



利用 **Cisco Secure Firewall** 迁移工具将 **Fortinet** 防火墙迁移到 **Cisco Secure Firewall Threat Defense**

首次发布日期: 2019 年 9 月 6 日

上次修改日期: 2022 年 8 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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. 保留所有权利。



目录

第 1 章

关于迁移 1

- 关于防火墙迁移工具 1
- 防火墙迁移工具的历史 3
- 防火墙迁移工具的许可 4
- 免责声明 4

第 2 章

准备迁移 5

- 适用于防火墙迁移工具的准则和限制 5
- 适用于 Fortinet 防火墙配置的准则和限制 7
- 适用于威胁防御设备的准则和限制 10
- 支持的迁移平台 10
- 支持迁移的软件版本 11
- 防火墙迁移工具的平台要求 12

第 3 章

运行迁移 13

- 从 Cisco.com 下载防火墙迁移工具 13
- 启动防火墙迁移工具 14
- 从 Fortinet 防火墙导出配置 15
 - 从 Fortinet 防火墙 GUI 导出 Fortinet 防火墙配置 16
 - 从 FortiManager 导出 Fortinet 防火墙配置 16
- 上传 Fortinet 配置文件 17
- 指定防火墙迁移工具的目标参数 18
- 查看迁移前报告 20
- 通过 Secure Firewall 设备管理器 威胁防御 接口映射 Fortinet 配置 21

	将 Fortinet 接口映射到安全区	22
	优化，检查和验证要迁移的配置	23
	ACL 优化的报告	24
	将迁移的配置推送到 Cisco Secure Firewall Management Center	26
	查看迁移后报告并完成迁移	27
	卸载防火墙迁移工具	29
<hr/>		
第 4 章	排除迁移问题	31
	关于防火墙迁移工具的故障排除	31
	用于排除故障的日志和其他文件	32
	Fortinet 文件上传失败故障排除	32
<hr/>		
第 5 章	防火墙迁移工具常见问题	33
	防火墙迁移工具常见问题	33
	防火墙迁移工具常见问题解答	33
<hr/>		
附录 A:	思科成功网络 - 遥测数据	37
	思科成功网络 - 遥测数据	37
<hr/>		
附录 B:	将 Fortinet 迁移到 Threat Defense 2100 - 示例	43
	将迁移到防火墙威胁防御 2100 - 示例	43
	在维护窗口之前执行以下任务	43
	在维护窗口期间执行以下任务	44
<hr/>		
附录 C:	云交付的防火墙管理中心迁移	45
	云交付的防火墙管理中心迁移	45



第 1 章

关于迁移

- [关于防火墙迁移工具，第 1 页](#)
- [防火墙迁移工具的历史，第 3 页](#)
- [防火墙迁移工具的许可，第 4 页](#)
- [免责声明，第 4 页](#)

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	<p>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。</p> <p>ACL 优化支持以下 ACL 类型：</p> <ul style="list-style-type: none"> • 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。 <p>注释 优化仅适用于 ACP 规则操作的 Fortinet。</p> <p>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。</p>

版本	支持的功能
2.3	<ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • 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。 <p>注释 管理中心 版本 6.6 及更高版本支持基于时间的对象。</p>

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。



第 2 章

准备迁移

- 适用于防火墙迁移工具的准则和限制，第 5 页
- 适用于 Fortinet 防火墙配置的准则和限制，第 7 页
- 适用于威胁防御设备的准则和限制，第 10 页
- 支持的迁移平台，第 10 页
- 支持迁移的软件版本，第 11 页
- 防火墙迁移工具的平台要求，第 12 页

适用于防火墙迁移工具的准则和限制

Fortinet 配置

您的 Fortinet 配置必须满足以下要求：

- Fortinet 配置支持迁移，如 [支持的迁移平台](#)，第 10 页 中所述。
- Fortinet 版本支持迁移，如 [支持迁移的软件版本](#)，第 11 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 10 页
 - 设备支持作为迁移的目标，如[支持的迁移平台](#)，第 10 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 11 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 11 页中所述。
- 您已获取并安装 威胁防御 的智能许可证，包括您计划从 Fortinet 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](#)，第 45 页中所述。

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 12 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 Fortinet 防火墙配置的准则和限制

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，而无论它们是否用于规则或策略。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 和 NAT 中未引用的对象）。

防火墙迁移工具处理如下不受支持的对象和规则：

- 不受支持的接口、对象、NAT 规则和路由不会被迁移。
- 不受支持的 ACL 规则将作为禁用的规则迁移到管理中心。

Fortinet 防火墙配置文件

您可以手动获取 Fortinet 防火墙配置文件。

您手动导入到防火墙迁移工具中的 Fortinet 防火墙配置文件必须满足以下要求：

- 具有从 Fortinet 设备导出的运行配置。防火墙迁移工具支持从全局和每 VDOM 导出进行配置备份。有关详细信息，请参阅[从 Fortinet 防火墙导出配置](#)。
- 仅包含有效的 Fortinet 防火墙配置。
- 不包含语法错误。
- 具有扩展名为 .conf 或 .txt 的文件类型。
- 使用 UTF-8 文件编码。
- 尚未手工编码或手动更改。如果您修改了 Fortinet 防火墙配置，则建议您在 Fortinet 防火墙设备上测试修改后的配置文件，以确保它是有效的配置。

Fortinet 防火墙配置限制

源 Fortinet 防火墙配置的迁移存在以下限制：

- 系统配置未迁移。
- 防火墙迁移工具不支持迁移被应用于 50 个或更多接口的单个 ACL 策略。您必须手动迁移已应用于超过 50 个或更多接口的 ACL 策略。
- 您无法将 Fortinet 防火墙配置（例如动态路由和 VPN）迁移到威胁防御。手动迁移这些配置。
- 不支持类型为虚拟线路、冗余接口、隧道接口、vdom-link 和 SDwan 接口或区域的 Fortinet 防火墙接口，它们不会被迁移。

Fortinet 硬件或软件交换机逻辑接口将作为 FTD L3 接口进行迁移。硬件或软件交换机成员接口不会使用防火墙迁移工具来进行迁移。

- 不支持迁移通配符 FQDN、通配符 IP、动态对象和排除组等对象。
- 无法迁移处于透明模式或透明 VDOM 的 Fortinet 防火墙设备。

- 管理中心不支持嵌套服务对象组和端口组。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。
- 防火墙迁移工具将一行中有源端口和目标端口的扩展服务对象或组拆分为跨多行的不同对象。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管理中心规则。

Fortinet 防火墙迁移指南

防火墙迁移工具会对威胁防御配置使用最佳实践。

ACL 日志迁移选项遵循对应于威胁防御的最佳实践。根据源 Fortinet 防火墙配置启用或禁用规则的日志选项。对于使用 **deny** 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 Fortinet 防火墙配置

防火墙迁移工具可完整迁移以下 Fortinet 防火墙配置：

- 网络对象和组（通配符 FQDN、通配符掩码、Fortinet 动态对象除外）
- 服务对象
- 服务对象组（嵌套服务对象组除外）



注释 由于管理中心不支持嵌套，因此防火墙迁移工具会扩展引用规则的内容。但是，系统会迁移规则及完整功能。

- IPv4 和 IPv6 FQDN 对象与组
- IPv6 转换支持（接口、静态路由、对象、ACL 和 NAT）
- 访问规则
- NAT 规则
- 未迁移的静态路由、ECMP 路由
- 物理接口
- 子接口（子接口 ID 在迁移时会始终被设为与 VLAN ID 相同的编号）
- 汇聚接口（端口通道）
- 防火墙迁移工具支持将各个 VDOM 作为单独的威胁防御设备从 Fortinet 防火墙进行迁移。
- 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 [优化、检查和验证配置](#) 页面中的规则验证对象。

基于时间的对象属于允许基于时间段进行网络访问的访问列表类型。如果您必须根据一天中的特定时间或一周中的特定天数限制出站或入站流量，则此类对象非常有用。



注释

- 您必须将时区配置从源 Fortinet 手动迁移到目标 FTD。
 - 非 FTD 流不支持基于时间的对象，它们将被禁用。
 - 防火墙管理中心版本 6.6 及更高版本支持基于时间的对象。
-

部分支持的 Fortinet 防火墙配置

防火墙迁移工具部分支持以下 Fortinet 防火墙配置的迁移。其中一些配置包括含高级选项的规则，这些规则在迁移后失去这些选项。如果管理中心支持这些高级选项，您可以在迁移完成后手动配置它们。

- 包含不受支持的地址对象的地址组。
- 所含服务对象的协议中包含 TCP 或 UDP 和 SCTP 的服务组。



注释 SCTP 协议将被删除，服务组将部分迁移。

不支持的 Fortinet 防火墙配置

防火墙迁移工具不支持以下 Fortinet 防火墙配置的迁移。如果这些配置在管理中心中受支持，您可以在迁移完成之后手动配置它们。

- 基于用户、基于设备和基于互联网服务 ID 的访问控制策略规则
- 带有不受支持 ICMP 类型和代码的服务对象
- 基于隧道协议的访问控制策略规则
- 配置有块分配选项的 NAT 规则
- 配置有 SCTP 的 NAT 规则
- 配置有主机“0.0.0.0”的 NAT 规则
- 源或目标中包含 FQDN 对象的 NAT 规则
- 以特殊字符开头或包含特殊字符的 FQDN 对象
- 通配符 FQDN
- Fortinet 允许配置结合了 IPv4 和 IPv6 的策略（合并策略）。



注释 防火墙迁移工具不支持此策略。

适用于 威胁防御设备的准则和限制

当您计划将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。

Fortinet 硬件或软件交换机逻辑接口将作为威胁防御 L3 接口进行迁移。硬件或软件交换机成员接口不会使用防火墙迁移工具来进行迁移。

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。
 - 如果目标威胁防御设备是容器实例，则必须至少具有与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。

支持的迁移平台

以下 Fortinet 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](#)。

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。

支持迁移的软件版本

以下是支持迁移的 Fortinet 和 威胁防御 版本：

支持的 Fortinet 防火墙版本

防火墙迁移工具支持迁移到运行 Fortinet 防火墙操作系统版本 5.0 及更高版本的 威胁防御。

源 Fortinet 防火墙配置支持的 管理中心 版本

对于 Fortinet 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



第 3 章

运行迁移

- 从 [Cisco.com](#) 下载防火墙迁移工具，第 13 页
- 启动防火墙迁移工具，第 14 页
- 从 Fortinet 防火墙导出配置，第 15 页
- 上传 Fortinet 配置文件，第 17 页
- 指定防火墙迁移工具的目标参数，第 18 页
- 查看迁移前报告，第 20 页
- 通过 Secure Firewall 设备管理器 威胁防御 接口映射 Fortinet 配置，第 21 页
- 将 Fortinet 接口映射到安全区，第 22 页
- 优化，检查和验证要迁移的配置，第 23 页
- 将迁移的配置推送到 Cisco Secure Firewall Management Center，第 26 页
- 查看迁移后报告并完成迁移，第 27 页
- 卸载防火墙迁移工具，第 29 页

从 Cisco.com 下载防火墙迁移工具

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。

步骤 1 在您的计算机上，为防火墙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。当防火墙迁移工具启动时，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防火墙迁移工具时，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 下面的防火墙迁移工具。您还可以从 威胁防御 设备下载区域中下载防火墙迁移工具。

步骤 3 将防火墙迁移工具的最新版本下载到您创建的文件夹中。

下载适用于 Windows 或 macOS 计算机的防火墙迁移工具的相应可执行文件。

启动防火墙迁移工具



注释 当您启动防火墙迁移工具时，会在单独的窗口中打开控制台。进行迁移时，控制台会显示防火墙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防火墙迁移工具后。

开始之前

- 从 [Cisco.com](#) 下载防火墙迁移工具
- 查看并验证适用于防火墙迁移工具的准则和限制，第 5 页部分中的要求。
- 确保您的计算机带有最新版本的 Google Chrome 浏览器以运行防火墙迁移工具。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。

步骤 1 在您的计算机上，导航至已在其中下载防火墙迁移工具的文件夹。

步骤 2 执行以下操作之一：

- 在您的 Windows 计算机上，双击防火墙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**)，以允许防火墙迁移工具对您的系统作出更改。

防火墙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，将防火墙迁移工具 *.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
```

防火墙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 当您尝试打开防火墙迁移工具时，因为没有可识别的开发人员在 Apple 中注册防火墙迁移工具，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防火墙迁移工具。

步骤 4 在防火墙迁移工具的登录页面上, 执行以下操作:

- 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。

注释 如果您没有 Cisco.com 帐户, 请在 Cisco.com 登录页面上创建帐户。

- 使用以下默认凭证登录:

- 用户名 - admin
- 密码 - Admin123

如果您已使用 Cisco.com 帐户登录, 请继续执行步骤 8。

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防火墙迁移工具。

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防火墙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:

- 如果必须使用防火墙迁移工具从 Fortinet 防火墙提取信息, 请继续执行从 [Fortinet 防火墙导出配置](#)。

从 Fortinet 防火墙导出配置

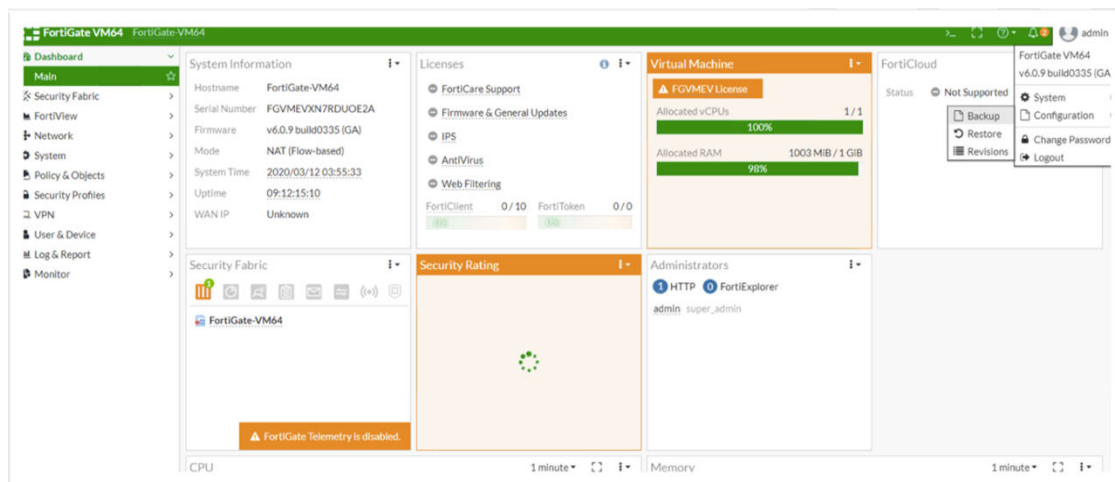
可以通过以下方式导出 Fortinet 防火墙配置:

- 从 Fortinet 防火墙 GUI 导出 Fortinet 防火墙配置
- 从 FortiManager 导出 Fortinet 防火墙配置

从 Fortinet 防火墙 GUI 导出 Fortinet 防火墙配置

按照以下步骤从 Fortinet 防火墙 GUI 提取配置：

步骤 1 从 FortiGate VM64 GUI 中，选择管理 > 配置 > 备份。



步骤 2 将备份定向到本地 PC 或 USB 磁盘。

注释 如果已启用 VDOM，请指明备份范围是用于整个 FortiGate 配置（全局）还是仅用于特定 VDOM 配置（VDOM）。

步骤 3 如果备份是 VDOM 配置，请从 **VDOM** 列表中选择 VDOM 名称。

注释 防火墙迁移工具需要未加密的文件才能继续备份过程。

步骤 4 选择确定。

Web 浏览器将提示您输入保存配置文件的位置。

配置文件的扩展名为 **.conf**。

下一步做什么

[上传 Fortinet 配置文件](#)

从 FortiManager 导出 Fortinet 防火墙配置

您可以从 FortiManager 提取相关设备配置。

-
- 步骤 1** 登录 FortiManager。
- 步骤 2** 找到您必须运行备份的正确 Fortigate 设备。
- 步骤 3** 在配置和安装状态下，选择总修订旁的图标以获取最新版本。
- 步骤 4** 点击下载 (**Download**)，下载新配置文件。
- 下载的文件是扩展名为 `.conf` 的文件类型。
-

下一步做什么

[上传 Fortinet 配置文件](#)

上传 Fortinet 配置文件

开始之前

将配置文件从源 Fortinet 设备导出为 `.conf` 或 `.txt`。



注释 不要上传手工编码的或手动更改的配置文件。文本编辑器会在文件中添加会导致迁移失败的空白行和其他问题。

-
- 步骤 1** 防火墙迁移工具 上传配置文件。对于大型配置文件，此步骤需要的时间较长。控制台提供一个逐行的进度日志视图，其中包含正在解析的 Fortinet 配置行。如果您没有看到控制台，可以在防火墙迁移工具后的单独窗口中找到它。**情景选择 (Context Selection)** 部分指定上传的配置是否对应于多情景 Fortinet。
- 步骤 2** 查看**情景选择 (Context Selection)** 部分，选择要迁移的 Fortinet VDOM。
- 步骤 3** **解析摘要**部分显示解析状态。
- 步骤 4** 查看 防火墙迁移工具在上传的配置文件中检测和解析的元素的摘要信息。
- 步骤 5** 点击**下一步 (Next)**，选择目标参数。
-

下一步做什么

[指定防火墙迁移工具的目标参数，第 18 页](#)

指定防火墙迁移工具的目标参数

开始之前

- 获得现场防火墙管理中心的 管理中心 的 IP 地址。
- 从防火墙迁移工具 3.0 开始，您可以在本地防火墙管理中心或云交付的防火墙管理中心之间选择。
- 对于云交付的防火墙管理中心，必须如[云交付的防火墙管理中心迁移](#)，第 45 页中所述提供区域和 API 令牌。
- （可选）如果要迁移设备特定的配置（例如接口和路由），请将目标 威胁防御 设备添加到管理中心。请参阅[将设备添加到防火墙管理中心](#)
- 如果它要求您在[检查和验证](#)页面中将 IPS 或文件策略应用于 ACL，我们强烈建议您在迁移之前在管理中心上创建策略。使用相同的策略，因为防火墙迁移工具从连接的管理中心获取策略。创建新策略并将其分配给多个访问控制列表可能会降低性能，也可能导致推送失败。

步骤 1 在选择目标 (**Select Target**) 屏幕的防火墙管理 (**Firewall Management**) 部分中，执行以下操作：您可以选择迁移到本地防火墙管理中心或云交付的防火墙管理中心：

- 要迁移到本地防火墙管理中心，请执行以下操作：

- a) 点击本地 **FMC (On-Prem FMC)** 单选按钮。
- b) 输入管理中心的 IP 地址或完全限定域名 (FQDN)。
- c) 在域下拉列表中，选择要迁移到的域。

如果要迁移到 威胁防御 设备，只能迁移到所选域中可用的 威胁防御 设备。

- d) 点击**连接 (Connect)** 并继续步骤 2。

- 要迁移到云交付的防火墙管理中心，请执行以下操作：

- a) 点击云交付的 **FMC (Cloud-delivered FMC)** 单选按钮。
- b) 选择区域并粘贴 CDO API 令牌。有关生成 CDO API 令牌的信息，请参阅[云交付的防火墙管理中心迁移](#)，第 45 页。
- c) 点击**连接 (Connect)** 并继续步骤 2。

步骤 2 在防火墙管理中心登录 (**Firewall Management Center Login**) 对话框中，输入防火墙迁移工具专用帐户的用户名和密码，然后点击**登录 (Login)**。

防火墙迁移工具将登录到管理中心，并检索由该管理中心管理的一系列 威胁防御 设备。您可以在控制台中查看此步骤的进度。

步骤 3 点击**继续 (Proceed)**。

步骤 4 在选择威胁防御 (**Choose Threat Defense**) 部分中，执行以下操作之一：

- 点击**选择防火墙威胁防御设备 (Select Firewall Threat Defense Device)**下拉列表，然后选中您要迁移 Fortinet 配置的设备。

选择的 管理中心 域中的设备将按 **IP 地址**和**名称**列出。

注释 您选择的本地 威胁防御 设备必须至少拥有与您要迁移的 Fortinet 配置相同数目的物理或端口通道接口。威胁防御 设备的容器实例必须至少具有相同数量的物理或端口通道接口和子接口。您必须为设备配置与 Fortinet 配置相同的防火墙模式。但是，两个设备上的这些接口不需要具有相同的名称。

防火墙迁移工具支持在启用远程部署的情况下将 Fortinet 防火墙迁移到 管理中心 或 威胁防御 6.7 或更高版本。但是，接口和路由必须手动迁移。

- 点击**忽略威胁防御并继续 (Proceed without Threat Defense)**，将配置迁移到 管理中心。

当您忽略威胁防御并继续时，防火墙迁移工具不会将任何配置或策略推送到威胁防御。因此，作为威胁防御 设备特定配置的接口和路由以及站点间 VPN 不会迁移。但是，所有其他受支持的配置（共享策略和对象）将迁移，例如 NAT、ACL 和端口对象。远程访问 VPN 是一种共享策略，即使没有威胁防御也可以迁移。

步骤 5 单击**继续 (Proceed)**。

根据迁移的目标，防火墙迁移工具允许您选择要迁移的功能。

步骤 6 点击**选择功能 (Select Features)** 部分以查看并选择要迁移到目标的功能。

- 如果要迁移到目标 威胁防御 设备，防火墙迁移工具会自动从**设备配置 (Device Configuration)** 和**共享配置 (Shared Configuration)** 部分的 Fortinet 配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。
- 如果要迁移到 管理中心，防火墙迁移工具会自动从**共享配置 (Shared Configuration)** 部分的 Fortinet 配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。

注释 当您未选择要迁移到的目标 威胁防御 设备时，**设备配置**部分不可用。

- 防火墙迁移工具支持目标安全区域，可在迁移期间启用 ACL 的目标区域映射。

根据源和目标网络对象或组和服务对象或族的性质，当从 Fortinet 迁移至 管理中心 时，此操作可能会导致 ACL 规则爆炸。

- 如果目标管理中心是 7.2 或更高版本，防火墙迁移工具支持迁移远程访问 VPN。远程访问 VPN 是一种无需威胁防御即可迁移的共享策略。如果选择使用威胁防御进行迁移，则威胁防御版本应为 7.0 或更高版本。
- （可选）在优化部分中，选择**仅迁移引用的对象**，以仅迁移访问控制策略和 NAT 策略中引用的对象。

注释 当您选择此选项时，不会迁移 Fortinet 配置中未引用的对象。这可以优化迁移时间并从配置中清除未使用的对象。

步骤 7 单击**继续 (Proceed)**。

步骤 8 在**规则转换/流程配置 (Rule Conversion/ Process Config)**部分中，单击**开始转换 (Start Conversion)** 以启动转换。

步骤 9 查看防火墙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 10 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（与防火墙迁移工具处于相同的位置）。

下一步做什么

[查看迁移前报告，第 20 页](#)

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 防火墙迁移工具 正在运行时下载报告。

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（与防火墙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 Fortinet 配置元素以及为迁移选择的特定 Fortinet 功能的摘要。
- 出错的配置行 - 因为防火墙迁移工具无法解析而不能成功迁移的 Fortinet 配置元素的详细信息。在 Fortinet 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 防火墙迁移工具，然后再继续。
- 部分支持的配置 - 仅可部分迁移的 Fortinet 配置元素的详细信息。这些配置元素包括含高级选项的规则和对象，其中的规则或对象可在无高级选项的情况下迁移。查看这些行，验证 管理中心中是否支持高级选项。如果支持，则计划在使用 防火墙迁移工具 完成迁移后手动配置这些选项。
- 不支持的配置 - 因防火墙迁移工具不支持迁移这些功能而无法迁移的 Fortinet 配置元素的详细信息。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划在使用防火墙迁移工具完成迁移后手动配置这些功能。
- 忽略的配置 - 因为不受 管理中心 或防火墙迁移工具支持而被忽略的 Fortinet 配置的详细信息。防火墙迁移工具不会解析这些行。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划手动配置这些功能。

有关 管理中心 和 威胁防御 中受支持功能的更多信息，请参阅[管理中心配置指南](#)。

步骤 3 如果迁移前报告建议执行纠正操作，请在 Fortinet 接口上完成这些纠正操作，重新导出 Fortinet 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 Fortinet 配置文件成功上传和解析之后，返回到防火墙迁移工具，然后点击下一步 (Next) 以继续迁移。

下一步做什么

[通过 Secure Firewall 设备管理器 威胁防御 接口映射 Fortinet 配置](#)

通过 Secure Firewall 设备管理器 威胁防御 接口映射 Fortinet 配置

威胁防御 设备必须具有与 Fortinet 配置相同或更多的物理接口和端口通道接口。两个设备上的这些接口不需要具有相同的名称。您可以选择所需的接口映射方式。

在映射威胁防御接口屏幕上，防火墙迁移工具将检索威胁防御设备上的接口的列表。默认情况下，防火墙迁移工具会根据其接口标识符映射 Fortinet 和 威胁防御 设备中的接口。

Fortinet 接口到 威胁防御 接口的映射因 威胁防御 设备类型而异：

- 如果目标 威胁防御 为本地类型：
 - 威胁防御 必须具有相同或更多数量的已使用 Fortinet 接口或端口通道(PC) 数据接口（Fortinet 配置中不包括管理专用接口和子接口）。如果其接口数量较少，请在目标威胁防御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接口或端口通道映射创建。
- 如果目标 威胁防御 为容器类型：
 - 威胁防御 必须具有相同或更多数量的已使用 Fortinet 接口、物理子接口、端口通道或端口通道子接口（Fortinet 配置中不包括管理专用接口）。如果其接口数量较少，请在目标威胁防御上添加所需类型的接口。例如，如果目标威胁防御上的物理接口和物理子接口的数量比 Fortinet 的接口数量少 100 个，则可以在目标威胁防御上创建更多物理接口或物理子接口。
 - 子接口不是由防火墙迁移工具创建的。物理接口、端口通道或子接口之间仅允许接口映射。

开始之前

确保您已连接到 管理中心 并将目标选择为 威胁防御。有关详细信息，请参阅[指定防火墙迁移工具的目标参数，第 18 页](#)。



注释 如果要迁移到无 威胁防御 设备的 管理中心，则此步骤不适用。

步骤 1 如果您想要更改接口映射，请点击**威胁防御接口名称 (Threat Defense Interface Name)** 下拉列表，并选择您想要映射到该 Fortinet 接口的接口。

不能更改管理接口的映射。如果 威胁防御 接口已分配到 Fortinet 接口，则您不能从下拉列表中选择该接口。所有已分配的接口将变为灰色且不可用。

您不需要映射子接口。防火墙迁移工具会在 威胁防御 设备上为 Fortinet 配置中的所有子接口映射子接口。

步骤 2 当您每个 Fortinet 接口映射到 威胁防御 接口时，请点击**下一步 (Next)**。

下一步做什么

将 Fortinet 接口映射到相应的 威胁防御 接口对象、安全区和接口组。有关详细信息，请参阅[将 Fortinet 接口映射到安全区](#)。

将 Fortinet 接口映射到安全区

为确保正确地迁移 Fortinet 配置，您需要将 Fortinet 接口映射到相应的 威胁防御 接口对象、安全区和接口组。在 Fortinet 配置中，访问控制策略和 NAT 策略使用接口名称 (nameif)。在管理中心中，这些策略使用接口对象。此外，管理中心策略将按以下项分组接口对象：

- 安全区 - 接口只能属于一个安全区。

防火墙迁移工具支持接口与安全区的一对一映射；当安全区映射到某个接口时，尽管管理中心允许，也不可映射到其他接口。有关管理中心中的安全区的详细信息，请参阅[安全区](#)。

步骤 1 要将接口映射到管理中心中的安全区和接口组，或映射到在配置文件中作为安全区类型对象并出现在下拉列表中的安全区和接口组，请执行以下操作：

- 在**安全区**栏中，选择该接口的安全区。
- 在**接口组**栏中，选择该接口的接口组。

步骤 2 要将接口映射到管理中心中的安全区，请在**安全区**栏中，选择该接口的安全区。

步骤 3 您可以手动映射或自动创建安全区。

要手动映射安全区，请执行以下操作：

- 点击**添加 SZ (Add SZ)**。
- 在**添加 SZ (Add SZ)**对话框中，点击**添加 (Add)**以添加新的安全区。
- 在**安全区**栏中输入安全区名称。允许的最大字符数为 48。
- 点击**关闭 (Close)**。

要通过自动创建映射安全区，请执行以下操作：

- 点击**自动创建 (Auto-Create)**。
- 在**自动创建**对话框中，选中**区域映射**。

c) 点击**自动创建 (Auto-Create)**。

点击**自动创建 (Auto-Create)**后，系统会自动映射源防火墙区域。如果管理中心上已存在相同的名称区域，则该区域将重新使用。映射页面将对重新使用的区域显示“(A)”。例如，**inside "(A)"**。

步骤 4 在已将所有接口映射到相应的安全区后，点击**下一步 (Next)**。

优化，检查和验证要迁移的配置

在将迁移的 Fortinet 配置推送到管理中心之前，优化并仔细检查配置并验证它是否正确且与您需要的威胁防御设备配置方式匹配。闪烁的选项卡表示您必须执行下一步操作。

此处，防火墙迁移工具会获取管理中心上已存在的入侵防御系统 (IPS) 策略和文件策略，并允许您将这些策略与要迁移的访问控制规则相关联。

文件策略是作为整体访问控制配置的一部分供系统用于执行网络高级恶意软件防护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。

同样，在允许流量继续到达其目标之前，可以使用 IPS 策略作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

要搜索选项卡中的特定配置项，请在列顶部的字段中输入项目名称。表中的行将筛选，仅显示与搜索术语匹配的项目。



注释 默认情况下，内联分组选项处于启用状态。

如果您在**优化、检查和验证配置**屏幕上关闭了防火墙迁移工具，它会保存进度并允许您在以后恢复迁移。如果在进入此屏幕之前关闭，则不会保存您的进度。如果解析后出现故障，防火墙迁移工具会继续从**接口映射**屏幕重新启动。

防火墙迁移工具 ACL 优化概述

防火墙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，防火墙迁移工具 会使用以下参数：



注释 优化仅适用于 ACP 规则操作的 Fortinet。

- 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：
 - 源和目标区域
 - 源和目标网络
 - 源和目标端口

对象优化

在迁移过程中会考虑以下对象以进行对象优化：

- 未引用的对象 - 可以选择在迁移开始时不迁移未被引用的对象。
- 重复对象 - 如果对象已存在于 管理中心 上，则不会创建重复对象，而是重复使用策略。
- 不一致的对象 - 如果存在名称相似但内容不同的对象，则在迁移推送之前 防火墙迁移工具 会修改对象名称。

ACL 优化的报告

ACL 优化报告中显示以下信息：

- 摘要表 (Summary Sheet) - 显示 ACL 优化的摘要。

Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremove_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

- 详细 ACL 信息 (Detailed ACL Information) - 显示基础 ACL 的详细信息。每个 ACL 都带有一个 ACL 类型 (Shadow 或 Redundant) 标记，用于标识基本 ACL 以便进行比较和与优化类别的关联。

Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	outsideACL_#1	outside	ANY	any	10.0.0.0/8	ANY	ANY	permit	
2	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
3	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
4	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
5	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
6	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
7	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
8	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
9	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
10	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
11	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
12	outsideACL_#12	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
13	outsideACL_#13	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
14	outsideACL_#17	outside	ANY	any	192.168.0.0/16	ANY	ANY	permit	
15	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
16	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

将迁移的配置推送到 Cisco Secure Firewall Management Center

如果您还未成功验证配置和解决所有对象冲突，则不能将迁移的 ASA Fortinet 配置推送到 Cisco Secure Firewall Management Center。

迁移过程中的此步骤会将迁移的配置发送至 Cisco Secure Firewall Management Center。此步骤不会将配置部署到 Cisco Secure Firewall Threat Defense 设备。但在此步骤中会擦除 Cisco Secure Firewall Threat Defense 上的任何现有配置。



注释 当防火墙迁移工具将迁移的配置发送到 Cisco Secure Firewall Management Center 时，不要更改任何配置或部署到任何设备。

步骤 1 在验证状态对话框中，查看验证摘要。

步骤 2 点击**推送配置 (Push Configuration)**，将迁移的 ASA Fortinet 配置发送至 Cisco Secure Firewall Management Center。

防火墙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 Cisco Secure Firewall Management Center。

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。

系统也会在 Resources 文件夹中保存**迁移前报告**的一个副本（与防火墙迁移工具处于相同的位置）。

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

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。有关详细信息，请参阅[优化](#)，[检查和验证要迁移的配置](#)，第 23 页

查看并验证对象：

- 类别
 - ACL 规则总数（源配置）
 - 考虑优化的 ACL 规则总数。例如，冗余、阴影等。
- 优化的 ACL 计数给出了优化前后计算得出的 ACL 规则总数。

如果您在迁移期间错过下载迁移后报告，请使用以下链接进行下载：

迁移后报告下载终端 — http://localhost:8888/api/downloads/post_migration_summary_html_format



注释 您只能在 防火墙迁移工具 正在运行时下载报告。

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 Fortinet 配置是如何迁移的：

- **迁移摘要** - 已成功从 Fortinet 迁移到 威胁防御 的配置的摘要信息，其中包括有关 Fortinet 接口、管理中心 主机名和域、目标 威胁防御 设备（如果适用）和已成功迁移的配置元素的信息。
- **选择性策略迁移** - 设备配置功能、共享配置功能和优化三个类别中可选择迁移的特定 Fortinet 功能的详细信息。
- **Fortinet 接口至 FTD 接口映射** - 已成功迁移的接口的详细信息，以及如何将 Fortinet 配置上的接口映射到 威胁防御 设备上的接口。确认这些映射符合您的预期。

注释 本部分不适用于没有目标 威胁防御 设备或者未选择迁移接口的迁移。

- **源接口名称至威胁防御安全区** - 已成功迁移的 Fortinet 逻辑接口和名称的详细信息，以及如何将它们映射到 威胁防御 中的安全区。确认这些映射符合您的预期。

注释 如果未选择迁移访问控制列表和 NAT，则此部分不适用。

- **对象冲突处理** - 已被确定为与 管理中心 中现有对象冲突的 Fortinet 对象的详细信息。如果对象具有相同的名称和配置，防火墙迁移工具重新使用 管理中心对象。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。

- **您选择不迁移的访问控制规则、NAT 和路由** - 您选择不让 防火墙迁移工具 迁移的规则 的详细信息。查看由 防火墙迁移工具 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。
- **部分迁移的配置** - 仅部分迁移的 Fortinet 规则的详细信息，包括带有高级选项的规则，其中，在没有高级选项的情况下也可以迁移规则。查看这些行，验证在 管理中心 中是否支持高级选项。如果支持，手动配置这些选项。
- **不支持的配置** - 因防火墙迁移工具不支持迁移这些功能而未被迁移的 Fortinet 配置元素的详细信息。查看这些行，验证 威胁防御 中是否支持每项功能。如果支持，请在 管理中心 中手动配置这些功能。
- **展开访问控制策略规则** - 在迁移期间已从一个 Fortinet Point 规则扩展到多个 威胁防御 规则的 Fortinet 访问控制策略规则的详细信息。
- **对访问控制规则采取的操作**
 - **您选择不迁移的访问规则** - 您选择不让 防火墙迁移工具 迁移的 Fortinet 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，可以手动配置这些规则。
 - **规则操作有更改的访问规则** - 使用 防火墙迁移工具 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，可以手动配置这些规则。
 - **应用了 IPS 策略和变量集的访问控制规则** - 应用了 IPS 策略的所有 Fortinet 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
 - **应用了文件策略的访问控制规则** - 应用了文件策略的所有 Fortinet 访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
 - **规则“日志”设置有更改的访问控制规则** - 使用 防火墙迁移工具 更改了“日志设置”的 Fortinet 访问控制规则的详细信息。日志设置值包括 False、事件查看器、系统日志。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。

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。建议您在 管理中心 中配置一个规则来确保 威胁防御 阻止此类流量。

注释 如果它要求您在 **检查和验证** 页面中将 IPS 或文件策略应用于 ACL，则强烈建议您在迁移之前在管理中心上创建策略。使用相同的策略，因为 防火墙迁移工具 从连接的管理中心获取策略。创建新策略并将其分配给多个策略可能会降低性能，也可能导致推送失败。

有关 管理中心 和 威胁防御 中的受支持功能的更多信息，请参阅 [管理中心配置指南，版本 6.2.3](#)。

步骤 3 打开 **迁移前报告**，并记下您必须在 威胁防御 设备上手动迁移的任何 Fortinet 配置项目。

步骤 4 在 管理中心 中，执行以下操作：

- a) 查看 威胁防御 设备的迁移配置，确认所有预期规则和其他配置项目（包括以下内容）均已迁移：
 - 访问控制列表 (ACL)
 - 网络地址转换规则
 - 端口和网络对象

- 路由
- 接口
- 动态路由对象

b) 配置所有未迁移的部分受支持、不受支持、已忽略和已禁用的配置项目和规则。

有关如何配置这些项目和规则的信息，请参阅[管理中心配置指南](#)。以下是需要手动配置的配置项目的示例：

- 平台设置，包括 SSH 和 HTTPS 访问，如[威胁防御的平台设置](#)中所述。
- 系统日志设置，如[配置系统日志](#)中所述
- 动态路由，如[威胁防御路由概述](#)中所述
- 服务策略，如 [FlexConfig 策略](#) 中所述
- VPN 配置，如[威胁防御 VPN](#) 中所述
- 连接日志设置，如[连接日志记录](#)中所述

步骤 5 完成检查之后，将已迁移的配置从 管理中心 部署到 威胁防御 设备。

验证**迁移后报告**中是否正确反映了不支持和部分支持的规则的数据。

防火墙迁移工具将策略分配到 威胁防御设备。验证运行配置中是否反映了更改。为帮助您识别已迁移的策略，这些策略的描述信息中包括 Fortinet 配置的主机名。

卸载防火墙迁移工具

所有组件均存储在与防火墙迁移工具相同的文件夹中。

步骤 1 导航至在其中放置防火墙迁移工具的文件夹。

步骤 2 如果要保存日志，请剪切或复制 log 文件夹并粘贴到另一个位置。

步骤 3 如果要保存迁移前报告和迁移后报告，请剪切或复制 resources 文件夹并粘贴到另一个位置。

步骤 4 删除在其中放置防火墙迁移工具的文件夹。

提示 日志文件与控制台窗口相关联。只要防火墙迁移工具的控制台窗口处于打开状态，就无法删除日志文件和文件夹。



第 4 章

排除迁移问题

- 关于防火墙迁移工具的故障排除，第 31 页
- 用于排除故障的日志和其他文件，第 32 页
- Fortinet 文件上传失败故障排除，第 32 页

关于防火墙迁移工具的故障排除

在 Fortinet 配置文件上传或将已迁移的配置推送到管理中心时，迁移通常会失败。

迁移过程失败的一些常见情况如下：

- Fortinet 配置文件中存在未知或无效字符
- Fortinet 配置文件中存在不完整或缺失元素
- 网络连接丢失或延迟

防火墙迁移工具支持捆绑包

防火墙迁移工具提供下载支持捆绑包的选项，以提取重要的故障排除信息，例如日志文件、数据库和配置文件。请执行以下操作：

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的。



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。

用于排除故障的日志和其他文件

可在以下文件中找到有助于识别和排除问题的信息。

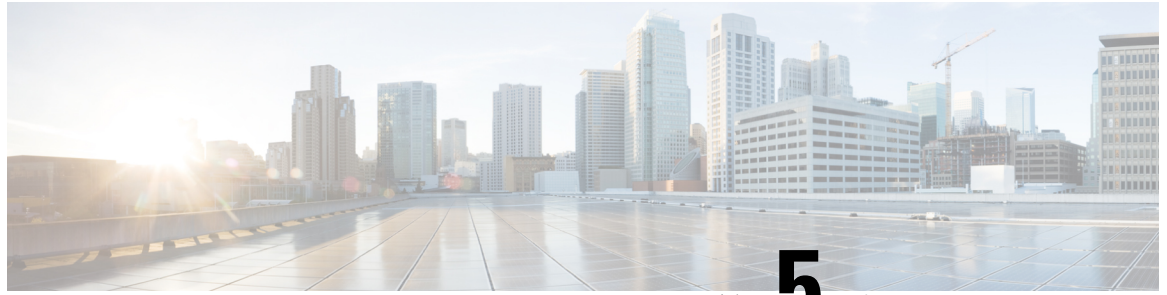
文件	位置
日志文件	<code><migration_tool_folder>\logs</code>
迁移前报告	<code><migration_tool_folder>\resources</code>
迁移后报告	<code><migration_tool_folder>\resources</code>
未解析文件	<code><migration_tool_folder>\resources</code>

Fortinet 文件上传失败故障排除

如果您的 Fortinet 配置文件上传失败，这是因为防火墙迁移工具无法解析文件中的一行或多行。

可在以下位置找到导致上传和解析失败的错误的相关信息：

- 防火墙迁移工具显示的错误消息 - 简要概括导致失败的原因。
- 迁移前报告 - 检查“出错的配置行”部分，查看 Fortinet 配置文件中的哪些行导致了失败。
- 日志文件 - 搜索“错误”一词以查看失败原因。
- 未解析文件 - 查看文件末尾部分，确定已成功解析的 Fortinet 配置文件中最后被忽略的行。



第 5 章

防火墙迁移工具常见问题

• [防火墙迁移工具常见问题](#)，第 33 页

防火墙迁移工具常见问题

防火墙迁移工具常见问题解答

问：版本 3.0.1 的 Cisco Secure Firewall 迁移工具支持哪些新功能？

答：Cisco Secure Firewall 迁移工具 3.0.1 现在仅支持将 Cisco Secure Firewall 3100 系列作为从 Fortinet 迁移的目标设备。

问：版本 3.0 的 Cisco Secure Firewall 迁移工具支持哪些新功能？

答：版本 3.0 支持的功能包括：

- 迁移到云交付的防火墙管理中心

问: 版本 2.5.2 的 Cisco Secure Firewall 迁移工具支持哪些新功能?

答: Fortinet 的 ACL 优化。

问: Cisco Secure Firewall 迁移工具 2.3 迁移策略的源平台和目标平台是什么?

答: Cisco Secure Firewall 迁移工具可以将策略从支持的 Fortinet 防火墙平台迁移到 FTD 平台。有关详细信息, 请参阅[支持的迁移平台](#)。

问: Cisco Secure Firewall 迁移工具 2.3 支持哪些新功能?

答: 防火墙迁移工具 2.3 可以将策略从支持的 Fortinet 平台迁移到 FTD 平台。

问: 支持哪些的源设备和代码版本?

答: 您可以使用防火墙迁移工具从运行 FortiOS 5.0 及更高版本的单 VDOM 或多 VDOM Fortinet 防火墙来迁移配置。有关设备列表的详细信息, 请参阅[支持的迁移平台](#)。

问: Fortinet 防火墙是否支持接口组?

答: 否。Fortinet 防火墙向 FTD 转换时, 不支持接口组。

问: 安全防火墙迁移工具支持哪些迁移功能?

答: 防火墙迁移工具支持将 L3/L4 Fortinet 配置迁移到 FTD, 并且还可以迁移以下 Fortinet 配置:

- 网络对象和组 (部分不支持的对象类型除外)
- 服务对象, 为源和目的配置的服务对象除外
- 服务对象组, 嵌套服务对象组除外



注释 由于防火墙管理中心不支持嵌套, 因此防火墙迁移工具会扩展引用规则的内容。但是, 系统会迁移规则及完整功能。

- IPv4 和 IPv6 FQDN 对象与组
- IPv6 转换支持 (接口、静态路由、对象、ACL 和 NAT)
- 访问规则
- NAT 规则
- 使用 VIP 和 IP 池的 NAT (不支持中央 NAT)
- 静态路由和未迁移的 ECMP 路由
- 物理接口
- 子接口
- 端口通道
- 区域 (Zones)

- 基于时间的对象

问: NAT 可使用防火墙管理中心不支持的 FQDN。应该怎么办?

答: 防火墙迁移工具和防火墙管理中心不支持在 NAT 字段中使用 FQDN-address-object。为了复制与源相同的配置, 您必须在迁移后手动配置与 FQDN 映射的整个 IP 地址集。

问: 当源防火墙的接口比目标防火墙更多时, 我该怎么办?

答: 如果源防火墙的接口比目标防火墙更多, 则在启动迁移之前在 FTD 上创建子接口。

问: 防火墙迁移工具是否会迁移汇聚接口(端口通道)?

答: 防火墙迁移工具不会迁移汇聚接口(端口通道)。在启动迁移之前, 必须在防火墙管理中心上配置端口通道接口。

问: 我应该如何处理被忽略的配置文件?

答: 忽略的配置文件包含仅特定于 Fortinet 并与防火墙管理中心无关的行。因此, 它们会被忽略。您必须仔细查看忽略的配置。应在防火墙管理中心手动配置反映在忽略部分中的任何不相关详细信息。

问: 我的迁移前报告中有一个错误。是否可以忽略接口并继续?

答: 如果您选择在没有接口的情况下继续, 则路由也不会迁移。

问: 解析失败的常见原因是什么?

答: 如果接口有多个 IP 地址或为其分配了子网中的 IP 地址(例如 /32 或 /128), 则发生解析失败。要继续, 您必须更正 IP 地址并重试迁移。

问: 如何导出 Fortinet 配置?

答: 您可以通过从 Fortigate 设备或 FortiManager (如果设备由 FortiManager 管理) 中提取来导出 Fortinet 配置。有关详细信息, 请参阅[从 Fortinet 防火墙导出配置](#)。

问: 是否需要依赖防火墙管理中心才能使用防火墙迁移工具中推出的新功能?

答: 是。目标防火墙管理中心 6.6 及更高版本支持基于时间的对象功能。



APPENDIX A

思科成功网络 - 遥测数据

• [思科成功网络 - 遥测数据](#)，第 37 页

思科成功网络 - 遥测数据

每当您在 防火墙迁移工具中启动迁移过程时，相应的遥测数据文件都存储在固定位置。在启用思科成功网络的情况下，当您将迁移的 Fortinet 配置推送到 管理中心时，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。如果您使用本地凭证而不是 Cisco.com 帐户凭证登录 防火墙迁移工具，遥测数据不会推送到云，并且数据文件位于以下位置：

```
<migration_tool_folder>\resources \ telemetry_data
```

下表提供有关遥测数据点、其说明和样本值的信息。

表 1: 系统信息

数据点	描述	示例值
操作系统	运行防火墙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 防火墙迁移工具 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 2: 源 Fortinet 信息

数据点	描述	示例值
源类型	源设备类型	Fortinet
源设备序列号	Fortinet 的序列号	设备序列号（如果存在）。
源设备型号	Fortinet 的型号	FGT80E
源设备版本	Fortinet 的版本	6.0.6

数据点	描述	示例值
源配置计数	源配置中的总行数	504
防火墙模式	Fortinet 上配置的防火墙模式 - 路由或透明	路由
情景模式	Fortinet 的情景模式。这可以是单情景或多情景。	单一
Fortinet 配置统计:		
ACL 计数	连接到访问组的 ACL 数量	46
访问规则计数	访问规则总数	46
NAT 规则计数	NAT 规则总数	17
网络对象计数	Fortinet 中配置的网络对象数	34
网络对象组计数	Fortinet 中的网络对象组数	6
端口对象计数	端口对象的数量	85
端口对象组计数	端口对象组的数量	37
不受支持的访问规则计数	不受支持的访问规则总数	3
不受支持的 NAT 规则计数	不受支持的 NAT 访问规则总数	0
基于 FQDN 的访问规则计数	基于 FQDN 的访问规则数量	7
基于时间范围的访问规则计数	基于时间范围的访问规则数量	1
基于 SGT 的访问规则计数	基于 SGT 的访问规则数量	0
工具无法解析的配置行摘要		
未解析的配置计数	解析器无法识别的配置行数	68
未解析的访问规则总数	未解析的访问规则的总数	3
更多 Fortinet 配置详细信息...		
是否配置了 RA VPN	是否在 Fortinet 上配置了 RA VPN	false
是否配置了 S2S VPN	是否在 Fortinet 上配置了站点间 VPN	false
是否配置了 BGP	是否在 Fortinet 上配置了 BGP	false
是否配置了 OSPF	是否在 Fortinet 上配置了 OSPF	false
本地用户计数	配置的本地用户数	0

表 3: 目标管理设备 (管理中心) 信息

数据点	描述	示例值
目标管理版本	管理中心的目标版本	6.2.3.3 (内部版本 76)
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
迁移工具版本	迁移工具的版本	1.1.0.1912

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
访问规则计数	迁移的 ACL 规则总数	0
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		
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

数据点	描述	示例值
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: 防火墙迁移工具 性能数据

数据点	描述	示例值
转换时间	解析 Fortinet 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 Fortinet 配置迁移到 管理中心 的状态	SUCCESS
错误消息	防火墙迁移工具 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

遥测 Fortinet 示例文件

以下例举了有关 Fortinet 配置向 威胁防御 迁移的遥测数据文件：

```
{
  "metadata": {
    "contentType": "application/json",
    "topic": "migrationtool.telemetry"
  },
  "payload": {
    "fortinet_config_stats": {
      "Ipv6_access_rule_counts": 3,
      "Ipv6_bgp_count": 0,
      "Ipv6_nat_rule_count": 3,
      "Ipv6_network_counts": 3,
      "Ipv6_static_route_counts": 6,
      "access_rules_counts": 62,
      "acl_counts": 62,
      "fqdn_based_access_rule_counts": 2,
      "nat_rule_counts": 27,
    }
  }
}
```

```

    "network_object_counts": 59,
    "network_object_group_counts": 11,
    "no_of_fqdn_based_objects": 9,
    "port_object_counts": 166,
    "port_object_group_counts": 37,
    "timerange_based_access_rule_counts": 0,
    "total_unparsed_access_rule_counts": 0,
    "tunneling_protocol_based_access_rule_counts": 0,
    "unparsed_config_count": 0,
    "unsupported_access_rules_count": 0,
    "unsupported_nat_rule_count": 0
  },
  "context_mode": "SINGLE",
  "error_description": null,
  "error_message": null,
  "firewall_mode": "ROUTED",
  "log_info_acl_count": 0,
  "migration_status": "SUCCESS",
  "migration_summary": {
    "access_control_policy": [
      [
        {
          "access_rule_counts": 62,
          "apply_file_policy_rule_counts": 0,
          "apply_ips_policy_rule_counts": 0,
          "apply_log_rule_counts": 0,
          "do_not_migrate_rule_counts": 0,
          "enable_hit_count": false,
          "expanded_acp_rule_counts": 1,
          "name": "FTD-Mig-ACP-1602513965",
          "partially_migrated_acl_rule_counts": 0,
          "time_based_acl_count": 0,
          "total_acl_element_counts": 69,
          "update_rule_action_counts": 0
        }
      ]
    ]
  },
  "interface_counts": 20,
  "interface_group_counts": 0,
  "interface_group_manually_created_counts": 0,
  "ip_sla_monitor_count": 0,
  "nat_Policy": [
    [
      {
        "NAT_rule_counts": 27,
        "do_not_migrate_rule_counts": 0,
        "name": "FTD-Mig-1602513959",
        "partially_migrated_nat_rule_counts": 0
      }
    ]
  ],
  "network_object_rename_counts": 0,
  "network_object_reused_counts": 37,
  "object_group_counts": 2,
  "objects_counts": 35,
  "port_object_rename_counts": 0,
  "port_object_reused_counts": 10,
  "prefilter_control_policy": [
    [
      {
        "do_not_migrate_rule_counts": 0,
        "name": null,
        "partially_migrated_acl_rule_counts": 0,
        "prefilter_rule_counts": 0
      }
    ]
  ]
}

```

```

    }
  ]
],
"security_zone_counts": 19,
"security_zone_manually_created_counts": 0,
"static_routes_counts": 9,
"sub_interface_counts": 20,
"time_out": false
},
"migration_tool_version": "2.3",
"mtu_info": {
  "interface_name": null,
  "mtu_value": null
},
"rule_change_acl_count": 0,
"selective_policy": {
  "acl": true,
  "acl_policy": true,
  "application": false,
  "csm": true,
  "interface": true,
  "interface_groups": true,
  "migrate_tunneled_routes": false,
  "nat": true,
  "network_object": true,
  "policy_assignment": true,
  "populate_sz": false,
  "port_object": true,
  "routes": true,
  "security_zones": true,
  "unreferenced": true
},
"source_config_counts": 0,
"source_device_model_number": "FGT80E",
"source_device_serial_number": null,
"source_device_version": "6.0.6",
"source_type": "FORTINET",
"system_information": {
  "browser": "Chrome/85.0.4183.121",
  "operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Cisco Firepower 9000 Series SM-24 Threat Defense",
"target_device_version": "76",
"target_management_type": "6.6.0 (build 56)",
"target_management_version": "6.6.0 (build 56)",
"template_version": "1.1",
"time": "2020-10-12 20:16:15",
"tool_analytics_data": {
  "objectsplit_100_count": 0
},
"tool_performance": {
  "config_push_time": 533,
  "conversion_time": 3,
  "migration_time": 1108
}
},
"version": "1.0"
}

```



附录 **B**

将 Fortinet 迁移到 Threat Defense 2100 - 示例

- [将迁移到防火墙威胁防御 2100 - 示例](#)，第 43 页

将迁移到防火墙威胁防御 2100 - 示例



注释 创建迁移完成后可在目标设备上运行的测试计划。

- [在维护窗口之前执行以下任务](#)，第 43 页
- [在维护窗口期间执行以下任务](#)，第 44 页

在维护窗口之前执行以下任务

开始之前

确保已安装并部署了管理中心。有关详细信息，请参阅相应的[管理中心硬件安装指南](#)和相应的[管理中心入门指南](#)。

- 步骤 1** 从要迁移的源 Fortinet 保存全局或每 VDOM 配置的副本。
- 步骤 2** 在网络中部署 Firepower 2100 系列设备，连接接口并打开设备电源。
有关详细信息，请参阅《[适用于使用管理中心的 2100 系列的思科威胁防御快速入门指南](#)》。
- 步骤 3** 注册 Firepower 2100 系列设备以接受管理中心的管理。
有关详细信息，请参阅[将设备添加到管理中心](#)。
- 步骤 4** （可选）如果源 Fortinet 配置具有汇聚接口，请在目标 Firepower 2100 系列设备上创建端口通道 (EtherChannel)。有关详细信息，请参阅[配置 EtherChannel 和冗余接口](#)。
- 步骤 5** 从 <https://software.cisco.com/download/home/286306503/type> 下载并运行最新版本的防火墙迁移工具。

在维护窗口期间执行以下任务

有关详细信息，请参阅 [从 Cisco.com 下载防火墙迁移工具](#)，第 13 页。

步骤 6 启动 防火墙迁移工具 并指定目标参数时，请确保选择注册到 管理中心的 Firepower 2100 系列 设备。

有关详细信息，请参阅 [指定防火墙迁移工具的目标参数](#)，第 18 页。

步骤 7 将 Fortinet 接口与 威胁防御 接口映射。

注释 防火墙迁移工具 允许您将 Fortinet 接口类型映射到 威胁防御 接口类型。

例如，您可以将 Fortinet 中的汇聚接口映射到 威胁防御 中的物理接口。

有关详细信息，请参阅[通过 Secure Firewall 设备管理器 威胁防御 接口映射 Fortinet 配置](#)。

步骤 8 将逻辑接口映射到安全区时，点击**自动创建 (Auto-Create)** 以允许 防火墙迁移工具 创建新的安全区。要使用现有安全区，请手动将 Fortinet 逻辑接口映射到安全区。

有关详细信息，请参阅[将 Fortinet 接口映射到安全区](#)。

步骤 9 按照本指南的说明依次检查和验证要迁移的配置，然后将配置推送到 管理中心。

步骤 10 查看迁移后报告，手动设置其他配置并部署到 威胁防御，完成迁移。

有关详细信息，请参阅[查看迁移后报告并完成迁移](#)，第 27 页。

步骤 11 使用您在计划迁移时创建的测试计划测试 Firepower 2100 系列 设备。

在维护窗口期间执行以下任务

开始之前

确保您已完成所有必须在维护窗口之前执行的任务。请参阅[在维护窗口之前执行以下任务](#)，第 43 页。

步骤 1 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

步骤 2 执行从周围交换基础设施到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试，确保它们可访问。

步骤 3 执行从需要第 3 层路由的设备到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试。

步骤 4 如果要为 Firepower 2100 系列 设备分配新的 IP 地址，而不是重新使用分配给 设备的 IP 地址，请执行以下步骤：

1. 更新指向该 IP 地址的任何静态路由，以使其现在指向 Firepower 2100 系列 设备 IP 地址。
2. 如果使用路由协议，请确保邻居将 Firepower 2100 系列 设备 IP 地址视为预期的下一跳目标。

步骤 5 运行全面的测试计划并监控管理 Firepower 2100 设备的 管理中心。



附录 C

云交付的防火墙管理中心迁移

• 云交付的防火墙管理中心迁移，第 45 页

云交付的防火墙管理中心迁移

云交付的防火墙管理中心是一个用于威胁防御设备的管理平台，它通过思科防御协调器 (CDO) 交付。云交付的防火墙管理中心提供了许多与管理中心相同的功能。

您可以从 CDO 访问云交付的防火墙管理中心。CDO 通过安全设备连接器 (SDC) 连接到云交付的防火墙管理中心。有关云交付的防火墙管理中心的更多信息，请参阅[使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 设备](#)。

Cisco Secure Firewall 迁移工具 3.0 现在支持将云交付的防火墙管理中心作为迁移的目标管理中心。

CDO 区域

CDO 可用于三个不同的区域中，并且可以使用 URL 扩展名来标识这些区域。

表 6: CDO 区域和 URL

地区	CDO URL
欧洲地区	https://defenseorchestrator.eu/
美国地区	https://defenseorchestrator.com/
总裁	https://www.apj.cdo.cisco.com/

从 CDO 门户生成 API 令牌

要从 CDO 门户生成 API 令牌，请执行以下步骤：

1. 登录到 CDO 门户。
2. 导航至设置 (Settings) > 常规设置 (General Settings) 以生成并复制 API 令牌。

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。