Comprendre l'authentification Web sur les contrôleurs LAN sans fil (WLC)

Contenu

Introduction

Ce document décrit les processus d'authentification Web sur les contrôleurs de réseau local sans fil (WLC).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez des connaissances de base sur la configuration WLC.

Components Used

Les informations de ce document sont basées sur tous les modèles de matériel WLC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Processus internes d'authentification Web

Positionnement de l'authentification Web en tant que fonctionnalité de sécurité

L'authentification Web (WebAuth) est une sécurité de couche 3. Il offre une sécurité conviviale qui fonctionne sur n'importe quelle station exécutant un navigateur.

Il peut être combiné à n'importe quelle sécurité de clé prépartagée (politique de sécurité de couche 2).

Bien que la combinaison de WebAuth et de PSK réduise la partie conviviale, elle présente l'avantage de chiffrer le trafic client.

WebAuth est une méthode d'authentification sans chiffrement.

WebAuth ne peut pas être configuré avec 802.1x/RADIUS (Remote Authentication Dial-In User Service) tant que le logiciel WLC version 7.4 n'est pas installé et configuré simultanément.

Les clients doivent passer à la fois par l'authentification point1x et Web. Il est destiné à l'ajout d'un portail Web pour les employés (qui utilisent 802.1x) et non pour les invités.

Il n'existe pas d'identifiant SSID (Service Set Identifier) tout-en-un pour dot1x pour les employés ou de portail Web pour les invités.

Fonctionnement de WebAuth

Le processus d'authentification 802.11 est ouvert, vous pouvez donc vous authentifier et vous associer sans aucun problème. Ensuite, vous êtes associé, mais pas dans le WLC **RUN** province.

Lorsque l'authentification Web est activée, vous restez **WEBAUTH_REQD** où vous ne pouvez accéder à aucune ressource réseau.

Vous devez recevoir une adresse IP DHCP avec l'adresse du serveur DNS dans les options.

Tapez une URL valide dans votre navigateur. Le client résout l'URL via le protocole DNS. Le client envoie ensuite sa requête HTTP à l'adresse IP du site Web.

Le WLC intercepte cette requête et retourne le **webauth** , qui imite l'adresse IP du site Web. Avec

un WebAuth externe, le WLC répond avec une réponse HTTP qui inclut l'adresse IP de votre site Web et indique que la page a été déplacée.

La page a été déplacée vers le serveur Web externe utilisé par le WLC. Lorsque vous êtes authentifié, vous accédez à toutes les ressources réseau et êtes redirigé vers l'URL demandée à l'origine par défaut (sauf si une redirection forcée a été configurée sur le WLC).

En résumé, le WLC permet au client de résoudre le DNS et d'obtenir une adresse IP automatiquement dans **WEBAUTH_REQD** province.

Pour surveiller un autre port au lieu du port 80, utilisez **config network web-auth-port** pour créer une redirection sur ce port également.

L'interface Web ACS (Access Control Server), qui se trouve sur le port 2002 ou d'autres applications similaires, en est un exemple.

> **Remarque sur la redirection HTTPS** : Par défaut, le WLC n'a pas redirigé le trafic HTTPS. Cela signifie que si vous tapez une adresse HTTPS dans votre navigateur, rien ne se passe. Vous devez taper une adresse HTTP afin d'être redirigé vers la page de connexion qui a été servie dans HTTPS.
>
> Dans les versions 8.0 et ultérieures, vous pouvez activer la redirection du trafic HTTPS à l'aide de la commande CLI **config network web-auth https-redirect enable.**
>
> Cela utilise beaucoup de ressources pour le WLC dans les cas où de nombreuses requêtes HTTPS sont envoyées. Il n'est pas conseillé d'utiliser cette fonctionnalité avant la version 8.7 du WLC où l'évolutivité de cette fonctionnalité a été améliorée. Notez également qu'un avertissement de certificat est inévitable dans ce cas. Si le client demande une URL (telle que https://www.cisco.com), le WLC présente toujours son propre certificat émis pour l'adresse IP de l'interface virtuelle. Cela ne correspond jamais à l'adresse URL/IP demandée par le client et le certificat n'est pas approuvé sauf si le client force l'exception dans son navigateur.

Diminution indicative des performances de la version logicielle du WLC antérieure à 8.7 mesurée :

Webauth	Taux atteint
3 URL - HTTP	140/seconde
1re URL - HTTP 2ème et 3ème URL - HTTPS	20/seconde
3 URL - HTTPS (grand déploiement)	<1/seconde
3 URL - HTTPS (maximum de 100 clients)	10/seconde

Dans ce tableau de performances, les 3 URL sont appelées :

- URL d'origine saisie par l'utilisateur final
- URL vers laquelle le WLC redirige le navigateur
- Envoi des identifiants finaux

Le tableau des performances indique les performances du WLC dans le cas où les 3 URL sont toutes HTTP, dans le cas où les 3 URL sont toutes HTTPS, ou si le client passe de HTTP à HTTPS (typique).

Comment faire fonctionner un WebAuth interne (local) avec une page interne

Pour configurer un WLAN avec une interface dynamique opérationnelle, les clients reçoivent également une adresse IP de serveur DNS via DHCP.

Avant toute **webauth** , est défini, vérifiez que le WLAN fonctionne correctement, que les requêtes DNS peuvent être résolues (**nslookup**) et les pages Web peuvent être consultées.

Définissez l'authentification Web en tant que fonctions de sécurité de couche 3. Créez des utilisateurs dans la base de données locale ou sur un serveur RADIUS externe.

Référez-vous au document Exemple de configuration d'authentification Web du contrôleur LAN sans fil.

Configuration d'une authentification Web locale personnalisée avec une page personnalisée

Personnalisé **webauth** peut être configuré avec **redirectUrl** a partir des versions **Security** s'affiche. Cela force une redirection vers une page Web spécifique que vous entrez.

Lorsque l'utilisateur est authentifié, il remplace l'URL d'origine demandée par le client et affiche la page pour laquelle la redirection a été attribuée.

La fonction personnalisée vous permet d'utiliser une page HTML personnalisée au lieu de la page de connexion par défaut. Téléchargez votre bundle de fichiers html et image sur le contrôleur.

Dans la page de téléchargement, recherchez **webauth bundle** au format tar. PicoZip crée des étoiles qui fonctionnent de manière compatible avec le WLC.

Pour obtenir un exemple d'ensemble WebAuth, reportez-vous à la page Download Software pour Wireless Controller WebAuth Bundles. Sélectionnez la version appropriée pour votre WLC.

Il est recommandé de personnaliser un bundle existant ; ne créez pas de nouveau bundle.

Il y a quelques limites avec **custom webauth** qui varient selon les versions et les bogues.

- la taille du fichier .tar (pas plus de 5 Mo)
- le nombre de fichiers dans le fichier .tar
- la longueur du nom de fichier des fichiers (pas plus de 30 caractères)

Si le package ne fonctionne pas, essayez un package personnalisé simple. Ajoutez individuellement des fichiers et de la complexité pour atteindre le package que l'utilisateur a essayé d'utiliser. Cela permet d'identifier le problème.

Pour configurer une page personnalisée, référez-vous à Création d'une page de connexion d'authentification Web personnalisée, une section dans le Guide de configuration du contrôleur LAN sans fil Cisco, version 7.6.

Remplacer la technique de configuration globale

Configurez avec la commande **override global config** et définissez un type WebAuth pour chaque WLAN. Cela permet une WebAuth interne/par défaut avec une WebAuth interne/par défaut personnalisée pour un autre WLAN.

Cela permet de configurer différentes pages personnalisées pour chaque WLAN.

Combinez toutes les pages dans le même bundle et téléchargez-les sur le WLC.

Définissez votre page personnalisée avec la commande **override global config** sur chaque WLAN et sélectionnez quel fichier est la page de connexion parmi tous les fichiers du bundle.

Choisissez une page de connexion différente à l'intérieur du bundle pour chaque WLAN.

Problème de redirection

Il y a une variable dans le bundle HTML qui permet la redirection. N'y placez pas votre URL de redirection forcée.

Pour les problèmes de redirection dans WebAuth personnalisé, Cisco recommande de vérifier le bundle.

Si vous entrez une URL de redirection avec **+=** dans l'interface graphique du WLC, cela pourrait écraser *ou* ajouter à l'URL définie à l'intérieur de l'ensemble.

Par exemple, dans l'interface utilisateur graphique du WLC, le **redirectURL** est défini sur www.cisco.com ; cependant, dans le bundle, il montre : **redirectURL+=** '(URL du site Web)'. Le signe **+=** redirige les utilisateurs vers une URL non valide.

Comment faire fonctionner une authentification Web externe (locale) avec une page externe

L'utilisation d'un serveur WebAuth externe n'est qu'un référentiel externe pour la page de connexion. Les informations d'identification de l'utilisateur sont toujours authentifiées par le WLC. Le serveur Web externe autorise uniquement une page de connexion spéciale ou différente.

Étapes effectuées pour un WebAuth externe :

1. Le client (utilisateur final) ouvre un navigateur Web et saisit une URL.

2. Si le client n'est pas authentifié et que l'authentification Web externe est utilisée, le WLC redirige l'utilisateur vers l'URL du serveur Web externe. Le WLC envoie une redirection HTTP au client avec l'adresse IP imitée et pointe vers l'adresse IP du serveur externe. L'URL de connexion de l'authentification Web externe est ajoutée avec des paramètres tels que **AP_Mac_Address**,les **client_url** (adresse URL du client) et **action_URL** nécessaire pour contacter le serveur web du commutateur.

3. L'URL du serveur Web externe envoie l'utilisateur à une page de connexion. L'utilisateur peut utiliser une liste de contrôle d'accès (ACL) de pré-authentification pour accéder au serveur.

4. La page de connexion renvoie la demande d'informations d'identification de l'utilisateur au **action_URL**, tel que http://192.0.2.1/login.html, du serveur Web du WLC. Il s'agit d'un paramètre d'entrée pour l'URL de redirection, où 192.0.2.1 est l'adresse de l'interface virtuelle sur le commutateur.

5. Le serveur Web WLC envoie le nom d'utilisateur et le mot de passe pour l'authentification.

6. Le WLC lance la requête du serveur RADIUS ou utilise la base de données locale sur le WLC, puis authentifie l'utilisateur.

7. Si l'authentification réussit, le serveur Web du WLC transfère l'utilisateur à l'URL de redirection configurée ou à l'URL entrée par le client.

8. Si l'authentification échoue, le serveur Web du WLC redirige l'utilisateur vers l'URL de connexion de l'utilisateur.

   Remarque : nous utilisons 192.0.2.1 comme exemple d'adresse IP virtuelle dans ce document. La plage 192.0.2.x est recommandée pour l'utilisation de l'adresse IP virtuelle car elle n'est pas routable. L'ancienne documentation fait peut-être référence à "1.1.1.x" ou est toujours ce qui est configuré dans votre WLC comme ceci était le paramètre par défaut. Cependant, notez que cette adresse IP est désormais une adresse IP routable valide et que le sous-réseau 192.0.2.x est donc conseillé à la place.

Si les points d'accès sont en mode FlexConnect, un **preauth** La liste ACL est sans objet. Des listes de contrôle d'accès flexibles peuvent être utilisées pour autoriser l'accès au serveur Web pour les clients qui n'ont pas été authentifiés.

Reportez-vous à l'Exemple de configuration d'authentification Web externe avec des contrôleurs LAN sans fil.

Passthrough Web

Le Web Passthrough est une variante de l'authentification Web interne. Elle affiche une page avec un avertissement ou une instruction d'alerte, mais ne demande pas d'informations d'identification.

L'utilisateur clique ensuite sur **OK**. Activez la saisie des e-mails et l'utilisateur peut saisir son adresse e-mail qui devient son nom d'utilisateur.

Lorsque l'utilisateur est connecté, vérifiez votre liste de clients actifs et assurez-vous que l'utilisateur est répertorié avec l'adresse e-mail qu'il a entrée comme nom d'utilisateur.

Pour plus d'informations, référez-vous à Exemple de configuration de passerelle Web du contrôleur LAN sans fil 5760/3850.

Redirection Web conditionnelle

Si vous activez une redirection Web conditionnelle, l'utilisateur est redirigé de manière conditionnelle vers une page Web particulière une fois l'authentification 802.1x terminée.

Vous pouvez spécifier la page de redirection et les conditions sous lesquelles celle-ci se produit sur votre serveur RADIUS.

Les conditions peuvent inclure le mot de passe lorsqu'il atteint la date d'expiration ou lorsque l'utilisateur doit payer une facture pour une utilisation/un accès continu.

Si le serveur RADIUS renvoie la paire AV Cisco **url-redirect**, l'utilisateur est redirigé vers l'URL spécifiée lorsqu'il ouvre un navigateur.

Si le serveur renvoie également la paire AV Cisco **url-redirect-acl**, la liste de contrôle d'accès spécifiée est installée en tant que liste de contrôle d'accès de pré-authentification pour ce client.

Le client n'est pas considéré comme entièrement autorisé à ce stade et ne peut transmettre que le trafic autorisé par la liste de contrôle d'accès de pré-authentification. Une fois que le client a terminé une opération particulière à l'URL spécifiée (par exemple, un changement de mot de passe ou un paiement de facture), il doit s'authentifier à nouveau.

Lorsque le serveur RADIUS ne renvoie pas de **url-redirect**, le client est considéré comme entièrement autorisé et autorisé à transmettre le trafic.

> **Note**: La fonction de redirection Web conditionnelle est disponible uniquement pour les réseaux locaux sans fil configurés pour la sécurité de couche 2 802.1x ou WPA+WPA2.

Après la configuration du serveur RADIUS, configurez la redirection Web conditionnelle sur le contrôleur avec l'interface graphique utilisateur ou CLI du contrôleur. Reportez-vous à ces guides pas à pas : Configuration de la redirection Web (GUI) et configuration de la redirection Web (CLI).

Redirection Web de la page de démarrage

Si vous activez la redirection Web de la page d'accueil, l'utilisateur est redirigé vers une page Web particulière une fois l'authentification 802.1x terminée. Une fois la redirection effectuée, l'utilisateur dispose d'un accès complet au réseau.

Vous pouvez spécifier la page de redirection sur votre serveur RADIUS. Si le serveur RADIUS renvoie la paire AV Cisco **url-redirect**, l'utilisateur est redirigé vers l'URL spécifiée lorsqu'il ouvre un navigateur.

Le client est considéré comme entièrement autorisé à ce stade et est autorisé à transmettre le trafic, même si le serveur RADIUS ne renvoie pas de **url-redirect**.

> **Note**: La fonction de redirection de la page de démarrage est disponible uniquement pour les réseaux locaux sans fil configurés pour la sécurité de couche 2 802.1x ou WPA+WPA2.

Après la configuration du serveur RADIUS, configurez la redirection Web de la page de démarrage sur le contrôleur avec l'interface graphique utilisateur ou l'interface de ligne de commande du contrôleur.

Échec de WebAuth sur le filtre MAC

Un WebAuth sur MAC Filter FaFailure vous demande de configurer des filtres MAC dans le menu de sécurité de la couche 2.

Si les utilisateurs ont été validés avec leurs adresses MAC, ils accèdent directement à la **run** province.

Si ce n'est pas le cas, ils se rendent au **WEBAUTH_REQD** et l'authentification web normale se produit.

> **Note**: Cette fonctionnalité n'est pas prise en charge avec le passthrough Web.Pour plus d'informations, suivez l'exercice sur la demande d'amélioration ID de bogue Cisco CSCtw73512

Authentification Web centralisée

L'authentification Web centrale fait référence à un scénario dans lequel le WLC n'héberge plus aucun service. Le client est directement envoyé au portail Web ISE et ne passe pas par 192.0.2.1 sur le WLC. La page de connexion et l'ensemble du portail sont externalisés.

L'authentification Web centrale a lieu lorsque le contrôle d'accès au réseau (NAC) RADIUS est activé dans les paramètres avancés des filtres WLAN et MAC.

Le WLC envoie une authentification RADIUS (généralement pour le filtre MAC) à ISE, qui répond avec la **redirect-url** paire de valeurs d'attribut (AV).

L'utilisateur est alors mis en **POSTURE_REQD** jusqu'à ce qu'ISE donne l'autorisation avec une demande de modification d'autorisation (CoA). Le même scénario se produit dans Posture ou Central WebAuth.

WebAuth Central n'est pas compatible avec WPA-Enterprise/802.1x, car le portail invité ne peut pas renvoyer de clés de session pour le cryptage comme il le fait avec le protocole EAP (Extensible Authentication Protocol).

Authentification utilisateur externe (RADIUS)

L'authentification d'utilisateur externe (RADIUS) n'est valide pour l'authentification Web locale que lorsque le WLC gère les informations d'identification ou lorsqu'une stratégie Web de couche 3 est activée. Authentifier les utilisateurs localement ou sur le WLC ou en externe via RADIUS.

Il y a un ordre dans lequel le WLC vérifie les informations d'identification de l'utilisateur.

1. Dans tous les cas, il commence par chercher dans sa propre base de données.
2. S'il ne trouve pas les utilisateurs, il se dirige vers le serveur RADIUS configuré dans le WLAN invité (s'il y en a un configuré).
3. Il vérifie ensuite la liste globale des serveurs RADIUS par rapport aux serveurs RADIUS où **network user** est cochée.

Ce troisième point répond à la question de ceux qui ne configurent pas RADIUS pour ce WLAN, mais notez qu'il vérifie toujours par rapport au RADIUS quand l'utilisateur n'est pas trouvé sur le contrôleur.

C'est parce que **network user** est comparé à vos serveurs RADIUS dans la liste globale.

WLC peut authentifier les utilisateurs sur le serveur RADIUS avec le protocole d'authentification de mot de passe (PAP), le protocole d'authentification à échanges confirmés (CHAP) ou EAP-MD5 (Message Digest5).

Il s'agit d'un paramètre global qui peut être configuré à partir de l'interface utilisateur graphique ou CLI :

À partir de la GUI : accéder à **Controller > Web RADIUS Authentication**

À partir de CLI : saisissez **config custom-web RADIUSauth**

> **Remarque** : le serveur invité NAC utilise uniquement le protocole PAP.

Comment configurer un WLAN invité filaire

Une configuration WLAN invité filaire est similaire à une configuration invité sans fil. Il peut être configuré avec un ou deux contrôleurs (seulement si l'un est auto-anchor).

Choisissez un VLAN comme VLAN pour les utilisateurs invités câblés, par exemple, sur le VLAN 50. Lorsqu'un invité câblé veut accéder à Internet, branchez l'ordinateur portable sur un port d'un commutateur configuré pour le VLAN 50.

Ce VLAN 50 doit être autorisé et présent sur le chemin via le port trunk WLC.

Dans le cas de deux WLC (une ancre et une ancre étrangère), ce VLAN invité câblé doit conduire au WLC étranger (nommé WLC1) et non à l'ancre.

WLC1 prend alors en charge le tunnel de trafic vers le WLC DMZ (l'ancre, nommée WLC2), qui libère le trafic dans le réseau routé.

Voici les cinq étapes à suivre pour configurer l'accès invité filaire :

1. **Configurez une interface dynamique (VLAN) pour l'accès utilisateur invité câblé.**

   Sur le WLC1, créez une interface dynamique VLAN50. Dans le **interface configuration** , vérifiez la **Guest LAN** , sélectionnez une option. Ensuite, les champs tels que **IP address** et **gateway** disparaissent. Le WLC doit reconnaître que le trafic est routé à partir du VLAN 50. Ces clients sont des invités filaires.

2. **Créez un réseau local filaire pour l'accès utilisateur invité.**

   Sur un contrôleur, une interface est utilisée lorsqu'elle est associée à un WLAN. Créez ensuite un WLAN sur les contrôleurs de votre bureau central. Naviguez jusqu'à **WLANs** et cliquez sur **New**. Dans **WLAN Type**, choisissez **Guest LAN**.

   Dans **Profile Name** et **WLAN SSID**, entrez un nom qui identifie ce WLAN. Ces noms peuvent être différents, mais ne peuvent pas contenir d'espaces. Le terme WLAN est utilisé, mais ce

profil réseau n'est pas lié au profil réseau sans fil.

Les **General** propose deux listes déroulantes : **Ingress** et **Egress**. Ingress est le VLAN dont proviennent les utilisateurs (VLAN 50) ; La sortie est le VLAN auquel vous les envoyez.

Pour **Ingress**, choisissez **VLAN50**.

Pour **Egress**C'est différent. Si vous n'avez qu'un contrôleur, créez une autre interface dynamique, un **standard** cette fois (pas un réseau local invité) et envoyer des utilisateurs câblés à cette interface. Dans ce cas, envoyez-les au contrôleur DMZ. Par conséquent, pour le **Egress** , sélectionnez l'option **Management Interface**.

Les **Security** Le mode de ce réseau local sans fil invité est WebAuth, ce qui est acceptable. Cliquer **Ok** afin de valider.

3. Configurez le contrôleur étranger (bureau central).

A partir des versions **WLAN list**, cliquez sur **Mobility Anchor** à la fin du **Guest LAN** et choisissez votre contrôleur DMZ. On suppose ici que les deux contrôleurs se reconnaissent. Si ce n'est pas le cas, accédez à **Controller** > **Mobility Management** > **Mobility group**, et ajoutez DMZWLC sur WLC1. Ajoutez ensuite WLC1 sur DMZ. Les deux contrôleurs ne doivent pas être dans le même groupe de mobilité. Sinon, les règles de sécurité de base sont enfreintes.

4. Configurez le contrôleur d'ancrage (le contrôleur DMZ).

Le contrôleur du bureau central est prêt. Préparez maintenant votre contrôleur DMZ. Ouvrez une session de navigateur Web sur votre contrôleur DMZ et accédez aux WLAN. Créez un nouveau WLAN. Dans **WLAN Type**, choisissez **Guest LAN**.

Dans **Profile Name** et **WLAN SSID**, entrez un nom qui identifie ce WLAN. Utilisez les mêmes valeurs que celles entrées sur le contrôleur du bureau central.

Les **Ingress** l'interface est **None**. Peu importe, car le trafic est reçu via le tunnel Ethernet sur IP (EoIP). Il n'est pas nécessaire de spécifier une interface d'entrée.

Les **Egress** est l'emplacement où les clients doivent être envoyés. Par exemple, le **DMZ VLAN** est VLAN 9. Créez une interface dynamique standard pour VLAN 9 sur votre DMZWLC, puis choisissez **VLAN 9** comme interface de sortie.

Configurez la fin du tunnel d'ancrage de mobilité. Dans la liste WLAN, sélectionnez **Mobility Anchor for Guest LAN**. Envoyez le trafic au contrôleur local, DMZWLC. Les deux extrémités sont maintenant prêtes.

5. Ajustez le réseau local invité.

Vous pouvez également affiner les paramètres WLAN aux deux extrémités. Les paramètres doivent être identiques aux deux extrémités. Par exemple, si vous cliquez sur le bouton **WLAN Advanced** , sélectionnez **Allow AAA override** sur WLC1, cochez la même case sur DMZWLC. S'il

existe des différences dans le WLAN de chaque côté, le tunnel se brise. DMZWLC refuse le trafic ; vous pouvez voir quand vous **run debug mobility**.

Gardez à l'esprit que toutes les valeurs sont réellement obtenues à partir de DMZWLC : Adresses IP, valeurs VLAN, etc. Configurez le côté WLC1 de manière identique, de sorte qu'il relaie la requête au WLCDMZ.

Certificats pour la page de connexion

Cette section fournit les processus permettant de placer votre propre certificat sur la page WebAuth ou de masquer l'URL WebAuth 192.0.2.1 et d'afficher une URL nommée.

Télécharger un certificat pour l'authentification Web du contrôleur

Via l'interface utilisateur graphique (**WebAuth** > **Certificate**) ou CLI (type de transfert **webauthcert**) vous pouvez télécharger un certificat sur le contrôleur.

Qu'il s'agisse d'un certificat créé avec votre autorité de certification (CA) ou d'un certificat officiel tiers, il doit être au format .pem.

Avant d'envoyer, vous devez également saisir la clé du certificat.

Après le téléchargement, un redémarrage est nécessaire pour que le certificat soit en place. Une fois redémarré, accédez à la page de certificat WebAuth dans l'interface utilisateur graphique pour trouver les détails du certificat que vous avez téléchargé (validité, etc.).

Le champ important est le nom commun (CN), qui est le nom attribué au certificat. Ce champ est traité dans ce document sous la section "Autorité de certification et autres certificats sur le contrôleur".

Après avoir redémarré et vérifié les détails du certificat, le nouveau certificat de contrôleur s'affiche sur la page de connexion WebAuth. Cependant, il peut y avoir deux situations.

1. Si votre certificat a été émis par l'une des rares autorités de certification racine principales auxquelles chaque ordinateur fait confiance, cela ne pose aucun problème. VeriSign en est un exemple, mais vous êtes généralement signé par une sous-autorité de certification Verisign et non par l'autorité de certification racine. Vous pouvez vérifier dans le magasin de certificats de votre navigateur si vous voyez l'autorité de certification mentionnée ici comme approuvée.

2. Si vous avez obtenu votre certificat d'une plus petite société/autorité de certification, tous les ordinateurs ne leur font pas confiance. Fournissez également le certificat de la société/l'autorité de certification au client, et l'une des autorités de certification racine émet ensuite ce certificat. Finalement, vous avez une chaîne telle que "Le certificat a été émis par CA x > Le certificat CA x a été émis par CA y > Le certificat CA y a été émis par cette CA racine de confiance". L'objectif final est d'atteindre une autorité de certification à laquelle le client fait confiance.

Autorité de certification et autres certificats sur le contrôleur

Afin de se débarrasser de l'avertissement « ce certificat n'est pas approuvé », entrez le certificat de l'AC qui a émis le certificat du contrôleur sur le contrôleur.

Le contrôleur présente ensuite les deux certificats (le certificat du contrôleur et son certificat CA). Le certificat d'autorité de certification doit être une autorité de certification approuvée ou disposer des ressources nécessaires pour vérifier l'autorité de certification. Vous pouvez en fait créer une chaîne de certificats d'autorité de certification qui mène à une autorité de certification approuvée au-dessus.

Placez la chaîne entière dans le même fichier. Le fichier contient alors un contenu tel que cet exemple :

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

Comment faire correspondre le certificat à l'URL

L'URL WebAuth est définie sur 192.0.2.1 afin de vous authentifier et le certificat est émis (il s'agit du champ CN du certificat WLC).

Pour modifier l'URL WebAuth en « myWLC.com », par exemple, accédez à la page **virtual interface configuration** (l'interface 192.0.2.1) et vous pouvez y entrer un **virtual DNS hostname**, par exemple myWLC.com.

Cette commande remplace l'adresse 192.0.2.1 dans votre barre d'URL. Ce nom doit également pouvoir être résolu. La trace du renifleur montre comment tout cela fonctionne, mais quand WLC envoie la page de connexion, WLC affiche l'adresse myWLC.com, et le client résout ce nom avec son DNS.

Ce nom doit être résolu comme 192.0.2.1. Cela signifie que si vous utilisez également un nom pour la gestion du WLC, utilisez un nom différent pour WebAuth.

Si vous utilisez myWLC.com mappé à l'adresse IP de gestion du WLC, vous devez utiliser un nom différent pour WebAuth, tel que myWLCwebauth.com.

Résoudre les problèmes de certificat

Cette section explique comment et quoi vérifier pour résoudre les problèmes de certificat.

Comment vérifier

Téléchargez OpenSSL (pour Windows, recherchez OpenSSL Win32) et installez-le. Sans configuration, vous pouvez accéder au répertoire bin et essayer **openssl s_client –connect (your web auth URL):443**,

si cette URL est l'URL à laquelle votre page WebAuth est liée sur votre DNS, reportez-vous à la section « Éléments à vérifier » dans la section suivante de ce document.

Si vos certificats utilisent une autorité de certification privée, placez le certificat de l'autorité de certification racine dans un répertoire sur un ordinateur local et utilisez l'option openssl **-CApath**. Si vous avez une autorité de certification intermédiaire, placez-la également dans le même

répertoire.

Pour obtenir des informations générales sur le certificat et le vérifier, utilisez :

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

Il est également utile de convertir les certificats avec l'utilisation d'openssl :

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Éléments à vérifier

Vous pouvez voir quels certificats sont envoyés au client lorsqu'il se connecte. Lire le certificat du périphérique : le CN doit être l'URL où la page Web est accessible.

Lisez la ligne « émis par » du certificat du périphérique. Il doit correspondre au CN du deuxième certificat. Ce deuxième certificat, « émis par », doit correspondre au CN du certificat suivant, et ainsi de suite. Sinon, il ne fait pas une véritable chaîne.

Dans le résultat OpenSSL affiché ici, notez que **openssl** ne peut pas vérifier le certificat du périphérique, car son « émis par » ne correspond pas au nom du certificat CA fourni.

Sortie SSL

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
```

```
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

Un autre problème possible est que le certificat ne peut pas être téléchargé sur le contrôleur. Dans cette situation, il n'est pas question de validité, de CA, etc.

Pour vérifier cela, vérifiez la connectivité TFTP (Trivial File Transfer Protocol) et essayez de transférer un fichier de configuration. Si vous saisissez la commande **debug transfer all enable** , notez que le problème est l'installation du certificat.

Cela peut être dû à une clé incorrecte utilisée avec le certificat. Il se peut également que le certificat soit dans un format incorrect ou endommagé.

Cisco vous recommande de comparer le contenu du certificat à un certificat valide connu. Cela vous permet de voir si un **LocalkeyID** affiche tous les 0 (déjà arrivé). Si tel est le cas, le certificat doit être reconverti.

Il existe deux commandes avec OpenSSL qui vous permettent de retourner de .pem à .p12, puis de réémettre un .pem avec la clé de votre choix.

Si vous avez reçu un fichier .pem contenant un certificat suivi d'une clé, copiez/collez la partie clé : **----BEGIN KEY ---- until ------- END KEY ------** du .pem dans "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? Vous êtes invité à saisir une clé ; saisissez **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** Il en résulte un .pem opérationnel avec le mot de passe **check123**.

Autres situations à dépanner

Bien que l'**ancre de mobilité n'**ait pas été abordée dans ce document, si vous êtes dans une situation d'**invité ancré**, assurez-vous que l'échange de mobilité se produit correctement et que vous voyez le client arriver sur l'ancre.

Tout autre problème WebAuth doit être résolu sur l'ancre.

Voici quelques problèmes courants que vous pouvez résoudre :

- **Les utilisateurs ne peuvent pas s'associer au WLAN invité**.

  Ceci n'est pas lié à WebAuth. Vérifiez la configuration du client, les paramètres de sécurité sur le WLAN, s'il est activé, et si les radios sont actives et opérationnelles, etc.

- **Les utilisateurs n'obtiennent pas d'adresse IP**.

Dans une situation d'ancrage invité, c'est le plus souvent parce que l'ancrage étranger et l'ancrage n'ont pas été configurés exactement de la même manière. Sinon, vérifiez la configuration DHCP, la connectivité, etc.

- Vérifiez si d'autres WLAN peuvent utiliser le même serveur DHCP sans problème. Ce n'est toujours pas lié à WebAuth.

- **L'utilisateur n'est pas redirigé vers la page de connexion**.

  C'est le symptôme le plus courant, mais il est plus précis. Deux scénarios sont possibles .

  L'utilisateur n'est pas redirigé (l'utilisateur entre une URL et n'atteint jamais la page WebAuth). Pour cette situation, vérifiez :

  qu'un serveur DNS valide a été attribué au client via DHCP (**ipconfig /all**,

  que le DNS est accessible à partir du client (**nslookup (website URL**,

  que l'utilisateur a saisi une URL valide pour être redirigé,

  que l'utilisateur est allé sur une URL HTTP sur le port 80 (par exemple, pour atteindre un ACS avec http://localhost:2002 ne vous redirige pas puisque vous avez envoyé sur le port 2002 au lieu de 80).

  L'utilisateur est redirigé vers 192.0.2.1 correctement, mais la page elle-même ne s'affiche pas.

  Cette situation est très probablement un problème de WLC (bogue) ou un problème côté client. Il se peut que le client dispose d'un pare-feu, d'un logiciel ou d'un bloc de stratégie. Il se peut également qu'ils aient configuré un proxy dans leur navigateur Web.

  Recommandation : Effectuez une analyse par renifleur sur le PC client. Il n'y a pas besoin d'un logiciel sans fil spécial, seulement Wireshark, qui fonctionne sur la carte sans fil et vous montre si le WLC répond et essaie de rediriger. Vous avez deux possibilités : soit il n'y a pas de réponse du WLC, soit quelque chose ne va pas avec la connexion SSL pour la page WebAuth. Pour le problème de connexion SSL, vous pouvez vérifier si le navigateur de l'utilisateur autorise SSLv3 (certains n'autorisent que SSLv2) et s'il est trop agressif lors de la vérification du certificat.

  Il est courant d'entrer manuellement http://192.0.2.1 afin de vérifier si la page Web apparaît sans DNS. En fait, vous pouvez taper http://10.0.0.0 et obtenir le même effet. Le WLC redirige toute adresse IP que vous entrez. Par conséquent, si vous entrez http://192.0.2.1, cela ne vous oblige pas à contourner la redirection Web. Si vous entrez https://192.0.2.1(secure), cela ne fonctionne pas parce que WLC ne redirige pas le trafic HTTPS (par défaut, ceci est effectivement possible dans la version 8.0 et ultérieure). La meilleure façon de charger la page directement sans redirection est d'entrer https://192.0.2.1/login.html.

- **Les utilisateurs ne peuvent pas authentifier**.

  Reportez-vous à la section de ce document qui traite de l'authentification. Vérifiez les

informations d'identification localement sur RADIUS.

- **Les utilisateurs peuvent s'authentifier avec succès via WebAuth, mais ils n'ont pas accès à Internet par la suite**.

  Vous pouvez supprimer WebAuth de la sécurité du WLAN, puis vous avez un WLAN ouvert. Vous pouvez ensuite essayer d'accéder au Web, au DNS, etc. Si vous rencontrez également des problèmes, supprimez complètement les paramètres WebAuth et vérifiez la configuration de vos interfaces.

Pour plus d'informations à ce sujet, consultez : Dépannage de l'authentification Web sur un contrôleur LAN sans fil (WLC).

Serveur proxy HTTP et son fonctionnement

Vous pouvez utiliser un serveur proxy HTTP. Si vous avez besoin que le client ajoute une exception dans son navigateur que 192.0.2.1 ne doit pas passer par le serveur proxy, vous pouvez faire que le WLC écoute le trafic HTTP sur le port du serveur proxy (habituellement 8080).

Afin de comprendre ce scénario, vous devez savoir ce qu'un proxy HTTP fait. Il s'agit d'un élément que vous configurez côté client (adresse IP et port) dans le navigateur.

Le scénario habituel lorsqu'un utilisateur visite un site Web consiste à convertir le nom en IP avec DNS, puis il demande la page Web au serveur Web. Le processus envoie toujours la requête HTTP pour la page au proxy.

Le proxy traite le DNS, si nécessaire, et le transfère au serveur Web (si la page n'est pas déjà mise en cache sur le proxy). La discussion est client-à-proxy uniquement. Le fait que le proxy obtienne ou non la page Web réelle n'est pas pertinent pour le client.

Voici le processus d'authentification Web :

- L'utilisateur saisit une URL.
- Le PC client envoie au serveur proxy.
- WLC intercepte et imite l'IP du serveur proxy ; il répond au PC avec une redirection vers 192.0.2.1

Àce stade, si le PC n'est pas configuré pour cela, il demande la page 192.0.2.1 WebAuth au proxy afin qu'elle ne fonctionne pas. Le PC doit faire une exception pour 192.0.2.1 ; puis il envoie une requête HTTP à 192.0.2.1 et continue avec WebAuth.

Une fois authentifiées, toutes les communications passent à nouveau par le proxy. Une configuration d'exception se trouve généralement dans le navigateur à proximité de la configuration du serveur proxy. Le message suivant s'affiche : "N'utilisez pas de proxy pour ces adresses IP".

Avec WLC version 7.0 et ultérieure, la fonctionnalité **webauth proxy redirect** peut être activé dans les options de configuration globale du WLC.

Lorsqu'il est activé, le WLC vérifie si les clients sont configurés pour utiliser manuellement un proxy. Dans ce cas, ils redirigent le client vers une page qui leur montre comment modifier leurs

paramètres de proxy pour que tout fonctionne.

La redirection proxy WebAuth peut être configurée pour fonctionner sur divers ports et est compatible avec l'authentification Web centrale.

Pour un exemple sur la redirection du proxy WebAuth, référez-vous à Exemple de configuration du proxy d'authentification Web sur un contrôleur LAN sans fil.

Authentification Web sur HTTP au lieu de HTTPS

Vous pouvez vous connecter à l'authentification Web sur HTTP au lieu de HTTPS. Si vous vous connectez sur HTTP, vous ne recevez pas d'alertes de certificat.

Pour le code antérieur à la version 7.2 du WLC, vous devez désactiver la gestion HTTPS du WLC et laisser la gestion HTTP. Cependant, cela permet seulement la gestion Web du WLC sur HTTP.

Pour le code WLC version 7.2, utilisez la **config network web-auth secureweb disable** pour désactiver. Cela désactive uniquement HTTPS pour l'authentification Web et non pour la gestion. Notez que cela nécessite un redémarrage du contrôleur !

Sur le code WLC version 7.3 et ultérieure, vous pouvez activer/désactiver HTTPS pour WebAuth uniquement via l'interface graphique et l'interface de ligne de commande.

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Télécharger le logiciel pour les ensembles WebAuth de contrôleur sans fil
- Création d'une page de connexion d'authentification Web personnalisée
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Exemple de configuration de la passerelle Web du contrôleur LAN sans fil 5760/3850
- Configuration de la redirection Web (GUI)
- Configuration de la redirection Web (CLI)
- Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration du proxy d'authentification Web sur un contrôleur LAN sans fil
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems

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.