Cisco Secure 防火墙威胁防御 模型迁移指南，版本 7.6.1

Revised: 2025 年 12 月 22 日

关于 Secure 防火墙威胁防御 模型迁移

Cisco Secure 防火墙威胁防御 模型迁移向导使您能够将配置从旧 防火墙威胁防御 模型迁移到新模型。迁移后，源 防火墙威胁防御 设备的所有路由和接口配置都将在目标 防火墙威胁防御 中可用。

该向导支持多个型号作为源设备和目标设备。

当您将 Firepower 4100 和 9300 系列设备迁移到受支持的型号时，现在可以根据您的要求配置接口属性。您可以将源设备接口映射到目标设备接口。迁移会锁定源设备和目标设备。

支持进行迁移的设备

支持的源设备

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140
- 思科 Firepower 4110
- 思科 Firepower 4120
- 思科 Firepower 4140
- 思科 Firepower 4150
- Cisco Firepower 9300 系列 SM-24
- Cisco Firepower 9300 系列 SM-36
- Cisco Firepower 9300 系列 SM-44

注释 源设备必须为 7.2.x 及更高版本。

支持的目标设备

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140
- Cisco Firepower 4215
- Cisco Firepower 4225
- Cisco Firepower 4245

注释 目标设备必须为 7.4.1 及更高版本。

支持的数据迁移路径

下表列出了可从源 防火墙威胁防御 型号迁移到的受支持目标 防火墙威胁防御 型号。

源型号	目标型号			
	Cisco Secure Firewall 3100 系列	**Cisco Secure Firewall 4200 系列**	**Cisco Secure Firewall 3100 系列中的实例**	**Cisco Secure Firewall 4200 系列中的实例**
Firepower 1100 系列	是	—	—	—
Firepower 2100 系列	是	—	—	—
Firepower 4100 系列	支持	支持	—	—
Firepower 9300 系列	支持	支持	—	—
Firepower 4100 系列中的实例	—	—	支持	支持
Firepower 9300 系列中的实例	—	—	支持	支持

迁移许可证

- 您的智能许可帐户必须具有目标设备的许可证授权。
- 您必须使用智能许可账户注册并注册设备。迁移会将源设备许可证复制到目标设备。

迁移的前提条件

- **一般设备前提条件**
  - 将源设备和目标设备注册到 防火墙管理中心。
  - 确保目标设备是新注册的设备，且无任何配置。
  - 源设备和目标设备必须处于相同状态和模式：
    - 域
    - 防火墙模式：路由或透明
    - 合规模式（CC 或 UCAPL）
    - 管理状态

      设备必须具有相同类型的管理器访问接口（管理接口或数据接口）。
    - 多实例模式或设备模式
  - 确保您具有设备修改权限。
  - 确保源设备上的配置有效且无错误。
  - 迁移期间，两台设备上均不得运行部署、导入或导出任务。源设备可以有待处理的部署。
- **变更管理的前提条件**
  - 确保源设备和目标设备未被变更管理故障单锁定。
  - 确保分配给源设备的共享策略未被变更管理故障单锁定。
- **HA 设备的前提条件**
  - 仅从主用 防火墙管理中心 迁移设备。
- **多实例模式设备前提条件**
  - 确保源设备和目标设备处于多实例模式。
  - 手动迁移机箱配置。在将实例配置迁移到目标实例之前，先创建实例。目标设备必须具有兼容的接口。例如，在目标设备上，必须创建 EtherChannel 接口，并为这些接口创建已标记、未标记、专用或共享接口。
- **带外配置设备的前提条件**
  - 确保确认带外更改，并在 防火墙管理中心 内匹配配置。您无法迁移具有这些配置的设备。要查看带外配置，请执行以下操作：

    1. 选择**设备** > **设备管理**。
    2. 点击设备旁边的编辑图标，然后点击**接口**选项卡。

- **具有管理器访问接口的设备的前提条件**

  确保设备未处于“数据传输”或“管理传输”状态。如果设备处于这些状态，则无法迁移。

  - 数据传输状态：管理器访问接口从数据接口更改为管理接口，但未在设备上部署变更时的设备状态。
  - 管理传输状态：管理器访问接口从管理接口更改为数据接口，但未在设备上部署变更时的设备状态。

- **带有合并管理和诊断接口的设备的前提条件**

  确保目标设备始终处于合并模式。

向导可以迁移哪些配置？

迁移向导会将以下配置从源设备复制到目标设备：

- 许可证
- 接口配置
- 内联集配置
- 路由配置
- DHCP 和 DDNS 配置
- 虚拟路由器配置
- Policies
- 关联的对象和对象覆盖
- 平台设置
- 远程分支机构部署配置

迁移向导会将以下策略配置从源设备复制到目标设备：

- 运行状况策略
- NAT 策略
- QoS 策略
- 远程访问 VPN 策略
- FlexConfig 策略
- 访问控制策略
- 预过滤器策略
- IPS 策略
- DNS 策略

- SSL 策略
- 恶意软件和文件策略
- 身份策略
- 共享策略

迁移向导会将以下路由配置从源设备复制到目标设备：

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- 策略型路由
- Static Route
- 组播路由
- 虚拟路由器

迁移向导会将以下接口从源设备复制到目标设备：

- 物理接口
- 子接口
- Etherchannel 接口
  - 在独立设备上，向导会将 EtherChannel 从源设备复制到目标设备。
  - 对于多实例模式下的设备，必须在机箱上创建 EtherChannel 并将其分配给实例。
- 网桥组接口
- VTI 接口
- VNI 接口
- 环回接口
- 内联接口
- VXLAN 隧道端点 (VTEP) 接口

迁移向导会保留目标设备的设备组。

迁移准则和限制

准则

- **对于多实例模式下的设备：**

  迁移期间，请确保按照下表映射接口：

源设备	目标设备
物理接口	物理接口
EtherChannel 接口	EtherChannel 接口
超级管理员配置的子接口	超级管理员配置的子接口
已标记的接口	已标记的接口
未标记的接口	未标记的接口
共享接口	共享和专用接口
专用接口	专用接口

  不能将超级管理员配置的子接口映射到实例创建的子接口。

- **对于 HA 设备**，您可以迁移：
  - 源 HA 设备到目标 HA 设备。
  - 源 HA 设备到目标独立设备。

- **对于远程分支部署中的设备：**
  - 将源管理器访问接口映射到目标管理器访问接口。
  - 确保源和目标 防火墙管理中心 的管理器访问接口属于相同的 IP 地址类型（静态或 DHCP）。
  - 两个管理器访问接口都必须具有 IPv4 或 IPv6 地址。
  - 如果管理器访问接口具有静态 IP 地址，请确保它们位于同一子网中。

- **对于 Snort：**
  - 如果目标设备使用 Snort 3，迁移后仍使用 Snort 3。
  - 如果源设备和目标设备都使用 Snort 2，迁移后目标设备仍使用 Snort 2。

- **对于使用诊断接口的设备：**

  迁移后，目标设备上仅提供合并的管理接口。

限制

- 迁移向导不迁移以下内容：
  - 站点间 VPN 策略
  - Firepower 2100 系列的 SNMP 设备配置

    在迁移后，您可以使用设备的平台设置来配置 SNMP。
- 一次只能执行一个迁移。
- 迁移后，远程访问 VPN 信任点证书不会注册。
- 对于 HA 设备：
  - 目标设备：不能将独立设备迁移为 HA 设备。
- 不支持群集。
- 对于远程分支部署中的设备：
  - 该向导不支持将单个 WAN 管理器访问数据接口迁移为双 WAN 管理器访问数据接口。

迁移安全 防火墙威胁防御

开始之前

确保您查看 迁移的前提条件，第 4 页 和 迁移准则和限制，第 7 页。

过程

步骤 1 选择**防火墙设备 > 设备管理**。

步骤 2 点击页面右上角的**迁移**。

步骤 3 在**选择源设备和目标设备中**：

a) 从**源设备**下拉列表中，选择一个设备。

b) 从**目标设备**下拉列表中，选择一个设备。

源设备和目标设备可以具有以下标记：

- 路由式：处于路由防火墙模式的设备。
- 透明式：处于透明防火墙模式的设备。
- 容器：处于多实例模式的设备。
- 高可用性：处于高可用性模式的设备。
- 仅分析：由 安全云控制 管理的设备，且 防火墙管理中心 仅接收和显示事件（仅分析 防火墙管理中心）。

如果该设备是 HA 对的一部分，则仅显示 HA 对名称。

步骤 4 点击**下一步 (Next)**。

步骤 5 （仅适用于设备模式下的 Firepower 4100 和 9300 系列设备）在**机箱管理器详细信息**中：

a) 如有需要，选中**跳过机箱管理器**复选框。

b) 在**机箱主机名或 IP 地址**字段中，输入值。

注释

- 验证 防火墙管理中心 可以访问 Cisco Secure Firewall 机箱管理器。
- 确保您为源设备选择了正确的机箱管理器，因为 防火墙管理中心 不会验证您的选择。

c) 点击**验证证书**，以验证机箱管理器的证书。

d) 在**用户名**和**密码**字段中，输入机箱管理器的凭据。

步骤 6 点击**下一步 (Next)**。

步骤 7 在**配置接口**中：

默认情况下，源接口和目标接口使用接口硬件名称进行映射。您必须映射命名接口、逻辑接口以及属于其他接口的接口。所有其他接口的映射不是必需的。向导会根据您提供的接口映射创建逻辑接口。

您不能映射属于 HA 故障转移配置的接口。这些接口会在向导中被禁用。

设备模式下的 Firepower 4100 和 9300 系列设备：

对于这些设备，防火墙管理中心 会从机箱管理器获取接口属性，如速度、双工模式和自动协商。

a) 点击以下选项之一，在目标设备上配置这些接口属性：

- **保留目标设备值**：（默认）保留在目标设备上配置的接口属性。
- **从源设备复制**：从源设备复制接口属性。

  只有当 防火墙管理中心 成功连接到机箱管理器时，此选项才会启用。建议您使用此选项。如果物理接口的速度、双工模式和自动协商值在目标设备中不兼容，则会将其设置为默认值。
- **自定义设备值** - 允许您在目标设备上配置所需接口属性的值。

b) 要从默认映射更改接口映射，请从**映射的接口**下拉列表中选择一个接口。

c) 对于 EtherChannel，您可以配置接口属性，并点击**添加成员接口**以添加成员接口。

EtherChannel 的接口属性根据第一个成员接口的接口属性进行配置。您最多可以添加 16 个成员接口。

Firepower 1100 和 2100 系列设备，以及多实例模式下的 Firepower 4100 和 9300 系列设备：

对于这些设备，您必须将源设备接口映射到目标设备接口。

对于多实例模式下的 Firepower 4100 和 9300 系列设备，您只能执行接口映射，无法配置接口属性（如速度、双工模式、自动协商和 FEC 模式）。

如果要从默认映射更改接口映射，请从**映射的接口**下拉列表中选择接口。

点击**重置**，以配置默认接口映射。例如，向导会将源设备中的 Ethernet1/1 映射到目标设备中的 Ethernet1/1。

接口可以具有以下标记：

- 已标记：机箱上的物理接口。
- 未标记：机箱上具有子接口的物理接口。
- 专用：分配给特定实例且不在多个实例间共享的接口。
- 共享：由多个实例共享的接口。
- 管理器访问：数据接口是管理器访问接口。

如有需要，选中**忽略警告**复选框。

步骤 8 点击**下一步 (Next)**。

步骤 9 点击**提交 (Submit)** 开始迁移。

步骤 10 要查看迁移状态，请单击 **通知** （消息中心），然后单击 **任务** 选项卡。

迁移完成后，会生成**设备型号迁移**报告。您可以在**通知 > 任务**页面中看到此报告的链接。

下一步做什么

迁移成功后，您必须完成以下任务：

- 查看 威胁防御 设备迁移最佳实践 ， 第 10 页 中的建议。
- 验证配置。
- 在设备上部署配置。

如果迁移失败，目标设备会回滚到初始状态。

威胁防御 设备迁移最佳实践

成功迁移后，我们建议您在部署之前执行以下操作：

- 接口的 IP 地址会从源设备复制到目标设备。如果源设备处于运行状态，请更改目标设备接口的 IP 地址。
- 确保使用修改后的 IP 地址来更新 NAT 策略。
- 如果在迁移后将接口速度设置为默认值，请配置接口速度。
- 在目标设备上重新注册设备证书（如有）。
- （可选）配置远程分支机构部署配置。

  如果源或目标设备具有通过数据接口的管理器访问权限，则在迁移后，管理器访问权限将丢失。更新目标设备上的管理器访问配置。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南 或联机帮助中的将管理器访问接口从“管理”更改为“数据 ”主题。
- 如需配置站点间 VPN，请进行相应配置。这些配置不会从源设备迁移。

- 在部署之前查看部署预览。从 **部署 (Deploy)** 下拉菜单中，点击 **高级部署 (Advanced Deploy)**，然后点击设备的 **预览** () 图标。
- 在运行状况监控器中监控设备运行状况（选择 > **运行状况** > **监控器系统** ()）。迁移后，源设备的运行状况策略会成为目标设备的运行状况策略。您还可以为设备配置新的运行状况策略。

  迁移后，由于设备迁移前后的UUID不同，设备监控仪表板可能会暂时显示冗余的彩色线条。这种冗余仅在迁移期间出现。迁移一小时后，仪表板的每个指标将仅显示一行。

美洲总部
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

亚太区总部
CiscoSystems(USA)Pte.Ltd.
Singapore

欧洲总部
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco 在全球拥有 200 多个办事处。相关地址、电话和传真号码可见于
Cisco 位于 www.cisco.com/go/offices 上的网站。

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。