユーザでもネットワークにアクセスできます。

Q. 共有鍵認証とは何か。

A. 共有鍵認証は類似した 1 つの主な違いを用いる認証を開くためにはたらきます。 WEP暗号化キーと開いた認証を使用するときデータを暗号化し、復号化するのに、WEPキーが使用されていますが認証ステップで使用されません。 共有鍵認証では、WEP暗号化は認証のために使用されます。 開いた認証のように、共有鍵認証はクライアントおよび AP は同じ WEPキーがあるように要求します。 共有鍵認証を使用する AP はクライアントにチャレンジ テキスト パケットを送ります。 クライアントはユーザ確認のためのテキストを暗号化し、それに続く認証要求と答えるのにローカルで設定された WEPキーを使用します。 AP が認証要求を復号化し、オリジナル ユーザ確認のためのテキストを取得できる場合 AP は認証応答とクライアントへのその対し応答します。

Q. 共有鍵認証はどんなステップをクライアントが AP と関連付けることができるように含みますか。

1. クライアントは AP にプローブ 要求を送信 します。
2. AP はプローブ応答を返します。
3. クライアントは AP 応答を評価し、推奨 AP を選択します。

4. クライアントは AP に認証要求を送ります。
5. AP は非暗号化ユーザ確認のためのテキストが含まれている認証応答を返します。
6. クライアントは WEPキーが付いているユーザ確認のためのテキストを暗号化し、AP にテキストを送ります。
7. AP は暗号化されたユーザ確認のためのテキストと非暗号化ユーザ確認のためのテキストを比較します。 認証がオリジナル ユーザ確認のためのテキストを復号化し、取得できる場合認証は正常です。

共有鍵認証はクライアント提携プロセスの間に WEP暗号化を使用します。

Q. 共有鍵認証の利点と欠点とは何か。

A. 共有鍵認証では、クライアントおよび AP はユーザ確認のためのテキスト (クリアテキスト) および暗号化されたチャレンジを交換します。 従って、認証のこの型はマン イン ザ ミドル不正侵入に脆弱です。 ハッカーは非暗号化チャレンジおよび暗号化されたチャレンジを受信できこの情報から WEPキー (共有鍵) を得ます。 ハッカーが WEPキーを知っているとき、全認証機構は妥協され、ハッカーは WLANネットワークにアクセスできます。 これは共有鍵認証を用いる主要な短所です。

Q. MAC アドレス認証とは何か。

A. 802.11 規格が MAC アドレス認証を規定 しないが、WLANネットワークは一般にこの認証手法を使用します。 それ故に、ワイヤレス デバイス ベンダーのほとんどは、Cisco を含んで、MAC アドレス認証をサポートします。

MAC アドレス認証では、クライアントはクライアントの MAC アドレスが AP または外部認証サーバで MAC アドレスのリストに対してローカルで保存した確認される MAC アドレスに基づいて認証されます。 MAC 認証は開いたより強い 802.11 が提供するセキュリティ機構および共有鍵認証です。 それ以上のこの認証方式はネットワークにアクセスできる不正 な デバイスの確率を下げます。

Q. MAC 認証が Cisco IOS ソフトウェア リリース 12.3(8)JA2 の Wi-Fi プロテクテッド アクセス (WPA) を使用しない理由

A. MAC 認証のための唯一のセキュリティ レベルは許可された MAC アドレスのリストに対してクライアントの MAC アドレスをチェックすることです。 これは非常に弱い考慮されます。 以前の Cisco IOS ソフトウェア リリースでは、MAC 情報を暗号化するために認証および WPA を設定する可能性があります。 しかし WPA 自体にチェックする MAC アドレスがあるので、Cisco はセキュリティ機能しか改良しないこの種の設定を新しい Cisco IOS ソフトウェア リリースのおよびことにされた可能にしないことにしました。

Q. 方式としてワイヤレス デバイスを認証するのに SSID を使用できますか。

A. サービス セット ID (SSID) は WLAN がネットワーク名として使用するユニークな、大文字/小文字の区別がある、英数字値です。 SSID は a -ワイヤレス LAN の論理的な分離を可能にするメカニズムです。 SSID はデータ 機密性 機能を提供しません、SSID 認証するは AP にクライアント実際に。 SSID 値はフレームのビーコン、プローブ 要求、プローブ応答および他のタイプのクリアテキストとしてブロードキャストです。 立ち聞きする人は Sniffer Pro 容易に 802.11 Wireless LAN パケット アナライザの使用の SSID を、たとえば判別、できます。 Cisco は WLANネットワークを保護するのに方式として SSID を使用することを推奨しません。

Q. SSID ブロードキャストを無効に する場合、WLANネットワークのまたセキュリティを実現できますか。

A. SSID ブロードキャストを無効に するとき、SSID はビーコン メッセージで送信 されません。 ただし、他の帯にのような、プローブ 要求およびプローブ応答にまだクリアテキストで SSID があります。 従って SSID を無効に する場合拡張 な ワイヤレスセキュリティを実現しません。 SSID はセキュリティ機構として使用のために設計されていませんでしたり、意図されていません。 さらに、SSID ブロードキャストを無効に すれば、混合クライアント配備のための Wi-Fi 相互運用性における問題に直面できます。 従って、Cisco はセキュリティのモードとして SSID を使用することを推奨しません。

Q. 802.11 セキュリティで発見される脆弱性とは何か。

A. 802.11 セキュリティの主要な脆弱性は次の通り要約することができます:

- 弱いデバイス専用認証: クライアントデバイスは、ないユーザ認証されます。
- 弱いデータ暗号化: Wired Equivalent Privacy（WEP）はずっとデータを暗号化する方法として証明された非効果的です。
- メッセージの整合性無し: Integrity Check Value （ICV）はずっとメッセージの整合性を確認する方法として証明された非効果的です。

Q. WLAN の 802.1X 認証のロールとは何か。

A. 802.11 規格が定義するオリジナル認証方式の欠点およびセキュリティーの脆弱性に対処するために、802.1X 認証フレームワークは 802.11 MAC 層セキュリティ拡張のためのドラフトに含まれています。 IEEE 802.11 タスクグループは I（TGi）現在これらの機能拡張を開発しています。 802.1X フレームワークは普通より高い層でだけ見られる拡張可能な認証をリンク層に、与えます。

Q. 802.1X フレームワークが定義する 3 つのエンティティとは何か。

A. 802.1X フレームワークはこの 3 つの論理構成体が WLANネットワークのデバイスを検証するように要求します。

1. **サプリカント**—サプリカントは Wireless LAN クライアントに常駐し、別名 EAP クライアントです。
2. **オーセンティケータ**—オーセンティケータは AP に常駐します。
3. **認証サーバ**—認証サーバは RADIUSサーバに常駐します。

Q. 802.1X 認証フレームワークを使用すると無線クライアント認証が行われる仕組み

A. 無線クライアント（EAP クライアント）がアクティブになるとき、無線クライアントは開いたか共用認証と認証を受けます。 802.1X は AP にクライアントの後で開いた認証を使用し、正常に関連付けます開始します。 クライアント ステーションは関連付けることができましたり正常な 802.1X 認証の後やっとデータトラフィックを通過できます。 802.1X 認証のステップはここにあります:

1. 802.1X のために設定される AP （オーセンティケータ）はクライアントからのユーザの識別を要求します。
2. クライアントは規定された時間以内のアイデンティティで応答します。
3. サーバはユーザの識別がデータベースにある場合ユーザの識別をチェックし、クライアントから認証を始めます。
4. サーバは AP に成功 メッセージを送信 します。
5. クライアントが認証されれば、サーバは/クライアントに出入して送信 される 復号化 トラフィック暗号化するのに使用されている AP に暗号化キーを転送します。
6. ステップ 4 では、ユーザの識別がデータベースになければ、サーバは認証を廃棄し、AP に失敗メッセージを送ります。
7. AP はクライアントにこのメッセージを転送し、クライアントは正しい資格情報と再度認証を受ける必要があります。

注: 802.1X 認証全体、AP はクライアントに出入してちょうど認証メッセージを転送します。

Q. 802.1X 認証フレームワークと使用できる異なる EAP バリアントとは何か。

A. 802.1X はクライアントを認証するためにプロシージャを定義します。 802.1X フレームワークで使用される EAP 型は 802.1X 交換で使用される信用証明書の種別および認証方式を定義します。 802.1X フレームワークはのこれらの EAP バリアント使用できます:

- EAP-TLS — Extensible Authentication Protocol（EAP） Transport Layer Security
- EAP-FAST —保護されたトンネルによる EAP 適用範囲が広い認証
- EAP-SIM — EAP SIM カード
- Cisco LEAP — Lightweight Extensible Authentication Protocol
- EAP-PEAP — Extensible Authentication Protocol（EAP）保護される EAP
- EAP-MD5 — EAP メッセージ ダイジェスト アルゴリズム 5
- EAP-OTP — EAP オン・タイム パスワード
- EAP-TTLS — EAP によってトンネル伝送される Transport Layer Security

Q. 利用可能な異なるバリアントから 802.1X EAP 方式を選択する方法

A. 考慮する必要がある重要な要因は EAP 方式がと互換性がある既存のネットワークかどうかです。 さらに、Cisco は相互認証をサポートする方式を選択することを推奨します。

Q. 何がローカル EAP 認証ありますか。

A. ローカル EAP は WLC が認証サーバとして機能するメカニズムです。 ユーザーの資格情報はリモートオフィスのバックエンド プロセスとして機能する WLC でサーバがダウン状態になるとき無線クライアントを認証するためにローカルで保存されます。 ユーザーの資格情報は WLC のローカル データベースまたは外部 LDAP サーバから取得することができます。 LEAP、EAP-TLS EAP-FAST、PEAPv0/MSCHAPv2 および PEAPv1/GTC はローカル EAP によってサポートされる異なる EAP 認証です。

Q. Cisco LEAP とは何か。

A. Lightweight Extensible Authentication Protocol（LEAP）は Cisco 独自の認証方式です。 Cisco LEAP はワイヤレス LAN（WLAN）に対する 802.1X 認証種別です。 Cisco LEAP は共用シークレットとしてログオン パスワードによってクライアントと RADIUSサーバ間の強い相互認証をサポートします。 Cisco LEAP はダイナミック ユーザごとの、セッションごとの暗号化キーを提供します。 LEAP は 802.1X を展開する最少複雑な方式で RADIUSサーバだけ必要とします。
LEAP の情報に関しては Cisco LEAP を参照して下さい。

Q. EAP-FAST はたらく仕組み

A. トンネル伝送された認証プロセスを実現させる EAP-FAST な使用対称鍵 アルゴリズム。 トンネル確立は EAP-FAST 動的に提供され、認証、許可、アカウンティング（AAA） サーバによって EAP-FAST によって管理することができる保護されたアクセス資格情報（PAC）に頼ります（Cisco Secure Access Control Server [3.2.3） ACS]のような v。 辞書不正侵入からの相互に認証されたトンネル、EAP-FAST なオファー保護およびマン イン ザ ミドル脆弱性を使って。
EAP-FAST のフェーズはここにあります:

EAP-FAST だけでなく、受動辞書不正侵入およびマン イン ザ ミドル不正侵入からの危険性を軽減しましたり、しかしまた現在展開されたインフラストラクチャに基づいてセキュア認証を有効に します。

- **フェーズ 1**： 互いを認証し、セキュアトンネルを確立するために tunnel —相互に認証されたクライアントおよび AAAサーバ 使用 PAC を確立して下さい。
- **フェーズ 2**： 確立された tunnel —クライアントでクライアント認証をクライアント許可 ポリシーを認証し、確立するために送信しますユーザネームおよびパスワードを行って下さい。
- 任意で、フェーズ 0 — EAP-FAST な認証はまれに動的に PAC と提供されるべきクライアントを有効に するのにこのフェーズを使用します。 このフェーズはユーザとネットワークの間でユーザごとのアクセス資格情報を安全に生成します。 認証のフェーズ 1 は PAC として知られているこのユーザごとの資格情報を使用します。

詳細については EAP-FAST な Cisco を参照して下さい。

Q. Cisco WLAN ネットワークの EAP を設定する方法を説明する cisco.com に文書がありますか。

A. WLANネットワークの EAP 認証を設定する方法の情報に関しては RADIUSサーバとの EAP 認証を参照して下さい。

PEAP 認証を設定する方法の情報に関しては保護された EAP アプリケーションノートを参照して下さい。

LEAP 認証を設定する方法の情報に関してはローカル RADIUSサーバとの LEAP 認証を参照して下さい。

Q. 無線ネットワークで最も広く使われた異なる暗号化メカニズムとは何か。

A. 無線ネットワークで使用される最も広く使われた暗号化方式はここにあります:

- WEP
- TKIP

- AES

AES は WEP および TKIP 暗号化がファームウェアで処理される一方、ハードウェア暗号化方式です。 ファームウェア アップグレード WEP を使うとデバイスは TKIP をサポートできます従って相互運用可能です。 AES は WEP が最も少なくセキュアである一方、セキュアおよび最も高速な方法です。

Q. WEP暗号化とは何か。

A. WEP は、Wired Equivalent Privacy の略です。 WEP は、WLAN デバイス間で送信されるデータ信号の暗号化および復号化に使用されます。 WEP は IEEE 802.11 のオプション機能で、転送中のパケットの暴露や改ざんを防止し、ネットワーク使用のアクセス コントロールを行います。 WEP によって、WLAN リンクは有線リンクと同程度の安全性になります。 規格が規定 すると同時に、WEP は 40 ビットまたは 104 ビット キーによって RC4 アルゴリズムを使用します。 RC4 ではデータの暗号化と復号化に同一のキーを使用するため、RC4 は対称アルゴリズムです。 WEP をイネーブルにすると、各無線「ステーション」にはキーが配備されます。 このキーは、電波を介してデータを送信する前に、データをスクランブルするために使用されます。 あるステーションが適切なキーでスクランブルされていないパケットを受信すると、そのステーションはそのパケットを廃棄します。このようなパケットはホストに配信されません。

WEP を設定する方法の情報に関しては Wired Equivalent Privacy（WEP）の設定を参照して下さい。

Q. ブロードキャスト キー ローテーションとは何か。 ブロードキャスト キー ローテーションの周波数とは何か。

A. ブロードキャスト キー回転は AP が最良ランダム Group 鍵を生成するようにします。 キー ローテーションを定期的にアップデートしますキー管理が可能なすべてのクライアントをブロードキャストして下さい。 ブロードキャスト WEPキー ローテーションを有効に するとき、AP はダイナミック ブロードキャスト WEPキーを提供し、間隔でキーをセット変更します。 ブロードキャスト キー ローテーションは TKIP へ Wireless LAN が Cisco クライアントデバイスのための最新版ファームウェアにアップグレードできないデバイスかシスコ以外のワイヤレス クライアントデバイスをサポートする場合優秀な代替です。 ブロードキャスト キー ローテーション機能を設定する方法の情報に関してはブロードキャスト キー ローテーションの有効に することおよび無効にを参照して下さい。

Q. TKIP とは何か。

A. TKIP は Temporal Key Integrity Protocol（TKIP）を意味します。 TKIP は WEP暗号化の欠点を当たるために導入されました。 TKIP は別名 WEPキー ハッシングで、最初に WEP2 と呼ばれました。 WEP キー再利用問題を解決する TKIP は一時ソリューションです。 TKIP は WEP と同じである暗号化を行うのに RC4 アルゴリズムを使用します。 WEP からの主な違いは TKIP が一時的なキーを各パケット変更することです。 各パケットのハッシュ値が変更するので一時的なキーの変更各パケット。

Q. TKIP を WEP暗号化を使用するデバイスによって相互運用するために使用しなさいデバイスはできますか。

A. TKIP の長所は WEP ベースの AP および無線の存在の WLAN が簡単なファームウェア パッチを通って TKIP にアップグレードできることです。 また、WEP だけ機器はまだ WEP を使用する TKIP 有効に された デバイスによって相互運用します。

Q. Message Integrity Check（MIC）とは何か。

A. MIC は WEP暗号化の脆弱性に対処する更に別の機能拡張です。 MIC はビットフリップします暗号化されたパケットの不正侵入を防ぎます。 ビットフリップ攻撃不正侵入の間に、侵入者は暗号化されたメッセージを代行受信し、メッセージを変え、次に変えられたメッセージを再送信します。 レシーバはメッセージが破損し、ない正当 な 1 であることを知りません。 この問題に対処するために、MIC 機能はワイヤレス フレームに MIC フィールドを追加します。 MIC フィールドは ICV と同じ数学欠点に脆弱ではないフレーム整合性チェックを提供します。 MIC はまたワイヤレス フレームに Sequence Number フィールドを追加します。 AP は帯によって受け取った順番が異なる廃棄します。

Q. WPA とは何か。 WPA どのように 2 は WPA とであるか。

A. WPA はネイティブ WLAN の脆弱性に対処する Wi-Fi 同盟からの標準ベース セキュリティソリューションです。 WPA は WLANシステムに拡張 な データ 保護およびアクセスコントロールを提供します。 WPA はオリジナル IEEE 802.11 セキュリティインプリメンテーションのすべての既知 Wired Equivalent Privacy（WEP）脆弱性に対処し、エンタープライズおよび small office，home office（SOHO）両方環境の WLANネットワークに即時セキュリティソリューションを持って来ます。

WPA2 は次世代の Wi-Fi セキュリティ機能です。 WPA2 は批准された IEEE 802.11i 規格の Wi-Fi 同盟相互運用可能な実装です。 WPA2 は国立標準技術研究所（NIST）を- Cipher Block Chaining Message Authentication Code プロトコル（CCMP）のカウンター モードの使用の推奨される高度暗号化規格（AES）暗号化アルゴリズム設定します。 AES カウンター モードは 128 ビット暗号化キーとのデータの 128 ビット ブロックを一度に暗号化するブロック 暗号です。 WPA2 は WPA よりセキュリティの上位レベルを提供します。 WPA2 は各アソシエーションの新しいセッションキーを作成します。 WPA2 がネットワークの各クライアントのために使用する暗号化キーはそのクライアントにユニーク、特定です。 最終的に、各パケットは一意キーを使って送信 された 地上波である暗号化されます。

WPA1 および WPA2 は両方 TKIP または CCMP 暗号化を使用できます。（それはいくつかのアクセス ポイントおよび何人かのクライアントが組み合わせを制限するが、ですこと本当そこに 4 つの考えられる組み合わせです）。 WPA1 と WPA2 の違いはビーコン、アソシエーション帯および 4 方法ハンドシェイク帯に入れられて得る情報要素にあります。 これらの情報要素のデータは基本的には同じですが、使用される識別は異なっています。 キー ハンドシェイクの主な違いは最初のグループ キーを提供するために WPA がこの余分ハンドシェイクをする必要がある一方 WPA2 は 4 方法ハンドシェイク Group 鍵頭文字が含まれている最初の Group 鍵 ハンドシェイクがスキップされることであり。 Group 鍵の鍵変更は同じように起こります。 ハンドシェイクはユーザ データグラムの伝達のための暗号スイートの選択および使用の前に（TKIP か AES）発生します。 WPA1 か WPA2 ハンドシェイクの間に、使用するべき暗号スイートは判別されます。 選択されて、暗号スイートはすべてのユーザトラフィックのために使用されます。 従って AES と WPA1 は WPA2 ではないです。 WPA1 はを（可能にしますが、頻繁に制限されるクライアント側）です TKIP または AES 暗号。

Q. AES とは何か。

A. AES は Advanced Encryption Standard（AES）を意味します。 AES は大いに強化暗号化を提供します。 AES は 128-、192-、および 256 ビット キー サポートとのブロック 暗号、RC4 より大いに強い Rijndael アルゴリズムを使用します。 AES をサポートする WLANデバイスに関してはハードウェアは WEP の代りに AES をサポートする必要があります。

Q. Microsoft Internet Authentication Service（IAS）サーバによってどんな認証方式がサポートされますか。

A. IAS はこれらの認証プロトコルをサポートします:

- Password Authentication Protocol（PAP）
- Shivaパスワード認証プロトコル（SPAP）
- Challenge Handshake Authentication Protocol（CHAP）
- Microsoft Challenge Handshake Authentication Protocol（MS-CHAP）
- Microsoft Challenge Handshake Authentication Protocol バージョン 2（MS-CHAP v2）
- 拡張可能な認証プロトコルメッセージ ダイジェスト 5 CHAP（EAP-MD5 CHAP）
- EAP-Transport Layer Security（EAP-TLS）
- 保護された EAP-MS-CHAP v2（PEAP-MS-CHAP v2）（別名 PEAPv0/EAP-MSCHAPv2）

Windows 2000 サーバサービス パック 4 がインストールされている場合 Windows 2000 サーバ サポート PEAP-MS-CHAP v2 の PEAP-TLS IAS および PEAP-TLS。 詳細については、IAS と併用するための認証方式を参照して下さい 。

Q. VPN はどのようにワイヤレス envrionment で設定されるか。

A. VPN はレイヤ3 セキュリティ機構です; ワイヤレス暗号化メカニズムは層 2. VPN で設定されています 802.1X、EAP、WEP、TKIP および AES に設定されています。 レイヤ2 メカニズムが時、VPN は実装にオーバーヘッドを追加します。 セキュリティが設定されていない公共ホットスポットおよびホテルのような場所では、VPN は設定するべき有用なソリューションです。

FAQ トラブルシューティングおよび設計

Q. あらゆる最良の方法が屋外ワイヤレス LAN のワイヤレスセキュリティを展開するありますか。

A. 屋外ワイヤレス セキュリティ用の最良の方法を参照して下さい。 この資料は屋外ワイヤレス LAN を配置するセキュリティ上の推奨事項で情報を提供したものです。

Q. 使用 RADIUSサーバが無線クライアントを認証することができるように Active Directory と Windows 2000 か 2003 サーバをできますか。

A. アクティブなディレクトリとの Windows 2000 か 2003 サーバは RADIUSサーバとしてはたらくことができます。 この RADIUSサーバを設定する方法の情報に関しては Cisco が Windows サーバ 設定をサポートしないので Microsoft に連絡する必要があります。

Q. サイトは PEAP ネットワークに開いた無線ネットワーク（350 および 1200 シリーズ AP）から移行することを約あります。 開いた SSID （Open 認証のために設定される SSID）および同じ AP の PEAP SSID （PEAP 認証のために設定される SSID）作業が両方あることを同時に望みます。 これは私達に PEAP SSID にクライアントを移行する時間を与えます。 方法が同時に同じ AP の開いた SSID および PEAP SSID をホストするありますか。

A. Cisco AP は VLAN（レイヤ2 だけ）をサポートします。 これは実際にたいと思うものを実現

させるし唯一の方法です。 2 VLAN を必要があります、（ネイティブおよび他の VLAN）作成する。 それから 1 つのための WEPキーおよび別のもののための WEPキーがないことができます。 こうすれば、Open 認証のための VLAN および PEAP 認証のための他の VLAN の 1 つを設定できます。 VLAN を設定する方法を理解したいと思う場合参照しま VLAN を Cisco Aironet ワイヤレス機器によって使用します。

以下の事項に注意して下さい: dot1Q と内側 VLANルーティング、L3 スイッチまたはルータのためのスイッチを設定する必要があります。

Q. Cisco 3005 VPN コンセントレータに無線ユーザ 認証するがあるために Cisco AP 1200 VxWorks を設定したいと思います。 どんな設定がこれを達成する AP およびクライアントにある必要がありますか。

A. このシナリオに AP かクライアントで必要な特定の設定がありません。 VPN コンセントレータのすべての設定をして下さい。

Q. Cisco 1232 AG AP を展開しています。 この AP と展開できるほとんどの安全な方法を知ることを望みます。 AAAサーバがないし、リソースだけ AP および Windows 2003 ドメインです。 方法について詳しく知っています静的な 128 ビット WEP キー、非ブロードキャスト SSID および MAC アドレス制限を使用する。 ユーザは windows XP ワークステーションおよびいくつかの PDA と大抵機能しています。 この設定用のセキュア実装とは何か。

A. Cisco ACS のような RADIUSサーバがない場合、LEAP、EAP-FAST なまたは MAC 認証のためのローカル RADIUSサーバで AP を設定できます。

注: 考慮する必要がある非常に重要な点はまたは EAP-FAST LEAP とクライアントを使用したいと思うかどうかです。 その場合、クライアントが EAP-FAST LEAP をサポートするユーティリティがなければ。Windows XP ユーティリティは PEAP か EAP-TLS だけをサポートします。

Q. PEAP 認証はエラー「SSL ハンドシェイクの間に」失敗される EAP-TLS とまたは PEAP 認証失敗します。 これは、なぜですか。

A. このエラーは Cisco バグ ID CSCee06008 （登録ユーザのみ）が原因で発生する場合があります。 PEAP は ADU 1.2.0.4 と失敗します。 この問題のための回避策は ADU の最新バージョンを使用することです。

Q. 同じ SSID の WPA およびローカル MAC 認証がある場合がありますか。

A. Cisco AP は同じサービス セット ID（SSID）のローカル MAC 認証および Wi-Fi Protected Access（WPA） Pre-share キー（WPA-PSK）をサポートしません。 WPA-PSK のローカル MAC 認証を有効に するとき、WPA-PSK ははたらきません。 この問題はローカル MAC 認証が設定から WPA-PSK ASCII パスワード行を削除するので発生します。

Q. 現在 3 Cisco がデータVLAN のための暗号 128 ビット WEP暗号化と設定される 1231 のワイヤレス AP あります。 SSID をブロードキャストしません。 環境の別途の RADIUSサーバがありません。 誰かはスキャン ツールを通して WEPキーを判別できワイヤレス トラフィックをモニタするのに二三週間のためのツールを使用しました。 どのようにこれを防ぎ、ネットワークをセキュアにすることができま

すか。

A. スタティックWEP はハッカーが十分なパケットを得るキャプチャすればことができ、同じ初期化ベクター（iv）が付いている 2つ以上のパケットを得られますこの問題に脆弱で。

この問題の発生を防ぐ複数の方法があります:

1. ダイナミック WEPキーを使用して下さい。
2. WPA を使用して下さい。
3. Cisco アダプタだけある場合、パケット キーおよび MIC ごとに有効に して下さい。

Q. 2 つの異なる WLAN がある場合、両方とも Wi-Fi プロテクテッド アクセス（WPA）のために設定しました-事前共有キー（PSK）、事前共有キーは WLAN ごとに異なりますか。 それらが異なっている場合、それは別の事前共有キーで設定される他の WLAN に影響を与えますか。

A. WPA-PSK の設定は WLAN ごとにあるはずです。 1 WPA-PSK を変更する場合、設定される他の WLAN に影響を与えるべきではありません。

Q. 環境ではプロ/ワイヤレス、拡張可能な認証プロトコル適用範囲が広いセキュアなトンネリングによる（EAP-FAST な）認証、および（Windows Active Directory（AD）にアカウントをリンクされる ACS） 3.3 Cisco Secure Access Control Server 大抵 Intel を使用します。 問題はユーザパスワードが約切れるとき Windows パスワードを変更するためにプロンプト表示しませんユーザをあります。 最終的に、アカウントは切れます。 ユーザをパスワードを変更するためにプロンプト表示させます Windows にソリューションがありますか。

A. Cisco Secure ACS パスワード エージング機能はユーザにこれらの状態の何れか一つ以上の下でパスワードを変更させます可能にします:

- の後幾日（経過時間によ日付ルール）の指定 番号
- の後ログオン（経過時間によ使用ルール）の指定 番号
- 新しいユーザがログオンする時最初に（パスワード変更ルール）

この機能のための Cisco Secure ACS を設定する方法の詳細については CiscoSecureユーザデータベースのためのパスワード エージングの有効にを参照して下さい。

Q. ユーザが LEAP を使用して無線でログオンするときそれらはログオン スクリプトをネットワーク ドライブをマップするために得ます。 ただし、PEAP 認証を用いる Wi-Fi プロテクテッド アクセス（WPA）か WPA2 を使用して、ログオン スクリプトは動作しません。 RADIUS（ACS）があるようにクライアントおよびアクセス ポイントは両方 Cisco です。 ログオン スクリプトはなぜ RADIUS（ACS）で動作しませんか。

A. マシン認証はログオン スクリプトがはたらくことができるがように必須です。 これはユーザがログオンする前にスクリプトをロードするためにネットワーク アクセスを得ることを無線ユーザが可能にします。

PEAP-MS-CHAPv2 でマシン認証を設定する方法の情報に関しては PEAP-MS-CHAPv2 マシン認

証での Cisco Secure ACS for Windows v3.2 の設定を参照して下さい。

Q. Cisco Aironet デスクトップ ユーティリティ ユーザが拡張可能な認証プロトコル転送する層セキュリティ（EAP-TLS）用のマシン認証を設定するとき（ADU）リリース 3.0 によって、ADU はユーザがプロファイルを作成することを可能にしません。 これは、なぜですか。

A. これは Cisco バグ ID CSCsg32032 （登録ユーザのみ）が理由でそうなったものです。 これはクライアントPC にインストールされるマシン 証明書が起こるあれば場合があり、ユーザ許可証がありません。

対応策はユーザ ストアへマシン 証明書をコピーすること、EAP-TLS プロファイルを作成し、次にマシン認証設定だけのためのユーザ ストアから証明書を取除きます。

Q. あらゆる方法がクライアントの MAC アドレスに基づいて Wireless LAN の VLAN を割り当てるありますか。

A. いいえ。 これは可能性のあるではないです。 RADIUSサーバからの VLAN 割り当ては 802.1X をだけ、ない MAC 認証使用します。 MAC アドレスが RADIUSサーバで認証される場合 MAC 認証を用いる VSAs を押すのに RADIUS を使用できます（LEAP/PEAP の USERID//パスワードと定義される）。

関連情報

- 無線ネットワーク セキュリティ
- ワイヤレスLANセキュリティ 白書
- ワイヤレスLANセキュリティ 概要
- ワイヤレス LAN ネットワークへの EAP-TLS の導入ガイド
- Cisco LEAP
- Wired Equivalent Privacy（WEP）の設定
- ワイヤレス製品に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems