

Firepower 迁移工具发行说明 v 1.3

首次发布日期: 2019 年 4 月 9 日

上次修改日期: 2019 年 10 月 31 日

欢迎使用 Firepower 迁移工具

本文档提供思科 Firepower 迁移工具的重要和版本特定信息。即使您熟悉 Firepower 版本，并且在迁移方面积累了经验，也要仔细阅读并理解本文档。

此版本中的新增功能

在此版本中，添加了以下功能：

- **ASA 登录：**借助迁移工具，您可以使用管理员凭证连接到 ASA，并按照 ASA 上的配置启用密码。

如果 ASA 没有配置启用密码，可以在迁移工具中将此字段留空。

- **支持捆绑功能：**如果迁移失败，提供客户支持以下载日志文件、数据库和配置文件。您还可以通过电子邮件向技术团队递交支持案例。

- **不迁移对 NAT 和路由的支持：**迁移工具提供了相应的支持，可跳过并不迁移所选的 NAT 规则和路由接口。之前版本的迁移工具仅为访问控制规则提供此选项。

- **支持 IPv6：**支持在对象、接口、ACL、NAT 和路由中迁移 IPv6 配置。

- **接口映射增强功能：**借助迁移工具，您可以将 ASA 接口名称映射到 FTD 对象类型（物理接口、端口通道和子接口）上的物理接口。例如，您可以将 ASA 中的端口通道映射到 FMC 中的物理接口。

- **内联分组支持：**迁移工具可用于解析 CSM 或 ASDM 托管配置。

当您选择清除内联分组 CSM 或 ASDM 托管配置时，预定义对象将替换为实际对象或成员名称。

如果不清除 CSM 或 ASDM 托管配置，预定义的对象名称将保留用于迁移。

- **各项更新**

- 您可以从查看和验证配置屏幕以 excel 或 CSV 格式下载解析的“访问控制”、“NAT”、“网络对象”、“端口对象”、“接口”和“路由”配置项。



注释 您无法导入 CSV 文件。

- 现在，您可以在 app_config 文件中配置批量推送的批处理大小限制，如下所示：

- 对于对象，批处理大小不能超过 500。迁移工具将值重置为 50 并继续批量推送。
- 对于 ACL、路由和 NAT，每个批处理大小不能超过 1000。迁移工具将值重置为 1000 并继续批量推送。

支持的配置

迁移支持以下配置元素：

- 网络对象
- 服务对象（在 Firepower 威胁防御中称为端口对象）
- 访问列表
- NAT 规则
- 接口（例外：冗余、路由模式-BVI、VTI（隧道接口））



注释 如果源 ASA 有端口通道接口，则必须在 Firepower 管理中心上创建端口通道接口；系统会自动创建子接口。

- 静态路由（无 SLA 跟踪，不支持动态路由）
- 已路由和透明防火墙模式
- 网络对象和组、ACL 及路由中支持的名称命令参考

迁移工作流程



注释 从版本 2.0 开始，迁移工具支持将检查点配置迁移到 FTD。请注意以下重要提示是迁移工作流的一部分。

您可以通过遵循以下方法之一来获取用于迁移的 ASA 配置项目：

- **手动上传方法：** 在单一上下文模式下，使用 **show run** 命令获取 ASA 配置。在多上下文模式下，使用 **show tech** 命令获取 ASA 配置
- **从迁移工具连接到 ASA：** 在多上下文 ASA 中，选择连接到 ASA 后要迁移的上下文，然后选择目标 Firepower 威胁防御设备。当您完成第一个情景的迁移后，重复这些步骤以迁移其他情景 - 连接到 ASA、选择要迁移的情景、选择目标 Firepower 威胁防御设备。

您可以通过手动上传方法获取用于迁移的检查点配置项。要通过手动上传方法收集检查点配置，请执行以下操作：

- **使用检查点 Web 可视化工具 (WVT) 导出配置：** 打开命令提示符窗口，到保存和提取 WVT 的目录，然后执行以下命令以获取检查点配置：

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file] [-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go] [-w Web_Visualization_Tool_installation_directory]
```
- **使用 FMT-CP 配置提取程序工具导出设备配置：** 打开 FMT-CP 配置提取程序工具，该工具是工作站上有权访问检查点安全网关的可执行文件 (.exe)。
- **压缩导出的文件：** 选择所有 8 个文件（Web 可视化工具 (WVT) 中的 7 个文件和 FMT-CP 配置提取程序工具中的一个 .txt 文件）并将其压缩为 Zip 文件。

Firepower 迁移工具功能

Firepower 迁移工具提供以下功能：

- 在迁移过程中进行验证，包括解析和推送操作
- 对象重复使用功能
- 对象冲突解决
- 接口映射
- 自动创建或重用接口对象（如果是安全区域和接口组映射，则为 ASA 名称）
- 支持创建用户定义的安全区域和接口组
- 目标 Firepower 威胁防御设备的子接口限制检查
- 支持的平台
 - 虚拟 ASA 到虚拟 FTD
 - 相同的硬件迁移（X 到 X 设备的迁移）
 - X 到 Y 设备的迁移（Y 的接口数量更大）

迁移报告

Firepower 迁移工具以 HTML 格式提供以下报告及迁移详情：

- 迁移前报告
- 迁移后报告

Firepower 迁移工具的平台要求

迁移工具对基础设施和平台的要求如下：

- Windows 10 操作系统或者 macOS 10.13 及更高版本
- 作为系统默认浏览器的 Google Chrome
- 每个系统的单一工具实例
- Firepower 管理中心和 Firepower 威胁防御必须为 6.2.3.3 或以上版本

文档

本发行说明附带以下文档：

- *Firepower* 迁移工具发行说明
- 利用 *Firepower* 迁移工具将 *ASA* 迁移到 *Firepower* 威胁防御
- 思科 *Firepower* 迁移工具中使用的开源

尚未解决和已解决的漏洞

可通过思科缺陷搜索工具查看这一版本中尚未解决和已解决的缺陷。通过这一基于 Web 的工具，您可以访问思科缺陷追踪系统，其中记录了关于此本产品和其他思科硬件及软件产品的缺陷和漏洞信息。



注释

您必须拥有 Cisco.com 帐户才能登录并访问思科缺陷搜索工具。如果没有，可以在 [Cisco.com](https://www.cisco.com) 上注册帐户。有关漏洞搜索工具的详细信息，请参阅[漏洞搜索工具帮助](#)。

在 Firepower 迁移工具中使用以下动态查询来获取最新的未解决和已解决警告问题列表：

- [未解决的警告](#)
- [已解决的警告](#)

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.

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: www.cisco.com/go/trademarks. 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)

© 2019 Cisco Systems, Inc. 保留所有权利。