Authentification de Web interne pour l'accès invité sur l'exemple autonome de configuration aps

Contenu

Introduction

Ce document décrit comment configurer pour l'accès invité sur les points d'accès autonome (aps) avec l'utilisation de la page Web interne qui est incluse dans AP lui-même.

Conditions préalables

Conditions requises

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

- Comment configurer des aps autonomes pour le fonctionnement de base
- Comment configurer le serveur local de RAYON sur des aps autonomes
- Comment authentification Web en tant que travaux d'une mesure de sécurité de la couche 3

Composants utilisés

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 15.2(4)JA1 de Cisco IOS®
- Adaptateur Sans fil avancé-n d'Intel Centrino 6200 AGN (version 13.4.0.9 de gestionnaire)
- Utilitaire de suppliant de Microsoft Windows 7

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.

Informations générales

L'authentification Web est une fonctionnalité de sécurité de la couche 3 (L3) qui permet aux aps autonomes de bloquer le trafic IP (excepté à paquets liés DHCP et de Domain Name Server (DN)) jusqu'à ce que l'invité fournisse un nom d'utilisateur valide et un mot de passe dans le portail web auquel le client est réorienté quand un navigateur est ouvert.

Avec l'authentification Web, un nom d'utilisateur et mot de passe distinct doit être défini pour chaque invité. L'invité est authentifié avec le nom d'utilisateur et mot de passe par le serveur local de RAYON ou un serveur RADIUS externe.

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

Configuration AP

> Remarque: Ce document suppose que l'interface virtuelle de passerelle (BVI) 1 sur AP a une adresse IP de 192.168.10.2 /24, et que le pool DHCP est défini intérieurement sur AP pour des adresses IP 192.168.10.10 par 192.168.10.254 (adresses IP 192.168.10.1 par 192.168.10.10 sont exclus).

Terminez-vous ces étapes afin de configurer AP pour l'accès invité :

1. Ajoutez un nouvel Identifiant SSID (Service Set Identifier), nommez-le **invité,** 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, où vous devez spécifier le protocole d'authentification de proxy, et nommez-la **web_auth** :

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

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

```
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 de méthode qui spécifie où les identifiants utilisateurs sont authentifiés. Joignez le nom de liste de méthode avec la règle d'authentification de **web_auth**, et nommez-le **web_list** :

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

5. Terminez-vous ces étapes afin de configurer l'Authentification, autorisation et comptabilité (AAA) sur AP et le serveur local de RAYON, et joignez la liste de méthode avec le serveur local de RAYON sur AP :

   AAA d'enable :

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

   Configurez le serveur local de RAYON :

```
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 vie (en quelques minutes). Créez un compte utilisateur avec un nom d'utilisateur et mot de passe d'**user1**, et placez la valeur de vie à 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.

   Remarque: Vous devez permettre au **radius-server local** afin de créer des comptes d'invité. Définissez AP en tant que serveur de RAYON :

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

   Joignez la liste d'authentification Web avec le serveur local :

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

Remarque: Vous pouvez utiliser un serveur RADIUS externe afin de héberger les comptes

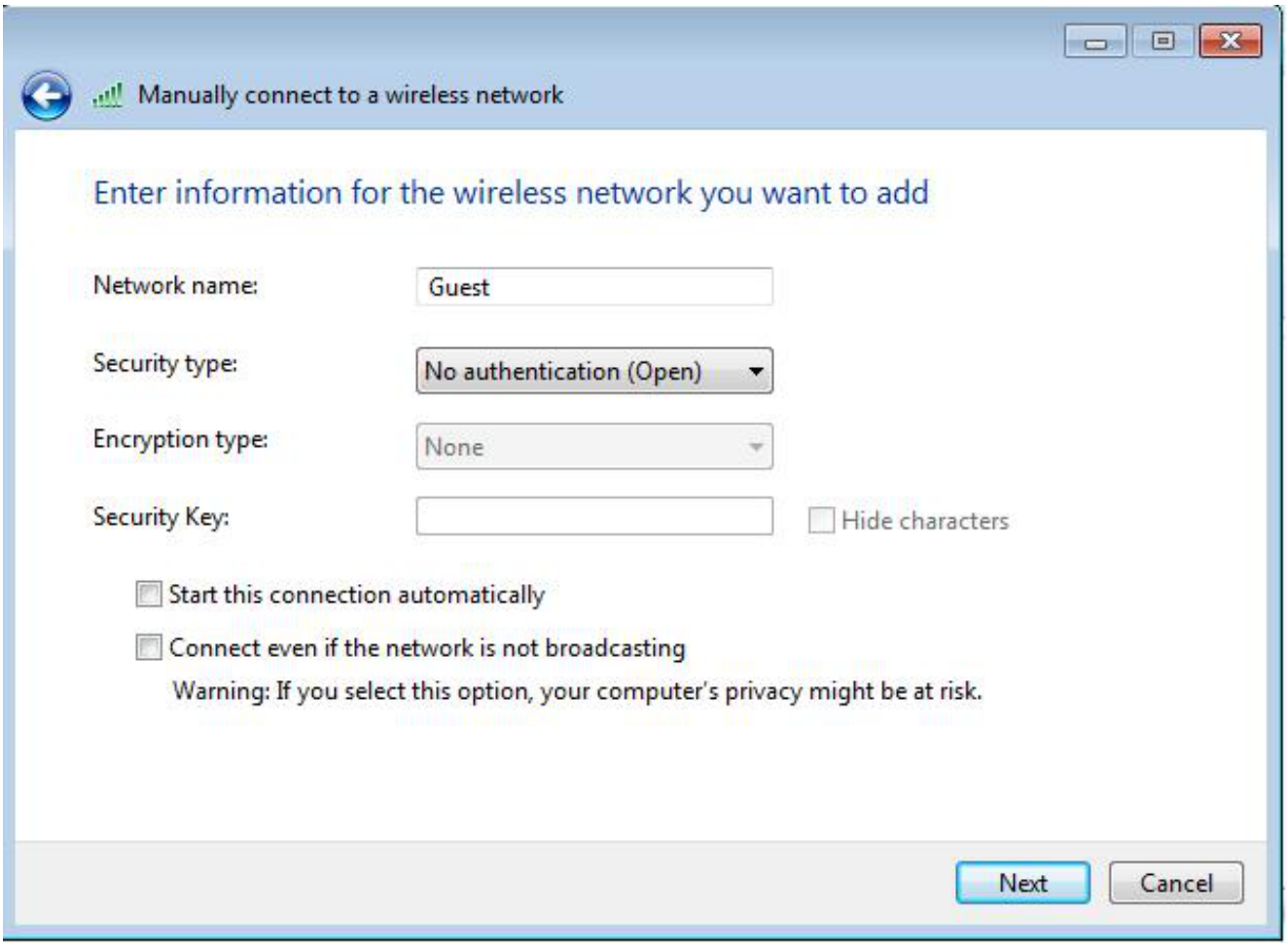
utilisateurs d'invité. Afin de faire ceci, configurez la commande d'**hôte de rayon-serveur** d'indiquer le serveur externe au lieu de l'adresse IP AP.

Configurez le client sans fil

Terminez-vous ces étapes afin de configurer le client sans fil :

1. Afin de configurer le réseau Sans fil sur vos fenêtres que l'utilitaire de suppliant avec le SSID a nommé **Guest**, naviguez vers le **réseau et l'Internet > gèrent des réseaux sans fil**, et cliquent sur Add.

2. Sélectionnez **se connectent manuellement à un réseau Sans fil**, et écrivent l'information requise, suivant les indications de cette image :



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

Vérifiez

Après que la configuration soit complète, le client peut se connecter au SSID normalement, et

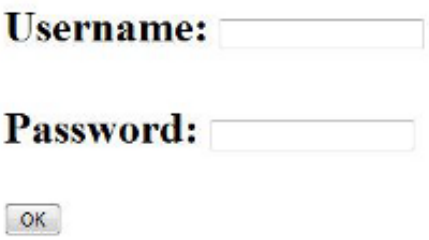
vous voyez ceci sur la console AP :

```
%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
```

Le client a une adresse IP dynamique de 192.168.10.11. Cependant, quand vous tentez de cingler l'adresse IP du client, il échoue parce que 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 des tentatives d'atteindre **http://1.2.3.4** par exemple, le client est réorienté à la page de connexion interne :

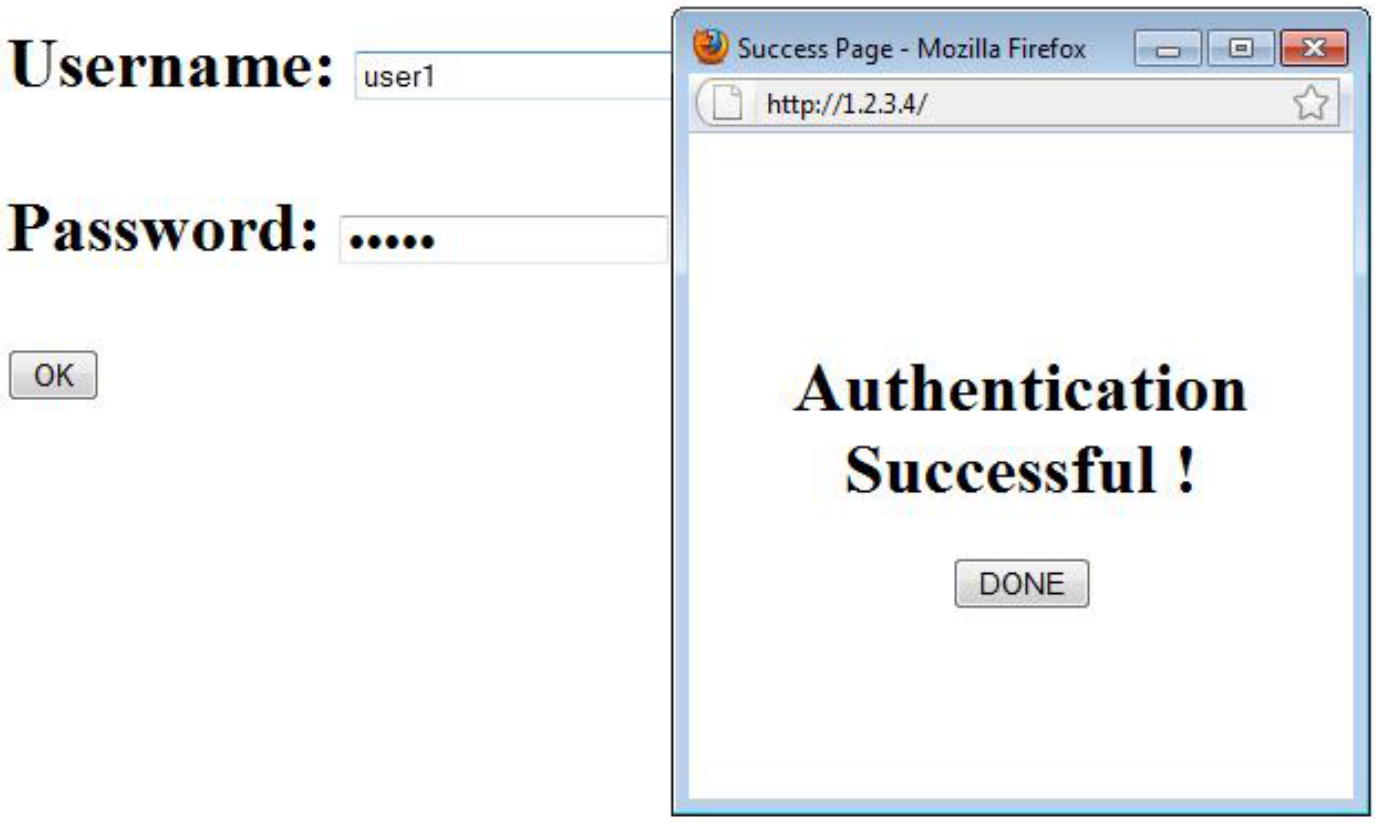


> Remarque: Ce test est terminé avec une adresse IP aléatoire écrite directement (ici l'URL écrit est **1.2.3.4**) sans besoin de traduction d'un URL par les DN, parce que les DN n'ont pas été utilisés dans le test. Dans les scénarios normaux, l'utilisateur écrit l'URL de page d'accueil, et le trafic DNS est permis jusqu'à ce que le client envoie le HTTP REÇOIVENT le

message à l'adresse résolue, qui est interceptée par AP. AP charrie l'adresse de site Web, et réoriente le client à la page de connexion enregistrée intérieurement.

Une fois que le client est réorienté à la page de connexion, les identifiants utilisateurs sont écrits et vérifiés contre le serveur local de RAYON, selon la configuration AP. Après l'authentification réussie, on permet entièrement le trafic qui provient et va au client.

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



Après l'authentification réussie, vous pouvez visualiser les informations IP de 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 pings au client après que l'authentification réussie soit complète devraient 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
```

Dépannez

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

> Remarque: Errer entre les aps pendant l'authentification Web ne fournit pas une expérience douce, parce que les clients doivent ouvrir une session à chaque nouvel AP auquel ils se connectent.

Personnalisation

Semblable à l'IOS sur des Routeurs ou des Commutateurs, vous pouvez personnaliser votre page avec un fichier fait sur commande ; cependant, il n'est pas possible au redirect to par page Web externe.

Employez ces commandes afin de personnaliser les fichiers portaiux :

- fichier de page de connexion d'ip admission proxy http
- l'ip admission proxy http a expiré fichier paginé
- fichier paginé de succès d'ip admission proxy http
- fichier paginé de panne d'ip admission proxy http