Configuration Cisco Access Registrar et LEAP

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 :**Note**: 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**.

```
06/28/2004 16:31:49: P1121: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1121: Checking Message-Authenticator
06/28/2004 16:31:49: P1121: Trace of Access-Request packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 146
06/28/2004 16:31:49: P1121:
   reqauth = e5:4f:91:27:0a:91:82:6b:a4:81:c1:cc:c8:11:86:0b
06/28/2004 16:31:49: P1121: User-Name = user1
06/28/2004 16:31:49: P1121: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1121: NAS-Port = 37
06/28/2004 16:31:49: P1121: Service-Type = Login
06/28/2004 16:31:49: P1121: Framed-MTU = 1400
06/28/2004 16:31:49: P1121: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1121: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1121: NAS-Identifier = frinket
06/28/2004 16:31:49: P1121: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1121: EAP-Message = 02:02:00:0a:01:75:73:65:72:31
06/28/2004 16:31:49: P1121:
   Message-Authenticator = f8:44:b9:3b:0f:33:34:a6:ed:7f:46:2d:83:62:40:30
06/28/2004 16:31:49: P1121: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1121: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1121: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1121: Authenticating and Authorizing with
   Service ap-localservice
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1121: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1121: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 61
06/28/2004 16:31:49: P1121:
```

```
   reqauth = 60:ae:19:8d:41:5e:a8:dc:4c:25:1b:8d:49:a3:47:c4
06/28/2004 16:31:49: P1121: EAP-Message =
   01:02:00:15:11:01:00:08:66:27:c3:47:d6:be:b3:67:75:73:65:72:31
06/28/2004 16:31:49: P1121: Message-Authenticator =
   59:d2:bc:ec:8d:85:36:0b:3a:98:b4:90:cc:af:16:2f
06/28/2004 16:31:49: P1121: Sending response to 10.48.86.230
06/28/2004 16:31:49: P1123: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1123: Checking Message-Authenticator
06/28/2004 16:31:49: P1123: Trace of Access-Request packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 173
06/28/2004 16:31:49: P1123:
   reqauth = ab:f1:0f:2d:ab:6e:b7:49:9e:9e:99:00:28:0f:08:80
06/28/2004 16:31:49: P1123: User-Name = user1
06/28/2004 16:31:49: P1123: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1123: NAS-Port = 37
06/28/2004 16:31:49: P1123: Service-Type = Login
06/28/2004 16:31:49: P1123: Framed-MTU = 1400
06/28/2004 16:31:49: P1123: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1123: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1123: NAS-Identifier = frinket
06/28/2004 16:31:49: P1123: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1123: EAP-Message =
   02:02:00:25:11:01:00:18:5e:26:d6:ab:3f:56:f7:db:21:96:f3:b0:fb:ec:6b:
   a7:58:6f:af:2c:60:f1:e3:3c:75:73:65:72:31
06/28/2004 16:31:49: P1123: Message-Authenticator =
   21:da:35:89:30:1e:e1:d6:18:0a:4f:3b:96:f4:f8:eb
06/28/2004 16:31:49: P1123: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1123: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1123: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1123: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1123: Calling external service ap-userservice
   for authentication and authorization
06/28/2004 16:31:49: P1123: Getting User user1's UserRecord
   from UserList ap-users
06/28/2004 16:31:49: P1123: User user1's MS-CHAP password matches
06/28/2004 16:31:49: P1123: Processing UserGroup ap-group's check items
06/28/2004 16:31:49: P1123: User user1 is part of UserGroup ap-group
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's BaseProfiles
   into response dictionary
06/28/2004 16:31:49: P1123: Merging BaseProfile ap-profile
   into response dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's Attributes
   into response Dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Removing all attributes except for
   EAP-Message from response - they will be sent back in the Access-Accept
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1123: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1123: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 44
06/28/2004 16:31:49: P1123:
   reqauth = 28:2e:a3:27:c6:44:9e:13:8d:b3:60:01:7f:da:8b:62
06/28/2004 16:31:49: P1123: EAP-Message = 03:02:00:04
06/28/2004 16:31:49: P1123: Message-Authenticator =
   2d:63:6a:12:fd:91:9e:7d:71:9d:8b:40:04:56:2e:90
06/28/2004 16:31:49: P1123: Sending response to 10.48.86.230
```

```
06/28/2004 16:31:49: P1125: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1125: Checking Message-Authenticator
06/28/2004 16:31:49: P1125: Trace of Access-Request packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 157
06/28/2004 16:31:49: P1125:
   reqauth = 72:94:8c:34:4c:4a:ed:27:98:ba:71:33:88:0d:8a:f4
06/28/2004 16:31:49: P1125: User-Name = user1
06/28/2004 16:31:49: P1125: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1125: NAS-Port = 37
06/28/2004 16:31:49: P1125: Service-Type = Login
06/28/2004 16:31:49: P1125: Framed-MTU = 1400
06/28/2004 16:31:49: P1125: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1125: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1125: NAS-Identifier = frinket
06/28/2004 16:31:49: P1125: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1125: EAP-Message =
   01:02:00:15:11:01:00:08:3e:b9:91:18:a8:dd:98:ee:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
   8e:73:2b:a6:54:c6:f5:d9:ed:6d:f0:ce:bd:4f:f1:d6
06/28/2004 16:31:49: P1125: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1125: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1125: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1125: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1125: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1125: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1125: Restoring all attributes to response
   that were removed in the last Access-Challenge
06/28/2004 16:31:49: P1125: No default Remote Session Service defined.
06/28/2004 16:31:49: P1125: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1125: Trace of Access-Accept packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 142
06/28/2004 16:31:49: P1125:
   reqauth = 71:f1:ef:b4:e6:e0:c2:4b:0a:d0:95:47:35:3d:a5:84
06/28/2004 16:31:49: P1125: Session-Timeout = 600
06/28/2004 16:31:49: P1125: EAP-Message =
02:02:00:25:11:01:00:18:86:5c:78:3d:82:f7:69:c7:96:70:35:31:bb:51:a7:ba:f8:48:8c:
45:66:00:e8:3c:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
7b:48:c3:17:53:67:44:f3:af:5e:17:27:3d:3d:23:5f
06/28/2004 16:31:49: P1125: Cisco-AVPair =
6c:65:61:70:3a:73:65:73:73:69:6f:6e:2d:6b:65:79:3d:04:f2:c5:2a:de:fb:4e:1e:8a:8d
:b8:1b:e9:2c:f9:9a:3e:83:55:ff:ae:54:57:4b:60:e1:03:05:fd:22:95:4c:b4:62
06/28/2004 16:31:49: P1125: Sending response to 10.48.86.230
```

Informations connexes

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