



## 利用迁移工具将 **Check Point** 防火墙迁移到 **Cisco Secure Firewall Threat Defense**

首次发布日期: 2022 年 11 月 17 日

上次修改日期: 2024 年 4 月 23 日

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. 保留所有权利。



## 目录

---

### 第 1 章

<b>Cisco Secure Firewall 迁移工具使用入门</b>	<b>1</b>
关于 Cisco Secure Firewall 迁移工具	1
Cisco Secure Firewall 迁移工具的新功能	4
Cisco Secure Firewall 迁移工具的许可	9
Cisco Secure Firewall 迁移工具的平台要求	9
威胁防御设备的要求和前提条件	10
Check Point 配置支持	10
准则和限制	13
支持的迁移平台	16
支持的迁移目标管理中心	17
支持迁移的软件版本	18

---

### 第 2 章

<b>Check Point 到威胁防御迁移工作流程</b>	<b>21</b>
端到端程序	21
迁移的前提条件	23
从 Cisco.com 下载 Cisco Secure Firewall 迁移工具	23
导出 Check Point 配置文件	24
导出 Check Point r77 配置文件	24
运行迁移	27
启动 Cisco Secure Firewall 迁移工具	27
在 Cisco Secure Firewall 迁移工具中使用演示模式	29
导出 Check Point r80 配置文件	30
使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取	30
导出 Check Point r80 配置文件的程序	37

提取其他配置文件	40
上传 Check Point 配置文件	41
为 Cisco Secure Firewall 迁移工具指定目标参数	41
查看迁移前报告	44
将 Check Point 防火墙 配置与 威胁防御 接口映射	45
将 Check Point 接口映射到安全区 和 接口组	46
优化, 检查和验证配置	47
将迁移的配置推送到 管理中心	51
查看 Check Point 的迁移后报告并完成迁移	52
卸载 Cisco Secure Firewall 迁移工具	52
迁移示例: Check Point 到 Threat Defense 2100	53
维护前窗口任务	53
维护窗口任务	54

---

第 3 章	思科成功网络 - 遥测数据	55
	思科成功网络 - 遥测数据	55

---

第 4 章	排除迁移问题	65
	Cisco Secure Firewall 迁移工具的故障排除	65
	用于排除故障的日志和其他文件	66
	Check Point 文件上传失败故障排除	66
	Check Point 故障排除示例: 找不到对象组的成员 (仅限 r75 - r77.30)	67
	Live Connect 的 Check Point (r80) 故障排除示例	67

---

第 5 章	Cisco Secure Firewall 迁移工具常见问题	71
	Cisco Secure Firewall 迁移工具常见问题解答	71



# 第 1 章

## 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<a href="#">使用迁移工具将 Check Point 防火墙迁移到威胁防御指南中的使用 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](#)。







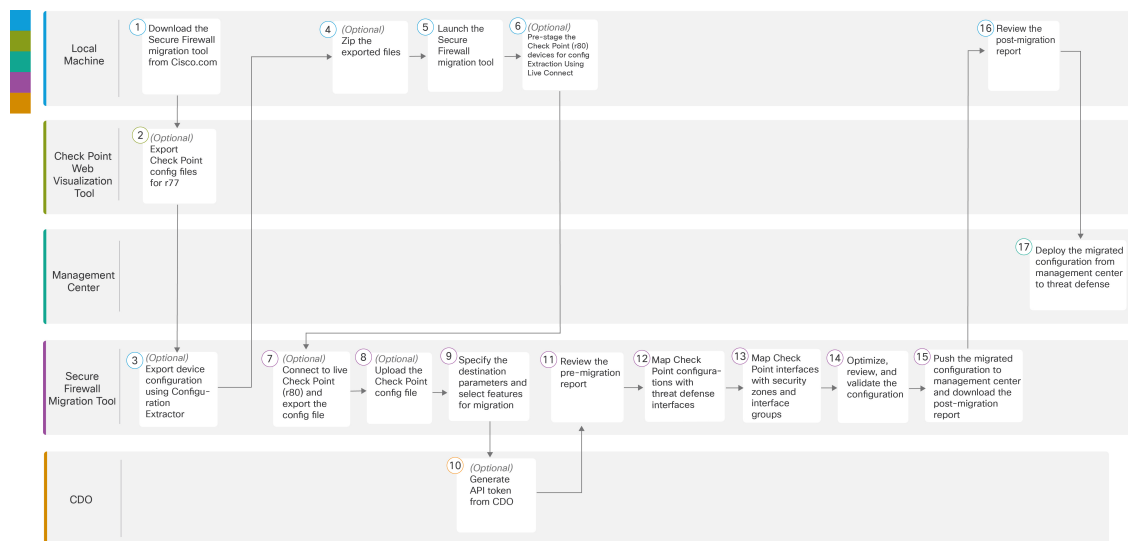
## 第 2 章

# Check Point 到威胁防御迁移工作流程

- 端到端程序，第 21 页
- 迁移的前提条件，第 23 页
- 运行迁移，第 27 页
- 卸载 Cisco Secure Firewall 迁移工具，第 52 页
- 迁移示例：Check Point 到 Threat Defense 2100，第 53 页

## 端到端程序

以下流程图说明了使用 Cisco Secure Firewall 迁移工具将 Check Point 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 <a href="#">Cisco.com</a> 下载 Cisco Secure Firewall 迁移工具。

	工作空间	步骤
2	Check Point Web 可视化工具	(可选) 导出 r77 的 Check Point 配置文件: 要导出 r77 的 Check Point 配置文件, 请参阅 <a href="#">导出 Check Point r77 配置文件</a> , 第 24 页。如果要使用 Cisco Secure Firewall 迁移工具的实时连接功能导出 r80 的配置文件, 请跳至步骤 5。
3	本地计算机	在本地计算机上启动 Cisco Secure Firewall 迁移工具, 然后根据您的要求在 <a href="#">源防火墙供应商</a> 下拉列表中选择 <b>Check Point (r75 - r77)</b> 或 <b>Check Point (r80 - r81)</b> 。有关详细信息, 请参阅 <a href="#">启动 Cisco Secure Firewall 迁移工具</a> 。
4	Cisco Secure Firewall 迁移工具	(可选) 从 Check Point (r75 - r77) 导出设备配置: 要使用 <a href="#">配置提取器</a> 通过安全网连接导出 r77 的设备配置, 请参阅 <a href="#">使用配置提取器导出设备配置</a> , 第 25 页。
5	本地计算机	(可选) 压缩导出的文件: 选择 r77 的所有导出配置文件, 并将其压缩为 zip 文件。有关详细步骤, 请参阅 <a href="#">压缩导出的文件</a> 。
6	本地计算机	预先配置 Check Point (r80) 设备以配置提取: 在防火墙迁移工具上使用 Live Connect 之前, 必须在 Check Point (r80) 设备上配置凭证。有关在 Check Point (r80) 设备上预先配置的凭证, 请参阅 <a href="#">使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取</a> 。仅当您计划迁移 r80 设备的配置文件时, 才需要执行此步骤。如果要从 r77 设备迁移配置, 请跳至步骤 8。
7	Cisco Secure Firewall 迁移工具	(可选) 连接到实时 Check Point (r80) 并导出配置文件: 要使用实时连接功能导出适用于 r80 的 Check Point 配置文件, 请参阅 <a href="#">导出 Check Point r80 配置文件的程序</a> 。
8	Cisco Secure Firewall 迁移工具	(可选) 上传 Check Point 配置文件: 有关上传 Check Point 配置文件的详细步骤, 请参阅 <a href="#">上传 Check Point 配置文件</a> 。
9	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 <a href="#">为 Cisco Secure Firewall 迁移工具指定目标参数</a> 。
10	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 <a href="#">为 Cisco Secure Firewall 迁移工具指定目标参数</a> 。
11	Cisco Secure Firewall 迁移工具	导航到下载预迁移前报告的位置并查看报告。有关详细步骤, 请参阅 <a href="#">查看迁移前报告</a> 。
12	Cisco Secure Firewall 迁移工具	Cisco Secure Firewall 迁移工具允许您将 Check Point 配置与威胁防御接口进行映射。有关详细步骤, 请参阅 <a href="#">将 Check Point 防火墙配置与威胁防御接口映射</a> 。

	工作空间	步骤
13	Cisco Secure Firewall 迁移工具	为确保正确地迁移 Check Point 配置，您需要将 Check Point 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 <a href="#">将 Check Point 接口映射到安全区和接口组</a> 。
14	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 <a href="#">优化、检查和验证配置</a> 。
15	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 <a href="#">将迁移的配置推送到管理中心</a> 。
16	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 <a href="#">查看 Check Point 的迁移后报告并完成迁移</a> 。
17	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 <a href="#">查看 Check Point 的迁移后报告并完成迁移</a> 。

## 迁移的前提条件

在迁移 Check Point 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。

下一步做什么

[导出 Check Point 配置文件](#)

## 导出 Check Point 配置文件

您可以为以下导出 Check Point 配置文件：

- [导出 Check Point r77 配置文件](#)
- [导出 Check Point r80 配置文件](#)

### 导出 Check Point r77 配置文件

要导出 Check Point r80 配置文件，请执行以下操作：

- [使用 Check Point Web 可视化工具 \(WVT\) 导出配置](#)
- [使用配置提取器导出设备配置，第 25 页](#)
- [压缩导出的文件](#)

#### 使用 Check Point Web 可视化工具 (WVT) 导出配置

**步骤 1** 在有权访问 Check Point 管理服务器的工作站上打开命令提示符。

**步骤 2** 从适用于 Check Point 防火墙版本的 [Check Point 门户](#) 下载 WVT。

**步骤 3** 解压缩 WVT zip 文件。

**步骤 4** 在提取 Check Point WVT 工具的同根文件夹下创建新的子文件夹。

**步骤 5** 将命令提示符中的目录更改为存储 WVT 的目录，并执行以下命令：

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file] [-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go] [-w Web_Visualization_Tool_installation_directory]
```

例如，

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1 -u admin -p admin123 -o Outputs
```

执行以下命令时，*Outputs* 目录中总共创建七个文件：

命令	说明
C:\Web_Visualisation_Tool	WVT 工具的根目录。
172.16.0.1	Check Point 管理服务器的 IP 地址。
admin	Check Point 管理服务器用户名。
Admin123	Check Point 管理服务器密码。
Outputs	存储输出文件的相对路径。

**注释** 安全策略和 NAT 策略文件的名称必须分别为 Security\_Policy.xml 和 NAT\_Policy.xml。如果文件名不同，请手动重命名。

如果有多个安全和 NAT 策略文件，请确保仅选择并保留要迁移的 Check Point 设备的 Security\_Policy.xml 和 NAT\_Policy.xml 文件。

---

## 下一步做什么

[使用配置提取器导出设备配置](#)

### 使用配置提取器导出设备配置

---

**步骤 1** 在 **选择源配置** 页面中，选择 **检查点 (r75 - r77)**，然后点击 **开始迁移**。

**步骤 2** 在 **配置提取器** 窗格上，点击 **连接** 到要使用 Cisco Secure Firewall 迁移工具迁移策略的 Check Point Security Gateway。

要进行连接，您需要以下信息：

- a) IP 地址
- b) 端口
- c) 管理用户名
- d) Admin 密码
- e) 专家密码
- f) (可选) 虚拟 ID 号

**步骤 3** 等待，直到您看到 networking.txt 文件下载到本地计算机。

以下命令由配置提取器在后台执行，并作为 networking.txt 文件下载：

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

例如，172.16.0.1 是要迁移策略的 Check Point Firewall Gateway 的 IP 地址。

**步骤 4** 如果您尝试从拥有虚拟 ID 的 Check Point VSX (Virtual System eXtension) 版本 R77 导出配置，背景中将执行以下命令：

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- 设置虚拟系统 <vsid>  
提示        **vsid** 表示虚拟系统 ID。
- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

**步骤 5** 将 .txt 文件移动到 Outputs 文件夹。

---

下一步做什么

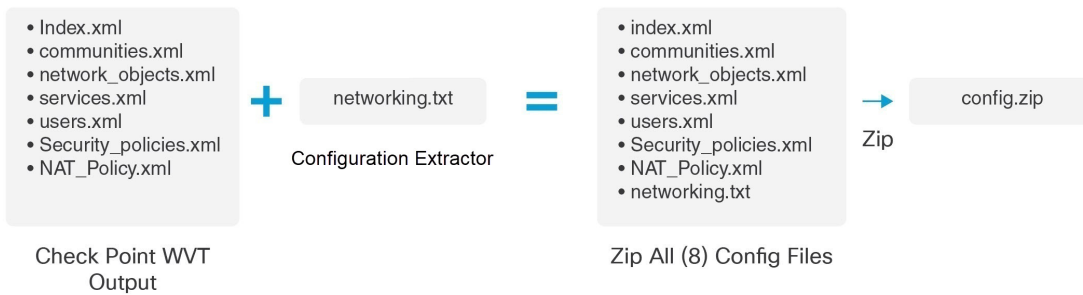
[压缩导出的文件](#)

## 压缩导出的文件

---

选择所有八个文件（Web 可视化工具 (WVT) 中的七个文件和配置提取器中的一个 .txt 文件）并将其压缩为 Zip 文件。

**注释**        在压缩要迁移的文件之前，请确保 Security\_Policy.xml 和 NAT\_Policy.xml 文件适用于要迁移到威胁防御的 Check Point 设备。



注释 不支持 .tar 或其他压缩文件类型。

下一步做什么

[上传 Check Point 配置文件](#)

## 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 [上传 Check Point 配置文件](#)。



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，第 17 页部分中的要求。
- 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：

- 如果已将 Check Point 配置导出到您的计算机，请继续执行[上传 Check Point 配置文件](#)。
- 如果必须使用 Cisco Secure Firewall 迁移工具从 Check Point (r77) 提取信息，请继续执行[导出 Check Point r77 配置文件](#)。
- 如果必须使用 Cisco Secure Firewall 迁移工具从 Check Point (r80) 提取信息，请继续执行[导出 Check Point r80 配置文件](#)。

## 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。

---

## 导出 Check Point r80 配置文件



**注释** 只有 Cisco Secure Firewall 迁移工具上的 Live Connect 功能支持导出 Check Point r80 配置。

要在 Check Point 设备上配置迁移所需的凭证并导出 Check Point 配置文件，请执行以下操作：

- 使用 [Live Connect 预先配置 Check Point \(r80\) 设备以进行配置提取](#)
- [导出 Check Point r80 配置文件的程序](#)

### 使用 Live Connect 预先配置 Check Point (r80) 设备以进行配置提取

迁移前，您可以使用以下任一步骤在 Check Point (r80) 设备上配置凭证：

- [从分布式 Check Point 部署导出](#) - 当您有独立的 Check Point 安全网关和 Check Point 安全管理器时。
- [从独立 Check Point 部署导出](#) - 当您的 Check Point 安全网关和 Check Point 安全管理器作为一个设备时。
- [从多域 Check Point 部署导出](#) - 当您有具备多域部署设置的 Check Point 安全网关和 Check Point 安全管理器时。

#### 从分布式 Check Point 部署导出

必须在使用 Cisco Secure Firewall 迁移工具上的 Live Connect 之前在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在分布式 Check Point 部署上预先配置凭证的程序包括以下步骤：

**步骤 1** 在 Gaia Console Check Point 安全网关上创建以下内容：

- 在 Web 浏览器中，通过 HTTPS 会话打开 Check Point Gaia Console 应用以连接到 Check Point 安全网关。
- 导航至 **用户管理 (User Management)** 选项卡，然后选择 **用户 (Users) > 添加 (Add)**。
- 在 **添加用户** 窗口中，使用以下详细信息创建新的用户名和密码：
  - 从 **Shell** 下拉列表中，选择 `/etc/cli.sh`。
  - 从可用角色中，选择 `adminRole`。
  - 保留其余字段的默认值。
  - 点击 **确定 (Ok)**。
- 通过 SSH 连接到 Check Point 安全网关，并使用以下命令创建新密码：
 

```
set expert-password <password>
```

- 注释
- 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
  - 您需要在连接至 **Check Point 安全网关** 页面上提供这些凭证，如 [步骤 3](#) 所示。

配置专家密码后，即完成为 Check Point r80 网关预先配置凭证的程序。

有关详细信息，请参阅 [图 3: 连接到 Check Point 安全网关](#)。

**步骤 2** 在 r80 的 Check Point 安全管理器上创建用户名和密码：

a) 在 SmartConsole 应用上，执行以下步骤：

1. 登录 Check Point 安全管理器。
2. 导航至 **管理和设置 > 权限和管理员 > 管理员**。
3. 点击 \* 创建新的用户名和密码，然后执行以下步骤：
  - 选择身份验证方式作为 **Check Point 密码**。
  - 点击 **设置新密码 (Set New Password)** 以设置新密码。  
注释 切勿选中用户下次登录时必须更改密码复选框。
  - 选择权限配置文件作为 **超级用户**。
  - 选择到期为 **从不**。
4. 点击 **发布 (Publish)** 在 Check Point SmartConsole 应用上保存配置更改。

b) 在 Check Point 安全管理器的 Gaia Console 上，执行以下步骤：

注释 确保您现在创建的用户名和密码与 [步骤 2a](#) 中在 SmartConsole 应用上创建的用户名和密码相同。

1. 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全管理器。
2. 导航至 **用户管理** 选项卡，然后选择 **用户 > 添加**。
3. 创建用户名和密码，必须与 [步骤 2a \(3\)](#) 中在 SmartConsole 应用上创建的用户名和密码相同。
  - 从 **Shell** 下拉列表中，选择 `/bin/bash`。
  - 从 **可用角色** 下拉列表中，选择 `adminRole`。
  - 保留其余字段的默认值。
  - 点击 **确定 (Ok)**。
4. 通过 SSH 连接到 Check Point 安全管理器，并使用以下命令创建专家密码：

```
set expert-password <password>
```

- 注释
- 如果您已配置专家密码，可以使用该密码。
  - 在 [步骤 2b \(3\)](#) 和 [步骤 2a \(3\)](#) 中创建的用户名和密码必须相同。

在 Check Point 安全管理器的分布式部署中，已完成在 Check Point 上预先配置凭证的程序。

您需要在[连接至 Check Point 安全管理器](#)页面上提供这些凭证，如[步骤 4](#)所示。

如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅[是否将自定义 API 端口用于 Check Point \(r80\) 安全管理器？](#)。

---

## 下一步做什么

### [导出 Check Point r80 配置文件的程序](#)

## 从独立 Check Point 部署导出

必须在使用 Cisco Secure Firewall 迁移工具上的 Live Connect 之前在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在独立 Check Point 部署上预先配置凭证的程序包括以下步骤：

**步骤 1** 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到管理 Check Point 安全网关和 Check Point 安全管理器的独立 Check Point 设备。

**步骤 2** 导航至[用户管理 \(User Management\)](#) 选项卡，然后选择 [用户 \(Users\)](#) > [添加 \(Add\)](#)。

a) 在[添加用户](#)窗口中，使用以下详细信息创建新的用户名和密码：

- 从 **Shell** 下拉列表中，选择 `/etc/cli.sh`。
- 从 **可用角色** 下拉列表中，选择 `adminRole`。
- 保留其余字段的默认值。
- 点击 **确定 (Ok)**。

您需要在[连接至 Check Point 安全网关](#)页面上提供这些凭证，如[步骤 3](#)所示。

有关详细信息，请参阅[图 3: 连接到 Check Point 安全网关](#)。

b) 在[添加用户](#)窗口中，使用以下详细信息创建另一用户名和密码：

- 从 **Shell** 下拉列表中，选择 `/bin/bash`。
- 从 **可用角色** 下拉列表中，选择 `adminRole`。
- 保留其余字段的默认值。
- 点击 **确定 (Ok)**。

**步骤 3** 在 Check Point 设备的 r80 SmartConsole 应用上创建以下内容：

**注释** 确保您现在创建的用户名和密码与上一步骤中在 Check Point Gaia Console 应用上创建的用户名和密码相同。

- a) 登录 Check Point 设备的 SmartConsole 应用。
- b) 导航至管理和设置 > 权限和管理员 > 管理员。
- c) 点击 \*，使用以下详细信息创建新的用户名和密码：

- 选择身份验证方式作为 **Check Point** 密码。
- 点击**设置新密码 (Set New Password)** 以设置新密码。

注释 切勿选中用户下次登录时必须更改密码复选框。

- 选择权限配置文件作为**超级用户**。
- 选择到期为**从不**。

步骤 2 的**步骤 b** 和步骤 3 的**步骤 c** 中创建的用户名和密码必须相同。

您需要在**连接至 Check Point 安全管理器**页面上提供这些凭证，如**步骤 4** 所示。

- d) 点击**发布 (Publish)** 在 Check Point SmartConsole 应用上保存配置更改。

**步骤 4** 通过 SSH 连接到 Check Point 设备，并使用以下命令创建专家密码：

```
set expert-password <password>
```

- 注释
- 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
  - 步骤 2 的**步骤 b** 和步骤 3 的**步骤 c** 中创建的用户名和密码必须相同。

在独立部署中，已完成 Check Point 设备凭证的预先配置。

如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 [是否将自定义 API 端口用于 Check Point \(r80\) 安全管理器？](#)。

---

## 下一步做什么

[导出 Check Point r80 配置文件的程序](#)

## 从多域 Check Point 部署导出

必须使用 Cisco Secure Firewall 迁移工具上的 Live Connect 在 Check Point (r80) 设备上配置凭证，以提取 Check Point 配置。

在多域 Check Point 部署上预先配置凭证的程序包括以下步骤：

**步骤 1** 在 Gaia Console Check Point 安全网关上创建以下内容：

- a) 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全网关。
- b) 导航至用户管理选项卡，然后选择 **用户 > 添加**。
- c) 在**添加用户**窗口中，使用以下详细信息创建新的用户名和密码：
  - 从 **Shell** 下拉列表中，选择 `/etc/cli.sh`。

- 从可用角色下拉列表中，选择 *adminRole*。
  - 保留其余字段的默认值。
  - 点击确定 (Ok)。
- d) 通过 SSH 连接到 Check Point 安全网关，并使用以下命令创建新密码：  
**set expert-password <password>**
- 在多域部署中，已完成在 Check Point 安全网关上预先配置凭证的程序。
- e) （可选）从虚拟系统扩展 (VSX) 设备导出配置时，请选中虚拟系统 ID (Virtual System ID) 复选框，以便能够输入虚拟系统 ID。

图 1: 连接至 Check Point 安全网关 - 多域部署

1 2 3

### Connect to Checkpoint Security Gateway

IP Address: 10.1.1.1      Port: 22

Admin Username: admin

Admin Password: ●●●●●●●●

Expert Password: ●●●●●●●●

Virtual System ID

Virtual ID Number: 2

Login

**步骤 2** 在 Check Point 安全管理器上创建用户名和密码：

- a) 在 SmartConsole (mds) 应用上，执行以下步骤：
1. 登录 Check Point 安全管理器。
  2. 导航至管理和设置 > 权限和管理员 > 管理员。
  3. 点击 \*，使用以下详细信息创建新的用户名和密码：
    - 选择身份验证方式作为 **Check Point** 密码。
    - 点击设置新密码 (**Set New Password**) 以设置新密码。

注释 切勿选中用户下次登录时必须更改密码复选框。

- 选择权限配置文件作为多域超级用户。
- 选择到期为从不。

4. 点击发布 (**Publish**) 在 Check Point SmartConsole 应用上保存配置更改。

如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 [是否将自定义 API 端口用于 Check Point \(r80\) 安全管理器？](#)。

b) 在 Check Point 安全管理器的 Gaia Console 上，执行以下步骤：

注释 确保您现在创建的用户名和密码与 [步骤 2a \(3\)](#) 中在 SmartConsole 应用上创建的用户名和密码相同。

1. 在 Web 浏览器中，通过 HTTPS 会话打开 Gaia Console 应用以连接到 Check Point 安全管理器。
2. 导航至用户管理选项卡，然后选择 用户 > 添加。
3. 创建用户名和密码，必须与 [步骤 2a \(3\)](#) 中在 SmartConsole 应用上创建的用户名和密码相同。
  - 从 **Shell** 下拉列表中，选择 `/bin/bash`。
  - 从可用角色下拉列表中，选择 `adminRole`。
  - 保留其余字段的默认值。
  - 点击确定 (**Ok**)。

4. 通过 SSH 连接到 Check Point 安全管理器，并使用以下命令创建新密码：

```
set expert-password <password>
```

- 注释
- 如果您已在 Check Point 设备上配置了专家密码，请重新使用该密码。
  - 在 [步骤 2a \(3\)](#) 和 [步骤 2b \(3\)](#) 中创建的用户名和密码必须相同。

在多域部署中，已完成在 Check Point 安全管理器上预先配置凭证的程序。

您需要使用凭证连接至 Live Connect，如图 2: [连接至 Check Point 安全管理器 - 多域部署](#) 所示。

图 2: 连接至 Check Point 安全管理器 - 多域部署

## 注释

- 如果在 Check Point 智能管理器上使用自定义 API 端口，请参阅 [是否将自定义 API 端口用于 Check Point \(r80\) 安全管理器？](#)。
- 无法提取用于多域部署的全局策略包。因此，在 Check Point CMA 下配置为配置的一部分的对象、ACE 规则和 NAT 规则只能导出和迁移。

## 下一步做什么

[导出 Check Point r80 配置文件的程序](#)



是否将自定义 API 端口用于 Check Point (r80) 安全管理器?



**注释** 如果您在 Check Point 智能管理器上使用自定义 API 端口，请执行以下步骤：

- 在 Live Connect 的 **Check Point 安全管理器**页面上，选中 **Check Point 多域部署**复选框。
- 如果使用多域部署，请添加 Check Point CMA 的 IP 地址和 API 端口详细信息。
- 如果是常规部署，请保留 Check Point 安全管理器的 IP 地址，并输入自定义 API 端口的详细信息。

## 导出 Check Point r80 配置文件的程序

### 开始之前

必须在 Check Point 设备上预先配置。有关迁移之前在 Check Point (r80) 设备上配置凭证的详细信息，请参阅[使用 Live Connect 预先配置 Check Point \(r80\) 设备以进行配置提取](#)。



- 注释**
- 我们建议您使用 Live Connect 提取 Check Point (r80) 配置。
  - 若使用未在 Cisco Secure Firewall 迁移工具中通过 Live Connect 导出的 Check Point (r80) 配置，会导致该配置在迁移中不受支持、部分迁移或迁移失败。
- 如果配置导出中的信息不完整，则某些配置不会迁移，并标记为不受支持。

要导出 Check Point r80 配置文件，请执行以下操作：

**步骤 1** 从[选择源配置](#)页面选择 Check Point (r80)。

**步骤 2** 点击[连接 \(Connect\)](#)。

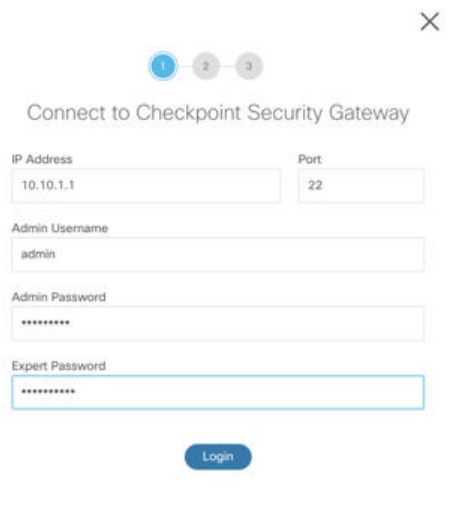
**注释** Live Connect 仅适用于 Check Point (r80)。

**步骤 3** 连接到 Check Point 安全网关。请执行以下操作：

a) 在 Check Point r80 安全网关中输入以下内容：

- IP 地址
- SSH 端口
- 管理用户名
- Admin 密码
- 专家密码

图 3: 连接到 Check Point 安全网关



Connect to Checkpoint Security Gateway

IP Address: 10.10.1.1      Port: 22

Admin Username: admin

Admin Password: \*\*\*\*\*

Expert Password: \*\*\*\*\*

Login

b) 点击 **登录 (Login)**。

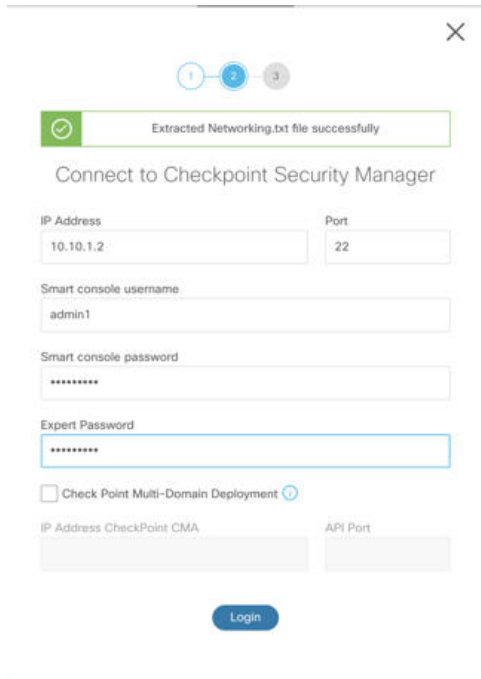
Cisco Secure Firewall 迁移工具会生成包含设备特定配置（例如接口和路由配置）的 *networking.txt* 文件。将 *networking.txt* 文件存储在 Cisco Secure Firewall 迁移工具当前会话的本地目录中。

**步骤 4** 连接到 Check Point 安全管理器。请执行以下操作：

a) 在 Check Point r80 安全管理器中输入以下内容：

- IP 地址
- SSH 端口
- 智能控制台用户名
- 智能控制台密码
- 专家密码

图 4: 连接到 Check Point 安全管理器



b) 点击登录 (**Login**)。

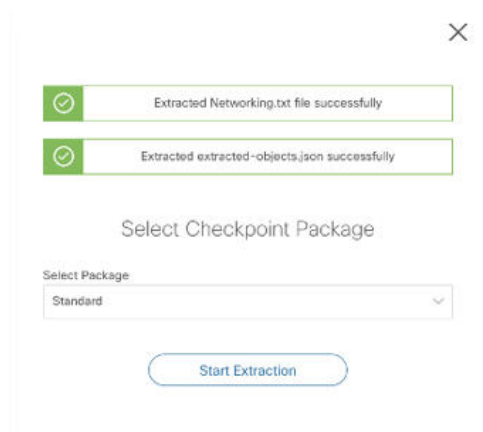
Cisco Secure Firewall 迁移工具会生成 *Extracted-objects.json* 文件，其中记录 Check Point 安全管理器中可用的完整网络和服务对象配置。

将 *Extracted-objects.json* 文件存储在 Cisco Secure Firewall 迁移工具当前会话的本地目录中。

**注释** 如果您已将 Cisco Secure Firewall 迁移工具连接到 Check Point 安全管理器，则会显示 Check Point 安全管理器中可用的策略包列表。

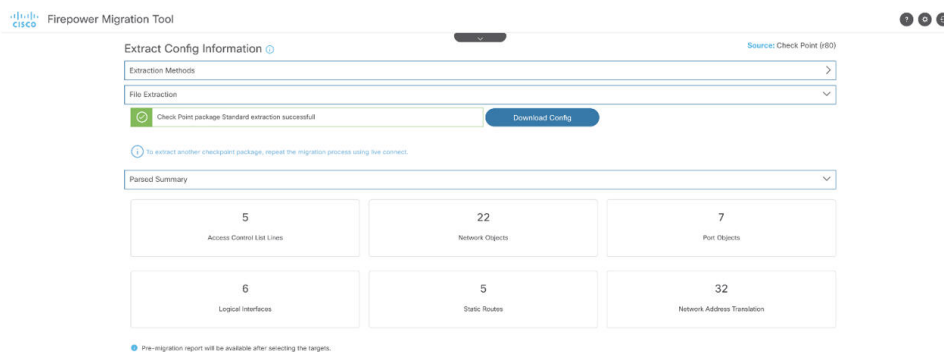
**步骤 5** 从选择 **Check Point 包 (Select Check Point Package)** 列表中选择要迁移的 Check Point 策略包，然后点击开始提取 (**Start Extraction**)。

图 5: 提取 Check Point 策略包



步骤 6 下载配置并继续迁移。

图 6: 在分布式部署和独立部署中，已完成 Check Point 配置提取



步骤 7 点击下一步 (Next) 以继续迁移 Check Point (r80) 配置。

下一步做什么

[上传 Check Point 配置文件](#)

## 提取其他配置文件

要提取其他配置文件，请执行以下步骤：

- 点击返回源选择 (**Back to source selection**) 以提取不同策略包的新配置，或者连接到不同的 Check Point (r80) 防火墙。
- 如果稍后必须迁移提取的 Check Point (r80) 配置，请下载当前配置。



注释 当前配置文件会下载到浏览器设置的默认下载位置。

您可以使用组装流水线方法来提取 r80 配置：

- 执行 Live Connect 以提取每个防火墙包或不同防火墙的 Check Point (r80) 配置文件。
- 为多个配置创建存储库。
- 使用稍后开始迁移选项，稍后再通过手动上传继续迁移。

## 上传 Check Point 配置文件

开始之前

将配置文件导出为 .zip 格式。

---

**步骤 1** 在提取配置信息 (Extract Config Information) 屏幕上的手动上传 (Manual Upload) 部分中，点击上传 (Upload) 以上传 Check Point 配置文件。

**步骤 2** 浏览到保存配置文件的位置。该配置文件是为 Check Point (r77) 提取的，并使用 Live Connect for Check Point (r80) 下载的。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。

预解析过程现已完成。

解析摘要部分显示解析状态。

**步骤 3** 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 4** 点击下一步 (Next)，选择目标参数。

---

下一步做什么

[为 Cisco Secure Firewall 迁移工具指定目标参数](#)

## 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 Check Point 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 Check Point 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 Check Point 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 Check Point 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 Check Point 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 Check Point 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 Check Point，在**共享配置**下选择相关的访问控制选项：
  - 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 **Any**。
  - 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。

**注释** 路由查找仅限于静态路由和动态路由（不考虑 PBR 和 NAT），并且根据源和目标网络对象的性质，此操作可能会导致规则爆炸。

路由信息从 `networking.txt` 文件中获取。此文件是 FMT-CP-Config-Extractor\_v4.0.1-8248 工具的输出，该工具使用 `netstat -rnv` 命令收集路由表。有关详细信息，请参阅[使用配置提取器导出设备配置](#)。

此版本不支持对基于区域的策略执行 IPv6 路由查找。确保全局策略或基于区域的策略的所有规则成功迁移。

在 **设备配置**下，选择要从 Check Point 防火墙迁移的接口、路由和站点间 VPN 隧道配置。请注意，只能迁移基于策略（加密映射）的站点间 VPN 隧道配置。

- （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 Check Point 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）。

---

下一步做什么

[查看迁移前报告，第 44 页](#)

## 查看迁移前报告

---

**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：

- **迁移摘要** - 可成功迁移到 Firepower Threat Defense 的受支持 Check Point 配置元素的总体摘要。例如，策略名称、规则计数等。
- **解析错误详细信息** - 突出显示导致解析失败的配置。这样做有助于编辑和更新配置以进行重试。
- **不支持的配置** - 以更详细的方式列出 FMT 不支持迁移的所有配置项目。例如，环回接口、别名接口、域对象。
- **部分支持的配置** - 仅可部分迁移的所有 Check Point 配置元素的列表。例如，使用 Ping 参数的静态路由。
- **跳过的配置** - 迁移期间被 FMT 忽略且不会转发到目标系统的所有 Check Point 配置元素的列表。

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 [《Firepower 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 Check Point 上完成这些纠正操作，重新导出 Check Point 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 Check Point 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。

## 将 Check Point 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 Check Point 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。

在 **映射 FTD 接口** 屏幕上，Cisco Secure Firewall 迁移工具将检索 威胁防御 设备上的接口的列表。默认情况下，Cisco Secure Firewall 迁移工具会根据其接口标识符映射 Check Point 和 威胁防御 设备中的接口。例如，Check Point 接口上的“管理专用”接口会自动映射到 威胁防御 设备上的“管理专用”接口，并且不可更改。

Check Point 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 Check Point 接口或端口通道 (PC) 数据接口 (Check Point 配置中不包括管理专用接口和子接口)。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 Check Point 接口、物理子接口、端口通道或端口通道子接口 (Check Point 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 Check Point 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。
  - 子接口不是由 Cisco Secure Firewall 迁移工具创建的。物理接口、端口通道或子接口之间仅允许接口映射。

### 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 [Cisco Secure Firewall 迁移工具指定目标参数](#)，第 41 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 Check Point 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 Check Point 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 Check Point 配置中的所有子接口映射子接口。

**步骤 2** 当您每个 Check Point 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 Check Point 接口映射到相应的威胁防御接口对象、安全区和接口组。有关详细信息，请参阅[将 Check Point 接口映射到安全区和接口组](#)。

## 将 Check Point 接口映射到安全区和接口组

为确保正确地迁移 Check Point 配置，请将 Check Point 接口映射到相应的威胁防御接口对象、安全区和接口组。在 Check Point 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，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。
- 接口组 - 接口可属于多个接口组。

Cisco Secure Firewall 迁移工具支持接口与安全区和接口组的一对一映射；当安全区或接口组映射到某个接口时，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和接口组的详细信息，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** 在映射安全区和接口组屏幕上，查看可用接口、安全区和接口组。

**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和接口组，或映射到在 Check Point (r80) 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 4** 您可以手动映射或自动创建安全区和接口组。

**步骤 5** 要手动映射安全区和接口组，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**) 以添加新的安全区或接口组。
- c) 在 **安全区** 栏中输入安全区名称。允许的最大字符数为 48。同样，您可以添加接口组。
- d) 点击关闭 (**Close**)。

要通过自动创建映射安全区和接口组，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，选中接口组和区域映射中的一个或两个。
- c) 点击自动创建 (Auto-Create)。

Cisco Secure Firewall 迁移工具将为这些安全区提供与 Check Point 接口相同的名称（例如 **outside** 或 **inside**），并在名称后显示“(A)”，以指示它是由 Cisco Secure Firewall 迁移工具创建的。将为接口组添加 **\_ig** 后缀，例如 **outside\_ig** 或 **inside\_ig**。此外，安全区和接口组与 Check Point 接口具有相同的模式。例如，如果 Check Point 逻辑接口是 L3 模式，则为该接口创建的安全区和接口组也是 L3 模式。

**步骤 6** 在已将所有接口映射到相应的安全区和接口组后，点击下一步 (Next)。

## 优化，检查和验证配置

在将迁移的 Check Point 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 Check Point。

- 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。

### 对象优化

在迁移过程中会考虑以下对象以进行对象优化：

- 未引用的对象 - 可以选择在迁移开始时不迁移未被引用的对象。
- 重复对象 - 如果对象已存在于管理中心上，则不会创建重复对象，而是重复使用策略。
- 不一致的对象 - 如果存在名称相似但内容不同的对象，则在迁移推送之前 Cisco Secure Firewall 迁移工具会修改对象名称。

**步骤 1**（可选）在优化、查看和验证配置 (Optimize, Review and Validate Configuration) 屏幕上，点击优化 ACL (Optimize ACL) 以运行优化代码，并执行以下操作：

- a) 要下载已识别的 ACL 优化规则，请点击 **下载 (Download)**。
- b) 选择规则，然后选择操作 (Actions) > 作为已禁用迁移 (Migrate as disabled) 或不迁移 (Do not migrate) 并应用其中一项操作。
- c) 点击 **保存 (Save)**。

迁移操作从不迁移 (**Do not migrate**) 更改为已禁用 (**Disabled**), 反之亦然。

您可以使用以下选项来批量选择规则

- 迁移 - 以默认状态迁移。
- 不迁移 - 忽略 ACL 的迁移。
- 作为已禁用迁移 (Migrate as disabled) - 迁移状态 (*State*) 字段被设为禁用 (*Disable*) 的 ACL。
- 迁移为已启用 (Migrate as enabled) - 迁移状态 (*State*) 字段被设为启用 (*Enable*) 的 ACL。

**步骤 2** 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。

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, 以便更轻松地将映射回 Check Point 配置文件。例如, 如果 Check Point 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。

- 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 3** 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、VPN 对象)
- NAT
- 接口
- 路由
- 站点间 VPN 隧道

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 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** (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 7** 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 8** 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 9** 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 51 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 Check Point 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 Check Point 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 Check Point 的迁移后报告并完成迁移

---

**步骤 1** 导航至您已将迁移后报告下载到的位置。

**步骤 2** 打开迁移后报告并仔细检查其内容，了解您的 ASA 配置是如何迁移的：

- **迁移摘要** - 已成功从 Check Point 迁移到 Firepower Threat Defense 的配置摘要。
- **选择性策略迁移** - 提供所选用于迁移和接口映射的特定 Check Point 功能的详细信息。
- **迁移转换** - 转换和推送详细信息，包括以下内容：
  - 网络/服务对象处理
  - 部分迁移的配置列表及其原因
  - 不支持的配置列表及原因
  - 扩展访问控制规则

---

## 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：Check Point 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** 使用 Check Point Web 可视化工具和 FMT-CP-Config-Extractor\_v4.0.1-8248 工具收集您尝试迁移的 Check Point 设备配置，并保存一份 Check Point 配置文件。
- 步骤 2** 查看 Check Point 配置 zip 文件。
- 步骤 3** 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 4** 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 5** （可选）如果源 Check Point 配置具有绑定接口，请在目标 Firepower 2100 系列设备上创建端口通道 (EtherChannel)。有关详细信息，请参阅[配置 EtherChannel 和冗余接口](#)。
- 步骤 6** 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 23 页。
- 步骤 7** 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 41 页。
- 步骤 8** 将 Check Point 接口与威胁防御接口映射。  
**注释** Cisco Secure Firewall 迁移工具允许您将 Check Point 接口类型映射到威胁防御接口类型。  
例如，您可以将 Check Point 中的绑定接口映射到威胁防御中的物理接口。  
有关详细信息，请参阅[将 Check Point 防火墙配置与威胁防御接口映射](#)。

**步骤 9** 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 Check Point 逻辑接口映射到安全区。

有关详细信息，请参阅[将 Check Point 接口映射到安全区 和 接口组](#)。

**步骤 10** 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 11** 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[查看 Check Point 的迁移后报告并完成迁移，第 52 页](#)。

**步骤 12** 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 53 页](#)。

---

**步骤 1** 通过 Gaia Console 连接到 Check Point 安全网关。

**步骤 2** 通过 Gaia Console 关闭意向安全网关的 Check Point 接口。

**步骤 3** （可选）访问 管理中心并配置动态路由、平台设置，以及 Cisco Secure Firewall 迁移工具未迁移、需要为 Firepower 2100 系列设备手动迁移的其他功能。

**步骤 4** 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

**步骤 5** 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 6** 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 7** 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 Check Point 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 8** 运行全面的测试计划并监控管理 Firepower 2100 设备的 管理中心。

---



## CHAPTER 3

# 思科成功网络 - 遥测数据

• [思科成功网络 - 遥测数据](#)，第 55 页

## 思科成功网络 - 遥测数据

Cisco Success Network 是 Cisco Secure Firewall 迁移工具中的一项永远在线的使用情况信息和指标收集功能，它通过迁移工具和思科云之间的安全云连接收集和传输使用情况统计信息。这些统计信息可帮助我们为未使用的功能提供额外支持，并改进我们的产品。每当您在 Cisco Secure Firewall 迁移工具中启动迁移过程时，相应的遥测数据文件都生成和存储在固定位置。

当您迁移的 Check Point 配置推送到管理中心时，推送服务会从该位置读取遥测数据文件，并在数据成功上传到云后将其删除。

迁移工具提供两个选项，用于传输遥测数据 - 有限 和 广泛。

将 **Cisco Success Network** 设置为 **有限**时，会收集以下遥测数据点：

表 2: 有限的遥测

数据点	描述	示例值
时间	收集遥测数据的时间和日期	2023-04-25 10:39:19
源类型	源设备类型	ASA
设备型号	ASA 型号	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 系列 2000 MHz, 1 CPU (4 核)
源版本	ASA 版本	9.2 (1)
目标管理版本	管理中心的目标版本	6.5 或更高版本
目标管理类型	目标管理设备的类型，即管理中心	管理中心
目标设备版本	目标设备的版本	75

数据点	描述	示例值
目标设备型号	目标设备的型号	Cisco Secure Firewall Threat Defense for VMware
迁移工具版本	The version of the migration tool	1.1.0.1912
迁移状态	ASA 配置迁移到管理中心的状态	SUCCESS

当 **Cisco Success Network** 设置为广泛时，下表提供有关遥测数据点、其说明和示例值的信息：

表 3: 广泛的遥测

数据点	描述	示例值
操作系统	运行 Cisco Secure Firewall 迁移工具的操作系统。它可以是 Windows7/Windows10 64 位/macOS High Sierra	Windows 7
浏览器	用于启动 Cisco Secure Firewall 迁移工具的浏览器。它可以是 Mozilla/5.0 或 Chrome/68.0.3440.106 或 Safari/537.36	Mozilla/5.0

表 4: 源 Check Point 信息

数据点	描述	示例值
时间	收集遥测数据的时间和日期	2023-04-25 10:39:19
源类型	源设备类型	Check Point
源设备序列号	Check Point 序列号	设备序列号（如果存在）。
源设备型号	Check Point 型号	
源设备版本	Check Point 的版本	R77.30
源配置计数	源配置中的总行数	504
防火墙模式	Check Point 上配置的防火墙模式 - 路由或透明	路由
情景模式	Check Point 的情景模式。这可以是单情景或多情景。	单一
<b>Check Point 配置统计信息：</b>		
ACL 计数	连接到访问组的 ACL 数量	46
访问规则计数	访问规则总数	46
NAT 规则计数	NAT 规则总数	17

数据点	描述	示例值
网络对象计数	在 Check Point 中配置的网络对象数	34
网络对象组计数	Check Point 中的网络对象组数	6
端口对象计数	端口对象的数量	85
端口对象组计数	端口对象组的数量	37
不受支持的访问规则计数	不受支持的访问规则总数	3
不受支持的 NAT 规则计数	不受支持的 NAT 访问规则总数	0
基于 FQDN 的访问规则计数	基于 FQDN 的访问规则数量	7
基于时间范围的访问规则计数	基于时间范围的访问规则数量	1
基于 SGT 的访问规则计数	基于 SGT 的访问规则数量	0
工具无法解析的配置行摘要		
未解析的配置计数	解析器无法识别的配置行数	68
未解析的访问规则总数	未解析的访问规则的总数	3

表 5: 目标管理设备 (管理中心) 信息

数据点	描述	示例值
目标管理版本	管理中心的目标版本	6.2.3.3 (内部版本 76)
目标管理类型	目标管理设备的类型, 即管理中心	管理中心
目标设备版本	目标设备的版本	75
目标设备型号	目标设备的型号	Cisco Secure Firewall Threat Defense for VMware
迁移工具版本	迁移工具的版本	1.1.0.1912

表 6: 迁移摘要

数据点	描述	示例值
访问控制策略		

数据点	描述	示例值
名称	访问控制策略的名称	不存在
访问规则计数	迁移的 ACL 规则总数	0
部分迁移的 ACL 规则计数	部分迁移的 ACL 规则总数	3
扩展的 ACP 规则计数	扩展的 ACP 规则的数量	0
<b>NAT 策略</b>		
名称	NAT 策略的名称	不存在
NAT 规则计数	迁移的 NAT 规则总数	0
部分迁移的 NAT 规则计数	部分迁移的 NAT 规则总数	0
<b>更多迁移详细信息...</b>		
接口计数	已更新接口的数量	0
子接口计数	已更新子接口的数量	0
静态路由计数	静态路由的数量	0
对象计数	创建的对象数	34
对象组计数	创建的对象组数	6
接口组计数	创建的接口组数	0
安全区域计数	创建的安全区域的数量	3
网络对象重用计数	重新使用的对象数	21
网络对象重命名计数	重命名的对象数	1
端口对象重用计数	重新使用的端口对象数	0
端口对象重命名计数	重命名的端口对象数	0

表 7: Cisco Secure Firewall 迁移工具性能数据

数据点	描述	示例值
转换时间	解析 Check Point 配置行所需的时间（以分钟为单位）	14

数据点	描述	示例值
迁移时间	端到端迁移所需的总时间（以分钟为单位）	592
配置推送时间	推送最终配置所需的时间（以分钟为单位）	7
迁移状态	将 Check Point 配置迁移到 管理中心 的状态	SUCCESS
错误消息	Cisco Secure Firewall 迁移工具显示的错误消息	null
错误说明	有关发生错误的阶段和可能的根本原因的说明	null

### Check Point r80 遥测文件示例

以下例举了有关 Check Point 配置向 威胁防御 迁移的遥测数据文件：

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "Check Point_config_stats": {
      "Ipv6_access_rule_counts": 0,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 0,
      "Ipv6_network_counts": 24,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 63,
      "acl_counts": 63,
      "fqdn_based_access_rule_counts": 0,
      "nat_rule_counts": 0,
      "network_object_counts": 143,
      "network_object_group_counts": 31,
      "no_of_fqdn_based_objects": 0,
      "ospfv3_count": 0,
      "port_object_counts": 370,
      "port_object_group_counts": 55,
      "sgt_based_access_rules_count": 0,
      "timerange_based_access_rule_counts": 0,
      "total_unparsed_access_rule_counts": 0,
      "tunneling_protocol_based_access_rule_counts": 0,
      "unparsed_config_count": 15,
      "unsupported_access_rules_count": 0,
      "unsupported_nat_rule_count": 0
    },
    "context_mode": "SINGLE",
    "error_description": null,
    "error_message": null,
    "firewall_mode": "ROUTED",
    "log_info_acl_count": 0,
    "migration_status": "SUCCESS",
    "migration_summary": {
      "access_control_policy": [
        [
          {
            "access_rule_counts": 63,
            "apply_file_policy_rule_counts": 0,
            "apply_ips_policy_rule_counts": 0,
            "apply_log_rule_counts": 0,
            "do_not_migrate_rule_counts": 0,

```

```

        "enable_Global-ACL-Policy": true,
        "enable_Zone-Specific-ACL-Policy": false,
        "enable_hit_count": false,
        "expanded_acp_rule_counts": 1,
        "name": "FTD-Mig-1566804327",
        "partially_migrated_acl_rule_counts": 0,
        "update_rule_action_counts": 0
    }
  ],
  "interface_counts": 12,
  "interface_group_counts": 0,
  "interface_group_manually_created_counts": 0,
  "nat_Policy": [
    [
      {
        "NAT_rule_counts": 0,
        "do_not_migrate_rule_counts": 0,
        "name": "Doesn't Exist",
        "partially_migrated_nat_rule_counts": 0
      }
    ]
  ],
  "network_object_rename_counts": 0,
  "network_object_reused_counts": 0,
  "object_group_counts": 15,
  "objects_counts": 54,
  "port_object_rename_counts": 0,
  "port_object_reused_counts": 5,
  "security_zone_counts": 13,
  "security_zone_manually_created_counts": 0,
  "static_routes_counts": 22,
  "sub_interface_counts": 11
},
"migration_tool_version": "2.0.3169",
"rule_change_acl_count": 0,
"source_config_counts": 0,
"source_device_model_number": "Check Point Model Not Exists",
"source_device_serial_number": null,
"source_device_version": "R77.30",
"source_type": "Check Point",
"system_information": {
  "browser": "Chrome/76.0.3809.100",
  "operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
"target_device_version": "76",
"target_management_type": "6.4.0.4 (build 31)",
"target_management_version": "6.4.0.4 (build 31)",
"template_version": "1.1",
"time": "2019-08-26 12:55:40",
"tool_analytics_data": {
  "objectsplit_100_count": 0
},
"tool_performance": {
  "config_push_time": 725,
  "conversion_time": 29,
  "migration_time": 1020
}
},
"version": "1.0"
}

```



## Check Point r80 遥测文件示例

以下例举了有关 Check Point 配置向 威胁防御 迁移的遥测数据文件：

```
{
"Check Point_config_stats":{
  "Ipv6_access_rule_counts":0,
  "Ipv6_bgp_count":0,
  "Ipv6_nat_rule_count":0,
  "Ipv6_network_counts":3,
  "Ipv6_static_route_counts":0,
  "access_rules_counts":726,
  "acl_category_count":0,
  "acl_counts":726,
  "fqdn_based_access_rule_counts":0,
  "nat_rule_counts":335,
  "network_object_counts":7645,
  "network_object_group_counts":268,
  "no_of_fqdn_based_objects":0,
  "port_object_counts":1051,
  "port_object_group_counts":66,
  "s2s_vpn_tunnel_counts":0,
  "sgt_based_access_rules_count":0,
  "timerange_based_access_rule_counts":0,
  "total_unparsed_access_rule_counts":0,
  "tunneling_protocol_based_access_rule_counts":0,
  "unparsed_config_count":234,
  "unsupported_access_rules_count":0,
  "unsupported_nat_rule_count":0},
  "context_mode":"SINGLE",
  "error_description":"No data.",
  "error_message":"push failed for object network",
  "firewall_mode":"ROUTED",
  "log_info_acl_count":0,
  "migration_status":"FAIL",
  "migration_summary":{
    "access_control_policy":[
      [
        {
          "access_rule_counts":0,
          "apply_file_policy_rule_counts":0,
          "apply_ips_policy_rule_counts":0,
          "apply_log_rule_counts":0,
          "do_not_migrate_rule_counts":0,
          "enable_Global-ACL-Policy":true,
          "enable_Zone-Specific-ACL-Policy":false,
          "enable_hit_count":false,
          "expanded_acp_rule_counts":1,
          "name":"Doesn't Exist",
          "partially_migrated_acl_rule_counts":0,
          "total_acl_element_counts":389416,
          "update_rule_action_counts":0
        }
      ]
    ],
    "interface_counts":11,
    "interface_group_counts":0,
    "interface_group_manually_created_counts":0,
    "nat_Policy":[
      [
        {
          "NAT_rule_counts":0,
          "do_not_migrate_rule_counts":0,
          "name":"Doesn't Exist",

```

```

        "partially_migrated_nat_rule_counts":0
    }
  ],
  "network_object_rename_counts":0,
  "network_object_reused_counts":0,
  "object_group_counts":222,"objects_counts":7148,
  "port_object_rename_counts":2,
  "port_object_reused_counts":30,
  "prefilter_control_policy":[
    [
      {
        "do_not_migrate_rule_counts":0,
        "name":null,
        "partially_migrated_acl_rule_counts":0,
        "prefilter_rule_counts":0
      }
    ]
  ],
  "security_zone_counts":11,
  "security_zone_manually_created_counts":0,
  "static_routes_counts":0,
  "sub_interface_counts":8,
  "time_out":false),
  "migration_tool_version":"2.1.4283",
  "mtu_info":{"interface_name":null,
  "mtu_value":null},
  "rule_change_acl_count":0,
  "selective_policy":
    {
      "acl":true,
      "acl_policy":true,
      "application":false,
      "csm":false,
      "interface":true,
      "interface_groups":true,
      "migrate_tunneled_routes":false,
      "nat":true,
      "network_object":true,
      "policy_assignment":true,
      "populate_sz":false,
      "port_object":true,
      "routes":true,
      "security_zones":true,
      "unreferenced":true},
  "source_config_counts":0,
  "source_device_model_number":"Check Point Model Not Exists",
  "source_device_serial_number":null,
  "source_device_version":"R77.30",
  "source_type":"Check Point",
  "system_information":
    {
      "browser":"Chrome/80.0.3987.163","operating_system":
      "Macintosh; Intel Mac OS X 10_15_4"},
      "target_device_model":"Cisco Firepower 4110 Threat Defense",
      "target_device_version":"76",
      "target_management_type":"6.5.0 (build 63)",
      "target_management_version":"6.5.0 (build 63)",
      "template_version":"1.1",
      "time":"2020-04-16 04:50:05",
      "tool_analytics_data":{"objectsplit_100_count":6},
      "tool_performance":
        {
          "config_push_time":1457,

```

```
    "conversion_time":279,  
    "migration_time":2637  
  }  
}
```





## 第 4 章

# 排除迁移问题

- [Cisco Secure Firewall 迁移工具的故障排除](#)，第 65 页
- [用于排除故障的日志和其他文件](#)，第 66 页
- [Check Point 文件上传失败故障排除](#)，第 66 页

## Cisco Secure Firewall 迁移工具的故障排除

在 Check Point 配置文件上传或将已迁移的配置推送到管理中心时，迁移通常会失败。

Check Point 配置迁移过程失败的一些常见情况如下：

- Check Point Config.zip 中文件缺失。
- Cisco Secure Firewall 迁移工具在 Check Point Config.zip 中检测到无效文件
- 如果 Check Point 配置文件是除 .zip 以外的任何压缩文件类型。

### Cisco Secure Firewall 迁移工具支持捆绑包

Cisco Secure Firewall 迁移工具提供下载支持捆绑包的选项，以提取重要的故障排除信息，例如日志文件、数据库和配置文件。请执行以下操作：

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的。



**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。

## 用于排除故障的日志和其他文件

可在以下文件中找到有助于识别和排除问题的信息。

文件	位置
日志文件	<migration_tool_folder>\logs
迁移前报告	<migration_tool_folder>\resources
迁移后报告	<migration_tool_folder>\resources
未解析文件	<migration_tool_folder>\resources

## Check Point 文件上传失败故障排除

如果 Check Point 配置文件上传失败，这通常是因为 Cisco Secure Firewall 迁移工具无法解析文件中的一行或多行。

可在以下位置找到导致上传和解析失败的错误的相关信息：

- 未解析文件 - 查看文件末尾部分，确定已成功解析的 Check Point 配置文件中最后被忽略的行。
- 意外文件 - 检测到的 Check Point 文件无效。例如，使用 Mac 操作系统压缩时会创建 Mac 系统文件。删除 Mac 文件。
- （仅适用于 r75-r77.30）命名不正确的文件 - 没有为 Check Point 正确命名安全策略和 NAT 策略文件。正确重命名 ACL 和 NAT 文件。
- 缺少文件 - Check Point config.zip 文件中缺少某些文件。添加所需的文件。



**注释** 对于 r77，手动提取缺失的配置文件。有关详细信息，请参阅[导出 Check Point r77 配置文件](#)。

对于 r80，使用 Live Connect 为 Cisco Secure Firewall 迁移工具提取正确的配置文件。有关详细信息，请参阅[导出 Check Point r80 配置文件](#)。

## Check Point 故障排除示例：找不到对象组的成员（仅限 r75 - r77.30）

在本示例中，由于一个元素的配置出错，Check Point 配置文件上传和解析失败。

**步骤 1** 查看错误消息以确定问题。

此失败生成以下错误消息：

位置	错误消息
Cisco Secure Firewall 迁移工具消息	Check Point 配置文件解析出错。 有关解析错误，请参阅 <a href="#">查看迁移前报告</a> 的错误部分；有关推送阶段发生的推送错误，请参阅 <a href="#">查看 Check Point 的迁移后报告并完成迁移</a> 。
日志文件	[ERROR   objectGroupRules] > "ERROR, SERVICE_GROUP_RULE not applied for port-group object [services_epacity_nt_abc] as CheckPoint object [ica] does not exist in <service> table;"  [INFO   objectGroupRules] > "Parsing object-group service:[services_gvxs06]"  [INFO   objectGroupRules] > "Parsing object-group service:[services_iphigenia]"  [INFO   objectGroupRules] > "Parsing object-group service:[Services_KPN_ISP]"

**步骤 2** 打开 Check Point `services.xml` 文件。

**步骤 3** 搜索名称为 `services_gvxs06` 的对象组。

**步骤 4** 使用智能控制面板创建对象组的缺失成员。

**步骤 5** 再次导出配置文件。有关详细信息，请参阅[导出 Check Point r77 配置文件](#)。

**步骤 6** 如果没有其他错误，将新 Check Point 配置 zip 文件上传到 Cisco Secure Firewall 迁移工具并继续执行迁移。

## Live Connect 的 Check Point (r80) 故障排除示例

**示例 1：** 在 Check Point 安全管理器上请求详细信息。

在本示例中，Cisco Secure Firewall 迁移工具请求了 Check Point 安全管理器的详细信息。

查看错误消息以确定问题。此失败生成以下错误消息：

位置	错误消息
Cisco Secure Firewall 迁移工具消息	筛选请求以提供 Check Point 安全管理器的详细信息。

位置	错误消息
日志文件	[ERROR   connect_cp] > "Unable to extract the Extracted-objects.json file due to credentials with insufficient privileges, time-out issues and so on. 有关详细信息，请参阅 Cisco Secure Firewall 迁移工具用户指南。  127.0.0.1 - - [20/Jul/2020 17:20:43] "POST /api/CP/connect HTTP/1.1" 500 -

凭证不正确。按照上述步骤预先配置凭证。用于 Check Point 安全管理器的 Check Point Gaia 上使用的凭证必须有 `/bin/bash` shell 配置文件。必须为具有正常部署的“超级用户”权限的 Check Point 安全管理器在 Check Point 智能控制台应用上部署相同的凭证。如果使用了多域部署，则权限必须是“超级用户”。有关更多信息，请参阅[使用 Live Connect 预先配置 Check Point \(r80\) 设备以进行配置提取](#)。

### 示例 2：错误的文件格式

在本例中，Cisco Secure Firewall 迁移工具迁移因文件格式错误而被阻止。

查看错误消息以确定问题。此失败生成以下错误消息：

位置	错误消息
Cisco Secure Firewall 迁移工具消息	已阻止
日志文件	[ERROR   cp_device_connection] > "Bad file format"  2020-07-20 17:10:57,347 [ERROR   connect_cp] > "Unable to download .tar file."  127.0.0.1 - - [20/Jul/2020 17:10:57] "GET /api/CP/generate_tar_file?package=Standard HTTP/1.1" 500 -

凭证不正确。按照上述步骤预先配置凭证。用于 Check Point 安全管理器的 Check Point Gaia 上使用的凭证必须有 `/bin/bash` shell 配置文件。必须为具有“超级用户”权限的 Check Point 安全管理器在 Check Point 智能控制台应用上部署相同的凭证。如果使用了多域部署，则必须授予“超级用户”权限。有关更多信息，请参阅[使用 Live Connect 预先配置 Check Point \(r80\) 设备以进行配置提取](#)。

### 示例 3：被阻止的 VSX 功能在威胁防御中不受支持

在本示例中，由于威胁防御中的 VSX 功能被阻止，Cisco Secure Firewall 迁移工具迁移失败。

查看错误消息以确定问题。此失败生成以下错误消息：

位置	错误消息
Cisco Secure Firewall 迁移工具消息	被阻止的 VSX 功能在 FTD 中不受支持。
日志文件	[ERROR   config_upload] > "VSX Feature is UNSUPPORTED in FTD"  Traceback (most recent call last)

问题描述 - 之所以出现该错误是因为从 Check Point r80.40 开始弃用了 `fw vsx stat` 命令。



解决方法是执行以下步骤：

1. 解压缩 *config.zip* 文件。
2. 打开 *networking.txt* 文件。

以下是样本输出的示例：

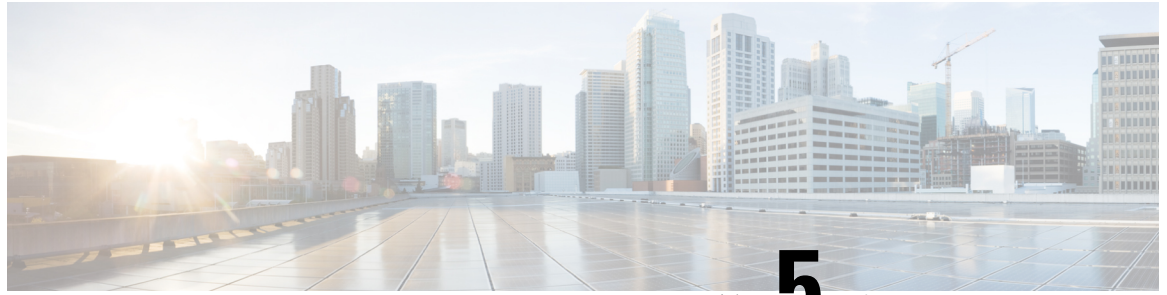
```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

按照如下步骤手动进行更换：

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. 选择所有文件并以 *.zip* 扩展名将它们压缩。





## 第 5 章

# Cisco Secure Firewall 迁移工具常见问题

- [Cisco Secure Firewall 迁移工具常见问题解答](#)，第 71 页

## Cisco Secure Firewall 迁移工具常见问题解答

问: 版本 3.0.1 的 Cisco Secure Firewall 迁移工具支持哪些新功能?

答: Cisco Secure Firewall 迁移工具 3.0.1 现在仅支持将 Cisco Secure Firewall 3100 系列作为从 Check Point 迁移的目标设备。

问: 版本 3.0 的 Cisco Secure Firewall 迁移工具支持哪些新功能?

答: 迁移到云交付的防火墙管理中心

问: 版本 2.5.2 的 Cisco Secure Firewall 迁移工具支持哪些新功能?

答: Check Point 的 ACL 优化。

问: 从 Check Point 转换到威胁防御有哪些硬件限制?

答: 如果配置文件与 Check Point Web 可视化工具以及 FMT-CP-Config-Extractor\_v4.0.1-8248 工具兼容，则您应该能够迁移源 Check Point。

问: 是否可以使用从 Check Point r76SP 导出的配置并将其迁移到 4100 和 6100 Firepower 平台?

答: 是。所有平台均支持 r75 至 r77.30。

只要提供了 Check Point Web 可视化工具，就能支持该平台。

问: 如何处理 Check Point 规则中的否定对象?

答: 如果对象属于排除类型对象/组，则 ACL 转换遵循 **permit** 和 **block** 组合。尽管不支持排除类型的网络对象/组，但 ACL 支持该转换。例如，在 Check Point ACE 规则引用了排除类型的对象组时。

- 如果 Check Point 规则操作为 **permit**:

- ACE 必须对 `<exception></exception>` XML 标记下引用的对象组的 **Deny** 执行一个操作，在规则附加一个例外对象组规则注释。

- ACE 必须对 `<base></base>` XML 标记下引用的对象组的 **Allow** 执行一个操作，在规则附加一个例外对象组规则注释。

- 如果 Check Point 规则操作为 **Deny/Reset**:
  - ACE 必须对 `<exception></exception>` XML 标记下引用的对象组的 **permit** 执行一个操作，为规则附加一个“例外对象组规则”注释。
  - ACE 必须对 `<base></base>` XML 标记下引用的对象组的 **Block(Deny)/Block with Reset(Reject)** 执行一个操作，在规则附加一个例外对象组规则注释。

问: Cisco Secure Firewall 迁移工具是否支持带否定单元的 ACE? 如果不支持, Cisco Secure Firewall 迁移工具会如何处理这些规则?

答: Cisco Secure Firewall 迁移工具不支持具有否定单元的 ACE, 它们通过将 ACE 视为普通 ACE 来进行转换。这些问题将在后续版本中加以解决。

问: 您看到“未能绑定到数据库。访问被拒绝”错误。您该怎么做?

答: 请执行以下操作:

- 打开管理服务器的 Check Point Gaia 控制台。
- 导航至 Gaia 控制台上的用户和角色设置。
- 在具有管理员角色的 Check Point 管理服务器 Gaia 控制台上使用主目录 `/home` 和 Shell `/etc/cli.sh` 参数的创建一个新的用户名凭证。

问: 在通过 Cisco Secure Firewall 迁移工具解析 Check Point 配置时, 您会看到解析计数为 0。您该怎么做?

答: 执行以下任一步骤:

使用 `FMT-CP-Config-Extractor_v4.0.1-8248` 工具解压缩 `network.txt` 文件, 并要避免使用手动编码的 `network.txt` 文件。

或

有可能出于任何原因而在 Check Point 安全网关上启用日志记录, 从那里输出的 `network.txt` 文件会被导出。由于启用了日志记录, 在 `network.txt` 文件中添加的无关信息会导致此类问题。如果是这样, 请执行以下操作:

- 检查 `network.txt` 文件。
- 通过删除附加的额外日志行来修复文件。
- 将新的压缩文件上传到 Cisco Secure Firewall 迁移工具。

问: 是否可以使用 VSX 从 Check Point 迁移配置?

答: 您可以导出与虚拟系统相关的特定策略包, 一次只能从一个虚拟系统导出。例如, 当您使用 Web 可视化工具 (r75 - r77.30) 导出配置时, 它就会导出所有虚拟系统的策略元素。因此, 请仅保留要迁移的虚拟系统的 NAT 和策略文件, 以及 `index.xml`、`community.xml`、`network_objects.xml` 和 `network.txt` (从要迁移的策略的安全网关), 以便让配置保持完整。

对于 r80, 当您通过 Live Connect 连接到 Check Point 安全管理器时, 选择特定虚拟系统的策略包, 这就是在您选择 Check Point 策略包并推导出配置时要在第 5 步中迁移的策略包。

当您还连接到 Check Point 安全网关时，请提供与 Check Point 策略包对应的正确 Check Point 虚拟系统 Check Point 防火墙包的正确详细信息。

如果仍然遇到问题，请联系思科 TAC 为这些故障创建 TAC 案例。

问: 您能否手动提取 Check Point (r80) 配置?

答: 不能。无法手动提取 Check Point (r80) 配置。使用 Cisco Secure Firewall 迁移工具上的 Live Connect 可导出完整的 r80 配置。当您使用手动变通方法提取配置或使用未在 Cisco Secure Firewall 迁移工具中配置的 Check Point (r80) 配置时，该配置是不完整的，并且也会作为不受支持的配置进行迁移、被部分迁移，甚至导致迁移失败。

有关详细信息，请参阅[导出 Check Point r80 配置文件的程序](#)。

问: 为不同的 Check Point (r80) 部署类型预先配置凭证的方式有哪些?

答: 迁移前，您可以通过以下任何一种方式在 Check Point (r80) 设备上配置凭证:

- [从分布式 Check Point 部署导出](#)
- [从独立 Check Point 部署导出](#)
- [从多域 Check Point 部署导出](#)

问: 我在 Check Point r80 上为 Check Point 安全管理器使用了自定义 API 端口。我必须怎样做才能完全提取配置?

答: 如果您在 Check Point 智能管理器上使用客户 API 端口来使用 Check Point API，请执行以下步骤:

- 在 Live Connect 的 **Check Point 安全管理器**页面上，选中 **Check Point 多域部署**复选框。
- 如果使用多域部署，请添加 Check Point CMA 的 IP 地址和 API 端口详细信息。
- 如果是常规部署，请保留 Check Point 安全管理器的 IP 地址，并输入自定义 API 端口的详细信息。

问: 我有一个 r80.40 版本的 Check Point 网关，并且通过 Live Connect 能够正常提取。但在解析时，我收到了错误消息：“Blocked VSX Feature is UNSUPPORTED in FTD”。我必须怎样做?

答: 之所以出现该错误是因为从 Check Point r80.40 开始弃用了 **fw vsx stat** 命令。在解析 *network.txt* 文件时，Cisco Secure Firewall 迁移工具在执行 **fw vsx stat** 命令后将无法对值进行解析。

解决方法是执行以下步骤:

1. 解压缩 *config.zip* 文件。
2. 打开 *networking.txt* 文件。

以下是样本输出的示例:

```
firewall> fw vsx stat
Deprecated command, Please see sk144112 for alternative
Deprecated commands: cphaprob cpinfo cplic fw ips raidconfig fwaccel
```

按照如下步骤手动进行更换:

```
firewall> fw vsx stat
VSX is not supported on this platform
```

3. 选择所有文件并以 .zip 扩展名将它们压缩。

## 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。