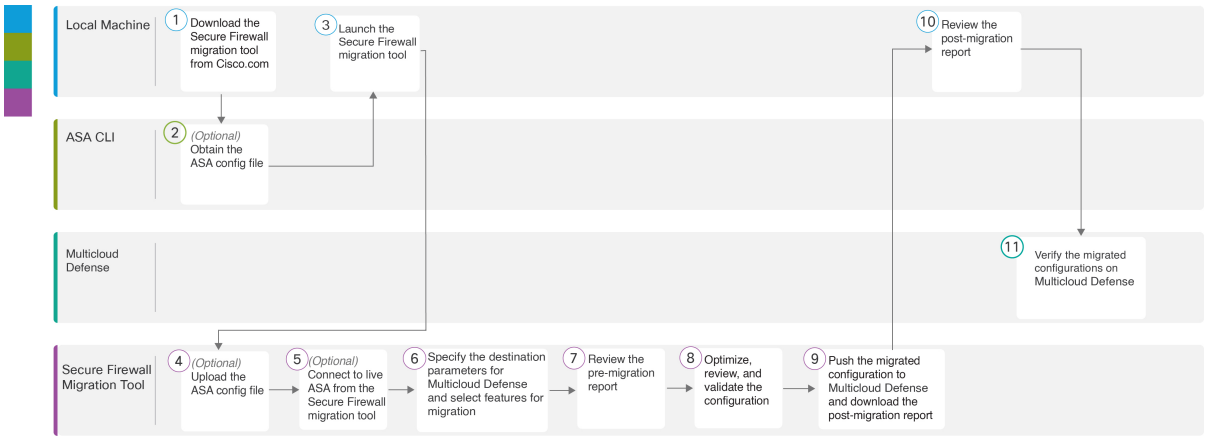
ASA 到多云防御迁移工作流程

端到端程序

以下流程图说明了使用 Cisco Secure Firewall 迁移工具迁移Cisco Secure Firewall ASA 到 多云防御的工作流程。



	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。
2	Cisco Secure Firewall ASA CLI	获取ASA配置文件：要从ASA CLI 获取ASA配置文件，请参阅获取 ASA 配置文件。 如果您想从迁移工具连接到ASA，请跳至步骤 3。

	工作空间	步骤
3	本地计算机	在本地计算机中，双击从Cisco.com下载的应用程序文件来启动安全防火墙迁移工具。
4	Cisco Secure Firewall 迁移工具	上传从 ASA CLI 获取的 ASA 配置文件，请参阅上传 ASA 配置文件，第 6 页。如果您计划连接到实时 ASA，请跳至步骤 6。
5	Cisco Secure Firewall 迁移工具	您可以从 Cisco Secure Firewall 迁移工具直接连接到实时 ASA。有关详细信息，请参阅从 Cisco Secure Firewall 迁移工具连接到 ASA，第 7 页。
6	Cisco Secure Firewall 迁移工具	指定多云防御的目标参数有关详细步骤，请参阅为多云防御指定目标参数，第 9 页。
7	Cisco Secure Firewall 迁移工具	导航到下载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，第 10 页。
8	Cisco Secure Firewall 迁移工具	优化并仔细检查配置并验证其是否正确。有关详细步骤，请参阅优化、检查和验证要迁移的配置，第 12 页。
9	Cisco Secure Firewall 迁移工具	推送配置到多云防御。
10	本地计算机	下载迁移后报告以验证迁移进展情况。有关详细步骤，请参阅查看迁移后报告并完成迁移，第 17 页。
11	多云防御	验证 多云防御 上的迁移配置，并根据需要在配置网关时使用它们。

迁移的前提条件

在迁移 ASA 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。

如果您想使用安全云控制上托管的迁移工具的云版本，请跳至步骤 4。

过程

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。

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

步骤 4 如果您是 安全云控制 用户并希望使用其上托管的迁移工具，请登录您的 安全云控制 租户，然后在左侧窗格中导航至 **管理 (Administration)** > **迁移 (Migration)** > **防火墙迁移工具 (Firewall Migration Tool)** 以创建迁移实例。

获取 ASA配置文件

您可以使用以下方法之一获取 ASA 配置文件：

- 导出 ASA 配置文件，第 3 页
- 从 Cisco Secure Firewall 迁移工具连接到 ASA，第 7 页

导出 ASA 配置文件

仅当您要手动上传 ASA 配置文件时，才需要执行此任务。如果要从 Cisco Secure Firewall 迁移工具连接到 ASA，请跳至 从 Cisco Secure Firewall 迁移工具连接到 ASA，第 7 页。

注释 在导出文件后，不要手工编码或更改ASA配置。这些更改将不会迁移，它们会在迁移过程中产生错误或导致迁移失败。例如，在终端中打开和保存配置文件会添加空格或空白行，导致 Cisco Secure Firewall 迁移工具无法解析。

确保导出的 ASA 配置文件不包含 “ **More** ”文本关键字，因为这可能会导致迁移失败。

过程

步骤 1 对要迁移的 ASA 设备或情景使用 **show running-config** 命令，并从中复制配置。请参阅查看运行配置。

也可对要迁移的 ASA 设备或情景使用自适应安全设备管理器 (ASDM)，选择**文件 > 在新窗口中显示运行配置**以获取配置文件。

步骤 2 将配置保存为 `.cfg` 或 `.txt`。

如果 ASA 配置具有不同的扩展，则您不能将其上传到 Cisco Secure Firewall 迁移工具。

步骤 3 将 ASA 配置文件转移到已下载了 Cisco Secure Firewall 迁移工具的计算机。

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 安全云控制上托管的迁移工具的云版本，请跳至 上传 ASA 配置文件，第 6 页。

注释 当您启动 Cisco Secure Firewall 迁移工具的桌面版本时，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
- 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。

过程

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。

  注释
  确保在浏览器中禁用所有弹出窗口阻止程序，因为它们可能阻止显示登录弹出窗口。

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 ASA 配置导出到您的计算机，请继续执行上传 ASA 配置文件。

在 Cisco Secure Firewall 迁移工具中使用演示模式

当您启动 Cisco Secure Firewall 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 、演示 FTD 设备以及 多云防御 ）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，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 Cisco Secure Firewall 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。

上传 ASA 配置文件

开始之前

将配置文件从源 从 设备导出为 `.cfg` 或 `.txt`。

注释 不要上传手工编码的或手动更改的配置文件。文本编辑器会在文件中添加会导致迁移失败的空白行和其他问题。

过程

步骤 1 在**提取 信息**页面上的**手动上传**部分中，点击**上传** 以上传 配置文件。

步骤 2 浏览到 ASA 配置文件所在的位置，然后点击**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。控制台提供一个逐行的进度日志视图，其中包含正在解析的 配置行。如果您没有看到控制台，可以在 Cisco Secure Firewall 迁移工具后的单独窗口中找到它。

步骤 3 点击**开始解析 (Start Parsing)**。

解析摘要部分显示解析状态。

步骤 4 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 5 点击**下一步 (Next)**，选择目标参数。

从 Cisco Secure Firewall 迁移工具连接到 ASA

Cisco Secure Firewall 迁移工具可以连接到要迁移的 ASA 设备，并提取所需的配置信息。

开始之前

- 下载并启动 Cisco Secure Firewall 迁移工具。

注释 如果 ASA 没有配置**启用密码**，可以在 Cisco Secure Firewall 迁移工具中将此字段留空。

过程

步骤 1 在**提取 ASA 信息 (Extract ASA Information)** 屏幕上的**连接 ASA (Connect to ASA)** 部分中，点击**连接 (Connect)** 以连接到要迁移的 ASA 设备。

步骤 2 在 **ASA 登录**屏幕中，输入以下信息：

1. 在 **ASA IP 地址/主机名**字段中，输入管理 IP 地址或主机名（对于单情景 ASA）或 admin 情景的 IP 地址或主机名（对于多情景 ASA）。

2. 在**用户名**、**密码**和**启用密码**字段中，输入相应的管理员登录凭证。

   注释
   如果 ASA 没有配置**启用密码**，可以在 Cisco Secure Firewall 迁移工具中将此字段留空。

3. 点击**登录 (Login)**。

当 Cisco Secure Firewall 迁移工具连接到 ASA 时，它会显示一条成功连接到 ASA 的消息。

步骤 3 从**情景**下拉列表中选择要迁移的 ASA 情景。

步骤 4 （可选）选择**收集命中计数**。

选中时，此工具会计算 ASA 规则的使用次数以及自 ASA 运行时间或上次 ASA 重新启动起最后一次使用该规则的时间，并在**检查和验证**页面上显示此信息。如此可在迁移之前评估规则的有效性和相关性。

步骤 5 点击**开始提取 (Start Extraction)**。

Cisco Secure Firewall 迁移工具连接到 ASA 并开始提取配置信息。提取成功完成后，**情景选择**部分会识别上传的配置对应于单情景还是多情景 ASA。

连接到由 Cisco Secure Firewall ASA 管理的 安全云控制，并提取配置

开始之前

此程序适用于使用 安全云控制上托管的迁移工具完成的迁移。

迁移工具会获取当前由 安全云控制 管理的设备，并允许您选择要从中迁移配置的设备。

注释 请确保 Cisco Secure Firewall ASA 设备处于在线并处于同步状态，以便迁移工具检测到该设备。

过程

步骤 1 在 **提取 Cisco ASA (8.4+) 信息** 页面中，迁移工具会显示由 安全云控制]管理的 Cisco Secure Firewall ASA设备。

步骤 2 从 **选择 ASA 设备** 下拉列表中，选择要迁移其配置的设备。

步骤 3 点击**连接 (Connect)**。

步骤 4 （可选） 选中 **Collect Hitcounts** 复选框。

选中后，此工具将计算自设备正常运行或上次重启以来规则的使用次数和上次使用时间，并在“**优化、审查和验证配置**”页面上显示此信息。如此可在迁移之前评估规则的有效性和相关性。

步骤 5 点击**开始提取 (Start Extraction)**。

为 多云防御指定目标参数

开始之前

- 确保您有一个具有多云防御的安全云控制租户已启用。
- 确保您已购买 多云防御 所需的运营许可证

注释 您甚至可以在 90 天的免费试用期间迁移配置到 多云防御，因为试用体验提供了付费订用的全部功能。

- 确保您已获取多云防御的基本 URL 和 安全云控制租户名称。
- 确保您已创建 API 密钥，并且还复制了创建 API 密钥时多云防御生成的 **API 密钥 ID** 和 **API 密钥密码** 。请参阅在 多云防御 中创建 API 密钥 了解更多信息。

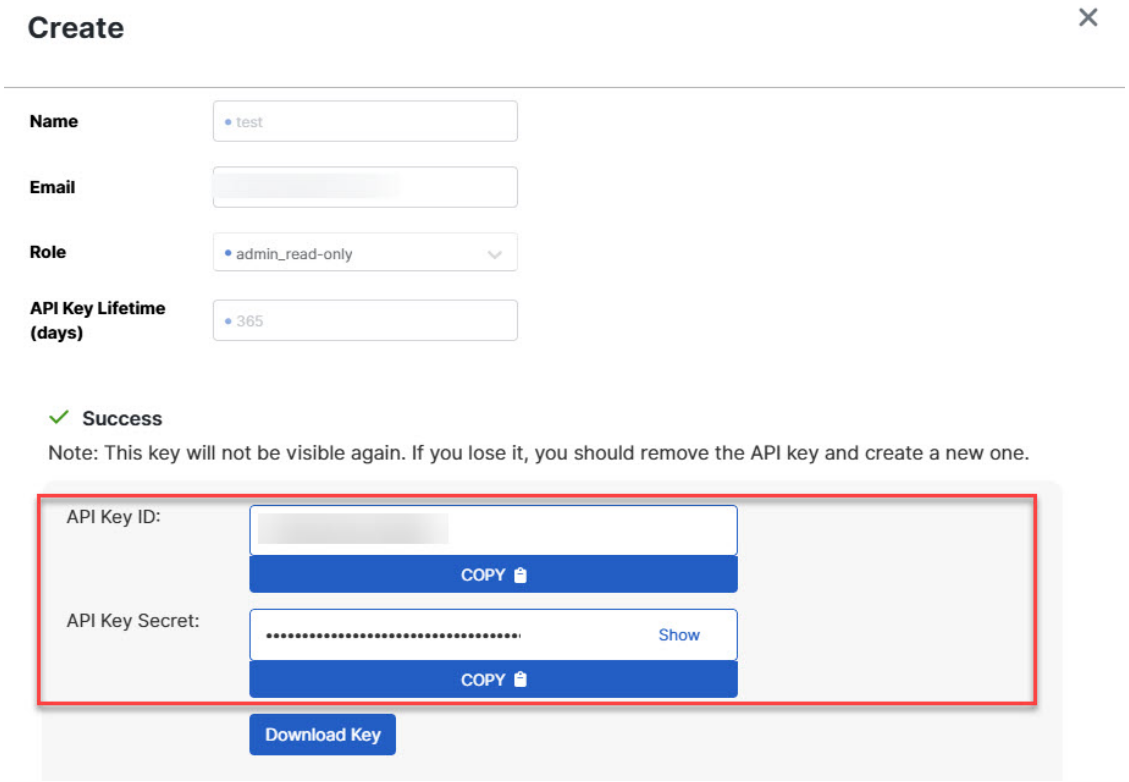
过程

步骤 1 在 **上选择目标** 窗口，选择**多云防御**。

步骤 2 在相应字段中指定以下参数以启用迁移工具和 多云防御之间的连接：

- **输入基本 URL**：这是您连接到 多云防御 控制器时在浏览器上看到的基本 URL。例如，当您在控制器仪表板中时，复制浏览器上的链接，但不包括 **/dashboard** 部分。URL 看起来像 https://xxxx.mcd.apj.cdo.cisco.com
- **输入租户姓名**：您的安全云控制租户的姓名。当您在多云防御窗口中时，从右上角的配置文件下拉菜单中复制它，或者如果您在安全云控制窗口中，则从**管理 (Administration)** > **常规设置 (General Settings)**中复制它。
- **输入 API 密钥 ID**：当您通过导航到**系统和大客户** > **API 密钥**创建 API 密钥时多云防御控制器生成的 **API 密钥 ID**。指定密钥的名称、您的电子邮件地址、您希望 API 密钥具有的角色以及 API 密钥的有效期以生成密钥。默认密钥有效期设置为 365 天。
- **输入 API Key 密码**：创建 API Key 时多云防御控制器生成的 **API Key 密码**。

  注释
  确保在创建 API 密钥时同时复制 **API 密钥 ID**和 **API 密钥密码**。如果您错过复制它们，请删除您创建的 API 密钥，生成一个新的，并确保这次复制它们。



步骤 3 单击“**连接**”并等待接收“**成功收集**”消息，该消息确认连接尝试多云防御成功。

步骤 4 通过**选择功能**，您可以选择要迁移到多云防御的配置。默认情况下，**访问控制**和**仅迁移参考对象**复选框默认处于选中状态。

请注意，此迁移不支持源防火墙的其他配置（例如接口和路由）。

步骤 5 点击 **继续** 并 **开始转换**。等待迁移工具分析源配置。

步骤 6 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 7 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）。

步骤 8 点击**下一步 (Next)**。

查看迁移前报告

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 Cisco Secure Firewall 迁移工具正在运行时下载报告。

过程

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：

- **总体摘要** - 用于提取 ASA配置信息或连接到实时 ASA配置的方法。

  可成功迁移到威胁防御的受支持的ASA设备配置元素或多云防御以及为迁移选择的特定功能摘要。

- **有错误的配置行** - 由于Cisco Secure Firewall 迁移工具无法解析而无法成功迁移的配置元素的ASA的详细信息。 在 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 Cisco Secure Firewall 迁移工具，然后再继续。

- **部分支持的配置** - 仅可部分迁移的 ASA 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 多云防御中是否支持高级选项。如果支持，则计划在使用 Cisco Secure Firewall 迁移工具完成迁移后手动配置这些选项。

- **对象和对象组冲突解决**- 在您尝试迁移的情景中存在冲突的 ASA 网络和服务对象以及对象、服务和协议对象组的详细信息。要查看有关这些对象冲突的详细信息，请点击 **冲突计数的链接**；您可以检查冲突的原因，还可以了解迁移工具如何处理冲突。

- **不支持的配置** - 因 Cisco Secure Firewall 迁移工具不支持迁移这些功能而无法迁移的 ASA 配置元素的详细信息。查看这些行，验证 多云防御中是否支持每项功能。如果支持，则计划在使用 Cisco Secure Firewall 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 多云防御 或 Cisco Secure Firewall 迁移工具支持而被忽略的 ASA配置的详细信息。Cisco Secure Firewall 迁移工具不会解析这些行。查看这些行，验证 多云防御中是否支持每项功能。如果支持，则计划手动配置这些功能。

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

步骤 4 在您的 ASA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**一步**以继续迁移。

优化、检查和验证要迁移的配置

开始之前

“**优化、审查和验证配置**”页面可让您审查和验证即将迁移到目标多云防御的配置参数。在此步骤中，迁移工具会对照多云防御上的现有配置验证配置，并就成功迁移所需执行的更改提出建议，例如关联访问控制规则以及重命名对象以避免目标 多云防御上重复。

验证后，闪烁的选项卡将指示需要在该选项卡上执行操作。

过程

步骤 1 在列出所有 **访问控制** 列表 (ACL) 条目的访问控制选项卡上，您可以执行以下操作：

- 点击 **优化 ACL** ，以便让迁移工具识别所有影子和冗余 ACL，并选择是将它们作为已禁用的 ACL 进行迁移，还是将其排除在迁移之外。

  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：

  - 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。有关 ACL 优化报告的更多信息，请参阅ACL 优化的报告，第 14 页。

  点击“**继续**”开始优化流程。

- 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配置文件。例如，如果 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。

- 如果您不想迁移或希望迁移某些处于禁用状态的ACL，请选中相应行的复选框，点击**迁移**，然后选择相关选项。点击 ”**选中所有条目**“ 复选框以执行批量更改。

步骤 2 在 **对象 (Objects)** 选项卡上，您可以执行以下操作：

选择以下选项卡并查看映射：

- 网络对象
- 端口对象
- FQDN 对象
- URL 对象

如果要重命名对象，请选中对象行的复选框，点击 **操作**，然后选择 **重命名**。点击 ”**选中所有条目**“ 复选框以执行批量更改。

步骤 3 （可选） 在**网络对象 (Network Objects)** 和**端口对象 (Port Objects)** 选项卡上，查看所有网络对象、网络组、端口对象、端口组及其值。要重命名对象或对象组，请选择对象，然后选择**操作 (Actions)** > **重命名 (Rename)**。

- 单击“**优化对象和组**”以在迁移对象之前优化对象列表。迁移工具会识别具有相同值的对象和组，并提示您选择保留哪些对象和组。
- 点击  可将对象从**检测到冲突 (Conflict Detected)** 列移至**保留的对象/组 (Objects/Groups Retained)** 列，然后点击  将对象移回原位。请注意，大多数配置中引用的配置以粗体显示。
- 点击**自动选择 (Auto Select)** 以自动选择具有最多引用对象的所有对象和组。但是，您仍然可以手动覆盖自动选择，在列之间移动对象，因为手动选择的优先级更高。
- 点击 **Optimize**（**优化**）。迁移工具会执行优化，并显示包含优化数据（包括保留和重复对象）的优化摘要。有关优化报告的详细内容，请参阅迁移后报告。
- 点击**继续 (Proceed)** 和**验证 (Validate)**。

  注释
  未被选择保留的对象和组不会被迁移，而是会被替换为它们所使用的配置中的保留对象，例如在 ACL 配置中。这样可以确保迁移的对象列表得到充分优化，并且不会迁移重复的对象。

步骤 4 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 多云防御，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 多云防御 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 多云防御 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 5 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 多云防御对象冲突。您可以接受默认后缀或将其替换为您自己的后缀。

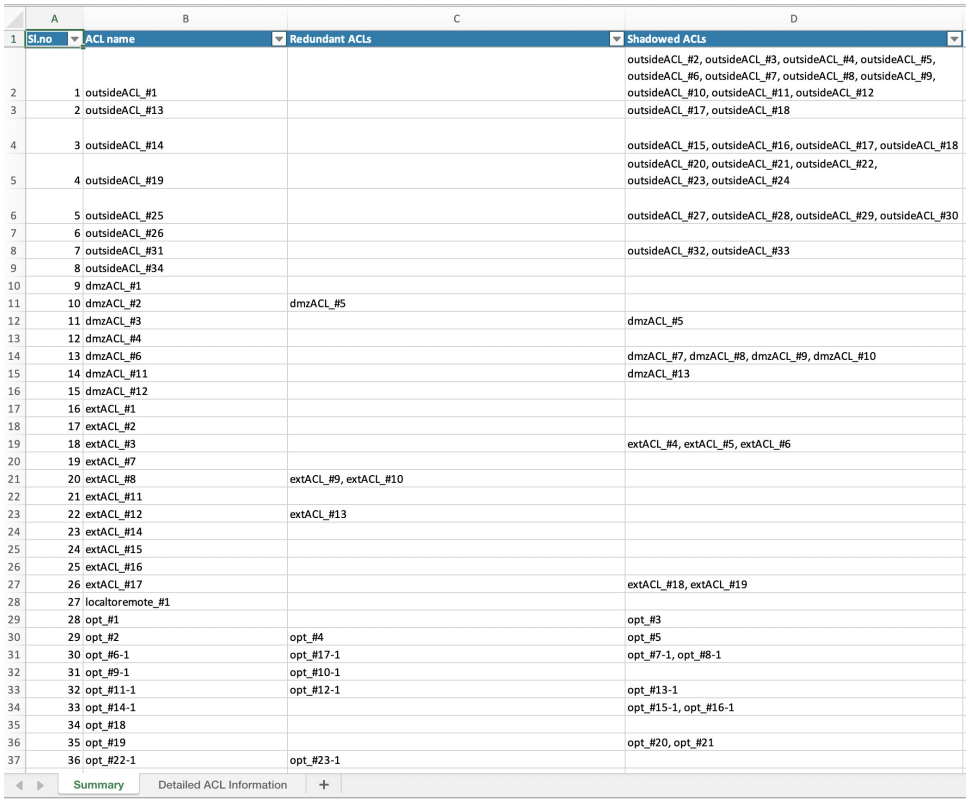
e) 点击**解决 (Resolve)**。
f) 在选项卡上解决所有对象冲突之后，点击**保存 (Save)**。
g) 点击**验证 (Validate)**，重新验证配置，并确认您已解决所有对象冲突。

步骤 6 当验证完成并且**验证状态**对话框显示消息**验证成功**时，继续将配置推送至多云防御。

ACL 优化的报告

ACL 优化报告中显示以下信息：

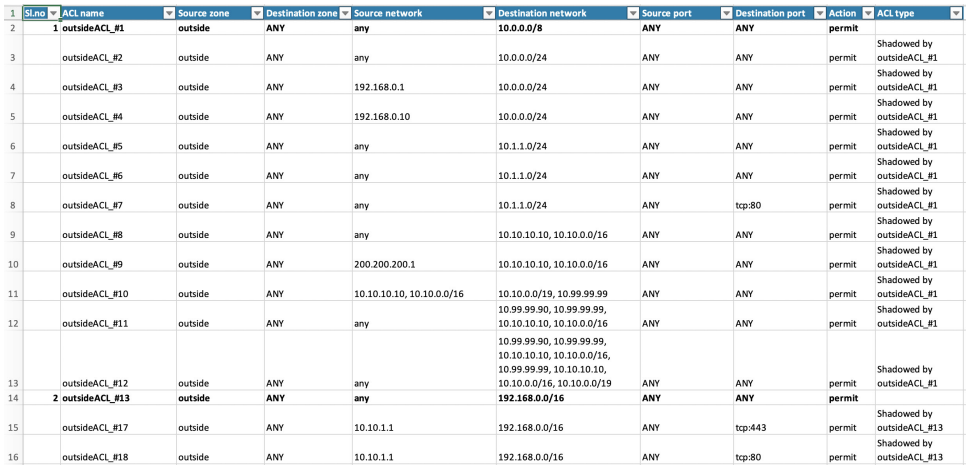
- 摘要表 (Summary Sheet) - 显示 ACL 优化的摘要。



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

推送配置到多云防御

开始之前

如果您还未成功验证配置和解决所有对象冲突，则不能将配置推送到 多云防御。

注释 当 Cisco Secure Firewall 迁移工具正在将配置发送到 多云防御时，请勿更改任何配置或部署到任何设备。

过程

步骤 1 在**验证状态**对话框中，查看验证摘要。

步骤 2 单击“**推送配置**”将源防火墙配置发送到多云防御。

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 多云防御。

注释
如果在批量推送配置时出现配置错误，迁移工具会发出警告，提示您中止迁移以手动修复错误，或继续迁移以剔除错误配置。您可以选择查看有错误的配置，然后选择**继续迁移 (Continue with migration)** 或**中止 (Abort)**。如果中止迁移，可以下载故障排除捆绑包，并与思科 TAC 共享以进行分析。

如果继续迁移，迁移工具会将迁移视为部分成功迁移。您可以下载迁移后报告，查看因推送错误而未迁移的配置列表。

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。

迁移后报告的副本也保存在与 Cisco Secure Firewall 迁移工具位于同一位置的资源文件夹中。

步骤 4 如果迁移失败，请仔细查看迁移后报告、日志文件和未解析的配置文件，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

开始之前

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。

过程

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，了解您的源配置是如何迁移的。

1. **迁移摘要**— 从源防火墙成功迁移到 多云防御的配置摘要。
2. **对象冲突处理** - 已确定与多云防御中现有对象冲突的对象的详细信息。如果对象具有相同的名称和配置，Cisco Secure Firewall 迁移工具重新使用 多云防御对象。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。
3. **您选择不迁移的访问控制规则** - 您选择不使用 Cisco Secure Firewall 迁移工具迁移的规则的详细信息。查看由 Cisco Secure Firewall 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。
4. **部分迁移的配置** - 仅部分迁移的规则的详细信息，包括带有高级选项的规则（无需高级选项即可迁移）。查看这些行，验证在 多云防御中是否支持高级选项。如果支持，手动配置这些选项。
5. **不支持的配置** - 未迁移的源防火墙配置元素的详细信息，因为 Cisco Secure Firewall 迁移工具不支持这些功能的迁移。查看这些行，验证 多云防御中是否支持每项功能。如果支持，请在 多云防御中手动配置这些功能。
6. **扩展的访问控制策略规则** - 迁移期间从单点规则扩展到多个多云防御规则的源防火墙访问控制策略规则的详细信息。
7. **对访问控制规则采取的操作**
   - **您选择不迁移的访问规则** - 您选择不使用 Cisco Secure Firewall 迁移工具迁移的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，您可以在 多云防御 中手动配置这些规则。
   - **规则操作有更改的访问规则** - 使用 Cisco Secure Firewall 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，您可以在 多云防御 中手动配置这些规则。

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。我们建议您配置一条规则多云防御以确保此流量被阻止。

步骤 3 打开**迁移前报告**并记下必须在多云防御上手动迁移的任何配置项。

步骤 4 验证并确保所有迁移的配置参数在多云防御上均可用。

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。