# Fehlerbehebung bei zentraler Webauthentifizierung (CWA) mit Wireless LAN Controller (WLC) 9800 und Identity Services Engine (ISE)

## Inhalt



## Einleitung

In diesem Dokument wird die Fehlerbehebung bei der zentralen Webauthentifizierung (CWA) mit dem WLC 9800 und der ISE beschrieben.

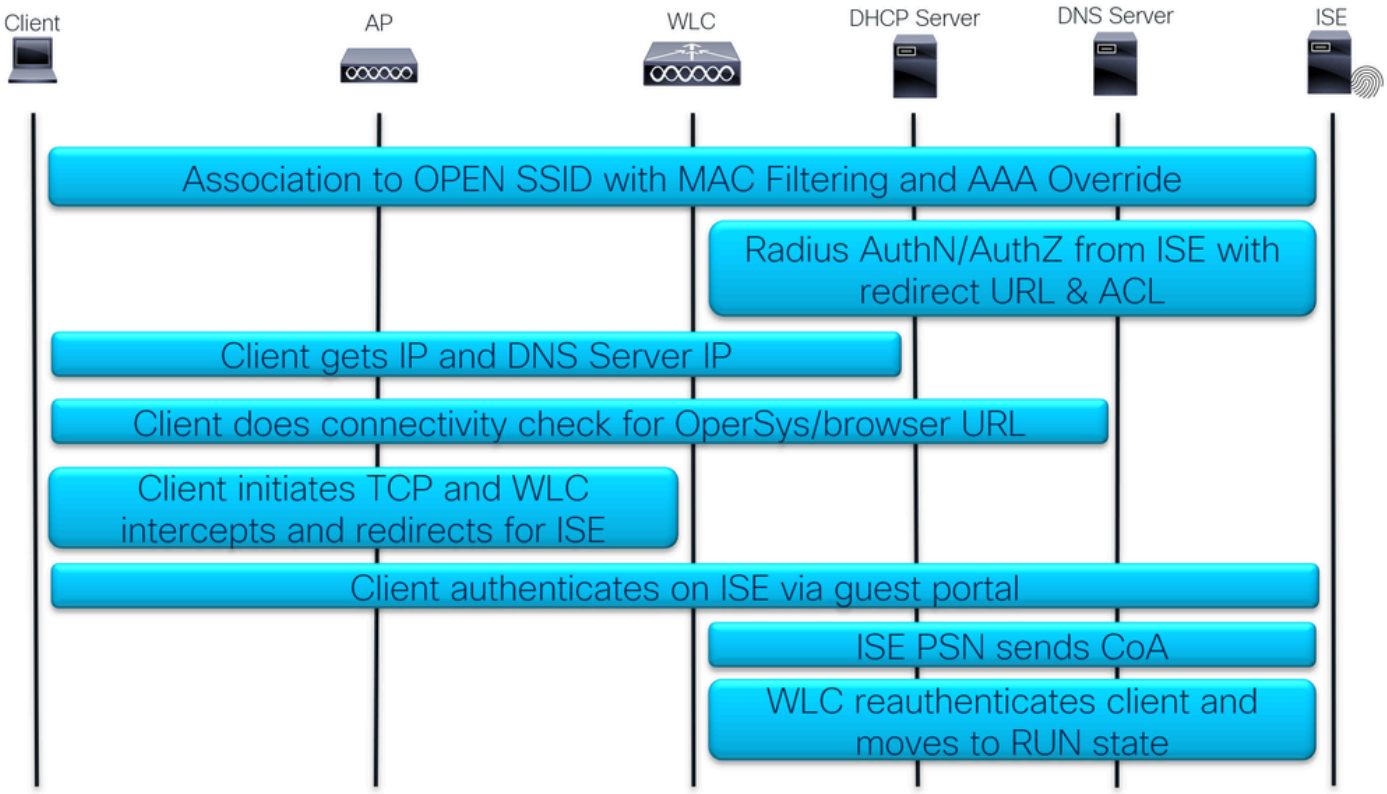
## Hintergrundinformationen

Es gibt derzeit so viele private Geräte, dass Netzwerkadministratoren, die den Wireless-Zugriff sichern möchten, sich normalerweise für Wireless-Netzwerke entscheiden, die CWA verwenden.
In diesem Dokument konzentrieren wir uns auf das Flussdiagramm von CWA, das bei der Fehlerbehebung von häufigen Problemen hilft, die uns betreffen.
Wir betrachten die allgemeinen Punkte des Prozesses, wie Protokolle im Zusammenhang mit dem CWA gesammelt werden, wie diese Protokolle analysiert werden und wie eine eingebettete

Paketerfassung auf dem WLC gesammelt wird, um den Datenverkehrsfluss zu bestätigen.

CWA ist die gängigste Konfiguration für Unternehmen, die Benutzern die Verbindung mit dem Unternehmensnetzwerk über ihre privaten Geräte, auch BYOD genannt, ermöglichen. Jeder Netzwerkadministrator ist an den erforderlichen Schritten zur Fehlerbehebung und -behebung interessiert, die er durchführen kann, um seine Probleme zu beheben, bevor er ein TAC-Ticket erstellt.

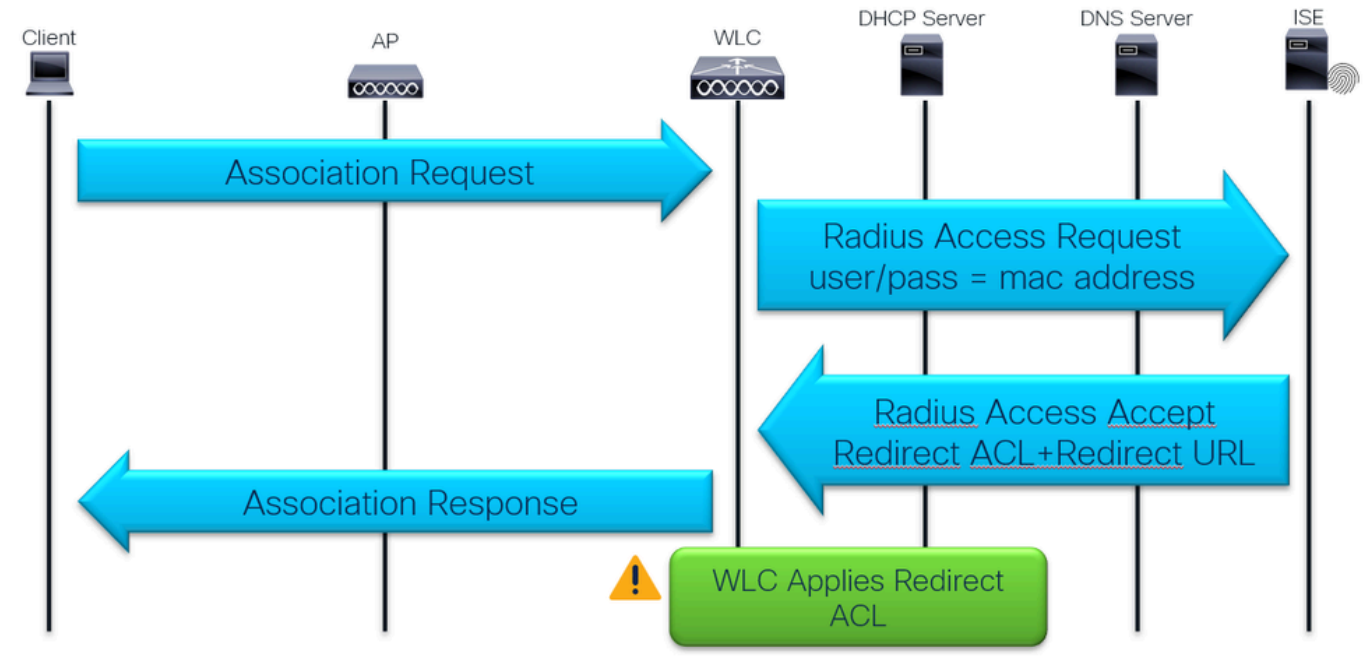
Dies ist der CWA-Paketfluss:




CWA-Paketfluss

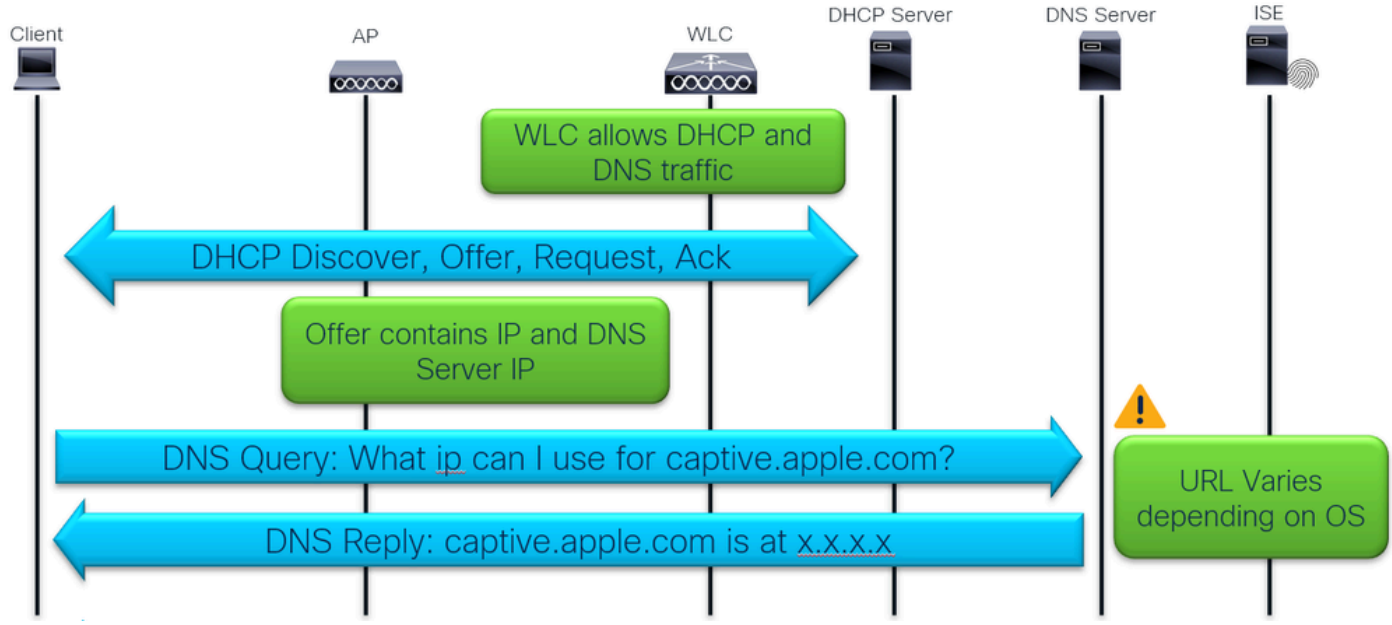
## Detaillierter Datenfluss

Erste Zuordnung und RADIUS-Authentifizierung:




Erste Zuordnung und RADIUS-Authentifizierung

DHCP, DNS und Verbindungsüberprüfung:




DHCP, DNS und Konnektivitätsprüfung

Die Konnektivitätsprüfung wird mithilfe der Captive Portal-Erkennung durch das Betriebssystem oder den Browser des Client-Geräts durchgeführt.

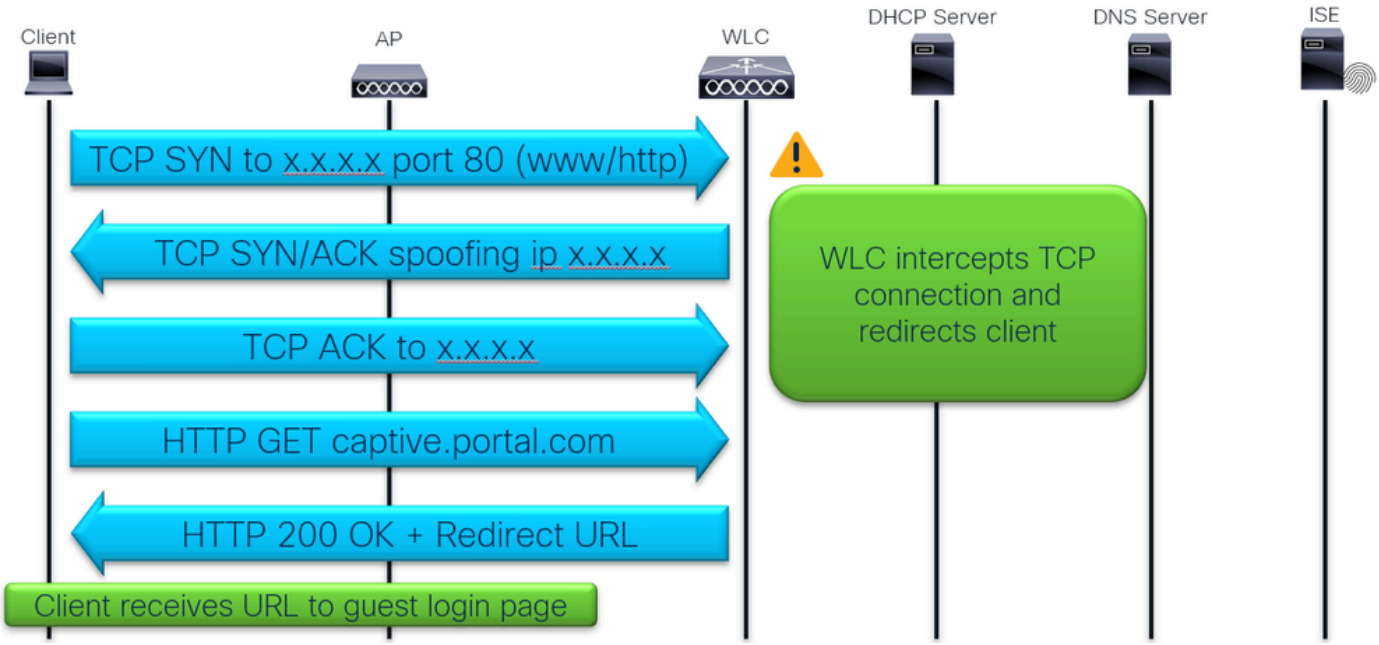
Es gibt ein Betriebssystem für Geräte, das für HTTP GET für eine bestimmte Domäne vorprogrammiert ist.

- Apple = captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnectest.com

Browser führen diese Prüfung auch beim Öffnen aus:

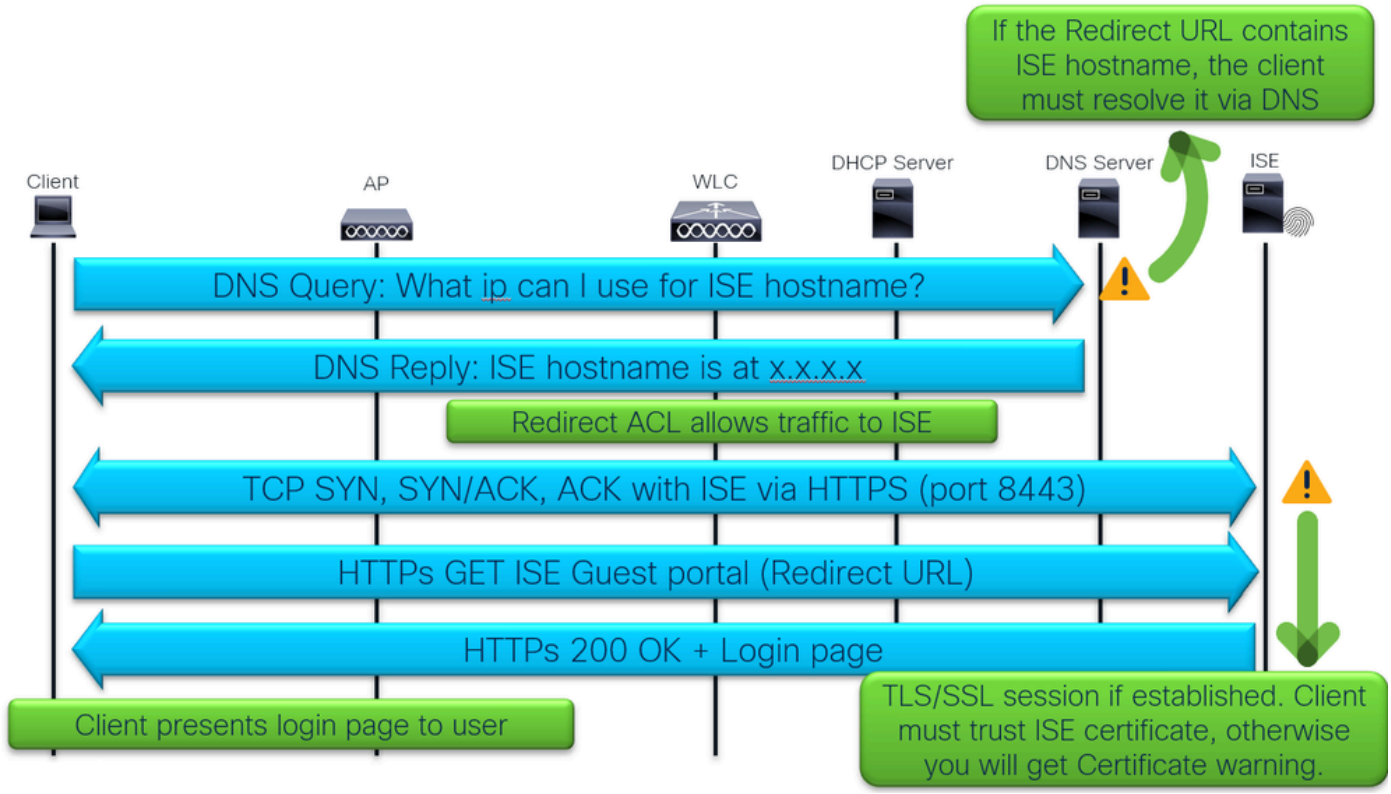
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Überwachung und Umleitung des Datenverkehrs:



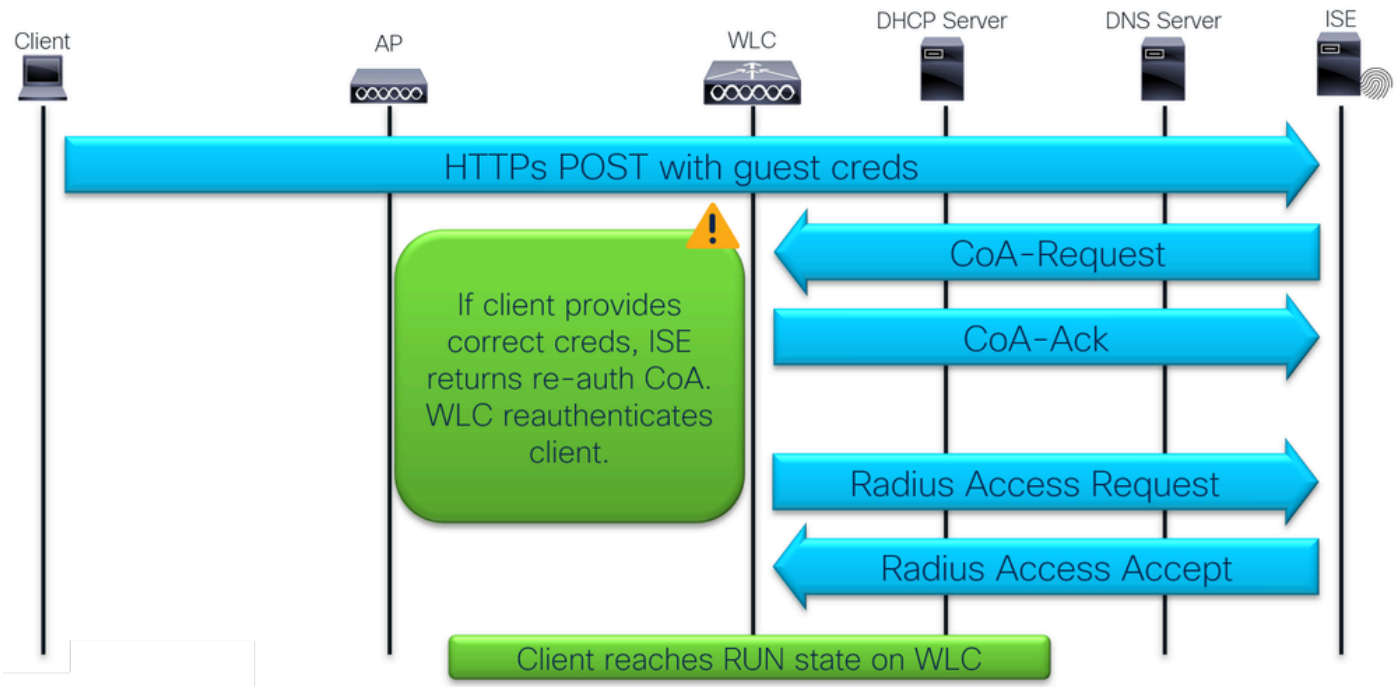

Überwachung und Weiterleitung des Datenverkehrs

Client-Anmeldung beim ISE-Gastanmeldeportal:




Client-Anmeldung beim ISE-Gastanmeldeportal

Client-Anmeldung und CoA:

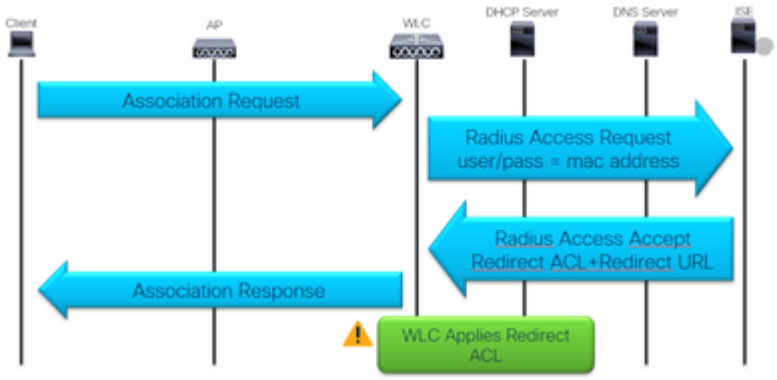



Client-Anmeldung und CoA

# Fehlerbehebung

## Häufige Symptome: Benutzer wird nicht zur Anmeldeseite weitergeleitet.

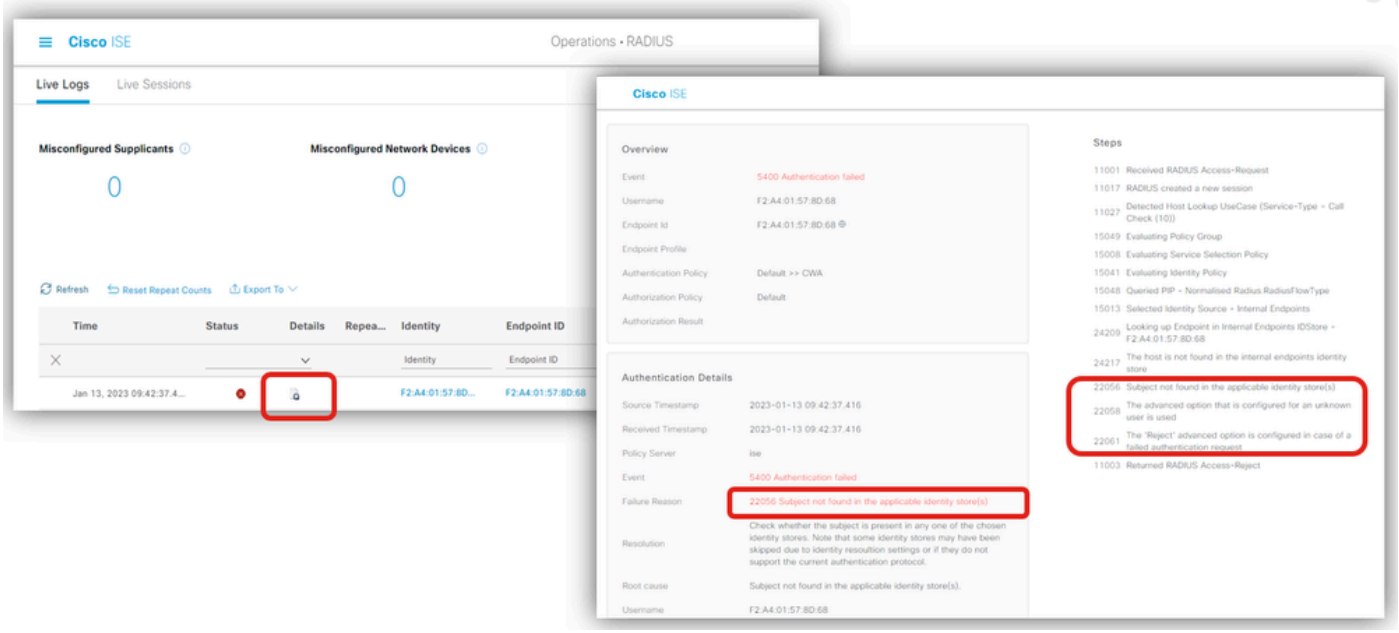
Beginnen wir mit dem ersten Teil des Flusses:




Erste Zuordnung und RADIUS-Authentifizierung

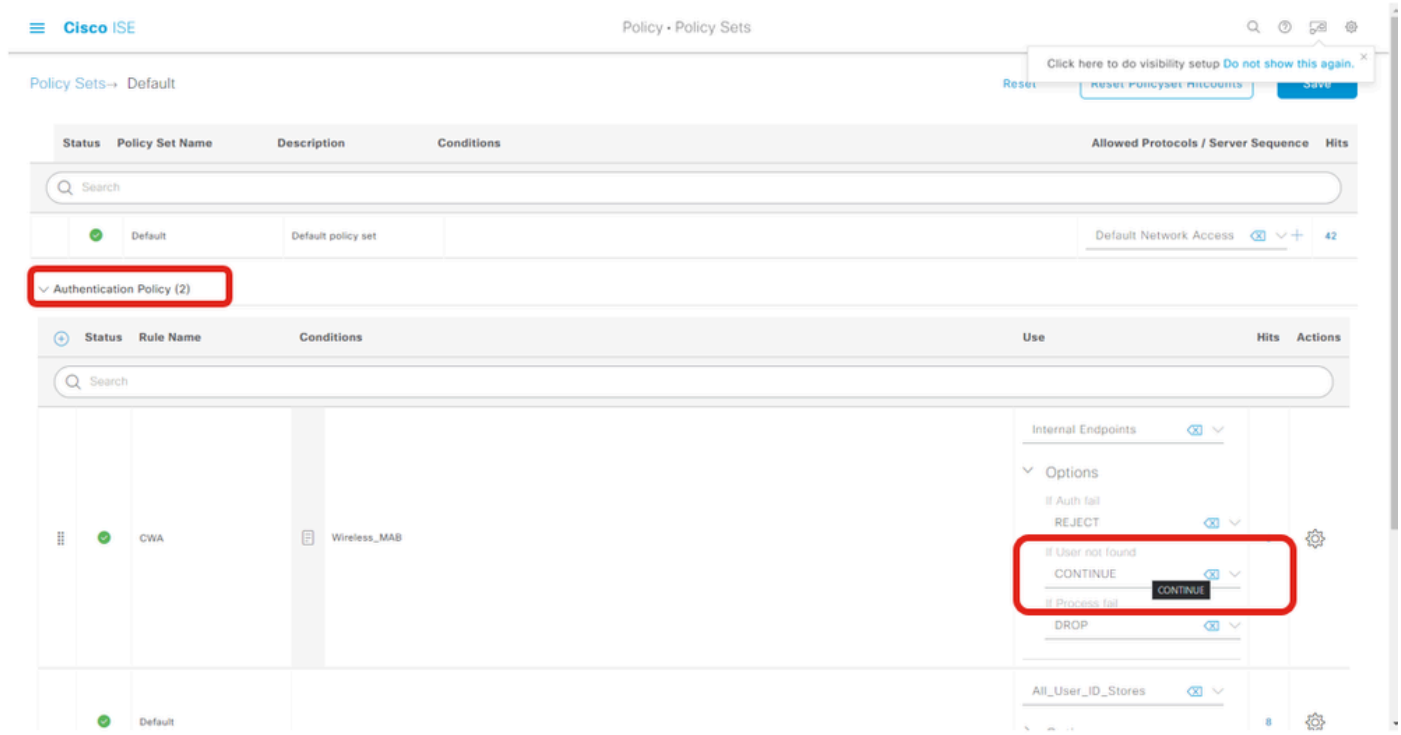
1 - Ist die erste RADIUS-Authentifizierung erfolgreich?

Ergebnis der MAC-Filterauthentifizierung überprüfen:




ISE-Live-Protokolle mit MAC-Filterauthentifizierungsergebnis

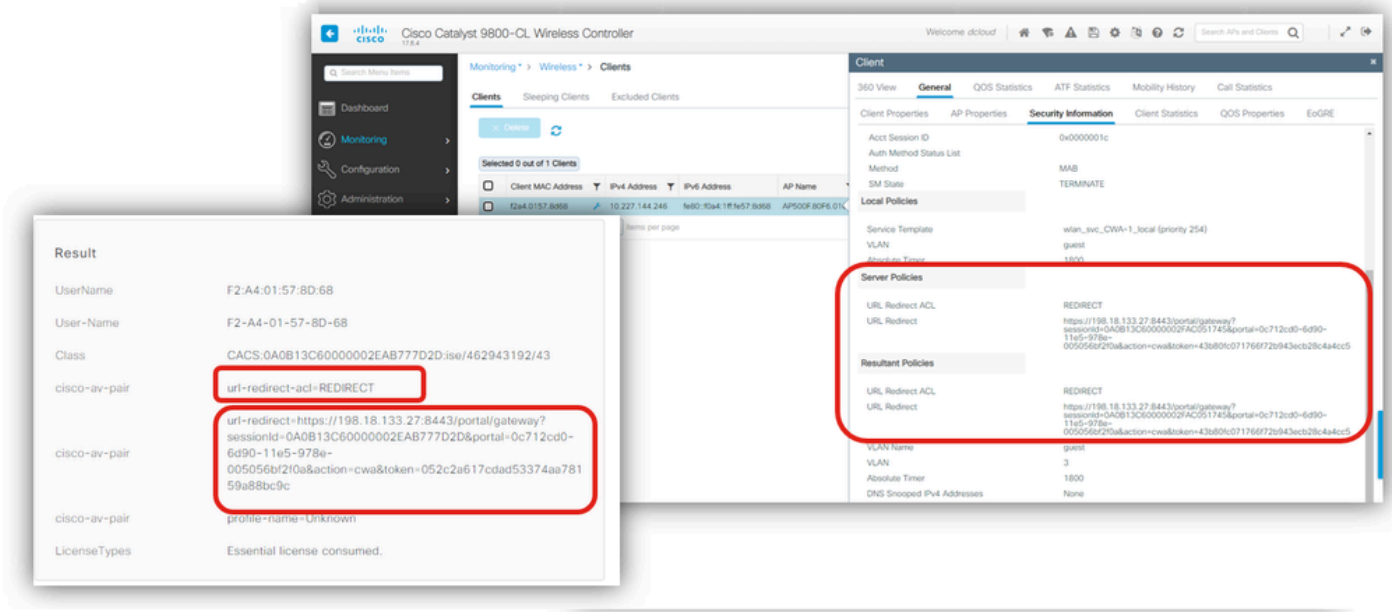
Stellen Sie sicher, dass die erweiterte Option für die Authentifizierung auf "Weiter" gesetzt ist, wenn der Benutzer nicht gefunden wurde:




Erweiterte Option wurde nicht gefunden

2 - WLC empfängt die URL und ACL für die Umleitung?

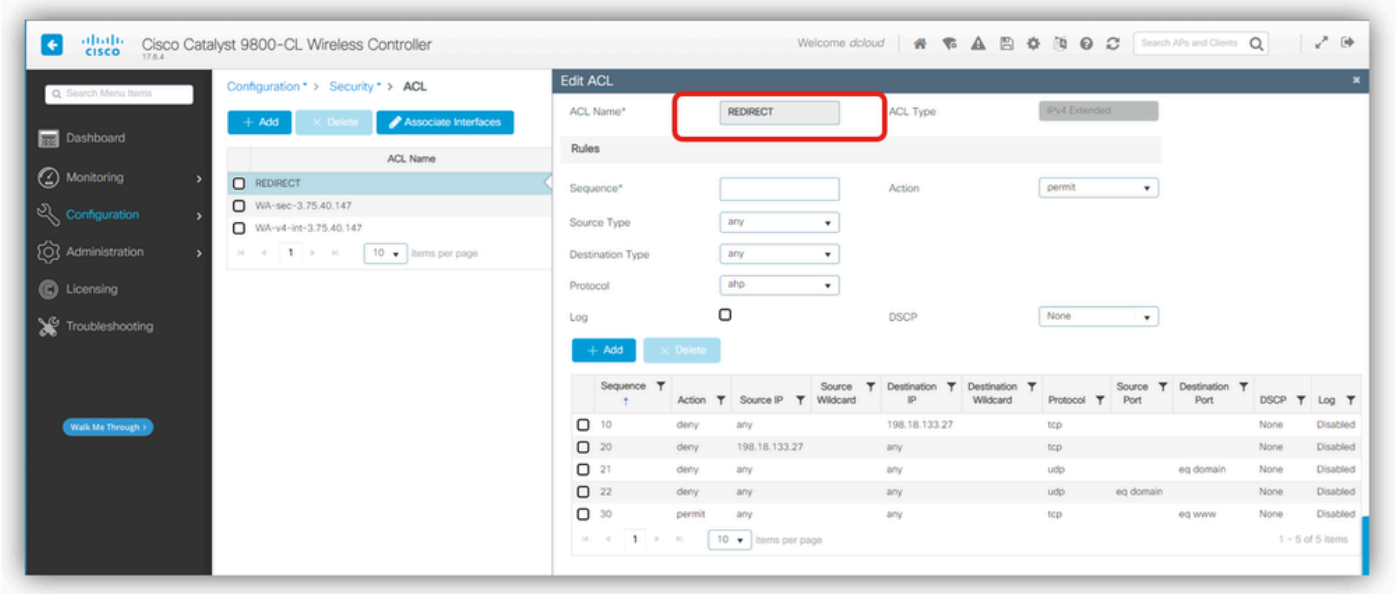
Überprüfen Sie die ISE-Live-Protokolle und die WLC-Client-Sicherheitsinformationen unter Überwachung. Überprüfen Sie, ob die ISE eine Umleitungs-URL und ACL im Access Accept sendet und diese vom WLC empfangen und in den Client-Details auf den Client angewendet werden:




ACL und URL umleiten

3 - Ist die Umleitungszugriffskontrollliste korrekt?

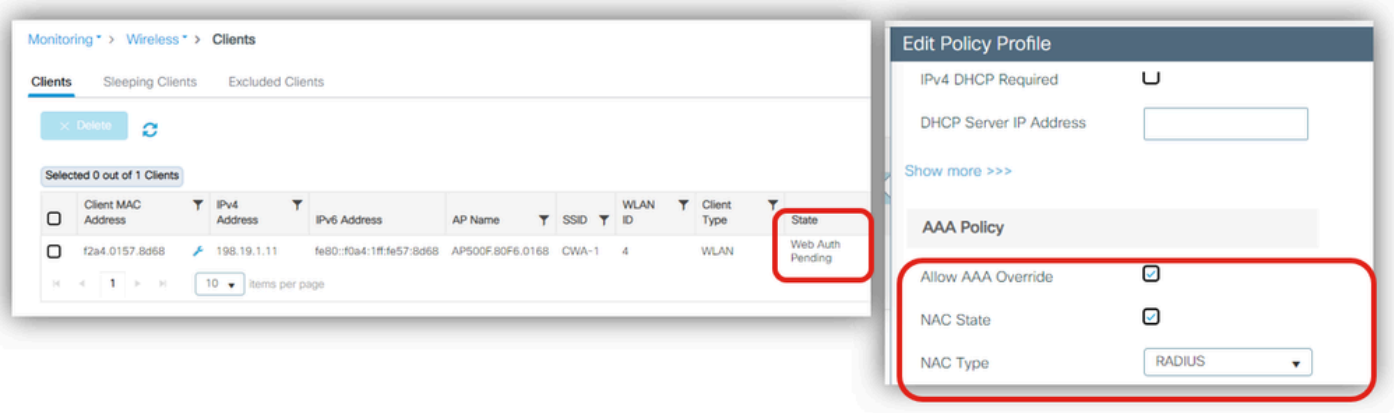
Überprüfen Sie den ACL-Namen für einen beliebigen Tippfehler. Vergewissern Sie sich, dass es genau so ist, wie es von der ISE gesendet wurde:




ACL-Überprüfung umleiten

4 - Wird der Client auf Web-Auth Pending (Webauthentifizierung ausstehend) verschoben?

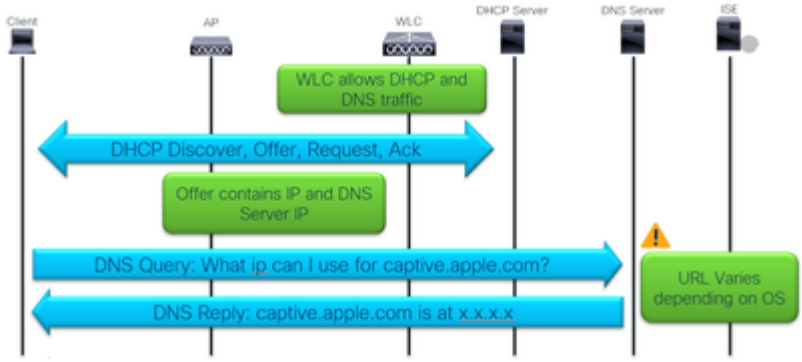
Überprüfen Sie die Clientdetails auf den Status "Webauthentifizierung ausstehend". Wenn sich der Status nicht in diesem Zustand befindet, überprüfen Sie, ob AAA override und Radius NAC im Richtlinienprofil aktiviert sind:




Client-Details, aaa override und RADIUS NAC

Funktioniert es immer noch nicht?

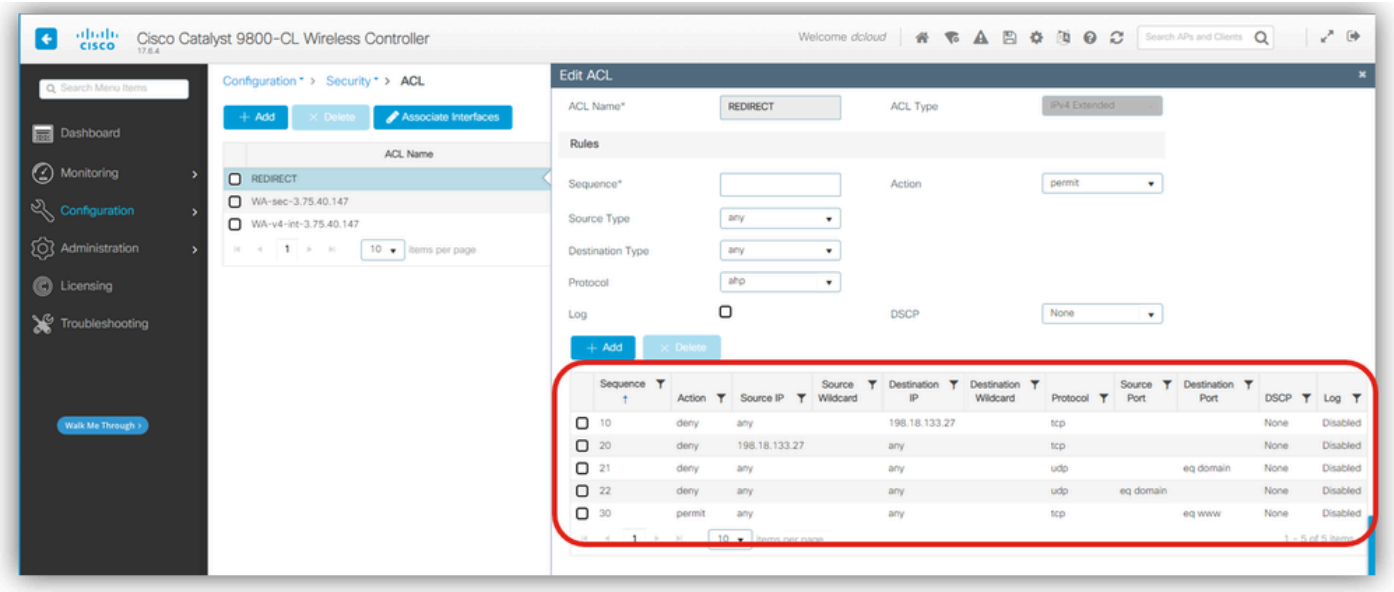
Sehen wir uns nun den Ablauf noch einmal an ...




DHCP, DNS und Konnektivitätsprüfung

5 - Lässt WLC DHCP- und DNS-Datenverkehr zu?

Überprüfen Sie den Inhalt der Umleitungszugriffskontrollliste im WLC:




ACL-Inhalte im WLC umleiten

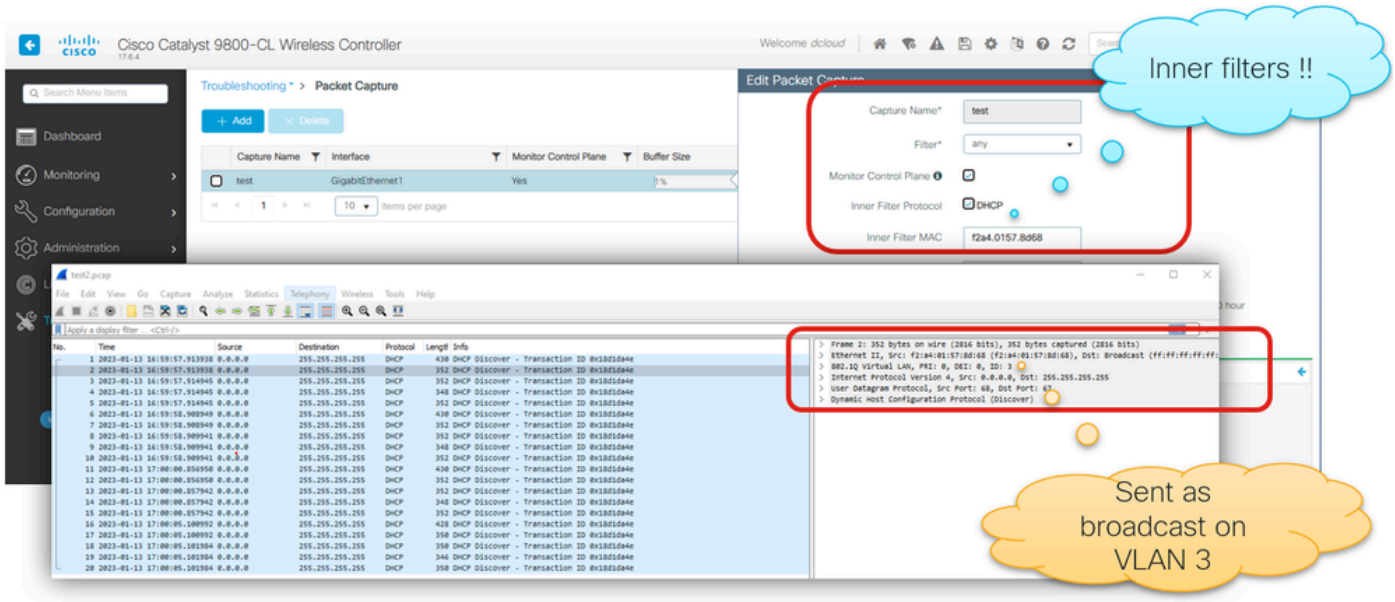
Die Umleitungs-ACL definiert, welcher Datenverkehr von der permit-Anweisung abgefangen und umgeleitet wird und welcher Datenverkehr von der Interception und Umleitung mit einer deny-Anweisung ignoriert wird.

In diesem Beispiel lassen wir zu, dass DNS- und Datenverkehr zu/von der ISE-IP-Adresse fließt, und unterbrechen den TCP-Datenverkehr auf Port 80 (www).

6 - Empfängt der DHCP-Server eine DHCP-Erkennung/Anforderung?

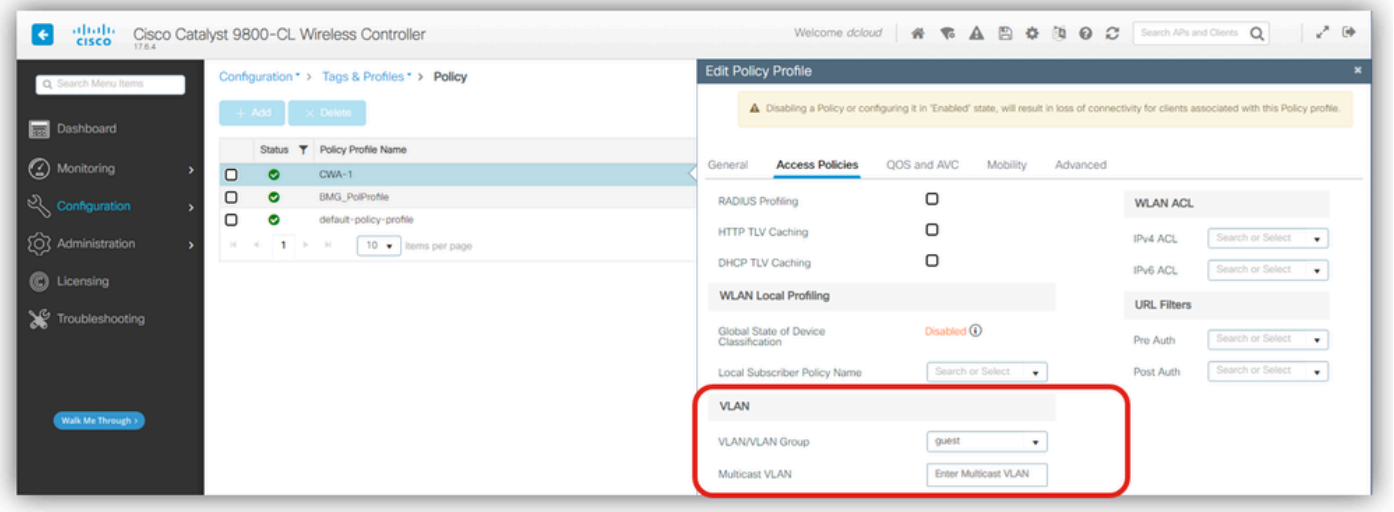
Mit EPC überprüfen, ob DHCP-Austausch erfolgt. EPC kann mit internen Filtern wie dem DHCP-Protokoll und/oder der inneren Filter-MAC-Adresse verwendet werden, wobei die MAC-Adresse des Client-Geräts verwendet werden kann und nur DHCP-Pakete vom EPC gesendet oder an die MAC-Adresse des Client-Geräts gesendet werden.

In diesem Beispiel werden die DHCP Discover-Pakete angezeigt, die als Broadcast über VLAN 3 gesendet wurden:



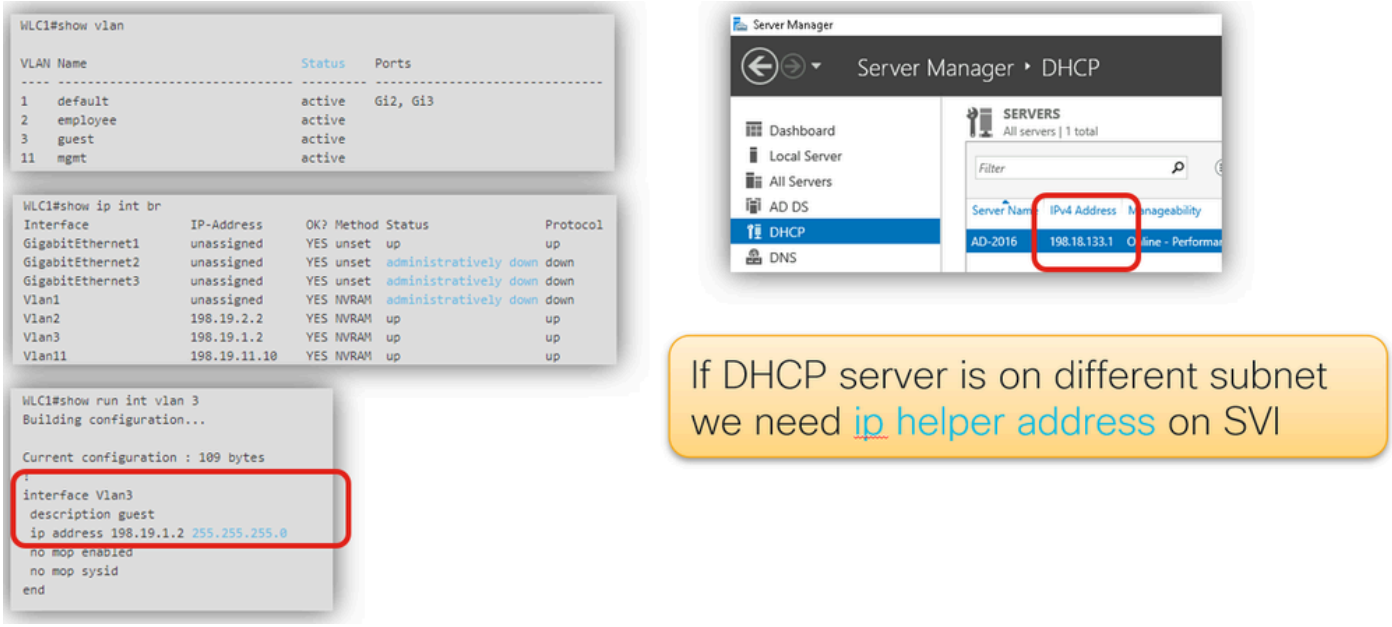

WLC-EPC zur DHCP-Verifizierung

Bestätigen Sie das erwartete Client-VLAN im Richtlinienprofil:



VLAN im Richtlinienprofil

Überprüfen der WLC-VLAN- und Switch-Port-Trunk-Konfiguration und des DHCP-Subnetzes



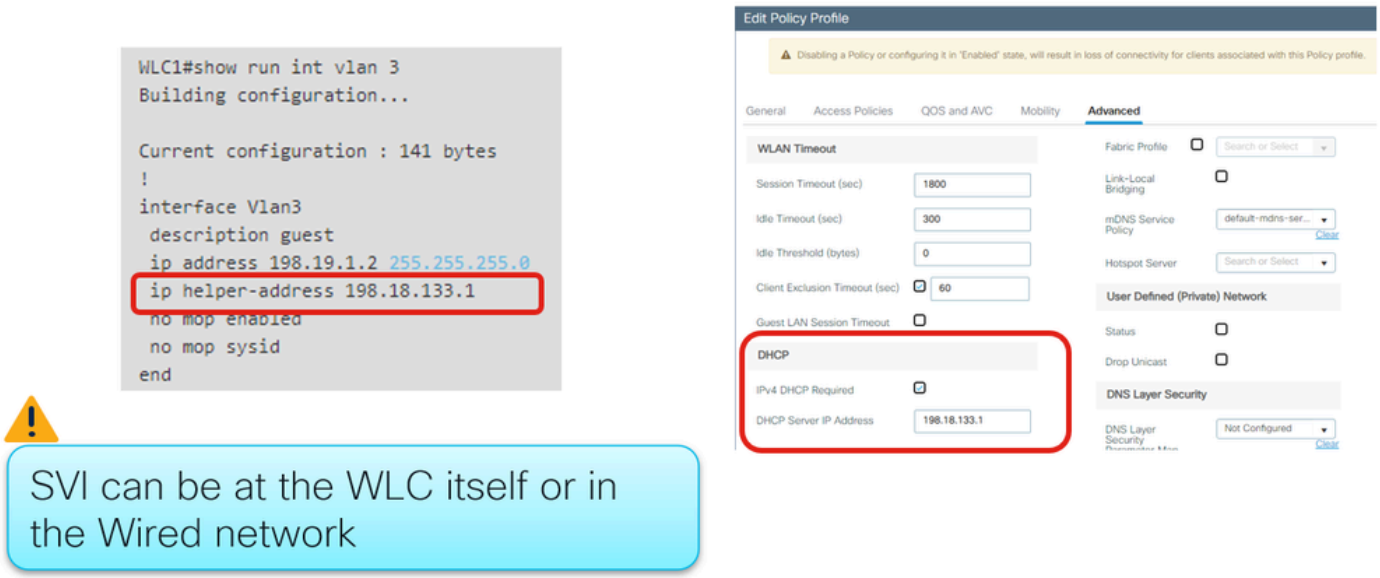

VLAN, Switch-Port und DHCP-Subnetz

Wie wir sehen können, ist VLAN 3 im WLC vorhanden und verfügt auch über SVI für VLAN 3. Wenn wir jedoch die IP-Adresse des DHCP-Servers in einem anderen Subnetz überprüfen, benötigen wir die IP Helper-Adresse auf der SVI.

Best Practices schreiben vor, dass SVI für Client-Subnetze in der kabelgebundenen Infrastruktur konfiguriert werden muss, um sie am WLC zu vermeiden.

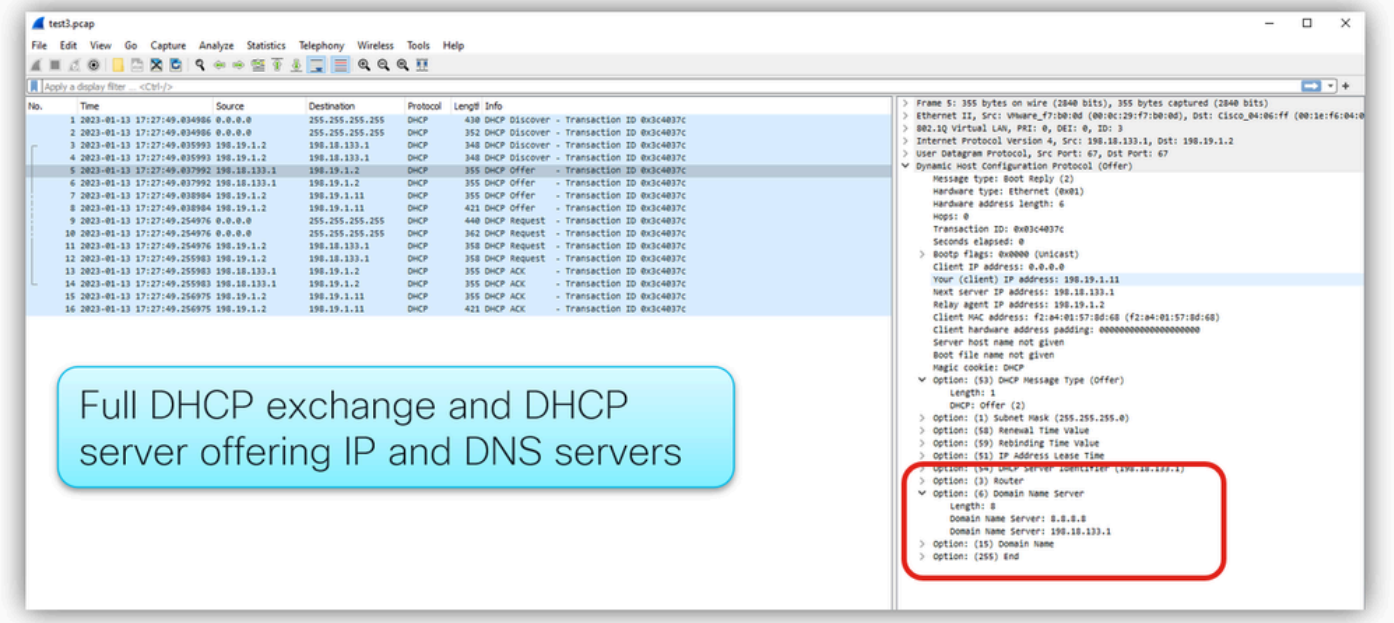
In allen Fällen muss der Befehl ip helper-address zur SVI hinzugefügt werden, unabhängig davon, wo sich diese befindet.

Eine Alternative besteht darin, die IP-Adresse des DHCP-Servers im Richtlinienprofil zu konfigurieren:



IP-Hilfsadresse bei SVI oder Richtlinienprofil

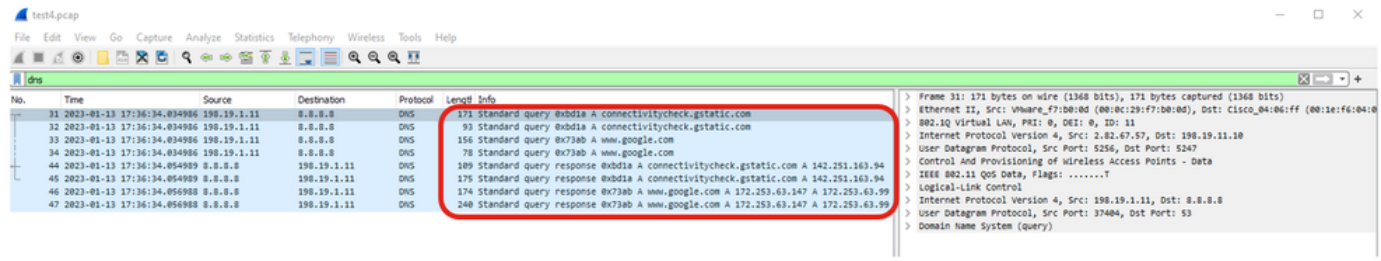
Anschließend können Sie mit EPC überprüfen, ob der DHCP-Austausch jetzt in Ordnung ist und ob der DHCP-Server eine oder mehrere DNS-Server-IP(s) bereitstellt:




DHCP-Angebotsdetails der DNS-Server-IP

7 - Wird die automatische Umleitung durchgeführt?

Mit WLC EPC überprüfen, ob der DNS-Server Abfragen beantwortet:

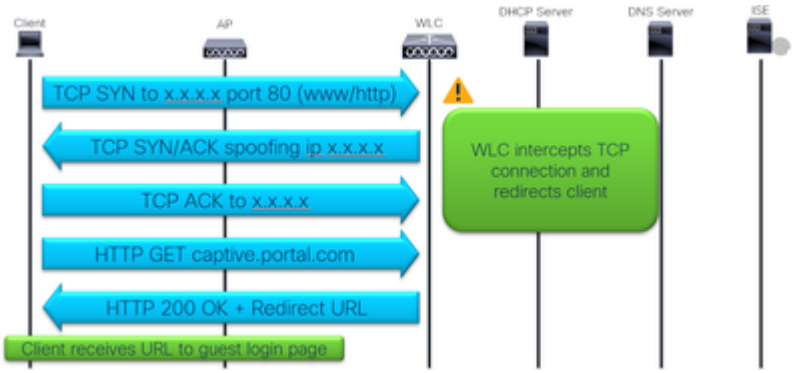


DNS-Abfrage und -Antworten

- Wenn die Umleitung nicht automatisch erfolgt, öffnen Sie einen Browser, und versuchen Sie eine zufällige IP-Adresse. Beispiel: 10.0.0.1.
- Wenn die Umleitung dann funktioniert, ist es möglich, dass Sie ein DNS-Auflösungsproblem haben.

Funktioniert es immer noch nicht?

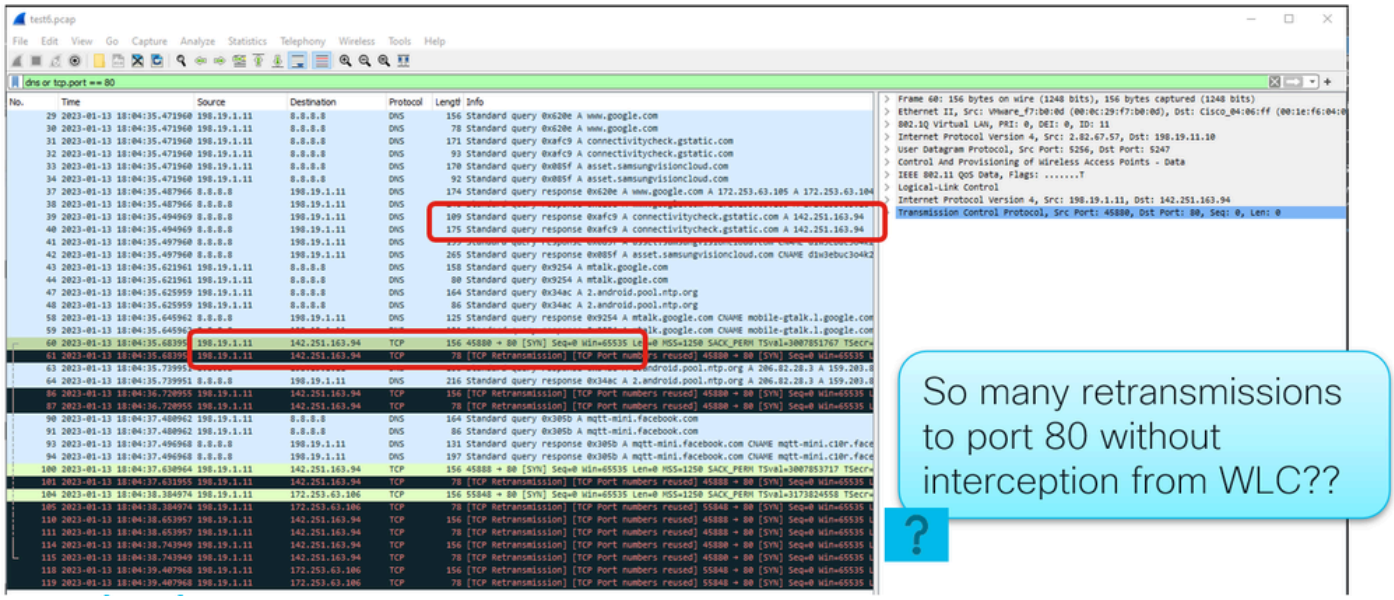
Sehen wir uns nun den Ablauf noch einmal an ...




Überwachung und Weiterleitung des Datenverkehrs

8 - Im Browser wird keine Anmeldeseite angezeigt?

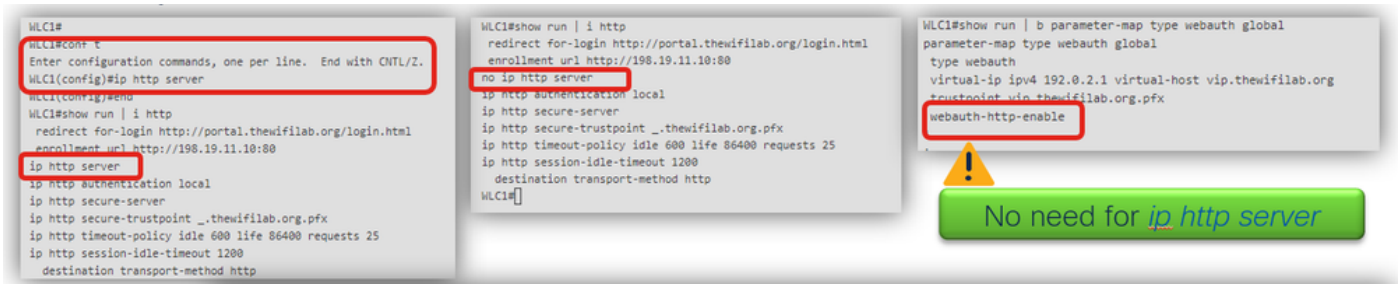
Überprüfen Sie, ob der Client das TCP-SYN an Port 80 sendet und der WLC es abfängt:




TCP-Neuübertragungen an Port 80

Hier können wir sehen, dass der Client TCP SYN Pakete an Port 80 sendet, aber keine Antwort erhält und TCP erneut sendet.

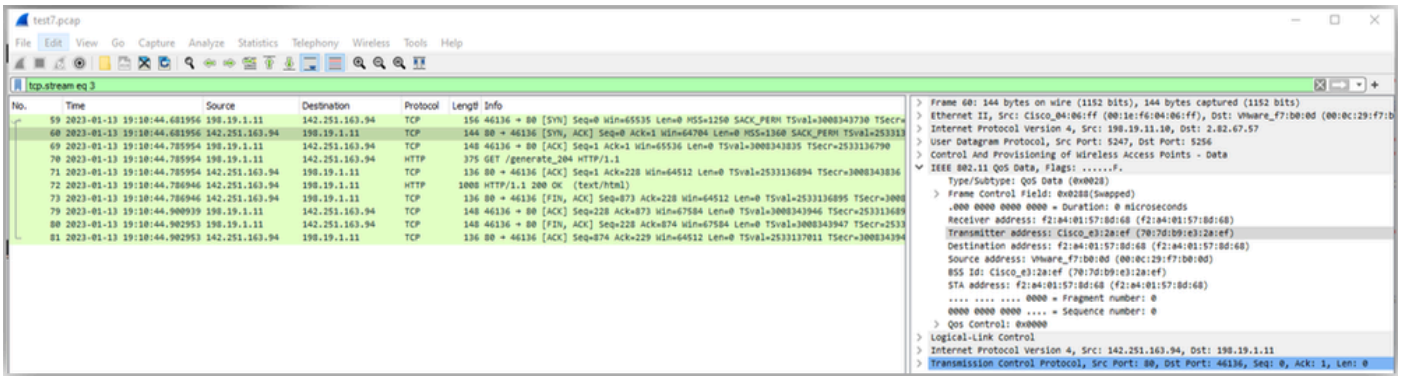
Vergewissern Sie sich, dass der Befehl ip http server in der globalen Konfiguration oder webauth-http-enable in der globalen Parameterzuordnung vorhanden ist:




HTTP-Interception-Befehle

Nach dem Befehl fängt der WLC das TCP ab und sendet Spoofs an die Ziel-IP-Adresse, um dem

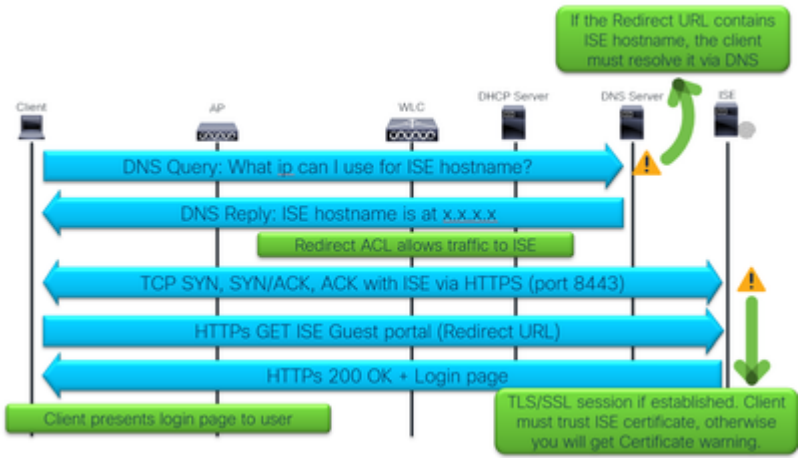
Client zu antworten und eine Umleitung vorzunehmen.



TCP-Abfangen durch WLC

Funktioniert es immer noch nicht?

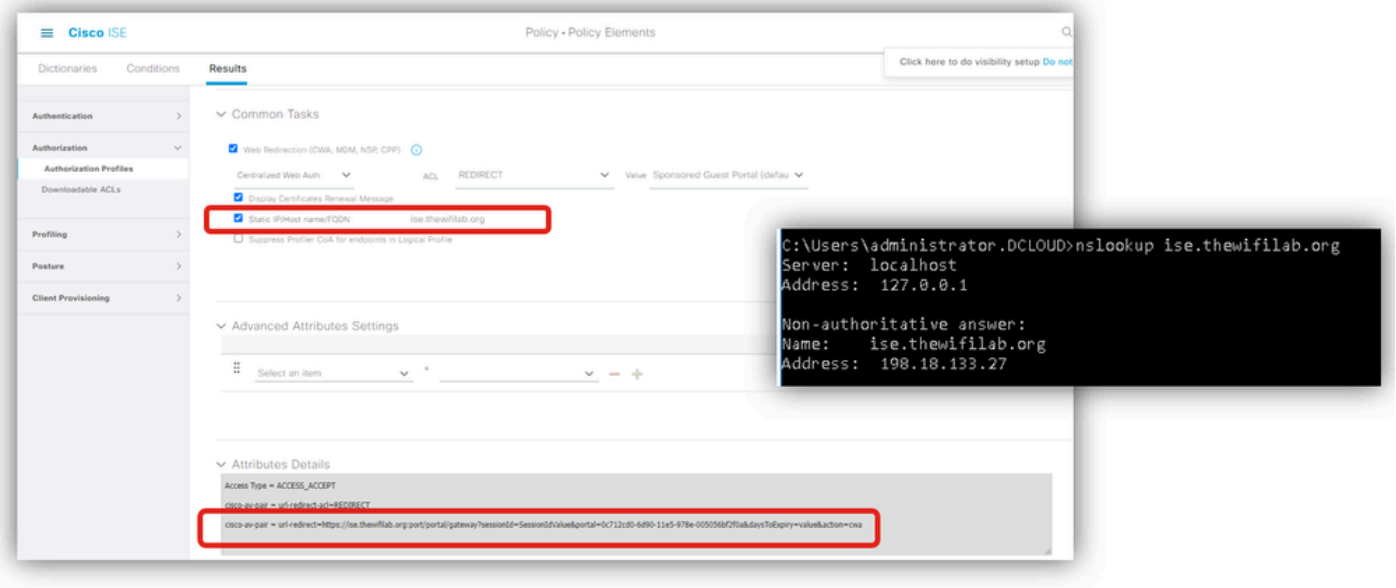
Es ist mehr im Fluss...




Client-Anmeldung beim ISE-Gastanmeldeportal

9 - Kann der Client den ISE-Hostnamen auflösen?

Überprüfen Sie, ob die Umleitungs-URL IP oder Hostnamen verwendet und ob der Client den ISE-Hostnamen auflöst:

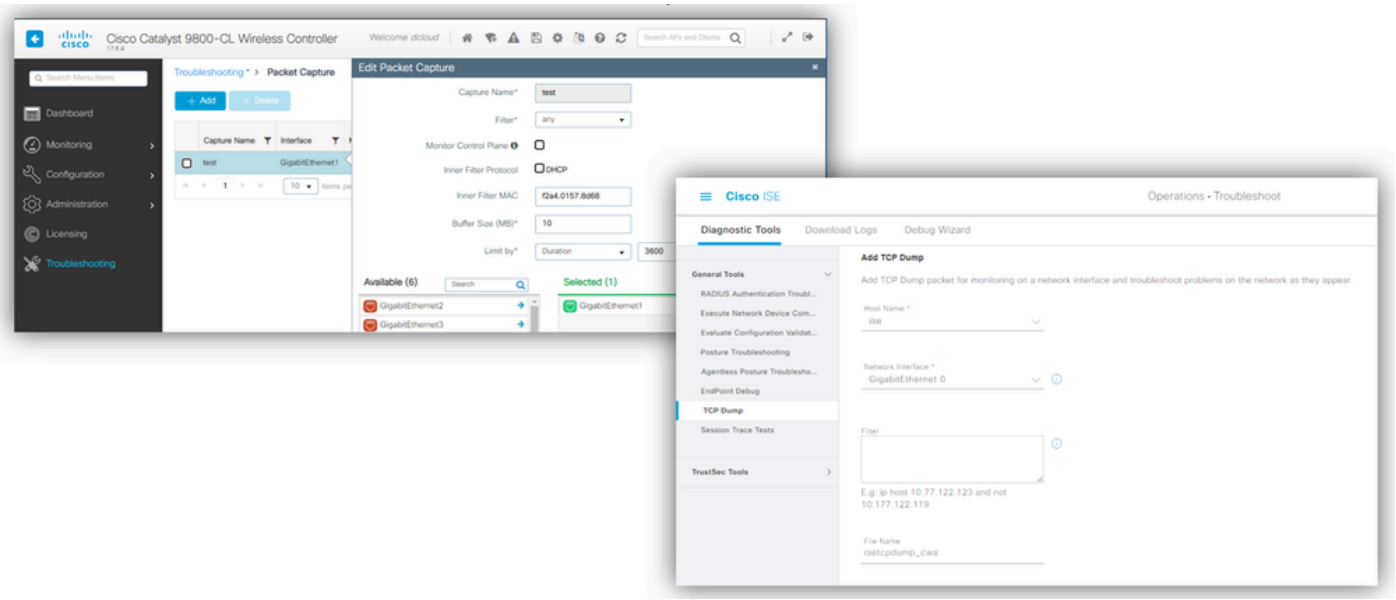



ISE-Hostnamenauflösung

Ein häufiges Problem tritt auf, wenn die Umleitungs-URL den ISE-Hostnamen enthält. Das Client-Gerät kann diesen Hostnamen jedoch nicht in die ISE-IP-Adresse auflösen. Wenn ein Hostname verwendet wird, stellen Sie sicher, dass dieser über DNS aufgelöst werden kann.

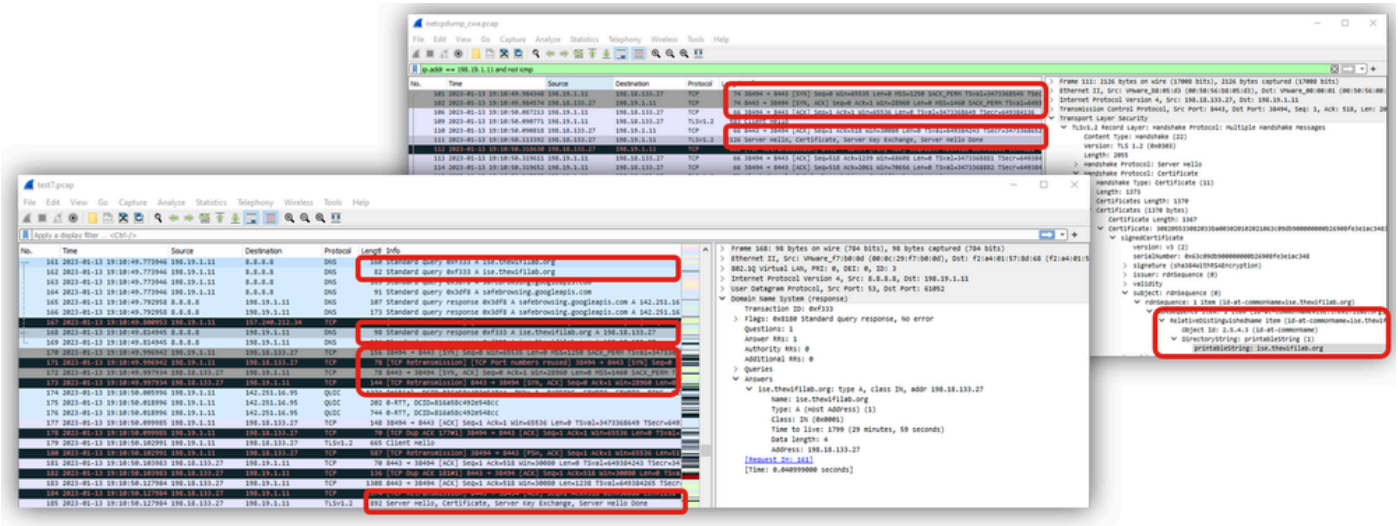
10 - Login-Seite immer noch nicht geladen?

Überprüfen Sie dies mit WLC EPC und ISE TCPdump, wenn der Client-Datenverkehr ISE PSN erreicht. Konfigurieren und Initiieren der Erfassungen auf WLC und ISE:




WLC EPC und ISE TCPDump

Erfassen Sie nach der Problemwiedergabe die erfassten Daten, und korrelieren Sie den Datenverkehr. Hier sehen wir den aufgelösten ISE-Hostnamen und dann die Kommunikation zwischen Client und ISE auf Port 8443:



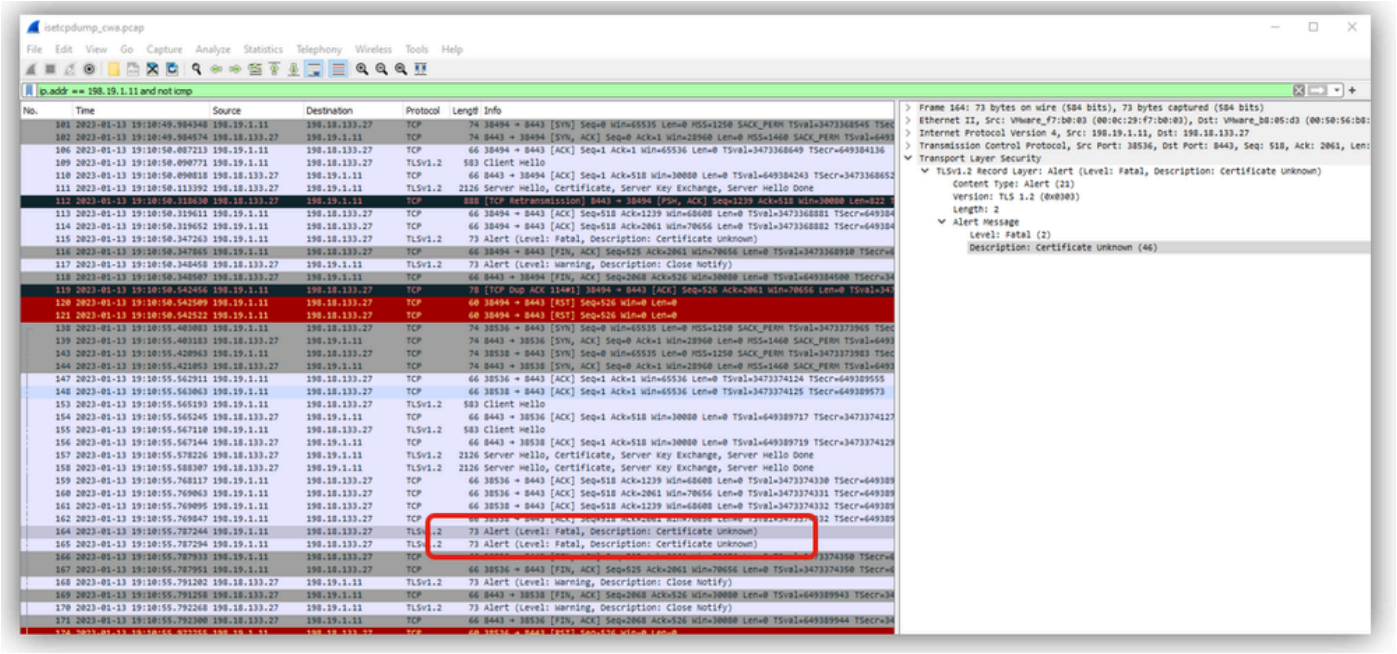
WLC- und ISE-Verkehr

11 - Warum wird die Sicherheit durch das Zertifikat verletzt?

Wenn Sie ein selbstsigniertes Zertifikat auf der ISE verwenden, wird erwartet, dass der Client eine Sicherheitswarnung ausgibt, wenn er versucht, die Anmeldeseite des ISE-Portals anzuzeigen.

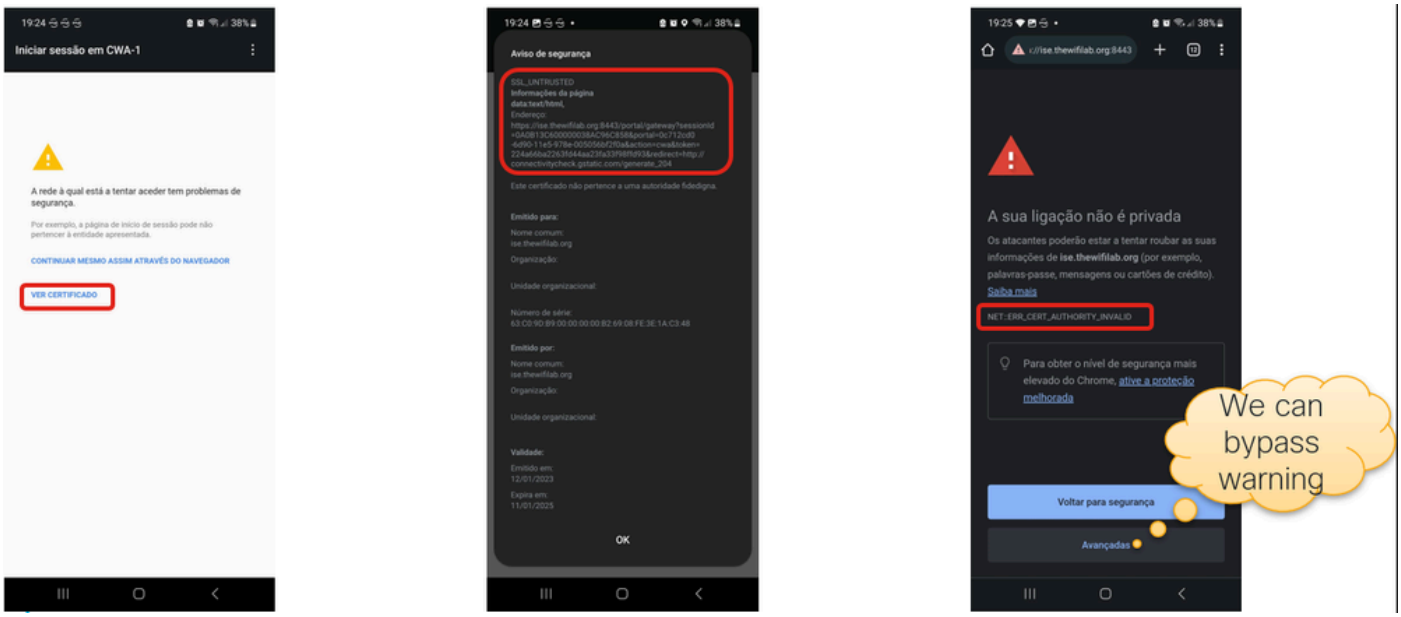
Auf dem WLC EPC oder ISE TCPdump können wir überprüfen, ob das ISE-Zertifikat vertrauenswürdig ist.

In diesem Beispiel sehen wir die Verbindung schließen vom Client mit Alert (Level: Fatal, Beschreibung: certificate Unknown), was bedeutet, dass das ISE-Zertifikat nicht bekannt ist (Trusted):



Nicht vertrauenswürdiges ISE-Zertifikat

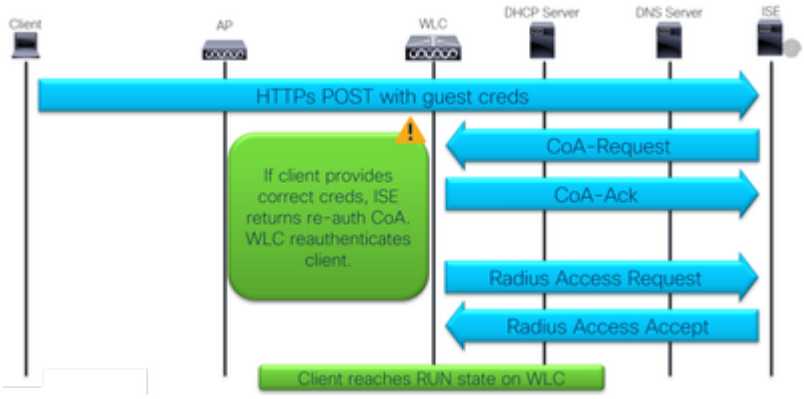
Wenn wir auf der Client-Seite überprüfen, sehen wir diese Beispielausgabe:




Client-Gerät, das dem ISE-Zertifikat nicht vertraut

Die Umleitung funktioniert!! Die Anmeldung schlägt fehl ...

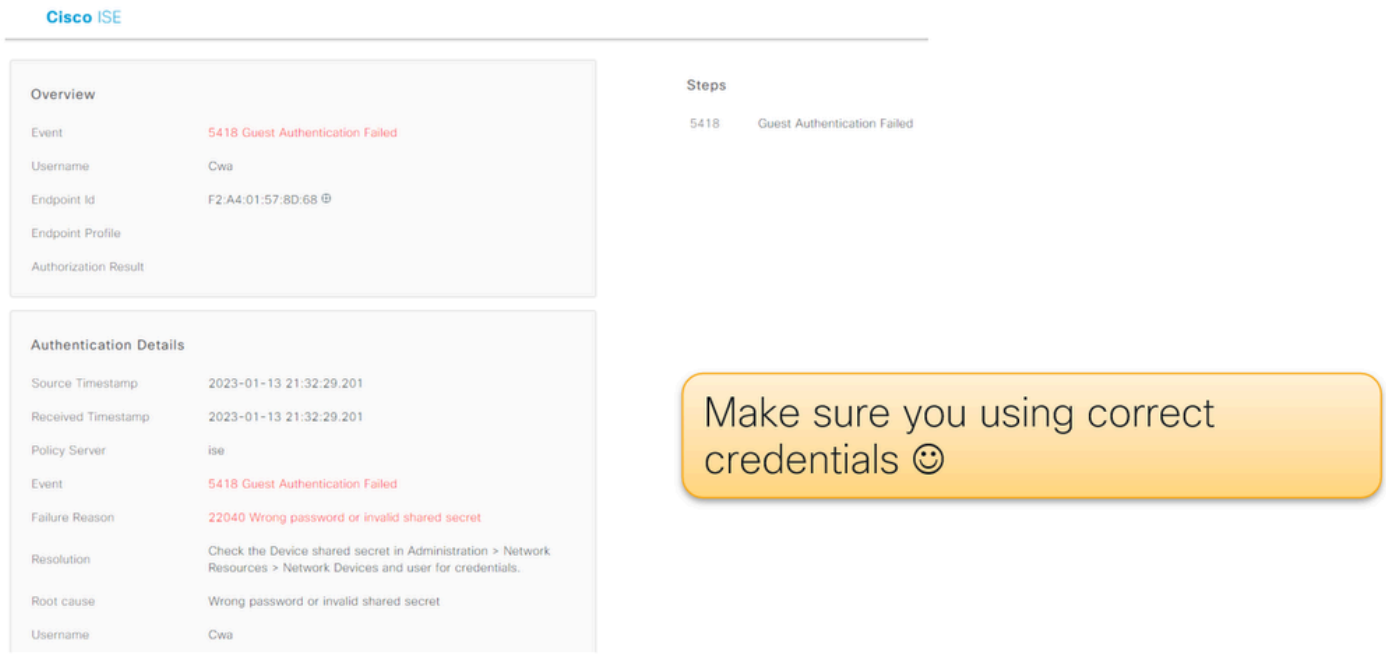
Ein letztes Mal den Fluss prüfen...




Client-Anmeldung und CoA

12 - Fehler bei der Gastanmeldung?

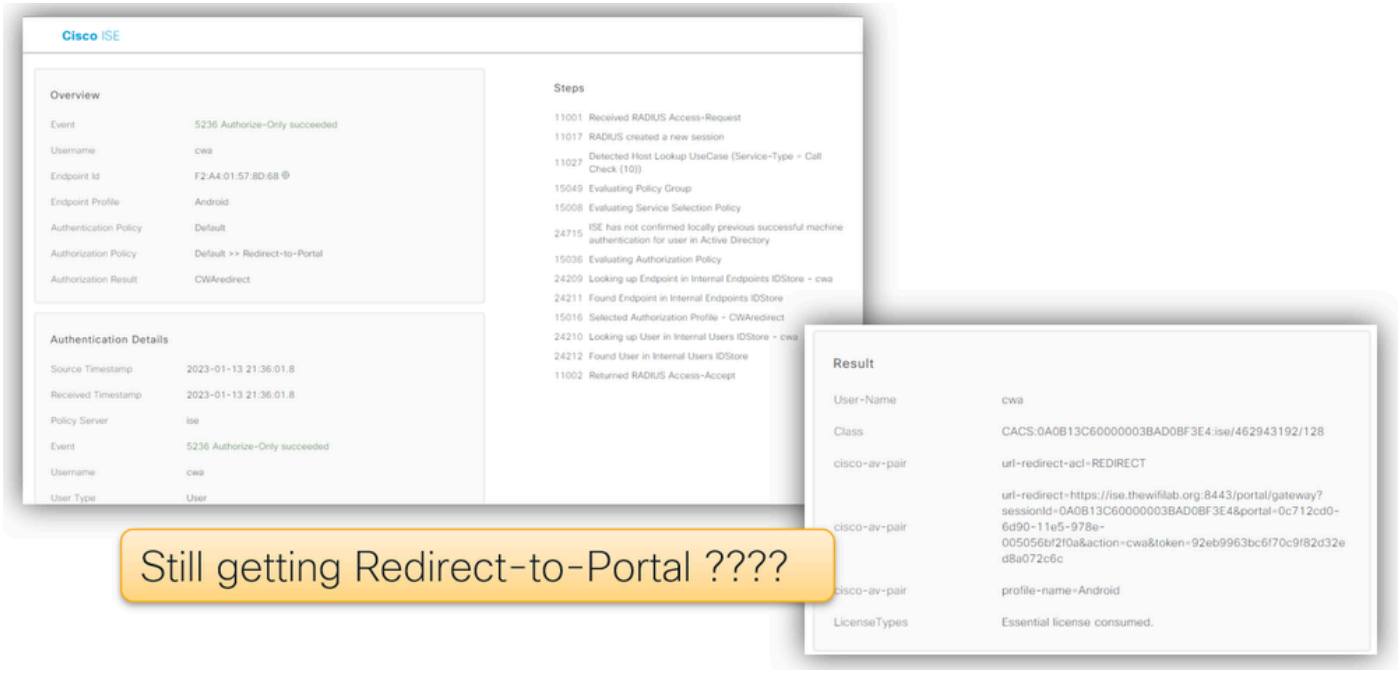
Überprüfen Sie die ISE-Protokolle auf fehlgeschlagene Authentifizierung. Stellen Sie sicher, dass die Anmeldeinformationen korrekt sind.




Fehler bei der Gastauthentifizierung aufgrund falscher Anmeldeinformationen.

13 - Anmeldung erfolgreich, aber nicht zu RUN?

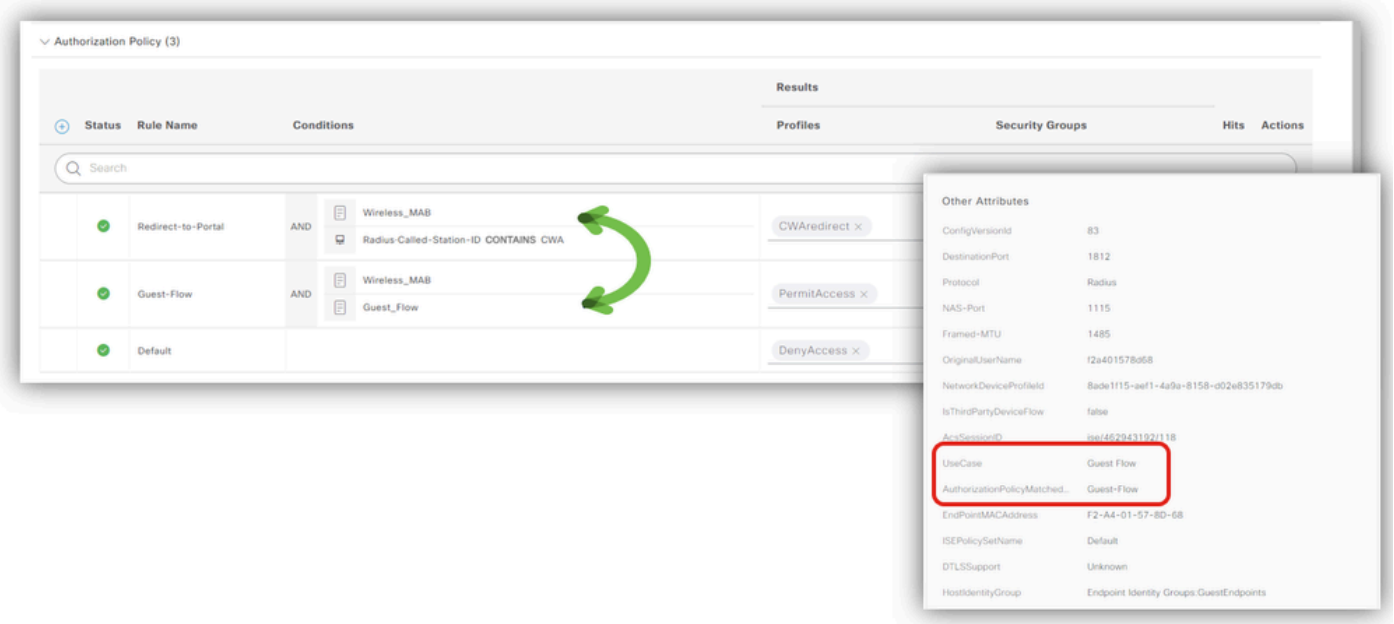
Überprüfen Sie die ISE-Protokolle auf Authentifizierungsdetails und Ergebnisse:




Umleitungsschleife

In diesem Beispiel erhält der Client erneut das Autorisierungsprofil, das die Umleitungs-URL und die Umleitungs-ACL enthält. Daraus ergibt sich eine Umleitungsschleife.

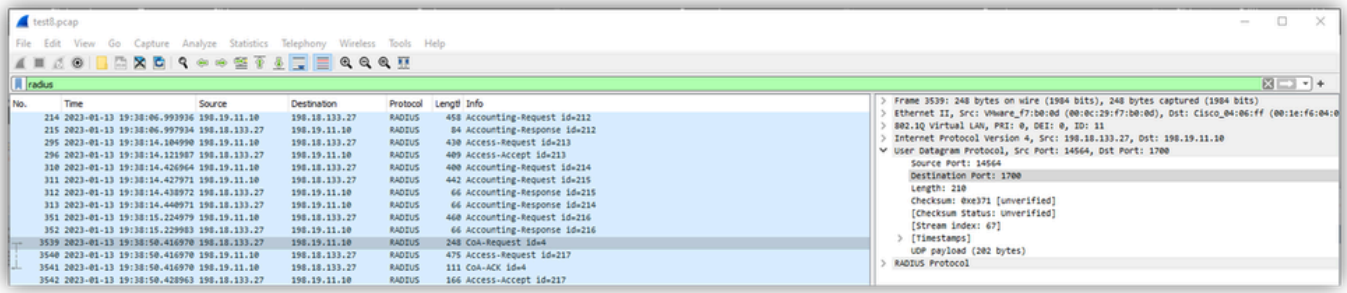
Aktivieren Sie Policy Set. Die Regelprüfung für Guest_Flow muss vor der Umleitung liegen:




Guest_Flow-Regel

14 - COA-Fehler?

Mit EPC und ISE TCPDump kann der CoA-Datenverkehr überprüft werden. Überprüfen Sie, ob der CoA-Port (1700) zwischen WLC und ISE offen ist. Stellen Sie sicher, dass der freigegebene geheime Schlüssel übereinstimmt.




CoA-Datenverkehr

Anmerkung: In Version 17.4.x und höher müssen Sie auch den CoA-Serverschlüssel konfigurieren, wenn Sie den RADIUS-Server konfigurieren. Verwenden Sie denselben Schlüssel wie den gemeinsamen geheimen Schlüssel (bei ISE sind sie standardmäßig identisch). Optional soll ein anderer Schlüssel für CoA als der gemeinsame geheime Schlüssel konfiguriert werden, wenn dies der Grund ist, für den der RADIUS-Server konfiguriert wurde. In Cisco IOS® XE 17.3 wurde für die Webbenutzeroberfläche lediglich derselbe geheime Schlüssel wie für den CoA-Schlüssel verwendet.

Ab Version 17.6.1 wird RADIUS (einschließlich CoA) über diesen Port unterstützt. Wenn Sie den Service-Port für RADIUS verwenden möchten, benötigen Sie folgende Konfiguration:

<#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**

# Schlussfolgerung

Dies ist die wiederaufgenommene CWA-Checkliste:

- Vergewissern Sie sich, dass sich der Client im richtigen VLAN befindet und IP-Adresse und DNS erhält.
    - Abrufen von Client-Details am WLC und Ausführen von Paketerfassungen, um den DHCP-Austausch anzuzeigen
- Überprüfen, ob der Client Hostnamen über DNS auflösen kann
    - Pingen Sie den Hostnamen von cmd.
- WLC muss auf Port 80 lauschen
    - Überprüfen Sie den globalen Befehl ip http server oder den globalen Parameterzuordnungsbefehl webauth-http-enable.
- Installieren Sie ein vertrauenswürdiges Zertifikat auf der ISE, um die Zertifikatswarnung loszuwerden.
    - Vertrauenswürdiges Zertifikat muss nicht auf WLC in CWA installiert werden.
- Authentifizierungsrichtlinie bei ISE - Erweiterte Option "Weiter" Wenn Benutzer nicht gefunden wird
    - Um gesponserten Gastbenutzern zu erlauben, sich zu verbinden und URL-Umleitung und ACL zu erhalten.

Die wichtigsten Tools zur Fehlerbehebung:

- WLC-EPC
    - Innenfilter: DHCP-Protokoll, MAC-Adresse
- WLC-Monitor
    - Überprüfen Sie die Details zur Client-Sicherheit.
- WLC RA-Verfolgung
    - Debugging mit detaillierten Informationen auf WLC Seite.
- ISE-Live-Protokolle
    - Authentifizierungsdetails.
- ISE-TCPDump
    - Sammeln von Paketerfassungen an der ISE-PSN-Schnittstelle

# Referenzen

Konfigurieren von Central Web Authentication (CWA) auf Catalyst 9800 WLC und ISE

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.