Guide de configuration d'EAP-FAST version 1.02

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour l'authentification Protocol-flexible d'authentification extensible par l'intermédiaire de la version 1.02 sécurisée de Tunnellisation (EAP-FAST).

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous répondez à ces exigences :

- IOS AP 12.2(13)JA3, 350, ou client CB20A avec la version 5.40 et la version 8.5 (client de micrologiciels de gestionnaire CB21AG à être 2H pris en charge CY2004)
- Serveur de contrôle d'accès (ACS) 3.2.3, Windows 2000, ou XP avec ACU 6.3 installée.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Installez AP sur l'ACS

Terminez-vous ces étapes pour installer le Point d'accès (AP) sur l'ACS :

1. Sur le serveur ACS, cliquez sur Network Configuration du côté gauche.
2. Pour ajouter un client d'AAA, cliquez sur Add l'**entrée**.
3. Écrivez ces valeurs dans les cases :Adresse IP de client d'AAA — IP_of_your_APClé — Composez un principal (assurez-vous que la clé apparie la clé secrète partagée par AP)Authentifiez utilisant — RAYON (Cisco Aironet)
4. Cliquez sur **Submit**.
5. Reprise.

Installez l'ACS pour l'EAP-FAST

Terminez-vous ces étapes pour installer l'ACS pour l'EAP-FAST :

1. Choisissez la **configuration système > installation globale d'authentification**.
2. Cochez la case d'**EAP-FAST d'autoriser**.
3. Écrivez une valeur dans la zone d'informations d'ID d'autorité (les espaces ne sont pas pris en charge).
4. Cochez la case **automatique de ravitaillement PAC d'autoriser**.**Remarque:** Le ravitaillement automatique PAC est une basse méthode supplémentaire de fournir au client une intrabande PAC. Il y a quelques mises en garde au ravitaillement automatique :L'approvisionnement automatique exige de l'authentification initiale d'EAP-FAST d'échouer.Des utilisateurs de LDAP *ne peuvent pas automatique*-provisioned et doivent manuellement provisioned.L'approvisionnement automatique est susceptible d'une attaque MITM pendant le ravitaillement initial.
5. Cochez la case de **serveur de maître d'EAP-FAST**.
6. Cliquez sur **Submit**.
7. Reprise.

Configurez AP

Terminez-vous ces étapes pour configurer AP :

1. Choisissez le **Security > Server Manager**.
2. De la liste déroulante en cours de liste de serveur, choisissez le RAYON.

3. Écrivez l'adresse IP ACS.
4. Écrivez le secret partagé (doit apparier la clé dans ACS).
5. Cliquez sur **Apply**.
6. De la liste déroulante d'authentification EAP, choisissez l'adresse IP du serveur de RAYON.
7. Cliquez sur **Apply**.

Gestionnaire de cryptage (cryptage WEP seulement)

Terminez-vous ces étapes pour le cryptage WEP seulement :

1. Choisissez **Security > Encryption Manager**.
2. Cliquez sur la case d'option de **cryptage WEP**.
3. De la liste déroulante, choisissez obligatoire.
4. Cliquez sur la case d'option de la **clé de chiffrement 1**.
5. Introduisez la clé.
6. De la liste déroulante de taille de clé, choisissez 128.
7. Cliquez sur **Apply**.

Gestionnaire de cryptage (Gestion de clé WPA)

Terminez-vous ces étapes pour la Gestion de clé WPA :

1. Choisissez **Security > Encryption Manager**.
2. Cliquez sur la case d'option de **chiffrement**.
3. De la liste déroulante, choisissez le TKIP.
4. Cliquez sur **Apply**.

Gestionnaire SSID (cryptage WEP seulement)

Terminez-vous ces étapes pour le cryptage WEP seulement :

1. Choisissez le SSID de la liste du courant SSID, ou écrivez un nouveau SSID dans le champ SSID.
2. Cochez la case **ouverte d'authentification**.
3. De la liste déroulante, choisissez avec l'EAP.
4. Cochez la case d'**EAP de réseau**.
5. Cliquez sur **Apply**.

Gestionnaire SSID (Gestion de clé WPA)

Terminez-vous ces étapes pour la Gestion de clé WPA :

1. Choisissez le SSID de la liste du courant SSID, ou écrivez un nouveau SSID dans le champ SSID.
2. Cochez la case **ouverte d'authentification**.
3. De la liste déroulante, choisissez avec l'EAP.
4. Cochez la case d'**EAP de réseau**.
5. Authenticated Key Management choisi.

6. De la liste déroulante, choisissez obligatoire.
7. Case du contrôle **WPA**.
8. Cliquez sur **Apply**.

Installez le client pour l'EAP-FAST

Cryptage WEP seulement

Terminez-vous ces étapes pour le cryptage WEP seulement :

1. Ouvrez l'ACU.
2. Choisi gérez le profil.
3. Créez un profil (ou éditez un).
4. Écrivez le nom de client et le SSID d'AP.
5. Cliquez sur l'**onglet Sécurité réseau**.
6. EAP-FAST choisi.
7. Cliquez sur **Configure**.
8. Cochez le **ravitaillement automatique PAC d'autoriser pour cette** case de **profil**.**Remarque:** Le ravitaillement automatique PAC est une basse méthode supplémentaire de fournir au client une intrabande PAC. Il y a quelques mises en garde au ravitaillement automatique :L'approvisionnement automatique exige de l'authentification initiale d'EAP-FAST d'échouer.Des utilisateurs de LDAP *ne peuvent pas automatique*-provisioned et doivent manuellement provisioned.L'approvisionnement automatique est susceptible d'une attaque MITM pendant le ravitaillement initial.
9. Cliquez sur **OK**.
10. Cliquez sur **OK**.
11. Cliquez sur **OK**.
12. Sélectionnez le profil que vous avez créé.

Gestion de clé WPA

Terminez-vous ces étapes pour la Gestion de clé WPA :

1. Ouvrez l'ACU.
2. Choisi gérez le profil.
3. Créez un profil (ou éditez un).
4. Écrivez le nom de client et le SSID d'AP.
5. Cliquez sur l'**onglet Sécurité réseau**.
6. Cochez la case du **WiFi Protected Access (WPA)**.
7. Pour le type de sécurité des réseaux, EAP-FAST choisi (WPA).
8. Cliquez sur **Configure**.
9. Cochez le **ravitaillement automatique PAC d'autoriser pour cette** case de **profil**.**Remarque:** Le ravitaillement automatique PAC est une basse méthode supplémentaire de fournir au client une intrabande PAC. Il y a quelques mises en garde au ravitaillement automatique :L'approvisionnement automatique exige de l'authentification initiale d'EAP-FAST d'échouer.Des utilisateurs de LDAP *ne peuvent pas automatique*-provisioned et doivent manuellement provisioned.L'approvisionnement automatique est susceptible d'une attaque

MITM pendant le ravitaillement initial.
10. Cliquez sur **OK**.
11. Cliquez sur **OK**.
12. Cliquez sur **OK**.
13. Sélectionnez le profil que vous avez créé.

Annexe manuelle de ravitaillement PAC

Cette section inclut les procédures qui varient de ceux déjà présentées pour configurer le ravitaillement manuel PAC.

Remarque: La génération de fichiers PAC d'EAP-FAST d'option n'est pas disponible sur ACS pour des fenêtres et la procédure doit être faite manuellement suivant la procédure définie dans cette section.

Options de l'installation ACS pour l'EAP-FAST

Ces étapes sont facultatives. Si vous voulez que quelques clients utilisent le ravitaillement automatique, laissez cette option vérifiée.

1. Choisissez la **configuration système > installation globale d'authentification**.
2. Décochez la case **automatique de ravitaillement PAC d'autoriser**.

Créez le PAC utilisant CSUtil.exe

Cette procédure peut varier considérablement selon vos conditions requises. Référez-vous au guide utilisateur pour le Cisco Secure ACS pour le pour en savoir plus des Windows Server 3.2.

La syntaxe de base pour couper un PAC avec CSUtil.exe est :

```
csutil [-t] [-filepath <full filepath>] [-passwd <password>] [[-a] [-g <group number>] [-u <user name>] [-f <full filepath>]]
```

`- le filepath` est facultatif et spécifie le répertoire pour la sortie (le répertoire doit déjà exister). Si non spécifiés, les PACs sont placés dans le répertoire ACS Utils (qui peut obtenir malpropre si vous créez beaucoup de PACs).

`- le passwd` est facultatif et spécifie le mot de passe pour protéger le PAC. Si non spécifié, il n'y a aucun mot de passe par défaut.

Cette zone que quelques exemples de création valide PAC commande :

- **csutil - t - filepath c:\acspac - le passwd 5p0rk5 - f c:\acspac\pac.txt** — crée le PAC pour des utilisateurs répertoriés dans un fichier nommé pac.txt.
- **csutil - t - filepath c:\acspac - le passwd 5p0rk5 - g 0** — crée le PAC pour des utilisateurs dans le groupe 0 ACS.
- **csutil - t - filepath c:\acspac - le passwd 5p0rk5 - vadablam u** — crée le PAC pour le vadablam de nom d'utilisateur dans ACS.
- **csutil - t - filepath c:\acspac - le passwd 5p0rk5 - a** — crée le PAC pour *tous les* utilisateurs dans ACS (ceci peut prendre tout à fait pendant quelque temps).

Terminez-vous ces étapes pour créer un PAC pour un seul utilisateur afin de tester :

1. Créez un répertoire pour sortir le PAC à (facultatif).
2. Vérifiez que l'utilisateur existe dans ACS.
3. Ouvrez une invite de commande.
4. Naviguez vers le répertoire ACS Utils.
5. Écrivez le **csutil - t - <filepath> de filepath - <password> de passwd -** commande de **<user> u**.
6. Copiez le nouveau fichier .pac sur l'hôte de l'utilisateur.

Terminez-vous ces étapes pour configurer le client pour le ravitaillement manuel PAC :

1. Après avoir sélectionné l'EAP-FAST en tant que votre sécurité des réseaux saisissez l'ACU, cliquent sur Configure.
2. Décochez le **ravitaillement automatique PAC d'autoriser pour cette** case de **profil**.
3. Cliquez sur **Import**.
4. Parcourez au .pac.
5. Sélectionnez le .pac.
6. Entrez le mot de passe (s'incité).
7. Cliquez sur **OK**.
8. Cliquez sur **OK**.
9. Cliquez sur **OK**.
10. Cliquez sur **OK**.
11. Sélectionnez le profil que vous avez créé.

Vérifiez

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

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Référez-vous à ces documents pour plus d'informations :

- LES INFORMATIONS : Codes d'erreur dans la partie de Windows NT de 2 (article I)
- Comment à codes d'erreur dans la partie de Windows NT de 2

Informations connexes

- Cisco Secure ACS pour la page d'assistance de Windows
- Cisco Secure ACS pour la page de support UNIX
- Support et documentation techniques - Cisco Systems