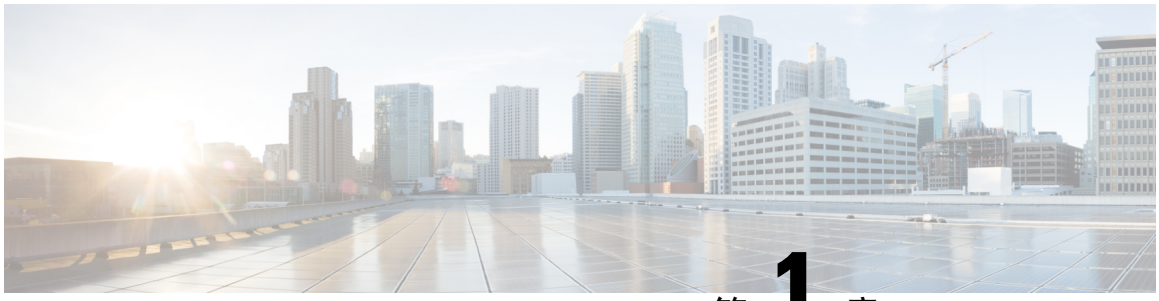
利用 Cisco Secure Firewall 迁移工具将 Check Point 防火墙迁移到 Cisco Secure Firewall Threat Defense

首次发布日期: 2019 年 9 月 6 日

上次修改日期: 2022 年 8 月 11 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

目录



第 1 章

关于迁移

关于防火墙迁移工具

文档

本书 使用 *Cisco Secure Firewall* 迁移工具将 *Check Point* 防火墙迁移到 *Cisco Secure Firewall Threat Defense* 中的所有信息均针对的 Cisco Secure Firewall 迁移工具的最新版本。按照从 Cisco.com 下载防火墙迁移工具中的说明下载防火墙迁移工具的最新版本。

从版本 2.0 开始，防火墙迁移工具支持将 Check Point (CP) 配置 (r75-r77.30) 迁移到 威胁防御。从版本 2.2 开始，防火墙迁移工具支持将 Check Point (CP) 配置 (r80) 迁移到 威胁防御。

防火墙迁移工具

防火墙迁移工具 可将支持的 Check Point 配置转换为支持的 威胁防御 平台。借助防火墙迁移工具，您可以自动迁移支持的 Check Point 功能和策略。您可能必须手动迁移不受支持的功能。

防火墙迁移工具收集 Check Point 信息，解析该信息，最后将其推送到管理中心。在解析阶段中，防火墙迁移工具会生成**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 会列出防火墙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。

防火墙迁移工具可保存您的进度，并允许您在迁移过程中的两个阶段恢复迁移：

- 成功完成 **Check Point** 配置文件解析之后

注释 如果存在解析错误或您在解析之前退出，防火墙迁移工具会要求您从头开始执行该活动。

- **优化、检查和验证**页面

注释 如果您在此阶段退出防火墙迁移工具并重新启动，它会显示**优化、检查和验证**页面。

控制台

当您启动防火墙迁移工具时，系统将打开控制台。控制台提供有关防火墙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防火墙迁移工具日志文件。

在打开和运行防火墙迁移工具时，控制台必须保持打开状态。

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

日志

防火墙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。

在以下位置可找到防火墙迁移工具的日志文件：`<migration_tool_folder>\logs`

资源

防火墙迁移工具会在 `resources` 文件夹中保存一份**迁移前报告**、**迁移后报告**、 Check Point PAN 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

在以下位置可找到未解析文件：`<migration_tool_folder>\resources`

防火墙迁移工具中的搜索

可以搜索防火墙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。防火墙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。防火墙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，防火墙迁移工具支持遥测：端口 8321-8331 和端口 8888。默认情况下，防火墙迁移工具使用端口 8888。要更改端口，请更新 `app_config` 文件中的端口信息。更新后，请确保重新启动防火墙迁移工具，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防火墙迁移工具。

防火墙迁移工具的历史

版本	支持的功能
3.0.1	对于 Check Point，仅支持将 Cisco Secure Firewall 3100 系列作为目标设备。
3.0	如果目标管理中心是 7.2 或更高版本，防火墙迁移工具 3.0 现已支持从 Check Point 迁移到云交付的防火墙管理中心。
2.5.2	防火墙迁移工具 2.5.2 现已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。 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。 • 影子 ACL - 第一个 ACL 完全镜像第二个 ACL 的配置。 **注释** 优化仅适用于 ACP 规则操作的 Check Point 。 如果目标 管理中心 是 7.1 或更高版本，则防火墙迁移工具 2.5.2 支持边界网关协议 (BGP) 和动态路由对象迁移。

版本	支持的功能

2.2	• 提供对 r80 Check Point 操作系统版本的支持
	• 为 Live Connect 提供支持，以从 Check Point (r80) 设备提取配置。
	• 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：
	  • 接口
	  • 静态路由
	  • 对象
	  • 网络地址转换
	  • 访问控制策略
	  • 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**，因为没有路由查找。
	  • 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（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。
	  注释 基于区域的策略的 IPv6 路由查找不受支持。

版本	支持的功能

2.0	• 通过防火墙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。
	• 防火墙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：
	  • 接口
	  • 静态路由
	  • 对象
	  • 访问控制策略
	  • 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（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。
	  • 网络地址转换
	• 支持 Check Point 操作系统版本 r75、r76、r77、r77.10、r77.20 和 r77.30。

防火墙迁移工具的许可

防火墙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。

思科成功网络

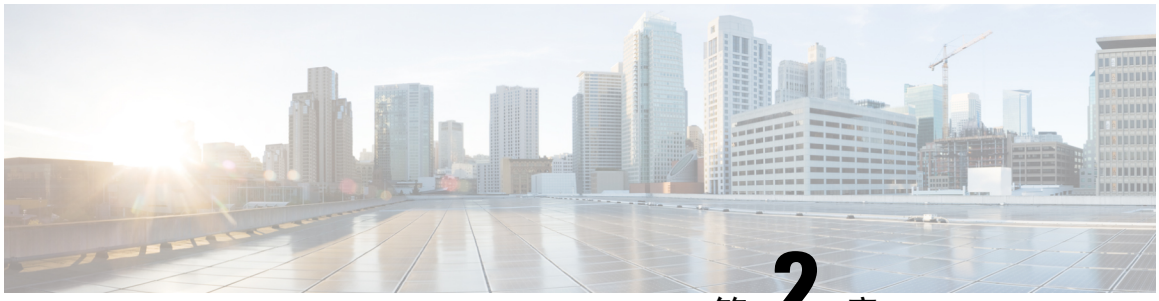
思科成功网络是一项用户启用的云服务。启用思科成功网络时，防火墙迁移工具与思科云之间会建立安全连接以传输使用情况信息和统计信息。数据流遥测提供一种机制，可从防火墙迁移工具选择感兴趣的数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 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更多技术支持服务和监控。
- 帮助思科改善我们的产品。

防火墙迁移工具将建立并始终维护该安全连接，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。

启用和禁用思科成功网络

当您同意在防火墙迁移工具的**最终用户许可协议 (End User License Agreement)** 页面上与思科成功网络共享信息时，可启用思科成功网络。有关详细信息，请参阅 启动防火墙迁移工具，第 18 页。在每次迁移中，您可以从防火墙迁移工具中的**设置 (Settings)** 按钮启用或禁用思科成功网络。有关与思科成功网络共享的特定遥测数据的详细信息，请参阅思科成功网络 - 遥测数据，第 57 页。



第 2 章

准备迁移

适用于防火墙迁移工具的准则和限制

Check Point 配置

您的 Check Point 配置必须满足以下要求：

- Check Point 配置支持迁移，如支持的迁移平台，第 14 页中所述。
- Check Point 版本支持迁移，如支持迁移的软件版本，第 15 页中所述。

（可选）目标 威胁防御 设备

当您迁移到 Cisco Secure Firewall Management Center 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。

- 您的目标 威胁防御 设备必须满足以下要求：
  - 设备满足硬件设备的准则，如此中所述： 适用于威胁防御设备的准则和限制，第 9 页
  - 设备支持作为迁移的目标，如支持的迁移平台，第 14 页中所述。
  - 威胁防御 软件版本支持迁移，如支持迁移的软件版本，第 15 页中所述。
  - 威胁防御 设备已在 管理中心 上注册。

管理中心

- 管理中心软件版本支持迁移，如支持迁移的软件版本，第 15 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
- 防火墙迁移工具 3.0 现在支持迁移到云交付的防火墙管理中心，如云交付的防火墙管理中心迁移，第 69 页中所述。

防火墙迁移工具

- 确保您用来运行防火墙迁移工具的计算机符合相关要求，如防火墙迁移工具的平台要求，第16页中所述。
- 防火墙迁移工具允许您在以下限制内配置批量推送的批处理大小：

配置项目	批处理大小限制	默认值
对象	500	50
ACL	1000	1000
NAT	1000	1000
路由	1000	1000

注释 对于对象，API 批处理大小不能超过 500。防火墙迁移工具将值重置为 50 并继续批量推送。

对于 ACL、路由和 NAT 规则，每个批处理大小不能超过 1000。防火墙迁移工具将值重置为 1000 并继续批量推送。

您可以在 `app_config` 文件中配置批处理大小限制，该文件位于：`<migration_tool_folder>\app_config.txt`.

注释 重启应用以使更改生效。

- 开始从防火墙迁移工具推送配置之后，不要在管理中心中对配置进行任何更改或更新，直至迁移完成。

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，防火墙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，防火墙迁移工具会重置接口配置。如果在策略中使用这些接口，则防火墙迁移工具无法重置它们，因此迁移会失败。

- 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。子接口由防火墙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，则必须至少具有与 Check Point 相同数量的已使用物理接口、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”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。
    - 防火墙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。

- 防火墙迁移工具可以根据 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，防火墙迁移工具不创建子接口，仅允许接口映射。

适用于 Check Point 配置的准则和限制

在转换期间，防火墙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，防火墙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）。

防火墙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 Cisco Secure Firewall Management Center 中。

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。
- 不支持实时防火墙和 VSX。

注释 VSX 不支持任何 Check Point 版本。

如果要从 Check Point VSX 迁移策略，可以导出与虚拟系统相关的特定策略包（每次一个虚拟系统），然后将策略从r77.30或r80或更高版本迁移到 FTD。

注释 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）都会被迁移到防火墙管理中心上的 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，则防火墙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，防火墙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，防火墙迁移工具迁移 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 到防火墙威胁防御）无法使用防火墙迁移工具进行迁移。手动迁移这些配置。
- Check Point 网桥、隧道和防火墙管理中心的别名接口无法迁移。
- 防火墙管理中心不支持嵌套服务对象组或端口组。在转换过程中，防火墙迁移工具会扩展引用的嵌套对象组或端口组的内容。
- 防火墙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防火墙管理中心规则。

Check Point 迁移指南

Check Point 日志选项的迁移遵循防火墙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 **drop** 或 **reject** 操作的规则，防火墙迁移工具会在连接开始时配置日志记录。如果操作是 **permit**，则防火墙迁移工具会在连接结束时配置日志记录。

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
- 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

注释 对于在 Check Point 中配置的在 Check Point 中具有相应 NAT 规则的 ACE，防火墙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，防火墙迁移工具不会映射 IP 地址。因此，在验证防火墙管理中心上迁移的 ACE 和 NAT 配置期间，您必须验证并手动更改与 FTD 数据包流对应的 ACE 规则。

注释 虽然防火墙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

防火墙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 Cisco Secure Firewall Management Center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防火墙迁移工具部分迁移到防火墙管理中心中的 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

防火墙迁移工具不支持对以下 Check Point 配置。如果这些配置在 Cisco Secure Firewall Management Center 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

防火墙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

支持的迁移平台

以下 Check Point 和 威胁防御 平台支持使用 防火墙迁移工具 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 防火墙迁移工具仅支持将独立模式或分布式 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 防火墙迁移工具将源 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
- 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

对于 Microsoft Azure 云，防火墙迁移工具支持迁移到 threat defense virtual。

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。

对于 AWS 云，防火墙迁移工具支持迁移到 threat defense virtual。

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，防火墙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 防火墙迁移工具之前完成 管理中心 或威胁防御虚拟的预先配置前提条件。

注释 防火墙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 防火墙迁移工具之前需要预先配置 IP 网络连接。

支持迁移的软件版本

以下是支持迁移的 Check Point 和 威胁防御 版本：

支持的 Check Point 版本

防火墙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”页面中选择相应的 Check Point 版本。

注释 不支持 VSX。

防火墙迁移工具支持从 Check Point 平台 Gaia 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，防火墙迁移工具 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

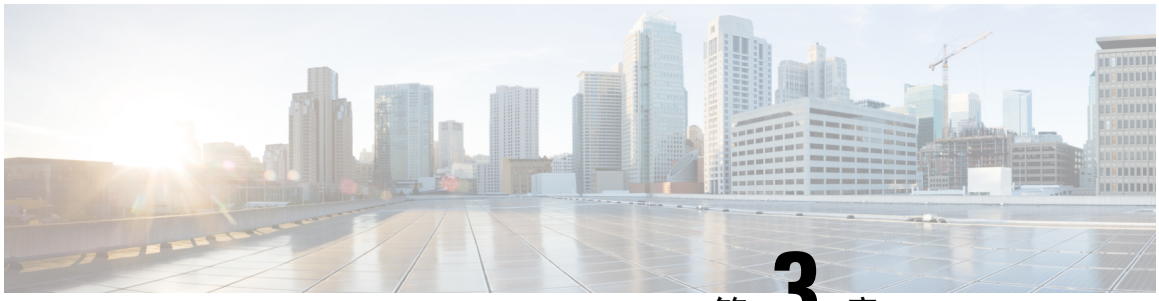
防火墙迁移工具迁移工具建议迁移到正在运行 威胁防御 版本 6.5 及更高版本的设备。

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。

防火墙迁移工具的平台要求

防火墙迁移工具对基础设施和平台的要求如下：

- 运行 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



第 3 章

运行迁移

从 Cisco.com 下载防火墙迁移工具

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，为防火墙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。当防火墙迁移工具启动时，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防火墙迁移工具时，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 下面的防火墙迁移工具。您还可以从 威胁防御 设备下载区域中下载防火墙迁移工具。

步骤 3 将防火墙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 计算机的防火墙迁移工具的相应可执行文件。

下一步做什么

导出 Check Point r77 配置文件

启动防火墙迁移工具

注释 当您启动防火墙迁移工具时，会在单独的窗口中打开控制台。进行迁移时，控制台会显示防火墙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防火墙迁移工具后。

开始之前

- 从 Cisco.com 下载防火墙迁移工具
- 查看并验证适用于防火墙迁移工具的准则和限制，第 7 页部分中的要求。
- 确保您的计算机带有最新版本的 Google Chrome 浏览器以运行防火墙迁移工具。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防火墙迁移工具的文件夹。

步骤 2 执行以下操作之一：

- 在您的 Windows 计算机上，双击防火墙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)**，以允许防火墙迁移工具对您的系统作出更改。

  防火墙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，将防火墙迁移工具 `*.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
  ```

  防火墙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 当您尝试打开防火墙迁移工具时，因为没有可识别的开发人员在 Apple 中注册防火墙迁移工具，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防火墙迁移工具。

步骤 4　在防火墙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。

  注释　　如果您没有 Cisco.com 帐户，请在 Cisco.com 登录页面上创建帐户。

- 使用以下默认凭证登录：
  - **用户名** - admin
  - **密码** - Admin123

如果您已使用 Cisco.com 帐户登录，请继续执行步骤 8。

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**。

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防火墙迁移工具。

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防火墙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。
- 如果必须使用防火墙迁移工具从 Check Point (r77) 提取信息，请继续执行导出 Check Point r77 配置文件。

- 如果必须使用防火墙迁移工具从 Check Point (r80) 提取信息，请继续执行导出 Check Point r80 配置文件。

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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置 ， 第 21 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 工具的同一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。

命令	说明
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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置

使用 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置

步骤 1 从思科防火墙迁移工具软件下载页面下载 FMT-CP-Config-Extractor_v3.0.1-7373 .exe。

步骤 2 打开 FMT-CP-Config-Extractor_v3.0.1-7373 工具，该工具是工作站上有权访问 Check Point Security Gateway 的 Windows 可执行文件 (.exe)。

步骤 3 连接到要使用防火墙迁移工具迁移策略的 Check Point Security Gateway。

要连接它，您需要：

a) IP 地址
b) 端口
c) 用户名
d) 密码

步骤 4 将派生自 FMT-CP-Config-Extractor_v3.0.1-7373 工具的输出文件重命名为 `networking.txt` 文件。

FMT-CP-Config-Extractor_v3.0.1-7373 工具执行以下命令：

- **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**

所有命令均由 FMT-CP-Config-Extractor_v3.0.1-7373 工具在后台执行，输出存储为 a.txt 文件。

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

步骤 5 将 .txt 文件移动到 `Outputs` 文件夹。

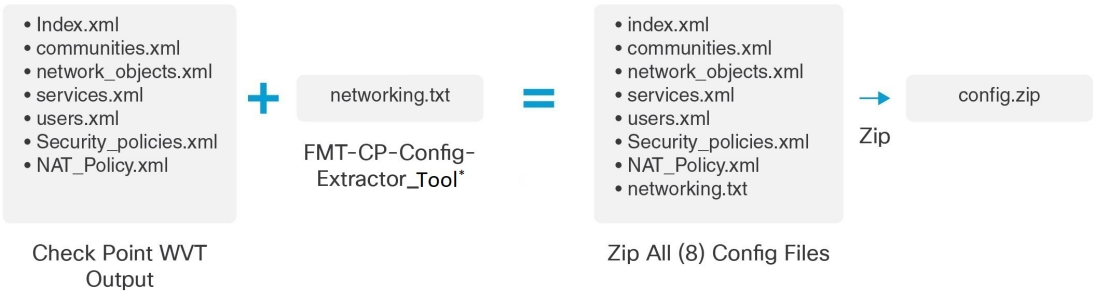
下一步做什么

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 FMT-CP-Config-Extractor_v3.0.1-7373 工具中的一个 .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 FTD 的 Check Point 设备。



*Check Point 提取器版本：FMT-CP-Config-Extractor_v3.0.1-7373

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

导出 Check Point r80 配置文件

注释 只有防火墙迁移工具上的 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

在防火墙迁移工具上使用 Live Connect 提取 Check Point 配置之前，必须在 Check Point (r80) 设备上配置凭证。

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：

a) 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。

b) 导航至**用户管理 (User Management)** 选项卡，然后选择 **用户 (Users)** > **添加 (Add)**。

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**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>

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

在防火墙迁移工具上使用 Live Connect 提取 Check Point 配置之前，必须在 Check Point (r80) 设备上配置凭证。

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

必须使用防火墙迁移工具上的 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：

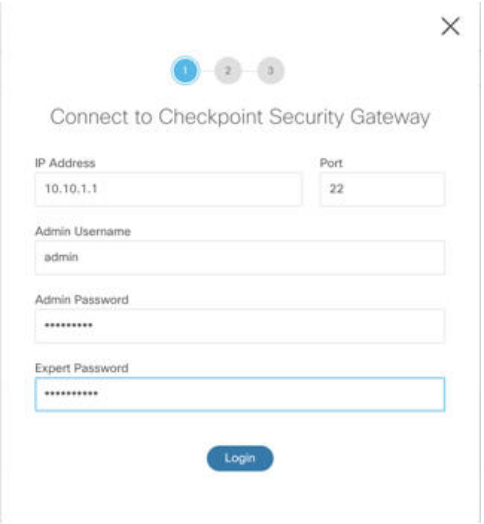
- 从 **Shell** 下拉列表中，选择 */etc/cli.sh*。

- 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。

图 *1:* 连接至 *Check Point* 安全网关 - 多域部署



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：

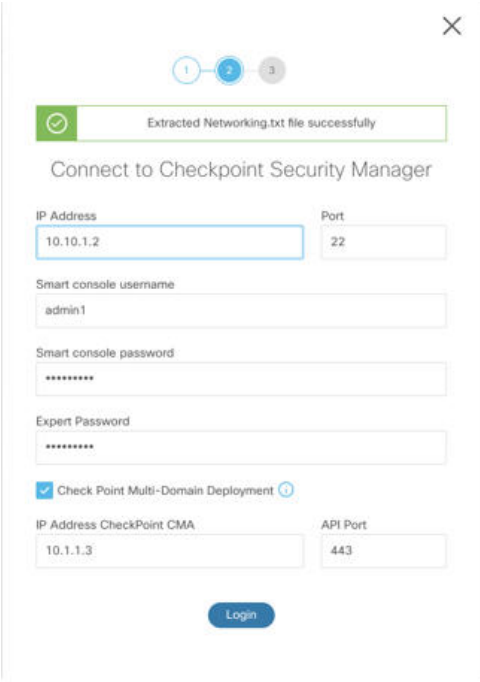
   set expert-password <password>

   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 设备上进行预先配置。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。
- 若使用未在防火墙迁移工具中通过 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)**。

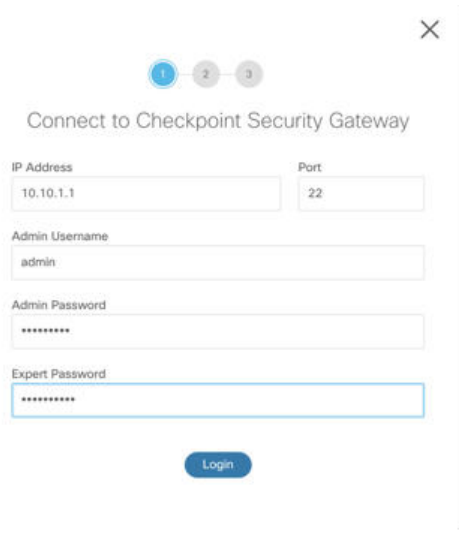
注释 Live Connect 仅适用于 Check Point (r80)。

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



b) 点击 **登录 (Login)**。

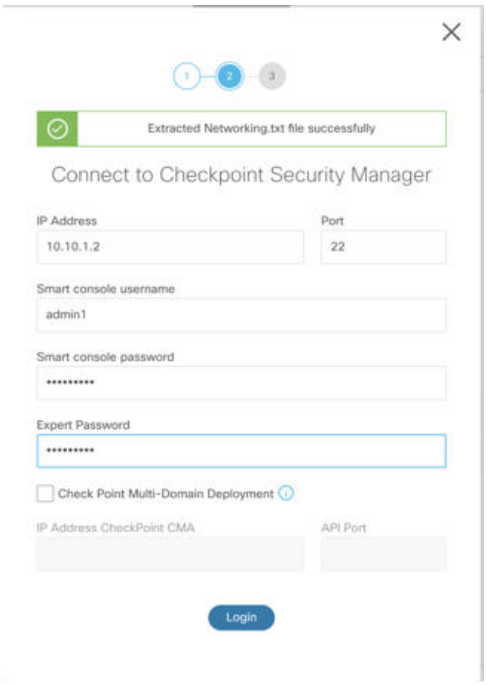
防火墙迁移工具会生成包含设备特定配置（例如接口和路由配置）的 *networking.txt* 文件。将 *networking.txt* 文件存储在防火墙迁移工具当前会话的本地目录中。

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)**。

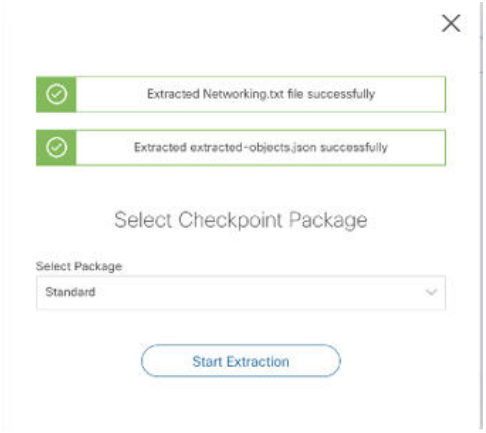
防火墙迁移工具会生成 *Extracted-objects.json* 文件，其中记录 Check Point 安全管理器中可用的完整网络和服务对象配置。

将 *Extracted-objects.json* 文件存储在防火墙迁移工具当前会话的本地目录中。

注释　如果您已将防火墙迁移工具连接到 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。

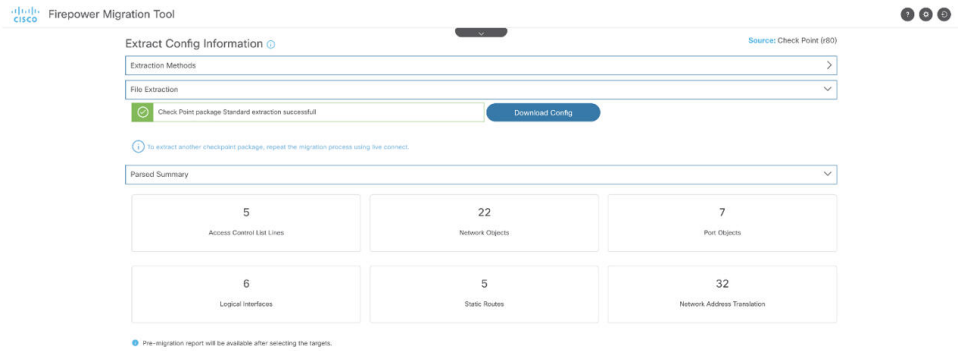
步骤 5 从**选择 Check Point 包 (Select Check Point Package)** 列表中选择要迁移的 Check Point 策略包，然后点击**开始提取 (Start Extraction)**。

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)**。

防火墙迁移工具上传配置文件。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 查看防火墙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

指定防火墙迁移工具的目标参数

指定防火墙迁移工具的目标参数

开始之前

- 获得现场防火墙管理中心的 管理中心 的 IP 地址。
- 从防火墙迁移工具 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，必须如云交付的防火墙管理中心迁移，第 69 页中所述提供区域和 API 令牌。

- （可选）如果要迁移设备特定的配置（例如接口和路由），请将目标 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**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，因为防火墙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。有关生成 CDO API 令牌的信息，请参阅云交付的防火墙管理中心迁移，第 69 页。
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，输入防火墙迁移工具专用帐户的用户名和密码，然后点击**登录 (Login)**。

防火墙迁移工具将登录到 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。

防火墙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**忽略威胁防御并继续 (Proceed without Threat Defense)**，将配置迁移到 管理中心。

当您忽略 威胁防御 并继续时，防火墙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。

步骤 5 点击**继续 (Proceed)**。

根据迁移的目标，防火墙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，防火墙迁移工具会自动从**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 管理中心，防火墙迁移工具会自动从**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。

  注释 当您未选择要迁移到的目标 威胁防御 设备时，**设备配置**部分不可用。

- 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组的性质，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_v3.0.1-7373 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 FMT-CP-Config-Extractor_v3.0.1-7373 工具导出设备配置。

    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。

- 如果目标管理中心是 7.2 或更高版本，防火墙迁移工具支持迁移远程访问 VPN。远程访问 VPN 是一种无需威胁防御即可迁移的共享策略。如果选择使用威胁防御进行迁移，则威胁防御版本应为 7.0 或更高版本。
- （可选）在**优化**部分中，选择**仅迁移引用的对象**，以仅迁移访问控制策略和 NAT 策略中引用的对象。

  注释 当您选择此选项时，不会迁移 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 查看防火墙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（与防火墙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 36 页

查看迁移前报告

注释 防火墙迁移工具 未解析的配置在**迁移前报告**中显示时，其 XML (r75-r77.30) 或 json (r80) 标签与源配置文件中完全相同。

如果您在迁移期间错过下载迁移前报告，请使用以下链接进行下载：

迁移前报告下载终端 — http://localhost:8888/api/downloads/pre_migration_summary_html_format

注释 您只能在 防火墙迁移工具 正在运行时下载报告。

步骤 1 导航到下载**迁移前报告**的位置。

系统也会在 Resources 文件夹中保存**迁移前报告**的一个副本（与防火墙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：

- **总体摘要** - 用于提取 Check Point 配置信息或手动上传到 CP 的方法。

  可成功迁移到 威胁防御 的受支持 Check Point 配置元素以及为迁移选择的特定 Check Point 功能的摘要。

- **出错的配置行** - 因为防火墙迁移工具无法解析而不能成功迁移的 Check Point 配置元素的详细信息。在 Check Point 配置上更正这些错误，导出新配置文件，将新配置文件上传到 防火墙迁移工具，然后再继续。

- **部分支持的配置** - 仅可部分迁移的 Check Point 配置元素的详细信息。这些配置元素包括含高级选项的规则和对象，其中的规则或对象可在无高级选项的情况下迁移。查看这些行，验证 管理中心中是否支持高级选项。如果支持，则计划在使用 防火墙迁移工具 完成迁移后手动配置这些选项。

- **不支持的配置** - 因防火墙迁移工具不支持迁移这些功能而无法迁移的 Check Point 配置元素的详细信息。查看这些行，验证 管理中心 中是否支持每项功能。如果支持，则计划在使用防火墙迁移工具完成迁移后手动配置这些功能。

- **忽略的配置** - 因为不受 管理中心 或防火墙迁移工具支持而被忽略的 Check Point 配置的详细信息。防火墙迁移工具不会解析这些行。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划手动配置这些功能。

有关 管理中心 和 威胁防御 中受支持功能的更多信息，请参阅管理中心配置指南。

步骤 3 如果**迁移前报告**建议执行纠正操作，请在 Check Point 接口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，返回到防火墙迁移工具，然后点击**下一步 (Next)** 以继续迁移。

下一步做什么

通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置

通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置

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**映射威胁防御接口**屏幕上，防火墙迁移工具将检索 威胁防御 设备上的接口的列表。默认情况下，防火墙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。
  - 子接口由防火墙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。
  - 子接口不是由防火墙迁移工具创建的。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，请参阅指定防火墙迁移工具的目标参数 ， 第 33 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**威胁防御接口名称 (Threat Defense Interface Name)** 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。防火墙迁移工具会在 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 当您将每个 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，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。在 Check Point 配置中，访问控制策略和 NAT 策略使用接口名称 (nameif)。在 管理中心中，这些策略使用接口对象。此外，管理中心策略将按以下项分组接口对象：

- 安全区 - 接口只能属于一个安全区。
- 接口组 - 接口可属于多个接口组。

防火墙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 管理中心中的安全区和接口组的更多信息，请参阅接口对象：接口组和安全区 。

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)**。

防火墙迁移工具迁移工具将为这些安全区提供与 ASA 具有 FPS 接口相同的名称（例如 **outside** 或 **inside**），并在名称后显示“(A)”，以指示它是由防火墙迁移工具创建的。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，检查和验证要迁移的配置

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。

此处，防火墙迁移工具会获取 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**屏幕上关闭了防火墙迁移工具防火墙迁移工具，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，防火墙迁移工具会继续从**接口映射**屏幕重新启动。

防火墙迁移工具 ACL 优化概述

防火墙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，防火墙迁移工具 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

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 防火墙迁移工具 会修改对象名称。

ACL 优化的报告

ACL 优化报告中显示以下信息：

- 摘要表 (Summary Sheet) - 显示 ACL 优化的摘要。

Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremote_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- 详细 ACL 信息 (Detailed ACL Information) - 显示基础 ACL 的详细信息。每个 ACL 都带有一个 ACL 类型（Shadow 或 Redundant）标记，用于标识基本 ACL 以便进行比较和与优化类别的关联。

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

将迁移的配置推送到 Cisco Secure Firewall Management Center

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 Cisco Secure Firewall Management Center。

迁移过程中的此步骤会将迁移的配置发送至 Cisco Secure Firewall Management Center。此步骤不会将配置部署到 Cisco Secure Firewall Threat Defense设备。但在此步骤中会擦除 Cisco Secure Firewall Threat Defense上的任何现有配置。

注释 当防火墙迁移工具将迁移的配置发送到 Cisco Secure Firewall Management Center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 Cisco Secure Firewall Management Center。

防火墙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 Cisco Secure Firewall Management Center。

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**迁移前报告**的一个副本（与防火墙迁移工具处于相同的位置）。

步骤 4 如果迁移失败，请仔细查看迁移后报告、日志文件和未解析文件，了解是什么原因导致失败。

您也可以联系支持团队进行故障排除。

迁移失败支持

如果迁移不成功，请联系支持部门。

1. 在**完成迁移 (Complete Migration)** 屏幕上，点击**支持 (Support)** 按钮。

   系统将显示“帮助”支持页面。

2. 选中**支持捆绑包**复选框，然后选择要下载的配置文件。

   注释 默认情况下，系统已选择要下载的日志和 dB 文件。

3. 点击**下载 (Download)**。

   支持捆绑包文件以 .zip 格式下载到您的本地路径。解压缩 Zip 文件夹以查看日志文件、DB 和配置文件。

4. 点击**给我们发送邮件 (Email us)**，通过电子邮件将故障详细信息发送给技术团队。

   您还可以将下载的支持文件附加到电子邮件中。

5. 点击**访问 TAC 页面 (Visit TAC page)**，在思科支持页面上创建 TAC 支持请求。

注释　您可以在迁移过程中随时从支持页面提交 TAC 支持请求。

查看迁移后报告并完成迁移

迁移后报告提供了不同类别下的 ACL 计数、ACL 优化以及对配置文件进行优化的整体视图等详细信息。有关详细信息，请参阅优化，检查和验证要迁移的配置，第 39 页

查看并验证对象：

- **类别**
  - ACL 规则总数（源配置）
  - 考虑优化的 ACL 规则总数。例如，冗余、阴影等。
- 优化的 ACL 计数给出了优化前后计算得出的 ACL 规则总数。

如果您在迁移期间错过下载迁移后报告，请使用以下链接进行下载：

迁移后报告下载终端 — http://localhost:8888/api/downloads/post_migration_summary_html_format

注释　您只能在 防火墙迁移工具 正在运行时下载报告。

步骤 1　导航至下载了**迁移后报告**的位置。

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

- **迁移摘要** - 已成功从 Check Point 迁移到 威胁防御 的配置的摘要信息，其中包括有关 Check Point 接口、管理中心 主机名和域、目标 威胁防御 设备（如果适用）和已成功迁移的配置元素的信息。
- **选择性策略迁移** - 设备配置功能、共享配置功能和优化三个类别中可选择迁移的特定 Check Point 功能的详细信息。
- **Check Point 接口至 FTD 接口映射** - 已成功迁移的接口的详细信息，以及如何将 Check Point 配置上的接口映射到 威胁防御 设备上的接口。确认这些映射符合您的预期。

  注释　本部分不适用于没有目标 威胁防御 设备或者**未**选择迁移**接口**的迁移。
- **源接口名称至 FTD 安全区和接口组** - 已成功迁移的 Check Point 逻辑接口和名称的详细信息，以及如何将它们映射到 威胁防御 中的安全区和接口组。确认这些映射符合您的预期。

  注释　如果**未**选择迁移**访问控制列表**和 **NAT**，则此部分不适用。
- **对象冲突处理** - 已被确定为与 管理中心 中现有对象冲突的 Check Point 对象的详细信息。如果对象具有相同的名称和配置，防火墙迁移工具重新使用 管理中心对象。如果对象具有相同名称但具有不同的配置，则重命名这些对象。仔细检查这些对象，并确认已正确解决冲突。

- **您选择不迁移的访问控制规则、NAT 和路由** - 您选择不让 防火墙迁移工具迁移的规则的详细信息。查看由 防火墙迁移工具禁用且未迁移的这些规则。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
- **部分迁移的配置** - 仅部分迁移的 Check Point 规则的详细信息，包括带有高级选项的规则，其中，在没有高级选项的情况下也可以迁移规则。查看这些行，验证在 管理中心中是否支持高级选项。如果支持，手动配置这些选项。
- **不支持的配置** - 因防火墙迁移工具不支持迁移这些功能而未被迁移的 Check Point 配置元素的详细信息。查看这些行，验证 威胁防御中是否支持每项功能。如果支持，请在 管理中心中手动配置这些功能。
- **展开访问控制策略规则** - 在迁移期间已从一个 Check Point Point 规则扩展到多个 威胁防御 规则的 Check Point 访问控制策略规则的详细信息。
- **对访问控制规则采取的操作**
  - **您选择不迁移的访问规则** - 您选择不让 防火墙迁移工具迁移的 Check Point 访问控制规则的详细信息。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **规则操作有更改的访问规则** - 使用 防火墙迁移工具更改了“规则操作”的所有访问控制策略规则的详细信息。规则操作值包括允许、信任、监控、阻止、阻止并重置。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **应用了 IPS 策略和变量集的访问控制规则** - 应用了 IPS 策略的所有 Check Point 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **应用了文件策略的访问控制规则** - 应用了文件策略的所有 Check Point 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **规则“日志”设置有更改的访问控制规则** - 使用 防火墙迁移工具更改了“日志设置”的 Check Point 访问控制规则的详细信息。日志设置值包括 False、事件查看器、系统日志。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。

注释 未迁移的不受支持的规则可能导致出现问题，使得不必要的流量通过您的防火墙。建议您在 管理中心中配置一个规则来确保 威胁防御阻止此类流量。

注释 如果它要求您在**检查和验证**页面中将 IPS 或文件策略应用于 ACL，则强烈建议您在迁移之前在管理中心上创建策略。使用相同的策略，因为 防火墙迁移工具 从连接的管理中心获取策略。创建新策略并将其分配给多个策略可能会降低性能，也可能导致推送失败。

有关 管理中心和 威胁防御中的受支持功能的更多信息，请参阅管理中心配置指南，版本 6.2.3。

步骤 3 打开**迁移前报告**，并记下您必须在 威胁防御 设备上手动迁移的任何 Check Point 配置项目。

步骤 4 在 管理中心中，执行以下操作：

a) 查看 威胁防御设备的迁移配置，确认所有预期规则和其他配置项目（包括以下内容）均已迁移：

- 访问控制列表 (ACL)
- 网络地址转换规则
- 端口和网络对象

- 路由
- 接口
- 动态路由对象

b) 配置所有未迁移的部分受支持、不受支持、已忽略和已禁用的配置项目和规则。

有关如何配置这些项目和规则的信息，请参阅管理中心配置指南 。以下是需要手动配置的配置项目的示例：

- 平台设置，包括 SSH 和 HTTPS 访问，如威胁防御的平台设置中所述。
- 系统日志设置，如配置系统日志中所述
- 动态路由，如威胁防御路由概述中所述
- 服务策略，如 FlexConfig 策略中所述
- VPN 配置，如威胁防御 VPN 中所述
- 连接日志设置，如连接日志记录中所述

步骤 5 完成检查之后，将已迁移的配置从 管理中心 部署到 威胁防御 设备。

验证**迁移后报告**中是否正确反映了不支持和部分支持的规则的数据。

防火墙迁移工具将策略分配到 威胁防御设备。验证运行配置中是否反映了更改。为帮助您识别已迁移的策略，这些策略的描述信息中包括 Check Point 配置的主机名。

卸载防火墙迁移工具

所有组件均存储在与防火墙迁移工具相同的文件夹中。

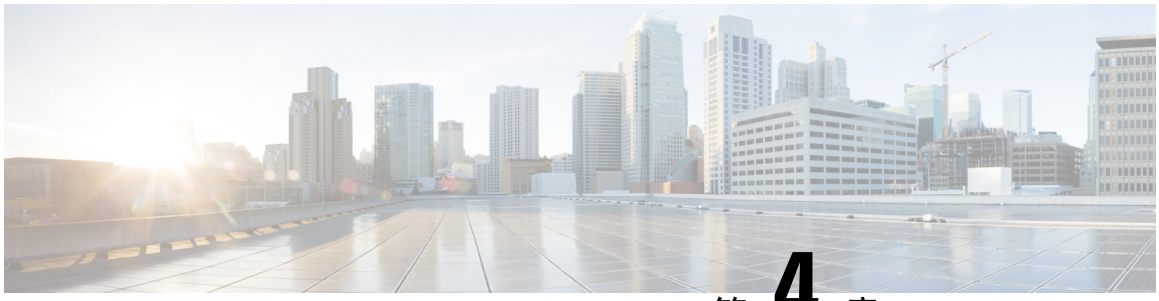
步骤 1 导航至在其中放置防火墙迁移工具的文件夹。

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 删除在其中放置防火墙迁移工具的文件夹。

提示 日志文件与控制台窗口相关联。只要防火墙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。



第 4 章

排除迁移问题

关于防火墙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。
- 防火墙迁移工具在 Check Point Cofig.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。

防火墙迁移工具支持捆绑包

防火墙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。

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，这通常是因为防火墙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为防火墙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
防火墙迁移工具消息	Check Point 配置文件解析出错。 有关解析错误，请参阅查看迁移前报告的错误部分；有关推送阶段发生的推送错误，请参阅查看迁移后报告并完成迁移。
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 文件上传到防火墙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，防火墙迁移工具请求了 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
防火墙迁移工具消息	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，请参阅防火墙迁移工具用户指南。 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，防火墙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
防火墙迁移工具消息	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 FTD 中不受支持

在本示例中，由于 FTD 中的 VSX 功能被阻止，防火墙迁移工具迁移失败。

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
防火墙迁移工具消息	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。

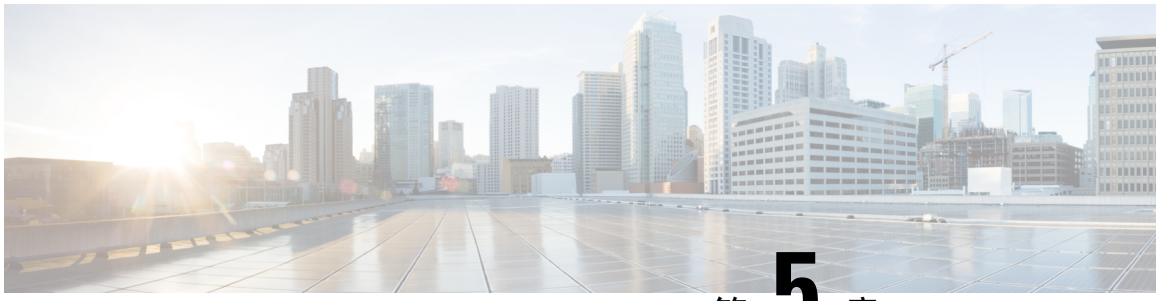
   以下是样本输出的示例：

   ```
   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

防火墙迁移工具常见问题

防火墙迁移工具常见问题

防火墙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 FTD 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_v3.0.1-7373 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： 防火墙迁移工具是否支持带否定单元的 ACE？如果不支持，防火墙迁移工具会如何处理这些规则？

答： 防火墙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： 在通过防火墙迁移工具解析 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_v3.0.1-7373 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防火墙迁移工具。

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。使用防火墙迁移工具上的 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防火墙迁移工具中配置的 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，防火墙迁移工具在执行 **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。

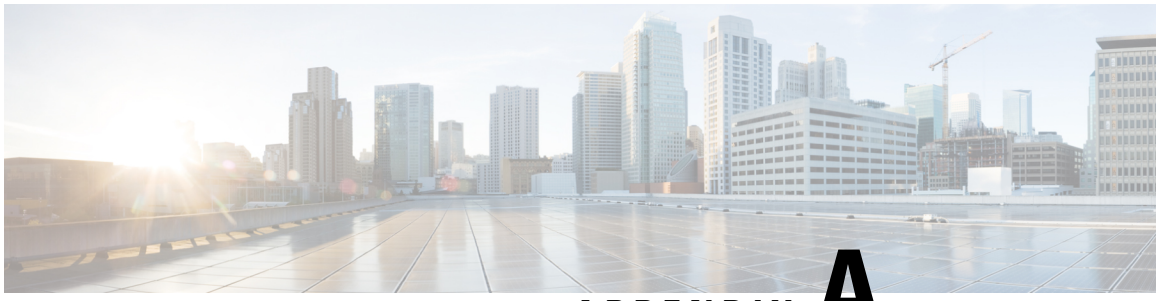
   以下是样本输出的示例：

```
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。



APPENDIX A

思科成功网络 - 遥测数据

思科成功网络 - 遥测数据

每当您在 防火墙迁移工具中启动迁移过程时，相应的遥测数据文件都存储在固定位置。在启用思科成功网络的情况下，当您将迁移的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。如果您使用本地凭证而不是 Cisco.com 帐户凭证登录 防火墙迁移工具，遥测数据不会推送到云，并且数据文件位于以下位置：

`<migration_tool_folder>\resources \ telemetry_data`

下表提供有关遥测数据点、其说明和样本值的信息。

表 *1:* 系统信息

数据点	描述	示例值
操作系统	运行 防火墙迁移工具 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 防火墙迁移工具 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 *2:* 源 *Check Point* 信息

数据点	描述	示例值
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

思科成功网络 - 遥测数据

数据点	描述	示例值
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
Check Point 配置统计信息：		
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
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 *3:* 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

思科成功网络 - 遥测数据

数据点	描述	示例值
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 *4*: 迁移摘要

数据点	描述	示例值
访问控制策略		
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
NAT 策略		
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
更多迁移详细信息...		
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

思科成功网络 - 遥测数据

数据点	描述	示例值
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 *5:* 防火墙迁移工具 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
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	防火墙迁移工具 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,
```

思科成功网络 - 遥测数据


```
  "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": {
```

思科成功网络 - 遥测数据


```
      "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：

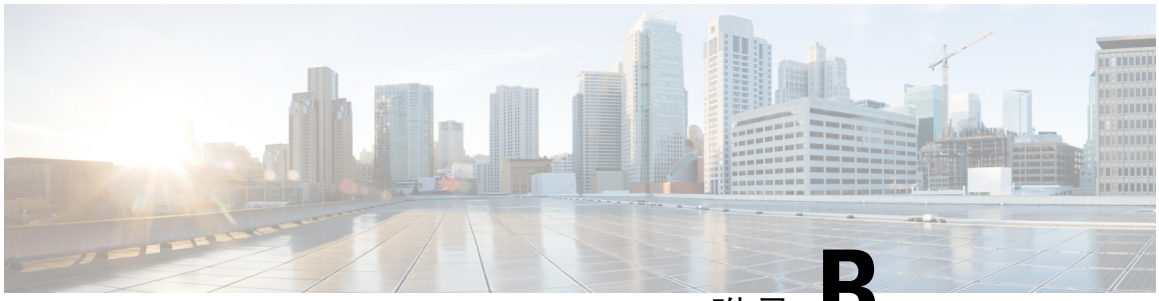

```
{
"Check Point_config_stats":{
        "Ipv6_access_rule_counts":0,
        "Ipv6_bgp_count":0,
        "Ipv6_nat_rule_count":0,
        "Ipv6_network_counts":3,
        "Ipv6_static_route_counts":0,
        "access_rules_counts":726,
        "acl_category_count":0,
        "acl_counts":726,
        "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,
```

思科成功网络 - 遥测数据


```
        "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,
```

思科成功网络 - 遥测数据


```
"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
        }
}
```



附录 B

将 Check Point 迁移到 Threat Defense 2100 - 示例

将 Check Point 迁移到防火墙威胁防御 2100 - 示例

注释 创建迁移完成后可在目标设备上运行的测试计划。

在维护窗口之前执行以下任务

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_v3.0.1-7373 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 防火墙迁移工具。

有关详细信息，请参阅 从 Cisco.com 下载防火墙迁移工具 ， 第 17 页。

步骤 7 启动 防火墙迁移工具 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 指定防火墙迁移工具的目标参数 ， 第 33 页。

步骤 8 将 Check Point 接口与 威胁防御 接口映射。

注释 防火墙迁移工具 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，请参阅通过 Secure Firewall 设备管理器 威胁防御 接口映射 Check Point 配置。

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 防火墙迁移工具 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 查看迁移后报告并完成迁移 ， 第 43 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。

在维护窗口期间执行以下任务

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。请参阅在维护窗口之前执行以下任务 ， 第 65 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，以及防火墙迁移工具未迁移、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 设备的 IP 地址，请执行以下步骤：

将 Check Point 迁移到 Threat Defense 2100 - 示例

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。

将 Check Point 迁移到 Threat Defense 2100 - 示例

附录 C

云交付的防火墙管理中心迁移

云交付的防火墙管理中心迁移

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 3.0 现在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。

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 *6: CDO* 区域和 *URL*

地区	CDO URL
欧洲地区	https://defenseorchestrator.eu/
美国地区	https://defenseorchestrator.com/
总裁	https://www.apj.cdo.cisco.com/

从 CDO 门户生成 API 令牌

要从 CDO 门户生成 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)** 以生成并复制 API 令牌。

云交付的防火墙管理中心迁移

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。