Version 5.2 ACS et WLC pour par l'exemple de configuration d'authentification WLAN

ID de document : 118661

Mis à jour : Janv. 14, 2015

Contribué par Brahadesh Srinivasaraghavan, ingénieur TAC Cisco.

PDF de téléchargement
Copie
Commentaires

Produits connexes

- Réseau local sans fil (WLAN)

Contenu

Introduction

Ce document fournit un exemple de configuration pour limiter l'accès de par-utilisateur à un RÉSEAU LOCAL Sans fil (WLAN) basé sur l'Identifiant SSID (Service Set Identifier).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le contrôleur LAN Sans fil (WLC) et le point d'accès léger (LAP) pour le fonctionnement de base
- Comment configurer le Cisco Secure Access Control Server (ACS)
- Point d'accès léger Protocol (LWAPP) et méthodes de sécurité sans fil

Composants utilisés

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

- Gamme Cisco 5500 WLC qui exécute la version 7.4.110 de micrologiciels
- RECOUVREMENT de gamme Cisco 1142
- Version 5.2.0.26.11 de serveur de Cisco Secure ACS

Configurez

Afin de configurer les périphériques pour cette installation, vous avez besoin :

1. Configurez le WLC pour les deux WLAN et serveurs de RAYON.
2. Configurez le Cisco Secure ACS.
3. Configurez les clients sans fil et vérifiez la configuration.

Configurez le WLC

Complétez ces étapes afin de définir le WLC pour cette configuration :

1. Configurez le WLC afin d'expédier les identifiants utilisateurs à un serveur RADIUS externe. Le serveur RADIUS externe (Cisco Secure ACS dans ce cas) alors valide les identifiants utilisateurs et permet d'accéder aux clients sans fil. Procédez comme suit : **Security > RADIUS Authentication** choisi du GUI de contrôleur afin d'afficher la page de serveurs d'authentification RADIUS.Cliquez sur New afin de définir les paramètres de serveur de RAYON.Ces paramètres incluent l'adresse IP du serveur RADIUS, secret partagé, numéro de port et état du serveur. Les cases à cocher d'utilisateur du réseau et de Gestion déterminent si l'authentification basée sur rayon s'applique pour la Gestion et les utilisateurs du réseau. Cet exemple utilise le Cisco Secure ACS en tant que serveur de RAYON avec l'adresse IP 10.104.208.56.Cliquez sur **Apply**.
2. Terminez-vous ces étapes afin de configurer un WLAN pour l'employé avec l'**employé** SSID et l'autre WLAN pour des sous-traitants avec le **sous-traitant** SSID. 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.Cliquez sur **New** pour configurer un nouveau WLAN.Cet exemple crée Employee nommé par WLAN et l'ID de WLAN est 1. cliquent sur Apply.Sélectionnez la fenêtre de **WLAN > Edit** et définissez les paramètres spécifiques au WLAN : De l'onglet Sécurité de la couche 2, **802.1x** choisi. Par défaut, l'option de degré de sécurité de la couche 2 est 802.1x. Ceci active 802.1 authentifications de Protocol d'authentification x/Extensible (EAP) pour le WLAN.De l'AAA les serveurs tabulent, sélectionnent le serveur compétent de RAYON de la liste

déroulante sous des serveurs de RAYON. Les autres paramètres peuvent être modifiés sur les conditions requises du réseau WLAN. Cliquez sur **Apply**.De même, afin de créer un WLAN pour des sous-traitants, répétez les étapes b à D.

Configurez le Cisco Secure ACS

Sur le serveur de Cisco Secure ACS vous avez besoin :

1. Configurez le WLC en tant que client d'AAA.
2. Créez la base de données utilisateur (qualifications) pour l'authentification basée sur SSID.
3. Authentification EAP d'enable.

Terminez-vous ces étapes sur le Cisco Secure ACS :

1. Afin de définir le contrôleur en tant que client d'AAA sur le serveur ACS, les **ressources de réseau** choisies **> les périphériques de réseau et les clients d'AAA du** GUI ACS. Sous des périphériques de réseau et des clients d'AAA**, le** clic **créent.**
2. Quand la page de configuration réseau paraît, définissez le nom du WLC, de l'adresse IP, et du secret et de la méthode d'authentification partagés (RAYON).
3. **Les utilisateurs** choisis **et l'identité enregistre > des groupes d'identité du** GUI ACS. Créez les groupes respectifs pour l'employé et le sous-traitant et le clic **créent**. Dans cet exemple le groupe créé est nommé Employees.
4. **Les utilisateurs** choisis **et l'identité enregistre > les mémoires internes d'identité**. Cliquez sur **créent** et écrivent le nom d'utilisateur. Placez-les dans le groupe correct, définissez leur mot de passe, et cliquez sur Submit. Dans cet exemple un utilisateur nommé employee1 dans l'employé de groupe est créé. De même, créez un utilisateur nommé contractor1 sous les sous-traitants de groupe.
5. **Filtres de station éléments de stratégie > d'états > d'extrémité** choisis de **réseau**. Cliquez sur **Create**.Écrivez un nom signicatif et sous l'onglet d'**adresse IP** écrivez l'adresse IP du WLC. Dans cet exemple les noms sont employé et sous-traitant.Sous l'onglet CLI/DNIS, laissez le CLI comme - et écrivez DNIS comme *<SSID>. Dans cet exemple, le champ DNIS est entré comme *Employee comme ce filtre de station d'extrémité est utilisé pour limiter l'accès seulement à l'employé WLAN. L'attribut DNIS définit le SSID qu'on permet à l'l'utilisateur pour accéder à. Le WLC envoie le SSID dans l'attribut DNIS au serveur de RAYON.Répétez les mêmes étapes pour le filtre de station d'extrémité de sous-traitant.
6. **Éléments de stratégie > autorisation et autorisations > profils** choisis d'**accès au réseau > d'autorisation**. Il devrait y a un profil par défaut pour l'autorisation Access.
7. Sélectionnez les **stratégies d'Access > les services d'accès > les règles de sélection de service**. Le clic **personnalisent**. Ajoutez n'importe quel état approprié. Cet exemple utilise Protocol comme rayon comme condition assortie.Cliquez sur **Create**. Nommez la règle. **Protocol** choisi et **rayon** choisi**.**Sous des **résultats**, choisissez le service d'accès compétent. Dans cet exemple, il est laissé en tant qu'**accès au réseau par défaut.**
8. **Stratégies d'Access > services d'accès > accès au réseau > identité** choisis de **par défaut**. Choisissez la sélection de résultat et la **source** simples d'**identité** comme utilisateurs internes.**Stratégies d'Access > services d'accès > accès au réseau > autorisation** choisis de **par défaut.** Cliquez sur **personnalisent** et ajoutent les conditions personnalisées. Cet exemple utilise le groupe d'identité, NDG : Type de périphérique, et filtre de station d'extrémité dans cette commande.Cliquez sur **Create**. Nommez la règle et choisissez le groupe approprié d'identité sous tous les groupes. Dans cet exemple c'est employé.Cliquez

sur la case d'option de **filtre de Stn de fin des employés** ou écrivez le nom que vous entrez dans Step1b dans la section « configurez WLC ».Cochez la case d'**Access d'autorisation**.Répétez les mêmes étapes ci-dessus pour des règles de sous-traitant aussi bien. Assurez que l'action par défaut est **de refuser Access**.Une fois que vous vous êtes terminé l'étape e, vos règles devraient ressembler à cet exemple :

Ceci conclut la configuration. Après que cette section, le client doive être configurée en conséquence avec les paramètres SSID et de Sécurité afin de se connecter.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Mis à jour : Janv. 14, 2015
ID de document : 118661