配置Firepower 6.1与ISE的pxGrid修正

目录

简介

本文描述如何配置Firepower 6.1 pxGrid修正用身份服务引擎(ISE)。Firepower 6.1+ ISE修正模块可以与ISE终端保护业务(EPS)一起使用自动化qurantine/列入黑名单在网络接入层的攻击者。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- 思科ISE
- 思科Firepower

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2.0 Patch4
- 思科Firepower 6.1.0
- 虚拟无线局域网控制器(vWLC) 8.3.102.0

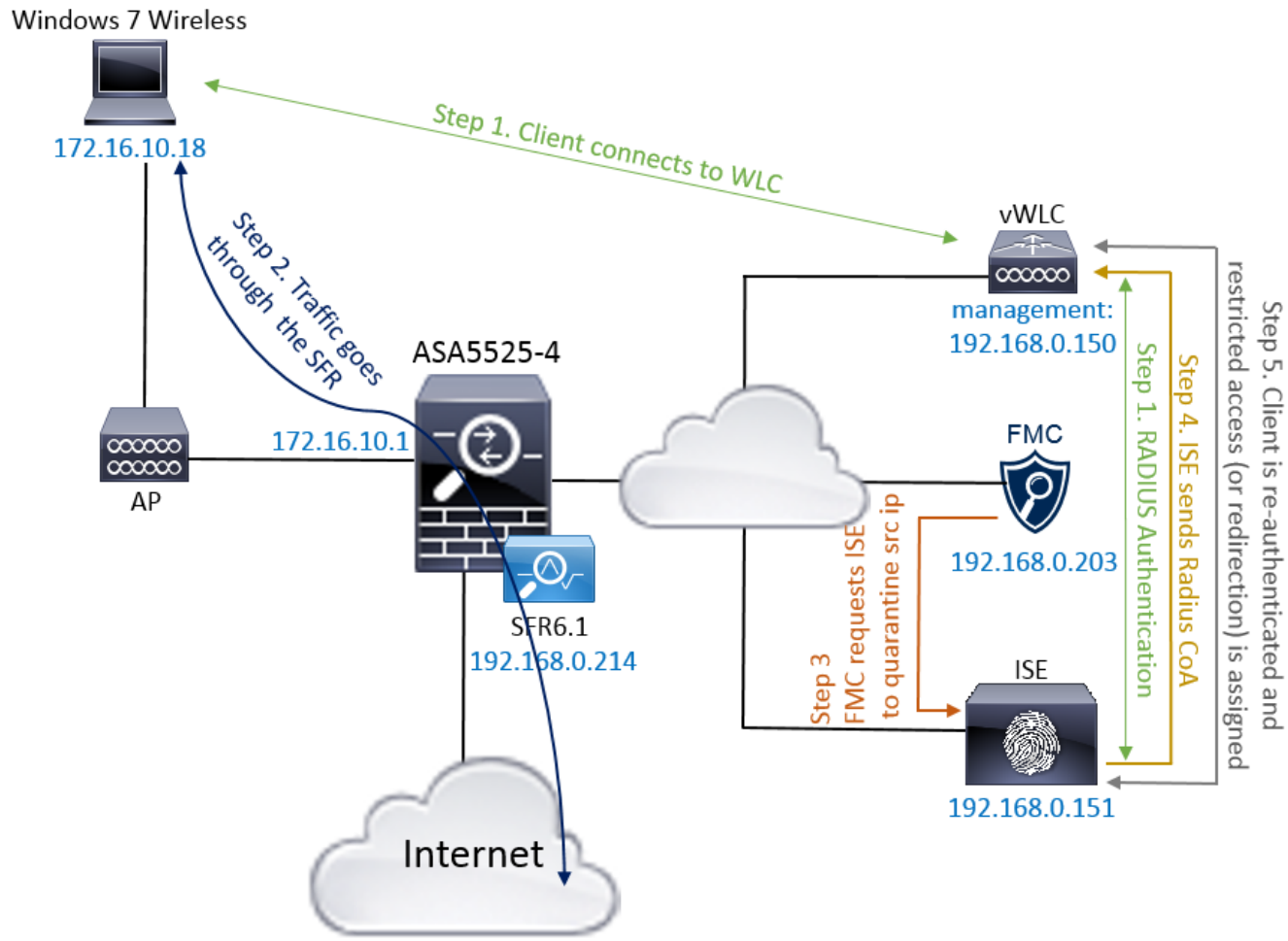
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

此条款用Firepower不包括ISE集成初始配置，与激活目录(AD)的ISE集成，与AD的Firepower集成。对于此信息请导航对References部分。Firepower 6.1修正模块允许Firepower系统使用ISE EPS功能(检疫、unquarantine，端口关闭)作为修正，当关联规则匹配时。

Note:端口关闭为无线部署不是可用的。

网络图



流说明：

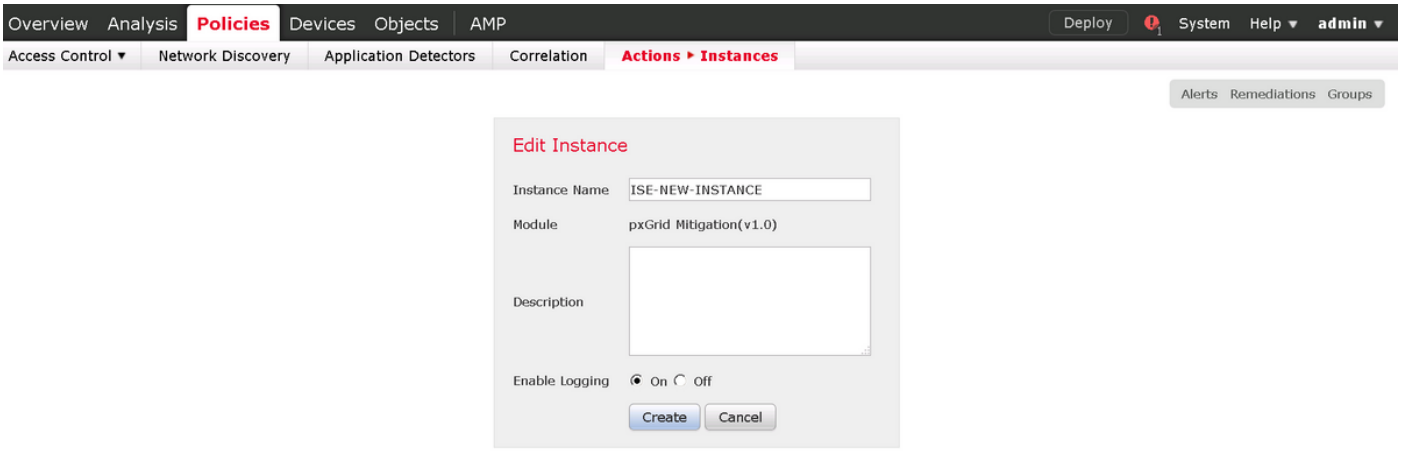
1. 客户端连接对网络，验证与ISE并且点击与准许对网络的无限制访问的授权配置文件的一个授权规则。
2. 从客户端的流量然后流经Firepower设备。
3. 用户开始执行恶意活动并且点击反过来触发Firepower管理中心的关联规则(FMC)通过pxGrid执行ISE修正。
4. ISE分配EPSStatus检疫到终端并且触发RADIUS授权崔凡吉莱对网络接入设备(WLC或交换机)。
5. 客户端点击分配限制访问的另一项授权策略(对门户的更改SGT或重定向或拒绝访问)。

Note:应该配置网络接入设备(纳季)发送认为的RADIUS到ISE为了提供它用于映射IP地址到终端的IP地址信息。

配置Firepower

步骤1.配置pxGrid缓解实例。

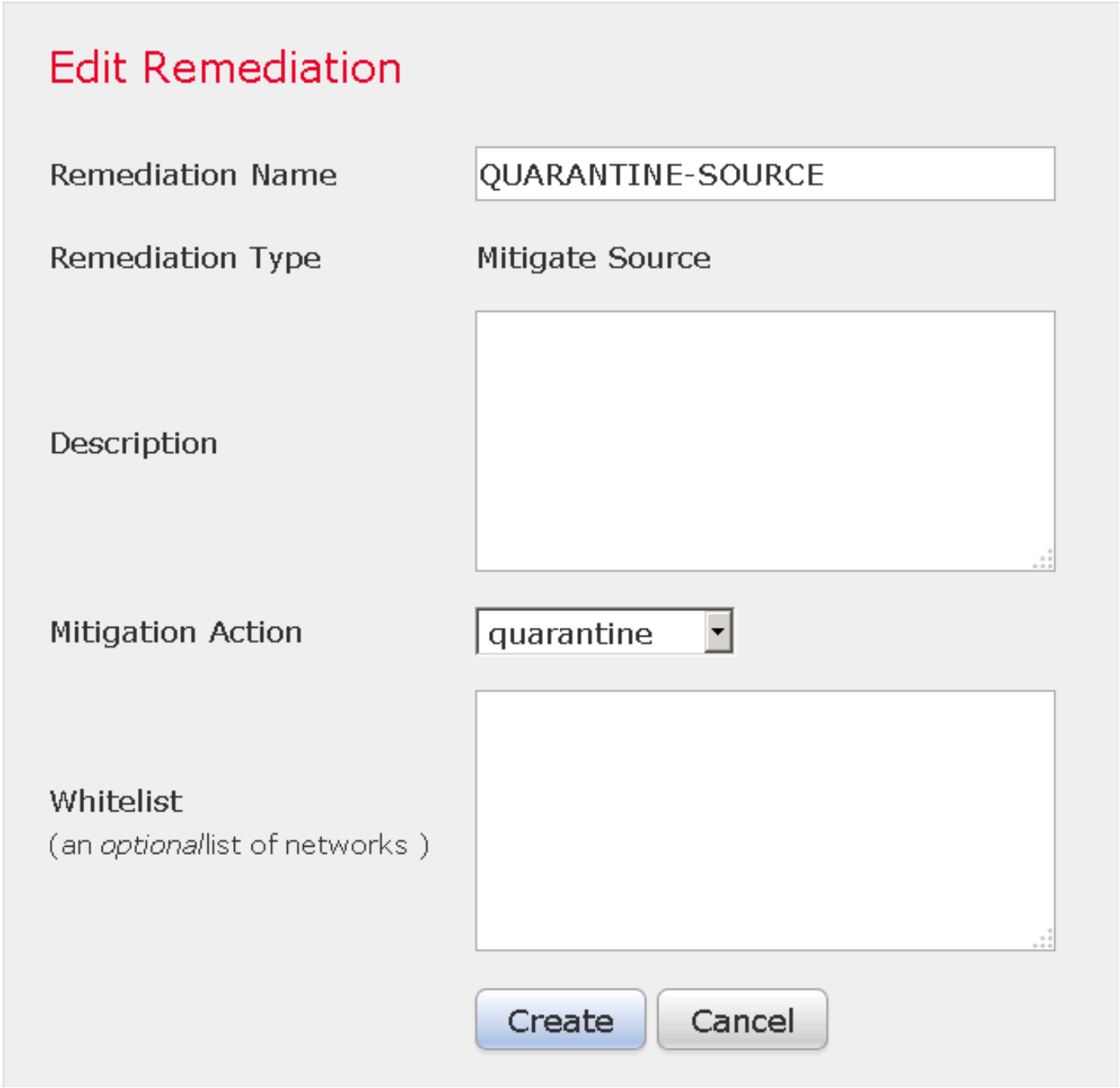
如镜像所显示，导航对**策略>操作>实例**并且添加pxGrid缓解实例。



步骤2.配置修正。

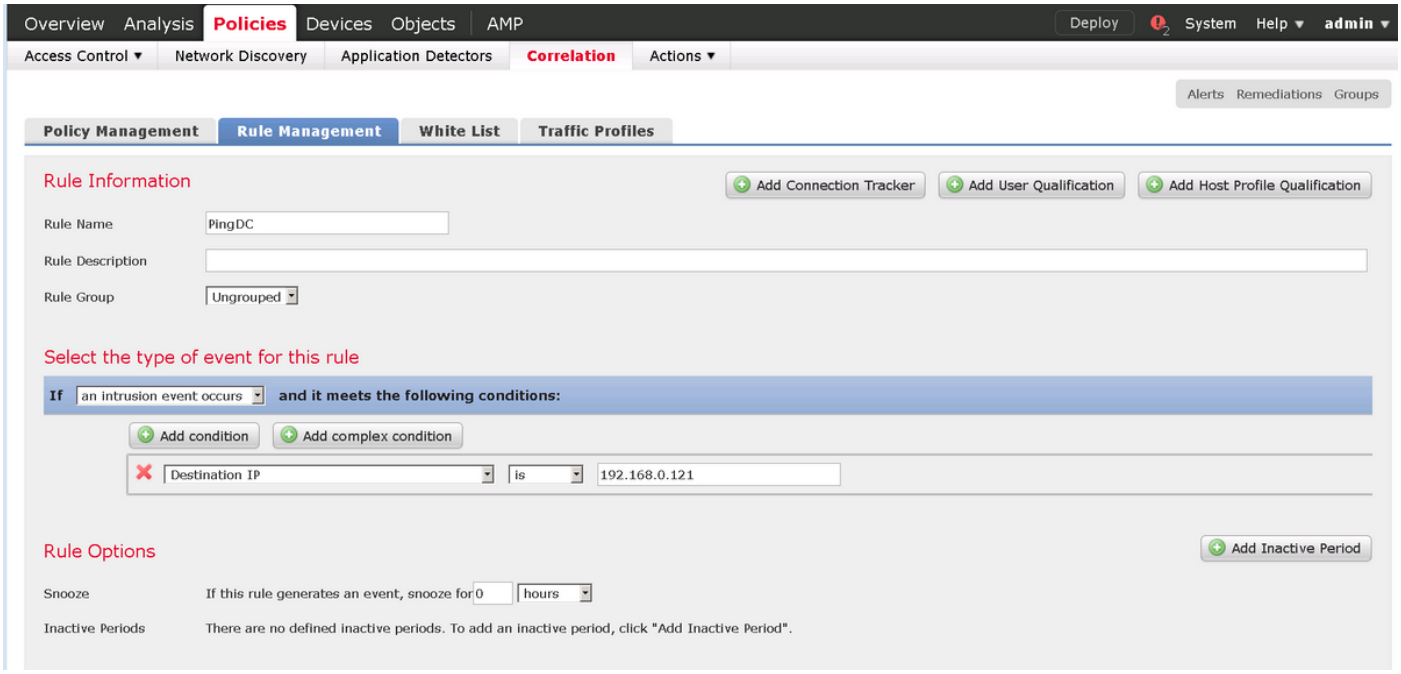
有两类型联机：缓和目的地并且缓和来源。在此示例来源使用缓解。如镜像所显示，选择修正类型并且单击**添加**：

如镜像所显示，分配缓解操作到修正：



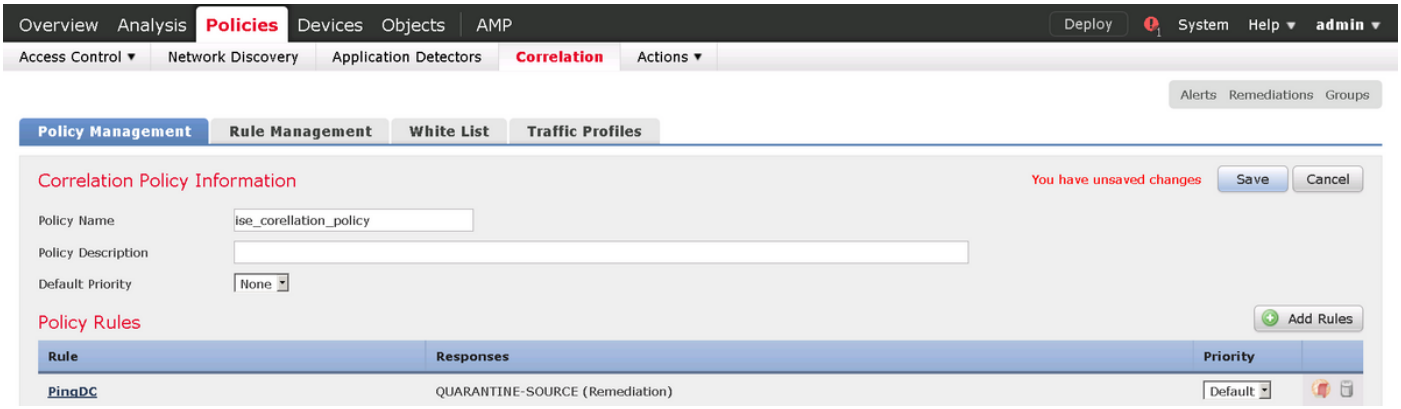
步骤3.配置关联规则。

导航对**策略>相关性>规则管理**并且单击**创建规则**关联规则是修正的触发能发生。关联规则能包含几个情况。在此示例关联规则**PingDC**点击，如果入侵事件发生，并且目的IP地址是192.168.0.121。如镜像所显示，匹配ICMP echo应答的自定义入侵规则为测验的目的配置：

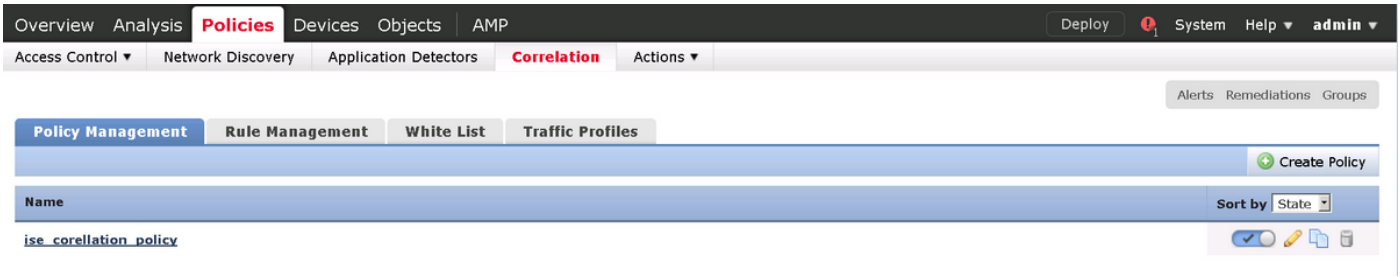


步骤4.配置相关性策略。

如镜像所显示，导航对**策略>相关性>Policy管理**并且单击**创建策略**，增加规则到策略并且分配对它的答复：



如镜像所显示，启用相关性策略：



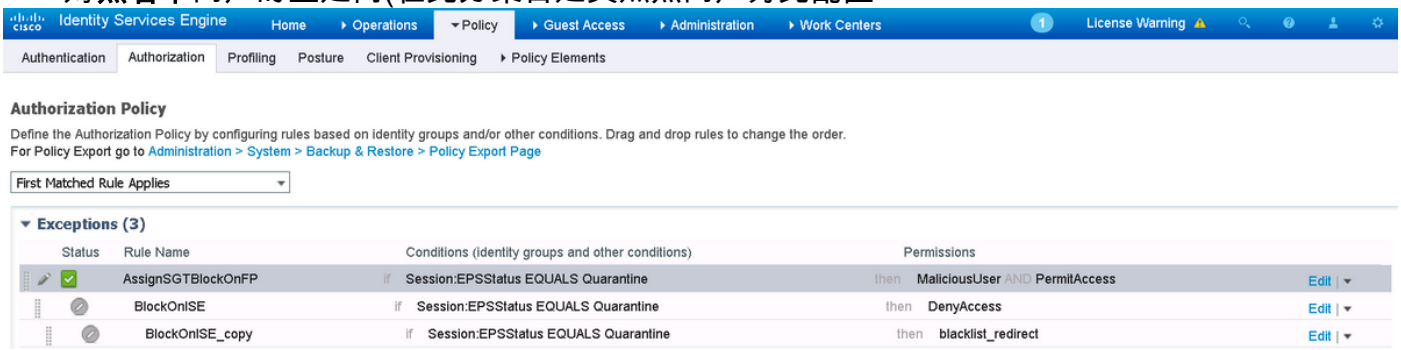
配置ISE

步骤1.配置授权策略。

导航对**策略>授权**并且添加将点击的一项新的授权策略，在修正发生后。使用**会话：EPSStatus等于检疫**作为情况。有可以使用结果的几个选项：

- 允许访问并且分配不同的SGT (请强制执行在网络设备的访问控制限制)

- 拒绝访问(用户应该插入在网络外面，并且不应该能再连接)
- 对**黑名单**门户的重定向(在此方案自定义热点门户为此配置

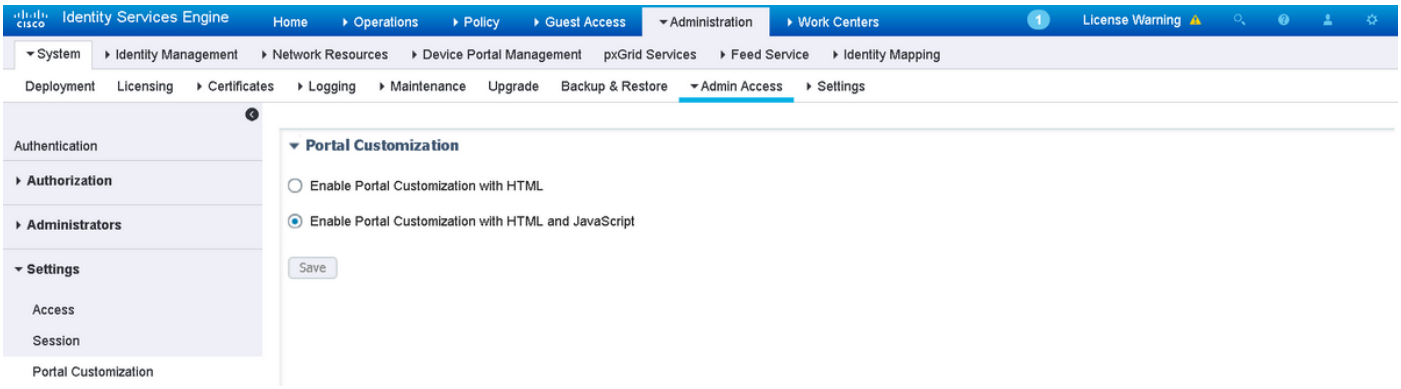


自定义Portal配置

在本例中，热点门户配置作为**黑名单**。有与自定义文本的仅Acceptable Use Policy (AUP)页，并且没有接受AUP的可能性(这执行与Javascript)。为了达到此，您首先需要启用Javascript然后粘贴隐藏AUP按钮和控制在门户自定义配置方面的代码。

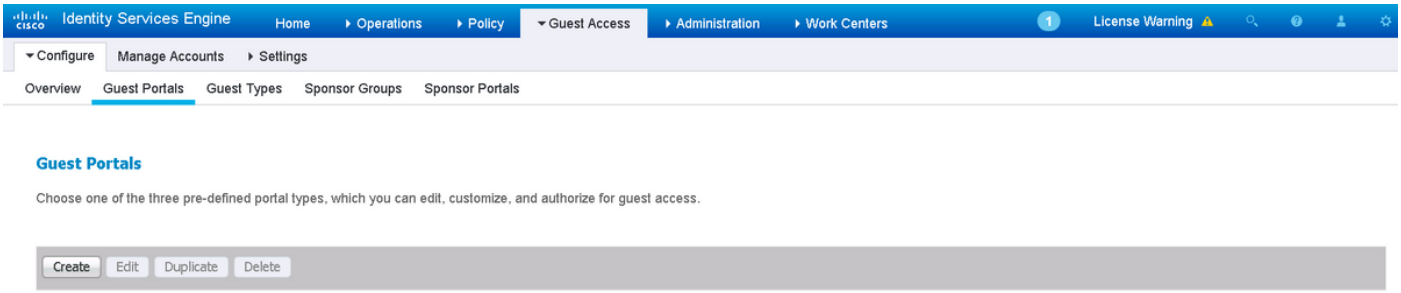
步骤1. Enable (event) Javascript。

导航对**管理>System > Admin Access>设置>门户自定义。**选择**与HTML和Javascript的Enable (event)门户自定义**并且点击**"Save"**。



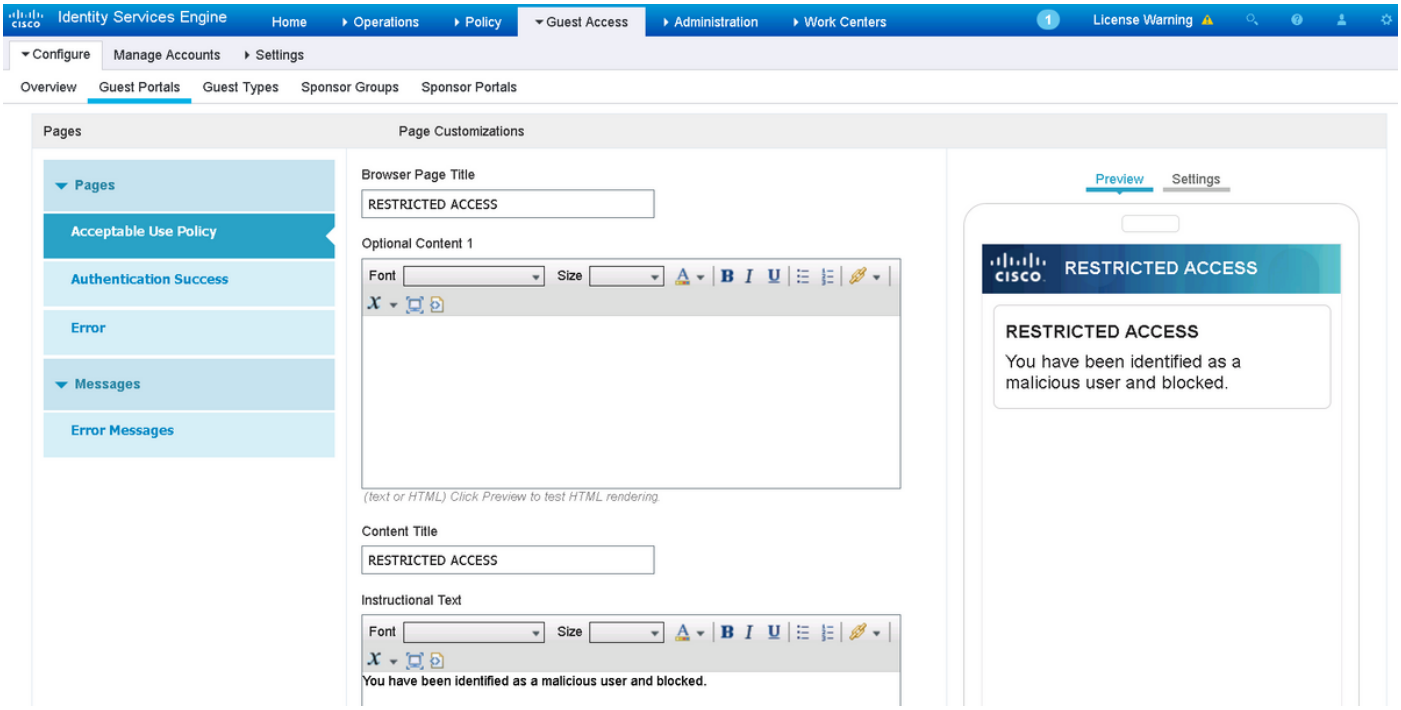
步骤2.创建热点门户。

导航对**访客访问>配置>访客门户**并且单击**创建**，然后选择热点类型。



步骤3.配置门户自定义。

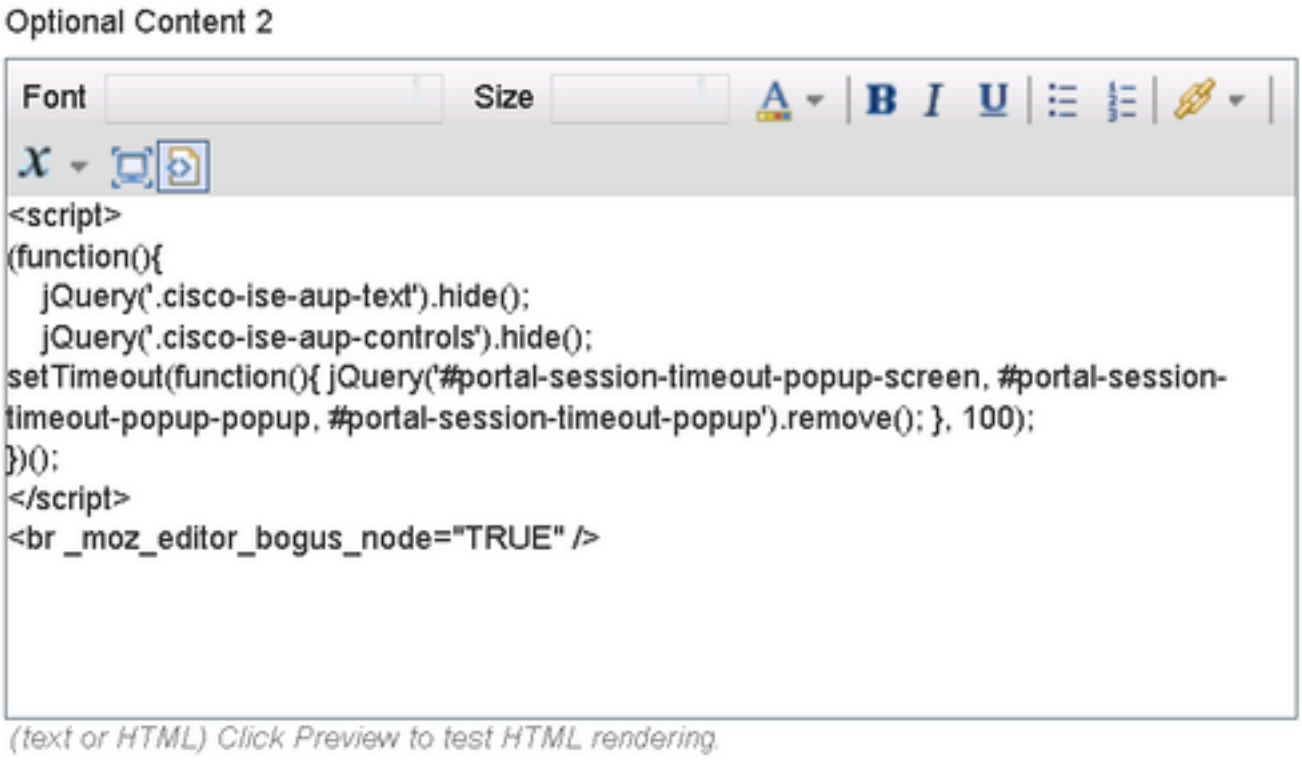
导航对**入口页面自定义**和更改标题和内容提供一适当的警告给用户。



移动对**选项内容2**，点击**乒乓键HTML来源**，并且粘贴脚本里面：

```
<script> (function(){ jQuery('.cisco-ise-aup-text').hide(); jQuery('.cisco-ise-aup-controls').hide(); setTimeout(function(){ jQuery('#portal-session-timeout-popup-screen, #portal-session-timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100); })(); </script>
```

点击**Untoggle HTML来源。**



验证

请使用在此部分被提供为了验证的信息您的配置适当地工作。

Firepower

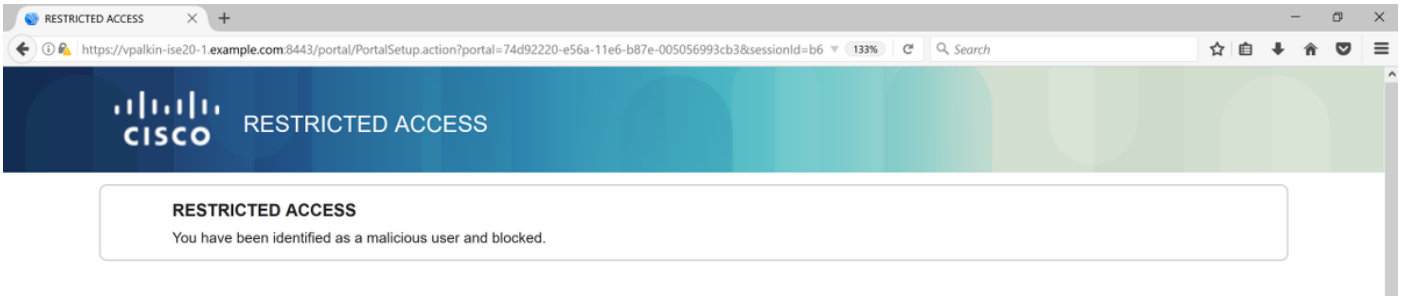
修正的触发能发生是相关性策略/规则命中数。导航对**分析>相关性>相关性事件**并且验证相关性事件发生。

ISE

ISE应该然后触发Radius ：CoA和重新鉴别用户，这些事件可以验证的运转中**> RADIUS Livelog。**

在本例中， ISE分配不同的SGT **MaliciousUser**到终端。一旦请**拒绝**用户丢失无线连接并且不能再连接的访问权限配置文件。

与黑名单门户的修正。如果修正授权规则配置重定向到门户，它如下所示:从攻击者方面：



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。

如此镜像所显示，导航对**分析>相关性>状态。**

结果消息应该返回**修正成功的完成**或特定的错误消息。验证Syslog ：**系统> Monitoring> Syslog**和过滤器输出了与**pxgrid**。同样日志在**/var/log/messages**可以验证。

相关信息

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html
- https://communities.cisco.com/docs/DOC-68284
- https://communities.cisco.com/docs/DOC-68285
- https://communities.cisco.com/thread/64870?start=0&tstart=0
- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html