思科 ASA 到 Firepower 威胁防御迁移指南，版本 6.2

首次发布日期: 2017 年 01 月 23 日

上次修改日期: 2017 年 02 月 08 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

文本部件号:

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。版权所有 © 1981，加州大学董事会。

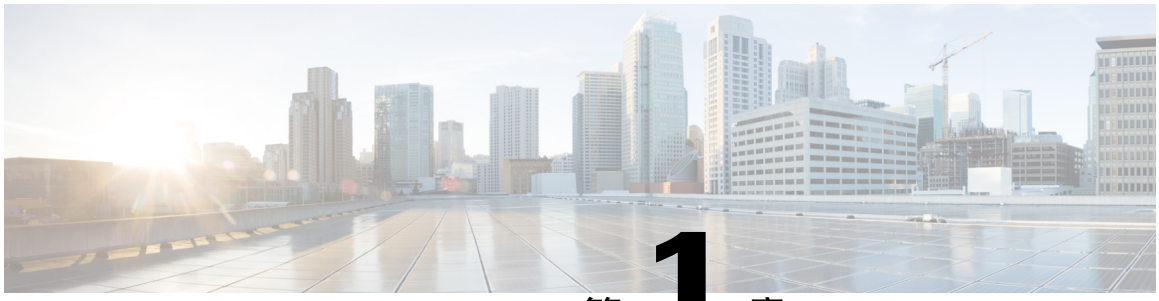
无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此网址：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录



第 1 章

思科 ASA 到 Firepower 威胁防御 迁移简介

本指南介绍如何使用思科的迁移工具从您的思科 ASA 中的防火墙策略设置迁移到 Firepower 威胁防御 设备。

思科 ASA 提供有状态的高级防火墙和 VPN 集中器功能。它长期以来一直是防火墙的行业标准。有关此产品的详细信息，请参阅 http://www.cisco.com/go/asa。

Firepower 威胁防御 表示在防火墙发展道路上又迈进了一步。它提供统一的下一代防火墙和下一代 IPS 功能。除了 Firepower 软件型号上可用的 IPS 功能之外，防火墙和平台功能还包括站点到站点 VPN、稳健路由、NAT、集群以及应用可视性和访问控制中的其他优化功能。Firepower 威胁防御 还支持高级恶意软件保护 (AMP) 和 URL 过滤。有关此产品的详细信息，请参阅 http://www.cisco.com/go/ngfw。

思科的迁移工具支持您将 ASA 配置中的特定功能转换为 Firepower 威胁防御 配置中的等同功能。在此转换后，思科建议您通过调整转换的策略并配置其他 Firepower 威胁防御 策略来手动完成迁移。

您可以将 ASA 配置迁移到新的 Firepower 威胁防御 设备，也可以在迁移到原始 ASA 设备（该设备作为 Firepower 威胁防御 设备被刷新后）。

迁移工具

要将 ASA 配置迁移到 Firepower 威胁防御 配置 Firepower 管理中心，请使用 ASA 到 Firepower 威胁防御迁移工具映像来准备专用 适用于 VMware 的 Firepower 管理中心虚拟。此专用管理中心不与任何设备通信。相反，该迁移工具允许您将 .cfg 或 .txt 格式的 ASA 配置文件转换为 .sfo 格式的 Firepower 导入文件，然后您可以在您的生产管理中心上导入该文件。

该迁移工具只能转换 ASA 配置格式的数据（即按照正确顺序排列的 ASA CLI 命令的平面文件）。当您使用该迁移工具时，系统会验证文件的格式。例如，文件必须包含ASA版本命令。如果系统无法验证该文件，则转换会失败。

ASA 设备要求

迁移工具可以从以下 ASA 设备迁移配置数据：

表 *1*：支持的平台和环境

支持的平台	支持的环境
任意	ASA 版本 9.7/ASDM 版本 7.7 ASA 版本 9.6/ASDM 版本 7.6 ASA 版本 9.5/ASDM 版本 7.5 ASA 版本 9.4/ASDM 版本 7.4 ASA 版本 9.3/ASDM 版本 7.3 ASA 版本 9.2/ASDM 版本 7.2 ASA 版本 9.1/ASDM 版本 7.1

此外，ASA 设备必须：

- 在单情景模式下运行。
- 是活动设备（如果它是故障切换对的一部分）。
- 是主设备（如果它是集群的一部分）。

ASA 设备可以在透明模式或路由模式下运行。

Firepower 设备要求

本文档中介绍的迁移过程需要以下 Firepower 设备：

- 在专用适用于 VMware 的 Firepower 管理中心虚拟 上运行的迁移工具。

- 您的生产 Firepower 管理中心。必须在受支持的平台上运行受支持的环境：

受支持的 Firepower 管理中心平台	受支持的 Firepower 管理中心环境
Firepower 管理中心：FS750、FS1500、FS2000、FS3500、FS4000、虚拟	必须是与迁移工具相同的版本。

- 您的生产 Firepower 威胁防御设备（可以是重新映像的 ASA 设备)。有关 Firepower 威胁防御 的受支持平台和环境的列表，请参阅 *Firepower* 系统兼容性指南。

许可证要求

若要使用本文档中介绍的迁移配置，您必须获有 Firepower 威胁防御 基本许可证。有关详细信息，请参阅 http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html。

迁移工具不会迁移许可证信息，因为 ASA 设备需要与 Firepower 威胁防御 设备不同的许可证。您必须为您的 Firepower 威胁防御 设备购买新许可证。若对迁移方面的许可证定价有任何疑问，请联系销售人员。

支持进行迁移的 ASA 功能

迁移工具支持您迁移以下 ASA 功能：

- 扩展的访问规则（可以分配给接口和全局分配）
- 两次 NAT 和网络对象 NAT 规则
- 与该工具转换的扩展访问规则和 NAT 规则关联的任何网络对象/组或服务对象/组

有关该工具如何将 ASA 配置转换为 Firepower 威胁防御 配置的说明，请参阅转换映射概述 ， 第 15 页。

迁移限制

迁移您的 ASA 配置时，请注意以下限制：

仅 ASA 配置

迁移工具仅转换 ASA 配置。它不会转换现有 ASA FirePOWER 配置。您必须手动将现有 ASA FirePOWER 配置转换为 Firepower 威胁防御 配置。

ACL 和 ACE 限制

该迁移工具支持包含总计多达 *2000000* 个访问规则元素的 ASA 配置文件。如果已转换的配置文件超过此限制，则迁移会失败。

您必须考虑ASA配置文件中所有访问规则元素的总和，而不是单个ACL的元素计数。要查看单个 ACL 的元素，请使用 ASA CLI 命令 `show access-list | i elements`。

仅应用的规则和对象

迁移工具仅转换应用于接口的 ACL；即，ASA 配置文件必须包含配对的 **access-list** 和 **access-group** 命令。

迁移工具仅转换与有效应用的 ACL 或 NAT 规则关联的对象；即，ASA 配置文件必须包含相应关联的 **object**、**access-list**、**access-group** 和 **nat** 命令。您无法单独迁移网络和服务对象。

不受支持的 ACL 和 NAT 配置

迁移工具支持大多数 ACL 和 NAT 配置，但存在一些例外。它处理不受支持的 ACL 和 NAT 配置的方法如下所示：

转换但会禁用 - 该迁移工具无法完全转换使用以下内容的 ACE：

- 时间范围对象
- 完全限定域名 (FQDN)
- 本地用户或用户组。
- 安全组 (SGT) 对象
- 源端口和目标端口的嵌套服务组

  它无法转换这些规则的某些元素，因为没有用于不受支持元素的等同Firepower功能。在这些情况下，该工具会转换具有等同Firepower功能的规则元素（例如，源网络），排除没有等同Firepower功能的规则元素（例如，时间范围），并在它创建的新访问控制或预过滤器策略中禁用该规则。

  对于每个禁用的规则，系统还会为规则名称附加 `(unsupported)`，并为该规则添加注释以指明系统为什么在迁移期间禁用该规则。在您的 Firepower 管理中心上导入禁用的规则后，您可以手动编辑或替换规则，以在 Firepower 系统中成功部署。

排除 - 该迁移工具会从其创建的策略中排除以下配置：EtherType 或 WebType ACL、使用主机地址名称别名的 ACE（由 **name** 命令指定）以及使用预定义（默认）服务对象的 ACE。有关这些已排除的配置的详细信息，请参阅 *CLI* 手册 *2*：思科 *ASA* 系列防火墙 *CLI* 配置指南或 *ASDM* 手册 *2*：思科 *ASA* 系列防火墙 *ASDM* 配置指南。

其他不受支持的 ASA 配置

该迁移工具不支持迁移本文档中指定的 ASA 功能之外的 ASA 功能。该工具处理 ASA 配置文件时，将忽略不受支持的功能的任何配置数据。

迁移检查清单

在使用该迁移工具之前，请验证以下项：

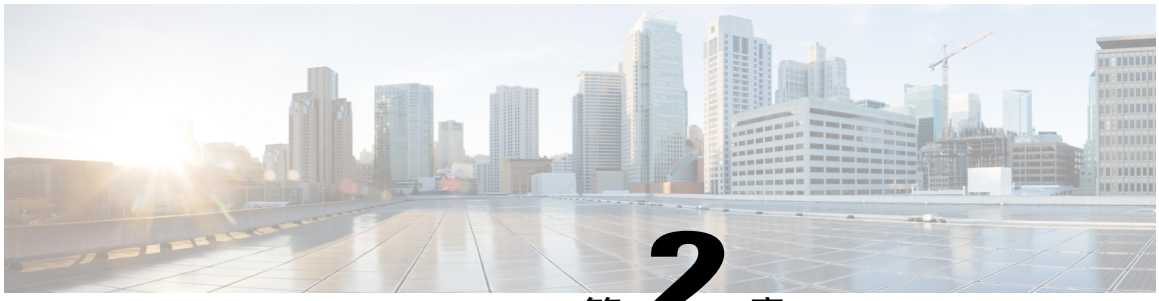
- ASA 设备符合迁移的所有要求；参阅ASA 设备要求，第 2 页。
- ASA 配置文件为 .cfg 或 .txt 格式。
- ASA 配置文件仅包含支持的配置且符合迁移所需的限制；参阅迁移限制，第 3 页。
- ASA 配置文件仅包含有效的 ASA CLI 配置。先更正任何不正确或不完整的命令，然后再继续。如果文件包含无效配置，迁移会失败。
- 要导入已转换的 ASA 配置文件，Firepower 管理中心必须运行与您转换配置所用的迁移工具相同的版本。此限制适用于主要版本和次要版本。例如，如果迁移工具运行的是 6.2 版本，但是您要导入文件的 Firepower 管理中心运行的是 6.1.0.2 版本，则您必须先升级到 Firepower 管理中心 6.2.0，然后才能导入转换的 ASA 配置文件。

文档体例

本文档提供将 ASA 配置转换为 Firepower 威胁防御 配置的示例。这些示例中的大多数列会直接映射至 Firepower 管理中心 上相关规则编辑器或对象管理器中的组件。下表列出了不直接映射至 Firepower UI 组件的列。

表 *2*：使用间接值的列

列	值	说明
启用	True/False	指定在访问控制或预过滤器规则中选中还是取消选中 **Enabled** 复选框。
操作	允许等同项	指定您在转换期间做出的选择所确定的值，如下所示： • 如果您选择将访问规则转换为访问控制规则，则还需选择此值是 **Allow** 还是 **Trust**。 • 如果您选择将访问规则转换为预过滤器规则，则还需选择此值是 **Fastpath** 还是 **Analyze**。
域	无	在转换时，此字段为空，因为系统不会分配域，直到您在您的生产 Firepower 管理中心上将其导入。在导入时，系统会根据您导入已转换配置的域分配域。
覆盖	True/False	指定在该对象中是选中还是取消选中 **Allow Overrides** 复选框。



第 2 章

将 ASA 配置迁移到 Firepower 威胁防御 配置

准备 ASA 以进行迁移

步骤 1 验证 ASA 设备是否符合配置迁移的要求；参阅 ASA 设备要求，第 2 页。

步骤 2 确定您要导出的访问控制列表 (ACL) 和 NAT 策略。

步骤 3 确定 ACL 中有多少个条目：

```
show access-list acl_name | i elements
```

步骤 4 如果配置包含超过 2000000 个元素，请尽可能多地删除无关紧要的元素。

安装迁移工具

注意 **请勿**在生产 Firepower 管理中心 上安装迁移工具。不支持在生产设备上使用该工具。在安装迁移工具后，您可以通过重新映像指定的 Firepower 管理中心 来卸载该工具。

步骤 1 从技术支持下载以下映像之一：

- 适用于 VMware 的 Firepower 管理中心虚拟
- 适用于 KVM 的 Firepower 管理中心虚拟

步骤 2 使用映像文件安装专用 Firepower 管理中心虚拟，如相应指南中所述：

- 适用于 *VMware* 部署的思科虚拟 *Firepower* 管理中心快速入门指南
- 适用于 *KVM* 部署的思科虚拟 *Firepower* 管理中心快速入门指南

步骤 3 使用 `admin` 用户名通过 `ssh` 连接到 Firepower 管理中心。

步骤 4 登录到根外壳：

```
sudo su -
```

步骤 5 运行以下命令：

```
enableMigrationTool.pl
```

注释 该过程完成后，刷新在 Firepower 管理中心 上运行的任何 Web 接口会话以使用该迁移工具。

保存 ASA 配置文件

迁移工具可以转换 .cfg 或 .txt 格式的 ASA 配置文件。

步骤 1 保存配置。
保存此配置所用的命令可能因您的ASA 设备版本而异。有关详细信息，请参阅相应版本的ASA配置指南，其在 http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#pgfId-126642 上的 ASA 文档规划图中列出。

步骤 2 将保存的配置文件转移到可从迁移工具访问的位置（例如，您的本地计算机或网络上的共享驱动器）。

转换 ASA 配置文件

按照以下步骤将 ASA 配置文件（.cfg 或 .txt）转换为 Firepower 配置文件 (.sfo)。

注意 迁移工具 UI 是 Firepower 管理中心 UI 的扩展。但是，仅在此程序中介绍的功能可行。

步骤 1 在迁移工具中，选择 **系统 (System)** > **工具 (Tools)** > **导出/导出 (Import/Export)**

步骤 2 点击 **Upload Package**。

步骤 3 点击 **Browse**，然后选择从 ASA 导出的配置文件。

步骤 4 点击 **Next**。

步骤 5 选择您希望系统在转换访问规则时使用的策略：

- **Prefilter Policy** - 将访问规则转换为预过滤器规则。
- **Access Control Policy** - 将访问规则转换为访问控制规则。

步骤 6 如果您选择了 **Prefilter Policy**，请选择您希望系统为具有允许操作的访问规则分配的操作：

- **Fastpath** - 让匹配流量免于进行进一步的各项检查和控制，包括访问控制、身份要求和速率限制。对隧道执行快速路径操作可为所有封装连接提供快速路径。
- **Analyze** - 允许其余访问控制继续分析流量。如果此流量通过访问控制和所有相关深度检查，则它也可能会受到速率限制。

步骤 7 如果您选择了 **Access Control Policy**，请选择您希望系统为具有允许操作的规则分配的操作：

- **Trust** - 允许流量通过，无需深度检查或网络发现。受信任的流量仍需符合身份策略施加的身份验证要求，以及速率限制。
- **Allow** - 允许匹配的流量通过。允许的流量仍需符合身份策略施加的身份验证要求、速率限制以及深度检查（如果已配置）。

步骤 8 指定您希望系统如何处理不受支持的规则：

- 作为禁用规则转换
- 不转换且不添加到迁移报告

步骤 9 选择系统在转换启用了日志记录的访问规则时应分配的操作：

- 在连接开始时
- 在连接结束时

- 两者

步骤 10 选择 **Next**。
系统将迁移作为任务排队。您可以在消息中心查看任务的状态。

步骤 11 点击 System Status 图标以显示消息中心。

步骤 12 点击 **Tasks** 选项卡。
迁移任务作为顶级消息列出，因为只有迁移工具任务可以在中间 Firepower 管理中心 上运行。

步骤 13 如果迁移失败，请查看相应日志中的错误消息；有关详细信息，请参阅排除转换故障，第 10 页。

步骤 14 如果迁移成功：

- 点击 **Download .sfo** 将转换的文件复制到本地计算机。
- 点击 **Migration Report** 查看迁移报告。

步骤 15 查看迁移报告。
迁移报告总结了迁移工具可能或无法成功转换为 Firepower 威胁防御 配置的 ASA 配置。未成功转换的配置包括：

- Firepower 系统中不支持的 ASA 配置
- Firepower 系统（具有 Firepower 等同项）中支持但迁移工具不转换的 ASA 配置

对于具有 Firepower 等同项的未成功转换配置，您可以在将转换的策略导入您的生产 Firepower 管理中心后手动添加它们。

排除转换故障

如果在专用 Firepower 管理中心 上转换失败，则迁移工具会在可下载至本地计算机的故障排除文件中记录错误数据。

步骤 1 选择**系统 (System)** > **运行状况 (Health)** > **监控器 (Monitor)**。

步骤 2 在设备列表的 **Appliance** 列中，点击专用 Firepower 管理中心 的名称。

步骤 3 点击 **Generate Troubleshooting Files**。

步骤 4 选中 **All Data** 复选框。

步骤 5 点击 **Generate**。

系统将故障排除文件的生成作为一项任务进行排队。

步骤 6 通过在消息中心查看任务来跟踪任务的进度。

步骤 7 在系统生成故障排除文件并且任务状态变更为 `Completed` 之后，点击 **Click to retrieve generated files**。

步骤 8 按照思科技术支持中心的指示将故障排除文件发送给思科。

导入转换的 ASA 配置

在 Firepower 管理中心 的多域部署中，系统会将转换的 ASA 配置分配到您将其导入的域。在导入时，系统会在转换的对象中填充 **Domain** 字段。

步骤 1 在您的生产 Firepower 管理中心上，选择 **系统 (System)** > **工具 (Tools)** > **导出/导出 (Import/Export)**

步骤 2 点击 **Upload Package**。

步骤 3 点击 **Choose File**，然后使用 Browse 选择本地计算机上的相应 .sfo 文件。

步骤 4 点击**Upload**。

步骤 5 选择要导入的策略。策略可以包含访问控制策略、预过滤器策略或 NAT 策略，具体取决于先前的迁移选择。

步骤 6 点击 **Import**。
系统会分析该文件并显示 Import Conflict 页面。

步骤 7 在 Import Conflict 页面上：

- 解决配置中的冲突；请参阅 *Firepower* 管理中心配置指南 中的“导入冲突解决方法”。
- 复制在原始 ASA 配置中按接口对规则分组的方式，或将该组关联替换为新的组管理。为此，您必须将访问控制规则分配给安全区，并将预过滤器或 NAT 规则分配给接口组，如下所示：

类型	来源	在以下情况下选择此区域或组：
系统生成的安全区域/接口组	迁移工具在转换期间会自动创建此安全区/接口组。	您希望复制在原始 ASA 配置中按接口对规则分组的方式。
在导入转换的 ASA 配置之前创建的安全区/接口组	您在导入转换的 ASA 配置之前创建此安全区/接口组。	您希望将这些规则与 Firepower 管理中心中已存在的安全区/接口组相关联。
在导入过程中即时创建的安全区/接口组	您通过从规则集旁边的下拉列表中选择 `New...` 创建此安全区/接口组。	您希望将这些规则与 Firepower 管理中心中的新安全区/接口组相关联。

提示 使用规则集旁边的箭头展开有关该集的其他信息。

注释　迁移工具不会转换接口配置；您必须手动添加设备并在导入转换的 ASA 配置后配置这些设备上的接口。但是，此导入步骤让您可以保留 ACL 或 NAT 策略与单个实体（安全区或接口组）之间的关联，以便您可以在新的 Firepower 威胁防御设备上将该实体与接口快速关联。有关将安全区/接口组与接口相关联的详细信息，请参阅配置迁移的策略，第 13 页。

步骤 8　点击 **Import**。
当导入完成时，系统会显示消息指导您访问消息中心。

步骤 9　点击 System Status 图标以显示消息中心。

步骤 10　点击 **Tasks** 选项卡。

步骤 11　点击导入任务中的链接以下载导入报告。

安装 Firepower 威胁防御

使用下表列出的相应快速入门指南安装 Firepower 威胁防御。

注释　快速入门指南程序包括在设备上安装新映像，以便您无论在新设备上安装 Firepower 威胁防御 还是将原始 ASA 重新映像到 Firepower 威胁防御 都可使用相同的程序。

平台	快速入门指南
Firepower 威胁防御：ASA 5506-X、ASA 5506H-X、ASA 5506W-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X、ASA 5545-X 和 ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
具备威胁防御的 Firepower 4100 系列：4110、4120 和 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
具备威胁防御的 Firepower 9300	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html
Firepower 威胁防御虚拟：VMware	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html
Firepower 威胁防御虚拟：AWS Cloud	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

配置迁移的策略

此程序介绍在 Firepower 管理中心 上配置迁移的策略的概要步骤。有关每个步骤的详细信息，请参阅 *Firepower* 管理中心配置指南 中的相关程序。

步骤 1 将 Firepower 威胁防御 设备上的接口分配给在转换过程中创建的安全区或接口组。

步骤 2 如果将 ASA 访问规则迁移到访问控制策略：

- （可选）通过启用或编辑已禁用的规则、添加规则、删除规则以及更改规则顺序来调整该策略中的规则。例如，您可能希望编辑指定不同源和目标协议或多个协议的任何规则；参阅指定多个协议的访问规则，第 25 页。
- （可选）为该工具不转换的 ASA 参数配置 Firepower 等同项：

访问规则参数	访问控制规则参数
用户	选定用户条件
安全组（源）	自定义 SGT 条件
启用日志记录	Log at Beginning of Connection 和/或 Log at End of Connection
日志记录级别	连接事件日志记录
日志记录间隔	连接事件日志记录

- 将访问控制策略分配到 Firepower 威胁防御 设备：

步骤 3 如果将 ASA 访问规则迁移到预过滤器策略：

- （可选）通过启用或编辑已禁用的规则、添加规则、删除规则以及更改规则顺序来调整该策略中的规则。例如，您可能希望编辑指定不同源和目标协议或多个协议的任何规则；参阅指定多个协议的访问规则，第 25 页。
- （可选）为该工具不转换的 ASA 参数配置 Firepower 等同项：

访问规则参数	预过滤器规则参数
启用日志记录	Log at Beginning of Connection 和/或 Log at End of Connection
日志记录级别	连接事件日志记录
日志记录间隔	连接事件日志记录

- 配置系统在转换期间创建的新访问控制策略，或将预过滤器策略与其他访问控制策略相关联。
- 将关联的访问控制策略分配到 Firepower 威胁防御 设备：

步骤 4 如果迁移 NAT 策略：

- （可选）通过启用或编辑已禁用的规则、添加规则、删除规则以及更改规则顺序来调整该策略中的规则。
- 将 NAT 策略分配到 Firepower 威胁防御 设备：

步骤 5 （可选）配置下一代防火墙功能，包括应用可视性与可控性、入侵保护、URL过滤和高级恶意软件防护(AMP)。

步骤 6 部署配置更改；请参阅部署配置更改，第 14 页。

部署配置更改

使用以下步骤部署迁移的配置。有关部署过程的详细信息，请参阅 *Firepower* 管理中心配置指南中的“部署配置更改”

步骤 1 在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。
“部署策略”(Deploy Policies) 对话框列出具有过期配置的设备。对话框顶部的**版本 (Version)** 指定上次进行配置更改的时间。设备表中的**当前版本 (Current Version)** 列指定上次将更改部署到每个设备的时间。

步骤 2 识别并选择要部署配置更改的设备。

- 排序 - 通过点击列标题对设备列表进行排序。
- 展开 - 点击加号图标 ( )，展开设备列表以查看要部署的配置更改。系统使用索引 ( ) 图标标记过期策略。
- 过滤 - 过滤设备列表。点击显示的任何列标题右上角的箭头，在**过滤器 (Filter)** 文本框中输入文本，然后按 Enter 键。

步骤 3 点击 **Deploy**（**部署**）。

步骤 4 如果系统识别出要部署的更改中的错误或警告，有以下选项可供选择：

- 继续 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 取消 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

附 录 A

转换映射

以下主题介绍迁移工具如何将 ASA 配置转换为 Firepower 威胁防御 配置：

转换映射概述

该迁移工具会按如下所示将 ASA 配置转换为 Firepower 威胁防御 配置：

表 *3*：转换映射摘要

实体	ASA 配置	Firepower 威胁防御 配置
网络对象	网络对象 网络对象组 嵌套网络对象组	网络对象 网络对象组 嵌套网络对象组
服务对象	服务对象 服务对象组 嵌套服务对象组	端口对象 端口对象组 平化端口对象组

实体	ASA 配置	Firepower 威胁防御 配置
访问规则	访问规则	访问控制策略或预过滤器策略（按照选择）
NAT 规则	两次 NAT 规则 网络对象 NAT 规则	手动 NAT 规则 自动 NAT 规则

转换的配置的命名约定

将 ASA 访问规则、NAT 规则和相关对象转换为 Firepower 威胁防御 等同项时，该迁移工具使用下文介绍的命名约定。

对象和对象组名称

转换对象和对象组时，该迁移工具会保留 ASA 配置文件中对象和对象组的名称。

例如：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
```

该工具将此配置转换为名为 `obj1` 和 `obj2` 的网络对象，以及名为 `obj_group1` 的网络对象组。

将服务对象和服务组转换为端口对象和端口对象组时，该工具在某些情况下会在原始对象或组名称后附加以下扩展名：

表 *4*：转换的服务对象和组的扩展名

扩展名	附加原因
`_dst`	将具有源和目标端口的服务对象拆分为两个端口对象。系统将此扩展名附加到用于存储转换后的目标端口数据的服务对象。有关详细信息，请参阅具有源和目标端口的服务对象，第 33 页。
`_src`	将具有源和目标端口的服务对象拆分为两个端口对象。系统将此扩展名附加到用于存储转换后的源端口数据的服务对象。有关详细信息，请参阅具有源和目标端口的服务对象，第 33 页。
`_#`	转换一个嵌套服务组；参阅嵌套服务组转换，第 35 页。

策略名称

ASA 配置文件包含一个 `hostname` 参数，用于指定 ASA 的主机名。迁移工具使用此值来命名其在转换文件时创建的策略：

- 访问控制策略 - *hostname*-AccessPolicy-*conversion_date*
- 预过滤器策略 - *hostname*-PrefilterPolicy-*conversion_date*
- NAT 策略 - *hostname*-NATPolicy-*conversion_date*

规则名称

对于转换的访问控制、预过滤器和 NAT 规则，系统会使用以下格式为每个新规则命名：

ACL_name-#rule_index

其中：

- *ACL_name* - 该规则所属的 ACL 的名称。
- *rule_index* - 系统生成的整数，指定相对于 ACL 中的其他规则转换该规则的顺序。

例如：

```
acl1#1
```

如果系统在服务对象转换期间必须将单个访问规则扩展到多个规则，则系统会附加一个扩展名：

ACL_name#rule_index_sub_index

其中附加的 # 表示新规则在扩展的序列中的位置。

例如：

```
acl1#1_1
acl1#1_2
```

如果系统确定规则名称长度超过 30 个字符，系统则会缩短 ACL 名称并以波形符 (~) 作为缩短名称的结尾：

```
ACL Name~#rule index
```

例如，如果原始 ACL 名称为 `accesslist_for_outbound_traffic`，则系统会将 ACL 名称截断为：

```
accesslist_for_outbound_tr~#1
```

安全区和接口组名称

迁移工具在 ASA 配置文件中转换 `access-group` 命令时，系统会通过创建安全区或接口组（根据您在转换期间进行的选择）捕获该命令中的入口和出口信息。它使用以下格式为这些新安全区或接口组命名：

`ACL_name_interface_name_direction_keyword_``zone`

其中：

- *ACL_name* - `access-group` 命令中的 ACL 名称。

- *interface_name* - `access-group` 命令中的接口名称。
- *direction_keyword* - `access-group` 命令中的方向关键字（`in` 或 `out`）。

例如：

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

该工具将此配置转换为名为 `acp1_outside_in_zone` 的安全区或接口组。

特定于 Firepower 对象和对象组的字段

Firepower 网络和端口对象/组中的少量字段是 ASA 对象和组中没有的。该迁移工具使用以下默认值填充已转换的网络和端口对象/组中的 Firepower 特定字段：

表 *5*：特定于 *Firepower* 对象/组的字段的默认值

Firepower 对象/组中的字段	转换的 ASA 对象/组的默认值
域	无
覆盖	错误

有关这些默认值的详细信息，请参阅文档体例，第 5 页。

访问规则转换

迁移工具可以将ASA访问规则转换为访问控制规则或预过滤器规则，具体取决于您在迁移过程中做出的选择。

访问规则转换为访问控制规则

如果您选择将 ASA 访问规则转换为 Firepower 威胁防御 访问控制规则：

- 系统将转换的规则添加到访问控制策略的 **Default** 规则部分。
- 系统会保留 Description 字段内容作为 **Comment History** 中与规则对应的条目。
- 系统会向 **Comment History** 添加条目，将该规则标识为已转换。
- 系统会按如下所示设置访问控制规则的 **Action**：

访问规则的操作	访问控制规则的操作
允许	**Allow** 或 **Trust**，具体取决于迁移时做出的选择

访问规则的操作	访问控制规则的操作
拒绝	**Block**

- 系统会设置访问控制规则的 **Source Zones** 和 **Destination Zones**，如下所示：

ACL 类型	源区域	目标区域
全局（应用于 `Any` 接口）	任何环境	任何环境
应用于特定接口	您在导入过程中选择的安全区	任意

- 如果访问规则处于非活动状态，该工具会将其转换为禁用的访问控制规则。

迁移工具会将转换的规则分配到具有以下默认参数的访问控制策略：

- 系统将新访问控制策略的默认操作设置为 **Block All Traffic**。
- 系统将访问控制策略与默认预过滤器策略相关联。

映射到访问控制规则字段的访问规则字段

迁移工具按照下表所述，将 ASA 访问规则中的字段转换为 Firepower 威胁防御 访问控制规则中的字段。

注意：

- 列 1（ASA 访问规则字段）中的字段名称对应于 ASDM 接口中的字段标签。
- 列 2（Firepower 访问控制规则字段）中的字段名称对应于 Firepower 管理中心 接口中的字段标签。

表 *6*：映射到 *Firepower* 访问控制规则字段的 *ASA* 访问规则字段

ASA 访问规则字段	**Firepower** 访问控制规则字段
接口	无等同字段
操作	操作
来源	源网络
用户	不转换；等同于 Selected Users 条件
安全组（源）	不转换；等同于自定义 SGT 条件

ASA 访问规则字段	Firepower 访问控制规则字段
目标	目标网络
安全组（目标）	无等同字段
服务	选定目标端口；如果指定了预定义服务对象，则不转换
说明	备注
启用日志记录	不转换；等同于 Log at Beginning of Connection 或 Log at End of Connection。
日志记录级别	不转换；等同于连接事件日志记录
启用规则	启用
流量方向	无等同字段
源服务	选定源端口；如果指定了预定义服务对象，则不转换
日志记录间隔	不转换；等同于连接事件日志记录
时间范围	无等同字段

特定于访问控制规则的字段

Firepower 威胁防御 访问控制规则包含 ASA 访问规则中不存在的少量字段。该迁移工具使用以下默认值填充已转换的访问控制规则中 Firepower 特定字段：

表 7：特定于访问控制规则的字段的默认值

访问控制规则字段	转换的访问规则的默认值
Name	系统生成（请参阅转换的配置的命名约定，第 16 页）
Source Zone	• 如果全局应用 ACL，则为 `Any` • 如果 ACL 应用于特定接口，则为工具在转换期间创建的安全区

访问控制规则字段	转换的访问规则的默认值
Destination Zone	Any（默认用于所有访问控制规则）
Selected VLAN Tags	没有默认值（您可以在导入后手动添加条件）
Selected Applications and Filters	没有默认值（您可以在导入后手动添加条件）
Selected URLs	没有默认值（您可以在导入后手动添加条件）

访问规则转换为预过滤器规则

如果您选择将 ASA 访问规则转换为 Firepower 威胁防御 预过滤器规则：

- 系统会保留 Description 字段内容作为 **Comment History** 中与规则对应的条目。
- 添加条目到 **Comment History**，将该规则标识为已转换。
- 系统会按如下所示设置预过滤器规则的 **Action**：

访问规则的操作	预过滤器规则的操作
允许	**Fastpath** 或 **Analyze**，具体取决于迁移时做出的选择
拒绝	**Block**

- 系统按如下所示设置预过滤器规则的 **Source Interface Objects** 和 **Destination Interface Objects**：

ACL 类型	源接口对象	目标接口对象
全局（应用于 Any 接口）	任何环境	任何环境
应用于特定接口	您在导入过程中选择的接口组	任意

- 如果访问规则处于非活动状态，该工具会将其转换为禁用的预过滤器规则。

迁移工具会将转换的规则分配到具有以下默认参数的预过滤器策略：

- 系统将新预过滤器策略的默认操作设置为 **Analyze All Tunnel Traffic**。
- 系统创建与预过滤器策略同名的访问控制策略，然后将预过滤器策略与该访问控制策略相关联。系统将新访问控制策略的默认操作设置为 **Block All Traffic**。

映射到预过滤器规则字段的访问规则字段

该迁移工具按照下表所述，将 ASA 访问规则中的字段转换为 Firepower 威胁防御 预过滤器规则中的字段。

注意：

- 列 1（ASA 访问规则字段）中的字段名称对应于 ASDM 接口中的字段标签。
- 列 2（Firepower 预过滤器规则字段）中的字段名称对应于 Firepower 管理中心 接口中的字段标签。

表 *8*：映射到 *Firepower* 预过滤器规则字段的 *ASA* 访问规则字段

ASA 访问规则字段	**Firepower** 预过滤器规则字段
接口	无等同字段
启用规则	启用
操作	操作
来源	源网络
用户	无等同字段
安全组（源）	无等同字段
目标	目标网络
安全组（目标）	无等同字段
服务	选定源端口 选定目标端口
说明	备注
启用日志记录	不转换；等同于 Log at Beginning of Connection 或 Log at End of Connection。
日志记录级别	不转换；等同于连接事件日志记录
流量方向	无等同字段
源服务	选定源端口；如果指定了预定义服务对象，则不转换

ASA 访问规则字段	Firepower 预过滤器规则字段
日志记录间隔	不转换；等同于连接事件日志记录
时间范围	无等同字段

特定于 Firepower 预过滤器规则的字段

Firepower 威胁防御 预过滤器规则包含在 ASA 访问规则中不存在的少量字段。该迁移工具使用以下默认值填充已转换的预过滤器规则中的 Firepower 特定字段：

表 *9*: *Firepower* 特定预过滤器规则的字段的默认值

预过滤器规则字段	转换的访问规则的默认值
Name	系统生成（请参阅转换的配置的命名约定，第 16 页）
Source Interface Objects	• 如果全局应用 ACL，则为 `Any` • 如果 ACL 应用于特定接口，则为工具在转换期间创建的接口组
Destination Interface Objects	`Any`（默认用于所有预过滤器规则）
Selected VLAN Tags	没有默认值（您可以在导入后手动添加条件）

访问规则中的端口参数运算符

扩展访问规则可以包含使用服务对象中所用的相同运算符的 `port_argument` 元素。迁移工具转换访问规则中的这些运算符的方式与其转换服务对象时转换相同运算符的方式略有不同，具体取决于访问规则是包含单个端口参数运算符还是多个端口参数运算符。

下表列出了可能的运算符并提供了单个运算符的使用示例。

表 *10*：访问规则中的端口参数运算符

运算符	描述	示例
`lt`	小于。	`access-list acp1 extended permit tcp any lt 300`
`gt`	大于。	`access-list acp2 extended permit tcp any gt 300`
`eq`	等于。	`access-list acp3 extended permit tcp any eq 300`
`neq`	不等于。	`access-list acp4 extended permit tcp any neq 300`
`range`	值的范围（包括边界值）。使用该运算符时，请指定两个端口编号（例如，range 100 200）。	`access-list acp5 extended permit tcp any range 9000 12000`

如果访问规则包含单个端口参数运算符，迁移工具会将访问规则转换为单个访问控制或预过滤器规则，如下所示：

表 *11*：具有单个端口参数运算符的访问规则转换为访问控制或预过滤器规则

Op	名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
`lt`	acp1#1	任何环境	任何环境	任何环境	任何环境	1-299	任意	允许等同项	真
`gt`	acp2#1	任何环境	任何环境	任何环境	任何环境	301-65535	任意	允许等同项	真
`eq`	acp3#1	任何环境	任何环境	任何环境	任何环境	300	任意	允许等同项	真
`neq`	acp4#1	任何环境	任何环境	任何环境	任何环境	1-299， 301-65535	任意	允许等同项	真
`range`	acp5#1	任何环境	任何环境	任何环境	任何环境	9000-2000	任意	允许等同项	真

此表中的 Original Operator (**Op**) 列是为了清楚起见而提供；它不并不代表访问控制规则中的字段。

如果访问规则包含多个端口运算符（例如，`access-list acp6 extended permit tcp any neq 300 any neq 400`），则迁移工具会将单个访问规则转换为多个访问控制或预过滤器规则，如下所示：

表 *12*：具有多个端口参数运算符的访问规则转换为访问控制规则

Op	名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
neq	acp6#1_1	任何环境	任何环境	任何环境	任何环境	1-299	1-399	允许等同项	真
neq	acp6#1_2	任何环境	任何环境	任何环境	任何环境	301-65535	1-399	允许等同项	真
neq	acp6#1_3	任何环境	任何环境	任何环境	任何环境	1-299	401-65535	允许等同项	真
neq	acp6#1_4	任何环境	任何环境	任何环境	任何环境	301-65535	401-65535	允许等同项	真

此表中的 Original Operator (**Op**) 列是为了清楚起见而提供；它不并不代表访问控制规则中的字段。

指定多个协议的访问规则

在ASA中，您可以在访问规则中配置源和目标端口，以使用指定多个协议的协议服务对象（例如，TCP 和 UDP）。例如：

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list acp1 extended permit object-group TCPUDP any any
```

但是，在 Firepower 系统中，您只能按如下所示配置访问控制或预过滤器规则：

- 源和目标端口必须指定相同的协议。
- 目标端口可以指定多个协议，但是，源端口必须指定无协议。

包含协议对象组 tcp 和 udp 的访问规则作为不受支持的规则进行迁移。因此，该规则会被禁用，并显示注释 **Object Group Protocol containing both tcp and udp is not supported**。

NAT 规则转换

ASA 的 NAT 和 Firepower 威胁防御 的 NAT 支持等同的功能，如下表中所示：

表 *13*：映射至 *Firepower* 威胁防御 *NAT* 策略的 *ASA NAT* 策略

ASA NAT 策略	Firepower 威胁防御 NAT 策略	定义特征
两次 NAT	手动 NAT	• 在单个规则中指定源和目标地址。 • 直接配置。 • 可以使用网络对象组。 • 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。
网络对象 NAT	自动 NAT	• 指定源地址或目标地址。 • 配置为网络对象的参数。 • 无法使用网络对象组。 • 自动在 NAT 表中排序。

迁移工具将 ASA NAT 配置转换为 Firepower 威胁防御 NAT 配置。但是，该工具无法转换使用不受支持的网络对象的 ASA NAT 配置；在这些情况下，转换会失败。

ASA NAT 规则字段与 Firepower 威胁防御 规则字段的对应关系

该迁移工具按照下表所述将 ASA NAT 规则中的字段转换为 Firepower 威胁防御 NAT 规则中的字段。

注意：

- 列 1（ASA NAT 规则字段）中的字段名称对应于 ASDM 接口中的字段标签。
- 列 2（Firepower 威胁防御规则字段）中的字段名称对应于 Firepower 管理中心 接口中的字段标签。

表 *14*：映射到 *Firepower* 威胁防御 *NAT* 规则字段的 *ASA NAT* 规则字段

ASA NAT 规则字段	Firepower 威胁防御 规则字段
Original Packet - Source Interface	Interface Objects - Source Interface Objects
Original Packet - Source Address	Original Packet - Original Source
Original Packet - Destination Interface	Interface Objects - Destination Interface Objects

ASA NAT 规则字段	Firepower 威胁防御 规则字段
Original Packet - Destination Address	Original Packet - Original Destination - Address Type Original Packet - Original Destination - Network
Original Packet - Service	Original Packet - Original Source Port Original Packet - Original Destination Port
Translated Packet - Source NAT Type	Type
Translated Packet - Source Address	Translated Packet - Translated Source - Address Type Translated Packet - Translated Source - Network
Translated Packet - Destination Address	Translated Packet - Translated Destination
Translated Packet - Service	Translated Packet - Translated Source Port Translated Packet - Translated Destination Port
Use one-to-one address translation	Advanced - Net to Net Mapping
PAT Pool Translated Address	PAT Pool - PAT - Address Type PAT Pool - PAT - Network
Round Robin	PAT Pool - Use Round Robin Allocation
Extend PAT uniqueness to per destination instead of per interface	PAT Pool - Extended PAT Table
Translate TCP and UDP ports into flat range 1024-65535	PAT Pool - Flat Port Range
Include range 1-1023	PAT Pool - Include Reserve Ports
Enable Block Allocation	No equivalent
Use IPv6 for source interface PAT	No equivalent
Use IPv6 for destination interface PAT	Advanced - IPv6
Enable rule	Enable
Translate DNS replies that match this rule	Advanced - Translate DNS replies that match this rule
Disable Proxy ARP on egress interface	Advanced - Do not proxy ARP on Destination Interface
Lookup route table to locate egress interface	No equivalent

ASA NAT 规则字段	Firepower 威胁防御 规则字段
Direction	Advanced - Unidirectional
Description	Description

网络对象和网络对象组转换

网络对象和网络对象组可以识别 IP 地址或主机名。在 ASA 和 Firepower 威胁防御 中，这些对象和组可在访问和 NAT 规则中使用。

在 ASA 中，网络对象可以包含主机、网络 IP 地址、IP 地址范围或完全限定域名 (FQDN)。在 Firepower 系统中，网络对象支持上述相同的值，但 FQDN 除外。

迁移工具会将 ASA 网络对象或组转换一次，无论对象是否在多个访问或 NAT 规则中使用都是如此。

网络对象转换

对于其转换的每个 ASA 网络对象，迁移工具会创建 Firepower 网络对象。

迁移工具会将 ASA 网络对象中的字段转换为 Firepower 网络对象中的字段，如下所示：

表 *15*：映射到 *Firepower* 网络对象字段的 *ASA* 网络对象字段

ASA 网络对象字段	Firepower 网络对象字段
Name	系统生成；参阅 转换的配置的命名约定，第 16 页
Type	Type
IP Version	无等同字段
IP Address	Value
Netmask	Value（包括在 CIDR 表示法中）
Description	Description
Object NAT Address	无等同字段

示例：访问控制列表中的网络对象

如果 ASA 配置文件中存在以下命令：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
access-list sample_acl extended permit ip object obj1 object obj2
access-list sample_acl extended permit ip object obj3 object obj1
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

系统会按如下所示转换这些对象：

名称	域	值（网络）	类型	覆盖
obj1	无	1.2.3.4	主机	错误
obj2	无	1.2.3.7-1.2.3.10	地址范围	错误
obj3	无	10.83.0.0/16	网络	错误

示例：NAT 规则中的网络对象

如果 ASA 配置文件中存在以下命令：

```
nat (gigabitethernet1/1,gigabitethernet1/2) source static obj1 obj1
```

系统将按照其在上述访问规则示例中转换对象 `obj1` 的相同方式来转换此规则中的对象 `obj1`。

网络对象组转换

对于其转换的每个 ASA 网络对象组，迁移工具会创建 Firepower 网络对象组。它还会转换该组中包含的对象（如果尚未转换）。

迁移工具会将 ASA 网络对象组中的字段转换为 Firepower 网络对象组中的字段，如下所示：

表 *16*：映射到 *Firepower* 网络对象组字段的 *ASA* 网络对象组字段

ASA 网络对象组字段	Firepower 网络对象组字段
组名称	名称
说明	说明
组中的成员	值（选定网络）

示例：访问控制列表中的网络对象组

如果 ASA 配置文件中存在以下命令：

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
 network-object object obj3
access-list sample_acl extended permit ip object-group obj_group1 any
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

系统会创建以下网络组：

名称	域	值（网络）	类型	覆盖
obj_group1	无	obj1 obj2 obj3	组	错误

如果尚未转换关联的对象，则系统将如网络对象转换，第 28 页中所述转换这些对象。

示例：NAT 规则中的网络对象组

如果 ASA 配置文件中存在以下命令：

```
nat (interface1,interface2) source static obj_group1 obj_group1
```

系统将按照其在上述访问规则示例中转换 `obj_group1` 的相同方式，转换此规则中的 `obj_group1`。

服务对象和服务组转换

在ASA中，服务对象和服务组会指定协议和端口，并将这些端口指定为源或目标端口。服务对象和组可在访问和 NAT 规则中使用。

在Firepower系统中，端口对象和端口对象组指定协议和端口，但是，仅当您将这些对象添加到访问控制、预过滤器或NAT规则时，系统才会将这些端口指定为源或目标端口。为了将服务对象转换为Firepower系统中具有等同功能的对象，迁移工具会将服务对象转换为端口对象或组，并对相关的访问控制、预过滤器或NAT规则进行特定更改。因此，在转换期间，该迁移工具可能会将单一安全对象及相关访问规则或 NAT 规则扩展到多个端口对象/组及相关访问控制、预过滤器或 NAT 规则。

服务对象转换

迁移工具通过创建一个或多个端口对象以及参考这些端口对象的一个或多个访问控制或预过滤器规则来转换 ASA 服务对象。

迁移工具可以转换以下服务对象类型：

- 协议
- TCP/UDP
- ICMP/ICMPv6

迁移工具会将 ASA 服务对象中的字段转换为 Firepower 端口对象中的字段，如下所示：

表 *17*：映射到 *Firepower* 端口对象字段的 *ASA* 服务对象字段

ASA 服务对象字段	**ASA** 服务对象类型	**Firepower** 端口对象字段
名称	任意	系统生成（请参阅转换的配置的命名约定，第 16 页）
服务类型	TCP/UDP，ICMP/ICMPv6	协议
协议	仅协议	协议
说明	任意	无等同项；放弃内容
目标端口/范围	仅 TCP/UDP	端口
源端口/范围	仅 TCP/UDP	端口
ICMP 类型	仅 ICMP/ICMPv6	类型
ICMP 代码	仅 ICMP/ICMPv6	代码

服务对象中的端口文字值

ASA 服务对象可以指定端口文字值，而不是端口号。例如：

```
object service http
 service tcp destination eq www
```

由于 Firepower 系统不支持这些端口文字值，因此迁移工具会将端口文字值转换为其表示的端口号。该工具会将上述示例转换为以下端口对象：

名称	类型	域	值（协议/端口）	覆盖
http	对象	无	TCP(6)/80	错误

有关端口文字值及关联的端口号的完整列表，请参阅 *CLI* 手册 *1*：思科 *ASA* 系列常规操作 *CLI* 配置指南中的 TCP 和 UDP 端口。

服务对象中的端口参数运算符

ASA 服务对象可在端口参数中使用以下运算符：

表 *18*：服务对象中的端口参数运算符

运算符	描述	示例
lt	小于。	object service testOperator service tcp source lt 100
gt	大于。	object service testOperator service tcp source gt 100
eq	等于。	object service http-proxy service tcp source eq 8080
neq	不等于。	object service testOperator service tcp source neq 200
range	值的范围（包括边界值）。	object service http-proxy service tcp source range 9000 12000

迁移工具按如下所示转换这些运算符：

表 *19*：具有端口参数运算符的服务对象转换为端口对象/组

运算符	转换为	端口对象值示例（协议/端口）
lt	指定小于指定数字的一系列端口号的单个端口对象。	TCP(6)/1-99
gt	指定大于指定数字的一系列端口号的单个端口对象。	TCP(6)/101-65535
eq	指定单个端口号的一个端口对象。	TCP(6)/8080
neq	两个端口对象和一个端口对象组。第一个端口对象指定低于指定端口的范围。第二个端口对象指定高于指定端口的范围。端口对象组包括这两个端口对象。	第一个对象 (testOperator_src_1)： TCP(6)/1-199 第二个对象 (testOperator_src_2)： TCP(6)/201-65535 对象组 (testOperator_src)： testOperator_src_1 testOperator_src_2
range	指定包含的值范围的单个端口对象。	TCP(6)/9000-12000

具有源和目标端口的服务对象

在 ASA 中，单个服务对象可以指定源端口和目标端口。在 Firepower 系统中，端口对象仅指定端口值。在访问控制或预过滤器规则中使用端口对象之前，系统不会将端口指定为源或目标。

为适应此差异，在迁移工具转换指定源和目标的ASA服务对象时，会将单个对象扩展为两个端口对象。它为对象名称附加扩展名以指示其原始目的地，源端口的扩展名为 *_src*，目标端口的扩展名为 *_dst*。

示例

```
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
```

该工具将此服务对象转换为以下端口对象：

名称	类型	域	值（协议/端口）	覆盖
http-proxy_src	对象	无	TCP(6)/9000-12000	错误
http-proxy_dst	对象	无	TCP(6)/8080	错误

示例：协议服务对象转换

ASA 配置：

```
object service protocolObj1
 service snp
 description simple routing
```

转换为：

表 *20*：端口对象

名称	类型	域	值（协议）	覆盖
protocolObj1	对象	无	SNP (109)	错误

示例：TCP/UDP 服务对象转换

ASA 配置：

```
object service servObj1
 service tcp destination eq ssh
```

转换为：

表 *21*：端口对象

名称	类型	域	值（协议/端口）	覆盖
servObj1	对象	无	TCP(6)/22	错误

示例：ICMP/ICMPv6 服务对象转换

ICMP

ASA 配置：

```
object service servObj1
 service icmp alternate-address 0
```

转换为：

表 *22*：端口对象

名称	类型	域	值（协议/类型：代码）	覆盖
servObj1	对象	无	ICMP(1)/备用主机地址：主机的备用地址	错误

ICMPv6

ASA 配置：

```
object service servObj1
 service icmp6 unreachable 0
```

转换为：

表 *23*：端口对象

名称	类型	域	值（协议/类型：代码）	覆盖
servObj1	对象	无	IPV6-ICMP (58)/无法访问目标：无法路由到目标	错误

服务组转换

迁移工具通过创建端口对象组并将这些端口对象组与相关的访问控制或预过滤器规则相关联来转换 ASA 服务组。

迁移工具可以转换以下服务组类型：

- 协议
- TCP/UDP
- ICMP/ICMPv6

迁移工具会将 ASA 服务对象中的字段转换为 Firepower 端口对象中的字段，如下所示：

表 *24*：映射到 *Firepower* 端口对象字段的 *ASA* 服务组字段

ASA 服务组字段	端口对象组字段
名称	系统生成（请参阅转换的配置的命名约定，第 16 页）
说明	说明
组中的成员	选定端口

嵌套服务组转换

ASA 支持嵌套服务组（即包含其他服务组的服务组）。Firepower 系统不支持嵌套端口对象组；但您可以通过将多个组与单个访问控制或预过滤器规则相关联，实现等同功能。转换嵌套服务组时，该迁移工具会“平化”组结构，将最内部的服务对象和组转换为端口对象和端口对象组，并将这些转换的组与访问控制或预过滤器规则相关联。

您最多可以将 50 个端口对象与单个访问控制或预过滤器规则相关联。如果新端口对象的数量超过 50，则该工具会创建重复的访问控制或预过滤器规则，直至其将所有新端口对象与规则相关联。

包含用作源和目标服务的嵌套服务对象的 Firepower 系统规则不受支持。

示例

```
object-group service http-8081 tcp
 port-object eq 80
 port-object eq 81

object-group service http-proxy tcp
 port-object eq 8080

object-group service all-http tcp
 group-object http-8081
 group-object http-proxy
```

```
access-list FMC_inside extended permit tcp host 33.33.33.33 object-group all-http host
33.33.33.33 object-group all-http
```

在以上示例中，服务对象 *http 8081* 和 *http-proxy* 嵌套在 *all-http* 服务组内。

在这种情况下，将忽略有关端口对象的规则。系统会导入对象，但禁用相关的访问控制或预过滤器规则，并将以下注释添加到规则：**Nested service groups at both Source and Destination are not supported**。

有关该工具用于转换的服务对象、服务组以及系统在转换期间可能创建的任何重复规则的命名约定的说明，请参阅 转换的配置的命名约定 ，第 16 页

示例

ASA 配置：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

转换为：

表 *25*：端口对象组

名称	类型	域	值（协议/端口）	覆盖
legServGroup1_1	对象	无	TCP(6)/78	错误
legServGroup1_2	对象	无	TCP(6)/79	错误
legServGroup2_1	对象	无	TCP(6)/80	错误
legServGroup2_2	对象	无	TCP(6)/81	错误
legServGroup1	组	无	legServGroup1_1 legServGroup1_2	错误
legServGroup2	组	无	legServGroup2_1 legServGroup2_2	错误

表 *26*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	允许等同项	真

示例：协议服务组转换

ASA 配置：

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

转换为：

表 *27*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
TCPUDP_1	对象	无	TCP(6)	错误
TCPUDP_2	对象	无	UDP(17)	错误
TCPUDP	组	无	TCPUDP_1 TCPUDP_2	错误

示例：TCP/UDP 服务组转换

在组创建过程中创建的对象

在 ASA 中，您可以在创建服务组时即时创建对象。这些对象分类为服务对象，但是 ASA 配置文件中的条目使用 `port-object`，而不是 `object service`。由于这些对象不是独立创建的，因此迁移工具使用的命名约定稍微不同于对独立于组创建所创建的对象使用的命名约定。

ASA 配置：

```
object-group service servGrp5 tcp-udp
 port-object eq 50
 port-object eq 55
```

转换为：

表 *28*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
servGrp5_1	对象	无	TCP(6)/50	错误
servGrp5_2	对象	无	TCP(6)/55	错误
servGrp5	组	无	servGrp5_1 servGrp5_2	错误

独立于组创建的对象

ASA 配置：

```
object service servObj1
 service tcp destination eq ssh
object service servObj2
 service udp destination eq 22
object service servObj3
 service tcp destination eq telnet
object-group service servGrp1
 service-object object servObj1
 service-object object servObj2
 service-object object servObj3
```

转换为：

表 *29*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
servObj1	对象	无	TCP(6)/22	错误
servObj2	对象	无	UDP(17)/22	错误
servObj3	对象	无	TCP(6)/23	错误
servGrp1	Group	无	servObj1 servObj2 servObj3	错误

示例：ICMP/ICMPv6 服务组转换

ICMP

ASA 配置：

```
object-group icmp-type servGrp4
 icmp-object echo-reply
```

转换为：

表 *30*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
servGrp4_1	对象	无	ICMP(1)/回应答复	错误
servGrp4	组	无	servGrp4_1	错误

ICMPv6

ASA 配置：

```
object-group service servObjGrp3
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
```

转换为：

表 *31*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
servObjGrp3_1	对象	无	IPV6-ICMP(58)/2	错误
servObjGrp3_2	对象	无	IPV6-ICMP(58)/4	错误
servObjGrp3	Group	无	servObjGrp3_1 servObjGrp3_2	错误

访问组转换

在 ASA 中，要应用 ACL，请在 CLI 中输入 `access-group` 命令，或在 ASDM 访问规则编辑器中选择 **Apply**。这两项操作都会在 ASA 配置文件中生成一个 `access-group` 条目（参见以下示例）。

`access-group` 命令可指定系统应用 ACL 的接口，以及系统将 ACL 应用到该接口的入站（入口）还是出站（出口）流量。

在 Firepower 系统中，要配置等同功能，您需要：

- 创建一个安全区，将该安全区与某个接口相关联，然后将安全区添加至访问控制规则，以作为源区域条件（用于入站流量）或目标区域条件（用于出站流量）。
- 创建一个接口组，将该接口组与某个接口相关联，然后将接口组作为源接口组条件（用于入站流量）或目标接口组条件（用于出站流量）添加到预过滤器规则。

当转换 access-group 命令时，迁移工具会捕获入口和出口信息，具体方法是：创建安全区或接口组，然后在相关访问控制或预过滤器规则中添加这些安全区和接口组作为条件。但是，迁移工具会以安全区或接口组的名义保留接口信息，却不会转换任何相关的接口或设备配置（您必须在导入转换的策略后手动添加这些相关配置）。在导入转换的策略后，您必须将策略与设备以及将安全区或接口组与接口手动相关联。

转换 ACL 时，系统会在将规则应用到特定接口之后定位全局应用的规则。

特殊情况

如果 ASA 配置将单个 ACL 应用到入口和出口接口，则该工具会将 ACL 转换为两组访问控制规则或预过滤器规则：

- 一组入口规则（已启用）
- 一组出口规则（已禁用）

如果 ASA 配置将单个 ACL 全局应用且应用到特定接口，则该工具会将 ACL 转换为两组访问控制规则或预过滤器规则：

- 与特定接口关联的一组规则（已启用）
- 源和目标区域设置为 Any 的一组规则（已启用）

示例：全局应用的 ACL

ASA 配置：

```
access-list global_access extended permit ip any any
access-group global_access global
```

迁移工具将此配置转换为：

表 *32*：访问控制或预过滤器规则

名称	源区域/接口组	目标区域/接口组	源网络	目标网络	源端口	目标端口	操作	启用
global_access#1	任何环境	任何环境	任何环境	任何环境	任何环境	任何环境	允许等同项	真

示例：ACL 应用于特定接口

ASA 配置：

```
access-list acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

在本例中，access-group 命令将名为 acp1 的 ACL 应用到名为 outside 的接口上的入站流量。

迁移工具将此配置转换为：

表 *33*：安全区/接口组

名称	接口类型	域	选定接口
acp1_outside_in_zone	• 路由（如果 ASA 设备在路由模式下运行） • 切换（如果 ASA 设备在透明模式下运行）	无	任意

表 *34*：访问控制或预过滤器规则

名称	源区域/接口组	目标区域/接口组	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	acp1_outside_in_zone	任何环境	任何环境	209.165.201.3	任意	TCP(6)/80	允许等同项	真

附 录 B

转换示例

本部分包含 ASA 配置，以及迁移工具将其转换到的 Firepower 威胁防御 规则和对象的示例。

示例

用于指定个别网络的访问规则

ASA 配置：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

转换为：

表 *35*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	允许等同项	真

具有网络对象组的访问规则

ASA 配置：

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

转换为：

表 *36*：网络对象组

名称	域	值（网络）	类型	替代
主机 1	无	obj1 obj2	组	错误
主机 2	无	obj3 obj4	组	错误

表 *37*：用于使用网络对象组的访问规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	主机 1	主机 2	任何环境	任何环境	允许等同项	真

用于指定个别网络和端口的访问规则

ASA 访问规则：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0 eq
80
access-group acp1 global
```

转换为：

表 *38*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/32	5.6.7.0/32	TCP(6)/90	TCP(6)/80	允许等同项	真

具有服务对象的访问规则

ASA 配置：

```
object service servObj1
 service tcp destination eq 78
access-list acp1 extended permit object servObj1 any any
access-group acp1 in interface outside
```

转换为：

表 *39*：端口对象

名称	类型	域	值（协议/端口）	覆盖
servObj1	对象	无	TCP(6)/78	错误

表 *40*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	任何环境	servObj1	允许等同项	真

有服务对象组的访问规则

ASA 配置：

```
object-group service legServGroup tcp
 port-object eq 78
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legServGroup
access-group acp1 global
```

转换为：

表 *41*：端口对象

名称	类型	域	值（协议/端口）	覆盖
legServGroup	对象	无	TCP(6)/78	错误

表 *42*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup	允许等同项	真

有嵌套服务对象组的访问规则

ASA 配置：

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list  acp1 extended permit tcp  3.4.5.0  255.255.255.0  5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acp1 global
```

转换为：

表 *43*：端口对象和组

名称	类型	域	值（协议/端口）	覆盖
legServGroup1_1	对象	无	TCP(6)/78	错误

名称	类型	域	值（协议/端口）	覆盖
legServGroup1_2	对象	无	TCP(6)/79	错误
legServGroup2_1	对象	无	TCP(6)/80	错误
legServGroup2_2	对象	无	TCP(6)/81	错误
legServGroup1	组	无	legServGroup1_1 legServGroup1_2	错误
legServGroup2	组	无	legServGroup2_1 legServGroup2_2	错误

请注意，已转换的配置不包含嵌套组 legacyServiceNestedGrp 的等同项，因为该组已简化。

表 *44*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/24	5.6.7.0/24	TCP(6)	legServGroup1 legServGroup2	允许等同项	真

有嵌套扩展服务对象组的访问规则

ASA 配置：

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
 service-object tcp destination eq 443
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

转换为：

表 *45*：端口对象

名称	类型	域	值（协议/端口）	覆盖
http_src	对象	无	TCP(6)/9000-12000	错误
http_dst	对象	无	TCP(6)/80	错误

名称	类型	域	值（协议/端口）	覆盖
http-proxy_src	对象	无	TCP(6)/9000-12000	错误
http-proxy_dst	对象	无	TCP(6)/8080	错误
all-httpz-dst	组	无	TCP(6)/443	错误

请注意，已转换的配置不包含嵌套组 all-httpz 的等同项，因为该组已简化。

表 *46*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1_1	任何环境	任何环境	任何环境	任何环境	http_src	http_dst	允许等同项	真
acp1#1_2	任何环境	任何环境	任何环境	任何环境	http-proxy_src	http-proxy_dst	允许等同项	真
acp1#1_3	任何环境	任何环境	任何环境	任何环境	任何环境	all-httpz-dst	允许等同项	真

有使用“gt”和“neq”运算符的服务对象的访问规则

ASA 配置：

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acp1 extended permit object testOperator any any
```

转换为：

表 *47*：端口对象

名称	类型	域	值（协议/端口）	覆盖
testOperator_src	对象	无	TCP(6)/101-65535	错误
testOperator_dst_1	对象	无	TCP(6)/1-199	错误
testOperator_dst_2	对象	无	TCP(6)/201-65535	错误
testOperator_dst	组	无	testOperator_dst_1，testOperator_dst_2	错误

表 *48*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	testOperator_src	testOperator_dst	允许等同项	真

有使用“**lt**”和“**gt**”运算符的安全对象的访问规则

ASA 配置：

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acp1 extended permit object testOperator any any
```

转换为：

表 *49*：端口对象

名称	类型	域	值（协议/端口）	覆盖
testOperator_src	对象	无	TCP(6)/101-65535	错误
testOperator_dst	对象	无	TCP(6)/1-199	错误

表 *50*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	testOperator_src	testOperator_dst	允许等同项	真

有使用“**eq**”运算符和端口文字值的 **TCP** 服务对象的访问规则

ASA 配置：

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acp1 extended permit object testOperator any any
```

转换为：

表 *51*：端口对象

名称	类型	域	值（协议/端口）	覆盖
svcObj1_src	对象	无	TCP(6)/21	错误
svcObj1_dst	对象	无	TCP(6)/22	错误

表 *52*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	svcObj1_src	svcObj1_dst	允许等同项	真

有 ICMP 服务对象的访问规则

ASA 配置：

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acp1 extended permit object icmpObj any any
```

转换为：

表 *53*：端口对象

名称	类型	域	值（协议/端口）	覆盖
icmpObj	对象	无	ICMP(1)/回应答复	错误

表 *54*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	任何环境	icmpObj	允许等同项	真

有协议服务对象的访问规则

ASA 配置：

```
object-group protocol testProtocol
 protocol-object tcp
access-list acp1 extended permit object testProtocol any any
```

转换为：

表 *55*：端口对象

名称	类型	域	值（协议/端口）	覆盖
testProtocol	对象	无	TCP(6)	错误

表 *56*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	任何环境	testProtocol	允许等同项	真

有扩展服务对象的访问规则（仅限源）

ASA 配置：

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

转换为：

表 *57*：端口对象

名称	类型	域	值（协议/端口）	覆盖
serviceObj_src_1	对象	无	TCP(6)/300	错误
serviceObj_src_2	对象	无	TCP(6)/800	错误
serviceObj	组	无	serviceObj_src_1 serviceObj_src_2	错误

表 *58*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	任何环境	serviceObj	允许等同项	真

有扩展服务对象的访问规则（源和目标）

ASA 配置：

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

转换为：

表 *59*：端口对象

名称	类型	域	值（协议/端口）	覆盖
serviceObj_src	对象	无	TCP(6)/300	错误
serviceObj_dst	对象	无	TCP(6)/400	错误

表 *60*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	serviceObj_src	serviceObj_dst	允许等同项	真

在源端口中有端口参数运算符“**neq**”的访问规则

ASA 配置：

```
access-list acp1 extended permit tcp any neq 300
```

转换为：

表 *61*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	任何环境	任何环境	1-299，301-65535	任意	允许等同项	真

在源和目标端口中有端口参数运算符“**neq**”的访问规则

ASA 配置：

```
access-list acp1 extended permit tcp any neq 300 any neq 400
```

转换为：

表 *62*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1_1	任何环境	任何环境	任何环境	任何环境	1-299	1-399	允许等同项	真
acp1#1_2	任何环境	任何环境	任何环境	任何环境	301-65535	1-399	允许等同项	真
acp1#1_3	任何环境	任何环境	任何环境	任何环境	1-299	401-65535	允许等同项	真
acp1#1_4	任何环境	任何环境	任何环境	任何环境	301-65535	401-65535	允许等同项	真

非互动访问规则

ASA 配置：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acp1 global
```

转换为：

表 *63*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	任何环境	任何环境	3.4.5.0/24	5.6.7.0/24	TCP(6)	任意	允许等同项	错误

应用于入站流量的访问控制列表

ASA 配置：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 in inside
```

转换为：

表 *64*：安全区/接口组

名称	接口类型	域	选定接口
acp1_inside_in_zone	• 路由（如果 ASA 设备在路由模式下运行） • 切换（如果 ASA 设备在透明模式下运行）	无	任意

表 *65*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	acp1_inside_in_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	允许等同项	真

应用于出站流量的访问控制列表

ASA 配置：

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

转换为：

表 *66*：安全区/接口组

名称	接口类型	域	选定接口
acp1_outside_out_zone	• 路由（如果 ASA 设备在路由模式下运行） • 切换（如果 ASA 设备在透明模式下运行）	无	任意

表 *67*：访问控制或预过滤器规则

名称	源区域	目标区域	源网络	目标网络	源端口	目标端口	操作	启用
acp1#1	acp1_outside_out_zone	任意	3.4.5.0/24	任意	TCP(6)/90	TCP(6)/80	允许等同项	真