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。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。

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。