Solucionar problemas da autenticação da Web central (CWA) com o Wireless Lan Controller (WLC) 9800 e o Identity Services Engine (ISE)

Contents

Introdução

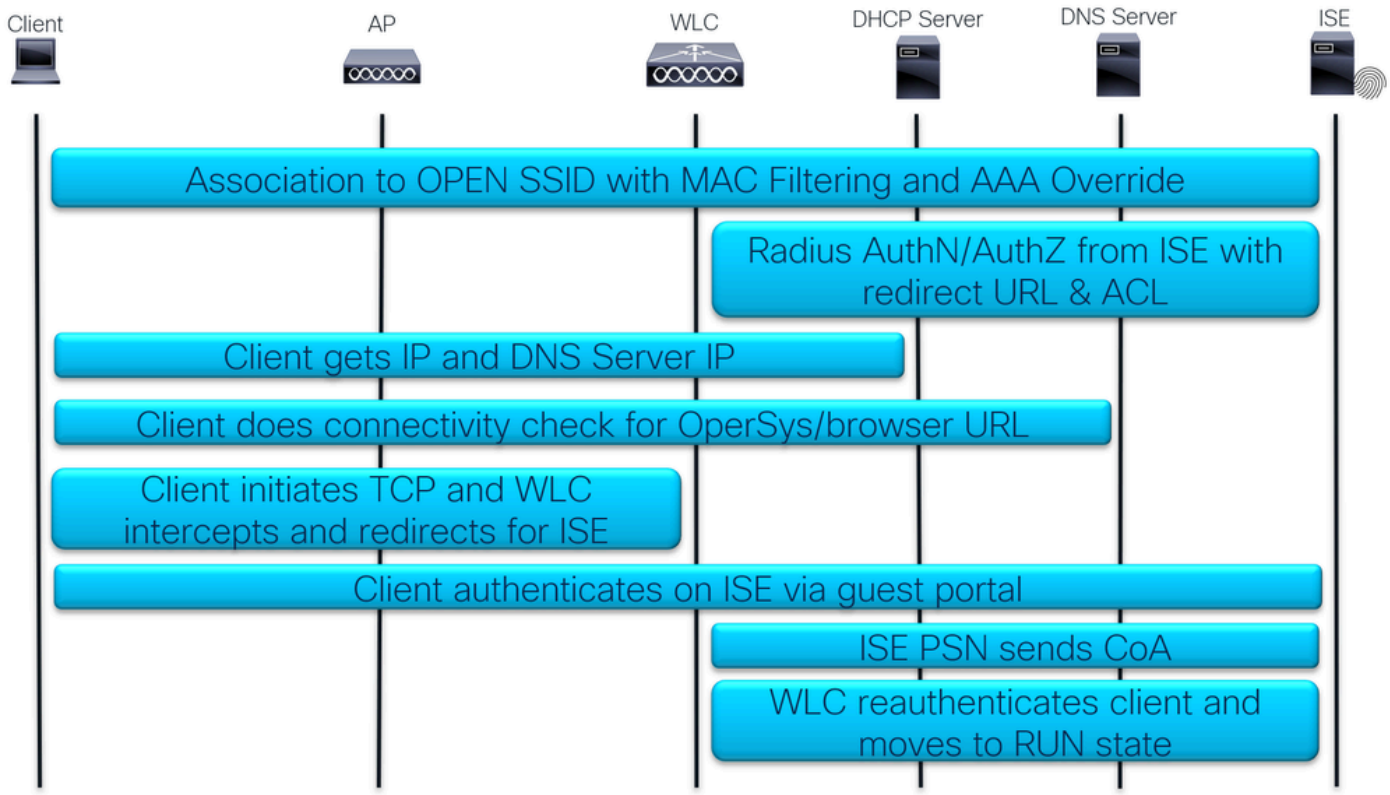
Este documento descreve como solucionar problemas da Central Web Authentication (CWA) com WLC 9800 e ISE.

Informações de fundo

Há tantos dispositivos pessoais atualmente que os administradores de rede que procuram proteger o acesso sem fio normalmente optam por redes sem fio que usam o CWA.
Neste documento, nos concentramos no fluxograma do CWA, que ajuda na solução de problemas comuns que nos afetam.
Examinamos os pontos comuns do processo, como coletar logs relacionados ao CWA, como analisar esses logs e como coletar uma captura de pacote incorporada no WLC para confirmar o fluxo de tráfego.

O CWA é a configuração mais comum para empresas que permitem que os usuários se conectem à rede corporativa usando seus dispositivos pessoais, também conhecidos como BYOD.
Qualquer administrador de rede está interessado nos pontos fracos e nas etapas de solução de problemas a serem executadas para corrigir seus problemas antes da abertura de um caso de TAC.

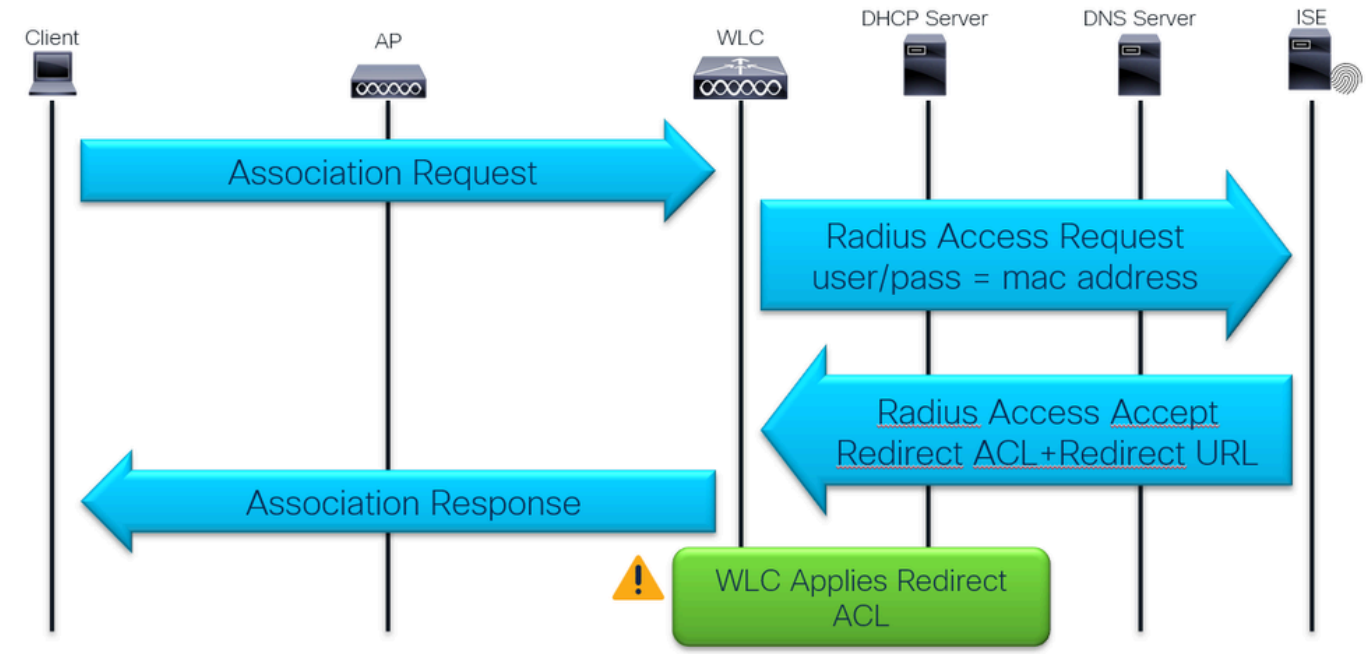
Este é o fluxo de pacotes do CWA:



Fluxo de pacotes do CWA

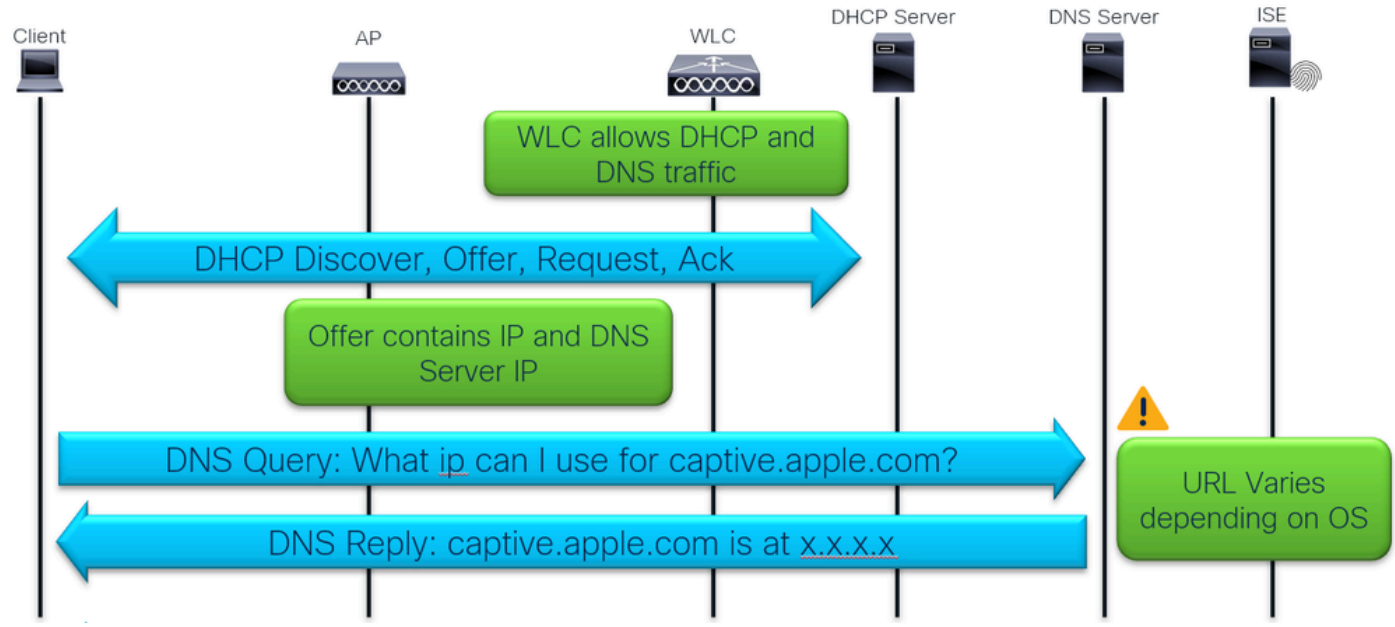
Fluxo detalhado

Primeira associação e autenticação RADIUS:



Primeira associação e autenticação RADIUS

Verificação de DHCP, DNS e conectividade:



DHCP, DNS e verificação de conectividade

A verificação de conectividade é feita usando a detecção do portal cativo pelo sistema operacional ou navegador do dispositivo cliente.

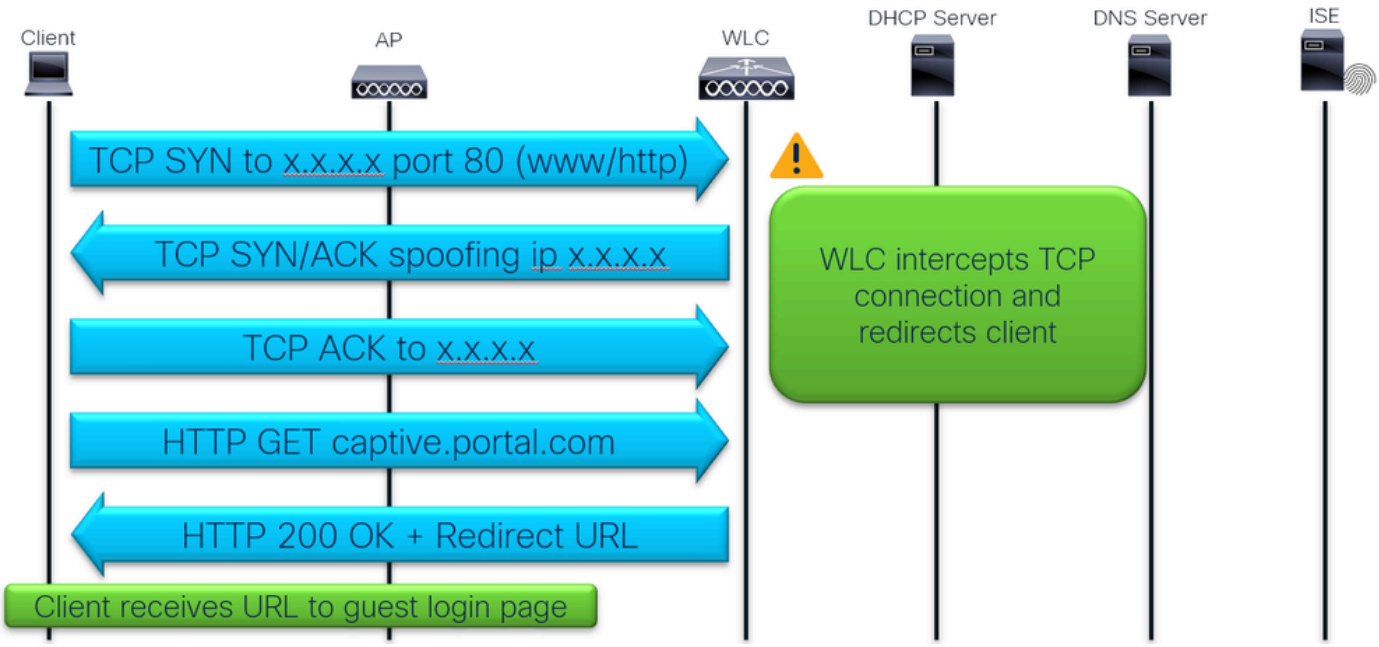
Há SO de dispositivo pré-programado para fazer HTTP GET em relação a um domínio específico

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

E os navegadores também executam esta verificação quando abertos:

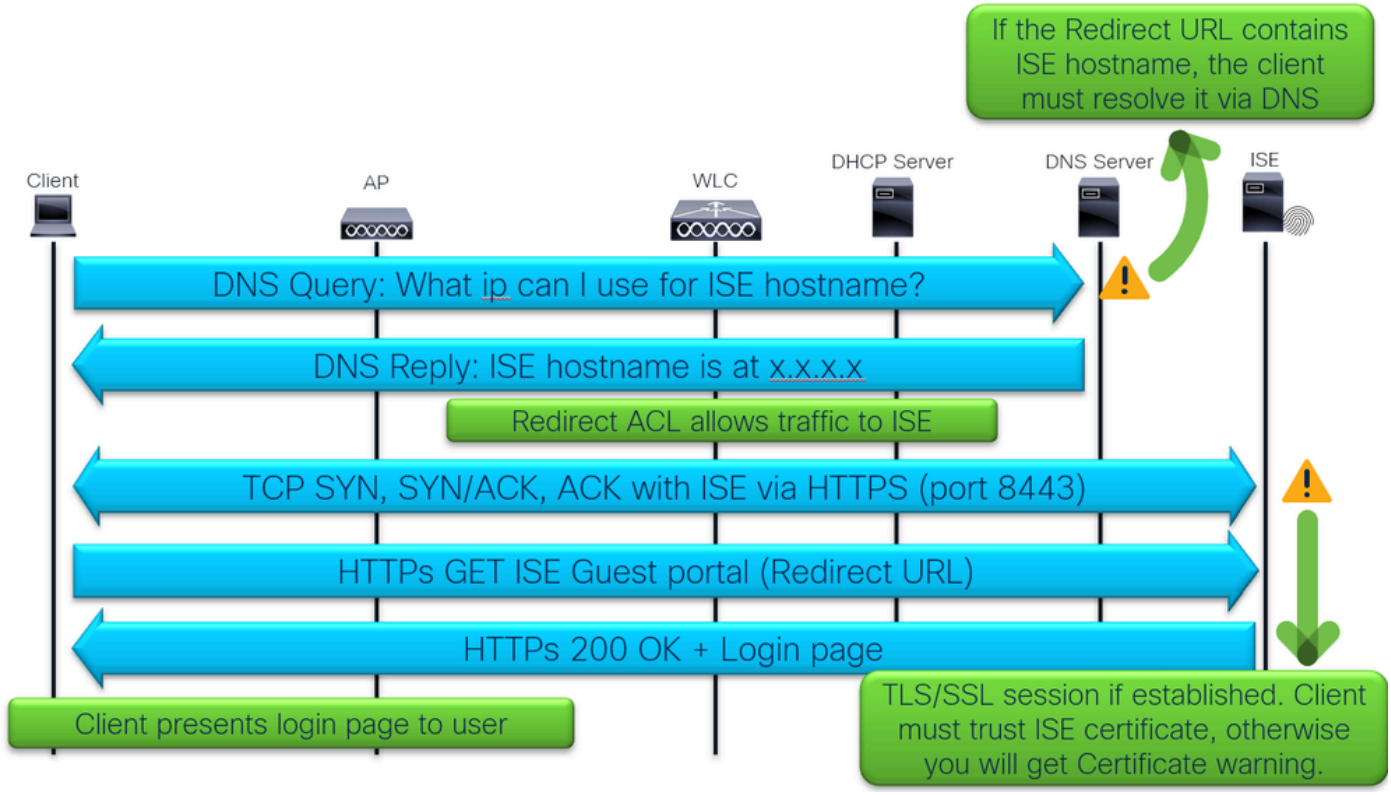
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Interceptação e redirecionamento de tráfego:



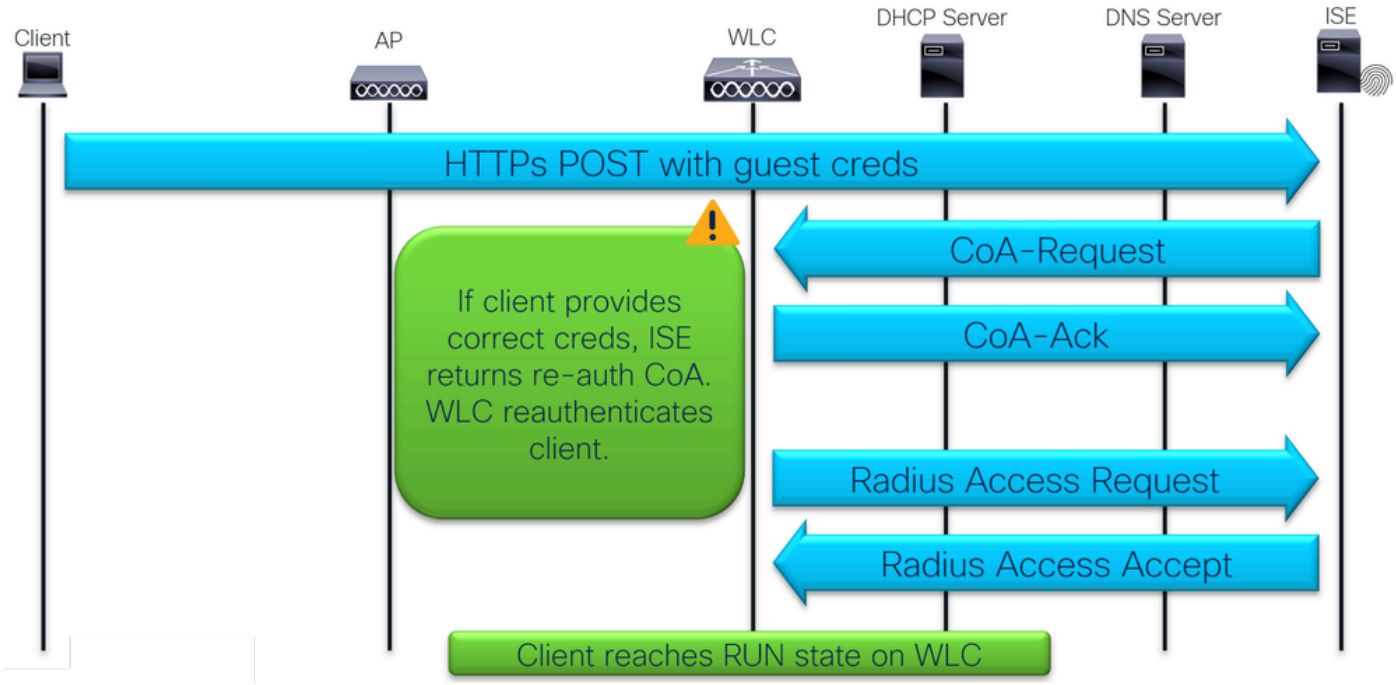
Interceptação e redirecionamento de tráfego

Login do cliente no portal de login de convidado do ISE:



Login do cliente no portal de login de convidado do ISE

Login e CoA do cliente:

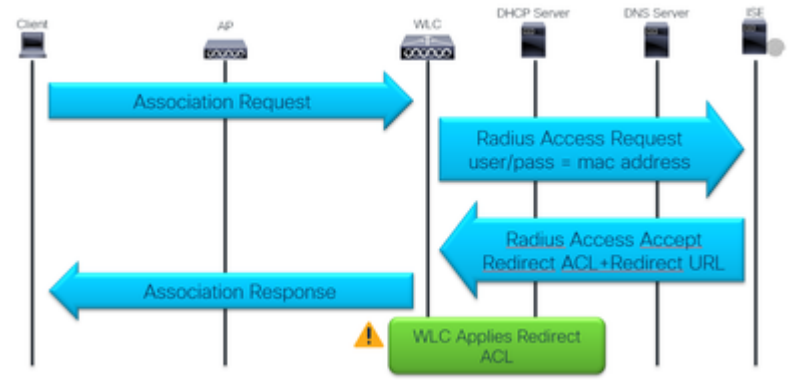


Login e CoA do cliente

Troubleshooting

Sintoma comum: O usuário não está sendo redirecionado para a página de login.

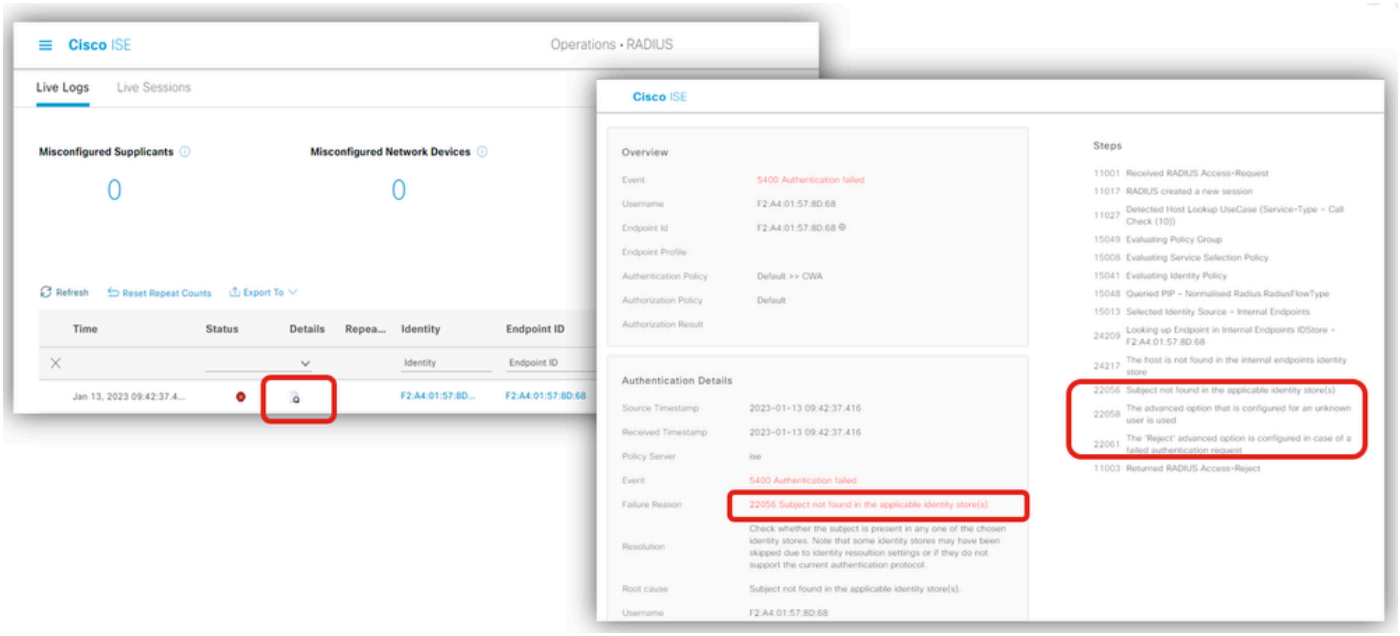
Vamos começar com a primeira parte do fluxo:



Primeira associação e autenticação RADIUS

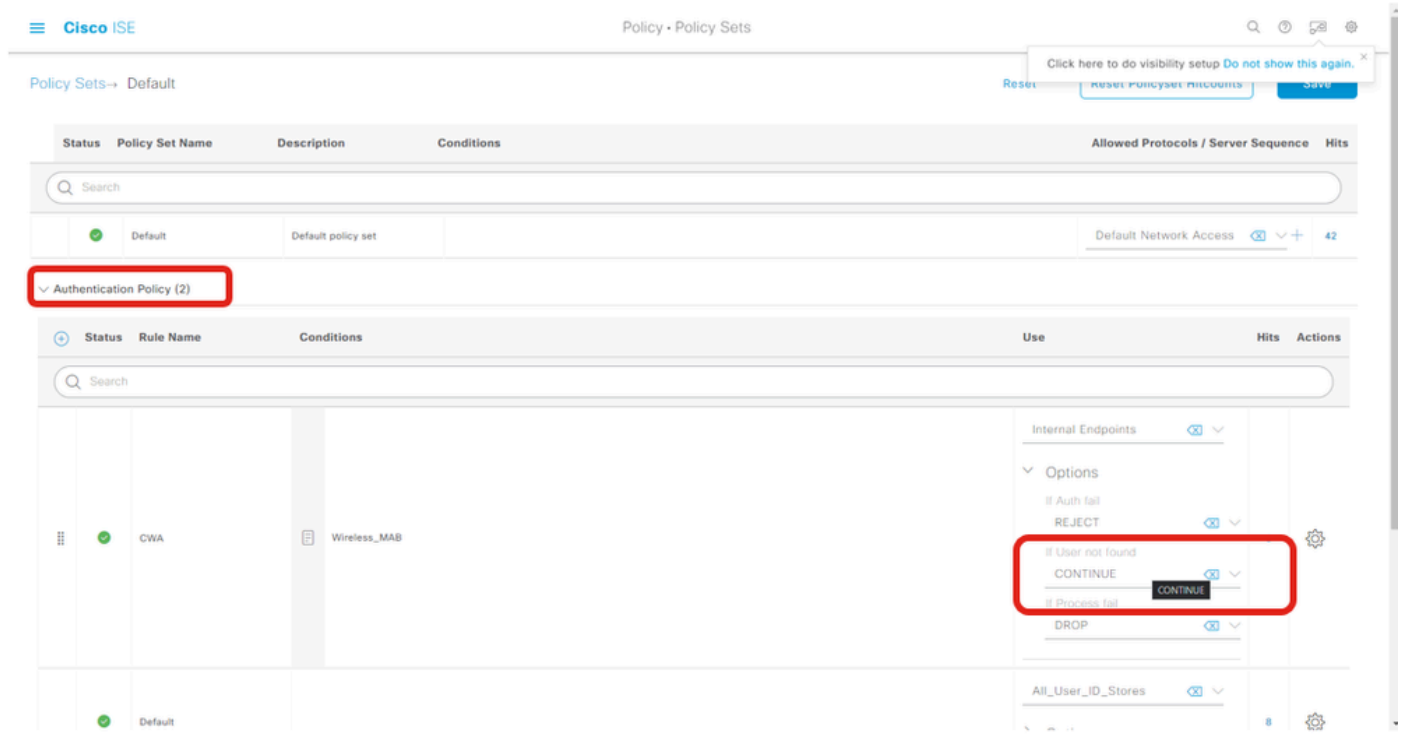
1 - A primeira autenticação RADIUS é bem-sucedida?

Verificar resultado de autenticação de filtragem MAC:



Logs do ISE ao vivo mostrando o resultado da autenticação de filtragem MAC

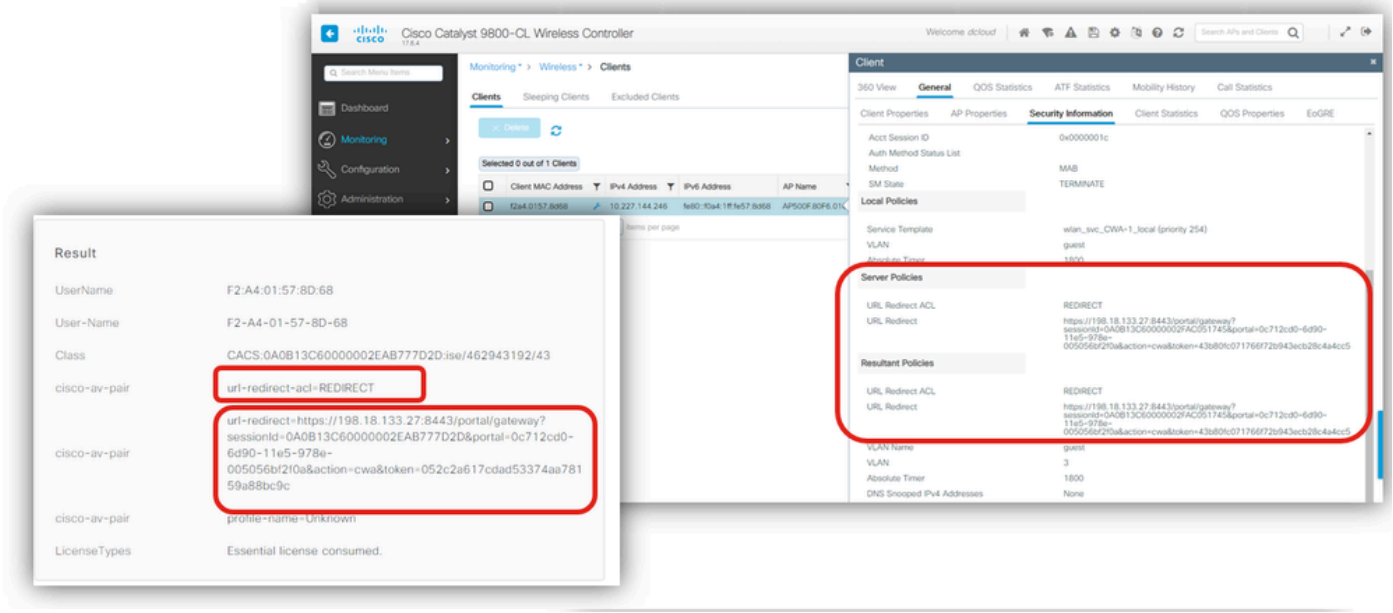
Verifique se a opção avançada para a autenticação está definida como "Continuar" se o usuário não for encontrado:



Opção avançada de usuário não encontrado

2 - A WLC recebe a URL e a ACL de redirecionamento?

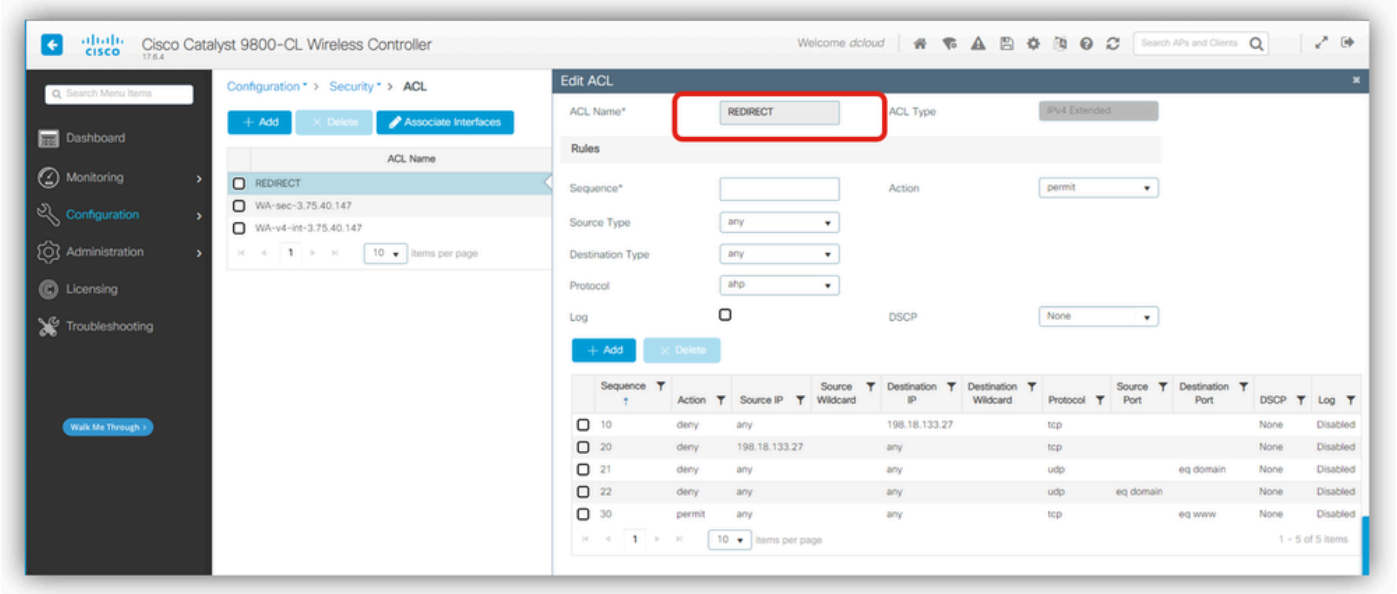
Verifique os logs ao vivo do ISE e as informações de segurança do cliente WLC em Monitoring (Monitoramento). Verifique se o ISE envia o URL de redirecionamento e a ACL em Access Accept (Aceitação de acesso) e se ele é recebido pelo WLC e aplicado ao cliente nos detalhes do cliente:



Redirecionar ACL e URL

3 - A ACL de redirecionamento está correta?

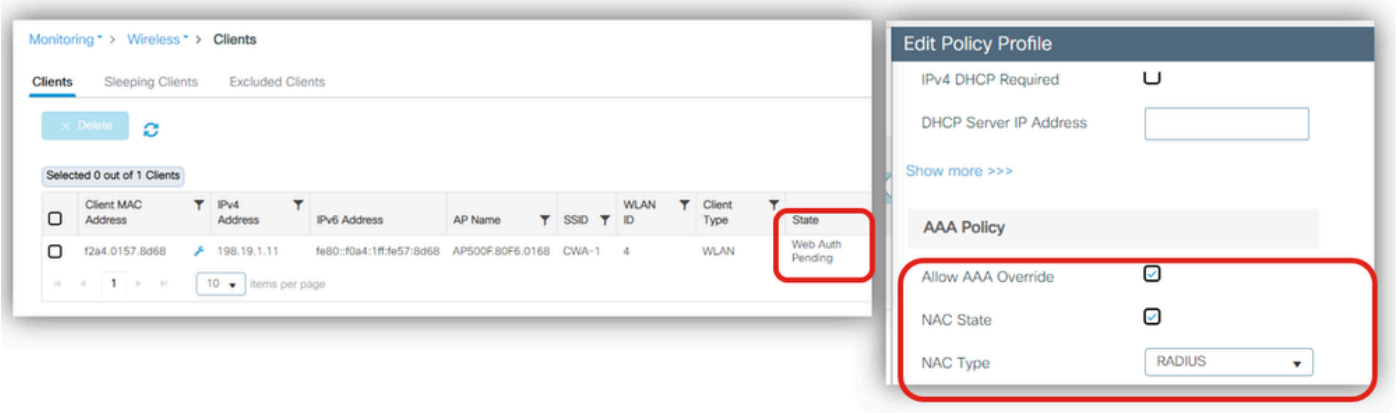
Verifique se há erros de digitação no nome da ACL. Certifique-se de que seja exatamente igual ao envio pelo ISE:



Redirecionar verificação de ACL

4 - O cliente foi movido para Web-Auth Pending?

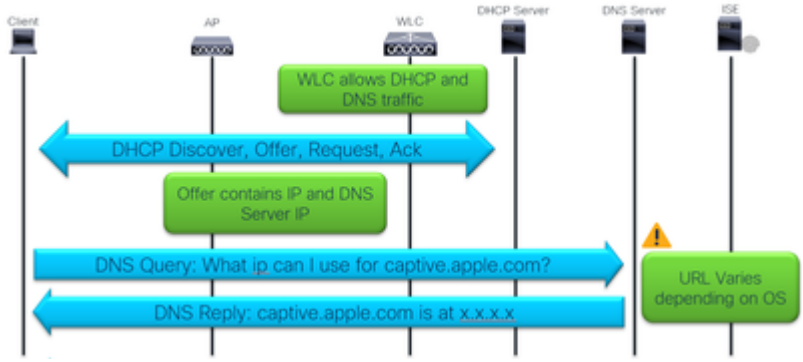
Verifique os detalhes do cliente para o estado "Autenticação da Web pendente". Se não estiver nesse estado, verifique se a substituição de AAA e o NAC Radius estão habilitados no perfil de política:



Detalhes do cliente, aaa override e RADIUS NAC

Ainda não está funcionando?

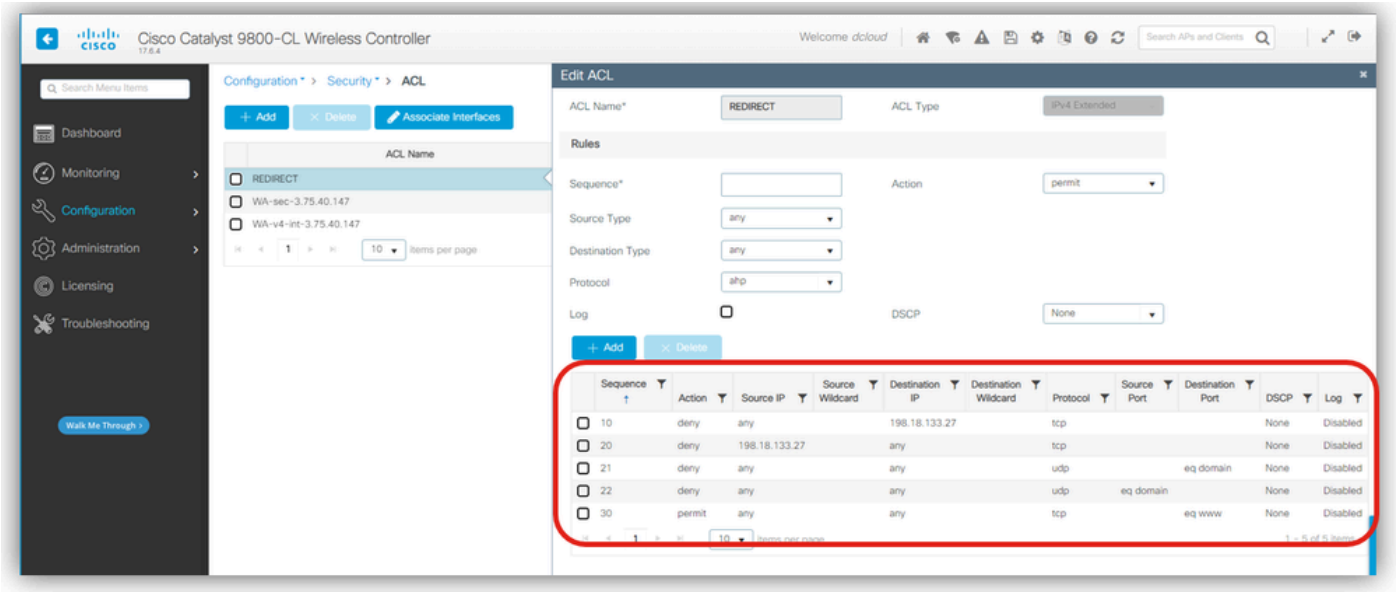
Vamos rever o fluxo...



DHCP, DNS e verificação de conectividade

5 - O WLC permite o tráfego DHCP e DNS?

Verifique o conteúdo da ACL de redirecionamento na WLC:



Redirecionar o conteúdo da ACL na WLC

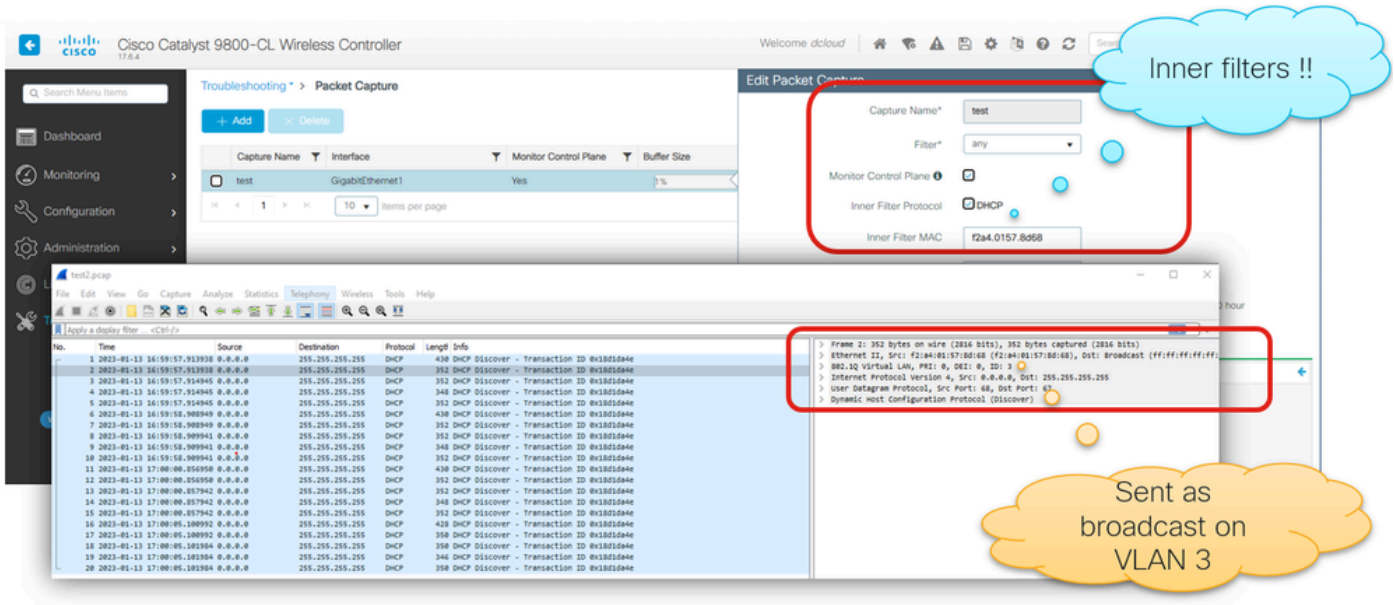
A ACL de redirecionamento define qual tráfego é interceptado e redirecionado pela instrução permit e qual tráfego é ignorado da interceptação e redirecionamento com uma instrução deny.

Neste exemplo, permitimos que o DNS e o tráfego de/para o endereço IP do ISE fluam e interceptem qualquer tráfego tcp na porta 80 (www).

6 - O servidor DHCP recebe a Descoberta/Solicitação DHCP?

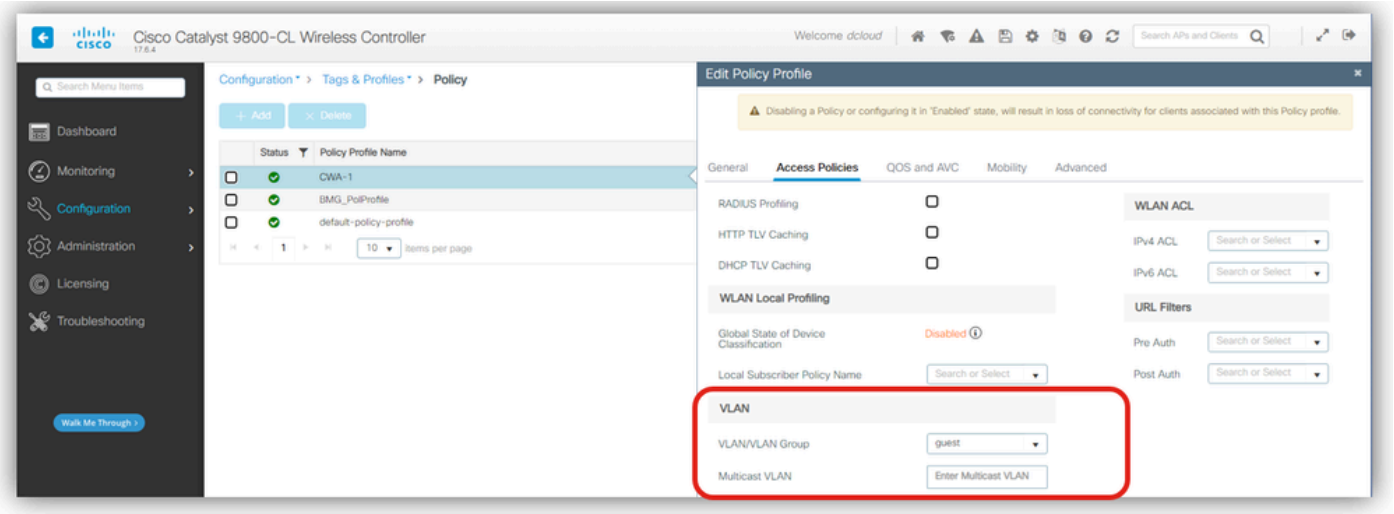
Verifique com o EPC se ocorre a troca de DHCP. O EPC pode ser usado com filtros internos, como o protocolo DHCP e/ou o MAC do filtro interno, onde podemos usar o endereço MAC do dispositivo cliente e obtemos no EPC apenas pacotes DHCP enviados pelo endereço MAC do dispositivo cliente ou enviados a ele.

Neste exemplo, podemos ver os pacotes DHCP Discover enviados como broadcast na VLAN 3:



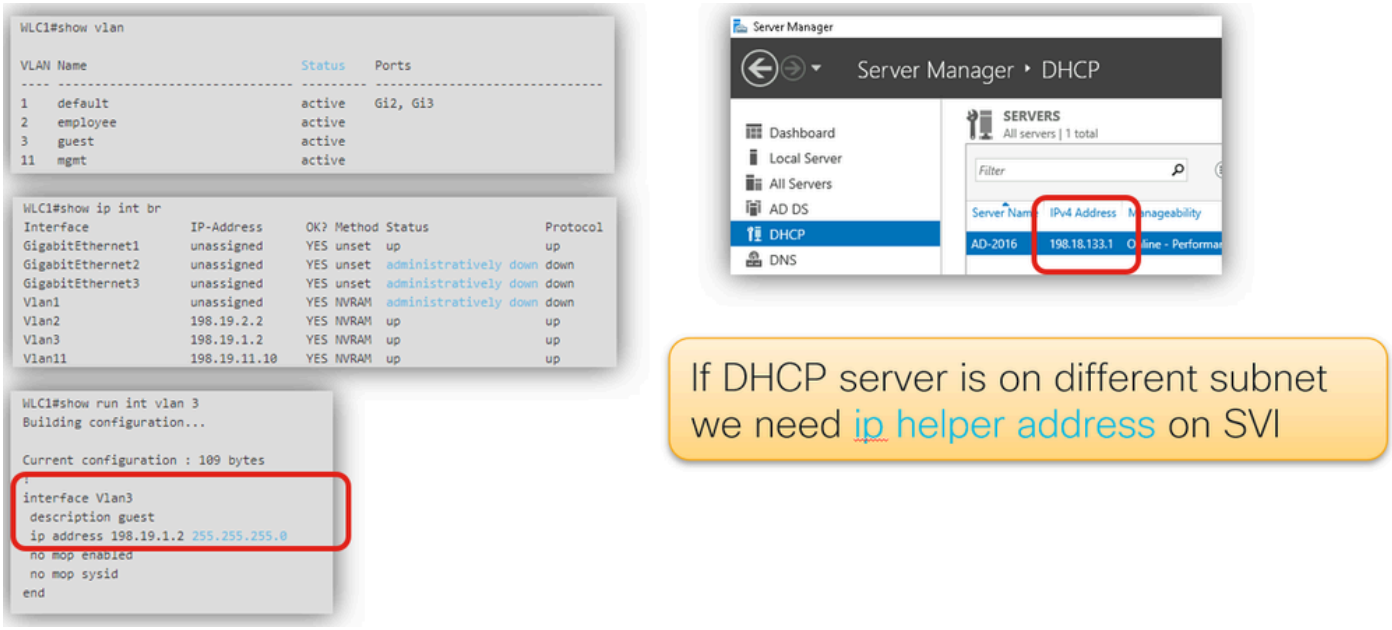
WLC EPC para verificar o DHCP

Confirme a VLAN do cliente esperada no perfil de política:



VLAN no perfil de política

Verifique a configuração da VLAN da WLC e do tronco da porta do switch e a sub-rede DHCP:



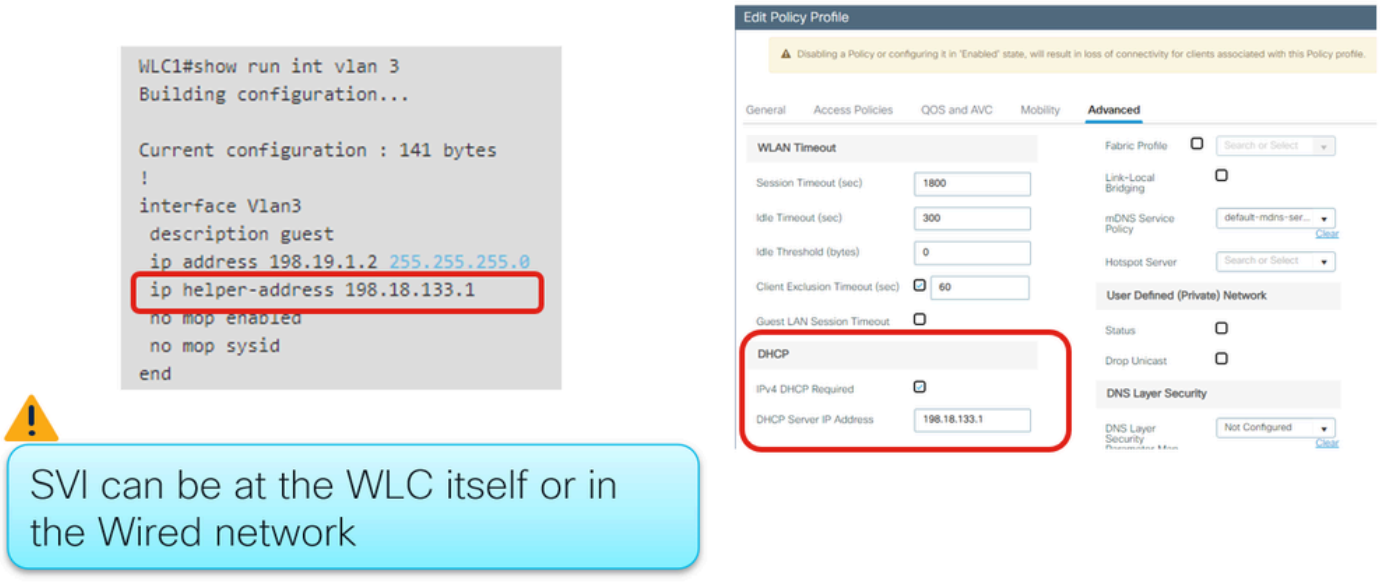
VLAN, porta do switch e sub-rede DHCP

Podemos ver que a VLAN 3 existe na WLC e também tem SVI para a VLAN 3. No entanto, quando verificamos o endereço IP do servidor DHCP, ele está em uma sub-rede diferente, portanto, precisamos do endereço IP do auxiliar na SVI.

As práticas recomendadas determinam que o SVI para sub-redes de clientes seja configurado na infraestrutura com fio e evite-o na WLC.

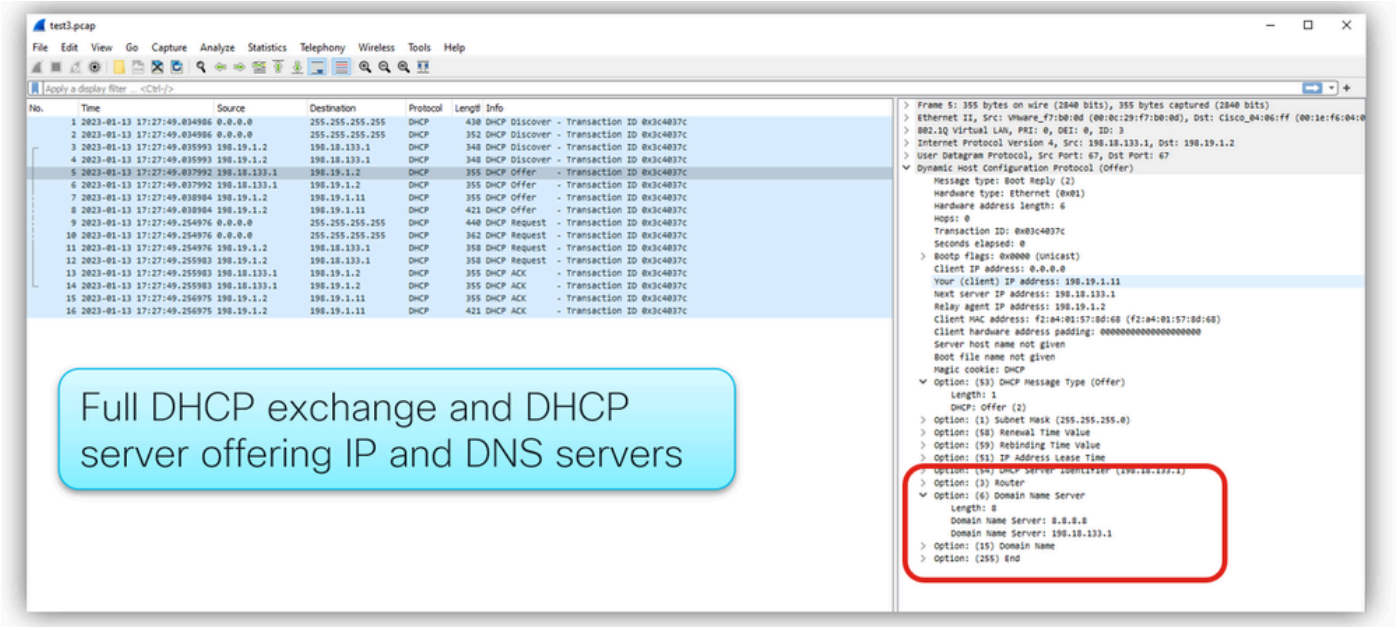
Em qualquer um dos casos, o comando ip helper-address precisa ser adicionado ao SVI, independentemente de onde ele resida.

Uma alternativa é configurar o endereço IP do servidor DHCP no perfil de Política:



Ip helper-address at SVI or Policy Profile

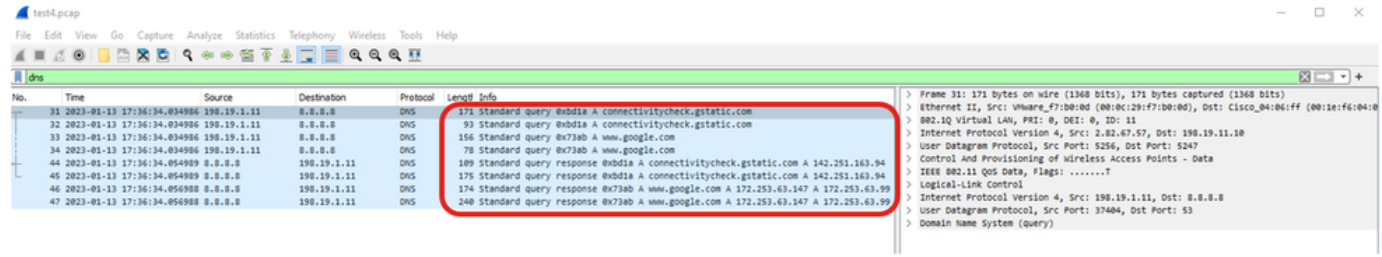
Você pode verificar com o EPC se a troca de DHCP agora está ok e se o servidor DHCP oferece IP(s) de servidor DNS:



Detalhes da oferta DHCP do IP do servidor DNS

7 - O redirecionamento automático ocorre?

Verifique com o WLC EPC se o servidor DNS responde às consultas:

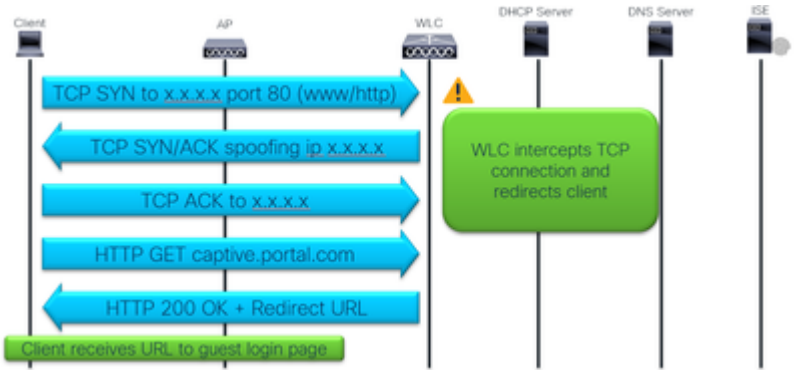


Consulta e respostas DNS

- Se o redirecionamento não for automático, abra um navegador e tente um endereço IP aleatório. Por exemplo, 10.0.0.1.
- Se o redirecionamento funcionar, é possível que você tenha um problema de resolução DNS.

Ainda não está funcionando?

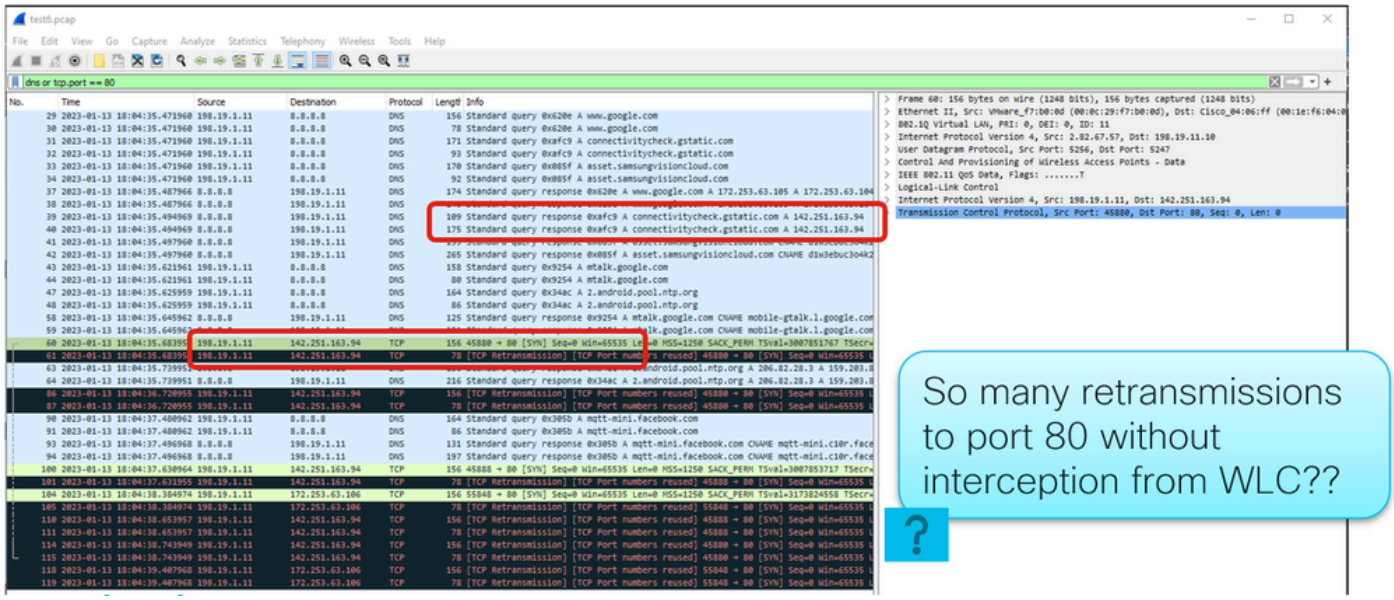
Vamos rever o fluxo...



Interceptação e redirecionamento de tráfego

8 - O navegador não mostra a página de login?

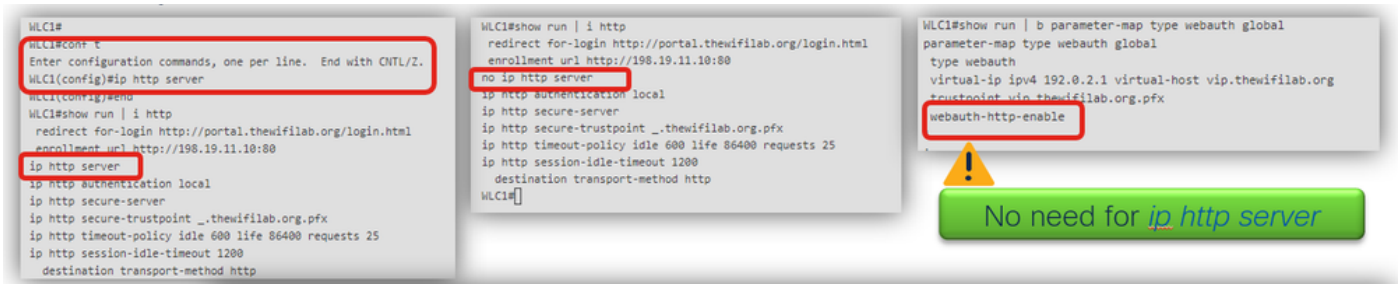
Verifique se o cliente envia o TCP SYN à porta 80 e o WLC o intercepta:



Retransmissões TCP para a porta 80

Aqui podemos ver que o cliente envia pacotes TCP SYN para a porta 80, mas não recebe nenhuma resposta e faz retransmissões TCP.

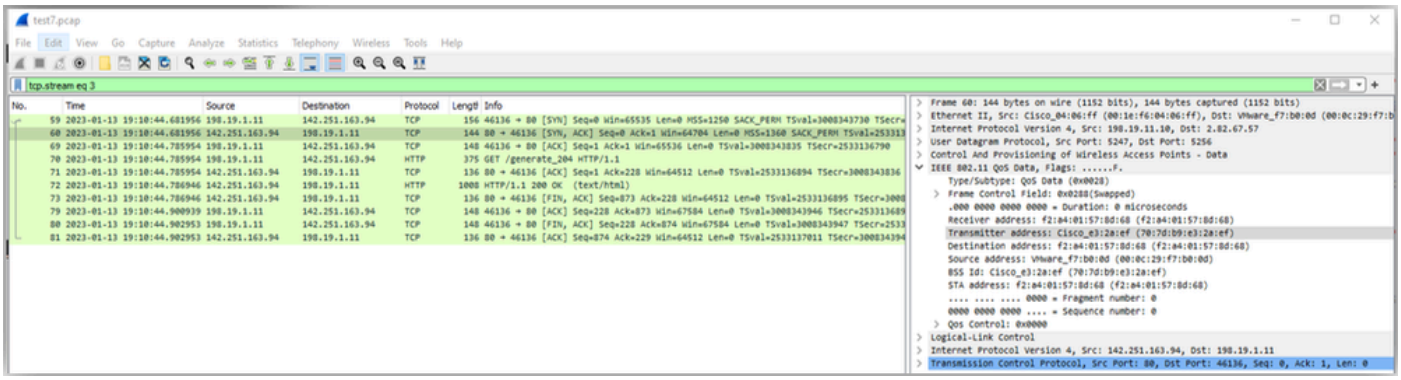
Certifique-se de ter o comando ip http server na configuração global ou webauth-http-enable no global parameter-map:



comandos de interceptação http

Após o comando, a WLC intercepta o TCP e falsifica o endereço IP de destino para responder ao

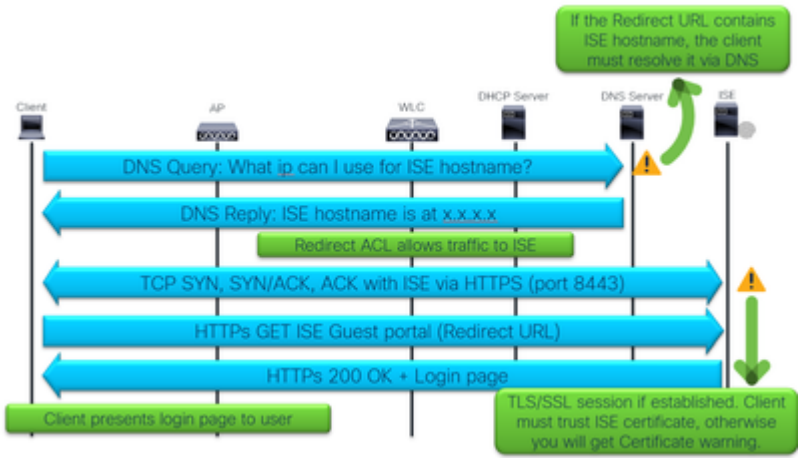
cliente e redirecioná-lo.



Interceptação TCP por WLC

Ainda não está funcionando?

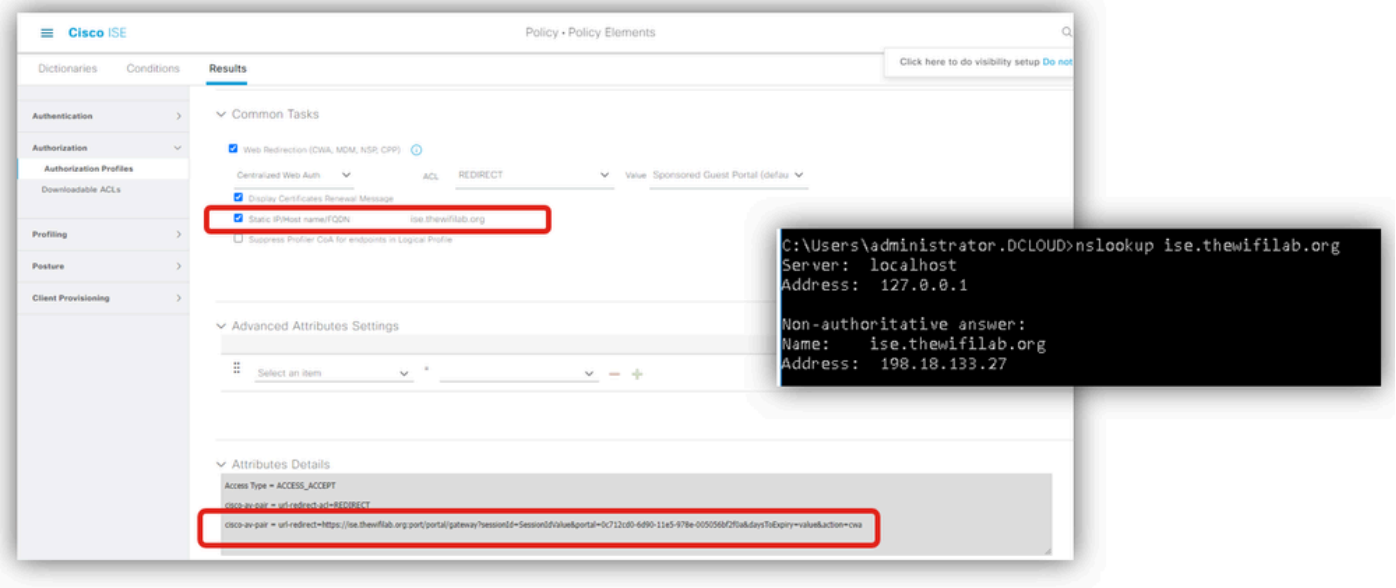
Há mais no fluxo...



Login do cliente no portal de login de convidado do ISE

9 - O cliente pode resolver o nome de host do ISE?

Verifique se a URL de redirecionamento usa IP ou nome de host e se o cliente resolve o nome de host ISE:

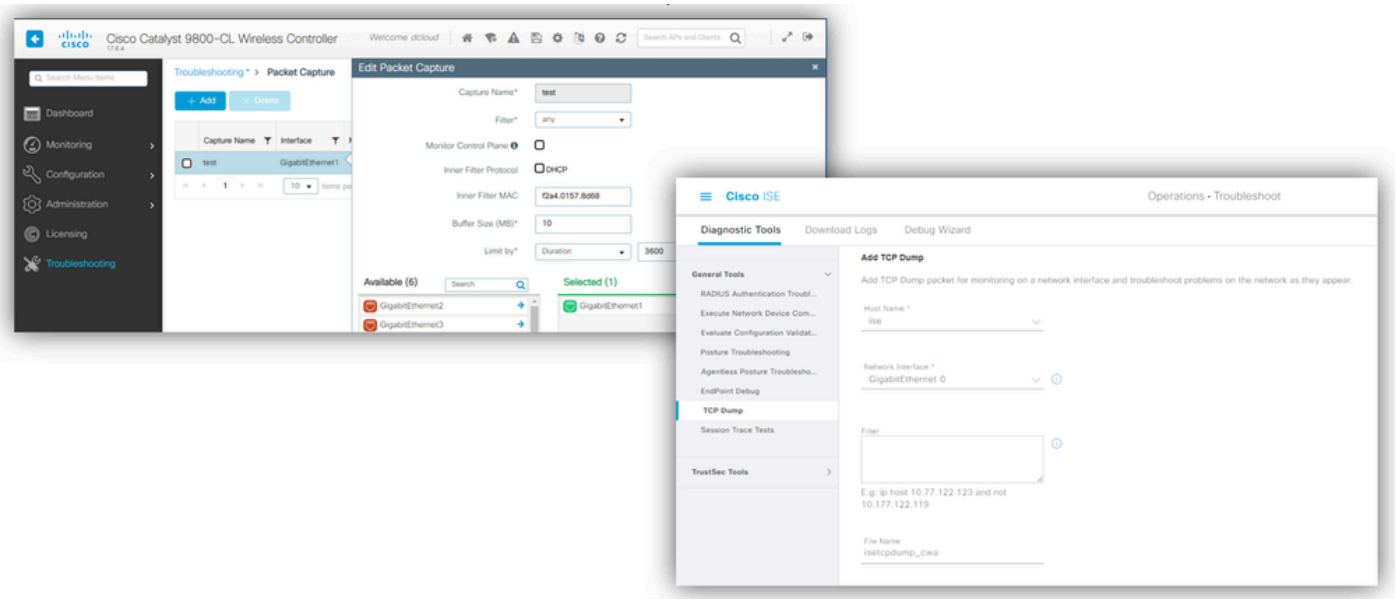


Resolução de nome de host ISE

Um problema comum é visto quando a URL de redirecionamento contém o nome de host do ISE, no entanto, o dispositivo cliente não consegue resolver esse nome de host para o endereço IP do ISE. Se o nome de host for usado, verifique se ele pode ser resolvido via DNS.

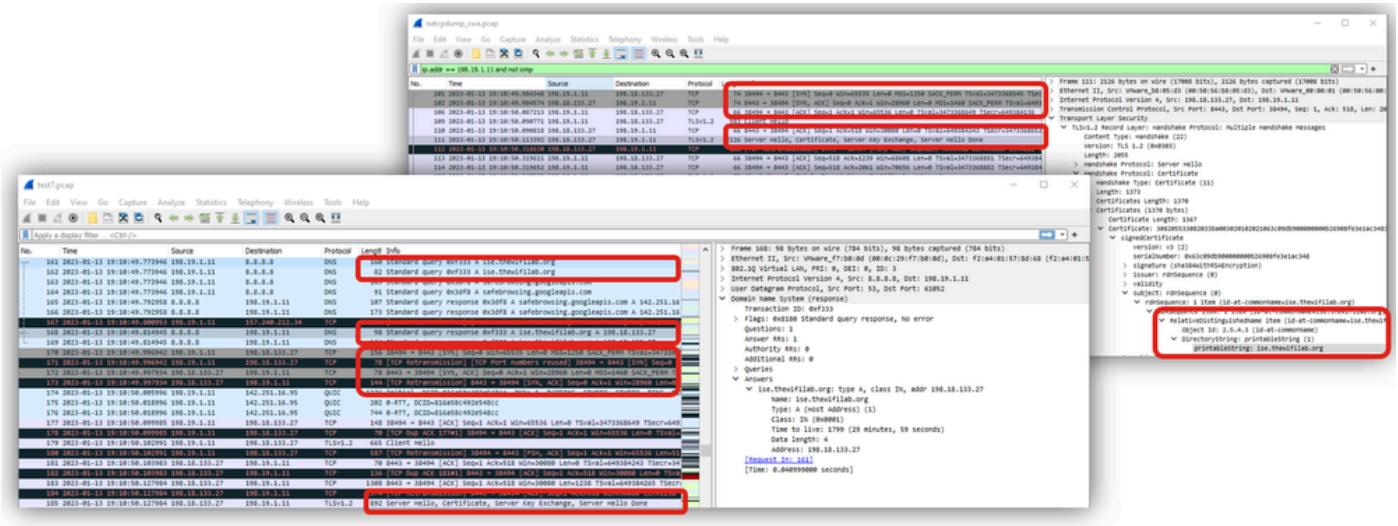
10 - A página de login ainda não é carregada?

Verifique com WLC EPC e ISE TCPdump se o tráfego do cliente alcança ISE PSN. Configure e inicie as capturas no WLC e no ISE:



WLC EPC e ISE TCPDump

Após a reprodução do problema, colete capturas e correlacione o tráfego. Aqui podemos ver o nome de host do ISE resolvido e depois a comunicação entre o cliente e o ISE na porta 8443:



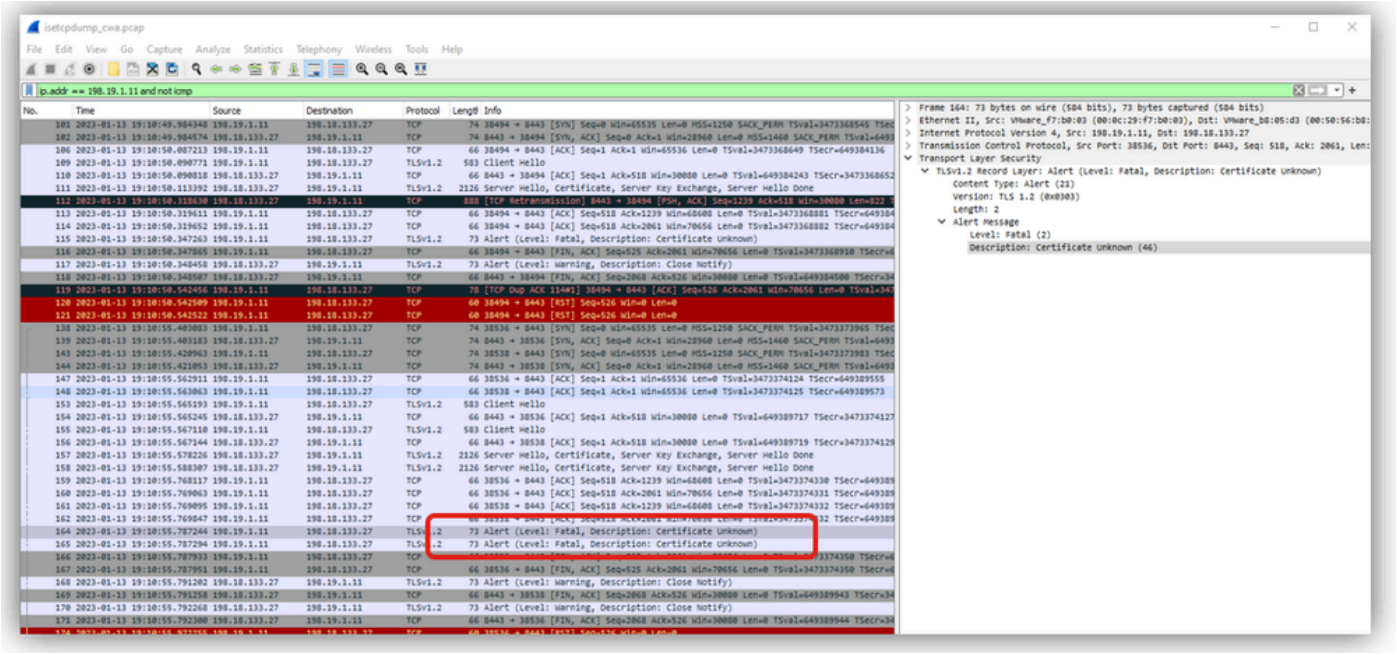
Tráfego WLC e ISE

11 - Por que temos uma violação de segurança devido ao certificado?

Se você usar o certificado autoassinado no ISE, espera-se que o cliente envie um aviso de segurança quando ele tentar apresentar a página de login do portal do ISE.

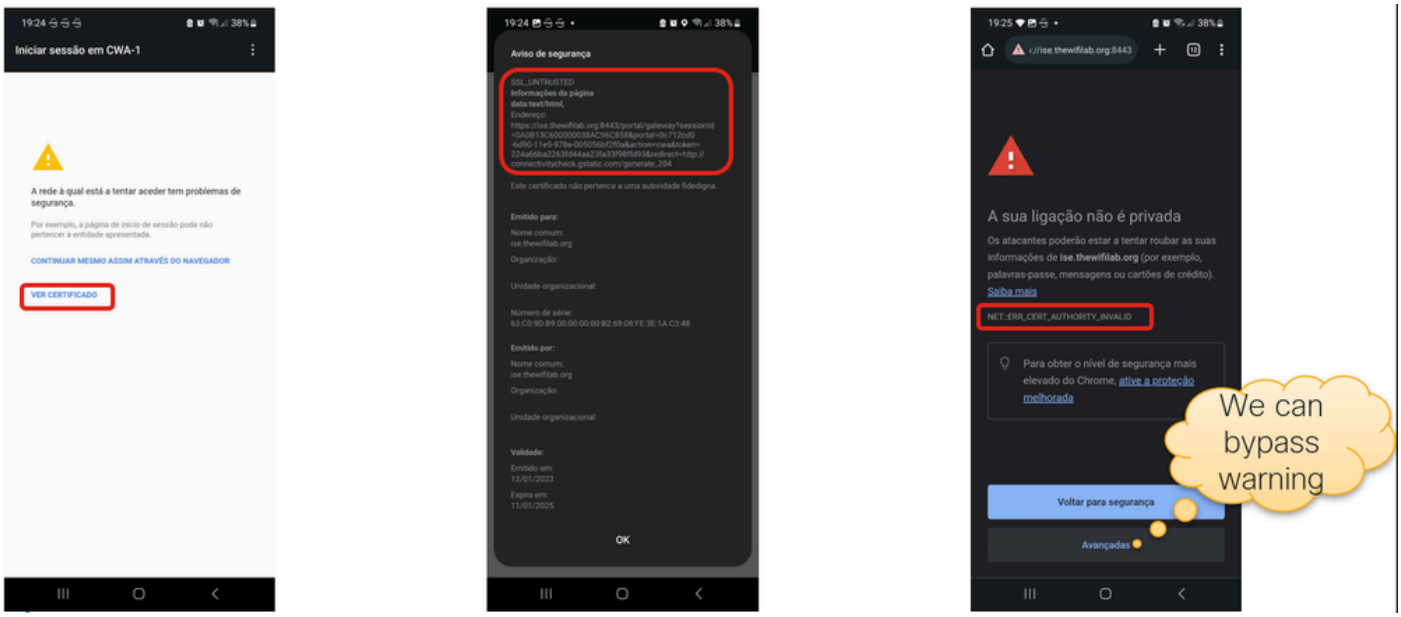
No despejo TCP do WLC EPC ou ISE, podemos verificar se o certificado ISE é confiável.

Neste exemplo, podemos ver conexão fechada de Cliente com Alerta (Nível: Fatal, Descrição: certificate Unknown), que significa que o certificado do ISE não é conhecido (Trusted):



Certificado não confiável do ISE

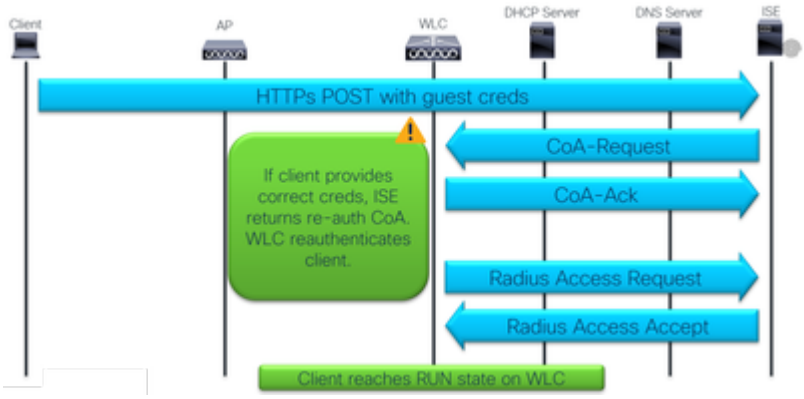
Se verificarmos o lado do cliente, veremos estes exemplos de saída:



Dispositivo cliente que não confia no certificado ISE

Finalmente, o redirecionamento está funcionando!! Mas o login falha...

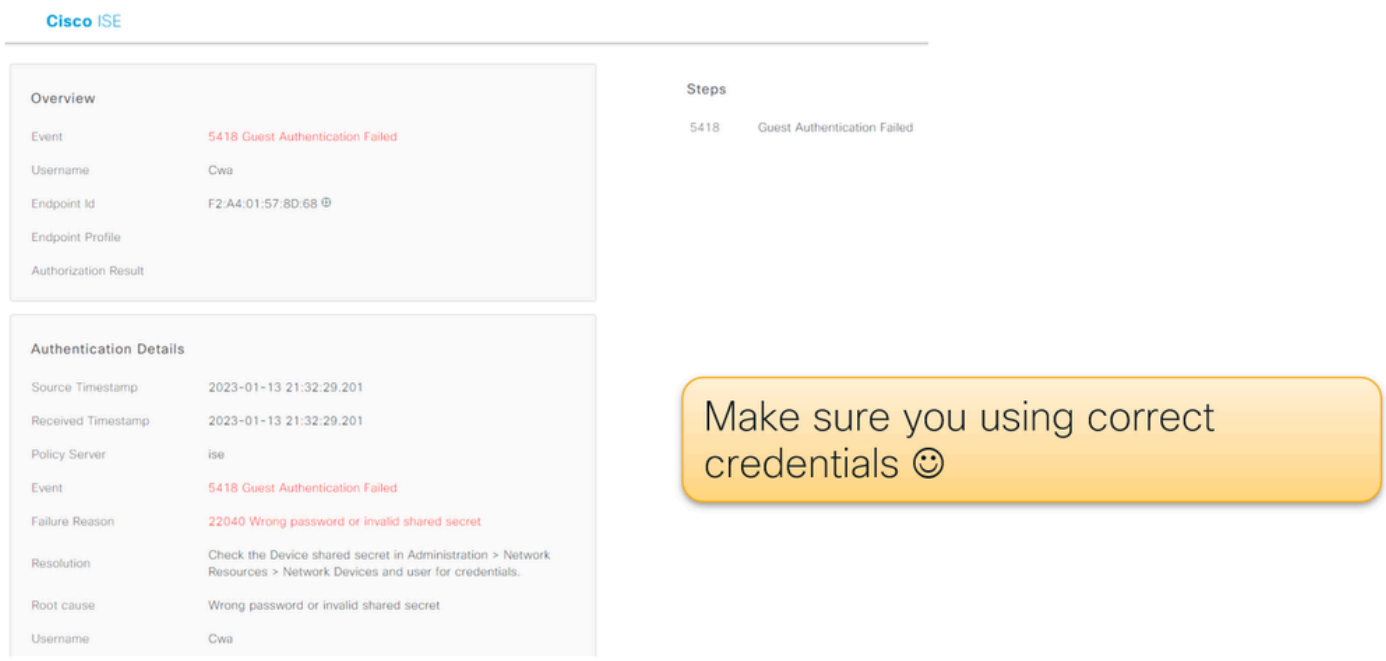
Última verificação do fluxo...



Login e CoA do cliente

12 - Falha de login de convidado?

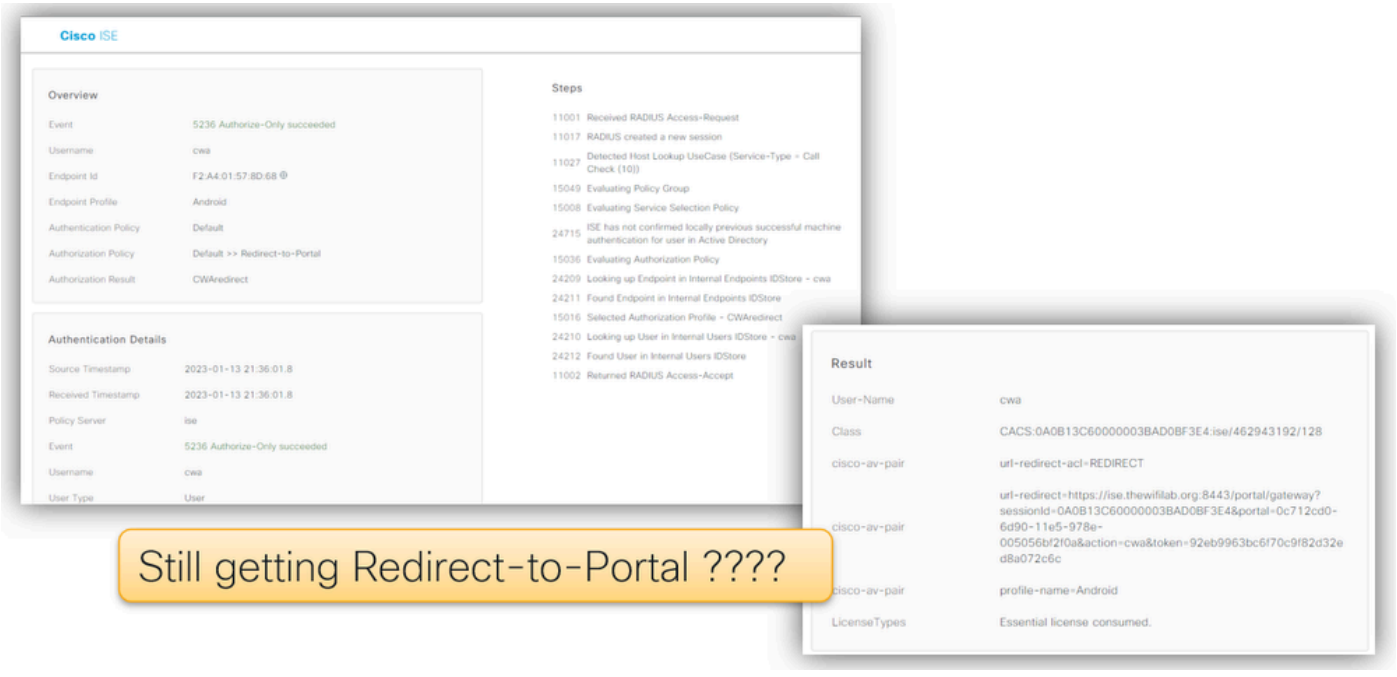
Verifique os logs do ISE quanto a falhas de autenticação. Verifique se as credenciais estão corretas.



Falha na autenticação do convidado devido a credenciais incorretas

13 - O login foi bem-sucedido, mas não foi movido para EXECUTAR?

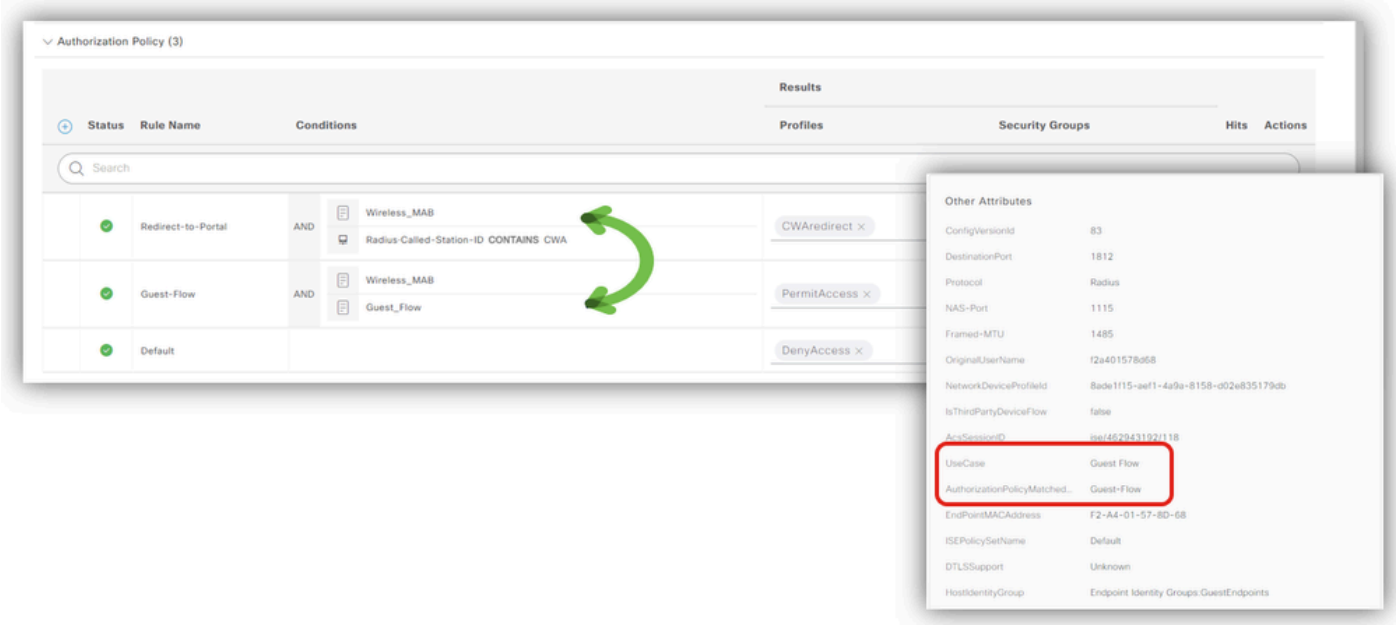
Verifique os logs do ISE para obter os detalhes e o resultado da autenticação:



Loop de redirecionamento

Neste exemplo, podemos ver o cliente obtendo novamente o perfil de autorização que contém a URL de redirecionamento e a ACL de redirecionamento. Isso resulta em um loop de redirecionamento.

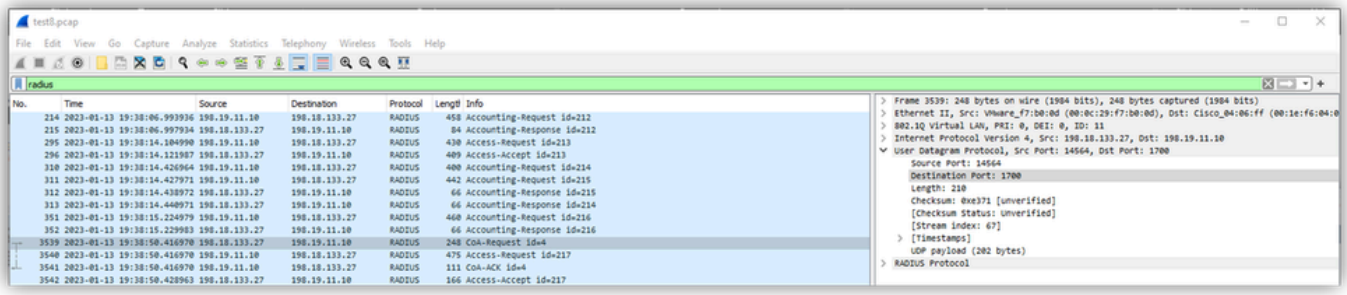
Verifique a Política definida. A verificação de regra Guest_Flow deve ser anterior ao Redirecionamento:



Regra Guest_Flow

14 - COA com falha?

Com o EPC e o ISE TCPDump, podemos verificar o tráfego de CoA. Verifique se a porta de CoA (1700) está aberta entre o WLC e o ISE. Verifique se o segredo compartilhado corresponde.



tráfego de CoA

Note: Na versão 17.4.X e posterior, certifique-se de configurar também a chave do servidor CoA ao configurar o servidor RADIUS. Use a mesma chave que o segredo compartilhado (eles são os mesmos por padrão no ISE). A finalidade é, opcionalmente, configurar uma chave para CoA diferente do segredo compartilhado, se for isso que o servidor RADIUS configurou. No Cisco IOS® XE 17.3, a interface do usuário da Web simplesmente usava o mesmo segredo compartilhado que a chave de CoA.

A partir da versão 17.6.1, o RADIUS (incluindo CoA) é suportado por meio dessa porta. Se quiser usar a Porta de serviço para RADIUS, você precisará desta configuração:

<#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
```

Conclusão

Esta é a lista de verificação do CWA retomada:

- Certifique-se de que o cliente esteja na VLAN correta e obtenha o endereço IP e DNS.

    - Obtenha detalhes do cliente na WLC e execute capturas de pacotes para ver a troca de DHCP.
- Verifique se o cliente pode resolver nomes de host via DNS.
    - Faça ping no nome do host a partir do cmd.
- A WLC deve estar escutando na porta 80
    - Verifique o comando global ip http server ou o comando global parameter map webauth-http-enable.
- Para se livrar do aviso de certificado, instale o certificado confiável no ISE.
    - Não é necessário instalar o certificado confiável na WLC no CWA.
- Política de autenticação na opção avançada do ISE "Continuar" Se o usuário não for encontrado
    - Para permitir que usuários convidados patrocinados se conectem e obtenham Redirecionamento de URL e ACL.

E as principais ferramentas usadas na solução de problemas:

- WLC EPC
    - Filtros internos: Protocolo DHCP, endereço MAC.
- Monitor WLC
    - Verifique os detalhes de segurança do cliente.
- Rastreamento de RA de WLC
    - Depurações com informações detalhadas no lado da WLC.
- Registros ativos do ISE
    - Detalhes da autenticação.
- TCPDump do ISE
    - Coletar capturas de pacotes na interface PSN do ISE.

Referências

Configurar a autenticação da Web central (CWA) no Catalyst 9800 WLC e ISE

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.