使用无线局域网控制器(WLC)9800和身份服务引擎(ISE)排除中央Web身份验证(CWA)故障

目录

简介

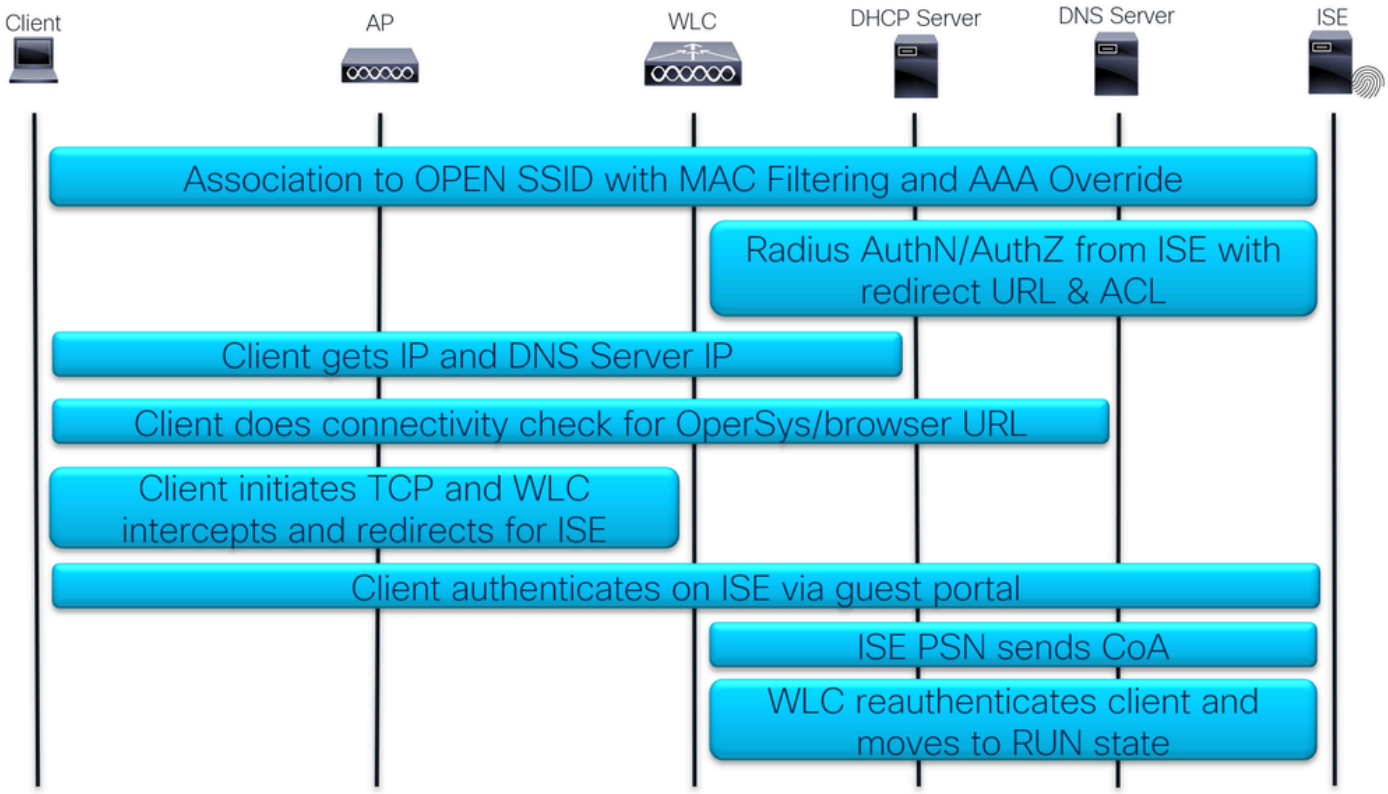
本文档介绍如何对WLC 9800和ISE的集中式Web身份验证(CWA)进行故障排除。

背景信息

目前个人设备非常多，网络管理员寻求无线接入安全时，通常会选择使用CWA的无线网络。
在本文档中，我们将重点介绍CWA的流程图，该流程图有助于排除影响我们的常见问题。
我们将查看该过程的常见陷阱、如何收集与CWA相关的日志、如何分析这些日志，以及如何在WLC上收集嵌入式数据包捕获以确认流量。

CWA是允许用户使用个人设备（也称为BYOD）连接到公司网络的公司最常见的设置。
任何网络管理员都对在打开TAC案例之前解决其问题所要执行的陷阱和故障排除步骤感兴趣。

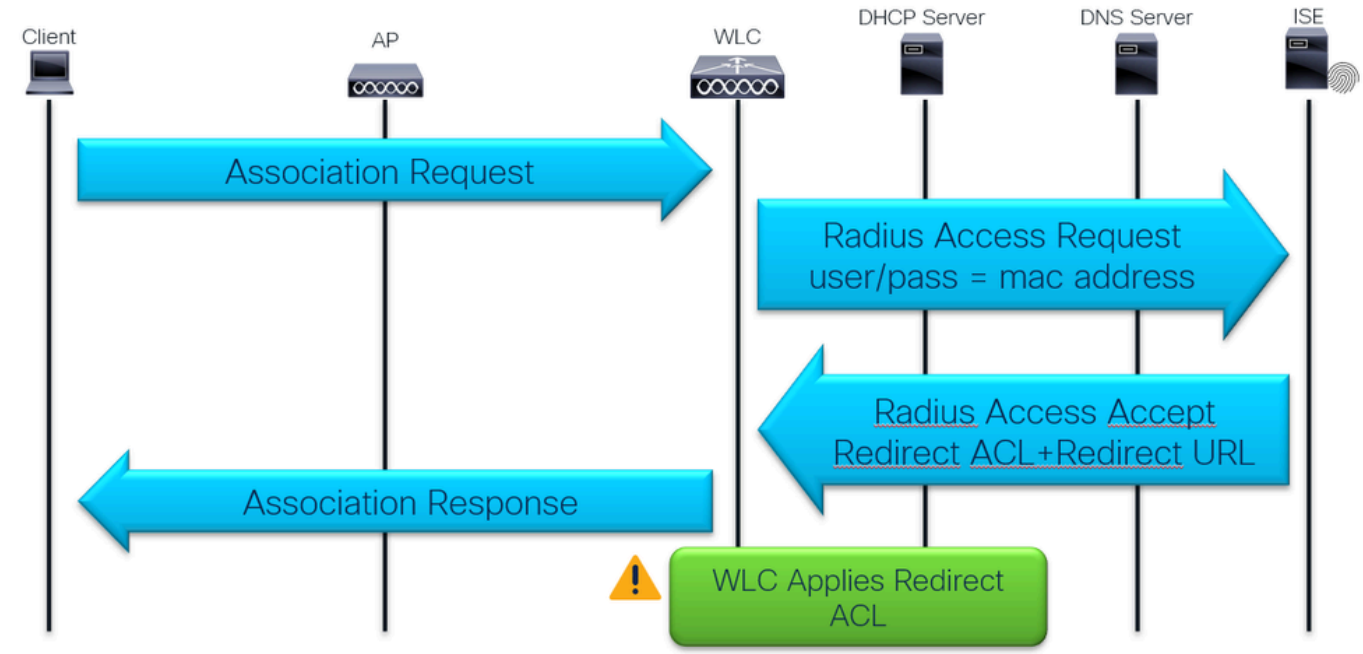
以下是CWA数据包流：



CWA数据包流

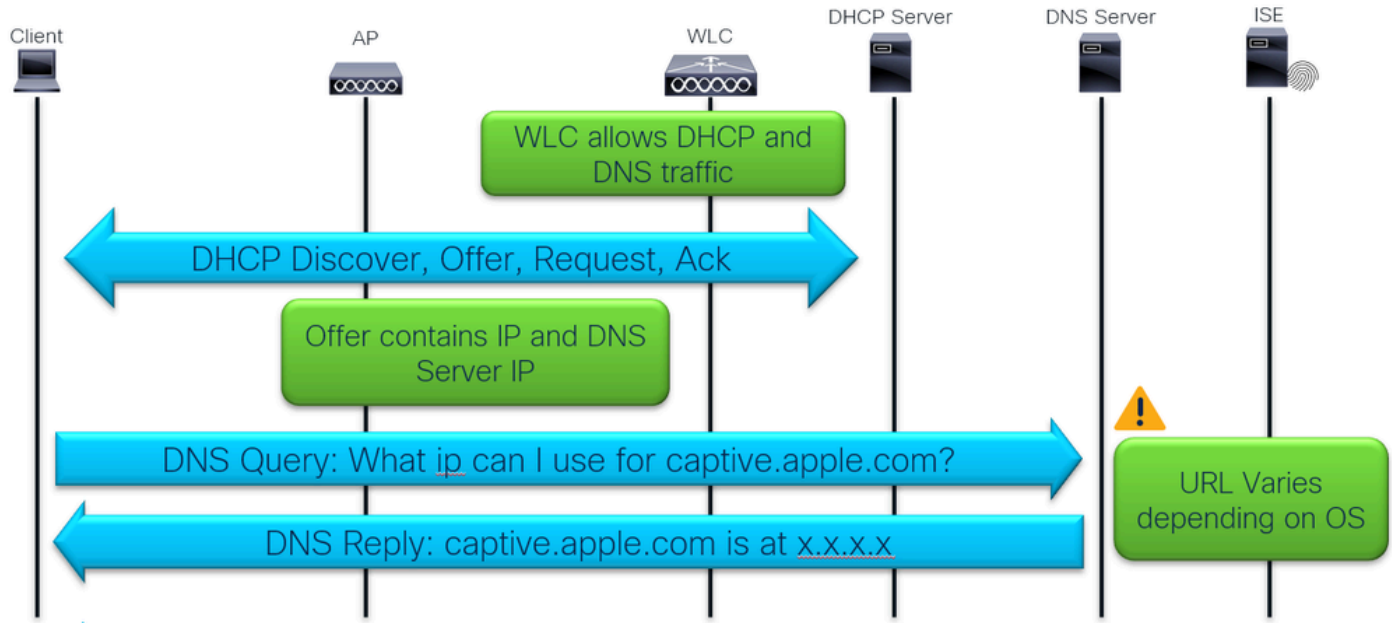
详细流程

首次关联和RADIUS身份验证：



首次关联和RADIUS身份验证

DHCP、DNS和连接检查：



DHCP、DNS和连接检查

连接检查由客户端设备操作系统或浏览器使用强制网络门户检测完成。

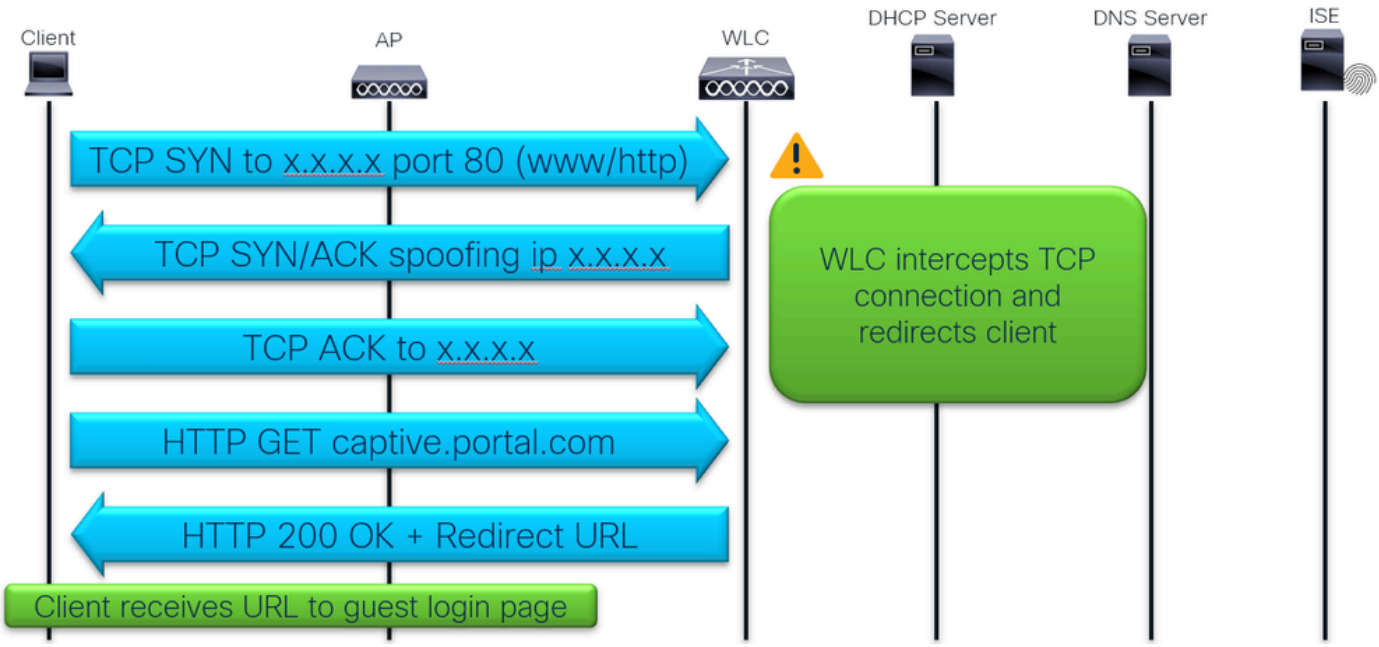
有预编程的设备操作系统可针对特定域执行HTTP GET

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

并且浏览器在打开时也会执行此检查：

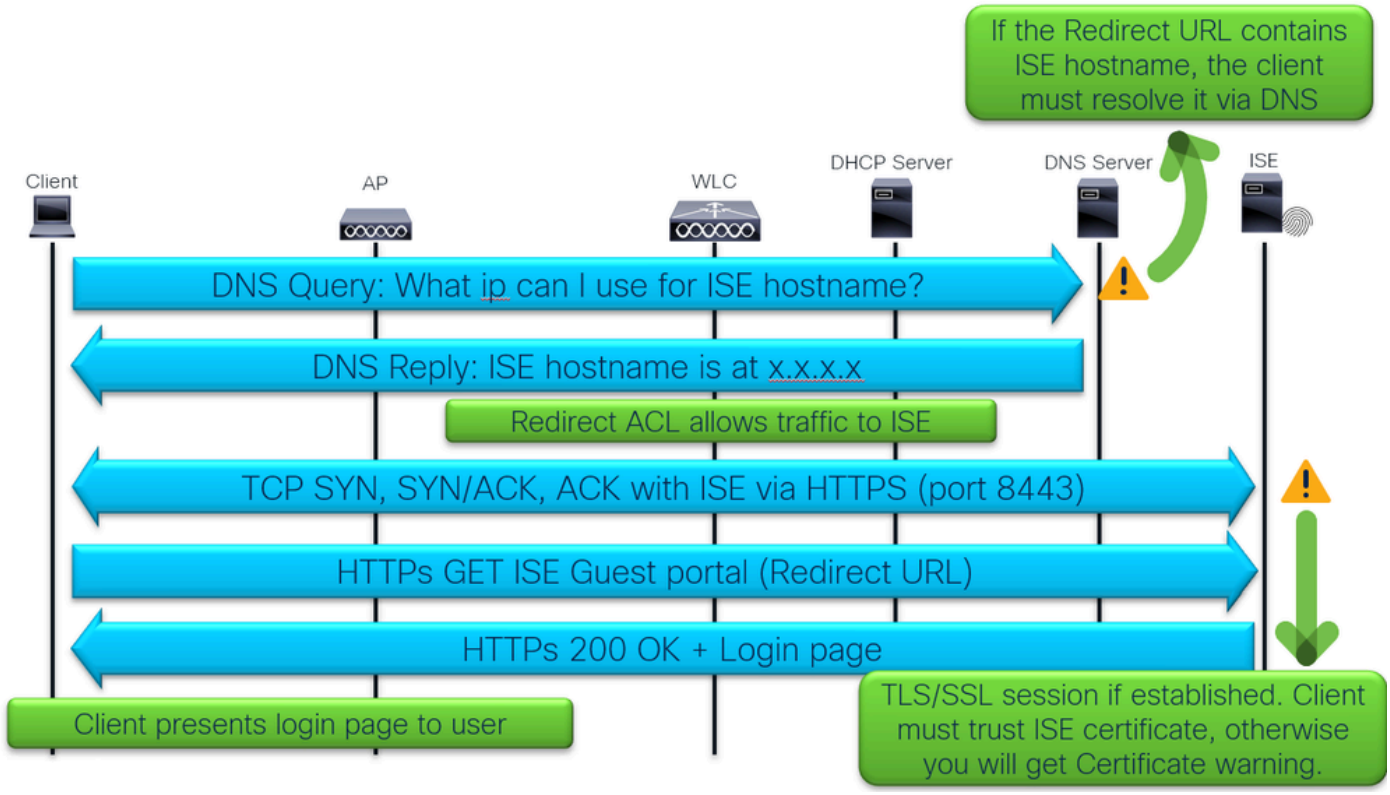
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

流量拦截和重定向：



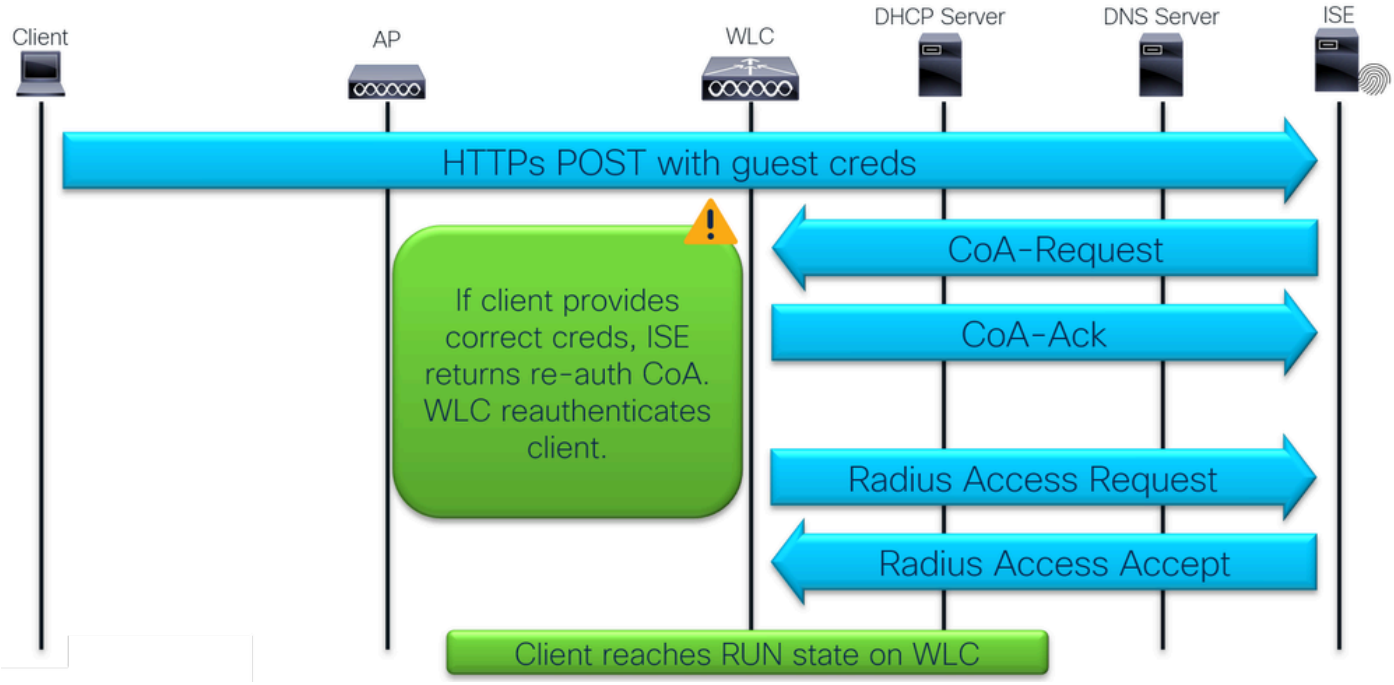
流量拦截和重定向

客户端登录ISE访客登录门户：



客户端登录ISE访客登录门户

客户端登录和CoA:

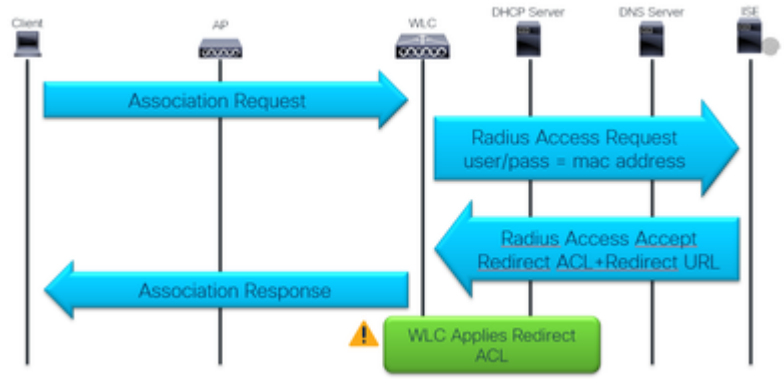


客户端登录和CoA

故障排除

常见症状：用户未重定向到登录页面。

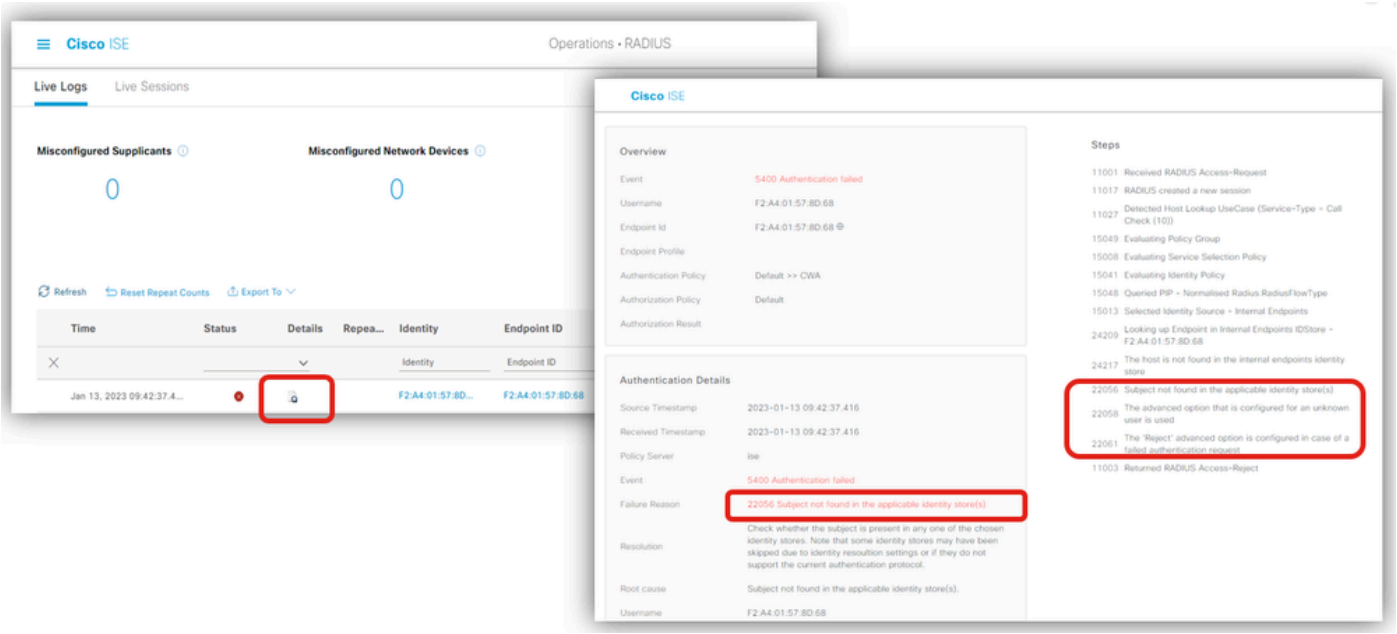
让我们从流程的第一部分开始：



首次关联和RADIUS身份验证

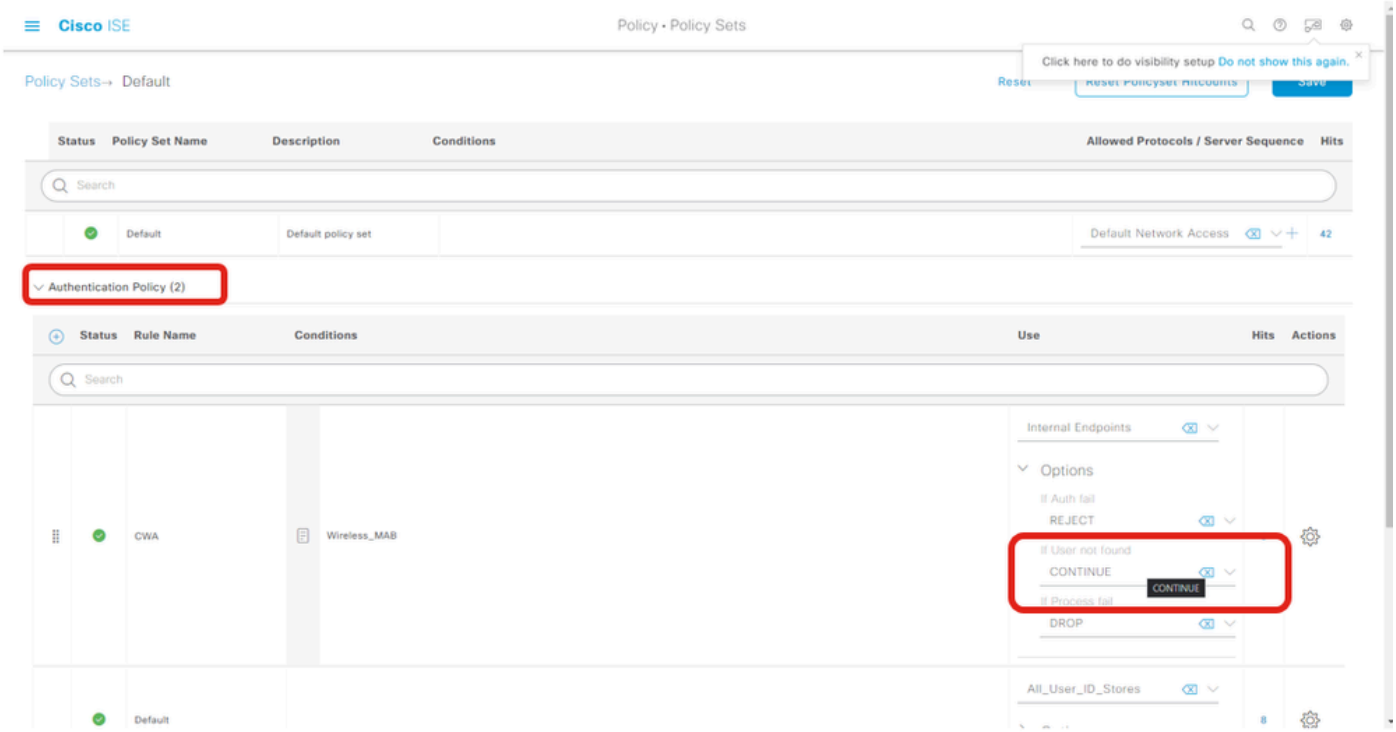
1 — 第一个RADIUS身份验证是否成功？

检查mac过滤身份验证结果：



显示MAC过滤身份验证结果的ISE实时日志

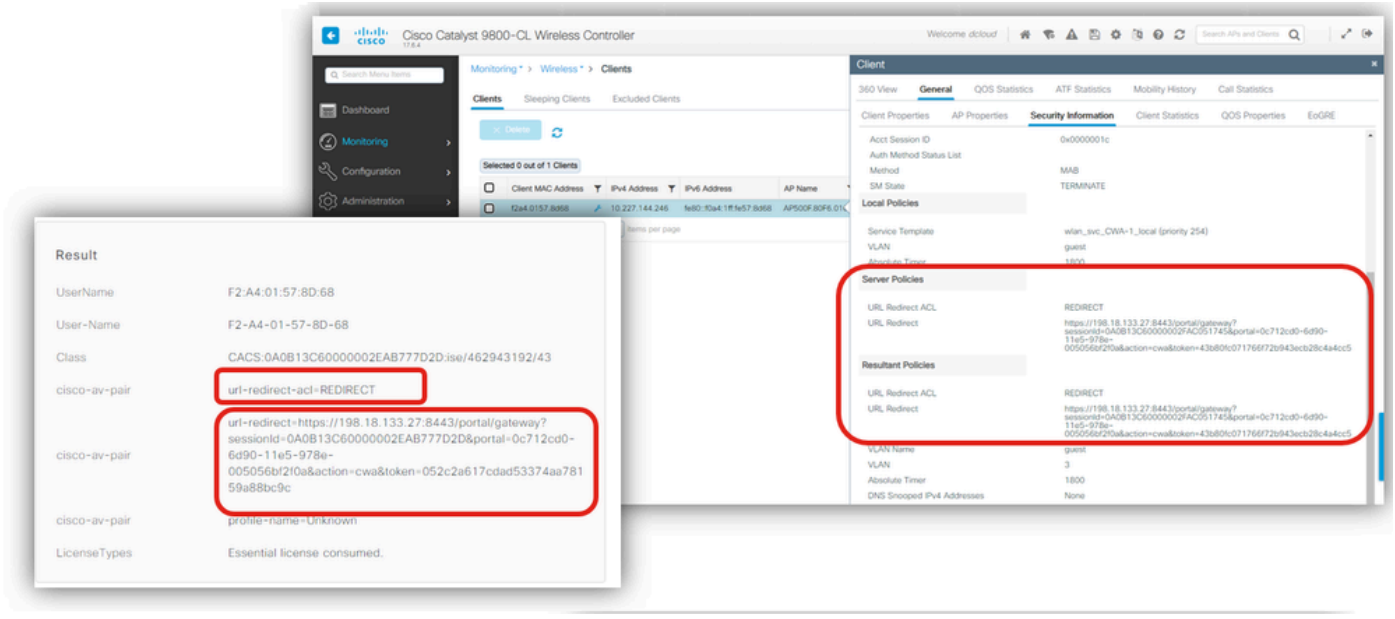
如果找不到用户，请确保身份验证的高级选项设置为“继续”：



找不到用户高级选项

2 - WLC是否收到重定向URL和ACL?

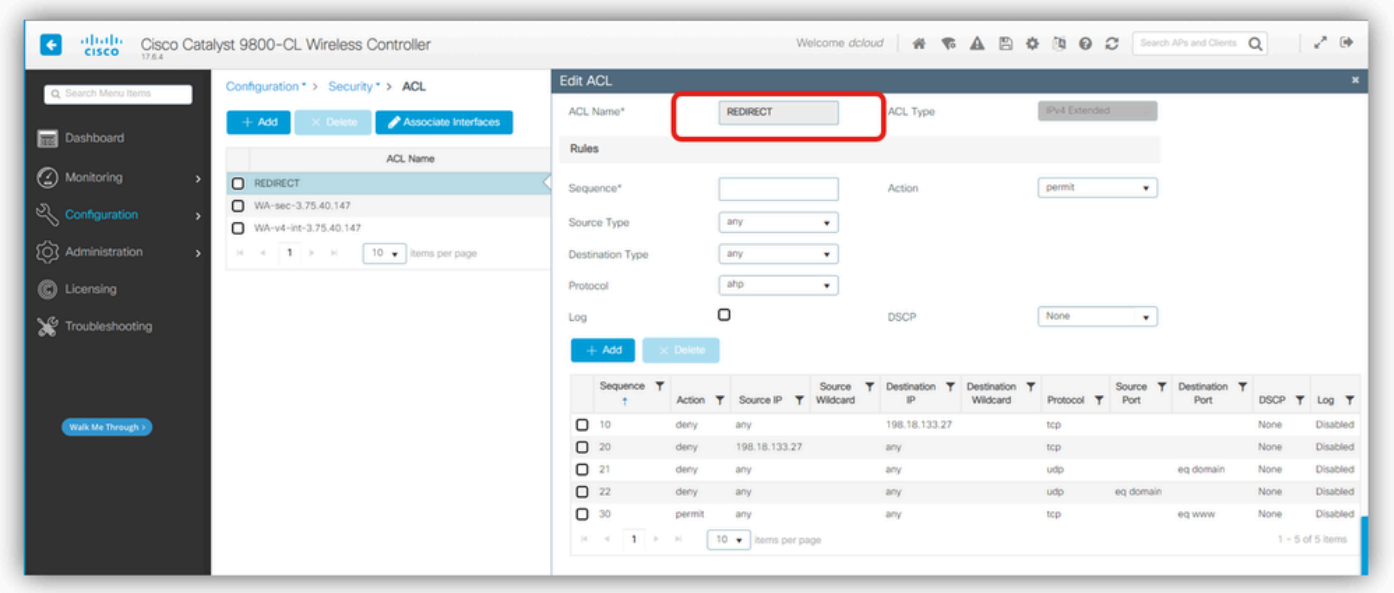
在Monitoring下检查ISE实时日志和WLC客户端安全信息，验证ISE在访问接受中发送重定向URL和ACL，并且WLC会收到该信息，并在客户端详细信息中将其应用于客户端：



重定向ACL和URL

3 — 重定向ACL是否正确？

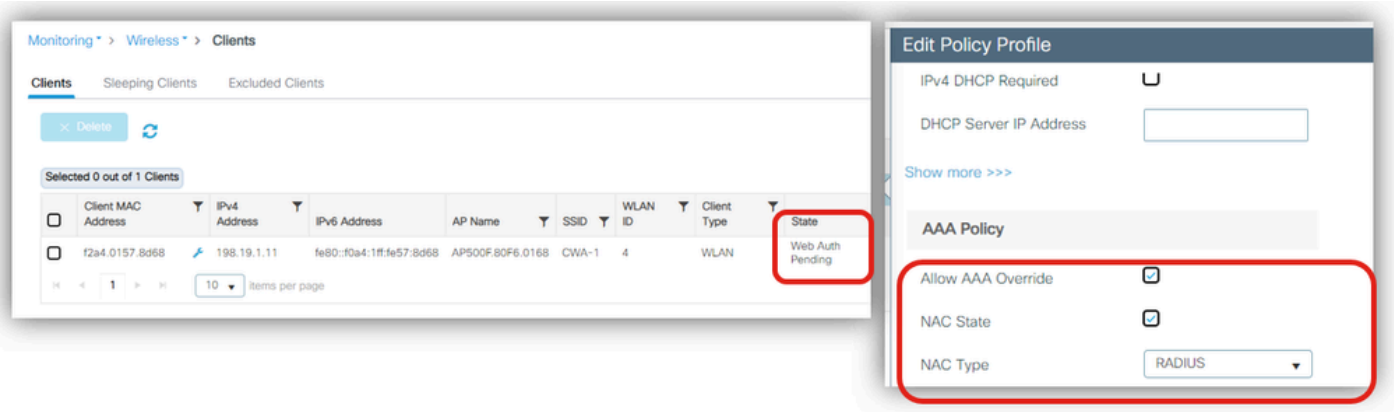
检查ACL名称中是否存在任何输入错误。确保它与ISE发送的完全相同：



重定向ACL验证

4 — 客户端是否移动到Web-Auth Pending?

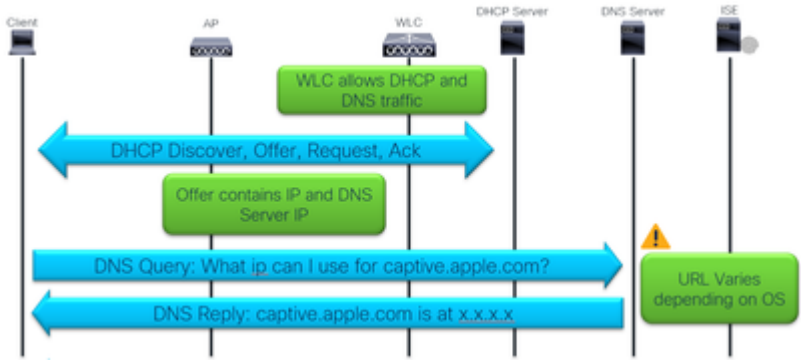
检查客户端详细信息以了解“Web Auth Pending”状态。如果它未处于该状态，则验证是否在策略配置文件中启用了AAA覆盖和Radius NAC:



客户端详细信息、aaa覆盖和RADIUS NAC

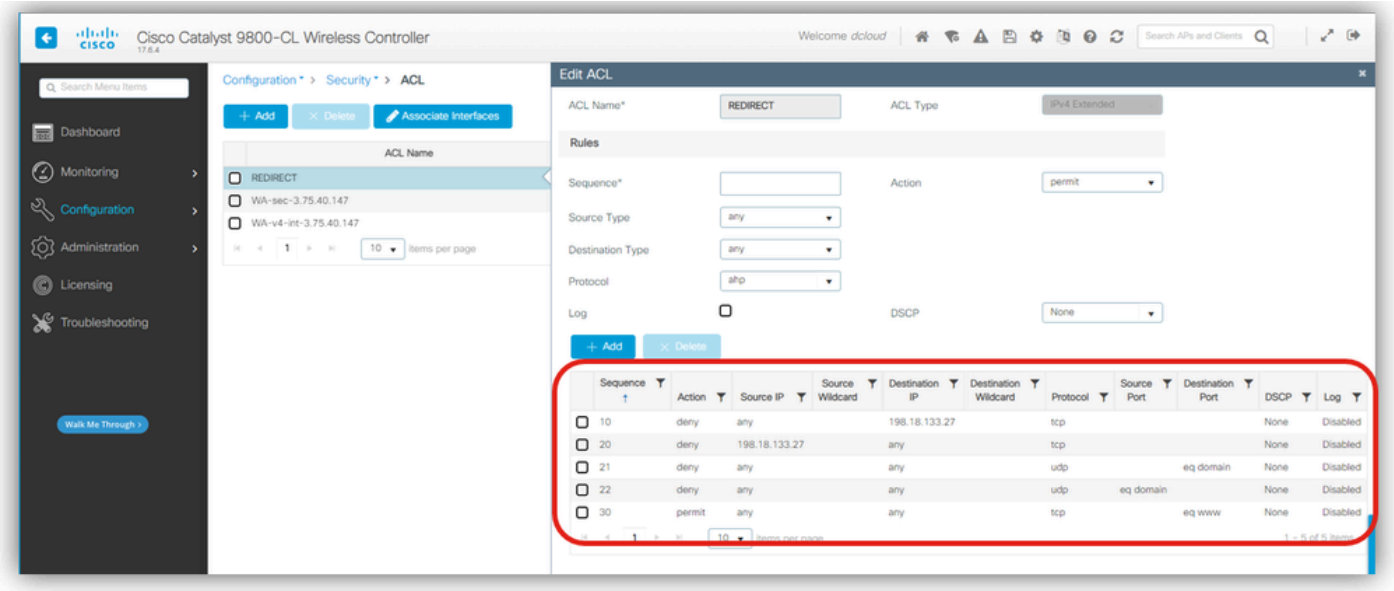
还是不工作？

让我们重新审视一下流程……



5 - WLC是否允许DHCP和DNS流量？

验证WLC中的重定向ACL内容：



重定向WLC中的ACL内容

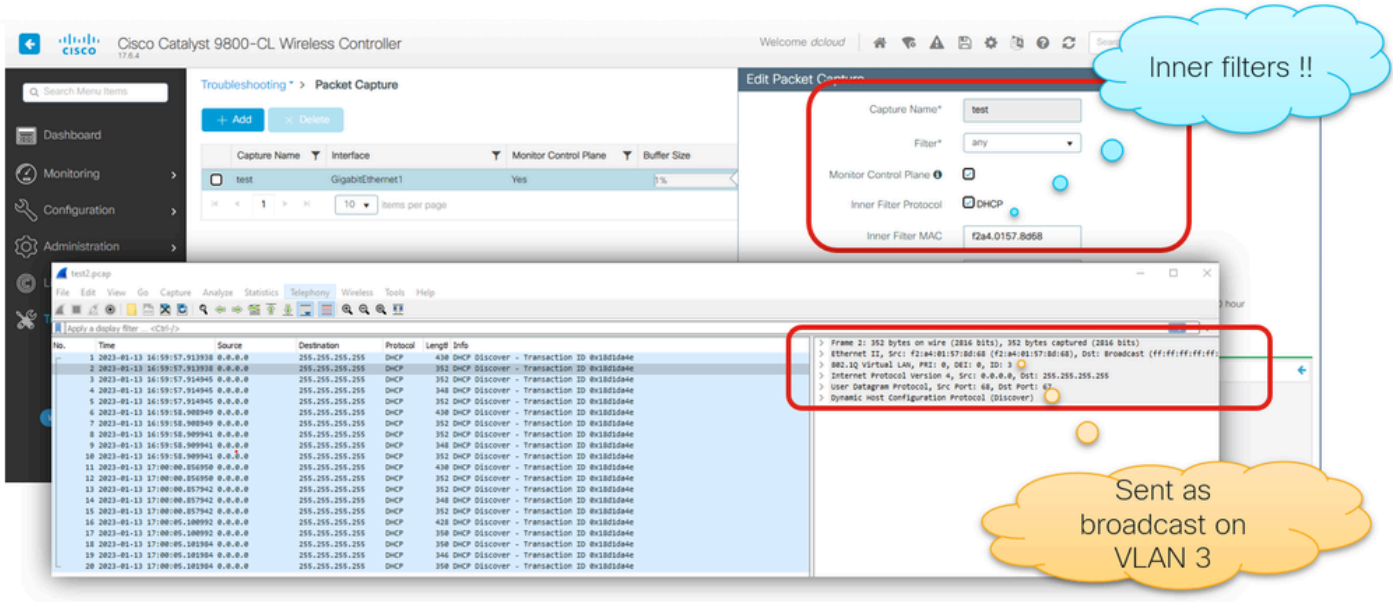
重定向ACL定义哪些流量被permit语句拦截和重定向，哪些流量被使用deny语句拦截和重定向。

在本示例中，我们允许流向/流向ISE IP地址的DNS和流量，并拦截端口80(www)上的任何tcp流量。

6 - DHCP服务器是否接收DHCP发现/请求？

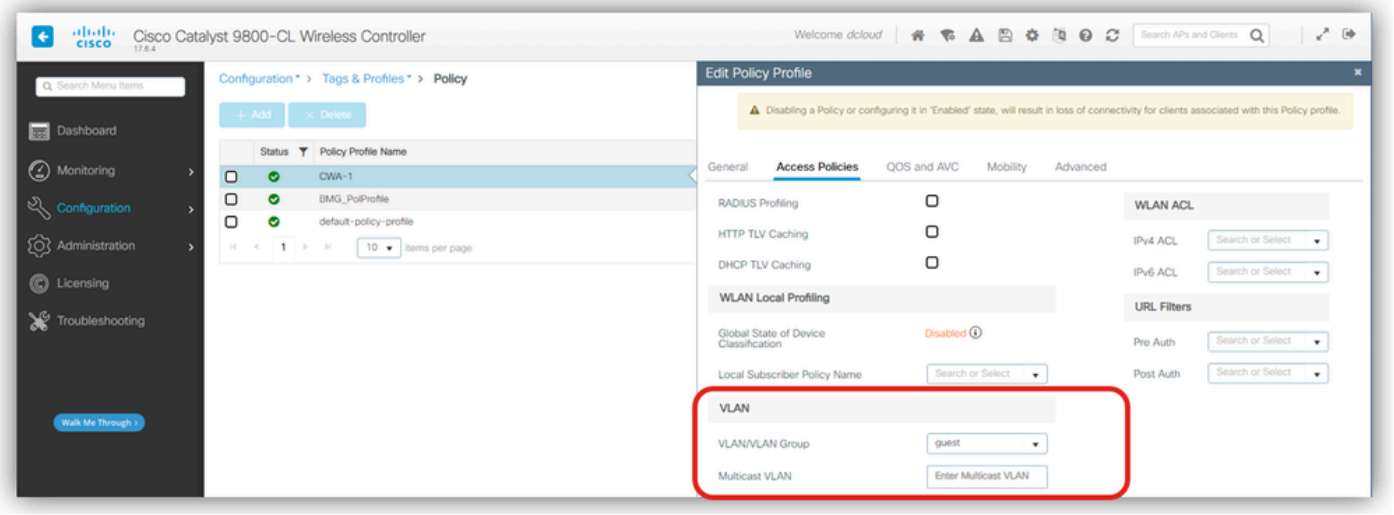
如果发生DHCP交换，请与EPC确认。EPC可以与内部过滤器（例如DHCP协议和/或内部过滤器MAC）一起使用，其中可以使用客户端设备MAC地址，并且只能在EPC中获取由客户端设备MAC地址发送或发送到客户端设备MAC地址的DHCP数据包。

在本示例中，我们可以看到DHCP发现数据包在VLAN 3上以广播形式发送：



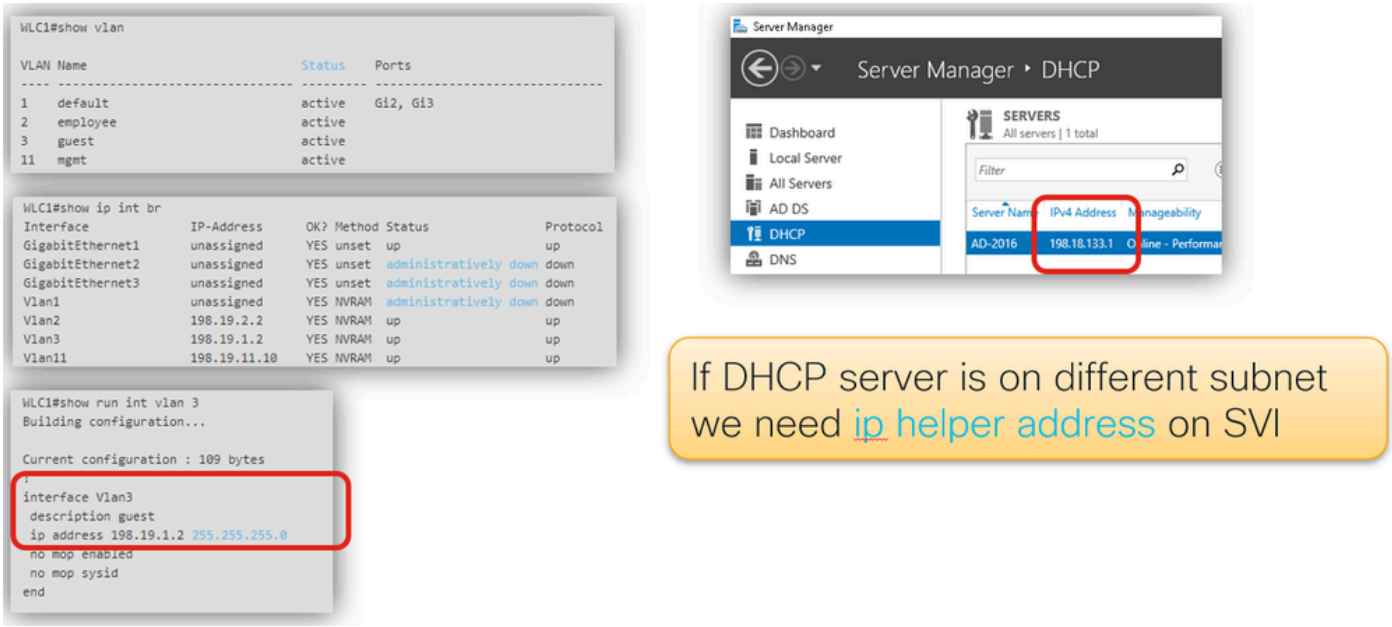
用于验证DHCP的WLC EPC

确认策略配置文件中预期的客户端VLAN:



策略配置文件中的VLAN

检验WLC VLAN和交换机端口中继配置和DHCP子网：



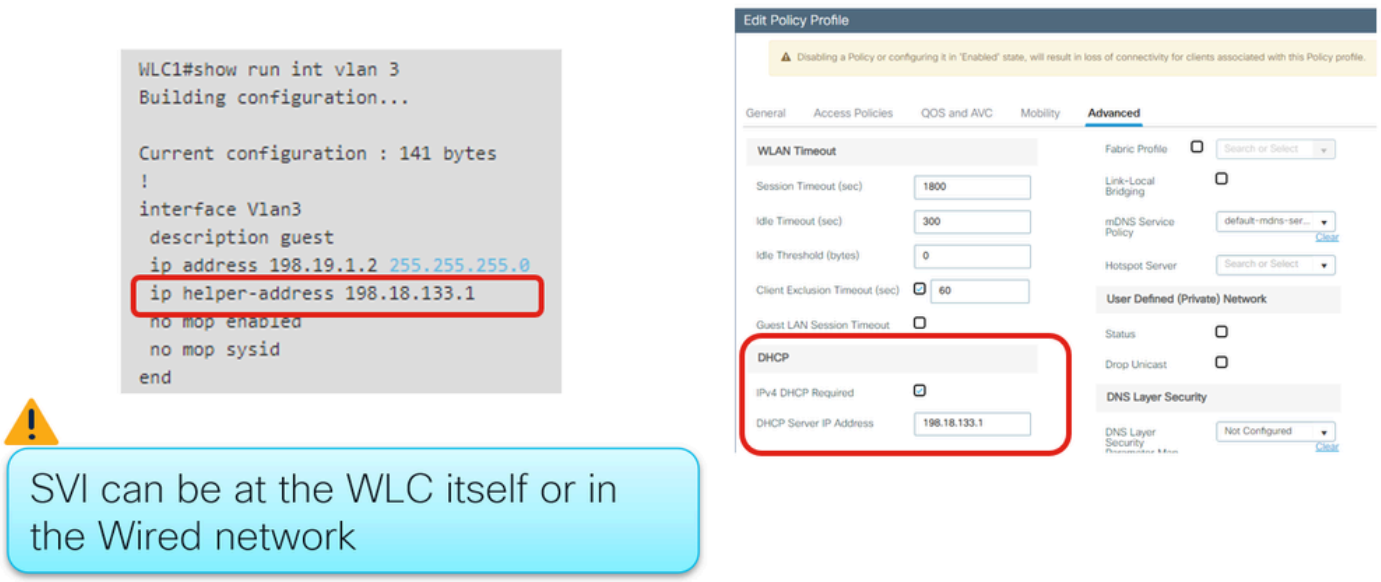
VLAN、交换机端口和DHCP子网

我们可以看到VLAN 3存在于WLC中，并且它也有用于VLAN 3的SVI，但是当我们验证DHCP服务器的ip地址时，它位于不同的子网上，因此我们需要在SVI上提供ip帮助地址。

最佳实践要求在有线基础架构中配置客户端子网的SVI，并在WLC上避免配置客户端子网。

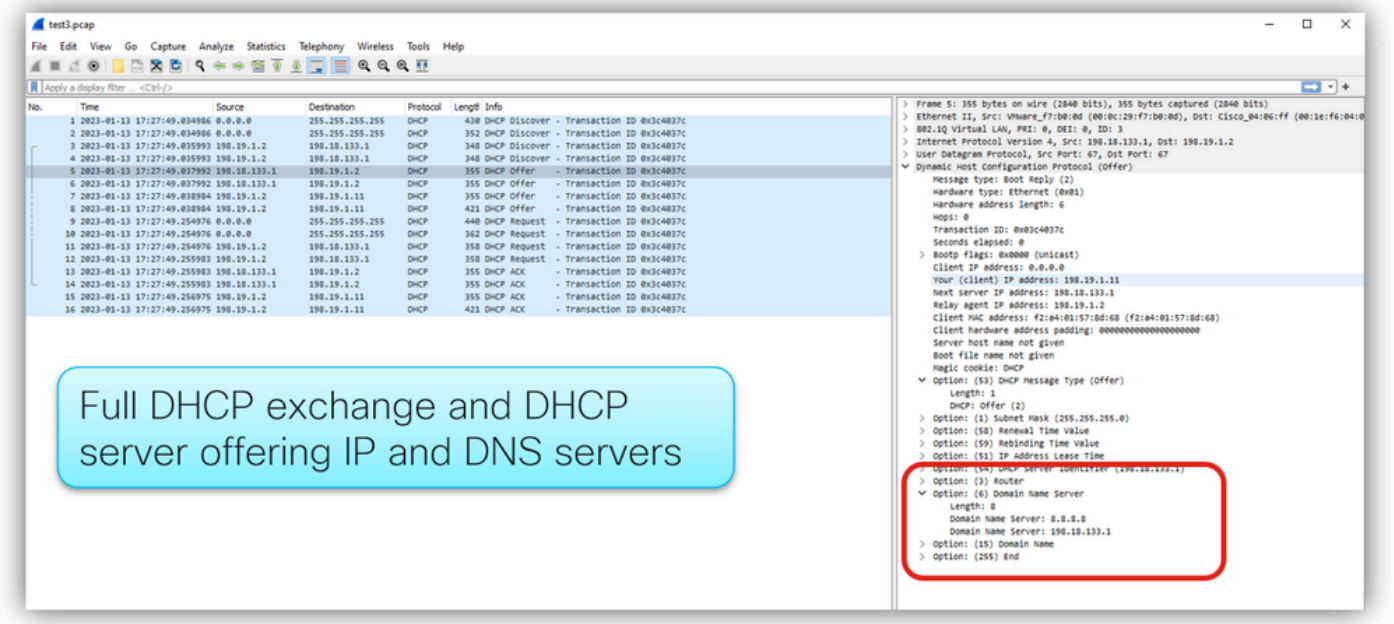
在任何情况下，都需要将ip helper-address命令添加到SVI，而不管它位于何处。

另一种方法是在策略配置文件中配置DHCP服务器ip地址：



SVI或策略配置文件的IP helper-address

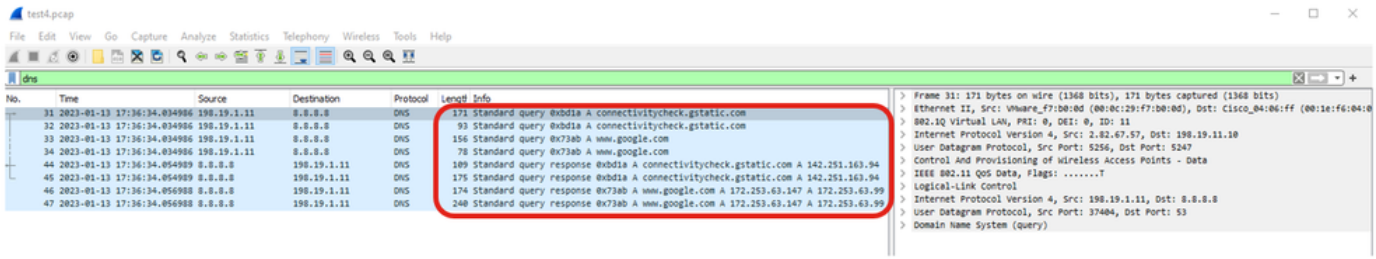
然后，您可以使用EPC验证DHCP交换现在是否正常，以及DHCP服务器是否提供DNS服务器IP:



DNS服务器ip的DHCP提供详细信息

7 — 是否发生自动重定向？

使用WLC EPC验证DNS服务器是否响应查询：

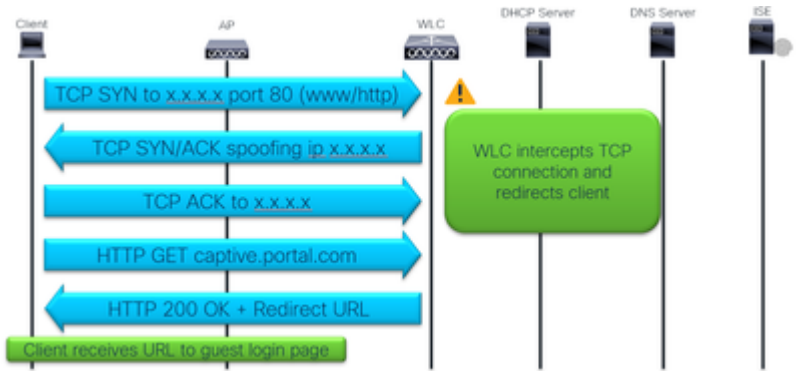


DNS查询和响应

- 如果重定向不是自动重定向，请打开浏览器并尝试使用随机IP地址。例如10.0.0.1。
- 如果重定向随后起作用，则可能存在DNS解析问题。

还是不工作？

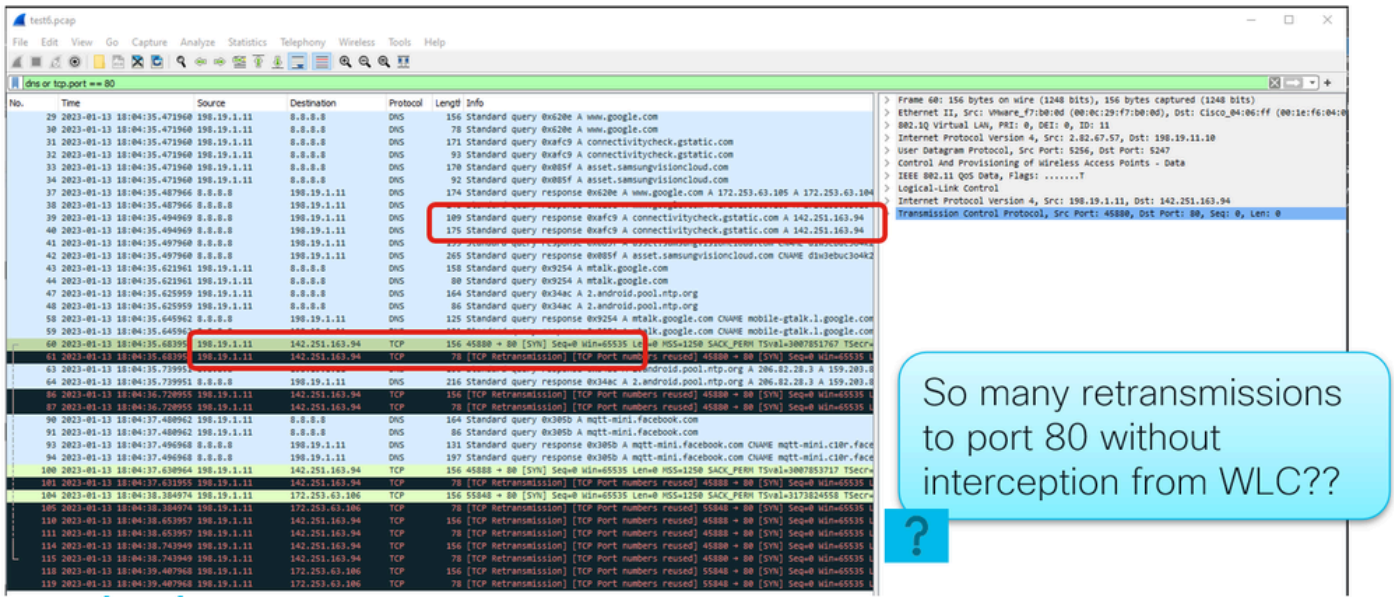
让我们重新审视一下流程……



流量拦截和重定向

8 — 浏览器不显示登录页面？

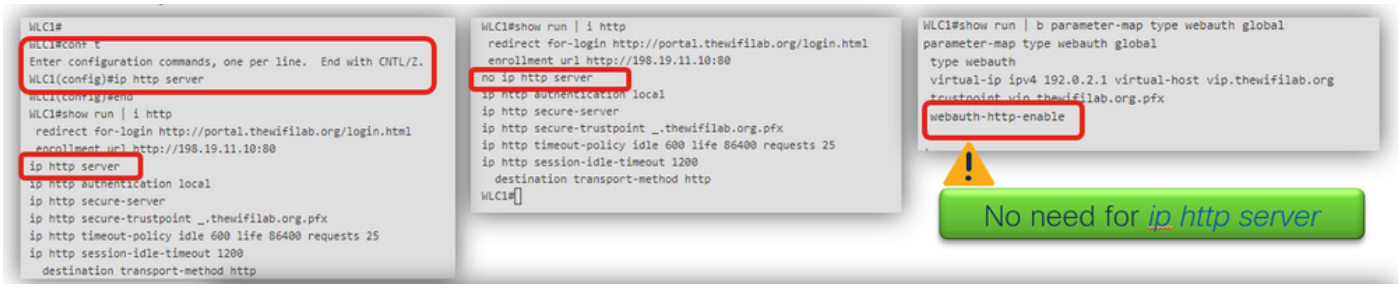
验证客户端是否将TCP SYN发送到端口80且WLC拦截它：



TCP重新传输至端口80

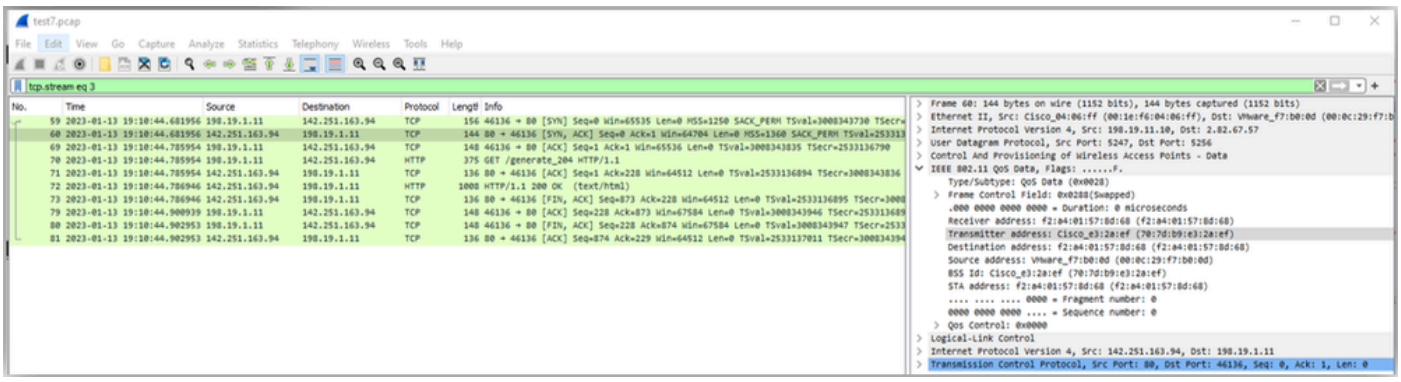
此处我们可以看到客户端向端口80发送TCP SYN数据包，但是没有收到任何回复，并且执行TCP重新传输。

确保在全局配置中具有ip http server命令，或在parameter-map global中具有webauth-http-enable命令：



http拦截命令

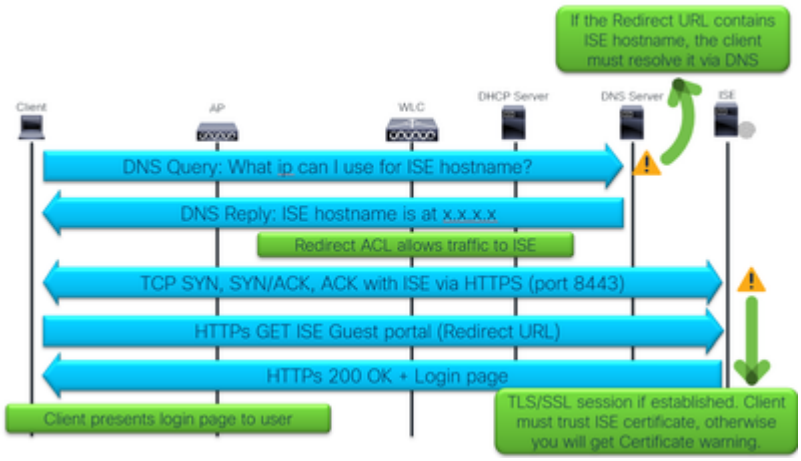
命令执行后，WLC拦截TCP并欺骗目标IP地址以回复客户端并重定向。



WLC的TCP拦截

还是不工作？

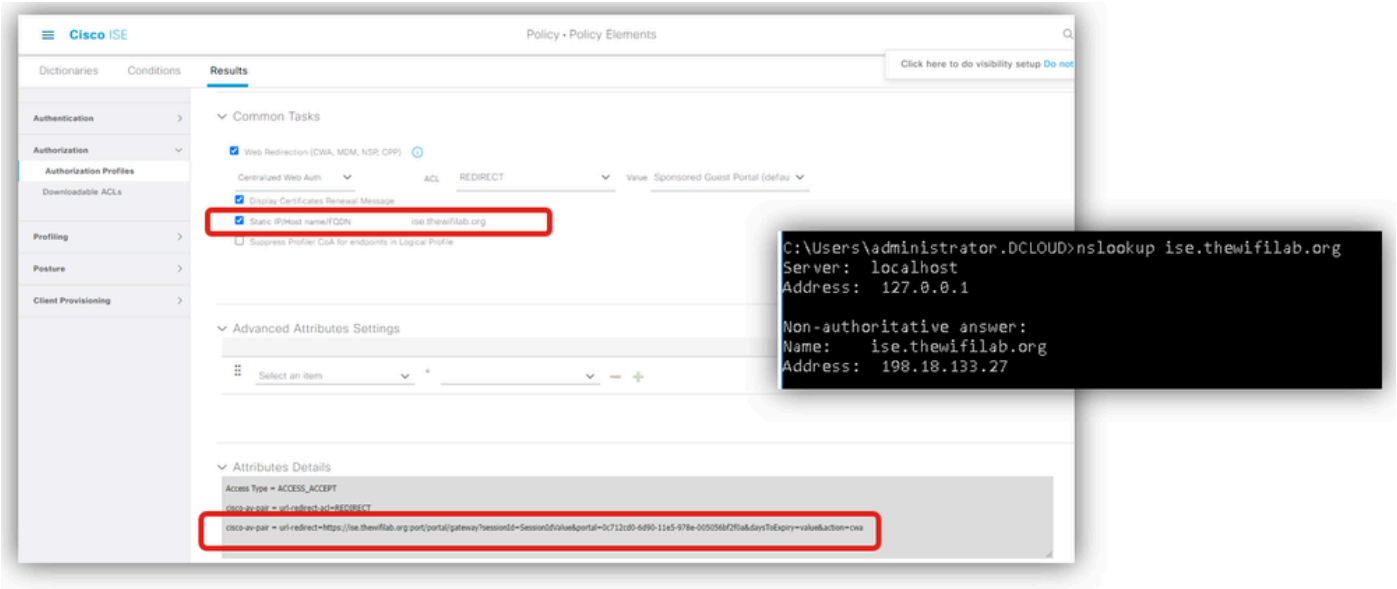
流程中有更多内容……



客户端登录ISE访客登录门户

9 — 客户端能否解析ISE主机名？

验证重定向URL是否使用IP或主机名，以及客户端是否解析ISE主机名：

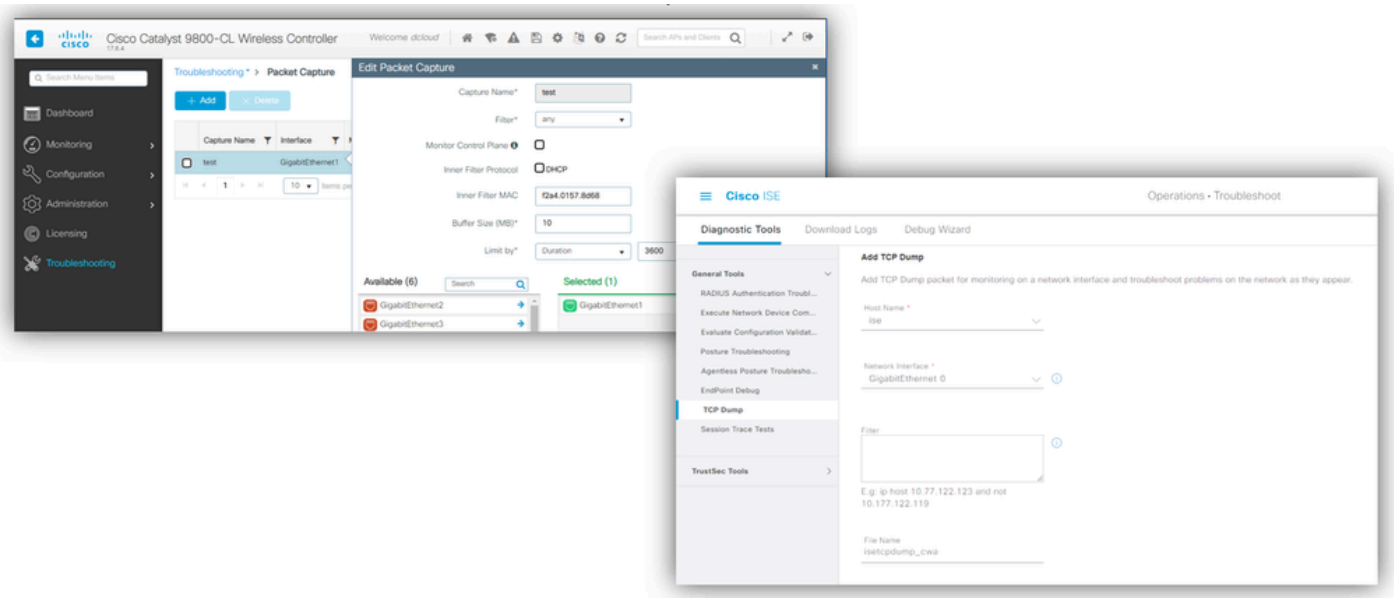


ISE主机名解析

当重定向URL包含ISE主机名时，会出现一个常见问题，但客户端设备无法将该主机名解析为ISE IP地址。如果使用主机名，请确保可通过DNS进行解析。

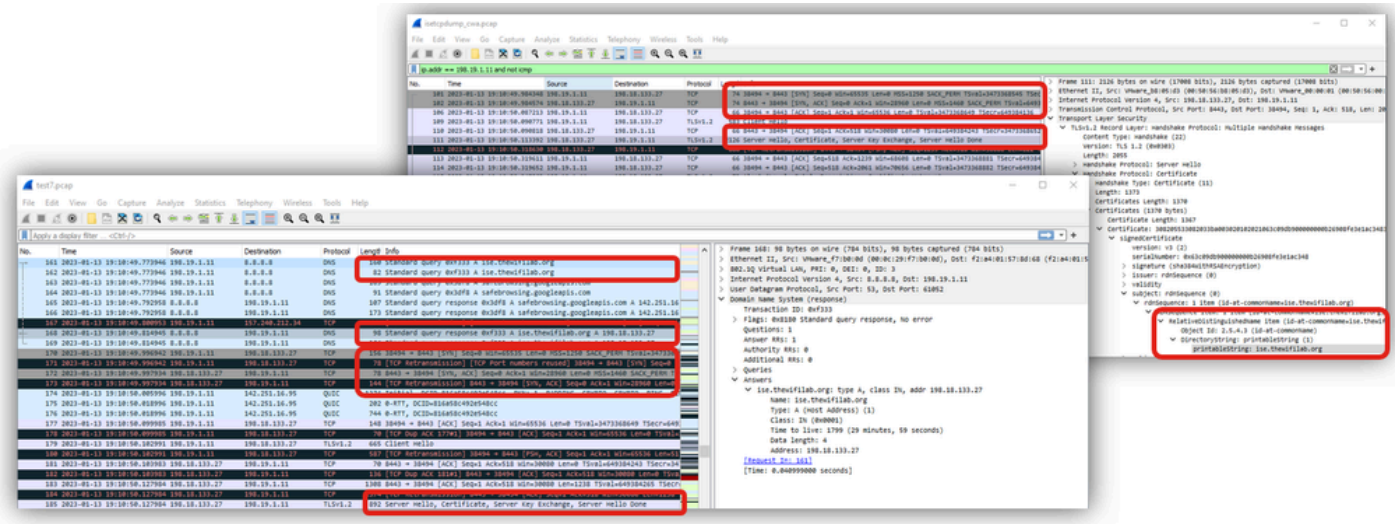
10 — 登录页是否仍无法加载？

如果客户端流量到达ISE PSN，请使用WLC EPC和ISE TCPdump进行验证。在WLC和ISE上配置并启动捕获：



WLC EPC和ISE TCPDump

在问题再现之后，收集捕获信息并关联流量。在这里，我们可以看到ISE主机名已解析，然后客户端和ISE之间通过端口8443进行通信：



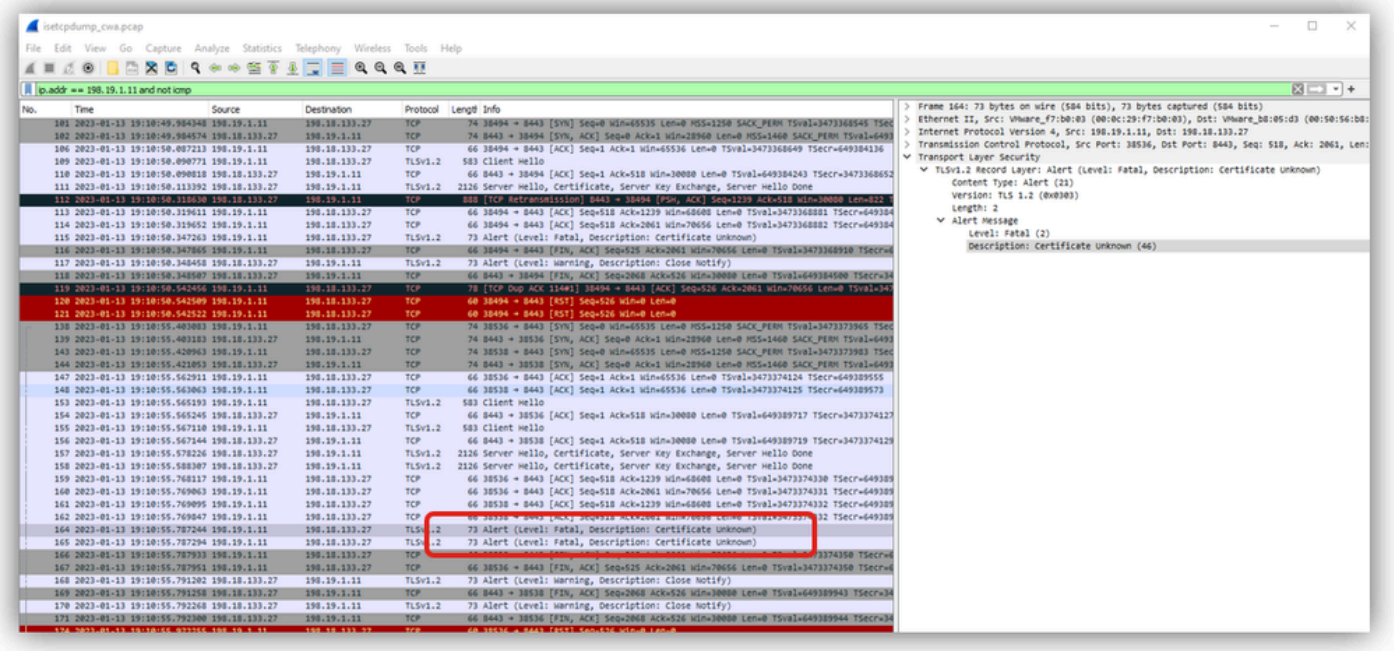
WLC和ISE流量

11 — 为什么由于证书而发生安全违规？

如果您在ISE上使用自签名证书，则客户端在尝试显示ISE门户登录页面时预期会抛出安全警告。

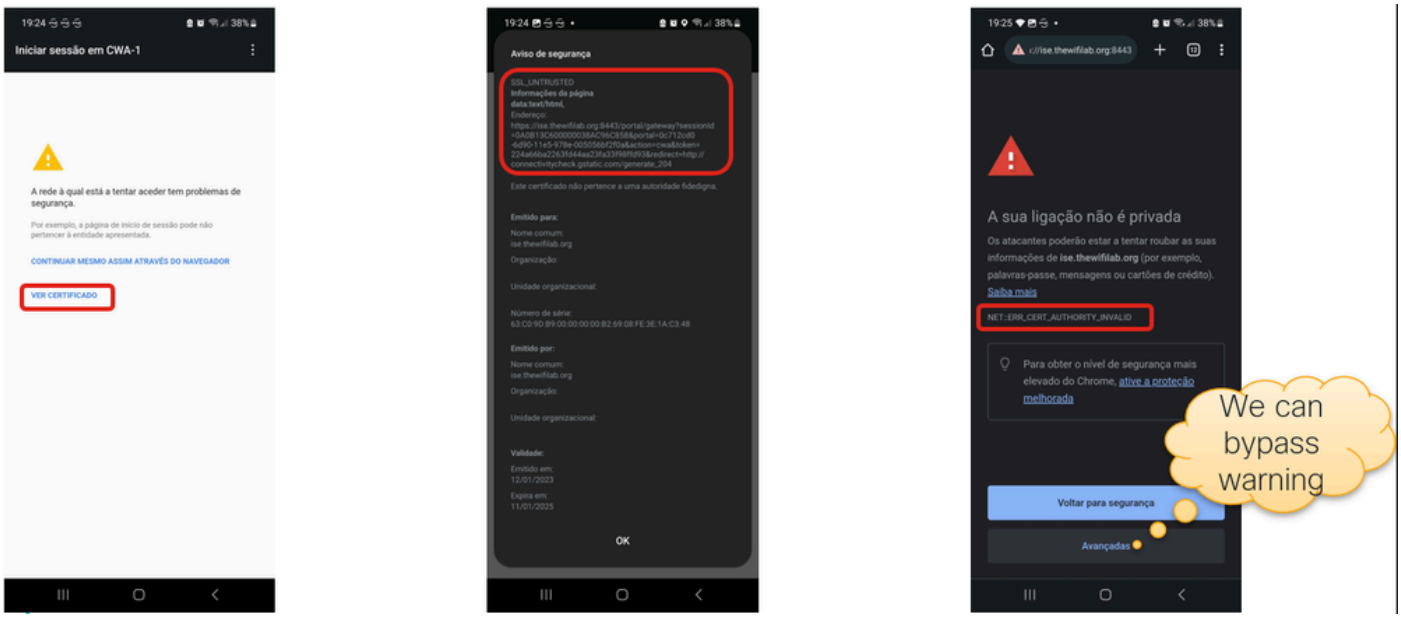
在WLC EPC或ISE TCPdump上，我们可以验证ISE证书是否受信任。

在本例中，我们可以看到连接从带有警报的客户端(级别：致命，说明：certificate Unknown)，表示ISE证书未知(Trusted):



ISE不受信任证书

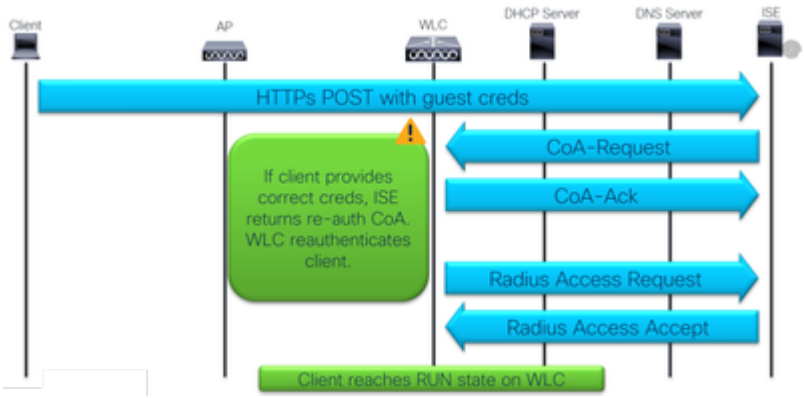
如果检查客户端，我们看到以下示例输出：



不信任ISE证书的客户端设备

最后，重定向正在起作用!!但登录失败……

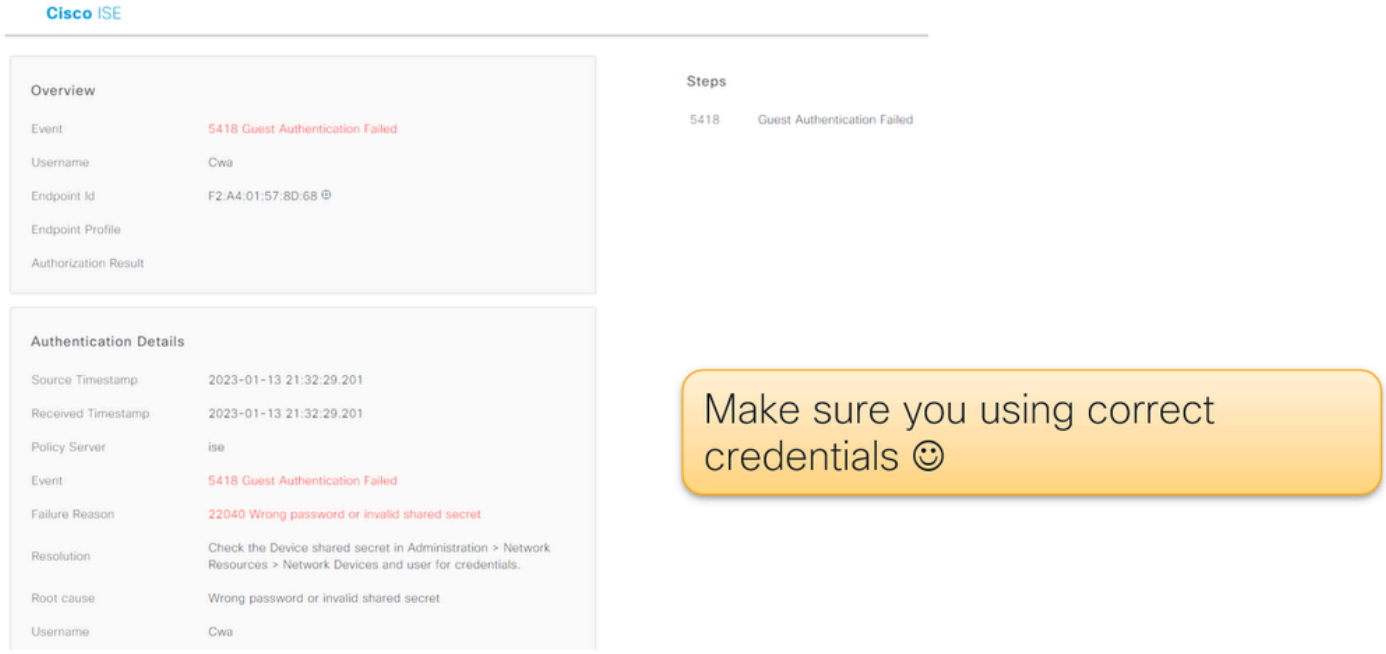
最后一次检查流量……



客户端登录和CoA

12 — 访客登录失败？

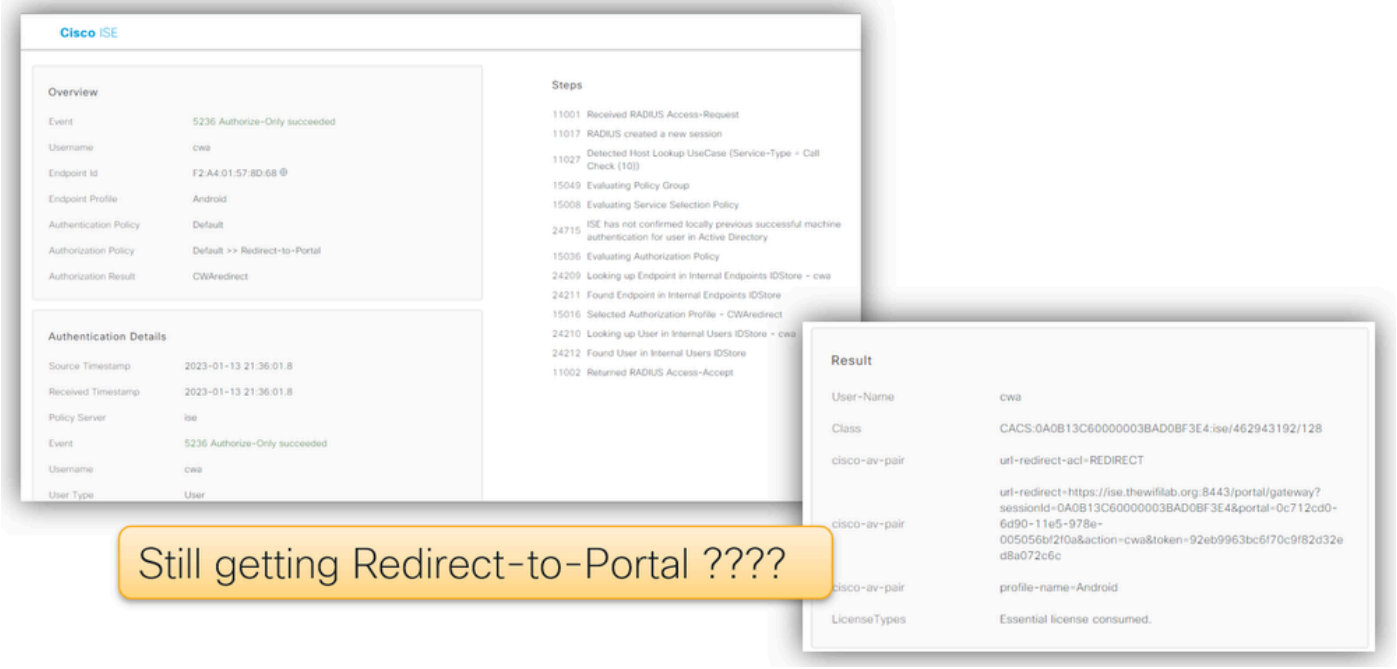
检查ISE日志的身份验证失败。确保凭据正确。



由于凭证错误，访客身份验证失败

13 — 登录成功但不转到RUN?

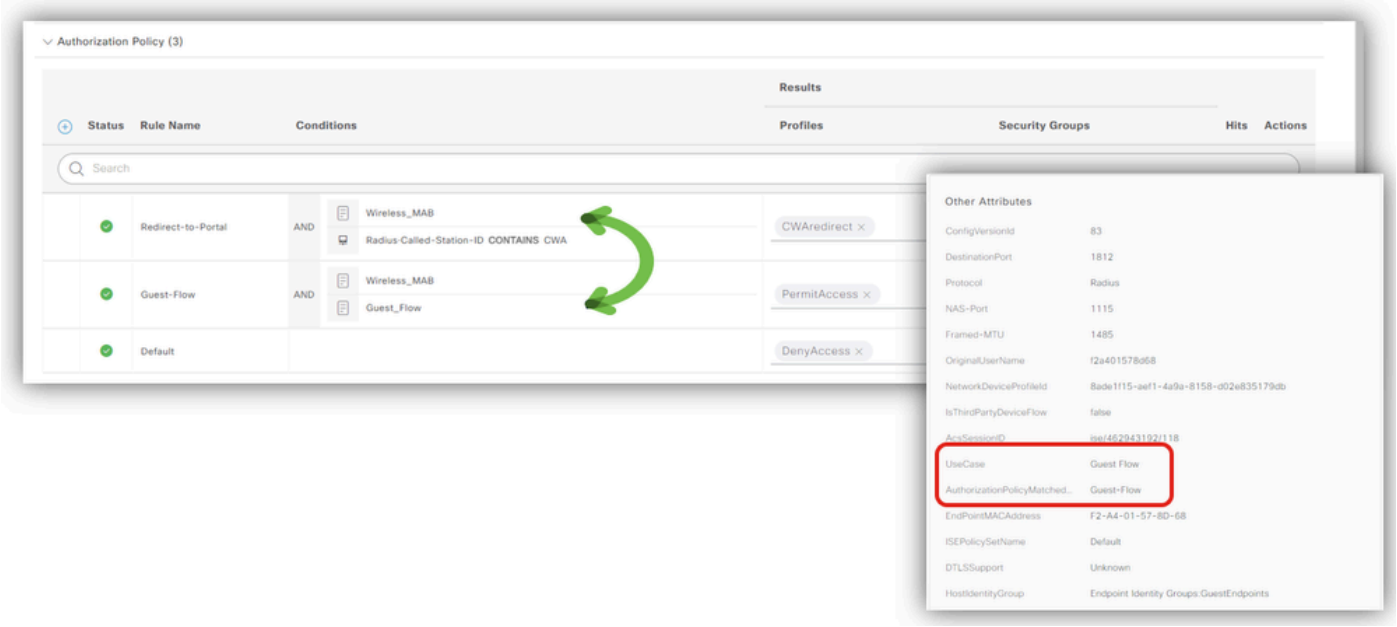
检查ISE日志的身份验证详细信息和结果：



重定向环路

在本示例中，我们可以看到客户端再次获取包含重定向URL和重定向ACL的授权配置文件。这会导致重定向环路。

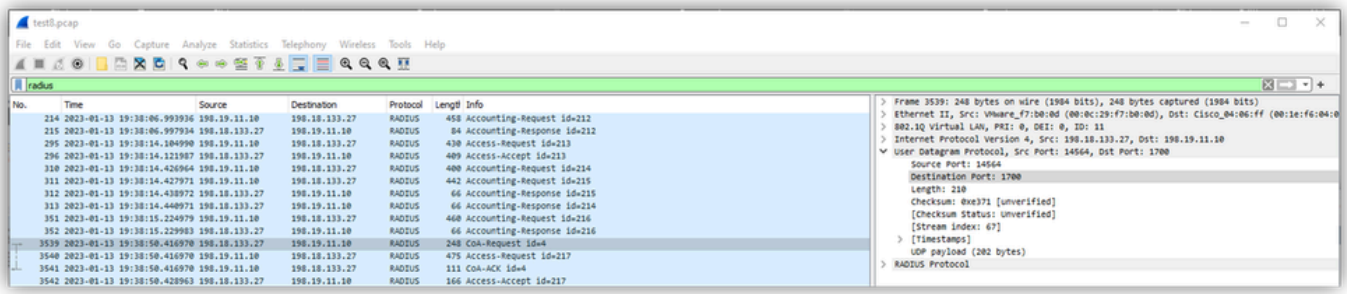
检查策略设置。在重定向之前必须检查规则Guest_Flow:



Guest_Flow规则

14 - COA失败？

通过EPC和ISE TCPDump，我们可以验证CoA流量。验证WLC和ISE之间的CoA端口(1700)是否打开。确保共享密钥匹配。



CoA流量

注意：在版本17.4.X及更高版本中，确保在配置RADIUS服务器时也配置CoA服务器密钥。使用与共享密钥相同的密钥（在ISE上默认使用相同的密钥）。 目的是为CoA配置不同于共享密钥的密钥（如果这是您的RADIUS服务器所配置的密钥）。在Cisco IOS® XE 17.3中，Web UI仅使用与CoA密钥相同的共享密钥。

从版本17.6.1开始，此端口支持RADIUS（包括CoA）。如果要使用RADIUS的服务端口，则需要此配置：

<#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

结论

这是恢复的CWA检查表：

- 确保客户端位于正确的VLAN上并获得IP地址和DNS。
  - 在WLC上获取客户端详细信息，并运行数据包捕获以查看DHCP交换。
- 确认客户端可以通过DNS解析主机名。
  - 从cmd对主机名执行ping操作。
- WLC必须在端口80上侦听
  - 验证全局命令ip http server或全局参数映射命令webauth-http-enable。
- 要清除证书警告，请在ISE上安装受信任证书。
  - 无需在CWA中的WLC上安装受信任证书。
- ISE高级选项下的身份验证策略“继续”(Continue)如果未找到用户
  - 允许发起人管理的访客用户连接并获取URL重定向和ACL。

故障排除中使用的主要工具：

- WLC EPC
  - 内部过滤器：DHCP协议、mac地址。
- WLC监控器
  - 检查客户端安全详细信息。
- WLC RA跟踪
  - WLC端包含详细信息的调试。
- ISE 实时日志
  - 身份验证详细信息。
- ISE TCPDump
  - 收集ISE PSN接口上的数据包捕获。

参考

在Catalyst 9800 WLC和ISE上配置中心Web身份验证(CWA)

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。