Authentification Web centrale avec FlexConnect aps sur un WLC avec l'exemple de configuration ISE

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Configurez](#)
[Diagramme du réseau](#)
[Configuration WLC](#)
[Configuration ISE](#)
[Créez le profil d'autorisation](#)
[Créez une règle d'authentification](#)
[Créez une règle d'autorisation](#)
[Activez le renouvellement IP (facultatif)](#)
[La circulation](#)
[Vérifiez](#)

Introduction

Ce document décrit comment configurer l'authentification Web centrale avec les Points d'accès de FlexConnect (aps) sur un contrôleur LAN Sans fil (WLC) avec le Cisco Identity Services Engine (ISE) en mode de commutation locale.

Remarque importante : À ce moment, l'authentification locale sur le FlexAPs n'est pas prise en charge pour ce scénario.

D'autres documents dans cette gamme

- Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine
- Authentification Web centrale exemple sur WLC et ISE configuration

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Logiciel Cisco Identity Services Engine (ISE), version 1.2.1
- Logiciel Sans fil de contrôleur LAN, version - 7.4.100.0

Configurez

Il y a de plusieurs méthodes pour configurer l'authentification Web centrale sur le contrôleur LAN Sans fil (WLC). La première méthode est l'authentification Web locale dans laquelle le WLC réoriente le trafic http à un interne ou à un serveur externe où l'utilisateur est incité à authentifier. Le WLC alors cherche les qualifications (renvoyées par l'intermédiaire d'une requête HTTP GET dans le cas d'un serveur externe) et fait une authentification de RADIUS. Dans le cas d'un utilisateur d'invité, un serveur externe (tel qu'engine de gestion d'identité (ISE) ou NAC Guest Server (NGS)) est exigé pendant que le portail fournit des caractéristiques telles que l'enregistrement et l'auto-ravitaillement de périphérique. Ce processus inclut ces étapes :

1. Les associés d'utilisateur à l'authentification Web SSID.
2. L'utilisateur ouvre leur navigateur.
3. Les redirect to WLC le portail d'invité (tel qu'ISE ou NGS) dès qu'un URL sera écrit.
4. L'utilisateur authentifie sur le portail.
5. Le portail d'invité réoriente de nouveau au WLC avec les qualifications entrées.
6. Le WLC authentifie l'utilisateur d'invité par l'intermédiaire de RADIUS.
7. Le WLC réoriente de nouveau à l'URL d'original.

Ce processus inclut beaucoup de redirection. La nouvelle approche est d'utiliser l'authentification Web centrale qui fonctionne avec ISE (versions plus tard que 1.1) et WLC (versions plus tard que 7.2). Ce processus inclut ces étapes :

1. Les associés d'utilisateur à l'authentification Web SSID.
2. L'utilisateur ouvre leur navigateur.
3. Les redirect to WLC le portail d'invité.
4. L'utilisateur authentifie sur le portail.
5. L'ISE envoie une modification de RADIUS de l'autorisation (CoA - port UDP 1700) d'indiquer au contrôleur que l'utilisateur est valide et pousse par la suite des attributs RADIUS tels que la liste de contrôle d'accès (ACL).
6. L'utilisateur est incité à relancer l'URL d'original.

Cette section décrit les étapes nécessaires pour configurer l'authentification Web centrale sur WLC et ISE.

Diagramme du réseau

Cette configuration utilise cette configuration réseau :

Configuration WLC

La configuration WLC est assez simple. Une « astuce ? est utilisé (mêmes que sur des Commutateurs) pour obtenir l'authentication url dynamique de l'ISE. (Puisqu'elle utilise le CoA, une session doit être créée comme ID de session fait partie de l'URL.) Le SSID est configuré pour utiliser le filtrage MAC, et l'ISE est configuré pour renvoyer un message d'Access-recevoir même si l'adresse MAC n'est pas trouvée de sorte qu'elle envoie l'URL de redirection pour tous les utilisateurs.

En outre, le Contrôle d'admission au réseau (NAC) de RADIUS et le dépassement d'AAA doivent être activés. RADIUS NAC permet à l'ISE pour envoyer une demande CoA qui indique que l'utilisateur est maintenant authentifié et peut accéder au réseau. Il est également utilisé pour l'estimation de posture dans laquelle l'ISE change le profil utilisateur basé sur le résultat de posture.

1. Assurez-vous que le serveur de RADIUS fait activer RFC3576 (CoA), qui est le par défaut.

2. Créez un nouveau WLAN. Cet exemple crée un nouveau *CWAFlex* nommé par WLAN et l'assigne à vlan33. (Note qu'elle n'aura pas beaucoup d'effet puisque le Point d'accès est en mode de commutation locale.)

3. Sur l'onglet Sécurité, filtrage MAC d'enable comme degré de sécurité de la couche 2.

4. Sur l'onglet de la couche 3, assurez que la Sécurité est désactivée. (Si l'authentification Web est activée sur la couche 3, l'authentification Web locale est activée, authentification Web non centrale.)

5. Sur l'onglet AAA Servers, sélectionnez le serveur ISE comme serveur de rayon pour le WLAN. Sur option, vous pouvez le sélectionner pour rendre compte afin d'avoir plus d'informations détaillées sur ISE.

6. Sur l'onglet Avancé, assurez que l'Allow AAA Override est vérifié et Radius NAC est sélectionné pour l'état NAC.

7. Créez un ACL de réorientation.

   ThisACL est mis en référence dans le message d'Access-recevoir du theISE et définit quel

trafic devrait être réorienté (refusé par le theACL) aussi bien que quel trafic ne devrait pas être réorienté (autorisé par le theACL). Fondamentalement, des DN et le trafic à/de le theISE doit être permis. **Note**: Une question avec FlexConnect aps est que vous devez créer un ACL de FlexConnect séparé de votre ACL normal. Cette question est documentée dans la bogue Cisco CSCue68065 et est réparée dans la version 7.5. Dans WLC 7.5 et plus tard, seulement un FlexACL est exigé, et aucun ACL standard n'est nécessaire. Le WLC prévoit que l'ACL de réorientation retourné par ISE est un ACL normal. Cependant, l'assurer fonctionne, vous a besoin du même ACL appliqué que l'ACL de FlexConnect.
Cet exemple affiche comment créer un ACL de FlexConnect nommé *flexred* :

Créez les règles de permettre le trafic DNS aussi bien que de trafiquer vers ISE et de refuser le repos.

Si vous voulez la sécurité maximale, vous pouvez permettre seulement le port 8443 vers ISE. (Si posant, vous devez ajouter les ports typiques de posture, tels que 8905,8906,8909,8910.)

(Seulement sur le code avant la version 7.5 due à CSCue68065) choisissez la **Sécurité > les listes de contrôle d'accès** pour créer un ACL identique avec le même nom.

Préparez le FlexConnect spécifique AP. Notez que pour un plus grand déploiement, vous utiliseriez typiquement des groupes de FlexConnect et n'exécuteriez pas ces éléments sur une base par-AP pour des raisons d'évolutivité.

Cliquez sur la **radio**, et sélectionnez le Point d'accès spécifique.Cliquez sur l'onglet de **FlexConnect**, et cliquez sur **Webauthentication externe ACLs**. (Avant la version 7.4, cette option a été nommée des *stratégies de Web*.)

Ajoutez l'ACL (nommé *flexred* dans cet exemple) à la zone de stratégies de Web. Ceci pré-poussers l'ACL au Point d'accès. Il n'est pas appliqué encore, mais le contenu d'ACL est donné à AP de sorte qu'il puisse s'appliquer une fois nécessaire.

La configuration WLC est maintenant complète.

Configuration ISE

Créez le profil d'autorisation

Terminez-vous ces étapes afin de créer le profil d'autorisation :

1. Cliquez sur la **stratégie**, et puis cliquez sur les **éléments de stratégie**.
2. **Résultats de** clic.
3. Développez l'**autorisation**, et puis cliquez sur le **profil d'autorisation**.
4. Cliquez sur le bouton d'**ajouter** afin de créer un nouveau profil d'autorisation pour le webauth central.
5. Dans la zone d'**identification**, écrivez un nom pour le profil. Cet exemple utilise *CentralWebauth*.
6. Choisissez **ACCESS_ACCEPT de la** liste déroulante de type d'Access.
7. Cochez la case d'**authentification Web**, et choisissez le **Web centralisé authentique de la** liste déroulante.
8. Dans le domaine d'ACL, écrivez le nom de l'ACL sur le WLC qui définit le trafic qui sera réorienté. Ce les exemples les utilise *flexred*.
9. Choisissez le **par défaut de la** liste déroulante de réorientation.

L'attribut de réorientation définit si l'ISE voit le portail de web par défaut ou un portail web fait sur commande que l'admin ISE a créés. Par exemple, l'ACL *flexred* dans cet exemple déclenche une redirection sur le trafic http du client à n'importe où.

Créez une règle d'authentification

Terminez-vous ces étapes afin d'employer le profil d'authentification pour créer la règle d'authentification :

1. Sous le menu de stratégie, **authentification de** clic. Cette image affiche un exemple de la façon configurer la règle de stratégie d'authentification. Dans cet exemple, on configure une règle qui déclenchera quand le filtrage MAC est détecté.

2. Écrivez un nom pour votre règle d'authentification. Cet exemple utilise le *mab Sans fil*.
3. Sélectionnez (**+**) l'icône plus dans si champ de condition.
4. Choisissez l'**état composé**, et puis choisissez **Wireless_MAB**.
5. Choisissez « l'accès au réseau par défaut » en tant que protocole permis.
6. Cliquez sur la flèche localisée à côté de **et…** afin de développer la règle plus loin.
7. Cliquez sur **+** icône dans le domaine de source d'identité, et choisissez les **points finaux internes**.
8. Choisissez **continuent du** si liste déroulante non trouvée d'utilisateur.

Cette option permet un périphérique à authentifier (par le webauth) même si son adresse MAC n'est pas connue. Les clients de dot1x peuvent encore authentifier avec leurs qualifications et ne devraient pas être concernés par cette configuration.

Créez une règle d'autorisation

Il y a maintenant plusieurs règles de configurer dans la stratégie d'autorisation. Quand le PC est

associé, il passera par le filtrage de MAC ; on le suppose que l'adresse MAC n'est pas connue, ainsi le webauth et l'ACL sont retournés. Cette règle *non connue de MAC* est affichée dans l'image ci-dessous et est configurée dans cette section.

Terminez-vous ces étapes afin de créer la règle d'autorisation :

1. Créez une nouvelle règle, et écrivez un nom. Cet exemple utilise le *MAC non connu*.
2. Cliquez sur (**+**) l'icône plus dans le domaine de condition, et choisissez de créer un nouvel état.
3. Développez la liste déroulante d'**expression**.
4. Choisissez l'**accès au réseau**, et développez-le.
5. Cliquez sur **AuthenticationStatus**, et choisissez l'opérateur d'**égaux**.
6. Choisissez **UnknownUser** dans le domaine droit.
7. Àla page générale d'autorisation, choisissez **CentralWebauth** (profil d'autorisation) dans le domaine à la droite du mot **alors**.Cette étape permet à l'ISE pour continuer quoique l'utilisateur (ou le MAC) ne soit pas connu.Des utilisateurs inconnus sont maintenant présentés avec la page de connexion. Cependant, une fois qu'ils entrent dans leurs qualifications, ils sont présentés de nouveau avec une demande d'authentification sur l'ISE ; donc, une autre règle doit être configurée avec une condition qui est remplie si l'utilisateur est un utilisateur d'invité. Dans cet exemple, *si l'invité d'égaux d'UseridentityGroup* est utilisé, et lui est supposé que tous les invités appartiennent à ce groupe.
8. Cliquez sur les actions se boutonnent situé à la fin de la règle *non connue de MAC*, et choisissent d'insérer une nouvelle règle ci-dessus.**Note**: Il est très important que cette nouvelle règle soit livré avant que la règle *non connue de MAC*.
9. Entrez dans le **2ème AUTHENTIQUE** dans la zone d'identification.
10. Sélectionnez un groupe d'identité comme condition. Cet exemple a choisi l'**invité**.
11. Dans le domaine de condition, cliquez sur (**+**) l'icône plus, et choisissez de créer un nouvel état.
12. Choisissez l'**accès au réseau**, et cliquez sur **UseCase**.
13. Choisissez les **égaux** en tant qu'opérateur.
14. Choisissez **GuestFlow** comme bon opérande. Ceci signifie que vous attraperez les utilisateurs qui ont juste ouvert une session sur la page Web et reviennent après qu'une modification de l'autorisation (la pièce d'écoulement d'invité de la règle) et seulement s'ils appartiennent au groupe d'identité d'invité.
15. Àla page d'autorisation, cliquez sur (**+**) l'icône plus (située à côté de *puis*) afin de choisir un résultat pour votre règle.

    Dans cet exemple, un profil préconfiguré (vlan34) est assigné ; cette configuration n'est pas affichée dans ce document.

Vous pouvez choisir une option d'**Access d'autorisation** ou créer un profil fait sur commande afin de renvoyer le VLAN ou les attributs ces vous aimez.

Remarque importante : Dans ISE Version1.3, selon le type d'authentification Web, le cas d'utilisation « d'écoulement d'invité » ne pourrait être produit plus. La règle d'autorisation devrait alors contenir l'usergroup d'invité comme seul état possible.

Activez le renouvellement IP (facultatif)

Si vous assignez un VLAN, la dernière étape est pour que le PC client renouvelle son adresse IP. Cette étape est réalisée par le portail d'invité pour des clients Windows. Si vous ne placiez pas un VLAN pour la *2ème* règle *AUTHENTIQUE* plus tôt, vous pouvez ignorer cette étape.

Notez que sur FlexConnect aps, le VLAN doit préexister sur AP lui-même. Par conséquent, s'il ne fait pas, vous pouvez créer un mappage VLAN-ACL sur AP lui-même ou sur le groupe de flexible où vous n'appliquez aucun ACL pour le nouveau VLAN vous voulez créer. Cela crée réellement un VLAN (sans l'ACL là-dessus).

Si vous assigniez un VLAN, terminez-vous ces étapes afin d'activer le renouvellement IP :

1. Cliquez sur la **gestion**, et puis cliquez sur la **Gestion d'invité**.
2. **Configurations de** clic.
3. Développez l'**invité**, et puis développez la **configuration Multi-portaile**.
4. Clic **DefaultGuestPortal** ou le nom d'un portail fait sur commande que vous avez pu avoir créé.
5. Cliquez sur la case de **release DHCP de VLAN**.**Note**: Cette option fonctionne seulement pour des clients Windows.

La circulation

Il peut sembler difficile de comprendre quel trafic est envoyé où dans ce scénario. Voici un examen rapide :

- Le client envoie la demande d'association au-dessus de l'air pour le SSID.
- Le WLC manipule l'authentification de filtrage MAC avec ISE (où il reçoit les attributs de redirection).
- Le client reçoit seulement une réponse d'assoc après que le filtrage MAC soit complet.
- Le client soumet une requête DHCP et cela est localement commuté par l'obain de Point d'accès une adresse IP du site distant.
- Dans l'état de Central_webauth, le trafic marqué pour refusent sur l'ACL de réorientation (ainsi le HTTP typiquement) est centralement commuté. Ainsi ce n'est pas AP qui fait la redirection mais le WLC ; par exemple, quand le client demande n'importe quel site Web, AP envoie ceci au WLC encapsulé dans CAPWAP et le WLC charrie cette adresse IP de site Web et la réoriente vers ISE.
- Le client est réorienté à l'ISE réorientent l'URL. Ceci est localement commuté de nouveau (parce qu'il frappe sur l'autorisation sur le flexible réorientent l'ACL).
- Une fois dans l'état de PASSAGE, le trafic est localement commuté.

Vérifiez

Une fois que l'utilisateur est associé au SSID, l'autorisation est affichée dans la page ISE.

Du bas, vous pouvez voir l'authentification de filtrage des adresses MAC qui renvoie les attributs CWA. Est ensuite la procédure de connexion portaile avec le nom d'utilisateur. L'ISE envoie alors un CoA au WLC et la dernière authentification est une authentification de filtrage de MAC de la couche 2 du côté WLC, mais ISE se souvient le client et le nom d'utilisateur et applique le VLAN nécessaire que nous avons configuré dans cet exemple.

Quand n'importe quelle adresse est ouverte sur le client, le navigateur est réorienté à l'ISE. Assurez que le Système de noms de domaine (DNS) est configuré correctement.

On accorde l'accès au réseau après que l'utilisateur reçoive les stratégies.

Sur le contrôleur, l'état de Policy Manager et des modifications d'état de RADIUS NAC de *POSTURE_REQD À S'EXÉCUTER*.