使用 Cisco Secure Firewall Management Center 在移动设备上配置基于应用的远程访问 VPN (Per App VPN)

首次发布日期: 2023 年 7 月 31 日

使用 Cisco Secure Firewall Management Center 在移动设备上配置基于应用的远程访问 VPN (Per App VPN)

关于 Per App VPN

当远程用户使用安全客户端从移动设备建立VPN连接时，所有流量（包括来自个人应用的流量）都将通过 VPN 传输。

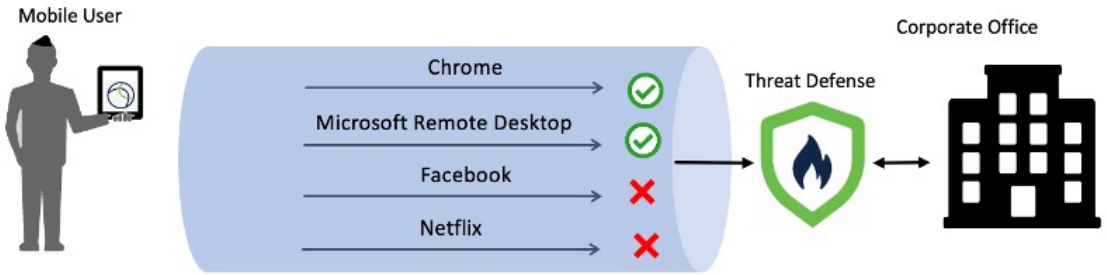
对于在 Android 或 iOS 上运行的移动设备，可以限制穿越 VPN 隧道的应用。这种基于应用的远程访问 VPN 称为 Per App VPN。

要使用 Per App VPN，必须执行以下操作：

1. 安装和配置第三方移动设备管理器 (MDM) 服务器。
2. 在 MDM 服务器中定义可通过 VPN 隧道使用的已批准应用的列表。
3. 将 Per App 配置从 MDM 服务器部署到移动设备。
4. 在托管前端威胁防御上配置 Per App VPN。

当MDM管理的移动设备使用安全客户端连接到VPN时，客户端会在通过隧道传输流量之前验证应用。威胁防御上配置的 Per App 策略将执行此验证。

下图显示了使用威胁防御的 Per App VPN 示例：



优势

- 限制企业网络上的 VPN 流量并释放 VPN 前端的资源。您可以防止：
  - 通过 VPN 访问 Netflix、Facebook 和 YouTube 等应用。
  - 受信任的云应用，例如 Outlook 和基于 VPN 的 Webex。
- 优化流量。
- 让延迟最小化。
- 保护企业 VPN 隧道免受移动设备上未经批准的恶意应用的影响。

本指南适用对象

本用例适用于使用管理中心为使用远程访问 VPN 连接到组织网络的远程员工配置 Per App VPN 的网络管理员。

在版本 6.4 至 6.7 中，您可以使用 FlexConfig 在 FTD 上启用 Per App VPN。有关更多信息，请参阅在移动设备上配置基于应用的（Per App VPN）远程访问 VPN。在 7.0 及更高版本中，您可以使用管理中心 UI 在威胁防御上启用 Per App VPN。

系统要求

下表列出了该功能支持的平台。

Product	Version	本文档使用的版本
Cisco Secure Firewall Threat Defense（之前的 Firepower 威胁防御/FTD）	7.0 及更高版本	7.3
Cisco Secure Firewall Management Center（之前的 Firepower 管理中心/FMC）	7.0 及更高版本	7.3
Cisco Secure Client（之前的 AnyConnect）	4.0 及更高版本	5.0
Android 设备	Android 5.0 及更高版本	-
Apple iOS 设备	Apple iOS 8.3 及更高版本and later	-

配置每个应用 VPN 隧道的前提条件

确保：

- 在管理中心配置远程接入 VPN 策略。

- 设置 MDM 服务器并将每个移动设备注册到 MDM 服务器。

  有关详细信息，请参阅 MDM 文档。

  建议您在 MDM 服务器中配置可以遍历 VPN 隧道的应用。这样可以简化前端配置。

- 从 Cisco 软件下载中心将 Cisco AnyConnect Enterprise 应用选择器下载并安装到本地主机。

  您需要此工具来定义 Per App VPN 策略。

许可证：

- 您需要以下安全客户端许可证之一：

  Cisco Secure Client Premier 或 Cisco Secure Client Advantage。

- 您的管理中心 Essentials 许可证必须允许导出控制功能。

  依次选择**系统 (System)** > **许可证 (Licenses)** > **智能许可证 (Smart Licenses)** 以在管理中心验证此功能。

如何使用管理中心配置 Per App VPN

步骤	相应操作	更多信息
1	确保您已满足前提条件。	配置每个应用 VPN 隧道的前提条件，第 2 页
2	确定隧道中应允许哪些应用。	-
3	确定移动应用的应用 ID。	确定移动应用的应用 ID，第 3 页
4	为 Android 和 Apple iOS 设备定义 Per App VPN 策略	为 Android 和 Apple iOS 设备定义 Per App VPN 策略，第 5 页
5	在管理中心将 Per App VPN 策略分配给远程接入 VPN	在管理中心将 Per App VPN 策略分配给远程接入 VPN，第 8 页
6	在威胁防御上部署配置。	在管理中心菜单栏中，单击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

确定移动应用的应用 ID

如果您决定要在前端配置允许的应用列表，则必须确定每种类型的终端上每个应用的应用 ID。

注释 建议您在 MDM 服务器中配置 Per App 策略。这样可以简化前端配置。

应用 ID（或 iOS 中的捆绑包 ID）是反向 DNS 名称。您可以使用星号作为通配符。例如，*.* 表示所有应用，com.cisco.* 表示所有 Cisco 应用。

要确定应用 ID，请执行以下操作：

- **Android**
  1. 在 Web 浏览器中，转至 Google Play (https://play.google.com/store/)。
  2. 点击**应用 (Apps)** 选项卡。
  3. 点击要在 VPN 隧道中允许的应用。

     应用 ID 是 URL 的一部分。
  4. 复制“id=”参数后面的字符串。

     对于 Microsoft 远程桌面，URL 为：

     https://play.google.com/store/apps/details?id=com.microsoft.rdc.androidx，应用 ID 为 com.microsoft.rdc.androidx。

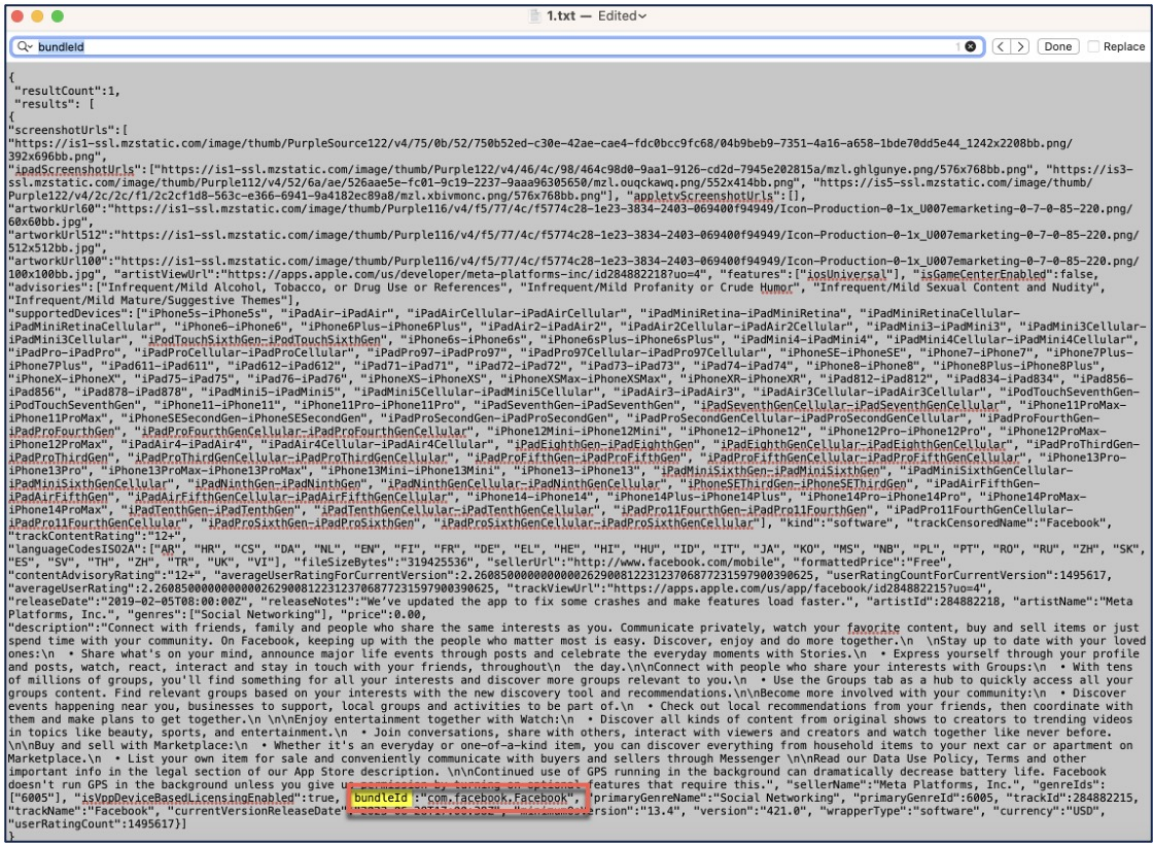
  对于 Google Play 上没有的应用，可下载软件包名称查看器来提取应用 ID。
- **iOS**
  1. 在 Web 浏览器中，转至 Apple App Store (https://www.apple.com/in/app-store/)。
  2. 在搜索结果中，搜索应用。

     应用 ID 是 URL 的一部分。
  3. 复制“id”字符串后面的数字。

     对于 Facebook，URL 为：

     https://apps.apple.com/in/app/facebook/id284882215，应用 ID 为 284882215。
  4. 打开一个新的浏览器窗口，然后将该数字添加到以下 URL 的末尾：https://itunes.apple.com/lookup?id=

     对于 Facebook，URL 为 https://itunes.apple.com/lookup?id=284882215。
  5. 下载文本文件，通常命名为 1.txt。
  6. 在文本编辑器中打开文件，然后搜索 bundleId。对于 Facebook，“bundleId”为“com.facebook.Facebook”。以此捆绑包 ID 作为应用 ID。



有了应用 ID 列表后，您就可以按照下面的步骤为移动设备定义策略了。

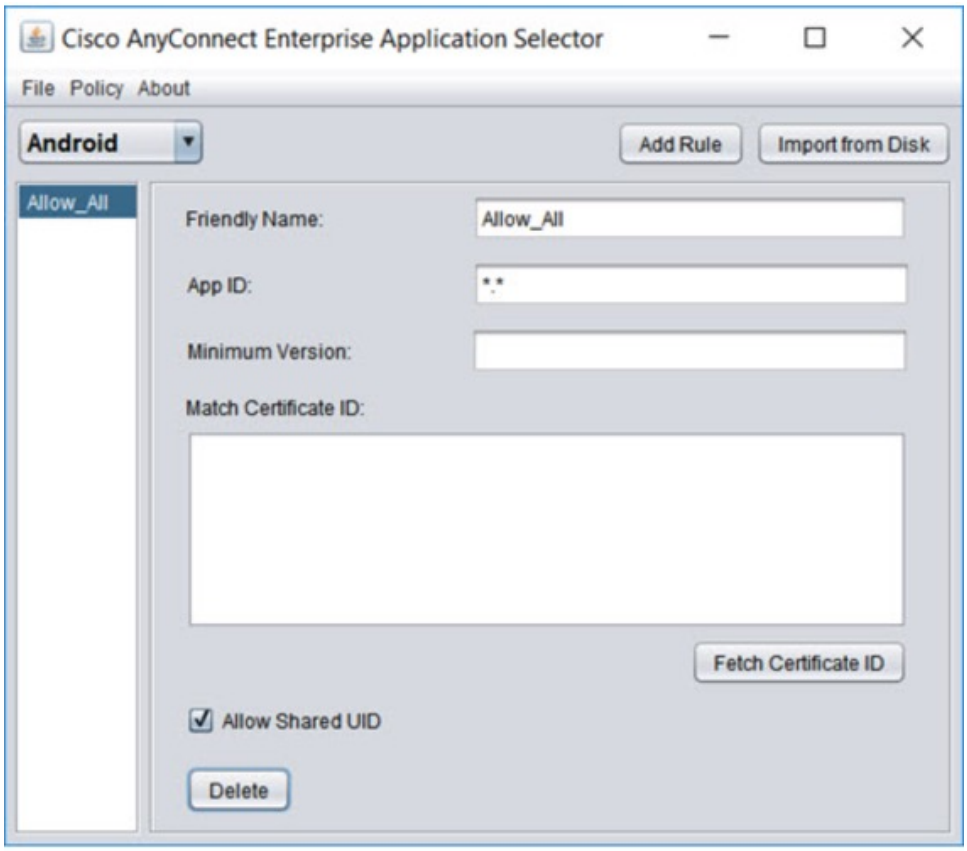
为 Android 和 Apple iOS 设备定义 Per App VPN 策略

使用 Cisco AnyConnect 企业应用选择器定义 Per App VPN 策略。

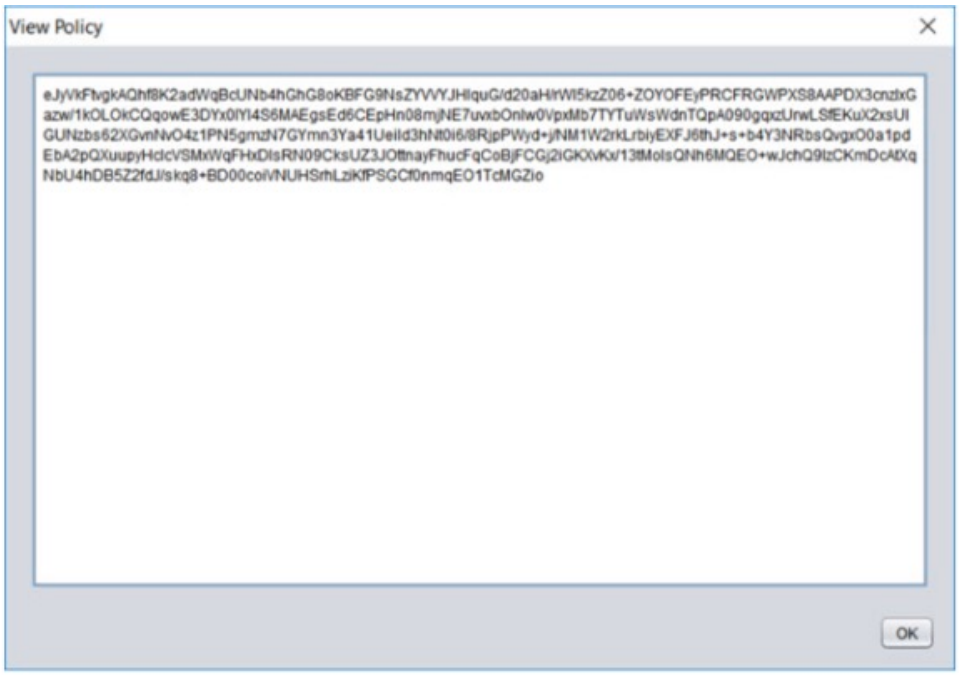
我们建议您创建一个简单的“全部允许”策略，并在 MDM 中定义允许的应用。但是，您可以从头端指定要允许和控制列表的应用列表。如果要包括特定应用，请使用唯一名称和应用的应用 ID 为每个应用创建单独的规则。

要使用 AnyConnect 企业应用选择器创建支持 Android 和 iOS 平台的**全部允许**策略（通配符策略），请执行以下操作：

1. 从下拉列表中选择 **Android** 或 **iOS** 作为平台类型。
2. 配置以下选项：
   - **友好名称**-输入策略的名称。例如，Allow_All。
   - **App ID**-输入 *.* 以匹配所有可能的应用。
   - 其他选项保持不变。

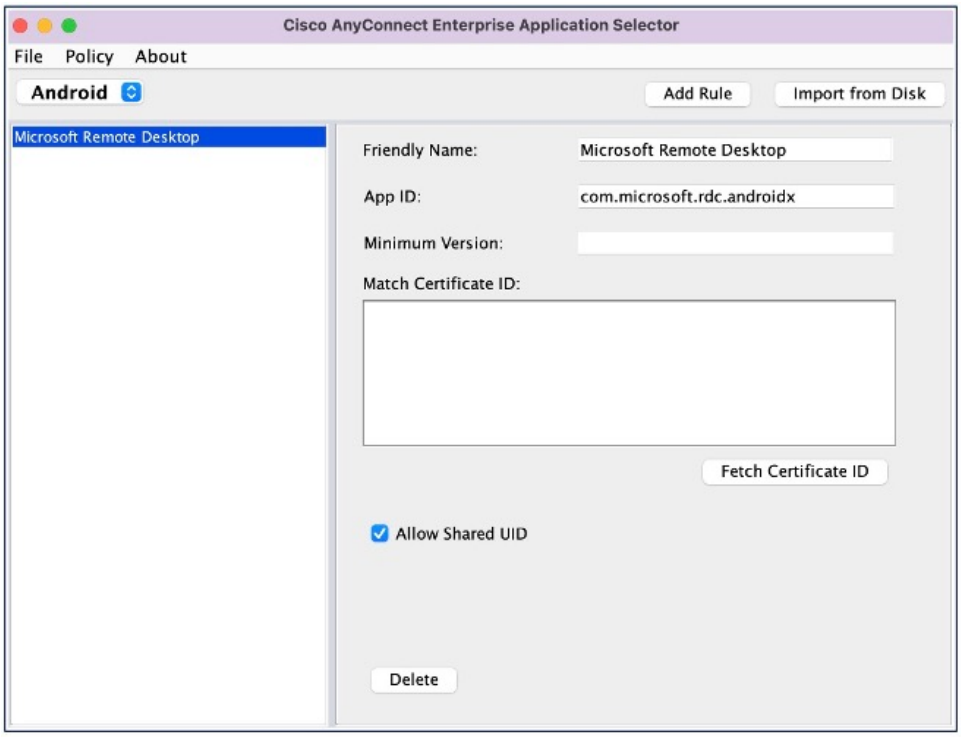


3. 依次选择**策略 (Policy)** > **查看策略 (View Policy)** 以获取策略的 base64 编码字符串。此字符串包含允许威胁防御查看策略的加密 XML 文件。复制此值。下一步在威胁防御上配置 Per App VPN 时需要此字符串。



要使用 AnyConnect Enterprise 应用选择器为 Microsoft 远程桌面应用创建策略，请执行以下操作：

1. 从下拉列表中选择 **Android** 作为平台类型。
2. 配置以下选项：
   - **友好名称 (Friendly Name)** - 输入策略的名称。
   - **App ID (应用 ID)** - 对于 Android，请输入 com.microsoft.rdc.androidx。
   - 其他选项保持不变。



3. 依次选择**策略 (Policy)** > **查看策略 (View Policy)** 以获取策略的 base64 编码字符串。

在管理中心将 Per App VPN 策略分配给远程接入 VPN

过程

步骤 1 选择**设备** > **远程访问**。

步骤 2 选择远程访问 VPN 策略，然后点击 **编辑**。

步骤 3 选择一个连接配置文件，然后点击**编辑 (Edit)**。

步骤 4 点击 **编辑组策略**。

步骤 5 点击**安全客户端 (Secure Client)** 选项卡。

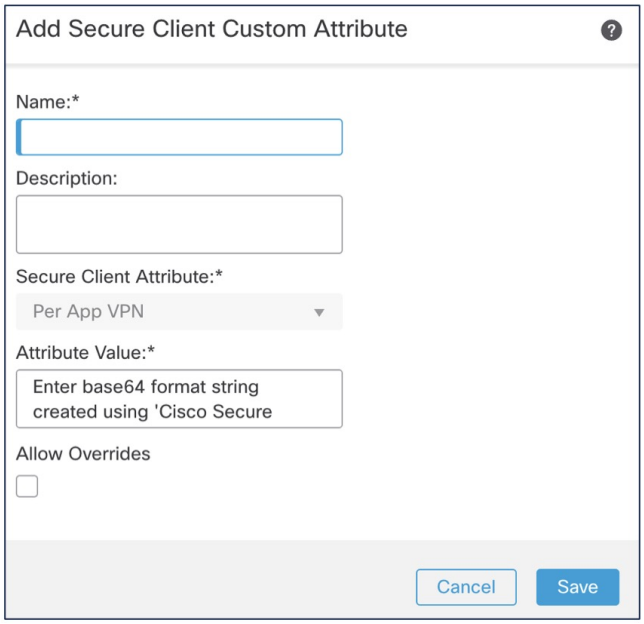
步骤 6 点击 **自定义属性**，然后点击 **+**。

步骤 7 从**安全客户端属性 (Secure Client Attribute)** 下拉列表中选择 Per App VPN。

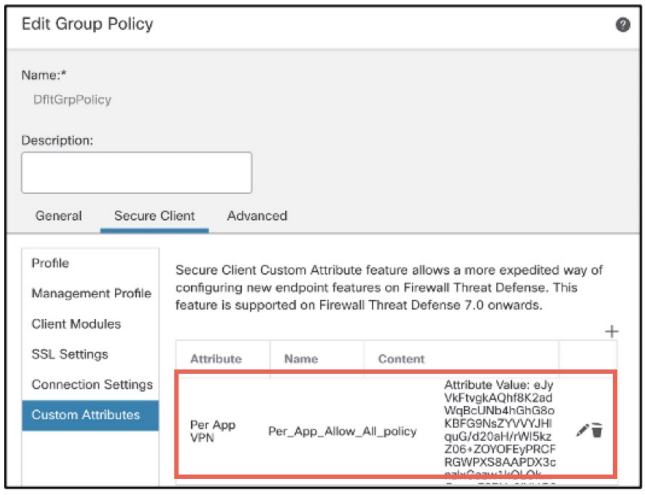
步骤 8 从 **自定义属性对象** 下拉列表中选择对象，或点击 **+** 添加对象。

在为 Per App VPN 添加新的自定义属性对象时：

1. 输入名称和说明。
2. 在**属性值 (Attribute Value)** 字段中，指定来自思科 AnyConnect 企业应用选择器的 base64 编码策略字符串。



步骤 9　点击保存 (Save) 并点击添加 (Add)。



步骤 10　单击保存。

下一步做什么

1. 在威胁防御上部署配置。
2. 使用安全客户端建立与威胁防御的 VPN 连接。
3. 验证 Per App VPN 配置。

验证 Per App VPN 配置

在威胁防御上

在威胁防御系统上使用以下命令验证 Per App 配置：

命令	说明
show run webvpn	查看安全客户端配置的详细信息。
show run group-policy <group_policy_name>	查看安全客户端的远程接入 VPN 组策略的详细信息。
show vpn-sessiondb anyconnect	查看活动安全客户端 VPN 会话的详细信息。
show run anyconnect-custom-data	查看 Per App 配置的详细信息。

sh run webvpn 的输出示例如下：

```
firepower# sh run webvpn
 webvpn
 enable inside
 anyconnect-custom-attr perapp description Per-App Allow
 http-headers
 hsts-server
 enable
 max-age 31536000
 include-sub-domains
 no preload
 hsts-client
 enable
 x-content-type-options
 x-xss-protection
 content-security-policy
 anyconnect image disk0:/csm/cisco-secure-client-win-5.0.03076-webdeploy-k9 1 regex "Windows"

 anyconnect enable
 tunnel-group-list enable
 cache
 no disable
 error-recovery disable
```

sh run anyconnect-custom-data 的输出示例如下：

```
firepower# sh run anyconnect-custom-data
anyconnect-custom-data perapp PerAppPolicy
eJw9kFtvgkAQhf8K2ae2GC+rqPFNgYjgBcUL2PRhCyuuZVlkuRv/
```

sh running-config group-policy 的输出示例如下：

```
firepower# sh running-config group-policy
 group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev2 ssl-client
 user-authentication-idle-timeout none
 anyconnect-custom perapp value PerAppPolicy
 webvpn
 anyconnect keep-installer none
```

```
anyconnect modules value none
anyconnect ask none default anyconnect
http-comp none
activex-relay disable
file-entry disable
file-browsing disable
url-entry disable
deny-message none
```

在终端上

在终端与威胁防御建立 VPN 连接后，点击安全客户端的**统计信息 (Statistics)** 图标：

- **隧道模式** 将是“应用隧道”，而不是“隧道所有流量”。
- **隧道应用** 将列出您在 MDM 中启用隧道的应用。

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)

© 2023 Cisco Systems, Inc. 保留所有权利。

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。