IW URWB 모드 무선에서 AES 암호화 구성

목차

소개

이 문서에서는 URWB 모드의 IW9165 및 IW9167 무선 장치에 대한 AES 매개변수 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 CLI 탐색 및 명령
- IW URWB 모드 무선 송수신 장치 이해

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- IW9165 및 IW9167 무선

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

AES - Advanced Encryption Standard는 데이터 통신을 보호하기 위한 암호화 표준입니다. 대칭 키 알고리즘으로, 데이터를 암호화하고 해독하는 데 동일한 키가 사용됨을 의미합니다.

URWB 모드의 IW Radio는 모든 제어 평면 데이터를 암호화하기 위해 구성된 패스프레이즈 매개변수를 사용합니다.

따라서 두 디바이스는 동일한 암호를 공유하는 경우에만 서로 통신하거나 동일한 네트워크의 다른

디바이스를 검색할 수 있습니다.

데이터 평면을 통해 전송되는 데이터는 기본적으로 암호화되지 않습니다. 이는 무선 장치에서 AES를 활성화하여 암호화할 수 있습니다.

두 디바이스 모두 AES가 활성화된 경우에만 두 디바이스가 서로 통신할 수 있습니다.

IW 무선 장치의 키 교체:

IW 무선 장치에 구성할 수 있는 다른 추가 보안 매개변수도 있어 암호화를 더욱 강화합니다. WPA 표준을 지원하기 위해 IW 무선 장치에서 키 회전을 활성화할 수 있습니다.

이는 서로 통신하는 두 장치가 패킷 암호화를 위해 새 Pairwise 임시 키 및 그룹 임시 키의 주기적인 재생성을 예약할 수 있도록 하는 키 컨트롤러 프로토콜에서 실행됩니다.

PTK(Pairwise Transient Key)는 일대일 또는 유니캐스트 트래픽을 보호하는 반면 GTK(Group Transient Key)는 그룹 또는 브로드캐스트/멀티캐스트 트래픽을 보호합니다.

이 기능을 활성화하면 실제로 공격이 발생한 경우 감염될 수 있는 데이터의 양이 줄어들어 보안이 향상됩니다.

암호화에 사용되는 키는 일시적이며 주기적으로 회전하므로 어디에도 저장되지 않습니다. 다른 모든 비밀과 인증서는 Cisco TAM을 통해 보호되는 암호화된 볼륨에 저장됩니다.

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

Fluidity networks를 실행할 때 키 순환을 활성화하면 특히 로밍 프로세스 중에 순환이 발생하면 통신 중단이 발생할 수 있습니다.

따라서 Fluidity 구축과 함께 사용하는 것은 권장되지 않습니다.

AES 암호화를 위한 매개변수는 CLI 액세스에서 또는 IoT OD 컨피그레이션을 통해서만 IW 디바이스에 구성할 수 있습니다.

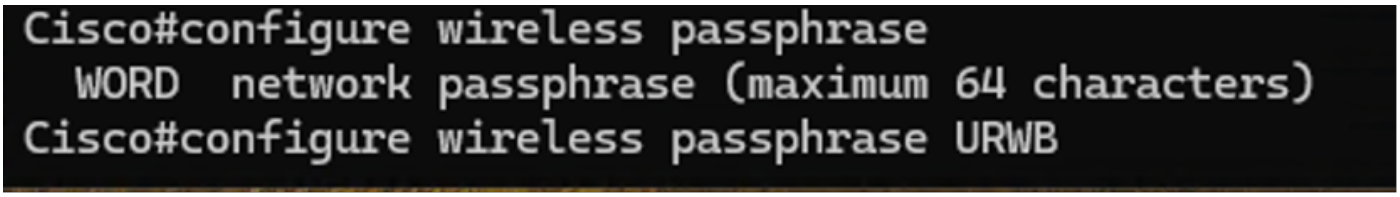
유동성 매개변수의 CLI 컨피그레이션

이러한 매개변수는 디바이스의 CLI에서 활성화 모드에서 구성할 수 있습니다.

1. 무선 장치에서 암호 구성:

이 매개변수는 무선 장치가 제어 평면 데이터를 암호화하는 데 사용됩니다.

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



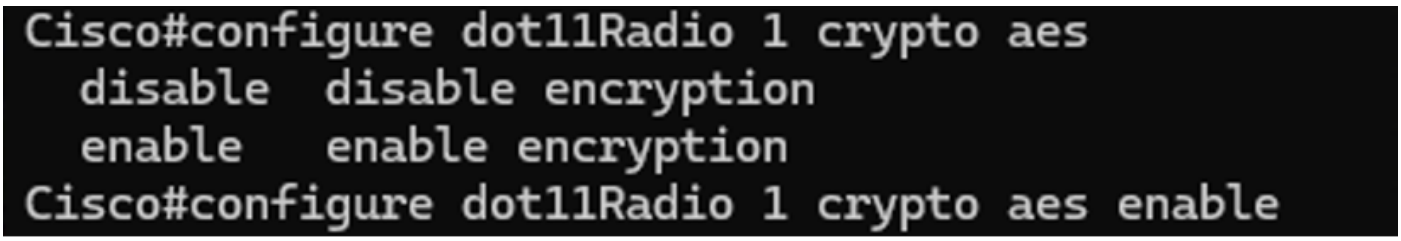
무선 암호 구성

2. 무선 장치에서 AES 암호화를 활성화합니다.

이 매개변수는 무선 인터페이스당 AES 암호화를 활성화할 수 있습니다.

```
Radio1#configure dot11Radio

        crypto aes enable
```



dot11Radio 구성 1

3. 무선 장치의 키 컨트롤러 활성화:

이 매개변수는 무선 장치에서 키 컨트롤러 알고리즘을 활성화하는 데 사용됩니다. 이 역시 무선 인터페이스별로 활성화되며 AES 키 순환을 사용하는 데 필요합니다.

```
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 암호화 키 제어

4. 무선 장치에서 키 순환 사용:

이 매개변수는 무선 장치에서 키 회전을 활성화하는 데 사용되며 인터페이스별로 활성화됩니다.

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
```

dot11무선 암호화 패킷-회전 구성

5. 무선 장치에서 키 순환 타이머를 구성합니다.

이 매개변수는 새 키가 생성되는 시간 간격을 구성하는 데 사용됩니다. 타이머 값은 초 단위로 추가되며 매개 변수는 <1-65535>부터 달라질 수 있습니다.

기본값은 3600초 또는 매시간으로 설정됩니다.

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
```

dot11무선 암호화 패킷-회전 구성

6. 무선 장치에서 주요 제어 알고리즘 매개변수 검증:

아래 명령을 사용하여 암호화 매개변수에 대한 무선 장치의 현재 컨피그레이션을 확인할 수 있습니다.

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#
```

dot11Radio 1 암호화 표시

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.