

在RV340或RV345路由器上配置站点到站点虚拟专用网络(VPN)连接

目标

虚拟专用网络(VPN)是本地网络和远程主机之间通过Internet的连接。本地和远程主机可以是计算机，也可以是已同步设置以允许它们通信的其他网络。在所有类型的VPN上都是如此。它通常允许两个网络访问连接两端的资源。VPN连接通常用于将第二个办公室连接到总部，或者允许远程员工连接到办公室的计算机网络，即使他并没有实际连接到网络基础架构。远程员工通常通过VPN软件客户端（如AnyConnect、Shrew Soft、GreenBow等）进行连接。

本文旨在展示如何在RV340和RV345路由器之间配置站点到站点VPN连接。它将主路由器称为本地路由器，而辅助路由器称为远程路由器。确保能够远程访问或物理访问辅助路由器。

LAN网络必须位于不同的子网（例如192.168.1.x和192.168.2.x）或完全不同的网络（例如192.168.1.x和10.10.1.x）上。如果两个网络位于同一子网中，路由器不会尝试通过VPN发送数据包。

适用设备

- RV340
- RV340W
- RV345
- RV345P

软件版本

- 1.0.03.15

特别注意：许可结构 — 固件版本1.0.3.15及更高版本。AnyConnect仅会对客户端许可证产生费用。

您需要通过 CDW 等合作伙伴或公司的设备采购部门购买客户端许可证。您可以选择适合 1 个用户使用的许可证 (L-AC-PLS-3Y-S5)，也可以选择适合 25 个用户使用的一年期许可证数据包 (AC-PLS-P-25-S)。还有其他许可证可供选择，包括永久许可证。有关许可的更多详细信息，请查看下面许可信息部分中的链接。

有关 RV340 系列路由器的 AnyConnect 许可的更多信息，请查看 [RV340 系列路由器的 AnyConnect 许可](#) 一文。

配置VPN连接

本地路由器

步骤1:登录本地路由器的基于Web的实用程序，然后选择VPN > Site-to-Site。

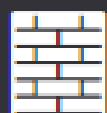
注意：在本示例中，使用RV340。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

第二步：单击plus图标。

Site to Site Table

Connection Name

Remote Endpoint

Interface

IPsec Profile

Local Traffic Selection

Remote Traffic Selection

Static IP

第三步：确保选中Enable复选框。默认是检查。

Basic Settings

Advanced Settings

Failover

Enable:

Connection Name:

Please Input Connection Name

IPsec Profile:

Default

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

第四步：在Connection Name字段中输入连接的名称。

注意：在本示例中，名称为TestVPN1。

Basic Settings

Advanced Settings

Failover

Enable:

☒

Connection Name:

TestVPN1

IPsec Profile:

Default

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

第五步：从IPSec Profile下拉列表中选择连接的安全设置。这些选项取决于创建的IPSec简档。有关如何创建IPSec配置文件的说明，请单击[此处](#)。

注意：在本示例中，选择了CiscoTestVPN。

Basic Settings

Advanced Settings

Failover

Enable:

☒

Connection Name:

TestVPN1

IPsec Profile:

CiscoTestVPN

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

第六步：选择本地路由器要使用的接口。选项有：

- WAN1 — 此选项将使用本地路由器广域网1(WAN1)接口的IP地址进行VPN连接。
- WAN2 — 此选项将使用本地路由器WAN2接口的IP地址进行VPN连接。WAN2在单WAN路由器中不可用。
- USB1 — 此选项将使用本地路由器的通用串行总线1(USB1)接口的IP地址进行VPN连接。

- USB2 — 此选项将使用本地路由器USB2接口的IP地址进行VPN连接。USB2在单USB路由器上不可用。

注意：在本例中，选择了WAN1。

Basic Settings

Advanced Settings

Failover

Enable:

☒

Connection Name:

IPsec Profile:

▼

Auto (IKEv1) Profile is Chosen.

Interface:

▼

Remote Endpoint:

▼

步骤 7.选择远程路由器WAN接口的标识符。选项有：

- 静态IP — 此选项将允许本地路由器在建立VPN连接时使用远程路由器的静态IP地址。如果在本地路由器上选择了此选项，则还应使用相同的选项配置远程路由器。
- FQDN — 建立VPN连接时，此选项将使用远程路由器的完全限定域名(FQDN)。
- 动态IP — 建立VPN连接时，此选项将使用远程路由器的动态IP地址。

注意：远程路由器上的接口标识符应与本地路由器的接口标识符相同。在本示例中，选择静态IP。

Basic Settings

Advanced Settings

Failover

Enable:

☒

Connection Name:

TestVPN1

IPsec Profile:

CiscoTestVPN

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

Static IP

FQDN

Dynamic IP

步骤 8输入远程路由器WAN接口的IP地址。

注意：在本示例中，使用124.123.122.123。

Enable:

☒

Connection Name:

TestVPN

IPsec Profile:

CiscoTestVPN

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

124.123.122.123

步骤 9点击所需的互联网密钥交换(IKE)身份验证方法的单选按钮。选项有：

- 预共享密钥(Preshared Key) — 此选项表示连接需要密码才能完成连接。VPN连接两端的预共享密钥应该相同。
- Certificate — 此选项表示连接时，身份验证方法使用路由器生成的证书而不是密码。

注意：在本示例中，选择预共享密钥。

IKE Authentication Method

☒ Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: ☒ Enable

Show Pre-shared Key: ☐ Enable

☐ Certificate:

步骤 10在预共享密钥字段中输入VPN连接的预共享密钥。

IKE Authentication Method

☒ Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity: ☒ Enable

Show Pre-shared Key: ☐ Enable

☐ Certificate:

步骤11. (可选) 如果要为VPN连接使用简单密码，请取消选中Minimum Preshared Key Complexity Enable复选框。默认情况下会选中此项。

IKE Authentication Method

☒ Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒ Enable

Show Pre-shared Key:

☐ Enable

☐ Certificate:

步骤 12. (可选) 选中Show plain text when edit Enable复选框以纯文本形式显示预共享密钥。默认情况下未选中此项。

IKE Authentication Method

☒ Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒ Enable

Show Pre-shared Key:

☐ Enable

☐ Certificate:

步骤 13从Local Identifier Type下拉列表中选择本地网络的标识符类型。选项有：

- 本地WAN IP — 此选项将通过接口的WAN IP标识本地网络。
- IP地址 — 此选项将通过本地IP地址标识本地网络。
- 本地FQDN — 此选项将通过FQDN标识本地网络 (如果具有FQDN) 。
- 本地用户FQDN(Local User FQDN) — 此选项将通过用户的FQDN (可以是其邮件地址) 标识本地网络。

注意：在本示例中，选择IP地址。

Local Group Setup

Local Identifier Type:

IP Address

Local WAN IP

IP Address

Local FQDN

Local User FQDN

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

步骤 14在本地标识符字段中输入本地网络的标识符。

注意：在本示例中，输入124.123.122.121。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

IP Address:

Subnet Mask:

步骤 15从Local IP Type下拉列表中，选择VPN客户端可以访问的IP Address type。选项有：

- 子网 — 此选项允许VPN的远程端访问指定子网中的本地主机。
- IP地址(IP Address) — 此选项允许VPN的远程端访问具有指定IP地址的本地主机。
- Any — 此选项允许VPN的远程端访问任何本地主机。

注意：在本例中，选择了子网。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

Subnet

IP Address

IP Group

GRE Interface

Any

IP Address:

Subnet Mask:

步骤 16在IP地址字段中输入要由VPN客户端访问的网络或主机的IP地址。

注意：在本示例中，IP地址为10.10.10.1。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

IP Address:

10.10.10.1

Subnet Mask:

步骤 17在Subnet Mask字段中输入IP地址的子网掩码。

注意：在本示例中，子网掩码为255.255.255.0。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.121

Local IP Type:

Subnet

IP Address:

10.10.10.1

Subnet Mask:

255.255.255.0

步骤 18.从下拉列表中选择Remote Identifier Type。选项有：

- 远程WAN IP — 此选项将通过接口的WAN IP标识远程网络。
- 远程FQDN — 此选项将通过FQDN识别远程网络（如果具有FQDN）。
- 远程用户FQDN(Remote User FQDN) — 此选项将通过用户的FQDN（可以是其邮件地址）标识远程网络。

注意：在本例中，选择了远程WAN IP。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

Remote WAN IP

Remote IP Type:

Remote FQDN

IP Address:

Remote User FQDN

Subnet Mask:

Subnet

IP Address:

Subnet Mask:

步骤 19.在远程标识符字段中输入远程路由器的WAN IP地址。

注意：在本示例中，远程标识符为124.123.122.123。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.123

Remote IP Type:

Subnet

IP Address:

Subnet Mask:

步骤 20.从Remote IP Type下拉列表中选择本地网络需要访问的网络类型。选项有：

- IP地址(IP Address) — 此选项允许本地主机访问具有指定IP地址的远程主机。
- 子网 — 此选项允许本地主机访问具有指定子网的远程主机上的资源。
- Any — 此选项允许本地主机使用任何IP地址访问远程主机上的资源。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.123

Remote IP Type:

Subnet

Subnet

IP Address

IP Group

Any

IP Address:

Subnet Mask:

步骤 21.在IP地址字段中输入远程网络的LAN IP地址。

注意：在本示例中，IP地址为192.168.2.1。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.123

Remote IP Type:

Subnet

IP Address:

192.168.2.1

Subnet Mask:

步骤 22.在子网掩码字段中输入远程网络的子网掩码。

注意：在本示例中，子网掩码为255.255.255.0。

Remote Group Setup

Remote Identifier Type:

Remote WAN IP

Remote Identifier:

124.123.122.123

Remote IP Type:

Subnet

IP Address:

192.168.2.1

Subnet Mask:

255.255.255.0

步骤 23.单击 Apply。

Add/Edit a New Connection

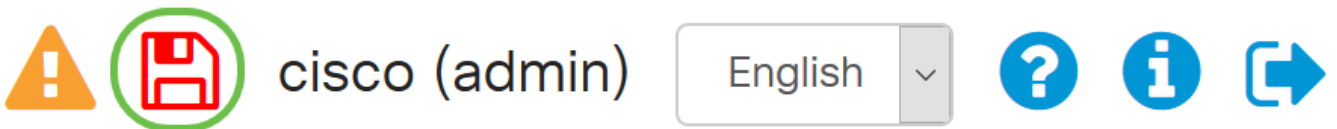
[Apply](#)[Cancel](#)

Local IP Type:	Subnet
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.123
Remote IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

步骤 24Click Save.



现在，您应该在本地路由器上配置VPN设置。

远程路由器

步骤1:确定本地路由器的VPN设置，例如：

- 用于VPN连接的本地和远程路由器的接口。
- 本地和远程路由器的广域网(WAN)互联网协议(IP)地址。
- 本地和远程网络的局域网(LAN)地址和子网掩码。
- VPN连接的预共享密钥、密码或证书。
- 本地路由器的安全设置。
- VPN连接的防火墙免除。

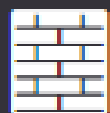
第二步：登录路由器的基于Web的实用程序，然后选择VPN > IPSec Profiles。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

2

Site-to-Site

Client-to-Site

Teleworker VPN Client

PPTP Server

第三步：配置远程路由器的VPN安全设置，使其与本地路由器的VPN安全设置匹配。如需指导，请点击[这里](#)。

第四步：在本地路由器的基于Web的实用程序上，选择VPN > Site-to-Site。



LAN



Routing



Firewall



VPN

1

VPN Status

IPSec Profiles

Site-to-Site

2

Client-to-Site

Teleworker VPN Client

PPTP Server

第五步：单击plus图标。

Site to Site Table ^

+

□

Connection Name

◆

Remote Endpoint

◆

Interface

◆

IPsec Profile

◆

Local Traffic Selection

◆

Remote Traffic Selection

◆

Static

◆

第六步：确保选中Enable复选框。默认是检查。

Enable:

✓

Connection Name:

Please Input Connection Name

IPsec Profile:

Default

▼

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

▼

Remote Endpoint:

Static IP

▼

步骤 7.在Connection Name字段中输入VPN连接的名称。远程路由器的连接名称可能与本地路由器中指定的连接名称不同。

Enable: ☒

Connection Name:

TestVPN

IPsec Profile:

Default

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

注意：在本示例中，连接名称为TestVPN。

步骤 8从下拉列表中选择IPSec Profile。这些选项取决于创建的IPSec简档。有关创建IPSec配置文件的说明，请单击[此处](#)。

注意：在本示例中，选择了CiscoTestVPN。

Enable: ☒

Connection Name:

TestVPN

IPsec Profile:

CiscoTestVPN

Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

Remote Endpoint:

Static IP

步骤 9 从下拉列表中选择远程路由器将用于VPN连接的接口。选项有：

- WAN1 — 此选项将使用远程路由器广域网1(WAN1)接口的IP地址进行VPN连接。
- WAN2 — 此选项将使用远程路由器WAN2接口的IP地址进行VPN连接。WAN2在单WAN路由器中不可用。
- USB1 — 此选项将使用远程路由器的通用串行总线1(USB1)接口的IP地址进行VPN连接。
- USB2 — 此选项将使用远程路由器USB2接口的IP地址进行VPN连接。USB2在单USB路由器上不可用。

注意：在本例中，选择了WAN1。

Enable:



Connection Name:

TestVPN

IPsec Profile:

CiscoTestVPN



Auto (IKEv1) Profile is Chosen.

Interface:

WAN1



Remote Endpoint:

Static IP



步骤 10 从Remote Endpoint下拉列表中选择本地路由器WAN接口的标识符。选项有：

- 静态IP — 此选项将允许远程路由器在建立VPN连接时使用本地路由器的静态IP地址。如果在本地路由器上选择了此选项，则还应使用相同的选项配置远程路由器。
- FQDN — 建立VPN连接时，此选项将使用本地路由的完全限定域名(FQDN)。
- 动态IP — 建立VPN连接时，此选项将使用本地路由器的动态IP地址。

注意：远程路由器上的接口标识符应与本地路由器的接口标识符相同。在本示例中，选择静态IP。

Enable: ☒

Connection Name:

IPsec Profile:

CiscoTestVPN

▼

 Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

▼

Remote Endpoint:

Static IP

▼

步骤 11输入本地路由器的WAN IP地址。

注意：在本示例中，IP地址为124.123.122.121。

Enable: ☒

Connection Name:

IPsec Profile:

CiscoTestVPN

▼

 Auto (IKEv1) Profile is Chosen.

Interface:

WAN1

▼

Remote Endpoint:

Static IP

▼

124.123.122.121

步骤 12点击所需的互联网密钥交换(IKE)身份验证方法的单选按钮。选项有：

- 预共享密钥(Preshared Key) — 此选项表示连接需要密码才能完成连接。VPN连接两端的预共享密钥应该相同。
- Certificate — 此选项表示连接时，身份验证方法使用路由器生成的证书而不是密码。

注意：在本示例中，选择预共享密钥。

IKE Authentication Method

☒ Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒ Enable

Show Pre-shared Key:

☐ Enable

☐ Certificate:

步骤 13在预共享密钥字段中输入VPN连接的预共享密钥。

IKE Authentication Method

☒ Pre-shared Key:

●●●●●●●●

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒ Enable

Show Pre-shared Key:

☐ Enable

☐ Certificate:

步骤14. (可选) 如果要对VPN连接使用简单密码，请取消选中Minimum Preshared Key Complexity复选框Enable。默认情况下会选中此项。

IKE Authentication Method

☒

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒

Enable

Show Pre-shared Key:

☐

Enable

☐

Certificate:

步骤 15. (可选) 选中Show plain text when edit Enable复选框以纯文本形式显示预共享密钥。默认情况下未选中此项。

IKE Authentication Method

☒

Pre-shared Key:

Pre-shared Key Strength Meter:

Minimum Pre-shared Key Complexity:

☒

Enable

Show Pre-shared Key:

☐

Enable

☐

Certificate:

- 步骤 16从远程路由器的Local Identifier Type下拉列表中选择远程网络的标识符类型。选项有：
- 本地WAN IP — 此选项将通过接口的WAN IP标识远程网络。
 - IP地址 — 此选项将通过本地IP地址标识远程网络。
 - 本地FQDN — 此选项将通过FQDN识别远程网络（ 如果它有一个 ）。
 - 本地用户FQDN(Local User FQDN) — 此选项将通过用户的FQDN（ 可以是其邮件地址 ）标识远程网络。

注意：在本示例中，选择IP地址。

Local Group Setup

Local Identifier Type:

IP Address

Local WAN IP

IP Address

Local FQDN

Local User FQDN

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

步骤 17在远程路由器的本地标识符字段中输入远程网络的标识符。

注意：在本示例中，输入124.123.122.123。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.123

Local IP Type:

Subnet

IP Address:

Subnet Mask:

步骤 18.从Local IP Type下拉列表中，选择VPN客户端可以访问的IP Address type。选项有：

- 子网 — 此选项允许VPN的本地端访问指定子网中的远程主机。
- IP地址(IP Address) — 此选项允许VPN的本地端访问具有指定IP地址的远程主机。
- Any — 此选项允许VPN的本地端访问任何远程主机。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.123

Local IP Type:

Subnet

IP Address:

Subnet Mask:

注意：在本例中，选择了子网。

步骤 19.在IP地址字段中输入要由VPN客户端访问的网络或主机的IP地址。

注意：在本示例中，IP地址为192.168.2.1。

Local Group Setup

Local Identifier Type:

IP Address

Local Identifier:

124.123.122.123

Local IP Type:

Subnet

IP Address:

192.168.2.1

Subnet Mask:

步骤 20.在Subnet Mask字段中输入IP地址的子网掩码。

注意：在本示例中，子网掩码为255.255.255.0。

Local Group Setup

Local Identifier Type:	IP Address
Local Identifier:	124.123.122.123
Local IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

步骤 21.从下拉列表中选择Local Identifier Type。选项有：

- 远程WAN IP — 此选项将通过接口的WAN IP标识本地网络。
- 远程FQDN — 此选项将通过FQDN标识本地网络（如果具有FQDN）。
- 远程用户FQDN(Remote User FQDN) — 此选项将通过用户的FQDN（可以是其邮件地址）标识本地网络。

注意：在本例中，选择了远程WAN IP。

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.121
Remote IP Type:	Subnet
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0

步骤 22.单击 Apply。

Add/Edit a New Connection

[Apply](#)[Cancel](#)

Local IP Type:	Subnet
IP Address:	192.168.2.1
Subnet Mask:	255.255.255.0

Remote Group Setup

Remote Identifier Type:	Remote WAN IP
Remote Identifier:	124.123.122.121
Remote IP Type:	Subnet
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0

步骤 23.Click Save.



cisco (admin)

English



现在，您应该在远程路由器上配置了VPN设置。

观看与本文相关的视频...

[点击此处查看思科的其他技术讲座](#)

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）。