Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil

Contenu

Introduction

Ce document fournit des conseils afin de dépanner des questions d'authentification Web dans un environnement Sans fil du contrôleur LAN (WLC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du contrôle et du ravitaillement des points d'accès sans fil (CAPWAP).
- La connaissance de la façon configurer le point d'accès léger (LAP) et le WLC pour le fonctionnement de base.
- Connaissance de base de l'authentification Web et comment configurer l'authentification Web sur WLCs. Pour les informations sur la façon dont configurer l'authentification Web sur WLCs, référez-vous à l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN.

Composants utilisés

Les informations dans ce document sont basées sur un WLC 5500 qui exécute la version 8.3.121 de micrologiciels.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut également être utilisé avec ce matériel :

- Contrôleurs sans fil de la gamme Cisco 5500
- Contrôleurs de radio de gamme Cisco 8500
- Contrôleurs sans-fil de la gamme Cisco 2500
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 3500
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 4000
- Contrôleurs sans-fil de la gamme Cisco Flex 7500
- Cisco Wireless Services Module 2 (WiSM2)

Authentification Web sur WLCs

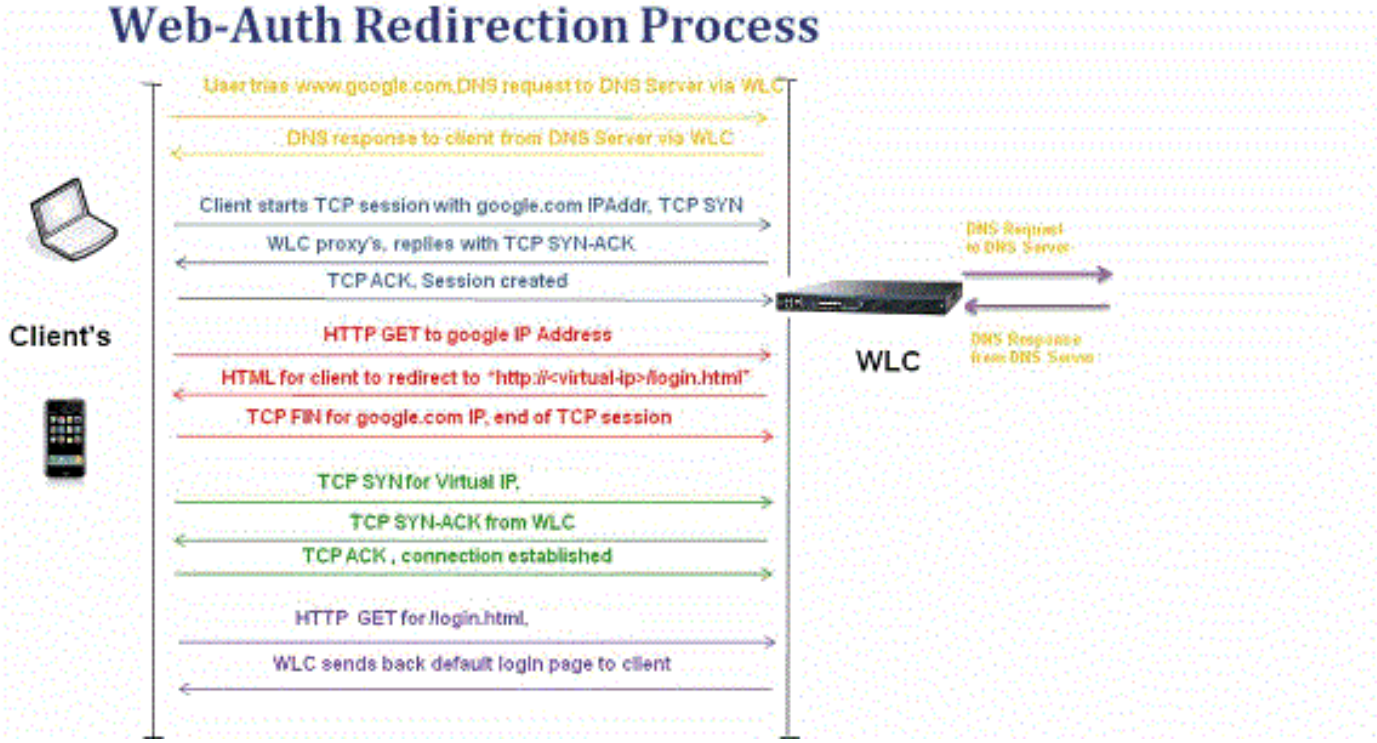
L'authentification Web est une fonctionnalité de sécurité de la couche 3 qui fait ne pas permettre le contrôleur le trafic IP, excepté à paquets liés de Système de noms de domaine (DNS) lié au DHCP de paquets, d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur valide et un mot de passe à une exception du trafic permise par une liste de contrôle d'accès de pre-auth (ACL). L'authentification Web est la seule stratégie de sécurité qui permet au client pour obtenir une adresse IP avant l'authentification. C'est une méthode d'authentification simple sans besoin de suppliant ou d'utilitaire client. L'authentification Web peut être faite localement sur un WLC ou via un serveur RADIUS. L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité.

Les débuts d'authentification Web quand le contrôleur intercepte le premier HTTP de TCP (port 80) OBTIENNENT le paquet du client. Pour que le navigateur Web du client obtienne ceci loin, le client doit d'abord obtenir une adresse IP, et fait une traduction de l'URL à l'adresse IP (résolution de DN) pour le navigateur Web. Ceci fait le navigateur Web connaître quelle adresse IP pour envoyer le HTTP OBTENEZ.

Quand l'authentification Web est configurée sur le WLAN, le contrôleur bloque tout le trafic (jusqu'à ce que la procédure d'authentification est terminée) du client, excepté le DHCP et le trafic DNS. Quand le client envoie le premier HTTP ARRIVEZ au port TCP 80, le contrôleur réoriente le client à https://192.0.2.1/login.html (si c'est l'IP virtuel qui est configuré) pour le traitement. Ce processus évoque par la suite la page Web de procédure de connexion.

> **Note**: Quand vous utilisez un web server externe pour l'authentification Web, les Plateformes WLC ont besoin d'un ACL de pré-authentification pour le web server externe.

Cette section explique le procédé de redirection d'authentification Web en détail.



- Vous ouvrez le navigateur Web et saisissez un URL, par exemple, http://www.google.com. Le client envoie une demande DNS liée à cet URL afin d'obtenir l'IP pour la destination. WLC passe la demande de DN au serveur DNS et le serveur DNS répond de retour avec une réponse de DN, qui contient l'adresse IP de la destination www.google.com, qui consécutivement est expédiée aux clients sans fil.
- Le client tente alors d'établir une connexion TCP avec l'adresse IP de destination. Il envoie un paquet de synchronisation de TCP destiné à l'adresse IP de www.google.com.
- Le WLC a des règles configurées pour le client et par conséquent peut agir en tant que proxy pour www.google.com. Il renvoie un paquet du TCP SYN-ACK au client avec la source comme adresse IP de www.google.com. Le client renvoie un paquet du TCP ACK afin de se terminer la prise de contact à trois voies de TCP et la connexion TCP est entièrement établie.
- Le client envoie un HTTP OBTIENNENT le paquet destiné à www.google.com. Le WLC intercepte ce paquet et l'envoie pour redirection. La passerelle d'application HTTP prépare un corps en HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à se rendre à l'URL de page Web par défaut du WLC, par exemple : http://<Virtual-Server-IP>/login.html.
- Le client ferme la connexion TCP avec l'adresse IP, par exemple www.google.com.
- Maintenant le client veut aller à http:// <virtualip>/login.html et ainsi il essaye d'ouvrir une connexion TCP avec l'adresse IP virtuelle du WLC. Il envoie un paquet de synchronisation de TCP pour 192.0.2.1 (qui est notre IP virtuel ici) au WLC.
- Le WLC répond par un TCP SYN-ACK, et le client renvoie un TCP ACK au WLC afin de terminer la liaison.
- Le client envoie un HTTP OBTIENNENT pour /login.html a destiné à 192.0.2.1 afin de demander la page de connexion.
- Cette demande est permise jusqu'au web server du WLC et le serveur répond de retour avec la page de connexion par défaut. Le client reçoit la page de connexion sur la fenêtre du navigateur, d'où l'utilisateur peut procéder à la connexion.

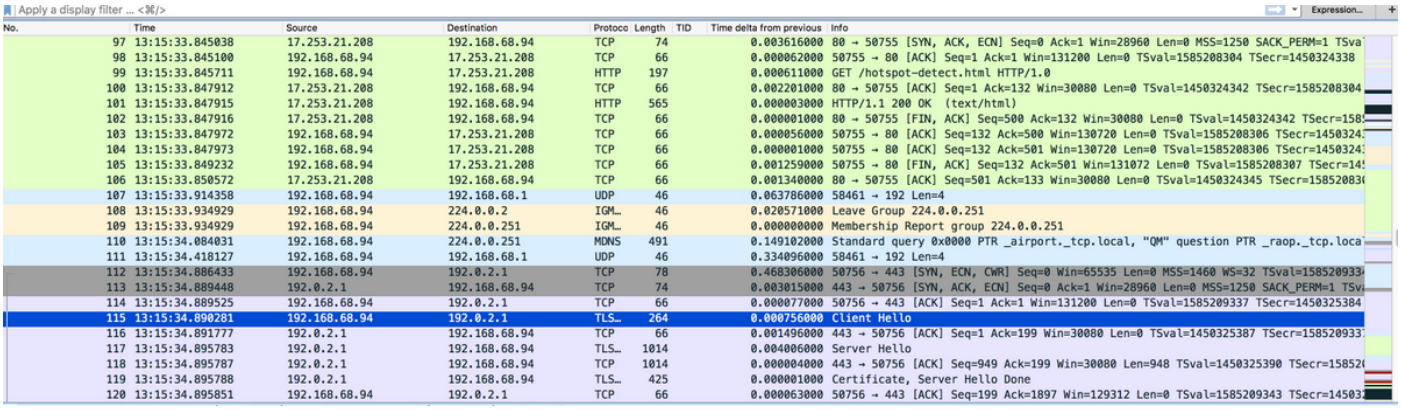
Dans cet exemple, l'adresse IP du client est 192.168.68.94. Le client a résolu l'URL au web server qu'il accédait à, 10.1.0.13. Comme vous pouvez voir, le client a fait la connexion en trois étapes

pour commencer la connexion TCP et a puis envoyé un HTTP OBTIENNENT le paquet commençant par le paquet 96 (00 est le paquet de HTTP). Ceci n'a pas été déclenché par l'utilisateur, mais était le déclenchement portail de détection automatisé par système d'exploitation (comme nous pouvons deviner de l'URL demandée). Le contrôleur intercepte les paquets et les réponses avec le code 200. Le paquet du code 200 a un URL de réorientation dans lui :

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

Il ferme alors la connexion TCP par la connexion en trois étapes.

Le client commence alors la connexion HTTPS à l'URL de réorientation qui l'envoie à 192.0.2.1, qui est l'adresse IP virtuelle du contrôleur. Le client doit valider le certificat de serveur ou l'ignorer afin d'apporter le tunnel SSL. Dans ce cas, c'est un certificat auto-signé ainsi le client l'a ignoré. La page Web de procédure de connexion est envoyée par ce tunnel SSL. Le paquet 112 commence les transactions.



No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=145
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=158520836
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=15852
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=14503

Vous avez l'option de configurer le nom de domaine pour l'adresse IP virtuelle du WLC. Si vous configurez le nom de domaine pour l'adresse IP virtuelle, ce nom de domaine est retourné dans le paquet d'OK de HTTP du contrôleur en réponse au HTTP OBTIENNENT le paquet du client. Vous alors devez exécuter une résolution de DN pour ce nom de domaine. Une fois qu'il obtient une adresse IP de la résolution de DN, il tente d'ouvrir une session TCP avec cette adresse IP, qui est une adresse IP configurée sur une interface virtuelle du contrôleur.

Par la suite, la page Web est traversée le tunnel au client et l'utilisateur renvoie le nom d'utilisateur/mot de passe par le tunnel de Secure Sockets Layer (SSL).

L'authentification Web est exécutée par une de ces trois méthodes :

- Utilisez une page Web interne (par défaut). Référez-vous à choisir la page d'authentication login de web par défaut pour plus d'informations sur l'utilisation de la page Web par défaut.
- Utilisez une page de connexion personnalisée. Référez-vous à créer une page de connexion personnalisée d'authentification Web pour plus d'informations sur la façon utiliser la page de connexion personnalisée.
- Utilisez une page de connexion d'un web server externe. Référez-vous utilisant une page de connexion personnalisée d'authentification Web d'un serveur Web externe pour plus

d'informations sur la façon utiliser une page de connexion d'un web server externe.

Remarques :
- Le paquet personnalisé d'authentification Web a une limite de jusqu'à 30 caractères pour des noms du fichier. Assurez-vous qu'aucun nom du fichier dans le paquet n'est plus grand que 30 caractères.

- De la version 7.0 WLC en avant, si l'authentification Web est activée sur le WLAN et vous avez également des règles d'ACL CPU, les règles basées sur client d'authentification Web ont toujours la priorité plus élevée tant que le client est unauthenticated dans l'état de WebAuth_Reqd. Une fois que le client va à l'état de PASSAGE, les règles d'ACL CPU obtiennent appliqué.

- Par conséquent, si CPU ACLs sont activées dans le WLC, une règle d'autoriser pour l'IP d'interface virtuelle est exigée (dans TOUTE direction) en ces conditions :
 - Quand l'ACL CPU n'a pas un autoriser TOUTE LA règle pour les deux directions.
 - Quand là existe un autoriser TOUTE LA règle, mais là existe également une règle de REFUSER pour le port 443 ou 80 d'une priorité plus élevée.

- La règle d'autoriser pour l'IP virtuel devrait être pour le protocole TCP et le port 80 si le secureweb est désactivé, ou le port 443 si le secureweb est activé. C'est nécessaire afin de permettre l'accès du client à l'authentification réussie de courrier d'adresse IP d'interface virtuelle quand CPU ACLs sont en place.

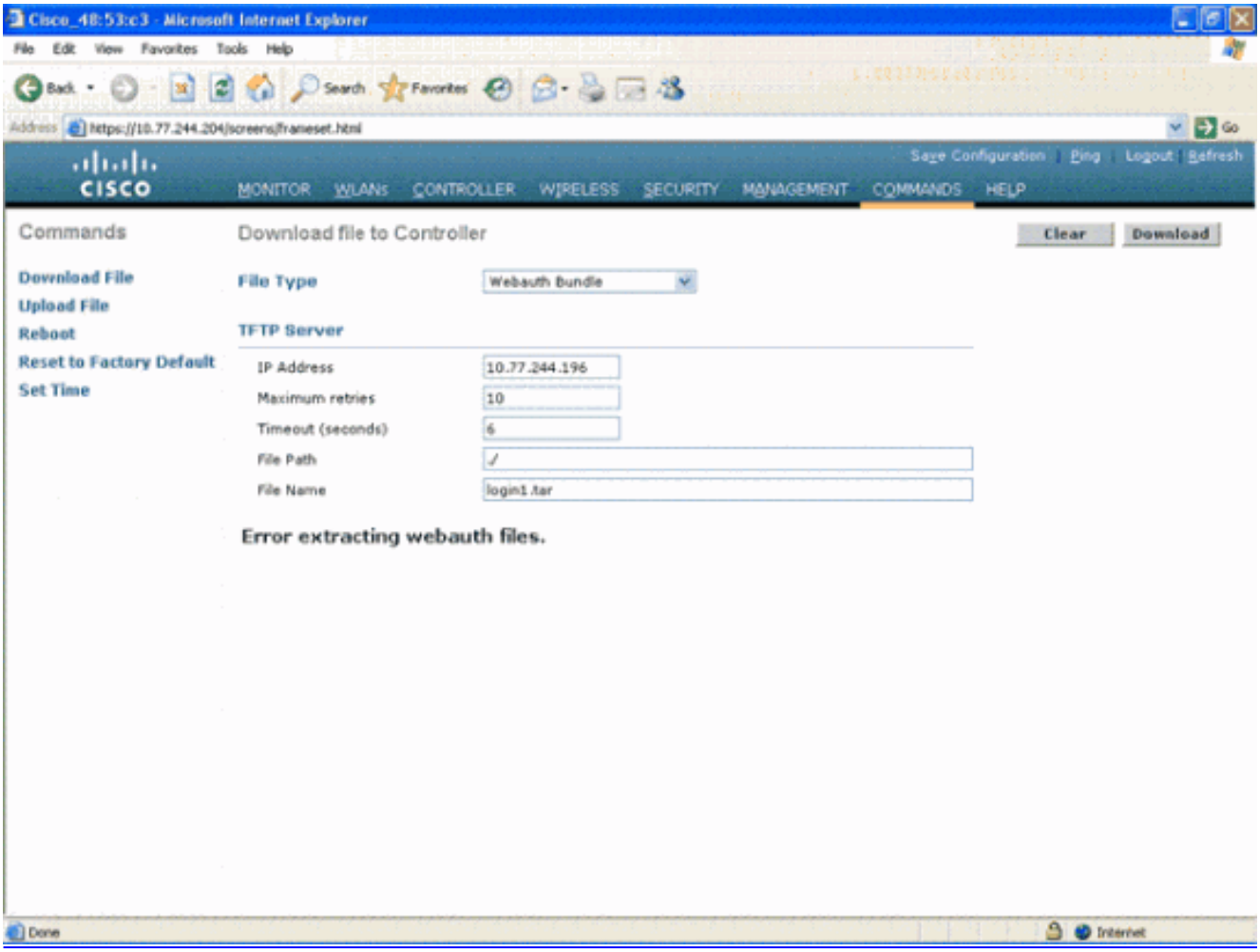
Dépanner l'authentification Web

Après que vous configuriez l'authentification Web et si la caractéristique ne fonctionne pas comme prévu, terminez-vous ces étapes :

1. Vérifiez si le client obtient une adresse IP. Sinon, les utilisateurs peuvent décocher le **DHCP ont exigé la** case sur le WLAN et donnent au client sans fil une adresse IP statique. Ceci assume l'association avec le Point d'accès.
2. L'étape suivante dans le processus est résolution de DN de l'URL dans le navigateur Web. Quand un client WLAN se connecte à un WLAN configuré pour l'authentification Web, le client obtient une adresse IP du serveur DHCP. L'utilisateur ouvre un navigateur Web et introduit une adresse de site Web. Le client exécute alors la résolution de DN d'obtenir l'adresse IP du site Web. Maintenant, quand les essais de client pour atteindre le site Web, le WLC intercepte le HTTP OBTENEZ la session du client et réorientez l'utilisateur à la page de connexion d'authentification Web.
3. , Assurez-vous par conséquent que le client peut exécuter la résolution de DN pour que la redirection fonctionne. Dans Microsoft Windows, choisissez le **Start > Run**, écrivez le **CMD** afin d'ouvrir une fenêtre de commandes, et faites un « nslookup www.cisco.com » et voyez si l'adresse IP revient. Dans des MACs/Linux, ouvrez un terminal window et faites un « nslookup www.cisco.com » et voyez si l'adresse IP revient.Si vous croyez le client n'obtient pas la résolution de DN, vous peut l'un ou l'autre :Écrivez ou l'adresse IP de l'URL (par exemple, http://www.cisco.com est http://198.133.219.25).Essayez de taper n'importe quelle adresse IP (même non-existante) qui devrait la résoudre par l'adaptateur Sans fil.Écrivant cet URL évoque la page Web ? Si oui, il est le plus susceptible un problème de DN. Ce pourrait également être un problème de certificat. Le contrôleur, par défaut, utilise un certificat auto-

signé et la plupart des navigateurs Web mettent en garde contre leur utilisation.

4. Pour l'authentification Web avec une page Web personnalisée, assurez-vous que code HTML pour la page Web personnalisée est approprié. Vous pouvez télécharger un script d'authentification Web d'échantillon des téléchargements logiciels de Cisco. Par exemple, pour les 5508 contrôleurs, choisissez les **Produits > la radio > contrôleur LAN Sans fil > Contrôleurs autonomes > contrôleurs LAN Sans fil de gamme Cisco 5500 > contrôleur LAN > logiciel de radio de Cisco 5508 sur le châssis > paquet Sans fil d'authentification Web de contrôleur réseau local** et téléchargez le **fichier webauth_bundle.zip**.Ces paramètres sont ajoutés à l'URL quand le navigateur Internet de l'utilisateur est réorienté à la page de connexion personnalisée :ap_mac - L'adresse MAC du Point d'accès auquel l'utilisateur de sans fil est associé.switch_url - L'URL du contrôleur auquel les identifiants utilisateurs devraient être signalés.réorientez - L'URL auquel l'utilisateur est réorienté après l'authentification est réussie.code statut - Code d'état est retourné du serveur de l'authentification Web du contrôleur.wlan - Le WLAN SSID auquel l'utilisateur de sans fil est associé.Ce sont codes d'état disponibles :Code d'état 1 - « vous êtes déjà ouvert une session. Aucune action supplémentaire n'est exigée sur votre cloison »Code d'état 2 - « vous n'êtes pas configuré pour authentifier contre le portail web. Aucune action supplémentaire n'est exigée sur votre cloison »Code d'état 3 - « le nom d'utilisateur spécifié ne peut pas être utilisé à ce moment. Peut-être le nom d'utilisateur est déjà connecté dans le système ? »Code d'état 4 - « vous avez été exclu. »Code d'état 5 - « la combinaison de nom d'utilisateur et de mot de passe que vous avez écrite est non valide. Essayez s'il vous plaît de nouveau. »
5. Tous les fichiers et images qui doivent apparaître sur la page Web personnalisée devraient être empaquetés dans un fichier de .tar avant qu'il soit téléchargé au WLC. Assurez-vous qu'un des fichiers inclus dans le paquet de .tar est login.html. Vous recevez ce message d'erreur si vous n'incluez pas le fichier de login.html :



Référez-vous aux instructions pour la section d'authentification Web Customized de l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN pour plus d'informations sur la façon créer une fenêtre personnalisée d'authentification Web.**Note**: Les fichiers qui sont grands et les fichiers qui ont de longs noms auront comme conséquence une erreur d'extraction. Les images d'il est recommandé que sont dans le format de .jpg.

6. Assurez-vous que l'option de **script** n'est pas bloquée sur le navigateur de client car la page Web personnalisée sur le WLC est fondamentalement un script HTML.
7. Si vous avez un **nom d'hôte** configuré pour l'**interface virtuelle du** WLC, assurez-vous que la résolution de DN est disponible pour le nom d'hôte de l'interface virtuelle. **Note**: Naviguez vers le menu de **Controller > Interfaces du** GUI WLC afin d'assigner une **adresse Internet de DN à l'**interface virtuelle.
8. Parfois le Pare-feu installé sur l'ordinateur client bloque la page de connexion d'authentification Web. Désactivez le Pare-feu avant que vous essayiez d'accéder à la page de connexion. Le Pare-feu peut être activé de nouveau une fois que l'authentification Web est terminée.
9. Le Pare-feu de topologie/solution peut être placé entre le client et le serveur de Web-auth, qui dépend du réseau. Quant à chaque conception de réseaux/solution mises en application, l'utilisateur final devrait s'assurer qu'on permet ces ports sur le pare-feu réseau.

10. Pour que l'authentification Web se produise, le client devrait d'abord s'associer au WLAN approprié sur le WLC. Naviguez vers le menu de **Monitor > Clients** sur le GUI WLC afin de voir si le client est associé au WLC. Vérifiez si le client a une adresse IP valide.
11. Désactivez les paramètres de proxy sur le navigateur de client jusqu'à ce que l'authentification Web soit terminée.

12. La méthode d'authentification de web par défaut est Password Authentication Protocol (PAP). Assurez-vous qu'on permet à l'authentification PAP sur le serveur de RADIUS pour que ceci fonctionne. Afin de vérifier le statut d'authentification client, vérifiez met au point et les messages de log du serveur de RADIUS. Vous pouvez employer le **debug aaa toute la** commande sur le WLC afin de visualiser met au point du serveur de RADIUS.
13. Mettez à jour le driver du matériel sur l'ordinateur au dernier code du site Internet du constructeur.
14. Vérifiez les configurations dans le suppliant (programme sur l'ordinateur portable).
15. Quand vous utilisez le suppliant de config de Windows Zero construit dans Windows : Vérifiez l'utilisateur fait installer les derniers correctifs.Exécutez-vous met au point sur le suppliant.
16. Sur le client, activez l'EAPOL (WPA+WPA2) et RASTLS se connecte d'une fenêtre de commandes. Choisissez le **Start > Run > le CMD** :
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    Afin de désactiver les logs, exécutez la même commande mais remplacez l'enable par le débronchement. Pour le XP, tous les logs veulent se trouvent dans C:\Windows\tracing.
17. Si vous n'avez toujours aucune page Web de procédure de connexion, collectez et analysez cette sortie d'un client simple :
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. Si la question n'est pas résolue après que vous vous terminiez ces étapes, collectez ces derniers gestionnaire de cas de support met au point et d'utilisation afin d'ouvrir une demande de service.
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Support et documentation techniques - Cisco Systems