使用LAP配置ACS 5.2进行基于端口的身份验证

目录

简介 <u>先决条件</u> 要求 使用的组件 <u>规则</u> 背景信息 配置 <u>网络图</u> 假设 配置步骤 配置LAP 配置交换机 配置RADIUS服务器 配置网络资源 配置用户 定义策略元素 应用访问策略 验证 <u>故障排除</u> 相关信息

简介

本文档介绍如何将轻量接入点(LAP)配置为802.1x请求方,以便根据RADIUS服务器(例如访问控制服务器(ACS)5.2)进行身份验证。

先决条件

要求

尝试进行此配置之前,请确保满足以下要求:

- 了解无线LAN控制器(WLC)和LAP的基本知识。
- 了解 AAA 服务器的功能.
- 全面了解无线网络和无线安全问题.

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 7.0.220.0 的 Cisco 5508 WLC
- Cisco 3502 系列 LAP
- 运行 5.2 版的 Cisco 安全 ACS
- Cisco 3560 系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

背景信息

LAP在工厂安装了X.509证书(由私钥签名),这些证书在制造时烧录到设备中。LAP使用此证书以 在加入过程中向WLC进行身份验证。此方法描述另一种验证LAP的方法。使用WLC软件,您可以在 Cisco Aironet接入点(AP)和Cisco交换机之间配置802.1x身份验证。在此实例中,AP充当802.1x请 求方,并由交换机针对使用带匿名PAC调配的EAP-FAST的RADIUS服务器(ACS)进行身份验证。一 旦配置为802.1x身份验证,交换机将不允许除802.1x流量外的任何流量通过端口,直到连接到端口 的设备成功进行身份验证。AP可以在加入WLC之前或加入WLC之后进行身份验证,在这种情况下 ,您可以在LAP加入WLC之后在交换机上配置802.1x。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置:



下面是此图中使用的组件的配置详细信息:

- ACS (RADIUS) 服务器的 IP 地址为 192.168.150.24。
- WLC的管理和AP管理器接口地址为192.168.75.44。
- DHCP服务器地址为192.168.150.25。
- LAP位于VLAN 253中。
- VLAN 253:192.168.153.x/24。网关:192.168.153.10
- VLAN 75:192.168.75.x/24。网关:192.168.75.1

假设

• 所有第3层VLAN都配置了交换机。

- 为DHCP服务器分配了一个DHCP作用域。
- 网络中的所有设备之间都存在第3层连接。
- LAP已连接到WLC。
- 每个VLAN都有一个/24掩码。
- ACS 5.2已安装自签名证书。

配置步骤

此配置分为三类:

- 1. <u>配置LAP。</u>
- 2. <u>配置交换机。</u>
- 3. <u>配置 RADIUS 服务器</u>。

配置LAP

假设:

LAP已使用选项43、DNS或静态配置的WLC管理接口IP注册到WLC。

请完成以下步骤:

1. 转到Wireless > Access Points > All APs以验证WLC上的LAP注册。

alala												Bris I L	igout Befreak
CISCO	MONITOR	MLANS	CONTROLLER	WIRELESS	SECURITY	MANADEMENT	COMMANDS	HELP	REDBACK				
Wireless	All APs											Entrie	n 1 - 1 of 1
 Access Points ALAPS 	Current File	ter		None		[Change	Fitar] [Clear B	iter]					
* H3005 802.11a/n 802.11b/g/h	Number of	APs		1									
Global Configuration											Operational	1	
r nevaloeu	AP Name		AP	Model		AP MAC	AP	Up Time		Admin Status	Status	Port	AP Mode
Mesh	3502e		AD	CAP3502E-A	115	00:07:48:78:53	19 14	42 h 32 e	n 42 s	Enabled	REG	13	Local
HREAP Groups													
▶ 802.11a/n													
▶ 802.11b/g/n													
Hedia Stream													
Country													
Timera													
1.0.5													
1 400													

- 2. 您可以通过两种方式为所有LAP配置802.1x凭证(即用户名/密码):
 - 全局

对于已加入的LAP,您可以全局设置凭证,以便加入WLC的每个LAP都将继承这些凭证 。

ululu cisco	MONETOR WEARS CONT	ROLLER WIRELESS	SECURETY MEMOREMENT	COMMANDS HELP	ETTERNOX	Saya Configuration Bing	Lapout Belie
Wireless	Global Configuration						Apply
CISCO Wireless * Access Points Al APs * Rodos R02.334/h R02.334/h R02.334/h R02.316/h R02.316/h * Advanced Hesh HREAP Groups * 802.116/n * 802.116/n * 802.116/n * 802.116/g * Redia Stream Country Timers * QaS	EDAPTOR YAUNA CON Global Configuration COP State Ethernet Interface# 0 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 3 Redits Sist# 0 1 2 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	ROLLER WINELESS		High Availabilit AP Heartbeat T Local Medie AP I H-REAP Mode A AP Primary Dis Dack-up Prima Back-up Prima Back-up Secon Dack-up Secon	IV Intervel (1-33) Test Heartbeet Timer Stelle # Paul Heartbeet Timer Stelle ry Controller name dary Controller name dary Controller name dary Controller name dary Controller name ast HSS Config Parameters Count Interval	50 50 50 50 50 50 50 50 50 50	<u>Acr</u> 47
	Username Password Confirm Password						
	AP Failover Priority Global AP Pailover Priorit AP Image Pre-downloa	v Disstile 🔹					
	Download Primary Interchange Image	Dewalo	ad Backup				

• 单独

配置每个AP的802.1 x配置文件。在我们的示例中,我们将配置每个AP的凭证。

a. 转至Wireless > All APs,然后选择相关的AP。

b. 在802.1x Supplicant Credentials字段中添加用户名和密码。

cisco	MONITOR MEANS CONTROLLER WEREISS SECURITY	MANAGEMENT COMMUNDS HELP	Sage Configuration Engl Logist Befre PERCHACK
Wireless	All APs > Details for 3502e		< Beck Apply
 Access Points All APs Eddos 802.113/n 002.113/n Advanced Mesh HREAP Groups B02.111n/n B02.111n/n B02.111h/g/n Media Stream Country Timers QoS 	General Credentials Interfaces High Availability Legin Credentials Vermide Gebel credentials Vermide Gebel credentials Vermide Gebel credentials Usernerre Fisco Password Vermide Gebel credentials Vermide Gebel credentials B02.1xt Supplicant Credentials Vermide Gebel credentials Vermide Gebel credentials Vermide Gebel credentials Dvermide Gebel credentials Vermide Gebel credentials Vermide Gebel credentials Vermide Gebel credentials Confirm Password Ference Confirm Password Ference Confirm Password	Inventory Advanced	

注意:登录凭证用于通过Telnet、SSH或控制台登录到AP。

3. 配置High Availability部分,然后单击Apply。

 cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP EEEDBACK	Days Configuration Brig	Logout Beires
Wireless	All APs > Details for 3502e	< Sock	Apply
 Access Points All AFs Rodos S32.114/n S32.114/n Globel Configuration Advanced Mesh HREAP Groups S02.11a/n S02.11a/n S02.11a/n S02.11b/g/n Media Stream Country Timers QoS 	General Credentials Interfaces High Availability Inventory Advanced Name Name Namespaneout 3P Address Primary Cantrollar \$568-3 \$92.368.75.44 Becondary Cantrollar Environment 3P Address Tertiary Cantrollar Environment 3P Address AP Failover Priority Low		

注意:保存后,这些凭证在WLC中保留并重新启动AP。仅当LAP加入新的WLC时,凭证才会 更改。LAP采用在新WLC上配置的用户名和密码。

如果AP尚未加入WLC,则必须通过控制台连接到LAP以设置凭证。在启用模式下发出以下 CLI命令:

LAP#Iwapp ap dot1x username <username> password <password>

或

LAP#capwap ap dot1x username <username> password <password>

注意:此命令仅适用于运行恢复映像的AP。

LAP的默认用户名和密码分别为cisco和Cisco。

配置交换机

交换机充当LAP的身份验证器,并根据RADIUS服务器对LAP进行身份验证。如果交换机没有兼容的 软件,请升级交换机。在交换机CLI中,发出以下命令以在交换机端口上启用802.1x身份验证:

<#root>

switch#

configure terminal

switch(config)#

dot1x system-auth-control

switch(config)#

aaa new-model

!--- Enables 802.1x on the Switch.

switch(config)#

aaa authentication dot1x default group radius

switch(config)#

radius server host 192.168.150.24 key cisco

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#

ip radius source-interface vlan 253

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.

注意:如果同一交换机上有其他AP,并且您不希望它们使用802.1x,您可以保留未为802.1x配置的 端口或发出以下命令:

<#root>

switch(config-if)authentication port-control force-authorized

配置RADIUS服务器

使用EAP-FAST对LAP进行身份验证。如果您未使用Cisco ACS 5.2,请确保您使用的RADIUS服务 器支持此EAP方法。

RADIUS服务器配置分为四个步骤:

- 1. <u>配置网络资源。</u>
- 2. <u>配置用户.</u>
- 3. <u>定义策略元素。</u>
- 4. <u>应用访问策略。</u>

ACS 5.x是基于策略的ACS。换句话说,ACS 5.x使用基于规则的策略模型,而不是4.x版本中使用 的基于组的模型。

ACS 5.x基于规则的策略模型提供比旧的基于组的方法更强大、更灵活的访问控制。 在旧的基于组的模型中,一个组定义策略,因为它包含三种类型的信息并将它们关联在一起:

- 身份信息 此信息可以基于AD或LDAP组中的成员资格或内部ACS用户的静态分配。
- 其他限制或条件 时间限制、设备限制等。
- 权限 VLAN或Cisco IOS®^权限级别。

ACS 5.x策略模型基于以下形式的规则:

如果condition,则结果

例如,我们使用为基于组的模型描述的信息:

如果为identity-condition、restriction-condition,则为authorization-profile。

因此,我们可以灵活地限制允许用户访问网络的条件,以及在满足特定条件时允许的授权级别。

配置网络资源

在本节中,我们将为RADIUS服务器上的交换机配置AAA客户端。

此过程说明如何将交换机添加为RADIUS服务器上的AAA客户端,以便交换机可以将LAP的用户凭 证传递到RADIUS服务器。

请完成以下步骤:

- 1. 在ACS GUI中,单击Network Resources。
- 2. 单击Network Device Groups。
- 3. 转至Location > Create(位于底部)。

	cisco Cisco Secure A	CS
	+ 🥳 My Workspace	Network Resources > Network Device Groups > Location
	🖌 🞲 Network Resources	Network Device Groups
	 Network Device Groups Location 	Filter: 💌 Match it 💌 Go 🛩
	Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description All Locations
ġ,	🛚 🎳 Users and identity Stores	
ie De	Policy Elements	
	+ 🔂 Access Policies	
	Monitoring and Reports	
	🖡 🍇 System Administration	

4. 添加必填字段,然后单击Submit。

cisco Cisco Secure ACS				
My Workspace	Network Resources > Network Device Groups > Location > Create			
	Device Group - General o Name: LAB Description: LAB Devices o Parent All Locations Select Select			
33 Users and Identity Stores				
Policy Elements				
Access Policies				
Monitoring and Reports				
🖌 🍓 System Administration				

5. 窗口将刷新:

cisco Cisco Secure ACS					
🕨 💮 My Workspace	Network Resources > Network Device Groups > Location				
🐱 🐙 Network Resources	Network Device Groups				
 Network Device Groups Location 	Filter: 💽 Match if: 💽 Go 🗢				
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description * <u>All Locations</u>				
Users and Identity Stores	LAB LAB Devices				
Policy Elements					
+ 🔂 Access Policies					
Monitoring and Reports					
System Administration					

6. 单击Device Type > Create。

cisco Cisco Secure A	NCS
+ 🛃 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device Type:Al Device Types:Switche
 Interview Resources 	Design design design
 Network Device Groups Location 	ø Name: Switches
Валоние Туре	Description: Switch where LAP is connected
Network Devices and AAA Clients Default Network Device	Parent All Device Types Select
External RADIUS Servers	• = Required fields
Users and Identity Stores	
+ Sp Policy Elements	
Access Policies	
Monitoring and Reports	Aller While the second second
🖌 🍇 System Administration	

7. 单击"Submit"。完成后,窗口将刷新:

Cisco Secure ACS					
🕨 🎲 My Workspace	Network Resources > Network Device Groups > Device Type				
🔹 🕼 Network Resources	Network Device Groups				
 Network Device Groups Location 	Filter. Match it. Go 🗢				
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description * <u>All Device Types</u> All Device Types				
Users and Identity Stores	Switches Switch where LAP is connected				
Policy Elements					
Access Policies					
Monitoring and Reports					
🕨 🍇 System Administration					

- 8. 转至Network Resources > Network Devices and AAA Clients。
- 9. 单击Create,并填写如下所示的详细信息:

cisco Cisco Secure /	ACS	acsadmin SALL ACSI2 (Primary)
→ ⊕ [*] Ny Workspace	Network Resources > Network Devices and AAA Clerks > Create	
 Network Device Groups 	o Nama: 2550-Dwady-LAP	
Location Device Tros	Description: Switch where LAP is connected Network Device Groups	
Default Network Devices and AAA Clients	Location Al Locations LAB	Select
External RADIUS Servers	Device Type All Device Types Switches	Select
Genes and identity Stores Genes Advantation Genes Policies Genes Policie	PAddress P Single P Address (* IP Range(s) • IP: 192.168.153.10	Authentication Options TxGACB+ RADUS RADUS Ghared Secret [ctrcs CaApsrt [1790 Enable KeyWrap
	• -Regard Salta	Key Encryption Key Massage Authenticator Code Key Key Ingut Format C ASCII C HEXADECIMAL

10. 单击"Submit"。窗口将刷新:

cisco Cisco Secure A	CS	economic SALIE.AC
* 💮 Mr Workspace	Nelwork Resources > Network Devices and AAA Clents	
- 🌆 Network Resources	Network Devices	Showin
Network Device Groups Location	Filter: Vilatch if. V Go V	
Network Devices and AM-Clients	Rame A #7/Mask NDGLocation NDG.Device Type D	lescription
Detaut Network Device External RADIUS Servers	Step-Switch-LAP 192.166.153.10/32 All Locations:LAB All Device Types:Switches 5	witch where LAP is connected
+ 🕌 Users and identity Stores		
+ Policy Elements		
» 🗓 Access Policies		
► → Monitoring and Reports		
+ 🤮 System Administration		

配置用户

在本节中,您将看到如何在之前配置的ACS上创建用户。您将将该用户分配到名为"LAP用户"的组 。

请完成以下步骤:

1. 转至Users and Identity Stores > Identity Groups > Create。

	cisco Cisco Secure ACS					
	🖌 💮 My Workspace	Users and identity Stores > identity Groups > Edit: "identityGroup:All Groups:Wireless Users"				
	Network Resources	Canacat				
		Veneral Name: LAP users Description: LAPs authenticating over wired Network Parent All Groups Select Select Select				
and the second second second	RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences					

2. 单击"Submit"。

Cisco Secure A	CS
My Workspace My Resources	Users and Identity Stores > Identity Groups
Users and Identity Stores Identity Groups	Filter: Go V
 Internal Identity Stores External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences 	Name Description * All Groups Identity Group Root LAP users LAPs authenticating over wired Network.

- 3. 创建3502e并将其分配到组"LAP用户"。
- 4. 转至Users and Identity Stores > Identity Groups > Users > Create。

Cisco Cisco Secure A	Users and identity Stores > internal identity Stores > Users > Create
	General Nama: 3502e Status: Enabled - O Description: LAP 3502e in vian 253 Identity Group: All Groups:LAP users Select
Hosts External Identity Stores Certificate Authonities Certificate Authentication Profile Identity Store Sequences Q: Policy Elements 	Password Information Password must • Contain 4 - 32 characters
Coress Policies Monitoring and Reports System Administration	Confirm Passwort Change password on next login User information There are no additional identity attributes defined for user records e = Required fields

5. 您将看到更新的信息:

💮 My Workspace	Users and	Identity Store	is > Internal identity Sto	res >	Users	
Network Resources	Interna	Users				
🔉 Users and Identity Stores				000000		_
Identity Groups	Finer.		Match if:		• <u> </u>	Ŷ
Internal Identity Stores	Г	Status	User Name		Identity Group	Description
Users			35028		All Groups:LAP users	LAP 3502e in vian 253

定义策略元素

验证Permit Access已设置。

cisco Cisco Secure A	ICS
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Appens > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Elltar Autobië
🗸 🏟 Policy Elements	There Bessieles
Session Conditions Authorization and Permissions	Permit Access
 Network Access Authorization Profiles 	
Device Administration Named Permission Objects	
+ 🔂 Access Policies	
 Monitoring and Reports 	
🕨 🍓 System Administration	

应用访问策略

在本部分中,您将选择EAP-FAST作为LAP的身份验证方法,以便进行身份验证。然后,您将基于 上述步骤创建规则。

请完成以下步骤:

1. 转至Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"。

cisco Cisco Secure A	cs
🕨 🚱 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
► 👌 Network Resources	
Users and Identity Stores	General Allowed Protocols
Policy Elements	Name: Default Network Access
🔹 🌉 Access Policies	Description: Default Network Access Service
 Access Services Service Selection Rules 	Service Type : Network Access
O Default Device Admin	Policy Structure
Oefault Network Access	Identity
► Ø deleterne	Group Mapping
Monitoring and Reports	Authorization
System Administration	

2. 确保已启用EAP-FAST和匿名带内PAC调配。

cisco Cisco Secure AC	CS
 My Workspace Network Resources Users and Identity Stores Policy Elements Access Policies Access Services Service Selection Rules Optical Device Admin Optical Network Access Identity Authorization Optical eleme Monitoring and Reports System Administration 	Access Policies > Access Services > Default Network Access > Edit "Default Network Access" General Allowed Protocols Process Host Lookup Authentication Protocols P Allow PAP/ASCII Allow CHAP Allow MS-CHAPv1 Allow MS-CHAPv2 Allow EAP-MD5
	 Allow EAP-TLS Allow LEAP Allow PEAP Allow EAP-FAST Preferred EAP protocol LEAP

• 🛼 Access Policies	► Allow LEAP
Access Services M Service Selection Rules O Default Device Admin O Default Device Admin O Default Network Access Identity Authorization ✓ deleteme Monitoring and Reports System Administration	 Allow PEAP PEAP Inner Methods Allow EAP-MS-CHAPv2 Allow Password Change Retries: 1 Allow EAP-GTC Allow Password Change Retries: 1
	 Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MS-CHAPv2 Allow Password Change Retries: 3 Allow EAP-GTC Allow TL3-Renegotiation Use PACs © Dont Use PACs Tunnel PAC Time To Live: 80 Days Proactive PAC update will occur after 10 % of PAC Time To Live has expired Allow Authenticated In-Band PAC Provisioning Server Returns Access Accept After Authenticated Provisioning Barbie Stabiless Session Resume Authorization PAC Time To Live: 1 Hours
	Submit Cancel

- 3. 单击"Submit"。
- 4. 验证您选择的身份组。在本示例中,使用Internal Users(在ACS上创建)并保存更改。

cisco Cisco Secure A	CS according SAL
🖕 🖌 My Workspace	Access Policies > Access Services > Default Network Access > Mently
+ B Network Resources	Single result selection Sule based result selection
+ 🏭 Users and Identity Stores	Identity Source: Internal Users Select
 Policy Elements 	* Advanced Options
🖌 🏂 Access Policies	if authentication failed React
Access Services Service Selection Rules O Detaut Device Admin	if user notifound Reject
O Delauit Network Access	Note: For authentications using FEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will
Authorization	be rejected
 Idenitating and Reports 	
 System Administration 	

5. 转至Access Policies > Access Services > Default Network Access > Authorization以验证授

权配置文件。

您可以自定义在什么条件下允许用户访问网络,以及经过身份验证后通过什么授权配置文件 (属性)。此精细度仅在ACS 5.x中可用。在本示例中,选择Location、Device Type、 Protocol、Identity Group和EAP Authentication Method。



6. 单击确定, 然后单击保存更改。

7. 下一步是创建规则。如果未定义规则,则允许LAP访问而不带任何条件。

8. 单击Create > Rule-1。此规则适用于组"LAP用户"中的用户。

cisco Cisco Secure At	CS **	tedmin S
+ 🕀 My Workspace	Access Policies > Access Services > Defaul Velocity Access > Authorization	
+ 🔄 Network Resources	Standard Balloui Europhics Dolor	
+ 🤮 Users and identity Stores	scareard Parcy Exception Porcy	
	Net Caco Secure ACS - Mozilla Finefex	×
Access Policies	Fill 192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do	<u>合</u>
Access Services Service Selection Rules O Default Device Admin O Default Network Access Identity Contract Network Access	Image: Status: Image:	
Monitoring and Reports	Conditione	
+ 🂐 System Administration	VIDGLocator: in VIAILocatorsLAB Select	
	NDG Device Type: In All Device Types: Switches Select	
	Protocol: match - Radius Select	
	✓ Identity Group: In ▲ All Groups LAP users Select 4	5
	Eap Authentication Method: AMF	
	Authorization Profiles: Permit Access Select Deselect	:1
	OK Cancel	Help
	The Default And and a second and an address of the second and an address of the second and a sec	
	Constant a Duralization of a Constant of the Instant of the Instan	
	VERBELT UNDER BUILDER KOVEID	
	Save Changes Discard Changes	

9. 点击Save Changes。如果希望拒绝不匹配条件的用户,请编辑默认规则以显示"拒绝访问"。

cisco Cisco Secure Al	CS	dmin SALB, ACSS2 (Primary) Log Dur Abour In
	Access Palces > Access Services > Defaul Network Access > Autorization Standood Palcy <u>Exception Policy</u> Network Access Authorization Policy Filter Status • Match if Equals • Enabled • <u>Court Filter</u> 60 •	
Access Services Service Selection Rules Softwith Device Admin Default Network Access Identity Content Device Admin Contents Contents Nontering and Reports Selection Administration	Status Name Conditions Bale:1 In All Locations LAB In All Device Types Dwitches match Redus In All Croups LAP users MT 4 Energies Energies defined or no enabled rule matches. Energies Energies	Results Hit on Authentication Method Authentication Profiles B Permit Access B Permit Access
	Create_1* Duplicate1* Edit Defete A Wove to V Save Changes Descard Changes	Customize HtCount

10. 最后一步是定义服务选择规则。使用此页可以配置简单策略或基于规则的策略,以确定将哪种

服务应用于传入请求。例如:

cisco Cisco Secure Ad	cs						eccedmin SALI		
* 📑 My Workspace	Access	Pulkies	> Access	Services >	Service Selection Rules				
* (3) Network Resources	Sincle result selection Field based result selection								
B Users and Identity Stores	Serv	ice Se	ection Po	licy					
+ Sy Policy Elements	Filte	e Sta	us *	Natch it	Equals + Enabled +	Clear Filter Go -			
 K Access Policies 					Conditions	Bocalts			
- Arross Resins			Status	Name	Protocal	Service	Hit Count		
O Default Device Admin	1			Rule-1	match Radius	Default Network Access	0		
 O Detault Network Access 	2			Rule-2	match Tacacs	Default Device Admin	0		
identity Authorization									
- 🖉 delaterno									
* 📄 Monitoring and Reports									
* 🧏 System Administration									

验证

一旦在交换机端口上启用了802.1x,除802.1x流量外的所有流量都会被阻塞通过该端口。已注册到 WLC的LAP将取消关联。只有在802.1x身份验证成功后,其他流量才允许通过。在交换机上启用 802.1x后,LAP成功注册到WLC表明LAP身份验证成功。

AP控制台:

<#root>

*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.75.44:5246 *Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 192.168.75.44:5247

!--- AP disconnects upon adding dot1x information in the gig0/11.

*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.

- *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
- *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
- *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to administratively down
- *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to administratively down
- *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset
- *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
- *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
- *Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to

reset

- Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
- *Jan 29 09:10:36.203: status of voice_diag_test from WLC is false

*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 2

!--- Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN *Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan wmmAC status is FALSEged state to CFG *Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11RadioO, changed state to down *Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11RadioO, changed state to reset *Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP *Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5508-3 *Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake. Wireless client traffic will be blocked until DTLS tunnel is established. *Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up *Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0] *Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to down *Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset *Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up *Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down *Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset *Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up *Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS keys are plumbed successfully. *Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel established. *Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.

ACS日志:

1. 查看命中次数:

如果您在身份验证的15分钟内检查日志,请确保刷新命中计数。在同一页面底部有一个"点击 计数"(Hit Count)选项卡。

cisco Cisco Secure A	CS	-	-	-			
+ 🛞 My Workspace	Access i	olicies	Access	Services >	Service Selection Rules		
+ 🎲 Network Resources	O si	ngle re	sult selec	nion 🖲 R	tule based result selection		
Users and Identity Stores	Servi	ce Sel	ection Po	licy			
Policy Elements	Filter	Stat	us -	Match if:	Equals - Enabled - Clea	r Filter Go 🔻	
Access Policies Access Services			Status	Name	Conditions	Results Service	Hit Count
B Default Device Admin	1			Bule-1	match Radius	Default Network Access	1
 O Default Network Access 	2		θ	Rule-2	match Tacaca	Default Device Admin	0
Authorization							
+ 📳 Monitoring and Reports							
🖌 🍇 System Administration							



2. 单击Monitoring and Reports,此时将显示一个新的弹出窗口。单击Authentications -RADIUS -Today。您也可以单击Details以验证应用了哪个服务选择规则。

			Launch Interactive Wesser		
Showing Rage 1 of 1 Pired Press News Loss Gets	Pager Go				
AAA Protocol > RADIUS Authentication					
Authentication Status : Pass or Pail Date : January 29, 2012 (Last 30 Minutes Last Hour Last 12 Hours Todler Yesterdar Last 7 Day	s (Last 30 Davs)				
Generated on January 29, 2012 3:15:01 PM EST					
Relad ≁=πass ★=πal №=⊂lick for datails ♀=™ouss over item for additional information					
Logged At Status Falure Details Username Address Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Go
Jan 29.12 9 11.12 965 PM 🕜 🧐 3502e CC-EF-J8-FA-53-19 Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3560-Switch-LAP	192.168.153.10	GicablEthemet0/11	

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科安全访问控制系统
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。