Secure a Flexconnect AP-switch met Dot1x

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram

Inleiding

Dit document beschrijft de configuratie om switches te beveiligen wanneer FlexConnect Access Point (AP) authentiek is met Dot1x met machine-verkeer-klasse=switch Radius VSA om verkeer van lokaal switched draadloze LAN's (WLAN's) toe te staan.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexConnect op draadloze LAN-controller (WLC)
- 802.1x op Cisco-Switches
- Network Edge-verificatietopologie (NEAT)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WS-C3560CX-8PC-S, 15.2(4)E1
- LUCHT-CT-2504-K9, 8.2.141.0
- Identity Services Engine (ISE) 2.0
- IOS-gebaseerde access points (x500,x600,x700 Series).

Wave 2 AP's gebaseerd op AP OS ondersteunen flexiconnect hoofdpunt1x niet vanaf het tijdstip van dit schrijven.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdiagram



Bij deze instelling fungeert het toegangspunt als de 802.1x-smeekbede en wordt geauthentiseerd door de switch tegen ISE met behulp van EAP-FAST. Zodra de poort is ingesteld voor 802.1x-verificatie, laat de switch geen ander verkeer dan 802.1x-verkeer door de poort lopen totdat het apparaat dat is aangesloten op de poort authentiek verklaard heeft.

Zodra het toegangspunt voor authentiek verklaard tegen ISE is, ontvangt de switch "device-trafficclass=switch van Cisco VSA-kenmerk en beweegt hij automatisch de poort naar de romp.

Dit betekent dat als AP de modus FlexConnect ondersteunt en SSID's lokaal is ingesteld, het gelabeld verkeer kan verzenden. Zorg ervoor dat de VLAN-ondersteuning is ingeschakeld op het AP en dat het juiste native VLAN is geconfigureerd.

AP configuratie:-

1. Als het AP reeds aan WLC is aangesloten, ga het tabblad Draadloos en klik op het access point. Gebruik het veld Gereedschappen en gebruik de optie 802.1x plus extra krediet, controleer het vakje **Gratis Global** aanmeldingsgegevens om de 802.1x-gebruikersnaam en het wachtwoord voor dit access point in te stellen.

cisco	<u>M</u> onitor <u>M</u>	<u>V</u> LANs <u>(</u>	ONTROLLER	WIRELESS	5 <u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MM/
Wireless	All APs > D	etails fo	r Aks_desk	_3502			
 Access Points All APs Radios 	General	Creden	tials Inte	rfaces	High Availabili	ity Inventory	Fle
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Creder	ntials Global cree	dentials				
Advanced Mesh	802.1x Supp	olicant Cre	dentials				
> ATF	Over-ride	Global cred	lentials				
RF Profiles	Usernan	ne	ritmahaj				
FlexConnect Groups	Passwor	rd	•••••				
FlexConnect ACLs FlexConnect VLAN Templates	Confirm	Password	•••••				

U kunt ook een veel te gebruiken naam en wachtwoord instellen voor alle access points die aangesloten zijn op de WLC in het menu Global Configuration.

	CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
14	Contains a	CDP State			۲		to 3	600)	, .	120
VV	ireless	Ethernet Interfac	ce# CDP	State			AP P	rimed :	loin Timeout(120 -	-
	Access Points	0					432	00 seco	nds)	0
1	All APs	1	×				Back	c-up Pri	mary Controller IP	-
	 Radios 	2	1				Add	ress(Ipv	v4/Ipv6)	
	802.11a/n/ac	3	 Image: A start of the start of				Back	c-up Pri	mary Controller name	
	802.11D/g/n Dual-Band Radios	4	2				Back	-up Se	condary Controller IP	_
	Global Configuration	Radio Slot#	CDP	State			Add	ress(Ip)	/4/Ipv6)	_
2	Advanced	0					Back	k-up Se	condary Controller	_
	Auvanceu	1	•				nam	e		_
	Mesh	2								
Þ	ATF	We want and the second of the second second					ТСР М	SS		
	RF Profiles	Login Credentia	Is				Globa 1363	al TCP /	Adjust MSS (IPv4: 536	- 🛛
	FlexConnect Groups	Username					1505	, 11 10.	1220 - 1551)	
	FlexConnect ACLs FlexConnect VLAN	Password					AP Re Paran	transi	mit Config	
	Templates	Enable Password		0			AP R	tetransr	nit Count	5
	OEAP ACLs						AP F	tetransr	nit Interval	3
	Network Lists	802.1x Supplica	int Credentials				74 1	ice and		~
Þ	802.11a/n/ac	802.1x Authentica	ation				OEAP	Confi	g Parameters	
	802.11b/g/n	Username					Disa	ble Loc	al Access	
Þ	Media Stream	Password					NOT	E: olina tl	is feature could viola	ate se
	Application Visibility And Control	Confirm Password	d				with com	in your	r organization. Please with all regulations	e mai befo.

2. Als het access point nog niet bij een WLC is aangesloten, moet u console in de LAP troosten om de aanmeldingsgegevens in te stellen en deze CLI-opdracht te gebruiken:

CLI voor LAP#debug-kapconsole

LAP#capwap dot1x gebruikersnaam <gebruikersnaam> <wachtwoord>

Configuratie switch:-

1. Schakel punt1x in op de switch en voeg ISE-server aan switch toe

nieuw model

!

aaa authenticatiedot1x standaardgroepsstraal

!

Standaard autorisatienetwerk groepsstraal

!

dot1x systeem-automatische controle

!

Straalserver ISE adres ipv4 10.48.39.161 16-poorts 1645 poort 1646 sleutel 7 123A0C0411045D5679

2. Stel nu de AP switch poort in

interface Gigabit Ethernet0/4 schakelpoort-toegangsnetwerk 231 schakelpoort-stam toegestaan VLAN 231.232 toegang tot de switchingmodus authenticatie host-mode multi-host echtheidscontrole dot1x Verificatie van poortregelaar dot1x pae-authenticator over-boom draagrand

ISE-configuratie:-

1. Op ISE kan NEAT voor het profiel met AP Authorization eenvoudig worden ingeschakeld om de juiste eigenschap op andere RADIUS-servers in te stellen. U kunt deze echter handmatig configureren.

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

2. Op ISE moet men ook het verificatiebeleid en het autorisatiebeleid configureren. In dit geval passen we de standaard authenticatieregel aan die wordt aangesloten op punt 1x, maar je kunt de regel aanpassen aan de eisen.

Wat betreft het autorisatiebeleid (Port_AuthZ) hebben we in dit geval de AP-referenties toegevoegd aan een gebruikersgroep (APs) en op basis hiervan het autorisatieprofiel (AP_Flex_Trunk) geduwd.

Auth	orizatio	n Policy				
Define For Po	the Autho blicy Export	rization Policy by configu t go to Administration > S	uring rules based on ider System > Backup & Rest	tity groups and/or other conditions. Drag and drop rules to chang ore > Policy Export Page	e the order.	
First	Matched R	ule Applies	*			
► E	xception	s (0)				
Sta	andard					
	Status	Rule Name		Conditions (identity groups and other conditions)	Permissions	
		Port_AuthZ	if	APs AND Wired_802.1X	then AP_Flex_Trunk	

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. In de switch, kan eens de opdracht "debug authenticatie optie autocfg all" gebruiken om te controleren of de poort al dan niet naar de boompoort wordt verplaatst.

20 feb. 12:34:18.19: %LINK-3-UPDOWN: Interface Gigabit Ethernet0/4, veranderde status in omhoog 20 feb. 12:34:19.122: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat aan omhoog akshat sw# akshat sw# 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle: 3372220456 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Apparaattype = Switch 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] nieuwe client 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [GI0/4] Interne automatische afschermingsmacrotoepassingsstatus: 1 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Apparaattype: 2 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische configuratie: stp heeft port fig 0x8577D8 20 feb. 12:38:11.13: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Automatische configuratie: stp port_fig heeft bpdu Guard_fig 2 20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Op de poort van toepassing. 20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] VLAN: VLAN-Str: 231 20 feb. 12:38:11.16: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Toepassing van dot1x autocfg supp macro 20 feb. 12:38:11.16: Bestellen toepassen... 'geen switchport toegang VLAN 231' bij Gi0/4

20 feb. 12:38:11.127: Bestellen toepassen... 'geen switchport nonegotiate' bij Gi0/4 20 feb. 12:38:11.127: Op bevel van toepassing... 'schakelport mode boomstam' op Gi0/4 20 feb. 12:38:11.134: Bezoek opdracht... 'switchport stam native vlan 231' bij Gi0/4 20 feb. 12:38:11.134: Op bevel toepassen... 'over-boom draagsnelle boomstam' bij Gi0/4 20 feb. 12:38:12.120: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat in beneden 20 feb. 12:38:15.139: %LINEPROTO-5-UPDOWN: Het protocol van de lijn op interface Gigabit Ethernet0/4, veranderde staat aan omhoog

2. De output van "show run int g0/4" toont aan dat de poort is veranderd in een boomstampoort.

Huidige configuratie: 295 bytes ! interface Gigabit Ethernet0/4 schakelpoort-stam toegestaan VLAN 231.232.239 switchport - moedertaal vlan 231 verbindingsmodems authenticatie host-mode multi-host echtheidscontrole dot1x Verificatie van poortregelaar dot1x pae-authenticator boomstam einde

3. Op ISE kan onder Operations> Radius Livelogs de echtheidscontrole succesvol zijn en kan het juiste autorisatieprofiel worden geduwd.

Time	Status	Details	Repeat Count	Identity 🕐	Endpoint ID	Endpoint Profile	Authentication Policy (1)	Authorization Policy	Authorization Profiles	
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	<u>o</u>		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ		a

4. Als we een client daarna verbinden, wordt het mac-adres geleerd op de AP switch poort in client VLAN 232.

akshat_sw#sh mac adres-tabel int g0/4 Mac-adrestabel

VLAN-adrespoorten

231 588d.0997.061d STATISCH Gi0/4 - AP 232 c0ee.fbd7.8824 DYNAMIC RGB0/4 - client

Op de WLC, in de details van de cliënt kan men zien dat deze cliënt vlan 232 behoort en SSID lokaal wordt geschakeld. Hier is een fragment.

(Cisco Controller) >Show client de	tail c0:ee:fb:d7:88:24
MAC-adres van client	c0:ee:fb:d7:88:24
Gebruikersnaam client	N.v.t.
AP MAC-adres	b4:14:89:82:cb:90
AP Naam	Aks_desk_3502
Identificatie van AP-radiogateway.	1

Clientstaat	geassocieerd
Clientgebruikersgroep	
ClientNAC OOB-status	Toegang
Draadloze LAN-id	2
Draadloze LAN-netwerknaam	(SSID) Poortaugustus
Naam draadloos LAN-profiel	Poortkantoor
Hotspot (802.11u)	Niet ondersteund
BSSID	b4:14:89:82:cb:9f
Verbonden voor	42 seconden
Kanaal	44
IP-adres	192.168.232.90
Gateway-adres	
Netmasker	
Associatie-id	
Verificatiealgoritme	Open systeem
Reden code	
Statuscode	

FlexConnect Data Switching	Lokaal
FlexConnect DHCP-status	Lokaal
FlexConnect VLAN-gebaseerde Centra	al-switching Nee
FlexConnect-verificatie	. Centraal
FlexConnect Central Association	Nee
FlexConnect VLAN-NAAM	VLAN 232
Quarantine VLAN	.0
Toegang tot VLAN	232
Local Bridging VLAN	232

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Als de authenticatie faalt, gebruik debug dot1x, debug authenticatie opdrachten.
- Als de poort niet naar romp is verplaatst, voer de **debug authenticatie optie in die alle** opdracht **heeft** geautoriseerd.
- Verzeker u hebt multi-host modus (authenticatie host-mode multi-host) ingesteld. Multi-Host moet worden ingeschakeld om client draadloze MAC-adressen toe te staan.
- De opdracht "een autorisatienetwerk" moet zodanig zijn geconfigureerd dat de switch de door ISE verzonden eigenschappen accepteert en toepast.

Cisco IOS-gebaseerde access points ondersteunen alleen TLS 1.0. Dit kan een probleem veroorzaken als uw RADIUS-server is geconfigureerd om alleen TLS 1.2 802.1X-authenticaties toe te staan