与FlexConnect AP的中央Web验证在与ISE配置示例的一WLC

目录

简介

本文描述如何配置中央Web验证用FlexConnect接入点(AP)在一个无线局域网控制器(WLC)用身份服务引擎(ISE)在本地交换模式。

重要说明：此时，在FlexAPs的本地认证不为此方案支持。

其他文档此系列

- 与交换机和身份服务引擎配置示例的中央Web验证
- 在WLC和ISE配置示例的中央Web验证

先决条件

要求

本文档没有任何特定的要求。

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1.2.1
- 无线局域网控制器软件，发行版本- 7.4.100.0

配置

有配置在无线局域网控制器(WLC)的中央Web验证的多种方法。第一种方法是WLC重定向HTTP数据流到内部或外部服务器用户提示验证的本地Web验证。WLC然后拿来凭证(被退还的通过一旦外部服务器的一HTTP GET请求)并且做RADIUS验证。一旦来宾用户，外部服务器(例如身份服务引擎(ISE)或美洲台访客服务器(NGS))要求作为门户提供功能例如设备注册和赛弗供应。此进程包括这些步骤：

1. 用户关联对Web验证SSID。
2. 用户打开他们的浏览器。
3. 对访客门户的WLC重定向(例如ISE或NGS)，当URL被输入。
4. 用户在门户验证。
5. 回到WLC的访客门户重定向与被输入的凭证。
6. WLC通过RADIUS验证来宾用户。
7. 回到原始URL的WLC重定向。

此进程包括很多重定向。新的方法将使用与ISE的中央Web验证(后版本一起使用比1.1)和WLC (后版本比7.2)。此进程包括这些步骤：

1. 用户关联对Web验证SSID。
2. 用户打开他们的浏览器。
3. 对访客门户的WLC重定向。
4. 用户在门户验证。
5. ISE发送RADIUS授权(CoA崔凡吉莱- UDP波尔特1700)表明到控制器用户有效和最终推送RADIUS属性例如访问控制表(ACL)。
6. 用户是被提示的重试原始URL。

此部分描述必要步骤配置在WLC和ISE的中央Web验证。

网络图

此配置使用以下网络设置：

WLC 配置

WLC配置是相当简单的。“窍门？使用(同一样在交换机)从ISE获取动态验证URL。(因为它使用CoA，会话需要创建作为会话ID是URL的一部分。)SSID配置使用过滤的MAC，并且ISE配置返回Access-Accept消息，即使没找到MAC地址，以便发送所有用户的重定向URL。

另外，必须启用RADIUS网络准入控制(NAC)和AAA覆盖。RADIUS美洲台允许ISE发送指示的CoA请求用户当前验证并且能访问网络。它也使用ISE更改根据状态结果的用户配置文件的状态评估。

1. 保证RADIUS服务器有(CoA)启用的RFC3576，是默认。

2. 创建一新的WLAN。此示例创建名为*CWAFlex的*一新的WLAN并且分配它到vlan33。(请注意它不会有效果，因为接入点在本地交换模式。)

3. 在安全选项卡，过滤作为第2层安全的enable (event) MAC。

4. 在第3层选项卡，请保证安全禁用。(如果Web验证在第3层启用，本地Web验证启用，不中央Web验证。)

5. 在AAA服务器上请选中，选择ISE服务器作为WLAN的RADIUS服务器。随意地，您能为认为选择它为了有关于ISE的详细信息。

6. 在高级选项卡。，请保证允许AAA覆盖被检查，并且Radius NAC为NAC状态选择。

7. 创建重定向ACL。

   ThisACL被参考theISE Access-Accept消息并且定义了应该重定向不应该重定向什么流量(拒绝由theACL)以及什么流量(允许由theACL)。基本上， DNS和流量到/从theISE需要允许。 **注意**：与FlexConnect AP的一个问题是您必须创建FlexConnect ACL分别于您的正常ACL。此问题在Cisco Bug CSCue68065方面在版本7.5描述和修复。 在WLC 7.5及以后，仅FlexACL要求，并且标准ACL不是需要的。WLC预计ISE返回的重定向ACL是正常ACL。然而，保证它工作，您需要象FlexConnect ACL应用的同样ACL。
   此示例显示如何创建名为*flexred的*FlexConnect ACL ：

   创建规则允许DNS流量以及流量往ISE和拒绝其余。

   如果想要最大安全性，您能允许往ISE的仅端口8443。(如果摆姿势，您必须添加典型的状态端口，例如8905,8906,8909,8910。)

   (仅在版本7.5前的代码由于CSCue68065)请选择创建与同一名称的相同的ACL的**安全>访问控制列表**。

准备特定FlexConnect AP。注意为一更加大的部署，您典型地会使用FlexConnect组和不会执行根据一个每个AP基本类型的这些项目为可扩展性原因。

点击**无线**，并且选择特定接入点。点击**FlexConnect**选项卡，并且点击**外部Webauthentication ACL**。(在版本7.4之前，此选项被命名了*Web策略*。)

添加ACL (命名*flexred*在本例中)到Web政策方面。这PRE推进对接入点的ACL。它没有应用，但是ACL内容给对AP，以便能应用，当需要。

WLC配置当前完成。

ISE配置

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**，然后单击**策略元素**。
2. 点击**结果**。
3. 展开**授权**，然后单击**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Web验证**。
8. 在ACL字段，请输入定义了流量将重定向ACL的名称在WLC的。此示例使用*flexred*。
9. 从重定向下拉列表选择**默认**。

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*flexred* ACL触发重定向在从客户端的HTTP数据流到任何地方。

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，将触发的规则配置，当MAC过滤检测时。

2. 输入一名称对于您的验证规则。此示例使用*无线mab*。
3. 选择正(+)在的图标，如果情况字段。

4. 选择**复合条件**，然后选择**Wireless_MAB**。
5. 选择"Default network access"作为允许协议。
6. 点击箭头查找在旁边**和...**为了进一步展开规则。
7. 点击**+**在标识Source字段的图标，并且选择**内部终端**。
8. 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PC关联，将通过mac过滤;假设， MAC地址不知道，因此webauth和ACL返回。此*MAC没已知*规则在下面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. 在Name字段进入**第2验证**。
10. 选择标识组作为情况。此示例选择**访客**。
11. 在情况字段，请点击正(+)图标，并且选择创造新的条件。
12. 选择**网络访问**，并且点击**UseCase**。
13. 选择**等于**作为操作员。
14. 选择**GuestFlow**作为正确的操作数。这意味着您将捉住在网页登陆并且回来，在授权后的用户(规则的访客流零件的崔凡吉莱)，并且，只有当他们属于访客标识组。
15. 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(vlan34)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。

重要说明：在ISE Version1.3，根据Web验证种类，“访客流”用例也许不再遇到。授权规则然后将必须包含访客用户组作为唯一的可能的情况。

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。

注意在FlexConnect AP， VLAN在AP需要事先存在。所以，如果它不，您能创建在AP的一VLAN-ACL映射或在您不申请任何ACL新的VLAN的弹性组您要创建。那实际上创建VLAN (没有对此的ACL)。

如果分配VLAN，请完成这些步骤为了启用IP续订：

1. 点击**管理**，然后单击**访客管理**。
2. 单击**设置**。
3. 展开**访客**，然后扩展多**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 Release复选框**。**注意：** 此选项为Windows客户端仅工作。

通信流

了解能似乎难哪个流量在此方案的地方发送。这是一快速复核：

- 客户端发送在空气的关联申请SSID的。
- WLC处理过滤与ISE的MAC验证(其中接收重定向属性)。
- 在MAC过滤完成后，客户端只收到assoc答复。
- 客户端提交DHCP请求，并且那**本地**由接入点为了obain交换远程站点的IP地址。
- 在Central_webauth状态下，流量标记为在重定向典型ACL (因此HTTP拒绝)**在中央**交换。不因此执行重定向，但是WLC的它是AP;例如，当客户端请求所有网站时， AP发送此对在CAPWAP和网站IP地址和重定向往ISE的WLC欺骗封装的WLC。
- 客户端重定向对ISE重定向URL。(因为在弹性重定向ACL的permit点击)，这**本地**再交换。
- 一旦在运转状态，流量本地交换。

验证

一旦用户关联对SSID，授权在ISE页显示。

从底部，返回CWA属性的您能看到MAC地址过滤验证。其次与用户名的门户登录。ISE然后发送CoA对WLC，并且最后验证是过滤在WLC侧的第2层mac验证，但是ISE记住客户端和用户名并且应用我们在本例中配置的必要的VLAN。

当所有地址在客户端时打开，浏览器重定向对ISE。保证域名系统(DNS)正确地配置。

在用户接受策略后，网络访问授权。

在控制器、Policy Manager状态和RADIUS美洲台状态变换从*POSTURE_REQD*到*RAN*。