ISEを使用したWLCでのFlexConnect APによる CWAの設定

```
内容
```

<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ネットワーク図</u>
<u>WLC の設定</u>
ISE 設定
<u>許可プロファイルの作成</u>
認証ルールの作成
<u>許可ルールの作成</u>
<u>IP 更新の有効化(オプション)</u>
Traffic flow
<u>関連情報</u>

はじめに

このドキュメントでは、ローカルスイッチングモードのWLC ISE上のFlexConnect APで中央 Web認証を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ Cisco Identity Services Engine (ISE) リリース 1.2.1
- ・ ワイヤレスLANコントローラ(WLC)ソフトウェア、リリースバージョン 7.4.100.0
- アクセスポイント(AP)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明



注:現時点では、FlexAPでのローカル認証はこのシナリオではサポートされていません 。

このシリーズの他のドキュメント

- <u>スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例</u>
- WLC と ISE での中央 Web 認証の設定例

設定

ワイヤレス LAN コントローラ(WLC)の中央 Web 認証を設定するには複数の方法があります。 最初の方法は、ローカル Web 認証です。この認証では、WLC で HTTP トラフィックを内部サー バまたは外部サーバにリダイレクトし、そこでユーザは認証のための入力を求められます。WLC では、次にクレデンシャル(資格情報)を取得して(外部サーバの場合は HTTP GET リクエスト によって送り返される)、RADIUS 認証を行います。ゲストユーザの場合、ポータルがデバイス 登録やセルフプロビジョニングなどの機能を提供するため、外部サーバ(Identity Service Engine(ISE)またはNACゲストサーバ(NGS)など)が必要です。このプロセスには、次のステップ があります。

- 1. ユーザが Web 認証 SSID に関連付けられます。
- 2. ユーザが自分のブラウザを開きます。
- URL を入力するとすぐに、WLC によってゲスト ポータル(ISE や NGS など)にリダイレ クトされます。
- 4. ポータルで認証します。
- 5. ゲスト ポータルは WLC にリダイレクトして入力されたクレデンシャルを戻します。
- 6. WLC で、RADIUS によってゲスト ユーザを認証します。
- 7. WLC が元の URL にリダイレクトします。

このプロセスには、多くのリダイレクトが含まれています。新しいアプローチは、ISE(1.1 より も後のバージョン)および WLC(7.2 よりも後のバージョン)で機能する中央 Web 認証を使用 することです。このプロセスには、次のステップがあります。

- 1. ユーザが Web 認証 SSID に関連付けられます。
- 2. ユーザが自分のブラウザを開きます。
- 3. WLC はゲストのポータルにリダイレクトします。
- 4. ポータルで認証します。
- 5. ISE では、そのユーザが有効であることをコントローラに示すために RADIUS 認可変更 (CoA - UDP ポート 1700)を送信し、最後にアクセス コントロール リスト(ACL)など の RADIUS 属性をプッシュします。
- 6. ユーザは元の URL の再試行を促されます。

この項では、WLC および ISE に中央 Web 認証を設定するために必要な手順について説明します 。

ネットワーク図

この設定では、次のネットワーク設定を使用します。



ネットワーク構成

WLC の設定

WLC の設定は比較的簡単です。ISEからダイナミックな認証URLを取得するために、(スイッチ 上と同じように)テクニックを使用します(CoAを使用するため、セッションIDがURLの一部で あるため、セッションを作成する必要があります)。 MAC フィルタリングを使用するように SSID を設定し、MAC アドレスが見つからない場合でも Access-Accept メッセージを返し、その 結果すべてのユーザにリダイレクション URL を送信するように ISE を設定します。

また、RADIUS のネットワーク アドミッション コントロール(NAC)と、AAA オーバーライド を有効にする必要もあります。RADIUS NAC を使用すると、ユーザが認証済みで、ネットワーク にアクセスできることを示す CoA 要求を ISE が送信できます。また、RADIUS NAC は、ISE が ポスチャ結果に基づいてユーザ プロファイルを変更するポスチャ アセスメントにも使用されます 。

1. RADIUS サーバで RFC3576(CoA)が有効(デフォルト)になっていることを確認します 。

cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	неср	FEEDBACK
Security	RADIUS A	uthenti	cation Server	s > Edit					
 AAA General BADUUS BADUUS Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Wreb Auth TrustSec SXP Advanced 	Server Ind Server Ad: Shared Se Shared Se Confirm SP Key Wrap Port Numb Server Sta Support fo Server Tim Network U Manageme JPSec	lex dress cret Form cret hared Secr er fus r RFC 357 wout ser Ht	et 6	1 10.48.39.200 ASCIL I (Oesigned fo 1812 Enabled I Enabled I Scable Enable Enable	r FDPS custome	trs and requires a l	key wrap complia	et RADIL	5 server)

RADIUSサーバにはRFC3576があります

2. 新規 WLAN を作成してください。この例では、CWAFlexという名前の新しいWLANを作成 し、それをvlan33に割り当てます(アクセスポイントがローカルスイッチングモードである ため、この設定はあまり効果がないことに注意してください)。

ONITOR WL	ANS CO	NTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
LANs > Ed	it 'CWAI	Flex'					
General	Security	QoS	Advanced				
		-					
Profile Nam	e	CWAPIex	1				
Type		WLAN					
SSID		CWAFlex					
Status		🥑 Enabl	ed				
Radio Policy	,	(Modificat	ions done under	r security tab i	vill appear after app	plying the change	is.)
Interface/In Group(G)	terface	vlan33	•				
Multicast VI	an Feature	🗌 Enable	sd				
Broadcast S	SID	🗹 Enable	bd				
NAS-ID		WLC					

- 3. [Security] タブで、MAC フィルタリングをレイヤ 2 セキュリティとして有効にします。

General	eneral Security		Advanced							
Layer 2	Layer 3		ervers							
Layer 2	Layer 2 Security MAC Filtering									
Fast Trans	ition	-								
Fast Transit	ion 🖂									

MAC フィルタリングの有効化

4. [Layer 3] タブで、セキュリティが無効であることを確認します(Web 認証がレイヤ 3 で有 効にされると、中央 Web 認証ではなく、ローカル Web 認証が有効になります)。

General	Security	QoS	Advanced								
Layer 2	Layer 3	AAA S	ervers								
Layer 3	Layer 3 Security None +										
Web Policy											

セキュリティが無効になっていることを確認する

5. [AAA Servers] タブで、ISE サーバを WLAN の RADIUS サーバとして選択します。オプションで、ISE に関する詳細情報を得るためにアカウンティング用に ISE サーバを選択できます。

Layer 2 Layer 3 AAA Set	vers			
elect AAA servers below to overri	de use of default servers on thi	s WLAN		
ladius Servers			LDAP Server	18
Radius Server Overwrite interface	Enabled		Server 1	None
	Authentication Servers	Accounting Servers	Server 2	None
	S Enabled	S Enabled	Server 3	None
Server 1	IP:10.48.39.208, Port:1812 +	IP:10.48.39.208, Port:1813	•	
Server 2	None :	None	E)	
Server 3	None :	None	•	
Server 4	None 1	None		
Server 5	None :	None		
Server 6	None I	None		
Radius Server Accounting				
		-		

ISEサーバの選択

6. [Advanced] タブで、[Allow AAA Override] がオンで [NAC State] に対して [Radius NAC] が 選択されていることを確認します。

General	Security	QoS A	dvanced				
Allow AA	A Override	🗹 Enabled	1			DHCP	
Coverage	e Hole Detection	Enables				DHCP Server	Override
Linear a		Sessio	Timeout (s	ecs)		DHCP Addr. Assignment	🛃 Required
Airones I	is Channel	Enabled				Management Frame Prot	ection (MFP)
Override	Interface ACL	JPv4 Nor	e 1	IPv6	None +	MFP Client Protection	Optional +
P2P Bloc	king Action	Disabled				DTIM Period (in beacon i	ntervals)
Client Ex	eclusion ²	Enabled	60 Timeout	Value (secs)		802.11a/n (1 - 255)	1
Maximur	m Allowed Clients	0				802.11b/g/n (1 - 255)	1
Static IP	Tunneling ¹¹	Cnabled				NAC	
Wi-Fi Dir	rect Clients Policy	Disabled	-			NAC State Radius NA	<u>c i</u>
Maximur	m Allowed Clients	200				Load Balancing and Band	Select
Per AP R	adio					Client Load Balancing	0
Clear Ho Configure	tSpot ation	Enabled				Client Band Select	0

Allow AAA Overrideがチェックされていることを確認します。

7. リダイレクト ACL を作成します。

このACLは、ISEのAccess-Acceptメッセージで参照され、リダイレクトする必要があるト ラフィック(ACLによって拒否される)だけでなく、リダイレクトしない必要があるトラフ ィック(ACLによって許可される)も定義します。基本的に、DNSとISEとの間のトラフィ ックを許可する必要があります



注意: FlexConnect APの問題は、通常のACLとは別にFlexConnect ACLを作成する 必要があることです。この問題は、Cisco Bug ID <u>CSCue68065</u>に記載されており、 リリース7.5で修正されています。WLC 7.5以降では、FlexACLのみが必要で、標準 ACLは必要ありません。WLC では、ISE によって返されるリダイレクト ACL が標 準 ACL であると想定します。ただし、確実に機能させるには、FlexConnect ACLと 同じACLを適用する必要があります(シスコの内部ツールおよび情報にアクセスで きるのは、登録ユーザのみです)。

次の例では、flexred という名前の FlexConnect ACL の作成方法を示しています。

cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY
Wireless	FlexConr	ect Acc	ess Control L	ists	
 Access Points All APs Radios	Acl Name flexred				
Advanced					
Mesh					
RF Profiles					
FlexConnect Groups FlexConnect ACLs					
Flexredという名前のFlexConnect A	CLの作成				

a. ISE へのトラフィックと同様に DNS トラフィックを許可し、残りのトラフィックを拒 否するルールを作成します。

	CISCO	MONI	TOR W	LANs <u>C</u> ONTR	OLLE	R WIRELESS	SE	CURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
W	fireless	Acce	ess Con	trol Lists > E	dit							
•	Access Points All APs Radios	Gene	eral									
✓ Radios 802.11a/n 802.11b/g/n Dual-Band Radios		Access List Name flexred			Destination							
	Global Configuration	Seq	Action	Source IP/Ma	sk	IP/Mask		Protocol	Source Port	Dest Port	DSCP	
Þ	Advanced	1	Permit	0.0.0.0	/	10.48.39.208 255.255.255.255	5	Any	Any	Any	Any	
	Mesh RF Profiles	2	Permit	10.48.39.208 255.255.255.2	/ 55	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	
	FlexConnect Groups FlexConnect ACLs	3	Permit	0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS	Any	
Þ	802.11a/n	4	Permit	0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	DNS	Any	Any	
*	802.11b/g/n Media Stream	5	Deny	0.0.0.0	/	0.0.0.0 0.0.0.0	/	Any	Any	Any	Any	٠

DNSトラフィックの許可

最大限のセキュリティが必要な場合は、ISEへのポート8443だけを許可します(ポス チャする場合は、8905、8906、8909、8910などの一般的なポスチャポートを追加す る必要があります)。

b. (Cisco Bug <u>IDCSCue68065</u>により、バージョン7.5より前のコードでのみ)Security > Access Control Listの順に選択し、同じ名前の同じACLを作成します。

cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY
Security	Access 0	Control L	ists		
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies 	Enable Co Name flexred	ounters		יד זו וו	ype >v4 🔽
Local EAP					
Certificate					
 Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs 					
同一のACLの作成					

- c. 特定の FlexConnect AP を用意します。より大規模な導入の場合、通常は FlexConnect グループを使用し、拡張性の理由から、次の項目を AP 単位で実行しな いことに注意してください。
 - 1. [Wireless] をクリックして、特定のアクセス ポイントを選択します。
 - 2. [FlexConnect] タブをクリックし、[External Webauthentication ACLs] をクリッ クします(バージョン 7.4 よりも前は、このオプションの名前は web policies で した)。

cisco	MONITOR	WUNS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDMOX	
Wireless	All APs >	Details	for FlexAP1							
 Access Points Al APs 	General	Cred	entials Inte	rfaces P	ligh Availabil	ity Inventor	y FlexCon	nect	Advanced	
 Radios 802.11a/n 802.11b/g/n Dual-Bend Radios Global Configuration 	VLAN S Native	lupport VLAN 10	33	V	AN Mappings	J				
Advanced	FlexCo	mest Grou	p Name	Not Configures	1					
RF Profiles	PreAuthentication Access Control Lists									
FlexConnect Groups FlexConnect ACLs	Externa	WebAuther	tication ACLa							
> 802.11a/m	Central	OmCP Proce	mina							



3. Web ポリシー領域に ACL(この例では flexred という名前)を追加します。こ れにより、この ACL がアクセス ポイントに事前にプッシュされます。この ACL はまだ適用されていませんが、必要な場合に適用できるように、ACL の内容が AP に提供されます。

cisco	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
Wireless	All APs >	FlexAP	1 > ACL Mapp	lings			
Access Points All APs Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration	AP Name Base Radio WLAN ACI	MAC L Mappi	FlexAP1 00:1c:f9:c2:42:30 ng	•			
Advanced	WLAN Id	0					
Mesh	WebAuth	ACL field	ared :				
RF Profiles		Ad	ы				
FlexConnect Groups FlexConnect ACLs	WLAN 1d	WLA	N Profile Name	WebA	wth ACL	_	
▶ 802.11a/n							
▶ 802.11b/g/n	WebPolici	es					
Media Stream	WebPolicy	ACL M	sored 1				
Application Visibility And Control		A	66				
Country	WebPolicy	Access C	ontrol Lists				
Timers	flexred						
Netflow							

Webポリシー領域へのACLの追加

WLC の設定はこれで完了しました。

ISE 設定

許可プロファイルを作成するには、次の手順を実行します。

- 1. [Policy] をクリックして、[Policy Elements] をクリックします。
- 2. [Results] をクリックします。
- 3. [Authorization] を展開して、[Authorization profile] をクリックします。
- 4. [Add] ボタンをクリックして、中央 webauth の新しい許可プロファイルを作成します。
- 5. [Name] フィールドに、プロファイルの名前を入力します。この例では「CentralWebauth」 という名前を使用します。
- 6. [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。
- 7. [Web Authentication] チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。
- 8. [ACL] フィールドに、リダイレクトされるトラフィックを定義する WLC 上の ACL の名前を 入力します。この例では、flexred を使用します。
- 9. [Redirect] ドロップダウン リストで [Default] を選択します。

[Redirect] 属性は、ISE がデフォルトの Web ポータルと ISE 管理者が作成したカスタム Web ポ ータルのいずれを参照するかを定義します。たとえば、この例のflexred ACLは、クライアントか ら任意の宛先へのHTTPトラフィックのリダイレクトをトリガーします。

🔥 Home Operations • Policy • Admini	adjustion •
🔒 Authentication 😹 Authorization 🖂 P	toffing 🔄 Pasture 🙀 Clerit Provisioning 📑 Security Group Access 🔺 Pulsy Demons
Dictionaries Conditions Results	
Results P ↓•• ■ 7目 ⊕• ↓•• ■ 7目 ⊕• ▲drentuction ● ▲drentuction ●	Authorization Profile * Name Description
Authorization Profiles	* Access Type ACCESS ACCEPT *
C Bachde, Wieless, Acces C Certralitiouch C Cecc. JP , Prenes	Common Tasks OAD Name
C DeryAcces C Permit Acces C polium	1 O WAR
C sharport C sharbo	Value Domain Permission
* Convertandation ACLa * Convertandation Rocker Profiles	Web Authentication Centralized * ACL ficaned Redirect Default *

ACLがクライアントから任意の場所へのHTTPトラフィックのリダイレクトをトリガーする

認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順を実行します。

1. [Policy] メニューで [Authentication] をクリックします。

この図は、認証ポリシー ルールの設定方法の例を示します。この例では、MAC フィルタリ ングの検出時にトリガーされるルールが設定されています。

٠	wireless MA8] : # [Wreless_MA8 \diamond	allow protocols	Allowed Protocol : Default Networ() and.	
•	MAB]:#	Wred_MA8 🔷	allow protocols	Allowed Protocol : Default Networco and	
*	Dot1X]:#	Wred_802.1X	allow protocols	Allowed Protocol : Default Networt	
	Default Rule (If no match)	: - añ	ow protocols Allowed Proto	col : Default Netw	and use identity source : Internal U	64 ()

ポリシールールの設定方法

- 2. 認証ルールの名前を入力します。この例では Wireless mab を使用しています。
- 3. [lf] 条件フィールドで、プラス([+]) アイコンをクリックします。
- 4. [Compound condition] を選択してから、[Wireless_MAB] を選択します。
- 5. 許可されるプロトコルとしてDefault network accessを選択します。
- 6. ルールをさらに展開するには、[and ...] の横にある矢印をクリックします。
- 7. [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します
- 8. [If user not found] ドロップダウン リストから [Continue] を選択します。

	wireless MAB : If Wirele	allow protocols Allowed Protocol : D
	Default : use	Internal Users 🗢
		Identity Source Internal Endpoints
		Options
		If authentication failed Reject *
	 MAB If Wired 	If user not found Continue *
		If process failed Drop *
	· Publy · If Mand	1
• • •		

Continueをクリックします

このオプションにより、MAC アドレスが不明な場合でも、webauth によってデバイスが認証済み となります。Dot1xクライアントはクレデンシャルを使用して引き続き認証できるため、この設 定を考慮する必要はありません。

許可ルールの作成

ここでは、許可ポリシーでいくつかのルールを設定します。PCが関連付けられると、MACフィ ルタリングが実行されます。MACアドレスが不明であると想定されるため、WebAuthとACLが返 されます。このMAC not knownルールは次の図に示され、このセクションで設定されます。

	*	2nd AUTH	if.	Network Access:UseCase EQUALS Guest Flow	then	vlan34
I	2	IS-a-GUEST	if.	IdentityGroup:Name EQUALS Guest	then	PermitAccess
l	2	MAC not known	1ť	Network Access:AuthenticationStatus EQUALS UnknownUser	then	CentralWebauth

MACが不明

許可ルールを作成するには、次の手順を実行します。

- 1. 新しいルールを作成し、名前を入力します。この例では、「MAC not known」という名前を 使用します。
- 2. 条件フィールドでプラス([+])アイコンをクリックして、新しい条件を作成します。
- 3. [expression] ドロップダウン リストを展開します。
- 4. [Network Access] を選択し、展開します。
- 5. [AuthenticationStatus] をクリックし、[Equals] 演算子を選択します。
- 6. 右側のフィールドで [UnknownUser] を選択します。
- 7. [General Authorization] ページの [then] という単語の右側のフィールドで、 [CentralWebauth](許可プロファイル)を選択します。

この手順により、ユーザ(または MAC アドレス)が不明でも、ISE を続行することができ ます。

不明なユーザには、ログインページが表示されます。ただし、クレデンシャルを入力すると 、ISEで再度認証要求が表示されます。したがって、ユーザがゲストユーザの場合に満たす 条件を使用して、別のルールを設定する必要があります。この例では、UseridentityGroupが Guestis usedと等しく、すべてのゲストがこのグループに属していると仮定しています。

8. [MAC not known] ルールの末尾にあるアクション ボタンをクリックして、上で説明した新 しいルールを挿入します。



注:この新しいルールは、MAC not knownルールの前に来ることが非常に重要です 。

- 9. 名前フィールドに、「2nd AUTH」と入力します。
- 10. 条件として ID グループを選択します。この例では、[Guest] を選択します。
- 11. 条件フィールドでプラス([+])アイコンをクリックして、新しい条件を作成します。
- 12. [Network Access] を選択し、[UseCase] をクリックします。
- 13. 演算子として [Equals] を選択します。
- 14. 右のオペランドとして [GuestFlow] を選択します。これは、Web ページでログインしたば かりで、認可変更(ルールのゲスト フローの部分)の後に戻ってきたユーザを捕捉するこ とを意味し、これはゲスト ID グループに属している場合にのみ実行されます。
- 15. 認可ページで、プラス(+)アイコン(横)をクリックして、ルールの結果を選択します。

この例では、事前に設定されたプロファイル(vlan34)が割り当てられます。この設定は、このドキュメントでは示されていません。

[Permit Access] オプションを選択するか、カスタム プロファイルを作成し、VLAN または 任意の属性に戻ることができます。



注意:ISEバージョン1.3では、Web認証のタイプに応じて、ゲストフローの使用例に遭遇 することはなくなりました。許可ルールには、唯一の可能な条件としてゲストユーザグ ループを含める必要があります。

IP 更新の有効化(オプション)

VLAN を割り当てる場合、最後のステップとして、クライアント PC 用の IP アドレスを更新しま す。このステップは、Windows クライアント用のゲスト ポータルによって実行できます。前の 手順で、2nd AUTHルールにVLANを設定していない場合は、このステップを省略できます。 FlexConnect AP では、VLAN が AP 自体に事前に存在している必要があることに注意してください。したがって、VLAN が事前に存在しない場合、AP 自体、または作成する新規 VLAN に ACL をなにも適用しない Flex グループに VLAN-ACL マッピングを作成することができます。これにより、VLAN が実際に作成されます(その VLAN に ACL なしで)。

VLAN を割り当てた場合は、次の手順を実行し、IP 更新を有効にします。

- 1. [Administration] をクリックして、[Guest Management] をクリックします。
- 2. [Setting] をクリックします。
- 3. [Guest] を展開してから、[Multi-Portal Configuration] を展開します。
- 4. DefaultGuestPortalをクリックするか、作成したカスタムポータルの名前をクリックします。
- 5. [VLAN DHCP Release] チェックボックスをオンにします。



注:このオプションは、Windowsクライアントでのみ機能します。

Settings General Spansor My Devices Guest	Multi-Portal General Occustomization Authentication Every Logn
Details Policy Language Template Multi-Portal Configurations DetautrQuestPortal Portal Policy Passecord Policy Time Profiles Username Policy	
Vlan DHCP Releaseチェックボ	ックスをクリックします

Traffic flow

このシナリオでは、どのトラフィックがどこに送信されるかを理解することが難しいように思われる可能性があります。再確認のために以下に簡単にまとめます。

- クライアントが無線で SSID のアソシエーション要求を送信します。
- WLC が ISE を使用して MAC フィルタリング認証を処理します(WLC がリダイレクト属性 を受信する場合)。
- ・ クライアントが、MAC フィルタリングの完了後にアソシエーション応答を受信します。
- クライアントはDHCP要求を送信し、リモートサイトのIPアドレスを取得するために、アク セスポイントによってその要求がローカルでスイッチされます。
- Central_webauth 状態では、リダイレクト ACL で拒否とマークされたトラフィック(通常 HTTP)は中央にスイッチしたがって、リダイレクションを実行するのはAPではなく WLCです。たとえば、クライアントが任意のWebサイトを要求すると、APはCAPWAPでカ プセル化してこれをWLCに送信し、WLCはそのWebサイトのIPアドレスをスプーフィング してISEにリダイレクトします。
- クライアントが ISE のリダイレクト URL にリダイレクトされます。このリダイレクトは、
 再度ローカルにスイッチされます(このリダイレクトが Flex のリダイレクト ACL で許可に ヒットするため)。
- 一度 RUN 状態になると、トラフィックはローカルにスイッチされます。

確認

ユーザが SSID に関連付けられると、認可が [ISE] ページに表示されます。

Apr 19,13 11:49:27.179 AM	6	No	01030317030	nizowit	viar34	Guest	NoNypicable	
Apr 08,13 11:49:27.174 APR	6			nicowitz				Dynamic Author
Apr 19,13 11:48:58.372 AM	6	No	0013130212013			Guest		Guest Authoritic.
Apr 00,13 1142 15425 AM	6	00.13.10.21.70.13	00131001217013	nicowit	CertraWebeuth		Pending	Authentication
許可が表示される								

CWA 属性を返す MAC アドレスのフィルタリング認証を下から上に確認できます。次は、ユーザ 名を使用したポータルのログインです。その次に、ISE が WLC に CoA を送信し、最後の認証は WLC 側のレイヤ 2 の MAC フィルタリング認証ですが、ISE はクライアントとユーザ名を記憶していて、この例で設定した必要な VLAN を適用します。

クライアントで任意のアドレスを開くと、そのブラウザが ISE にリダイレクトされます。ドメイン ネーム システム (DNS) が正しく設定されていることを確認します。





ISEにリダイレクト

ユーザがポリシーを受け入れるとネットワーク アクセスが許可されます。



Signed on successfully You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.

コントローラでは、ポリシー マネージャの状態と RADIUS NAC の状態が POSTURE_REQD から RUN に変わります。

関連情報

シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。