Autenticación del Web externa de la configuración con el acceso convergido (5760/3650/3850)

Contenido

Introducción

Este documento define cómo configurar el auth del Web externa con los reguladores convergidos del acceso. Autenticación porta de la página y de las credenciales del invitado es ambas en el Identity Services Engine (ISE) en este ejemplo.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

1. Cisco convergió los reguladores del acceso.

2. Autenticación Web

3. Cisco ISE

Componentes Utilizados

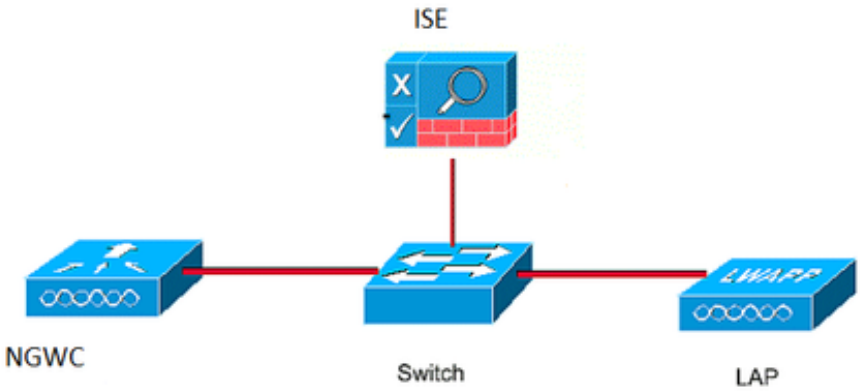
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

1. Regulador de Cisco 5760 (NGWC en el diagrama abajo), 03.06.05E

2. ISE 2.2

Configurar

Diagrama de la red



Configuración de CLI

Configuración de RADIUS en el regulador

paso 1: Defina al servidor RADIUS externo

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

paso 2:. Defina RADIUS AAA al grupo y especifique al servidor de RADIUS que se utilizará

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

paso 3. Defina la lista de métodos que señala al grupo del radio y asocíela bajo la red inalámbrica (WLAN).

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

Configuración de asignación del parámetro

paso 4. Configure la correspondencia del Parámetro global con la dirección IP virtual que se requiere para el webauth externo e interno. Aplicaciones del botón Logout Button IP virtual. Su siempre una práctica adecuada de configurar un no routable IP virtual.

```
parameter-map type webauth global
type webauth
```

```
virtual-ip ipv4 1.1.1.1
```

paso 5: Configure una correspondencia Nombrada del parámetro. Actuará como un tipo de método del webauth. Esto será llamada bajo config de la red inalámbrica (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
```

Pre autenticación ACL. Esto también será llamada bajo la red inalámbrica (WLAN).

paso 6: Configure Preauth_ACL que permita el acceso al ISE, al DHCP y al DNS antes de que la autenticación haya terminado

```
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 de la red inalámbrica (WLAN)

paso 7: configure la red inalámbrica (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
```

paso 8: Gire el servidor HTTP.

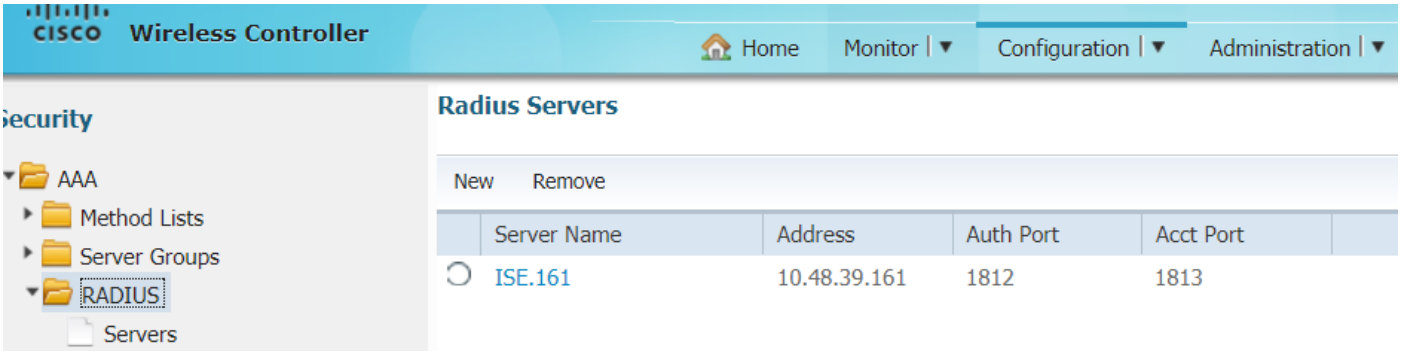
```
ip http server

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

Configuración del GUI

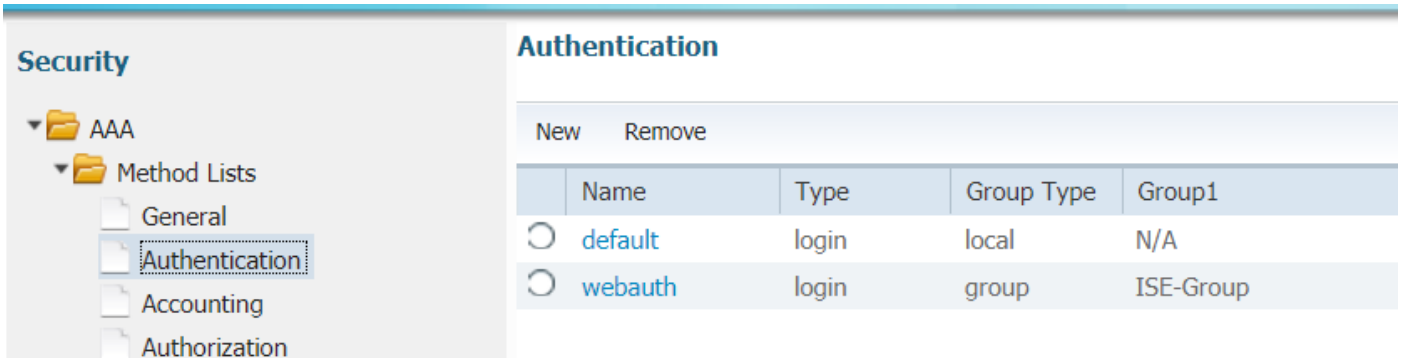
Somos siguientes aquí los mismos pasos que arriba. El screenshots apenas se proporciona para la referencia cruzada.

paso 1: Defina a un servidor RADIUS externo



paso 2:. Defina RADIUS AAA al grupo y especifique al servidor de RADIUS que se utilizará

paso 3. Defina la lista de métodos que señala al grupo del radio y asocíela bajo la red inalámbrica (WLAN).



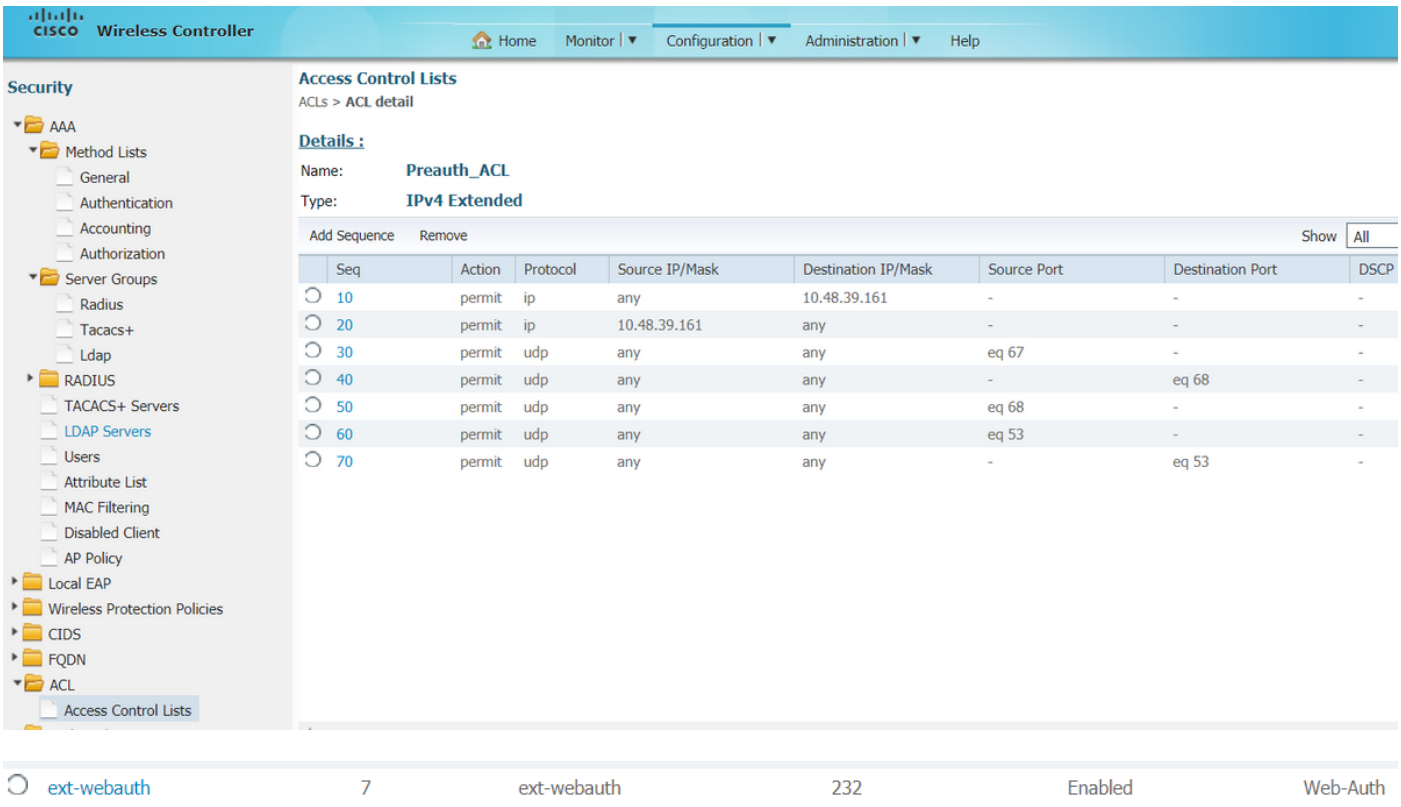
Configuración de asignación del parámetro

paso 4. Configure la correspondencia del Parámetro global con la dirección IP virtual que se requiere para el webauth externo e interno. Aplicaciones del botón Logout Button IP virtual. Su siempre una práctica adecuada de configurar un no routable IP virtual.

paso 5: Configure una correspondencia Nombrada del parámetro. Actuará como un tipo de método del webauth. Esto será llamada bajo config de la red inalámbrica (WLAN).

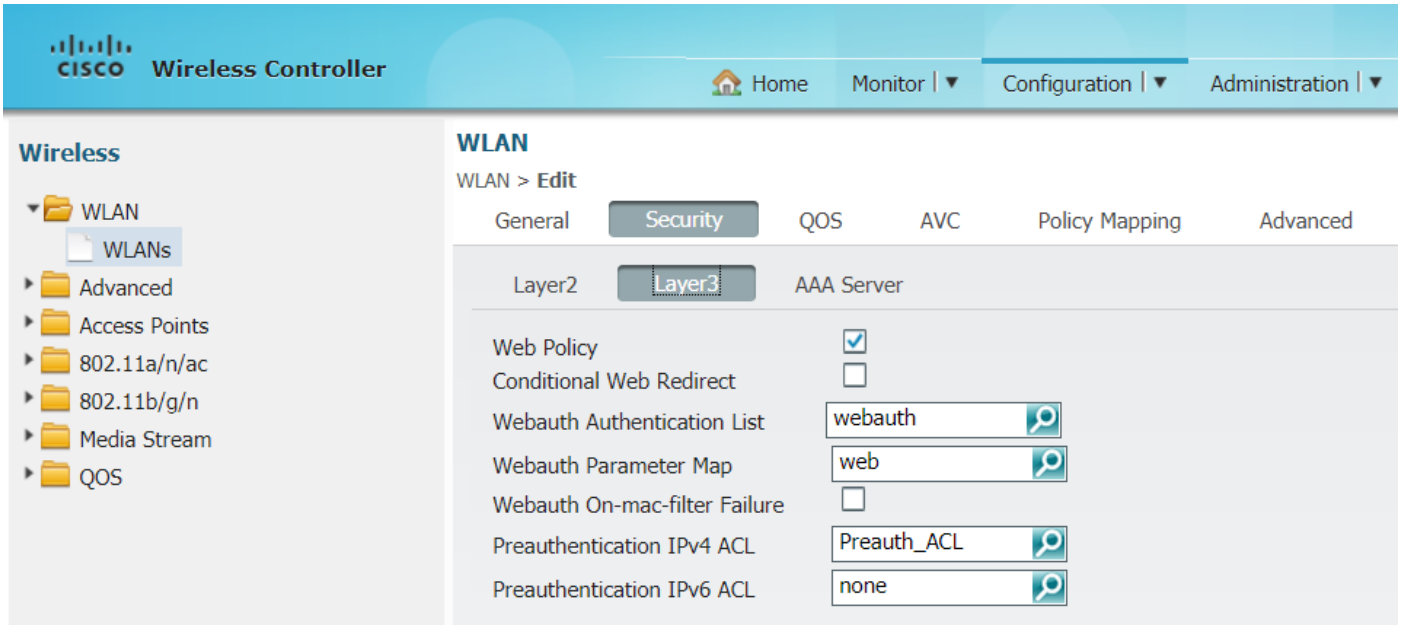
Pre autenticación ACL. Esto también será llamada bajo la red inalámbrica (WLAN).

paso 6: Configure Preauth_ACL que permita el acceso al ISE, al DHCP y al DNS antes de que la autenticación haya terminado



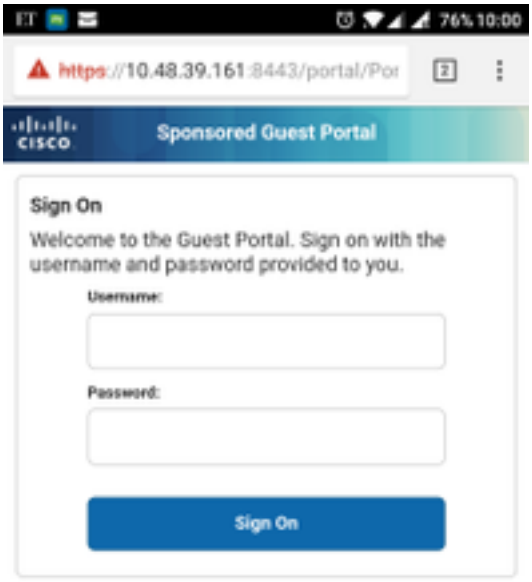
Config de la red inalámbrica (WLAN)

paso 7: configure la red inalámbrica (WLAN)

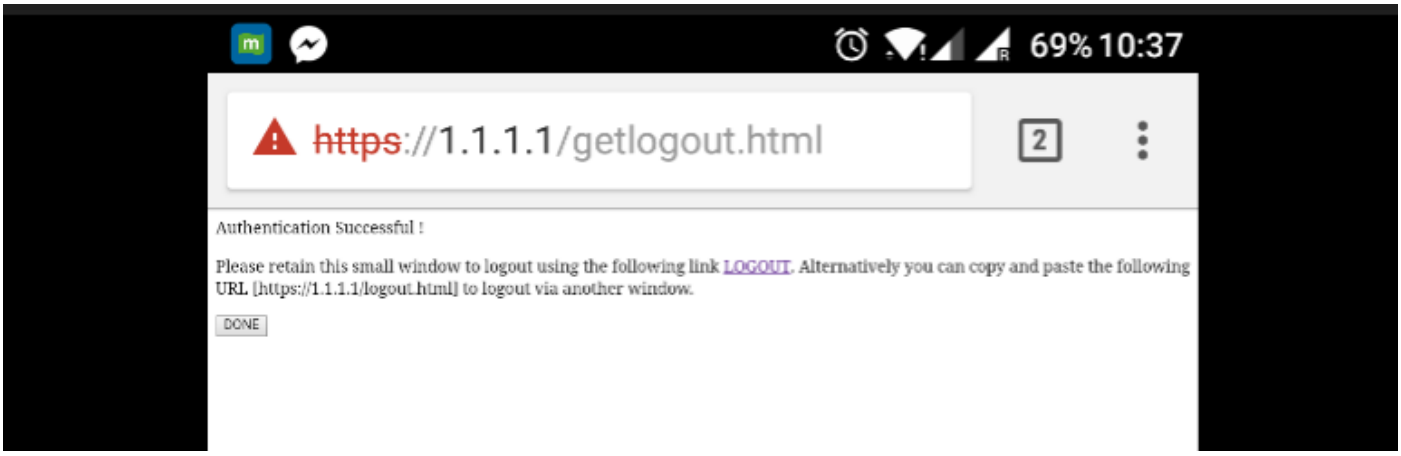


Verificación

Conecte a un cliente y aseegurese que si usted abre a un navegador, reorientarán al cliente a su página porta del login. El tiro de pantalla abajo ilustra la página porta del invitado ISE.



Una vez que se someten las credenciales apropiadas, la página del éxito será mostrada:



El servidor ISE señalará a dos la autenticación: uno en la página sí mismo del invitado (lo importante con solamente el nombre de usuario) y una segunda autenticación una vez que el WLC proporciona el mismo nombre de usuario/la contraseña con la autenticación de RADIUS (solamente esta autenticación hará que el cliente se mueve a la fase del éxito). Si no ocurre la autenticación de RADIUS (con el MAC address y los detalles del WLC como NAS), la configuración de RADIUS debe ser verificada.