演示9800无线局域网控制器上的客户端分析

目录

简介 使用的组件 分析过程 MAC地址OUI分析 本地管理的MAC地址问题 DHCP分析 <u>HTTP分析</u> <u>RADIUS</u>分析 **DHCP RADIUS分析** HTTP RADIUS分析 在9800 WLC上配置分析 本地分析配置 RADIUS分析配置 分析使用案例 基于本地分析分类应用本地策略 思科ISE中的高级策略集的RADIUS分析 FlexConnect部署中的分析 集中身份验证、本地交换 本地身份验证、本地交换 故障排除 放射性痕迹 数据包捕获

简介

本文档介绍设备分类和分析如何在Cisco Catalyst 9800无线LAN控制器上运行。

使用的组件

- •运行17.2.1映像的9800 CL WLC
- •1815i接入点
- Windows 10 Pro无线客户端
- 思科ISE 2.7

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。

分析过程

本文深入了解设备分类和分析如何在Cisco Catalyst 9800无线LAN控制器上运行,描述了潜在的使 用案例、配置示例以及排除故障所需的步骤。 设备分析是一项功能,用于查找有关已加入无线基础设施的无线客户端的其他信息。

执行设备分析后,可以使用它来应用不同的本地策略或匹配特定RADIUS服务器规则。

Cisco 9800 WLC能够执行三(3)种类型的设备分析:

1. MAC地址OUI

2. DHCP

3. HTTP

MAC地址OUI分析

MAC地址是每个无线(有线)网络接口的唯一标识符。它是通常以十六进制格式 MM:MM:SS:SS:SS写下的48位数字。

前24位(或3个二进制八位数)称为OUI(组织唯一标识符),它们唯一标识供应商或制造商。

它们由IEEE购买和分配。一家供应商或制造商可以购买多个OUI。

示例:

00:0D:4B - owned by Roku, LLC 90:78:B2 - owned by Xiaomi Communications Co Ltd

无线客户端与接入点关联后,WLC会执行OUI查找以确定制造商。

在Flexconnect本地交换部署中,AP仍会将相关客户端信息中继到WLC(例如DHCP数据包和客户端MAC地址)。

仅基于OUI的分析极其有限,可以将设备分类为特定品牌,但它无法区分笔记本电脑和智能手机。

本地管理的MAC地址问题

出于隐私考虑,许多制造商开始在他们的设备中实施mac随机化功能。

本地管理的MAC地址是随机生成的,并且地址第一个八位组的第二个最低有效位设置为1。

此位充当一个标志,用于宣布mac地址实际上是一个随机生成的地址。

本地管理的MAC地址有四种可能的格式(x可以是任何十六进制值):

x2-xx-xx-xx-xx-xx x6-xx-xx-xx-xx-xx xA-xx-xx-xx-xx-xx xE-xx-xx-xx-xx-xx

默认情况下,Android 10设备在每次连接到新的SSID网络时使用随机生成的本地管理MAC地址。

由于控制器识别出地址是随机化的,并且不执行任何查找,因此此功能完全破坏了基于OUI的设备 分类。

DHCP分析

DHCP分析由WLC通过调查无线客户端发出的DHCP数据包来执行。

如果使用DHCP分析对设备进行分类,**show wireless client mac-address [MAC_ADDR] detailed**命 令的输出包括:

Device Type : Microsoft-Workstation Device Name : MSFT 5.0 Protocol Map : 0x000009 (OUI, DHCP) Protocol : DHCP

WLC检查无线客户端发送的数据包中的多个DHCP选项字段:

1.选项12 — 主机名

此选项表示客户端主机名,可在DHCP发现和DHCP请求数据包中找到:

No.	Time	Source	Destination	Protocol	Length	Info		
	376 476.750338	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discove	er - Transactio	on ID 0x1e69cc75
> > > >	Ethernet II, Src: Internet Protocol User Datagram Pro Dynamic Host Conf Message type: Hardware type: Hardware addre	: EdimaxTe_f6:76:1 l Version 4, Src: otocol, Src Port: figuration Protoco Boot Request (1) : Ethernet (0x01) :ss length: 6	<pre>Pe (74:da:38:f6:76:f0), Dst 0.0.0.0, Dst: 255.255.255. 68, Dst Port: 67 al (Discover)</pre>	: Broadca 255	st (ff:	ff:ff:ff:ff:	11)	
	Hops: 0 Transaction ID Seconds elapse > Bootp flags: 0 Client IP addr Your (client) Next server IP Relay agent IP Client MAC add Client hardwar Server host na	0: 0x1e09cc75 d: 0 hx0000 (Unicast) ress: 0.0.0.0 P address: 0.0.0 Address: 0.0.0.0 ress: EdimaxTe_ff re address padding me not given	0.0 9 9:75:f0 (74:da:38:f6:76:f0) 1: 000000000000000000000000000000000000					
	Boot file name Magic cookie: > Option: (53) 0	e not given DHCP DHCP Message Type	(Discover)					
[> Option: (61) (DESKTOP-KLREØMA						

2.选项60 — 供应商类别标识符

此选项也在DHCP发现数据包和请求数据包中找到。

使用此选项,客户端可以向DHCP服务器标识自身,然后可以将服务器配置为仅响应具有特定供应 商类别标识符的客户端。

此选项最常用于识别网络中的接入点,并且仅使用选项43对接入点做出响应。

供应商类标识符示例

- "MSFT 5.0" 适用于所有Windows 2000客户端(及更高版本)
- "MSFT 98" 适用于所有Windows 98和Me客户端
- "MSFT" 适用于所有Windows 98、Me和2000客户端

默认情况下,Apple MacBook设备不会发送选项60。

从Windows 10客户端捕获数据包的示例:

Option: (60) Vendor class identifier Length: 8 Vendor class identifier: MSFT 5.0

3.选项55 — 参数请求列表

DHCP Parameter Request List选项包含DHCP客户端向DHCP服务器请求的配置参数(选项代码)。它是以逗号分隔记法书写的字符串(例如1,15,43)。

它不是一个完美的解决方案,因为它生成的数据取决于供应商,并且可以通过多种设备类型进行复 制。

例如,默认情况下,Windows 10设备始终请求特定参数列表。Apple iPhone和iPad使用不同的参数 集,可以在这些参数集上进行分类。

从Windows 10客户端捕获的示例:

```
Option: (55) Parameter Request List
   Length: 14
   Parameter Request List Item: (1) Subnet Mask
   Parameter Request List Item: (3) Router
   Parameter Request List Item: (6) Domain Name Server
   Parameter Request List Item: (15) Domain Name
   Parameter Request List Item: (31) Perform Router Discover
   Parameter Request List Item: (33) Static Route
   Parameter Request List Item: (43) Vendor-Specific Information
   Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
   Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
   Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
   Parameter Request List Item: (119) Domain Search
   Parameter Request List Item: (121) Classless Static Route
   Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
   Parameter Request List Item: (252) Private/Proxy autodiscovery
```

4.选项77 — 用户类

User class是默认情况下最常使用的选项,需要手动配置客户端。例如,可以在windows计算机上使 用以下命令配置此选项:

ipconfig /setclassid "ADAPTER_NAME" "USER_CLASS_STRING" 适配器名称可在控制面板中的"网络和共享中心"中找到:



在CMD中为Windows 10客户端配置DHCP选项66(需要管理员权限):



由于Windows实施了选项66,wireshark无法解码此选项,选项66之后的部分数据包显示为格式不正确:

HTTP分析

HTTP分析是分析9800 WLC支持的最高级方法,它提供了最详细的设备分类。

对于要进行HTTP分析的客户端,它需要处于"运行"状态并执行HTTP GET请求。

WLC会拦截请求,并检查数据包的HTTP报头中的"User-Agent"字段。

此字段包含可用于对无线客户端进行分类的其他信息。

默认情况下,几乎所有制造商都实施了无线客户端尝试执行Internet连接检查的功能。

此检查也用于自动访客门户检测。 如果设备收到状态代码为200(OK)的HTTP响应,则表示未使用 webauth保护WLAN。

如果是,则WLC执行必要的拦截,以执行身份验证的其余部分。 此初始HTTP GET不是唯一一个WLC可用于分析设备。

每个后续HTTP请求都由WLC检测,并且可能会产生更详细的分类。

Windows 10设备使用域**msftconnecttest.com**执行此测试。Apple设备使用**captive.apple.com**,而 Android设备通常使用**connectivitycheck.gstatic.com**。

执行此检查的Windows 10客户端的数据包捕获可在下面找到。User Agent(用户代理)字段填充了 Microsoft NCSI,这导致在WLC上客户端被分析为Microsoft-Workstation:

No.	Time	Source	Destination	Protocol	Length 3rfs
	32 11.230352	10.48.39.235	64.182.6.247	DNS	83 Standard query Bx66e8 AAAA www.msftconnecttest.com
	48 11.344857	64.182.6.247	38.48.39.235	DNS	349 Standard query response Buildis A way.msftconnecttest.com CNAPE vinc
4	55 11.354877	10.48.39.235	13.107.4.52	HTTP	165 GET /connecttest.txt HTTP/1.1
	70 11.378889	13.107.4.52	10.48.39.235	HTTP	624 HTTP/1.1 200 OK (text/plain)
> #	rame 55: 165 byte	is on ware (1320 bit	s), 165 bytes capture	d (1320 bit	ts) on interface \Device\APF_(95AD0002-0027-4F05-8918-90A8465039A8), id 0
> 8	thernet II, Srci	Edimente_f6:76:f0 (74:da:38:f6:76:f0), 0	st: Cisco_i	19:41:e1 (24:7e:12:19:41:e1)
> 1	sternet Protocol	Version 4, Sect 18.	48.39.235, Dati 13.18	7.4.52	
> 1	ranseduction Contr	ol Protocol, Src Po	rt: 56815, Dat Port:	80, Seg: 1.	, Ack: 1, Len: 111
~ H	opertext Transfer	Protocol			
	GET /connecttes	A. DAT HTTP/1.11/Pie			
) [Expert Info	(Chat/Sequence): 6	ET /connecttest.txt H	TP/1.1\r\a	s]
	Request Path	odi GET			4
	Request URT:	/connecttest.txt			
	Request Very	Loss HTTP/1-1			
	Connection: Che	adaha			
	tinger, Lagard 1 mile	second willing			
	Dier-Agenci Pac	Pesert Mattria			
	POSTI MANURSTEE	OUNSCEEDE COM OF 78			
	1/ VA				
	[Full request 0	R1: http://www.wsft	connecttest.com/conne	CEDELE-DAL	
	[HTTP request 1	/1]			
	Response in fr	ame: 20]			

对于通过HTTP分析的客户端, show wireless client mac-address [MAC_ADDR]的详细示例输出:

:	Microsoft-Workstation
:	MSFT 5.0
:	0x000029 (OUI, DHCP, HTTP)
:	Windows NT 10.0; Win64; x64; rv:76.0
:	НТТР
	: : : :

RADIUS分析

当涉及用于设备分类的方法时,本地和RADIUS分析没有区别。

如果启用了Radius分析,则WLC会通过一组特定供应商特定的RADIUS属性将其了解到的设备信息 转发到RADIUS服务器。

DHCP RADIUS分析

通过DHCP分析获取的信息将作为供应商特定的RADIUS AVPair发送到记帐请求内的RADIUS服务器 cisco-av-pair:dhcp-option=<DHCP选项>

显示DHCP选项12、60和55的AVPairs的记帐请求数据包示例,分别从WLC发送到RADIUS服务器 (选项55值可能因Wireshark解码而损坏):

ю.	Tine	Source	Destination	Protocol	Langth	Source Part	Destination Port	2-fs
14	829 9.293998	10.48.39.252	38.48.73.92	8400/5	783	64589	1413	Accounting-Request 54+392
÷	849 9.198995	10.48.71.92	38.48.39.212	840075	62	1813	64189	Accounting-Response \$44-282
ч.	858 9.198995	10.48.71.92	38.48.39.212	RADOVS	62	1813	64189	Accounting-Response 1d+282, Duplicate Response
<								
3	Frane \$20: 783 by	tes on wire (4264 b)	Ash, 283 lights capture	of (1204 birts)				
5	Othernet II, Seco	00.00.00 00.00.00	(00.00.00.00.00.00), De	A1 00:00:00 00:			(88)	
5	Internet Protocol	Version 4, Sect 18.	48.39.212, Dvt: 18.48.	71.92				
5	User Detegrae Pro	tocal, Sec Parts 645	URP. Dut Porti 1813					
*	AdduS Protocol							
	Code: AccountS	ng-Request (4)						
	Packet IdentIA	Leri Bula (202)						
	Longth: 243							
	AuthentEcators	201205404040427368	1582ce382576c5					
	Ethe response.	to this request is i	a frame \$491					
	- Attribute Value	e Pairs						
	> AVP: trivend	or-Specific(36) 1+45	vnd-clacelystees(9)					
	> AVP: ErVend	or-Specific(36) 3+30	vndvcEscolystees(9)					
	> JUP: ErVend	or-Specific(26) 1-65	underEscolystees(9)					
	> anthi E-mende	or-Specific(36) b-M	und-classifystees(9)					
	> AVP: D-Vend	or-Specific(36) 1-M	wed-classifystees(9)					
	> AVP: t-Vends	or-specific(36) 1+25	und-classigatees(9)					
	W AVP: E-Vend	or-Specific(36) 1+39	vol-classigation(9)					
	Type: 26							
	Longth	79						
	Vendor 22	Di claistystees (9)						
	> VEAL KHO	Lace-#VPaLr(1) 3+03	val-dhop-option+\abbitf	VANAL/2015/07/04	-KLREIPHA			
	* AVP: E-Vend	or-Specific(26) 1+32	wind-classifystees(9)					
	Type: 26							
	Longth:	32						
	Vendor 22	Di classifystema (9)						
	 VSA: 4-6 	Concentrate (S) 3+26	NACING CONTRACTORS	000'045FT 5.0				
	* JUP: Criteral	or-Specific(36) 5+38	wed-classifystees(9)					
	Type: 26							
	Length: 3	38						
	Vendor 10: claceSystems (9)							
	I VSA: tell	Inco-Aventation 1+32	val-dup-option-laters	00010105-00011005	Version and Print	Place North	•	

HTTP RADIUS分析

通过HTTP分析获取的信息(来自HTTP GET请求报头的用户代理字段)作为供应商特定RADIUS AVPair发送到记帐请求内部的RADIUS服务器 **cisco-av-pair:http-tlv=User-Agent=<user-agent>**

初始连接检查HTTP GET数据包在User-Agent字段中不包含太多信息,只有"Microsoft NCSI"。将此简单值转发到RADIUS服务器的记帐数据包示例:

Name Description Description <thdescription< th=""> <thde< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th></thde<></thdescription<>							
HESS 5283, #75080 38.48.71.42 38.48.35.112 84005 42 1813 57397 Accounting-Response 14-885 HESS 5283, #75080 18.48.71.42 38.48.35.112 84005 42 1813 57397 Accounting-Response 14-885 Deer Datagram Protocol, Sri, Parti 57397, Col Parti 1813 Accounting-Response 14-885 57397 Accounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 57397 Accounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Mathematication: 0001abilit/15043Admined/15075451244 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Authematication: 0001abilit/15043Admined/15075451244 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Authematication: 0001abilit/15043Admined/15043Admined/15075451244 Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Authematication: 001a Authematication: 001a Code: Alcounting-Response 14-885 Code: Alcounting-Response 14-885 Authematicator: 001a Authematicator: 001a <td>4847 3583,868996</td> <td>38.48.39.252</td> <td>38.48.71.92</td> <td>8400V5</td> <td>708 57397</td> <td>1813</td> <td>Accounting-Request 1d-185</td>	4847 3583,868996	38.48.39.252	38.48.71.92	8400V5	708 57397	1813	Accounting-Request 1d-185
4855 5983,875088 38.48.71.92 58.48.79.212 8A0105 42 1813 57397 Accounting-Response 14-185, buplicate Response Der Datagnam Proteopil, Sci. Parti 5787, Dot Parti 5813 AA0105 42 1813 57397 Accounting-Response 14-185, buplicate Response Der Datagnam Proteopil, Sci. Parti 5787, Dot Parti 5813 AA0105 42 42 1813 57397 Accounting-Response 14-185, Sci. Parti 5787, Dot Parti 5813 AA0105 42 42 1813 57397 Accounting-Response 14-185, Sci. Parti 5787, Dot Parti 5813 AA0105 42 42 1813 57397 Cole: Accounting-Response 14-186, Dot Sci. Sci. Parti 5813 Accounting-Response 14-186, Dot Sci. Sci. Parti 5813 57397 57397 57397 Automation Sci. Sci. Sci. Parti 5787, Dot Parti 5813 Accounting-Response 14-186, Dot Sci. Sci. Parti 5813 57397 57397 57397 Automation Sci. Sci. Sci. Parti 581 Accounting-Response 14-186, Dot Sci. Sci. Parti 5813 57397 57397 57397 Automation Sci. Sci. Sci. Parti 581 Accounting-Response 14-186, Dot Sci. Sci. Sci. Sci. Sci. Sci. Sci. Sci.	4854 3583,875888	38.48.71.92	10.48.39.212	RA02V5	62 1813	57397	Accounting-Response id-105
<pre>Voer Detagram Protocold, Srit Parts 57307, Det Parts 5633 AADDAG Protocold Code: Alcounting: Request (4) Paintet LidentSfor: Back (100) Length: 054 AuthentListor: BetMode/Sfor(AldarbedGIDF70012044 (The response to This request is in frame 4054) V ARt+Diver Value Patrs 3 ADP, friendler-Spic(If1(24) 2-47 undre(Sintystems(9) 3 ADP, triendler-Spic(If1(24) 2-47) undre(Sintyst</pre>	4855 3583.875988	38.48.71.92	10.48.39.212	8400V5	62 1813	\$7397	Accounting-Response id-105, Duplicate Response
Verer Datagram Protocol, Sri Parti 57307, Dol Parti 1883 AADDAS Protocol Cole: Actourting/Report (4) Packet LearDifter: Book (20) Length: SSA ArtHouse Pates * Affiliate Value Pates * Affiliate V							
<pre>Super Destagram Protocol: Code: Addomnting:Request (4) Packet LidentFiber: Bubb (100) Length: 518 Authom Listor: Bobbick(07)6(4)AdministionTPOHI2044 (The requests for State Pairs > Addy: Evendor-Spec(EfL(24) 2-40 under(Sate)pitems(9) > Addy: Evendor-Spec(EfL(24) 2-50 under(Sate)pitems(9) > Addy: Evendor-Spec(EfL(24) 2-50 under(Sate)pitems(9) > Addy: Evendor-Spec(EfL(24) 2-50 under(Sate)pitems(9)</pre>							
NADEUS Produced Code: ActionElegrameters (4) Parket LidentEffor: Bob (100) Length: SSA AuthentLicker: Bob (100) Length: SSA AuthentLicker: Bob (101) Sade: Evendor-Specific(21) 2-04 volc(Ssidpstees(3)) > AUD: Evendor-Specific(21) 2-03 volc(Ssidpstees(3)) > AUD: Evendor-Specific(21) 2-03 volc(Ssidpstees(3)) > AUD: Evendor-Specific(22) 2-03 volc(Ssidpstees(3)) > AUD: Evendor-Specific(23) 2-03 volc(Ssidpstees(3)) > AUD: Evendor-Specific(24) 2-03 volc(Ssidpstees(3)) > Wolce 20: (Ssidpstees(4))	User Datagram Proto-	cel, Sec Ports 573	107, Dot Port: 1813				
Code: Accounting: Respect (4) Packet identifier: Rude (365) Length: 816 AuthentIcator: Bookan(27)(4)Advise(3)070401244 (The respect to 515, report 1 is in frame 4004) Advisors Nobae Pales Advisors Nobae Pales Advisors Nobae Pales Adv: Evender-Specific(24) 2+32 under(ising)stems(9) Adv: Evender(24) 2+32 under(24) 2+32 under(24) 2+32 under(24) 2	AADDUS Protocol						
Partiet LdentSTGeri Bull (198) Length: 618 AuthentLater: 0000arb(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(0)(Code: Accounting	Request (4)					
Cength: 618 AuthentLoater: 0000arb(0f)06(0)Ada/s00(0)079601244 The respect to 10% report 1: i.e. frame.004	Packet LdentDfLer	ri 0x60 (105)					
Auflenticator: 0000a0c0736c43Adar0003375052244 [The response to TMA respect 1:: 0.: > 400% (respective to TMA respect 1:: 0:: > 400% (respect 1::	Length: 658						
(The response to this repert is in frame 404) * - ADP: (Needer-Specific(24) 2-31 vehr(Saidystem(9))) - ADP: (Needer-Specific(24) 2-31 vehr(Saidystem(9))) - ADP: (Needer-Specific(24) 2-32 vehr(Saidystem(9))) - ADP: (Needer-Specific(24) 2-31 vehr(Saidystem(9)))) - ADP: (Needer-Specific(24) 2-31 vehr(Saidystem(9))))))))))))))))))))))))))))))))))))	Authentication: B	Mark Print Alekson	0481075001244				
<pre>> Attr: Evendor Table Pates > Attr: Evendor Table (Ed.) 2014 under(Escapatement(E)) > Attr: Evendor Table (Ed.) 2017 under(Escapatement(E)) Type: 28 Evendor End: Escapatement(E) </pre>	fthe response to	this report is i	a frame anta'				
<pre>> ADP: {-viewedur-Spec(JfL(2A) }=+44. vnd=(1sinSystems(9) > ADP: {-viewedur-Spec(JfL(2A) }=+37. vnd=(1sinSystems(9) > ADP: {-viewedur-Spec(JfL(2A) }=+29. vnd=(1sinSystems(9) > Type: 24 Length: 25 Viewdur 1: {-viewedur-Spec(JfL(2A) }=+29. vnd=(1sinSystems(9) > Viewdur-Spec(JfL(2A) }=+29. vnd=(1sinSystems(9) > Viewdur-Spec(JfL(2A) =+29. vnd=(1sinSystems(9) > Views(0A) =+29. vnd=(1sinSystems(9) > Views(0A) =+29. vnd=(1sinSy</pre>	V Attailants Value I	Balles	a contraction of the second				
<pre>> Adv: ('veendur-jope()fi(2)(3) =>0 =========()) > Adv: ('veendur-jope()fi(2)(3) =>0 =======()) > Adv: ('veendur-jope()fi(2)(3) =>0 ======()) > Adv: ('veendur-jope()fi(2)(3) =>0 =====()) > Adv: ('veendur-jope()fi(2)(3) =>0 ====()) > Adv: ('veendur-jope()fi(2)(3) =>0 ===()) > Adv: ('veendur-jope()fi(2)(3) =>0 ===())</pre>	ALL SPACE PROPERTY	NAMES OF TAXABLE PARTY.	and the first state of the set (11).				
<pre>> Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) > Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) > Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) > Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) > Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) * Add: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) * Juli: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) * Juli: (*vendor-spec(FLs(24) 2+3) vode(sisily)tems(9) * Vendor 23: (\$isoly)tems (8) Vendor 23: (\$isoly)tems (8)</pre>	> Auri tryender	-Ster (1411(58) 5+68	Andwit Petrophotome (a.b.				
<pre>> ddP: (-Veendor-Spec(F1c(2A) 2=40; veder(ising)vtems(9) > ddP: (-Veendor-Spec(F1c(2A) 2=50; veder(ising)vtems(9) > ddP: (-Veendor-Spec(F1c(2A) 2=50; veder(ising)vtems(9) > ddP: (-Veendor-Spec(F1c(2A) 2=50; veder(ising)vtems(9) > ddP: (-Veendor-Spec(F1c(2A) 2=51; veder(ising)vtems(9) Type: 24 Compt: 25 Veedor 20: (Sicollyvtems (8) Veedor 20: (Sicollyvtems (8)</pre>	> AVP1 Envendor-	-20e(TAT(50) 5+01	under(Localitystees(*)				
<pre>> ddP: Evendor-Specific(24) >>2 vobe(Lisidystees(9) > ddP: Evendor-Specific(24) >>2 vobe(Lisidystees(9) > ddP: Evendor-Specific(24) >>2 vobe(Lisidystees(9)</pre>	> July: E-Vendor-	-SpectPlc(26) 2+68	vedvcLscallystees(P)				
> dd9: t-Vendor-Spec(f1c(24) 2-30 vedec(sistyptees(9) > dd9: t-Vendor-Spec(f1c(24) 2-3) vedec(sistyptees(9) * dd9: t-Vendor-Spec(f1c(24) 2-3) vedec(sistyptees(9) Type: 26 Length: 25 Vendor 20: (Sicolyttees (8) - Vendor 20: (Sicolyttees (8)	> AVP: t-Vendor-	SpecIATC(58) 2+58	ved=cLscsSystems(#)				
3 ddP: Evendor-Specific(24) 2-21 undriteintystem(9) w ddP: Evendor-Specific(24) 2-21 undriteintystem(9) Type: 28 Compth: 25 Vendor 25: classfystem (9) Vendor 25: classfystem (9)	> AVP: E-Vendor-	SpecI/L(24) 1+98	ved=cLscsSystems(#)				
<pre>v duBt twiendor-Specific(26) 2+35 vnd+classSystems(9) Type: 26 Length: 35 Vendor 20: 414005ystems (8) Vendor 20: 414005ystems (8)</pre>	> AVP: E-Vendor-	-SpecI/Lc(26) 1+26	vnd=cLscsSystems(#)				
Type: 26 Length: 25 Vendor ID: classifystees (%)	AuP: t-Vendor-	-Spect/Lc(24) 1+95	und-classifystees(9)				
Length: 25 Wender ID: classfyttees (9)	Type: 26						
Verder Britischyvtes (8)	Length: 35						
A MARK PARTY AND	Vendor ID:	classifystees (8)					
	> VIAL DECLAR		walking - the Magnetic	Marcan Internation	E MCLC		

一旦用户开始浏览Internet并创建一些额外的HTTP GET请求,就有可能获得有关它的更多信息。

如果检测到此客户端的新用户代理值,WLC会向ISE发送其他记帐数据包。

在本示例中,可以看到客户端使用Windows 10 64位和Firefox 76:

4744 3595.182888 18.48.39.212 18.	48.71.92 RADD/5	765 57397	1813	Accounting-Request 1d-106
4749 3595.111994 38.48.71.92 38.	48.39.212 RADD/S	62 1813	\$7397	Accounting-Response id-386
4758 3595.111994 38.48.71.92 38.	48.39.212 RADDUS	62 1813	\$7397	Accounting-Response id-106, Duplicate Response
Dare Dalaaran Brahara), See Barks 57397, Dat	Parts 1813			
BADDUS, Protocol	POP CT BRED			
Code: Accounting-Response (4)				
Parket LiestLifter: Bula (186)				
Langth: 233				
Autorities additional and a second	beautout.			
The resource to this reparet is in frame	47497			
w Stirling Value Pales				
> SUP: Tolendor (Seprific(24) Sala under to	scolorshees/90			
) #VP: tolendor (Specific(24) 1a/7 underin	arefughters (%)			
) #VP: tolendor (Specific (24) last under to	arefughters (%)			
) #VP: tolendor (Specific (24) 1a24 under to	arefughters (%)			
) #VP: tolendor (Specific (34) 1a/4 under to	arefughters (%)			
) #VP1 tolendor (Specific (34) 1a34 under to	arefunction (10)			
w auto totandor Gaar (Min 736) hald under to	arefundamented			
Puter 26	and a second			
Langthy 99				
Wandor 18: claceSystems (9)				
) while the large definite (1) lots valuates	- The later and an end of the	S.A. Mindows NY 18.8: Min	ALC: WHEN THE R.	1 decks/Jackablet /Scafes/16.8

在9800 WLC上配置分析

本地分析配置

为了使Local分析正常工作,只需在Configuration > Wireless > Wireless Global下启用Device Classification。此选项同时启用MAC OUI、HTTP和DHCP分析:

Configuration - > Wireless - > Wireless Global

Default Mobility Domain *	default 🗎
RF Group Name*	default
Maximum Login Sessions Per User*	0
Management Via Wireless	
Device Classification	
AP LAG Mode	

此外,在Policy configuration(策略配置)下,您可以启用HTTP TLV Caching(HTTP TLV缓存)和DHCP TLV Caching(DHCP TLV缓存)。即使没有配置文件,WLC也会执行分析。

启用这些选项后,WLC将缓存以前了解的此客户端信息,并避免检查此设备生成的其他数据包。

Edit Policy Profile							
General	Access Policies	QOS and AVC	Mobility	Advanced			
RADIUS P	rofiling						
HTTP TLV	Caching						
DHCP TL	/ Caching						
WLAN Lo	ocal Profiling						
Global Sta Classificat	te of Device tion	Enabled 🤅	\rangle				
Local Sub	scriber Policy Name	BlockPoli	cy 🗙 🔻)			

RADIUS分析配置

要使RADIUS分析生效,除了全局启用设备分类(如本地分析配置中所述),还需要:

1.使用指向RADIUS服务器的"身份"类型配置AAA记帐方法:

Configuration * > Securi	y*> AAA				
+ AAA Wated					
Servers / Groups	Method List AAA Advanced				
Authentication					
Authorization	+ Add X Deare				
Accounting	Name < Type	< Group 1	< Group2	< Group3	≺ Group4 v
	AccMethod Identity	15622	NIA	N/A	NA
	H + 1 + H 20 •	toms per page			1 - 1 of 1 home

2.需要在Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced下添加会计方法:

ieneral	Access Policies	QOS and AVC	Mobility	Advanced	
WLAN T	ïmeout			Fabric Profile	Search or Select
Session 1	Timeout (sec)	1800		mDNS Service Policy	default-mdns-servici •
Idle Time	out (sec)	300		Hoterod Savar	Search or Select
Idle Thre	shold (bytes)	0		Thompson Over Hur	
Client Ex	clusion Timeout (sec)	60		User Private Networ	ſk
Guest LA	N Session Timeout	0		Status	
DHCP		-		Drop Unicast	
		-		Umbrella	
DHCP Se	P Required			Umbrella Parameter Map	Not Configured
how more	333			Flex DHCP Option for DNS	
AAA Po	licy			DNS Traffic Redirect	IGNORE
Allow AA	A Override			WLAN Flex Policy	
NAC Stat	te			VLAN Central Switching	na 🗖
NAC Typ	0	RADIUS	•	Split MAC ACL	Search or Select
Policy Na	me	default-aaa-policy y	• •		
Announti	an List	AcctMethod		Air Time Fairness Po	olicies

3.最后,需要在Configuration > Tags & Profiles > Policy下勾选RADIUS Profiling复选框此复选框启 用HTTP和DHCP RADIUS分析(旧的AireOS WLC有2个单独的复选框):

Edit Policy Profile						
General Access	Policies	QOS a	nd AVC	Mobility		Advanced
RADIUS Profiling						
HTTP TLV Caching						
DHCP TLV Caching			 Image: A start of the start of			
WLAN Local Profil	ing					
Global State of Devic Classification	CB	E	Enabled (i)]		
Local Subscriber Po	licy Name		BlockPolic	y x	•	

分析使用案例

基于本地分析分类应用本地策略

此示例配置演示了本地策略的配置,该本地策略具有QoS配置文件阻止youtube和facebook访问,仅应用于被分析为Windows-Workstation的设备。

只需稍作更改,即可修改此配置,例如,仅对无线电话设置特定DSCP标记。

导航到配置 > 服务 > QoS以创建QoS配置文件。点击add以创建新策略:

dudu Cisco	Cisco Catalyst 9800 - CL Wroless Controller	Veloces white A R R R R R R R R R R R R R R R R R R
Q Second Marcola	Configuration * > Services * > Qot	
Deshboard	T AM	Deater AutoGrl5
C Montoring	Policy Name - Associated Class-Maps	 Associated Interfaces/Profiles
Conternation	a a d a a 20 a term prope	No here to digitary

指定策略名称并添加新的类映射。从可用协议中,选择需要被阻止、已标记DSCP或已限制带宽的 协议。

在本例中,youtube和facebook被阻止。请确<u>保不</u>将此QoS配置文件应用于QoS窗口底部的任何策 略配置文件:

QoS								
Auto QOS	DISABLED							
Policy Name*	block							
Description								
Match v Match Value	< Mark Type	< Mark Value	< Polk (kbp	ce Value 🖂 ss)	Drop ~	AVC/User Defined	~	Actions ~
н н О н н	20 🔹 itom	s per page					No ite	ms to display
	× Delete							
AVC/User Defined	AVC							
Match	⊛ Any (D AI						
Drop								
Match Type	protocol	٠						
	A mitchie Protoco	a(n)		10.000				
	Available Protoco		Selecte	d Protocol(s)				
	3com-amp3 3com-tsmux	^ >	youtub	d Protocol(s)	^			
	3com-amp3 3com-tsmux 3pc 4chan		youtub facebo	od Protocol(s) 50 50k	< >			ų
	3com-amp3 3com-tsmux 3pc 4chan	* > *	youtut facebo	d Protocol(s) be ook	¢	D Can	eet 1	₽
	3com-amp3 3com-tsmux 3pc 4chan	* > *	youtub facebo	o Protocol(s)	< >	D Can	cel	€ Save
vailable (8)	3com-amp3 3com-tsmux 3pc 4chan	* > v	youtut facebo	Selected ())	D Can	cel	₽ Save
kvailable (8) Yofiles	3com-amp3 3com-tsmux 3pc 4chan	× ×	Selecte youtub facebo	Selected (I)	D Care Ing	ress	Save Egress
vailable (8) rofiles	3com-amp3 3com-tsmux 3pc 4chan	*	yound facebo	Selected (I)	D Care	ress	Save Egress
wailable (8) rofiles vasa	3com-amp3 3com-tsmux 3pc 4chan	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	yound facebo	Selected (I)	D Care Ing	ress	Save Egress
Ivailable (8) Irofiles Irofiles Vasa Irofiles Vasa Irofiles Vasa Irofiles Vasa Irofiles Vasa Irofiles Irofiles	3com-amp3 3com-tsmux 3pc 4chan	* *	Selecte youtub facebo	Selected (I))	D Carv	ress	Save Egress
Ivailable (8) rofiles is vasa is 33nps is webauth is 11webauth	3com-amp3 3com-tsmux 3pc 4chan	* * *	yound facebo	Selected (I))	D Carr	ross	Save Egress
Ivailable (8) Ivofiles Ivasa Ivas Ivas	3com-amp3 3com-tsmux 3pc 4chan	* * *	Seecte yound facebo	Selected (I))	D Carr	ress	Egress
Available (8) Irofiles Irofiles Irofiles Incolority Incolority Incolority Incolority Incolority Incolority	3com-amp3 3com-tsmux 3pc 4chan	* * * *	Selecte yound facebo	Selected (/ Profiles))	D Carr	ross	Egress

I

导航到Configuration > Security > Local Policy并创建新的服务模板:

Configuration * > Security * > Local Policy		
Service Template Policy Map		
+ Add × Deem		
Service Template Name	< Source	~
webeuth-global-inactive		
DIFAUT_CRITICAL_DATA_TEMPLATE		
DEFAULT_CRITICAL_VOCE_TEMPLATE		
DEFAULT_LINKSEC_POLICY_MUST_SECURE		
DEFAULT_LINKSEC_POUCY_SHOULD_SECURE		
H H 1 H 20 e hame per page		1 - 5 of 5 items

指定在上一步中创建的入口和出口QoS配置文件。在此步骤中还可以应用访问列表。如果无需更改 VLAN,请将vlan字段留空:

Create Service Templat	е	×
Service Template Name*	BlockTemplate	
VLAN ID	1-4094	
Session Timeout (secs)	1-65535	
Access Control List	None 🔻	
Ingress QOS	block x v	
Egress QOS	block x v	
mDNS Service Policy	Search or Select	Ŷ
D Cancel		Apply to Device

导航到Policy Map选项卡,然后点击add:

Configuration * > Security * > Local Policy	
Service Template Policy Map	
+ Add × Delete	
Policy Map Name	*
BULTN, AUTOCONF, POLICY	
H + 1 + H 20 + Harris per page	1 - 1 of 1 Items

设置策略映射名称并添加新条件。指定在上一步中创建的服务模板,并选择应用此模板的设备类型 。

在本例中,使用Microsoft-Workstation。如果定义了多个策略,则使用第一个匹配项。

另一个常见使用案例是指定基于OUI的匹配条件。如果部署具有大量相同型号的扫描仪或打印机,它们通常具有相同的MAC OUI。

这可用于应用特定QoS DSCP标记或ACL:

ate Policy Map Co	guration
olicy Map Name *	BlockPolicy
latch Criteria List	
+ Add X Deb	Move To All All Move Down
Device Type(Match Criteria)	✓ User Role(Match ∨ User Name(Match ∨ OUI(Match ∨ OUI(Match ∨ Address(Match ∨ Address(Match ⊂ Horizeria))
	20 kerns per page No items to display
ervice Template *	BlockTemplate x · Microsoft · Workstatic ·
evice Type	eq • Microsoft-Workstatic •
ser Role	Select Filter Type Enter User Role
ser Name	Select Filter Type Enter User Name
u	Select Filter Type
IAC Address	Select Filter Type
Add Criteria	novi
	Į,

为了使WLC能够识别youtube和facebook流量,需要打开应用可视性。

导航到**配置 > 服务 > 应用可视性** e对您的WLAN的策略配置文件启用可视性:

and a second second second second	president function			
Inable AVC Define Pr	licy .			
0 Peterset				
rag and Drop, double click or click o	the button from Selected Profiles to addition Enabled (1)	ove Profiles	Q, Search	E Assi
holies	Profiles	Visibility	Collector Address	
vofiles	Profiles	Vsibility	Collector Address	
tofies 11webauth	Profiles Profiles Toverride	Visbility	Collector Address	+
Yoffes Illwebauth Illwebluth Illwebluty Illweblity Illprofiling	Profiles Profiles Toverride	Visbility	Collector Address	+
Voties Illwobauth Illwobility Illprofiling Illprofiling Illprofiling	Profiles Profiles Profiles	Vability	Collector Address	*
holies illwebauth illw	Profiles	Vsibility	Collector Address	÷

验证在策略Profile下,已启用HTTP TLV缓存、DHCP TLV缓存、全局设备分类,并且本地用户策略 指向在以上步骤之一中创建的本地策略映射:

eneral	Access Policies	QOS and AVC	Mobility	Advanced			
RADIUS	Profiling				WLAN ACL		
HTTP TU	V Caching	2			IPv4 ACL	Search or Select	•
DHCP TL	.V Caching				IPv6 ACL	Search or Select	•
WLAN I	Local Profiling				URL Filters		
Global St Classific:	tate of Device ation	Enabled (Þ		Pre Auth	Search or Select	•
Local Su	bscriber Policy Name	BlockPol	cy 🛪 •		Post Auth	Search or Select	•
VLAN							
VLAN/VL	AN Group	VLAN00	39 •]			
Multicast	VLAN	Enter M	ulticast VLAN	1			

客户端连接后,可以检查是否已应用本地策略,并测试youtube和facebook是否实际被阻止。

show wireless client mac-address [MAC_ADDR] detailed的输出包括:

Input Policy Name	: block
Input Policy State	: Installed
Input Policy Source	e : Native Profile Policy
Output Policy Name	: block
Output Policy State	e : Installed
Output Policy Sour	ce : Native Profile Policy
Local Policies:	
Service Template	: BlockTemplate (priority 150)
Input QOS	: block
Output QOS	: block
Service Template	: wlan_svc_11override_local (priority 254)
VLAN	: VLAN0039
Absolute-Timer	: 1800
Device Type :	Microsoft-Workstation
Device Name :	MSFT 5.0
Protocol Map :	0x000029 (OUI, DHCP, HTTP)
Protocol :	HTTP

思科ISE中的高级策略集的RADIUS分析

启用RADIUS分析后,WLC将分析信息转发到ISE。根据此信息,可以创建高级身份验证和授权规 则。

本文不包括ISE配置。有关详细信息,请参阅<u>Cisco ISE分析设计指南</u>。

此工作流程通常需要使用CoA,因此请确保在9800 WLC上启用此工作流程。

FlexConnect部署中的分析

集中身份验证、本地交换

在此设置中,本地和RADIUS分析继续按前几章所述工作。如果AP进入独立模式(AP失去与WLC的连接),设备分析将停止工作,并且没有新的客户端能够连接。

本地身份验证、本地交换

如果AP处于连接模式(AP加入到WLC),分析将继续工作(AP将客户端DHCP数据包的副本发送 到WLC以执行分析过程)。

尽管分析工作正常,但由于身份验证在AP上本地执行,因此分析信息不能用于任何本地策略配置或 RADIUS分析规则。

故障排除

放射性痕迹

排除WLC上的客户端配置文件故障的最简单方法是使用放射性跟踪。导航到**故障排除 > 放射跟踪** ,输入客户端无线适配器MAC地址,然后点击"开始":

Troubleshooting - > Radioactive Trace

Co	nditional Debug Global Stat	te: Started	
+	Add × Delete	Start Stop	
	MAC/IP Address	Trace file	
	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt 📥	► Generate
14	< 1 ► H 20	 items per page 	1 - 1 of 1 items

将客户端连接到网络,并等待它达到运行状态。停止跟踪,然后单击Generate。确保启用内部日志 (此选项仅存在于17.1.1版本及更高版本中):

Enter time interval		×
Enable Internal Logs		
Generate logs for last	10 minutes	
	O 30 minutes	
	O 1 hour	
	o since last boot	
	O 0-4294967295 seconds v	
	Ŷ	
Cancel	Apply to Device	

放射性痕迹的相关片段可在以下位置找到:

WLC将客户端分析为Microsoft-Workstation:

2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_9000004] Device type for the session is detected as Microsoft-Workstation and old device-type not classified earlier &Device name for the session is detected as MSFT 5.0 and old device-name not classified earlier & Old protocol map 0 and new is 41 2020/06/18 10:46:41.052367 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (debug): [74da.38f6.76f0:capwap_9000004] updating device type Microsoft-Workstation, device name MSFT 5.0

WLC缓存设备分类:

(debug): [74da.38f6.76f0:unknown] Updating cache for mac [74da.38f6.76f0] device_type: Microsoft-Workstation, device_name: MSFT 5.0 user_role: NULL protocol_map: 41 WLC在缓存中查找设备分类:

(info): [74da.38f6.76f0:capwap_90000004] Device type found in cache Microsoft-Workstation WLC应用基于分类的本地策略:

(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match for 74da.38f6.76f0 / 0x9700001A (info): device-type Filter evaluation succeeded (debug): match device-type eq "Microsoft-Workstation" :success WLC发送包含DHCP和HTTP分析属性的记帐数据包:

```
[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Getting active filter list
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found http
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found dhcp
[aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0
[aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-
Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa)
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50
2d 4b 4c 52 45 30 4d 41
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e
30
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b
2c 2e 2f 77 79 f9 fc
```

http profiling sent in a separate accounting packet
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49

数据包捕获

在集中交换部署中,可以在WLC本身上执行数据包捕获。导航到**故障排除 > Packet Capture**,并在 此客户端正在使用的其中一个接口上创建新的捕获点。

需要在vlan上具有SVI才能对其执行捕获,否则需要在物理端口本身上捕获数据

Troubleshooting * > Packet Capture	
Capture - Name Interface - Monitor Control Plane - Buffer Size - Filter by - Limit 1	katus - Action
x x 0 x x 20 x here per page	
Create Packet Capture	×
Capture Name* Cepture	
Filter* My +	
Monitor Control Plane	
Buffer Size (M8)* 10	
Limit by* Duration • 3600 secs -+ 1.00 hour	
Available (4) Search Q Selected (1)	
Ggabitthemeti + CV Van39	*
GgiotEneret2 +	
Ggabilitemed +	
Л	
Cancel E Apoly to Dev	ce

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)。