

在RV34x系列路由器上配置客户端到站点虚拟专用网络(VPN)连接

目标

在客户端到站点虚拟专用网络(VPN)连接中，来自Internet的客户端可以连接到服务器以访问公司网络或服务器后的局域网(LAN)，但仍然维护网络及其资源的安全。此功能非常有用，因为它创建了新的VPN隧道，使远程工作人员和商务旅客能够使用VPN客户端软件访问您的网络，而不会影响隐私和安全性。

本文档旨在向您展示如何在RV34x系列路由器上配置客户端到站点VPN连接。

适用设备

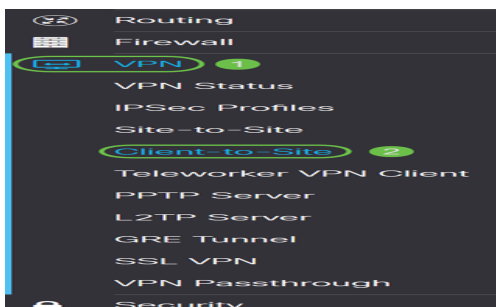
- RV34x系列

软件版本

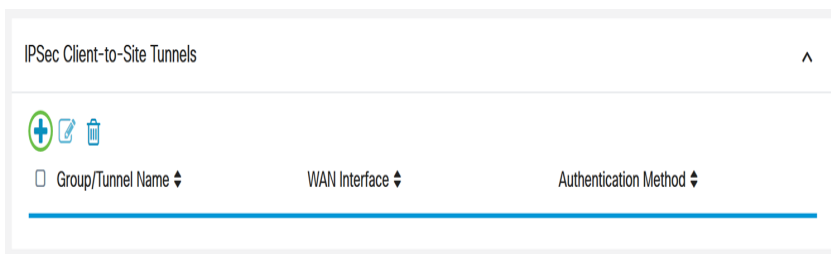
- 1.0.01.16

配置客户端到站点VPN

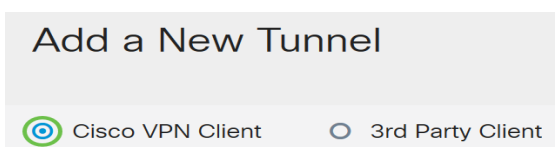
步骤1. 登录到路由器基于Web的实用程序，然后选择VPN > Client-to-Site。



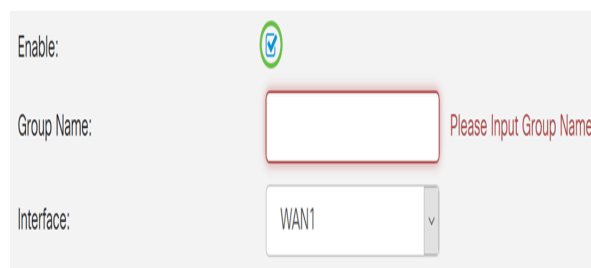
步骤2. 单击“IPSec客户端到站点隧道”部分下的“添加”按钮。



步骤3. 在Add a New Tunnel区域，单击Cisco VPN Client单选按钮。



步骤4.选中Enable复选框以启用配置。

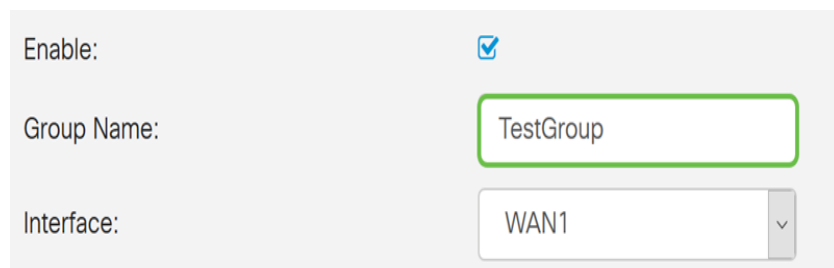


Enable:

Group Name: Please Input Group Name

Interface: WAN1

步骤5.在提供的字段中输入组名。这将在互联网密钥交换(IKE)协商期间用作此组所有成员的标识符。



Enable:

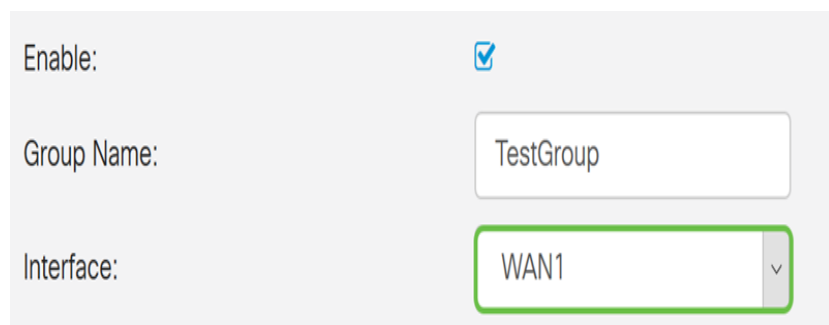
Group Name: TestGroup

Interface: WAN1

注意：输入A到Z或0到9之间的字符。组名称不允许使用空格和特殊字符。在本例中，使用TestGroup。

步骤6.点击下拉列表选择接口。选项有：

- WAN1
- WAN2
- USB1
- USB2



Enable:

Group Name: TestGroup

Interface: WAN1


注意：在本例中，选择WAN1。这是默认设置。

步骤7.在IKE Authentication Method区域中，选择要在基于IKE的隧道的IKE协商中使用的身份验证方法。选项有：

- 预共享密钥 — IKE对等体通过计算和发送包含预共享密钥的数据的密钥散列来相互验证。如果接收对等体能够使用其预共享密钥独立创建相同的哈希值，则它知道两个对等体必须共享相同的密钥，从而对另一个对等体进行身份验证。预共享密钥扩展不良，因为每个IPSec对等体必须配置其建立会话的所有其他对等体的预共享密钥。
- 证书 — 数字证书是包含载体的证书身份等信息的包：名称或IP地址、证书的序列号到期日期，以及证书持有者的公钥副本。标准数字证书格式在X.509规范中定义。X.509第3版定义证书的数据结构。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable


Certificate:

注意：在本例中，选择预共享密钥。这是默认设置。

步骤8.在提供的字段中输入预共享密钥。这将是IKE对等体组中的身份验证密钥。

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9. (可选) 选中Minimum Pre-shared Key Complexity (最小预共享密钥复杂性) 的 **Enable** (启用) 复选框，以查看Pre-shared Key Strength Meter (预共享密钥强度计) 并确定密钥的强度。密钥的强度定义如下：

- 红色 — 密码很弱。
- 橙色 — 密码相当强。
- 绿色 — 密码强。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

注意：您可以选中“显示预共享密钥”字段中的“启用”复选框，以纯文本形式检查密码。

IKE Authentication Method

Pre-shared Key: 2

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: 1 Enable

Certificate:

步骤10. (可选) 单击“用户组”表中的加号图标可添加组。

User Group Table


Group Name 

第11步. (可选) 从下拉列表中选择用户组是用于管理员还是用于访客。如果您使用用户帐户创建了自己的用户组，则可以选择它。在本例中，我们将选择TestGroup。

注意：测试组是我们在“系统配置”>“用户组”中创建的用户组。

User Group Table

Group Name 

TestGroup

TestGroup

VPNUsers

Mode: admin

Mode: guest

Pool Range: [unclear]

注意：在本例中，选择TestGroup。如果要删除用户组，还可以选中用户组旁的框，然后单击“删除”按钮。

步骤12.单击单选按钮选择模式。选项有：

- 客户端 — 此选项允许客户端请求IP地址，并且服务器从配置的地址范围提供IP地址。
- 网络扩展模式(NEM) — 此选项允许客户端建议其子网，需要将VPN服务应用于服务器后的LAN与客户端建议的子网之间的流量。

Mode: Client NEM

注意：在本例中，选择Client。

步骤13.在“开始IP”字段中输入起始IP地址。这是池中可分配给客户端的第一个IP地址。

Pool Range for Client LAN

Start IP:

End IP:

注意：在本例中，使用192.168.100.1。

步骤14.在End IP (结束IP) 字段中输入结束IP地址。这是池中可分配给客户端的最后一个IP地址。

Pool Range for Client LAN

Start IP:

End IP:

注意：在本例中，使用192.168.100.100。

步骤15. (可选) 在Mode Configuration区域下，在提供的字段中输入主DNS服务器的IP地址。

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

注意：在本例中，使用192.168.1.1。

步骤16. (可选) 在提供的字段中输入辅助DNS服务器的IP地址。

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

注意：在本例中，使用192.168.1.2。

步骤17. (可选) 在提供的字段中输入主WINS服务器的IP地址。

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text"/>

注意：在本例中，使用192.168.1.1。

步骤18. (可选) 在提供的字段中输入辅助WINS服务器的IP地址。

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text" value="192.168.1.2"/>

注意：在本例中，使用192.168.1.2。

步骤19. (可选) 在提供的字段中输入远程网络中使用的默认域。

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

注意：在本例中，使用sample.com。

第20步。(可选) 在备份服务器1字段中，输入备份服务器的IP地址或域名。这将是设备在主IPSec VPN服务器发生故障时启动VPN连接的位置。在提供的字段中最多可输入三台备份服务器。备份服务器1在三台服务器中具有最高优先级，而备份服务器3具有最低优先级。

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text" value="example.com"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

注意：在本例中，Example.com用于备份服务器1。

步骤21. (可选) 选中Split Tunnel复选框以启用拆分隧道。分割隧道允许您同时访问专用网络和互联网的资源。

Split Tunnel:

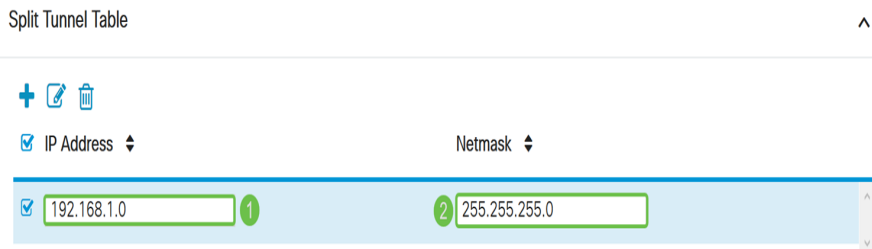


步骤22. (可选) 在分割隧道表下，单击加号图标为分割隧道添加IP地址。

Split Tunnel Table

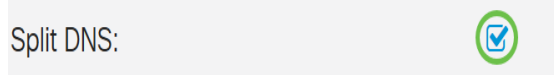


步骤23. (可选) 在提供的字段中输入拆分隧道的IP地址和子网掩码。



注意：在本例中，使用192.168.1.0和255.255.255.0。您还可以选中该框并单击Add、Edit和Delete按钮，分别添加、编辑或删除拆分隧道。

步骤24. (可选) 选中Split DNS复选框以启用拆分DNS。分割DNS允许您为内部和外部网络创建单独的DNS服务器，以维护网络资源的安全和隐私。



步骤25. (可选) 单击“拆分DNS表”下的加号图标，为拆分DNS添加域名。

Split DNS Table



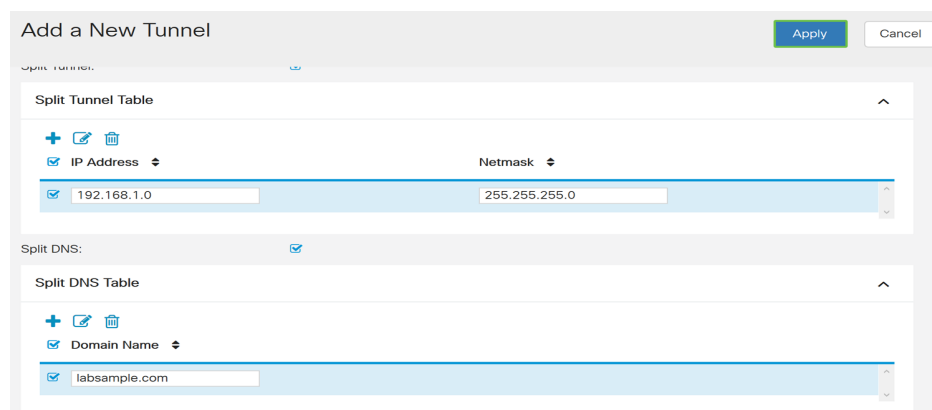
步骤26. (可选) 在提供的字段中输入拆分DNS的域名。

Split DNS Table



注意：在本例中，使用labsample.com。您还可以选中该框并单击**Add**、**Edit**和**Delete**按钮，分别添加、编辑或删除拆分DNS。

步骤27.单击“应用”。



结论

您现在应该已在RV34x系列路由器上成功配置了客户端到站点连接。

点击以下文章以了解有关以下主题的详细信息：

- [在RV34x系列路由器上配置远程工作人员VPN客户端](#)
- [使用GreenBow VPN客户端连接RV34x系列路由器](#)
- [在RV34x路由器上为VPN客户端设置创建用户帐户](#)
- [在RV34x路由器上为VPN设置创建用户组](#)

查看与本文相关的视频.....

[单击此处查看思科提供的其他技术讲座](#)