Configurer l'authentification Web pour les invités sur les points d'accès autonomes

Contenu

Introduction

Ce document décrit comment configurer l'accès invité sur des points d'accès autonomes avec l'utilisation de la page Web interne qui est intégrée dans le point d'accès lui-même.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur les sujets suivants avant de tenter cette configuration :

- Comment configurer des AP autonomes pour le fonctionnement de base
- Comment configurer le serveur RADIUS local sur les points d'accès autonomes
- Fonctionnement de l'authentification Web en tant que mesure de sécurité de couche 3

Components Used

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

- AIR-CAP3502I-E-K9 qui exécute l'image Cisco IOS® 15.2(4)JA1

- Carte sans fil Intel Centrino Advanced-N 6200 AGN (version 13.4.0.9 du pilote)
- Utilitaire Microsoft Windows 7 supplicant

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'authentification Web est une fonctionnalité de sécurité de couche 3 (L3) qui permet aux AP autonomes de bloquer le trafic IP (à l'exception des paquets liés à DHCP et DNS) jusqu'à ce que l'invité fournisse un nom d'utilisateur et un mot de passe valides dans le portail Web vers lequel le client est redirigé lorsqu'un navigateur est ouvert.

Avec l'authentification Web, un nom d'utilisateur et un mot de passe distincts doivent être définis pour chaque invité. L'invité est authentifié avec le nom d'utilisateur et le mot de passe soit par le serveur RADIUS local, soit par un serveur RADIUS externe.

Cette fonctionnalité a été introduite dans Cisco IOS version 15.2(4)JA1.

Configuration de point d'accès

> **Note**: Ce document suppose que Bridge Virtual Interface (BVI) 1 sur l'AP a une adresse IP de 192.168.10.2 /24, et que le pool DHCP est défini en interne sur l'AP pour les adresses IP 192.168.10.10 à 192.168.10.254 (adresses IP) 192.168.10.1 à 192.168.10.10 sont exclus).

Complétez ces étapes afin de configurer le point d'accès pour l'accès invité :

1. Ajoutez un nouveau SSID (Service Set Identifier) , nommez-le **Guest** et configurez-le pour l'authentification Web :

```
ap(config)#dot11 ssid Guest

ap(config-ssid)#authentication open

ap(config-ssid)#web-auth

ap(config-ssid)#guest-mode

ap(config-ssid)#exit
```

2. Créez une règle d'authentification, dans laquelle vous devez spécifier le protocole d'authentification proxy et lui attribuer un nom **web_auth** :

```
ap(config)#ip admission name web_auth proxy http
```

3. Appliquez le SSID (**Guest**) et la règle d'authentification (**web_auth**) à l'interface radio. Cet exemple utilise la radio 802.11b/g :

```
ap(config)#interface dot11radio 0

ap(config-if)#ssid Guest

ap(config-if)#ip admission web_auth

ap(confi-if)#no shut

ap(config-if)#exit
```

4. Définissez la liste des méthodes qui spécifie l'emplacement d'authentification des informations d'identification de l'utilisateur. Liez le nom de la liste de méthodes à la règle d'authentification **web_auth** et nommez-le **web_list** :

```
ap(config)#ip admission name web_auth method-list authentication web_list
```

5. Complétez ces étapes afin de configurer l'authentification, l'autorisation et la comptabilité (AAA) sur l'AP et le serveur RADIUS local, et lier la liste de méthodes avec le serveur RADIUS local sur l'AP :

   Activer AAA :

```
ap(config)#aaa new-model
```

   Configurez le serveur RADIUS local :

```
ap(config)#radius-server local

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Créez les comptes d'invité et spécifiez leur durée de vie (en minutes). Créez un compte d'utilisateur avec un nom d'utilisateur et un mot de passe **user1**, et définissez la valeur de durée de vie sur 60 minutes :

```
ap(config)#dot11 guest

ap(config-guest-mode)#username  user1 lifetime 60 password user1

ap(config-guest-mode)#exit

ap(config)#
```

Vous pouvez créer d'autres utilisateurs avec le même processus.

Note: Vous devez activer **radius-server local** afin de créer des comptes invités. Définissez le point d'accès en tant que serveur RADIUS :

```
ap(config)#radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

Liez la liste d'authentification Web au serveur local :

```
ap(config)#aaa authentication login web_list group radius
```

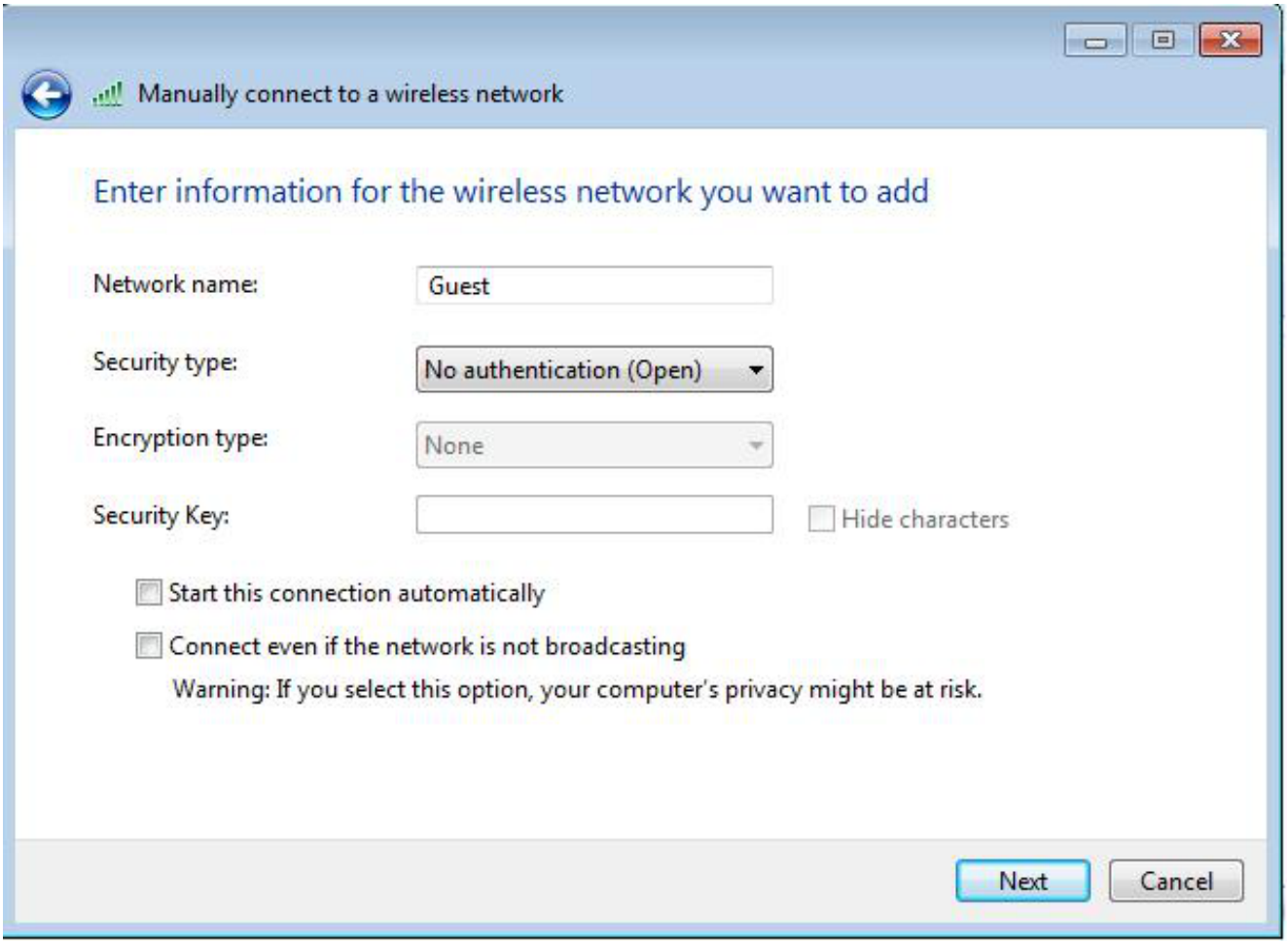
Note: Vous pouvez utiliser un serveur RADIUS externe afin d'héberger les comptes d'utilisateurs invités. Pour ce faire, configurez la commande **radius-server host** pour pointer vers le serveur externe au lieu de l'adresse IP AP.

Configuration du client sans fil

Complétez ces étapes afin de configurer le client sans fil :

1. Afin de configurer le réseau sans fil de votre utilitaire Windows supplicant avec le SSID nommé **Guest**, accédez à **Réseau et Internet > Gérer les réseaux sans fil**, puis cliquez sur **Ajouter**.

2. Sélectionnez **Connexion manuelle à un réseau sans fil**, puis saisissez les informations requises, comme illustré dans cette image :



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

Vérification

Une fois la configuration terminée, le client peut se connecter au SSID normalement, et vous voyez ceci sur la console AP :

```
%DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880
 Associated KEY_MGMT[NONE]

ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address    IP address   IPV6 address  Device    Name  Parent  State

0027.10e1.9880  0.0.0.0     ::           ccx-client  ap   self    Assoc
```

L’adresse IP dynamique du client est 192.168.10.11. Cependant, lorsque vous essayez d'envoyer une requête ping à l'adresse IP du client, elle échoue car le client n'est pas entièrement authentifié :

```
ap#PING 192.168.10.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)
```

Si le client ouvre un navigateur et tente d'atteindre **http://1.2.3.4** par exemple, le client est redirigé vers la page de connexion interne :

Username:

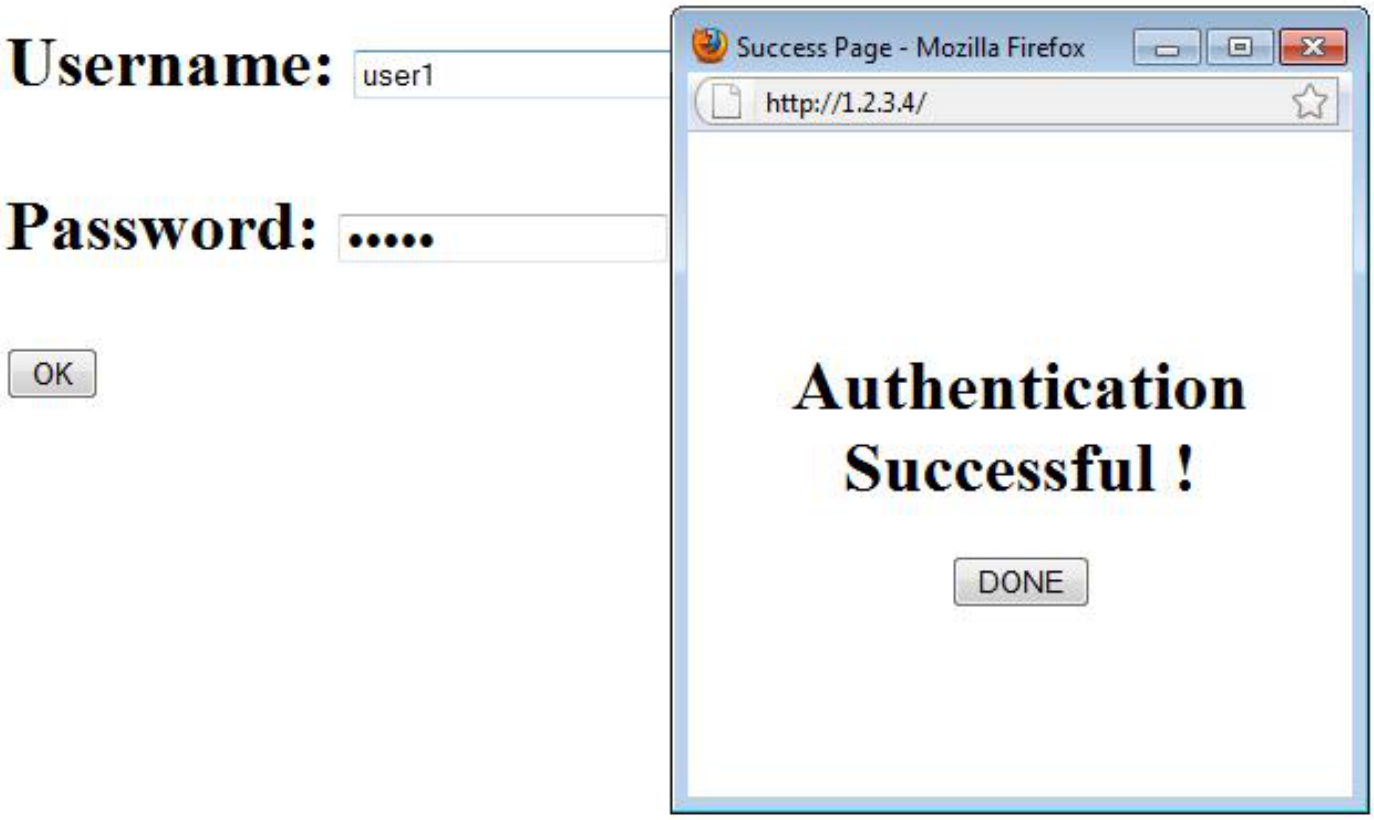
Password:

OK

> **Note**: Ce test est complété par une adresse IP aléatoire entrée directement (l'URL entrée est **1.2.3.4**) sans traduction d'une URL via le DNS, car le DNS n'a pas été utilisé dans le test. Dans des scénarios normaux, l'utilisateur entre l'URL de la page d'accueil et le trafic DNS est autorisé jusqu'à ce que le client envoie le message HTTP GET à l'adresse résolue, qui est interceptée par le point d'accès. Le point d'accès falsifie l'adresse du site Web et redirige le client vers la page de connexion stockée en interne.

Une fois le client redirigé vers la page de connexion, les informations d'identification de l'utilisateur sont entrées et vérifiées sur le serveur RADIUS local, conformément à la configuration de l'AP. Après une authentification réussie, le trafic qui vient et va au client est entièrement autorisé.

Voici le message envoyé à l'utilisateur après une authentification réussie :



Après une authentification réussie, vous pouvez afficher les informations IP du client :

```
ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address    IP address    IPV6 address  Device   Name  Parent  State

0027.10e1.9880  192.168.10.11 ::       ccx-client  ap    self   Assoc
```

Les requêtes ping envoyées au client une fois l'authentification terminée doivent fonctionner correctement :

```
ap#ping 192.168.10.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

Dépannage

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

> **Note**: L'itinérance entre les points d'accès lors de l'authentification Web ne fournit pas une expérience fluide, car les clients doivent se connecter à chaque nouveau point d'accès auquel ils se connectent.

Personnalisation

Àl’instar de l’IOS sur les routeurs ou les commutateurs, vous pouvez personnaliser votre page à l’aide d’un fichier personnalisé ; cependant, il n'est pas possible de rediriger vers une page web externe.

Utilisez ces commandes afin de personnaliser les fichiers du portail :

- **ip admission proxy http login page file**
- **ip admission proxy fichier de page expirée http**
- **fichier de la page de succès http du proxy d'admission ip**
- **fichier de page ip admission proxy http fail**