Configure AES Encryption on IW URWB Mode Radios

Contents

Introduction

This document describes the configuration of AES parameters on IW9165 and IW9167 radios in URWB mode.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic CLI navigation and commands
- Understanding of IW URWB mode radios

Components Used

The information in this document is based on these software and hardware versions:

- IW9165 and IW9167 radios

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

AES – Advanced Encryption Standard is a cryptographic encryption standard to secure communication of data. It is a symmetric-key algorithm which means the same key is used to both encrypt and decrypt data.

IW Radios in URWB mode, use the passphrase parameter configured on them to encrypt all of the control plane data.

Hence, any two devices can only communicate with each other or discover other devices in the same network if they share the same passphrase.

The data sent over the data plane is not encrypted by default. This can be encrypted by enabling AES on the radios.

Two devices can only communicate with each other, if they both have AES enabled on them.

Key rotation on IW radios :

There are other additional security parameters that can be configured on the IW radios to make encryption stronger. To support WPA standards, key rotation can be enabled on the IW radios.

This runs on Key controller protocol which allows two devices communicating with each other to schedule periodic regeneration of new Pairwise Transient Key and Group Transient Key for packet encryption.

The Pairwise Transient Key (PTK) secures one-to-one or unicast traffic, while the Group Transient Key (GTK) secures group or broadcast/multicast traffic.

Enabling this feature enhances security by reducing the amount of data that can be compromised if there is indeed an attack.

The keys used for encryption are temporary and rotate periodically, therefore, they are not stored anywhere. All other secrets and certificates are stored in an encrypted volume which is secured via Cisco TAM.

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

When running Fluidity networks if you enable key rotation, you can experience disruption in the communication, especially if the rotation happens during the roaming process.

Hence it is not recommended to be used alongside Fluidity deployments.

Parameters for AES encryption can be configured on the IW devices only from the CLI access or via IoT OD configuration.

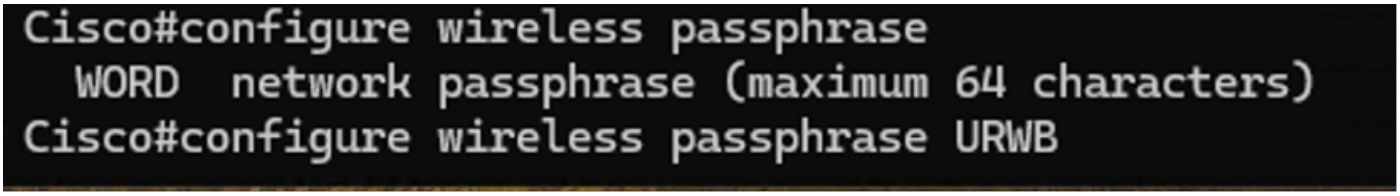
CLI configuration of Fluidity parameters

These parameters can be configured from enable mode on the CLI of the devices.

1. Configuring passphrase on the radios:

This parameter is used for the radios to encrypt the control plane data.

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



Configure Wireless Passphrase

2. Enabling AES encryption on the radios:

This parameter allows enabling AES encryption per radio interface.

```
Radio1#configure dot11Radio <interface> crypto aes enable
```

```
Cisco#configure dot11Radio 1 crypto aes
  disable  disable encryption
  enable   enable encryption
Cisco#configure dot11Radio 1 crypto aes enable
```

Configure dot11Radio 1

3. Enabling key controller on the radios:

This parameter is used to enable key controller algorithm on the radios. This is also enabled per radio interface, and is required to use AES key rotation.

```
Radio1#configure dot11Radio <interface> 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. Enabling key rotation on the radios:

This parameter is used to enabled key rotation on the radios and is enabled per interface.

```
Radio1#configure dot11Radio <interface> 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
```

Configure dot11Radio crypto ket-rotation

5. Configure key rotation timer on the radios:

This parameter is used to configure the time interval at which new keys are generated. The timer value is added in seconds, and the parameter can vary from <1-65535>.

The default value is set to 3600 seconds or every hour.

```
Radio1#configure dot11Radio <interface> 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
```

Configure dot11Radio crypto ket-rotation

6. Validating key control algorithm parameters on the radios:

The current configuration on the radio regarding encryption parameters can be validated with the command below.

```
Radio1#show dot11Radio <interface> 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