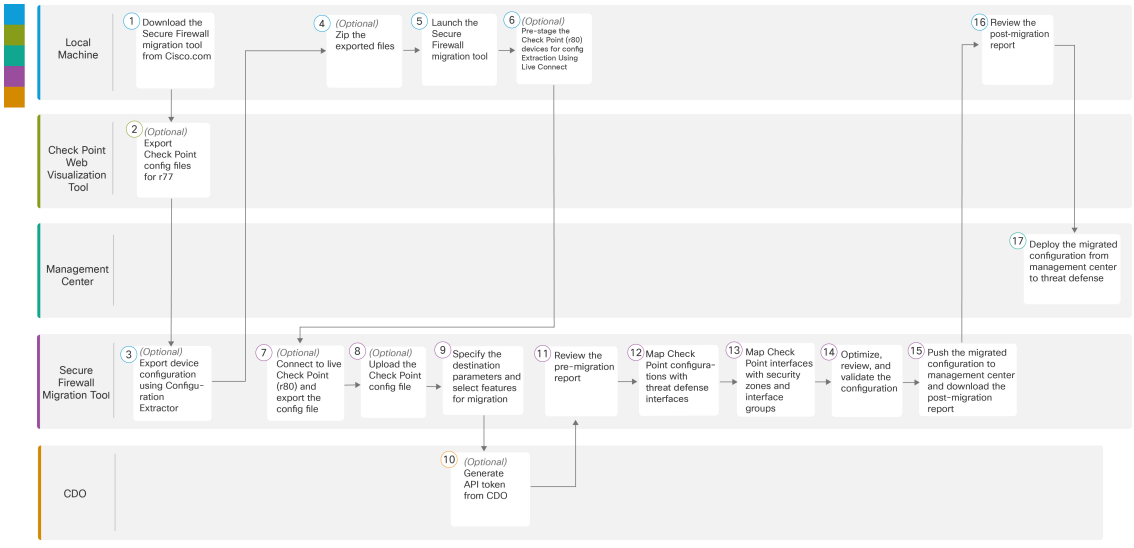
Check Point 到威胁防御迁移工作流程

端到端程序

以下流程图说明了使用 Cisco Secure Firewall 迁移工具将 Check Point 防火墙迁移到威胁防御的工作流程。



	工作空间	步骤
1	本地计算机	从 Cisco.com 下载最新版本的 Cisco Secure Firewall 迁移工具。有关详细步骤，请参阅从 Cisco.com 下载 Cisco Secure Firewall 迁移工具。

	工作空间	步骤
2	Check Point Web 可视化工具	（可选）导出 r77 的 Check Point 配置文件：要导出 r77 的 Check Point 配置文件，请参阅 导出 Check Point r77 配置文件，第 4 页。如果要使用 Cisco Secure Firewall 迁移工具的实时连接功能导出 r80 的配置文件，请跳至步骤 5。
3	本地计算机	在本地计算机上启动 Cisco Secure Firewall 迁移工具，然后根据您的要求在 **源防火墙供应商** 下拉列表中选择 **Check Point (r75 – r77)** 或 **Check Point (r80 – r81)** 。有关详细信息，请参阅 启动 Cisco Secure Firewall 迁移工具 。
4	Cisco Secure Firewall 迁移工具	（可选）从 Check Point (r75 – r77) 导出设备配置：要使用 **配置提取器** 通过安全网关连接导出 r77 的设备配置，请参阅 使用配置提取器导出设备配置，第 5 页。
5	本地计算机	（可选）压缩导出的文件：选择 r77 的所有导出配置文件，并将其压缩为 zip 文件。有关详细步骤，请参阅 压缩导出的文件。
6	本地计算机	预先配置 Check Point (r80) 设备以配置提取：在防火墙迁移工具上使用 Live Connect 之前，必须在 Check Point (r80) 设备上配置凭证。有关在 Check Point (r80) 设备上预先配置的凭证，请参阅 使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取。仅当您计划迁移 r80 设备的配置文件时，才需要执行此步骤。如果要从 r77 设备迁移配置，请跳至步骤 8。
7	Cisco Secure Firewall 迁移工具	（可选）连接到实时 Check Point (r80) 并导出配置文件：要使用实时连接功能导出适用于 r80 的 Check Point 配置文件，请参阅 导出 Check Point r80 配置文件的程序。
8	Cisco Secure Firewall 迁移工具	（可选）上传 Check Point 配置文件：有关上传 Check Point 配置文件的详细步骤，请参阅 上传 Check Point 配置文件。
9	Cisco Secure Firewall 迁移工具	在此步骤中，您可以指定迁移的目标参数。有关详细步骤，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数。
10	CDO	（可选）此步骤为可选，并且仅当您选择云交付的防火墙管理中心作为目标管理中心时才需要。有关详细步骤，请参阅 为 Cisco Secure Firewall 迁移工具指定目标参数。
11	Cisco Secure Firewall 迁移工具	导航到下载预迁移前报告的位置并查看报告。有关详细步骤，请参阅查看迁移前报告。
12	Cisco Secure Firewall 迁移工具	Cisco Secure Firewall 迁移工具允许您将 Check Point 配置与威胁防御接口进行映射。有关详细步骤，请参阅 将 Check Point 防火墙 配置与 威胁防御 接口映射。

	工作空间	步骤
13	Cisco Secure Firewall 迁移工具	为确保正确地迁移 Check Point 配置，您需要将 Check Point 接口映射到相应的威胁防御接口对象、安全区和接口组。有关详细步骤，请参阅 将 Check Point 接口映射到安全区 和 接口组。
14	Cisco Secure Firewall 迁移工具	优化并仔细检查配置并验证它是否正确且与您需要的威胁防御设备配置方式匹配。有关详细步骤，请参阅优化， 检查和验证配置。
15	Cisco Secure Firewall 迁移工具	迁移过程中的这一步骤会将迁移的配置发送到管理中心，并允许您下载迁移后报告。有关详细步骤，请参阅将迁移的配置推送到管理中心。
16	本地计算机	导航到下载迁移后报告的位置并查看报告。有关详细步骤，请参阅查看 Check Point 的迁移后报告并完成迁移。
17	管理中心	将迁移的配置从管理中心部署到威胁防御。有关详细步骤，请参阅查看 Check Point 的迁移后报告并完成迁移。

迁移的前提条件

在迁移 Check Point 配置之前，请执行以下活动：

从 Cisco.com 下载 Cisco Secure Firewall 迁移工具

开始之前

您必须拥有 Windows 10 64 位或者 macOS 10.13 或更高版本的计算机，并通过互联网连接至 Cisco.com。

步骤 1 在您的计算机上，为 Cisco Secure Firewall 迁移工具创建一个文件夹。

建议您不要在此文件夹中存储任何其他文件。当 Cisco Secure Firewall 迁移工具启动时，它会将日志、资源和所有其他文件置于此文件夹中。

注释 每当您下载最新版本的 Cisco Secure Firewall 迁移工具时，请确保创建新文件夹，而不使用现有文件夹。

步骤 2 浏览到 https://software.cisco.com/download/home/286306503/type，然后点击**防火墙迁移工具 (Firewall Migration Tool)**。

上面的链接会引导您进入防火墙 NGFW Virtual 下面的 Cisco Secure Firewall 迁移工具。您还可以从 威胁防御 设备下载区域中下载 Cisco Secure Firewall 迁移工具。

步骤 3 将 Cisco Secure Firewall 迁移工具的最新版本下载到您创建的文件夹中。

下载适用于 Windows 或 macOS 计算机的 Cisco Secure Firewall 迁移工具的相应可执行文件。

下一步做什么

导出 Check Point 配置文件

导出 Check Point 配置文件

您可以为以下导出 Check Point 配置文件：

- 导出 Check Point r77 配置文件
- 导出 Check Point r80 配置文件

导出 Check Point r77 配置文件

要导出 Check Point r80 配置文件，请执行以下操作：

- 使用 Check Point Web 可视化工具 (WVT) 导出配置
- 使用配置提取器导出设备配置 ， 第 5 页
- 压缩导出的文件

使用 Check Point Web 可视化工具 (WVT) 导出配置

步骤 1 在有权访问 Check Point 管理服务器的工作站上打开命令提示符。

步骤 2 从适用于 Check Point 防火墙版本的 Check Point 门户下载 WVT。

步骤 3 解压缩 WVT zip 文件。

步骤 4 在提取 Check Point WVT 工具的同一根文件夹下创建新的子文件夹。

步骤 5 将命令提示符中的目录更改为存储 WVT 的目录，并执行以下命令：

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file] [-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go] [-w Web_Visualization_Tool_installation_directory]
```

例如，

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1  -u admin -p admin123 -o  Outputs
```

执行以下命令时，*Outputs* 目录中总共创建七个文件：

命令	说明
C:\Web_Visualisation_Tool	WVT 工具的根目录。
172.16.0.1	Check Point 管理服务器的 IP 地址。
admin	Check Point 管理服务器用户名。
Admin123	Check Point 管理服务器密码。
Outputs	存储输出文件的相对路径。

注释 安全策略和 NAT 策略文件的名称必须分别为 `Security_Policy.xml` 和 `NAT_Policy.xml`。如果文件名不同，请手动重命名。

如果有多个安全和 NAT 策略文件，请确保仅选择并保留要迁移的 Check Point 设备的 `Security_Policy.xml` 和 `NAT_Policy.xml` 文件。

下一步做什么

使用配置提取器导出设备配置

使用配置提取器导出设备配置

步骤 1 在 **选择源配置** 页面中，选择 **检查点 (r75 - r77)**，然后点击 **开始迁移**。

步骤 2 在 **配置提取器** 窗格上，点击 **连接** 到要使用 Cisco Secure Firewall 迁移工具迁移策略的 Check Point Security Gateway。

要进行连接，您需要以下信息：

a) IP 地址
b) 端口
c) 管理用户名
d) Admin 密码
e) 专家密码
f) （可选） 虚拟 ID 号

步骤 3 等待，直到您看到 `networking.txt` 文件下载到本地计算机。

以下命令由配置提取器在后台执行，并作为 `networking.txt` 文件下载：

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

例如，172.16.0.1 是要迁移策略的 Check Point Firewall Gateway 的 IP 地址。

步骤 4 如果您尝试从拥有虚拟 ID 的 Check Point VSX (Virtual System eXtension) 版本 R77 导出配置，背景中将执行以下命令：

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **设置虚拟系统 <vsid>**

  提示　　**vsid** 表示虚拟系统 ID。

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

步骤 5 将 .txt 文件移动到 `Outputs` 文件夹。

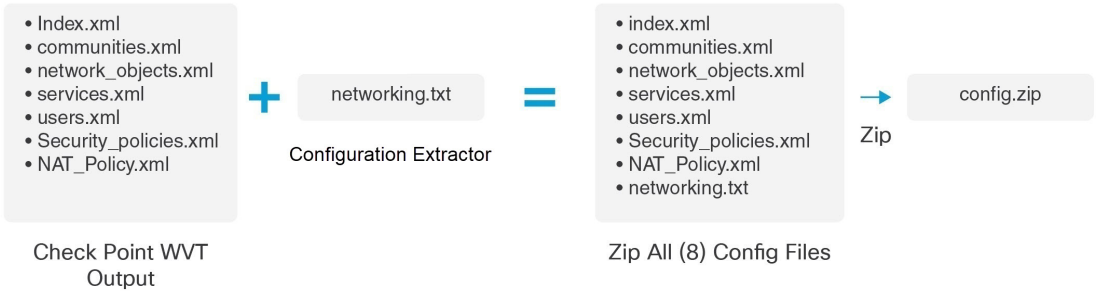
下一步做什么

压缩导出的文件

压缩导出的文件

选择所有八个文件（Web 可视化工具 (WVT) 中的七个文件和配置提取器中的一个 .txt 文件）并将其压缩为 Zip 文件。

注释　　在压缩要迁移的文件之前，请确保 `Security_Policy.xml` 和 `NAT_Policy.xml` 文件适用于要迁移到威胁防御的 Check Point 设备。



注释　不支持 .tar 或其他压缩文件类型。

下一步做什么

上传 Check Point 配置文件

运行迁移

启动 Cisco Secure Firewall 迁移工具

只有在使用桌面版本的 Cisco Secure Firewall 迁移工具时此任务才适用。如果您使用的是 CDO 上托管的迁移工具的云版本，请跳至 上传 Check Point 配置文件 。

注释　当您启动 Cisco Secure Firewall 迁移工具时，会在单独的窗口中打开控制台。进行迁移时，控制台会显示 Cisco Secure Firewall 迁移工具中的当前步骤的进度。如果控制台未显示在屏幕上，则它最有可能隐藏在 Cisco Secure Firewall 迁移工具后。

开始之前

- 从 Cisco.com 下载 Cisco Secure Firewall 迁移工具
- 查看并验证支持的迁移目标管理中心部分中的要求。
- 确保您的计算机带有最新版本的 Google Chrome 浏览器以运行 Cisco Secure Firewall 迁移工具。有关如何将 Google Chrome 设置为默认浏览器的信息，请参阅将 Chrome 设置为默认 Web 浏览器。
- 如果您计划迁移大型配置文件，请配置睡眠设置，以便在迁移推送时系统不会进入睡眠状态。

步骤 1　在您的计算机上，导航至已在其中下载 Cisco Secure Firewall 迁移工具的文件夹。

步骤 2　执行以下操作之一：

- 在您的 Windows 计算机上，双击 Cisco Secure Firewall 迁移工具可执行文件，在 Google Chrome 浏览器中启动它。

  如果出现提示，请点击**是 (Yes)**，以允许 Cisco Secure Firewall 迁移工具对您的系统作出更改。

  Cisco Secure Firewall 迁移工具会创建所有相关文件并将文件存储在其驻留的文件夹中，包括日志和资源文件夹。

- 在 Mac 上，将 Cisco Secure Firewall 迁移工具 `*.command` 文件移动到所需文件夹，启动终端应用，浏览到安装防火墙迁移工具的文件夹并运行以下命令：

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  # ./Firewall_Migration_Tool-version_number.command
  ```

  Cisco Secure Firewall 迁移工具会创建所有相关文件并将文件存储在其驻留的文件夹中，包括日志和资源文件夹。

  提示 当您尝试打开 Cisco Secure Firewall 迁移工具时，因为没有可识别的开发人员在 Apple 中注册 Cisco Secure Firewall 迁移工具，系统会显示警告对话框。有关无法识别的开发人员打开应用的信息，请参阅无法识别的开发人员打开应用。

  注释 使用 MAC 终端 zip 方法。

步骤 3 在**最终用户许可协议 (End User License Agreement)** 页面上，如果要与思科共享遥测信息，请点击**我同意与思科成功网络共享数据 (I agree to share data with Cisco Success Network)**，否则请点击**我稍后再执行 (I'll do later)**。

当您同意将统计信息发送到思科成功网络时，系统会提示您使用 Cisco.com 帐户登录。如果您选择不向思科成功网络发送统计信息，则使用本地凭证登录 Cisco Secure Firewall 迁移工具。

步骤 4 在 Cisco Secure Firewall 迁移工具的登录页面上，执行以下操作之一：

- 要与思科成功网络共享统计信息，请点击**使用 CCO 登录 (Login with CCO)** 链接，用您的单点登录凭证登录您的 Cisco.com 帐户。如果您没有 Cisco.com 帐户，请在 Cisco.com 登录页面上创建帐户。

  如果您已使用 Cisco.com 帐户登录，请继续执行步骤 8。

- 如果您在没有互联网访问权限的气隙网络中部署了防火墙，请联系思科技术支持中心以接收使用管理员凭证的内部版本。请注意，此版本不会向思科发送使用情况统计信息，并且思科技术支持中心可以为您提供凭证。

步骤 5 在**重置密码**页面上，输入您的旧密码、新密码，然后确认新密码。

新密码必须包含 8 个或更多字符，并且必须包含大写和小写字母、数字和特殊字符。

步骤 6 点击**重置 (Reset)**。

步骤 7 使用新密码登录。

注释 如果忘记了密码，请从 <*migration_tool_folder*> 中删除所有现有数据并重新安装 Cisco Secure Firewall 迁移工具。

步骤 8 查看迁移前核对表并确保您已完成所有列出的项目。

如果您未完成该核对表中的一个或多个项目，请完成所有项目，然后再继续。

步骤 9 点击**新迁移 (New Migration)**。

步骤 10 在**软件更新检查 (Software Update Check)** 屏幕上，如果您不确定自己是否正在运行 Cisco Secure Firewall 迁移工具的最新版本，请点击 Cisco.com 上的链接以验证版本。

步骤 11 点击**继续 (Proceed)**。

下一步做什么

您可以继续执行以下步骤：

- 如果已将 Check Point 配置导出到您的计算机，请继续执行上传 Check Point 配置文件。
- 如果必须使用 Cisco Secure Firewall 迁移工具从 Check Point (r77) 提取信息，请继续执行导出 Check Point r77 配置文件。
- 如果必须使用 Cisco Secure Firewall 迁移工具从 Check Point (r80) 提取信息，请继续执行导出 Check Point r80 配置文件。

在 Cisco Secure Firewall 迁移工具中使用演示模式

当您启动安全防火墙迁移工具并位于 **选择源配置** 页面时，您可以选择使用 **开始迁移开始执行迁移** 或进入 **演示模式**。

演示模式提供使用虚拟设备执行演示迁移的机会，并可视化实际迁移流程的外观。迁移工具会根据您在**源防火墙供应商**下拉列表中所做的选择触发演示模式；您还可以上传配置文件或连接到实时设备并继续迁移。您可以通过选择演示源和目标设备（例如演示 FMC 和演示 FTD 设备）来继续执行演示迁移。

注意 选择 **演示模式** 会清除现有的迁移工作流程（如果有）。如果在 **恢复迁移**中有活动迁移时使用演示模式，则在使用演示模式后，活动迁移会丢失，需要重新启动。

您还可以下载并验证迁移前报告、映射接口、映射安全区域、映射接口组，并像在实际迁移工作流程中一样执行所有其他操作。但是，您只能在验证配置之前执行演示迁移。您无法将配置推送到所选的演示目标设备，因为这只是演示模式。您可以验证验证状态和摘要，然后点击**退出演示模式**以再次转到 **选择源配置** 页面以开始实际迁移。

注释 在演示模式下，您可以利用安全防火墙迁移工具的整个功能集（推送配置除外），并在执行实际迁移之前试用端到端迁移程序。

导出 Check Point r80 配置文件

注释 只有 Cisco Secure Firewall 迁移工具上的 Live Connect 功能支持导出 Check Point r80 配置。

要在 Check Point 设备上配置迁移所需的凭证并导出 Check Point 配置文件，请执行以下操作：

- 使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取
- 导出 Check Point r80 配置文件的程序

使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取

迁移前，您可以使用以下任一步骤在 Check Point (r80) 设备上配置凭证：

- 从分布式 Check Point 部署导出 - 当您有独立的 Check Point 安全网关和 Check Point 安全管理器时。
- 从独立 Check Point 部署导出 - 当您的 Check Point 安全网关和 Check Point 安全管理器作为一个设备时。
- 从多域 Check Point 部署导出 - 当您有具备多域部署设置的 Check Point 安全网关和 Check Point 安全管理器时。

从分布式 Check Point 部署导出

必须在使用 Cisco Secure Firewall 迁移工具上的 Live Connect 之前在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在分布式 Check Point 部署上预先配置凭证的程序包括以下步骤：

步骤 1 在 Gaia Console Check Point 安全网关上创建以下内容：

a) 在 Web 浏览器中，通过 HTTPS 会话打开 Check Point Gaia Console 应用以连接到 Check Point 安全网关。

b) 导航至**用户管理 (User Management)** 选项卡，然后选择 **用户 (Users)** > **添加 (Add)**。

c) 在**添加用户**窗口中，使用以下详细信息创建新的用户名和密码：

- 从 **Shell** 下拉列表中，选择 */etc/cli.sh*。
- 从**可用角色**中，选择 *adminRole*。
- 保留其余字段的默认值。
- 点击**确定 (Ok)**。

d) 通过 SSH 连接到 Check Point 安全网关，并使用以下命令创建新密码：
set expert-password <password>

注释
- 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
- 您需要在**连接至 Check Point 安全网关**页面上提供这些凭证，如步骤 3 所示。

配置专家密码后，即完成为 Check Point r80 网关预先配置凭证的程序。

有关详细信息，请参阅图 3: 连接到 Check Point 安全网关。

步骤 2 在 r80 的 Check Point 安全管理器上创建用户名和密码：

a) 在 SmartConsole 应用上，执行以下步骤：

1. 登录 Check Point 安全管理器。
2. 导航至**管理和设置** > **权限和管理员** > **管理员**。
3. 点击 ***** 创建新的用户名和密码，然后执行以下步骤：
   - 选择**身份验证方式**作为 **Check Point 密码**。
   - 点击**设置新密码 (Set New Password)** 以设置新密码。

     注释 切勿选中**用户下次登录时必须更改密码**复选框。
   - 选择**权限配置文件**作为**超级用户**。
   - 选择**到期**为**从不**。
4. 点击**发布 (Publish)** 在 Check Point SmartConsole 应用上保存配置更改。

b) 在 Check Point 安全管理器的 Gaia Console 上，执行以下步骤：

注释 确保您现在创建的用户名和密码与步骤 2a 中在 SmartConsole 应用上创建的用户名和密码相同。

1. 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全管理器。
2. 导航至**用户管理**选项卡，然后选择 **用户** > **添加**。
3. 创建用户名和密码，必须与步骤 2a (3) 中在 SmartConsole 应用上创建的用户名和密码相同。
   - 从 **Shell** 下拉列表中，选择 */bin/bash*。
   - 从**可用角色**下拉列表中，选择 *adminRole*。
   - 保留其余字段的默认值。
   - 点击**确定 (Ok)**。
4. 通过 SSH 连接到 Check Point 安全管理器，并使用以下命令创建专家密码：

   set expert-password <password>

   注释
   - 如果您已配置专家密码，可以使用该密码。
   - 在步骤 2b (3) 和步骤 2a (3) 中创建的用户名和密码必须相同。

在 Check Point 安全管理器的分布式部署中，已完成在 Check Point 上预先配置凭证的程序。

您需要在**连接至 Check Point 安全管理器**页面上提供这些凭证，如步骤 4 所示。

如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 是否将自定义 API 端口用于 Check Point (r80) 安全管理器？ 。

下一步做什么

导出 Check Point r80 配置文件的程序

从独立 Check Point 部署导出

必须在使用 Cisco Secure Firewall 迁移工具上的 Live Connect 之前在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在独立 Check Point 部署上预先配置凭证的程序包括以下步骤：

步骤 1 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到管理 Check Point 安全网关和 Check Point 安全管理器的独立 Check Point 设备。

步骤 2 导航至**用户管理 (User Management)** 选项卡，然后选择 **用户 (Users)** > **添加 (Add)**。

a) 在**添加用户**窗口中，使用以下详细信息创建新的用户名和密码：

- 从 **Shell** 下拉列表中，选择 */etc/cli.sh*。
- 从**可用角色**下拉列表中，选择 *adminRole*。
- 保留其余字段的默认值。
- 点击**确定 (Ok)**。

您需要在**连接至 Check Point 安全网关**页面上提供这些凭证，如步骤 3 所示。

有关详细信息，请参阅图 3: 连接到 Check Point 安全网关。

b) 在**添加用户**窗口中，使用以下详细信息创建另一用户名和密码：

- 从 **Shell** 下拉列表中，选择 */bin/bash*。
- 从**可用角色**下拉列表中，选择 *adminRole*。
- 保留其余字段的默认值。
- 点击**确定 (Ok)**。

步骤 3 在 Check Point 设备的 r80 SmartConsole 应用上创建以下内容：

注释 确保您现在创建的用户名和密码与上一步骤中在 Check Point Gaia Console 应用上创建的用户名和密码相同。

a) 登录 Check Point 设备的 SmartConsole 应用。
b) 导航至**管理和设置** > **权限和管理员** > **管理员**。
c) 点击 *****，使用以下详细信息创建新的用户名和密码：

- 选择**身份验证方式**作为 **Check Point 密码**。
- 点击**设置新密码 (Set New Password)** 以设置新密码。

  注释　　切勿选中**用户下次登录时必须更改密码**复选框。

- 选择**权限配置文件**作为**超级用户**。
- 选择**到期**为**从不**。

步骤 2 的步骤 b 和步骤 3 的步骤 c 中创建的用户名和密码必须相同。

您需要在**连接至 Check Point 安全管理器**页面上提供这些凭证，如步骤 4 所示。

d) 点击**发布 (Publish)** 在 Check Point SmartConsole 应用上保存配置更改。

步骤 4 通过 SSH 连接到 Check Point 设备，并使用以下命令创建专家密码：

set expert-password <password>

注释
- 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
- 步骤 2 的步骤 b 和步骤 3 的步骤 c 中创建的用户名和密码必须相同。

在独立部署中，已完成 Check Point 设备凭证的预先配置。

如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 是否将自定义 API 端口用于 Check Point (r80) 安全管理器？。

下一步做什么

导出 Check Point r80 配置文件的程序

从多域 Check Point 部署导出

必须使用 Cisco Secure Firewall 迁移工具上的 Live Connect 在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在多域 Check Point 部署上预先配置凭证的程序包括以下步骤：

步骤 1 在 Gaia Console Check Point 安全网关上创建以下内容：

a) 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全网关。
b) 导航至**用户管理**选项卡，然后选择 **用户** > **添加**。
c) 在**添加用户**窗口中，使用以下详细信息创建新的用户名和密码：

- 从 **Shell** 下拉列表中，选择 */etc/cli.sh*。

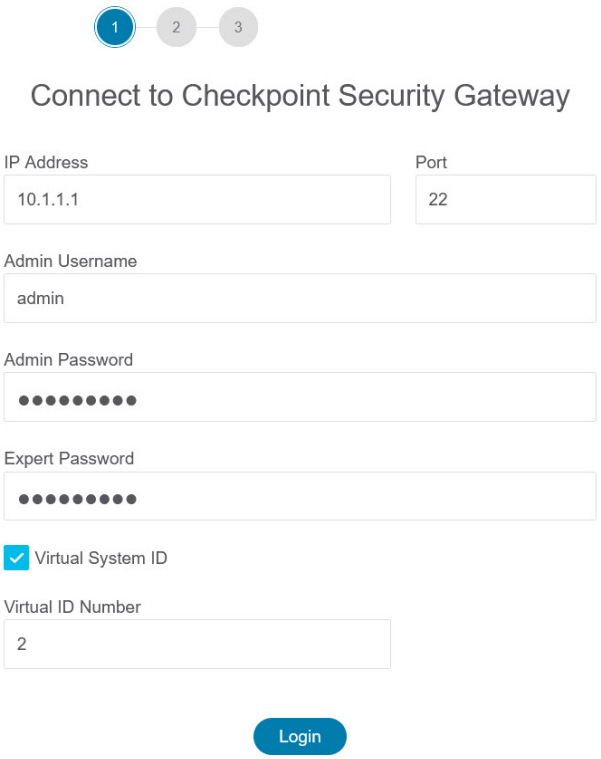
- 从**可用角色**下拉列表中，选择 *adminRole*。
- 保留其余字段的默认值。
- 点击**确定 (Ok)**。

d) 通过 SSH 连接到 Check Point 安全网关，并使用以下命令创建新密码：
set expert-password <password>

在多域部署中，已完成在 Check Point 安全网关上预先配置凭证的程序。

e) （可选）从虚拟系统扩展 (VSX) 设备导出配置时，请选中**虚拟系统 ID (Virtual System ID)** 复选框，以便能够输入虚拟系统 ID。

图 *1:* 连接至 ***Check Point*** 安全网关 - 多域部署



步骤 2 在 Check Point 安全管理器上创建用户名和密码：

a) 在 SmartConsole (mds) 应用上，执行以下步骤：

1. 登录 Check Point 安全管理器。
2. 导航至**管理和设置** > **权限和管理员** > **管理员**。
3. 点击 *****，使用以下详细信息创建新的用户名和密码：
   - 选择**身份验证方式**作为 **Check Point 密码**。
   - 点击**设置新密码 (Set New Password)** 以设置新密码。

注释　　切勿选中**用户下次登录时必须更改密码**复选框。

- 选择**权限配置文件**作为**多域超级用户**。
- 选择**到期**为**从不**。

4. 点击**发布 (Publish)** 在 Check Point SmartConsole 应用上保存配置更改。

   如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 是否将自定义 API 端口用于 Check Point (r80) 安全管理器？ 。

b) 在 Check Point 安全管理器的 Gaia Console 上，执行以下步骤：

注释　　确保您现在创建的用户名和密码与步骤 2a (3) 中在 SmartConsole 应用上创建的用户名和密码相同。

1. 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全管理器。
2. 导航至**用户管理**选项卡，然后选择 **用户** > **添加**。
3. 创建用户名和密码，必须与步骤 2a (3) 中在 SmartConsole 应用上创建的用户名和密码相同。
   - 从 **Shell** 下拉列表中，选择 */bin/bash*。
   - 从**可用角色**下拉列表中，选择 *adminRole*。
   - 保留其余字段的默认值。
   - 点击**确定 (Ok)**。
4. 通过 SSH 连接到 Check Point 安全管理器，并使用以下命令创建新密码：

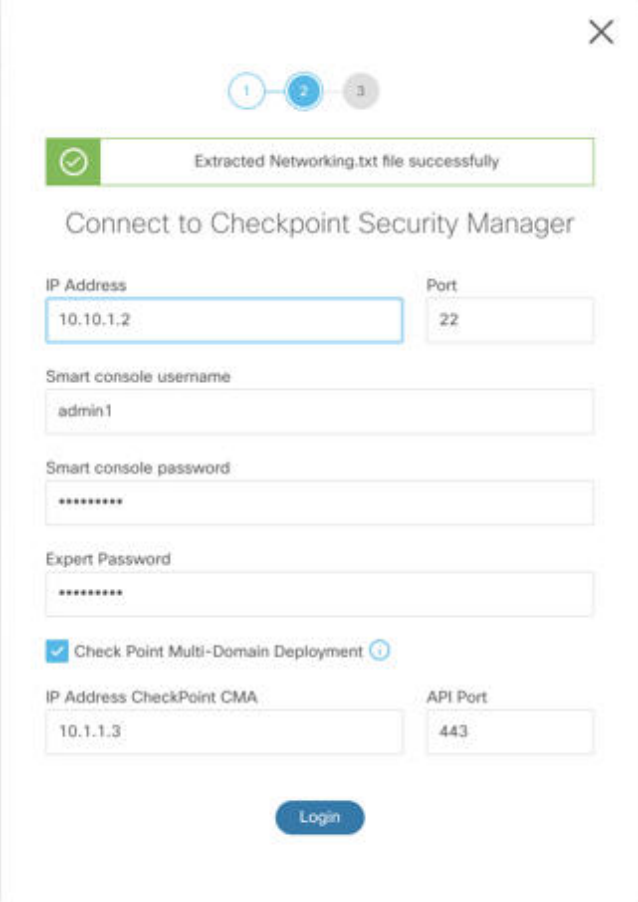
   set expert-password <password>

   注释
   - 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
   - 在步骤 2a (3) 和步骤 2b (3) 中创建的用户名和密码必须相同。

在多域部署中，已完成在 Check Point 安全管理器上预先配置凭证的程序。

您需要使用凭证连接至 Live Connect，如图 2: 连接至 Check Point 安全管理器 - 多域部署 所示。

图 2: 连接至 *Check Point* 安全管理器 - 多域部署



注释

- 如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 是否将自定义 API 端口用于 Check Point (r80) 安全管理器？。
- 无法提取用于多域部署的全局策略包。因此，在 Check Point CMA 下配置为配置的一部分的对象、ACE 规则和 NAT 规则只能导出和迁移。

下一步做什么

导出 Check Point r80 配置文件的程序

是否将自定义 **API** 端口用于 **Check Point (r80)** 安全管理器？

注释 如果您在 Check Point 智能管理器上使用自定义 API 端口，请执行以下步骤：

- 在 Live Connect 的 **Check Point 安全管理器**页面上，选中 **Check Point 多域部署**复选框。
- 如果使用多域部署，请添加 Check Point CMA 的 IP 地址和 API 端口详细信息。
- 如果是常规部署，请保留 Check Point 安全管理器的 IP 地址，并输入自定义 API 端口的详细信息。

导出 Check Point r80 配置文件的程序

开始之前

必须在 Check Point 设备上进行预先配置。有关迁移之前在 Check Point (r80) 设备上配置凭证的详细信息，请参阅使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取。

注释
- 我们建议您使用 Live Connect 提取 Check Point (r80) 配置。
- 若使用未在 Cisco Secure Firewall 迁移工具中通过 Live Connect 导出的 Check Point (r80) 配置，会导致该配置在迁移中不受支持、部分迁移或迁移失败。

  如果配置导出中的信息不完整，则某些配置不会迁移，并标记为**不受支持**。

要导出 Check Point r80 配置文件，请执行以下操作：

步骤 1 从**选择源配置**页面选择 Check Point (r80)。

步骤 2 点击**连接 (Connect)**。

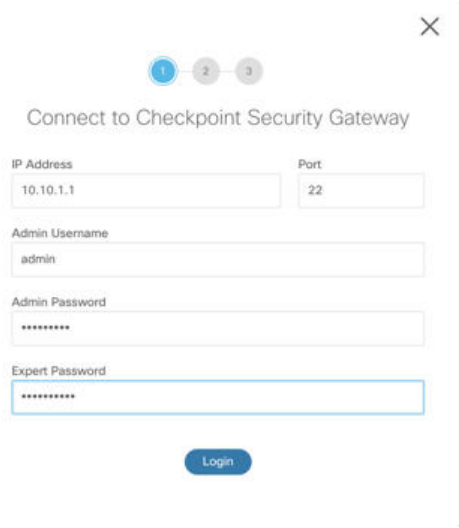
注释 Live Connect 仅适用于 Check Point (r80)。

步骤 3 连接到 Check Point 安全网关。请执行以下操作：

a) 在 Check Point r80 安全网关中输入以下内容：

- IP 地址
- SSH 端口
- 管理用户名
- Admin 密码
- 专家密码

图 *3:* 连接到 *Check Point* 安全网关



b) 点击 **登录 (Login)**。

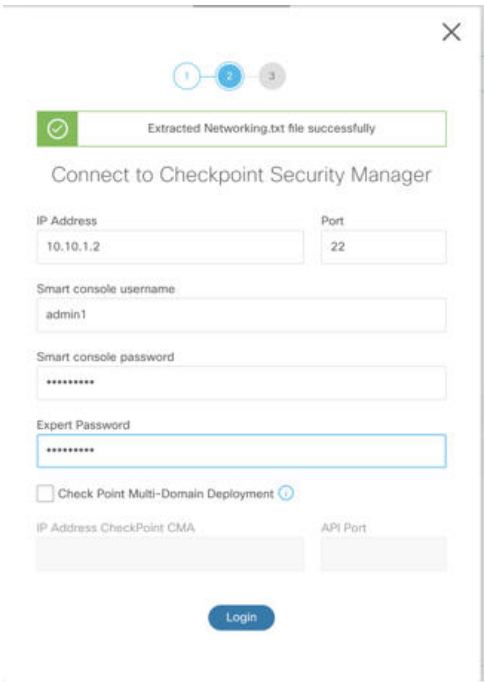
Cisco Secure Firewall 迁移工具会生成包含设备特定配置（例如接口和路由配置）的 *networking.txt* 文件。将 *networking.txt* 文件存储在 Cisco Secure Firewall 迁移工具当前会话的本地目录中。

步骤 4 连接到 Check Point 安全管理器。请执行以下操作：

a) 在 Check Point r80 安全管理器中输入以下内容：

- IP 地址
- SSH 端口
- 智能控制台用户名
- 智能控制台密码
- 专家密码

图 *4:* 连接到 *Check Point* 安全管理器



b) 点击**登录 (Login)**。

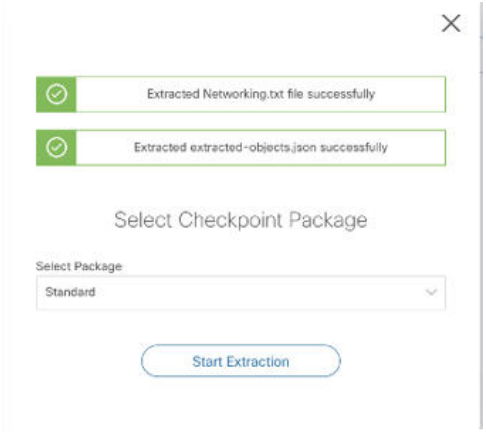
Cisco Secure Firewall 迁移工具会生成 *Extracted-objects.json* 文件，其中记录 Check Point 安全管理器中可用的完整网络和服务对象配置。

将 *Extracted-objects.json* 文件存储在 Cisco Secure Firewall 迁移工具当前会话的本地目录中。

注释　　如果您已将 Cisco Secure Firewall 迁移工具连接到 Check Point 安全管理器，则会显示 Check Point 安全管理器中可用的策略包列表。

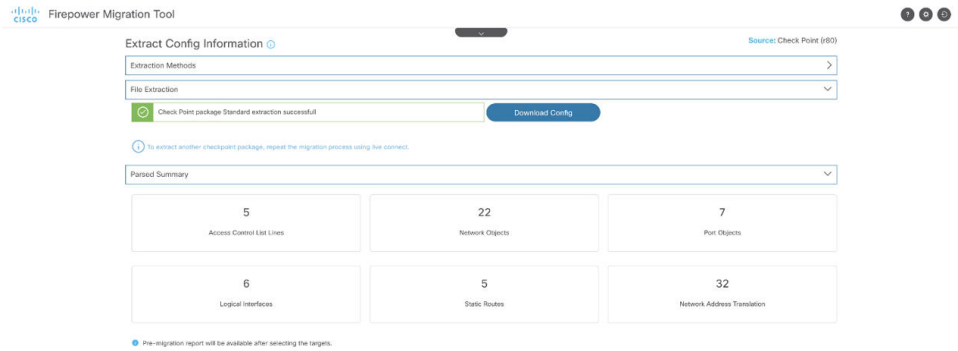
步骤 5 从**选择 Check Point 包 (Select Check Point Package)** 列表中选择要迁移的 Check Point 策略包，然后点击**开始提取 (Start Extraction)**。

图 *5:* 提取 ***Check Point*** 策略包



步骤 6 下载配置并继续迁移。

图 *6:* 在分布式部署和独立部署中，已完成 ***Check Point*** 配置提取



步骤 7 点击**下一步 (Next)** 以继续迁移 Check Point (r80) 配置。

下一步做什么

上传 Check Point 配置文件

提取其他配置文件

要提取其他配置文件，请执行以下步骤：

- 点击**返回源选择 (Back to source selection)** 以提取不同策略包的新配置，或者连接到不同的 Check Point (r80) 防火墙。
- 如果稍后必须迁移提取的 Check Point (r80) 配置，请下载当前配置。

注释 当前配置文件会下载到浏览器设置的默认下载位置。

您可以使用组装流水线方法来提取 r80 配置：

- 执行 Live Connect 以提取每个防火墙包或不同防火墙的 Check Point (r80) 配置文件。
- 为多个配置创建存储库。
- 使用**稍后开始迁移**选项，稍后再通过手动上传继续迁移。

上传 Check Point 配置文件

开始之前

将配置文件导出为 .zip 格式。

步骤 1 在**提取配置信息 (Extract Config Information)** 屏幕上的**手动上传 (Manual Upload)** 部分中，点击**上传 (Upload)** 以上传 Check Point 配置文件。

步骤 2 浏览到保存配置文件的位置。该配置文件是为 Check Point (r77) 提取的，并使用 Live Connect for Check Point (r80) 下载的。点击**打开 (Open)**。

Cisco Secure Firewall 迁移工具会上传配置文件。对于大型配置文件，此步骤需要的时间较长。

预解析过程现已完成。

解析摘要部分显示解析状态。

步骤 3 查看 Cisco Secure Firewall 迁移工具在上传的配置文件中检测和解析的元素的摘要信息。

步骤 4 点击**下一步 (Next)**，选择目标参数。

下一步做什么

为 Cisco Secure Firewall 迁移工具指定目标参数

为 Cisco Secure Firewall 迁移工具指定目标参数

开始之前

- 获得现场防火墙管理中心的 管理中心 的 IP 地址。
- 从 Cisco Secure Firewall 迁移工具 3.0 开始，您可以在本地防火墙管理中心或云交付的防火墙管理中心之间选择。
- 对于云交付的防火墙管理中心，必须提供区域和 API 令牌。关于更多信息，请参阅 支持的迁移目标管理中心。
- （可选） 如果要迁移特定于设备的配置（例如接口和路由），请添加目标 威胁防御 迁移到 管理中心，则将目标威胁防御设备添加到管理中心。请参阅将设备添加到防火墙管理中心

- 如果它要求您在**检查和验证 (Review and Validate)** 页面中将 IPS 或文件策略应用于 ACL，我们强烈建议您在迁移之前在 管理中心 上创建策略。使用相同的策略，因为 Cisco Secure Firewall 迁移工具从连接的管理中心获取策略。创建新策略并将其分配给多个访问控制列表可能会降低性能，也可能导致推送失败。

步骤 1 在**选择目标 (Select Target)** 屏幕的**防火墙管理 (Firewall Management)** 部分中，执行以下操作：您可以选择迁移到本地防火墙管理中心或云交付的防火墙管理中心：

- 要迁移到本地防火墙管理中心，请执行以下操作：

a) 点击**本地 FMC (On-Prem FMC)** 单选按钮。
b) 输入管理中心的 IP 地址或完全限定域名 (FQDN)。
c) 在**域**下拉列表中，选择要迁移到的域。

如果要迁移到 威胁防御 设备，只能迁移到所选域中可用的 威胁防御 设备。

d) 点击**连接 (Connect)** 并继续**步骤 2**。

- 要迁移到云交付的防火墙管理中心，请执行以下操作：

a) 点击**云交付的 FMC (Cloud-delivered FMC)** 单选按钮。
b) 选择区域并粘贴 CDO API 令牌。要从 CDO 生成 API 令牌，请执行以下步骤：

1. 登录到 CDO 门户。
2. 导航至**设置 (Settings)** > **常规设置 (General Settings)** 并复制 API 令牌。

c) 点击**连接 (Connect)** 并继续**步骤 2**。

步骤 2 在**防火墙管理中心登录 (Firewall Management Center Login)** 对话框中，输入 Cisco Secure Firewall 迁移工具专用帐户的用户名和密码，然后点击**登录 (Login)**。

Cisco Secure Firewall 迁移工具将登录到 管理中心，并检索由该 管理中心管理的一系列 威胁防御设备。您可以在控制台中查看此步骤的进度。

步骤 3 点击**继续 (Proceed)**。

步骤 4 在**选择威胁防御 (Choose Threat Defense)** 部分中，执行以下操作之一：

- 点击**选择防火墙威胁防御设备 (Select Firewall Threat Defense Device)**下拉列表，然后选中您要迁移 Check Point 配置的设备。

选择的 管理中心 域中的设备将按 **IP 地址**和**名称**列出。

注释 您选择的本地 威胁防御 设备必须至少拥有与您要迁移的 Check Point 配置相同数目的物理或端口通道接口。威胁防御 设备的容器实例必须至少具有相同数量的物理或端口通道接口和子接口。您必须为设备配置与 Check Point 配置相同的防火墙模式。但是，两个设备上的这些接口不需要具有相同的名称。

注释 仅当支持的目标威胁防御平台是具有管理中心版本 6.5 或更高版本的 Firewall 1010 时，FDM 5505 迁移支持才适用于共享策略，而不适用于设备特定策略。当您忽略威胁防御并继续时，Cisco Secure Firewall 迁移工具不会将任何配置或策略推送到威胁防御。因此，作为威胁防御设备特定配置的接口和路由以及站点间 VPN 不会迁移。但是，所有其他受支持的配置（共享策略和对象）将迁移，例如 NAT、ACL 和端口对象。远程访问 VPN 是一种共享策略，即使没有威胁防御也可以迁移。

Cisco Secure Firewall 迁移工具支持在启用远程部署的情况下将 Check Point 防火墙迁移到 管理中心 或 威胁防御 6.7 或更高版本。接口和路由的迁移必须手动完成。

- 点击**忽略 FTD 并继续**，将配置迁移到 管理中心。

  当您忽略 威胁防御 并继续时，Cisco Secure Firewall 迁移工具不会将任何配置或策略推送到 威胁防御。因此，作为 威胁防御 设备特定配置的接口和路由以及站点间 VPN 不会迁移，需要手动在 管理中心上配置。但是，所有其他受支持的配置（共享策略和对象）将迁移，例如 NAT、ACL 和端口对象。远程访问 VPN 是一种共享策略，即使没有威胁防御也可以迁移。

步骤 5 点击**继续 (Proceed)**。

根据迁移的目标，Cisco Secure Firewall 迁移工具允许您选择要迁移的功能。

步骤 6 点击**选择功能 (Select Features)** 部分以查看并选择要迁移到目标的功能。

- 如果要迁移到目标 威胁防御 设备，Cisco Secure Firewall 迁移工具会自动从**设备配置 (Device Configuration)** 和**共享配置 (Shared Configuration)** 部分的 Check Point 配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。
- 如果要迁移到目标 管理中心设备，Cisco Secure Firewall 迁移工具会自动从 **设备配置**、 **共享配置**和 **优化** 部分的 Check Point 配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。
- 对于 Check Point，在**共享配置**下选择相关的**访问控制**选项：
  - 全局策略 - 如果选择此选项，则 ACL 策略的源和目标区域会迁移为 **Any**。
  - 基于区域的策略 - 如果选择此选项，则会通过源和目标网络对象或组的路由机制根据谓词路由查找来得出源和目标区域。

    注释 路由查找仅限于静态路由和动态路由（不考虑 PBR 和 NAT），并且根据源和目标网络对象组的性质，此操作可能会导致规则爆炸。

    路由信息从 `networking.txt` 文件中获取。此文件是 FMT-CP-Config-Extractor_v4.0.1-8248 工具的输出，该工具使用 **netstat -rnv** 命令收集路由表。有关详细信息，请参阅使用配置提取器导出设备配置。

    此版本不支持对基于区域的策略执行 IPv6 路由查找。确保全局策略或基于区域的策略的所有规则成功迁移。

  在 **设备配置**下，选择要从 Check Point 防火墙迁移的接口、路由和站点间 VPN 隧道配置。请注意，只能迁移基于策略（加密映射）的站点间 VPN 隧道配置。
- （可选）在**优化**部分中，选择**仅迁移引用的对象**，以仅迁移访问控制策略和 NAT 策略中引用的对象。

注释　　当您选择此选项时，不会迁移 Check Point 配置中未引用的对象。这可以优化迁移时间并从配置中清除未使用的对象。

步骤 7　点击**继续 (Proceed)**。

步骤 8　在**规则转换/流程配置 (Rule Conversion/ Process Config)**部分中，点击**开始转换 (Start Conversion)** 以启动转换。

步骤 9　查看 Cisco Secure Firewall 迁移工具转换的元素的摘要。

要检查配置文件是否已成功上传和解析，请在继续迁移之前下载并验证**迁移前报告**。

步骤 10　点击**下载报告 (Download Report)**，并保存**迁移前报告 (Pre-Migration Report)**。

系统也会在 `Resources` 文件夹中保存**迁移前报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

下一步做什么

查看迁移前报告，第 24 页

查看迁移前报告

步骤 1　导航到下载**迁移前报告**的位置。

系统也会在 `Resources` 文件夹中保存**迁移前报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

步骤 2　打开**迁移前报告**并仔细检查其内容，以确定可能会导致迁移失败的任何问题。

迁移前报告包括以下信息：

- **迁移摘要** - 可成功迁移到 Firepower Threat Defense 的受支持 Check Point 配置元素的总体摘要。例如，策略名称、规则计数等。
- **解析错误详细信息** - 突出显示导致解析失败的配置。这样做有助于编辑和更新配置以进行重试。
- **不支持的配置** - 以更详细的方式列出 FMT 不支持迁移的所有配置项目。例如，环回接口、别名接口、域对象。
- **部分支持的配置** - 仅可部分迁移的所有 Check Point 配置元素的列表。例如，使用 Ping 参数的静态路由。
- **跳过的配置** - 迁移期间被 FMT 忽略且不会转发到目标系统的所有 Check Point 配置元素的列表。

有关 管理中心 和 威胁防御 中受支持功能的更多信息，请参阅《Firepower 管理中心配置指南》。

步骤 3　如果**迁移前报告**建议执行纠正操作，请在 Check Point 上完成这些纠正操作，重新导出 Check Point 配置文件，将更新的配置文件上传，然后再继续。

步骤 4 在您的 Check Point 配置文件成功上传和解析之后，返回到 Cisco Secure Firewall 迁移工具，然后点击**下一步 (Next)**以继续迁移。

将 Check Point 防火墙 配置与 威胁防御 接口映射

威胁防御 设备必须具有与 Check Point配置相同或更多的物理接口和端口通道接口。两个设备上的这些接口不需要具有相同的名称。您可以选择所需的接口映射方式。

在 **映射 FTD 接口** 屏幕上，Cisco Secure Firewall 迁移工具将检索 威胁防御 设备上的接口的列表。默认情况下，Cisco Secure Firewall 迁移工具会根据其接口标识符映射 Check Point和 威胁防御 设备中的接口。例如， Check Point 接口上的“管理专用”接口会自动映射到 威胁防御 设备上的“管理专用”接口，并且不可更改。

Check Point 接口到 威胁防御 接口的映射因 威胁防御 设备类型而异：

- 如果目标 威胁防御 为本地类型：
  - 威胁防御 必须具有相同或更多数量的已使用 Check Point 接口或端口通道 (PC) 数据接口（Check Point 配置中不包括管理专用接口和子接口）。如果其接口数量较少，请在目标 威胁防御 上添加所需类型的接口。
  - 子接口由 Cisco Secure Firewall 迁移工具根据物理接口或端口通道映射创建。
- 如果目标 威胁防御 为容器类型：
  - 威胁防御 必须具有相同或更多数量的已使用 Check Point 接口、物理子接口、端口通道或端口通道子接口（ Check Point 配置中不包括管理专用接口）。如果其接口数量较少，请在目标 威胁防御 上添加所需类型的接口。例如，如果目标 威胁防御 上的物理接口和物理子接口的数量比 Check Point 的接口数量少 100 个，则可以在目标 威胁防御 上创建更多物理接口或物理子接口。
  - 子接口不是由 Cisco Secure Firewall 迁移工具创建的。物理接口、端口通道或子接口之间仅允许接口映射。

开始之前

确保您已连接到管理中心 并将目标选择为 威胁防御。有关详细信息，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数 ， 第 21 页。

注释 如果要迁移到无 威胁防御 设备的 管理中心，则此步骤不适用。

步骤 1 如果您想要更改接口映射，请点击 **FTD 接口名称** 下拉列表，并选择您想要映射到该 Check Point 接口的接口。

不能更改管理接口的映射。如果 威胁防御 接口已分配到 Check Point 接口，则您不能从下拉列表中选择该接口。所有已分配的接口将变为灰色且不可用。

您不需要映射子接口。Cisco Secure Firewall 迁移工具会在 威胁防御 设备上为 Check Point 配置中的所有子接口映射子接口。

步骤 2 当您将每个 Check Point 接口映射到 威胁防御 接口时，请点击**下一步 (Next)**。

下一步做什么

将 Check Point 接口映射到相应的 威胁防御 接口对象、安全区和接口组。有关详细信息，请参阅将 Check Point 接口映射到安全区 和 接口组。

将 Check Point 接口映射到安全区 和 接口组

为确保正确地迁移 Check Point 配置，请将 Check Point 接口映射到相应的 威胁防御 接口对象、安全区 和接口组。在 Check Point 配置中，访问控制策略和 NAT 策略使用接口名称 (nameif)。在 管理中心中，这些策略使用接口对象。此外，管理中心策略将按以下项分组接口对象：

- 安全区 - 接口只能属于一个安全区。
- 接口组 - 接口可属于多个接口组。

Cisco Secure Firewall 迁移工具支持接口与安全区 和 接口组的一对一映射；当安全区或接口组映射到某个接口时，尽管 管理中心 允许，也不可映射到其他接口。有关 管理中心中安全区域和接口组的详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南中的 安全区域和接口组 。

步骤 1 在**映射安全区和接口组**屏幕上，查看可用接口、安全区和接口组。

步骤 2 要将接口映射到 管理中心 中的安全区和接口组，或映射到在配置文件中作为安全区类型对象并出现在下拉列表中的安全区和接口组，请执行以下操作：

a) 在 **安全区** 栏中，选择该接口的安全区。
b) 在 **接口组** 栏中，选择该接口的接口组。

步骤 3 要将接口映射到 管理中心 中的安全区和接口组，或映射到在 Check Point (r80) 配置文件中作为安全区类型对象并出现在下拉列表中的安全区和接口组，请执行以下操作：

a) 在**安全区**栏中，选择该接口的安全区。
b) 在**接口组**栏中，选择该接口的接口组。

步骤 4 您可以手动映射或自动创建安全区和接口组。

步骤 5 要手动映射安全区和接口组，请执行以下操作：

a) 点击**添加 SZ 和 IG (Add SZ & IG)**。
b) 在**添加 SZ 和 IG (Add SZ & IG)** 对话框中，点击**添加 (Add)** 以添加新的安全区或接口组。
c) 在**安全区**栏中输入安全区名称。允许的最大字符数为 48。同样，您可以添加接口组。
d) 点击**关闭 (Close)**。

要通过自动创建映射安全区和接口组，请执行以下操作：

a) 点击**自动创建 (Auto-Create)**。

b) 在**自动创建**对话框中，选中**接口组**和**区域映射**中的一个或两个。

c) 点击**自动创建 (Auto-Create)**。

Cisco Secure Firewall 迁移工具将为这些安全区提供与 Check Point 接口相同的名称（例如 **outside** 或 **inside**），并在名称后显示“(A)”，以指示它是由 Cisco Secure Firewall 迁移工具创建的。将为接口组添加 `_ig` 后缀，例如 **outside_ig** 或 **inside_ig**。此外，安全区和接口组与 Check Point 接口具有相同的模式。例如，如果 Check Point 逻辑接口是 L3 模式，则为该接口创建的安全区和接口组也是 L3 模式。

步骤 6 在已将所有接口映射到相应的安全区和接口组后，点击**下一步 (Next)**。

优化， 检查和验证配置

在将迁移的 Check Point 配置推送到 管理中心 之前，优化并仔细检查配置并验证它是否正确且与您需要的 威胁防御 设备配置方式匹配。闪烁的选项卡表示您必须执行下一步操作。

注释 如果您在**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 屏幕上关闭了 Cisco Secure Firewall 迁移工具，它会保存进度并允许您在以后恢复迁移。如果在进入此屏幕之前关闭 Cisco Secure Firewall 迁移工具，则不会保存您的进度。如果解析后出现故障，Cisco Secure Firewall 迁移工具继续从**接口映射 (Interface Mapping)** 屏幕重新启动。

此处，Cisco Secure Firewall 迁移工具会获取 管理中心 上已存在的入侵防御系统 (IPS) 策略和文件策略，并允许您将这些策略与要迁移的访问控制规则相关联。

文件策略是作为整体访问控制配置的一部分供系统用于执行网络高级恶意软件防护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。

同样，在允许流量继续到达其目标之前，可以使用 IPS 策略作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

要搜索选项卡中的特定配置项，请在列顶部的字段中输入项目名称。表中的行将筛选，仅显示与搜索术语匹配的项目。

注释 默认情况下，内联分组选项处于启用状态。

如果您在**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 屏幕上关闭了 Cisco Secure Firewall 迁移工具，它会保存进度并允许您在以后恢复迁移。如果在进入此屏幕之前关闭，则不会保存您的进度。如果解析后出现故障，Cisco Secure Firewall 迁移工具继续从**接口映射 (Interface Mapping)** 屏幕重新启动。

Cisco Secure Firewall 迁移工具 ACL 优化概述

Cisco Secure Firewall 迁移工具支持从防火墙规则库中识别和隔离可优化（禁用或删除）的 ACL，而不会影响网络功能。

ACL 优化支持以下 ACL 类型：

- 冗余 ACL - 当两个 ACL 具有相同的配置和规则集时，删除非基本 ACL 并不会影响网络。例如，如果任意两个规则允许同一个网络上的 FTP 和 IP 流量，而没有为拒绝访问定义规则，则可以删除第一个规则。
- 影子 ACL - 第一个 ACL 完全镜像第二个 ACL 的配置。如果两个规则具有相似的流量，则第二个规则不会应用于任何流量，因为它稍后会出现在访问列表中。如果两个规则对流量指定了不同的操作，则您可能需要移动阴影规则或编辑两条规则之一，以便实施所需的策略。例如，对于给定的源或目标，基本规则可能会拒绝 IP 流量，而阴影规则可能会允许 FTP 流量。

在比较 ACL 优化规则时，Cisco Secure Firewall 迁移工具会使用以下参数：

注释 优化仅适用于 ACP 规则操作的 Check Point 。

- 在优化过程中不会考虑已禁用的 ACL。
- 源 ACL 将扩展为相应的 ACE（内联值），然后对比以下参数：
  - 源和目标区域
  - 源和目标网络
  - 源和目标端口

点击 **下载报告** 以查看 ACL 名称以及 Excel 文件中列出的相应冗余和阴影 ACL。使用 **详细 ACL 信息** 表查看更多 ACL 信息。

对象优化

在迁移过程中会考虑以下对象以进行对象优化：

- 未引用的对象 - 可以选择在迁移开始时不迁移未被引用的对象。
- 重复对象 - 如果对象已存在于 管理中心 上，则不会创建重复对象，而是重复使用策略。
- 不一致的对象 - 如果存在名称相似但内容不同的对象，则在迁移推送之前 Cisco Secure Firewall 迁移工具会修改对象名称。

步骤 1 （可选）在**优化、查看和验证配置 (Optimize, Review and Validate Configuration)** 屏幕上，点击**优化 ACL (Optimize ACL)** 以运行优化代码，并执行以下操作：

a) 要下载已识别的 ACL 优化规则，请点击**下载 (Download)**。
b) 选择规则，然后选择**操作 (Actions)** > **作为已禁用迁移 (Migrate as disabled)** 或**不迁移 (Do not migrate)** 并应用其中一项操作。
c) 点击**保存 (Save)**。

迁移操作从**不迁移 (Do not migrate)** 更改为**已禁用 (Disabled)**，反之亦然。

您可以使用以下选项来批量选择规则

- 迁移 - 以默认状态迁移。
- 不迁移 - 忽略 ACL 的迁移。
- 作为已禁用迁移 (Migrate as disabled) - 迁移**状态** ***(State)*** 字段被设为**禁用** ***(Disable)*** 的 ACL。
- 迁移为已启用 (Migrate as enabled) - 迁移**状态** ***(State)*** 字段被设为**启用** ***(Enable)*** 的 ACL。

步骤 2 在**优化、检查和验证配置**屏幕上，点击**访问控制规则**，并执行以下操作：

a) 对于此表中的每个条目，查看映射并验证它们是否正确。

迁移的访问策略规则使用 ACL 名称作为前缀，并在后面附加 ACL 规则编号，以便更轻松地映射回到 Check Point 配置文件。例如，如果 Check Point ACL 被命名为“inside_access”，则 ACL 中的第一个规则（或 ACE）行将命名为“inside_access_#1”。如果因为 TCP 或 UDP 组合、扩展的服务对象或一些其他原因而必须扩展规则，则 Cisco Secure Firewall 迁移工具会在名称中添加编号的后缀。例如，如果 allow 规则扩展为两个迁移规则，它们命名为“inside_access _#1-1”和“inside_access_#1-2”。

对于包括不受支持对象的任何规则，Cisco Secure Firewall 迁移工具将“_UNSUPPORTED”后缀附加到名称中。

b) 如果您不想迁移一个或多个访问控制列表策略，根据策略选中复选框来选择行，选择 **操作** > **不迁移** ，然后点击 **保存**。

您选择为不进行迁移的所有规则都会在表中变灰。

c) 如果要将 管理中心 文件策略应用于一个或多个访问控制策略，请选中相应行的复选框，然后选择**操作** > **文件策略**。

在**文件策略 (File Policy)** 对话框中，选择适当的文件策略并将其应用于所选的访问控制策略，然后点击**保存 (Save)**。

d) 如果要将 管理中心 IPS 策略应用于一个或多个访问控制策略，请选中相应行的复选框，然后选择**操作** > **IPS 策略**。

在 **IPS 策略 (IPS Policy)** 对话框中，选择适当的 IPS 策略和对应的变量集并将其应用于所选的访问控制策略，然后点击**保存 (Save)**。

e) 如果要更改已启用日志记录的访问控制规则的日志记录选项，请选中相应行的复选框，然后选择**操作** > **日志**。

在**日志**对话框中，您可以在连接开始和/或结尾时启用日志记录事件。如果启用日志记录，则必须选择将连接事件发送到**事件查看器**和/或**系统日志**。当您选择将连接事件发送到系统日志服务器时，可以从**系统日志**下拉菜单中选择已在 管理中心 上配置的系统日志策略。

f) 如果要更改访问控制表中已迁移的访问控制规则的操作，请选中相应行的复选框，然后选择**操作** > **规则操作**。

提示 对于 **允许** 选项除外的所有规则操作，附加到访问控制规则的 IPS 和文件策略将自动删除。

您可以按升序、降序、等于、大于和小于过滤顺序来过滤 ACE 计数。

要清除现有过滤条件并加载新搜索，请点击**清除过滤器 (Clear Filter)**。

注释 基于 ACE 对 ACL 进行排序的顺序仅供查看。ACL 将基于发生的时间顺序推送。

步骤 3 点击以下选项卡并查看配置项：

- 访问控制
- 对象（网络对象、端口对象、VPN 对象）
- NAT
- 接口
- 路由
- 站点间 VPN 隧道

如果您不想迁移一个或多个NAT规则或路由接口，请选中相应行的复选框，选择 操作>不迁移，然后点击 保存。

您选择为不进行迁移的所有规则都会在表中变灰。

步骤 4 您可以从 路由 区域查看路由，并通过选择一个条目并选择 操作 > 不迁移来选择您不想迁移的路由。

步骤 5 在 站点间 VPN 隧道 部分，列出了源防火墙配置中的 VPN 隧道。查看 VPN 隧道数据，例如每行的 源接口、 VPN 类型以及 IKEv1 和 IKEv2 配置，并确保为所有行提供预共享密钥值。

步骤 6 （可选）要下载网格中每个配置项目的详细信息，请点击下载 (Download)。

步骤 7 完成检查后，点击验证 (Validate)。请注意，需要注意的必填字段会一直闪烁，直到您在其中输入值。只有在填写所有必填字段后， 验证 按钮才会启用。

在验证期间，Cisco Secure Firewall 迁移工具会连接到 管理中心，检查现有对象，然后将这些对象与要迁移的对象列表进行比较。如果 管理中心 中已存在对象，Cisco Secure Firewall 迁移工具会执行以下操作：

- 如果对象具有相同的名称和配置，Cisco Secure Firewall 迁移工具会重新使用现有对象，而不会在 管理中心 中创建新对象。
- 如果对象具有相同名称但具有不同的配置，Cisco Secure Firewall 迁移工具会报告对象冲突。

您可以在控制台中查看验证进度。

步骤 8 验证完成后，如果验证状态对话框显示一个或多个对象冲突，请执行以下操作：

a) 点击解决冲突 (Resolve Conflicts)。

根据报告的对象冲突位置，Cisco Secure Firewall 迁移工具会在网络对象 (Network Objects) 和/或端口对象 (Port Objects) 选项卡中显示一个警告图标。

b) 点击选项卡，检查对象。

c) 检查存在冲突的每个对象的条目，然后选择操作 (Actions) > 解决冲突 (Resolve Conflicts)。

d) 在解决冲突窗口中，完成建议的操作。

例如，系统可能会提示您为对象名称添加后缀，以避免与现有 管理中心对象冲突。您可以接受默认后缀或将其替换为您自己的后缀。

e) 点击解决 (Resolve)。

f) 在选项卡上解决所有对象冲突之后，点击保存 (Save)。

g) 点击验证 (Validate)，重新验证配置，并确认您已解决所有对象冲突。

步骤 9 在验证完成且**验证状态**对话框显示消息**已成功验证**时，继续执行将迁移的配置推送到 管理中心，第 31 页。

将迁移的配置推送到 管理中心

如果您还未成功验证配置和解决所有对象冲突，则不能将迁移的 Check Point配置推送到 管理中心。

迁移过程中的此步骤会将迁移的配置发送至管理中心。此步骤不会将配置部署到威胁防御设备。但在此步骤中会擦除 威胁防御上的任何现有配置。

注释 当 Cisco Secure Firewall 迁移工具将迁移的配置发送到 管理中心时，不要更改任何配置或部署到任何设备。

步骤 1 在**验证状态**对话框中，查看验证摘要。

步骤 2 点击**推送配置 (Push Configuration)**，将迁移的 Check Point 配置发送至 管理中心。

Cisco Secure Firewall 迁移工具会显示迁移进度的摘要信息。您可以在控制台中查看详细的逐行进度信息，了解正在将哪些组件推送至 管理中心。

步骤 3 在迁移完成后，点击**下载报告 (Download Report)**，下载并保存迁移后报告。

系统也会在 `Resources` 文件夹中保存**迁移后报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

步骤 4 如果迁移失败，请仔细查看迁移后报告、日志文件和未解析文件，了解是什么原因导致失败。

您也可以联系支持团队进行故障排除。

迁移失败支持

如果迁移不成功，请联系支持部门。

1. 在**完成迁移 (Complete Migration)** 屏幕上，点击**支持 (Support)** 按钮。

   系统将显示“帮助”支持页面。

2. 选中**支持捆绑包**复选框，然后选择要下载的配置文件。

   注释 默认情况下，系统已选择要下载的日志和 dB 文件。

3. 点击**下载 (Download)**。

   支持捆绑包文件以 .zip 格式下载到您的本地路径。解压缩 Zip 文件夹以查看日志文件、DB 和配置文件。

4. 点击**给我们发送邮件 (Email us)**，通过电子邮件将故障详细信息发送给技术团队。

   您还可以将下载的支持文件附加到电子邮件中。

5. 点击**访问 TAC 页面 (Visit TAC page)**，在思科支持页面上创建 TAC 支持请求。

注释　　您可以在迁移过程中随时从支持页面提交 TAC 支持请求。

查看 Check Point 的迁移后报告并完成迁移

步骤 1 导航至您已将迁移后报告下载到的位置。

步骤 2 打开迁移后报告并仔细检查其内容，了解您的 ASA 配置是如何迁移的：

- **迁移摘要** - 已成功从 Check Point 迁移到 Firepower Threat Defense 的配置摘要。
- **选择性策略迁移** - 提供所选用于迁移和接口映射的特定 Check Point 功能的详细信息。
- **迁移转换** - 转换和推送详细信息，包括以下内容：
  - 网络/服务对象处理
  - 部分迁移的配置列表及其原因
  - 不支持的配置列表及原因
  - 扩展访问控制规则

卸载 Cisco Secure Firewall 迁移工具

所有组件均存储在与 Cisco Secure Firewall 迁移工具相同的文件夹中。

步骤 1 导航至在其中放置 Cisco Secure Firewall 迁移工具的文件夹。

步骤 2 如果要保存日志，请剪切或复制 `log` 文件夹并粘贴到另一个位置。

步骤 3 如果要保存迁移前报告和迁移后报告，请剪切或复制 `resources` 文件夹并粘贴到另一个位置。

步骤 4 删除在其中放置 Cisco Secure Firewall 迁移工具的文件夹。

提示　　日志文件与控制台窗口相关联。如果 Cisco Secure Firewall 迁移工具的控制台窗口处于打开状态，就无法删除日志文件和文件夹。

迁移示例： Check Point 到 Threat Defense 2100

注释 创建迁移完成后可在目标设备上运行的测试计划。

- 维护前窗口任务
- 维护窗口任务

维护前窗口任务

开始之前

确保已安装并部署了 管理中心。有关详细信息，请参阅相应的管理中心硬件安装指南和相应的管理中心入门指南。

步骤 1 使用 Check Point Web 可视化工具和 FMT-CP-Config-Extractor_v4.0.1-8248 工具收集您尝试迁移的 Check Point 设备配置，并保存一份 Check Point 配置文件。

步骤 2 查看 Check Point 配置 zip 文件。

步骤 3 在网络中部署 Firepower 2100 系列 设备，连接接口并打开设备电源。

有关详细信息，请参阅《适用于使用管理中心的 2100 系列的思科威胁防御快速入门指南》。

步骤 4 注册 Firepower 2100 系列 设备以接受 管理中心 的管理。

有关详细信息，请参阅将设备添加到管理中心。

步骤 5 （可选）如果源 Check Point 配置具有绑定接口，请在目标 Firepower 2100 系列 设备上创建端口通道 (EtherChannel)。

有关详细信息，请参阅配置 EtherChannel 和冗余接口。

步骤 6 从 https://software.cisco.com/download/home/286306503/type 下载并运行最新版本的 Cisco Secure Firewall 迁移工具。

有关详细信息，请参阅从 Cisco.com 下载 Cisco Secure Firewall 迁移工具 ， 第 3 页。

步骤 7 启动 Cisco Secure Firewall 迁移工具并指定目标参数时，请确保选择注册到 管理中心 的 Firepower 2100 系列 设备。

有关详细信息，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数 ， 第 21 页。

步骤 8 将 Check Point 接口与 威胁防御 接口映射。

注释 Cisco Secure Firewall 迁移工具允许您将 Check Point 接口类型映射到 威胁防御 接口类型。

例如，您可以将 Check Point 中的绑定接口映射到 威胁防御 中的物理接口。

有关详细信息，请参阅将 Check Point 防火墙 配置与 威胁防御 接口映射。

步骤 9 将逻辑接口映射到安全区时，点击**自动创建 (Auto-Create)** 以允许 Cisco Secure Firewall 迁移工具创建新的安全区。要使用现有安全区，请手动将 Check Point 逻辑接口映射到安全区。

有关详细信息，请参阅将 Check Point 接口映射到安全区 和 接口组。

步骤 10 按照本指南的说明依次检查和验证要迁移的配置，然后将配置推送到 管理中心。

步骤 11 查看迁移后报告，手动设置其他配置并部署到 威胁防御，完成迁移。

有关详细信息，请参阅查看 Check Point 的迁移后报告并完成迁移 ， 第 32 页。

步骤 12 使用您在计划迁移时创建的测试计划测试 Firepower 2100 系列 设备。

维护窗口任务

开始之前

确保您已完成所有必须在维护窗口之前执行的任务。请参阅维护前窗口任务 ， 第 33 页。

步骤 1 通过 Gaia Console 连接到 Check Point 安全网关。

步骤 2 通过 Gaia Console 关闭意向安全网关的 Check Point 接口。

步骤 3 （可选）访问 管理中心并配置动态路由、平台设置，以及 Cisco Secure Firewall 迁移工具未迁移、需要为 Firepower 2100 系列设备手动迁移的其他功能。

步骤 4 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

步骤 5 执行从周围交换基础设施到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试，确保它们可访问。

步骤 6 执行从需要第 3 层路由的设备到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试。

步骤 7 如果要为 Firepower 2100 系列 设备分配新的 IP 地址，而不是重新使用分配给 Check Point的 IP 地址，请执行以下步骤：

1. 更新指向该 IP 地址的任何静态路由，以使其现在指向 Firepower 2100 系列 设备 IP 地址。
2. 如果使用路由协议，请确保邻居将 Firepower 2100 系列 设备 IP 地址视为预期的下一跳目标。

步骤 8 运行全面的测试计划并监控管理 Firepower 2100 设备的 管理中心。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。