

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

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Gedetailleerde flow](#)

[Probleemoplossing](#)

[Algemeen symptoom: gebruiker wordt niet doorgestuurd naar aanmeldpagina.](#)

[1 - Is de eerste RADIUS-verificatie succesvol?](#)

[2 - WLC ontvangt de Redirect URL en ACL?](#)

[3 - Is de omleiding ACL correct?](#)

[4 - Is de client verplaatst naar Web-Auth in afwachting?](#)

[5 - Staat WLC DHCP- en DNS-verkeer toe?](#)

[6 - Ontvangt de DHCP-server DHCP Discover/Request?](#)

[7 - Gebeurt automatische omleiding?](#)

[8 - Browser toont geen inlogpagina?](#)

[9 - Kan de client de ISE-hostnaam oplossen?](#)

[10 - Login pagina nog steeds niet geladen?](#)

[11 - Waarom krijgen we een beveiligingsschending vanwege een certificaat?](#)

[12 - Login van gast mislukt?](#)

[13 - Login geslaagd maar niet verplaatsen naar RUN?](#)

[14 - COA faalt?](#)

[Conclusie](#)

[Referenties](#)

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.

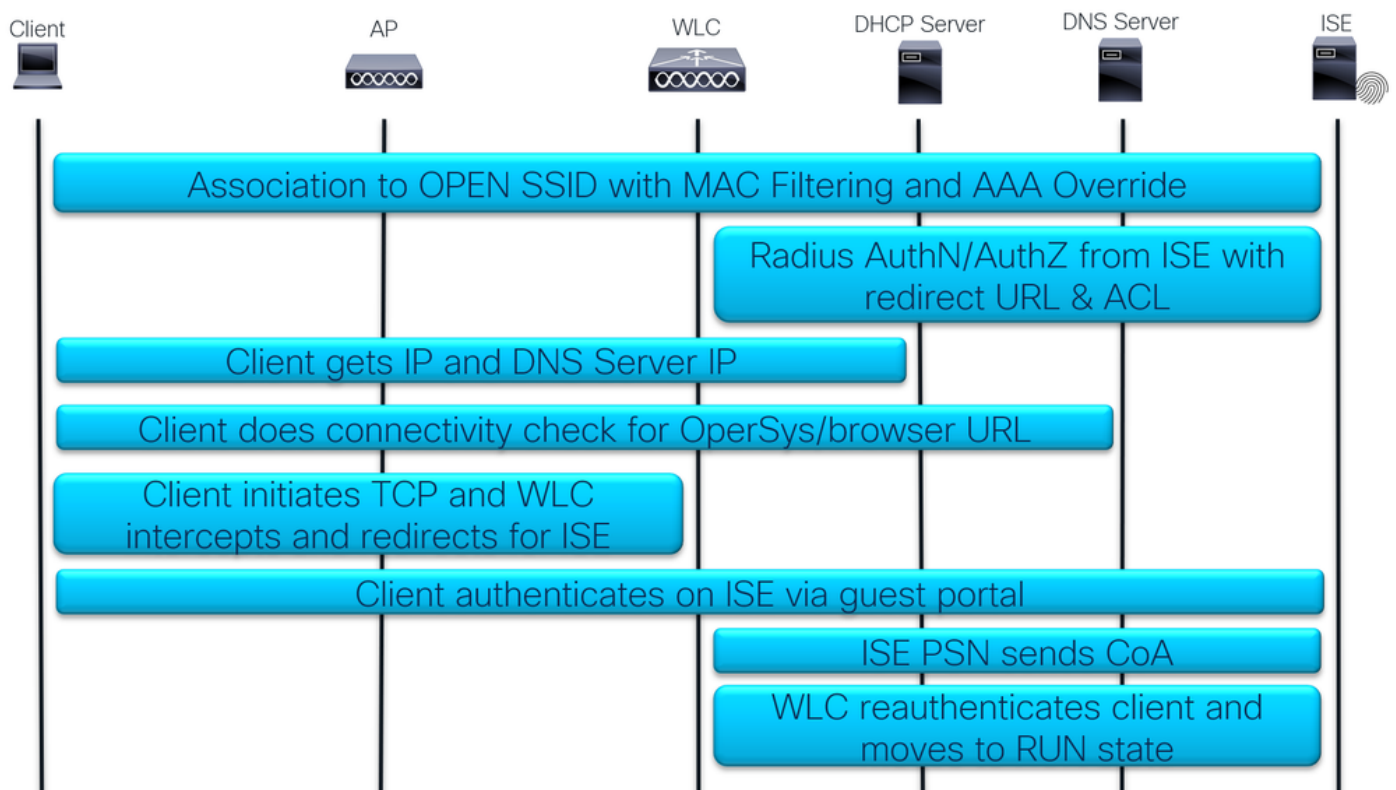
We kijken naar de gemeenschappelijke gotchas van het proces, hoe logs met betrekking tot CWA

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.

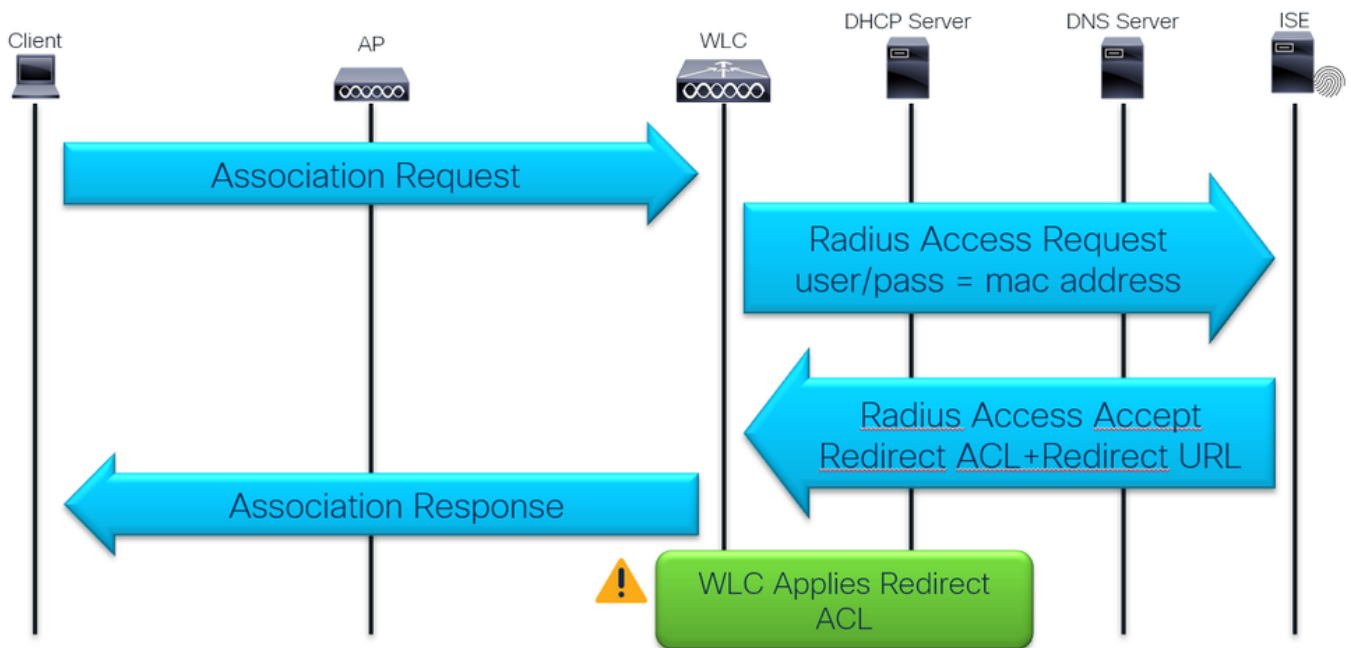
Hier is de CWA-pakketstroom:



CWA-pakketstroom

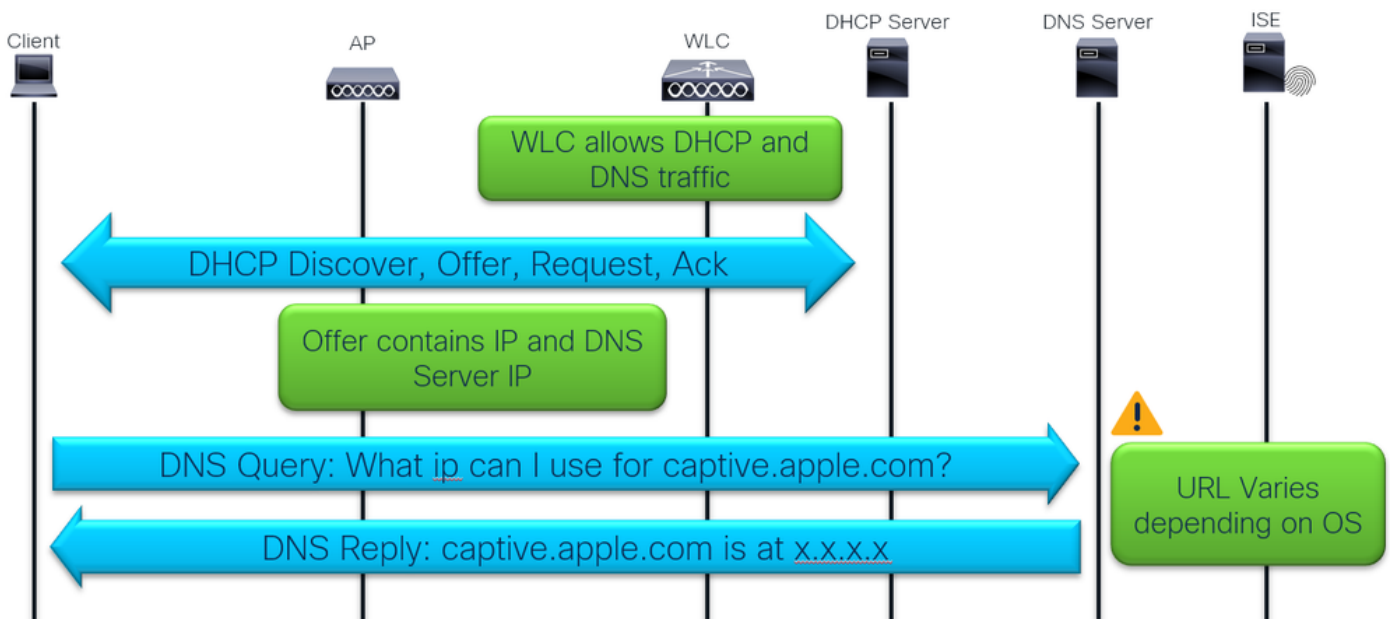
Gedetailleerde flow

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.

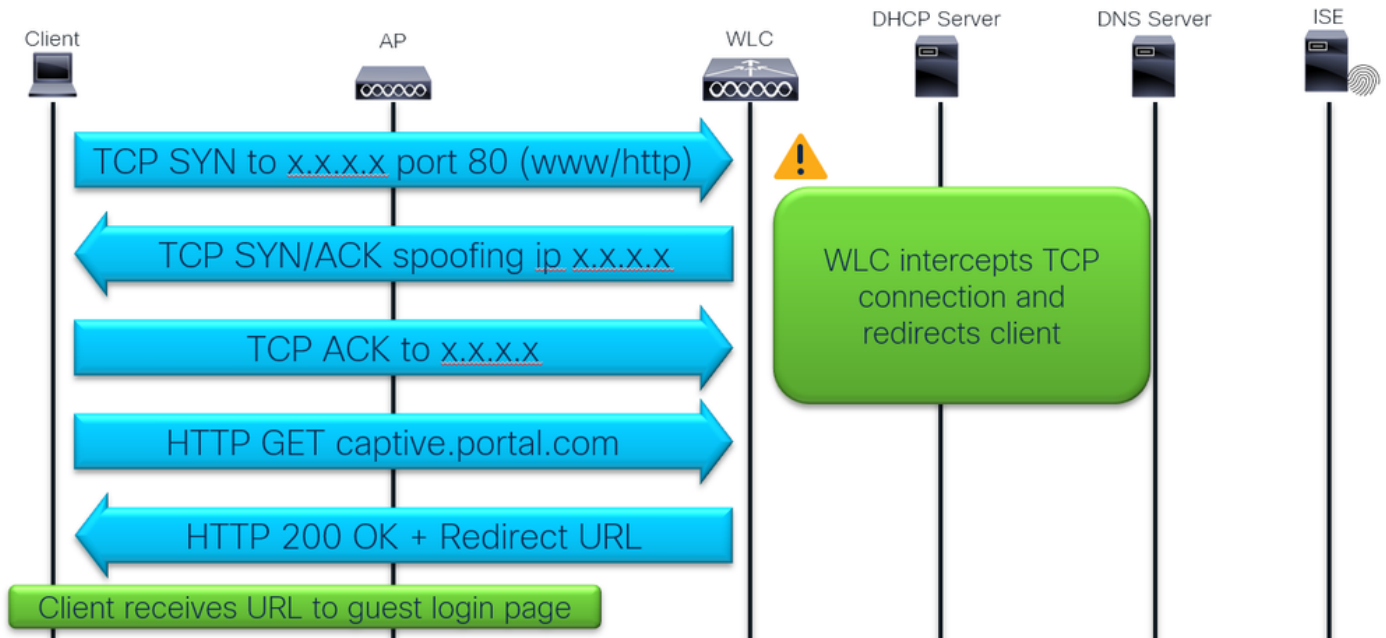
Er zijn voorgeprogrammeerde besturingssystemen voor apparaten om HTTP GET naar een specifiek domein uit te voeren

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

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

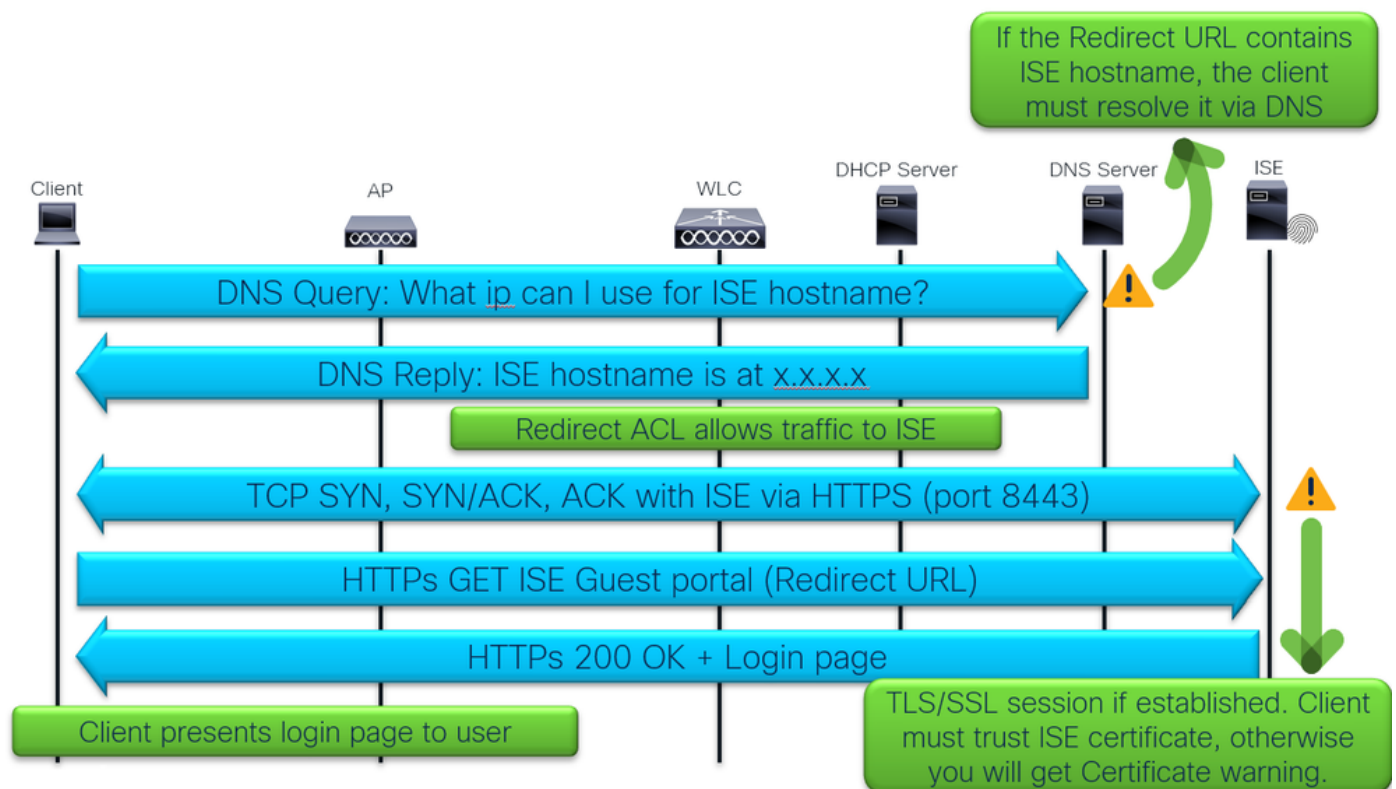
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Interceptie en omleiding van het verkeer:



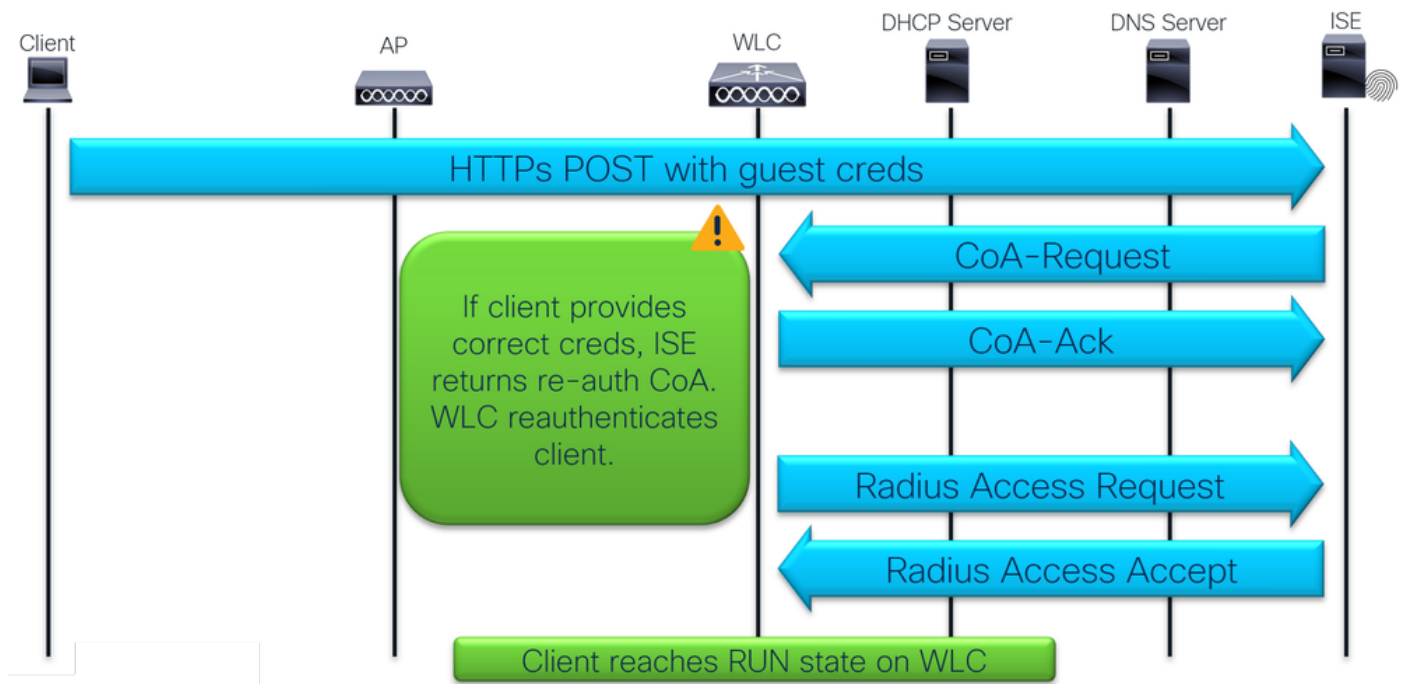
Interceptie en omleiding van het verkeer

Client login in ISE guest login portal:



Client login in ISE guest login portal

Client login en CoA:

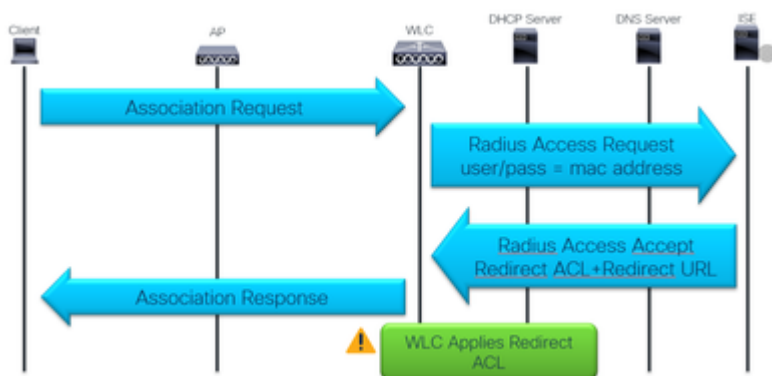


Client login en CoA

Probleemoplossing

Algemeen symptoom: gebruiker wordt niet doorgestuurd naar aanmeldpagina.

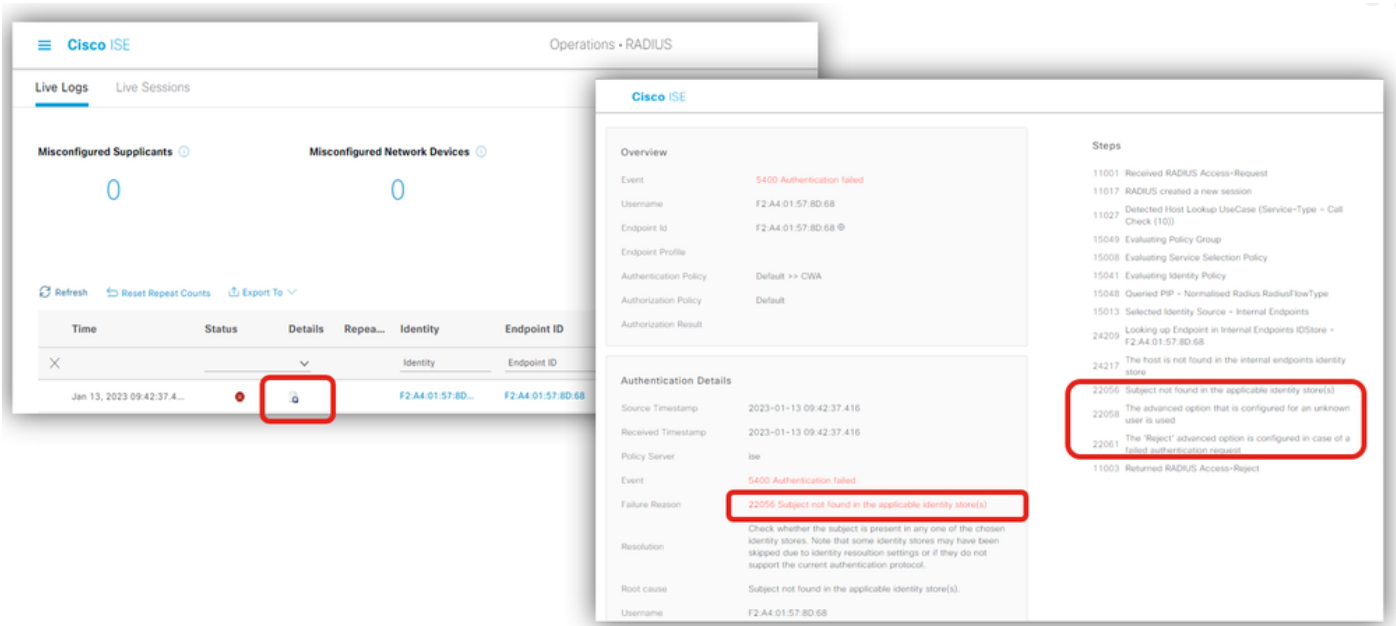
Laten we beginnen met het eerste deel van de flow:



Eerste associatie en RADIUS-verificatie

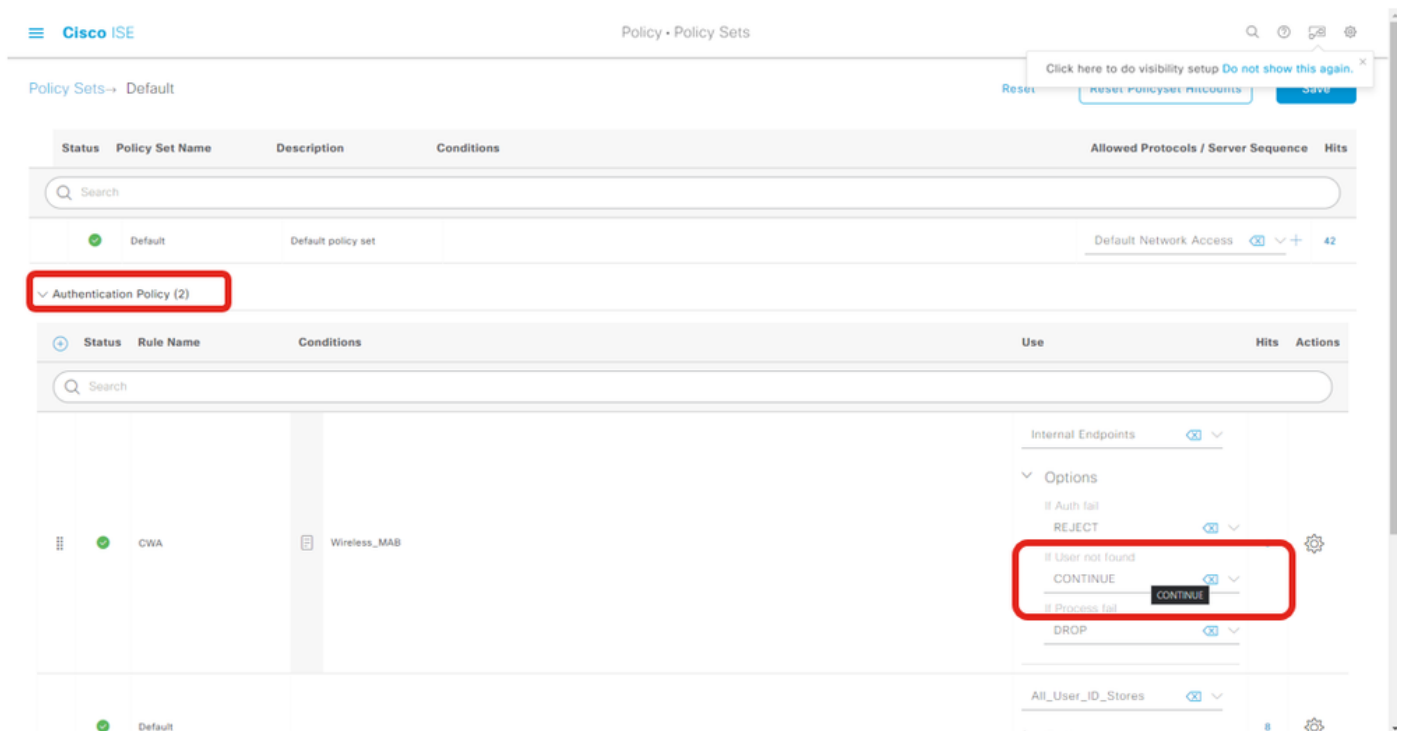
1 - Is de eerste RADIUS-verificatie succesvol?

Controleer het verificatieresultaat van de mac-filtering:



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

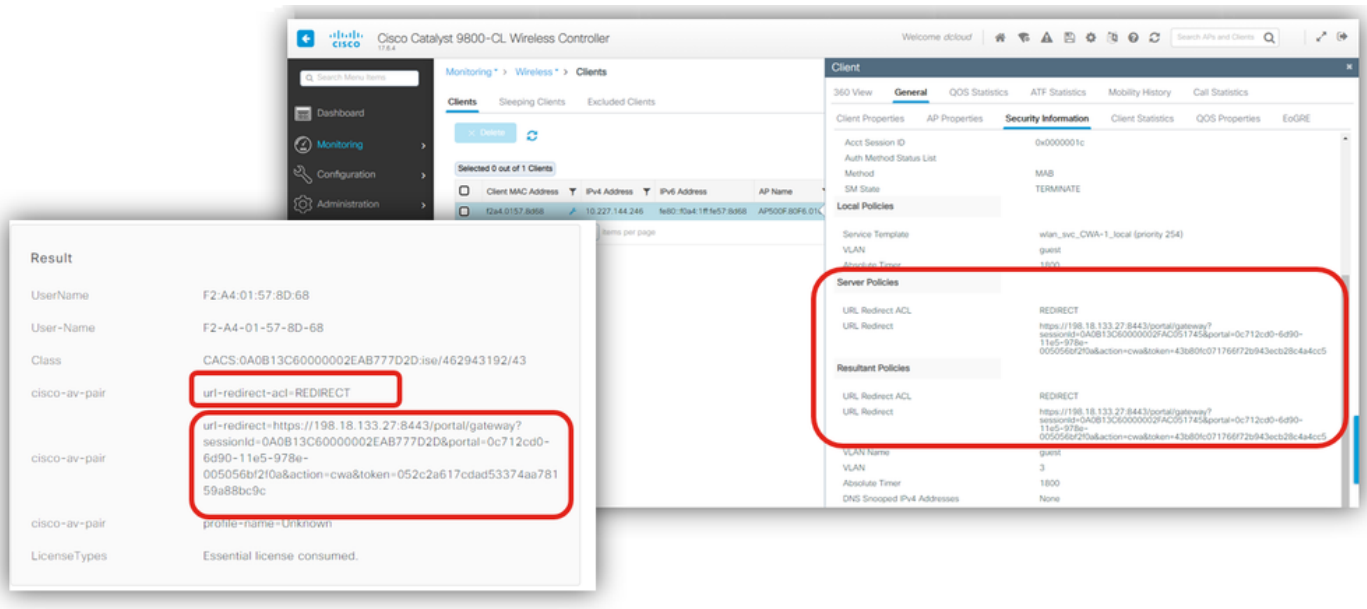
Zorg ervoor dat de geavanceerde optie voor de verificatie is ingesteld op "Doorgaan" als de gebruiker niet wordt gevonden:



Gebruiker niet gevonden geavanceerde optie

2 - WLC ontvangt de Redirect URL en ACL?

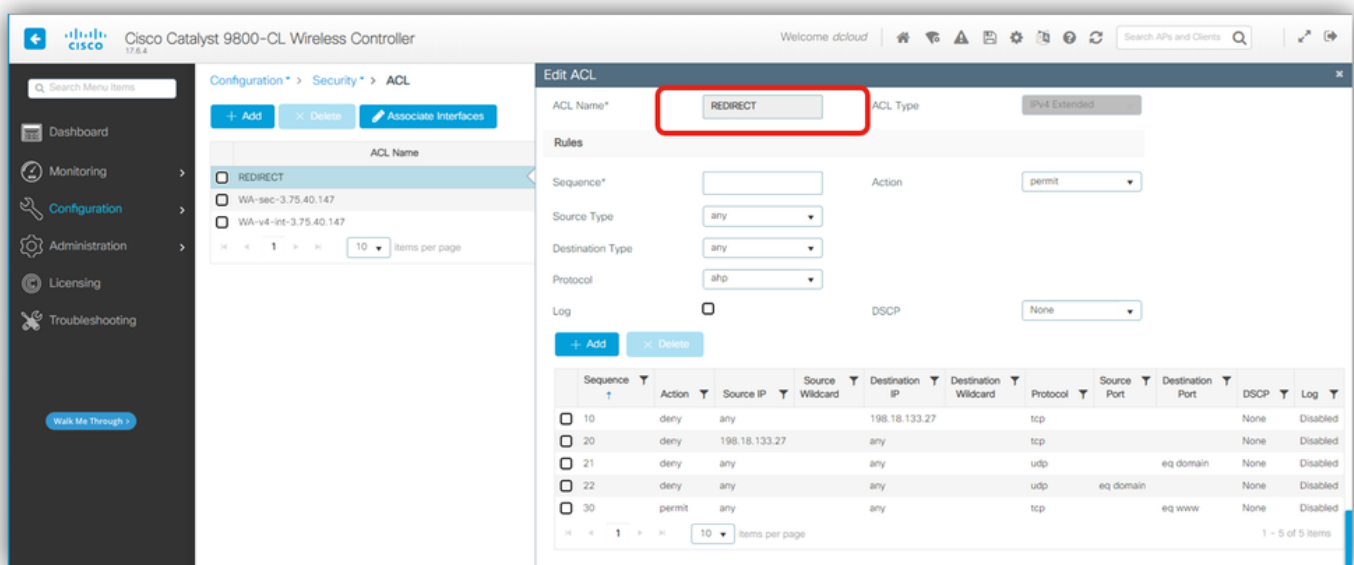
Controleer ISE live-logs en WLC-clientbeveiligingsinformatie onder Bewaken Controleer of de ISE Redirect-URL en ACL in de toegangsacceptatie worden verzonden en door WLC worden ontvangen en op de client worden toegepast in de clientgegevens:



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:

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
☒

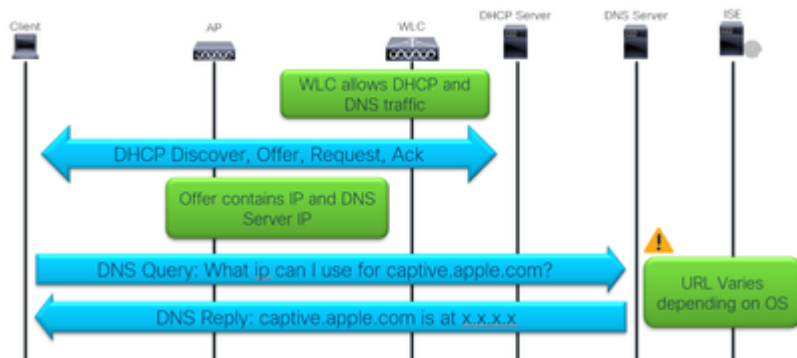
NAC State
☒

NAC Type
RADIUS

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:

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
permit

Source Type
any

Destination Type
any

Protocol
http

Log
☐
DSCP
None

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

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:

Inner filters !!

Sent as broadcast on VLAN 3

WLC EPC om DHCP te verifiëren

Bevestig het verwachte client-VLAN in het beleidsprofiel:

VLAN

VLAN/VLAN Group: guest

Multicast VLAN: Enter Multicast VLAN

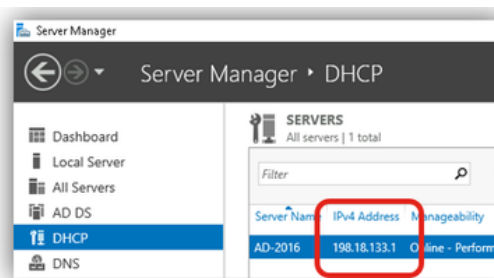
WLC VLAN- en switchport Trunk-configuratie en DHCP-subnet controleren:

```
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                     unassigned    YES NVRAM  up        up
Vlan2                     198.19.2.2    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, 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.

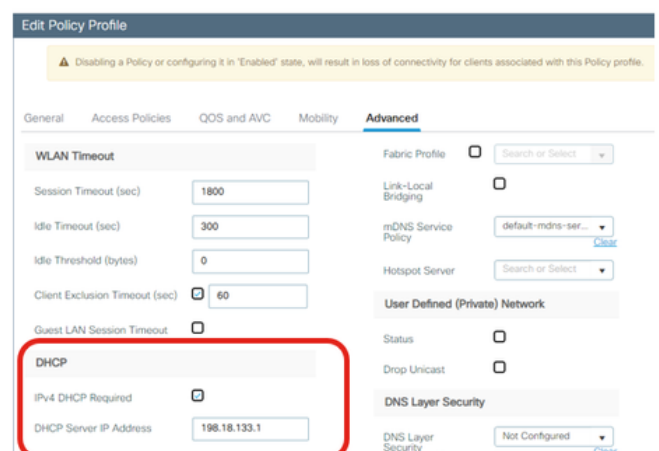
Best practices schrijven voor dat SVI voor clientsubnetten in de bekabelde infrastructuur moet worden geconfigureerd en bij de WLC moet worden vermeden.

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:

```
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

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

Full DHCP exchange and DHCP server offering IP and DNS servers

DHCP Aanbieding details van DNS server ip

7 - Gebeurt automatische omleiding?

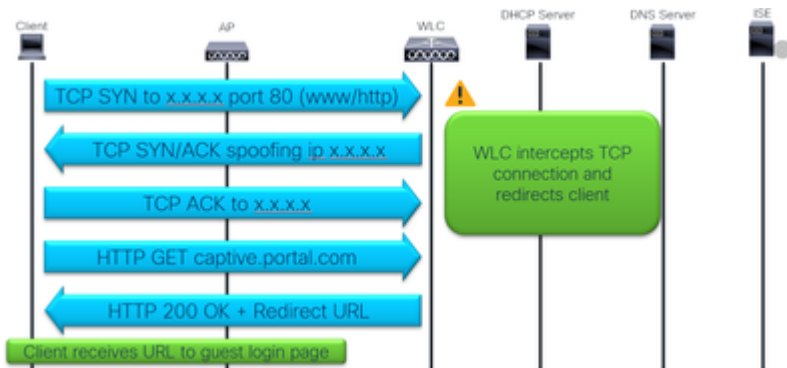
Controleer met WLC EPC of de DNS-server de volgende vragen beantwoordt:

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

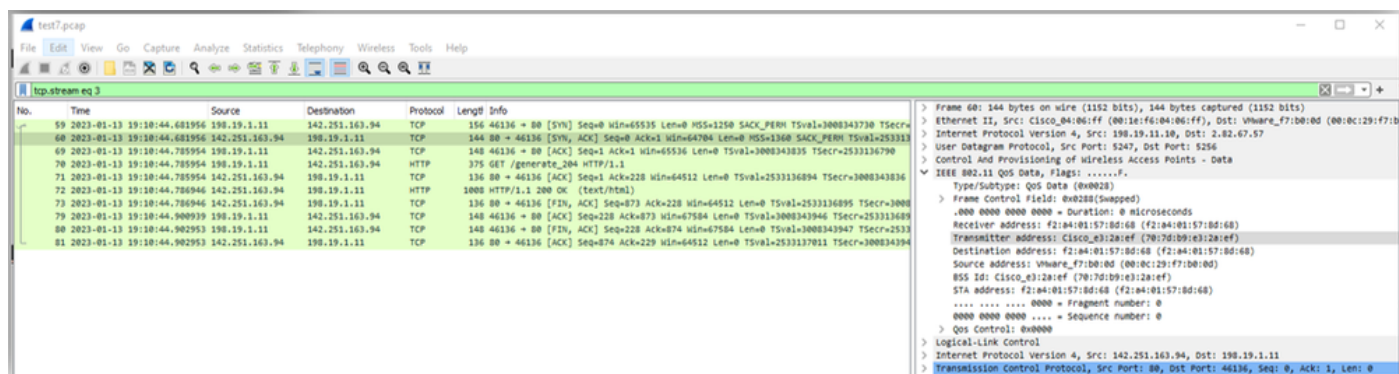
Hier kunnen we zien dat de client TCP SYN-pakketten naar poort 80 stuurt, maar geen antwoord krijgt en TCP-hertransmissies uitvoert.

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

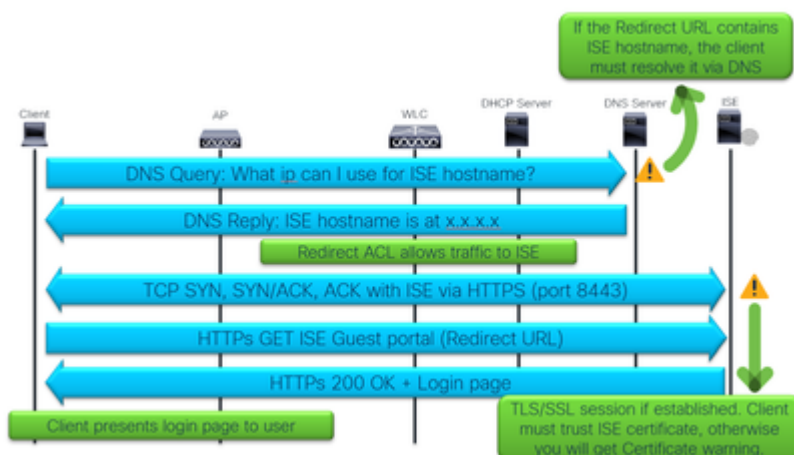
reageren op de client en om te leiden.



TCP-interceptie door WLC

Nog steeds niet werken?

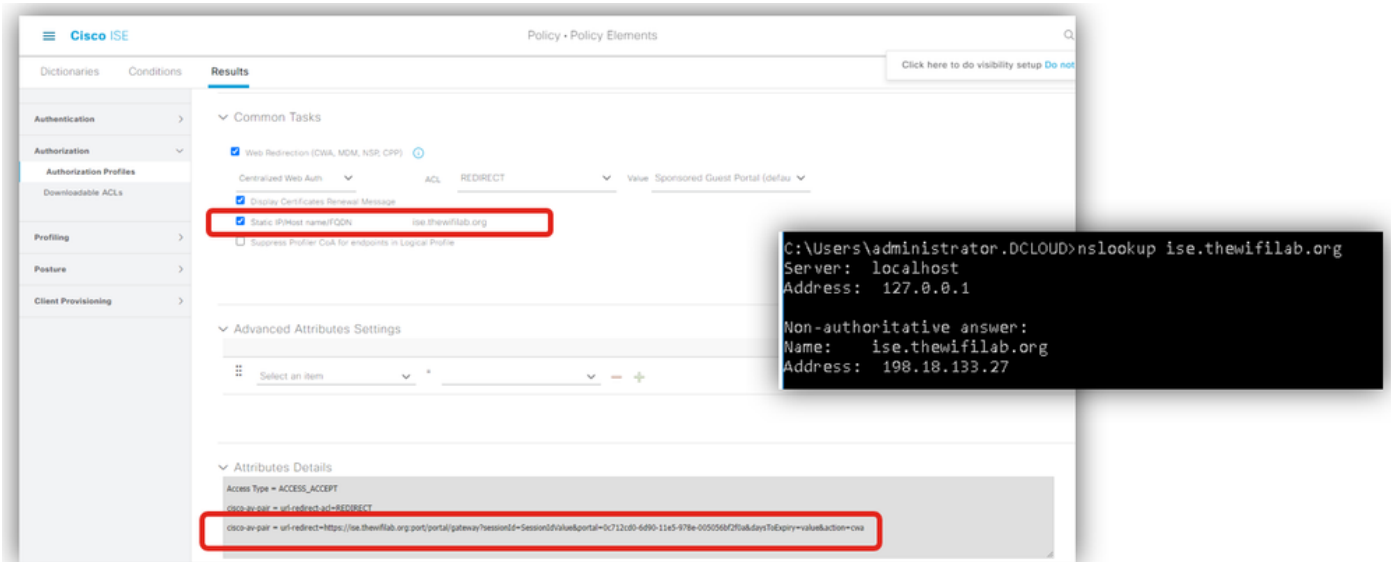
Er zit meer in de flow...



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:

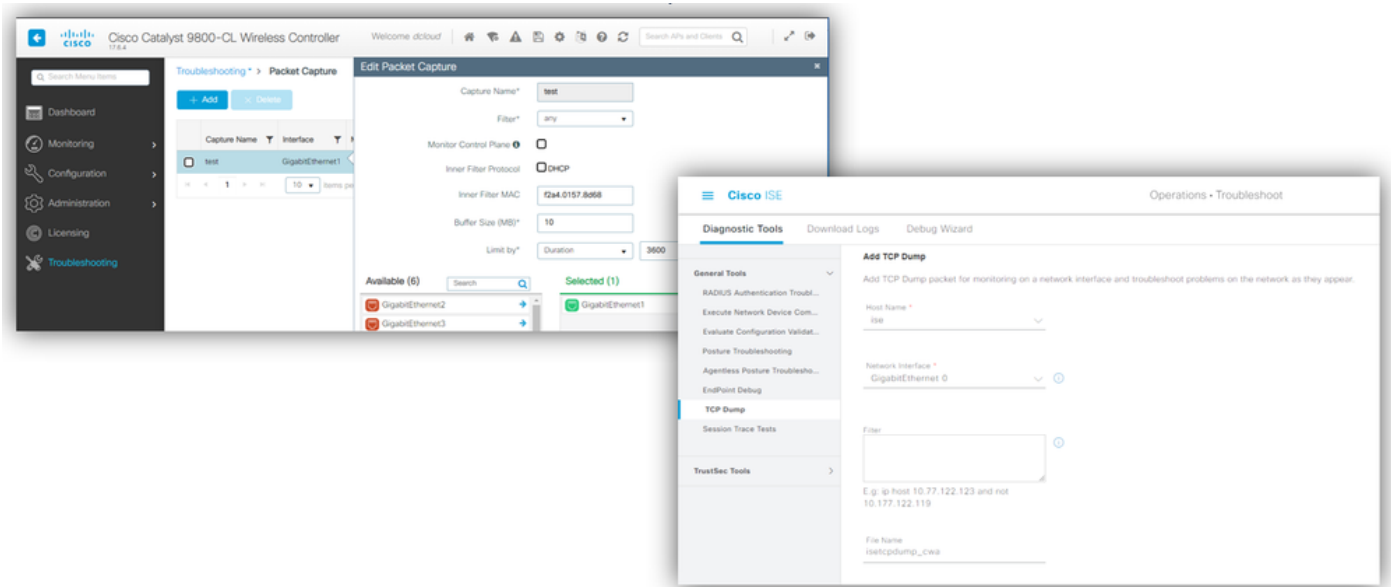


ISE Hostname-resolutie

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.

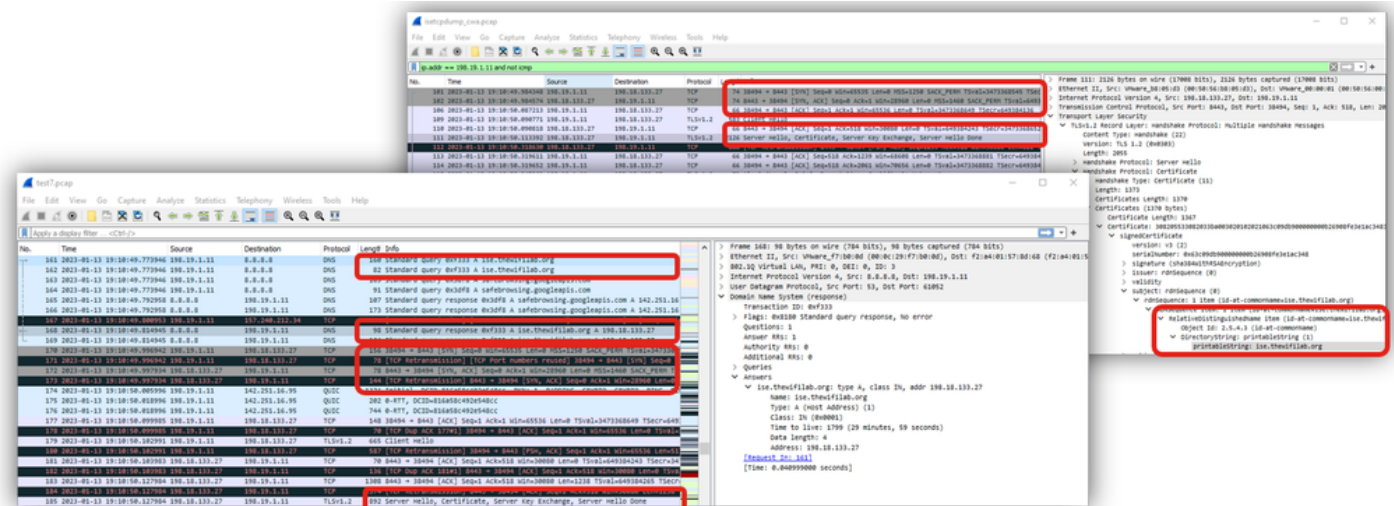
10 - Login pagina nog steeds niet geladen?

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:



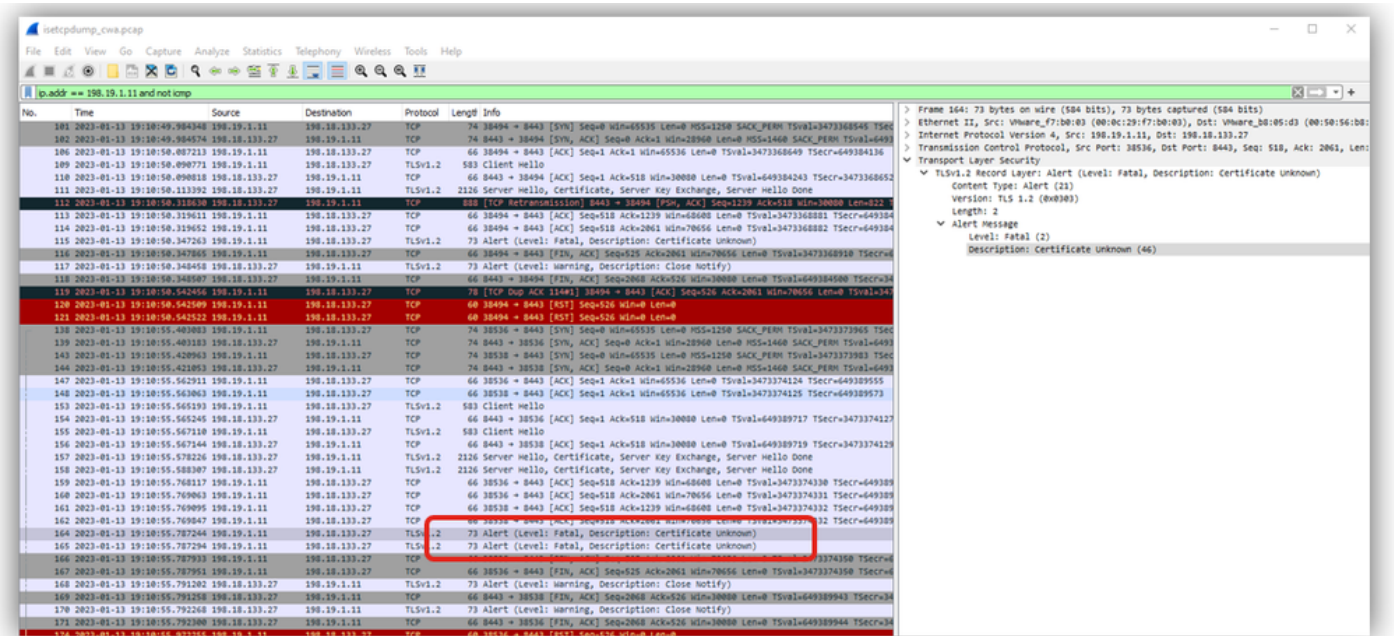
WLC- en ISE-verkeer

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.

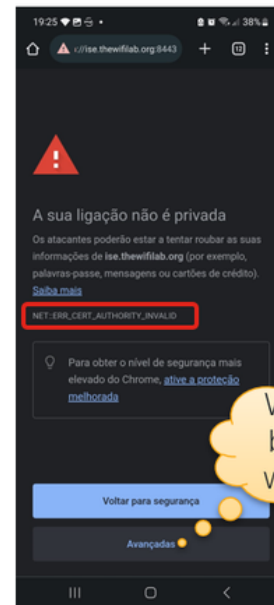
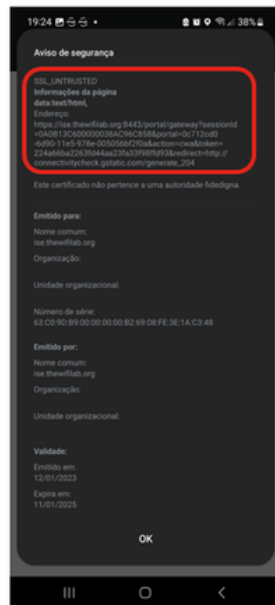
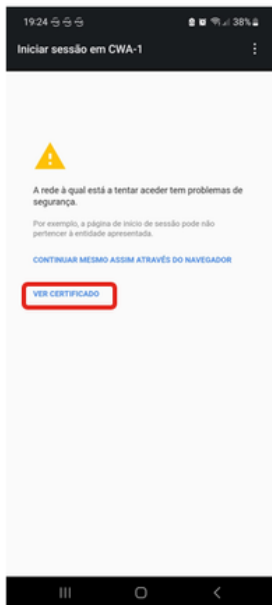
Op de WLC EPC of ISE TCPdump kunnen we controleren of het ISE-certificaat vertrouwd is.

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

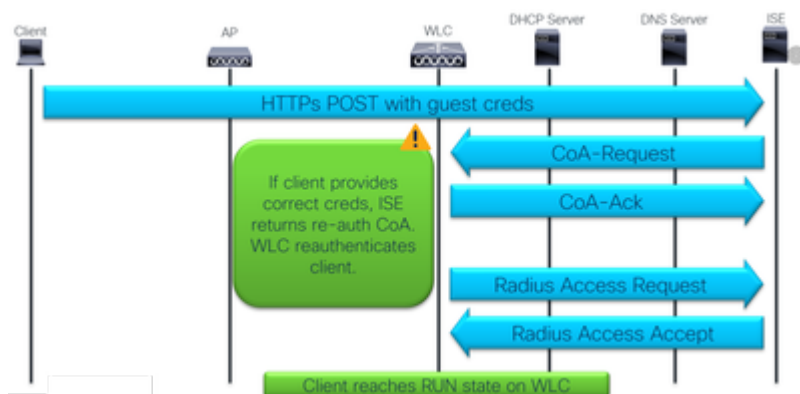
Als we aan de kant van de klant controleren, zien we deze voorbeelden:



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.

Overview	
Event	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

Steps	
5418	Guest Authentication Failed

Make sure you using correct credentials 😊

Gastverificatie mislukt door verkeerde referenties

13 - Login geslaagd maar niet verplaatsen naar RUN?

Controleer ISE-logs voor verificatiedetails en resultaat:

Cisco ISE																																																																										
<table border="1"> <thead> <tr> <th colspan="2">Overview</th> </tr> </thead> <tbody> <tr> <td>Event</td> <td>5236 Authorize-Only succeeded</td> </tr> <tr> <td>Username</td> <td>cwa</td> </tr> <tr> <td>Endpoint Id</td> <td>F2:A4:01:57:8D:68 @</td> </tr> <tr> <td>Endpoint Profile</td> <td>Android</td> </tr> <tr> <td>Authentication Policy</td> <td>Default</td> </tr> <tr> <td>Authorization Policy</td> <td>Default >> Redirect-to-Portal</td> </tr> <tr> <td>Authorization Result</td> <td>CWARedirect</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">Authentication Details</th> </tr> </thead> <tbody> <tr> <td>Source Timestamp</td> <td>2023-01-13 21:36:01.8</td> </tr> <tr> <td>Received Timestamp</td> <td>2023-01-13 21:36:01.8</td> </tr> <tr> <td>Policy Server</td> <td>ise</td> </tr> <tr> <td>Event</td> <td>5236 Authorize-Only succeeded</td> </tr> <tr> <td>Username</td> <td>cwa</td> </tr> <tr> <td>User Type</td> <td>User</td> </tr> </tbody> </table>		Overview		Event	5236 Authorize-Only succeeded	Username	cwa	Endpoint Id	F2:A4:01:57:8D:68 @	Endpoint Profile	Android	Authentication Policy	Default	Authorization Policy	Default >> Redirect-to-Portal	Authorization Result	CWARedirect	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	<table border="1"> <thead> <tr> <th colspan="2">Steps</th> </tr> </thead> <tbody> <tr> <td>11001</td> <td>Received RADIUS Access-Request</td> </tr> <tr> <td>11017</td> <td>RADIUS created a new session</td> </tr> <tr> <td>11027</td> <td>Detected Host Lookup UseCase (Service-Type = Call Check (10))</td> </tr> <tr> <td>15049</td> <td>Evaluating Policy Group</td> </tr> <tr> <td>15008</td> <td>Evaluating Service Selection Policy</td> </tr> <tr> <td>24715</td> <td>ISE has not confirmed locally previous successful machine authentication for user in Active Directory</td> </tr> <tr> <td>15036</td> <td>Evaluating Authorization Policy</td> </tr> <tr> <td>24209</td> <td>Looking up Endpoint in Internal Endpoints IDStore - cwa</td> </tr> <tr> <td>24211</td> <td>Found Endpoint in Internal Endpoints IDStore</td> </tr> <tr> <td>15016</td> <td>Selected Authorization Profile - CWARedirect</td> </tr> <tr> <td>24210</td> <td>Looking up User in Internal Users IDStore - cwa</td> </tr> <tr> <td>24212</td> <td>Found User in Internal Users IDStore</td> </tr> <tr> <td>11002</td> <td>Returned RADIUS Access-Accept</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="2">Result</th> </tr> </thead> <tbody> <tr> <td>User-Name</td> <td>cwa</td> </tr> <tr> <td>Class</td> <td>CACS:0A0B13C60000003BAD0BF3E4:ise/462943192/128</td> </tr> <tr> <td>cisco-av-pair</td> <td>url-redirect-acl=REDIRECT</td> </tr> <tr> <td>cisco-av-pair</td> <td>url-redirect=https://ise.thewifilab.org.8443/portal/gateway?sessionId=0A0B13C60000003BAD0BF3E4&portal=0c712cd0-6d90-11e5-978e-005056b2f0a&action=cwa&token=92eb9963bc6f70c9f82d32ed8a072c6c</td> </tr> <tr> <td>cisco-av-pair</td> <td>profile-name=Android</td> </tr> <tr> <td>LicenseTypes</td> <td>Essential license consumed.</td> </tr> </tbody> </table>	Steps		11001	Received RADIUS Access-Request	11017	RADIUS created a new session	11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))	15049	Evaluating Policy Group	15008	Evaluating Service Selection Policy	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	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	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.
Overview																																																																										
Event	5236 Authorize-Only succeeded																																																																									
Username	cwa																																																																									
Endpoint Id	F2:A4:01:57:8D:68 @																																																																									
Endpoint Profile	Android																																																																									
Authentication Policy	Default																																																																									
Authorization Policy	Default >> Redirect-to-Portal																																																																									
Authorization Result	CWARedirect																																																																									
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																																																																									
Steps																																																																										
11001	Received RADIUS Access-Request																																																																									
11017	RADIUS created a new session																																																																									
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))																																																																									
15049	Evaluating Policy Group																																																																									
15008	Evaluating Service Selection Policy																																																																									
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory																																																																									
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																																																																									
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 ????

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:

Authorization Policy (3)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Redirect-to-Portal	AND Wireless_MAB Radius Called-Station-ID CONTAINS CWA	CWRedirect x			
✓	Guest-Flow	AND Wireless_MAB Guest_Flow	PermitAccess x			
✓	Default		DenyAccess x			

Other Attributes

ConfigVersionId	83
DestinationPort	1812
Protocol	Radius
NAS-Port	1115
Framed-MTU	1485
OriginalUserName	f2a401578a68
NetworkDeviceProfileId	8ade1115-aef1-4a9a-8158-002e835179db
IsThirdPartyDeviceFlow	false
AcctSourceId	10a12523a311021118
UseCase	Guest-Flow
AuthorizationPolicyMatched...	Guest-Flow
EndPointMACAddress	F2-A4-01-57-8D-68
ISEPolicySetName	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:GuestEndpoints

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.

Wireshark packet capture showing RADIUS and CoA traffic. The packet list shows several RADIUS Accounting-Request and Accounting-Response packets. The packet details pane shows a CoA-Request packet (ID=4) with a destination port of 1700.

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 TCPCDump
 - 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.