如何通过 pxGrid 实现思科 Firepower 管理中心 6.0 与 ISE 和 TrustSec 的集成

目录

关于本文档

本文档专门面向希望使用平台交换架构 (pxGrid) 部署思科 Firepower 管理中心 (FMC) 6.0 和思科身份服务引擎（ISE 1.3 或更高版本）的思科工程师和思科客户。

请注意，思科 Firepower 管理中心 (FMC) 6.0 不支持 pxGrid 漏洞修复模块。

目前，思科 Firepower 管理中心 (FMC) 6.0 可根据通过 pxGrid 获取的 ISE 会话属性信息，来执行组织安全策略。这些策略可以应用到（通过思科 Firepower 执行）受管的 NGIPS 传感器和/或具备 Firepower 服务的 ASA。而且，具备 Firepower 服务的 ASA 上提供相应的选项，可以通过 ASDM 本地管理这些策略。

本文档详细说明如何使用自签证书或 CA（证书颁发机构）签名证书，在 ISE 独立环境中配置思科 Firepower 管理中心 (FMC) 6.0 和 pxGrid 与 ISE 的集成。有关如何在 ISE 生产环境中部署 pxGrid，请参阅 http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf。

在本文档中，我们将使用 ASA Firepower (SFR) 模块来配置一个具备 Firepower 服务的 ASA，并将其注册到思科 Firepower 管理中心 (FMC) 6.0，以便使用思科 Firepower 管理中心集中管理的策略。我们还将为这个具备 Firepower 服务的 ASA 配置独立于 FMC 的本地 Firepower 入侵策略和访问控制规则。

思科 Firepower 管理中心管理的安全策略和 ASA 本地 Firepower 管理策略都将包含一条入侵策略和“员工”(Employee) SGT 访问控制规则，用于拒绝对特定网络类别的访问。

本文档的使用者应熟悉 ISE、思科 Firepower 管理中心和 pxGrid 的相关知识。

解决方案简介：通过 pxGrid 将思科 Firepower 管理中心 6.0 与 TrustSec 和 ISE 集成

思科 Firepower 管理中心 (FMC) 6.0 通过将入侵策略和访问控制规则应用到 NGIPS 传感器和具备 Firepower 服务的 ASA，来集中管理和实施组织安全策略。

FMC 6.0 使用网络发现协议获取用户身份信息。此外，它还能使用 SFUA（Sourcefire 用户代理）获取更精细的用户详细信息。SFUA 用于获取用户与 IP 的映射。但是，SFUA 与 ISE 不可同时使用。

终端用户身份验证按 AD 或 LDAP 领域进行。FMC 6.0 会根据用户组信息，将包含组织安全策略的默认策略应用到思科 Firepower NGIPS 传感器或具备 Firepower 服务的 ASA。安全策略中可以包含入侵策略（以实施预先设置的均衡安全级别）以及用户组特定的访问控制规则。

思科平台交换架构 (pxGrid) 能够提供额外的 ISE 属性：安全组标记 (SGT)、终端配置文件设备信息，以及位置 IP。这些信息可在思科 Firepower 管理中心 6.0 访问控制规则策略中使用。

SGT（安全组标记）是 TrustSec 的组件之一，在 ISE 中定义，并且根据组织的安全策略在 ISE 中作为身份验证策略实施，用于身份访问权限管理。例如，所有使用公司推荐设备的有线网络用户在成功通过 ISE 进行身份验证后，分配“员工”(Employee) SGT；而使用非公司推荐设备的无线网络用户在成功进行身份验证后，分配“非员工”(Non-Employee) SGT。这些用户必须存在于 Firepower 管理中心 ISE 领域中。

FMC 6.0 会根据这些安全组标记应用访问控制规则。不仅如此，FMC 6.0 还可以使用额外的 ISE pxGrid 属性，基于情景实施 Firepower 管理中心 6.0 策略。

思科身份服务引擎 (ISE) 用于提供身份解决方案和思科平台交换架构 (pxGrid) 框架。

思科 Firepower 管理中心 6.0

思科 Firepower 管理中心 (FMC) 提供基于 Web 界面的集中管理控制台，用于管理 Firepower 设备 (NGIPS) 和 Firepower 服务。FMC 可以执行管理、分析和报告任务。它还能自动汇聚和关联入侵活动、文件、恶意软件、发现结果、连接和性能数据，从而评估事件在特定主机上的影响，并使用危害表现为主机添加标记。

思科 TrustSec

安全组标记 (SGT) 是思科 TrustSec 解决方案的一部分。它在 ISE 中定义，并在入口（网络进入点）应用。SGT 可以代表一组用户、一组终端设备、一个业务部门或一组其他对象。这样的 SGT 可以应用到网络访问策略，供设备用于做出转发决策，进而在整个网络基础设施中共享访问控制策略。SGT 是分配给安全组的一个唯一的 16 位安全组编号。除了使用 SGT 外，您也可以为安全组添加描述性名称。

SGT 在 ISE 授权策略中作为授权配置文件定义和实施（ISE 授权策略中包含用于定义组织安全策略的条件规则）。

SGT 有助于确保组织在整个网络范围实施统一的全局安全策略。

在本文档中，我们将创建一条 ISE 授权策略，使所有成功通过身份验证的终端用户划归到 /users/domain Windows 组，并为其分配“员工”(Employee) SGT。该“员工”(Employee) SGT 将用于一个由思科 Firepower 管理的访问控制规则策略，以便通过该策略拒绝对“流媒体”、“点对点应用”、“黑客”、“恶意网站”和“赌博”网络类别的访问。

思科身份服务引擎 (ISE)

身份服务引擎 (ISE) 是一项安全策略管理和身份访问权限管理平台解决方案。ISE 通过定义/颁发/执行 802.1x 身份验证、访客管理策略、终端安全评估、客户端调配和 TrustSec 策略来实现集中管理。对于 IEEE 802.1x 身份验证用户，ISE 会话目录可以提供丰富的情景信息，这些信息可用于安全解决方案，以通过 pxGrid 实现基于情景的策略。

不仅如此，ISE 还有助于轻松满足有线、无线和 VPN 连接的访问控制和安全合规要求，并推动企业安全策略计划的实施。

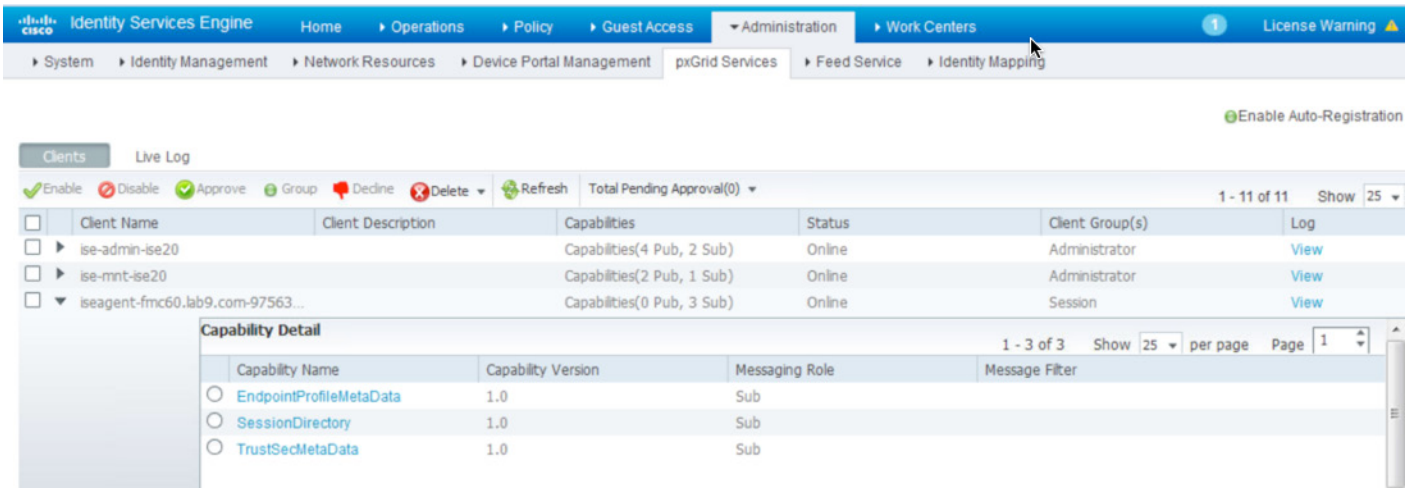
思科 pxGrid

思科平台交换架构 (pxGrid) 可在 IT 基础设施的不同部分（例如安全监控和检测系统、网络策略平台、物理和虚拟资产配置管理、身份和访问管理平台，以及几乎所有其他 IT 操作平台）之间实现跨平台的多供应商网络系统协作。

根据业务或运营需要，思科安全解决方案（如 Firepower 管理中心 6.0）和生态系统合作伙伴可以使用 pxGrid 以公开和/或订用方式交换情景信息。

技术概述

思科 Firepower 管理中心 6.0 将作为 pxGrid 客户端注册到 ISE pxGrid 节点，并通过订用 ISE 发布的主题或功能来接收 ISE 会话信息，具体包括：安全组标记 (SGT)、终端配置文件设备信息，以及终端位置。这些信息将用于 Firepower 管理中心 6.0 的访问控制功能。



ISE 会话信息包含以下函数：

- TrustsecMetadata - 提供安全组标记的编号和说明

```
SecurityGroup : id=150138d0-cfc7-11e3-9e0e-000c29e66166, name=Engineering, desc=, tag=3
```

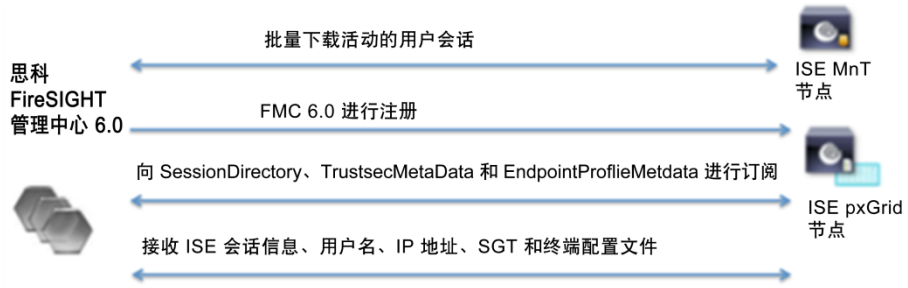
- EndpointProfileMetadata - 提供 ISE 终端策略信息，例如对 ISE 分析策略的更改/修改

```
Endpoint Profile : id=886f7570-bd0c-11e3-a88b-005056bf2f0a, name=Apple-iDevice, fqname Apple-Device:Apple-
iDevice
```

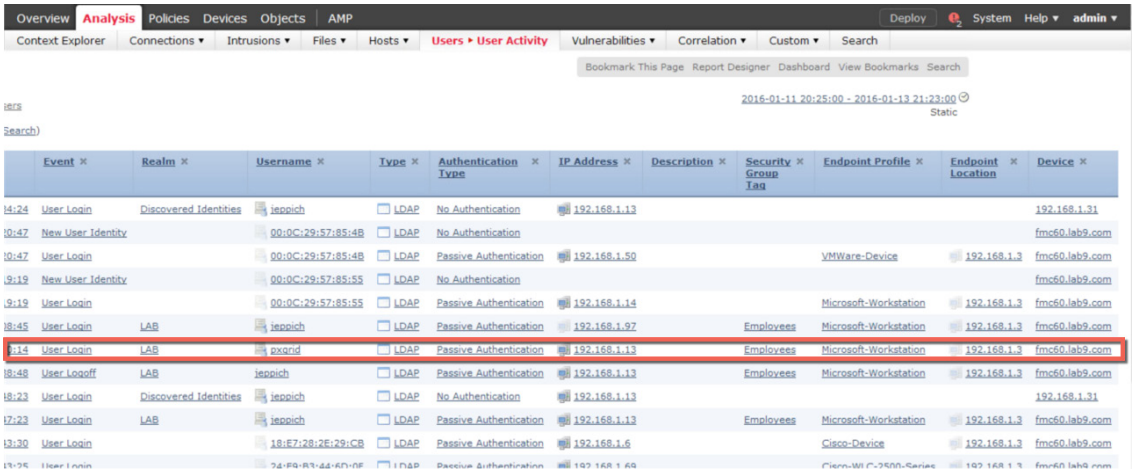
- SessionDirectory - 提供与经过身份验证的用户相关的会话属性信息，例如用户名和设备信息

```
session (ip=192.168.1.14, Audit Session Id=0A0301030000001E00FEBAD7, User Name=jsmith, Domain=lab4.com,
Calling station id=00:0C:29:77:A8:C7, Session state= STARTED, Epsstatus=null,Security Group=Engineering,
Endpoint Profile=Microsoft-Workstation, NAS IP=192.168.1.2, NAS Port=GigabitEthernet1/0/9,
RADIUSAVPairs=[ Acct-Session-Id=00000027], Posture Status=null, Posture Timestamp=, Session Last Update
Time=Tue Apr 29 15:11:46 GMT-05:00 2014
```

思科 Firepower 管理中心在启动或重新启动时，会批量下载当前活动的用户会话。此会话信息批量下载操作是通过 ISE RESTful API 在 ISE MNT 节点进行的。下载的会话信息包括：用户名、IP 地址、SGT 和终端配置文件。如果会话信息有任何更新（例如出现刚刚经过身份验证的新 ISE 用户，或者现有 SGT 被修改），这些更改会实时在思科 Firepower 管理中心的主题描述部分体现出来：



从 ISE 获得的 ISE 会话信息显示在 Firepower 管理中心的“用户活动”(User Activity) 页面中。



请注意，只有从 ISE 获得的 IEEE 802.1X 用户身份验证用户名可以应用到 FMC 6.0 策略，而且这些用户必须存在于 Firepower ISE 领域中。IEEE 802.1X 机器身份验证主机名或 MAC 地址用户名无法应用到 FMC 6.0 策略。

思科身份服务引擎动态安全组标记

组织安全策略可以根据安全组标记 (SGT) 定义。这可以确保组织能够在整个网络范围实施统一的全局安全策略。如果组织交换机中启用了 TrustSec，安全组标记也将能够实施到网络中。通常情况下，安全组标记 2 会分配给交换机、路由器和防火墙等网络设备。

在本文档中，我们为成功通过身份验证，并且属于 Windows 用户域组的终端用户分配名为“员工”(Employee) 的动态 SGT。该 SGT 将被用于一条由 Firepower NGIPS 虚拟传感器和具备 Firepower 服务的 ASA 使用并实施的 Firepower 管理中心访问控制规则。

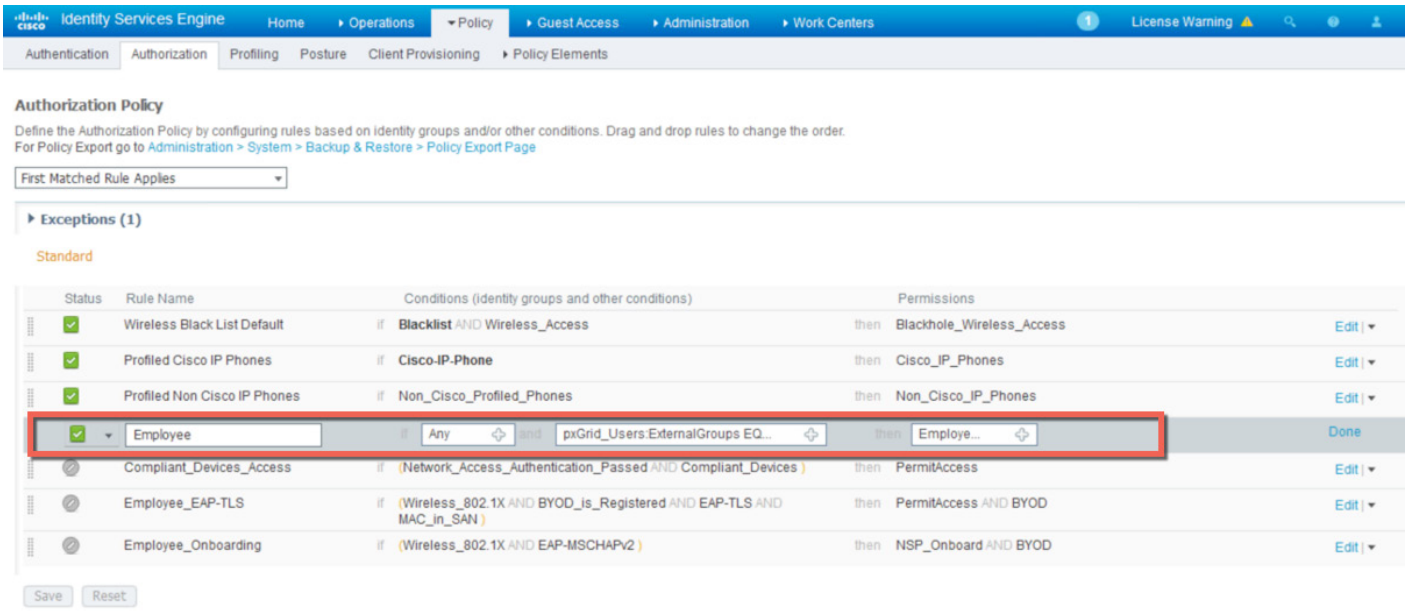
请注意，您可以直接从 ISE 身份验证策略或 ISE 的“工作中心”(Work Center) -> TrustSec ->“组件”(Components) ->“安全组”(Security Groups) 菜单配置更多安全组标记。

步骤 1 创建“员工”(Employee) 安全组标记

选择“策略”(Policy) -> “授权”(Authorization) ->  -> 

，然后输入以下信息：

角色名称：Employee；
新建条件：External Groups:equals:pxGrid_Users
授权配置文件：Employee and Permit Access



步骤 2 选择**完成 (Done)**

选择**保存 (Save)**

使用自签证书的操作步骤

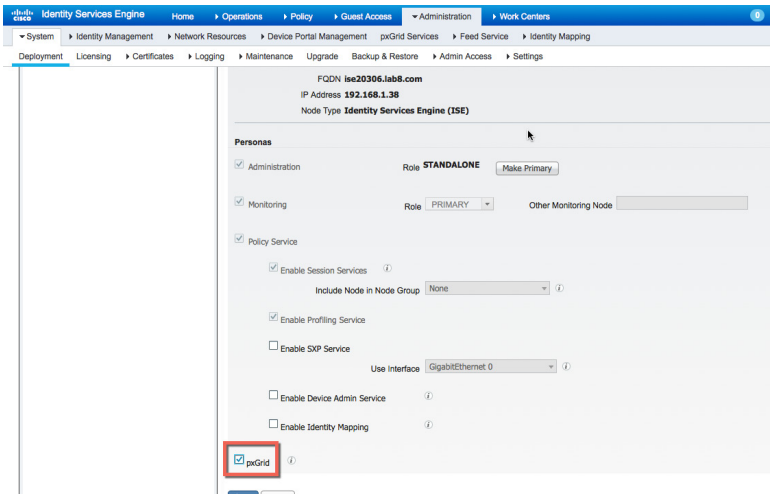
使用自签证书的操作步骤仅适用于 POC 环境。如果您需要部署 CA 签名证书，本节内容为可选操作。

配置 ISE 2.0

自签证书可用于 POC 环境。在本配置中，ISE 以独立配置部署。

注意：ISE 2.0 不再像 ISE 1.3 和 ISE 1.4 那样，需要将自签身份证书导出到 ISE 受信任证书库中。

步骤 1 选择**管理 (Administration) -> 系统 (System) -> 部署 (Deployment)，然后选择节点，点击编辑 (Edit)，并选中 pxGrid 复选框**

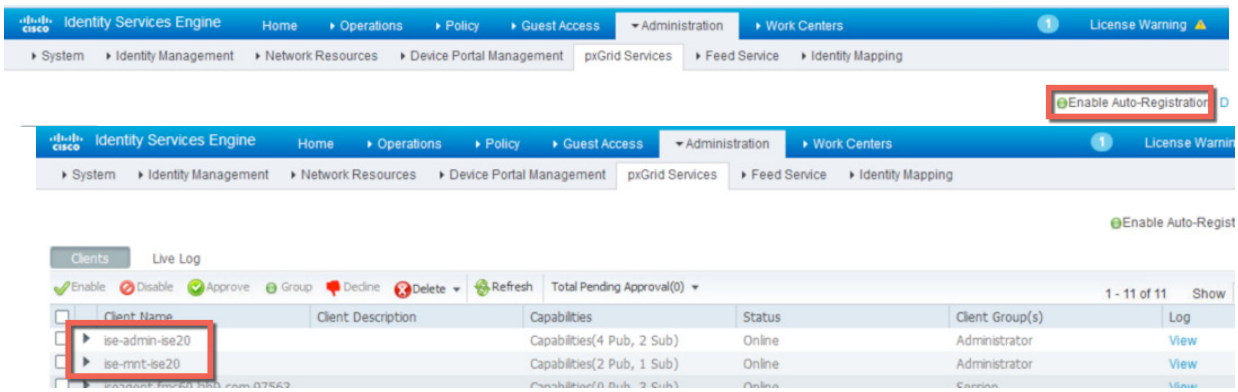


步骤 2 选择**保存 (Save)**

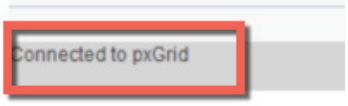
步骤 3 确认已发布的节点显示在“pxGrid 服务”(pxGrid Services) 下，而且状态为已连接。
管理 (Administration) -> pxGrid 服务 (pxGrid Services)

注意：已发布的节点可能需要经过一段时间后才会显示。您可以通过在 ISE VM 节点上运行 **sh application status ise** 命令来检查 pxGrid 服务是否已经启动。

步骤 4 选中**启用自动注册 (Enable Auto-Registration)**



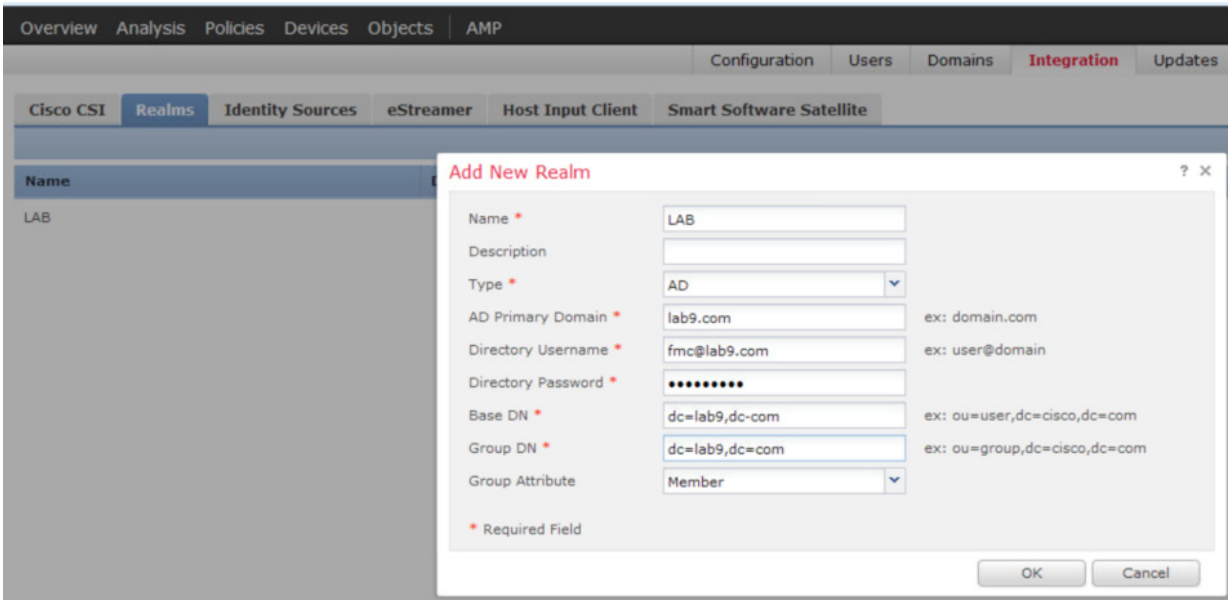
步骤 5 确认状态是否为**已连接到 pxGrid (Connected to pxGrid)**



创建 Firepower ISE 领域

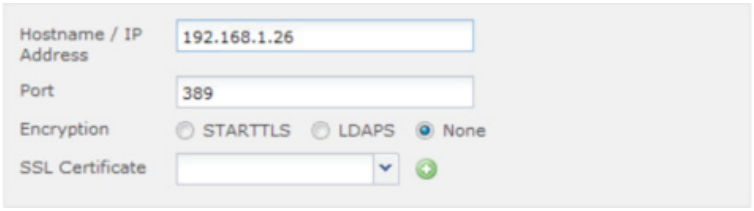
ISE 领域用于 ISE 身份验证，需要在 Firepower 管理中心 6.0 的身份策略中使用。

步骤 1 选择**系统 (System) -> 集成 (Integration) -> 领域 (Realms) -> 新建领域 (New Realm)**



步骤 2 选择**确定 (OK)**

步骤 3 选择**添加目录 (Add Directory)**，然后输入 FQDN 主机名或相关信息



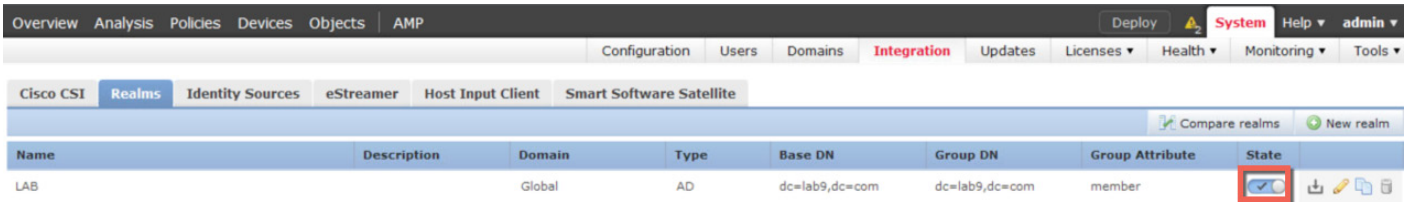
步骤 4 选择**测试 (Test)**，您应看到**已成功测试连接 (Test Connection has succeeded)** 消息，此时选择**确定 (OK)**

注意：如果系统提示尝试失败，请检查“领域配置”(Realm Configuration) 中是否设置了正确的目录用户名和目录密码。

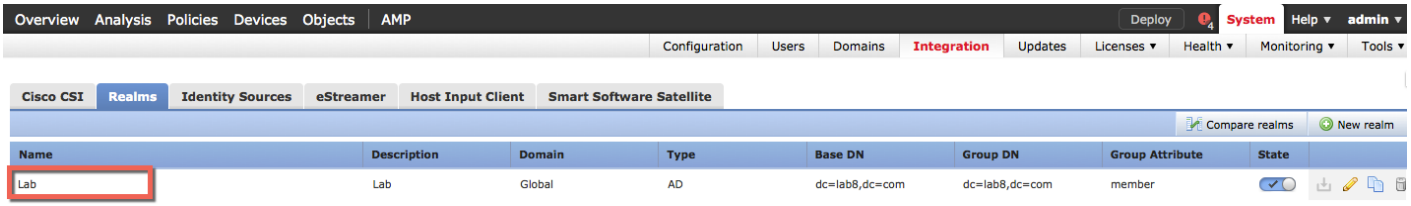
步骤 5 选择**确定 (OK)**

步骤 6 选择**保存 (Save)**

步骤 7 选择  启用状态



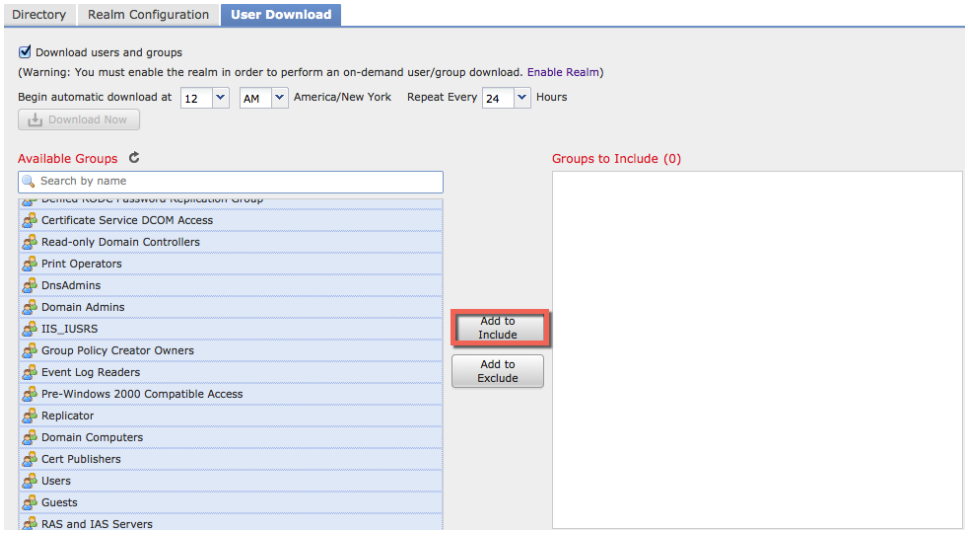
步骤 8 点击**领域 (Realm)**，然后选择一个名字



步骤 9 点击**用户下载 (User Download)**

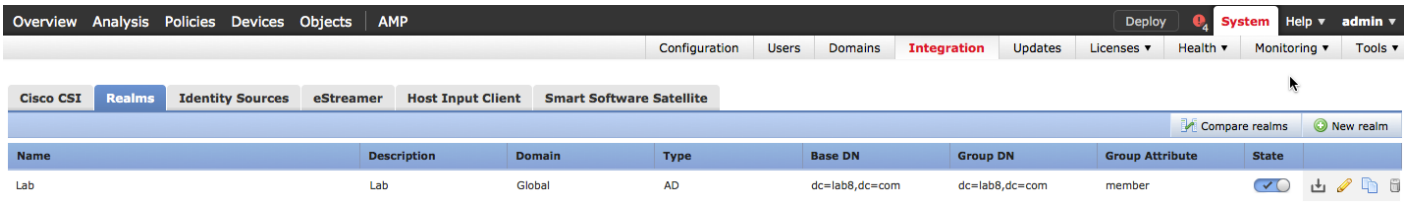
步骤 10 选中**下载用户和组 (Download users and groups)**

步骤 11 选中“可用组”(Available Groups) 下的所有项使其突出显示，然后选择**添加到包括项 (Add to Include)**



步骤 12 选择**保存 (Save)**

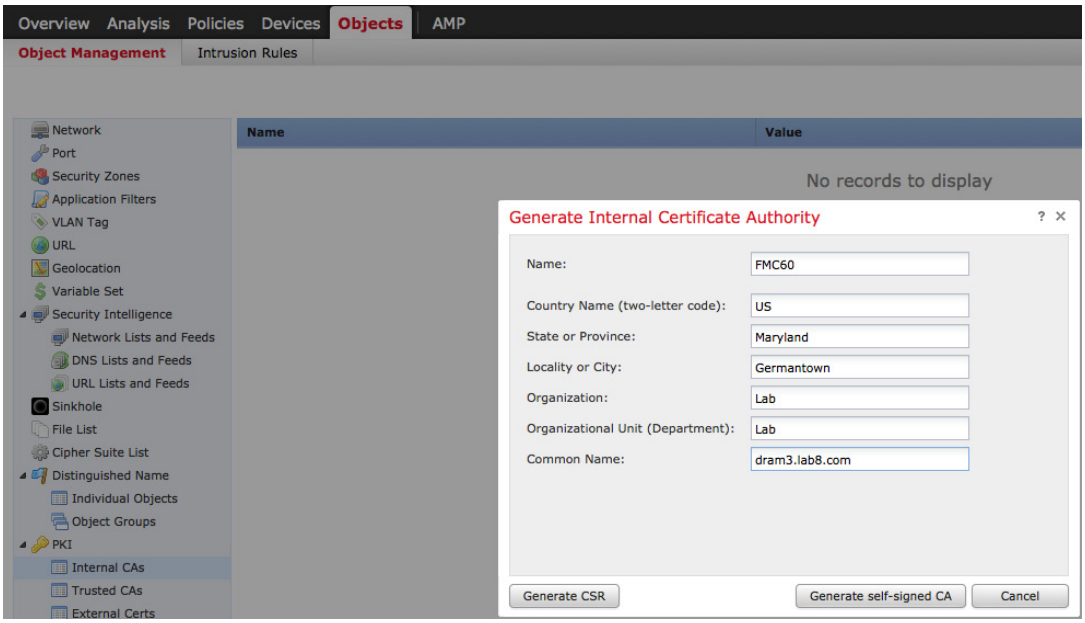
步骤 13 您将看到以下内容：



配置 Firepower 管理中心 6.0

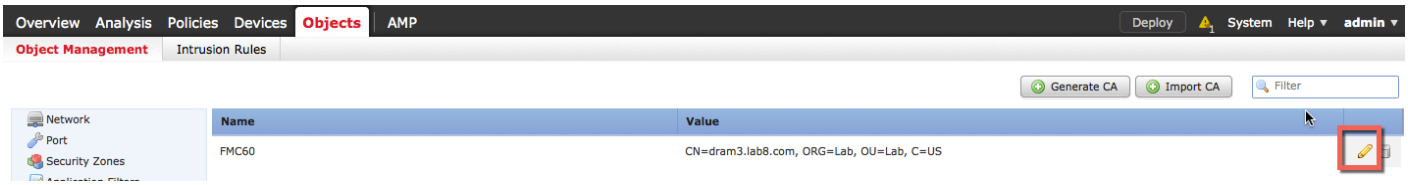
在本节中，我们将配置 Firepower 管理中心 (FMC)，以使用自签证书执行 ISE pxGrid 节点操作。我们将在 Firepower 管理中心中创建一个内部 FMC 证书颁发机构，然后将其转换为证书，导入到 Firepower 管理中心的内部证书库。我们还将把内部 FMC 公共证书导出到 ISE 证书受信任系统库中，并将 ISE 身份自签公共证书导入到 Firepower 管理中心受信任 CA 库。

步骤 1 选择**对象 (Objects) -> 对象管理 (Object Management) -> PKI -> 内部 CA (Internal CAs) -> 生成 CA (Generate CA)**，然后提供下图所示的证书信息：
在本例中，内部 CA 被命名为“FMC60”

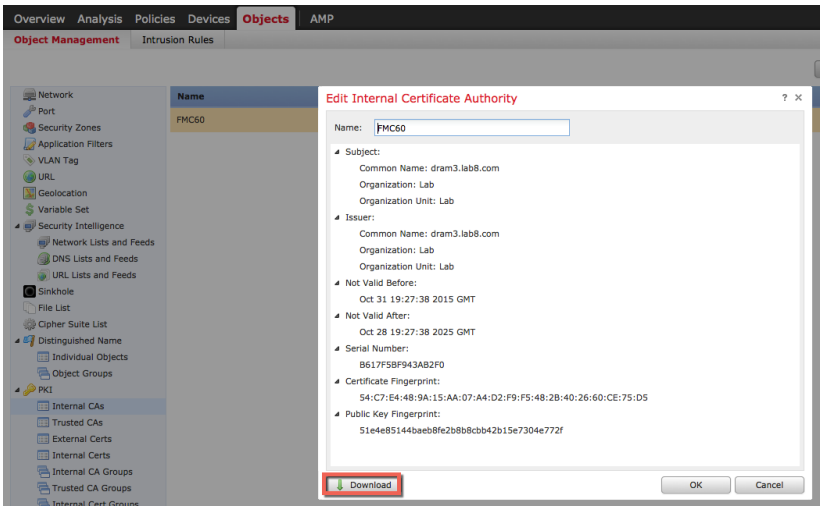


步骤 2 选择**生成自签名 CA (Generate self-signed CA)**

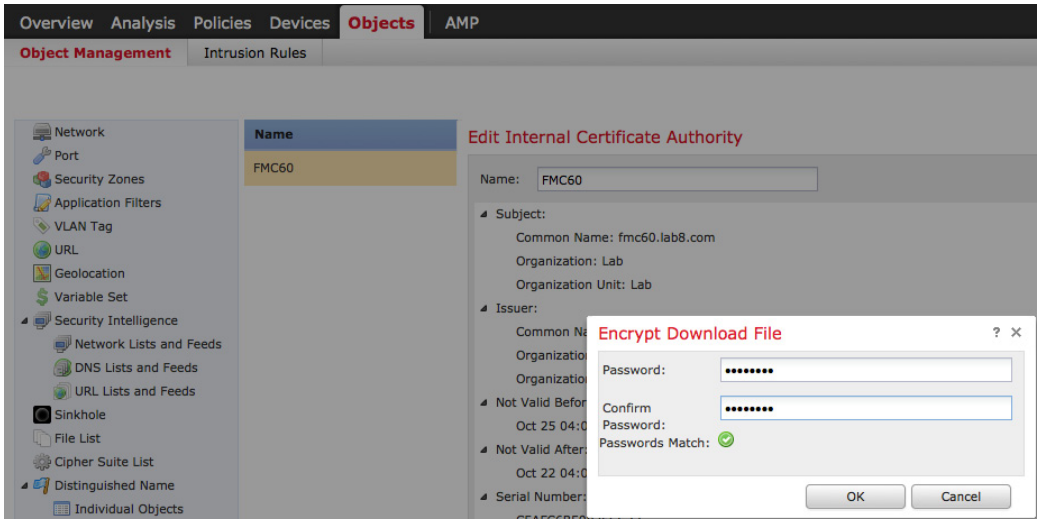
步骤 3 点击下图所示的“铅笔”图标，下载 CA 证书文件



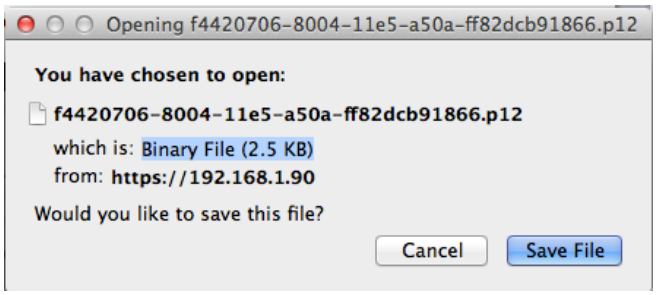
步骤 4 选择**下载 (Download)**



步骤 5 输入加密密码，然后选择**确定 (OK)**。本例中输入的密码是 cisco123

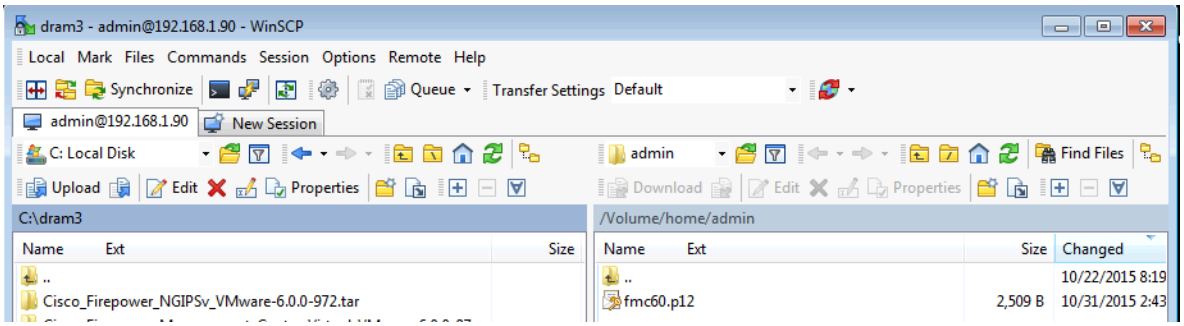


步骤 6 在本地保存 .p12 文件



步骤 7 重命名该 .p12 文件名以使其更易于处理。在本例中，文件被重命名为“fmc60.p12”。

步骤 8 使用 WinSCP 或其他工具将文件上传到 Firepower 管理控制台



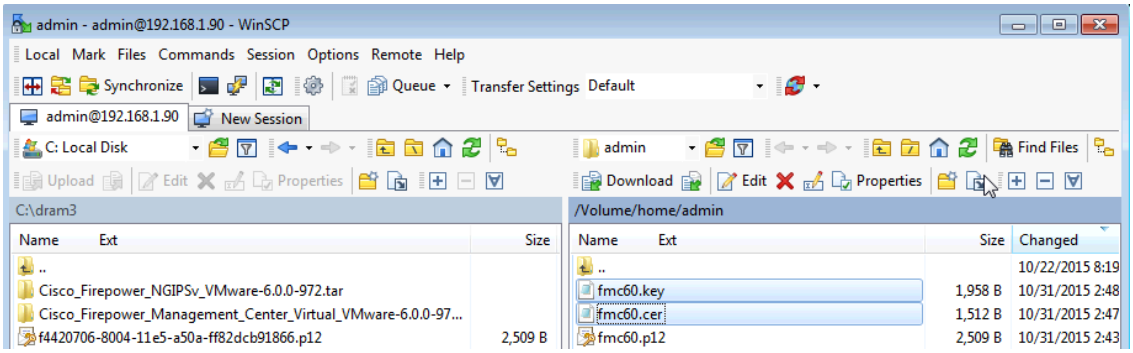
步骤 9 通过 SSH 连接到 Firepower 管理控制台

步骤 10 通过键入以下命令将 .p12 文件转换为 CER 和 KEY 文件：

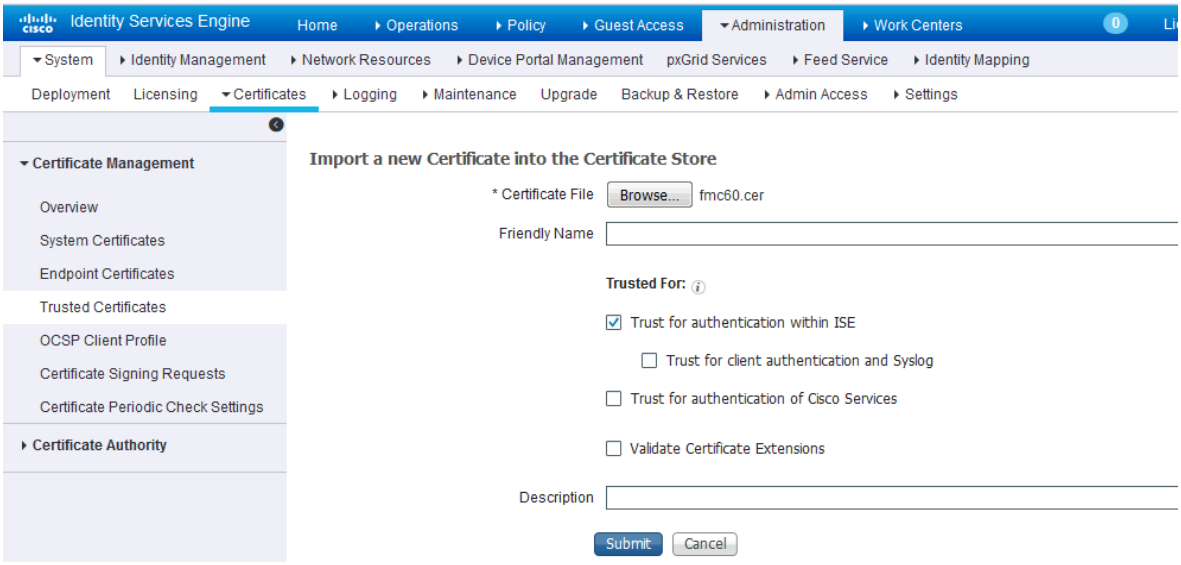
注意：CER 和 KEY 文件名是随机的。我们将原始 .p12 文件重命名为“fmc60.p12”。首先，系统会提示您输入 sudo 密码。导入密码和 PEM 口令是您之前输入的加密密钥密码。

```
sudo openssl pkcs12 -nokeys -clcerts -in fmc60.p12 -out fmc60.cer
Enter Import Password:
MAC verified OK
admin@sd:~$



sudo openssl pkcs12 -nocerts -in fmc60.p12 -out fmc601.key
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
admin@sd:~$
```

步骤 11 使用 WinSCP 将 fmc60.cer 和 fmc60.key 文件从 Firepower 管理中心复制到本地 PC。

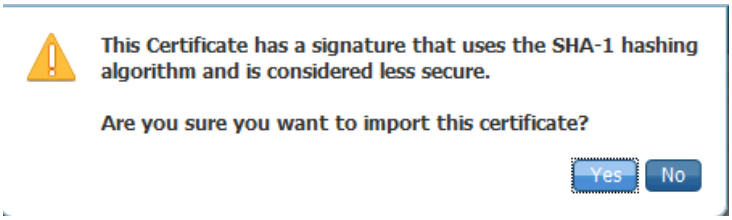


步骤 12 Firepower 管理中心内部 CA 公共证书将被导出到 ISE 证书信任库中。
选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 受信任证书 (Trusted Certificates) -> 浏览 (Browse)**，然后上传 fmc60.cer

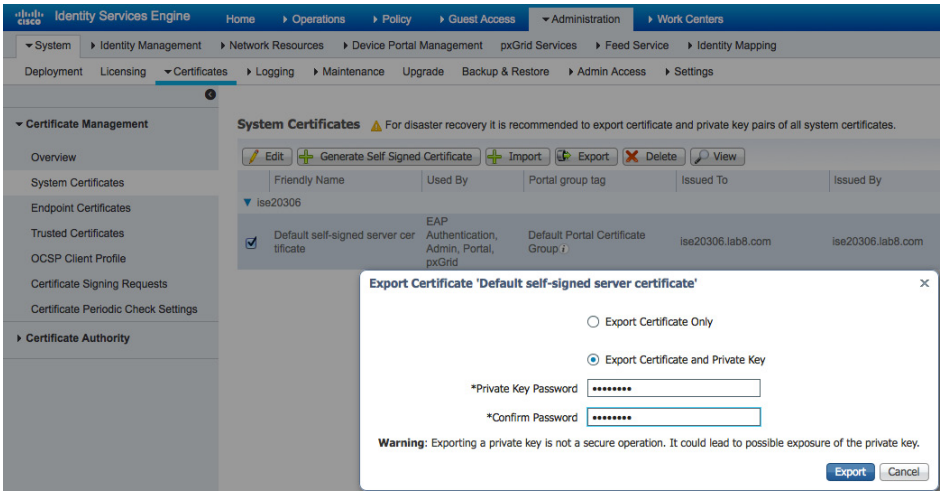


步骤 13 选中“信任 ISE 内的身份验证”(Trust for authentication within ISE)，然后选择**提交 (Submit)**

步骤 14 在导入 FMC 证书时，您会看到如下警告消息，选择**是 (Yes)**



步骤 15 选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates)，选择 ISE 身份自签证书，点击导出 (Export)**，然后选中“导出证书和私钥”(Export Certificate and Private Key)

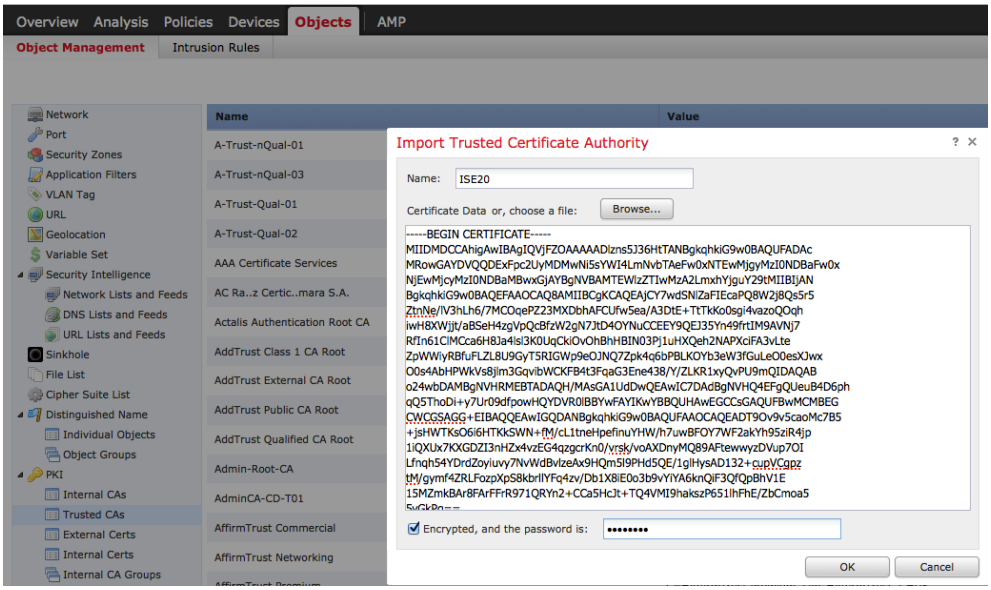


注意：文件将保存为 Defaultserversignedcerti.zip 文件。您需要解压该文件，仅将公共证书 PEM 文件导出到 FMC 受信任库。您可以将文件重命名为 ISE2.0.pem，以使其更易于识别。

步骤 16 将 ISE 自签身份证书导入到 Firepower 管理中心受信任 CA 库中

选择**对象 (Objects) -> 对象管理 (Object Management) -> PKI -> 受信任 CA (Trusted CAs) -> 添加受信任 CA (Add Trusted CA)**，然后输入名称。本例中使用的是“ISE”。

为 ISE 输入加密密钥密码，然后点击**确定 (OK)**

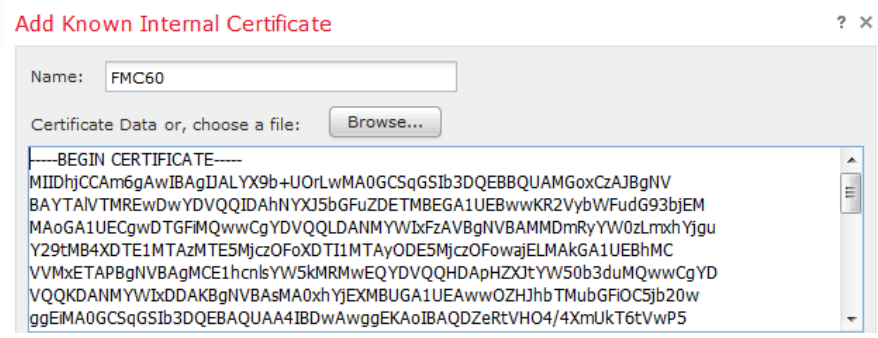


步骤 17 将 Firepower 管理中心内部 CA 公钥/密钥对导入到 Firepower 管理中心的内部证书库

选择**对象 (Objects) -> PKI -> 内部证书 (Internal Certs) -> 添加内部证书 (Add Internal Cert)**

针对私钥按照同一程序执行操作

注意：删除袋属性，直至到达 ----Begin Certificates



步骤 18 请删除密钥文件的袋属性，直至您正好位于“---Begin…”之前。

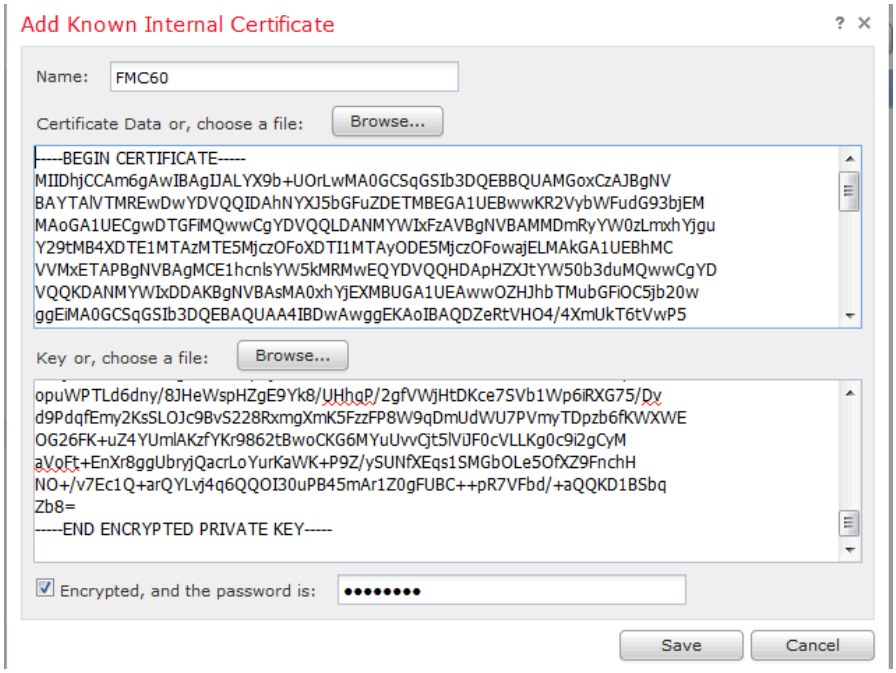
```
Bag Attributes
    localKeyID: 3D DA 20 3E A2 9A 99 ED 5D 2C 30 53 73 8E 1D 67 4A 52 8E 9C
Key Attributes: <no attributes="">
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQIIpjU/hWvevACAggA
MBQGCCqGSIb3DQMHBAgh7ZvVZ8MMGgSCBMjooxQEN+/wWMHo6FH2cJ+qAHhD0V3T
hHVq2py8G19lBecv5R6ltY6oY2kpaYjRY3jSkuCxGcwtpUFW03uVBHde7E2vNpXP
mpVX2sZqQ/xuRhS7a3ihh9qq357jAA1ecI+nJ9N1omMriX16r87VJKDfjqCBJ+HI
```

步骤 19 还需要删除“</no>”

```
McCjBykAv73MXKY8FQJl2MyWoYmJ84qr2NTajqhpyS/UFavOkMsx2l9nBtzV+Hxd
DPycz8/fK1jQWwE7Y/6SUOeQ8hUMMaAeNYqfagA0Jhwntn/8y+A6R3ytK4AoZCtQ
9WQMizAi2N9jneQxjI4SOjnjUSiwqKHwB2wHFEFu9pR6ZfMoN7xU3eYDlJ/n1SgO
ENlYYGfOjCs7kNxVwqtc21FfQ0URkEZ9jOUFuj55EqTdXxbCdFTTKmHjZdQmCICA
3hOWu5IkHHTA5Kre05AYLe1lhW3xE5qL8yH5XOSfdREwq1aX2GU4BEQqGMDtkGbq
D7w=
-----END ENCRYPTED PRIVATE KEY-----
</no>
```

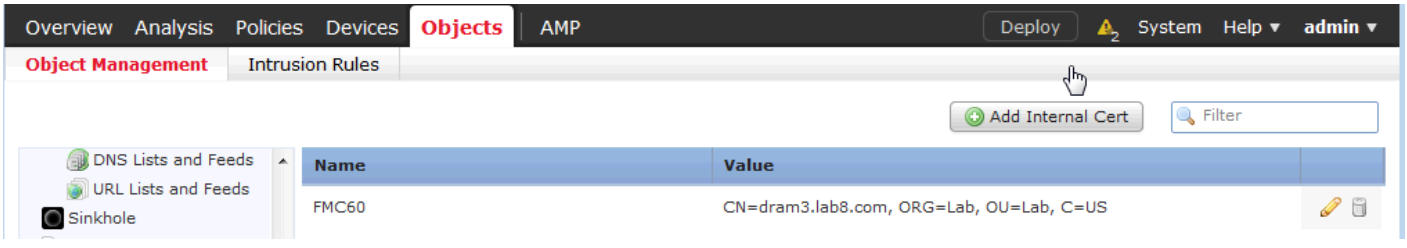
步骤 20 输入加密密码

步骤 21 您将看到以下内容：



步骤 22 选择**保存 (Save)**

您将看到以下内容：

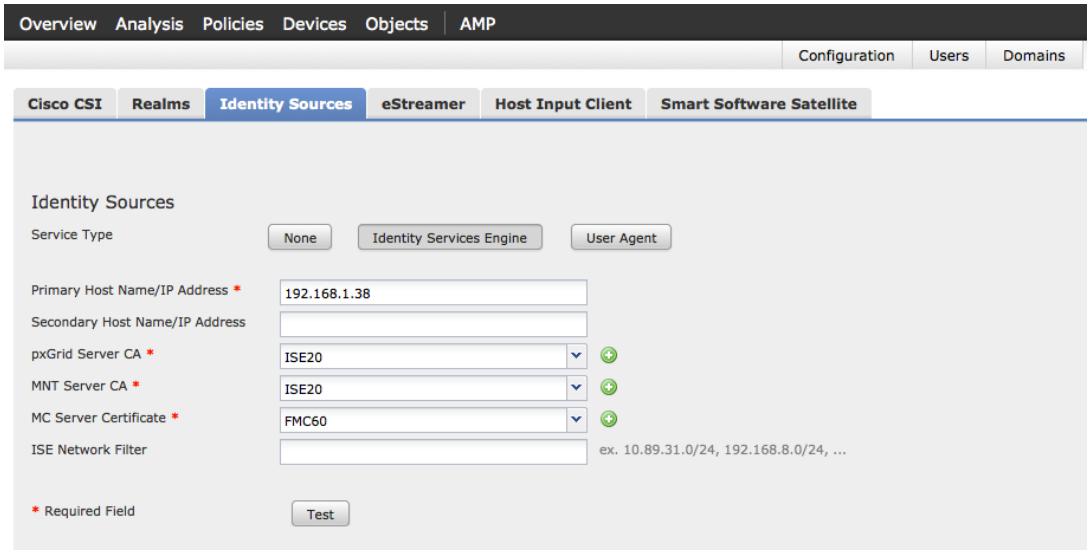


配置 Firepower ISE 身份源

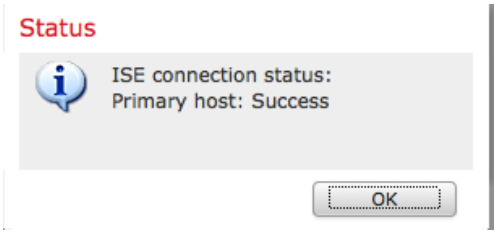
身份源引擎配置定义了 ISE pxGrid 节点连接参数、ISE MnT 节点证书和 FMC 6.0 身份证书。

步骤 1 选择**系统 (System) -> 集成 (Integration) -> 身份源 (Identity Sources) -> 身份服务引擎 (Identity Services Engine)**

主要主机名称/IP 地址 (Primary Host Name/IP Address) - 主 FQDN pxGrid 的名称或 IP 地址
辅助主机名称/IP 地址 (Secondary Host Name/IP address) - 辅助 FQDN pxGrid 的名称或 IP 地址
**pxGrid 服务器 CA (pxGrid Server CA)* - ISE pxGrid 节点证书（导入的 ISE 自签身份证书）
**mnt 服务器 CA (mnt Server CA)* - ISE pxGrid 节点证书（导入的 ISE 自签身份证书）
MC 服务器证书 (MC Server Certificate) - FMC 身份证书（导入的内部证书）

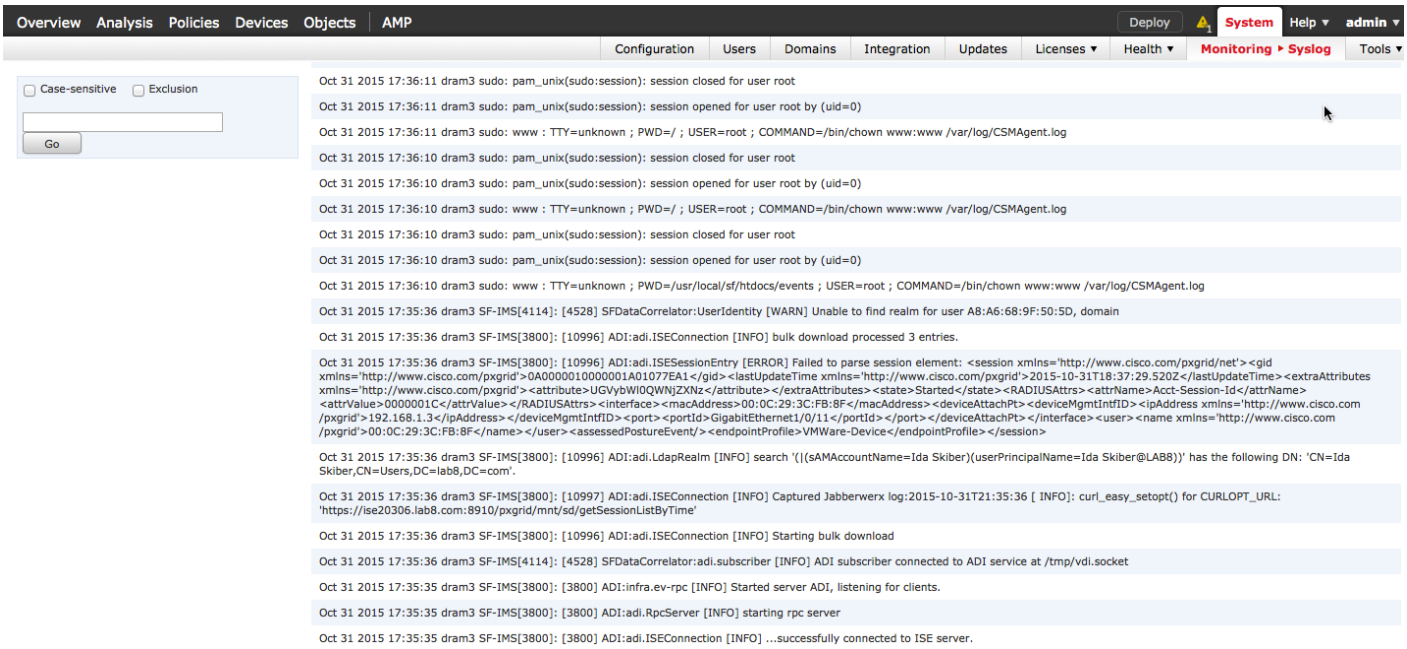


步骤 2 选择**测试 (Test)**
您应该看到以下内容

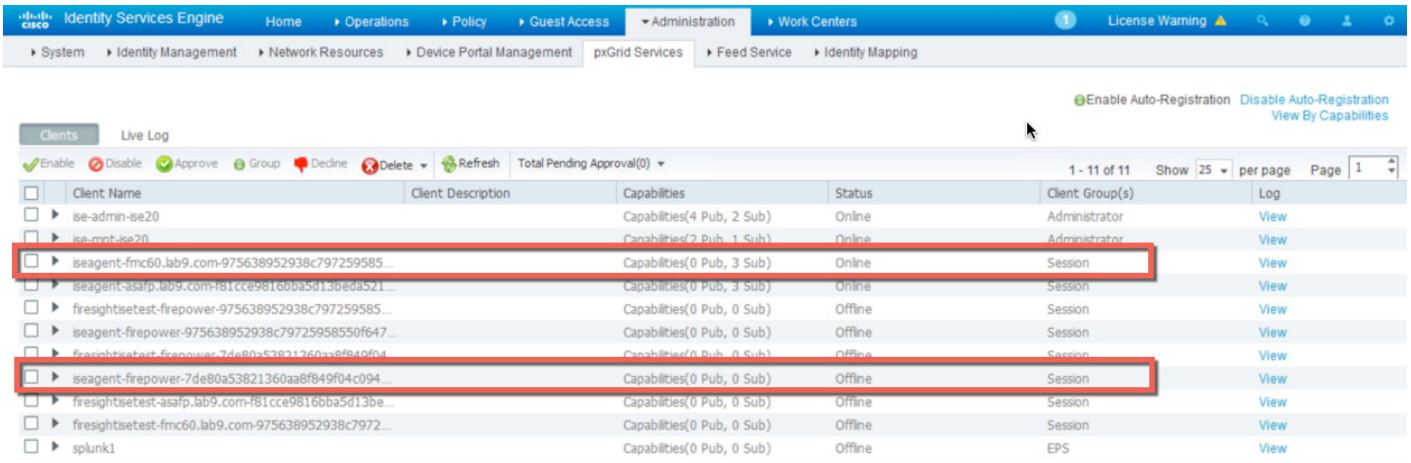


步骤 3 选择**确定 (OK)**
步骤 4 选择**保存 (Save)**

步骤 5 选择**系统 (System) -> 监控 (Monitoring) -> 系统日志 (Syslog)**
注意查看 FMC 是否已成功连接到 ISE 服务器



步骤 6 您应在 ISE 中看到下列项



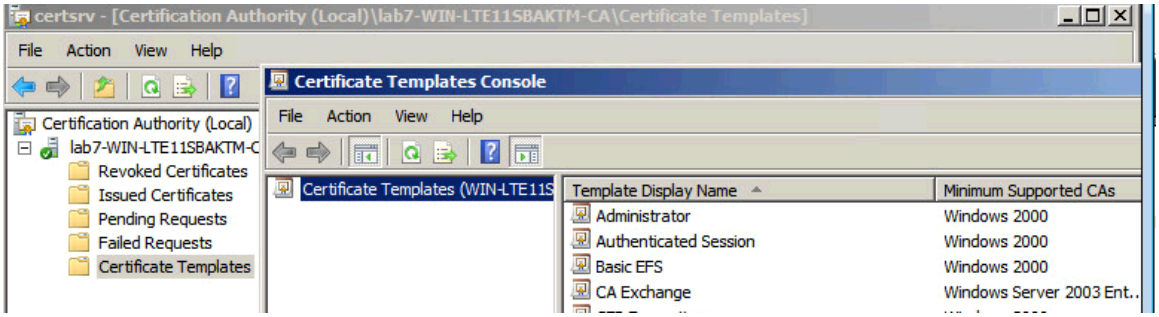
使用 CA（证书颁发机构）签名证书的操作步骤

本节介绍在 ISE 独立环境中部署 ISE 2.0 和思科 Firepower 管理中心 6.0 的详细配置信息。如果您需要部署自签证书，本节内容为可选操作。

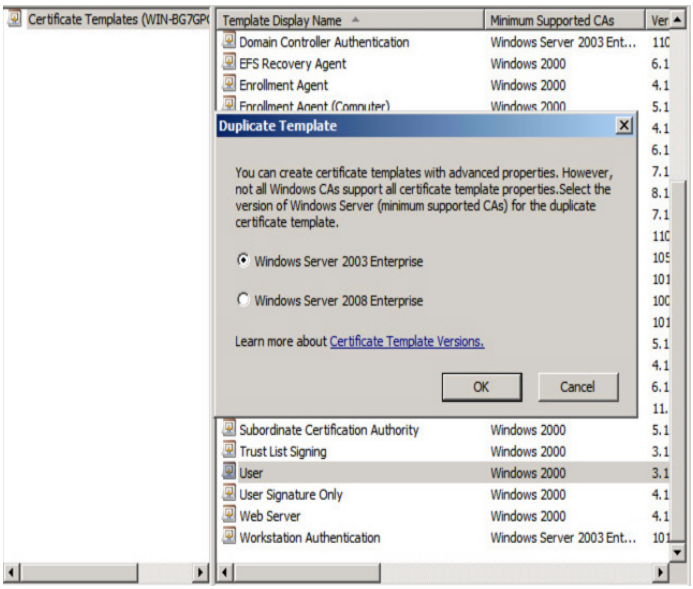
用于 CA 签名证书操作步骤的自定义 pxGrid 模板

要在 pxGrid 客户端、Firepower 管理中心和 ISE pxGrid 节点之间实现 pxGrid 操作，必须创建一个自定义 pxGrid 模板，并在其中加入同时支持客户端身份验证和服务器身份验证的增强型密钥用法 (EKU)。对于 Firepower 管理中心和 ISE pxGrid 节点均由同一证书颁发机构 (CA) 进行签名的 CA 签名环境，此步骤是必需的。

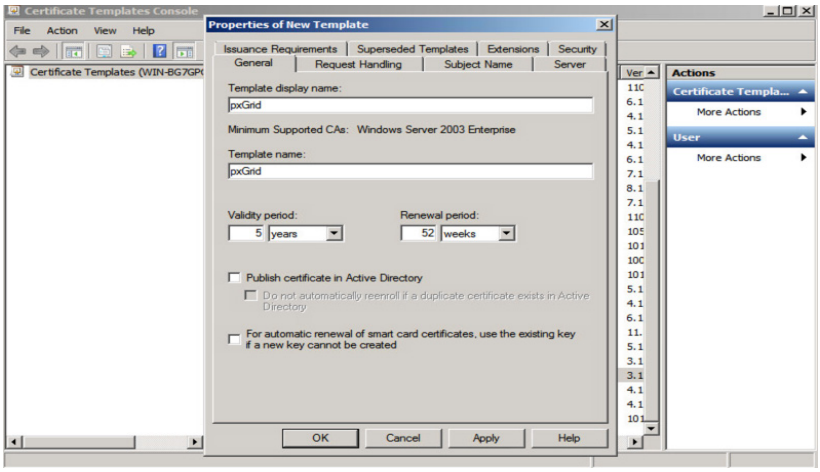
步骤 7 选择**管理工具 (Administrative Tools) -> 证书颁发机构 (Certificate Authority)**，点击 CA 服务器旁边的“+”展开下拉列表，然后右键点击**证书模板 (Certificate Templates)**，选择**管理 (Manage)**



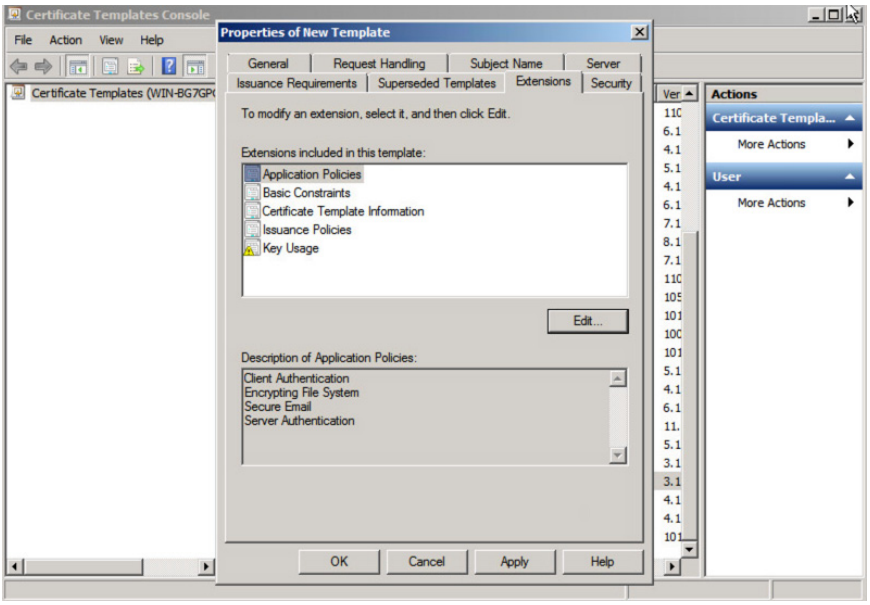
步骤 8 右键点击并复制用户模板，选中 **Windows Server 2003 Enterprise，并点击确定 (OK)**



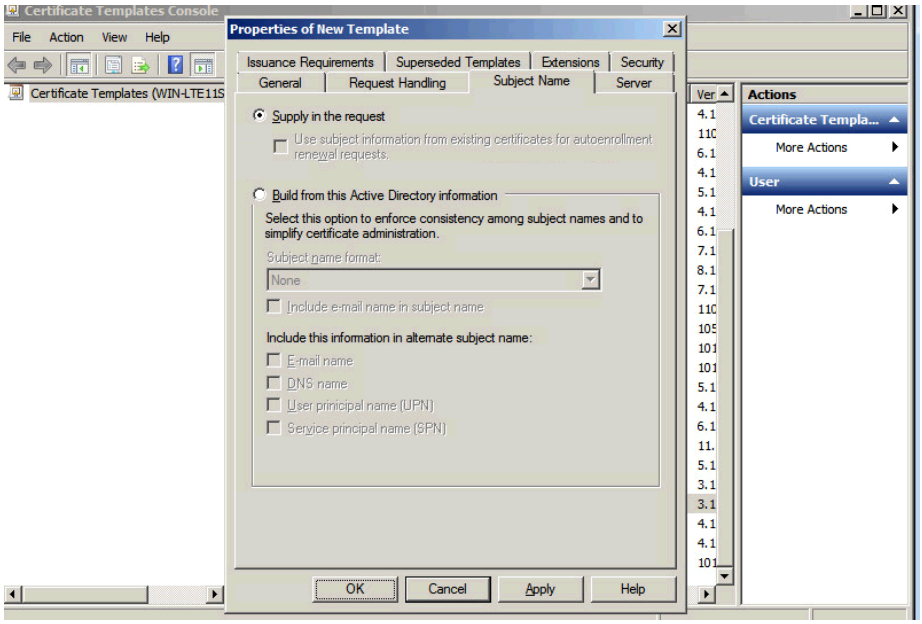
步骤 9 输入证书模板的名称，取消选中“在 Active Directory 中发布证书”(Publish certificate in Active Directory)，并提供有效期和更新期。



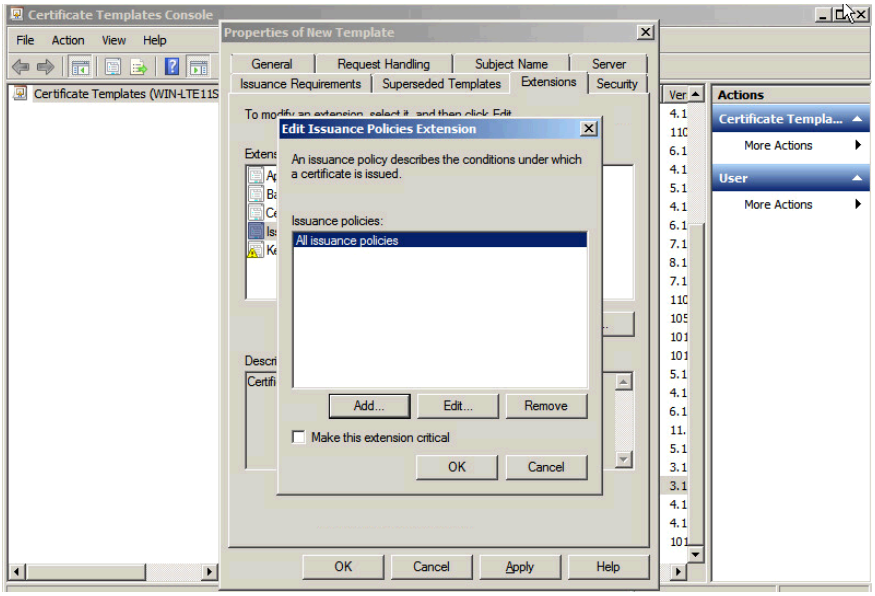
步骤 10 点击“扩展”(Extensions)，选择**添加 (Add) -> 服务器身份验证 (Server Authentication) -> 确定 (OK) -> 应用 (Apply)**



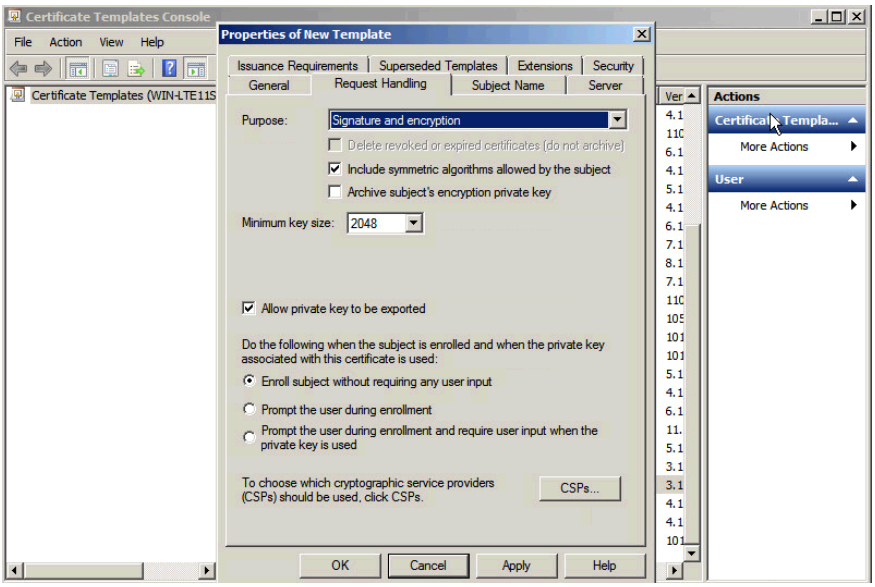
步骤 11 点击“主题名称”(Subject Name)，选中“在请求中提供”(Supply in the request)



步骤 12 点击**扩展 (Extensions) -> 颁发策略 (Issuance Policies) -> 编辑 (Edit) -> 所有颁发策略 (All Issuance Policies)**

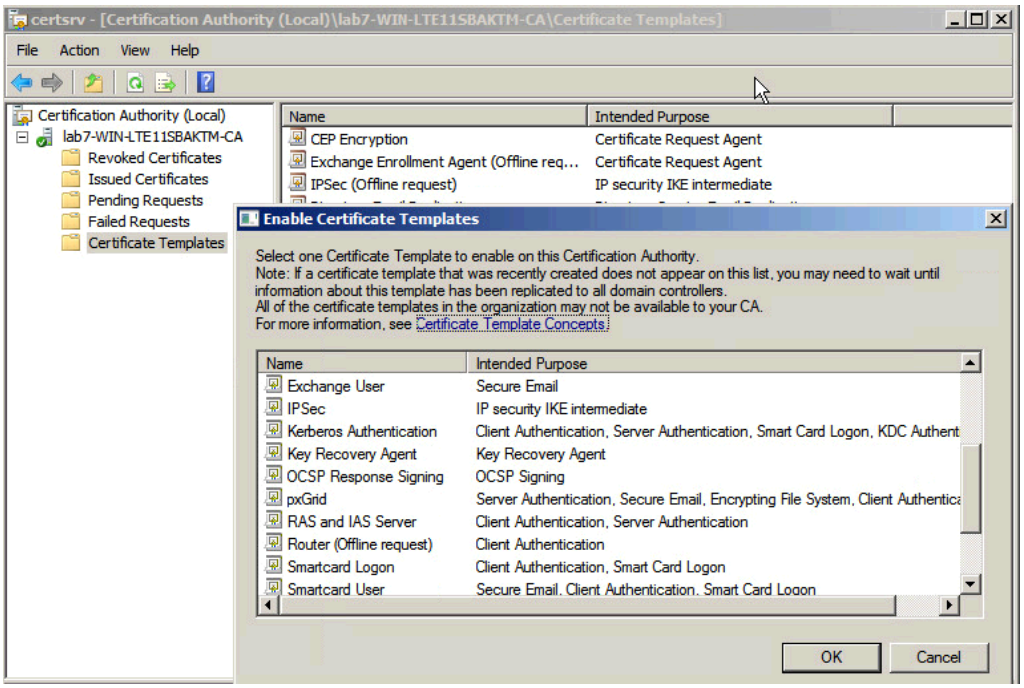


步骤 13 保留请求处理的默认设置

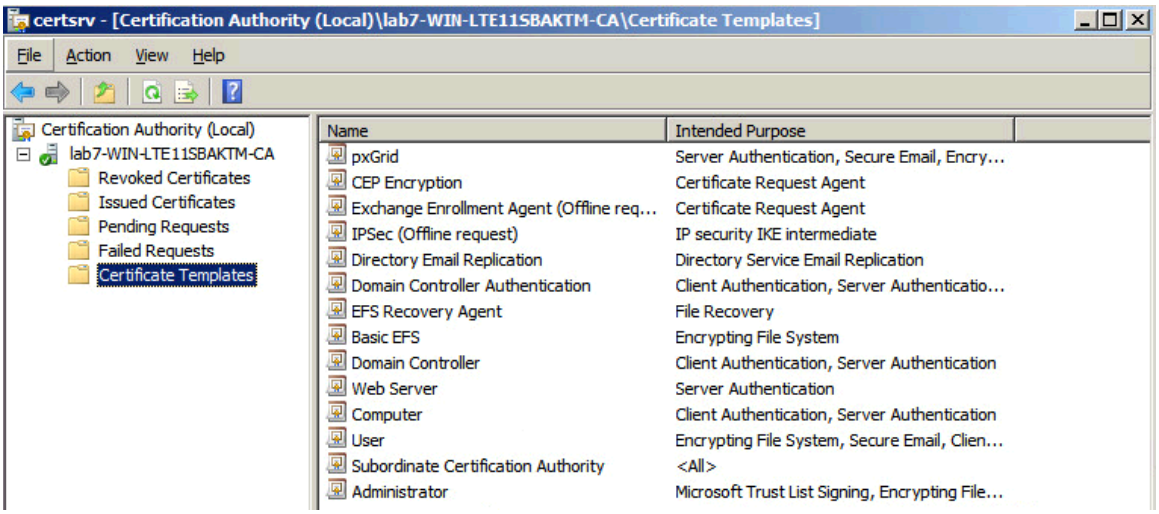


步骤 14 右键点击“证书模板”(Certificate Templates)

步骤 15 选择**要颁发的新模板 (New Template to issue) -> pxGrid**



步骤 16 您应该看到 pxGrid 模板



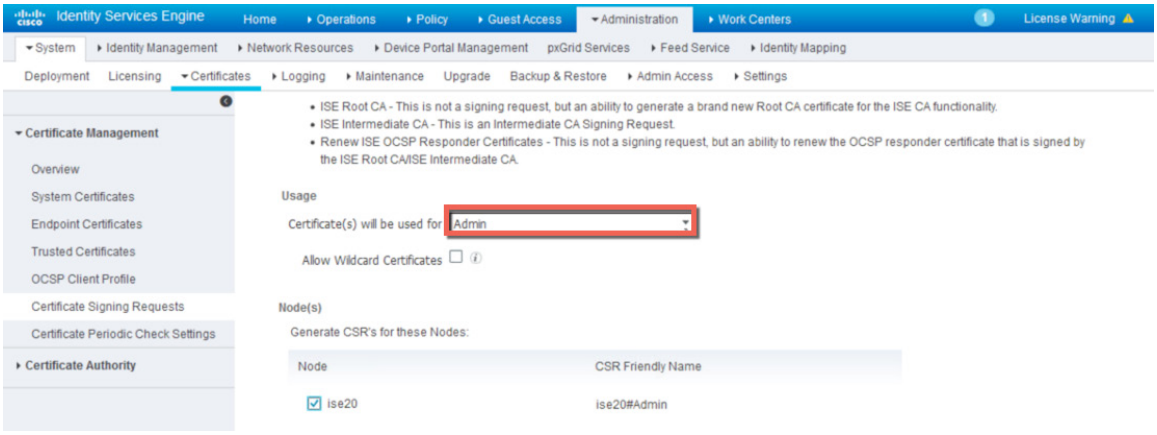
配置 ISE 2.0

接下来，我们将为独立配置的证书颁发机构 (CA) 签名环境配置 ISE pxGrid 节点。最初，使用 pxGrid 自定义模板从 ISE 节点生成“pxGrid”CSR 请求并由 CA 服务器签名。证书将绑定到初始 ISE CSR 请求。

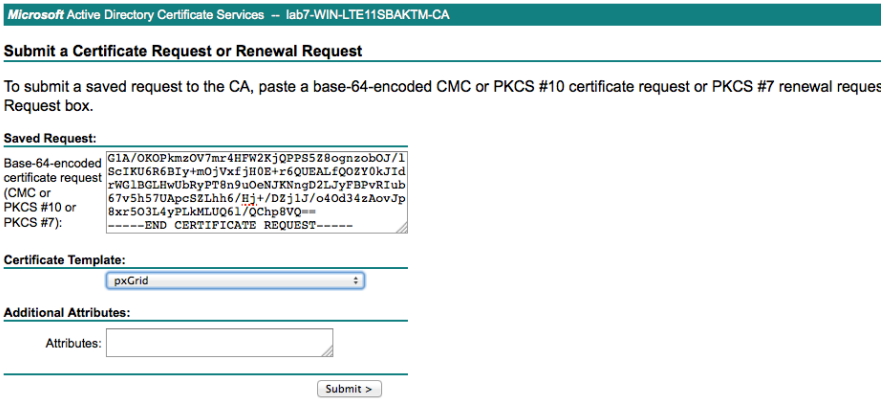
CA 根证书将导入到 ISE 证书受信任库中。ISE 身份证书将在 ISE 证书系统库中导出。将为 pxGrid 操作启用 ISE 节点。

步骤 1 请为将成为 ISE pxGrid 节点的 ISE 节点生成 CSR 请求
管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 证书签名请求 (Certificate Signing Requests) -> 生成 (Generate)

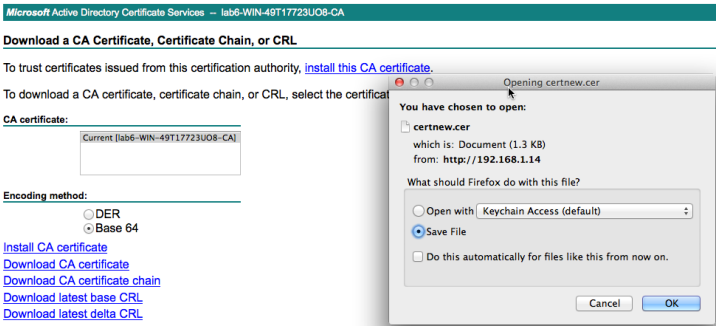
注意：证书使用选项应设置为“管理员”(Admin)。要保证 FMC 6.0 批量下载活动会话，必须进行此设置



步骤 2 选择“请求证书”(Request a Certificate) ->“高级证书请求”(Advanced Certificate Request)，将 CSR 请求复制并粘贴到“已保存的请求”(Saved Request) 部分，然后选择自定义 pxGrid 模板，并点击“提交”(Submit)

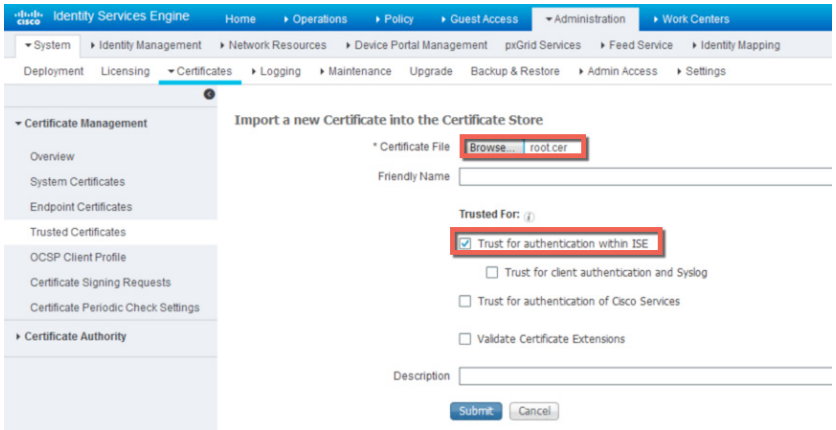


步骤 3 下载 Base 64 编码格式的 CA 根证书



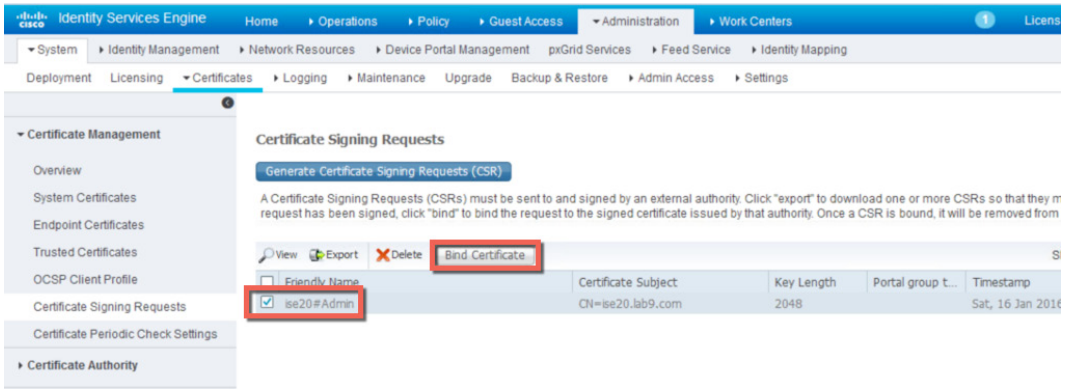
步骤 4 将 CA 根证书上传到 ISE 证书受信任系统库中
选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 受信任证书 (Trusted Certificates)**，并上传 CA 根证书

步骤 5 选中“信任 ISE 内的身份验证”(Trust for authentication within ISE)，然后选择**提交 (Submit)**



步骤 6 将 ISE pxGrid 节点证书上传到 ISE 证书系统库中

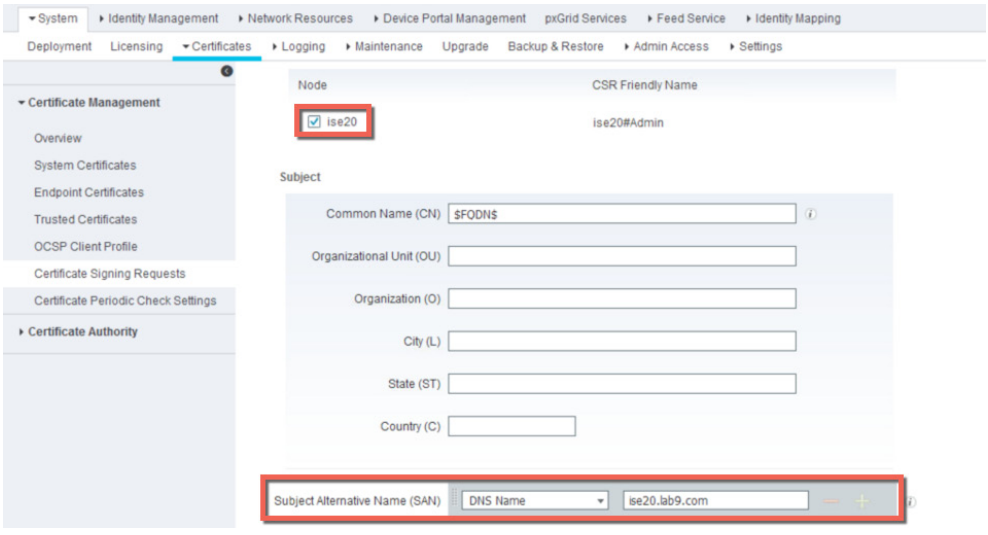
选择管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 证书管理 (Certificate Management) -> 证书签名请求 (Certificate Signing Requests)，然后点击“绑定证书”(Bind Certificate)，并选中 CSR 请求



步骤 7 选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 证书管理 (Certificate Management) -> 证书签名请求 (Certificate Signing Requests) -> 生成证书签名请求 (CSR) (Generate Certificate Signing Requests [CSR])**，然后将证书使用选项设置为**管理员(Admin)**

步骤 8 在**节点 (Node)** 下选择节点

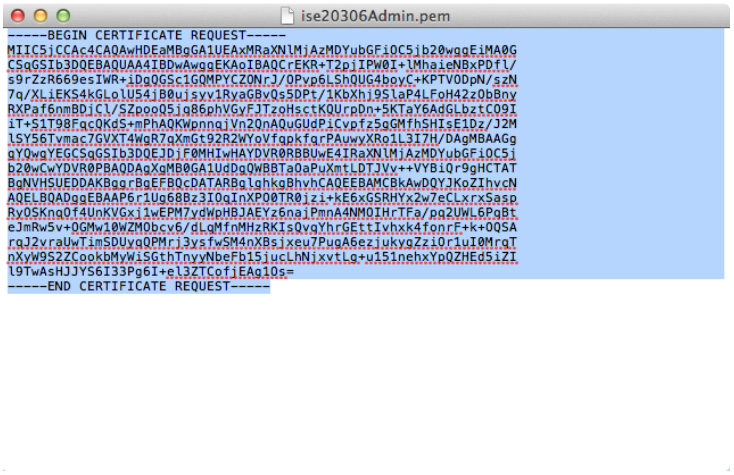
步骤 9 在**主题别名 (SAN) (Subject Alternative Name [SAN])** 部分，选择 **DNS 名称 (DNS Name)**，并输入 DNS 名称



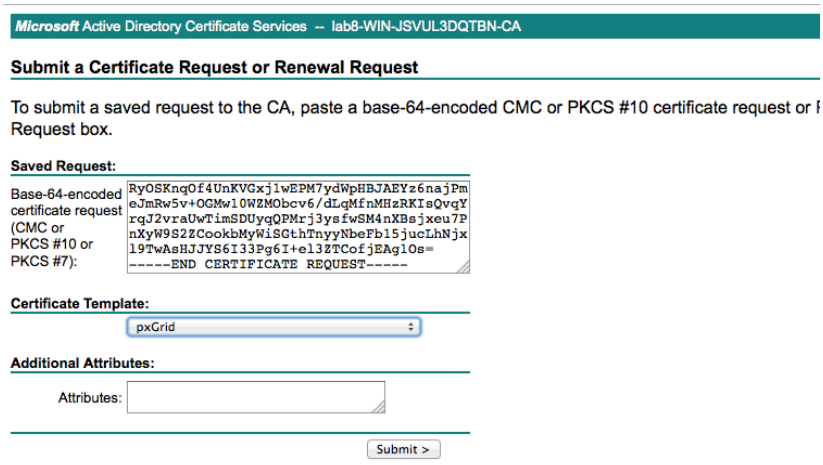
步骤 10 选择**生成 (Generate)**

步骤 11 选择**导出 (Export)**

步骤 12 打开 pem 文件，将 CSR 请求复制并粘贴到自定义 pxGrid 模板

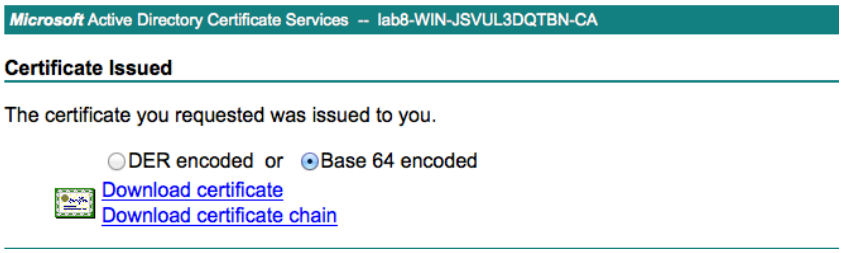


步骤 13 选择“请求证书”(Request a Certificate) ->“高级证书请求”(Advanced Certificate Request)，将 CSR 请求粘贴到“已保存的请求”(Saved Request) 部分，然后选择自定义 pxGrid 模板，并点击“提交”(Submit)

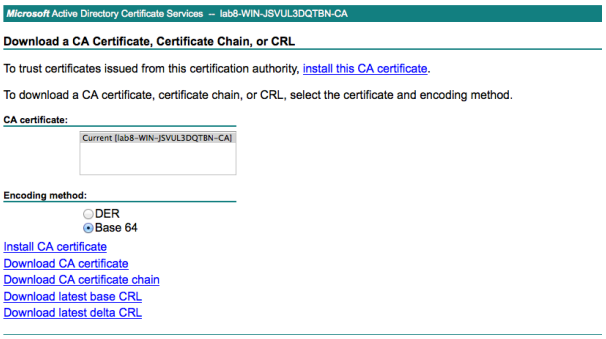


步骤 14 选择**提交 (Submit)**

步骤 15 下载 Base 64 编码格式的证书

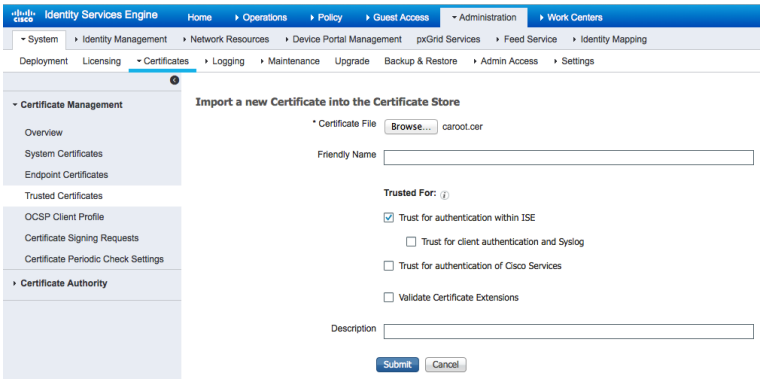


步骤 16 下载 Base 64 格式的 CA 根证书



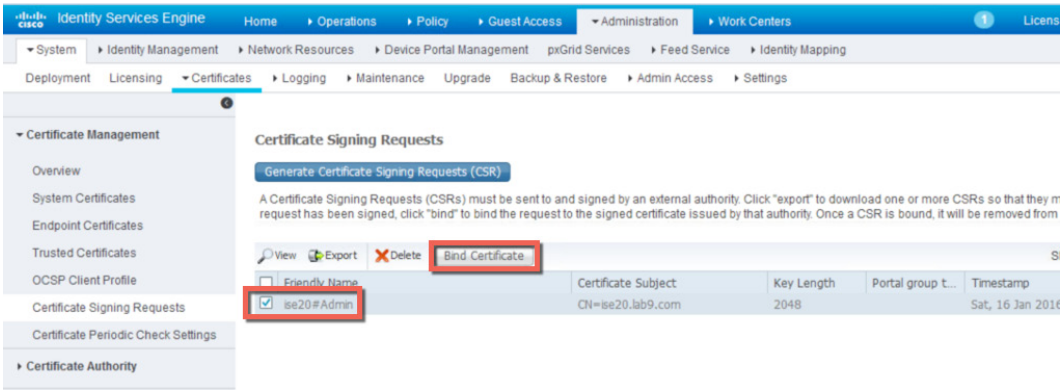
步骤 17 选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 证书管理 (Certificate Management) -> 受信任证书 (Trusted Certificates)**，然后导入根证书

步骤 18 选中**信任 ISE 中的身份验证 (Trust for authentication within ISE)**

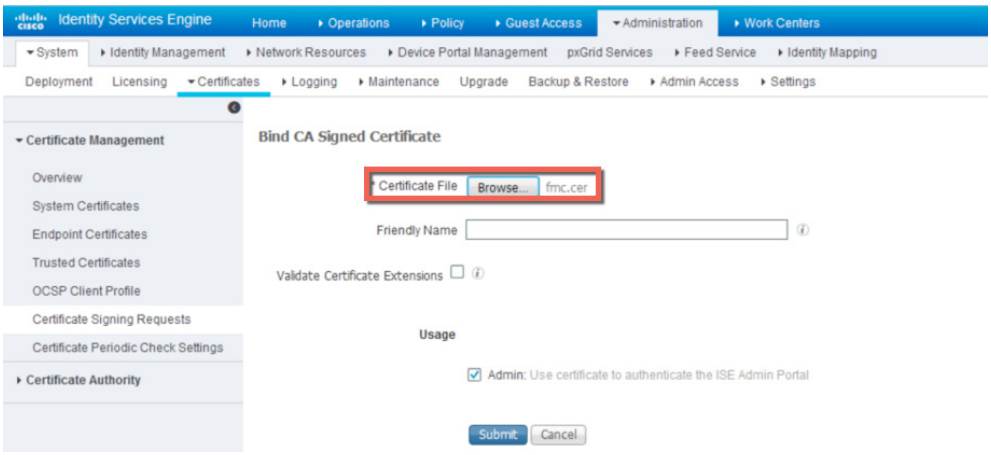


步骤 19 选择**提交 (Submit)**

步骤 20 选择**管理 (Administration) -> 系统 (System) -> 证书 (Certificates) -> 证书管理 (Certificate Management) -> 证书签名请求 (Certificate Signing Requests)**，选择 CSR 请求，然后点击**绑定证书 (Bind Certificate)**

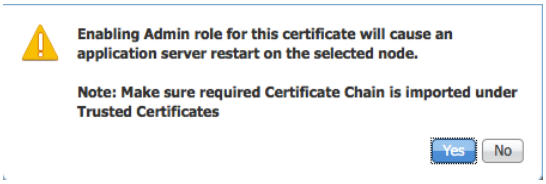


步骤 21 上传 ISE CA 签名身份证书

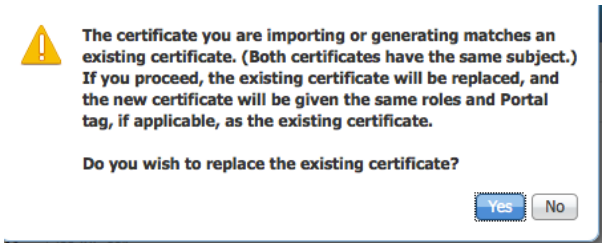


步骤 22 选择**提交 (Submit)**

步骤 23 当看到如下警告消息时，选择**是 (Yes)**：

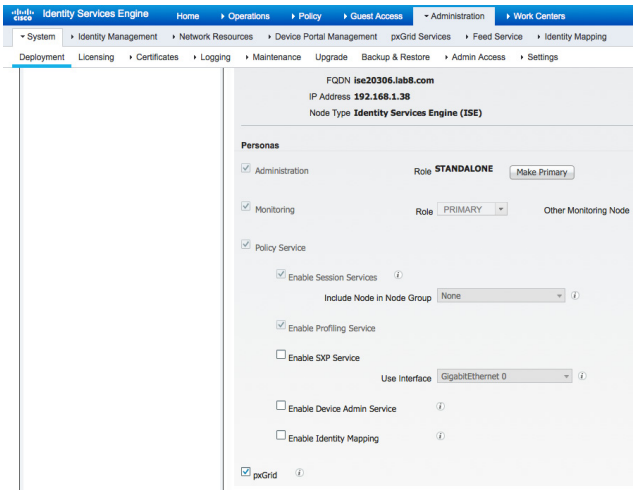


步骤 24 当看到如下警告消息时，选择**是 (Yes)**



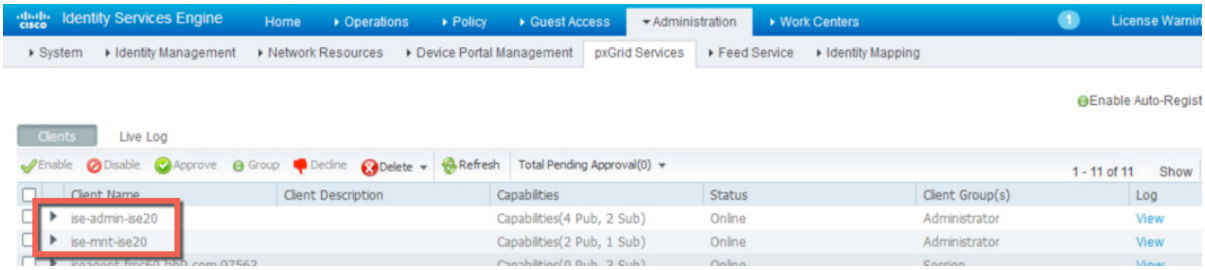
步骤 25 然后，系统将重新启动，并返回至 GUI

步骤 26 选择**管理 (Administration) -> 系统 (System) -> 部署 (Deployment)**，编辑**主机名 (Hostname)**，并选中 **pxGrid**



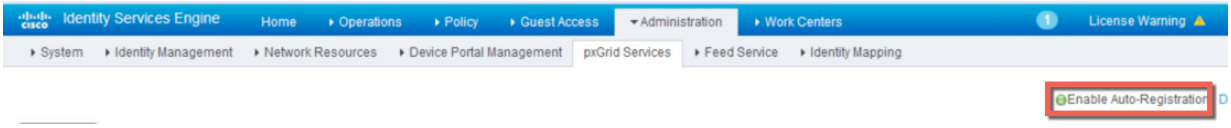
步骤 27 选择**保存 (Save)**

步骤 28 选择**管理 (Administration) -> pxGrid 服务 (pxGrid Services)**，确认已发布的服务显示在列表中

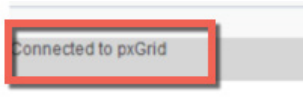


注意：已发布的节点可能需要经过几秒才会显示。您可以通过在 ISE VM 节点上运行“sh application status ise”命令来检查 pxGrid 服务是否已经启动。

步骤 29 选中**启用自动注册 (Enable Auto Registration)**



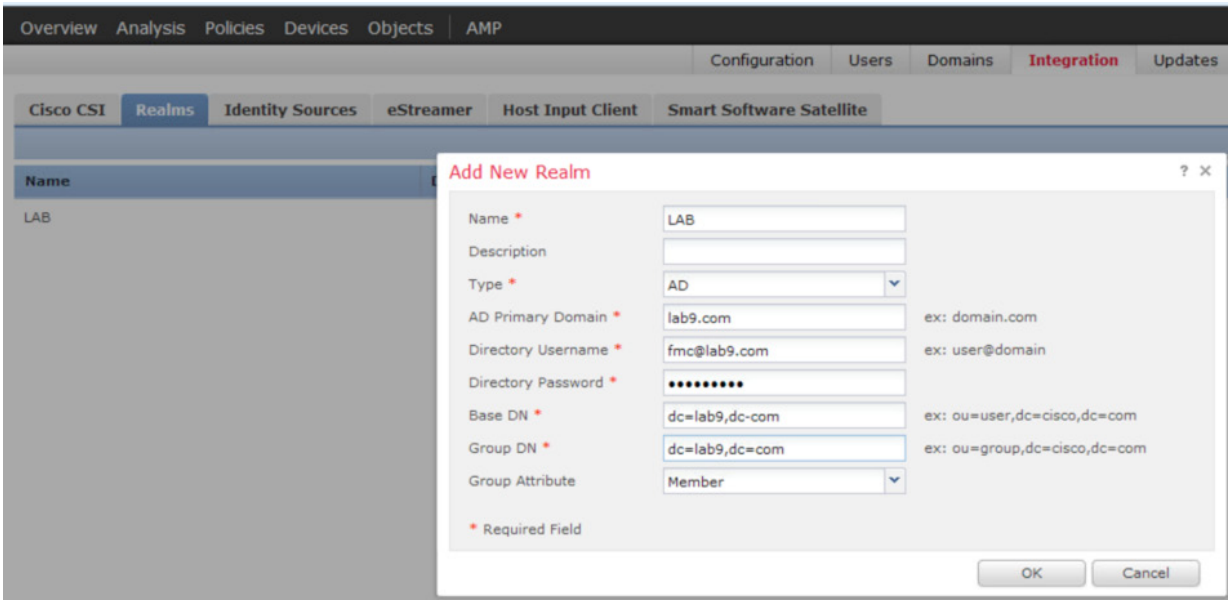
步骤 30 确认状态是否为**已连接到 pxGrid (Connected to pxGrid)**



创建 Firepower ISE 领域

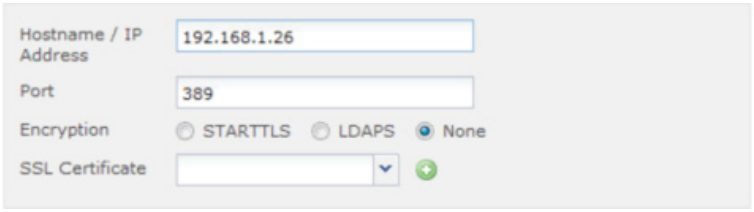
ISE 领域用于 ISE 身份验证，需要在 Firepower 管理中心 6.0 的身份策略中使用。

步骤 1 选择**系统 (System) -> 集成 (Integration) -> 领域 (Realms) -> 新建领域 (New Realm)**



步骤 2 选择**确定 (OK)**

步骤 3 选择**添加目录 (Add Directory)**，然后输入 FQDN 主机名或相关信息



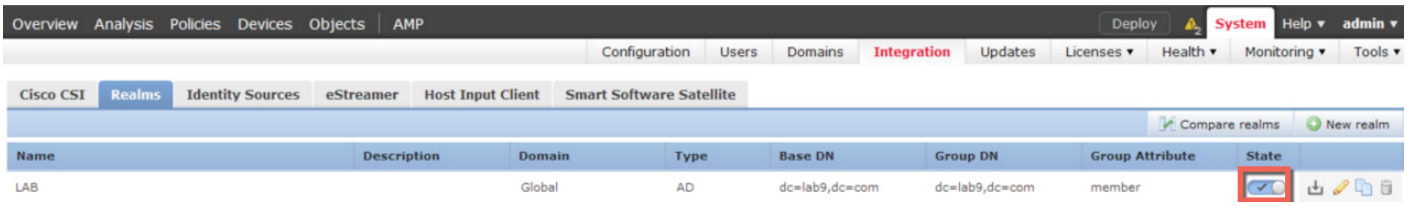
步骤 4 选择**测试 (Test)**，您应看到**已成功测试连接 (Test Connection has succeeded)** 消息，此时选择**确定 (OK)**

注意：如果系统提示尝试失败，请检查“领域配置”(Realm Configuration) 中是否设置了正确的目录用户名和目录密码。

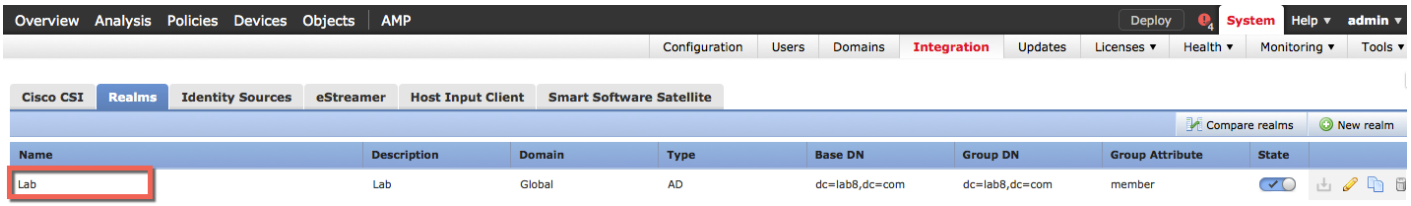
步骤 5 选择**确定 (OK)**

步骤 6 选择**保存 (Save)**

步骤 7 选择  启用状态



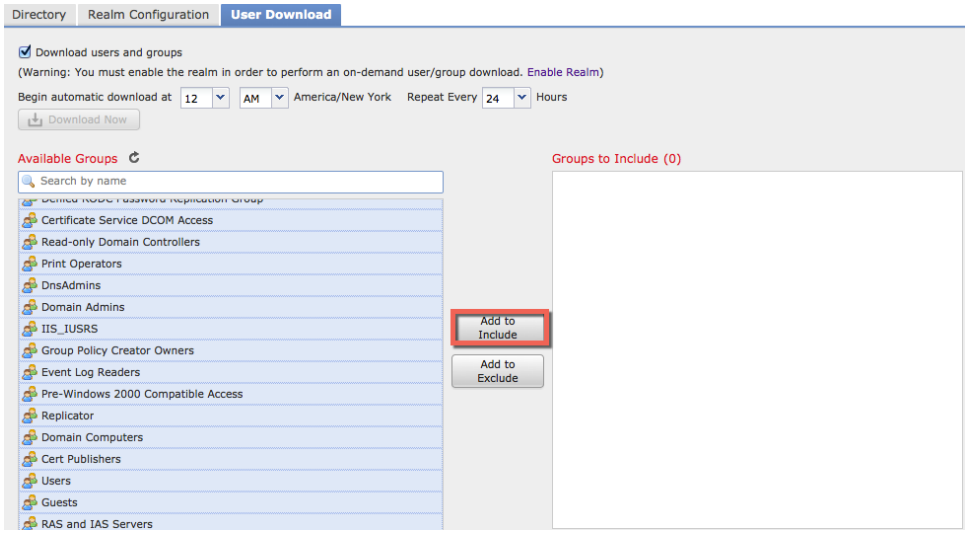
步骤 8 点击**领域 (Realm)**，然后选择一个名字



步骤 9 点击**用户下载 (User Download)**

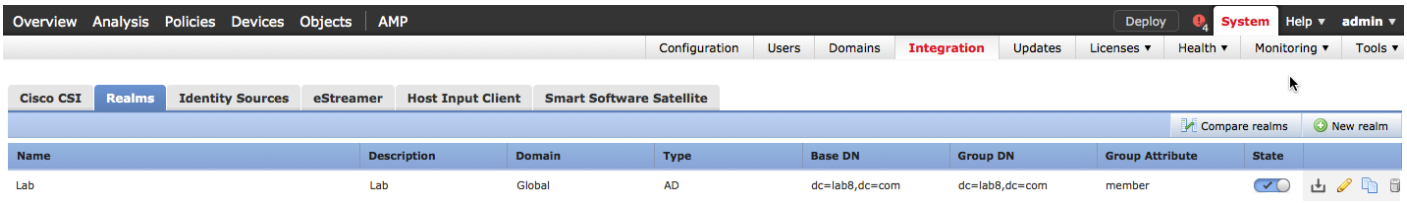
步骤 10 选中**下载用户和组 (Download users and groups)**

步骤 11 选中“可用组”(Available Groups) 下的所有项使其突出显示，然后选择**添加到包括项 (Add to Include)**



步骤 12 选择**保存 (Save)**

步骤 13 您将看到以下内容：



配置 Firepower 管理中心 6.0

在本部分，我们将针对使用证书颁发机构 (CA) 签名证书的情况配置 Firepower 管理中心 (FMC)。首先，需要从 Firepower 管理中心控制台 (FMC) 创建 Firepower 管理中心私钥和 CSR 请求。然后使用自定义 pxGrid 模板，通过 CA 服务器对 CSR 请求进行签名，并提供 FMC 身份证书。

我们还要将 FMC 证书和 FMC 密钥上传到 FMC 内部证书库中，并将 CA 根证书上传到 FMC 受信任 CA 库中。

步骤 1　生成 Firepower 私钥

注意：此处的密码将在 pxGrid 代理配置中进行定义

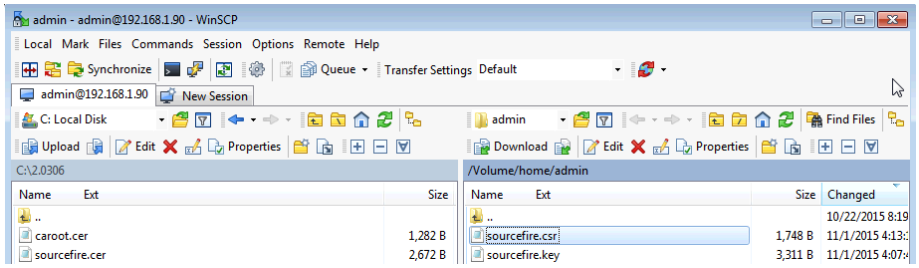
```
openssl genrsa -des3 -out sourcefire.key 4096
```

步骤 2　生成 CSR 请求

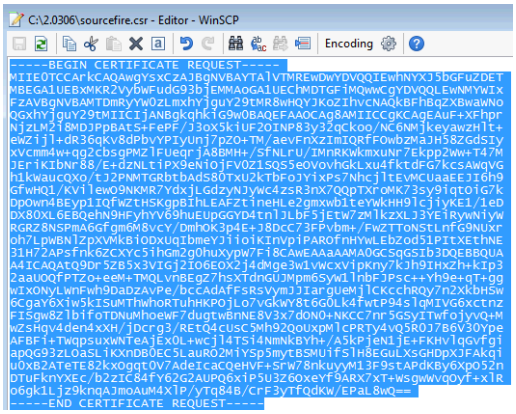
注意：系统会提示您输入密码，此密码应与您之前输入的密码相同

```
openssl req -new -key sourcefire.key -out sourcefire.csr
```

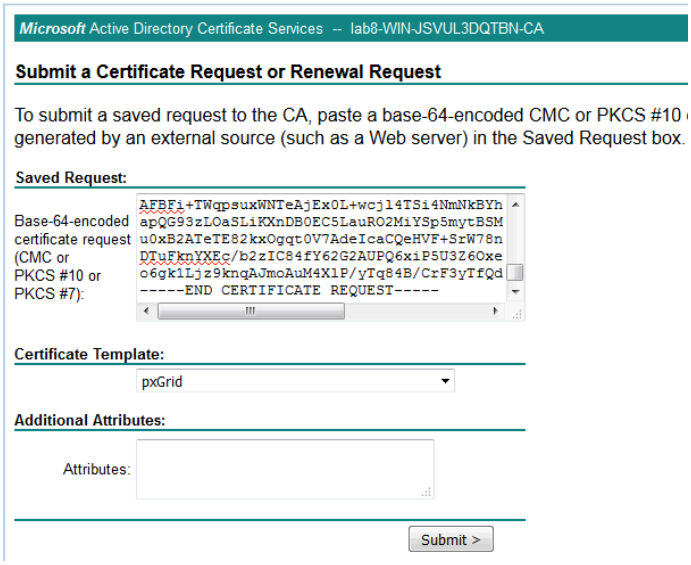
步骤 3　使用 WinSCP 将 sourcefire.csr 和 sourcefire.key 文件从 Firepower 管理中心 (FMC) 复制到本地 PC



步骤 4　使用编辑器打开 CSR 请求，并复制 CSR 请求的内容

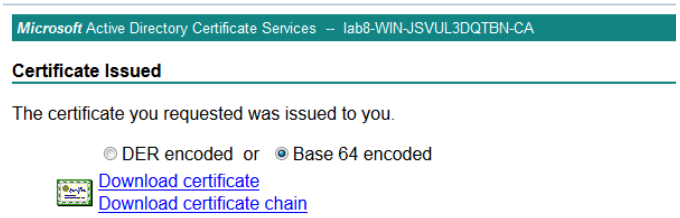


步骤 5 选择“请求证书”(Request a Certificate) ->“高级用户请求”(Advanced User Request)，将 FMC CSR 请求粘贴到“已保存的请求”(Saved Request) 部分，然后选择自定义 pxGrid 模板，并点击“提交”(Submit)。下载 Base 64 编码格式的证书

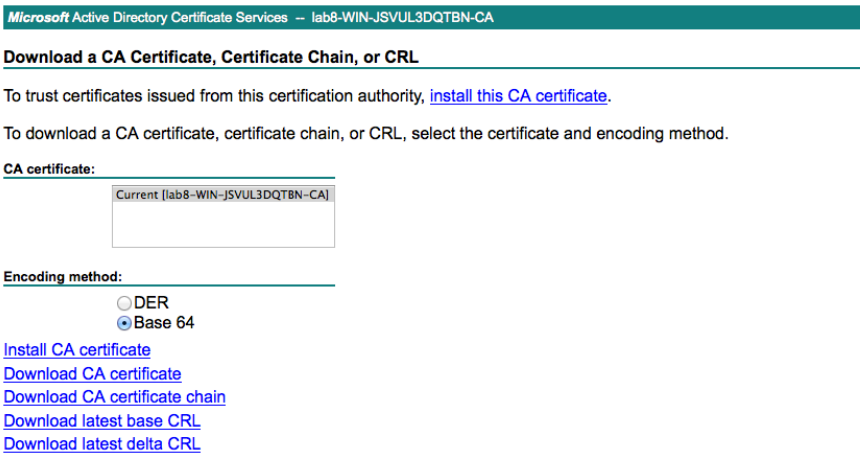


步骤 6 选择**提交 (Submit)**

步骤 7 下载 Base 64 格式的证书

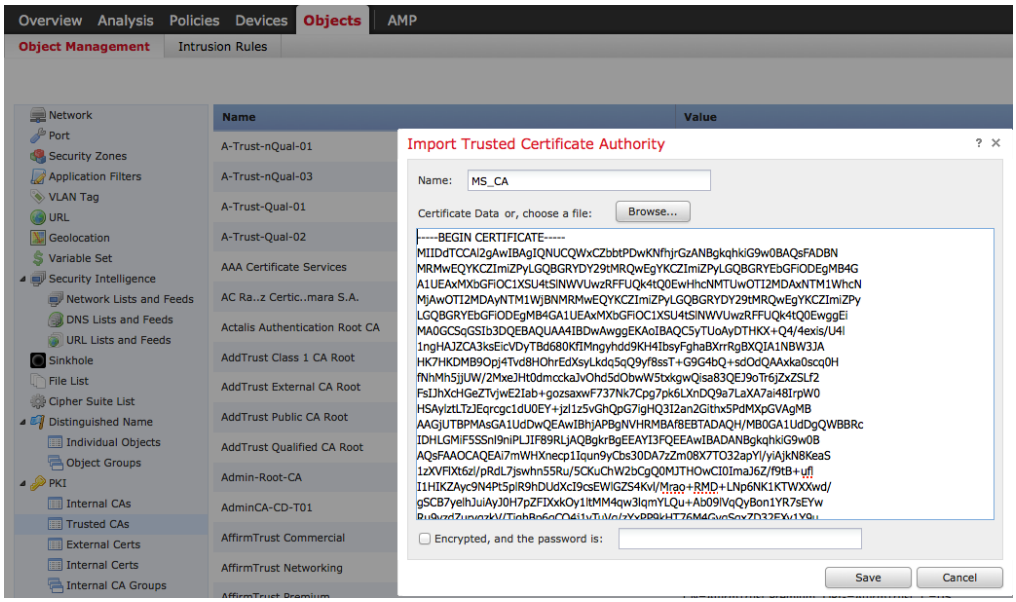


步骤 8 下载 Base 64 编码格式的 CA 根证书



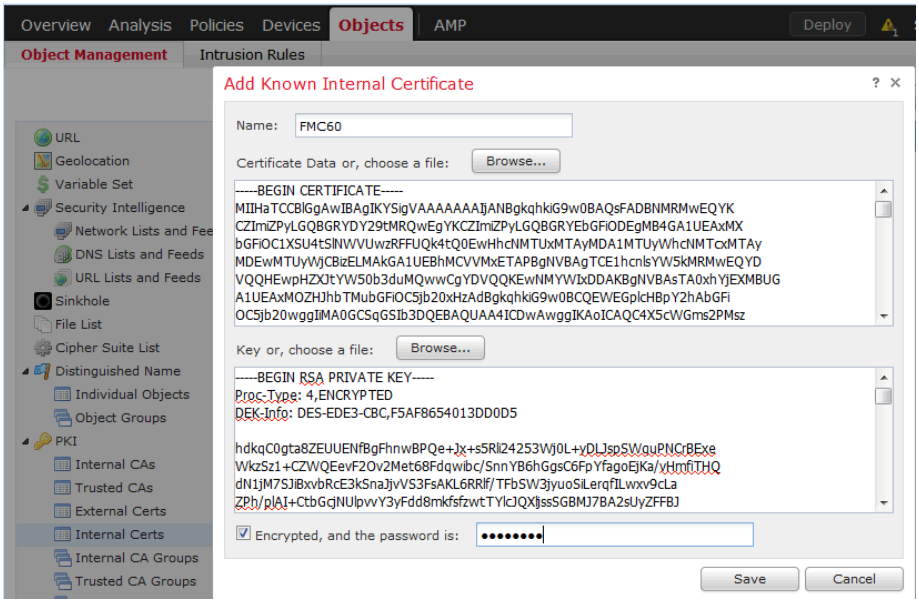
步骤 9 将 CA 根证书上传到 Firepower 管理受信任 CA 库中

选择**对象 (Objects) -> 对象管理 (Object Management)-> PKI -> 受信任 CA (Trusted CAs) -> 添加受信任 CA (Add Trusted CA)**，提供一个名称并上传根 CA 证书，然后选择**保存 (Save)**



步骤 10 将 Firepower 管理中心公共证书和私钥上传到 FMC 内部证书库中

选择**对象 (Objects) -> 对象管理 (Object Management) -> PKI -> 内部证书 (Internal Certs)**，添加 Sourcefire CER 文件和 Sourcefire KEY 文件，输入密码，然后点击**保存 (Save)**



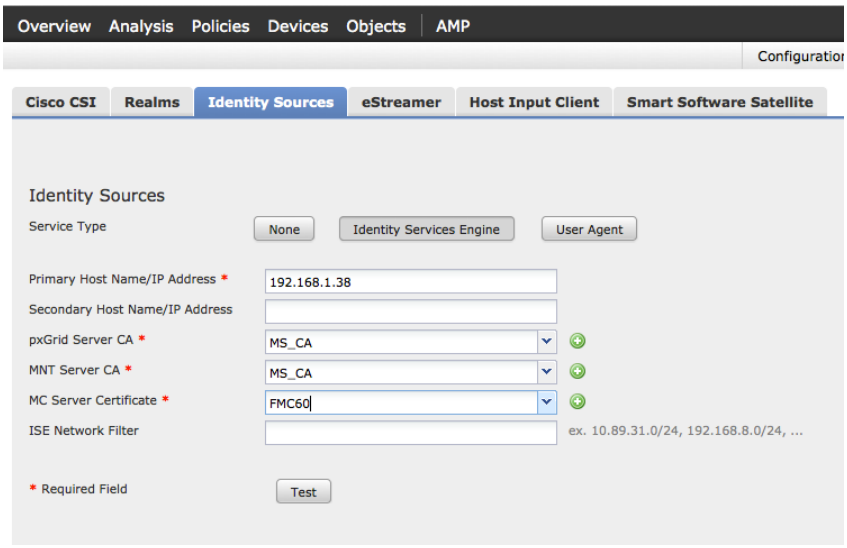
ISE 身份源 CA 签名证书配置

身份源引擎配置定义了 ISE pxGrid 节点连接参数、ISE MnT 节点证书和 FMC 身份证书。请注意，此配置将用于 ISE 独立部署下的 CA 签名环境。

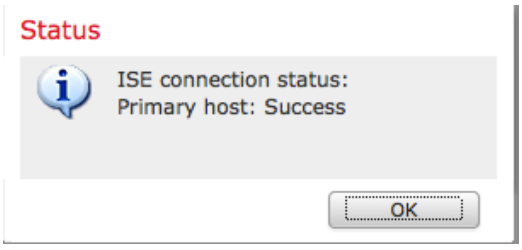
步骤 1 选择**系统 (System) -> 集成 (Integration) -> 身份源 (Identity Sources) -> 身份服务引擎 (Identity Services Engine)**

主要主机名称/IP 地址 (Primary Host Name/IP Address) - 主 FQDN pxGrid 的名称或 IP 地址
辅助主机名称/IP 地址 (Secondary Host Name/IP address) - 辅助 FQDN pxGrid 的名称或 IP 地址
**pxGrid 服务器 CA (pxGrid Server CA)* - ISE pxGrid 节点和 FMC 的根 CA 签名证书
**mnt 服务器 CA (mnt Server CA)* - ISE pxGrid 节点和 FMC 的根 CA 签名证书
MC 服务器证书 (MC Server Certificate) - FMC 的 CA 签名身份证书

**CA 签名环境 (CA Signed Environment)*

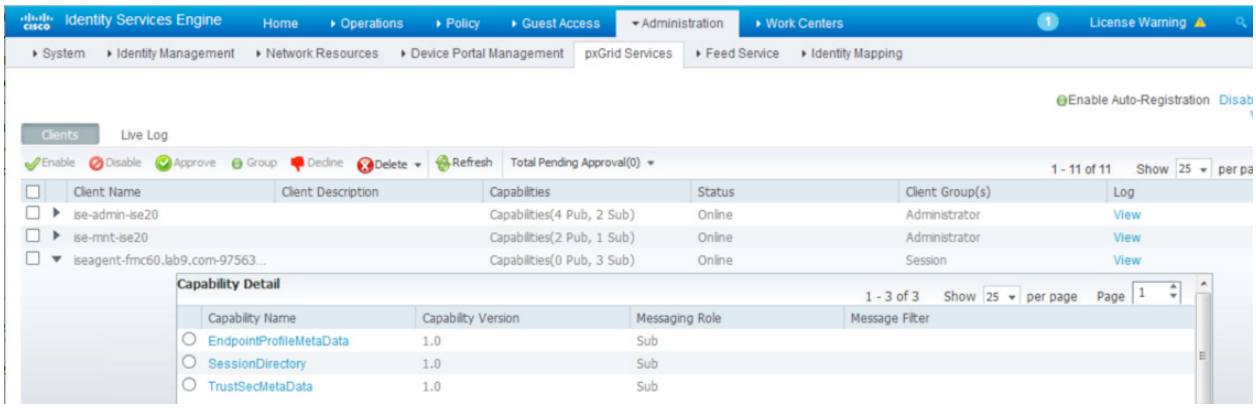


步骤 2 选择**测试 (Test)**
您应该看到以下内容：



步骤 3 选择**保存 (Save)**

步骤 4 您应在 ISE pxGrid 节点中看到下列项
选择**管理 (Administration) -> pxGrid 服务 (pxGrid Services)**



完成上述步骤后，FMC 即成功注册到 ISE pxGrid 节点，并且可以对 EndPointProfileMetada、SessionDirectory 和 TrustsecMetaData 功能进行描述。

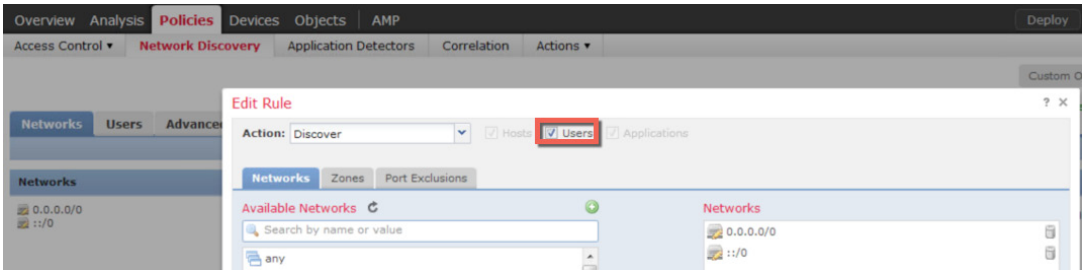
Firepower 管理中心

启用网络发现

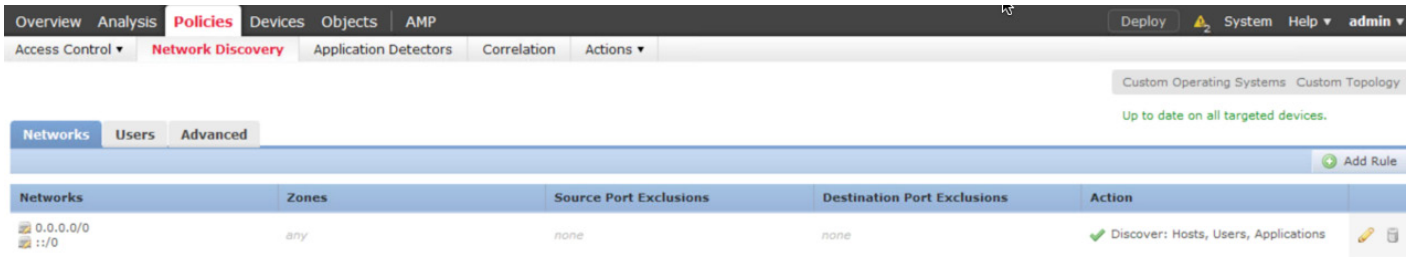
启用网络发现以获取用户身份信息

步骤 1 选择“策略”(Policies) ->“网络发现”(Network Discovery)，然后点击  打开“编辑规则”(Edit Rule) 窗口

步骤 2 选中“用户”(Users)



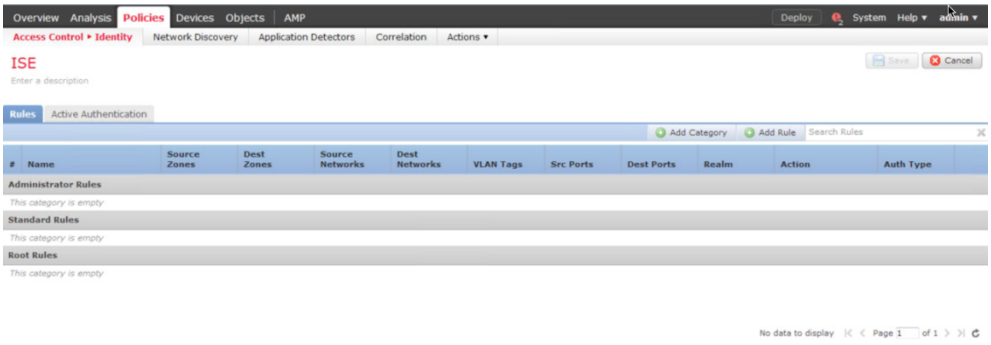
步骤 3 选择**保存 (Save)**
您应该看到以下内容



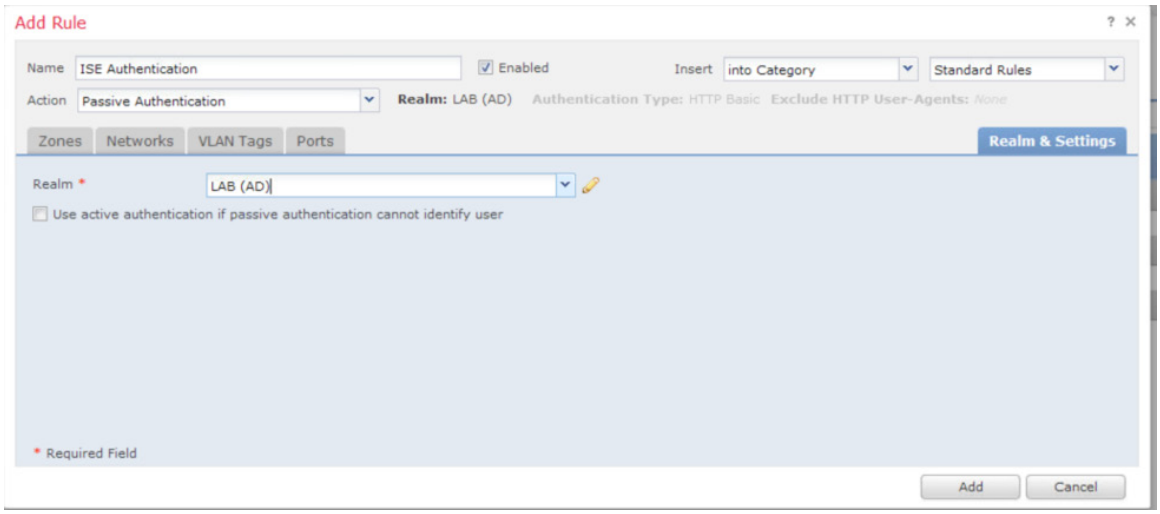
ISE 身份策略

要允许被动 ISE 身份验证，需在 Firepower 管理中心的默认访问控制策略中使用 ISE 身份策略。

步骤 1 选择**策略 (Policies) -> 访问控制 (Access Control) -> 身份 (Identity) -> 新建策略 (New Policy) -> 新建身份策略 (New Identity Policy)**，输入名称，然后点击**保存 (Save)**
您将看到以下内容：



步骤 2 选择**添加规则 (Add Rule)**
步骤 3 在“名称”(Name) 框中输入：**ISE Authentication**
步骤 4 在“操作”(Action) 框中输入：**Passive Authentication**
步骤 5 选择**领域 (Realm)**，点击**添加 (Add)**，然后选择您之前定义的 ISE 领域
您的屏幕显示应与下图相似



步骤 6 点击**保存 (Save)** 保存更改

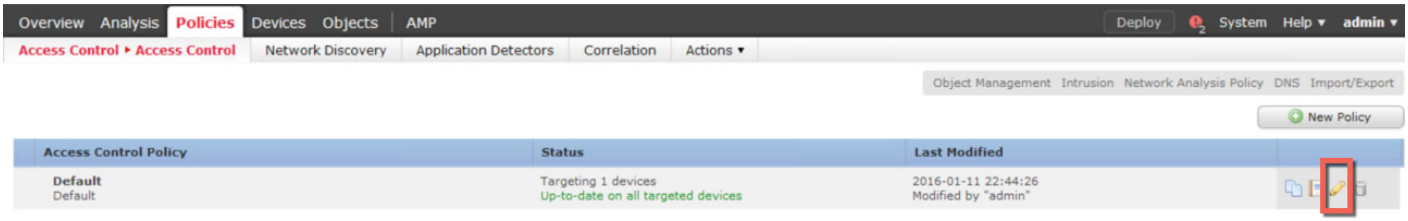
默认访问控制策略

默认访问控制策略包含 ISE 身份策略、用于阻止事务的传输/网络层预处理器设置、访问控制规则，以及 Firepower 管理中心的入侵策略。

添加 ISE 身份策略

在默认访问策略中添加 ISE 身份策略

步骤 1 选择**策略 (Policies) -> 访问控制 (Access Control)**，然后编辑默认访问策略



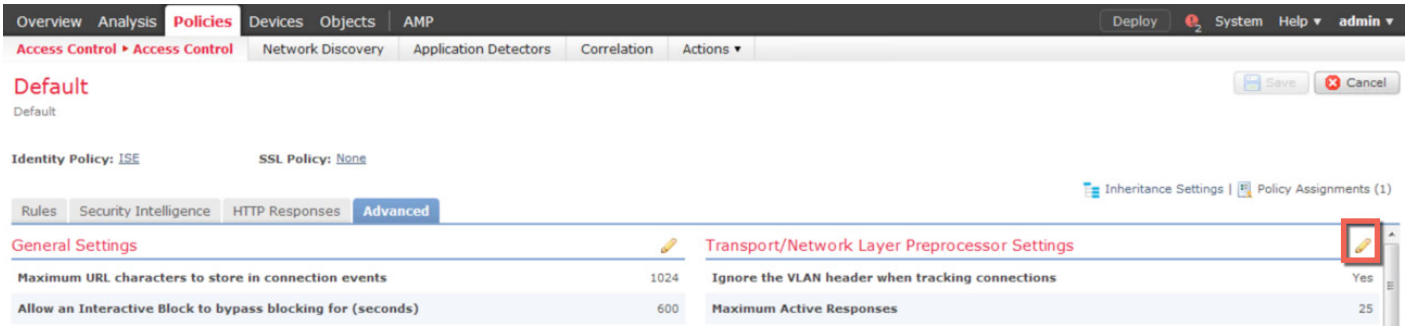
步骤 2 点击**无 (None) -> 身份策略 (Identity Policy)**，从下拉菜单中选择“ISE”

步骤 3 选择**保存 (Save)**

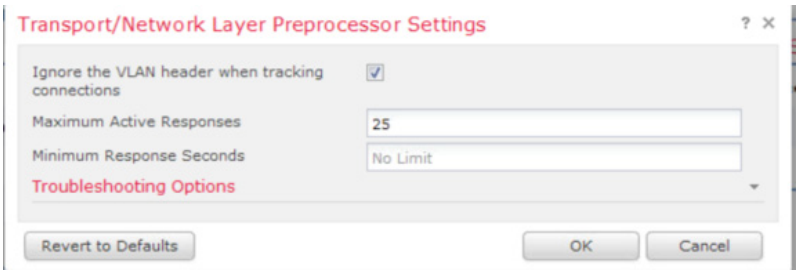
传输/网络层预处理器设置

要阻止经过 Firepower 管理的入侵策略处理的流量，需修改这些设置。

步骤 1 编辑“传输/网络层预处理器设置”(Transport/Network Layer Preprocessor Settings)



步骤 2 按照如下屏幕进行设置

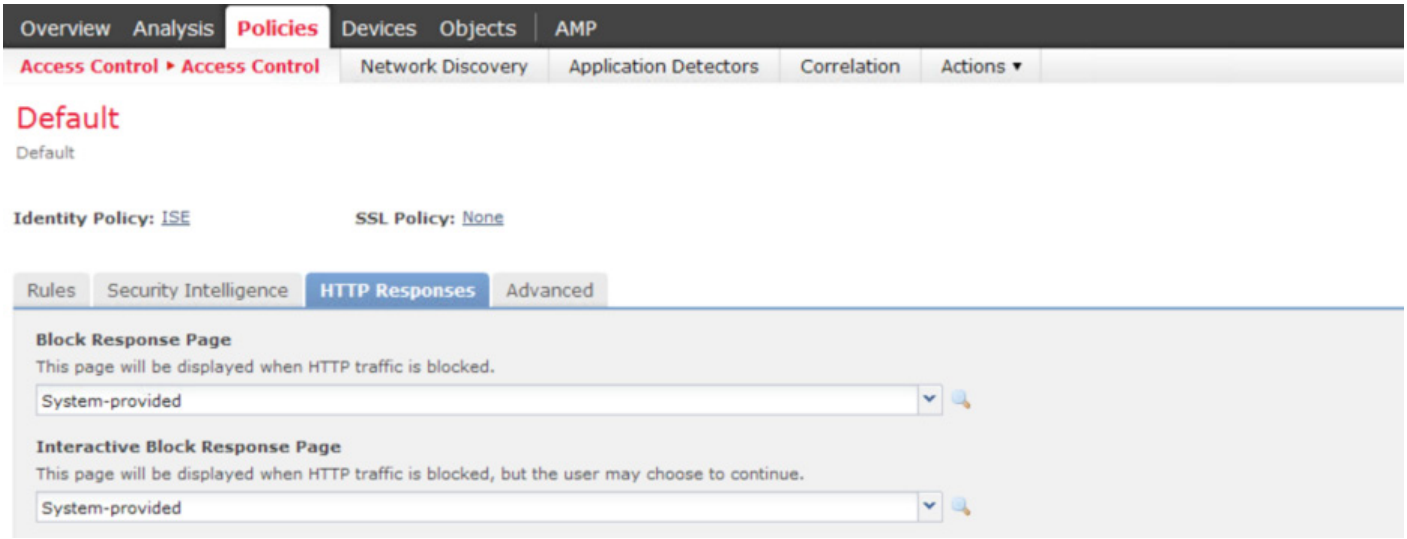


步骤 3 选择“确定”(OK)

添加阻止响应页面

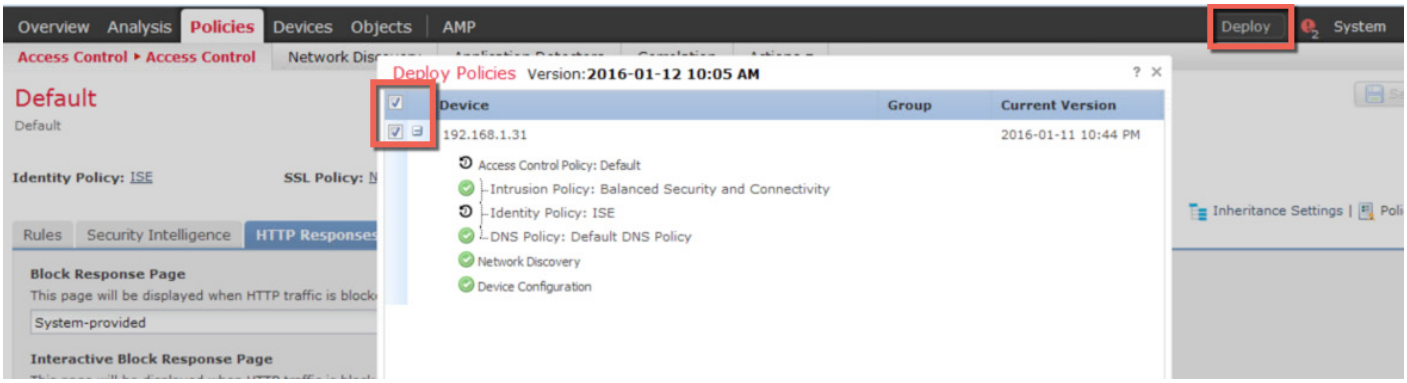
根据 Firepower 管理中心的访问控制策略，被阻止的网络类别将显示系统提供的阻止响应页面。

步骤 1 选择 **HTTP 响应 (HTTP Responses)**，然后对响应页面进行如下设置

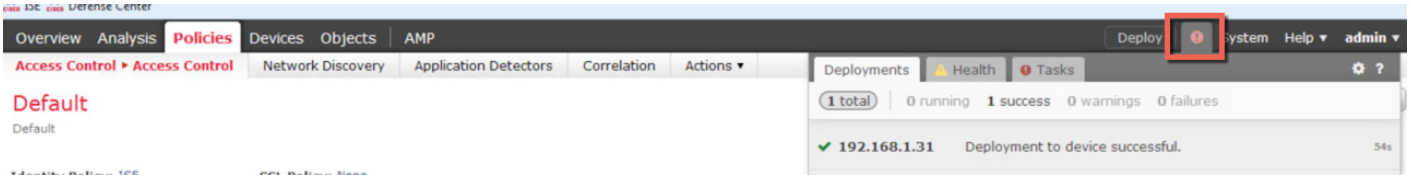


步骤 2 点击**保存 (Save)** 保存更改

步骤 3 选择**部署 (Deploy)**，将更改**部署**到传感器



步骤 4 在状态栏中选择“部署”(Deploy) 可以查看进度

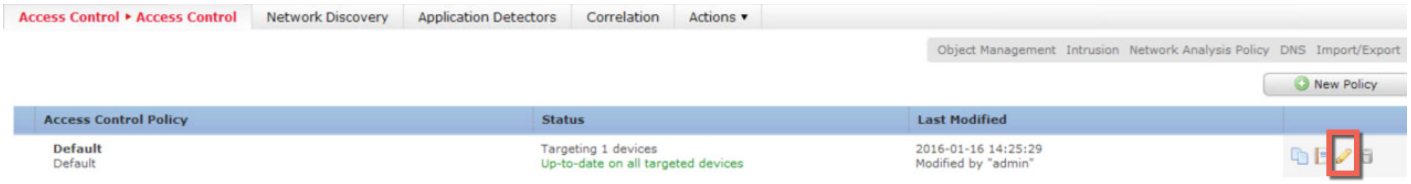


创建“员工”SGT 标签访问控制规则

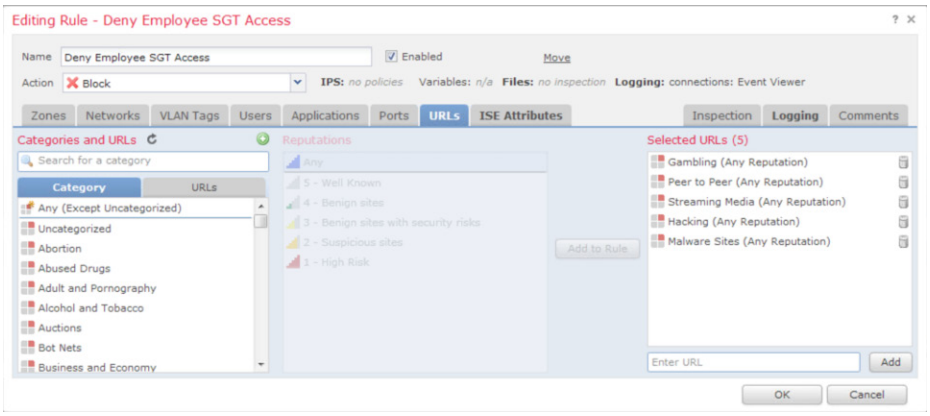
我们将模仿组织的可接受使用策略，创建一个“员工”(Employee) SGT 访问控制策略。

此可接受使用策略将拒绝用户访问“赌博类”网站、“黑客类”网站、流媒体、社交媒体和点对点应用。

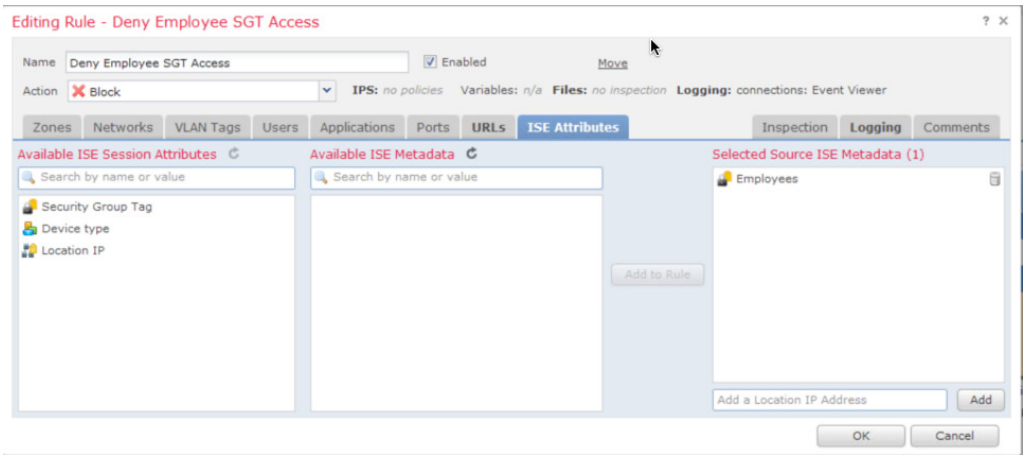
步骤 1 选择**策略 (Policies) -> 访问控制 (Access Control) -> 访问控制 (Access Control) -> 规则 (Rules)**，然后点击  进行编辑



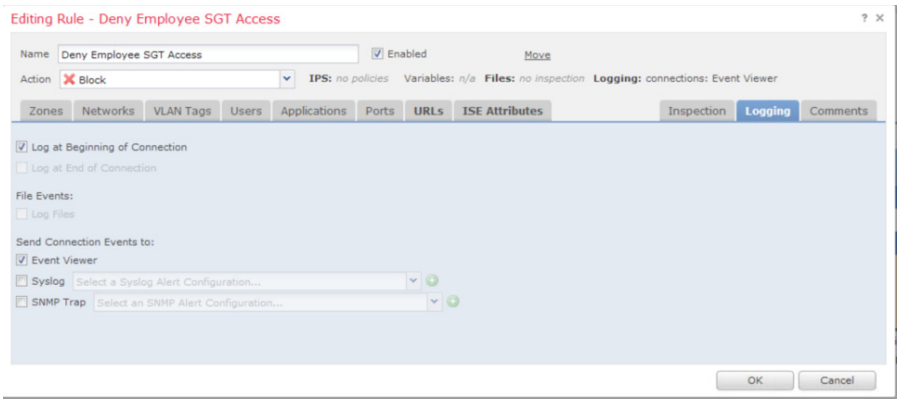
步骤 2 选择**添加规则 (Add Rule)**，在**名称 (Name)** 框中输入：**Deny Employee SGT Access**，在**操作 (Action)** 框中输入：**Block**，将 **IPS** 设置为 **pxGrid 入侵策略 (pxGrid Intrusion Policy)**。然后选择 **URLs -> 类别 (Category)**，选中**赌博 (Gambling)**、**点对点 (Peer-to-Peer)**、**流媒体 (Streaming Media)** 和**黑客 (Hacking)**，点击**添加到规则 (Add to Rule)**



步骤 3 选择 **ISE 属性 (ISE Attributes) -> 可用 ISE 会话属性 (Available ISE session attributes) -> 安全组标记 (Security Group Tag) -> 可用 ISE 元数据 (Available ISE Metadata)**，选择**员工 (Employees)**，然后点击**添加到规则 (Add to Rule)**

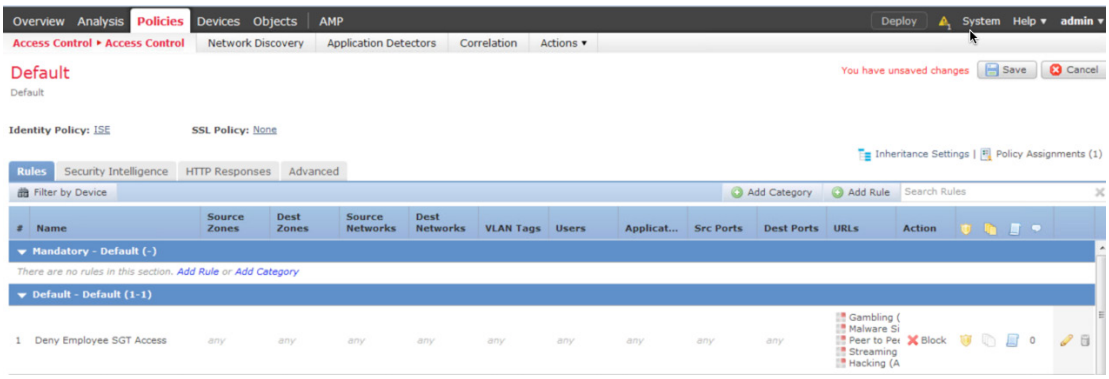


步骤 4 选择**日志记录 (Logging)**，并按照下图进行配置



步骤 5 选择**确定 (OK)**

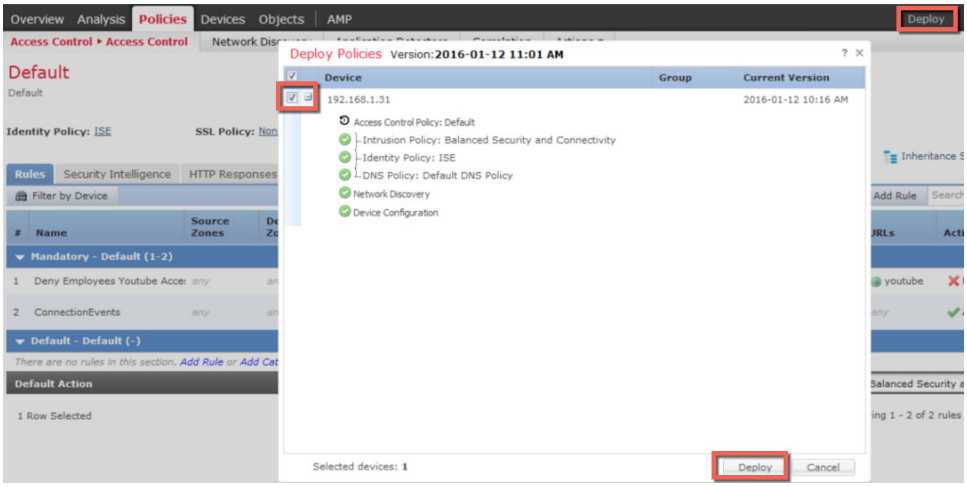
您应该看到以下内容



步骤 6 选择**保存 (Save)**

步骤 7 将更改部署到传感器

点击**部署 (Deploy)**，选择传感器，再次点击**部署 (Deploy)**



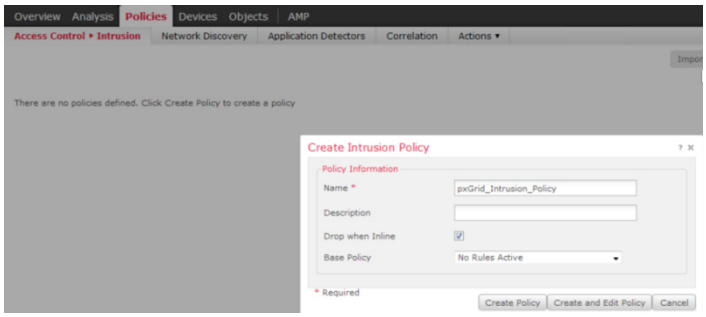
步骤 8 点击 查看任务状态，确认操作已经成功。

Firepower pxGrid 入侵策略

在本节中，我们将创建 pxGrid 入侵策略，并将其部署到 Firepower NGIPS 虚拟传感器。此策略包含“SERVER IIS CMD.EXE 访问”(SERVER IIS CMD.EXE access) 规则，如果终端用户在浏览器中输入 www.yahoo.com/cmd.exe，便会触发入侵事件，系统将执行内联丢弃，且 Firepower 管理控制台的“分析入侵事件”(Analysis Intrusion Events) 日志中将生成事件。在本文档中，pxGrid 策略也将用于集中管理具备 Firepower 服务的 ASA。

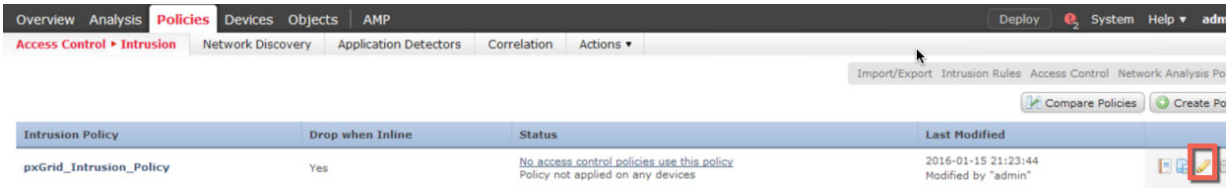
此外，我们还将通过 ASDM 在具备 Firepower 服务的 ASA 本地创建这条策略。

步骤 1 选择**策略 (Policies) -> 访问控制 (Access Control) -> 入侵 (Intrusion) -> 入侵策略 (Intrusion Policy) -> 创建策略 (Create Policy)**，然后输入名称 **pxGrid_Intrusion_Policy**，并选中**内联时丢弃 (Drop when Inline)**

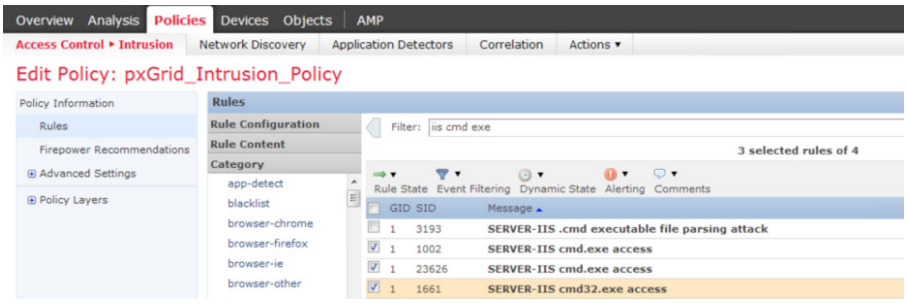


步骤 2 点击**创建策略 (Create Policy)**

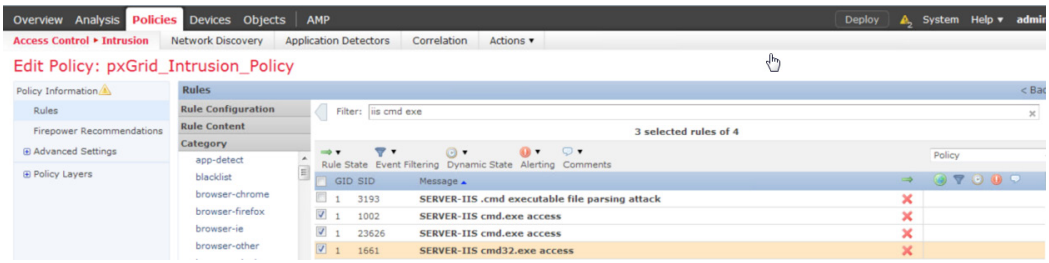
步骤 3 点击  编辑新建的策略



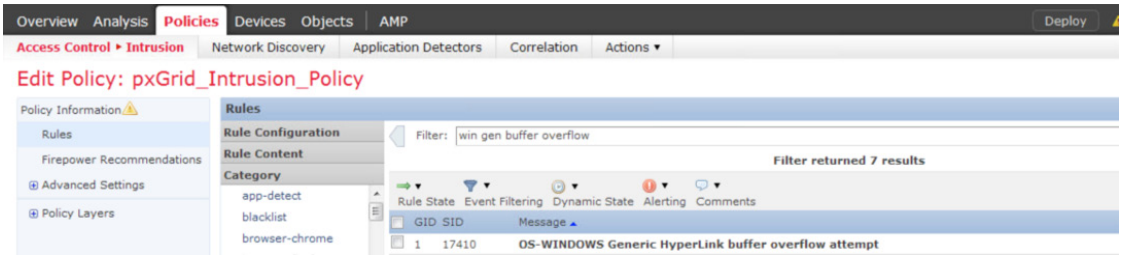
步骤 4 点击**规则 (Rules)**，在**过滤器 (Filter)** 字段中输入：**iis cmd exe**，然后按下图所示进行选择



步骤 5 点击**规则状态 (Rule State)**，选择**丢弃并生成事件 (Drop and Generate Events)**，点击**确定 (OK)**
您将看到以下内容：

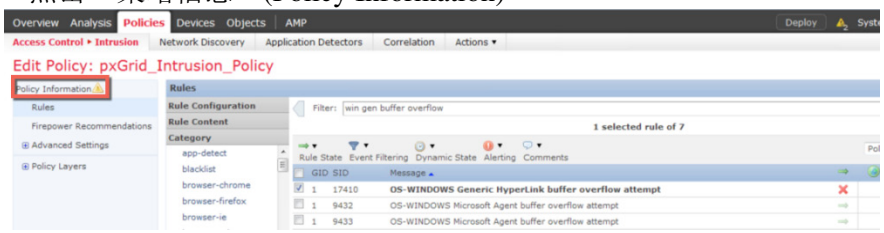


步骤 6 然后，在**过滤器 (Filter)** 字段中输入：**win gen buffer overflow**，并选择**操作系统-Windows 通用超链接缓冲区溢出尝试 (OS-Windows Generic Hyperlink Buffer Overflow Attempt)**

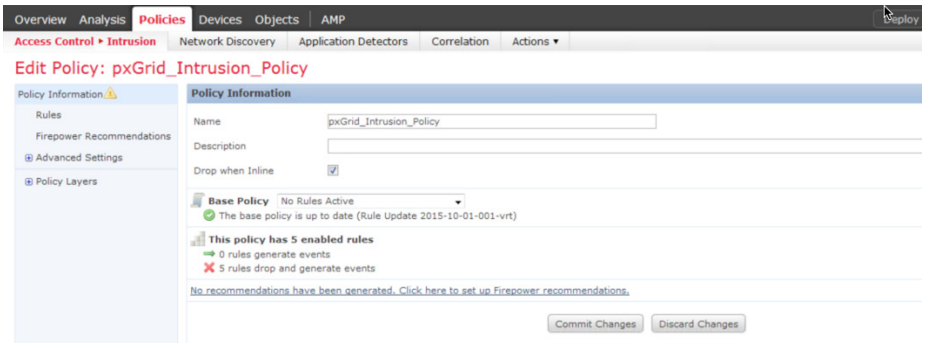


步骤 7 点击**规则状态 (Rule State)**，选择**丢弃并生成事件 (Drop and Generate Events)**，点击**确定 (OK)**

步骤 8 点击“策略信息”(Policy Information)

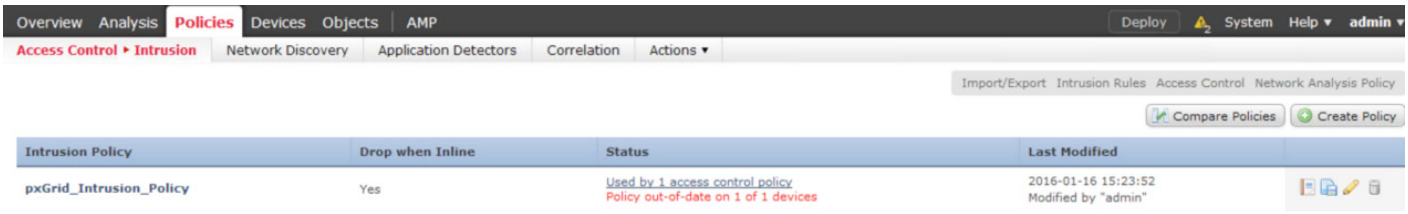


步骤 9 您将看到以下内容：



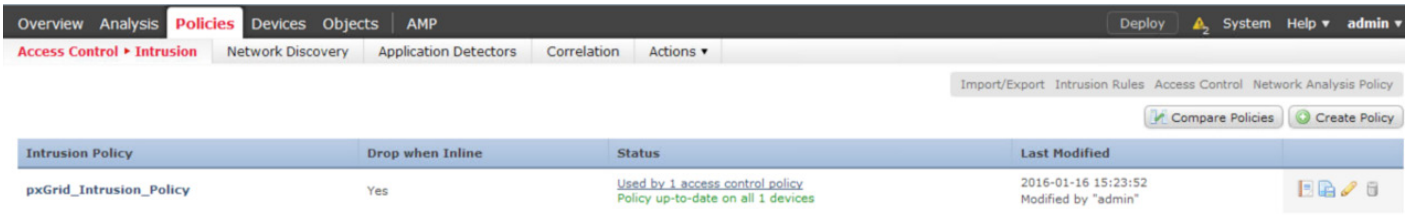
步骤 10 选择**提交更改 (Commit Changes)**

步骤 11 点击“确定”(OK)
您应该看到以下内容

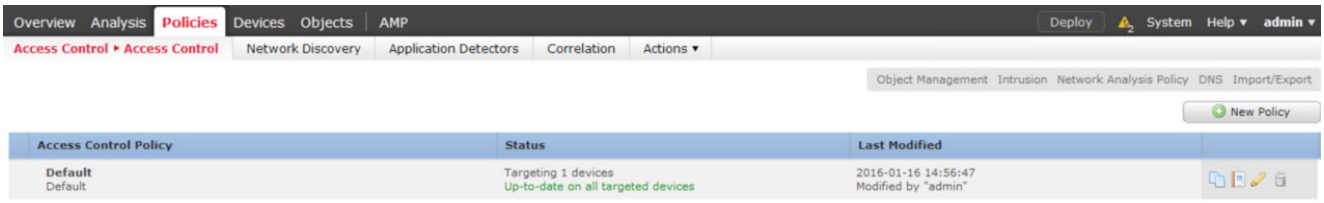


步骤 12 点击“部署”(Deploy)，选择传感器，再次点击“部署”(Deploy)

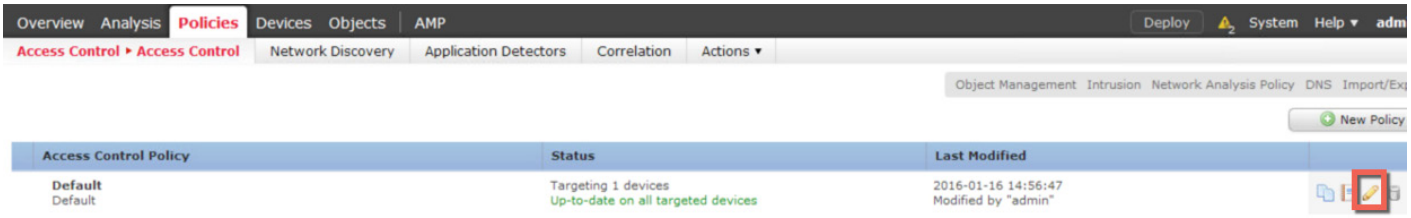
步骤 13 选择**策略 (Policies) -> 访问控制 (Access Control) -> 入侵访问控制 (Intrusion Access Control)**，您应该看到以下内容：



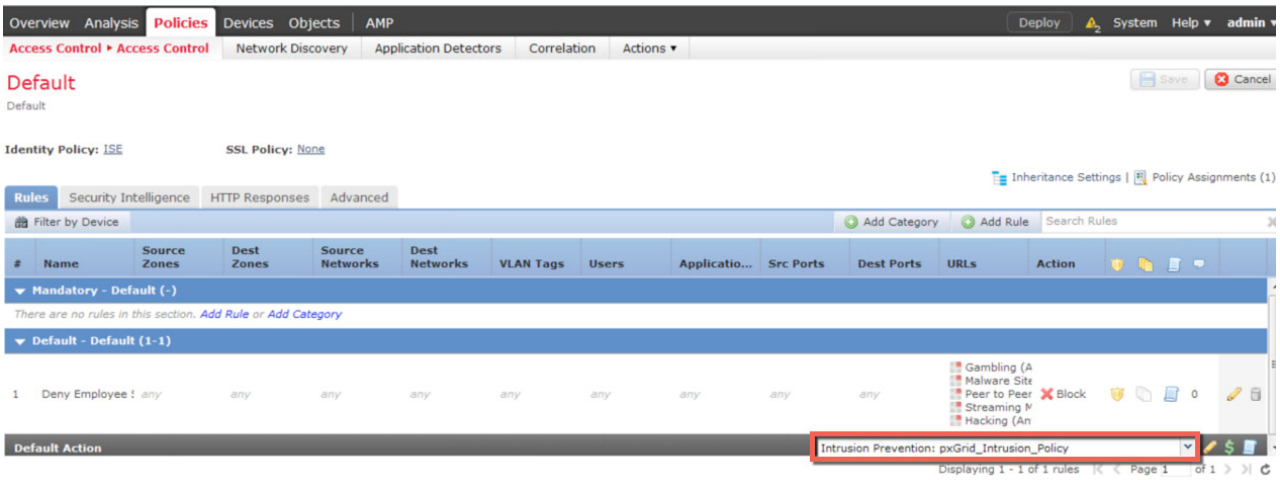
步骤 14 选择**策略(Policies) -> 访问控制 (Access Control) -> 访问控制 (Access Control)**
您应看到默认访问策略



步骤 15 点击  编辑默认访问策略



步骤 16 在“默认操作”(Default actions) 部分，从下拉列表中选择“pxGrid_Intrusion_Policy”
您应该看到以下内容



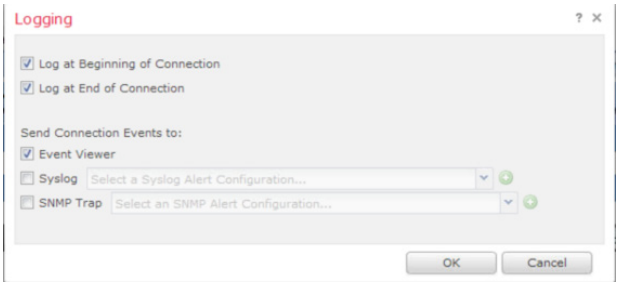
注意：系统可能会提示您添加访问控制策略。我们稍后将根据“员工”(Employee) SGT 来添加策略

步骤 17 点击**保存 (Save)**

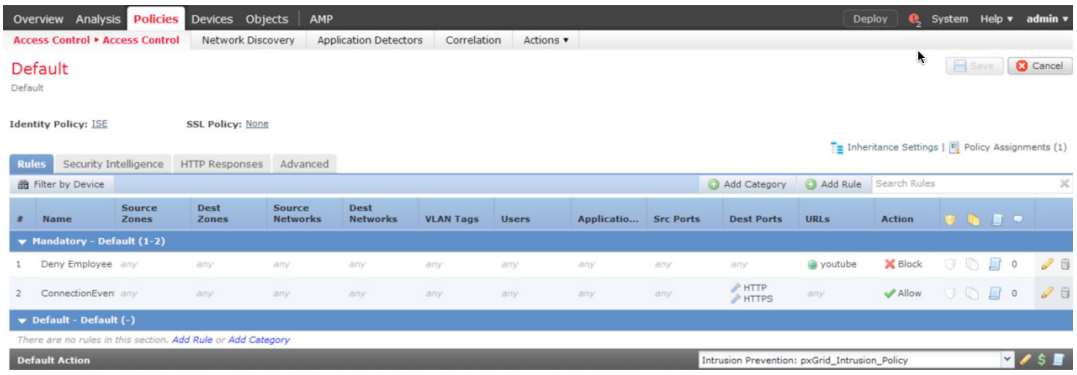
步骤 18 编辑 SGT 访问控制策略，在其中添加 pxGrid 入侵策略

步骤 19 点击  打开**日志记录 (Logging)**

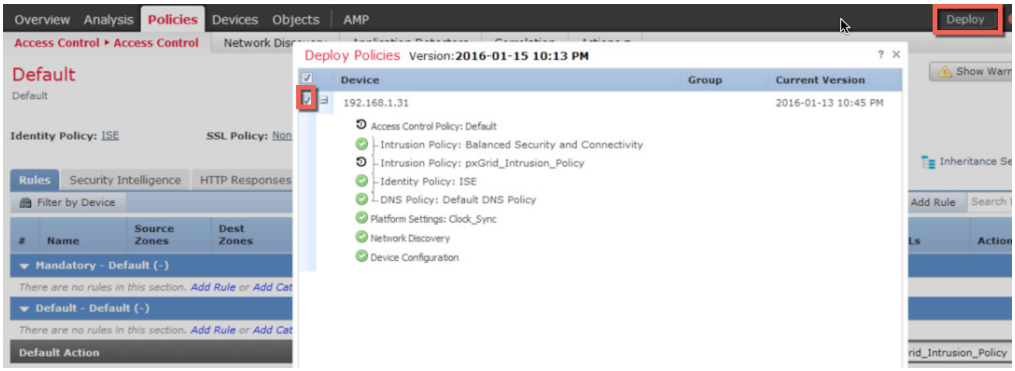
步骤 20 按照如下屏幕进行设置，然后点击**确定 (OK)**



步骤 21 点击**保存 (Save)**

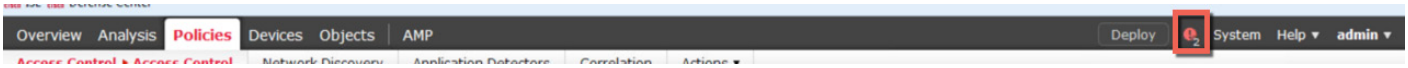


步骤 22 点击**部署 (Deploy)**，选择设备



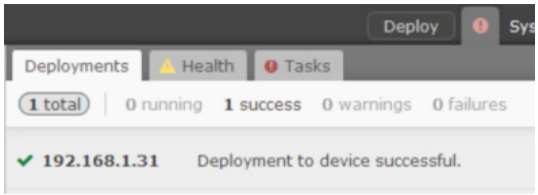
步骤 23 选择**部署 (Deploy)**

步骤 24 点击  查看任务状态



注意：点击“任务状态”(Task Status) 可查看部署周期状态

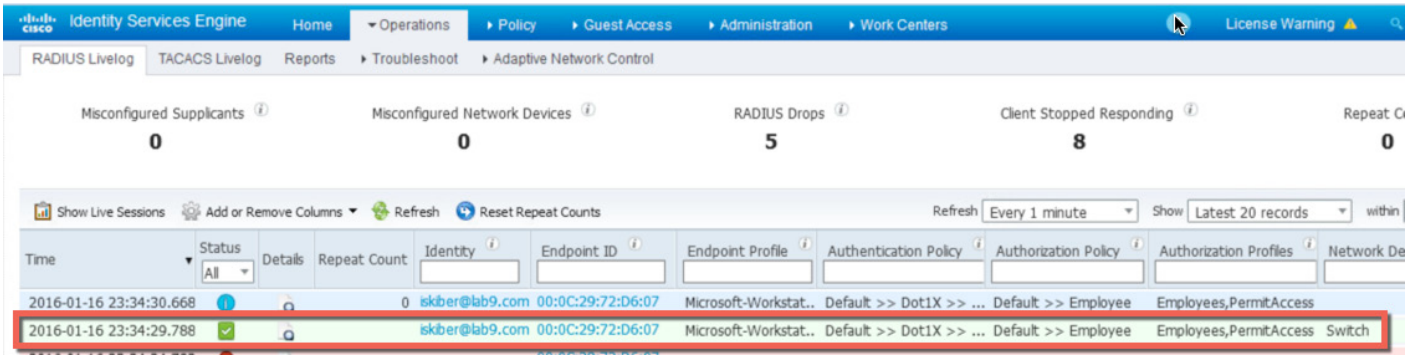
您应看到一条成功消息，表明策略已部署到传感器



通过 Firepower 虚拟传感器使用“员工”SGT 对用户进行测试

在此使用案例中，我们为终端用户分配“员工”(Employee) SGT，并将其设置为接收 Firepower 管理中心的访问控制策略，拒绝带有此 SGT 标记的员工访问“黑客类”网站、“赌博类”网站、点对点应用和流媒体应用。此外，我们还实施入侵策略，以拒绝对受感染的 Web 服务器的访问。

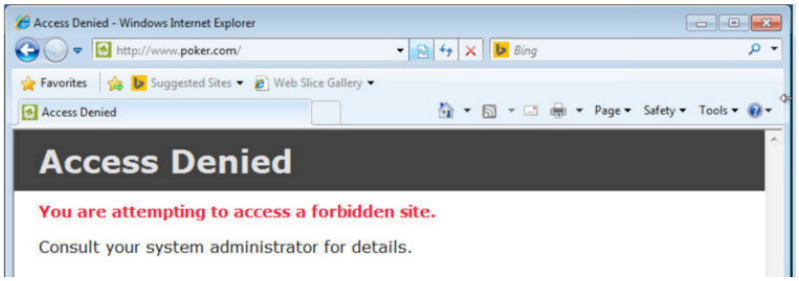
成功通过 IEEE 802.1X 进行身份验证的终端用户会被标记一个“员工”(Employee) SGT（如下所示）。



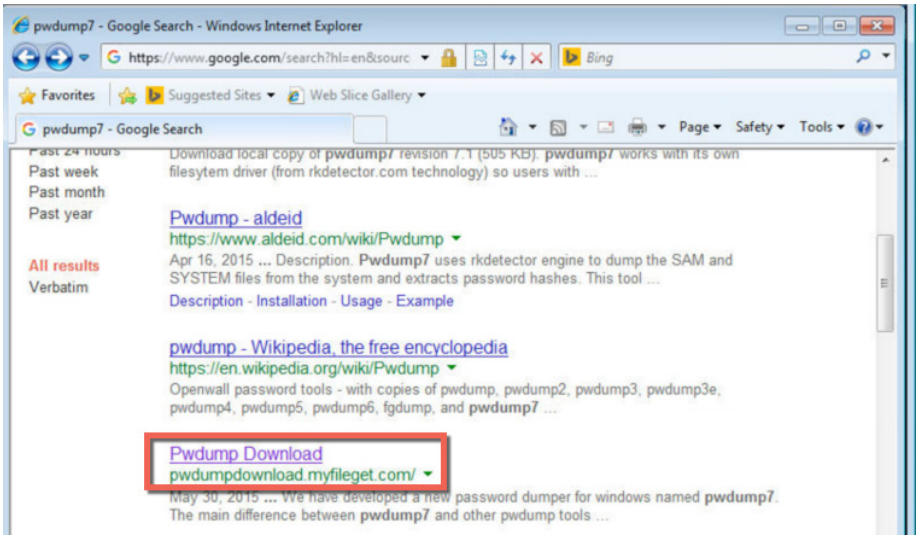
Firepower 管理中心 6.0 会获取 ISE 会话信息，并在“用户活动”(User Activity) 页面上显示这些信息。

请注意以下 ISE 会话属性：“用户名”(Username)、“安全组标记”(Security Group Tag)、“终端配置文件”(Endpoint Profile) 和“终端位置”(Endpoint Location)。我们已使用“安全组标记”(Security Group Tag) 属性创建了一条 FMC 访问控制策略。

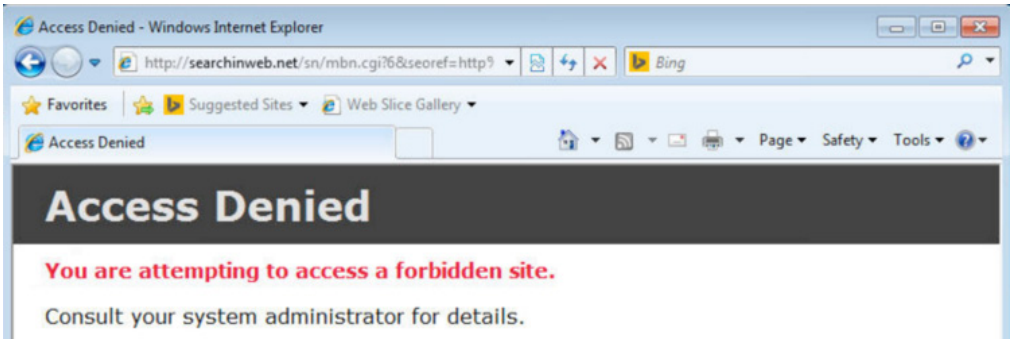
如果终端用户打开浏览器并访问 poker.com，系统将阻止该事务，并显示 Firepower 管理中心阻止响应页面。



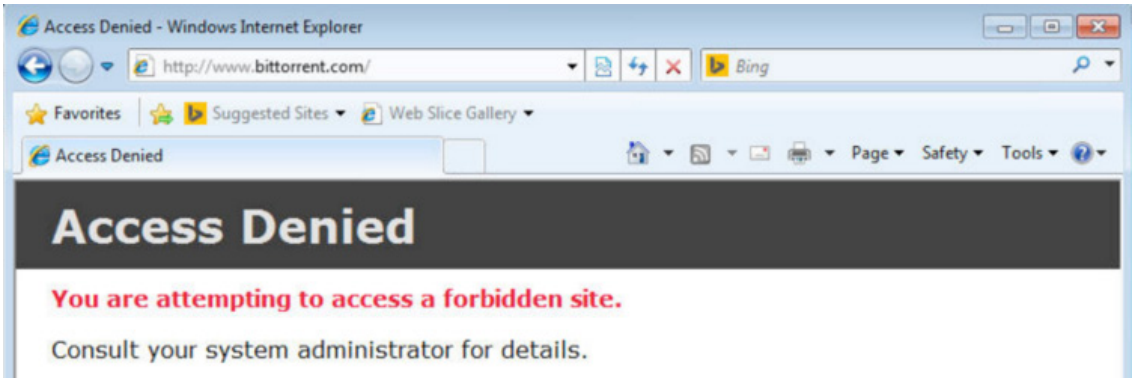
如果终端用户打开浏览器并试图下载 pwdump7。



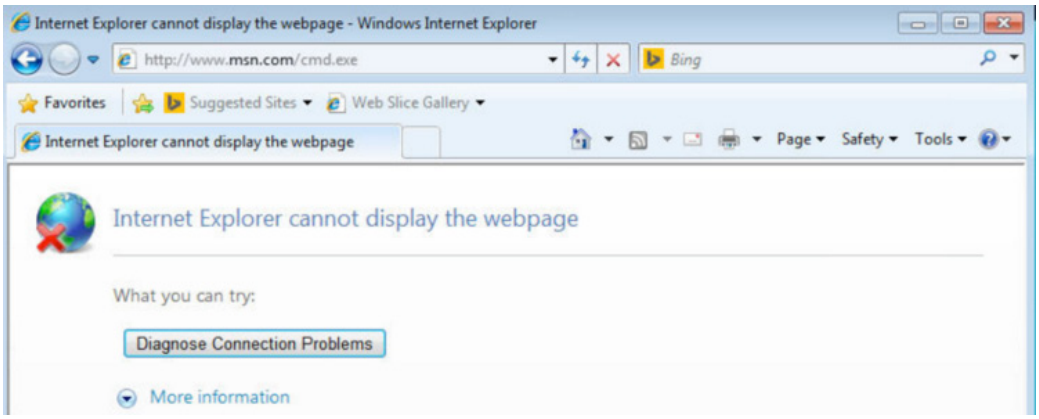
系统会将终端用户重定向到阻止响应页面，并阻止其访问活动。



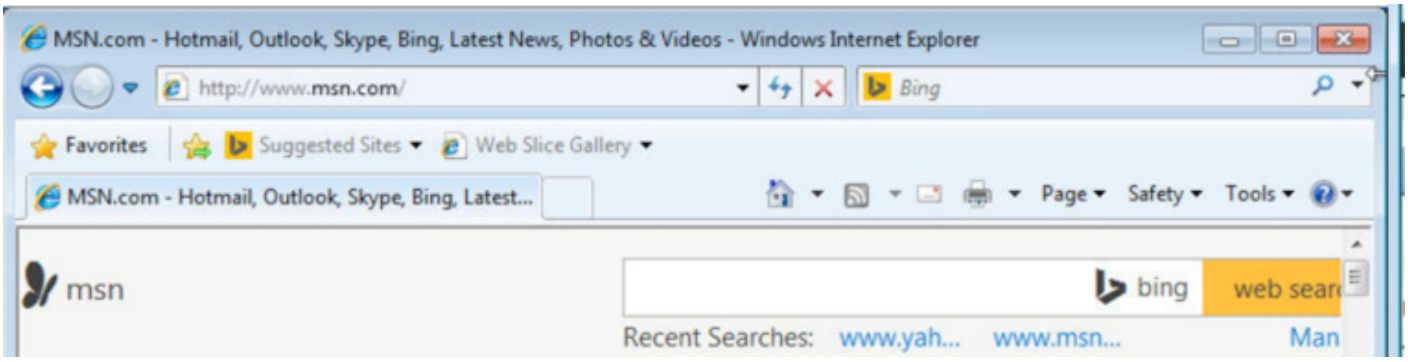
如果终端用户尝试访问 bittorrent 网站，其访问活动将被阻止。



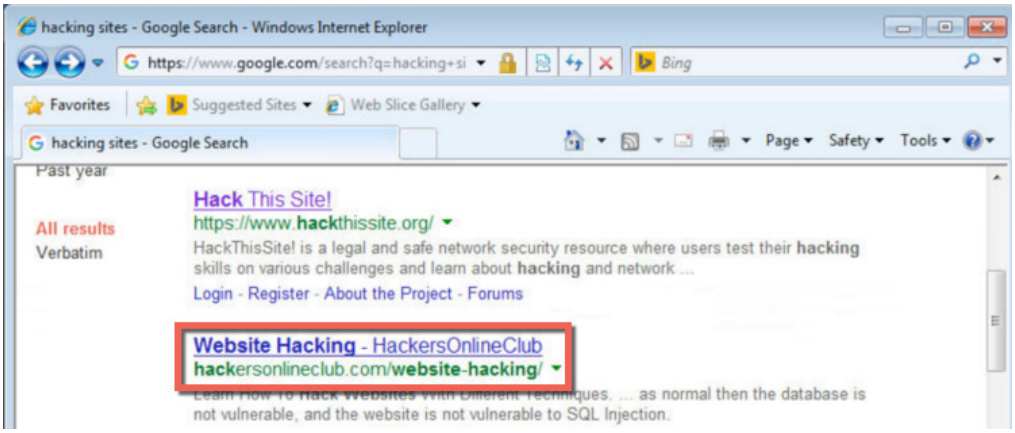
如果终端用户在地址栏中输入带有 cmd.exe 的网站链接（模拟受感染的 Web 服务器），其访问活动也会被阻止。



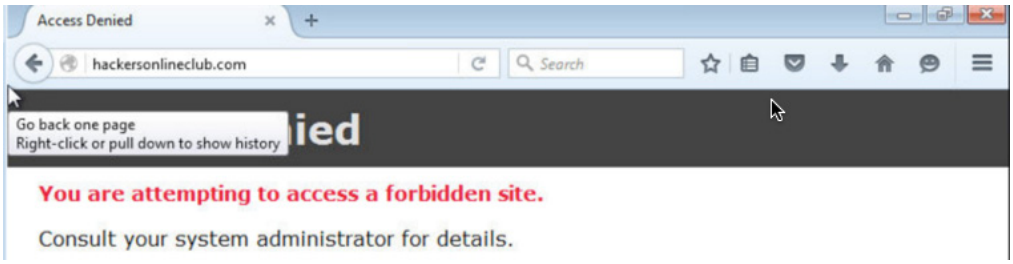
要证明所有其他访问活动能够正常工作，终端用户可以访问有效的网站。



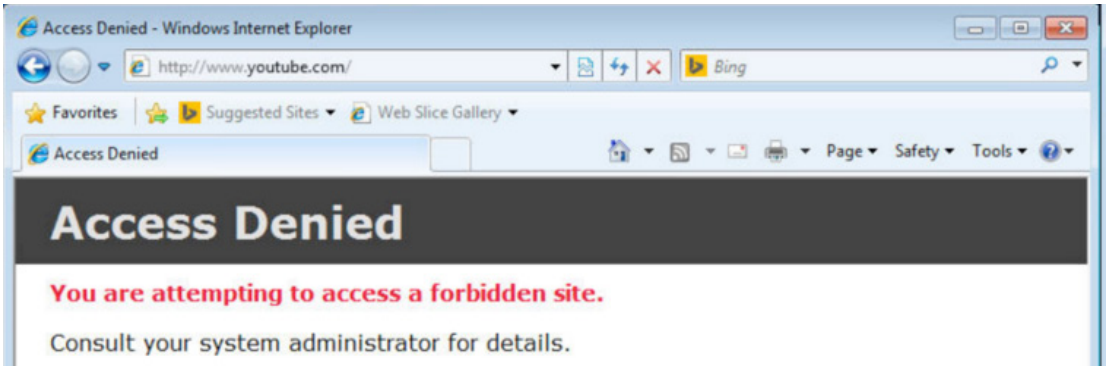
如果终端用户试图加入黑客俱乐部，其访问活动将被阻止。



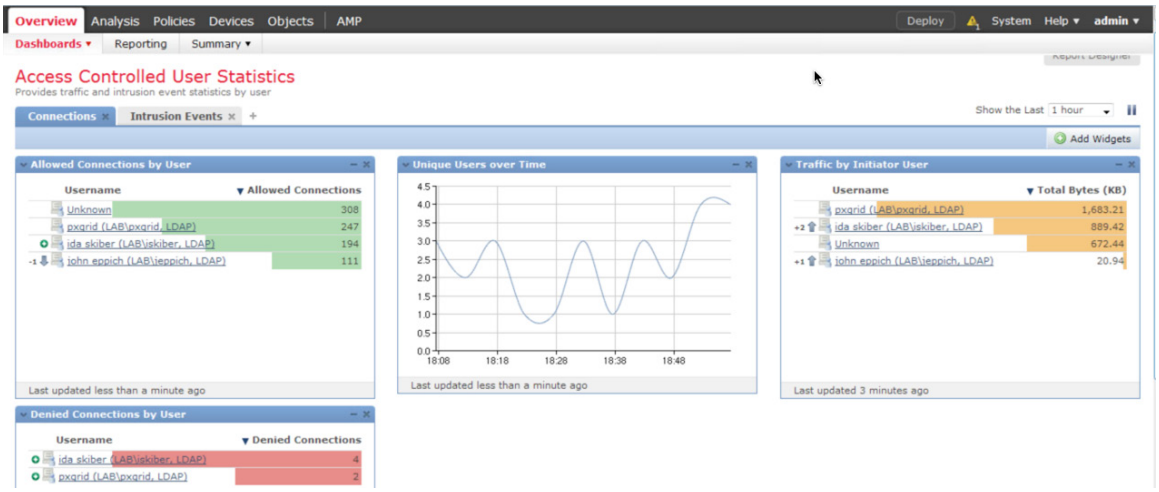
终端用户尝试加入黑客俱乐部，结果被阻止。



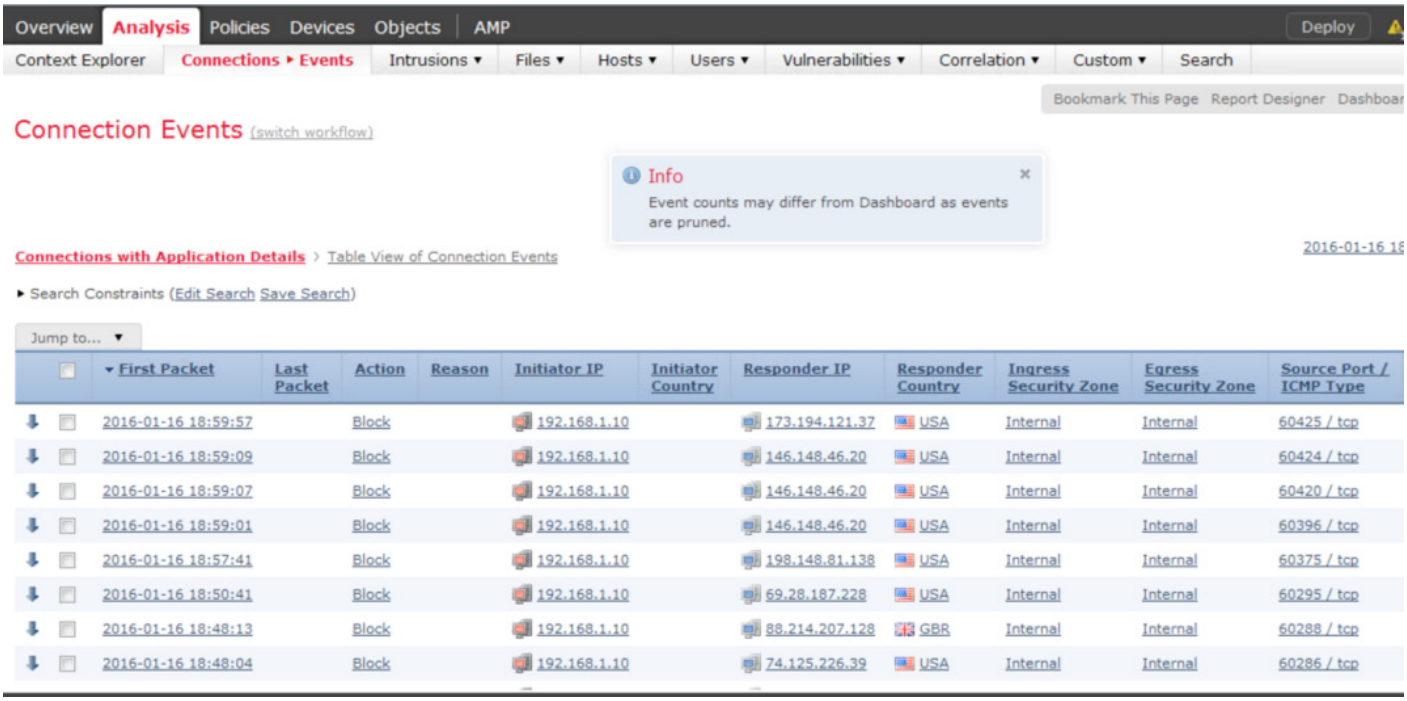
如果终端用户试图访问 www.youtube.com，也将遭到拒绝。



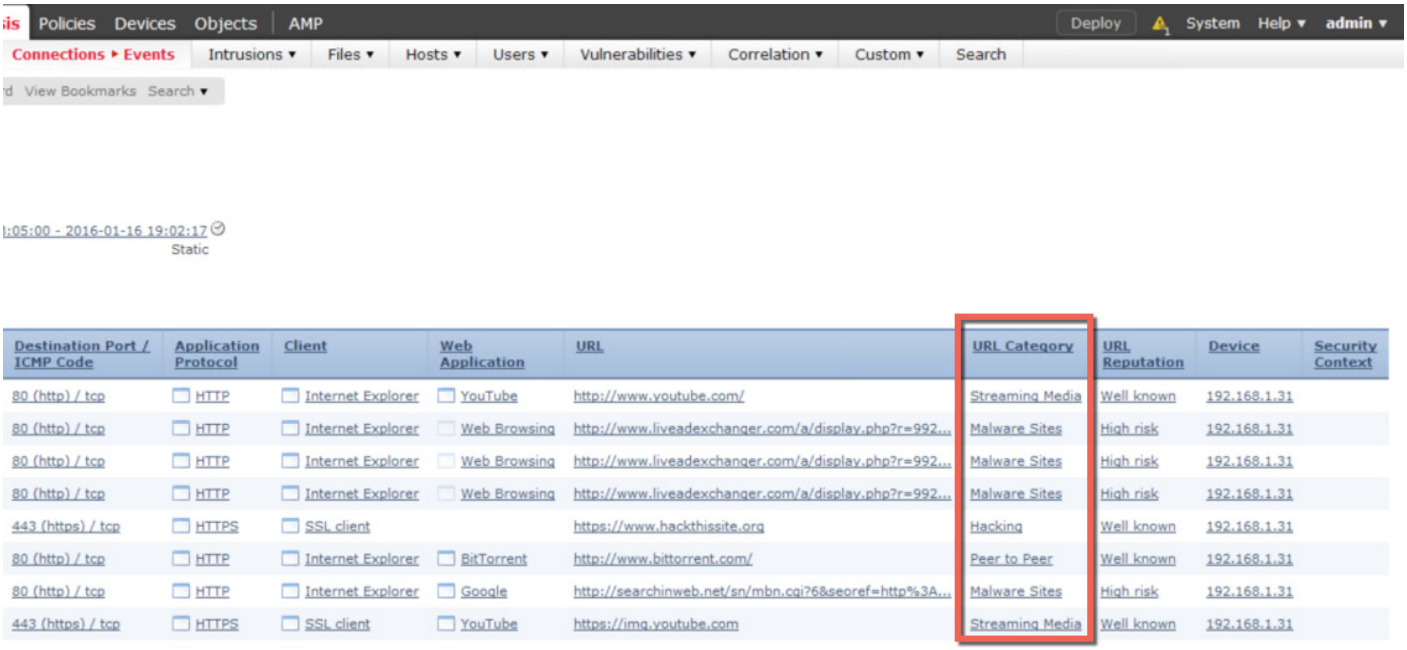
在 Firepower 管理中心“受访问控制的用户统计数据”(Access Controlled User Statistics) 控制面板中，您可以通过用户 iskiber 数据查看被拒绝的连接



如果点击与 iskiber 对应的“被拒绝连接”(Denied Connections)，系统将显示被拒绝的 URL 类别。这些被拒绝的类别表示 Firepower 管理中心访问控制规则“拒绝员工 SGT 的访问”(Deny Employee SGT Access) 中定义的 URL 类别。



下面的屏幕截图是上图的延续。



Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL	URL Category	URL Reputation	Device	Security Context
80 (http) / tcp	HTTP	Internet Explorer	YouTube	http://www.youtube.com/	Streaming Media	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Web Browsing	http://www.liveadexchanger.com/a/display.php?r=992...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client		https://www.hackthissite.org	Hacking	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	BitTorrent	http://www.bittorrent.com/	Peer to Peer	Well known	192.168.1.31	
80 (http) / tcp	HTTP	Internet Explorer	Google	http://searchinweb.net/sn/mbn.cgi?6&seoref=http%3A...	Malware Sites	High risk	192.168.1.31	
443 (https) / tcp	HTTPS	SSL client	YouTube	https://img.youtube.com	Streaming Media	Well known	192.168.1.31	

具备 FirePOWER 服务的 ASA

在本文档中，我们使用 ASA 5506W 执行测试。我们将安装 ASA Firepower (SFR) 模块，并针对以下内容对其进行测试：

- 托管 Firepower pxGrid 入侵策略和“员工”(Employee) SGT 访问控制规则。
- 本地托管 Firepower pxGrid 入侵策略和“员工”(Employee) SGT 访问控制规则。

使用集中的 Firepower 管理中心策略

在本节中，我们将安装 ASA Firepower (SFR) 模块。完成配置后，我们将把 ASA 注册到 Firepower 管理中心，通过它对 ASA 执行托管思科 Firepower 策略。

注意：请确保为所要托管的具备 Firepower 服务的 ASA 安装智能许可证或传统许可证。

安装 ASA Firepower (SFR) 并将其注册到 Firepower 管理中心

步骤 1 下载 ASDM 7.5.2 和 ASA 9.5.2，然后将下载文件上传到 ASA

步骤 2 安装 ASA Firepower 模块

```
ciscoasa# sw-module module sfr recover configure image disk0:/asasfr-5500x-6.0.0.img
```

步骤 3 打开调试功能，以便更容易地发现错误

```
ciscoasa# sh debug
ciscoasa# debug module
```

步骤 4 加载 ASA Firepower 引导映像

```
ciscoasa# sw-module module module sfr recover boot
```

步骤 5 等待大约 5-15 分钟，以便 ASA Firepower 完成启动过程，然后从控制台打开与当前运行的 ASA Firepower 引导映像的会话。您可以按几次 Enter 键，然后键入以下命令：

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is ‘CTRL_^X’.

Cisco ASA SFR Boot Image 5.3.1
asasfr login:admin
Password: Admin123
```

步骤 6 使用系统安装命令安装软件系统映像，下面为使用 ftp 的命令示例：

```
asa-boot>system install http://jeppich:password@192.168.1.8/asasfr-5500x-6.0.0.img
```

系统会在完成此命令后关闭并重新启动。在 SFR 恢复运行之前，您可能需要等待一段时间。对于本例中使用的 ASA 5506，等待时间在 30 分钟以上。您可以输入如下命令检查重启情况

```
sh module sfr
```

如果重启完成，您会看到 SFR 模块；如果 SFR 仍在恢复状态，则说明模块正在安装

步骤 7 打开与 ASA Firepower 模块的会话

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr.Escape character sequence is ‘CTRL- ^X’ .

Sourcefire3D login: admin
Password: Admin123
```

步骤 8 阅读并接受 EULA，然后完成系统配置

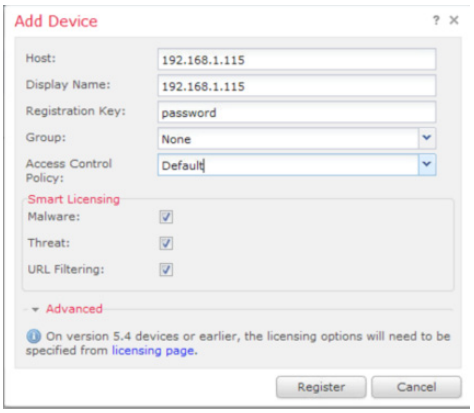
步骤 9 将具备 ASA Firepower 服务添加到 Firepower Management 6.0

```
> configure manager add (ip address of Cisco Firepower Management Console) password
```

步骤 10 确保您为 ASA 安装了正确的许可证

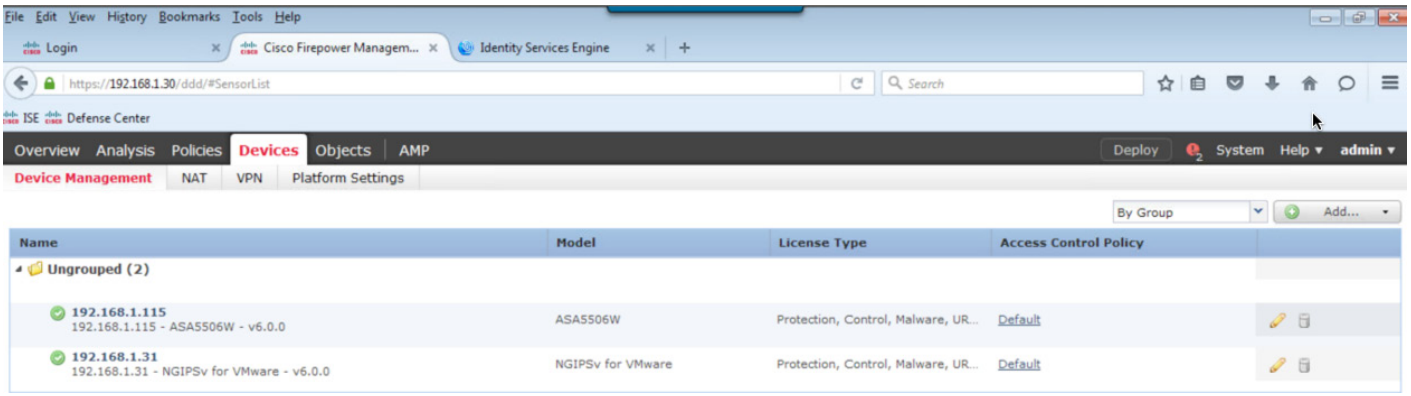
步骤 11 将 ASA Firepower 设备添加到 Firepower 管理中心 6.0，然后输入设备信息，并启用许可证

选择**设备 (Devices) -> 设备管理 (Device Management) -> 添加 (Add) -> 添加设备 (Add Device)**



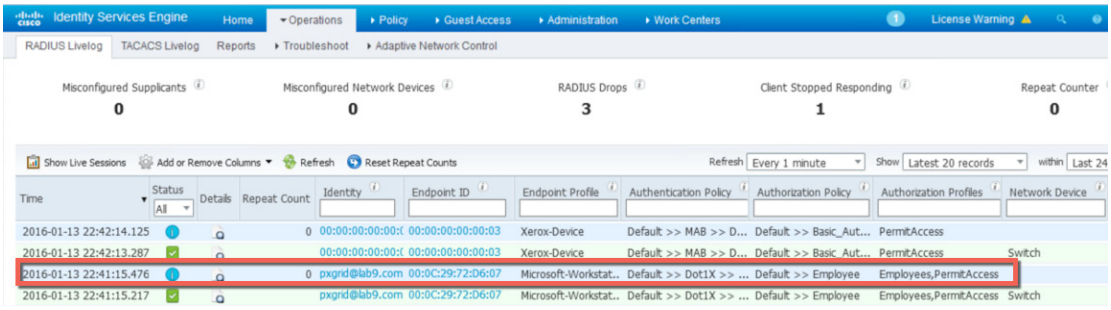
步骤 12 选择“注册”(Register)

步骤 13 ASA Firepower 成功注册后，您应看到下图所示的内容：

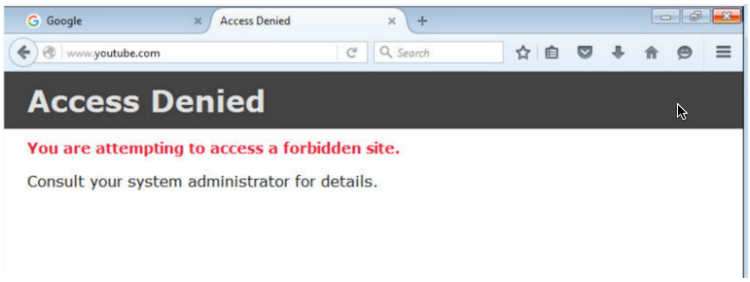


通过托管 Firepower 管理策略使用“员工”SGT 测试用户

在本节中，我们将针对一名标记为“员工”(Employee) 的终端用户测试我们创建的 FMC 6.0 策略。根据 ISE 身份验证策略，终端用户在成功通过 802.1X 身份验证后被分配“员工”(Employee) SGT。

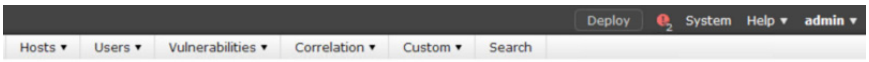


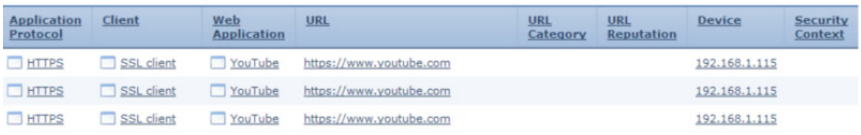
如果终端用户打开浏览器并访问 www.youtube.com，访问将被拒绝



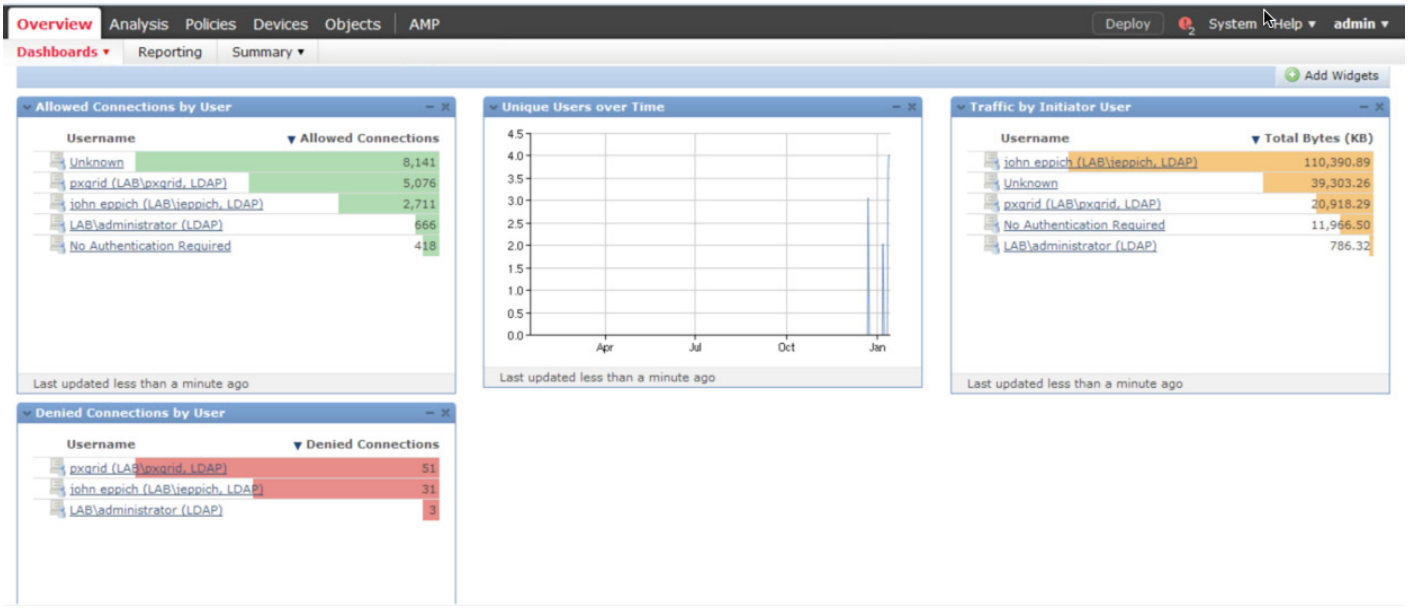
在 Firepower 管理中心中，选择**分析 (Analysis) -> 连接 (Connection) -> 事件 (Events)**，查看被阻止的事务的详细信息

在下面的延续屏幕截图中，可以看到 www.youtube.com

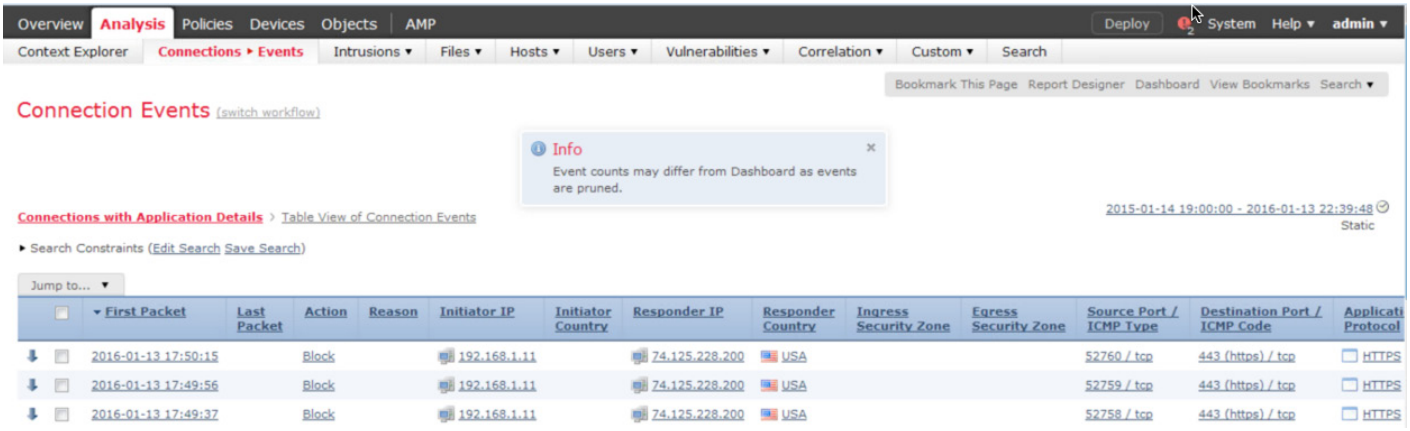




在 Firepower 管理中心中，选择**概览 (Overview) -> 控制面板 (Dashboards) -> 受访问控制的用户统计数据 (Access Controlled User Statistics)**，然后点击**按用户统计的被拒绝连接数 (Denied Connections by User)** 下的 pxGrid



您会看到与 www.youtube.com 相关的阻止连接事件



本地 Firepower 策略管理

本节将详细说明如何通过 ASDM 对具备 Firepower 服务的 ASA 进行本地管理。请注意，要通过 ASDM 在 ASA 中实施本地 Firepower 策略，您需要使用单独的许可证，并且需要针对 CA 签名环境配置具备 Firepower 服务的 ASA。

从 Firepower 管理中心 6.0 中删除 ASA

步骤 1 从 Firepower 管理中心 6.0 中删除 ASA5500 设备

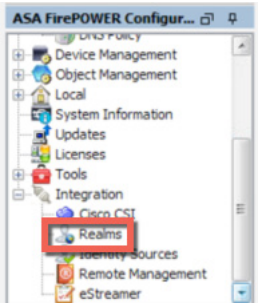
选择**设备 (Devices) -> 设备管理 (Device Management)**，然后点击  删除 ASA 5500 传感器

注意：如果您没有从 FMC 6.0 中删除 ASA 设备，ASDM 将无法看到 ASA Firepower 配置详细信息。您还需要一组单独的许可证，进行本地注册

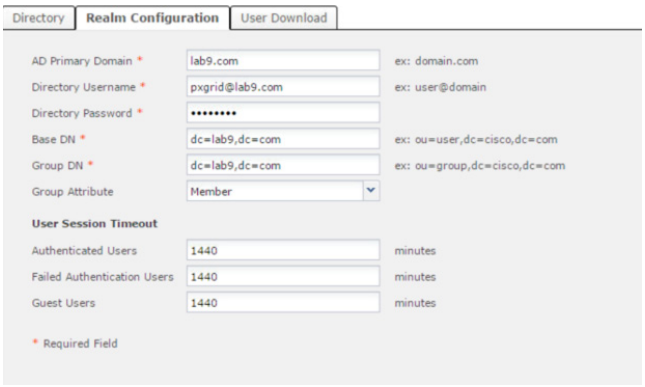
ISE 领域配置

首先，我们需要在 ISE 中配置 ISE 领域

步骤 1 选择 **ASA Firepower 配置 (ASA Firepower Configuration) -> 领域 (Realms)**

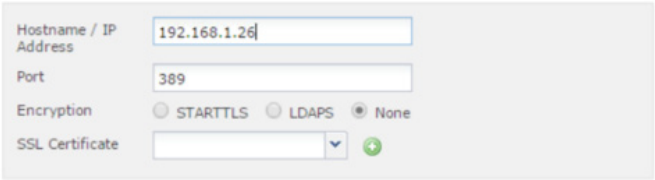


步骤 2 选择**新建领域 (New Realm)**，并输入领域配置详细信息



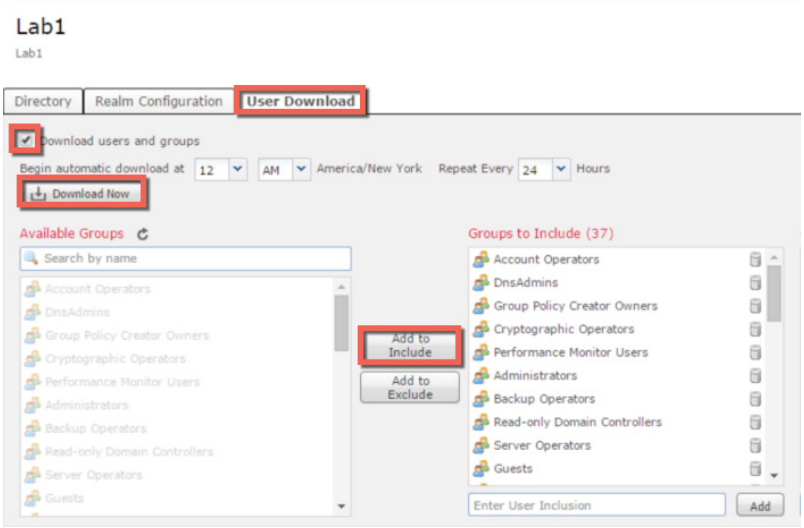
步骤 3 选择**确定 (OK)**，然后点击**状态 (State)** 启用新建的领域

步骤 4 选择**添加目录 (Add Directory)**，并按照如下屏幕输入信息



步骤 5 选择**测试 (Test)**，您应看到操作成功的提示

步骤 6 点击**用户下载 (User Download)**，选中**下载用户和组 (Download users and groups)**，然后点击**立即下载 (Download Now) -> 添加到包括项 (Add to Include)**

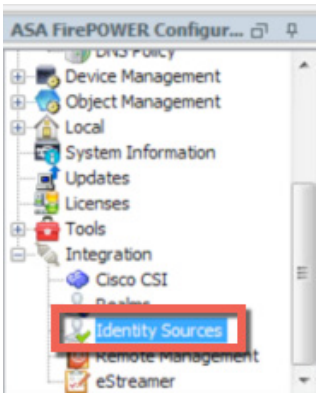


步骤 7 点击**存储 ASA Firepower 更改 (Store ASA Firepower Changes)**

ISE 身份源配置

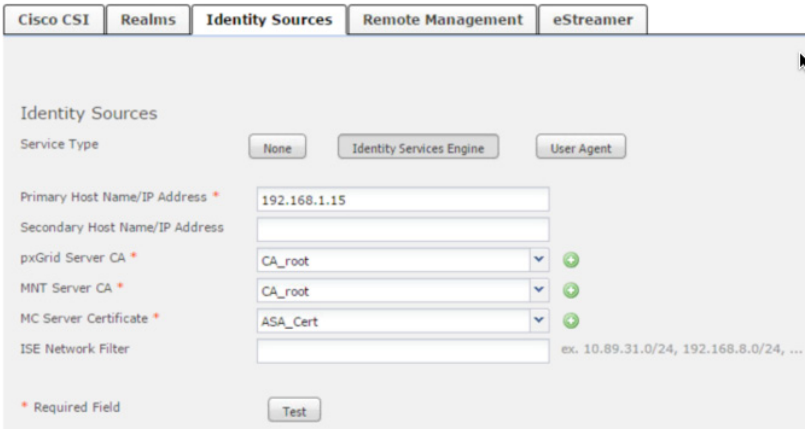
身份源配置包含具备 Firepower 服务的 ASA 与 ISE pxGrid 节点之间的连接参数。请注意，ASA 具有 CA 签名证书。如果您不熟悉证书安装操作，请参阅使用 CA 签名证书的操作步骤。

步骤 1 选择 **ASA Firepower 配置更改 (ASA Firepower Configuration Changes) -> 身份源 (Identity Sources)**

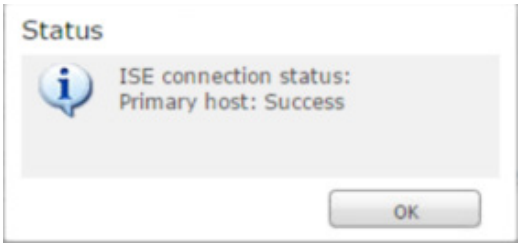


步骤 2 选择**身份源引擎 (Identity Sources Engine)**，然后按照下图所示提供 ISE pxGrid 配置：

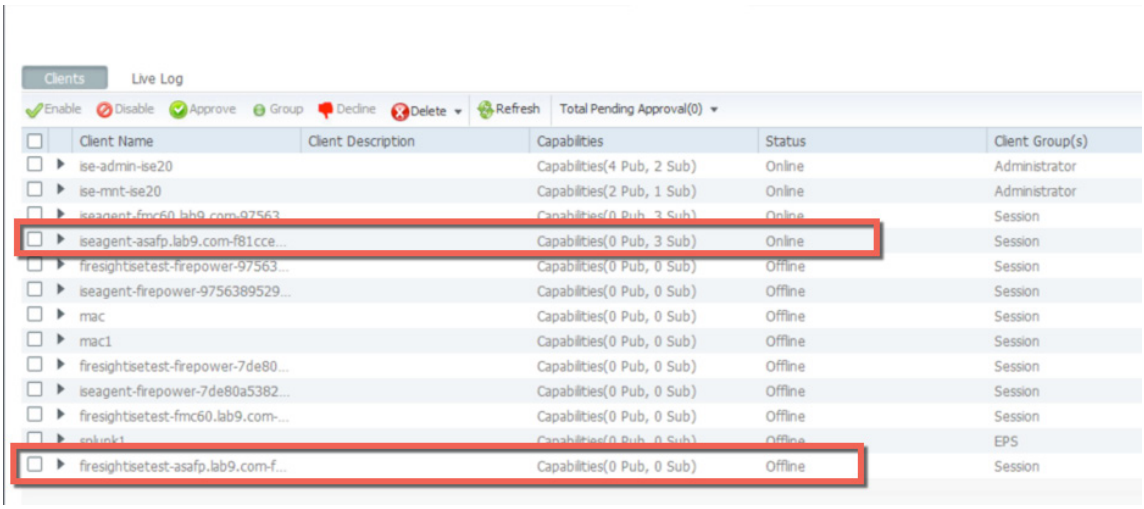
注意：请为自签证书和 CA 签名证书提供正确的证书信息



步骤 3 选择**测试 (Test)** 检查与 ISE pxGrid 节点的连接，您应看到如下提示：



步骤 4 您应看到 ASA Firepower 已成功注册为 pxGrid 客户端
选择**管理 (Administration) -> pxGrid 服务 (pxGrid Services)**



步骤 5 如果系统提示尝试失败，

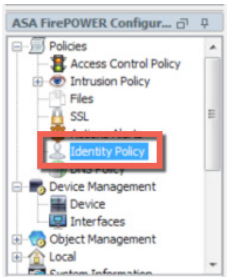
步骤 6 请选择**监控 (Monitoring) -> ASA Firepower 监控 (ASA Firepower Monitoring)**，以查看相关的详细信息

注意：此处的失败很可能是因为证书问题导致的

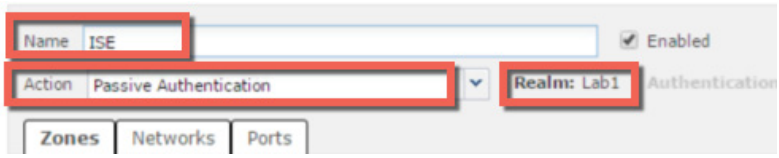
ISE 身份策略

接下来，我们将配置 ISE 身份策略，以支持被动身份验证，并在 Firepower 管理中心默认访问控制规则中使用该策略进行 ISE 身份验证。

步骤 1 选择 **ASA Firepower 配置 (ASA Firepower Configuration) -> 策略 (Policies) -> 身份策略 (Identity Policy)**

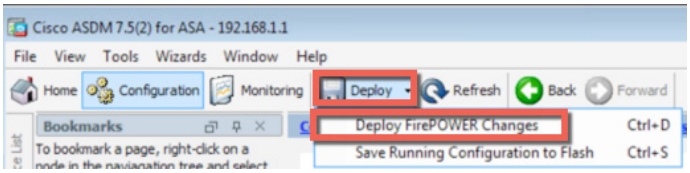


步骤 2 点击**添加规则 (Add Rule)**，输入规则名称，选择**被动身份验证 (Passive Authentication)**，并设置**领域 (Realm)**



步骤 3 选择**存储 ASA Firepower 更改 (Store ASA Firepower Changes)**

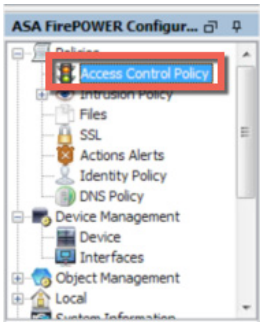
步骤 4 选择**部署 (Deploy) -> 部署 Firepower 更改 (Deploy Firepower Changes) -> 部署 (Deploy) -> 确定 (OK)**



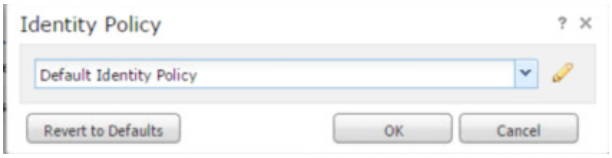
添加 ISE 身份策略

下面，我们需要将 ISE 身份策略添加到 Firepower 管理中心的默认访问策略

步骤 1 选择 **ASA Firepower 配置 (ASA Firepower Configuration) -> 策略 (Policies) -> 访问控制策略 (Access Control Policy)**



步骤 2 选择 **ASA Firepower -> 添加规则 (Add Rule) -> 身份策略 (Identity Policy) -> 无 (None)**，然后从下拉列表中选择**默认身份策略 (Default Identity Policy)**



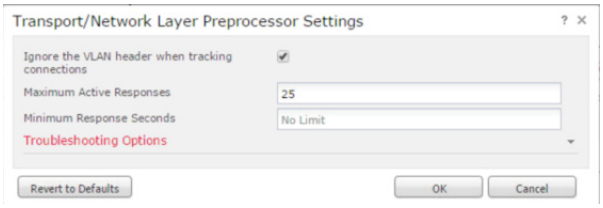
步骤 3 选择**确定 (OK)**

步骤 4 点击**存储 ASA Firepower 更改 (Store ASA Firepower Changes)**

传输/网络层预处理器设置

我们还需要修改传输/网络层预处理器设置，以便根据 Firepower 入侵策略阻止网络访问。

步骤 1 点击**高级 (Advanced) -> 传输/网络层预处理器设置 (Transport/Network Layer Preprocessor Settings) ->**  ，然后按照如下图示进行设置：



步骤 2 选择**确定 (OK)**

添加阻止响应页面

下一步是添加系统提供的阻止响应页面，作为对 Firepower 访问控制文件的阻止响应。

步骤 1 点击 **HTTP 响应 (HTTP Responses)**，然后按照如下图示进行设置：

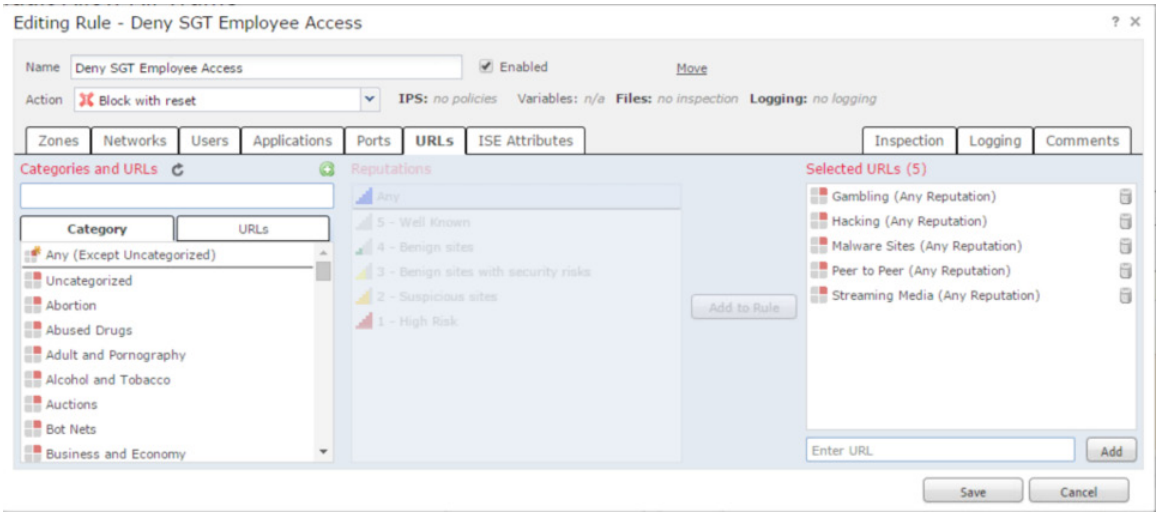
步骤 2 点击**存储 ASA Firepower 更改 (Store ASA Firepower Changes)**

在 ASA 中创建“员工”SGT 标签访问控制规则

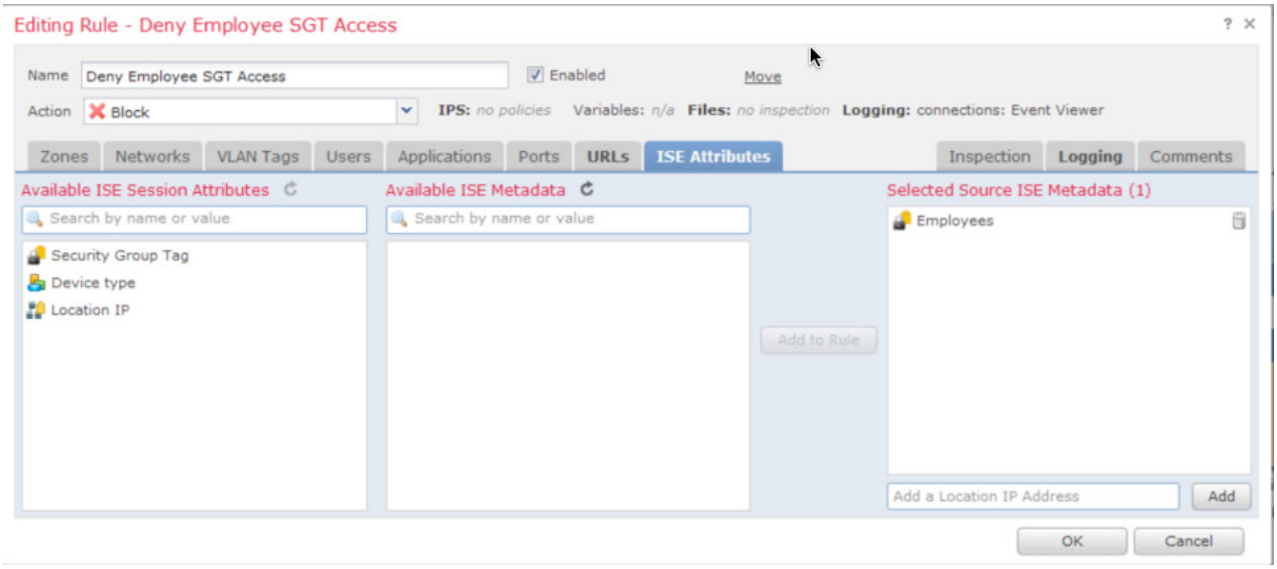
“员工”(Employee) SGT 标签访问控制规则用于定义一条公司可接受使用策略，以阻止对以下资源类型的访：“黑客类”网站、流媒体、点对点应用、“恶意软件类”网站和“赌博类”网站

步骤 1 选择 **ASA Firepower 配置 (ASA Firepower Configuration) -> 访问控制策略 (Access Control Policy) -> ASA Firepower -> 添加规则 (Add Rule)**

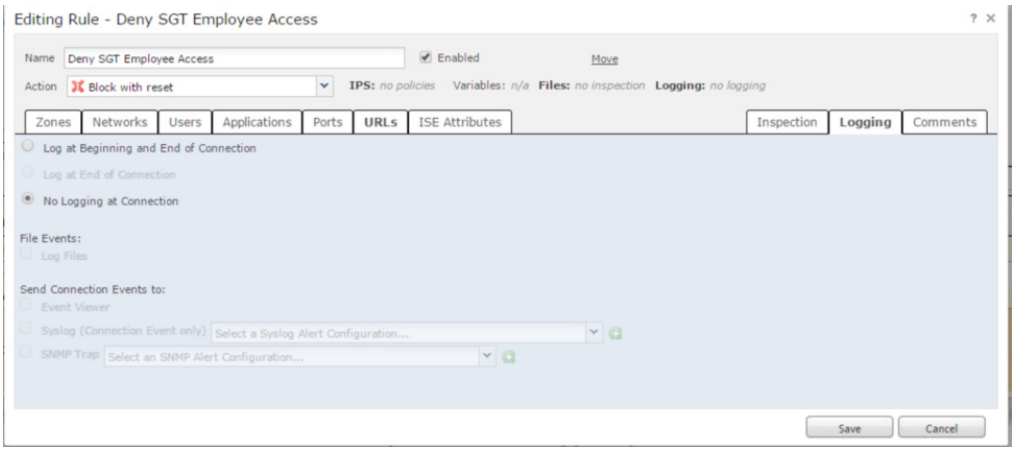
步骤 2 选择**添加规则 (Add Rule)**，在**名称 (Name)** 框中输入：**Deny Employee SGT Access**，在**操作 (Action)** 框中输入：**Block with reset**，将 **IPS** 设置为 **pxGrid 入侵策略 (pxGrid Intrusion Policy)**。然后选择 **URLs -> 类别 (Category)**，选中**赌博 (Gambling)**、**点对点 (Peer-to-Peer)**、**流媒体 (Streaming Media)** 和**黑客 (Hacking)**，点击**保存 (Save)**



步骤 3 选择 **ISE 属性 (ISE Attributes) -> 可用 ISE 会话属性 (Available ISE session attributes) -> 安全组标记 (Security Group Tag) -> 可用 ISE 元数据 (Available ISE Metadata)**，选择**员工 (Employees)**，然后点击**添加到规则 (Add to Rule)**

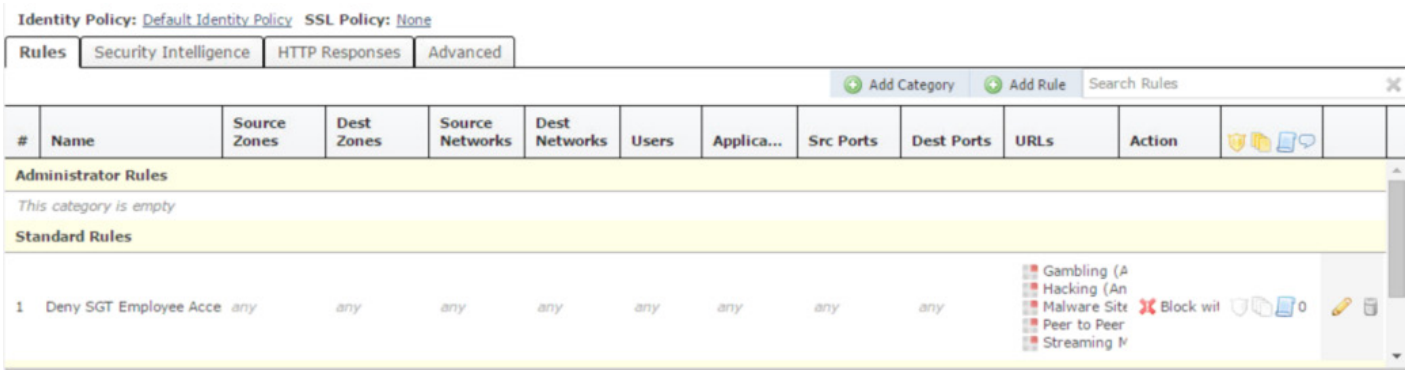


步骤 4 选择“日志记录”(Logging)，并按照下图进行配置



步骤 5 选择**保存 (Save)**

您应该看到以下内容



步骤 6 选择**保存 (Save)**

步骤 7 选择**存储 ASA Firepower 更改 (Store ASA Firepower Changes)**

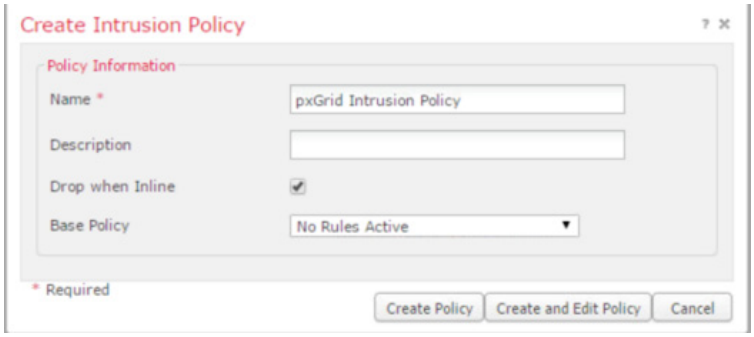
步骤 8 选择**部署 (Deploy) -> 部署 Firepower 更改 (Deploy Firepower Changes) -> 部署 (Deploy) -> 确定 (OK)**

步骤 9 选择**监控 (Monitoring) -> ASA Firepower 监控 (ASA Firepower Monitoring) -> 任务状态 (Task Status)**，查看部署状态

ASA Firepower pxGrid 入侵策略

在本节中，我们将创建 pxGrid 入侵策略，并将其部署到 Firepower 传感器。此策略包含“SERVER IIS CMD.EXE 访问”(SERVER IIS CMD.EXE access) 规则，如果终端用户在浏览器中输入 www.yahoo.com/cmd.exe，便会触发入侵事件，系统将执行内联丢弃，且 Firepower 管理控制台的“分析入侵事件”(Analysis Intrusion Events) 日志中将生成事件

步骤 1 选择“ASA Firepower 配置”(ASA Firepower Configuration) ->“入侵策略”(Intrusion Policies) ->“创建策略”(Create Policy)，然后按照下图进行配置：

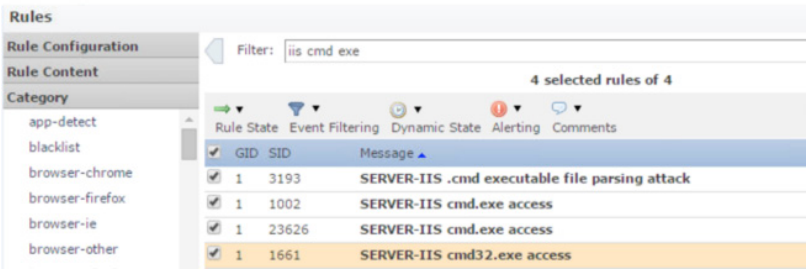


步骤 2 点击**创建策略 (Create Policy)**

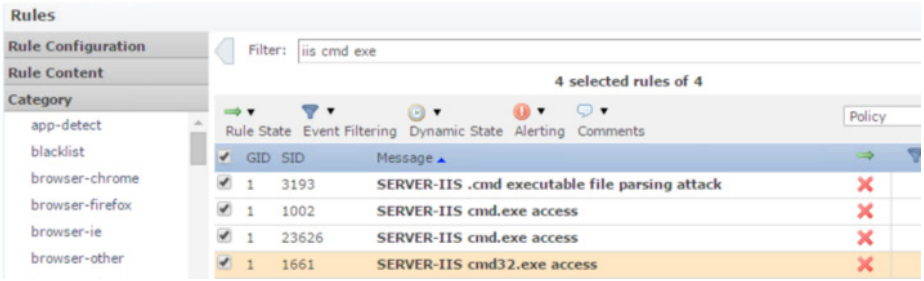
步骤 3 您应该看到以下内容

步骤 4 点击  编辑新建的策略

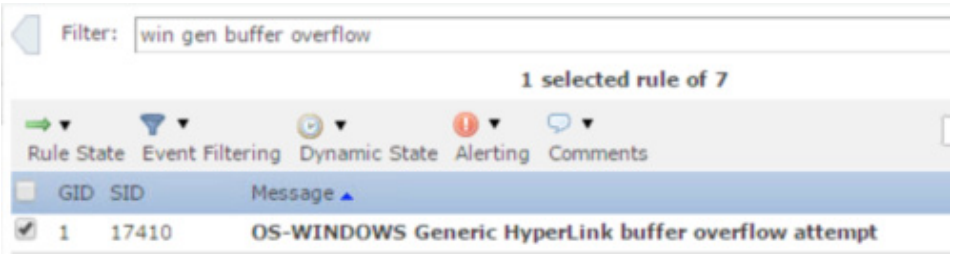
步骤 5 点击**规则 (Rules)**，在**过滤器 (Filter)** 字段中输入：**iis cmd exe**，然后按下图所示进行选择



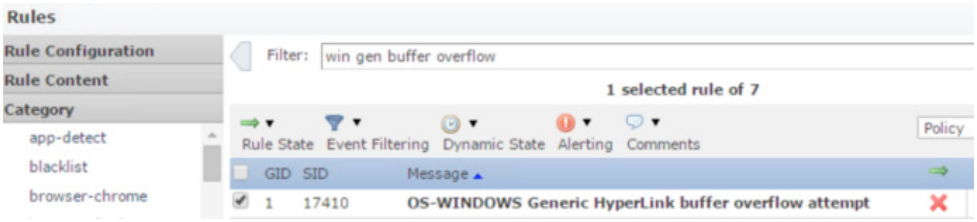
步骤 6 点击**规则状态 (Rule State)**，选择**丢弃并生成事件 (Drop and Generate Events)**，点击**确定 (OK)**
您将看到以下内容：



步骤 7 然后，在“过滤器”(Filter) 字段中输入：**win gen buffer overflow**，并选择**操作系统-Windows 通用超链接缓冲区溢出尝试 (OS-Windows Generic Hyperlink Buffer Overflow Attempt)**

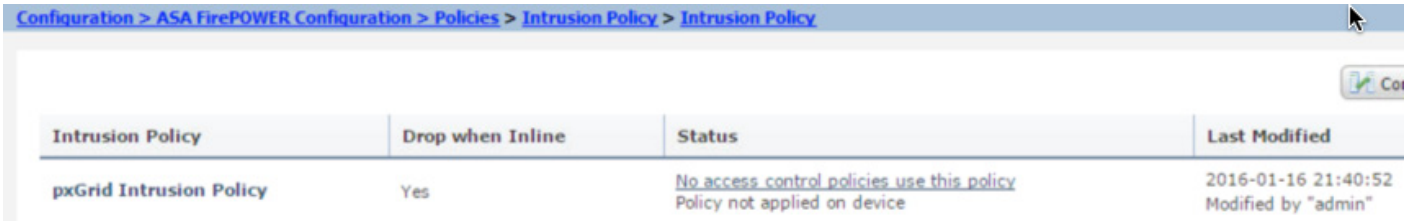


步骤 8 **点击规则状态 (Rule State)，选择丢弃并生成事件 (Drop and Generate Events)，点击确定 (OK)**



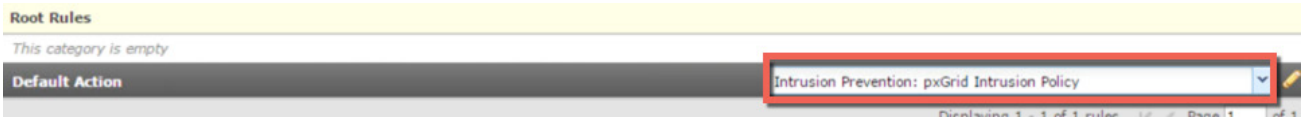
步骤 9 点击“策略信息”(Policy Information) 提交更改

步骤 10 点击“提交更改”(Commit Changes) ->“确定”(OK)。
步骤 11 您应该看到以下内容

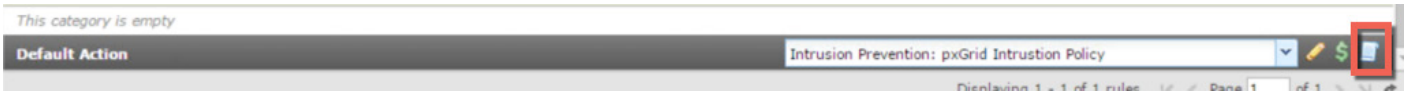


步骤 12 将 pxGrid 入侵策略添加到默认访问控制策略

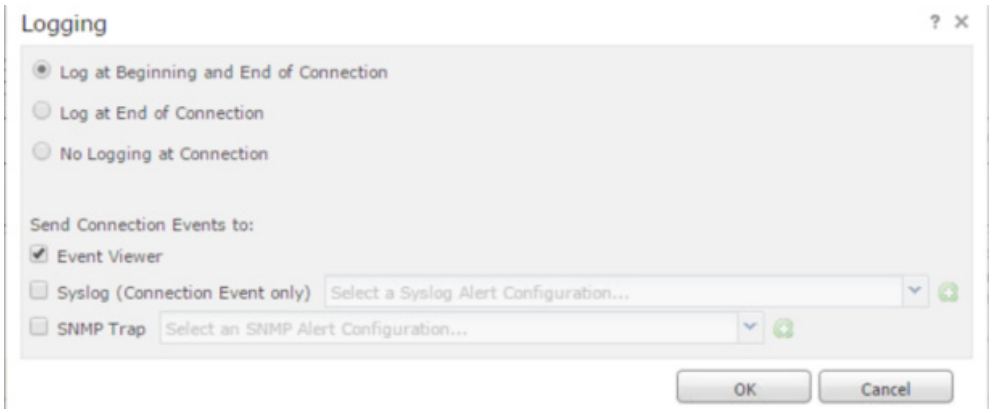
选择“ASA Firepower 配置”(ASA Firepower Configuration) ->“策略”(Policies) ->“访问控制策略”(Access Control Policy)，从下拉列表中选择“入侵防护：pxGrid 入侵策略”(Intrusion Prevention: pxGrid Intrusion Policy)



步骤 13 选择  配置日志记录设置



步骤 14 按照下图所示配置日志记录设置



步骤 15 点击“确定”(OK)

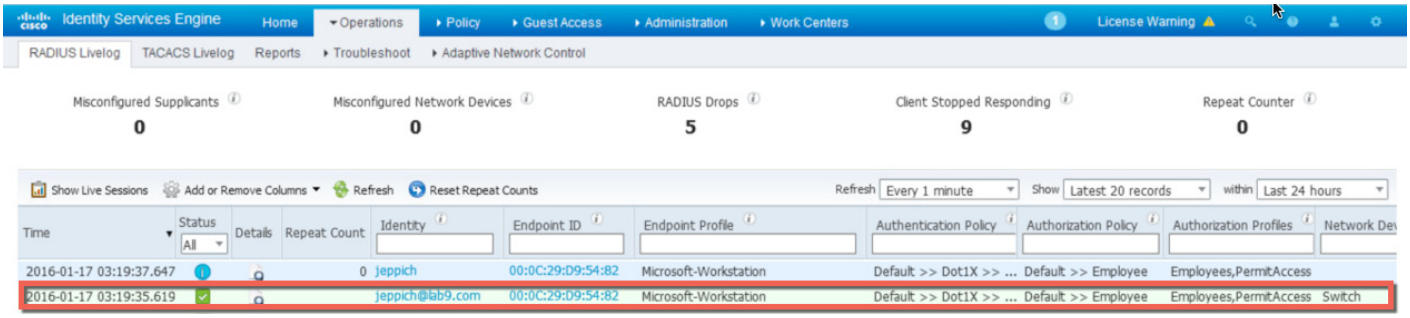
步骤 16 点击“存储 ASA Firepower 更改”(Store ASA Firepower Changes)

步骤 17 点击“部署”(Deploy) ->“部署 Firepower 更改”(Deploy Firepower Changes) ->“部署”(Deploy) ->“确定”(OK)

步骤 18 点击“监控”(Monitoring) ->“ASA Firepower 监控”(ASA Firepower Monitoring) ->“任务”(Task)，查看部署状态

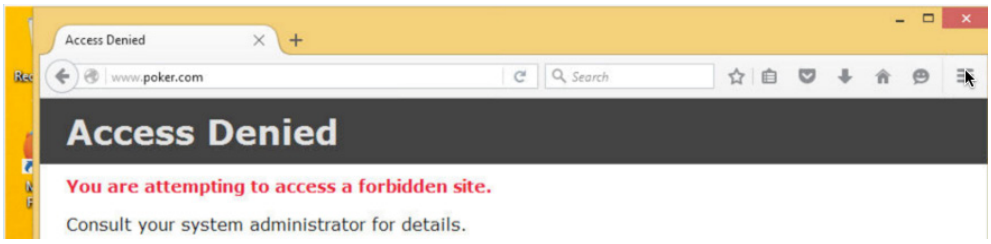
通过本地 Firepower 管理策略使用“员工”SGT 测试用户

员工成功进行 ISE 身份验证后，会被分配一个“员工”(Employee) SGT。

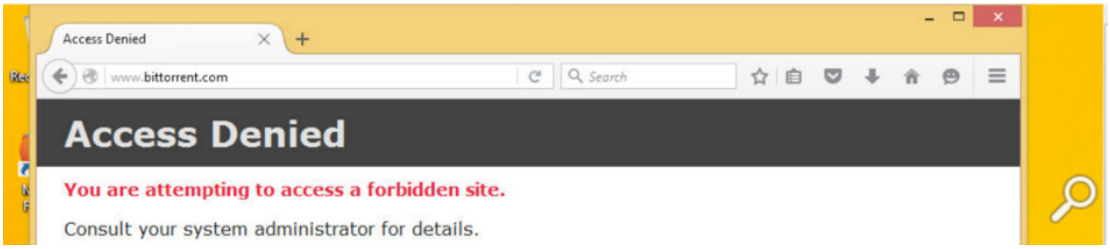


我们看到 Firepower 管理中心已经获得了用户会话信息

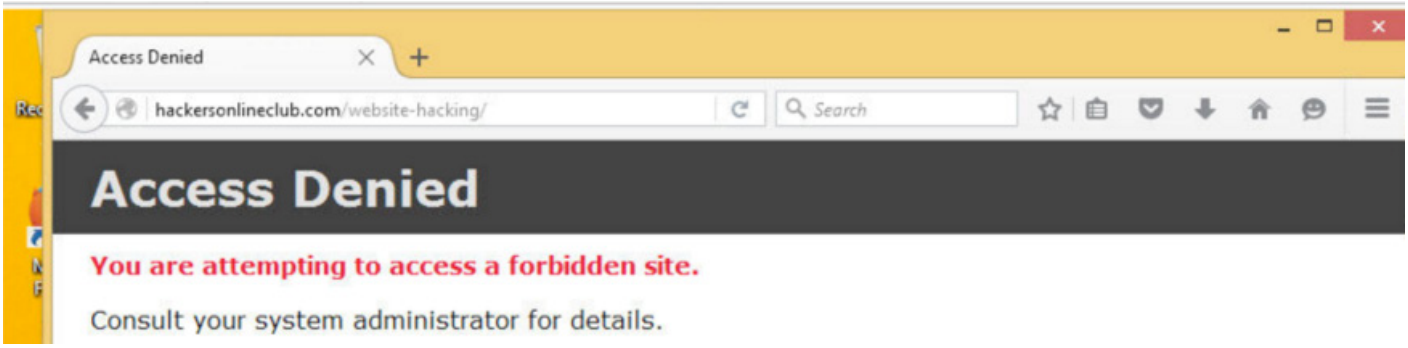
如果该员工访问 www.poker.com，则会遭到拒绝



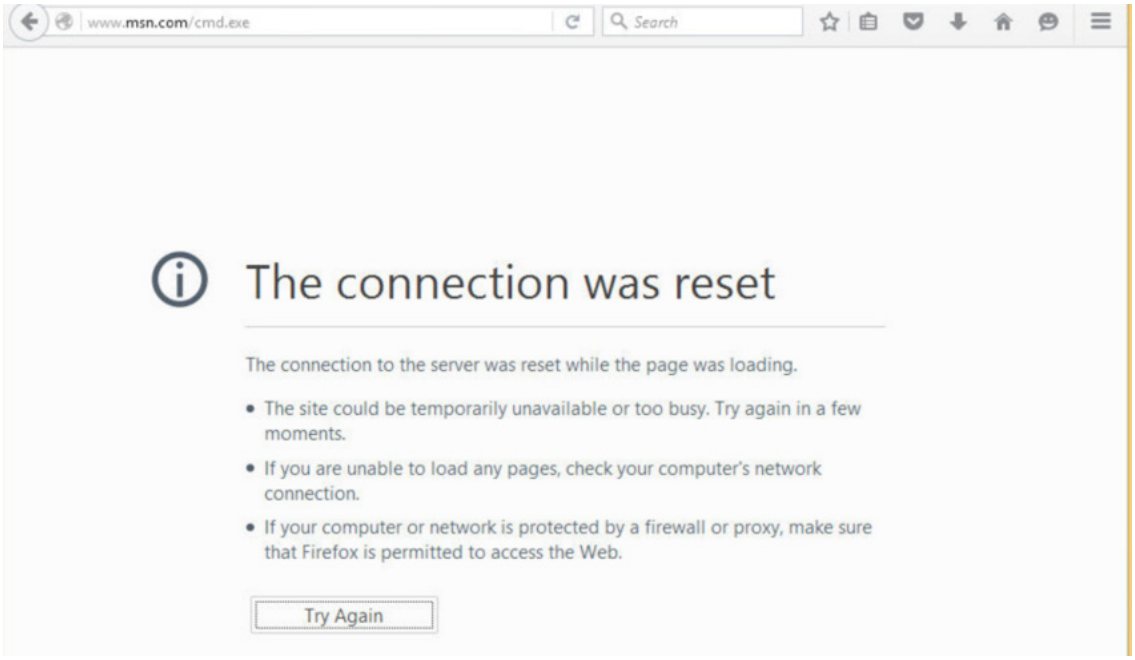
若该员工访问 www.bittorent.com，也会被拒绝



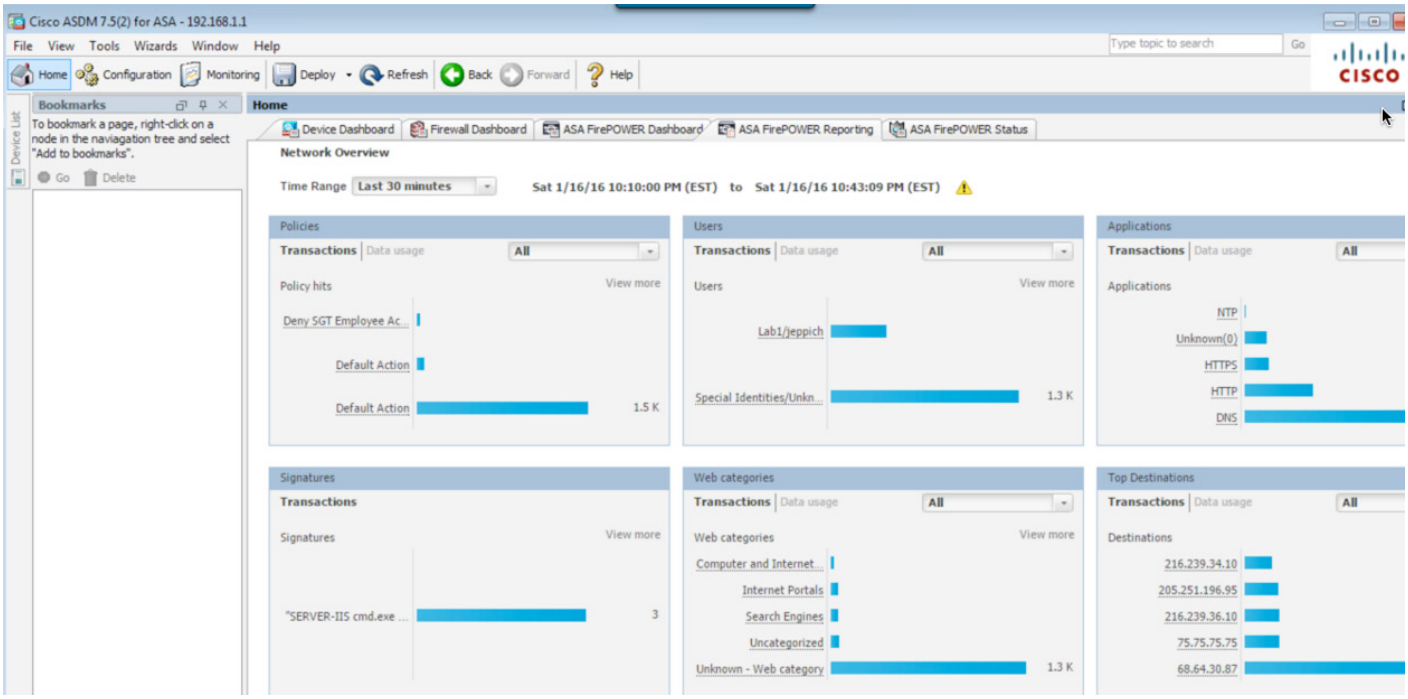
如果该员工试图加入黑客俱乐部 (www.hackersonlineclub.com)，同样会被拒绝



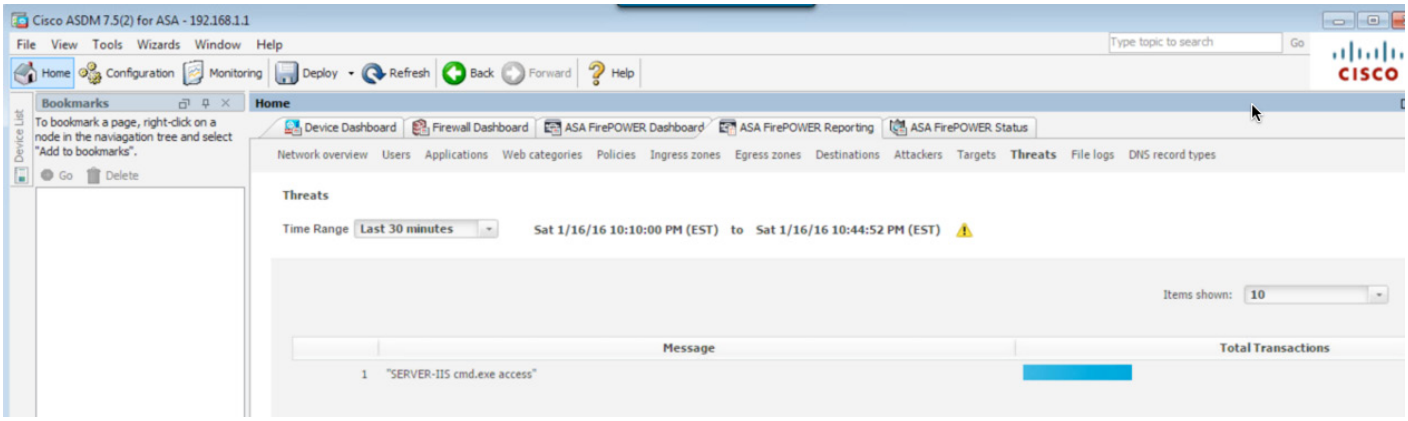
如果该员工尝试在浏览器中输入 www.msn.com/cmd.exe，则会被拒绝访问。



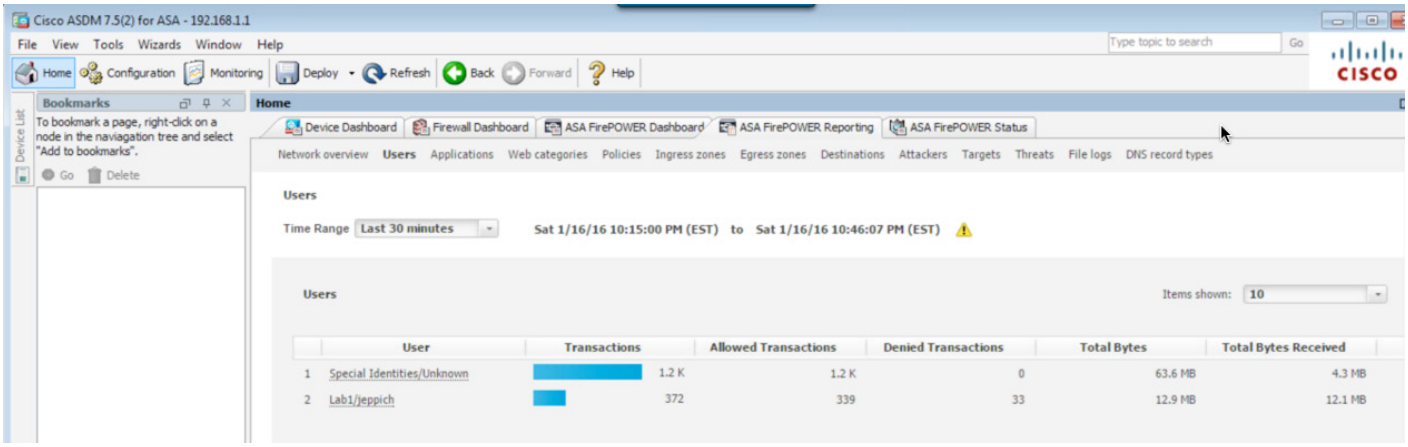
您可以在“ASA Firepower 报告”(ASA Firepower Reporting) 中查看报告。请注意被拒绝的网络类别事务以及被禁止的服务器 IIS-Web 签名



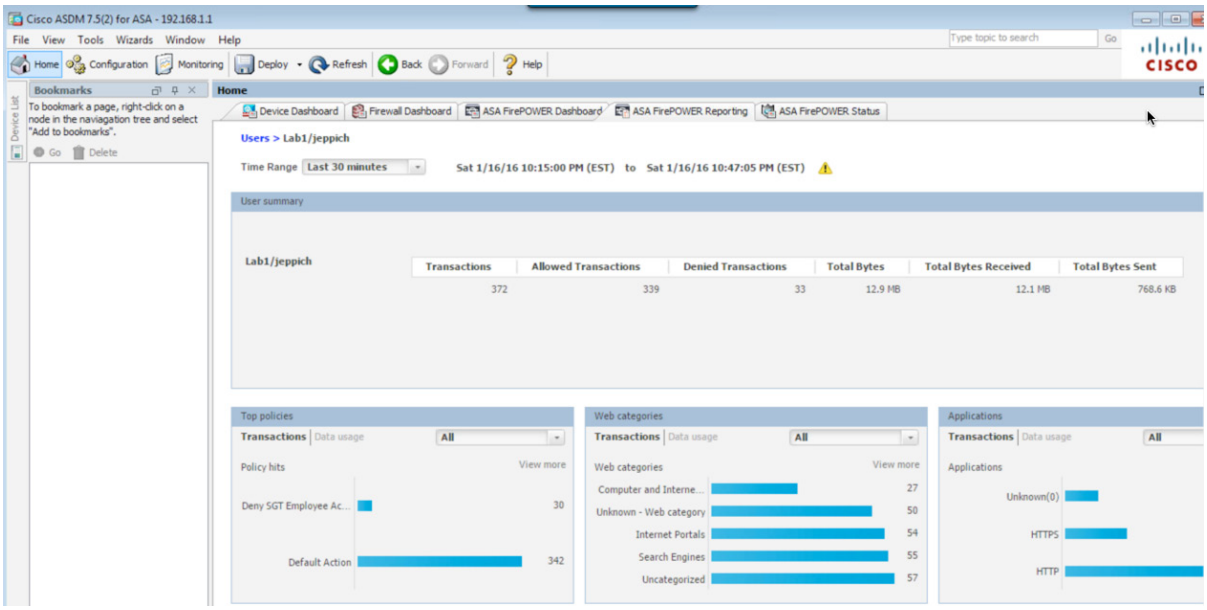
如果您点击下图所示的“威胁”(Threat) 报告，请注意 SERVER-IIS 的签名



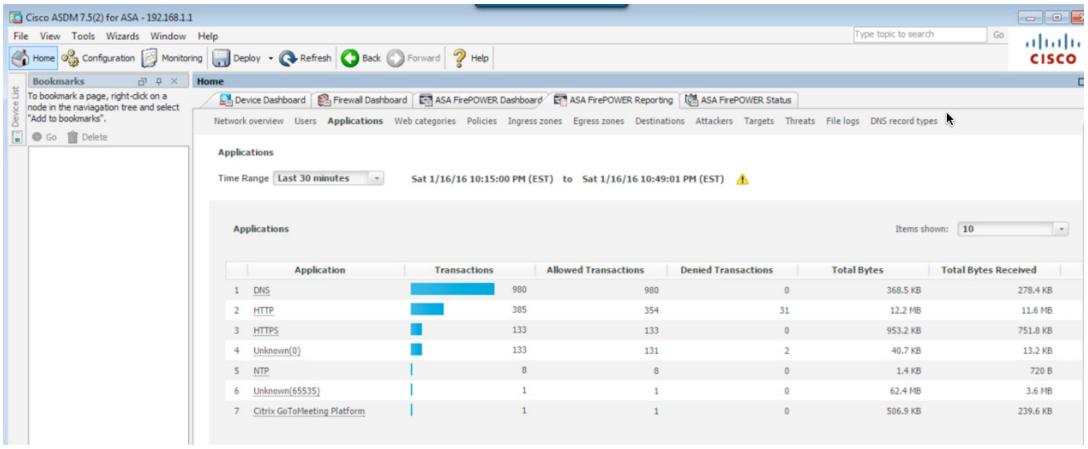
如果您选择按用户显示的报告，并点击 jeppich



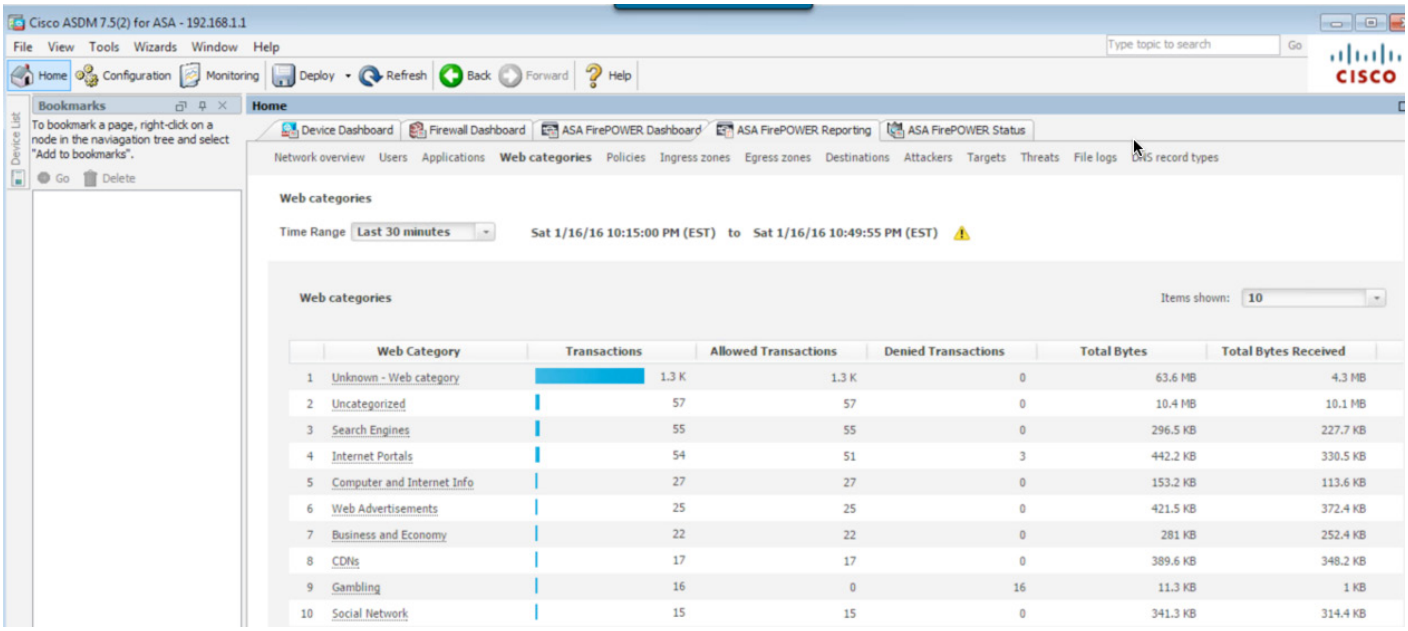
您将看到最主要的事务、网络类别和应用



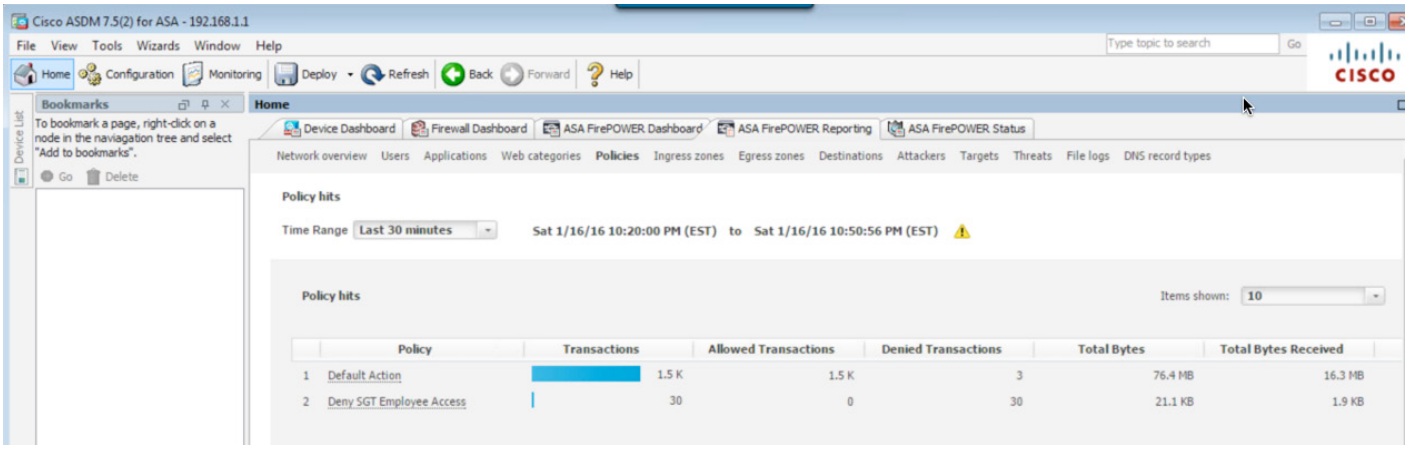
您还可以查看“应用”(Applications) 报告了解详细信息



您也可以查看“策略”(Applications) 报告，



以及“策略命中数”(Policy Hits) 报告



故障排除

ISE pxGrid 节点

系统未显示 pxGrid 发布的节点，而且找不到 pxGrid 连接

- 如果在 ISE 1.3/1.4 环境中使用自签证书，请确保在启用 pxGrid 之前，先将 ISE 自签身份证书导出到 ISE 系统的受信任证书库中。
- 如果使用 CA 签名证书，请确保在启用 pxGrid 之前，已在自定义 pxGrid 模板中加入同时支持服务器身份验证和客户端身份验证的 EKU。
- 如果是在生产环境中部署 pxGrid，请确保使用专用的 ISE pxGrid 节点，并将其公钥/私钥对导入到 PPAN 和 PMNT 节点中。如果部署了主用-备用 pxGrid 节点，请确保将辅助 pxGrid 节点的公钥/私钥对导入到辅助 SPAN 和辅助 SMNT 节点中。
  请仅在能够处于活动状态的 pxGrid 节点上运行应用状态 ISE，以确保 ISE pxGrid 节点为活动节点。
- 关闭 ISE 并重新启动，然后运行 **application stop ise/application start ise** 命令。您也可以从 ISE 节点禁用 pxGrid，停止并重新启用 ISE 服务，然后再启用 pxGrid。
- 请确保下载的证书是 Base 64 编码格式

Firepower 管理中心 6.0

系统集成 ISE 证书测试失败

- 如果您是在使用自签证书的独立 POC 环境中使用 ISE 1.3/1.4，而且您没有将 ISE 设置为主设备，可能会遇到已知的批量下载会话错误，导致 FQDN 解析问题。将 ISE 改为主设备可以解决这个问题。在 ISE 2.0 中不会遇到此问题。
- 如果在 CA 签名的独立环境中使用 ISE，请确保 CSR 请求的目的是“管理”(Admin)，而不是 pxGrid。这对于批量下载活动会话记录是必须的。
- 如果使用 CA 签名证书：
- 如果使用自签证书：
- FMC 6.0、ISE pxGrid 节点和设备都应支持 DNS 解析。

无法从 ISE 查看关联事件

- 请确保 FMC 和 ISE 的时间已经同步。此外，您还应该在 FMC 与所有注册设备之间进行时间同步。

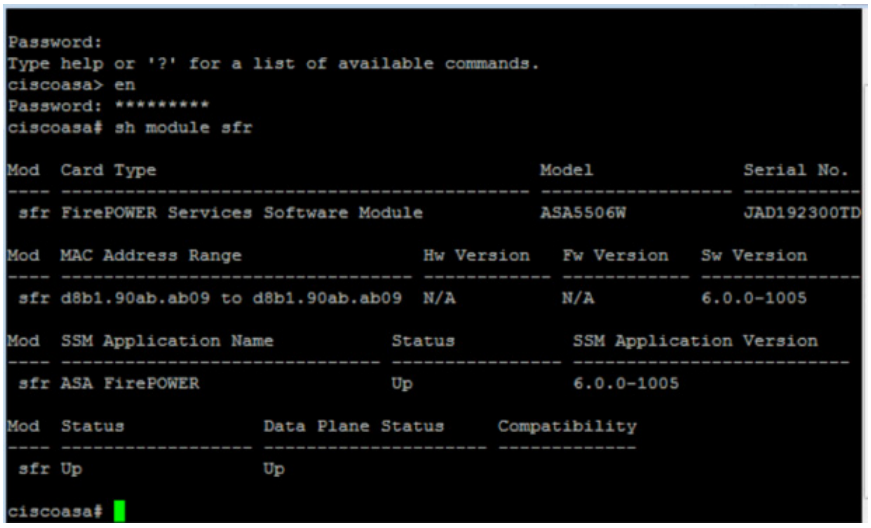
具备 FirePOWER 服务的 ASA

无法在 Firepower 管理中心修改已注册 ASA 设备的参数

- 请确保在 Firepower 管理中心中为所用的 ASA 型号提供了正确的设备许可证。

SFR 一直处于恢复状态

- 重新执行 SFR 安装时，可能需要一段时间。对于本文档中使用的 ASA 5506，这个时间超过了 30 分钟。您可以运行 sh module sfr 命令，来检查 SFR 是否已重新启动



```
Password:
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *********
ciscoasa# sh module sfr

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
 sfr FirePOWER Services Software Module           ASA5506W           JAD192300TD

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
 sfr d8b1.90ab.ab09 to d8b1.90ab.ab09  N/A          N/A          6.0.0-1005

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 sfr ASA FirePOWER                  Up               6.0.0-1005

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
 sfr Up                 Up

ciscoasa#
```

ASA Firepower 报告中无流量信息

- 请配置流向 ASA Firepower 服务的所有流量
- 配置示例如下：

```
ciscoasa# conf t
ciscoasa(config)# sh run policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
```

```
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class class-default
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)#
ciscoasa(config-pmap-c)# sh service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 5531, lock fail 0, drop 0, reset-drop 0, 5-min-

pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,

5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5

-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-

min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 15, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0

pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options _default_ip_options_map, packet 0, lock fail 0, drop 0, reset-

drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default

      Default Queueing      SFR: card status Up, mode fail-open
        packet input 250, packet output 250, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
```

```
ciscoasa(config-pmap-c)

ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 264, packet output 264, drop 0, reset-drop 0
ciscoasa(config-pmap-c)# sh service-policy sfr

Global policy:
  Service-policy: global_policy
    Class-map: class-default
      SFR: card status Up, mode fail-open
        packet input 290, packet output 290, drop 0, reset-drop 0
ciscoasa(config-pmap-c)#
```

解决方案警告

pxGrid 和身份映射服务重新启动

说明：只要从 ISE 部署的信任库导入/删除证书，pxGrid 和身份映射服务就会在 ISE pxGrid 节点上重新启动

提交的缺陷：CSCuv43145

解决方法：无需任何操作，因为将自动重新启动服务，但在服务处于重新启动状态时，将不处理新的隔离事件。

解析计划：ISE Carlsbad 2016 年春季版本

主动 pxGrid 节点未反映在 GUI 中；它反映在 CLI 中

说明：当 pxGrid HA 部署中提供两个 pxGrid 节点时，一个处于主动状态，另一个处于待机状态。识别哪个节点处于主动状态，并且管理员需要在 CLI 中审查 pxGrid 状态。状态在 UI 部署页面中不可视。将在 Carlsbad 中进行此添加。

解决方法：使用 CLI 确定主动/被动状态

解析计划：ISE Carlsbad 2016 年春季版本

参考资料

在分布式 ISE 环境中配置 pxGrid：http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-88-Configuring-pxGrid-in-an-ISE-Distributed-Environment.pdf

如何使用思科 pxGrid 部署证书：配置 CA 签名的 ISE pxGrid 节点和 CA 签名的 pxGrid 客户端：http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-89-CA_signed_pxGridISEnode_CAsigned_pxGridclient.pdf

如何使用思科 pxGrid 部署证书：ISE pxGrid 节点和 pxGrid 客户端的自签名证书：http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-90-Self_signed_pxGridClient_selfsigned_pxGrid.pdf

思科 Firepower 管理中心 6.0 配置指南

http://www.cisco.com/c/en/us/td/docs/security/Firepower/60/configuration/guide/fpmc-config-guide-v60.html