与交换机和身份服务引擎配置示例的中央Web验证

目录

简介

本文描述如何配置与有线的客户端的中央Web验证连接对交换机在身份服务引擎(ISE)帮助下。

中央Web验证的概念被反对本地Web验证，是在交换机的通常Web验证。在该系统中，在dot1x/mab失败，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验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验证比较是被转移到Layer2与mac/dot1x验证一起。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验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，并且交换机授权站点(通过MAC验证旁路[MAB])，但是放置访问列表重定向Web流量到门户。一旦在访客门户的用户登录，它通过CoA (授权的崔凡吉莱是可能)重新启动交换机端口，以便一新的Layer2 MAB验证出现。ISE能然后记住它是webauth用户和适用Layer2属性(类似动态范assignment)对用户。ActiveX组件能也强制客户端PC刷新其IP地址。

先决条件

要求

Cisco 建议您了解以下主题：

- 身份服务引擎(ISE)
- Cisco IOS交换机配置

使用的组件

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系列交换机

  注意：步骤为其他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软件版本的这些步骤Catalyst。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

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. 创建验证规则。
4. 创建授权规则。
5. 启用IP续订(可选)。

创建可下载的ACLs

这不是一个必须步骤。重定向ACL退还与中央webauth配置文件确定哪个流量(HTTP或HTTPS)重定向对ISE。可下载的ACLs允许您定义什么流量允许。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。

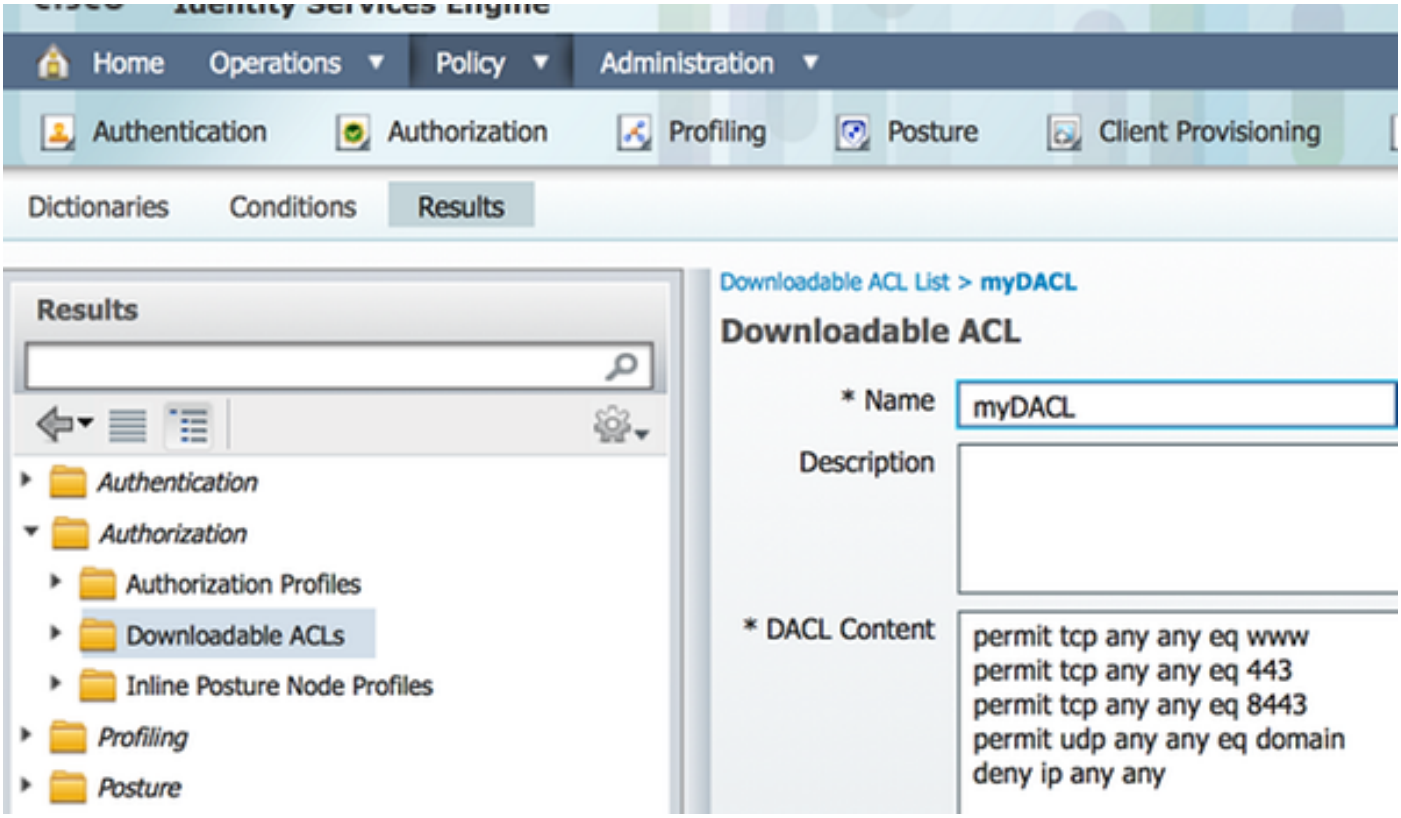
完成这些步骤为了创建可下载的ACLs ：

1. 点击**策略**，并且点击**策略元素**。
2. 点击**结果**。
3. 展开**授权**，并且点击**可下载的ACLs**。
4. 点击**Add按钮**为了创建一个新的可下载的ACLs。
5. 在**Name字段**，请输入一名称对于DACL。此示例使用*myDACL*。

此镜像显示典型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 -请担当访客门户端口

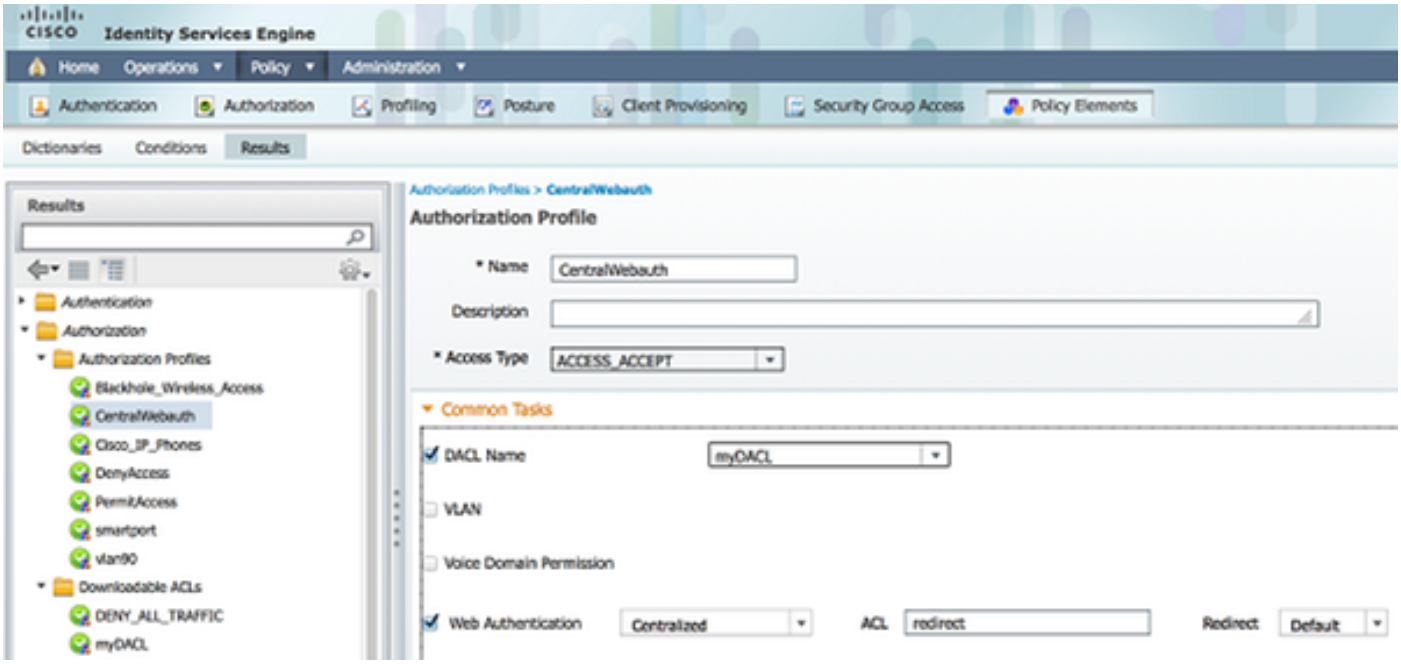


创建授权配置文件

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. 展开**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的一新的授权配置文件。
5. 在**Name字段**，请输入一名称对于配置文件。此示例使用*CentralWebauth*。
6. 从访问类型下拉列表选择**ACCESS_ACCEPT**。
7. 检查**Web验证**复选框，并且从下拉列表选择**集中化**。
8. 在ACL字段，请输入ACL的名称在定义了将重定向的流量的交换机的。此示例使用*重定向*。
9. 从重定向下拉列表选择**默认**。
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名称**复选框，并且从下拉式lsit选择**myDACL**。

重定向属性定义了ISE是否看到默认Web的万维网门户或该一个自定义的Web门户ISE admin创建。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在交换机定义后在本例中配置示例。

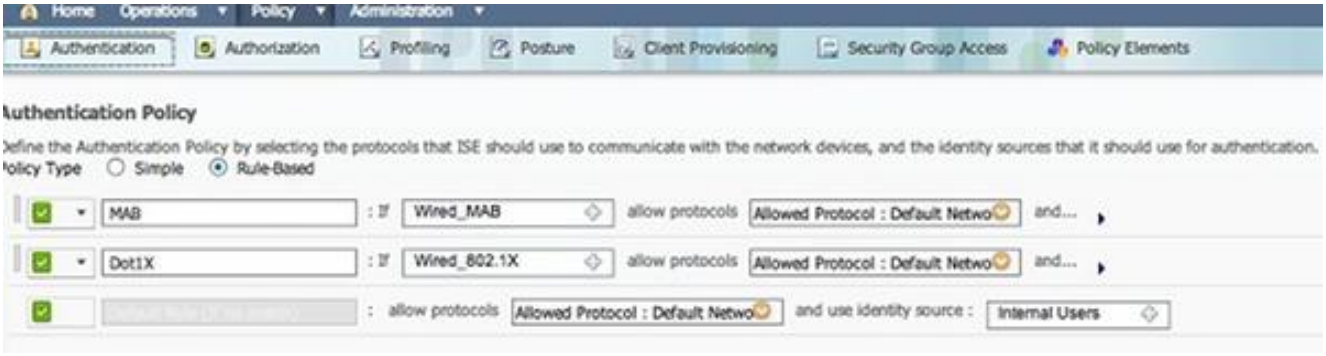


创建验证规则

完成这些步骤为了使用验证配置文件创建验证规则：

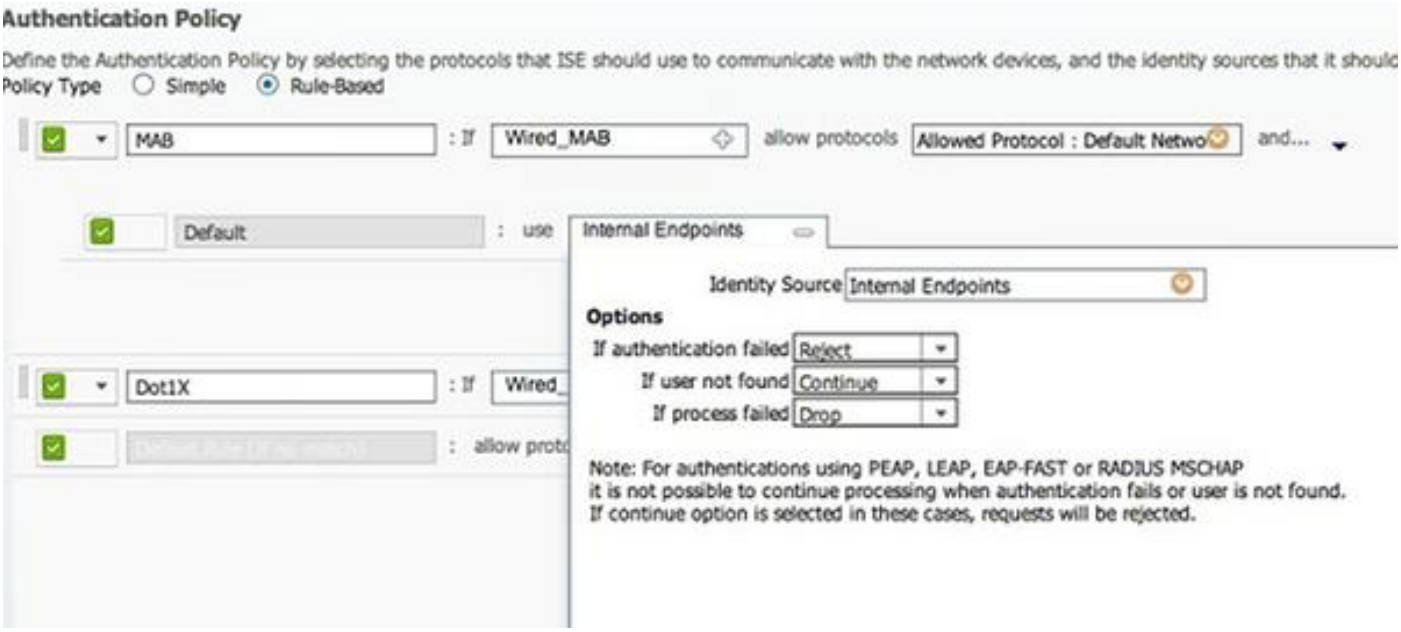
1. 在策略菜单下，请点击**验证**。

   此镜像显示示例如何配置验证策略规则。在本例中，触发的规则配置，当MAB检测时。



2. 输入一名称对于您的验证规则。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. 点击箭头查找在旁边**和…**为了进一步展开规则。
6. 点击**+**在标识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。

   此选项允许将验证的设备(通过webauth)，即使其MAC地址不知道。Dot1x客户端仍然验证与他们的凭证，并且不应该牵涉到此配置。



创建授权规则

当前有几个规则配置在授权策略。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*规则在此镜像在此部分显示和配置：

完成这些步骤为了创建授权规则：

1. 创建新规则，并且输入名称。此示例使用没*已知的MAC*。
2. 在情况字段点击正(+)图标，并且选择创造新的条件。
3. 展开**表达式**下拉列表。
4. 选择**网络访问**，并且展开它。
5. 点击**AuthenticationStatus**，并且选择**等于**操作员。
6. 在右边的字段选择**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。

   未知用户当前提交与登录页。然而，一旦他们输入他们的凭证，他们再提交与在ISE的认证请求;因此，必须配置另一个规则以符合的情况，如果用户是来宾用户。在本例中，*如果UseridentityGroup*使用*等于访客*和它假设，所有访客属于此组。
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。

   注意：重要的是非常此新规则来，在*MAC没已知*规则前。
9. 输入一名称对于新规则。此示例使用是*访客*。
10. 选择匹配您的来宾用户的情况。

    此示例使用*InternalUser ：IdentityGroup等于访客*，因为所有来宾用户一定给*访客*组(或您在您的赞助商设置配置)的另一组。

11. 选择在结果方框的**PermitAccess** (查找在词右边*然后*)。

    当用户在登录页时授权， ISE重新启动在交换机端口的一Layer2验证，并且新的MAB发生。在此方案中，差异是一隐身标志设置为了ISE能记住它是一个访客验证的用户。此规则是*第2验证*，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，并且交换机端口为新的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MAB验证的VLAN90。
12. 点击**操作**(查找在是访客规则结束时)，并且选择**上面插入新规则**。
13. 在Name字段进入**第2验证**。
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**作为操作员。
17. 选择**GuestFlow**作为正确的操作数。
18. 在授权页，请点击正(+)图标(查找在*然后旁边*)为了选择您的规则的一种结果。

    在本例中，一预先配置的配置文件(vlan90)分配;此配置在本文没有显示。

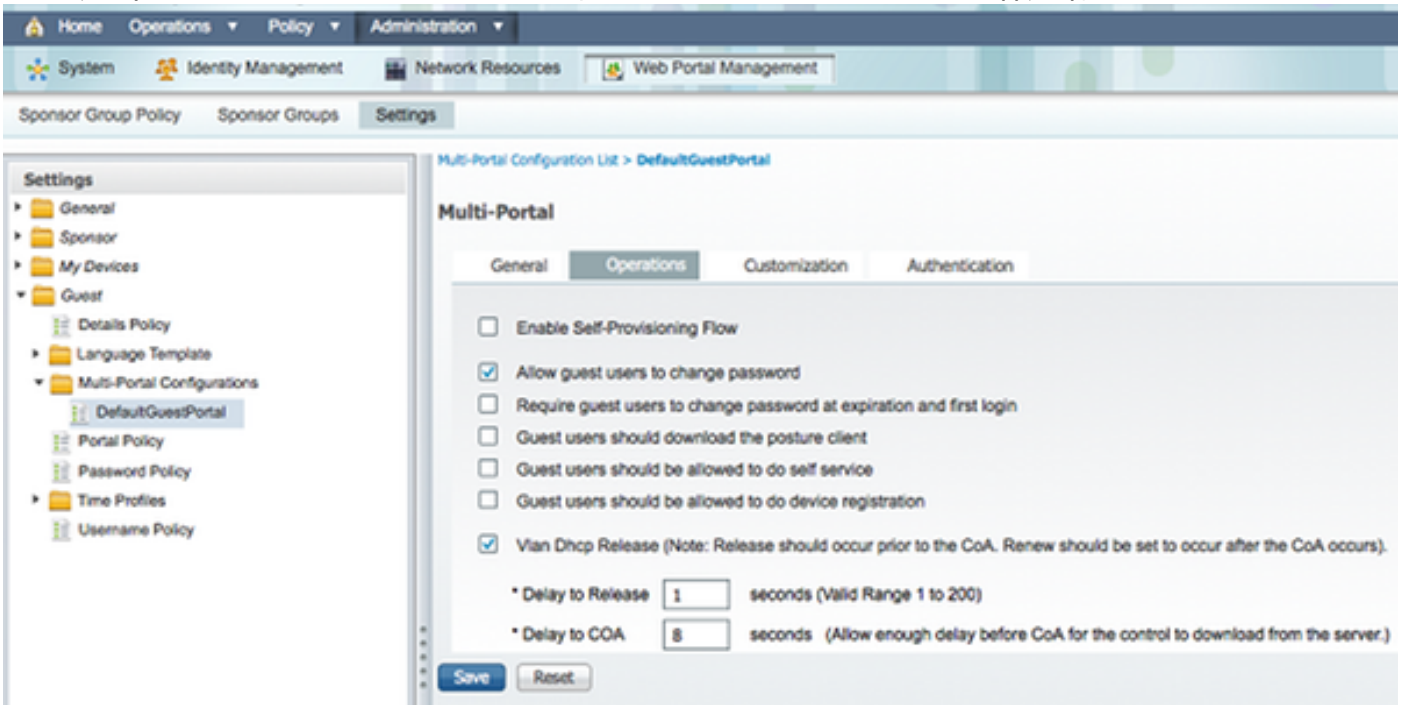
    您能选择**Permit访问**选项或创建一自定义配置文件为了返回您喜欢的VLAN或属性。

启用IP续订(可选)

如果分配VLAN，最后一步是为了客户端PC能更新其IP地址。此步骤由Windows客户端的访客门户达到。如果没有设置*第2个验证*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启用IP续订：

1. 点击**管理**，并且点击**访客管理**。
2. 单击**设置**。
3. 展开**访客**，并且扩展多**PORTAL配置**。
4. 点击**DefaultGuestPortal**或您可能创建一个自定义门户的名称。
5. 点击**VLAN DHCP Releasecheck**方框。 **注意**：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(全双工)关于完全配置。

此示例显示一简单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该提供全双工网络连通性。默认端口ACL (已命名*webauth*)应用并且定义作为显示此处：

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

此配置示例提供全双工网络访问，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浏览不工作没有验证(每个另一个ACL)，因为ISE配置使用重定向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
```

在交换机在哪个流量必须定义此访问列表为了定义交换机将执行重定向。(它在*permit*配比。)在本例中、任何HTTP或者HTTPS流量客户端发送触发Web重定向。此示例也拒绝ISE IP地址，因此对ISE的流量在环路去ISE，并且不重定向。(在此方案，请拒绝不阻塞流量;它就是不重定向流量。)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定义了仅内部网络服务器的一permit，客户端可能浏览Web，无需验证，但是遇到重定向，如果他们设法访问内部网络服务器。

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>
```

此命令要求为了交换机能重定向基于HTTP数据流：

```
ip http server
```

此命令要求重定向基于HTTPS流量：

```
ip http secure-server
```

这些命令也是重要：

```
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
```

注意：尽管一成功的MAB验证，重定向ACL，因为MAC地址不由ISE，知道放置。

交换机配置(全双工)

此部分列出全交换的配置。一些多余的接口和命令行省略;因此，应该用于此配置示例仅参考并且不应该复制。

```
Building configuration...

Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
```

```
!
!
!
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
vtp interface Vlan61
udld enable

nmsp enable
ip routing
ip dhcp binding cleanup interval 600
!
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsakeypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
```

```
!
!
!
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
!
ip sla enable reaction-alerts
logging esm config
logging trap warnings
logging facility auth
logging 10.48.76.31
snmp-server community c3560public RO
snmp-server community c3560private RW
snmp-server community private RO
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send authentication
radius-server vsa send accounting
!
!
!
privilege exec level 15 configure terminal
privilege exec level 15 configure
privilege exec level 2 debug radius
privilege exec level 2 debug aaa
privilege exec level 2 debug
!
line con 0
line vty 0 4
exec-timeout 0 0
password Cisco123
authorization commands 1 MyTacacs
authorization commands 2 MyTacacs
authorization commands 15 MyTacacs
authorization exec MyTacacs
login authentication MyTacacs
line vty 5 15
!
ntp server 10.48.76.33
end
```

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
- 发送所有他们的流量给该代理

为了安排交换机侦听在非常规的端口(例如， 8080)，请使用这些命令：

```
ip http port 8080
ip port-map http port 8080
```

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功能。如果不添加ISE的例外，您遇到环路验证页。

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的重要提示

此时，交换机需要Switch Virtual Interface (SVI)为了应答对客户端和发送Web门户重定向对客户端。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中的任一和发送流量如对客户端路由表定义。这典型地含义流量发送到在网络的核心的另一个网关;此流量回来到接入交换机在客户端子网里面。

典型防火墙块流量从和对同一交换机，正如在此方案，因此重定向也许不适当地运作。应急方案是允许在防火墙的此行为或创建在接入交换机的一SVI在客户端子网。

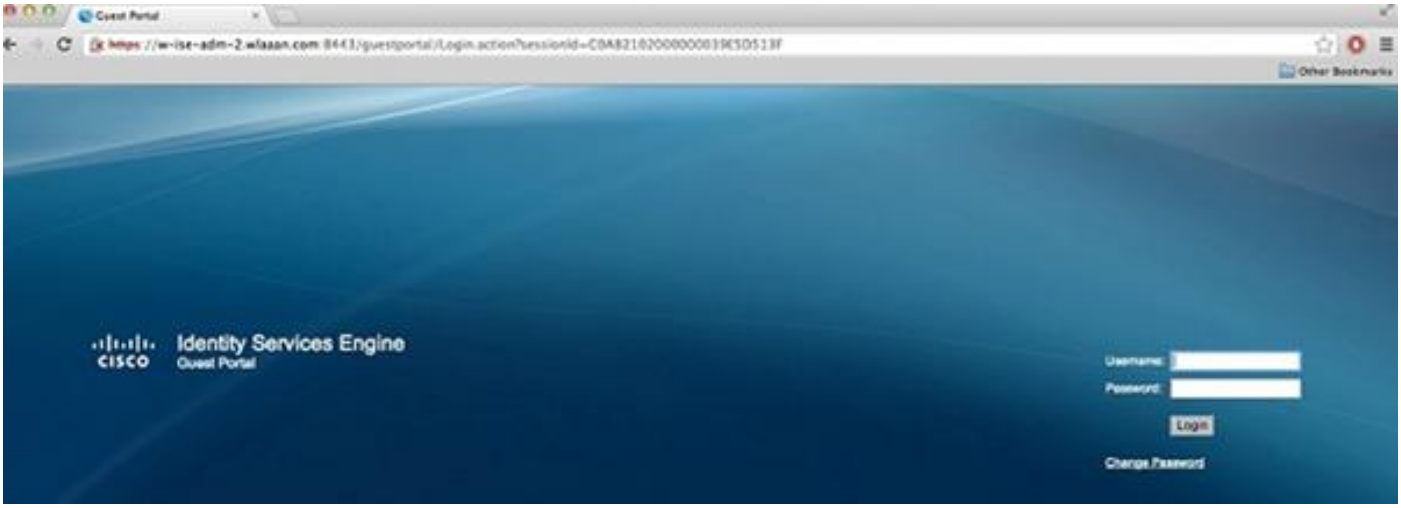
关于HTTPS的重定向的重要提示

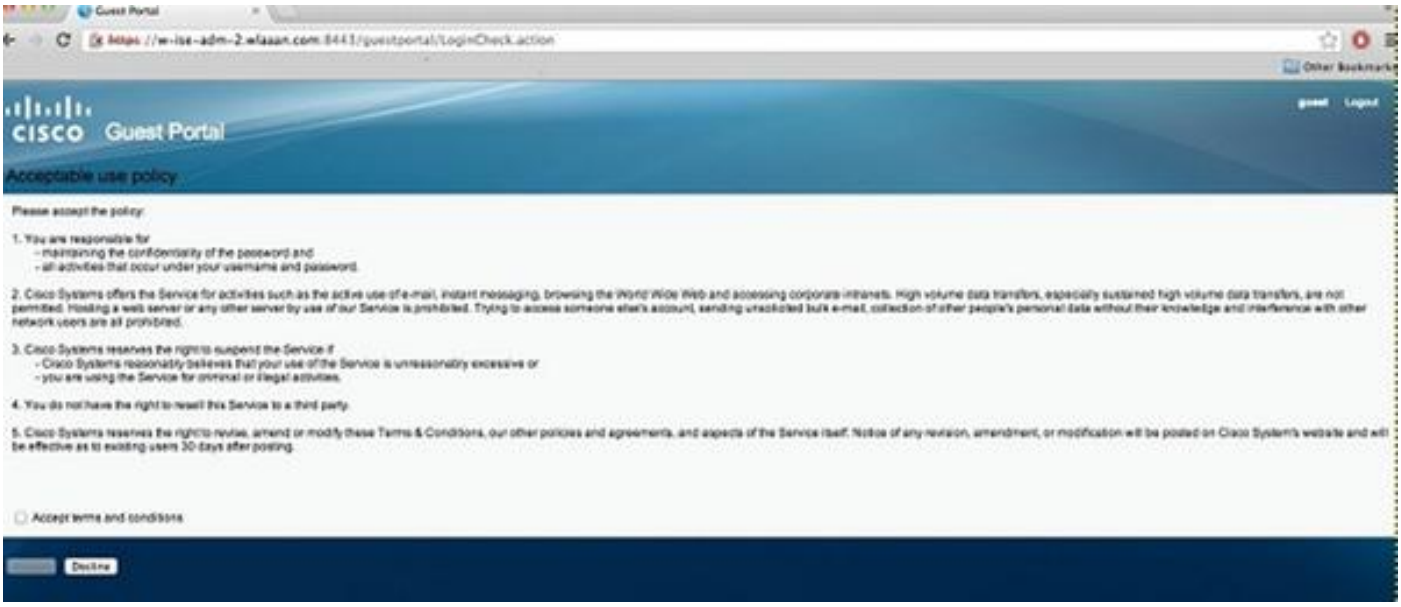
交换机能重定向HTTPS流量。因此，如果访客客户端有主页在HTTPS，重定向正确地发生。

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，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)握手的自己的证书。因为这不是证书和一样网站最初请求，多数浏览器问题主要警报。浏览器正确地处理另一证书的重定向和演示作为安全性问题。没有应急方案此的和没有办法交换机的能伪装您的原始网站证书。

最终结果

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





当登录页的验证是成功的时， ISE通过授权的崔凡吉莱重新启动switchport，再开始Layer2 MAB验证。

然而， ISE知道它是一个前webauth客户端并且授权根据webauth凭证的客户端(虽然这是Layer2验证)。

在ISE验证日志， MAB验证在日志的底部出现。虽然它未知， MAC地址验证并且被描出了，并且webauth属性返回。其次，验证发生在用户的用户名(即用户类型他的在登录页的凭证)。在验证之后，一新的Layer2验证发生在用户名作为凭证;此验证步骤是您能回来归因于这样动态VLAN的地方。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 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)的集成与思科WLC (无线局域网控制器)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems