Proteja um Flexconnect AP Switchport com Dot1x

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Diagrama de Rede

_ <u>Verificar</u> <u>Troubleshoot</u>

Introduction

Este documento descreve a configuração para proteger as portas de switch em que os pontos de acesso (AP) FlexConnect se autenticam com Dot1x usando o VSA Radius de classe de tráfego de dispositivo para permitir o tráfego de LANs sem fio (WLANs) comutadas localmente.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexConnect no Wireless Lan Controller (WLC)
- 802.1x em switches Cisco
- Topologia de Autenticação de Borda de Rede (NEAT)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Identity Service Engine (ISE) 2.0
- Pontos de acesso baseados em IOS (série x500,x600,x700).

Os APs de onda 2 baseados em AP OS não suportam o dot1x de tronco flexconnect a partir do momento dessa gravação.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Nesta configuração, o access point atua como o suplicante 802.1x e é autenticado pelo switch em relação ao ISE usando EAP-FAST. Quando a porta é configurada para autenticação 802.1x, o switch não permite que nenhum tráfego diferente do 802.1x passe pela porta até que o dispositivo conectado à porta se autentique com êxito.

Quando o access point se autentica com êxito em relação ao ISE, o switch recebe o atributo Cisco VSA "device-traffic-class=switch e move automaticamente a porta para o tronco.

Isso significa que, se o AP suportar o modo FlexConnect e tiver SSIDs comutados localmente configurados, ele poderá enviar tráfego marcado. Verifique se o suporte de vlan está ativado no AP e se a vlan nativa correta está configurada.

Configuração de AP:-

1. Se o AP já estiver associado à WLC, vá até a guia Wireless (Sem fio) e clique no ponto de acesso. Vá para o campo Credetials e, no cabeçalho 802.1x Supplicant Credentials (Credenciais do candidato 802.1x), marque a caixa **Over-ride Global Credenciais** para definir o nome de usuário e a senha 802.1x para este ponto de acesso.

cisco	MONITOR WLA	Ns <u>C</u> ONT	ROLLER WI	RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MM/
Wireless	All APs > Deta	ails for Al	s_desk_35	02			
 Access Points All APs Radios 	General	redentials	Interface	es Hi	gh Availabili	ty Inventory	/ Fle
802.11a/17/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Credentia	als bal credentia	als				
 Advanced Mesh 	802.1x Supplica	ant Credent	ials				
> ATF	Over-ride Glo	bal credentia	ls				
RF Profiles	Username	ritn	nahaj				
FlexConnect Groups	Password •••••						
FlexConnect ACLs FlexConnect VLAN Templates	Confirm Pa	ssword •••	•••				

Você também pode definir um nome de usuário e uma senha de comando para todos os pontos de acesso que estão conectados à WLC com o menu Configuração global.

	CISCO	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
W	iroloce	CDP Stat	e			۲		to	3600) [′]		120
	1101055	Etherne	et Interface	e# CDF	State			AP	Primed	Join Timeout(120 -	0
-	Access Points	0		1				43	200 seco	onds)	0
	All APs	1						Ba	ck-up Pr	mary Controller IP	-
	Radios	2		1				Ad	dress(Ip	v4/Ipv6)	
	802.11a/n/ac	3		2				Ba	ck-up Pr	mary Controller name	
	Dual-Band Radios	4		×				Ba	ck-up Se	condary Controller IP	-
	Global Configuration	Radio S	slot#	CDF	State			Ad	dress(Ip	v4/Ipv6)	-
s.	Advanced	0						Ba	ck-up Se	condary Controller	1
	March	1		•				na	me		-
	Mesn	2		1				TCD	MCC		
Þ	ATF	Login C	redential	2				TCP	M55		
	RF Profiles	Login C	redential	S	16-			Glo 136	bal TCP	Adjust MSS (IPv4: 536 1220 - 1331)	- 0
	FlexConnect Groups	Userna	ame					40.0		mit Confin	
	FlexConnect ACLs	Passw	ord					Para	meters	init Coning	
	Templates	Enable	e Password					AP	Retrans	mit Count	5
	OEAP ACLS							40	Patrane	mit Interval	2
	Network Lists	802.1x	Supplica	nt Credentials				01	Retrans	the the val	5
۶	802.11a/n/ac	802.1x	Authenticat	ion				OEAI	P Confi	g Parameters	
	802.11b/g/n	Userna	ame					Di	sable Loo	al Access	
Þ	Media Stream	Passw	ord					NC En	TE: ablina ti	his feature could viol	late se
•	Application Visibility And Control	Confin	m Password					with	thin you opliance	r organization. Pleas with all regulations	se mai s befo.

2. Se o ponto de acesso ainda não ingressou em uma WLC, você deve usar o console no LAP para definir as credenciais e usar este comando CLI:

LAP#debug capwap console cli

LAP#capwap ap dot1x username <username> password <password>

Configuração do switch:-

1. Ative o dot1x no switch globalmente e adicione o servidor ISE ao switch

aaa new-model

!

aaa authentication dot1x default group radius

!

aaa authorization network default group radius

!

dot1x system-auth-control

!

radius server ISE address ipv4 10.48.39.161 auth-port 1645 acct-port 1646 tecla 7 123A0C0411045D5679

2. Agora configure a porta do switch AP

interface GigabitEthernet0/4 switchport access vlan 231 switchport trunk allowed vlan 231.232 switchport mode access authentication host-mode multi-host ordem de autenticação dot1x authentication port-control auto autenticador dot1x pae borda portfast de spanning tree

Configuração do ISE:-

1. No ISE, é possível simplesmente habilitar o NEAT para o perfil de autorização do AP para definir o atributo correto; no entanto, em outros servidores RADIUS, você pode configurar manualmente.

Authorization Profiles > AP	Flex_Trunk
Authorization Profil	e
* Name	AP_Flex_Trunk
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	dette Cisco 👻 🕀
Service Template	
Track Movement	
Common Toolo	

Common Tasks

2. No ISE, também é necessário configurar a política de autenticação e a política de autorização. Nesse caso, clicamos na regra de autenticação padrão, que é o dot1x com fio, mas é possível personalizá-la de acordo com o requisito.

Quanto à política de autorização (Port_AuthZ), neste caso, adicionamos as credenciais de AP a um grupo de usuários (APs) e enviamos o Perfil de autorização (AP_Flex_Trunk) com base nisso.

Authorizatio	on Policy				
Define the Author For Policy Expo	orization Policy by cor ort go to Administration	figuring rules based on ider > System > Backup & Rest	tity groups and/or other conditions. Drag and drop rules to change ore > Policy Export Page	the order.	
First Matched R	Rule Applies	*			
Exception	ns (0)				
Standard					
Status	Rule Name		Conditions (identity groups and other conditions)	Permissions	
1	Port_AuthZ	if	APs AND Wired_802.1X	then AP_Flex_Trunk	
Standard Status	Rule Name Port_AuthZ	if	Conditions (identity groups and other conditions) APs AND Wired_802.1X	Permissions then AP_Flex_Trunk	

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. No switch, uma vez pode usar o comando "debug authentication feature autocfg all" para verificar se a porta está sendo movida para a porta de tronco ou não.

20 de fevereiro 12:34:18.119: %LINK-3-UPDOWN: Interface GigabitEthernet0/4, estado alterado para ativado 20 de fevereiro 12:34:19.122: %LINEPROTO-5-UPDOWN: Protocolo de linha na interface GigabitEthernet0/4, estado alterado para ativado akshat sw# akshat sw# 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: No dot1x AutoCfg start_fn, epm handle: 3372220456 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Tipo de dispositivo = Switch 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] novo cliente 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Status Interno Do Aplicativo Macro Autocfg: 1 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Tipo de dispositivo: 2 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Configuração automática: stp tem port_config 0x85777D8 20 de fevereiro 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Configuração automática: stp port_config tem bpdu guard_config 2 20 de fevereiro 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Aplicando autocfg na porta. 20 de fevereiro 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231 20 de fevereiro 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Aplicando a macro dot1x_autocfg_supp

20 de fevereiro 12:38:11.116: Aplicando comando... 'no switchport access vlan 231' em Gi0/4 20 de fevereiro 12:38:11.127: Aplicando comando... 'no switchport nonegotiate' em Gi0/4 20 de fevereiro 12:38:11.127: Aplicando comando... 'switchport mode trunk' em Gi0/4 20 de fevereiro 12:38:11.134: Aplicando comando... 'switchport trunk native vlan 231' em Gi0/4 20 de fevereiro 12:38:11.134: Aplicando comando... 'spanning-tree portfast trunk' em Gi0/4 20 de fevereiro 12:38:12.120: %LINEPROTO-5-UPDOWN: Protocolo de linha na interface GigabitEthernet0/4, estado alterado para inativo 20 de fevereiro 12:38:15.139: %LINEPROTO-5-UPDOWN: Protocolo de linha na interface GigabitEthernet0/4, estado alterado para inativo

2. A saída de "show run int g0/4" mostrará que a porta foi alterada para uma porta de tronco.

Configuração atual: 295 bytes

! interface GigabitEthernet0/4 switchport trunk allowed vlan 231.232.239 switchport trunk native vlan 231 tronco de modo de porta de comutação authentication host-mode multi-host ordem de autenticação dot1x authentication port-control auto autenticador dot1x pae tronco de borda portfast de spanning tree fim

3. No ISE, em Operations>>Radius Livelogs, é possível verificar se a autenticação foi bemsucedida e se o perfil de autorização correto está sendo impresso.

Time	Status	Details	Repeat Count	Identity 🕐	Endpoint ID	Endpoint Profile	Authentication Policy (i)	Authorization Policy	Authorization Profiles	
2017-02-20 15:05:48.991	0	<u>.</u>	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	1	à		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk	ā
2017-02-20 15:04:49.272		ò		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ		a

4. Se conectarmos um cliente depois disso, seu endereço mac será aprendido na porta do switch AP na vlan 232 do cliente.

akshat_sw#sh mac address-table int g0/4 Tabela de endereço MAC

Portas Do Tipo De Endereço Mac Da Vlan

231 588d.0997.061d ESTÁTICA Gi0/4 - AP 232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Cliente

Na WLC, nos detalhes do cliente, pode-se ver que esse cliente pertence à vlan 232 e que o SSID é comutado localmente. Aqui está um trecho.

(Controlador Cisco) > show client of	detail c0:ee:fb:d7:88:24
Endereço MAC cliente	c0:ee:fb:d7:88:24
Nome de usuário do cliente	N/A
Endereço MAC do AP	b4:14:89:82:cb:90
Nome do AP	Aks_desk_3502

D do slot de rádio do AP 1	
Estado do cliente Associado	
Grupo de Usuários Clientes	
Estado OOB NAC do Cliente Acesso	
D da LAN sem fio 2	
Nome da rede LAN sem fio (SSID) Autenticação de por	rta
Nome do perfil da LAN sem fio Port-auth	
Hotspot (802.11u) Not Supported	
BSSIDb4:14:89:82:cb:9f	
Conectado para 42 seg	
Canal	
P Address 192.168.232.90	
Endereço do gateway 192.168.232.1	
Máscara de rede	
D da associação1	
Algoritmo de autenticação Sistema aberto	
Código de razão 1	
Código de status0	

Comutação de dados FlexConnect	Local
Status do FlexConnect Dhcp	Local
Comutação Central Baseada Em Vlan I	FlexConnect No
Autenticação FlexConnect	Central
Associação Central FlexConnect	No
NOME DA VLAN FlexConnect	vlan 232
Quarentena de VLAN	0
Acessar VLAN	232
Local Bridging VLAN	. 232

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Se a autenticação falhar, use os comandos debug dot1x, debug authentication.
- Se a porta não for movida para o tronco, insira o comando debug authentication feature autocfg all.
- Certifique-se de que o modo multi-host (autenticação host-modo multi-host) esteja configurado. Vários hosts precisam ser habilitados para permitir endereços MAC sem fio do cliente.
- o comando "aaa authorization network" deve ser configurado para que o switch aceite e aplique os atributos enviados pelo ISE.

Os pontos de acesso baseados no Cisco IOS suportam apenas TLS 1.0. Isso pode causar um problema se o servidor RADIUS estiver configurado para permitir somente autenticações TLS 1.2 802.1X