Configurazione della crittografia AES sulle radio in modalità IW URWB

Sommario

Introduzione

Questo documento descrive la configurazione dei parametri AES sulle radio IW9165 e IW9167 in modalità URWB.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Navigazione e comandi CLI di base
- Informazioni sulle radio in modalità URWB IW

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Radio IW9165 e IW9167

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

AES - Advanced Encryption Standard è uno standard di crittografia per la comunicazione sicura dei dati. Si tratta di un algoritmo a chiave simmetrica che consente di utilizzare la stessa chiave sia per crittografare che per decrittografare i dati.

Le radio IW in modalità URWB utilizzano il parametro della passphrase configurato su di esse per crittografare tutti i dati del control plane.

Pertanto, due dispositivi possono comunicare tra loro o rilevare altri dispositivi nella stessa rete solo se condividono la stessa passphrase.

Per impostazione predefinita, i dati inviati tramite il piano dati non vengono crittografati. È possibile crittografare questa impostazione abilitando AES sulle radio.

Due dispositivi possono comunicare solo tra loro, se su entrambi è abilitato AES.

Rotazione dei tasti sulle radio IW:

Nelle radio IW è possibile configurare altri parametri di sicurezza per rendere più sicura la crittografia. Per supportare gli standard WPA, è possibile abilitare la rotazione dei tasti sulle radio IW.

Questa operazione viene eseguita sul protocollo del controller della chiave, che consente a due dispositivi in comunicazione tra loro di pianificare la rigenerazione periodica della nuova chiave temporanea Pairwise e della nuova chiave temporanea di gruppo per la crittografia dei pacchetti.

La chiave temporanea Pairwise (PTK) protegge il traffico uno a uno o unicast, mentre la chiave temporanea del gruppo (GTK) protegge il traffico di gruppo o broadcast/multicast.

L'attivazione di questa funzione migliora la sicurezza riducendo la quantità di dati che può essere compromessa in caso di attacco.

Le chiavi utilizzate per la crittografia sono temporanee e vengono ruotate periodicamente, pertanto non vengono memorizzate in alcun punto. Tutti gli altri segreti e certificati sono archiviati in un volume crittografato protetto tramite Cisco TAM.

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

Quando si eseguono reti Fluidity se si abilita la rotazione delle chiavi, si possono verificare interruzioni nella comunicazione, soprattutto se la rotazione avviene durante il processo di roaming.

Pertanto non è consigliabile utilizzarlo insieme alle distribuzioni Fluidity.

I parametri per la crittografia AES possono essere configurati sui dispositivi IW solo dall'accesso CLI o tramite la configurazione OD IoT.

Configurazione CLI dei parametri di fluidità

Questi parametri possono essere configurati dalla modalità di abilitazione nella CLI dei dispositivi.

1. Configurazione della passphrase per le radio:

Questo parametro viene utilizzato per le radio per crittografare i dati del control plane.

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

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

Configura passphrase wireless

2. Abilitazione della crittografia AES sulle radio:

Questo parametro consente di abilitare la crittografia AES per interfaccia 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
```

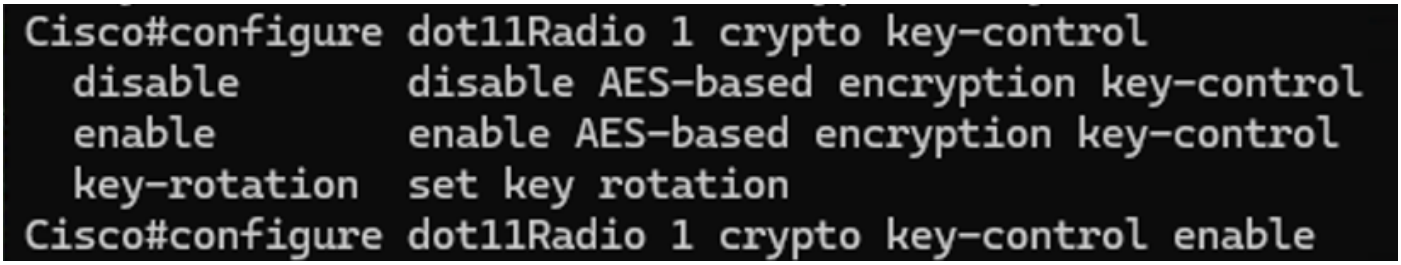
Configura dot11Radio 1

3. Attivazione del controller della chiave sulle radio:

Questo parametro viene utilizzato per abilitare l'algoritmo del controller della chiave nelle radio. Questa funzionalità è disponibile anche per le interfacce radio ed è necessaria per utilizzare la rotazione delle chiavi AES.

```
Radio1#configure dot11Radio

        crypto key-control enable
```



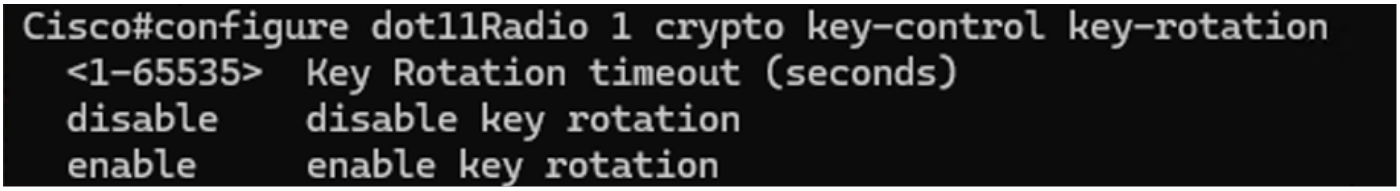
dot11Radio 1 crypto key-control

4. Abilitazione della rotazione dei tasti sulle radio:

Questo parametro viene utilizzato per attivare la rotazione delle chiavi sulle radio e viene attivato per interfaccia.

Radio1#configure dot11Radio

crypto key-control key-rotation enable



Configurare la rotazione ket della crittografia dot11Radio

5. Configurare il timer di rotazione delle chiavi sulle radio:

Questo parametro viene utilizzato per configurare l'intervallo di tempo in base al quale vengono generate le nuove chiavi. Il valore del timer viene aggiunto in secondi e il parametro può variare da <1-65535>.

Il valore predefinito è 3600 secondi o ogni ora.

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
```

Configurare la rotazione ket della crittografia dot11Radio

6. Convalida dei parametri dell'algoritmo di controllo a chiave sulle radio:

La configurazione corrente della radio relativa ai parametri di crittografia può essere convalidata con il comando seguente.

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#
```

Mostra crittografia dot11Radio 1

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).