أستكشاف أخطاء المصادقة المركزية للويب (CWA) وإصلاحها باستخدام وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC) 9800 ومحرك خدمات الهوية (ISE)

المحتويات

المقدمة
معلومات أساسية
تفصيلي نايرج
استكشاف الأخطاء وإصلاحها
الأعراض الشائعة: لم يتم إعادة توجيه المستخدم إلى صفحة تسجيل الدخول.
1 - هل تنجح مصادقة RADIUS الأولى؟
2 - هل تتلقى لجنة التحكم في الشبكة المحلية اللاسلكية عنوان URL المعاد توجيهه وقوائم التحكم في الوصول (ACL)؟
3 - هل قائمة التحكم في الوصول (ACL) المعاد توجيههاه صحيحة؟
4 - هل تم نقل العميل إلى Web-Auth معلق؟
5 - هل تسمح وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بحركة مرور بيانات DHCP و DNS؟
6 - هل يستقبل خادم DHCP اكتشاف/طلب DHCP؟
7 - هل تحدث إعادة التوجيه التلقائية؟
8 - لا يظهر المستعرض صفحة تسجيل الدخول؟
9 - هل يمكن للعميل حل اسم المضيف ISE؟
10 - هل ما زالت صفحة تسجيل الدخول لا تحمل؟
11 - لماذا نحصل على انتهاك للأمان بسبب الشهادة؟
12 - فشل تسجيل دخول الضيوف؟
13 - هل تنجح عملية تسجيل الدخول أم لم تنتقل إلى RUN؟
14 - فشل الكاكاو؟
القرار
المراجع

المقدمة

يصف هذا وثيقة كيف أن يتحرى مركزي ويب صحة هوية (CWA) مع WLC 9800 و ISE.

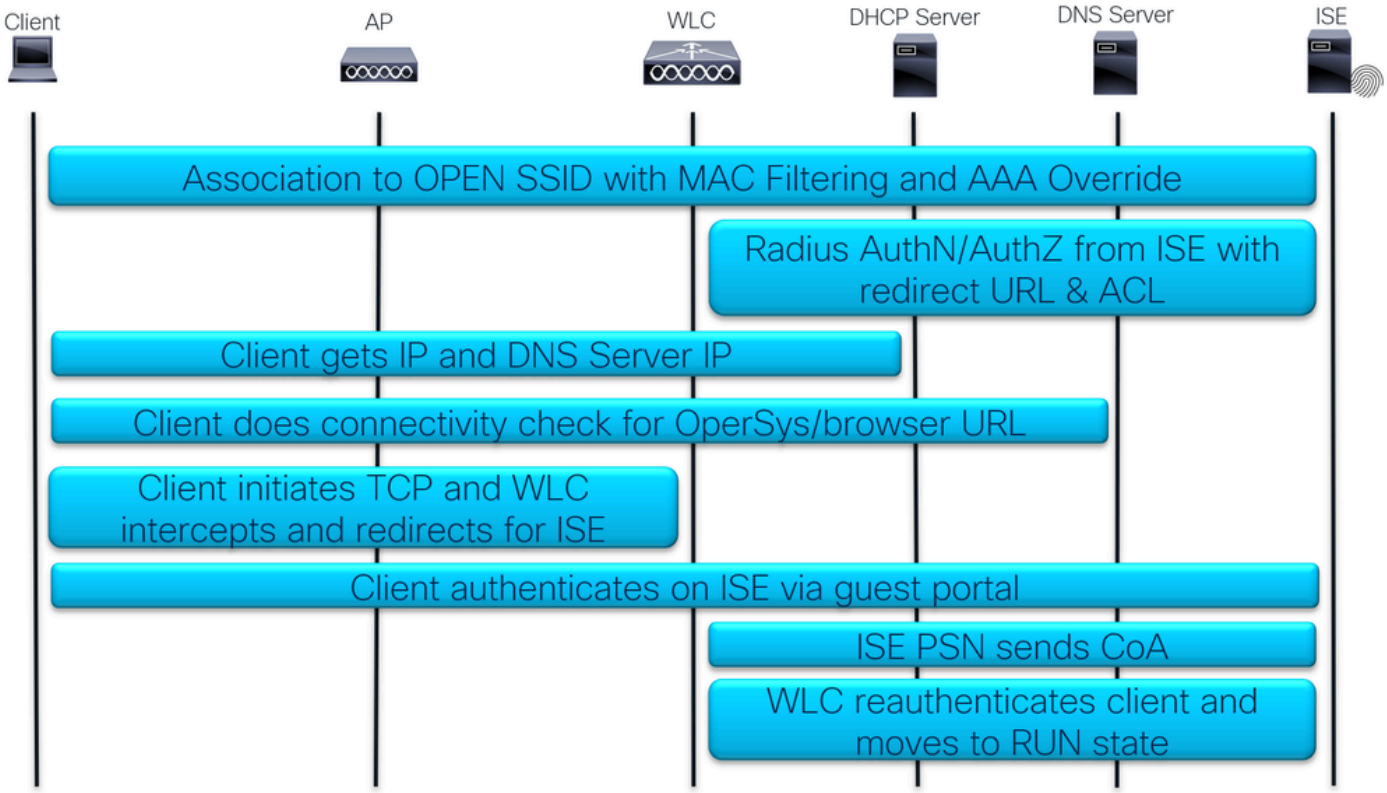
معلومات أساسية

يوجد حاليا العديد من الأجهزة الشخصية حتى أن مسؤولي الشبكة الذين يبحثون عن تأمين الوصول اللاسلكي عادة ما يختارون الشبكات اللاسلكية التي تستخدم CWA.
في هذا المستند، نركز على مخطط تدفق CWA، الذي يساعد في أستكشاف المشكلات الشائعة التي تؤثر علينا وإصلاحها.
ننظر إلى الخطوات العامة للعملية، وكيفية تجميع السجلات المتعلقة ب CWA، وكيفية تحليل هذه السجلات، وكيفية تجميع التقاط حزمة مضمنة على عنصر التحكم في

الشبكة المحلية اللاسلكية (WLC) لتأكيد تدفق حركة المرور.

يعتبر CWA الإعداد الأكثر شيوعا للشركات التي تسمح للمستخدمين بالاتصال بشبكة الشركة باستخدام أجهزتهم الشخصية، المعروفة أيضا باسم BYOD.
أي مسؤول شبكة مهتم بالخطوات Gotchas وخطوات أستكشاف الأخطاء وإصلاحها التي يتم تنفيذها لإصلاح مشكلاتهم قبل فتح حالة مركز المساعدة الفنية.

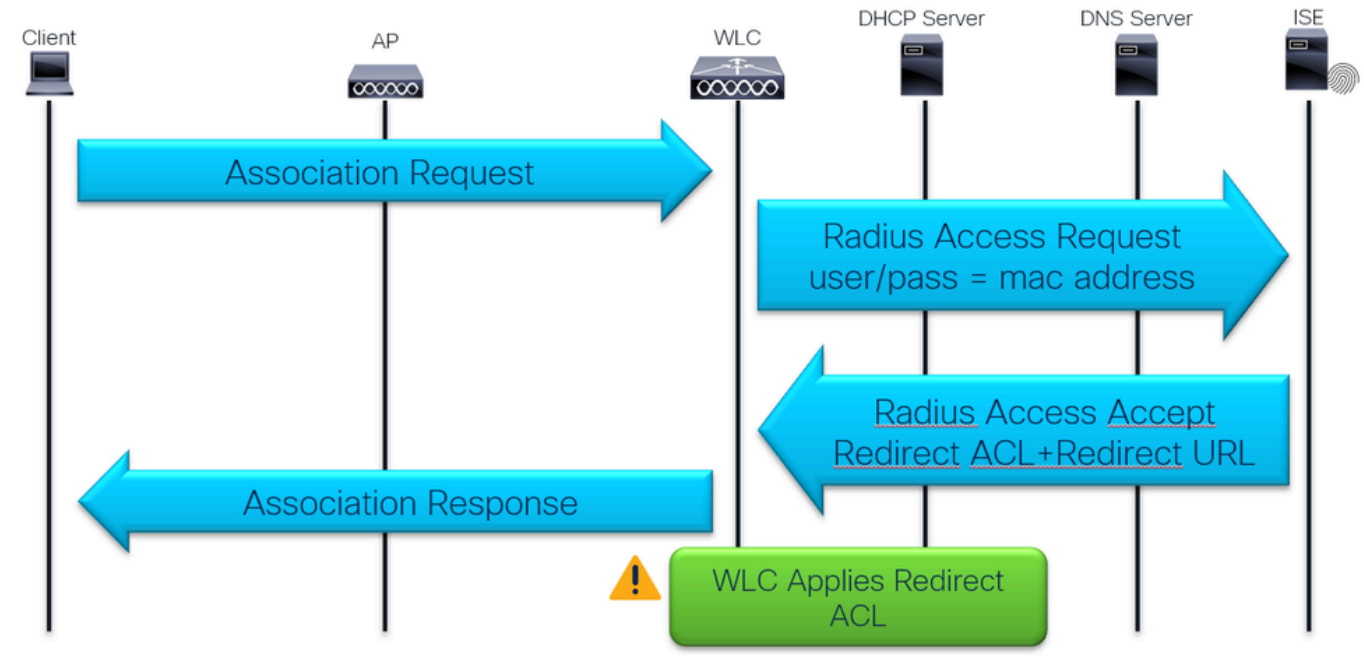
هنا تدفق حزمة CWA:



تدفق حزم CWA

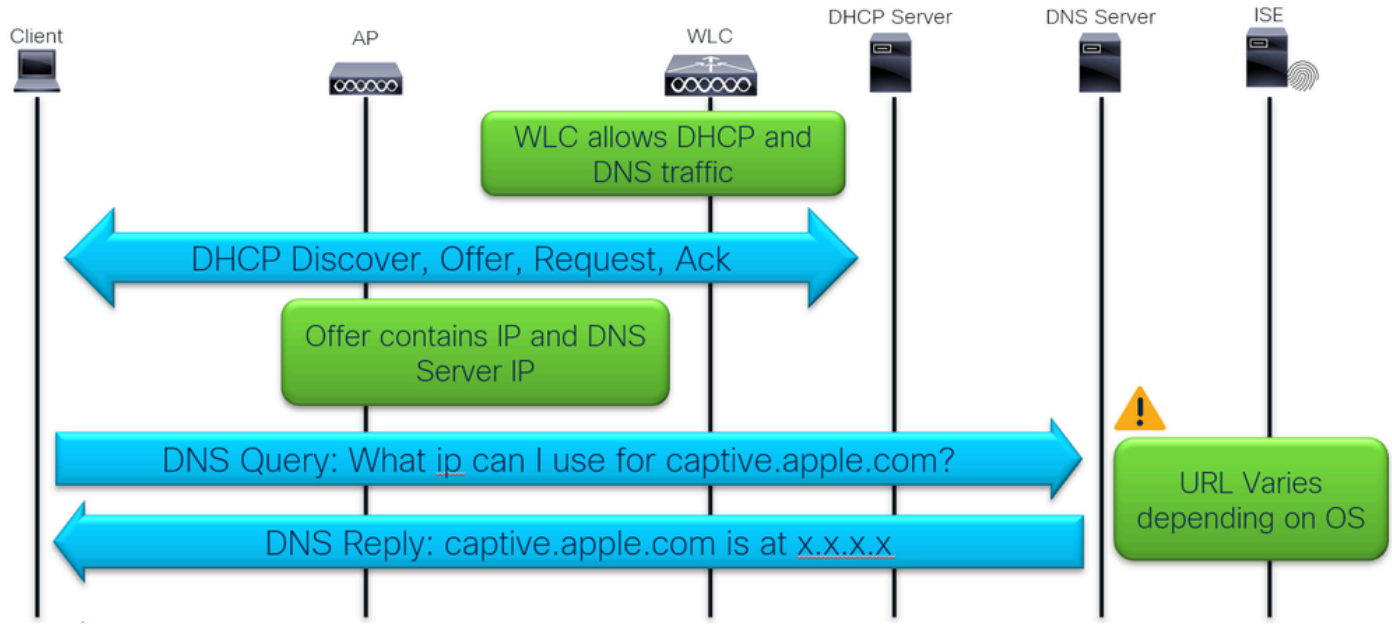
جريان تفصيلي

القتران الأول ومصادقة RADIUS:



أول اقتران ومصادقة RADIUS

فحص DHCP و DNS والاتصال:



فحص DHCP و DNS والاتصال

يتم التحقق من الاتصال باستخدام الكشف عن المدخل المقيد بواسطة نظام تشغيل الجهاز العميل أو المستعرض.

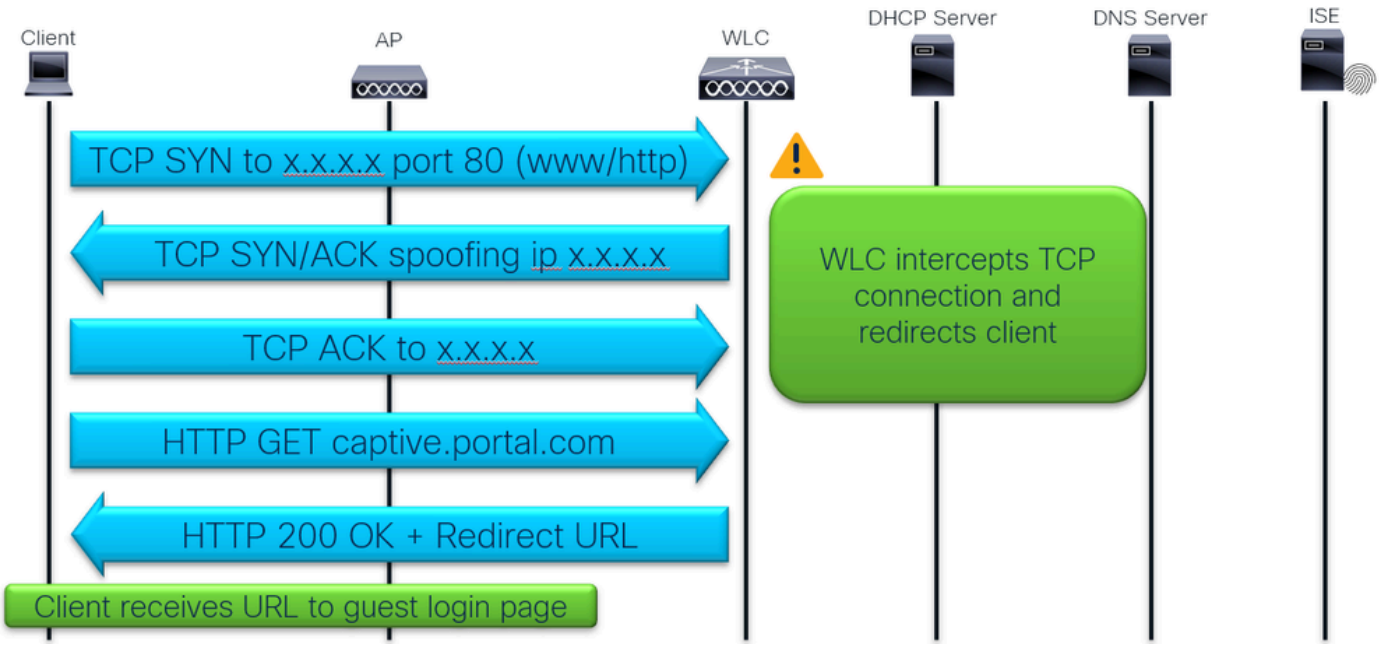
يوجد نظام تشغيل جهاز تم برمجته مسبقا للقيام ب HTTP للوصول إلى مجال معين

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

وتقوم المستعرضات أيضا بهذا التحقق عند فتحه:

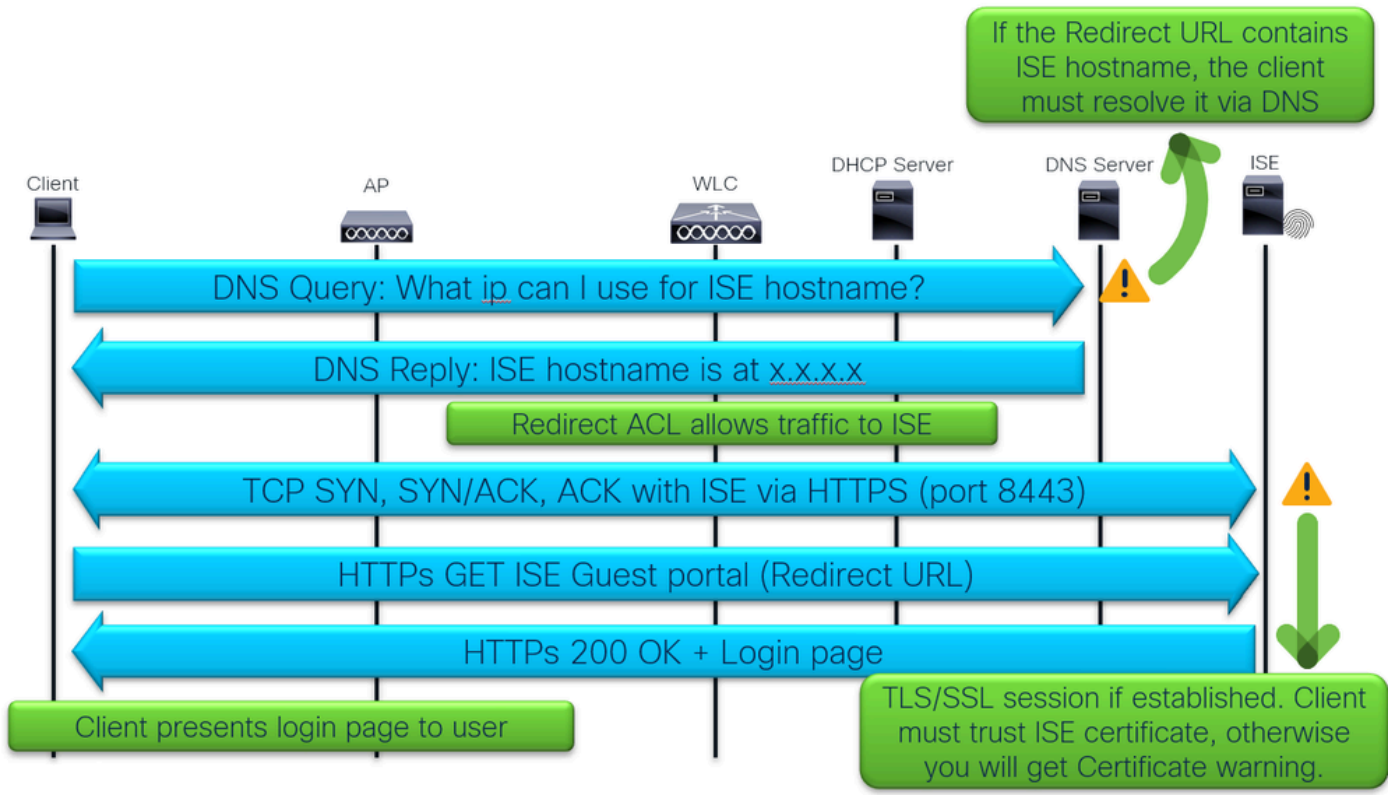
- الكروم = clients3.google.com
- Firefox = detectportal.firefox.com

اعتراض حركة المرور وإعادة التوجيه:



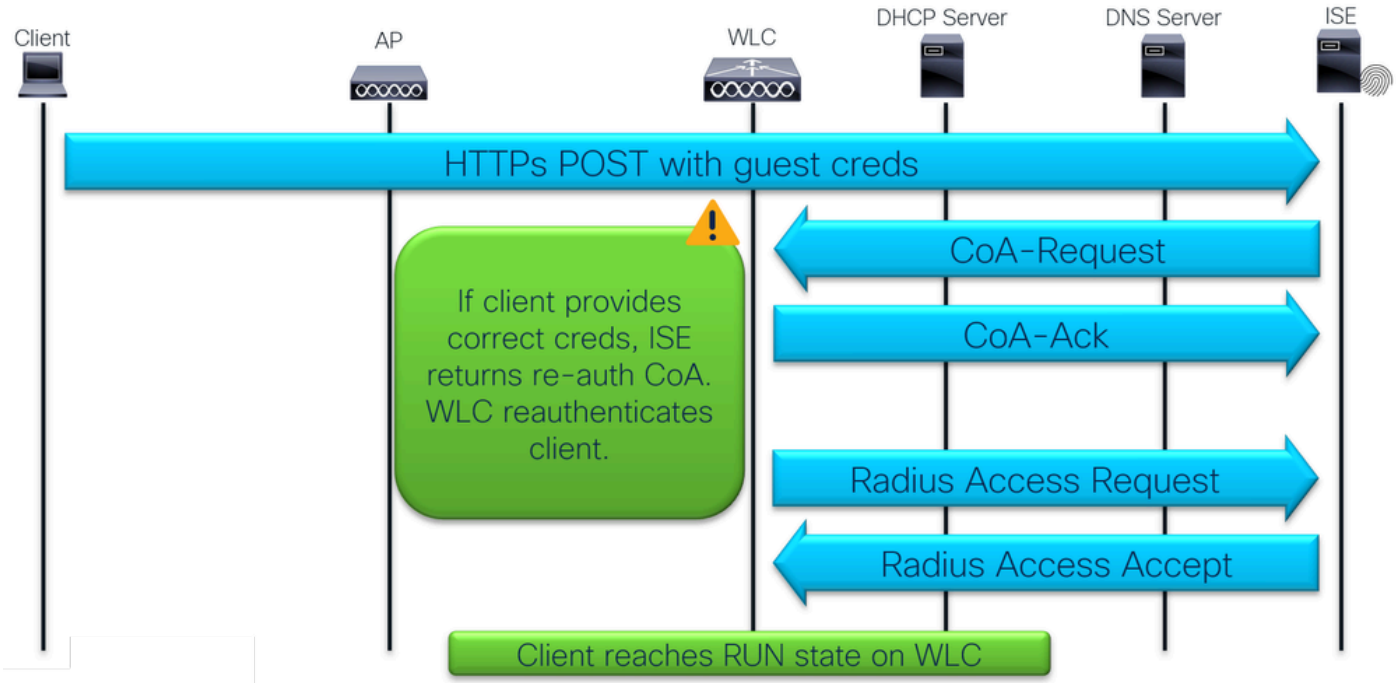
اعتراض حركة المرور وإعادة توجيهها

تسجيل دخول العميل إلى بوابة تسجيل دخول ضيف ISE:



تسجيل دخول العميل إلى بوابة تسجيل دخول ضيف ISE

تسجيل دخول العميل وتسجيل CoA:

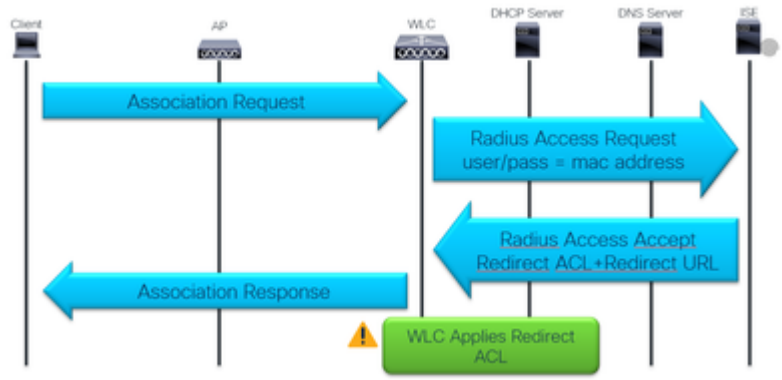


تسجيل دخول العميل وتسجيل CoA

استكشاف الأخطاء وإصلاحها

الأعراض الشائعة: لم يتم إعادة توجيه المستخدم إلى صفحة تسجيل الدخول.

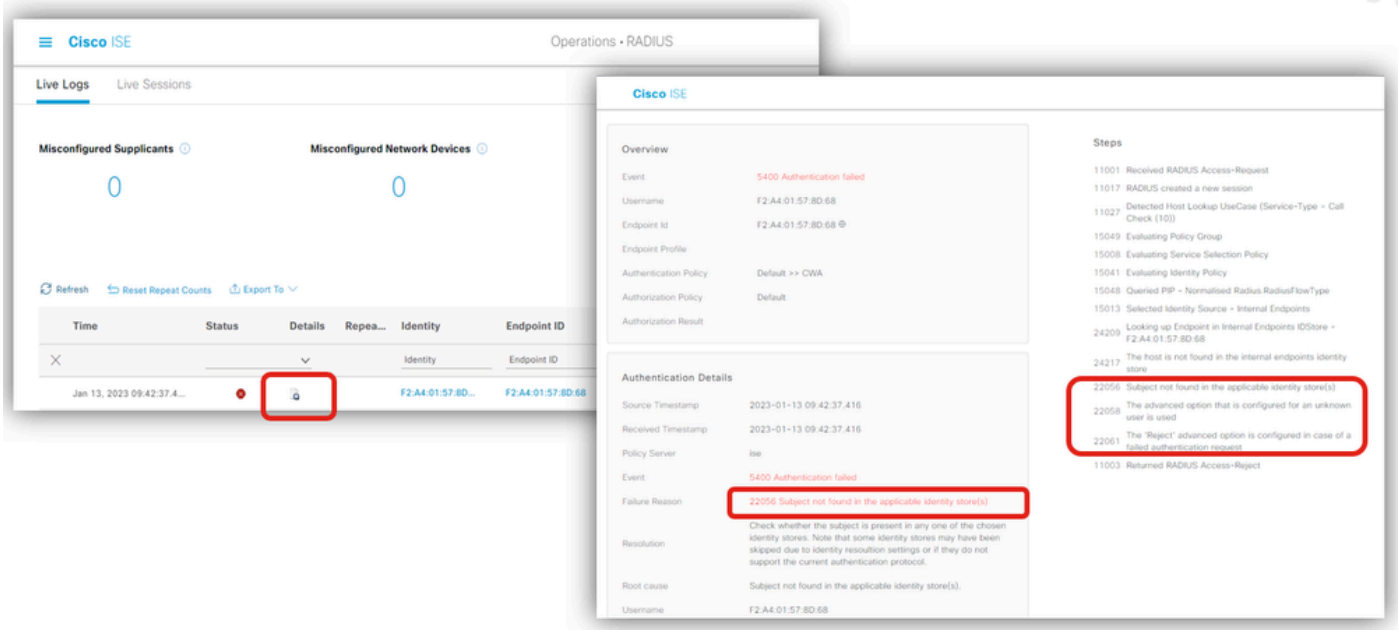
فلنبدأ بالجزء الأول من التدفق:



أول اقتران ومصادقة RADIUS

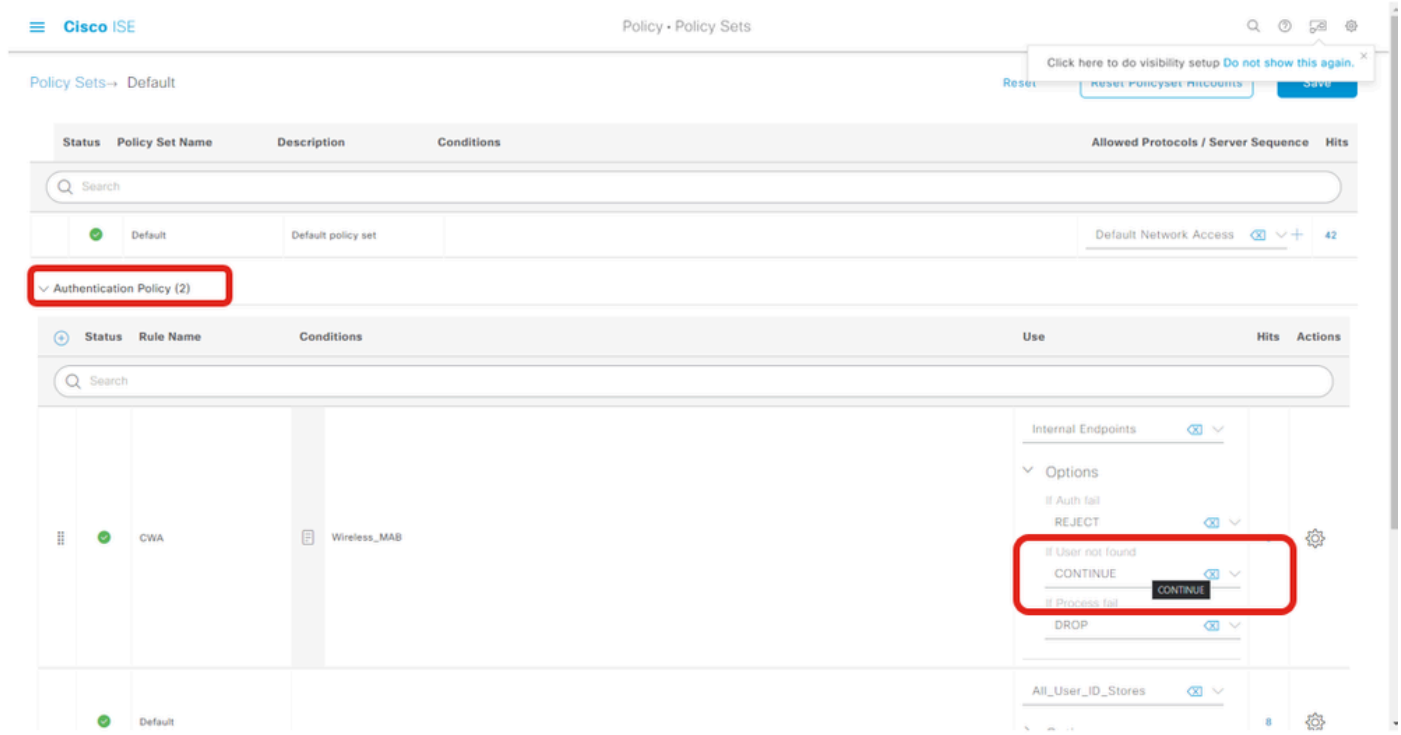
1 - هل نجحت مصادقة RADIUS الأولى؟

تحقق من نتيجة مصادقة تصفية MAC:



سجلات ISE Live التي تظهر نتيجة مصادقة تصفية MAC

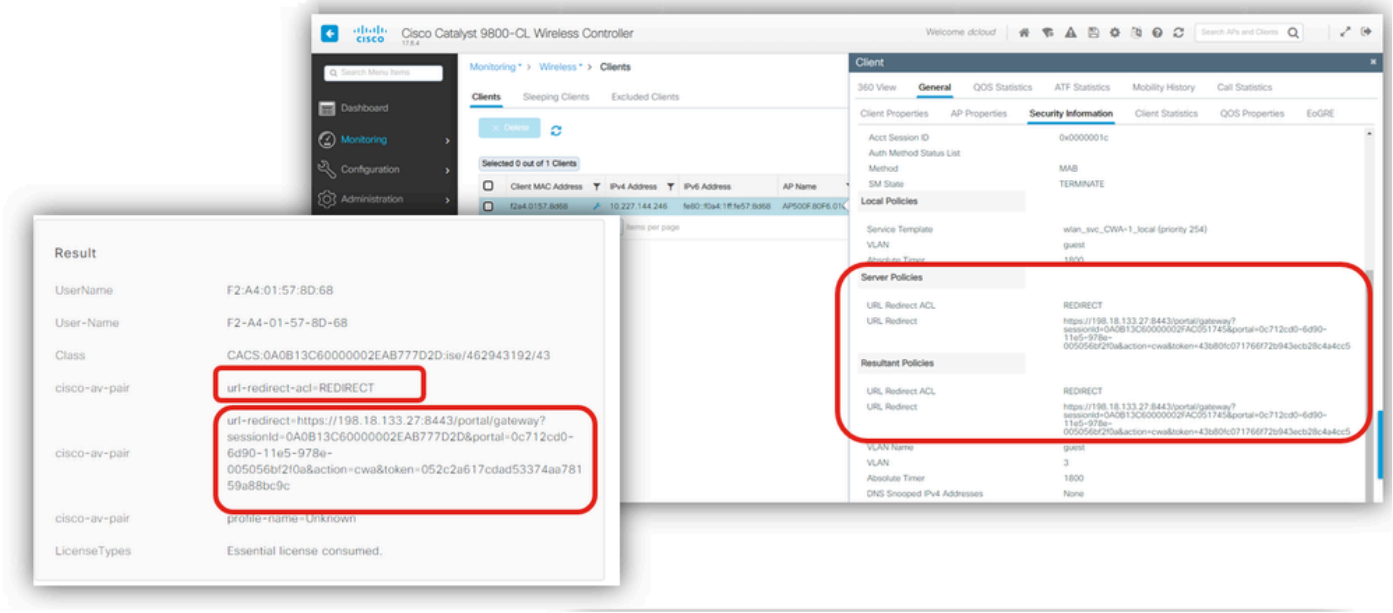
تأكد من تعيين الخيار المتقدم للمصادقة على "متابعة" إذا لم يعثر المستخدم على:



لم يتم العثور على خيار متقدم للمستخدم

2 - هل تتلقى لجنة التحكم في الشبكة المحلية اللاسلكية عنوان URL المعاد توجيهه وقوائم التحكم في الوصول (ACL)؟

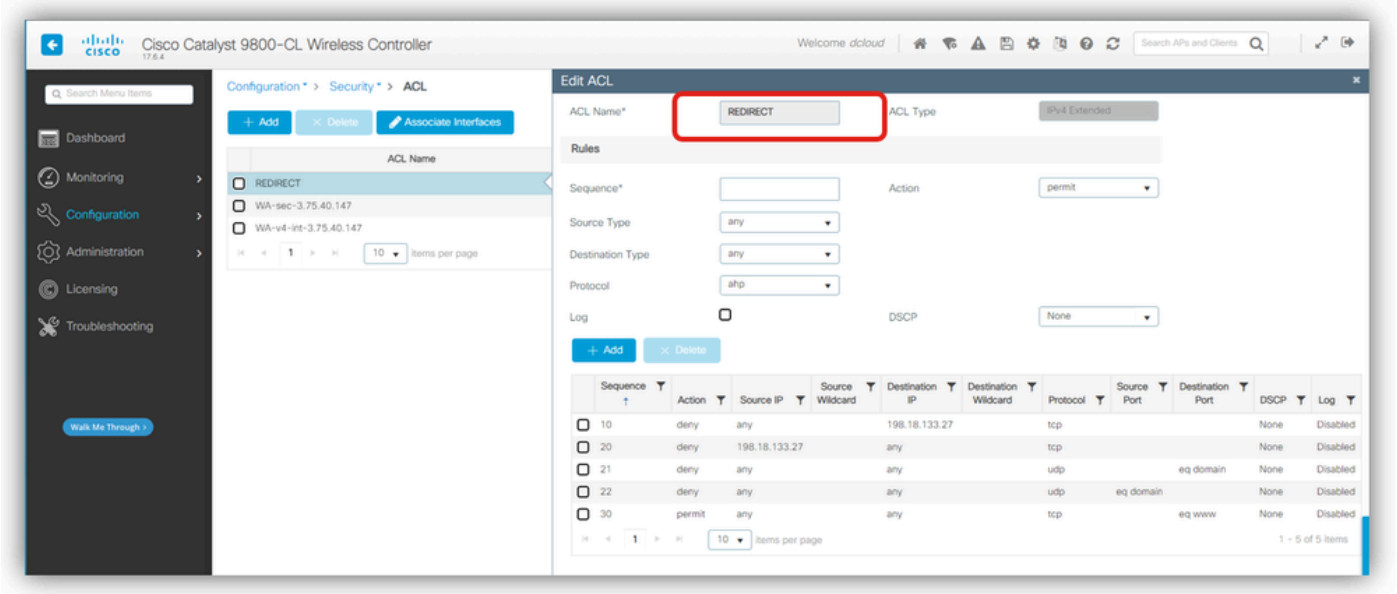
تحقق من سجلات ISE المباشرة ومعلومات أمان عميل WLC تحت المراقبة تحقق من أن ISE يرسل عنوان URL إعادة التوجيه وقائمة التحكم في الوصول في قبول الوصول ويتم إستلامه بواسطة WLC ويتم تطبيقه على العميل في تفاصيل العميل:



إعادة توجيه قائمة التحكم في الوصول (ACL) و URL

3 - هل قائمة التحكم في الوصول (ACL) المعاد توجيهها صحيحة؟

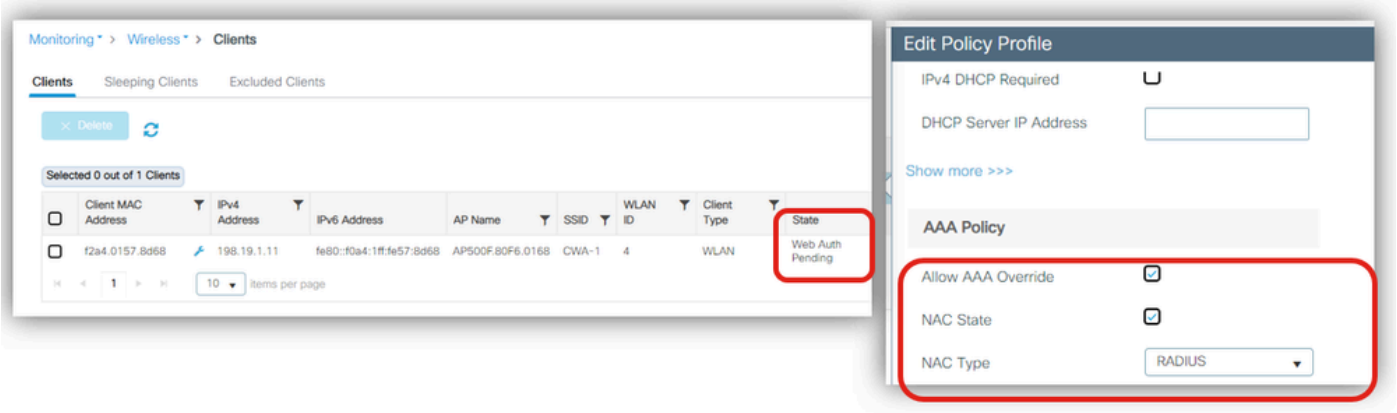
تحقق من اسم قائمة التحكم بالوصول (ACL) لأي خطأ مطبعي. تأكد من أنها تمامًا مثل التي أرسلها ISE:



التحقق من قائمة التحكم في الوصول (ACL) المعاد توجيهها

4 - هل تم نقل العميل إلى Web-Auth معلق؟

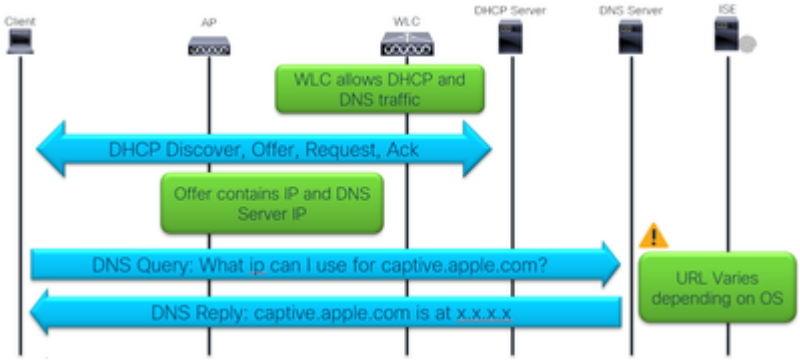
تحقق من تفاصيل العميل للحالة "تعليق مصادقة ويب". إذا لم يكن في هذه الحالة، فتحقق من تمكين تجاوز AAA و Radius NAC في ملف تعريف السياسة:



تفاصيل العميل وتجاوز المصادقة والتفويض والمحاسبة (AAA) و RADIUS NAC

ما زلت لا تعمل؟

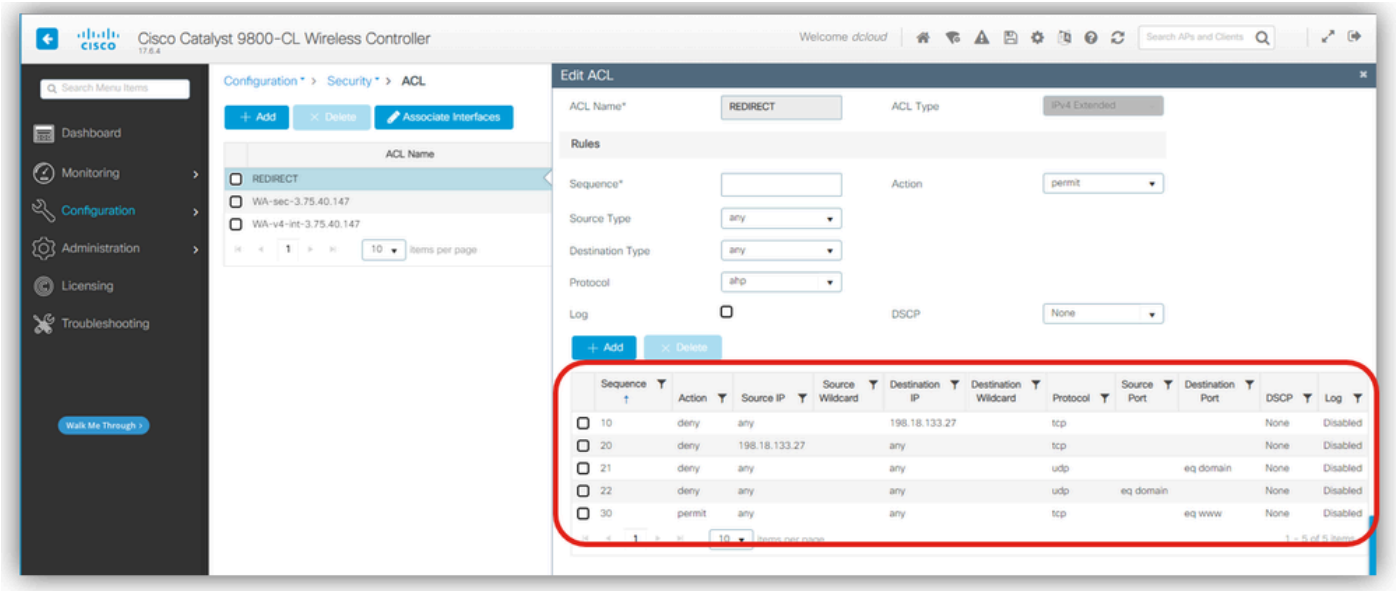
دعنا نعيد النظر في التدفق...



فحص DHCP و DNS والاتصال

5 - هل تسمح وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بحركة مرور بيانات DHCP و DNS؟

تحقق من إعادة توجيه محتويات قائمة التحكم في الوصول (ACL) في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC):



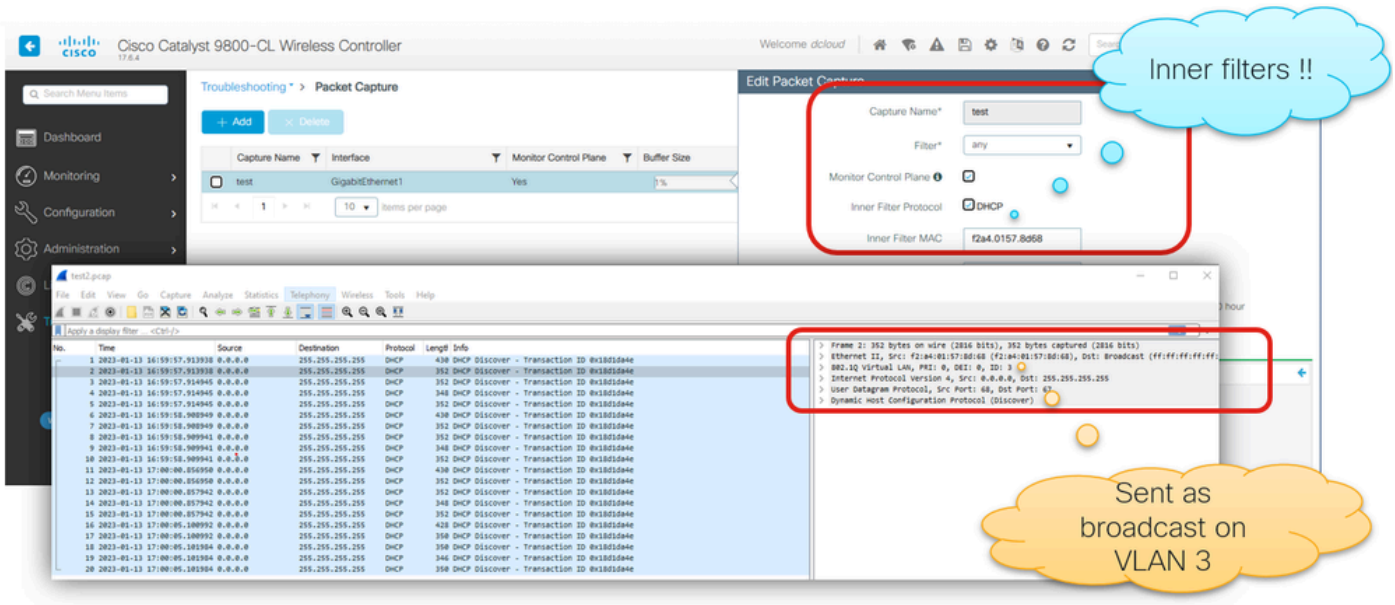
تحدد قائمة التحكم في الوصول (ACL) المعاد توجيهها حركة المرور التي يتم اعتراضها وإعادة توجيهها بواسطة بيان الترخيص وحركة المرور التي يتم تجاهلها من الاعتراض وإعادة التوجيه باستخدام بيان الرفض.

في هذا المثال، نسمح بتدفق بيانات DNS وحركة المرور إلى/من عنوان ISE IP، واعتراض أي حركة مرور لـ TCP على المنفذ 80 (www).

6 - هل يستقبل خادم DHCP اكتشاف/طلب DHCP؟

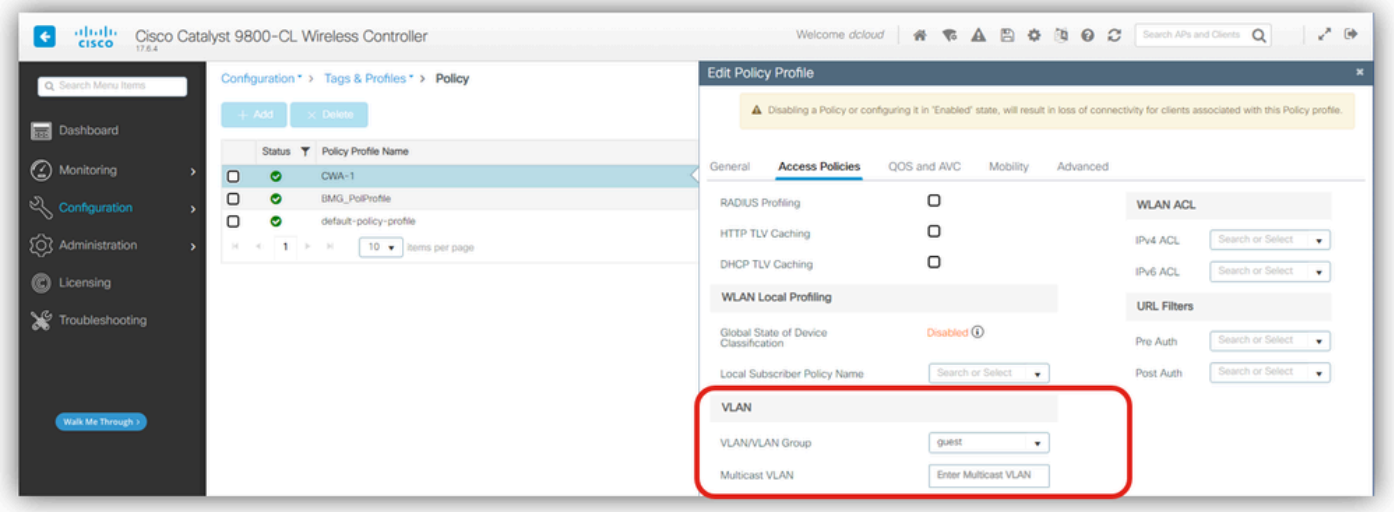
تحقق مع EPC إذا حدث تبادل DHCP. يمكن إستخدام EPC مع المرشحات الداخلية مثل برووتوكول DHCP و/أو Internal Filter MAC حيث يمكننا إستخدام عنوان MAC لجهاز العميل ونحصل على حزم EPC التي يتم إرسالها بواسطة عنوان MAC لجهاز العميل أو إرسالها إليه فقط.

في هذا المثال، يمكننا رؤية الحزم DHCP Discover التي يتم إرسالها كبث على شبكة VLAN رقم 3:



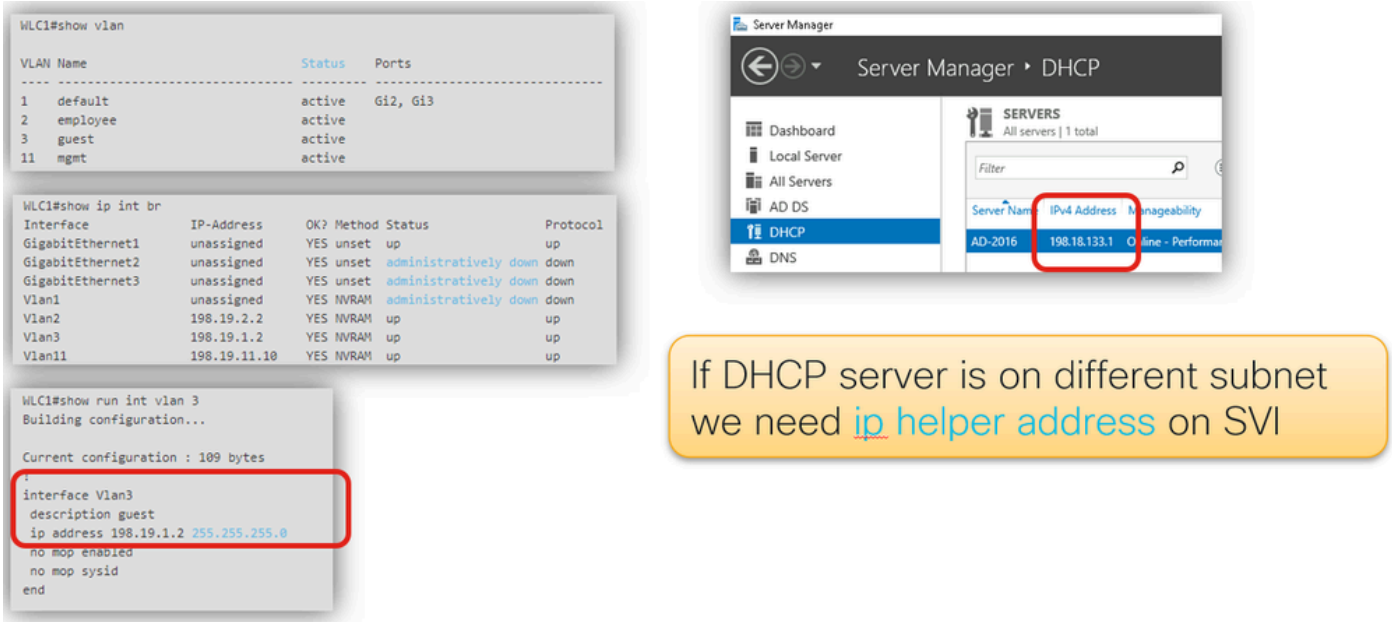
WLC EPC للتحقق من DHCP

تأكيد شبكة VLAN الخاصة بالعميل المتوقع في ملف تعريف النهج:



VLAN في ملف تعريف السياسة

دققت WLC VLAN و switchport شنطة تشكيل و DHCP subnet:



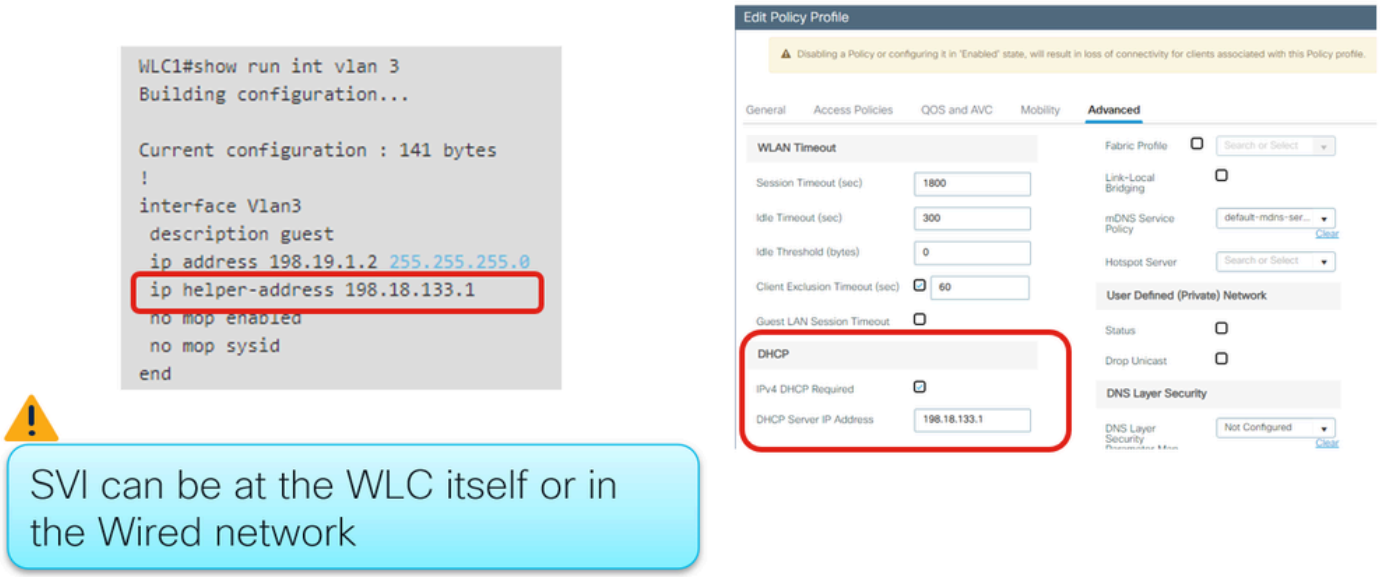
VLAN و switchport وشبكة DHCP الفرعية

يمكن أن نرى أن VLAN 3 يتواجد في ال WLC وهو أيضا يتلقى SVI ل VLAN 3، غير أن عندما نحن دققت ال DHCP نادل عنوان، وه على شبكة فرعية مختلف، لذلك نحن بحاجة ip مساعد عنوان على ال SVI.

تتطلب أفضل الممارسات تكوين SVI للشبكات الفرعية للعملاء في البنية الأساسية السلكية وتجنبها في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

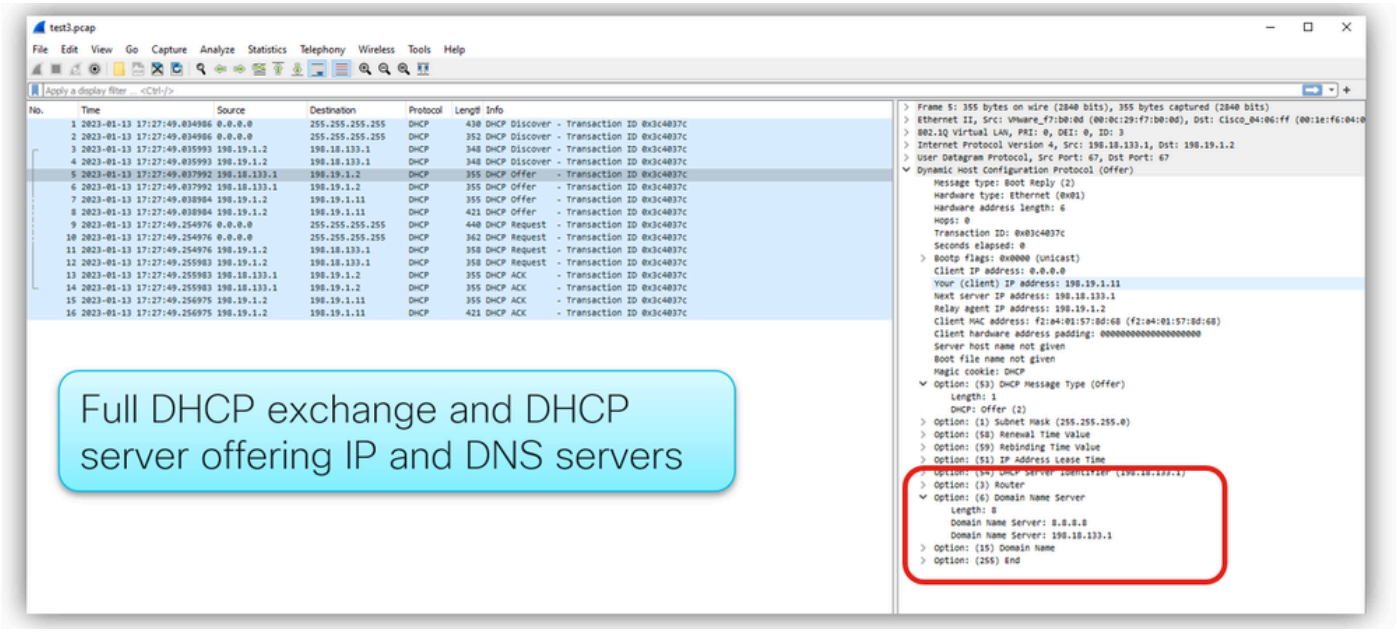
في أي من الحالات، يلزم إضافة الأمر ip helper-address إلى SVI بغض النظر عن مكان وجوده.

البديل هو تكوين عنوان IP لخادم DHCP في ملف تعريف السياسة:



عنوان مساعد IP في SVI أو ملف تعريف السياسة

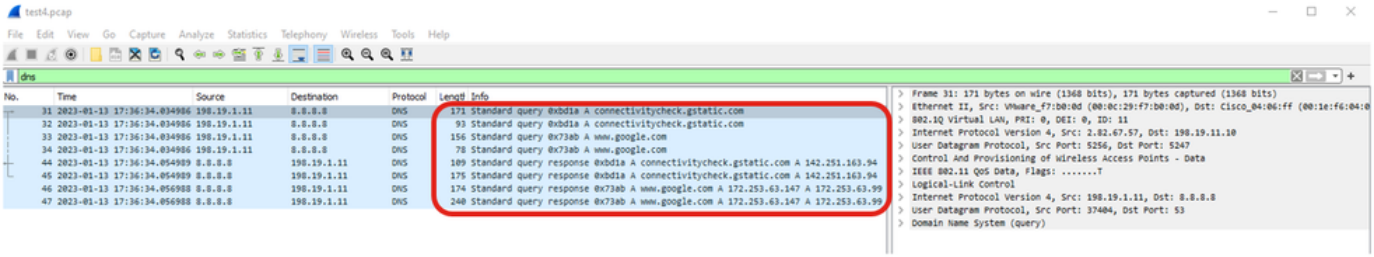
يمكنك بعد ذلك التحقق باستخدام EPC إذا كان تبادل DHCP الآن موافق وإذا كان خادم DHCP يوفر IP (عنوانين) DNS server:



تفاصيل عرض DHCP لخادم DNS

7 - هل تحدث إعادة التوجيه التلقائية؟

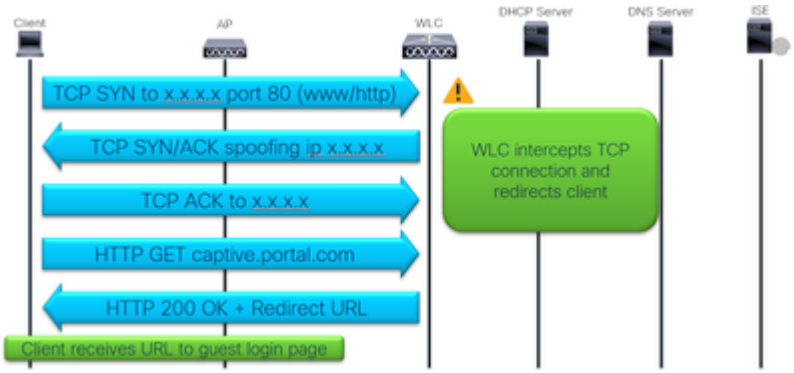
التحقق باستخدام WLC EPC إذا رد خادم DNS على الاستعلامات:



- إذا لم تكن عملية إعادة التوجيه تلقائية، فافتح المستعرض وحاول إستخدام عنوان IP عشوائي. على سبيل المثال، 10.0.0.1.
- إذا كانت عملية إعادة التوجيه تعمل، فمن المحتمل أن تكون لديك مشكلة في حل DNS.

ما زلت لا تعمل؟

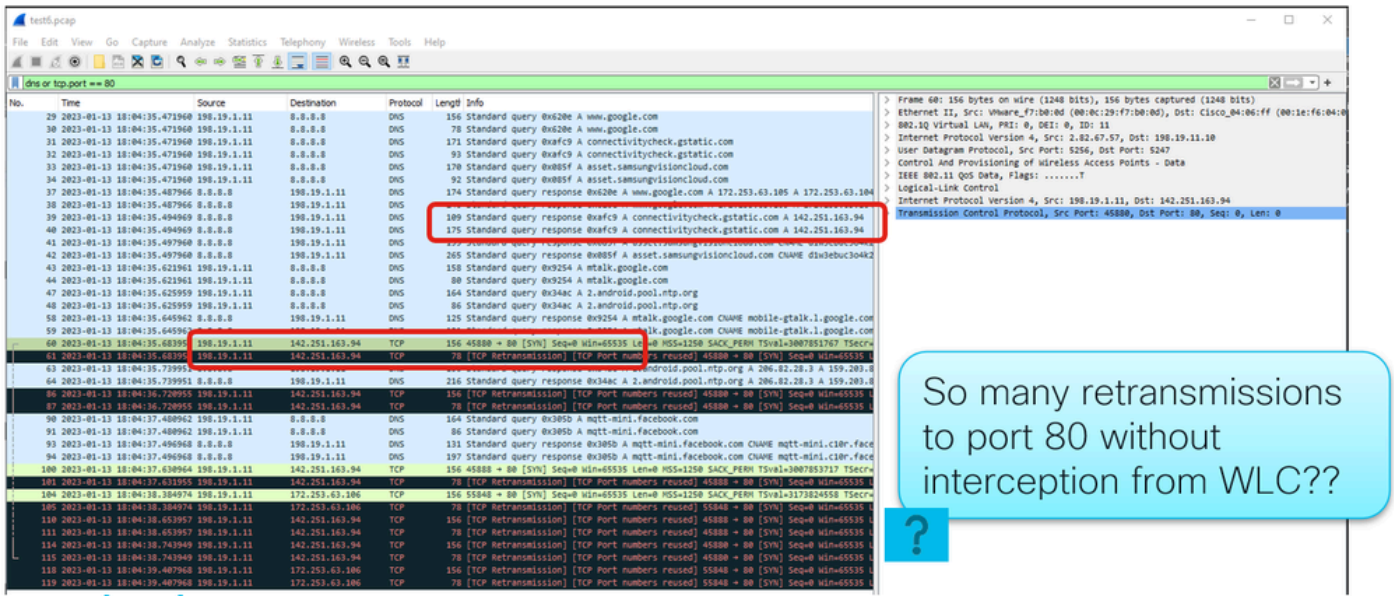
دعنا نعيد النظر في التدفق...



اعتراض حركة المرور وإعادة توجيهها

8 - لا يظهر المستعرض صفحة تسجيل الدخول؟

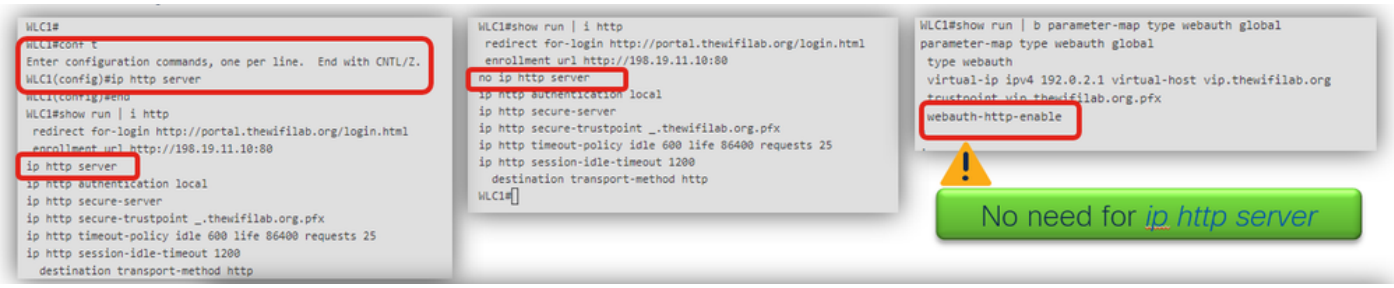
تحقق مما إذا كان العميل يرسل نظام TCP إلى المنفذ 80 ويقوم WLC باعتراضه:



عمليات إعادة إرسال بروتوكول TCP إلى المنفذ 80

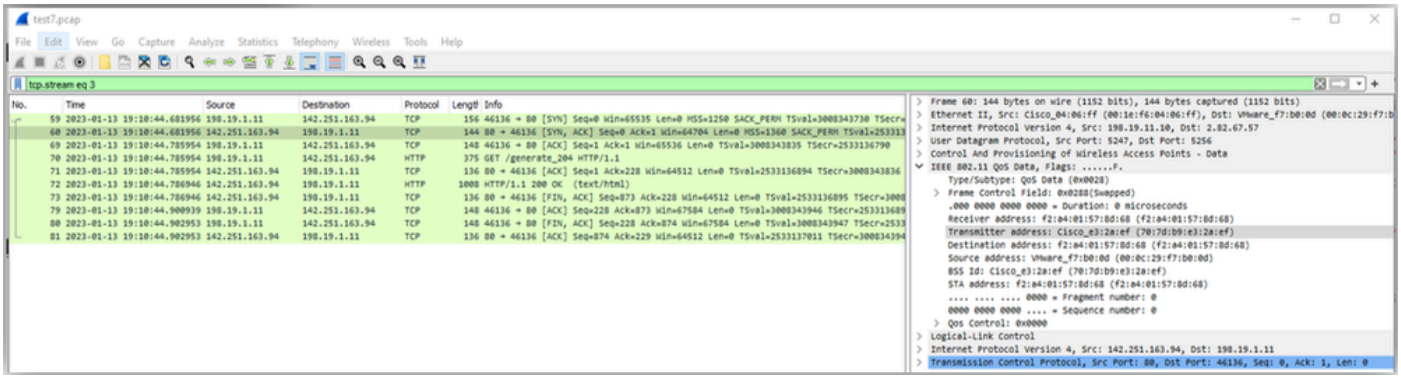
هنا يمكننا أن نرى أن العميل يرسل حزم TCP syn إلى المنفذ 80 ولكنه لا يحصل على أي رد ويقوم بإعادة إرسال TCP.

تأكد من أن لديك الأمر ip http server في التكوين العام أو webAuth-http-enable في parameter-map global:



أوامر اعتراض HTTP

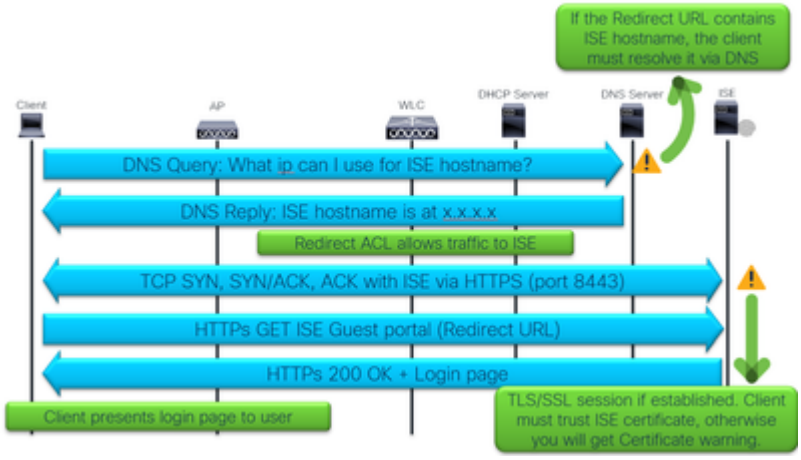
بعد الأمر، تعترض WLC بروتوكول TCP وتنتهك عنوان IP للوجهة للرد على العميل وإعادة التوجيه.



اعتراض TCP بواسطة WLC

ما زلت لا تعمل؟

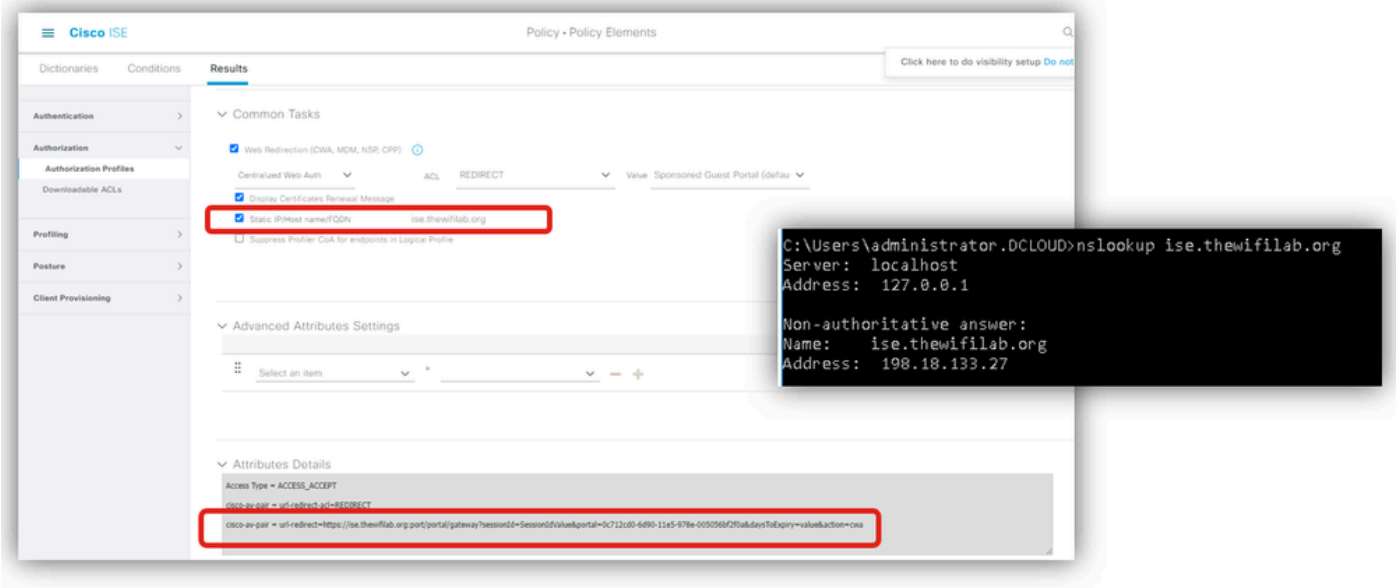
هناك المزيد في التدفق...



تسجيل دخول العميل إلى بوابة تسجيل دخول ضيف ISE

9 - هل يمكن للعميل حل اسم المضيف ISE؟

تحقق مما إذا كان عنوان URL لإعادة التوجيه يستخدم IP أو اسم المضيف وما إذا كان العميل يقوم بحل اسم المضيف ISE:

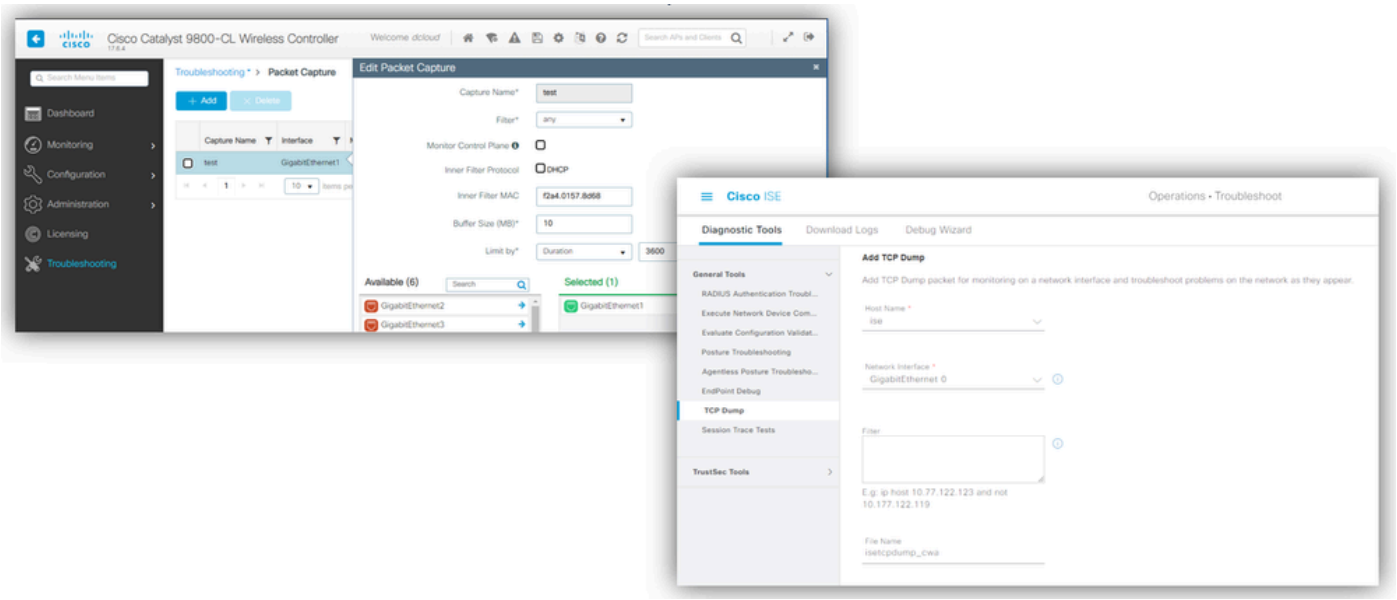


دقة اسم المضيف ل ISE

تظهر مشكلة مشتركة عندما يحتوي عنوان URL لإعادة التوجيه على اسم المضيف ISE، ومع ذلك يتعذر على جهاز العميل حل اسم المضيف هذا إلى عنوان IP الخاص ب ISE. إذا تم إستخدام اسم المضيف، تأكد من أنه قابل للحل عبر DNS.

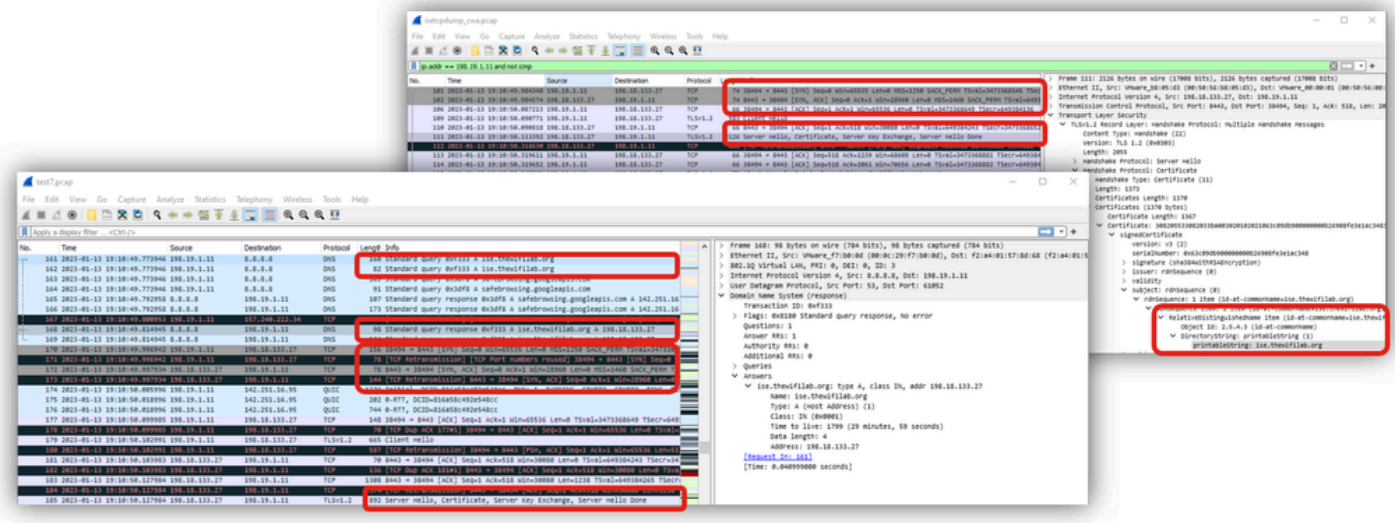
10 - هل ما زالت صفحة تسجيل الدخول لا تحمل؟

تحقق من خلال WLC EPC و ISE TCPdump إذا وصلت حركة مرور العميل إلى ISE PSN. تكوين عمليات الالتقاط وبدء تشغيلها على WLC و ISE:



WLC EPC و ISE TCPDump

بعد نسخ المشكلة، قم بجمع عمليات الالتقاط وربط حركة المرور. هنا يمكن أن نرى ISE hostname حللت وبعد ذلك الاتصال بين العميل و ISE على ميناء 8443:



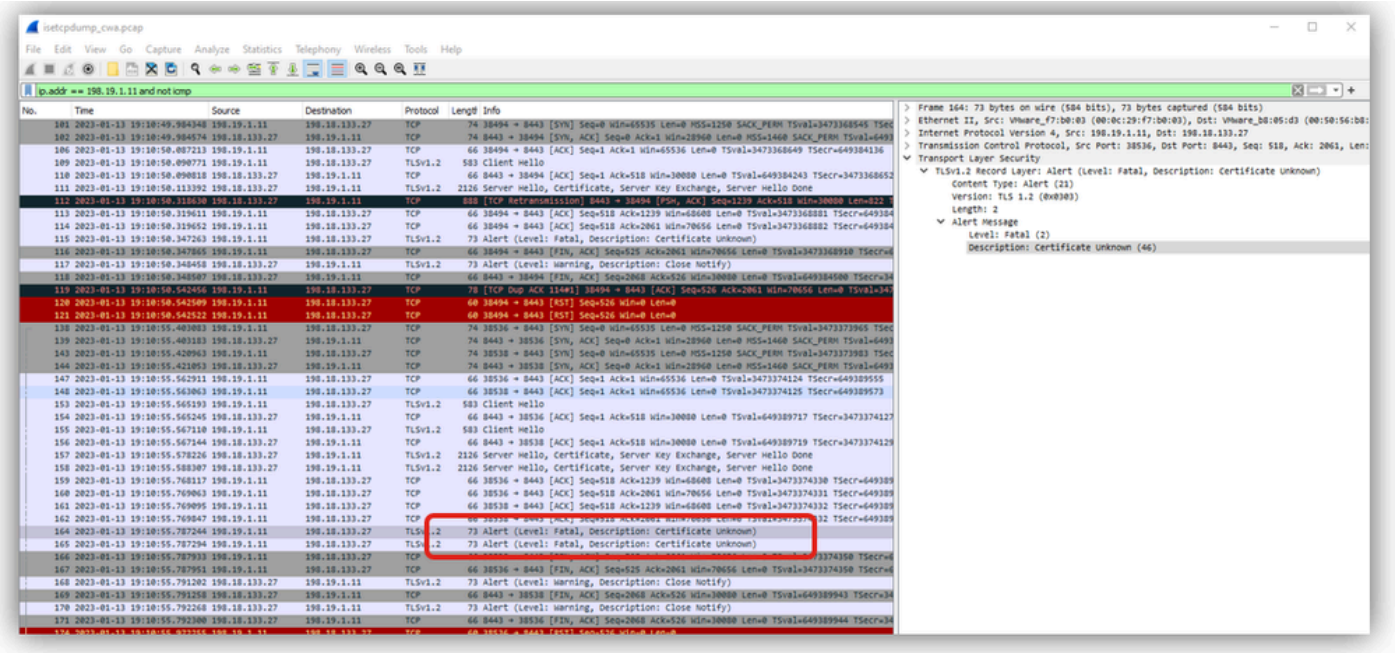
حركة مرور WLC و ISE

11 - لماذا نحصل على انتهاك للأمان بسبب الشهادة؟

إذا كنت تستخدم شهادة موقعة ذاتيا على ISE، فمن المتوقع أن يقوم العميل بتوجيه تحذير أمان عند محاولة تقديم صفحة تسجيل دخول ISE Portal.

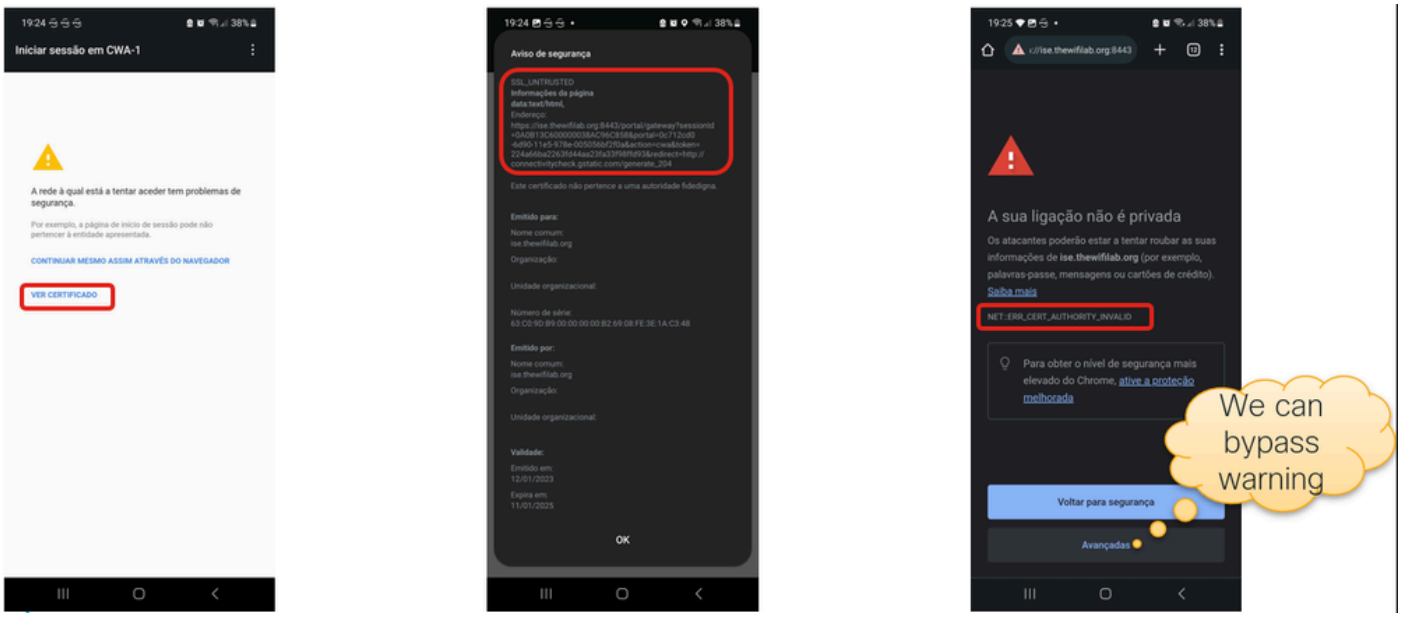
على WLC EPC أو ISE TCPdump يمكننا التحقق مما إذا كانت شهادة ISE موثوق بها.

في هذا المثال، يمكننا رؤية اتصال إغلاق من عميل مع تنبيه (المستوى: ميت، الوصف: الشهادة غير معروفة) مما يعني أن شهادة ISE غير معروفة (موثوق بها):



شهادة ISE غير الموثوق بها

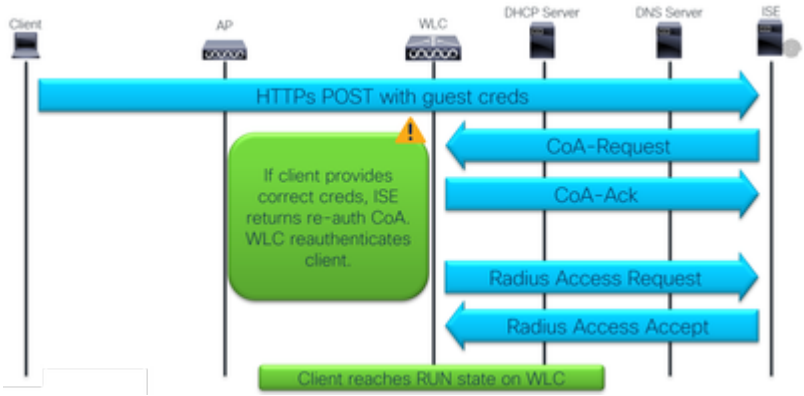
إذا قمنا بالتحقق من جانب العميل، فسنرى الأمثلة التالية للمخرجات:



جهاز العميل الذي ال يثق بشهادة ISE

أخيرا، إعادة التوجيه تعمل!! لكن تسجيل الدخول يفشل...

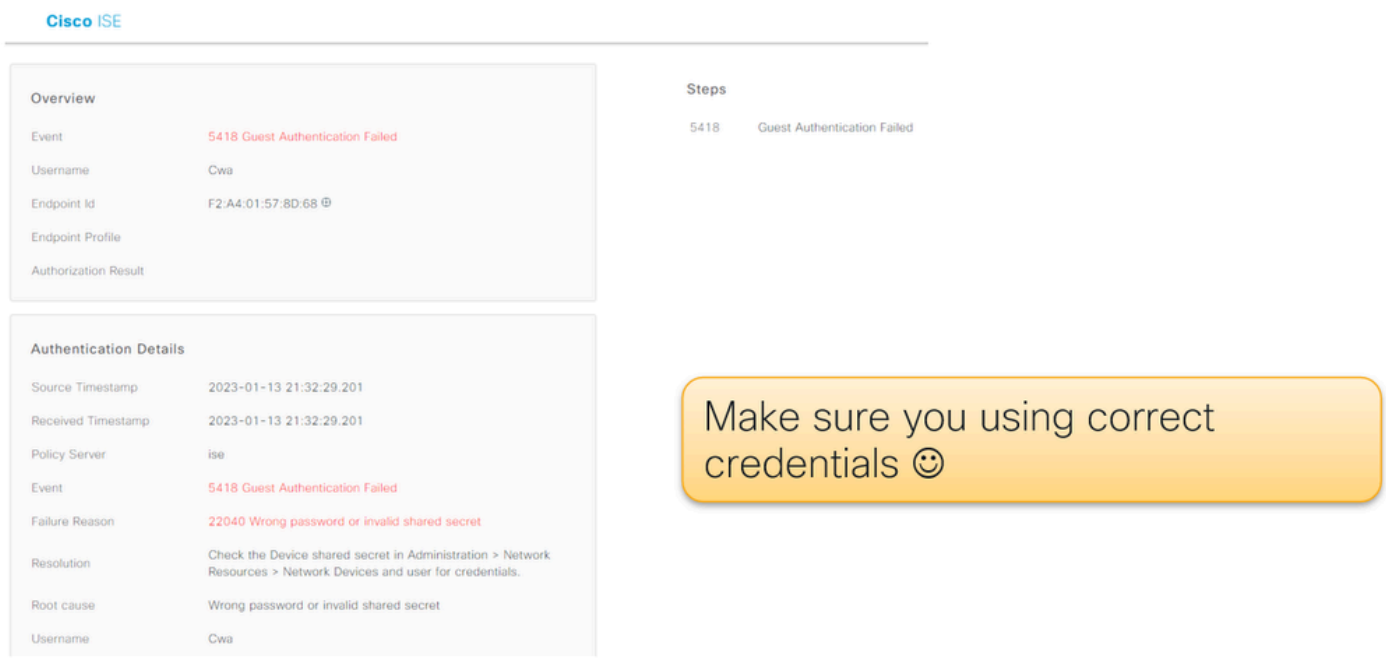
آخر مرة يتم فيها التحقق من التدفق...



تسجيل دخول العميل وتسجيل CoA

12 - فشل تسجيل دخول الضيوف؟

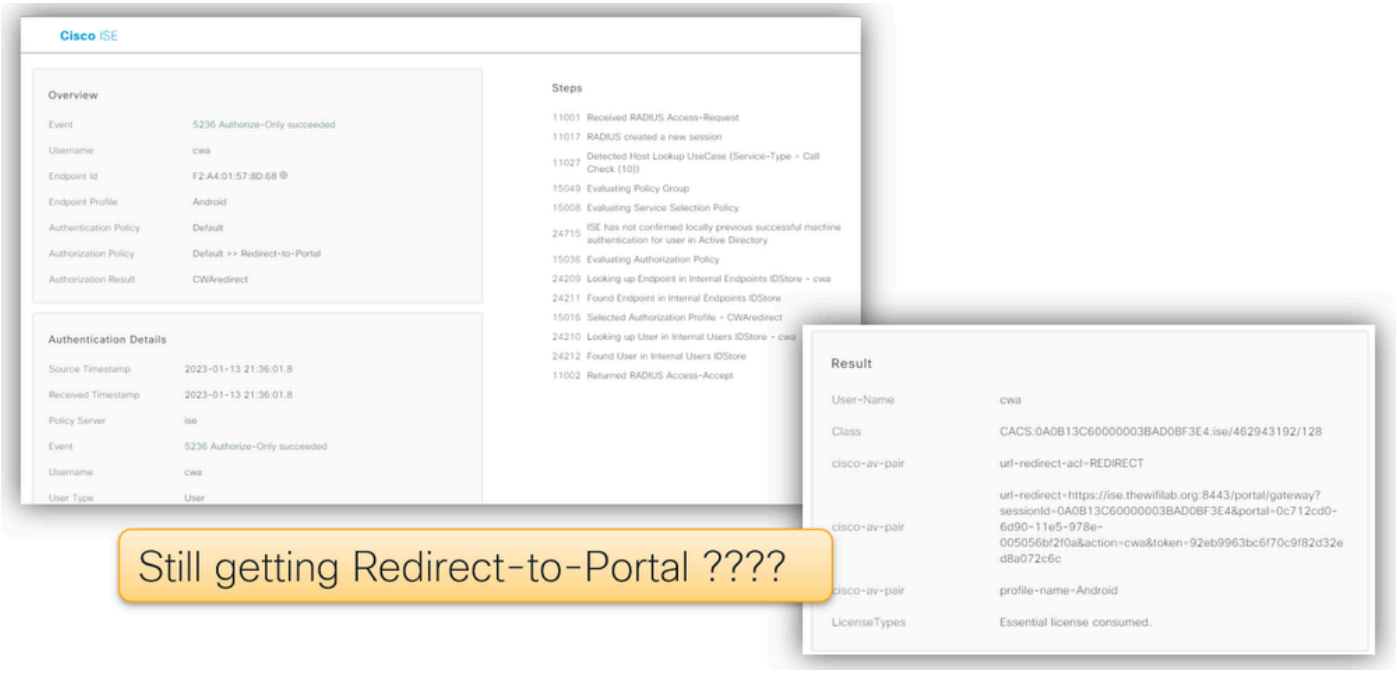
تحقق من سجلات ISE بحثا عن مصادقة فاشلة. تأكد من صحة بيانات الاعتماد.



فشلت مصادقة الضيف بسبب بيانات اعتماد غير صحيحة

13 - هل نجحت عملية تسجيل الدخول أم لم تنتقل إلى RUN؟

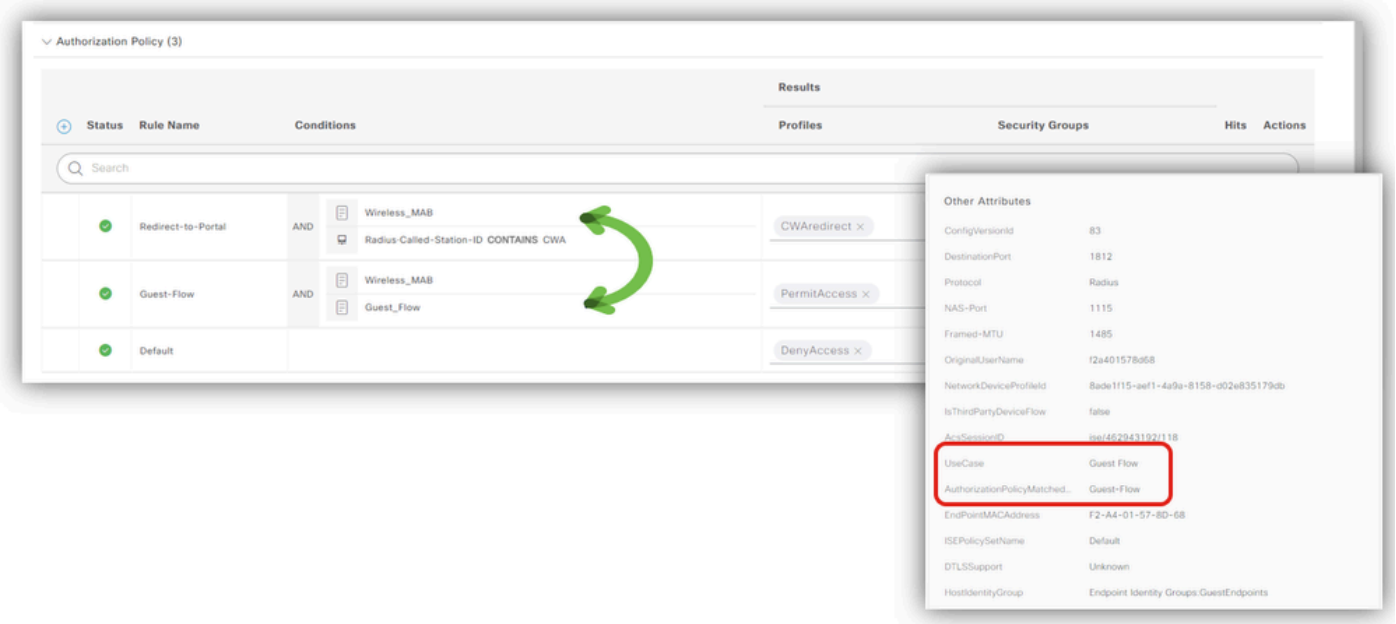
تحقق من سجلات ISE للحصول على تفاصيل المصادقة والنتيجة:



حلقة إعادة التوجيه

في هذا المثال، يمكننا رؤية العميل يحصل مرة أخرى على ملف تعريف التخويل الذي يحتوي على URL لإعادة التوجيه وقوائم التحكم في الوصول (ACL) لإعادة التوجيه. هذا ينتج في إعادة توجيه أنشوطة.

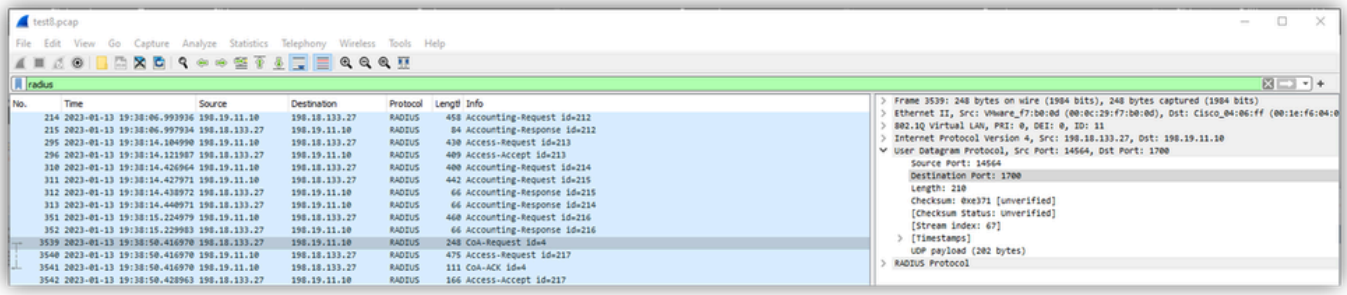
تحقق من مجموعة النهج. يجب أن يكون فحص القاعدة Guest_Flow قبل إعادة التوجيه:



قاعدة Guest_Flow

14 - فشل الكاكاو؟

تحقق مما إذا كان منفذ CoA. يمكنك التحقق من حركة مرور ISE TCPDump و EPC باستخدام CoA (1700) مفتوح بين WLC و ISE. تأكد من التطابقات السريعة المشتركة.



حركة مرور CoA

ملاحظة: في الإصدار 17.4.x والإصدارات الأحدث، تأكد أيضا من تكوين مفتاح خادم CoA عند تكوين خادم RADIUS. أستخدم المفتاح نفسه مثل السر المشترك (هو نفس التقصير على ISE). الغرض هو أن يشكل إختياري مفتاح مختلف ل CoA من المفتاح المشترك إن يكون هذا هو ما قام خادم RADIUS بتكوينه. في Cisco IOS® XE 17.3، أستخدم واجهة مستخدم الويب ببساطة نفس السر المشترك مثل مفتاح CoA.

اعتبارا من الإصدار 17.6.1، يتم دعم RADIUS (بما في ذلك CoA) من خلال هذا المنفذ. إذا كنت ترغب في إستخدام منفذ الخدمة ل RADIUS، فأنت بحاجة إلى هذا التكوين:

<#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
```

القرار

هذه هي قائمة CWA المرجعية المستأنفة:

- تأكد من أن العميل يجلس على شبكة VLAN الصحيحة ويحصل على عنوان IP و DNS.
  - احصل على تفاصيل العميل في عنصر التحكم في الشبكة المحلية

اللاسلكية (WLC) وقم بتشغيل التقاط الحزم لعرض تبادل بروتوكول DHCP.

- تحقق من أنه يمكن للعميل حل أسماء المضيف عبر DNS.
  - اسم مضيف إختبار الاتصال من cmd.
- يجب أن تنصت WLC على المنفذ 80
  - تحقق من الأمر العام ip http server أو أمر خريطة المعلمة العامة webAuth-http-enable.
- للتخلص من تحذير الشهادة، قم بتثبيت شهادة موثوق بها على ISE.
  - لا توجد حاجة لتثبيت شهادة موثوق بها على WLC في CWA.
- نهج المصادقة في الخيار ISE Advanced "متابعة" إذا لم يتم العثور على المستخدم
  - للسماح للمستخدمين الضيوف المدعومين بالاتصال وإعادة توجيه URL وقوائم التحكم في الوصول (ACL).

والأدوات الأساسية المستخدمة في أستكشاف الأخطاء وإصلاحها:

- WLC EPC
  - عوامل التصفية الداخلية: بروتوكول DHCP، عنوان MAC.
- شاشة WLC
  - تحقق من تفاصيل أمان العميل.
- تتبع WLC RA
  - تصحيح الأخطاء بمعلومات تفصيلية على جانب WLC.
- سجلات ISE المباشرة
  - تفاصيل المصادقة.
- ISE TCPDump
  - قم بتجميع التقاط الحزم في واجهة ISE PSN.

المراجع

تكوين المصادقة المركزية للويب (CWA) على Catalyst 9800 WLC و ISE

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).