运行迁移

- 从 Cisco.com 下载防火墙迁移工具， 第 1 页
- 启动防火墙迁移工具， 第 2 页
- 导出 Check Point 配置文件， 第 4 页
- 上传 Check Point 配置文件， 第 17 页
- 指定防火墙迁移工具的目标参数， 第 17 页
- 查看迁移前报告， 第 20 页
- 通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置， 第 21 页
- 将 Check Point 接口映射到安全区和接口组， 第 22 页
- 优化，检查和验证要迁移的配置， 第 23 页
- 将迁移的配置推送到 Cisco Secure Firewall Management Center， 第 26 页
- 查看迁移后报告并完成迁移， 第 27 页
- 卸载防火墙迁移工具， 第 29 页

从 Cisco.com 下载防火墙迁移工具

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，为防火墙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。当防火墙迁移工具启动时，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防火墙迁移工具时，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 下面的防火墙迁移工具。您还可以从 威胁防御 设备下载区域中下载防火墙迁移工具。

步骤 3 将防火墙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 计算机的防火墙迁移工具的相应可执行文件。

下一步做什么

导出 Check Point r77 配置文件

启动防火墙迁移工具

注释 当您启动防火墙迁移工具时，会在单独的窗口中打开控制台。进行迁移时，控制台会显示防火墙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防火墙迁移工具后。

开始之前

- 从 Cisco.com 下载防火墙迁移工具
- 查看并验证适用于防火墙迁移工具的准则和限制部分中的要求。
- 确保您的计算机带有最新版本的 Google Chrome 浏览器以运行防火墙迁移工具。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防火墙迁移工具的文件夹。

步骤 2 执行以下操作之一：

- 在您的 Windows 计算机上，双击防火墙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)**，以允许防火墙迁移工具对您的系统作出更改。

  防火墙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，将防火墙迁移工具 `*.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
  ```

  防火墙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 当您尝试打开防火墙迁移工具时，因为没有可识别的开发人员在 Apple 中注册防火墙迁移工具，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防火墙迁移工具。

步骤 4　在防火墙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。

  注释　　如果您没有 Cisco.com 帐户，请在 Cisco.com 登录页面上创建帐户。

- 使用以下默认凭证登录：
  - **用户名** - admin
  - **密码** - Admin123

如果您已使用 Cisco.com 帐户登录，请继续执行步骤 8。

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**。

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防火墙迁移工具。

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防火墙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。
- 如果必须使用防火墙迁移工具从 Check Point (r77) 提取信息，请继续执行导出 Check Point r77 配置文件。

- 如果必须使用防火墙迁移工具从 Check Point (r80) 提取信息，请继续执行导出 Check Point r80 配置文件。

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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置 ， 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。

命令	说明
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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置

使用 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置

步骤 1 从思科防火墙迁移工具软件下载页面下载 FMT-CP-Config-Extractor_v3.0.1-7373 .exe。

步骤 2 打开 FMT-CP-Config-Extractor_v3.0.1-7373 工具，该工具是工作站上有权访问 Check Point Security Gateway 的 Windows 可执行文件 (.exe)。

步骤 3 连接到要使用防火墙迁移工具迁移策略的 Check Point Security Gateway。

要连接它，您需要：

a) IP 地址
b) 端口
c) 用户名
d) 密码

步骤 4 将派生自 FMT-CP-Config-Extractor_v3.0.1-7373 工具的输出文件重命名为 `networking.txt` 文件。

FMT-CP-Config-Extractor_v3.0.1-7373 工具执行以下命令：

- **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**

所有命令均由 FMT-CP-Config-Extractor_v3.0.1-7373 工具在后台执行，输出存储为 a.txt 文件。

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

步骤 5 将 .txt 文件移动到 `Outputs` 文件夹。

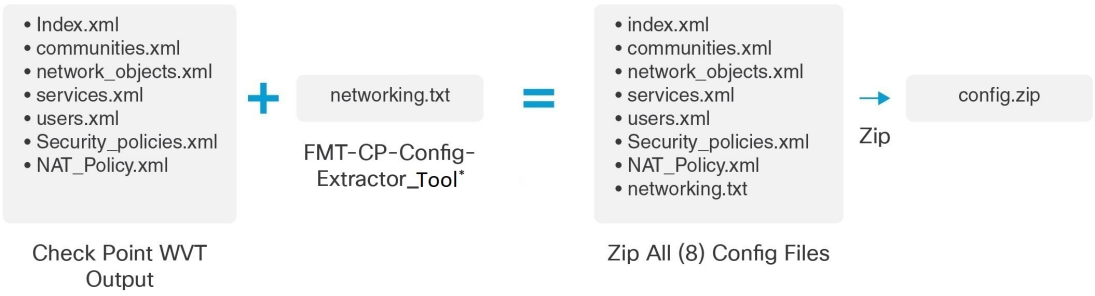
下一步做什么

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 FMT-CP-Config-Extractor_v3.0.1-7373 工具中的一个 .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 FTD 的 Check Point 设备。



*Check Point 提取器版本：FMT-CP-Config-Extractor_v3.0.1-7373

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

导出 Check Point r80 配置文件

注释 只有防火墙迁移工具上的 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

在防火墙迁移工具上使用 Live Connect 提取 Check Point 配置之前，必须在 Check Point (r80) 设备上配置凭证。

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

在防火墙迁移工具上使用 Live Connect 提取 Check Point 配置之前，必须在 Check Point (r80) 设备上配置凭证。

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

必须使用防火墙迁移工具上的 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：

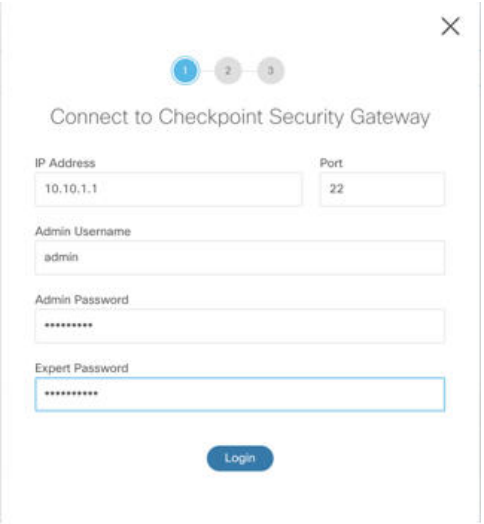
- 从 **Shell** 下拉列表中，选择 */etc/cli.sh*。

- 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。

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：

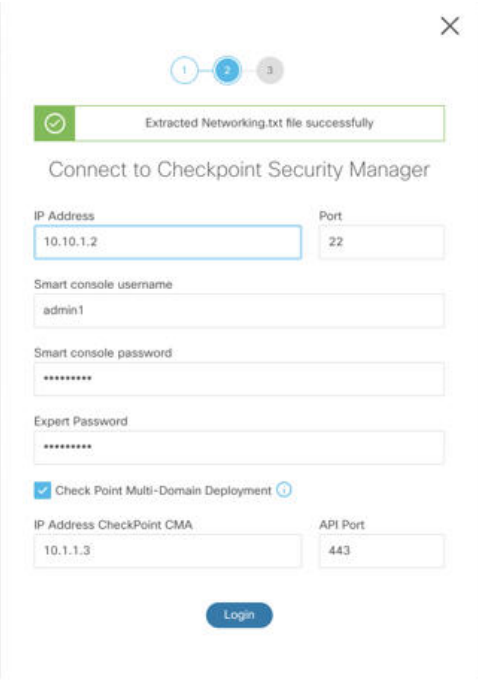
   set expert-password <password>

   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。
- 若使用未在防火墙迁移工具中通过 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)**。

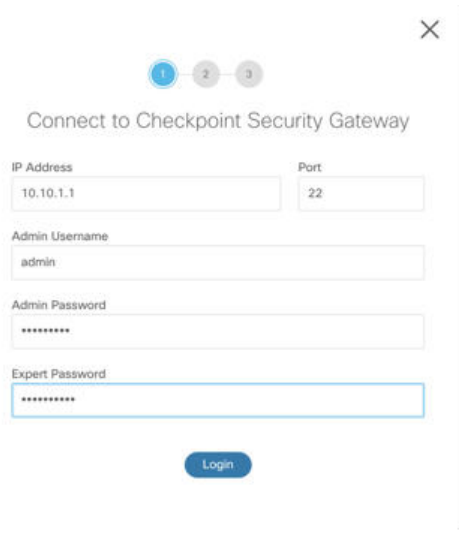
注释 Live Connect 仅适用于 Check Point (r80)。

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)**。

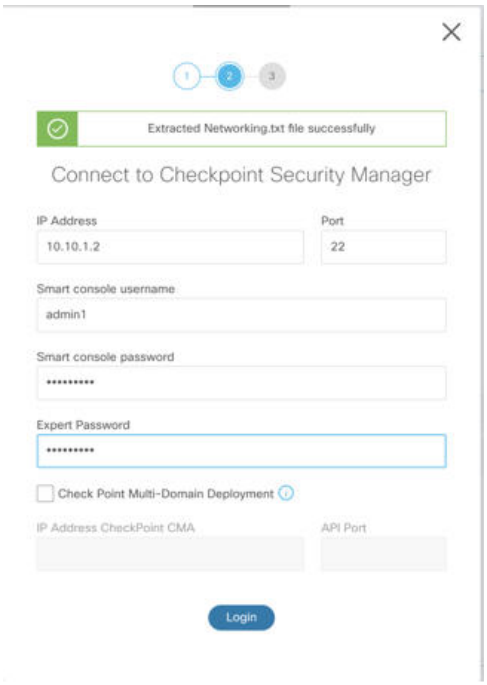
防火墙迁移工具会生成包含设备特定配置（例如接口和路由配置）的 *networking.txt* 文件。将 *networking.txt* 文件存储在防火墙迁移工具当前会话的本地目录中。

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)**。

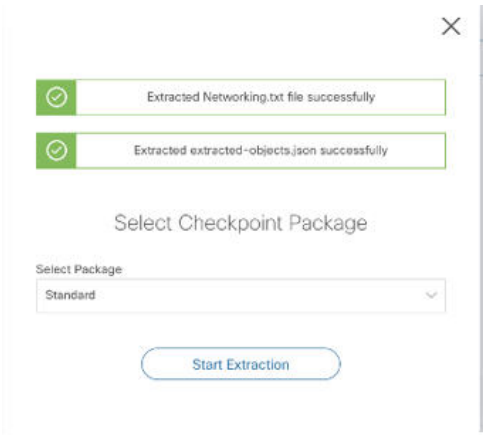
防火墙迁移工具会生成 *Extracted-objects.json* 文件，其中记录 Check Point 安全管理器中可用的完整网络和服务对象配置。

将 *Extracted-objects.json* 文件存储在防火墙迁移工具当前会话的本地目录中。

注释　如果您已将防火墙迁移工具连接到 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。

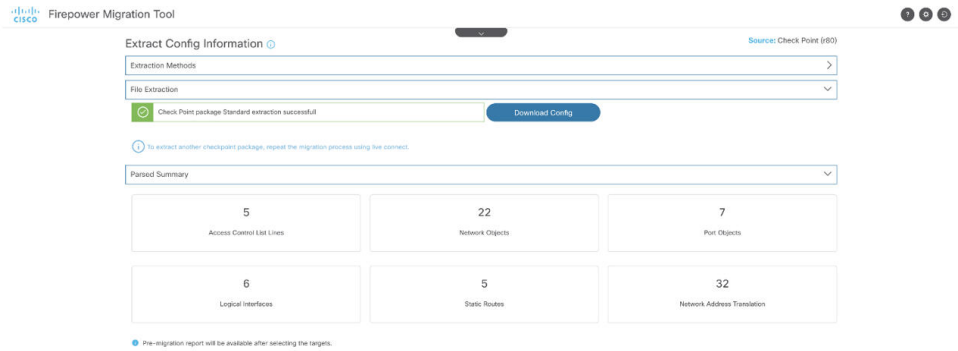
步骤 5 从**选择 Check Point 包 (Select Check Point Package)** 列表中选择要迁移的 Check Point 策略包，然后点击**开始提取 (Start Extraction)**。

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)**。

防火墙迁移工具上传配置文件。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 查看防火墙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

指定防火墙迁移工具的目标参数

指定防火墙迁移工具的目标参数

开始之前

- 获得现场防火墙管理中心的 管理中心 的 IP 地址。
- 从防火墙迁移工具 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，必须如云交付的防火墙管理中心迁移中所述提供区域和 API 令牌。

- （可选）如果要迁移设备特定的配置（例如接口和路由），请将目标 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**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，因为防火墙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。有关生成 CDO API 令牌的信息，请参阅云交付的防火墙管理中心迁移。
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，输入防火墙迁移工具专用帐户的用户名和密码，然后点击**登录 (Login)**。

防火墙迁移工具将登录到 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。

防火墙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**忽略威胁防御并继续 (Proceed without Threat Defense)**，将配置迁移到 管理中心。

当您忽略 威胁防御 并继续时，防火墙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。

步骤 5 点击**继续 (Proceed)**。

根据迁移的目标，防火墙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，防火墙迁移工具会自动从**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 管理中心，防火墙迁移工具会自动从**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。

  注释 当您未选择要迁移到的目标 威胁防御 设备时，**设备配置**部分不可用。

- 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_v3.0.1-7373 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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置。

    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。

- 如果目标管理中心是 7.2 或更高版本，防火墙迁移工具支持迁移远程访问 VPN。远程访问 VPN 是一种无需威胁防御即可迁移的共享策略。如果选择使用威胁防御进行迁移，则威胁防御版本应为 7.0 或更高版本。
- （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 查看防火墙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（与防火墙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 20 页

查看迁移前报告

注释 防火墙迁移工具 未解析的配置在**迁移前报告**中显示时，其 XML (r75-r77.30) 或 json (r80) 标签与源配置文件中完全相同。

如果您在迁移期间错过下载迁移前报告，请使用以下链接进行下载：

迁移前报告下载终端 — http://localhost:8888/api/downloads/pre_migration_summary_html_format

注释 您只能在 防火墙迁移工具 正在运行时下载报告。

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（与防火墙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：

- **总体摘要** - 用于提取 Check Point 配置信息或手动上传到 CP 的方法。

  可成功迁移到 威胁防御 的受支持 Check Point 配置元素以及为迁移选择的特定 Check Point 功能的摘要。

- **出错的配置行** - 因为防火墙迁移工具无法解析而不能成功迁移的 Check Point 配置元素的详细信息。在 Check Point 配置上更正这些错误，导出新配置文件，将新配置文件上传到 防火墙迁移工具，然后再继续。

- **部分支持的配置** - 仅可部分迁移的 Check Point 配置元素的详细信息。这些配置元素包括含高级选项的规则和对象，其中的规则或对象可在无高级选项的情况下迁移。查看这些行，验证 管理中心中是否支持高级选项。如果支持，则计划在使用 防火墙迁移工具 完成迁移后手动配置这些选项。

- **不支持的配置** - 因防火墙迁移工具不支持迁移这些功能而无法迁移的 Check Point 配置元素的详细信息。查看这些行，验证 管理中心 中是否支持每项功能。如果支持，则计划在使用防火墙迁移工具完成迁移后手动配置这些功能。

- **忽略的配置** - 因为不受 管理中心 或防火墙迁移工具支持而被忽略的 Check Point 配置的详细信息。防火墙迁移工具不会解析这些行。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划手动配置这些功能。

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 接口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，返回到防火墙迁移工具，然后点击**下一步 (Next)** 以继续迁移。

下一步做什么

通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置

通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置

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**映射威胁防御接口**屏幕上，防火墙迁移工具将检索 威胁防御 设备上的接口的列表。默认情况下，防火墙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。
  - 子接口由防火墙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。
  - 子接口不是由防火墙迁移工具创建的。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，请参阅指定防火墙迁移工具的目标参数 ， 第 17 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**威胁防御接口名称 (Threat Defense Interface Name)** 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。防火墙迁移工具会在 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，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。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。

防火墙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 管理中心中的安全区和接口组的更多信息，请参阅接口对象：接口组和安全区 。

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)**。

防火墙迁移工具迁移工具将为这些安全区提供与 ASA 具有 FPS 接口相同的名称（例如 **outside** 或 **inside**），并在名称后显示“(A)”，以指示它是由防火墙迁移工具创建的。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，检查和验证要迁移的配置

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。

此处，防火墙迁移工具会获取 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**屏幕上关闭了防火墙迁移工具防火墙迁移工具，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，防火墙迁移工具会继续从**接口映射**屏幕重新启动。

防火墙迁移工具 ACL 优化概述

防火墙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，防火墙迁移工具 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

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 防火墙迁移工具 会修改对象名称。

ACL 优化的报告

ACL 优化报告中显示以下信息：

- 摘要表 (Summary Sheet) - 显示 ACL 优化的摘要。

Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremote_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- 详细 ACL 信息 (Detailed ACL Information) - 显示基础 ACL 的详细信息。每个 ACL 都带有一个 ACL 类型（Shadow 或 Redundant）标记，用于标识基本 ACL 以便进行比较和与优化类别的关联。

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

将迁移的配置推送到 Cisco Secure Firewall Management Center

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 Cisco Secure Firewall Management Center。

迁移过程中的此步骤会将迁移的配置发送至 Cisco Secure Firewall Management Center。此步骤不会将配置部署到 Cisco Secure Firewall Threat Defense设备。但在此步骤中会擦除 Cisco Secure Firewall Threat Defense上的任何现有配置。

注释 当防火墙迁移工具将迁移的配置发送到 Cisco Secure Firewall Management Center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 Cisco Secure Firewall Management Center。

防火墙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 Cisco Secure Firewall Management Center。

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**迁移前报告**的一个副本（与防火墙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。

查看迁移后报告并完成迁移

迁移后报告提供了不同类别下的 ACL 计数、ACL 优化以及对配置文件进行优化的整体视图等详细信息。有关详细信息，请参阅优化，检查和验证要迁移的配置，第 23 页

查看并验证对象：

- **类别**
  - ACL 规则总数（源配置）
  - 考虑优化的 ACL 规则总数。例如，冗余、阴影等。
- 优化的 ACL 计数给出了优化前后计算得出的 ACL 规则总数。

如果您在迁移期间错过下载迁移后报告，请使用以下链接进行下载：

迁移后报告下载终端 — http://localhost:8888/api/downloads/post_migration_summary_html_format

注释　您只能在 防火墙迁移工具 正在运行时下载报告。

步骤 1　导航至下载了**迁移后报告**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 Check Point 配置是如何迁移的：

- **迁移摘要** - 已成功从 Check Point 迁移到 威胁防御 的配置的摘要信息，其中包括有关 Check Point 接口、管理中心 主机名和域、目标 威胁防御 设备（如果适用）和已成功迁移的配置元素的信息。
- **选择性策略迁移** - 设备配置功能、共享配置功能和优化三个类别中可选择迁移的特定 Check Point 功能的详细信息。
- **Check Point 接口至 FTD 接口映射** - 已成功迁移的接口的详细信息，以及如何将 Check Point 配置上的接口映射到 威胁防御 设备上的接口。确认这些映射符合您的预期。

  注释　本部分不适用于没有目标 威胁防御 设备或者**未**选择迁移**接口**的迁移。
- **源接口名称至 FTD 安全区和接口组** - 已成功迁移的 Check Point 逻辑接口和名称的详细信息，以及如何将它们映射到 威胁防御 中的安全区和接口组。确认这些映射符合您的预期。

  注释　如果**未**选择迁移**访问控制列表**和 **NAT**，则此部分不适用。
- **对象冲突处理** - 已被确定为与 管理中心 中现有对象冲突的 Check Point 对象的详细信息。如果对象具有相同的名称和配置，防火墙迁移工具重新使用 管理中心对象。如果对象具有相同名称但具有不同的配置，则重命名这些对象。仔细检查这些对象，并确认已正确解决冲突。

- **您选择不迁移的访问控制规则、NAT 和路由** - 您选择不让 防火墙迁移工具迁移的规则的详细信息。查看由 防火墙迁移工具禁用且未迁移的这些规则。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
- **部分迁移的配置** - 仅部分迁移的 Check Point 规则的详细信息，包括带有高级选项的规则，其中，在没有高级选项的情况下也可以迁移规则。查看这些行，验证在 管理中心中是否支持高级选项。如果支持，手动配置这些选项。
- **不支持的配置** - 因防火墙迁移工具不支持迁移这些功能而未被迁移的 Check Point 配置元素的详细信息。查看这些行，验证 威胁防御中是否支持每项功能。如果支持，请在 管理中心中手动配置这些功能。
- **展开访问控制策略规则** - 在迁移期间已从一个 Check Point Point 规则扩展到多个 威胁防御 规则的 Check Point 访问控制策略规则的详细信息。
- **对访问控制规则采取的操作**
  - **您选择不迁移的访问规则** - 您选择不让 防火墙迁移工具迁移的 Check Point 访问控制规则的详细信息。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **规则操作有更改的访问规则** - 使用 防火墙迁移工具更改了“规则操作”的所有访问控制策略规则的详细信息。规则操作值包括允许、信任、监控、阻止、阻止并重置。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **应用了 IPS 策略和变量集的访问控制规则** - 应用了 IPS 策略的所有 Check Point 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **应用了文件策略的访问控制规则** - 应用了文件策略的所有 Check Point 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **规则“日志”设置有更改的访问控制规则** - 使用 防火墙迁移工具更改了“日志设置”的 Check Point 访问控制规则的详细信息。日志设置值包括 False、事件查看器、系统日志。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。

注释 未迁移的不受支持的规则可能导致出现问题，使得不必要的流量通过您的防火墙。建议您在 管理中心中配置一个规则来确保 威胁防御阻止此类流量。

注释 如果它要求您在**检查和验证**页面中将 IPS 或文件策略应用于 ACL，则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 防火墙迁移工具 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策略可能会降低性能，也可能导致推送失败。

有关 管理中心和 威胁防御中的受支持功能的更多信息，请参阅管理中心配置指南，版本 6.2.3。

步骤 3 打开**迁移前报告**，并记下您必须在 威胁防御 设备上手动迁移的任何 Check Point 配置项目。

步骤 4 在 管理中心中，执行以下操作：

a) 查看 威胁防御设备的迁移配置，确认所有预期规则和其他配置项目（包括以下内容）均已迁移：

- 访问控制列表 (ACL)
- 网络地址转换规则
- 端口和网络对象

- 路由
- 接口
- 动态路由对象

b) 配置所有未迁移的部分受支持、不受支持、已忽略和已禁用的配置项目和规则。

有关如何配置这些项目和规则的信息，请参阅管理中心配置指南 。以下是需要手动配置的配置项目的示例：

- 平台设置，包括 SSH 和 HTTPS 访问，如威胁防御的平台设置中所述。
- 系统日志设置，如配置系统日志中所述
- 动态路由，如威胁防御路由概述中所述
- 服务策略，如 FlexConfig 策略中所述
- VPN 配置，如威胁防御 VPN 中所述
- 连接日志设置，如连接日志记录中所述

步骤 5 完成检查之后，将已迁移的配置从 管理中心 部署到 威胁防御 设备。

验证**迁移后报告**中是否正确反映了不支持和部分支持的规则的数据。

防火墙迁移工具将策略分配到 威胁防御设备。验证运行配置中是否反映了更改。为帮助您识别已迁移的策略，这些策略的描述信息中包括 Check Point 配置的主机名。

卸载防火墙迁移工具

所有组件均存储在与防火墙迁移工具相同的文件夹中。

步骤 1 导航至在其中放置防火墙迁移工具的文件夹。

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 删除在其中放置防火墙迁移工具的文件夹。

提示 日志文件与控制台窗口相关联。只要防火墙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。

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。