Dépannage de l'authentification Web centrale (CWA) avec le contrôleur de réseau local sans fil (WLC) 9800 et Identity Services Engine (ISE)

Table des matières

Introduction

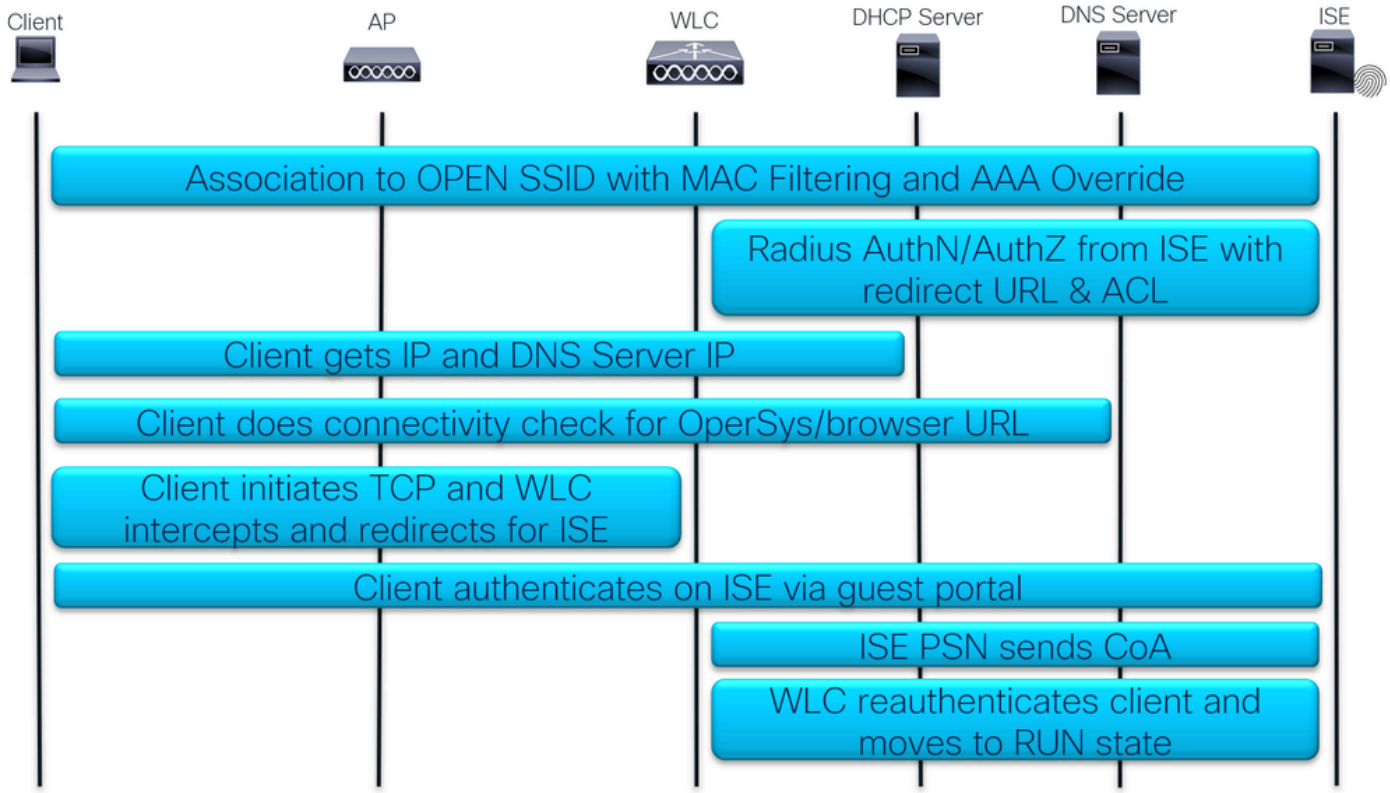
Ce document décrit comment dépanner l'authentification Web centrale (CWA) avec WLC 9800 et ISE.

Informations de fond

Il existe actuellement tellement de périphériques personnels que les administrateurs réseau qui cherchent à sécuriser l'accès sans fil optent généralement pour des réseaux sans fil qui utilisent CWA.
Dans ce document, nous nous concentrons sur l'organigramme de CWA, qui aide à résoudre les problèmes courants qui nous affectent.
Nous examinons les points communs du processus, comment collecter les journaux liés à CWA, comment analyser ces journaux, et comment collecter une capture de paquets intégrée sur le WLC pour confirmer le flux de trafic.

CWA est la configuration la plus courante pour les entreprises qui permettent aux utilisateurs de se connecter au réseau de l'entreprise à l'aide de leurs appareils personnels, également appelés BYOD.
Tout administrateur réseau est intéressé par les tâches et les étapes de dépannage à effectuer pour résoudre ses problèmes avant d'ouvrir un dossier TAC.

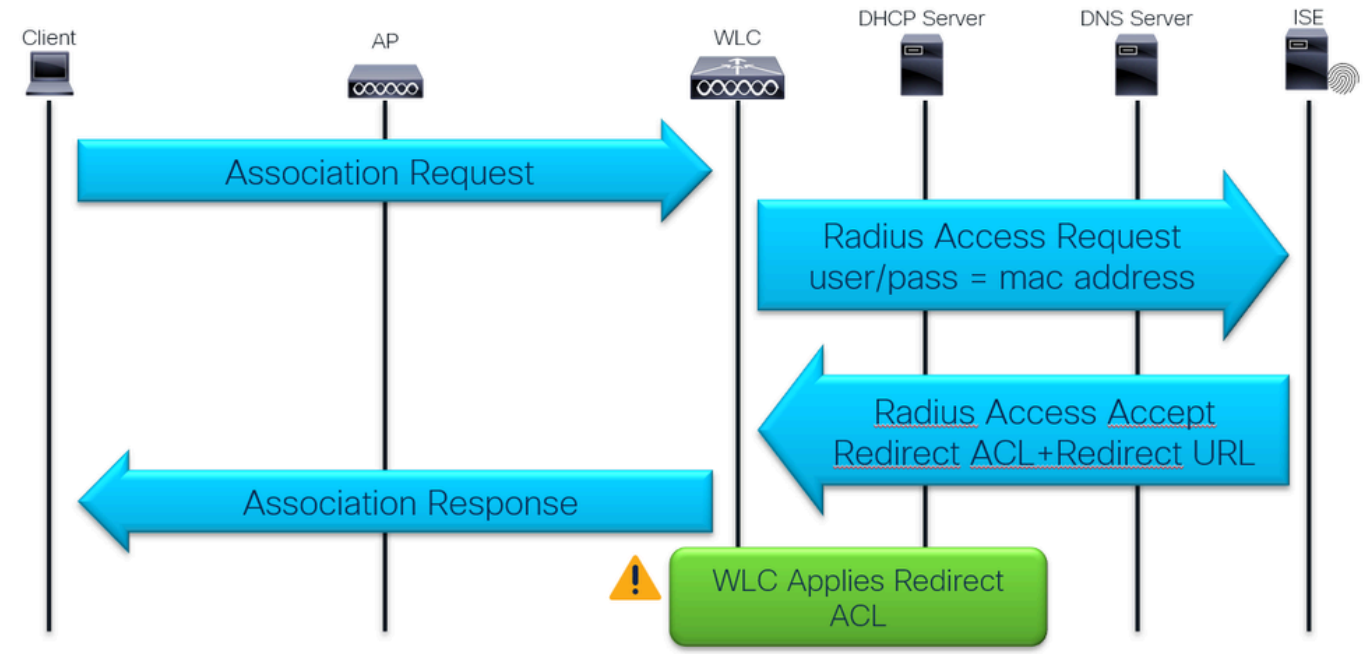
Voici le flux de paquets CWA :



Flux de paquets CWA

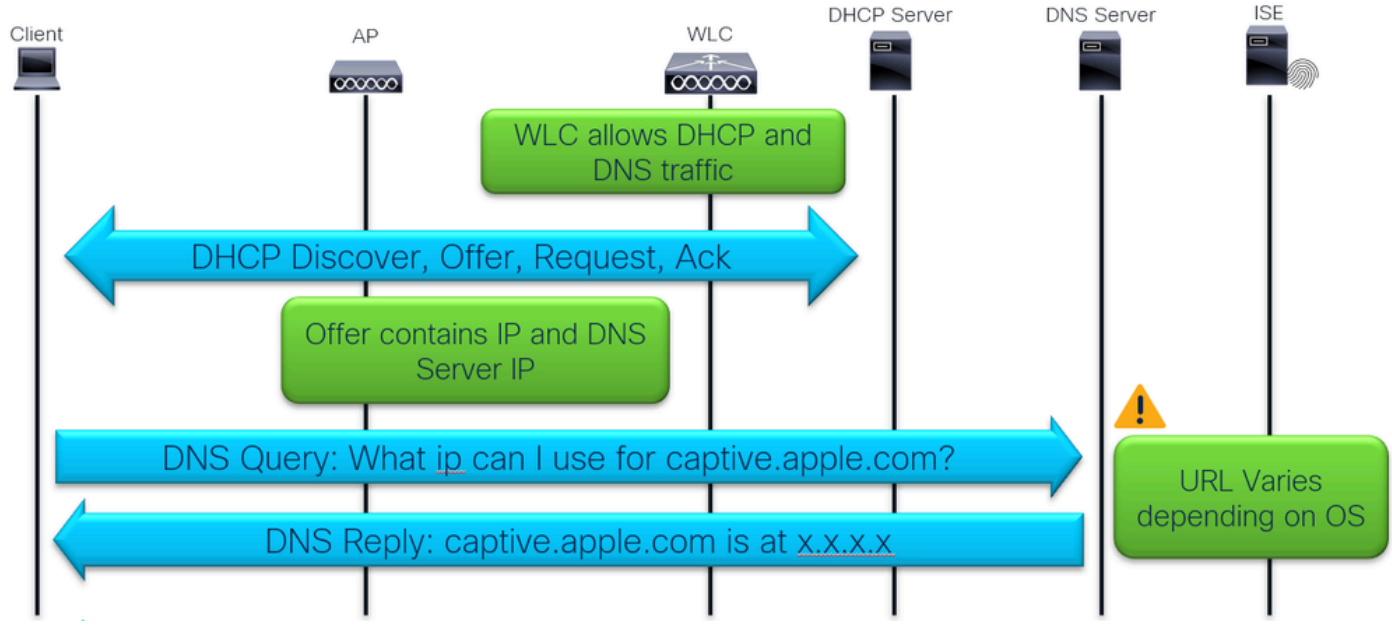
Flux détaillé

Première association et authentification RADIUS :



Première association et authentification RADIUS

DHCP, DNS et vérification de la connectivité :



DHCP, DNS et vérification de la connectivité

La vérification de connectivité est effectuée à l'aide de la détection de portail captif par le système d'exploitation ou le navigateur du périphérique client.

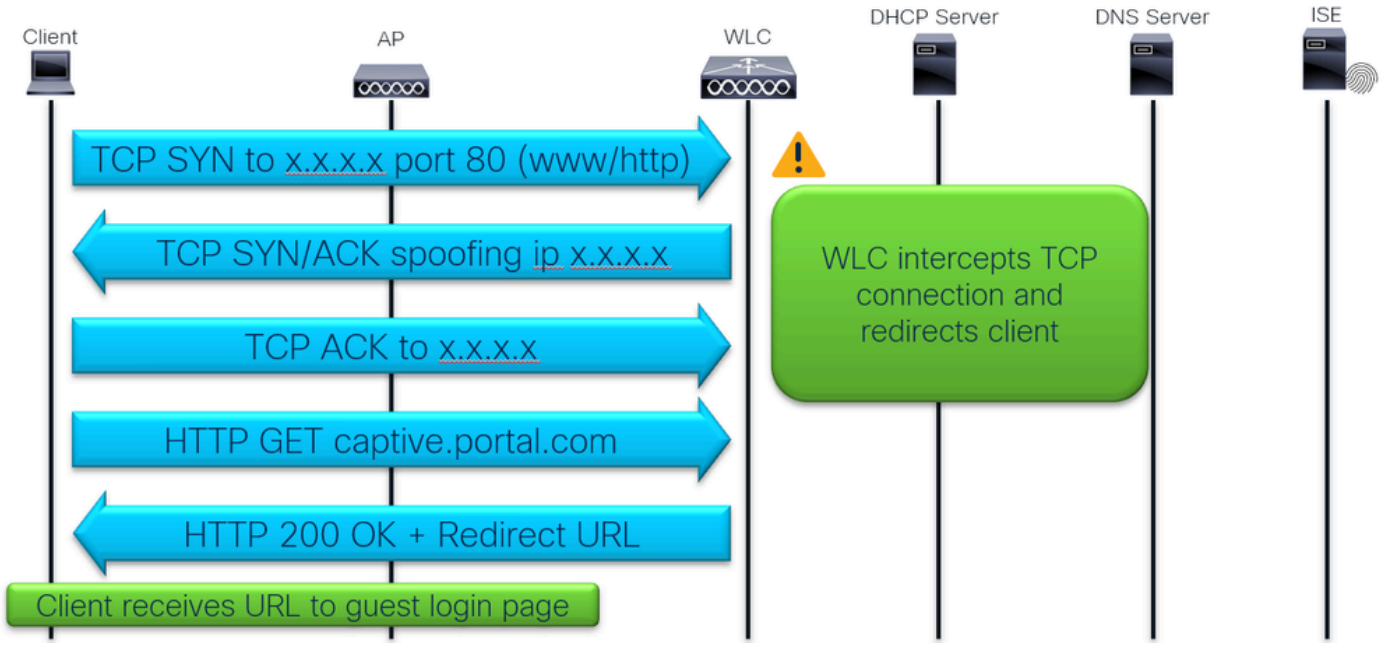
Il existe un système d'exploitation de périphérique préprogrammé pour effectuer HTTP GET vers un domaine spécifique

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

Les navigateurs effectuent également cette vérification à l'ouverture :

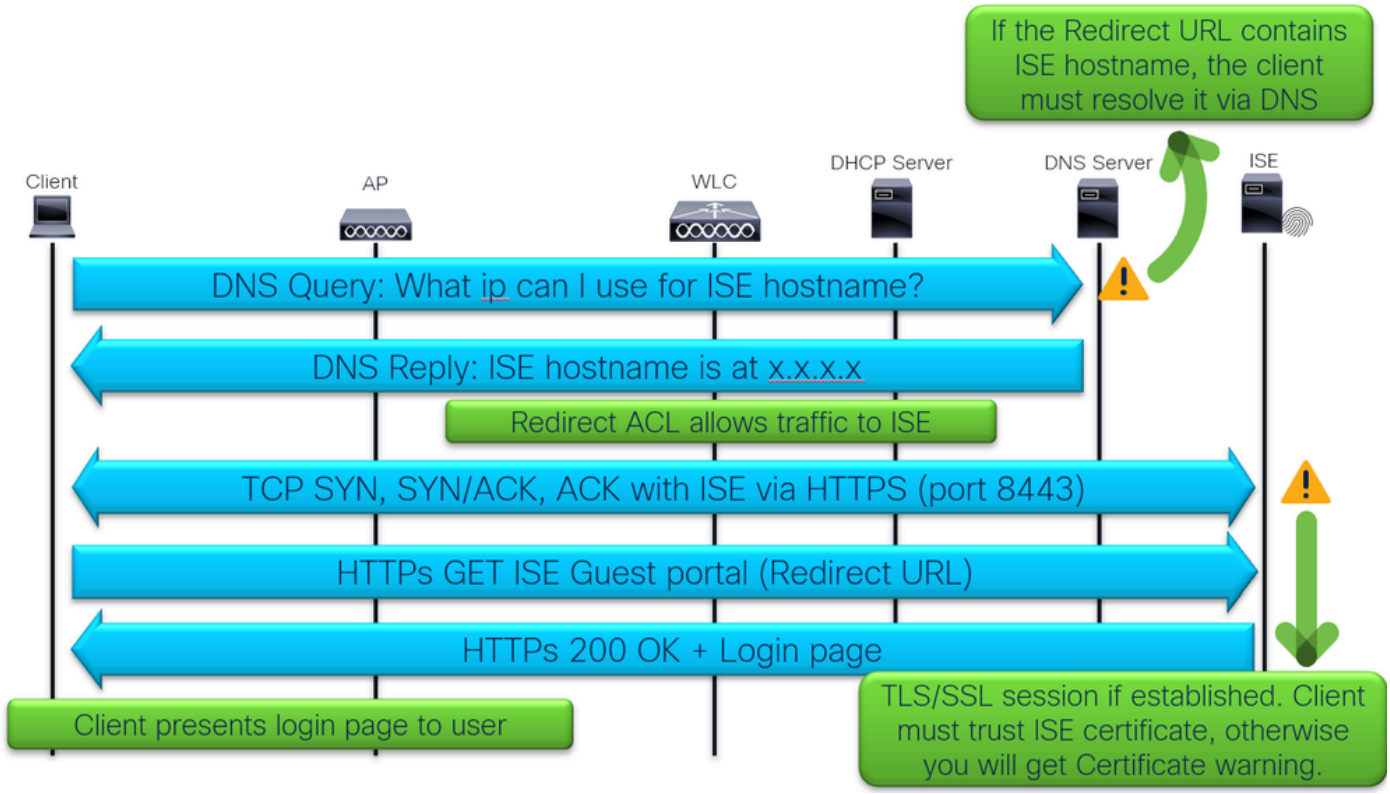
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Interception et redirection du trafic :



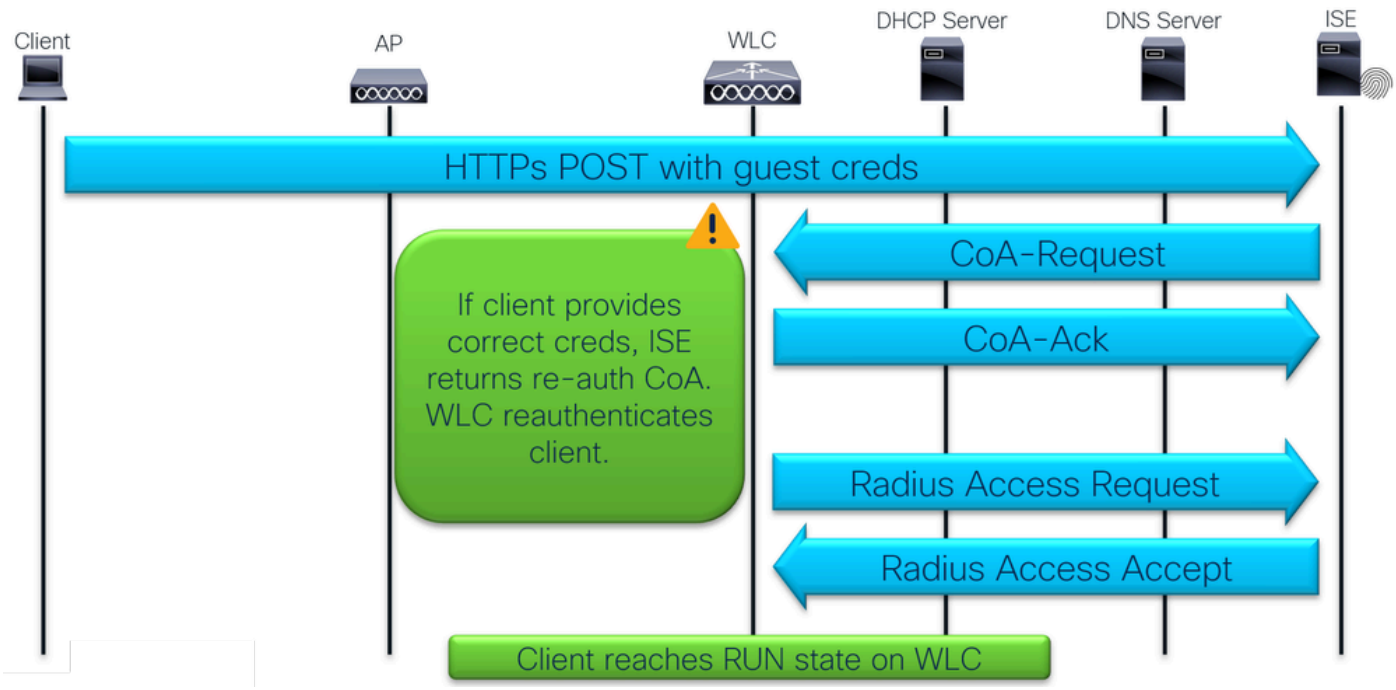
Interception et redirection du trafic

Connexion client au portail de connexion invité ISE :



Connexion du client au portail de connexion des invités ISE

Connexion client et CoA :

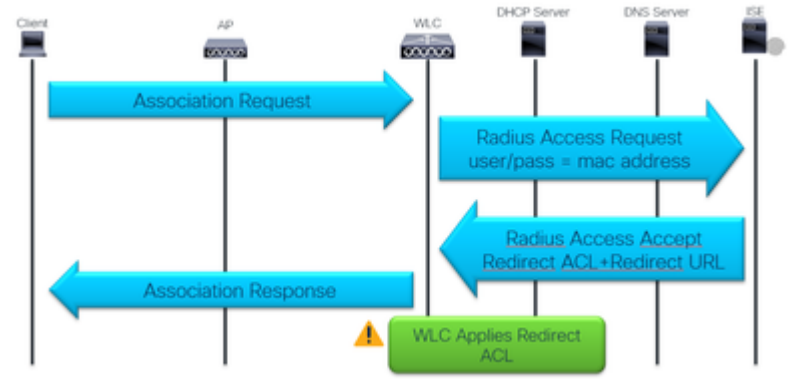


Connexion client et CoA

Dépannage

Symptôme courant : Utilisateur non redirigé vers la page de connexion.

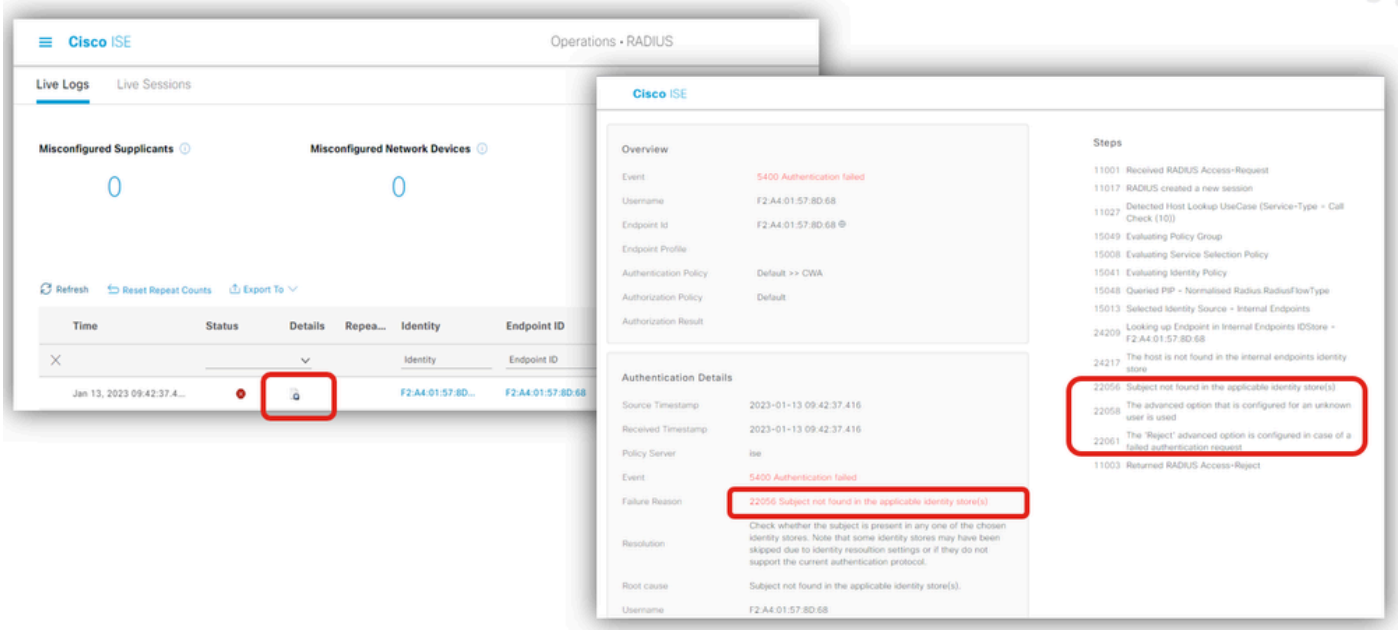
Commençons par la première partie du flux :



Première association et authentification RADIUS

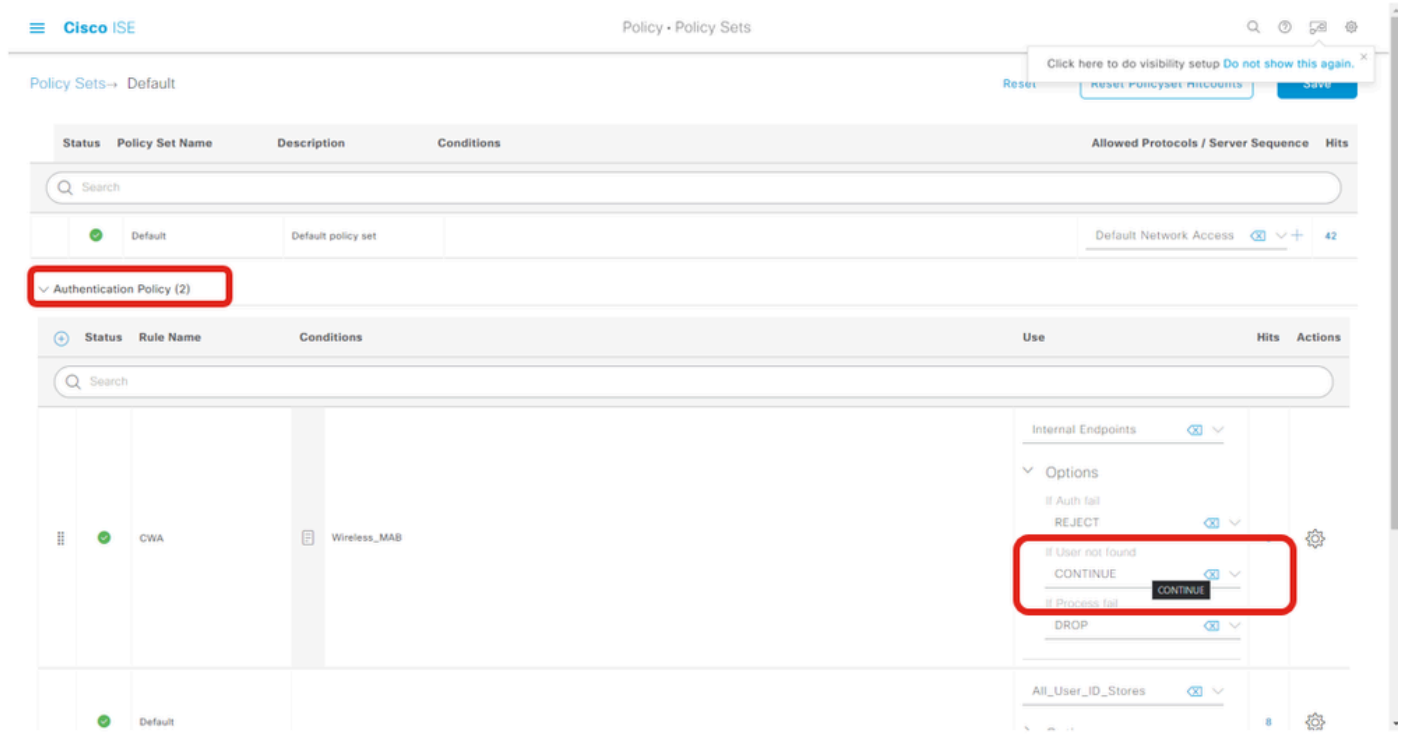
1 - La première authentification RADIUS a-t-elle réussi ?

Vérifiez le résultat d'authentification du filtrage MAC :



Journaux ISE Live montrant le résultat de l'authentification de filtrage MAC

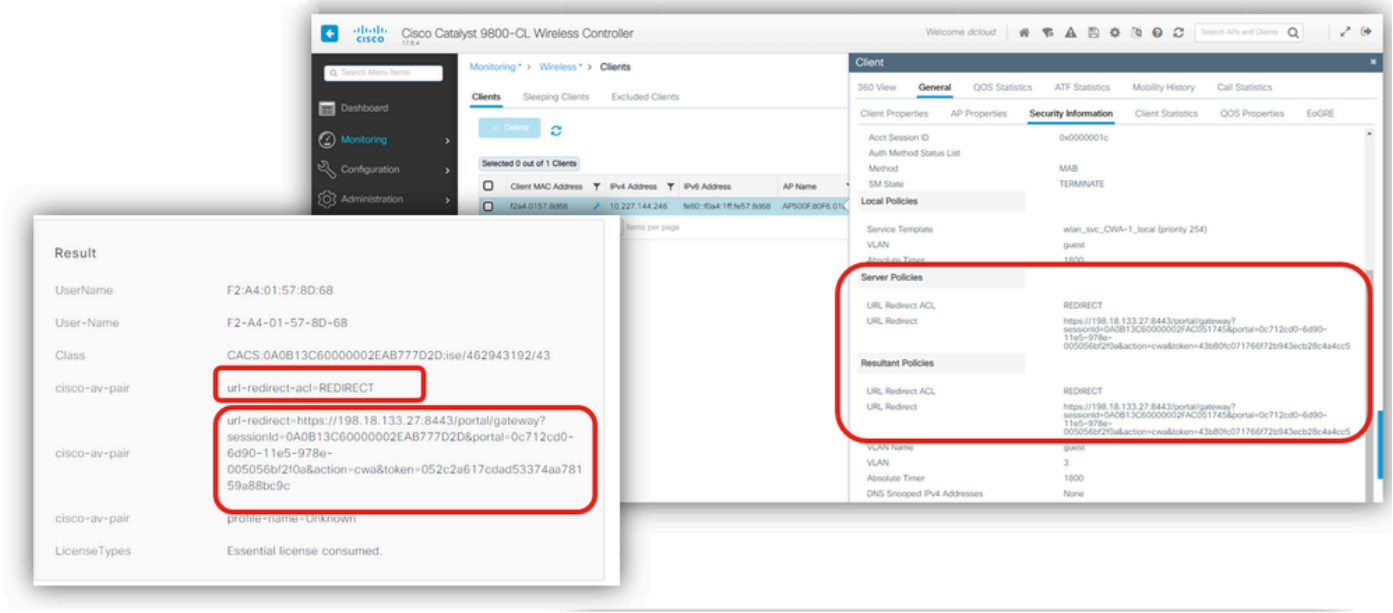
Assurez-vous que l'option avancée pour l'authentification est définie sur « Continuer » si l'utilisateur est introuvable :



Option avancée Utilisateur introuvable

2 - WLC reçoit l'URL de redirection et l'ACL ?

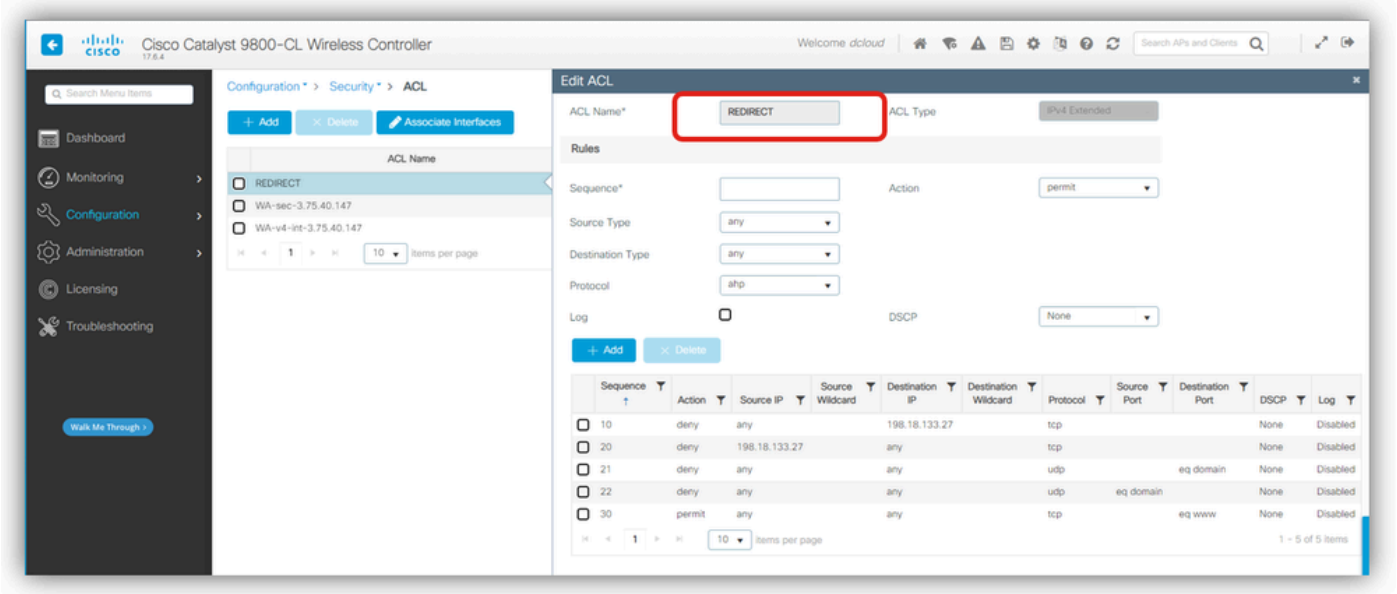
Vérifiez les journaux en direct ISE et les informations de sécurité du client WLC sous Surveillance Vérifiez que l'ISE envoie l'URL de redirection et l'ACL dans l'acceptation d'accès et qu'elle est reçue par le WLC et appliquée au client dans les détails du client :



Redirection ACL et URL

3 - La liste de contrôle d'accès de redirection est correcte ?

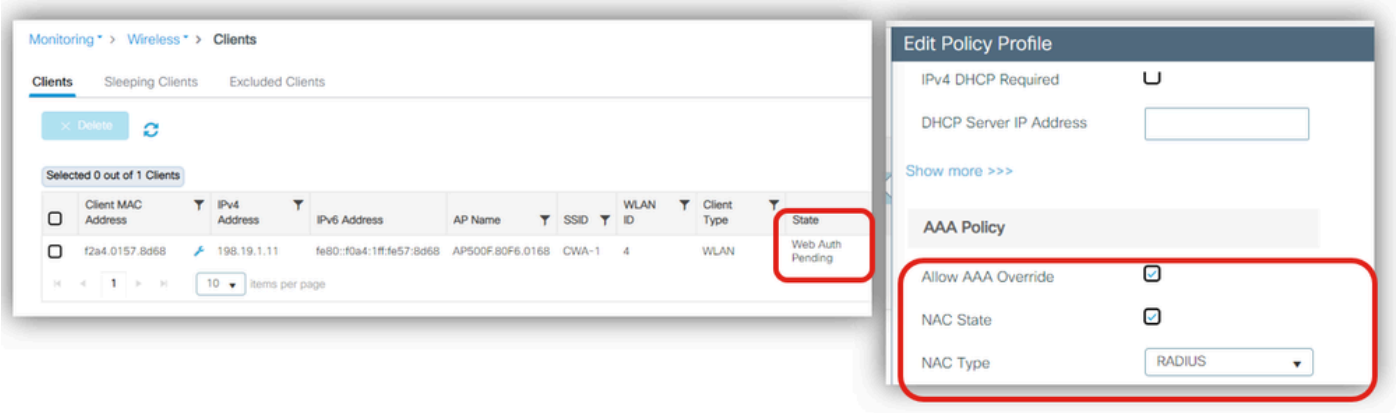
Vérifiez le nom de la liste de contrôle d'accès. Assurez-vous qu'elle est exactement identique à celle envoyée par l'ISE :



Vérification ACL de redirection

4 - Le client est-il déplacé vers Web-Auth Pending ?

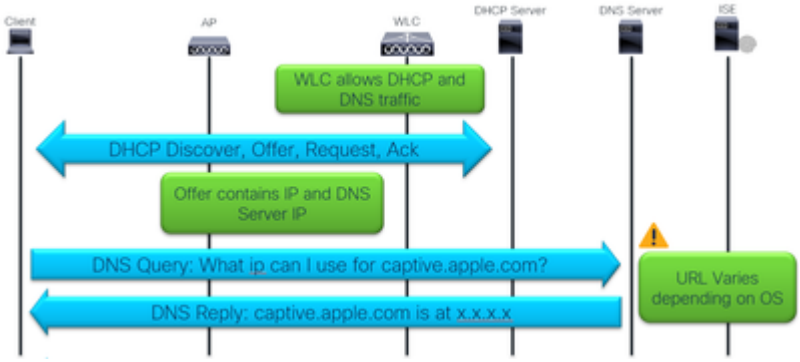
Vérifiez les détails du client pour l'état « Authentification Web en attente ». S'il n'est pas dans cet état, vérifiez si le remplacement AAA et le contrôle d'accès réseau Radius sont activés dans le profil de stratégie :



Détails du client, remplacement aaa et NAC RADIUS

Ça ne marche toujours pas ?

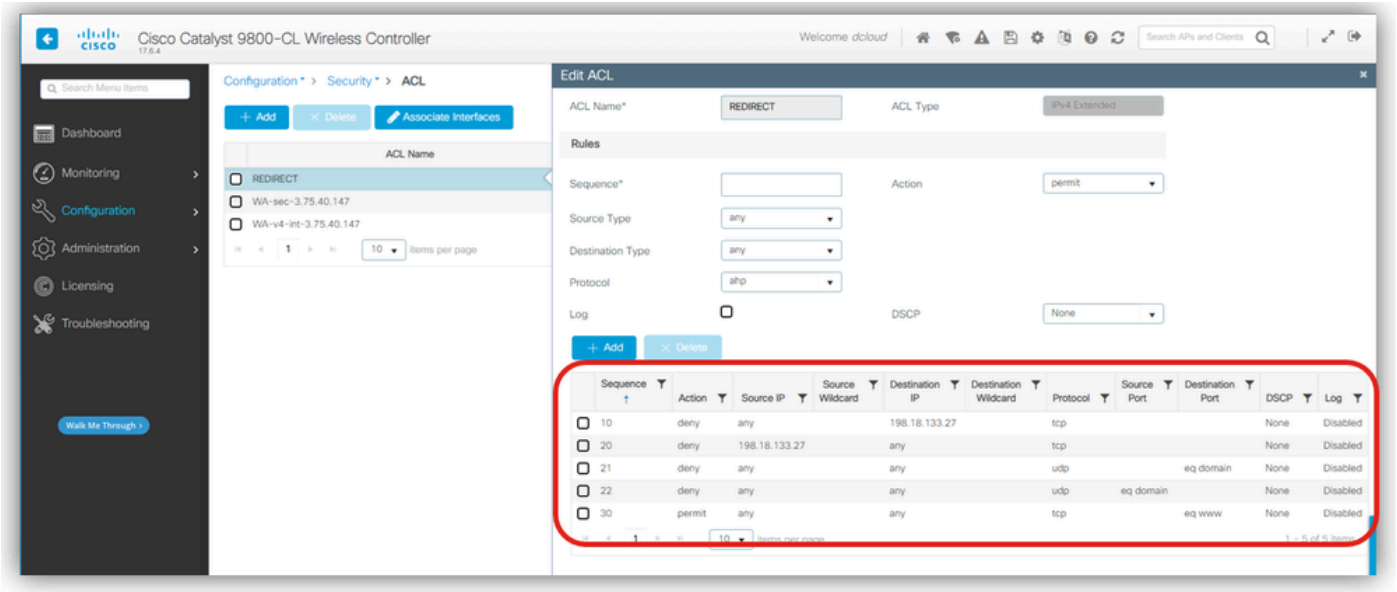
Revoyons le flux... (en anglais)



DHCP, DNS et vérification de la connectivité

5 - Le WLC autorise-t-il le trafic DHCP et DNS ?

Vérifiez le contenu des ACL de redirection dans le WLC :



Rediriger le contenu ACL dans le WLC

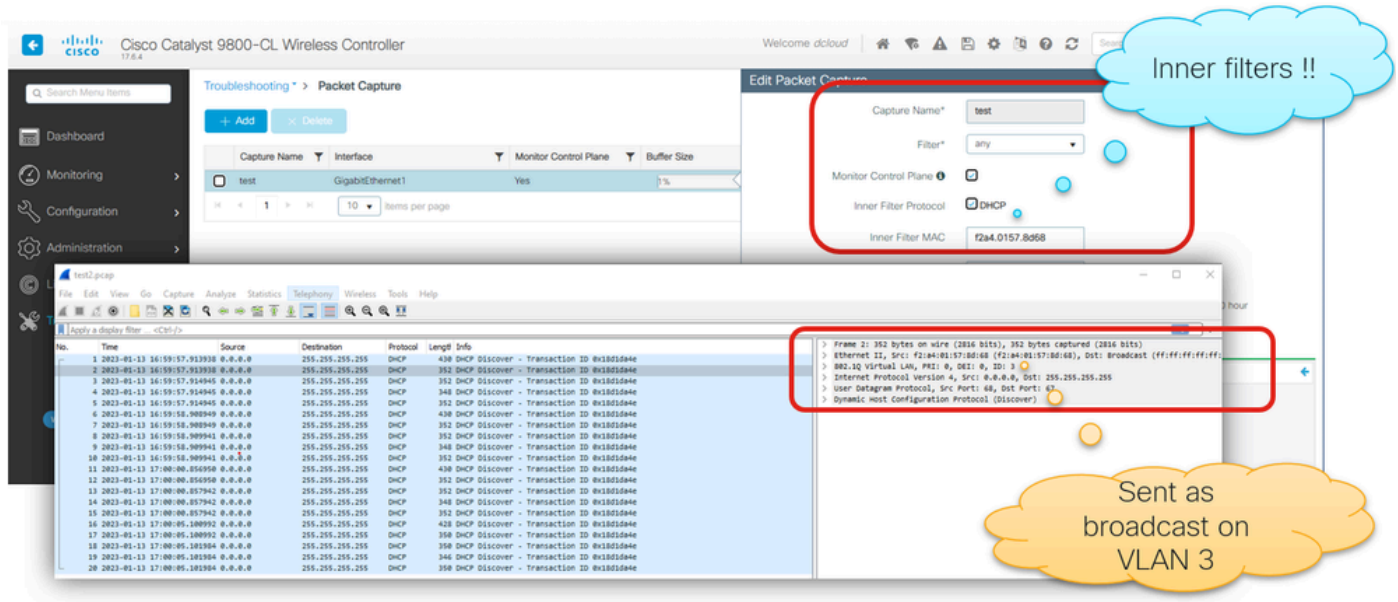
La liste de contrôle d'accès Redirect définit le trafic intercepté et redirigé par l'instruction permit et le trafic ignoré de l'interception et de la redirection avec une instruction deny.

Dans cet exemple, nous autorisons le flux de trafic DNS et de trafic vers/depuis l'adresse IP ISE, et nous interceptons tout trafic TCP sur le port 80 (www).

6 - Le serveur DHCP reçoit-il une détection/requête DHCP ?

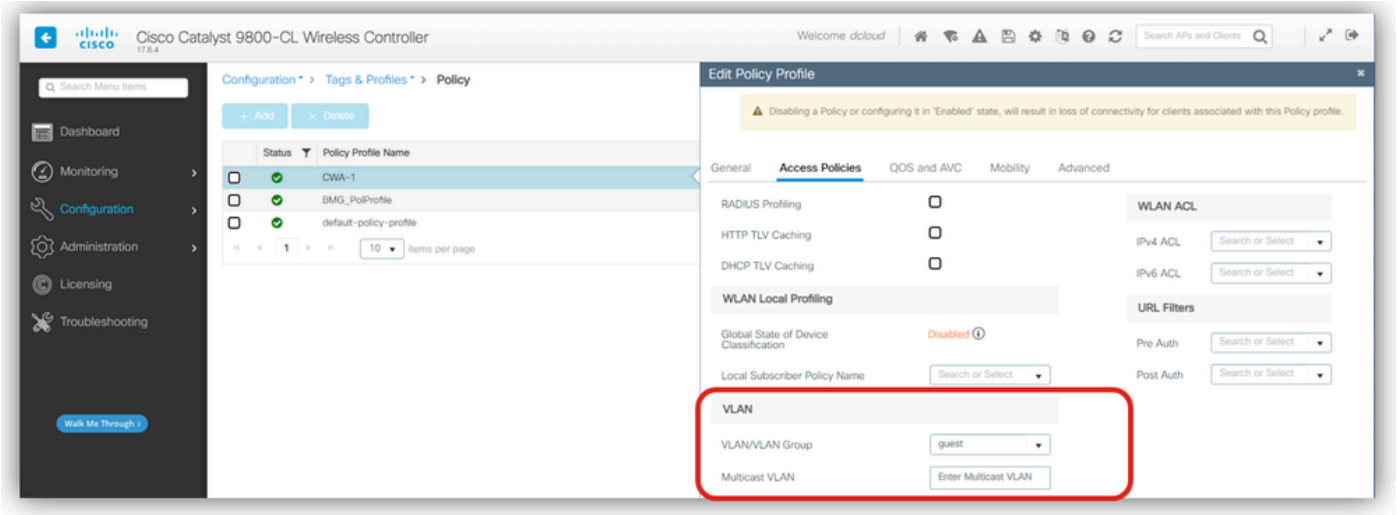
Vérifiez auprès de l'EPC si un échange DHCP a lieu. EPC peut être utilisé avec des filtres internes comme le protocole DHCP et/ou le filtre interne MAC où nous pouvons utiliser l'adresse MAC du périphérique client et nous obtenons dans l'EPC uniquement les paquets DHCP envoyés par ou envoyés à l'adresse MAC du périphérique client.

Dans cet exemple, nous pouvons voir les paquets de détection DHCP envoyés en tant que diffusion sur le VLAN 3 :



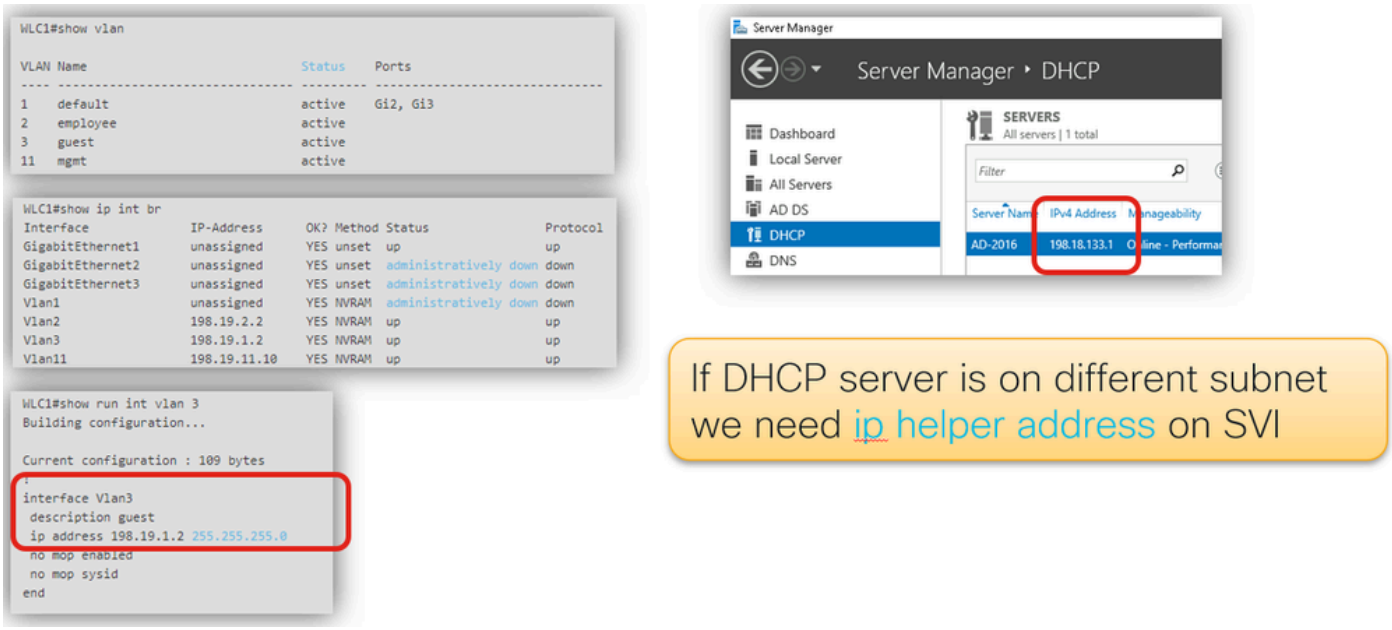
WLC EPC pour vérifier DHCP

Confirmez le VLAN client attendu dans le profil de stratégie :



VLAN dans le profil de stratégie

Vérifier la configuration de VLAN WLC et de switchport Trunk et le sous-réseau DHCP :



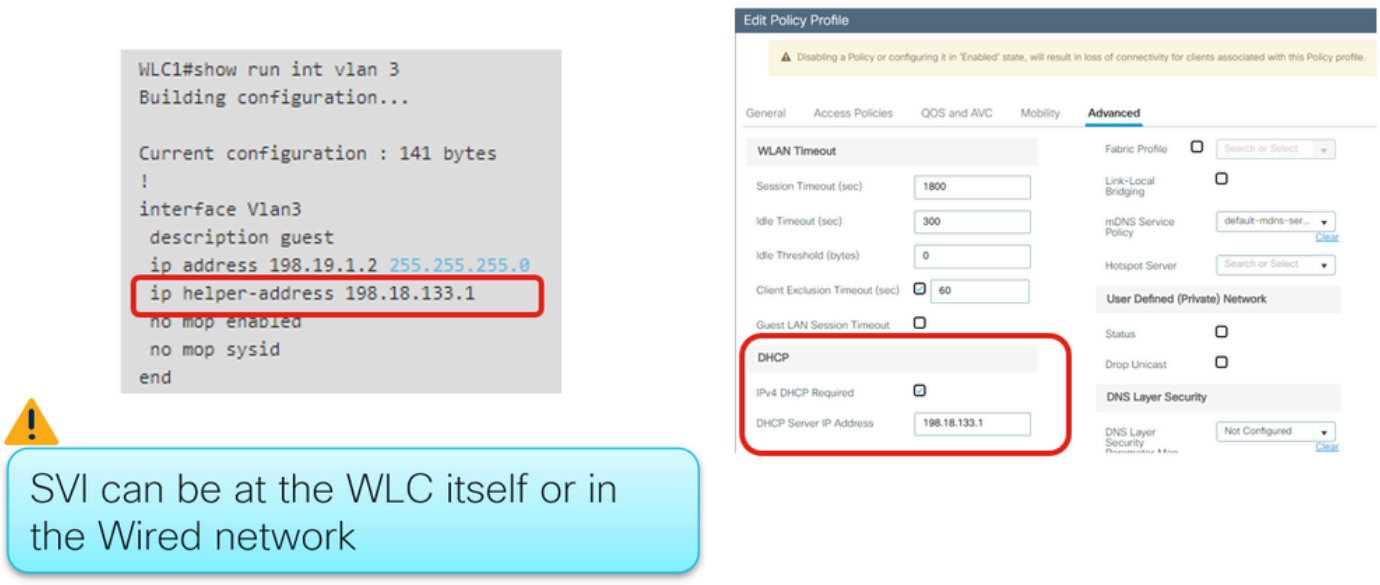
VLAN, port de commutation et sous-réseau DHCP

Nous pouvons voir que VLAN 3 existe dans le WLC et qu'il a également SVI pour VLAN 3, cependant quand nous vérifions l'adresse ip du serveur DHCP, son sur un sous-réseau différent, nous avons donc besoin de l'adresse ip helper sur le SVI.

Les meilleures pratiques exigent que l'interface SVI pour les sous-réseaux clients soit configurée dans l'infrastructure filaire et évitent de les configurer au niveau du WLC.

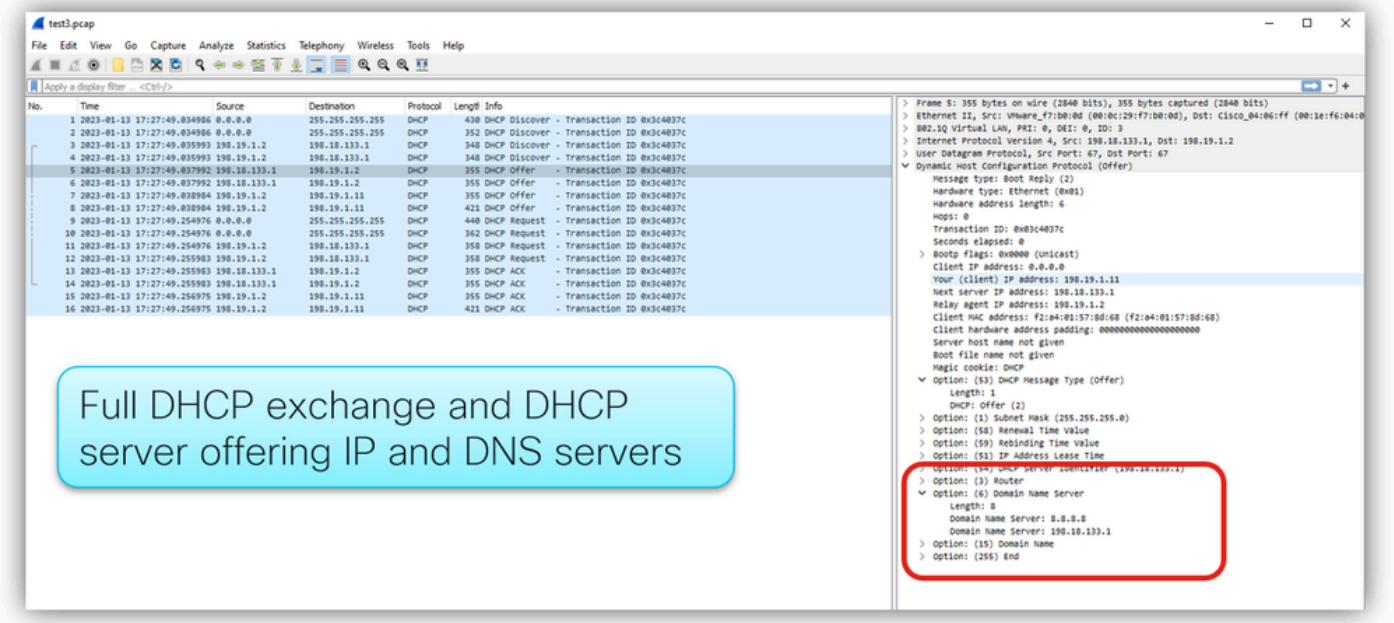
Dans tous les cas, la commande ip helper-address doit être ajoutée à l'interface SVI, quel que soit son emplacement.

Vous pouvez également configurer l'adresse IP du serveur DHCP au niveau du profil de stratégie :



Adresse Ip helper au niveau de l'interface SVI ou du profil de stratégie

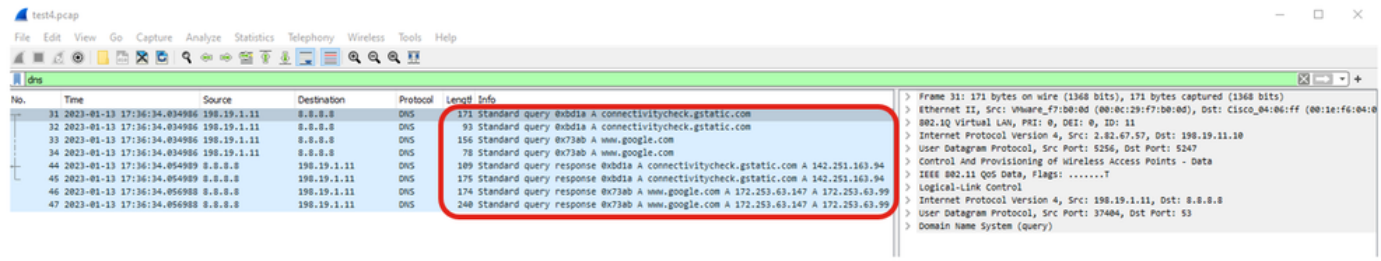
Vous pouvez ensuite vérifier auprès d'EPC si l'échange DHCP est maintenant correct et si le serveur DHCP offre des adresses IP de serveur DNS :



Offre DHCP Détail de l'adresse IP du serveur DNS

7 - La redirection automatique a-t-elle lieu ?

Vérifiez avec WLC EPC si le serveur DNS répond aux requêtes :

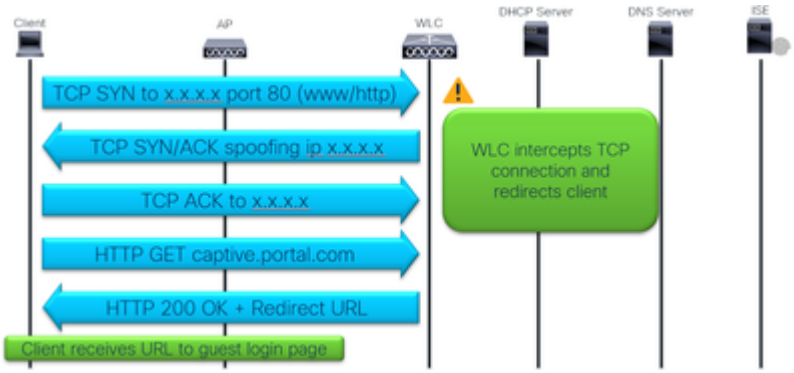


Requêtes et réponses DNS

- Si la redirection n'est pas automatique, ouvrez un navigateur et essayez une adresse IP aléatoire. Par exemple 10.0.0.1.
- Si la redirection fonctionne alors, il est possible que vous ayez un problème de résolution DNS.

Ça ne marche toujours pas ?

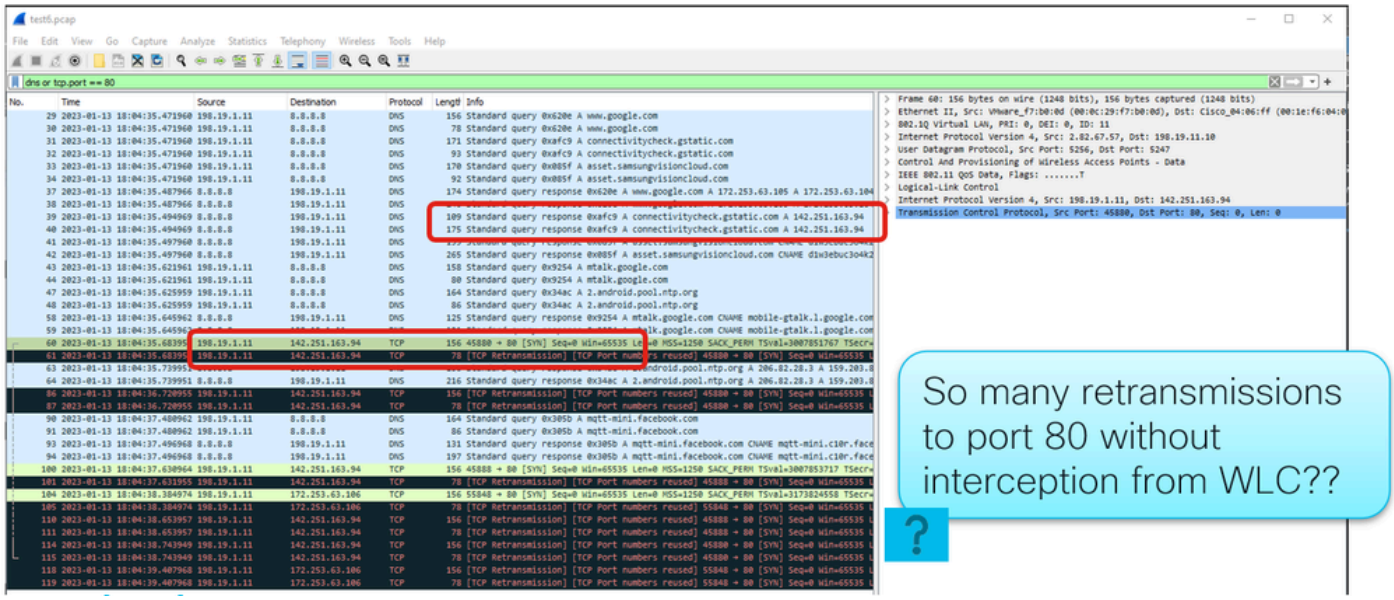
Revenons sur le flux...



Interception et redirection du trafic

8 - Le navigateur n'affiche pas la page de connexion ?

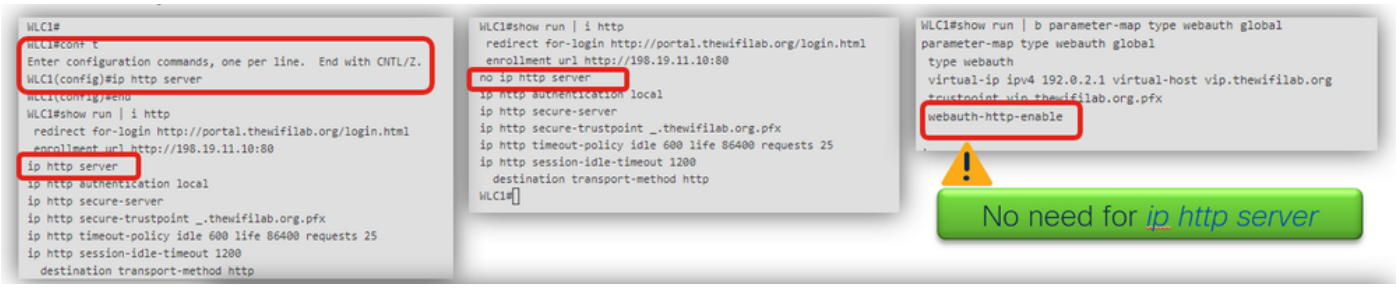
Vérifiez si le client envoie le SYN TCP au port 80 et que le WLC l'intercepte :



Retransmissions TCP vers le port 80

Ici, nous pouvons voir que le client envoie des paquets TCP SYN au port 80 mais n'obtient aucune réponse et effectue des retransmissions TCP.

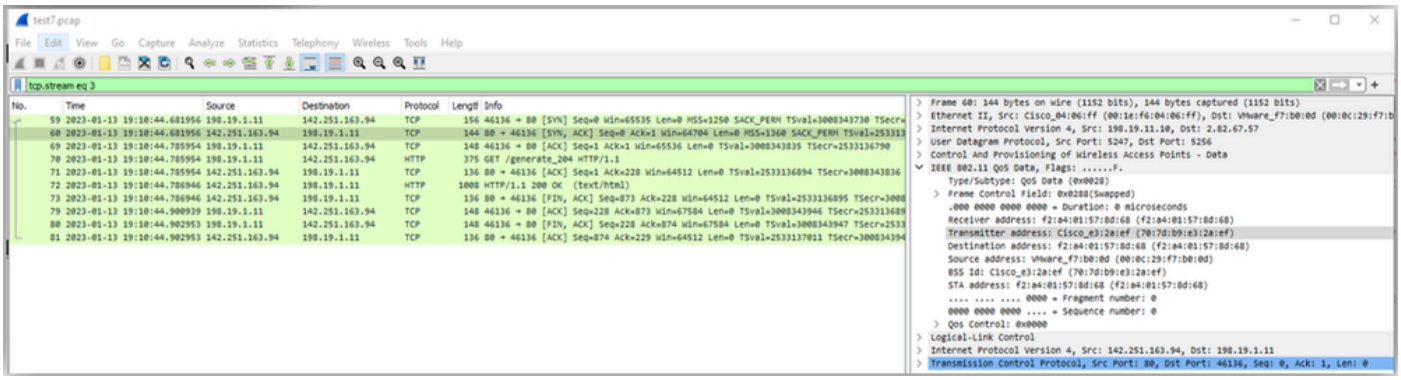
Assurez-vous que vous avez la commande ip http server dans la configuration globale ou webauth-http-enable dans le parameter-map global :



commandes d'interception http

Après la commande, WLC intercepte le TCP et usurpe l'adresse IP de destination pour répondre

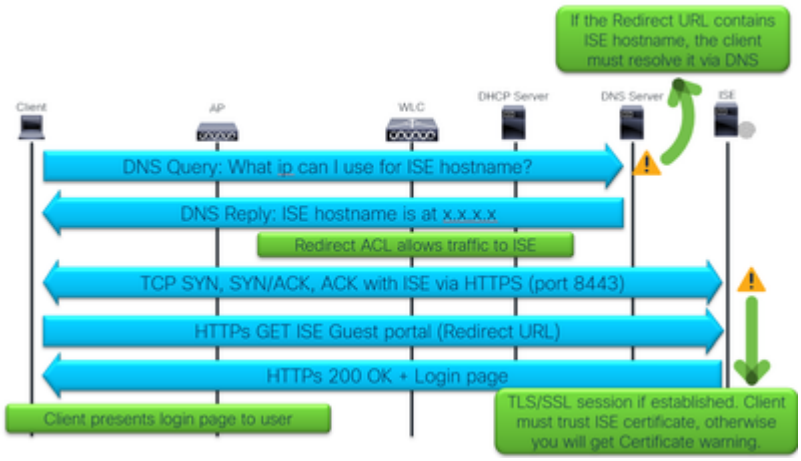
au client et rediriger.



Interception TCP par WLC

Ça ne marche toujours pas ?

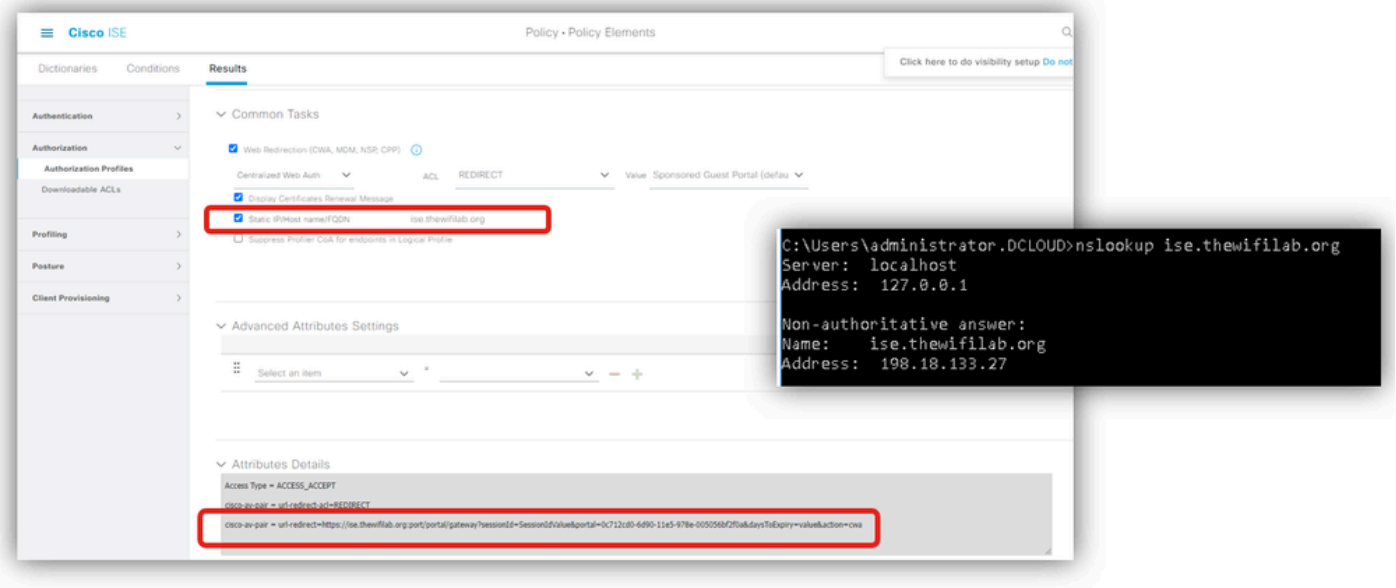
Il y a plus dans le flux...



Connexion du client au portail de connexion des invités ISE

9 - Le client peut-il résoudre le nom d'hôte ISE ?

Vérifiez si l'URL de redirection utilise IP ou le nom d'hôte et si le client résout le nom d'hôte ISE :

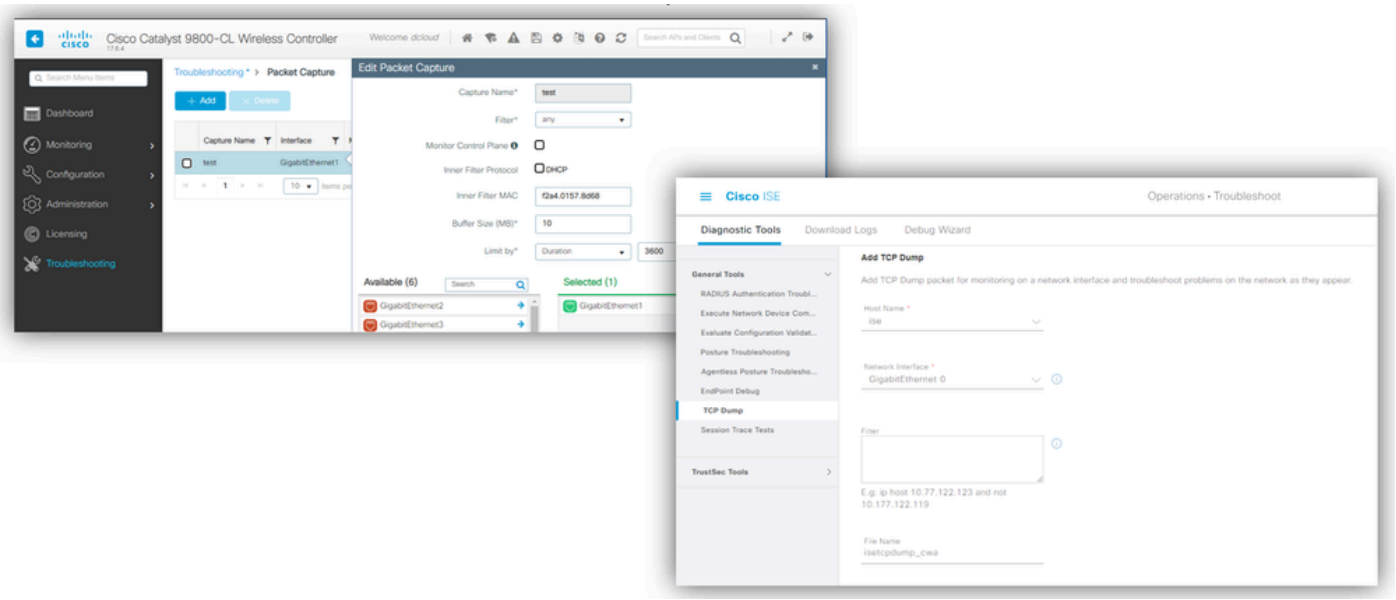


Résolution des noms d'hôte ISE

Un problème courant se produit lorsque l'URL de redirection contient le nom d'hôte ISE, mais le périphérique client ne parvient pas à résoudre ce nom d'hôte en adresse IP ISE. Si le nom d'hôte est utilisé, assurez-vous qu'il peut être résolu via DNS.

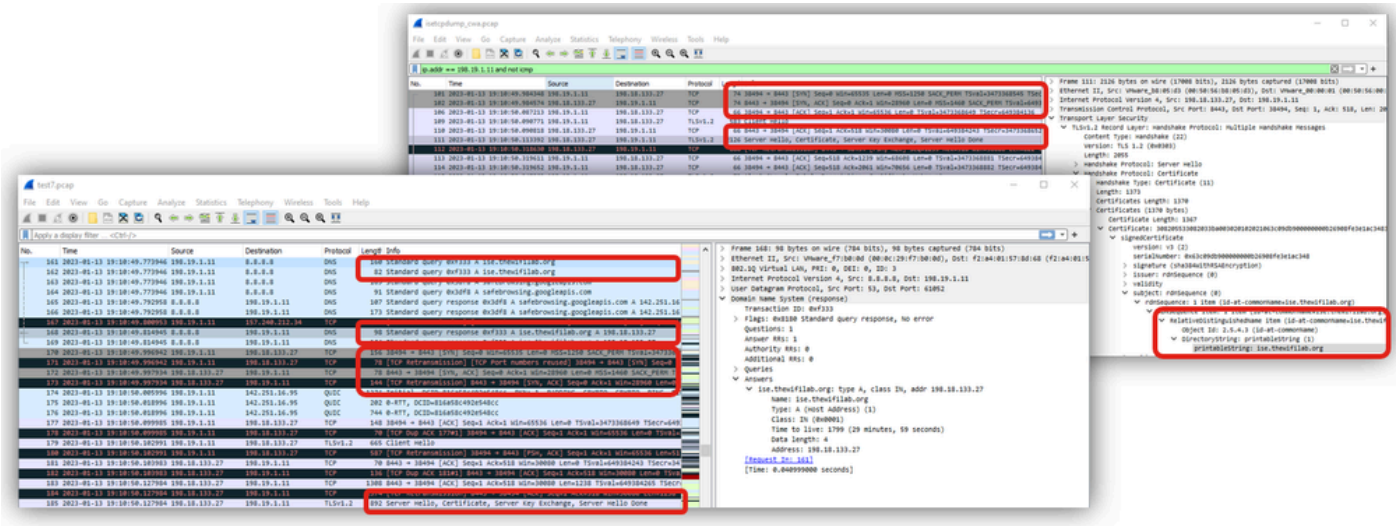
10 - La page de connexion ne se charge toujours pas ?

Vérifiez avec WLC EPC et ISE TCPdump si le trafic client atteint ISE PSN. Configurez et lancez les captures sur WLC et ISE :



WLC EPC et ISE TCPDump

Après la reproduction du problème, collecter les captures et corréler le trafic. Ici, nous pouvons voir le nom d'hôte ISE résolu, puis la communication entre le client et ISE sur le port 8443 :



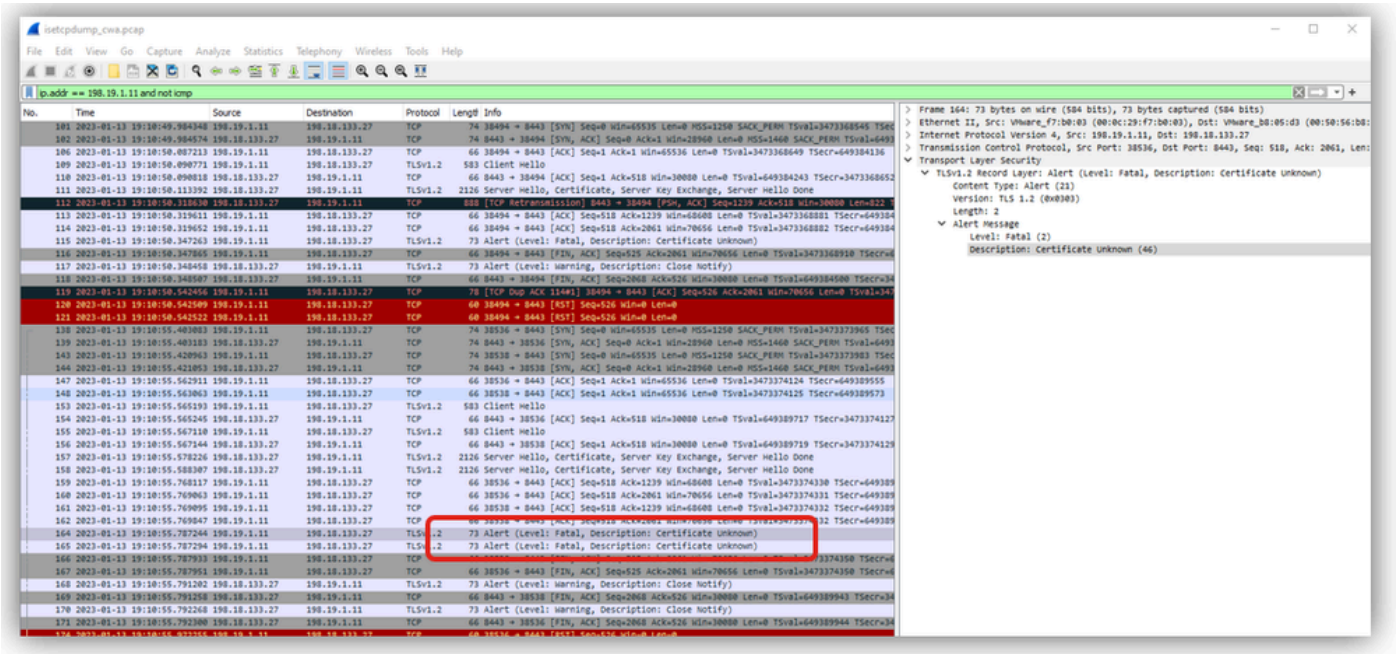
Trafic WLC et ISE

11 - Pourquoi y a-t-il violation de la sécurité en raison d'un certificat ?

Si vous utilisez un certificat auto-signé sur ISE, le client doit lancer un avertissement de sécurité lorsqu'il tente de présenter la page de connexion du portail ISE.

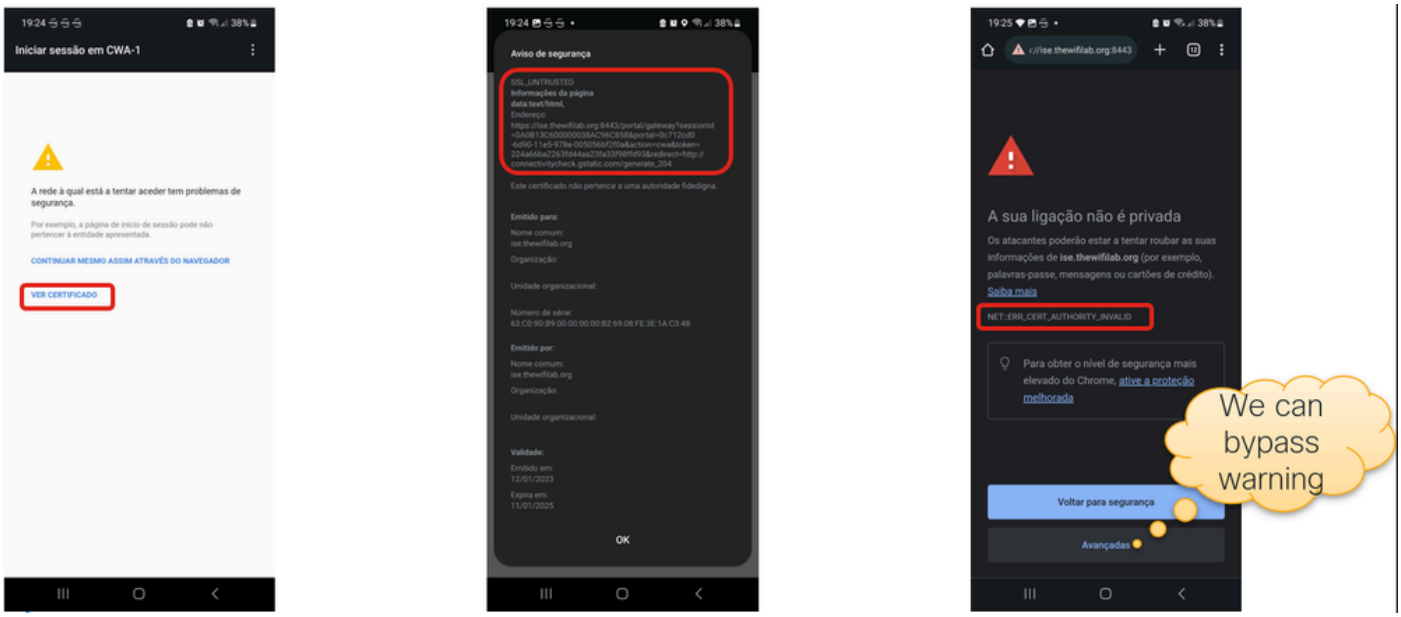
Sur le WLC EPC ou le TCPdump ISE, nous pouvons vérifier si le certificat ISE est approuvé.

Dans cet exemple, nous pouvons voir la fermeture de la connexion à partir du client avec alerte (niveau : Fatal, Description : certificate Unknown), ce qui signifie que le certificat ISE est inconnu (approuvé) :



Certificat ISE non approuvé

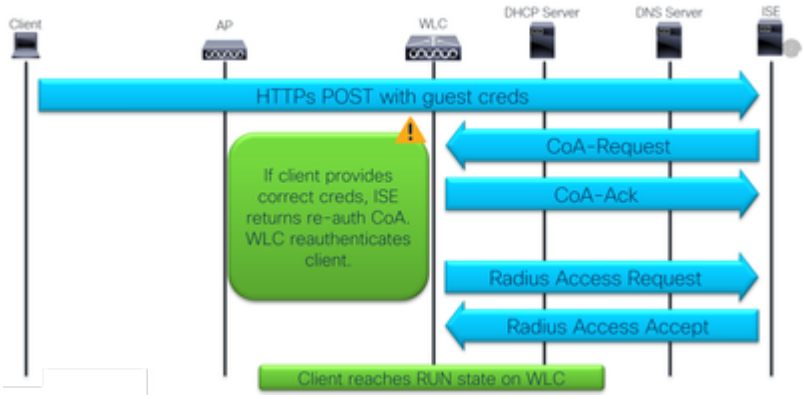
Si nous vérifions côté client, nous voyons ces exemples de sortie :



Périphérique client qui ne fait pas confiance au certificat ISE

Enfin, la redirection fonctionne!! Mais la connexion échoue...

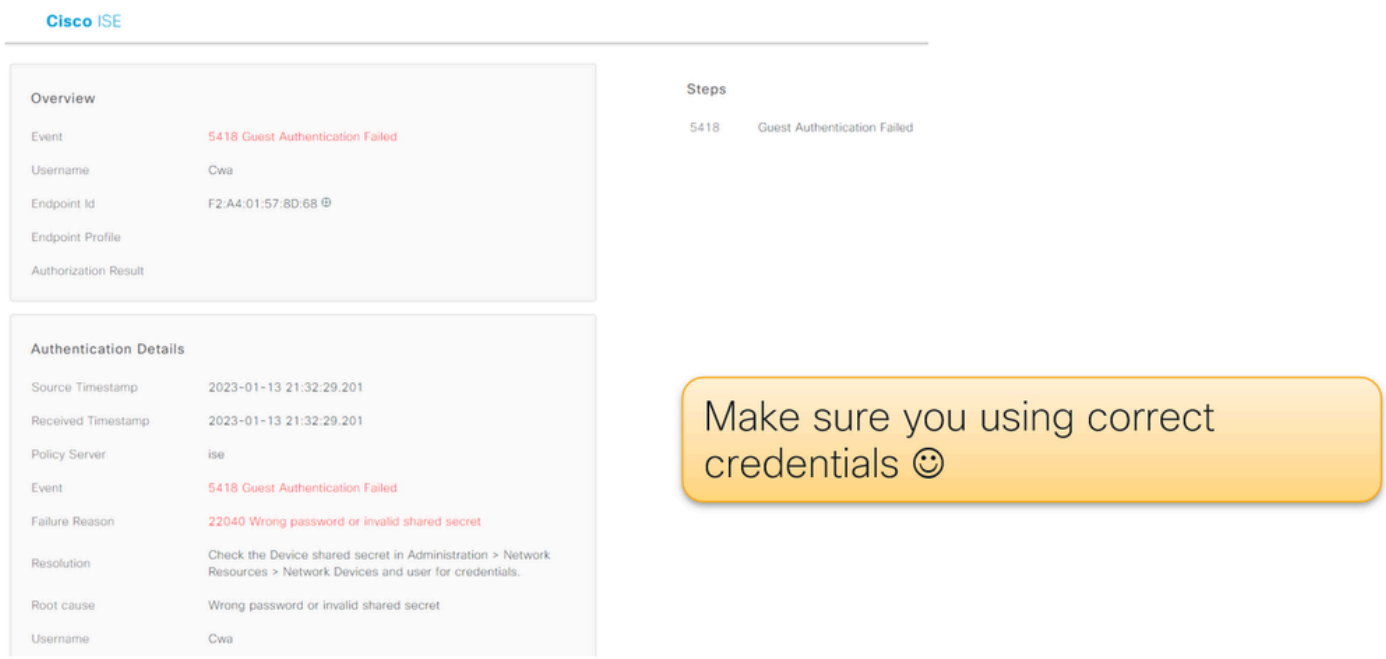
Une dernière fois, vérifier le flux...



Connexion client et CoA

12 - Echec de la connexion invité ?

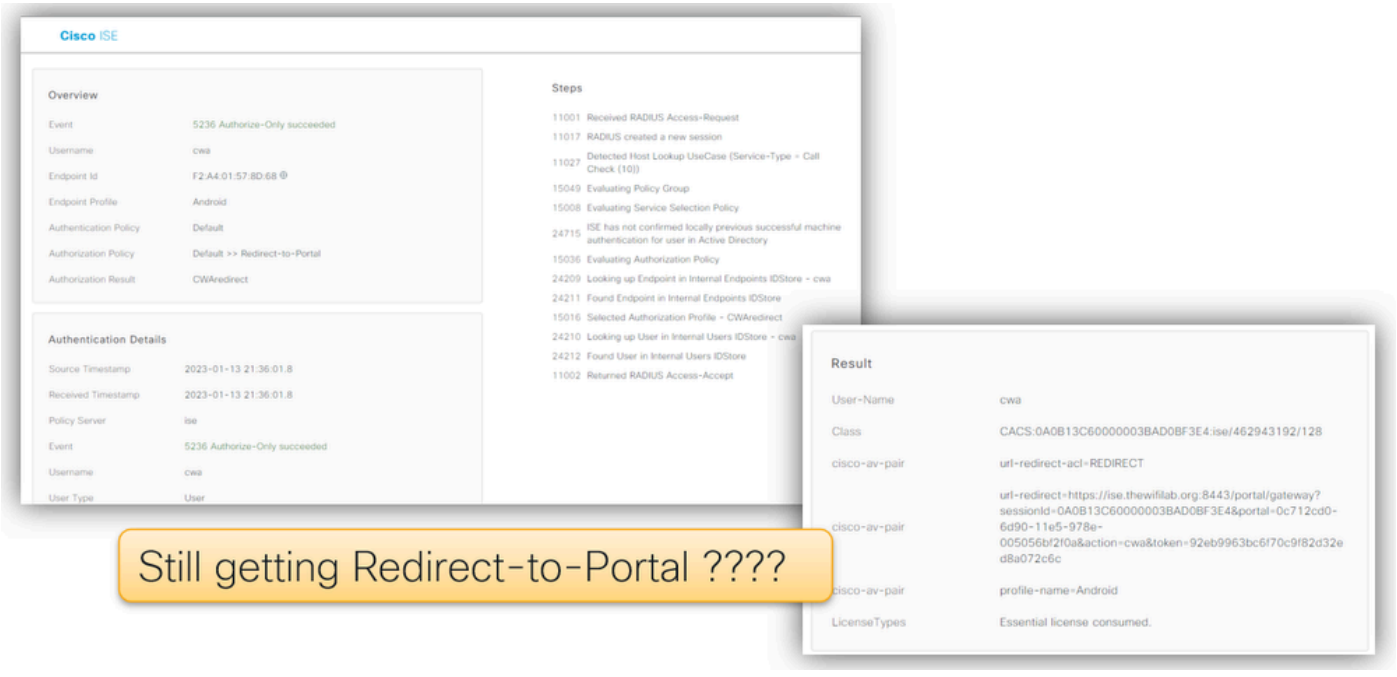
Recherchez les erreurs d'authentification dans les journaux ISE. Vérifiez que les informations d'identification sont correctes.



L'authentification des invités échoue en raison de références incorrectes

13 - La connexion réussit mais ne passe pas à l'exécution ?

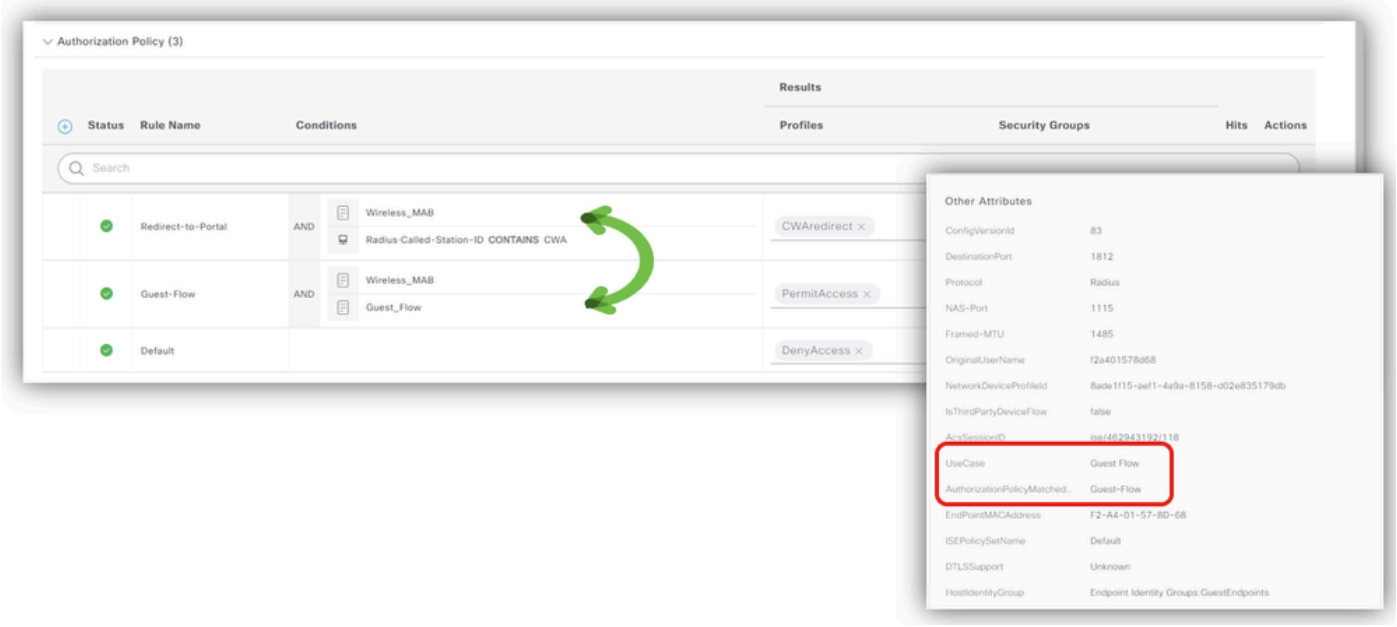
Consultez les journaux ISE pour connaître les détails et le résultat de l'authentification :



Boucle de redirection

Dans cet exemple, nous pouvons voir le client obtenir à nouveau le profil d'autorisation qui contient l'URL de redirection et l'ACL de redirection. Il en résulte une boucle de redirection.

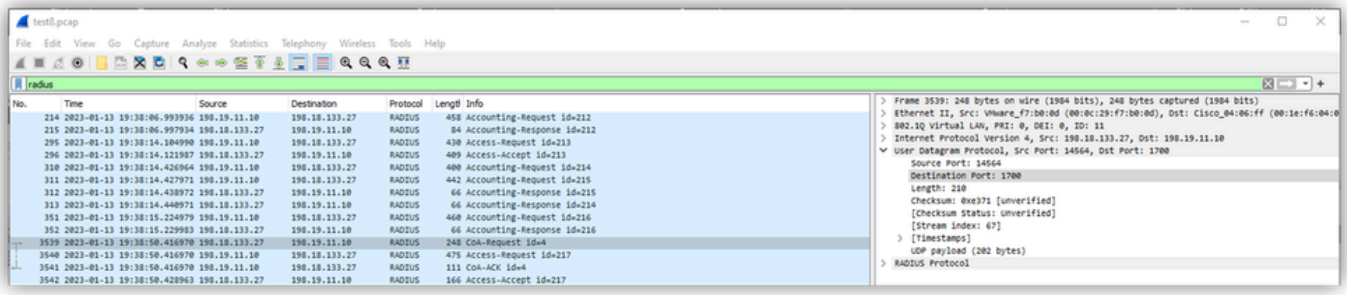
Cochez Stratégie définie. La vérification de la règle Guest_Flow doit être effectuée avant la redirection :



Règle Guest_Flow

14 - Échec du certificat d'authenticité ?

Avec EPC et ISE TCPDump, nous pouvons vérifier le trafic CoA. Vérifiez si le port CoA (1700) est ouvert entre WLC et ISE. Assurez-vous que le secret partagé correspond.



trafic CoA

Remarque : Sur les versions 17.4.X et ultérieures, assurez-vous de configurer également la clé du serveur CoA lorsque vous configurez le serveur RADIUS. Utilisez la même clé que le secret partagé (ils sont identiques par défaut sur ISE). L'objectif est de configurer éventuellement une clé différente pour CoA que le secret partagé si c'est ce que votre serveur RADIUS a configuré. Dans Cisco IOS® XE 17.3, l'interface utilisateur Web utilisait simplement le même secret partagé que la clé CoA.

À partir de la version 17.6.1, RADIUS (y compris CoA) est pris en charge par ce port. Si vous souhaitez utiliser le port de service pour RADIUS, vous devez disposer de la configuration suivante :

<#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
```

Conclusion

Voici la liste de contrôle CWA reprise :

- Assurez-vous que le client se trouve sur le VLAN correct et obtient l'adresse IP et le DNS.

    - Obtenez les détails du client au niveau du WLC et exécutez des captures de paquets pour voir l'échange DHCP.
- Vérifiez que le client peut résoudre les noms d'hôte via DNS.
    - Envoyez une requête ping à hostname depuis cmd.
- WLC doit être à l'écoute sur le port 80
    - Vérifiez la commande globale ip http server ou la commande de mappage de paramètre global webauth-http-enable.
- Pour vous débarrasser de l'avertissement de certificat, installez le certificat de confiance sur ISE.
    - Pas besoin d'installer un certificat de confiance sur le WLC dans CWA.
- Stratégie d'authentification à l'option avancée ISE « Continuer » Si l'utilisateur est introuvable
    - Permettre aux utilisateurs invités parrainés de se connecter et d'obtenir la redirection d'URL et l'ACL.

Et les principaux outils utilisés dans le dépannage :

- EPC WLC
    - Filtres internes : Protocole DHCP, adresse MAC.
- Moniteur WLC
    - Vérifiez les détails de sécurité du client.
- Suivi WLC RA
    - Débogue avec des informations détaillées côté WLC.
- Journaux en direct ISE
    - Détails d'authentification.
- ISE TCPDump
    - Collecter les captures de paquets sur l'interface PSN ISE.

Références

Configurer l'authentification Web centrale (CWA) sur le WLC Catalyst 9800 et ISE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.