关于迁移

关于防火墙迁移工具

文档

本书中的所有信息 使用 *Cisco Secure Firewall* 迁移工具将 *Fortinet* 迁移到 *Cisco Secure Firewall Threat Defense* 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 2.3 开始，防火墙迁移工具支持将 Fortinet 防火墙配置迁移到 威胁防御。防火墙迁移工具用于将 Fortinet 配置迁移到 威胁防御。

这种 防火墙迁移工具

防火墙迁移工具 可将支持的 Fortinet 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 Fortinet 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 Fortinet 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：

- 已完全迁移、部分迁移、迁移不支持和迁移中忽略的 Fortinet 配置项目
- 出错的 Fortinet 配置行，列出防火墙迁移工具无法识别的 Fortinet CLI；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，将接口映射到 威胁防御 接口，映射应用，映射安全区，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 Fortinet 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**、 Fortinet 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 Fortinet，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 Fortinet 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 Fortinet 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 Fortinet。 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
2.3	• 支持 Fortinet 防火墙操作系统版本 5.0 及更高版本 • 防火墙迁移工具允许将以下 Fortinet 配置元素迁移到 威胁防御： • 接口 • 区域 (Zones) • 静态路由 • 网络对象和组 • 服务对象和组 • 访问控制列表 • NAT 从属对象（IP 池、虚拟 IP） • NAT 规则 • VDOM • 基于时间的对象 - 当防火墙迁移工具检测到通过访问规则引用的基于时间的对象时，防火墙迁移工具会迁移基于时间的对象并映射这些对象与相应的访问规则。根据检查和验证配置页面中的规则验证对象。 **注释** 管理中心 版本 6.6 及更高版本支持基于时间的对象。

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。

免责声明

防火墙迁移工具（简称“工具”）旨在帮助您将受支持的第三方产品配置转换为获得有效许可和支持的平台上的 Cisco Secure Firewall Threat Defense（简称“威胁防御”）配置。该工具创建的安全策略和配置在完成转换后可能需要您手动配置。在实施任何配置之前，您应全权负责检查和测试配置，以确保其准确和完整。本工具按“原样”提供，思科不表示或担保该工具将符合您的业务需求或适合您现有的系统。

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。