ACS 5.2版和WLC的每WLAN身份验证配置示例

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 配置 WLC 配置 Cisco Secure ACS 验证 故障排除

简介

本文档提供一个配置示例,根据服务集标识符(SSID)限制每个用户对无线LAN(WLAN)的访问。

先决条件

要求

Cisco 建议您了解以下主题:

- 如何针对基本运行来配置无线 LAN 控制器 (WLC) 和轻量接入点 (LAP)
- 如何配置思科安全访问控制服务器(ACS)
- •轻量接入点协议 (LWAPP) 和无线安全方法

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件版本7.4.110的Cisco 5500系列WLC
- Cisco 1142 系列 LAP
- •思科安全ACS服务器版本5.2.0.26.11

配置

为了针对此设置配置设备,您需要:

- 1. 需要为 WLC 配置两个 WLAN 和 RADIUS 服务器。
- 2. 配置 Cisco Secure ACS。
- 3. 配置无线客户端并检验配置。

配置 WLC

要配置 WLC 使用该设置,请完成以下步骤:

 1. 配置WLC以将用户凭证转发到外部RADIUS服务器。外部 RADIUS 服务器(在这种情况下是 Cisco Secure ACS)然后验证用户凭证并提供对无线客户端的访问权限。请完成以下步骤: 从控制器GUI中选择Security > RADIUS Authentication以显示"RADIUS身份验证服务器"页。

cisco	MONITOR WLANS CONTROLLER AGRELESS SECLETY NOVADERENT CONVANCE HELE EBEDRACK
Security	RADIUS Authentication Servers Rem
AAA General Ex0005 Ex005 Ex005	Cell Statum 15 Type 7 IF Address IF Une AllE Rey Wark IF (Designed for FPS customers and requires a key area tractartRADILS server) Rod Designed IF (Rey et and the server address Fort Pher Address Port Pher Address Network line - Nanagement Server address Fort Pher Address Port Pher Address 2. Cell Status 25 Type ad as applicable any to non 200-11 muterful Status
E Local EAP	
Priority Order	
▶ Certificate	
Access Control Lists	
+ Wireless Protection Policies	
Web Auth	
TrestSec SXP	
Advanced	

单击 New 以定义 RADIUS 服务器参数。 这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。网络用户和管理复选框确定基于RADIUS的身份验证是否适用于管理和网络用户。此示例使用Cisco Secure ACS作为IP地址为10.104.208.56的 RADIUS服务器。

cisco	MONITOR WLAN	CONTROLLER	W(RELESS	GECLETY	ивлавенелт	CONVANCE	HE,F	ESEMACK
Security	RADIUS Auther	ntication Serve	rs > New					
General	Server Index (Pr	ion Ry)	1 .					
Kappus Authantication Accounting	Starver 3P Addres Shared Secret Fo	s mat	4903	5				
* TAGROS+ LDAP	Shared Secret Confirm Shared 3	Secret	*******					
Local Net Divers MAC Differing Disabled Clients	Kay Wrap	,	Casgradia	TRA areas		key arep total	A-9 820	II Convert)
Hear Liven Evinaer Am Palicies Paremant Enimae	Pert Bamber Server Status		lolz Teshari 🛥					
E Local EAP	Support for RFC	25.76	backed in					
 Priority Order Certificate 	Server Tropolit Notwork User		Z Enable	e				
Access Control Lists Wireless Protection	Planagement		E Grable E - Insbie					
Policies • Web Auth								
TrustSec SXP Advanced								

单击 Apply。

2. 完成以下步骤,为具有SSID Employee的员工配置一个WLAN,为具有SSID Contractor的承包商配置一个WLAN,为另一个WLAN配置SSID Contractor。要创建 WLAN,请从控制器 GUI 中单击 WLANs。随即显示 WLAN 窗口。该窗口列出了控制器中配置的 WLAN。要配置新的 WLAN,请单击 New。此示例创建名为Employee的WLAN,WLAN ID为1。单击"应用"。

cisco	MONITOR MLANE CONTR	OLLER AGRELESS SECURTY	NAVAGENENT ODMVAN	са неца ресовчок	Sage Configuration ging 1	agaut Bafrash
WLANs	WLANs > New				< Batik	Apply
 WULANS WULUE ▶ Advanced 	Type Profile Name SSID BD	eLM				

选择"WLAN**">"编辑**"窗口并定义特定于WLAN的参数: 从Layer 2 Security选项卡中,选**择** 802.1x。默认情况下,Layer 2 Security 选项为 802.1x。这为WLAN启用802.1 x/可扩展身份验 证协议(EAP)身份验证。

cisco	NOVITOR WILANE CONTROLLER WIRELESS SECURITY NEVABENE'S CONTAINS HELE ESSENACY	Saga Configuration Drip Liquid Battach
WLANs	WLANs > Edit 'Employee'	< Back Apply
WLANS MLANS	General Security QaS Advanced	
➤ Advanced	Loyer 2 Loyer 3 AAA Sorvers	
	Lagar 2 Security * What we ap	Î
	Paul Transform Paul transform Protoc ted Pranagement Pranage	
	INP Usellel +	z
	WPA I WPA2 Parameters	
	WP4 Policy WP42 Policy WP42 Policy WP42 Environ WF45 Environ	
	Authentication Key Nanagement	
	002.04 M Instea CCCM Engle	
	PSK El Insta xn	
	Post Notes 2 Web Poles secret is used in combostics with Plant	

从AAA服务器选项卡,从RADIUS服务器下的下拉列表中选择适当的RADIUS服务器。可以根据 WLAN 网络的需要修改其他参数。单击 **Apply**。

Ns	WLANs > Edit 'Employee'		< Back Apply
UNS UANS UNIS	WLANS > Edit "Employee" General Security QuS Layer 2 Layer 3 AA8 Se Select AA8 servers below to over Robus Servers Anti- Server 1 Stror 2 Server 3 Server 5	Advanced Trees Tre	< Back Apply
	Radius Server Accounting Jiteelm Update Lucal EAP Authentication	10 T	

同样,要为承包商创建WLAN,请重复步骤b到d。

配置 Cisco Secure ACS

在 Cisco Secure ACS 服务器上,您需要:

- 1. 配置 WLC 作为 AAA 客户端。
- 2. 为基于SSID的身份验证创建用户数据库(凭证)。
- 3. 启用 EAP 认证。

在 Cisco Secure ACS 上完成以下步骤:

- 1. 要将控制器定义为ACS服务器上的AAA客户端,请从ACS GUI中选择**Network Resources > Network Devices and AAA Clients**。在Network Devices and AAA Clients下,单**击Create**。
- 2. 当Network Configuration页面显示时,定义WLC的名称、IP地址和共享密钥和身份验证方法 (RADIUS)。

second a lot of a				State of the local division of the local div			
🧲 🕞 🌀 Large / 20.284.200.56/14121	nin/ 💭 + 🔾 Cettic., 🗄	d 🗙 👩 Clico Securi ACS	×		-		A 🖈 🖾
🗙 🥃 Shara Browner WebEc 🔹							
cisco Secure Al	CS				acadmin	acalomyblic (Princey)	Log Cut. About 1940
» ∰ MyWorkspace	Network Resources > Network	Devices and AAA Clients > Create					
Volteck Resources Notech Device Groups Locaton Device Trap Device Trap	Name: D074 Description: Network Device Group Location Device Type P Address Single IP Addres B IP: 10.105.98.4	e Ali Lotatore Al Deice Types s	(Benet) (Benet)	Authentication Options + TACACS+ Shared Secret Single Connect Device B Legaxy MCACS+ Single + RADUS Shared Secret CoApet 1780 Erable KeyWap	e Connect Suppor	t.	
				Hay Encryption Rey:			
	Submit Cancel						

3. 从ACS **GUI中选择Users and Identity Stores > Identity Groups。**为"员工"(Employee)和"承包 商"(Contractor)创建各自的组,然后单**击"创建**"。在本例中,创建的组命名为Employees。

	D + O Cattle, B d X	PERSONAL PROPERTY AND	- Annual -	
X Share Browner WebEc +				
cisco Secure Al cisco Eval(Days with 5)	CS		anadeir	acationsplate (Primary) Log Out About Help
» G MyWorkspace	Users and kiertity Stone > Keniky Groups > Grade			
Policy Resources Poli	General Nama: Employees Description: Parent Al Sroups D = Required fields	(Serect)		
Poicy Elements Concess Policies Monitoring and Reports Signifem Administration	Submit Cance			

4. 选择用户和身份库>内部身份库。单击Create并输入用户名。将其放在正确的组中,定义其密

码,然后单击**提交**。在本示例中,创建了组Employee中名为employee1的用户。同样,在组 承包商下创建名为contractor1的用户。



5. 选择策略元素>网络条件>终端站过滤器。Click Create.



输入有意义的名称,在"IP地**址"选**项卡下输入WLC的IP地址。在本例中,名称为Employee和 Contractor。

X Shere Browser WebEr •	HY D×O Cette. ⊇ C X Science Secure ACS ×		i a artic
Cisco Secure Al cisco Eval(Days MIL 5)	CS	acandesite acatomybala (Princary) Log Cut Abo	of 1980
» ∰ MyWorkspace	Policy Bernerts > Session Conditions > Network Conditions > End Station Pitters > Creats		
Polivork Resources Solutions Go Policy Exercise Go Policy Exercise Section Conditions Date and Time	General Name: Employee Description: Address IAPC Address CLIONIS		
Custom * Nation: Conditions Conditions Conditions Device Plate Device Plate Device Plate * Automation and Parmissions * Automation and	Network Devices Filter: End Station P • Match & Contains • Chear Filter: Do * End Station P 10.105.98.4	Showing 1-1 of 1 50 👻 yer page 🖓	
Autorization Profiles Device Administration Named Permission Objects To Access Policies	Create, Dupitate Est Deete Exposts File Replace from File	Page 1 of1 4 4 P P	-
 Idenitoring and Reports System Administration 			
	Suomit Carce		

在CLI/DNIS选项卡下,将CLI保留为 — ANY-,并输入DNIS作为*<SSID>。在本示例中 ,DNIS字段输入为*Employee,因为此终端站过滤器仅用于限制对员工WLAN的访问。DNIS 属性定义了允许用户访问的 SSID。WLC 将 DNIS 属性中的 SSID 发送到 RADIUS 服务器。 对承包商终端站过滤器重复相同步骤。

A ST P & South Part	And a second sec	
C 100, 18 4 200, 58 / scrat	anin/ D + O Cettle E d X / Circo Stours AC5 X	
× Shara Browner WebEc -		
Julia Lisco Secure A	ACS	econolmin acationsphere (Primary) Log Cut About Help
CISCO EVAL(Days left: 5)		
»	Policy Bernetia > Session Conditions > Network Conditions > Ted Station Places > Bdt "Braj	iave Dd Sin Piler'
> (3) Nelwork Resources		
+ 2 Users and Identity Stores	General	
- Ry Paties Demanda	Frame: Engloyee Engloyee	
* Session Conditions	Description:	
Date and Time	IP Address INPC Address CLITINIS	e] Cisco Secure ACS Webpage Dialog
Custom	Network Devices	🙆 https://33.534.200.56/horsedexin/project/inservent/Actp.jpp. 🔘 Cartificate error
End Station Filters	Filer, CLI + Match #, Contains +	CHUTTHE DO
Device Filters		
Device Port Filters	2 CLI DNB	DNB: W "Employee
* Network Access	ANY- Employee	
Authorization Profiles	Create Dupicate Edit Delete Eporto Fie	Replace from File
 Device Administration 		
Kamed Permission Objects		
· Carlotte Policies		OK Dose Hep
In The Monitoring and Happins		
 System Administration 		
	Submit Carcel	

A REAL PROPERTY AND ADDRESS OF TAXABLE		· ····································	
Caller Competition 38 4 2001 58 / second	nn/ D + O Cettic. E d X Cisco Securi ACS ×		
X Gara Browser WebE: -			
cisco Secure A	CS	acaudmin acalumptels (Prin a	ny) Lag Clat About Help
» ∰ MyWorkspace	Policy Bernetia > Session Conditions > Network Conditions > End Station Place > Edd 7	Contractor Brid Sin Piller"	
Nateori, Resources Solutions Desire and Identity Stores Solutions Debt and Time Custom Nateori, Canations Desire Anno Solution and Parmissions Nateori, Access Authorization and Parmission Nateori, Access Authorization Profiles Desire Administration Named Parmission Objects Solutions Mander Parmission Named Parmission Objects Solutions Maniform and Reports Solution Administration	Sumet, Cance	Char File Replace from File Ck Class	Cartificate array

6. 选择**策略元素>授权和权限>网络访问>授权配置文件**。应该有允许访问的默认配置文件。

C (0) (0) (0) (0) (0) (0) (0) (0) (0) (0)	min/ D × O Cetter, E C X Circo Secure ACS ×			6 2 3
🗙 🍚 Shara Browser WebEc 🔹				
Cisco Secure A Cisco EvAL(Days left: 5)	CS	acastein	acaliemplaie (Primary)	Log Out About Help
» ∯ My/Workspace	Policy Bernetia > Authorization and Permissions > Table on Accessa > Authorization Profiles			
* (59 Nelwork Resources	Authorization Profiles		Stowing 1-1 of 1 5	0 • perpaga 30
B Users and Identity Stores	Filter: • Nelsh #: • 00 *			
Excelos Constants	Name - Description			
Date and Time	E Parmit Access			
Custom v Natwork Candilians				
End Station Filture				
Device Fitters Device Port Fitters				
* Authorization and Permissions				
* Network Access Autorization Profess				
 Device Administration 				
Named Hermission Objects				
Monitering and Reports				
» 🍇 Bystem Administration				
	Create Duplicate Edit Delate		H e Paga	1 of 1 b bi

7. 选择访问策略>访问服务>服务选择规则。单击"Customize(自定义)"。添加任何合适的条件。 本示例使用协议作为Radius作为匹配条件。Click Create.命名规则。选择协议并选择Radius。 在结果下,选择适当的访问服务。在本例中,它保留为"默认网络访问"。

		×
遵 https://10.104.208.56/acsadm	in/PolicyInputAction.do	😵 Certificate error
Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Selected: Protocol	
OK Cancel		

Cisco Secure ACS Webpage Dia	ilog	×
😂 https://10.104.208.56/acsadmin/P	olicyInputAction.do	😒 Certificate error
General		
Name: Rule-4	Status: Enabled 💌 🖲	
The Customize butto conditions and resu	on in the lower right area of Its are available here for us	the policy rules screen controls which policy e in policy rules.
Conditions		
Protocol: match	- Radius	Select
Service: Default Network Acces	9 ▼	
OK Cancel		Help

8. 选择Access Policies > Access Services > Default Network Access > Identity。选择Single Result Selection和Identity Source作为内部用户。

		and the second second second second			1
(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	min/ D + O Centric. E C × Clicco Secure AC	5 ×			6 2 8
× Shara Browner WebEc -					
					and the second second second
ululu Cisco Secure A	CS		aca admin	acatemplate (Primary)	Log Out About Help
CISCO EVAL(Days left: 5)					
* @ MyWorkspace	Access Rolden > Access Services > Default Network Acces	us > Kerky			
> (b) Nelwork Resources	Single result selection	lection			
Users and Identity Stores	Identity Source: Internal Users	(Select.)			
> Q> PolicyElements					
- 🐍 Access Policies	 Advanced Options 				
* Access Services					
1 Service Selection Rules					
identiv					
Authorization					
O Debuit Network Access					
Authorization					
 Monitoring and Reports 					
» 💐 System Administration					
	Save Changes Discard Changes				

选择**访问策略>访问服务>默认网络访问>授权。单**击**自定义**并添加自定义条件。本示例按此顺 序使用身份组、NDG:设备类型和终端站过滤器。

🧃 Webpage Dialog		X
😂 https://10.104.208.56/acsadmin/	PolicyInputAction.do	😮 Certificate error
Customize Conditions Available: ACS Host Name Authentication Method Authentication Status Compound Condition Device Filter Device IP Address Device Port Filter Eap Authentication Method Eap Tunnel Building Method NDG:Location	Selector. Identity Group NDG:Device Type End Station Filter	
OK Cancel		٥

Click Create.将规则命名并在All Groups下选择相应的身份组。在本例中为Employee。

P Goo secure ALS Wetpage balog	E Coo seure ALS metalage bang
🖉 https://10.114.200.16/accuderies/Palicylepathetism.do 📀 Carificate area	🍘 https://10.114.200, 🖬 / scradinin, Nichwork Davies Groups (Frystall-tion de Prontest Data, externa Fritanz Identity Group-Standbylin 💿 🛛
General Name: Rute 2 Datus: Enabled + @	Patur: • Malch II • 💿 🔻
The Custerrize butten in the lower right area of the policy rakes screen controls which policy conditions and results are available here for use in policy rakes.	Name Description All Description Contractor Contractor
Conditions	Instant
R Idently Group: In	MLC .
R NDO.Devke Type. In	
C End Station Filter: math *	AL) Flow Service AFS Wittenays Rodes
Results	Persyndy TE TELETER W/w net miny for word for a straight Persyndant wat an a straight for a straight for a straight Person Pe
You may refect multiple suffertiation profiles. Affilutes addining in multiple profiles will use the wave from the first profile defined.	
	(ME) (ME)

单击**Employee End Stn Filter**单选按钮,或在"Configure the WLC"部分输入您在步骤1b中输入 的名称。

🗿 Cisco S	Secure ACS Webpage Dia	og	×
🧉 https:	//10.104.208.56/acsadmin/N	ARsLPInputAction.do?listType=EndStation	😣 Certificate error
End St	ation Filters	Showing 1-2 of 2	50 🝷 per page 🙆
Filter:	 Match if: 	- Go -	
	Name 🔺	Description	
0	Contractor End Stn Filter		
۲	Employee End Stn Filter		
Creat	te Duplicate Edit	Delete II Page	a 1 of 1 🕨 利
OK C	ancel		Help

选中允**许访问**复选框。

4	Cisco	Secure ACS W	ebpage Dialog				 -				x
	🥝 http	s://10.104.208.56/	acsadmin/Netw	orkAccessLPIn					۲	Certificate	e error
	Auth	orization Profiles					Showing 1-2	of 2 50) -	per page	Go
	Filte	с 📃 🖣	Match if:		- Go -	~					
		Name 🔺	Description								
	2	DehyAccess									
	P	Permit Access)							
	Cre	ate Duplicate	Edit De	ete				Page	1	of 1 🕨	M
	OK	Cancel								н	leip

对"承包商规则"(Contractor Rules)也重复上述步骤。确保默认操作为拒**绝访问**。 完成步骤e后

,规则应如下所示

Isco Eval(Days left 5)	ACS							ecastein	acatomplate (Primary)	Leg Out About
St My/Workspace	Att	een Polici	n > Acco	n Sevten e D	intend Vieter ark Access > Auth	orization				
(b) Network Resources	5	andard P	olicy End	eption Policy						
Users and identity Stores	- 18	letwork./	Access A	uthorization P	olicy					
Qv PolicyElements	-	iter St	atuo		Match it Equals •	Glear Fi	ter 😡 🖛			
Access Services	1		Status	Name	Identity Group	Conditions NDG:Dexice Type	End Station Filter	Results Authorization Photies	HECOVE	
O Debut/Devel Autority Authorization O Debut/Network Access Identity Subcrastice			•	Englose	in All Groups Employee	in All Device Types WLC	match Contractor End Stri Filter	Pernit Access	5	
 Monitoring and Reports System Administration 	L									
	н		Detaut		Eno tules defined at no e	mabled rule matches.		DenyAccess		

配置到此结束。在本部分之后,需要为客户端相应地配置SSID和安全参数,以便连接。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。