ISE版本1.3热点配置示例

目录

简介

思科身份服务引擎(ISE)版本1.3有访客门户呼叫的Hotspot新类型。此种门户允许您提供访客访问给网络，并且不迫使用户提供任何凭证。本文描述如何配置和排除故障此功能。

先决条件

要求

思科建议您有与ISE这些主题配置和基础知识的体验：

- ISE部署和访客流
- 无线局域网控制器(WLCs)的配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco WLC版本7.6和以上
- ISE软件，版本1.3和以上

拓扑和流

此方案是为接受Acceptable Use Policy (AUP)的来宾用户和那时给对互联网(或其他有限访问的)访问。

步骤1.服务集标识(SSID)的来宾用户关联：热点。这是与过滤与验证的ISE的MAC的一个开放式网络。此验证匹配在ISE的第二个授权规则和授权配置文件重定向对热点。ISE返回与两Cisco AV对的一RADIUS Access-Accept ：

- 流量应该重定向的url-redirect-acl (和在WLC定义的本地访问控制表(ACL)名称)
- url重新定向(在哪里重定向该数据流到ISE)

第二步：来宾用户重定向对ISE，接受AUP和或者提供一秘密接入代码。

步骤3. ISE发送RADIUS授权(CoA) Admin重置崔凡吉莱对WLC。当发送RADIUS Access-Request时， WLC重新鉴别用户。ISE回应在WLC定义的本地Access-Accept和Airespace ACL，对仅互联网的提供访问。

> **Note**:CoA Admin重置为热点功能是特定并且描述在Cisco Bug ID CSCus46754。ISE版本1.2的行为与访客门户不同的;CoA重新鉴别或Terminate发送。

第四步：来宾用户希望对网络的访问。网络管理员肯定用户接受AUP。来宾用户可以重定向到原始URL、静态配置的URL或者成功页。ISE显示的所有页可以定制。

与一可选状态检查的集成在最后一部分被提交。

配置

WLC

1. 添加验证和核算的新的RADIUS服务器。导航对**安全>AAA > Radius>验证**为了启用RADIUS CoA (RFC 3576)。

   有核算的一相似的配置。也建议配置WLC发送在被叫站ID属性的SSID，允许ISE配置根据SSID的灵活规则：

2. 在WLAN选项卡下，请创建无线局域网(WLAN)热点并且配置正确接口。设置Layer2安全对**无**与MAC过滤。在安全/验证、授权和统计(AAA)服务器中，请选择两验证和核算的(核算ISE IP地址可选)。在高级选项卡。，请启用**AAA覆盖**并且设置网络准入控制(NAC)状态为RADIUS NAC (CoA支持)。

3. 导航到**安全>访问控制列出>访问控制列表**并且建立两访问列表：

   HotspotRedirect，允许流量不应该重定向并且重定向其他流量互联网，为公司网络拒绝并且为其他允许

这是HotspotRedirect ACL (需要示例从重定向排除到/从ISE的流量) ：

ISE

1. 导航对**访客访问>配置>访客门户**，并且创建一个新的门户类型，热点访客门户：

2. 选择将被参考授权配置文件的门户名称。为了定制从门户行为和流设置的门户，请启用AUP和安全代码(可选) ：

   几个更多选项可以启用在入口页面自定义下;被提交的所有页可以定制。

3. 导航对**策略>结果>授权>授权配置文件**为了配置授权配置文件。

   热点(与对热点门户名称和ACL HotspotRedirect)的重定向：

   互联网(用Airespace ACL等于互联网) ：

4. 为了验证授权规则，请导航对**策略>授权**。在ISE版本1.3默认情况下失败的MAC验证旁路(MAB)访问的(没找到的MAC地址)，验证继续(没拒绝)。因为没有需要更改任何东西在默认验证规则，这为访客门户是非常有用的。

   对于第一MAB验证，第二个规则匹配(终端不在任何标识组中)。然后用户重定向对webportal(热点)，接受AUP和或者键入正确秘密接入代码。ISE发送RADIUS CoA，并且WLC执行再验证。对于第二验证，第一个规则与在WLC应用的授权配置文件PermitInternet一起匹配并且返回ACL名称(这次，终端已经在GuestEndpoints组中)。

   默认情况下，接受AUP的访客被放到GuestEndpoints标识组。为那些终端分配的标识组配置在访客Portal配置下，可以是不同的为每个门户。

5. 添加WLC作为网络接入设备从**Administration >网络资源>网络设备**。

验证

使用本部分可确认配置能否正常运行。

1. 在来宾用户与SSID热点产生关联并且键入URL后，他们重定向对AUP ：

2. 如果接入代码配置在访客门户下，则要求。如果用户提供一个不正确代码，错误显示：

3. 这是显示的屏幕，如果正确代码被输入：

4. 一旦正确代码被输入， WLC执行再验证并且提交附加的互联网ACL给会话。

另外的状态

如果有需要提供存取对于来宾用户，但是，只有当他们满足一项特定策略(状态)时例如新抗病毒更新和Microsoft Windows更新，则可以用这些规则完成：

热点规则不会提供存取对于互联网，反而执行重定向对状态服务。然后Web代理程序可推送到站点(客户端供应规定)和执行策略检查(状态规则)。报告标准由Web代理程序发送对ISE。在站点是兼容的后， ISE发送另一CoA重新鉴别，触发在WLC的一次授权更新。 然后HotSpot_Compliant规则遇到，并且对于互联网提供存取。

状态配置用NAC或Web代理程序是非常类似的正如在ISE版本1.2并且是出于本文的范围(请参阅相关信息部分欲知更多信息)。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

ISE应该提交：

这是流：

- 来宾用户遇到第二个授权规则和重定向对热点(“成功的验证”)。
- 在用户接受AUP后， ISE发送CoA Admin重置，由WLC (“成功的动态授权确认”)。
- WLC执行再验证，并且ACL名称返回(“成功的授权”)。

如果导航对**操作>报告> ISE报告>访客访问报告> AUP接受状态，**这可以也验证：

相关信息

- 在思科ISE配置指南的状态服务

- 思科ISE 1.3管理员指南
- 在WLC和ISE配置示例的中央Web验证
- 与FlexConnect AP的中央Web验证在与ISE配置示例的一WLC
- 技术支持和文档 - Cisco Systems