

ワイヤレスLANコントローラ(WLC)9800およびIdentity Services Engine(ISE)での中央Web認証(CWA)のトラブルシューティング

内容

[はじめに](#)

[背景説明](#)

[詳細フロー](#)

[トラブルシューティング](#)

[一般的な症状：ユーザがログインページにリダイレクトされない。](#)

[1-最初のRADIUS認証は成功しましたか。](#)

[2-WLCがリダイレクトURLとACLを受信する](#)

[3-リダイレクトACLは正しいですか。](#)

[4-クライアントはWeb-Auth Pendingに移行されましたか。](#)

[5-WLCではDHCPとDNSのトラフィックを許可していますか。](#)

[6-DHCPサーバはDHCPディスカバリ/要求を受信しますか。](#)

[7-自動リダイレクションは行われますか。](#)

[8-ブラウザにログインページが表示されない](#)

[9-クライアントはISEホスト名を解決できますか。](#)

[10-ログインページがまだロードされない](#)

[11-証明書によってセキュリティ違反が発生するのはなぜですか。](#)

[12-ゲストログインが失敗しますか？](#)

[13-ログインは成功するが、実行に移らない？](#)

[14-COAが失敗しているか](#)

[結論](#)

[参考資料](#)

はじめに

このドキュメントでは、WLC 9800およびISEを使用した中央Web認証(CWA)のトラブルシューティング方法について説明します。

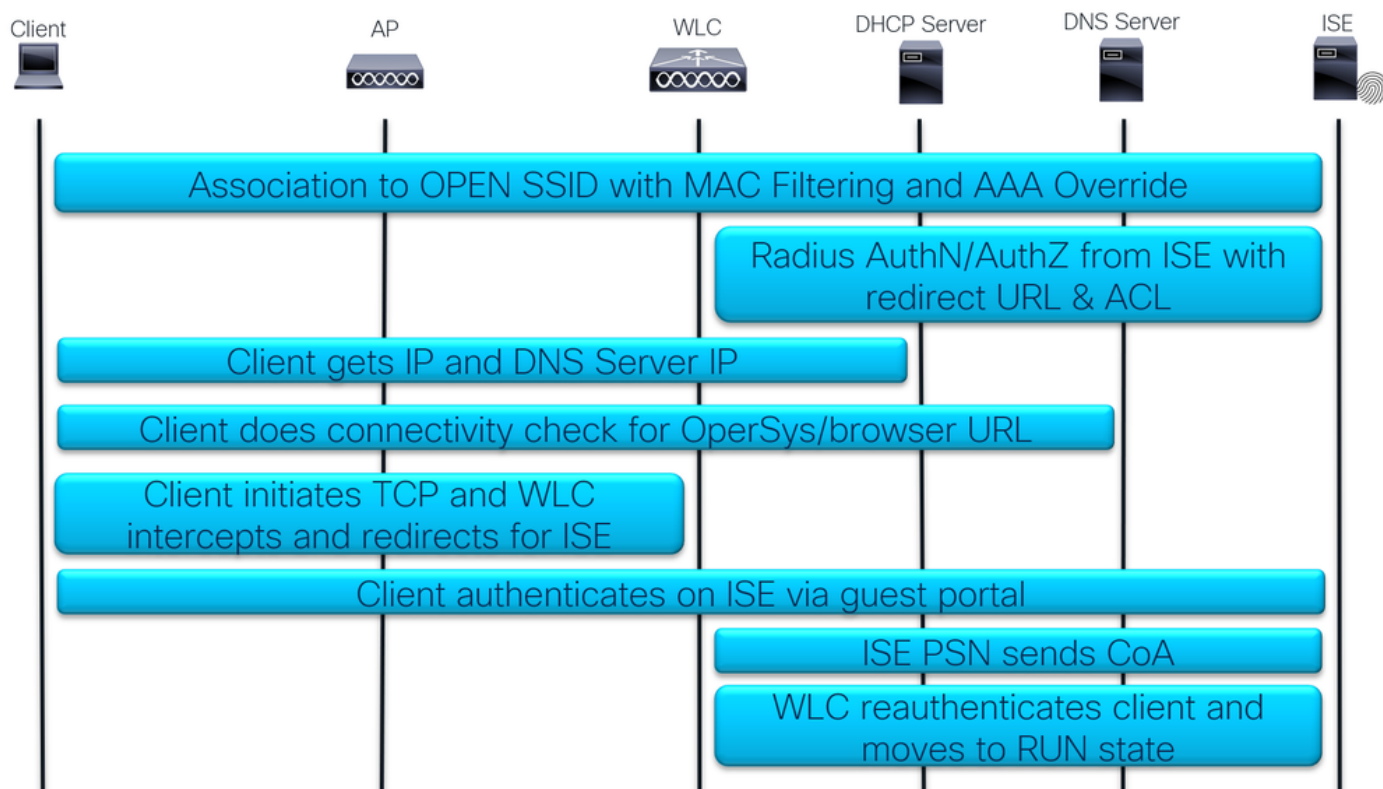
背景説明

現在、非常に多くのパーソナルデバイスがあるため、ワイヤレスアクセスの保護を求めるネットワーク管理者は、通常、CWAを使用するワイヤレスネットワークを選択します。このドキュメントでは、CWAのフローチャートに焦点を当て、影響を受ける一般的な問題のトラブルシューティングに役立てます。プロセスの一般的な目標、CWAに関連するログの収集方法、これらのログの分析方法、およびトラフィックフローを確認するためにWLCで埋め込みパケットキャプチャを収集する方法について説明します。

CWAは、ユーザが個人所有のデバイス（BYODとも呼ばれる）を使用して会社のネットワークに接続することを許可する企業で最も一般的なセットアップです。

ネットワーク管理者は、TACサービスリクエストをオープンする前に、問題を修正するために実行する手順の概要とトラブルシューティングに関心があります。

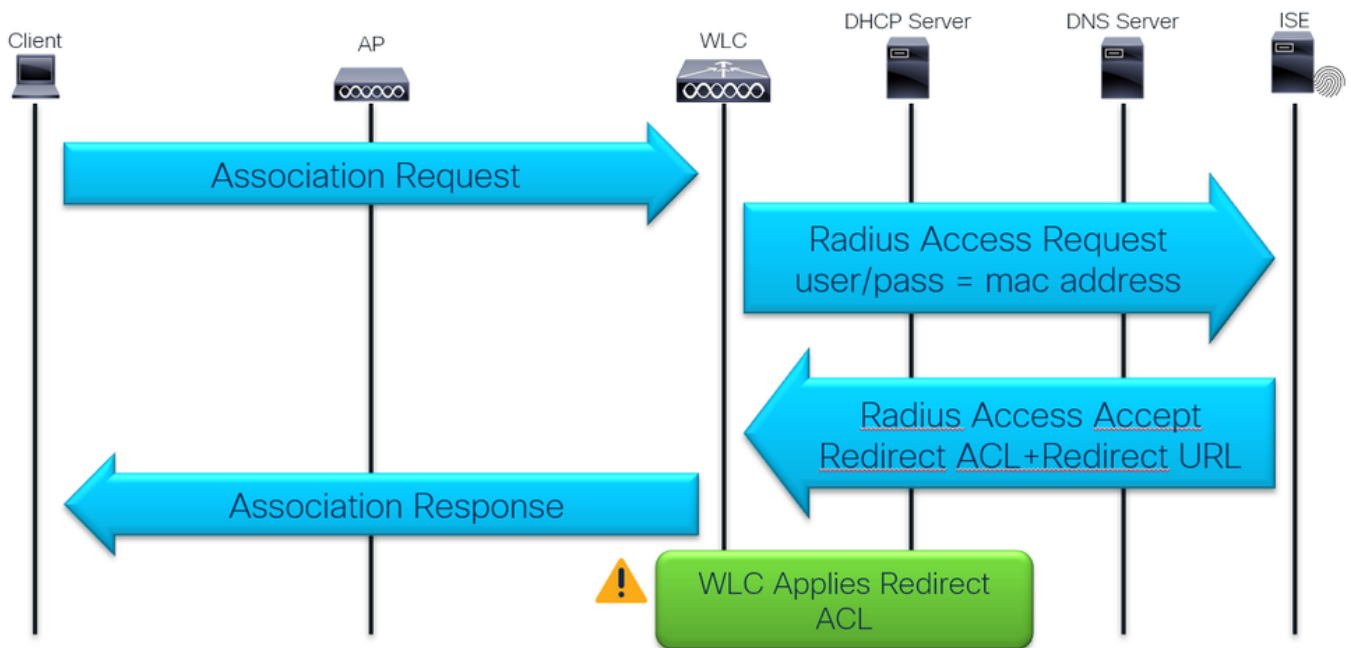
CWAのパケットフローを次に示します。



CWAパケットフロー

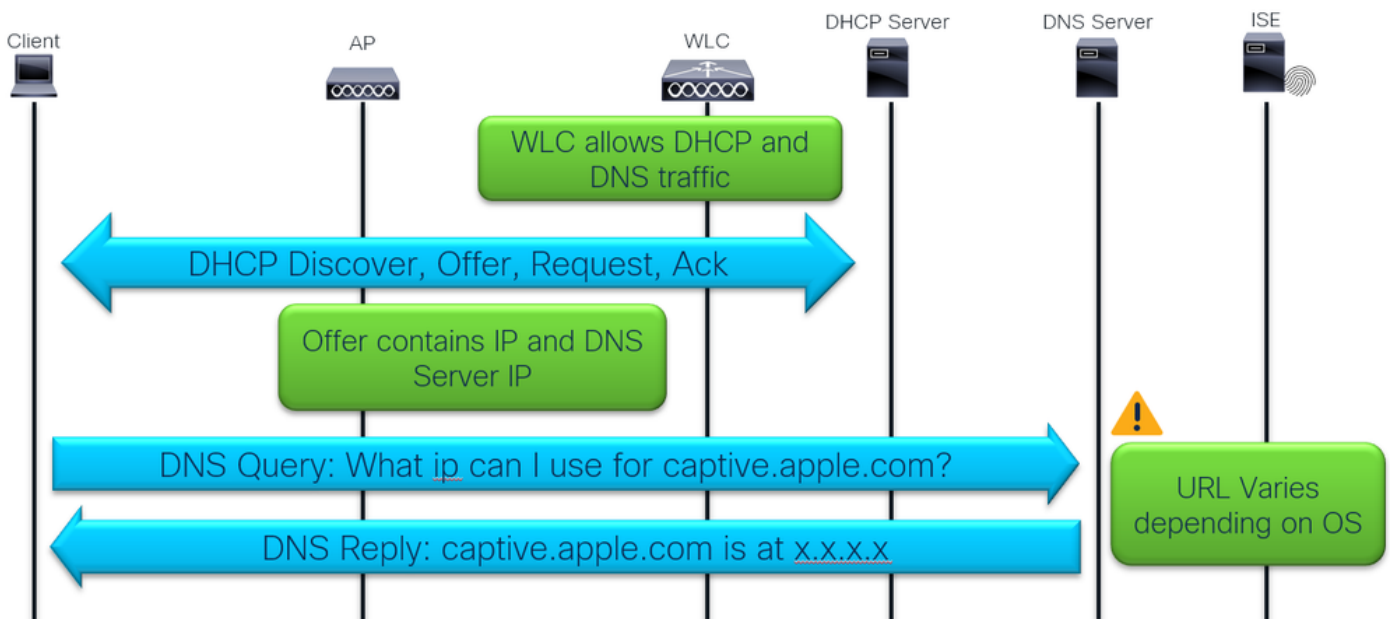
詳細フロー

最初のアソシエーションとRADIUS認証：



最初の関連付けとRADIUS認証

DHCP、DNS、および接続の確認：



DHCP、DNS、および接続の確認

接続チェックは、クライアントデバイスのオペレーティングシステムまたはブラウザによるキャプティブポータル検出を使用して行われます。

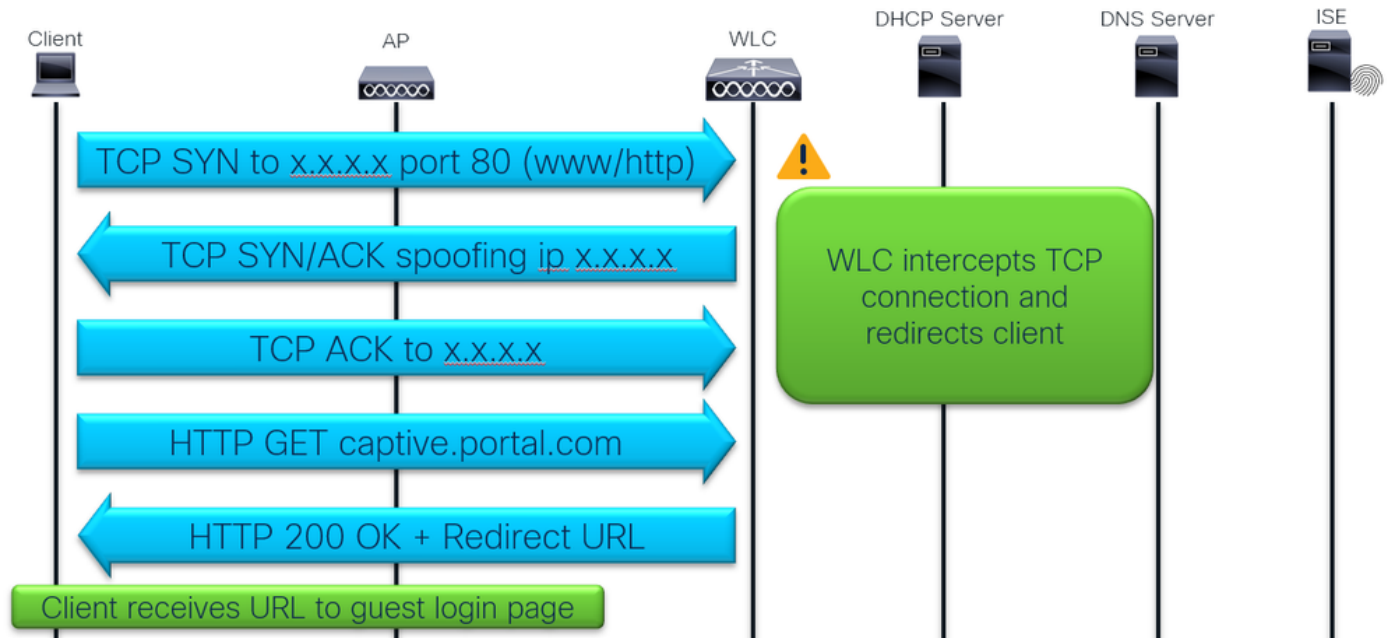
特定のドメインに対してHTTP GETを実行するように事前にプログラムされたデバイスOSがあります

- Apple社= captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windowsの場合= msftconnecttest.com

また、ブラウザを開いた場合も、次のチェックが実行されます。

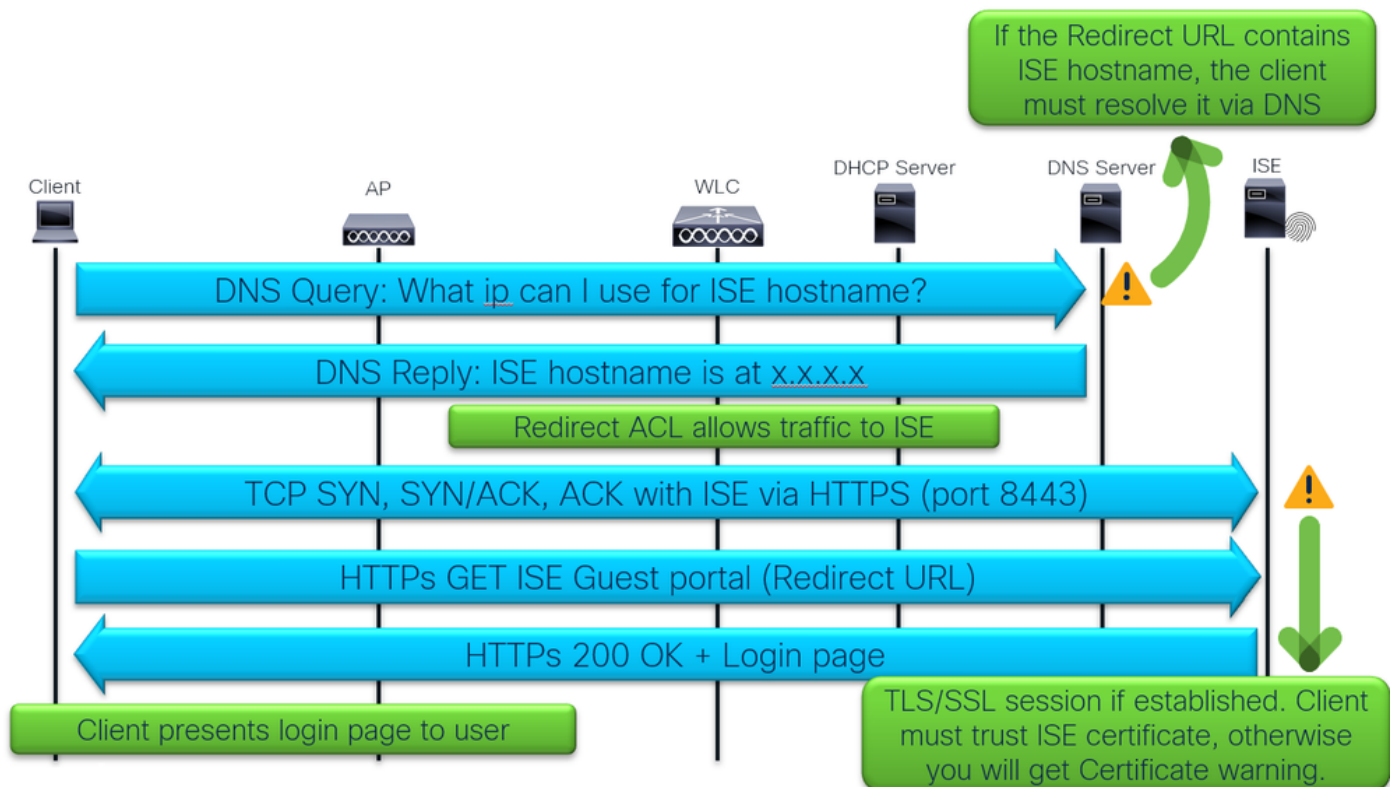
- クロム= clients3.google.com
- Firefox = detectportal.firefox.com

トラフィックの代行受信とリダイレクト：



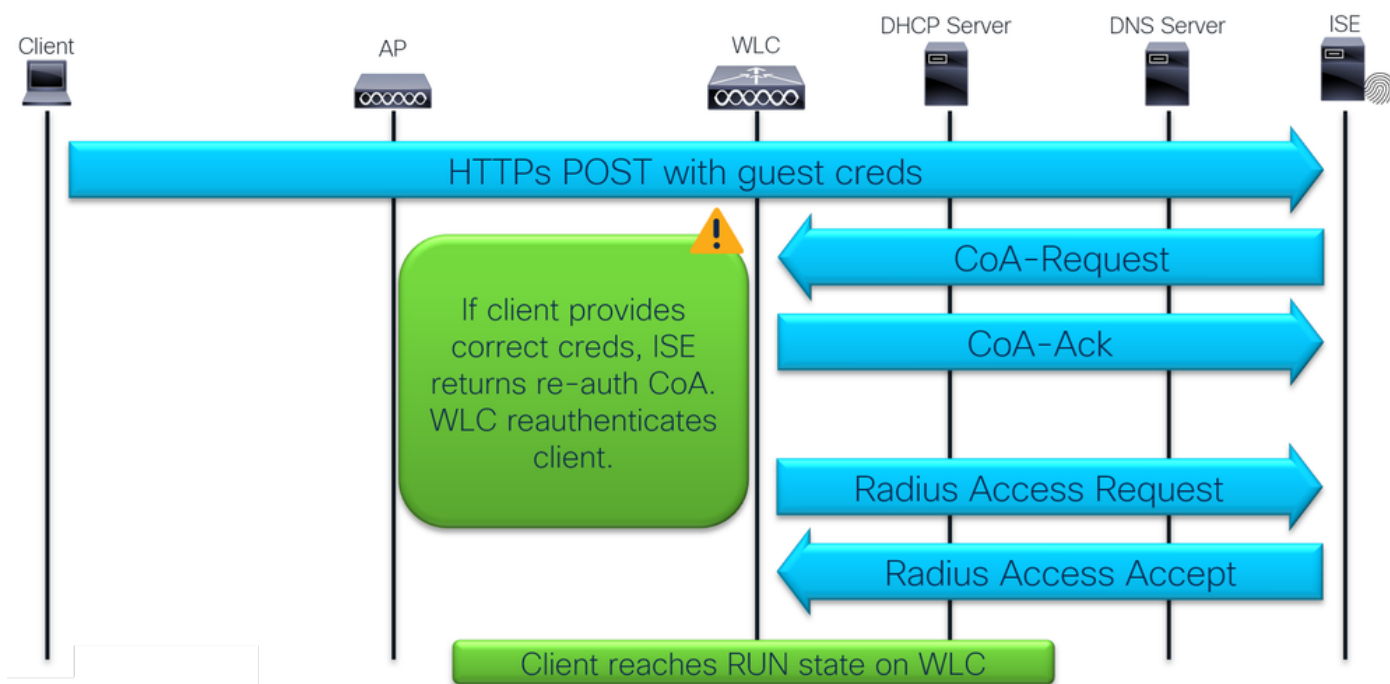
トラフィックの代行受信とリダイレクト

ISEゲストログインポータルへのクライアントログイン：



ISEゲストログインポータルへのクライアントログイン

クライアントログインおよびCoA:

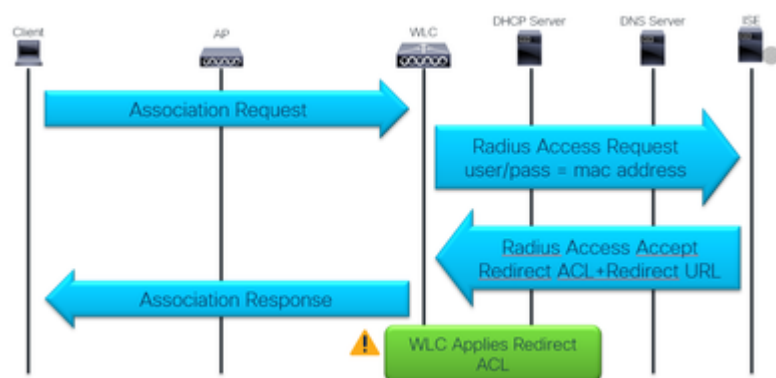


クライアントログインおよびCoA

トラブルシューティング

一般的な症状：ユーザがログインページにリダイレクトされない。

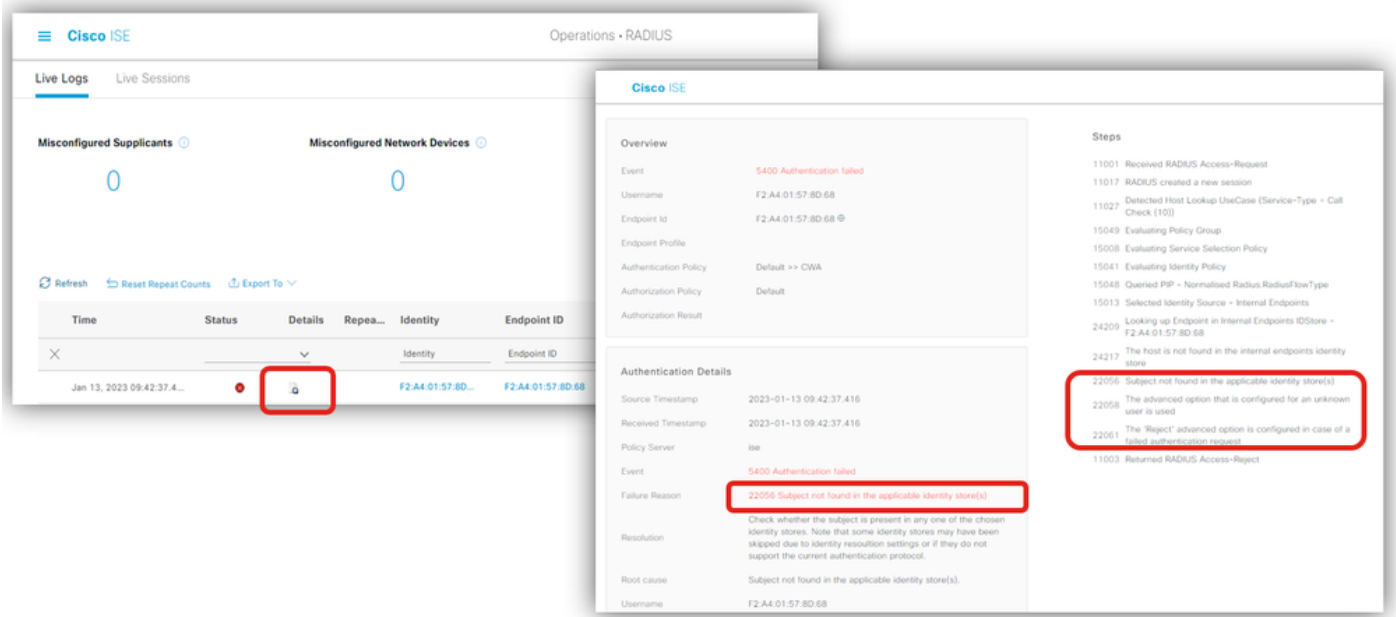
フローの最初の部分から説明します。



最初の関連付けとRADIUS認証

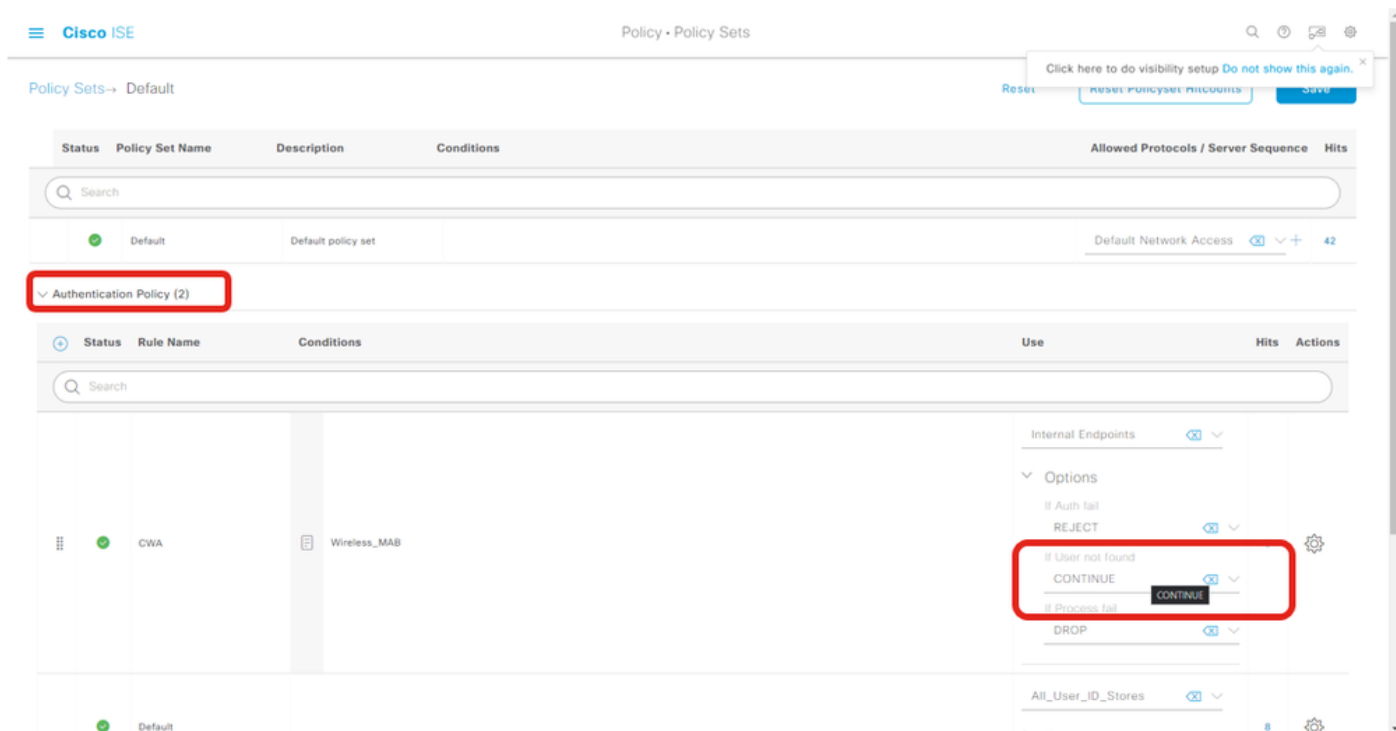
1 – 最初のRADIUS認証は成功しましたか。

MACフィルタリングの認証結果を確認します。



MACフィルタリング認証結果を示すISEライブログ

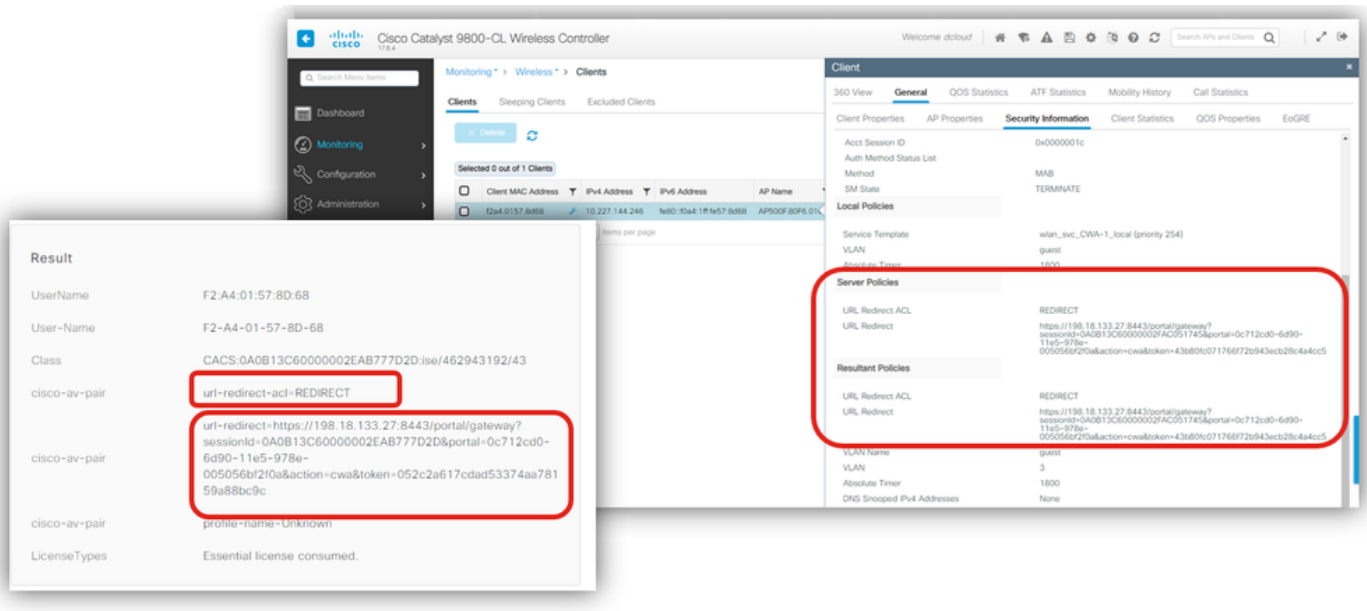
ユーザが見つからない場合は、認証の詳細オプションが「Continue」に設定されていることを確認します。



User not found advancedオプション

2 - WLCがリダイレクトURLとACLを受信する

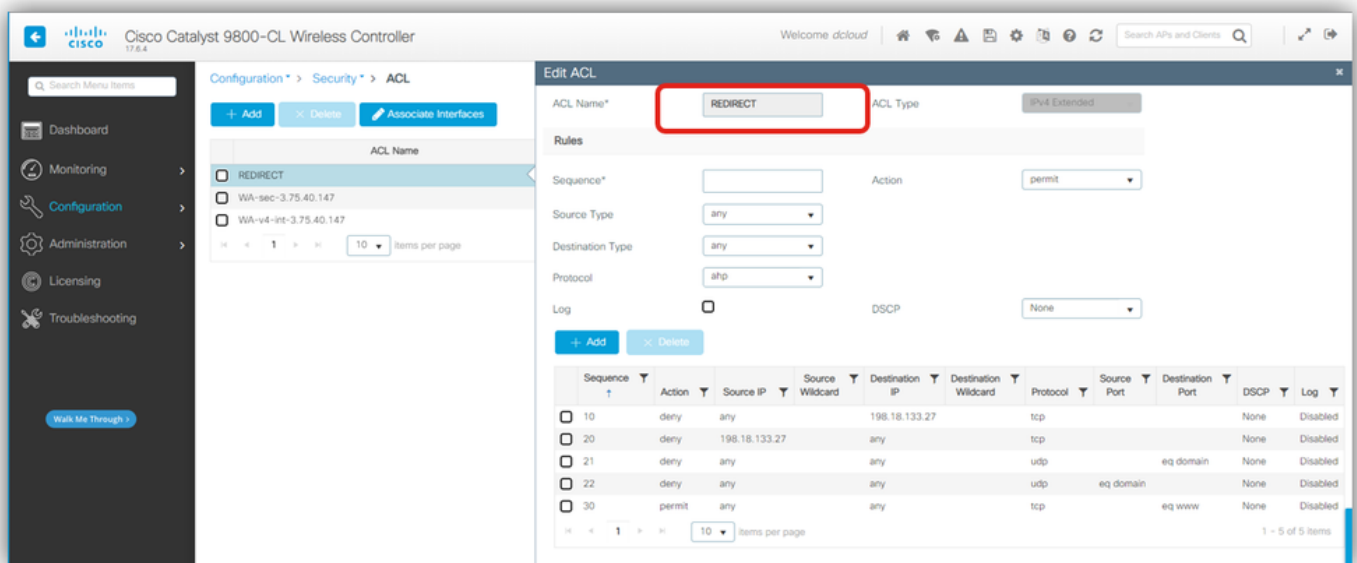
モニタリングでISEライブログとWLCクライアントのセキュリティ情報を確認します。ISEがリダイレクトURLとACLをAccess Acceptで送信し、WLCで受信されてクライアントに適用されていることを、クライアントの詳細情報で確認します。



リダイレクトACLとURL

3 – リダイレクトACLは正しいですか。

ACL名のタイプミスをチェックします。ISEから送信されたものとまったく同じであることを確認します。



リダイレクトACLの検証

4 – クライアントはWeb-Auth Pendingに移行されましたか。

クライアントの詳細で「Web Auth Pending」状態を確認します。この状態でない場合は、AAA OverrideおよびRadius NACがポリシープロファイルで有効になっているかどうかを確認します。

Monitoring > Wireless > Clients

Clients
Sleeping Clients
Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type	State
☐	f2a4.0157.8d68	198.19.1.11	fe80::f0a4:1ff:fe57:8d68	AP500F.80F6.0168	CWA-1	4	WLAN	Web Auth Pending

1
10 Items per page

Edit Policy Profile

IPv4 DHCP Required
☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override
☒

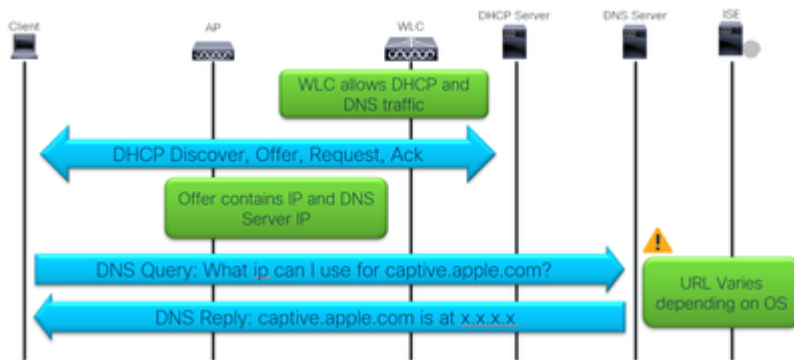
NAC State
☒

NAC Type
RADIUS

クライアントの詳細、aaa override、およびRADIUS NAC

まだ動いてないのか？

フローを見直してみましょう。



DHCP、DNS、および接続の確認

5 - WLCではDHCPとDNSのトラフィックを許可していますか。

WLCでリダイレクトACLの内容を確認します。

Cisco Catalyst 9800-CL Wireless Controller
Welcome dcloud

Configuration > Security > ACL

Add
Delete
Associate Interfaces

ACL Name

☐ REDIRECT
☐ WA-sec-3.75.40.147
☐ WA-v4-int-3.75.40.147

1
10 Items per page

Edit ACL

ACL Name* REDIRECT
ACL Type IPv4 Extended

Rules

Sequence*
Action
Source Type
Destination Type
Protocol
Log
DSCP

+ Add
Delete

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
☐ 10	deny	any		198.18.133.27		tcp			None	Disabled
☐ 20	deny	198.18.133.27		any		tcp			None	Disabled
☐ 21	deny	any		any		udp		eq domain	None	Disabled
☐ 22	deny	any		any		udp		eq domain	None	Disabled
☐ 30	permit	any		any		tcp		eq www	None	Disabled

1
10 Items per page

WLCでのACLコンテンツのリダイレクト

リダイレクトACLでは、permit文によって代行受信およびリダイレクトされるトラフィックと、代行受信およびリダイレクトから無視されるトラフィックをdeny文で定義します。

この例では、DNSおよびISE IPアドレスとの間のトラフィックのフローを許可し、ポート80(www)でtcpトラフィックをインターセプトします。

6 - DHCPサーバはDHCPディスカバリ/要求を受信しますか。

DHCP交換が発生するかどうかをEPCで確認します。EPCは、DHCPプロトコルや内部フィルタMACなどの内部フィルタと組み合わせて使用できます。内部フィルタMACでは、クライアントデバイスのMACアドレスを使用し、クライアントデバイスのMACアドレスで送受信されるDHCPパケットのみをEPCに取得できます。

この例では、VLAN 3でブロードキャストとして送信されたDHCP Discoverパケットを確認できます。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Packet Capture' tab is active, displaying a list of captured packets. A red box highlights the 'Edit Packet Capture' dialog, showing the 'Filter' set to 'any', 'Monitor Control Plane' checked, 'Inner Filter Protocol' set to 'DHCP', and 'Inner Filter MAC' set to 'f2a4.0157.8d68'. A blue cloud callout points to this dialog with the text 'Inner filters !!'. Another red box highlights a packet entry in the list, showing details for a DHCP Discover packet. A yellow cloud callout points to this entry with the text 'Sent as broadcast on VLAN 3'.

DHCPを確認するWLC EPC

ポリシープロファイルで想定されるクライアントVLANを確認します。

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface, specifically the 'Policy' configuration page. The 'Access Policies' tab is selected. A red box highlights the 'VLAN' section, showing the 'VLAN/VLAN Group' set to 'guest' and 'Multicast VLAN' set to 'Enter Multicast VLAN'.

WLC VLANとスイッチポートトランクの設定およびDHCPサブネットを確認します。

```
WLC1#show vlan

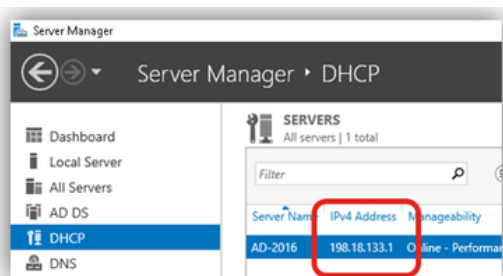
VLAN Name                Status    Ports
-----
1    default                active    Gi2, Gi3
2    employee                active
3    guest                   active
11   mgmt                     active

WLC1#show ip int br

Interface      IP-Address      OK? Method Status    Protocol
GigabitEthernet1  unassigned      YES unset  up        up
GigabitEthernet2  unassigned      YES unset  administratively down down
GigabitEthernet3  unassigned      YES unset  administratively down down
Vlan1          198.19.2.2      YES NVRAM  up        up
Vlan2          198.19.1.2      YES NVRAM  up        up
Vlan3          198.19.1.2      YES NVRAM  up        up
Vlan11         198.19.11.10   YES NVRAM  up        up

WLC1#show run int vlan 3
Building configuration...

Current configuration : 109 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 no mop enabled
 no mop sysid
end
```



If DHCP server is on different subnet we need **ip helper address** on SVI

VLAN、スイッチポート、およびDHCPサブネット

WLCにVLAN 3が存在し、VLAN 3のSVIも存在していることがわかります。ただし、DHCPサーバのIPアドレスを確認する際には、IPアドレスが異なるサブネット上にあるため、SVIにはIPヘルパーアドレスが必要です。

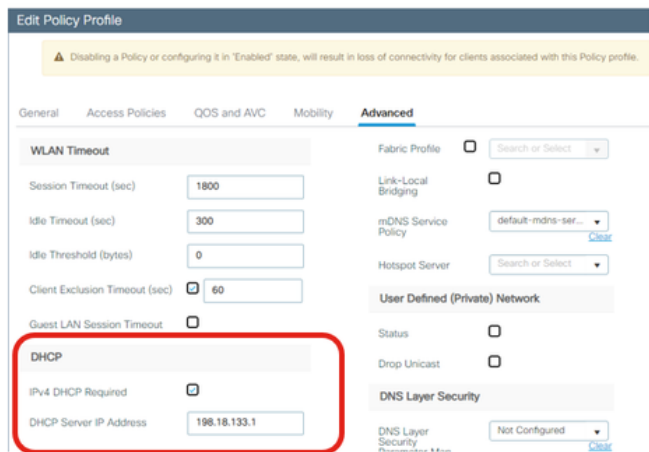
ベストプラクティスでは、クライアントサブネットのSVIを有線インフラストラクチャで設定し、WLCではこれを回避することが規定されています。

いずれの場合でも、SVIの配置場所に関係なく、ip helper-addressコマンドをSVIに追加する必要があります。

別の方法として、ポリシープロファイルでDHCPサーバのIPアドレスを設定することもできます。

```
WLC1#show run int vlan 3
Building configuration...

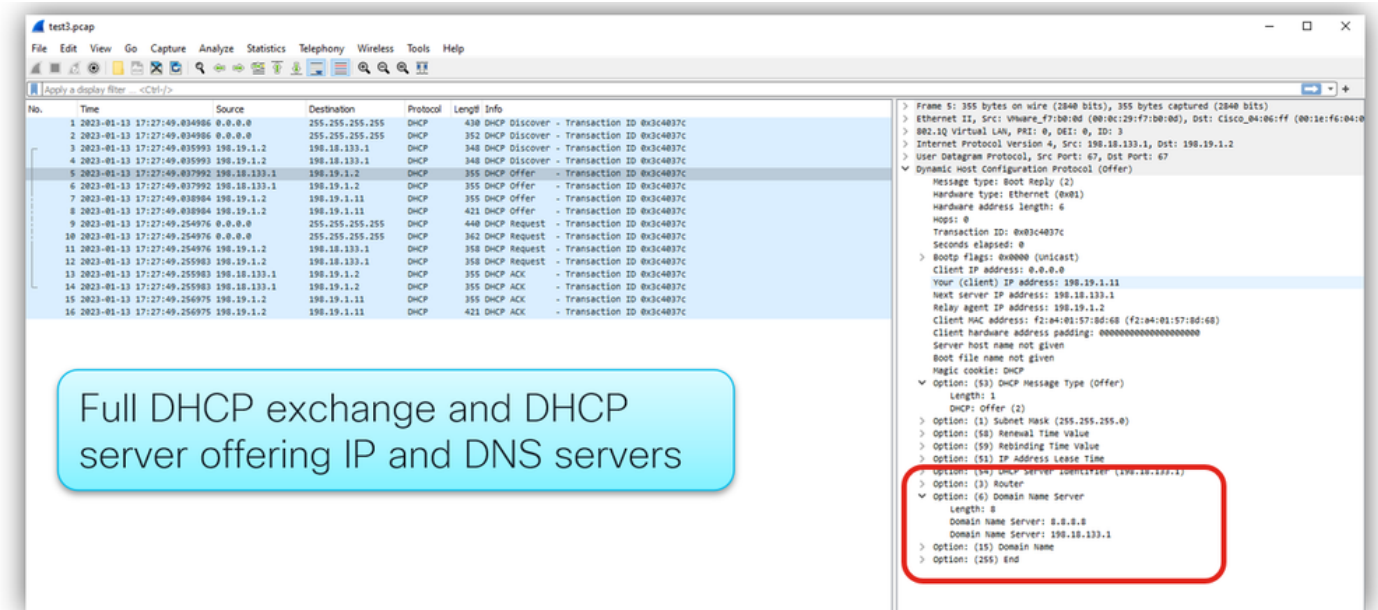
Current configuration : 141 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 ip helper-address 198.18.133.1
 no mop enabled
 no mop sysid
end
```



SVI can be at the WLC itself or in the Wired network

SviまたはポリシープロファイルでのIPヘルパーアドレス

次に、EPCを使用して、DHCP交換が正常に行われ、DHCPサーバがDNSサーバIPを提供しているかどうかを確認します。



Full DHCP exchange and DHCP server offering IP and DNS servers

DNSサーバipのDHCPオファアの詳細

7 – 自動リダイレクションは行われますか。

DNSサーバがクエリーに応答するかどうかをWLC EPCで確認します。

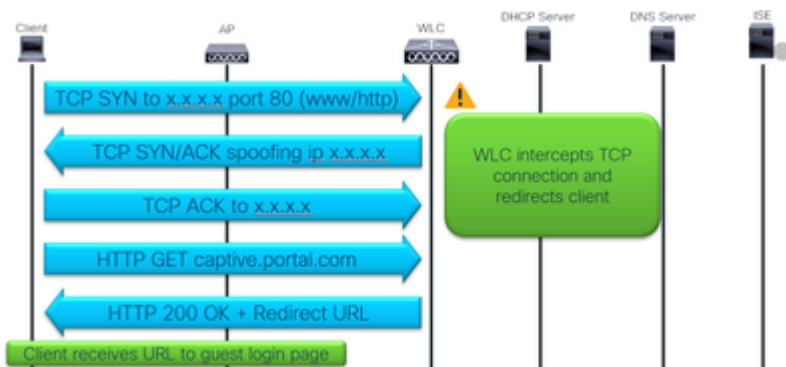


DNSクエリと応答

- ・リダイレクトが自動でない場合は、ブラウザを開いてランダムなIPアドレスを試してください。たとえば、10.0.0.1などです。
- ・リダイレクトが機能する場合は、DNS解決に問題がある可能性があります。

まだ動いてないのか？

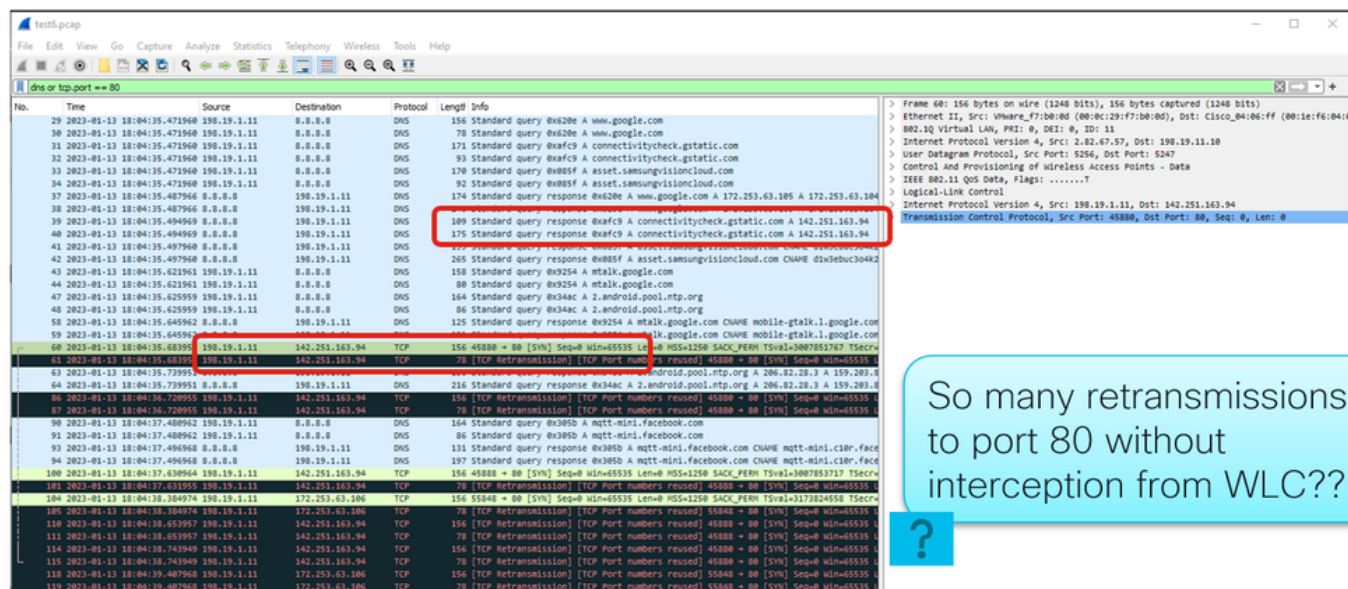
フローを見直してみましょう。



トラフィックの代行受信とリダイレクト

8 - ブラウザにログインページが表示されない

クライアントがTCP SYNをポート80に送信し、WLCがそれをインターセプトするかどうかを確認します。

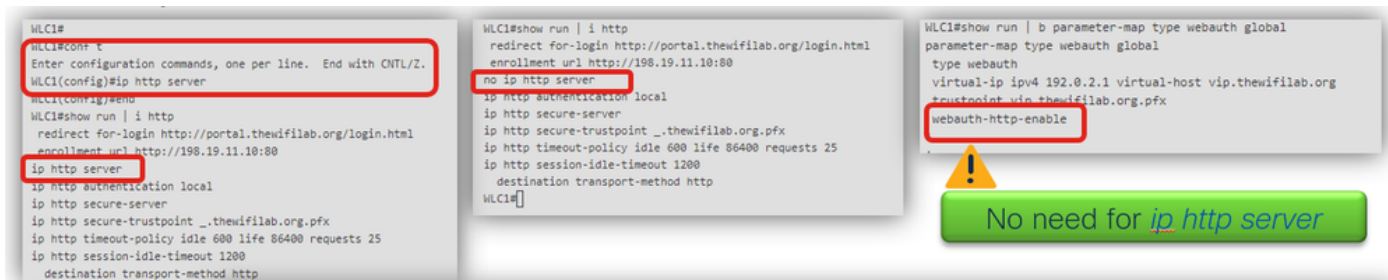


So many retransmissions to port 80 without interception from WLC??

ポート80へのTCP再送信

ここでは、クライアントがTCP SYNパケットをポート80に送信したものの、応答を受信せず、TCPの再送信を行っていることがわかります。

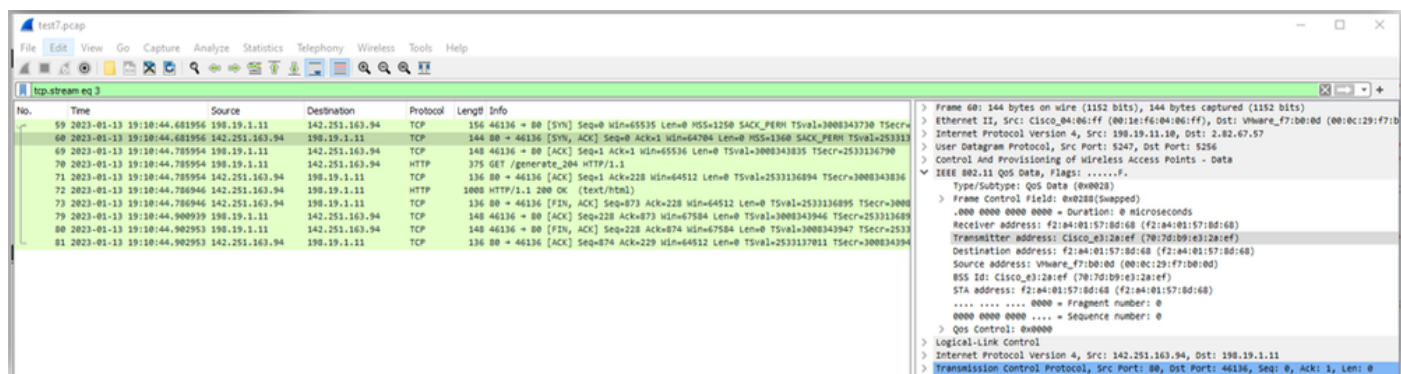
グローバルフィギュレーションにip http serverコマンドが指定されていること、またはparameter-map globalにwebauth-http-enableコマンドが指定されていることを確認します。



No need for ip http server

HTTP代行受信コマンド

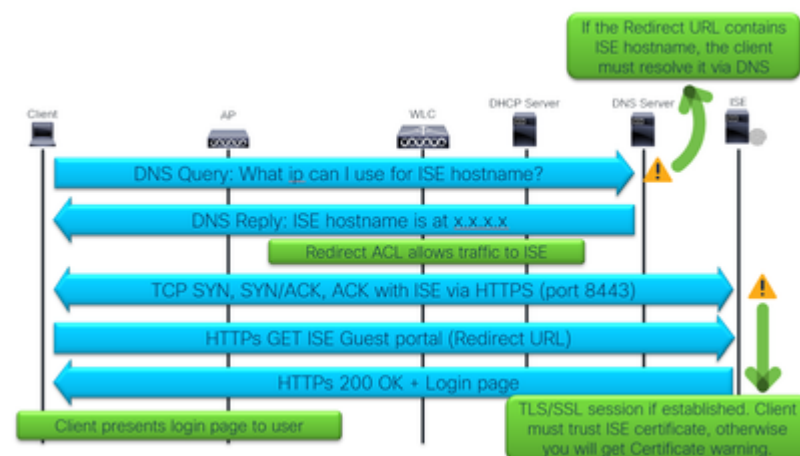
コマンドの後、WLCはTCPをインターセプトし、クライアントに応答してリダイレクトするために宛先IPアドレスをスプーフィングします。



WLCによるTCPインターセプション

まだ動いてないのか？

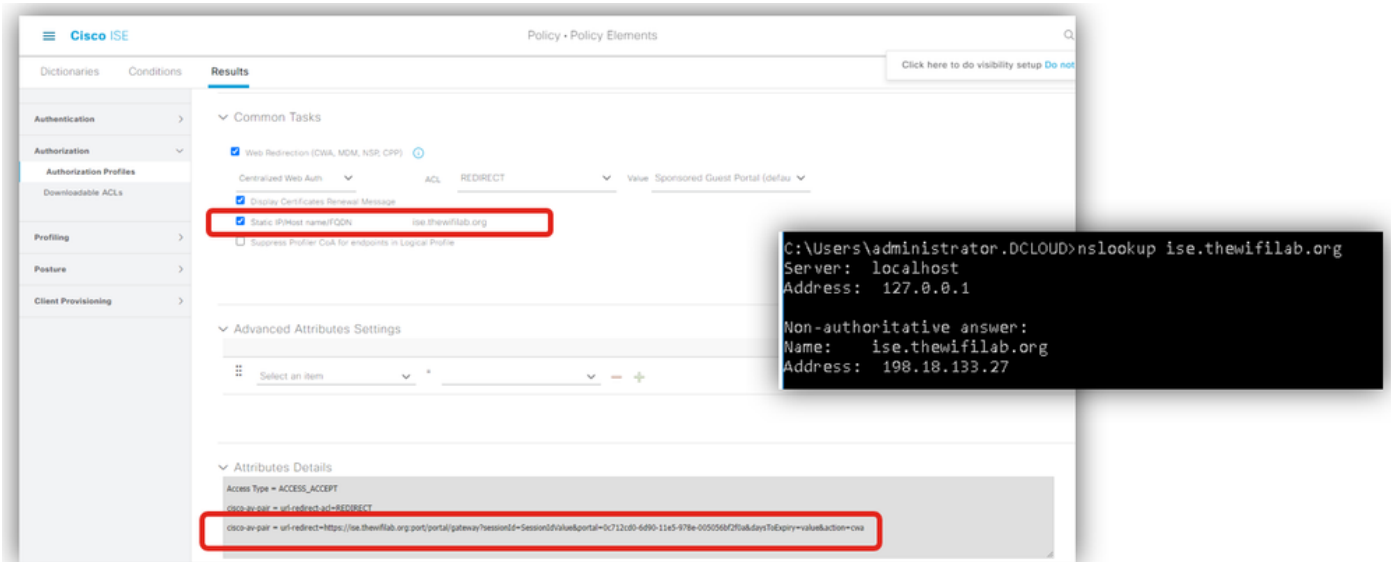
この流れには、さらに多くの要素が含まれています。



ISEゲストログインポータルへのクライアントログイン

9 – クライアントはISEホスト名を解決できますか。

リダイレクトURLがIPまたはホスト名を使用するかどうか、およびクライアントがISEホスト名を解決するかどうかを確認します。

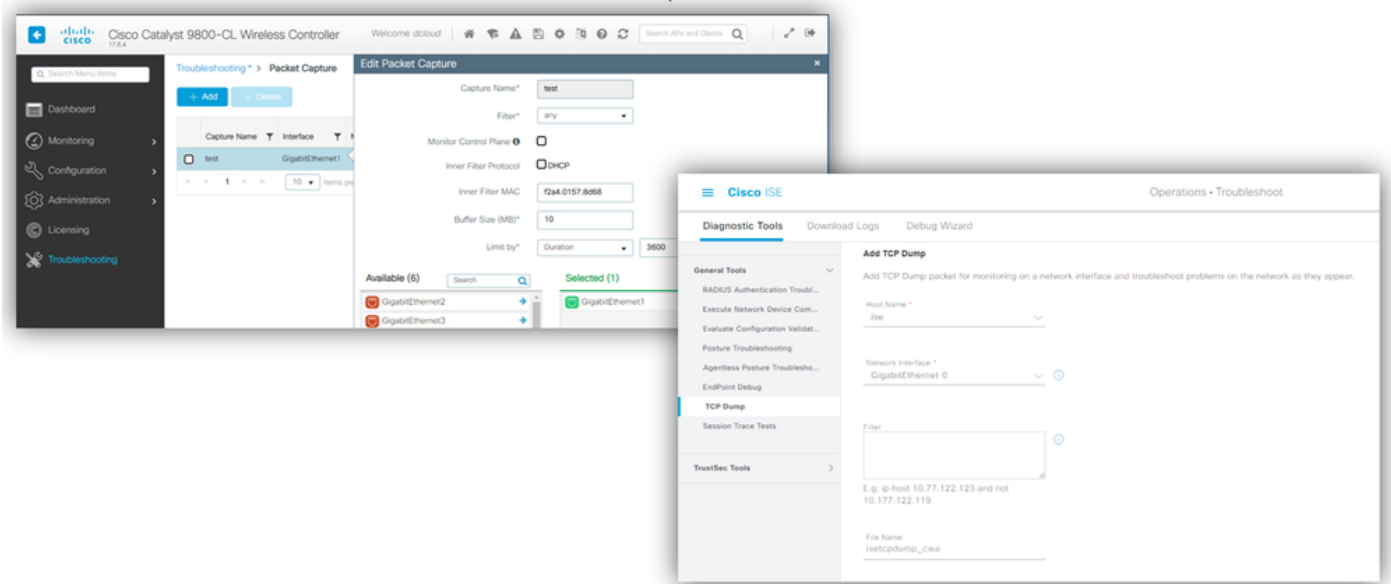


ISEホスト名解決

リダイレクトURLにISEホスト名が含まれていても、クライアントデバイスがそのホスト名をISE IPアドレスに解決できない場合に、一般的な問題が発生します。hostnameを使用する場合は、がDNS経由で解決可能であることを確認します。

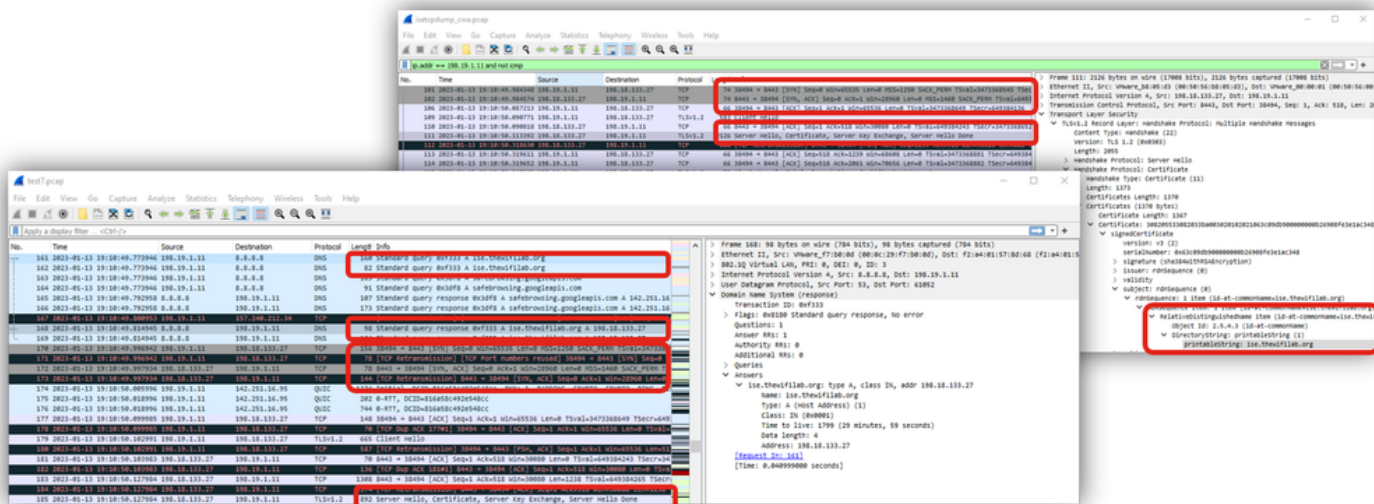
10 - ログインページがまだロードされない

クライアントトラフィックがISE PSNに到達するかどうかをWLC EPCおよびISE TCPdumpで確認します。WLCとISEでキャプチャを設定して開始します。



WLC EPCおよびISE TCPDump

問題の再現後に、キャプチャを収集してトラフィックを関連付けます。次に、ISEホスト名が解決され、ポート8443でクライアントとISE間の通信が行われていることがわかります。



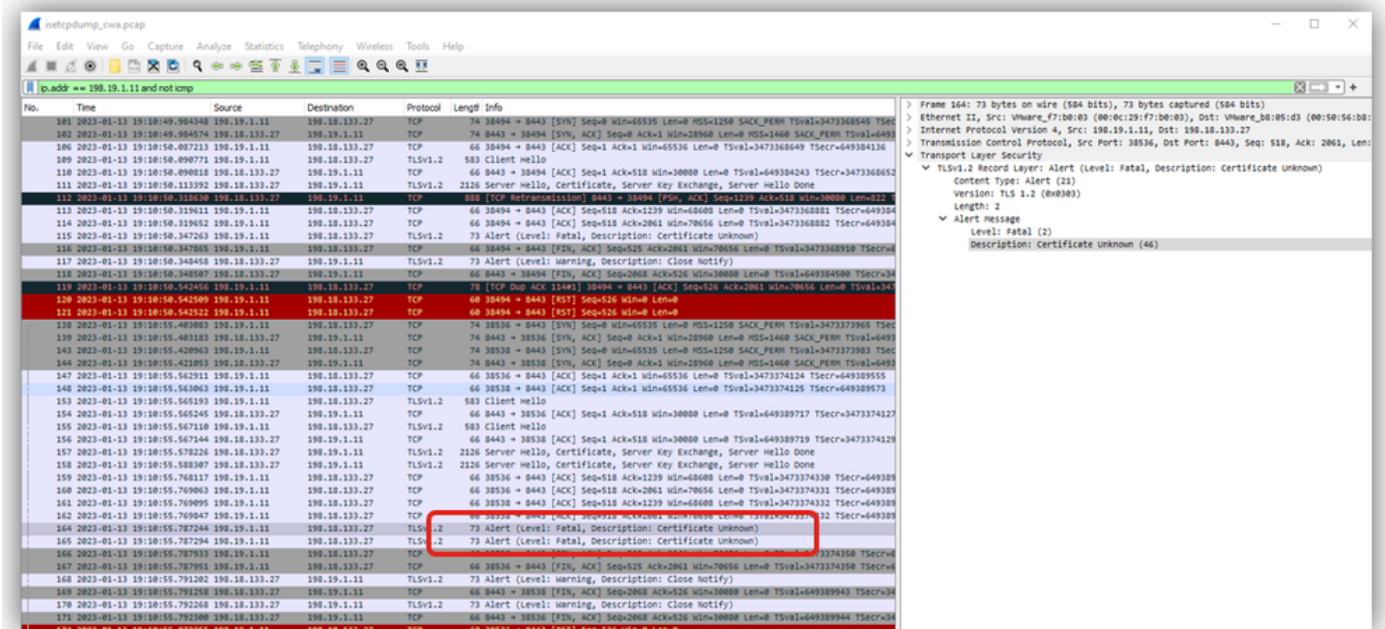
WLCおよびISEトラフィック

11 – 証明書によってセキュリティ違反が発生するのはなぜですか。

ISEで自己署名証明書を使用する場合、クライアントがISEポータルログインページを表示しようとすると、クライアントがセキュリティ警告をスローすることが想定されます。

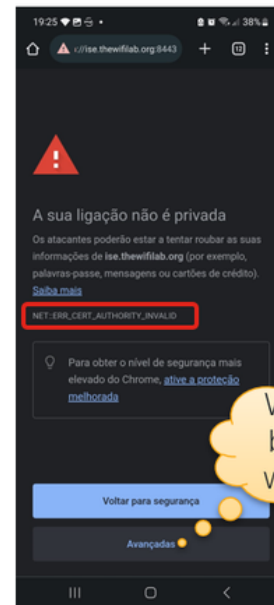
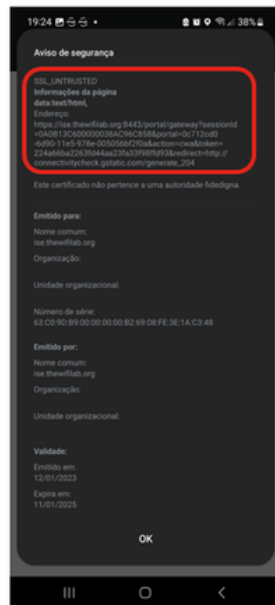
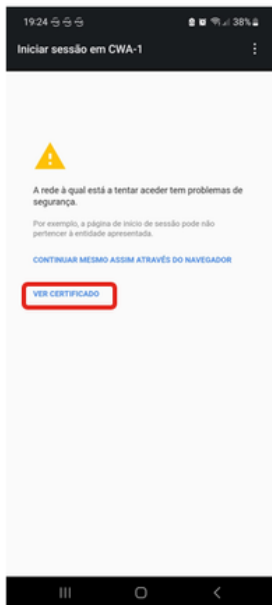
WLC EPCまたはISE TCPdumpで、ISE証明書が信頼できるかどうかを確認できます。

この例では、ISE証明書が不明（信頼できる）であることを意味するアラート（レベル：Fatal、説明：certificate Unknown）を伴うクライアントからの接続の終了を確認できます。



ISEの信頼できない証明書

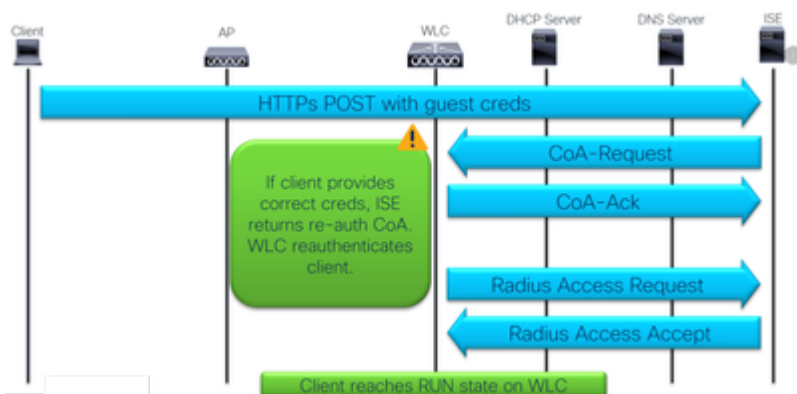
クライアント側で確認すると、次の出力例が表示されます。



ISE 証明書を信頼しないクライアントデバイス

最後に、リダイレクションが機能している!!しかし、ログインは失敗します。

最後にもう1回フローを確認します。



クライアントログインおよびCoA

12 – ゲストログインが失敗しますか？

ISEログで認証の失敗を確認します。クレデンシャルが正しいことを確認します。

Overview		Steps	
Event	5418 Guest Authentication Failed	5418	Guest Authentication Failed
Username	Cwa		
Endpoint Id	F2:A4:01:57:8D:68 @		
Endpoint Profile			
Authorization Result			

Authentication Details	
Source Timestamp	2023-01-13 21:32:29.201
Received Timestamp	2023-01-13 21:32:29.201
Policy Server	ise
Event	5418 Guest Authentication Failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	Cwa

Make sure you using correct credentials 😊

クレデンシャルが間違っているため、ゲスト認証が失敗する

13 – ログインは成功するが、実行に移らない？

ISEログで認証の詳細と結果を確認します。

Overview		Steps	
Event	5236 Authorize-Only succeeded	11001	Received RADIUS Access-Request
Username	cwa	11017	RADIUS created a new session
Endpoint Id	F2:A4:01:57:8D:68 @	11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
Endpoint Profile	Android	15049	Evaluating Policy Group
Authentication Policy	Default	15008	Evaluating Service Selection Policy
Authorization Policy	Default >> Redirect-to-Portal	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
Authorization Result	CWAredirect	15036	Evaluating Authorization Policy
		24209	Looking up Endpoint in Internal Endpoints IDStore - cwa
		24211	Found Endpoint in Internal Endpoints IDStore
		15016	Selected Authorization Profile - CWAredirect
		24210	Looking up User in Internal Users IDStore - cwa
		24212	Found User in Internal Users IDStore
		11002	Returned RADIUS Access-Accept

Authentication Details	
Source Timestamp	2023-01-13 21:36:01.8
Received Timestamp	2023-01-13 21:36:01.8
Policy Server	ise
Event	5236 Authorize-Only succeeded
Username	cwa
User Type	User

Result	
User-Name	cwa
Class	CACS:0A0B13C60000003BAD0BF3E4:ise/462943192/128
cisco-av-pair	url-redirect-acl=REDIRECT
cisco-av-pair	url-redirect=https://ise.thewifilab.org:8443/portal/gateway?sessionId=0A0B13C60000003BAD0BF3E4&portal=0c712cd0-6d90-11e5-978e-005056b2f0a&action=cwa&token=92eb9963bc6f70c9f82d32ed8a072c6c
cisco-av-pair	profile-name=Android
LicenseTypes	Essential license consumed.

Still getting Redirect-to-Portal ????

リダイレクトループ

この例では、リダイレクトURLとリダイレクトACLを含む認可プロファイルをクライアントが再度取得していることがわかります。その結果、リダイレクトループが発生します。

ポリシーセットを確認します。Guest_Flowのルールチェックは、リダイレクトの前に行う必要があります。

Guest_Flowルール

14 - COAが失敗しているか

EPCとISE TCPDumpを使用すると、CoAトラフィックを確認できます。WLCとISEの間でCoAポート(1700)が開いているかどうかを確認します。共有秘密が一致していることを確認します。

No.	Time	Source	Destination	Protocol	Length	Info
214	2023-01-13 19:38:06.999336	198.19.11.10	198.18.133.27	RADIUS	468	Accounting-Request id=212
215	2023-01-13 19:38:06.999734	198.18.133.27	198.19.11.10	RADIUS	84	Accounting-Response id=212
296	2023-01-13 19:38:14.104990	198.19.11.10	198.18.133.27	RADIUS	408	Access-Request id=213
296	2023-01-13 19:38:14.121987	198.18.133.27	198.19.11.10	RADIUS	409	Access-Accept id=213
310	2023-01-13 19:38:14.426964	198.19.11.10	198.18.133.27	RADIUS	400	Accounting-Request id=214
311	2023-01-13 19:38:14.427971	198.19.11.10	198.18.133.27	RADIUS	442	Accounting-Request id=215
312	2023-01-13 19:38:14.438972	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=215
313	2023-01-13 19:38:14.444971	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=214
351	2023-01-13 19:38:15.224979	198.19.11.10	198.18.133.27	RADIUS	468	Accounting-Request id=216
352	2023-01-13 19:38:15.229983	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=216
3539	2023-01-13 19:38:50.416970	198.18.133.27	198.19.11.10	RADIUS	248	CoA-Request id=4
3540	2023-01-13 19:38:50.416970	198.19.11.10	198.18.133.27	RADIUS	475	Access-Request id=217
3541	2023-01-13 19:38:50.416970	198.18.133.27	198.19.11.10	RADIUS	111	CoA-Ack id=4
3542	2023-01-13 19:38:50.428963	198.18.133.27	198.19.11.10	RADIUS	166	Access-Accept id=217

CoAトラフィック

注：バージョン17.4.X以降では、RADIUSサーバを設定する際に、CoAサーバキーも必ず設定してください。共有秘密と同じキーを使用します（ISEではデフォルトで同じです）。RADIUSサーバで設定されている場合は、共有秘密キーとは異なるキーをCoAにオプションで設定します。Cisco IOS® XE 17.3では、Web UIはCoAキーと同じ共有秘密を使用していました。

バージョン17.6.1以降では、RADIUS（CoAを含む）がこのポートでサポートされています。RADIUSのサービスポートを使用する場合は、次の設定が必要です。

<#root>

```
aaa server radius dynamic-author  
client 10.48.39.28
```

```
vrf
```

```
Mgmt-intf
```

```
server-key cisco123
```

```
interface GigabitEthernet0
```

```
vrf
```

```
forwarding
```

```
Mgmt-intf
```

```
ip address x.x.x.x x.x.x.x
```

```
!if using aaa group server:  
aaa group server radius group-name  
server name nicoISE
```

```
ip
```

```
vrf
```

```
forwarding
```

```
Mgmt-intf
```

```
ip
```

```
radius
```

```
source
```

```
-interface GigabitEthernet0
```

結論

再開されたCWAチェックリストを次に示します。

- ・ クライアントが正しいVLANに配置され、IPアドレスとDNSを取得することを確認します。

- WLCでクライアントの詳細を取得し、パケットキャプチャを実行してDHCP交換を表示します。
- クライアントがDNS経由でホスト名を解決できることを確認します。
 - cmdからホスト名にpingを実行します。
- WLCはポート80でリッスンしている必要があります
 - グローバルコマンドip http serverまたはグローバルパラメータマップコマンドwebauth-http-enableを確認します。
- 証明書に関する警告を回避するには、信頼できる証明書をISEにインストールします。
 - CWAのWLCに信頼できる証明書をインストールする必要はありません。
- ISEでの認証ポリシーの詳細オプション「Continue」（ユーザが見つからない場合）
 - スポンサーされたゲストユーザが接続し、URLリダイレクトとACLを取得できるようにするため。

また、トラブルシューティングで使用される主なツールは次のとおりです。

- WLC EPC
 - 内部フィルタ：DHCPプロトコル、MACアドレス。
- WLCモニタ
 - クライアントセキュリティの詳細を確認します。
- WLC RAトレース
 - WLC側の詳細情報を含むデバッグ。
- ISE ライブログ
 - 認証の詳細。
- ISEのTCPDump
 - ISE PSNインターフェイスでパケットキャプチャを収集します。

参考資料

[Catalyst 9800 WLCおよびISEでの中央Web認証\(CWA\)の設定](#)

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。