使用Dot1x保护Flexconnect AP交换机端口

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> 配置 <u>网络图</u>

<u>验证</u> <u>故障排除</u>

简介

本文档介绍用于保护交换机端口的配置,其中FlexConnect接入点(AP)使用device-trafficclass=switch Radius VSA向Dot1x进行身份验证,以允许来自本地交换的无线LAN(WLAN)的流量。

先决条件

要求

Cisco 建议您了解以下主题:

- •无线局域网控制器(WLC)上的FlexConnect
- 思科交换机上的802.1x
- 网络边缘身份验证拓扑(NEAT)

使用的组件

本文档中的信息基于以下软件和硬件版本:

- WS-C3560CX-8PC-S , 15.2(4)E1
- AIR-CT-2504-K9、8.2.141.0
- •身份服务引擎(ISE)2.0
- •基于IOS的接入点(x500、x600、x700系列)。

自撰写本文时起,基于AP OS的第2波AP不支持flexconnect trunk dot1x。

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



在此设置中,接入点充当802.1x请求方,由交换机使用EAP-FAST对ISE进行身份验证。一旦端口配 置为802.1x身份验证,交换机将不允许除802.1x流量以外的任何流量通过端口,直到连接到端口的 设备成功进行身份验证。

一旦接入点根据ISE成功进行身份验证,交换机将收到Cisco VSA属性"device-trafficclass=switch,并自动将端口移至中继。

这意味着,如果AP支持FlexConnect模式并配置了本地交换SSID,它将能够发送标记流量。确保在 AP上启用了VLAN支持,并配置了正确的本征VLAN。

AP配置:-

1.如果AP已加入WLC,请转到Wireless(无线)选项卡,然后点击接入点。转到Credetials字段 ,在802.1x Supplicant Credentials标题下,选中**Over-ride Global credentials**框,设置此接入点的 802.1x用户名和密码。

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ontroller	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MM/
Wireless	All APs > [Details fo	or Aks_desk	_3502			
 Access Points All APs Radios 	General	Creden	ntials Inte	rfaces	High Availabili	ty Inventory	/ Fle
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Crede	e ntials Global cre	dentials				
 Advanced Mesh 	802.1x Sup	plicant Cre	edentials				
▶ ATF	Over-ride Global credentials						
RF Profiles	Username ritmahaj						
FlexConnect Groups	Passwo	ord	•••••				
FlexConnect ACLs FlexConnect VLAN Templates	Confirm	n Password	•••••				

您还可以使用全局配置菜单为加入WLC的所有接入点设置命令用户名和密码。

	CISCO	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Wir	alace	CDP State	2			۲		to	3600)		120
***	61633	Etherne	t Interface	# CDI	P State			AF	P Primed	Join Timeout(120 -	0
- 1	Access Points	0		2				4.	3200 seco	inds)	-
	All APs	1		2 2				Ba	ack-up Pri	mary Controller IP v4/Inv6)	
	802.11a/n/ac	3							ade un De	many Controllor name	_
	802.11b/g/n	4		1				Ba	аск-ир Рп	mary Controller name	
Г	Dual-Band Radios Global Configuration	Radio S	lot#	CDI	State			Ba	ack-up Se ddress(Ip	condary Controller IP v4/Ipv6)	
5	duanced	0						Ba	ack-up Se	condary Controller	-
	auvanceu	1		1				na	ame		
1	Mesh	2		1							
1 1	ATF							TCP	MSS		
F	RF Profiles	Login Cr	redentials	5				Glo 13	bal TCP	Adjust MSS (IPv4: 536	- 🗊
F	lexConnect Groups	Userna	me					10	00, 11 10.	1220 1331)	
1	FlexConnect ACLs FlexConnect VLAN	Passwo	ord					AP F Para	meters	mit Config	
i i	Templates	Enable	Password		1			A	P Retrans	mit Count	5
9	DEAP ACLs								Betrane	mit Intorval	2
r	Network Lists	802.1x	Supplican	t Credentials	5			A	r Keu ans	nit friter var	2
۶ م	302.11a/n/ac	802.1x	Authenticati	ion				OEA	P Confi	g Parameters	
• 8	302.11b/g/n	Userna	ime					Di	isable Loc	al Access	
) I	Media Stream	Passwo	ord					NO	DTE:	ais feature could vial	ate si
+ /	Application Visibility And Control	Confirm	n Password					wi	thin you mpliance	r organization. Pleas with all regulations	e mai befo.

2.如果接入点尚未加入WLC,则必须控制台进入LAP以设置凭证并使用以下CLI命令:

LAP#debug capwap console cli LAP#capwap ap dot1x username <username> password <password>

交换机配置:-

1.在交换机上全局启用dot1x并向交换机添加ISE服务器

aaa new-model

!

aaa authentication dot1x default group radius

!

AAA授权网络默认组RADIUS

!

dot1x system-auth-control

!

RADIUS服务器ISE address ipv4 10.48.39.161 auth-port 1645 acct-port 1646 键7 123A0C0411045D5679

2.现在配置AP交换机端口

interface GigabitEthernet0/4	
switchport access vlan 231	
switchport trunk allowed vlan 231,232)
switchport mode access	
authentication host-mode multi-host	
身份验证顺序dot1x	
身份验证端口控制自动	
dot1x pae authenticator	
生成树portfast边缘	

ISE配置:-

1.在ISE上,只需为AP授权配置文件启用NEAT即可设置正确的属性,但是,在其他RADIUS服务器 上,您可以手动配置。

Authorization Profiles > AP_Flex_Trunk						
Authorization Profil	e					
* Name	AP_Flex_Trunk					
Description						
* Access Type	ACCESS_ACCEPT					
Network Device Profile	ditto Cisco 💌 🕀					
Service Template						
Track Movement						
 Common Tasks 						
NEAT						

2.在ISE上,还需要配置身份验证策略和授权策略。在这种情况下,我们点击了默认身份验证规则 ,即wired dot1x,但您可以根据要求对其进行自定义。

对于授权策略(Port_AuthZ),在本例中,我们将AP凭证添加到用户组(AP),并根据此推送授权配置 文件(AP_Flex_Trunk)。

Authorization Policy

	d Rule Applies	*		
Except	ons (0)			
Standard				
				2
Statu	is Rule Name		Conditions (identity groups and other conditions)	Permissions

验证

使用本部分可确认配置能否正常运行。

1.在交换机上,一旦可以使用命令"debug authentication feature autocfg all"检查端口是否移动到中 继端口。

2月20日12:34:18.119:%LINK-3-UPDOWN:接口GigabitEthernet0/4,状态更改为up 2月20日12:34:19.122:%LINEPROTO-5-UPDOWN:接口GigabitEthernet0/4上的线路协议,状态更 改为up akshat sw# akshat sw# 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:在dot1x AutoCfg start_fn中 , epm_handle:3372220456 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[588d.0997.061d, Gi0/4]设备类型=交换机 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[588d.0997.061d, Gi0/4]新客户端 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]内部Autocfg宏应用状态:1 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]设备类型:2 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]自动配置:stp有port_config 0x85777D8 2月20日12:38:11.113:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]自动配置:stp port_config有bpdu guard_config 2 2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]在端口上应用auto-cfg。 2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4] VLAN:231 VLAN-STR:231 2月20日12:38:11.116:AUTH-FEAT-AUTOCFG-EVENT:[Gi0/4]应用dot1x autocfg supp宏 2月20日12:38:11.116:正在应用命令…… Gi0/4上的"no switchport access vlan 231" 2月20日12:38:11.127:正在Gi0/4应用命令……"no switchport nonegotiate" 2月20日12:38:11.127:正在Gi0/4应用命令……"switchport mode trunk" 2月20日12:38:11.134:正在应用命令…… Gi0/4上的"switchport trunk native vlan 231" 2月20日12:38:11.134:正在Gi0/4应用命令……"spanning-tree portfast trunk" 2月20日12:38:12.120:%LINEPROTO-5-UPDOWN:接口GigabitEthernet0/4上的线路协议,状态更 改为down 2月20日12:38:15.139:%LINEPROTO-5-UPDOWN:接口GigabitEthernet0/4上的线路协议,状态更

改为up

2. "show run int g0/4"的输出将显示该端口已更改为中继端口。

当前配置295 bytes

! interface GigabitEthernet0/4 switchport trunk allowed vlan 231,232,239 switchport trunk native vlan 231 switchport mode trunk authentication host-mode multi-host 身份验证顺序dot1x 身份验证端口控制自动 dot1x pae authenticator 生成树portfast边缘中继 结束

3.在ISE上,在Operations>>Radius Livelogs下,我们可以成功进行身份验证并推送正确的授权配置 文件。

Time •	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles 1
2017-02-20 15:05:48.991	0	ò	0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991		ò		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk a
2017-02-20 15:04:49.272	1	ò		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	a

4.如果在此之后连接客户端,则其mac地址将在客户端vlan 232的AP交换机端口上学习。

akshat_sw#sh mac address-table int g0/4 MAC 地址表

Vlan Mac Address Type Ports

231 588d.0997.061d静态Gi0/4 - AP 232 c0ee.fbd7.8824动态Gi0/4 — 客户端

在WLC上,在客户端详细信息中可以看到此客户端属于vlan 232,并且SSID在本地交换。这是代码 片断。

(思科控制器)>show client	t detail c0:ee:fb:d7:88:24
客户 MAC 地址	c0:ee:fb:d7:88:24
客户端用户名	不适用
AP MAC地址	b4:14:89:82:cb:90
AP 名称	Aks_desk_3502
AP无线电插槽ID	1
客户端状态	
客户端用户组	
客户端NAC OOB状态	接入
无线LAN ID	2
无线LAN网络名称(SSID)。	端口身份验证
无线LAN配置文件名称	端口身份验证
热点(802.11u)。	Not Supported
BSSID	b4:14:89:82:cb:9f

已连接	
通道	
IP Address	
网关地址	
网络掩码	
关联ID	1
验证法则	。开放系统
原因代码	
状态代码	0

FlexConnect数据交换	本地
FlexConnect DHCP状态	本地
基于FlexConnect VLAN的中央交换.	无
FlexConnect身份验证	中心
FlexConnect中心关联	无
FlexConnect VLAN名称	vlan 232
隔离VLAN0	
Access VLAN	232
本地桥接VLAN23	32

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 如果身份验证失败,请使用debug dot1x和debug authentication命令。
- 如果端口未移动到中继,请输入debug authentication feature autocfg all命令。
- •确保已配置多主机模式(身份验证主机模式多主机)。必须启用多主机才能允许客户端无线 MAC地址。

• 必须配置"aaa authorization network"命令,交换机才能接受并应用ISE发送的属性。

基于Cisco IOS的接入点仅支持TLS 1.0。如果RADIUS服务器配置为仅允许TLS 1.2 802.1X身份验 证,则这可能导致问题