Problemen oplossen met Central Web Authentication (CWA) met Wireless Lan Controller (WLC) 9800 en Identity Services Engine (ISE)

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen kunt oplossen met Central Web Authentication (CWA) met WLC 9800 en ISE.

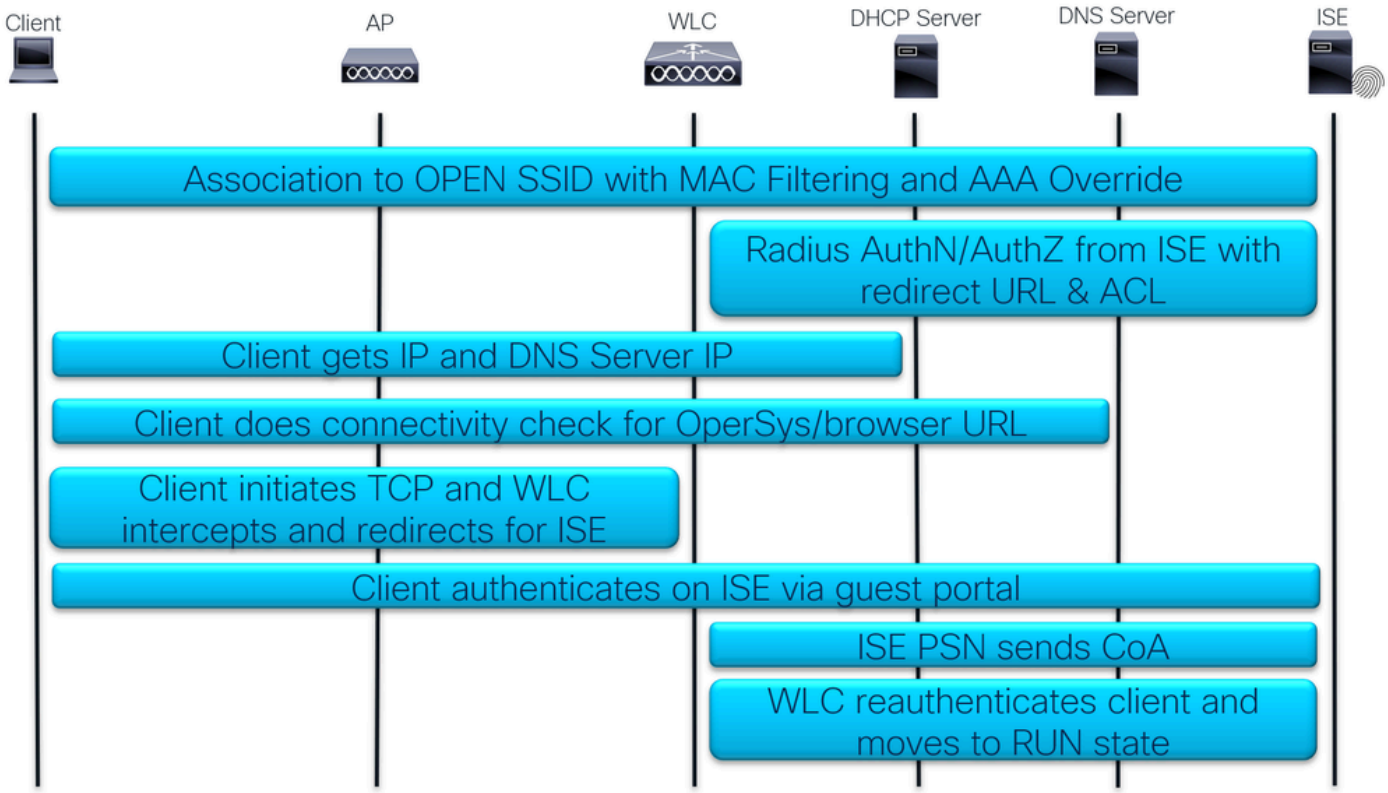
Achtergrondinformatie

Er zijn momenteel zoveel persoonlijke apparaten dat netwerkbeheerders die op zoek zijn naar het beveiligen van draadloze toegang, normaal gesproken kiezen voor draadloze netwerken die CWA gebruiken.
In dit document richten we ons op het stroomschema van CWA, dat helpt bij het oplossen van de veelvoorkomende problemen die ons beïnvloeden.
We kijken naar de gemeenschappelijke gotchas van het proces, hoe logs met betrekking tot CWA

te verzamelen, hoe deze logs te analyseren en hoe een ingesloten pakketopname op de WLC te verzamelen om de verkeersstroom te bevestigen.

CWA is de meest voorkomende configuratie voor bedrijven die gebruikers in staat stellen om verbinding te maken met het bedrijfsnetwerk met behulp van hun persoonlijke apparaten, ook bekend als BYOD.
Elke netwerkbeheerder is geïnteresseerd in de gotcha's en de stappen voor probleemoplossing die moeten worden uitgevoerd om hun problemen op te lossen voordat een TAC-geval wordt geopend.

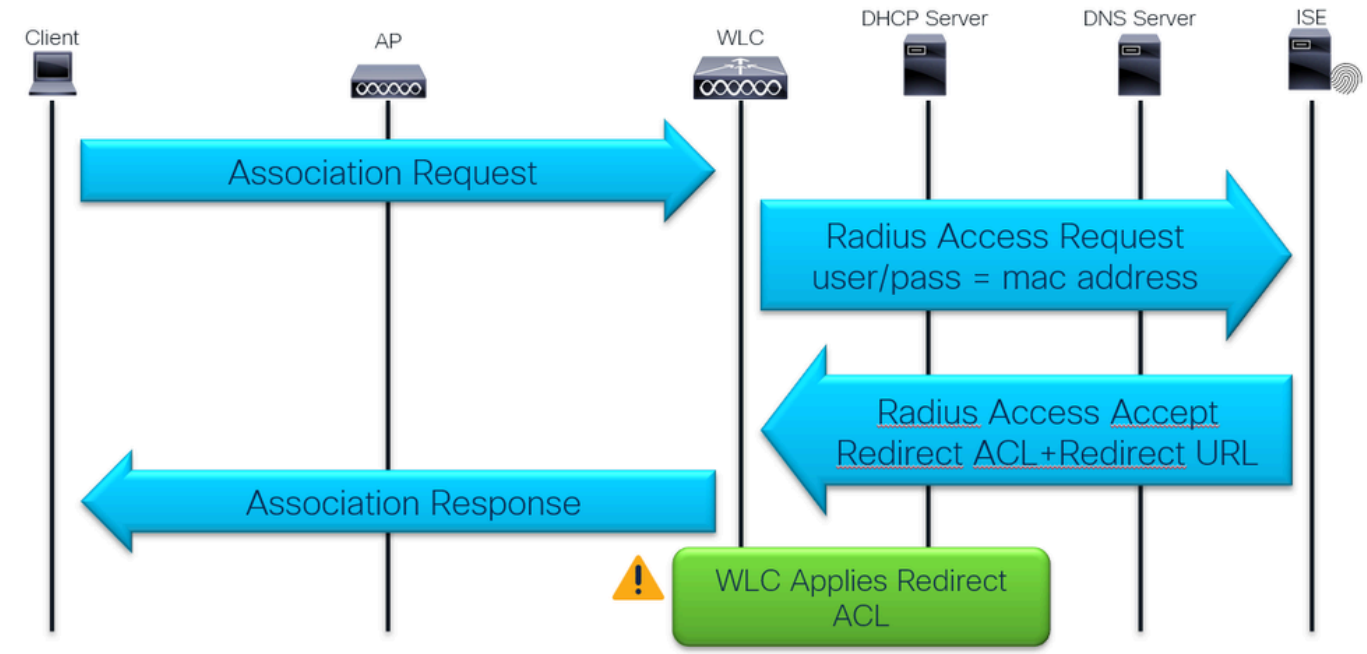
Hier is de CWA-pakketstroom:



CWA-pakketstroom

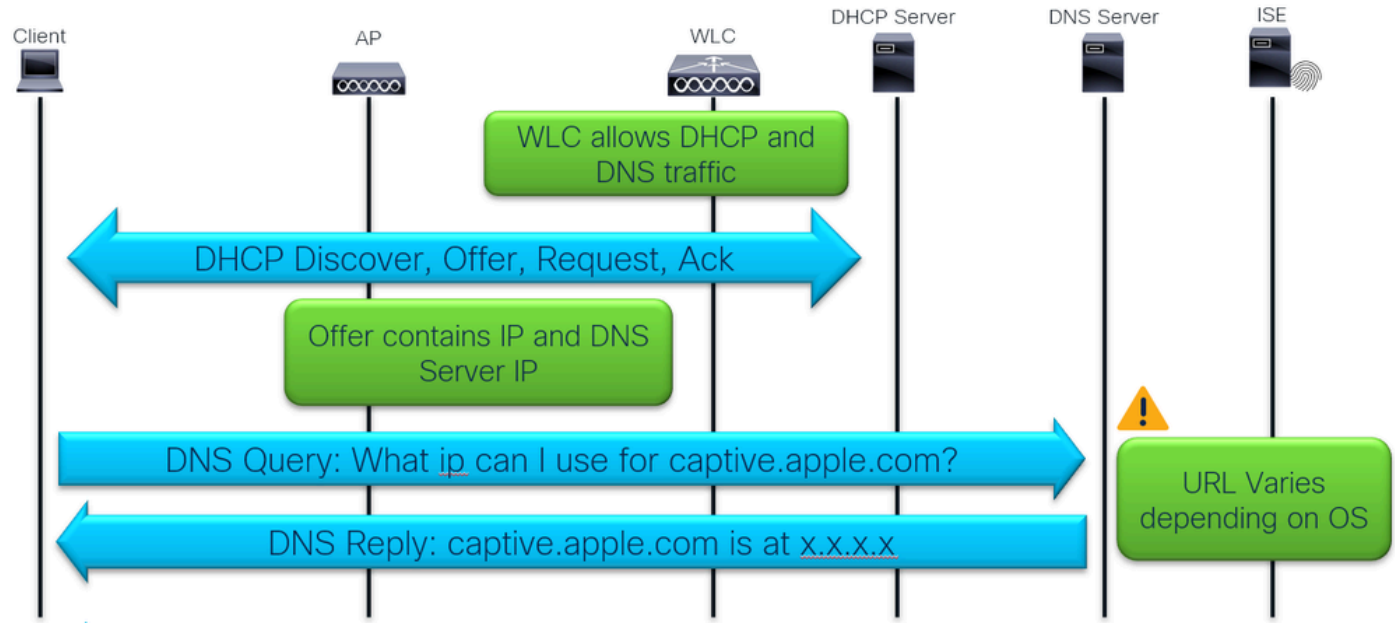
Gedetailleerde flow

Eerste associatie en RADIUS-verificatie:



Eerste associatie en RADIUS-verificatie

DHCP, DNS en connectiviteitscontrole:



DHCP-, DNS- en connectiviteitscontrole

De connectiviteitscontrole wordt uitgevoerd met behulp van captive portal-detectie door het besturingssysteem of de browser van het clientapparaat.

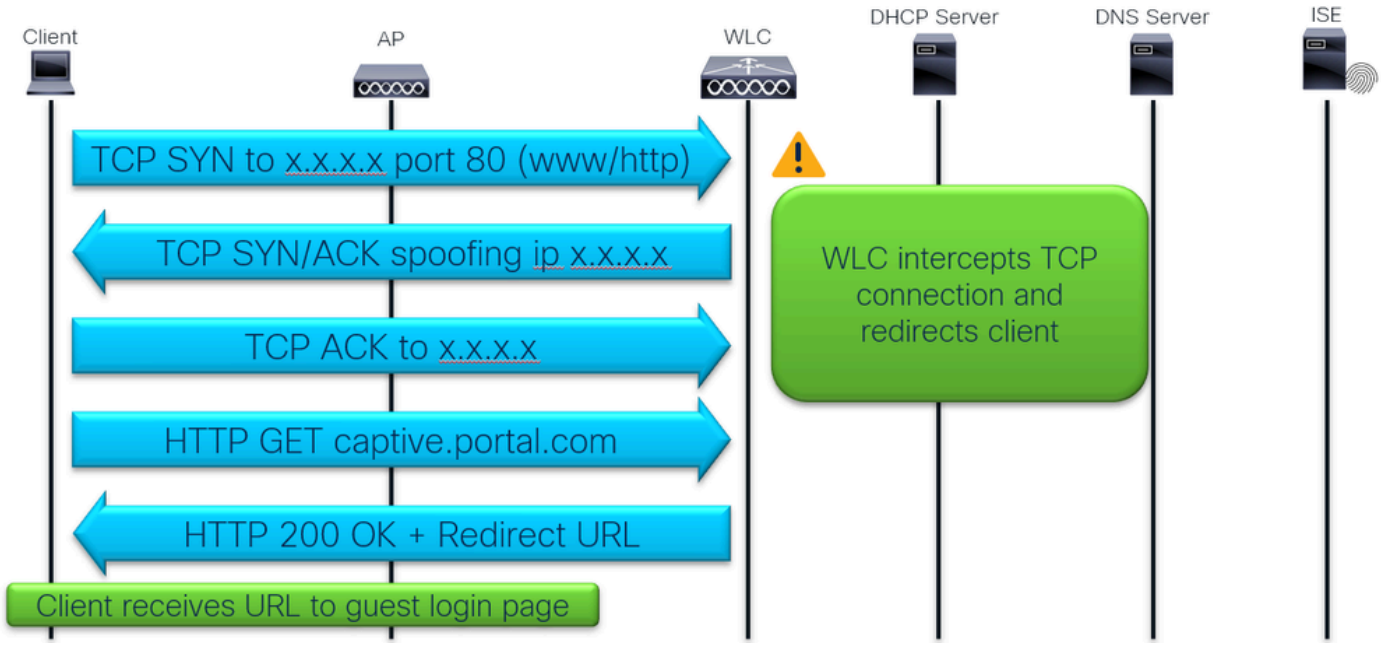
Er zijn voorgeprogrammeerde besturingssystemen voor apparaten om HTTP GET naar een specifiek domein uit te voeren

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

En browsers voeren deze controle ook uit wanneer ze worden geopend:

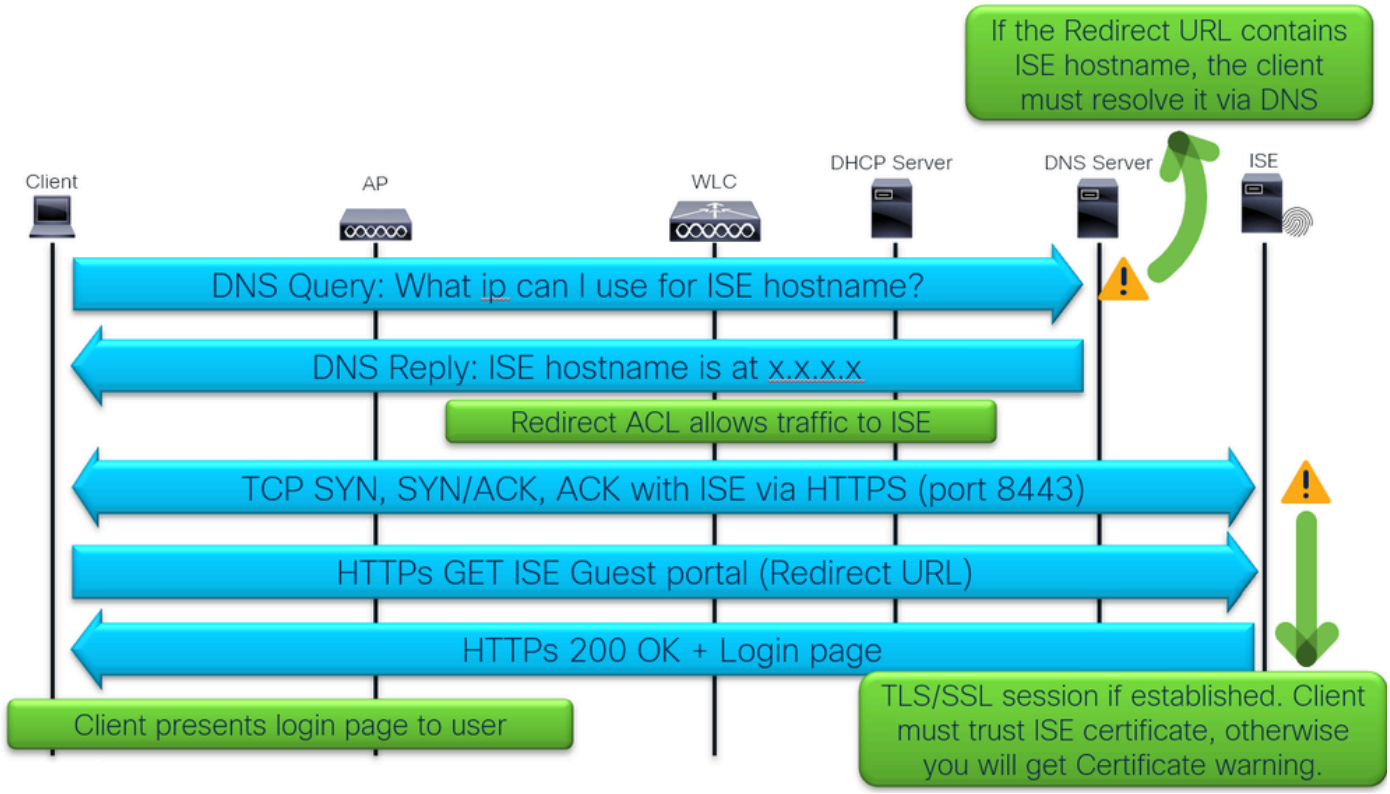
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Interceptie en omleiding van het verkeer:



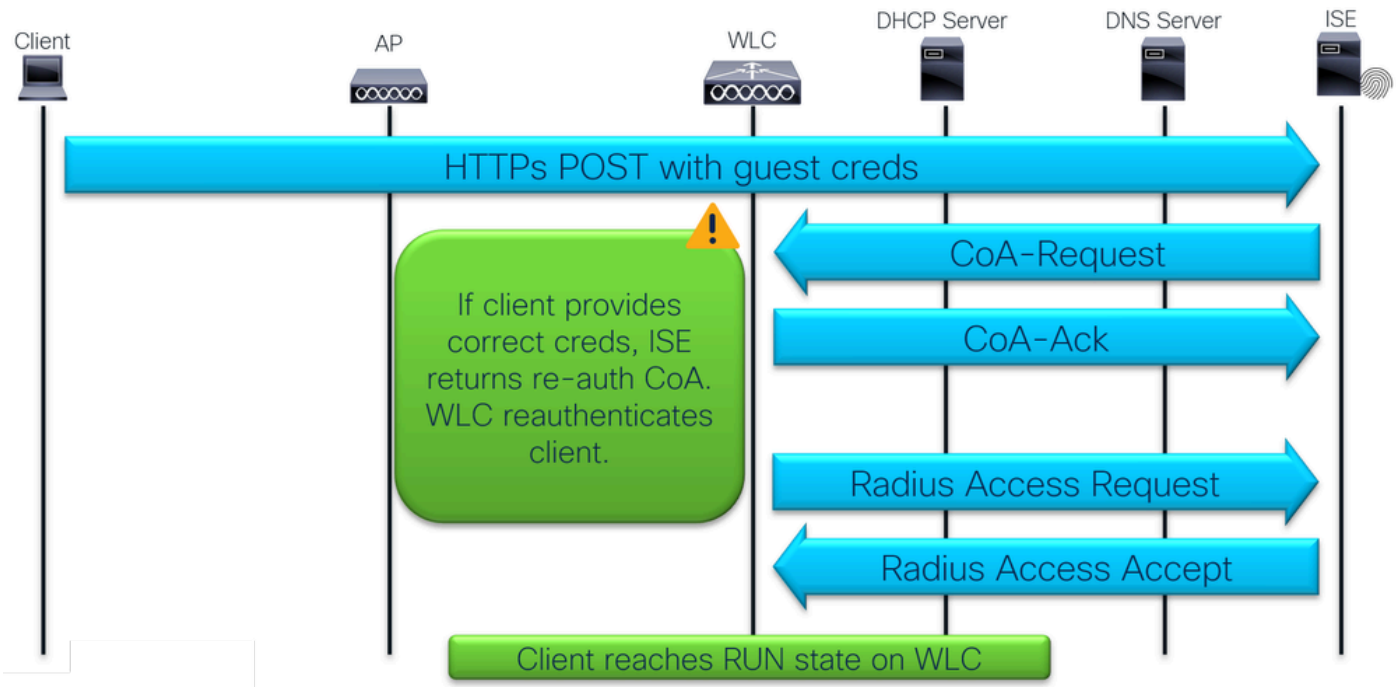
Interceptie en omleiding van het verkeer

Client login in ISE guest login portal:



Client login in ISE guest login portal

Client login en CoA:

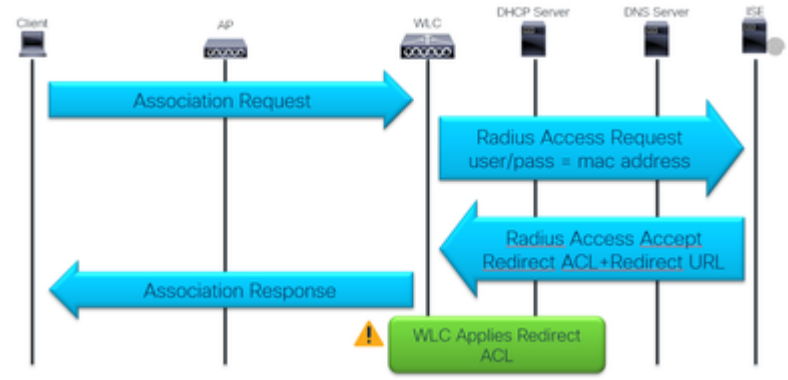


Client login en CoA

Probleemoplossing

Algemeen symptoom: gebruiker wordt niet doorgestuurd naar aanmeldpagina.

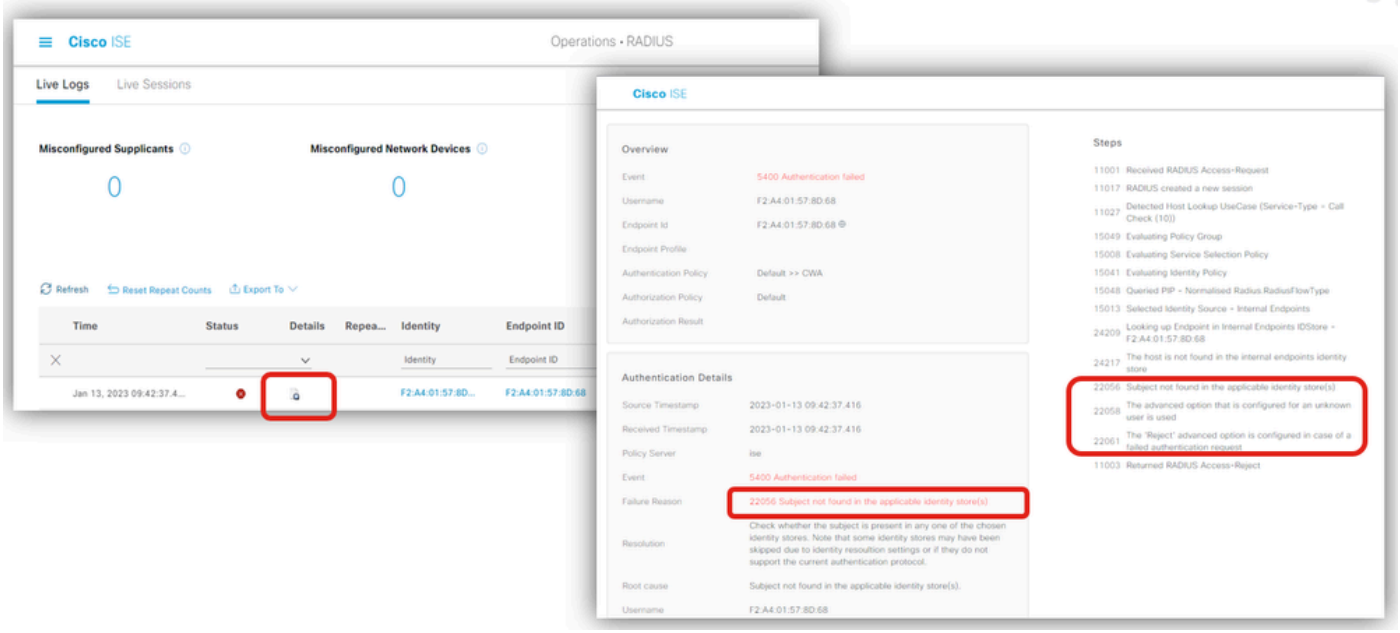
Laten we beginnen met het eerste deel van de flow:



Eerste associatie en RADIUS-verificatie

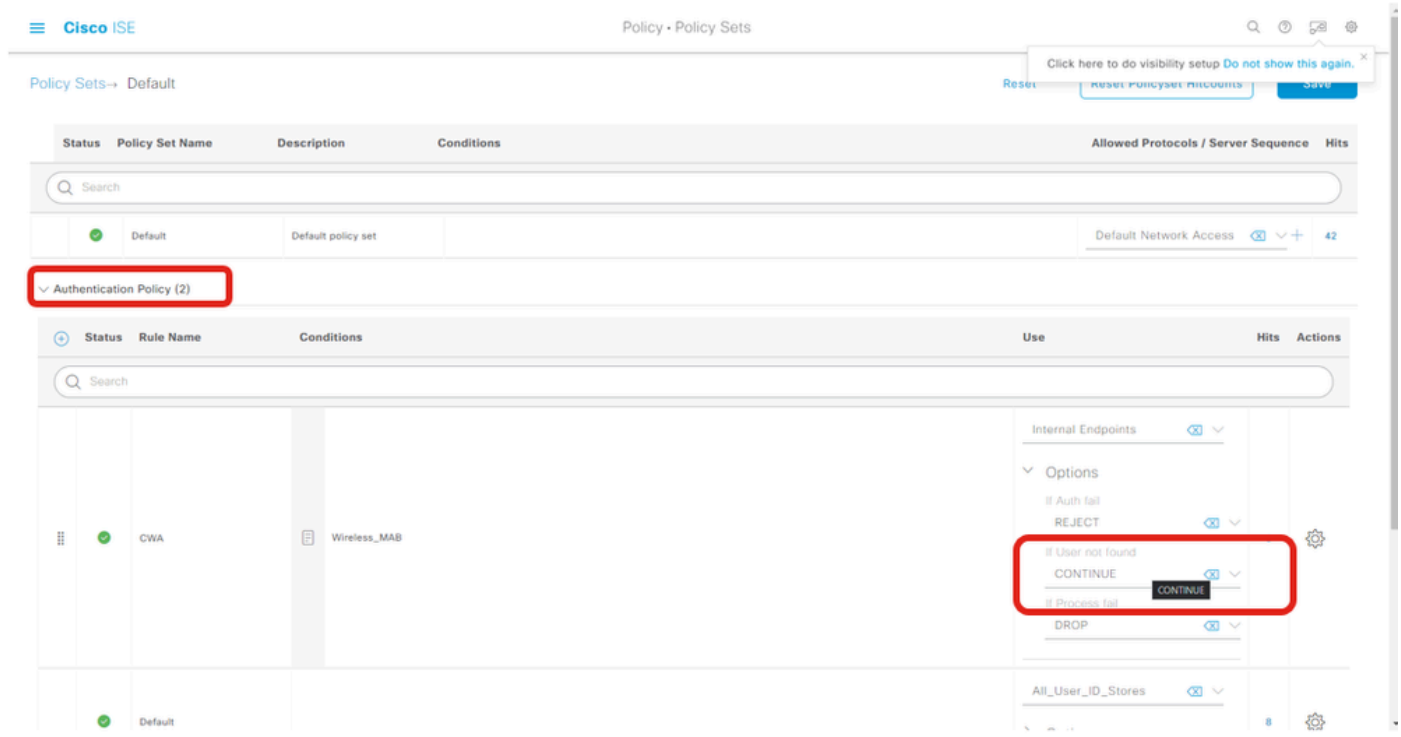
1 - Is de eerste RADIUS-verificatie succesvol?

Controleer het verificatieresultaat van de mac-filtering:



ISE Live-logboeken die het verificatieresultaat van mac-filtering weergeven

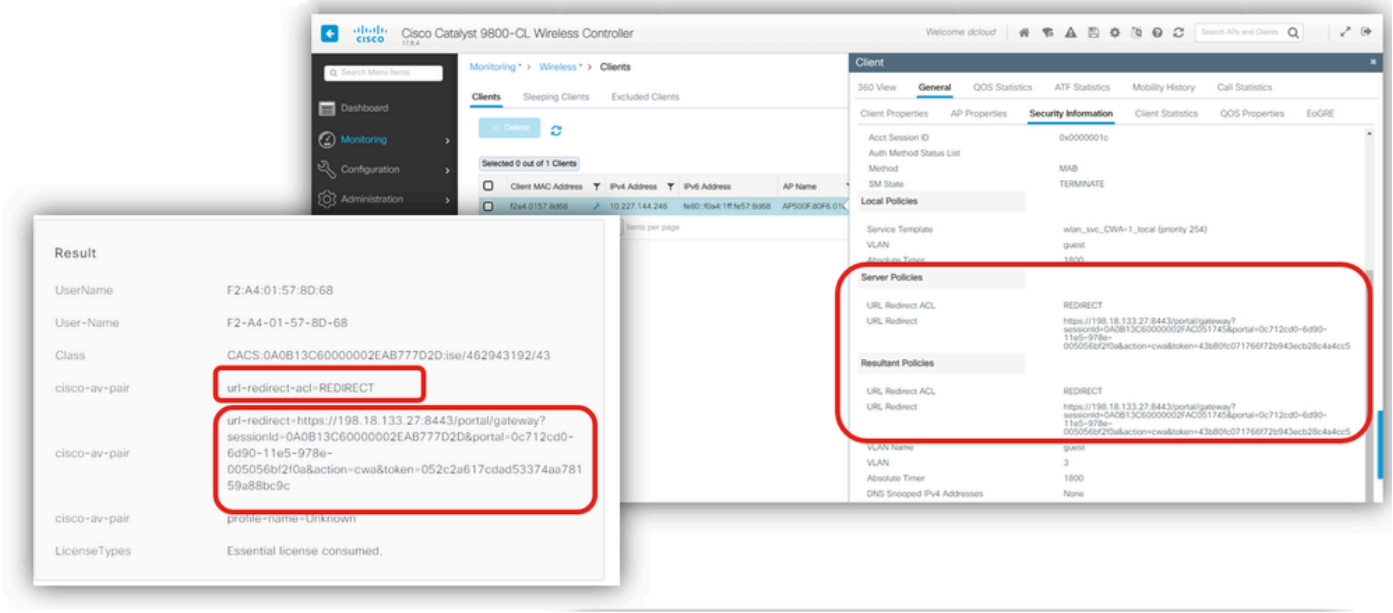
Zorg ervoor dat de geavanceerde optie voor de verificatie is ingesteld op "Doorgaan" als de gebruiker niet wordt gevonden:



Gebruiker niet gevonden geavanceerde optie

2 - WLC ontvangt de Redirect URL en ACL?

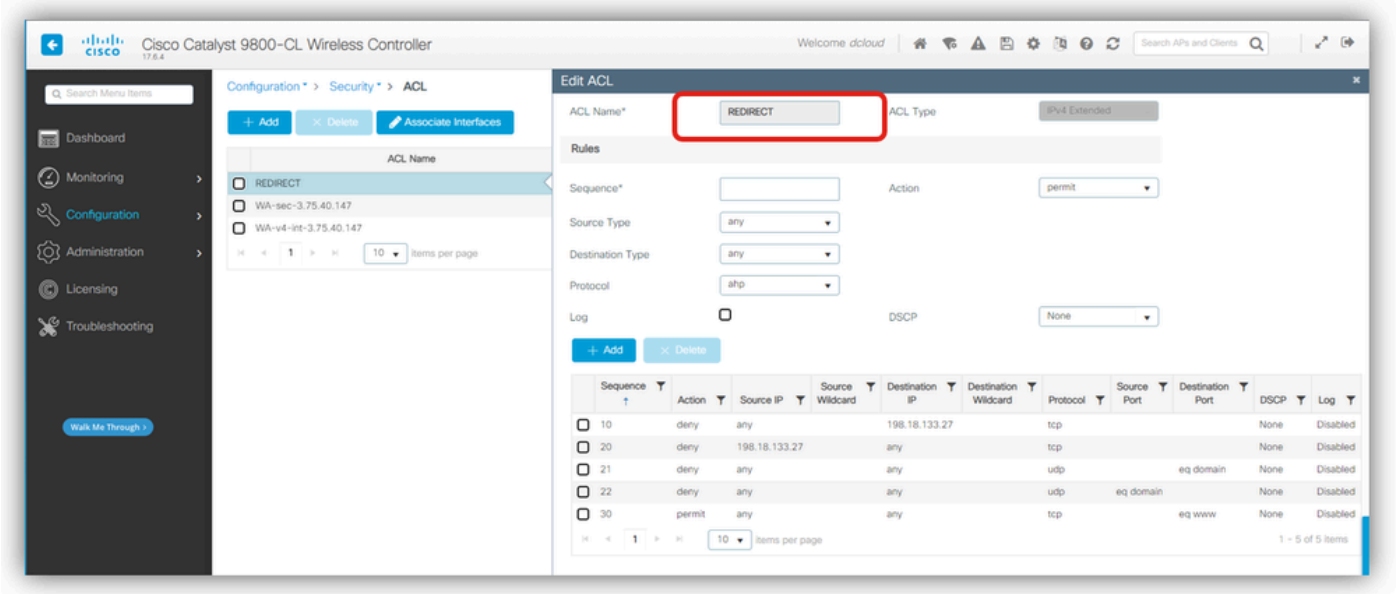
Controleer ISE live-logs en WLC-clientbeveiligingsinformatie onder Bewaken Controleer of de ISE Redirect-URL en ACL in de toegangsacceptatie worden verzonden en door WLC worden ontvangen en op de client worden toegepast in de clientgegevens:



ACL en URL omleiden

3 - Is de omleiding ACL correct?

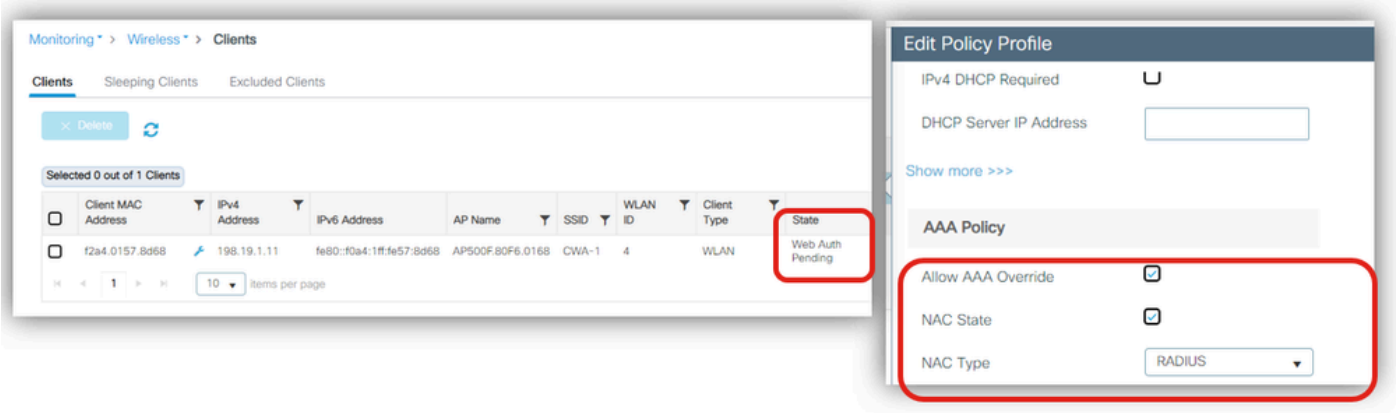
Controleer de ACL-naam voor een typefout. Zorg ervoor dat het precies is zoals het door de ISE wordt verzonden:



ACL-verificatie omleiden

4 - Is de client verplaatst naar Web-Auth in afwachting?

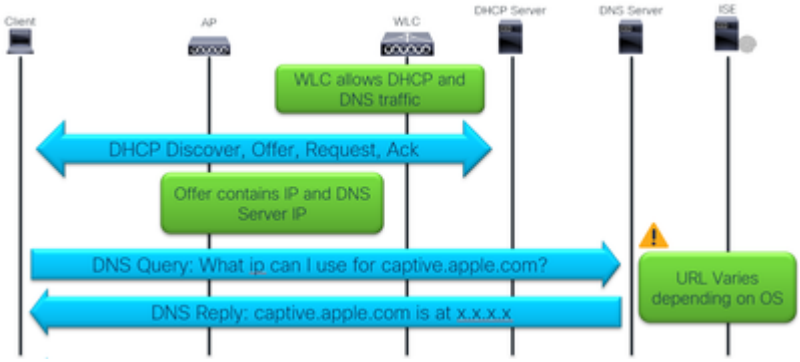
Controleer de clientgegevens voor de status "Web Auth Pending". Als de status niet in die staat is, controleert u of AAA-overschrijving en Radius NAC zijn ingeschakeld in het beleidsprofiel:



Clientgegevens, aaa-overschrijving en RADIUS NAC

Nog steeds niet werken?

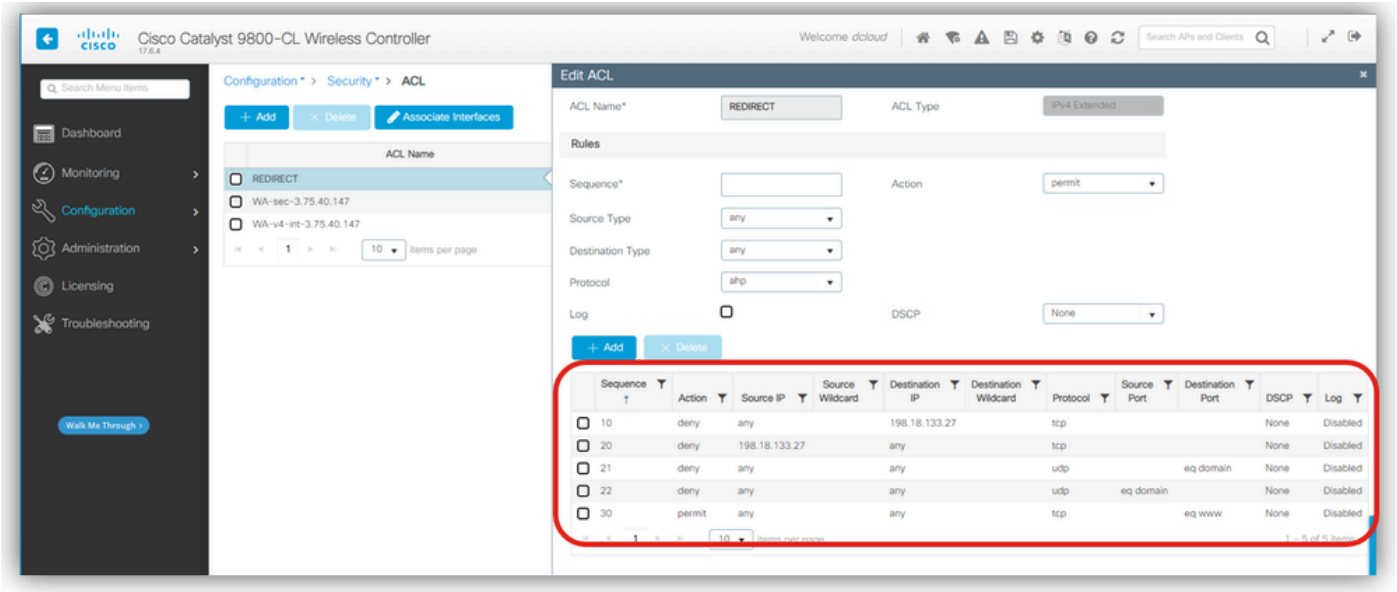
Laten we de flow nog eens bekijken….



DHCP-, DNS- en connectiviteitscontrole

5 - Staat WLC DHCP- en DNS-verkeer toe?

Verifieer de ACL-inhoud omleiden in de WLC:



ACL-inhoud in de WLC omleiden

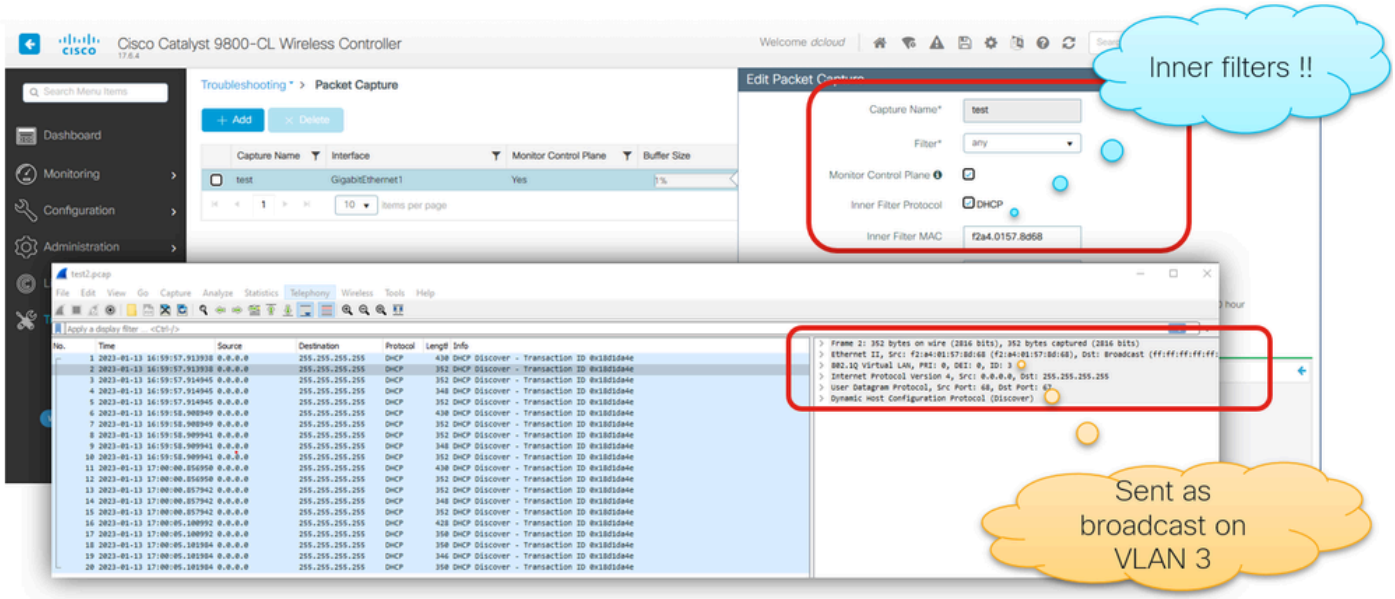
De Redirect ACL definieert welk verkeer wordt onderschept en omgeleid door de vergunningsverklaring en welk verkeer wordt genegeerd van onderschepping en omleiding met een weigeringsverklaring.

In dit voorbeeld laten we DNS en verkeer van/naar het ISE IP-adres stromen en onderscheppen we elk tcp-verkeer op poort 80 (www).

6 - Ontvangt de DHCP-server DHCP Discover/Request?

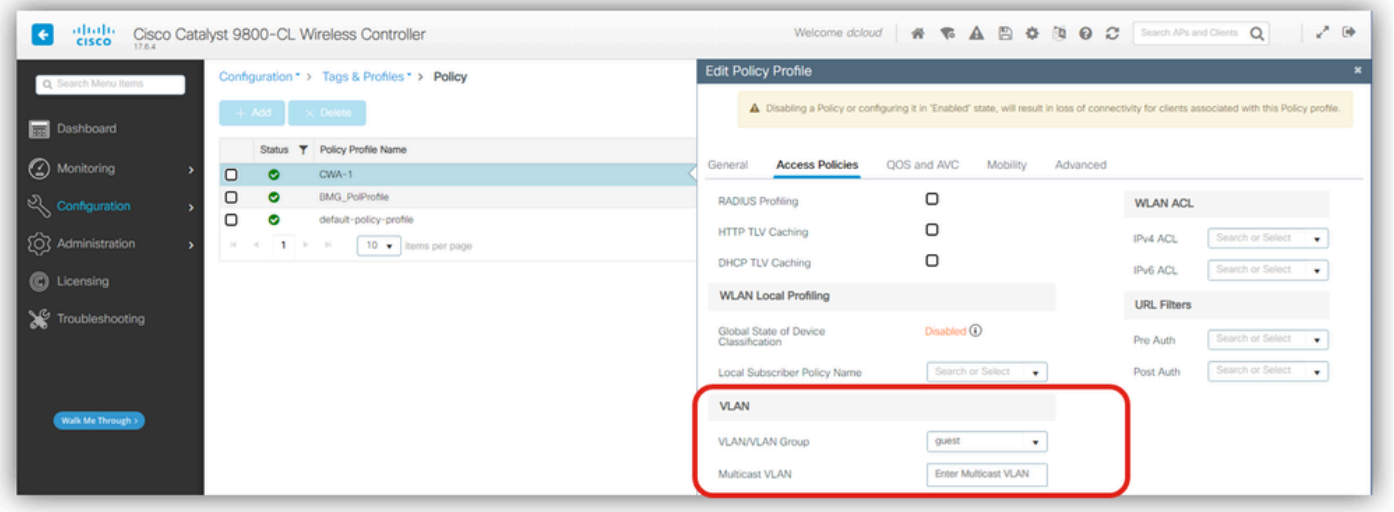
Neem contact op met EPC als er een DHCP-uitwisseling plaatsvindt. EPC kan worden gebruikt met Inner Filters zoals het DHCP-protocol en/of Inner Filter MAC, waar we het MAC-adres van het clientapparaat kunnen gebruiken en we in de EPC alleen DHCP-pakketten krijgen die worden verzonden door of verzonden naar het MAC-adres van het clientapparaat.

In dit voorbeeld kunnen we de DHCP Discover-pakketten zien die worden verzonden als uitzending op VLAN 3:



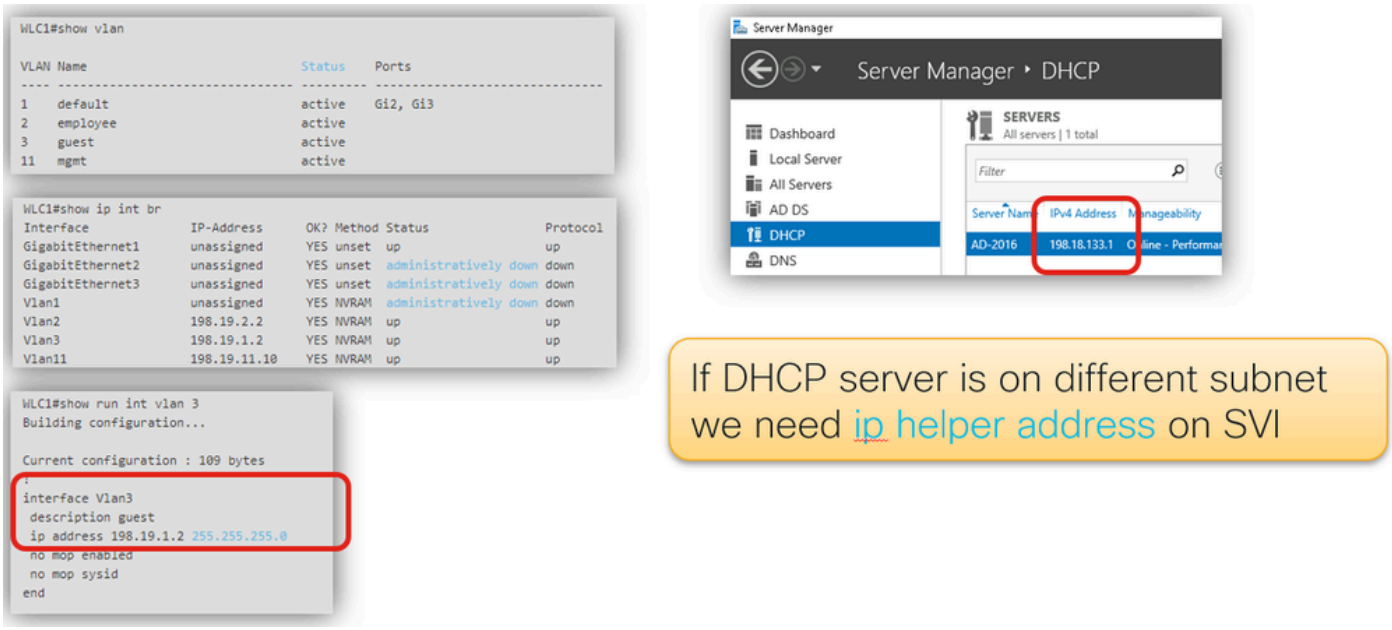
WLC EPC om DHCP te verifiëren

Bevestig het verwachte client-VLAN in het beleidsprofiel:



VLAN in het beleidsprofiel

WLC VLAN- en switchport Trunk-configuratie en DHCP-subnet controleren:



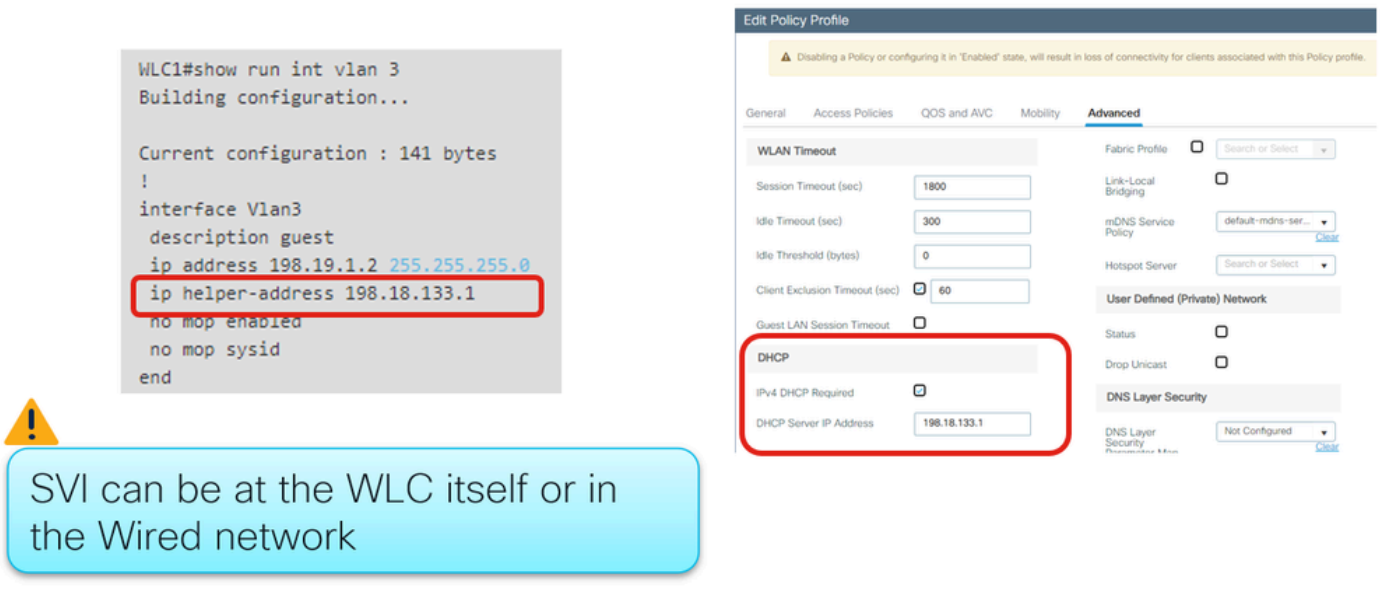
VLAN, switchport en DHCP-subnet

We kunnen zien dat VLAN 3 bestaat in de WLC en het heeft ook SVI voor VLAN 3, maar wanneer we het IP-adres van de DHCP-server controleren, op het verschillende subnet, daarom hebben we het IP-helperadres op de SVI nodig.

Best practices schrijven voor dat SVI voor clientsubnetten in de bekabelde infrastructuur moet worden geconfigureerd en bij de WLC moet worden vermeden.

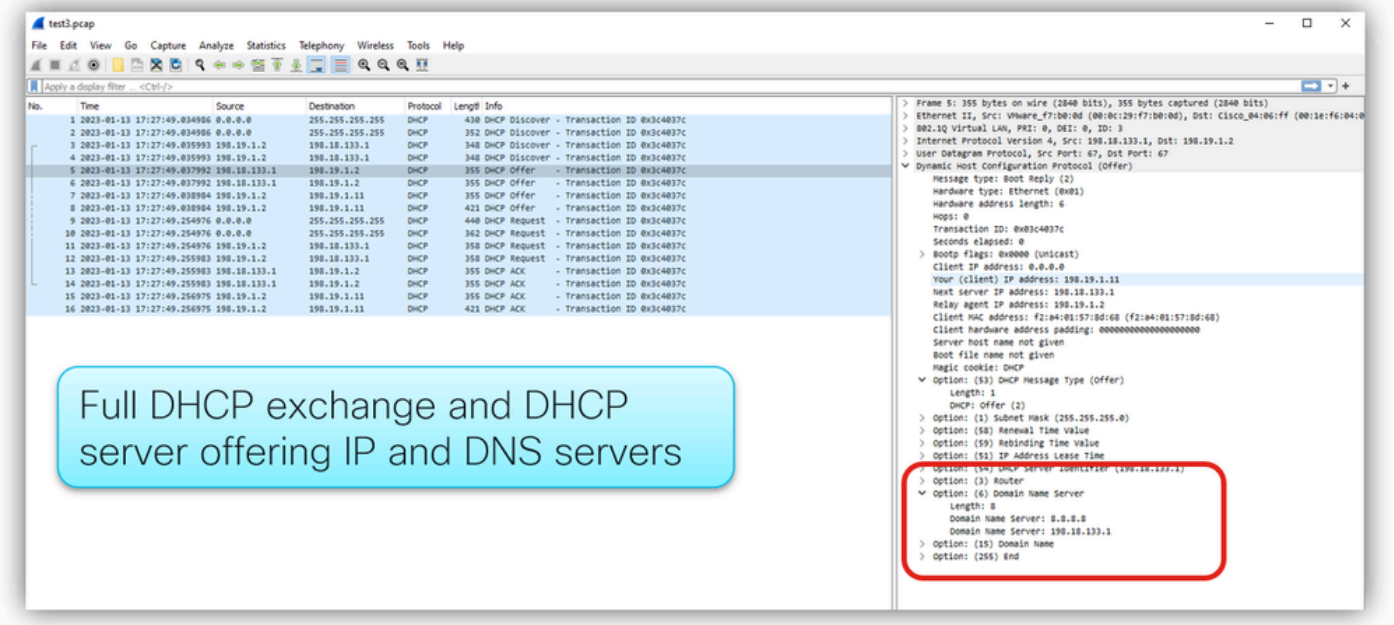
In elk van de gevallen moet de opdracht ip-helper-adres worden toegevoegd aan de SVI, ongeacht waar deze zich bevindt.

Een alternatief is het IP-adres van de DHCP-server configureren in het beleidsprofiel:



IP-helper-adres bij SVI of Beleidsprofiel

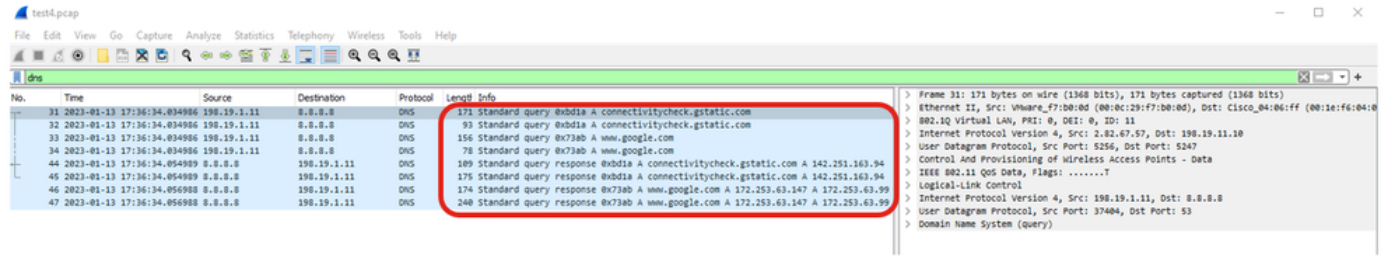
U kunt vervolgens met EPC controleren of de DHCP-uitwisseling nu in orde is en of de DHCP-server DNS-server-IP's biedt:



DHCP Aanbieding details van DNS server ip

7 - Gebeurt automatische omleiding?

Controleer met WLC EPC of de DNS-server de volgende vragen beantwoordt:

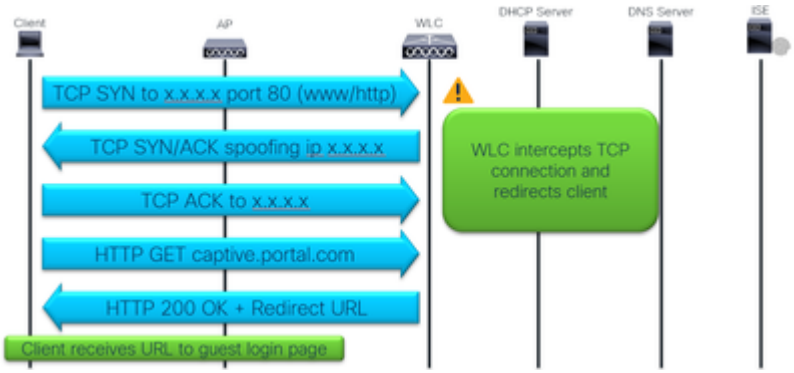


DNS-query en -antwoorden

- Als de omleiding niet automatisch is, opent u een browser en probeert u een willekeurig IP-adres. Bijvoorbeeld 10.0.0.1.
- Als omleiding dan werkt, is het mogelijk dat u een DNS-oplossingsprobleem heeft.

Nog steeds niet werken?

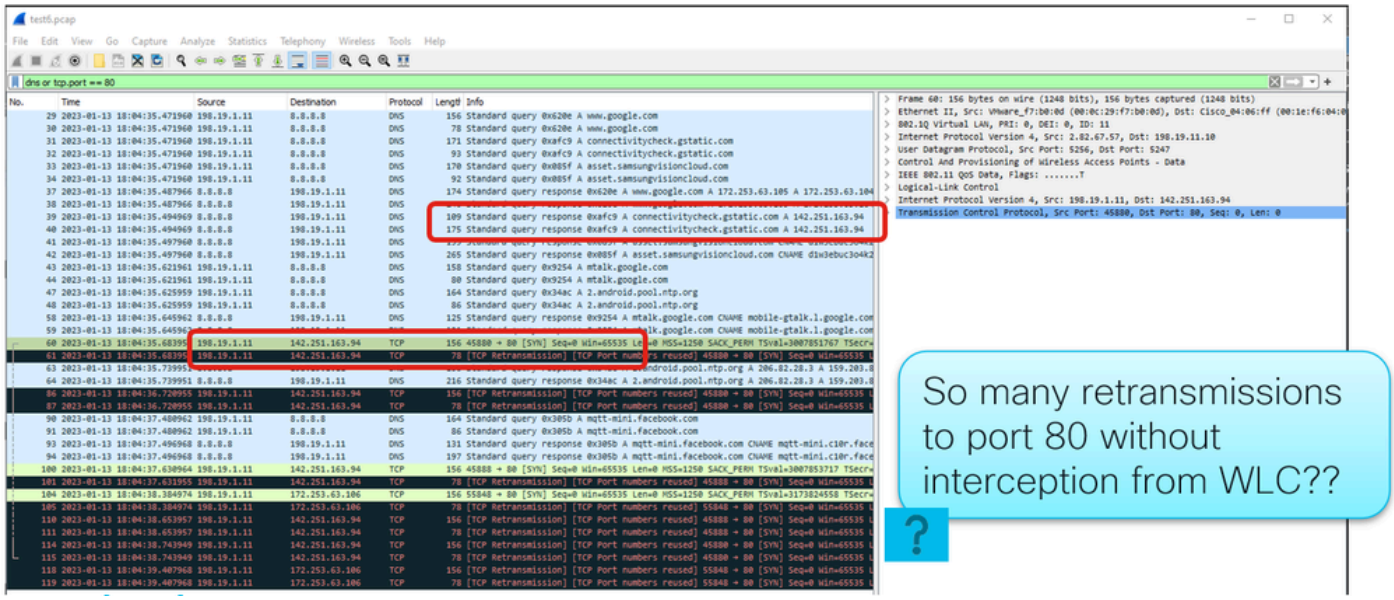
Laten we de flow nog eens bekijken…



Interceptie en omleiding van het verkeer

8 - Browser toont geen inlogpagina?

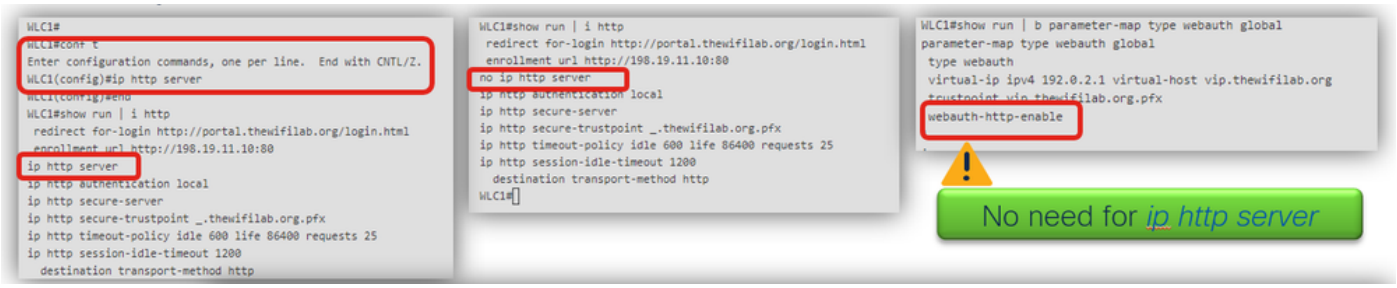
Controleer of de client het TCP SYN naar poort 80 verzendt en WLC het onderschept:



TCP-hertransmissies naar poort 80

Hier kunnen we zien dat de client TCP SYN-pakketten naar poort 80 stuurt, maar geen antwoord krijgt en TCP-hertransmissies uitvoert.

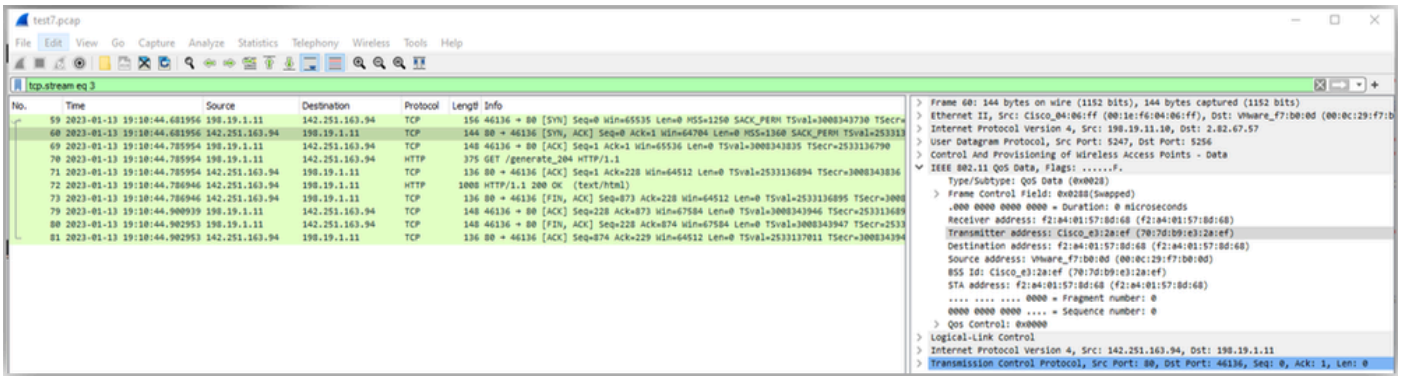
Zorg ervoor dat u de opdracht ip http server hebt in de globale configuratie of webauth-http-enable in de globale parameter-map:



HTTP-interceptiecommando's

Na de opdracht onderschept WLC de TCP en spoofs het IP-adres van de bestemming om te

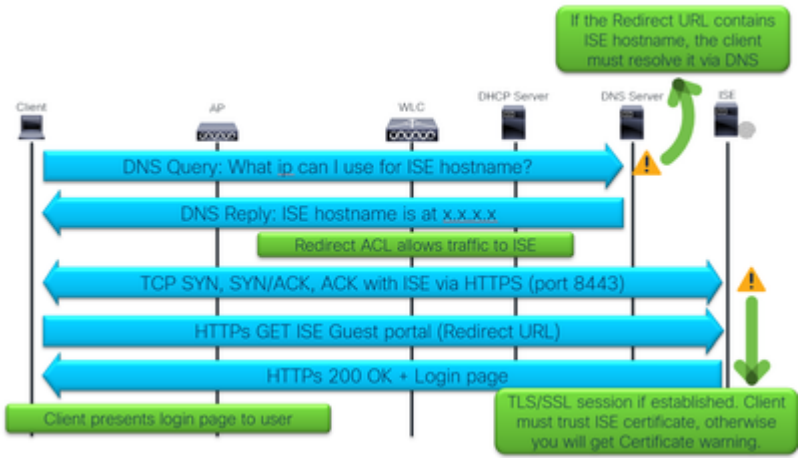
reageren op de client en om te leiden.



TCP-interceptie door WLC

Nog steeds niet werken?

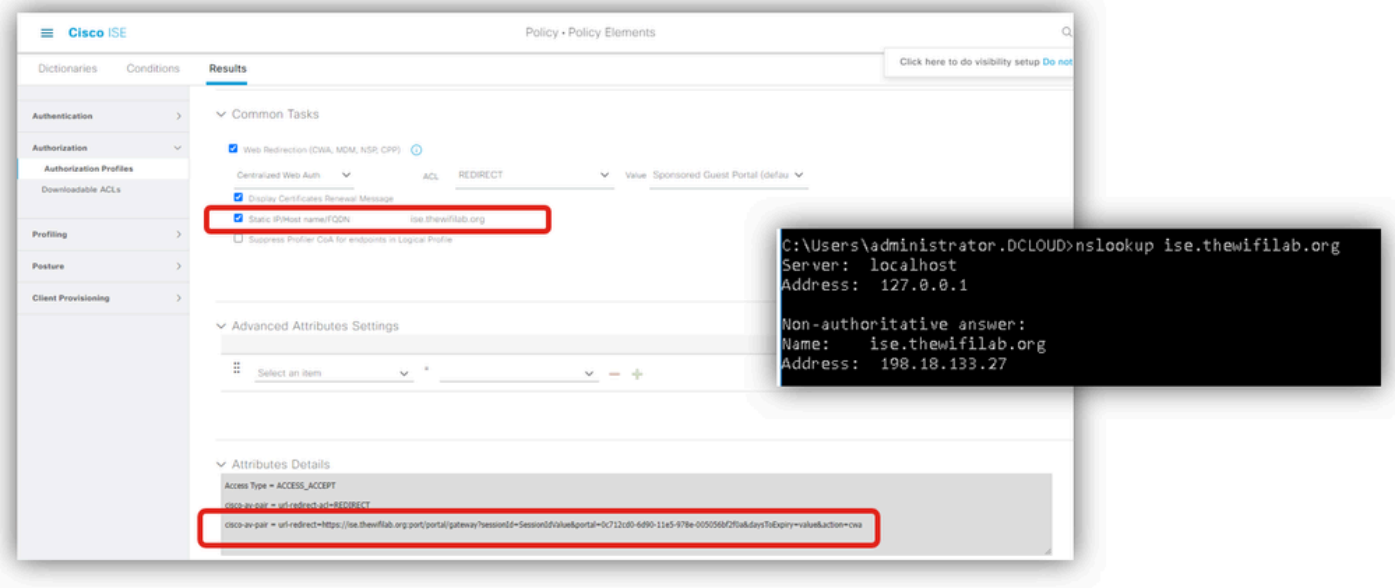
Er zit meer in de flow…



Client login in ISE guest login portal

9 - Kan de client de ISE-hostnaam oplossen?

Controleer of de URL voor omleiden IP of hostnaam gebruikt en of de client de ISE-hostnaam oplost:

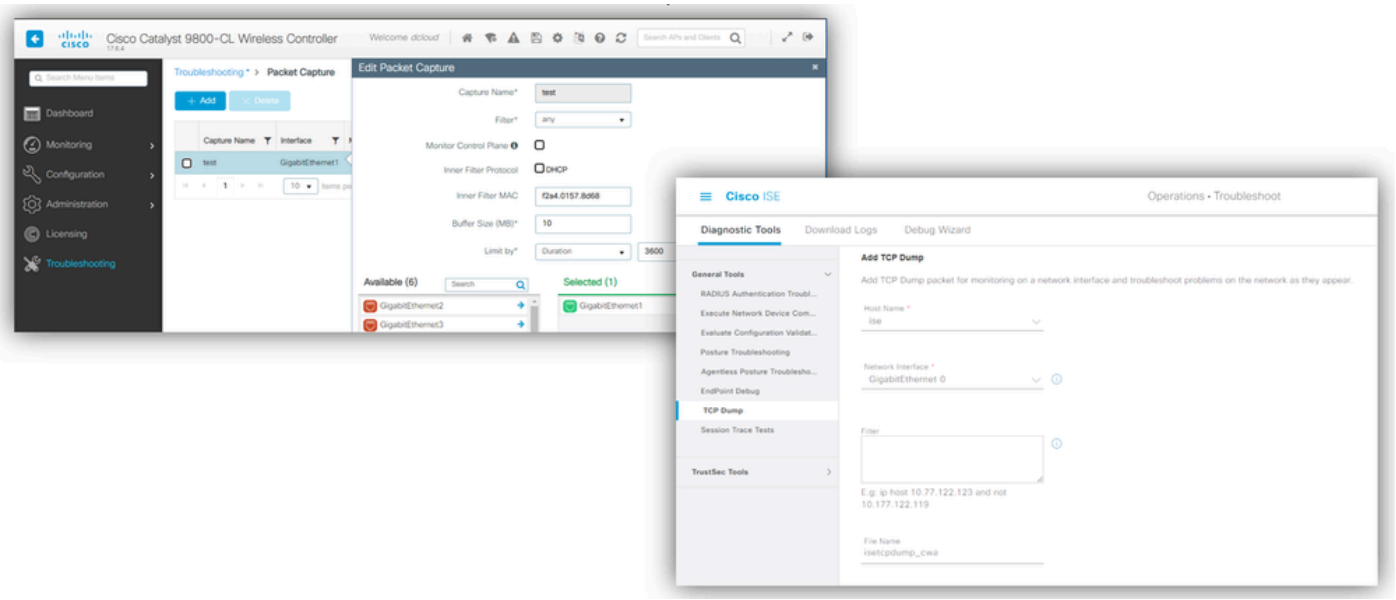


ISE Hostname-resolutie

Een veelvoorkomend probleem wordt gezien wanneer de omleidings-URL de ISE-hostnaam bevat, maar het clientapparaat kan die hostnaam niet oplossen naar het ISE IP-adres. Als de hostnaam wordt gebruikt, zorg er dan voor dat dit via DNS kan worden opgelost.

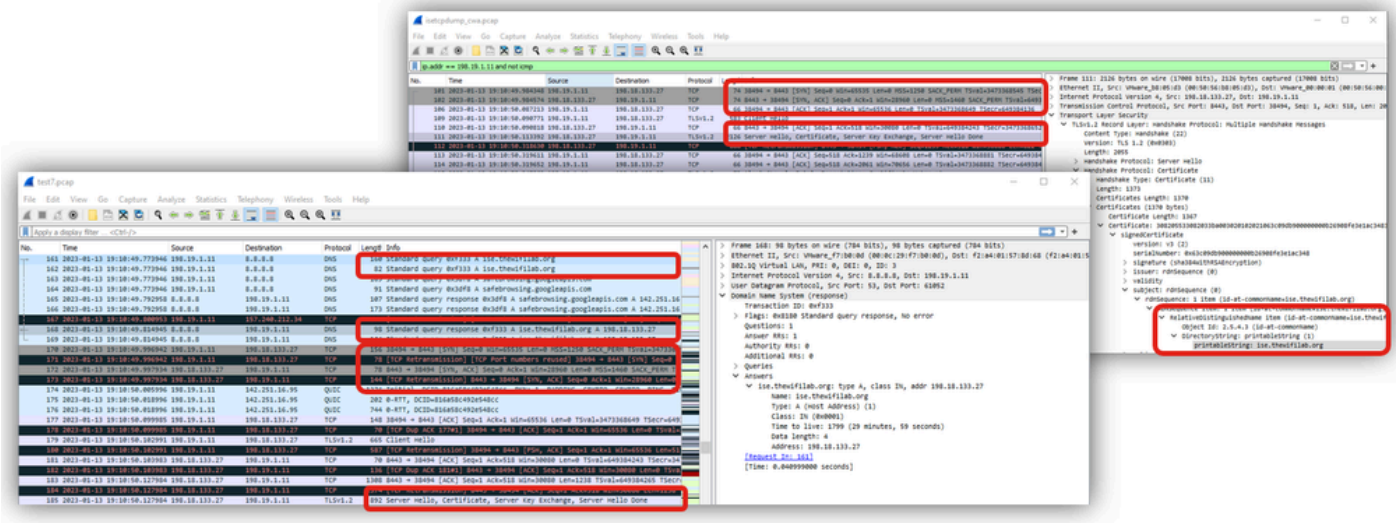
10 - Login pagina nog steeds niet geladen?

Controleer met WLC EPC en ISE TCPdump of clientverkeer ISE PSN bereikt. De opnamen configureren en starten op WLC en ISE:



WLC EPC en ISE TCPDump

Na de reproductie van het probleem wordt het verkeer vastgelegd en gecorreleerd. Hier kunnen we zien ISE hostnaam opgelost en vervolgens de communicatie tussen client en ISE op poort 8443:



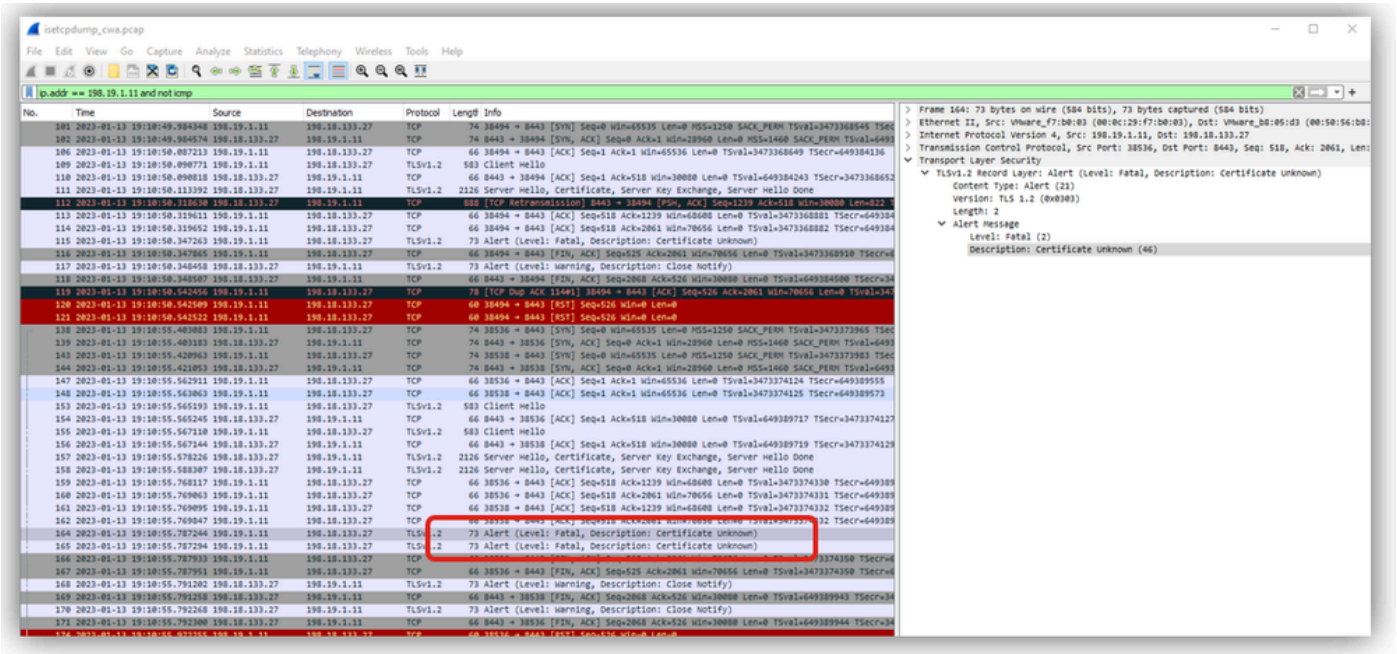
WLC- en ISE-verkeer

11 - Waarom krijgen we een beveiligingsschending vanwege een certificaat?

Als u een zelf ondertekend certificaat op ISE gebruikt, wordt verwacht dat de client een beveiligingswaarschuwing geeft wanneer deze probeert de ISE-portaalaanmeldingspagina te presenteren.

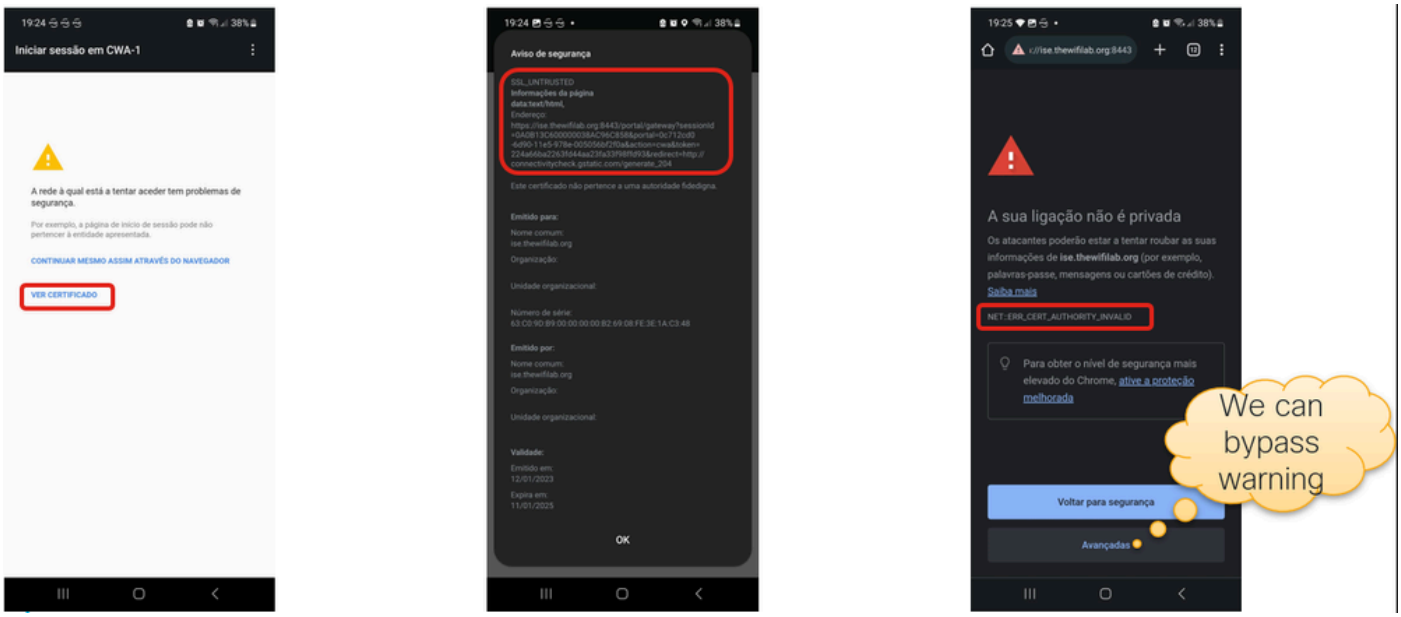
Op de WLC EPC of ISE TCPdump kunnen we controleren of het ISE-certificaat vertrouwd is.

In dit voorbeeld zien we een nauwe verbinding van Client met Alert (Level: Fatal, Description: certificate Unknown), wat betekent dat het ISE-certificaat niet bekend is (Trusted):



ISE niet-vertrouwd certificaat

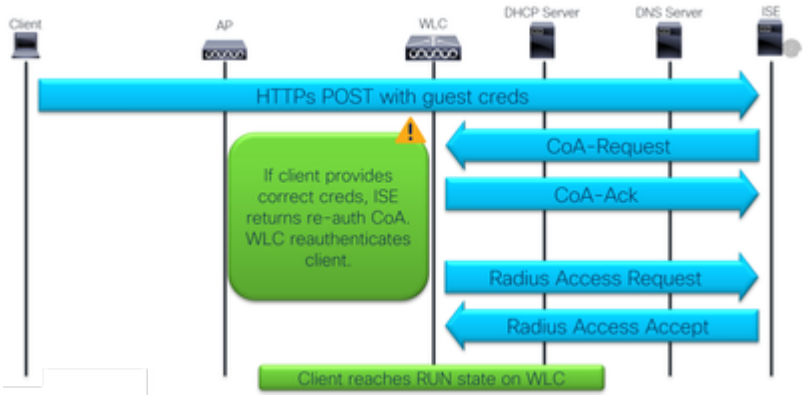
Als we aan de kant van de klant controleren, zien we deze voorbeelden:



Clientapparaat dat het ISE-certificaat niet vertrouwt

Eindelijk, redirection werkt!! Inloggen mislukt...

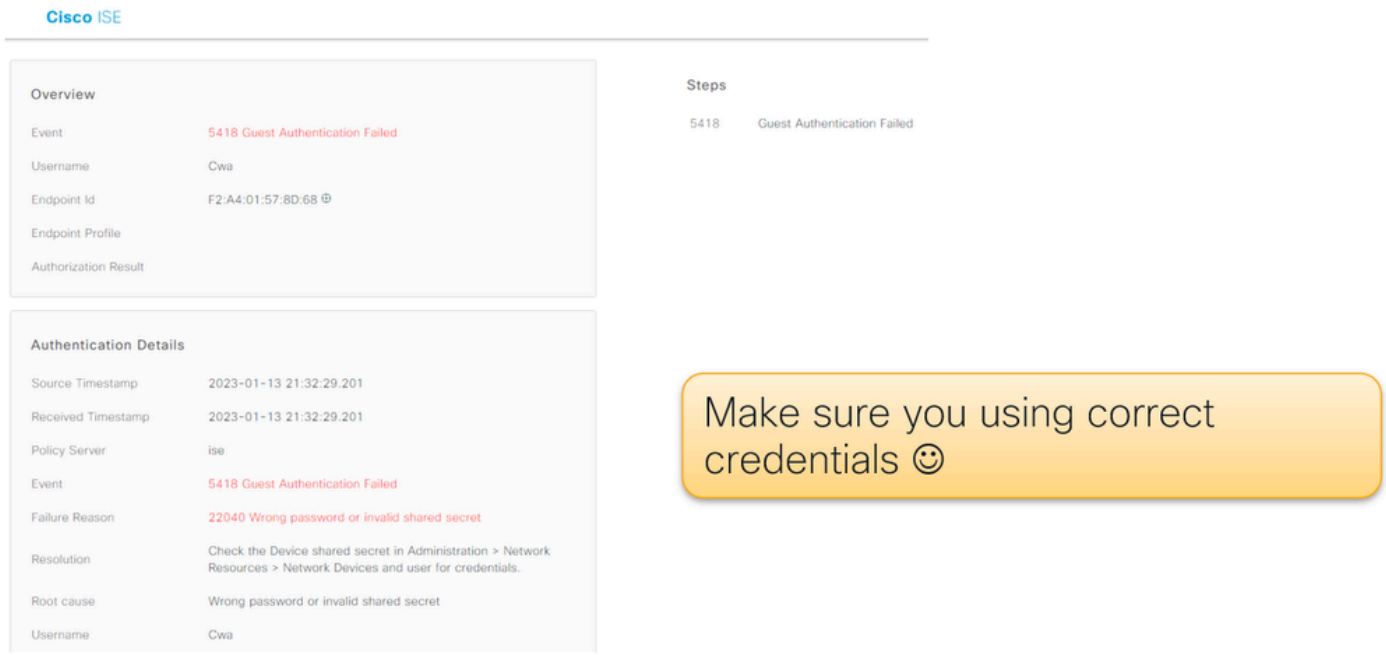
Nog een laatste keer de flow checken...



Client login en CoA

12 - Login van gast mislukt?

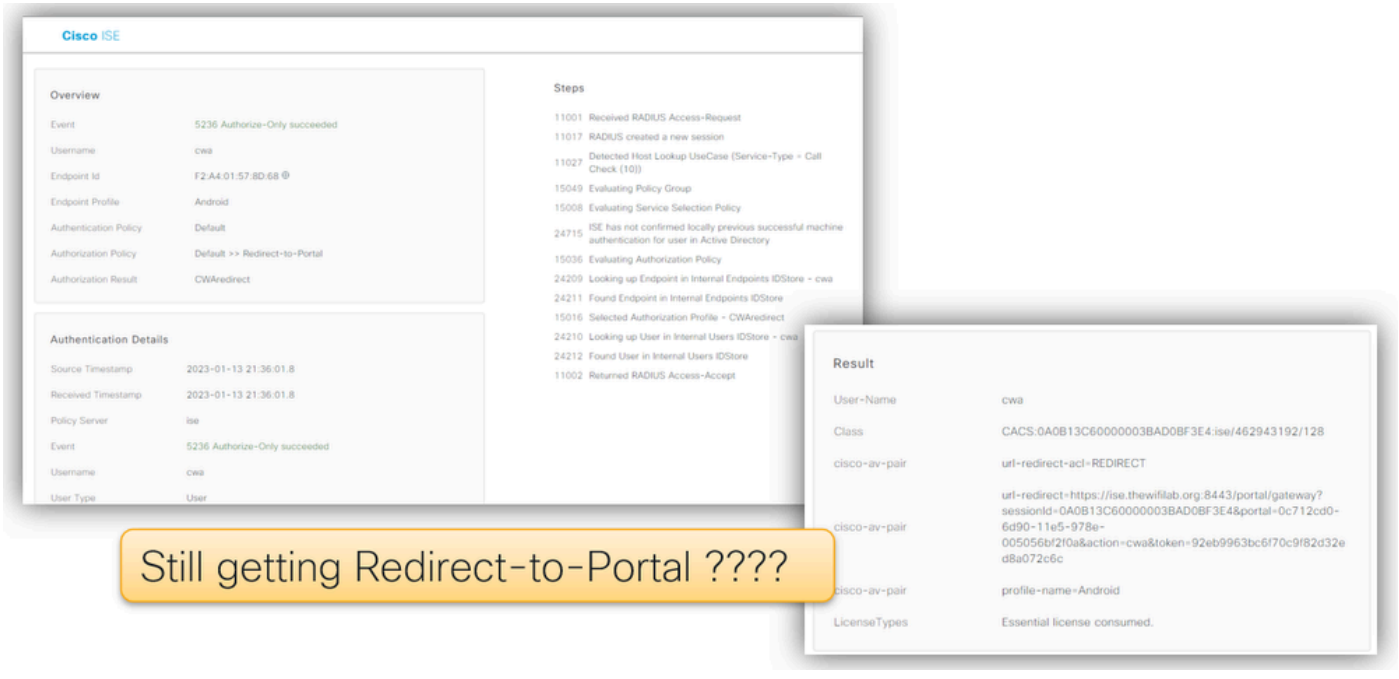
Controleer ISE-logs op mislukte verificatie. Controleer of de referenties juist zijn.



Gastverificatie mislukt door verkeerde referenties

13 - Login geslaagd maar niet verplaatsen naar RUN?

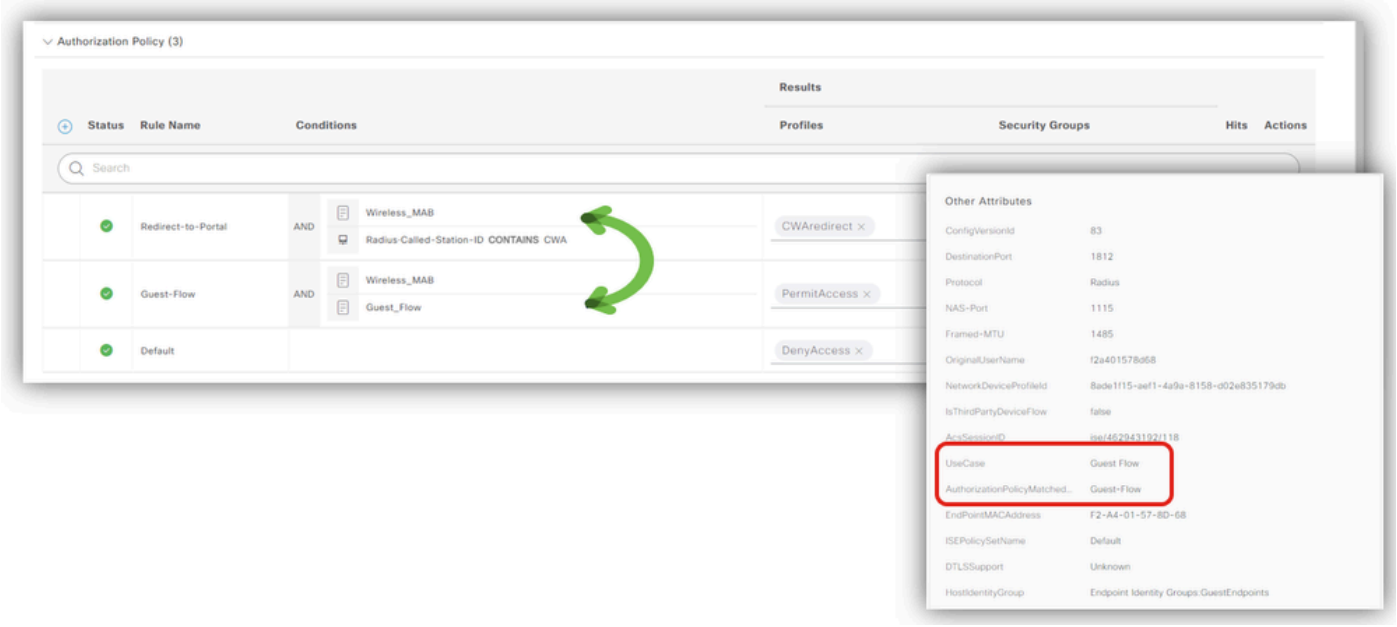
Controleer ISE-logs voor verificatiedetails en resultaat:



Omleidingslus

In dit voorbeeld kunnen we zien dat de client opnieuw het autorisatieprofiel krijgt dat de Redirect URL en Redirect ACL bevat. Dit resulteert in een omleiding.

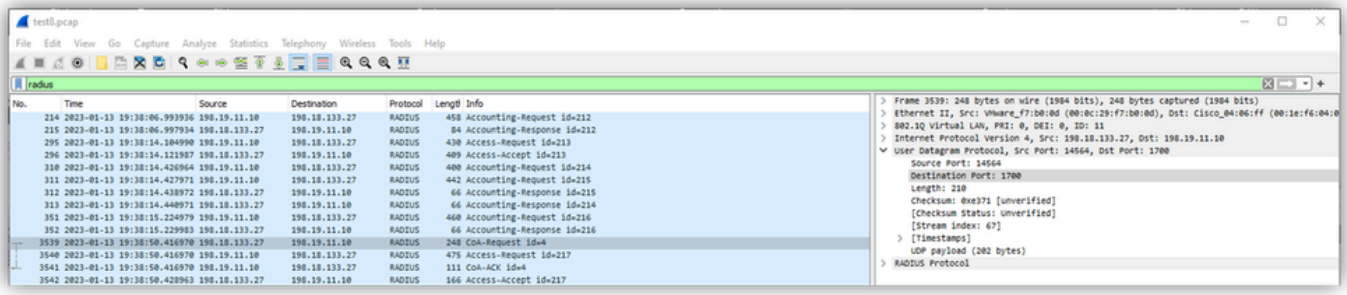
Beleid controleren ingesteld. Regelcontrole Guest_Flow moet vóór de omleiding zijn:



regel Guest_Flow

14 - COA faalt?

Met EPC en ISE TCPDump kunnen we CoA-verkeer verifiëren. Controleer of de CoA-poort (1700) is geopend tussen WLC en ISE. Zorg voor gedeelde geheime matches.



CoA-verkeer

Opmerking: zorg er bij versie 17.4.X en hoger voor dat u ook de CoA-serversleutel configureert wanneer u de RADIUS-server configureert. Gebruik dezelfde sleutel als het gedeelde geheim (ze zijn standaard hetzelfde op ISE). Het doel is om optioneel een andere sleutel voor CoA te configureren dan het gedeelde geheim als dat is wat uw RADIUS-server heeft geconfigureerd. In Cisco IOS® XE 17.3 gebruikte de web-gebruikersinterface gewoon hetzelfde gedeelde geheim als de CoA-sleutel.

Vanaf versie 17.6.1 wordt RADIUS (inclusief CoA) ondersteund via deze poort. Als u de servicepoort voor RADIUS wilt gebruiken, hebt u deze configuratie nodig:

<#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
```

Conclusie

Dit is de CWA checklist:

- Zorg ervoor dat de client op het juiste VLAN zit en het IP-adres en DNS krijgt.

    - Krijg klantgegevens bij WLC en voer pakketopnames uit om DHCP-uitwisseling te zien.
- Controleer of de client hostnamen via DNS kan oplossen.
    - Ping-hostnaam van cmd.
- WLC moet luisteren op poort 80
    - Verifieer global command ip http server of global parameter map command webauth-http-enable.
- Installeer een vertrouwd certificaat op ISE om de certificaatwaarschuwing te verwijderen.
    - U hoeft geen vertrouwd certificaat op WLC in CWA te installeren.
- Verificatiebeleid bij ISE Advanced optie "Doorgaan" Als gebruiker niet wordt gevonden
    - Om gesponsorde gastgebruikers in staat te stellen verbinding te maken en URL-redirect en ACL te krijgen.

En de belangrijkste hulpmiddelen die worden gebruikt bij het oplossen van problemen:

- WLC EPC
    - Binnenfilters: DHCP-protocol, MAC-adres.
- WLC-monitor
    - Controleer de beveiligingsgegevens van de client.
- WLC RA-tracering
    - Debugs met gedetailleerde informatie aan de WLC-kant.
- ISE Live Logs
    - Authenticatiegegevens.
- ISE TCPDump
    - Verzamel pakketopnames op de ISE PSN-interface.

Referenties

Centrale webverificatie (CWA) configureren op Catalyst 9800 WLC en ISE

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.