Configuration du chiffrement AES sur les radios en mode IW URWB

Table des matières

Introduction

Ce document décrit la configuration des paramètres AES sur les radios IW9165 et IW9167 en mode URWB.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation et commandes de base CLI
- Présentation des radios en mode IW URWB

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Radios IW9165 et IW9167

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

AES - Advanced Encryption Standard est une norme de cryptage permettant de sécuriser la communication des données. Il s'agit d'un algorithme à clé symétrique qui signifie que la même clé est utilisée pour chiffrer et déchiffrer les données.

IW Radios en mode URWB, utilisez le paramètre de phrase de passe configuré sur eux pour chiffrer toutes les données du plan de contrôle.

Par conséquent, deux périphériques ne peuvent communiquer entre eux ou découvrir d'autres périphériques sur le même réseau que s'ils partagent la même phrase de passe.

Les données envoyées sur le plan de données ne sont pas chiffrées par défaut. Il est possible de chiffrer ce code en activant AES sur les radios.

Deux périphériques ne peuvent communiquer entre eux que s'ils sont tous deux équipés de la fonction AES.

Rotation des clés sur les radios IW :

D'autres paramètres de sécurité supplémentaires peuvent être configurés sur les radios IW pour renforcer le chiffrement. Pour prendre en charge les normes WPA, la rotation des clés peut être activée sur les radios IW.

Cette commande s'exécute sur le protocole de contrôleur de clé qui permet à deux périphériques communiquant entre eux de programmer la régénération périodique des nouvelles clés Pairwise Transient Key et Group Transient Key pour le cryptage des paquets.

La PTK (Pairwise Transient Key) sécurise le trafic de monodiffusion ou de monodiffusion, tandis que la GTK (Group Transient Key) sécurise le trafic de groupe ou de diffusion/multidiffusion.

L'activation de cette fonctionnalité renforce la sécurité en réduisant la quantité de données pouvant être compromises en cas d'attaque.

Les clés utilisées pour le cryptage sont temporaires et tournent périodiquement, par conséquent, elles ne sont stockées nulle part. Tous les autres secrets et certificats sont stockés dans un volume chiffré sécurisé via Cisco TAM.

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

Lors de l'exécution de réseaux Fluidité, si vous activez la rotation des clés, vous risquez d'être perturbé dans la communication, en particulier si la rotation se produit pendant le processus d'itinérance.

Par conséquent, il n'est pas recommandé de l'utiliser avec les déploiements Fluidité.

Les paramètres de cryptage AES peuvent être configurés sur les périphériques IW uniquement à partir de l'accès CLI ou via la configuration IoT OD.

Configuration CLI des paramètres de fluidité

Ces paramètres peuvent être configurés à partir du mode enable sur l'interface de ligne de commande des périphériques.

1. Configuration de la phrase de passe sur les radios :

Ce paramètre est utilisé par les radios pour chiffrer les données du plan de contrôle.

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

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

Configurer la phrase de passe sans fil

2. Activation du cryptage AES sur les radios :

Ce paramètre permet d'activer le cryptage AES par interface radio.

```
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
```

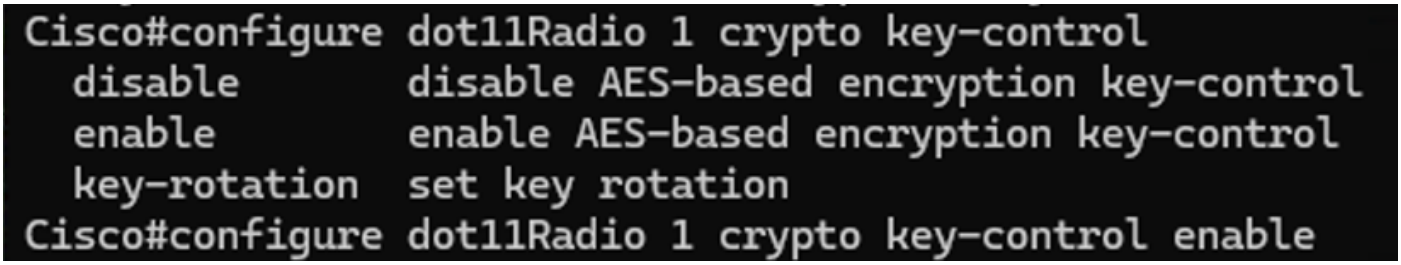
Configuration de dot11Radio 1

3. Activation du contrôleur clé sur les radios :

Ce paramètre est utilisé pour activer l'algorithme de contrôleur de clé sur les radios. Cette option est également activée par interface radio et est requise pour utiliser la rotation des clés AES.

```
Radio1#configure dot11Radio

        crypto key-control enable
```



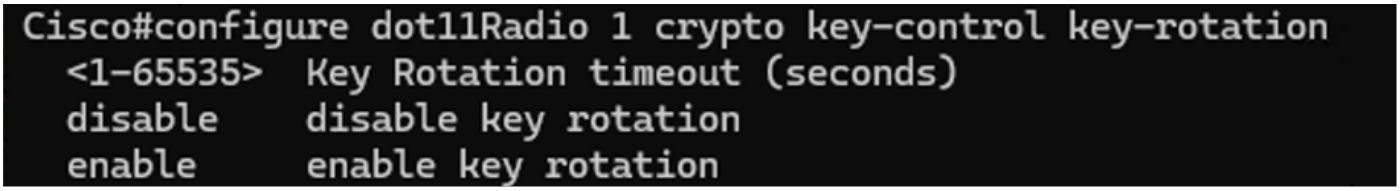
dot11Contrôle de clé de chiffrement Radio 1

4. Activation de la rotation des touches sur les radios :

Ce paramètre est utilisé pour activer la rotation des clés sur les radios et est activé par interface.

Radio1#configure dot11Radio

crypto key-control key-rotation enable



Configurer la rotation de cryptage radio dot11Radio

5. Configurez le minuteur de rotation des clés sur les radios :

Ce paramètre est utilisé pour configurer l'intervalle de temps auquel les nouvelles clés sont générées. La valeur du minuteur est ajoutée en secondes et le paramètre peut varier de **<**1-65535**>**.

La valeur par défaut est de 3 600 secondes ou toutes les heures.

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
```

Configurer la rotation de cryptage radio dot11Radio

6. Validation des paramètres de l'algorithme de contrôle clé sur les radios :

La configuration actuelle de la radio relative aux paramètres de cryptage peut être validée à l'aide de la commande ci-dessous.

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 dot11Crypto Radio 1

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.