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 8 页中所述。
- Check Point 版本支持迁移，如支持迁移的软件版本，第 9 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 3 页
  - 设备支持作为迁移的目标，如支持的迁移平台，第 8 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 9 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 9 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10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

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。