

對使用無線Lan控制器(WLC)9800和身分識別服務引擎(ISE)的中央Web驗證(CWA)進行排解疑難

目錄

[簡介](#)

[背景資訊](#)

[詳細流程](#)

[疑難排解](#)

[常見症狀：使用者沒有重新導向至登入頁面。](#)

[1 — 第一個RADIUS身份驗證是否成功？](#)

[2 - WLC收到重新導向URL和ACL？](#)

[3 — 重定向ACL是否正確？](#)

[4 — 是否將使用者端移至Web-Auth Pending？](#)

[5 - WLC是否允許DHCP和DNS流量？](#)

[6 - DHCP伺服器是否接收DHCP發現/請求？](#)

[7 — 是否發生自動重定向？](#)

[8 — 瀏覽器不顯示登入頁面？](#)

[9 — 客戶端是否可以解析ISE主機名？](#)

[10 — 登入頁面仍無法載入？](#)

[11 — 為什麼由於證書導致安全違規？](#)

[12 — 訪客登入失敗？](#)

[13 — 登入成功，但不移至RUN？](#)

[14 - COA失敗？](#)

[結論](#)

[參考資料](#)

簡介

本檔案介紹如何對WLC 9800和ISE的中央Web驗證(CWA)進行疑難排解。

背景資訊

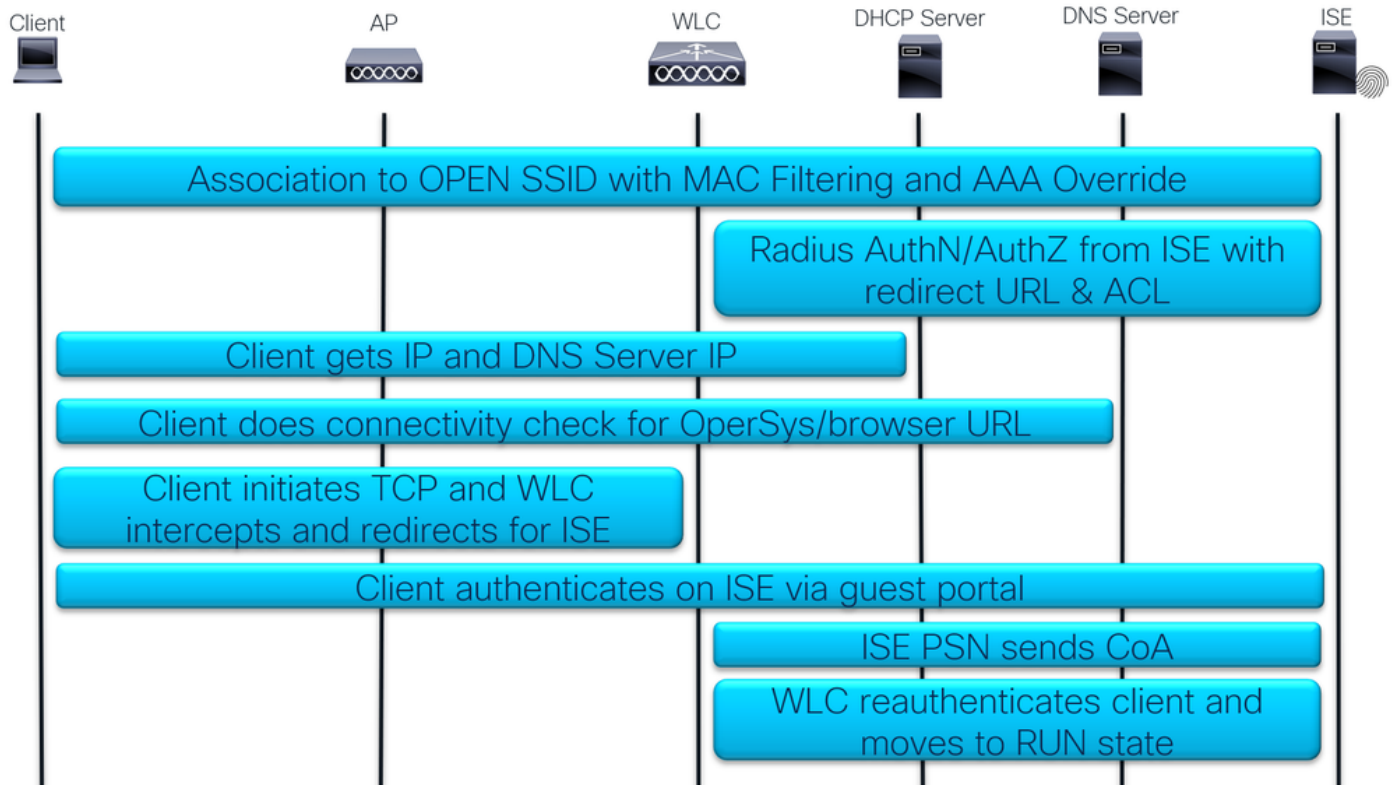
當前存在如此多的個人裝置，以致於尋求保護無線接入的網路管理員通常選擇使用CWA的無線網路。

在本文檔中，我們將重點介紹CWA的流程圖，它有助於排除影響我們的常見問題。

我們將檢視該過程的常見陷阱、如何收集與CWA相關的日誌、如何分析這些日誌，以及如何在WLC上收集嵌入式資料包捕獲以確認流量。

CWA是允許使用者使用個人裝置（也稱為BYOD）連線到公司網路的公司最常見的設定。任何網路管理員都對在開啟TAC案例之前執行修復問題和故障排除步驟感興趣。

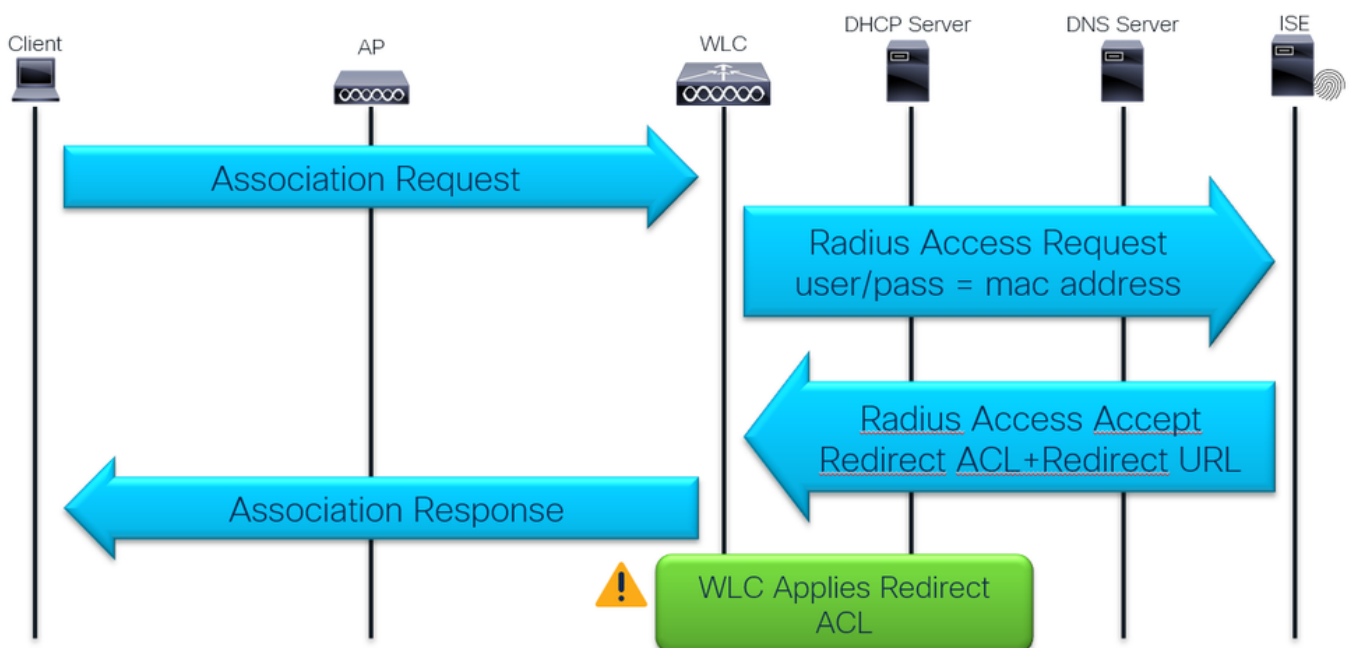
以下是CWA資料包流：



CWA封包流

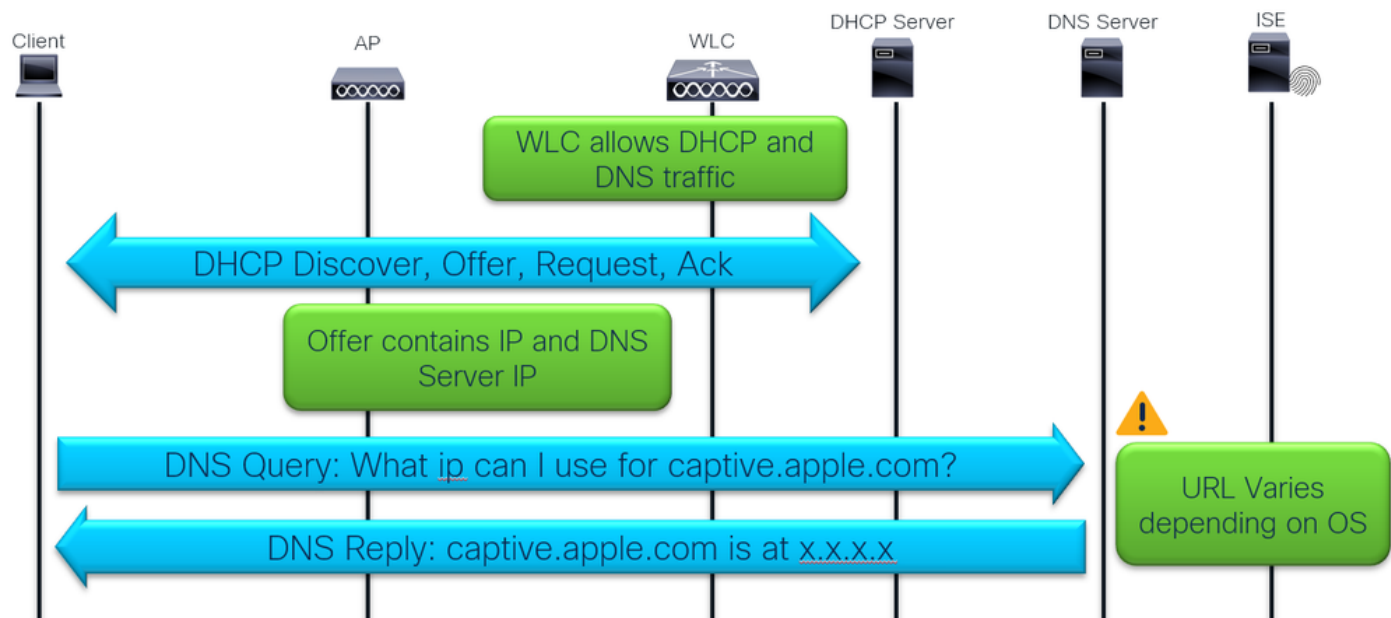
詳細流程

首次關聯和RADIUS身份驗證：



首次關聯和RADIUS身份驗證

DHCP、DNS和連線檢查：



DHCP、DNS和連線檢查

連線檢查由客戶端裝置作業系統或瀏覽器使用強制網路門戶檢測完成。

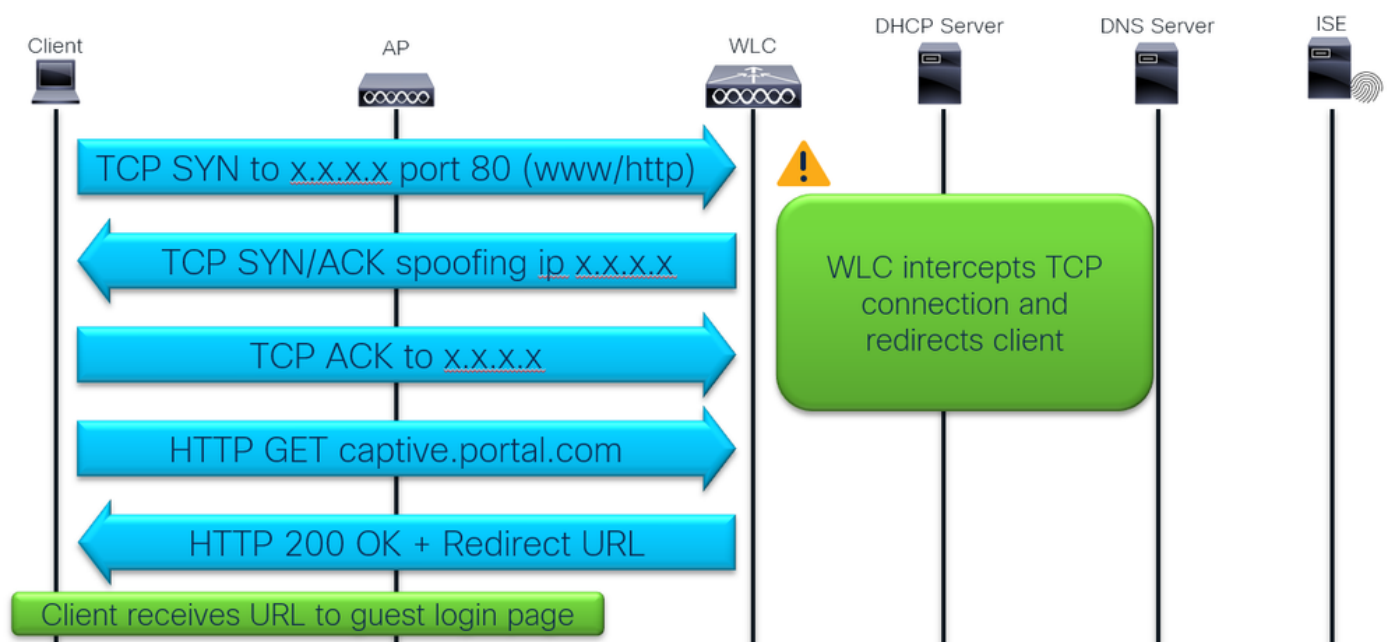
有預程式設計的裝置作業系統可針對特定域執行HTTP GET

- 蘋果 = captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnecttest.com

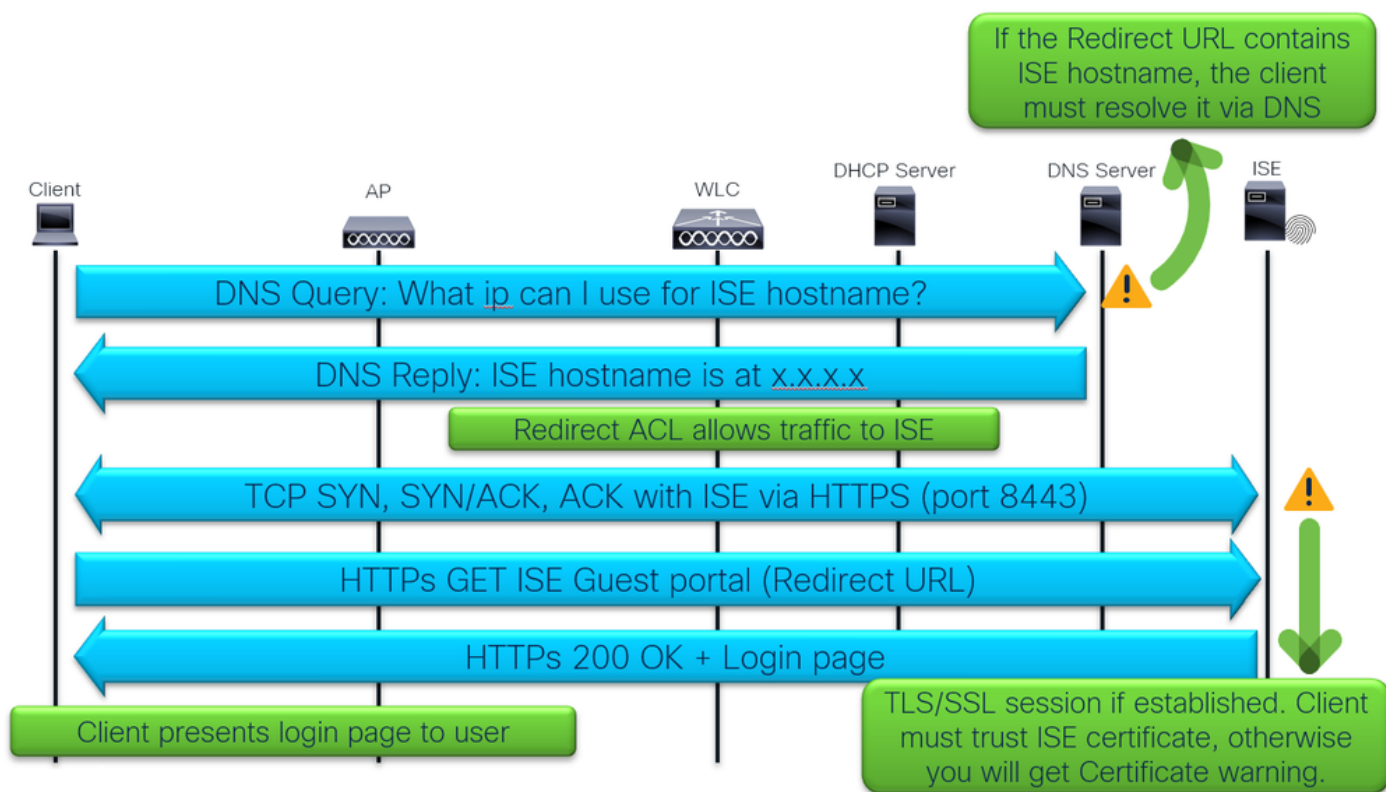
並且瀏覽器在開啟時也會執行此檢查：

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

流量攔截和重定向：

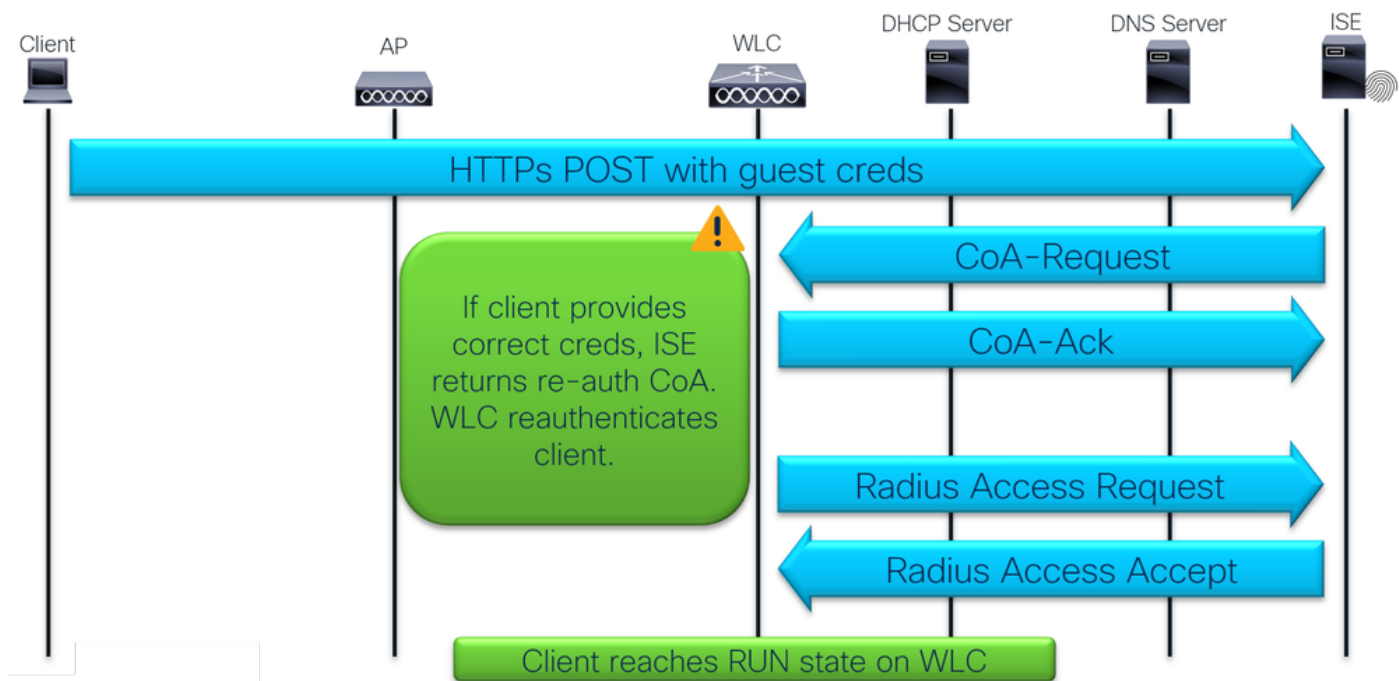


客戶端登入到ISE訪客登入門戶：



客戶端登入到ISE訪客登入門戶

客戶端登入和CoA:

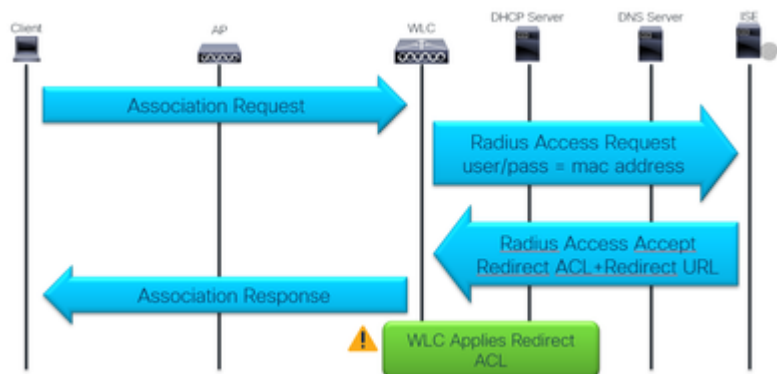


客戶端登入和CoA

疑難排解

常見症狀：使用者沒有重新導向至登入頁面。

讓我們從流程的第一部分開始：



首次關聯和RADIUS身份驗證

1 — 第一個RADIUS身份驗證是否成功？

檢查mac過濾驗證結果：

The screenshot shows the Cisco ISE interface. On the left, the 'Live Logs' tab is selected, displaying a table of log entries. The entry for 'Jan 13, 2023 09:42:37.4...' is highlighted with a red box. On the right, the 'Authentication Details' for this event are shown. The 'Event' is '5400 Authentication failed'. The 'Failure Reason' is '22056 Subject not found in the applicable identity store(s)'. The 'Steps' section on the right shows the sequence of events, with the step '22056 Subject not found in the applicable identity store(s)' highlighted with a red box.

Time	Status	Details	Repea...	Identity	Endpoint ID
Jan 13, 2023 09:42:37.4...	Failed	🔒		F2:A4:01:57:8D:68	F2:A4:01:57:8D:68

Authentication Details

Event: 5400 Authentication failed

Failure Reason: 22056 Subject not found in the applicable identity store(s)

Resolution: Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol.

Root cause: Subject not found in the applicable identity store(s).

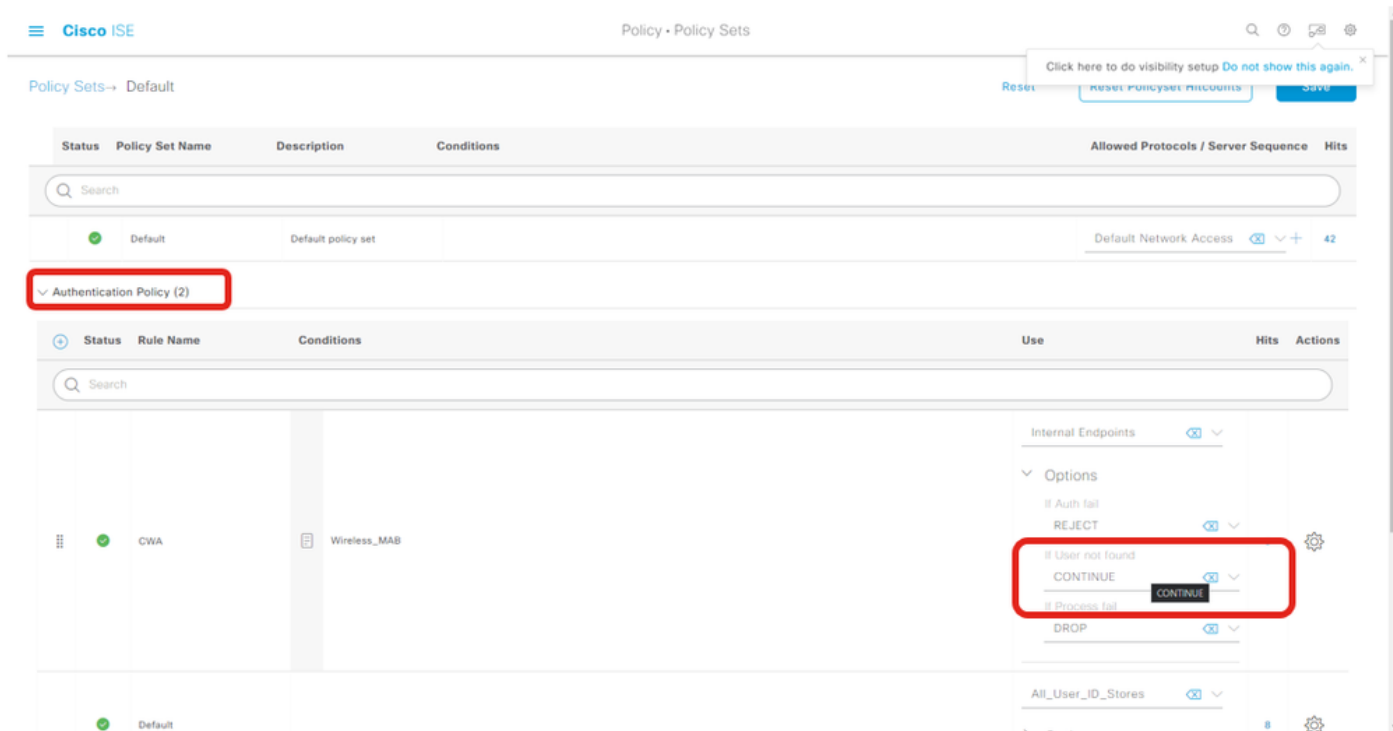
Username: F2:A4:01:57:8D:68

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11027 Detected Host Lookup UseCase (Service-Type = Call Check (100))
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15041 Evaluating Identity Policy
- 15048 Queried PIP = Normalised Radius RadiusIotType
- 15013 Selected Identity Source = Internal Endpoints
- 24209 Looking up Endpoint in Internal Endpoints IDStore - F2:A4:01:57:8D:68
- 24217 The host is not found in the internal endpoints identity store
- 22056 Subject not found in the applicable identity store(s)
- 22058 The advanced option that is configured for an unknown user is used
- 22061 The 'Reject' advanced option is configured in case of a failed authentication request
- 11003 Returned RADIUS Access-Reject

顯示mac過濾身份驗證結果的ISE Live日誌

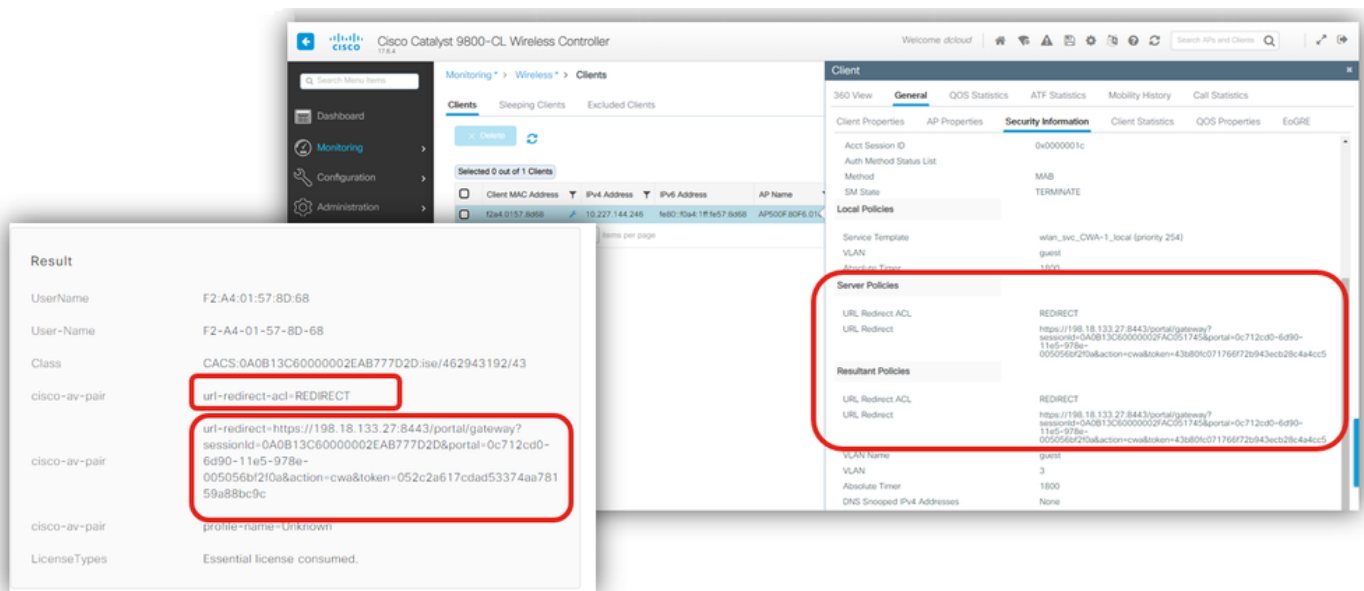
如果找不到使用者，請確保身份驗證的高級選項設定為「繼續」：



未找到使用者高級選項

2 - WLC收到重新導向URL和ACL?

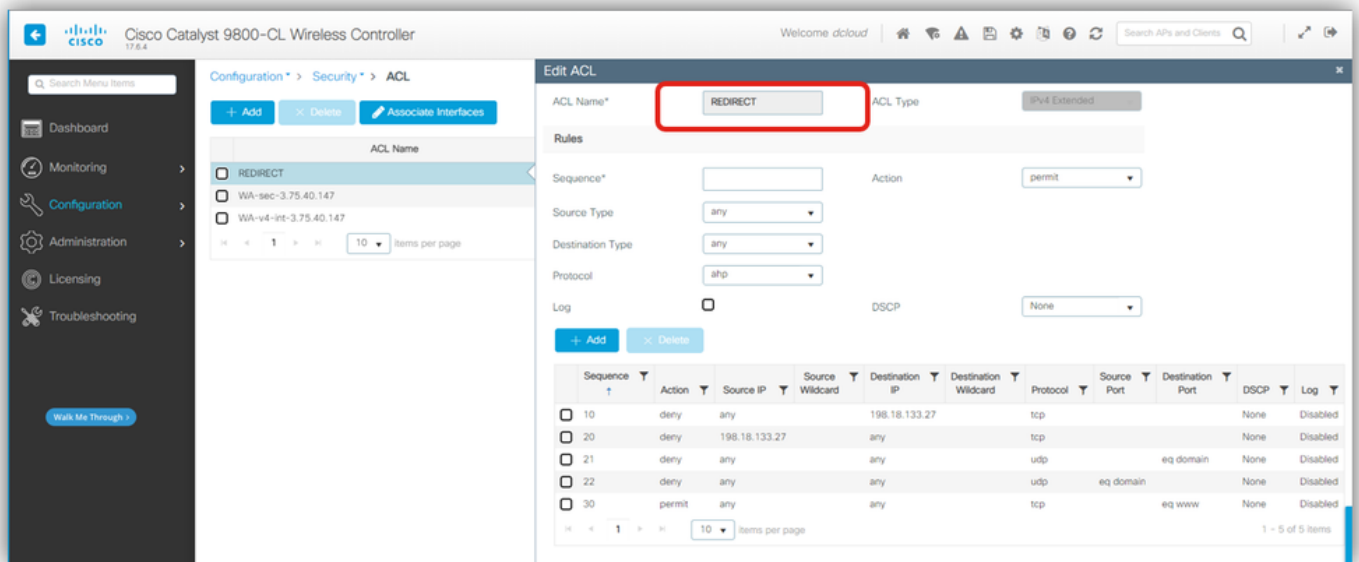
檢查Monitoring下的ISE即時日誌和WLC客戶端安全資訊驗證ISE在Access Accept中傳送Redirect URL和ACL，並且WLC會收到該資訊，並在客戶端詳細資訊中將其應用到客戶端：



重新導向ACL和URL

3 — 重定向ACL是否正確？

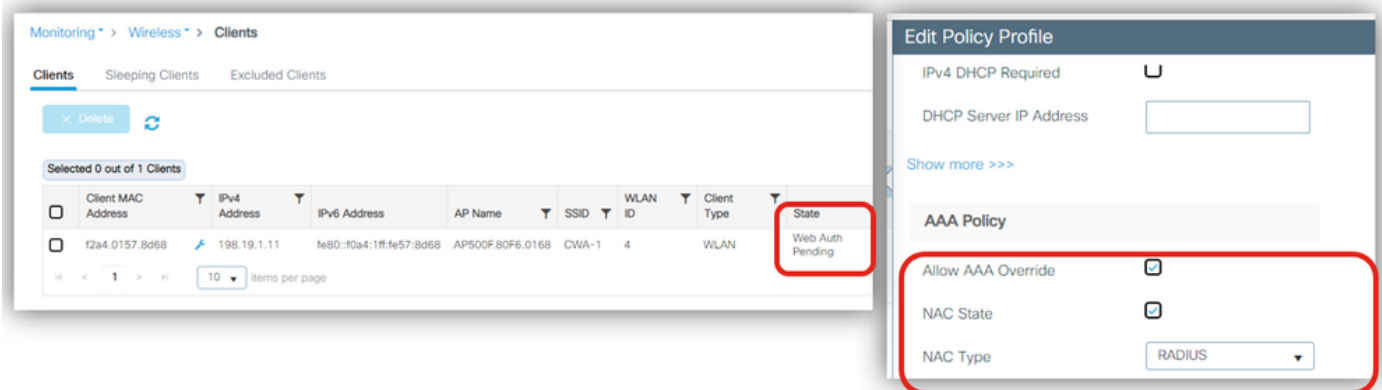
檢查ACL名稱中是否存在任何拼寫錯誤。確保它與ISE傳送的完全相同：



重新導向ACL驗證

4 — 是否將使用者端移至Web-Auth Pending?

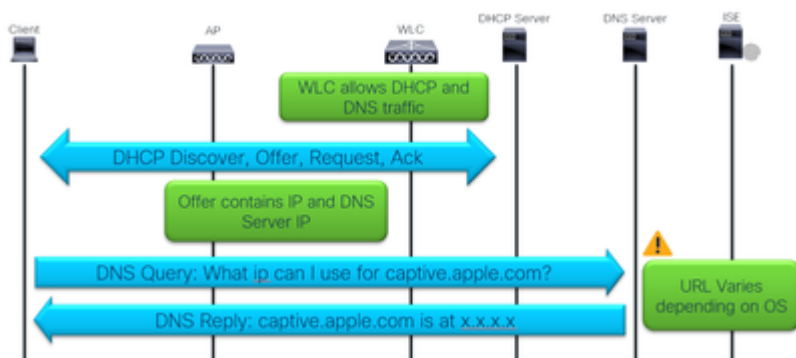
檢查使用者端詳細資訊，瞭解「Web Auth Pending」狀態。如果它未處於該狀態，則驗證是否已在策略配置檔案中啟用AAA覆蓋和Radius NAC:



客戶端詳細資訊、aaa覆蓋和RADIUS NAC

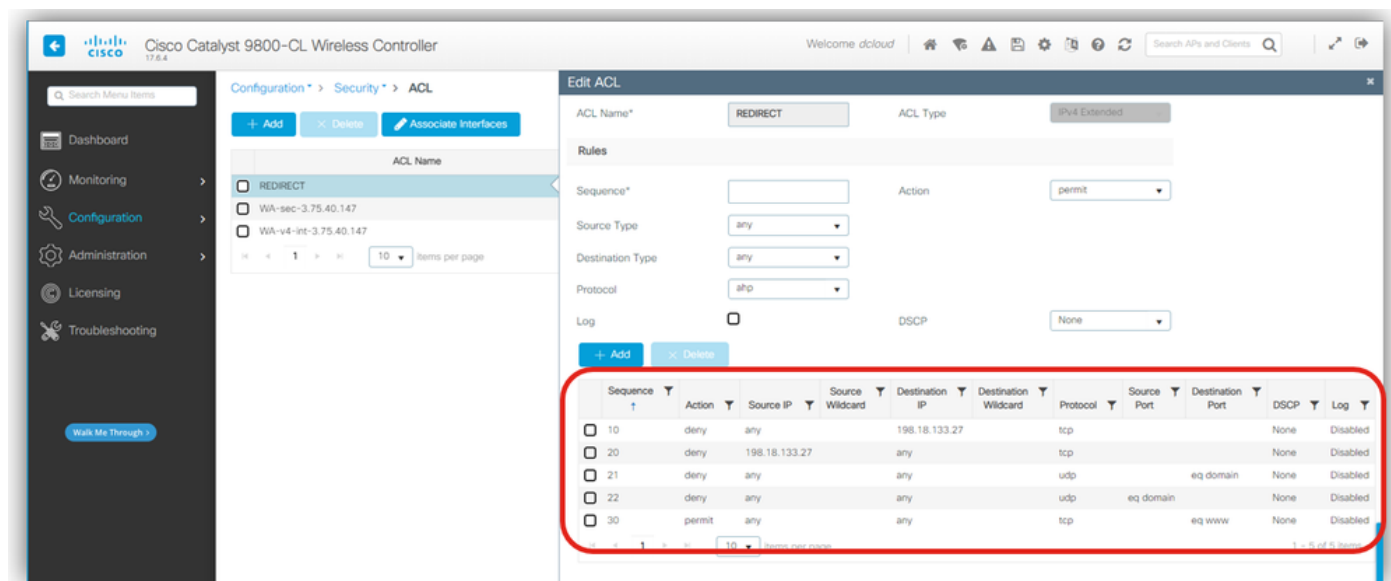
還是不工作？

讓我們重新審視一下流程.....



5 - WLC是否允許DHCP和DNS流量？

驗證WLC中的重新導向ACL內容：



在WLC中重新導向ACL內容

重定向ACL定義哪些流量被permit語句攔截和重定向，哪些流量被以deny語句從攔截和重定向中忽略。

在本例中，我們允許DNS和流量流入/流出ISE IP地址，並攔截埠80(www)上的任何tcp流量。

6 - DHCP伺服器是否接收DHCP發現/請求？

如果發生DHCP交換，請檢查EPC。EPC可以與內部過濾器（例如DHCP協定和/或內部過濾器MAC）一起使用，其中我們可以使用客戶端裝置MAC地址，並且我們只能在EPC中獲取由客戶端裝置MAC地址傳送或傳送到客戶端裝置MAC地址的DHCP資料包。

在本例中，我們可以看到VLAN 3上的DHCP發現資料包以廣播形式傳送：

用於驗證DHCP的WLC EPC

確認策略配置檔案中預期的客戶端VLAN:

策略配置檔案中的VLAN

驗證WLC VLAN和switchport Trunk配置和DHCP子網：

```
WLC1#show vlan

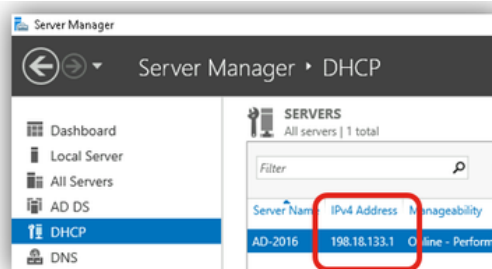
VLAN Name                Status    Ports
-----
1    default                active    Gi2, Gi3
2    employee               active
3    guest                  active
11   mgmt                    active

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           198.19.2.2      YES NVRAM  up        up
Vlan2           198.19.1.2      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和DHCP子網

我們可以看到VLAN 3存在於WLC中，而且它也有用於VLAN 3的SVI，但是當我們驗證DHCP伺服器
的IP地址時，它位於不同的子網中，因此我們需要在SVI上提供IP幫助地址。

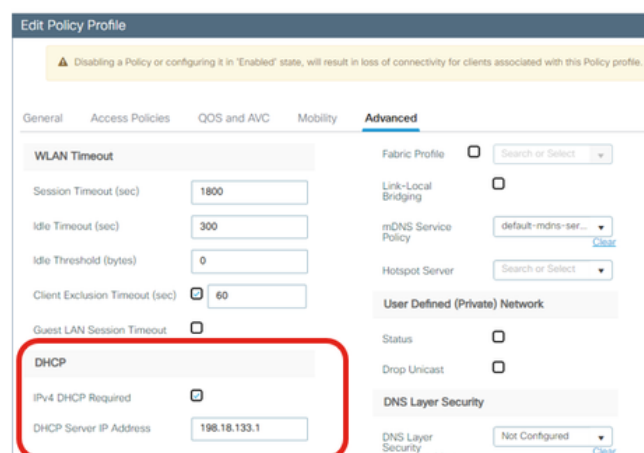
最佳實踐要求在有線基礎架構中配置客戶端子網的SVI，並在WLC上避免配置。

在任何情況下，都需要將ip helper-address命令新增到SVI，無論它位於何處。

另一種方法是在策略配置檔案中配置DHCP伺服器IP地址：

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

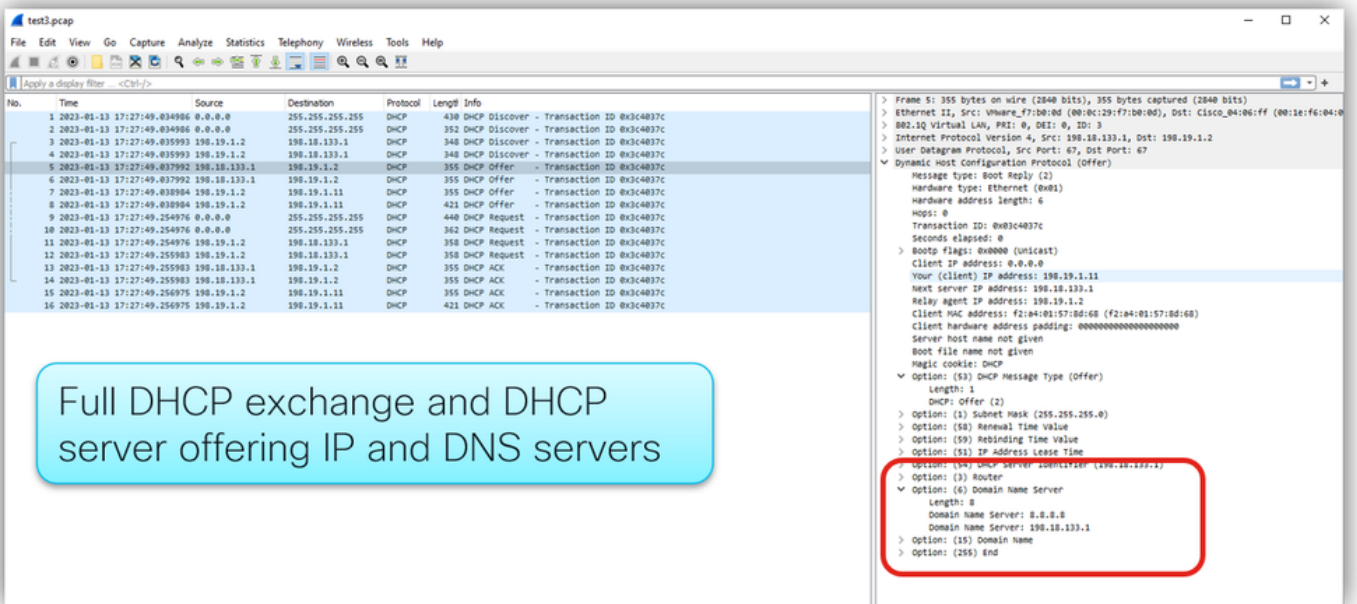
Current configuration : 141 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 ip helper-address 198.18.133.1
 no mop enabled
 no mop sysid
end
```



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

SVI或策略配置檔案的IP幫助程式地址

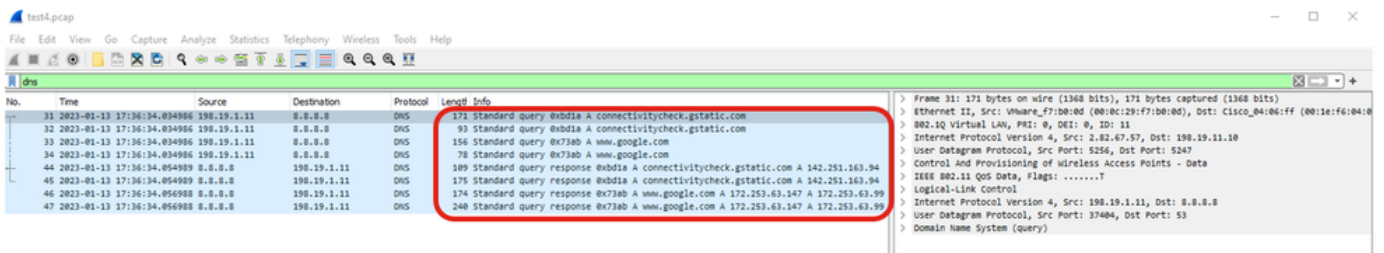
然後，您可以使用EPC驗證DHCP交換現在是否正常，以及DHCP伺服器是否提供DNS伺服器IP：



DNS伺服器IP的DHCP提供詳細資訊

7 — 是否發生自動重定向？

使用WLC EPC驗證DNS伺服器是否響應查詢：

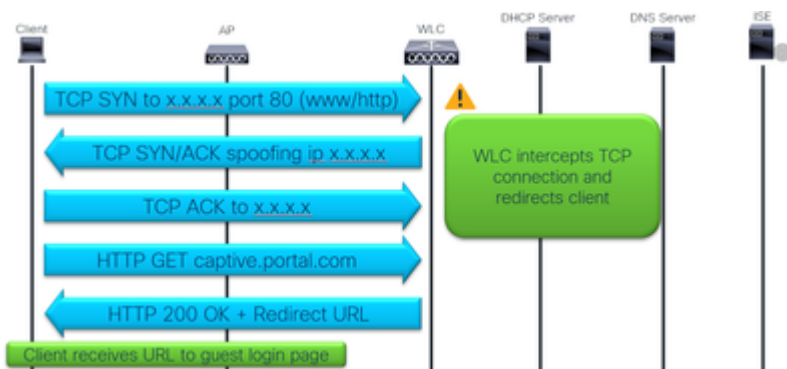


DNS查詢和響應

- 如果重新導向不是自動的，請開啟瀏覽器並嘗試隨機的IP地址。例如10.0.0.1。
- 如果重新導向隨後生效，則可能會遇到DNS解析問題。

還是不工作？

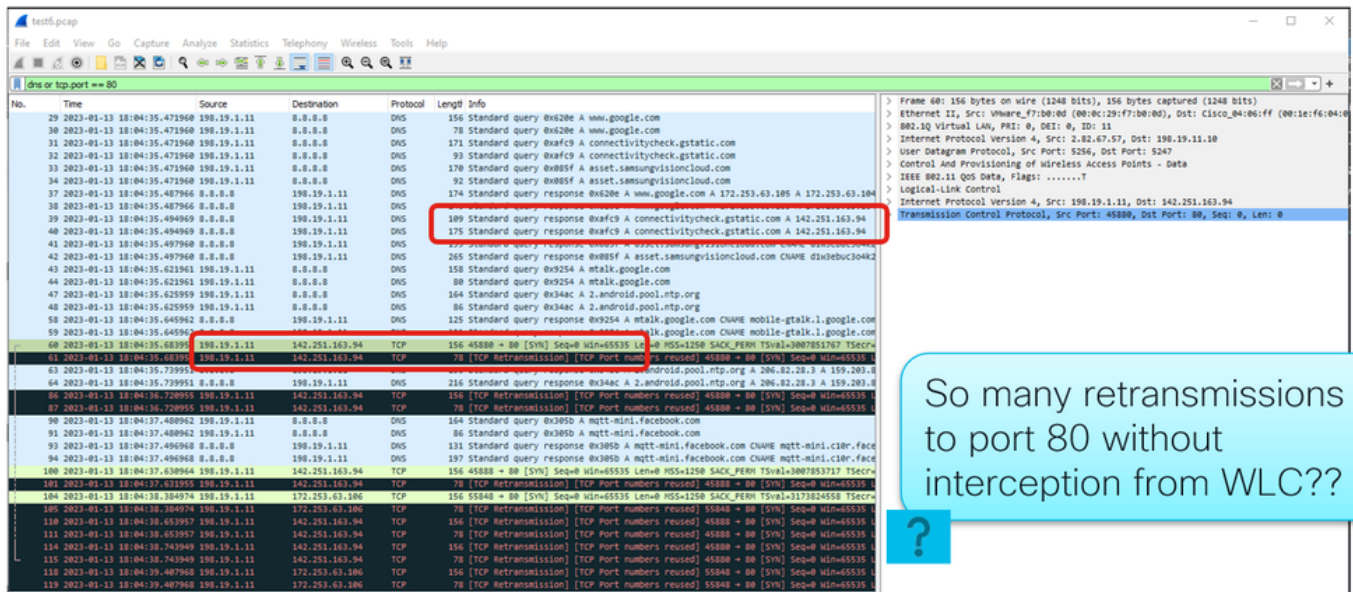
讓我們重新審視一下流程.....



流量攔截和重定向

8 — 瀏覽器不顯示登入頁面？

驗證使用者端是否將TCP SYN傳送到連線埠80，然後WLC攔截該連線埠：

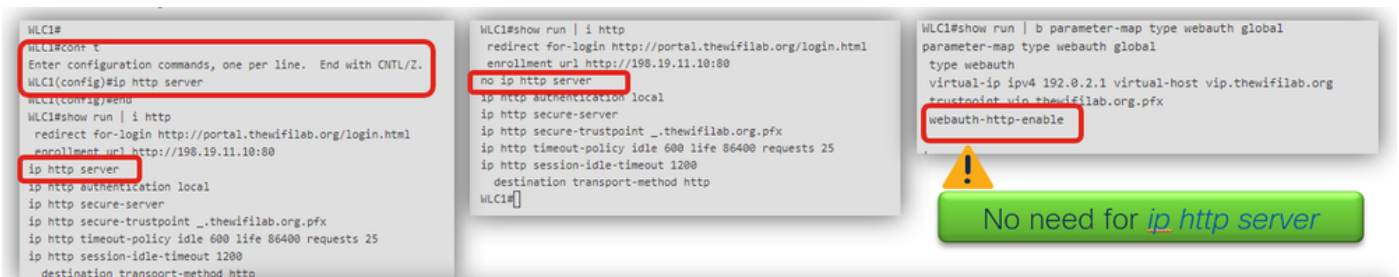


The image shows a Wireshark packet capture of traffic on interface 'eth0'. The filter is 'dns or tcp.port == 80'. The packet list shows numerous DNS queries and responses, followed by a series of TCP SYN packets to port 80. A red box highlights a specific SYN packet (No. 109) and its corresponding retransmissions (Nos. 110, 111, 112, 113, 114, 115, 116, 117, 118, 119). A blue callout box with a question mark contains the text: 'So many retransmissions to port 80 without interception from WLC??'.

TCP重新傳輸到埠80

此處我們可以看到使用者端將TCP SYN封包傳送到連線埠80，但沒有取得任何回覆，而且會執行TCP重新傳輸。

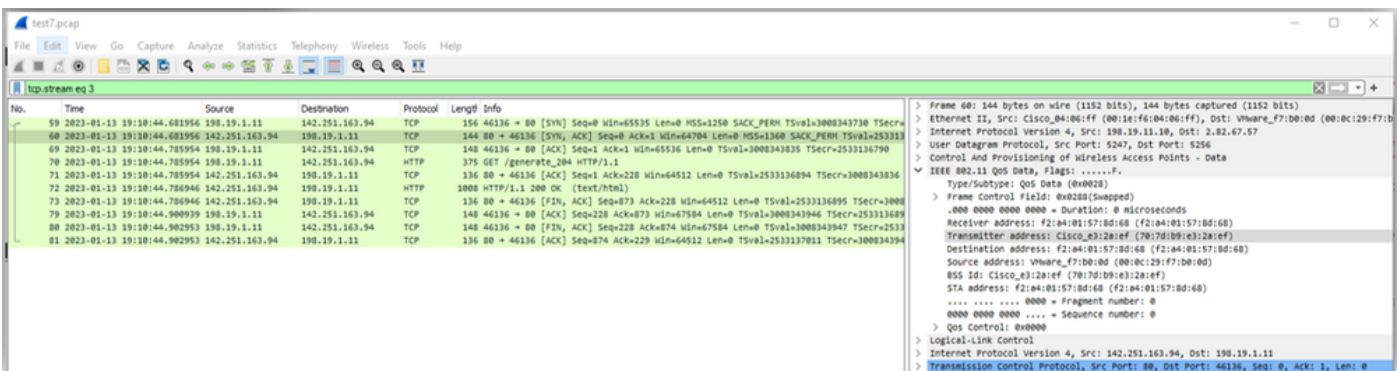
確保在全域性配置中使用ip http server命令，或在引數對映全域性配置中使用webauth-http-enable：



The image displays three configuration snippets for WLC1. The first snippet shows the configuration of the http server: 'WLC1#conf t', 'WLC1(config)#ip http server', 'WLC1(config)#ip http server', 'WLC1#show run | i http', 'redirect for-login http://portal.thewifilab.org/login.html', 'enrollment url http://198.19.11.10:80', 'ip http server', 'ip http authentication local', 'ip http secure-server', 'ip http secure-trustpoint _thewifilab.org.pfx', 'ip http timeout-policy idle 600 life 86400 requests 25', 'ip http session-idle-timeout 1200', 'destination transport-method http'. The second snippet shows the configuration of the webauth-http-enable: 'WLC1#show run | i http', 'redirect for-login http://portal.thewifilab.org/login.html', 'enrollment url http://198.19.11.10:80', 'no ip http server', 'ip http authentication local', 'ip http secure-server', 'ip http secure-trustpoint _thewifilab.org.pfx', 'ip http timeout-policy idle 600 life 86400 requests 25', 'ip http session-idle-timeout 1200', 'destination transport-method http', 'WLC1#'. The third snippet shows the configuration of the webauth-http-enable: 'WLC1#show run | b parameter-map type webauth global', 'parameter-map type webauth global', 'type webauth', 'virtual-ip ipv4 192.0.2.1 virtual-host vip.thewifilab.org', 'trustpoint vip.thewifilab.org.pfx', 'webauth-http-enable'. A green callout box with a green arrow points to the 'webauth-http-enable' command, containing the text: 'No need for ip http server'.

http攔截命令

執行此命令後，WLC會攔截TCP並偽裝目的地IP位址，以回覆使用者端並進行重新導向。

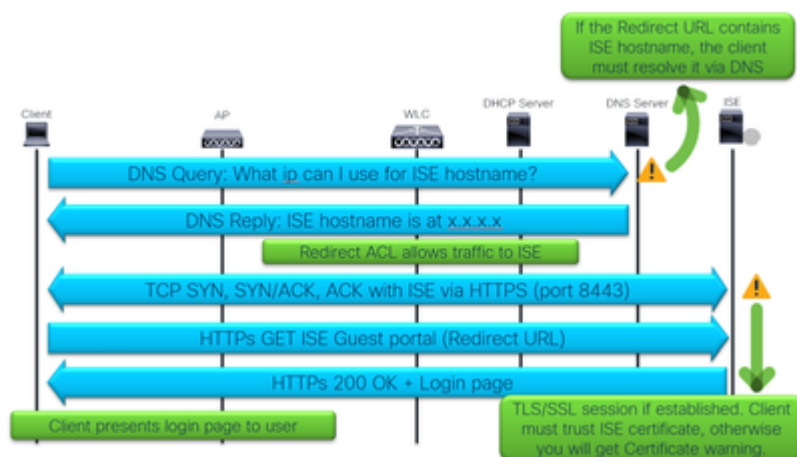


The image shows a Wireshark packet capture of traffic on interface 'eth0'. The filter is 'tcp.stream eq 3'. The packet list shows a series of TCP SYN packets to port 80. A red box highlights a specific SYN packet (No. 109) and its corresponding retransmissions (Nos. 110, 111, 112, 113, 114, 115, 116, 117, 118, 119). A blue callout box with a question mark contains the text: 'So many retransmissions to port 80 without interception from WLC??'.

WLC的TCP攔截

還是不工作？

流程中有更多內容.....



客戶端登入到ISE訪客登入門戶

9 — 客戶端是否可以解析ISE主機名？

驗證重定向URL是否使用IP或主機名，以及客戶端是否解析ISE主機名：

```
C:\Users\administrator.DCLOUD>nslookup ise.thewifilab.org
Server: localhost
Address: 127.0.0.1

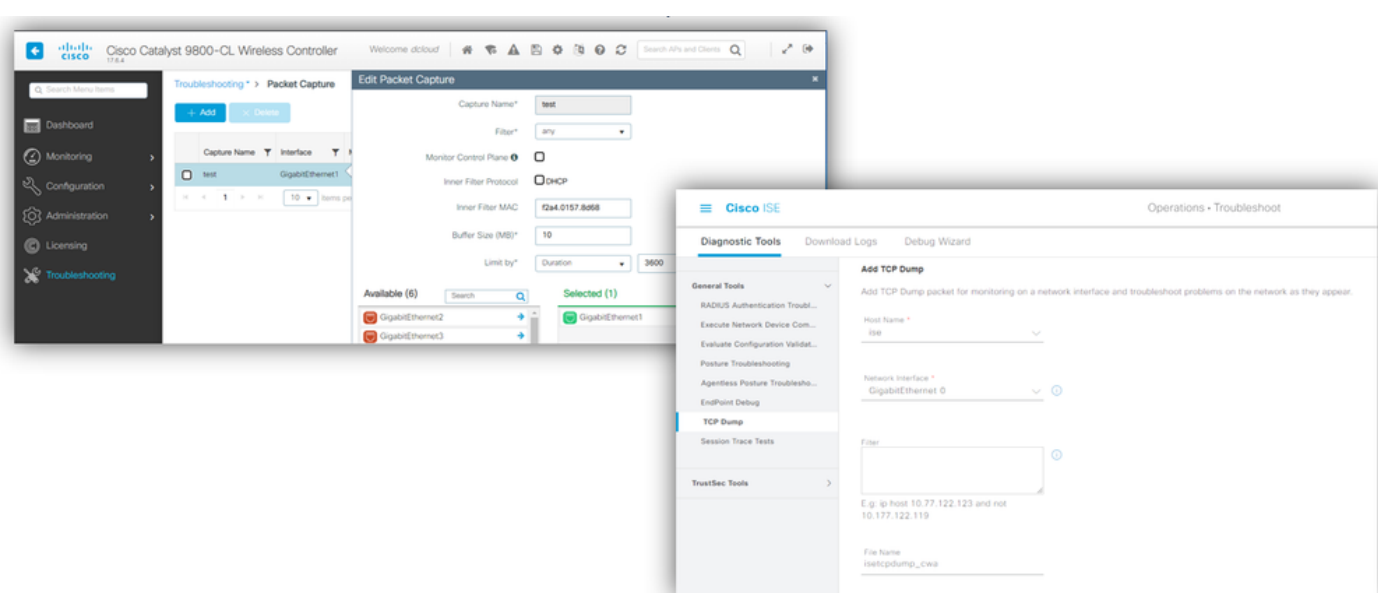
Non-authoritative answer:
Name: ise.thewifilab.org
Address: 198.18.133.27
```

ISE主機名解析

當重定向URL包含ISE主機名時會出現一個常見問題，但客戶端裝置無法將該主機名解析為ISE IP地址。如果使用主機名，請確保可以通過DNS解析。

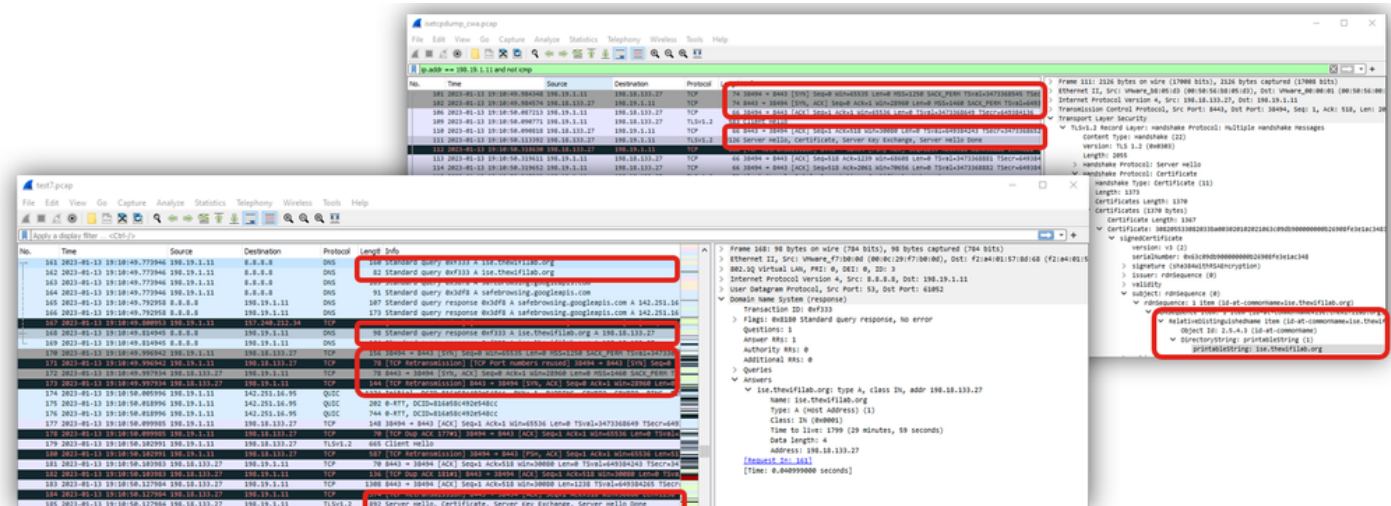
10 — 登入頁面仍無法載入？

如果客戶端流量達到ISE PSN，使用WLC EPC和ISE TCPdump進行驗證。在WLC和ISE上配置並啟動捕獲：



WLC EPC和ISE TCPDump

問題再現後，收集捕獲並關聯流量。在此我們可以看到ISE主機名已解析，然後客戶端和ISE在埠8443上通訊：



WLC和ISE流量

11 — 為什麼由於證書導致安全違規？

如果您在ISE上使用自簽名證書，則當客戶端嘗試顯示ISE門戶登入頁面時，客戶端會發出安全警告。

在WLC EPC或ISE TCPdump上，我們可以驗證ISE證書是否受信任。

在本例中，我們可以看到連線從客戶端關閉並發出警報(級別：致命，描述：certificate Unknown)，表示ISE證書未知（受信任）：

No.	Time	Source	Destination	Protocol	Length	Info
101	2023-01-13 19:10:49.994348	198.19.1.11	198.18.133.27	TCP	74	38494 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=3473368545 TSecr=0
102	2023-01-13 19:10:49.994574	198.18.133.27	198.19.1.11	TCP	74	8443 → 38494 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=649384136 TSecr=3473368545
106	2023-01-13 19:10:50.007213	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3473368649 TSecr=649384136
109	2023-01-13 19:10:50.090775	198.19.1.11	198.18.133.27	TLSv1.2	583	Client hello
110	2023-01-13 19:10:50.090818	198.18.133.27	198.19.1.11	TCP	66	8443 → 38494 [ACK] Seq=1 Ack=518 Win=30800 Len=0 TSval=649384243 TSecr=3473368652
111	2023-01-13 19:10:50.111392	198.18.133.27	198.19.1.11	TLSv1.2	2126	Server hello, Certificate, Server key exchange, Server hello done
112	2023-01-13 19:10:50.116108	198.18.133.27	198.19.1.11	TCP	66	38494 → 8443 [RST] Seq=1239 Ack=518 Win=0 Len=0
113	2023-01-13 19:10:50.119611	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [ACK] Seq=518 Ack=1239 Win=68000 Len=0 TSval=3473368881 TSecr=649384
114	2023-01-13 19:10:50.119652	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [ACK] Seq=518 Ack=2061 Win=70656 Len=0 TSval=3473368882 TSecr=649384
115	2023-01-13 19:10:50.134763	198.19.1.11	198.18.133.27	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate unknown)
116	2023-01-13 19:10:50.134765	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [FIN, ACK] Seq=525 Ack=2061 Win=70656 Len=0 TSval=3473368918 TSecr=649384
117	2023-01-13 19:10:50.134858	198.18.133.27	198.19.1.11	TLSv1.2	73	Alert (Level: warning, Description: Close notify)
118	2023-01-13 19:10:50.134859	198.18.133.27	198.19.1.11	TCP	66	8443 → 38494 [FIN, ACK] Seq=2068 Ack=526 Win=0 Len=0 TSval=649384506 TSecr=3473368918
119	2023-01-13 19:10:50.145456	198.19.1.11	198.18.133.27	TCP	72	8443 → 38494 [ACK] Seq=2068 Ack=526 Win=0 Len=0 TSval=649384506 TSecr=3473368918
120	2023-01-13 19:10:50.145459	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [RST] Seq=526 Win=0 Len=0
121	2023-01-13 19:10:50.145522	198.19.1.11	198.18.133.27	TCP	66	38494 → 8443 [RST] Seq=526 Win=0 Len=0
130	2023-01-13 19:10:55.403803	198.19.1.11	198.18.133.27	TCP	74	38536 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=3473373965 TSecr=0
139	2023-01-13 19:10:55.403833	198.18.133.27	198.19.1.11	TCP	74	8443 → 38536 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=649384903 TSecr=3473373965
143	2023-01-13 19:10:55.420963	198.19.1.11	198.18.133.27	TCP	74	38536 → 8443 [SYN] Seq=0 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=3473373983 TSecr=0
144	2023-01-13 19:10:55.421053	198.18.133.27	198.19.1.11	TCP	74	8443 → 38536 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=649384903 TSecr=3473373983
147	2023-01-13 19:10:55.562911	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3473374124 TSecr=649389555
148	2023-01-13 19:10:55.563063	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3473374125 TSecr=649389573
153	2023-01-13 19:10:55.565193	198.19.1.11	198.18.133.27	TLSv1.2	583	Client hello
154	2023-01-13 19:10:55.565245	198.18.133.27	198.19.1.11	TCP	66	8443 → 38536 [ACK] Seq=1 Ack=518 Win=30800 Len=0 TSval=649389717 TSecr=3473374127
155	2023-01-13 19:10:55.567118	198.19.1.11	198.18.133.27	TLSv1.2	583	Client hello
156	2023-01-13 19:10:55.567144	198.18.133.27	198.19.1.11	TCP	66	8443 → 38536 [ACK] Seq=1 Ack=518 Win=30800 Len=0 TSval=649389719 TSecr=3473374129
157	2023-01-13 19:10:55.578226	198.18.133.27	198.19.1.11	TLSv1.2	2126	Server hello, Certificate, Server key exchange, Server hello done
158	2023-01-13 19:10:55.588307	198.18.133.27	198.19.1.11	TLSv1.2	2126	Server hello, Certificate, Server key exchange, Server hello done
159	2023-01-13 19:10:55.768137	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=518 Ack=1239 Win=68000 Len=0 TSval=3473374330 TSecr=6493898
160	2023-01-13 19:10:55.769063	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=518 Ack=2061 Win=70656 Len=0 TSval=3473374331 TSecr=6493898
161	2023-01-13 19:10:55.769095	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=518 Ack=1239 Win=68000 Len=0 TSval=3473374332 TSecr=6493898
162	2023-01-13 19:10:55.769647	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [ACK] Seq=518 Ack=1239 Win=68000 Len=0 TSval=3473374332 TSecr=6493898
164	2023-01-13 19:10:55.787246	198.19.1.11	198.18.133.27	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate unknown)
165	2023-01-13 19:10:55.787294	198.19.1.11	198.18.133.27	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate unknown)
166	2023-01-13 19:10:55.787933	198.19.1.11	198.18.133.27	TCP	66	38536 → 8443 [FIN, ACK] Seq=525 Ack=2061 Win=70656 Len=0 TSval=3473374358 TSecr=6493898
167	2023-01-13 19:10:55.787953	198.18.133.27	198.19.1.11	TCP	66	38536 → 8443 [FIN, ACK] Seq=525 Ack=2061 Win=70656 Len=0 TSval=3473374358 TSecr=6493898
168	2023-01-13 19:10:55.791282	198.18.133.27	198.19.1.11	TLSv1.2	73	Alert (Level: warning, Description: Close notify)
169	2023-01-13 19:10:55.791288	198.18.133.27	198.19.1.11	TCP	66	8443 → 38536 [FIN, ACK] Seq=2068 Ack=526 Win=0 Len=0 TSval=649389943 TSecr=3473374358
170	2023-01-13 19:10:55.792268	198.18.133.27	198.19.1.11	TLSv1.2	73	Alert (Level: warning, Description: Close notify)
171	2023-01-13 19:10:55.792308	198.18.133.27	198.19.1.11	TCP	66	8443 → 38536 [FIN, ACK] Seq=2068 Ack=526 Win=0 Len=0 TSval=649389944 TSecr=3473374358
176	2023-01-13 19:10:55.816354	198.18.133.27	198.19.1.11	TCP	66	38536 → 8443 [FIN, ACK] Seq=525 Ack=2061 Win=70656 Len=0 TSval=649389944 TSecr=3473374358

ISE不受信任的證書

如果在客戶端進行檢查，則會看到以下示例輸出：

19:24 38%
Iniciar sessão em CWA-1

A rede à qual está a tentar aceder tem problemas de segurança.
Por exemplo, a página de início de sessão pode não pertencer à entidade esperada.

CONTINUAR MESMO ASSIM ATRAVÉS DO NAVEGADOR

VER CERTIFICADO

19:24 38%
Aviso de segurança

SSL_UNTRUSTED
Informação de página data não é confiável.
Endereço: https://ise.thewiflab.org:8443/portal/gateway/tesseond...
Este certificado não pertence a uma autoridade fiável.

Entidade para:
Nome comum: ise.thewiflab.org
Organização:
Unidade organizacional:
Número de série: 63 C0 9D 89 00 00 00 00 82 68 08 FE 3E 1A C3 48

Entidade por:
Nome comum: ise.thewiflab.org
Organização:
Unidade organizacional:
Validade:
Emitido em: 12/01/2023
Copia em: 11/01/2023

OK

19:25 38%
A sua ligação não é privada
Os atacantes poderão estar a tentar roubar as suas informações de ise.thewiflab.org (por exemplo, palavras-passe, mensagens ou cartões de crédito).

Saiba mais

NET::ERR_CERT_AUTHORITY_INVALID

Para obter o nível de segurança mais elevado do Chrome, [ative a proteção melhorada](#).

Voltar para segurança

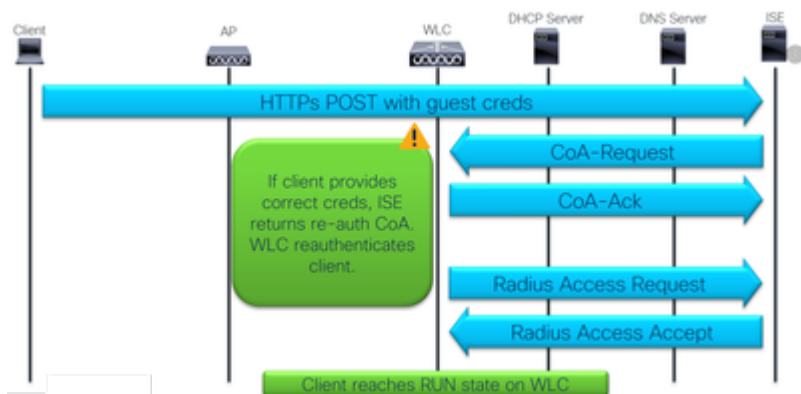
Avançadas

We can bypass warning

不信任ISE證書的客戶端裝置

最後，重定向正在起作用!!但登入失敗.....

最後一次檢查流量.....



客戶端登入和CoA

12 — 訪客登入失敗？

檢查ISE日誌以確認身份驗證失敗。確保憑據正確。

Cisco ISE

Overview

Event: 5418 Guest Authentication Failed

Username: Cwa

Endpoint Id: F2-A4:01:57:8D:68 @

Endpoint Profile:

Authorization Result:

Steps

5418 Guest Authentication Failed

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 😊

由於憑據錯誤，來賓身份驗證失敗

13 — 登入成功，但不移至RUN？

檢查ISE日誌，瞭解身份驗證詳細資訊和結果：

Cisco ISE

Overview

Event	5236 Authorize-Only succeeded
Username	cwa
Endpoint Id	F2:A4:01:57:8D:68 @
Endpoint Profile	Android
Authentication Policy	Default
Authorization Policy	Default >> Redirect-to-Portal
Authorization Result	CWAredirect

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

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 11027 Detected Host Lookup UseCase (Service-Type = Call Check (10))
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
- 15036 Evaluating Authorization Policy
- 24209 Looking up Endpoint in Internal Endpoints IDStore - cwa
- 24211 Found Endpoint in Internal Endpoints IDStore
- 15016 Selected Authorization Profile - CWAredirect
- 24210 Looking up User in Internal Users IDStore - cwa
- 24212 Found User in Internal Users IDStore
- 11002 Returned RADIUS Access-Accept

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-005056b2f10a&action=cwa&token=92eb9963bc6f70c9f82d32ed8a072c6c
cisco-av-pair	profile-name=Android
LicenseTypes	Essential license consumed.

Still getting Redirect-to-Portal ????

重新導向回圈

在此範例中，我們可以看到使用者端再次取得包含重新導向URL和重新導向ACL的授權設定檔。這會導致重新導向回圈。

檢查策略集。在重定向之前必須檢查Guest_Flow:

Authorization Policy (3)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Redirect-to-Portal	AND Wireless_MAB Radius-Called-Station-ID CONTAINS CWA	CWAredirect x			
✓	Guest-Flow	AND Wireless_MAB Guest_Flow	PermitAccess x			
✓	Default		DenyAccess x			

Other Attributes

ConfigVersionId	83
DestinationPort	1812
Protocol	Radius
NAS-Port	1115
Framed-MTU	1485
OriginalUserName	f2a401578d68
NetworkDeviceProfileId	8ade1115-ae11-4a9a-8158-d02a835179db
IsThirdPartyDeviceFlow	false
AuthSessionId	ise/462943192/118
UseCase	Guest Flow
AuthorizationPolicyMatched...	Guest-Flow
EndPointMACAddress	f2-a4-01-57-8d-68
ISEPolicySetName	Default
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups GuestEndpoints

Guest_Flow規則

14 - COA失敗？

使用EPC和ISE TCPDump，我們可以驗證CoA流量。驗證WLC和ISE之間的CoA埠(1700)是否開啟。確保共用金鑰匹配。

No.	Time	Source	Destination	Protocol	Length	Info
214	2023-01-13 19:38:06.993936	198.19.11.10	198.18.133.27	RADIUS	458	Accounting-Request id=212
215	2023-01-13 19:38:06.997934	198.18.133.27	198.19.11.10	RADIUS	84	Accounting-Response id=212
295	2023-01-13 19:38:14.104990	198.19.11.10	198.18.133.27	RADIUS	430	Access-Request id=213
296	2023-01-13 19:38:14.121987	198.18.133.27	198.19.11.10	RADIUS	489	Access-Accept id=213
310	2023-01-13 19:38:14.426964	198.19.11.10	198.18.133.27	RADIUS	480	Accounting-Request id=214
311	2023-01-13 19:38:14.439971	198.19.11.10	198.18.133.27	RADIUS	442	Accounting-Request id=215
312	2023-01-13 19:38:14.439972	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=215
313	2023-01-13 19:38:14.440971	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=214
351	2023-01-13 19:38:15.224979	198.19.11.10	198.18.133.27	RADIUS	468	Accounting-Request id=216
352	2023-01-13 19:38:15.229983	198.18.133.27	198.19.11.10	RADIUS	66	Accounting-Response id=216
3539	2023-01-13 19:38:50.416970	198.18.133.27	198.19.11.10	RADIUS	248	CoA-Request id=4
3540	2023-01-13 19:38:50.416970	198.19.11.10	198.18.133.27	RADIUS	475	Access-Request id=217
3541	2023-01-13 19:38:50.416970	198.19.11.10	198.18.133.27	RADIUS	111	CoA-ACK id=4
3542	2023-01-13 19:38:50.420963	198.18.133.27	198.19.11.10	RADIUS	166	Access-Accept id=217

CoA流量



附註：在17.4.X及更高版本中，請確保在配置RADIUS伺服器時也配置CoA伺服器金鑰。使用與共用金鑰相同的金鑰（在ISE上預設使用相同的金鑰）。其目的是為CoA配置一個不同於共用金鑰的金鑰（如果共用金鑰是RADIUS伺服器配置的金鑰）。在Cisco IOS® XE 17.3中，Web UI僅使用與CoA金鑰相同的共用金鑰。

自版本17.6.1起，此連線埠支援RADIUS（包括CoA）。如果要將服務連線埠用於RADIUS，則需要此組態：

```
<#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

結論

這是恢復的CWA核對表：

- 確保客戶端位於正確的VLAN上並獲得IP地址和DNS。
 - 在WLC上獲取客戶端詳細資訊並運行資料包捕獲以檢視DHCP交換。
- 驗證客戶端是否可通過DNS解析主機名。
 - 從cmd ping主機名。
- WLC必須在埠80上偵聽
 - 驗證全域命令ip http server或全域引數對映命令webauth-http-enable。
- 若要消除證書警告，請在ISE上安裝受信任證書。
 - 無需在CWA的WLC上安裝受信任憑證。
- ISE高級選項「Continue」處的身份驗證策略（如果未找到使用者）
 - 允許受贊助的訪客使用者連線並獲取URL重定向和ACL。

以及故障排除中使用的主要工具：

- WLC EPC
 - 內部篩選器：DHCP協定，mac地址。
- WLC監控器
 - 檢查客戶端安全詳細資訊。
- WLC RA追蹤
 - 在WLC端使用詳細資訊進行偵錯。
- ISE 即時記錄
 - 身份驗證詳細資訊。
- ISE TCPDump
 - 在ISE PSN介面收集資料包捕獲。

參考資料

[在Catalyst 9800 WLC和ISE上配置中央Web驗證\(CWA\)](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。