在IW URWB模式无线电上配置AES加密

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

流动性参数的CLI配置

简介

本文档介绍在URWB模式下的IW9165和IW9167无线电上配置AES参数。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本CLI导航和命令
- 了解IW URWB模式无线电

使用的组件

本文档中的信息基于以下软件和硬件版本：

- IW9165和IW9167无线电

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

AES — 高级加密标准是用于保护数据通信的加密加密标准。它是对称密钥算法，这意味着使用相同的密钥来加密和解密数据。

在URWB模式下的IW无线电，使用配置在其上的密码短语参数加密所有控制平面数据。

因此，如果任何两台设备共享相同的口令，则它们只能相互通信或发现同一网络中的其它设备。

默认情况下不会加密通过数据平面发送的数据。这可以通过在无线电上启用AES进行加密。

如果两台设备都启用了AES，则它们只能相互通信。

IW无线电上的密钥轮替：

在IW无线电上还可以配置其他安全参数，以增强加密能力。为了支持WPA标准，可以在IW无线电上启用密钥轮替。

这运行在密钥控制器协议上，该协议允许两台设备相互通信，以计划定期重新生成新的成对临时密钥和组临时密钥以进行数据包加密。

成对瞬时密钥(PTK)保护一对一或单播流量，而组瞬时密钥(GTK)保护组或广播/组播流量。

启用此功能可减少在确实存在攻击时可能受到危害的数据量，从而提高安全性。

用于加密的密钥是临时的，并且会定期旋转，因此它们不会存储在任何地方。所有其他机密和证书都存储在加密卷中，该卷通过Cisco TAM进行保护。

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

运行流动性网络时，如果启用密钥轮替，可能会在通信中遇到中断，特别是在漫游过程中发生轮替时。

因此，不建议将其与Fluidity部署一起使用。

AES加密的参数只能从CLI访问或通过IoT OD配置在IW设备上配置。

流动性参数的CLI配置

这些参数可在设备的CLI的启用模式下配置。

1. 在无线电上配置口令：

此参数用于无线电以加密控制平面数据。

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

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

配置无线口令

2.在无线电上启用AES加密：

此参数允许对每个无线电接口启用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.在无线电上启用密钥控制器：

此参数用于在无线电上启用密钥控制器算法。此功能也针对每个无线电接口启用，并且需要使用AES密钥轮替。

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
```

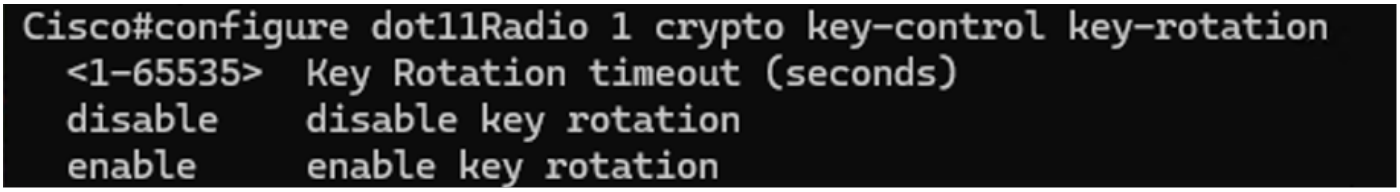
dot11Radio 1 crypto key-control

4.启用无线电上的密钥轮替：

此参数用于在无线电上启用密钥轮替，并在每个接口上启用。

Radio1#configure dot11Radio

crypto key-control key-rotation enable



配置dot11无线加密密钥轮替

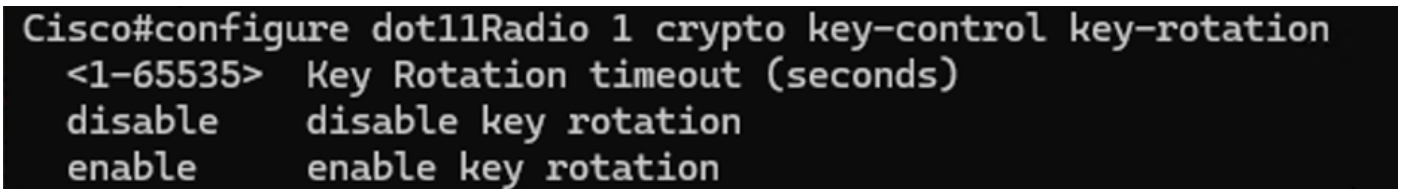
5.在无线电上配置密钥轮换计时器：

此参数用于配置生成新密钥的时间间隔。计时器值以秒为单位添加，参数可以从<1-65535>变化。

默认值设置为3600秒或每小时。

Radio1#configure dot11Radio

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



配置dot11无线加密密钥轮替

6.验证无线电设备上的关键控制算法参数：

可使用以下命令验证无线电上有关加密参数的当前配置。

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。