自治接入點上的WEP配置示例

目錄

簡介

本檔案介紹如何在思科自主存取點(AP)上使用和設定有線等效保密(WEP)。

必要條件

需求

本檔案假設您可以建立與WLAN裝置的管理連線,且裝置在未加密環境中正常運作。要配置標準 40位WEP,您必須有兩個或多個無線電單元相互通訊。

採用元件

本檔案中的資訊是根據執行Cisco IOS[®]版本15.2JB的1140 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。

背景資訊

WEP是802.11(Wi-Fi)標準中內建的加密演算法。WEP使用<u>串流密碼</u> <u>RC4</u> 作為機密性,並使用 <u>循環冗餘檢查–32</u> (CRC-32)校驗和<u>integrity</u> 。

標準64位WEP使用<u>40位</u>金鑰(也稱為WEP-40),該金鑰與<u>24位</u><u>初始化向量</u>(<u>IV</u>)<u>串聯</u> <u>,以便形成</u><u>RC4</u>金<u>鑰。</u>64位WEP金鑰通常以包含10個十六進位制(以16為基數)字元(0到 9和A-F)的字串形式輸入。每個字元代表四位,四位的10位代表每位40位;如果新增24位IV,則會 生成完整的64位WEP金鑰。 128位WEP金鑰通常作為包含26個十六進位制字元的字串輸入。26位(每位4位)等於104位;如果 新增24位IV,則會生成完整的128位WEP金鑰。大多數裝置允許使用者以13個ASCII字元輸入金鑰 。

驗證方法

WEP可以使用兩種身份驗證方法:開放系統身份驗證和共用金鑰身份驗證。

使用開放系統驗證時,WLAN客戶端無需向AP提供憑證以進行驗證。任何客戶端都可以通過AP進行 身份驗證,然後嘗試關聯。實際上,不進行身份驗證。隨後,可以使用WEP金鑰加密資料幀。此時 ,客戶端必須具有正確的金鑰。

使用共用金鑰身份驗證時,WEP金鑰用於四步質詢 — 響應握手:

- 1. 客戶端向AP傳送身份驗證請求。
- 2. AP以明文<u>質詢回</u> 覆。
- 3. 客戶端使用配置的WEP金鑰加密質詢文本,並以另一個身份驗證請求進行響應。
- 4. AP解密響應。如果響應與challenge-text匹配,則AP會傳送肯定應答。

驗證與關聯後,也使用預先共用的WEP金鑰對RC4的資料訊框進行加密。

乍一看,共用金鑰身份驗證似乎比開放系統身份驗證更安全,因為後者不提供真正的身份驗證。然 而,情況正好相反。如果在共用金鑰身份驗證中捕獲質詢幀,則可以匯出用於握手的金鑰流。因此 ,建議對WEP身份驗證使用開放系統身份驗證,而不是共用金鑰身份驗證。

臨時金鑰完整性協定(TKIP)的建立是為了解決這些WEP問題。與WEP類似,TKIP使用RC4加密。 但是,TKIP通過新增諸如每資料包金鑰雜湊、消息完整性檢查(MIC)和廣播金鑰輪替等措施來增強 WEP,以便解決已知的WEP漏洞。TKIP使用RC4流密碼和128位金鑰進行加密,64位金鑰進行身份 驗證。

設定

本節提供WEP的GUI和CLI配置。

GUI配置

完成這些步驟,以便使用GUI配置WEP。

- 1. 通過GUI連線到AP。
- 2. 從視窗左側的Security選單中,為要配置靜態WEP金鑰的無線電介面選擇Encryption Manager。
- 3. 在Encryption Modes下,按一下WEP Encryption,然後從客戶端的下拉選單中選擇 Mandatory。

工作站使用的加密模式為:

- 預設(無加密) 要求客戶端在不進行任何資料加密的情況下與AP通訊。不建議使用 此設定。
- 可選 允許客戶端使用或不使用資料加密與AP通訊。通常,當您有無法建立WEP連線

的客戶端裝置(例如128位WEP環境中的非思科客戶端)時,會使用此選項。

- 強制(完全加密) 要求客戶端在與AP通訊時使用資料加密。不使用資料加密的客戶 端不允許通訊。如果您希望最大限度地提高WLAN的安全性,建議使用此選項。
- 4. 在Encryption Keys下,選擇Transmit Key單選按鈕,然後輸入10位十六進位制金鑰。確保金 鑰大小設定為40位。

為40位WEP金鑰輸入10個十六進位制數字,為128位WEP金鑰輸入26個十六進位制數字。金 鑰可以是以下數字的任意組合:

- 0到9
- a到f
- A到F

ı. cısco	Ном	E DETWORK ASSOCIATION	WPELESS SECURITY	SERVICES SOFTWARE EVENTLO	0	Sage Configuration Bing Logout B
Security	ſ	RADIO8-802.11N ^{2.6}	ax 📔	RADIO1-882 11N ^{50HZ}		
Admin Access Incryption Manager SSID Manager Server Manager		Hostname ap				ap uptime is 3 hours, 41 minutes
		Security: Encryption Manager	- Radio0-802.11N ^{2.4GHz}			
		Encryption Nodes				
AP Authentication		© None				
Intrusion Detection Local RADIUS Server		· WEP Encryption	Mandalary *			
Advance Security				Cisco Compliant TKIP Feature	Enable Message Integrity Check (MIC)	
		Cipher	WEP 128 bit	•	Enable Per Pacest Keying (PPK)	
		Encryption Keys				
				Transmit Key	Encryption Key (Hexadecima)	Key Size
			Encryption Key 1:	•	*******	40 bit -
			Encryption Key 2:	0		128 bit -
			Encryption Key 3:	0		120 bit -
			Encryption Key 4:	0		128 bè -

5. 按一下Apply-All以在兩個無線電上應用配置。

Global Properties	Global Properties					
Broadcast Key Rotation Interval:	Disable Rotation					
	C Enable Rotation with Interval DISABLED (10-10000000 sec)					
WPA Group Key Update:	Enable Group Key Update On Membership Termination					
	Enable Group Key Update On Member's Capability Change					
	Apply-Radia0 Apply-All Car					

6. 使用Open Authentication建立服務集識別符號(SSID),然後按一下Apply以在兩個無線電上啟 用它。

 Interface Interface			슈 코 C OF Totoo	₽ ♦ 🕇
cisco	HOME NETWORK ASSOCIATION WIPELESS SECURITY	SERVICES SOFTWARE EVENTLOG		Sage Configuration Eng Logout E
Security Admin Access Encryption Manager	Hostname ap			ap uptime is 3 hours, 45 minutes
	Security: Global SSID Nanager			
	SSID Properties			
Server Manager	Current SSID List			
AP Authentication	< NEW > *	SSD:	wep-config	
Local RADIUS Server		VLANE	< NONE > Define VLANs Reckup 1:	
Advance Security	-		Backap 2	
		Band Calent	Backap 3	
		bind-oewet.	Band Select End Select End Select Added A	
			Radio0-302.11N ⁻¹⁴⁴	
		Network ID:	(0-4096)	
	Debits			
	Client Authentication Settings			
	Nethods Accepted:			
	Open Authentication:	< NO ADDITION> +		
	Shared Authentication:	< NO ADDITION> *		

2101-	
Radio0-802.11N ^{2.1040}	
Set Beacon Mode:	Single BSSD Set Single Goest Mode SSD wap-config •
	C Multiple BSSD
Set Infrastructure SSID:	< NONE > Force infrastructure Devices to associate only to this SSID
Radio1-802.11N ⁻⁰⁴⁴ :	
Set Beacce Mode:	Single BSSID Set Single Guest Mode SSID: wep-config •
	C Multiple BSSID
Set Infrastructure SSID:	< NONE > • E Force infrastructure Devices to associate only to this SSID

7. 導航到網路,然後啟用2.4 GHz和5 GHz的無線電話,以便使其運行。

CLI組態

使用本節內容,以便使用CLI設定WEP。

<#root>

ap#

show run

Building configuration...

```
Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```
hostname ap
1
I
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
1
no aaa new-model
ip cef
!
1
dot11 syslog
1
  dot11 ssid wep-config
  authentication open
  guest-mode
1
!
crypto pki token default removal timeout 0
1
1
username Cisco password 7 0802455D0A16
Т
1
bridge irb
I
1
interface Dot11Radio0
no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 I
 ssid wep-config
 1
 antenna gain 0
 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
I
interface Dot11Radio1
 no ip address
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 1
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 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
ï
interface GigabitEthernet0
no ip address
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface BVI1
ip address dhcp
ï
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
1
bridge 1 route ip
!
!
Т
line con 0
line vty 0 4
login local
transport input all
!
end
```

驗證

輸入以下命令可確認您的組態是否正常運作:

<#root>

ap#

show dot11 associations

802.11 Client S	Stations on Dot1	1Radio0:			
SSID [wep-confi	ig] :				
MAC Address	IP address	Device	Name	Parent	State
1cb0.94a2.f64c	10.106.127.251	unknown	-	self	Assoc

疑難排解

使用本節內容,對組態進行疑難排解。

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

以下debug命令可用於對組態進行疑難排解:

- debug dot11 events 為所有dot1x事件啟用調試。
- debug dot11 packets 為所有dot1x資料包啟用調試。

以下範例顯示使用者端成功與WLAN建立關聯時的記錄日誌:

*Mar 1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station 1cb0.94a2.f64c Associated KEY_MGMT[NONE]

使用者端輸入錯誤金鑰時,系統會顯示以下錯誤:

*Mar 1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c *Mar 1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating Station 1cb0.94a2.f64c Reason: Sending station has left the BSS *Mar 1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。