Aruba Clearpass 与 Meraki AP 结合 实现 Web 认证

	512
\mathbf{H}	12

第一章	Meraki 设置(摘取自网络)	3
第二章	ClearPass Policy Manager 设置	7
第三章	ClearPass Guest 设置	12
第四章	Mac+WebAuth 流程	18

第一章 Meraki 设置(摘取自网络)

(1) 创建 SSID,选择启用,然后单击编辑设置



(2) 后续部分配置

- a. Association requirements: *MAC-based access control (no encryption)
- b. Splash page: *Cisco Identity Services Engine (ISE) Authentication
- c. RADIUS servers: *<IP of the ClearPass Server(s)> port: 1812 and the secret you put in for your Meraki APs in the Network Devices of the ClearPass server
- d. RADIUS testing: *RADIUS testing enabled
- e. RADIUS CoA support: *RADIUS CoA enabled
- f. RADIUS attribute specifying group policy name: *Aruba-User-Role
- g. RADIUS accounting: *RADIUS accounting is enabled
- h. RADIUS accounting servers: *<IP of the ClearPass Servers> port 1813 and the secret you put in for your Meraki APs in the Network Devices of the ClearPass server
- i. RADIUS proxy: *Do not use Meraki proxy
- j. Assign group policies by device type: (Whatever your network requires here) I chose: Disabled: do not assign group policies automatically
- k. Walled garden: *Walled garden is enabled: Put your IPs of the ClearPass servers/floating IPs.
- I. Client IP assignment: Bridge mode: Make clients part of the LAN
- m. VLAN tagging: *(If your guest/employee/etc network requires VLANS put your VLAN in here)
- n. RADIUS override: Ignore VLAN attribute in RADIUS responses (This is what I' m using, for more advanced setups you can choose to enable this)
- o. Content filtering: Whatever your network requires
- p. Bonjour forwarding: Disable Bonjour Forwarding (Whatever your network requires)
- q. Mandatory DHCP: (Whatever your network requires)
- r. Band selection: (Whatever your network requires)
- s. Minimum bitrate (Mbps): (Whatever your network requires)

Access control

SSID: Guest-CPPMTest v

Network access										
Association requirements	O Open (no encryption) Any user can associate									
	O Pre-shared key (PSK) Users must enter a pa	Pre-shared key (PSK) Users must enter a passphrase to associate								
	MAC-based access of RADIUS server is que	MAC-based access control (no encryption) RADIUS server is queried at association time								
	O Enterprise with Mera User credentials are v	ki Cloud Authen validated with	tication 🧹 802.1X at association time							
	O Identity PSK with RAI RADIUS server is que	DIUS ried at associ	ation time to obtain a passphrase	e for a device ba	sed on its M	AC address				
Splash page	O None (direct access) Users can access the	network as s	oon as they associate							
	O Click-through Users must view and	acknowledge	your splash page before being a	allowed on the ne	etwork					
	O Sponsored guest logi Guests must enter a v	in valid sponsor	email and own email address be	fore being allowe	ed on the ne	twork				
	O Sign-on with Meraki Users must enter a us	Cloud Authentic sername and p	ation 🧹	on the network						
	O Sign-on with SMS Au Users enter a mobile After a trial period of	uthentication phone numbe 25 texts, you	er and receive an authorization co will need to connect with your Ty	ode via SMS. wilio account on	the <u>Network</u>	-wide settings page.				
	Cisco Identity Service Users are redirected	es Engine (ISE to the Cisco IS) Authentication ① SE web portal for device posturin	ng and guest acc	ess					
	O Systems Manager Se	ntry enrollmer	nt 🕲							
RADIUS servers	# Host	Port	Secret		Actions					
	1	1812	•••••	۹	÷Χ	Test				
	2 Add a server	1812	******	P	÷Χ	Test				
RADIUS testing	RADIUS testing enabled v]								
RADIUS CoA support 📵	RADIUS CoA enabled									
RADIUS attribute specifying group policy name	Aruba-User-Role	0								
RADIUS accounting	RADIUS accounting is enable	ed 🗸								
RADIUS accounting servers	# Host	Port	Secret		Actions					
		1813	*******	٩	$\oplus \; X$					
	2	1813	•••••	٩	ψX					
	Add a server									
RADIUS proxy 📵	Do not use Meraki proxy 👳									
Assign group policies by device type	Disabled: do not assign grou	p policies autor	natically v							
Walled garden 🕚	Walled garden is enabled	-								
Walled garden ranges	132									
	/32									
	/32 1/32 2/32		4							

Addressing and traf	he design of the second s								
Client IP assignment	NAT mode: Use Meraki DHCP								
	Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID frewall settings permit.								
	Intrige mode: Make clients part of the LAN Merials devices operate transparently (no NAT or DHCP). Weeless clients will receive DHCP leases from a server on the LAN or use static IPs. Use this for wireless clients requiring seamless roaming, shared printers, file sharing, and writeless cameras.								
	O Layer 3 reaming Clients receive DHCP leases from the LAN or use static IPs, similar to bridge mode. If the client roams to an AP where their original IP subnet is not available, then the client's traffic will be forwarded to an anchor AP on their original subnet. This allows the client to keep the same IP address, even when traversing IP subnet boundaries.								
	O Layer 3 transing with a concentrator Clients are humeled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.								
	VPN: turnel data to a concentrator Meraki devices send traffic over a secure tunnel to an MX concentrator.								
	Note: VFN and Layer 3 roaming with concentrator require an MX. Add an MX to use them.								
VLAN tagging (1) Bridge mode and layer 3 roaming only	Line VLAN tagging v								
VLAN ID ()	AP tags VLAN ID Actions								
	All other APs 9								
	Add VLAN								
RADIUS override	Ignore VLAN attribute in RADUS responses 🖉								
Content filtering () NAT mode only	Don't filter content								
Bonjour forwarding () Bridge mode and layer 3 roaming only	Deate Borjour Forwarding 👦								
Mandatory DHCP ()	Enable Mandatory DHCP								
Wireless option	15								
1									
Band select	on and minimum bitrate settings may be overridden by RF profiles. Go to RF Profiles								
Band selection	O Dual band operation (2.4 GHz and 5 GHz)								
	 5 GHz band only 5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it. 								
	Dual band operation with Band Steering Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.								
Minimum bitrate (Mb	ps) Lower Density Higher Density								
	0								
	802.11a/b/g/n/ac devices supported								
	Save Changes or cancel								
	(Please allow 1-2 minutes for changes to take effect.)								

(3) 在防火墙和流量整形中,选择您的环境所需的内容。这不会影响 ClearPass 服务器(除非您出于某种原因阻止对服务器的访问)

Firewall & traffic shaping

SSID: Guest-CPPMTest	~]						
Block IPs and ports Layer 2 LAN isolation	Disabled	(br	idge mode	only)				
Layer 3 firewall rules ()	# Pol	licy	Protocol	Destination	Port	Comment	Actions	
	De	ny 🗸	Any	Local LAN	Any	Wireless clients accessing LAN		
	Allo	w	Any	Any	Any	Default rule		
	Add a la	ayer 3	firewall rule					
Block applications ar	nd cont	tent o	ategorie	es				
Layer 7 firewall rules	There a	re no r	ules defined	d for this SSID.				
	Add a la	ayer 7	firewall rule					
DNS layer protection (Cisco Umbrella)	Enable	Umbre	ella protecti	on				
Route DNS requests								
DNS and deny DNS								
Umbrella policies.								
Traffic shaping rules								
Per-client bandwidth limit	2 Mbps	_	details	Enable S	SpeedB	urst		
Per-SSID bandwidth limit	5 Mbps		details					
Shape traffic	Don't sha	ape traffi	c on this SSIE					

(4) 对于 Splash 页面,这将显示为灰色。你将无法改变任何事情

Splash page
SSID: Guest-CPPMTest
Splash pages on this SSID are disabled because this SSID is configured to dynamically redirect users based on the authorization profile and captive portal configuration on the Cisco ISE server. You can change this setting on the <u>access control subtab</u> .
Official themes @
Modern NEW
○ Fluid
Custom themes (9)
Copy of Modern
Create something new
Custom splash URL
O or provide a URL where users will be redirected: https://clearpass.uiu.edu/guest
What is this?
Customize your page

(5) 根据您的环境要求设置其余的无线部分。本节中没有 ClearPass 设置。

(6) 转到 Network-wide -> Group policies

a.您需要设置与您在 ClearPass 中为设备配置文件设置的 Role 相对应的 Group policies Name。

b.可以设置 Employee 和 Contractor 角色。与 ClearPass 上 Role 配合,本功能未测试。

Group policies								
Name	Affecting	Bandwidth	VLAN ()	Splash ()	Bonjour	Traffic	Actions	
Employee	1 clients	Default	VLAN 9	Default	Default	Default	Clone X	
Contractor	0 clients	Default	VLAN 9	Default	Default	Default	Clone X	
Add a group								
© 2020 Cisco Systems, Inc. Privacy - Terms		Last log C Data for	gin: <u>3 days ago</u> from your current IP add Current session started: <u>5 minutes ago</u> r this organization is hosted in <u>North Am</u>	iress erica			Make a wish	

第二章 ClearPass Policy Manager 设置

- 1) 确保您的 Meraki 接入点与 ClearPass 能互相通信,并带有两边设置的相应的 RADIUS 密 钥。
- 2) 本次测试涉及到两个服务。为了方便识别,我们在服务前面添加了对应的标识字段,比 如 Meraki-Wireless,就像下面的例子一样。

5.	5	Meraki-Wireless-MAC Authentication	RADIUS	MAC 身份验证	2667	0
6. 0	6	Meraki-Wireless-CaptivePortal-Webauth	WEBAUTH	基于 Web 的身份验证	13	0
	a)	您需要创建一个强制	制配置文件,可	以配置对应的 Role	相关的强制领	策略, 与
		Merike Group policie	es 配置 Name 保	持一致,本次全访	客网络不涉及	& 此配置
Enforce	ement Pi	ofiles - TEST-Meraki-Wi	eless-Employee De	vice Profile		
			Note: Th	is Enforcement Profile is creat	ed by Service Templa	te
Summar	ry Profile	Attributes				
Profile:						
Inmes		TECT Maraki Windoos Employe	e Device Profile			
lame:		TEST-Meraki- wireless-Employe				
escription	n:	Role/VLAN enforcement for Em	bloyee			
lescription Type:	n:	Role/VLAN enforcement for Em	oloyee			
Vame: Description Fype: Action:	n:	Role/VLAN enforcement for Employee Role/VLAN enforcement for Emp RADIUS Accept	oloyee			
Varrie: Description Type: Action: Device Gro	n: oup List:	Role/VLAN enforcement for Em RADIUS Accept	bloyee			
Description Type: Action: Device Gro	n: oup List: s:	Role/VLAN enforcement for Em Role/VLAN enforcement for Em RADIUS Accept	loyee			
Contention Contention Contention: Contention	n: oup List: s: /pe	Role/VLAN enforcement for Em RADIUS Accept -	Nome		Value	
Action: Oevice Gro Action: Device Gro Attributes Ty 1. Rai	n: oup List: s: pe dius:Aruba	Role/VLAN enforcement for Em RADIUS Accept	oloyee Name Aruba-User-Role		Value = Employee	

b) 您需要创建一个强制配置文件,将认证用户做一个1周的MAC Caching (缓存 时间自定义)

配置

配置 > 强制 > 配置文件 > Edit Enforcement Profile - YST-Guest Guest MAC Caching 强制配置文件 - YST-Guest Guest MAC Caching								
				ĩ	主意:此强制配置文件由服务模	板创建		
摘要	配置文件	属性						
配置文	(件:							
名称:			YST-Guest Guest MAC Caching					
描述:			来宾的端点属性更新					
类型:			Post-Authentication					
操作:								
设备组	1列表:		2					
属性:								
	类型		名和	称			值	
1.	Endpoint		Use	ername		=	%{Authentication:Username}	
2.	Endpoint		Gue	uest Role ID		=	%{GuestUser:Role ID}	
3.	Endpoint		MA	AC-Auth Expiry		=	%{Authorization:[Time Source]:One Week DT}	

c) 您需要创建一个强制配置文件,将用户重定向到您创建的访客门户。

配置	»强制 » 配置文(* Edit Enforcement Profile - Meraki-Wireless-Redirect		
强制	訓配置文件 -	Meraki-Wireless-Redirect		
103	配置文件	属性		
配置文	文件:			
名称:		Meraki-Wireless-Redirect		
描述:				
类型:		RADIUS		
操作:		Accept		
设备组	组列表:	-		
属性:				
-	类型	名称		值
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https:// `al_meraki.php? switchip=%{Connection:NAD-IP-Address}&mac=%{Connection:Client-Mac- Address-NoDelim}

Meraki AP 不支持在 AP 上定义 URL, 需要通过 Radius 属性内带 URL 给 Meraki AP 弹 Portal。 格式如下:

(url-redirect=https://<ClearPassURL or

IP>/guest/<Guest-Page>.php?switchip=%{Connection:NAD-IPAddress}&mac=%{Connection:Client -Mac-Address-NoDelim})

d) 您需要创建一个强制配置文件来终止会话,此配置用于改变用户状态,让客户 端重新发起认证请求。

配置	記置 > 强制 > 配置文件 > Edit Enforcement Profile - Meraki-Wireless-terminate session							
强制	强制配置文件 - Meraki-Wireless-terminate session							
摘要	配置文件 属性							
配置力	5件:							
名称:		Meraki-Wireless-terminate sessio	n					
描述:								
类型:		RADIUS_DynAuthZ						
操作:		CoA						
设备组	设备组列表:							
属性:								
	类型	名	称		值			
1.	Radius: IETF	Ca	alling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}			
2.	Radius:IETF	Ad	ct-Session-Id		%{Radius:IETF:Acct-Session-Id}			
3.	Radius: IETF	E	ent-Timestamp	=	%{Radius:IETF:Event-Timestamp}			

3) 您还需要创建两个执行策略。

配置 » 强制 » 茶館 强制決略 ClearPass 通过评估与服务关联的强制策略未控制网络访问。		 ➡ 添加 ▲ 导入 ▲ 全部导出
筛进器:名称	执行 清除筛选器	显示 20 💙 记录
#	类型 描述	
1.	RADIUS	
2.	WEBAUTH	
正在显示 1-2 个, 共 2 个	8	開き、「「「「「」」」

配置 » 强制 » 策略 » 编辑 - Meraki-Wireless-MAC Authentication Enforcement Policy 强制策略 - Meraki-Wireless-MAC Authentication Enforcement Policy

JE UJ X		Teruk	i wireless like Autre	indication Enrorcement Policy	
摘要	强制	规则			
强制:					
名称:			Meraki-Wireless-MAC Authen	tication Enforcement Policy	
描述:					
强制类型:			RADIUS		
默认配置文	件:		[Deny Access Profile]		
规则:					
规则评估算	法:		First applicable		
Cond	litions			Actions	
1. [MAC C	Role	MATCHE	S_ALL [User Authenticated]	[Allow Access Profile]	
2. [Contra [Emplo [Guest	:Role / actor] oyee]	MATCHE	S_ANY [Other]	Meraki-Wireless-Redirect	

 記置 » 强制 » 策略 » 编辑 强制策略 - Merak 23 23 34 34 34 	- Meraki-Wireless-Webauth ki-Wireless-Webauth	
强制:		
名称:	Meraki-Wireless-Webauth	
描述:		
强制类型:	WEBAUTH	
默认配置文件:	Meraki-Wireless-terminate session	
规则:		
规则评估算法:	First applicable	
Conditions		Actions
1. (Tips:Role EQUALS	[User Authenticated])	Meraki-Wireless-terminate session, YST-Guest Guest MAC Caching

1. (Tips:Role EQUALS [User Authenticated])

4) 您需要创建一个角色映射

配置»身份»角色映	射 » 编辑 - YST-Guest MAC Authentication Role Mapping		
角色映射 - YS	T-Guest MAC Authentication Role Mapping		
	注意:此角色映射策略由服务模板创建		
摘要 策略 映	射规则		
策略:			
策略名称:	YST-Guest MAC Authentication Role Mapping		
描述:			
默认规则:	[Other]		
映射规则:			
规则评估算法:	Evaluate all		
Conditions		Role Name	
1. (Authorization: AND (Author	[Endpoints Repository]:Unique-Device-Count EXISTS) rization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry})	[MAC Caching]	
2. (Endpoint:Gue	st Role ID EQUALS 1)	[Contractor]	
3. (Endpoint:Gue	st Role ID EQUALS 2)	[Guest]	
4. (Endpoint:Gue	st Role ID EQUALS 3)	[Employee]	

5) 您需要创建两个服务

a. Meraki-Wireless-MAC Authentication

_	a procession and			
摘要	服务 身份验证	授权 角色 强制 记帐代理		
服务:				
名称:		Meraki-Wireless-MAC Authentication		
描述:		基于 MAC 的身份验证服务		
类型:		MAC 身份验证		
状态:		Enabled		
监视模	lyt:	Disabled		
更多选	;项:	1. 授权 2. 记帐代理		
			服労规则	
匹配以	下所有条件:			
	类型	88	运 具符	1
1.	Connection	Client-Mac-Ad	dress EQUALS	%{Radius:IETF:User-Name}
	Connection	5510	CONTAINS	100
身份验	证:			
身份验	(证方法:	[Allow All MAC AUTH]		
身份验	证源:	[Endpoints Repository] [Local SQL DB]		
去除用	沪名规则:	•		
授权:				
授权详	细信息:	1. [Time Source] [Local SQL DB] 2. [Guest User Repository] [Local SQL DB] 3. [Local User Repository] [Local SQL DB]		
角色:				
角色缺	射策略:	-Guest MAC Authentication Role Mapping		
强制:				
使用缓	存的结果:	Disabled		
强制策	略:	Meraki-Wireless-MAC Authentication Enforcement Po	icy	
	COTRINES.			11 M 42 12 12

Л	复制	保存	取消	

1049 11255	自伤检证 振权 角色 强制 记帐代理					
名称:	Meraki-Wireless-MAC Authentication					
苗述:	基于 MAC 的身份验证服务	p				
6型:	MAC 身份验证					
大志:	Enabled					
被模式:	□ 启用以监视无强制的网络访问					
1多选项:	☑ 授权 □ 审核终端主机 □ 分析媒	㎞ ☑ 记帐代理				
			服务规则			
□配 ○ 任何司	以下所有条件:					
类型		名称	运算符	<u>(i</u>		
1. Conn	ection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	Ra	*
2. Conn	ection	SSID	CONTAINS		Ba	8
3. Click	to add					

配置»服务»编唱 - Meral	ki-Wireless-MAC Authentication	
服务 - Meraki-Wi	reless-MAC Authentication	
論要 服务 身份绘证	授权 角色 强制 记帐代理	
身份验证方法:	[Allow All MAC AUTH]	上版 ;
	Select to Add	
身份验证源:	[Endpoints Repository] [Local SQL DB]	上版 :
	Select to Add	
去餘用戶名規则:	□ 启用以指定用于去除用户名前缀或后缀的	逗号分開的规则列表

論要 服祭 自何助证	1517 66 3331 记能任用	
授权详细信息:	用于获取角色映射操性的授权源(针对每个身份验证源)	
	身份检证源	屬性的获取来源
	1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]
	用于获取角色缺射圈性的耳他授权源。	
	Time Source] [Local SQL DB] [Guest User Repository] [Local SQL DB] [Local User Repository] [Local SQL DB]	36008H
	-Select to Add-	

配置 » 服务	·» 编辑 - Meraki-	-Wireless-MAC Authentication		
服务 - 1	Meraki-Wire	eless-MAC Authentication		
油亚	网络 身份给证	授权 角色 强制 记帐代理		
角色映射策	略:	YST-Guest MAC Authentication Role Mapping v 修改		添加新的角色映射策略
			角色映射策略详细信息	
描述:				
默认规则:		[Other]		
规则评估算	法:	evaluate-all		
\$	#		角色	
1. (A	uthorization:[En ND (Authorizat	<pre>idpoints Repository]:Unique-Device-Count EXISTS) tion:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry})</pre>	[MAC Caching]	
2. (E	ndpoint:Guest R	tole ID EQUALS 1)	[Contractor]	
3. (E	ndpoint:Guest Re	ole ID EQUALS 2)	[Guest]	
4. (E	ndpoint:Guest Re	tole ID EQUALS 3)	[Employee]	

配置	» 服务 » 编辑 - Merak	ki-Wireless-MAC Authentication				
服务	5 - Meraki-Wir	reless-MAC Authentication				
拍卖	医服务 身份验证	授权 角色 强制 记帐代理				
使用领	爱存的结果:	□ 使用先前会话中缓存的角色和状况属性				
强制争	6略 :	Meraki-Wireless-MAC Authentication Enforcement Policy	✔ 修改			添加新的强制策略
				强制策略详细信息		
描述:						
默认喜	記攬文件:	[Deny Access Profile]				
规则证	平估算法:	first-applicable				
	条件				强制配置文件	
1.	(Tips:Role MAT	CHES_ALL [User Authenticated]			[Allow Access Profile]	
2.	(Tips:Role MAT [Contractor] [Employee] [Guest])	CHES_ANY [Other]			Meraki-Wireless-Redirect	

b. Meraki-Wireless-CaptivePortal-Webauth

論要 服务 身份检证	E 授权 角色 强制			
服务:				
名称:	Meraki-Wireless-CaptivePortal-Webauth			
描述:				
类型:	基于 Web 的身份验证			
状态:	Enabled			
监视模式:	Disabled			
更多选项:	授权			
		8	务规则	
匹配以下任何条件:				
类型	名称		运算符	<u>۵</u>
1. Host	Check	Туре	MATCHES_ANY	Authentication
身份验证:				
the first and how have				

STUTELAL:	
身份验证源:	[Guest User Repository] [Local SQL DB]
去除用户名规则:	-
授权:	
授权详细信息:	1. [Local User Repository] [Local SQL DB] 2. [Time Source] [Local SQL DB] 3. [Endpoints Repository] [Local SQL DB]
角色:	
角色映射策略:	YST-Guest User Authentication with MAC Caching Role Mapping
强制:	
使用缓存的结果:	Disabled
强制策略:	Meraki-Wireless-Webauth

配置 » 服务 » 鏡眉 - Meraki-Wireless-CaptivePortal-Webauth 服务 - Meraki-Wireless-CaptivePortal-Webauth

100,75	<u>mcm</u> melaki wileless captiver of all webduth							
摘要	服务 身份验证	授权 角色 强制						
名称:		Meraki-Wireless-CaptivePortal-Webauth						
描述:			A					
类型;		基于 Web 的身份验证						
状态:		Enabled						
监视模	式:	□ 启用以监视无强制的网络访问						
更多选	Ø;	☑ 授权 □ 状况合规性						
				服务规则				
匹配 🤇	四記 🖲 任何成 〇 以下所有条件:							
	类型		名称	运算符	<u>a</u>			
1.	Host		CheckType	MATCHES_ANY	Authentica	tion	Ba	*
2.	Click to add							

1000					
摘要 服务 身份给证	授权 角色 强制				
身份验证源:	[Guest User Repository] [Local SQL DB]	上 55 : 下 55 : 期 38 徵君(1) 48(点)章 例 32			添加新的身份验
	Select to Add	~			

協委 服务 自构论证	海辺 角色 強制					
調査 調告 対け加加						
	身份验证票	關性的获取来源				
	1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]				
	TO T PARTY A REAL PRIMATE CONTRACTOR					
	用于软收用包裹的属性的具态投放。 Il ocal Liser Repositon II ocal SOL DB1	·潘加斯伯				
	[Time Source] [Local SQL DB]					
	[Endpoints Repository] [Local SQL DB]					
	Select to Add					
置»服务»编组-Mera 夏务-Meraki-Wi 擴要 服务 身份编证	ki-Wireless-CaptivePortal-Webauth reless-CaptivePortal-Webauth					
9色映射策略:	YST-Guest Liser Authentication with MAC Caching Role Mapping	添加新聞				
		● 鱼色地动等跳过带的皮				
祗:		17 mars (15%), i and 1 definition				
状认规则:	[Other]					
舰则评估算法:	evaluate-all					
条件		角色				
(GuestUser:Role	ID EQUALS 1)	[Contractor]				
(GuestUser:Role	ID EQUALS 2)	[Guest]				
(Guestuser:Role	ID EQUALS 3)	[Employee]				
2置 > 服务 > 编组 - Mi	raki-Wireless-CaptivePortal-Webauth					
記置 » 服务 » 编辑 - Me 服务 - Meraki-V	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth					
記言 > 服务 > 編組 - Ma 服务 - Meraki-V 梅香 解教 白田省	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 時期9月前後の1984					
記雪。服务。编组-Mu 服务 - Meraki-V 論要 服务 身份指 由印度在2004年。	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 谜 微松 命合 名紙					
2回。服务。编组-M 服务 - Meraki-V 論要 服务 身份指 E用缓存的结果: admifititi	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 通 現紀 角色 容易 回 使用影响会话中语学习的自己以及课程					
2置。服务。编组-M 限务 - Meraki-V 論要 服务 身份器 即爆行的结果: 副消略:	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 經 現紀 指命 電話 @ 使用先期全話中提示的角色的状況調性 [Meraki-Wieless-Webauth 》 (新文	765087				
2回 > 服务 > 编组 - M 很务 - Meraki-l 编章 服务 身份 用模符的标果: 趣简编:	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 延 接致 角色 33 @ 使用作助金法中展升的角色和优况属性 [Meraki-Wireless-Webauth 文 備文	按2008年 强制师能详细信念				
2 ※服务 ※編组 - Mu 服务 - Meraki-V 相様 離 第 身份報 相様存的体現: 細糖菌略: 副誌:	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 種 現极 角色 祭師 回日月500余活中等行的角色和状况课性 Meraki-Wireless-Webauth 《 新文	运动和能祥相约:8				
2回 ※服务 ※領田 - M 股务 - Meraki-	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 通 現紀 角色 934 @ @用》加合這中培行的角色成状況現在 [Meraki-Wireless-Webauth ~) (新文 Meraki-Wireless-terminate session	15038 2008				
 2回 ※ 服务 ※ 範田 - PA 2回 ※ 服务 ※ 範田 - PA 2回 ● ● ● ● ● ● ● ● ● ● ● ● 2回 ● ● ● ● ● ● ● 2回 ● ● ● ● 2回 ● ● ● 2回 ● ● 2回 ● ● 2回 ●	raki-Wireless-CaptivePortal-Webauth Vireless-CaptivePortal-Webauth 經 現紀 前後 高級 @ 使用先期全話中提供的時能加於記篇性 [Meraki-Wireless-Webauth 》	沒如你能详细公会				

第三章 ClearPass Guest 设置

由于 Meraki 不支持 Post 的方式提交表单,来做 Portal 认证。目前测试下来 Meraki 支持 MAC+WEBAuth 的方式认证。

WEBAuth 表单提交的是给 Clearpass 的, Clearpass 内置 Portal Html 字段都已 经配置在内,因此无需定制开发,但是,如果客户想自定义 Portal 需要我们自 己写 Html 脚本。

如何找到需要的字段呢?

ClearPass Guest 内置 Portal 是已经可以认证的界面,因此我们只需要抓取内置 Portal 的交互就可以。



打开浏览器开发者模式,打开 Portal 页面提交一次正常的认证,就可以看到内置 Portal 提交了哪些数据上去。后续提交给开发就可以把这个界面做出来。

1) ClearPass Guest 内置 Portal

创建一个新的"WEB 登入"页面,随意命名。红色框部分需要注意,按照 Meraki 无线要求调整。

主页 » 配置 » 页面 » Web 登录					
Web 登录 (new)					
使用此表单创建新的 We	2 <i>b 登录</i> 。				
	Web 登录编辑器				
* 名称:	Meraki-Local 输入此 Web 登录页面的名称。				
页面名称:	Meraki-Local2 为此 Web 登录输入页面名称。 Web 登录可从"/guest/page_name.php"进行访问。				
描述:	有关 Web 登录的注释或描述性文本。				
* 供应商设置:	Cisco Systems 选择一组适合标准网络配置的预定义设置。				
登录方法:	服务器发起 - 更改发送给控制器的权限(RFC 3576) > 选择如何处理用户的网络登录。 服务器发起的登录要求提供用户的 MAC 地址,通常来自于强制网络门户重定向过程。				
登录表单 用于指定登录表单的行为和[内容的洗顶.				
身份验证:	● 「先据 - 需要用户名和密码 ✓ 选择身份验证要求。 **访问代码"需要输入单个代码(用户名)。 **适名"公许仅需要条款或"登录"按钮的空白表单。需要预先存在的帐户。 **适名"名"以、但页面将自动提交。 *访问代码"和"置名"要求帐户必须设置"用户名身份验证"字段。				
自定义表单:	□ 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。				
自定义标签:	夏盖默认标签和错误消息 如果选定,您将能够更改当前登录表单的标签和错误消息。				
用户名后缀:	将登录表单提交到 NAS 之前,后缀将自动附加到用户名。				
* 身份验证前检查:	无 - 不进行额外检查 选择在继续 NAS 身份验证之前应如何检查用户名和密码。				
条款:	需要确认条款和条件 如果选中,将会强制用户接受"条款和条件"复选框。				
CAPTCHA:	无 ✓ 选择 CAPTCHA 模式。				

重定向必须配置,但是 URL 可以随意填写

强制网络 强制网络	約门户 約一戶检测属性	
	阻止 CNA:	□ 启用绕过 Apple Captive Network Assistant Apple Captive Network Assistant (CNA)是在连接具有强制网络门户的网络时显示的弹出式浏览器 注意,此选项可能不适用于所有供应商,这取决于如何实施强制网络门户。
CAPPOI	RT Venue URL:	输入可选 URL 以作为 CAPPORT RFC-8908 的 Venue Info URL 发送。 https://www.rfc-editor.org/rfc/rfc8908.html
默认目标	<u>,</u>	
用于控制	客戶端住登录后将3	皇王问到的目标的选项。
	* 默认 URL:	www.baidu.com 输入要将客户端重定向到的默认 URL。 请确保在任何外部域的前面追加 "http://"。
	覆盖目标:	☑ 强制所有客户端的默认目标 如果选中,无论客户端的默认目标值如何都会将其覆盖。
<mark>登录页</mark> 用于控制	登录页外观和感觉的	的选项。
	* 皮肤:	Galleria Skin ✓ 选择显示此 Web 登录页面时要使用的皮肤。
	标题:	要在 Web 登录页上显示的标题。 留空以使用默认值(登录)。
	页眉 HTML:	[inwa_cookiecheck] {if \$statusCode == 1} {nwa_icontext type=info} You are already logged in. No further action is required on your part. {/nwa_icontext} {elseif \$statusCode == 2} {nwa_icontext type=warn} You are not configured to authenticate against web portal. No further action is required on your part. {/nwa_icontext} {elseif \$statusCode == 3} {nwa_icontext type=error} [插入 在登录表单之前显示的 HTML 模板代码。
	页脚 HTML:	<pre>{nwa_text id=7979} Contact a staff member if you are experiencing difficulty logging in. {/nwa_text}</pre>

这个登入延迟必须写,建议5秒以上。

	//nwa_text;
登录消息:	
	插入 ✓
	进行登录尝试时显示的 HTML 模板代码。
* 登录延迟:	[10] 显示登录消息时的延迟时间(秒)。
云标识 可选择向来宾提供各种云标	月/社交登录选项。
已启用:	□ 使用云标识/社交网络凭据启用登录
多重身份验证	
身份验证时需要辅助因素。	
提供程序:	无多重身份验证・・
网络登录访问 控制对登录页面的访问。	
已允许访问:	输入允许其进行登录访问的 IP 地址和网络。
已拒绝访问:	
* 拒绝行为:	制入已出来进行显示的问题 IP ADUITING 。 [发送 HTTP 404 未找到状态 ↓] 选择系统对不允许请求的响应。
身份验证后 成功预身份验证后要执行的	操作。
运行状况检查:	□ 需要成功执行 OnGuard 运行状况检查 如果选中,在访问网络之前,来宾必须通过运行状况检查。
更新端点:	□ 将用户的 MAC 地址标记为已知端点 如果选中,还将使用用户帐户的其他详细信息更新端点的属性。
	📲 保存更改 🛛 🧖 保存并重新上传
[•] 必填字段	

2) ClearPass Guest 自定义 Portal

Web 登录编辑器	
* 名称:	(yst-sms (meraki) 输入此 Web 登录页面的名称。
页面名称:	yst-sms-portal_meraki 为此 Web 登录输入页面名称。 Web 登录可从*/guest/page_name.php ^r 进行访问。
描述:	
	有关 Web 登录的注释或描述性文本。
*供应商设置:	Cisco Systems 选择一组适合标准网络配置的预定义设置。
登录方法:	服务器发起 - 更改发送给控制器的权限(RFC 3576) ~ 选择如何处理用户的网络登录。 服务器发起的登录要求提供用户的 MAC 地址,通常来自于强制网络门户重定向过程。
2000年1月11日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日	
身份验证:	【光话 - 希安用/-"石相径"的
身份验证: 自定义表单:	 【沈佑 - 斋安用/**凸相径的 ★送择身份验证要求。 **访问代调"需要给入单个代码(用户名)。 **匿名 "允许仅需要条款或"登录 "按钮的空白表单。需要预先存在的帐户。 **诘询"当"置名 "唱似,但页面将自动提交。 **访问代码"虾管客" "要求账户必须设置"由户名身份验证"字段。 ☑ 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。
身份验证: 自定义表单: 自定义标签:	 □九店 - 斋安用/* 凸相密的 > 选择身份验证要求。 * 访问代码"需要输入单个代码(用户名)。 * 筐名 "允许仅需要条款或"登录 "按钮的空白表单。需要预先存在的帐户。 * "自动"与"置名"相似,但页面将自动提交。 * "访问代码"打"置客"理求账户必须设置"田户名身份验证"字段。 ジ访问代码"打"置客"理求账户必须设置"田户名身份验证"字段。 ② 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。 > 覆盖默认标签和错误消息。 如果选定,您将能够更改当前登录表单的标签和错误消息。
身份验证: 自定义表单: 自定义标签: 用户名后缀:	 【六店 - 斋安用/ "右札密的 ✓ 送择身份验证要求。 "访问代码"繁要缺入单个代码(用户名)。 "富名"方许仅需要条款或"登录"按钮的空白表单。需要预先存在的帐户。 "官动"与"匿名""用说,但页面将自动提交。 "访问代码"和"匿名"要求账户必须设置"用户名身份验证"字段。 【 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。 【 要盖默认标签和错误消息 如果选走,您将能够更改当前登录表单的标签和错误消息。 将登录表单提交到 NAS 之前,后缀将自动附加到用户名。
身份验证: 自定义表单: 自定义标签: 用户名后缀: 身份验证前检查:	 □ 沈佑 - 斋安用/ "石相密的 ▼ 沈海科易份验证要求。 **访问代酒"雾要執入单个代码(用户名)。 **匿名"允许仅需要条款或"登录"按钮的空白表单。需要预先存在的帐户。 **诘词代酒""町置名""君以,但页面将自动提交。 **访问代酒""町置名""要求账户必须设置"由户名身份验证"字段。 ✓ 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。 □ 覆盖默认标签和错误消息。 如果选定,您将能够更改当前登录表单的标签和错误消息。 /* 按示,您将能够更改当前登录表单的标签和错误消息。 /* 按查录表单提交到 NAS 之前,后缀将自动附加到用户名。 /* 无 不进行额外检查 >> <
身份验证: 自定义表单: 自定义标签: 用户名后缀: 身份验证前检查: 条款:	 □大店 - 高安用/ "石札徑的 ▼ □法择身份验证要求。 >*⑤同代码"需要款如 全异 论钮的空白表单。需要预先存在的帐户。 **首都"方下仅需要条款或" 登录 "按钮的空白表单。需要预先存在的帐户。 **首动"与"匿名""相似,但页面将自动提交。 **方面代码"和"匿名"要求账户必须设置"用户名身份验证"字段。 ● 通 提供自定义登录表单 如果选中,必须在标头或页脚 HTML 区域中提供您自己的 HTML 登录表单。 □ 覆盖默认标签和错误消息。 如果选定,您将能够更改当前登录表单的标签和错误消息。 ● 接登录表单提交到 NAS 之前,后缀将自动附加到用户名。 ● 无 - 不进行额外检查 ▼ 选择在继续 NAS 身份验证之前应如何检查用户名和密码。 □ 需要确认条款和条件 如果选中,将会强制用户接受"条款和条件"复选框。

强制网络门户 强制网络门户检测属性						
阻止 CNA:	□ 启用绕过 Apple Captive Network Assistant Apple Captive Network Assistant (CNA)是在宝辉具有强制网络门户的网络时显示的弹出式浏览器, 注意,此选项可能不适用于所有供应南,这取决于如何实施强制网络门户。					
CAPPORT Venue URL:	輸入可造 URL 以作为 CAPPORT RFC-8908 的 Venue Info URL 送達。 https://www.rfc-editor.org/rfc/rfc8908.html					
默认目标 用于控制客户端在登录后将	重 定向到的目标台选项。					
* 默认 URL:	[https://www.baidu.com/ 输入要将客户缚重定向到的默认 URL。 请确保在任何外部域的前面追加 "http://"。					
覆盖目标:	强制所有客户端的默认目标 如果选中,无论客户端的默认目标值如何都会将其覆盖。					
登录页 用于控制登录页外观和感觉的						
* 皮肤:	Blank Skin 」 批將显示此 Web 登吳匹鳳的要使用的皮肤。					
标题:	 要在 Web 登录页上显示的标题。 第次以使用我认值(登录)、					
页眉 HTML:	<pre>(/form method='post' action='/guest/yst=sms=portal_meraki, php?_browser=1' name='ulogin' (form method='post' action='/guest/yst=sms=portal_meraki, php?_browser=1' name='ulogin' (nput type='hidden' name='user' value=''/> (input type='hidden' name='switchip' id='switchip'> (input type='hidden' name='switchip' id='redirect_url'' (input type='hidden' name='mac' id='mac'> (span class='span1')% :W: (/span> (span class='span1')% :W: (/span> (span class='span1')% :W: (/span> (span class='span2')<input <br="" class="i=box" id="password" name="password" type="password"/>(p) (p class='i=hint') (/p) (/div) (div class='i=view')</pre>					

Post 动作指回到自己登入页面即可。

Input 字符还需要通过 html 函数把实际客户端提交的参数填写进去,因此,最好需要网页开发的人员配合实施。

页脚 HTML:	「插入マ 在登录表準之后显示的 HTML 博版代码。 (1D0CTVFE htal PIBLIC * / / WSC / / DTD XHTML 1.0 Transitional / FN*				
登录消息:	插入 ✓ 进行登录学述的显示的 HTML 模板代码。				
* 登录延迟:	5 显示登录得局时的延迟时间(秒)。				
云标识 可选择向来真提供各种云标	月/杜交登录选项。				
已启用:	□ 使用云标识/社交网络凭掘启用登录				
多重身份验证 身份验证时需要辅助因素。	多種身份验证				
提供程序:	无多重身份验证				
网络登录访问 控制对登录页面的访问。					
已允许访问:					
	输入允许其进行登录访问的 IP 地址和网络。				
已拒绝访问:					
* 拒绝行为:	** 拒绝行为:: 世援美化町7500(1):11 / 20世代町993)。 * 拒绝行方:: 世援美化町750(1):200 世援美化町750(1):200 世援美術切方の(1):100 世援美術切方の(1):100 世景系統)				
身份验证后 成功预身份验证后要执行的	Ŗ(r,				
运行状况检查:	□ 需要成功执行 OnGuard 运行状况检查 如果选中,在访问网络之前,来美必须通过运行状况检查。				
更新端点:	□ 将用户的 MAC 地址标记为已知端点 如果选中,还将使用用户帐户的其他详细信息更新读点的量性。				
	📲 保存更改 🦷 保存并重新上传				

第四章 Mac+WebAuth 流程

初次连接:

新客户端接入时,首先进行 MAC 认证。

获取 Portal 指令:

完成 MAC 认证后,客户端会接收到弹出 Portal 的指令,提示用户填写账号密码。

提交数据到 ClearPass:

用户在 Portal 中填写账号密码后,数据会提交至 ClearPass 进行身份验证。

验证成功:

ClearPass 会将客户端的认证信息缓存,同时踢下线客户端(COA),使其重新进行认证。

重新认证:

客户端可能不会自动关联到原有的 SSID。此时,用户需要手动选择 SSID 重新连接。客 户端此时会再次进行 MAC 认证,但由于已有 MAC 地址缓存,认证会直接通过。

缓存失效:

如果 MAC 地址缓存过期,客户端将重新获取到弹出 Portal 的策略,再次进行 Portal 认证。