EAP-FAST バージョン 1.02 設定ガイド

目次

概要

このドキュメントでは、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）バージョン 1.02 の設定例を紹介します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- ファームウェア バージョン 5.40 およびドライバ バージョン 8.5 導入済の IOS AP 12.2(13)JA3、350、または CB20A クライアント（CB21AG クライアントは 2H CY2004 でサポート予定）
- ACU 6.3 がインストールされている Access Control Server（ACS）3.2.3、Windows 2000、または XP

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

ACS での AP の設定

ACS で Access Point（AP; アクセス ポイント）をセットアップするには、次の手順を実行します。

1. ACS サーバで、左側にある [Network Configuration] をクリックします。
2. AAA クライアントを追加するには、**[Add Entry]** をクリックします。
3. ボックスに次の値を入力します。AAA Client IP Address：AP の IP アドレスKey：キーを作成します（キーが AP 共有秘密鍵と一致することを確認します）Authenticate Using：RADIUS（Cisco Aironet）
4. [Submit] をクリックします。
5. 再起動します。

EAP-FAST を使用するための ACS のセットアップ

EAP-FAST を使用できるように ACS をセットアップするには、次の手順を実行します。

1. [System Configuration] > [Global Authentication Setup] を選択します。
2. Allow EAP-FAST ボックスにチェックマークを付けます。
3. Authority ID Info フィールドに値を入力します（スペースは使用できません）。
4. Allow automatic PAC provisioning ボックスにチェックマークを付けます。**注:** PAC の自動プロビジョニングは、クライアントにインバンドで PAC を提供する、オーバーヘッドの少ない方法です。 自動プロビジョニングには、注意事項がいくつかあります。最初の EAP-FAST 認証に失敗しないと、自動プロビジョニングは実行されません。LDAP ユーザには自動プロビジョニングを行えないため、手動でプロビジョニングを行う必要があります。自動プロビジョニングでは、最初のプロビジョニング時に MITM 攻撃を受けやくなります。
5. EAP-FAST master server ボックスにチェックマークを付けます。
6. [Submit] をクリックします。
7. 再起動します。

AP の設定

AP を設定するには、次の手順を実行します。

1. [Security] > [Server Manager] を選択します。
2. Current Server List ドロップダウン リストから、RADIUS を選択します。
3. ACS の IP アドレスを入力します。

4. 共有秘密鍵を入力します（ACS 内のキーと一致する必要があります）。
5. [Apply] をクリックします。
6. EAP Authentication ドロップダウン リストから、RADIUS サーバの IP アドレスを選択します。
7. [Apply] をクリックします。

Encryption Manager（WEP 暗号化のみ）

WEP 暗号化のみを使用する場合は、次の手順を実行します。

1. [Security] > [Encryption Manager]を選択します。
2. [**WEP Encryption**] オプション ボタンをクリックします。
3. ドロップダウン リストから、Mandatory を選択します。
4. [**Encryption Key 1**] オプション ボタンをクリックします。
5. 鍵を入力します。
6. Key Size ドロップダウン リストから、128 を選択します。
7. [Apply] をクリックします。

Encryption Manager（WPA キー管理）

WPA キー管理を使用する場合は、次の手順を実行します。

1. [Security] > [Encryption Manager]を選択します。
2. Cipher オプション ボタンをクリックします。
3. ドロップダウン リストから、TKIP を選択します。
4. [Apply] をクリックします。

SSID Manager（WEP 暗号化のみ）

WEP 暗号化のみを使用する場合は、次の手順を実行します。

1. Current SSID List から SSID を選択するか、SSID フィールドに新しい SSID を入力します。
2. [**Open Authentication**] ボックスにチェックマークを入れます。
3. ドロップダウン リストから、EAP を選択します。
4. **[Network EAP]** ボックスにチェックマークを入れます。
5. [Apply] をクリックします。

SSID Manager（WPA キー管理）

WPA キー管理を使用する場合は、次の手順を実行します。

1. Current SSID List から SSID を選択するか、SSID フィールドに新しい SSID を入力します。
2. [**Open Authentication**] ボックスにチェックマークを入れます。
3. ドロップダウン リストから、EAP を選択します。
4. **[Network EAP]** ボックスにチェックマークを入れます。
5. Authenticated Key Management を選択します。

6. ドロップダウン リストから、Mandatory を選択します。
7. WPA ボックスにチェックマークを付けます。
8. [Apply] をクリックします。

EAP-FAST を使用するためのクライアントのセットアップ

WEP 暗号化のみ

WEP 暗号化のみを使用する場合は、次の手順を実行します。

1. ACU を開きます。
2. Manage Profile を選択します。
3. プロファイルを作成 (または編集) します。
4. AP のクライアント名と SSID を入力します。
5. **[Network Security]** タブをクリックします。
6. EAP-FAST を選択します。
7. [Configure] をクリックします。
8. Allow Automatic PAC Provisioning for This Profile ボックスにチェックマークを付けます。**注 :** PAC の自動プロビジョニングは、クライアントにインバンドで PAC を提供する、オーバーヘッドの少ない方法です。 自動プロビジョニングには、注意事項がいくつかあります。最初の EAP-FAST 認証に失敗しないと、自動プロビジョニングは実行されません。LDAP ユーザには自動プロビジョニングを行えないため、手動でプロビジョニングを行う必要があります。自動プロビジョニングでは、最初のプロビジョニング時に MITM 攻撃を受けやくなります。
9. [OK] をクリックします。
10. [OK] をクリックします。
11. [OK] をクリックします。
12. 作成したプロファイルを選択します。

WPA キー管理

WPA キー管理を使用する場合は、次の手順を実行します。

1. ACU を開きます。
2. Manage Profile を選択します。
3. プロファイルを作成 (または編集) します。
4. AP のクライアント名と SSID を入力します。
5. **[Network Security]** タブをクリックします。
6. WiFi Protected Access (WPA) ボックスにチェックマークを付けます。
7. Network Security Type に、EAP-FAST (WPA) を選択します。
8. [Configure] をクリックします。
9. Allow Automatic PAC Provisioning for This Profile ボックスにチェックマークを付けます。**注 :** PAC の自動プロビジョニングは、クライアントにインバンドで PAC を提供する、オーバーヘッドの少ない方法です。 自動プロビジョニングには、注意事項がいくつかあります。最初の EAP-FAST 認証に失敗しないと、自動プロビジョニングは実行されません。LDAP ユーザには自動プロビジョニングを行えないため、手動でプロビジョニングを行う必要があります。自動プロビジョニングでは、最初のプロビジョニング時に MITM 攻撃を受けやくな

ります。
10. [OK] をクリックします。
11. [OK] をクリックします。
12. [OK] をクリックします。
13. 作成したプロファイルを選択します。

PAC の手動プロビジョニングに関する補足

このセクションでは、すでに説明した手動 PAC プロビジョニングの設定方法とは異なる手順について説明します。

注: オプション **EAP-FAST な PAC ファイル生成は**ウィンドウに ACS で利用できないし、プロシージャはこのセクションで定義されるプロシージャを使用して手動でする必要があります。

EAP-FAST を使用するための ACS オプションのセットアップ

次の手順はオプションです。 一部のクライアントで自動プロビジョニングを使用したい場合は、このオプションにチェックマークを付けたままにしてください。

1. [System Configuration] > [Global Authentication Setup] を選択します。
2. Allow automatic PAC provisioning ボックスのチェックマークをはずします。

CSUtil.exe を使用して PAC を作成して下さい

次の手順は、要件に応じて大きく変わります。 詳細については、『Cisco Secure ACS for Windows Server 3.2 ユーザ ガイド』を参照してください。

CSUtil.exe を使用して PAC を作成するための基本構文は次のとおりです。

```
csutil [-t] [-filepath <full filepath>] [-passwd <password>] [[-a] [-g <group number>] [-u <user name>] [-f <full filepath>]]
```

-filepath は省略可能です。この部分には、出力先のディレクトリを指定します（すでに存在しているディレクトリを指定する必要があります）。 これを指定しなかった場合、PAC は ACS Utils のディレクトリに保存されます（多数の PAC を作成する場合は混乱する可能性があります）。

-passwd は省略可能です。この部分には、PAC を保護するためのパスワードを指定します。 これを指定しなかった場合、デフォルトのパスワードはありません。

次に、有効な PAC 作成コマンドの例をいくつか示します。

- **csutil - t -ファイル パス c:\acspac -パスワード 5p0rk5 - f c:\acspac\pac.txt** — pac.txt と名付けられるファイルにリストされているユーザ向けの PAC を作成します。
- **csutil - t -ファイル パス c:\acspac -パスワード 5p0rk5 - g 0** — ACS グループ 0 のユーザ向けの PAC を作成します。
- **csutil - t -ファイル パス c:\acspac -パスワード 5p0rk5 - u vadablam** — ACS のユーザ名 vadablam のための PAC を作成します。
- **csutil - t -ファイル パス c:\acspac -パスワード 5p0rk5 - a** — ACS のすべてのユーザ向けの PAC を作成します（これはかなりしばらく奪取できます）。

テストとして 1 人のユーザに対して PAC を作成するには、次の手順を実行します。

1. PAC の出力先ディレクトリを作成します（省略可能）。
2. そのユーザが ACS に存在することを確認します。
3. コマンド プロンプトを開きます。
4. ACS Utils のディレクトリに移動します。
5. **csutil を- t -ファイル パス <filepath> -パスワード <password> - u <user>** コマンド入力して下さい。
6. ユーザのホストに新しい .pac ファイルをコピーします。

次の手順を実行して、手動 PAC プロビジョニングを行うようにクライアントを設定します。

1. ACU で、Network Security Type として EAP-FAST を選択し、Configure をクリックします。
2. Allow Automatic PAC Provisioning for This Profile ボックスのチェックマークをはずします。
3. [Import] をクリックします。
4. .pac の場所を参照します。
5. .pac を選択します。
6. パスワードを入力します（要求された場合）。
7. [OK] をクリックします。
8. [OK] をクリックします。
9. [OK] をクリックします。
10. [OK] をクリックします。
11. 作成したプロファイルを選択します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

詳細は、次のドキュメントを参照してください。

- INFO: 2 の Windows NT Part 1 のエラーコード（技術情報 I）
- How To Error Codes in Windows NT Part 2 of 2

関連情報

- Cisco Secure ACS for Windows に関するサポート ページ
- Cisco Secure ACS for UNIX 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