Contenu

Introduction

Services Access Registrar (AR) de Cisco Networking Light Extensible Authentication Protocol de 3.0 supports (LEAP) (radio d'Eap-Cisco). Ce document affiche comment configurer des Aironet Client Utility Sans fil et Cisco Aironet 340, 350, ou des Points d'accès de gamme 1200 (aps) pour l'authentification de LEAP à Cisco AR.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique 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 :

- Cisco Aironet® 340, 350, ou Points d'accès de gamme 1200
- Microprogramme d'AP 11.21 ou plus tard pour le LEAP de Cisco
- Cartes d'interface réseau de gamme 340 ou 350 de Cisco Aironet (NIC)
- Versions 4.25.30 ou ultérieures de micrologiciels pour le LEAP de Cisco
- Spécification NDIS (NDIS) 8.2.3 ou plus tard pour le LEAP de Cisco
- Versions 5.02 ou ultérieures des Aironet Client Utility (ACU)
- Le Cisco Access Registrar 3.0 ou plus tard est exigé pour fonctionner et authentifier Cisco des demandes SAUTEZ et d'authentification MAC

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurant la radio d'Eap-Cisco (LEAP de Cisco)

Cette section couvre les configurations de base du LEAP de Cisco sur le serveur de Cisco AR, l'AP, et de divers clients.

Instructions pas à pas

Suivez ces instructions de configurer le LEAP :

1. Changez le port sur le serveur de Cisco AR.AP envoie les informations de RAYON sur les ports de Protocole UDP (User Datagram Protocol) 1812 (authentification) et 1813 (comptabilité). Puisque Cisco AR écoute sur les ports UDP 1645 et 1646 par défaut, vous devez configurer Cisco AR pour écouter sur les ports UDP 1812 et 1813.Émettez la commande de **/radius/advanced/ports de cd**.Émettez la commande de l'**ajouter 1812** d'ajouter le port 1812.Si vous prévoyez de faire la comptabilité, émettez la commande de l'**ajouter 1813** d'ajouter le port 1813.Sauvegardez la configuration, et puis redémarrez les services.
2. Pour ajouter AP au serveur de Cisco AR, émettez ces commandes :**cd /Radius/Clientsajoutez ap350-1cd ap350-1placez l'IP address 171.69.89.1placez le sharedsecret Cisco**
3. Pour configurer le délai d'attente de session de clé de Confidentialité équivalente aux transmissions par fil (WEP), émettez ces commandes :**Remarque:** le 802.1x spécifie une option de réauthentification. Cisco SAUTENT l'algorithme utilise cette option d'expirer la clé de session du courant WEP pour l'utilisateur et d'émettre une nouvelle clé de session WEP.**cd /Radius/Profilesajoutez l'AP-profilAP-profil de cdattributs de cdplacez la session-timeout 600**
4. Pour créer un groupe d'utilisateurs qui utilise les profils a ajouté dans l'étape 3, émettent ces commandes :**cd /Radius/Usergroupsajoutez l'AP-groupeAP-groupe de cdplacez l'AP-profil baseprofile**Les utilisateurs à ce groupe d'utilisateurs héritent du profil et reçoivent à leur tour le délai d'attente de session.
5. Pour créer des utilisateurs dans une liste des utilisateurs et ajouter les utilisateurs au groupe d'utilisateurs défini dans l'étape 4, émettez ces commandes :**cd /Radius/Userlistsajoutez les AP-utilisateursAP-utilisateurs de cdajoutez user1cd user1set password CiscoAP-groupe de set group**
6. Pour créer un service d'authentification locale et d'autorisation pour utiliser UserService « AP-userservice » et pour placer le type de service « eap-LEAP », émettez ces commandes :**cd /Radius/Servicesajoutez AP-localservicecd AP-localserviceeap-LEAP de set typeplacez UserService AP-userservice**
7. Pour créer un utilisateur entretenez « AP-userservice » pour utiliser la liste des utilisateurs

définie dans l'étape 5, émettent ces commandes :**cd /Radius/Servicesajoutez AP-userservicecd AP-localservicegens du pays de set typeplacez les AP-utilisateurs d'userlist**
8. Pour placer l'authentification par défaut et l'autorisation entretenez que les utilisations de Cisco AR au service défini dans l'étape 6, émettent ces commandes :**cd /radiusplacez le defaultauthenticationservice AP-localserviceplacez le defaultauthorizationservice AP-localservice**
9. Pour sauvegarder et recharger la configuration, émettez ces commandes :**sauvegardezrecharge**

Activation d'Eap-Cisco (LEAP de Cisco) sur AP

Instructions pas à pas

Suivez ces étapes pour activer Cisco SAUTENT sur AP :

1. Parcourez à AP.
2. De la page d'état récapitulatif, **INSTALLATION de** clic.
3. Dans le menu services, cliquez sur Security **> serveur d'authentification**.
4. Sélectionnez la version du 802.1x pour s'exécuter sur cet AP dans le menu déroulant de version de Protocol de 802.1x.
5. Configurez l'adresse IP de Cisco AR dans la zone de texte du serveur Name/IP.
6. Vérifiez le menu déroulant de type de serveur est placé au **RAYON**.
7. Changez la zone de texte de port à **1812**. C'est le numéro de port correct IP à l'utiliser avec Cisco AR.
8. Configurez la zone de texte secrète partagée avec la valeur utilisée sur Cisco AR.
9. Sélectionnez la case d'**authentification EAP**.
10. Modifiez la zone de texte de délai d'attente si ainsi désiré. C'est la valeur du dépassement de durée pour une demande d'authentification pour Cisco AR.
11. Cliquez sur OK pour retourner à l'écran de configuration de la sécurité.Si vous faites également la comptabilité de RAYON, vérifiez que le port à la page d'installation de comptabilité est conforme au port configuré à Cisco AR (placent pour 1813).
12. **Chiffrement de données par radio de** clic **(WEP)**.
13. Configurez une clé WEP d'émission en tapant dans un 40- ou la valeur 128-bit principale dans la zone de texte de la clé WEP 1.
14. Sélectionnez les types d'authentification pour l'utiliser. Assurez-vous que, au minimum, la case de **Network-EAP** est sélectionnée.
15. Vérifiez l'utilisation du menu déroulant de chiffrement de données est placé à **facultatif** ou au **chiffrement complet**. Facultatif permet l'utilisation des clients non-WEP et WEP sur même AP. Rendez-vous compte que c'est un mode de fonctionnement non sécurisé. Chiffrement complet d'utilisation si possible.
16. Cliquez sur OK pour terminer.

Configurer ACU 6.00

Instructions pas à pas

Suivez ces étapes pour configurer l'ACU :

1. Ouvrez l'ACU.
2. **Gestionnaire de profil de** clic sur la barre d'outils.
3. Cliquez sur Add pour créer un nouveau profil.
4. Écrivez le nom de profil dans la zone de texte, et puis cliquez sur OK.
5. Entrez dans l'Identifiant SSID (Service Set Identifier) approprié dans la zone de texte SSID1.
6. **Sécurité des réseaux de** clic.
7. **LEAP** choisi du menu déroulant de type de sécurité des réseaux.
8. Cliquez sur **Configure**.
9. Configurez les paramètres du mot de passe comme nécessaires.
10. Cliquez sur **OK**.
11. Cliquez sur OK sur l'écran de sécurité des réseaux.

Suivis de Cisco AR

Émettez le **suivi /r 5** pour obtenir des informations de suivi sur Cisco AR. Si vous avez besoin d'AP mettez au point, vous pouvez se connecter à AP par l'intermédiaire du telnet et émettre les commandes **eap_diag1_on** et **eap_diag2_on**.

Informations connexes

- Page de support de Cisco Access Registrar
- Support et documentation techniques - Cisco Systems