带AireOS控制器的DNA空间强制网络门户配置示 例

目录

简介 <u>先决条件</u> 要求 使用的组件 配置 网络图 配置 将WLC连接到思科DNA空间 在DNA空间上创建SSID 控制器上的ACL配置 **DNA空间上没有RADIUS服务器的强制网络门户** 在DNA空间上具有RADIUS服务器的强制网络门户 在DNA空间上创建门户 在DNA空间上配置强制网络门户规则 验证 故障排除

简介

本文档介绍如何使用Cisco DNA Spaces和AireOS控制器配置强制网络门户。

作者: Andres Silva Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题:

- 对无线控制器的命令行界面(CLI)或图形用户界面(GUI)访问
- 思科DNA空间

使用的组件

本文档中的信息基于以下软件和硬件版本:

•5520无线LAN控制器版本8.10.112.0

配置

网络图



配置

将WLC连接到思科DNA空间

控制器需要使用任何可用的设置(直接连接)、通过DNA空间连接器或使用CMX Tethering连接到 DNA空间。

在本例中,虽然强制网络门户的配置方式对所有设置都相同,但直接连接选项仍在使用。

要将控制器连接到思科DNA空间,它必须能够通过HTTPS访问思科DNA空间云。有关如何将控制器 连接到DNA空间的更多信息,请参阅以下链接:<u>DNA空间直接连接配置示例</u>

在DNA空间上创建SSID

步骤1:点击DNA空间控制面板中的强制网络门户:



第二步:单击页面左上角的三行图标打开强制网络门户菜单,然后单击SSID:

⊕ - ⊂ e	A Margan Marganese A Super-School Control of Control	- 0 6 🕴
Cisco DNA Spa	sces	C surse
D Partal		
IF Capital Participate		impat/Configure 1500
♥ \$50%	350v	
A Reports		
.A. User Management		

第三步:单击**Import/Configure SSID**,选择**CUWN(CMX/WLC)**作为"Wireless Network"类型,然后 输入SSID名称:

= Cisco DNA Spaces		C Serte
Ciaco Meneti (SICo		Ingun/Configure 380
	SSID Configuration Yoursent satisf any Case Model 2004 yet. Select between a part standed	

控制器上的ACL配置

由于这是Web身份验证SSID,因此需要预身份验证ACL。当无线设备连接到SSID并收到IP地址时 ,设备的策略管理器状态将变为**Webauth_Reqd**状态,并且ACL将应用于客户端会话,以限制设备 可以访问的资源。

步骤1:导航到**安全>访问控制列表>访问控制列表**,单击**新建**并配置规则以允许无线客户端之间到 DNA空间的通信,如下所示。使用所用帐户的DNA空间提供的IP地址替换:

Gen	eral									
Acces	a List Name	DNASpece	m-ACL							
Deny	Counters	٥								
Seq	Action	Source IP/Hask	Destination IP/Mask	Protocol	Source Port	Dext Port	OSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	34.235.248.212 /	TCP	Any	HTTPS	Any	Any	0	•
2	Permit	34.235.248.212 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•
1	Permit	0.0.0.0 /	52.55.235.39 / 255.255.255.255	Any	Any	Any	Any	Any	0	•
4	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	•

注:要获取ACL中允许的DNA空间的IP地址,请在ACL配置部分下的**在DNA空间上创建** SSID部分的第3步中创建的SSID中单击Configure Manually选项。

可以将SSID配置为使用RADIUS服务器或不使用RADIUS服务器。如果会话持续时间、带宽限制或 无缝调配Internet在强制网络门户规则配置的**操作**部分配置,则需要使用RADIUS服务器配置 SSID,否则无需使用RADIUS服务器。两种配置都支持DNA空间上的各种门户。

DNA空间上没有RADIUS服务器的强制网络门户

控制器上的SSID配置

步骤1:导航到WLAN > WLANs。创建新的WLAN。配置配置文件名称和SSID。确保SSID名称与在 DNA空间上创建SSID部分步骤3中配置的名称相同。

cisco	-	- CONTROLLER	WORDLESS SEQURITY	NANAGEMENT COMPO	MOS HELP	rtt5840K			
WLANs	WLANs								
WLANA WLANA	Correct Filters	ament Pitani None (Danja Film) (Dan Film)							
> Advanced	WLAN DD TH	e Profile Na	w w	AN SEED	Admin Status	Security Policie			
	0 L W9	UNL AND	.44	0	traded	[8942][649-099	())		

第二步:配置第2层安全性。导航到WLAN Configuration选项卡中的**Security > Layer 2**选项卡,然 后从Layer 2 Security的下拉菜单中选择**None。**确保MAC过滤已禁用。

uluilu cisco	MONITOR WEARS C	ONTROLLER	WIRELESS	SECURITY N	MANAGEMENT
WLANs	WLANs > Edit 'Aire	BOS-DNAS	paces'		
VLANs WLANS	General Security	y QoS	Policy-Mapp	aing Advar	rced
Advanced	Layer 2 Layer	3 AAA Se	ervers		
	Layer 2 Security # MAC Filtering # OWE Transition Mo Fast Transition Fast Transition Over the DS Reassociation Time	Non de Adap sut 20	e ptive 😧 Seconds		

第三步:配置第3层安全性。导航到WLAN configuration选项卡中的Security > Layer 3选项卡,将 Web **Policy配置为第3层安全方法,Enable Passthrough,配置预身份验证ACL,启用Override Global Config**,将**Web Auth Type**设置为**External,**配置Redirect URL。

altalta cisco	MONITON MENSE CONTROLLER WORKLESS SECURITY MANAGEMENT COMMANDS HELP REEDENCK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANS WLANS	General Security QeS Policy-Mapping Advanced
> Advanced	Labori 3 Security Broke Palay Captive Rothersteader Captive Rothe
	Presetherbication ACs. By d. Dryvipacee-ACs. B By d. None B WebAuth Res IPV4 Act. None B WebAuth Res IPV6 Act. B WebAuth Res IPV6 Act. None B WebAuth Res IPV6 Act. None B WebAuth Res IPV6 Act. B Web

注:要获取重定向URL,请点击Configure Manually选项,该选项位于SSID配置部分下Create the SSID on DNA Spaces第3步中创建的SSID中。

在DNA空间上具有RADIUS服务器的强制网络门户

注意:DNA空间RADIUS服务器仅支持来自控制器的PAP身份验证。

控制器上的RADIUS服务器配置

步骤1:导航到**安全> AAA > RADIUS >身份验证**,单击**新建**并输入RADIUS服务器信息。Cisco DNA Spaces充当RADIUS服务器进行用户身份验证,它可以对两个IP地址做出响应。配置两台 RADIUS服务器:

alialia cisco	HONITOR	25.4%	CONTROLL	IR WORKLES	S SECURITY	HANAGEMENT	COMMUNICS	нυ	ELEDBACK		
Security	RADIUS	Authentic	ation Ser	vers							
• AAA Conerol • RADIOS Authentication Accounting Auth-Centred Users Fallbock DAS	Auth Ca Una ABS MAC De Pramed	Had Station II Kay Wrap Imitar MTU	- 1997 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	NAC Address Designed for FDP typhen 300	SSID B S customers and r	tquints a key arlıq	i compliant Audi	US seve	n		
Downloaded AVP + TAGACE+	Nativork User	Manageme	Tunnel nt Presy	Server Index 8	erver Address(3	pr4/1pr4)		Port	(Pfec	Admin Status	1
LOAP Local Net Users HAC Piltering	0	0		1 1 2 1	4.197.346.505			1812 1812	Disabled Disabled	Enabled Enabled	0

注:要获取主服务器和辅助服务器的RADIUS IP地址和密钥,请点击在DNA空间上创建 SSID部分**第3步中创建的SSID中的Configure Manually**选项,然后导航至RADIUS Server Configuration部分。

第二步:配置记帐RADIUS服务器。导航到**Security>AAA>RADIUS>Accounting**,然后单击 New。配置相同的两台RADIUS服务器:

cisco	BOALLON	WLANS O	owniouze	wpeness	SECURITY MAN	иденент	сонников	нци	TEDBACK		
Security	RADIUS	Accountin	g Servers								
• AAA General • RADRUS Authentication Accounting	Aut Call MAC Del AP Event	ed Station 10 1 initiar In Accounting	han Se Ma	nam MAC Addres phan 📑 Inable							
Pailback Davis	Network User	Managaman	Tunnel S Prany 3	ndex .	Server Address(Ipv	4/3pv6)	r	Port	1Pliec	Admin Statue	
Downloaded #xP			0 1		34.197.146.105			1813	Orabled	Enabled	
TRCACS+ LOAP	0		0		34.228.1.05			1813	Cashled	Enabled	

控制器上的SSID配置

重要信息:在开始配置SSID之前,请确保在Controller > General下将**Web Radius** Authentication设置为"PAP"。

步骤1:导航到WLAN > WLANs。创建新的WLAN。配置配置文件名称和SSID。确保SSID名称与在 DNA空间上创建SSID部分步骤3中配置的名称相同。

cisco	MONETOR MEANS C	ONTROLLER WIRELESS	SECURITY PRAVAGEMENT	COMMANDS HELP	(TEDBACK			
WLANs	WLANs							
WLANS WLANS	Correct Filters None	(Change Filter)	(Dear Filter)			Craste Non	8	64
> Advanced	WLAN ID Type	Profile Name	WLAN SED	Admin Status	Security Policie			
	U WAN	.AND	.AND	Brabled	[8992][649(99	91		

第二步:配置第2层安全性。导航到WLAN Configuration选项卡中的**Security > Layer 2**选项卡。将 第2层安全配置为**None**。启用Mac过滤。

սիսիս cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 1 None
	OWE Transition Mode
	Fast Transition Adaptive C Over the DS
	Reassociation Timeout 20 Seconds

第三步:配置第3层安全性。导航到WLAN configuration选项卡中的Security > Layer 3选项卡,将 Web Policy配置为第3层安全方法,Enable On Mac Filter failure,配置预身份验证ACL,启用 Override Global Config,将Web Auth Type设置为External,配置Redirect URL。

cisco	MONILLON RETWON CONTROLTER MÜRTTERE BEOTRILLA HÄVVERHENL OÖMHVINDE HETA LEEDEVOK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs MLANs	General Security QoS Policy-Happing Advanced
> Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security web Palicy
	Capitive Nationark Assistant Bygans None
	Authentication Pearthrough
	Conditional Web Redirect
	Splash Page Web Redmot
	O On MAC Filter Takunati
	Presultentization AC. IPv4 DAASpecies AC. 📑 IPv5 Nore 🔂 Webhath Files IPv4 Ad. Nore 📑 Webhath Files IPv5 Ad. Nore 📑
	Redivert URL Miger/Append.despects.kr/p2/movem/1
	Sleoping Cliont Auto Authenticate 🚺 Enable
	Override Global Config ²⁰ 2 Ender Web Auth type External (Se direct to external server)

第四步:配置AAA服务器。导航到WLAN configuration选项卡中的**Security > AAA Servers**选项卡 ,启用**Authentication Servers**和**Accounting Servers**,然后从下拉菜单中选择两个RADIUS服务器:

alialia cisco	HONITOR WU	ANS CONTROL	LER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	ния	EEEDBACK
WLANs	WLANs > Edit	t 'AireOS-DI	(ASpaces'					
* WLANs WLANS	General	Security Q	S Policy-Ha	pping Ad	vanced			
Advanced	Layer 2	Layer 3 A	A Servers					
	Apply Coo	aver Overwrite in a 15E Default Sett	terface Enabled	Accounting Se	truers	4		
		Enabled		C Enabled				
	Server 1	IP:34.397.146	105, Port: 1812	IP:34.197.14	6.105, Port:1813	8		
	Server 2	IP:34.228.1.95	, Port: 1812	IP:34.228.1.5	95, Part:1813	8		
	Server 3	None	6	None		3		
	Server 4	Nene		None		0		
	Server 5	None		None		0		
	Server 6	None		None		•		

第六步:配置Web**-auth用户的身份验证优先级顺序**。导航到WLAN configuration选项卡中的 Security > AAA Servers选项卡,并将RADIUS设置为顺序中的第一个。

alialia cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
 WLANs WLANs Advanced 	General Security QoS Policy-Mapping Advanced PADDUS Authentication Survivability

步骤 7.导航到WLAN配置选项卡中的Advanced选项卡,并启用Allow AAA Override。

cisco	MONITOR MLANI CONTR	OLLER WIRELESS SECURITY MEANGEMENT	COMMANDS HELP (TEDBACK		
VLANs	WLANs > Edit 'AireOS-I	DNASpaces"			
WLANs	General Security (QoS Policy-Mapping Advanced			
Advanced	Allow AAA Override	C Enabled	DHICP		
	Coverage Hole Detection	C Enabled	DRCP Server Overlide		
	Enable Session Timeaut	28800 Session Timeout (seco)	DRCP Adds. Assignment C Required		
	Aironet 30	Enabled	Management Frame Protection (MPP)		
	Diagneetite Dhannel 48 Override Interface ACL Layer2 Act	Enabled Det None D Det None D	MIP Clent Protection f Optional		
	URL AD, F2F Blocking Adlan Clarit Exclusion 7	None D Dealted D Stratical 180	803.113a/m (1 - 255) 1 803.113a/m (1 - 255) 1 804		
	Havinum Allowed Clients	d	NAC State None		
	Static 3 ^a Tunneling 44 Wi-Pi Direct Clerite Policy Macimum Alternal Clerite	Evalued Disabled	Olient Load Balancing Olient Balancing		

在DNA空间上创建门户

步骤1:点击DNA空间控制面板中的强制网络门户:



第二步:点击Create New,输入门户名称,并选择可使用门户的位置:

	0			
	Partial Inform	nten Automication	Data Copture	User Agreement
PORTAL NAME				
AirwOS-DNASpaces				
Cathle this portal	ty all incations			
Location Hierard	714		Selecto	d Locations
			C	Designment K
MEX-EAST	-1		L1 1000-11	
MEX-EAST	-1			
MEX-EAST	-1 I-CMEK I-Connector			
MEX-EAST	-1 I-CMK I-Connector I-DirectConnect			

第三步:选择身份验证类型,选择是否要在门户主页上显示数据捕获和用户协议,以及是否允许用 户选择接收消息。单击"下一步":

	Paraji i Normation		a Decision	the Appendix	×
Intel Televisional Pre		Ų	1		
Vature readile salent free and to access the mome.	e partaliharne pege		-		
Allow users to Opt in to receive message					

第四步:配置数据捕获元素。如果要捕获来自用户的数据,请选中Enable Data Capture框,然后单击+Add Field Element以添加所需的字段。单击"下一步":

	0	-0	-0		×
	Partal Information	Administration	Date Captore	tion Agreeteens	
E Bruther Data Capture					-
Forn Falsh				+ Add Field Denerit	
A Finit Name					
A Latiture					
		See .	Pres Nave 1		

第五步:选中Enable Terms & Conditions,然后单击Save & Configure Portal:

	Parial Information	Automicators	Date Capture	the Agreements	
a another allows you to enable and combya-	a fama & Conditions and Preacy pd	kry Subervice.			
Fagler Write & Canditions					
ING & CENDYRON MESSAGE					Or 1 from
					Q
			0.0.0		
him	An I A B M D				
the close close					
M.P. Serve of Unit Lost-product Department	27.898				
These Wild Terms & Canadiana Of Sea (the N	6/ Terra; spather with the 10 Relia (of	126E geven your use at the MAT is	ankica.		
Description of the Derivice					
The Samite provides you with nimitees access or product using the Denniar is annum Plat user	to the Internet within the premises. We di to comply with these 10-15 There analysis	to tot, as an ordinary practice, proved for law, although I constrain the right	inds menter the activities of Now In do no.	etto ase the Senice or exercise any adicital sort	trol over any makenal terramitiest, heated
e possi conj te te ca i ecce te an	e codd ac can pro pea site (

第六步:根据需要编辑门户,点击**保存:**

Partal - Aired COMAgazon /	Martines (at turns /	Ø Ø Bantantatar № ⁰ (Bell
Toucher: Bad / Badd / Badd /	The form (very conjuster module)	NOTEL PROTECT Cased Scenar (*) Cased Systems Vencome to Sponstand SeGe UP FOR VERF Complete the form before its opmast to internet (************************************

在DNA空间上配置强制网络门户规则

步骤1:打开强制网络门户菜单,然后点击**强制网络门户规则:**

⊖ ở ô	A https://dnaspaces.io/captiveportal/hules/captive-portal/hules/cap	rtal
Cisco DNA Spac	es	
Portal		
E Captive Portal Rules		Created
ଙ୍କ \$\$10s		Feb 24, 2020
al Reports	> ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	○ 8:02 PM

第二步:单击**+ Create New Rule**。输入规则名称,选择先前配置的SSID,并选择此门户规则可用 于的位置:

	TUDENARY
When a user is on WHI - and connected to Avecto-Wildpaces -	NUL MAI smith Onlinera
ETCHS - When do you want the rule to fina?	10.400
	When your is an NPI and yourseled to dowD IDANgeose
At any of the tolswing locations	LODATIONE .
+ Appliancelore)	For all locations under
	1010-1 (Descharment
Rith + Granifacture X	and the d
	1040.41

第三步:选择强制网络门户的操作。在这种情况下,当规则被命中时,将显示门户。单击**保存并发**

AC7046	1000.0
Show Caption Partial Chases a Partial to be depayed to Davis when they connectify the will.	504D4.5
Ave05-DMAgeras -	ACTON Blue Capitor Parket Parket: AcroCh. Of Mission
Section Duration	
Bandweidt-Lines	
Searchardy Physiolocileteeteel Orenity presses interest without accounts and wretication	
O Deny Internet Bog some frem somsning the Internet	
Tage them easts as Decase - have a function from to charactery.	
* Altit Tage	
C Trigger ARI	

验证

布。

要确认连接到SSID的客户端的状态,请导航到**Monitor > Clients**,点击MAC地址并查找Policy Manager State:

MONITOR	MIAN	CONTROLLER	WPIELESS	SECORITY	HANAGEHENT	COMMANDS	HELP	EEDBACK	
Clients >	Detail								< Back
Max Numb	er of Recor	ds 10 * Ck	ter AVC Stats	1					
General	AVC 5	tatistics							
						AP radio alo	4.34	1	
Cient 1	lype	Regular				WLAN Profil		AireOS-ONASpaces	
Client 1	Unnel Type	Simple IP				WLAN SSID		AireOS-ONASpaces	
User Na	ine					Status		Associated	
Webeut	th User Nam	None				Association	10	1	
Port Nu	mber	1				802.11 Aut	hentication	Open System	
proerfer	0e	management				Reason Cod	e	1	
VLAN II	D	20				Status Code		0	
Quaran	tine VLAN II	0				CF Pollable		Not Implemented	
CCX Ve	raion	Not Supported				CF Pull Reg.	HR.	Not Implemented	
E2E Ver	neian	Not Supported				Short Pream	sble	Not Implemented	
Mobility	Role	Local				PBCC		Not Implemented	
Mobility Address	Peer IP	N/A				Channel Age	iky	Not Implemented	
Hobility	Move Court					Timeput		0	
Pency P State	lereger	RUN				WEP State		WEP Disable	

故障排除

在测试确认客户端的关联和身份验证过程之前,可以在控制器中启用以下命令。

(5520-Andressi) >debug client

以下是在连接到没有RADIUS服务器的SSID时,在关联/身份验证过程中成功尝试识别每个阶段的输 出:

802.11关联/身份验证:

*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1 *apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4 *apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280 *apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode (1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22) *apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0 station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1

DHCP和第3层身份验证:

*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD *webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in HTTP GET, client mac=34:e1:2d:23:a6:68 *webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68 user_agent = AnyConnect Agent 4.7.04056 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configured Web-Auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, using virtual IP =192.0.2.1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN ID:1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using URL:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio), redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"</pre> content="no-cache"><META http-equiv="Pragma" content="</pre> *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is HTTP/1.1 200 OK

Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34: *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Url:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Url:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send **勾口目的**

第3层身份验证成功,将客户端移至RUN状态:

*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255, URL ACL ID 255, URL ACL
Action 0)

*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user

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)。