与交换机和身份服务引擎配置示例的中央Web认证

Contents

Introduction

本文描述如何用有线客户端配置中央Web认证被联络到交换机在身份服务引擎(ISE)帮助下。

中央Web认证的概念被反对本地Web认证，是在交换机的通常Web认证。在该系统中，在dot1x/mab故障，交换机故障切换对webauth配置文件和重定向客户端的流量到在交换机的一个网页。

中央Web认证提供可能性有作为Web门户的一个中央设备(在Th是示例， ISE)。主要区别与通常本地Web认证比较是被转移与mac/dot1x认证一起分层堆积2。概念也有所不同因为RADIUS服务器(在本例中的ISE)返回表明到交换机的特殊属性Web重定向必须发生。此解决方案有排除的优点是必要为了Web认证能插入的所有延迟。全局，如果客户端工作站的MAC地址不由RADIUS服务器(但是其他标准知道能也使用)，服务器回归重定向属性，并且交换机核准位置(通过MAC验证旁路[MAB])，但是放置访问列表重定向Web数据流到门户。一旦在客户门户的用户登录，它通过CoA(授权的更改是可能)重新启动交换端口，以便一个新的第2层MAB认证出现。ISE能然后切记它是webauth用户和适用第2层属性(类似动态范assignment)于用户。ActiveX组件能也强制客户端PC机刷新其IP地址。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)
- Cisco IOS交换机配置

Components Used

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎(ISE)，版本1.1.1
- 运行软件版本12.2.55SE3的Cisco Catalyst 3560 Series Switch

  Note:程序为其他Catalyst交换机型号是类似或相同的。您能除非陈术否则使用在所有Cisco IOS Software Releases的这些步骤Catalyst。

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.

Configure

概述

ISE配置被做这五个步骤：

1. 创建可下载的访问控制表(ACL)。
2. 创建授权配置文件。
3. 创建一个认证规则。
4. 创建一个授权规则。
5. Enable (event) IP续订(可选)。

创建可下载的ACLS

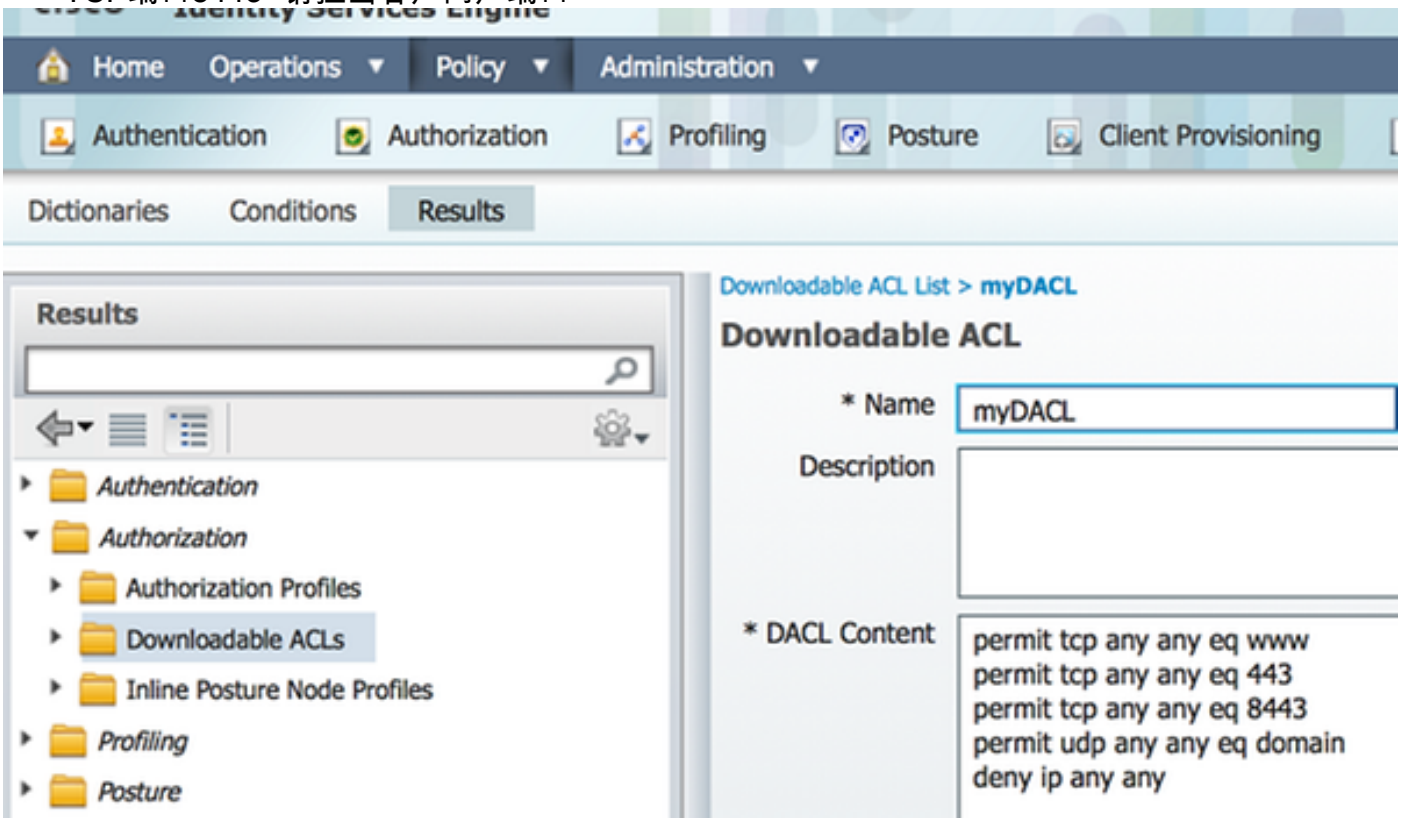
这不是一个必须的步骤。用中央webauth配置文件传送的重定向ACL确定哪数据流(HTTP或HTTPS)重定向对ISE。可下载的ACLS允许您定义什么数据流允许。您应该典型地允许DNS，HTTP和8443和拒绝其余。否则，交换机重定向HTTP数据流，但是允许其他协议。

完成这些步骤为了创建可下载的ACLS ：

1. 点击**策略**，并且点击**策略元素**。
2. 点击**结果**。
3. 扩展**授权**，并且点击**可下载的ACLs**。
4. 点击**Add按钮**为了创建新的可下载的ACLS。
5. 在名称字段，请输入一个名字对于DACL。此示例使用*myDACL*。

此镜像显示典型的DACL内容，准许：

- DNS解析ISE门户主机名-
- HTTP和HTTPS -请允许重定向
- TCP端口8443 -请担当客户门户端口

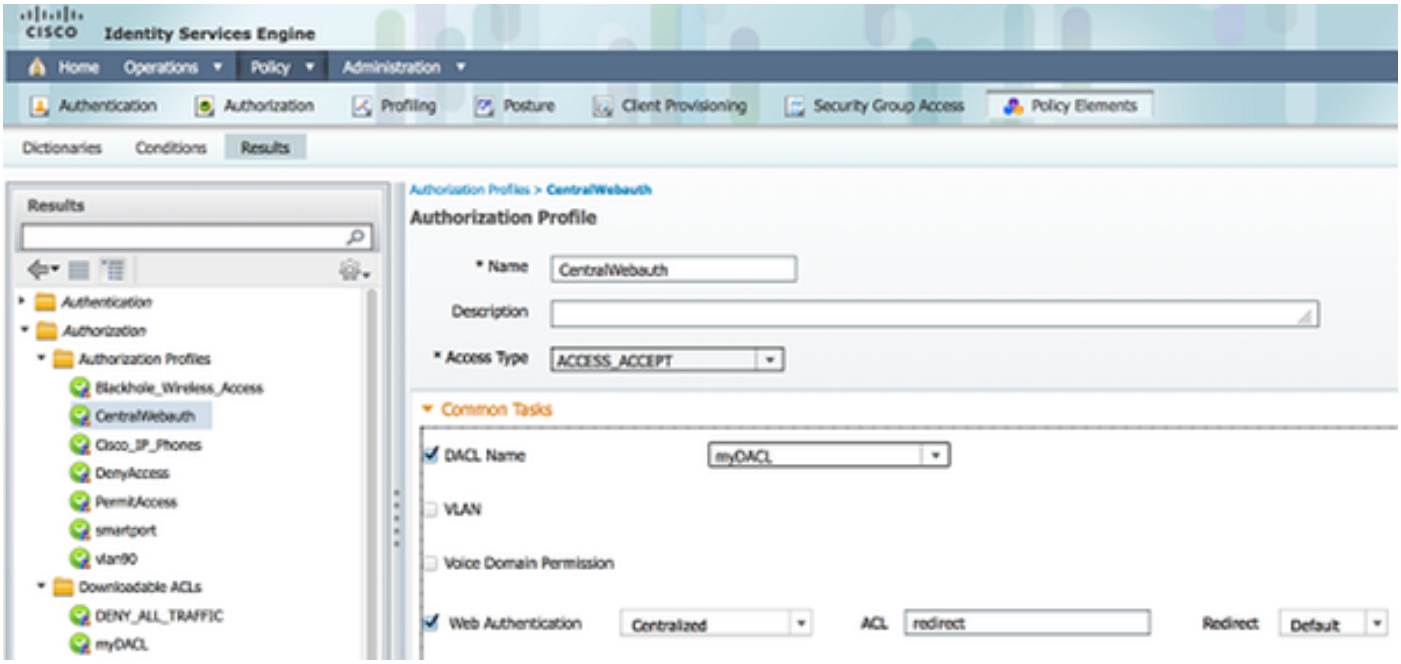


创建授权配置文件

完成这些步骤为了创建授权配置文件：

1. 点击**策略**，并且点击**策略元素**。
2. 点击**结果**。
3. 扩展**授权**，并且点击**授权配置文件**。
4. 点击**Add按钮**为了创建中央webauth的一个新的授权配置文件。
5. 在名称字段，请输入一个名字对于配置文件。此示例使用*CentralWebauth*。
6. 从访问类型下拉列表选择**ACCESS_ACCEPT**。
7. 检查**Web认证**复选框，并且从下拉列表选择**集中化**。
8. 在ACL字段，请输入ACL的名字在定义了将重定向的数据流的交换机的。此示例使用*重定向*。
9. 从重定向下拉列表选择**默认值**。
10. 如果决定使用DACL而不是在交换机的静态端口ACL请检查**DACL名字**复选框，并且从下拉式lsit选择**myDACL**。

重定向属性定义了ISE是否看到ISE admin创建的默认Web门户或一个自定义Web门户。例如，在本例中的*重定向*ACL触发从客户端的重定向在HTTP或HTTPS流量到任何地方。ACL在交换机后被定义在此配置示例。

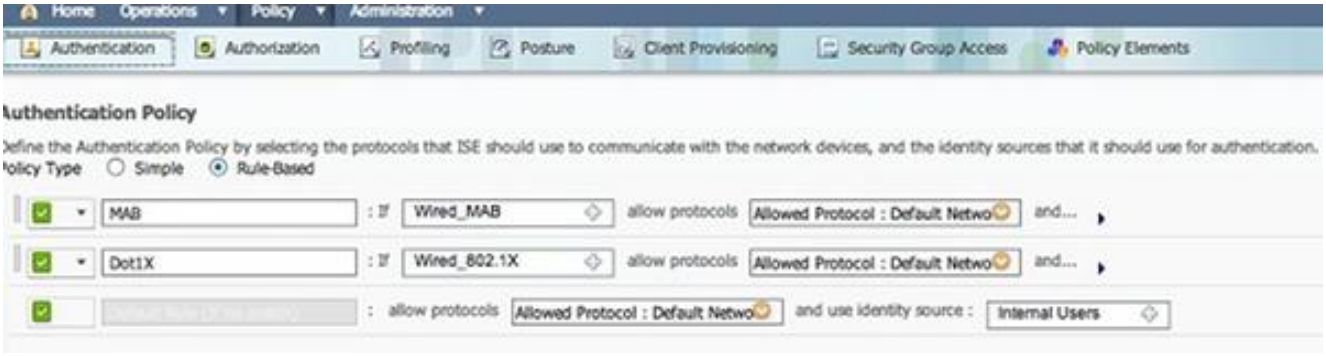


创建认证规则

完成这些步骤为了使用认证配置文件创建认证规则：

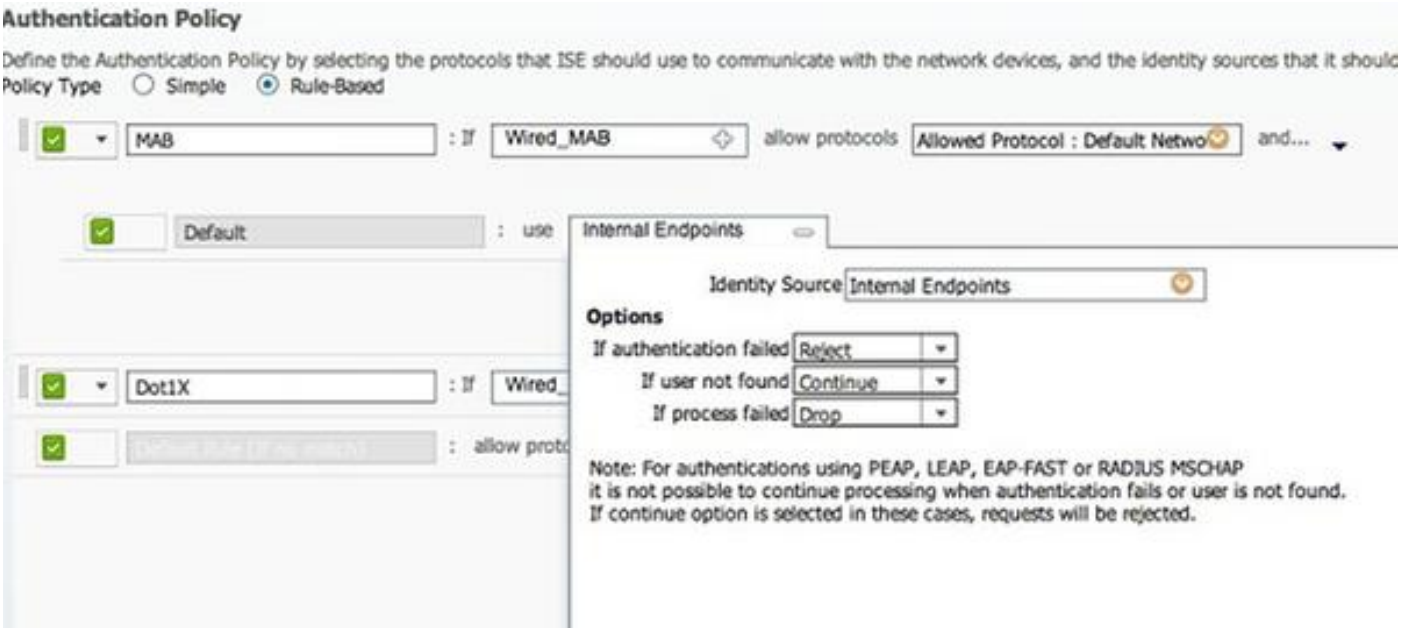
1. 在策略菜单下，请点击**认证**。

   此镜像显示示例如何配置认证策略规则。在本例中的规则触发配置，当发现时MAB。



2. 输入一个名字对于您的认证规则。此示例使用*MAB*。
3. 选择正(+)在的图标，如果情况字段。
4. 选择**复合条件**，并且选择**Wired_MAB**。
5. 点击箭头被找出在旁边**和…**为了进一步扩展规则。
6. 点击**+**在身份Source字段的图标，并且选择**内部终端**。
7. 选择从**继续**‘如果用户没被找到的’下拉列表。

   此选项允许设备验证(通过webauth)，即使其MAC地址不知道。Dot1x客户端仍然验证与他们的证件，并且不应该牵涉到此配置。



创建授权规则

当前有配置的几个规则在授权策略。当接通PC时，通过MAB;假设， MAC地址不知道，因此webauth和ACL返回。此*MAC没已知*规则在此镜像显示和在此部分被配置：

完成这些步骤为了创建授权规则：

1. 创建一新规则，并且输入名字。此示例使用没*已知的MAC*。
2. 点击正(+)在情况字段的图标，并且选择创造新的条件。
3. 扩展**表达式**下拉列表。
4. 选择**网络访问**，并且扩展它。
5. 点击**AuthenticationStatus**，并且选择**等于**运算符。
6. 选择在右边的字段的**UnknownUser**。
7. 在一般授权页，请在*然后*词右边选择**CentralWebauth** (授权配置文件)在字段。

   此步骤允许ISE继续，即使用户(或MAC)不知道。

   未知用户当前向用户显示登录页。然而，一旦他们输入他们的证件，他们再看到在ISE的认证请求;因此，必须配置有另一个规则符合的情况，如果用户是客人身份的用户。在本例中，*如果UseridentityGroup*使用*等于客户*和它假设，所有客户属于此组。
8. 点击Action按钮查找在*MAC没已知*规则结束时，并且选择插入上面新规则。

   Note:重要的是非常此新规则在*MAC没已知*规则前来。
9. 输入一个名字对于新规则。此示例使用是*客户*。
10. 选择匹配您的客人身份的用户的情况。

    此示例使用*InternalUser ：IdentityGroup等于客户*，因为所有客人身份的用户一定对*客户*组(或您在您的赞助商设置配置)的另一个组。

11. 选择在结果机箱的**PermitAccess** (位于在词右边*然后*)。

    当用户在登录页时被认证， ISE重新启动在交换端口的一个第2层认证，并且新的MAB发生。在此方案中，区别是一个无形的标志位设置为了ISE能记得它是一个客户验证的用户。此规则是*第2个AUTH*，并且情况是*网络访问：UseCase等于GuestFlow*。此情况符合，当用户通过webauth时验证，并且交换端口为新的MAB再设置。您能分配您喜欢的所有属性。此示例分配配置文件*vlan90*，以便用户分配在他的第二个MAB认证的VLAN90。
12. 点击**动作**(位于在是客户规则结束时)，并且选择**上面插入新规则**。
13. 输入**第2个AUTH**在名称字段。
14. 在情况字段，请点击正(+)图标，并且选择创造新的条件。
15. 选择**网络访问**，并且点击**UseCase**。
16. 选择**等于**作为运算符。
17. 选择**GuestFlow**作为正确的操作数。
18. 在授权页，请点击正(+)图标(位于在*然后旁边*)为了选择您的规则的一个结果。

    在本例中，一个预先配置的配置文件(vlan90)分配;此配置在本文没有显示。

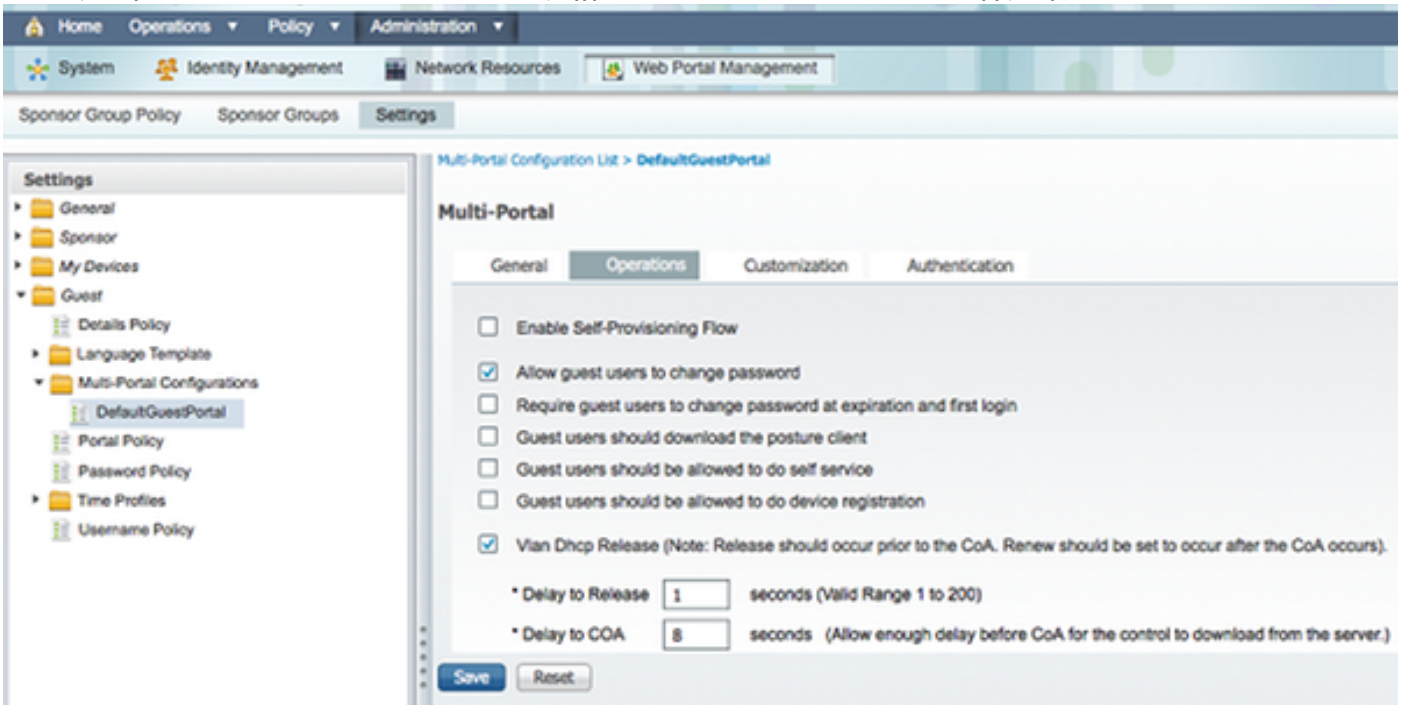
    您能选择**许可证访问**选项或创建一个自定义配置文件为了返回您喜欢的VLAN或属性。

Enable (event) IP续订(可选)

如果分配VLAN，最终步骤是为了客户端PC机能更新其IP地址。此步骤由Windows客户端的客户门户达到。如果没有设置*第2个AUTH*规则的VLAN前，您能跳到此步骤。

如果分配VLAN，请完成这些步骤为了enable (event) IP续订：

1. 点击**管理**，并且点击**客户管理**。
2. 单击**设置**。
3. 扩展**客户**，并且扩展多**PORTAL配置**。
4. 点击**DefaultGuestPortal**或您可能创建了一个自定义门户的名字。
5. 点击**VLAN DHCP Releasecheck**机箱。 **Note**:此选项为Windows客户端仅工作。



交换机配置(摘要)

此部分提供交换机配置的摘要。请参阅交换机配置(充分)关于完全配置。

此示例显示一种简单的MAB配置。

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 100是VLAN该提供充分的网络连通性。默认端口ACL (已命名*webauth*)是适用和定义成显示这里：

```
ip access-list extended webauth
permit ip any any
```

此配置示例提供充分的网络访问，即使用户没有验证;因此，您也许要限制对未认证的用户的访问。

在此配置中， HTTP和HTTPS访问不工作没有认证(每个另一个ACL)，因为配置ISE使用重定向ACL (已命名*重定向*)。这是在交换机的定义：

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

在交换机在哪数据流必须定义此访问列表为了定义交换机将执行重定向。(它在*许可证*配比。)在本例中、客户端发送触发器Web重定向的任何HTTP或者HTTPS流量。此示例也拒绝ISE IP地址，因此对ISE的数据流在循环去ISE，并且不重定向。(在此方案，请拒绝不阻塞数据流;它就是不重定向数据流。)如果使用异常的HTTP端口或一个代理，您能添加其他端口。

另一种可能性是允许HTTP访问到一些网站和重定向其他网站。例如，如果在ACL定义了仅内部Web服务器的一个许可证，客户端可能访问Web，无需验证，但是遇到重定向，如果他们设法访问一内部Web服务器。

最后一步是允许在交换机的CoA。否则， ISE不能强制交换机重新鉴别客户端。

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

此命令对于交换机是必需的重定向基于HTTP数据流：

```
ip http server
```

要求此命令重定向基于HTTPS流量：

```
ip http secure-server
```

这些命令也是重要的：

```
radius-server vsa send authentication
radius-server vsa send accounting
```

如果用户没有验证， **show authentication会话int <interface num>**返回此输出：

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Note:尽管一个成功的MAB认证，重定向ACL，因为MAC地址不由ISE，知道放置。

交换机配置(充分)

此部分列出充分的交换机配置。一些多余的接口和命令行被省略;因此，应该用于此配置示例仅参考并且不应该复制。

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
```

```
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

HTTP代理配置

如果使用一个HTTP代理您的客户端，意味着您的客户端：

- 请使用一个非常规的端口HTTP协议
- 发送所有他们的数据流到该代理

为了安排交换机监听在非常规的端口(例如， 8080)，请使用这些命令：

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

您也需要配置所有客户端继续使用他们的代理，但是不使用代理ISE IP地址。所有浏览器包括允许您输入主机名或IP地址不应该使用代理的一个功能。如果不添加ISE的例外，您遇到循环认证页。

您在代理端口(8080也需要修改您的重定向ACL允许在本例中)。

关于交换机SVIs的注意事项

此时，交换机需要Switch Virtual Interface (SVI)为了回复客户端和发送Web门户重定向到客户端。此SVI不一定必须在客户端子网/VLAN。然而，如果交换机没有SVI在客户端子网/VLAN，它必须使用另一SVIs中的任一和发送数据流如对客户端路由表定义。这典型地意味着数据流被发送到在网络的核心的另一个网关;此数据流回来到接入交换机在客户端子网里面。

典型防火墙块数据流从和对同一台交换机，正如在此方案，因此重定向也许不适当地运作。解决方法是允许在防火墙的此工作情况或创建在接入交换机的一SVI在客户端子网。

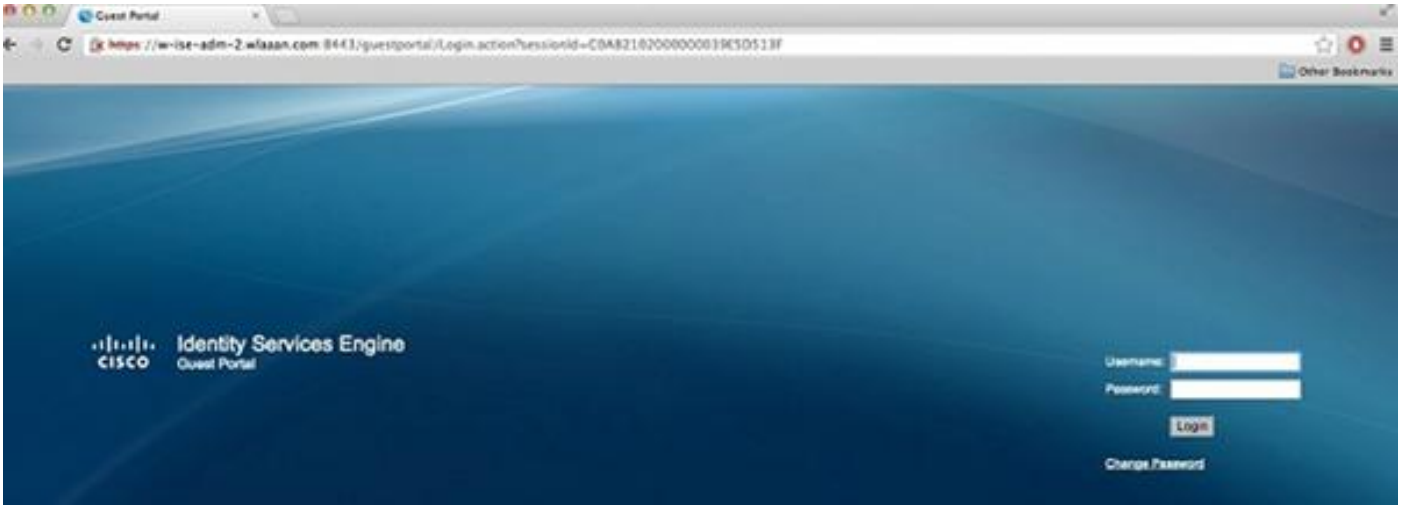
关于HTTPS重定向的注意事项

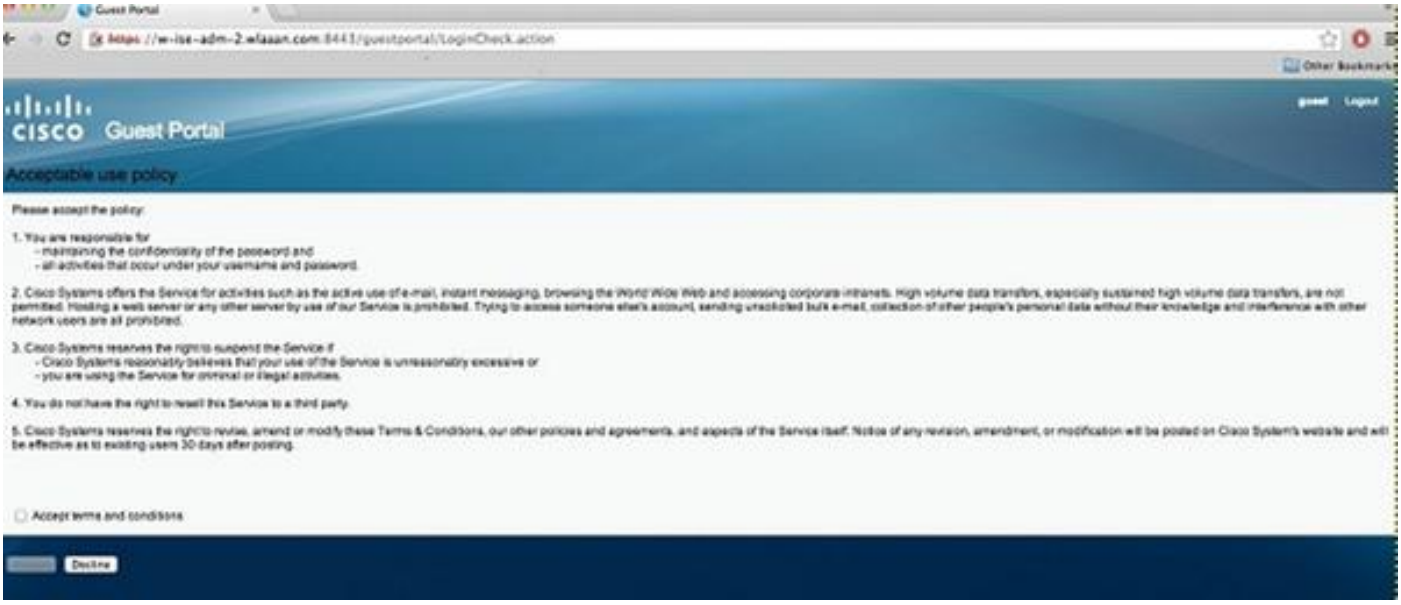
交换机能重定向HTTPS流量。因此，如果客户客户端有主页在HTTPS，重定向正确地发生。

重定向的全部的概念根据事实设备(在这种情况下，交换机)伪装网站IP地址。然而，一个主要问题出现，当交换机拦截并且重定向HTTPS流量，因为交换机能提交其唯一在传输层安全(TLS)握手的自己的认证。因为这不是和一样网站最初请求的认证，多数浏览器问题主要戒备。浏览器正确地处理另一个认证的重定向和介绍作为安全性问题。没有解决方法的此和没有办法的伪装的交换机您的原始网站认证。

最终结果

客户端PC机接通并且执行MAB。MAC地址不知道，因此ISE推进重定向属性回到交换机。用户设法去网站和重定向。





当登录页的认证是成功的时， ISE通过授权的更改重新启动连接孔，再开始第2层MAB认证。

然而， ISE知道它是一个前webauth客户端并且核准根据webauth证件的客户端(虽然这是第2层认证)。

在ISE认证日志， MAB认证出现于日志的底部。虽然它未知， MAC地址验证并且被描出了，并且webauth属性返回了。其次，认证发生在用户的用户名(即用户类型他的在登录页的证件)。在认证之后，一个新的第2层认证发生在用户名作为证件;此认证步骤是您能回来归因于这样动态VLAN的地方。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- 思科身份服务引擎
- 思科身份服务引擎命令参考指南
- ISE (身份服务引擎)的集成与Cisco WLC (无线局域网控制器)
- 请求注解 (RFC)
- Technical Support & Documentation - Cisco Systems