配置与Firepower设备的Active Directory集成

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 步骤1.配置Firepower用户代理进行单点登录
- 步骤2.将Firepower管理中心(FMC)与用户代理集成
- 步骤3.将Firepower与Active Directory集成
  - 第3.1步创建领域
  - 第3.2步添加目录服务器
  - 第3.3步修改领域配置
  - 第3.4步下载用户数据库
- 步骤4.配置身份策略
  - 第4.1步强制网络门户（主动身份验证）
  - 第4.2步单点登录（被动身份验证）
- 步骤5.配置访问控制策略
- 步骤6.部署访问控制策略
- 步骤7.监控用户事件和连接事件

验证和故障排除

- 检验FMC和用户代理之间的连接（被动身份验证）
- 检验FMC和Active Directory之间的连接
- 验证Firepower传感器与终端系统之间的连接（主动身份验证）
- 验证策略配置和策略部署
- 分析事件日志

相关信息

简介

本文档介绍如何配置强制网络门户身份验证（主动身份验证）和单点登录（被动身份验证）。

先决条件

要求

Cisco 建议您了解以下主题：

- Sourcefire Firepower设备
- 虚拟设备模型

- 轻量级目录服务(LDAP)
- Firepower用户代理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Firepower管理中心(FMC)6.0.0版及更高版本
- Firepower传感器6.0.0及更高版本

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

强制网络门户身份验证或主动身份验证会提示登录页面，并且主机需要用户凭证才能访问互联网。

单点登录或被动身份验证为用户提供无缝的身份验证，以便进行网络资源和互联网访问，而无需多次用户凭证出现。单点登录身份验证可通过Firepower用户代理或NTLM浏览器身份验证实现。

注意：对于强制网络门户身份验证，设备必须处于路由模式。

配置

步骤1.配置Firepower用户代理进行单点登录

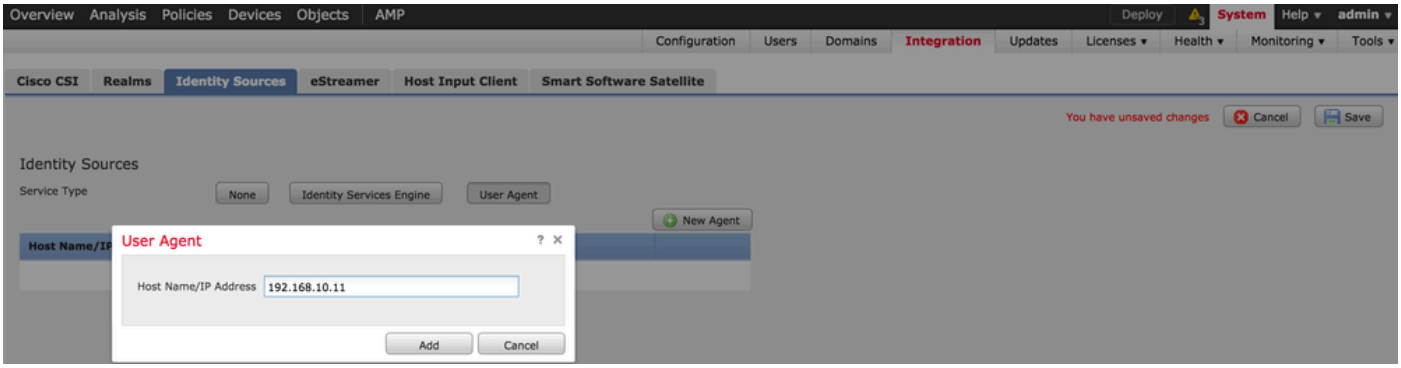
本文解释如何在Windows计算机中配置Firepower用户代理：

[安装和卸载Sourcefire用户代理]

步骤2.将Firepower管理中心(FMC)与用户代理集成

登录到Firepower管理中心，导航到系统>集成>身份源。单击新代理选项。配置用户代理系统的IP地址，然后单击Add按钮。

单击Save按钮保存更改。



步骤3.将Firepower与Active Directory集成

第3.1步创建领域

登录到FMC，导航到System > Integration > Realm。单击Add New Realm选项。

名称和说明：提供名称/说明以唯一标识领域。

类型：AD

AD主域：Active Directory的域名

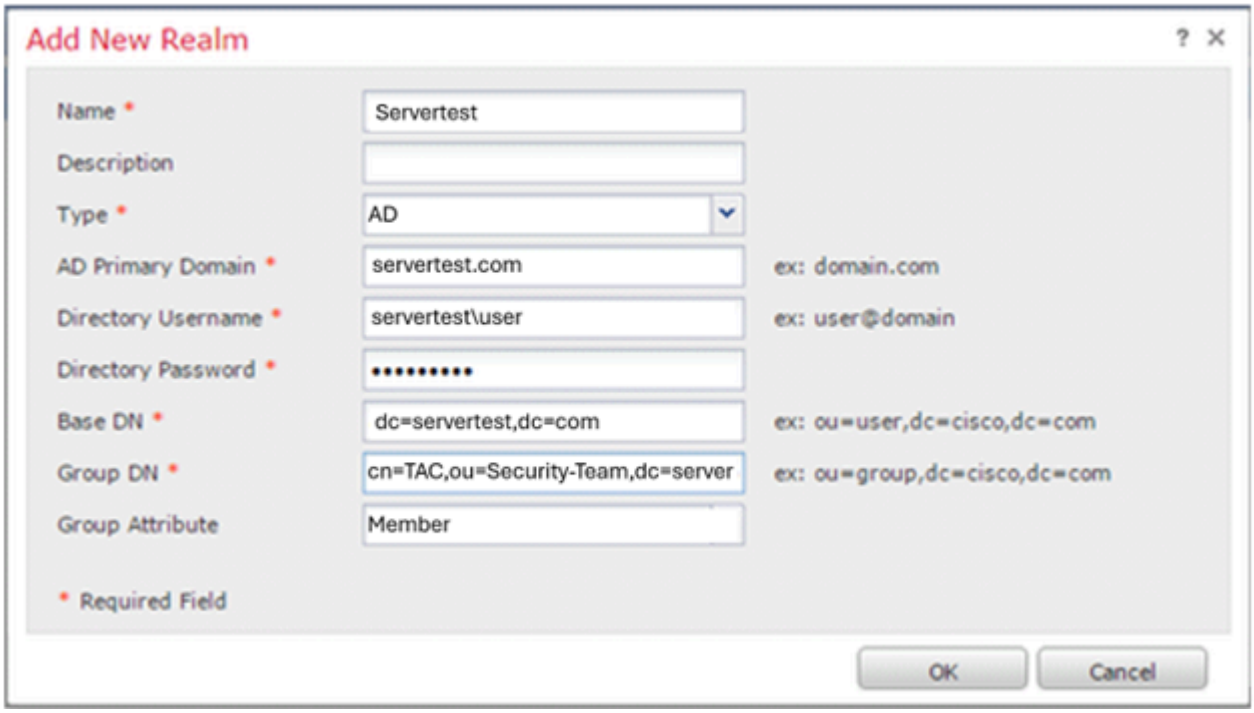
目录用户名: <username>

目录密码:<password>

基本DN:系统从LDAP数据库中开始搜索的域或特定OU DN

组DN:组DN

组属性：成员



本文可帮助您确定基本DN和组DN值。

[确定Active Directory LDAP对象属性]

第3.2步添加目录服务器

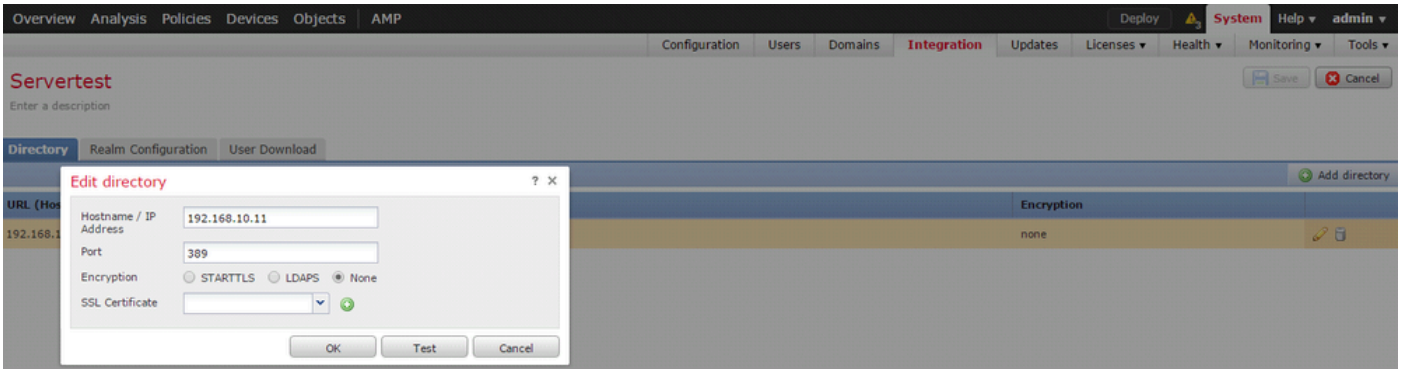
单击Add按钮以导航到下一步，然后点击Add directory选项。

主机名/IP地址：配置AD服务器的IP地址/主机名。

端口： 389（Active Directory LDAP端口号）

加密/SSL证书:(可选)要加密FMC和AD服务器之间的连接，请参阅

文章：[验证通过SSL/TLS进行Microsoft AD身份验证的FireSIGHT系统上的身份验证对象。]



单击Test按钮以验证FMC是否能够连接到AD服务器。

第3.3步修改领域配置

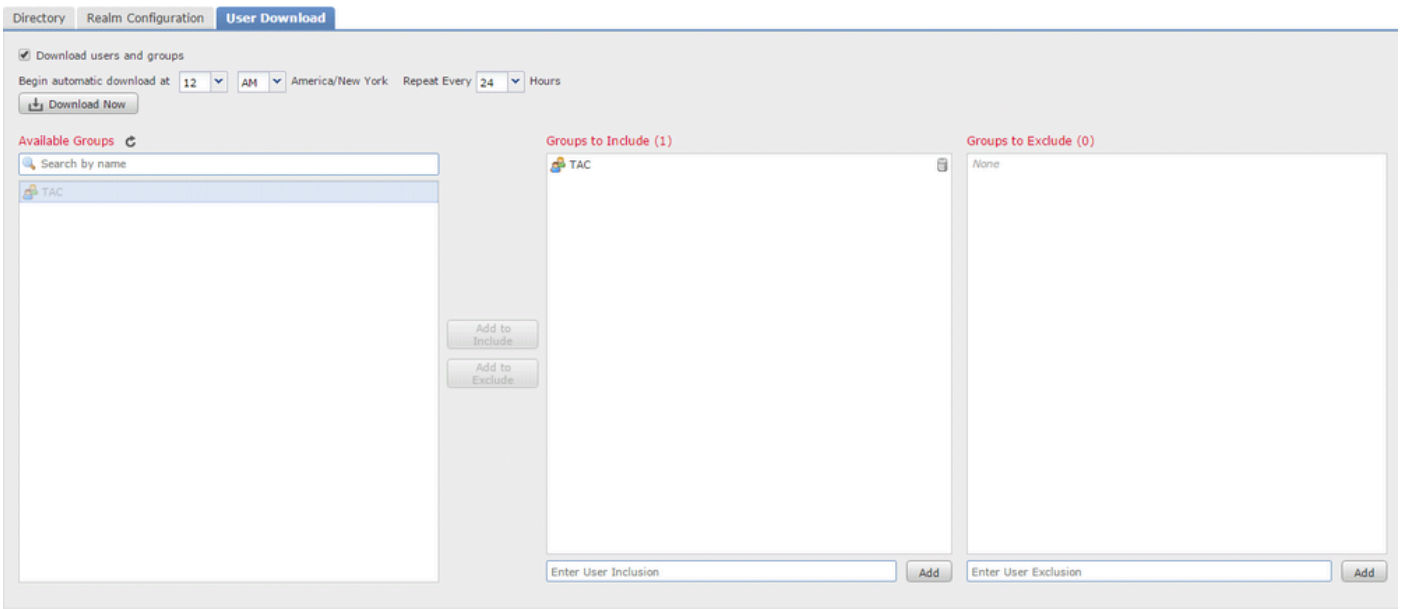
导航到领域配置以验证AD服务器的集成配置，您可以修改AD配置。

第3.4步下载用户数据库

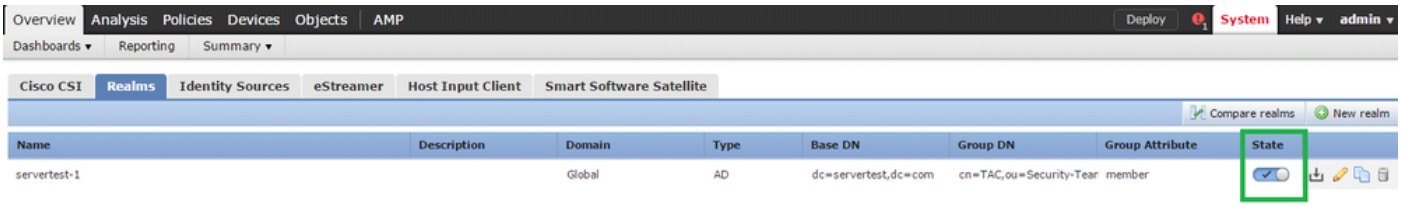
导航到User Download选项，从AD服务器获取用户数据库。

启用此复选框可下载下载用户和组，并定义有关FMC联系AD下载用户数据库频率的时间间隔。

选择组，并将其放入要为其配置身份验证的Include选项中。



如图所示，启用AD状态：



步骤4.配置身份策略

身份策略执行用户身份验证。如果用户未进行身份验证，则拒绝访问网络资源。这会对组织的网络和资源实施基于角色的访问控制(RBAC)。

第4.1步强制网络门户（主动身份验证）

主动身份验证要求在浏览器中输入用户名/密码，以识别用户身份以允许任何连接。 浏览器使用身份验证页面对用户进行身份验证，或使用NTLM身份验证进行静默身份验证。 NTLM使用Web浏览器来发送和接收身份验证信息。主动身份验证使用各种类型来验证用户的身份。身份验证的不同类型包括：

1. HTTP基本信息：在此方法中，浏览器会提示输入用户凭证。
2. NTLM: NTLM使用Windows工作站凭证，并通过Web浏览器与Active Directory进行协商。您需要在浏览器中启用NTLM身份验证。用户身份验证以透明方式进行，不提示输入凭证。它为用户提供单点登录体验。
3. HTTP协商：在此类型中，系统尝试使用NTLM进行身份验证。如果失败，则传感器使用HTTP Basic身份验证类型作为回退方法，并提示对话框提供用户凭证。
4. “HTTP响应”页：这类似于HTTP基本类型，但是，在此提示用户将身份验证填入可自定义的HTML表单。

每个浏览器都有启用NTLM身份验证的特定方法，因此它们遵循浏览器指南以启用NTLM身份验证。

要安全地与路由的传感器共享凭证，您需要在身份策略中安装自签名服务器证书或公开签名的服务器证书。

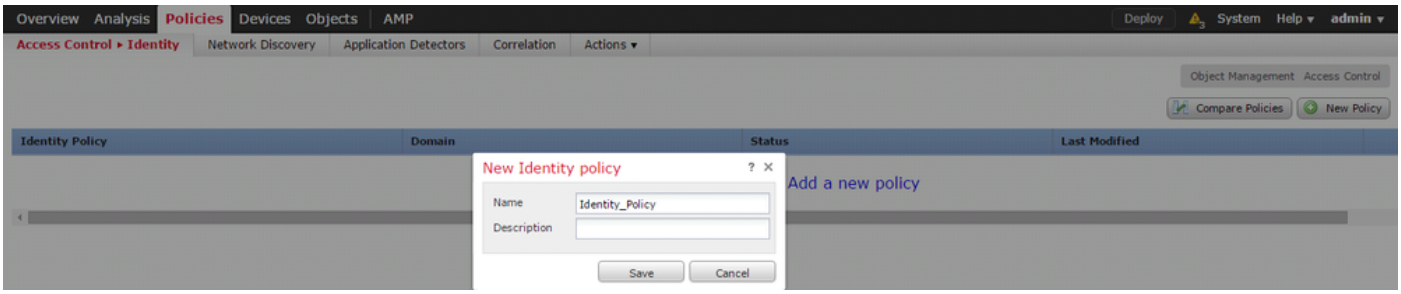
```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

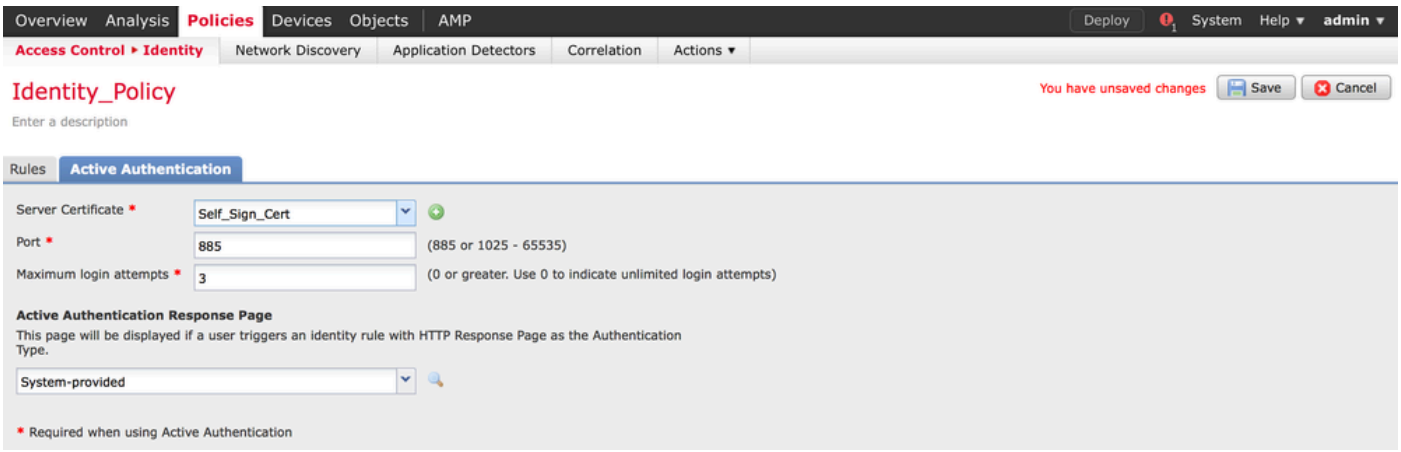
Step 2.   Generate Certificate Signing Request (CSR)
               openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
               openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

导航到策略>访问控制>身份。单击Add Policy，为策略指定名称并保存它。

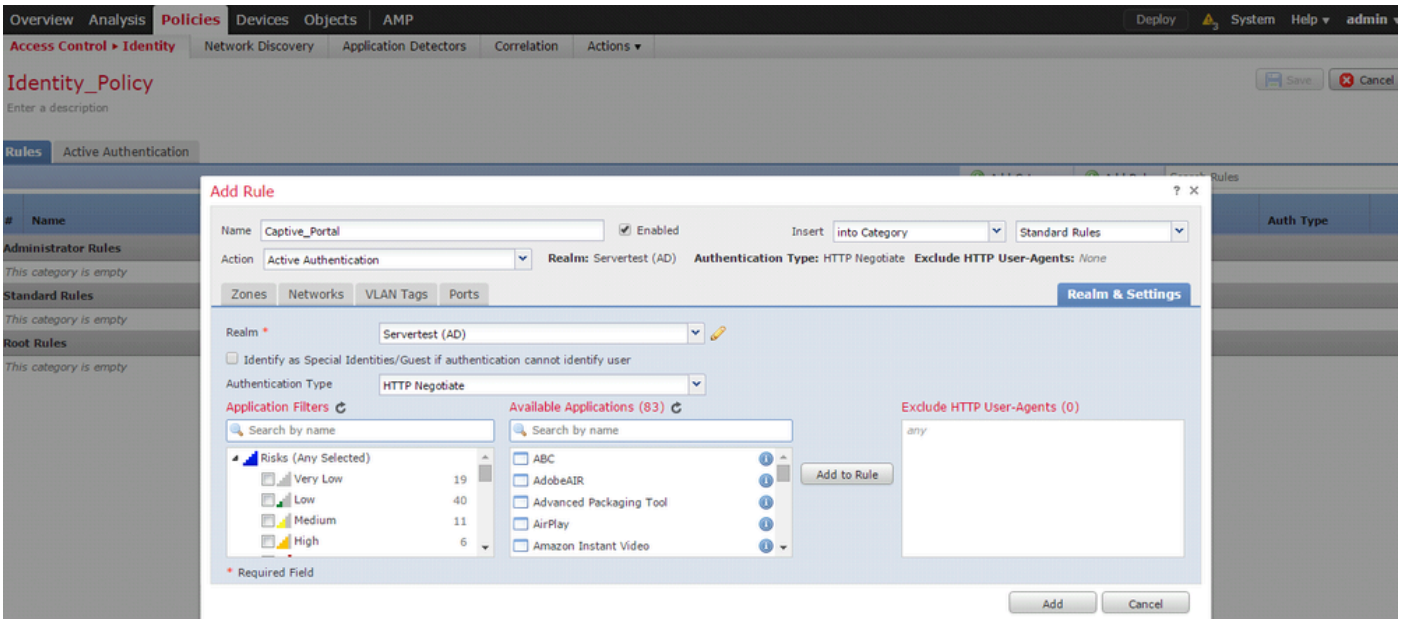


导航到Active Authentication选项卡，在Server Certificate选项中，点击图标(+)，然后上传在上一步使用openSSL生成的证书和私有密钥。



现在，单击Add rule按钮，为规则指定名称，然后选择作为Active Authentication的操作。定义要为其启用用户身份验证的源/目标区域、源/目标网络。

选择在上一步中配置的Realm以及最适合您的环境的身份验证类型。



强制网络门户的ASA配置

对于ASA Firepower模块，请在ASA上配置这些命令以配置强制网络门户。

```
ASA(config)# captive-portal global port 1055
```

确保在Identity Policy Active Authentication选项卡的port选项中配置服务器端口TCP 1055。

要验证活动规则及其命中计数，请运行命令：

```
ASA# show asp table classify domain captive-portal
```

注意： captive portal命令在ASA 9.5(2)版及更高版本中可用。

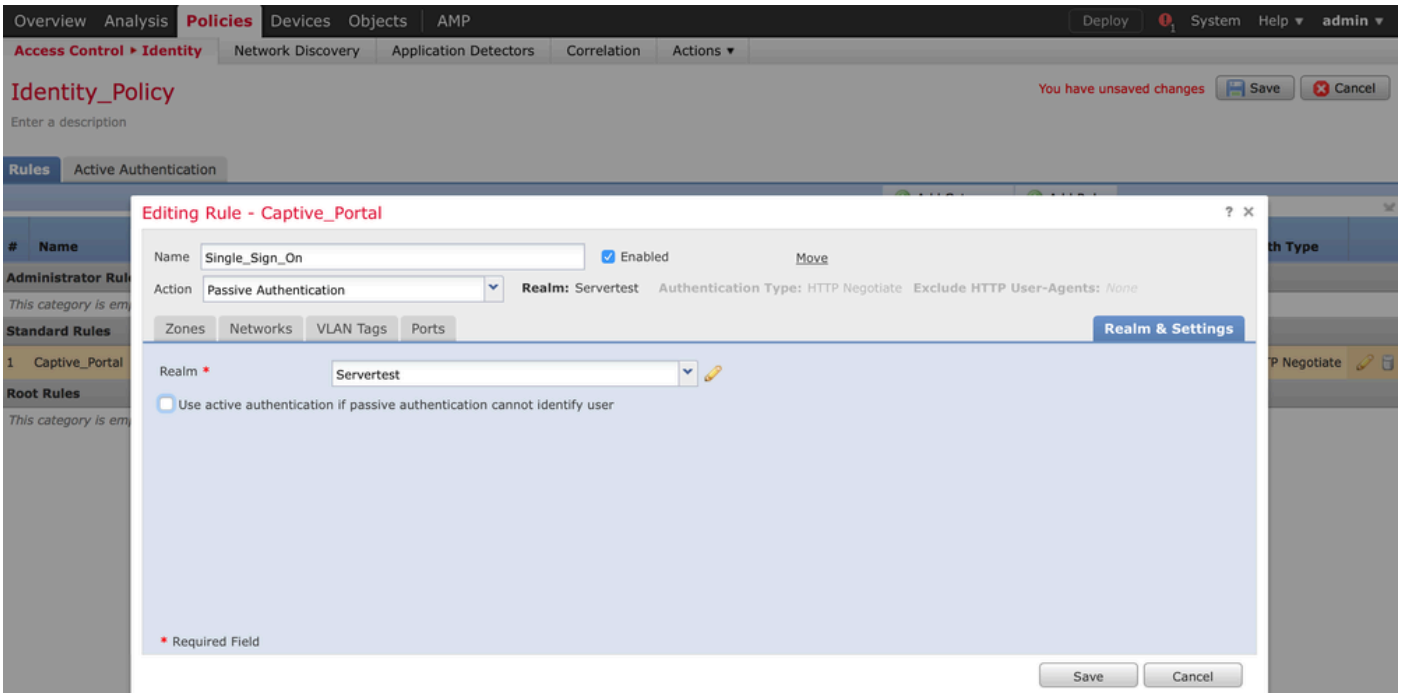
第4.2步单点登录（被动身份验证）

在被动身份验证中，当域用户登录且能够对AD进行身份验证时，Firepower用户代理从AD的安全日志轮询用户 — IP映射详细信息，并与Firepower管理中心(FMC)共享此信息。FMC将这些详细信息发送到传感器以实施访问控制。

单击Add rule按钮，为规则指定名称，然后选择Action作为Passive Authentication。定义要为其启用用户身份验证的源/目标区域、源/目标网络。

选择您在上一步中配置的领域以及最适合您环境的身份验证类型，如下图所示。

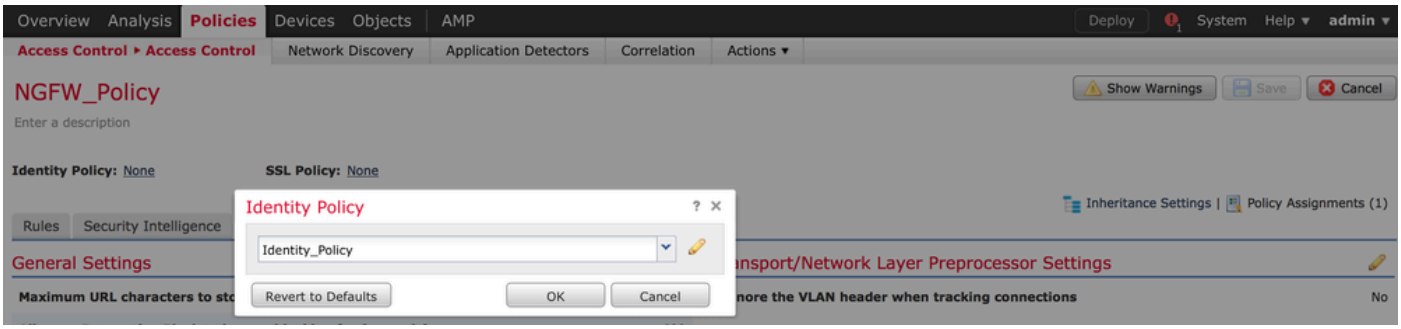
如果被动身份验证无法识别用户身份，您可以在此处选择回退方法作为主动身份验证。



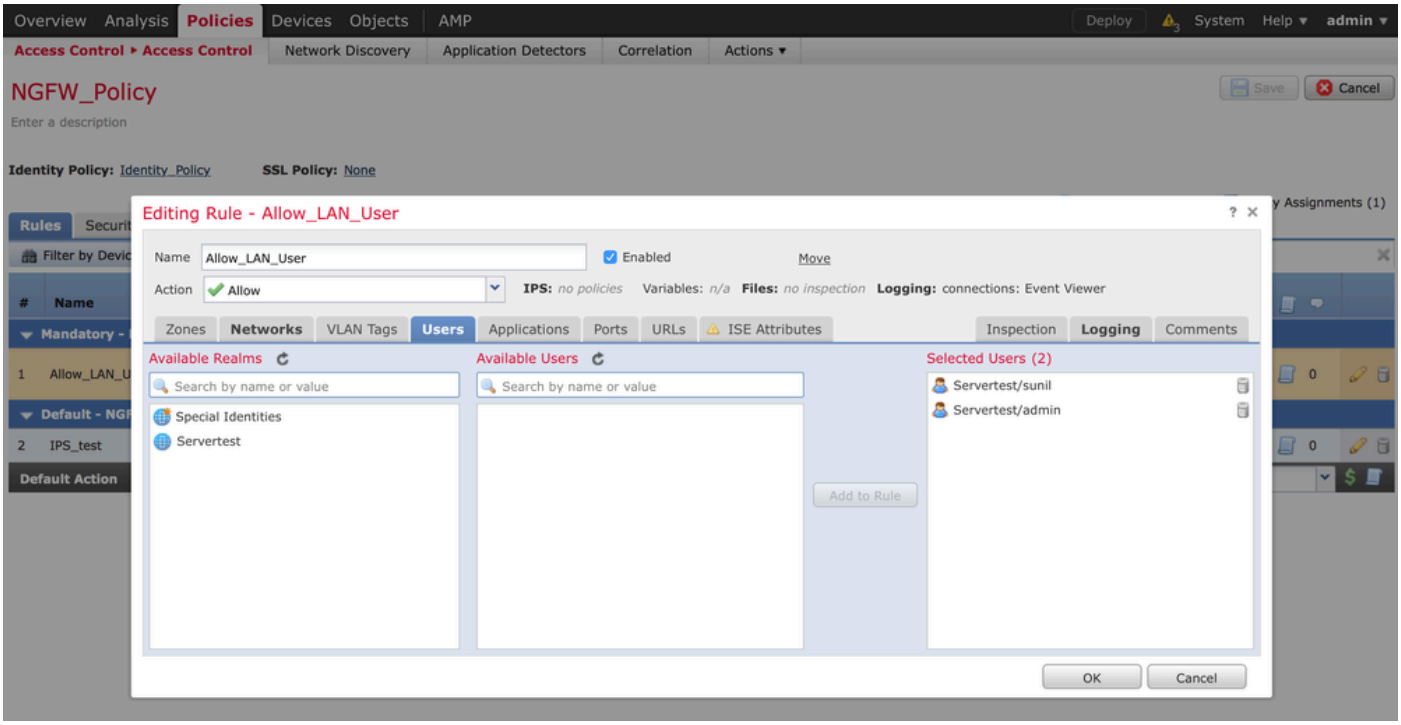
步骤5.配置访问控制策略

导航到Policies > Access Control > Create/Edit a Policy。

单击Identity Policy（左侧上角），选择您在上一步中配置的Identify Policy，然后单击OK按钮，如下图所示。

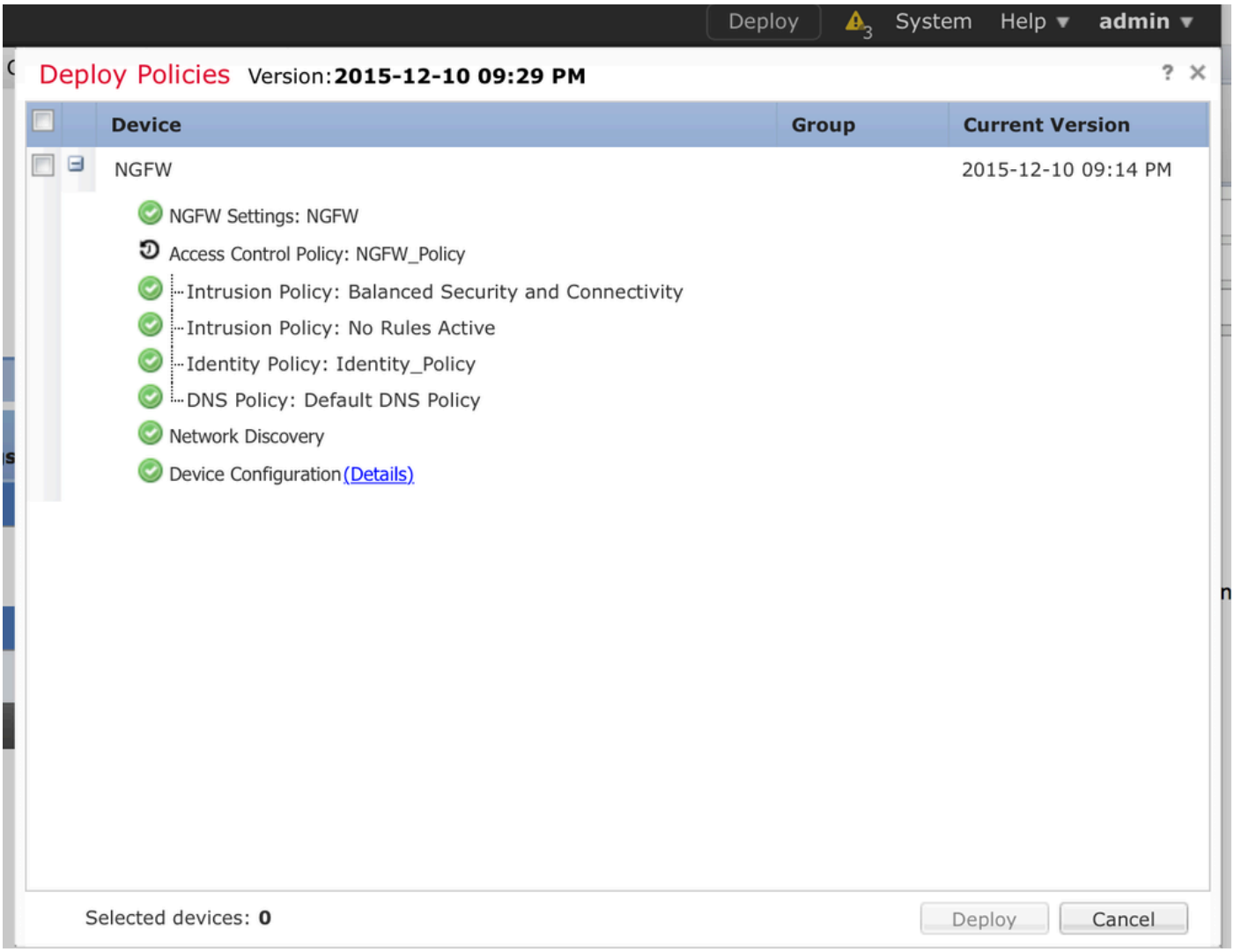


单击Add rule按钮添加新规则。导航到Users并选择对其实施访问控制规则的用户，如下图所示。单击OK，然后单击Save以保存更改。



步骤6.部署访问控制策略

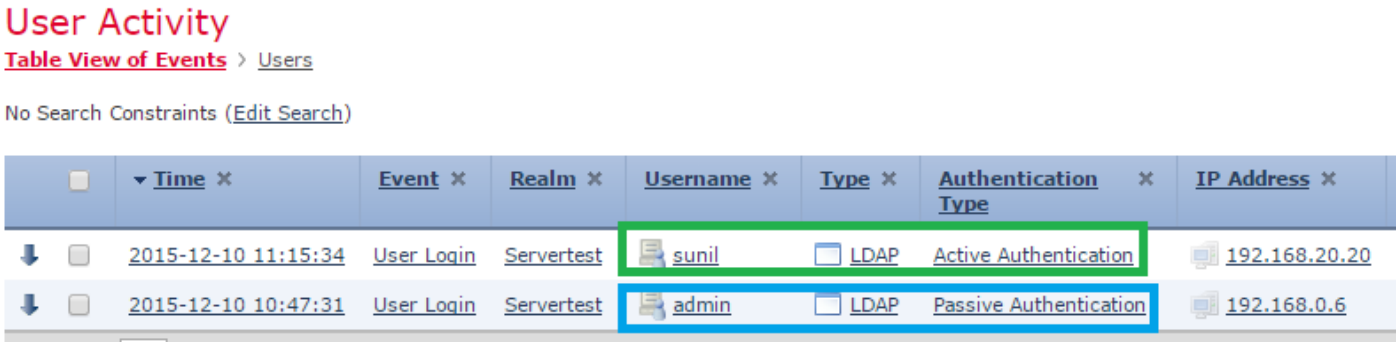
导航到部署选项。选择Device，然后单击Deploy选项将配置更改推送到传感器。从消息中心图标（部署和系统选项之间的图标）选项监控策略的部署，并确保策略必须成功应用，如本图所示。



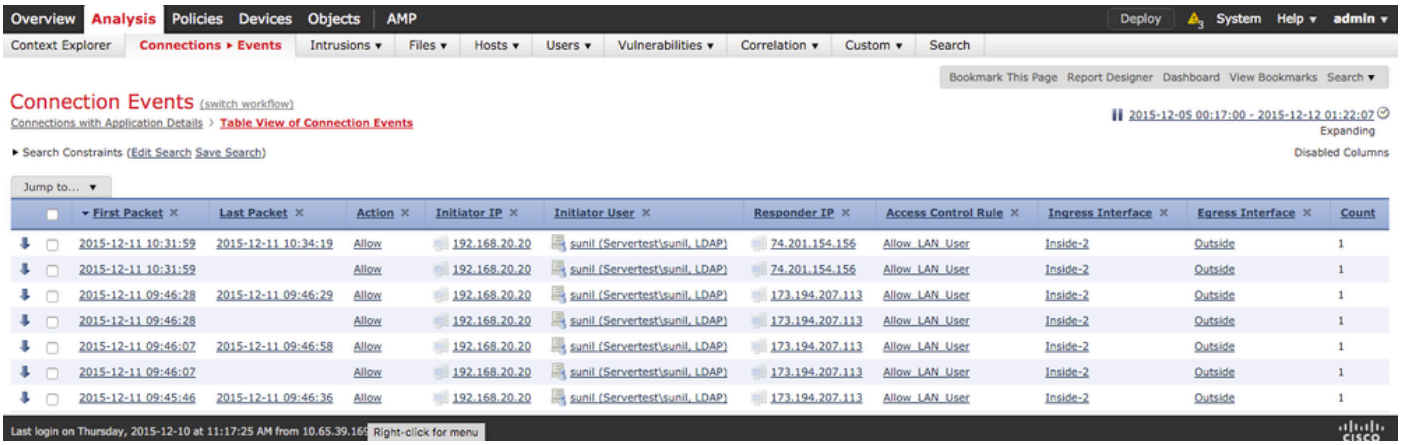
步骤7.监控用户事件和连接事件

当前，活动用户会话在分析>用户>用户部分中可用。

用户活动监控有助于确定哪个用户与哪个IP地址相关联，以及系统如何通过主动或被动身份验证检测用户：分析(Analysis)>用户(Users)>用户活动(User Activity)。



导航到分析>连接>事件以监控用户使用的流量类型。



验证与故障排除

导航到**分析>用户**，以验证与流量相关的用户身份验证/身份验证类型/用户 — IP映射/访问规则。

检验FMC和用户代理之间的连接（被动身份验证）

Firepower管理中心(FMC)使用TCP端口3306，以便从用户代理接收用户活动日志数据。

要验证FMC服务状态，请在FMC中使用此命令。

```
admin@firepower:~$ netstat -tan | grep 3306
```

在FMC上运行数据包捕获以验证与用户代理的连接。

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

导航到分析>用户>用户活动，以验证FMC是否从用户代理接收用户登录详细信息。

检验FMC和Active Directory之间的连接

FMC使用TCP端口389从检索用户数据库 Active Directory.

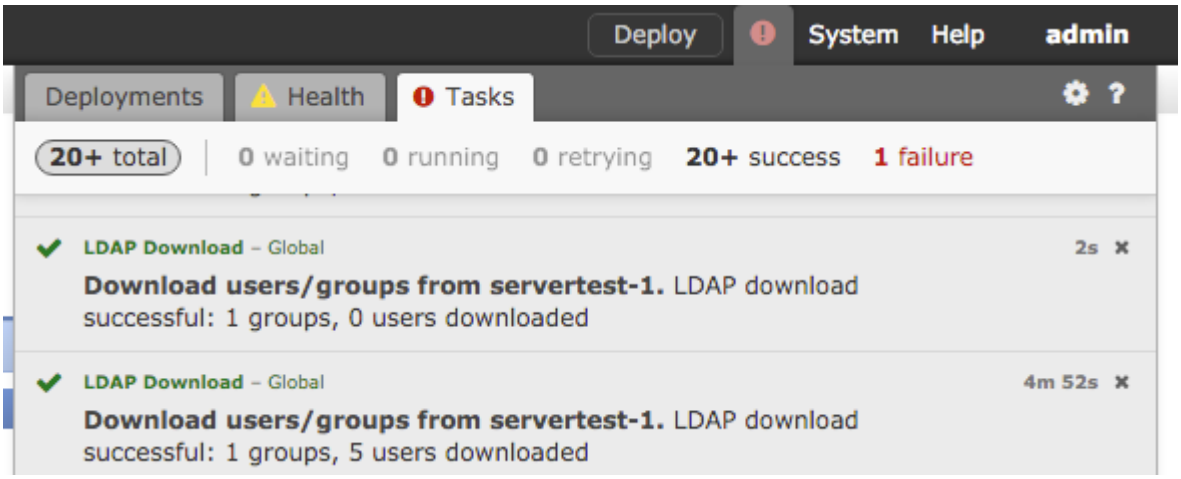
在FMC上运行数据包捕获以验证与Active Directory的连接。

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

确保FMC领域配置中使用的用户凭据具有足够的权限来获取AD用户数据库。

验证FMC领域配置，确保下载了用户/组并且正确配置了用户会话超时。

导航到消息中心>任务，并确保任务用户/组下载成功完成，如此图所示。



验证Firepower传感器与终端系统之间的连接（主动身份验证）

对于主动身份验证，请确保在FMC身份策略中正确配置证书和端口。默认情况下，Firepower传感器在TCP端口885上侦听活动身份验证。

验证策略配置和策略部署

确保在身份策略中正确配置领域、身份验证类型、用户代理和操作字段。

确保身份策略与访问控制策略正确关联。

导航到消息中心>任务，并确保策略部署成功完成。

分析事件日志

连接和“用户活动”事件可用于诊断用户登录是否成功。这些事件

还可以验证在流上应用了哪个访问控制规则。

导航到分析>用户以检查用户事件日志。

导航到分析>连接事件以检查连接事件。

相关信息

- 技术支持和文档

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。