使用FlexConnect本地交换的外部Web身份验证部 署指南

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>规则</u> <u>功能概述</u> 相关信息

简介

本文档说明如何将外部Web服务器与FlexConnect本地交换一起用于不同的Web策略。

先决条件

要求

尝试进行此配置之前,请确保满足以下要求:

- 有关FlexConnect架构和接入点(AP)的基本知识
- 有关如何设置和配置外部 Web 服务器的知识
- 有关如何设置和配置 DHCP 和 DNS 服务器的知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件版本7.2.110.0的Cisco 7500无线LAN控制器(WLC)
- 思科3500系列轻量接入点(LAP)
- •托管 Web 身份验证登录页面的外部 Web 服务器
- •本地站点上的DNS和DHCP服务器,用于向无线客户端分配地址解析和IP地址

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。虽然7500系列WLC用于本部署指南,但 2500、5500和WiSM-2 WLC支持此功能。本文档中使用的所有设备最初均采用原始(默认)配置。 如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 <u>Cisco 技术提示规则。</u>

功能概述

此功能将对具有本地交换流量(FlexConnect — 本地交换)的WLAN从AP在FlexConnect模式下将 执行Web身份验证的功能扩展到外部Web服务器。 在WLC版本7.2.110.0之前,对于具有集中交换 流量的WLAN(FlexConnect — 中央交换),本地模式或FlexConnect模式下的AP,支持外部服务 器的Web身份验证。

此功能通常称为外部Web身份验证,它扩展了FlexConnect本地交换WLAN的功能,以支持控制器当 前提供的所有第3层Web重定向安全类型:

- Web 身份验证
- Web直通
- Web条件重定向
- 启动页条件重定向

考虑为Web身份验证和本地交换配置的WLAN,此功能背后的逻辑是直接在AP级别而非WLC级别分 发和应用预身份验证FlexConnect访问控制列表(ACL)。这样,AP将在本地交换来自ACL允许的无线 客户端的数据包。不允许的数据包仍通过CAPWAP隧道发送到WLC。另一方面,当AP通过有线接 口接收流量时(如果ACL允许),会将其转发到无线客户端。否则,将丢弃该数据包。一旦客户端 经过身份验证和授权,即会删除预身份验证FlexConnect ACL,并允许所有客户端数据流量在本地 交换。

注意:此功能的工作假设是客户端可以从本地交换的VLAN到达外部服务器。



摘要:

- •为FlexConnect本地交换和L3安全配置的WLAN
- FlexConnect ACL将用作预身份验证ACL
- 配置后的FlexConnect ACL必须通过Flex组或单个AP推送到AP数据库,或者可以应用到WLAN

要配置此功能,请完成以下步骤:

1. 为FlexConnect本地交换配置WLAN。

CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAG	EMENT COMMANDS HELP FEEDBACK
CISCO /LANs WLANs MULANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGE WLANS > Edit 'Store 1' General Security QoS Advanced Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Naximum Allowed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Static IP Tunneling Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Naximum Allowed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Maximum Allowed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Maximum Allowed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Maximum Allowed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Observed Clients Image: Client Exclusion = Image: Client Exclusion = Image: Client Exclusion = Observed Client = Image: Client Exclusion = Image: Client = Image: Client = Observed Client = Image: Client = Image: Client =	EMENT COMMANDS HELP FEEDBACK
	Scan Defer Time(msecs) 100 FlexConnect	Voice Media Session Snooping Enabled Re-anchor Roamed Voice Clients Enabled KTS based CAC Policy Enabled
	Switching 2	Client Profiling

2. 要启用外部Web身份验证,您需要将Web策略配置为本地交换WLAN的安全策略。这包括以下 四个选项之一:身份验证直通条件Web重定向启动页Web重定向本文档捕获了Web身份验证的 示例

.ı ı.ı ı. cısco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
WLANs	WLANs > Edit 'S	Store 1'					
WLANs	General Secu	rity QoS	Advanced				
Advanced	Layer 2 Lay	er 3 AAA Se	ervers				
	Layer 3 Securit Web Policy Authenticati Passthrough Conditional Splash Page On MAC Filt Preauthenticati	Web Redirect Web Redirect Web Redirect er failure ¹⁰ on ACL IPv4	None ÷	IPv6 None :	WebAuth Flex	Acl None ÷	

前两种方法相似,可从配置角度分组为Web身份验证方法。第二个(条件重定向和启动页)是 Web策略,可以按Web策略方法分组。

3. 需要配置预身份验证FlexConnect ACL,以允许无线客户端访问外部服务器的IP地址。ARP、 DHCP和DNS流量是自动允许的,无需指定。在"安全">"访问控制列表"下,选择FlexConnect ACL。然后,单击Add,将名称和规则定义为普通控制器ACL。

Acce	ccess Control Lists > Edit									
Gene	ral									
Access	List Name	e flex_	pre_auth							
Seq	Action	Source IP/M	ask	Destination I	P/Mask	Protocol	Source Port	Dest Port	DSCP	
1	Permit	0.0.0.0	/ 0.0.0.0	10.1.1.29	/ 255.255.255.255	Any	Any	Any	Any	

注意:您每次都需要为流量创建反向规则。

4. 创建FlexConnect ACL后,应应用该ACL,该ACL可在不同级别执行:AP、FlexConnect组和WLAN。最后一个选项(WLAN上的Flex ACL)仅用于Web策略下的其他两种方法(如条件和启动重定向)的Web身份验证和Web传递。ACL只能应用于AP或Flex组。以下是在AP级别分配的ACL的示例。转至"无**线">选择AP**,然后单击"FlexConnect**"选**项卡

All APs > D	etails for 3600	1.0418				
General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced
VLAN Su	pport	Ø				
Native V	LAN ID	1	VLAN Mappings			
FlexConr	ect Group Name	Not C	Configured			
PreAuthent	ication Access Co	ntrol Lists				
External V	VebAuthentication AC					
OfficeExten	d AP					
Enable O	fficeExtend AP					
Enable L	east Latency Contro	oller Join Rese	et Personal SSID			

单击"外部**Web身份验证ACL"**链接。然后,为特定WLAN ID选择 ACL:

cisco	<u>M</u> ONITOR <u>W</u> LAN	s <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	не
Wireless	All APs > 36001	.0418 > ACL Ma	ppings				
 Access Points All APs Radios 802.11a/n 802.11b/g/n Global Configuration 	AP Name Base Radio MAC	36001.0418 64:d9:89:42:0e:20	0				
 Advanced Mesh 	WLAN ACL Map	ping					
RF Profiles FlexConnect Groups FlexConnect ACLs	WebAuth ACL	AP-flex-ACL					
802.11a/n	WLAN Id WLAN Pr	ofile Name	WebA	uth ACL	~		
Media Stream Country	1 flex		AP-fle	x-ACL			
Timers QoS	WebPolicy ACL	AP-flex-ACL	-				
	WebPolicy Access	s Control Lists	<u> </u>	- 4 > 4		+n	

同样,对于Web策略ACL(例如,条件重定向或启动页重定向),在点击同一外部Web身份验 证ACL链接后,您将收到一个选项以在WebPolicies下选择Flex Connect ACL。如下所示 :

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	н
Wireless	All APs > 36001.	0418 > ACL Ma	ppings				
 Access Points All APs Radios 802.11a/n 802.11b/g/n 	AP Name Base Radio MAC	3600I.0418 64:d9:89:42:0e:20	D				
Global Configuration Advanced	WLAN ACL Map	ping					
Mesh	WLAN Id 0						
RF Profiles	WebAuth ACL	AP-flex-ACL					
FlexConnect Groups FlexConnect ACLs	1	Add					
🖹 802.11a/n	WLAN Id WLAN Pro	file Name	WebA	uth ACL			
🖹 802.11b/g/n	1 flex		AP-fie	x-ACL	•		
Media Stream							
Country	WebPolicies						
Timers	WebPolicy ACL	AP-flex-ACL	-				
QoS		Add					
	WebPolicy Access	Control Lists					

5. ACL也可应用于FlexConnect组级别。为此,请转至FlexConnect组配**置中的WLAN-**ACL映射 选项卡。然后,选择要应用的WLAN Id和ACL。单击 **Add**。当您要为一组AP定义ACL时,此 功能非常有用。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless	FlexConnect Groups > Edit 'Store1-Flex'
Access Points All APs Radios	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping WebPolicies
802.11a/n 802.11b/g/n Global Configuration	WLAN ACL Mapping
Advanced	
Mesh	
RF Profiles	WebAuth ACL
FlexConnect Groups FlexConnect ACLs	Add
▶ 802.11a/n	WLAN To WI AN Reofile Name WebAuth ACI
▶ 802.11b/g/n	1 flex
Media Stream	
Country	
Timers	
▶ QoS	

同样,对于Web策略ACL(用于条件和启动页Web重定向),您需要选择Web策略**选项**卡。



6. Web身份验证和Web直通Flex ACL也可应用于WLAN。为此,请从WLAN > Security中的 Layer 3选项卡下的WebAuth FlexACL下拉菜单中选择ACL。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'Store 1'
WLANS	General Security QoS Advanced
▶ Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security None 💌
	Web Policy A
	Authentication
	O Passthrough
	O Conditional Web Redirect
	O Splash Page Web Redirect
	On MAC Filter failure ¹⁰
	Preauthentication ACL IPv4 None V IPv6 None WebAuth FlexAcl Group-Flex-Acl V
	Over-ride Global Config Enable Group-Flex-Acl

7. 对于外部Web身份验证,需要定义重定向URL。这可以在全局级别或WLAN级别执行。对于WLAN级别,单击Over-ride Global Config复选标记并插入URL。在全局级别,转到Security > Web Auth > Web Login Page:

	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK
C	Web Log	jin Page							
	Web Aut	hentication	Туре	Ext	ternal (Redirect	to external server)	•	_	
	Redirect	URL after I Webauth U	login IRL	http://:	10.1.1.29/logi	n.html			

限制:Web身份验证(内部或外部服务器)要求Flex AP处于连接模式。如果Flex AP处于独立 模式,则不支持Web身份验证。Web身份验证(内部或外部服务器)仅支持集中身份验证。如 果为本地交换配置的WLAN配置了本地身份验证,则无法执行Web身份验证。所有Web重定向 都在WLC上执行,而不是在AP级别执行。

相关信息

• <u>技术支持和文档 - Cisco Systems</u>