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

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。