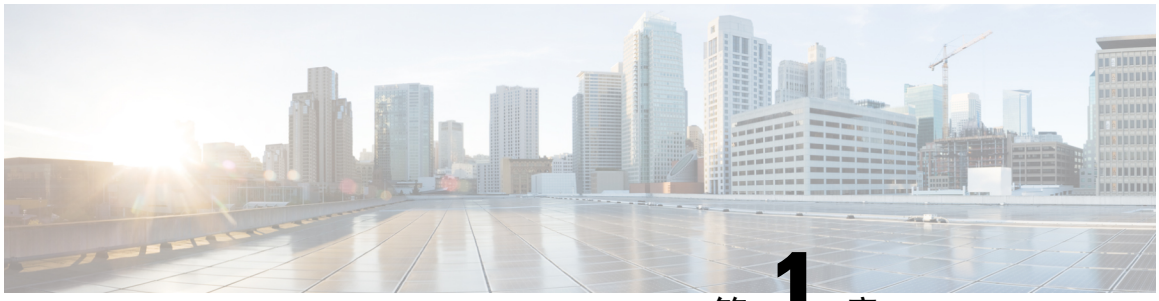
利用迁移工具将 Palo Alto Networks 防火墙迁移到思科多云防御

上次修改日期: 2025 年 7 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

Cisco Secure Firewall 迁移工具使用入门

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。

Cisco Secure Firewall 迁移工具会将受支持的 PAN配置转换为受支持的Cisco Secure Firewall Threat Defense平台 或 多云防御。Cisco Secure Firewall 迁移工具允许您将受支持的 PAN功能和策略自动迁移到威胁防御或多云防御。您必须检查迁移前报告中是否存在任何不受支持的配置，并在迁移后手动配置它们。

Cisco Secure Firewall 迁移工具收集 PAN 信息，对其进行解析，最后将其推送到Cisco Secure Firewall Management Center 或 多云防御 。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 PAN 配置 XML 行
- PAN 会列出 Cisco Secure Firewall 迁移工具无法识别的 PAN XML 行。报告**迁移前报告**和控制台日志中错误部分下的 XML 配置行；这些配置行会阻止迁移

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 迁移工具会将 **迁移前报告**、 **迁移后报告**、 PAN 配置和日志的副本保存在**资 源** 文件夹中。

在以下位置可找到 **resources** 文件夹： *<migration_tool_folder>\resources*

未解析文件

Cisco Secure Firewall 迁移工具会在未解析文件中记录有关其忽略的配置行的信息。当 Cisco Secure Firewall 迁移工具解析 具备FPS 的 ASA PAN 配置文件时，它会创建此文件。

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。

通知中心

所有通知（包括迁移期间弹出的成功消息、错误消息和警告）都在通知中心捕获，并分类为**成功 (Successes)**、**警告 (Warnings)** 和**错误 (Errors)**。在迁移过程中，您可以随时点击右上角的 

图标，查看弹出的各种通知，以及它们在工具中弹出的时间。

Cisco Success Network

Cisco Success Network 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
7.7.10	本版本包含以下新功能： • 您现在可以使用 Cisco Secure Firewall 迁移工具将配置从 Microsoft Azure Native 防火墙迁移到 威胁防御 。有关更多信息和迁移步骤，请参阅使用迁移工具将 Microsoft Azure 本地防火墙迁移到 Cisco Secure Firewall Threat Defense。 • 您现在可以使用 Cisco Secure Firewall 迁移工具将配置从 Check Point 防火墙迁移到 多云防御 。有关更多信息和迁移步骤，请参阅使用迁移工具 将 Check Point 防火墙迁移到思科多云防御 。 • 您现在可以使用 Cisco Secure Firewall 迁移工具将配置从 Fortinet 防火墙迁移到 多云防御 。有关更多信息和迁移步骤，请参阅使用迁移工具 将 Fortinet 防火墙迁移到思科多云防御 。
7.7	本版本包含以下新功能： • 您现在可以使用 Cisco Secure Firewall 迁移工具将配置从 Cisco Secure Firewall ASA 迁移到 多云防御 。有关详细信息和迁移步骤，请参阅 使用迁移工具将 Cisco Secure Firewall ASA 迁移到思科多云防御 。 • 您现在可以使用 Cisco Secure Firewall 迁移工具将配置从 Palo Alto Networks 防火墙迁移到多云防御。有关详细信息和迁移步骤，请参阅使用迁移工具将 Palo Alto Networks 防火墙迁移到思科多云防御 。

版本	支持的功能
7.0.1	

版本	支持的功能
	本版本包含以下新功能和增强功能： • 现在，您可以将配置从您的思科防火墙（如 ASA 和 FDM 管理的设备）和第三方防火墙迁移到 Cisco Secure Firewall 1200 系列设备。 请参阅：Cisco Secure Firewall 1200 系列 • 现在，您可以一次更新多个站点间 VPN 隧道配置的预共享密钥。将**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 页面中的站点间 VPN 表导出到 Excel 工作表，在相应的单元格中指定预共享密钥，然后重新上传工作表。迁移工具从 Excel 中读取预共享密钥并更新表格。 请参阅优化、检查和验证配置 支持迁移：全部 • 现在，您可以选择忽略妨碍迁移的不正确配置，并继续推进迁移的最后阶段。以前，即使单个对象的推送因错误而失败，整个迁移也会失败。现在，您还可以手动中止迁移，以修复错误并重试迁移。 请参阅：将迁移的配置推送到管理中心 支持迁移：全部 • 现在，Cisco Secure Firewall 迁移工具可检测目标威胁防御设备中的现有站点间 VPN 配置，并提示您选择是否要删除它们，而无需登录到管理中心。您可以选择**否 (No)** 并从管理中心手动将其删除，以继续执行迁移。 请参阅优化、检查和验证配置 支持迁移：全部 • 如果您在目标管理中心管理的一台威胁防御设备上配置了现有的中心辐射型拓扑，则可以选择直接从迁移工具中将目标威胁防御设备添加为现有拓扑的辐射之一，而无需在管理中心上手动操作。 请参阅优化、检查和验证配置 支持迁移：Cisco Firewall ASA • 在迁移第三方防火墙时，现在可以选择威胁防御设备作为目标，这些设备是高可用性对的一部分。以前，您只能选择独立的威胁防御设备作为目标设备。 支持的迁移：Palo Alto Networks、Check Point 和 Fortinet 防火墙迁移 • Cisco Secure Firewall 迁移工具现在提供更增强、更直观的演示模式，在每个步骤中都有引导式迁移说明。此外，您还可以看到各种版本的目标威胁防御设备，以便根据自己的要求进行选择和测试。 支持迁移：全部

版本	支持的功能
7.0	本版本包含以下新功能和增强功能： **Cisco Secure Firewall ASA 迁移到 Cisco Secure Firewall Threat Defense** • 现在，您可以在目标管理中心配置威胁防御高可用性 (HA) 对，并将配置从 Cisco Secure Firewall ASA HA 对迁移到管理中心。在**选择目标 (Select Target)** 页面上选择**继续进行高可用性对配置 (Proceed with HA Pair Configuration)**，然后选择主用和备用设备。选择主动威胁防御设备时，请确保管理中心有相同的设备，以便 HA 对配置成功。有关详细信息，请参阅《使用迁移工具将 *Cisco Secure Firewall ASA* 迁移到 *Cisco Secure Firewall Threat Defense*》一书中的为安全防火墙迁移工具指定目标参数。 • 从 ASA 设备迁移站点间 VPN 配置时，现在可以使用威胁防御设备配置站点间中心辐射型 VPN 拓扑。在**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 页面上，在**站点间 VPN 隧道 (Site-to-Site VPN Tunnels)** 下点击**添加中心和辐射拓扑 (Add Hub & Spoke Topology)**。有关详细信息，请参阅《使用迁移工具将 *Cisco Secure Firewall ASA* 迁移到 *Cisco Secure Firewall Threat Defense*》一书中的优化、查看和验证配置。 **Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense** • 现在，您可以将 SSL VPN 和中央 SNAT 配置中的 IPv6 和多接口及接口区域 Fortinet 防火墙迁移到威胁防御设备。有关详细信息，请参阅《使用迁移工具将 *Cisco Secure Firewall ASA* 迁移到 *Cisco Secure Firewall Threat Defense*》一书中的 Fortinet 配置支持。

版本	支持的功能
6.0.1	本版本包含以下新功能和增强功能： **Cisco Secure Firewall ASA 迁移到 Cisco Secure Firewall Threat Defense** • 现在，当您将配置从 Cisco Secure Firewall ASA 迁移到威胁防御时，可以优化网络和端口对象。在**优化、查看和验证配置 (Optimize, Review and Validate Configuration)** 页面中相应的选项卡中查看这些对象，然后点击**优化对象和组 (Optimize Objects and Groups)** 以优化对象列表，然后再将它们迁移到目标管理中心。迁移工具会识别具有相同值的对象和组，并提示您选择保留哪些对象和组。有关详细信息，请参阅优化、检查和验证配置。 **FDM 托管设备迁移到 Cisco Secure Firewall Threat Defense** • 现在，您可以将 DHCP、DDNS 和 SNMPv3 配置从 FDM 管理的设备迁移到威胁防御设备。确保选中**选择功能 (Select Features)** 页面上的 **DHCP** 复选框以及**服务器 (Server)**、**中继 (Relay)** 和 **DDNS** 复选框。有关详细信息，请参阅优化、检查和验证配置。 **Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense** • 现在，除其他对象类型外，您还可以将 URL 对象从 Fortinet 防火墙迁移到威胁防御设备。在迁移期间，查看**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 页面中**对象 (Objects)** 窗口中的 **URL 对象 (URL Objects)** 选项卡。有关详细信息，请参阅优化、检查和验证配置。 **Palo Alto Networks 防火墙到 Cisco Secure Firewall Threat Defense Migration 的迁移** • 现在，除其他对象类型外，您还可以将 URL 对象从 Palo Alto Networks 防火墙迁移到威胁防御设备。确保在迁移期间，查看**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 页面中**对象 (Objects)** 窗口中的 **URL 对象 (URL Objects)** 选项卡。有关详细信息，请参阅优化、检查和验证配置。 **Check Point 防火墙迁移到 Cisco Secure Firewall Threat Defense** • 现在，您可以将端口对象、FQDN 对象和对象组从 Check Point 防火墙迁移到威胁防御设备。在迁移过程中，查看**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 页面中的**对象 (Objects)** 窗口。有关详细信息，请参阅优化、检查和验证配置。

版本	支持的功能
6.0	本版本包含以下新功能和增强功能： **Cisco Secure Firewall ASA 迁移到 Cisco Secure Firewall Threat Defense** • 现在，您可以将 Cisco Secure Firewall 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 **选择功能** 页面中的 **WebVPN** 复选框，并查看 **优化、查看和验证配置** 页面中的新 **WebVPN** 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。 • 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 **选择功能** 页面中的 **SNMP** 和 **DHCP** 复选框。如果您在 Cisco Secure Firewall 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。 • 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 **路由** 磁贴现在还包括 ECMP 区域，您可以在 **优化、查看和验证配置** 页面的 **路由** 选项卡下对其进行验证。 • 现在，您可以将动态隧道从 Cisco Secure Firewall 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 **Map ASA Interfaces to Security Zones**、**Interface Groups, and VRFs** 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。 **FDM 托管设备迁移到 Cisco Secure Firewall Threat Defense** • 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 **选择功能** 页面中的 **平台设置** 和 **文件和恶意软件策略** 复选框。 **Check Point 防火墙迁移到 Cisco Secure Firewall Threat Defense** • 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 **选择功能** 页面中选中 **站点间 VPN 隧道** 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 **不使用 FTD 继续**，则迁移工具不会显示这些配置。 **Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense** • 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 **优化、查看和验证配置** 页面中的 **优化 ACL** 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。

版本	支持的功能
5.0.1	本版本包含以下新功能和增强功能： • 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。 在一种或多种情景具有 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。 有关详细信息，请参阅选择 ASA 安全情景。 • 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 **选择功能** 窗格中，选择要迁移的 VPN 功能。请参阅使用迁移工具将 Palo Alto Networks 防火墙迁移到 Cisco Secure Firewall Threat Defense 和使用迁移工具 将 Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense 指南中的指定 Cisco Secure Firewall 迁移工具的目标参数部分。 • 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。
5.0	• 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种情景迁移配置，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，请参阅选择 ASA 主要安全情景。 • 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 **已解析摘要** 页面的新 **VRF 磁** 贴中检查迁移工具在新 **情景** 磁贴中检测到的情景数量。此外，迁移工具会在将接口映射 **到安全区域和接口组** 页面中显示这些 VRF 映射到的接口。 • 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，请参阅使用防火墙迁移工具中的演示模式。 • 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。

版本	支持的功能
4.0.3	Cisco Secure Firewall 迁移工具 4.0.3 包括漏洞修补和以下新增强功能： • 迁移工具现在提供增强的 **应用映射** 屏幕，用于将 PAN 配置迁移到威胁防御。有关详细信息，请参阅使用迁移工具将 *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。
4.0.2	Cisco Secure Firewall 迁移工具 4.0.2 包括以下新功能和增强功能： • 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 **Settings** > **Send Telemetry Data to Cisco?** 。

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， 安全云控制 租户和 多云防御 必须具有所需的许可证。

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

迁移到思科的要求和必备条件 多云防御

要将配置从 迁移到 多云防御，请确保满足以下要求和前提条件：

- 您有一个 安全云控制 租户，并已在其上启用了 多云防御 。
- 您已购买 多云防御所需的操作许可证。

注释 您甚至可以在 90 天的免费试用期间迁移配置到 多云防御，因为试用体验提供了付费订用的全部功能。

- 您已掌握多云防御的基本 URL 和安全云控制租户名称。
- 您已创建 API 密钥，并复制了 多云防御 在您创建 API 密钥时生成的 **API 密钥 ID** 和 **API 密钥秘密** 。请参阅在 多云防御 中创建 API 密钥 了解更多信息。

PAN 防火墙配置支持 多云防御

支持的配置

Cisco Secure Firewall 迁移工具支持以下 PAN配置的迁移到 多云防御：

- 访问控制列表
- 网络对象
- 端口对象
- FQDN 对象
- 服务对象
- URL 对象

迁移到多云防御的指南和限制

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，而不管它们在转换期间是否用于规则或策略。Cisco Secure Firewall 迁移工具提供优化功能，允许您排除未使用的对象（任何 ACL 中未引用的对象）的迁移。

支持的 PAN 配置

Cisco Secure Firewall 迁移工具支持以下 PAN配置的迁移到 多云防御：

- 访问控制列表
- 网络对象和组
- 服务对象
- URL 对象
- 服务对象组

- 端口对象
- 完全限定域名 (FQDN) 对象

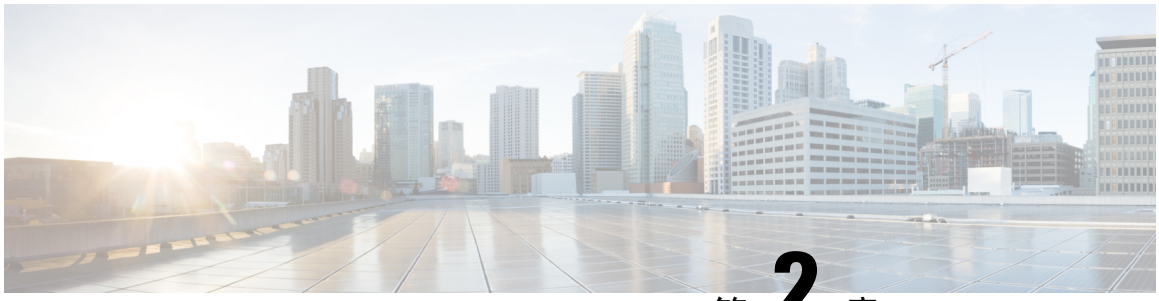
支持迁移的软件版本

Cisco Secure Firewall 迁移工具支持将PAN防火墙操作系统版本 8.0 及更高版本迁移到多云防御 。

相关文档

本部分总结了各种 多云防御相关的用户指南：

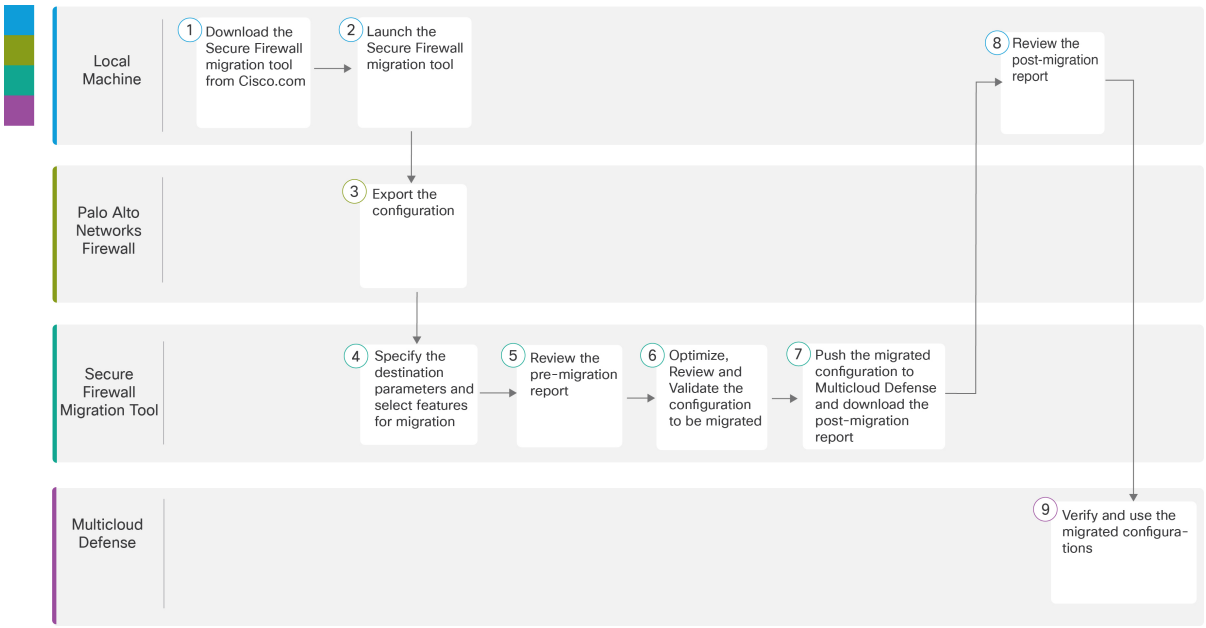
- 思科多云防御用户指南
- 多云防御版本说明
- 多云防御命名约定
- 多云防御组件的推荐版本
- 思科安全调配和管理中的多云防御



第 2 章

PAN 到 多云防御的迁移工作流程

端到端程序



	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 Cisco.com 下载 Cisco Secure Firewall 迁移工具。
2	本地计算机	在本地计算机中，双击从 Cisco.com 下载的应用程序文件来启动 Cisco Secure Firewall 迁移工具。

	工作空间	步骤
3	Palo Alto Networks 防火墙	导出配置文件：要从 Palo Alto Networks 防火墙导出配置，请参阅从 Palo Alto Networks 防火墙导出配置，第 20 页。
4	Cisco Secure Firewall 迁移工具	在此步骤中，您可以指定多云防御的目标参数。有关详细步骤，请参阅 为多云防御指定目标参数，第 21 页。
5	Cisco Secure Firewall 迁移工具	导航到下载迁移前报告的位置并查看报告。有关详细步骤，请参阅 查看迁移前报告，第 23 页。
6	Cisco Secure Firewall 迁移工具	优化并仔细检查配置并验证其是否正确。有关详细步骤，请参阅优化、检查和验证要迁移的配置，第 24 页。
7	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多云防御，并允许您下载迁移后报告。有关详细步骤，请参阅 推送配置到多云防御，第 26 页。
8	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 查看迁移后报告并完成迁移，第 27 页。
9	多云防御	验证迁移的配置，并根据需要在配置网关时使用这些配置。

迁移的前提条件

在迁移 PAN 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。

如果您想使用安全云控制上托管的迁移工具的云版本，请跳至步骤 4。

过程

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。

确保下载适用于 Windows 或 macOS 计算机的 Cisco Secure Firewall 迁移工具的相应可执行文件。

步骤 4 如果您是 安全云控制 用户并希望使用其上托管的迁移工具，请登录您的 安全云控制 租户，然后在左侧窗格中导航至 **管理 (Administration)** > **迁移 (Migration)** > **防火墙迁移工具 (Firewall Migration Tool)** 以创建迁移实例。

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 安全云控制 上托管的迁移工具的云版本，请跳至 从 Palo Alto Networks 防火墙导出配置 。

注释 当您启动 Cisco Secure Firewall 迁移工具的桌面版本时，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
- 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。

过程

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。

  注释
  确保在浏览器中禁用所有弹出窗口阻止程序，因为它们可能阻止显示登录弹出窗口。

  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：

- 如果必须使用 Cisco Secure Firewall 迁移工具从 PAN 防火墙提取信息，请继续执行从 Palo Alto Networks 防火墙导出配置。

在 Cisco Secure Firewall 迁移工具中使用演示模式

当您启动 Cisco Secure Firewall 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 、演示 FTD 设备以及 多云防御 ）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，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 Cisco Secure Firewall 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。

从 Palo Alto Networks 防火墙导出配置

可以通过以下方式导出配置文件：

Palo Alto 防火墙的配置文件（并非由 Panorama 管理）

按照以下步骤从网关提取配置：

过程

步骤 1 导航至**设备** > **设置** > **操作**，然后选择**保存指定配置** <*file_name.xml*>。

步骤 2 点击**确定 (Ok)**。

步骤 3 导航至**设备 (Device)** > **设置 (Setup)** > **操作 (Operations)**，然后点击**导出指定配置 (Export Named Configuration)**。

步骤 4 选择 <*file_name.xml*> 文件。

步骤 5 点击**确定 (Ok)**。

步骤 6 选择包含您运行的配置 <*file_name.xml*> 的 XML 文件，然后点击**确定 (Ok)** 以导出配置文件。

步骤 7 将导出的文件保存到防火墙外部的一个位置。您可以使用此备份上传到 Cisco Secure Firewall 迁移工具来迁移配置。

步骤 8 （可选）如果在您的 NAT 策略中，目标 NAT 具有相同的源和目标区域，请执行以下步骤：

a) 从防火墙上的 CLI 运行 **show routing route** 命令。

b) 将路由表复制到 *.txt* 文件。

c) 将 *.txt* 文件添加到您将从中压缩 .txt 和 .xml 文件以及 *panconfig.xml* 的文件夹中。

这些步骤对于迁移并非强制性的。如果不执行这些步骤，目标区域将不会在 Cisco Secure Firewall 迁移工具迁移期间映射，并将包括在迁移报告中。

注释

使用 **show routing route** 命令提取路由表详细信息。将提取的输出粘贴到记事本中。

Palo Alto 防火墙的配置文件（由 Panorama 管理）

如果您的设备是由 Panorama 管理的，则必须从网关提取配置。合并 Panorama 配置和网关并提取配置。

在 Cisco Secure Firewall 迁移工具用户界面中，执行以下操作：

开始之前

使用超级用户帐户来登录 Palo Alto 防火墙 Web UI。

过程

步骤 1 导航到**设备 (Device)** > **支持 (Support)** > **技术支持文件 (Tech Support File)**。

步骤 2 点击**生成技术支持文件 (Generate Tech Support File)**。

步骤 3 生成的文件可用后，点击**下载技术支持文件 (Download Tech Support File)**。

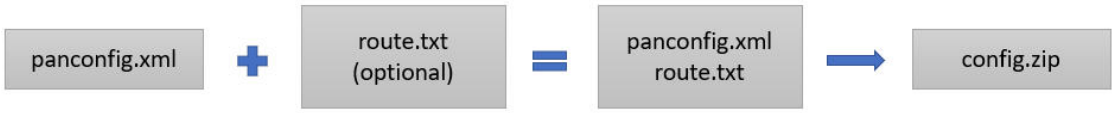
步骤 4 解压缩并解压缩文件，然后导航到路径 *\opt\pancfg\mgmt\saved-configs* 以检索 *mapped-running-config.xml* 文件。

下一步做什么

压缩导出的文件

压缩导出的文件

导出 Palo Alto 网关防火墙的 *panconfig.xml* 以及 *route.txt* （如果您的 NAT 规则具有相同的源区域和目标区域）。



为 多云防御指定目标参数

开始之前

- 确保您有一个具有多云防御的安全云控制租户已启用。
- 确保您已购买 多云防御 所需的运营许可证

注释 您甚至可以在 90 天的免费试用期间迁移配置到 多云防御，因为试用体验提供了付费订用的全部功能。

- 确保您已获取多云防御的基本 URL 和 安全云控制租户名称。
- 确保您已创建 API 密钥，并且还复制了创建 API 密钥时多云防御生成的 **API 密钥 ID** 和 **API 密钥密码** 。请参阅在 多云防御 中创建 API 密钥 了解更多信息。

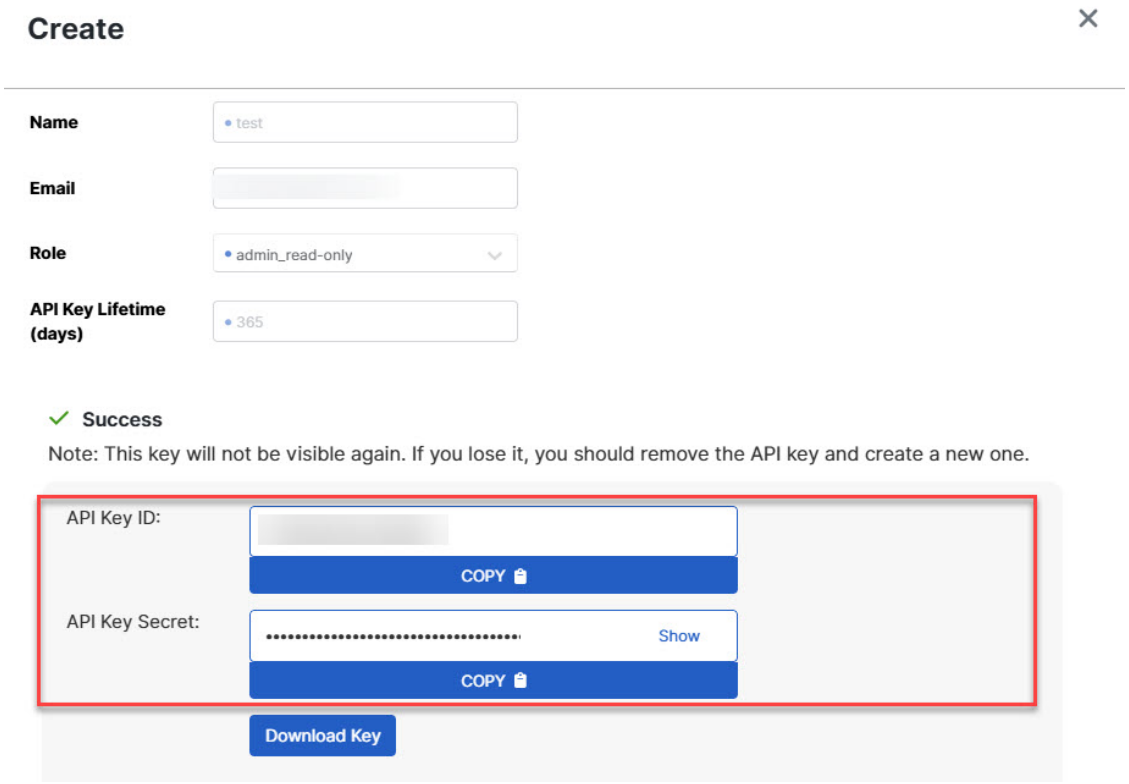
过程

步骤 1 在 **上选择目标** 窗口，选择**多云防御**。

步骤 2 在相应字段中指定以下参数以启用迁移工具和 多云防御之间的连接：

- **输入基本 URL**：这是您连接到 多云防御 控制器时在浏览器上看到的基本 URL。例如，当您在控制器仪表板中时，复制浏览器上的链接，但不包括 **/dashboard** 部分。URL 看起来像 https://xxxx.mcd.apj.cdo.cisco.com
- **输入租户姓名**：您的安全云控制租户的姓名。当您在多云防御窗口中时，从右上角的配置文件下拉菜单中复制它，或者如果您在安全云控制窗口中，则从**管理 (Administration)** > **常规设置 (General Settings)**中复制它。
- **输入 API 密钥 ID**：当您通过导航到**系统和大客户** > **API 密钥**创建 API 密钥时多云防御控制器生成的 **API 密钥 ID**。指定密钥的名称、您的电子邮件地址、您希望 API 密钥具有的角色以及 API 密钥的有效期以生成密钥。默认密钥有效期设置为 365 天。
- **输入 API Key 密码**：创建 API Key 时多云防御控制器生成的 **API Key 密码**。

  注释
  确保在创建 API 密钥时同时复制 **API 密钥 ID**和 **API 密钥密码**。如果您错过复制它们，请删除您创建的 API 密钥，生成一个新的，并确保这次复制它们。



步骤 3 单击“**连接**”并等待接收“**成功收集**”消息，该消息确认连接尝试多云防御成功。

步骤 4 通过**选择功能**，您可以选择要迁移到多云防御的配置。默认情况下，**访问控制**和**仅迁移参考对象**复选框默认处于选中状态。

请注意，此迁移不支持源防火墙的其他配置（例如接口和路由）。

步骤 5 点击 **继续** 并 **开始转换**。等待迁移工具分析源配置。

步骤 6 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 7 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）。

步骤 8 点击**下一步 (Next)**。

查看迁移前报告

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 Cisco Secure Firewall 迁移工具正在运行时下载报告。

过程

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：

- 可成功迁移到威胁防御的受支持的设备配置元素或多云防御以及为迁移选择的特定功能摘要。
- **有错误的配置行** - 由于Cisco Secure Firewall 迁移工具无法解析而无法成功迁移的配置元素的的详细信息。在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Cisco Secure Firewall 迁移工具，然后再继续。
- **忽略的配置** - 因为不受 多云防御 或 Cisco Secure Firewall 迁移工具支持而被忽略的 配置的详细信息。Cisco Secure Firewall 迁移工具不会解析这些行。查看这些行，验证 多云防御中是否支持每项功能。如果支持，则计划手动配置这些功能。

步骤 3 如果**迁移前报告**建议执行纠正操作，请在接口上完成这些纠正操作，重新导出配置文件，将更新的配置文件上传，然后再继续。

步骤 4 在您的 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**一步** 以继续迁移。

优化、检查和验证要迁移的配置

开始之前

“优化、审查和验证配置”页面可让您审查和验证即将迁移到目标多云防御的配置参数。在此步骤中，迁移工具会对照多云防御上的现有配置验证配置，并就成功迁移所需执行的更改提出建议，例如关联访问控制规则以及重命名对象以避免目标 多云防御上重复。

验证后，闪烁的选项卡将指示需要在该选项卡上执行操作。

过程

步骤 1 在列出所有 **访问控制** 列表 (ACL) 条目的访问控制选项卡上，您可以执行以下操作：

- 点击 **优化 ACL**，以便让迁移工具识别所有影子和冗余 ACL，并选择是将它们作为已禁用的 ACL 进行迁移，还是将其排除在迁移之外。

  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：

  - 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。

点击“**继续**”开始优化流程。

- 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，以便更轻松地映射回到配置文件。例如，如果 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。

- 如果您不想迁移或希望迁移某些处于禁用状态的ACL，请选中相应行的复选框，点击**迁移**，然后选择相关选项。点击 ”**选中所有条目**“ 复选框以执行批量更改。

步骤 2 在 **对象 (Objects)** 选项卡上，您可以执行以下操作：

选择以下选项卡并查看映射：

- 网络对象
- 端口对象
- FQDN 对象
- URL 对象

如果要重命名对象，请选中对象行的复选框，点击 **操作**，然后选择 **重命名**。点击 ”**选中所有条目**“ 复选框以执行批量更改。

步骤 3 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 多云防御，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 多云防御 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 多云防御 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 4 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 多云防御对象冲突。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 5 当验证完成并且**验证状态**对话框显示消息**验证成功**时，继续将配置推送至多云防御。

推送配置到多云防御

开始之前

如果您还未成功验证配置和解决所有对象冲突，则不能将配置推送到 多云防御。

注释 当 Cisco Secure Firewall 迁移工具正在将配置发送到 多云防御时，请勿更改任何配置或部署到任何设备。

过程

步骤 1 在**验证状态**对话框中，查看验证摘要。

步骤 2 单击“**推送配置**”将源防火墙配置发送到多云防御。

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 多云防御。

注释
如果在批量推送配置时出现配置错误，迁移工具会发出警告，提示您中止迁移以手动修复错误，或继续迁移以剔除错误配置。您可以选择查看有错误的配置，然后选择**继续迁移 (Continue with migration)** 或**中止 (Abort)**。如果中止迁移，可以下载故障排除捆绑包，并与思科 TAC 共享以进行分析。

如果继续迁移，迁移工具会将迁移视为部分成功迁移。您可以下载迁移后报告，查看因推送错误而未迁移的配置列表。

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。

迁移后报告的副本也保存在与 Cisco Secure Firewall 迁移工具位于同一位置的资源文件夹中。

步骤 4 如果迁移失败，请仔细查看迁移后报告、日志文件和未解析的配置文件，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

开始之前

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。

过程

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，了解您的源配置是如何迁移的。

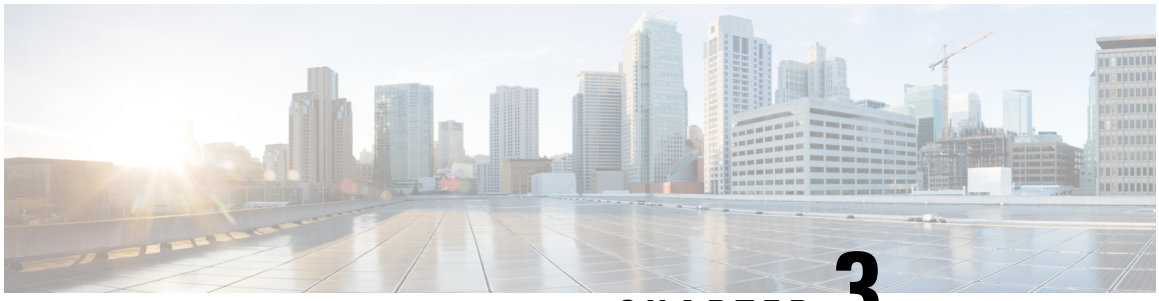
1. **迁移摘要**— 从源防火墙成功迁移到 多云防御的配置摘要。

2. **对象冲突处理** - 已确定与多云防御中现有对象冲突的对象的详细信息。如果对象具有相同的名称和配置，Cisco Secure Firewall 迁移工具重新使用 多云防御对象。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。
3. **您选择不迁移的访问控制规则** - 您选择不使用 Cisco Secure Firewall 迁移工具迁移的规则的详细信息。查看由 Cisco Secure Firewall 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。
4. **部分迁移的配置** - 仅部分迁移的规则的详细信息，包括带有高级选项的规则（无需高级选项即可迁移）。查看这些行，验证在 多云防御中是否支持高级选项。如果支持，手动配置这些选项。
5. **不支持的配置** - 未迁移的源防火墙配置元素的详细信息，因为 Cisco Secure Firewall 迁移工具不支持这些功能的迁移。查看这些行，验证 多云防御中是否支持每项功能。如果支持，请在 多云防御中手动配置这些功能。
6. **扩展的访问控制策略规则** - 迁移期间从单点规则扩展到多个多云防御规则的源防火墙访问控制策略规则的详细信息。
7. **对访问控制规则采取的操作**
   - **您选择不迁移的访问规则** - 您选择不使用 Cisco Secure Firewall 迁移工具迁移的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，您可以在 多云防御 中手动配置这些规则。
   - **规则操作有更改的访问规则** - 使用 Cisco Secure Firewall 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，您可以在 多云防御 中手动配置这些规则。

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。我们建议您配置一条规则多云防御以确保此流量被阻止。

步骤 3 打开**迁移前报告**并记下必须在多云防御上手动迁移的任何配置项。

步骤 4 验证并确保所有迁移的配置参数在多云防御上均可用。



CHAPTER 3

思科成功网络 - 遥测数据

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。

当您将迁移的 配置推送到管理中心或多云防御时，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 *1:* 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

思科成功网络 - 遥测数据

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 *2:* 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 *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

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
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		

思科成功网络 - 遥测数据

数据点	描述	示例值
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
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: 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 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 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

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。