思科 Firepower 下一代防火墙 6.2 实验 v1

最后更新日期：2017 年 10 月 31 日

关于本演示

本预配置演示指南包括以下内容：

注意：建议您**不要**尝试在一个会话中完成所有练习。这些练习总共可能需要大约 6 个小时。在决定要尝试演示哪些场景时，请考虑以下依赖关系。

- 所有场景都依赖于场景 1 和场景 2。必须按顺序完成这两个场景。
- 场景 3 至 6 涵盖 Ra VPN 的详情。但是，完成场景 3 就足以获得对 RA VPN 配置的基本了解。
- 场景 13 使用场景 10 中的静态 NAT 配置。

要求

下表列出了本预配置演示的要求。

表 1. 要求

必需	可选
• 笔记本电脑	• 思科 AnyConnect®

关于此解决方案

当今世界正在经历全数字化带来的颠覆，随着消费者、企业和政府机构纷纷利用全数字化来推动创新，这将引发规模空前的互联。然而，我们的互联程度越高，给网络犯罪分子带来的可乘之机也越多。企业要在当今环境中高效运作，就必须在当前瞬息万变的威胁形势下，将安全工作的重点放在阻止高级威胁上。

为此，IT 团队需要东拼西凑地使用很多孤立的单点产品来管理安全性，以传统的下一代防火墙 (NGFW) 为首，这些单点产品是重点针对应用设计的，而在威胁防范上只能做到尽力而为。因此，这些传统的 NGFW 无法为企业提供应对当今现代威胁所需的情景信息、自动化功能和确定优先级功能。面对现今老练狡猾的黑客和高度复杂的恶意软件，您要想比对手领先一步，就需要一款完全集成的安全解决方案，借此获得全面的网络可视性、威胁情报和追溯性安全技术，从而能够快速应对各种攻击。

思科 Firepower 4100 系列下一代防火墙 (NGFW) 是业界首款完全集成的专注于威胁防御的下一代防火墙，可以解决上述问题。

思科 Firepower NGFW 采用全新设计，旨在增强组织的安全性。Firepower NGFW 还提供完全集成的安全功能，利用单一界面减轻管理负担，从而控制传统 NGFW 产生的成本和复杂性。通常，公司管理的一大堆安全技术已然杂乱无章，我们不会忙中添乱，增加更多设备或控制台。

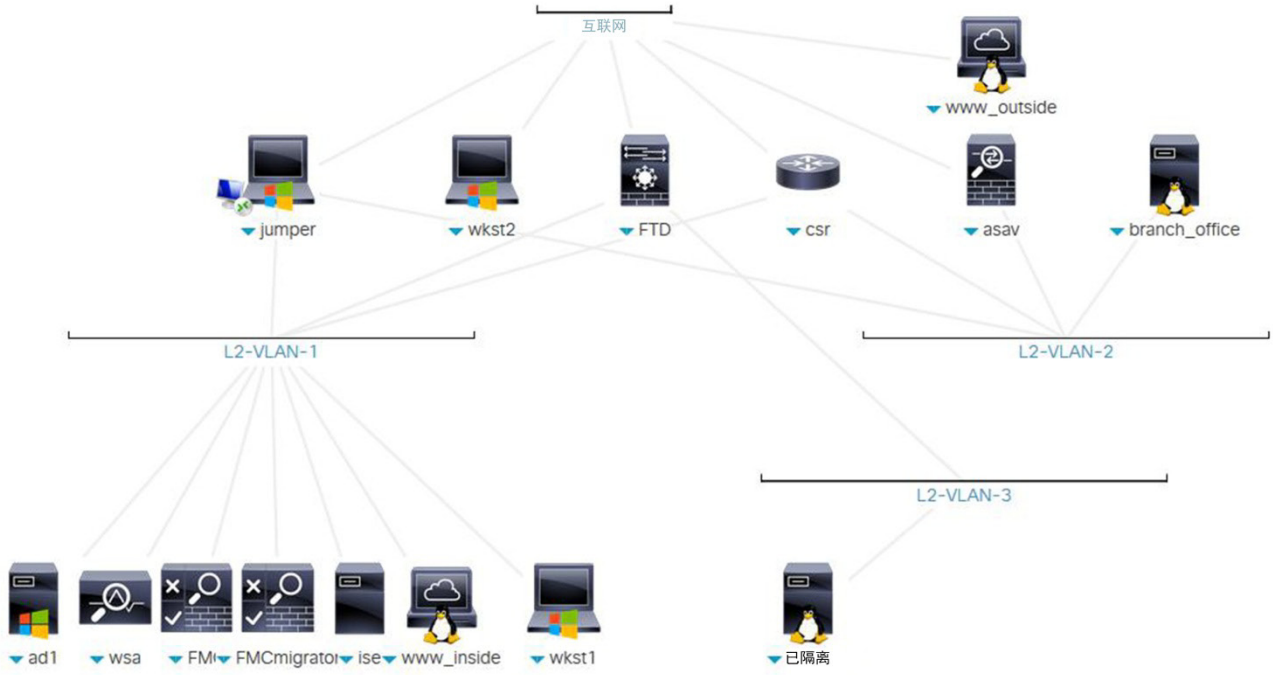
这使得思科 Firepower NGFW 在演进过程中，能够专注于帮助企业实时阻止现代威胁，确定其优先级，把握相关情况并实现自动化响应。Firepower NGFW 在注重威胁方面独树一帜，凭借全面的网络可视性、一流的威胁情报和高效的威胁防范，可以有效地应对已知和未知的威胁。Firepower NGFW 还能实现追溯性安全，通过高级恶意软件防护及时回溯，快速发现可能已穿越防御的复杂攻击，并且执行补救措施。这使思科客户的检测时间 (TTD) 相比行业平均水平显著缩短。

思科 Firepower NGFW 还利用从网络外延至终端的高级威胁防护来解决客户面临的挑战。同时，我们已实现面向终端的 AMP、AMP Threat Grid 和思科身份服务引擎 (ISE) 与该平台的无缝集成。这使思科能够将 Firepower NGFW 的功能和可视性扩展至网络，并且直接延伸到终端。

拓扑

本部分内容包括用于说明解决方案脚本化场景和功能的预配置用户和组件。大多数组件完全可以使用预定义的管理用户帐户进行配置。通过点击活动会话的**拓扑**菜单中的组件图标，您可以查看用于访问组件的 IP 地址和用户帐户凭证，在需要用到 IP 地址和用户帐户凭证的场景步骤中也同样如此。

图 1. dCloud 拓扑



开始演示

演示前的准备

思科 dCloud 强烈建议您事先使用活动会话执行本文档中的任务，然后再给现场观众演示。这样您将熟悉文档和内容的结构。

遵循本指南后，有必要安排一个新会话，以将环境重置为其原始配置。

细致的准备对于一场成功的演示至关重要。

按照步骤安排内容会话并配置演示环境。

1. 启动 dCloud 会话。[查看具体操作]

注意：激活会话可能需要 10 分钟的时间。

2. 使用思科 dCloud 远程桌面客户端连接到工作站 [查看具体操作]。

注意：您还可以使用**思科 AnyConnect VPN** [查看具体操作] **和您的笔记本电脑上的本地 RDP 客户端** [查看具体操作] 连接到工作站

Jumper：**198.18.133.50**，用户名：**administrator**，密码：**C1sco12345**

场景 1：使用 REST API 进行设备部署

本实验的目标是执行简单的 NGFW 部署。其中大部分操作都将使用 REST API python 脚本来完成。但是，您必须先执行一些预备步骤。此外，REST API 尚不支持路由配置，因此您需要手动执行此操作。

步骤

将 NGFW 配置为由 FMC 进行管理

1. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为 **NGFW** 的预配置会话。使用用户名 **admin** 和密码 **C1sco12345** 登录。

注意：如果您在键入特殊字符时遇到问题，请打开 Jump Desktop 上名为 *Strings to cut and paste.txt* 的文件。

2. 键入命令 **configure manager add fmc.dcloud.local C1sco12345**。
3. 阅读警告。
4. 系统询问您是否要继续时，请键入 **yes** 作为回答。请勿键入 **y**。如果键入 **y** 代替 **yes**，系统会将该命令默认为 **no**。

注意：NGFW 在安装时已启用内部管理器（Firepower 设备管理器或 FDM）。这是默认配置。这就是您会收到此警告的原因。我们在本课程中没有内部管理实验练习，但可以提供此类练习。不过请注意，在不删除 NGFW 配置的情况下，无法在 FMC 和 FDM 之间进行切换。

5. 使此 PuTTY 会话保持打开状态。在整个实验中，您将使用此会话。

在 FMC 上启用智能许可证

对于 NGFW，必须使用智能许可。对于本实验，您将使用内置的 90 天评估许可证。

注意：对于本课程，我们使用的是自定义软件。在生产代码中，不能使用评估许可证部署 RA VPN。

1. 打开 Firefox，然后在 Jump Desktop 上打开 Firepower 管理中心（标识为 FMC）。系统将预填充登录名和密码。
2. 点击**登录**。
3. 导航至**系统 > 许可证 > 智能许可证**。
4. 点击**评估模式**，然后在出现提示时点击**是**。

运行 REST API 脚本以注册和配置 NGFW

为演示 REST API，您需要运行用于执行以下操作的 Python 脚本。

1. 创建访问控制策略。
2. 将 NGFW 注册到 FMC
3. 配置 NGFW 接口。

注意：此脚本仅用于培训目的，并未充分完善。如果您希望检查此脚本，请转至 **`/usr/local/bin`**。它被命名为 **`register_config.py`**，并且使用 **`connect.py`** 生成的 Python 模块。命令 **`runapiscript`** 是指向 **`register_config.py`** 的符号链接。本指南的附录 B 中也包含这些脚本。

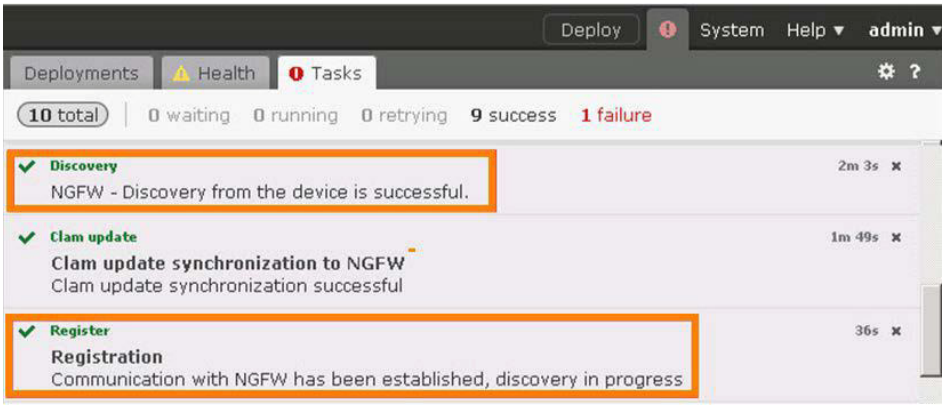
4. 从 Jump Desktop 启动 PuTTY。双击**内部 Linux 服务器**会话。使用用户名 **`root`** 和密码 **`C1sco12345`** 登录。
5. 在内部 Linux 服务器 CLI 上，运行 **`runapiscript`**。
    a. 系统询问**是否注册受管设备？[y/n]** 时，输入 **y** 并按 **<Return>**。
    b. 系统提示**输入访问控制策略名称**时，输入合理的名称，例如 **`NGFW Access Control Policy`**。
    c. 等待确认消息。
    d. 在 FMC UI 中，确认设备发现已完成，然后按 **y** 继续，或者按 **n** 退出。[y/n]
    e. 接着执行下一步，然后再继续执行脚本。

注意：如果您未等待发现完成，则会收到错误。在此情况下，请等待发现完成，然后再次运行脚本，但是此次在系统询问您是否要注册设备时，请输入 **n**。

6. 在 FMC 上，点击*部署*按钮右侧的图标，然后选择*任务*选项卡。
    a. 请稍等。可能需要片刻才会启动任务。

注意：如果超过一分钟而未启动任何任务，请查看是否启用了演示智能许可证。如果未启用，则应将其启用，然后再次运行 **`runapiscript`** 脚本。请确保对访问控制策略使用不同的名称，或者删除脚本所创建的策略。

    b. 等待发现任务完成。不要担心失败的任务。重要的是注册和发现必须成功完成。



7. 在内部 Linux 服务器 CLI 上，继续运行 **`runapiscript`** 脚本。

    a. 输入 **y** 并按 **<Return>**。

    b. 系统询问**是否想要配置设备接口？[y/n]** 时，输入 **y** 并按 **<Return>**。等待脚本完成。

    c. 使此 PuTTY 会话保持打开状态。在整个实验中，您将使用此会话。

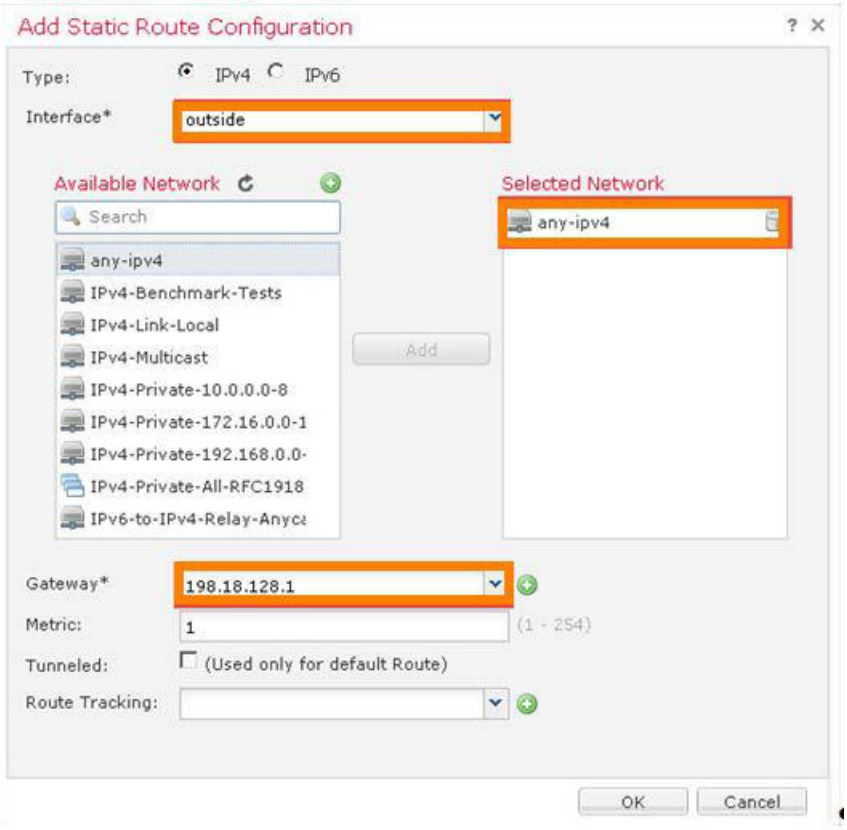
配置默认路由

1. 在 FMC 中，导航至**设备 > 设备管理**。点击铅笔图标以编辑设备设置。
2. 应当选择“接口”选项卡。确认 REST API 脚本是否配置了 NGFW 的内部和外部接口。
3. 选择“路由”选项卡。

    a. 选择**静态路由**，然后点击**添加路由**按钮。

    b. 在外部接口上将默认路由设置为 **`198.18.128.1`**，如下图中所示。

    c. 点击**确定**。



4. 点击**保存**以保存路由配置。

注意：要节省时间，请勿部署路由配置。此外，为节省时间，**`runapiscript`** 脚本不包含接口配置的部署。您将在下一个实验练习中执行更多配置步骤，然后一起部署所有配置更改。

场景 2：基本配置

此练习包含以下任务：

- 创建练习所需的对象
- 修改访问控制策略
- 创建 NAT 策略
- 修改网络发现策略
- 部署配置更改
- 测试 NGFW 配置
- 允许出站连接，并阻止其他连接尝试
- 在这些出站连接上，执行文件类型和恶意软件阻止
- 在这些出站连接上，提供入侵防御

步骤

创建练习所需的对象

1. 导航至**对象 > 对象管理**。
    a. 点击**添加网络 > 添加对象**。
    b. 在**名称**字段，输入 **Lab_Networks**。
    c. 输入 `198.18.0.0/15`。这包括实验 pod 中使用的所有 IP 地址。
    d. 点击**保存**。
2. 从左侧导航面板中选择**接口**。
    a. 点击**添加 > 安全区域**。

注意：有两种类型的接口对象：安全区域和接口组。关键区别在于接口组可以重叠。在访问控制策略规则中只能使用安全区域。

    b. 在**名称**字段，输入 **InZone**。从**接口类型**下拉菜单中选择**路由**。
    c. 选择内部接口。点击**添加**，然后点击**保存**。
    d. 点击**添加 > 安全区域**。
    e. 在“名称”字段，输入 **OutZone**。从“接口类型”下拉菜单中选择**路由**。
    f. 选择外部接口。点击**添加**，然后点击**保存**。

修改访问控制策略

1. 导航至**策略 > 访问控制 > 访问控制**。请注意，REST API 脚本已创建一条访问控制策略。
2. 点击该访问控制策略右侧的**铅笔图标**即可进行编辑。
3. 点击**添加规则**。
    a. 在“名称”字段，输入**允许出站连接**。
    b. 从**插入**下拉列表中选择**插入到默认规则集**。

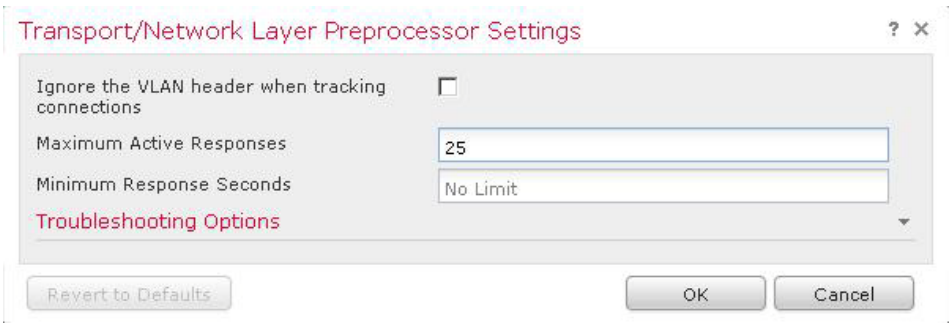
注意：在策略中，规则划分为各个规则集。系统预定义了以下两个规则集：
• 强制性规则集，其中的规则优先于子策略的规则
• 默认规则集，其中的规则在子策略的规则之后进行评估

在此练习中，您不需要创建子策略，但是需要使用默认规则集，以便确保最后评估此规则。

    c. 系统应已选择**区域**选项卡。
        i. 选择 **InZone**，然后点击**添加到源**。
        ii. 选择 **OutZone**，然后点击**添加到目的地**。
    d. 选择**检查**选项卡。
        i. 从**入侵策略**下拉列表中选择**演示入侵策略**。
        ii. 从**文件策略**下拉列表中选择**演示文件策略**。

注意：为节省时间，演示入侵策略和文件策略已预先配置。有关如何创建这些策略的说明，请参阅**附录 A**。

    e. 点击**添加**以添加规则。
4. 选择 **HTTP 响应**选项卡。
5. 从**阻止响应页面**下拉列表中，选择**系统提供**。
6. 选择**高级**选项卡。
    a. 点击**铅笔图标**，编辑**传输/网络层预处理器设置**。
    b. 在**最大活动响应数**文本字段中，输入 **25**。
    c. 点击**确定**。



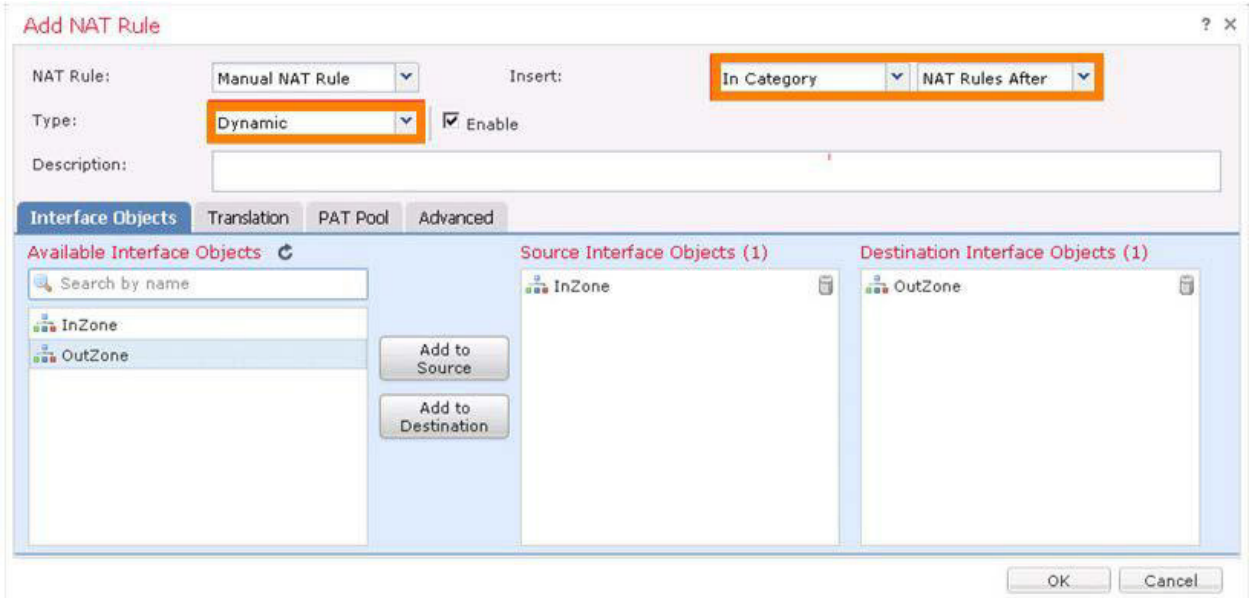
注意：将“最大活动响应数”设置为大于 0 的值可使丢包的规则发送 TCP 重置来关闭连接。通常，系统向客户端和服务器均发送 TCP 重置。完成以上配置后，如果系统发现来自此连接的其他流量，最多可以启动 25 个活动响应（TCP 重置）。

在生产部署中，可能最好是将此项设置为默认值。这样，系统就不会发送重置，并且恶意系统将无法知悉是否已被检测到。但是对于测试和演示，通常最好是在数据包匹配丢弃规则时发送重置。

7. 点击**保存**以保存对访问控制策略的更改。

创建 NAT 策略

1. 导航至**设备 > NAT**。
2. 点击**新建策略**按钮，然后选择**威胁防御 NAT**。
    a. 在“名称”字段，输入**默认 PAT**。
    b. 选择 **NGFW**。点击**添加到策略**，然后点击**保存**。
    c. 等待该策略打开以进行编辑。
3. 点击**添加规则**。
    a. 从“插入”下拉列表中选择**类别中**和 **NAT 规则后**。这将确保在自动 NAT（对象 NAT）规则后评估此规则。
    b. 从**类型**下拉列表中选择**动态**。
    c. 您将进入**接口对象**选项卡。选择 **InZone**，然后点击**添加到源**。
    d. 选择 **OutZone**，然后点击**添加到目的地**。

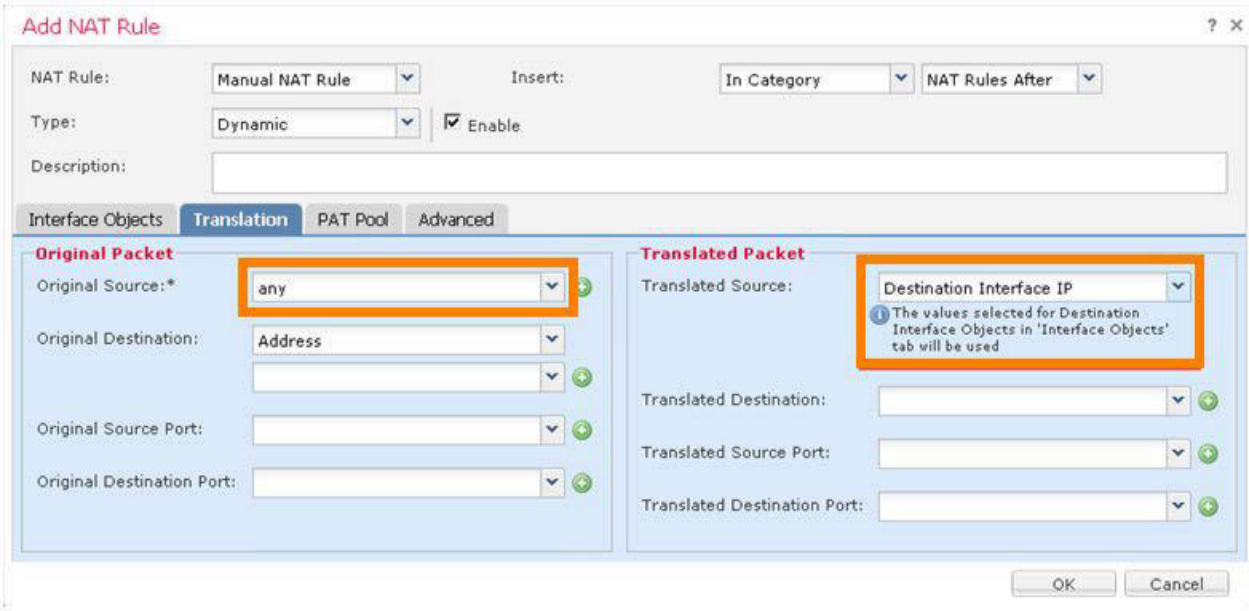


e. 选择**转换**选项卡。

f. 从**原始源**下拉列表中选择任意一项。

g. 从“已转换的源”下拉列表中选择**目的接口 IP**。

h. 点击**确定**以保存 NAT 规则。



4. 点击**保存**以保存 NAT 策略。

修改网络发现策略

默认网络发现策略配置为发现所有内部和外部应用。我们将需要添加主机和用户发现。在生产环境中，这可能会超出 FMC Firepower 主机许可证的范围。因此，最佳做法是修改策略。

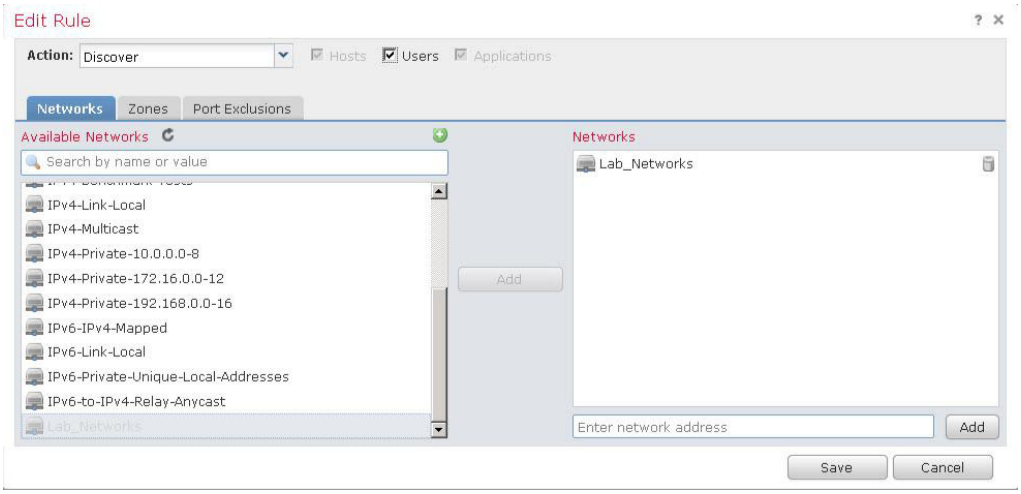
1. 导航至**策略 > 网络发现**。

a. 点击右侧的**铅笔图标**以编辑现有规则。

b. 选中**用户**复选框。“主机”复选框将自动选中。

c. 同时删除 **0.0.0.0/0** 和 **::/0**。

2. 选择网络 **Lab_Networks**，然后点击**添加**。



3. 点击**保存**。

部署配置更改

1. 点击 FMC 右上角的**部署**。

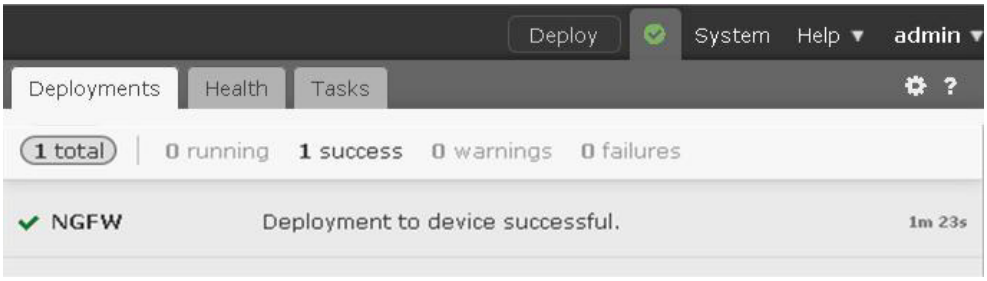
    a. 选中 NGFW 设备，然后展开列表以查看详细信息。

    b. 在“设备配置”的右侧，将鼠标悬停在**详细信息**上方。页面应如下图所示。

c. 确认修改 **NGFW 设置**、NAT 策略网络发现、接口和静态路由配置。

d. 点击**部署**按钮。

e. 点击 FMC 右上角的**部署**链接右侧的**图标**。等待直至部署完成。



测试 NGFW 部署

1. 在**内部 Linux 服务器** CLI 上：

   a. 输入 **`wget cisco.com`**。此命令应该会成功。这可确认 NAT 和路由。

   b. 输入 **`ping outside`**。此命令应该会成功。输入 **`Ctrl+C`** 以退出 ping。

   c. 输入 **`ftp outside`**。使用用户名 **`guest`** 和密码 **`C1sco12345`** 登录。

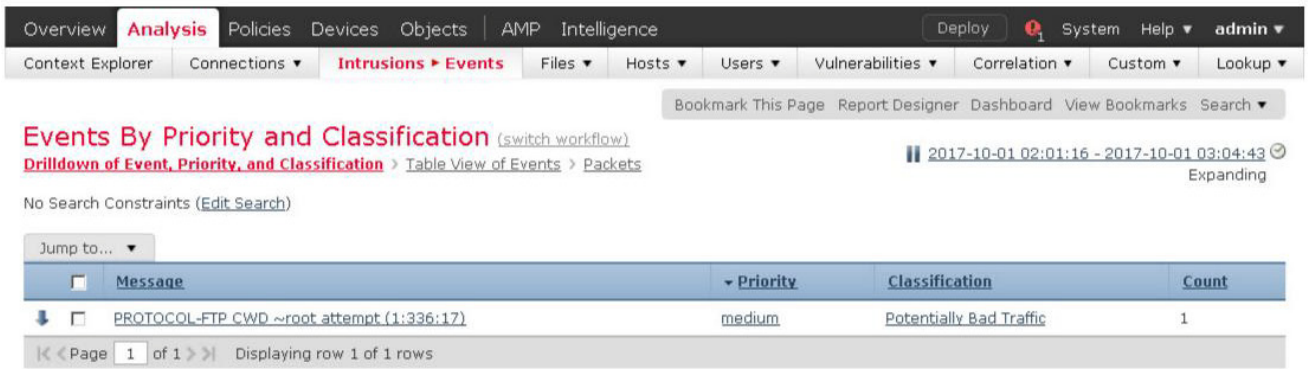
   d. 键入 **`cd ~root`**。您应该看到以下消息：421 服务不可用，远程服务器已关闭连接。这确认了 IPS 正在工作。

注意：如果 FTP 会话挂起，则表明您可能忘记在访问控制策略中启用活动响应。您无需解决此问题，但要记住理应出现上述行为。

   e. 键入 **`quit`** 以退出 FTP。

2. 在 FMC 中，导航至**分析 > 入侵 > 事件**。

注意：观察是否**已触发 Snort 规则 336**。在演示入侵策略中，此规则的规则状态设置为“丢弃并生成事件”。在系统定义的入侵策略（例如平衡的安全性和连接性）中已禁用此规则。



注意：在生产环境中，如果遇到未出现相应事件的情况，则首先要检查的是 NGFW 和 FMC 之间的时间同步。但是，在此实验中，问题更可能与夜间进程有关。如果发生此情况，请尝试重新启动这些进程，如下所示。在 NGFW CLI 上，运行以下命令。

```
pmtool restartbytype EventProcessor
```

从 Jumper Desktop 中，使用预定义 PuTTY 会话连接到 FMC。使用 **admin** 用户名和密码 **FPlab123!** 登录，并运行以下命令。

```
sudo pmtool restartbyid SFDataCorrelator
sudo pmtool restartbyid sftunnel
```

sudo 密码为 `FPlab123!`。

a. **点击左侧的箭头**以深入查看事件的表视图。观察是否显示事件的详细信息。

b. **点击事件左侧的箭头**以进一步深入查看。请注意，系统会向您提供广泛的信息，包括 Snort 规则的详细信息。

c. **展开操作**并注意可以从此处禁用规则，但请勿禁用！

d. **展开数据包字节**可查看已触发规则的数据包的内容。

3. 测试文件和恶意软件阻止功能。可以从 Jump Desktop 上名为 Strings 的文件剪切并粘贴这些 Wget 命令，以便剪切并粘贴文本。

   a. 作为控制测试，**使用 WGET 下载未阻止的文件**。

   ```
   wget -t 1 outside/files/ProjectX.pdf
   ```

   此命令应该会成功。

   b. 接下来，**使用 WGET 尝试下载按类型阻止的文件**。

   ```
   wget -t 1 outside/files/test3.avi
   ```

   请注意，系统仅下载了文件的很小一部分。这是因为 NGFW 可以在发现第一个数据块时检测出文件类型。演示文件策略配置为阻止 AVI 文件。

   c. 最后，**使用 WGET 尝试下载恶意软件**。

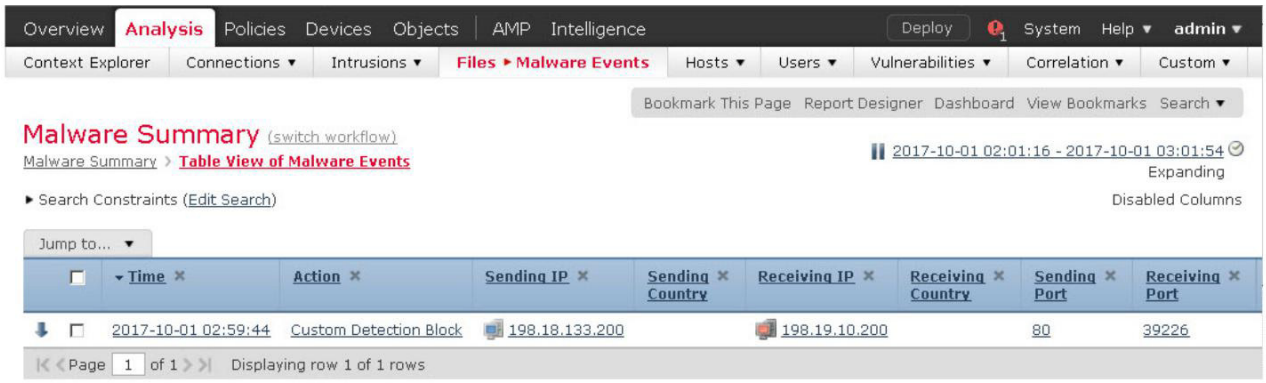
   ```
   wget -t 1 outside/files/Zombies.pdf
   ```

   请注意，系统下载了文件的大约 99% 部分。这是因为 NGRW 需要整个文件来计算 SHA。NGFW 会一直检测完最后一个数据块，直至计算并找出散列值。演示文件策略配置为阻止在 PDF 文件中检测到的恶意软件。

4. 在 FMC 中，导航至**分析 > 文件 > 恶意软件事件**。

   a. 观察是否已阻止一个文件 Zombies.pdf。

   b. 点击左侧的箭头以深入查看事件的表视图。请注意，主机 **198.19.10.200** 以红色图标表示。这是内部 Linux 服务器。红色图标表示已为主机分配感染指标。



注意：该操作报告为“自定义检测块”，而不是“恶意软件块”。这是因为我们已将 Zombies.pdf 添加到自定义检测列表，以防实验在连接到云时出现问题。有关详细信息，请参阅附录 A。

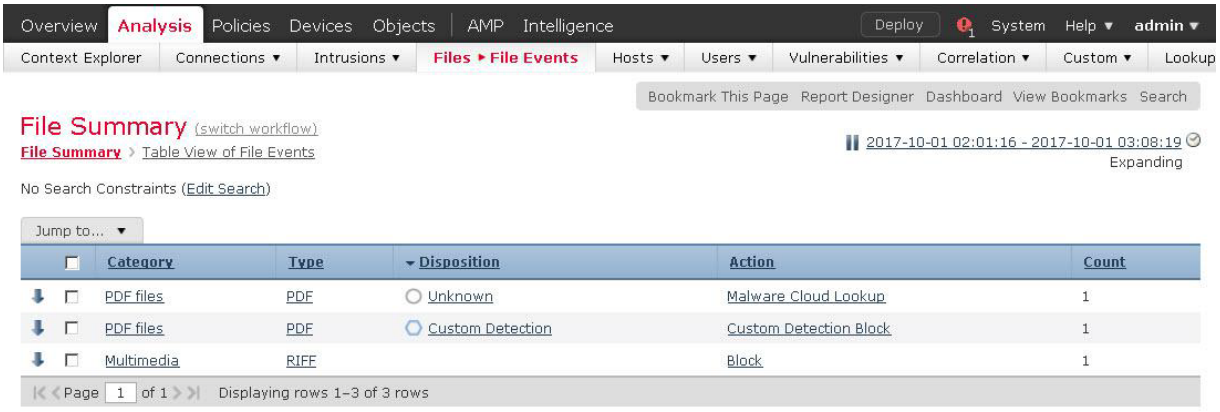
如果您愿意，可以尝试以下操作。

```
wget -t 1 outside/malware/Buddy.exe
```

此操作应报告为*恶意软件块*。但是，在此特定实验环境中，云查找可能会失败。因此，文件可能未受阻止。

5. **点击红色计算机图标**。这将打开主机配置文件页面。浏览此页面，然后将其关闭。

6. 导航至**分析 > 文件 > 文件事件**。您应该会看到有关全部三个文件事件的信息。



如果您愿意，可以深入查看更多详细信息。

场景 3：AnyConnect 远程接入 VPN

此练习包含以下任务：

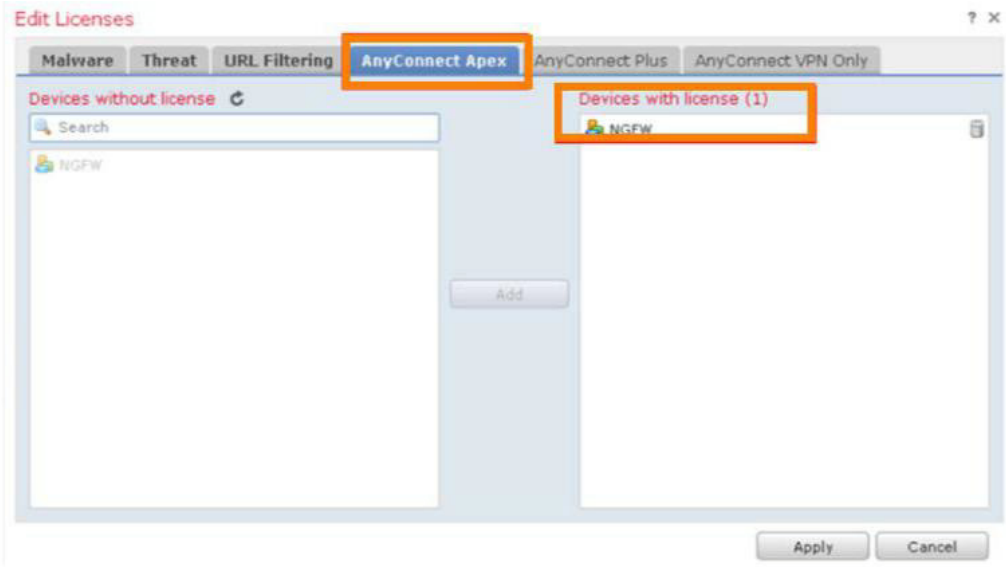
- 启用 AnyConnect 智能许可证
- 创建 AnyConnect RA VPN 对象
- 修改默认组策略
- 运行 RA VPN 向导
- 配置设备证书
- 修改访问控制策略以允许入站 AnyConnect 访问
- 配置 NAT 免除
- 配置 VPN 日志记录
- 部署并验证 NGFW RA VPN 配置
- 测试配置

此练习的目的是了解并配置思科 Firepower NGFW 上提供的 AnyConnect 远程接入 VPN 功能。

步骤

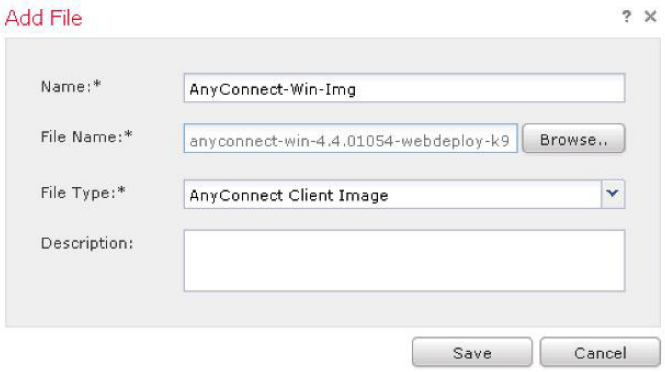
启用 AnyConnect 智能许可证

1. 在 FMC 中，导航至**系统 > 许可证 > 智能许可证**。
    a. 点击**编辑许可证**。
    b. 在**编辑许可证**窗口中，选择 **AnyConnect Apex** 选项卡。
    c. 选择 **NGFW** 设备。点击**添加**和**应用**。

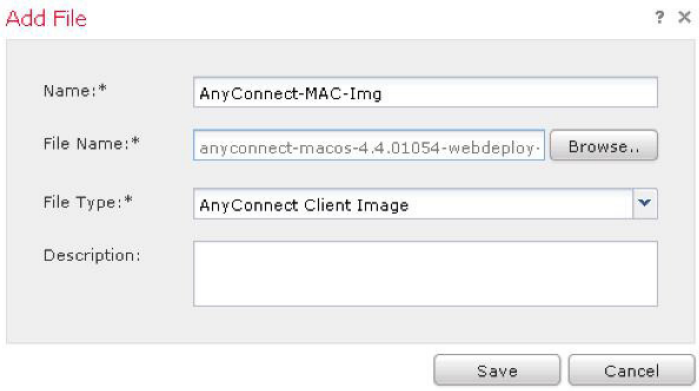


创建 AnyConnect RA VPN 对象

1. 为 Windows 创建一个 AnyConnect 映像对象。
    a. 在 FMC 中，导航至**对象 > 对象管理 > VPN > AnyConnect 文件**。
    b. 点击**添加 AnyConnect 文件**。
    c. 在**名称**字段，输入 **`AnyConnect-Win-Img`**。
    d. 点击**浏览**，然后导航至 Jump Desktop 上的 **RA VPN** 文件夹。
    e. 选择 **anyconnect-win-4.4.01054-webdeploy-k9.pkg** 文件。
    f. 点击**打开**。请注意，**文件类型**文本字段会预填充正确的值。
    g. 点击**保存**。



2. 为 MAC 操作系统创建另一个 AnyConnect 映像对象。
    a. 点击**添加 AnyConnect 文件**。
    b. 在**名称**字段，输入 **`AnyConnect-MAC-Img`**。
    c. 点击**浏览**，然后从 Jump Desktop 上的 **RA VPN** 文件夹中选择 **anyconnect-macos-4.4.01054-webdeploy-k9.pkg** 文件。
    d. 点击**打开**。请注意，**文件类型**文本字段会预填充正确的值。
    e. 点击**保存**。



3. 创建 AnyConnect 客户端配置文件对象。

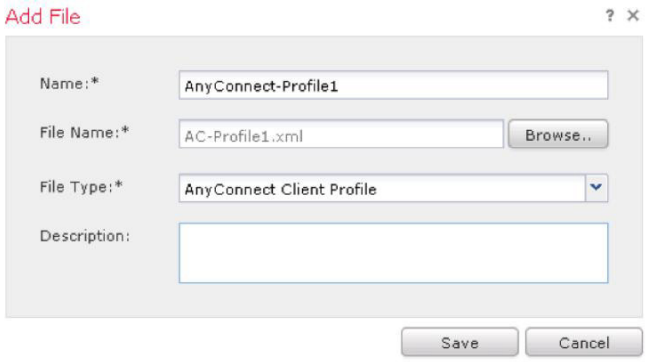
    a. 点击**添加 AnyConnect 文件**。

    b. 在“名称”字段，输入 **AnyConnect-Profile1**。

    c. 点击**浏览**，然后从 Jump Desktop 上的 **RA VPN** 文件夹中选择 **AC-Profile1.xml** 文件。

    d. 点击**打开**。请注意，**文件类型**文本字段会预填充正确的值。

    e. 点击**保存**。



注意：可以使用 cisco.com 上提供的 *VPN 配置文件编辑器*工具来创建 AnyConnect 客户端配置文件。VPN 配置文件编辑器工具在 Jump 中也可用。可以通过**开始 > 所有程序 > 思科 > 思科 AnyConnect 配置文件编辑器 > VPN 配置文件编辑器**访问该工具。

4. 创建 IP 池。

    a. 在 FMC 中，导航至**对象 > 对象管理 > 地址池 > IPv4 池**。

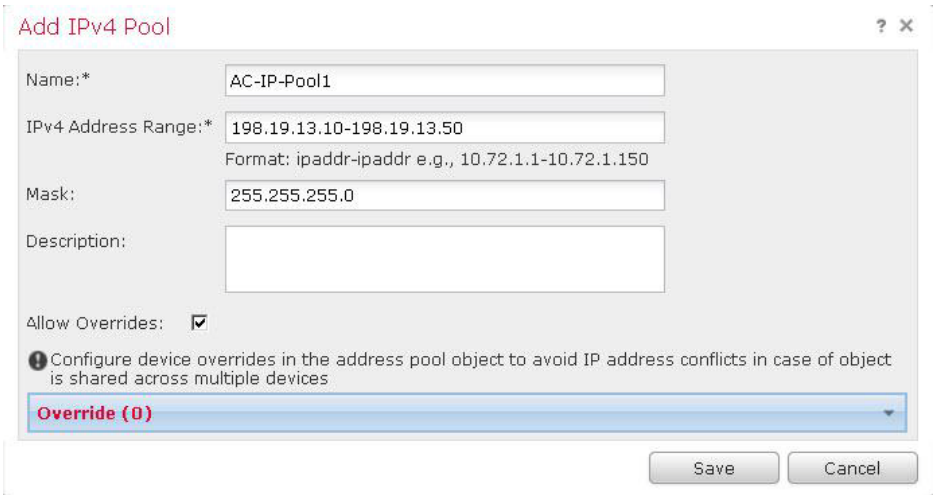
    b. 点击**添加 IPv4 池**。

    c. 在“名称”字段，输入 **AC-IP-Pool1**。

    d. 对于 **IPv4 地址范围**，输入 **198.19.13.10-198.19.13.50**。

    e. 在“掩码”字段，输入 **255.255.255.0**。

    f. 点击**保存**。



5. 创建与 IPv4 池对应的网络对象。

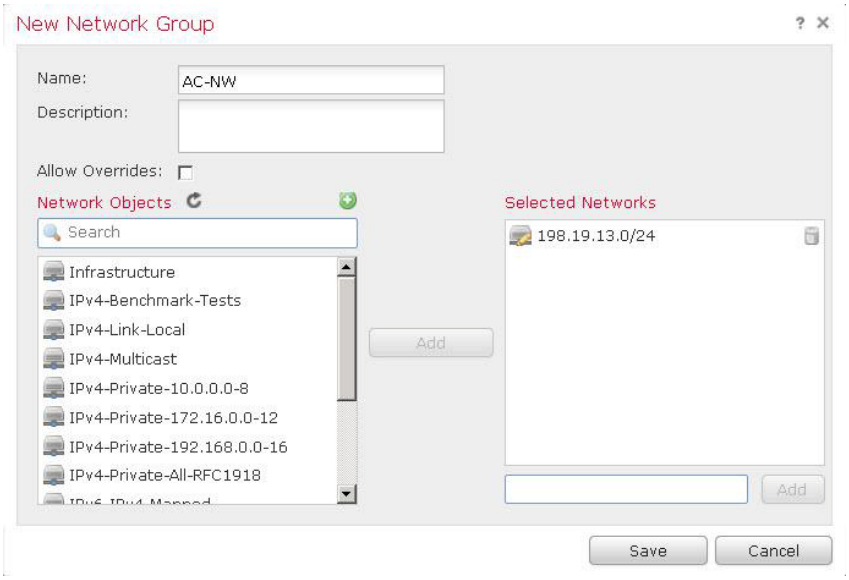
    a. 在 FMC 中，导航至**对象 > 对象管理 > 网络**。

    b. 点击**添加网络**，然后选择**添加组**。

    c. 在**名称**字段，输入 **AC-NW**。

    d. 在**所选网络**下的底部文本字段中，输入 **198.19.13.0/24**，然后点击**添加**。

    e. 点击**保存**。



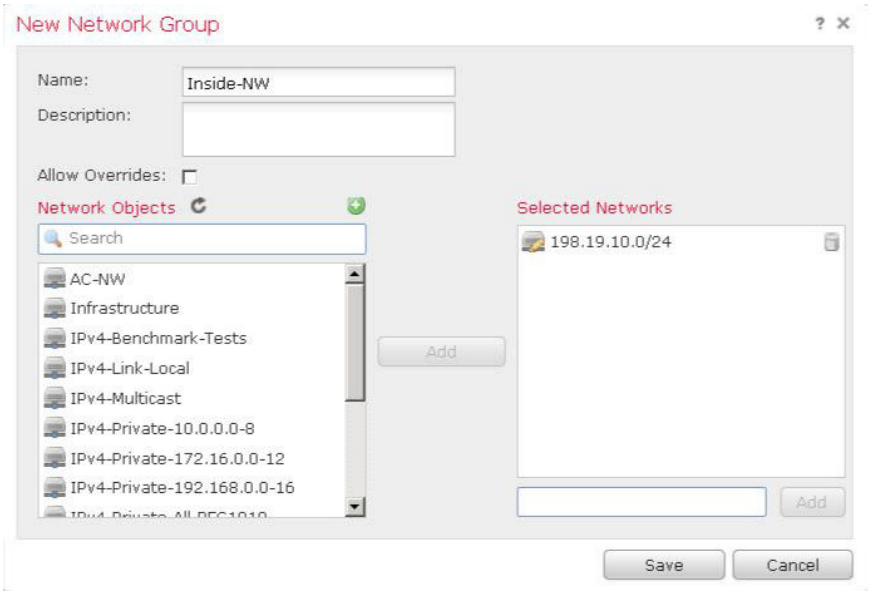
6. 为内部网络创建网络对象。

    a. 点击**添加网络**，然后选择**添加组**。

    b. 在“名称”字段，输入 **Inside-NW**。

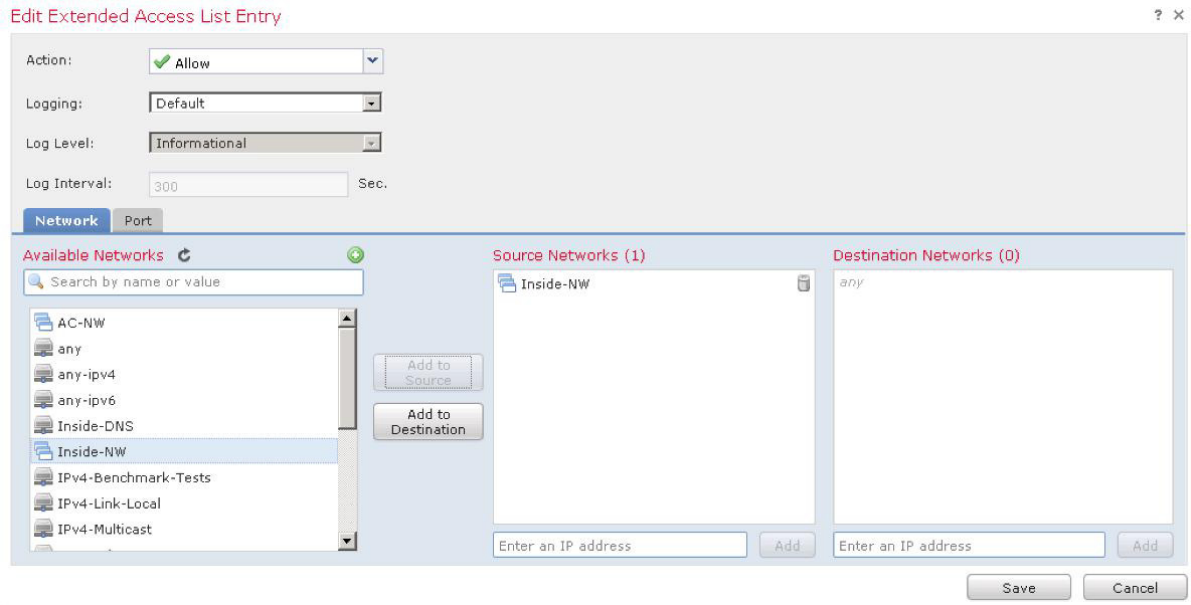
    c. 在**所选网络**下的底部文本字段中，输入 **198.19.10.0/24**，然后点击**添加**。

    d. 点击**保存**。

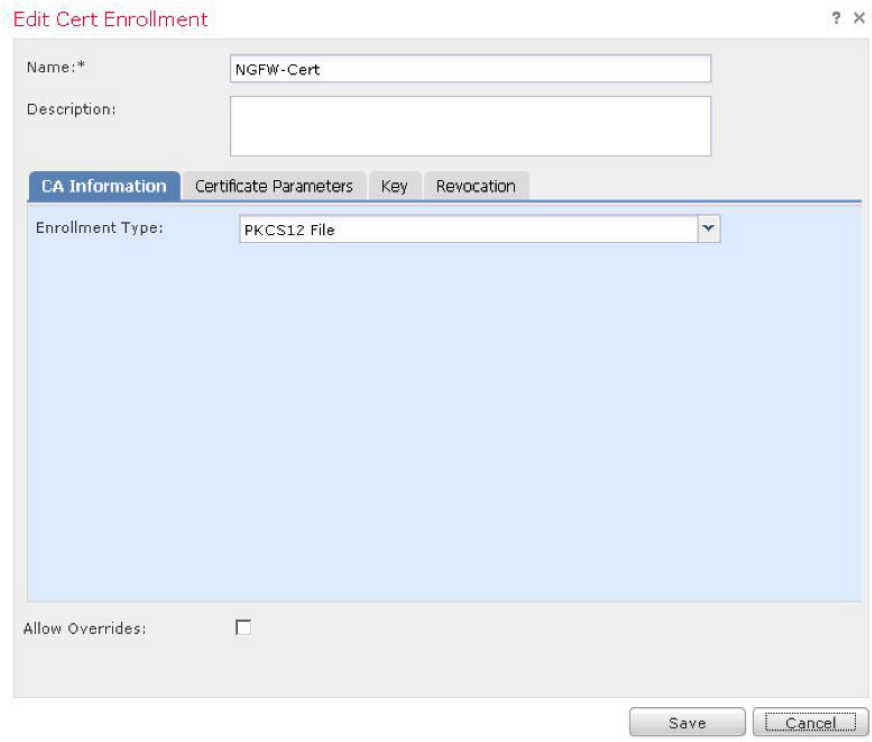


注意：您应使用网络对象组而不是网络对象，因为在下一个实验练习中，您将添加另一个子网，由于您使用的是网络组，因此只需修改此对象即可，而不必直接修改访问控制和 NAT 策略。

7. 为 RA VPN 拆分隧道配置创建 ACL。
    a. 在 FMC 中，导航至**对象 > 对象管理 > 访问列表 > 扩展**。
    b. 点击**添加扩展访问列表**。
    c. 在“名称”字段，输入 **AC-SplitTunnel1**。
    d. 点击**添加**。
    e. 从**可用网络**中选择 **Inside-NW**，然后点击**添加到源**。
    f. 点击“添加”。
    g. 点击**保存**。



8. 创建设备证书对象。
    a. 在 FMC 中，导航至**对象 > 对象管理 > PKI > 证书注册**。
    b. 点击**添加证书注册**。
    c. 在“名称”字段，输入 **NGFW-Cert**。
    d. 在**注册类型**中，选择 **PKCS12 文件**。
    e. 点击**保存**。



9. 为 ISE RADIUS 服务器创建对象。

    a. 在 FMC 中，导航至**对象 > 对象管理 > RADIUS 服务器组**。

    b. 点击**添加 RADIUS 服务器组**。

    c. 在“名称”字段，输入 **ISE-AAA**。

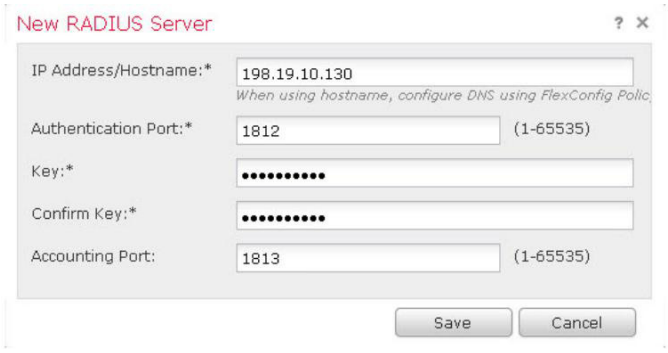
    d. 点击“RADIUS 服务器”部分中的 (+) 图标。

    e. 在“IP 地址”字段，输入 **198.19.10.130**。

    f. 在**密钥**和**确认密钥**字段，输入 **C1sco12345**。

    g. 在**新建 RADIUS 服务器**页面上，点击**保存**。

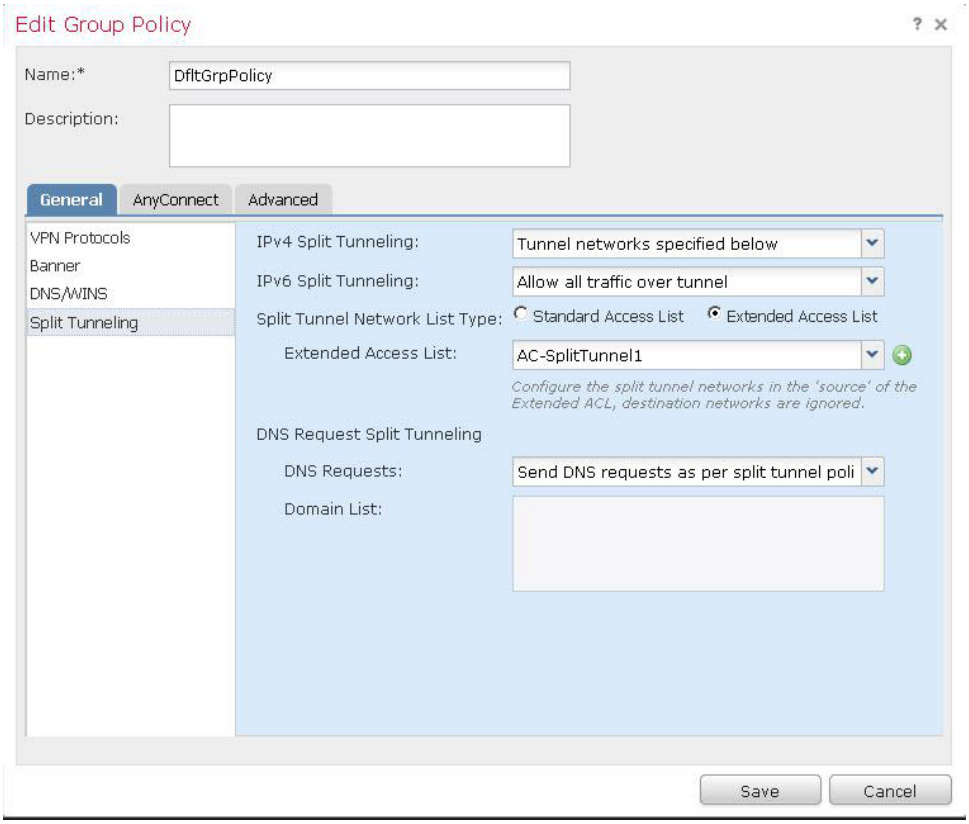
    h. 在**添加 RADIUS 服务器组**页面上，点击**保存**。



注意：为节省时间，ISE 已面向所有实验练习使用所有必需配置进行了预配置。如果要检查 ISE 配置，请参阅附录 C

修改默认组策略

1. 在 FMC 中，导航至**对象 > 对象管理 > VPN > 组策略**。
2. 选择并编辑 **DfltGrpPolicy**。
3. 在**常规**选项卡中，选择**拆分隧道**。
    a. 对于 **IPv4 拆分隧道**，选择**下面指定的隧道网络**。
    b. 选中**扩展访问列表**单选按钮。
    c. 对于**访问列表**，选择 **AC-SplitTunnel1**。

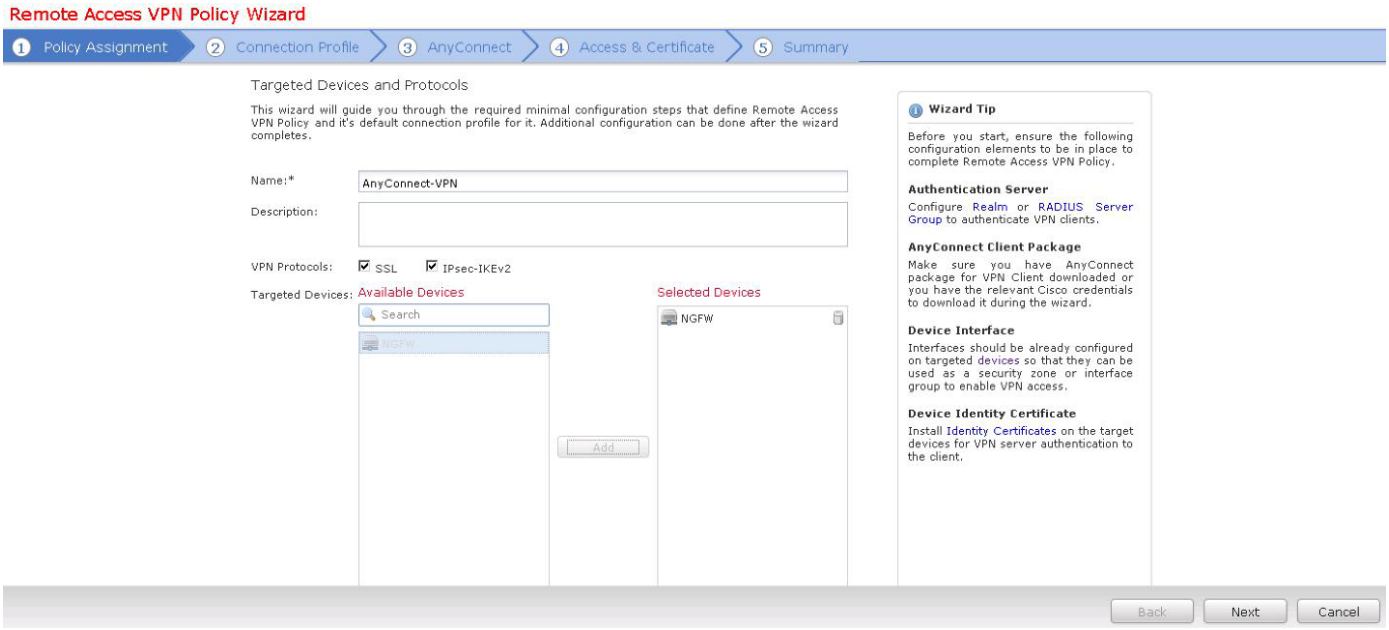


4. 在**常规**选项卡中，选择 **DNS/WINS**。
    a. 对于**主 DNS 服务器**，点击 (+) 图标。
    b. 在**名称**字段，输入 **`Inside-DNS`**。
    c. 在**网络**字段，输入 **`198.19.10.100`**。
    d. 点击**保存**。
5. 选择 **AnyConnect** 选项卡。对于**客户端配置文件**，选择 **AnyConnect-Profile1**。

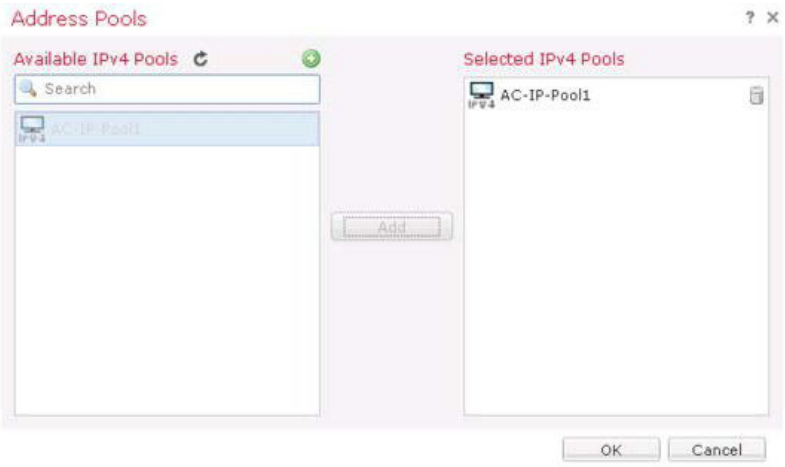
6. 点击**保存**以保存对组策略的更改。

运行 RA VPN 向导

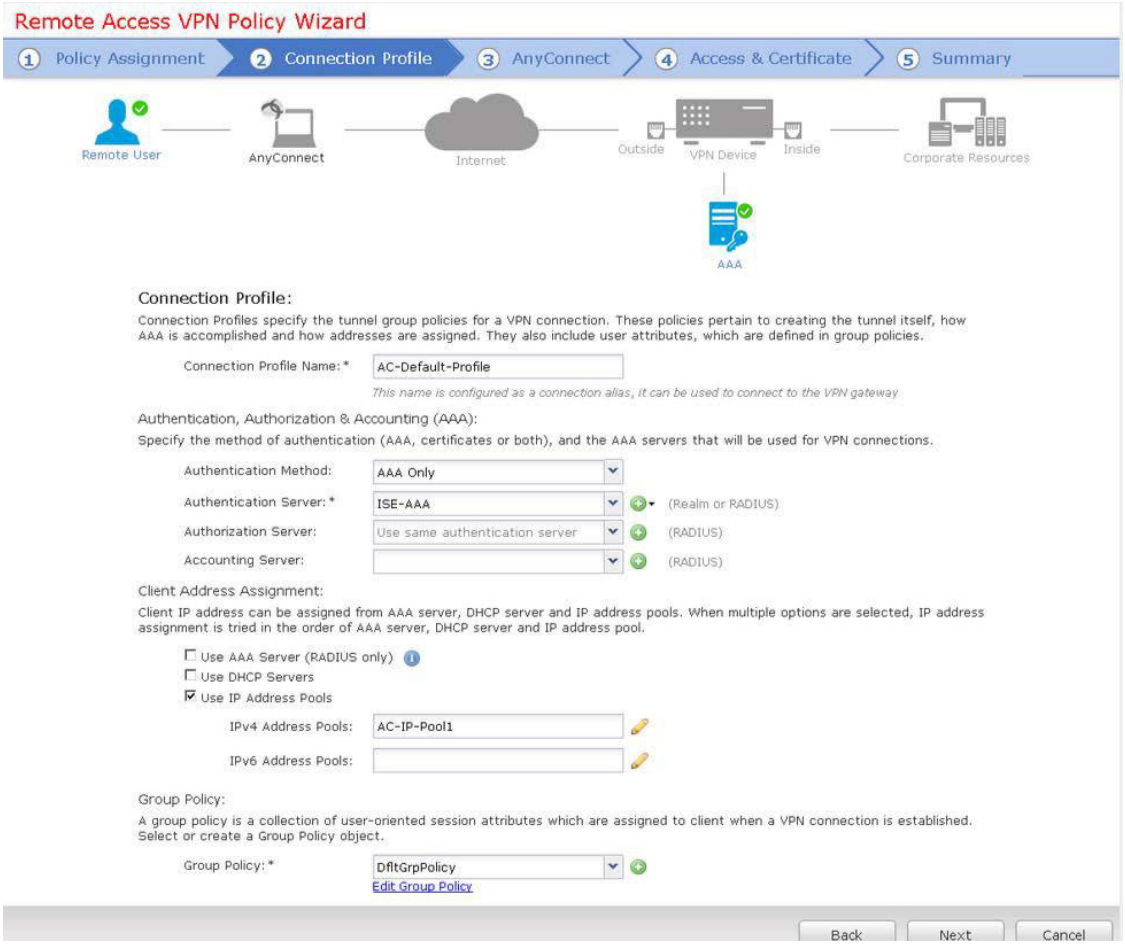
1. 在 FMC 中，导航至**设备 > VPN > 远程接入**。点击**添加**。系统将启动向导。
2. 完成向导的**策略分配**页面。
    a. 在**名称**字段，输入 **AnyConnect-VPN**。
    b. 从**目标设备**中选择 **NGFW**。点击**添加**。
    c. 点击**下一步**。



3. 完成向导的**连接配置文件**页面。
    a. 在**连接配置文件名称**字段，输入 **AC-Default-Profile**。
    b. 确认对于**身份验证方法**，已选择**仅 AAA**。
    c. 对于“身份验证服务器”，选择 **ISE-AAA**。
    d. 在**地址池**下，编辑 **IPv4 地址池**。
    e. 从 **IPv4 地址池**中选择 **AC-IP Pool1**。点击**添加**，然后点击**确定**。



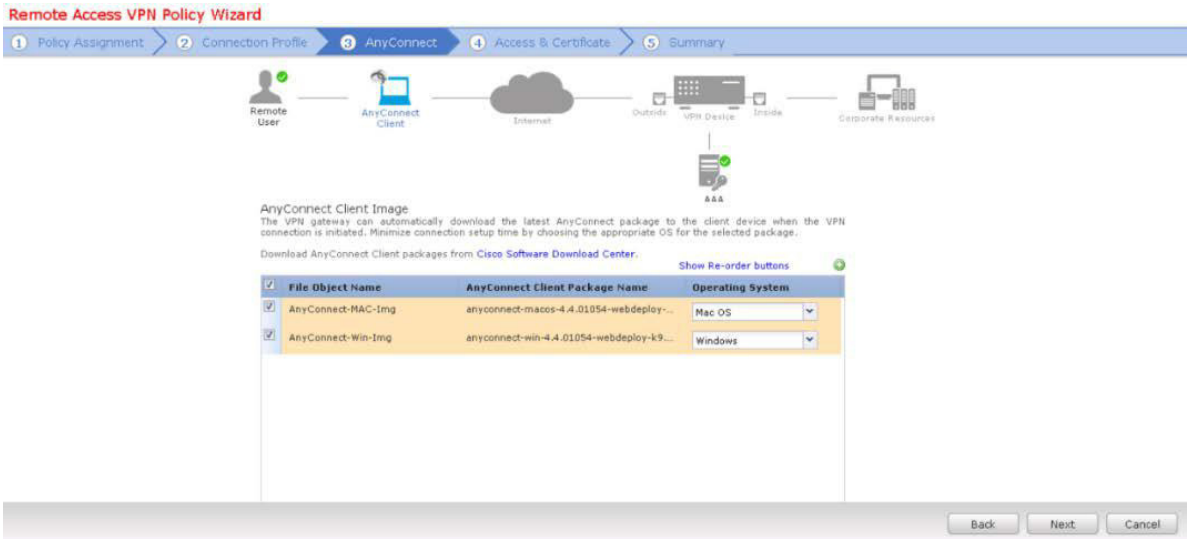
4. 确认**组策略**设置为 **DfltGrpPolicy**。点击**下一步**。



5. 完成向导的 **AnyConnect** 页面。

   a. 选中两个文件对象复选框。

   b. 点击**下一步**。

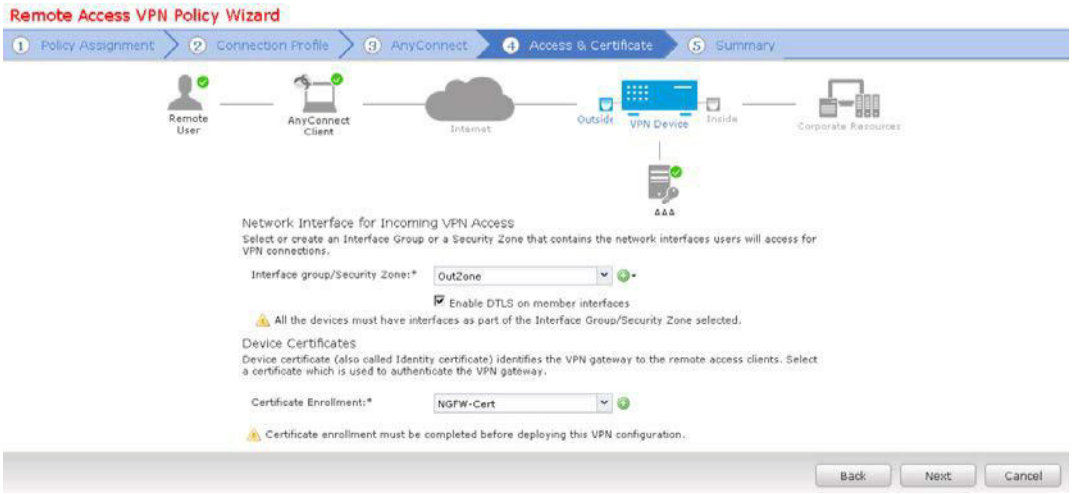


6. 完成向导的**访问和证书**页面。

   a. 对于**接口组/安全区域**，选择 **OutZone**。

   b. 对于**证书注册**，选择 **NGFW-Cert**。

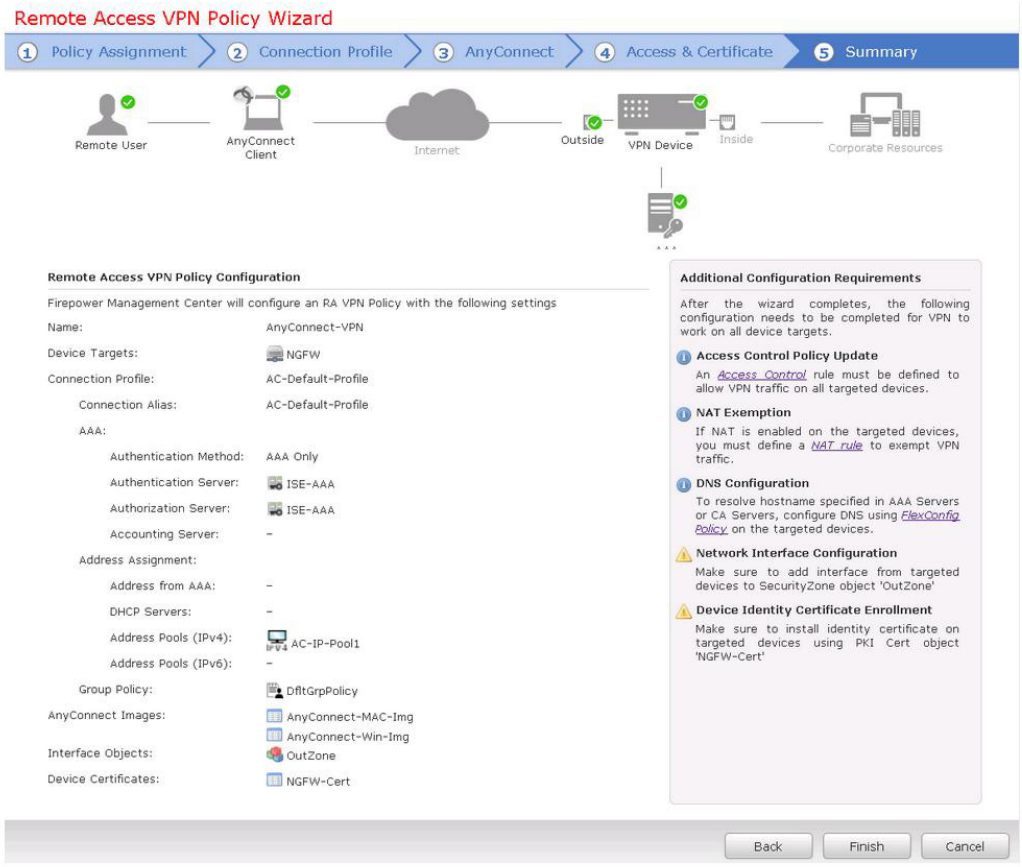
   c. 点击**下一步**。



7. 查看向导的**摘要**页面。

   a. 查看此页面中显示的配置。

   b. 点击**完成**。

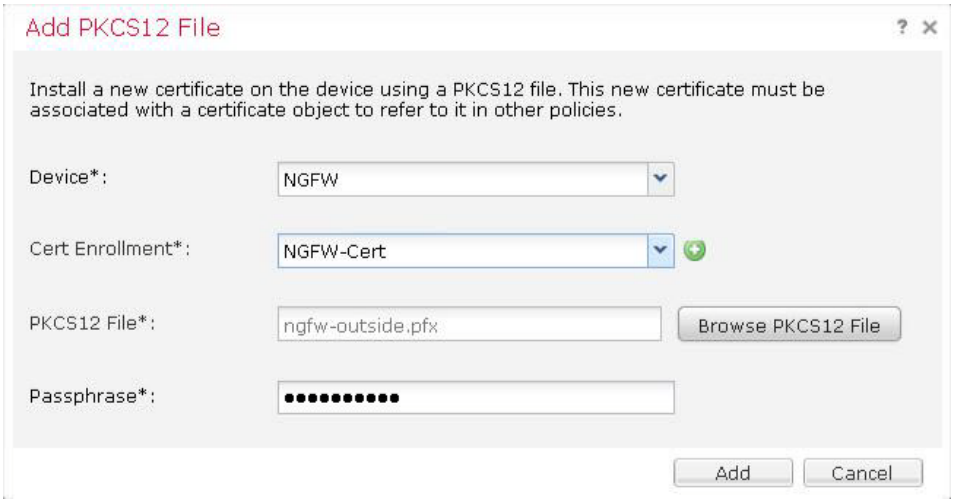


配置设备证书

1. 在 FMC 中，导航至**设备 > 证书**。
2. 点击**添加**，然后选择 **PKCS12 文件**。
    a. 对于**设备**，选择 **NGFW**。
    b. 对于**证书注册**，选择 **NGFW-Cert**。

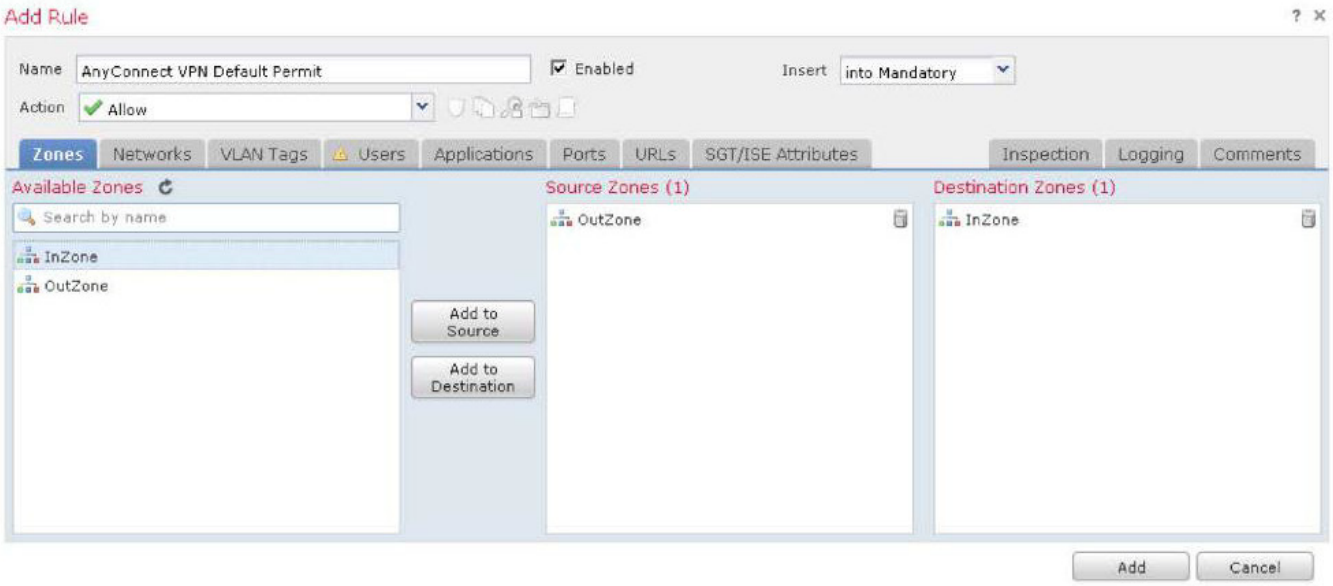
注意：请确保点击文本字段右侧的向下箭头。如果在文本区域中点击，您将看到字符串 **admin**。这是一种浏览器故障。

    c. 对于 **PKCS12 文件**，点击**浏览 PKCS12** 文件。导航至 Jump Desktop 上的 **Certificates** 文件夹，然后选择 **ngfw-outside**。点击**打开**。
    d. 对于**口令**，输入 `C1sco12345`。
    e. 点击**添加**。



修改访问控制策略以允许入站 AnyConnect 访问

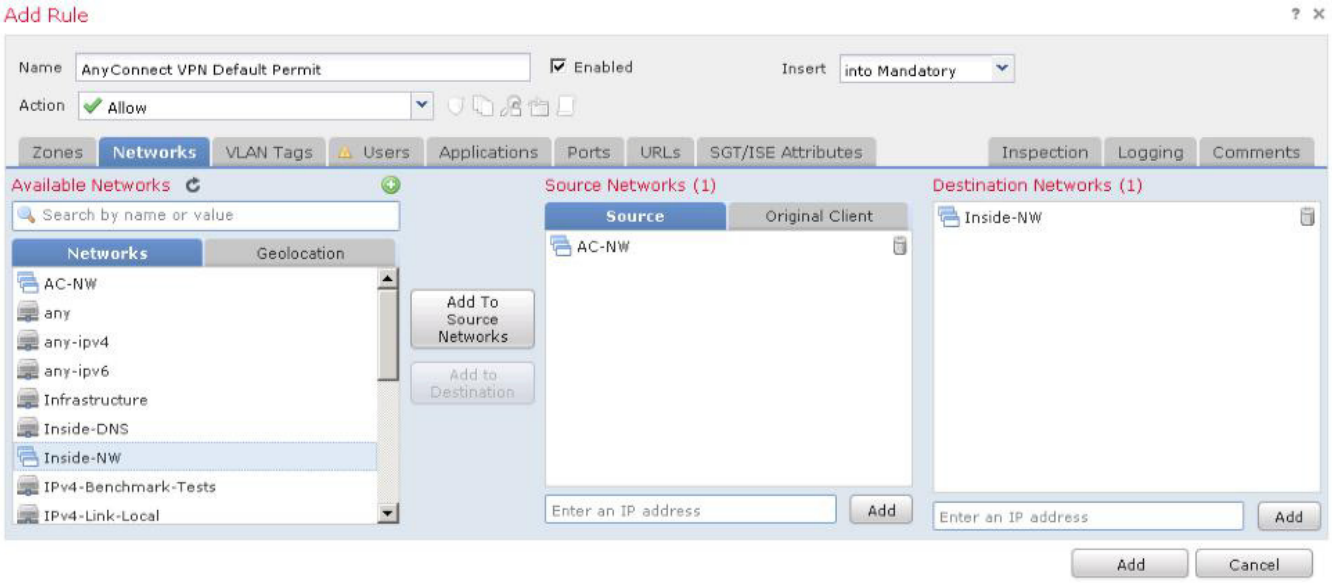
1. 在 FMC 中，导航至**策略 > 访问控制 > 访问控制**。
2. 选择并编辑访问控制策略。点击**添加规则**。
    a. 在**名称**字段，输入 **AnyConnect VPN Default Permit**。
    b. 从**插入**下拉列表中，选择**插入到默认规则集**
    c. 系统应已选择**区域**选项卡。
    d. 选择 **OutZone**，然后点击**添加到源**。
    e. 选择 **InZone**，然后点击**添加到目的地**。



f. 选择**网络**选项卡。

i. 选择 **AC-NW**，然后点击**添加到源**。

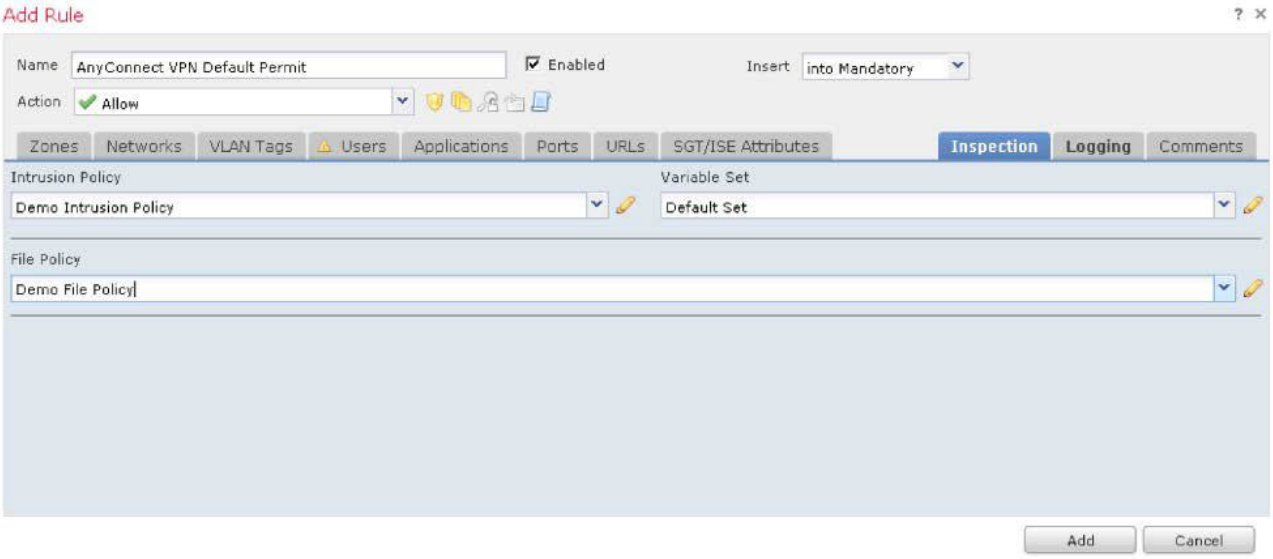
ii. 选择 **Inside-NW**，然后点击**添加到目的地**。



g. 选择**检查**选项卡。

i. 从“入侵策略”下拉列表中选择“演示入侵策略”。

ii. 从“文件策略”下拉列表中选择“演示文件策略”。



h. 点击**添加**以添加规则。

i. 点击**保存**以保存对访问控制策略的更改。

配置 NAT 免除

1. 在 FMC 中，导航至**设备 > NAT**。

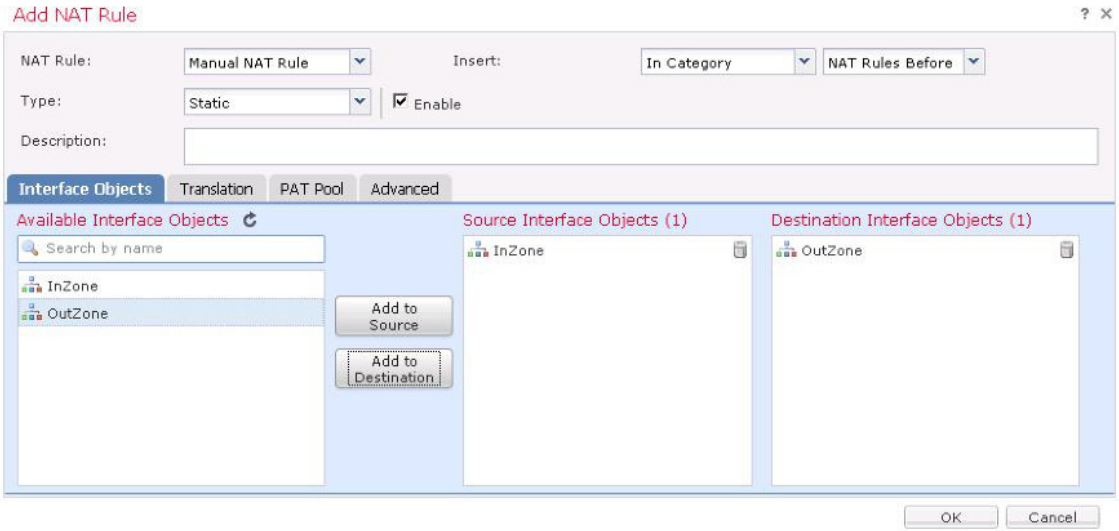
2. 选择并编辑现有 **NAT 策略**。确认在右上方看到灰显的**保存**按钮。如果看不到，请导航离开并重试编辑。这是已知漏洞。

3. 点击**添加规则**。

a. 您将进入“接口对象”选项卡。

i. 选择 **InZone**，然后点击**添加到源**。

ii. 选择 **OutZone**，然后点击**添加到目的地**。



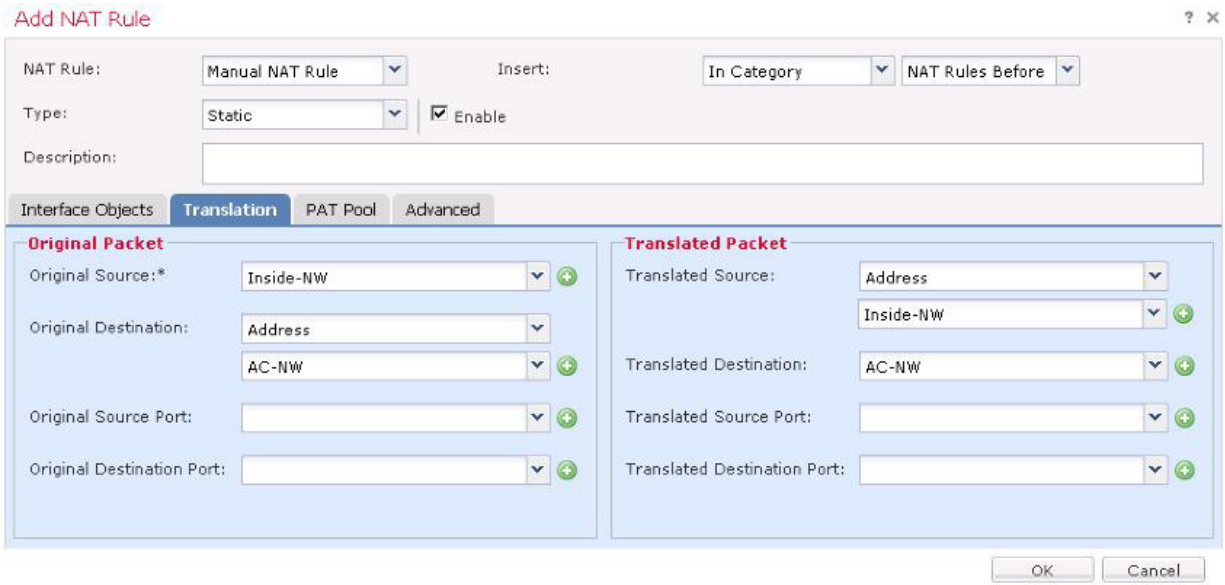
b. 选择**转换**选项卡。

i. 对于**原始源**，选择 **Inside-NW**。

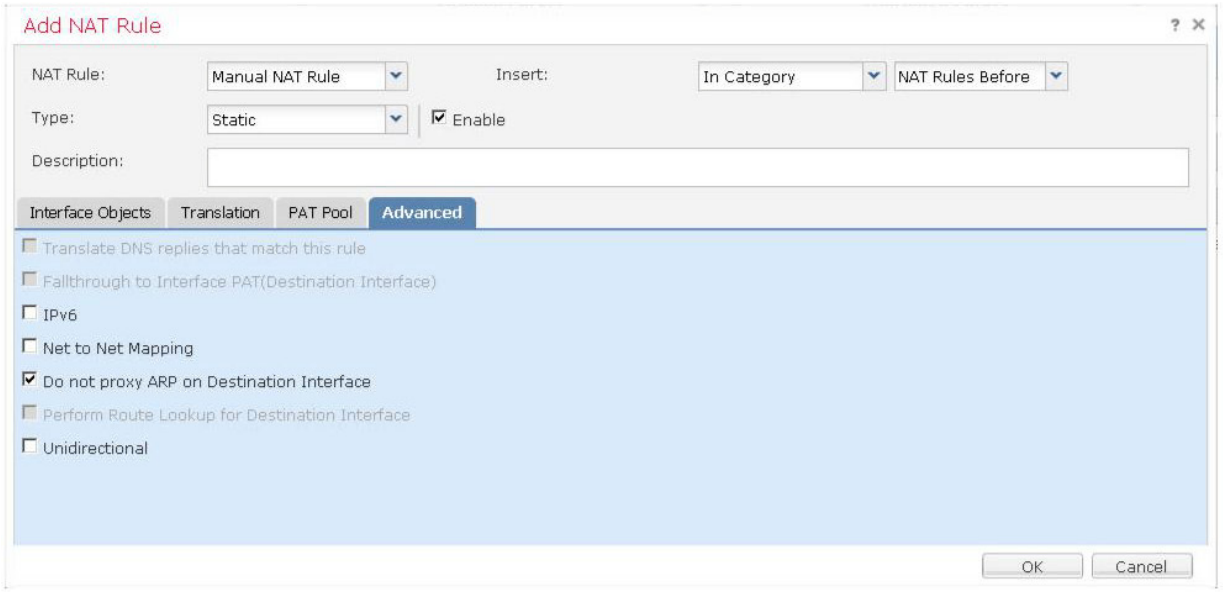
ii. 对于**原始目的地**，选择 **AC-NW**。

iii. 对于**已转换的源**，选择 **Inside-NW**。

iv. 对于**已转换的目的地**，选择 **AC-NW**。



c. 选择**高级**选项卡，然后选择**不在目的接口上使用代理 ARP**。



注意：启用**不在目的接口上使用代理 ARP** 在此实验练习中至关重要。如果您遗漏此步骤，您的 pod 可能会出现访问问题，因为所有设备都是在频段内进行管理。

d. 点击**确定**以保存 NAT 规则

e. 点击**保存**以保存对 NAT 策略的更改。

配置 VPN 日志记录

为便于故障排除，您需要将 VPN 日志记录级别从默认（错误）更改为参考。在实验期间的任何时候，您都可以导航至**设备 > VPN > 故障排除**以查看记录的信息，从而帮助对配置进行故障排除。

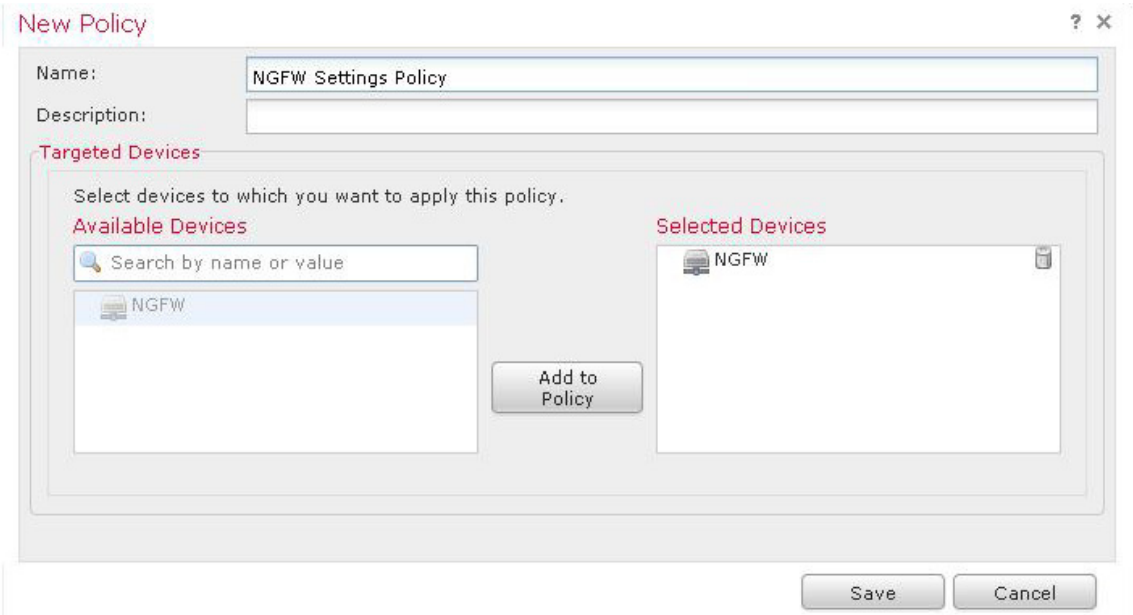
注意：在生产环境中，您不需要将 VPN 日志记录保持设置为参考。

1. 在 FMC 中，导航至**设备 > 平台设置**。

   a. 点击蓝色文本**威胁防御设置策略**。

   b. 将策略命名为 **`NGFW Settings Policy`**。

   c. 选择 **NGFW** 设备，然后点击**添加到策略**。

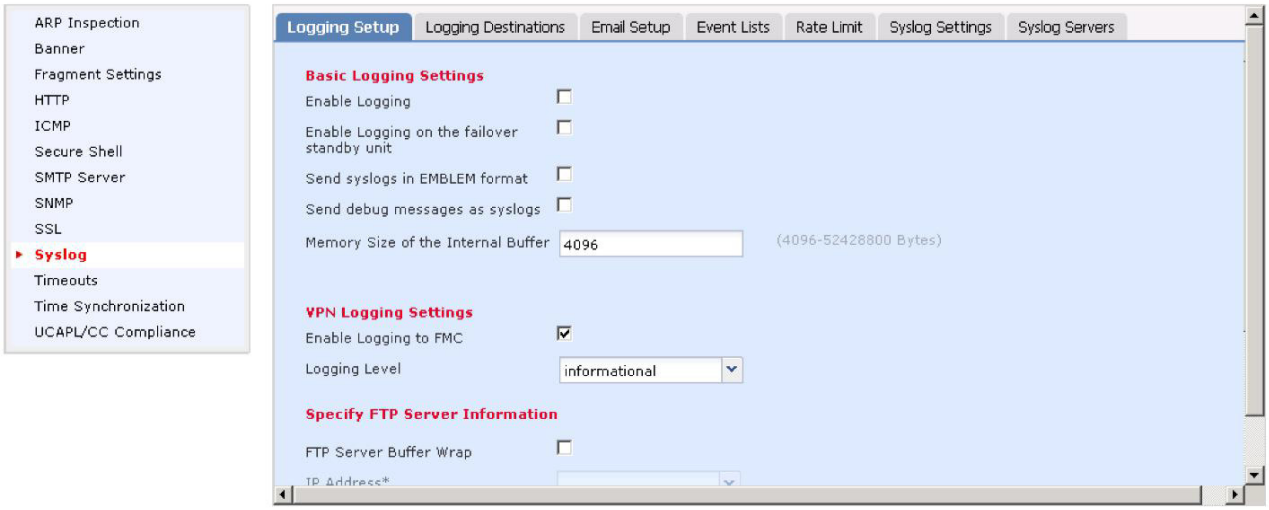


d. 点击**保存**。等待该策略打开以进行编辑。

e. 在左侧导航窗格中，选择**系统日志**。

f. 在 **VPN 日志记录设置**下，将日志记录级别更改为**参考**。请注意，在生产环境中，建议将此日志记录级别设置为错误或警报。

g. 点击**保存**。



部署并验证 NGFW RA VPN 配置

1. 将策略部署到设备中。

    a. 在 FMC 中，点击**部署**按钮。

    b. 选择 **NGFW**，然后点击**部署**。

    c. 等待部署完成。

2. 您应该仍有一个与 NGFW CLI 的活动 PuTTY 会话。运行以下部分或全部命令。

    a. `show running-config tunnel-group`

    b. `show running-config group-policy`

    c. `show running-config crypto`

    d. `show running-config ip local pool`

    e. `show running-config nat`

3. 通过在 NGFW CLI 上运行以下命令来测试 AAA。
   `test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'`

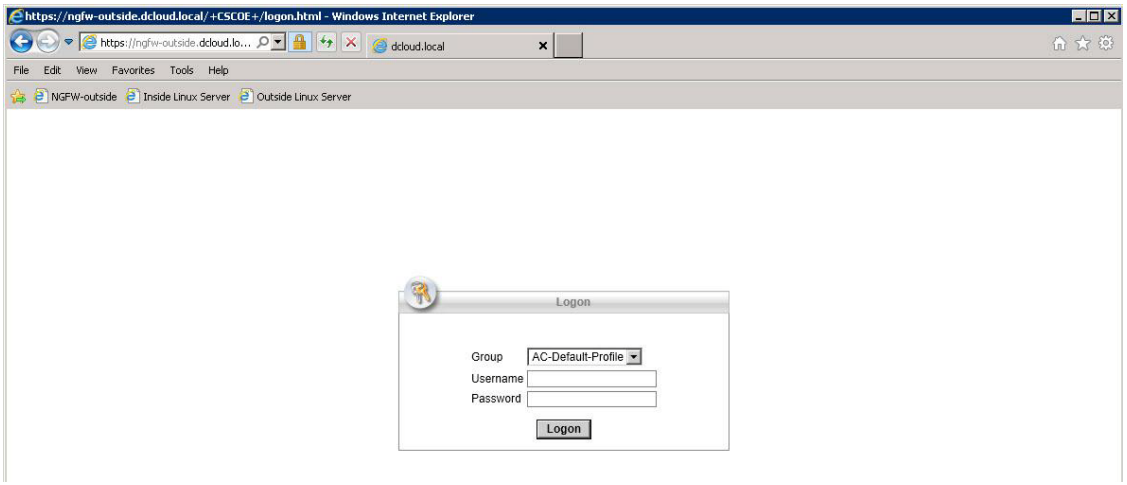
   您可以从 Jump Desktop 上的 Strings to cut and paste.txt 文本文件剪切并粘贴此命令。

```
> test aaa-server authentication ISE-AAA host 198.19.10.130 username ira password 'C1sco12345'
INFO: Attempting Authentication test to IP address (198.19.10.130) (timeout: 32 seconds)
INFO: Authentication Successful
>
```

测试配置

1. 打开 Jump Desktop 上的 **Remote Desktops** 文件夹，然后双击 **Outside-PC**。

    a. 打开 **Internet Explorer**，点击收藏夹工具栏上的 **NGFW-outside**。

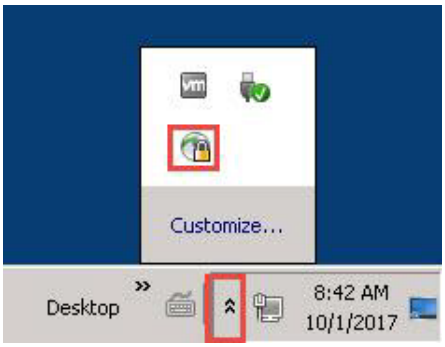


    b. 对于**用户名**，输入 `ira`。在**密码**字段，输入 `C1sco12345`。点击**登录**。

    c. 点击页面底部的**安装**按钮。系统提示时，再次点击**安装**。

d. 成功安装后，AnyConnect 将自动连接。

e. 从 Outside-PC 的右下方打开 AnyConnect 客户端 UI，如下所示。



2. 点击齿轮图标，打开 AnyConnect 客户端 UI 的**高级**窗口，如下所示。

a. 选择客户端的**统计信息**选项卡，获取服务器 IP 地址。

b. 选择**路由详细信息**选项卡以确认拆分隧道：只有到 198.19.10.0/24 的流量才被视为安全路由。换言之，只有到 198.19.10.0/24 的流量才通过 VPN 以隧道方式传输。请注意，198.19.10.100/32 也被列为安全路由。这是因为 VPN 组策略将 198.19.10.100 分配给作为 DNS 服务器的客户端。

3. 通过在 NGFW CLI 上运行以下命令来验证此会话：
`show vpn-sessiondb detail anyconnect`。

```
> show vpn-sessiondb detail
anyconnect

Session Type: AnyConnect Detailed
Username     : ira                    Index        : 60244
Assigned IP  : 198.19.13.10           Public IP    : 198.18.133.23
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : Clientless: (1)AES256  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (
1)AES256
Hashing      : Clientless: (1)SHA256  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA          1
(省略部分输出)
```

4. 在 Outside-PC 上，打开命令提示符。
    a. 运行 **`nslookup inside.dcloud.local`**。确认 PC-outside 使用的是 IP 地址为 198.19.10.100 的内部 DNS 服务器。
    b. 运行以下命令。
    `ftp inside.dcloud.local`
    使用用户名 **`guest`** 和密码 **`C1sco12345`** 登录。这可确认对内部服务器的访问。
    c. 键入 **`cd ~root`**。您应该看到以下消息。
    `Connection closed by remote host.`
    这确认入侵防御正在工作。
5. 在 Internet Explorer 中，点击收藏夹工具栏上的**内部 Linux 服务器**。
    a. 点击**文件**链接。
    b. 点击 **ProjectX.pdf** 链接，然后点击网页底部的**打开**按钮，以确认可以下载 PDF。
    c. 点击 **Zombies.pdf** 链接，然后点击网页底部的**打开**按钮。您将在网页底部看到以下消息。这是因为面向网络的 AMP 已阻止该文件。

6. 在 FMC 中，导航至**分析 > 入侵 > 事件**。
    a. 观察是否已触发 Snort 规则 336。
    b. 深入查看**事件的表视图**，以确认源 IP 地址来自 VPN 池。
7. 在 FMC 中，导航至**分析 > 文件 > 恶意软件事件**。
    a. 观察是否已阻止 **Zombies.pdf**
    b. 深入查看恶意软件事件的表视图，以确认源地址来自 VPN 池。
8. 在继续进行下一个实验练习之前，请断开连接 AnyConnect VPN。

场景 4：具有 RADIUS 属性的 AnyConnect

此练习包含以下任务：

- 创建新组策略
- 创建新 IP 池
- 修改访问控制和 NAT 策略
- 修改连接配置文件
- 部署和测试配置

在此练习中，我们将使用 ISE RADIUS 属性根据用户的 AD 组来动态分配组策略、IP 池和可下载 ACL (DACL)。

- 如果 RA VPN 用户是 IT 组的成员，则他们应该对内部网络 (174.16.1.0/24) 上的任何设备都具有完全访问权限。
- 如果 RA VPN 用户不是 IT 组的成员，则他们应该只能访问以下两个内部设备：
    - 域控制器 ad1.dcloud.local (198.19.10.100)
    - 内部 Linux 服务器 inside.dcloud.local (198.19.10.200)。
- 应从单独的 IP 池来为作为 IT 组成员的用户提供 IP 地址。

为节省时间，ISE 面向所有实验练习使用所有必需配置进行了预配置。这包括根据 AD 组成员身份选择组策略和 IP 池。**因此，新组策略和 IP 池的名称必须与说明中给定的名称完全相同。**如果要查看 ISE 配置，请参阅附录 C

步骤

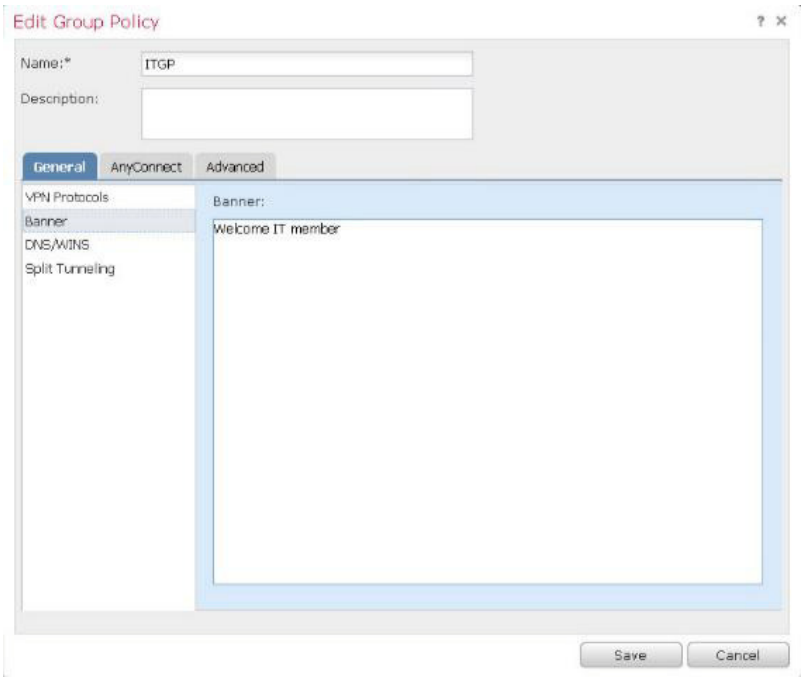
创建新组策略

您需要创建一个与 DfltGrpPolicy 基本相同的组策略。您要演示的是 ISE 如何能够根据用户的 Active Directory 组来分配组策略。添加特定的自定义设置可能更有趣，但是这对于此场景并不重要。

1. 在 FMC 中，导航至**对象 > 对象管理 > VPN > 组策略**。
2. 点击**添加组策略**。

3. 在“名称”字段，输入 **ITGP**。由于 ISE 配置，这必须是确切的组名。

4. 在**常规**选项卡中，选择**横幅**。输入文本 **Welcome IT Member。**



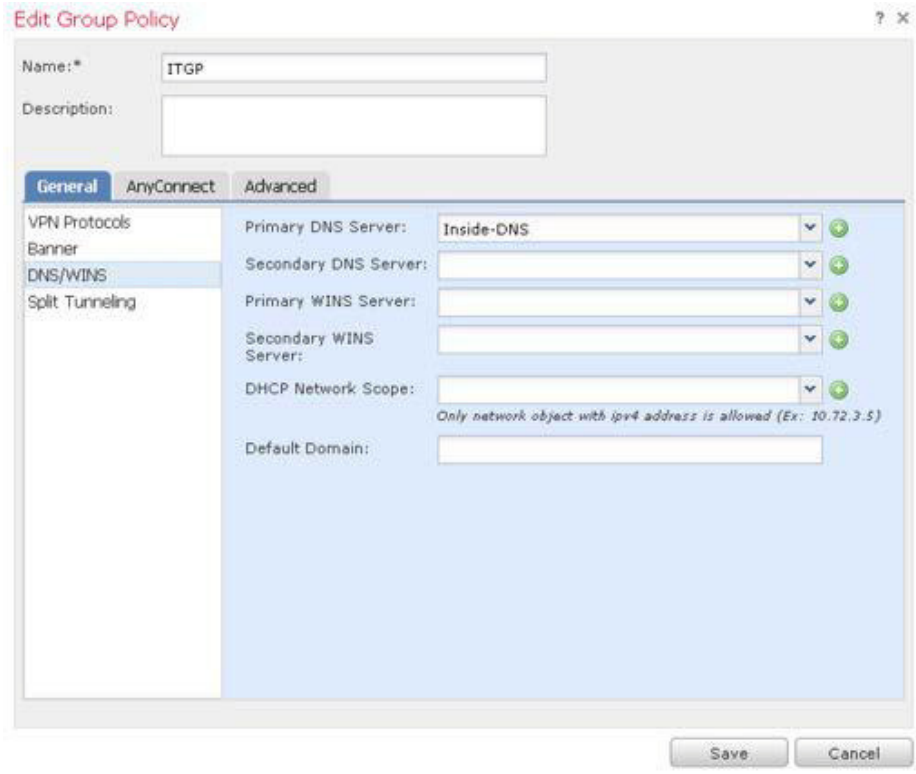
5. 在**常规**选项卡中，选择**拆分隧道**。

    a. 对于 **IPv4 拆分隧道**，选择**下面指定的隧道网络**。

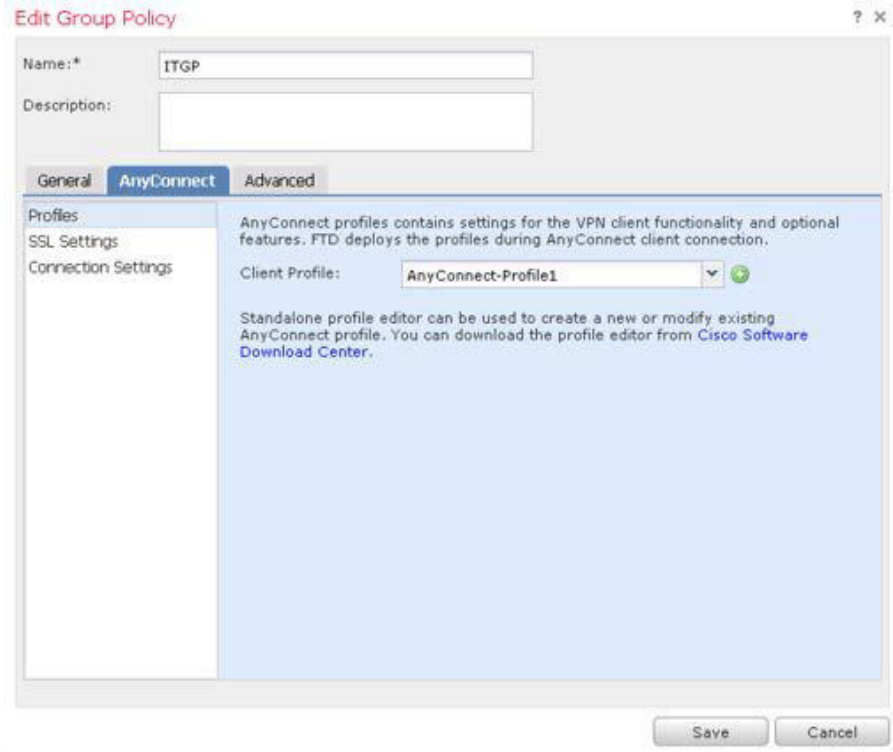
    b. 选中**扩展访问列表**单选按钮。

    c. 对于**访问列表**，选择 **AC-SplitTunnel1**。

6. 在**常规**选项卡中，选择 **DNS/WINS**。对于**主 DNS 服务器**，选择 **Inside-DNS**。



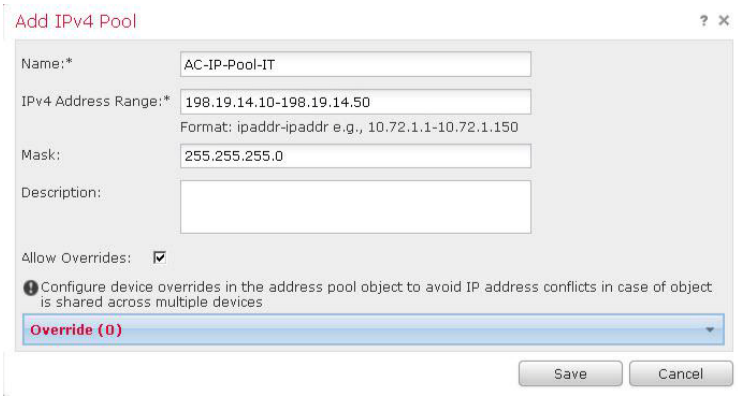
7. 选择 **AnyConnect** 选项卡。对于“客户端配置文件”，选择 **AnyConnect-Profile1**。



8. 点击**保存**以保存组策略。

创建新 IP 池

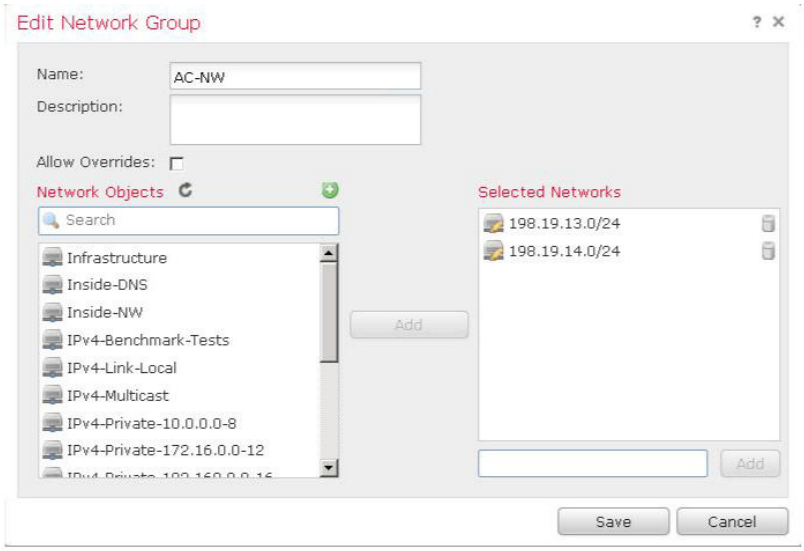
1. 创建 IP 池。
    a. 在 FMC 中，导航至**对象 > 对象管理 > 地址池 > IPv4 池**。
    b. 点击**添加 IPv4 池**。
    c. 在“名称”字段，输入 **AC-IP-Pool-IT**。由于 ISE 配置，这必须是确切的组名。
    d. 对于 **IPv4 地址范围**，输入 **198.19.14.10-198.19.14.50**。
    e. 在“掩码”字段，输入 **255.255.255.0**。
    f. 点击**保存**。



修改访问控制和 NAT 策略

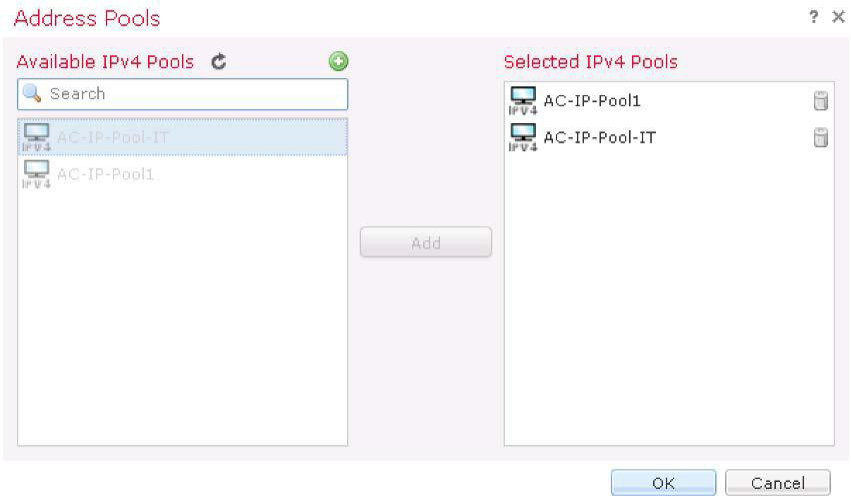
要同时修改访问控制策略和 NAT 策略，只需修改 **AC-NW** 网络组对象即可。

1. 在 FMC 中，导航至**对象 > 对象管理 > 网络**。
    a. 选择并编辑网络组 **AC-NW**。
    b. 在**所选网络**下的底部文本字段中，输入 **198.19.14.0/24**，然后点击**添加**。
    c. 点击**保存**。

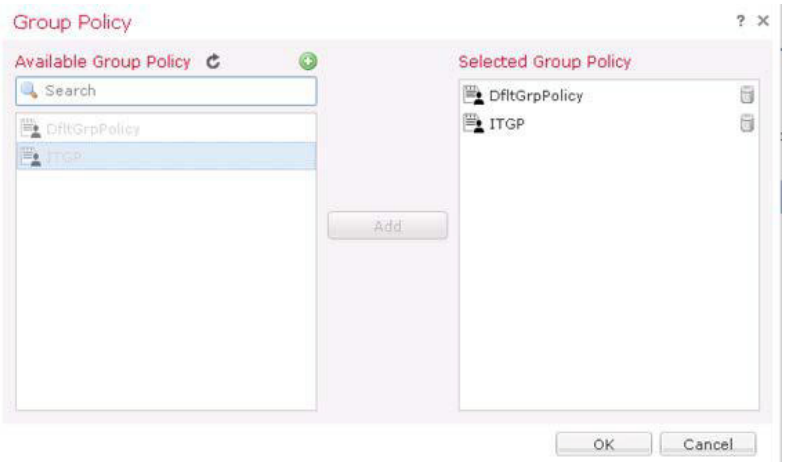


修改连接配置文件

1. 在 FMC 中，导航至**设备 > VPN > 远程接入**。
2. 编辑 **AnyConnect-VPN**。然后，选择并编辑 **AC-Default-Profile** 连接配置文件。
3. 添加新创建的 IP 池。
    a. 系统应已选择客户端**地址分配**选项卡。
    b. 在**地址池**下，点击 (**+**) 图标，然后选择 **IPv4**。
    c. 选择 **AC-IP-Pool-IT**，然后点击**添加**。



    d. 点击**确定**。
    e. 点击**编辑连接配置文件**窗口上的**保存**。
4. 添加新创建的组策略。
    a. 选择 AnyConnect-VPN 页面的**高级**选项卡，然后从左侧导航窗格中选择**组策略**。
    b. 点击 (**+**) 图标。
    c. 选择 **ITGP**，然后点击**添加**。



    d. 点击**确定**，然后点击**保存**。

部署和测试配置

1. 将更改部署到 NGFW。等待部署完成。
2. 返回到 Outside-PC 远程桌面会话。
    a. 点击 AnyConnect 客户端上的“连接”。

    b. 使用用户名 **harry** 和密码 **C1sco12345** 进行登录。Harry 不是 IT 组的成员。

    c. 连接 AnyConnect 后，从 Outside-PC 命令提示符运行以下两个命令。
        i. **ping inside.dcloud.local**。此命令应该会成功。
        ii. **ping altinside.dcloud.local**。此命令应该会失败。默认情况下，ISE 分配的 DACL 只允许访问域控制器和内部 Linux 服务器。

3. 在 NFGW CLI 上，运行以下命令。

   show vpn-sessiondb detail anyconnect

   观察输出上的以下值。

   a. 用户名：**harry**

   b. 分配的 IP：**198.19.13.x**

   c. 组策略：**DfltGrpPolicy**

   d. 过滤器名称：**#ACSACL#-IP-AC-DACL- Default-x**

```
> show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed
Username     : harry                  Index        : 53216
Assigned IP  : 198.19.13.10           Public IP    : 198.18.133.23
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15410                  Bytes Rx     : 516
Pkts Tx      : 16                     Pkts Rx      : 8
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : AC-Default-Profile
(省略部分输出)

> Filter
Name            : #ACSACL#-IP-AC-DACL-Default-598b5954
```

4. 返回到 Outside-PC 远程桌面会话。

   a. 断开 AnyConnect VPN 会话连接。

   b. 启动新 AnyConnect VPN 会话。

   c. 使用用户名 **rita** 和密码 **C1sco12345** 进行登录。Rita 是 IT 组的成员。

   d. 确认您看到在 ITGP 中配置的横幅，然后点击**接受**。

   e. 连接 AnyConnect 后，从 Outside-PC 命令提示符运行以下两个命令。

      i. **ping inside.dcloud.local**。此命令应该会成功。

      ii. **ping altinside.dcloud.local**。此命令也应成功。ISE 分配给 IT 组的 DACL 允许访问任何内部设备。

5. 在 NFGW CLI 上，运行以下命令。

   show vpn-sessiondb detail anyconnect

   观察输出上的以下值。

   a. 用户名：**rita**

   b. 分配的 IP：**198.18.14.x**

   c. 组策略：**ITGP**

   d. 过滤器名称：**#ACSACL#-IP-AC-DACL-IT-x**

```
> show vpn-sessiondb detail anyconnectInde
Username     : rita                    x            : 4998
Assigned IP  : 198.19.14.10            Public IP    : 198.18.133.23
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15375                   Bytes Rx     : 691
Pkts Tx      : 16                      Pkts Rx      : 9
Pkts Tx Drop : 0                       Pkts Rx Drop : 0
Group Policy : ITGP                    Tunnel Group : AC-Default-Profile (Output omitted)
 (Output omitted)

>
Filter   Name  : #ACSACL#-IP-AC-DACL-IT-598b1f19
```

6. 断开 AnyConnect VPN 客户端连接。

场景 5：具有客户端证书的 AnyConnect

此练习包含以下任务：

- 修改连接配置文件
- 部署和测试配置

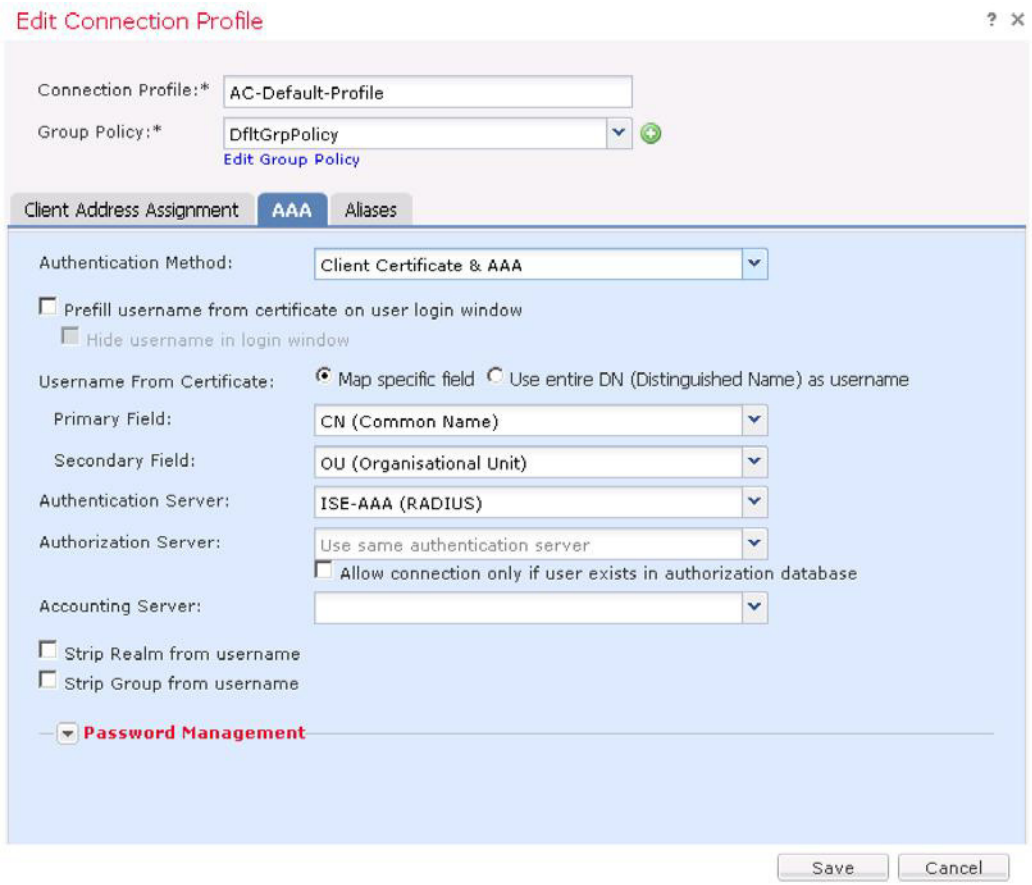
在此练习中，我们将帮助用户为 RA VPN 配置双重身份验证（证书和 AAA）。

注意：为节省时间，在 Outside-PC 上已安装客户端证书。

步骤

修改连接配置文件

1. 在 FMC 中，导航至**设备 > VPN > 远程接入**。编辑 **AnyConnect-VPN**。
    a. 在**连接配置文件**下，选择并编辑 **AC-Default-Profile** 连接配置文件。
    b. 选择 **AAA** 选项卡并将**身份验证方法**更改为**客户端证书和 AAA**。



    c. 在**编辑连接配置文件**页面上，点击**保存**。
    d. 在 **AnyConnect-VPN** 页面上，点击**保存**。

部署和测试配置

1. 将更改部署到 NGFW。等待部署完成。
2. 返回到 Outside-PC 远程桌面
    a. 连接 AnyConnect 客户端。
    b. 使用用户名 **rita** 和密码 **C1sco12345** 进行登录。用户对于此实验练习无关紧要。
3. 在 NFGW CLI 上，运行以下命令。
   show vpn-sessiondb detail anyconnect
   确认 Auth Mode 为 **Certificate and userPassword**。

```
> show vpn-sessiondb detail anyconnect
  (Output omitted)
AnyConnect-Parent:
  Tunnel ID     : 52614.1
  Public IP     : 198.18.133.23
  Encryption    : none                    Hashing       : none
  TCP Src Port : 49286                    TCP Dst Port : 443
  Auth Mode     : Certificate and userPassword


>(Output omitted)
```

4. **请勿断开 AnyConnect VPN 连接**。立即继续进行下一个实验练习。

场景 6：监控和故障排除

此练习包含以下任务：

- 监控 AnyConnect 用户活动
- 故障排除

您需要使用 AnyConnect 来监控 AnyConnect 用户活动和进行故障排除。

步骤

监控 AnyConnect 用户活动

在此部分中，您可以监控已通过 AnyConnect 登录的所有活动用户。

1. 在 FMC 中，导航至**概述 > 控制面板 > 访问受控用户统计信息**
2. 选择 **VPN** 选项卡。请注意，有 7 个专用于 VPN 流量的构件。
3. 导航至**分析 > 用户 > 活动会话**。
    a. 请注意，您会看到 Rita 的 VPN 会话。
    b. 选中 Rita 的会话左侧的复选框，然后点击**注销**。系统提示时，点击**继续**。

您还可能看到通过网络发现所发现的其他活动会话。例如，您可能会看到通过 FTP 会话发现的访客。为简洁起见，上图中省略了这些会话。如果您希望了解有关用户及其发现情况的详细信息，请导航至“分析”>“用户”>“用户”。

4. 在 Outside-PC 上，确认 Rita 已注销。
5. 在 FMC 中，导航至**分析 > 用户 > 用户活动**。在此窗口中，您将看到当前和过去用户会话的详细信息。花几分钟时间查看此页面上的信息。

故障排除

在此部分中，您需要修改 NGFW 上的 VPN 事件的系统日志级别。您还需要从 NGFW CLI 运行一些基本的故障排除命令。

1. 在 FMC 中，导航至**设备 > VPN > 故障排除**。您应该看到记录。如果看不到，请尝试调整此页面上的时间窗口。

2. 在 NGFW CLI 上，运行下列其中一些命令以获取故障排除功能的大致范围。下列命令有助于对 RA VPN 进行故障排除，主要用于参考用途。

    a. `show vpn-sessiondb ?`

    b. `test aaa-server ?`

    c. `debug crypto ca ? (good for trouble-shooting certificate issues)`

    d. `debug crypto ipsec ?`

    e. `debug ldap ?`

    f. `debug aaa ?`

场景 7：思科威胁情报导向器 (CTID)

此练习包含以下任务：

- 从 Web 服务器检索 STIX 文件
- 分析复杂指标及其关联的可观察对象
- 将 URL 列表上传到将触发事件的 CTID
- 使 CTID 订用 TAXII 源
- 生成 CTID 事件

CTID 是可以使用第三方网络威胁情报指标的 FMC 的一个组件；CTID 可以解析这些指标，以产生 NGFW 可以检测的可观察对象。NGFW 将对于可观察对象的检测报告给 CTID。然后，CTID 确定观察是否构成事件。

它支持两种文件格式。

- 平面文件 - 简单指标的列表，例如 IP 地址、URL 或 SHA256 散列
- STIX 文件 - 可以描述简单或复杂指标的 XML 文件

有 3 种方法可以检索这些文件

- 从正在运行 FMC UI 的计算机上传
- 从远程 Web 服务器上的 URL 检索
- 从 TAXII 源接收（仅限 STIX 文件）

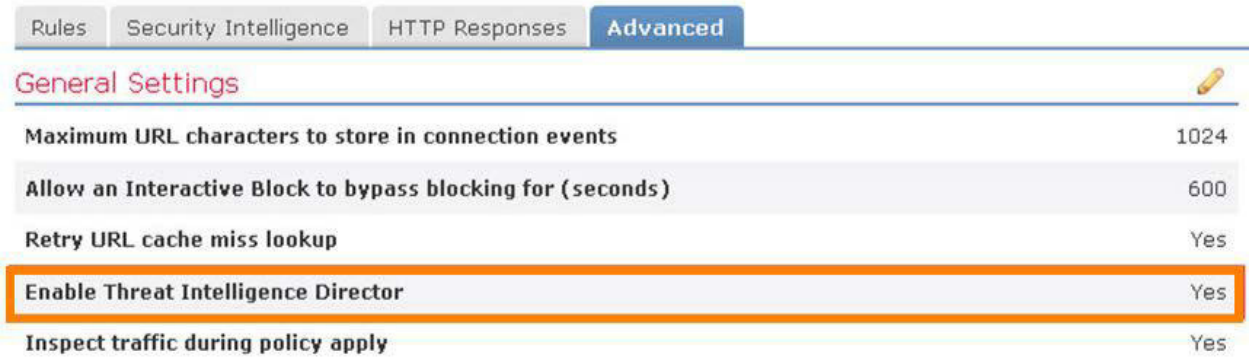
此练习旨在配置和测试 CTID。

步骤

确认 CTID 会将可观察对象发布到 NGFW

1. 导航至**策略 > 访问控制 > 访问控制**。
2. 点击该访问控制策略右侧的**铅笔图标**即可进行编辑。
3. 选择**高级**选项卡。

4. 观察默认情况下是否启用了**启用威胁情报导向器**。

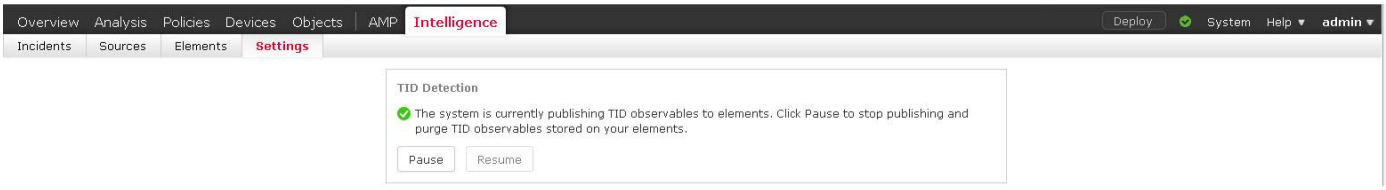


5. 使用此高级设置，可以在访问策略级别启用或禁用 CTID。

6. 导航至**情报 > 元素**。

7. 确认 **NGFW** 是一个元素。这意味着 CTID 可以将可观察对象发布到 NGFW。

8. 导航至**情报 > 设置**。确认系统配置为将可观察对象发布到 CTID 元素。



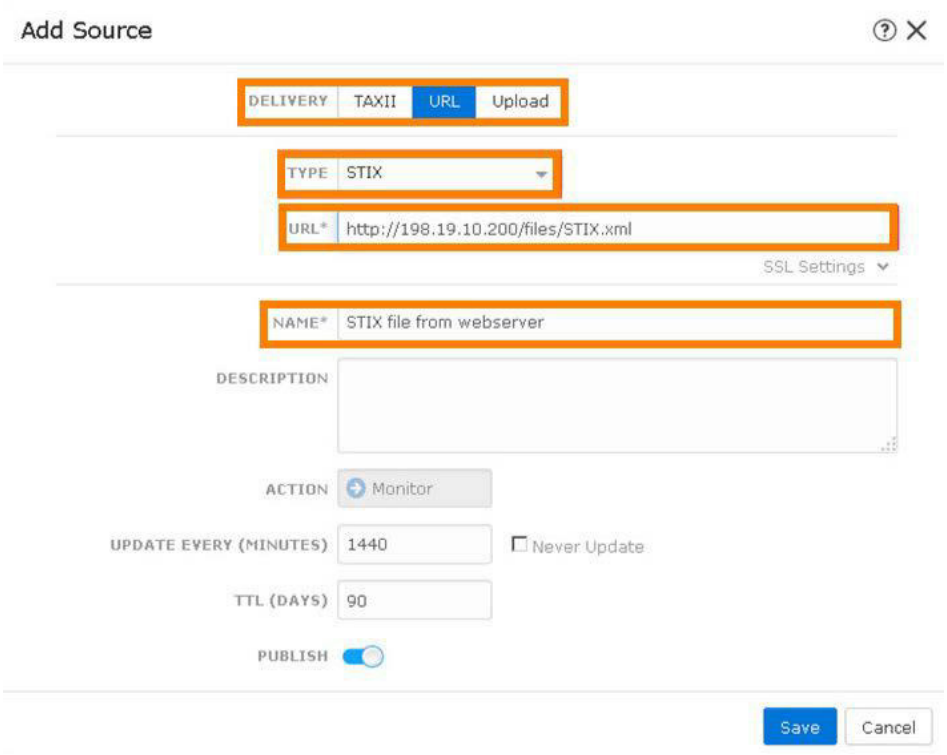
注意：此处可以全局启用或禁用 CTID。点击“暂停”将停止 CTID 向所有元素进行发布。

从 Web 服务器检索 STIX 文件

1. 导航至**情报 > 来源 > 来源**。

2. 点击右侧的加号 (**+**) 以添加情报来源。

3. 对于**交付**，选择 **URL**。
4. 对于**类型**，确认选择 **STIX**。
5. 在 **URL** 字段，输入 **`http://198.19.10.200/files/STIX.xml`**。
6. 在**名称**字段，输入 **`STIX file from webserver。`** .



7. 点击**保存**。

注意：不能将 STIX 文件的操作从“监控”更改为“阻止”。STIX 文件可以显示复杂指标，因此 NGFW 无法根据可观察对象来决定是否满足指标的条件。

但是，即使对于复杂指标，也可以将个别可观察对象的操作设置为“阻止”。

8. 等待几秒钟。导航至**情报 > 来源 > 指标**。确认已添加复杂指标。
9. 点击该指标的名称 **Weatherman PUA**。观察指标的详细信息。
10. 点击**关闭**以关闭“指标详细信息”页面。
11. 导航至**情报 > 来源 > 可观察对象**。确认已添加两个 SHA-256 和一个 IPv4 可观察对象。

将 URL 列表上传到将触发事件的 CTID

1. 导航至**情报 > 来源 > 来源**。点击右侧的加号 (**+**) 以添加情报来源。
2. 对于**交付**，选择**上传**。
3. 对于**类型**，选择**平面文件**。系统将显示**内容**下拉列表。
4. 对于**内容**，选择 **URL**。
5. 在**文件**区域中点击，然后从 Jump Desktop 上的 **Files** 文件夹中选择 **URL_LIST.txt**。
6. 在**名称**字段，输入 **`Local URL list`**。
7. 对于**操作**，选择**阻止**。

8. 点击**保存**。
9. 等待几秒钟。导航至**情报 > 来源 > 指标**。确认已添加两个 URL 指标。
10. 导航至**情报 > 来源 > 可观察对象**。确认已添加两个类型的 URL 可观察对象。

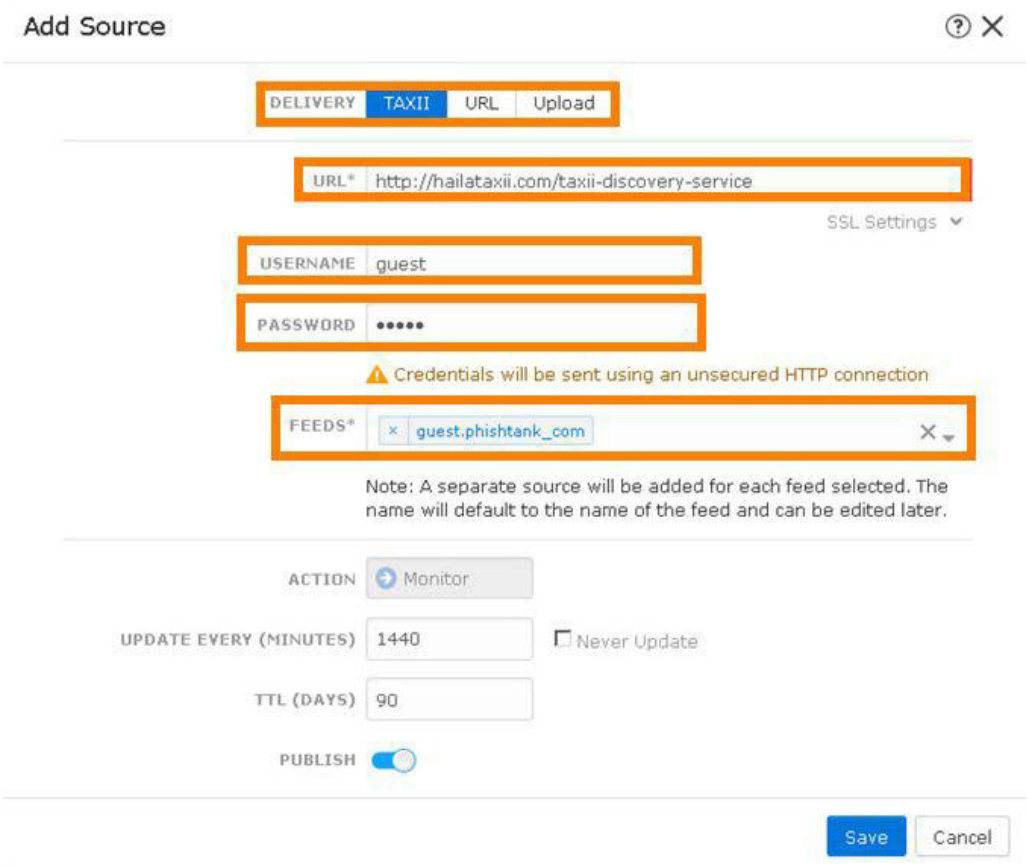
使 CTID 订用 TAXII 源

注意：此处使用的 TAXII 源来自 Hail a TAXII。如果您对这些源有疑问，可以使用 Alien Vault。有关详细信息，请参阅附录 D。

1. 导航至**情报 > 来源 > 来源**。点击右侧的加号 (**+**) 以添加情报来源。
2. 对于**交付**，选择 **TAXII**。
3. 在 **URL** 字段，输入 **`http://hailataxii.com/taxii-discovery-service`**。
4. 在**用户名**字段，输入 **guest**。
5. 在**密码**字段，输入 **`guest`**。
6. 对于**源**，选择 **guest_phishtank_com**。

注意：填充“源”下拉列表可能需要几秒钟时间。

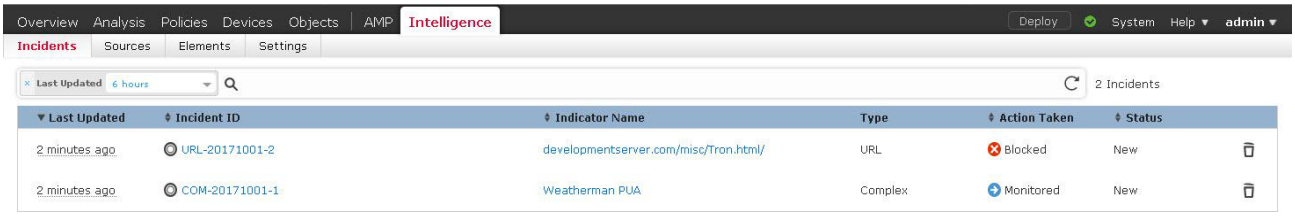
7. 确认屏幕如下图所示。



8. 点击**保存**。
9. 等待直至此源的“状态”列更改为**正在解析**。不要等待解析完成，这将花费太长时间。
10. 导航至**情报 > 来源 > 指标**。确认已添加多个 URL 指标。
11. 导航至**情报 > 来源 > 可观察对象**。确认已添加多个 URL 可观察对象。

生成 CTID 事件

1. 在 FMC 上有一个后台守护程序，它每 5 分钟将可观察对象与 NGFM 同步一次。因此，将可观察对象发布到传感器可能需要几分钟时间。在此步骤中，您将看到如何发布特定可观察对象。在 NGFW CLI 中，执行以下操作：
    a. 键入 **expert** 以进入专家模式。
    b. 键入 **ls -d /var/sf/*download**。请注意，已列出多个目录。
    ```
    admin@ngfw:~$ ls -d /var/sf/*download
    /var/sf/clamupd_download  /var/sf/iprep_download  /var/sf/sifile_download
    /var/sf/cloud_download/var/sf/sidns_download  /var/sf/siurl_download
    ```
    其中四个目录（iprep_download、sidns_download、sifile_download 和 siurl_download）供安全情报和 CTID 使用。
    c. 键入 grep **developmentserver /var/sf/*download/*lf**
    ```
    admin@ngfw:~$ grep developmentserver /var/sf/*download/*lf
    /var/sf/siurl_download/731625d4-9512-11e7-915c-
    7e7252ae92ac.lf:developmentserver.com/misc/Tron.html/
    ```
    如果您看不到此内容，请稍候，然后重试。必须等待发布此内容，然后再继续操作。如果仍然失败，请删除 CTID 源，然后将其重新添加。
    d. 键入 **grep 198.18.133.200 /var/sf/*download/*lf**
    ```
    admin@ngfw:~$ grep 198.18.133.200 /var/sf/*download/*lf
    /var/sf/iprep_download/730f187a-9512-11e7-915c-7e7252ae92ac.blf:198.18.133.200
    ```
    如果您看不到此内容，请稍候，然后重试。必须等待发布此内容，然后再继续操作。如果仍然失败，请删除 CTID 源，然后将其重新添加。
    e. 键入 **exit** 以退出专家模式。
2. 在内部 Linux 服务器 CLI 上：
    a. 运行 **wget -t 1 outside/files/ProjectX.doc**。此命令应该会成功。
    b. 运行 **wget -t 1 developmentserver.com/misc/Tron.html**。此操作应该会受阻止。
3. 在 FMC 上，导航至 ***情报 > 事件***。确认有 2 个事件。



4. 深入查看事件并观察此事件的详细信息。
5. 确认 URL 指标存在对应的事件。深入查看事件并观察此事件的详细信息。

场景 8：FlexConfig

此练习包含以下任务：

- 创建用户定义的 FlexConfig 对象
- 修改在系统定义的 FlexConfig 对象中使用的文本对象
- 创建并配置 FlexConfig 策略
- 部署更改并测试配置

FlexConfig 是允许将配置直接部署到 FTD 中的 Lina (ASA) 配置的功能。这可用于部署 FTD 中还不可用的功能。此实验练习有两个目标：

- 使用用户定义的 FlexConfig 对象来配置 EIGRP。
- 使用系统定义的 FlexConfig 对象来禁用 SIP 检查。

注意：存在用于配置 EIGRP 的单独的系统定义 FlexConfig 对象。对于可能随时间更改的配置，最好使用这些对象。但是为演示 FlexConfig 的简易性和功能，将使用用户定义的 FlexConfig 对象。

系统定义的 FlexConfig 对象将用于将 FTD 配置为 NetFlow 数据源。

创建用户定义的 FlexConfig 对象

1. 在 FMC UI 中，导航至**对象 > 对象管理**。
2. 在左侧导航面板的底部，在 **FlexConfig** 下选择 **FlexConfig 对象**。
3. 点击**添加 FlexConfig 对象**。
    a. 在“名称”字段，输入 **myEIGRP**。
    b. 在主文本区域中，输入以下命令。请注意，网络掩码为 /18 而不是 /24。

```
router eigrp 10
 network 198.18.128.0 255.255.192.0
```

    c. 点击**保存**。

修改系统定义的 FlexConfig 对象的文本对象

1. 您应该仍然处在 FMC UI 中的**对象管理**页面上。
2. 点击名为 **Default_Inspect_Protocol_Disable** 的 Flex 对象右侧的放大镜图标。您无法编辑此对象，但是需要时可以复制。

注意：FlexConfig 对象使用 Apache Velocity 语言编写而成。此语言支持循环和 if 语句。这些语句以 # 开头。这不是注释。它指示该行不是要包含在输出中的文字文本。注释以 ## 开头。

请注意，此 FlexConfig 对象在名为 **disableInspectProtocolList** 的文本对象上循环。现在，您将编辑此文本对象。

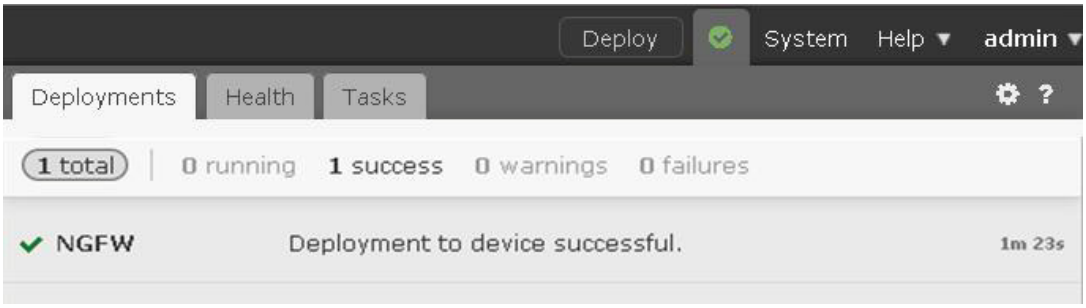
3. 点击**关闭**。
4. 在**对象管理**页面的左侧导航窗格的底部，在 **FlexConfig** 下选择**文本对象。**
5. 编辑名为 **disableInspectProtocolList** 的文本对象。
6. 此变量可采用多个值。保持将值设置为 **1**。
7. 输入值 `sip`。
8. 点击**保存**。

创建并配置 FlexConfig 策略

1. 导航至**设备 > FlexConfig**。点击**新建策略**。
    a. 在**名称**字段，输入 `NGFW Flex Policy`。
    b. 选择设备 **NGFW**。点击**添加到策略**。
    c. 点击**保存**。
2. 等待几秒钟以打开该策略进行编辑。
    a. 在左列中的**用户定义**下，选择 **myEIGRP**。点击 > 以将 FlexConfig 对象添加到策略中。
    b. 在左列中的**系统定义**下，选择 **Default_Inspect_Protocol_Disable**。点击 > 以将 FlexConfig 对象添加到策略中。
    c. 点击**保存**。
3. 点击**预览配置**。
    a. 从**选择设备**下拉列表中选择 **NGFW**。
    b. 等待几秒钟，然后将显示配置更改。确认命令是否正确。您还将看到多个多余的 VPN 命令。此缺陷对于配置没有影响，并将在未来版本中进行更正。
    c. 点击**关闭**。

部署更改并测试配置

1. 从 NGFW CLI 运行 **show running-config policy-map**。确认已启用 SIP 检查。
2. 从内部 Linux 服务器会话中，键入 **ping 204.44.14.1**。此命令应该会失败。
3. 部署所做的更改。等待直至部署完成。



4. 从 NGFW CLI 运行 **show running-config policy-map**。确认现已禁用 SIP 检查。
5. 从 NGFW CLI 运行以下命令。
    a. 运行 **show eigrp neighbors**。确认 FTD 和 CSR 路由器之间已形成邻接。
    b. 运行 **show eigrp topology**。确认已接收到 EIGRP 路由。
    c. 运行 **show route eigrp**。确认 NGFW 现在在其路由表中具有 EIGRP 获知的路由。
6. 从内部 Linux 服务器会话中，键入 **ping 204.44.14.1**。此命令现在应该成功。

场景 9：ASA 到 NGFW 的迁移

此练习包含以下任务：

- 将 FMC 转换为迁移工具
- 迁移 ASA 对象
- 迁移 NAT 和不受支持的功能，并探索对象的重复使用

此练习的目标是使学生熟悉迁移工具。

- 如何配置
- 如何使用

在 FMC 转换为迁移工具后，将迁移两个配置。我们将揭示迁移的多个方面，包括对象拼合以及如何处理不受支持的功能。

步骤

将 FMC 转换为迁移工具

1. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为**迁移程序**的预配置会话。使用用户名 **admin** 和密码 **C1sco12345** 登录。

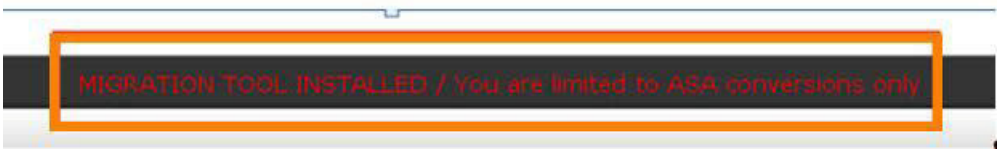
注意：执行迁移所需的工具是修改后的 FMC。通过运行脚本来完成修改。此 FMC 通常是与生产 FMC 分开的虚拟 FMC，您不应尝试使用生产 FMC 作为迁移工具。

2. 键入 **sudo enableMigrationTool.pl**。
    a. 出现提示时，输入密码 **C1sco12345**。
    b. 阅读警告 - 不错，仔细阅读！
    c. 当询问您是否要继续时，输入 **Y**。
    d. 等待脚本完成。这将需要不到一分钟时间。
3. 在 Firefox 浏览器上，打开新标签。
    a. 点击书签栏链接**迁移工具**。点击**高级**，然后点击**添加例外**。出现提示时，点击**确认安全接受**。

注意：用作迁移工具的此 FMC 在安装后未修改。您迄今为止使用的 FMC 是预配置。此预配置包括添加可信证书。有关详细信息，请参阅附录 A。

    b. 使用用户名 **admin** 和密码 **C1sco12345** 登录。

c. 确认您在 UI 顶部看到红色横幅，其内容如下：
迁移工具已安装/仅限于 ASA 转换

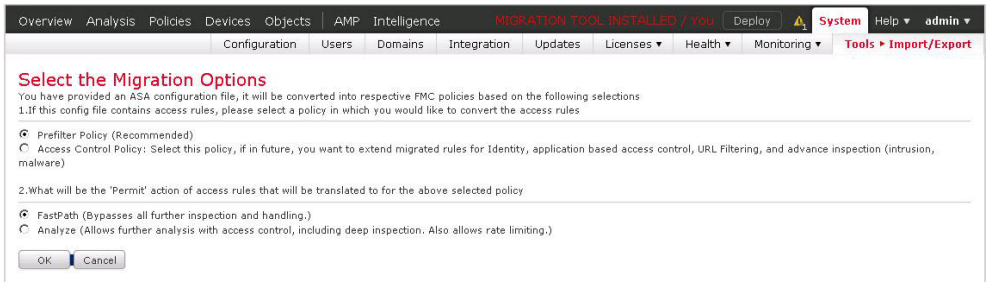


迁移 ASA 对象

此练习的目标如下。

- 了解迁移过程。
- 了解网络和服务对象及对象组的迁移方式。

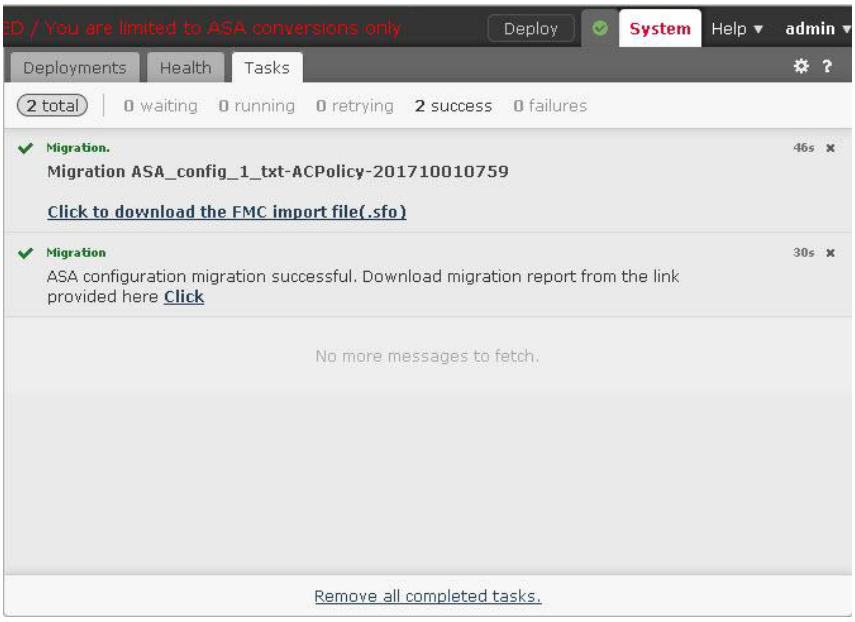
1. 在 Jump 上的 Files 文件夹中，打开文件 **ASA_config_1.txt**。
   a. 观察是否有嵌套的网络和服务对象。
   b. 观察是否有引用这些对象的访问列表和访问组。如果没有访问组，则对象将不会迁移，因为它们对于策略配置不会有任何影响。
2. 在迁移程序 UI（不是 FMC）中，导航至**系统 > 工具 > 导入/导出**。
   a. 点击**上传软件包**。
   b. 点击**浏览**，然后从 **Files** 文件夹中选择文件 **ASA_config_1.txt**。
   c. 点击**上传**。
3. 在下一页上，保持所有设置不变，如下所示，然后点击**确定**。



4. 等待直至返回到**上传**页面。

    a. 点击**部署**按钮右侧的图标。

    b. 点击**任务**选项卡并等待任务完成。



    c. 点击文本**点击下载 FMC 导入文件 (.sfo)** 并保存 SFO 文件。

    d. 点击文本**点击**，然后选择默认值**使用 Google Chrome 打开**以在新标签中打开迁移报告。确认转换报告不含任何错误。关闭 Chrome。

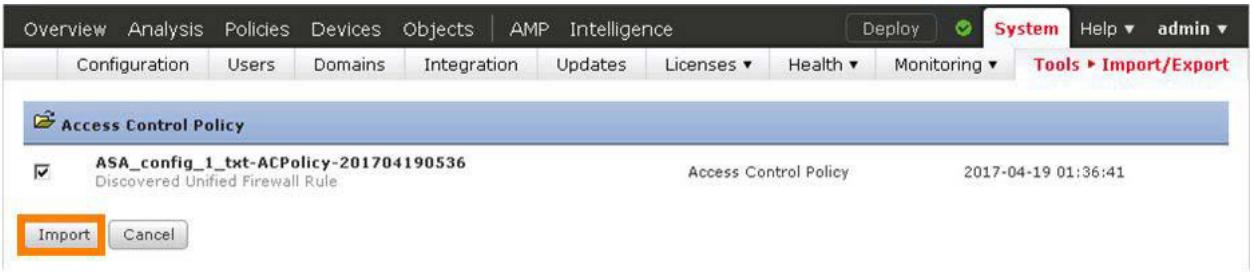
5. 在（生产）FMC UI 中，导航至**系统 > 工具 > 导入/导出**。

    a. 点击**上传软件包**。

    b. 点击**浏览**，然后从 **Downloads** 文件夹中选择 SFO 文件。它将具有格式为 **ExportForMigration-<some UUID>.sfo** 的名称。点击**打开**。

    c. 点击**上传**。

6. 在下一页上，点击**导入**。



7. 等待导入完成。

8. 导航至**对象 > 对象管理**。

   a. 系统将选择**网络**对象页面。请注意所创建的对象。

      - 四个网络对象 **net1**、**net2**、**net3** 和 **net4**
      - 两个网络组 **net12** 和 **net34**
      - 一个嵌套网络组 **net1234**

注意：这些正是在 ASA 配置中存在的网络对象和网络组对象。

   b. 在左侧导航窗格中，选择**端口**。请注意所创建的对象。

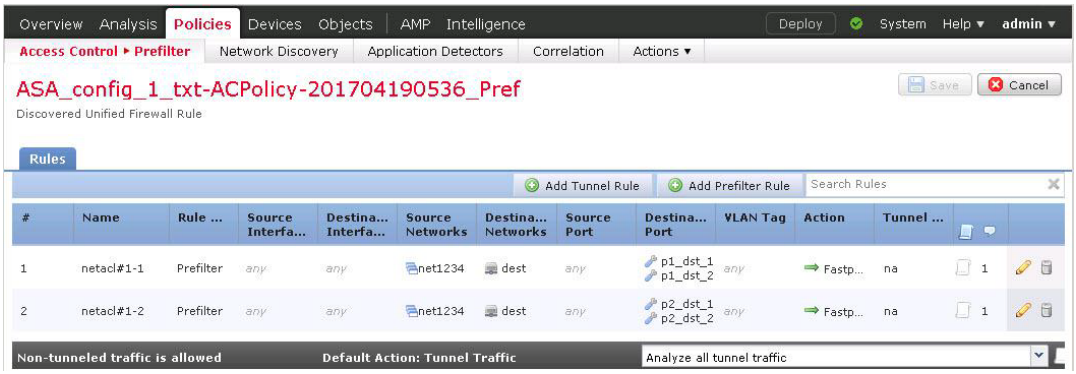
      - 四个端口对象 **p1_dst_1**、**p1_dst_2**、**p2_dst_1** 和 **p2_dst_2**
      - 零个端口组

注意：ASA 端口组 p1 和 p2 已拼合，并且没有 p12。

9. 导航至**策略 > 访问控制 > 预过滤**。

   a. 请注意，存在新的预过滤策略。编辑该策略，从而可以检查规则。

   b. 请注意，此单一 ACE 现在是由 2 个单独预过滤规则组成的 ASA 配置。



10. 导航至**策略 > 访问控制 > 访问控制**。

   a. 请注意，存在新的访问控制策略。编辑该策略，从而可以对其进行检查。

   b. 请注意，没有任何规则，并且默认操作设置为“阻止”。

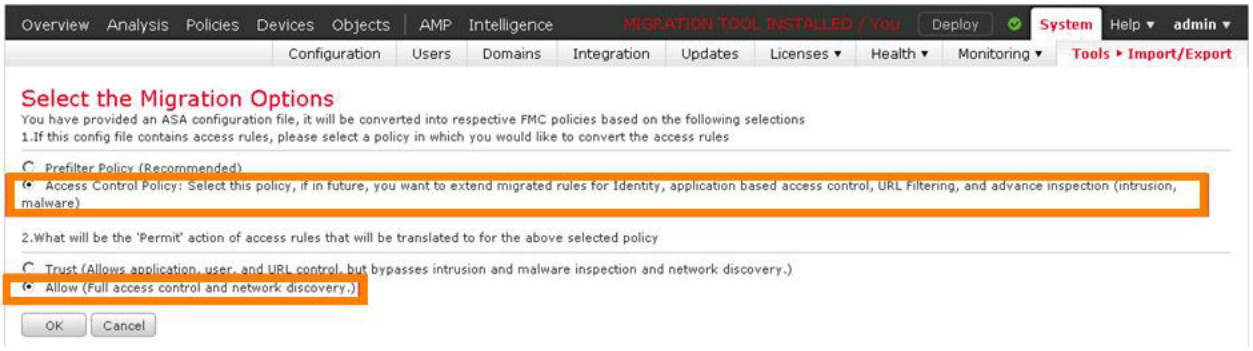
   c. 请注意，预过滤策略设置为上一步中检查的预过滤策略。

迁移 NAT 和不受支持的功能，并探索对象的重复使用

在此任务中有三个单独的目标。它们不直接相关。将它们放在一起只是为了方便起见。

- 迁移 NAT 策略。
- 了解对象的重复使用。
- 尝试迁移基于时间的 ACL，并了解如何处理不受支持的功能。

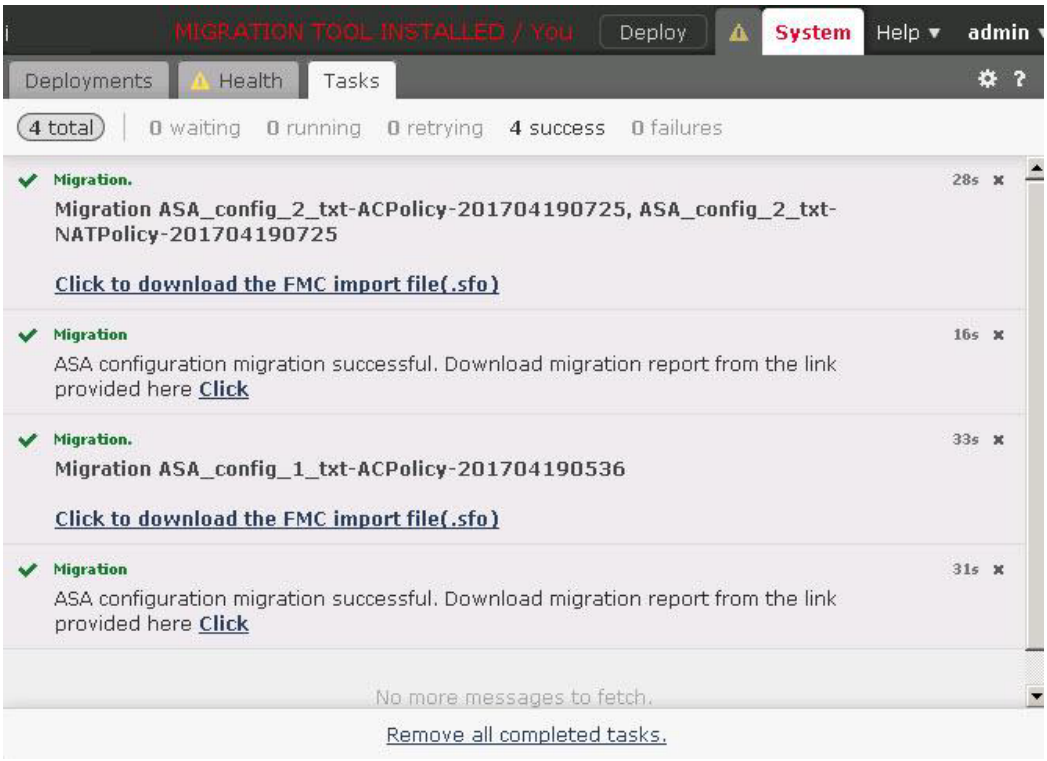
1. 在 Jump 上的 **Files** 文件夹中，打开文件 **ASA_config_2.txt**。
    a. 观察在 FMC 中是否已经存在 ASA 配置中的两个网络对象。
        - 网络对象 **net1**，它具有与同名的现有对象不同的定义
        - 网络对象 **net2**，它具有与同名的现有对象相同的定义
    b. 观察是否存在静态 NAT 规则
    c. 观察是否存在基于时间的 ACL。此功能当前不受支持。
2. 在迁移程序 UI（不是 FMC）中，导航至**系统 > 工具 > 导入/导出**。
    a. 点击**上传软件包**。
    b. 点击**浏览**，然后从 **Files** 文件夹中选择 **ASA_config_2.txt**。点击**打开**。
    c. 点击**上传**。
3. 在下一页上，选中**访问控制策略**和**允许**单选按钮，如下所示。点击**确定**。



4. 您将返回到上传页面。

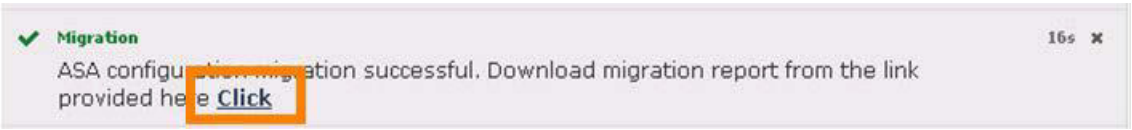
    a. 点击**部署**按钮右侧的图标。

    b. 点击**任务**选项卡并等待任务完成。



    c. 点击文本**点击下载 FMC 导入文件 (.sfo)** 并保存 SFO 文件。

    d. 点击文本**点击**，然后选择默认值**使用 Google Chrome 打开**以在新标签中打开迁移报告。观察此迁移报告是否发出警告，提示不支持基于时间的 ACL。关闭 Chrome。



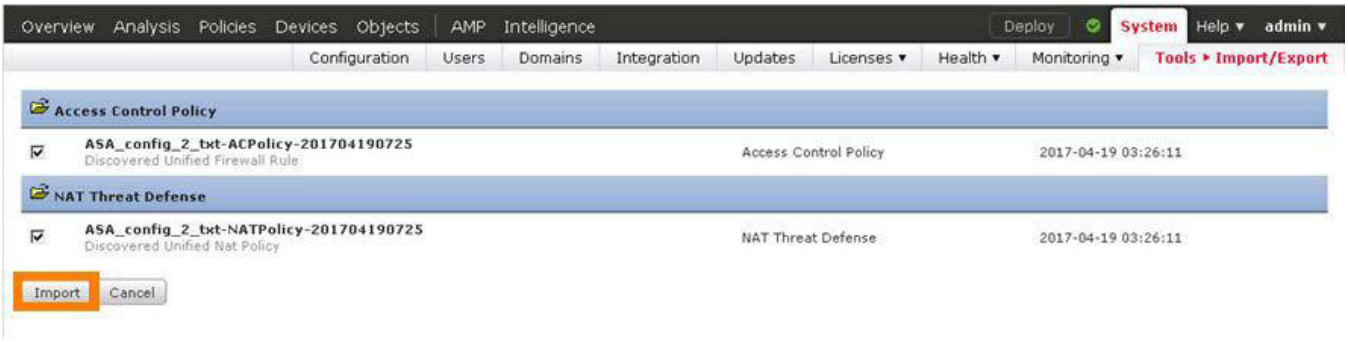
5. 在（生产）FMC UI 中，导航至**系统 > 工具 > 导入/导出**。

   a. 点击**上传软件包**按钮。

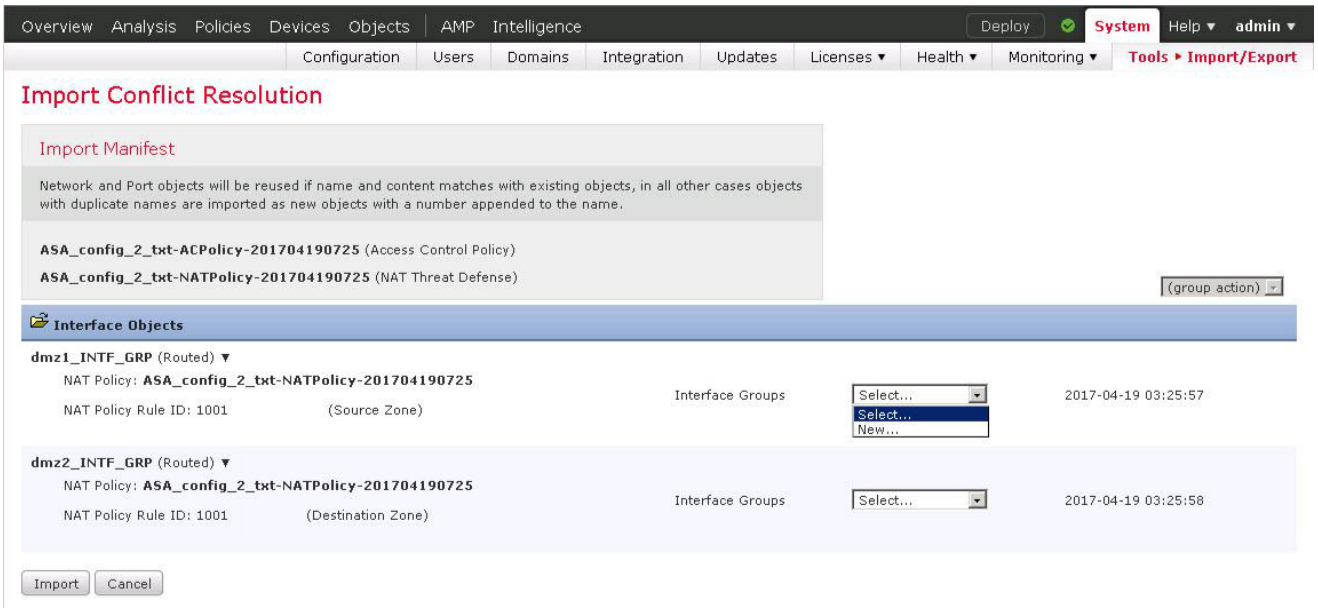
   b. 点击**浏览**，然后从 Downloads 文件夹中选择 SFO。它将具有格式为 **ExportForMigration-<some UUID>.sfo** 的名称。请务必选择最近创建的 SFO 文件。

   c. 点击**上传**。

6. 在下一页上，点击**导入**。



7. 在下一页上执行以下子步骤。请参阅下图。



   a. 阅读有关对象冲突解决方法的信息

   b. 使用此页面上的下拉列表创建两个接口组。已迁移的 NAT 规则中的接口引用必须放在接口组中。不允许使用安全区域。您可能会将其称为 **`IF1`** 和 **`IF2`**

   c. 点击**导入**。

8. 导航至**对象 > 对象管理**。系统将选择**网络**对象页面。

    a. 请注意，已创建对象 **net1_1**。这是因为 **net1** 的定义在两个已迁移的 ASA 配置中不同。因此，该对象进行了重命名。

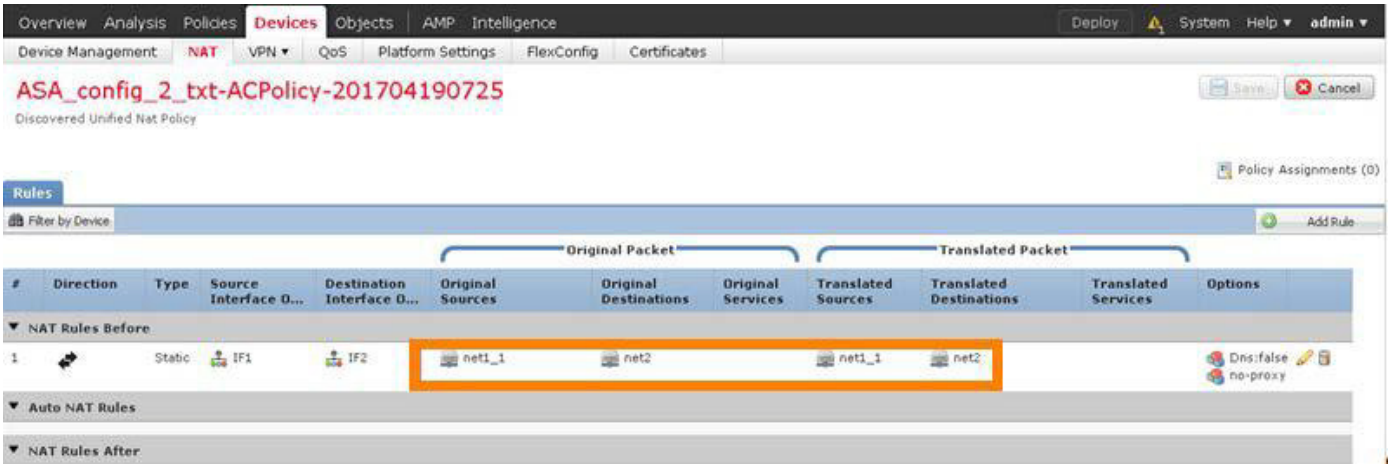
    b. 请注意，未创建对象 **net2_1**。这是因为 **net2** 的定义在两个已迁移的 ASA 配置中相同。因此，该对象进行了重用。

注意：此行为在 Firepower 6.2.1 版本中发生了更改。在 Firepower 6.2 中，两个对象均进行了重命名。

9. 导航至**设备 > NAT**。

    a. 请注意，存在新的 NAT 策略。编辑该策略，从而可以检查规则。

    b. 请注意，在此策略中引用了对象 **net1_1** 和 **net2**。

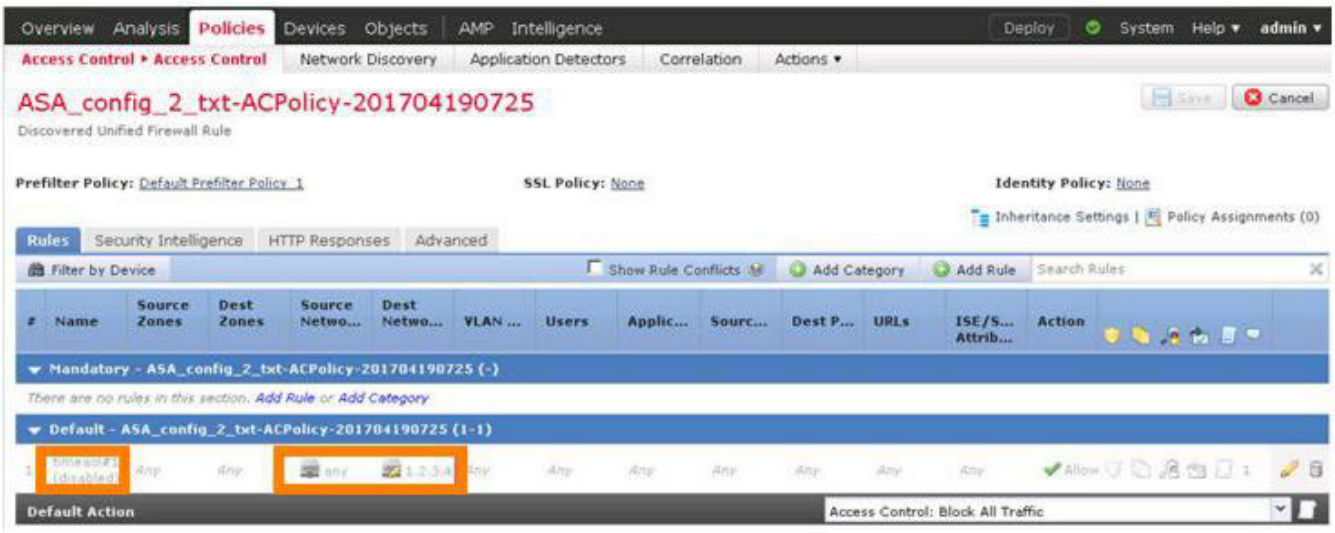


10. 导航至**策略 > 访问控制 > 访问控制**。

    a. 请注意，存在新的访问控制策略。编辑该策略，从而可以检查规则。

    b. 来自原始 ASA 配置的 ACL 如下：
    access-list timeacl extended permit ip any host 1.2.3.4 time-range office_hours
    请注意，这已转换为具有相同源和目标的访问控制策略规则。但是，在访问控制策略规则中没有时间范围属性。

c. 请注意，该规则已禁用。如果您愿意，可以启用该规则。



注意：迁移工具附带 ACL，其中同时包含网络条件和基于时间的的条件。由于当前不支持基于时间的 ACL，因此迁移规则可能仅包含网络条件。由于这可能不可接受，因此该规则已禁用，并且必须手动启用。

场景 10：NAT 和路由

此练习包含以下任务：

- 创建此实验练习所需的对象
- 配置静态 NAT
- 修改访问控制策略以允许对 wwwin 进行外部访问
- 配置 BGP
- 部署更改并测试配置
- 创建公共 Web 服务器
- 配置 BGP

第一个目标将涉及创建网络对象，从而创建访问控制列表。此外，还将配置静态 NAT 和动态路由。

步骤

创建此实验练习所需的对象

1. 导航至**对象 > 对象管理**。系统将选择**网络**对象页面。
    a. 点击**添加网络 > 添加对象**。
    b. 在**名称**字段，输入 **wwwin**。
    c. 在**网络**字段，输入 **198.19.10.202**。
    d. 点击**保存**。
    e. 点击**添加网络 > 添加对象**。
    f. 在**名称**字段，输入 **wwwout**。
    g. 在网络字段，输入 **198.18.128.202**。
    h. 点击**保存**。
    i. 点击**添加网络 > 添加对象**。
    j. 在**名称**字段，输入 **203.14.10.0**。
    k. 在**网络**字段，输入 **203.14.10.0/24**。
    l. 点击**保存**。

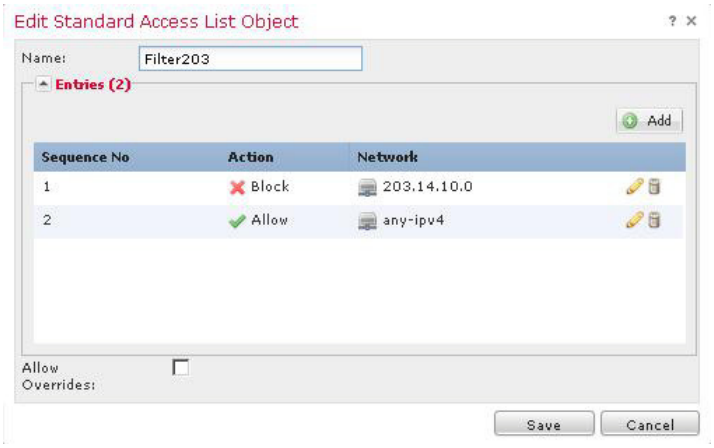
2. 从左侧导航窗格中选择**访问列表 > 标准**。

    a. 点击**添加标准访问列表**。

    b. 在**名称**字段，输入 **Filter203**。

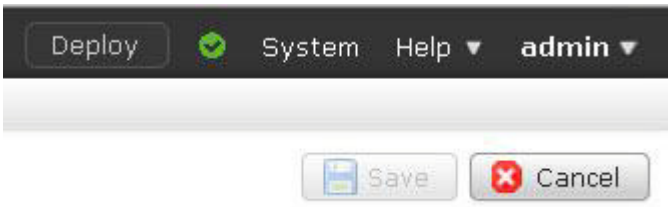
    c. 添加下面显示的 2 个访问控制条目。第二个条目至关重要，因为在列表的末尾有一个隐式的全部拒绝。

    d. 点击**保存**。



配置静态 NAT

1. 导航至**设备 > NAT**。
2. 点击铅笔图标以编辑**默认 PAT** 策略。确认在右上方看到灰显的**保存**按钮。如果看不到，请导航离开并重试编辑。这是已知漏洞。

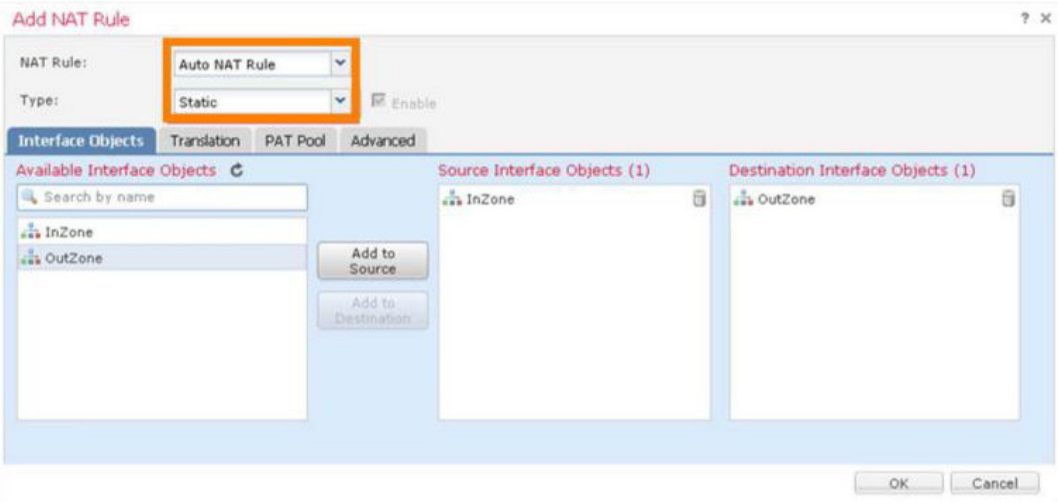


3. 点击**添加规则**。

    a. 从**类型**下拉列表中选择**自动 NAT 规则**。

    b. 您将进入“接口对象”选项卡。选择 **InZone**，然后点击**添加到源**。
    如果您执行了迁移方案，则还可以选择两个接口组。可以将其忽略。

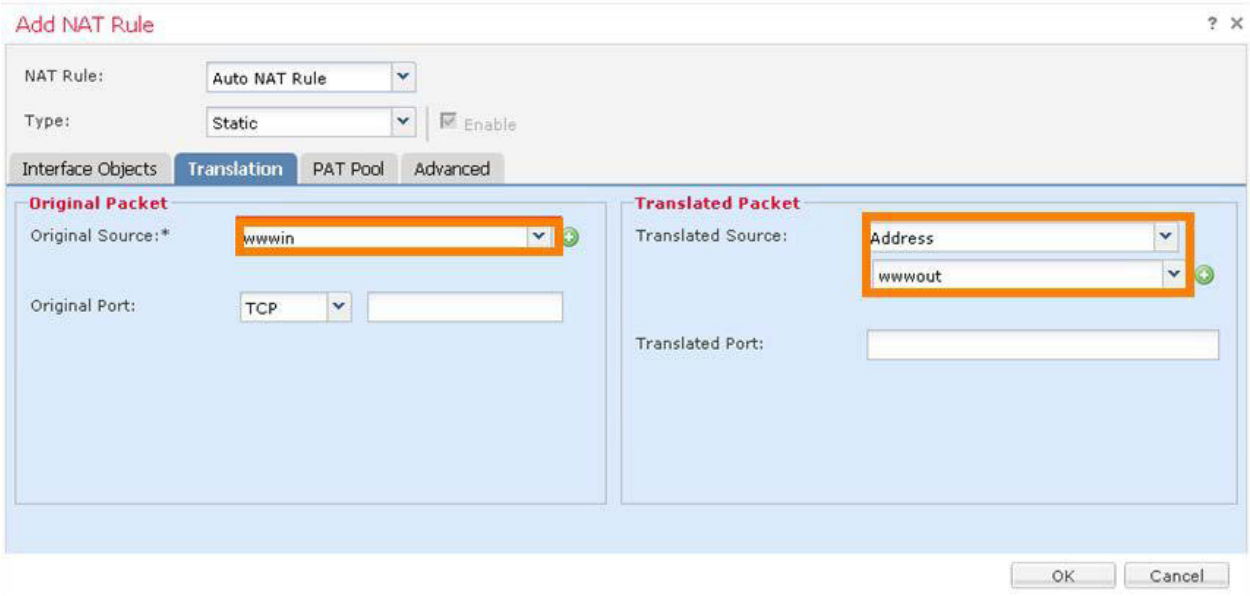
    c. 选择 **OutZone**，然后点击**添加到目的地**。



d. 选择**转换**选项卡。

e. 从**原始源**下拉列表中选择 **wwwin**。

f. 从**已转换的源**下拉列表中选择**地址**和 **wwwout**。



g. 点击**确定**以保存 NAT 规则。

4. 点击**保存**以保存 NAT 策略。

修改访问控制策略以允许对 wwwin 进行外部访问

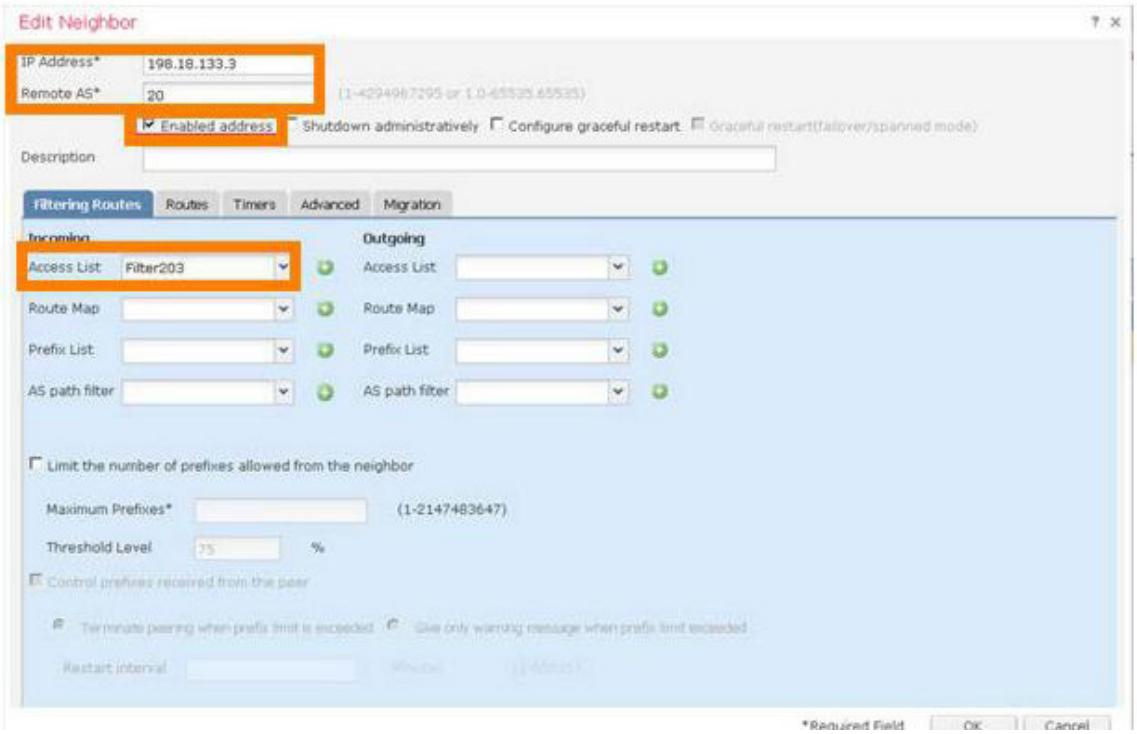
1. 导航至**策略 > 访问控制 > 访问控制**。编辑 **NGFW 访问控制策略**。
2. 点击“添加规则”。
    a. 在“名称”字段，输入 **Web Server Access**。
    b. 从“插入”下拉列表中选择**插入到默认规则集**。
    c. 系统应已选择**区域**选项卡。选择 **InZone**，然后点击**添加到目的地**。
    d. 选择 **OutZone**，然后点击**添加到源**。
    e. 选择**网络**选项卡。
    f. 选择 **wwwin**，然后点击**添加到目的地**。

注意：请注意，我们使用的是 Web 服务器的真实 IP，而不是客户端将连接到的经过 NAT 转换的地址。

    g. 选择**端口**选项卡。
    h. 选择 **HTTP** 和 **HTTPS**，然后点击**添加到目的地**。
    i. 选择**检查**选项卡。
    j. 从**入侵策略**下拉列表中选择**演示入侵策略**。
    k. 从**文件策略**下拉列表中选择**演示文件策略**。
    l. 点击**添加**以添加规则。
3. 点击**保存**以保存访问控制策略更改。

配置 BGP

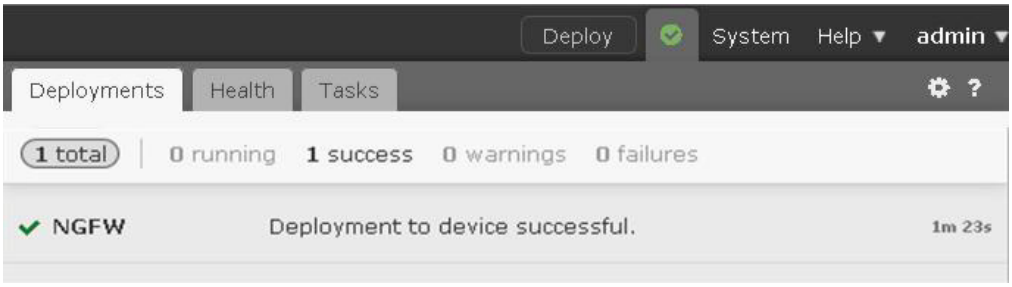
1. 导航至**设备 > 设备管理**。
2. 点击铅笔图标以编辑设备 **NGFW** 的设备设置。
3. 选择**路由**选项卡。
    a. 选择 **BGP**，然后选中**启用 BGP** 复选框。
    b. 将 **AS 编号**设置为 **10**。
    c. 展开左侧导航窗格中的 **BGP**，然后选择 **IPv4**。
    d. 选中**启用 IPv4** 复选框。
    e. 点击**邻居**选项卡，然后点击**添加**。
        i. 对于 **IP 地址**，输入 **198.18.133.3**。
        ii. 对于**远程 AS**，输入 **20**。
        iii. 选中**启用地址**复选框。
        iv. 从“传入访问列表”下拉列表中选择 **Filter203**。
        v. 点击**确定**以添加邻居。



f. 点击**保存**以保存 BGP 配置。

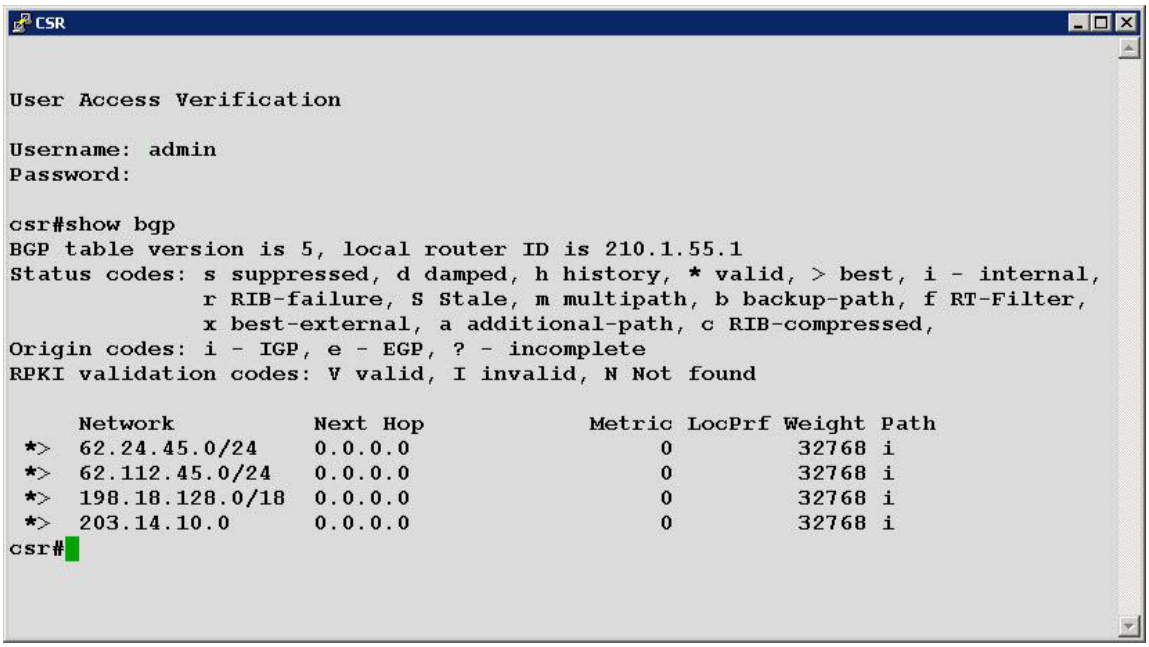
部署更改并测试配置

1. 部署更改，然后等待直至部署完成。



2. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为**外部 Linux 服务器**的预配置会话。使用用户名 **root** 和密码 **C1sco12345** 登录。
    a. 键入 **curl wwwout**。此命令应该会成功。
    b. 键入 **ssh wwwout**。此命令应该会失败。
3. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为 **CSR** 的预配置会话。使用用户名 **admin** 和密码 **C1sco12345** 登录。

4. 在 CSR CLI 上，运行命令 **show bgp**，并确认显示 4 个路由。



5. 从 NGFW CLI 中：

   a. 运行 **show route**。确认从 BGP 获知的唯一路由是 62.24.45.0/24 和 62.112.24.0/24。请注意，已从 BGP 中成功过滤掉 203.14.10.0/24。但是，如果您执行了 FlexConfig 方案，则会将此路由视为外部 EIGRP 路由。

   b. 运行 **show bgp** 和 **show bgp rib-failure**。这显示未在路由表中插入 198.18.128.0/18 路由，因为有更好的路由（已连接）。

注意：您也可以从 FMC 运行此命令。
1. 导航至**设备 > 设备管理**。
2. 编辑 **NGFW** 设备并选择**设备**选项卡
3. 在**运行状况**部分中，点击**状态**右侧的图标。
4. 点击**高级故障排除**。
5. 选择**威胁防御 CLI** 选项卡。
您可以从此处运行多个 NGFW CLI 命令。

6. 从内部 Linux 服务器会话中，键入 **ping 62.24.45.1**。此命令应该会成功。

场景 11：站点间 VPN

此练习包含以下任务：

- 创建此实验练习所需的对象
- 配置站点间 VPN
- 创建 NAT 免除
- 修改访问控制策略并部署更改
- 部署更改并测试配置

此练习的目标是在 NGFW 和 ASA 之间配置站点间 VPN 隧道。

步骤

创建此实验练习所需的对象

1. 导航至**对象 > 对象管理**。系统将选择**网络**对象页面。
    a. 点击**添加网络 > 添加对象**。
    b. 在**名称**字段，输入 **`MainOfficeNetwork`**。
    c. 在网络字段，输入 **`198.19.10.0/24`**。
    d. 点击**保存**。
    e. 点击**添加网络 > 添加对象**。
    f. 在**名称**字段，输入 **`BranchOfficeNetwork`**。
    g. 在网络字段，输入 **`198.19.11.0/24`**。
    h. 点击**保存**。

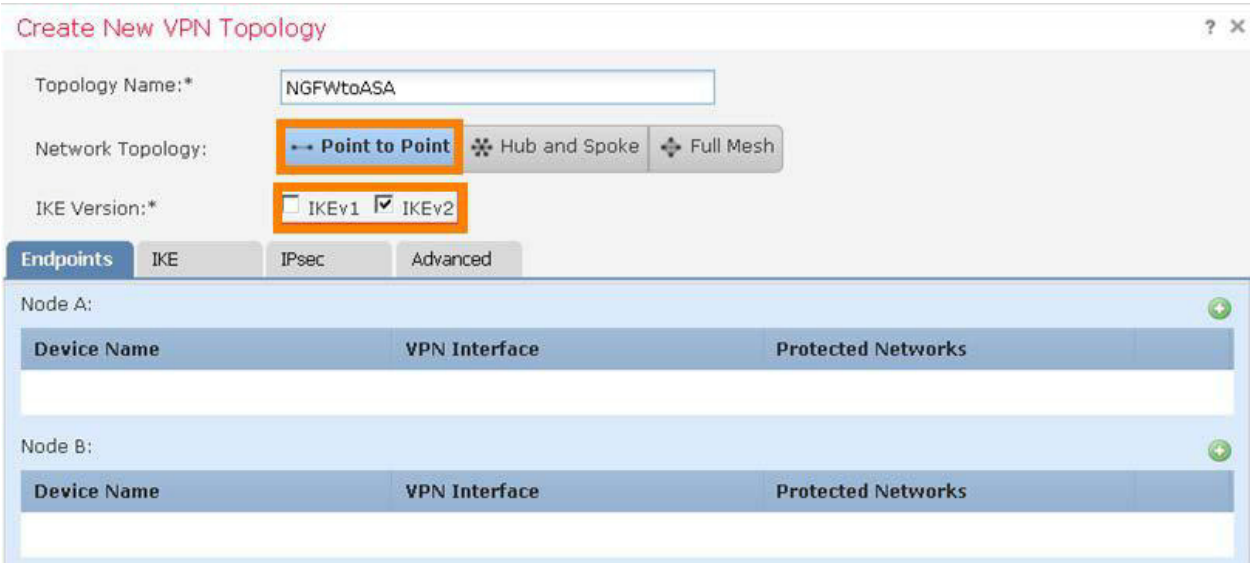
配置站点间 VPN

1. 导航至**设备 > VPN > 站点间**。点击**添加 VPN > Firepower 威胁防御设备**。

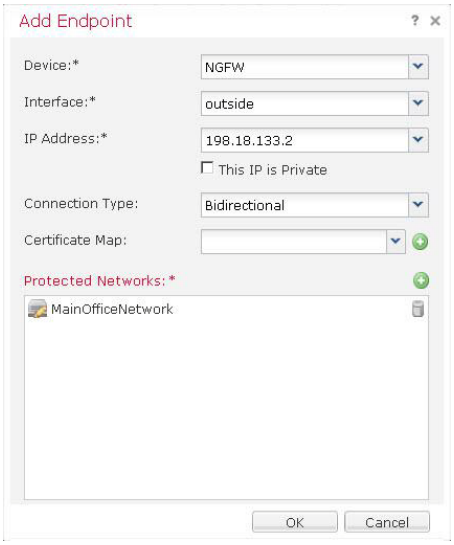
注意：另一个 VPN 选项（Firepower 设备）用于在 Firepower 设备之间配置安全隧道。

2. 在**名称**字段，输入 **`NGFWtoASA`**。

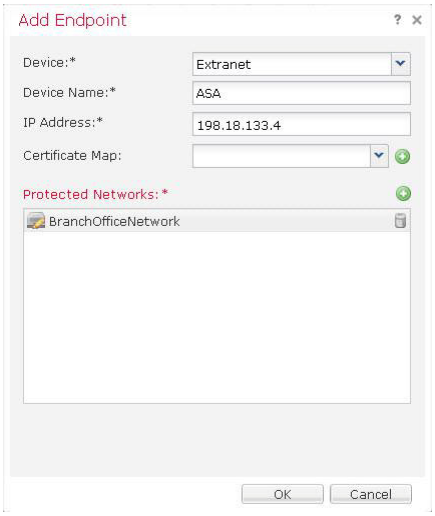
3. 确认对于“网络拓扑”，选择“点对点”。确认对于“IKE 版本”，未选中 IKEv1，而是选中 IKEv2。



4. 点击**节点 A** 右侧的绿色加号。按照下图所示进行填写，然后点击**确定**。



5. 点击**节点 B** 右侧的绿色加号。按照下图所示进行填写，然后点击**确定**。



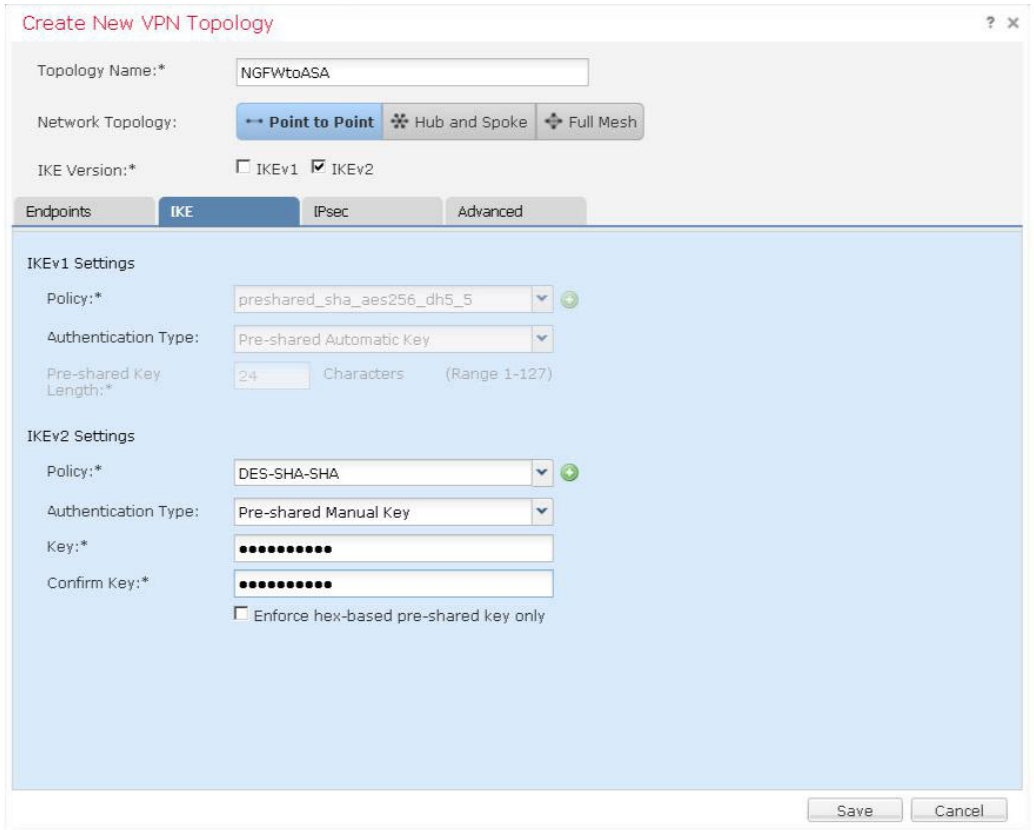
6. 选择 **IKE** 选项卡。

   a. 在 **IKEv2** 设置下，对于“策略”，选择 **DES-SHA-SHA**。

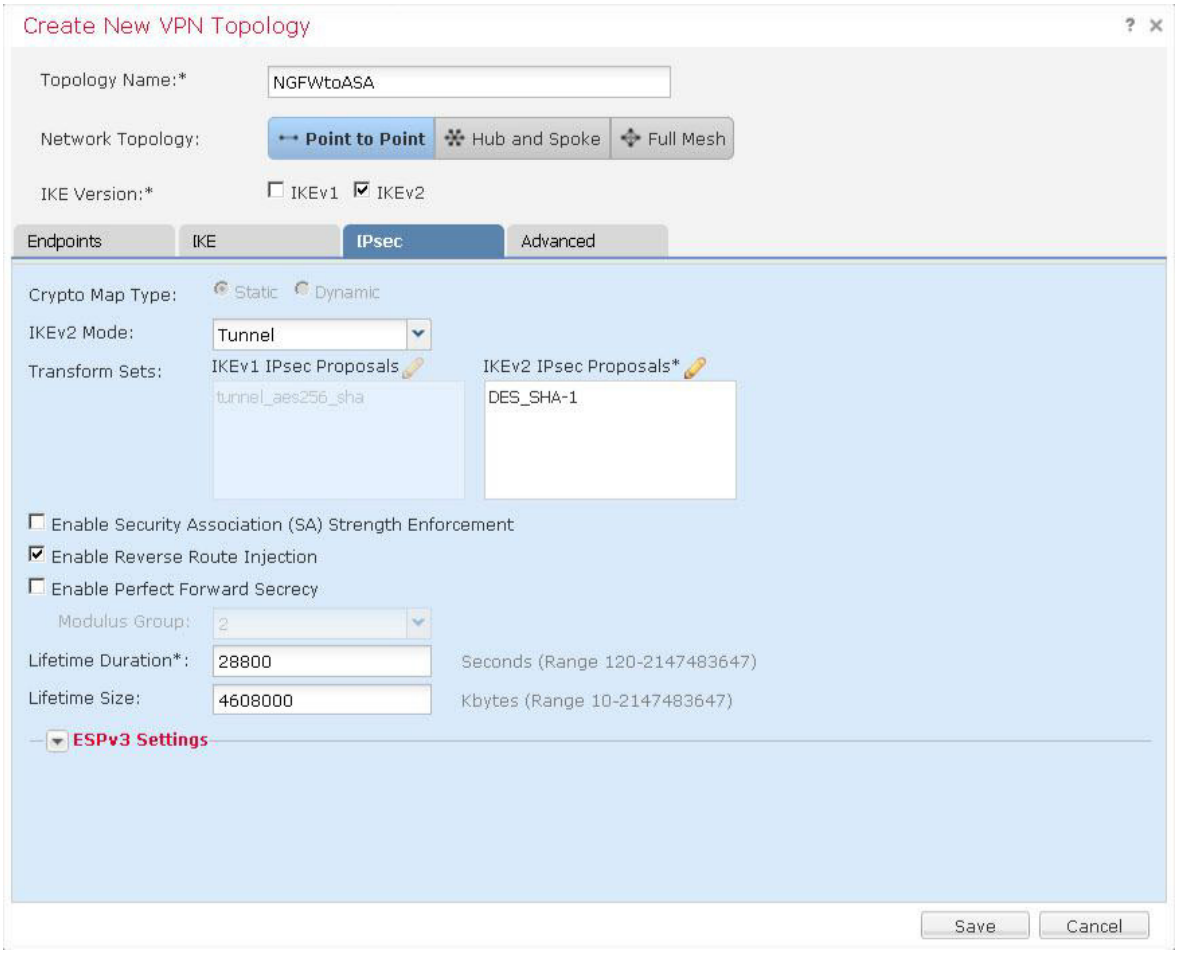
   b. 在 IKEv2 设置下，对于**身份验证类型**，选择**预共享手动密钥**。

注意：只有在 FMC 同时管理两个终端时，才能使用“自动”设置。在此情况下，FMC 可以生成随机共享密钥。

   c. 在 **IKEv2** 设置下，对于**密钥**，输入 `C1sco12345`，并且确认输入。



7. 选择 **IPsec** 选项卡，将 **IKEv2 IPsec 提议**更改为 **DES_SHA-1**。



8. 点击**保存**以保存 VPN 设置。

创建 NAT 免除

1. 导航至**设备 > NAT**。
2. 点击铅笔图标以编辑**默认 PAT** 策略。
3. 点击**添加规则**。
    a. 保持选定 **NAT 规则**下拉列表中的**类别中**和 **NAT 规则在前**。
    b. 您将进入“接口对象”选项卡。
        i. 选择 **InZone**，然后点击**添加到源**。
        ii. 选择 **OutZone**，然后点击**添加到目的地**。

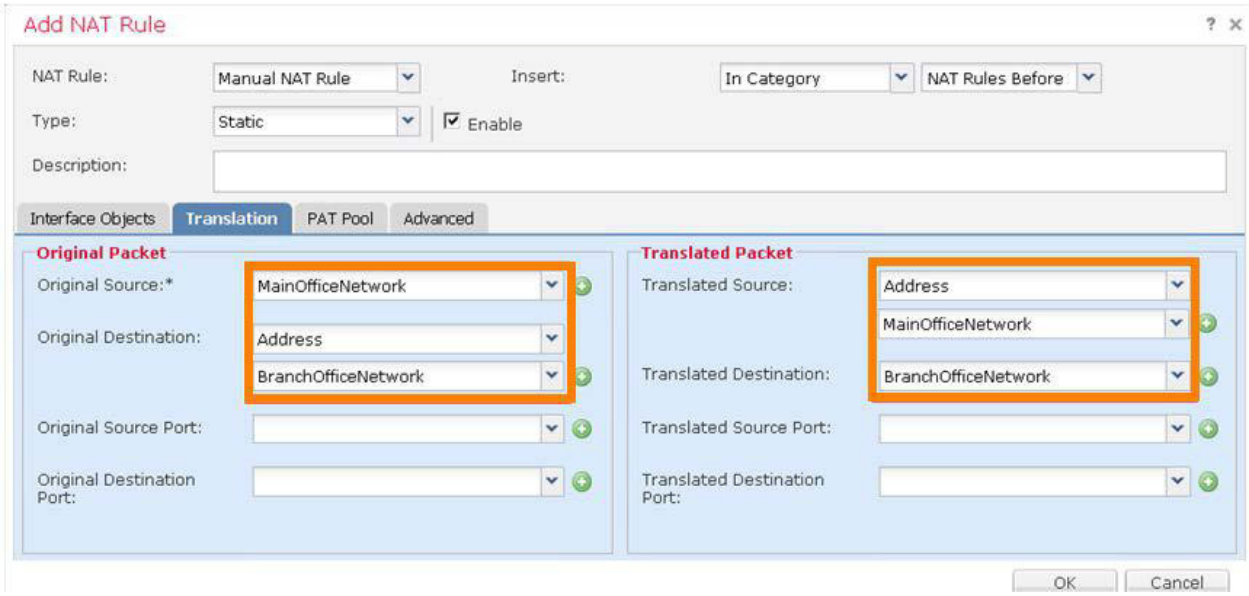
c. 选择“转换”选项卡。

i. 从**原始源**下拉列表中选择 **MainOfficeNetwork**。

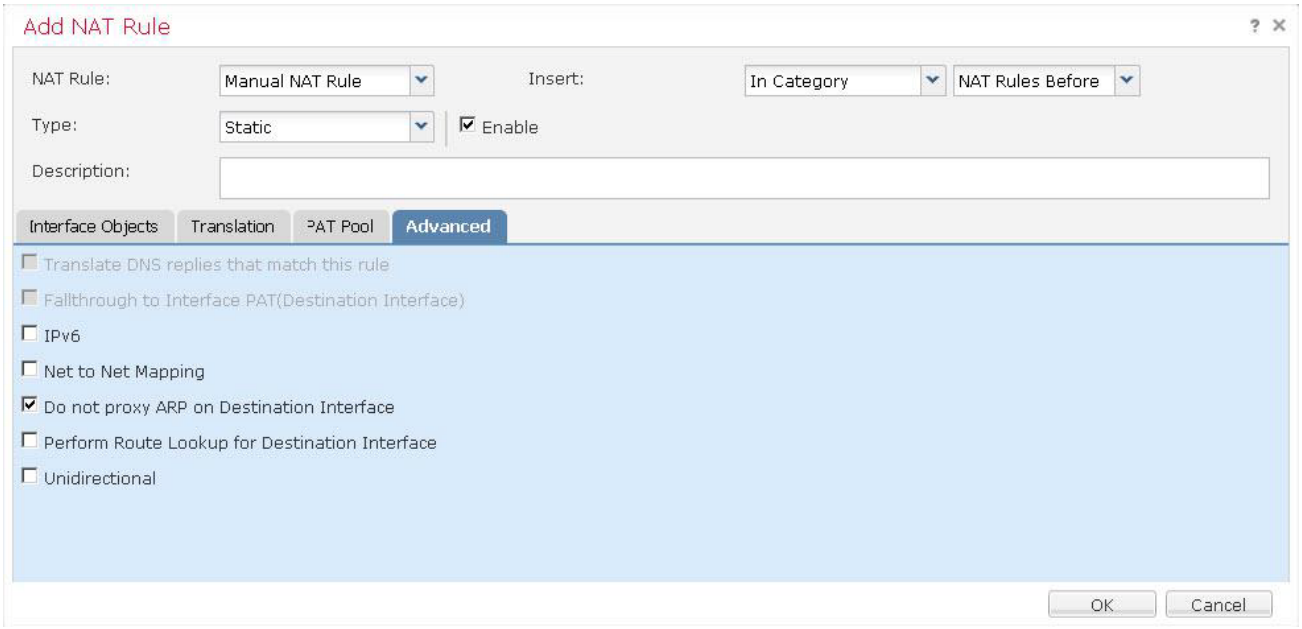
ii. 从**已转换的源**下拉列表中选择 **MainOfficeNetwork**。

iii. 从**原始目的地**下拉列表中选择 **BranchOfficeNetwork**。

iv. 从**已转换的目的地**下拉列表中选择 **BranchOfficeNetwork**。



d. 选择“高级”选项卡，然后选中**不在目的接口上使用代理 ARP** 复选框。



e. 点击**确定**以保存 NAT 规则。

4. 点击**保存**以保存 NAT 策略。

修改访问控制策略并部署更改

现在，您将创建一个规则，以允许分支机构与总部之间的流量。

1. 导航至**策略 > 访问控制 > 访问控制**。编辑 NGFW 访问控制策略。
2. 点击**添加规则**。
    a. 调用规则 **`VPN Access`**。
    b. 从**插入**下拉列表中选择**插入到默认规则集**。这将成为访问控制策略中的最后一个规则。
    c. 将操作保持为**允许**。
    d. 系统应已选择**区域**选项卡。
    e. 选择 **OutZone**，然后点击**添加到源**。
    f. 选择 **InZone**，然后点击**添加到目的地**。
    g. 选择**网络**选项卡，选择 **BranchOfficeNetwork**，然后点击**添加到源**。
    h. 选择**网络**选项卡，选择 **MainOfficeNetwork**，然后点击**添加到目的地**。
    i. 选择**检查**选项卡。
        i. 从**入侵策略**下拉列表中选择**演示入侵策略**。
        ii. 从**文件策略**下拉列表中选择**演示文件策略**。
    j. 点击**添加**以将此规则添加到访问控制策略中。
3. 点击**保存**以保存访问控制策略。

部署更改并测试配置

1. 部署更改，然后等待部署完成。
2. 从 NGFW CLI 中，键入 **`show crypto ipsec sa`**。应该没有任何 IPSec 安全关联。
3. 从内部 Linux 服务器 CLI 中，键入 **`ping branch`**。等待几秒钟，然后 ping 应该会成功。
4. 从 NGFW CLI 中，键入 **`show crypto ipsec sa`**。现在应该有 IPSec 安全关联。
5. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为**分支机构 Linux 服务器**的预配置会话。
    a. 使用用户名 **`root`** 和密码 **`C1sco12345`** 登录。
    b. 键入 **`curl inside`**。此命令应该会成功。

场景 12：Web 代理集成

此练习包含以下任务：

- 修改 WSA 配置
- 配置 XFF 类型报头的使用
- 部署访问控制策略
- 部署更改并测试配置

NGFW 可以使用 XFF 类型的报头在实际客户端而不是代理服务器上实施策略。此练习的目标是使学生熟悉 True-Client-IP 功能。此功能允许 NGFW 实施用于使终端通过 Web 代理来传递流量的策略。

请注意，您配置的规则是虚假规则，但是便于进行测试

步骤

修改 WSA 配置

1. 在 Jump Desktop 上，打开 PuTTY 链接。双击名为 **WSA** 的预配置会话。使用用户名 **admin** 和密码 **C1sco12345** 登录。
2. 在 WSA CLI 上使用以下 CLI 命令：

```
wsa.dcloud.local> setgateway

Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Set the default gateway for:
1. IPv4
2. IPv6
[1]> 1

Enter new default gateway:
[198.19.10.11]> 198.19.10.1

wsa.dcloud.local> commit

Please enter some comments describing your changes:
[]> Changing gateway

Changes committed: Mon Oct 02 00:01:11 2017 GMT
wsa.dcloud.local>
```

3. 确认 WSA 配置为生成 X-Forwarded-For 报头。请注意，这不是默认值。
    a. 在 Firefox 浏览器上，打开新标签。
    b. 点击书签栏链接 **WSA**。使用用户名 **admin** 和密码 **C1sco12345** 登录（系统应该会预填充这些凭证）。
    c. 在 WSA UI 中，导航至“安全服务”>“Web 代理”。
    d. 在**高级设置**下，对于**生成报头**，确认发送的是 **X_Forwarded-For** 报头。

配置 XFF 类型报头的使用

1. 在 FMC 选项卡上，导航至**策略 > 访问控制 > 访问控制**。编辑 NGFW 访问控制策略。
2. 点击**添加规则**。
    a. 调用规则 **Test XFF Feature**。
    b. 将“操作”设置为**通过重置进行阻止**。
    c. 从“插入”下拉列表中选择**插入到强制性规则集**。
    d. 在**区域**选项卡中，选择 **InZone**，然后点击**添加到源**。
    e. 在**区域**选项卡中，选择 **OutZone**，然后点击**添加到目的地**。
    f. 选择**网络**选项卡。
        i. 在**源网络**区域中，选择**源**子选项卡。在页面底部，输入 **198.19.10.101**，然后点击**添加**。这是 WSA 代理服务器的 IP 地址。
        ii. 在**源网络**区域中，选择**原始客户端**子选项卡。在页面底部，输入 **198.19.10.201**，然后点击“添加”。
        iii. 在页面底部的**目标网络**区域中，输入 **198.18.133.201**，然后点击**添加**。
    g. 选择**日志记录**选项卡。选中**在连接开始时进行日志记录**复选框。
    h. 点击**添加**以将规则添加到策略中。
    i. 点击**保存**以保存策略更改。

部署更改并测试配置

1. 部署更改，然后等待部署完成。
2. 返回到内部 Linux 服务器 PuTTY 会话。运行以下命令以测试配置。
    a. 运行（单行）命令：
    `wget --bind-address=198.19.10.201 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`
    您应该获取 403（禁止访问）响应代码。
    b. 运行（单行）命令：
    `wget --bind-address=198.19.10.200 -e use_proxy=yes -e http_proxy=198.19.10.101 198.18.133.201`
    此命令应该会成功。

注意：现在文件已缓存在 WSA 上，如果重复步骤 2a，则将下载该文件。为在生产中避免此情况，您必须在客户端和 WSA 之间部署 NGFW。为进行测试，可以通过依次键入 **`diagnostic`**、**`PROXY`**、**`CACHE`**.来从 WSA CLI 中清除 WSA 代理缓存。

3. 在 FMC 中，导航至**分析 > 连接 > 事件**。
    a. 点击文本**连接事件的表视图**。
    b. 默认情况下，未显示**原始客户端 IP** 列。现在，您将添加此列。
    c. 要添加此列，请执行以下步骤。
        i. 点击未使用的任何列顶部的 **X**。
        ii. 将列选择器向下滚动到**已禁用的列**。
        iii. 选中**原始客户端 IP** 复选框。
        iv. 向下滚动到列选择器底部，然后点击**应用**。
    d. 确认 WSA IP (198.19.10.101) 和客户端 IP (198.19.10.201) 均已显示。

场景 13：预过滤策略

此练习包含以下任务：

- 调查隧道流量的 NGFW 默认行为
- 创建隧道区域
- 创建预过滤策略
- 修改访问控制策略
- 部署更改并测试配置

预过滤策略具有两种类型的规则（预过滤和隧道）。预过滤规则更为常用。它们指定应在 Lina 数据平面中丢弃哪些流量，哪些流量应绕过 Snort，以及哪些流量应发送到 Snort。这可能有助于提升性能。您将在此场景中的稍后部分配置预过滤规则，但是此场景将侧重于隧道规则，因为它们更微妙。

如果有明文隧道，则 NGFW 访问控制策略应用于**隧道**流量。预过滤策略提供对**隧道**协议的控制。系统支持以下隧道协议。

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo

预过滤策略通过隧道标记与访问控制策略进行通信。预过滤策略将隧道标记分配给指定的隧道。然后，访问控制策略可以包含仅应用于通过这些指定隧道传递的流量的规则。

在此练习中，您需要在内部和外部 CentOS 服务器之间创建 GRE 隧道。

然后，您需要将 NGFW 配置为通过此 GRE 隧道来阻止 ICMP。

注意：此练习以场景 10 作为先决条件。这是因为此练习采用静态 NAT 规则，该规则将 198.19.10.202 转换为 198.18.128.202。要了解隧道接口的配置，可以在内部和外部服务器上检查 **`/etc/sysconfig/network-scripts/ifcfg-tun0`**。

步骤

调查隧道流量的 NGFW 默认行为

在此任务中，您需要确认访问控制策略规则应用于隧道流量。

1. 您应该仍然有已与内部 Linux 服务器打开的 SSH 会话。
2. 如果您没有已与外部 Linux 服务器打开的 SSH 会话，请从 Jump Desktop 启动 PuTTY，然后双击预定义**外部 Linux 服务器**会话。使用用户名 **root** 和密码 **C1sco12345** 登录。
3. 在内部 Linux 服务器和外部 Linux 服务器之间创建 GRE 隧道。
    a. 在外部 Linux 服务器 CLI 上，键入 **ifup tun0**。
    b. 在内部 Linux 服务器 CLI 上，键入 **ifup tun0**。
    c. 在内部 Linux 服务器上，确认可以使用以下命令 ping 通隧道。**ping 10.3.0.2**
4. 测试 IPS 功能。
    a. 从内部 Linux 服务器 CLI 中运行以下命令。**ftp 10.3.0.2**
    b. 使用用户名 **guest** 和密码 **C1sco12345** 登录。
    c. 键入 **cd ~root**。您应该看到以下消息：
    421 Service not available, remote server has closed connection
    d. 键入 **quit** 以退出 FTP。
5. 在 FMC 中，导航至**分析 > 入侵 > 事件**。
    a. 点击左侧的箭头以深入查看事件的表视图。
    b. 观察源和目标 IP 是否分别为 10.3.0.1 和 10.3.0.2。
6. 通过在内部 Linux 服务器 CLI 上运行以下命令来测试文件和恶意软件阻止功能。

注意：可以从 Jump Desktop 上名为 Strings to cut and paste.txt 的文件剪切并粘贴这些 Wget 命令。

a. 作为控制测试，使用 WGET 下载未阻止的文件。
wget -t 1 10.3.0.2/files/ProjectX.pdf
此命令应该会成功。

b. 接下来，使用 WGET 下载按类型阻止的文件。
wget -t 1 10.3.0.2/files/test3.avi
请注意，系统仅下载了文件的很小一部分。这是因为 NGFW 可以在发现第一个数据块时检测出文件类型。

c. 最后，使用 WGET 下载恶意软件。
wget -t 1 10.3.0.2/files/Zombies.pdf
请注意，系统下载了文件的大约 99% 部分。这是因为 NGFW 需要整个文件来计算 SHA。NGFW 会一直检测完最后一个数据块，直至计算并找出散列值。

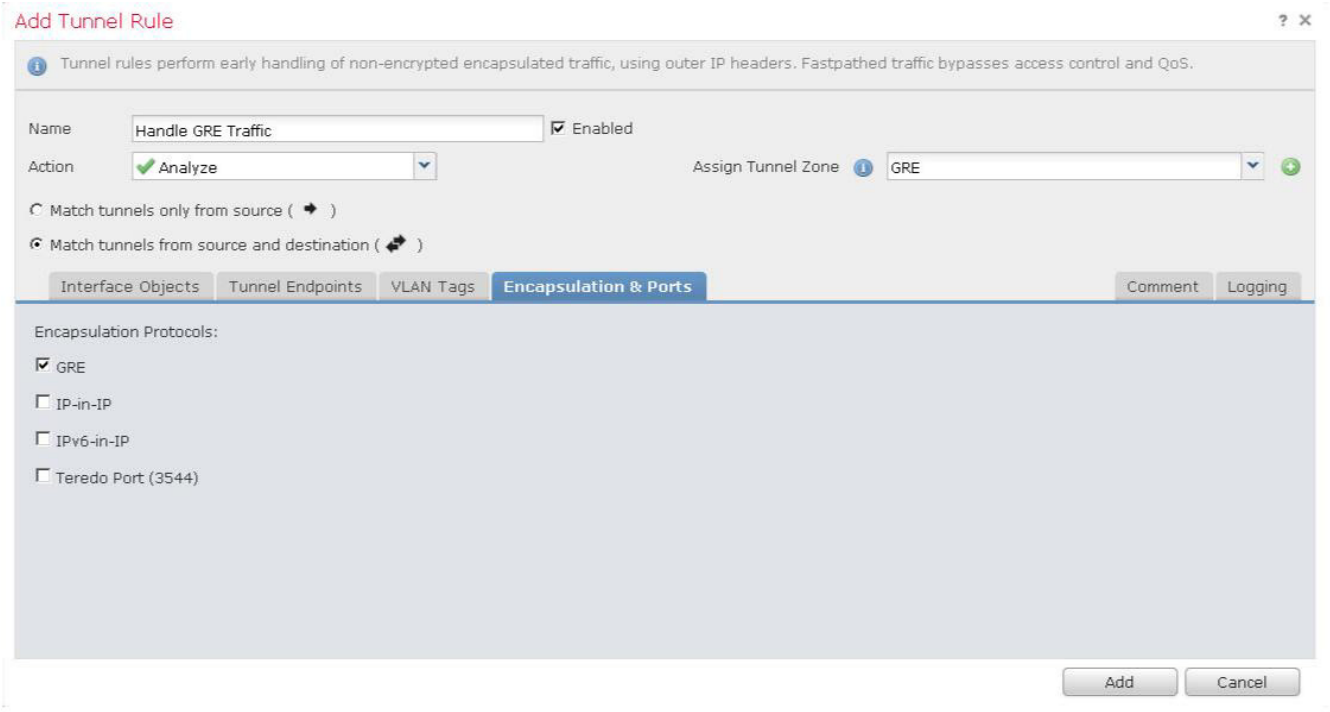
7. 在 FMC 中，导航至**分析 > 文件 > 文件事件**。
    a. 点击**文件事件的表视图**。
    b. 观察发送和接收 IP 是否分别为 **10.3.0.2** 和 **10.3.0.1**。

创建隧道区域

1. 导航至**对象 > 对象管理**。
    a. 从左侧导航窗格中选择**隧道区域**。
    b. 点击**添加隧道区域**。
    c. 在**名称**字段，输入 **GRE**。
    d. 点击**保存**。

创建预过滤策略

1. 导航至**策略 > 访问控制 > 预过滤**。
2. 点击**新建策略**。输入名称，例如 **NGFW Prefilter Policy**。点击**保存**。
3. 等待几秒钟以打开该策略进行编辑
4. 点击**添加隧道规则**。
    a. 在**名称**字段，输入 **Handle GRE Traffic**。
    b. 从**分配隧道区域**下拉列表中选择 **GRE**。
    c. 选择**封装和端口**选项卡，然后选中 **GRE** 复选框。



注意：有 3 个操作
• 分析 - 流量将传递到 Snort，并将应用访问策略规则
• 阻止 - 阻止流量
• 快速路径 - 允许流量，并且流量会绕过任何进一步检查
您还可以为此策略创建预过滤规则。借此能够根据第 2 层至第 4 层信息对流量进行分析、阻止或通过快速路径传递。

d. 点击**添加**以添加规则。

5. 现在，您需要添加一个规则，该规则将为目的地为 198.18.133.202 的任何流量绕过 Snort。您信任此地址。点击**添加预过滤规则**。
   a. 在**名称**字段，输入 **`Example of Fastpath`**。
   b. 从**操作**下拉列表中选择**快速路径**。
   c. 选择**网络**选项卡。
   d. 在**目标网络**列的底部，输入 **`198.18.133.202`**。
   e. 点击**添加**以添加目标网络。
6. 点击**添加**以添加预过滤规则。
7. 点击**保存**以保存预过滤策略。

修改访问控制策略

1. 导航至**策略 > 访问控制 > 访问控制**。编辑 NGFW 访问控制策略。
2. 点击策略规则上方的字符串**预过滤策略**右侧的链接**默认预过滤策略**。选择 NGFW 预过滤策略。点击**确定**。
3. 选择**规则**选项卡。
4. 点击**添加规则**。
   a. 调用规则 **`Block ICMP Over GRE`**。
   b. 从**插入**下拉列表中选择**插入到强制性规则集**。
   c. 将“操作”设置为**通过重置进行阻止**。
   d. 在**可用区域**列中，选择 **GRE**，然后点击**添加到源**。
   e. 在**应用**列中，选择 **ICMP**，然后点击**添加到规则**。
   f. 选择**日志记录**选项卡。选中**在连接开始时进行日志记录**复选框。
   g. 点击**添加**以将规则添加到策略中。
5. 点击**添加规则**。
   a. 调用规则 **Allow GRE Traffic**。
   b. 从“插入”下拉列表中选择**插入到默认规则集**。这将成为访问控制策略中的最后一个规则。
   c. 在**可用区域**列中，选择 **GRE**，然后点击**添加到源**。
   d. 选择**检查**选项卡。

i. 从**入侵策略**下拉列表中选择**演示入侵策略**。

ii. 从**文件策略**下拉列表中选择**演示文件策略**。

e. 点击**添加**以将规则添加到策略中。

6. 点击**保存**以保存访问控制策略。

部署更改并测试配置

1. 照常部署更改。等待部署完成。
2. 在外部 Linux 服务器上，运行 **tcpdump -n -i tun0** 以监控隧道流量。
3. 在内部 Linux 服务器 CLI 上运行以下命令。

   a. wget 10.3.0.2

   此命令应该会成功。

   b. ping 10.3.0.2

   您应该看到以下输出，指示 ping 受到阻止。

   From 10.3.0.2 icmp_seq=1 Packet filtered

4. 检查外部 Linux 服务器上的 `tcpdump` 命令的输出，以确认 ping 未能到达 10.3.0.2。
5. 拆除隧道：

   a. 在外部 Linux 服务器 CLI 上，键入 `ifdown tun0`。

   b. 在内部 Linux 服务器 CLI 上，键入 `ifdown tun0`。

6. 现在测试预过滤规则。

   a. 键入

   wget -t 1 198.18.133.200/files/Zombies.pdf

   此命令应受阻止。

   b. 键入

   wget -t 1 198.18.133.202/files/Zombies.pdf

   由于流量绕过 Snort，因此应该会允许此命令。

场景 14：集成路由和桥接 (IRB)

此练习包含以下任务：

- 创建此实验练习所需的对象
- 修改 NGFW 接口配置
- 修改 NAT 策略
- 修改访问控制策略
- 部署和测试配置

在实验中，在单独的 VLAN 上有一个连接到 GigabitEthernet0/2 的 Linux 服务器。此服务器的 FQDN 为 **isolated.dcloud.local**，并且其 IP 地址为 198.19.10.220/24。请注意，此地址与内部网络位于同一子网中。

目标是使用 NGFW 上的桥组加入这些 VLAN。系统将检查这些 VLAN 之间的流量。

注意：在此练习中，桥组中的两个接口均放在同一安全区域中。但这不是必然要求。桥组可以包含不同安全区域中的接口。这样可以对同一桥组中的接口之间的流量进行更精细的控制。

步骤

创建此实验练习所需的对象

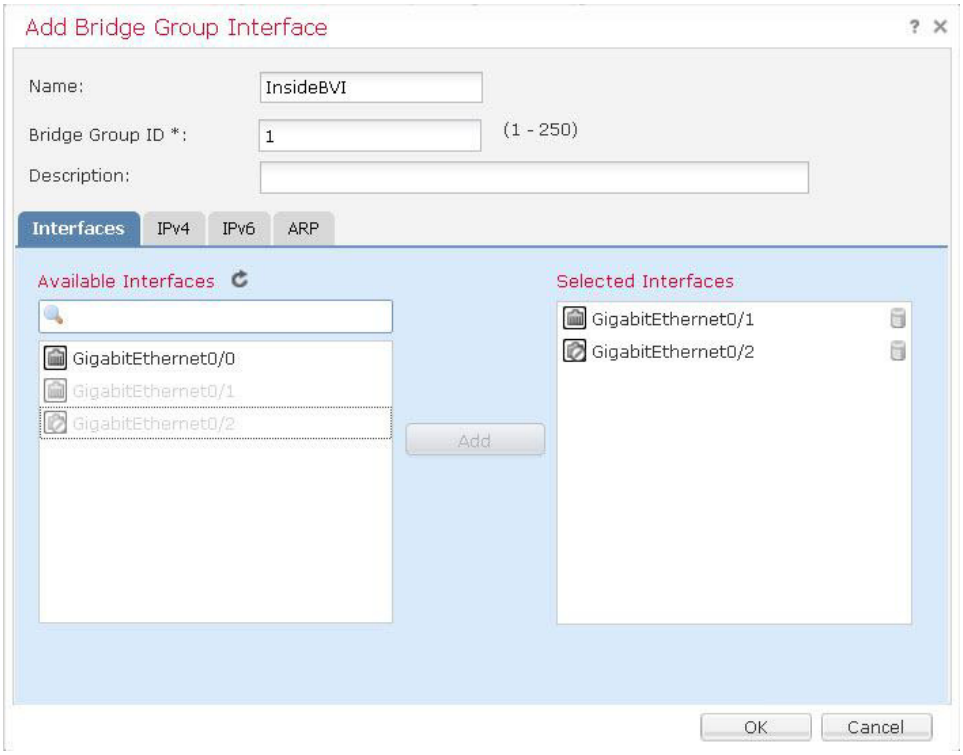
1. 导航至**对象 > 对象管理**。从左侧导航面板中选择**接口**。
2. 点击**添加 > 安全区域**。
    a. 在“名称”字段，输入 **`BVIZone`**。
    b. 从**接口类型**下拉菜单中选择**交换**。
    c. 点击**保存**。

修改 NGFW 接口配置

1. 导航至**设备 > 设备管理**。
2. 点击铅笔图标以编辑 NGFW 设备配置，然后选择**接口**选项卡。
3. 点击铅笔图标以编辑 **GigabitEthernet0/1** 接口。
4. 删除 **IPv4 地址**，然后点击**确定**。必须删除此 IP，以便它可以在另一个接口上使用。
5. 点击**添加接口**，然后选择**桥组接口**。
    a. 在**名称**字段，输入 **`InsideBVI`**。

b. 对于“桥组 ID”，输入 **1**。

c. 选择 **GigabitEthernet0/1** 和 **GigabitEthernet0/2**，然后点击**添加**。



d. 选择 IPv4 选项卡，然后输入 IP 地址 **198.19.10.1/24**。

e. 点击**确定**。当显示确认请求时，请阅读消息，然后点击**是**。

6. 点击铅笔图标以编辑 **GigabitEthernet0/1** 接口。

a. 在**名称**字段，输入 **`inside1`**。

b. 确认选中**启用**复选框。

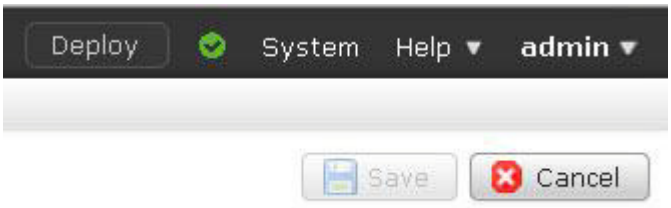
c. 从**安全区域**下拉列表中选择 **BVIZone**。

d. 点击**确定**。

7. 点击**铅笔图标**以编辑 **GigabitEthernet0/2 接口**。
    a. 在**名称**字段，输入 **`inside2`**。
    b. 选中**启用**复选框。
    c. 从**安全区域**下拉列表中选择 **BVIZone**。
    d. 点击**确定**。
8. 点击**保存**以保存设备配置。

修改 NAT 策略

1. 如果您执行了场景 10，并且希望静态 NAT 规则适用于 BVI 接口，则必须完成此步骤。这是因为对象 NAT 不允许使用具有多个接口的接口对象。
    a. 导航至**对象 > 对象管理**。从左侧导航面板中选择**接口**。
    b. 点击**添加 > 接口组**。
        i. 在**名称**字段，输入 **`InGroup1`**。
        ii. 对于**接口类型**，选择**交换**。
        iii. 选择接口 **inside1**，然后点击**添加**。
        iv. 点击**保存**。
2. 导航至**设备 > NAT**。
3. 编辑**默认 PAT** 策略。确认在右上方看到灰显的**保存**按钮。如果看不到，请导航离开并重试编辑。

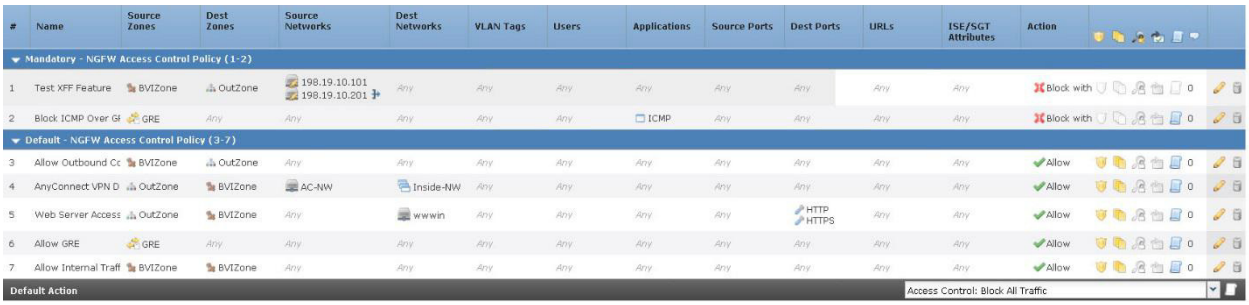


    a. 如果在场景 10 中进行了静态 NAT 配置，请在自动 NAT 规则中将 **InZone** 替换为 **InGroup1**。不能使用 **BVIZone**，因为自动 NAT 不允许使用具有多个接口的安全区域。变通方法将是创建一个接口组。
    b. 在其他每个规则中将 **InZone** 替换为 **BVIZone**。
    c. NAT 规则应为如下所示。根据所执行的场景，您可能具有更多或更少的规则。

    d. 点击**保存**以保存 NAT 策略。

修改访问控制策略

1. 导航至**策略 > 访问控制 > 访问控制**，然后编辑访问控制策略。
2. 点击**铅笔图标**以编辑 NGFW 设备配置，然后选择**接口**选项卡。
    a. 在每个规则中将 **InZone** 替换为 **BVIZone**。
    b. 添加访问控制规则以允许（但要检查）**BVIZone** 中的接口之间的流量。
        i. 在**名称**字段，输入 **`Allow Internal Traffic`**。
        ii. 从**插入**下拉列表中选择*插入到***默认规则集**
        iii. 系统应已选择**区域**选项卡。
        iv. 选择 **BVIZone**，然后点击**添加到源**。
        v. 选择 **BVIZone**，然后点击**添加到目的地**。
        vi. 选择**检查**选项卡。
        vii. 从“入侵策略”下拉列表中选择**演示入侵策略**。
        viii. 从“文件策略”下拉列表中选择**演示文件策略**。
        ix. 点击**添加**以添加规则。
    c. 访问控制策略应如下所示。根据所执行的场景，您可能具有更多或更少的规则。



    d. 点击**保存**以保存对访问控制策略的更改。

部署和测试配置

1. 部署配置更改，然后等待部署完成。
2. 从内部 Linux 服务器 CLI 中，键入 **`ping isolated`** 来测试连接。此命令应该会成功。
3. 从内部 Linux 服务器 CLI 中，测试 IPS 功能。
    a. 从内部 Linux 服务器 CLI 中运行以下命令。**`ftp isolated`**
    b. 使用用户名 **`guest`** 和密码 **`C1sco12345`** 登录。
    c. 键入 **`cd ~root`**。您应该看到以下消息：
    `421 Service not available, remote server has closed connection`

4. 从内部 Linux 服务器 CLI 中，测试文件和恶意软件阻止功能。

   a. 作为控制测试，使用 WGET 下载未阻止的文件。

      wget -t 1 isolated/files/ProjectX.pdf

      此命令应该会成功。

   b. 接下来，使用 WGET 尝试下载按类型阻止的文件。

      wget -t 1 isolated/files/test3.avi

      请注意，系统仅下载了文件的很小一部分。这是因为 NGFW 可以在发现第一个数据块时检测出文件类型。*演示文件策略*配置为阻止 AVI 文件。

   c. 最后，使用 WGET 尝试下载恶意软件。

      wget -t 1 isolated/files/Zombies.pdf

注意：系统下载了文件的大约 99% 部分。这是因为 NGFW 需要整个文件来计算 SHA。NGFW 会一直检测完最后一个数据块，直至计算并找出散列值。*演示文件策略*配置为阻止在 PDF 文件中检测到的恶意软件。

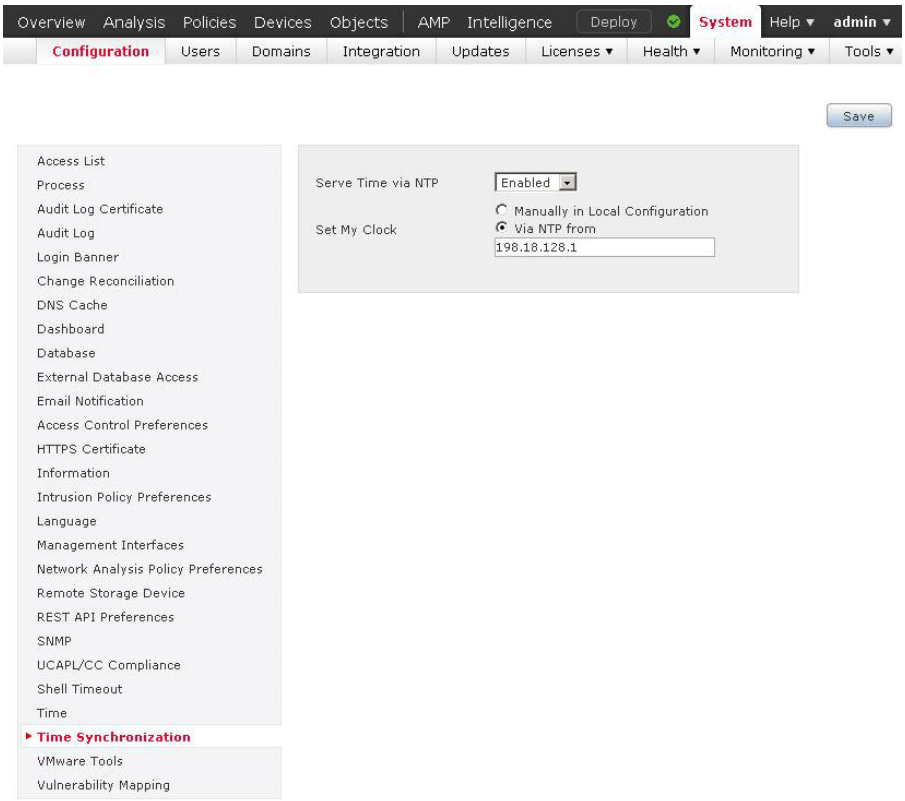
附录 A：FMC 预配置

在初始安装后，在 FMC 上执行了多个配置步骤以加快实验练习。本附录详细介绍这些配置步骤。

- 配置 A1.1：NTP 设置
- 配置 A1.2：演示文件策略
- 配置 A1.3：演示入侵策略
- 配置 A1.4：演示 SSL 策略
- 配置 A1.5：自定义检测列表
- 配置 A1.6：添加 resetapiuser
- 配置 A1.7：安装服务器证书

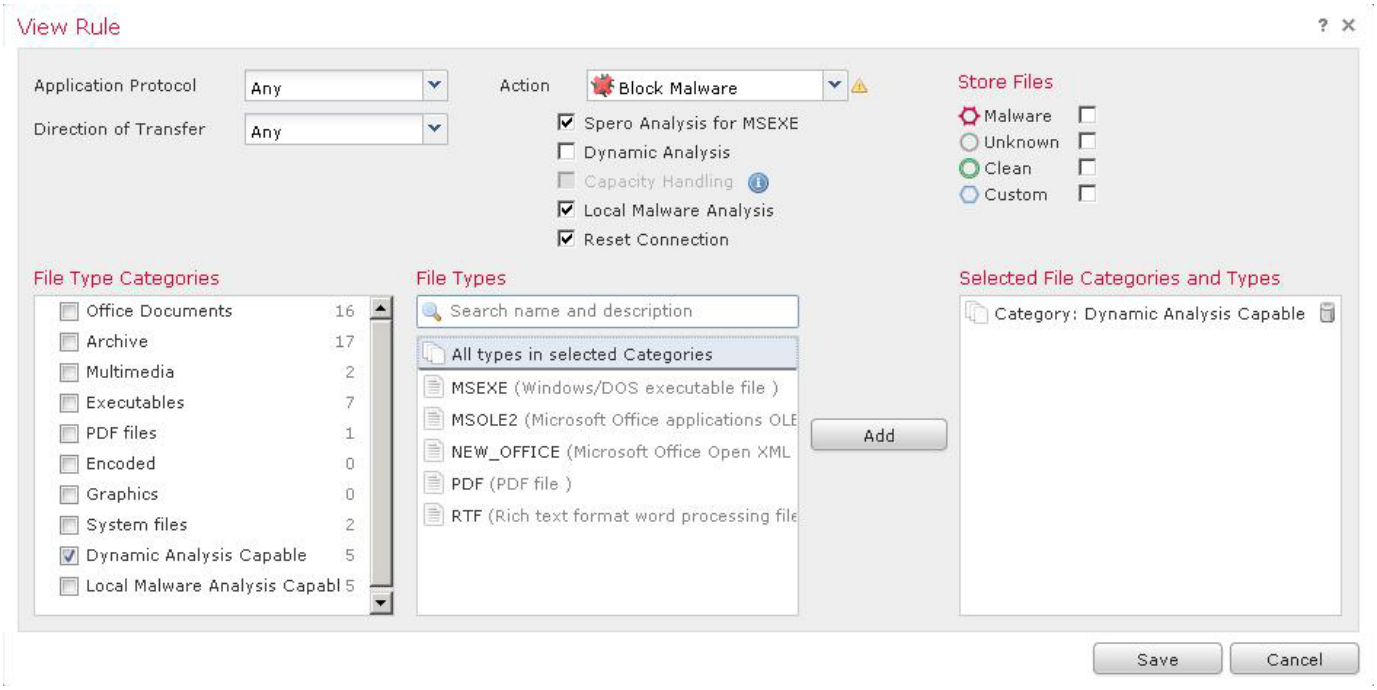
配置 A1.1：NTP 设置

1. 在 FMC 上配置 NTP 设置。
    a. 在 FMC 中，导航至**系统 > 配置**。
    b. 从左侧导航窗格中选择**时间同步**。
    c. 将默认 NTP 服务器替换为 **198.18.128.1**。
    d. 点击“保存”。



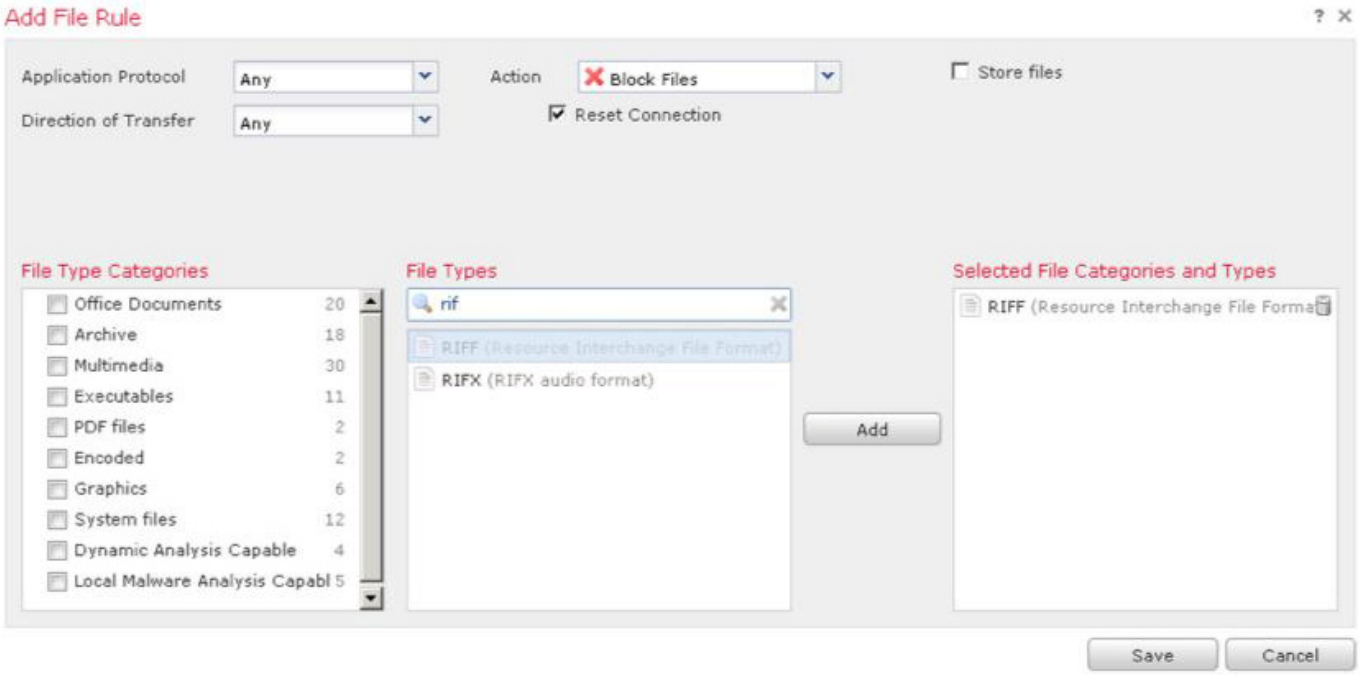
配置 A1.2：演示文件策略

1. 导航至**策略 > 访问控制 > 恶意软件和文件**。
2. 点击**新建文件策略**。输入名称 **`Demo File Policy`**。点击**保存**。
3. 点击**添加文件规则**。此规则将阻止在文件 MSEXE、MSOLE2、NEW_OFFICE 和 PDF 中发现的恶意软件。
    a. 对于**操作**，选择**阻止恶意软件**。
    b. 选中 Spero 和**本地恶意软件分析**复选框。
    c. 在**文件类型类别**下，选中*具有动态分析功能*。请注意，多个文件类型属于此类别。点击**添加**。
    d. 您的屏幕应如下图所示。



    e. 点击**保存**。当出现提示时，忽略警告，然后点击**确定**。

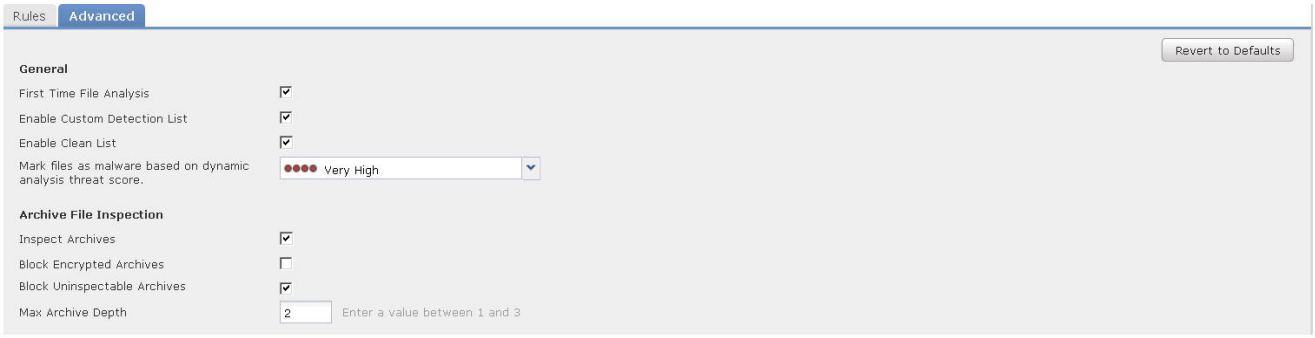
4. 点击**添加文件规则**。此规则将阻止 RIFF 文件。您将使用 AVI 文件来测试此规则，因为 AVI 文件是一种 RIFF 文件。但请注意，AVI 未单独列为一种文件类型。
    a. 对于**操作**，选择**阻止文件**。
    b. 在**文件类型**下，在搜索框中键入 **`rif`**。从列表中选择 **RIFF**。点击**添加**。
    c. 为其他设置使用默认值。您的屏幕应如下图所示。
    d. 点击**保存**。



注意：不能更改所创建的规则的顺序。规则的顺序无关紧要。规则的操作确定其优先级。操作的优先级如下所示。

1. 阻止文件
2. 阻止恶意软件
3. 恶意软件云查找
4. 检测文件

5. 选择**高级**选项卡。确认选中**启用自定义检测列表**。选中**检查存档**复选框。



注意：无法检查的存档是损坏的存档或者深度超过最大存档深度的存档。

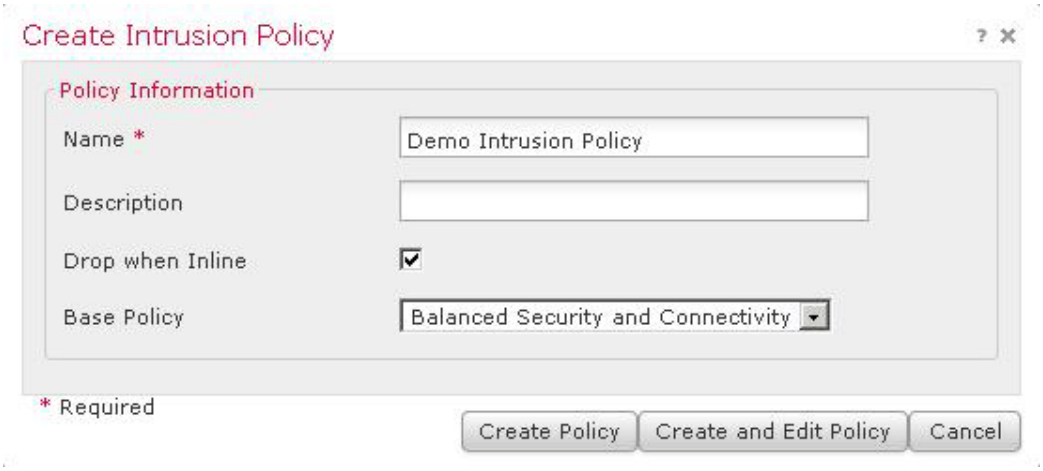
6. 点击右上方的**保存**按钮以保存文件策略。

配置 A1.3：演示入侵策略

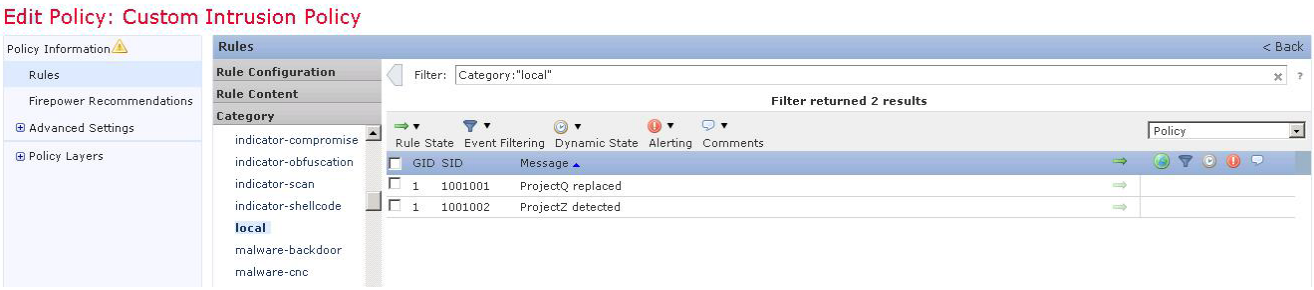
1. 导航至**对象 > 入侵规则**。点击**导入规则**。
    a. 选中**要上传和安装的规则更新或文本规则文件**单选按钮。
    b. 点击**浏览**，然后打开 Jump Desktop 的 **Files** 文件夹中的 **Snort_Rules.txt** 文件。

注意：此文件包含两个有助于测试 IPS 的简单 Snort 规则。它们不同于已发布的 Snort 规则。**alert tcp any any -> any any (msg:"ProjectQ replaced"; content:"ProjectQ"; replace:"ProjectR"; sid: 1001001; rev:1;)**
alert tcp any any -> any any (msg:"ProjectZ detected";
content:"ProjectZ"; sid: 1001002; rev:1;)
第一个规则将字符串 ProjectQ 替换为 ProjectR。第二个规则检测字符串 ProjectZ。由于规则没有指定字符串在流中的位置，因此它们在生产部署中可能会造成问题。

    c. 点击**导入**。导入过程将需要一到两分钟时间。完成后，您将看到**规则更新导入日志**页面。确认两个规则均已成功导入。
2. 导航至**策略 > 访问控制 > 入侵**。
3. 点击**创建策略**。
    a. 将名称设置为**演示入侵策略**。
    b. 确保选中**内联时丢弃**。
    c. 选择“平衡的安全性和连接性”作为**基本策略**。



    d. 点击**创建并编辑策略**。
4. 现在，您将修改此新策略的规则状态。
    a. 点击**编辑策略**页面左侧的“策略信息”菜单下的**规则**。
    b. 从规则的“类别”部分中选择**本地**。您应该看到两个已上传的规则。每个规则右侧的浅绿色箭头指示对于此策略禁用规则。



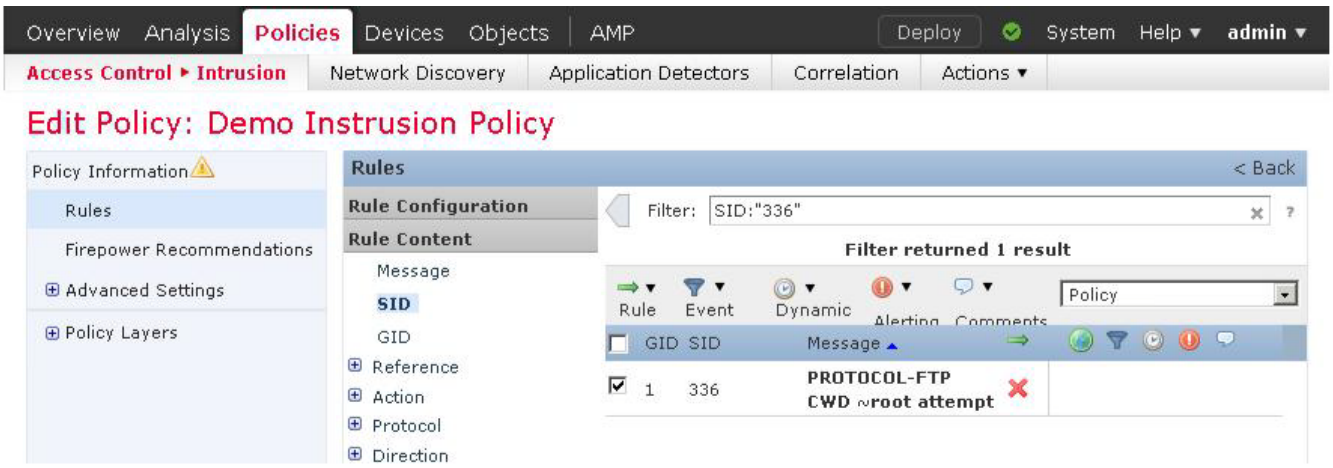
c. 选中第一个规则旁边的复选框。从**规则状态**下拉列表中选择**生成事件**。点击“确定”。取消选中第一个规则旁边的复选框。

d. 选中第二个规则旁边的复选框。从**规则状态**下拉菜单中选择**丢弃并生成事件**。点击“确定”。

e. 通过点击**过滤器**文本字段右侧的 **X** 来清除过滤器。

f. 从规则的**规则内容**部分中选择 **SID**。在**输入 SID** 过滤器弹出窗口中输入 **336**。点击**确定**。

g. 选中规则旁边的复选框。从**规则状态**下拉菜单中选择**丢弃并生成事件**。点击**确定**。



注意：此规则在端口 21 上建立的 FTP 流量中查找对根主目录的更改。它仅查找来自外部网络的流量，但是在实验中，我们使用 $EXTERNAL_NET 的默认值（即 any），从而双向均可触发规则。

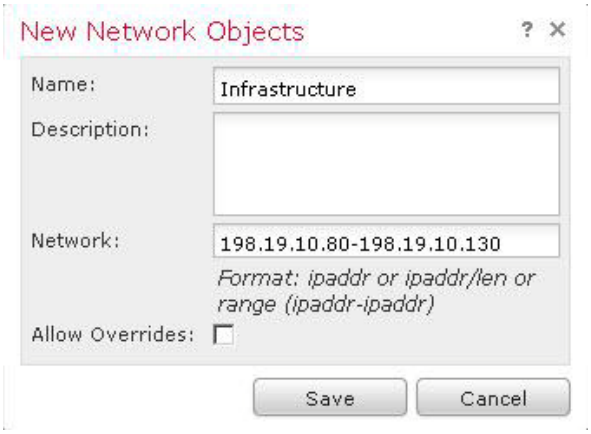
一个有趣的练习是修改此规则以在任意方向的 FTP 流量中进行搜索，以及使用 appid 属性检测任何端口上的 FTP 流量。

5. 点击左上方菜单中的**策略信息**。

6. 点击**确认更改**。点击**确定**。

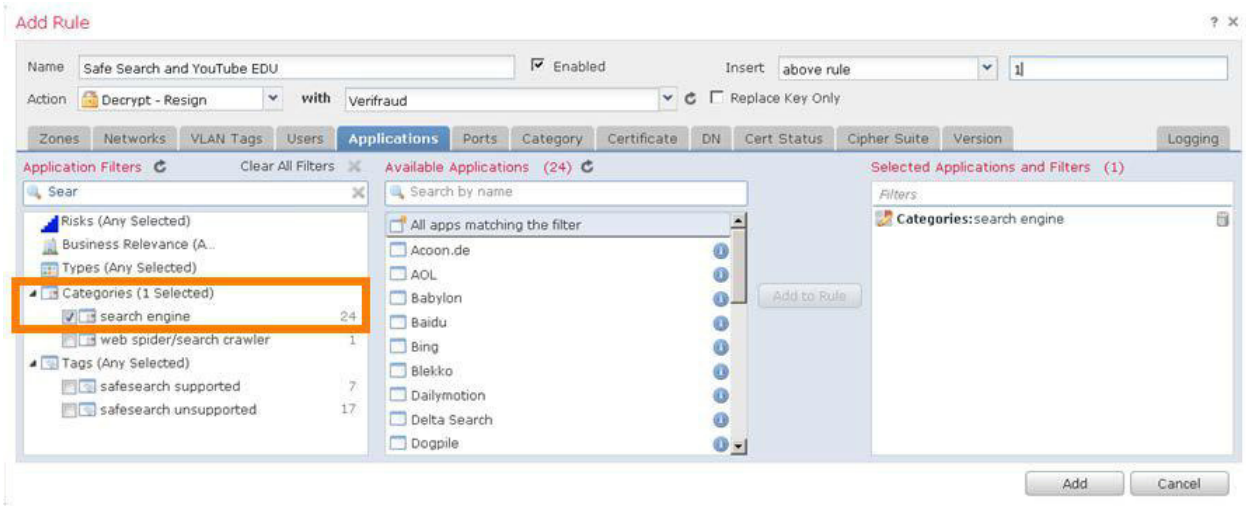
配置 A1.4：演示 SSL 策略

1. 导航至**对象 > 对象管理 > PKI > 内部 CA**。
    a. 点击**导入 CA**。
    b. 在**名称**字段，输入 **`Verifraud`**。
    c. 点击文本**证书数据**右侧的**浏览**按钮，**或者选择文件**。
    d. 浏览至 Jump Desktop 上的 **Certificates** 文件夹。
    e. 上传 **Verifraud_CA.cer**。
    f. 点击文本*密钥*右侧的**浏览**按钮，*或者选择文件*。
    g. 上传 **Verifraud_CA.key**。
    h. 点击**保存**。
2. 系统会将您从解密基础结构设备（例如，FMC 和 AMP 私有云）中免除。为此，请创建包含这些设备的网络对象。
    a. 导航至**对象 > 对象管理 > 网络**。
    b. 点击**添加网络 > 添加对象**。
    c. 在**名称**字段，输入 **`Infrastructure`**。
    d. 在“网络”字段，输入 **`198.19.10.80-198.19.10.130`**。



    e. 点击**保存**以保存网络对象。
3. 导航至**策略 > 访问控制 > SSL**。
4. 点击文本**添加新策略**或点击**新建策略**按钮。
    a. 在**名称**字段，输入 **`Demo SSL Policy`**。
    b. 使默认操作保留为**不解密**。
    c. 点击**保存**。等待几秒钟，然后该策略将打开进行编辑。

5. 点击**添加规则**。
    a. 在**名称**字段，输入 **`Exempt Infrastructure`**。
    b. 使**操作**保留设置为**不解密**。
    c. 在**网络**选项卡中的**网络**下，选择**基础结构**，然后点击**添加到源**。
    d. 点击**添加**以将此规则添加到 SSL 策略中。
6. 点击**添加规则**。
    a. 在**名称**字段，输入 **Decrypt Search Engines**。
    b. 将**操作**设置为**解密 - 重新签名**。
    c. 从词语**带有**右侧的下拉列表中选择 **Verifraud**。
    d. 在**应用**选项卡中的**应用过滤器**下，搜索 **`Sear`**。您将在**类别**下看到**搜索引擎**。选中此复选框，然后点击**添加到规则**。



    e. 选择**日志记录**选项卡，然后选中**在连接结束时进行日志记录**复选框。
    f. 点击**添加**以将此规则添加到 SSL 策略中。
7. 点击**添加规则**。
    a. 在“名称”字段，输入 **`Decrypt Other`**。
    b. 将**操作**设置为**解密 - 重新签名**。
    c. 从词语**带有**右侧的下拉列表中选择 Verifraud。
    d. 选择**日志记录**选项卡，然后选中**在连接结束时进行日志记录**复选框。
    e. 点击**添加**以将此规则添加到 SSL 策略中。

8. 点击**保存**以保存 SSL 策略。

注意：“替换密钥”复选框需要附带说明。只要操作设置为“解密 - 重新签名”，Firepower 就将替换公钥。“替换密钥”复选框确定如何将解密操作应用于自签名服务器证书。

• 如果取消选中“替换密钥”，则自签名证书将与任何其他服务器证书一样处理。在此情况下 Firepower 会替换密钥并对证书进行重新签名。通常，终端配置为信任 Firepower，因此将信任此重新签名的证书。

• 如果选中“替换密钥”，则会以不同方式处理自签名证书。在此情况下 Firepower 会替换密钥并生成新的自签名证书。终端上的浏览器将生成证书警告。

换言之，选中“替换密钥”复选框将使重新签名操作保持对自签名证书缺乏信任。

配置 A1.5：自定义检测列表

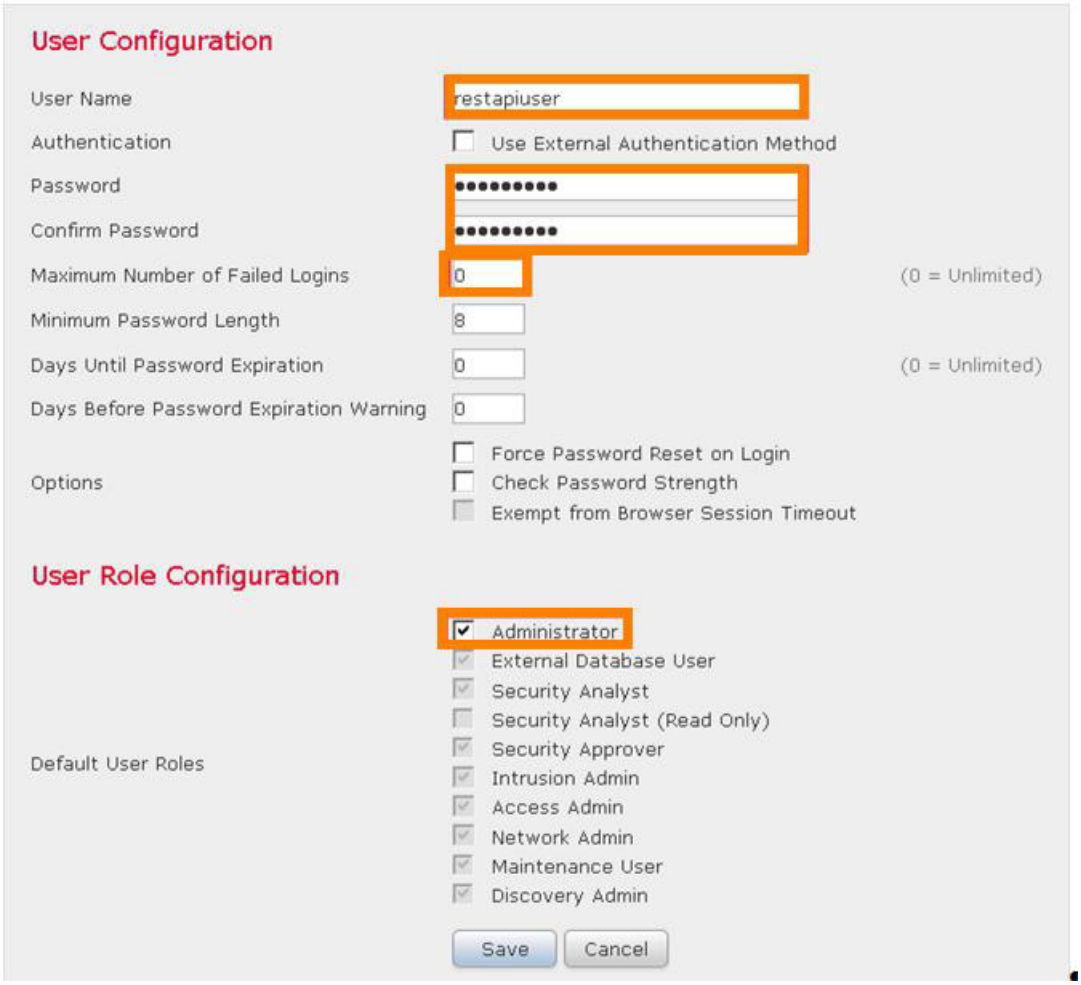
有一个名为 Zombies.pdf 的无害文件，如果云查找成功，它会触发恶意软件事件。有时，实验会出现云连接问题。因此，该文件将添加到自定义检测列表中，以确保它会触发恶意软件事件。

1. 导航至**对象 > 对象管理 > 文件列表**。
2. 点击铅笔图标以编辑 **Custom-Detection-List**。
    a. 从**添加方式**下拉列表中选择**计算 SHA**。
    b. 点击**浏览**。
    c. 浏览至 Jump Desktop 上的 Files 文件夹。
    d. 选择 **Zombies.pdf**，然后点击**确定**。
    e. 点击**计算并添加 SHA**。
    f. 点击**保存**。

配置 A1.6：添加 restapiuser

单独使用 API 资源管理器很方便。这样可以同时使用 FMC 和 API 资源管理器。

1. 导航至**系统 > 用户**。点击**创建用户**。
    a. 在**用户名**字段，输入 **restapiuser**。
    b. 在**密码**字段，输入 **C1sco12345**。确认密码。
    c. 将“最大失败登录次数”设置为 **0**。
    d. 选中**管理员**选项卡。



配置 A1.7：安装服务器证书

默认情况下，FMC UI 使用自签名证书。该证书会替换为 Jump 浏览器信任的 pod AD 服务器签名的证书。

1. 导航至**对象 > 对象管理 > PKI > 可信 CA**。
    a. 点击**添加可信 CA**。
    b. 在**名称**字段，输入 **dCloud**。
    c. 点击文本**证书数据**右侧的**浏览**按钮，**或者选择文件**。
    d. 浏览至 Jump Desktop 上的 **Certificates** 文件夹。
    e. 上传 **AD-ROOT-CA-CERT.cer**。
    f. 点击**保存**。
2. 通过 SSH 连接到 FMC CLI。通过键入 **sudo -i** 成为 root。Sudo 密码为 **C1sco12345**
    a. 键入 **cd /etc/ssl**，然后键入 **cp server* /root**。
    b. 键入 **cat > /etc/ssl/server.crt**
    c. 从 Jump Desktop 上的 **Certificates** 文件夹中，使用 Notepad++ 编辑文件 **fmc.cer**。
    d. 全选，然后复制并粘贴到 FMC CLI 中
    e. 键入 **Ctrl+D**。
    f. 键入 **cat > /etc/ssl/server.key**
    g. 从 Jump Desktop 上的 **Certificates** 文件夹中，使用 Notepad++ 编辑文件 **fmc.key**。
    h. 全选，然后复制并粘贴到 FMC CLI 中
    i. 键入 **Ctrl+D**。
    j. 键入 **pmtool restartbyid httpsd**。

附录 B：REST API 脚本

以下是在第一个实验练习中使用的两个 Python 脚本。您只运行了第一个脚本 **register_config.py**。它将调用第二个脚本 **connect.py**，该脚本将会创建已编译的文件 **connect.pyc**。

Python 脚本 register_config.py

```
#!/usr/bin/python
import json
import connect
import sys

host = "fmc.example.com"
username = "restapiuser"
password = "C1sco12345"
name="NGFW"

#connect to the FMC API
headers,uuid,server = connect.connect (host, username, password)

user_input = str(raw_input("Would you like to register the managed device? [y/n]"))
if user_input == "y":
 policy_name = str(raw_input("Enter name of new Access Control Policy to be create:"))
 access_policy = {
 "type": "AccessPolicy",
 "name": policy_name,
 "defaultAction": { "action": "BLOCK" }
 }
 post_response = connect.accesspolicyPOST(headers,uuid,server,access_policy)
 policy_id = post_response["id"]
 print "\n\nAccess Control Policy\n" + policy_name + "\ncreated\n\n"
 device_post = {
 "name": name,
 "hostName": "ngfw.example.com",
 "regKey": "C1sco12345",
 "type": "Device",
 "license_caps": [
 "BASE",
 "MALWARE",
 "URLFilter",
 "THREAT"
 ],
 "accessPolicy": {
 "id": policy_id,
 "type": "AccessPolicy"
 }
 }
 post_data = json.dumps(device_post)

 output = connect.devicePOST (headers, uuid, server, post_data)
# print "\n\nPost request is: \n" + json.dumps(output,indent=4) + "\n\n"

# GET ALL THE DEVICES AND THEIR corresponding interfaces

user_input = str(raw_input("In the FMC UI, confirm that the device discovery has completed and then
press 'y' to continue or 'n' to exit.[y/n]"))
headers,uuid,server = connect.connect (host, username, password)
```

```
if user_input == "n":
 quit()

devices = connect.deviceGET(headers,uuid,server)
for device in devices["items"]:
 if device["name"] == name:
 print "DEVICE FOUND, setting ID"
 device_id = device["id"]

# NOW THAT WE HAVE THE DEVICE ID WE NEED TO GET ALL THE INTERFACES

interfaces = connect.interfaceGET(headers,uuid,server,device_id)
# Interfaces i want to change
interface_1 = "GigabitEthernet0/0"
interface_2 = "GigabitEthernet0/1"

for interface in interfaces["items"]:
 if interface["name"] == interface_1:
 interface_1_id = interface["id"]
 print "interface 1 found"
 if interface["name"] == interface_2:
 interface_2_id = interface["id"]
 print "interface 2 found"

user_input = str(raw_input("Would you like to configure device interfaces? [y/n]"))

if user_input == "y":
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "outside",
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/0",
 "id": interface_1_id,
 "ipv4" : {
 "static": {
 "address":"198.18.133.2",
 "netmask":"18"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_1_id)
 interface_put = {
 "type": "PhysicalInterface",
 "hardware": {
 "duplex": "AUTO",
 "speed": "AUTO"
 },
 "enabled": True,
 "MTU": 1500,
 "managementOnly": False,
 "ifname": "inside",
```

```
 "enableAntiSpoofing": False,
 "name": "GigabitEthernet0/1",
 "id": interface_2_id,
 "ipv4" : {
 "static": {
 "address":"198.19.10.1",
 "netmask":"24"
 }
 }
 }
 put_data = json.dumps(interface_put)
 connect.interfacePUT (headers, uuid, server, put_data,device_id,interface_2_id)
```

Python 脚本 connect.py

```
#!/usr/bin/python
import json
import sys
import requests
#Surpress HTTPS insecure errors for cleaner output
from requests.packages.urllib3.exceptions import InsecureRequestWarning

requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

#define fuction to connect to the FMC API and generate authentication
token def connect (host, username, password):
 headers = {'Content-Type': 'application/json'}
 path = "/api/fmc_platform/v1/auth/generatetoken"
 server = "https://"+host
 url = server + path
 try:
 r = requests.post(url, headers=headers, auth=requests.auth.HTTPBasicAuth(username,password),
verify=False)
 auth_headers = r.headers
 token = auth_headers.get('X-auth-access-token', default=None)
 uuid = auth_headers.get('DOMAIN_UUID', default=None)
 if token == None:
 print("No Token found, I'll be back terminating....")
 sys.exit()
 except Exception as err:
 print ("Error in generating token --> "+ str(err))
 sys.exit()
 headers['X-auth-access-token'] = token

 return headers,uuid,server


def devicePOST (headers, uuid, server, post_data):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.post(url, data=post_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
```

```
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 201 or status_code == 202:
 print("Post was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response


def deviceGET (headers, uuid, server):
 api_path= "/api/fmc_config/v1/domain/" + uuid + "/devices/devicerecords"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfaceGET (headers, uuid, server, device_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces"
 url = server+api_path
 try:
 r = requests.get(url, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200:
 print("GET was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def interfacePUT (headers, uuid, server, put_data,device_id, interface_id):
 api_path= "/api/fmc_config/v1/domain/" + uuid +
"/devices/devicerecords/"+device_id+"/physicalinterfaces/"+interface_id
```

```
 url = server+api_path
 try:
 r = requests.put(url, data=put_data, headers=headers, verify=False)
 status_code = r.status_code
 resp = r.text
 json_response = json.loads(resp)
 print("status code is: "+ str(status_code))
 if status_code == 200 :
 print("Put was sucessfull...")
 else:
 r.raise_for_status()
 print("error occured in POST -->"+resp)
 except requests.exceptions.HTTPError as err:
 print ("Error in connection --> "+str(err))
 finally:
 if r: r.close()
 return json_response

def accesspolicyPOST (headers, uuid, server, post_data):
    api_path= "/api/fmc_config/v1/domain/" + uuid + "/policy/accesspolicies"
    url = server+api_path
    try:
            r = requests.post(url, data=json.dumps(post_data), headers=headers, verify=False)
            status_code = r.status_code
            resp = r.text
            json_response = json.loads(resp)
            print("status code is: "+ str(status_code))
            if status_code == 201 or status_code == 202:
                    print("Post was sucessfull...")
            else:
                    r.raise_for_status()
                    print("error occured in POST -->"+resp)
    except requests.exceptions.HTTPError as err:
            print ("Error in connection --> "+str(err))
    finally:
            if r: r.close()
    return json_response
```

附录 C：ISE RA VPN 配置

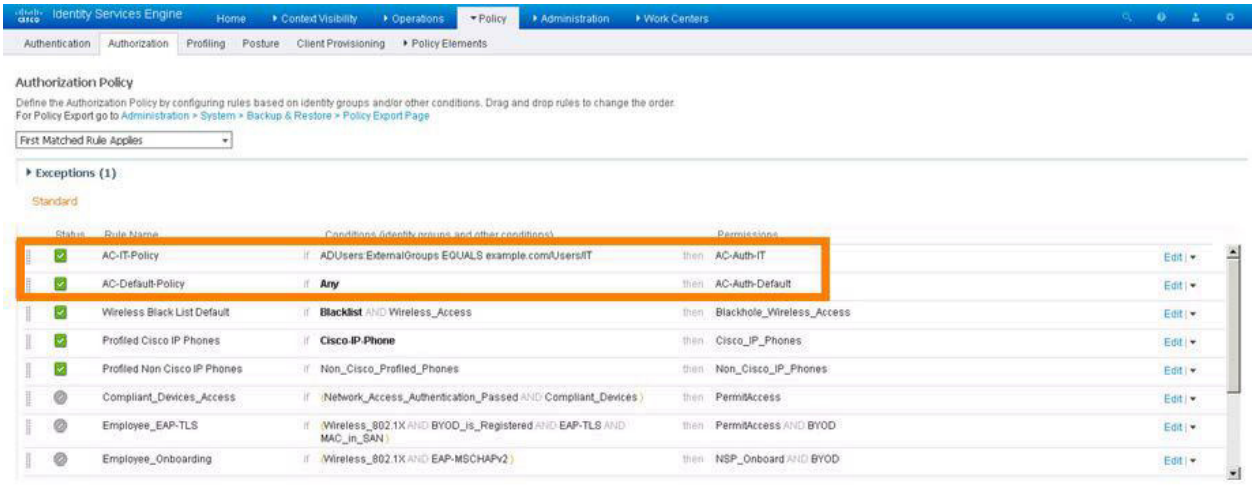
ISE 配置为支持所有实验练习。在本附录中，对此配置进行了总结。请注意，在 Firefox 书签工具栏上有一个 ISE 链接。凭证应该会预填充。其中，用户名为 **admin**，密码为 **C1sco12345**。

注意：本附录不是关于 ISE 的教程。它没有详细说明如何配置 ISE，只介绍为本指南中的实验练习配置 RA VPN 组件所需的详细信息。配置以自上而下的方式进行了描述。要创建此配置，您可能会首选自下而上构建这些对象。

授权策略

1. 导航至**策略 > 授权**。系统为此实验创建了前两个策略：**AC-IT-Policy** 和 **AC-Default-Policy**。

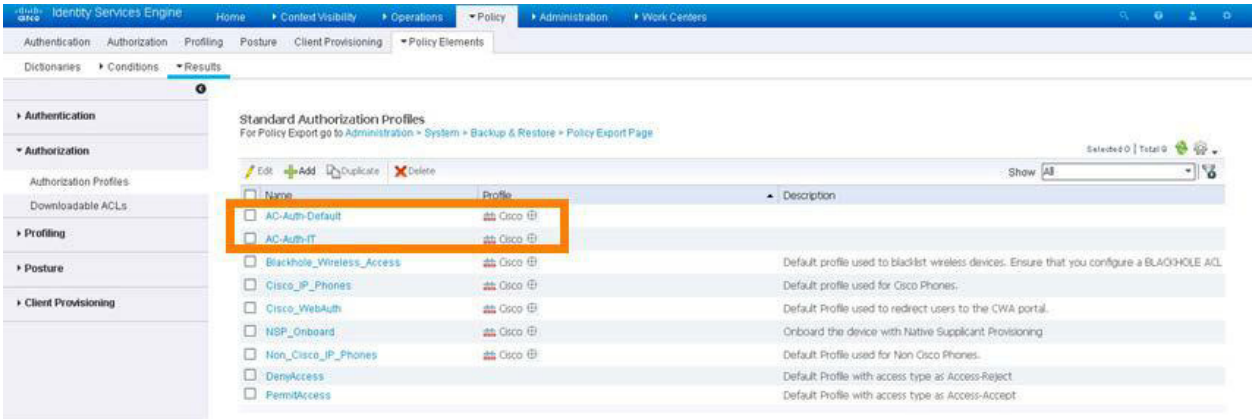
   这些策略引用下面描述的两个授权配置文件：**AC-Auth-IT** 和 **AC-Auth-Default**。



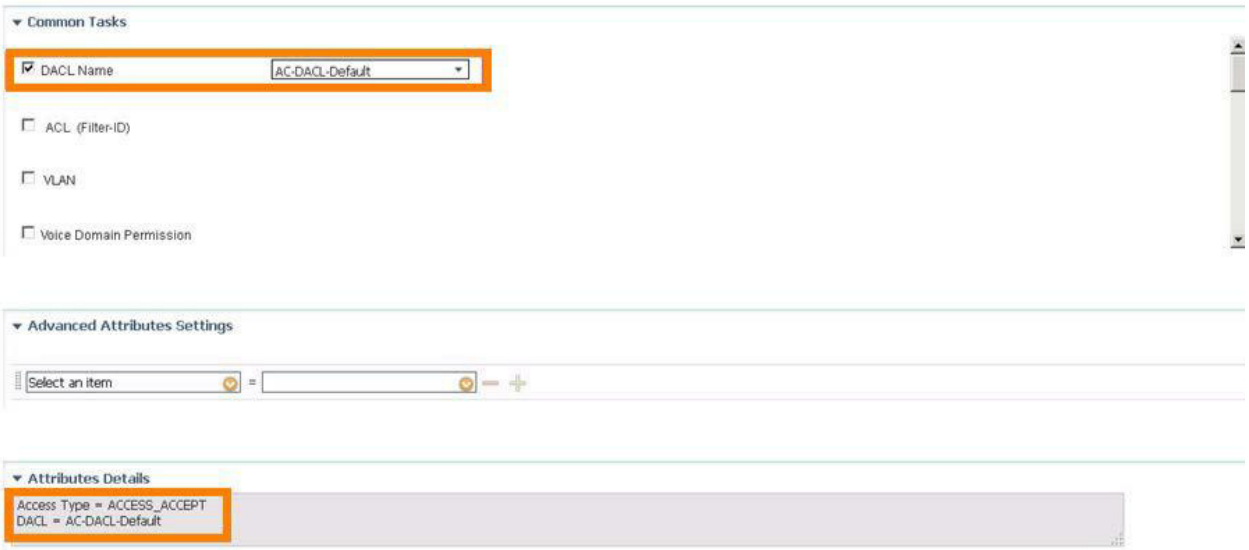
这些策略引用两个授权配置文件：AC-Auth-IT 和 AC-Auth-Default。

授权配置文件

1. 导航至**策略 > 策略元素 > 结果 > 授权 > 授权配置文件**。系统为此实验创建了前两个配置文件：**AC-Auth-Default** 和 **AC-Auth-IT**。



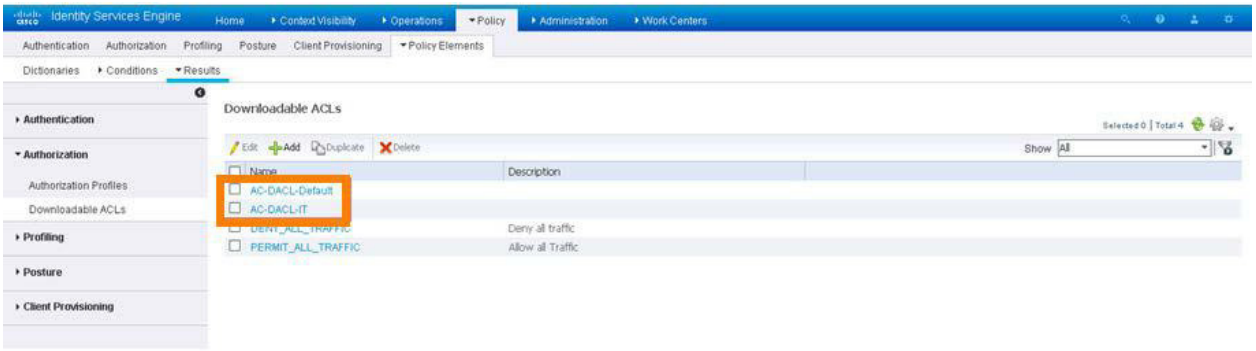
2. 如果深入查看 **AC-Auth-Default**，您会发现它引用的是下面描述的 **DACL AC-DACL-Default**。



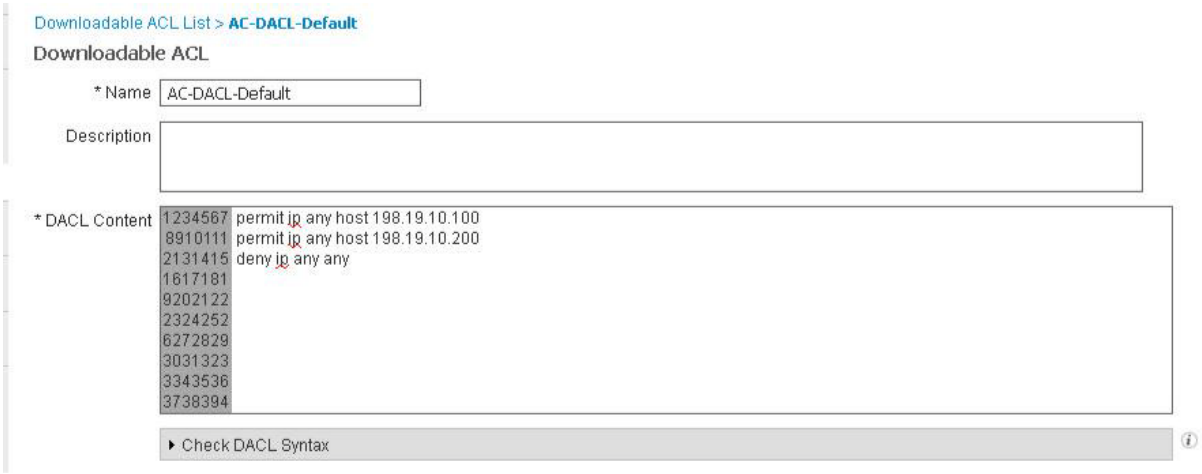
3. 如果深入查看 **AC-Auth-IT**，您会发现它引用的是下面描述的 **DACL AC-DACL-IT**。它还具有两个高级属性：一个用于地址池，一个用于组策略。

可下载 ACL

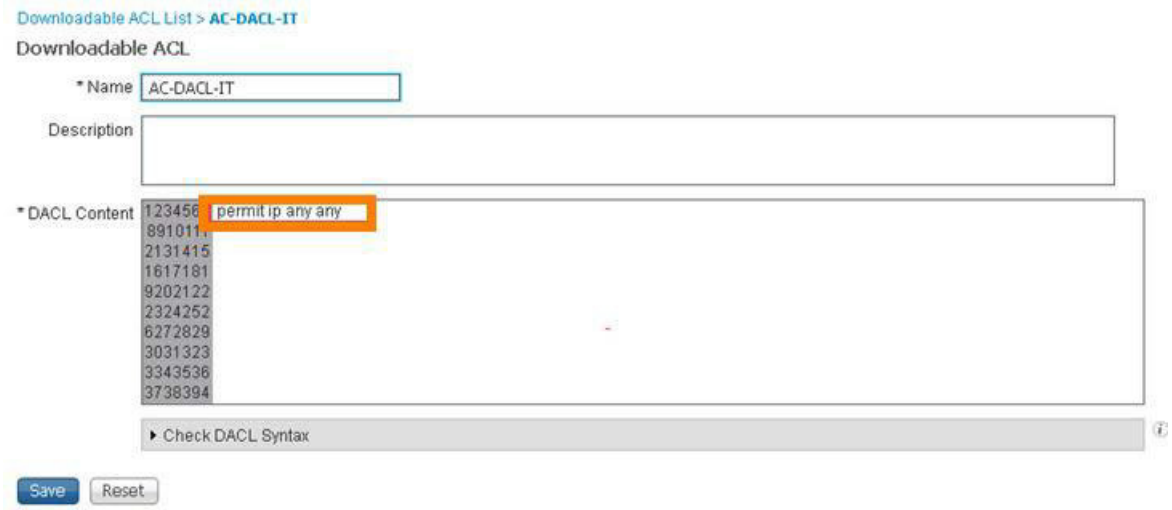
1. 导航至**策略 > 策略元素 > 授权 > 可下载 ACL**。系统为此实验创建了前两个 DACL：**AC-DACL-Default** 和 AC-DACL-IT。



2. 如果深入查看 **AC-DACL-Default**，您会发现它将访问限于 198.19.10.100 和 198.19.10.200。



3. 如果深入查看 **AC-DACL-IT**，您会发现没有任何限制。



附录 D：使用 Alien Vault 作为 TAXII 源

本附录提供免费 TAXII 源 Hail a TAXII 的替代方法。这包含以下任务：

- 在 Alien Vault 中创建帐户
- 获取 API 令牌
- 使 CTID 订阅 Alien Vault TAXII 源

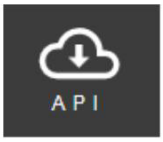
步骤

在 Alien Vault 中创建帐户

1. 导航至 https://otx.alienvault.com
    a. 输入用户名、有效邮件地址和密码。
    b. 点击**登录**。
2. 登录到您用于步骤 1a 的邮件帐户，然后点击确认链接。
    a. 点击确认链接。
    点击来自陌生帐户的邮件中的链接？是的！
    b. 在**确认**按钮出现时点击该按钮。
    c. 点击**登录**以登录到您的 Alien Vault 帐户。

获取 API 令牌

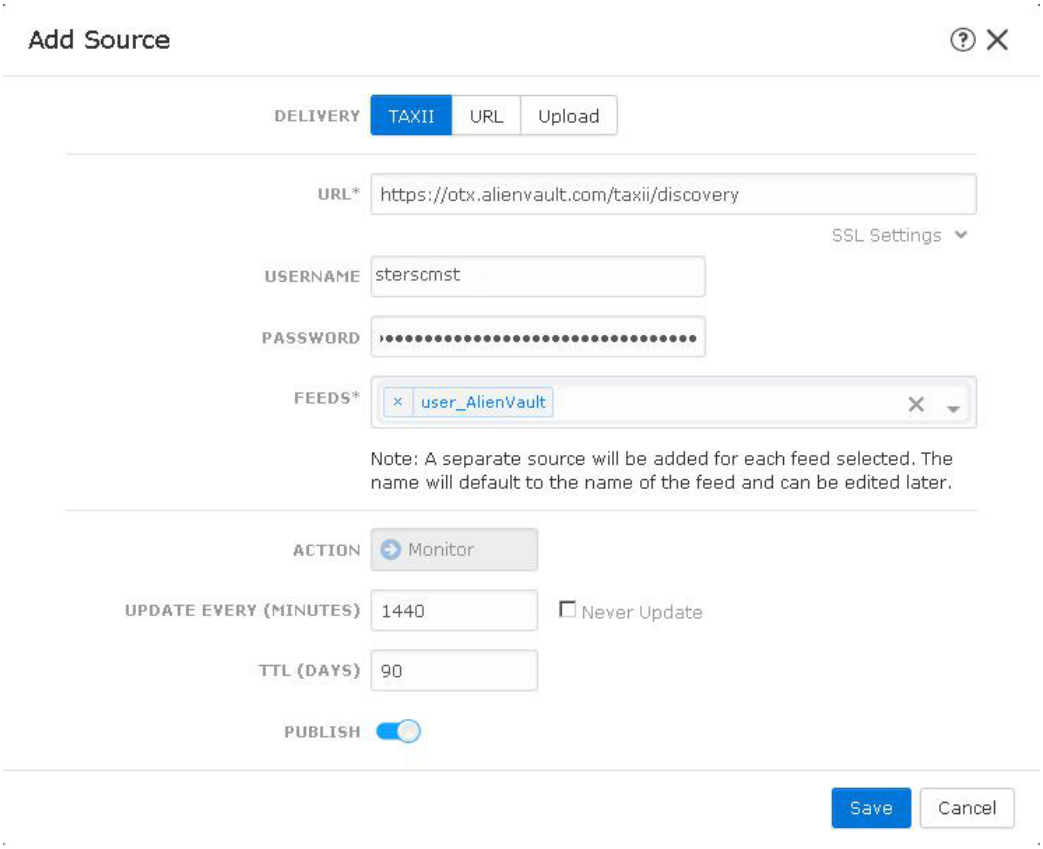
1. 在您的 Alien Vault 帐户中，点击页面中心顶部附近的 API 链接。



2. 在页面的右侧，点击 API 令牌右侧的“复制”按钮。您可能希望将此令牌保存到文件。

使 CTID 订阅 Alien Vault TAXII 源

1. 导航至**情报 > 来源 > 来源**。点击右侧的加号以添加情报来源。
    a. 对于**交付**，选择 **TAXII**。
    b. 在 **URL** 字段，输入 **https://otx.alienvault.com/taxii/discovery**
    c. 在**用户名**字段，输入 Alien Vault 登录名。
    d. 在**密码**字段，粘贴从 Alien Vault 帐户复制的 API 令牌。
    e. 对于**源**，选择 **user_AlienVault**。请注意，填充**源**下拉列表可能需要几秒钟时间。
    f. 确认屏幕如下图所示。



    g. 点击*保存*。

2. 等待直至此源的“状态”列从“正在下载”更改为“正在解析”。不要等待解析完成，这将花费太长时间。
3. 导航至**情报 > 来源 > 指标**。确认已添加多个 URL 指标。
4. 导航至**情报 > 来源 > 可观察对象**。确认已添加多个 URL 可观察对象。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。