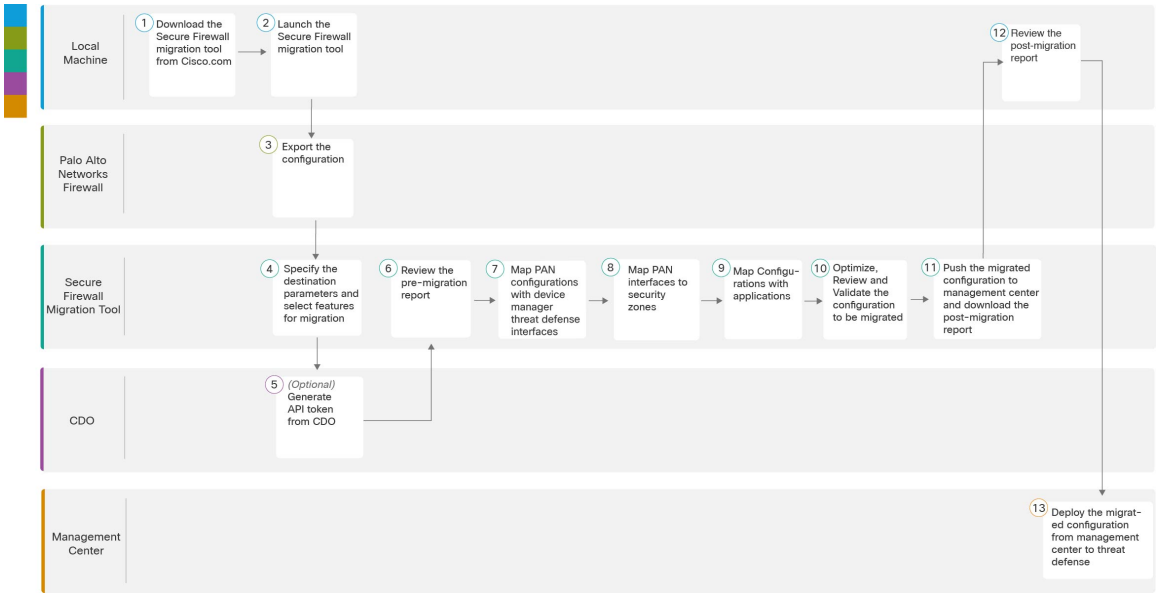
Palo Alto Networks 防火墙到威胁防御的迁移工作流程

端到端程序

以下流程图说明了使用 Cisco Secure Firewall 迁移工具将 Palo Alto 网络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。
2	本地计算机	在本地计算机上启动 Cisco Secure Firewall 迁移工具，请参阅启动 Cisco Secure Firewall 迁移工具。
3	Palo Alto Networks 防火墙	导出配置文件：要从 Palo Alto Networks 防火墙导出配置，请参阅 从 Palo Alto Networks 防火墙导出配置。
4	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。
5	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。
6	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。
7	Cisco Secure Firewall 迁移工具	为确保正确地迁移 PAN 配置，您需要将 PAN 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PAN防火墙 配置与 威胁防御 接口映射
8	Cisco Secure Firewall 迁移工具	将PAN接口映射到适当的安全区域，有关详细步骤，请参阅将 将PAN接口映射到安全区 接口组 。
9	Cisco Secure Firewall 迁移工具	您可以将PAN配置映射到相应的目标应用，有关详细步骤，请参阅 映射配置和应用 。
10	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。
11	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。
12	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，请参阅查看迁移后报告并完成迁移。
13	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，请参阅查看迁移后报告并完成迁移。

迁移的前提条件

在迁移 PAN 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。

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 从 Palo Alto Networks 防火墙导出配置 。

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：

- 如果必须使用 Cisco Secure Firewall 迁移工具从 PAN 防火墙提取信息，请继续执行Palo Alto 防火墙的配置文件（并非由 Panorama 管理）。

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。

从 Palo Alto Networks 防火墙导出配置

可以通过以下方式导出配置文件：

Palo Alto 防火墙的配置文件（并非由 Panorama 管理）

按照以下步骤从网关提取配置：

步骤 1 导航至**设备** > **设置** > **操作**，然后选择**保存指定配置** <*file_name.xml*>。

步骤 2 点击**确定 (Ok)**。

步骤 3 导航至**设备 (Device)** > **设置 (Setup)** > **操作 (Operations)**，然后点击**导出指定配置 (Export Named Configuration)**。

步骤 4 选择 <*file_name.xml*> 文件。

步骤 5 点击**确定 (Ok)**。

步骤 6 选择包含您运行的配置 <*file_name.xml*> 的 XML 文件，然后点击**确定 (Ok)** 以导出配置文件。

步骤 7 将导出的文件保存到防火墙外部的一个位置。您可以使用此备份上传到 Cisco Secure Firewall 迁移工具，将配置迁移到 威胁防御。

步骤 8 （可选）如果在您的 NAT 策略中，目标 NAT 具有相同的源和目标区域，请执行以下步骤：

a) 从防火墙上的 CLI 运行 **show routing route** 命令。

b) 将路由表复制到 *.txt* 文件。

c) 将 *.txt* 文件添加到您将从中压缩 .txt 和 .xml 文件以及 *panconfig.xml* 的文件夹中。

这些步骤对于迁移并非强制性的。如果不执行这些步骤，目标区域将不会在 Cisco Secure Firewall 迁移工具迁移期间映射，并将包括在迁移报告中。

注释 使用 **show routing route** 命令提取路由表详细信息。将提取的输出粘贴到记事本中。

Palo Alto 防火墙的配置文件（由 Panorama 管理）

如果您的设备是由 Panorama 管理的，则必须从网关提取配置。合并 Panorama 配置和网关并提取配置。

在 Cisco Secure Firewall 迁移工具用户界面中，执行以下操作：

开始之前

使用超级用户帐户来登录 Palo Alto 防火墙 Web UI。

步骤 1 导航到**设备 (Device)** > **支持 (Support)** > **技术支持文件 (Tech Support File)**。

步骤 2 点击**生成技术支持文件 (Generate Tech Support File)**。

步骤 3 生成的文件可用后，点击**下载技术支持文件 (Download Tech Support File)**。

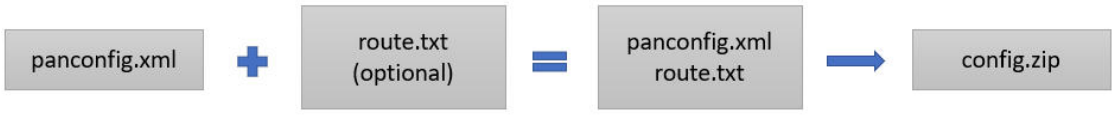
步骤 4 解压缩并解压缩文件，然后导航到路径 *\opt\pancfg\mgmt\saved-configs* 以检索 *mapped-running-config.xml* 文件。

下一步做什么

压缩导出的文件

压缩导出的文件

导出 Palo Alto 网关防火墙的 *panconfig.xml* 以及 *route.txt* （如果您的 NAT 规则具有相同的源区域和目标区域）。



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 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 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 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 Palo Alto Networks 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)**。

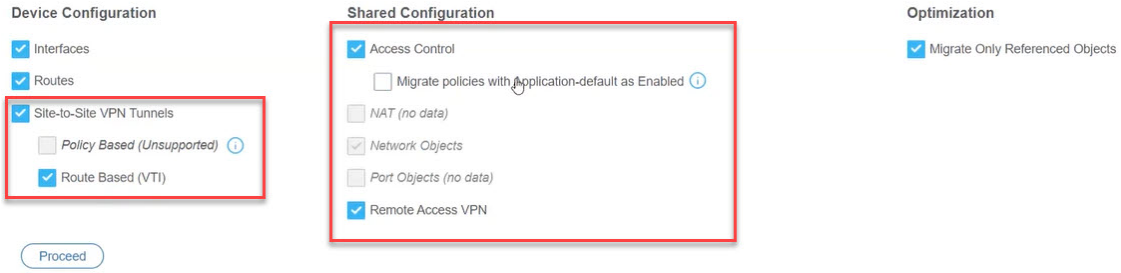
根据迁移的目标，Cisco Secure Firewall 迁移工具允许您选择要迁移的功能。

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 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 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 PAN，在**共享配置**下选择相关的**访问控制**选项：

  迁移已启用 Application-Default 的策略 - 选择此选项时，PAN 应用将迁移。仅当选中此复选框时，才能看到**迁移已启用 Application-Default 的策略**选项。

  注释 仅当选择迁移的策略时，才会启用**应用映射**。



如果要从 VPN 配置的 Palo Alto Networks 防火墙迁移配置，则可以选择或取消选择 **设备配置** 窗格下 **的站点间 VPN 隧道** 和 **共享配置** 窗格下的 **远程访问 VPN** 。请注意，不支持基于策略的站点到站点 VPN 配置，因为 Palo Alto Networks 防火墙不支持此配置。

服务为“Application-Default”的策略

服务为“**application-default**”的策略以及成员或组被引用的应用将根据您在**功能选择 (Feature Selection)** 页面上所做的选择而迁移。管理中心 没有与 **application-default** 等效的功能，所以推送此类策略时服务为“any”。如果复制与 **application-default** 类似的功能，则从 Palo Alto 网络防火墙找出应用所使用的端口，并在 管理中心 中策略的端口部分下配置这些端口。

例如，将包含“**web-browsing**”且服务为“**application-default**”的策略迁移为应用 HTTP（相当于 web-browsing），端口为“**any**”。要复制与“**application-default**”相同的功能，请将端口配置为 TCP/80 和 TCP/8080。Web-browsing 使用端口 TCP 80 和 TCP 8080。如果策略有多个应用，请配置每个应用使用的端口。

如果策略中有多个应用，我们建议您在配置端口之前拆分策略，因为它可能允许对其他应用的额外访问。

应用配置为“**any**”且服务配置为“**application-default**”的策略会以禁用状态迁移，而与**功能选择**页面上的可用选项无关（应用为“**any**”，服务为“**any**”）。如果可接受此行为，请启用应用并执行更改。否则，请选择所需的应用或服务，并启用策略。

按规则拆分应用访问控制列表

迁移包含配置到多个应用的一个规则的访问控制列表时，可以选择拆分 ACL，这会将规则拆分为多个规则，每个规则一个应用。您可以通过选中 **Split ACLs with applications per rule** 复选框来执行此操作。但是，如果您尝试迁移的配置不包含每个访问规则配置的多个应用，则不会显示该复选框。

每条规则都会转换为多个规则，每个规则一个应用，您可以在**优化、查看和验证配置**页面中查看这些规则。

- 如果目标管理中心是 7.2 或更高版本，Cisco Secure Firewall 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 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）。

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。

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：

- 可成功迁移到 威胁防御 的受支持 配置元素以及为迁移选择的特定 功能的摘要。
- **出错的配置行** - 因为 Cisco Secure Firewall 迁移工具无法解析而不能成功迁移的 配置元素的详细信息。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 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 Cisco Secure Firewall 迁移工具完成迁移后手动配置这些选项。

- **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 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 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 管理中心 或 Cisco Secure Firewall 迁移工具支持而被忽略的 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 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 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 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。

下一步做什么

将 PAN 防火墙 配置与 威胁防御 接口映射

将 PAN 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。

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 PAN 接口或端口通道 (PC) 数据接口或子接口（PAN 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。
  - 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 PAN 接口、物理子接口、端口通道或端口通道子接口（ 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PAN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。

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 7 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 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 配置中的所有子接口映射子接口。

注释 如果源防火墙上的接口数量大于目标防火墙的接口数量，则在目标防火墙上创建子接口并重试迁移。

步骤 2 当您将每个 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 PAN 接口映射到相应的 威胁防御 接口对象和安全区。有关详细信息，请参阅将 PAN 接口映射到安全区 接口组。

将 PAN 接口映射到安全区 接口组

为确保正确地迁移 配置，请将 接口映射到相应的 威胁防御 接口对象、安全区。在 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。

Cisco Secure Firewall 迁移工具支持接口与安全区的一对一映射；当安全区映射到某个接口时，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**屏幕上，查看可用接口和安全区。

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，请在**安全区**栏中，选择该接口的安全区。

步骤 4 您可以手动映射或自动创建安全区。

要手动映射安全区，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。

c) 在**安全区**栏中输入安全区名称。允许的最大字符数为 48。
d) 点击**关闭 (Close)**。

要通过自动创建映射安全区，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**区域映射**。
c) 点击**自动创建 (Auto-Create)**。

点击**自动创建 (Auto-Create)**后，系统会自动映射源防火墙区域。如果 管理中心 上已存在相同的名称区域，则该区域将重新使用。映射页面将对重新使用的区域显示“(A)”。例如，**inside** "(A)"。

步骤 5 在已将所有接口映射到相应的安全区后，点击**下一步 (Next)**。

映射配置和应用

您可以将应用映射到相应的目标应用。您可以迁移基于应用的规则。

此选项卡中列出了 管理中心 的预定义应用列表和配置文件中的一些应用。 管理中心 中存在的一些预定义映射已经映射。

注释 您将无法编辑预定义映射。

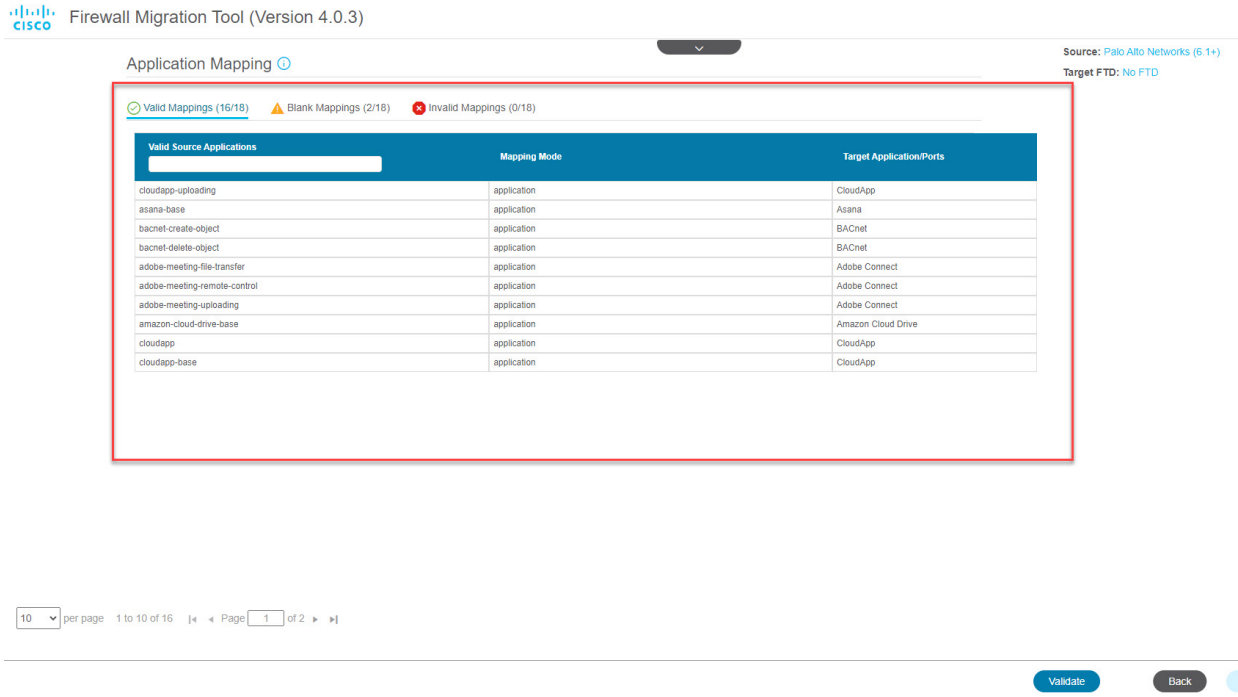
应用映射页面显示以下选项卡：

- 无效映射 - 查看该迁移的无效映射列表。

  在以下情况下，映射叫做**无效**映射：

  - 当**映射模式**选择为**应用**或**端口**，但**目标**为空时。
  - 当**映射模式**为**端口**且端口语法不正确时。要继续迁移，**无效**映射必须为零。

注释 在正确验证之前，**下一步**按钮将被禁用。



当您从源获取预定义的映射列表时，系统会自动映射预定义的应用。如果存在未映射的应用，则必须将它们手动映射到端口或应用。

- 空白映射 - 显示未映射的应用，需要用户操作。**应用**必须映射到**应用**或**端口**。

注释 建议映射所有 **应用** 条目，但不强制要求。

如果已选择映射模式，并且目标应用具备有效数据，则属于有效映射。

注释 默认情况下，**有效映射**选项卡中提供所有预定义映射。

- 有效映射 - 显示正确的映射。对于常用应用，Cisco Secure Firewall 迁移工具拥有自己的 PAN 和威胁防御 应用预定义映射数据库。如果 PAN 应用与预定义映射数据库匹配，这些应用将自动映射，并显示在有效映射下。

  应用映射到**空白映射**中的**应用**或**端口**后，它会在验证后移至**有效映射**。

注释 预定义映射不可编辑。

无效、有效和空白映射的计数基于迁移而不断变化。

下表显示应用映射属性。

表 *1:* 应用映射表属性

字段	说明
源应用	显示 Palo Alto Networks 防火墙上使用的应用列表。
映射模式	选择“应用”或“端口”作为映射模式。 • 应用 - 从可用目标应用列表中选择要映射的应用。您只能映射一个应用。 • 端口 - 从可用端口列表中选择要映射的端口。当您选择端口时，以指定的格式输入相关端口信息。例如，tcp/80 和 udp/80。 **注释** 字符之间不能有空格。
目标应用	显示基于映射模式的目标应用或端口的列表。

ICMP 和 Ping 应用将迁移为 **ICMP** 和 **ping** 服务。此操作由 Cisco Secure Firewall 迁移工具自动完成，因此不会显示在 **应用映射** 页面中。

步骤 1 点击**有效映射 (Valid Mappings)** 选项卡，查看该迁移的有效映射数量。在有效的**映射模式**下映射**有效的源应用**和**目标应用**。

当映射变为有效映射时，可以看到有效映射的数量增加。

步骤 2 点击**空白映射 (Blank Mappings)** 以查看该迁移的空白映射列表。在有效的**映射模式**下映射**空白源应用**和**目标应用**。

例如，如果选择映射模式并保存它而不输入目标，则空白映射的数量会增加。查看选项卡，正确映射后继续进行迁移。

注释 即使存在空白映射，也仍可继续进行迁移。

步骤 3 点击**无效映射 (Invalid Mappings)** 选项卡，查看无效映射列表。请执行以下操作：

a) 无效映射 - 显示迁移期间的无效映射。
b) 映射模式 - 选择“应用”或“端口”作为映射模式。
c) 目标应用 - 选择应用映射的目标应用。

例如，如果您已选择映射模式，但将应用映射到其他目标，则无法继续使用其他选项卡。查看**无效映射**选项卡，输入正确的目标应用，然后执行应用映射。

步骤 4 在每个选项卡中点击**验证 (Validate)**，以验证该迁移的无效、空白或有效映射。

步骤 5 点击**下一步 (Next)** 继续操作。

步骤 6 在验证之前，点击 **清除映射数据** 以清除您手动执行的映射。建议您仅在完全确定正在执行的映射后点击 **验证**，因为在点击验证后映射将变为有效，您将无法撤消映射。

下一步做什么

优化， 检查和验证配置

优化， 检查和验证配置

在将迁移的 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 PAN 。

- 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。

动态 IP/端口回退接口

在 **优化、查看和验证配置** 页面上查看 NAT 配置以将 Palo Alto 网络迁移到威胁防御时，您可以检查 NAT 规则是否具有 **动态 IP/端口回退** 配置，以及是否已迁移或丢弃该规则。

如果配置的动态 IP 或端口回退接口地址与目的区域地址相同，则 Cisco Secure Firewall 迁移工具会迁移 NAT 规则。如果不同，则规则不会迁移并被列为不受支持，因为 Cisco Secure Firewall 管理中心只能将目标地址用作动态 IP 或端口回退接口。如果 NAT 规则没有回退配置，则迁移无需任何验证，并在 **动态 IP/端口回退** 列中列为 **不适用** 。

步骤 1 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。

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 2 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**）
- **NAT**
- **接口**
- **路由**
- **站点间 VPN 隧道**
- **远程接入 VPN**

注释 对于站点间和远程访问 VPN 配置，VPN 过滤器配置和与其相关的扩展访问列表对象将被迁移，并且可以在相应的选项卡下进行查看。

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 3 （可选）在查看配置时，您可以在 **网络对象** 选项卡或 **端口对象** 选项卡中通过选择对象和选择 **操作** > **重命名**来重命名一个或多个网络或端口对象。

引用重命名对象的访问规则和 NAT 策略也会更新，以使用新的对象名称。

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 在 **远程访问 VPN** 部分，与远程接入 VPN 对应的所有对象都从 Palo Alto 网络防火墙 迁移到管理中心并显示：

- **策略分配**：查看并验证连接配置文件、其 VPN 协议、目标设备以及 VPN 接口的名称。要重命名连接配置文件，请选择相应的条目，然后选择 **操作** > **重命名**。
- **IKEV2**：查看并验证 IKEv2 协议配置（如果有）以及与其映射的源接口。
- **Anyconnect 软件包**：检索 AnyConnect 软件包 和 AnyConnect 配置文件应从源 设备检索且必须可用于迁移。

  作为迁移前活动的一部分，将所有 AnyConnect 软件包上传到管理中心。您可以将 AnyConnect 配置文件直接上传到管理中心或从 Cisco Secure Firewall 迁移工具上传。

  选择从管理中心检索的现有 Anyconnect、Hostscan 或外部浏览器 软件包。 您必须至少选择一个 AnyConnect 软件包。 您必须选择 Hostscan、dap.xml、data.xml 或外部浏览器（如果在源配置中可用）。AnyConnect 配置文件为可选。

  确保从源防火墙检索到正确的 Dap.xml 文件。对配置文件中可用的 dap.xml 文件执行验证。您必须上传并选择所有必需的文件来进行验证。更新失败将被标记为不完整，并且 Cisco Secure Firewall 迁移工具不会继续进行验证。
- **地址池**-检查所有显示在这里的 IPv4 和 IPv6 池。
- **组策略**-从此区域中选择或删除用户配置文件、管理配置文件和客户端模块配置文件，此区域显示带客户端配置文件的组策略、管理配置文件、客户端模块和不带配置文件的组策略。如果配置文件是在 AnyConnect 文件部分中添加的，则会显示为预选。您可以选择或删除用户配置文件、管理配置文件和客户端模块配置文件。
- **连接配置文件**-检查此处显示的所有连接配置文件/隧道组。
- **信任点** - 信任点或 PKI 对象从 PAN 防火墙 迁移到管理中心是迁移前活动的一部分，并且也是成功迁移远程访问 VPN 所必不可少的。 **映射远程访问接口** 部分中的全局 SSL、IKEv2 和接口的信任点，以继续执行后续迁移步骤。

  如果存在安全断言标记语言 (SAML) 对象，则可以在 SAML 部分中映射 SAML IDP 和 SP 的信任点。SP 证书上传为可选。也可以覆盖特定隧道组的信任点。如果覆盖的 SAML 信任点配置在源 中可用，则可以在 **覆盖 SAML**选项中选择该配置。

步骤 7 （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 8 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 9 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 10 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 20 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 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 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， 检查和验证配置 ，第 16 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 Cisco Secure Firewall 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 配置是如何迁移的：

- **迁移摘要** - 已成功从 迁移到 威胁防御 的配置的摘要信息，其中包括有关 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 功能的详细信息。

- **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 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。

- **源接口名称至威胁防御安全区** - 已成功迁移的 PAN 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。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 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 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 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。

- **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，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 Cisco Secure Firewall 迁移工具不支持迁移这些功能而未被迁移的 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 Point 规则扩展到多个 威胁防御 规则的 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 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，可以手动配置这些规则。

  - **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，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 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 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 Cisco Secure Firewall 迁移工具更改了“日志设置”的 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 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 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。

Cisco Secure Firewall 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 配置的主机名。

解析摘要

解析摘要显示对象、接口、NAT、策略和应用的数量。摘要有三个组成部分：解析前摘要、解析摘要和推送前摘要。

- **解析前摘要** - 上传配置后显示解析前摘要。在此阶段，Cisco Secure Firewall 迁移工具显示各种组成部分的计数。仅显示自定义应用或组中使用的应用。如果配置为多 VSYS，则显示完整 *VSYS* 的接口计数。解析前摘要不会显示所有应用，因为策略中直接调用的应用不计算在内。因此，

应用计数不同于解析摘要。NAT 上也有类似的情况。解析前摘要的几个组成部分可能显示零计数，但这并不意味着这些配置有零个配置元素。

- **解析摘要** - 点击“开始转换”后显示解析摘要。在此阶段，Cisco Secure Firewall 迁移工具已对配置执行操作，并从摘要计数中删除了所有不受支持的配置。不受支持的策略包含在计数中，因为不受支持的策略在迁移到管理中心后处于禁用状态。配置的每个组成部分都会被解析。解析摘要中显示的计数是将要迁移的确切配置计数。
- **推送前摘要**-在系统提示您将配置推送到 管理中心之前，显示推送前摘要。根据 Cisco Secure Firewall 迁移工具采取的操作，解析前摘要计数可能不同于解析摘要。NAT 中直接引用的 IP 将作为对象推送。如果将应用映射到端口，服务计数会增加，应用计数会下降。如果应用映射留空，应用计数会减少。如果静态路由有重复条目，该条目将被删除且计数将减少。

迁移失败

迁移期间的解析失败如下：

- **解析失败** - 将配置上传到 Cisco Secure Firewall 迁移工具后发生解析失败。原因是接口配置错误。如果配置了多个 IP 或将 /32 或 /128 IP 分配给了接口，则会导致解析失败。

  如果为接口分配了多个 IP 或者隧道、环回或 VLAN 接口包含在路由中，则会导致推送失败。

  解决方法 - 下载**迁移前报告**，并参阅迁移报告中**出错的配置行**部分。此部分显示导致该问题的配置的详细信息。您必须纠正该问题并将配置重新上传到 Cisco Secure Firewall 迁移工具。

  如果推送失败是由路由中的隧道、环回或 VLAN 接口导致的，则必须删除此类路由并重试迁移，因为 管理中心不支持此类接口。

- **推送失败** - 当 Cisco Secure Firewall 迁移工具已迁移配置并且正在推送到 管理中心时，发生推送失败。**迁移后报告**中会记录推送失败。

  解决方法 - 下载**迁移后报告**，并参阅迁移报告中的**错误报告**部分。此部分显示导致该问题的配置的详细信息。您必须在 **检查和验证** 页面上纠正该问题，方法是对于显示失败的部分选择 **不迁移**选项，也可以在源配置中修复该问题并将配置重新上传到 Cisco Secure Firewall 迁移工具。

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： PAN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 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 2 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 3 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 4 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 7 页。

步骤 5 将 接口与 威胁防御 接口映射。

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

有关详细信息，请参阅将 PAN 防火墙 配置与 威胁防御 接口映射。

步骤 6 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 逻辑接口映射到安全区。

有关详细信息，请参阅将 PAN 接口映射到安全区 接口组。

步骤 7 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 8 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。

步骤 9 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 25 页。

步骤 1 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

步骤 2 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 3 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 4 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 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 5 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。