配置与聚合的访问(5760/3650/3850)的外部Web验证

目录

简介

本文定义了如何配置外部Web验证用聚合的访问控制器。访客入口页面和凭证验证是两个在身份服务引擎(ISE)在本例中。

先决条件

要求

Cisco 建议您了解以下主题：

1. 思科聚合访问控制器。

2. Web验证

3. 思科ISE

使用的组件

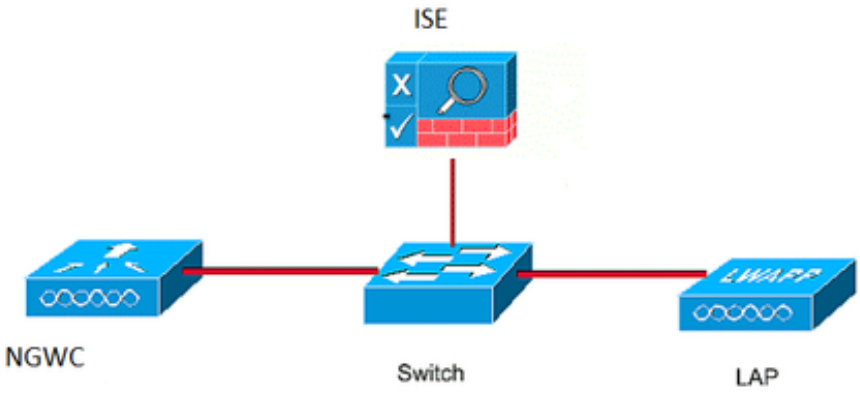
本文档中的信息基于以下软件和硬件版本：

1. 思科5760控制器(在下面的图表的NGWC)， 03.06.05E

2. ISE 2.2

配置

网络图



CLI 配置

在控制器的RADIUS配置

step1 ：定义外部RADIUS服务器

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

步骤2 ：。定义AAA RADIUS组并且指定将使用的RADIUS服务器

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

步骤3.定义指向radius组的方法列表并且映射它在WLAN下。

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

参数映射配置

步骤4.配置全局参数地图用为外部和内部webauth要求的虚拟IP地址。logout按钮用途虚拟IP。其总是良好的做法配置一个不可路由的虚拟IP。

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

步骤5 ：配置指定参数地图。它将操作类似webauth方法的类型。这将呼叫在WLAN设置下。

```
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
```

前验证ACL。这也将呼叫在WLAN下。

步骤6 ：配置允许对ISE、DHCP和DNS的访问的Preauth_ACL，在验证结束前

```
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
```

WLAN设置

步骤7 ：配置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
```

步骤8 ：打开HTTP服务器。

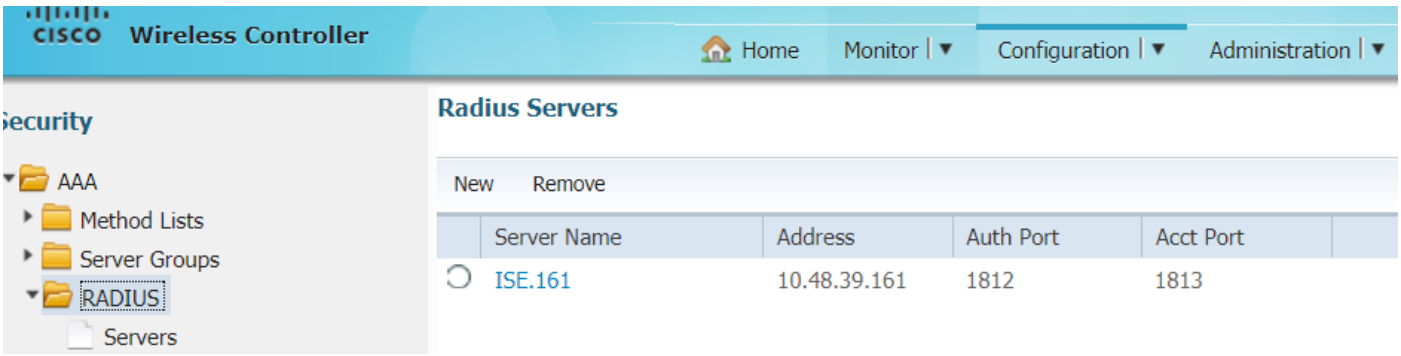
```
ip http server

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

GUI配置

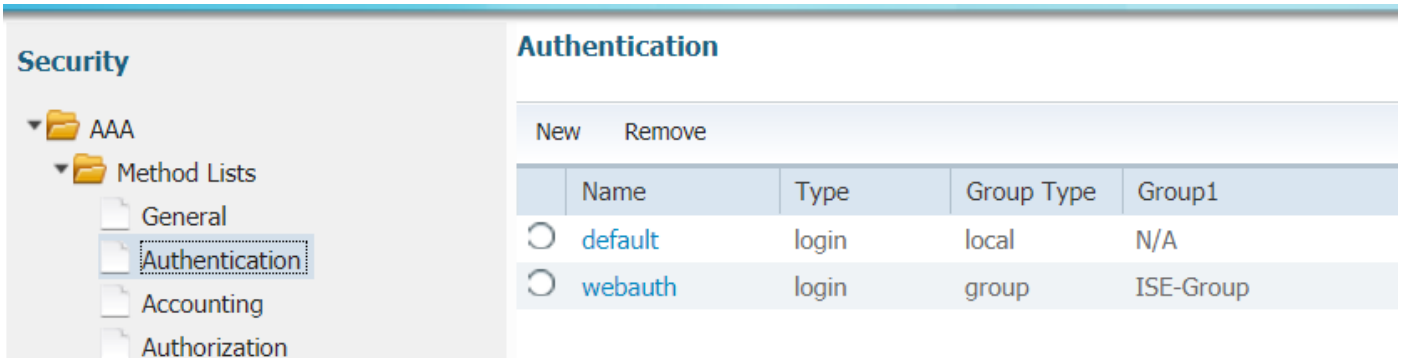
我们在以下此处步骤和上述一样。屏幕画面为参照提供。

step1 ：定义外部RADIUS服务器



步骤2 ：。定义AAA RADIUS组并且指定将使用的RADIUS服务器

步骤3.定义指向radius组的方法列表并且映射它在WLAN下。



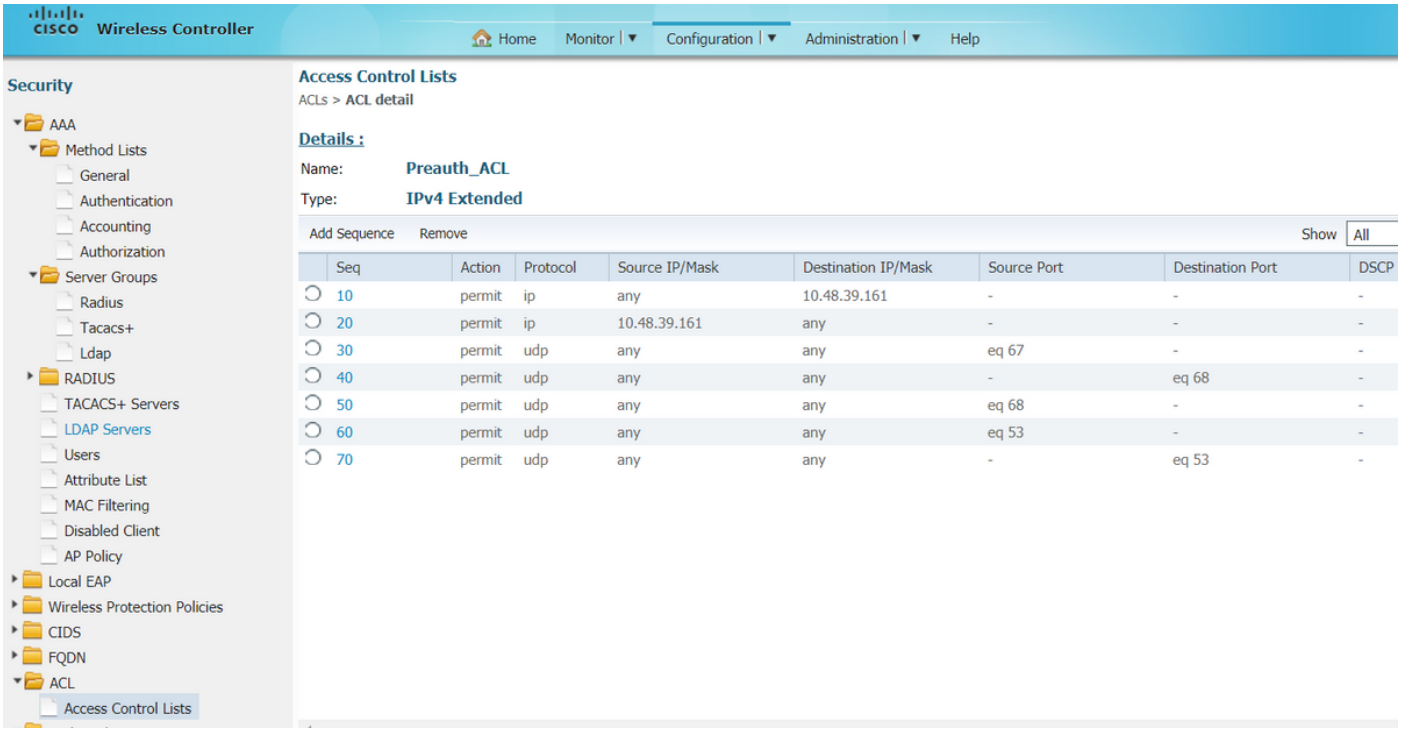
参数映射配置

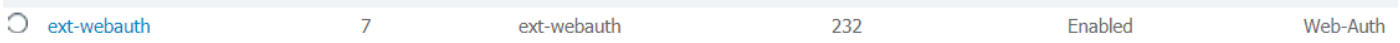
步骤4.配置全局参数地图用为外部和内部webauth要求的虚拟IP地址。logout按钮用途虚拟IP。其总是良好的做法配置一个不可路由的虚拟IP。

步骤5 ：配置指定参数地图。它将操作类似webauth方法的类型。这将呼叫在WLAN设置下。

前验证ACL。这也将呼叫在WLAN下。

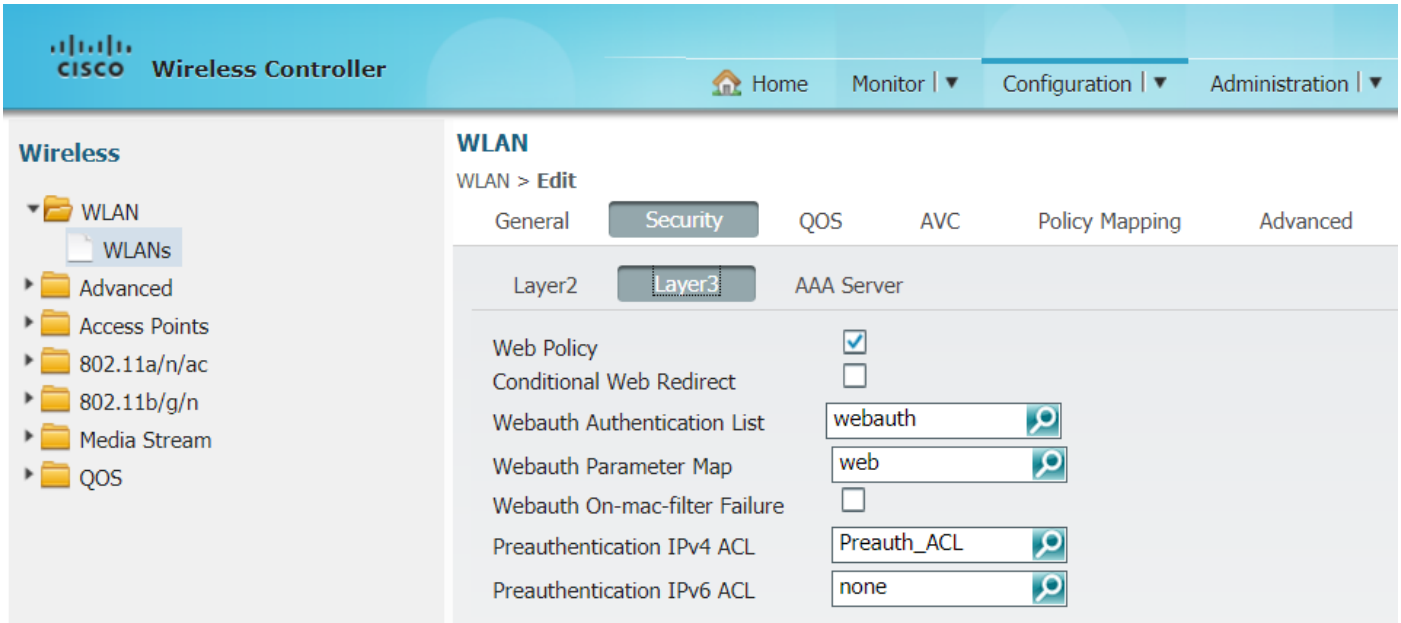
步骤6 ：配置允许对ISE、DHCP和DNS的访问的Preauth_ACL，在验证结束前





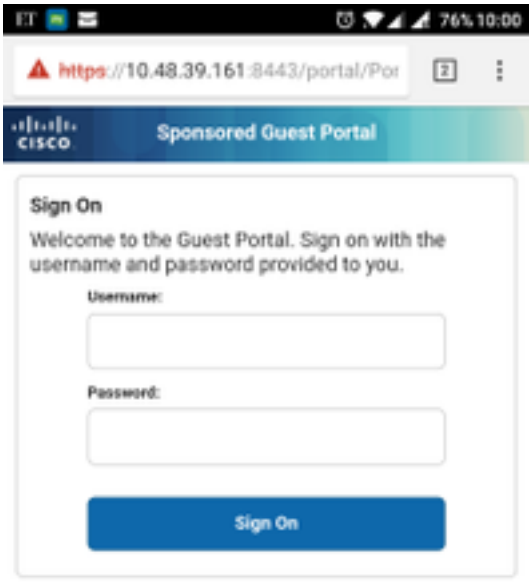
WLAN设置

步骤7 ：配置WLAN

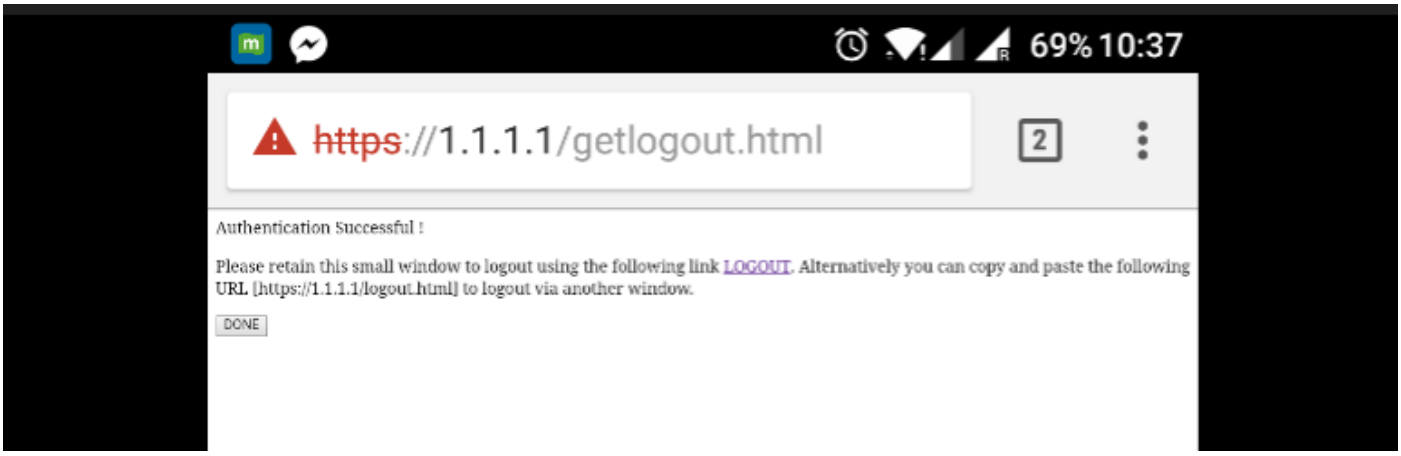


验证

联络客户端并且确保，如果打开浏览器，客户端将重定向对您的登录入口页面。下面的屏幕画面说明ISE访客入口页面。



一旦适当的凭证提交，成功页将显示：



ISE服务器将报告两验证：一在guest页本身(与仅用户名的最后一行)和秒钟验证，一旦WLC通过RADIUS验证(仅此验证提供相同用户名/密码将使客户端移动向成功相位)。如果RADIUS验证(与MAC地址和WLC详细信息作为NAS)不出现， RADIUS配置将验证。