Konfigurieren der AES-Verschlüsselung für IW-URWB-Modus-Funkmodule

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

- [Anforderungen](#)
- [Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[CLI-Konfiguration der Fluiditätsparameter](#)

Einleitung

Dieses Dokument beschreibt die Konfiguration der AES-Parameter für IW9165- und IW9167-Funkmodule im URWB-Modus.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende CLI-Navigation und -Befehle
- Verständnis von IW-URWB-Modusradios

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- IW9165- und IW9167-Funkeinheiten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

AES - Advanced Encryption Standard ist ein Verschlüsselungsstandard zur sicheren Datenkommunikation. Es handelt sich um einen Algorithmus mit symmetrischem Schlüssel, d. h. der gleiche Schlüssel wird zum Verschlüsseln und Entschlüsseln von Daten verwendet.

IW-Funkmodule im URWB-Modus verwenden den auf ihnen konfigurierten Passphrase-Parameter zur Verschlüsselung aller Daten auf der Kontrollebene.

Daher können zwei beliebige Geräte nur dann miteinander kommunizieren oder andere Geräte im gleichen Netzwerk erkennen, wenn sie die gleiche Passphrase verwenden.

Die über die Datenebene gesendeten Daten sind standardmäßig nicht verschlüsselt. Dies kann verschlüsselt werden, indem AES auf den Funkmodulen aktiviert wird.

Zwei Geräte können nur miteinander kommunizieren, wenn für beide AES aktiviert ist.

Schlüsselrotation bei IW-Funkmodulen:

Es gibt weitere zusätzliche Sicherheitsparameter, die auf den IW-Funkmodulen konfiguriert werden können, um die Verschlüsselung zu stärken. Zur Unterstützung von WPA-Standards kann die Schlüsselrotation für die IW-Funkmodule aktiviert werden.

Dies wird auf dem Key-Controller-Protokoll ausgeführt, das es zwei miteinander kommunizierenden Geräten ermöglicht, die regelmäßige Regeneration des neuen paarweisen Übergangsschlüssels und des Gruppen-Übergangsschlüssels für die Paketverschlüsselung zu planen.

Der Pairwise Transient Key (PTK) sichert den One-to-One- oder Unicast-Datenverkehr, während der Group Transient Key (GTK) den Gruppen- oder Broadcast-/Multicast-Datenverkehr sichert.

Durch die Aktivierung dieser Funktion wird die Sicherheit erhöht, da die Datenmenge reduziert wird, die bei einem Angriff kompromittiert werden kann.

Die für die Verschlüsselung verwendeten Schlüssel sind temporär und drehen sich regelmäßig, daher werden sie nirgendwo gespeichert. Alle anderen Geheimnisse und Zertifikate werden in einem verschlüsselten Volume gespeichert, das über Cisco TAM gesichert wird.

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

Wenn Sie Fluidity Networks ausführen und die Schlüsselrotation aktivieren, kann es zu Unterbrechungen in der Kommunikation kommen, insbesondere wenn die Rotation während des Roaming-Prozesses stattfindet.

Daher wird die Verwendung zusammen mit Fluidity-Bereitstellungen nicht empfohlen.

Parameter für die AES-Verschlüsselung können auf den IW-Geräten nur über den CLI-Zugriff oder über die IoT-OD-Konfiguration konfiguriert werden.

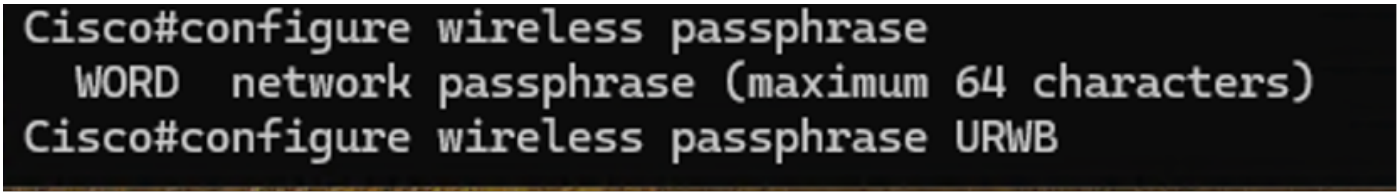
CLI-Konfiguration der Fluiditätsparameter

Diese Parameter können über den privilegierten Modus (enable mode) in der CLI der Geräte konfiguriert werden.

1. Konfigurieren der Passphrase auf den Funkmodulen:

Dieser Parameter wird für die Funkmodule zur Verschlüsselung der Steuerungsebenendaten verwendet.

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



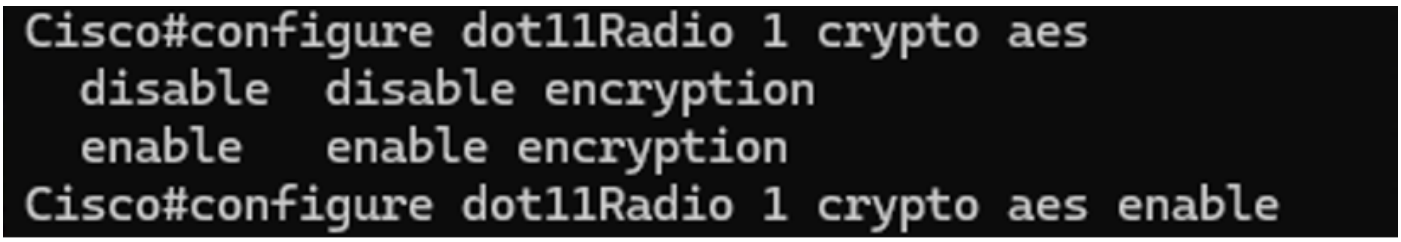
Wireless-Passphrase konfigurieren

2. Aktivieren der AES-Verschlüsselung auf Funkgeräten:

Dieser Parameter ermöglicht die Aktivierung der AES-Verschlüsselung pro Funkschnittstelle.

```
Radio1#configure dot11Radio

        crypto aes enable
```



dot11Radio 1 konfigurieren

3. Aktivieren der Schlüsselsteuerung auf den Funkgeräten:

Mit diesem Parameter wird der Schlüsselcontrolleralgorithmus für die Funkmodule aktiviert. Diese Funktion ist auch pro Funkschnittstelle aktiviert und für die AES-Schlüsselrotation erforderlich.

```
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 Verschlüsselungsschlüssel-Steuerung

4. Aktivieren der Schlüsselrotation auf den Funkgeräten:

Mit diesem Parameter wird die Schlüsselrotation für die Funkmodule aktiviert und für jede Schnittstelle aktiviert.

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 konfigurieren

5. Konfigurieren Sie den Zeitgeber für die Schlüsselrotation für die Funkmodule:

Dieser Parameter dient zum Konfigurieren des Zeitintervalls, in dem neue Schlüssel generiert werden. Der Timer-Wert wird in Sekunden hinzugefügt, und der Parameter kann von <1-65535> abweichen.

Der Standardwert ist 3600 Sekunden oder jede Stunde.

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 konfigurieren

6. Validieren der Parameter des Schlüsselkontrollalgorithmus für die Funkmodule:

Die aktuelle Konfiguration der Verschlüsselungsparameter kann mit dem folgenden Befehl validiert werden.

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#
```

Zeige dot11Radio 1 crypto

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.