RV130和RV130W VPN路由器上的互联网密钥交换(IKE)策略设置

目标

Internet密钥交换(IKE)是在两个网络之间建立安全通信的协议。使用IKE时，数据包使用双方使用的密钥进行加密和锁定以及解锁。

在配置VPN策略之前，需要创建Internet密钥交换策略。有关详细信息，请参阅*RV130和RV130W上的VPN策略配置*。

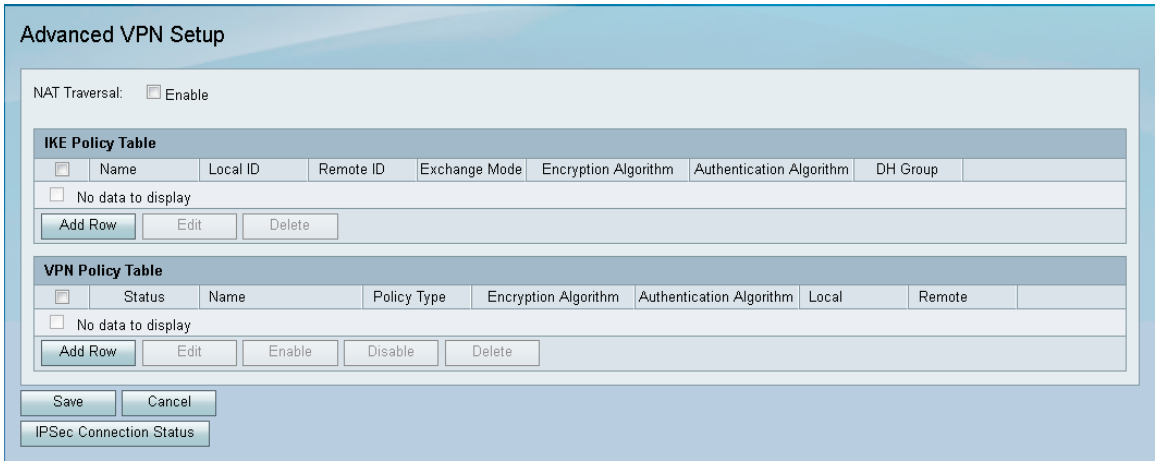
本文档的目的是向您展示如何向RV130和RV130W VPN路由器添加IKE配置文件。

适用设备

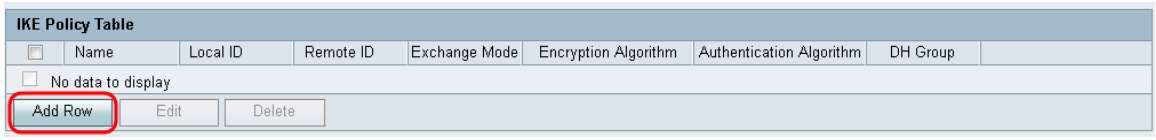
·RV130
· RV130W

程序步骤

步骤1.使用路由器配置实用程序从左侧菜单中选择**VPN >站点到站点IPSec VPN > Advanced VPN Setup**。系统将显示*Advanced VPN Setup*页面：

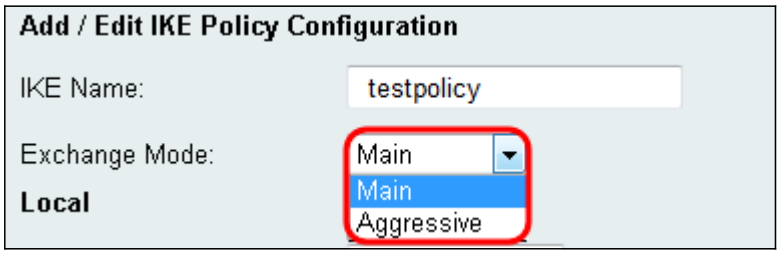


步骤2.在IKE策略表下，单击**Add Row**。系统将显示一个新窗口：



步骤3.在*IKE Name*（IKE名称）字段中输入*IKE策略的*名称。

步骤4.从*Exchange Mode*下拉菜单中，选择使用密钥交换建立安全通信的模式。

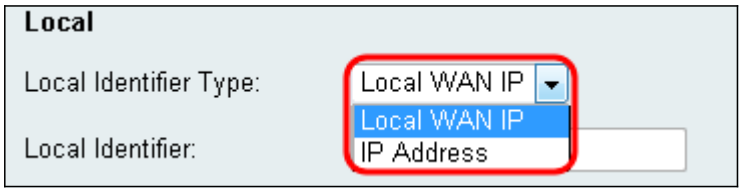


可用选项定义如下：

·Main — 保护对等体的身份以提高安全性。

·主动 — 不保护对等体身份，但提供更快的连接。

第5步：从*Local Identifier Type*下拉菜单中，选择配置文件具有的身份类型。

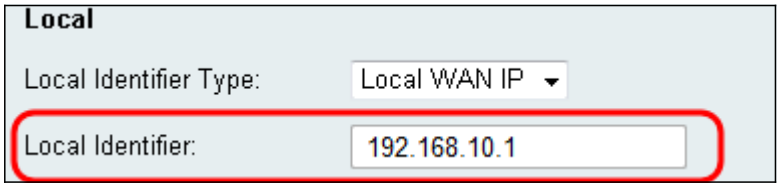


可用选项定义如下：

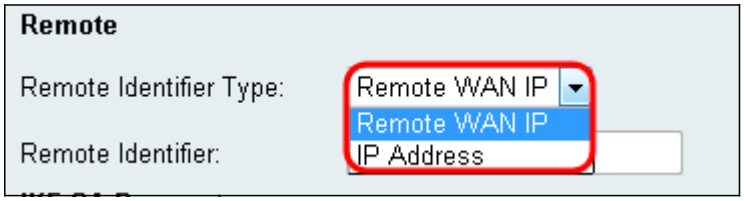
·本地WAN(Internet)IP — 通过Internet连接。

·IP地址 — 由句点分隔的唯一数字字符串，用于标识使用Internet协议的每台计算机，以便通过网络通信。

第6步。（可选）如果在第5步中的下拉列表中选择**IP Address**，请在*Local Identifier*字段中输入本地IP地址。



步骤7.从*Remote Identifier Type*下拉菜单中，选择配置文件具有的身份类型。

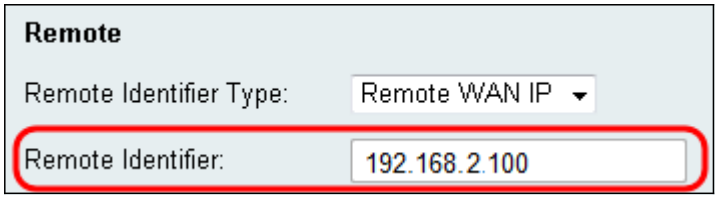


可用选项定义如下：

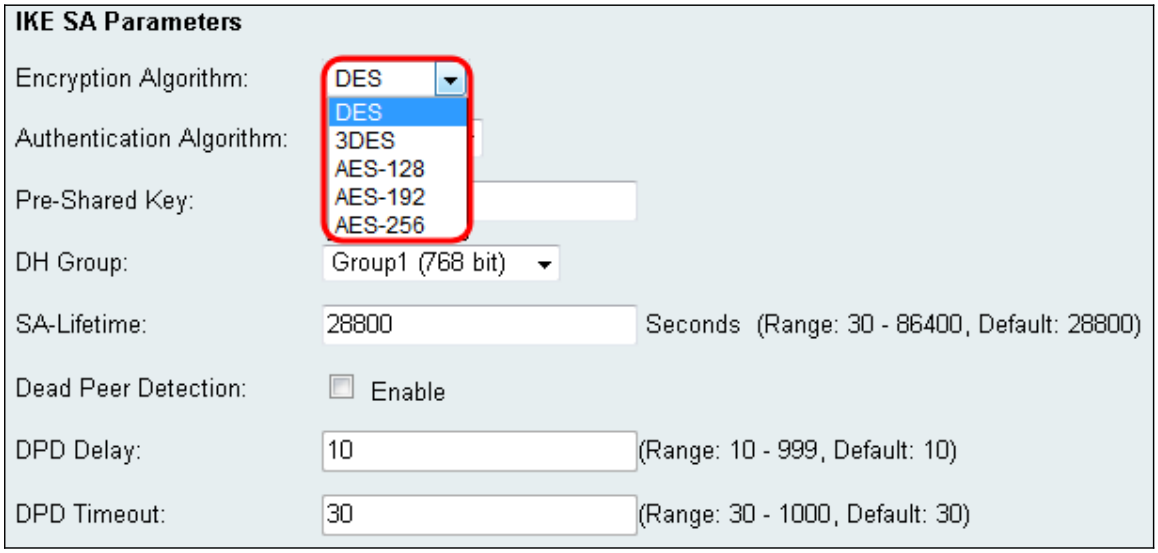
·本地WAN(Internet)IP — 通过Internet连接。

·IP地址 — 由句点分隔的唯一数字字符串，用于标识使用Internet协议的每台计算机，以便通过网络通信。

第8步。（可选）如果在第7步中的下拉列表中选择**IP Address**，请在*Remote Identifier*字段中输入远程IP地址。



步骤9.从*Encryption Algorithm*下拉菜单中选择加密通信的算法。**默认选择AES**-128。



可用选项按从低到高的安全性列出：

•DES – 数据加密标准。

·3DES — 三重数据加密标准。

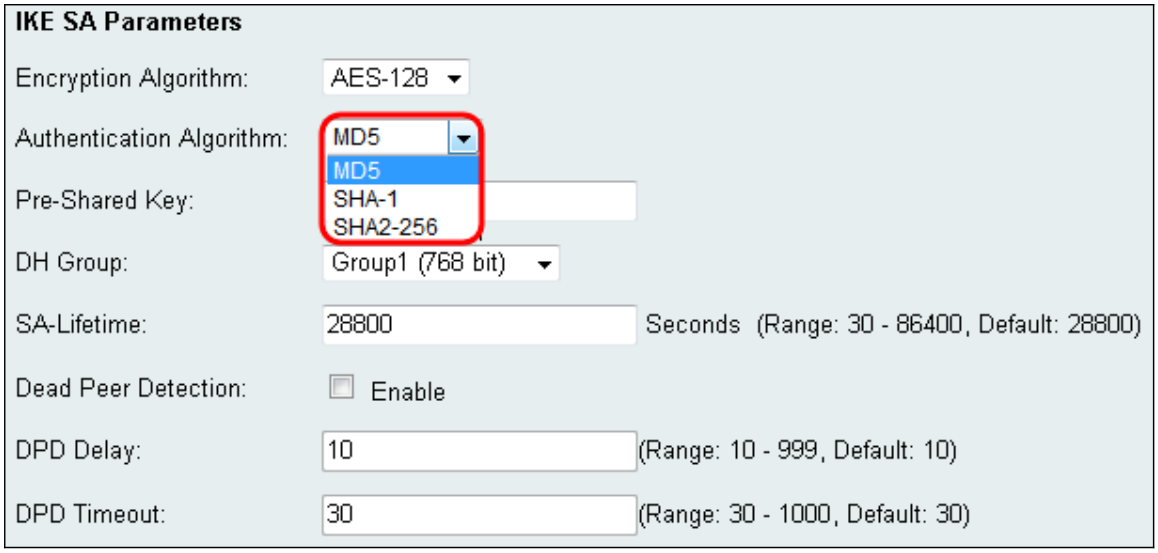
·AES-128 — 高级加密标准使用128位密钥。

·AES-192 — 高级加密标准使用192位密钥。

·AES-256 — 高级加密标准使用256位密钥。

注意：AES是DES和3DES加密的标准方法，因为它具有更高的性能和安全性。延长AES密钥将提高安全性，但性能会下降。建议使用AES-128，因为它在速度和安全性之间提供了最佳折衷。

步骤10.从*Authentication Algorithm*下拉菜单中，选择一个算法以对您的通信进行身份验证。**默认选择SHA**-1。



可用选项定义如下：

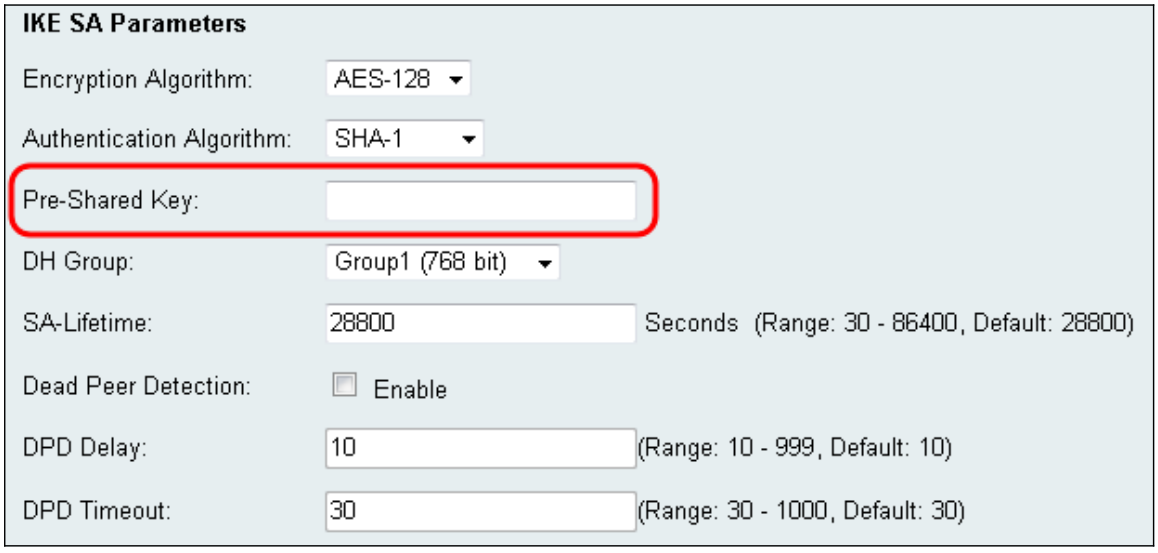
·MD5 — 消息摘要算法具有128位散列值。

·SHA-1 — 安全散列算法具有160位散列值。

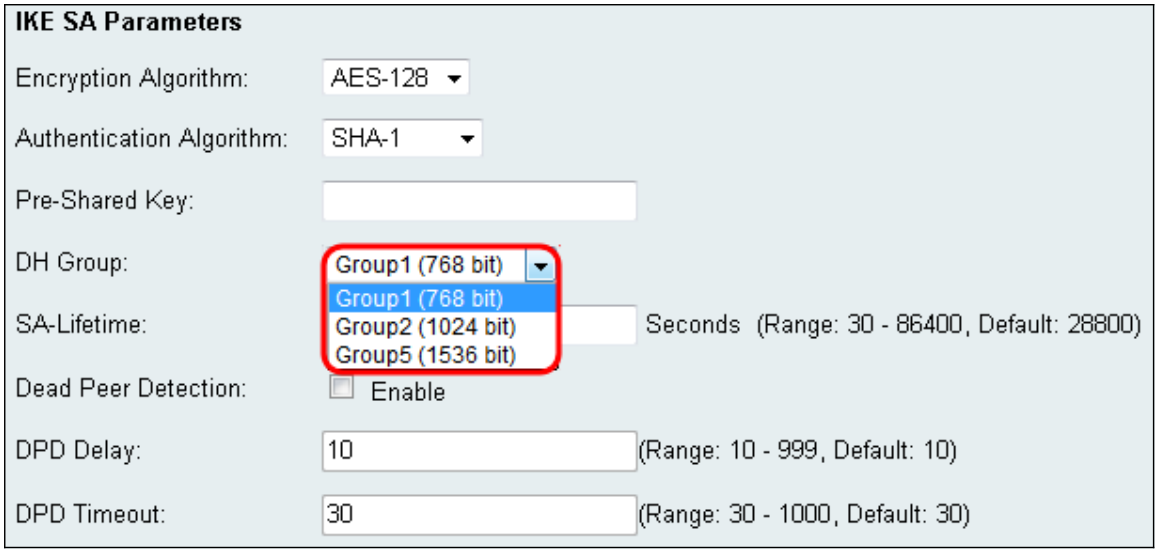
·SHA2-256 — 具有256位哈希值的安全哈希算法。

注意：MD5和SHA都是加密散列函数。他们获取一段数据，将其压缩，然后创建通常不可重复的唯一十六进制输出。MD5基本上不提供散列冲突的安全保护，应仅用于不需要防冲突的小型企业环境。与MD5相比，SHA1是更好的选择，因为它能够以极低的速度提供更好的安全性。为了获得最佳效果，SHA2-256没有实际相关的已知攻击，并将提供最佳安全性。如前所述，安全性越高，速度越慢。

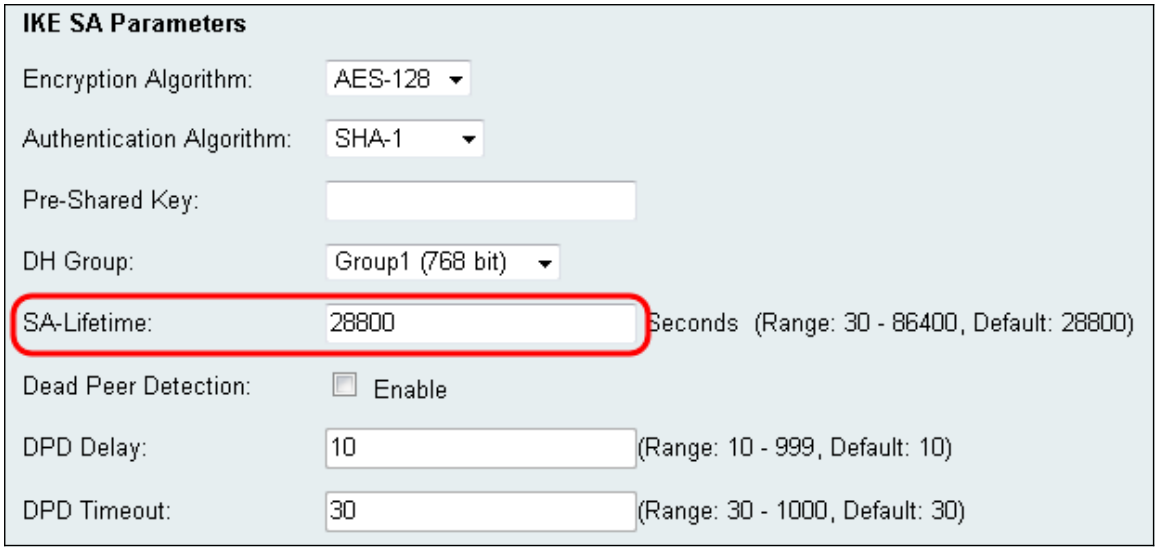
步骤11.在*预共享密钥*字段中，输入长度介于8到49个字符之间的密码。



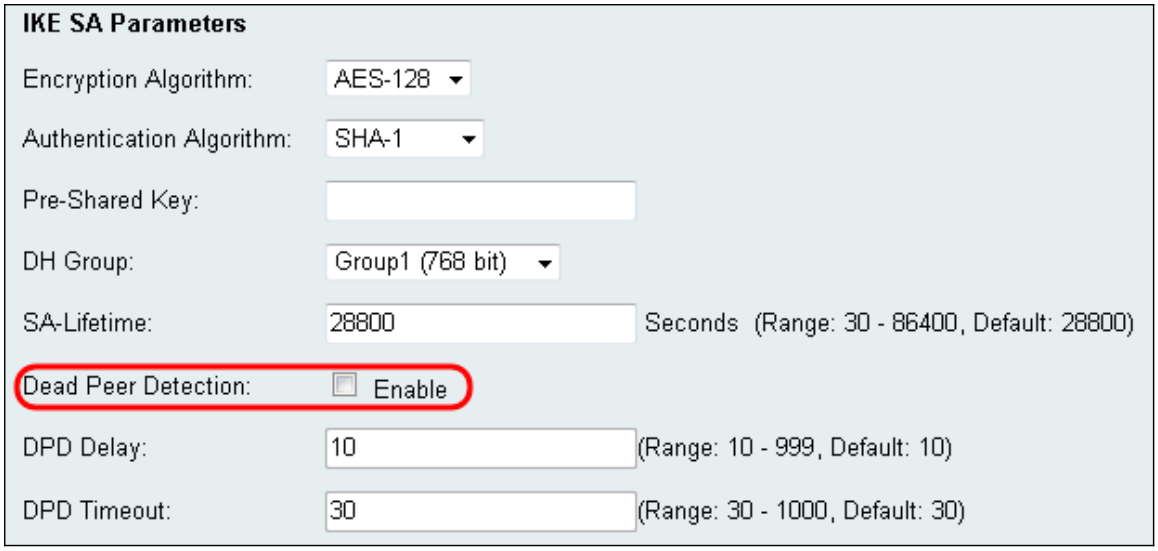
步骤12.从*DH Group*下拉菜单中，选择DH组。位数表示安全级别。连接的两端必须位于同一个组中。



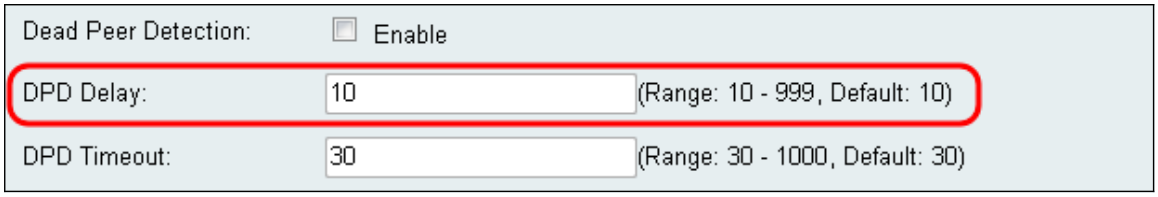
步骤13.在*SA-Lifetime字段*中，输入安全关联的有效时间（以秒为单位）。默认时间为 28800 秒钟。



步骤14.（可选）如果要禁用与非活动对等体的连接，请选中*失效对等体检测*字段中的**启用**复选框。如果未启用Dead peer Detection，请跳到步骤17。

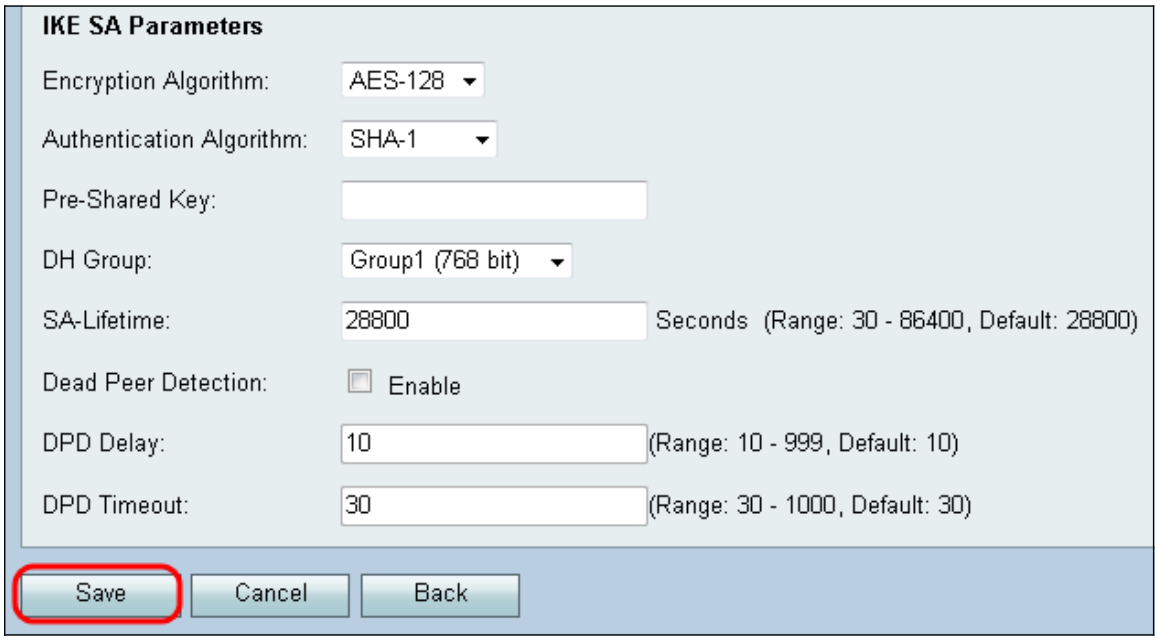


步骤15.（可选）如果启用了失效对等体检测，请在*DPD延迟*字段中输入值。此值将指定路由器等待检查客户端连接的时间长度。



步骤16.（可选）如果启用了失效对等体检测，请在*DPD超时*字段中输入值。此值将指定客户端在超时之前保持连接的时间。

步骤17.单击**Save**保存更改。



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。