使用AireOS和下一代WLC配置ISE无线CWA和热 点流

目录

简介 <u>先决条件</u> 要求 使用的组件 配置 网络图 配置Unified 5508 WLC 全局配置 配置访客的服务集标识符(SSID): 配置重定向ACL <u>HTTPS重定向</u> 主动故障转移 强制网络旁路 配置融合3850 NGWC 全局配置 SSID 配置 重定向 ACL 配置 命令行界面(CLI)配置 配置ISE 常见ISE配置任务 使用案例1:在每个用户连接中具有访客身份验证的CWA 使用案例2:CWA with Device Registration enforcing guest authentication everyday.(带设备注册的 CWA每天执行一次访客身份验证。) 使用案例3:HostSpot门户 验证 使用案例1 使用案例2 使用案例3 AireOS中的FlexConnect本地交换 外部锚点方案 故障排除 AireOS和融合接入WLC上的常见断开状态 **AireOS WLC** NGWC ISE 相关信息

简介

本文档介绍如何在带有Cisco AireOS和下一代无线局域网控制器的身份服务引擎中配置三个访客案例。

先决条件

要求

Cisco 建议您了解以下主题:

- •思科无线局域网控制器(统一和融合接入)
- •身份服务引擎 (ISE)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科身份服务引擎版本2.1
- •思科无线局域网控制器5508,带8.0.121.0
- •下一代无线控制器(NGWC)catalyst 3850(WS-C3850-24P),带03.06.04.E

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

网络图



本文档介绍的步骤介绍统一接入WLC和融合接入WLC上的典型配置,以支持任何使用ISE的访客流 。

配置Unified 5508 WLC

无论在ISE中配置何种使用案例,从WLC的角度来看,它都以无线端点开始,该端点连接到启用了 MAC过滤的开放式SSID(以及AAA覆盖和RADIUS NAC),该端点指向ISE作为身份验证和记帐服 务器。 这可以确保ISE将必要的属性动态推送到WLC,以便成功实施重定向到ISE的访客门户。

全局配置

1.将ISE全局添加为身份验证和记帐服务器。

• 导航到**安全> AAA >身份验证**,然后点击**新建**

Security	RADIUS Authentication Se	rvers > Edit
 ▼ AAA General ▼ RADIUS Authentication Accounting Suback 	Server Index Server Address(Ipv4/Ipv6) Shared Secret Format	6 ASCII T
DNS	Shared Secret	•••
Downloaded AVP TACACS+	Confirm Shared Secret	•••
LDAP Local Net Users	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Filtering Disabled Clients	Port Number	1812
User Login Policies	Server Status	Enabled *
AP Policies Password Policies	Support for RFC 3576	Enabled *
Local EAP	Server Timeout	S seconds
Advanced EAP	Network User	🗹 Enable
Priority Order	Management	C Enable
Certificate	Realm List	
Access Control Lists	IPSec	Enable Enable

- 输入ISE服务器IP和共享密钥
- •确保服务器状态和RFC 3676支持(授权更改或CoA支持)均设置为启用。
- ・在服务器超时下,默认情况下AireOS WLC有2秒。取决于网络特征(延迟、不同位置的ISE和WLC),将服务器超时至少增加到5秒可避免不必要的故障切换事件。
- 单击 Apply。
- 如果有多个要配置的策略服务节点(PSN),请继续创建其他服务器条目。

注意:此特定配置示例包括2个ISE实例

- 导航到**安全> AAA > RADIUS >记帐**,然后点击**新建**
- 输入ISE服务器IP和共享密钥
- •确保Server Status设置为Enabled
- •如有必要,增加服务器超时(默认值为2秒)。
- 2.回退配置。

在统一环境中,一旦触发服务器超时,WLC将移至下一个配置的服务器。WLAN中的下一行。如果 没有其它可用服务器,则WLC会选择全局服务器列表中的下一个可用服务器。当故障切换发生后 ,在SSID(主、辅助)上配置多个服务器时,WLC默认继续将身份验证和(或)记帐流量永久发送 到辅助实例,即使主服务器重新联机也是如此。

为了缓解此行为,请启用回退。导航到**安全> AAA > RADIUS >回退。**默认行为是关闭的。从服务 器关闭事件恢复的唯一方法需要管理员干预(全局退回服务器的管理员状态)。

要启用回退,您有两个选项:

- 被动 在被动模式下,如果服务器不响应WLC身份验证请求,则WLC将服务器移至非活动队列并设置计时器(Interval in Sec选项)。当计时器到期时,WLC将服务器移至活动队列,而不考虑服务器的实际状态。如果身份验证请求导致超时事件(这意味着服务器仍然停机),服务器条目会再次移动到非活动队列,并且计时器再次启动。如果服务器成功响应,则它仍保留在活动队列中。此处的可配置值范围为180至3600秒。
- **主用** 在主用模式下,当服务器不响应WLC身份验证请求时,WLC将服务器标记为停机,然 后将服务器移至非主用服务器池,并定期开始发送探测消息,直到该服务器响应为止。如果服

务器响应,则WLC将失效服务器移至活动池并停止发送探测消息。 在此模式下,WLC要求您输入用户名和探测间隔(以秒为单位)(180到3600)。

注意:WLC探测功能不需要身份验证成功。无论哪种方式,成功或失败的身份验证都被视为 服务器响应,足以将服务器提升到活动队列。

配置访客的服务集标识符(SSID):

• 导航到WLANs选项卡,在Create New选项下单击Go:

WLANs							
Current Filter: None	[Change Filte	r] [Clear Filter]			1	Create New	▼ _Go
• 输入配置文件1 • 在General选项	名称和SSID名和 〔卡下,选择要	弥。单击 / 使用的接□	Apply 。 □或接口组	(访客VLAN)。		
Radio Policy		All		•			
Interface/Inter	face Group(G) gues	t2 '				
・在Security > L WLANs > Ec General	ayer 2 > Layer dit 'Guest' Security	2 Securit QoS	y下选择No Policy	one并启用Mad -Mapping	c Filtering复 Advanc	选框。 ed	
Layer 2	Layer 3	AAA	Servers				
Layer 2	Security 🖉 🛛 N MA	one C Filterin	g2 🕑	T			
Fast Transi	tion						
Fast Transiti	on 🗌						

• 在AAA Servers选项卡下,将Authentication and Accounting servers设置为**enabled**,并选择您 的主要和辅助服务器。

eneral	Security	QoS	Policy-	Mapping	Advanced	
Layer 2	Layer 3	AAA S	ervers			
Radius Serv	ers		-			
Radius Se	Authentica	ite interfact	ce ©Ena ers	Accounting) Servers	-
Radius Se	Authentica	tion Serve	ers	Accounting	Servers	
Radius Se Server 1	Authentica C Enabled IP:	ite interfac tion Serv 57.210, Pc	ce Ena ers ort:1812 •	Accounting C Enabled IP:	57.210 , Port:1813	•
Server 1 Server 2	Authentica C Enabled IP:	ite interfac tion Serve 57.210, Po 57.21, Por	ce ©Ena ers ort:1812 ¥ t:1812 ¥	Accounting	57.210, Port:1813	3 ¥
Server 1 Server 2 Server 3	Authentica C Enabled IP: IP: None	ite interfac tion Serve 57.210, Pc 57.21, Por	ce UEna ers ort:1812 * t:1812 *	Accounting C Enabled IP	57.210, Port:1813	3 ¥ ¥
Server 1 Server 2 Server 3 Server 4	Authentica C Enabled IP: IP: None None	ite interfac tion Serve 57.210, Po 57.21, Por	ce UEna ers ort:1812 * t:1812 * *	Accounting Counting Counting Counting Counting IP Co	57.210, Port:1813	•
Server 1 Server 2 Server 3 Server 4 Server 5	Authentica Cenabled IP: IP: None None None	ite interfac tion Serv 57.210, Pc 57.21, Por	ce UEna ers ort:1812 * t:1812 * * *	Accounting Calculation Accounting Calculation Enabled IP IP IP IP IP IP IP IP IP IP	57.210, Port:1813	•

•临时更新:这是一个可选配置,不会为此流程增加任何优势。如果您希望启用它,则WLC必须 运行8.x或更高版本的代码:

已禁用:功能已完全禁用。

启用0间隔:每当客户端的移动站控制块(MSCB)条目(即IPv4或IPv6地址分配或更改,客户端漫游事件。) 不会发送额外的定期更新。

使用已配置的临时间隔启用:在此模式下,WLC在客户端的MSCB条目更改时向ISE发送通知,并 在已配置的间隔发送其他定期记帐通知(无论任何更改)。

- 在Advanced Tab Enable Allow AAA Override下,在NAC state下,选择RADIUS NAC。这可确 保WLC应用来自ISE的任何属性值对(AVP)。
- •导航到SSID常规选项卡,并将SSID状态设置为**Enabled**

WLANs > Edit 'Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Na	ime	Gu	iest	
Туре		W	LAN	
SSID		Gu	iest	
Status			Enabled	

•应用更改。

配置重定向ACL

此ACL由ISE引用,它确定重定向哪些流量以及允许哪些流量通过。

- •转至Security选项卡> Access Control Lists,然后单击New
- 这是ACL的一个示例

Acce	iss Cont	rol Lists > Edit	1								1	< 8ack
Gene	eral											
Acces	s List Name	e Guest_Rer	lirect									
Deny	Counters	0										
Seq	Action	Source IP/Mask		Destination IP/	Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	_
1	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	Any	DNS	Any	Any	0	
2	Permit	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	UDP	DNS	Any	Any	Any	0	
1	Permit	0.0.0	/ 0.0.0.0	.157.210	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	
4	Permit	157.210	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	
5	Permit	0.0.0.0	/ 0.0.0.0	.157.21	/ 255.255.255.255	TCP	Any	8443	Any	Any	0	
<u>6</u>	Permit	157.21	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	TCP	8443	Any	Any	Any	0	

此ACL必须允许通过TCP端口8443访问DNS服务和ISE节点。底部有一个隐式拒绝,表示其余流量 重定向到ISE的访客门户URL。

HTTPS重定向

此功能在AireOS版本8.0.x及更高版本中受支持,但默认情况下处于关闭状态。要启用HTTPS支持 ,请转到WLC **Management > HTTP-HTTPS > HTTPS Redirection**并将其设置为**Enabled**,或在 CLI中应用此命令:

(Cisco Controller) >config network web-auth https-redirect enable

启用HTTPS重定向后的证书警告

启用https-redirect后,用户可能会在重定向期间遇到证书信任问题。即使控制器上有有效的链式证书,并且即使该证书由第三方受信任证书颁发机构签名,也会出现这种情况。原因是WLC上安装的证书已颁发给其虚拟接口主机名或IP地址。当客户端尝试https://cisco.com时,浏览器期望将证书颁发给cisco.com。但是,为了让WLC能够截取客户端颁发的GET,它首先需要建立HTTPS会话,WLC在SSL握手阶段为其提供其虚拟接口证书。这会导致浏览器显示警告,因为在SSL握手过程中显示的证书尚未颁发给客户端尝试访问的原始网站(即,与WLC的虚拟接口主机名相对cisco.com)。您可以在不同的浏览器中看到不同的证书错误消息,但是这些错误消息都与同一问题有关。

主动故障转移

默认情况下,此功能在AireOS WLC中启用。启用主动故障切换时,WLC会将AAA服务器标记为无响应,并在RADIUS超时事件影响一个客户端后移至下一个配置的AAA服务器。

禁用此功能后,仅当至少3个客户端会话发生RADIUS超时事件时,WLC才会故障切换到下一台服务 器。此命令可以禁用此功能(此命令不需要重新启动): (Cisco Controller) > show radius summary

Vendor Id Backward Compatibility	Disabled
Call Station Id Case	lower
Acct Call Station Id Type	Mac Address
Auth Call Station Id Type	AP's Radio MAC Address:SSID
Extended Source Ports Support	Enabled
Aggressive Failover	Disabled

强制网络旁路

支持强制网络助手(CNA)机制以发现强制网络门户并自动启动登录页的终端通常通过受控窗口中的 伪浏览器执行此操作,而其他终端则启动完全功能的浏览器以触发此操作。对于CNA启动伪浏览器 的终端,这会中断流 重定向至ISE强制网络门户时。 这通常影响Apple IOS设备,在需要设备注册 、VLAN DHCP释放和合规性检查的流中尤其有负面影响。

根据使用的流量的复杂性,建议启用强制绕行。在这种情况下,WLC忽略CNA门户发现机制,客户 端需要打开浏览器以启动重定向过程。

验证功能的状态:

(Cisco Controller) > show network summary

Web Auth Redirect Ports80,3Web Auth Proxy RedirectDisaWeb Auth Captive-BypassDisaWeb Auth Secure WebEnabWeb Auth Secure RedirectionEnab	abled
Web Auth Proxy RedirectDisaWeb Auth Captive-BypassDisaWeb Auth Secure WebEnabWeb Auth Secure RedirectionEnab	3128
Web Auth Captive-Bypass Disa Web Auth Secure Web Enab Web Auth Secure Redirection Enab	able
Web Auth Secure Web Enable Enable Auth Secure Redirection Enable En	abled
Web Auth Secure Redirection Enab	ble
	ble

要启用此功能,请键入以下命令:

(Cisco Controller) >config network web-auth captive-bypass enable Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect. WLC提醒用户.要使更改生效.需要重新启动重置系统。

此时,show network summary将功能显示为已启用,但是要使更改生效,需要重新启动WLC。

配置融合3850 NGWC

全局配置

1.全局添加ISE作为身份验证和记帐服务器

- 导航到Configuration > Security > RADIUS > Servers, 然后单击New
- 输入反映环境条件的ISE服务器IP地址、共享密钥、服务器超时和重试计数。
- •确保支持RFC 3570(CoA支持)。
- 重复此过程以添加辅助服务器条目。

RADIUS Servers		0
Radius Servers > New		
	r	
Server Name	ISE1	
Server IP Address	.157.210	
Shared Secret	******	
Confirm Shared Secret	•••••	
Auth Port (0-65535)	1812	
Acct Port (0-65535)	1813	
Server Timeout (1-1000)secs	5	
Retry Count (0-100)	2	
Support for RFC 3576	Enable 💌	

2.创建ISE的服务器组

- 导航到Configuration > Security > Server Groups,然后单击New
- •为组分配名称并输入Dead-time值(分钟)。这是控制器将服务器保留在"非活动"队列中的时间 ,然后才会将其再次提升到活动服务器列表。
- •从Available Servers列表中将其添加到Assigned Servers列。

Radius Server Group			
Radius Server Group > New			
Name	ISE_Group		
MAC-delimiter	colon 💌		
MAC-filtering	none 💌		
Dead-time (0-1440) in mir	utes 10		
Group Type	radius		
	Available Servers	Assigned Servers	
		A ISE2 ISE1	÷
Servers In This Group		< >	
		-	*

3.全**局启用Dot1x**

• 导航到Configuration > AAA > Method Lists > General并启用Dot1x system Auth Control

General	
Dot1x System Auth Control	
Local Authentication	None 💌
Local Authorization	None 💌

4.配置方法列表

 导航到Configuration > AAA > Method Lists > Authentication,然后创建新的方法列表。在本例 中,它是Dot1x和Group ISE_Group(在上一步中创建的组)。然后点击Apply

Authentication Authentication > New				
Method List Name	ISE_Method			
Type: Group Type: Fallback to local	dot1x O login group O local			
	Available Server Groups		Assigned Server Groups	
		*	ISE_Group	
Groups In This Method		< >		
		+		*

• 对记帐(Configuration > AAA > Method Lists > accounting)和授权(Configuration > AAA > Method Lists > Authorization)执行相同操作。他们一定长这样

Accounting		
Accounting > New		-
Method List Name	ISE_Method	
Type:	O dot1x O exec identity O network O commands	
000	Available Server Groups Assigned Server Groups	
	ISE_Group	-
Groups In This Method	< >	
	*	*
Groups In This Method	*	

Authorization Authorization > New				
Method List Name	ISE_Method			
Type: Group Type:	network ○ exec ○ credential-dox group ○ local	wnload		
	Available Server Groups		Assigned Server Gro	ups
			ISE_Group	*
Groups In This Method	6	< >]	
				*

5.创建授权MAC过滤器方法。

稍后会从SSID设置调用此项。

- 导航到Configuration > AAA > Method Lists > Authorization, 然后单击New。
- 输入方**法列表名称**。选择**类型=网络**和组类型组。
- •将ISE_Group添加到Assigned Server Groups字段。

Authorization Authorization > New			
Method List Name	MacFilterMethod		
Type: Group Type:	network O exec O credential-download group O local		
0.18	Available Server Groups	Assigned Server Groups	
	*	ISE_Group	
Groups In This Method	< >		
	*		*

SSID 配置

1.创**建访客SSID**

- 导航到**配置>无线> WLANs**,然后单击**新建**
- 输入WLAN ID、SSID和配置文件名称,然后点击Apply。
- 进入Interface / Interface Group下的SSID设置后,选择Guest VLAN Layer 3 interface。

VLAN > Edit		5000				
Security	QOS	AVC	Policy Mapping	Advanced		
Profile Name	Guest					
Туре	WLAN					
SSID	Guest					
Chahus	P Enabled					
And And A	Cas Enabled					
Security Policies	[WPA2][Aut	h(802.1x)]				
Security Policies	[WPA2][Aut (Modifica	h(802.1x)] itions done	under security tab will	appear after ap	plying the change	s.)
Security Policies Radio Policy	[WPA2][Auti (Modifica	h(802.1x)] itions done	under security tab will Interface/In	appear after ap Iterface Grou	plying the change Ip Dialog	s.) ×
Security Policies Radio Policy Interface/Interface Group(G) Broadcast SSID	[WPA2][Auti (Modifica All • default	h(802.1x)) itions done	under security tab will Interface/In	appear after ap iterface Grou	plying the change Ip Dialog	s.)
Security Policies Radio Policy Interface/Interface Group(G) Broadcast SSID Multicast VLAN Feature	(WPA2)[Aut (Modifica All • default	h(802.1x)] itions done	under security tab will Interface/In Interface/Inter	appear after ap iterface Grou face Group(G)	plying the change up Dialog default default	s.) X
Security Policies Radio Policy Interface/Interface Group(G) Broadcast SSID Multicast VLAN Feature	[WPA2][Aut (Modifica All • default	h(802.1x)] itions done	under security tab will Interface/In Interface/Inter	appear after ap iterface Grou face Group(G)	plying the change p Dialog default default VLAN0010	s.) ×
Security Policies Radio Policy Interface/Interface Group(G) Broadcast SSID Multicast VLAN Feature	[WPA2][Auti (Modifica All • default	h(802.1x)) itions done	under security tab will Interface/In Interface/Inter	appear after ap iterface Grou face Group(G)	plying the change p Dialog default default VLAN0010 VLAN0011	s.)
Security Policies Radio Policy Interface/Interface Group(G) Broadcast SSID Multicast VLAN Feature	[WPA2][Aut (Modifica All • default	h(802.1x)] itions done	under security tab will Interface/In Interface/Inter	appear after ap iterface Grou face Group(G)	plying the change p Dialog default default VLAN0010 VLAN0011 VLAN0050 VI AN0301	s.) X X

- 在Security > Layer 2下,选择None,然后在Mac Filtering旁边输入先前配置的Mac Filter Method List Name(MacFilterMethod)。
- 在**Security > AAA Server**选项卡下,</mark>选择正确的身份验证和记帐方法列表(ISE_Method)。

WLAN WLAN > Edit General	Security	QOS	AVC		
Layer2	Layer3	AAA Ser	ver		
Layer 2 Secu MAC Filtering	nity None 💌	lethoc			
WLAN > Edit General	Securi	ty J	QOS	AVC	Policy Mapping
Layer2	Layer	3	WA Serve	ar -	
Authentic Accountir Local EAP	ation Metho ng Method Authenticat	d	ISE_M	lethod	D

• 在Advanced选项卡下,启用Allow AAA Override和NAC state。其他设置必须根据每个部署要 求(会话超时、客户端排除、支持Aironet扩展)进行调整。

WLAN WLAN > Edit						
General	Security	QOS	AVC	Policy	y Mapping Advanced	
Allow AAA Ov	verride le Detection				DHCP	
Session Time	out (secs)	28800]		DHCP Server IP Address	0.0.0.0
Aironet IE					DHCP Address Assignment required	
Diagnostic Ch	nannel				DHCP Option 82	
P2P Blocking	Action	Disabled •]		DHCP Option 82 Format	None 💌
Media Stream	Multicast-direct				DHCP Option 82 Ascii Mode	
Client Exclusi	ion				DHCP Option 82 Rid Mode	
Timeout Valu	e(secs) 60				NAC	
Max Allowed	Client 0				NAC State 🗹	

•导航到General选项卡,将Status设置为Enabled。然后点击应用。

重定向 ACL 配置

ISE稍后在响应初始MAB请求的access-accept中引用此ACL。NGWC使用它来确定重定向哪些流量 以及必须允许哪些流量通过。

- 导航到configuration > security > ACL > Access Control Lists,然后单击Add New。
- •选择扩展并输入ACL名称。
- 下图显示典型重定向ACL的示例:

ACO	> ACL deta	ol Lists ail					
Det	ails :						
Nam	e:	Guest_Red	irect				
Туре		IPv4 Exter	ded				
Add	Sequence	Remove					
	Seq	Actio	n Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
0	10	deny	icmp	any	any		-
0	20	deny	udp	any	any		eq 67
0	30	deny	udp	any	any		eq 68
0	40	deny	udp	any	any	-	eq 53
0	50	deny	tcp	any	1400.157.210	×	eq 8443
0	60	deny	tcp	any	.157.21	-	eq 8443
0	70	perm	lit tcp	any	any		eq 80
0	80	perm	it tcp	any	any	-	eq 443

注:行10是可选的。这通常是为建议进行故障排除而添加的。此ACL必须允许访问DHCP、 DNS服务以及ISE服务器端口TCP 8443(拒绝ACE)。HTTP和HTTPS流量被重定向(允许 ACE)。

命令行界面(CLI)配置

前面步骤中讨论的所有配置也可以通过CLI应用。

802.1x全局启用

dot1x system-auth-control

全局AAA配置

```
aaa new-model
1
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
1
aaa server radius dynamic-author
client 172.16.157.210 server-key *****
client 172.16.157.21 server-key *****
auth-type any
!
radius server ISE1
address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
timeout 5
retransmit 2
key *****
!
radius server ISE2
address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
timeout 5
retransmit 2
key *****
!
1
aaa group server radius ISE_Group
server name ISE2
server name ISE1
deadtime 10
mac-delimiter colon
Ţ
```

WLAN 配置

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2
ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
```

no shutdown

重定向ACL示例

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
10 deny icmp any any
20 deny udp any any eq bootps
30 deny udp any any eq bootpc
40 deny udp any any eq domain
50 deny tcp any host 172.16.157.210 eq 8443
60 deny tcp any host 172.16.157.21 eq 8443
70 permit tcp any any eq www
80 permit tcp any any eq 443
```

HTTP和HTTPS支持

3850#show run | inc http ip http server ip http secure-server

注意:如果应用ACL以限制通过HTTP访问WLC,则会影响重定向。

配置ISE

本节介绍ISE上支持本文档中讨论的所有使用案例所需的配置。

常见ISE配置任务

- 1. 登录到ISE并导航到管理>网络资源>网络设备,然后点击添加
- 2. 输入与WLC关联的Name和设备IP地址。
- 3. 选中RADIUS身份验证设置框,并键入WLC端配置的共享密钥。然后请点击提交。

Network Devices List > Cisco_5508
Network Devices
* Name Cisco_5508
Description LAB_AireOS_WLC
* IP Address:
* Device Profile 🗰 Cisco 👻 🕕
Model Name
Software Version
* Network Device Group
Device Type All Device Types 📀 Set. To Default
Location Al Locations Set To Default
PADI IS Authenticolian Sellinge
 Pound's Autrentication Settings
Enable Authentication Settings
Protocol RADIUS
* Shared Secret Show Show

4.定位至"策略">"验证",在"MAB"下单击"编辑",并确保在**使用:内部终端**下,选项如果未找到 用户设置为继续(默认情况下必须存在)。

Authentication Policy

Define the Authentication Policy by selecting the protocols the For Policy Export go to Administration > System > Backup & F Policy Type O Simple I Rule-Based	at ISE should use to communicate with the network devices, and the identity sources that it should u Restore > Policy Export Page	ise for au
✓ MAB : If Will	red_MAB OR Wireless_MAB	and -
Default : Use	Internal Endpoints	
	Identity Source Internal Endpoints Options If authentication failed Reject If user not found Continue If process failed Drop	
Dot1X : If Wire Wireless_802.1XAllow Protocols : Default Network Acce	Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS 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 be rejected.	

使用案例1:在每个用户连接中具有访客身份验证的CWA

流概述

1. 无线用户连接到访客SSID。

- 2. WLC根据终端在ISE上的MAC地址作为AAA服务器对终端进行身份验证。
- 3. ISE返回back和access-accept两个属性值对(AVP):url-redirect和url-redirect-acl。一旦WLC将 此AVP应用于终端会话,该站点将转换为DHCP-Required,一旦它获取了IP地址,它将保留在 CENTRAL_WEB_AUTH中。在此步骤中,WLC准备开始重定向客户端的http/https流量。
- 4. 最终用户打开Web浏览器,一旦生成HTTP或HTTPS流量,WLC会将用户重定向到ISE访客门 户。
- 5. 用户进入访客门户后,会提示输入访客凭证(在本例中为发起人创建)。
- 6. 凭证验证后,ISE显示AUP页面,客户端接受后,会向WLC发送动态CoA类型重新身份验证。
- 7. WLC重新处理MAC过滤身份验证,而不向移动站发出取消身份验证。这对终端必须是无缝的
 - o
- 8. 发生重新身份验证事件后,ISE会重新评估授权策略,并且此次,终端被授予允许访问权限 ,因为之前有一个成功的访客身份验证事件。

每次用户连接到SSID时,此过程都会重复。

配置

- 9航至ISE并导航至工作中心(Work Centers)>访客接入(Guest Access)>配置(Configure)>访客 门户(Guest Portals)>选择发起人访客门户(Select Sponsored Guest Portal)(或创建新的门户 类型Sponsored-Guest)。
- 2. 在Guest Device Registration settings下,取消选中所有选项,然后单击Save。

▼ Gu	est Device Registration Settings
	Automatically register guest devices
	A message displays to guests when they reach the maximum number of supported devices.
	Allow guests to register devices
	You can set the maximum number of supported devices in the guest type settings.
De	vice information will be stored in the endpoint identity group specified in the guest type

3.定位至"策略">"策略要素">"结果">"授权">"授权配置文件"。单击 Add。

4.响应初始Mac身份验证绕行(MAB)请求,此配置文件通过**Redirect-URL**和**Redirect-URL-ACL**推送 到WLC。

 选中Web重定向(CWA、MDM、NSP、CPP)后,选择Centralized Web Auth,然后在ACL字段 下键入Redirect ACL name,并在Value下选择Sponsored Guest Portal(default)(或之前步骤中 创建的任何其他特定门户)。

配置文件必须与此图片中的配置文件类似。然后单击保存。

Authorization Profiles > CWA_Redirect

Wireless Guest Redirect

Authorization Profile	
* Name	CWA_Redirect
Description	
* Access Type	ACCESS_ACCEPT T
Network Device Profile	🚓 Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
Web Redirection (C	NA, MDM, NSP, CPP) (j)
Centralized Web Au	th ACL Guest_Redirect Value onsored Guest Portal (default)
Display Certifica	ates Renewal Message
Static IP/Host n	ame/FQDN

页面底部的Attribute Details(属性详细信息)将属性值对(AVP)推送到WLC

•	▼ Attributes Details
	Access Type = ACCESS_ACCEPT cisco-av-pair = url-redirect-acl=Guest_Redirect cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa

5.定位至**Policy > Authorization**,然后插入新规则。此规则是触发重定向进程以响应来自WLC的初 始MAC身份验证请求的规则。(在本例中称为**Wireless_Guest_Redirect**)。

6.在Conditions下,选择Select Existing Condition from Library,然后在condition name下,选择 Compound condition。选择名为Wireless_MAB的预定义复合条件。

注:此条件包含源自WLC的访问请求中预期的2个Radius属性(NAS-Port-Type= IEEE 802.11 <存在于所有无线请求中>和Service-Type = Call Check<(表示特定的mac身份验证绕行请求))

7.在结果下,选择**Standard>CWA_Redirect**(在上一步中创建的授权配置文件)。然后单击**完成**并 保存

then CWA Redirect

Edit | -

8.导航到CWA_Redirect规则**的结尾**,然后点击Edit旁边的箭头。然后选择duplicate above。

9.修改名称,因为这是ISE的CoA重新验证会话后终端匹配的策略(本例中为 Wireless_Guest_Access)。

if Wireless MAB

10.在Wireless_MAB复合条件旁边,单击+符号展开条件,并在Wireless_MAB条件结束时单击添加

属性/值。

Wireless_MAB		
Wireless_Guest_Access if Any 💠 and Wireless_MAB	2	then PermitAccess 슧
Add All Conditions Below to Library		en CWA_Redirect
Condition Name Description		en PermitAccess
Wireless_MAB 📀 Normalised Radius:RadiusFlowType EQUALS WirelessMAB	ê-	
	Add	Attribute/Value
Save Reset	Add	Condition from Library
	Del	ete

11.在"选择属性"下,选择网络访问>用例等于访客流

Add All Conditions Below	w to clorary	
Condition Name	Description	AND +
Wireless_MAB 📀	Normalised Radius:RadiusFlowType EQUALS WirelessMAB	AND
٥	Network Access:U 😋 Equals 🔹 Guest Flow	0

12.在**权限**下,选择PermitAccess。然后单击完成并保存

								-	_
ø	~	Ŧ	Wireless_Guest_Access	Any	÷	Wireless_MAB AND Network Acce	÷	PermitAccess	\$
									_

两个策略必须如下所示:

	Wireless_Guest_Access	if	(Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow)	then	PermitAccess
 Image: A set of the set of the	Wireless_Guest_Redirect	if	Wireless_MAB	then	CWA_Redirect

使用案例2:CWA with Device Registration enforcing guest authentication everyday.(带设备注册的 CWA每天执行一次访客身份验证。)

流概述

- 1. 无线用户连接到访客SSID。
- 2. WLC根据终端在ISE上的MAC地址作为AAA服务器对终端进行身份验证。
- 3. ISE返回back和access-accept并包含两个属性值对(AVP)(url-redirect和url-redirect-acl)。
- 4. 一旦WLC将此AVP应用于终端会话,该站点将转换为DHCP-Required,一旦它获取了IP地址 ,它将保留在CENTRAL_WEB_AUTH中。在此步骤中,WLC准备开始重定向客户端的 http/https流量。
- 5. 最终用户打开Web浏览器,一旦生成HTTP或HTTPS流量,WLC会将用户重定向到ISE访客门 户。
- 6. 用户进入访客门户后,系统会提示他输入发起人创建的凭证。
- 7. 凭证验证后,ISE会将此终端添加到特定(预配置的)终端身份组(设备注册)。
- 8. 显示AUP页面,一旦客户端接受,动态CoA类型重新进行身份验证。发送到WLC。
- 9. WLC重新处理MAC过滤身份验证,而不向移动站发出取消身份验证。这对终端必须是无缝的。
- 10. 发生重新身份验证事件后,ISE会重新评估授权策略。这次,由于终端是正确终端身份组的成

员,ISE返回无限制的访问接受。

11. 由于终端已在步骤6中注册,因此每次用户返回时,都允许其在网络上,直到从ISE手动将其 删除,或者终端清除策略运行刷新符合条件的终端。

在本实验场景中,身份验证每天执行一次。重新身份验证触发器是终端清除策略,它每天删除已使 用的终端身份组的所有终端。

注意:可以根据自上次AUP接受以来经过的时间实施访客身份验证事件。如果您需要更频繁地 实施Guest Logon(例如每4小时),则可以选择此选项。

配置

- 在ISE上,导航至工作中心(Work Centers)>访客接入(Guest Access)>配置(Configure)>访客门 户(Guest Portals)>选择发起人访客门户(Select Sponsored Guest Portal)(或创建新的门户类 型Sponsored-Guest)。
- 2. 在Guest Device Registration设置下,验证选中Automatically register guest devices选项。 Click Save.



3.导航到**工作中心>访客接入>配置>访客类型**,或只需单击门户中"访客设备注册设置"下指定的快捷 方式。

 Guest Device Registration Settings
Automatically register guest devices
A message displays to guests when they reach the maximum number of supported devices.
Allow guests to register devices
You can set the maximum number of supported devices in the guest type settings.
Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.
Configure guest types at:
Work Centers > Guest Access > Configure > Guest Types

4.发起人用户创建访客帐户时,会为其分配访客类型。每个访客类型可以有一个属于不同终端身份 组的注册终端。要分配设备必须添加到的终端身份组,请选择发起人用于这些访客用户的访客类型 (此使用案例基于每周(默认))。

5.进入访客类型后,在Login Options下,从下拉菜单Endpoint Identity group for guest device registration中选择Endpoint Group

Maximum devices guests can register: 5 (1-999)

Endpoint identity group for guest device registration: GuestEndpoints

6.定位至"策略">"策略要素">"结果">"授权">"授权配置文件"。单击 Add。

7.响应初始Mac身份验证绕行(MAB)请求,此配置文件通过**Redirect-URL**和**Redirect-URL-ACL**推送 到WLC。

•选中Web重定向(CWA、MDM、NSP、CPP)后,选择**Centralized Web Auth**,然后在**ACL**字段 下键入Redirect ACL name,然后在**Value**下选择为此流创建的门户

Authorization Profiles > New	Authorization Profile
Authorization Profile	
* Name	CWA_DeviceRegistration
Description	
* Access Type	ACCESS_ACCEPT *
Network Device Profile	🚓 Cisco 💌 🕀
Service Template	
Track Movement	
Passive Identity Tracking	
▼ Common Tasks	
VLAN	
Voice Domain Permis	sion
Web Redirection (CV	NA, MDM, NSP, CPP) (j)
Centralized Web Aut	h ACL Guest_Redirect Value CWA_DeviceRegistration

8.定位至**策略>授权**,然后插入新规则。此规则是触发重定向进程以响应来自WLC的初始MAC身份 验证请求的规则。(在本例中称为**Wireless_Guest_Redirect**)。

9.在Conditions下,选择Select Existing Condition from Library,然后在condition name下,选择 Compound。选择名为Wireless_MAB的预定义复合条件。

10.在结果下,选择**Standard > CWA_DeviceRegistration**(在上一步中创建的授权配置文件)。然 后单击**完成**并保存

1	Wireless_Guest_Redirect	if Wireless_MAB	CWA_DeviceRegistration

11.复制上述策略,修改其名称,因为这是终端从重新身份验证事件(称为 Wireless_Guest_Access)返回后触发的策略。

12.在Identity Group Details框中,选择Endpoint Identity Group,然后在Guest

Type(GuestEndpoints)下选择您引用的组。

13.在"结果"下,选择PermitAccess。单击Done并Save更改。

~	Wireless_Guest_Access	if GuestEndpoints AND Wireless_MAB	then	PermitAccess
~	Wireless_Guest_Redirect	if Wireless_MAB	then	CWA_DeviceRegistration

14.创建并清除每天清除访客终端组的终端策略。

- 导航到管理>身份管理>设置>终端清除
- 在Purge规则下,默认情况下,如果经过时间超过30天,则必须有一个触发访客终端删除的规则。
- 修改GuestEndpoints的现有策略或创建新策略(如果默认策略已删除)。请注意,清除策略在 定义的时间里每天运行。

在这种情况下,条件为已用天数小于1天的访客终端的成员

使用案例3:HostSpot门户

流概述

- 1. 无线用户连接到访客SSID。
- 2. WLC使用ISE作为AAA服务器,根据终端的MAC地址对终端进行身份验证。
- 3. ISE返回具有两个属性值对(AVP)的access-accept:url-redirect和url-redirect-acl。
- 4. 一旦WLC将此AVP应用于终端会话,该站点将转换为DHCP-Required,一旦它获取了IP地址 ,它将保留在CENTRAL_WEB_AUTH中。在此步骤中,WLC已准备好重定向客户端的 http/https流量。
- 5. 最终用户打开Web浏览器,一旦生成HTTP或HTTPS流量,WLC会将用户重定向到ISE热点门 户。
- 6. 进入门户后,系统会提示用户接受可接受的使用策略。
- 7. ISE将终端MAC地址(终端ID)添加到已配置的终端身份组。
- 8. 处理请求的策略服务节点(PSN)向WLC发出动态CoA类型Admin-Reset。
- 9. WLC处理完传入CoA后,会向客户端发出取消身份验证(连接丢失,客户端返回所需的时间很 长)。
- 客户端重新连接后,会创建新的会话,因此ISE端没有会话连续性。这意味着身份验证将作为 新线程处理。
- 11. 由于终端已添加到已配置的终端身份组,并且存在检查终端是否属于该组的授权策略,因此 新身份验证与此策略匹配。结果是对访客网络的完全访问权限。
- 12. 除非终端身份对象因终端清除策略而从ISE数据库中清除,否则用户不得再次接受AUP。

配置

- 1. 创建新终端身份组以在注册后将这些设备移动到。导航到工作中心(Work Centers)>访客接入 (Guest Access)>身份组(Identity Groups)>终端身份组(Endpoint Identity Groups),然后单击
- 输入组名称(本例中为HotSpot_Endpoints)。添加说明,无需父组。

Endpoint Identity	Endpoint Identity Group List > HotSpot_Endpoints							
Endpoint Identity Group								
* Name	HotSpot_Endpoints							
Description	Members of this group will accept AUP every week							
Parent Group								

2.定位至工作中心>访客访问权限>配置>访客门户>选择热点门户(默认)。

3.展开Portal Settings,然后在Endpoint Identity Group下**选择Endpoint** Identity Group下**的** HostSpot_Endpoints组。这会将注册设备发送到指定的组。

Endpoint	HotSpot_Endpoints					
identity	Configure endpoint identity groups at:					
group: *	Work Centers > Guest Access > Identity Groups					

4.**保存**更改。

5.创建在WLC发起的MAB身份验证时调用HotSpot门户的授权配置文件。

- 导航到Policy > Policy elements > Results > authorization > Authorization Profiles并创建一个 (HotSpotRedirect)。
- 选中Web redirection(CWA, MDM, NSP, CPP)后,选择Hot Spot,然后在ACL字段中键入 Redirect ACL名称(Guest_Redirect),并作为Value选择正确的门户(Hotspot Portal(default))。

Add New Standard Profi	le			
Authorization Profile				
* Name	HotSpotRedirect			
Description				
* Access Type	ACCESS_ACCEPT *			
Network Device Profile	🚓 Cisco 💌 🕀			
 Common Tasks 				
Voice Domain Permission	1			
Web Redirection (CWA, Hot Spot	MDM, NSP, CPP) () ACL Guest_Redirect Value Hotspot	Guest Portal (default) *		
Static IP/Host name	e/FQDN			
▼ Attributes Details				
Access Type = ACCESS_ACCEPT cisco-av-pair = url-redirect-acl=Guest_Redirect cisco-av-pair = url-redirect=https://lp:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw				

- 导航到Policy > Authorization并插入新规则。此规则是触发重定向过程以响应来自WLC的初始 MAC身份验证请求的规则。(在本例中称为Wireless_HotSpot_Redirect)。
- 在Conditions下选择Select Existing Condition from Library,然后在condition name下选择 Compound condition
- 在results下,选择Standard > HotSpotRedirect(在上一步中创建的授权配置文件)。然后单击
 完成并保存

7.创建第二个授权策略。

- 复制上述策略,修改其名称,因为这是终端从重新身份验证事件(称为 Wireless_HotSpot_Access)返回后触发的策略。
- 在Identity Group Details框中,选择Endpoint Identity Group,然后选择之前创建的组 (HotSpot_Endpoints)。
- 在Results下,选择**PermitAccess**。单击**Done**并**Save**更改。

~	Wireless_HotSpot_Access	if	HotSpot_Endpoints AND Wireless_MAB	then	PermitAccess
~	Wireless_HotSpot_Redirect	if	Wireless_MAB	then	HotSpotRedirect

8.配置清除策略,清除运行时间超过5天的终端。

- 导航到Administration > Identity Management > Settings > Endpoint Purge,然后在Purge rules下创建新策略。
- 在Identity Group Details框中,选择Endpoint Identity Group > HotSpot_Endpoints
- 在conditions下,单击Create New Condition(Advanced Option)。
- 在"选择属性"(Select Attribute)下选择"终端清除:已用天数"(ENDPOINTPURGE: ElapsedDays GREATERETHAN 5天)

HotSpot_Endpoints_PurgeRule if HotSpot_Endpoints AND ENDPOINTPURGE:ElapsedDays GREATERTHAN 5

验证

使用案例1

- 1. 用户连接到访客SSID。
- 2. 他打开浏览器,一生成HTTP流量,就会显示访客门户。
- 3. 访客用户验证并接受AUP后,将显示成功页面。
- 4. 重新验证CoA发送出去(对客户端透明)。
- 5. 终端会话将重新进行身份验证,具有对网络的完全访问权限。
- 6. 任何后续访客连接都必须通过访客身份验证,才能获得网络访问权限。

CISCO Sponsored Guest Portal

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:
Password:
Sign On
Don't have an account?

CISCO Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

CISCO Sponsored Guest Portal

Success

You now have Internet access through this network.

来自ISE RADIUS实时日志的流量:

1	0	t001	68:7F:74:72:18:2E	Windows7-Wo	Default >> MAB	Default >> Wir	PermitAccess	Ŷ	Accounting Start
~	0	t001	68:7F:74:72:18:2E	Windows7-Wo	Default >> MAB	Default >> Wir	PermitAccess		Re-Authentication Event
	0		68:7F:74:72:18:2E					$\langle $	CoA Event
~	0	1001	68:7F:74:72:18:2E						Guest Authenitcation Event
×	Q	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo	Default >> MA	Default >> Wir	CWA_Redirect	$\langle $	Initial MAB request

使用案例2

- 1. 用户连接到访客SSID。
- 2. 他打开浏览器,一生成HTTP流量,就会显示访客门户。
- 3. 访客用户验证并接受AUP后,设备即注册。
- 4. 系统将显示成功页面,并发送Re-authenticate CoA(对客户端透明)。
- 5. 终端会话将重新进行身份验证,具有对网络的完全访问权限。
- 6. 只要终端仍位于已配置的终端身份组中,就允许任何后续访客连接9s而不实施访客身份验证。

CISCO Sponsored Guest P	ortal
Sign On	
Welcome to the Guest Portal. Sign on with	the username and password provided to you.
	Username:
	Password:
	Sign On
	Don't have an account?

CISCO Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

Ξ

CISCO Sponsored Guest Portal

Welcome Message

Click **Continue** to connect to the network. You're very close to gaining network access.

Continue



来自ISE RADIUS实时日志的流量:

Reset Repeat Cou	nts				🔻 Filter 🗸 🔹 🗸		
Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group		
0	à	68:7F:74:72:1	68:7F:74:72:	PermitAccess		\bigvee	Accounting Start
۲	à	68:7F:74:72:1	68:7F:74:72:	PermitAccess	GuestEndpoints	$\langle $	Subsequent MAB request(no redirect to guest portal)
	à	hfr592	68:7F:74:72:	PermitAccess	User Identity Groups:GuestType_Contractor (default)	$\langle \rangle$	Re-Authentication Event
	à		68:7F:74:72:			$\langle $	CoA Reauth Event
	Q	hfr592	68:7F:74:72:		GuestType_Contractor (default)	\bigvee	Guest Authentication and Device Registration
	à	68:7F:74:72:1	68:7F:74:72:	CWA_DeviceRegistration	Profiled		Initial MAB request

使用案例3

- 1. 用户连接到访客SSID。
- 2. 他打开浏览器,一生成HTTP流量,就会显示AUP页面。
- 3. 访客用户接受AUP后,即注册设备。
- 4. 系统将显示成功页面,并发送Admin-Reset CoA(对客户端透明)。
- 5. 终端以完全访问网络的方式重新连接。
- 6. 只要终端保留在已配置的终端身份组中,就允许任何后续突风连接,而无需执行AUP接受(除 非另外配置)。

Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy:You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password.Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.Cisco Systems reserves the right to suspend the Service ifCisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party.Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.



Hotspot Portal

You have successfully connected to the network.

AireOS中的FlexConnect本地交换

配置FlexConnect本地交换时,网络管理员需要确保:

- 重定向ACL配置为FlexConnect ACL。
- 重定向ACL已作为策略应用通过AP自身在FlexConnect选项卡> External WebAuthentication ACLs > Policies >选择重定向ACL下并点击Apply

All APs > [Details for aaa	-ap-3				
General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
VLAN Su	pport 🔽					
Native VI	LAN ID 3	01 VL	AN Mappings			
FlexConn Name	nect Group Not	Configured				
PreAuthent	ication Access Co	ontrol Lists				
External \	WebAuthentication /	ACLS				
Local Spli	t ACLs					
Central D	HCP Processing					
Layerz Au	<u>els</u>					
Policies						
Dalian (
Policy P	ACL CWA_Re	direct 🔻				
	Add					
Policy Ad	ccess Contro	Lists				
CWA_Red	direct				-	

或者通过将策略ACL添加到FlexConnect组所属的(**Wireless > FlexConnect Groups >选择正确的组>** ACL Mapping > Policies选择重定向ACL并点击Add)

FlexConne	ect Groups > Edit 't	est'			
General	Local Authentication	Image Upgrade	ACL Mapping	Central DHCP	WLAN VLAN mapping
	AN-ACL mapping WL	AN-ACL mapping	Policies		
Policies Policy	ACL CWA_Redirect Add				
CWA_Re TOR_Re	direct				

添加策略ACL会触发WLC将配置的ACL向下推送到FlexConnect组的AP成员。否则会导致Web重定 向问题。

外部锚点方案

在自动锚点(外部锚点)场景中,必须强调以下事实:

- •需要在外部和锚点WLC上定义重定向ACL。即使仅在锚点上强制执行。
- 第2层身份验证始终由外部WLC处理。这在设计阶段(对于故障排除也很重要)非常重要,因为所有RADIUS身份验证和记帐流量都发生在ISE和外部WLC之间。
- 重定向AVP应用于客户端会话后,外部WLC通过移动切换消息更新锚点中的客户端会话。
- •此时,锚点WLC开始使用已预配置的重定向ACL实施重定向。
- 必须在锚点WLC SSID上完全关闭记账,以避免来自锚点和外部的指向ISE的记账更新(引用相 同的身份验证事件)。
- •基于URL的ACL在外部锚点场景中不受支持。

故障排除

AireOS和融合接入WLC上的常见断开状态

1. 客户端无法加入访客SSID

show client detailed xx:xx:xx:xx:xx:xx:xx显示客户端卡在START中。 通常,这是指示WLC无法应用 AAA服务器返回的属性。

验证ISE推送的重定向ACL名称与WLC上预定义ACL的名称完全匹配。

同样的原理适用于已配置ISE向下推送到WLC的任何其他属性(VLAN ID、接口名称、Airespace-ACL)。然后,客户端必须转换到DHCP,然后转换到CENTRAL_WEB_AUTH。

2. 重定向AVP已应用于客户端会话,但重定向不起作用

验证客户端的策略管理器状态为CENTRAL_WEB_AUTH,其中有效的IP地址与为SSID配置的动态 接口一致,并且重定向ACL和URL重定向属性已应用于客户端的会话。

重定向ACL

在AlreOS WLC中,重定向ACL必须明确允许不得重定向的流量,例如TCP端口8443上的DNS和 ISE两个方向,并且隐式deny ip any any any会触发其余的流量重定向。

在融合接入中,逻辑正好相反。拒绝ACE绕过重定向,而允许ACE触发重定向。这就是为什么建议 明确允许TCP端口80和443。

验证从访客VLAN通过端口8443对ISE的访问。如果从配置角度看一切正常,最简单的前进方法是获 取客户端无线适配器后面的捕获并验证重定向中断的位置。

- 是否发生DNS解析?
- •TCP三次握手是否已针对请求的页面完成?
- 客户端启动GET后,WLC是否返回重定向操作?
- •是否完成了通过8443与ISE的TCP三次握手?

3. 在ISE推送访客流结束时的VLAN更改后,客户端无法访问网络

一旦客户端在流开始时抓取了IP地址(Pre Redirect状态),如果发生Guest身份验证(CoA重新身份验证后)后推下VLAN更改,强制在访客流中进行DHCP释放/续约的唯一方法(无状态代理)是通过Java小程序,在移动设备中该小程序不起作用。

这会使客户端在VLAN X中保持黑洞,IP地址为VLAN Y。 规划解决方案时必须考虑这一点。

4. 在重定向期间,ISE在访客客户端的浏览器中显示"HTTP 500 Internal error, Radius session not found"消息

这通常是ISE上会话丢失的指示符(会话已终止)。最常见的原因是部署了外部锚点后,在锚点WLC上配置了记账。 要修复此在锚点上禁用记帐,并保留外部句柄Authentication and Accounting。

5. 客户端在ISE的热点门户中接受AUP后会断开连接并保持断开连接或连接到不同的SSID。

由于此流程中涉及的授权动态更改(CoA)导致WLC向无线站发出取消身份验证,因此在HotSpot中可 能会出现这种情况。大多数无线终端在取消身份验证后没有任何问题可返回到SSID,但在某些情况 下,客户端会连接到另一个首选SSID以响应取消身份验证事件。从ISE或WLC中无法进行任何操作 来阻止此过程,因为要由无线客户端将原始SSID粘贴或连接到另一个可用(首选)SSID。

在这种情况下,无线用户必须手动连接回热点SSID。

AireOS WLC

```
(Cisco Controller) >debug client
```

Debug client set to DEBUG a set involved in Client State Machine changes.

```
(Cisco Controller) >show debug
MAC Addr 1..... AA:AA:AA:AA:AA:AA:AA
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  dot1x states enabled.
  mobility client handoff enabled.
  pem events enabled.
  pem state enabled.
  802.11r event debug enabled.
  802.11w event debug enabled.
  CCKM client debug enabled.
```

调试AAA组件

(Cisco Controller) >debug aaa {events, detail and packets} enable 这可能影响资源,具体取决于通过MAB或Dot1X SSID连接的用户数量。 DEBUG级别的这些组件 记录WLC和ISE之间的AAA事务,并在屏幕上打印RADIUS数据包。

如果ISE无法提供预期属性,或者WLC无法正确处理这些属性,则这一点至关重要。

Web-Auth redirect

(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa

这可用于检验WLC是否成功触发重定向。以下示例说明了从调试中重定向必须是什么样子:

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*typ://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050

NGWC

Debug client set to DEBUG a set involved in Client State Machine changes.

3850#debug client mac-address <client MAC> 此组件在屏幕上打印RADIUS数据包(身份验证和记帐)。当您需要验证ISE是否提供正确的AVP以 及验证CoA是否正确发送和处理时,这非常方便。

3850#debug radius

这将涉及无线客户端的所有AAA过渡(身份验证、授权和记帐)。这对于验证WLC正确解析AVP并 将其应用于客户端会话至关重要。

3850#debug aaa wireless all 当您怀疑NGWC上存在重定向问题时,可以启用此功能。

3850#debug epm plugin redirect all 3850#debug ip http transactions 3850#debug ip http url

ISE

RADIUS实时日志

验证初始MAB请求已在ISE中正确处理且ISE回推预期属性。导航到**操作> RADIUS >实时日志**,并 使用**终端ID**下的客户端MAC过滤输出。找到身份验证事件后,单击详细信息,然后验证作为接受的 一部分推送的结果。

Jul 🗹 🚺	68:7F:74:72:18:2E 68:7F:74:72:18:2E GuestSSO_Portal	Cisco_5508
Result		
UserName	68:7F:74:72:18:2E	
User-Name	68-7F-74-72-18-2E	
State	ReauthSession:0e249a0500000682577ee2a2	
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120	
cisco-av-pair	url-redirect-acl=TOR_Redirect	
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal /gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648	a2-11e6- 533fea

TCPDump

此功能可用于深入研究ISE和WLC之间的RADIUS数据包交换。这样,您可以证明ISE在accessaccept中发送正确的属性,而无需在WLC端启用调试。要使用TCDump启动捕获,请导航到**操作 >故障排除>诊断工具** >常规工具> TCPDump。

这是通过TCPDump捕获的正确流的示例

Source	Destination	Protocol	Length	Info
154.5	157.1 3	RADIUS	299	Access-Request(1) (id=0, 1=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	.157.13	RADIUS	340	Accounting-Request(4) (id=8, 1=298)
.157.13	11100 .154.5	RADIUS	62	Accounting-Response(5) (id=8, 1=20)
.157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, 1=202)
154.5	.157.13	RADIUS	80	CoA-ACK(44) (id=1, 1=38)
.154.5	.157.13	RADIUS	299	Access-Request(1) (id=1, 1=257)
.157.13	.154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

以下是响应初始MAB请求而发送的AVP(以上屏幕截图中的第二个数据包)。

```
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: fleaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
AVP: l=55 t=Class(25): 434143533a306532343961303530303030616130353536...
AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
```

```
AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
VSA: l=189 t=Cisco-AVPair(1): url-
redirect=https://ise2la.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal
=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
```

终端调试:

如果您需要深入了解涉及策略决策、门户选择、访客身份验证的ISE流程,CoA处理此问题的最简单 方法是启用Endpoit Debugs,而不必将完整组件设置为调试级别。

要启用此功能,请导航到操作>故障排除> DiagnosticTools > General Tools > EndPoint Debug。

Overview							
Event	5200 Authentication succeeded						
Username	00:24:97:BA:84:81						
Endpoint Id	00:24:97:BA:84:81 ⊕ Endpoint Debug	_					
Endpoint Profile	Cisco-Device	_					
Authentication Policy	Default >> MAB >> Default						
Authorization Policy	Default >> Wireless_CWA_RedirectSSO						
Authorization Result	GuestSSO_Portal						

进入终端调试页面后,输入终端MAC地址,并在准备重新创建问题时点击start。

Endpoint Debug
Status:
Status. Stopped Start
MAC Address () IP 68:7F:74:72:18:2E ()
Automatic disable after 10 Minutes (1)

调试停止后,单击标识终端ID的链接以下载调试输出。

Endpoint Debug				
Status:	Processing	Stop		
 MAC Address IP Automatic disable after 	68:7F:74:72:18:2E	(i)		
			Se	elected 0 Total 1
XDelete Files efresh				
File Name	 Host Name 	Modified Da	te Size (Bytes)	
68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448	

相关信息

TAC推荐的AireOS版本

思科无线控制器配置指南,版本8.0。

<u>思科身份服务引擎管理员指南,版本2.1</u>

带身份服务引擎的通用NGWC无线配置

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)。