Exemple de configuration de filtres MAC avec des contrôleurs de réseau local sans fil (WLC)

Contenu

Introduction

Ce document explique comment configurer des filtres d'adresses MAC avec les contrôleurs de réseau local sans fil (WLC) avec un exemple de configuration. Ce document discute également comment autoriser des points d'accès léger (LAP) contre un serveur AAA.

Conditions préalables

Conditions requises

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

- Connaissance de base de la configuration des LAP et des WLC Cisco
- Connaissance de base des solutions de sécurité de Cisco Unified Wireless

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 logiciel 5.2.178.0
- Recouvrements de gamme de Cisco 1230AG
- adaptateur client sans fil du 802.11 a/b/g avec le micrologiciel 4.4
- Version 4.4 d'Aironet Desktop Utility (ADU)

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.

Filtre d'adresse MAC (authentification MAC) sur WLCs

Quand vous créez un filtre d'adresse MAC sur WLCs, on accorde des utilisateurs ou l'accès refusé au réseau WLAN sont basés sur l'adresse MAC du client qu'ils les utilisent.

Il y a deux types d'authentification MAC qui sont pris en charge sur WLCs :

- Authentification MAC locale
- Authentification MAC utilisant un serveur de RAYON

Avec l'authentification MAC locale, des adresses MAC d'utilisateur sont enregistrées dans une base de données sur le WLC. Quand des essais d'un utilisateur pour accéder au WLAN qui est configuré pour le filtrage MAC, l'adresse MAC de client est validés contre la base de données locale sur le WLC, et le client est accordé l'accès au WLAN si l'authentification est réussie.

Par défaut, les supports de base de données locale WLC jusqu'à 512 entrées d'utilisateur.

La base de données locale des utilisateurs est limitée à un maximum de 2048 entrées. La base de données locale enregistre des entrées pour ces éléments :

- Utilisateurs locaux de Gestion, qui inclut des ambassadeurs de lobby
- Utilisateurs de réseau local, qui inclut des utilisateurs d'invité
- Entrées de filtre d'adresses MAC
- Entrées de la liste d'exclusion
- Entrées de la liste d'autorisation de Point d'accès

Ensemble, tous ces types d'utilisateurs ne peuvent pas dépasser la taille de la base de données configurée.

Afin d'augmenter la base de données locale, utilisez cette commande du CLI :

```
<Cisco Controller>config database size ?
<count>        Enter the maximum number of entries (512-2048)
```

Alternativement, l'authentification d'adresse MAC peut également être exécutée utilisant un serveur de RAYON. La seule différence est que la base de données d'adresse MAC d'utilisateurs

est enregistrée dans le serveur de RAYON au lieu du WLC. Quand une base de données utilisateur est enregistrée sur un serveur de RAYON le WLC en avant l'adresse MAC du client au serveur de RAYON pour la validation de client. Puis, le serveur de RAYON valide l'adresse MAC basée sur la base de données qu'elle a. Si l'authentification client est réussie, on accorde le client l'accès au WLAN. N'importe quel serveur de RAYON qui prend en charge l'authentification d'adresse MAC peut être utilisé.

Configurez l'authentification MAC locale sur WLCs

Terminez-vous ces étapes afin de configurer l'authentification MAC locale sur le WLCs :

1. Configurez un WLAN et activez le filtrage MAC
2. Configurez la base de données locale sur le WLC avec des adresses MAC de clientNote: Avant que vous configuriez l'authentification MAC, vous devez configurer le WLC pour le fonctionnement de base et enregistrer les recouvrements au WLC. Ce document suppose que le WLC est déjà 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).Note: Il n'y a aucune configuration spéciale requise sur le client sans fil afin de prendre en charge l'authentification MAC.

Configurez un WLAN et activez le filtrage MAC

Terminez-vous ces étapes afin de configurer un WLAN avec le filtrage MAC :

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 *MAC-WLAN* et l'ID de WLAN est *1.*
3. Cliquez sur **Apply**.
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Sous des stratégies de sécurité > le degré de sécurité de la couche 2, cochez la case de **filtrage MAC**.Ceci active l'authentification MAC pour le WLAN.Sous des stratégies générales > le nom d'interface, sélectionnez l'interface à laquelle le WLAN est tracé.Dans cet exemple, le WLAN est tracé à l'interface de gestion.Sélectionnez les autres paramètres, qui dépendent des conditions requises de conception du WLAN.Cliquez sur **Apply**.

L'étape suivante est de configurer la base de données locale sur le WLC avec les adresses MAC de client.

Référez-vous aux VLAN sur l'exemple Sans fil de configuration de contrôleurs LAN pour les informations sur la façon dont configurer les interfaces dynamiques (VLAN) sur WLCs.

Configurez la base de données locale sur le WLC avec des adresses MAC de client

Terminez-vous ces étapes afin de configurer la base de données locale avec une adresse MAC de client sur le WLC :

1. Cliquez sur Security du GUI de contrôleur, et puis cliquez sur le **filtrage MAC du** menu de côté gauche.La fenêtre de filtrage MAC apparaît.
2. Cliquez sur New afin de créer une entrée d'adresse MAC de base de données locale sur le WLC.
3. Dans les filtres d'adresses MAC > la nouvelle fenêtre, écrivent l'adresse MAC, le nom de profil, la description et le nom d'interface pour le client.Voici un exemple :
4. Cliquez sur **Apply**.
5. Répétez les étapes 2-4 afin d'ajouter plus de clients à la base de données locale.Maintenant, quand les clients se connectent à ce WLAN, le WLC valide l'adresse MAC de clients contre la base de données locale et si la validation est réussie, le client est accordé l'accès au réseau.**Note**: Dans cet exemple, seulement un filtre d'adresse MAC sans n'importe quel autre mécanisme de sécurité de la couche 2 a été utilisé. Cisco recommande que l'authentification d'adresse MAC devrait être utilisée des méthodes avec autre degré de sécurité de la couche 2 ou de la couche 3. Il n'est pas recommandé d'employer seulement l'authentification d'adresse MAC pour sécuriser votre réseau WLAN parce qu'il ne fournit pas un mécanisme de forte sécurité.

Configurez l'authentification MAC utilisant un serveur de RAYON

Terminez-vous ces étapes afin de configurer l'authentification MAC utilisant un serveur de RAYON. Dans cet exemple, le serveur de Cisco Secure ACS est utilisé en tant que serveur de RAYON.

1. Configurez un WLAN et activez le filtrage MAC
2. Configurez le serveur de RAYON avec des adresses MAC de client

Configurez un WLAN et activez le filtrage MAC

Terminez-vous ces étapes afin de configurer un WLAN avec le filtrage MAC :

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 *MAC-ACS-WLAN* et l'ID de WLAN est *2.*
3. Cliquez sur **Apply**.
4. Dans la fenêtre WLAN > Edit, définissez les paramètres spécifiques au WLAN.Sous des stratégies de sécurité > le degré de sécurité de la couche 2, cochez la case de **filtrage MAC**.Ceci active l'authentification MAC pour le WLAN.Sous des stratégies générales > le nom d'interface, sélectionnez l'interface à laquelle le WLAN est tracé.Sous des serveurs de RAYON, sélectionnez le serveur de RAYON qui sera utilisé pour l'authentification MAC.**Note**: Avant que vous puissiez sélectionner le serveur de RAYON de la fenêtre de WLAN > Edit, vous devriez définir le serveur de RAYON dans la fenêtre d'authentification de Sécurité > de rayon et activer le serveur de RAYON.Sélectionnez les autres paramètres, qui dépendent des conditions requises de conception du WLAN.Cliquez sur **Apply**.
5. Cliquez sur Security **> filtrage MAC**.
6. Dans la fenêtre de filtrage MAC, choisissez le type de serveur de RAYON sous le mode

compatible de RAYON.Cet exemple utilise Cisco ACS.
7. Du délimiteur de MAC abaissez le menu, choisissent le délimiteur de MAC.Cet exemple utilise des deux points.
8. Cliquez sur **Apply**.

L'étape suivante est de configurer le serveur ACS avec les adresses MAC de client.

Configurez le serveur de RAYON avec des adresses MAC de client

Terminez-vous ces étapes afin d'ajouter une adresse MAC à l'ACS :

1. Définissez le WLC en tant que client d'AAA sur le serveur ACS. Cliquez sur **Network Configuration** depuis l'interface graphique ACS.
2. Quand la fenêtre de configuration réseau apparaît, définissez le nom du WLC, de l'adresse IP, du secret partagé et de la méthode d'authentification (RAYON Cisco Aironet ou RAYON Airespace).Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS.**Note**: les clés secrètes partagées que vous configurez sur le WLC et le serveur ACS doivent correspondre. Le secret partagé distingue les majuscules et minuscules.
3. Du menu principal ACS, cliquez sur User Setup.
4. Dans la zone de texte d'utilisateur, écrivez l'adresse MAC afin d'ajouter à la base de données utilisateur.**Note**: L'adresse MAC doit être exactement pendant qu'elle est envoyée par le WLC pour le nom d'utilisateur et le mot de passe. Si l'authentification échoue, vérifiez les essais ratés se connectent pour voir comment le MAC est signalé par le WLC. Ne coupez-collez pas l'adresse MAC, comme ceci peut introduire les caractères fantômes.
5. Dans la fenêtre d'installation utilisateur, écrivez l'adresse MAC dans la zone de texte du mot de passe Sécurisé-PAP.**Note**: L'adresse MAC doit être exactement pendant qu'elle est envoyée par le WLC pour le nom d'utilisateur et le mot de passe. Si l'authentification échoue, vérifiez les essais ratés se connectent pour voir comment le MAC est signalé par AP. Ne coupez-collez pas l'adresse MAC, comme ceci peut introduire les caractères fantômes.
6. Cliquez sur **Submit**.
7. Répétez les étapes 2-5 afin d'ajouter plus d'utilisateurs à la base de données ACS.Maintenant, quand les clients se connectent à ce WLAN, le WLC passe les qualifications au serveur ACS. Le serveur ACS valide les qualifications contre la base de données ACS. Si l'adresse MAC de client est présente dans la base de données, le serveur de RAYON ACS renvoie un succès d'authentification au WLC et le client sera accordé l'accès au WLAN.

Employez le CLI pour configurer le filtre d'adresses MAC sur WLC

Ce document discuté préalablement comment utiliser le GUI WLC pour configurer des filtres d'adresses MAC. Vous pouvez également employer le CLI afin de configurer des filtres d'adresses MAC sur le WLC. Vous pouvez employer ces commandes afin de configurer le filtre d'adresses MAC sur WLC :

- Émettez la commande de **wlan_id d'enable de config wlan mac-filtering** afin d'activer le filtrage MAC. le bEnter la commande de **show wlan** afin de vérifier que vous avez le filtrage MAC a activé pour le WLAN.
- commande de **config macfilter add** :La commande de **config macfilter add** vous permet

d'ajouter un macfilter, interface, description, et ainsi de suite.Employez la commande de **config macfilter add** afin de créer une entrée de filtre d'adresses MAC sur le contrôleur LAN de radio de Cisco. Employez cette commande afin d'ajouter un client localement à un RÉSEAU LOCAL Sans fil sur le contrôleur LAN de radio de Cisco. Ce filtre saute la procédure d'authentification de RAYON.

```
config macfilter add MAC_address wlan_id [interface_name]
[description] [IP address]
```

Exemple :Écrivez une reproduction d'adresses MAC-à-IP statique. Ceci peut être fait pour prendre en charge un *client passif*, c.-à-d., un qui n'utilise pas le DHCP et ne transmet pas les paquets IP non sollicités.

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

- commande de **config macfilter ip-address**La commande de **config macfilter ip-address** vous permet de tracer un filtre d'adresses MAC existant à une adresse IP. Employez cette commande afin de configurer une adresse IP dans la base de données locale de filtre d'adresses MAC :

```
config macfilter ip-address
 MAC_address IP address
```

Exemple :

```
>config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Configurez un délai d'attente pour les clients handicapés

Vous pouvez configurer un délai d'attente pour les clients handicapés. Des clients qui n'authentifient pas trois fois pendant les tentatives de s'associer sont automatiquement désactivés d'autres de tentatives d'association. Après le délai d'inactivité expire, le client est permis pour relancer l'authentification jusqu'à ce qu'elle s'associe ou échoue authentification et est exclu de nouveau.

Sélectionnez la commande de **délai d'attente de wlan_id de config wlan exclusionlist** afin de configurer le délai d'attente pour les clients handicapés. La valeur du dépassement de durée peut être de 1 à 65535 secondes, ou vous pouvez écrire 0 afin de désactiver de manière permanente le client.

Vérifiez

Employez ces commandes afin de vérifier si le filtre d'adresses MAC est configuré correctement :

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **résumé de show macfilter** — Affiche un résumé de toutes les entrées de filtre d'adresses MAC.
- *adresse MAC* ***<client de détail de show macfilter >*** — Affichage détaillé d'une entrée de filtre d'adresses MAC.

Voici un exemple de la commande **récapitulative de show macfilter** :

```
(Cisco Controller) >show macfilter summary

MAC Filter RADIUS Compatibility mode..... Cisco ACS
```

```
MAC Filter Delimiter.......................... None

Local Mac Filter Table

MAC Address               WLAN Id          Description
-----------------------   -------------    --------------------------------
00:40:96:ac:e6:57           1              Guest


(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57
```

Voici un exemple de la commande de **détail de show macfilter** :

```
(Cisco Controller) >show macfilter detail 00:40:96:ac:e6:57

MAC Address..................................... 00:40:96:ac:e6:57
WLAN Identifier................................. 1
Interface Name.................................. mac-client
Description..................................... Guest
```

Dépannez

Vous pouvez utiliser ces commandes de dépanner votre configuration :

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **le debug aaa tout activent** — Fournit l'élimination des imperfections de tous les messages d'AAA.
- **debug mac addr <adresse-MAC-client xx:** *xx : xx : xx : xx : xx* **>** — Afin de configurer l'élimination des imperfections de MAC, utilisez la commande de **debug mac**.

Voici un exemple du **debug aaa toute la** commande d'**enable** :

```
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: Looking up local blacklist 004096ace657
Wed May 23 11:13:55 2007: User 004096ace657 authenticated
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Returning AAA Error 'Success' (0)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: AuthorizationResponse: 0xbadff97c
Wed May 23 11:13:55 2007: structureSize.............................76
Wed May 23 11:13:55 2007: resultCode.................................0
Wed May 23 11:13:55 2007: protocolUsed.............................0x00000008
Wed May 23 11:13:55 2007: proxyState.................................
                                00:40:96:AC:E6:57-00:00
Wed May 23 11:13:55 2007: Packet contains 2 AVPs:
Wed May 23 11:13:55 2007:     AVP[01] Service-Type.............................
                                    0x0000000a (10) (4 bytes)
Wed May 23 11:13:55 2007:     AVP[02] Airespace / Interface-Name..............
                                    staff-vlan (10 bytes)
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[0]: attribute 6
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 processing avps[1]: attribute 5
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Applying new AAA override for
                          station 00:40:96:ac:e6:57
Wed May 23 11:13:55 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
source: 2, valid bits: 0x200 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff,
sessionTimeout: -1dataAvgC: -1, rTAvgC: -1, dataBurstC:

-1, rTimeBurstC: -1vlanIfName: 'mac-client'
```

Quand un client sans fil n'est pas présent dans la base de données d'adresse MAC sur le WLC (base de données locale) ou sur les essais de serveur de RAYON pour s'associer au WLAN, ce client sera exclu. Voici un exemple du **debug aaa toute la** commande d'**enable** pour une authentification MAC infructueuse :

```
Wed May 23 11:05:06 2007: Unable to find requested user entry for 004096ace657
Wed May 23 11:05:06 2007: AuthenticationRequest: 0xa620e50
Wed May 23 11:05:06 2007: Callback.....................................0x807e724
Wed May 23 11:05:06 2007: protocolType.................................0x00000001
Wed May 23 11:05:06 2007: proxyState...................................
                                 00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 14 AVPs (not shown)
Wed May 23 11:05:06 2007: 00:40:96:ac:e6:57 Returning AAA Error 'No Server' (-7)
                          for mobile 00:40:96:ac:e6:57
Wed May 23 11:05:06 2007: AuthorizationResponse: 0xbadff7e4
Wed May 23 11:05:06 2007: structureSize................................28
Wed May 23 11:05:06 2007: resultCode...................................-7
Wed May 23 11:05:06 2007: protocolUsed.................................0xffffffff
Wed May 23 11:05:06 2007: proxyState...................................
                                 00:40:96:AC:E6:57-00:00
Wed May 23 11:05:06 2007: Packet contains 0 AVPs:
```

Des clients sans fil qui essayent d'authentifier par l'adresse MAC sont rejetés ; L'état d'authentification défaillante affiche des erreurs internes

Quand vous utilisez ACS 4.1 qui fonctionne sur un serveur d'entreprise de Microsoft Windows 2003, des clients qui essayent d'authentifier par l'adresse MAC sont rejetés. Ceci se produit quand un client d'AAA envoie la valeur d'attribut Service-Type=10 au serveur d'AAA. C'est en raison de l'ID de bogue Cisco CSCsh62641 (clients enregistrés seulement). Les clients d'AAA affectés par cette bogue incluent WLCs et Commutateurs qui utilisent la dérivation d'authentification MAC.

Les contournements sont :

- Déclassifiez à ACS 4.0.ou
- Ajoutez les adresses MAC à authentifier à une protection d'accès au réseau (PETIT SOMME) sous la table interne d'adresse MAC de DB ACS.

Non capable ajouter un filtre d'adresses MAC utilisant le GUI WLC

Ceci peut se produire becaue de l'ID de bogue Cisco CSCsj98722 (clients enregistrés seulement). La bogue est réparée dans la release 4.2 du code. Si vous êtes des versions courantes plus tôt que 4.2, vous pouvez améliorer le micrologiciel à 4.2 ou utiliser ces deux contournements pour cette question.

- Employez le CLI afin de configurer le filtre d'adresses MAC avec cette commande :

  config macfilter add <MAC address> <WLAN ID#> <Interface>
- Du GUI de Web du contrôleur, choisissez **n'importe quel WLAN** sous l'onglet Sécurité et écrivez l'adresse MAC à filtrer.

Client silent non placé dans l'état de passage

Si le DHCP exigé n'est pas configuré sur le contrôleur, les aps apprennent l'adresse IP des clients sans fil quand les clients sans fil envoient le premier paquet IP ou ARP. Si les clients sans fil sont les périphériques passifs, par exemple, les périphériques qui n'initient pas une transmission, alors les aps n'apprend pas l'adresse IP des périphériques sans fil. En conséquence, le contrôleur attend dix secondes le client pour envoyer un paquet IP. S'il n'y a aucune réponse du paquet du

client, alors le contrôleur relâche tous les paquets aux clients sans fil passifs. Cette question est documentée dans l'ID de bogue Cisco CSCsq46427 (les clients enregistrés seulement)

Pendant qu'un contournement recommandé pour les périphériques passifs comme des imprimantes, AP Sans fil pompe et ainsi de suite, vous devez placer le WLAN pour le filtrage MAC et faire vérifier le dépassement d'AAA afin de permettre ces périphériques à connecter.

Un filtre d'adresse MAC peut être créé sur le contrôleur qui trace l'adresse MAC du périphérique sans fil à une adresse IP.

Note: Ceci exige du filtrage des adresses MAC d'être activé sur la configuration WLAN pour le degré de sécurité de la couche 2. Il exige également `permettent l'AAA Overide` à activer dans les configurations anticipées de la configuration WLAN.

Du CLI, sélectionnez cette commande afin de créer le filtre d'adresse MAC :

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

Voici un exemple :

```
config macfilter add <MAC address>  <WLAN ID#> <Interface>
```

Informations connexes

- Exemple de configuration de listes de contrôle d'accès sur un contrôleur de réseau local sans fil
- Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.1
- Page de support de la technologie sans fil
- Support et documentation techniques - Cisco Systems