# Risoluzione dei problemi di autenticazione Web centrale (CWA) con Wireless Lan Controller (WLC) 9800 e Identity Services Engine (ISE)

## Sommario



## Introduzione

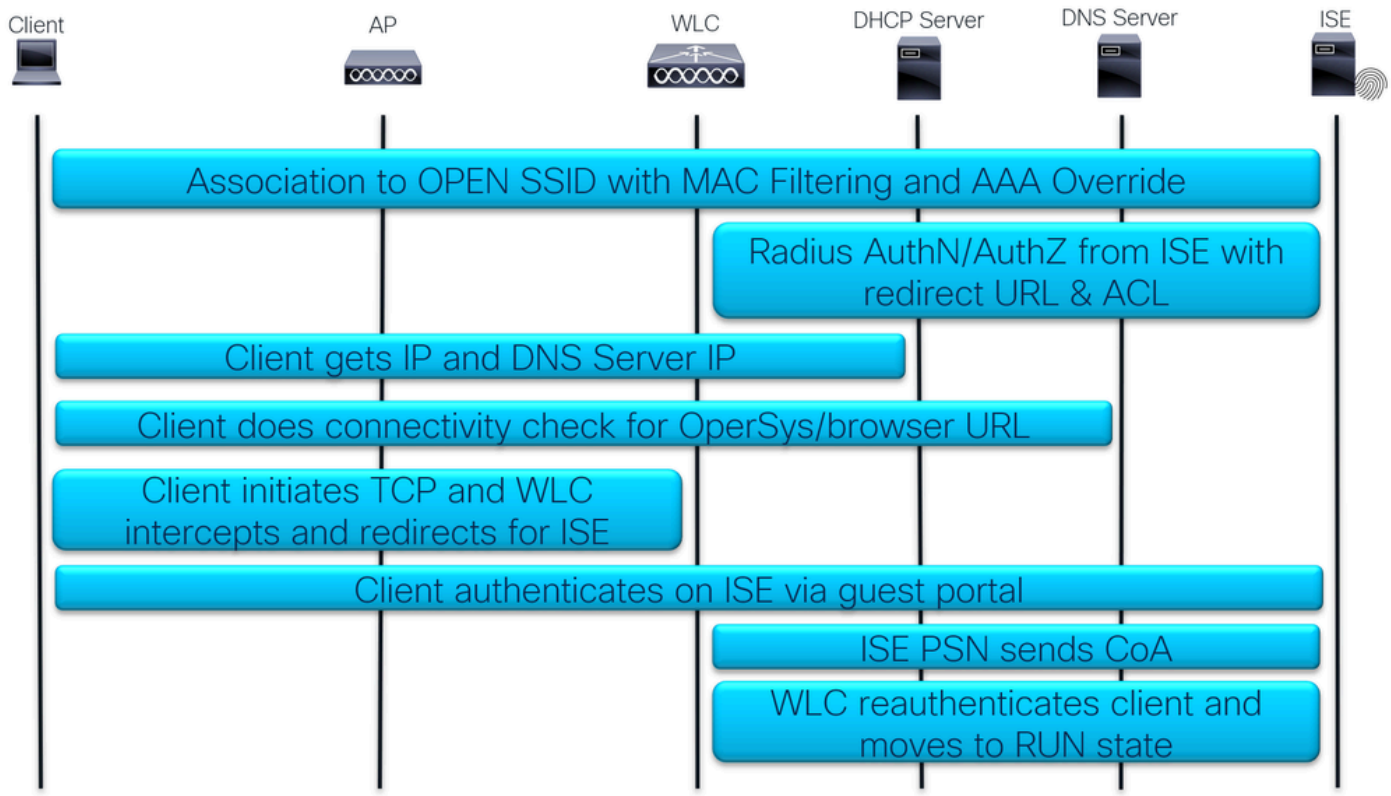
Questo documento descrive come risolvere i problemi di autenticazione Web centrale (CWA) con WLC 9800 e ISE.

## Informazioni sullo sfondo

Al momento sono presenti così tante periferiche personali che gli amministratori di rete che cercano di proteggere l'accesso wireless normalmente optano per le reti wireless che utilizzano CWA.
In questo documento, ci concentriamo sul diagramma di flusso di CWA, che aiuta nella risoluzione dei problemi comuni che ci riguardano.
Esaminiamo i gateway comuni del processo, come raccogliere i log relativi a CWA, come analizzare questi log e come raccogliere un'acquisizione di pacchetti incorporata sul WLC per confermare il flusso del traffico.

CWA è l'impostazione più comune per le società che consente agli utenti di connettersi alla rete aziendale utilizzando i propri dispositivi personali, noti anche come BYOD.
Tutti gli amministratori di rete sono interessati alle operazioni di accesso e risoluzione dei problemi da eseguire per risolvere i problemi prima di aprire una richiesta TAC.

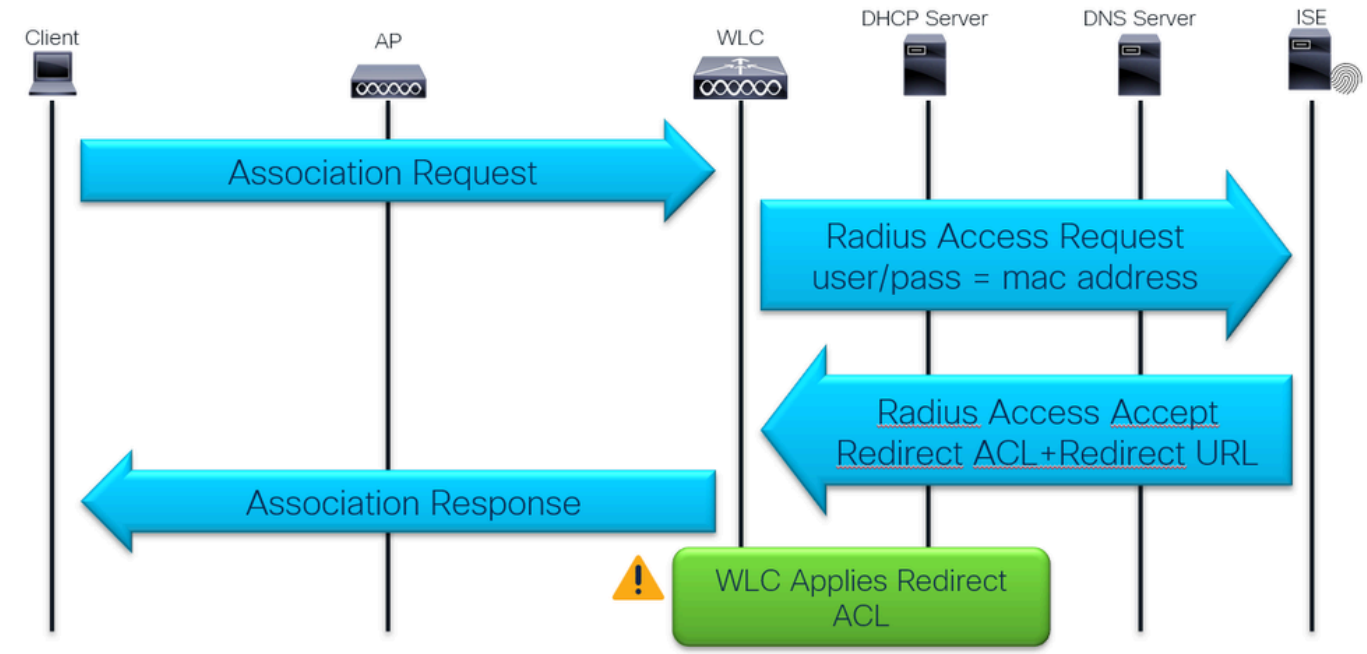
Di seguito è riportato il flusso del pacchetto CWA:




Flusso pacchetti CWA

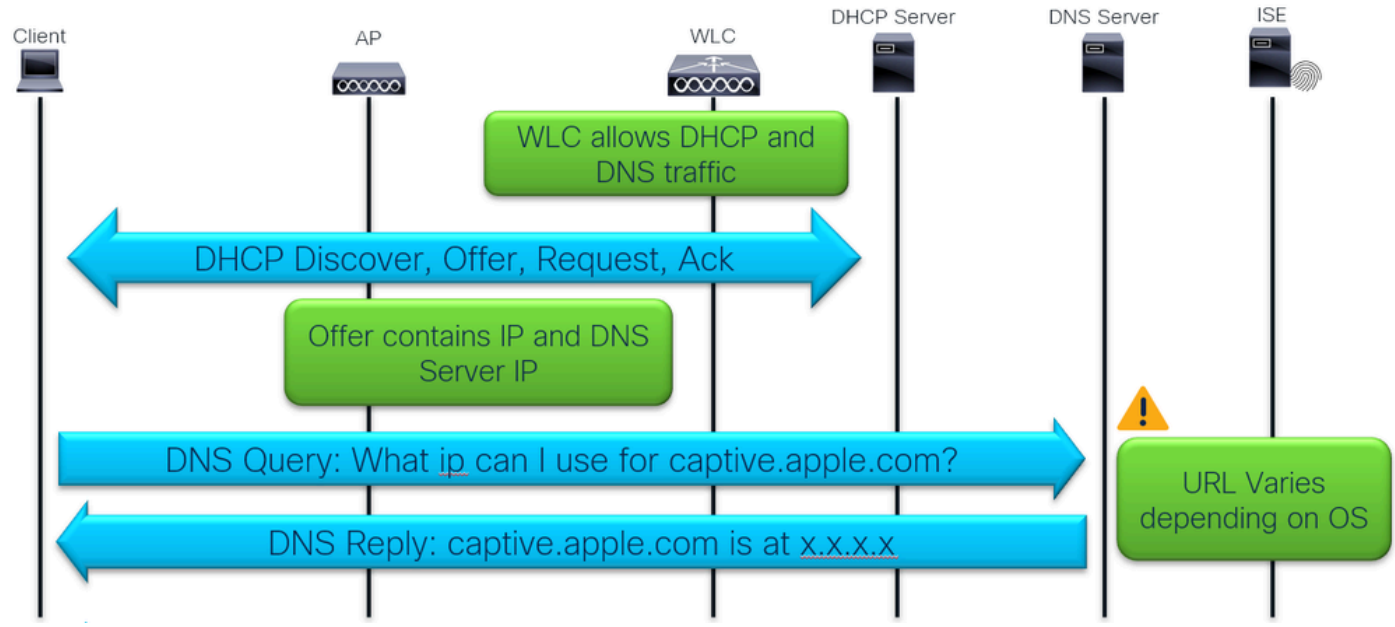
## Flusso dettagliato

Prima associazione e autenticazione RADIUS:




Prima associazione e autenticazione RADIUS

Controllo DHCP, DNS e connettività:




Verifica di DHCP, DNS e connettività

Il controllo della connettività viene eseguito utilizzando il rilevamento del portale vincolato da parte del browser o del sistema operativo del dispositivo client.

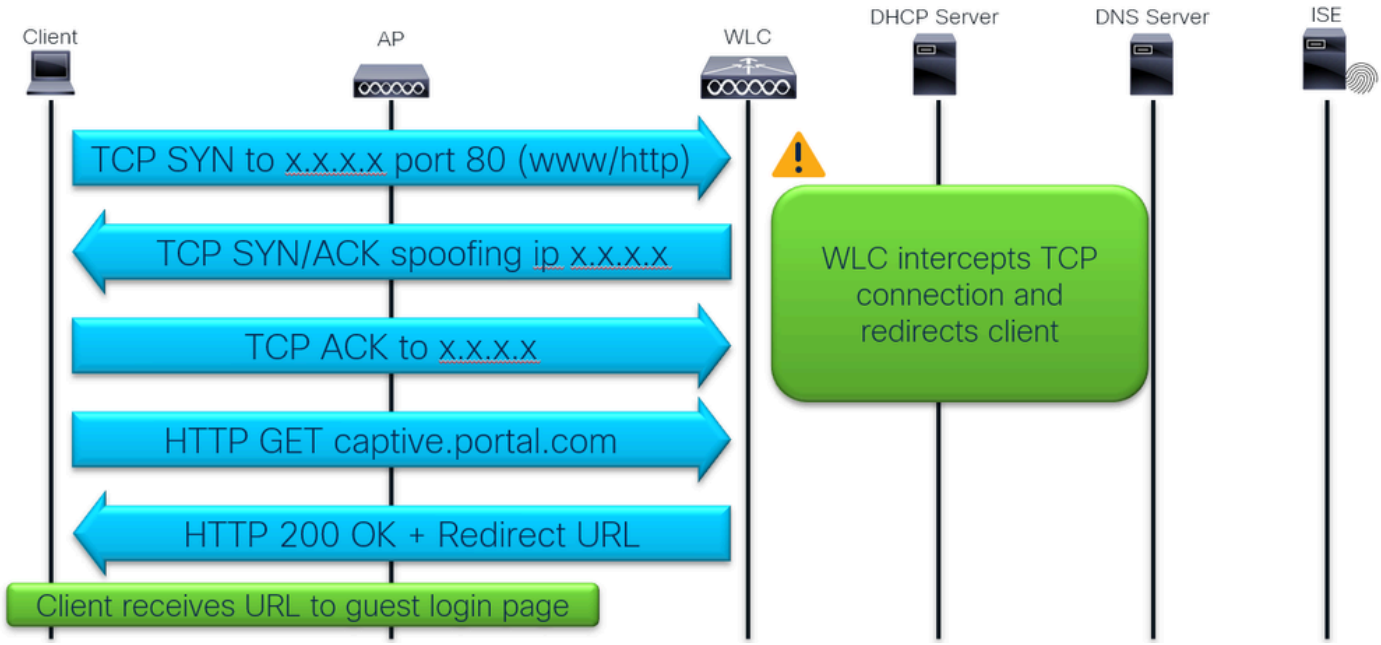
Esistono sistemi operativi dei dispositivi preprogrammati per eseguire HTTP GET verso un dominio specifico

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

I browser eseguono inoltre questo controllo all'apertura:

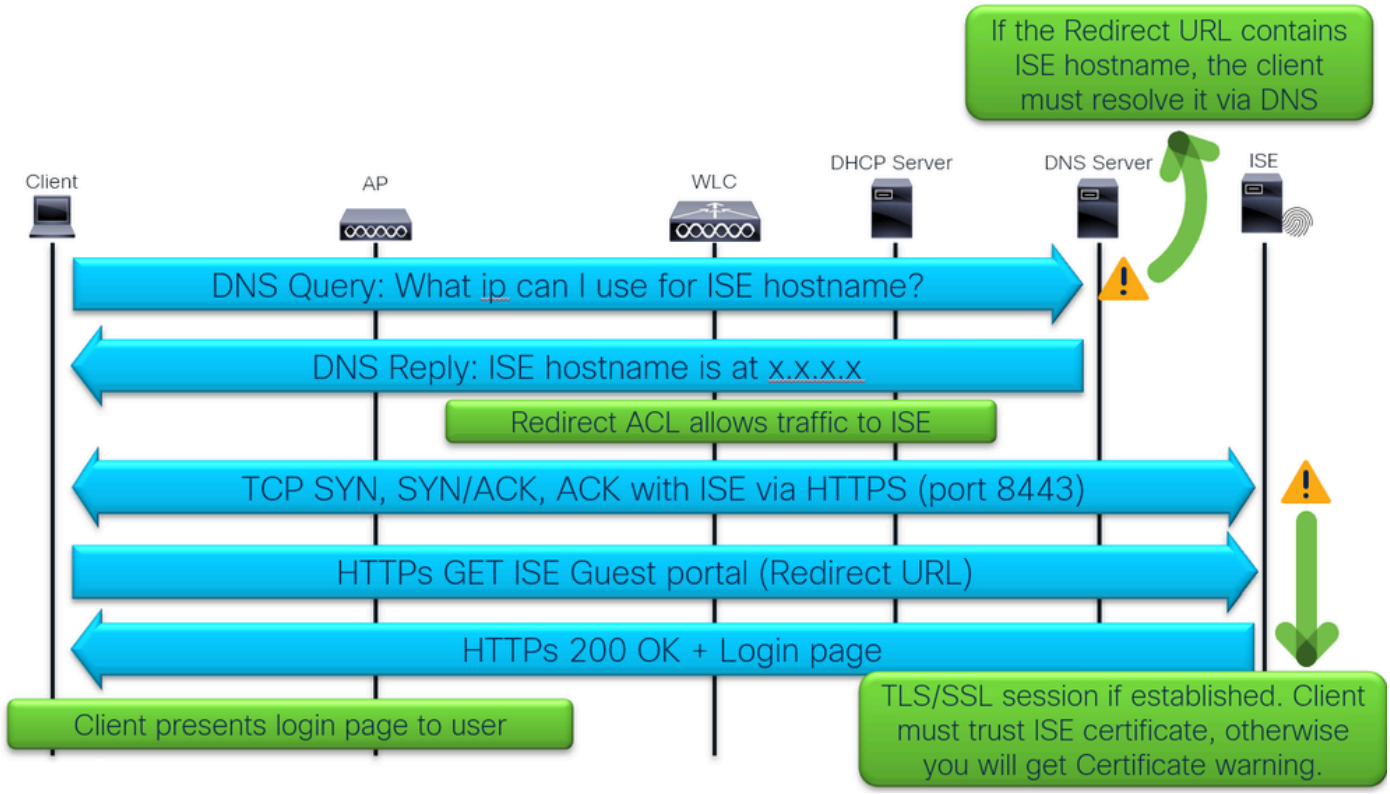
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Intercettazione e reindirizzamento del traffico:



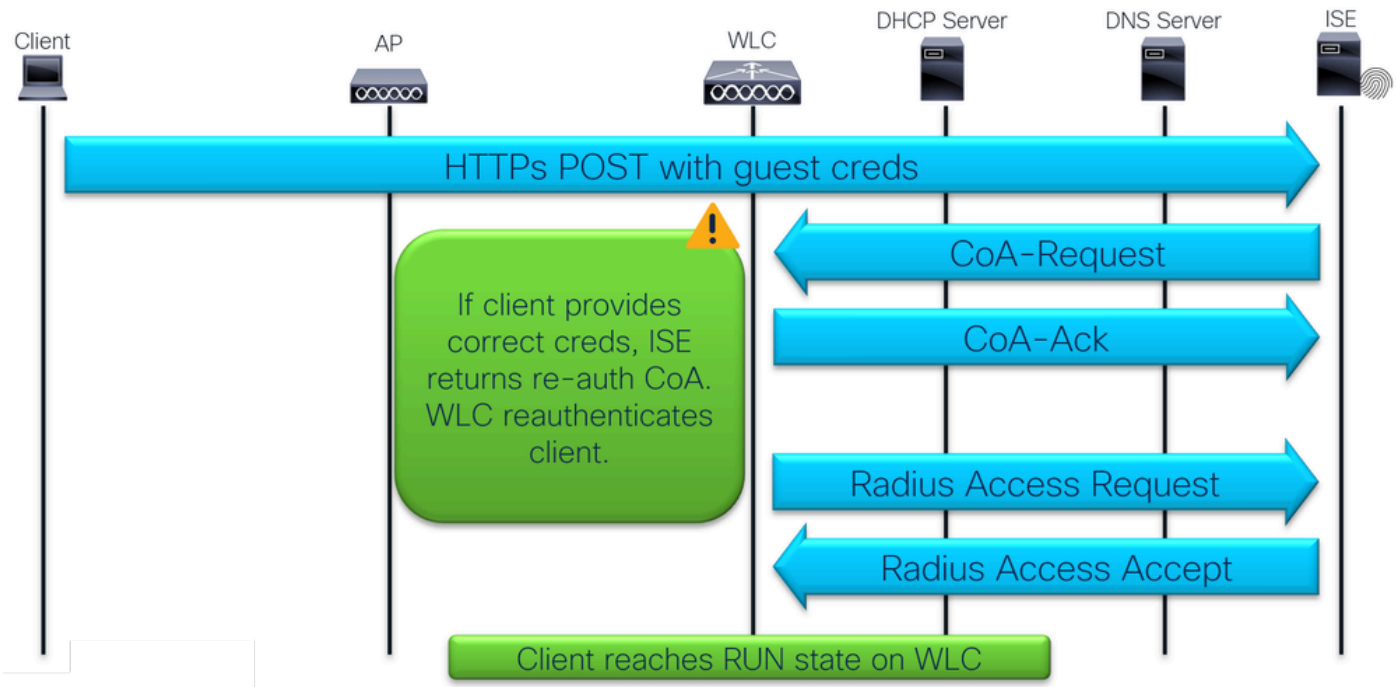

Intercettazione e reindirizzamento del traffico

Accesso client al portale di accesso guest ISE:




Accesso client al portale di accesso guest ISE

Accesso client e CoA:

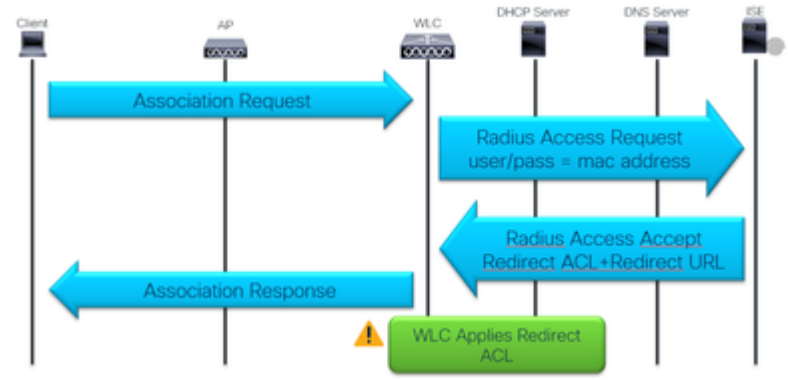



Accesso client e CoA

# Risoluzione dei problemi

## Sintomo comune: L'utente non viene reindirizzato alla pagina di accesso.

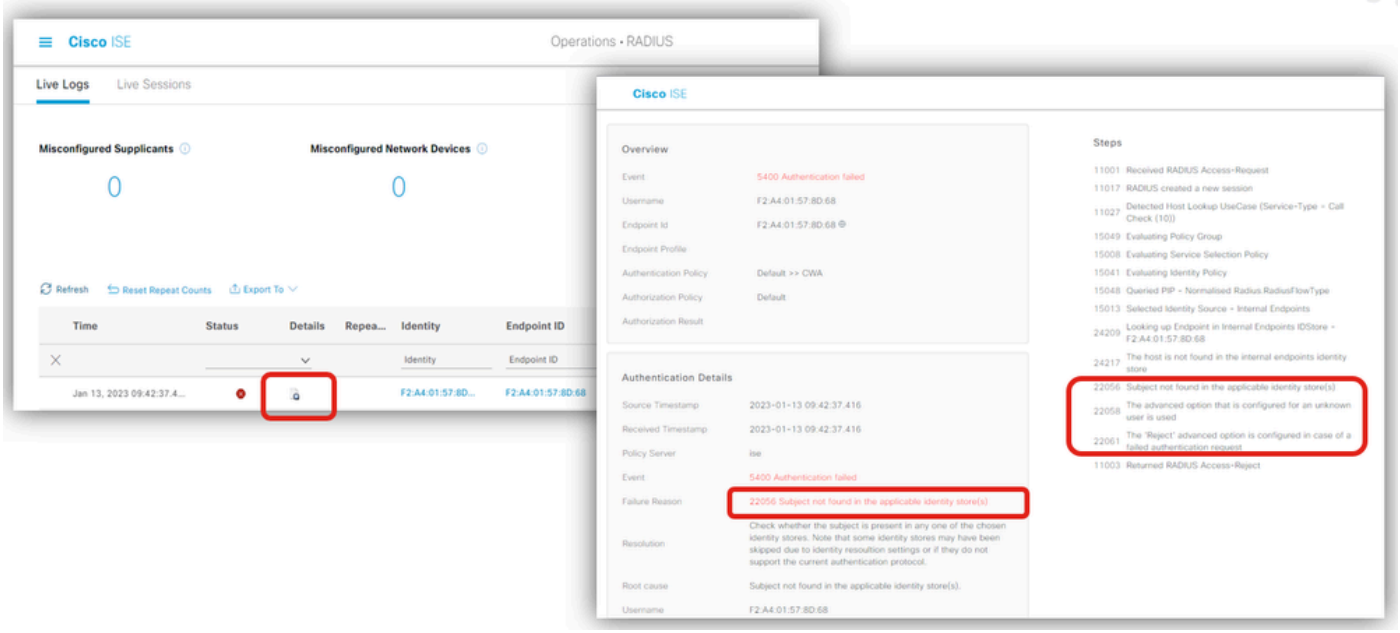
Cominciamo con la prima parte del flusso:




Prima associazione e autenticazione RADIUS

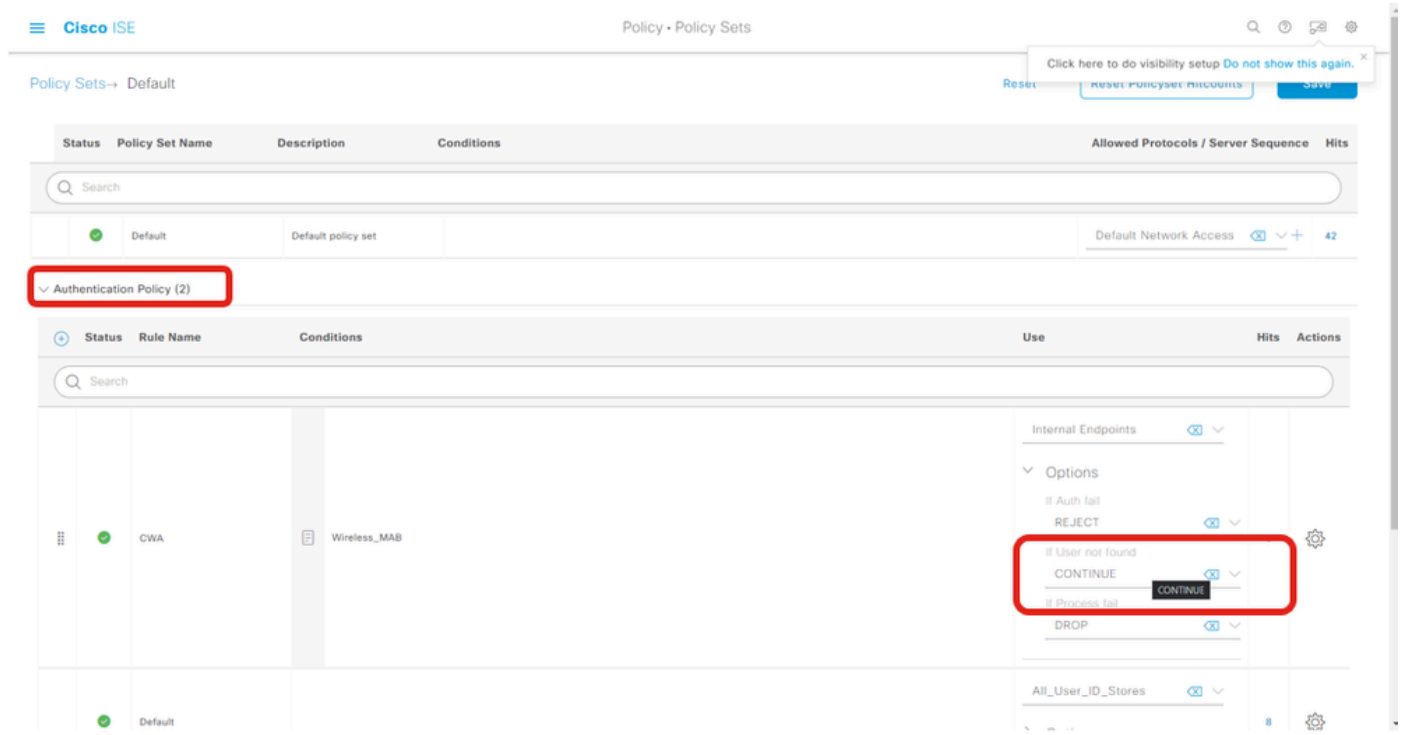
1 - La prima autenticazione RADIUS è riuscita?

Verificare il risultato dell'autenticazione del filtro MAC:




Log ISE Live che mostrano il risultato dell'autenticazione del filtro MAC

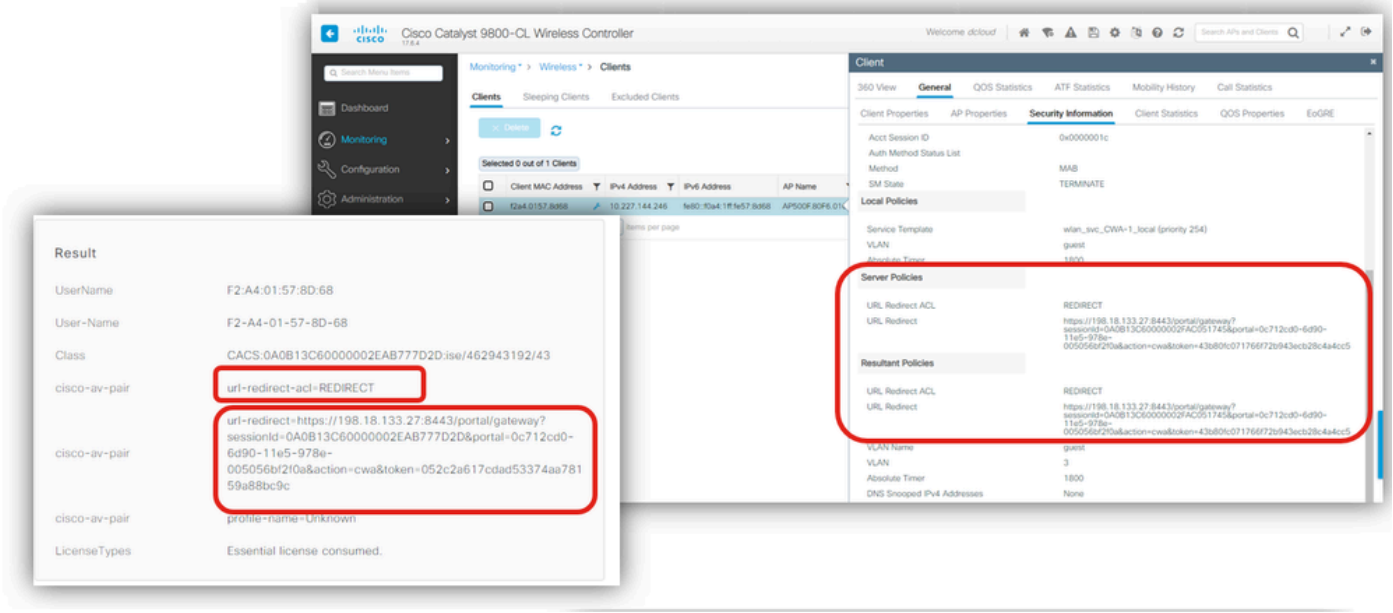
Assicurarsi che l'opzione avanzata per l'autenticazione sia impostata su "Continua" se l'utente non viene trovato:




Opzione avanzata utente non trovato

2 - Il WLC riceve l'URL di reindirizzamento e l'ACL?

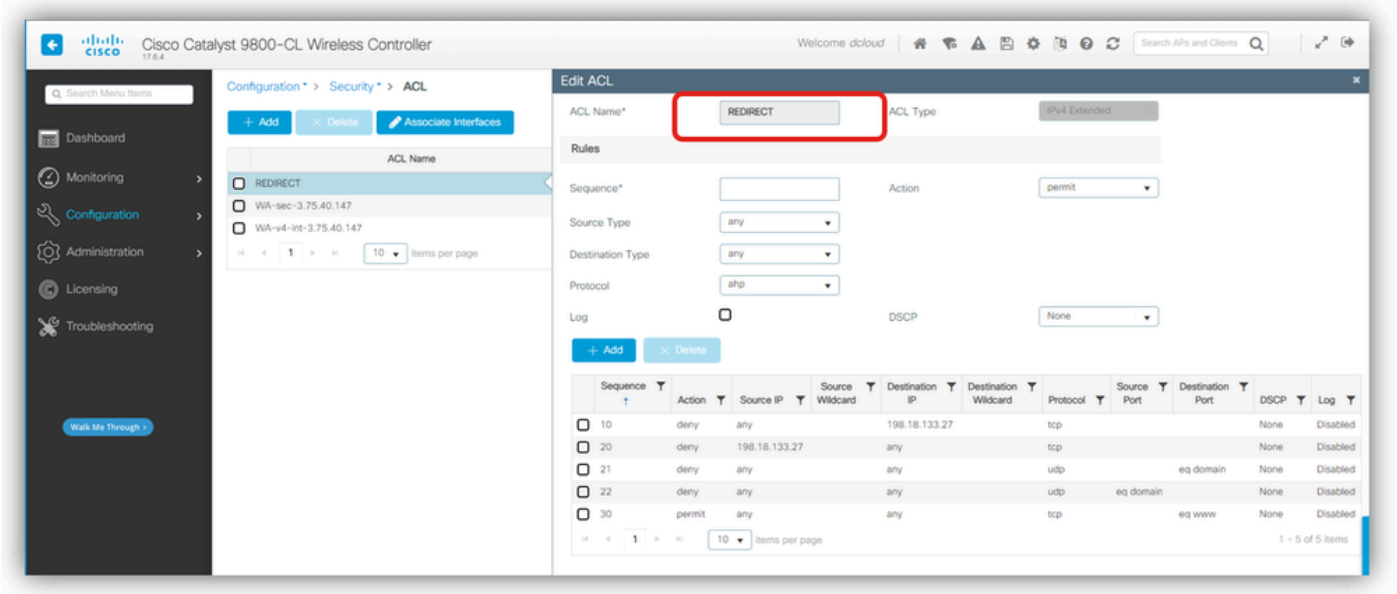
Controllare i log ISE in tempo reale e le informazioni sulla sicurezza del client WLC in Monitoraggio Verificare che ISE invii l'URL di reindirizzamento e l'ACL nell'Access Accept e che venga ricevuto dal WLC e applicato al client nei dettagli del client:




Reindirizzamento di ACL e URL

3 - L'ACL di reindirizzamento è corretto?

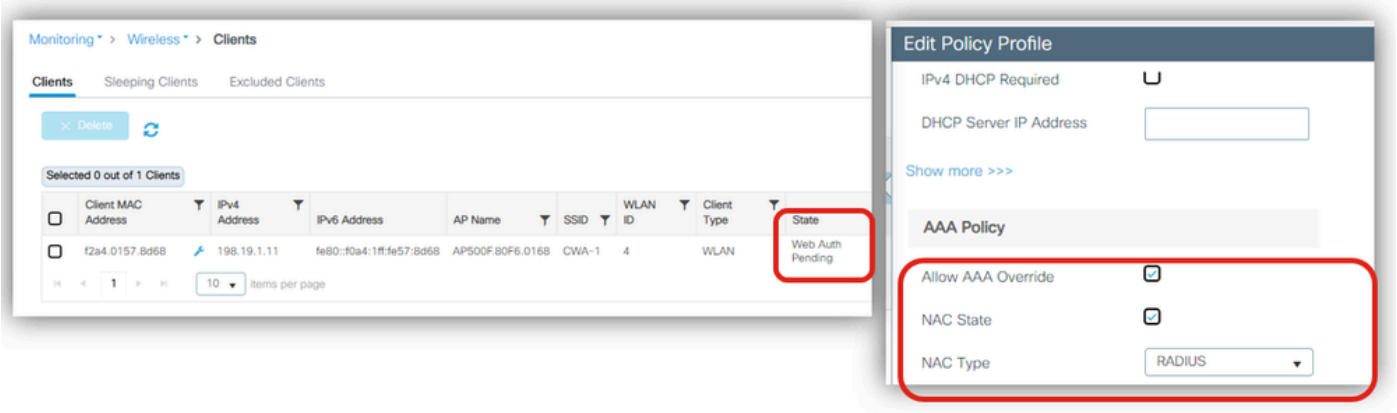
Controllare se il nome dell'ACL è stato digitato. Accertarsi che sia esattamente come quando viene inviato dall'ISE:




Verifica ACL di reindirizzamento

4 - Il client viene spostato in Web-Auth in sospeso?

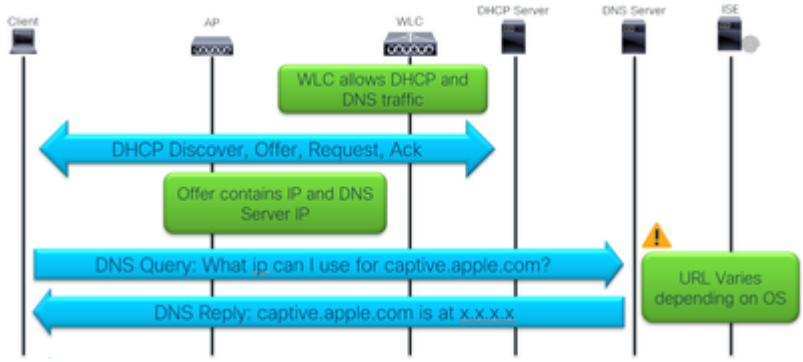
Verificare nei dettagli del client lo stato "Autenticazione Web in sospeso". Se non è in questo stato, verificare se nel profilo della policy sono abilitate le sostituzioni AAA e il NAC Radius:




Dettagli client, aaa override e RADIUS NAC

## Ancora non funziona?

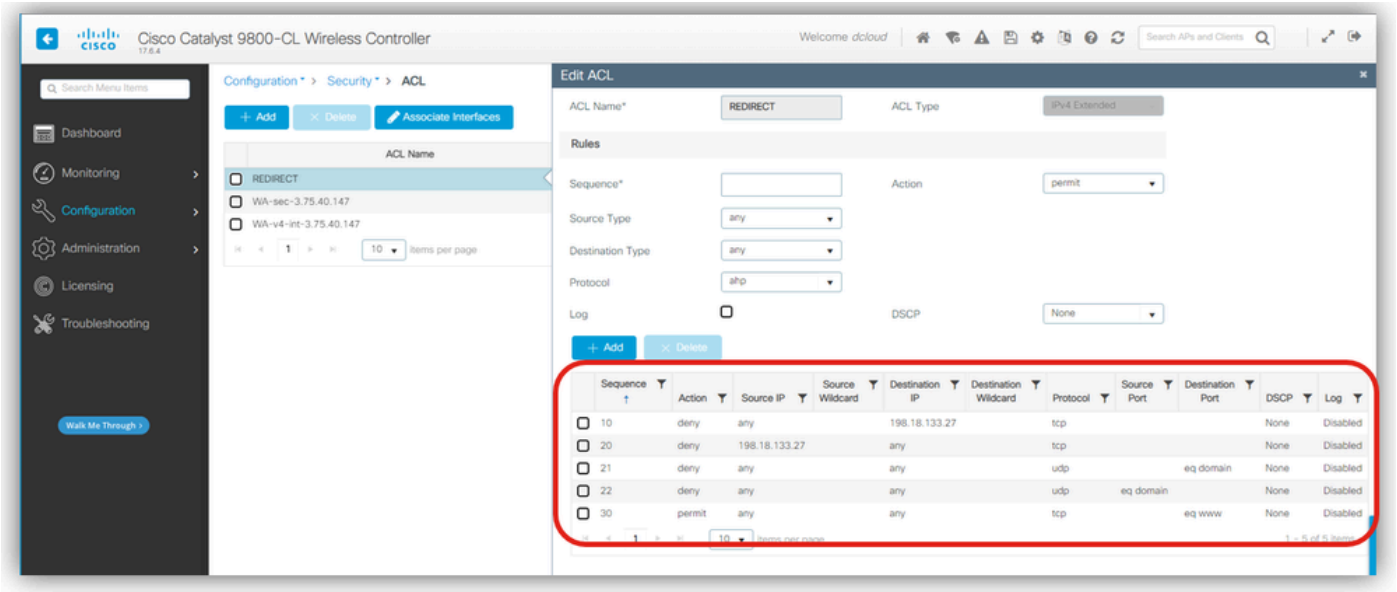
## Rivediamo il flusso...




Verifica di DHCP, DNS e connettività

## 5 - Il WLC consente il traffico DHCP e DNS?

## Verificare il contenuto dell'ACL di reindirizzamento nel WLC:




Reindirizza i contenuti dell'ACL nel WLC

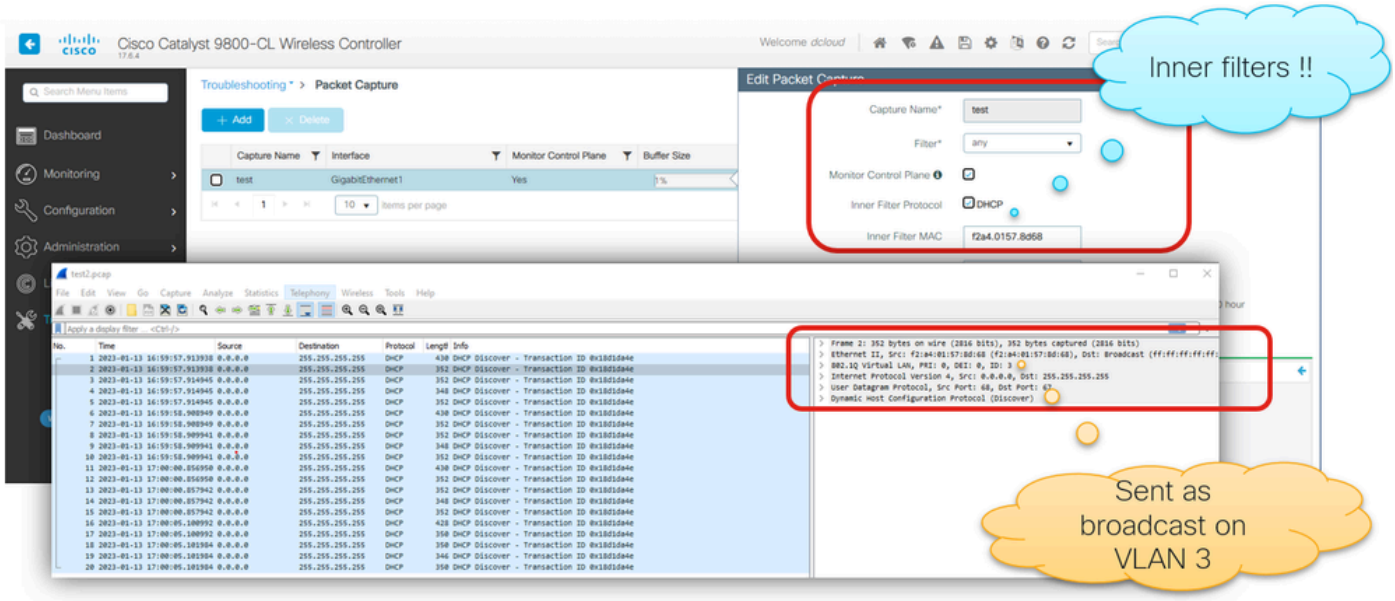
L'ACL di reindirizzamento definisce il traffico intercettato e reindirizzato dall'istruzione allow e il traffico ignorato dall'intercettazione e dal reindirizzamento con un'istruzione deny.

Nell'esempio, viene consentito il flusso del DNS e del traffico da/verso l'indirizzo IP ISE e viene intercettato qualsiasi traffico tcp sulla porta 80 (www).

6 - Il server DHCP riceve una richiesta/individuazione DHCP?

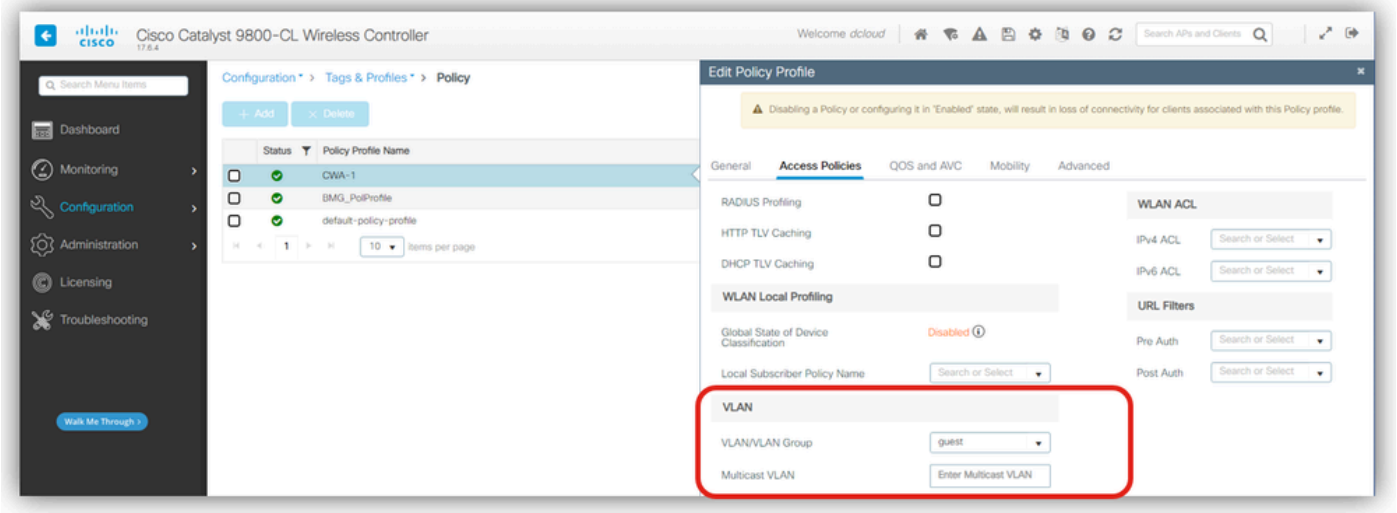
Verificare con l'EPC se avviene lo scambio DHCP. EPC può essere utilizzato con i filtri interni come il protocollo DHCP e/o l'indirizzo MAC del filtro interno dove possiamo usare l'indirizzo MAC del dispositivo client e ricevere nell'EPC solo i pacchetti DHCP inviati da o inviati all'indirizzo MAC del dispositivo client.

Nell'esempio, viene mostrato come inviare i pacchetti DHCP Discover come broadcast sulla VLAN 3:



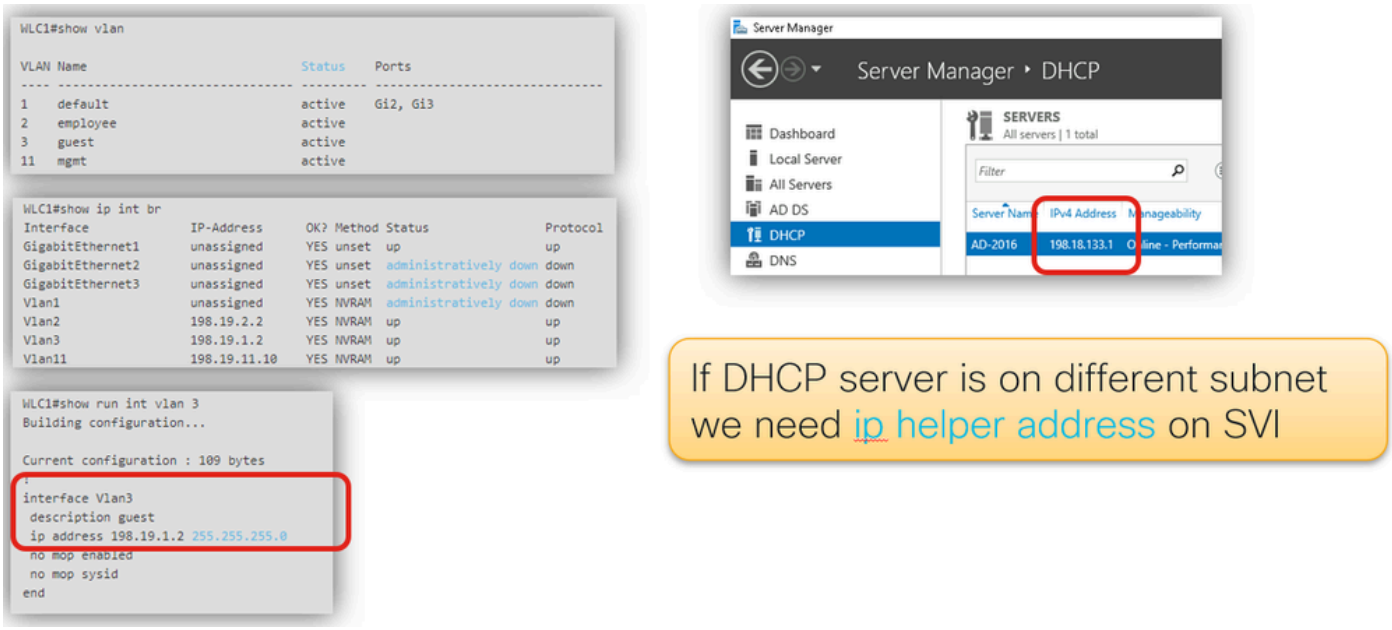

EPC WLC per verificare DHCP

Confermare la VLAN client prevista nel profilo dei criteri:



VLAN nel profilo dei criteri

Verificare la configurazione della VLAN WLC e del trunk della porta switch e la subnet DHCP:



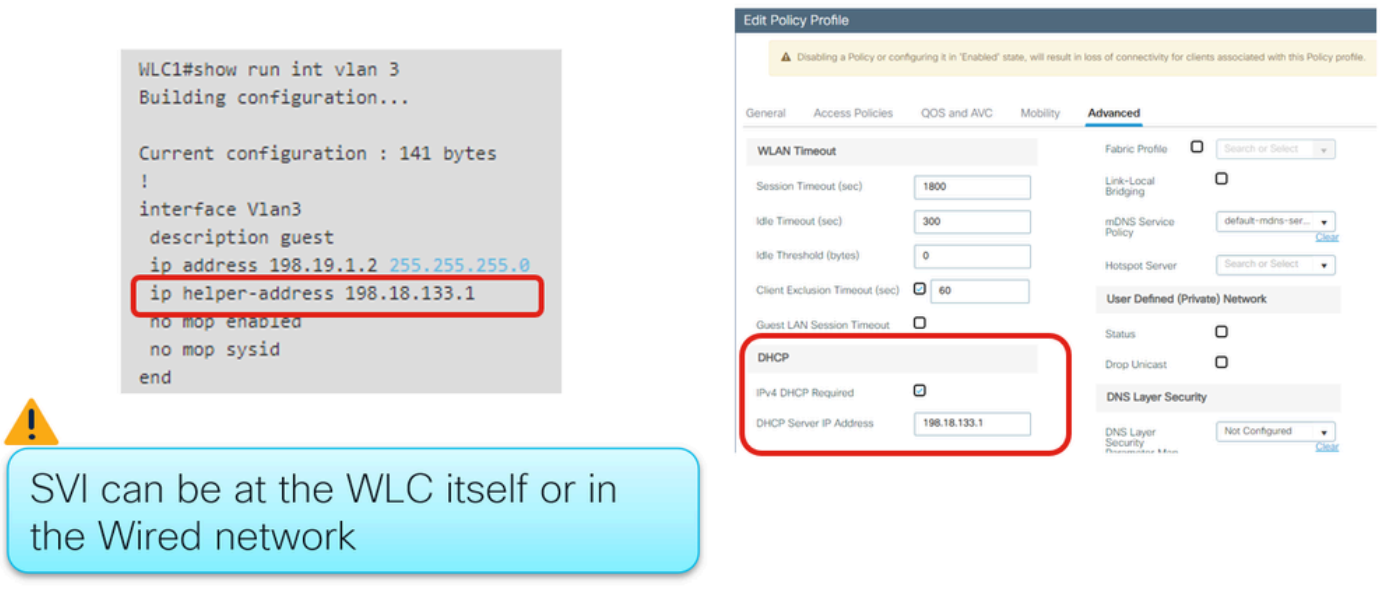

VLAN, switchport e subnet DHCP

Possiamo vedere che la VLAN 3 esiste nel WLC e ha anche SVI per la VLAN 3, ma quando verifichiamo l'indirizzo IP del server DHCP, che si trova su una subnet diversa, abbiamo bisogno dell'indirizzo dell'helper IP sulla SVI.

Le best practice richiedono che la SVI per le subnet client sia configurata nell'infrastruttura cablata ed evita che avvenga sul WLC.

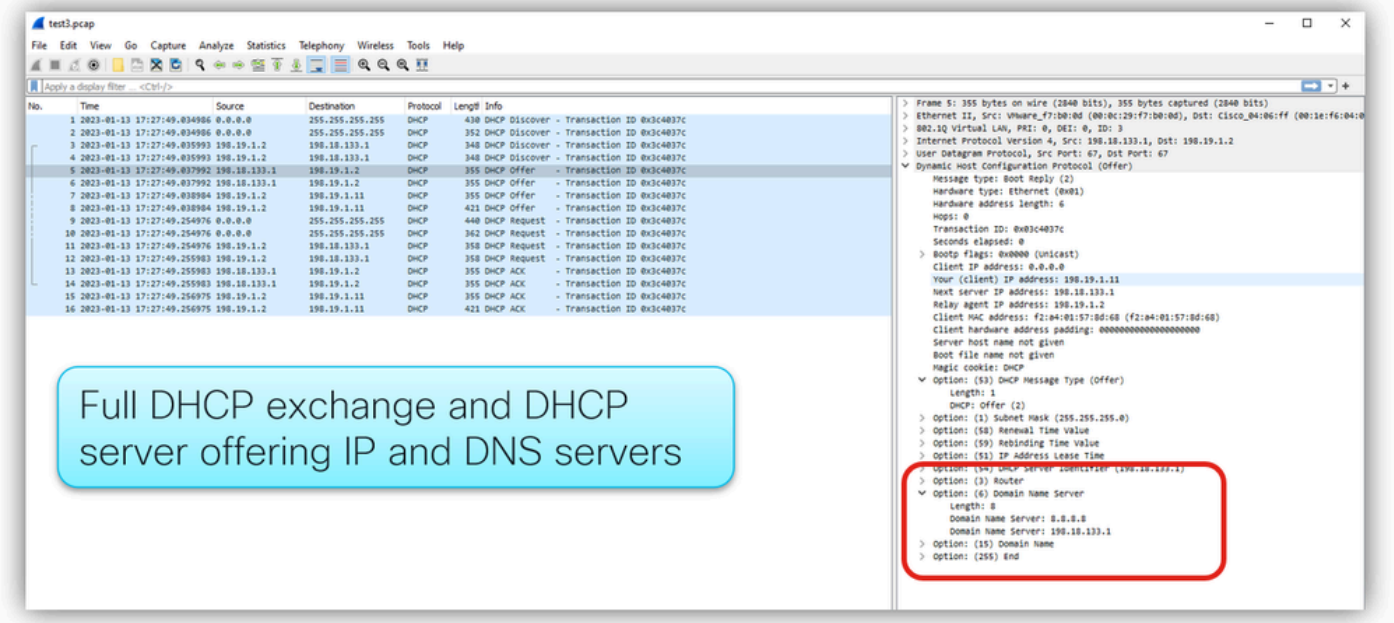
In uno dei casi, il comando ip helper-address deve essere aggiunto all'SVI, indipendentemente dalla sua posizione.

In alternativa, è possibile configurare l'indirizzo IP del server DHCP nel profilo dei criteri:



Indirizzo dell'helper IP presso SVI o Policy Profile

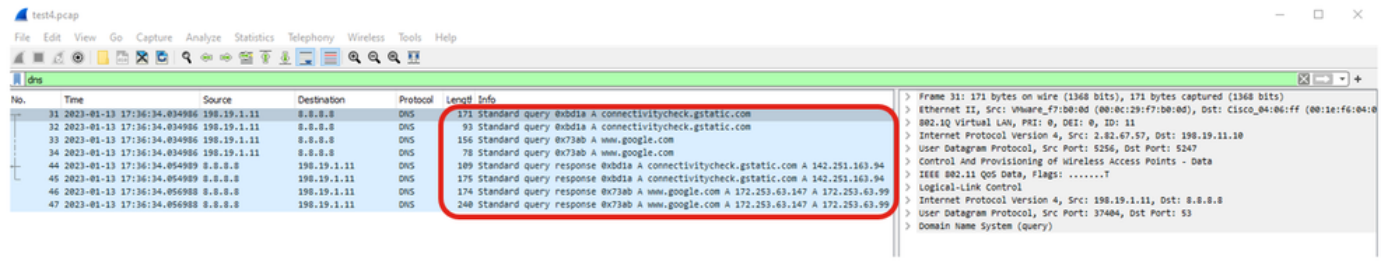
È quindi possibile verificare con EPC se lo scambio DHCP è ora corretto e se il server DHCP offre IP server DNS:




Dettagli offerta DHCP dell'indirizzo IP del server DNS

7 - Viene eseguito il reindirizzamento automatico?

Verificare con EPC WLC se il server DNS risponde alle query:

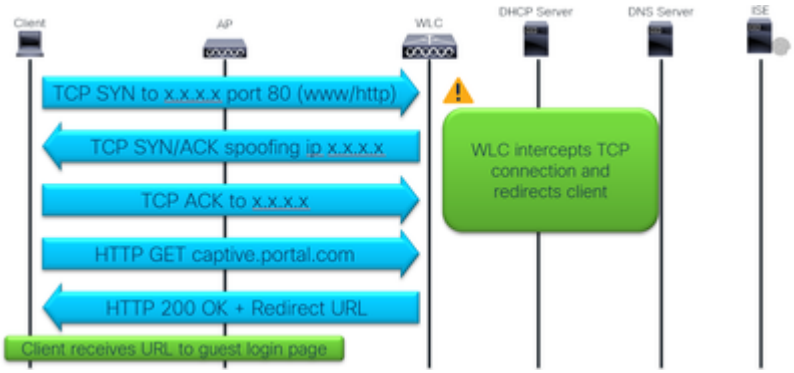


Query e risposte DNS

- Se il reindirizzamento non è automatico, aprire un browser e provare con un indirizzo IP casuale. Ad esempio 10.0.0.1.
- Se il reindirizzamento funziona, è possibile che si sia verificato un problema di risoluzione DNS.

Ancora non funziona?

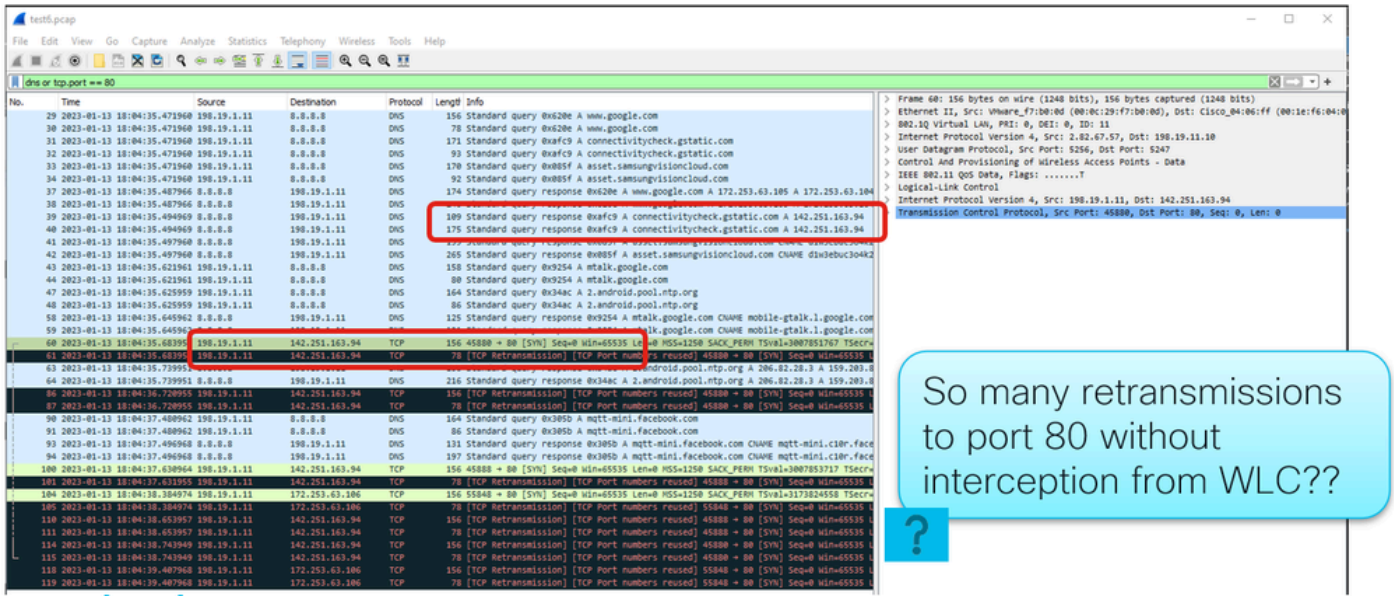
Rivediamo il flusso...




Intercettazione e reindirizzamento del traffico

8 - Il browser non visualizza la pagina di accesso?

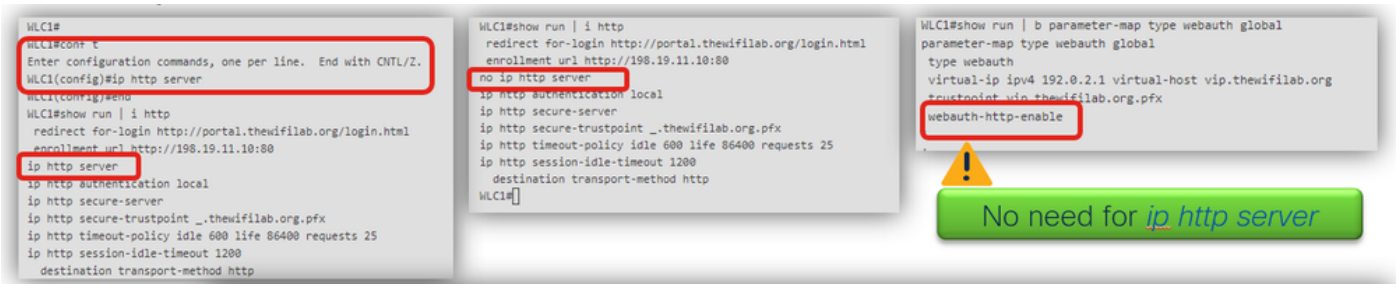
Verificare se il client invia il comando TCP SYN alla porta 80 e se il WLC lo intercetta:




Ritrasmissioni TCP sulla porta 80

Qui possiamo vedere che il client invia i pacchetti TCP SYN alla porta 80 ma non riceve alcuna risposta ed esegue le ritrasmissioni TCP.

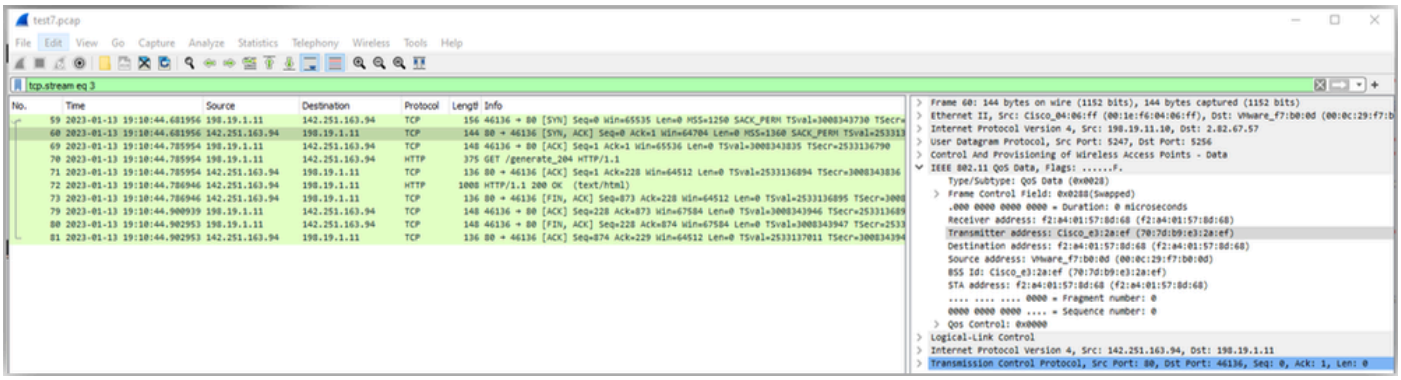
Verificare che il comando ip http server sia nella configurazione globale o webauth-http-enable nella mappa dei parametri globale:




comandi di intercettazione http

Dopo l'esecuzione del comando, il WLC intercetta il TCP e falsifica l'indirizzo IP di destinazione

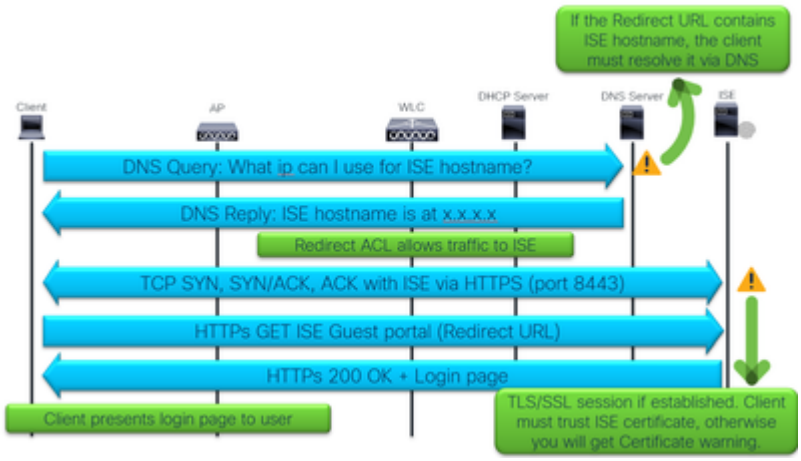
per rispondere al client e reindirizzarlo.



Intercettazione TCP da parte del WLC

Ancora non funziona?

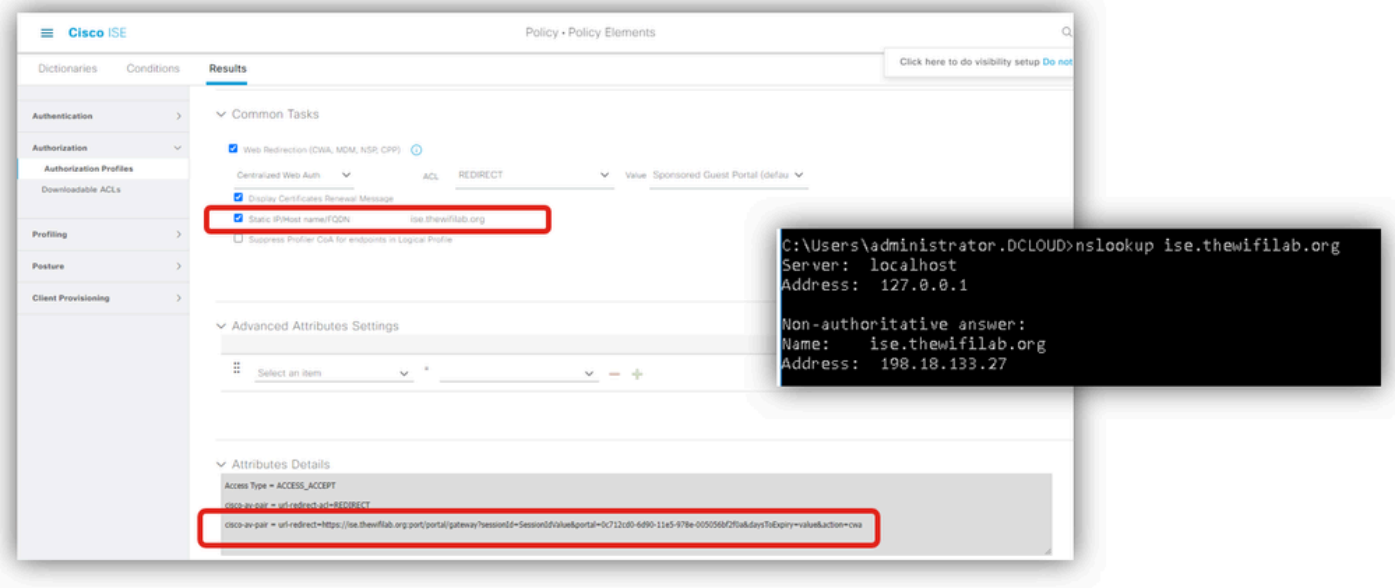
C'è altro nel flusso...




Accesso client al portale di accesso guest ISE

9 - Il client è in grado di risolvere il problema relativo al nome host ISE?

Verificare se l'URL di reindirizzamento utilizza un indirizzo IP o un nome host e se il client risolve il problema relativo al nome host ISE:

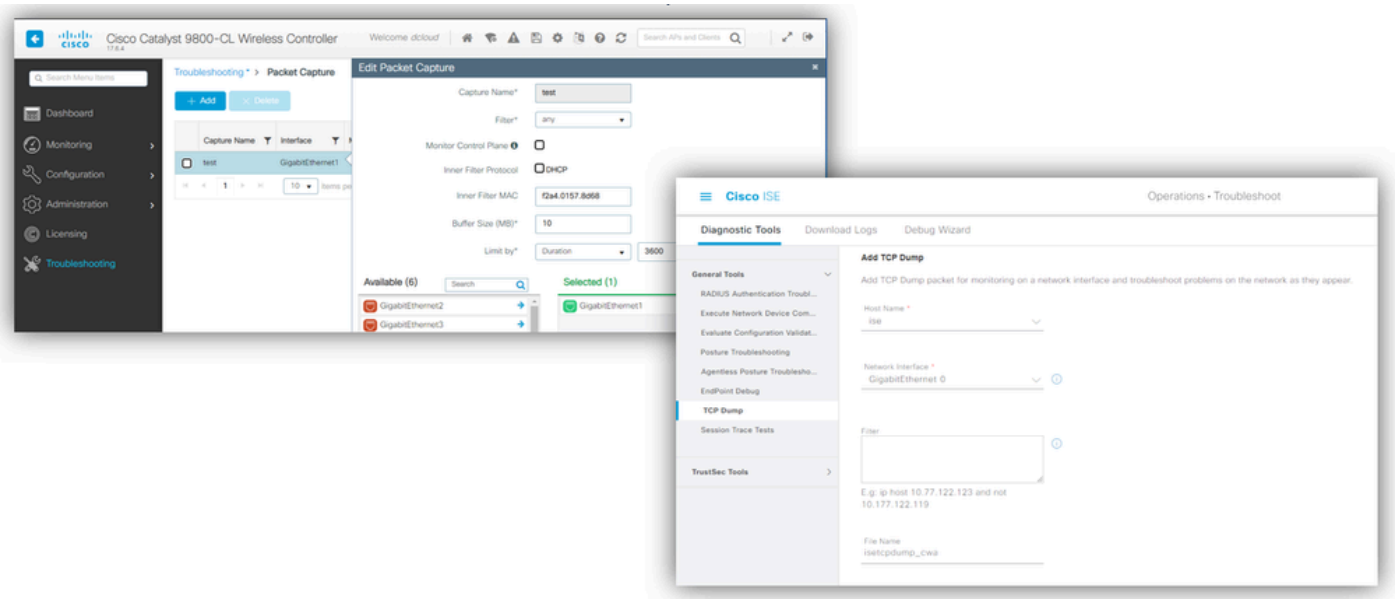



Risoluzione ISE Hostname

Un problema comune si verifica quando l'URL di reindirizzamento contiene il nome host ISE, ma il dispositivo client non è in grado di risolvere tale nome host nell'indirizzo IP ISE. Se si utilizza hostname, assicurarsi che sia risolvibile tramite DNS.

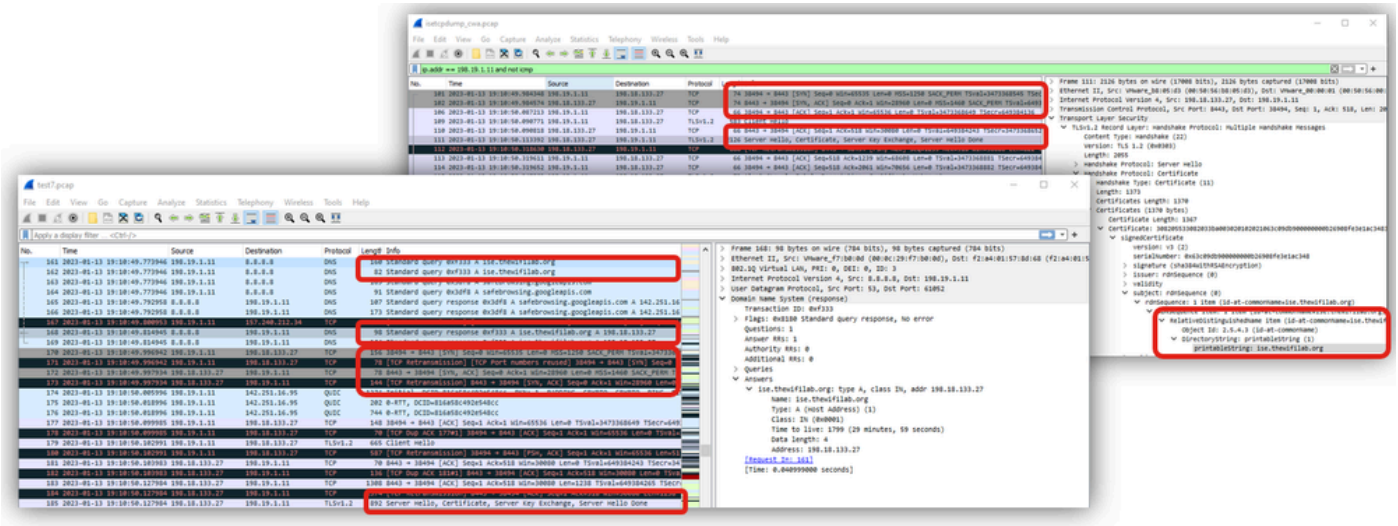
10 - La pagina di accesso non viene ancora caricata?

Verificare con WLC EPC e ISE TCPdump se il traffico del client raggiunge ISE PSN. Configurare e avviare le clip su WLC e ISE:




WLC EPC e ISE TCPDump

Dopo la riproduzione, è possibile raccogliere le immagini acquisite e correlare il traffico. Qui è possibile vedere ISE hostname risolto e la comunicazione tra il client e ISE sulla porta 8443:



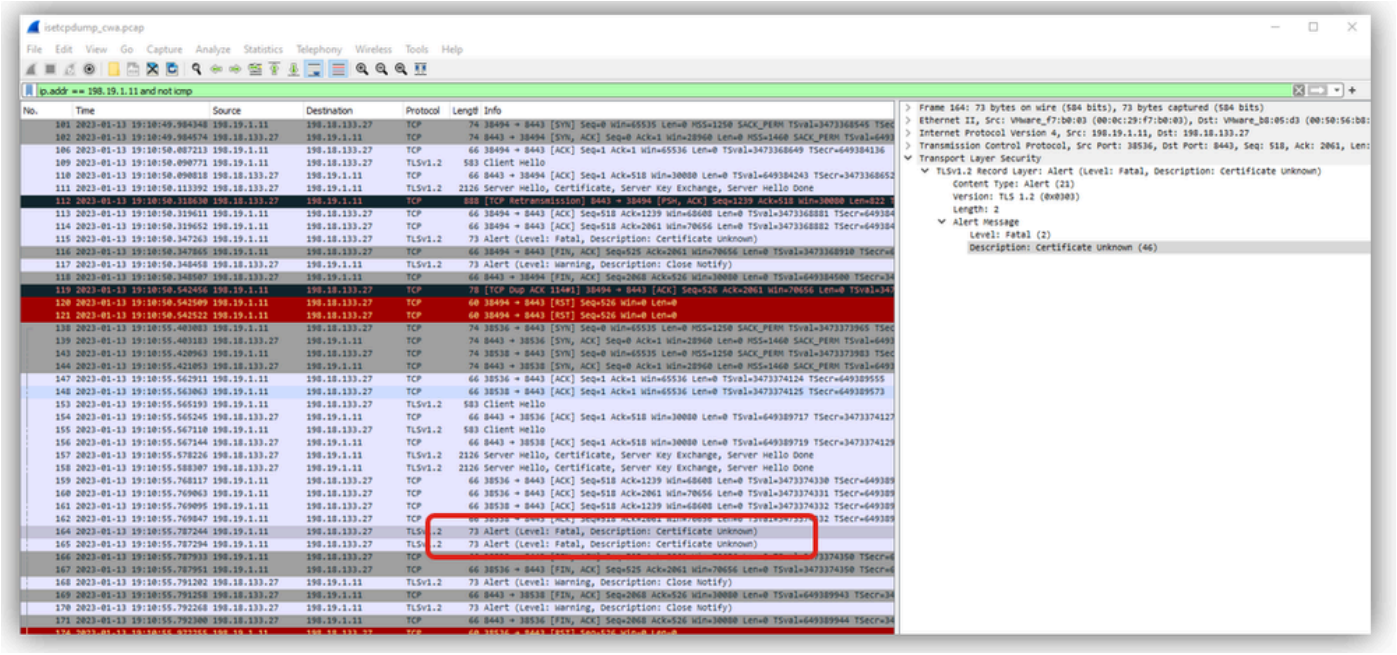
Traffico WLC e ISE

11 - Perché si verificano violazioni della sicurezza dovute al certificato?

Se si utilizza un certificato autofirmato su ISE, è previsto che il client visualizzi un avviso di protezione quando tenta di presentare la pagina di accesso del portale ISE.

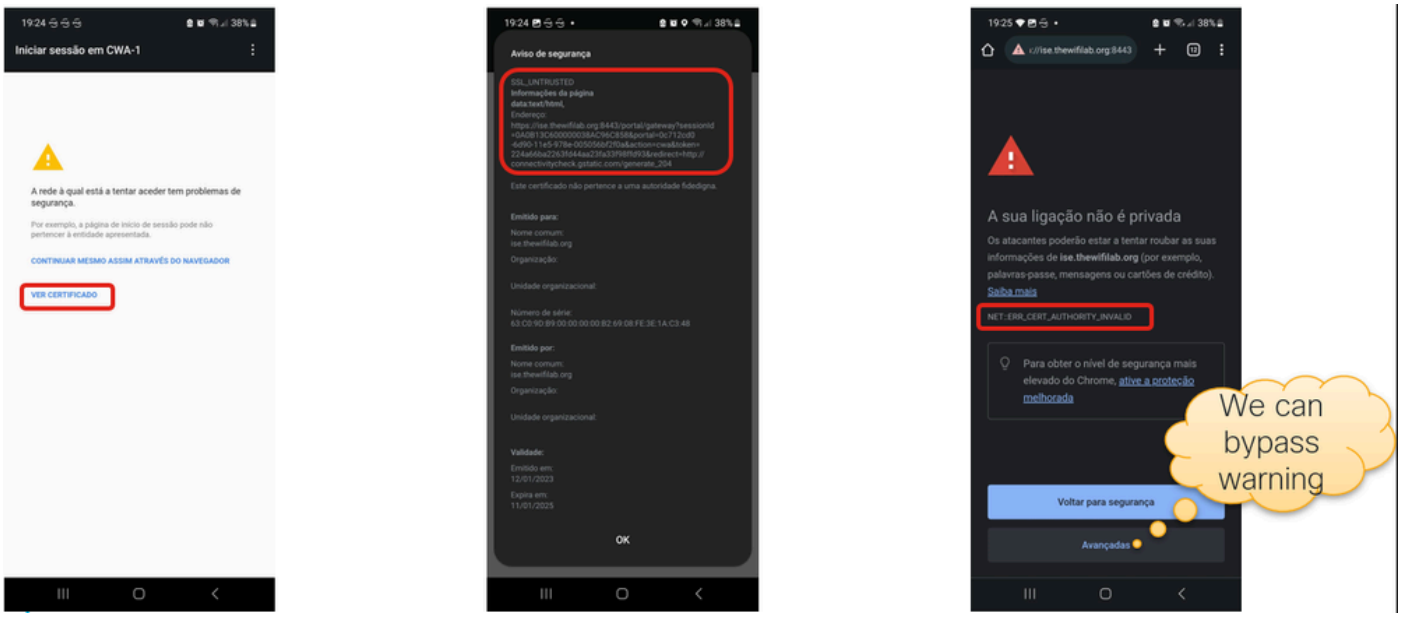
Sul WLC EPC o ISE TCP dump possiamo verificare se il certificato ISE è attendibile.

In questo esempio è possibile vedere la connessione vicina dal client con l'avviso (Livello: Fatal, Descrizione: certificato sconosciuto), ovvero il certificato ISE non è noto (attendibile):



certificato ISE non attendibile

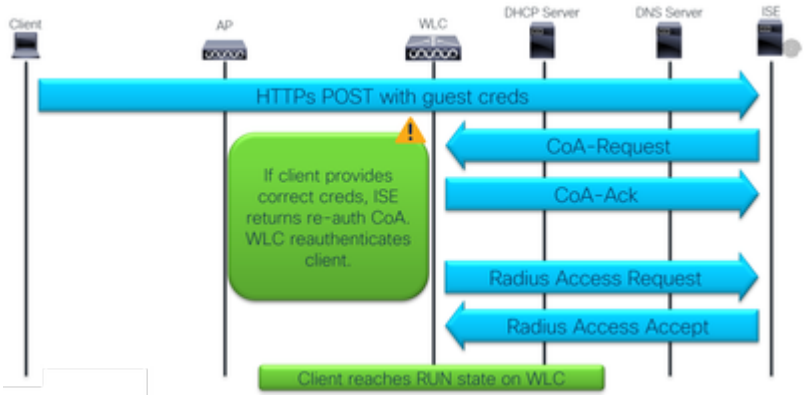
Se si controlla il lato client, vengono riportati i seguenti esempi:




Dispositivo client non attendibile con certificato ISE

Finalmente il reindirizzamento sta funzionando. Ma l'accesso non riesce...

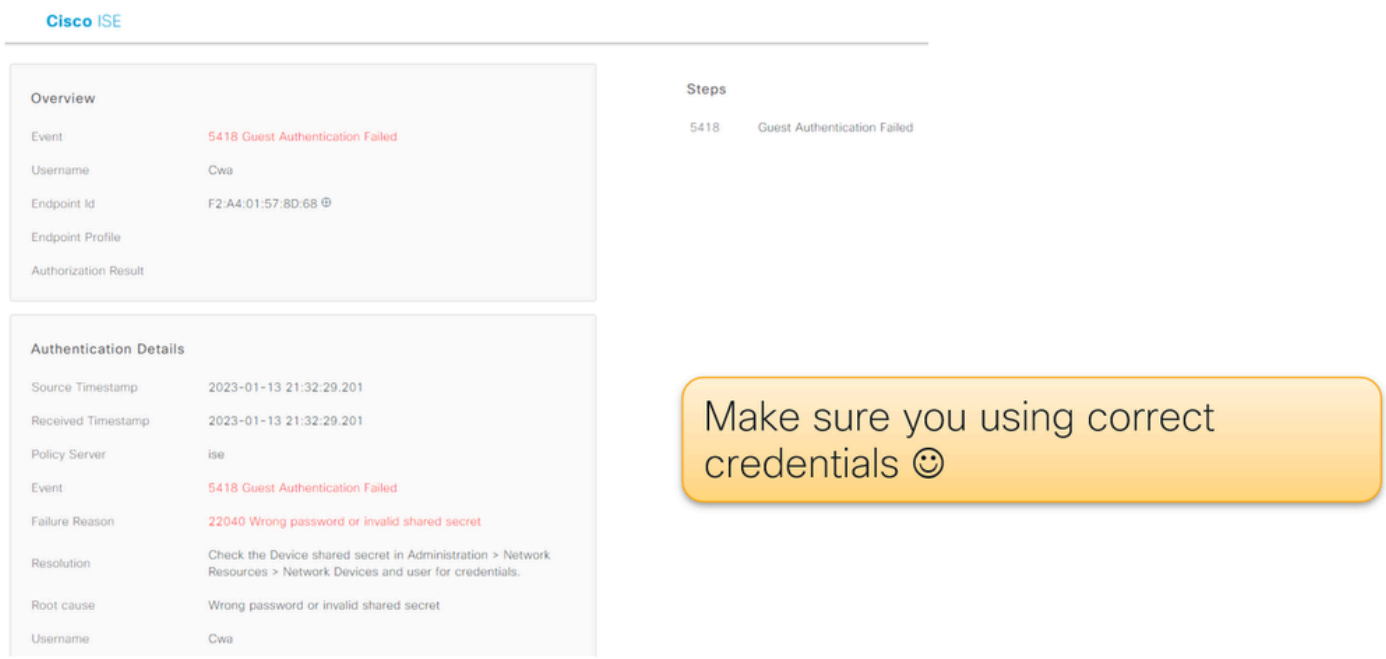
Ultimo controllo del flusso in corso...




Accesso client e CoA

12 - Accesso guest non riuscito?

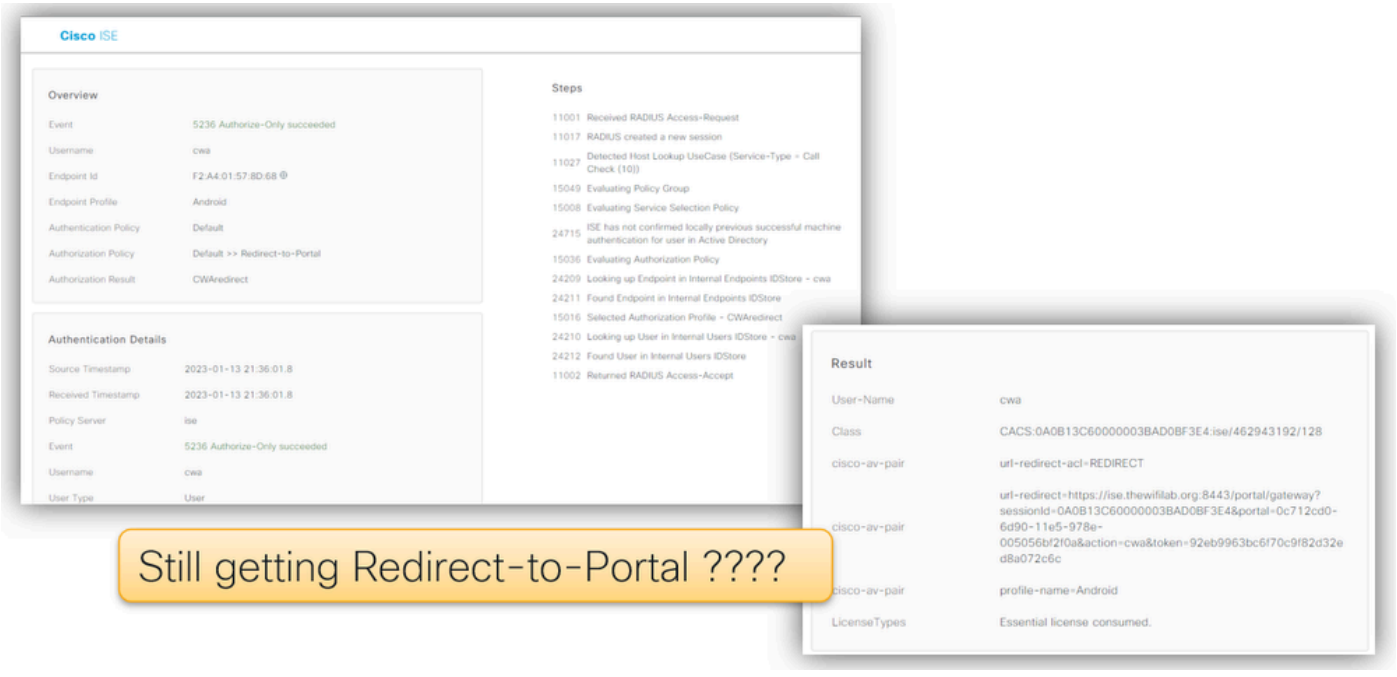
Controllare i registri ISE per verificare se l'autenticazione non è riuscita. Verificare che le credenziali siano corrette.




Autenticazione guest non riuscita a causa di credenziali errate

13 - L'accesso ha esito positivo ma non viene eseguito il passaggio a RUN?

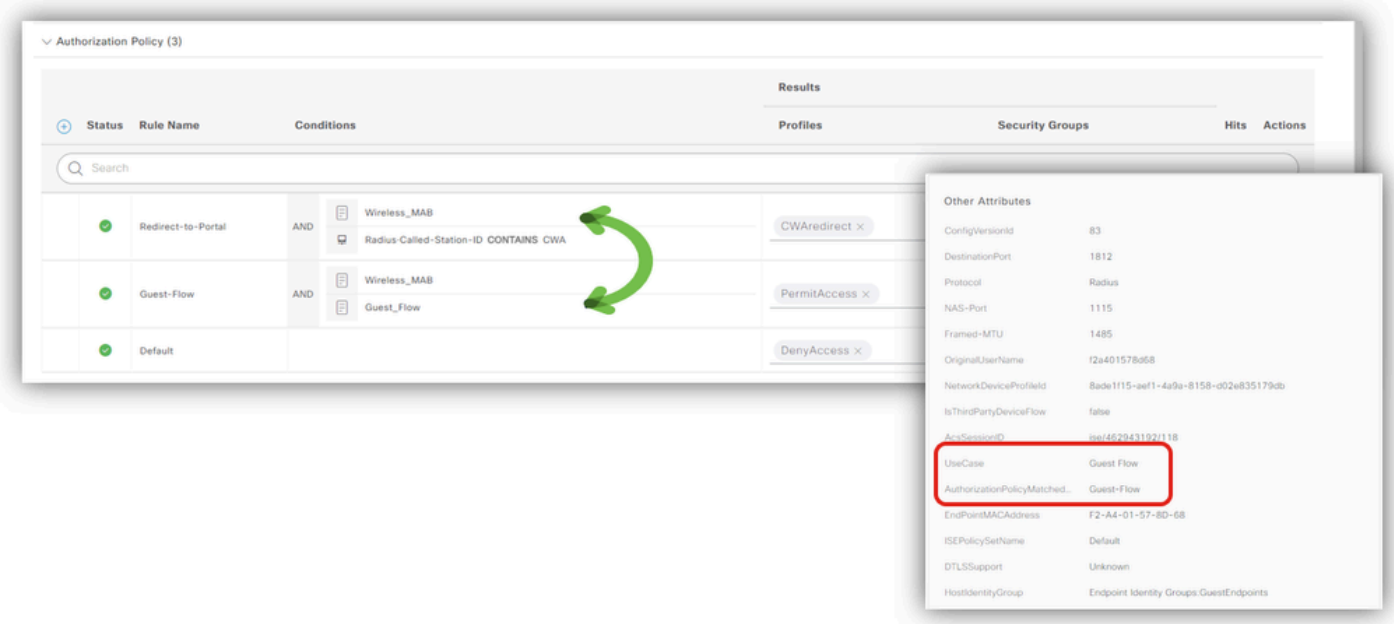
Per i dettagli e i risultati dell'autenticazione, controllare i log ISE:




Ciclo di reindirizzamento

Nell'esempio, il client riceve nuovamente il profilo di autorizzazione contenente l'URL di reindirizzamento e l'ACL di reindirizzamento. Il risultato è un ciclo di reindirizzamento.

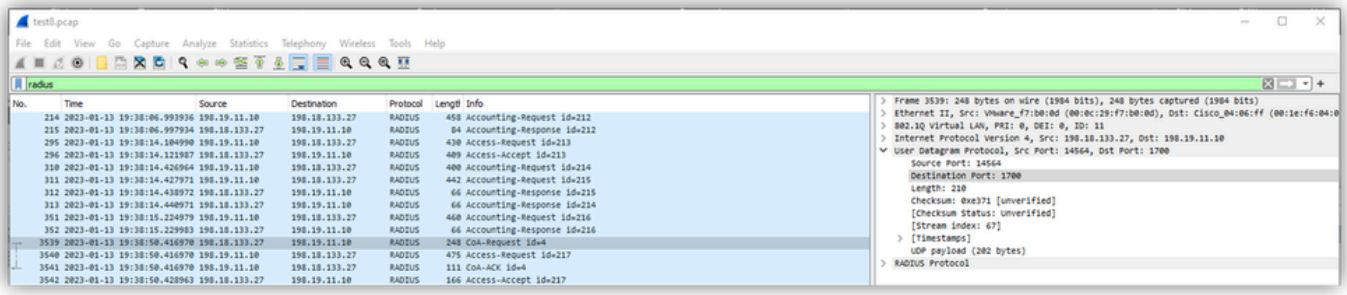
Controllare il set di criteri. Il controllo delle regole Guest_Flow deve essere eseguito prima del reindirizzamento:




Regola Guest_Flow

14 - Il Cacao fallisce?

Con EPC e ISE TCPDump è possibile verificare il traffico CoA. Verificare se la porta CoA (1700) è aperta tra WLC e ISE. Assicurarsi che la chiave privata condivisa corrisponda.




Traffico CoA

---

Nota: Nella versione 17.4.X e successive, assicurarsi di configurare anche la chiave del server CoA quando si configura il server RADIUS. Utilizzare la stessa chiave del segreto condiviso (per impostazione predefinita, sono le stesse in ISE). Lo scopo è quello di configurare facoltativamente una chiave diversa per il certificato di autenticità (CoA) rispetto al segreto condiviso, se questo è ciò che è stato configurato dal server RADIUS. In Cisco IOS® XE 17.3, l'interfaccia utente Web ha semplicemente utilizzato lo stesso segreto condiviso della chiave CoA.

---

A partire dalla versione 17.6.1, questa porta supporta RADIUS (incluso CoA). Se si desidera utilizzare la porta di servizio per RADIUS, è necessaria la configurazione seguente:

<#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
```

# Conclusioni

Questa è la lista di controllo di CWA ripristinata:

- Verificare che il client si trovi sulla VLAN corretta e ottenga l'indirizzo IP e il DNS.

    - Ottieni i dettagli del client sul WLC ed esegui le acquisizioni dei pacchetti per vedere lo scambio DHCP.
- Verificare che il client sia in grado di risolvere i nomi host tramite DNS.
    - Eseguire il ping del nome host dal comando.
- Il WLC deve essere in ascolto sulla porta 80
    - Verificare il comando globale ip http server o il comando webauth-http-enable della mappa dei parametri globali.
- Per eliminare l'avviso del certificato, installare il certificato attendibile in ISE.
    - Non è necessario installare un certificato attendibile su WLC in CWA.
- Criteri di autenticazione all'opzione avanzata ISE "Continua" se l'utente non viene trovato
    - Per consentire agli utenti guest sponsorizzati di connettersi e ottenere URL Redirect e ACL.

Gli strumenti principali utilizzati per la risoluzione dei problemi sono:

- EPC WLC
    - Filtri interni: Protocollo DHCP, indirizzo MAC.
- Monitor WLC
    - Verificare i dettagli di protezione del client.
- Traccia WLC RA
    - Debug con informazioni dettagliate sul lato WLC.
- log ISE in tempo reale
    - Dettagli autenticazione.
- IPT ISE
    - Raccogli le clip dei pacchetti sull'interfaccia PSN ISE.

# Riferimenti

Configurazione dell'autenticazione Web centrale (CWA) su Catalyst 9800 WLC e ISE

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).