Encrypted Tunnel Deployment Guide

Revised: March 23, 2018,

Introduction

This document introduces the 8.7 Mobility Encrypted Tunnel and provides general guidelines for its deployment. The purpose of this document is to:

- Provide an overview of 8.7 Mobility Encrypted Tunnel Feature
- Highlight supported Key Features
- Provide details on deploying and managing the 8.7 Mobility Encrypted Tunnel Feature

Pre-requisite

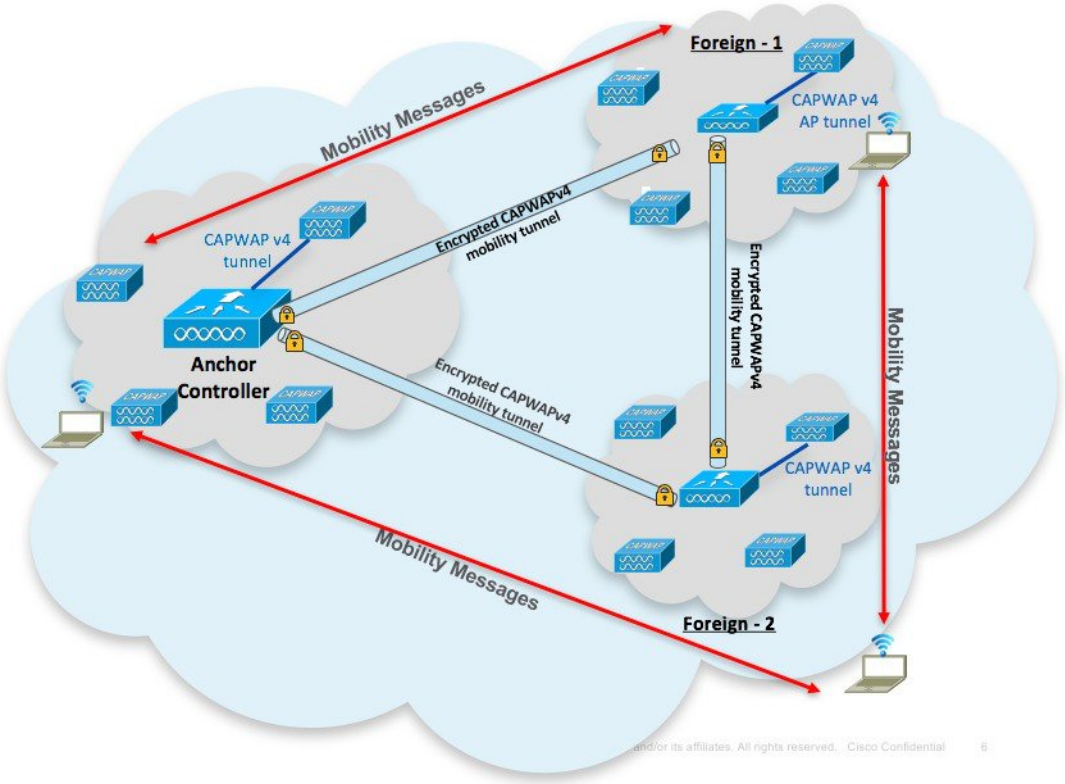
You must have AireOS 8.0 or higher release on a Wireless LAN Controller in order to upgrade to the 8.5MR1 or 8.7 code.

Note This feature is functional only in 8.5MR1 and 8.7 and above releases and is supported on 3504, 5520 and 8540 controllers.

Product or Feature Overview

The scope of the document is to provide a high level system description of support for End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC. The document also describes the basic assumptions from the WLC perspective to support End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC.

The architecture for End-to-End encryption of Mobility tunnel between Anchor and Foreign WLC is shown in the diagram below. In this architecture the WLCs are connected through CAPWAP based mobility tunnels which use DTLS encryption between the WLCs. The client data passes through secure DTLS encrypted CAPWAP tunnel between AP to WLC and between the Foreign and Anchor WLCs it passes through the CAPWAP based mobility tunnels which use DTLS encryption. Thus, through the entire data path from the client network to the Anchor WLC the client data is passing through encrypted tunnel with no scope for Man in the Middle snooping.



- In release 8.7 end-to-end Tunnel encrypted between Anchor and Foreign Controllers
- The encrypted tunnel passes through CAPWAP v4 with DTLS encryption
- Old and New Mobility Architecture will be supported
- Client SSO will be supported
- Supported on 3504, 5520 and 8540 controllers

Configuring Encrypted Mobility Tunnel

To configure End to End Encrypted Mobility Tunnel in the release 8.7 follow the steps as indicated below.

Procedure

Step 1 Configure all the controllers that need to participate in the Mobility Group exchange. All controllers have to be configured with each other information.


```
(Cisco Controller) >config mobility group member add ?

<IP addr>      Member switch IP address
```

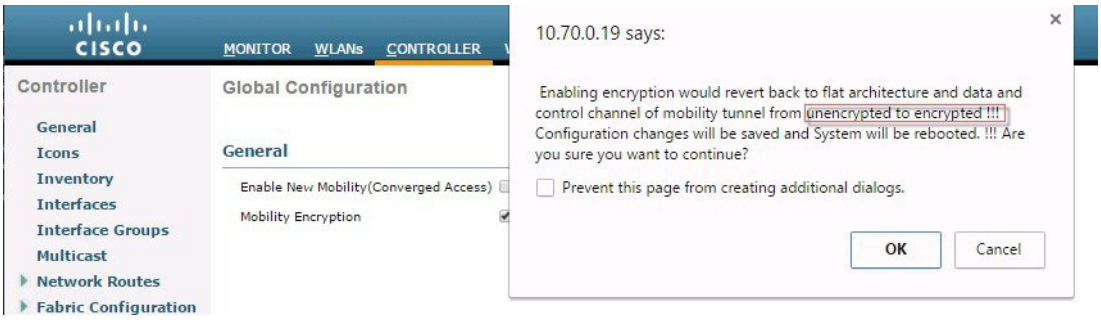
Step 2 Enable Mobility Encryption on each controller.
After enabling Mobility Encryption, the controller will reboot.


```
(Cisco Controller) >config mobility encryption ?

enable          Enables the encryption feature.

disable         Disables the encryption feature.
```

Step 3 Before rebooting, the controller will display the following message, hit OK and then Apply the change.



Step 4 After controllers that were configured with Encrypted Mobility Tunnel come up they will show with Status Up.

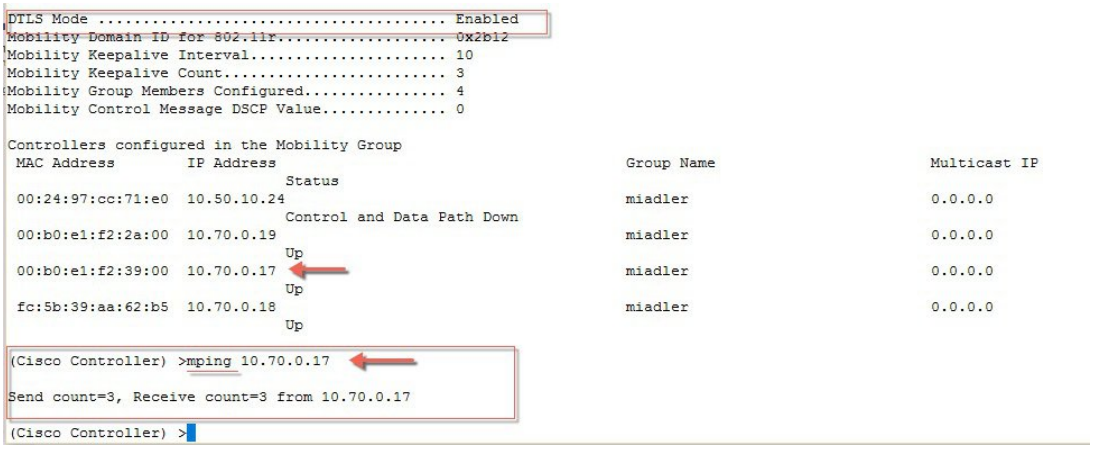
Figure 1:

```
(Cisco Controller) >show mobility summary

Mobility Protocol Port.......................... 16666
Default Mobility Domain......................... miadler
Multicast Mode ................................. Disabled
DTLS Mode ...................................... Enabled
Mobility Domain ID for 802.11r.................. 0x2b12
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Members Configured............... 4
Mobility Control Message DSCP Value............. 0

Controllers configured in the Mobility Group
 MAC Address       IP Address                                Group Name                     Multicast IP
                                 Status
 00:24:97:cc:71:e0 10.50.10.24                               miadler                        0.0.0.0
                                 Control and Data Path Down
 00:b0:e1:f2:2a:00 10.70.0.19                                miadler                        0.0.0.0
                                 Up
 00:b0:e1:f2:39:00 10.70.0.17                                miadler                        0.0.0.0
                                 Up
 fc:5b:39:aa:62:b5 10.70.0.18                                miadler                        0.0.0.0
                                 Up
```

Step 5 After the Mobility Encryption is enabled and Tunnel Link status shows as UP, one more check can be done to verify the encrypted connection is established. Perform MPING from one Controller to another Controller IP address over the Encrypted Tunnel and make sure MPING is successful.


DTLS Mode ..... Enabled
Mobility Domain ID for 802.11r..... 0x2b12
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 4
Mobility Control Message DSCP Value..... 0
Controllers configured in the Mobility Group
MAC Address IP Address Group Name Multicast IP
Status
00:24:97:cc:71:e0 10.50.10.24 miadler 0.0.0.0
Control and Data Path Down
00:b0:e1:f2:2a:00 10.70.0.19 miadler 0.0.0.0
Up
00:b0:e1:f2:39:00 10.70.0.17 miadler 0.0.0.0
Up
fc:5b:39:aa:62:b5 10.70.0.18 miadler 0.0.0.0
Up
(Cisco Controller) >mping 10.70.0.17
Send count=3, Receive count=3 from 10.70.0.17
(Cisco Controller) >

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands