IW URWBモード無線でのAES暗号化の設定

内容

はじめに

このドキュメントでは、URWBモードのIW9165およびIW9167無線でのAESパラメータの設定について説明します。

前提条件

要 件

次の項目に関する知識があることが推奨されます。

- 基本的なCLIナビゲーションとコマンド
- IW URWBモード無線の理解

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IW9165およびIW9167無線

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

AES:Advanced Encryption Standard(AES)は、データ通信を保護するための暗号化規格です。対称キーアルゴリズムであるため、データの暗号化と復号化の両方に同じキーが使用されます。

URWBモードのIW無線では、設定されているパスフレーズパラメータを使用して、すべてのコントロールプレーンデータを暗号化します。

したがって、2台のデバイスが互いに通信するか、同じパスフレーズを共有している場合は、同じネットワーク内の他のデバイスを検出することしかできません。

データプレーンを介して送信されるデータは、デフォルトでは暗号化されません。これは、無線でAESを有効にすることで暗号化できます。

両方のデバイスでAESが有効になっている場合、2台のデバイスは互いにしか通信できません。

IW無線でのキーローテーション：

暗号化を強化するためにIW無線で設定できる追加のセキュリティパラメータは他にもあります。WPA標準をサポートするために、IW無線でキーローテーションを有効にできます。

これはキーコントローラプロトコルで実行されます。このプロトコルにより、2台のデバイスが相互に通信し、パケット暗号化のための新しいPairwise Transient KeyとGroup Transient Keyの定期的な再生成をスケジュールできます。

Pairwise Transient Key(PTK)は1対1またはユニキャストトラフィックを保護し、Group Transient Key(GTK)はグループまたはブロードキャスト/マルチキャストトラフィックを保護します。

この機能を有効にすると、実際に攻撃が発生した場合に侵害される可能性のあるデータの量が減るため、セキュリティが強化されます。

暗号化に使用されるキーは一時的で、定期的に回転するため、どこにも保存されません。その他の秘密と証明書はすべて、Cisco TAMを介して保護される暗号化ボリュームに保存されます。

(https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trustworthy-technologies-datasheet.pdf)

Fluidityネットワークを実行している場合にキーのローテーションを有効にすると、通信が中断されることがあります。特にローミングプロセス中にローテーションが発生した場合には中断が発生します。

そのため、Fluidityの展開と一緒に使用することは推奨されません。

AES暗号化のパラメータは、CLIアクセスまたはIoT OD設定を介してのみIWデバイスで設定できます。

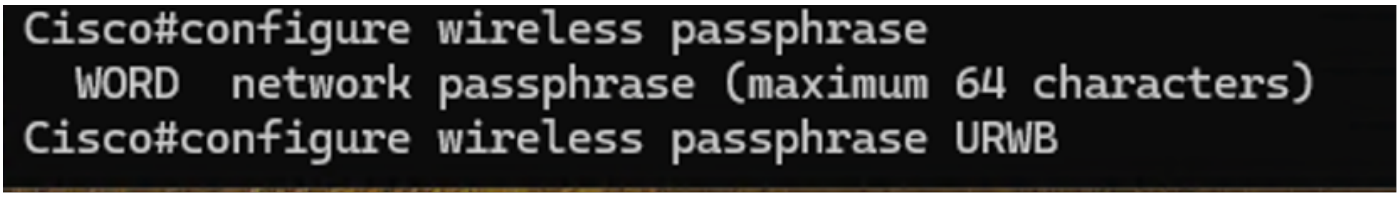
流動性パラメータのCLI設定

これらのパラメータは、デバイスのCLIのイネーブルモードから設定できます。

1. 無線でのパスフレーズの設定：

このパラメータは、無線でコントロールプレーンデータを暗号化するために使用されます。

```
Radio1#configure wireless passphrase URWB
```



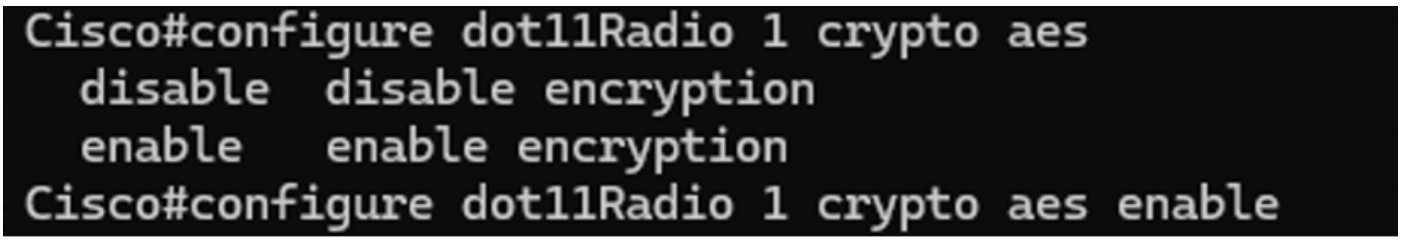
ワイヤレスパスフレーズの設定

2. 無線でAES暗号化を有効にする：

このパラメータにより、無線インターフェイスごとにAES暗号化を有効にできます。

Radio1#configure dot11Radio

crypto aes enable



dot11Radio 1の設定

3. 無線のキーコントローラを有効にします。

このパラメータは、無線でキーコントローラアルゴリズムを有効にするために使用されます。これは無線インターフェイスごとに有効にすることもでき、AESキーローテーションを使用するために必要です。

Radio1#configure dot11Radio

crypto key-control enable

```
Cisco#configure dot11Radio 1 crypto key-control
  disable       disable AES-based encryption key-control
  enable        enable AES-based encryption key-control
  key-rotation  set key rotation
Cisco#configure dot11Radio 1 crypto key-control enable
```

dot11Radio 1 crypto key-control（暗号化キー制御）

4. 無線でのキーローテーションを有効にする：

　このパラメータは、無線でキーローテーションを有効にするために使用され、インターフェイスごとに有効になります。

Radio1#configure dot11Radio

crypto key-control key-rotation enable

```
Cisco#configure dot11Radio 1 crypto key-control key-rotation
  <1-65535>  Key Rotation timeout (seconds)
  disable    disable key rotation
  enable     enable key rotation
```

dot11Radio crypto ket-rotationの設定

5. 無線でキーローテーションタイマーを設定します。

　このパラメータは、新しいキーが生成される時間間隔を設定するために使用されます。タイマー値は秒単位で追加され、パラメータは<1 ~ 65535>の範囲で変更できます。

　デフォルト値は3600秒（1時間ごと）に設定されています。

Radio1#configure dot11Radio

crypto key-control key-rotation <1 – 65535>

```
Cisco#configure dot11Radio 1 crypto key-control key-rotation
  <1-65535>  Key Rotation timeout (seconds)
  disable    disable key rotation
  enable     enable key rotation
```

dot11Radio crypto ket-rotationの設定

6. 無線のキー制御アルゴリズムパラメータを検証します。

暗号化パラメータに関する無線の現在の設定は、次のコマンドで検証できます。

Radio1#show dot11Radio

crypto

```
Cisco#show dot11Radio 1 crypto

Passphrase:             d0a3c370a6b508acadf7143243890068ab602e7b1a43f1f4b9fca940b4eb6348
AES encryption:         enabled
AES key-control:        enabled
Key rotation:           enabled
Key rotation timeout:   6800(second)
Cisco#
```

Show dot11Radio 1 crypto (隠しコマンド)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。