

Resolución de problemas de autenticación web central (CWA) con el controlador de LAN inalámbrica (WLC) 9800 e Identity Services Engine (ISE)

Contenido

[Introducción](#)

[Información de fondo](#)

[Flujo detallado](#)

[Resolución de problemas](#)

[Síntoma frecuente: El usuario no es redirigido a la página de inicio de sesión.](#)

- [1 - ¿La primera autenticación RADIUS es exitosa?](#)
- [2 - ¿El WLC recibe la URL y la ACL de redireccionamiento?](#)
- [3 - ¿Es correcta la ACL de redirección?](#)
- [4 - ¿Está pendiente el traslado del cliente a Web-Auth?](#)
- [5 - ¿El WLC permite el tráfico DHCP y DNS?](#)
- [6 - ¿El servidor DHCP recibe la detección/solicitud de DHCP?](#)
- [7 - ¿Se produce la redirección automática?](#)
- [8 - ¿El navegador no muestra la página de inicio de sesión?](#)
- [9 - ¿Puede el cliente resolver el nombre de host de ISE?](#)
- [10 - ¿La página de inicio de sesión sigue sin cargarse?](#)
- [11 - ¿Por qué se produce una violación de la seguridad debido al certificado?](#)
- [12 - ¿Falla el inicio de sesión de invitado?](#)
- [13 - ¿Se ha iniciado sesión correctamente pero no se ha movido a RUN?](#)
- [14 - ¿Falla el COA?](#)

[Conclusión](#)

[Referencias](#)

Introducción

Este documento describe cómo resolver problemas de autenticación web central (CWA) con WLC 9800 e ISE.

Información de fondo

En la actualidad, hay tantos dispositivos personales que los administradores de red que buscan garantizar la seguridad del acceso inalámbrico optan normalmente por redes inalámbricas que utilizan CWA.

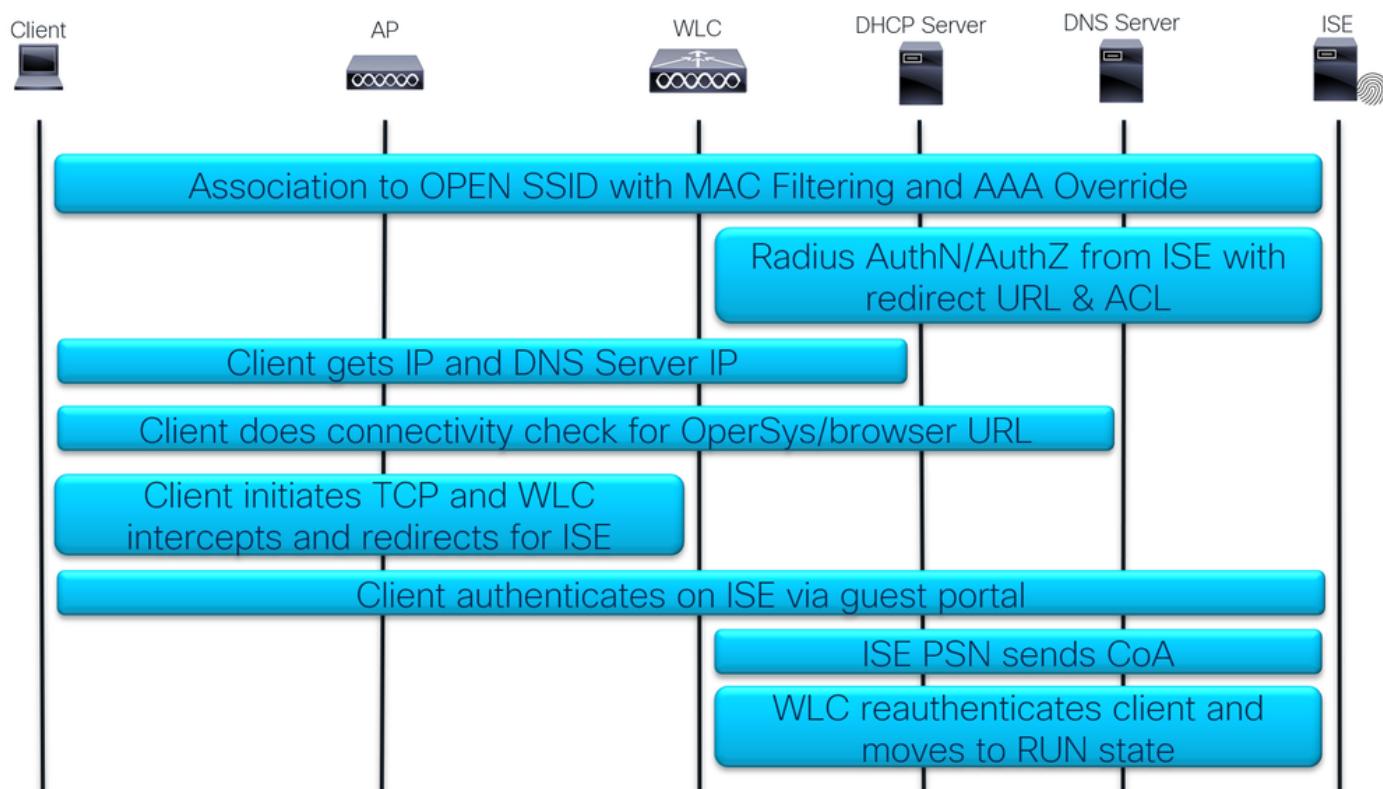
En este documento, nos centramos en el diagrama de flujo de CWA, que ayuda en la resolución de problemas comunes que nos afectan.

Observamos las trampas comunes del proceso, cómo recolectar registros relacionados con CWA,

cómo analizar estos registros, y cómo recolectar una captura de paquetes embebida en el WLC para confirmar el flujo de tráfico.

CWA es la configuración más común para las empresas que permite a los usuarios conectarse a la red de la empresa mediante sus dispositivos personales, también conocidos como BYOD. Cualquier administrador de red está interesado en los pasos de detección y solución de problemas que debe realizar para solucionar sus problemas antes de abrir un caso de TAC.

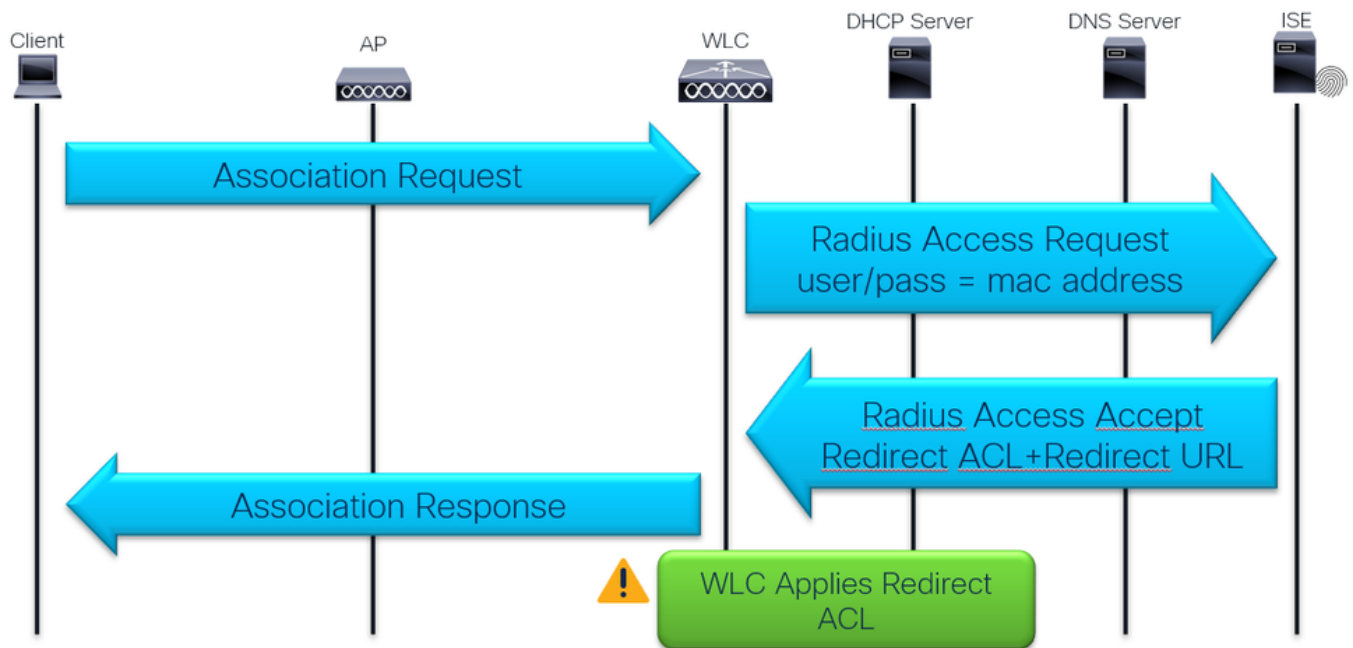
Este es el flujo de paquetes de CWA:



Flujo de paquetes CWA

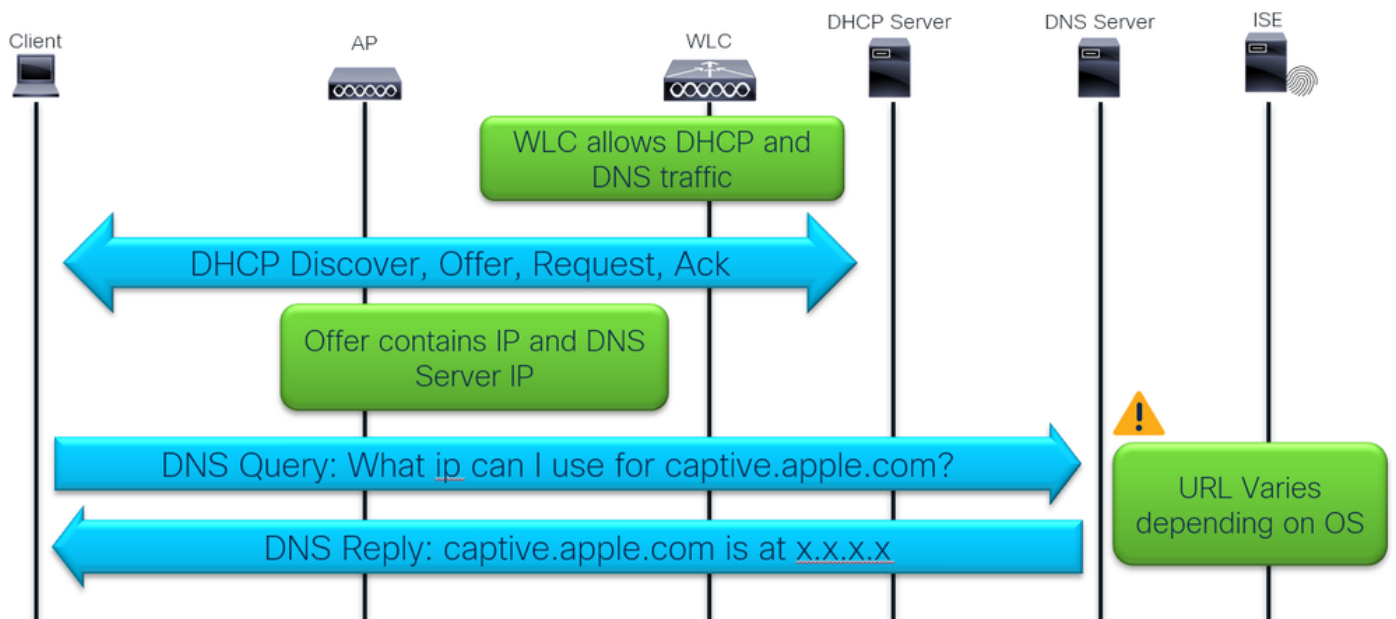
Flujo detallado

Primera asociación y autenticación RADIUS:



Primera asociación y autenticación RADIUS

DHCP, DNS y comprobación de conectividad:



DHCP, DNS y comprobación de conectividad

La comprobación de la conectividad se realiza mediante la detección del portal cautivo mediante el sistema operativo o el explorador del dispositivo cliente.

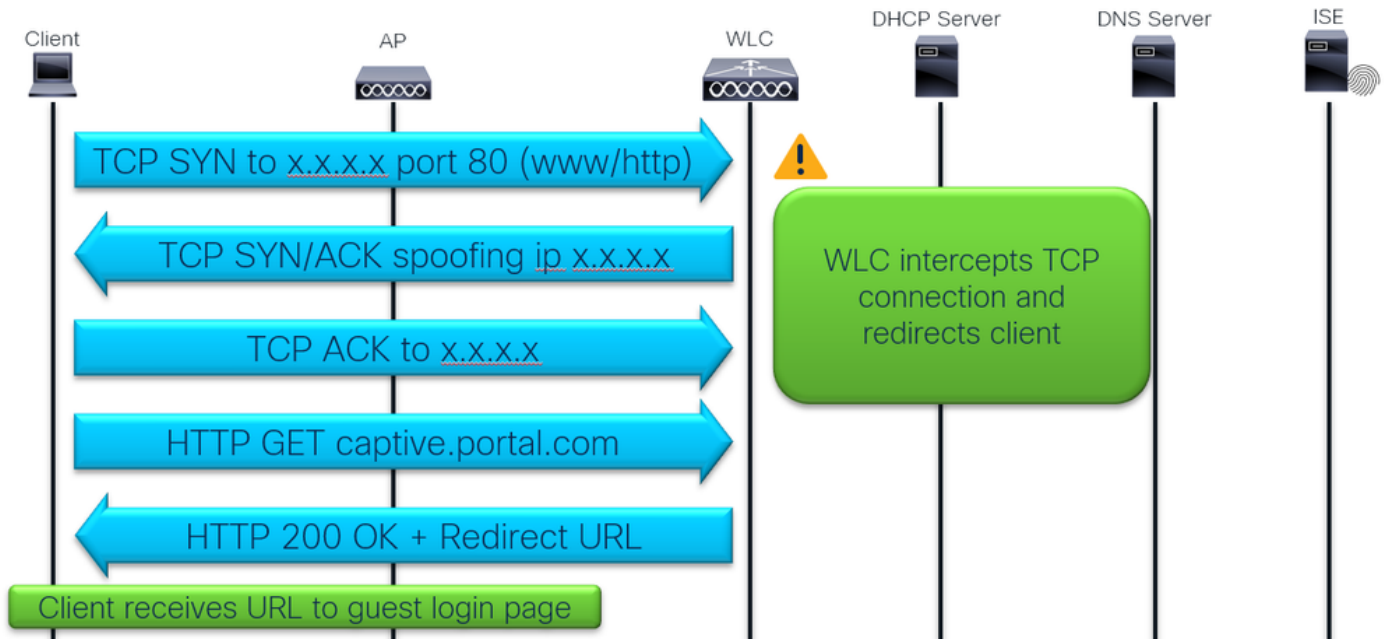
Hay SO de dispositivo preprogramado para hacer HTTP GET hacia un dominio específico

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

Y los navegadores también realizan esta comprobación cuando se abren:

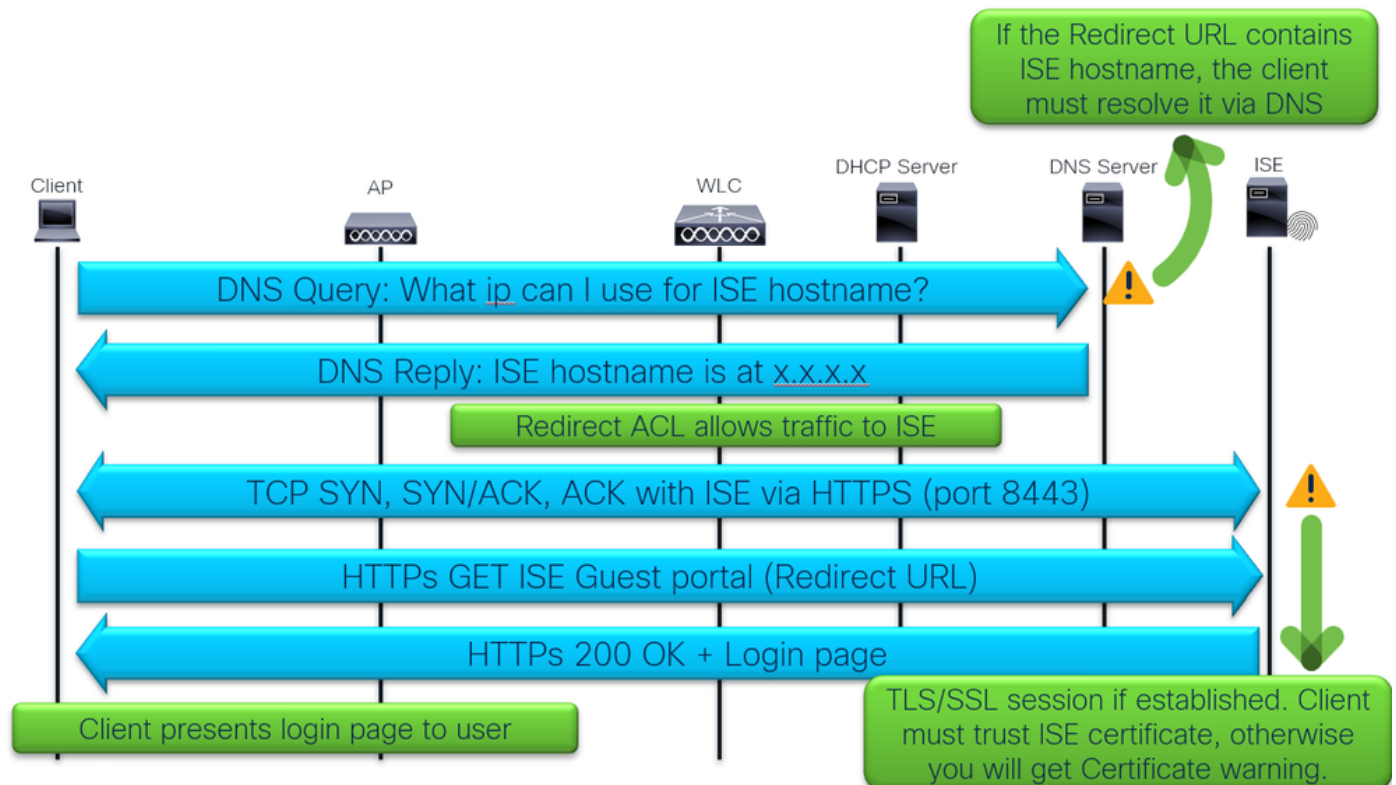
- Cromo = clients3.google.com
- Firefox = detectportal.firefox.com

Interceptación y redirección del tráfico:



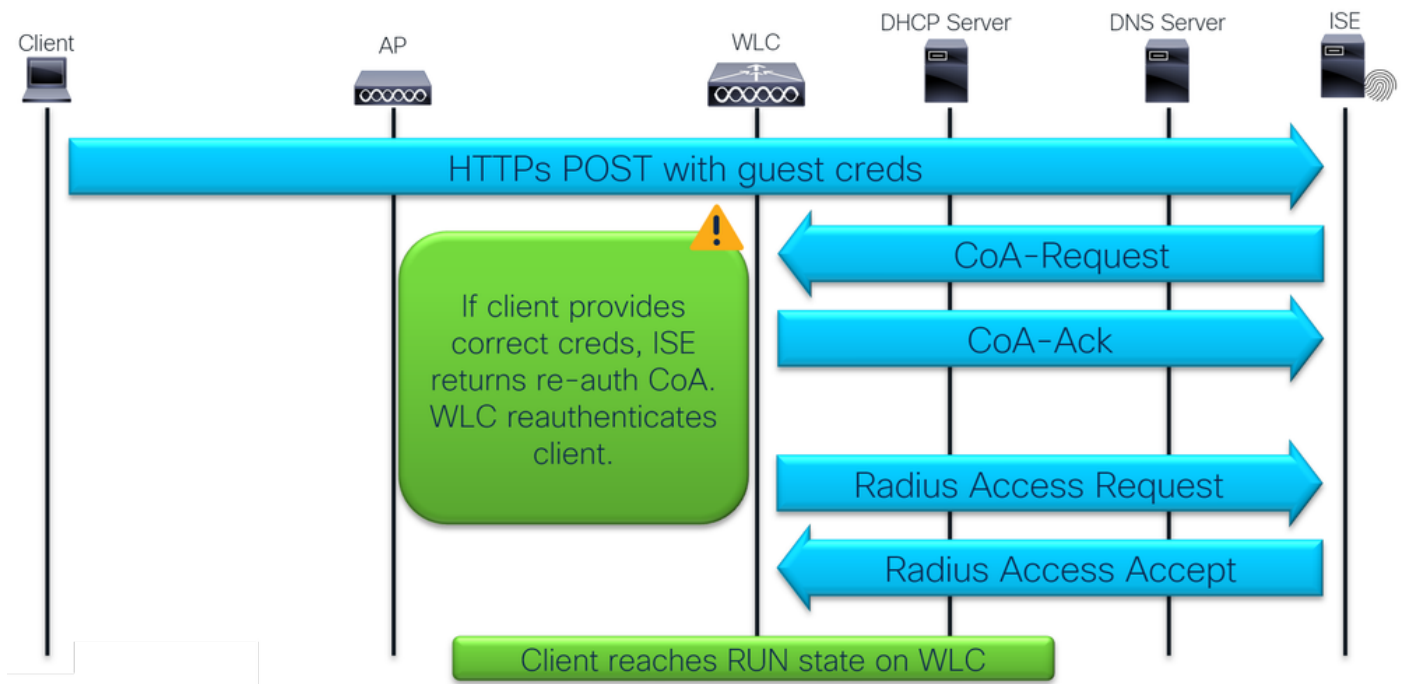
Interceptación y redirección del tráfico

Inicio de sesión de cliente en el portal de inicio de sesión de invitado ISE:



Inicio de sesión de cliente en el portal de inicio de sesión de invitado ISE

Inicio de sesión del cliente y CoA:

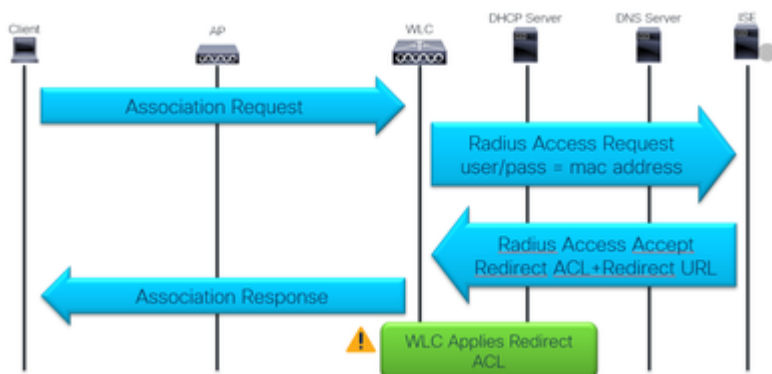


Inicio de sesión del cliente y CoA

Resolución de problemas

Síntoma frecuente: El usuario no es redirigido a la página de inicio de sesión.

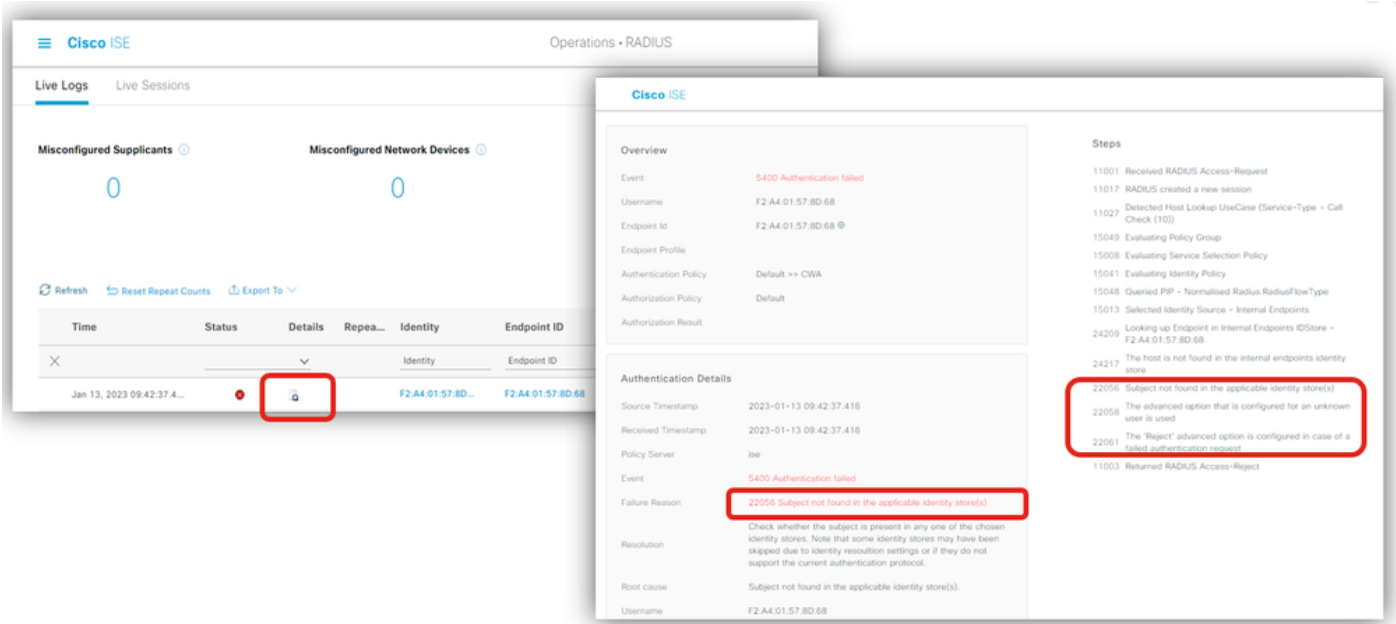
Comencemos con la primera parte del flujo:



Primera asociación y autenticación RADIUS

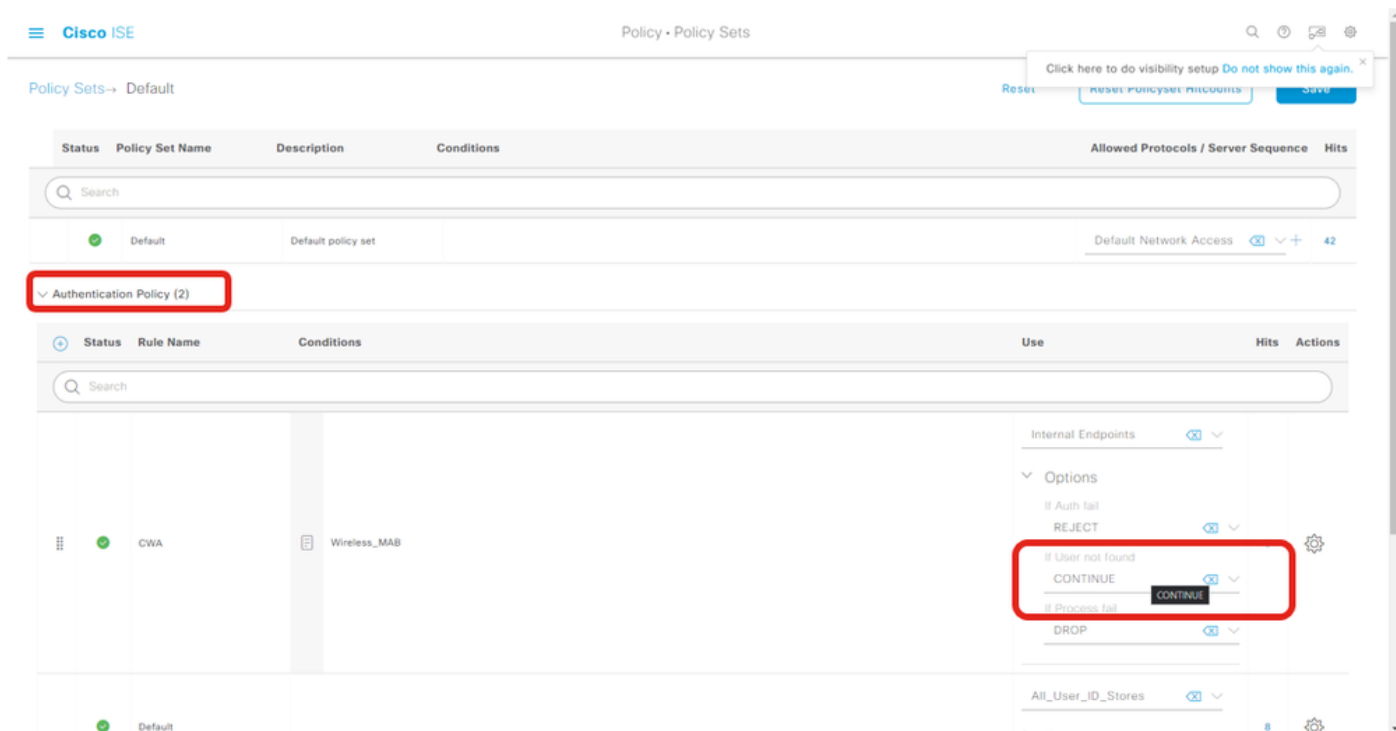
1 - ¿La primera autenticación RADIUS es exitosa?

Comprobar resultado de autenticación de filtrado de MAC:



Registros en directo de ISE que muestran el resultado de autenticación de filtrado de MAC

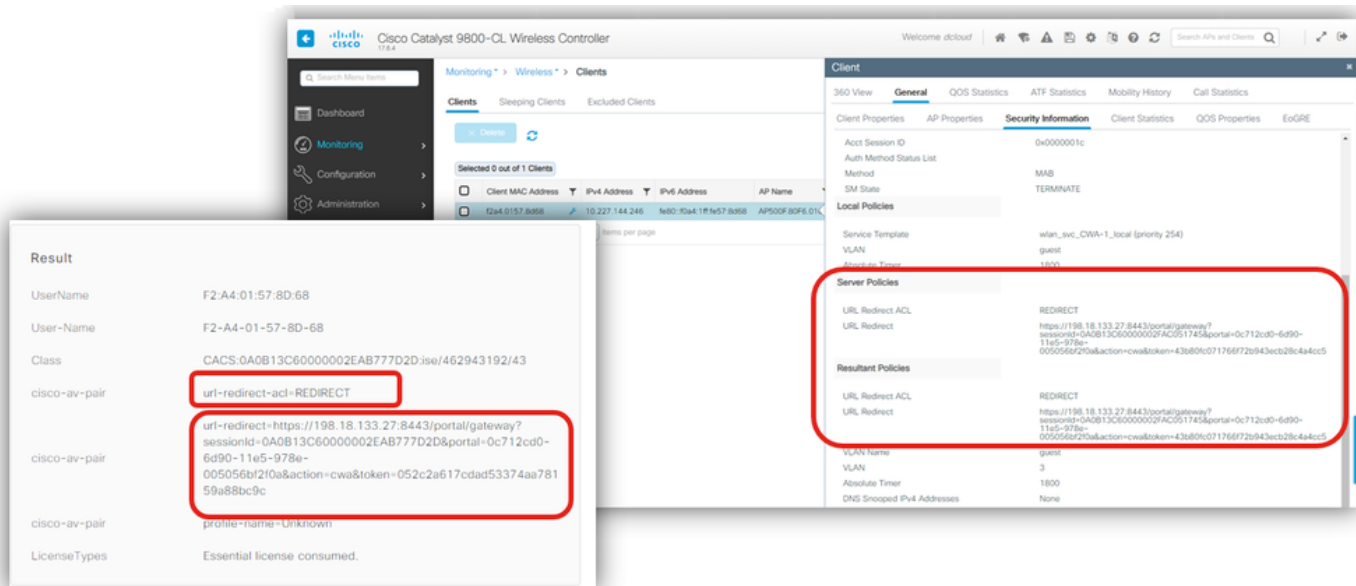
Asegúrese de que la opción avanzada para la autenticación esté establecida en "Continuar" si no se encuentra el usuario:



Opción avanzada Usuario no encontrado

2 - ¿El WLC recibe la URL y la ACL de redireccionamiento?

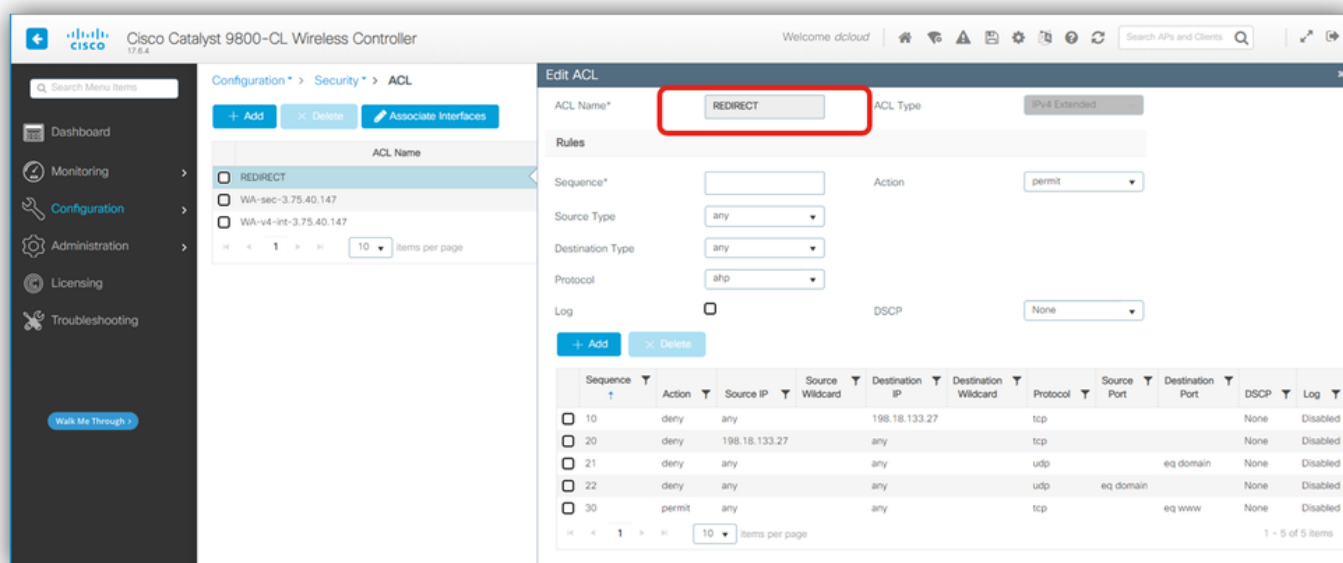
Verifique los registros en vivo de ISE y la información de seguridad del cliente de WLC bajo Supervisión Verifique que ISE envíe la URL de redirección y la ACL en la aceptación de acceso y que WLC la reciba y la aplique al cliente en los detalles del cliente:



Redirigir ACL y URL

3 - ¿Es correcta la ACL de redirección?

Verifique el nombre de ACL para cualquier error tipográfico. Asegúrese de que es exactamente como lo envía ISE:



Verificación de ACL de redirección

4 - ¿Está pendiente el traslado del cliente a Web-Auth?

Verifique los detalles del cliente para el estado "Pendiente de autenticación Web". Si no está en ese estado, verifique si la invalidación AAA y Radius NAC están habilitadas en el perfil de política:

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
☒

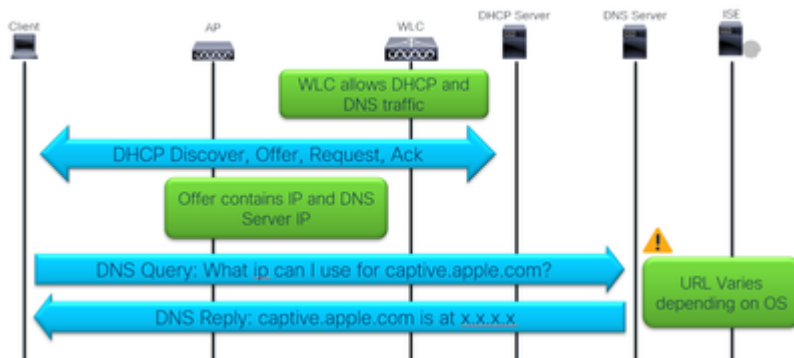
NAC State
☒

NAC Type
RADIUS

Detalles del cliente, anulación de aaa y RADIUS NAC

¿Aún no funciona?

Repasemos el flujo de trabajo...



DHCP, DNS y comprobación de conectividad

5 - ¿El WLC permite el tráfico DHCP y DNS?

Verifique el contenido de ACL de redirección en el 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

Redireccione el contenido de ACL en el WLC

La ACL de redirección define qué tráfico es interceptado y redirigido por la sentencia permit y qué tráfico es ignorado de la interceptación y redirección con una sentencia deny.

En este ejemplo, permitimos que el DNS y el tráfico hacia/desde la dirección IP de ISE fluyan, e interceptamos cualquier tráfico tcp en el puerto 80 (www).

6 - ¿El servidor DHCP recibe la detección/solicitud de DHCP?

Verifique con EPC si ocurre el intercambio DHCP. EPC se puede utilizar con filtros internos como el protocolo DHCP y/o MAC de filtro interno, donde podemos utilizar la dirección MAC del dispositivo cliente y obtenemos en el EPC sólo paquetes DHCP enviados o enviados a la dirección MAC del dispositivo cliente.

En este ejemplo, podemos ver los paquetes de detección DHCP enviados como broadcast en la VLAN 3:

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 'f2a4.0157.8d58'. A blue cloud callout points to this dialog with the text 'Inner filters !!'. Another red box highlights a packet in the list, showing details for a DHCP Discover packet. A yellow cloud callout points to this packet with the text 'Sent as broadcast on VLAN 3'.

WLC EPC para verificar DHCP

Confirme la VLAN de cliente esperada en el perfil de política:

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'.

VLAN en el perfil de políticas

Verifique la configuración de VLAN WLC y switchport Trunk y la subred DHCP:

```
WLC1#show vlan

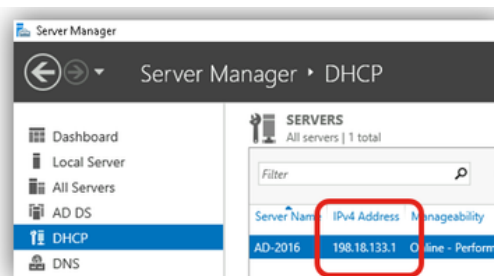
VLAN Name                Status    Ports
-----
1    default                active    Gi2, Gi3
2    employee                active
3    guest                   active
11   mgmt                    active

WLC1#show ip int br

Interface      IP-Address      OK? Method Status  Protocol
GigabitEthernet1  unassigned      YES unset  up      up
GigabitEthernet2  unassigned      YES unset  down    down
GigabitEthernet3  unassigned      YES unset  down    down
Vlan1           unassigned      YES NVRAM  up      down
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, puerto de switch y subred DHCP

Podemos ver que la VLAN 3 existe en el WLC y también tiene SVI para la VLAN 3; sin embargo, cuando verificamos la dirección IP del servidor DHCP, está en una subred diferente, por lo tanto, necesitamos la dirección de ayudante ip en la SVI.

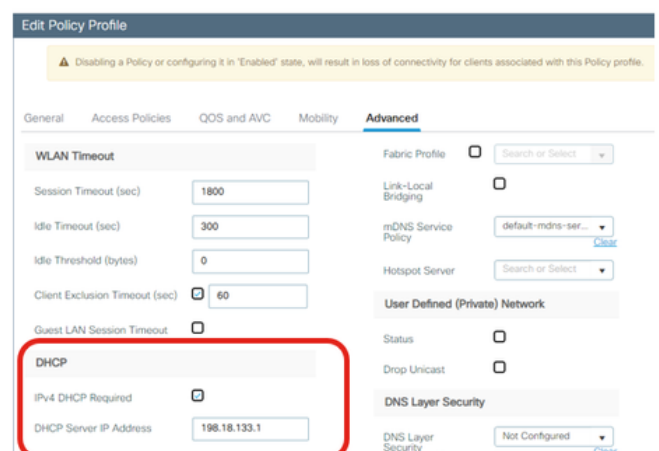
Las prácticas recomendadas establecen que la SVI para las subredes del cliente se debe configurar en la infraestructura cableada y evitarla en el WLC.

En cualquiera de los casos, el comando ip helper-address debe agregarse a la SVI independientemente de dónde resida.

Una alternativa es configurar la dirección IP del servidor DHCP en el perfil de la política:

```
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

Ip helper-address at SVI or Policy Profile

A continuación, puede comprobar con EPC si el intercambio DHCP funciona correctamente y si el servidor DHCP ofrece direcciones IP de servidor DNS:

Full DHCP exchange and DHCP server offering IP and DNS servers

Detalles de la oferta DHCP de IP del servidor DNS

7 - ¿Se produce la redirección automática?

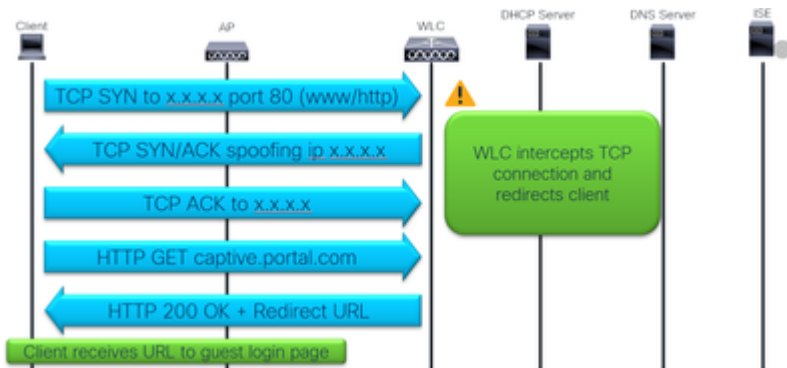
Verifique con WLC EPC si el servidor DNS responde a las consultas:

Consultas y respuestas de DNS

- Si la redirección no es automática, abra un explorador y pruebe con una dirección IP aleatoria. Por ejemplo 10.0.0.1.
- Si la redirección funciona, es posible que tenga un problema de resolución de DNS.

¿Aún no funciona?

Repasemos el flujo de trabajo...



Intercepción y redirección del tráfico

8 - ¿El navegador no muestra la página de inicio de sesión?

Verifique si el cliente envía el TCP SYN al puerto 80 y el WLC lo intercepta:

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

Retransmisiones TCP al puerto 80

Aquí podemos ver que el cliente envía paquetes TCP SYN al puerto 80 pero no obtiene ninguna respuesta y realiza retransmisiones TCP.

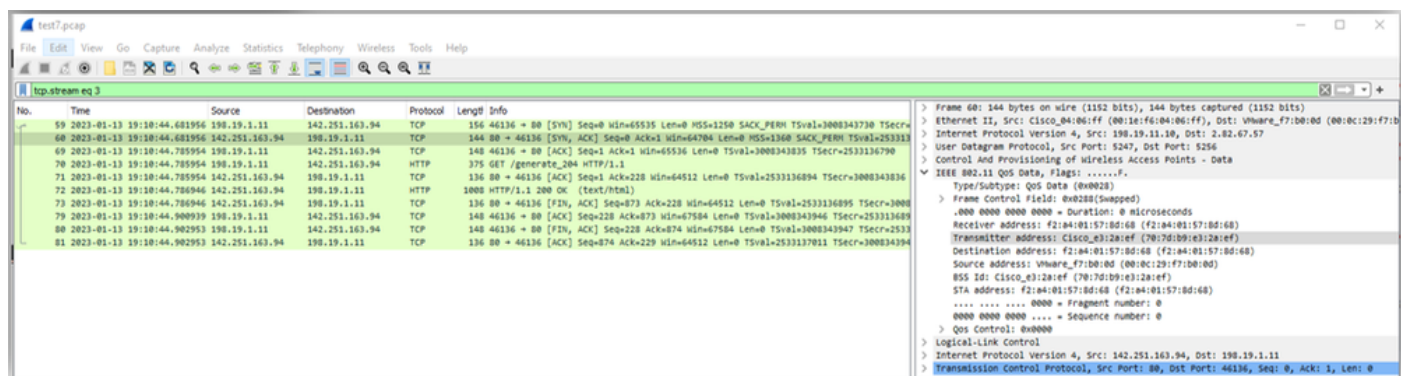
Asegúrese de tener el comando `ip http server` en la configuración global o `webauth-http-enable` en `parameter-map global`:

No need for ip http server

comandos de intercepción http

Después del comando, el WLC intercepta el TCP y falsifica la dirección IP de destino para

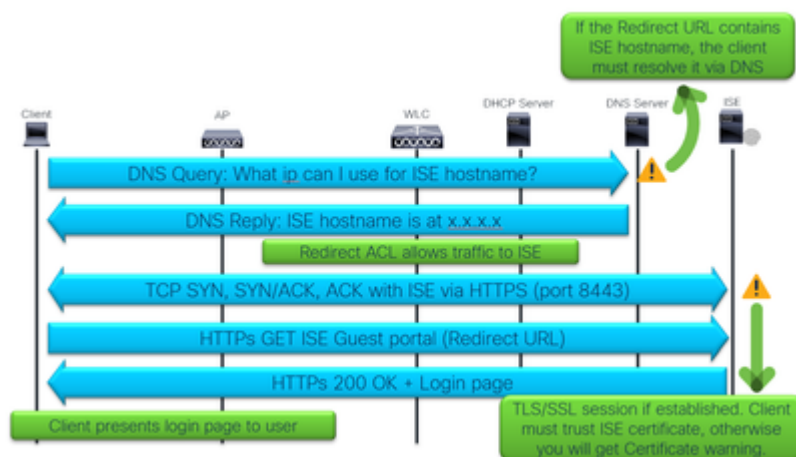
responder al cliente y redirigir.



Intercepción de TCP por WLC

¿Aún no funciona?

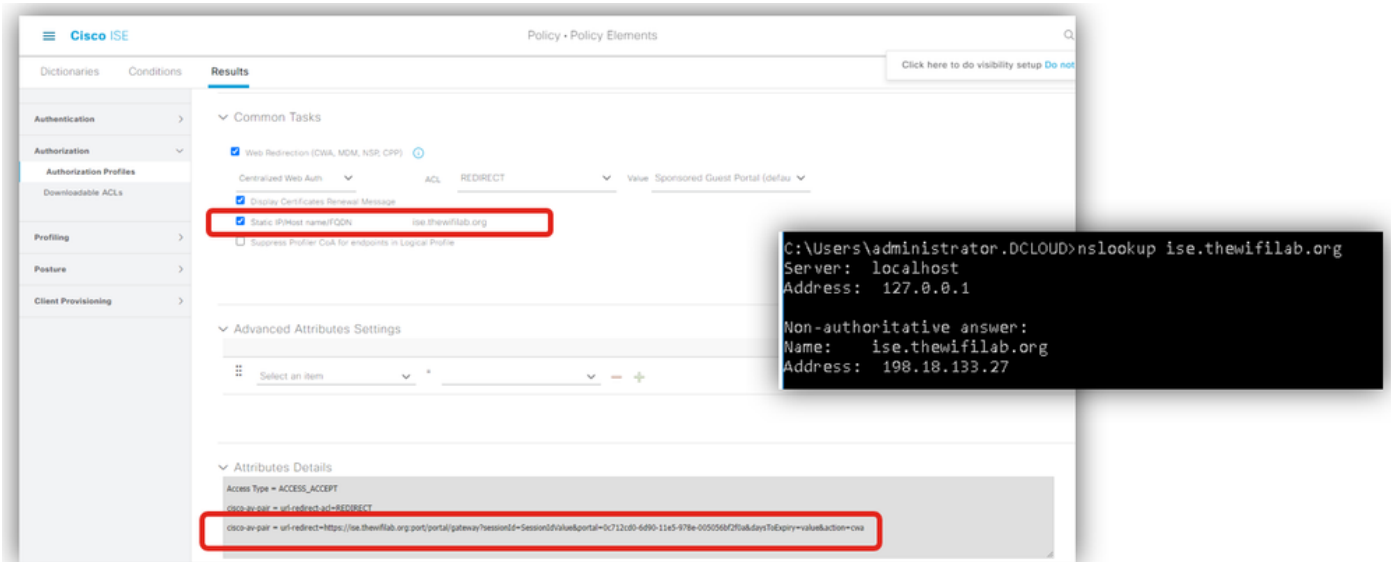
Hay más en el flujo...



Inicio de sesión de cliente en el portal de inicio de sesión de invitado ISE

9 - ¿Puede el cliente resolver el nombre de host de ISE?

Verifique si la URL de redirección utiliza IP o nombre de host y si el cliente resuelve el nombre de host ISE:

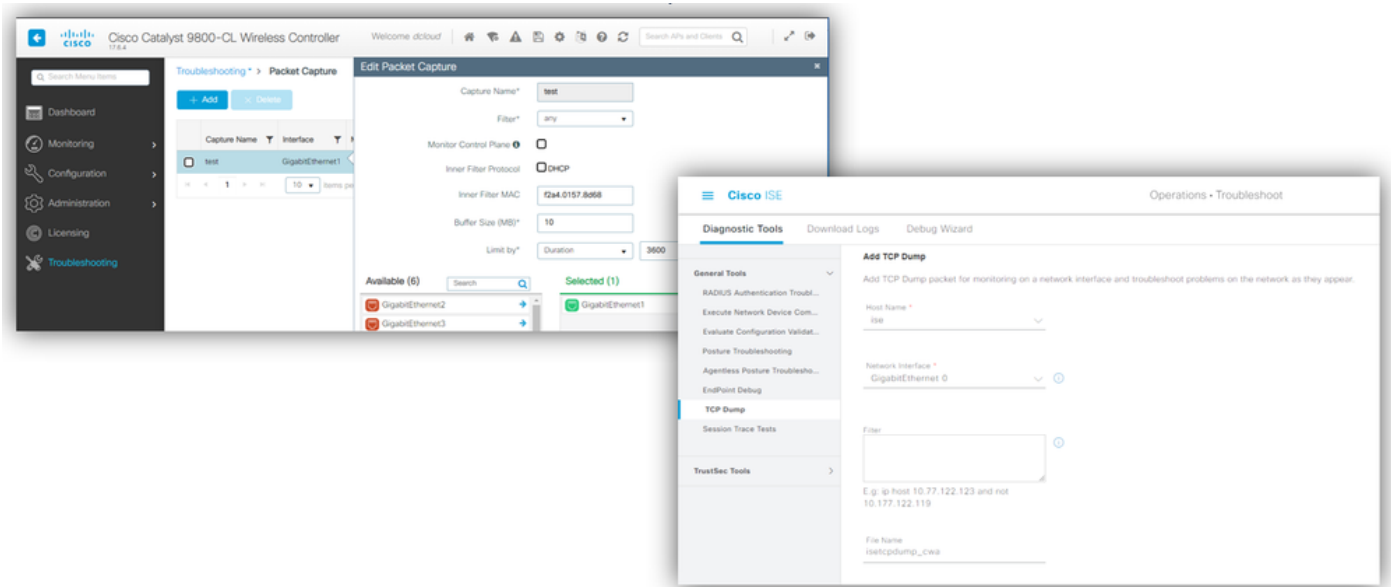


Resolución de nombre de host ISE

Se observa un problema común cuando la URL de redirección contiene el nombre de host de ISE; sin embargo, el dispositivo cliente no puede resolver ese nombre de host en la dirección IP de ISE. Si se utiliza el nombre de host, asegúrese de que se pueda resolver mediante DNS.

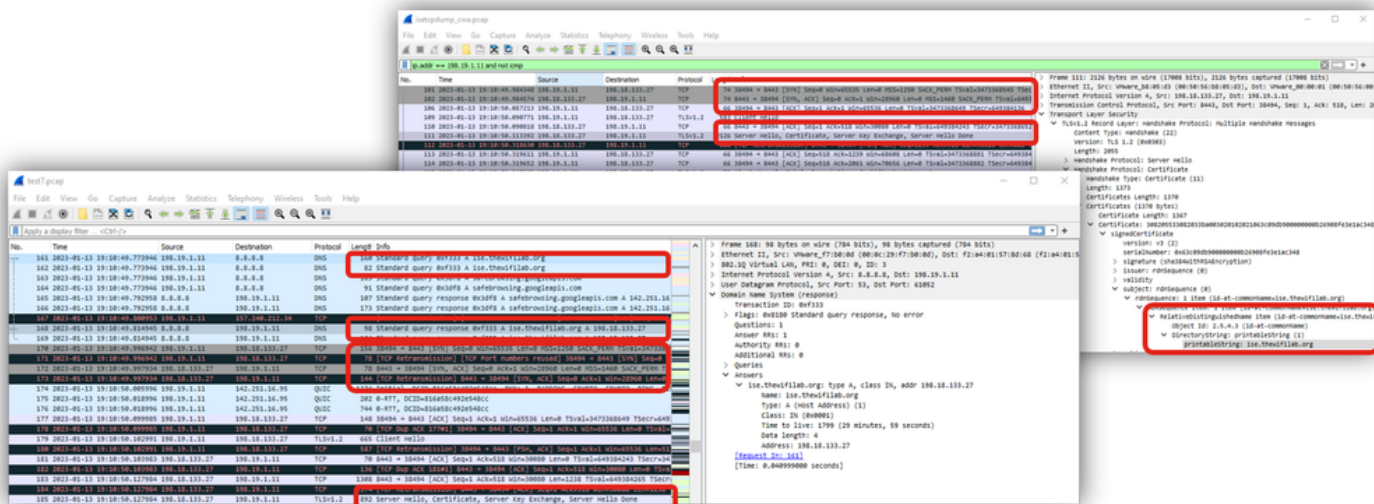
10 - ¿La página de inicio de sesión sigue sin cargarse?

Verifique con WLC EPC e ISE TCPdump si el tráfico del cliente alcanza ISE PSN. Configure e inicie las capturas en WLC e ISE:



WLC EPC e ISE TCPDump

Después de la reproducción del problema, recopile las capturas y correlacione el tráfico. Aquí podemos ver el nombre de host de ISE resuelto y, a continuación, la comunicación entre el cliente e ISE en el puerto 8443:



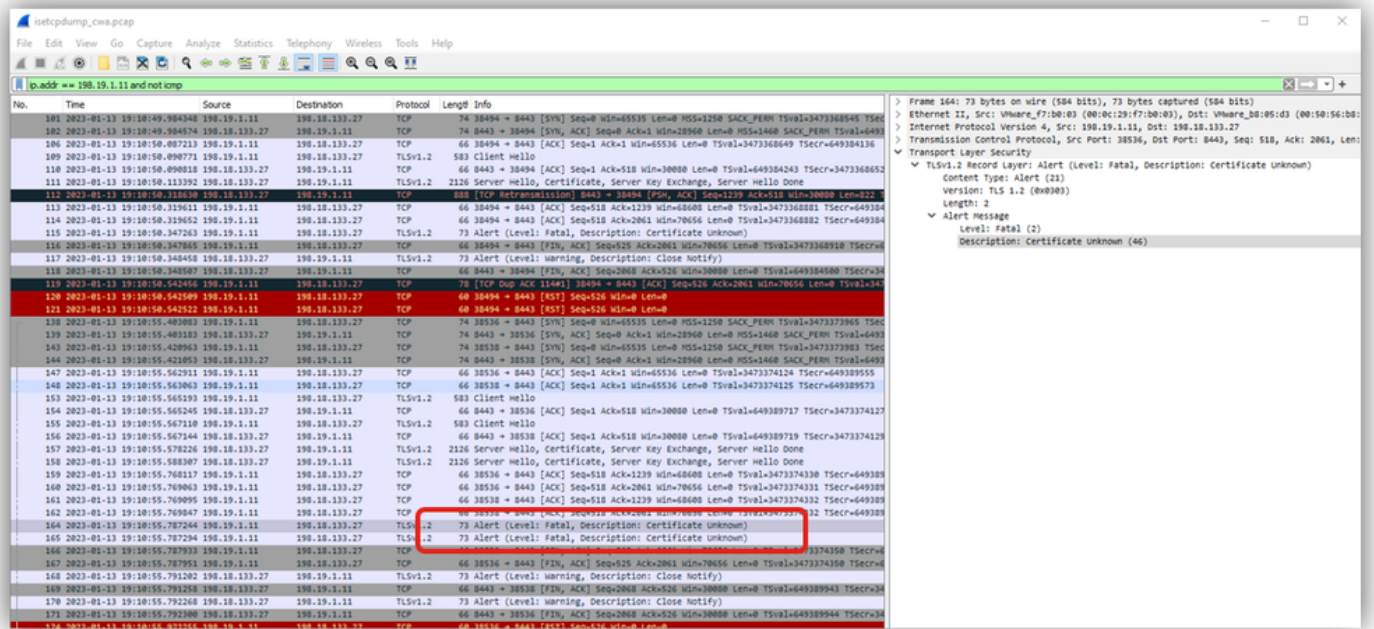
Tráfico WLC e ISE

11 - ¿Por qué se produce una violación de la seguridad debido al certificado?

Si utiliza un certificado autofirmado en ISE, se espera que el cliente emita una advertencia de seguridad cuando intente presentar la página de inicio de sesión del portal de ISE.

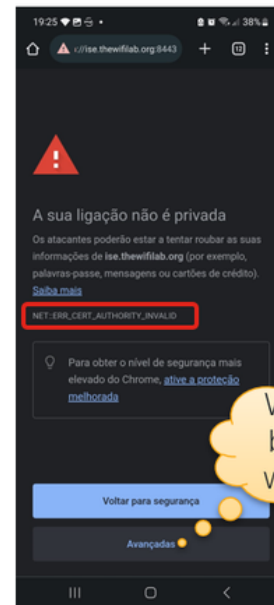
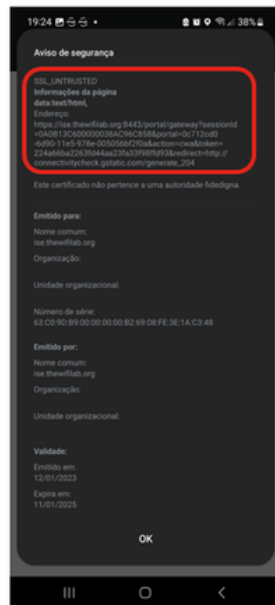
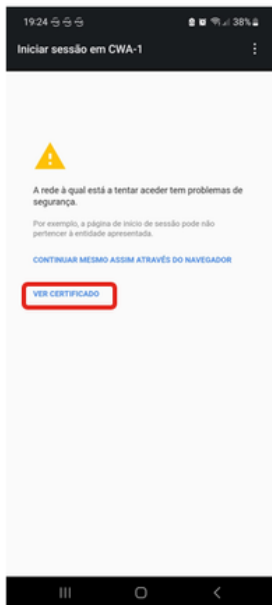
En el volcado de TCP de ISE o EPC del WLC, podemos verificar si el certificado de ISE es confiable.

En este ejemplo, podemos ver el cierre de la conexión desde Cliente con alerta (Nivel: Grave, Descripción: certificate (Unknown) (Desconocido), lo que significa que el certificado de ISE no se conoce (Trusted):



certificado no fiable de ISE

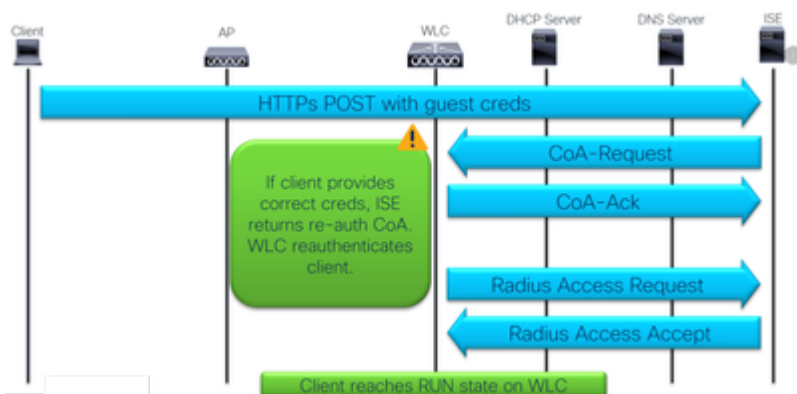
Si verificamos en el lado del cliente, vemos estos ejemplos de salida:



Dispositivo cliente que no confia en el certificado ISE

Finalmente, la redirección está funcionando!! Pero el login falla...

Una última vez comprobando el flujo...



Inicio de sesión del cliente y CoA

12 - ¿Falla el inicio de sesión de invitado?

Compruebe los registros de ISE para ver si hay errores de autenticación. Asegúrese de que las credenciales son correctas.

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 😊

La autenticación de invitado falla debido a credenciales erróneas

13 - ¿Se ha iniciado sesión correctamente pero no se ha movido a RUN?

Consulte los registros de ISE para obtener los detalles de autenticación y los resultados:

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

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=act=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 ????

Loop de redirección

En este ejemplo podemos ver al cliente obteniendo nuevamente el perfil de autorización que contiene la URL de redireccionamiento y la ACL de redireccionamiento. Esto da como resultado un loop de redirección.

Marque Conjunto de directivas. La verificación de reglas Guest_Flow debe ser anterior a la redirección:

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	Bade1115-aef1-4a9a-8158-002e835179db
IsThirdPartyDeviceFlow	false
AcctSessionId	0012523811021118
UseCase	Guest-Flow
AuthorizationPolicyMatched...	Guest-Flow
EndPointMACAddress	F2-A4-01-57-8D-68
ISEPolicySetName	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:GuestEndpoints

Regla Guest_Flow

14 - ¿Falla el CoA?

Con EPC e ISE TCPDump podemos verificar el tráfico CoA. Verifique si el puerto CoA (1700) está abierto entre WLC e ISE. Asegúrese de compartir coincidencias secretas.

Wireshark - radius

No.	Time	Source	Destination	Protocol	Length	Info
214	2023-01-13 19:38:06.993936	190.18.133.27	190.19.11.10	RADIUS	458	Accounting-Request id=212
215	2023-01-13 19:38:06.997934	190.18.133.27	190.19.11.10	RADIUS	84	Accounting-Response id=212
295	2023-01-13 19:38:14.184990	190.18.133.27	190.19.11.10	RADIUS	430	Access-Request id=213
296	2023-01-13 19:38:14.321987	190.18.133.27	190.19.11.10	RADIUS	489	Access-Accept id=213
310	2023-01-13 19:38:14.420664	190.18.133.27	190.19.11.10	RADIUS	480	Accounting-Request id=214
311	2023-01-13 19:38:14.427971	190.18.133.27	190.19.11.10	RADIUS	442	Accounting-Request id=215
312	2023-01-13 19:38:14.438972	190.18.133.27	190.19.11.10	RADIUS	66	Accounting-Response id=215
313	2023-01-13 19:38:14.440971	190.18.133.27	190.19.11.10	RADIUS	66	Accounting-Response id=214
351	2023-01-13 19:38:15.224979	190.18.133.27	190.19.11.10	RADIUS	468	Accounting-Request id=216
352	2023-01-13 19:38:15.229983	190.18.133.27	190.19.11.10	RADIUS	66	Accounting-Response id=216
3539	2023-01-13 19:38:16.416970	190.18.133.27	190.19.11.10	RADIUS	248	CoA-Request id=4
3540	2023-01-13 19:38:16.416970	190.18.133.27	190.19.11.10	RADIUS	475	Access-Request id=217
3541	2023-01-13 19:38:16.416970	190.18.133.27	190.19.11.10	RADIUS	111	CoA-ACK id=4
3542	2023-01-13 19:38:16.420963	190.18.133.27	190.19.11.10	RADIUS	166	Access-Accept id=217

Frame 3539: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
 Ethernet II, Src: Vmware_77:08:0d (00:0c:29:77:08:0d), Dst: Cisco_04:06:ff (00:1e:f6:04:06:ff)
 IP: 190.18.133.27, Src: 190.18.133.27, Dst: 190.19.11.10
 User Datagram Protocol, Src Port: 14564, Dst Port: 1700
 RADIUS Protocol
 Length: 218
 Checksum: 0xe371 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 67]
 [Timestamps]
 UDP payload (202 bytes)
 RADIUS Protocol

tráfico CoA



Nota: En la versión 17.4.X y posteriores, asegúrese de configurar también la clave del servidor CoA cuando configure el servidor RADIUS. Utilice la misma clave que el secreto compartido (son las mismas de forma predeterminada en ISE). El propósito es configurar opcionalmente una clave diferente para CoA que el secreto compartido si es lo que su servidor RADIUS configuró. En Cisco IOS® XE 17.3, la interfaz de usuario web simplemente utilizaba el mismo secreto compartido que la clave CoA.

A partir de la versión 17.6.1, RADIUS (incluida CoA) es compatible con este puerto. Si desea utilizar el puerto de servicio para RADIUS, necesita esta configuración:

<#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
```

Conclusión

Esta es la lista de verificación de CWA reanudada:

- Asegúrese de que el cliente esté en la VLAN correcta y obtenga la dirección IP y el DNS.

- Obtenga detalles del cliente en el WLC y ejecute capturas de paquetes para ver el intercambio DHCP.
- Verifique que el cliente pueda resolver los nombres de host a través de DNS.
 - Haga ping al nombre de host desde cmd.
- El WLC debe estar escuchando en el puerto 80
 - Verifique el comando global ip http server o el comando global parameter map webauth-http-enable.
- Para eliminar la advertencia de certificado, instale el certificado de confianza en ISE.
 - No es necesario instalar el certificado confiable en el WLC en CWA.
- Política de autenticación en ISE Opción avanzada "Continuar" Si no se encuentra el usuario
 - Para permitir que los usuarios invitados patrocinados se conecten y obtengan la redirección URL y ACL.

Y las herramientas principales usadas en la resolución de problemas:

- WLC EPC
 - Filtros internos: protocolo DHCP, dirección MAC.
- Monitor WLC
 - Compruebe los detalles de seguridad del cliente.
- seguimiento WLC RA
 - Depuraciones con información detallada en el lado del WLC.
- registros en vivo de ISE
 - Detalles de autenticación.
- TCPDump de ISE
 - Recopile capturas de paquetes en la interfaz PSN de ISE.

Referencias

[Configuración de Central Web Authentication \(CWA\) en Catalyst 9800 WLC e ISE](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).