Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document explique comment employer un serveur Web externe afin d'installer un contrôleur de réseau local sans fil (WLC) pour l'authentification Web.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance de base de la configuration du Point d'accès léger (recouvrements) et des Cisco WLC

- Connaissance de base de point d'accès léger Protocol (LWAPP) et contrôle et ravitaillement des points d'accès sans fil (CAPWAP)
- La connaissance sur la façon dont installer et configurer un web server externe
- La connaissance sur la façon dont installer et configurer le DHCP et les serveurs DNS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco 4400 WLC qui exécute la version de microprogramme 7.0.116.0
- RECOUVREMENT de gamme de Cisco 1131AG
- Adaptateur client sans fil de Cisco 802.11a/b/g qui exécute la version de microprogramme 3.6
- Web server externe qui héberge la page de connexion d'authentification Web
- DN et serveurs DHCP pour l'address resolution et l'allocation d'adresse IP aux clients sans fil

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

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 DHCP et de DN) d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur valide et un mot de passe. L'authentification Web est une méthode d'authentification simple sans besoin de suppliant ou d'utilitaire client.

L'authentification Web peut être exécutée utilisant :

- Fenêtre de connexion par défaut sur le WLC
- Version modifiée de la fenêtre de connexion par défaut sur le WLC
- Une fenêtre de connexion personnalisée que vous configurez sur un web server externe (l'authentification de Web externe)
- Une fenêtre de connexion personnalisée que vous téléchargez au contrôleur

Ce document fournit un exemple de configuration pour expliquer comment configurer le WLC pour utiliser un script de connexion d'un web server externe.

Procédure d'authentification de Web externe

Avec l'authentification de Web externe, la page de connexion utilisée pour l'authentification Web est enregistrée sur un web server externe. C'est la séquence d'opérations quand les essais d'un client sans fil pour accéder à un réseau WLAN qui a l'authentification de Web externe ont activé :

1. Le client (utilisateur final) se connecte au WLAN et ouvre un navigateur Web et écrit un URL, tel que www.cisco.com.
2. Le client envoie une demande de DN à un serveur DNS afin de résoudre www.cisco.com à l'adresse IP.
3. Le WLC en avant la demande au serveur DNS qui, consécutivement, résout www.cisco.com à l'adresse IP et envoie une réponse de DN. Le contrôleur en avant la réponse au client.
4. Essais de client pour initier une connexion TCP avec l'adresse IP de www.cisco.com en envoyant le paquet de synchronisation de TCP à l'adresse IP de www.cisco.com.
5. Le WLC a des règles configurées pour le client et par conséquent peut agir en tant que proxy pour www.cisco.com. Il renvoie un paquet du TCP SYN-ACK au client avec la source comme adresse IP de www.cisco.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.
6. Le client envoie un HTTP OBTIENNENT le paquet destiné à www.google.com. Le WLC intercepte ce paquet, l'envoie pour la manipulation de redirection. La passerelle d'application de HTTP prépare un corps HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client à aller à l'URL par défaut de page Web du WLC, par exemple, http:// <Virtual-Server-IP>/login.html.
7. Le client commence alors la connexion HTTPS à l'URL de réorientation qui l'envoie à 1.1.1.1. C'est l'adresse IP virtuelle du contrôleur. Le client doit valider le certificat de serveur ou l'ignorer afin d'apporter le tunnel SSL.
8. Puisque l'authentification de Web externe est activée, le WLC réoriente le client au web server externe.
9. L'URL authentique de procédure de connexion de Web externe est ajouté avec des paramètres tels que l'AP_Mac_Address, le client_url (www.cisco.com) et l'action_URL du lequel le client a besoin pour entrer en contact avec le web server de contrôleur.**Note**: L'action_URL indique au web server que le nom d'utilisateur et mot de passe est enregistré sur le contrôleur. Les qualifications doivent être renvoyées au contrôleur afin d'obtenir authentifié.
10. L'URL externe de web server mène l'utilisateur à une page de connexion.
11. La page de connexion prend l'entrée d'identifiants utilisateurs, et envoie la demande de nouveau à l'action_URL, exemple http://1.1.1.1/login.html, du web server WLC.
12. Le web server WLC soumet le nom d'utilisateur et mot de passe pour l'authentification.
13. Le WLC initie la demande de serveur de RAYON ou utilise la base de données locale sur le WLC et authentifie l'utilisateur.
14. Si l'authentification est réussie, le web server WLC l'un ou l'autre en avant l'utilisateur au configuré réorientent l'URL ou à l'URL le client a commencé par, comme www.cisco.com.
15. Si l'authentification échoue, alors le web server WLC réoriente l'utilisateur de nouveau à l'URL de procédure de connexion de client.

Note: Afin de configurer le webauthentication externe pour utiliser des ports autres que le HTTP et le HTTPS, émettez cette commande :

```
(Cisco Controller) >config network web-auth-port

<port>         Configures an additional port to be redirected for web authentication.
```

Configuration du réseau

L'exemple de configuration utilise cette installation. UN RECOUVREMENT est enregistré au WLC.

Vous devez configurer un **invité** WLAN pour les utilisateurs d'invité et devez activer l'authentification Web pour les utilisateurs. Vous devez également s'assurer que le contrôleur réoriente l'utilisateur à l'URL externe de web server (pour l'authentification de Web externe). Le web server externe héberge la page de connexion de Web qui est utilisée pour l'authentification.

Les identifiants utilisateurs doivent être validés contre la base de données locale mise à jour sur le contrôleur. Après l'authentification réussie, on devrait permettre aux utilisateurs l'accès à l'invité WLAN. Le contrôleur et d'autres périphériques doivent être configurés pour cette installation.

Note: Vous pouvez utiliser une version personnalisée du script de connexion, qui sera utilisé pour l'authentification Web. Vous pouvez télécharger un script d'authentification Web d'échantillon de la page de téléchargements logiciels de Cisco. Par exemple, pour les 4400 contrôleurs, naviguez vers les **Produits > la radio > contrôleur LAN Sans fil > Contrôleurs autonomes > Contrôleurs de réseau local sans fil de la gamme Cisco 4400 > contrôleur LAN sans fil Cisco 4404 > logiciel sur le châssis > l'authentification Web Sans fil Bundle-1.0.1 de contrôleur réseau local** et téléchargez le **fichier webauth_bundle.zip**.

Note: Le paquet authentique personnalisé de 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.

Note: Ce document suppose que le DHCP, les DN et les web server externes sont configurés. Référez-vous à la documentation appropriée de tiers pour les informations sur la façon dont configurer le DHCP, les DN et le web server externe.

Configurez

Avant que vous configuriez le WLC pour l'authentification de Web externe, vous devez configurer le WLC pour le fonctionnement de base et enregistrer les recouvrements au WLC. Ce document suppose que WLC est configuré pour les opérations de base et que les LAP sont enregistrés au WLC. Référez-vous à l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC) si vous êtes un nouvel utilisateur essayant d'installer le WLC pour le fonctionnement de base avec des recouvrements.

Terminez-vous ces étapes afin de configurer les recouvrements et le WLC pour cette installation :

1. Créez une interface dynamique pour les utilisateurs d'invité
2. Créez un ACL de Préauthentification
3. Créez une base de données locale sur le WLC pour les utilisateurs d'invité
4. Configurez le WLC pour l'authentification de Web externe
5. Configurez le WLAN pour des utilisateurs d'invité

Créez une interface dynamique pour les utilisateurs d'invité

Terminez-vous ces étapes afin de créer une interface dynamique pour les utilisateurs d'invité :

1. Du GUI WLC, choisissez les **contrôleurs > les interfaces**.La fenêtre Interfaces apparaît. Cette fenêtre liste les interfaces qui sont configurées sur le contrôleur. Ceci inclut les interfaces par défaut, qui sont l'interface de gestion, interface d'AP-gestionnaire, l'interface virtuelle et l'interface de port de service, et les interfaces dynamiques définies par l'utilisateur.
2. Afin de créer une nouvelle interface dynamique, cliquez sur **New**.

3. Dans les **interfaces > la nouvelle** fenêtre, écrivent le nom d'interface et l'ID de VLAN. Cliquez ensuite sur **Apply**.Dans cet exemple, l'interface dynamique est nommée **invité** et l'ID de VLAN est assigné **10.**
4. Dans la fenêtre d'**Interfaces > Edit**, pour l'interface dynamique, entrez dans l'adresse IP, le masque de sous-réseau, et la passerelle par défaut. Attribuez-la à un port physique sur le WLC et entrez l'adresse IP sur le serveur DHCP. Cliquez ensuite sur **Apply**.

Créez un ACL de Préauthentification

En utilisant un web server externe pour l'authentification Web, certaines des Plateformes WLC ont besoin d'un ACL de pré-authentification pour le web server externe (le contrôleur de gamme Cisco 5500, une gamme Cisco 2100 contrôleur, la gamme Cisco 2000 et le module réseau de contrôleur). Pour les autres Plateformes WLC l'ACL de pré-authentification n'est pas obligatoire.

Cependant, l'il est conseillé de configurent un ACL de Préauthentification pour le web server externe en utilisant l'authentification de Web externe.

Terminez-vous ces étapes afin de configurer l'ACL de Préauthentification pour le WLAN :

1. Du GUI WLC, choisissez la **Sécurité > les listes de contrôle d'accès**.Cette fenêtre te permet pour visualiser ACLs en cours qui sont semblable au Pare-feu standard ACLs.
2. Cliquez sur New afin de créer un nouvel ACL.
3. Écrivez le nom de l'ACL et cliquez sur Apply.Dans cet exemple, l'ACL est nommé Pré-Auth-pour-Externe-Web-**Serveur**.
4. Pour le nouvel ACL créé, cliquez sur Edit.L'ACL > éditent la fenêtre apparaît. Cette fenêtre permet l'utilisateur de définir de nouvelles règles ou de modifier les règles de l'ACL qui existent.
5. Cliquez sur Add la **nouvelle règle**.
6. Définissez une règle d'ACL qui permet l'accès pour les clients au web server externe.Dans cet exemple, 172.16.1.92 est l'adresse IP externe de web server.
7. Cliquez sur Apply afin de commettre les modifications.

Créez une base de données locale sur le WLC pour les utilisateurs d'invité

La base de données utilisateur pour les utilisateurs d'invité peut être enregistrée sur la base de données locale Sans fil du contrôleur LAN, ou pourrait être externe enregistré du contrôleur.

Dans ce document la base de données locale sur le contrôleur est utilisée pour authentifier des utilisateurs. Vous devez créer un utilisateur du réseau local et définir un mot de passe pour la connexion de client d'authentification Web. Terminez-vous ces étapes afin de créer la base de données utilisateur sur le WLC :

1. Du GUI WLC, choisissez la **Sécurité**.
2. Cliquez sur les **utilisateurs du réseau locaux du** menu d'AAA du côté gauche.
3. Cliquez sur New afin de créer un nouvel utilisateur.D'une nouvelle affichages fenêtre qui demande les informations de nom d'utilisateur et mot de passe.
4. Entrez un nom d'utilisateur et un mot de passe afin de créer un nouvel utilisateur, puis confirmez le mot de passe que vous voulez utiliser.Cet exemple crée l'utilisateur nommé **User1**.

5. Ajoutez une description, le cas échéant.Cet exemple utilise l'**invité User1**.
6. Cliquez sur **Apply** pour sauvegarder la nouvelle configuration utilisateur.
7. Répétez les étapes 3-6 pour ajouter plus d'utilisateurs à la base de données.

Configurez le WLC pour l'authentification de Web externe

L'étape suivante est de configurer le WLC pour l'authentification de Web externe. Procédez comme suit :

1. Du GUI de contrôleur, choisissez la **Sécurité > le Web authentiques > page Web Login** afin d'accéder à la page Web Login.
2. De la liste déroulante de type d'authentification Web, choisissez **externe (serveur externe de redirect to)**.
3. Dans la section **externe de serveur Web**, ajoutez le nouveau web server externe.
4. Dans l'**URL de réorientation après que le** champ de **procédure de connexion**, écrivent l'URL de la page à laquelle l'utilisateur final sera réorienté à sur l'authentification réussie. Dans le **champ URL authentique de Web externe**, écrivez l'URL où la page de connexion est enregistrée sur le web server externe.**Note**: Dans des versions 5.0 et ultérieures WLC, la page de déconnexion pour l'authentification Web peut également être personnalisée. Référez-vous à la panne de procédure de connexion, de procédure de connexion d'assigner et aux pages de déconnexion par section WLAN de la *configuration Sans fil Guide,5.2 de contrôleur LAN* pour plus d'informations sur la façon la configurer.

Configurez le WLAN pour des utilisateurs d'invité

La dernière étape est de créer des WLAN pour les utilisateurs d'invité. Procédez comme suit :

1. Cliquez sur **WLANs** depuis l'interface utilisateur graphique (GUI) du contrôleur afin de créer un WLAN.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le contrôleur.
2. Cliquez sur **New** pour configurer un nouveau WLAN.Dans cet exemple, le WLAN est nommé **Guest** et l'ID de WLAN est **1.**
3. Cliquez sur **Apply**.
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Pour le WLAN invité, dans l'onglet Général, choisissez l'interface appropriée du champ Interface Name.Cet exemple trace l'**invité d'**interface dynamique qui a été précédemment créé à l'invité WLAN.Allez à l'onglet Sécurité. Sous le degré de sécurité de la couche 2, **aucun** n'est sélectionné dans cet exemple.**Note**: L'authentification Web n'est pas prise en charge avec l'authentification de 802.1x. Ceci signifie que vous ne pouvez pas choisir le 802.1x ou un WPA/WPA2 avec le 802.1x comme degré de sécurité de la couche 2 quand vous utilisez l'authentification Web. L'authentification Web est prise en charge avec tous autres paramètres de degré de sécurité de la couche 2.Dans le domaine de degré de sécurité de la couche 3, cochez la case de **stratégie de Web** et choisissez l'option d'**authentification**.Cette option est choisie parce que l'authentification Web est utilisée pour authentifier les clients Sans fil d'invité.Choisissez l'ACL approprié de Préauthentification du menu déroulant.Dans cet exemple, l'ACL de Préauthentification qui a été créé précédemment est utilisé.Cliquez sur **Apply**.

Vérifiez

Le client sans fil monte et l'utilisateur écrit l'URL, tel que www.cisco.com, dans le navigateur Web. Puisque l'utilisateur n'a pas été authentifié, le WLC réoriente l'utilisateur à l'URL de procédure de connexion de Web externe.

L'utilisateur est incité pour les identifiants utilisateurs. Une fois que l'utilisateur soumet le nom d'utilisateur et mot de passe, la page de connexion prend l'entrée d'identifiants utilisateurs et soumet en fonction envoie la demande de nouveau à l'exemple d'action_URL, http://1.1.1.1/login.html, du web server WLC. Ceci est fourni pendant qu'un paramètre d'entrée au client réorientent l'URL, où 1.1.1.1 est l'adresse d'interface virtuelle sur le commutateur.

Le WLC authentifie l'utilisateur contre la base de données locale configurée sur le WLC. Après l'authentification réussie, le web server WLC l'un ou l'autre en avant l'utilisateur au configuré réorientent l'URL ou à l'URL le client a commencé par, comme www.cisco.com.

Dépannez

Employez ces commandes de débogage afin de dépanner votre configuration.

- debug mac addr <adresse-MAC-client xx: xx : xx : xx : xx : xx>
- **debug aaa all enable**
- enable d'état de debug pem
- debug pem events enable
- enable de message de debug dhcp
- enable de paquet de debug dhcp
- enable de ssh-appgw de debug pm
- enable de ssh-TCP de debug pm

Utilisez cette section pour dépanner votre configuration.

Les clients réorientés au serveur d'authentification de Web externe reçoivent un avertissement de certificat

Problème : Quand des clients sont réorientés au serveur d'authentification du Web externe de Cisco, ils reçoivent un avertissement de certificat. Il y a un certificat valide sur le serveur, et si vous vous connectez au serveur d'authentification de Web externe directement l'avertissement de certificat n'est pas reçu. Est-ce que c'est parce que l'adresse IP virtuelle (1.1.1.1) du WLC est présentée au client au lieu de l'adresse IP réelle du serveur d'authentification de Web externe qui est associé avec le certificat ?

Solution : Oui. Si vous exécutez l'authentification de gens du pays ou de Web externe, vous frappez toujours le web server interne sur le contrôleur. Quand vous redirect to un web server externe, vous recevez toujours l'avertissement de certificat du contrôleur à moins que vous ayez un certificat valide sur le contrôleur lui-même. Si la réorientation est envoyée aux https, vous recevez l'avertissement de certificat du contrôleur et du web server externe, à moins que chacun des deux aient un certificat valide.

Afin de se débarasser tous de certificat des avertissements ensemble, vous devez avoir un certificat de niveau de racine délivré et téléchargé sur votre contrôleur. Le certificat est délivré

pour un nom d'hôte et vous mettez que nom d'hôte dans la case de nom d'hôte de DN sous l'interface virtuelle sur le contrôleur. Vous devez également ajouter le nom d'hôte à votre serveur DNS local et l'indiquer l'adresse IP virtuelle (1.1.1.1) du WLC.

Référez-vous à la génération de la demande de signature de certificat (CSR) pour un tiers certificat sur un pour en savoir plus du contrôleur WLAN (WLC).

Erreur : la « page ne peut pas être affichée »

Problème : Après que le contrôleur soit mis à jour à 4.2.61.0, la « page ne peut pas être » message d'erreur affiché apparaît quand vous utilisez une page Web téléchargée pour l'authentification Web. Ceci fonctionné bien avant la mise à jour. La page Web interne par défaut charge sans problème.

Solution : De la version 4.2 et ultérieures WLC une nouvelle caractéristique est introduite où vous pouvez avoir le multiple les pages de connexion cutomized pour l'authentification Web.

Afin d'avoir le chargement de page Web correctement, il n'est pas suffisant de placer le type d'authentification Web comme **personnalisé** globalement dans la **Sécurité > le Web authentiques > page de connexion de Web**. Il doit également être configuré sur un WLAN particulier. Pour ce faire, suivez ces étapes :

1. Connectez-vous dans le GUI du WLC.
2. Cliquez sur en fonction l'onglet **WLAN**, et accédez au profil du WLAN configuré pour l'authentification Web.
3. Àla page de WLAN > Edit, cliquez sur l'**onglet Sécurité**. Puis, choisissez la **couche 3.**
4. Àcette page, n'en choisissez **aucun** comme degré de sécurité de la couche 3.
5. Cochez la case de **stratégie de Web**, et choisissez l'option d'**authentification**.
6. Cochez la case d'**enable de** configuration globale de priorité, choisissez **personnalisé (téléchargé)** comme type authentique de Web, et sélectionnez la page de connexion désirée du menu de **Pagepull de procédure de connexion** vers le bas. Cliquez sur **Apply**.

Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Vidéo : Authentification Web sur les contrôleurs LAN Sans fil de Cisco (WLCs)
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Support et documentation techniques - Cisco Systems