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

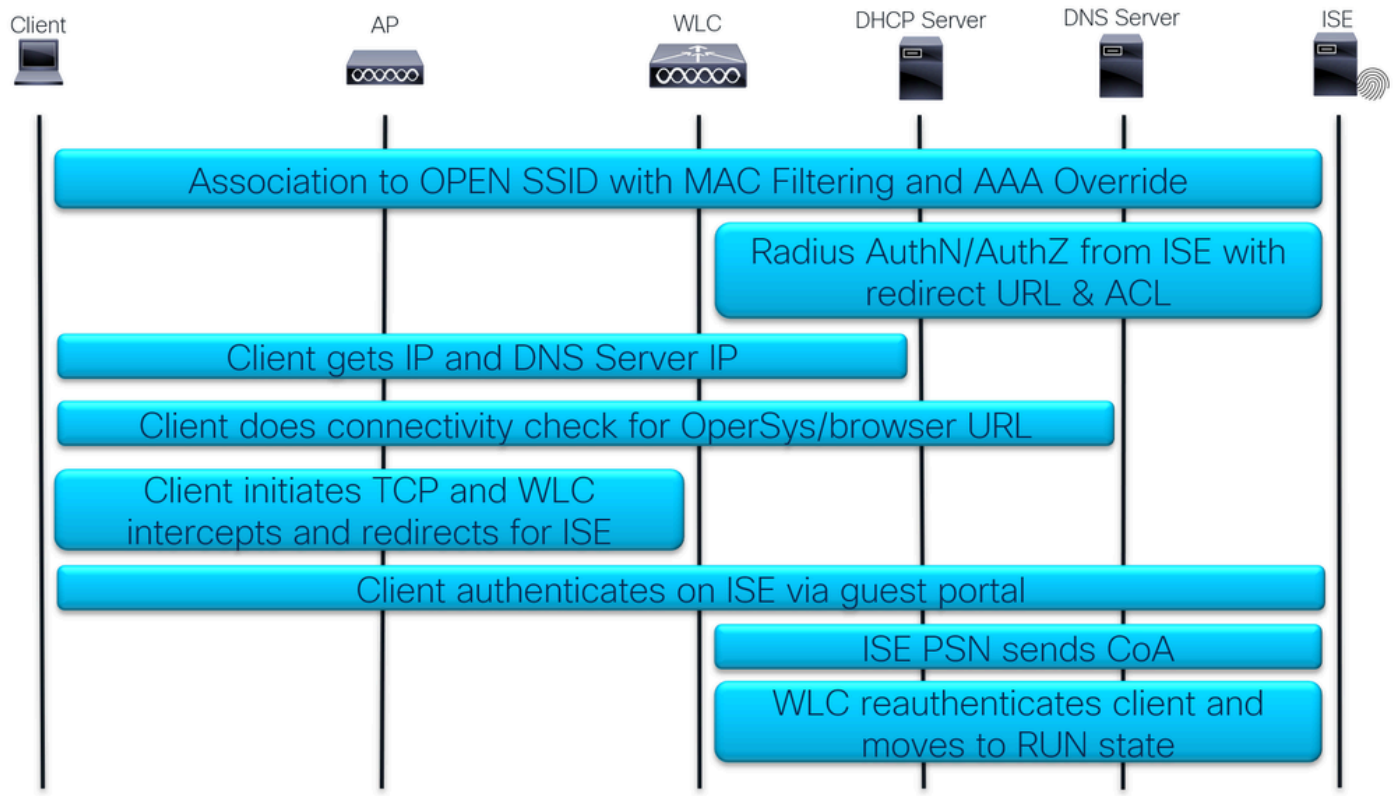
このドキュメントでは、WLC 9800およびISEを使用した中央Web認証(CWA)のトラブルシューティング方法について説明します。

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。

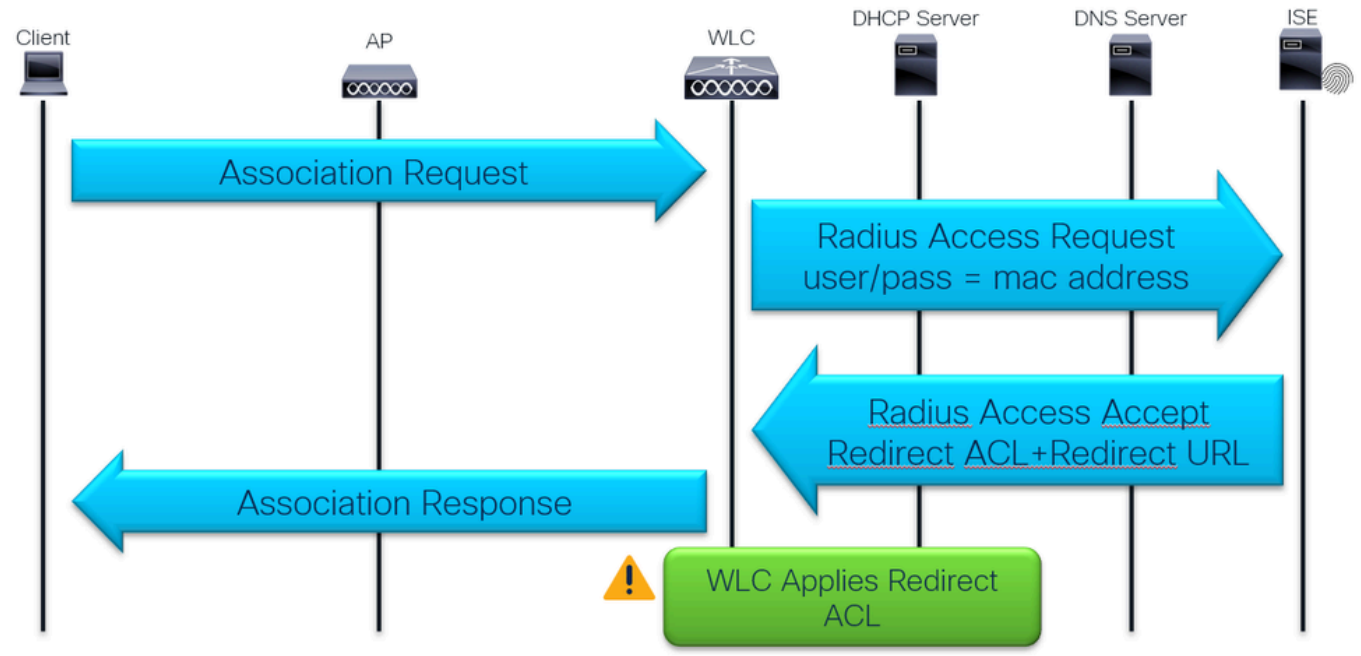
CWAのパケットフローを次に示します。



CWAパケットフロー

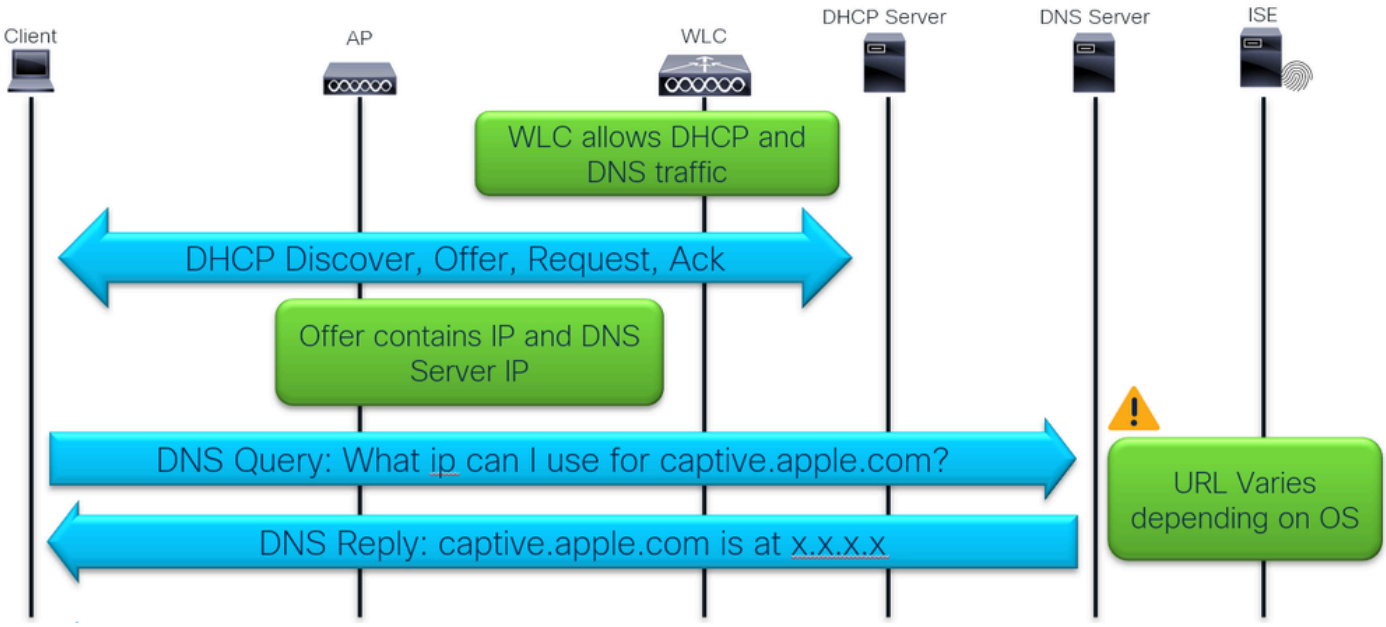
詳細フロー

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。

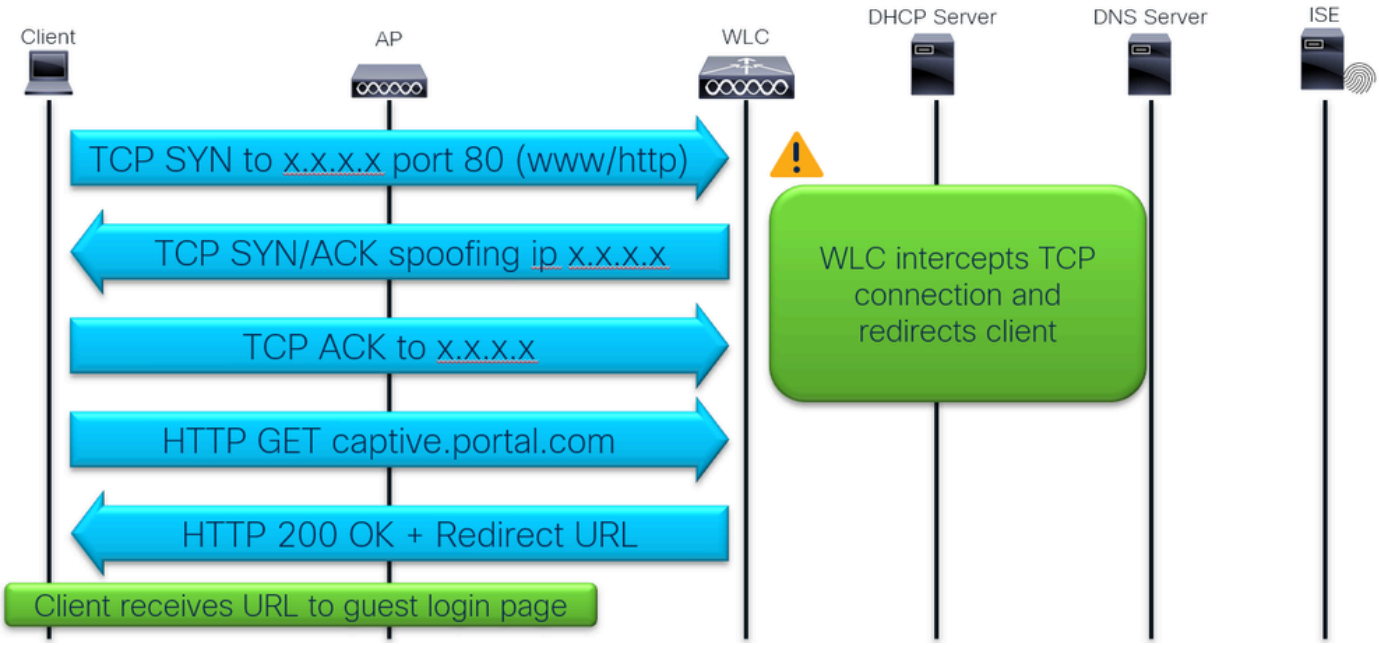
特定のドメインに対してHTTP GETを実行するように事前にプログラムされたデバイスOSがあります

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

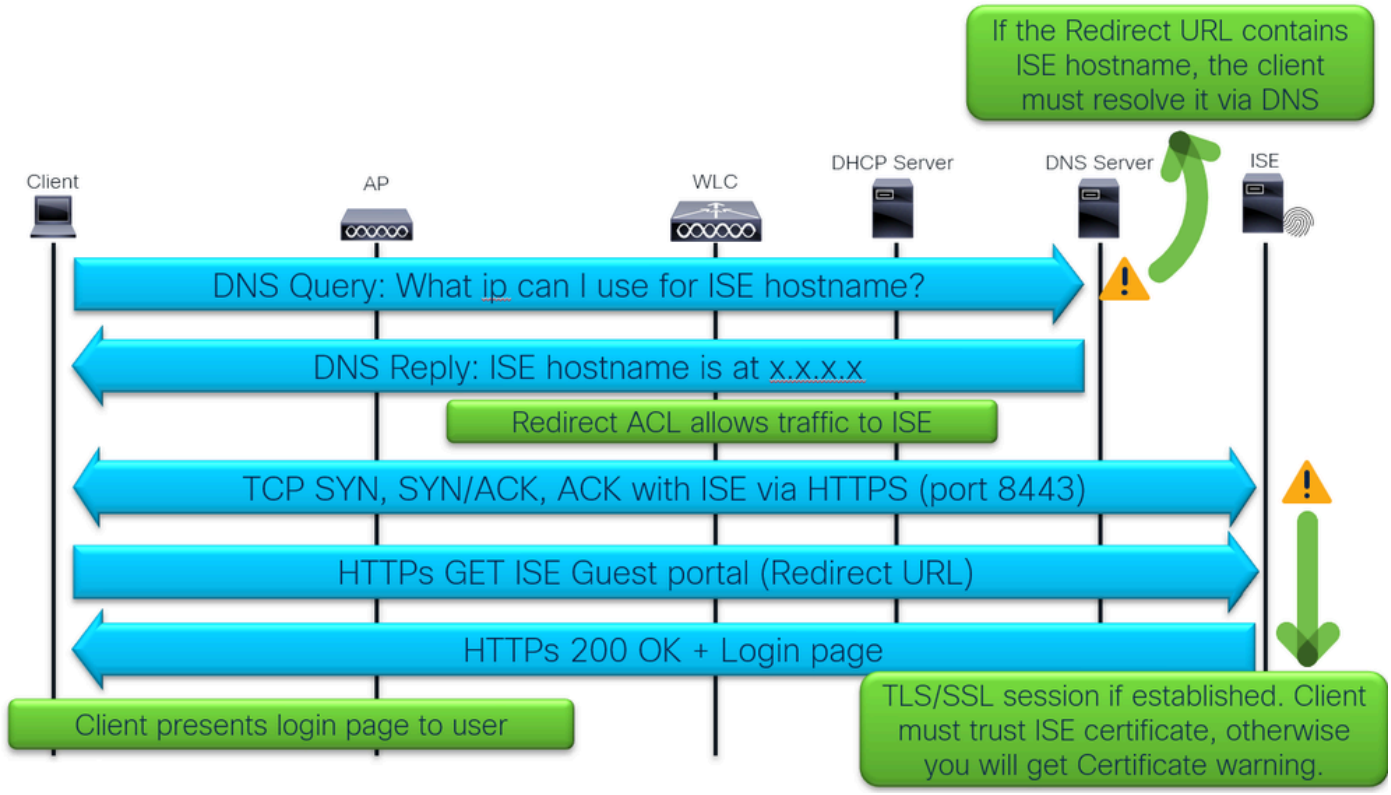
- クロム= clients3.google.com
- Firefox = detectportal.firefox.com

トラフィックの代行受信とリダイレクト：



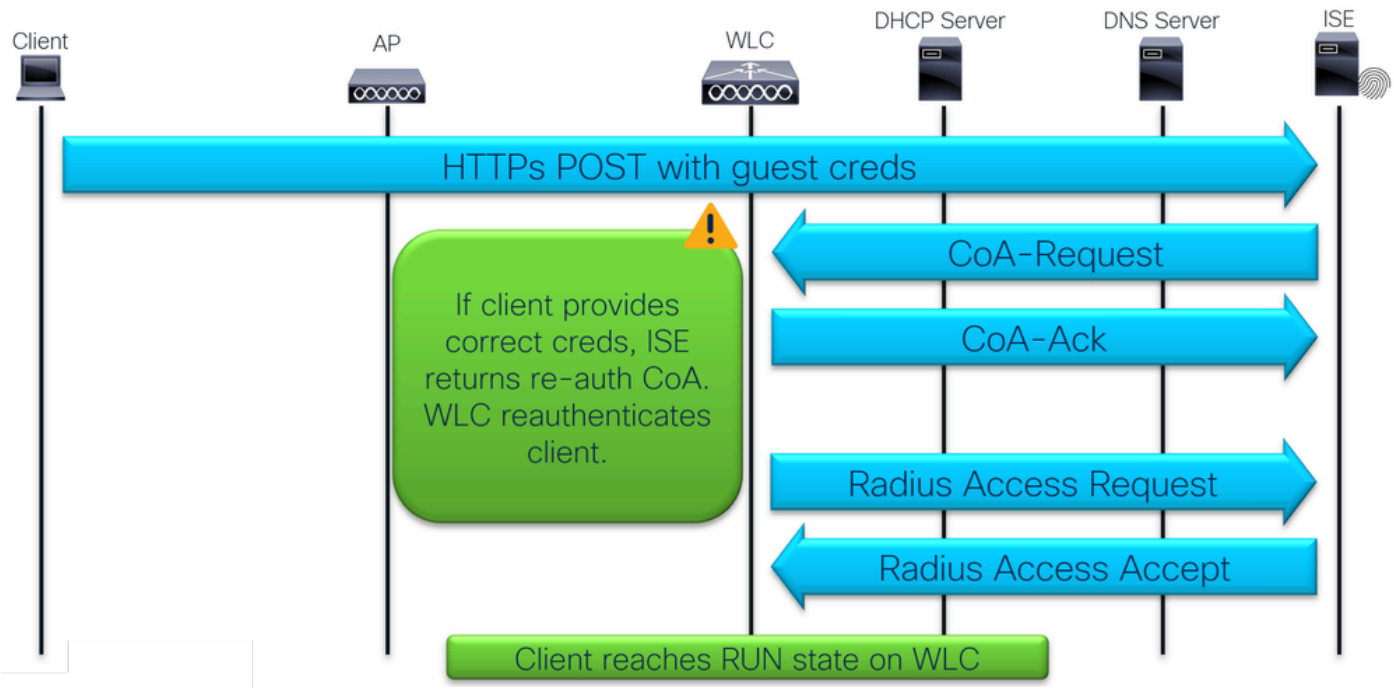
トラフィックの代行受信とリダイレクト

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:

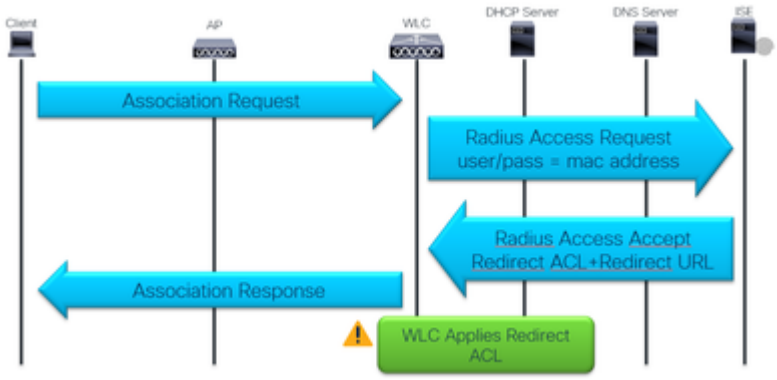


クライアントログインおよびCoA

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。

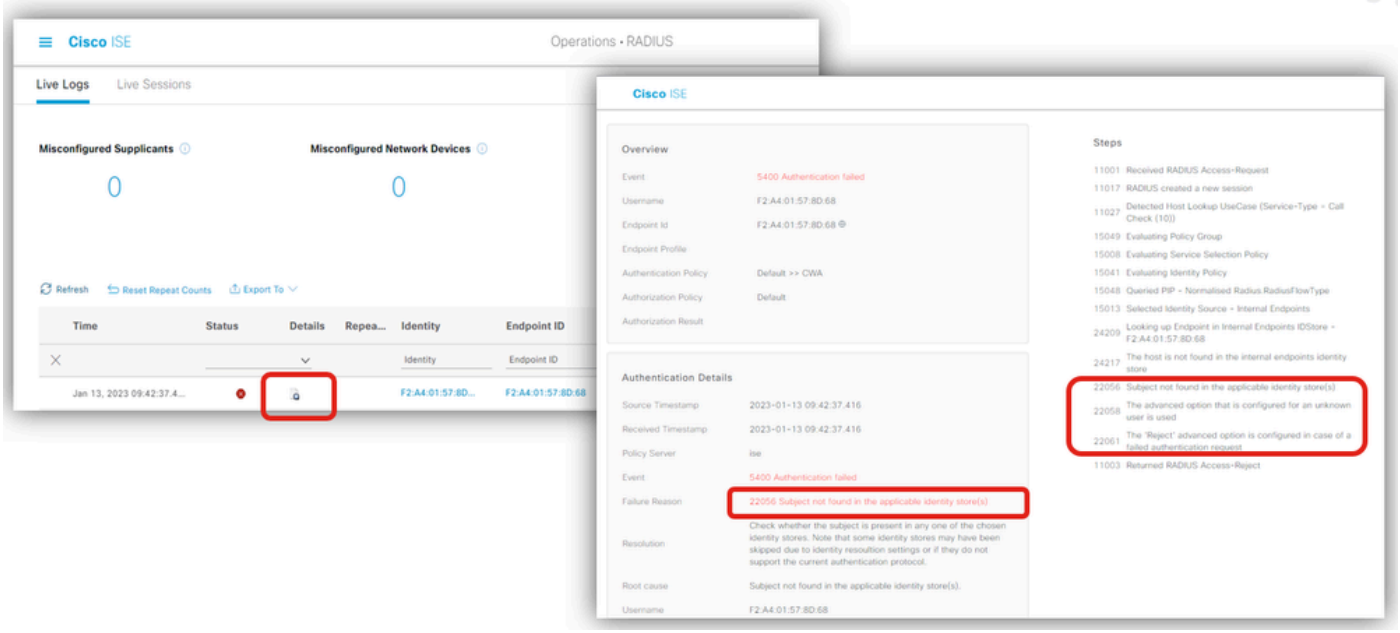
フローの最初の部分から説明します。



最初の関連付けとRADIUS認証

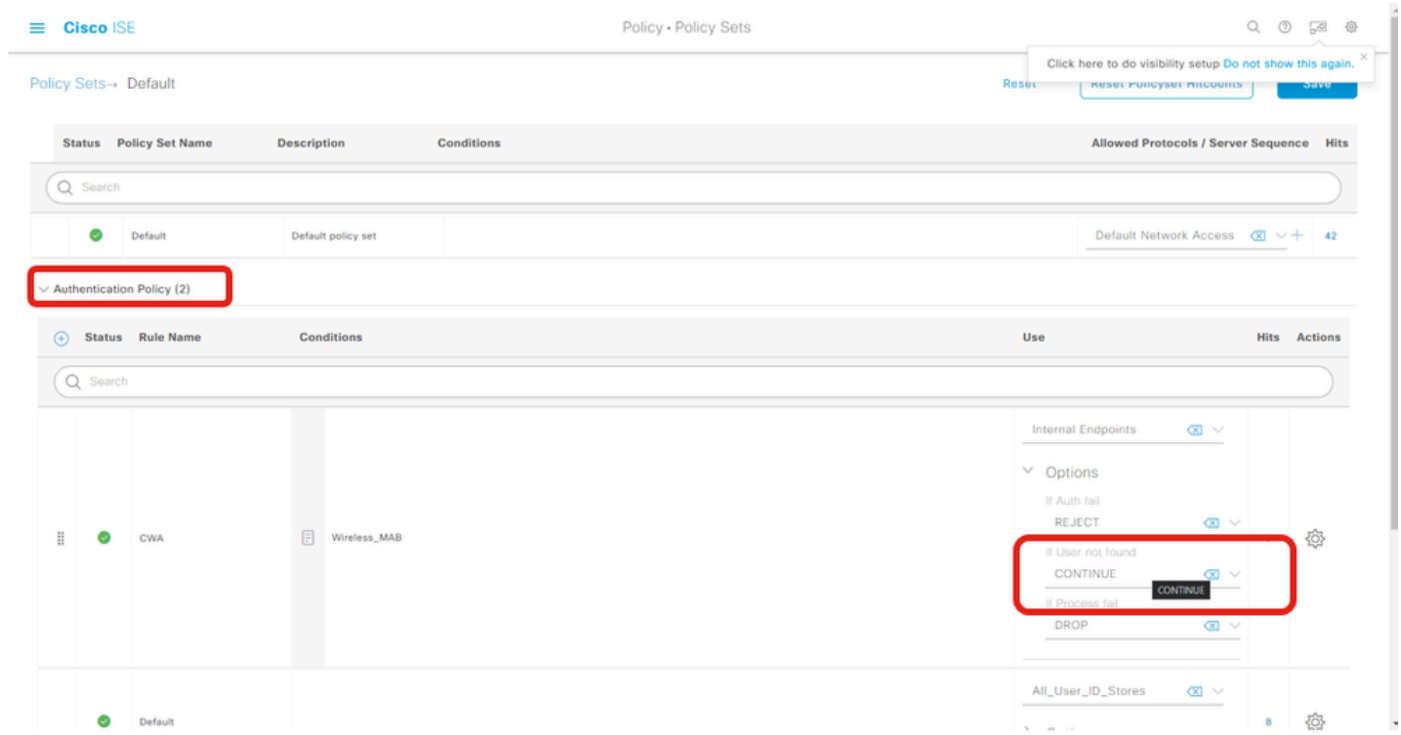
1 – 最初のRADIUS認証は成功しましたか。

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

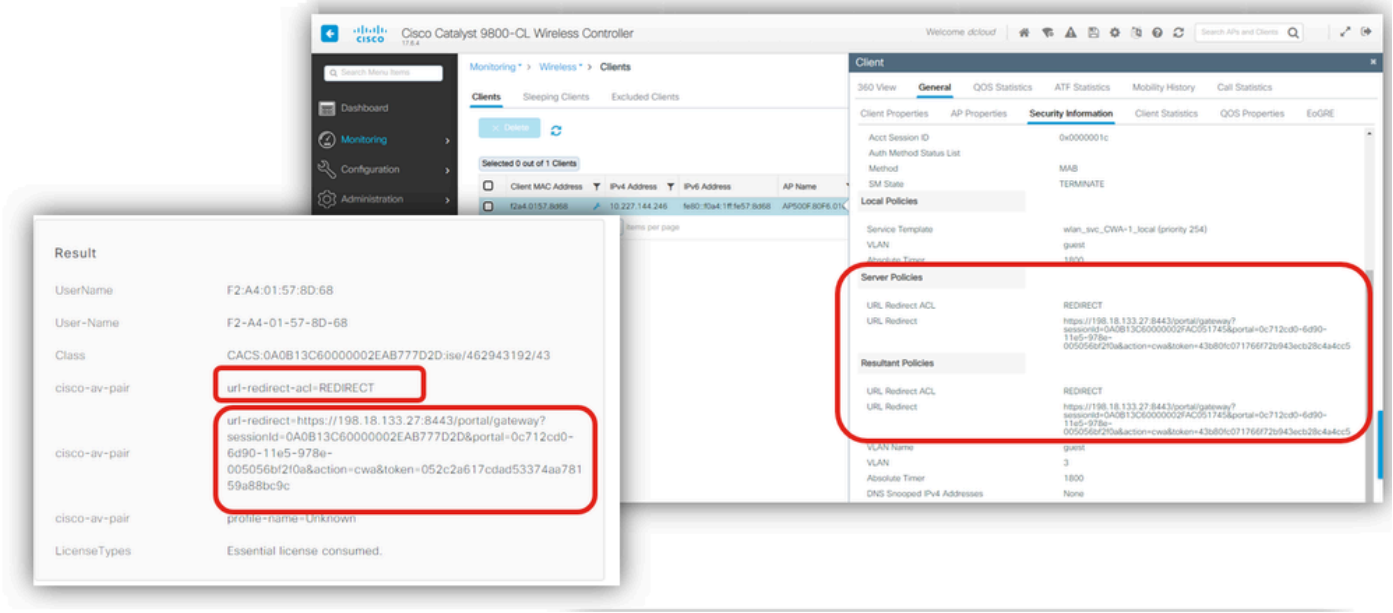
ユーザが見つからない場合は、認証の詳細オプションが「Continue」に設定されていることを確認します。



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

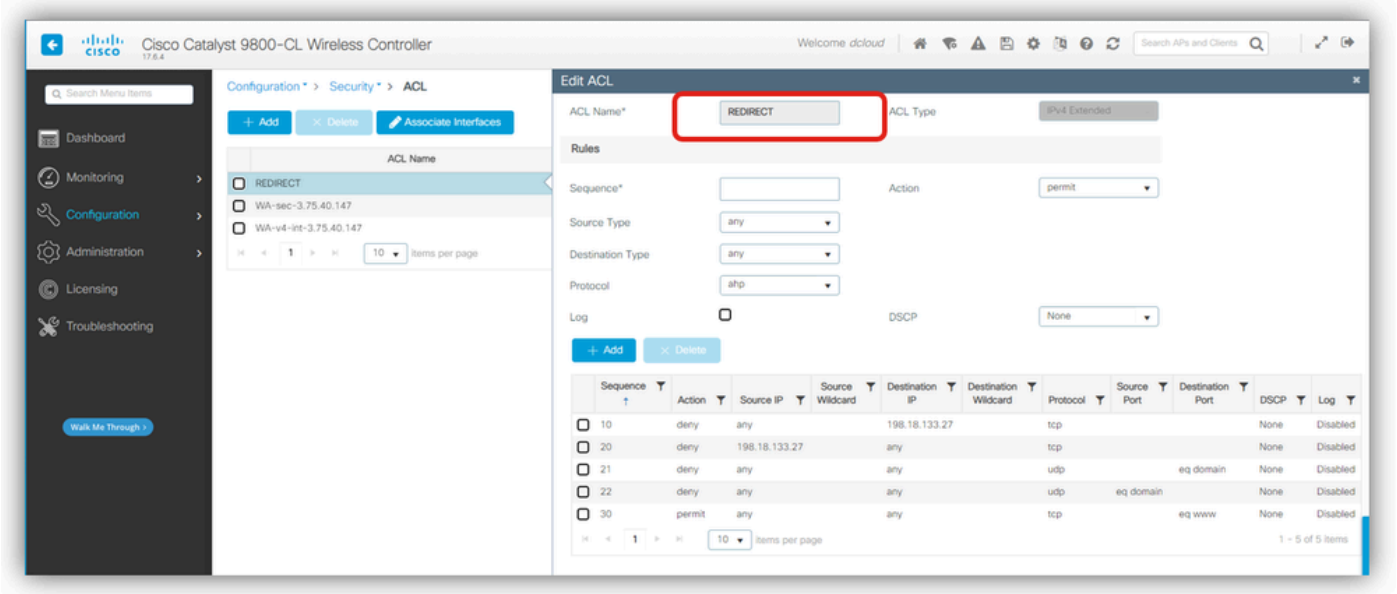
モニタリングでISEライブログとWLCクライアントのセキュリティ情報を確認します。ISEがリダイレクトURLとACLをAccess Acceptで送信し、WLCで受信されてクライアントに適用されていることを、クライアントの詳細情報で確認します。



リダイレクトACLとURL

3 – リダイレクトACLは正しいですか。

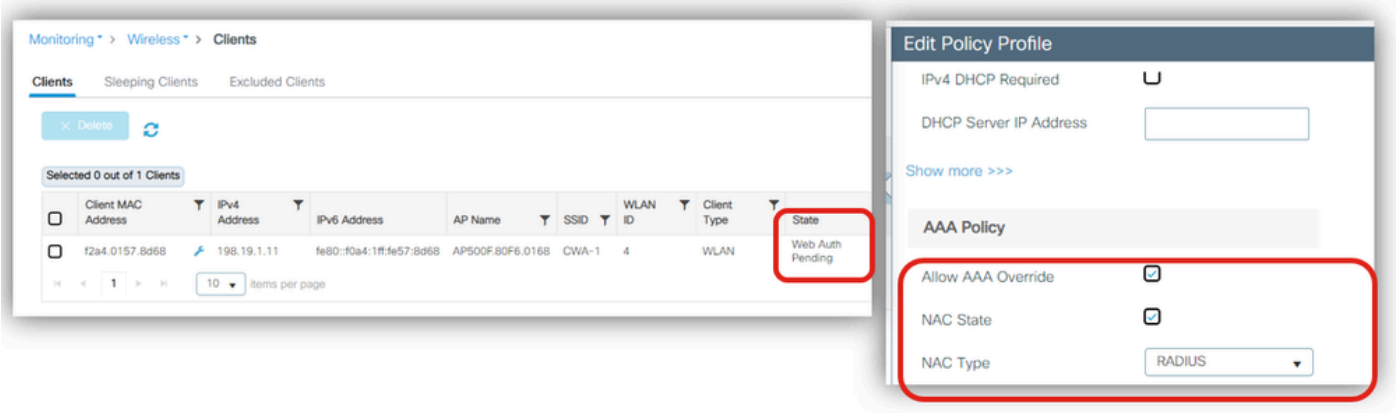
ACL名のタイプミスをチェックします。ISEから送信されたものとまったく同じであることを確認します。



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。

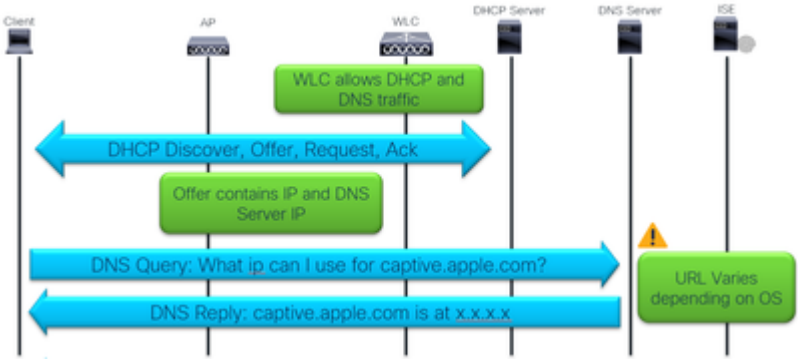
クライアントの詳細で「Web Auth Pending」状態を確認します。この状態でない場合は、AAA OverrideおよびRadius NACがポリシープロファイルで有効になっているかどうかを確認します。



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？

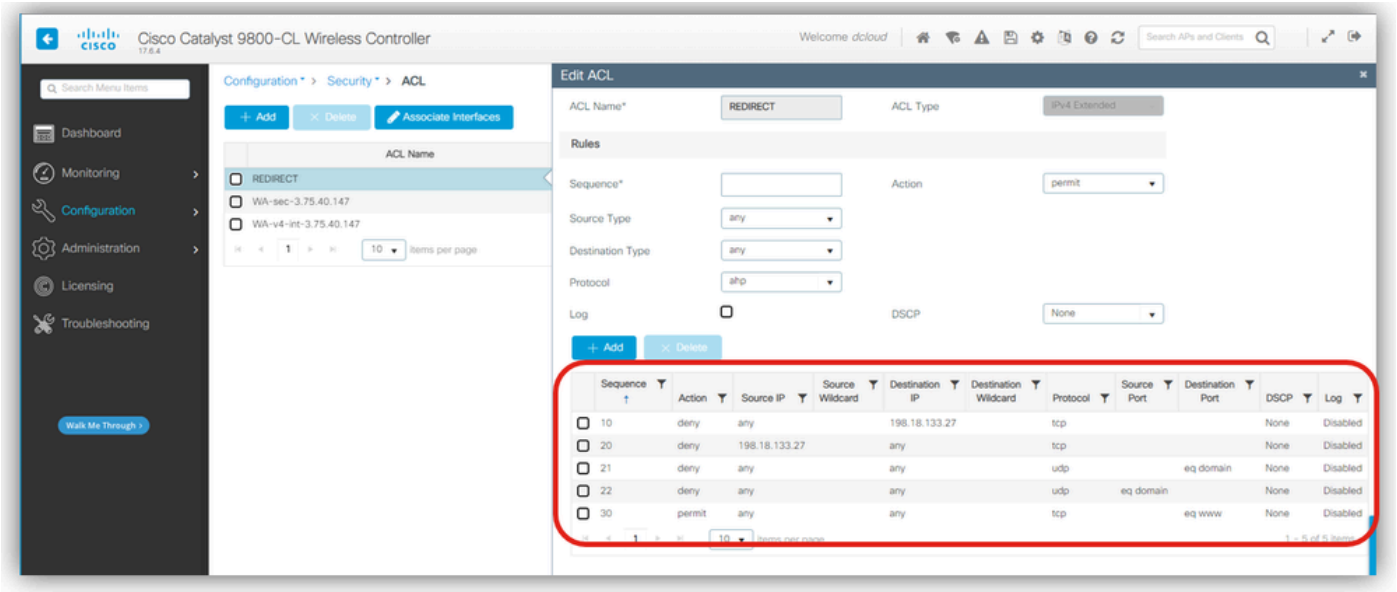
フローを見直してみましょう。



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。



WLCでのACLコンテンツのリダイレクト

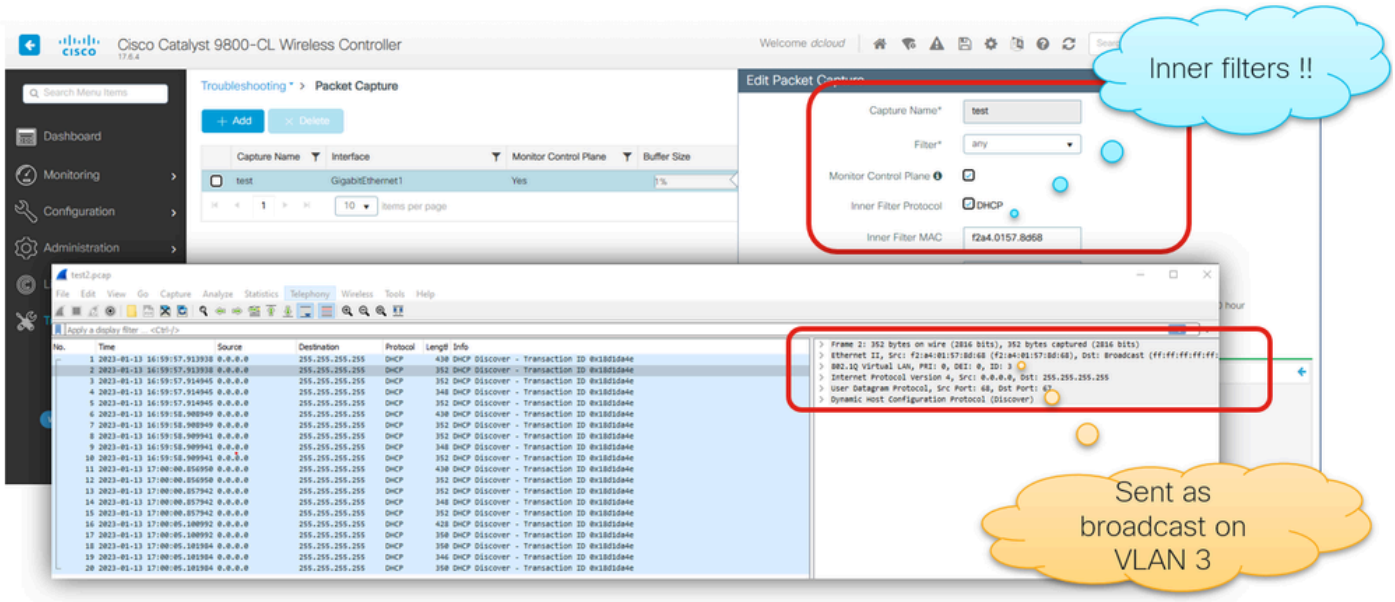
リダイレクトACLでは、permit文によって代行受信およびリダイレクトされるトラフィックと、代行受信およびリダイレクトから無視されるトラフィックをdeny文で定義します。

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。

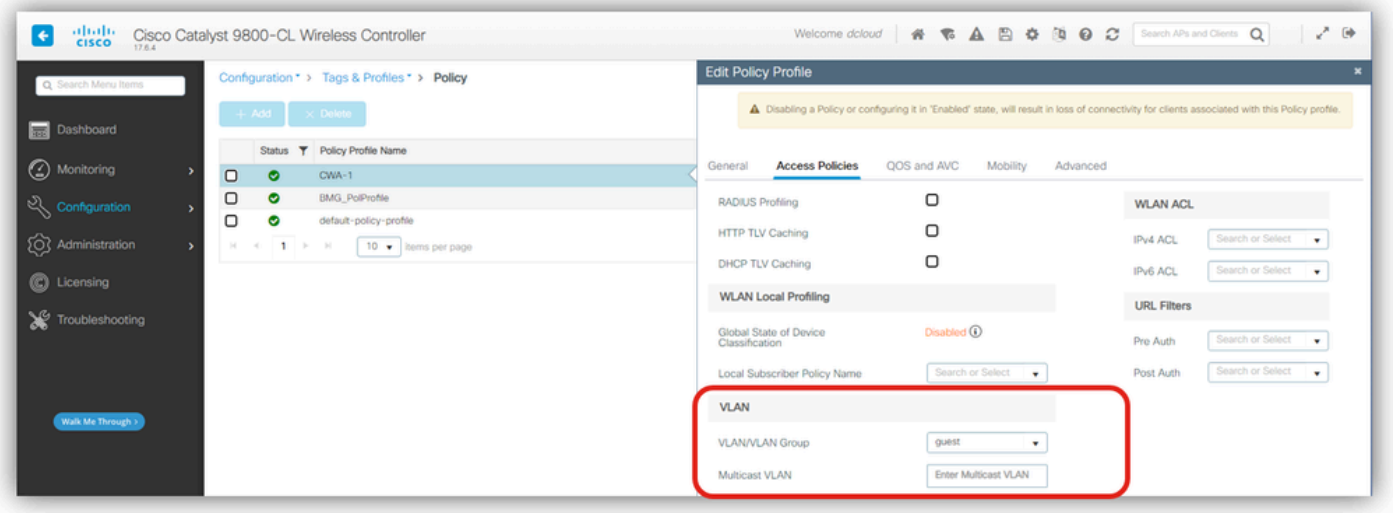
DHCP交換が発生するかどうかをEPCで確認します。EPCは、DHCPプロトコルや内部フィルタMACなどの内部フィルタと組み合わせて使用できます。内部フィルタMACでは、クライアントデバイスのMACアドレスを使用し、クライアントデバイスのMACアドレスで送受信されるDHCPパケットのみをEPCに取得できます。

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。



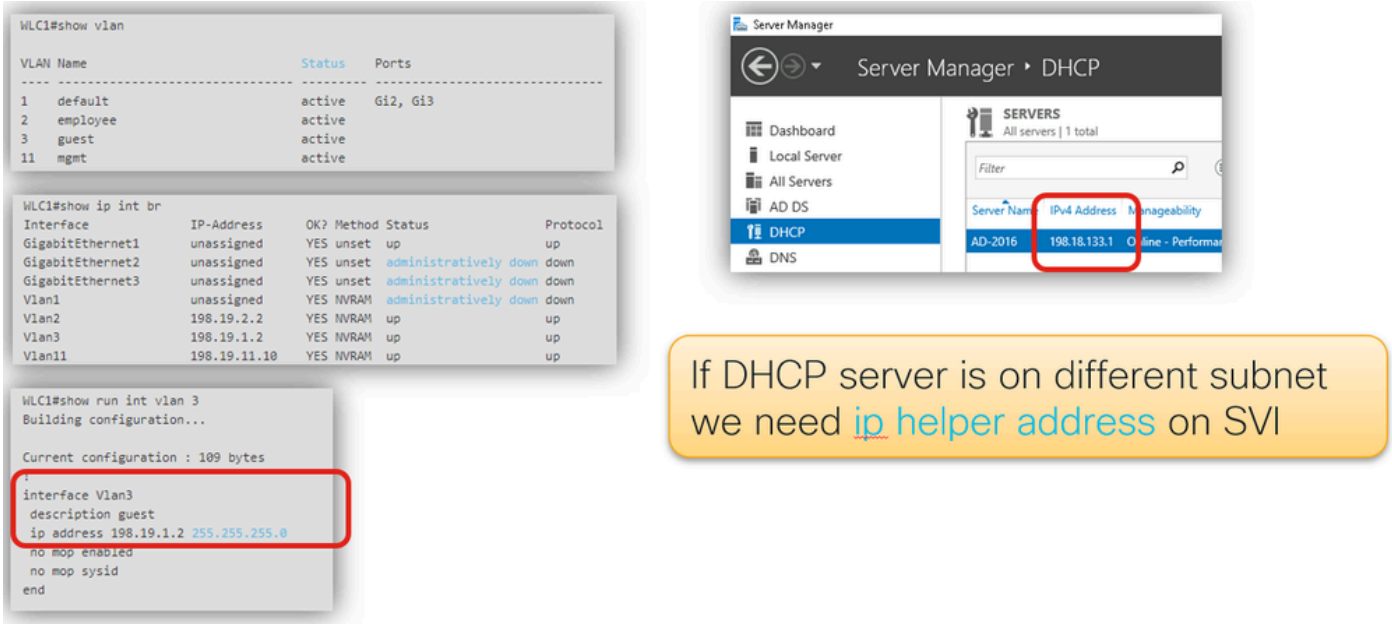
DHCPを確認するWLC EPC

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。



ポリシープロファイルの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。



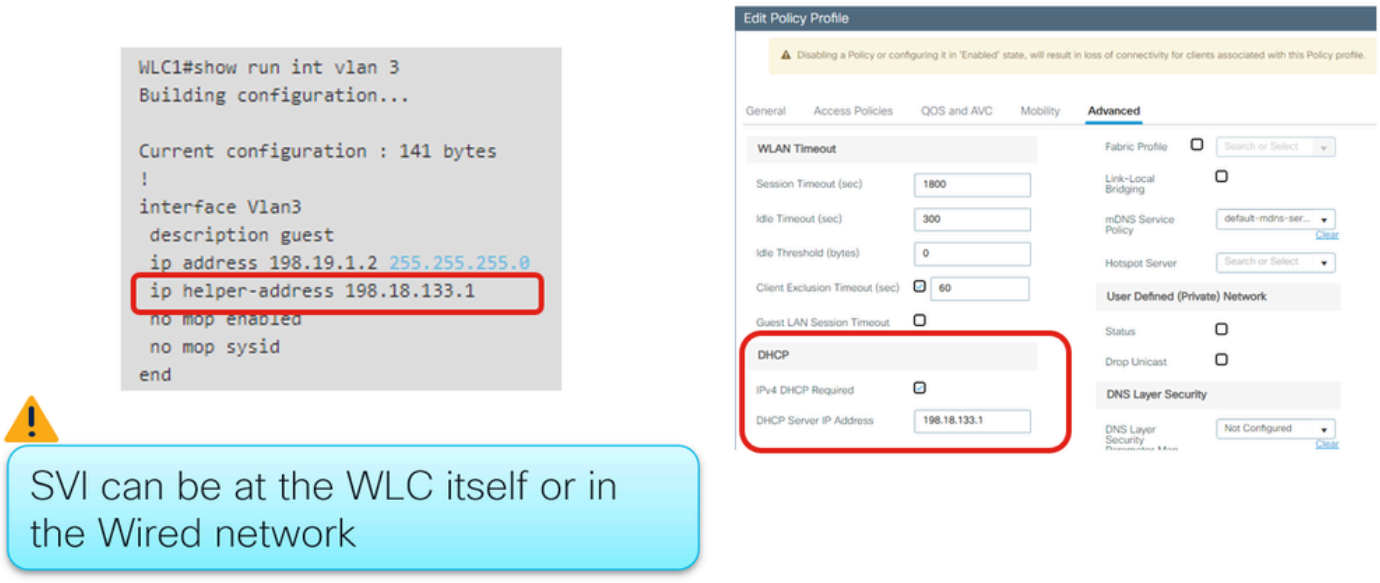
VLAN、スイッチポート、およびDHCPサブネット

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。

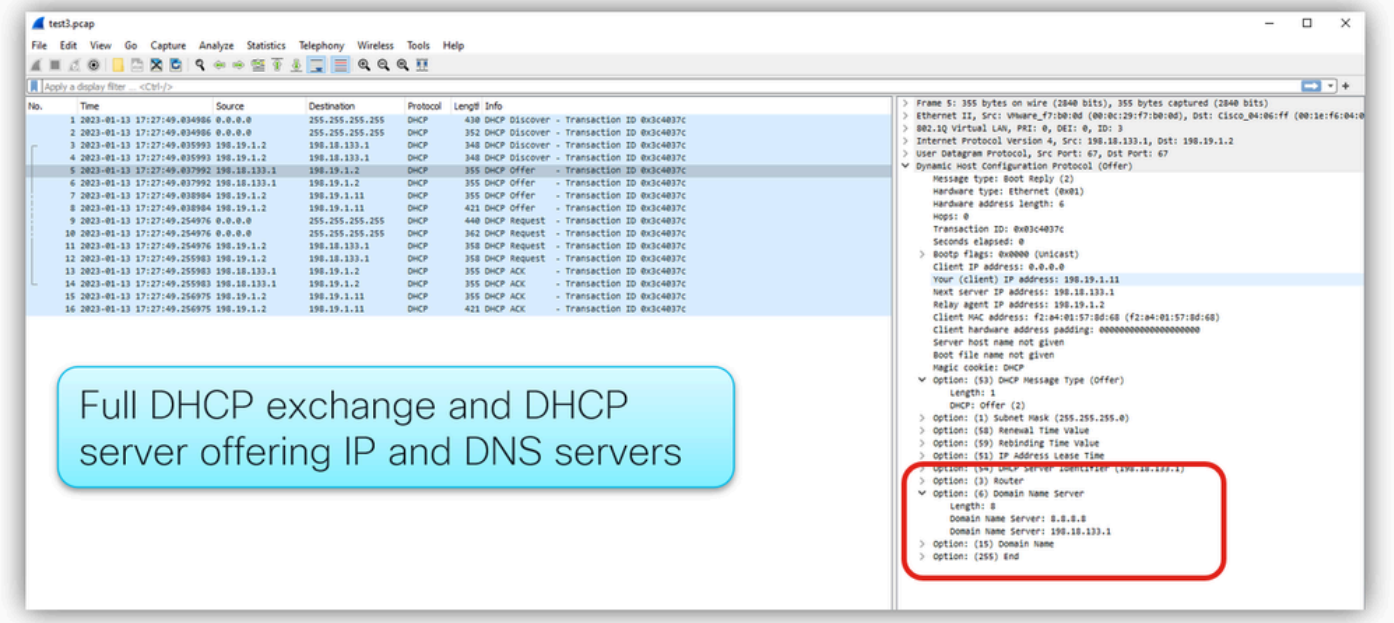
いずれの場合でも、SVIの配置場所に関係なく、ip helper-addressコマンドをSVIに追加する必要があります。

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。



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

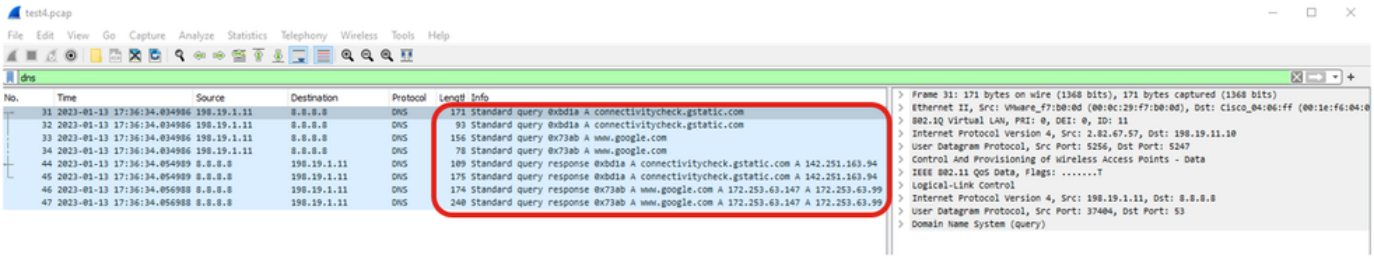
次に、EPCを使用して、DHCP交換が正常に行われ、DHCPサーバがDNSサーバIPを提供しているかどうかを確認します。



DNSサーバipのDHCPオファーの詳細

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。

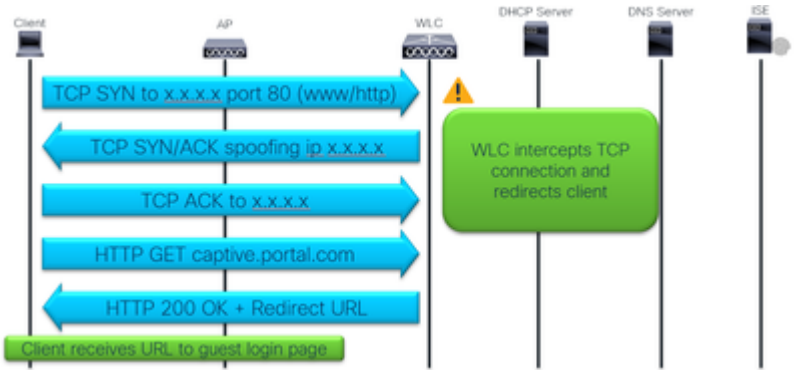


DNSクエリと応答

- 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？

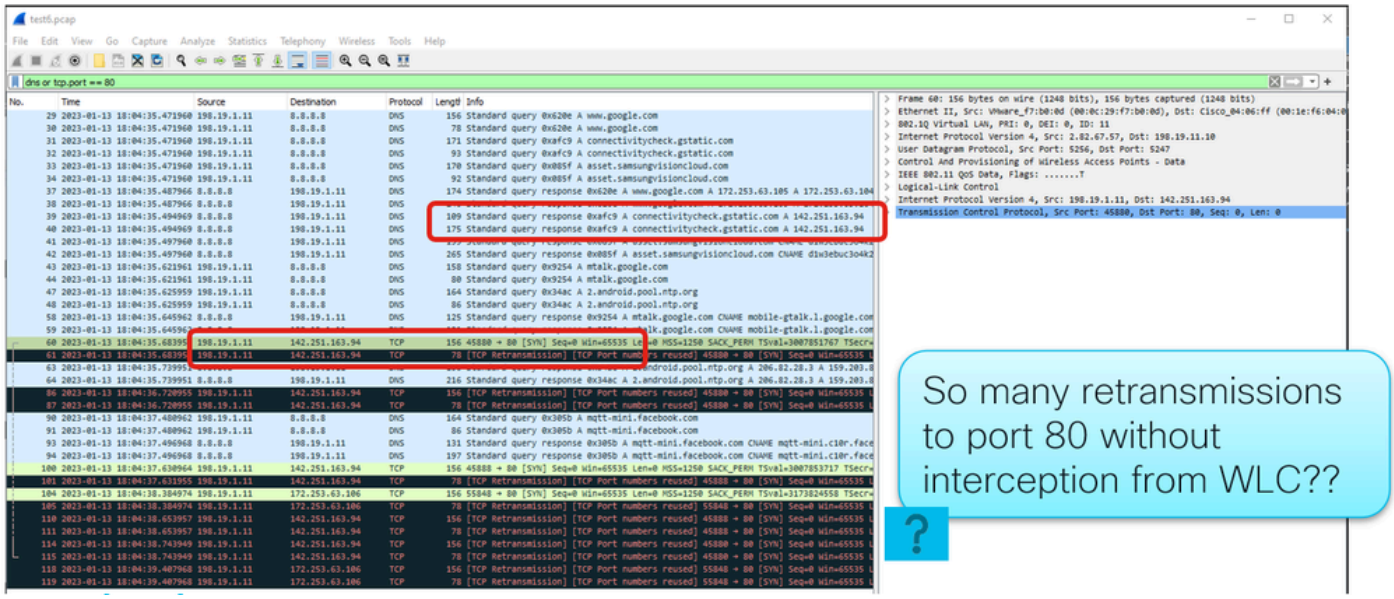
フローを見直してみましょう。



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

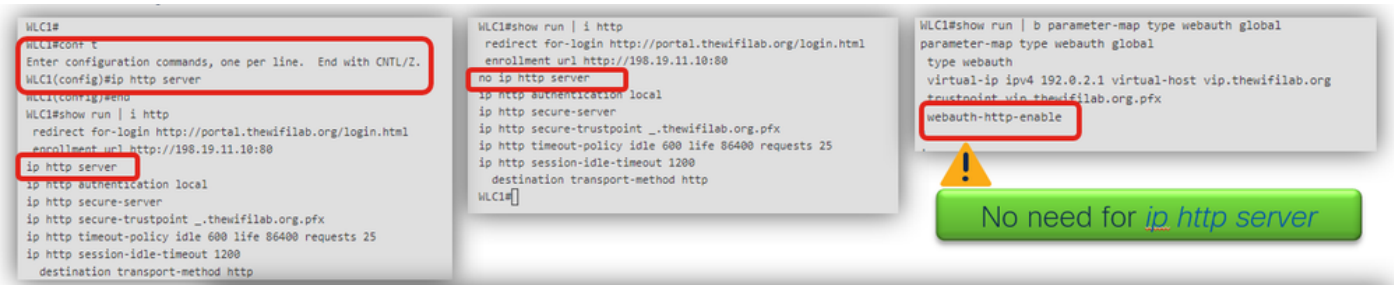
クライアントがTCP SYNをポート80に送信し、WLCがそれをインターセプトするかどうかを確認します。



ポート80へのTCP再送信

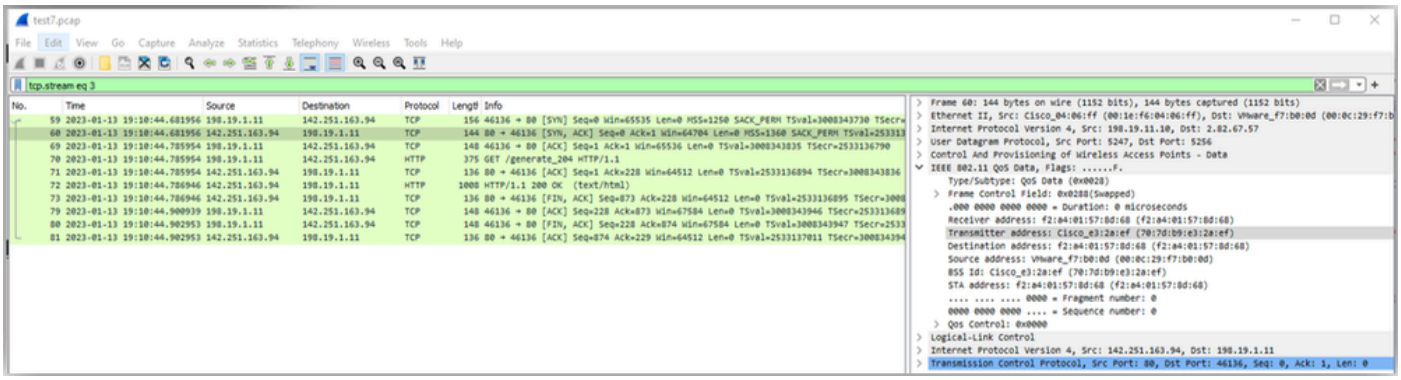
ここでは、クライアントがTCP SYNパケットをポート80に送信したものの、応答を受信せず、TCPの再送信を行っていることがわかります。

グローバルコン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。



HTTP代行受信コマンド

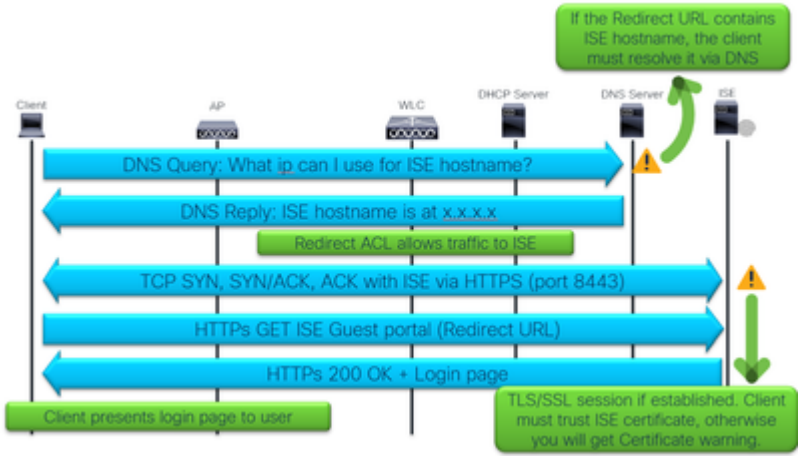
コマンドの後、WLCはTCPをインターセプトし、クライアントに応答してリダイレクトするために宛先IPアドレスをスプーフィングします。



WLCによるTCPインターセプション

まだ動いてないのか？

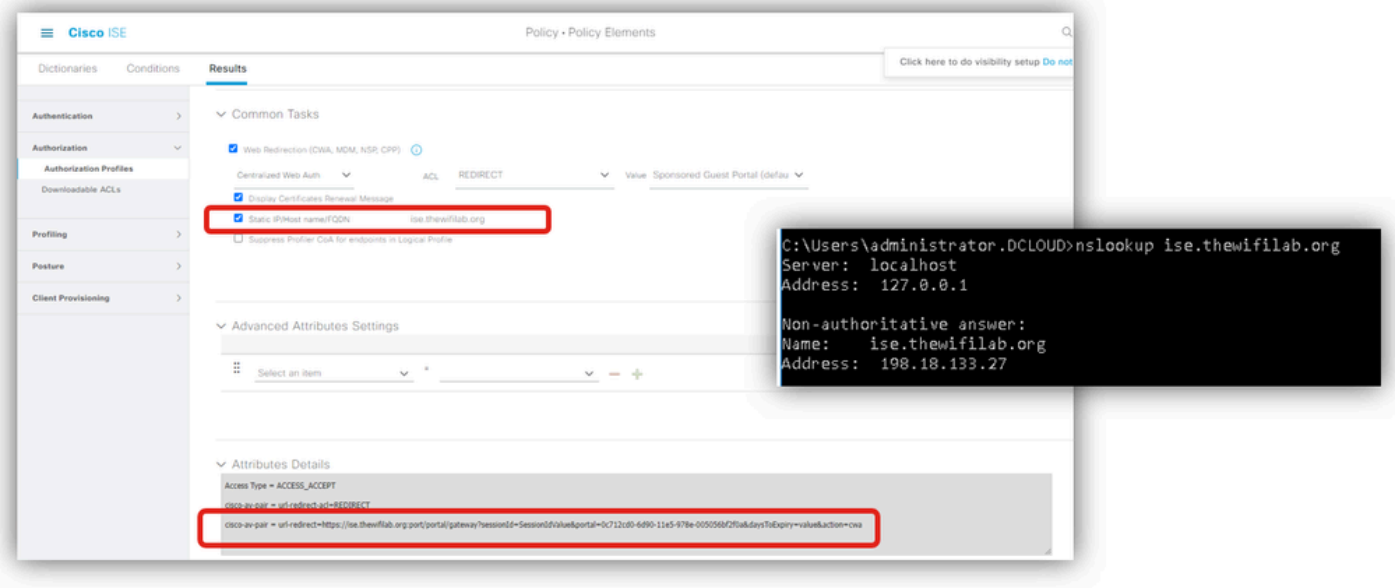
この流れには、さらに多くの要素が含まれています。



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。

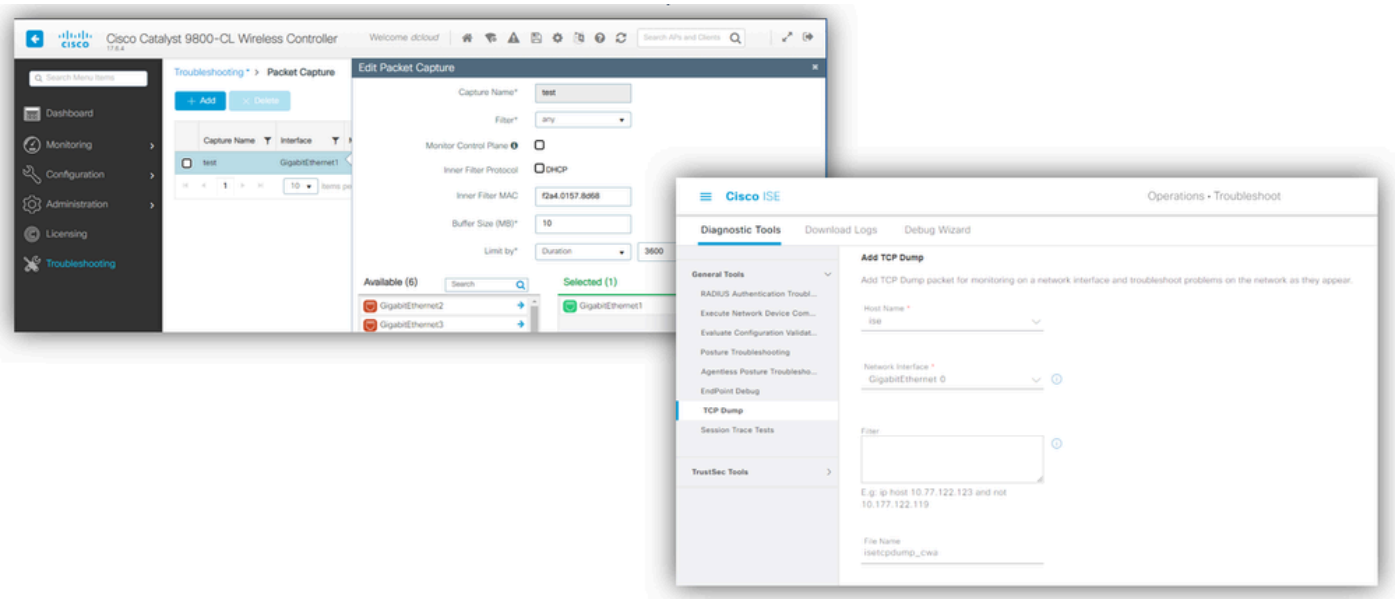


ISEホスト名解決

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。

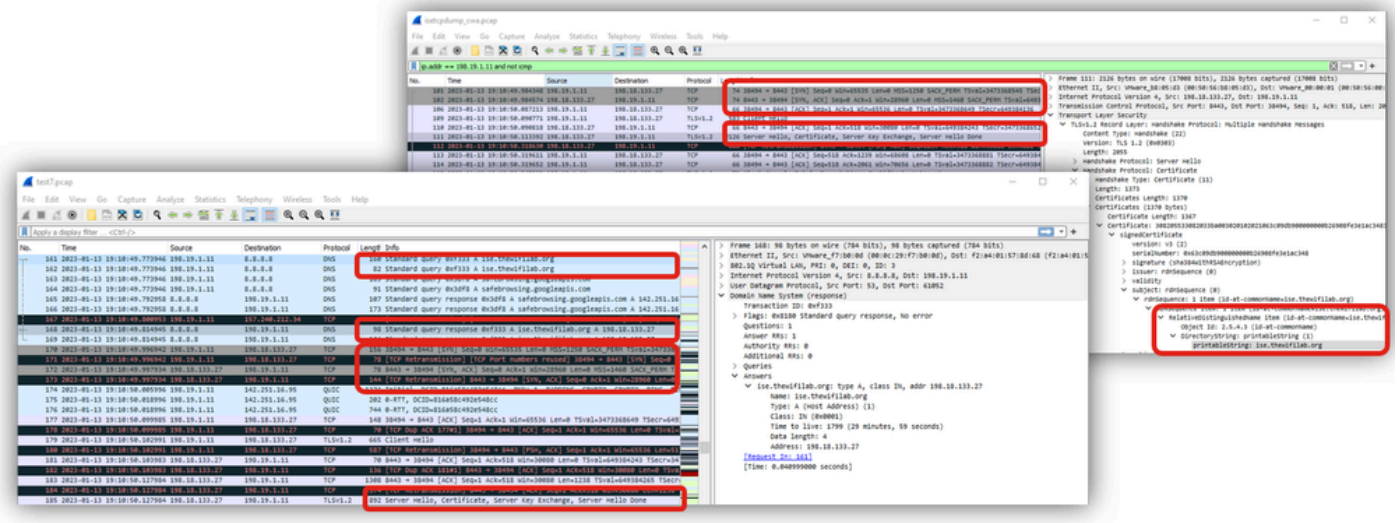
10 – ログインページがまだロードされない

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。



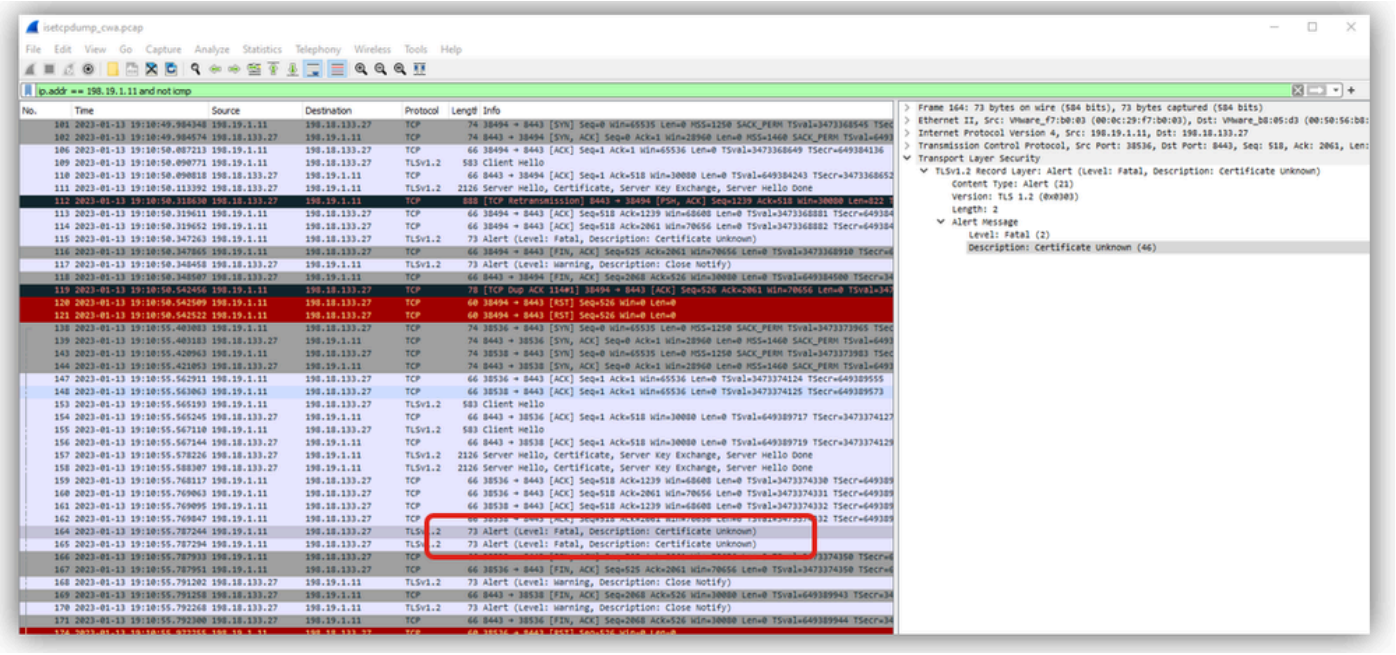
WLCおよびISEトラフィック

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ポータルの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。

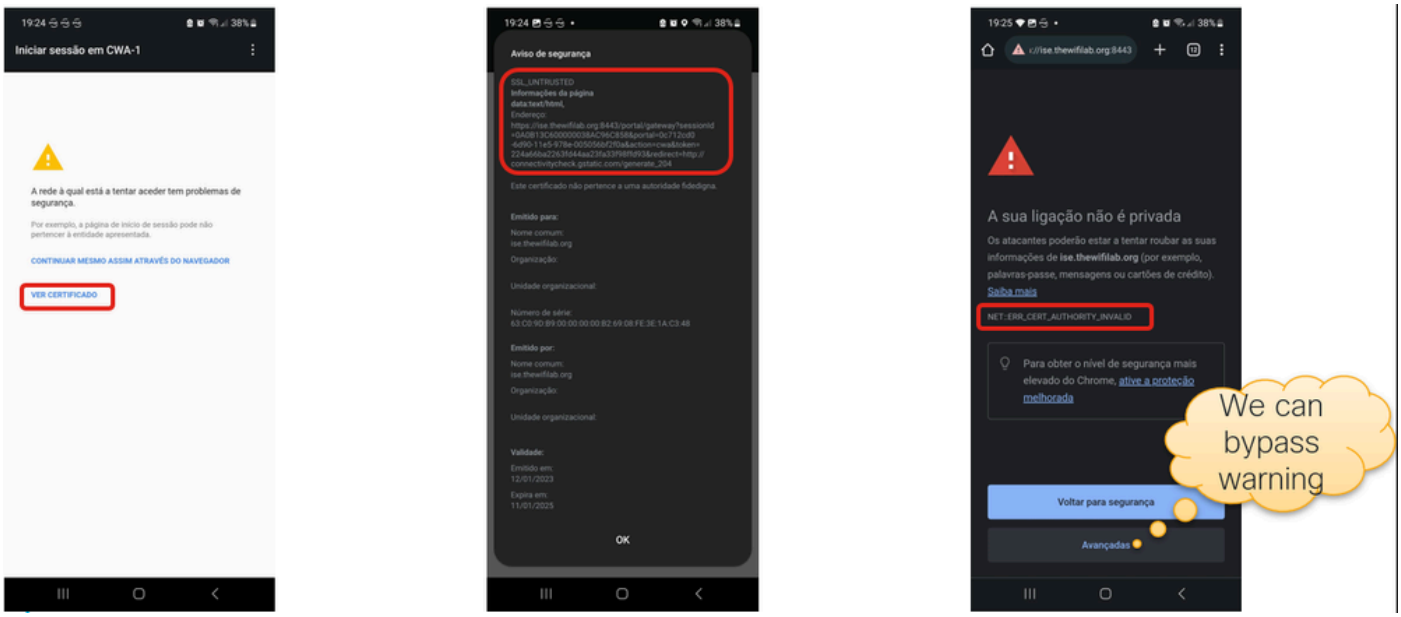
WLC EPCまたはISE TCPdumpで、ISE証明書が信頼できるかどうかを確認できます。

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

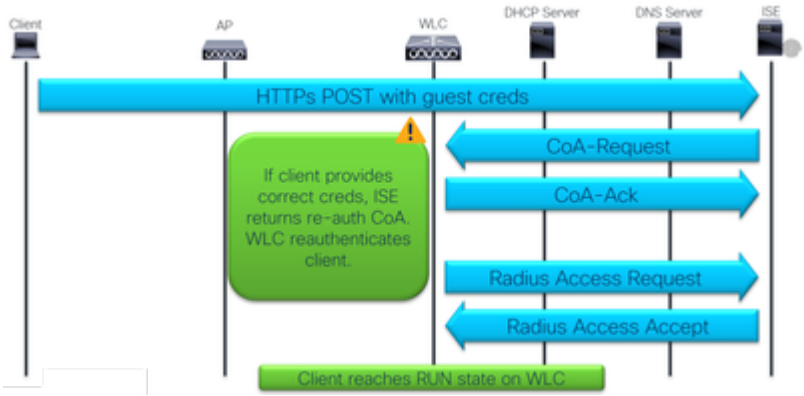
クライアント側で確認すると、次の出力例が表示されます。



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。

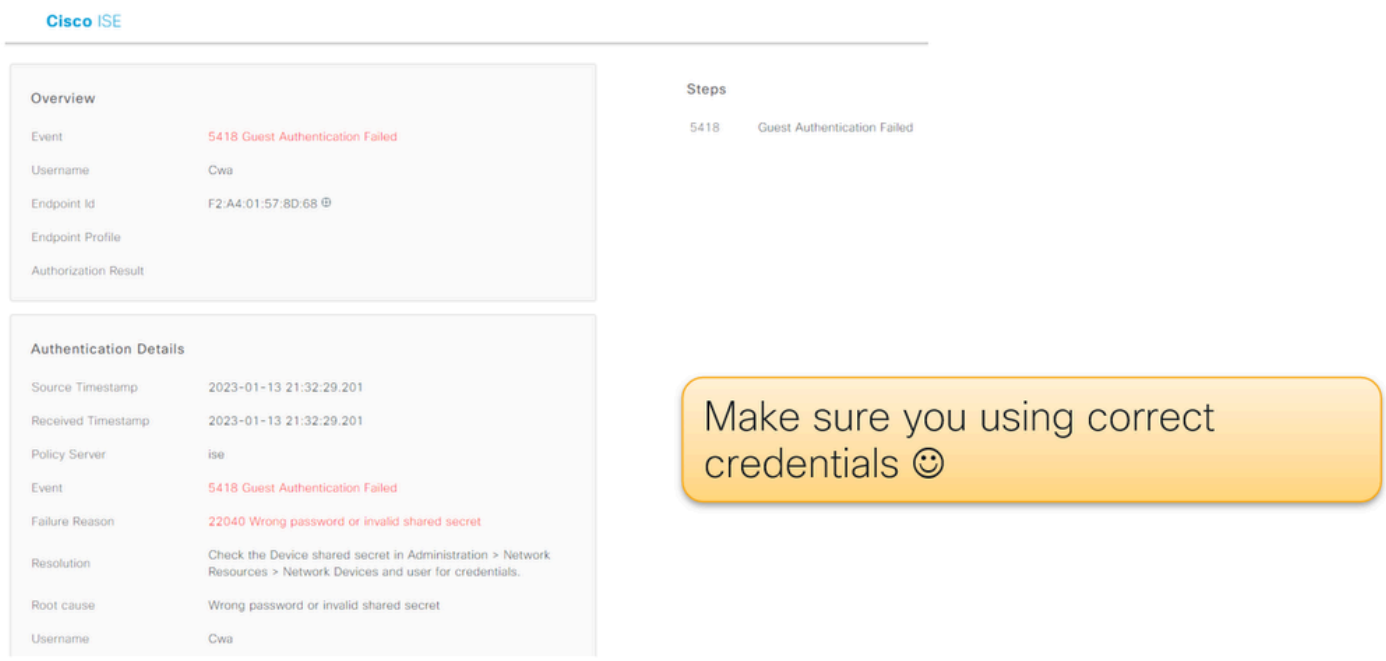
最後にもう1回フローを確認します。



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？

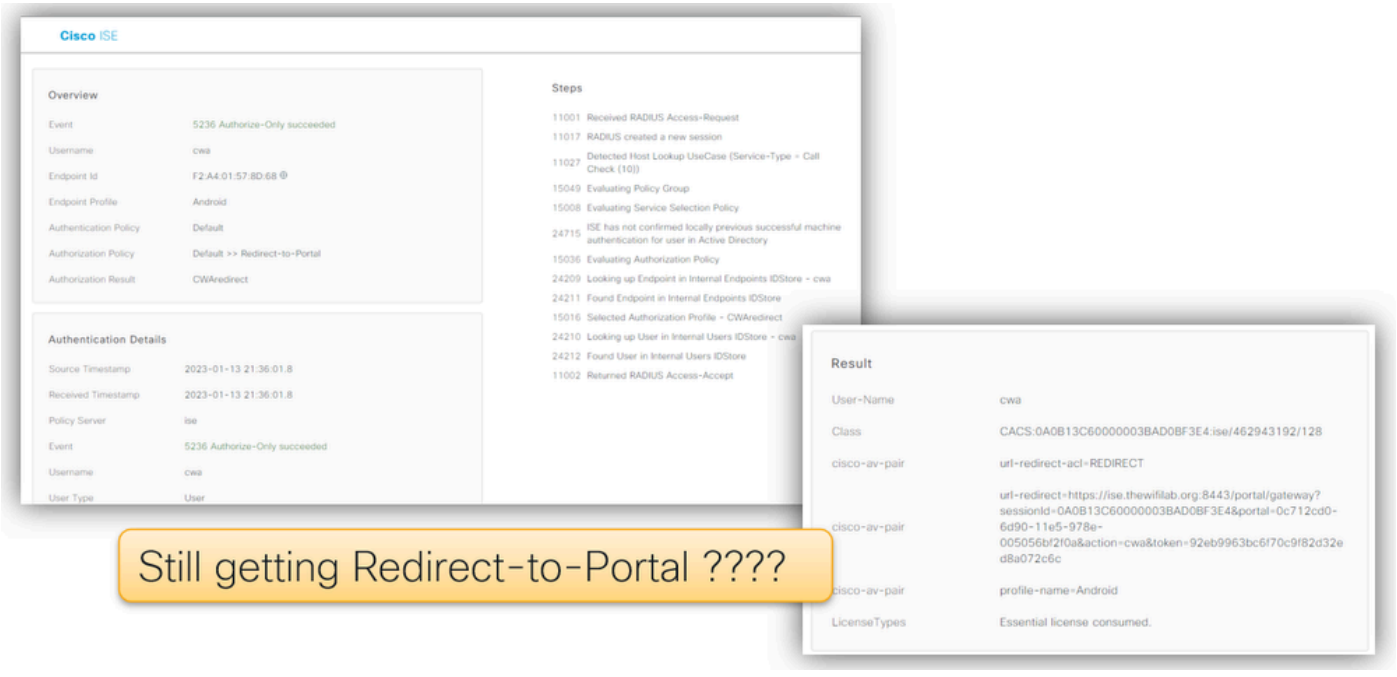
ISEログで認証の失敗を確認します。クレデンシャルが正しいことを確認します。



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？

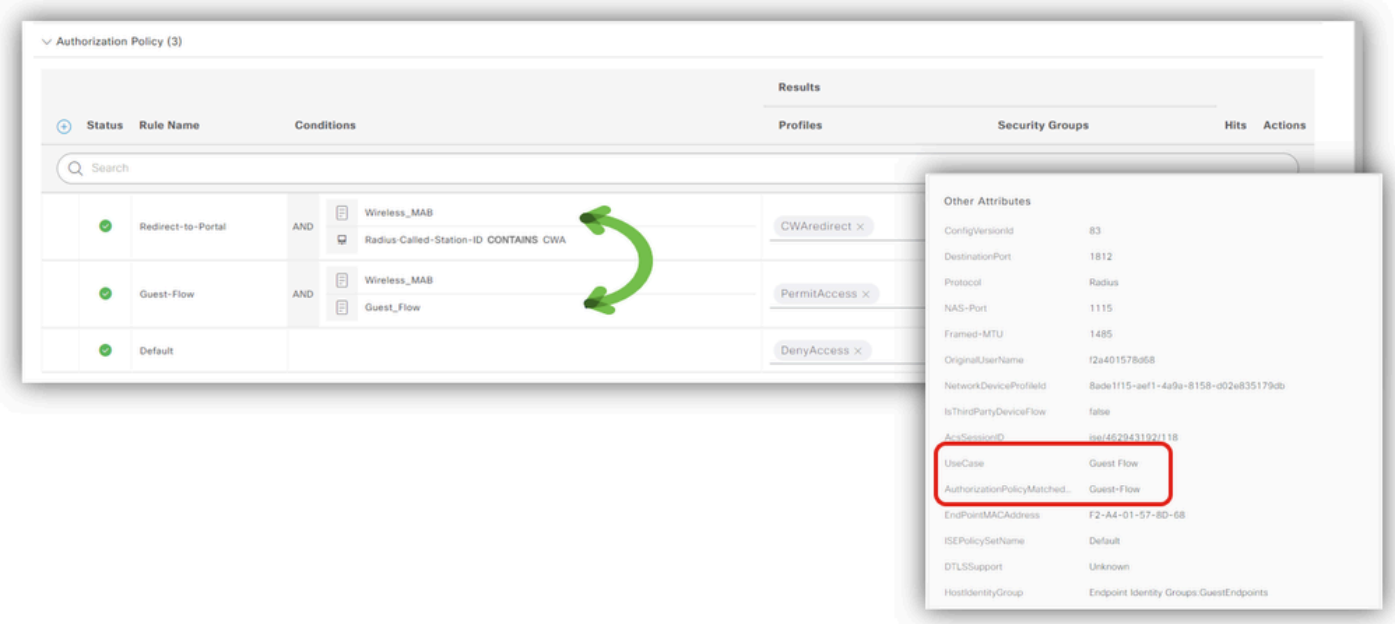
ISEログで認証の詳細と結果を確認します。



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。

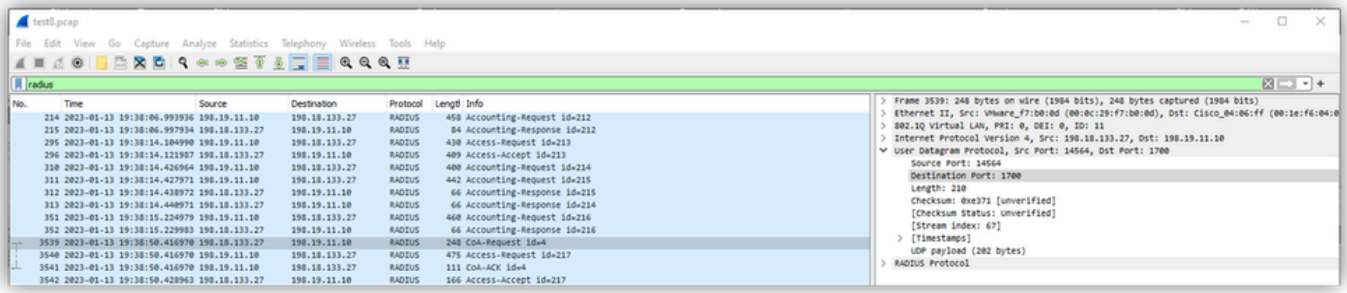
ポリシーセットを確認します。Guest_Flowのルールチェックは、リダイレクトの前に行う必要があります。



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。



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。