



# Cisco Secure Firewall 迁移工具使用入门

- [关于 Cisco Secure Firewall 迁移工具](#)，第 1 页
- [Cisco Secure Firewall 迁移工具的新功能](#)，第 4 页
- [Cisco Secure Firewall 迁移工具的许可](#)，第 9 页
- [Cisco Secure Firewall 迁移工具的平台要求](#)，第 9 页
- [威胁防御设备的要求和前提条件](#)，第 10 页
- [Check Point 配置支持](#)，第 10 页
- [准则和限制](#)，第 13 页
- [支持的迁移平台](#)，第 16 页
- [支持的迁移目标管理中心](#)，第 17 页
- [支持迁移的软件版本](#)，第 18 页

## 关于 Cisco Secure Firewall 迁移工具

本指南包含有关如何下载 Cisco Secure Firewall 迁移工具和完成迁移的信息。此外，它还提供故障排除提示，以便帮助您解决可能遇到的迁移问题。

本书中包含的迁移程序示例（[迁移示例：Check Point 到 Threat defense 2100](#)）有助于对迁移过程的理解。

Cisco Secure Firewall 迁移工具会将支持的 Check Point 配置转换为支持的 Cisco Secure Firewall Threat Defense 平台。Cisco Secure Firewall 迁移工具允许您将支持的 Check Point 功能和策略自动迁移到威胁防御。您必须手动迁移所有不支持的功能。

Cisco Secure Firewall 迁移工具收集 Check Point 信息、解析相关信息，最后将它推送到 Cisco Secure Firewall Management Center。在解析阶段中，Cisco Secure Firewall 迁移工具会生成**迁移前报告**，其中会列明以下各项：

- 出错的 Check Point 配置 XML 或 JSON 行
- Check Point 会列出 Cisco Secure Firewall 迁移工具无法识别的 Check Point XML 或 JSON 行。报告**迁移前报告**和控制台日志中错误部分下的 XML 或 JSON 配置行；这些配置行会阻止迁移

如果存在解析错误，您可以纠正问题，重新上传新配置，连接到目标设备，将 Check Point 接口映射到威胁防御接口，映射安全区和接口组，然后继续检查和验证您的配置。接下来即可将配置迁移到目标设备。

## 控制台

当您启动 Cisco Secure Firewall 迁移工具时，系统将打开控制台。控制台提供有关 Cisco Secure Firewall 迁移工具中各步骤进度的详细信息。控制台的内容也会写入 Cisco Secure Firewall 迁移工具日志文件。

在打开和运行 Cisco Secure Firewall 迁移工具时，控制台必须保持打开状态。



---

**重要事项** 当您通过关闭运行 Web 界面的浏览器退出 Cisco Secure Firewall 迁移工具时，控制台会继续在后台运行。要完全退出 Cisco Secure Firewall 迁移工具，请按键盘上的 Command 键 + C 退出控制台。

---

## 日志

Cisco Secure Firewall 迁移工具会为每个迁移创建日志。这些日志包含每个迁移步骤中所发生事件的详细信息，如果迁移失败，可以帮助您确定失败的原因。

在以下位置可找到 Cisco Secure Firewall 迁移工具的日志文件：`<migration_tool_folder>\logs`

## 资源

Cisco Secure Firewall 迁移工具会在 **resources** 文件夹中保存一份 **迁移前报告**、**迁移后报告**、**Check Point 配置和日志**。

在以下位置可找到 **resources** 文件夹：`<migration_tool_folder>\resources`


## 未解析文件

可在以下位置找到未解析文件：

`<migration_tool_folder>\resources`

## Cisco Secure Firewall 迁移工具中的搜索

可以搜索 Cisco Secure Firewall 迁移工具中所显示表格中的项目，例如**优化**、**检查和验证**页面上的项目。

要搜索表格的任何列或行中的项目，请点击表格上方的**搜索**（），然后在字段中输入搜索词。Cisco Secure Firewall 迁移工具会筛选表格行，并仅显示包含搜索词的那些项目。

要搜索单列中的项目，请在相应列标题中提供的**搜索**字段中输入搜索词。Cisco Secure Firewall 迁移工具会筛选表格行，并仅显示匹配搜索词的那些项目。

## 端口

在以下 12 个端口之一上运行时，Cisco Secure Firewall 迁移工具支持遥测：端口 8321-8331 和端口 8888。默认情况下，Cisco Secure Firewall 迁移工具使用端口 8888。要更改端口，请更新 *app\_config* 文件中的端口信息。更新后，请确保重新启动 Cisco Secure Firewall 迁移工具，以使端口更改生效。在以下位置可找到 *app\_config* 文件：<migration\_tool\_folder>\app\_config.txt。



---

**注释** 我们建议您使用端口 8321-8331 和端口 8888，因为只有这些端口支持遥测。如果启用思科成功网络，则无法将任何其他端口用于 Cisco Secure Firewall 迁移工具。

---

## 思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，Cisco Secure Firewall 迁移工具与思科云之间会建立安全连接以传输使用情况信息和统计信息。数据流遥测提供一种机制，可从 Cisco Secure Firewall 迁移工具选择感兴趣的数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 通知您在网络中可用来改进产品效果的未使用功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品。

Cisco Secure Firewall 迁移工具将建立并维护该安全连接，使您能够注册思科成功网络。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。

# Cisco Secure Firewall 迁移工具的新功能

版本	支持的功能
6.0	

版本	支持的功能
	<p>本版本包含以下新功能和增强功能</p> <p><b>Cisco Secure Firewall ASA 迁移到 Secure Firewall Threat Defense</b></p> <ul style="list-style-type: none"> <li>现在，您可以将安全防火墙 ASA 上的 WebVPN 配置迁移到威胁防御设备上的零信任访问策略配置。确保选中 <b>选择功能</b> 页面中的 <b>WebVPN</b> 复选框，并查看 <b>优化、查看和验证配置</b> 页面中的新 <b>WebVPN</b> 选项卡。威胁防御设备和目标管理中心必须在 7.4 或更高版本上运行，并且必须将 Snort3 作为检测引擎运行。</li> <li>现在，您可以将简单网络管理协议 (SNMP) 和动态主机配置协议 (DHCP) 配置迁移到威胁防御设备。确保选中 <b>选择功能</b> 页面中的 <b>SNMP</b> 和 <b>DHCP</b> 复选框。如果您在安全防火墙 ASA 上配置了 DHCP，请注意，也可以选择迁移 DHCP 服务器或中继代理和 DDNS 配置。</li> <li>现在，您可以在执行多情景 ASA 设备到单实例威胁防御合并情景迁移时迁移等价多路径 (ECMP) 路由配置。已解析摘要中的 <b>路由</b> 磁贴现在还包括 ECMP 区域，您可以在 <b>优化、查看和验证配置</b> 页面的 <b>路由</b> 选项卡下对其进行验证。</li> <li>现在，您可以将动态隧道从安全防火墙 ASA 的动态虚拟隧道接口 (DVTI) 配置迁移到威胁防御设备。您可以在 <b>Map ASA Interfaces to Security Zones, Interface Groups, and VRFs</b> 页面中进行映射。确保您的 ASA 版本为 9.19 (x) 及更高版本，此功能才适用。</li> </ul> <p><b>FDM 托管设备迁移到 Cisco Secure Firewall Threat Defense</b></p> <ul style="list-style-type: none"> <li>现在，您可以将第 7 层安全策略（包括 SNMP 和 HTTP）以及恶意软件和文件策略配置从 FDM 管理的设备迁移到威胁防御设备。确保目标管理中心版本为 7.4 或更高版本，并且选中 <b>选择功能</b> 页面中的 <b>平台设置</b> 和 <b>文件和恶意软件策略</b> 复选框。</li> </ul> <p><b>Check Point 防火墙迁移到 Cisco Secure Firewall Threat Defense</b></p> <ul style="list-style-type: none"> <li>现在，您可以将 Check Point 防火墙上的站点间 VPN（基于策略）配置迁移到威胁防御设备。请注意，此功能适用于 Check Point R80 或更高版本，以及管理中心和威胁防御版本 6.7 或更高版本。确保在 <b>选择功能</b> 页面中选中 <b>站点间 VPN 隧道</b> 复选框。请注意，由于这是特定于设备的配置，因此如果您选择 <b>不使用 FTD 继续</b>，则迁移工具不会显示这些配置。</li> </ul> <p><b>Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense</b></p> <ul style="list-style-type: none"> <li>现在，您可以在将配置从 Fortinet 防火墙迁移到威胁防御设备时优化应用访问控制列表 (ACL)。使用 <b>优化、查看和验证配置</b> 页面中的 <b>优化 ACL</b> 按钮查看冗余和影子 ACL 列表，并下载优化报告以查看详细的 ACL 信息。</li> </ul>

版本	支持的功能
5.0.1	<p>本版本包含以下新功能和增强功能：</p> <ul style="list-style-type: none"> <li>• Cisco Secure Firewall 迁移工具现在支持将多个透明防火墙模式安全情景从 Cisco Secure Firewall ASA 设备迁移到威胁防御设备。您可以将 Cisco Secure Firewall ASA 设备中的两个或多个透明防火墙模式情景合并到一个透明模式实例，并进行迁移。</li> </ul> <p>在一个或多个情景具有 VPN 配置的 VPN 配置的 ASA 部署中，您只能选择一个要将其 VPN 配置迁移到目标威胁防御设备的情景。在未选择的情景中，仅忽略 VPN 配置，并迁移所有其他配置。</p> <p>有关详细信息，请参阅 <a href="#">选择 ASA 安全情景</a>。</p> <ul style="list-style-type: none"> <li>• 您现在可以使用 Cisco Secure Firewall 迁移工具将站点间和远程访问 VPN 配置从 Fortinet 和 Palo Alto Networks 防火墙迁移到威胁防御。从 <a href="#">选择功能</a> 窗格中，选择要迁移的 VPN 功能。请参阅使用迁移工具将 <a href="#">Palo Alto Networks 防火墙迁移到 Cisco Secure Firewall Threat Defense</a> 和使用 <a href="#">迁移工具</a> 将 <a href="#">Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense</a> 指南中的指定 Cisco Secure Firewall 迁移工具的目标参数部分。</li> <li>• 现在，您可以从 Cisco Secure Firewall ASA 设备中选择一个或多个路由或透明防火墙模式安全情景，并使用 Cisco Secure Firewall 迁移工具执行单情景或多情景迁移。</li> </ul>
5.0	<ul style="list-style-type: none"> <li>• Cisco Secure Firewall 迁移工具现在支持将多个安全情景从 Cisco Secure Firewall ASA 迁移到威胁防御设备。您可以选择从其中一个情景迁移配置，也可以合并所有路由防火墙模式情景中的配置并进行迁移。即将推出对合并多个透明防火墙模式情景的配置的支持。有关详细信息，请参阅 <a href="#">选择 ASA 主要安全情景</a>。</li> <li>• 迁移工具现在利用虚拟路由和转发 (VRF) 功能来复制在多情景 ASA 环境中观察到的隔离流量，这将是新合并配置的一部分。您可以在 <a href="#">已解析摘要</a> 页面的新 <b>VRF</b> 磁贴中检查迁移工具在新 <b>情景</b> 磁贴中检测到的情景数量。此外，迁移工具会在将接口映射到 <a href="#">安全区域和接口组</a> 页面中显示这些 VRF 映射到的接口。</li> <li>• 现在，您可以使用 Cisco Secure Firewall 迁移工具中的新演示模式尝试整个迁移工作流程，并直观地了解实际迁移的情况。有关详细信息，请参阅 <a href="#">使用防火墙迁移工具中的演示模式</a>。</li> <li>• 借助新的增强功能和漏洞修复，Cisco Secure Firewall 迁移工具现在可提供改进、更快的迁移体验，用于将 Palo Alto Networks 防火墙迁移到威胁防御。</li> </ul>

版本	支持的功能
4.0.3	<p>Cisco Secure Firewall 迁移工具 4.0.3 包括漏洞修补和以下新增强功能：</p> <ul style="list-style-type: none"> <li>迁移工具现在提供增强的 <b>应用映射</b> 屏幕，用于将 PAN 配置迁移到威胁防御。有关详细信息，请参阅 <a href="#">使用迁移工具将 Palo Alto Networks 防火墙迁移到 Cisco Secure Firewall Threat Defense 指南中的映射配置与应用</a>。</li> </ul>
4.0.2	<p>Cisco Secure Firewall 迁移工具 4.0.2 包括以下新功能和增强功能：</p> <ul style="list-style-type: none"> <li>Cisco Secure Firewall 迁移工具 4.0.2 引入了内置配置提取器工具，该工具现在显示在 <b>提取配置信息</b> 页面上。这简化了配置提取，并消除了下载提取器工具的任务。请注意，FMT-CP-Config-Extractor 工具不再作为独立应用下载。有关详细信息，请参阅 <a href="#">使用配置提取器导出设备配置</a>。</li> <li>迁移工具现在具有永远在线的遥测功能；但是，您现在可以选择发送有限或广泛的遥测数据。有限的遥测数据包含很少的数据点，而广泛的遥测数据会发送更详细的遥测数据列表。您可以从 <b>Settings &gt; Send Telemetry Data to Cisco?</b>。</li> </ul>
4.0.1	<p>Cisco Secure Firewall 迁移工具 4.0.1 包括以下新功能和增强功能：</p> <ul style="list-style-type: none"> <li>您现在可以将 Check Point R81 配置迁移到 Cisco Secure Firewall Threat Defense。</li> <li>现在，您可以选择在连接到 Check Point 安全网关时添加虚拟系统 ID，以便从多域虚拟系统扩展 (VSX) 部署导出配置。</li> <li>您可以通过手动执行几个命令，从 Check Point VSX 版本 R77 提取配置。有关详细信息，请参阅使用迁移工具将 <i>Check Point</i> 防火墙迁移到威胁防御指南中的<a href="#">使用 FMT-CP-Config-Extractor_v4.0-7965 工具导出设备配置</a>。</li> </ul>
3.0.1	<ul style="list-style-type: none"> <li>对于具有 FirePOWER 服务的 ASA、Check Point、Palo Alto Networks 和 Fortinet，仅支持将 Cisco Secure Firewall 3100 系列作为目标设备。</li> </ul>
3.0	<p>如果目标管理中心是 7.2 或更高版本，Cisco Secure Firewall 迁移工具 3.0 支持从 Check Point 迁移到云交付的防火墙管理中心。</p>

版本	支持的功能
2.5.2	<p>Cisco Secure Firewall 迁移工具 2.5.2 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 Check Point 防火墙的网络功能。</p> <p>ACL 优化支持以下 ACL 类型：</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 影子 ACL - 第一个 ACL 完全镜像第二个 ACL 的配置。</li> </ul> <p>注释        优化仅适用于 ACP 规则操作的 Check Point 。</p> <p>如果目标 管理中心 是 7.1 或更高版本，则 Cisco Secure Firewall 迁移工具 2.5.2 支持边界网关协议 (BGP) 和动态路由对象迁移。</p>
2.2	<ul style="list-style-type: none"> <li>• 提供对 r80 Check Point 操作系统版本的支持</li> <li>• 为 Live Connect 提供支持，以从 Check Point (r80) 设备提取配置。</li> <li>• 您可以将以下受支持的 Check Point 配置元素迁移到 r80 设备的 威胁防御： <ul style="list-style-type: none"> <li>• 接口</li> <li>• 静态路由</li> <li>• 对象</li> <li>• 网络地址转换</li> <li>• 访问控制策略 <ul style="list-style-type: none"> <li>• 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 <b>Any</b>，因为没有路由查找。</li> <li>• 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。</li> </ul> </li> </ul> </li> </ul> <p>注释        路由查找仅限于静态路由和动态路由（PBR 和 NAT 除外），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。</p> <p>注释        基于区域的策略的 IPv6 路由查找不受支持。</p>



版本	支持的功能
2.0	<ul style="list-style-type: none"> <li>• 通过 Cisco Secure Firewall 迁移工具中的新优化功能，可以使用搜索过滤器快速获取迁移结果。</li> <li>• Cisco Secure Firewall 迁移工具允许将以下支持的 Check Point 配置元素迁移到 威胁防御： <ul style="list-style-type: none"> <li>• 接口</li> <li>• 静态路由</li> <li>• 对象</li> <li>• 访问控制策略 <ul style="list-style-type: none"> <li>• 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 <b>Any</b>。</li> <li>• 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。  <p>注释 路由查找仅限于静态路由和动态路由（PBR 和 NAT 除外），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。</p> </li> </ul> </li> <li>• 网络地址转换</li> </ul> </li> <li>• 支持 Check Point 操作系统版本 r75、r76、r77、r77.10、r77.20 和 r77.30。</li> </ul>

## Cisco Secure Firewall 迁移工具的许可

Cisco Secure Firewall 迁移工具应用是免费的，不需要许可证。但是，管理中心 必须具有相关 威胁防御 功能所需的许可证，才能成功注册 威胁防御 并向其部署策略。

## Cisco Secure Firewall 迁移工具的平台要求

Cisco Secure Firewall 迁移工具对基础设施和平台的要求如下：

- 运行 Microsoft Windows 10 64 位操作系统或者 macOS 10.13 或更高版本
- 使用 Google Chrome 作为系统默认浏览器
- (Windows) “电源和睡眠”中的“睡眠”设置配置为“从不让 PC 进入睡眠”，以便在大型迁移推送时系统不会进入睡眠状态
- (macOS) 配置了“节能模式”设置，以便在大型迁移推送时计算机和硬盘不会进入睡眠状态

## 威胁防御设备的要求和前提条件

当您迁移到管理中心时，它可能已添加目标威胁防御设备，也可能未添加。您可以将共享策略迁移到管理中心，以便将来部署到威胁防御设备。要将设备特定的策略迁移到威胁防御，必须将其添加到管理中心。当您计划将 Check Point 配置迁移到威胁防御时，请考虑以下要求和先决条件：

- 目标威胁防御设备必须向管理中心注册。
- 威胁防御设备可以是独立设备或容器实例。它不能是集群或高可用性配置的一部分。
  - 目标本地威胁防御设备必须至少具有与 Check Point 相同数量的已使用物理数据或端口通道接口或子接口（不包括“管理专用”接口）；否则，必须在目标威胁防御设备上添加所需类型的接口。子接口由 Cisco Secure Firewall 迁移工具根据物理或端口通道映射创建。
  - 如果目标威胁防御设备是容器实例，则其使用的物理接口、物理子接口、端口通道接口和端口通道子接口（不包括“管理专用”）的数量必须至少与 Check Point 数量相同；否则，您必须在目标威胁防御设备上添加所需的接口类型。



### 注释

- Cisco Secure Firewall 迁移工具不创建子接口，仅允许接口映射。
- 它允许不同接口类型之间的映射，例如：物理接口可以映射到端口通道接口。

## Check Point 配置支持

### 支持的 Check Point 配置

- 接口（物理接口、VLAN 接口和绑定接口）
- 网络对象和组：Cisco Secure Firewall 迁移工具支持将所有 Check Point 网络对象迁移到威胁防御
- 服务对象
- 网络地址转换
- IPv6 转换支持（接口、静态路由和对象）并且 IPv6 基于区域的 ACL 除外
- 全局应用的访问规则，并且支持将全局 ACL 转换为基于区域的 ACL
- 静态路由，但将范围配置为本地且使用逻辑接口作为无下一跳 IP 地址的静态路由的出口接口的路由除外
- 具有其他日志记录类型的 ACL

- 适用于 Check Point R80 及更高版本的基于策略的站点间 VPN：基于 IPv4 和预共享密钥 (PSK) 的身份验证。我们建议您使用 **实时连接** 选项迁移 VPN 配置。



**注释** 对于在 Check Point 中配置的在 Check Point 中具有相应 NAT 规则的 ACE，Cisco Secure Firewall 迁移工具不会将实际 IP 地址与相应迁移的 ACE 规则中的已转换 IP 地址进行映射。由于缺少 ACE 规则与 NAT 规则的参考信息，Cisco Secure Firewall 迁移工具不会映射 IP 地址。因此，在验证管理中心上迁移的 ACE 和 NAT 配置期间，您必须验证并手动更改与威胁防御数据包流对应的 ACE 规则。



**注释** 虽然 Cisco Secure Firewall 迁移工具不会迁移服务对象（配置了源和目标，以及具有在对象组中调用的同一类型对象的端口组合），但已迁移的参考 ACL 规则具有完整功能。

有关不受支持的检查点配置的详细信息，请参阅[不受支持的 Check Point 配置](#)。

### 部分支持的 Check Point 配置

Cisco Secure Firewall 迁移工具部分支持以下用于迁移的 Check Point 配置。其中一些配置包括含高级选项的规则，可在不使用这些选项的情况下进行迁移。如果管理中心支持这些高级选项，您可以在迁移完成后手动配置它们。

- 带有 rank 和 ping 参数的静态路由会被部分迁移。
- 具有模式、XOR、活动备份、轮询类型的绑定接口会通过 Cisco Secure Firewall 迁移工具部分迁移到管理中心中的 LACP 类型。
- 别名接口配置是父接口（例如物理接口或绑定接口）的一部分，忽略的和父接口属性的别名接口配置会按原样迁移。
- 排除类型的网络对象组通过 ACL 来支持，以保持含义完整。
- 带有 Add 日志记录类型的 ACL 和带有时间范围的 ACL。

### 不受支持的 Check Point 配置

Cisco Secure Firewall 迁移工具不支持对以下 Check Point 配置。如果这些配置在管理中心中受支持，您可以在迁移完成之后手动配置它们。

- 别名、桥接、6IN4 隧道、环回和 PPPoE 接口
- 网络对象和组：
  - UTM-1 Edge 网关
  - Check Point 主机
  - 网关集群
  - 外部托管网关或主机

- 开放安全扩展 (OSE) 设备
- 逻辑服务器
- 动态对象
- VoIP 域
- 区
- CP 安全网关
- CP 管理服务器
- 排除类型的网络对象组
- 服务对象：
  - RPC
  - DCE-RPC
  - 复合 TCP
  - GTP
  - 其他 Check Point 特定服务对象
- ACL 策略且具有：
  - 不受支持的 ACE 操作类型（客户端身份验证、会话身份验证、用户身份验证和其他自定义身份验证类型）使用 Allow 操作类型进行迁移，但处于禁用状态
  - 基于身份的 ACL 策略
  - 包含 IPv6 路由查找的基于区域的策略
  - 基于用户的访问控制策略规则
  - 全局多域系统规则无法迁移



---

**注释** 无法导出 Check Point 多域部署中全局多域系统的配置。因此，只能导出和迁移与特定 CMA 相关的配置。

---

- 带有不受支持 ICMP 类型和代码的对象
- 基于隧道协议的访问控制策略规则
- 隐式 ACL 规则
- 带否定参数的 ACE

- 当选择了基于区域的 ACE 且具有范围值大于 100 的范围对象时，ACE 的区域会被迁移并被标记为 **Any**，且没有附加到 ACE 名称和响应注释上的查找功能
- 选择基于区域的 ACE 时，带有 IPv6 地址的 ACE 区域会被标记为 **Any**，并且该 ACE 不受支持并带有相应的注释。

### 不受支持的 NAT 规则

Cisco Secure Firewall 迁移工具不支持以下 NAT 规则：

- 隐藏在网关后的自动 NAT 规则
- 使用 Check Point 安全网关的手动 NAT 规则。
- 包含具有双类型 IP 地址的网络对象的手动 NAT 规则
- 手动 NAT 规则，包含其继承对象具有 IPv6 配置的对象组
- 包含服务组的手动 NAT 规则
- IPv6 NAT 规则

### 不受支持的静态路由

- 在 `netstat -rnv` 中未找到出口接口时的静态路由
- 将逻辑网关作为送出接口的静态路由
- ECMP 类型的静态路由
- 具有本地范围属性作为送出接口的静态路由

## 准则和限制

在转换期间，Cisco Secure Firewall 迁移工具会为所有支持的对象和规则创建一对一映射，而不管它们是否用于规则或策略。但是，Cisco Secure Firewall 迁移工具提供优化功能，允许您在迁移中排除未使用的对象（任何 ACL 中未引用的对象）。

Cisco Secure Firewall 迁移工具处理指定的不受支持的对象和规则：

- 不受支持的对象和路由不会被迁移。
- 不受支持的 ACL 规则将作为禁用的规则迁移到管理中心。

### Check Point 配置限制

源 Check Point 配置的迁移存在以下限制：

- 系统配置未迁移。
- 只有 Check Point (r80) 和更高版本才支持防火墙的实时连接。

- 所有明确的安全策略（适用于 r77.30 及更低版本的 Security\_Policy.xml 中以及适用于 r80 及更高版本的安全策略文件）都会被迁移到管理中心上的 ACP。Check Point Smart 控制板上的规则不会迁移，因为隐式规则不是导出配置的一部分。



#### 注释

- 对于 Check Point (r80) 及更高版本，如果 L4 安全更新策略附加了单独的应用层策略，则 Cisco Secure Firewall 迁移工具会将其作为 **不受支持** 进行迁移。此外，在此类情况下，将有两个包含 ACE 配置的文件：一个用于安全层，另一个用于应用层。在配置压缩文件的 *index.json* 中，Cisco Secure Firewall 迁移工具会根据接入层中可用的优先级信息进行迁移。
- 对于包含多域部署设置、全局策略以及客户管理加载项 (CMA) 特定策略的 Check Point 版本 r80 及更高版本，Cisco Secure Firewall 迁移工具迁移 Check Point 配置的顺序将与源配置中的顺序略有不同。此外，在此类情况下，将有两个包含 ACE 配置的文件：一个用于全局策略，另一个用于 CMA 策略。在域层下配置的 ACE 将作为 **不受支持** 进行迁移。
- 在提取的配置中，ACE 规则的顺序定义不完整，该规则是为在多域系统中将操作作为域层的 CMA 配置的。因此，如果您在源配置中将全局策略附加到特定 CMA 策略，请验证提取的配置中的规则编号索引，以便确保其顺序正确。

- 某些 Check Point 配置（例如动态路由和 VPN 到威胁防御）无法使用 Cisco Secure Firewall 迁移工具进行迁移。手动迁移这些配置。
- Check Point 网桥、隧道接口和管理中心的别名接口无法迁移。
- 管理中心不支持嵌套服务对象组或端口组。在转换过程中，Cisco Secure Firewall 迁移工具会扩展引用的嵌套对象组或端口组的内容。
- Cisco Secure Firewall 迁移工具会将服务对象或组与在同一对象内配置的源和目标端口进行拆分。对此类访问控制规则的引用将转换为具有完全相同含义的管理中心规则。

### Check Point 迁移指南

Check Point 日志选项的迁移遵循威胁防御的最佳实践。根据源 Check Point 配置启用或禁用规则的日志选项。对于使用 **丢弃** 或 **拒绝** 操作的规则，Cisco Secure Firewall 迁移工具会在连接开始时配置日志记录。如果操作是 **允许**，则 Cisco Secure Firewall 迁移工具会在连接结束时配置日志记录。

### 对象迁移准则

服务对象（在威胁防御中称为端口对象）具有不同的对象配置准则。例如，一个或多个对象在 Check Point 中可具有相同的名称。一个对象的名称为小写，另一个对象的名称为大写。但是，每个对象都必须具有唯一的名称，无论在威胁防御中如何。Cisco Secure Firewall 迁移工具会分析所有 Check Point 对象，并通过以下方式之一处理它们向威胁防御的迁移：

- 每个 Check Point 对象都有唯一的名称和配置。Cisco Secure Firewall 迁移工具无需更改即可成功迁移对象。
- Check Point 服务对象的名称包含一个或多个管理中心不支持的特殊字符。Cisco Secure Firewall 迁移工具会使用 “\_” 字符来重命名对象名称中的特殊字符，以便满足管理中心对象命名条件。
- Check Point 服务对象与管理中心中的现有对象具有相同的名称和配置。Cisco Secure Firewall 迁移工具将管理中心对象重新用于威胁防御配置，并且不会迁移 Check Point 对象。
- Check Point 服务对象与管理中心中的现有对象具有相同的名称，但具有不同的配置。Cisco Secure Firewall 迁移工具会报告对象冲突，并允许您通过向 Check Point 服务对象的名称添加用于迁移的唯一后缀来解决冲突。
- 多个 Check Point 服务对象具有相同的名称，但大小写不同。Cisco Secure Firewall 迁移工具会重命名此类对象，以便满足威胁防御对象命名条件。

### 适用于 威胁防御设备的准则和限制

当您计划将 Check Point 配置迁移到 威胁防御时，请考虑以下准则和限制：

- 如果威胁防御上有任何现有的设备特定配置（例如路由、接口等），则在推送迁移期间，Cisco Secure Firewall 迁移工具会自动清除设备并从 Check Point 配置执行覆盖。



---

**注释** 为防止设备（目标威胁防御）配置数据意外丢失，我们建议您在迁移之前手动清理设备。

---

在迁移期间，Cisco Secure Firewall 迁移工具会重置接口配置。如果在策略中使用这些接口，则 Cisco Secure Firewall 迁移工具无法重置它们，因此迁移会失败。

- Cisco Secure Firewall 迁移工具可以根据 Check Point 配置在 威胁防御 设备的本地实例上创建子接口。在开始迁移之前，在目标威胁防御设备上手动创建接口和端口通道接口。例如，如果已为您的 Check Point 配置分配以下接口和端口通道，则在迁移之前，必须在目标 威胁防御 设备上创建它们：
  - 五个物理接口
  - 五个端口通道
  - 两个管理专用接口



---

**注释** 对于 威胁防御 设备的容器实例，Cisco Secure Firewall 迁移工具不创建子接口，仅允许接口映射。

---

## 支持的迁移平台

以下 Check Point 和 威胁防御 平台支持通过 Cisco Secure Firewall 迁移工具进行迁移。有关支持的 威胁防御 平台的更多信息，请参阅 [Cisco Secure Firewall 兼容性指南](#)。



---

**注释** Cisco Secure Firewall 迁移工具仅支持将单机模式或分布式 Check Point 配置迁移到独立 威胁防御 设备。

---

### 支持的目标 威胁防御 平台

您可以使用 Cisco Secure Firewall 迁移工具将源 Check Point 配置迁移到 威胁防御 平台的以下独立实例或容器实例：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Cisco Secure Firewall 4200 系列
- Firepower 9300 系列包括：
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware 上的威胁防御，使用 VMware ESXi、VMware vSphere Web 客户端或 vSphere 独立客户端部署
- Microsoft Azure 云或 AWS 云上的 Threat Defense Virtual



---

**注释**

- 有关 Azure 中 threat defense virtual 的前提条件和预先配置，请参阅 [Cisco Secure Firewall Threat Defense Virtual](#) 和 [Azure 入门](#)。
- 有关 AWS 云中 threat defense virtual 的必备条件和预先配置，请参阅 [Threat Defense Virtual 前提条件](#)。

---



对于每一个这些环境，Cisco Secure Firewall 迁移工具在按照要求进行预先配置后，都需要网络连接才能连接到 Microsoft Azure 或 AWS 云中的 管理中心，然后再将配置迁移到云中的 管理中心。



**注释** 要成功迁移，必须在使用 Cisco Secure Firewall 迁移工具之前完成 管理中心 或威胁防御虚拟的预先配置前提条件。



**注释** Cisco Secure Firewall 迁移工具需要与云中托管的任何设备建立网络连接，方可提取源配置 (CP (r80) Live Connect) 或将手动上传的配置迁移到云中的 管理中心。因此，作为前提条件，在使用 Cisco Secure Firewall 迁移工具之前需要预先配置 IP 网络连接。

## 支持的迁移目标管理中心

Cisco Secure Firewall 迁移工具支持迁移到管理中心托管的威胁防御设备以及云交付的防火墙管理中心。

### 管理中心

管理中心是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。您可以使用本地和虚拟管理中心作为迁移的目标管理中心。

管理中心应满足以下迁移准则：

- 管理中心软件版本支持迁移，如 [支持迁移的软件版本](#)，第 18 页中所述。
- 支持 Check Point 迁移的 管理中心 软件版本为 6.2.3.3 及更高版本。
- 您已获取并安装 威胁防御 的智能许可证，包括您计划从 Check Point 接口迁移的所有功能，如下所述：
  - Cisco.com 上的 [思科智能账户](#) “入门指南” 部分。
  - [在思科智能软件管理器中注册防火墙管理中心](#)。
  - [许可防火墙系统](#)
  - 您已为 REST API 启用 管理中心。

在 管理中心 web 接口，导航至 **系统 > 配置 > Rest API 首选项 > 启用 Rest API** 并选中 **启用 Rest API** 复选框。



**重要事项** 您需要在管理中心中拥有管理员用户角色，才能启用 REST API。有关管理中心用户角色的详细信息，请参阅 [用户角色](#)。

### 云交付的防火墙管理中心

云交付的防火墙管理中心是一个用于威胁防御设备的管理平台，它通过思科防御协调器 (CDO) 交付。云交付的防火墙管理中心提供了许多与管理中心相同的功能。

您可以从 CDO 访问云交付的防火墙管理中心。CDO 通过安全设备连接器 (SDC) 连接到云交付的防火墙管理中心。有关云交付的防火墙管理中心的更多信息，请参阅 [使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 设备](#)。

Cisco Secure Firewall 迁移工具支持将云交付的防火墙管理中心作为迁移的目标管理中心。要选择将云交付的防火墙管理中心作为迁移的目标管理中心，则需要添加 CDO 区域并从 CDO 门户生成 API 令牌。

### CDO 区域

CDO 可用于三个不同的区域中，并且可以使用 URL 扩展名来标识这些区域。

表 1: CDO 区域和 URL

地区	CDO URL
欧洲地区	<a href="https://defenseorchestrator.eu/">https://defenseorchestrator.eu/</a>
美国地区	<a href="https://defenseorchestrator.com/">https://defenseorchestrator.com/</a>
总裁	<a href="https://www.apj.cdo.cisco.com/">https://www.apj.cdo.cisco.com/</a>

## 支持迁移的软件版本

以下是支持迁移的 Cisco Secure Firewall 迁移工具、Check Point 和 威胁防御 版本：

### 支持的 Cisco Secure Firewall 迁移工具版本

software.cisco.com 上发布的版本是我们的工程和支持组织正式支持的版本。我们强烈建议您从 [software.cisco.com](https://software.cisco.com) 下载最新版本的 Cisco Secure Firewall 迁移工具。

### 支持的 Check Point 版本

Cisco Secure Firewall 迁移工具支持迁移到运行 Check Point 操作系统版本 r75-r77.30 和 r80-r80.40 的威胁防御。在 **选择源 (Select Source)** 页面中选择相应的 Check Point 版本。

Cisco Secure Firewall 迁移工具支持从 Check Point 平台 Gaia 和 Virtual System Extension (VSX) 迁移。

### 源 Check Point 防火墙配置支持的 管理中心 版本

对于 Check Point 防火墙，Cisco Secure Firewall 迁移工具支持迁移到运行 6.2.3.3 或更高版本的 管理中心 所管理的 威胁防御 设备。



---

**注释** 当前不支持迁移到 6.7 威胁防御 设备。因此，如果设备配置了用于 管理中心 访问的数据接口，则迁移可能会失败。

---

### 支持的 威胁防御 版本

Cisco Secure Firewall 迁移工具建议迁移到正在运行 威胁防御 版本 6.5 及更高版本的设备。

有关思科防火墙软件和硬件兼容性的详细信息（包括 威胁防御 的操作系统和托管环境要求），请参阅 [思科防火墙兼容性指南](#)。



## 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。