

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

Sommario

[Introduzione](#)

[Informazioni sullo sfondo](#)

[Flusso dettagliato](#)

[Risoluzione dei problemi](#)

[Sintomo comune: L'utente non viene reindirizzato alla pagina di accesso.](#)

- [1 - La prima autenticazione RADIUS è riuscita?](#)
- [2 - Il WLC riceve l'URL di reindirizzamento e l'ACL?](#)
- [3 - L'ACL di reindirizzamento è corretto?](#)
- [4 - Il client viene spostato in Web-Auth in sospeso?](#)
- [5 - Il WLC consente il traffico DHCP e DNS?](#)
- [6 - Il server DHCP riceve una richiesta/individuazione DHCP?](#)
- [7 - Viene eseguito il reindirizzamento automatico?](#)
- [8 - Il browser non visualizza la pagina di accesso?](#)
- [9 - Il client è in grado di risolvere il problema relativo al nome host ISE?](#)
- [10 - La pagina di accesso non viene ancora caricata?](#)
- [11 - Perché si verificano violazioni della sicurezza dovute al certificato?](#)
- [12 - Accesso guest non riuscito?](#)
- [13 - L'accesso ha esito positivo ma non viene eseguito il passaggio a RUN?](#)
- [14 - Il Cacao fallisce?](#)

[Conclusioni](#)

[Riferimenti](#)

Introduzione

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

Informazioni sullo sfondo

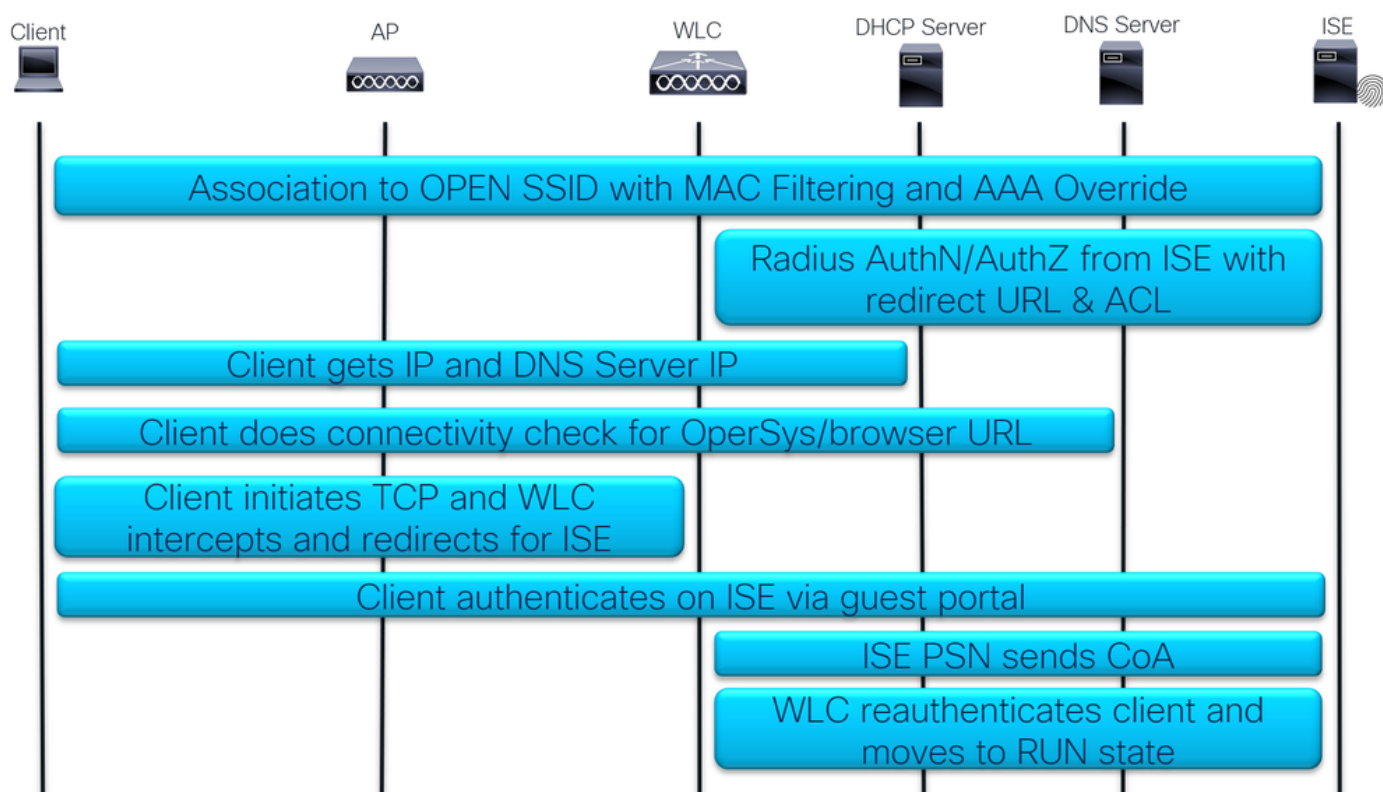
Al momento sono presenti così tante periferiche personali che gli amministratori di rete che cercano di proteggere l'accesso wireless normalmente optano per le reti wireless che utilizzano CWA.

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.

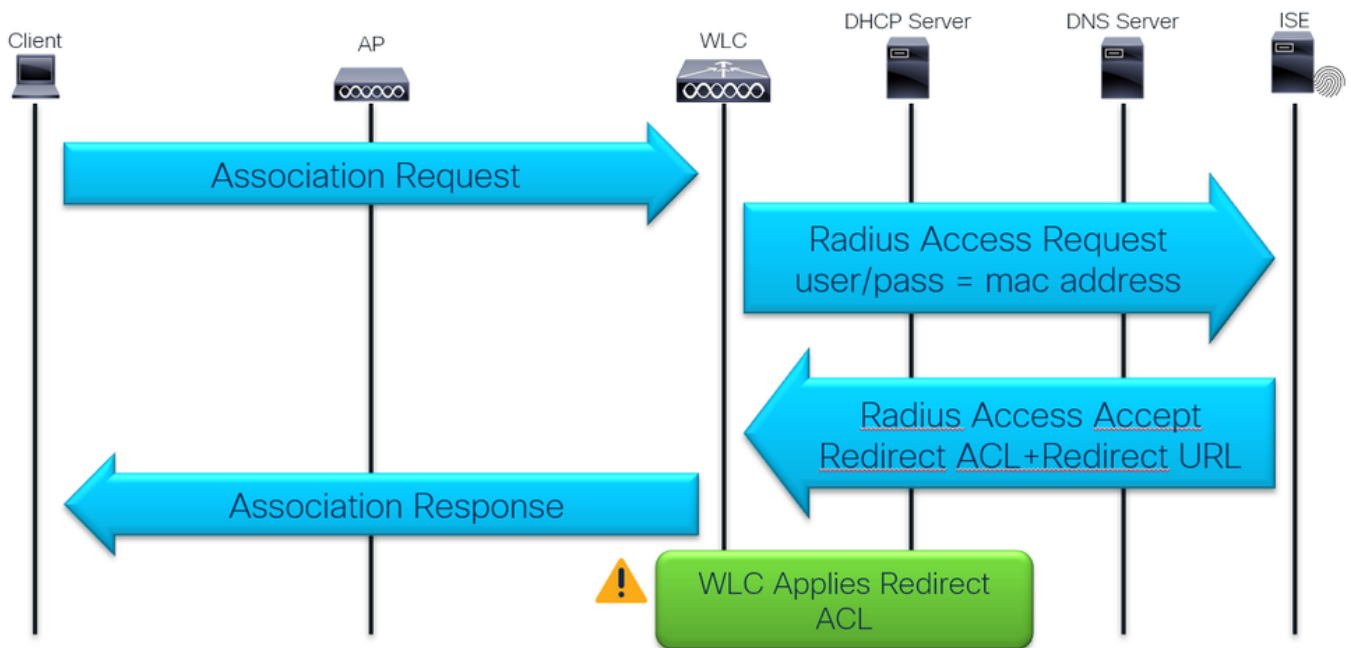
Di seguito è riportato il flusso del pacchetto CWA:



Flusso pacchetti CWA

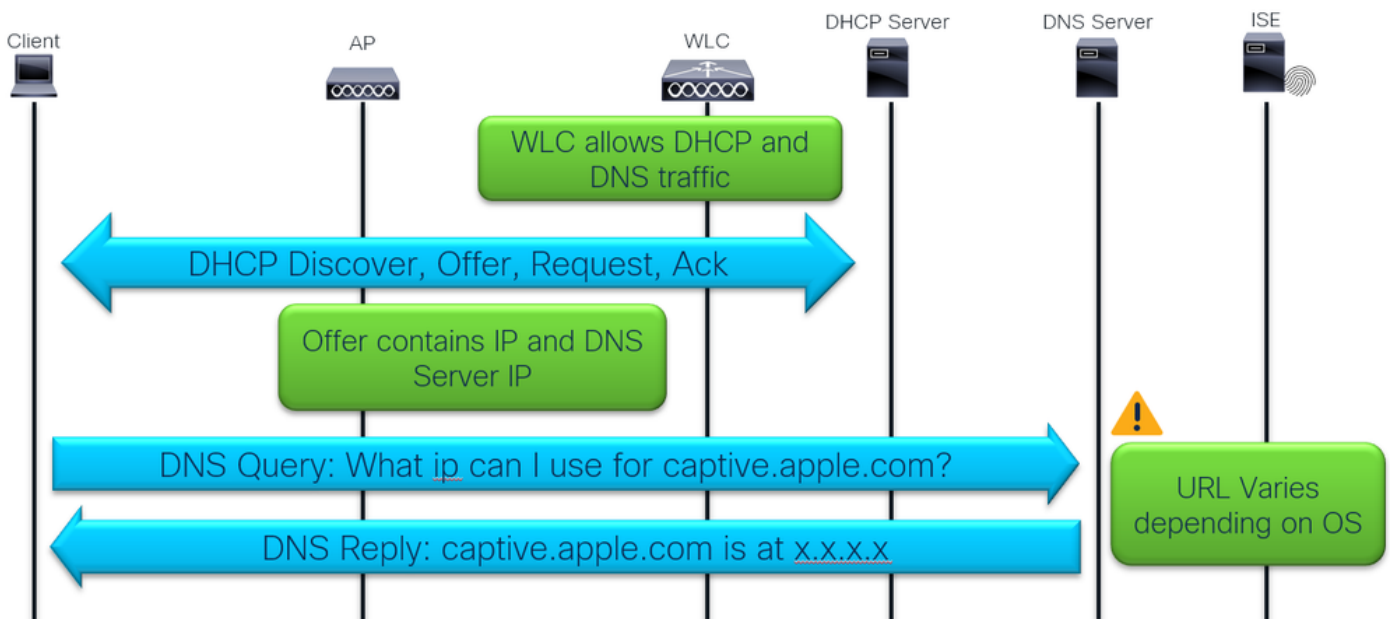
Flusso dettagliato

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.

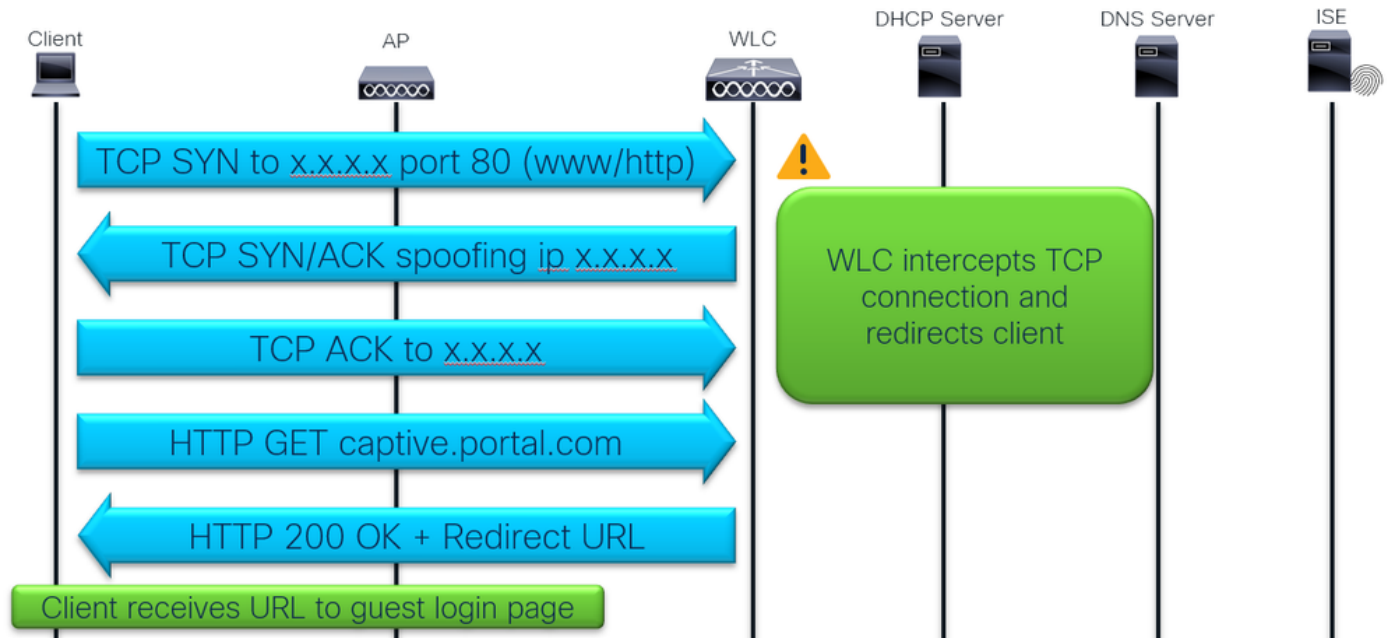
Esistono sistemi operativi dei dispositivi preprogrammati per eseguire HTTP GET verso un dominio specifico

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

I browser eseguono inoltre questo controllo all'apertura:

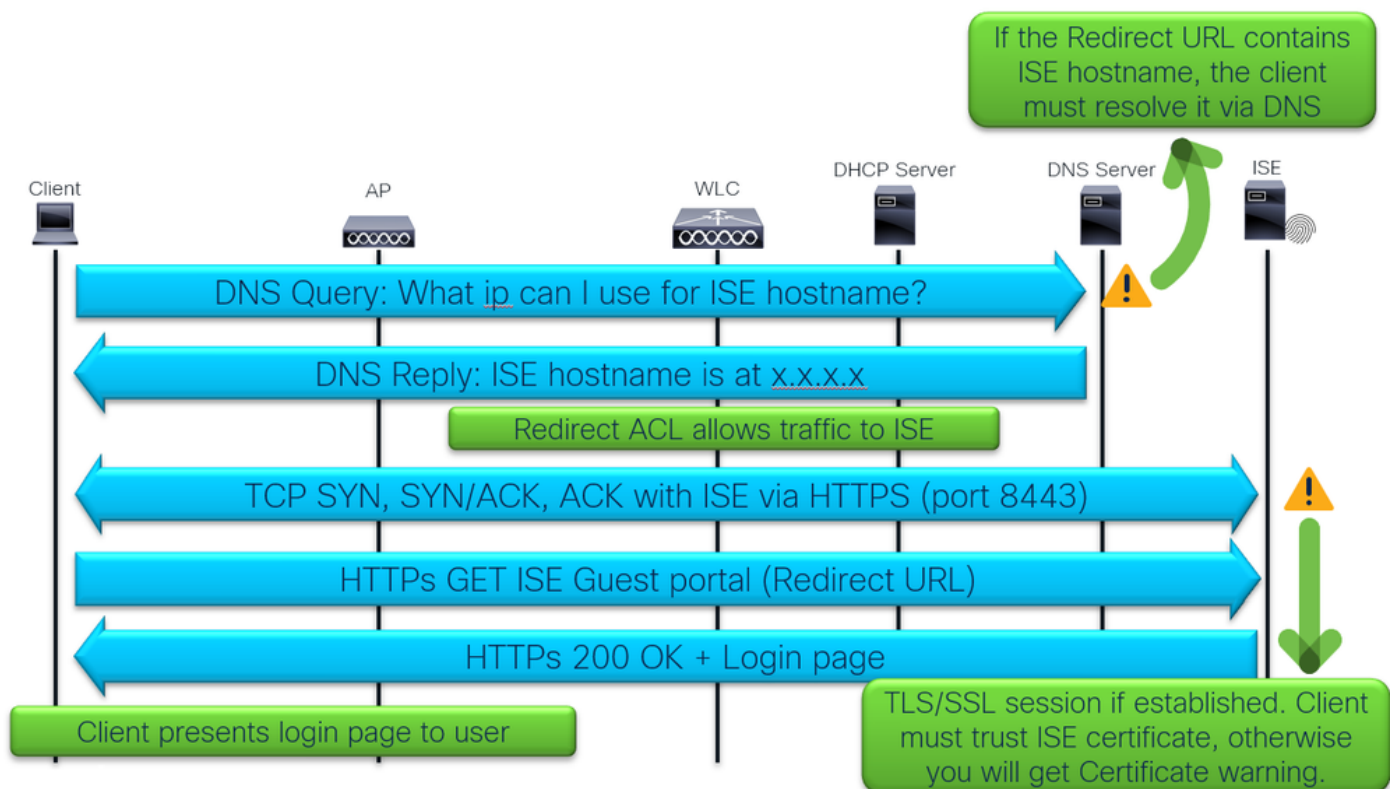
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Intercettazione e reindirizzamento del traffico:



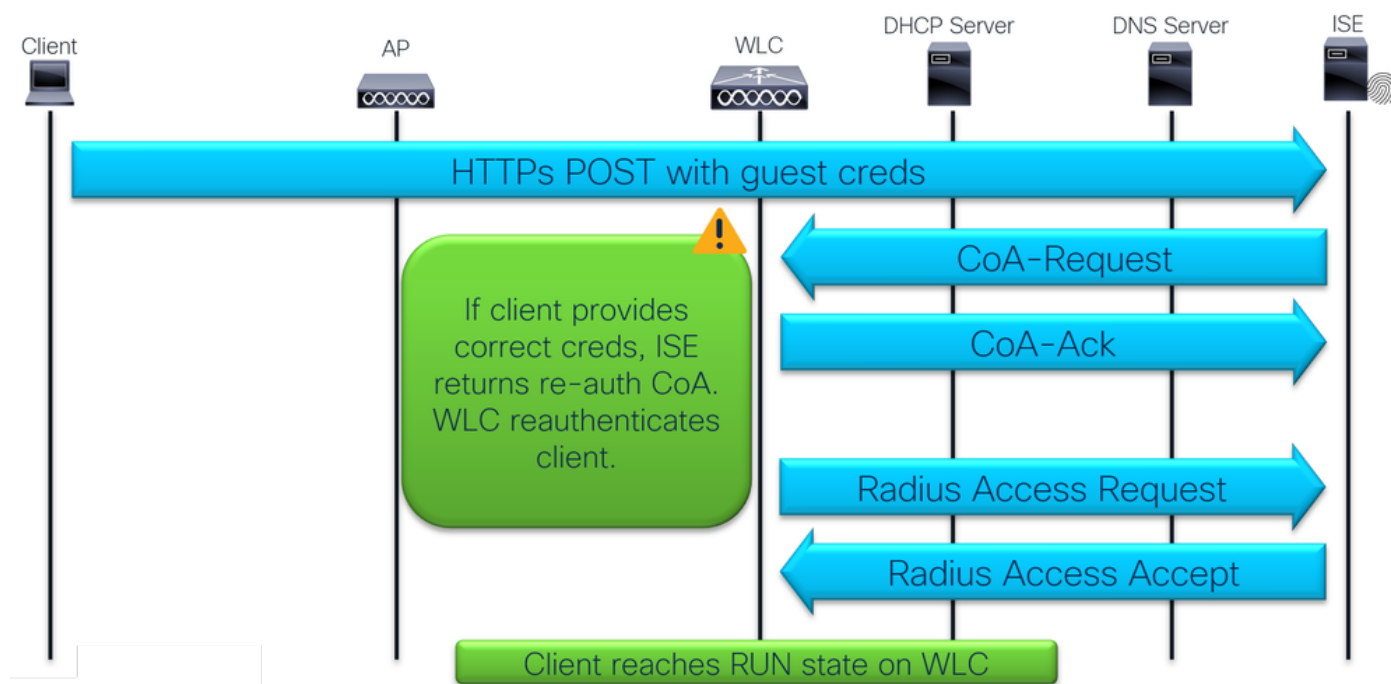
Intercettazione e reindirizzamento del traffico

Accesso client al portale di accesso guest ISE:



Accesso client al portale di accesso guest ISE

Accesso client e CoA:

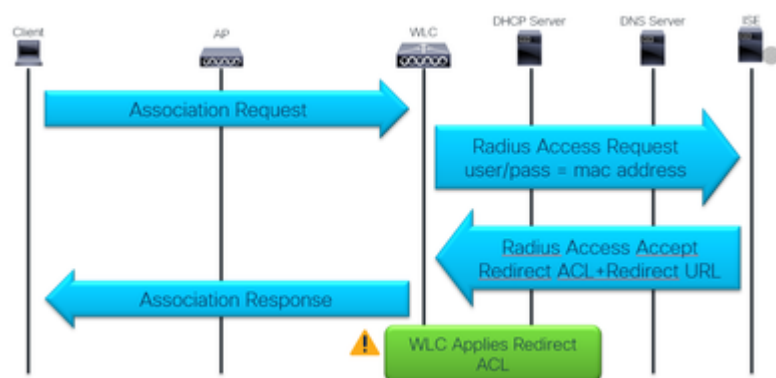


Accesso client e CoA

Risoluzione dei problemi

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

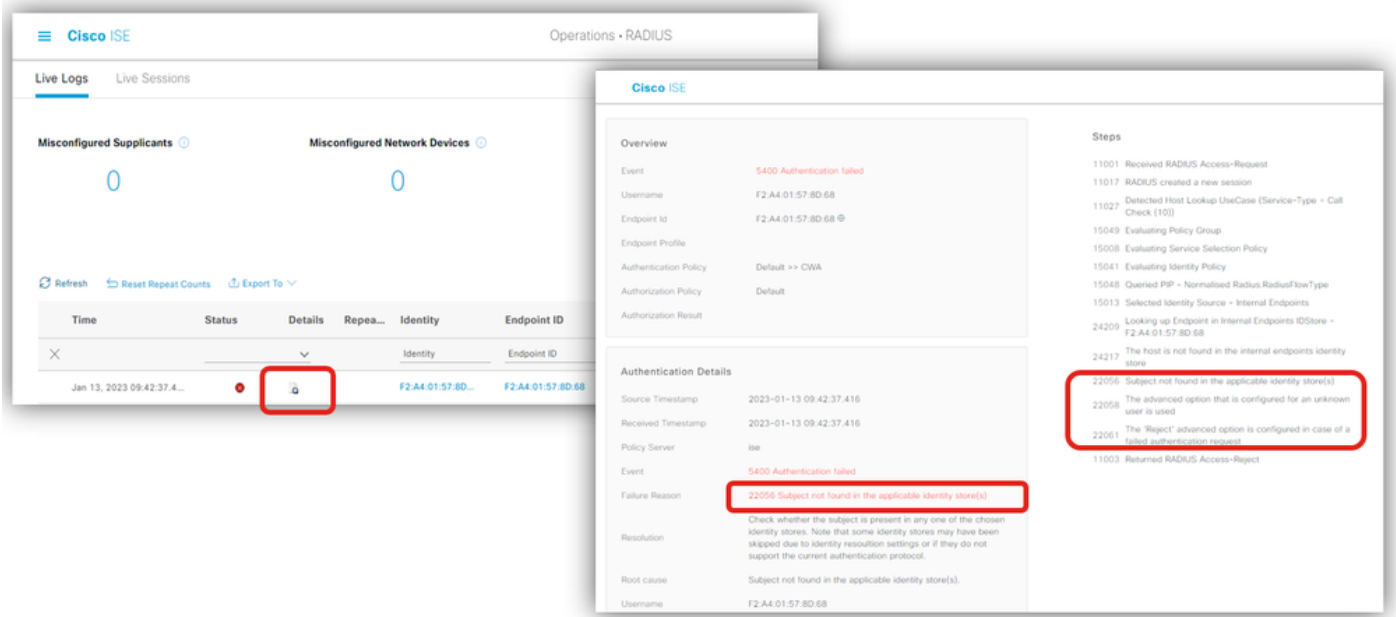
Cominciamo con la prima parte del flusso:



Prima associazione e autenticazione RADIUS

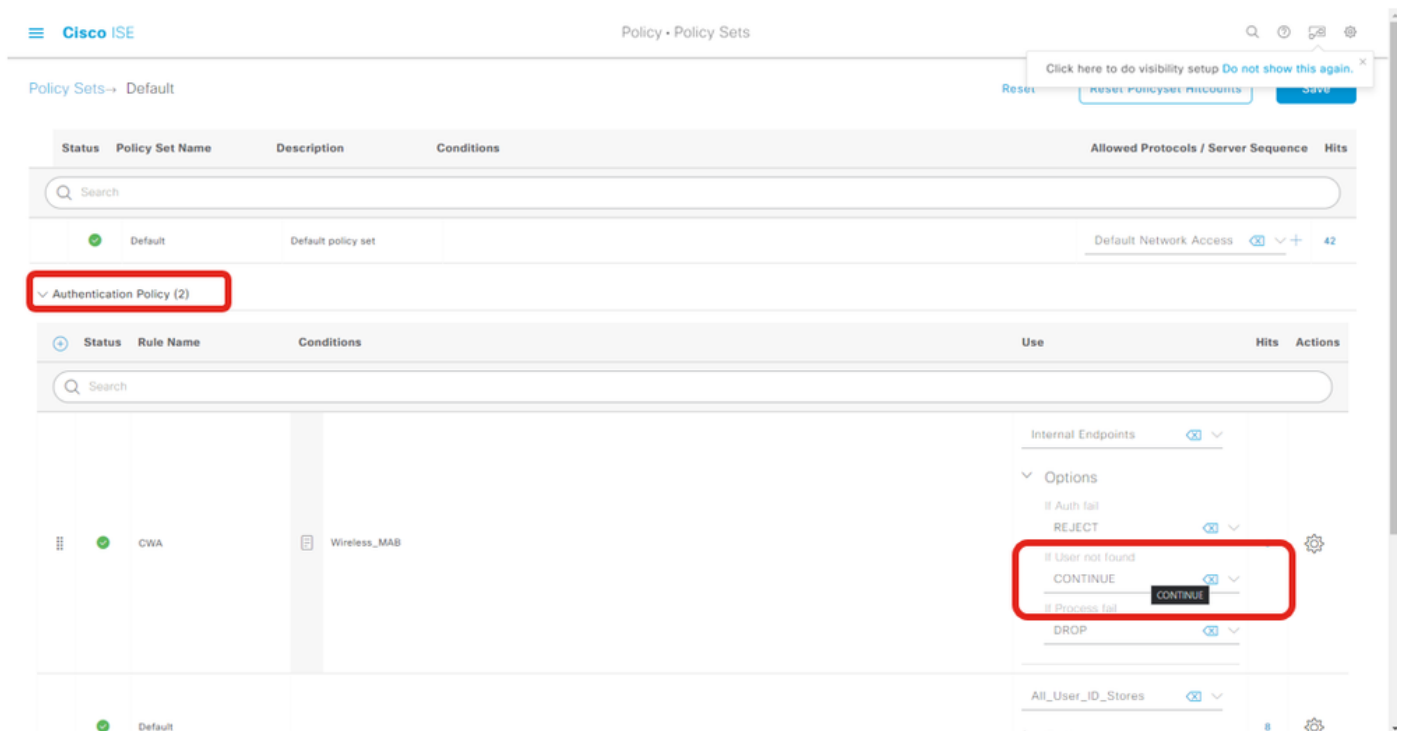
1 - La prima autenticazione RADIUS è riuscita?

Verificare il risultato dell'autenticazione del filtro MAC:



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

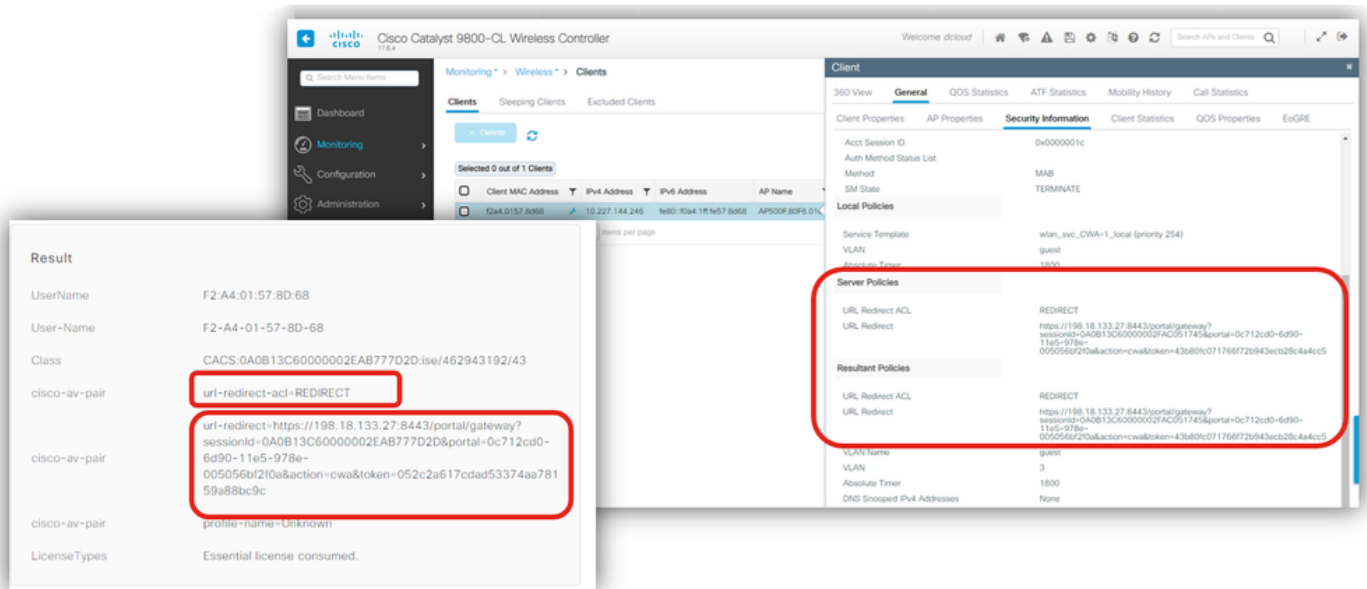
Assicurarsi che l'opzione avanzata per l'autenticazione sia impostata su "Continua" se l'utente non viene trovato:



Opzione avanzata utente non trovato

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

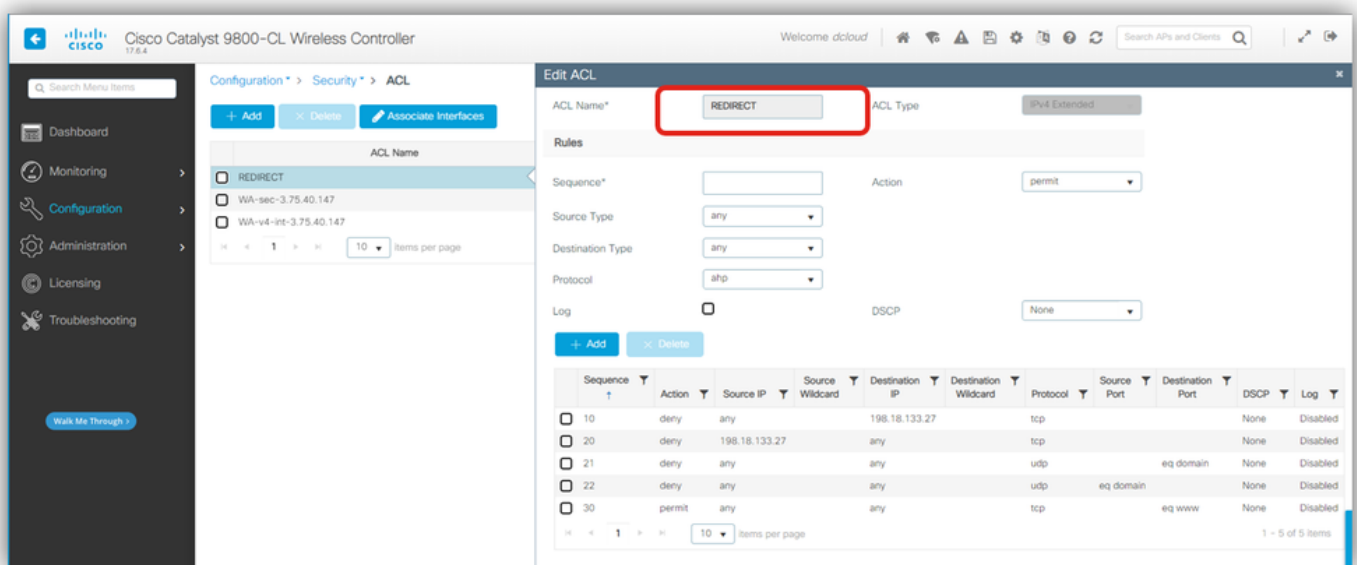
Controllare i log ISE in tempo reale e le informazioni sulla sicurezza del client WLC in Monitoraggio Verificare che ISE invii l'URL di reindirizzamento e l'ACL nell'Access Accept e che venga ricevuto dal WLC e applicato al client nei dettagli del client:



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:

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
☒

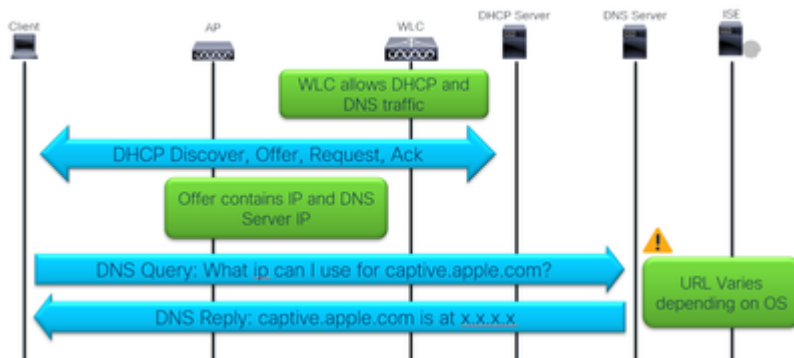
NAC State
☒

NAC Type
RADIUS

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:

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

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:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Packet Capture' section is active, displaying a list of captured packets. A red box highlights the 'Edit Packet Capture' settings, showing 'Capture Name' as 'test', 'Filter' as 'any', 'Monitor Control Plane' as 'Yes', 'Inner Filter Protocol' as 'DHCP', and 'Inner Filter MAC' as 'f2a4.0157.8d58'. A blue cloud callout says 'Inner filters !!'. Another red box highlights the packet details for a DHCP Discover packet, showing it is sent as broadcast on VLAN 3. An orange cloud callout says 'Sent as broadcast on VLAN 3'.

EPC WLC per verificare DHCP

Confermare la VLAN client prevista nel profilo dei criteri:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Policy' section is active, displaying a list of policy profiles. The 'Edit Policy Profile' window is open, showing the 'Access Policies' tab. The 'VLAN' section is highlighted with a red box, showing 'VLAN/VLAN Group' set to 'guest' and 'Multicast VLAN' set to 'Enter Multicast VLAN'.

VLAN nel profilo dei criteri

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

```
WLC1#show vlan

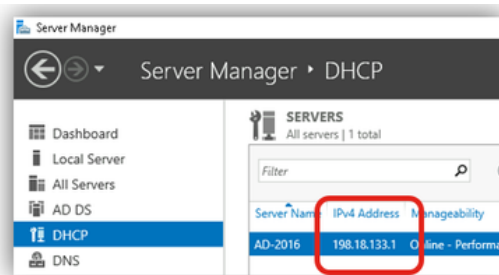
VLAN Name                Status    Ports
-----
1    default                active    Gi2, Gi3
2    employee               active
3    guest                  active
11   mgmt                    active

WLC1#show ip int br

Interface      IP-Address      OK? Method Status    Protocol
GigabitEthernet1  unassigned      YES unset  up        up
GigabitEthernet2  unassigned      YES unset  administratively down down
GigabitEthernet3  unassigned      YES unset  administratively down down
Vlan1          unassigned      YES NVRAM  up        up
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, 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.

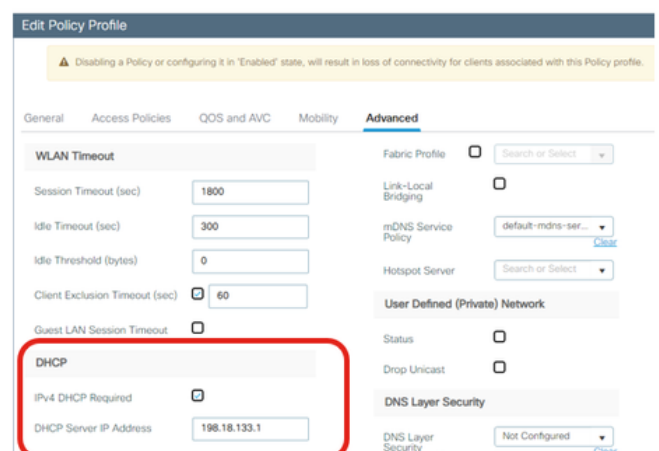
Le best practice richiedono che la SVI per le subnet client sia configurata nell'infrastruttura cablata ed evita che avvenga sul WLC.

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:

```
WLC1#show run int vlan 3
Building configuration...

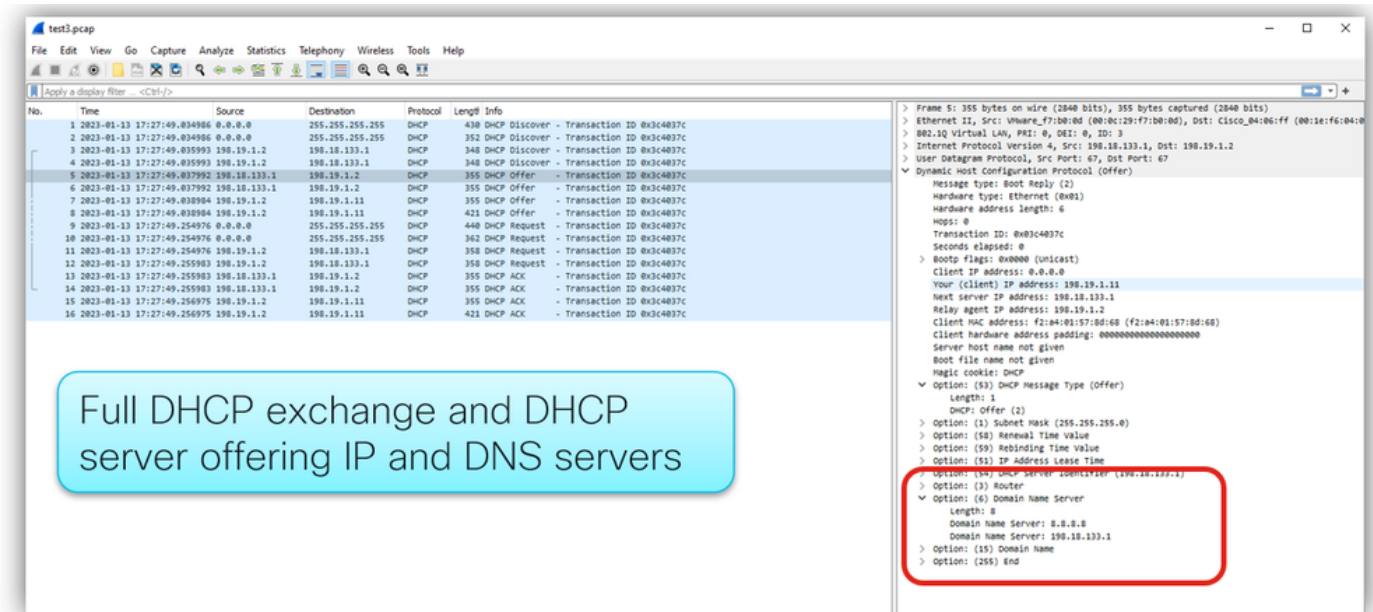
Current configuration : 141 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 ip helper-address 198.18.133.1
 no mop enabled
 no mop sysid
end
```



SVI can be at the WLC itself or in the Wired network

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:



Full DHCP exchange and DHCP server offering IP and DNS servers

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:

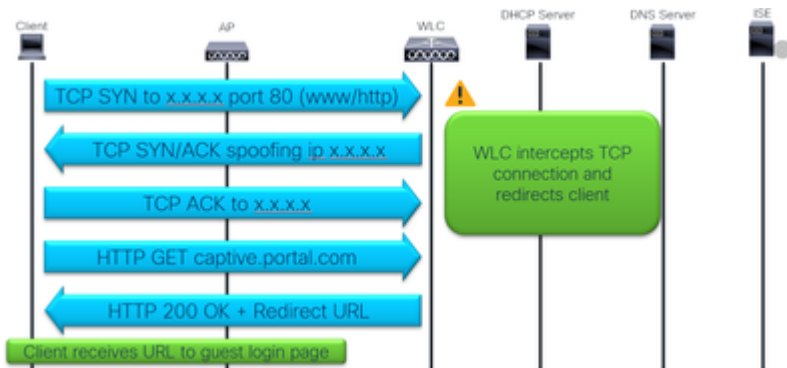


Query e risposte DNS

- 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?

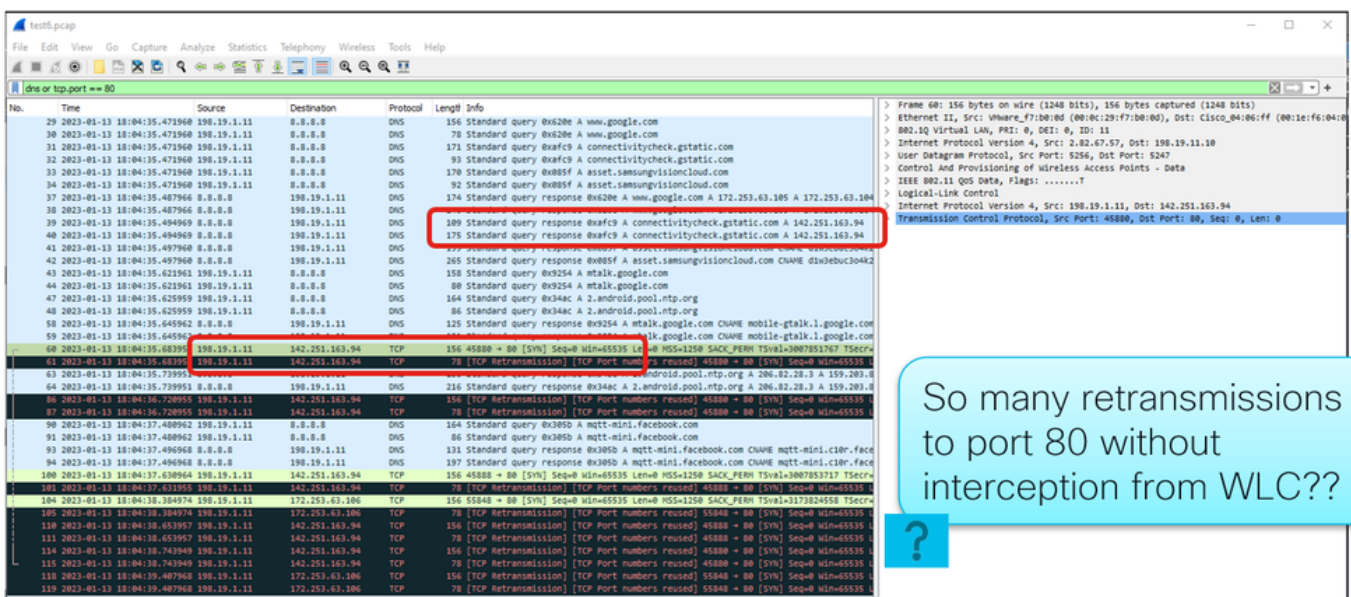
Rivediamo il flusso...



Intercettazione e reindirizzamento del traffico

8 - Il browser non visualizza la pagina di accesso?

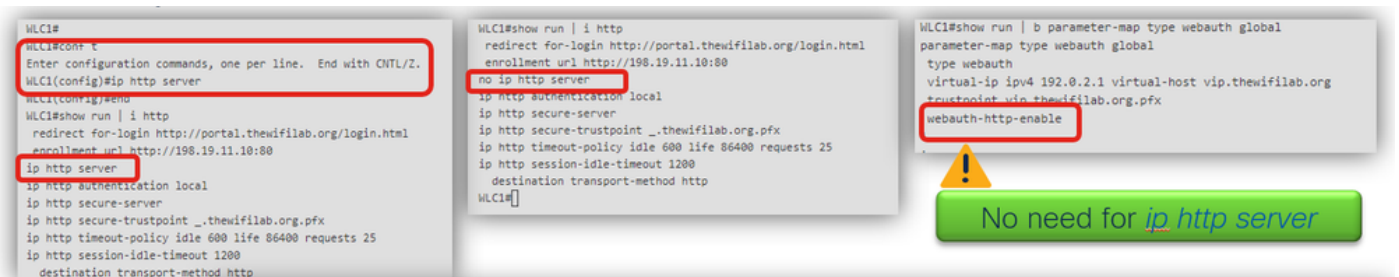
Verificare se il client invia il comando TCP SYN alla porta 80 e se il WLC lo intercetta:



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.

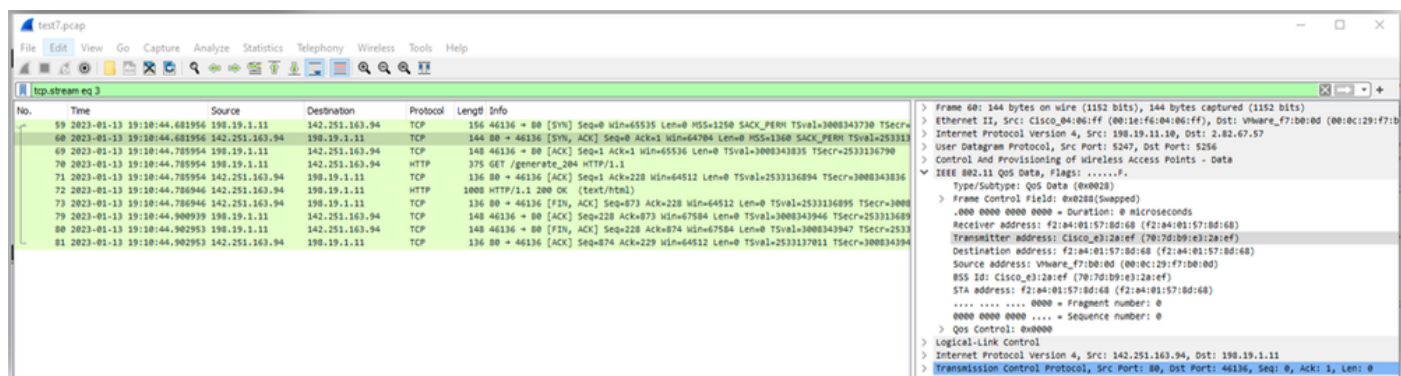
Verificare che il comando ip http server sia nella configurazione globale o webauth-http-enable nella mappa dei parametri globale:



comandi di intercettazione http

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

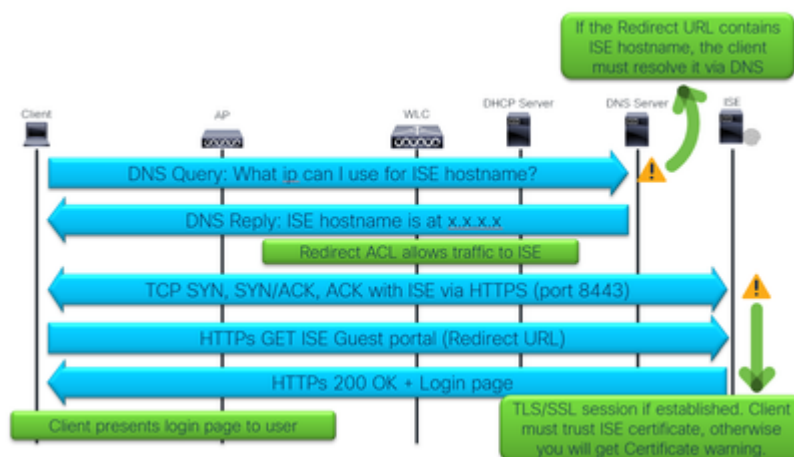
per rispondere al client e reindirizzarlo.



Intercettazione TCP da parte del WLC

Ancora non funziona?

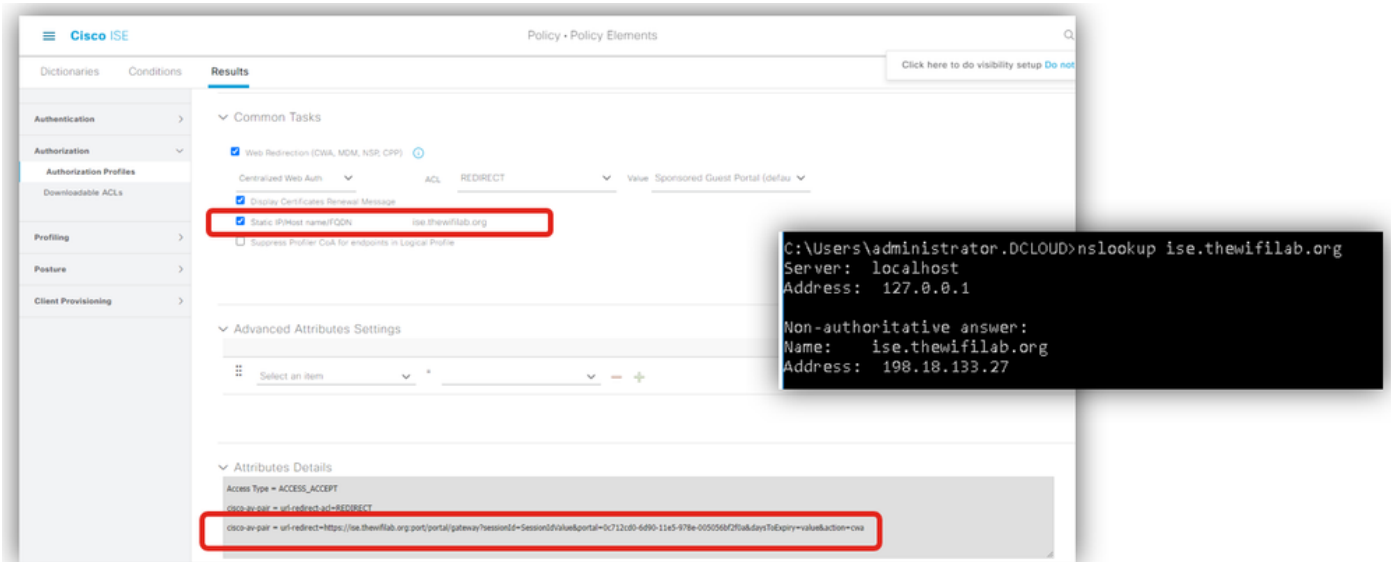
C'è altro nel flusso...



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:

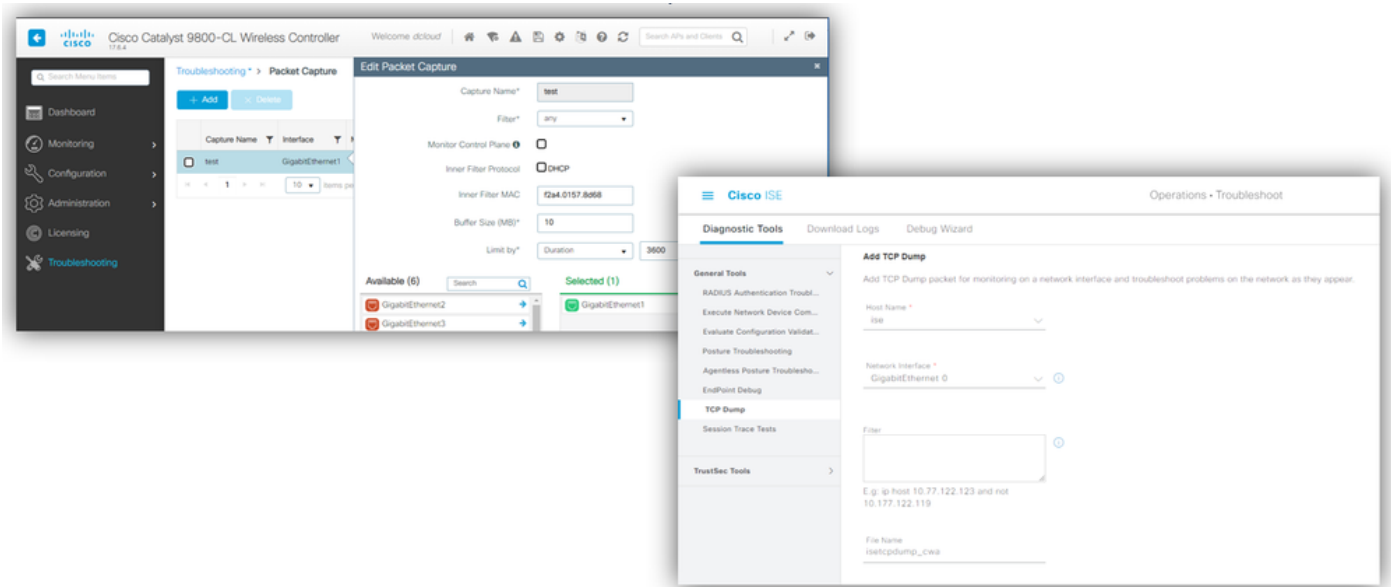


Risoluzione ISE Hostname

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.

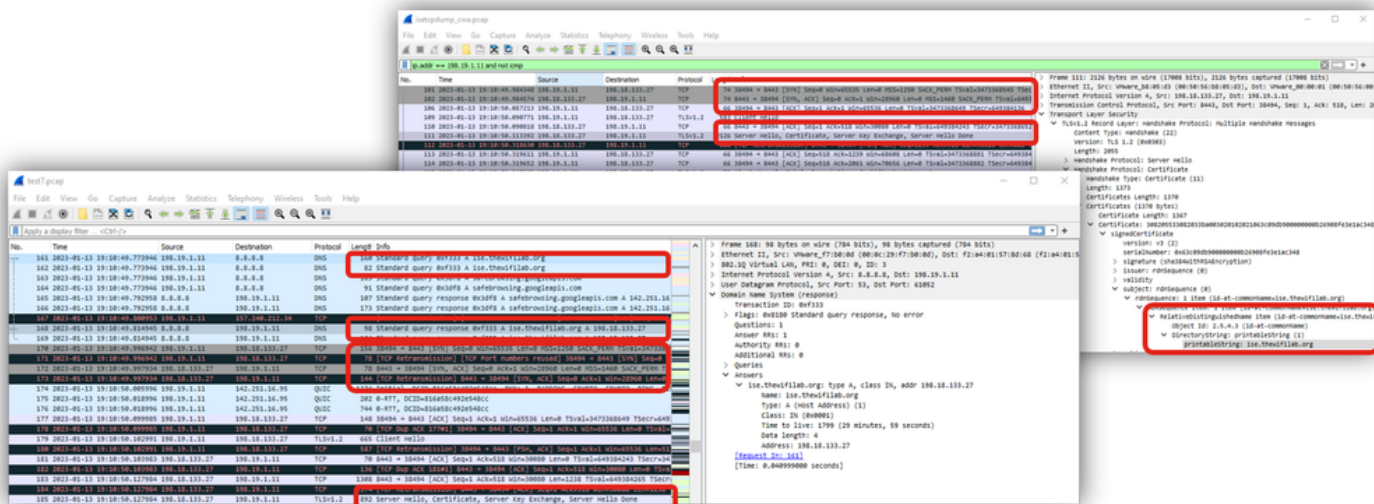
10 - La pagina di accesso non viene ancora caricata?

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:



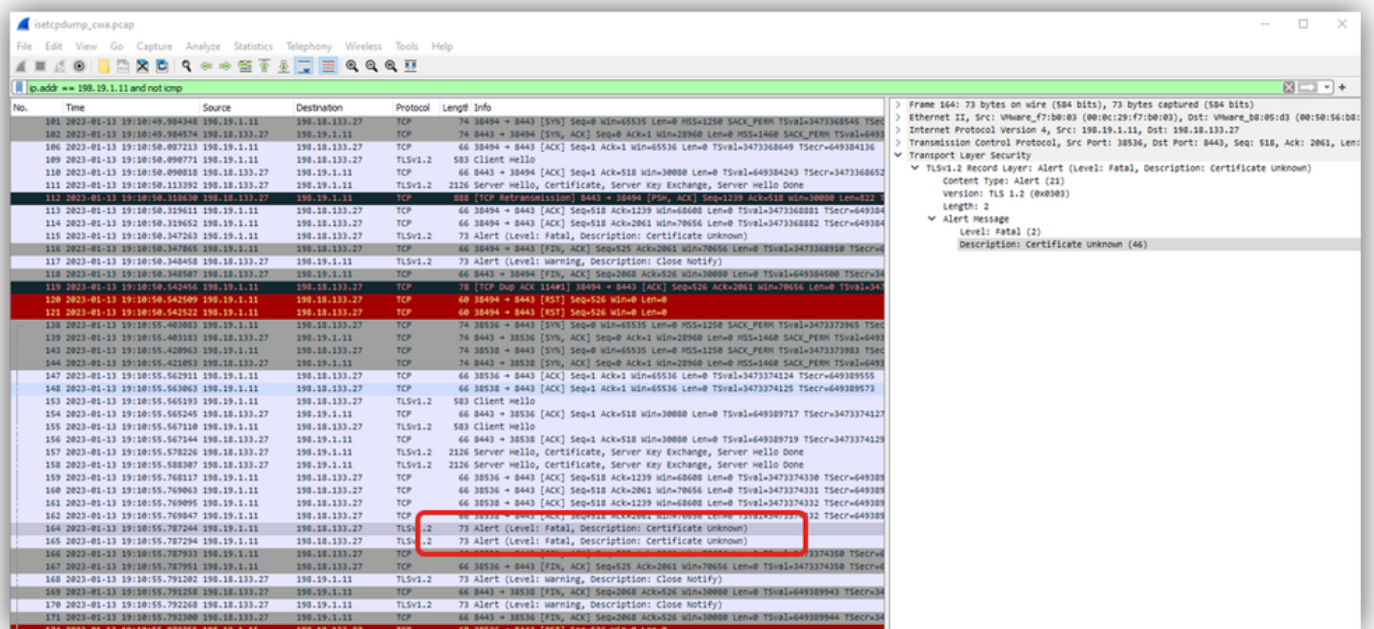
Traffico WLC e ISE

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.

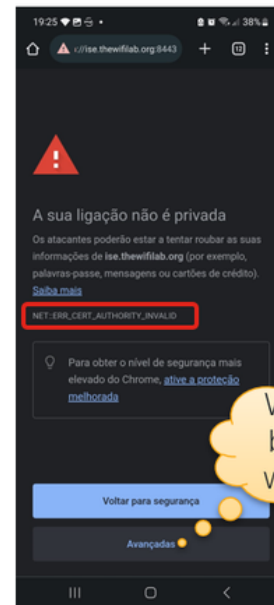
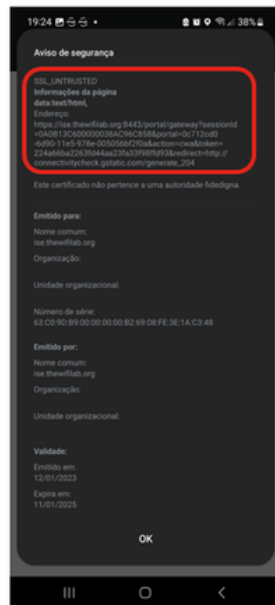
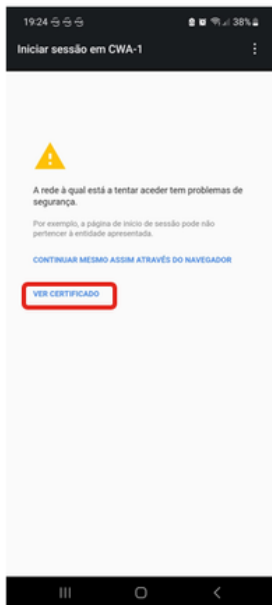
Sul WLC EPC o ISE TCP dump possiamo verificare se il certificato ISE è attendibile.

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

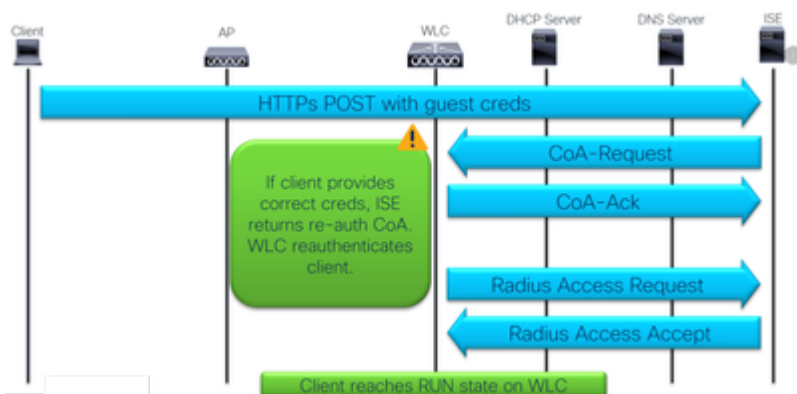
Se si controlla il lato client, vengono riportati i seguenti esempi:



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.

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 😊

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:

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-acl=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 ????

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.

No.	Time	Source	Destination	Protocol	Length	Info
214	2023-01-13 19:38:06.993936	190.18.133.27	190.18.133.27	RADIUS	458	Accounting-Request id=212
215	2023-01-13 19:38:06.997934	190.18.133.27	190.18.133.27	RADIUS	84	Accounting-Response id=212
295	2023-01-13 19:38:14.184990	190.18.133.27	190.18.133.27	RADIUS	430	Access-Request id=213
296	2023-01-13 19:38:14.321987	190.18.133.27	190.18.133.27	RADIUS	489	Access-Accept id=213
310	2023-01-13 19:38:14.420964	190.18.133.27	190.18.133.27	RADIUS	480	Accounting-Request id=214
311	2023-01-13 19:38:14.427971	190.18.133.27	190.18.133.27	RADIUS	442	Accounting-Request id=215
312	2023-01-13 19:38:14.438972	190.18.133.27	190.18.133.27	RADIUS	66	Accounting-Response id=215
313	2023-01-13 19:38:14.440971	190.18.133.27	190.18.133.27	RADIUS	66	Accounting-Response id=214
351	2023-01-13 19:38:15.224979	190.18.133.27	190.18.133.27	RADIUS	468	Accounting-Request id=216
352	2023-01-13 19:38:15.229983	190.18.133.27	190.18.133.27	RADIUS	66	Accounting-Response id=216
3539	2023-01-13 19:38:16.416970	190.18.133.27	190.18.133.27	RADIUS	248	CoA-Request id=4
3540	2023-01-13 19:38:16.416970	190.18.133.27	190.18.133.27	RADIUS	475	Access-Request id=217
3541	2023-01-13 19:38:16.416970	190.18.133.27	190.18.133.27	RADIUS	111	CoA-ACK id=4
3542	2023-01-13 19:38:16.420963	190.18.133.27	190.18.133.27	RADIUS	166	Access-Accept id=217

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).