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

Contenido

Introducción

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

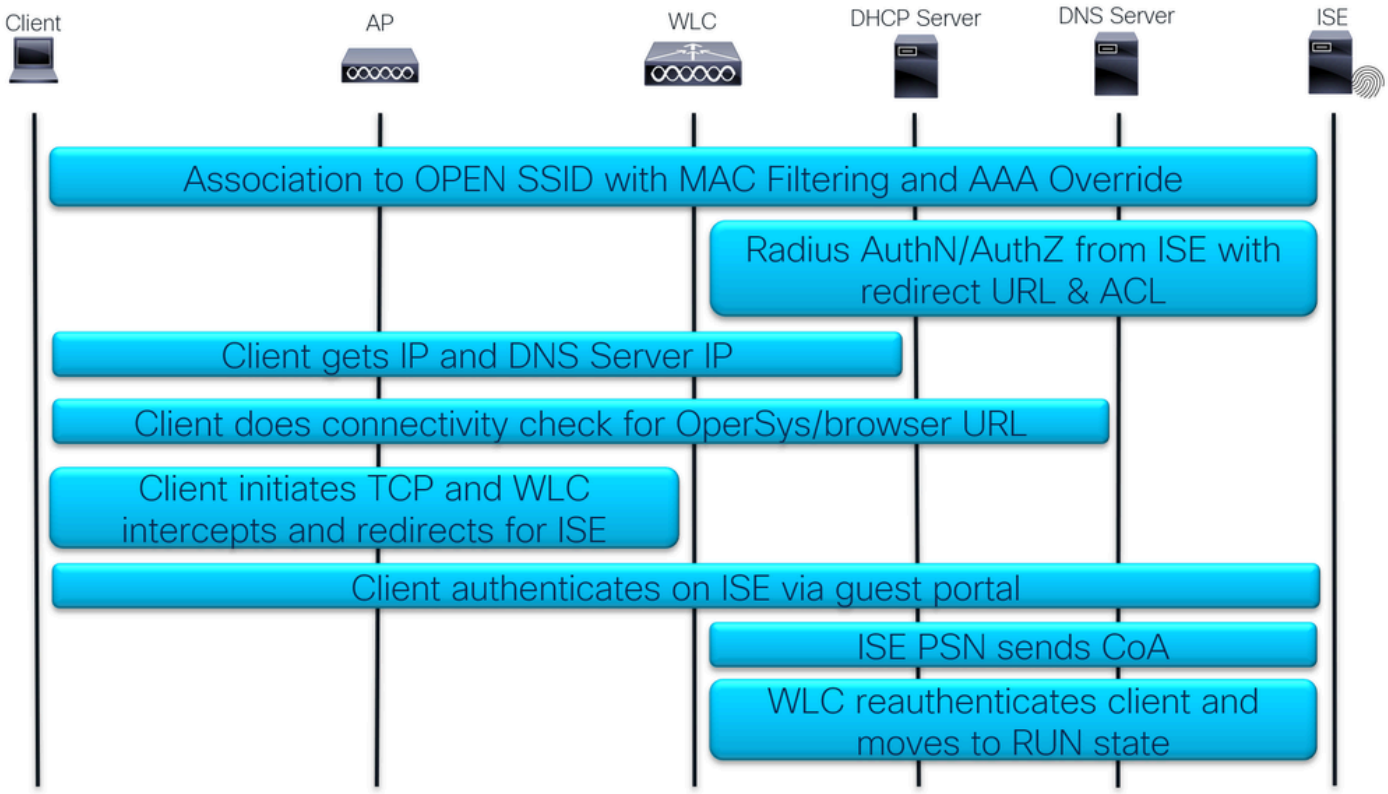
Información de fondo

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.

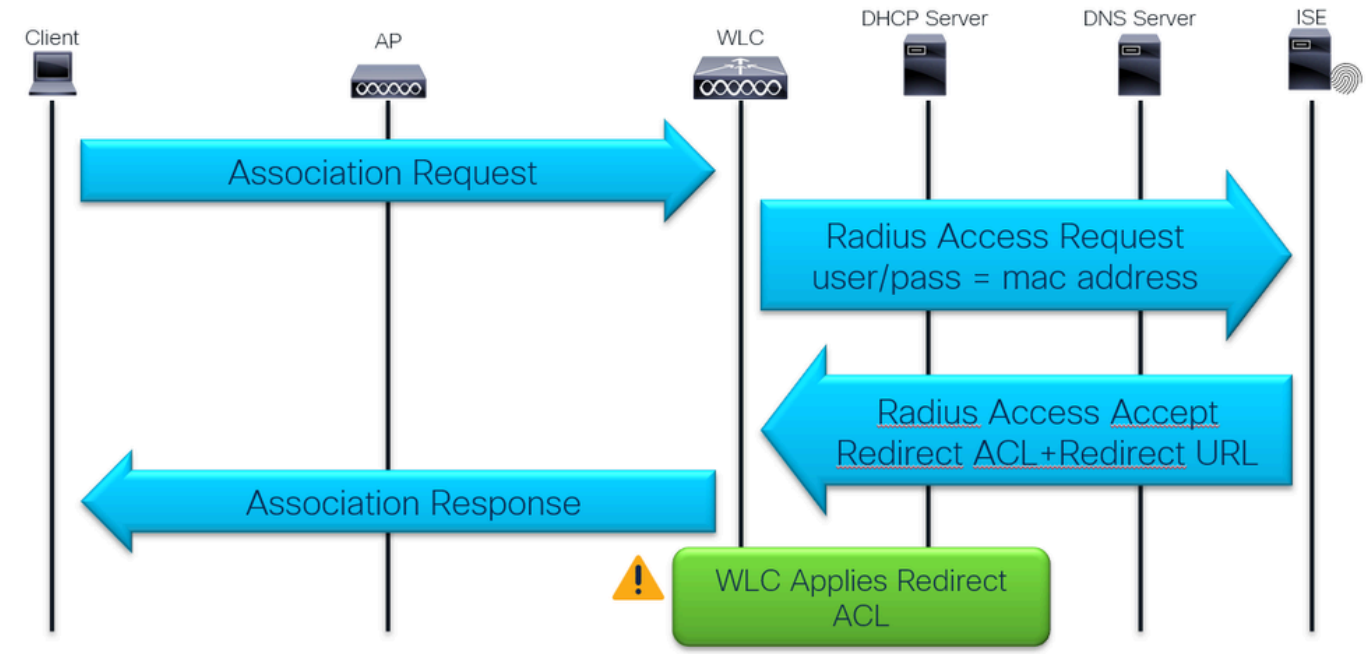
Este es el flujo de paquetes de CWA:



Flujo de paquetes CWA

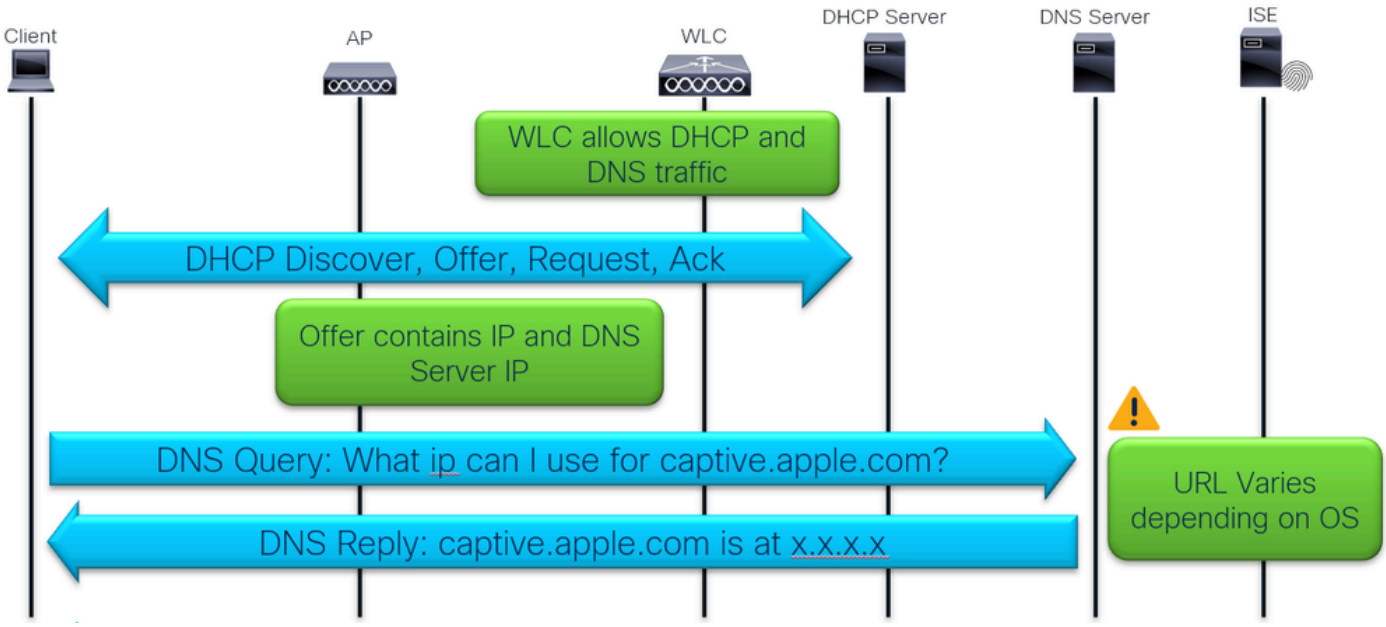
Flujo detallado

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.

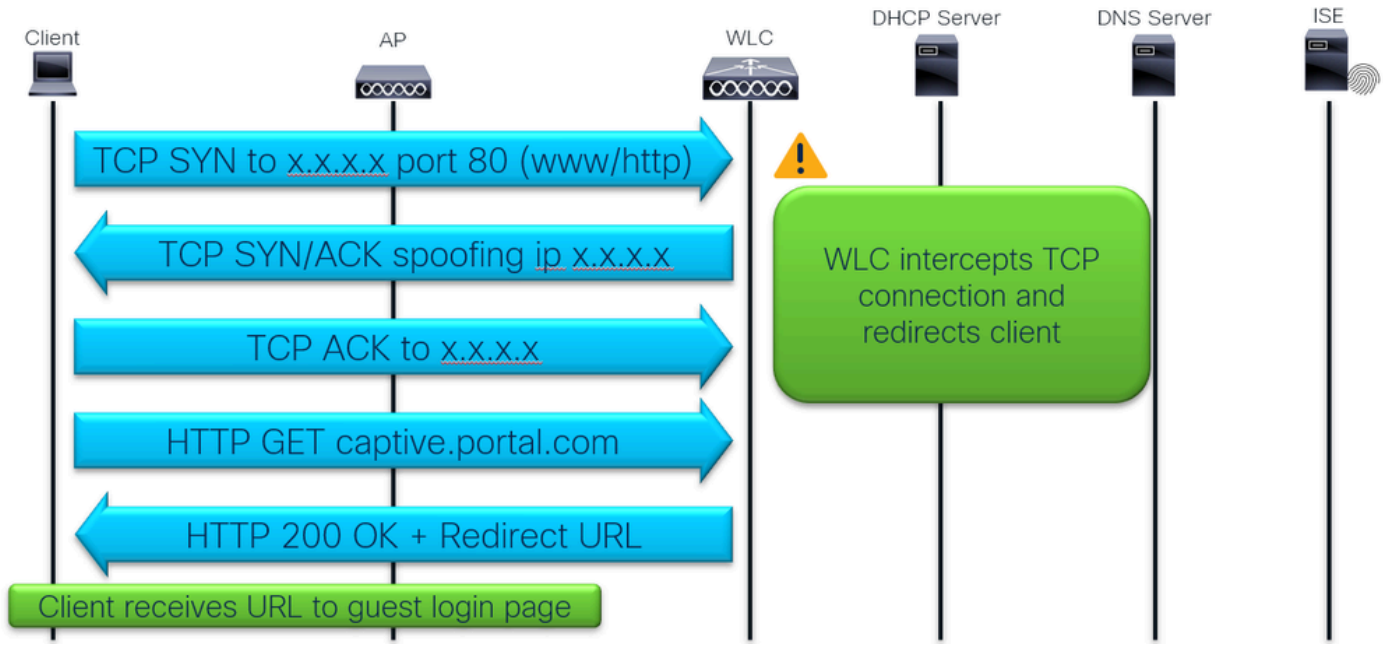
Hay SO de dispositivo preprogramado para hacer HTTP GET hacia un dominio específico

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

Y los navegadores también realizan esta comprobación cuando se abren:

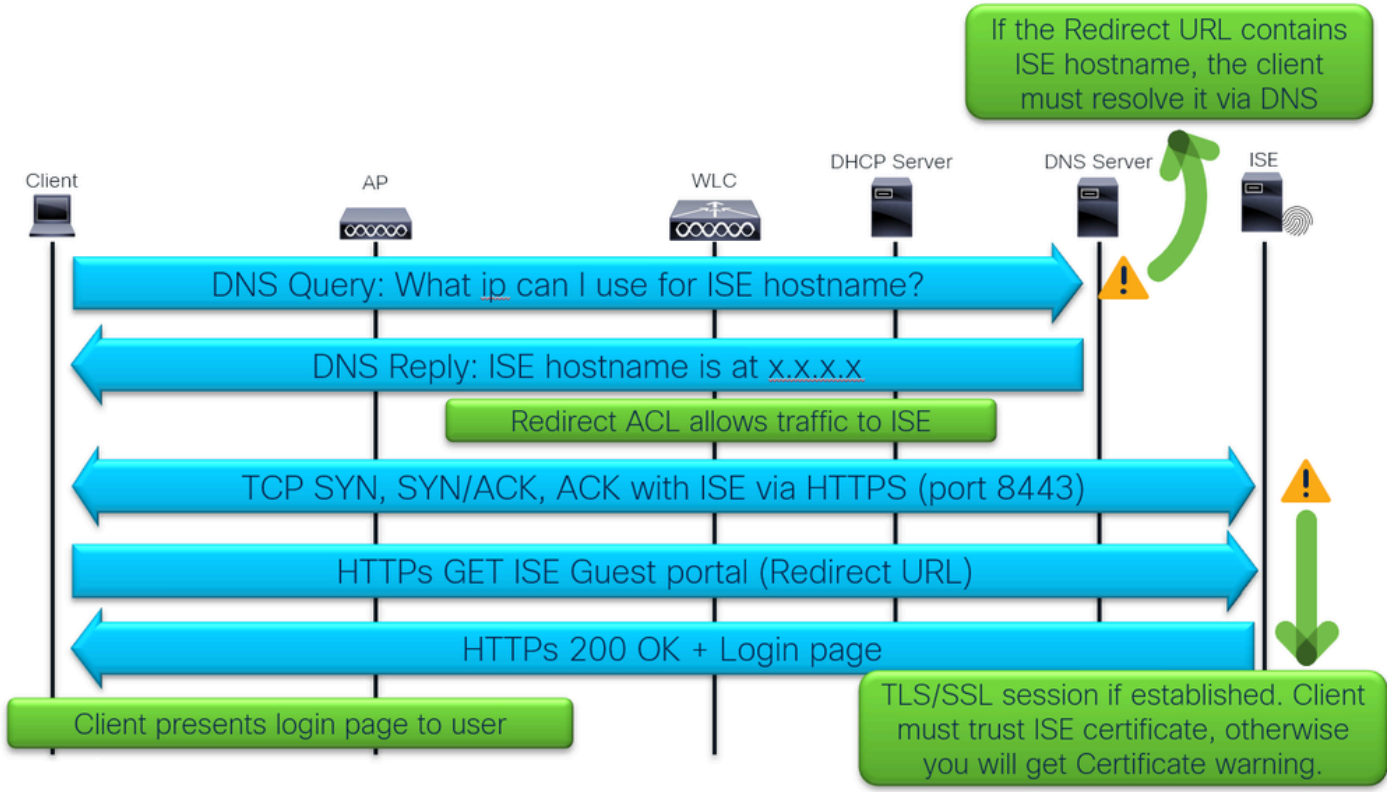
- Cromo = clients3.google.com
- Firefox = detectportal.firefox.com

Interceptación y redirección del tráfico:



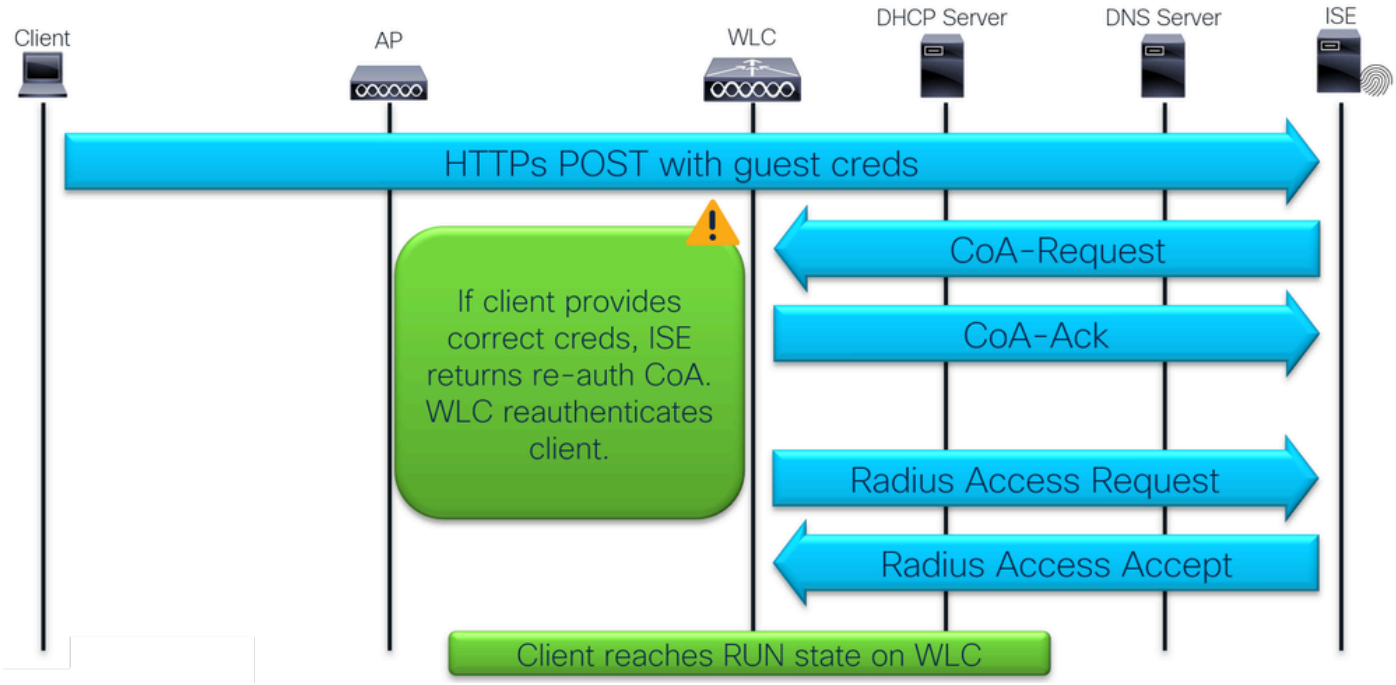
Interceptación y redirección del tráfico

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:

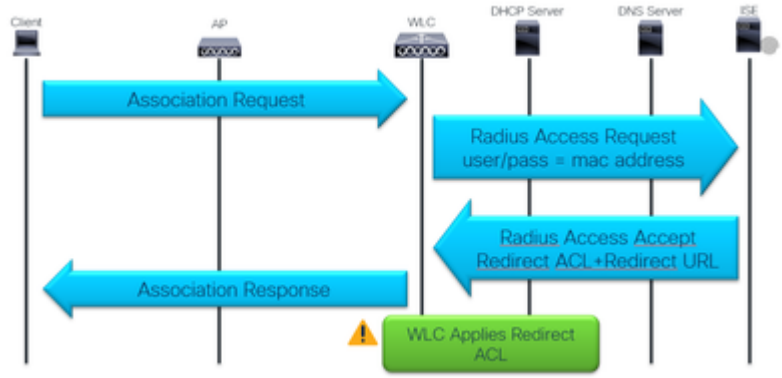


Inicio de sesión del cliente y CoA

Resolución de problemas

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

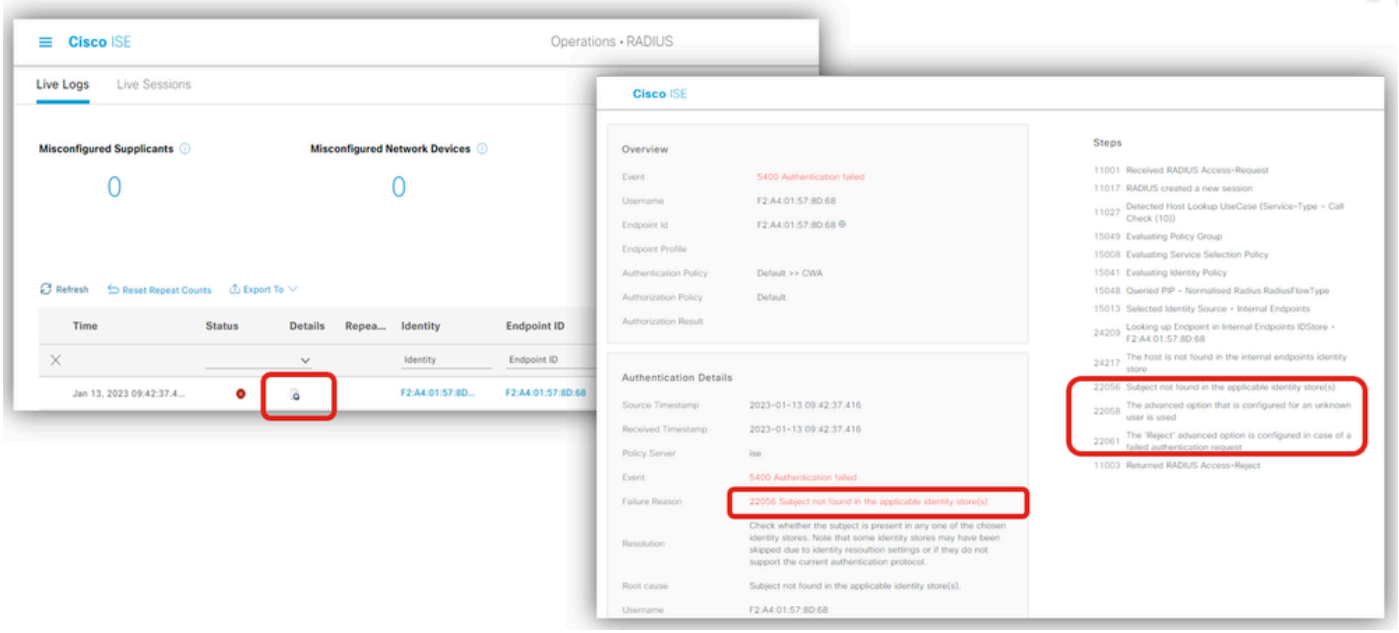
Comencemos con la primera parte del flujo:



Primera asociación y autenticación RADIUS

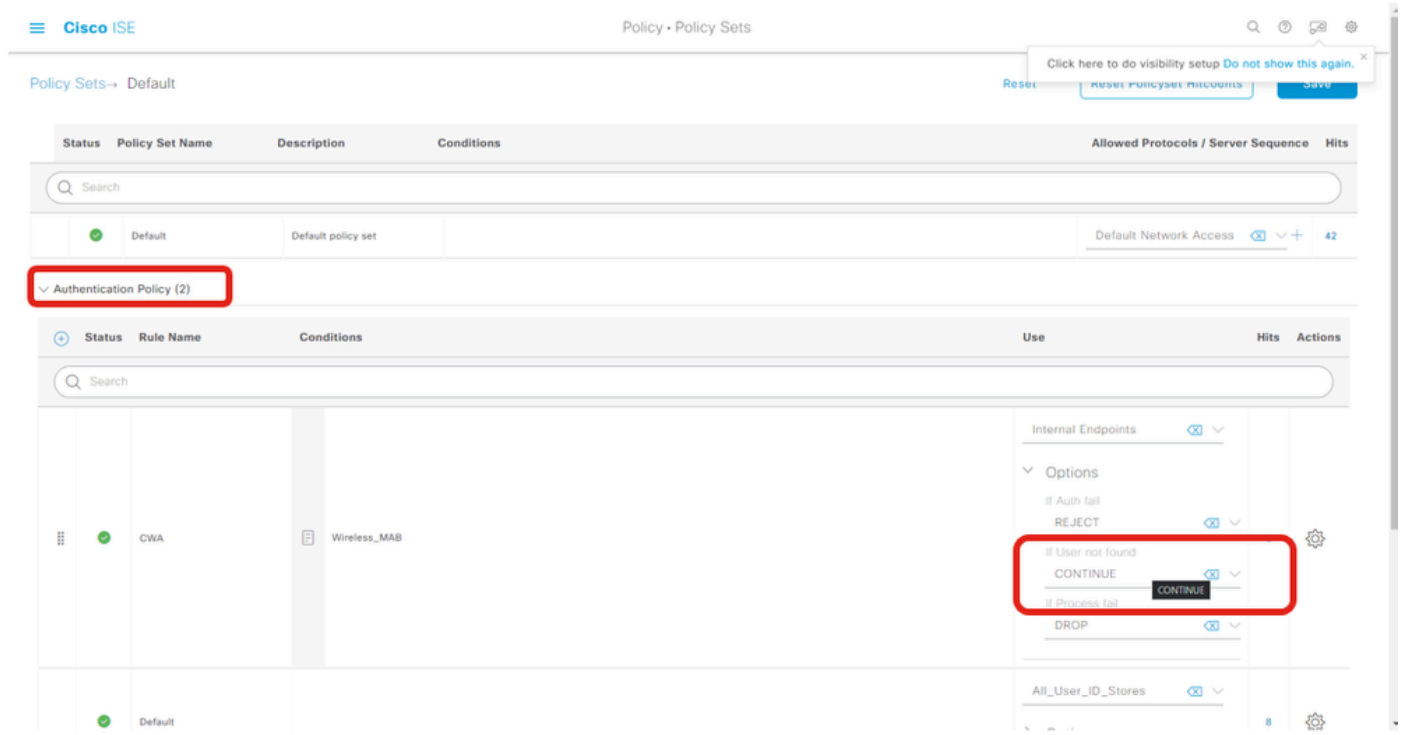
1 - ¿La primera autenticación RADIUS es exitosa?

Comprobar resultado de autenticación de filtrado de MAC:



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

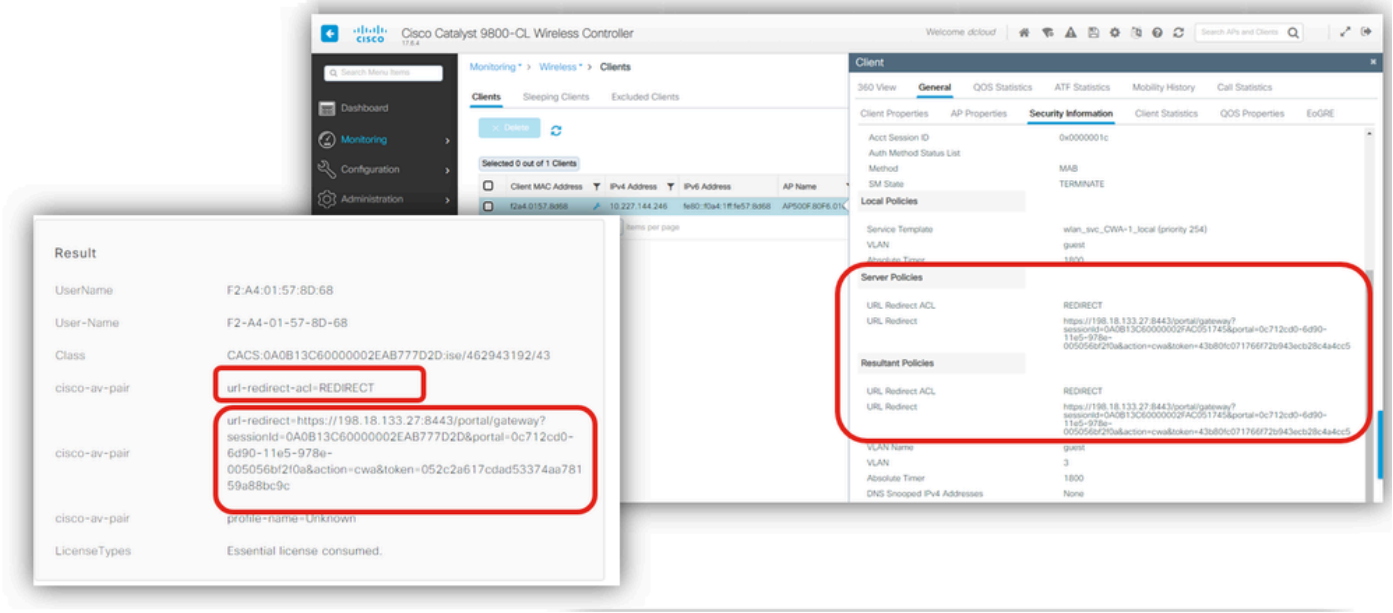
Asegúrese de que la opción avanzada para la autenticación esté establecida en "Continuar" si no se encuentra el usuario:



Opción avanzada Usuario no encontrado

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

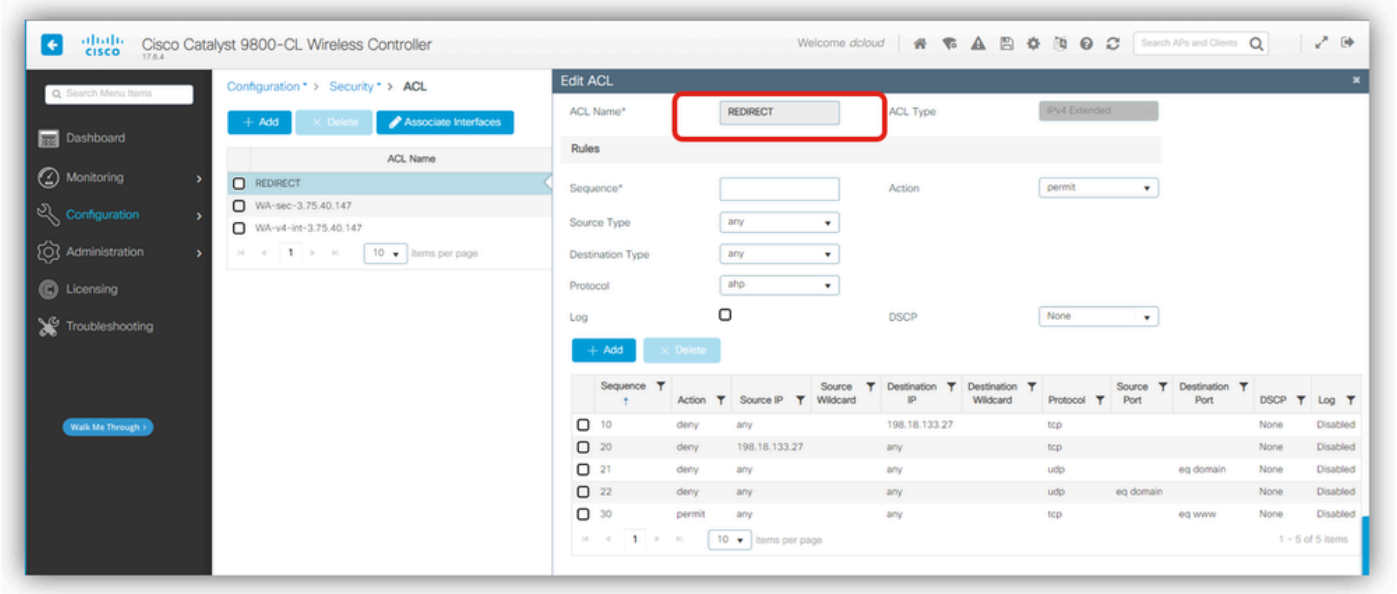
Verifique los registros en vivo de ISE y la información de seguridad del cliente de WLC bajo Supervisión Verifique que ISE envíe la URL de redirección y la ACL en la aceptación de acceso y que WLC la reciba y la aplique al cliente en los detalles del cliente:



Redirigir ACL y URL

3 - ¿Es correcta la ACL de redirección?

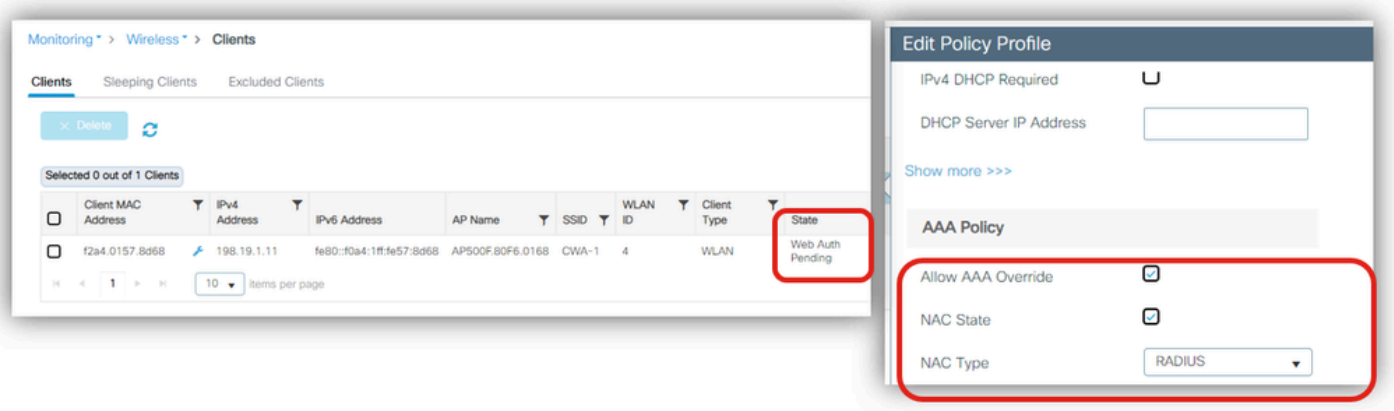
Verifique el nombre de ACL para cualquier error tipográfico. Asegúrese de que es exactamente como lo envía ISE:



Verificación de ACL de redirección

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

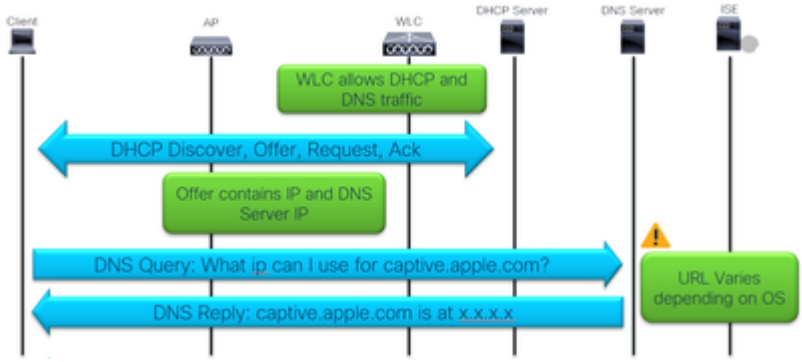
Verifique los detalles del cliente para el estado "Pendiente de autenticación Web". Si no está en ese estado, verifique si la invalidación AAA y Radius NAC están habilitadas en el perfil de política:



Detalles del cliente, anulación de aaa y RADIUS NAC

¿Aún no funciona?

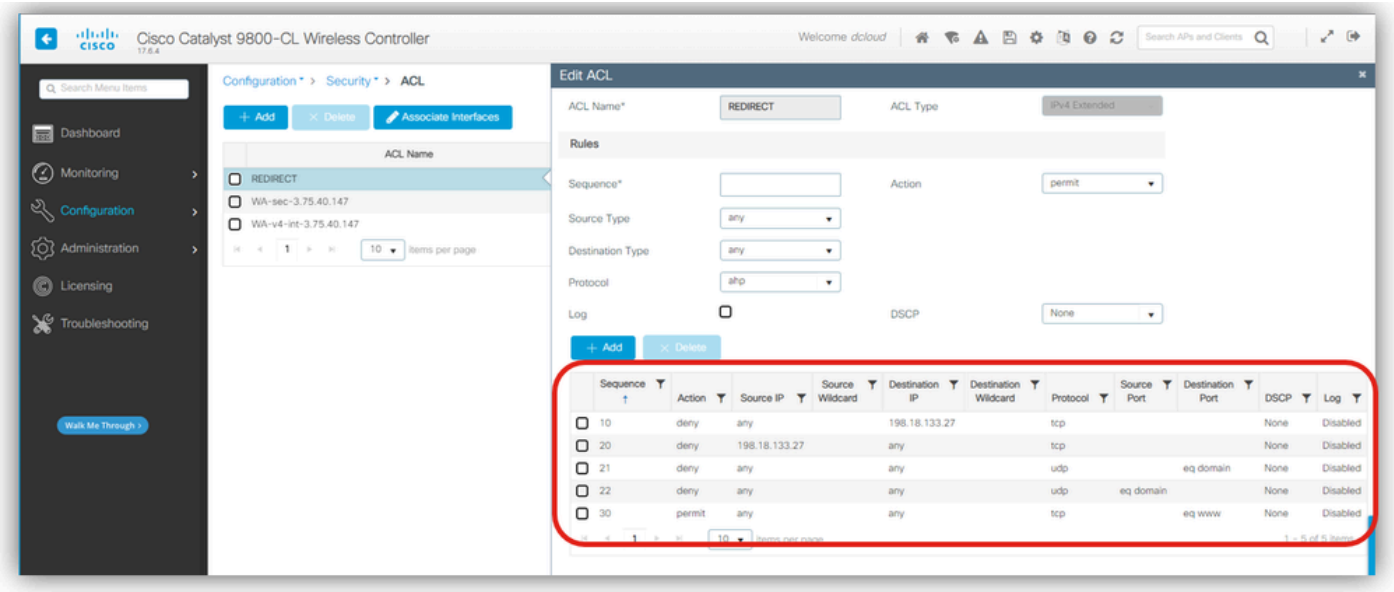
Repasemos el flujo de trabajo...



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:



Redireccione el contenido de ACL en el WLC

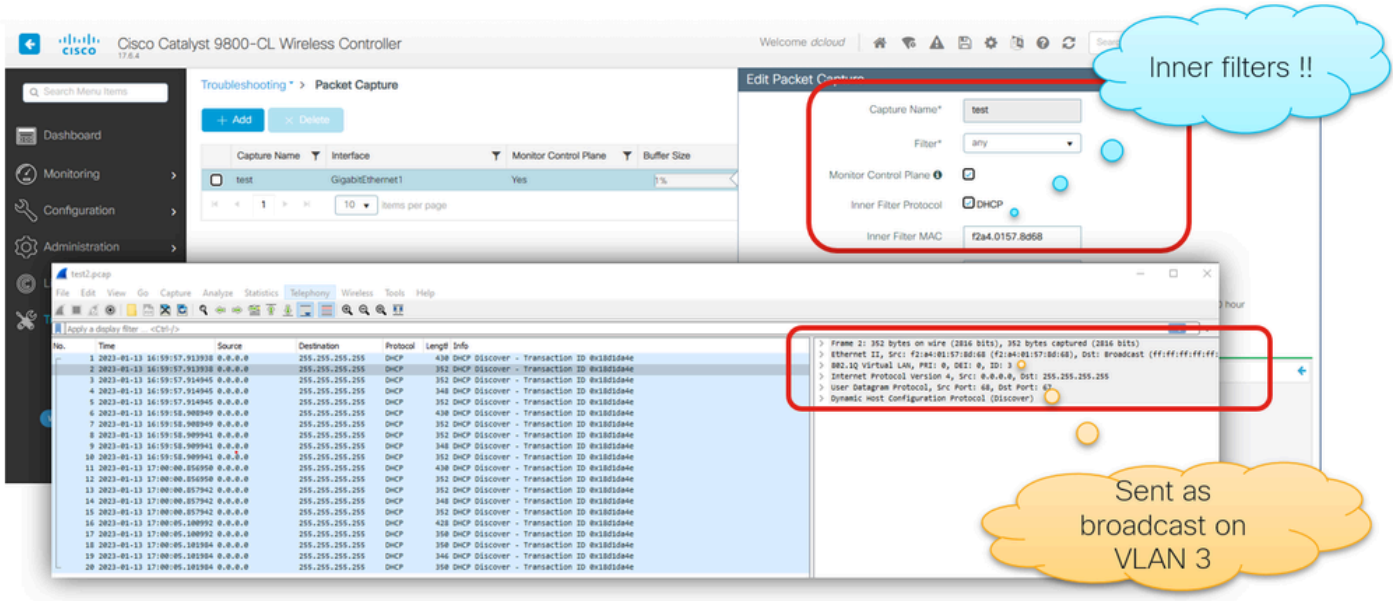
La ACL de redirección define qué tráfico es interceptado y redirigido por la sentencia permit y qué tráfico es ignorado de la interceptación y redirección con una sentencia deny.

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?

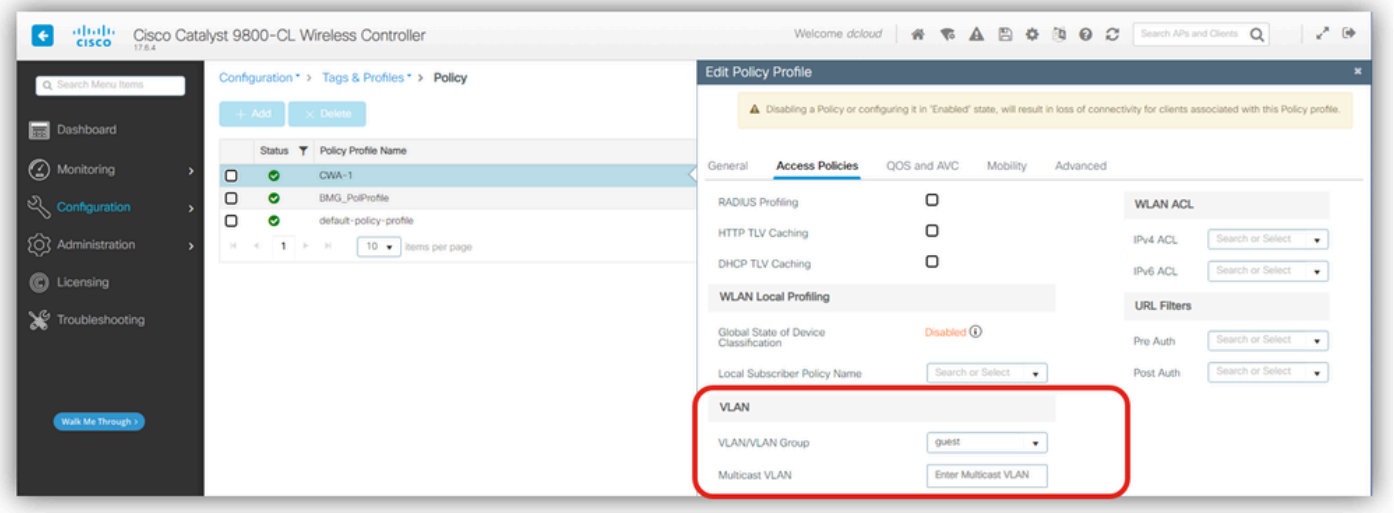
Verifique con EPC si ocurre el intercambio DHCP. EPC se puede utilizar con filtros internos como el protocolo DHCP y/o MAC de filtro interno, donde podemos utilizar la dirección MAC del dispositivo cliente y obtenemos en el EPC sólo paquetes DHCP enviados o enviados a la dirección MAC del dispositivo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

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



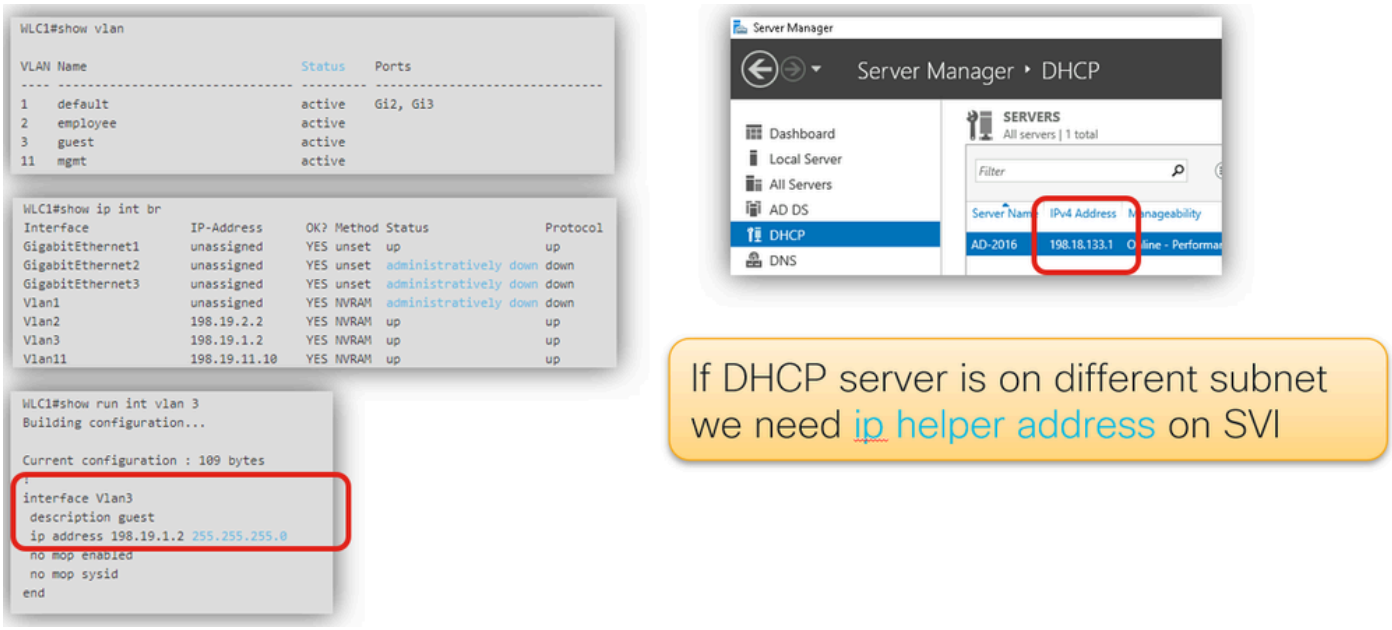
WLC EPC para verificar DHCP

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



VLAN en el perfil de políticas

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



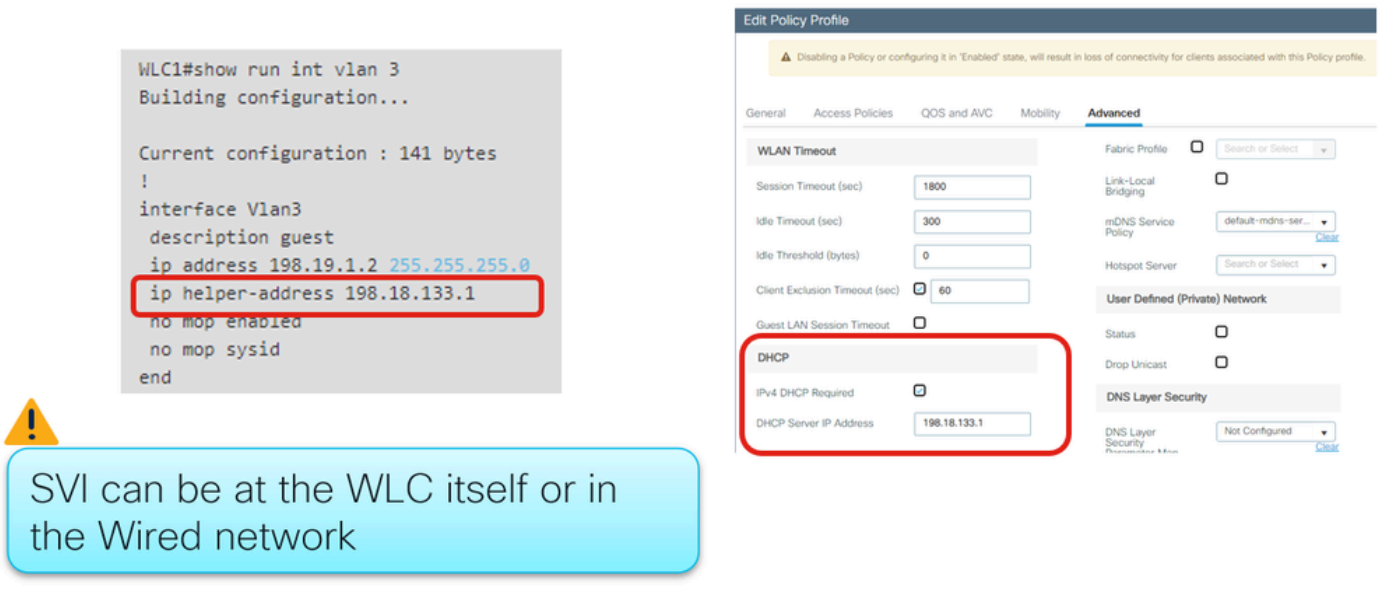
VLAN, puerto de switch y subred DHCP

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.

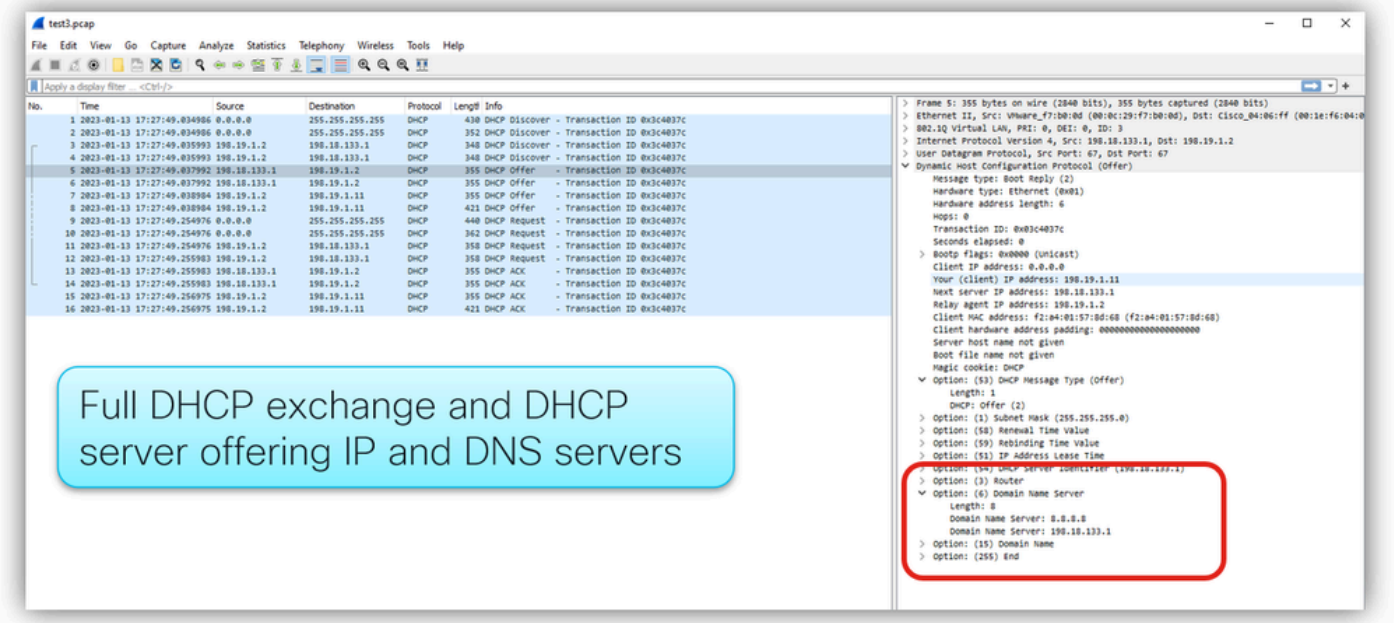
En cualquiera de los casos, el comando ip helper-address debe agregarse a la SVI independientemente de dónde resida.

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



Ip helper-address at SVI or Policy Profile

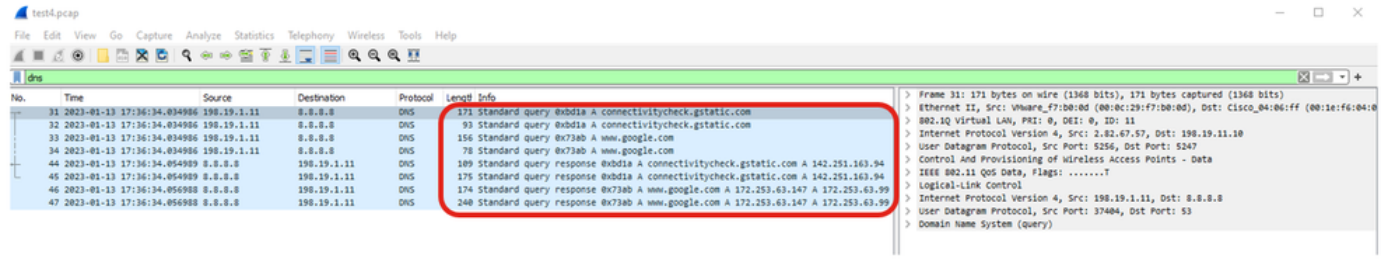
A continuación, puede comprobar con EPC si el intercambio DHCP funciona correctamente y si el servidor DHCP ofrece direcciones IP de servidor DNS:



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:

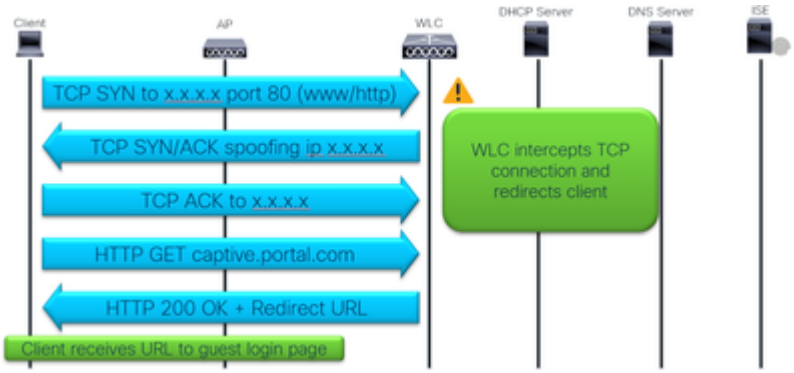


Consultas y respuestas de DNS

- 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?

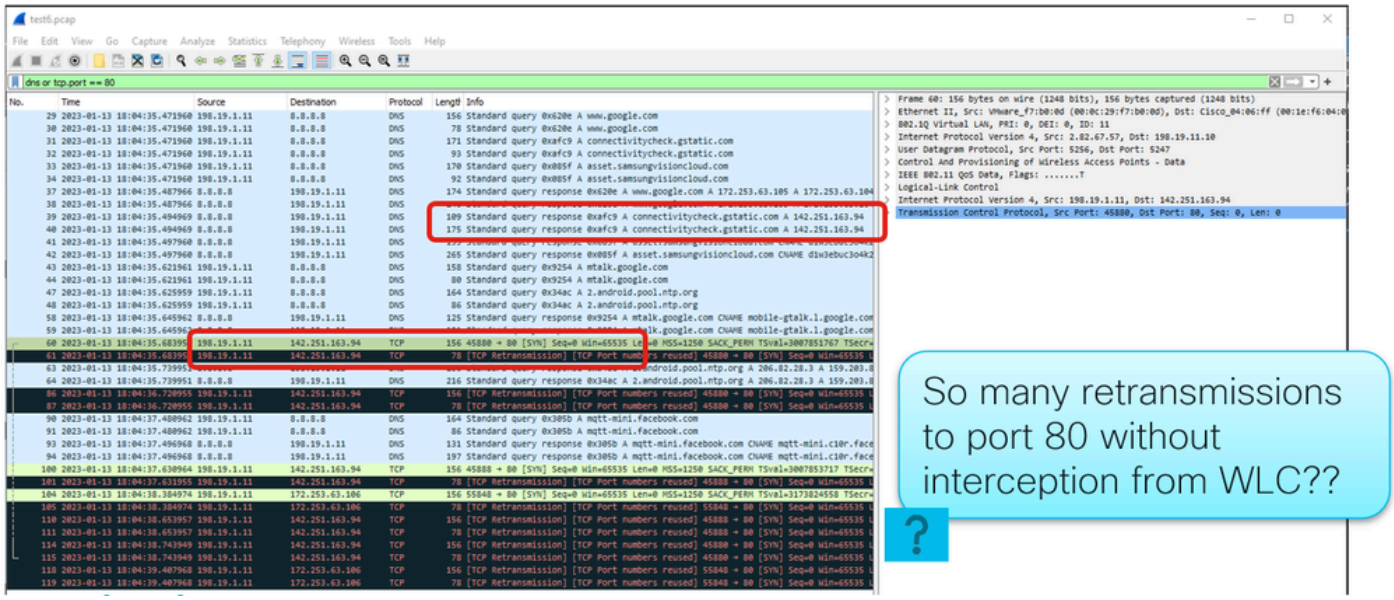
Repasemos el flujo de trabajo...



Interceptación y redirección del tráfico

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

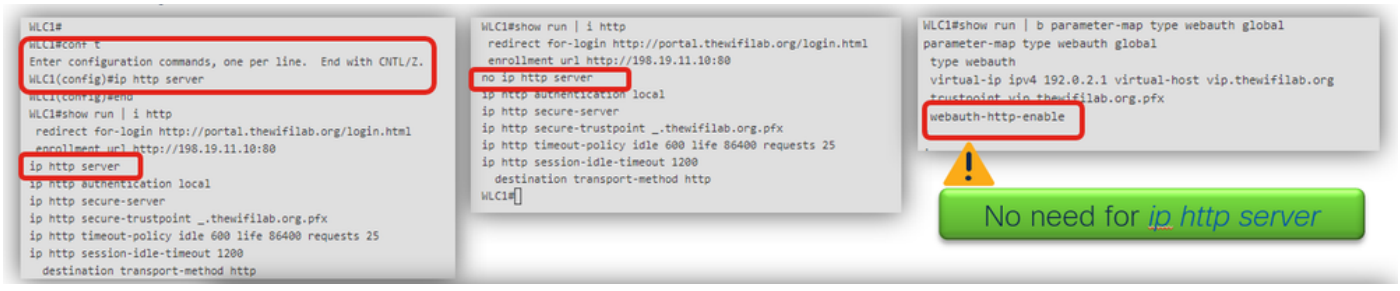
Verifique si el cliente envía el TCP SYN al puerto 80 y el WLC lo intercepta:



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.

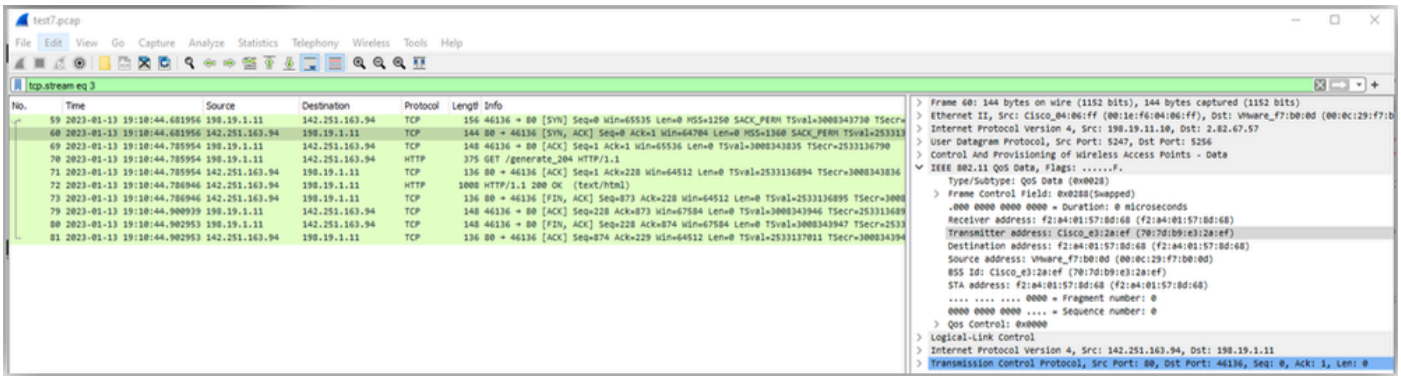
Asegúrese de tener el comando ip http server en la configuración global o webauth-http-enable en parameter-map global:



comandos de intercepción http

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

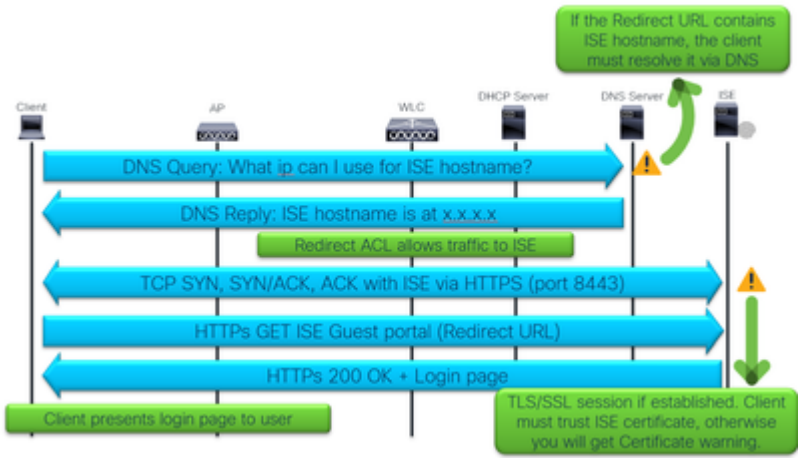
responder al cliente y redirigir.



Interceptación de TCP por WLC

¿Aún no funciona?

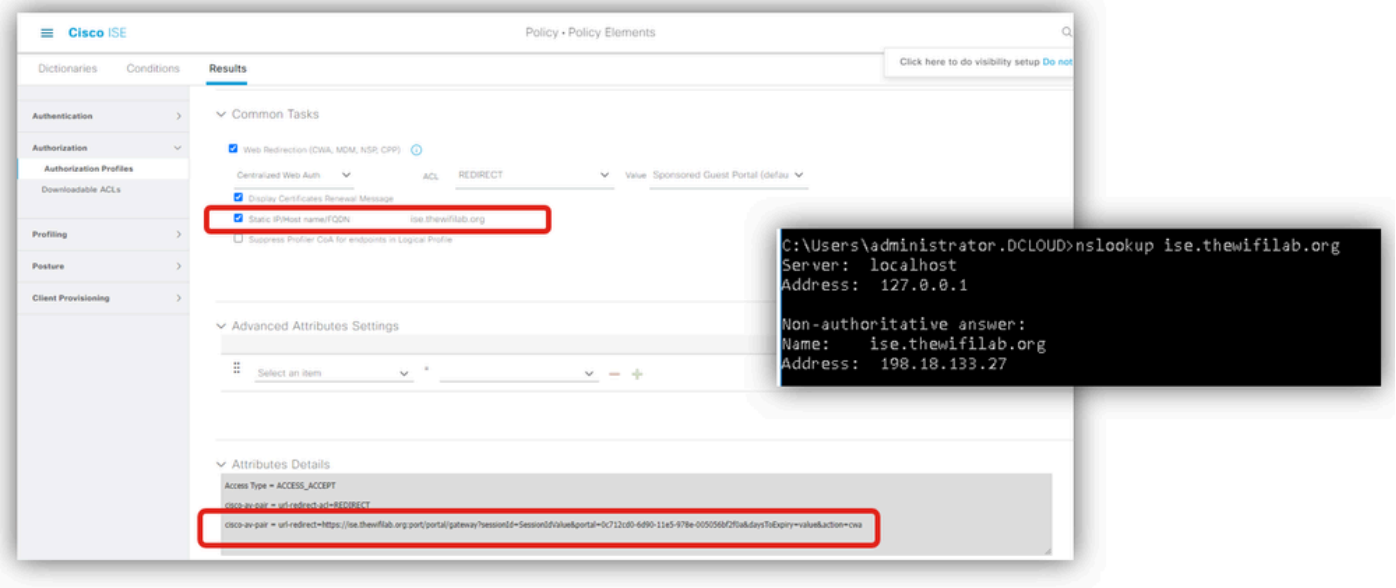
Hay más en el flujo...



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:

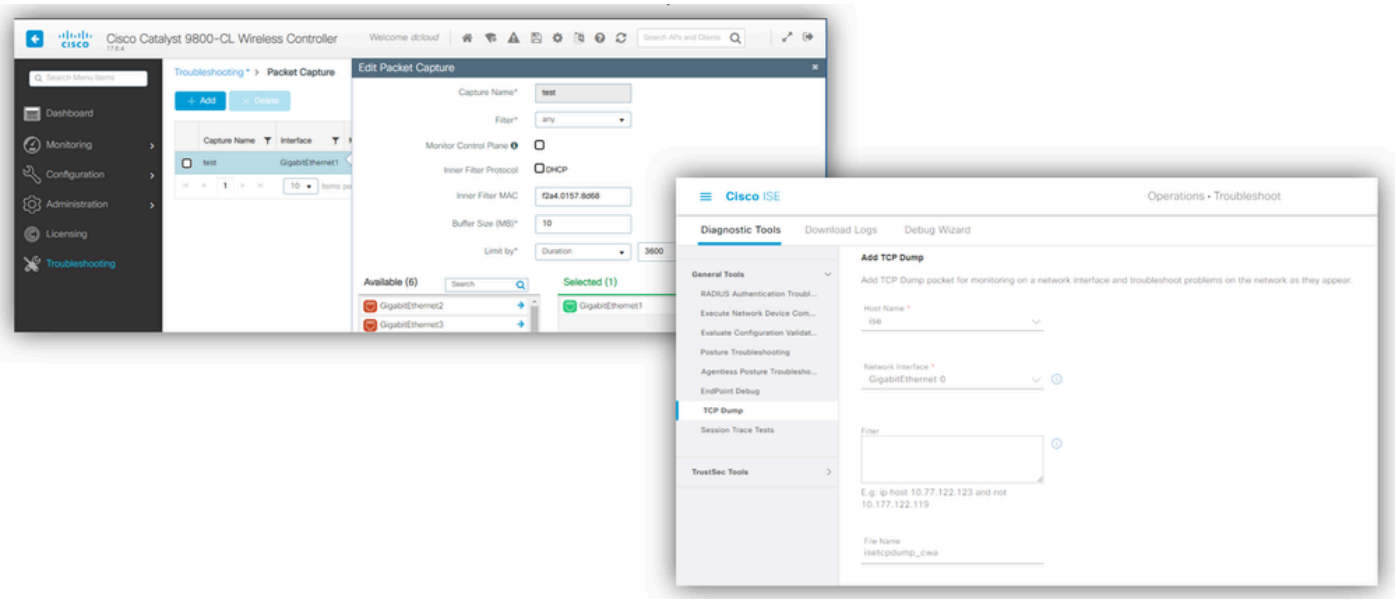


Resolución de nombre de host ISE

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.

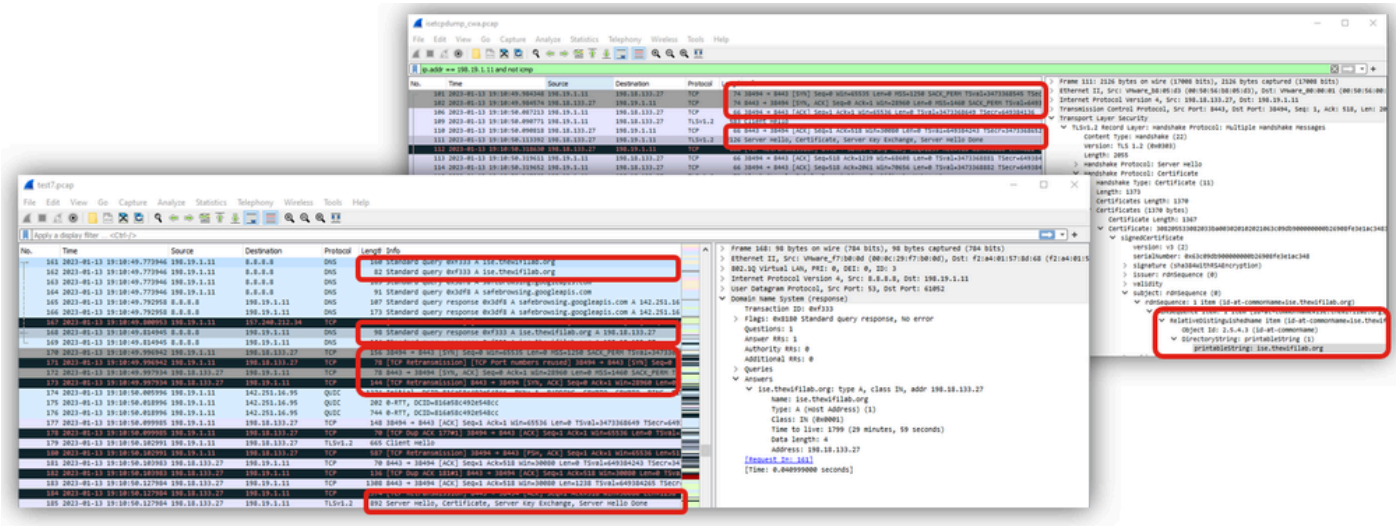
10 - ¿La página de inicio de sesión sigue sin cargarse?

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:



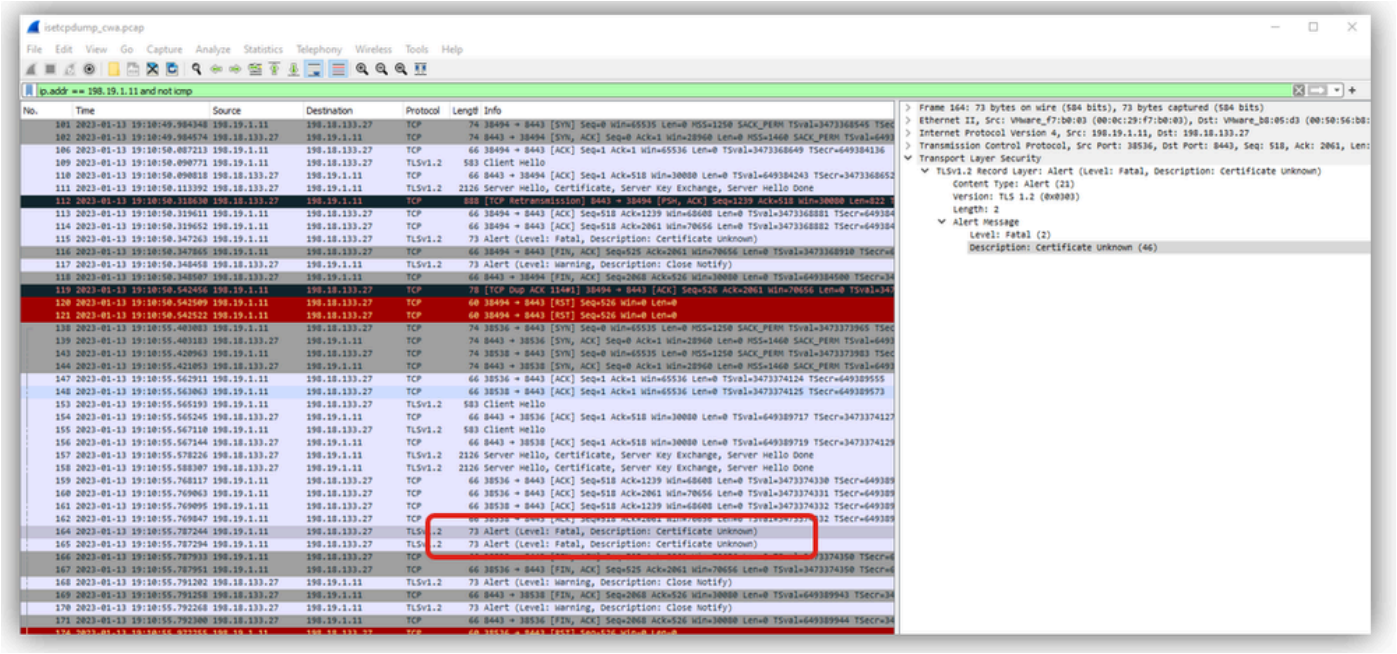
Tráfico WLC e ISE

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.

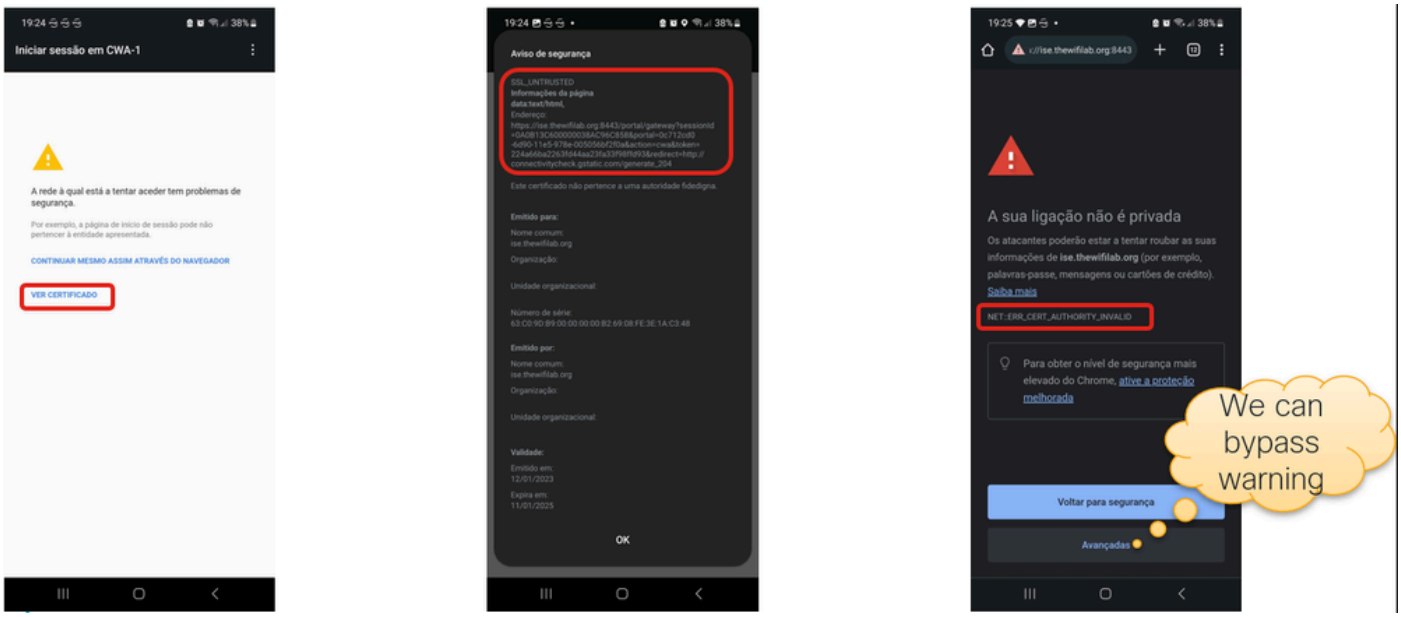
En el volcado de TCP de ISE o EPC del WLC, podemos verificar si el certificado de ISE es confiable.

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

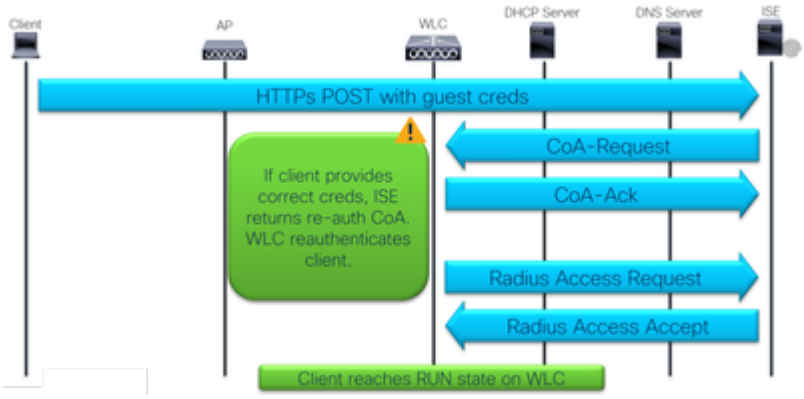
Si verificamos en el lado del cliente, vemos estos ejemplos de salida:



Dispositivo cliente que no confía en el certificado ISE

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

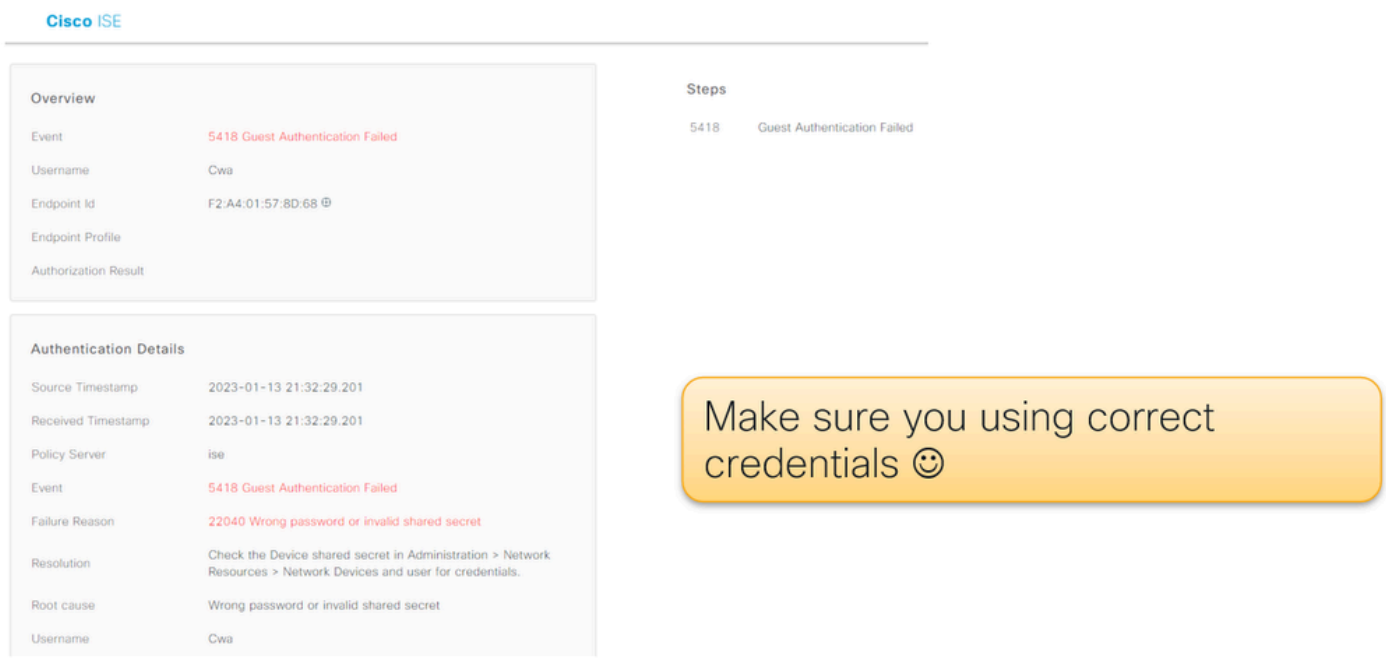
Una última vez comprobando el flujo...



Inicio de sesión del cliente y CoA

12 - ¿Falla el inicio de sesión de invitado?

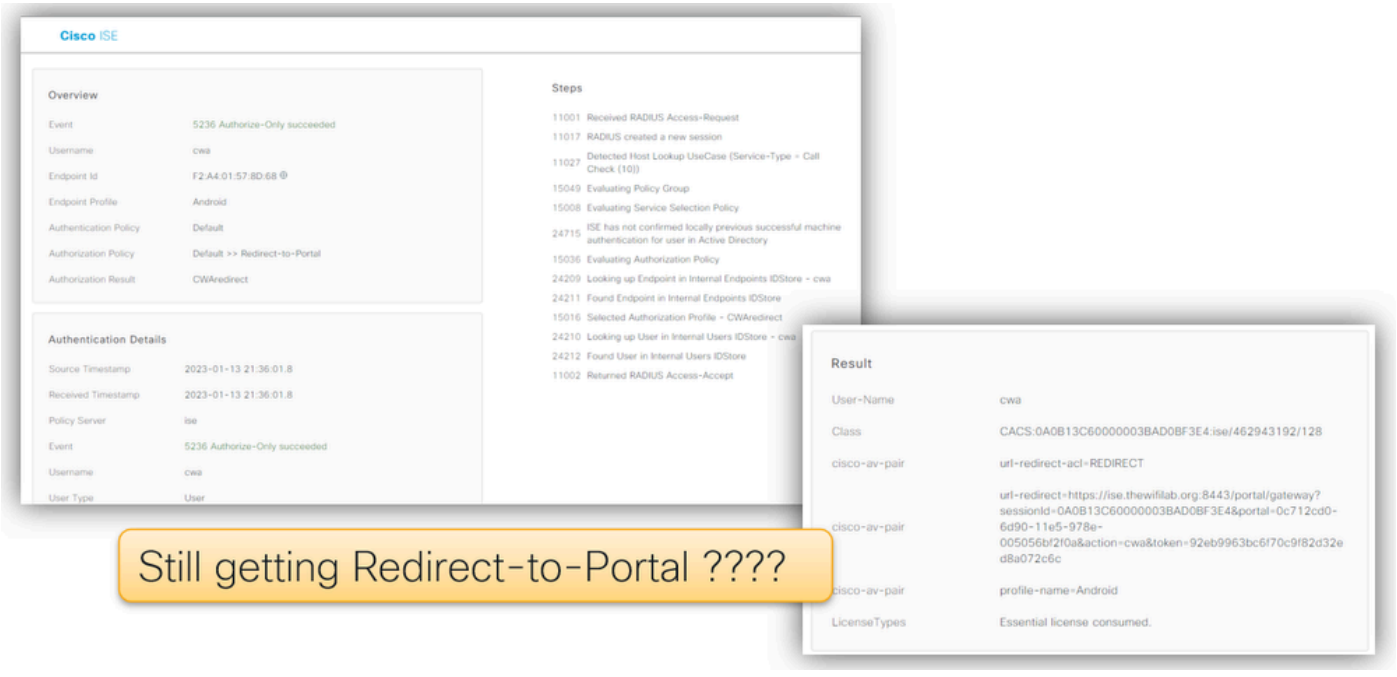
Compruebe los registros de ISE para ver si hay errores de autenticación. Asegúrese de que las credenciales son correctas.



La autenticación de invitado falla debido a credenciales erróneas

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

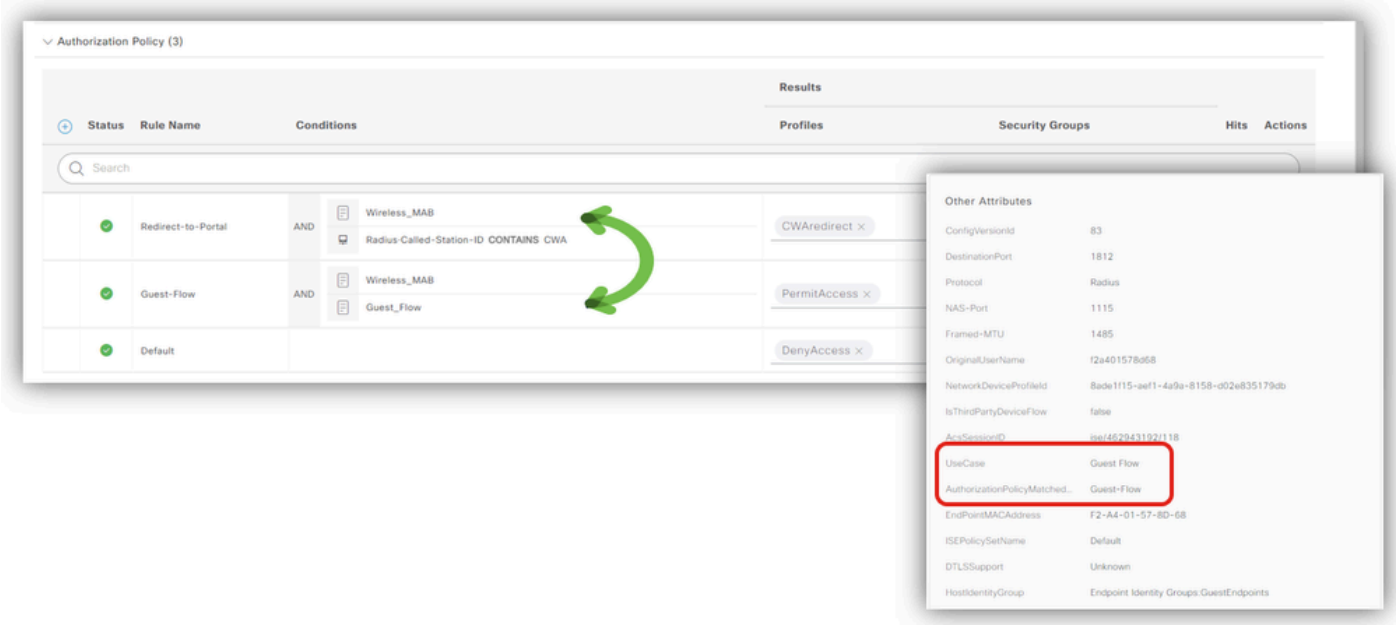
Consulte los registros de ISE para obtener los detalles de autenticación y los resultados:



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.

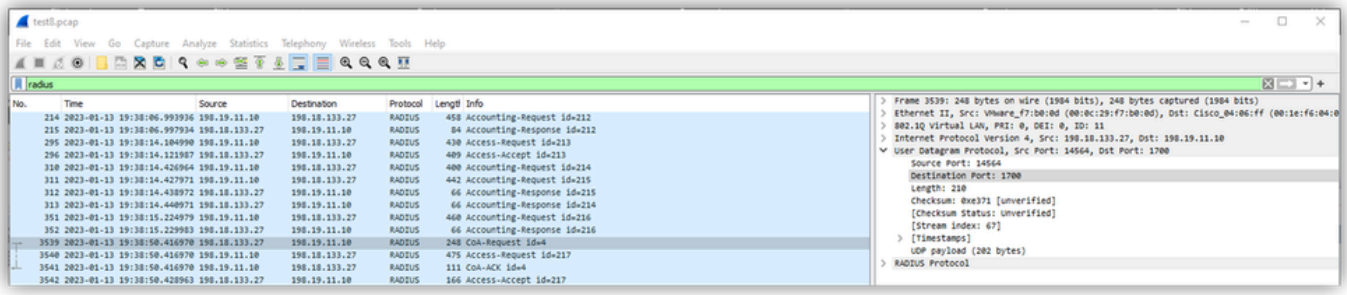
Marque Conjunto de directivas. La verificación de reglas Guest_Flow debe ser anterior a la redirección:



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.



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).