WLC(Wireless Lan Controller) 9800 및 ISE(Identity Services Engine)로 CWA(Central Web Authentication) 문제 해결

목차

소개

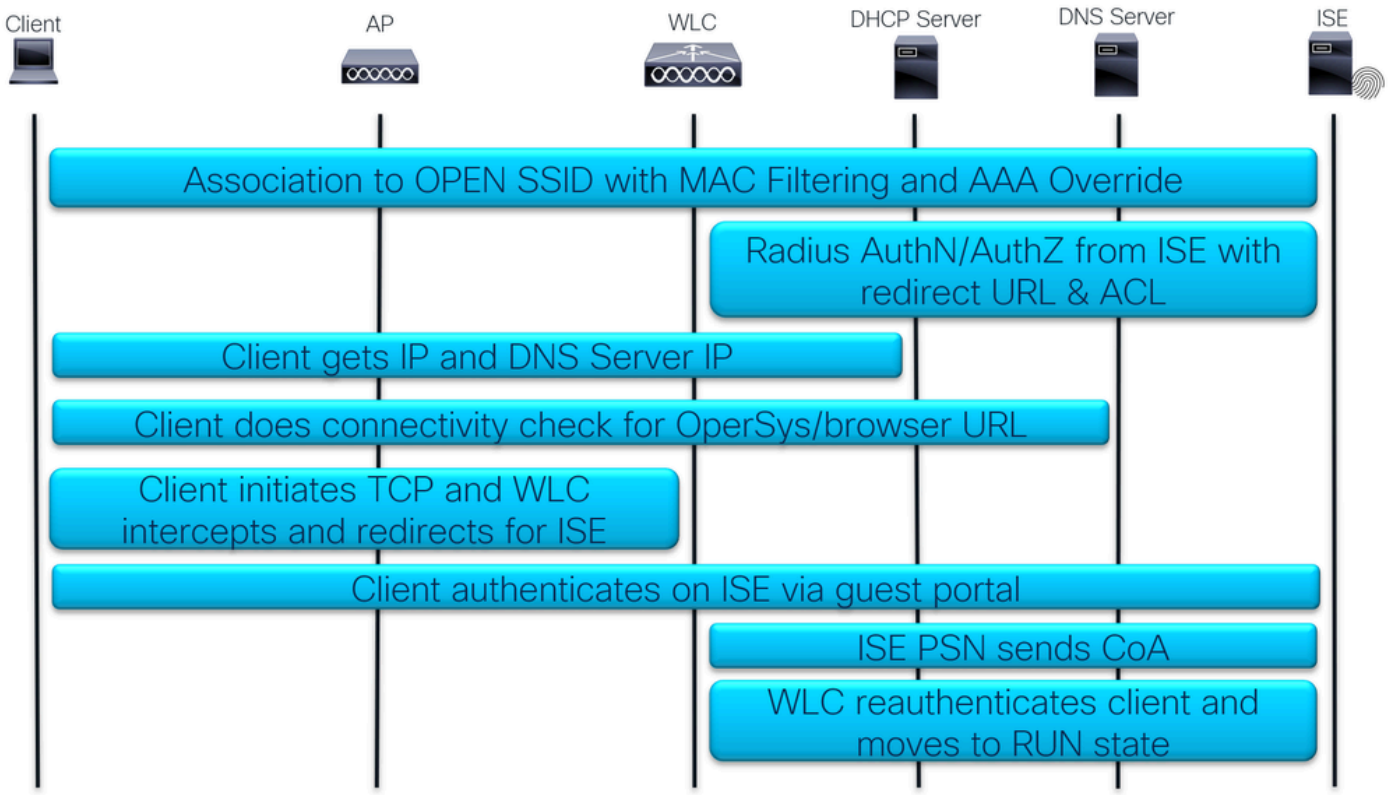
이 문서에서는 WLC 9800 및 ISE에서 CWA(Central Web Authentication)의 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

현재 개인 장치가 너무 많아 무선 액세스 보안을 찾는 네트워크 관리자는 일반적으로 CWA를 사용하는 무선 네트워크를 선택합니다.
이 문서에서는 CWA의 흐름도를 중점적으로 살펴봅니다. 이는 Cisco에 영향을 미치는 일반적인 문제의 트러블슈팅에 도움이 됩니다.
이 프로세스의 일반적인 방법, CWA와 관련된 로그를 수집하는 방법, 이러한 로그를 분석하는 방법, 트래픽 흐름을 확인하기 위해 WLC에 포함된 패킷 캡처를 수집하는 방법을 살펴봅니다.

CWA는 사용자가 개인 장치(BYOD라고도 함)를 사용하여 회사 네트워크에 연결할 수 있도록 하는 회사의 가장 일반적인 설정입니다.
모든 네트워크 관리자가 TAC 케이스를 열기 전에 문제를 해결하기 위해 수행할 수 있는 해결 방법 및 문제 해결 단계에 관심이 있습니다.

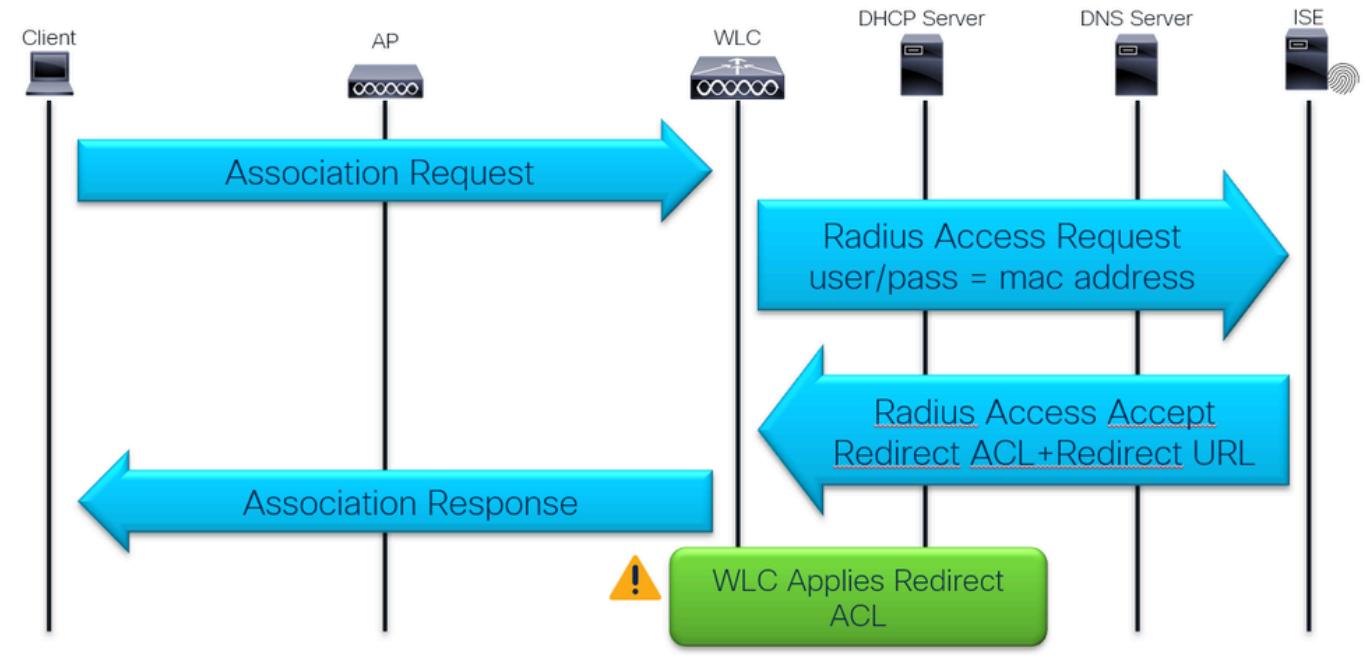
다음은 CWA 패킷 흐름입니다.



CWA 패킷 흐름

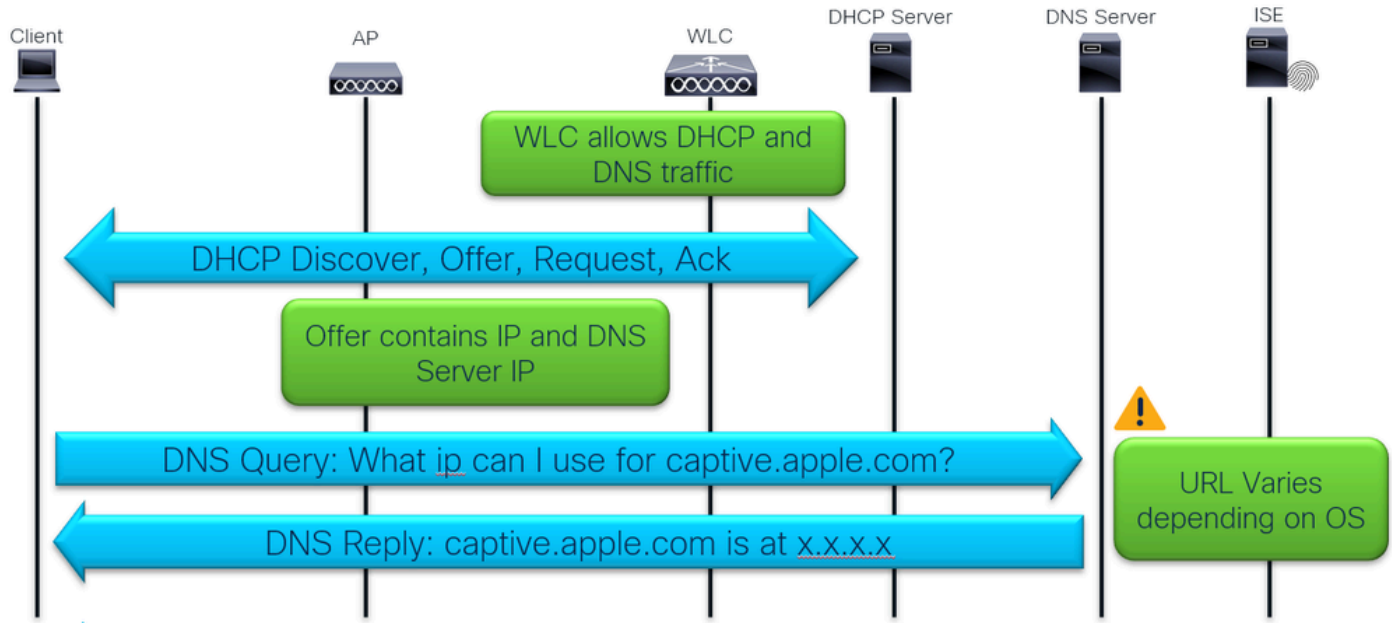
세부 흐름

첫 번째 연결 및 RADIUS 인증:



첫 번째 연결 및 RADIUS 인증

DHCP, DNS 및 연결 확인:



DHCP, DNS 및 연결 확인

연결 확인은 클라이언트 디바이스 운영 체제 또는 브라우저에서 종속 포털 탐지를 사용하여 수행됩니다.

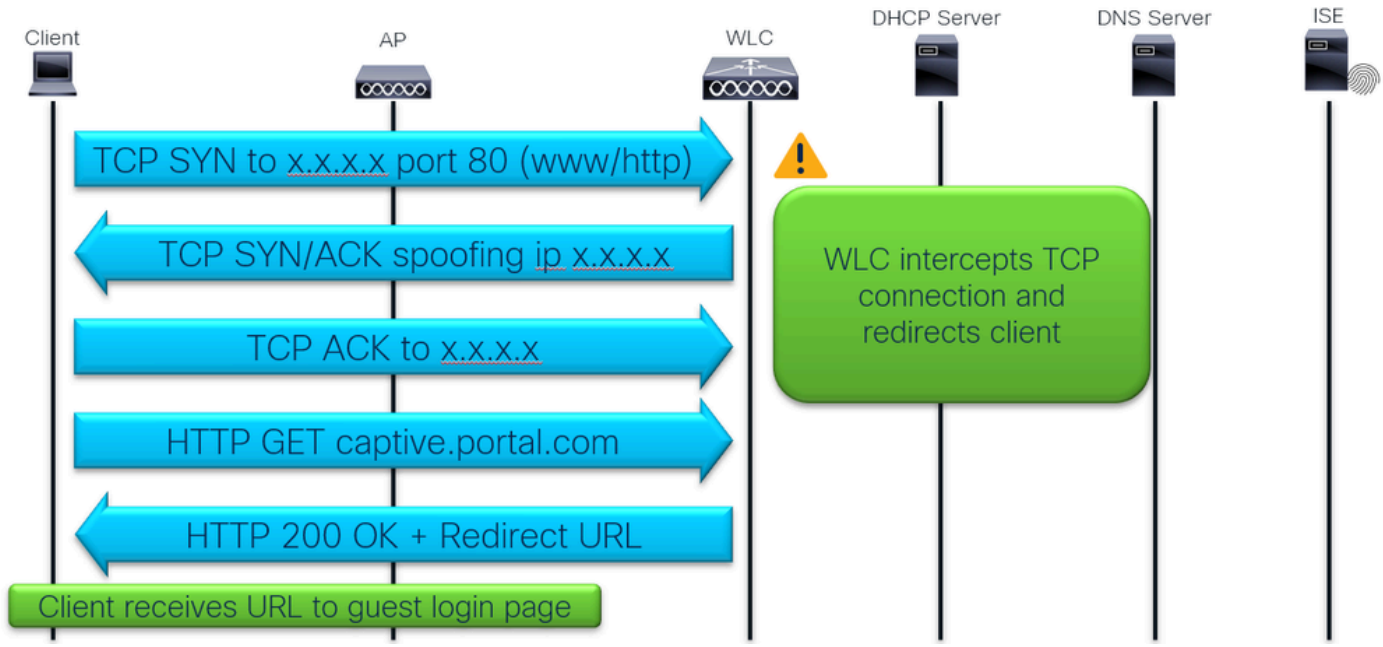
특정 도메인에 대해 HTTP GET을 수행하도록 사전 프로그래밍된 디바이스 OS가 있습니다

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

또한 브라우저를 열 때 이 검사를 수행합니다.

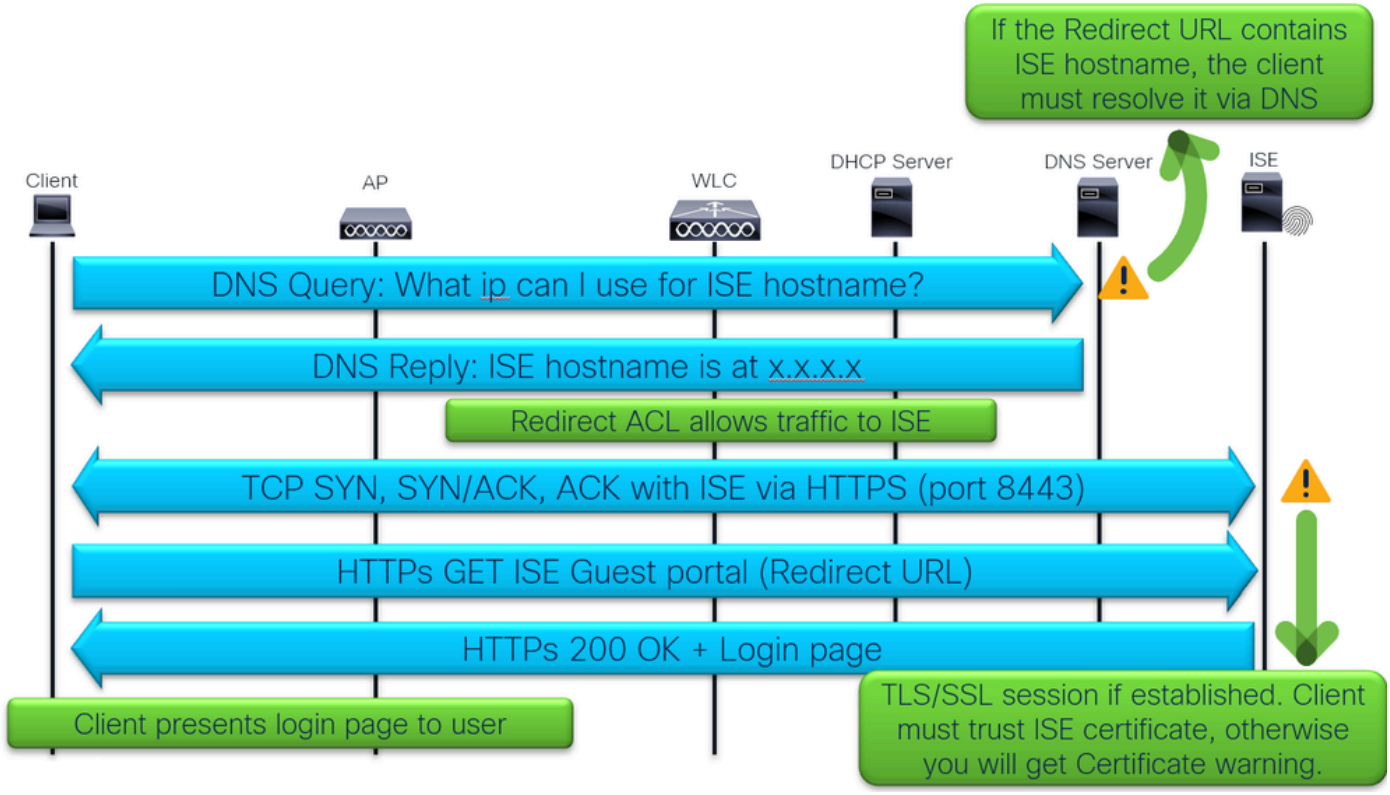
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

트래픽 차단 및 리디렉션:



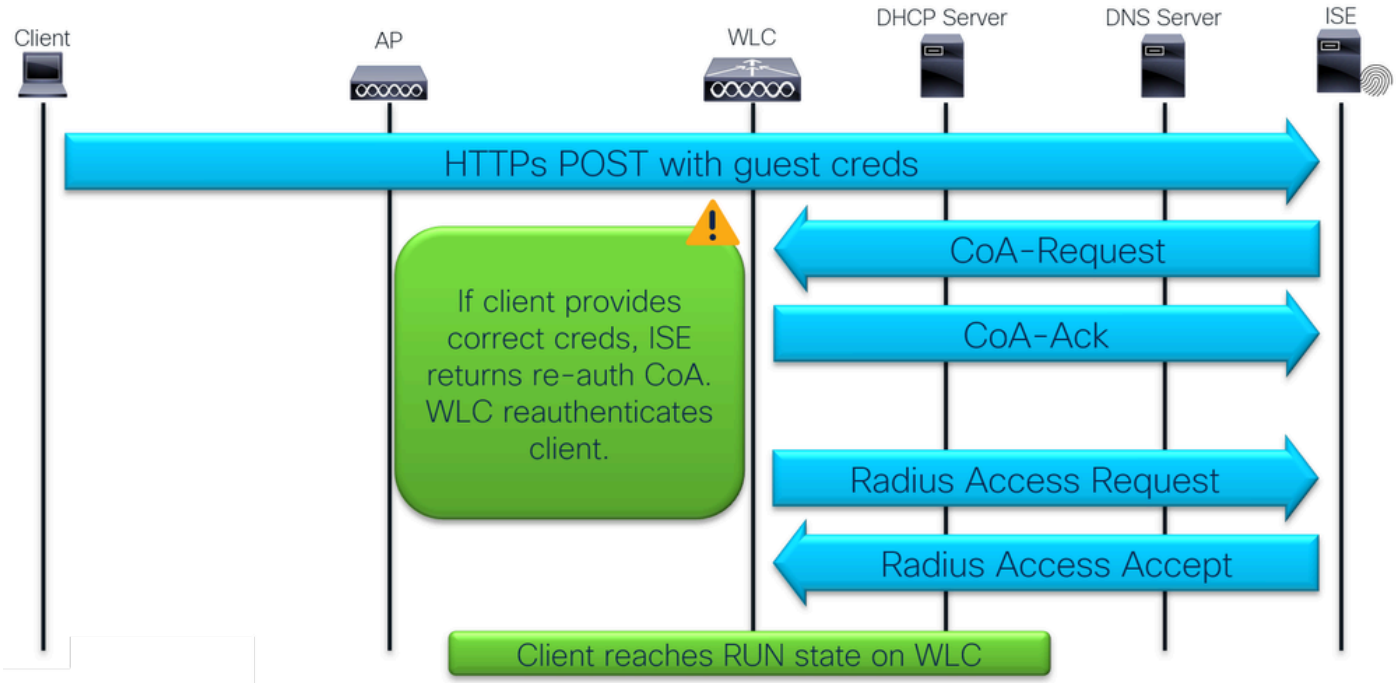
트래픽 차단 및 리디렉션

ISE 게스트 로그인 포털에 클라이언트 로그인:



ISE 게스트 로그인 포털에 클라이언트 로그인

클라이언트 로그인 및 CoA:

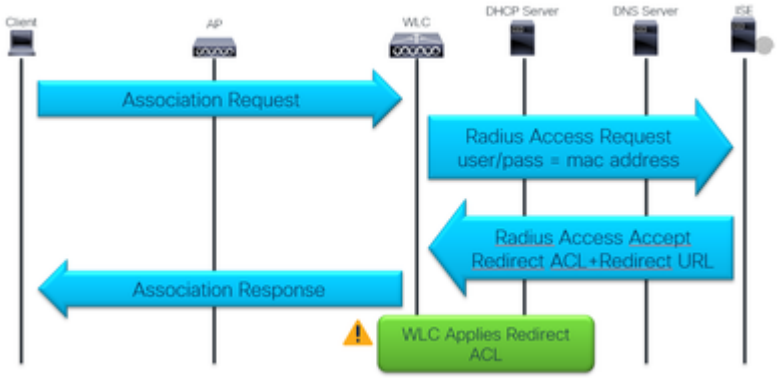


클라이언트 로그인 및 CoA

문제 해결

일반적인 증상: 사용자가 로그인 페이지로 리디렉션되지 않습니다.

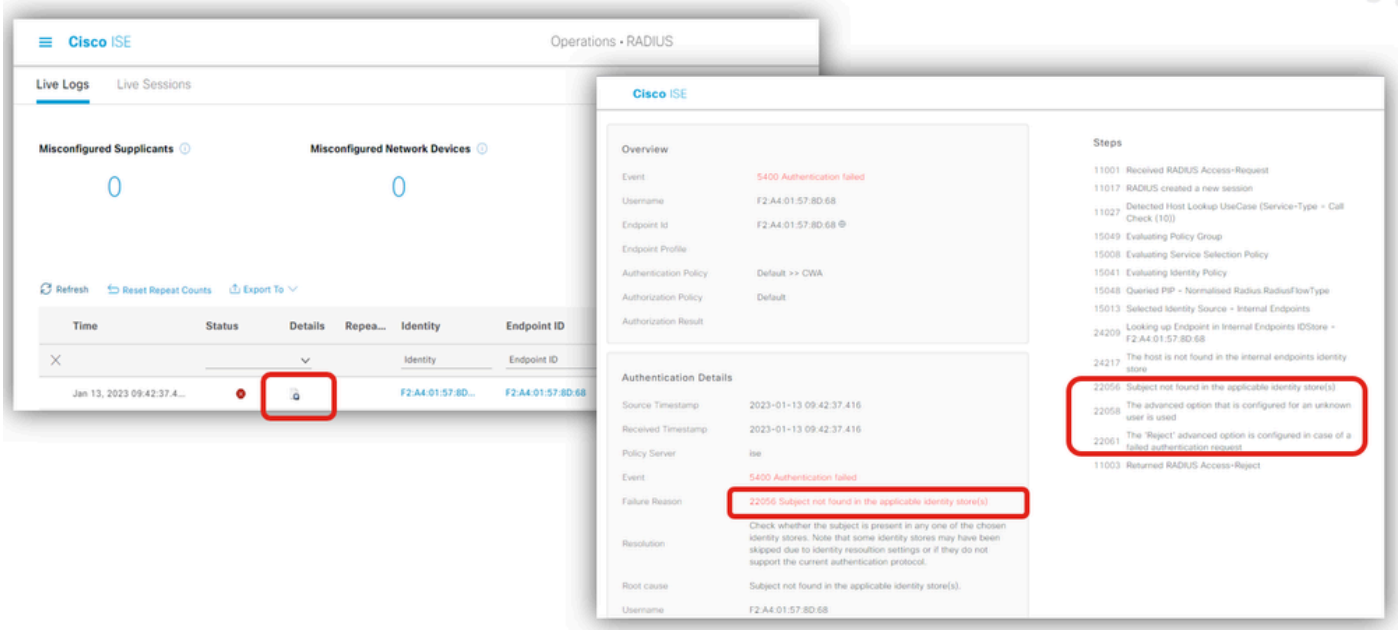
흐름의 첫 부분부터 살펴보겠습니다.



첫 번째 연결 및 RADIUS 인증

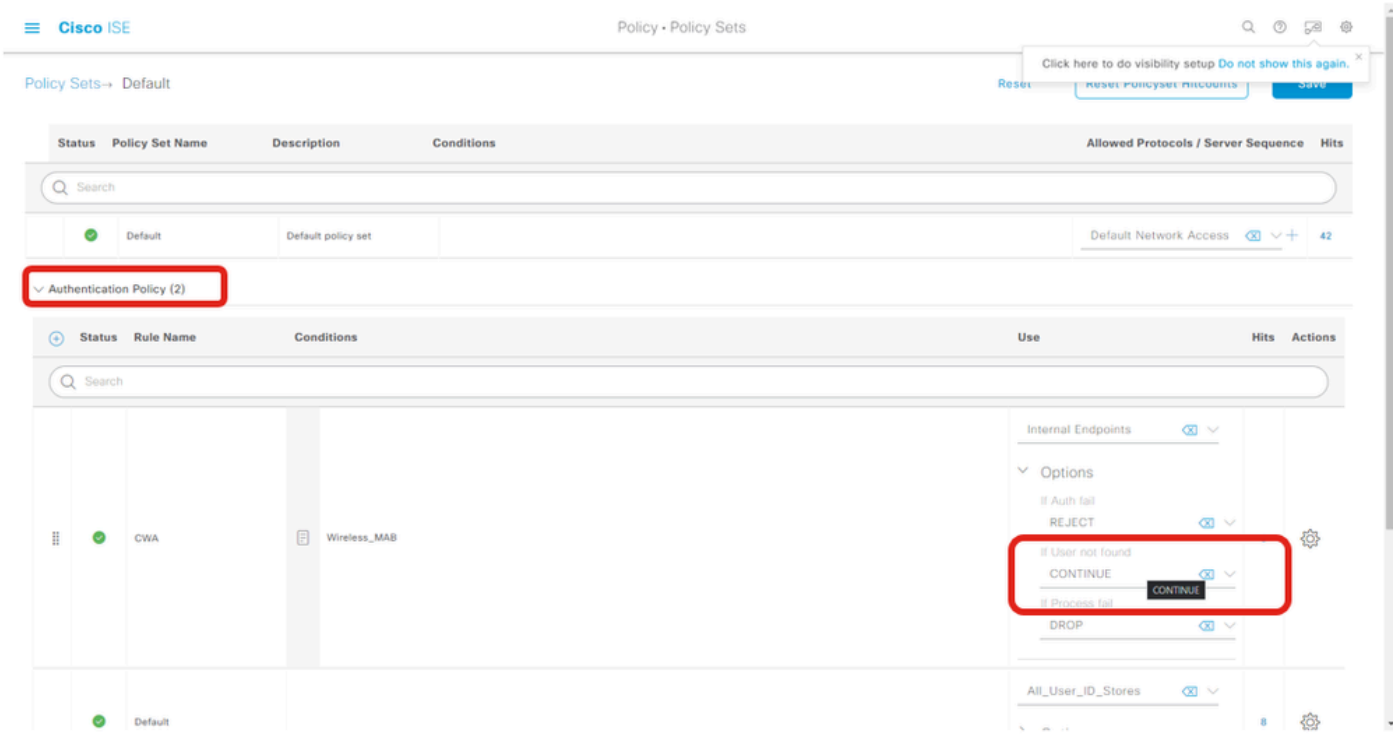
1 - 첫 번째 RADIUS 인증에 성공했습니까?

MAC 필터링 인증 결과 확인:



ISE 라이브 로그 - mac 필터링 인증 결과 표시

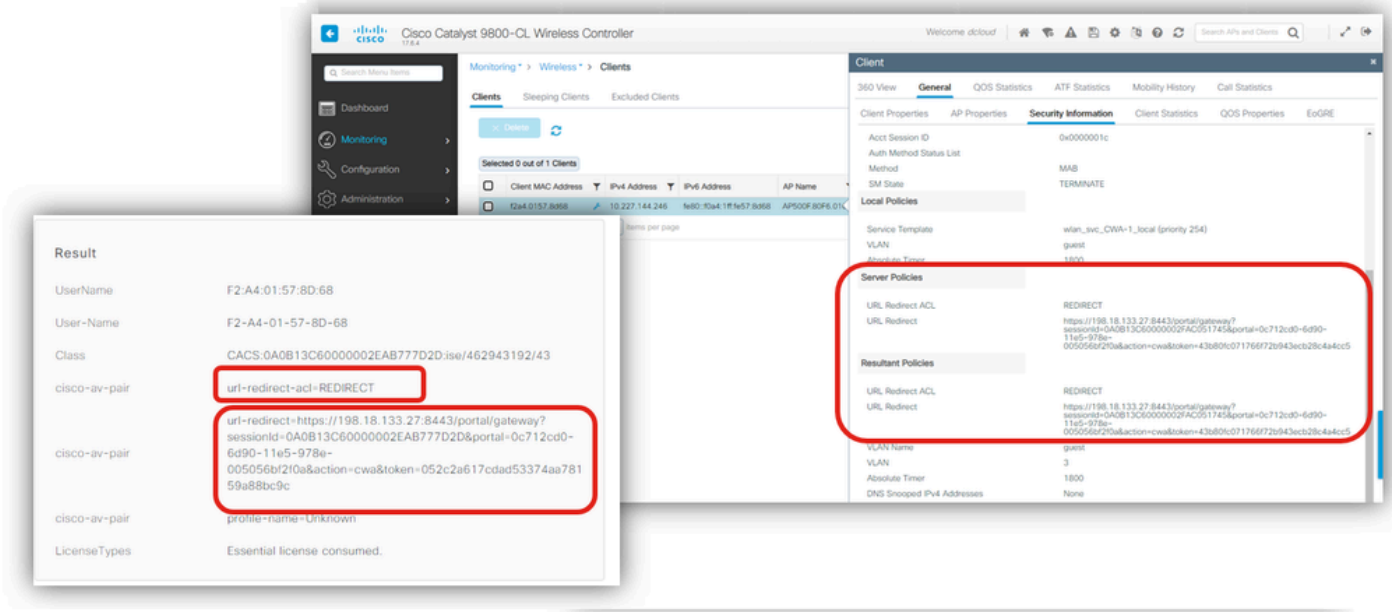
사용자를 찾을 수 없는 경우 인증에 대한 고급 옵션이 "Continue(계속)"로 설정되어 있는지 확인합니다.



사용자가 고급 옵션을 찾을 수 없음

2 - WLC가 리디렉션 URL 및 ACL을 수신합니까?

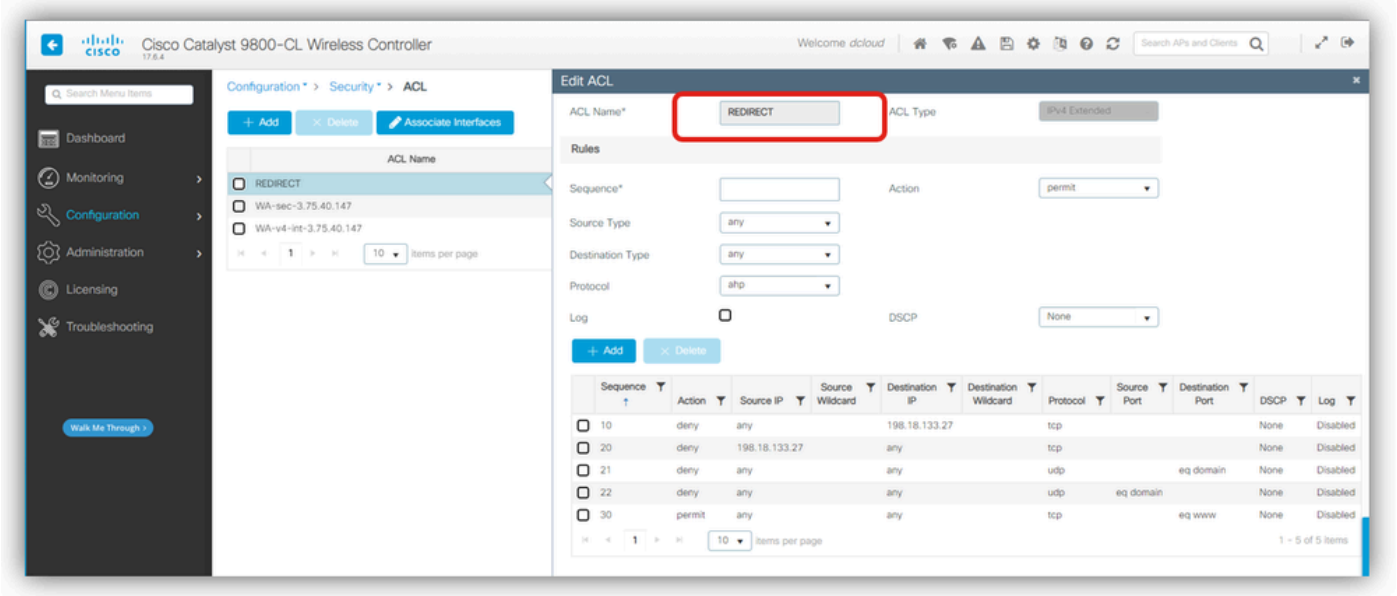
Monitoring(모니터링) 아래에서 ISE 라이브 로그 및 WLC 클라이언트 보안 정보를 확인합니다. ISE가 Access Accept(액세스 수락)에서 리디렉션 URL 및 ACL을 전송하고 WLC에서 이를 수신하여 클라이언트 세부사항의 클라이언트에 적용되는지 확인합니다.



ACL 및 URL 리디렉션

3 - 리디렉션 ACL이 정확합니까?

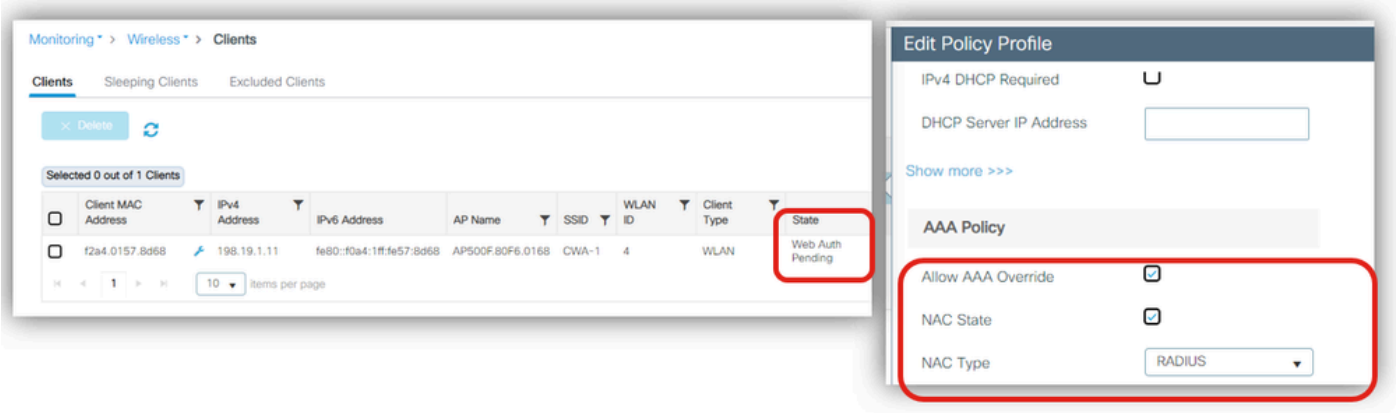
ACL 이름에서 오타를 확인합니다. ISE에서 전송하는 것과 동일한지 확인합니다.



리디렉션 ACL 확인

4 - 클라이언트가 웹 인증 보류 중으로 이동되었습니까?

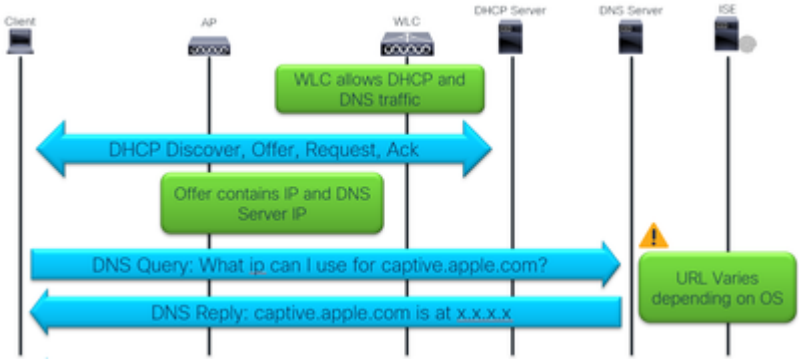
"웹 인증 보류 중" 상태에 대한 클라이언트 세부 정보를 확인하십시오. 이 상태가 아닌 경우 AAA 재정의 및 Radius NAC가 정책 프로파일에서 활성화되었는지 확인합니다.



클라이언트 세부사항, aaa 재정의 및 RADIUS NAC

아직도 안 먹혀?

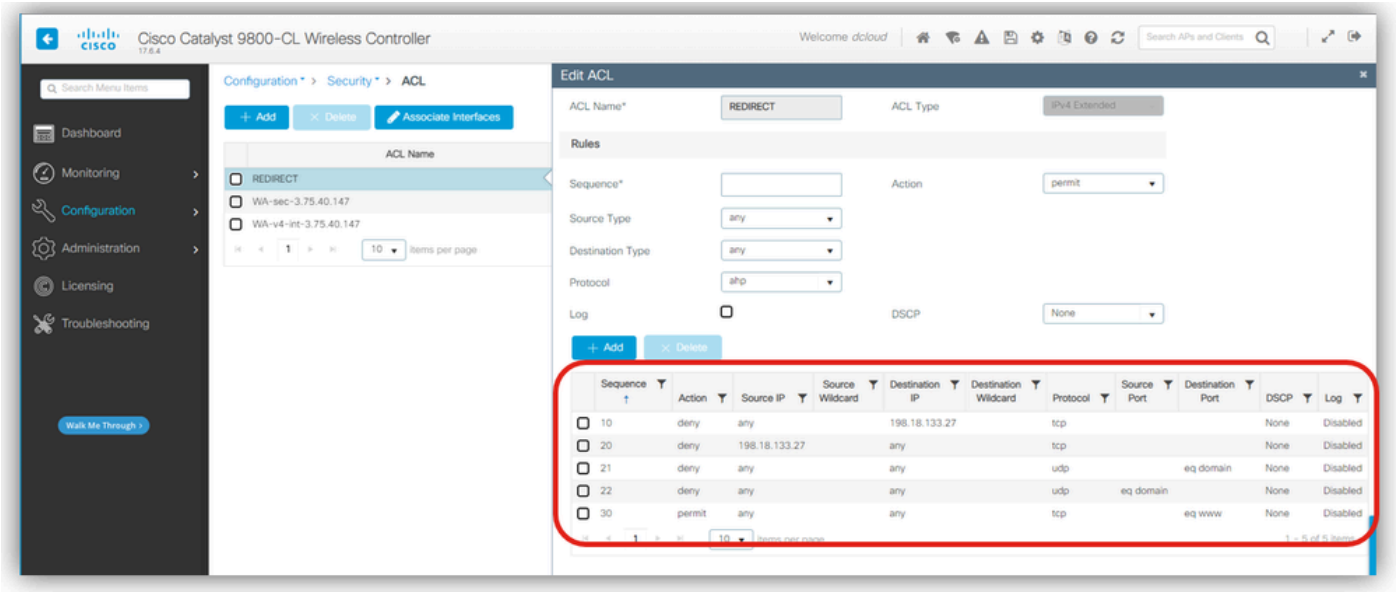
흐름을 다시 살펴보겠습니다.



DHCP, DNS 및 연결 확인

5 - WLC에서 DHCP 및 DNS 트래픽을 허용합니까?

WLC에서 리디렉션 ACL 내용을 확인합니다.



WLC에서 ACL 내용 리디렉션

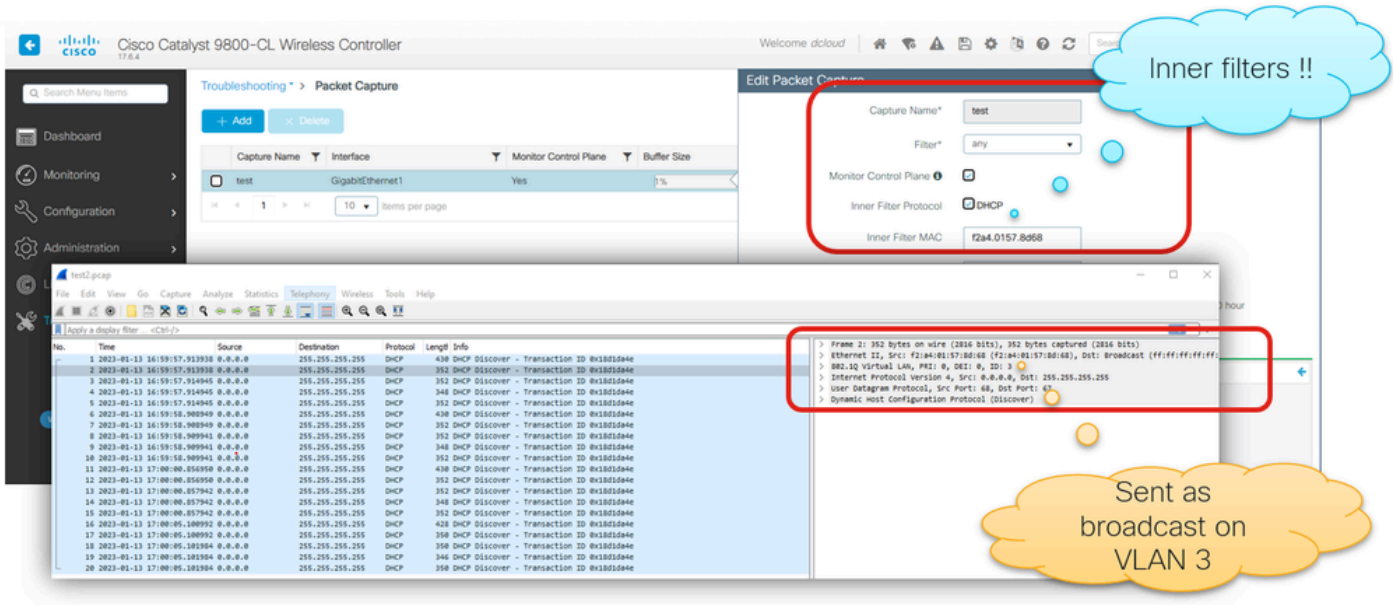
리디렉션 ACL은 permit 문에서 가로채고 리디렉션하는 트래픽과 deny 문을 사용하여 가로채고 리디렉션하는 트래픽에 대해 정의합니다.

이 예에서는 ISE IP 주소로 들어오고 나가는 DNS 및 트래픽이 흐르도록 허용하고 포트 80(www)에서 모든 tcp 트래픽을 가로챕니다.

6 - DHCP 서버가 DHCP Discover/Request를 수신합니까?

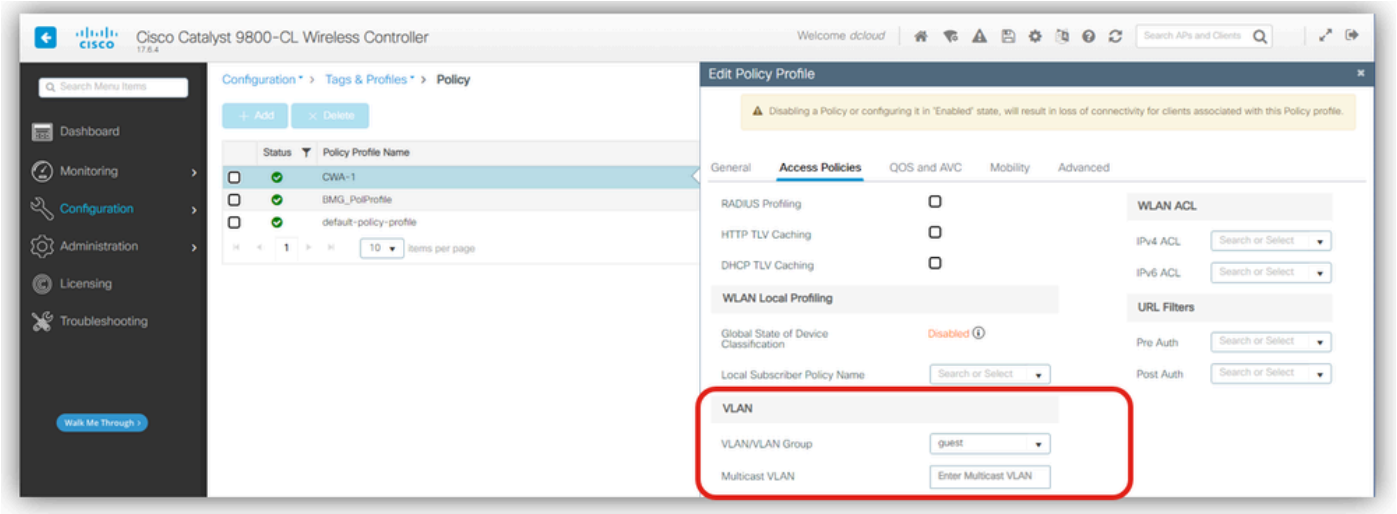
DHCP 교환이 발생하면 EPC에 문의하십시오. EPC는 DHCP 프로토콜 및/또는 Inner Filter MAC와 같은 Inner Filters와 함께 사용할 수 있습니다. 여기서 클라이언트 디바이스 MAC 주소를 사용할 수 있으며, 클라이언트 디바이스 MAC 주소에 의해 전송되거나 클라이언트 디바이스 MAC 주소로 전송된 DHCP 패킷만 EPC에 수신합니다.

이 예에서는 VLAN 3에서 브로드캐스트로 전송된 DHCP Discover 패킷을 확인할 수 있습니다.



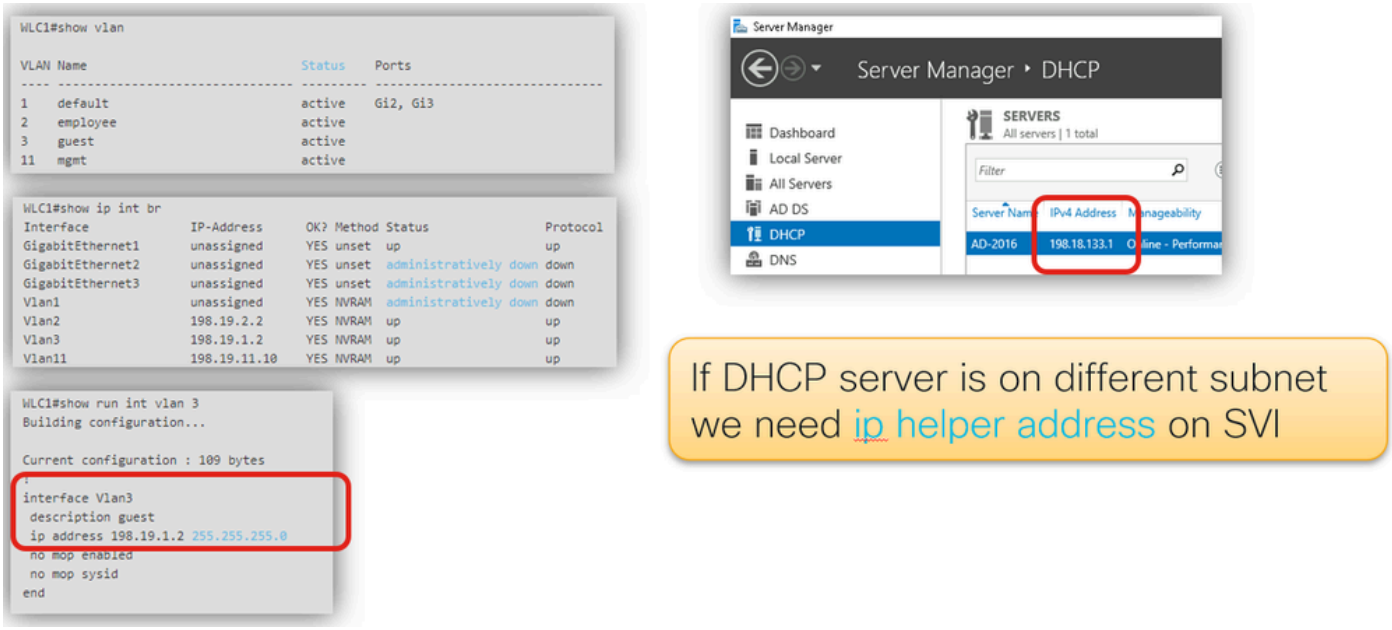
DHCP를 확인하는 WLC EPC

정책 프로필에서 필요한 클라이언트 VLAN을 확인합니다.



정책 프로필의 VLAN

WLC VLAN 및 switchport 트렁크 컨피그레이션과 DHCP 서브넷을 확인합니다.



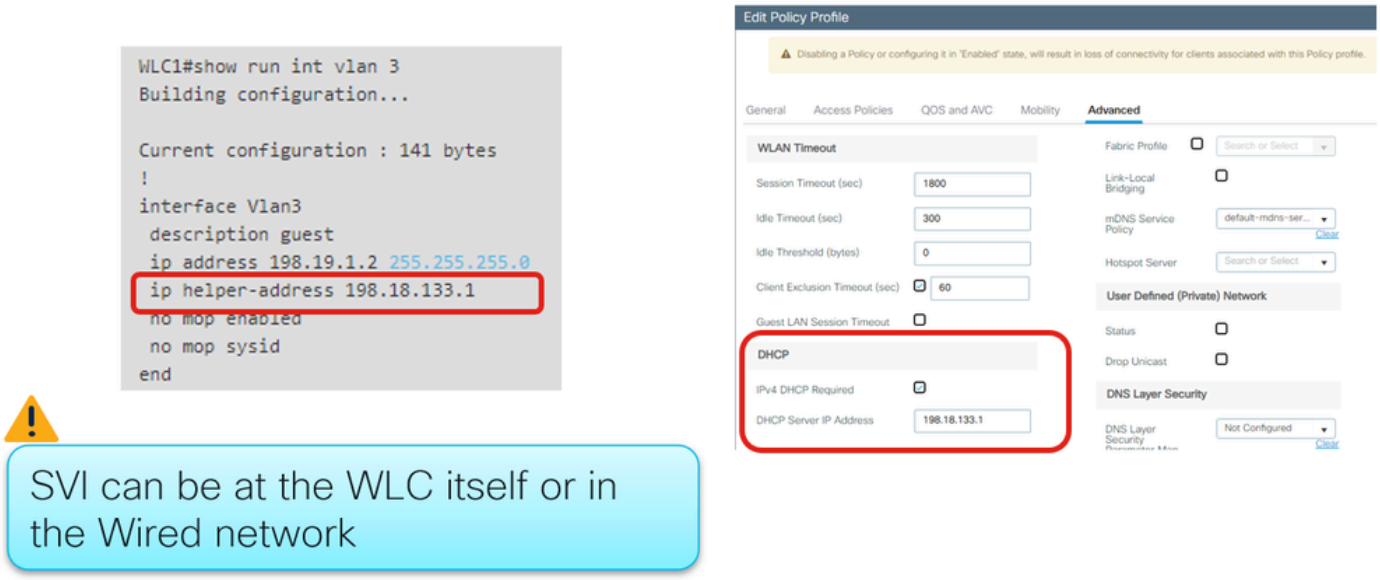
VLAN, 스위치포트 및 DHCP 서브넷

VLAN 3이 WLC에 있으며 VLAN 3에 대한 SVI도 있지만 DHCP 서버 IP 주소를 확인할 때는 다른 서브넷에 있으므로 SVI에 ip helper 주소가 필요합니다.

모범 사례에서는 클라이언트 서브넷에 대한 SVI를 유선 인프라에 구성하고 WLC에서 이를 방지해야 합니다.

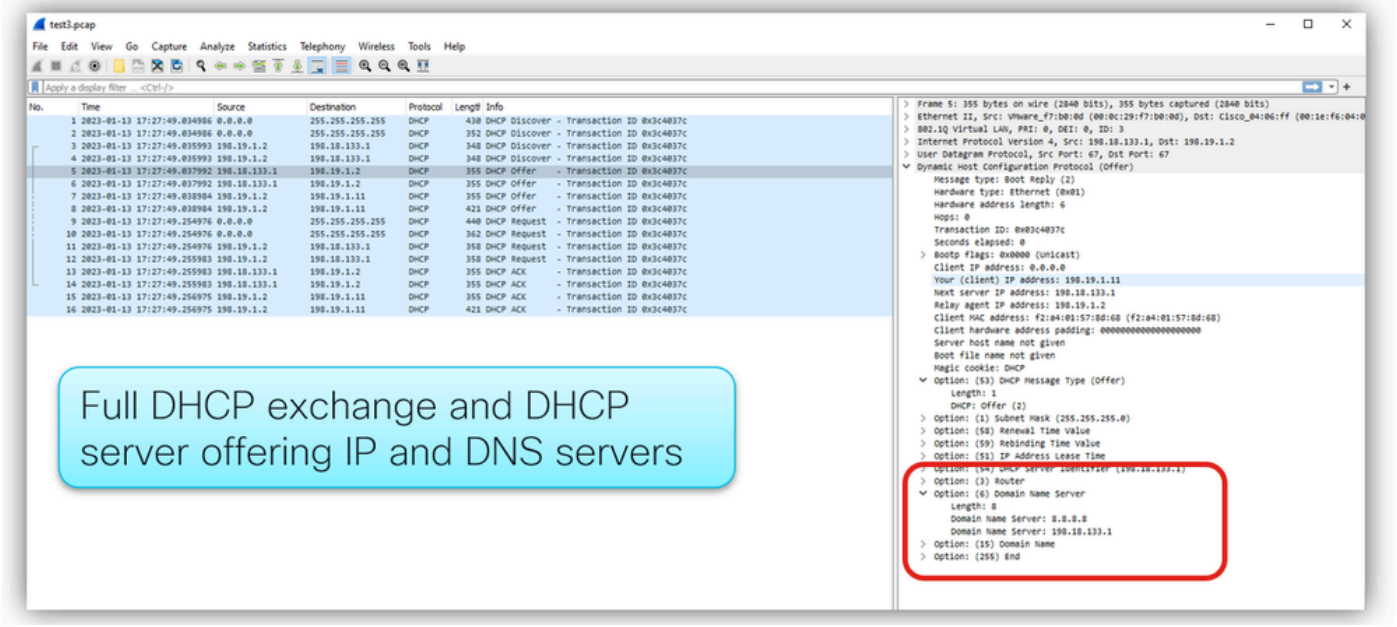
어떤 경우에도 상주하는 위치에 관계없이 ip helper-address 명령을 SVI에 추가해야 합니다.

또는 정책 프로필에서 DHCP 서버 ip 주소를 구성하는 방법이 있습니다.



SVI 또는 정책 프로필의 IP 헬퍼 주소

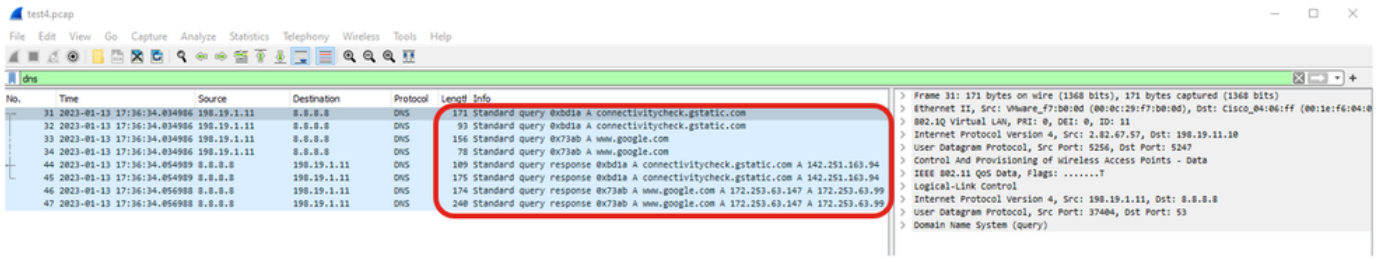
그러면 DHCP exchange가 정상이고 DHCP 서버가 DNS 서버 IP를 제공하는지 EPC로 확인할 수 있습니다.



DNS 서버 IP의 DHCP 제공 세부 정보

7 - 자동 리디렉션이 수행됩니까?

DNS 서버가 쿼리에 응답하는지 WLC EPC로 확인합니다.

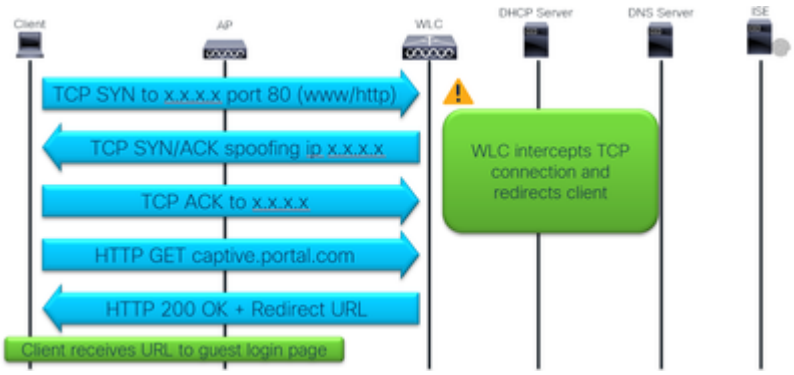


DNS 쿼리 및 응답

- 리디렉션이 자동이 아니면 브라우저를 열고 임의의 IP 주소를 시도합니다. 예: 10.0.0.1.
- 리디렉션이 작동하면 DNS 확인 문제가 발생할 수 있습니다.

아직도 안 먹혀?

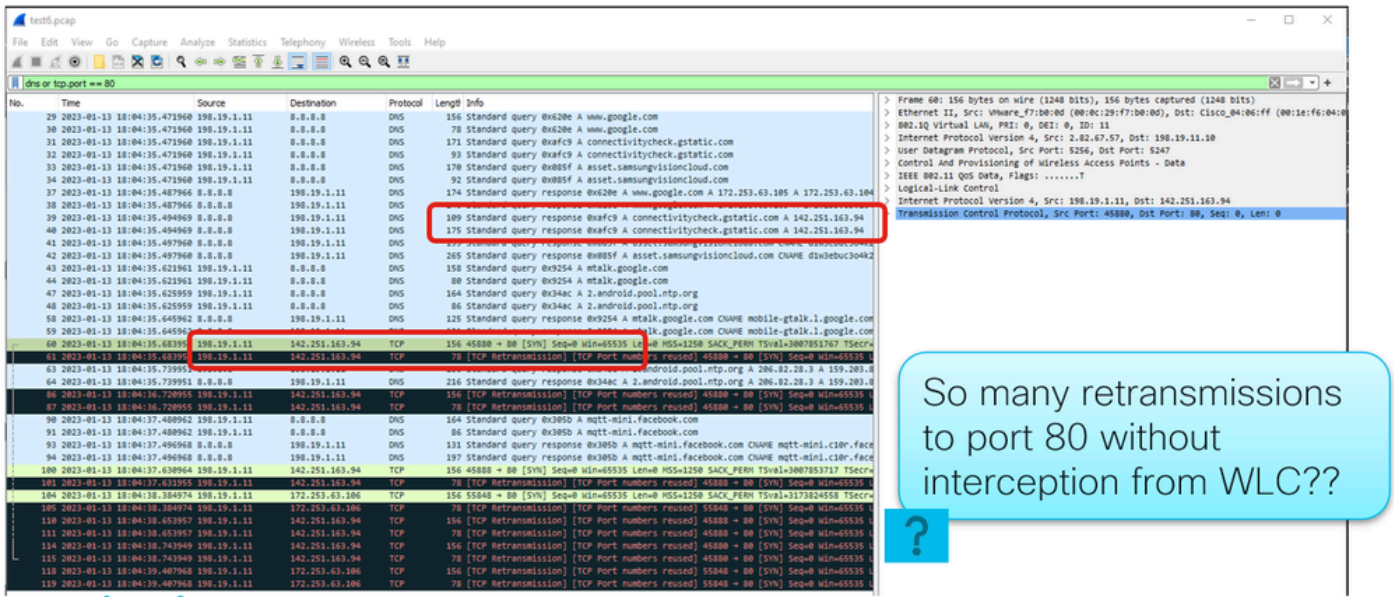
흐름을 다시 살펴보겠습니다.



트래픽 차단 및 리디렉션

8 - 브라우저에 로그인 페이지가 표시되지 않습니까?

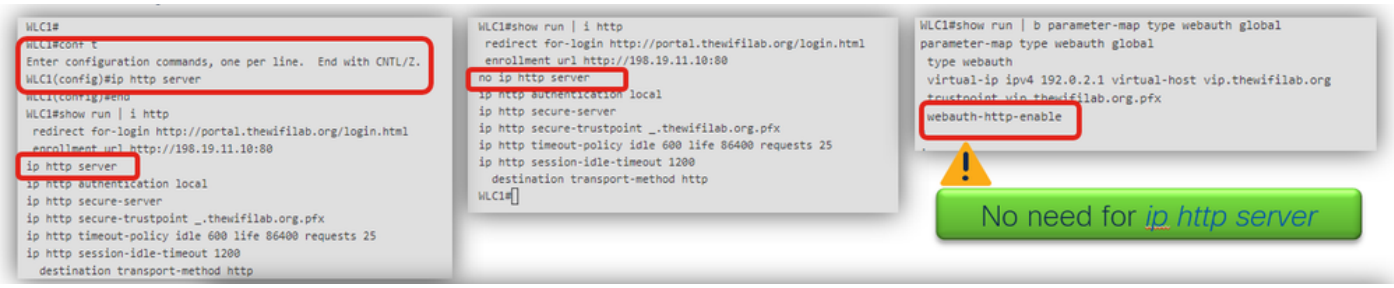
클라이언트가 TCP SYN을 포트 80으로 전송하고 WLC가 이를 가로채는지 확인합니다.



포트 80으로 TCP 재전송

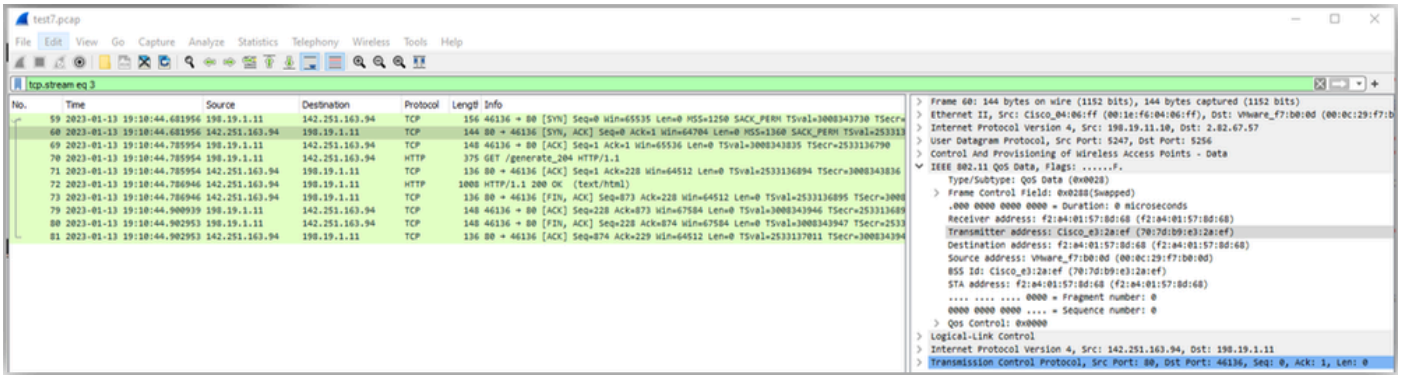
여기에서 클라이언트가 포트 80으로 TCP SYN 패킷을 전송하지만 응답을 받지 않고 TCP 재전송을 수행하는 것을 확인할 수 있습니다.

전역 컨피그레이션에서 ip http server 명령을 사용하거나 parameter-map 전역에서 webauth-http-enable 명령을 사용해야 합니다.



http 가로채기 명령

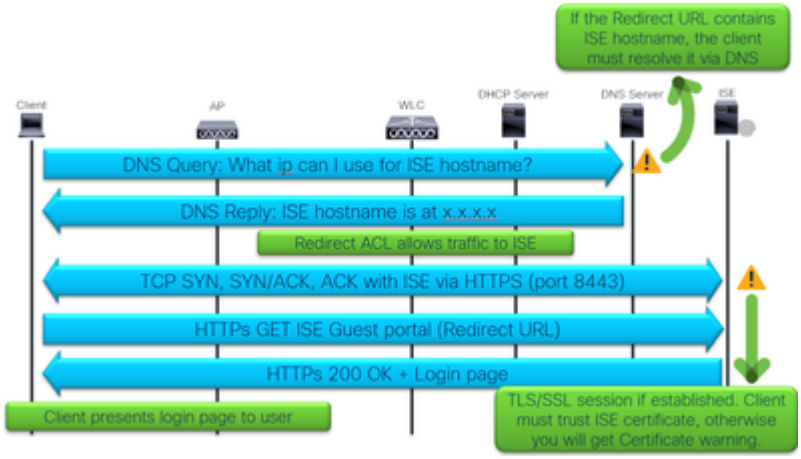
명령 후 WLC는 TCP를 가로채고 대상 IP 주소를 스푸핑하여 클라이언트에 응답하고 리디렉션합니다.



WLC에 의한 TCP 차단

아직도 안 먹혀?

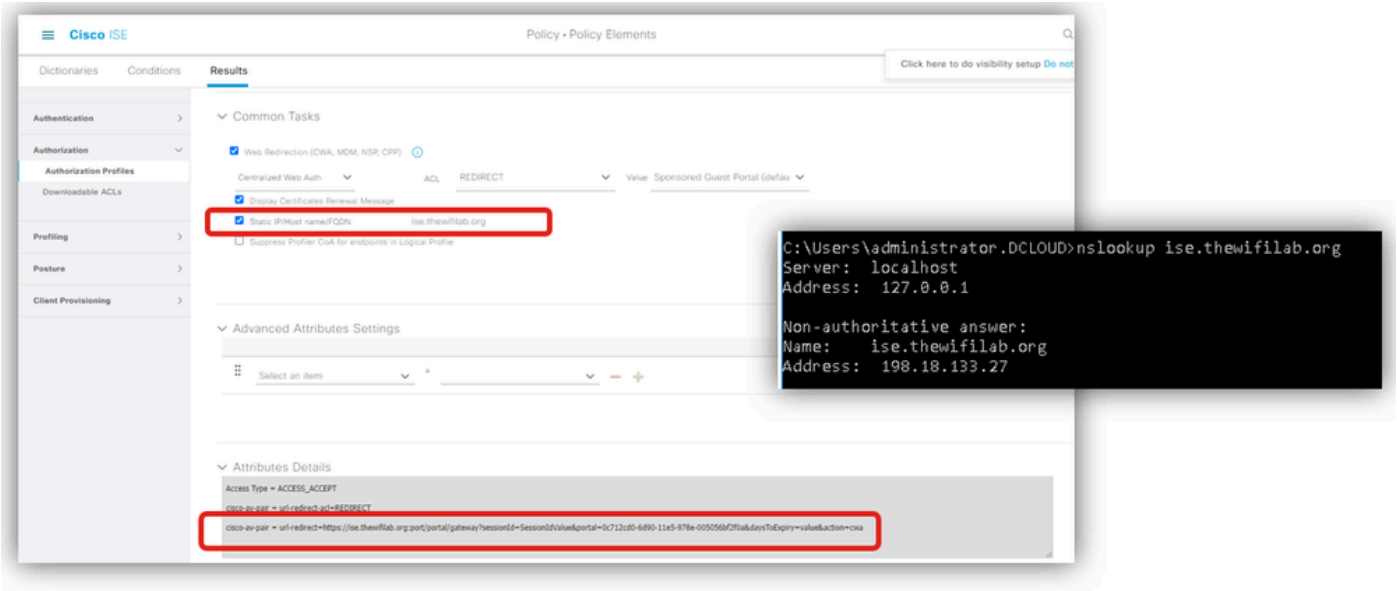
그 흐름에는 더 많은 것이 있습니다.



ISE 게스트 로그인 포털에 클라이언트 로그인

9 - 클라이언트가 ISE 호스트 이름을 확인할 수 있습니까?

리디렉션 URL이 IP 또는 호스트 이름을 사용하는지, 클라이언트가 ISE 호스트 이름을 확인하는지 확인합니다.



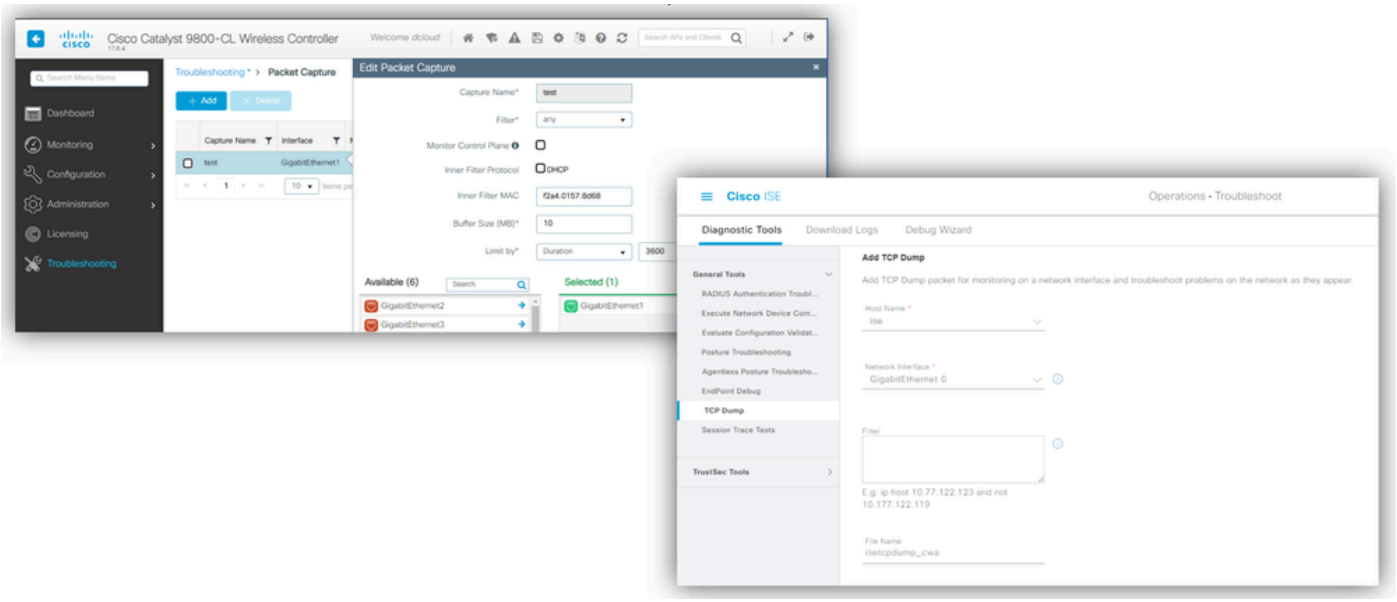
ISE 호스트 이름 확인

리디렉션 URL에 ISE 호스트 이름이 포함되어 있지만 클라이언트 디바이스에서 해당 호스트 이름을 ISE IP 주소로 확인할 수 없는 경우 일반적인 문제가 발생합니다. 호스트 이름을 사용하는 경우 DNS를 통해 확인할 수 있는지 확인합니다.

10 - 로그인 페이지가 여전히 로드되지 않습니까?

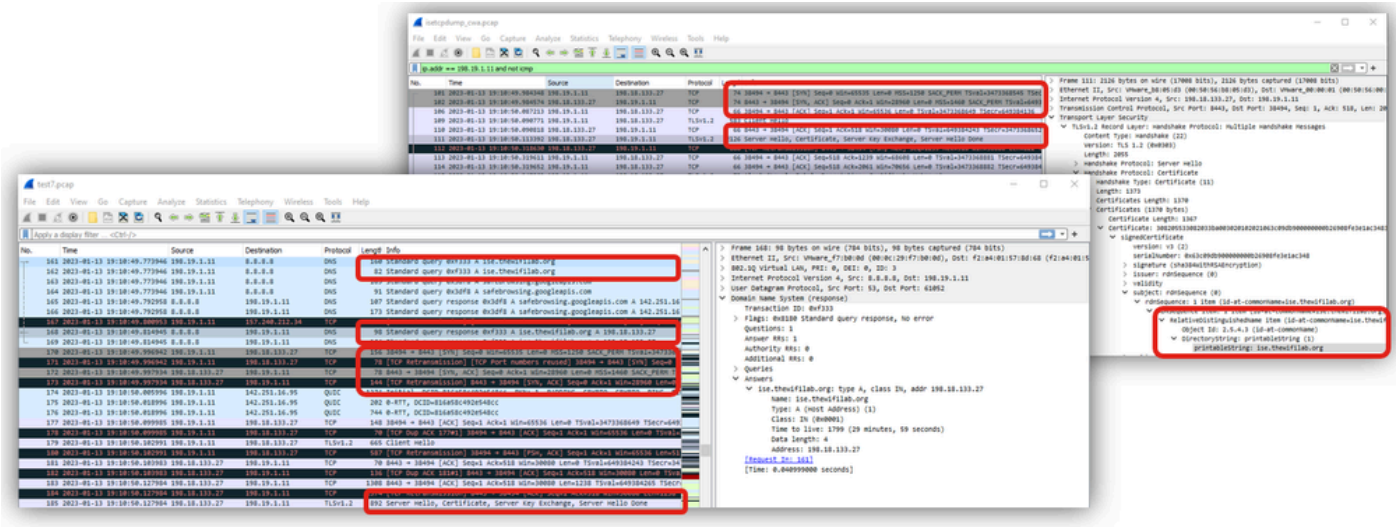
클라이언트 트래픽이 ISE PSN에 도달하는 경우 WLC EPC 및 ISE TCPdump로 확인합니다. WLC

및 ISE에서 캡처를 구성하고 시작합니다.



WLC EPC 및 ISE TCPDump

이슈 재현 후, 캡처를 수집하고 트래픽의 상관성을 분석합니다. 여기서는 ISE 호스트 이름이 확인된 다음 포트 8443에서 클라이언트와 ISE 간의 통신을 확인할 수 있습니다.



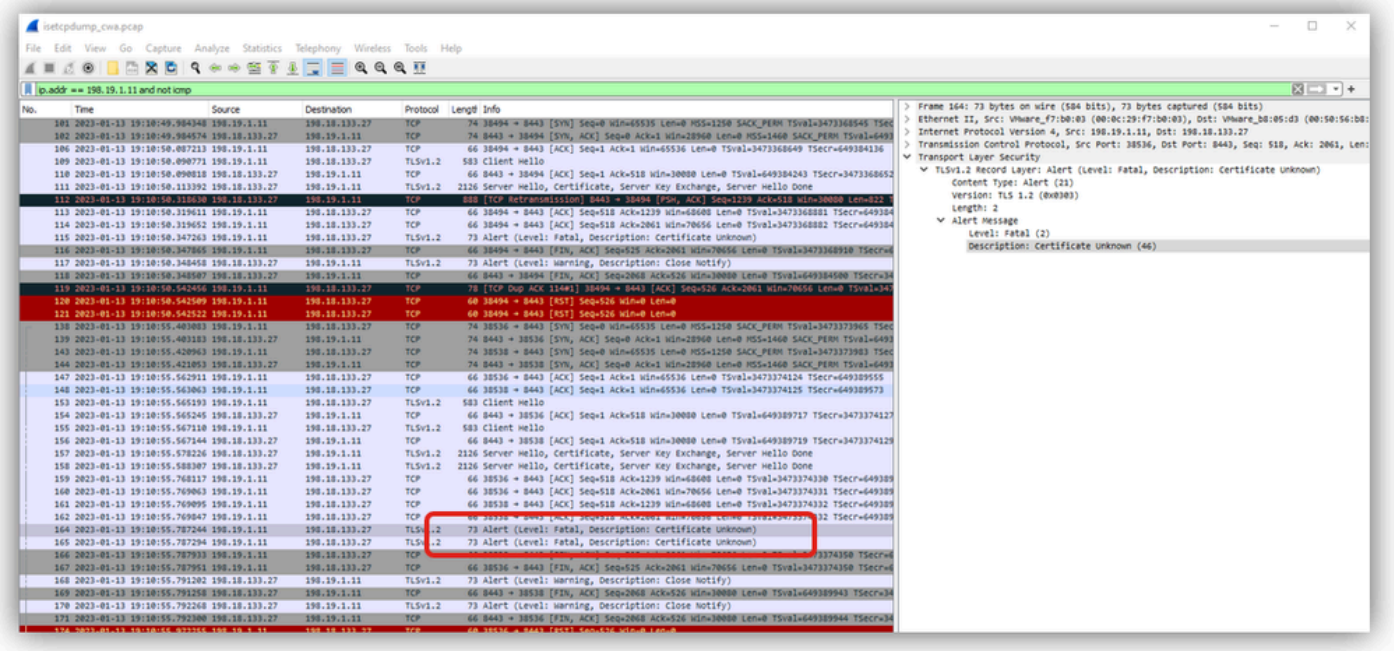
WLC 및 ISE 트래픽

11 - 인증서로 인해 보안 위반이 발생하는 이유는 무엇입니까?

ISE에서 자체 서명 인증서를 사용하는 경우 클라이언트에서 ISE 포털 로그인 페이지를 표시하려고 시도할 때 보안 경고를 발생시킬 것으로 예상됩니다.

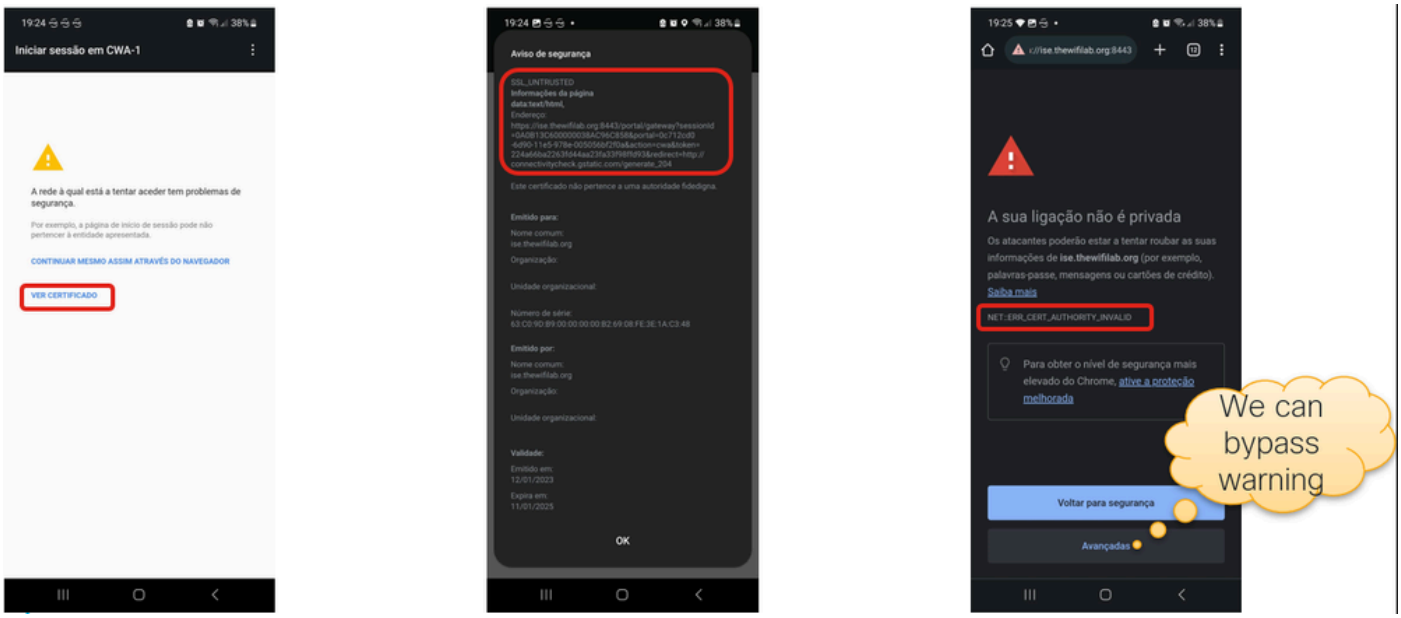
WLC EPC 또는 ISE TCPdump에서 ISE 인증서를 신뢰할 수 있는지 확인할 수 있습니다.

이 예에서는 Alert(Level: 치명적, 설명: unknown(알 수 없는 인증서) - ISE 인증서를 알 수 없음(신뢰할 수 있음):



ISE 신뢰할 수 없는 인증서

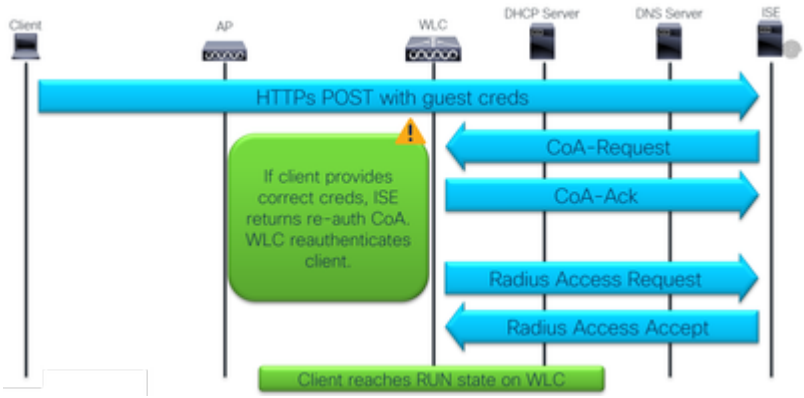
클라이언트 측에서 확인하면 다음 예제가 출력됩니다.



ISE 인증서를 신뢰하지 않는 클라이언트 디바이스

마지막으로 리디렉션이 작동합니다!! 그러나 로그인은 실패합니다...

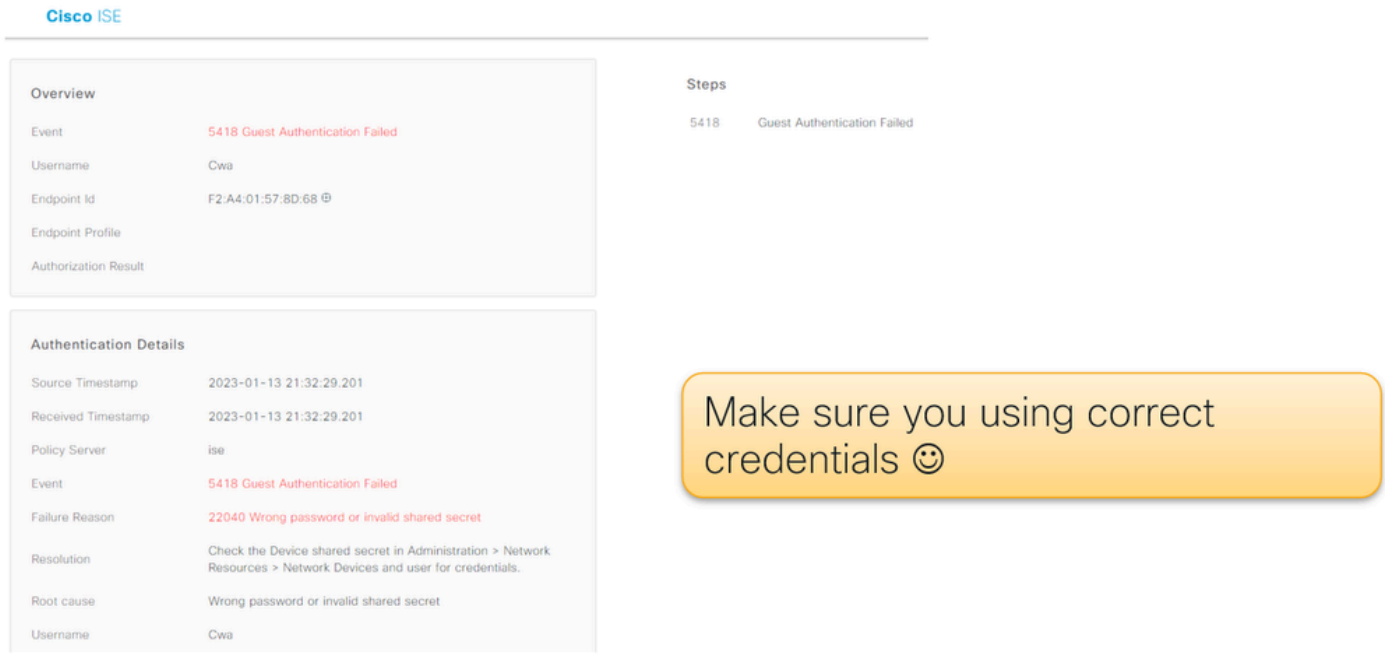
마지막으로 흐름을 확인하는 중...



클라이언트 로그인 및 CoA

12 - 게스트 로그인에 실패합니까?

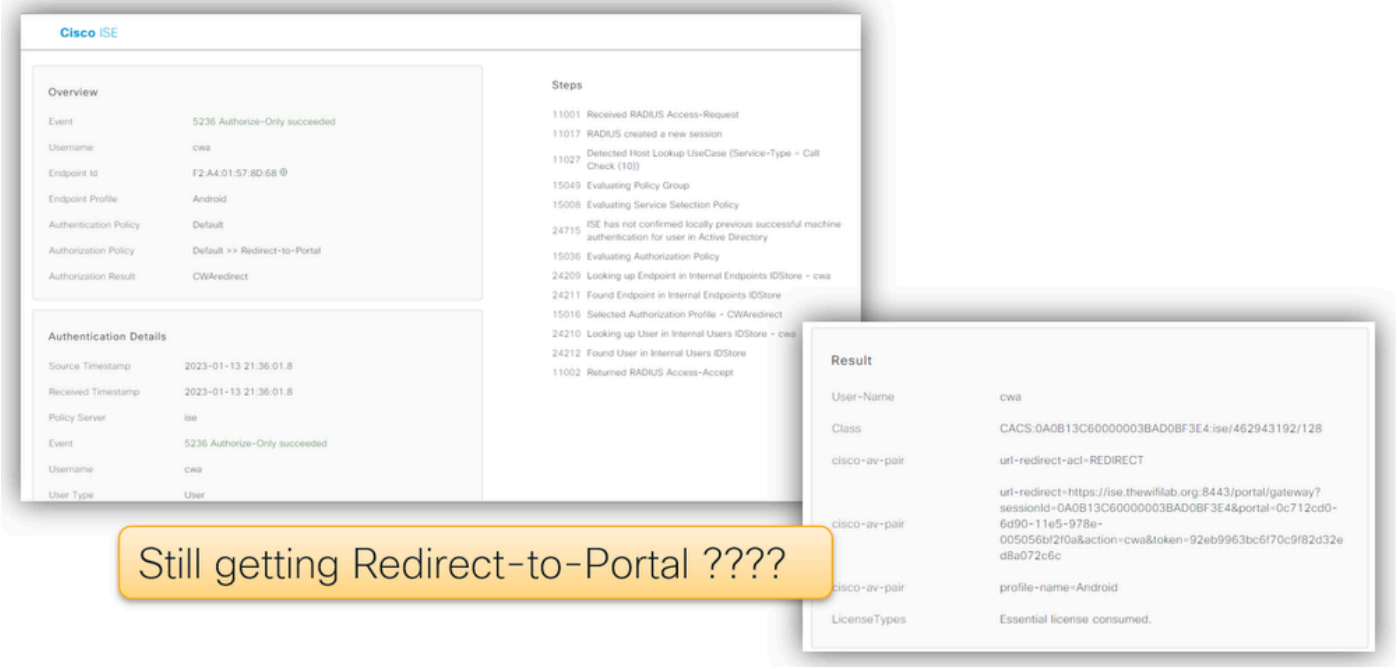
ISE 로그에서 실패한 인증을 확인합니다. 자격 증명이 올바른지 확인하십시오.



잘못된 자격 증명으로 인해 게스트 인증 실패

13 - 로그인은 성공하지만 RUN으로 이동하지 않습니까?

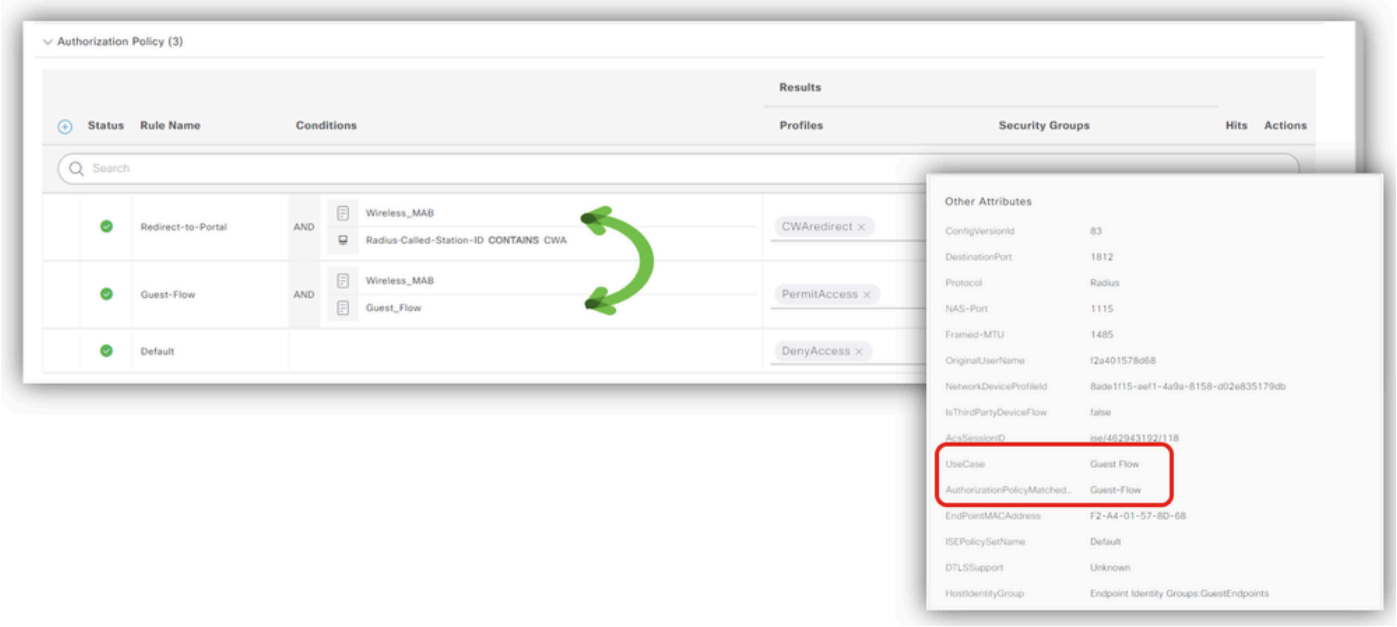
ISE 로그에서 인증 세부사항 및 결과를 확인합니다.



리디렉션 루프

이 예에서는 클라이언트가 리디렉션 URL 및 리디렉션 ACL을 포함하는 권한 부여 프로파일을 다시 가져오는 것을 볼 수 있습니다. 이렇게 하면 리디렉션 루프가 발생합니다.

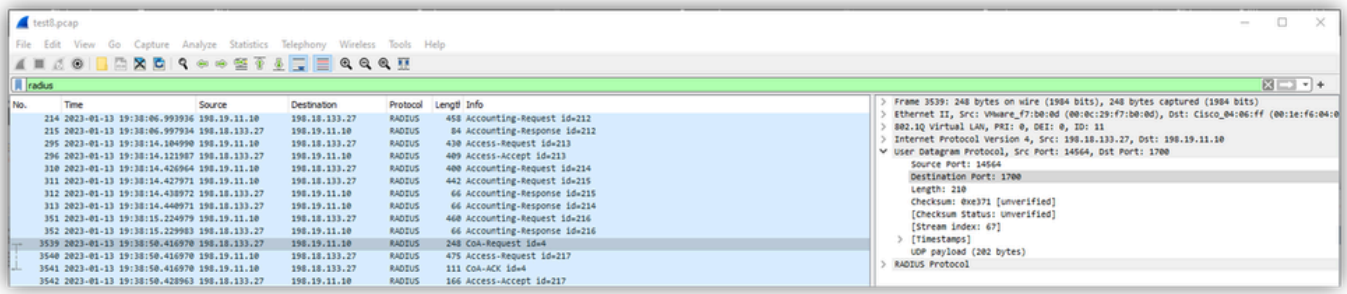
Policy set(정책 설정)를 선택합니다. 규칙 검사 Guest_Flow는 리디렉션 전에 있어야 합니다.



Guest_Flow 규칙

14 - COA 실패?

EPC 및 ISE TCPDump를 사용하여 CoA 트래픽을 확인할 수 있습니다. WLC와 ISE 간에 CoA 포트(1700)가 열려 있는지 확인합니다. 공유 암호가 일치하는지 확인합니다.



CoA 트래픽

참고: 버전 17.4.X 이상에서는 RADIUS 서버를 구성할 때 CoA 서버 키도 구성해야 합니다. 공유 암호와 동일한 키를 사용합니다(ISE에서는 기본적으로 동일함). RADIUS 서버가 구성한 공유 암호가 아닌 CoA에 대해 다른 키를 선택적으로 구성하는 것이 목적입니다. Cisco IOS® XE 17.3에서는 웹 UI에서 CoA 키와 동일한 공유 암호를 사용했습니다.

버전 17.6.1부터 RADIUS(CoA 포함)가 이 포트를 통해 지원됩니다. RADIUS에 대한 서비스 포트를 사용하려면 다음 컨피그레이션이 필요합니다.

<#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

결론

다음은 재개된 CWA 체크리스트입니다.

- 클라이언트가 올바른 VLAN에 있고 IP 주소 및 DNS를 가져와야 합니다.
  - WLC에서 클라이언트 세부 정보를 얻고 패킷 캡처를 실행하여 DHCP 교환을 확인합니다.
- 클라이언트가 DNS를 통해 호스트 이름을 확인할 수 있는지 확인합니다.
  - cmd에서 호스트 이름을 ping합니다.
- WLC는 포트 80에서 수신 대기해야 합니다.
  - 전역 명령 ip http server 또는 전역 매개변수 맵 명령 webauth-http-enable을 확인합니다.
- 인증서 경고를 제거하려면 ISE에 신뢰할 수 있는 인증서를 설치합니다.
  - CWA의 WLC에 신뢰할 수 있는 인증서를 설치할 필요가 없습니다.
- 사용자를 찾을 수 없는 경우 ISE의 인증 정책 고급 옵션 "계속"
  - 스폰서 게스트 사용자가 연결하고 URL 리디렉션 및 ACL을 가져올 수 있도록 허용

트러블슈팅에 사용되는 기본 도구는 다음과 같습니다.

- WLC EPC
  - 내부 필터: DHCP 프로토콜, mac 주소
- WLC 모니터
  - 클라이언트 보안 세부 정보를 확인합니다.
- WLC RA 추적
  - WLC 측에서 자세한 정보가 포함된 디버깅
- ISE 라이브 로그
  - 인증 세부 정보.
- ISE TCPDump
  - ISE PSN 인터페이스에서 패킷 캡처를 수집합니다.

참조

Catalyst 9800 WLC 및 ISE에서 CWA(Central Web Authentication) 구성

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.