cisco.



Encrypted Tunnel Deployment Guide

Introduction 2

Pre-requisite 2 Product or Feature Overview 2 Configuring Encrypted Mobility Tunnel 3 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.

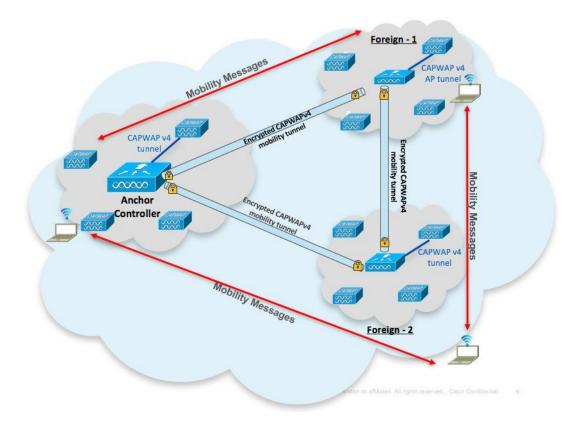


Note This feature is functional only in 8.5MR1 and 8.7 and above releases and is supported on 3504, 5520 and 8540 controllers.

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.

Icons	Local Mobility Group	miadler				
Inventory	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
Interfaces	fc:5b:39:aa:62:b5	10.70.0.18	miadler	0.0.0.0	Up	none
Interface Groups Multicast	00:24:97:cc:71:e0	10.50.10.24	miadler	0.0.0.0	Up	none
Network Routes	00:b0:e1:f2:2a:00	10.70.0.19	miadler	0.0.0.0	Up	none
Fabric Configuration	00:b0:e1:f2:39:00	10.70.0.17	miadler	0.0.0.0	Up	none
Redundancy	fc:5b:39:aa:62:b5	2001::10:70:18	miadler	11	Up	none
Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging						

<ip< th=""><th>addr></th><th>Member</th><th>switch</th><th>IP</th><th>address</th><th></th></ip<>	addr>	Member	switch	IP	address	
--	-------	--------	--------	----	---------	--

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

cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Controller General Icons Inventory	Global C		ation Converged Access)	_			
Interfaces Interface Groups Multicast Network Routes	Mobility Er		converged Access)	3 4			
Fabric Configuration Redundancy Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config							
Multicast Messaging))config	mobil	itu encrun	tion 2			
			ption feat				
disable Di	sables th	le encr	yption fea	ture.			

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

ululu cisco	MONITOR WLANS CONTROLLER V	10.70.0.19 says:
Controller General Icons Inventory Interfaces Interface Groups	Global Configuration General Enable New Mobility(Converged Access)	Enabling encryption would revert back to flat architecture and data and control channel of mobility tunnel from <u>unencrypted to encrypted !!!</u> Configuration changes will be saved and System will be rebooted. !!! Are you sure you want to continue? Prevent this page from creating additional dialogs.
Multicast Network Routes Fabric Configuration		OK Cancel

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

uluilu cisco	MONITOR WLANS		TY MANAGEMENT CO	MMANDS HELP FEEDBACK		Sa <u>v</u> e Con
Controller	Static Mobility Gro	oup Members				
General Icons	Local Mobility Group	p miadler		8		
Inventory	MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key
Interfaces	fc:5b:39:aa:62:b5	10.70.0.18	miadler	0.0.0.0	Up	none
Interface Groups Multicast	00:24:97:cc:71:e0	10.50.10.24	miadler	0.0.0.0	Up	none
Network Routes	00:b0:e1:f2:2a:00	10.70.0.19	miadler	0.0.0.0	Up	none
Fabric Configuration	00:b0:e1:f2:39:00	10.70.0.17	miadler	0.0.0.0	Up	none
Redundancy	fc:5b:39:aa:62:b5	2001::10:70:18	miadler		Up	none
Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging						

Figure 1:

(Cisco Controller)	>show mobility summary			
Mobility Protocol 1	Port	16666		
Default Mobility Do	main	miadler		
Multicast Mode		Disabled		
DTLS Mode		Enabled		
Mobility Domain ID	for 802.11r	0x2b12		
Mobility Keepalive	Interval	10		
Mobility Keepalive	Count	3		
Mobility Group Memb	ers Configured	4		
Mobility Control Me	ssage DSCP Value	0		
-				
Controllers configu	ared 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 Da	ata Path Down		
00:b0:e1:f2:2a:00	10.70.0.19		miadler	0.0.0.0
	συ			
00:b0:e1:f2:39:00	10.70.0.17		miadler	0.0.0.0
	αU			
fc:5b:39:aa:62:b5	-		miadler	0.0.0.0
	σU			
	25			

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	Ena	bled
Mobility Domain ID	for 802.11r0x2	b12
Mobility Keepalive	Interval 10	
Mobility Keepalive	Count	
Mobility Group Memb	ers Configured 4	
Mobility Control Me	ssage DSCP Value 0	
Controllers configu	red in the Mobility Group	
MAC Address	IP Address	Group Name
	Status	
00:24:97:cc:71:e0	10.50.10.24	miadler
	Control and Data Path	Down
00:b0:e1:f2:2a:00	10.70.0.19	miadler
	Up	
00:b0:e1:f2:39:00	10.70.0.17	miadler
	Up	
fc:5b:39:aa:62:b5	10.70.0.18	miadler
	Up	
(Cisco Controller)	>mping 10.70.0.17	
Send count=3, Recei	ve count=3 from 10.70.0.17	
	-	
(Cisco Controller)	>	

Multicast IP 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 © 2018 Cisco Systems, Inc. All rights reserved.



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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.