

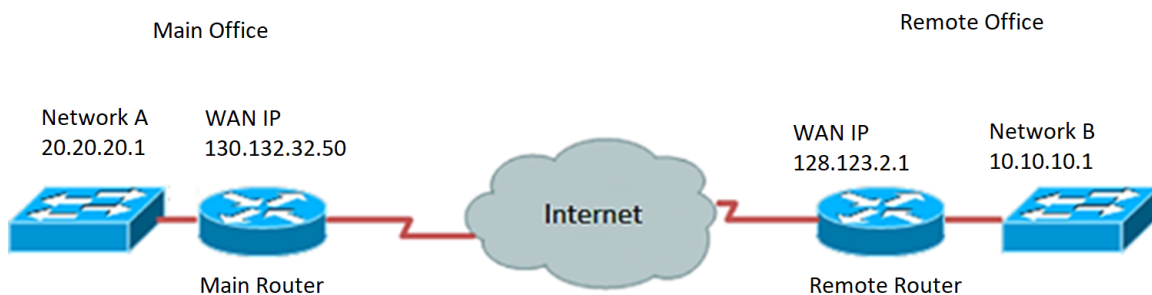
在RV34x系列路由器上使用设置向导配置虚拟专用网络(VPN)连接

目标

虚拟专用网络(VPN)连接允许用户通过公共或共享网络 (如Internet) 访问、发送和接收数据到专用网络和从专用网络接收数据，但仍确保与底层网络基础设施的安全连接以保护专用网络及其资源。

VPN隧道建立一个专用网络，该专用网络可以使用加密和身份验证安全地发送数据。公司办公室大多使用VPN连接，因为即使员工不在办公室，也允许其访问其专用网络既有用也是必要的。

VPN允许远程主机像位于同一本地网络一样工作。路由器支持50个隧道。VPN设置向导可为站点到站点IPSec隧道配置安全连接。此功能使配置变得简单，并防止了复杂的设置和可选参数。这样，任何人都可以快速高效地建立IPSec隧道。



使用VPN连接的优势：

1. 使用VPN连接有助于保护机密网络数据和资源。
2. 为远程员工或公司员工提供方便和可访问性，因为他们将能够轻松访问总部，而无需在现场，同时仍可维护专用网络及其资源的安全。
3. 与其他远程通信方法相比，使用VPN连接的通信提供了更高级别的安全性。当今先进的技术使这成为可能，从而保护专用网络免受未经授权的访问。
4. 用户的实际地理位置受到保护，不会暴露在公共或共享网络 (如Internet) 中。
5. 将新用户或用户组添加到网络很容易，因为VPN是可调整的。无需额外的新组件或复杂的配置，即可实现网络扩展。

使用VPN连接的风险：

1. 配置错误导致的安全风险。由于VPN的设计和实现可能非常复杂，因此需要将连接配置任务委托给知识渊博且经验丰富的专业人员来确保专用网络的安全不会受到损害。
2. 可靠性.由于VPN连接需要Internet连接，因此选择经过验证和测试的提供商来提供卓越的Internet服务并保证最短甚至不会出现停机，这一点非常重要。
3. 可扩展性.如果出现需要添加新基础设施或设置新配置的情况，则可能会出现技术问题，因为不兼容，特别是如果不兼容涉及您已经使用的产品或供应商以外的其他产品或供应商。
4. 移动设备的安全问题。有时，当在启动VPN连接时使用移动设备时，安全问题可能会出现，尤其是当使用无线连接时。某些未经验证的提供程序伪装成“免费VPN提供程序”，甚

至可以在您的计算机上安装恶意软件。因此，可以添加更多安全措施来防止使用移动设备时出现此类问题。

5. 连接速度慢。如果您使用的是提供免费VPN服务的VPN客户端，则可能预期您的连接速度会降低，因为这些提供商不会优先处理连接速度。

本文档的目的是向您展示如何使用安装向导在RV34x系列路由器上配置VPN连接。

适用设备

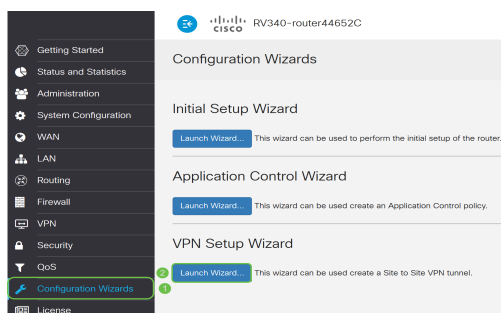
- RV34x系列

软件版本

- 1.0.01.16

使用设置向导配置VPN连接

步骤1. 登录到基于Web的路由器实用程序并选择配置向导。然后单击“VPN Setup Wizard (VPN设置向导)”部分下的Launch Wizard。



步骤2. 在提供的字段中，输入标识此连接的名称。

This Setup Wizard helps you to configure a secure connection between two routers that physically separated over the IPsec VPN tunnel. Before you begin, you need to know the subnet addresses of your local and remote networks, and import the digital certificates for authentication between two peers if needed.

Give this connection a name: E.g Homeoffice

注意：在本例中，使用TestVPN。

步骤3. 在Interface区域，点击下拉菜单并选择要启用此连接的接口。选项有：

- WAN1
- WAN2
- USB1
- USB2



注意：在本例中，使用WAN1。

步骤4.单击“下一步”。

Give this connection a name: TestVPN E.g Homeoffice
Interface: WAN1

Next Cancel

步骤5.点击下拉箭头选择Remote Connection Type。选项有：

- IP Address — 如果要使用VPN隧道另一端的远程路由器的IP地址，请选择此选项。
- FQDN — (完全限定域名) 如果要在VPN隧道的另一端使用远程路由器的域名，请选择此选项。

Remote Connection Type: IP Address

Remote Connection: Enter WAN IP Address

注意：在本例中，选择IP地址。

步骤6.在提供的字段中输入远程连接的WAN IP地址，然后单击“下一步”。

Remote Connection Type: IP Address

Remote Connection: 128.123.2.1 Enter WAN IP Address

Back Next Cancel

注意：在本例中，使用128.123.2.1。

步骤7.在Local Traffic Selection区域下，点击下拉列表选择Local IP。选项有：

- 子网 — 如果要输入本地网络的IP地址和子网掩码，请选择此项。
- IP地址(IP Address) — 如果只想输入本地网络的IP地址，请选择此选项。
- 任意 — 如果您想要其中任意一个，请选择此选项。

Local Traffic Selection

Local IP: Subnet

IP Address: Subnet

Subnet Mask: IP Address

Remote Traffic Selection:

Remote IP: Subnet

IP Address:

Subnet Mask:

注意：在本例中，选择Any。

步骤8.在Remote Traffic Selection区域下，点击下拉箭头选择Remote IP。在提供的字段中输入远程IP地址和子网掩码，然后单击Next。选项有：

- 子网 — 如果要输入远程网络的IP地址和子网掩码，请选择此项。
- IP地址(IP Address) — 如果只想输入远程网络的IP地址，请选择此选项。

Local Traffic Selection

Local IP:

Remote Traffic Selection:

Remote IP:

IP Address:

Subnet Mask:

Back Cancel

注意：在本例中，选择子网。输入10.10.10.0作为IP地址，输入255.255.255.0作为子网掩码。

步骤9.点击IPSec Profile区域中的下拉箭头，选择要使用的配置文件。

IPSec Profile:

IKE Version: IKEv1 IKEv2

注意：在本例中，选择Default。

步骤10.在Phase 1 Options区域下，在提供的字段中输入此连接的预共享密钥。这是用于验证远程互联网密钥交换(IKE)对等体的预共享密钥。VPN隧道的两端必须使用相同的预共享密钥。此密钥最多允许使用30个字符或十六进制值。

注意：强烈建议定期更改预共享密钥，以保持VPN连接的安全性。

Pre-Shared Key:

Pre-shared Key Strength Meter: 


Show Pre-shared Key: Enable

注意：预共享密钥强度计根据以下信息指示您输入的密钥的强度：

- 红色 — 密码弱。
- 琥珀色 — 密码相当强。
- 绿色 — 密码强。

步骤11. (可选) 编辑时，您还可以选中Show plain text中的**Enable**复选框，以便以纯文本形式查看密码。

Pre-Shared Key:

Pre-shared Key Strength Meter: 

Show Pre-shared Key: Enable

步骤12.单击“下一步”。

步骤13.然后，该页面将显示VPN连接的所有配置详细信息。单击“Submit”。

VPN Setup Wizard



Getting Started

Remote Router Settings

Local and Remote Networks

Profile

Summary

Connection Name: TestVPN

Local Interface: WAN1

IPSec Profile: Default

Phase I Options

DH Group: Group5 - 1536 bit

Encryption: AES 128

Authentication: SHA1

Lifetime(sec) 28800

Pre-Shared Key: CiscoTest123!

Perfect Forward Secrecy: Enable

Phase II Options:

DH Group: Group5 - 1536 bit

Protocol Selection: ESP

Back

Submit

Cancel

现在，您应该已使用安装向导在RV34x系列路由器上成功配置了VPN连接。要成功连接站点到站点VPN，您需要在远程路由器上配置设置向导。