Authentification de Web externe utilisant un serveur de RAYON

Contenu

Introduction

Ce document explique comment effectuer l'authentification Web externe au moyen un serveur RADIUS externe.

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
- La connaissance de la façon installer et configurer un web server externe
- La connaissance de la façon configurer le Cisco Secure ACS

Composants utilisés

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

- Contrôleur LAN Sans fil qui exécute la version 5.0.148.0 de micrologiciels
- RECOUVREMENT de gamme Cisco 1232
- Adaptateur client sans fil 3.6.0.61 de Cisco 802.11a/b/g
- Web server externe qui héberge la page de connexion d'authentification Web
- Version de Cisco Secure ACS qui exécute la version 4.1.1.24 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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ce sont les adresses IP utilisées dans ce document :

- WLC utilise l'adresse IP 10.77.244.206
- Le RECOUVREMENT est enregistré à WLC avec l'adresse IP 10.77.244.199
- Le serveur Web utilise l'adresse IP 10.77.244.210
- Le serveur ACS de Cisco utilise l'adresse IP 10.77.244.196
- Le client reçoit une adresse IP de l'interface de gestion qui est tracée au WLAN - 10.77.244.208

Conventions

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

Authentification de Web externe

L'authentification Web est un mécanisme d'authentification de la couche 3 utilisé pour authentifier des utilisateurs d'invité pour l'accès d'Internet. Les utilisateurs authentifiés utilisant ce processus ne pourront pas accéder à l'Internet jusqu'à ce qu'ils complètent avec succès la procédure d'authentification. Pour des informations complètes sur la procédure d'authentification de Web externe, lisez la procédure d'authentification de Web externe de section de l'authentification de Web externe de document avec l'exemple Sans fil de configuration de contrôleurs LAN.

Dans ce document, nous regardons un exemple de configuration, dans lequel l'authentification de Web externe est exécutée utilisant un serveur RADIUS externe.

Configurez le WLC

Dans ce document, nous supposons que le WLC est déjà configuré et a un RECOUVREMENT enregistré au WLC. Ce document autre suppose que le WLC est configuré pour le fonctionnement de base et que les recouvrements sont enregistrés au WLC. Si vous êtes un nouvel utilisateur qui essaie d'installer le WLC pour l'opération de base avec les LAP, consultez l'Enregistrement léger AP (LAP) sur un contrôleur LAN sans fil (WLC). Pour visualiser les recouvrements qui sont enregistrés au WLC, naviguez vers la **radio > tous les aps**.

Une fois que le WLC est configuré pour le fonctionnement de base et a un ou plusieurs recouvrements enregistrés à lui, vous pouvez configurer le WLC pour l'authentification de Web externe utilisant un web server externe. Dans notre exemple, nous utilisons une version 4.1.1.24 de Cisco Secure ACS en tant que serveur de RAYON. D'abord, nous configurerons le WLC pour ce serveur de RAYON, et alors nous regarderons la configuration priée sur le Cisco Secure ACS pour cette installation.

Configurez le WLC pour le Cisco Secure ACS

Exécutez ces étapes afin d'ajouter le serveur de RAYON sur le WLC :

1. Du GUI WLC, cliquez sur le **menu Security**.
2. Sous le menu d'**AAA**, naviguez vers le sous-menu de **rayon** > d'**authentification**.
3. Cliquez sur New, et écrivez l'adresse IP du serveur de RAYON. Dans cet exemple, l'adresse IP du serveur est *10.77.244.196*.
4. Écrivez le secret partagé dans le WLC. Le secret partagé devrait être configuré les mêmes sur le WLC.
5. Choisissez l'**ASCII** ou **ensorcellez** pour le format de secret Shared. Le même format doit être choisi sur le WLC.
6. **1812** est le numéro de port utilisé pour l'authentification de RAYON.
7. Assurez-vous que l'option Server Status est placée à **activer**.
8. Cochez la case de Network User Enable pour authentifier les utilisateurs du réseau.
9. Cliquez sur **Apply**.

Configurez le WLAN sur WLC pour l'authentification Web

L'étape suivante est de configurer le WLAN pour l'authentification Web sur WLC. Exécutez ces étapes afin de configurer le WLAN sur WLC :

1. Cliquez sur le menu **WLAN du** GUI de contrôleur, et choisissez **nouveau**.
2. Choisissez le **WLAN** pour le type.
3. Écrivez un nom de profil et un WLAN SSID de votre choix, et cliquez sur Apply.**Note**: Le WLAN SSID distingue les majuscules et minuscules.
4. Sous l'**onglet Général**, assurez-vous que l'option **activée** est état et Broadcast SSID vérifiés.**Configuration WLAN**
5. Choisissez une interface pour le WLAN. Typiquement, une interface configurée dans un seul VLAN est tracée au WLAN de sorte que le client reçoive une adresse IP dans ce VLAN. Dans cet exemple, nous utilisons la *Gestion* pour l'interface.
6. Choisissez l'**onglet Sécurité**.
7. Sous le menu de la **couche 2**, n'en choisissez **aucun** pour le degré de sécurité de la couche

2.
8. Sous le menu de la **couche 3**, n'en choisissez **aucun** pour le degré de sécurité de la couche 3. Vérifiez la case à cocher de **stratégie de Web**, et choisissez l'**authentification**.
9. Sous le menu de **serveurs d'AAA**, pour le serveur d'authentification, choisissez le serveur de RAYON qui a été configuré sur ce WLC. D'autres menus devraient demeurer aux valeurs par défaut.

Configurez les informations de serveur Web sur WLC

Le web server qui héberge la page d'authentification Web devrait être configuré sur le WLC. Exécutez ces étapes pour configurer le web server :

1. Cliquez sur la **Sécurité** tableau vont au **Web authentique > page Web Login**.
2. Placez le type d'authentification Web comme **externe**.
3. Dans le champ IP Address de serveur Web, écrivez l'adresse IP du serveur qui héberge la page d'authentification Web, et cliquez sur Add le **serveur Web**. Dans cet exemple, l'adresse IP est *10.77.244.196*, qui apparaît sous les serveurs Web externes.
4. Écrivez l'URL pour la page d'authentification Web (dans cet exemple, *http://10.77.244.196/login.html)* dans le champ URL.

Configurez le Cisco Secure ACS

Dans ce document nous supposons que le serveur de Cisco Secure ACS est déjà installé et s'exécutant sur un ordinateur. Le pour en savoir plus comment installer le Cisco Secure ACS se rapportent au guide de configuration pour le Cisco Secure ACS 4.2.

Configurez les informations utilisateur sur le Cisco Secure ACS

Exécutez ces étapes afin de configurer des utilisateurs sur le Cisco Secure ACS :

1. Choisissez User Setup du GUI de Cisco Secure ACS, écrivez un nom d'utilisateur, et cliquez sur Add**/l'éditez**. Dans cet exemple, l'utilisateur est *user1*.
2. Par défaut, le PAP est utilisé pour authentifier des clients. Le mot de passe pour l'utilisateur est entré sous l'**authentification d'installation utilisateur** > de **mot de passe > PAP Cisco Secure**. Veillez-vous pour choisir des **ACS Internal Database** pour l'authentification de mot de passe.
3. Les besoins de l'utilisateur d'être assigné un groupe auquel l'utilisateur appartient. Choisissez le **groupe par défaut**.
4. Cliquez sur **Submit**.

Configurez les informations WLC sur le Cisco Secure ACS

Exécutez ces étapes afin de configurer les informations WLC sur le Cisco Secure ACS :

1. Dans le GUI ACS, cliquez sur l'onglet de **configuration réseau**, et cliquez sur Add l'**entrée**.
2. L'écran de client d'AAA d'ajouter apparaît.
3. Écrivez le nom du client. Dans cet exemple, nous utilisons *WLC*.
4. Écrivez l'adresse IP du client. L'adresse IP Du WLC est *10.77.244.206*.

5. Écrivez la clé secrète partagée et le format principal. Ceci devrait apparier l'entrée faite dans le **menu Security du** WLC.
6. Choisissez l'**ASCII** pour le format de principal intrant, qui devrait être identique sur le WLC.
7. Choisissez le **RAYON (Cisco Airespace)** pour Authenticate utilisant afin de placer le protocole utilisé entre le WLC et le serveur de RAYON.
8. Cliquez sur Submit **+ appliquez**.

Procédé d'authentification client

Configuration du client

Dans cet exemple, nous employons Cisco Aironet Desktop Utility pour exécuter l'authentification Web. Exécutez ces étapes afin de configurer Aironet Desktop Utility.

1. Ouvrez Aironet Desktop Utility de **début** > de **Cisco Aironet** > d'**Aironet Desktop Utility**.
2. Cliquez sur en fonction l'onglet de **Profile Management**.
3. Choisissez le profil **par défaut**, et le clic **modifient**.Cliquez sur l'**onglet Général**.Configurez un nom de profil. Dans cet exemple, le *par défaut* est utilisé.Configurez le SSID sous des noms de réseau. Dans cet exemple, *WLAN1* est utilisé.**Note**: Le SSID distingue les majuscules et minuscules et il devrait apparier le WLAN configuré sur le WLC.Cliquez sur l'onglet **Security**.N'en choisissez **aucun** comme Sécurité pour l'authentification Web.Cliquez sur l'onglet **Advanced**.Sous le menu **Sans fil de mode**, choisissez la fréquence à laquelle le client sans fil communique avec le RECOUVREMENT.Sous le **niveau de puissance de transmission**, choisissez l'alimentation qui est configurée sur le WLC.Laissez la valeur par défaut pour le mode d'économie d'énergie.Choisissez l'**infrastructure** comme type de réseau.Placez le préambule 802.11b en tant que **sous peu et long** pour une meilleure compatibilité.Cliquez sur **OK**.
4. Une fois que le profil est configuré sur le logiciel client, le client est associé avec succès et reçoit une adresse IP du groupe VLAN configuré pour l'interface de gestion.

Processus de connexion de client

Cette section explique comment la connexion de client se produit.

1. Ouvrez une fenêtre du navigateur et entrez n'importe quel URL ou adresse IP. La page d'authentification Web est alors affichée sur le client. Si le contrôleur exécute n'importe quelle release plus tôt que 3.0, l'utilisateur doit entrer dans *https://1.1.1.1/login.html* pour apporter la page d'authentification Web. Une fenêtre d'alerte de sécurité s'affiche.
2. Cliquez sur **Yes** pour poursuivre.
3. Quand la fenêtre de connexion apparaît, écrivez le nom d'utilisateur et mot de passe qui est configuré sur le serveur de RAYON. Si votre procédure de connexion est réussie, vous verrez deux fenêtres du navigateur. La fenêtre plus grande indique la procédure de connexion réussie, et vous peut cette fenêtre parcourir l'Internet. Utilisez la fenêtre plus petite pour vous déconnecter une fois l'utilisation du réseau invité terminée.

Vérifiez

Pour une authentification Web réussie, vous devez vérifier si les périphériques sont configurés d'une manière appropriée. Cette section explique comment vérifier les périphériques utilisés dans le processus.

Vérifier ACS

1. Cliquez sur User Setup, et puis cliquez sur List All Users sur le GUI ACS.Assurez-vous que l'état de l'utilisateur *est activé* et que le groupe par défaut est tracé à l'utilisateur.
2. Cliquez sur l'onglet de **configuration réseau**, et l'aspect dans la table de **clients d'AAA** afin de vérifier que le WLC est configuré en tant que client d'AAA.

Vérifiez WLC

1. Cliquez sur le menu **WLAN du** GUI WLC.Assurez-vous que le WLAN utilisé pour l'authentification Web est répertorié à la page.Assurez-vous qu'Admin Status pour le WLAN *est activé*.Assurez-vous la stratégie de sécurité pour le *Web-Auth d'*expositions WLAN.
2. Cliquez sur le **menu Security du** GUI WLC.Assurez-vous que le Cisco Secure ACS (10.77.244.196) est répertorié à la page.Assurez-vous que la case Network User est cochée.Assurez-vous que le port est *1812* et qu'Admin Status *est activé*.

Dépannez

Il y a beaucoup de raisons pour lesquelles une authentification Web n'est pas réussie. L'authentification Web de dépannage de document sur un contrôleur LAN Sans fil (WLC) explique clairement ces raisons en détail.

Dépannage des commandes

Note: Référez-vous aux informations importantes sur des commandes de debug avant que vous utilisiez ces commandes de **débogage**.

Le telnet dans le WLC et émettent ces commandes de dépanner l'authentification :

- **debug aaa all enable**

```
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00  00 00 00 00 00 00 0
0 00  ...s............
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73  65 72 31 02 12 93 c
3 66  ......user1....f
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
      user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010:       structureSize.............................89
Fri Sep 24 13:59:52 2010:       resultCode................................0
Fri Sep 24 13:59:52 2010:       protocolUsed..............................0x0
0000001
Fri Sep 24 13:59:52 2010:       proxyState................................00:
```

```
40:96:AC:DD:05-00:00
Fri Sep 24 13:59:52 2010:       Packet contains 2 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] Framed-IP-Address..................
.....0xffffffff (-1) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Class..............................
.....CACS:0/5183/a4df4ce/user1 (25 bytes)
Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for statio
n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
:ac:dd:05
                source: 48, valid bits: 0x1
        qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
                                                              vlanIfName: '',
aclName:
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
tation 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
Fri Sep 24 13:59:52 2010:       Packet contains 12 AVPs:
Fri Sep 24 13:59:52 2010:           AVP[01] User-Name..........................
.....user1 (5 bytes)
Fri Sep 24 13:59:52 2010:           AVP[02] Nas-Port...........................
.....0x00000002 (2) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[03] Nas-Ip-Address.....................
.....0x0a4df4ce (172881102) (4 bytes)
Fri Sep 24 13:59:52 2010:           AVP[04] Framed-IP-Address..................
.....0x0a4df4c7 (172881095) (4 bytes)
```

- **enable de détail de debug aaa**

Des tentatives d'authentification défaillante sont répertoriées dans le menu situé aux **états et à l'activité >** aux **essais ratés**.

Informations connexes

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