在IW URWB模式無線電上配置AES加密

目錄

簡介

本文檔介紹URWB模式下IW9165和IW9167無線電上的AES引數配置。

必要條件

需求

思科建議您瞭解以下主題：

- 基本CLI導航和命令
- 瞭解IW URWB模式無線電

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- IW9165和IW9167無線電

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AES — 高級加密標準是用於保護資料通訊的加密加密標準。這是一種對稱金鑰演算法，這意味著使用相同的金鑰對資料進行加密和解密。

在URWB模式下的IW無線電中，使用在其上配置的密碼引數加密所有控制平面資料。

因此，如果任何兩台裝置共用相同的密碼，則它們只能相互通訊或發現同一網路中的其他裝置。

預設情況下，透過資料平面傳送的資料不會加密。可通過在無線電上啟用AES對此進行加密。

如果兩台裝置都啟用了AES，則它們只能相互通訊。

IW無線電上的金鑰輪替：

可以在IW無線電上配置其他安全引數，以增強加密能力。為了支援WPA標準，可在IW無線電上啟用金鑰輪替。

此命令在金鑰控制器協定上運行，該協定允許相互通訊的兩台裝置計畫定期重新生成新的成對臨時金鑰和組臨時金鑰，以便進行資料包加密。

成對瞬變金鑰(PTK)保護一對一或單點傳播流量，而群組瞬變金鑰(GTK)保護群組或廣播/多點傳播流量。

啟用此功能可降低在確實發生攻擊時可能受到威脅的資料量，從而增強安全性。

用於加密的金鑰是臨時的，並且會定期旋轉，因此，它們不會儲存在任何地方。所有其他機密和證書都儲存在加密卷中，該卷通過Cisco TAM進行保護。

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

如果啟用金鑰輪替，則在運行Fluidity網路時，可能會在通訊過程中遇到中斷，特別是在漫遊過程中發生輪替時。

因此，不建議將其與Fluidity部署一起使用。

只能通過CLI訪問或通過IoT OD配置在IW裝置上配置AES加密的引數。

流動引數的CLI配置

這些引數可在裝置的CLI上從啟用模式進行配置。

1. 在無線電上配置口令：

此引數用於無線電以加密控制平面資料。

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

```
Cisco#configure wireless passphrase
  WORD  network passphrase (maximum 64 characters)
Cisco#configure wireless passphrase URWB
```

設定無線密碼

2.在無線電上啟用AES加密：

此引數允許為每個無線電介面啟用AES加密。

Radio1#configure dot11Radio

crypto aes enable

```
Cisco#configure dot11Radio 1 crypto aes
  disable  disable encryption
  enable   enable encryption
Cisco#configure dot11Radio 1 crypto aes enable
```

配置dot11Radio 1

3.啟用無線電上的金鑰控制器：

此引數用於在無線電上啟用金鑰控制器演算法。每個無線電介面也會啟用此功能，並且使用AES金鑰輪替時需要啟用此功能。

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
```

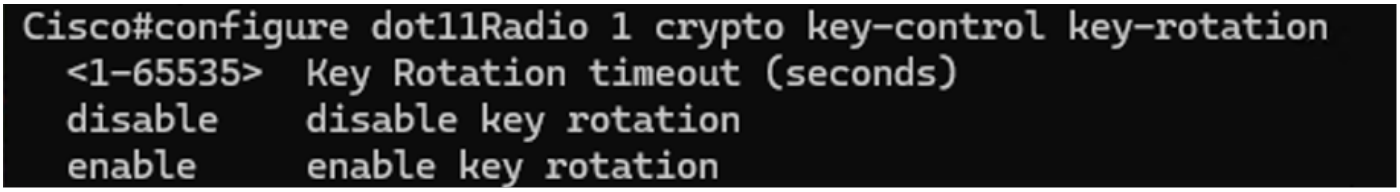
dot11Radio 1加密金鑰控制

4.啟用無線電上的金鑰輪替：

此引數用於在無線電上啟用金鑰輪替，並且在每個介面上啟用。

Radio1#configure dot11Radio

crypto key-control key-rotation enable



配置dot11無線加密金鑰輪替

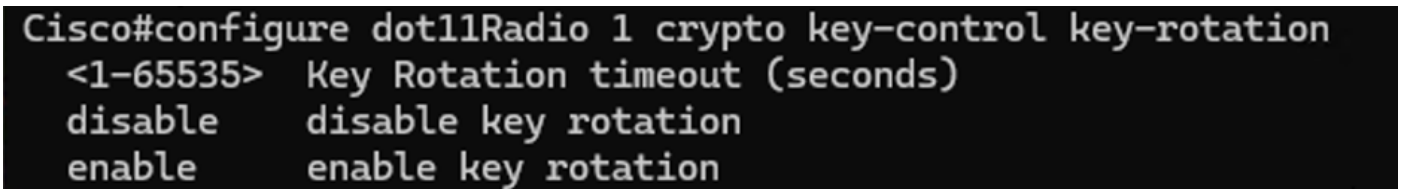
5.在無線電上配置金鑰輪替計時器：

此引數用於配置生成新金鑰的時間間隔。計時器值以秒為單位新增，引數可以從<1-65535>變化。

預設值設定為3600秒或每小時。

Radio1#configure dot11Radio

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



配置dot11無線加密金鑰輪替

6.驗證無線電上的關鍵控制演算法引數：

可使用以下命令驗證無線電上有關加密引數的當前配置。

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。