Configuración de la Encriptación AES en Radios de Modo IW URWB

Contenido

Introducción

Este documento describe la configuración de los parámetros AES en radios IW9165 e IW9167 en modo URWB.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Navegación y comandos básicos de CLI
- Comprensión de las radios de modo URWB de IW

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Radios IW9165 e IW9167

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

AES: Estándar de cifrado avanzado es un estándar de cifrado criptográfico para proteger la comunicación de datos. Es un algoritmo de clave simétrica que significa que la misma clave se utiliza para cifrar y descifrar datos.

Radios IW en modo URWB, utilice el parámetro de frase de paso configurado en ellas para cifrar todos los datos del plano de control.

Por lo tanto, dos dispositivos cualesquiera solo pueden comunicarse entre sí o descubrir otros dispositivos en la misma red si comparten la misma frase de contraseña.

Los datos enviados a través del plano de datos no están cifrados de forma predeterminada. Esto se puede cifrar habilitando AES en las radios.

Dos dispositivos solo pueden comunicarse entre sí, si ambos tienen habilitado AES.

Rotación de teclas en radios IW:

Existen otros parámetros de seguridad adicionales que se pueden configurar en las radios IW para reforzar el cifrado. Para admitir los estándares WPA, se puede habilitar la rotación de teclas en las radios IW.

Esto se ejecuta en el protocolo del controlador de claves que permite que dos dispositivos que se comunican entre sí programen la regeneración periódica de la nueva clave transitoria de pares y la clave transitoria de grupo para el cifrado de paquetes.

La clave transitoria en pares (PTK) protege el tráfico unidifusión o de uno a uno, mientras que la clave transitoria de grupo (GTK) protege el tráfico de difusión/multidifusión o de grupo.

Al activar esta función, se mejora la seguridad al reducir la cantidad de datos que pueden estar en peligro si se produce un ataque.

Las claves utilizadas para el cifrado son temporales y giran periódicamente, por lo que no se almacenan en ningún lugar. El resto de secretos y certificados se almacenan en un volumen cifrado que se protege mediante Cisco TAM.

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

Al ejecutar redes Fluidity si habilita la rotación de claves, puede experimentar una interrupción en la comunicación, especialmente si la rotación ocurre durante el proceso de roaming.

Por lo tanto, no se recomienda su uso junto con implementaciones de fluidez.

Los parámetros para el cifrado AES se pueden configurar en los dispositivos IW solamente desde el acceso CLI o a través de la configuración OD de IoT.

Configuración CLI de los parámetros de fluidez

Estos parámetros se pueden configurar desde el modo de habilitación en la CLI de los dispositivos.

1. Configuración de la frase de contraseña en las radios:

Este parámetro se utiliza para que las radios cifren los datos del plano de control.

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

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

Configurar frase de paso inalámbrica

2. Habilitación del cifrado AES en las radios:

Este parámetro permite habilitar el cifrado AES por interfaz de 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
```

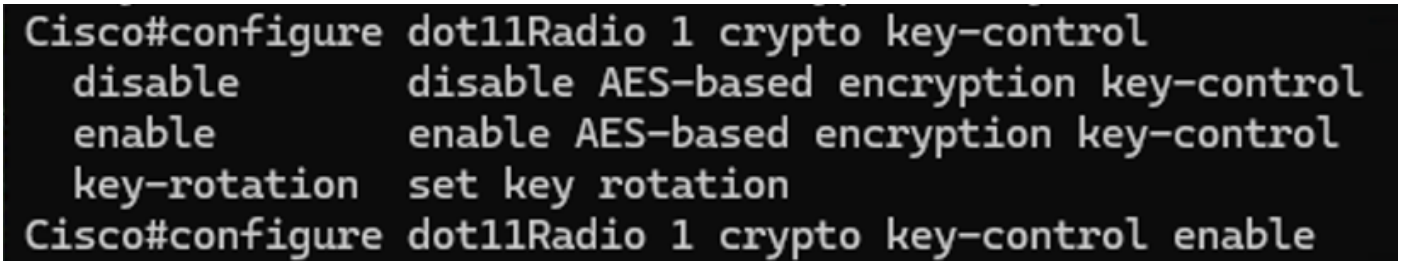
Configuración de dot11Radio 1

3. Habilitación del controlador de la llave en las radios:

Este parámetro se utiliza para habilitar el algoritmo del controlador de claves en las radios. Esto también se habilita por interfaz de radio y es necesario para utilizar la rotación de claves AES.

```
Radio1#configure dot11Radio

        crypto key-control enable
```



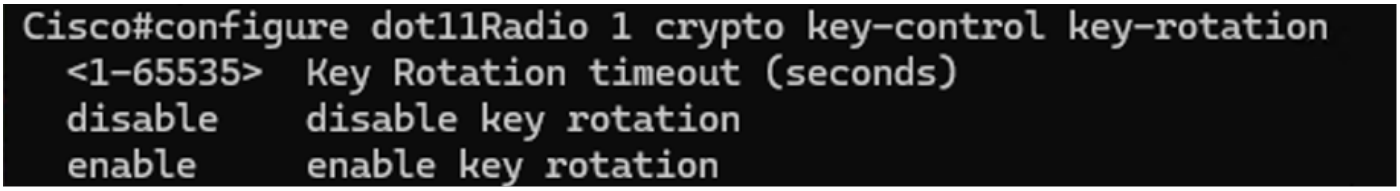
dot11Radio 1 crypto key-control

4. Activación de la rotación de llaves en las radios:

Este parámetro se utiliza para habilitar la rotación de teclas en las radios y se habilita por interfaz.

Radio1#configure dot11Radio

crypto key-control key-rotation enable



Configurar dot11Radio crypto ket-rotation

5. Configure el temporizador de rotación de teclas en las radios:

Este parámetro se utiliza para configurar el intervalo de tiempo en el que se generan las nuevas claves. El valor del temporizador se agrega en segundos y el parámetro puede variar de <1-65535>.

El valor predeterminado se establece en 3600 segundos o cada hora.

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
```

Configurar dot11Radio crypto ket-rotation

6. Validación de los parámetros del algoritmo de control de claves en las radios:

La configuración actual en la radio con respecto a los parámetros de encripción se puede validar con el siguiente comando.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).