使用思科防御协调器中的防火墙迁移工具来迁移防火墙

本文档可帮助您使用思科防御协调器 (CDO) 上托管的 Cisco Secure Firewall 迁移工具的云版本。

CDO 托管了 Cisco Secure Firewall 迁移工具的云版本，您可以使用该工具将现有防火墙配置迁移到 CDO 租户上部署的由云提供的防火墙管理中心管理的 Cisco Secure Firewall Threat Defense 设备。

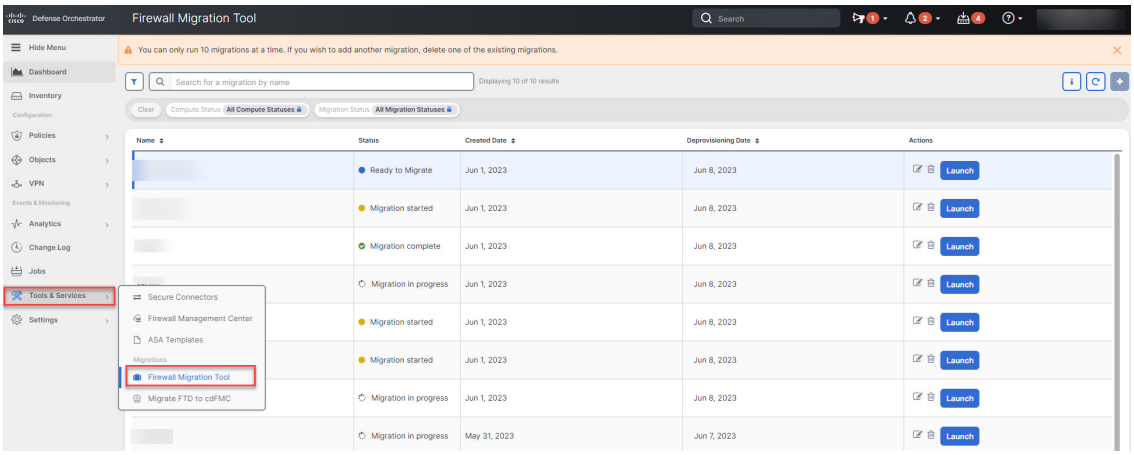
本指南适用对象

如果您使用的 CDO 管理 Cisco Secure Firewall ASA 设备和 FDM 托管的威胁防御设备，或者您使用的第三方防火墙（例如 Palo Alto Networks、Check Point 和 Fortinet 防火墙），并且希望迁移到 Cisco Secure Firewall Threat Defense。您可以使用 CDO 中的 Cisco Secure Firewall 迁移工具将所有现有防火墙配置迁移到由云交付的防火墙管理中心托管的威胁防御设备。本文档介绍迁移配置所需执行的操作。

思科防御协调器中的防火墙迁移工具使用入门

在验证配置后，CDO 中的迁移工具会从您选择的源设备或上传的配置文件中提取设备配置，然后将其迁移到 CDO 租户上调配的云交付的防火墙管理中心。迁移工具支持大多数配置；必须在云交付的防火墙管理中心中手动配置不受支持的配置。请参阅 支持的配置， 第 2 页。

当您在**工具和服务 (Tools & Services)** > **防火墙迁移工具 (Firewall Migration Tool)**中初始化新的迁移并**启动**它时，系统会在新的浏览器选项卡中打开一个迁移工具的云实例，让您能够使用逐步引导的工作流程来执行迁移任务。CDO 中的迁移工具使您无需下载和维护桌面版本的 Cisco Secure Firewall 迁移工具。



您可以使用 CDO 上托管的迁移工具将以下思科和第三方防火墙配置迁移到 Cisco Secure Firewall Threat Defense 设备：

- Cisco Secure Firewall ASA
- 由防火墙设备管理器管理的 Cisco Secure Firewall Threat Defense
- Check Point 防火墙
- Palo Alto Networks 防火墙
- Fortinet 防火墙

重要事项 您需要在 CDO 中拥有管理员或超级管理员用户角色，才能使用防火墙迁移工具。

支持的配置

迁移工具部分支持以下配置：

- 网络对象和组
- 服务对象，为源和目标配置的除外
- 引用的 ACL 和 NAT 规则
- 服务对象组

注释 由于云交付的管理中心不支持嵌套，因此请在迁移之前将嵌套的服务对象组内容细分为单个对象。

- IPv4 和 IPv6 FQDN 对象与组
- IPv6 转换（接口、静态路由、对象、ACL 和 NAT）

- 应用于入口接口的访问规则
- 全局 ACL
- 自动 NAT、手动 NAT 和对象 NAT
- 静态路由、等价多路径 (ECMP) 路由和基于策略的路由 (PBR)
- 物理接口
- 子接口
- 端口通道
- Virtual Tunnel Interface
- 透明模式下的网桥组
- IP SLA 对象 - 迁移工具会创建它们、使用静态路由映射它们，然后再迁移它们
- 基于时间的对象
- 站点到站点 VPN
  - 站点间 VPN - 当防火墙迁移工具检测到源 ASA 或 FDM 托管设备中的加密映射配置时，Cisco Secure Firewall 迁移工具会将其作为点对点拓扑迁移到管理中心 VPN。
  - ASA 和 FDM 托管设备的基于加密映射（静态/动态）的 VPN
  - 基于路由 (VTI) 的 ASA 和 FDM VPN
  - 源于 ASA 和 FDM 托管设备的基于证书的 VPN 迁移

重要事项 如果源设备中有站点间 VPN 配置，请确保在云交付的防火墙管理中心中手动配置 ASA 和 FDM 托管的设备信任点或证书。

- 远程访问 VPN
  - SSL 和 IKEv2 协议
  - 身份验证方式 - 仅 AAA、仅客户端证书、SAML、AAA 和客户端证书
  - AAA - Radius、本地、LDAP 和 AD
  - 连接配置文件、组策略、动态访问策略、LDAP 属性映射和证书映射
  - 标准和扩展 ACL
  - 自定义属性和 VPN 负载均衡

重要事项 如果已在源防火墙中配置远程访问 VPN，请确保执行以下任务：

- 在管理中心上将 ASA 和 FDM 管理的设备信任点手动配置为 PKI 对象
- 从源 ASA 和 FDM 托管设备检索 AnyConnect 包、Hostscan 文件（Dap.xml、Data.xml、Hostscan 包）、外部浏览器包和 AnyConnect 配置文件
- 将所有 AnyConnect 软件包和配置文件上传到管理中心

- 动态路由对象、BGP 和 EIGRP
  - 策略列表
  - 前缀列表
  - 社区列表
  - 自治系统 (AS) 路径
  - 路由映射

注释 迁移工具会根据名称和配置来分析所有对象和对象组，并重新使用具有相同名称和配置的对象；但是，远程访问 VPN 配置中的 XML 配置文件仅使用其名称来进行验证。

许可证

Cisco Secure Firewall 迁移工具不需要从 CDO 访问任何其他许可证。

但是，您需要具有 CDO 基础订用和要迁移的 威胁防御 功能的许可证。

初始化新的迁移实例

步骤 1 登录 CDO 租户。

步骤 2 选择**工具和服务 (Tools & Services)** > **防火墙迁移工具 (Firewall Migration Tool)**。

步骤 3 点击蓝色加号 按钮以初始化新的迁移实例。

注释 通过使用防火墙迁移工具，您可以创建最多 10 个迁移并同时启动所有迁移 - 每个迁移实例都将在新的浏览器选项卡中打开。但是，如果您的租户上调配了多个用户，则请注意，您只能启动自己创建的迁移。

如果要在已有 10 个迁移的情况下初始化新的迁移实例，请删除其中一个现有的迁移实例。

步骤 4 CDO 会自动为您的迁移生成名称；您可以使用自动生成的名称，也可以根据需要进行更改。

步骤 5 点击**确定 (OK)** 并等待，直到您看到状态从**正在初始化 (Initializing)** 更改为**迁移就绪 (Ready to Migrate)**。当您的迁移准备就绪时，CDO 还会在**通知 (Notifications)** 窗格中显示新的通知。

步骤 6 在新迁移中，点击**启动 (Launch)**。

迁移工具将在新的浏览器选项卡中打开，并且不需要进行任何身份验证。

注释 CDO 中的迁移自创建之日起 7 天内有效，之后将自动取消调配。这样可确保不时释放 CDO 资源。您可以在**创建日期 (Created Date)** 和**取消调配日期 (Deprovisioning Date)** 列中查看日期。

CDO 在**状态 (Status)** 列中显示所有迁移的状态；您可以根据迁移的状态来过滤迁移。您还可以在右侧窗格中选择迁移以查看其详细信息，例如创建日期和时间、开始日期和时间、源和目标设备名称以及创建者。请注意，在您的 CDO 租户上调配多个用户时，您只能启动自己创建的迁移。

删除迁移实例

如果打算在CDO自动取消调配之前手动取消调配迁移，请执行以下步骤。例如，您可以在迁移任务完成后删除迁移。

步骤 1 选择**工具和服务 (Tools & Services)** > **防火墙迁移工具 (Firewall Migration Tool)**。

步骤 2 在要删除的迁移上，点击**操作 (Actions)** 窗格下的**删除 (Delete)**。

步骤 3 点击**删除 (Delete)** 确认您的操作。

迁移思科防御协调器管理的安全防火墙 ASA

通过 CDO 中的 Cisco Secure Firewall 迁移工具，您可以从由 CDO 管理的实时 ASA 设备或使用从 ASA 设备提取的配置文件来迁移配置。

选择源配置

从CDO启动迁移实例后，在**选择源配置 (Select Source Configuration)** 中选择**思科 ASA (Cisco ASA)**，然后点击**开始迁移 (Start Migration)**。您可以手动上传 ASA 配置文件，也可以选择**连接到 ASA (Connect to ASA)** 窗格中列出的任何 CDO 管理的 ASA 设备。如果您尝试选择 CDO 管理的设备，请注意**配置状态 (Configuration Status)** 为**已同步 (Synced)** 的设备仅由迁移工具列出；如果在列表中没有看到要迁移的设备，请检查设备配置更改是否是最新的并与CDO同步。请注意，多个用户可以同时选择一台 ASA 设备作为源设备，并且配置提取会无缝进行。如果您在 ASA 设备上配置了一个或多个安全情景，则迁移工具允许您选择要迁移的情景；您还可以将所有情景都合并到一个实例中，然后再进行迁移。有关详细信息，请参阅选择 ASA 主要安全情景。

迁移工具会解析设备配置并显示包含已解析配置的摘要。点击**下一步 (Next)**。

选择目标

在**选择目标”(Select Target)** 页面中，默认情况下会选择 CDO 租户上调配的 Firewall Management Center 云交付调配，并会列出该管理中心管理的 威胁防御 设备。您可以选择要将 ASA 配置迁移到的 威胁防御 设备，也可以选择**不使用 FTD 继续 (Proceed without FTD)**。请注意，列出的威胁防御设备会根据设备是否正在另一个迁移实例中使用而显示为**正在使用 (In Use)** 或**可用 (Available)**。但是，您可以通过点击**更改设备状态 (Change Device Status)**，从**正在使用 (In Use)** 列表中选择设备，然后点击**继续 (Continue)** 来执行覆盖，这将使设备可被选为目标。

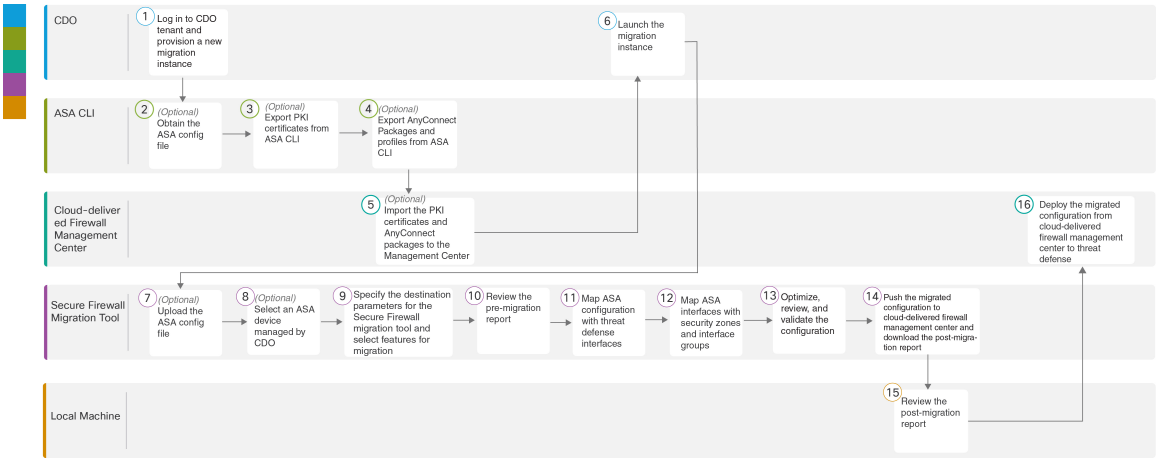
⚠

注意 将设备状态从**正在使用 (In Use)**更改为**可用 (Available)** 会影响已在使用设备的正在进行的迁移实例。我们建议您在执行此操作时保持谨慎。

选择**不使用 FTD 继续 (Proceed without FTD)** 的情况下只会将 NAT 对象、ACL 和端口对象推送到云交付的防火墙管理中心。有关常用 ASA 功能及其等效威胁防御功能的详细信息，请参阅 Cisco Secure Firewall ASA 到威胁防御功能映射指南。

以下流程图说明了在 CDO 中使用防火墙迁移工具来将 ASA 迁移到 威胁防御 的逐步程序。

图 *1:* 使用 *CDO* 中的防火墙迁移工具将 *ASA* 迁移到 *FTD* 的端到端程序



要执行包含更详细步骤的程序，请继续参阅使用迁移工具将 Cisco Secure Firewall ASA 迁移到威胁防御指南中的获取 ASA 配置文件。

	工作空间	步骤
1	首席数据官	登录到您的 CDO 租户，导航至**工具和服务 (Tools & Services)** > **防火墙迁移工具 (Firewall Migration Tool)**，，然后点击蓝色加号 按钮开始调配新的迁移实例。
2	ASA CLI	（可选）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。如果要在**选择源配置 (Select Source Configuration)** 中选择 CDO 管理的 ASA 设备，请跳至步骤 3。

	工作空间	步骤
3	ASA CLI	（可选）从 ASA CLI 导出公钥基础设施 (PKI) 证书：仅在打算将站点间 VPN 和 RAVPN 配置从 ASA 迁移到威胁防御时，才需要执行此步骤。要从 ASA CLI 导出 PKI 证书，请参阅从 ASA 导出 PKI 证书并导入管理中心中的步骤 1。如果您的设备上没有远程访问 VPN 配置，或者不打算迁移站点间 VPN 和远程访问 VPN，请跳至步骤 7。
4	ASA CLI	(可选）从 ASA CLI 导出 AnyConnect 包和配置文件：只有打算将远程访问 VPN 功能从 ASA 迁移到威胁防御时，才需要执行此步骤。要从 ASA CLI 导出 AnyConnect 软件包和配置文件，请参阅检索 AnyConnect 软件包和配置文件。
5	云交付的防火墙管理中心	（可选）将 PKI 证书和 AnyConnect 软件包导入管理中心：要将 PKI 证书导入管理中心，请参阅从 ASA 导出 PKI 证书并导入管理中心中的步骤 2 和检索 AnyConnect 软件包和配置文件。
6	首席数据官	确保您创建的迁移实例的状态为**迁移就绪 (Ready to Migrate)**，然后点击**启动 (Launch)**；Cisco Secure Firewall 迁移工具将在新的浏览器选项卡中打开。
7	Cisco Secure Firewall 迁移工具	（可选）上传从 ASA CLI 获取的 ASA 配置文件，请参阅上传 ASA 配置文件。如果要从 CDO 管理的 ASA 设备迁移配置，请跳至步骤 8。
8	Cisco Secure Firewall 迁移工具	从显示的由 CDO 租户管理的 ASA 设备列表中，选择要迁移其配置的设备。如果在 ASA 设备上配置了多个安全情景，请在**主情景选择 (Primary Context Selection)** 下拉列表中选择要迁移的情景，或者选择将所有情景合并到单个实例。有关详细信息，请参阅选择 ASA 主要安全情景。
9	Cisco Secure Firewall 迁移工具	在**选择目标 (Select Target)** 页面上，默认情况下会选择在 CDO 租户上调配的云交付的防火墙管理中心。
10	Cisco Secure Firewall 迁移工具	从由云交付的防火墙管理中心管理的威胁防御设备列表中选择目标设备，或选择**不使用 FTD 继续 (Proceed without FTD)** 并继续。
11	Cisco Secure Firewall 迁移工具	下载迁移前报告并查看已解析配置的详细摘要。有关详细步骤，请参阅查看迁移前报告。
12	Cisco Secure Firewall 迁移工具	使用 ASA 配置来**映射 FTD 接口**。 由于 ASA 和威胁防御设备上的物理接口和端口通道接口的名称并不总是相同，因此您可以选择要将 ASA 接口映射到目标威胁防御设备中的哪个接口。有关更多信息，请参阅将 ASA 配置映射到 Cisco Secure Firewall 设备管理器威胁防御接口。
13	Cisco Secure Firewall 迁移工具	将 ASA 接口映射到现有的威胁防御安全区域和接口组。有关详细步骤，请参阅将 ASA 接口映射到安全区域和接口组。

	工作空间	步骤
14	Cisco Secure Firewall 迁移工具	请谨慎**优化、查看和验证配置**，并确保按照目标威胁防御设备的预期来配置 ACL、对象、NAT、接口、路由、站点间 VPN 和远程访问 VPN 规则。请参阅优化、检查和验证配置。
15	Cisco Secure Firewall 迁移工具	配置验证成功后，**推送配置**到云交付的的防火墙管理中心。有关更多信息，请参阅将迁移的配置推送到管理中心。
16	本地计算机	下载并查看迁移后报告。要了解有关迁移后报告包含的信息的详细信息，请参阅查看迁移后报告和完成迁移。
17	云交付的防火墙管理中心	将新迁移的配置部署到威胁防御设备。

迁移思科防御协调器管理的 FDM 托管设备

您可以使用配置文件来迁移 FDM 管理的设备配置，或者只需选择载入 CDO 的 FDM 托管设备即可。

选择源配置

从 CDO 启动迁移实例后，请在**选择源配置 (Select Source Configuration)** 中选择**Cisco Secure Firewall 设备管理器 (Cisco Secure Firewall Device Manager)**，然后从以下选项中进行选择：

- **迁移 Firepower 设备管理器（仅限共享配置）**
- **迁移 Firepower 设备管理器（包括设备和共享配置）**
- **将 Firepower 设备管理器（包括设备和共享配置）迁移到 FTD 设备（新硬件）**

点击**继续 (Continue)** 时，迁移工具使您能够手动上传 FDM 托管设备配置文件，或选择任何一个载入 CDO 的 FDM 托管设备（列于**连接到 FDM (Connect to FDM)**）窗格中，然后点击**下一步 (Next)**。

选择目标

在**选择目标”(Select Target)** 页面中，默认情况下会选择 CDO 租户上调配的 Firewall Management Center 云交付调配，并会列出该管理中心管理的 威胁防御 设备。您可以选择要将配置迁移到的 威胁防御 设备，然后继续迁移。

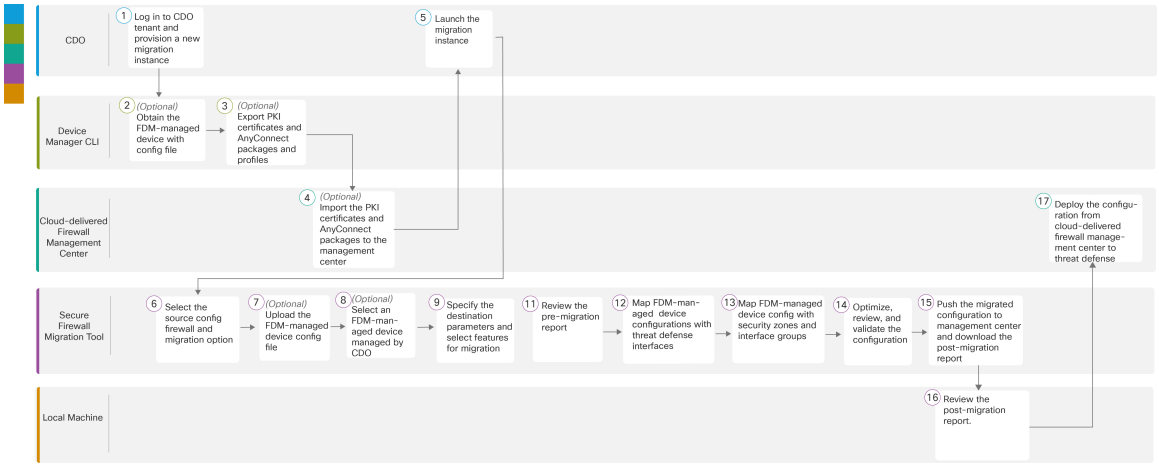
请注意，列出的威胁防御设备会根据设备是否正在另一个迁移实例中使用而显示为**正在使用 (In Use)** 或**可用 (Available)**。但是，您可以通过点击**更改设备状态 (Change Device Status)**，从**正在使用 (In Use)** 列表中选择设备，然后点击**继续 (Continue)** 来执行覆盖，这将使设备可被选为目标。

⚠

注意 将设备状态从**正在使用 (In Use)**更改为**可用 (Available)** 会影响已在使用设备的正在进行的迁移实例。我们建议您在执行此操作时保持谨慎。

以下流程图说明了在 CDO 中使用防火墙迁移工具来迁移 FDM 托管设备的逐步程序。

图 2: 使用 *CDO* 中的防火墙迁移工具将 *FDM* 托管设备迁移到 *FTD* 的端到端程序



要执行包含更详细步骤的程序，请继续参阅使用迁移工具将FDM管理的设备迁移到安全防火墙威胁防御指南中的获取 FDM 管理的设备配置文件。

	工作空间	步骤
1	首席数据官	登录到您的 CDO 租户，导航至**工具和服务 (Tools & Services)** > **防火墙迁移工具 (Firewall Migration Tool)**，，然后点击蓝色加号  按钮开始调配新的迁移实例。
2	设备管理器 CLI	（可选）获取FDM托管设备配置文件：要从设备管理器CLI获取FDM托管设备配置文件，请参阅获取FDM托管设备配置文件。如果要在**选择源配置 (Select Source Configuration)** 中选择 CDO 管理的 FDM 设备，请跳至步骤 3。
3	设备管理器 CLI	（可选）导出 PKI 证书和 AnyConnect 软件包和配置文件：仅当您计划将站点间 VPN 和远程访问 VPN 功能从 FDM 托管设备迁移到威胁防御时，才需要执行此步骤。要从设备管理器 CLI 导出 PKI 证书，请参阅在防火墙管理中心导出和导入 PKI 证书中的步骤 1。要从设备管理器 CLI 导出 AnyConnect 软件包和配置文件，请参阅检索 AnyConnect 软件包和配置文件中的步骤 1。如果您不打算迁移站点间 VPN 和远程访问 VPN 配置，请跳至步骤 7。
4	云交付的防火墙管理中心	（可选）将 PKI 证书和 AnyConnect 软件包导入管理中心：要将 PKI 证书导入管理中心，请参阅在防火墙管理中心导出和导入 PKI 证书中的步骤 2 和检索 AnyConnect 软件包和配置文件。
5	首席数据官	确保您创建的迁移实例的状态为**就绪 (Ready)**，然后点击**启动 (Launch)**；Cisco Secure Firewall 迁移工具将在新的浏览器选项卡中打开。
6	Cisco Secure Firewall 迁移工具	要选择源配置防火墙和迁移选项，请参阅选择源配置防火墙和迁移。

	工作空间	步骤
7	Cisco Secure Firewall 迁移工具	（可选）上传从设备管理器 CLI 获取的 FDM 托管设备配置文件，请参阅上传 FDM 托管设备配置文件。如果要从已自行激活的 FDM 托管设备将配置迁移到 CDO，请跳至步骤 8。
8	Cisco Secure Firewall 迁移工具	从显示的由 CDO 租户管理的 FDM 托管设备列表中，选择要迁移其配置的设备。
9	Cisco Secure Firewall 迁移工具	在**选择目标 (Select Target)** 页面上，默认情况下会选择在 CDO 租户上调配的云交付的防火墙管理中心。
10	Cisco Secure Firewall 迁移工具	从由云交付的防火墙管理中心管理的威胁防御设备列表中选择目标设备，或选择**不使用 FTD 继续 (Proceed without FTD)** 并继续。
11	Cisco Secure Firewall 迁移工具	下载迁移前报告并查看已解析配置的详细摘要。有关详细步骤，请参阅查看迁移前报告。
12	Cisco Secure Firewall 迁移工具	使用 FDM 管理的设备配置来**映射 FTD 接口**。 由于FDM和威胁防御设备上的物理接口和端口通道接口的名称并不总是相同，因此您可以选择要将FDM托管设备接口映射到目标威胁防御设备中的哪个接口。有关更多信息，请参阅将FDM托管设备配置映射到 Cisco Secure Firewall 设备管理器威胁防御接口。
13	Cisco Secure Firewall 迁移工具	将FDM托管设备接口映射到现有的威胁防御安全区域和接口组。有关详细步骤，请参阅将 FDM 托管接口映射到安全区域和接口组。
14	Cisco Secure Firewall 迁移工具	请谨慎**优化、查看和验证配置**，并确保按照目标威胁防御设备的预期来配置 ACL、对象、NAT、接口、路由、站点间 VPN 和远程访问 VPN 规则。请参阅优化、检查和验证配置。
15	Cisco Secure Firewall 迁移工具	配置验证成功后，**推送配置**到云交付的的防火墙管理中心。有关更多信息，请参阅将迁移的配置推送到管理中心。
16	本地计算机	下载并查看迁移后报告。要了解有关迁移后报告包含的信息的详细信息，请参阅查看迁移后报告和完成迁移。
17	云交付的防火墙管理中心	将新迁移的配置部署到威胁防御设备。

恢复迁移

如果您已从CDO开始迁移并希望稍后再继续，则只需关闭防火墙迁移工具选项卡即可。如果要继续迁移，可以登录 CDO，然后在**防火墙迁移工具 (Firewall Migration Tool)** 中点击要继续迁移的**启动 (Launch)**。迁移工具检测到您正在迁移，并让您能够从中断的位置继续。但是，要让迁移工具检测到您有正在进行的迁移，则必须至少执行源配置解析。如果在执行此步骤之前停止了迁移，您仍然可以从 CDO 启动相同的迁移，但必须从第一个开始迁移。

相关文档

要了解有关使用 CDO 中的 Cisco Secure Firewall 迁移工具迁移第三方防火墙的详细信息，请根据您的要求参阅以下文档：

- 要了解有关防火墙迁移工具的最新功能和版本特定信息，请参阅 Cisco Secure Firewall 迁移工具版本说明。

注释 思科防御协调器托管了最新版本的 Cisco Secure Firewall 迁移工具。

- 要将配置从 Check Point 防火墙迁移到威胁防御，请从将 Check Point 防火墙迁移到威胁防御指南中的导出检查点配置文件开始。
- 要将配置从 Palo Alto Networks 防火墙迁移到威胁防御，请从将 Palo Alto Networks 防火墙迁移到威胁防御指南中的从 Palo Alto Networks 防火墙导出配置开始。
- 要将配置从 Fortinet 防火墙迁移到威胁防御，请从将 Fortinet 防火墙迁移到威胁防御指南中的从 Fortinet 防火墙导出配置开始。

重要事项 与 ASA 和 FDM 管理的设备迁移不同，您只能上传手动提取的配置文件，以便将第三方防火墙配置迁移到威胁防御。

如果您希望阅读有关安全防火墙迁移工具和所有相关文档的整体信息，请参阅 Cisco Secure Firewall 迁移工具。

相关文档

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。