使用預共用金鑰配置WPA/WPA2:IOS 15.2JB及更 高版本

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>使用GUI配置</u> <u>使用CLI進行配置</u> <u>驗證</u> <u>疑難排解</u>

簡介

本檔案介紹使用預先共用金鑰(PSK)的無線保護存取(WPA)和WPA2的組態範例。

必要條件

需求

思科建議您瞭解以下主題:

- 熟悉Cisco IOS®軟體的GUI或命令列介面(CLI)
- 熟悉PSK、WPA和WPA2的概念

採用元件

本檔案中的資訊是根據執行Cisco IOS軟體版本15.2JB的Cisco Aironet 1260存取點(AP)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

使用GUI配置

以下過程介紹如何在Cisco IOS軟體GUI中使用PSK配置WPA和WPA2:

1. 為為服務集識別符號(SSID)定義的VLAN設定加密管理器。 導覽至Security > Encryption Manager,確保啟用密碼,然後選擇AES CCMP + TKIP作為兩個SSID使用的密碼。

cisco sont si	THORK ASSOCIATION HIPELESS	provente gravaces gort	must Extra roo		Bage La Papa and Song Lagran (Sec
Security	Workness 141_512_1_4				ish_5982,5_d optime is 1 week, 3 days, 6 hours, 5 nimulae
Encryption Nameper	Security Broughton Manager				
1120 Hanager Terrer Hanager	Set Encryption Mode and Neys for VLAD				Daths: 3488
AP Authoritication	Encryption Modes				
Sofrades Defection Local RADIOS Server	© 16/4				
Advance Security	O wer progeton	Optional m		-	
			Clean Compliant Fit	P Frankreis: E Erabin Message Integrity Chiele (MIC)	
	-			Enables Per Pasket Keying (PPr)	
	Opher	Act cover + them			
	Encryption Neye				
			Transvel Fay	Droryption Key (Neradectine)	Hey Sine
		Droryption Ray 1	0		120.041
		Enorgéen Kay 2	•		420 to 1
		Droryption Ray 3.	0		120.04
		Enorgetion King &	0		420 tot 💌
	Bobel Properties				
	Broadcast Rep Rotation Herval:		O suble Existen		
			County Rotation with Int	avat [0:0.40.00] (10-10000000 avd)	
	with Group Key Update		Enables Group Key Upda	a On Minnbeship Termination	
			Enable Group Key Spile	In On Ministerity Capability Change	
-					Error Form
					Balanty Kilant

2. 使用步驟1中定義的加密引數啟用正確的VLAN。導航到**Security > SSID Manager**,然後從 Current SSID List中選擇SSID。此步驟對於WPA和WPA2配置都是通用的。

curly	Security: Bittel 150 Hereger			
deale Access	650 Properties			the second s
scryption Honoper	Current 558 List			
ID Hanager	· NEW'S	550	inter a second s	
erene Hanager	444	VLAN	Dates Matte	
P Authentication			Roday 1	
rbusies Detection			Burbap 2	
ecal RADIUS Server			Barkey 3.	
desace Security		Etchd Select:	C Band Salari	
		Pliefbie:	Tantat and and and and	
			Kada 1402, 118 King	
		Network C:	(0-4090)	
	00000			
	Datete			

3. 在SSID頁面中,將Key Management設定為**Mandatory**,然後選中**Enable WPA**覈取方塊。從 下拉選單中選擇**WPA**以啟用WPA。輸入WPA預共用金鑰。

Client Authenticated Key Management				
Key Management:	Mandatory .	ССНИ	Enable WPA WPA	
WPA Pre-shared Key.		· ASCII	C Hevadecimal	

4. 從下拉選單中選擇WPA2以啟用WPA2。

Client Authenticated Key Management				
Key Management:	Mandatory 💌	CCHW	Enable WPA WPA2	• <
WPA Pre-shared Key.	=	· ASCII C) Hexadecimal	

使用CLI進行配置

附註:

使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

<u>輸出直譯器工具(</u>僅供<u>已註冊</u>客戶使用)支援某些show命令。使用輸出直譯器工具來檢視 show命令輸出的分析。

此配置與CLI中的配置相同:

```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname ish_1262_1_st
!
1
logging rate-limit console 9
enable secret 5 $1$Iykv$1tUkNYeB6omK41S181TbQ1
!
no aaa new-model
ip cef
ip domain name cisco.com
1
1
!
dot11 syslog
1
dot11 ssid wpa
vlan 6
authentication open
authentication key-management wpa
mbssid guest-mode
wpa-psk ascii 7 060506324F41584B56
1
dot11 ssid wpa2
vlan 7
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 110A1016141D5A5E57
!
bridge irb
1
!
!
interface Dot11Radio0
```

```
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
1
ssid wpa
1
ssid wpa2
1
antenna gain 0
mbssid
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
1
interface Dot11Radio0.6
encapsulation dot10 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
1
interface Dot11Radio0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
1
interface Dot11Radio1
no ip address
no ip route-cache
1
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
1
ssid wpa2
1
antenna gain 0
no dfs band block
mbssid
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
```

```
1
interface Dot11Radio1.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
1
interface Dot11Radio1.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
1
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
1
interface GigabitEthernet0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 spanning-disabled
no bridge-group 6 source-learning
1
interface GigabitEthernet0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 spanning-disabled
no bridge-group 7 source-learning
1
interface BVI1
ip address 10.105.132.172 255.255.255.128
no ip route-cache
1
ip forward-protocol nd
ip http server
ip http secure-server
```

驗證

若要確認組態是否正常運作,請導覽至Association,驗證使用者端是否已連線:

wity Time out	Rostname ish_1282_1_st				ish_t	82_1_st uptime is 1 week	, 3 days, 5 hours, 38 má	
	Association							
	Clertic 1			Intradiusture clientic D				
	West 🗷 Client 🗷 Infrastruc	lure cliend					A	
	Radio8-882, NW ^{2 ADM}							
	\$140 wpe :							
	Device Type	Name	IF Address	MAC Address	State	Parent	VLAR	
	cos-diett.	84,1292,1,8	64.103.236.67	2877.0304.0x40	Associated	orest .	4	
	Radio1-882.118 ^{0 Linu}							

您也可以在CLI中使用此系統日誌消息驗證客戶端關聯:

*Mar 11 05:39:11.962: %DOT11-6-ASSOC: Interface Dot11Radio0, Station ish_1262_1_st 2477.0334.0c40 Associated KEY_MGMT[WPAv2 PSK]

疑難排解

附註:使用 debug 指令之前,請先參閱 有關 Debug 指令的重要資訊。

使用以下debug命令可對連線問題進行疑難排解:

- debug dot11 aaa manager keys 此調試顯示AP和客戶端之間的握手,作為成對臨時金鑰 (PTK)和組臨時金鑰(GTK)協商。
- debug dot11 aaa authenticator state-machine 此調試顯示客戶端在關聯和身份驗證時經歷的 各種協商狀態。狀態名稱表示這些狀態。
- debug dot11 aaa authenticator process 此調試可幫助您診斷協商通訊的問題。詳細資訊顯 示協商中的每個參與者傳送的內容,並顯示另一個參與者的響應。您還可以將此調試與debug radius authentication命令結合使用。
- debug dot11 station connection failure 此調試可幫助您確定客戶端連線是否失敗,並幫助您 確定失敗的原因。