与静态重定向的ISE隔离访客网络配置示例的

目录

简介

本文描述如何配置思科身份服务引擎(ISE)有隔离访客网络的静态重定向的为了维护冗余。它也描述如何配置策略节点，以便客户端没有用一不能证实的证书警告提示。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ISE中央Web验证(CWA)和所有相关组件
- 证书有效性的浏览器验证
- Cisco ISE版本1.2.0.899或以上
- Cisco无线LAN控制器(WLC)版本7.2.110.0或以上(版本7.4.100.0或以后更喜欢)

Note:CWA在WLC和ISE配置示例的中央Web验证描述Cisco条款。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ISE版本1.2.0.899
- Cisco虚拟WLC (vWLC)版本7.4.110.0
- Cisco可适应安全工具(ASA)版本8.2.5

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

在许多请带来您自己的设备(BYOD)环境，网络从在非敏感区域(DMZ)的内部网络充分地隔离的访客。通常，在访客DMZ提供公共域名称系统(DNS)服务器的DHCP对来宾用户，因为提供的唯一的服务是互联网访问。

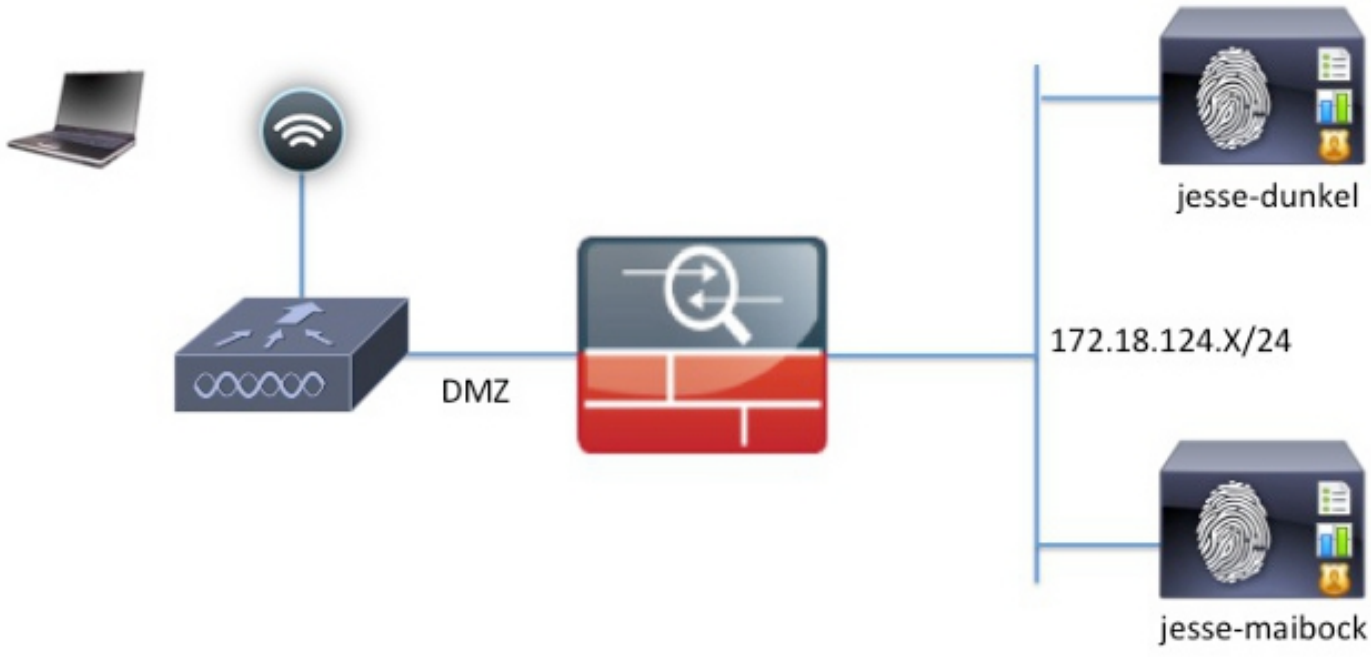
因为ISE重定向客户端对Web验证的，完全合格的域名(FQDN)这在ISE做访客重定向困难在版本1.2之前。然而，与ISE版本1.2和以上，管理员能重定向来宾用户到静态IP地址或主机名。

配置

网络图

这是逻辑图。

> **Note**:实际上，有在内部网络的一个无线控制器，接入点(AP)在内部网络和服务集设置识别(SSID)停住对DMZ控制器。参考思科WLCs的文档欲知更多信息。



配置

在WLC的配置依然是不可更改从正常CWA配置。SSID配置为了准许MAC过滤与RADIUS验证的和往两个或多个ISE策略节点的RADIUS认为的点。

本文着重ISE配置。

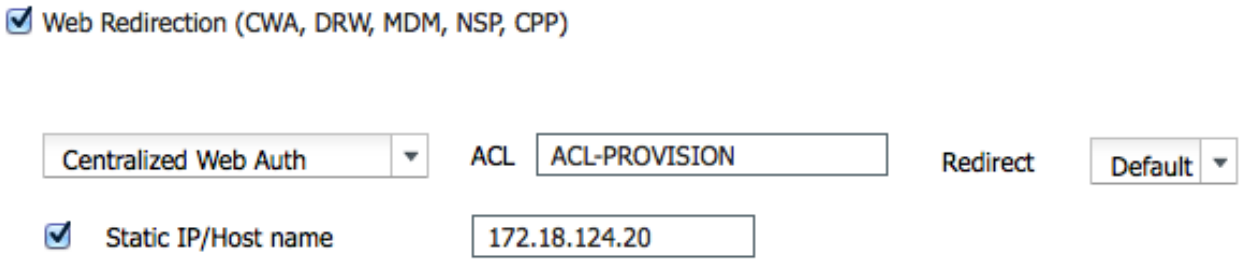
Note:在本例中配置示例，策略节点是**杰西dunkel** (172.18.124.20)和**杰西maibock** (172.18.124.21)。

CWA流开始，当WLC发送RADIUS MAC验证旁路(MAB)请求对ISE。与重定向URL的ISE回复对控制器为了重定向HTTP数据流到ISE。重要的是RADIUS和HTTP数据流去Services节点同一项的策略(PSN)，因为会话在单个PSN保养。这用单个规则通常执行，并且PSN插入其自己的主机名到CWA URL。然而，与静态重定向，您必须创建每个PSN的一个规则为了保证RADIUS和HTTP数据流发送对同样PSN。

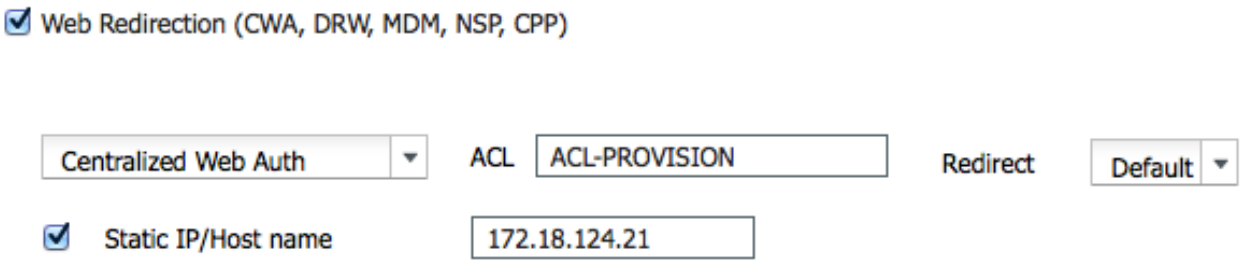
完成这些步骤为了配置ISE ：

1. 设置两个规则为了重定向客户端到PSN IP地址。导航对**策略>Policy元素>结果>授权>授权配置文件**。

   这些镜像显示配置文件名称的**DunkelGuestWireless**信息：

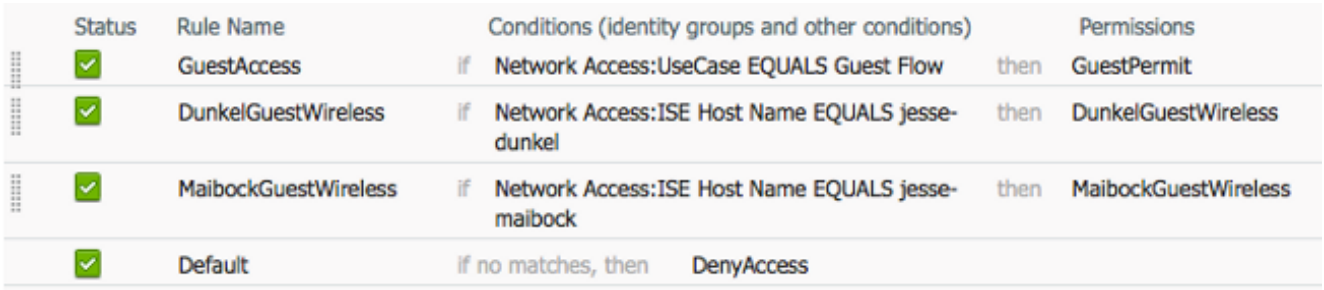


   这些镜像显示配置文件名称的**MaibockGuestWireless**信息：



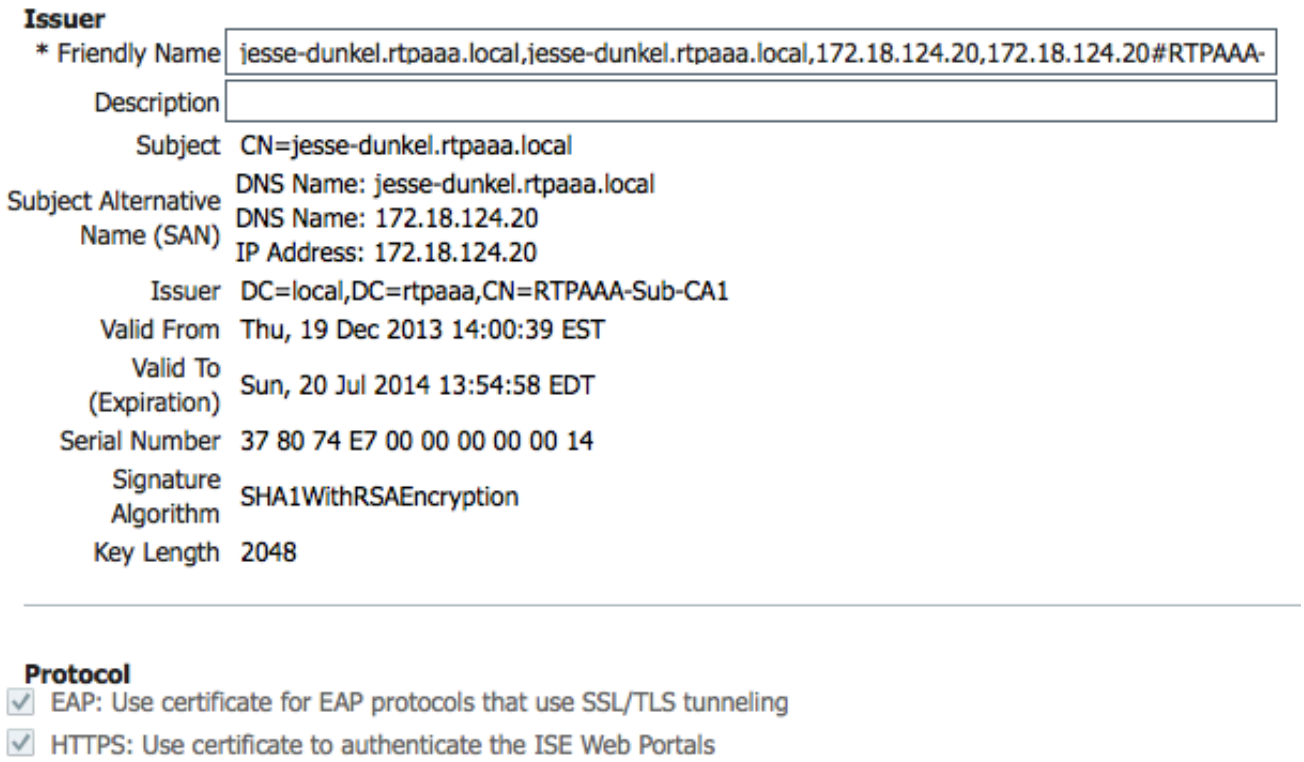
Note:在WLC配置为了允许客户端与ISE联络在验证的**ACL-PROVISION**是本地访问控制表(ACL)。参考[在WLC和ISE配置示例的中央Web验证](#)Cisco条款欲知更多信息。

2. 配置授权修正，以便他们在**网络访问**配比：**ISE主机名**属性和提供适当的授权配置文件：



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then MaibockGuestWireless
✓	Default	if no matches, then DenyAccess	

即然客户端重定向对IP地址，用户收到证书警告，因为URL不匹配在证书的信息。例如，在证书的FQDN是**杰西dunkel.rtpaaa.local，但是URL是172.18.124.20**。Hereis允许浏览器验证证书用IP地址的**示例**证书：



使用使用附属的替代方案名称(SAN)条目，包括IP地址172.18.124.20的浏览器能验证URL。必须创建三个SAN条目为了寻址多种客户端不相容。

3. 创建DNS名的一个SAN条目并且保证匹配从主题字段的**CN=**条目。

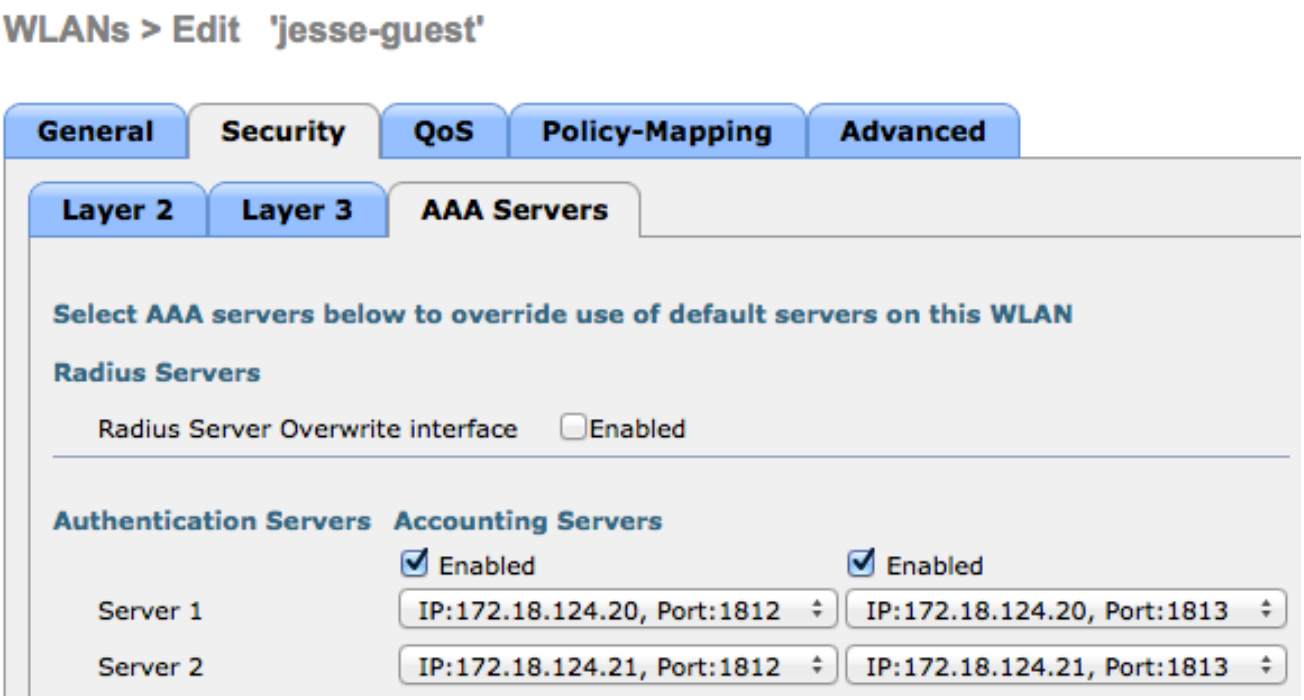
4. 创建两个条目为了允许客户端验证IP地址;这些是为IP地址的DNS名以及在IP地址属性出现的IP地址。一些客户端只参考DNS名。其他不接受在DNS名属性的一个IP地址，反而参考IP地址属性。

   Note:关于证书生成的更多信息，参考**思科身份服务引擎硬件安装指南，版本1.2。**

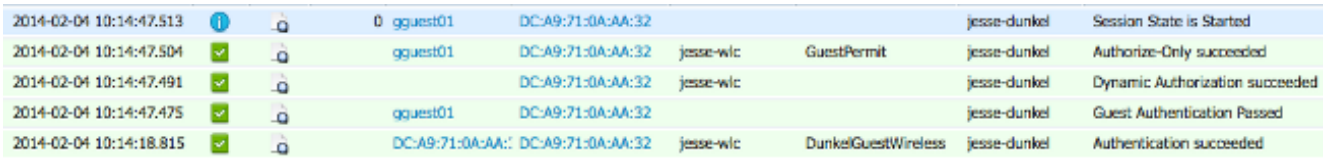
验证

完成这些步骤为了确认您的配置适当地工作：

1. 为了验证两个规则是工作，手工设置在WLAN配置ISE PSN的命令：



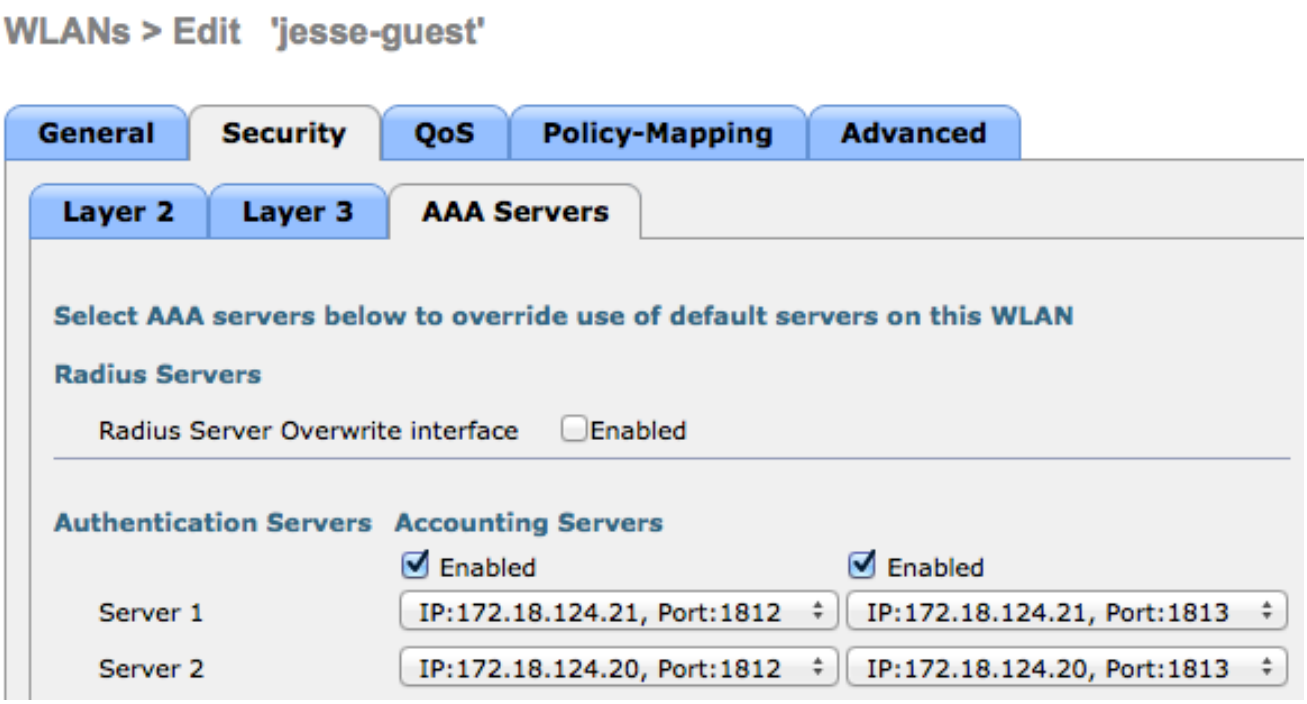
2. 登录访客SSID，导航对在ISE的**操作>认证**，并且验证正确授权规则点击：



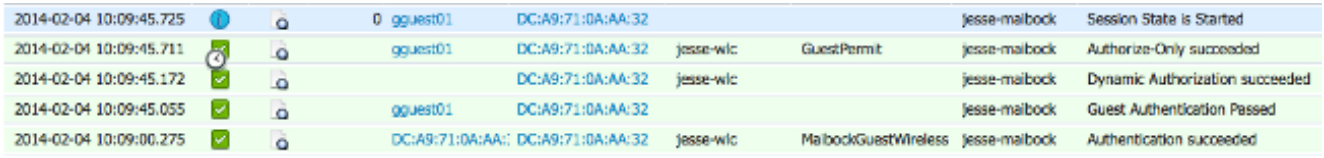
初始MAB验证给对**DunkelGuestWireless**授权配置文件。这是特别地重定向给**杰西dunkel**，是第一个ISE节点的规则。在**gguest01**用户登录以后， **GuestPermit**正确最终权限给。

3. 为了清除从WLC的验证会话，从无线网络请断开客户端设备，导航给WLC的**监视器>客户端**，并且删除从输出的会话。 默认情况下WLC举行空闲会话五分钟，因此为了执行一有效测验，您必须重新开始。

4. 倒转ISE PSN的命令在访客WLAN配置下：



5. 登录访客SSID，导航对在ISE的**操作>认证**，并且验证正确授权规则点击：



对于第二尝试， **MaibockGuestWireless**授权配置文件为初始MAB验证正确地点击。类似于第一次尝试于**杰西dunkel** (步骤2)，对**杰西maibock的**验证正确地点击最终授权的**GuestPermit**。由于没有在**GuestPermit**授权配置文件的PSN特定信息，单个规则可以用于对所有PSN的验证。

故障排除

Details窗口的验证是显示认证/授权进程的每个步骤的一张强大的视图。为了访问它，请导航对**操作>认证**并且单击放大镜图标在Details列下。请使用此窗口为了验证认证/授权规则条件适当地配置。

在这种情况下，策略服务器领域是重点主要区域。此字段包含验证服务ISE PSN的主机名：

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

比较策略服务器条目对规则情况并且保证两匹配(此值区分大小写) ：

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

Note:请记住您必须从SSID断开和从WLC清除客户端条目在测验之间。