NPS, contrôleurs LAN Sans fil, et exemple de configuration réseau de réseaux sans fil

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour le Protected Extensible Authentication Protocol (PEAP) en authentification de version 2 de la Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) dans un réseau de Cisco Unified Wireless en policy server de réseau Microsoft (NPS) en tant que serveur de RAYON.

Conditions préalables

Conditions requises

Assurez-vous que vous êtes au courant de ces procédures avant que vous tentiez cette configuration :

- La connaissance de l'installation de base de Windows 2008
- La connaissance de l'installation de contrôleur de Cisco

Assurez-vous que ces exigences ont été répondues avant que vous tentiez cette configuration :

- Installez le système d'exploitation de la Microsoft Windows Server 2008 sur chacun des serveurs dans le laboratoire de test.
- Mettez à jour tous les packs de services.
- Installez les contrôleurs et le Point d'accès léger (recouvrements).
- Configurez les dernières mises à jour logicielles.

Pour l'installation initiale et les informations de configuration pour les contrôleurs Sans fil de gamme Cisco 5508, référez-vous au guide d'installation Sans fil de contrôleur de gamme Cisco 5500.

Remarque: Ce document est destiné pour donner aux lecteurs un exemple sur la configuration exigée sur un serveur de Microsoft pour l'authentification PEAP-MS-CHAP. La configuration du serveur de Microsoft Windows présentée dans ce document a été testée dans le laboratoire et avérée pour fonctionner comme prévue. Si vous avez des ennuis avec la configuration, contactez Microsoft pour l'aide. Le centre d'assistance technique Cisco (TAC) ne prend en charge pas la configuration du serveur de Microsoft Windows.

Microsoft Windows 2008 guides d'installation et de configuration peut être trouvé sur le net de tech de Microsoft.

Composants utilisés

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

- Contrôleur sans-fil Cisco 5508 qui exécute la version 7.4 de micrologiciels
- Cisco Aironet 3602 Points d'accès (AP) avec le point d'accès léger Protocol (LWAPP)
- Windows 2008 Enterprise Server avec NPS, Autorité de certification (CA), Dynamic Host Control Protocol (DHCP), et services de Système de noms de domaine (DNS) installés
- PC client de Microsoft Windows 7
- Commutateur de gamme Cisco Catalyst 3560

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.

Présentation de PEAP

Les utilisations PEAP transportent la Sécurité de niveau (TLS) pour créer un canal chiffré entre un client authentifiant PEAP, tel qu'un ordinateur portable sans fil, et un authentificateur PEAP, tel que Microsoft NPS ou n'importe quel serveur de RAYON. Le PEAP ne spécifie pas une méthode

d'authentification, mais fournit la Sécurité supplémentaire pour d'autres protocoles d'authentification extensible (eap), comme EAP-MS-CHAP v2, qui peut fonctionner par le canal Tls-chiffré fourni par PEAP. La procédure d'authentification PEAP se compose de deux phases principales.

Première phase PEAP : La Manche Tls-chiffrée

Les associés de client sans fil avec AP. Une association d'IEEE 802.11-based fournit un système ouvert ou une authentification principale partagée avant qu'une association sécurisée soit créée entre le client et le Point d'accès. Après que l'association d'IEEE 802.11-based soit avec succès établie entre le client et le Point d'accès, la session de TLS est étée en pourparlers avec AP. Après l'authentification est avec succès terminée entre le client sans fil et le NPS, la session de TLS est négociée entre le client et le NPS. La clé qui dérive de cette négociation est utilisée pour crypter toute la communication ultérieure.

Deuxième phase PEAP : communication authentifiée d'EAP

La communication d'EAP, qui inclut la négociation d'EAP, se produit à l'intérieur du canal de TLS créé par PEAP dans la première phase du processus d'authentification de PEAP. Le NPS authentifie le client sans fil avec EAP-MS-CHAP v2. Le RECOUVREMENT et les messages en avant de contrôleur seulement entre le client sans fil et le serveur de RAYON. Le contrôleur LAN Sans fil (WLC) et le RECOUVREMENT ne peuvent pas déchiffrer ces messages parce que ce n'est pas le point final de TLS.

L'ordre de message de RAYON pour une tentative réussie d'authentification (où l'utilisateur a fourni les qualifications basées sur mot de passe valides avec PEAP-MS-CHAP v2) est :

1. Le NPS envoie un message de demande d'identité au client : Requête EAP/Identité.
2. Le client répond avec un message de réponse d'identité : Réponse EAP/Identité.
3. Le NPS envoie un message de défi MS-CHAP v2 : Requête-EAP/Type-EAP=EAP MS-CHAP-V2 (défi).
4. Le client répond avec un défi et la réponse MS-CHAP v2 : Réponse-EAP/Type-EAP=EAP-MS-CHAP-V2 (réponse).
5. Le NPS renvoie un paquet de succès MS-CHAP v2 quand le serveur a avec succès authentifié le client : Requête-EAP/Type-EAP=EAP-MS-CHAP-V2 (réussite).
6. Le client de routage répond avec un paquet de réussite MS-CHAP v2 quand le client a authentifié le serveur avec succès : Réponse-EAP/Type-EAP=EAP-MS-CHAP-V2 (réussite).
7. Le NPS envoie une Eap-type-longueur-valeur (TLV) qui indique l'authentification réussie.
8. Le client répond avec un message de réussite d'état EAP-TLV.
9. Le serveur se termine l'authentification et envoie un message d'Eap-succès en texte brut. Si des VLAN sont déployés pour l'isolation du client, les attributs VLAN sont inclus dans ce message.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer PEAP-MS-CHAP v2.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus

d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Cette configuration utilise cette configuration réseau :

Dans cette installation, un serveur de Microsoft Windows 2008 exécute ces rôles :

- Contrôleur de domaine pour le domaine wireless.com
- Serveur DHCP/DNS
- Serveur CA
- NPS ? pour authentifier les utilisateurs de sans fil
- Répertoire actif ? pour mettre à jour la base de données utilisateur

Le serveur se connecte au réseau câblé par un commutateur de la couche 2 comme affiché. Les WLC et le RECOUVREMENT enregistré se connectent également au réseau par le commutateur de la couche 2.

Les clients sans fil emploient l'accès protégé par Wi-Fi 2 (WPA2) - authentification PEAP-MS-CHAP v2 pour se connecter au réseau Sans fil.

Configurations

L'objectif de cet exemple est de configurer le serveur de Microsoft 2008, le contrôleur LAN Sans fil, et le poids léger AP pour authentifier les clients sans fil avec l'authentification PEAP-MS-CHAP v2. Il y a trois étapes principales dans ce processus :

1. Configurez le serveur de Microsoft Windows 2008.
2. Configurez le WLC et le poids léger aps.
3. Configurez les clients sans fil.

Configurez le serveur de Microsoft Windows 2008

Dans cet exemple, une configuration complète du serveur de Microsoft Windows 2008 inclut ces étapes :

1. Configurez le serveur comme contrôleur de domaine.
2. Installez et configurez les services DHCP.
3. installez et configurez le serveur en tant que serveur CA.
4. Connectez les clients au domaine.
5. Installez le NPS.
6. Installez un certificat.
7. Configurez le NPS pour l'authentification PEAP.
8. Ajoutez les utilisateurs au Répertoire actif.

Configurez le serveur de Microsoft Windows 2008 comme contrôleur de domaine

Terminez-vous ces étapes afin de configurer le serveur de Microsoft Windows 2008 comme

contrôleur de domaine :

1. **Début de** clic > **gestionnaire du serveur**.

2. **Les rôles de** clic > **ajoutent des rôles**.

3. Cliquez sur **Next** (Suivant).

4. Sélectionnez les **services de domaine de Répertoire actif de** service, et cliquez sur Next.

5. Passez en revue l'introduction aux services de domaine de Répertoire actif, et cliquez sur Next.

6. Le clic **installent** pour commencer le processus d'installation.

   L'installation poursuit et se termine.

7. Cliquez sur **étroitement cet assistant et lancez l'assistant d'installation de services de domaine de Répertoire actif (dcpromo.exe)** pour continuer l'installation et la configuration du Répertoire actif.

8. Le clic **à côté de** exécutent l'assistant d'installation de services de domaine de Répertoire actif.

9. Examinez les informations sur Compatbilty du système d'exploitation, et cliquez sur Next.

10. Le clic **créent un nouveau domaine dans une nouvelle forêt > ensuite** afin de créer un nouveau domaine.

11. Écrivez le plein nom DNS pour le nouveau domaine (wireless.com **dans** cet exemple), et cliquez sur Next**.**

12. Sélectionnez le niveau fonctionnel de forêt pour votre domaine, et cliquez sur Next.

13. Sélectionnez le niveau fonctionnel de domaine pour votre domaine, et cliquez sur Next.

14. Assurez que le serveur DNS est sélectionné, et cliquez sur Next.

15. Cliquez sur **oui** pour que l'assistant d'installation crée une nouvelle zone dans des DN pour le domaine.

16. Sélectionnez les répertoires que le Répertoire actif devrait l'utiliser pour ses fichiers, et cliquez sur Next.

17. Entrez le mot de passe administrateur, et cliquez sur Next.

18. Passez en revue vos sélections, et cliquez sur Next.

    Le montant d'installation.

19. Cliquez sur Finish **pour fermer l'assistant.**

20. Redémarrez le serveur pour que les modifications prennent effet.

Installez et configurez les services DHCP sur le serveur de Microsoft Windows 2008

Le service DHCP sur le serveur de Microsoft 2008 est utilisé pour fournir des adresses IP aux

clients sans fil. Terminez-vous ces étapes afin d'installer et configurer des services DHCP :

1. **Début de** clic > **gestionnaire du serveur**.

2. **Les rôles de** clic > **ajoutent des rôles**.

3. Cliquez sur **Next** (Suivant).

4. Sélectionnez le **serveur de** service dhcp, et cliquez sur Next.

5. Passez en revue l'introduction au serveur DHCP, et cliquez sur Next.

6. Sélectionnez l'interface que le serveur DHCP devrait surveiller pour des demandes, et cliquez sur Next.

7. Configurez les configurations par défaut de DN que le serveur DHCP devrait fournir aux clients, et cliquez sur Next.

8. Configurez les WINS si les supports réseau GAGNE.

9. Cliquez sur Add **pour utiliser l'assistant pour créer une portée de DHCP ou le clic à côté de** créent une portée de DHCP plus tard. Cliquez sur **Next** pour continuer.

10. Le support d'enable ou de débronchement DHCPv6 sur le serveur, et cliquent sur Next.

11. Configurez les configurations de DN d'IPv6 si DHCPv6 était activé dans l'étape précédente. Cliquez sur **Next** pour continuer.

12. Fournissez les qualifications d'administrateur de domaine pour autoriser le serveur DHCP dans le Répertoire actif, et cliquez sur Next.

13. Passez en revue la configuration à la page de confirmation, et le clic **installent** pour se terminer l'installer.

    Le montant d'installation.

14. Le clic **près de** ferment l'assistant.

    Le serveur DHCP est maintenant installé.

15. Cliquez sur le **début** > les **outils d'administration** > le **DHCP** pour configurer le service DHCP.

16. Développez le serveur DHCP (win-mvz9z2umms.wireless.com dans cet exemple), cliquez avec le bouton droit l'ipv4, et choisissez la **nouvelle portée**. pour créer une portée de DHCP.

17. Le clic **à côté de** configurent la nouvelle portée par l'intermédiaire du nouvel assistant de portée.

18. Fournissez un nom pour la nouvelle portée (clients sans fil dans cet exemple), et cliquez sur Next.

19. Écrivez la plage des adresses IP disponibles qui peuvent être utilisées pour des baux DHCP. Cliquez sur **Next** pour continuer.

20. Créez une liste facultative d'adresses exclues. Cliquez sur **Next** pour continuer.

21. Configurez la durée de bail, et cliquez sur Next.

22. Cliquez sur **oui, je veux configurer ces options maintenant**, et clique sur Next.

23. Écrivez l'adresse IP de la passerelle par défaut pour cette portée, cliquez sur Add **> ensuite**.

24. Configurez les DN nom de domaine et serveur DNS à utiliser par les clients. Cliquez sur **Next** pour continuer.

25. Écrivez les informations de WINS pour cette portée si les supports réseau GAGNE. Cliquez sur **Next** pour continuer.

26. Pour lancer cette portée, cliquez sur **oui, je veulent lancer cette portée maintenant > ensuite**.

27. Cliquez sur Finish pour se terminer et fermer l'assistant.

Installez et configurez le serveur de Microsoft Windows 2008 en tant que serveur CA

Le PEAP avec EAP-MS-CHAP v2 valide le serveur de RAYON basé sur le certificat actuel sur le serveur. Supplémentaire, le certificat de serveur doit être délivré par un public CA qui est de confiance par l'ordinateur client (c'est-à-dire, le certificat de CA public existe déjà dans le répertoire d'Autorité de certification racine approuvée sur la mémoire de certificat d'ordinateur client).

Terminez-vous ces étapes afin de configurer le serveur de Microsoft Windows 2008 en tant que serveur CA qui fournit le certificat au NPS :

1. **Début de** clic **> gestionnaire du serveur**.

2. **Les rôles de** clic **> ajoutent des rôles**.

3. Cliquez sur **Next** (Suivant).

4. Sélectionnez les **services de certificat de Répertoire actif de** service, et cliquez sur Next.

5. Passez en revue l'introduction aux services de certificat de Répertoire actif, et cliquez sur Next.

6. Sélectionnez l'**autorité de certification**, et cliquez sur Next.

7. **L'entreprise** choisie, et cliquent sur Next.

8. **La racine** choisie **CA**, et cliquent sur Next.

9. Choisi **créez une nouvelle clé privée**, et cliquez sur Next.

10. Cliquez sur Next sur configurer le chiffrement pour le CA.

11. Le clic **à côté de** reçoivent le nom commun par défaut pour ce CA.

12. Sélectionnez la durée que ce certificat de CA est valide, et cliquez sur Next.

13. Le clic **à côté de** reçoivent l'emplacement par défaut de base de données de certificat.

14. Passez en revue la configuration, et le clic **installent** pour commencer les services de

certificat de Répertoire actif.

15. Après que l'installer soit terminé, **fin de** clic.

Connectez les clients de routage au domaine de routage

Terminez-vous ces étapes afin de connecter les clients au réseau câblé et télécharger les informations spécifiques de domaine du nouveau domaine :

1. Connectez les clients au réseau câblé avec une droite par un câble Ethernet.
2. Initialisez le client, et la procédure de connexion avec le nom d'utilisateur et mot de passe de client.
3. Cliquez sur le **Start > Run**, écrivez le **cmd**, et cliquez sur OK.
4. À l'invite de commande, écrivez l'**ipconfig**, et le clic **entrent** pour vérifier que le DHCP fonctionne correctement et que le client a reçu une adresse IP du serveur DHCP.
5. Afin de joindre le client au domaine, au **début de** clic, **ordinateur de** clic droit, choisir Properties, et choisir des **configurations de modification au** en bas à droite.
6. Cliquez sur **Change**.
7. Cliquez sur le **domaine**, entrez dans **wireless.com**, et cliquez sur OK.

8. Écrivez l'**administrateur de** nom d'utilisateur et la particularité de mot de passe au domaine auquel le client se joint. C'est le compte administrateur dans le Répertoire actif sur le serveur.

9. Cliquez sur OK, et cliquez sur OK de nouveau.

10. Clic **étroit > reprise maintenant** pour redémarrer l'ordinateur.
11. Une fois que l'ordinateur a redémarré, connectez-vous avec les informations suivantes : Nom d'utilisateur = **Administrateur** ; Mot de passe = **<mot de passe**domaine>; Domaine = radio.
12. Cliquez sur le **début**, cliquez avec le bouton droit l'**ordinateur**, choisissez Properties, et choisissez les **configurations de modification au** en bas à droite pour vérifier que vous êtes sur le domaine de wireless.com.
13. L'étape suivante consiste à vérifier que le client a reçu le certificat d'authentification (de confiance) du serveur.

14. Cliquez sur le **début**, écrivez le **MMC**, et l'appuyez sur **entrent**.

15. Cliquez sur **File**, puis cliquez sur le jeu d'outils **Add/Remove**.
16. Choisissez les **Certificats**, et cliquez sur Add.

17. Cliquez sur le **compte d'ordinateur**, et cliquez sur Next.

18. Cliquez sur l'**ordinateur local**, et cliquez sur Next.

19. Cliquez sur **OK**.
20. Développez les répertoires de **Certificats (ordinateur local)** et d'**Autorités de certification racine approuvée**, et cliquez sur les **Certificats**. Trouvez le **CERT Sans fil du domaine CA** dans la liste. Dans cet exemple, le CERT CA s'appelle le wireless-WIN-MVZ9Z2UMNMS-CA.

21. Répétez cette procédure pour ajouter plus de clients au domaine.

Installez le serveur de politique réseau sur le serveur de Microsoft Windows 2008

Dans cette installation, le NPS est utilisé en tant que serveur de RAYON pour authentifier des clients sans fil avec l'authentification PEAP. Terminez-vous ces étapes afin d'installer et configurer NPS sur le serveur de Microsoft Windows 2008 :

1. **Début de** clic > **gestionnaire du serveur**.

2. **Les rôles de** clic > **ajoutent des rôles**.

3. Cliquez sur **Next** (Suivant).

4. Sélectionnez la **politique réseau et les services d'accès de** service, et cliquez sur Next.

5. Passez en revue l'introduction à la politique réseau et aux services d'accès, et cliquez sur Next.

6. **Le serveur** choisi de **politique réseau**, et cliquent sur Next.

7. Passez en revue la confirmation, et le clic **installent**.

   Après que l'installer soit terminé, un écran semblable à celui-ci est affiché.

8. Cliquez sur **Fermer**.

Installez un certificat

Terminez-vous ces étapes afin d'installer le certificat d'ordinateur pour le NPS :

1. Cliquez sur le **début**, écrivez le **MMC**, et l'appuyez sur **entrent**.
2. **Fichier > ajout/suppression de** clic SNAP-**dans**.
3. Choisissez les **Certificats**, et cliquez sur Add.

4. Choisissez **Computer account**, puis cliquez sur **Next**.

5. **L'ordinateur local** choisi, et cliquent sur Finish.

6. Cliquez sur OK pour retourner au Microsoft Management Console (MMC).

7. Développez les **Certificats (ordinateur local)** et les répertoires **personnels**, et cliquez sur les **Certificats**.

8. Cliquez avec le bouton droit dans le whitespace sous le certificat de CA, et choisissez **tous les tâches > certificat de demande nouveau**.

9. Cliquez sur **Next** (Suivant).

10. **Le contrôleur de domaine** choisi, et le clic **s'inscrivent**.

11. Cliquez sur Finish une fois que le certificat est installé.

    Le certificat NPS est maintenant installé.

12. Assurez-vous que le but visé du certificat lit l'**authentification client, authentification de serveur**.

Configurez le service de serveur de politique réseau pour l'authentification PEAP-MS-CHAP v2

Terminez-vous ces étapes afin de configurer le NPS pour l'authentification :

1. **Début de** clic **> outils d'administration > serveur de politique réseau**.
2. Cliquez avec le bouton droit **NPS (gens du pays)**, et choisissez le **serveur de registre dans le Répertoire actif**.

3. Cliquez sur **OK**.

4. Cliquez sur **OK**.

5. Ajoutez le contrôleur LAN Sans fil en tant que client d'Authentification, autorisation et comptabilité (AAA) sur le NPS.
6. Développez les **clients RADIUS et les serveurs**. Cliquez à droite sur **RADIUS Clients**, puis choisissez **New RADIUS Client**.

7. Écrivez un nom amical (WLC dans cet exemple), l'adresse IP de Gestion du WLC (192.168.162.248 dans cet exemple) et un secret partagé. Le même secret partagé est utilisé pour configurer le WLC.

8. Cliquez sur OK pour retourner à l'écran précédent.

9. Créez une nouvelle politique réseau pour des utilisateurs de sans fil. Développez les **stratégies**, cliquez avec le bouton droit les **politiques réseau**, et choisissez **nouveau**.

10. Écrivez un nom de stratégie pour cette règle (radio PEAP dans cet exemple), et cliquez sur Next.

11. Pour faire permettre cette stratégie seulement les utilisateurs Sans fil de domaine, ajoutez ces trois conditions, et cliquez sur Next :

    - Groupes de Windows - Utilisateurs de domaine
    - Type de port de NAS - Radio - IEEE 802.11
    - Type d'authentification - EAP

12. Cliquez sur **Autorisation d'accès** pour accorder les tentatives de connexion qui apparient cette stratégie, et cliquez sur Next.

13. Désactivez toutes les méthodes d'authentification sous moins des méthodes d'authentification sécurisées.

14. Cliquez sur Add, sélectionnez le PEAP, et cliquez sur OK **pour activer le PEAP.**

15. **Microsoft** choisi **: L'EAP protégé (PEAP)**, et cliquent sur Edit. Assurez que le certificat précédemment créé de contrôleur de domaine est sélectionné dans la liste déroulante émise par certificat, et cliquez sur l'**ok**.

16. Cliquez sur **Next** (Suivant).

17. Cliquez sur **Next** (Suivant).

18. Cliquez sur **Next** (Suivant).

19. Cliquez sur **Finish** (Terminer).

Ajoutez les utilisateurs à l'Active Directory

Dans cet exemple, la base de données utilisateur est mise à jour sur le Répertoire actif. Terminez-vous ces étapes afin d'ajouter des utilisateurs à la base de données de Répertoire actif :

1. Ouvrez les utilisateurs et les ordinateurs de Répertoire actif. **Début de** clic > **outils d'administration** > **utilisateurs et ordinateurs de Répertoire actif**.
2. Dans l'arborescence de la console d'utilisateurs et d'ordinateurs de Répertoire actif, développez le domaine, cliquez avec le bouton droit les **utilisateurs** > **nouveau**, et choisissez l'**utilisateur**.
3. Dans le nouvel objet ? La boîte de dialogue d'utilisateur, écrivent le nom de l'utilisateur de sans fil. Cet exemple utilise le nom Client1 dans le domaine de prénom et Client1 dans le nom de connexion d'utilisateur mettent en place. Cliquez sur **Next** (Suivant).

4. Dans le nouvel objet ? La boîte de dialogue d'utilisateur, entrent un mot de passe de votre choix dans les domaines de mot de passe et de confirmation du mot de passe. Décochez l'**utilisateur doit changer le mot de passe à la prochaine** case de **connexion**, et clique sur Next.

5. Dans le nouvel objet ? La boîte de dialogue d'utilisateur, cliquent sur Finish.

6. Répétez les étapes 2 à 4 afin de créer des comptes d'utilisateur supplémentaires.

Configurez le contrôleur LAN et les recouvrements Sans fil

Configurez les périphériques sans fil (les contrôleurs LAN et les recouvrements Sans fil) pour cette installation.

Configurez le WLC pour l'authentification de RAYON

Configurez le WLC pour utiliser le NPS en tant que serveur d'authentification. Le WLC doit être configuré afin d'expédier les identifiants utilisateurs à un serveur RADIUS externe. Le serveur RADIUS externe alors valide les identifiants utilisateurs et permet d'accéder aux clients sans fil.

Terminez-vous ces étapes afin d'ajouter le NPS en tant que serveur de RAYON dans la page de **Security > RADIUS Authentication** :

1. Choisissez le **Security > Radius > Authentication de l'**interface de contrôleur pour afficher la page de serveurs d'authentification RADIUS. Cliquez sur New afin de définir un serveur de RAYON.

2. Définissez 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 d'utilisateur du réseau et de Gestion déterminent si l'authentification basée sur rayon s'applique aux utilisateurs de Gestion et de réseau (radio). Cet exemple utilise le NPS en tant que serveur de RAYON avec une adresse IP de 192.168.162.12. Cliquez sur **Apply**.

Configurez un WLAN pour les clients de routage

Configurez l'ensemble de services identfier (SSID) (WLAN) auquel les clients sans fil se connecte. Dans cet exemple, créez le SSID, puis nommez-le **PEAP**.

Définissez l'authentification de la couche 2 comme WPA2 de sorte que les clients exécutent l'authentification basée sur eap (PEAP-MS-CHAP v2 dans cet exemple) et utilisent le Norme AES (Advanced Encryption Standard) comme mécanisme de chiffrement. Laissez toutes autres valeurs à leurs paramètres par défaut.

Remarque: Ce document relie le WLAN aux interfaces de gestion. Quand vous avez plusieurs VLAN dans votre réseau, vous pouvez créer un VLAN séparé et le relier au SSID. Pour les informations sur la façon de configurer des VLAN sur les WLC, reportez-vous aux VLAN sur l'exemple de configuration de contrôleurs LAN sans fil.

Terminez-vous ces étapes afin de configurer un WLAN sur le WLC :

1. Cliquez sur les **WLAN de l'**interface de contrôleur afin d'afficher la page WLAN. Cette page énumère les WLAN qui existent sur le contrôleur.
2. Sélectionnez **New** afin de créer un nouveau WLAN. Saisissez l'ID WLAN et le SSID WLAN pour le WLAN, puis cliquez sur **Apply**.

3. Pour configurer le SSID pour le 802.1x, terminez-vous ces étapes : Cliquez sur l'**onglet Général** et activez le WLAN.

   Cliquez sur les onglets de **Sécurité** > de **couche 2**, placez le degré de sécurité de la couche

2 à **WPA + WPA2**, vérifiez les boxesas de contrôle des paramètres WPA+WPA2 (par exemple, WPA2 AES) requis, et cliquez sur le **802.1x** en tant que gestion des clés d'authentification.

Cliquez sur les onglets de **Security > AAA Servers**, choisissez l'adresse IP du NPS de la liste déroulante du **serveur 1**, et cliquez sur Apply.

Configurez les clients sans fil pour l'authentification PEAP-MS-CHAP v2

Terminez-vous ces étapes pour configurer le client sans fil avec l'outil de config de Windows Zero pour se connecter au PEAP WLAN.

1. Cliquez sur l'**icône réseau** dans la barre des tâches. Cliquez sur le **PEAP** SSID, et le clic **se connectent**.

2. Le client devrait maintenant être connecté au réseau.

3. Si la connexion échoue, essayez de rebrancher au WLAN. Si la question persiste, référez-vous à la section de dépannage.

Vérifiez

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

Dépannez

Si votre client ne se connectait pas au WLAN, cette section fournit des informations que vous pouvez employer pour dépanner la configuration.

Il y a deux outils qui peuvent être utilisés pour diagnostiquer des échecs d'authentification de 802.1x : l'ordre de **client de débogage** et le **visualisateur d'événements** dans Windows.

En exécutant un client mettez au point du WLC n'est pas ressource intensive et ne fait pas service d'imnpact. Pour commencer une session de débogage, ouvrir l'interface de ligne de commande (CLI) du WLC, et entrer **mettez au point le** *MAC address de* **client**, où le MAC address est le MAC address Sans fil du client sans fil qui ne peut pas se connecter. Tandis que ceci mettent au point des passages, essayez de connecter le client ; là devrait être sorti sur le CLI du WLC ce des sembler semblables à cet exemple :

C'est un exemple d'une question qui pourrait se produire avec une mauvaise configuration. Ici, les WLC mettent au point des expositions que le WLC est entrées dans l'état authentifiant, qui signifie que le WLC attend une réponse du NPS. C'est habituellement dû à un secret partagé incorrect sur le WLC ou le NPS. Vous pouvez confirmer ceci par l'intermédiaire du visualisateur d'événements de Windows Server. Si vous ne trouvez pas un log, la demande ne l'a jamais fait au NPS.

Un autre exemple qui est trouvé du WLC mettent au point est une Access-anomalie. Une access-anomalie prouve que le NPS a reçu et a rejeté les qualifications de client. C'est un exemple d'un client recevant une Access-anomalie :

Quand vous voyez une Access-anomalie, vérifiez les logins les journaux d'événements de Windows Server pour déterminer pourquoi le NPS a répondu au client avec une Access-anomalie.

Une authentification réussie fait mettre au point un Access-recevoir dans le client, comme vu dans cet exemple :

Le dépannage des Access-anomalies et des temporisations de réponse exige l'accès au serveur de RAYON. Le WLC agit en tant qu'authentificateur qui passe des messages d'EAP entre le client et le serveur de RAYON. Un serveur de RAYON répondant avec une Access-anomalie ou une temporisation de réponse devrait être examiné et diagnostiqué par le fabricant du service RADIUS.

Remarque: Le TAC ne fournit pas le Soutien technique pour de tiers serveurs de RAYON ; cependant, les logins le serveur de RAYON expliquent généralement pourquoi une demande de client a été rejetée ou ignorée.

Afin de dépanner des Access-anomalies et des temporisations de réponse du NPS, examinez le NPS ouvre une session le visualisateur d'événements de Windows sur le serveur.

1. Cliquez sur le **début** > l'**administrateur usine** > **visualisateur d'événements** pour mettre en marche le visualisateur d'événements et pour passer en revue les logs NPS.
2. Développez les **vues** > les **rôles** > la **politique réseau faits sur commande de serveur et les accédez à**.

Dans cette section de la vue d'événement, il y a des logs de passer et des authentifications défaillantes. Examinez ces logs pour dépanner pourquoi un client ne passe pas l'authentification. Passé et les authentifications défaillantes apparaissent comme informationnel. Parcourez les logs pour trouver le nom d'utilisateur qui a l'authentification défaillante et reçu une Access-anomalie selon le WLC met au point.

C'est un exemple du NPS refusant un accès client :

En passant en revue un visualiseur d'instruction de refus en cas, examinez la section de détails d'authentification. Dans cet exemple, vous pouvez voir que le NPS a refusé l'accès client dû à un nom d'utilisateur incorrect :

La vue d'événement sur le NPS assiste également le dépannage si le WLC ne reçoit pas une réponse de retour du NPS. Ceci est habituellement provoqué par un secret partagé incorrect

entre le NPS et le WLC.

Dans cet exemple, le NPS jette la demande du WLC dû à un secret partagé incorrect :

Informations connexes

- Support et documentation techniques - Cisco Systems