目录

简介

本文在允许重定向用第三方网络访问设备的身份服务引擎(ISE)方面描述新特性(NAD)发生。

先决条件

要求

Cisco 建议您了解以下主题：

- 在ISE的访客流
- DNS和DHCP协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalys 2960系列交换机
- 思科ISE，版本2.1

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。

背景信息

高级特性类似访客，状态和带来您自己的设备(BYOD)在流行网络，要求客户端设备和AAA服务器之间的直接通信。在上一个ISE版本中这通过发送动态重定向URL和访问控制表(ACL)完成对纳季。

有在重定向的一授权配置文件发送在attribute-value巴黎的两个必要属性(AVs) ：

- Cisco AV对？URL 重定向：URL值动态，并且为每会话创建。重定向URL的重要部分是策略服务节点Fuly合格的域名(PSN FQDN)和会话ID。
- Cisco AV对？重定向ACL ： 此AV对包含在纳季必须存在的ACL名称。在此ACL帮助下，纳季决定数据包应该是否通过纳季重定向或允许。

传统重定向方法可能用思科纳季设备只实现。对于第三方纳季支持，静态网域名称转址在ISE 2.0被添加了。当此方法是独立时更多的平台，仍然要求在纳季的HTTP重定向支持。

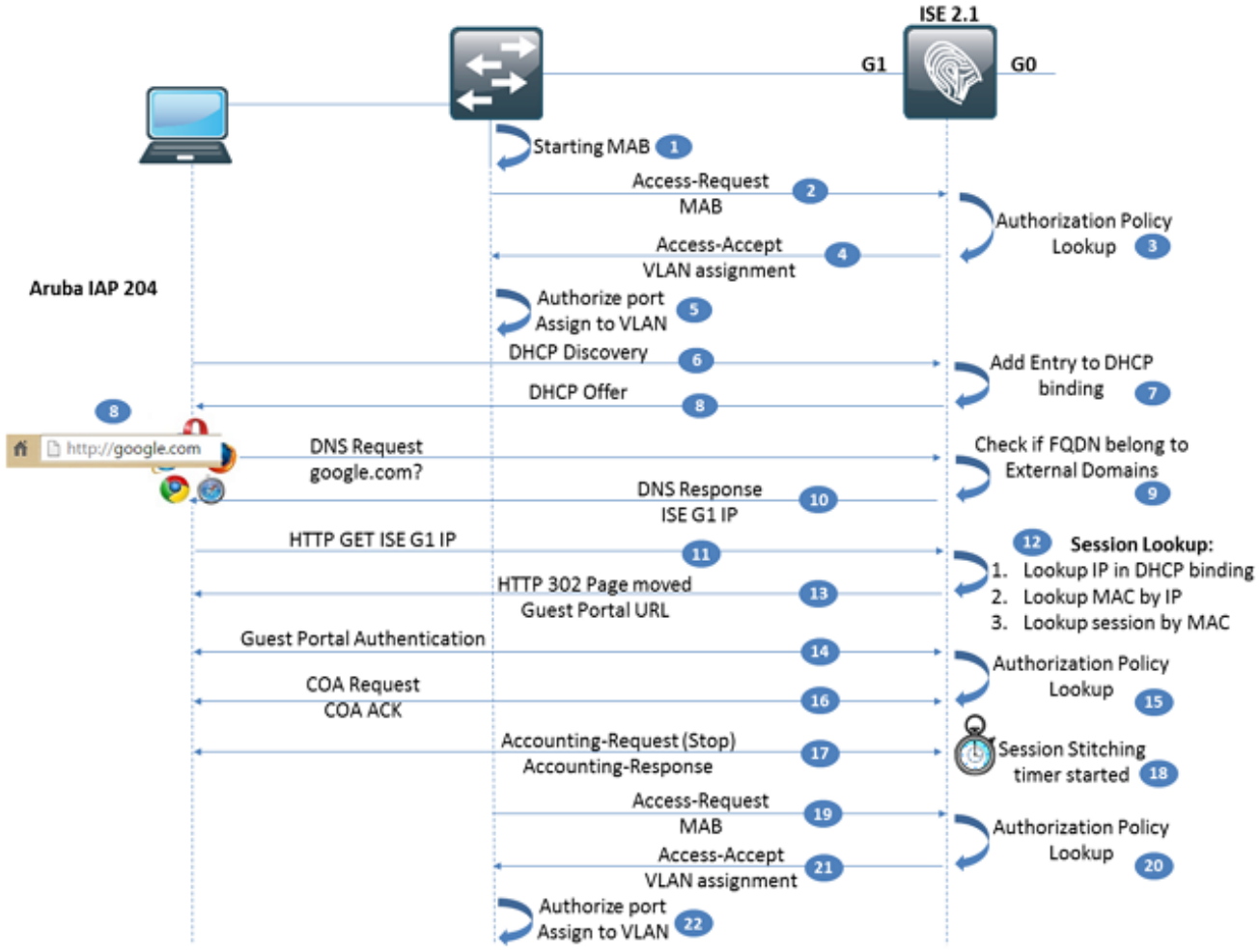
开始与ISE 2.1新式重定向被添加了。此方法不要求在纳季的HTTP重定向支持。在此方法后的主要想法是使用ISE作为DNS污水池。

DNS和DHCP服务器功能被添加到ISE 2.1版本为了使用它作为DNS污水池。现在ISE服务器能分配IP地址到需要重定向的用户并且定义了自己作为DNS服务器。这允许ISE重定向对本身的用户连接，不用在纳季的任何Web服务器功能。然而，纳季应该仍然支持授权(COA)和动态VLAN分配的崔凡吉莱。

在ISE，此方法可以用于这些重定向流：

- 访客流：对用户启动的任何DNS请求的ISE答案用其自己的IP地址。此答复造成客户端设立与ISE的一个HTTP连接。就此而论， ISE返回重定向URL使用被移动的标准HTTP代码302页。
- BYOD/Posture (仅Anyconnect) ？在两种情况下，设置(NSP)应用程序或Anyconnect状态模块的本地请求方首次对enroll.cisco.com的连接，重新定向对ISE使用步骤和访客流一样。

数据包流



1. 纳季开始连接的设备的MAB进程。在Cisco交换机的MAB进程根据认证方法优先级开始，并且没有，在第一帧从终端设备前接收。
2. MAB访问请求发送对ISE。
3. ISE评估流入的访问请求的认证和授权策略。在授权策略评估时，网络设备设备类型(纳季成水平设置)与在授权配置文件定义的网络设备设备类型比较。匹配的网络设备设备类型仅授权配置文件可以选择。

注意：访客VLAN重定向，包含Web重定向的ISE需要选择授权配置文件(CWA， MDM， NSP， CPP)和VLAN分配。客户端需要分配到有ISE作为唯一的DHCP服务器的网段。

1. ISE返回与VLAN信息的一Access-Accept。
2. 交换授权端口并且应用VLAN设置。
3. 客户端启动DHCP发现。如果PC在分段查找和ISE一样，数据包直接地到达ISE。在L3客户端和ISE之间的连接的情况下，应该配置ISE IP作为在纳季的一IP辅助工具地址DHCP中继的。
4. ISE添加客户端信息到其DHCP绑定表。ISE使用客户端IP和MAC会话查找。
5. DHCP提供发送给客户端。在此提供， ISE IP地址指定作为DNS服务器。
6. 用户打开触发DNS请求对ISE的Web浏览器并且导航对google.com。
7. ISE检查目标FQDN是否属于外部域。如果它，则ISE发送此请求到在DHCP池设置定义的DNS服务器。如果不是ISE返回其在答复的自己的IP地址。
8. Web浏览器启动对ISE的一TCP google.com的连接和请求。
9. 在此阶段ISE为传入的HTTP GET请求查寻认证的会话。这对构件正确重定向URL是重要。

注意：ISE使用这些规则会话查找：
1. 在DHCP绑定的查找IP
2. 由IP的查找MAC
3. 由MAC的查找会话

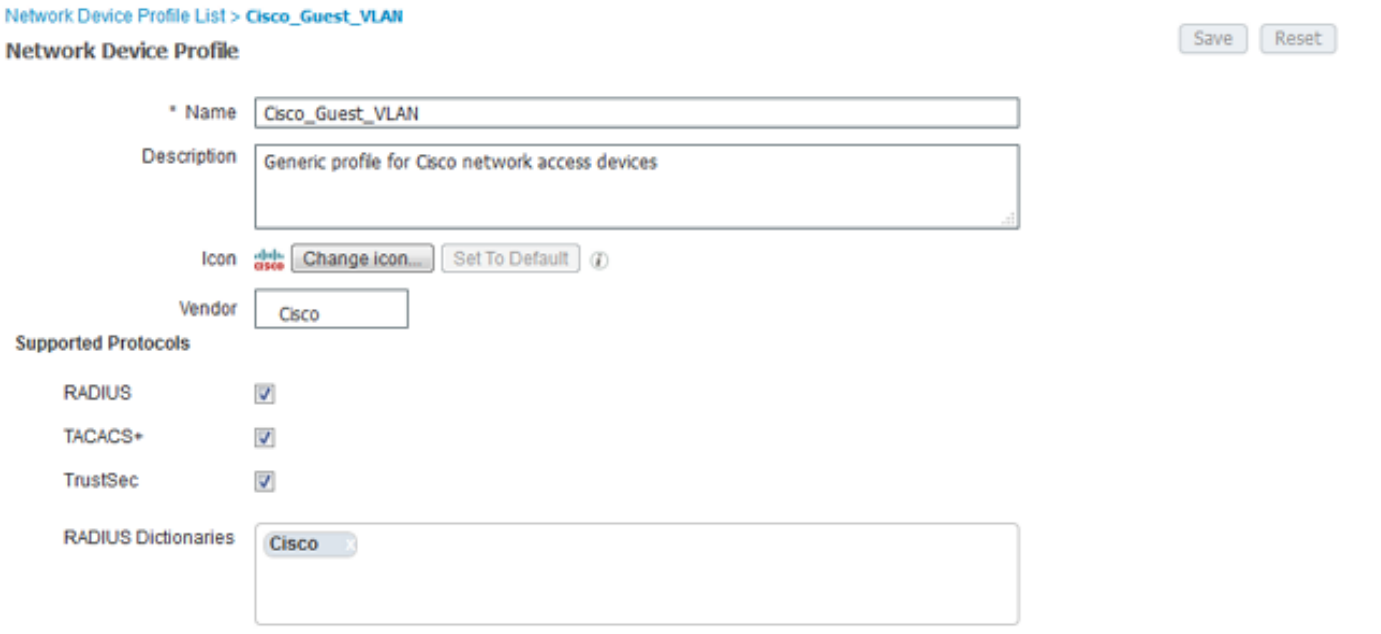
1. ISE回应被移动的HTTP 302页对重定向URL。
2. 用户因而重定向给门户的访客，并且在ISE配置的整个访客流发生此处。
3. 在一成功的访客验证以后， ISE通过授权策略更加运行检查其中任一新建的属性是否被添加了到会话，并且在访客流期间的终端是否要求授权(CoA)的崔凡吉莱。一旦下项授权策略识别，ISE准备CoA请求。
4. CoA请求/CoA ACK交换发生在ISE和纳季之间。因为这触发获取在最终VLAN的一个新的IP地址端口跳动或Admin重置CoA是当务之急。纳季需要支持Radius或SNMP CoA此步骤的能工作。
5. 断开会话的记帐请求终止发送对ISE。ISE通过发送记帐响应确认此请求。
6. ISE启动会话缝的计时器(20秒默认情况下)。在此时间所有会话属性(前：GUEST_TYPE，使用case=Guest流)由ISE保持。在此时间，万一同一个呼叫站ID的一新的访问请求接收，所有会话属性一定对个新会话。
7. 新的MAB访问请求为终端设备发送，在CoA端口跳动后。
8. ISE了解新要求的认证/授权具体政策。在此阶段ISE使用会话属性和终端属性正确策略选择。
9. Access-Accept用最终VLAN信息传送。可下载的访问控制表(DACL)可以发送，限制在默认VLAN的流量。
10. 交换授权新的VLAN的端口并且应用DACL，如果包括。

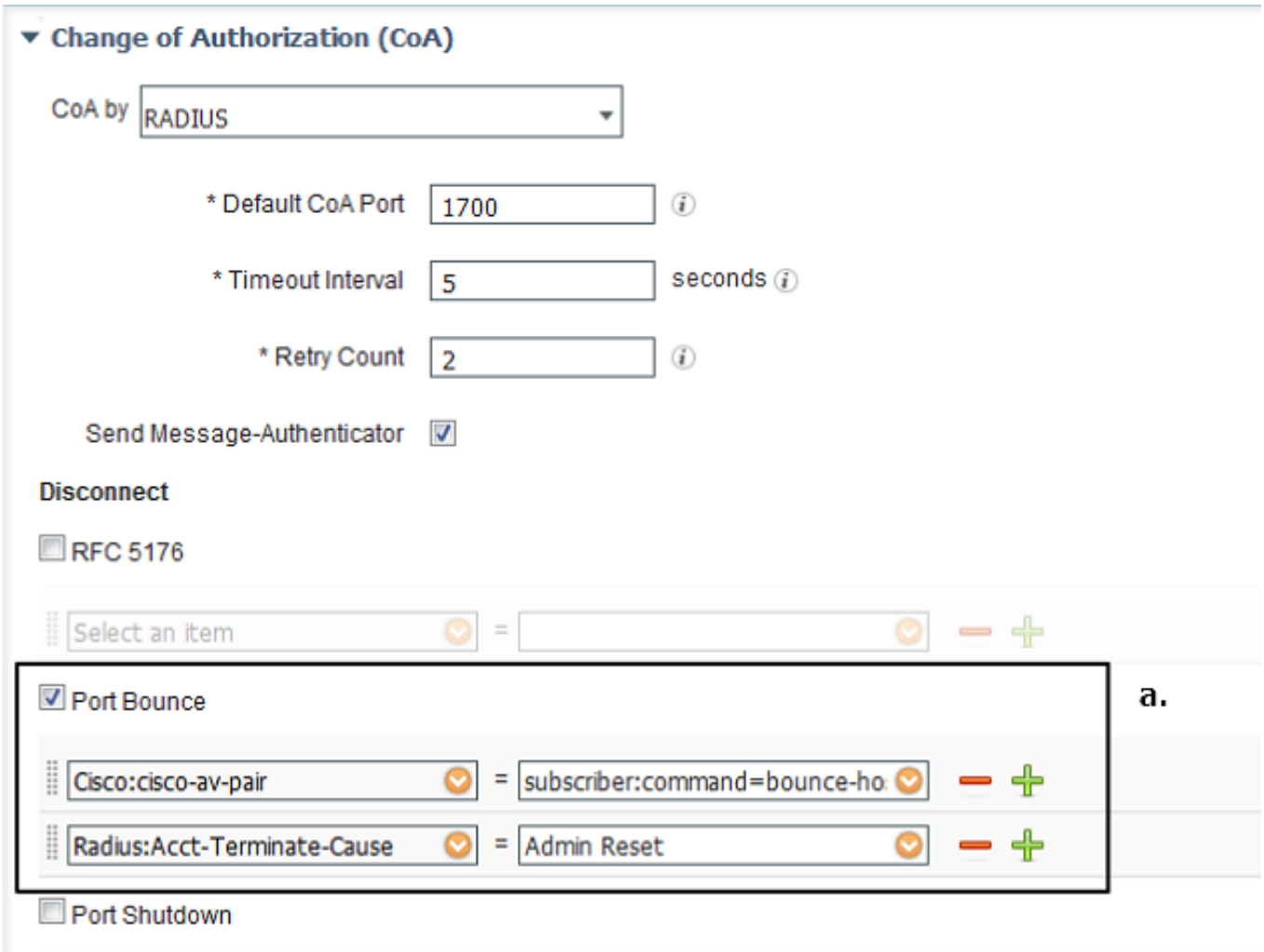
配置

配置ISE

1. 创建网络设备配置文件

此特定的示例， Cisco交换机使用作为纳季。所以，现有Cisco网络设备配置文件被复制和修改如所需求。导航对Administration >网络资源>网络设备配置文件并且添加新配置文件。





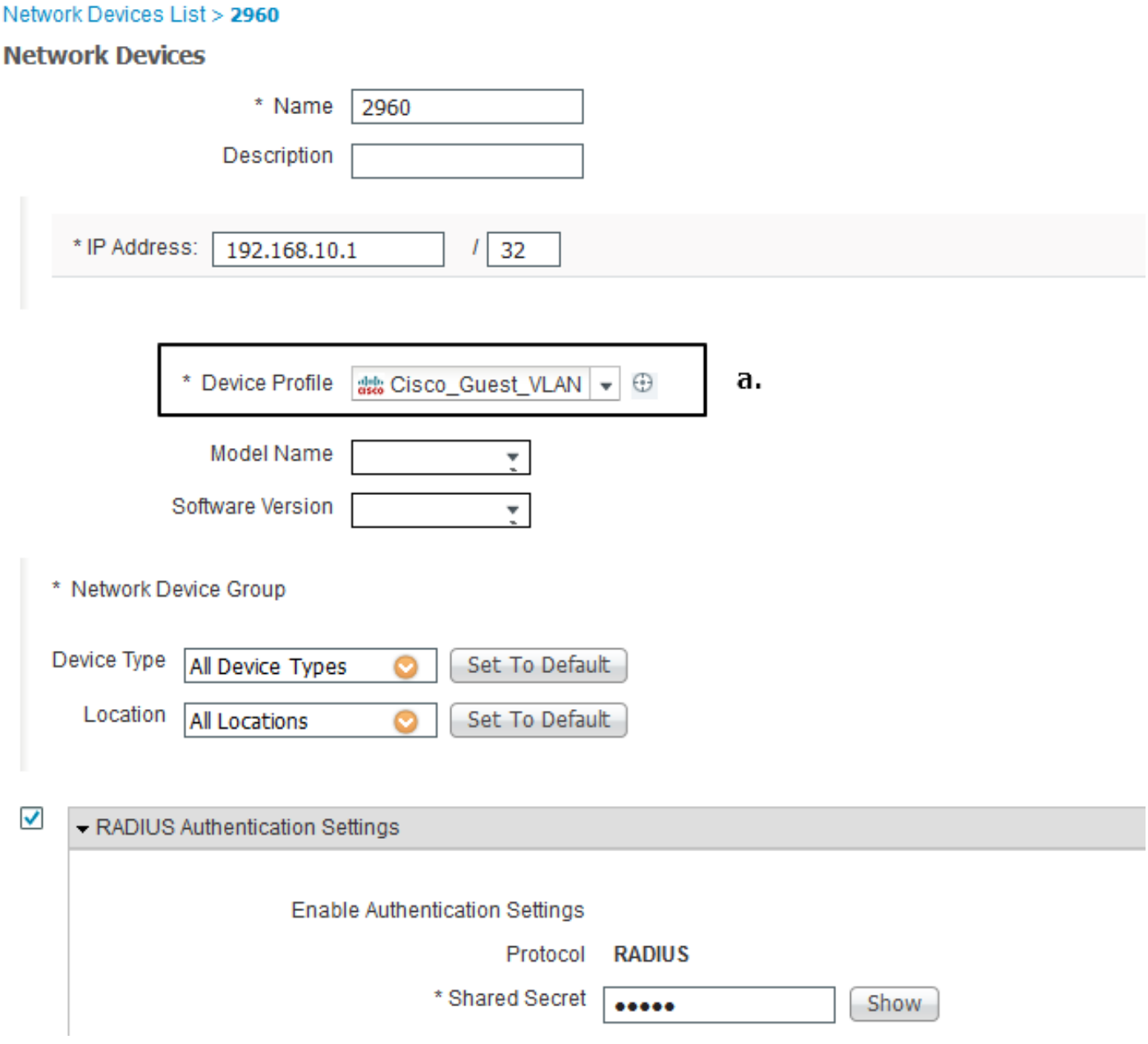
a.重新配置的CoA类型安排仅端口跳动启用

b.重定向类型从动态更改到静态

c. SSID名称从静态重定向URL删除

2. 创建网络设备

导航到Administration >网络资源>网络设备为了添加新设备。



a. 注释网络设备配置文件的设置。

b. 其他设置标准。

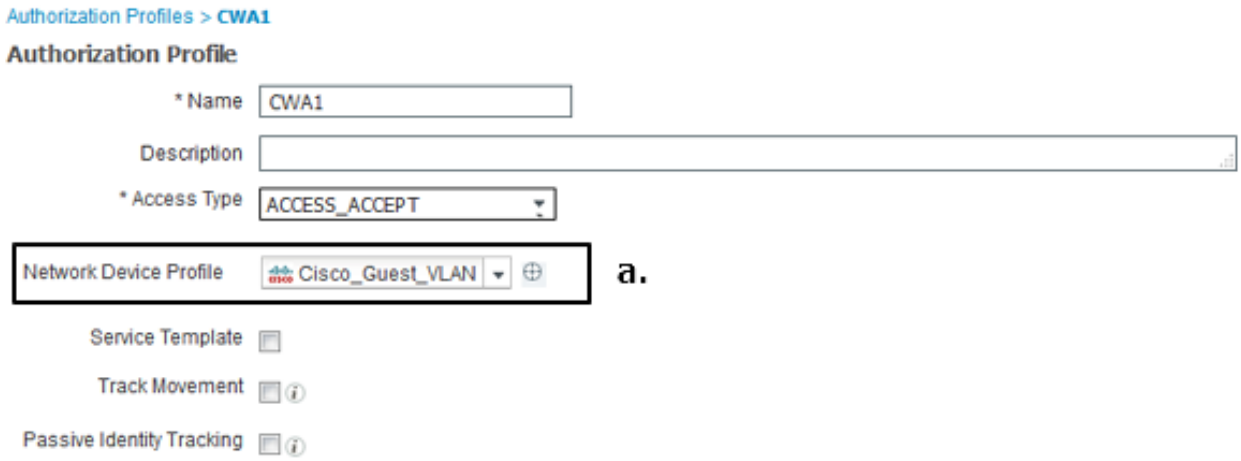
3. 配置DHCP服务器

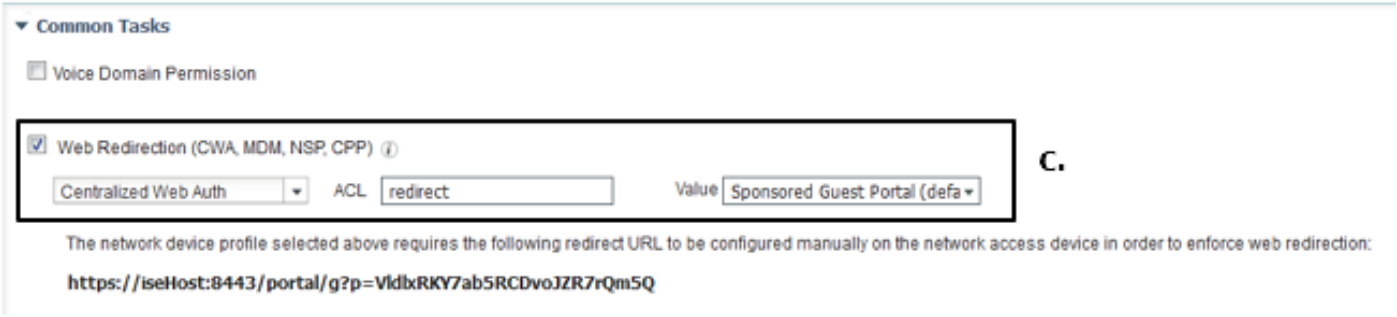
DHCP服务器池一定对一个特定的ISE节点和其接口。导航对管理>System >设置> DHCP & DNS Services>添加

导航[illegible]。

4. 配置授权配置文件

- 重定向授权配置文件(CWA1)
- Permit访问权限配置文件(PermitCWA2)

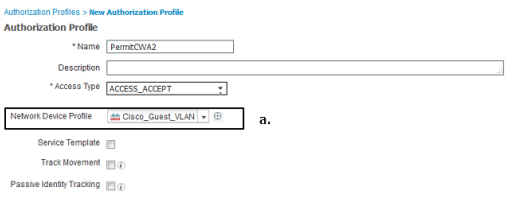




a.网络设备配置文件：来自NAD的仅认证请求分配到此配置文件可能导致此授权配置文件，

b. VLAN设置：定义的VLAN此处在纳季必须存在。为DHCP配置的ISE接口应该或者应该属于此VLAN或配置作为在服务此VLAN的网关的IP辅助。

c.重定向设置：对于当前示例中央Web验证定义作为重定向类型，并且赞助了访客门户定义作为访客门户。表仍然请求重定向ACL名称。因为网络设备配置文件为静态URL重定向重新配置，此ACL名称不会发送给纳季。

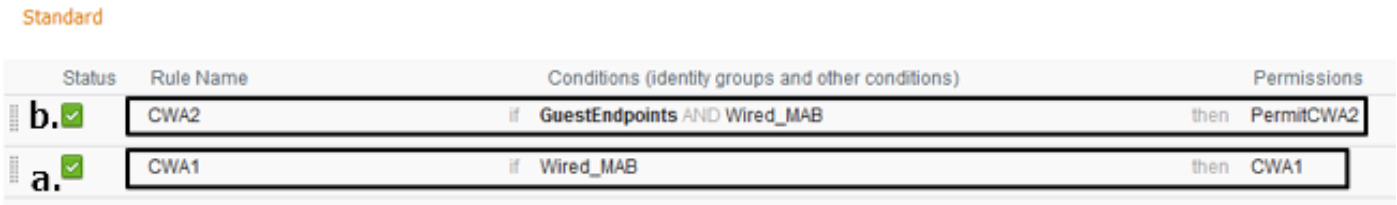


a.网络设备配置文件：来自NAD的仅认证请求分配到此配置文件可能导致此授权配置文件，

b. VLAN设置：在分配客户端端口以后到此VLAN，用户应该从一个正常DHCP服务器获得IP地址。

5. 配置访客访问的授权策略

导航对策略>授权。配置两项策略：一重定向操作的和其他在验证以后的用户访问的在访客门户。



a.结果第一项授权策略匹配有线MAB作为认证方法和重定向授权配置文件分配。

b.第二项授权策略可以会话属性(用例=访客流/访客类型外部AD组，如果使用AD验证的来宾用户)或根据终端属性(终端标识组)。设备已注册在访客门户需要启用使用终端标识组。

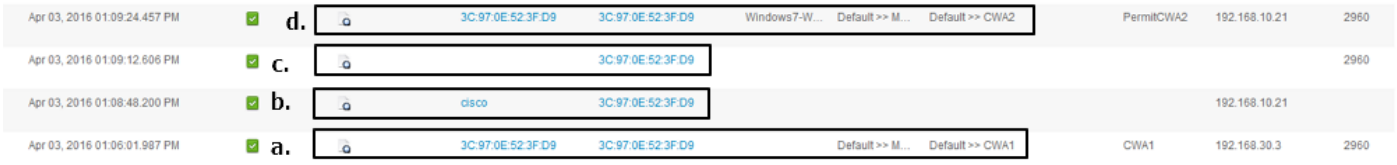
配置纳季

Cisco交换机为在接口的MAB配置并且有COA支持。

注意：Cisco技术支持中心(TAC)不提供第三方NAD的配置的任何支持。

验证

一个成功的访客流看上去象这个在ISE操作> Radius Livelog ：



a.这是第一MAB验证。与重定向的结果授权配置文件选择。

b.这是访客验证。在此操作ISE执行策略再估价决定后CoA是否是需要的。

c.CoA顺利地完成。

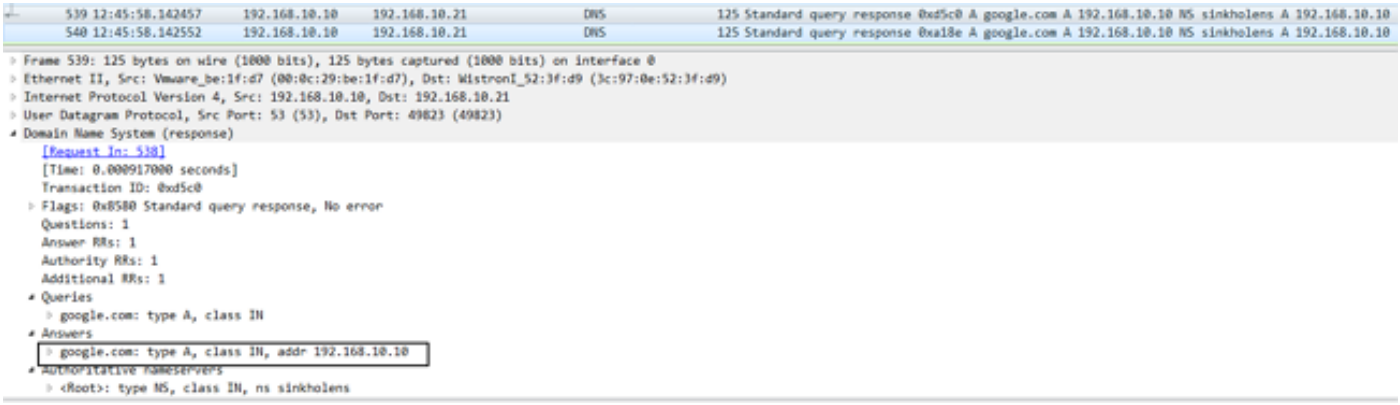
D.这是第二MAB验证。访客访问的结果授权配置文件选择。

故障排除

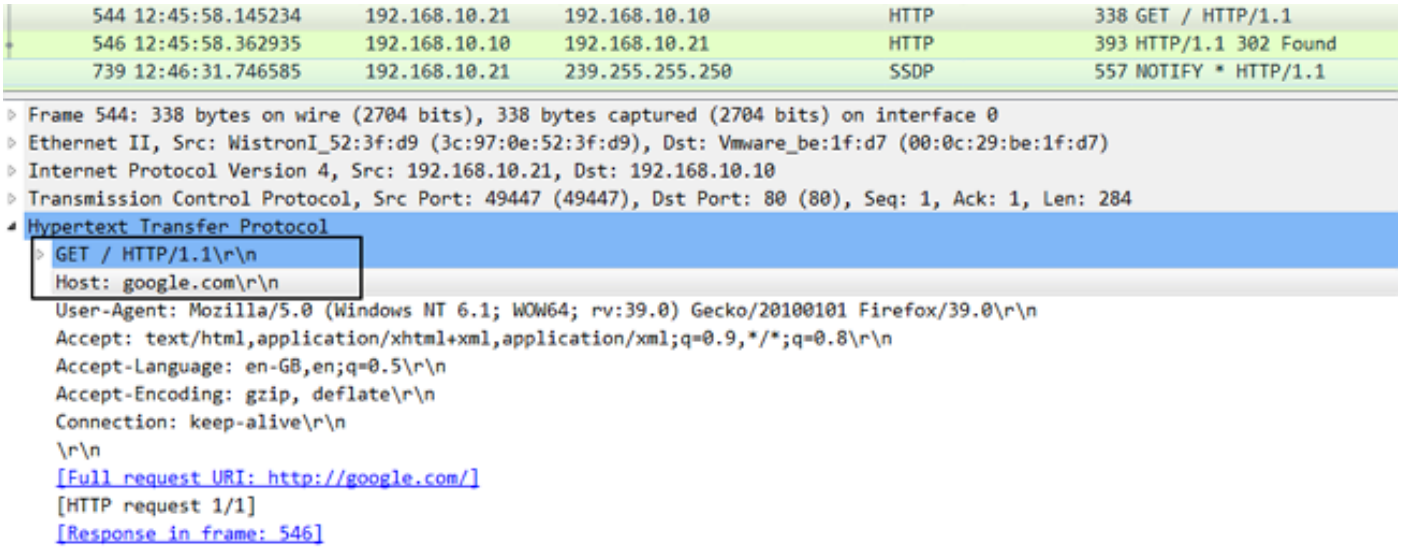
检查IP地址是否正确地分配到客户端。这可以由收集客户端或ISE的一数据包捕获完成。

从客户端的此捕获显示与DNS IP的成功的DHCP握手同ISE一样。

检查ISE是否适当地作为DNS污水池。数据包捕获可帮助确认请求是否去ISE，并且ISE是否响应对它用其自己的IP地址：



检查HTTP重定向是否适当地运作。在它获得资源IP地址并且建立对ISE后的TCP连接，客户端发送HTTP GET请求对ISE。这在客户端数据包捕获可以被确认：



同时， ISE确定任何会话是否为此客户端存在。会话查找此进程在ISE的可以是被登记的prrt管理日志：

在会话查找以后， ISE返回重定向URL给HTTP 302答复的客户端：