Configurez l'authentification de Web externe avec Access convergé (5760/3650/3850)

Contenu

Introduction

Ce document définit comment configurer le Web externe authentique avec les contrôleurs convergés d'Access. La page du portail d'invité et l'authentification de qualifications sont tous deux sur le Cisco Identity Services Engine (ISE) dans cet exemple.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

1. Cisco a convergé des contrôleurs d'accès.

2. Authentification Web

3. Cisco ISE

Composants utilisés

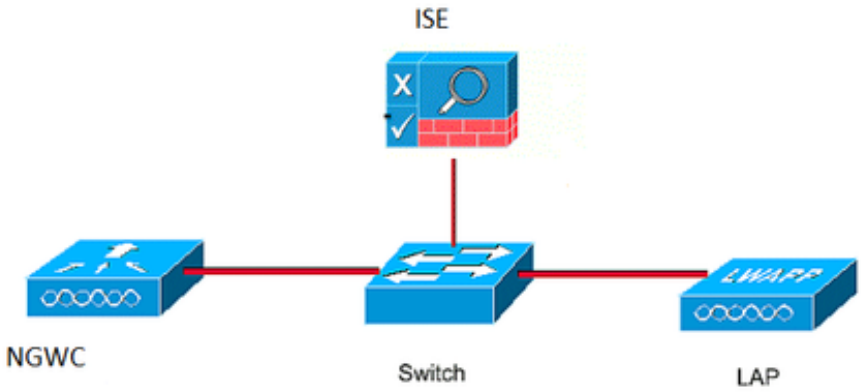
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

1. Contrôleur de Cisco 5760 (NGWC sur le diagramme ci-dessous), 03.06.05E

2. ISE 2.2

Configurez

Diagramme du réseau



Configuration CLI

Configuration RADIUS sur le contrôleur

étape 1 : Définissez le serveur RADIUS externe

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

étape 2 :. Définissez le groupe d'AAA RADIUS et spécifiez le serveur de rayon à utiliser

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

étape 3. Définissez la liste de méthode indiquant le groupe de rayon et tracez-la sous le WLAN.

```
aaa authentication login webauth group ISE-Group
```

Configuration de carte de paramètre

étape 4. Configurez la carte de paramètre global avec l'IP address virtuel qui est exigé pour le webauth externe et interne. Le bouton de déconnexion utilise l'IP virtuel. Son toujours une bonne pratique de configurer un IP virtuel non-routable.

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

étape 5 : Configurez une carte Désignée de paramètre. Il agira comme un type de méthode de webauth. Ceci s'appellera sous le config WLAN.

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

Pré ACL d'authentification. Ceci également s'appellera sous le WLAN.

étape 6 : Configurez Preauth_ACL qui permet l'accès à ISE, à DHCP et à DN avant que l'authentification soit terminée

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

Config WLAN

étape 7 : configurez le WLAN

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

étape 8 : Activez le serveur de HTTP.

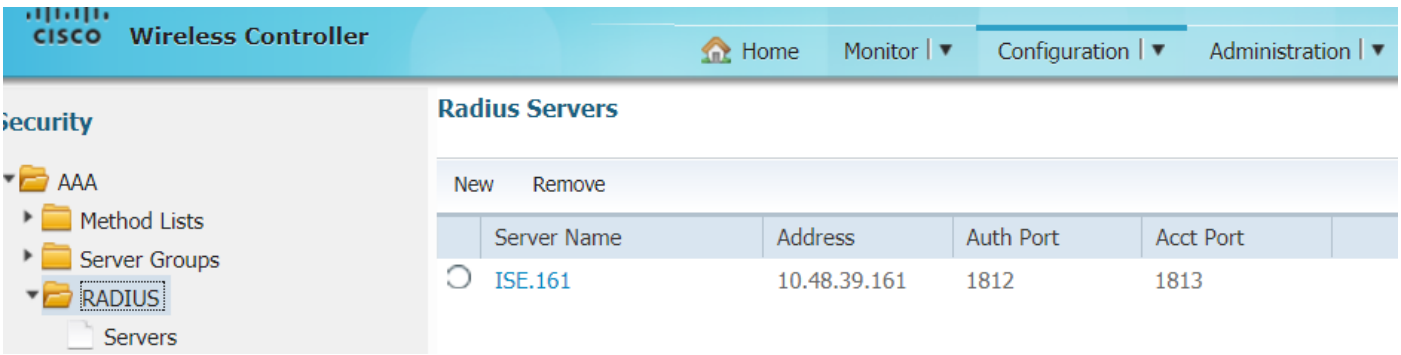
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

Configuration GUI

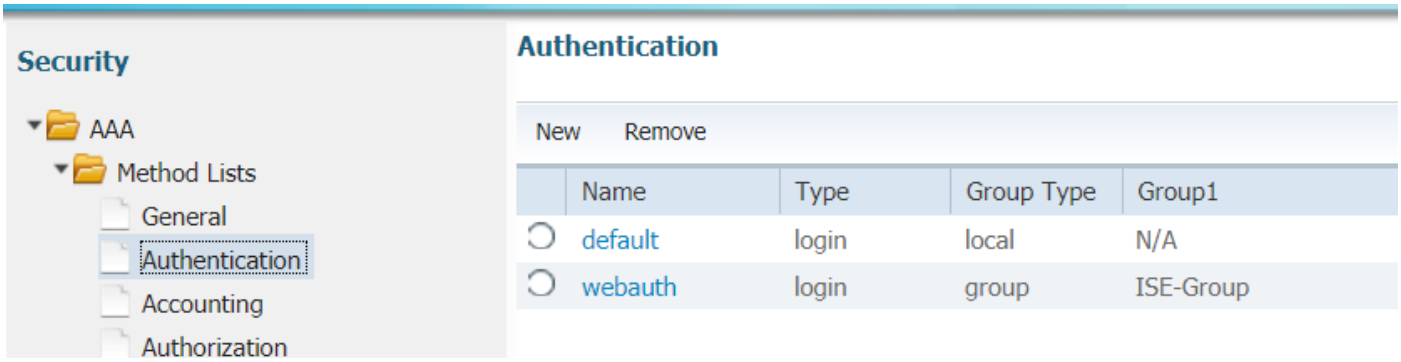
Nous sommes suivants ici les mêmes étapes comme ci-dessus. Les captures d'écran sont juste données pour la référence croisée.

étape 1 : Définissez un serveur RADIUS externe



étape 2 :. Définissez le groupe d'AAA RADIUS et spécifiez le serveur de rayon à utiliser

étape 3. Définissez la liste de méthode indiquant le groupe de rayon et tracez-la sous le WLAN.



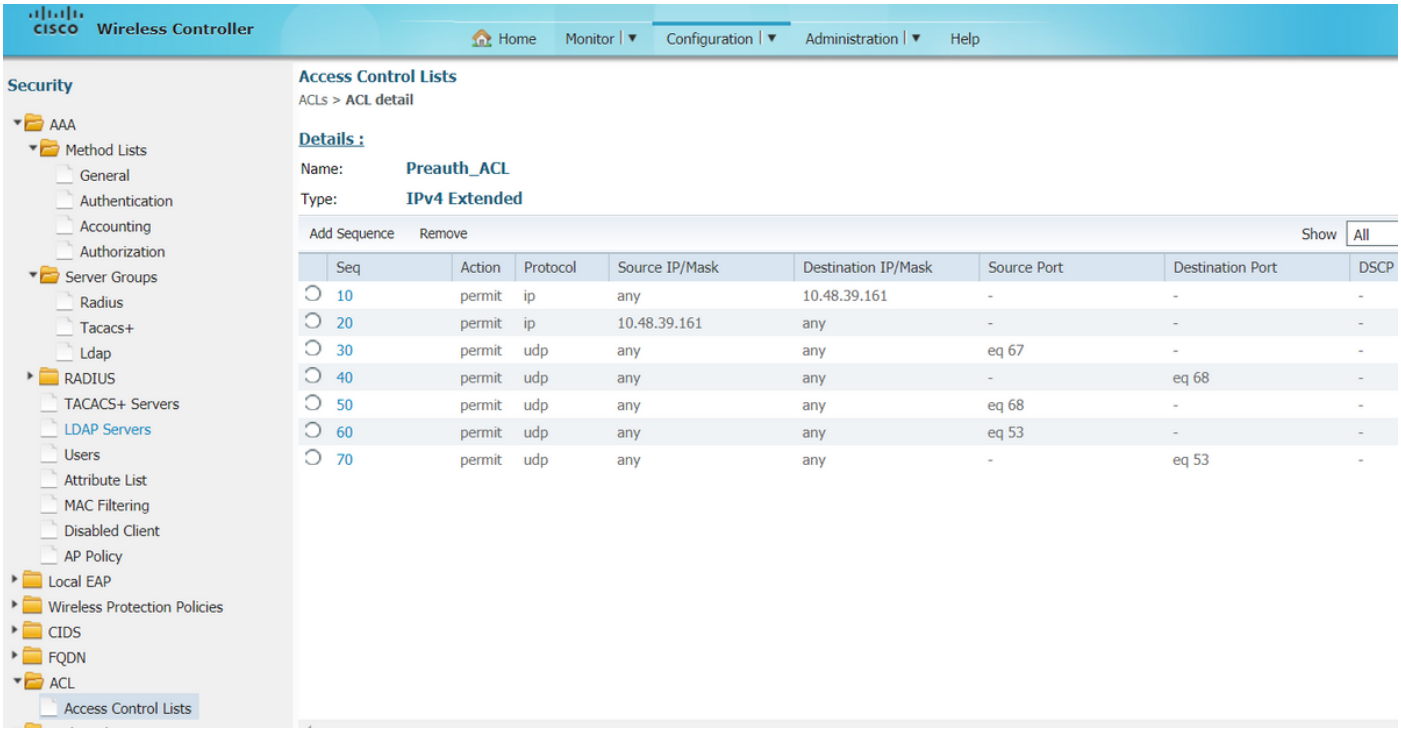
Configuration de carte de paramètre

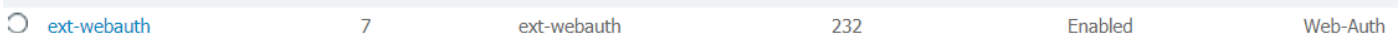
étape 4. Configurez la carte de paramètre global avec l'IP address virtuel qui est exigé pour le webauth externe et interne. Le bouton de déconnexion utilise l'IP virtuel. Son toujours une bonne pratique de configurer un IP virtuel non-routable.

étape 5 : Configurez une carte Désignée de paramètre. Il agira comme un type de méthode de webauth. Ceci s'appellera sous le config WLAN.

Pré ACL d'authentification. Ceci également s'appellera sous le WLAN.

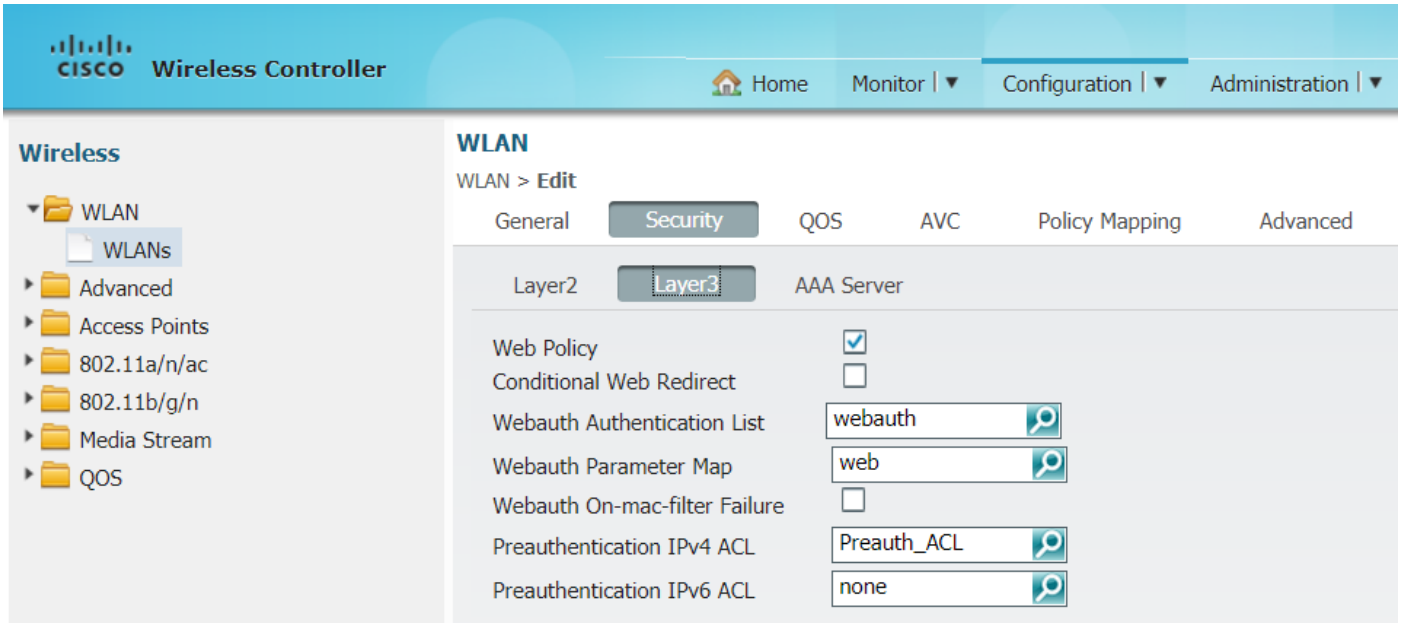
étape 6 : Configurez Preauth_ACL qui permet l'accès à ISE, à DHCP et à DN avant que l'authentification soit terminée





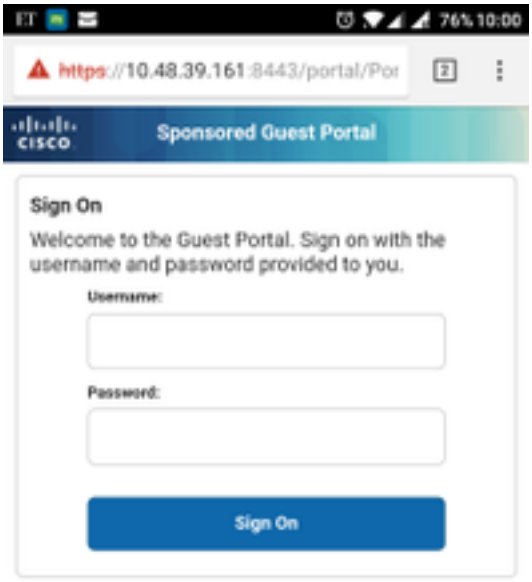
Config WLAN

étape 7 : configurez le WLAN

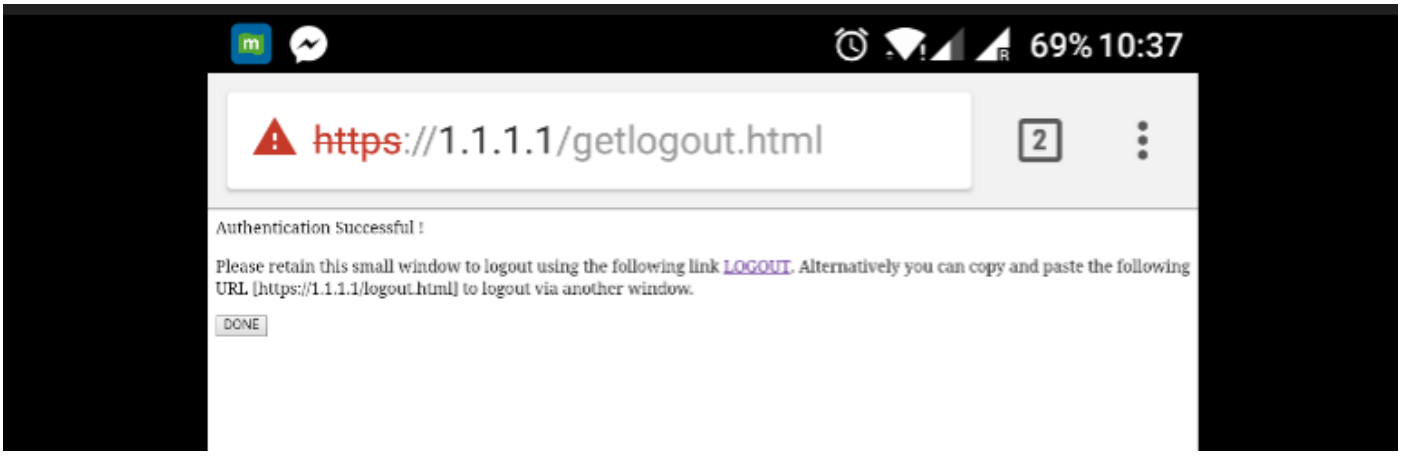


Vérifiez

Connectez un client et assurez-vous que si vous ouvrez un navigateur, le client sera réorienté à votre page du portail de procédure de connexion. Le tir d'écran ci-dessous illustre la page du portail d'invité ISE.



Une fois que des qualifications appropriées sont soumises, la page de succès sera affichée :



Le serveur ISE signalera l'authentification deux : un à la page d'invité elle-même (la ligne inférieure avec seulement le nom d'utilisateur) et à une deuxième authentification une fois que le WLC fournit le même nom d'utilisateur/mot de passe par l'authentification de rayon (seulement cette authentification incitera le client à se déplacer à la phase de succès). Si l'authentification de rayon (avec le MAC address et les détails WLC comme NAS) ne se produit pas, la configuration RADIUS doit être vérifiée.