

# 在RV320和RV325 VPN路由器系列上配置组客户端到网关虚拟专用网络(VPN)

## 目标

虚拟专用网络(VPN)是专用网络，用于通过公共网络虚拟连接远程用户的设备以提供安全性。其中一种VPN类型是客户端到网关VPN。通过客户端到网关，您可以远程连接位于不同地理区域的公司不同分支机构，以便更安全地在区域之间传输和接收数据。组VPN可轻松配置VPN，因为它无需为每个用户配置VPN。RV32x VPN路由器系列最多可支持两个VPN组。

本文档的目标是说明如何在RV32x系列VPN路由器上配置组客户端到网关VPN。

## 适用设备

- RV320双WAN VPN路由器
- RV325千兆双WAN VPN路由器

## 软件版本

- v1.1.0.09

## 配置组客户端到网关VPN

步骤1.登录路由器配置实用程序并选择VPN > Client to Gateway。系统将打开 *Client to Gateway* (客户端到网关) 页面：

## Client to Gateway

### Add a New Tunnel

Tunnel     Group VPN     Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

Enable:

### Local Group Setup

Local Security Gateway Type:

IP Only

IP Address:

0.0.0.0

Local Security Group Type:

Subnet

IP Address:

192.168.1.0

Subnet Mask:

255.255.255.0

### Remote Client Setup

Remote Security Gateway Type:

IP Only

IP Address

:

步骤2.单击Group VPN单选按钮以添加组客户端到网关VPN。



### Client to Gateway

**Add a New Group VPN**

Tunnel     Group VPN     Easy VPN

Group No.    1

Tunnel Name:    tunnel\_1

Interface:    WAN1

Keying Mode:    IKE with Preshared key

Enable:   

---

**Local Group Setup**

Local Security Group Type:    Subnet

IP Address:    192.168.1.0

Subnet Mask:    255.255.255.0

---

**Remote Client Setup**

Remote Client:    DomainName(FQDN)

Domain Name:   

**注意：**组编号 — 表示组编号。它是自动生成的字段。

步骤2.从接口(Interface)下拉列表中，选择VPN组连接网关时所使用的适当接口。



### Client to Gateway

**Add a New Group VPN**

Tunnel     Group VPN     Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

---

**Remote Client Setup**

Remote Client: DomainName(FQDN)

Domain Name:

**注意：**键控模式 — 显示使用的身份验证模式。带预共享密钥的IKE是唯一的选项，这意味着Internet密钥交换(IKE)协议用于自动生成和交换预共享密钥，以建立隧道的经过身份验证的通信。

步骤4.要保存您到目前为止的设置并将其余设置保留为默认值，请向下滚动并单击“保存”以保存设置。

## 本地组设置

步骤1.从Local Security Group Type下拉列表中选择可以访问VPN隧道的适当的本地LAN用户或用户组。默认为子网。

### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: Subnet

IP Address: Subnet

Subnet Mask: 255.255.255.0

---

**Remote Client Setup**

Remote Client: DomainName(FQDN)

Domain Name:

可用选项定义如下：

- IP — 只有一个特定LAN设备可以访问隧道。如果选择此选项，请在“IP Address”（IP 地址）字段中输入 LAN 设备的 IP 地址。默认 IP 地址为 192.168.1.0。
- 子网 — 特定子网上的所有LAN设备都可以访问隧道。如果选择此选项，请分别在“IP Address”（IP 地址）和“Subnet Mask”（子网掩码）字段中输入 LAN 设备的 IP 地址和子网掩码。默认掩码为 255.255.255.0。
- IP范围 — 一系列LAN设备可以访问隧道。如果选择此选项，请在开始IP和结束IP字段中分别输入范围的第一个和最后一个。默认范围为 192.168.1.0 到 192.168.1.254。

步骤2.要保存您目前拥有的设置并将其余设置保留为默认值，请向下滚动并单击“保存”以保存设置。

## 远程客户端设置

步骤1.从Remote Security Group Type下拉列表中，选择可以访问VPN隧道的相应远程LAN用户或用户组。

### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: IP

IP Address: 192.168.3.0

---

**Remote Client Setup**

Remote Client: 
DomainName(FQDN)
  
DomainName(FQDN)
  
Email Address(USER FQDN)
  
Microsoft XP/2000 VPN Client

Domain Name:

可用选项定义如下：

- 域名(FQDN)身份验证 — 可以通过注册的域访问隧道。如果选择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。
- 邮件地址(USER FQDN)身份验证 — 可通过邮件地址访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。
- Microsoft XP/2000 VPN客户端 — 可通过内置Microsoft XP或2000 VPN客户端软件的客户端软件访问隧道。

步骤2.要保存您目前拥有的设置并将其余设置保留为默认值，请向下滚动并单击“保存”以保存设置。

## IPSec 设置选项

步骤1.从Phase 1 DH组下拉列表中选择适当的Diffie-Hellman(DH)组。第1阶段用于在隧道两端之间建立单工逻辑安全关联(SA)，以支持安全的身份验证通信。Diffie-Hellman是用于第1阶段连接的加密密钥交换协议，用于共享密钥以验证通信。



**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

可用选项定义如下：

- 组1 ( 768位 ) — 计算密钥的速度最快，但安全性最低。
- 组2 ( 1024位 ) — 计算密钥的速度较慢，但比组1更安全。
- 组5 ( 1536位 ) — 计算最慢的密钥，但最安全。

步骤2.从Phase 1 Encryption下拉列表中选择适当的加密方法来加密密钥。AES-128因其高安全性和快速性能而被推荐。VPN隧道两端均需使用相同的加密方法。

**Remote Client Setup**

Remote Client: Microsoft XP/2000 VPN Client

---

**IPSec Setup**

Phase 1 DH Group: Group 2 - 1024 bit

Phase 1 Encryption: DES (highlighted in blue and circled in red)

Phase 1 Authentication: 3DES

Phase 1 SA Lifetime: sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Advanced +

可用选项定义如下：

- DES — 数据加密标准(DES)是一种56位旧式加密方法，它不是一种非常安全的加密方法，但可能需要它才能向后兼容。
- 3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，用于增加密钥大小，因为它对数据加密三次。这比DES提供更高的安全性，但比AES安全性更低。
- AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，AES也比3DES更快、更安全。AES-128比AES-192和AES-256更快，但安全性较低。
- AES-192 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，比AES-256快但不安全。
- AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步骤3.从“第1阶段身份验证”下拉列表中选择适当的身份验证方法。VPN隧道需要对两端使用相同的身份验证方法。

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

可用选项定义如下：

- MD5 — 消息摘要算法5(MD5)表示128位哈希函数，通过校验和计算保护数据免受恶意攻击。
- SHA1 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全。

步骤4.在 *Phase 1 SA Life Time* 字段中，输入VPN隧道在第1阶段保持活动状态的时间量（以秒为单位）。默认时间为28,800秒。

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

步骤5. ( 可选 ) 要为密钥提供更多保护，请选中**Perfect Forward Secrecy**复选框。此选项允许您在任何密钥被泄露时生成新密钥。推荐采取此操作，因为它可以提供更高的安全性。

**注意：**如果在步骤5中取消选中完全向前保密，则无需配置第2阶段DH组。

步骤6.从第2阶段DH组下拉列表中选择适当的DH组。

**IPSec Setup**

Phase 1 DH Group: Group 2 - 1024 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 2700 sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: Group 1 - 768 bit

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Advanced +

可用选项定义如下：

- 组1（768位）— 计算密钥的速度最快，但安全性最低。
- 组2（1024位）— 计算密钥的速度较慢，但比组1更安全。
- 组5（1536位）— 计算最慢的密钥，但最安全。

步骤2.从Phase 1 Encryption下拉列表中选择适当的加密方法来加密密钥。AES-128因其高安全性和快速性能而被推荐。VPN隧道两端均需使用相同的加密方法。

**IPSec Setup**

Phase 1 DH Group: Group 2 - 1024 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 2700 sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group: Group 2 - 1024 bit

Phase 2 Encryption: DES

Phase 2 Authentication:

Phase 2 SA Lifetime: sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Advanced +

可用选项定义如下：

·DES — 数据加密标准(DES)是一种56位旧式加密方法，它不是一种非常安全的加密方法，但可能需要它才能向后兼容。

·3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，用于增加密钥大小，因为它对数据加密三次。这比DES提供更高的安全性，但比AES安全性更低。

·AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，AES也比3DES更快、更安全。AES-128比AES-192和AES-256更快，但安全性较低。

·AES-192 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，比AES-256快但不安全。

·AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步骤8.从第2阶段身份验证下拉列表中选择适当的身份验证方法。VPN隧道需要对其两端使用相同的身份验证方法。

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

可用选项定义如下：

- MD5 — 消息摘要算法5(MD5)表示128位哈希函数，通过校验和计算保护数据免受恶意攻击。
- SHA1 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全。

步骤9.在*Phase 2 SA Lifetime*字段中，输入VPN隧道在第2阶段保持活动状态的时间量（以秒为单位）。默认时间为3600秒。

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter: 

步骤10. ( 可选 ) 如果要启用预共享密钥的强度计，请选中Minimum Preshared Key Complexity复选框。

**注意：**如果选中Minimum Preshared Key Complexity复选框，预共享密钥强度计通过彩色条显示预共享密钥的强度。红色表示弱强度，黄色表示可接受强度，绿色表示强度。

步骤11.在预共享密钥字段中输入所需的密钥。最多可使用30个十六进制数作为预共享密钥。VPN隧道的两端需要使用相同的预共享密钥。

**注意：**强烈建议频繁更改IKE对等体之间的预共享密钥，以保护VPN。

步骤12.要保存您到目前为止的设置并将其余设置保留为默认值，请向下滚动并单击“保存”以保存设置。

## 高级设置

步骤1.单击“高级”以配置高级设置。



**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter:

**Advanced +**

系统将显示Advanced区域，其中新字段可用。

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter:

**Advanced -**

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

步骤2. ( 可选 ) 如果网络速度较低，请选中Aggressive Mode复选框。主动模式在SA连接期间以明文交换隧道端点的ID，这需要更少的交换时间，但安全性较低。

步骤3. ( 可选 ) 如果要压缩IP数据报的大小，请选中**Compress(Support IP Payload Compression Protocol(IPComp))**复选框。IPComp是一种IP压缩协议，用于在网络速度较低以及用户希望快速传输数据而不造成任何损失时压缩IP数据报的大小。

步骤4. ( 可选 ) 如果始终希望VPN隧道的连接保持活动状态，请选中**Keep-Alive**复选框。Keep-Alive有助于在任何连接变为非活动状态时立即重新建立连接。

步骤5. ( 可选 ) 如果要对数据源进行身份验证、通过校验和进行的数据完整性和扩展到IP报头的保护，请选中**AH Hash Algorithm**复选框。然后从下拉列表中选择适当的身份验证方法。隧道两端的算法应相同。

可用选项定义如下：

- MD5 — 消息摘要算法5(MD5)表示128位哈希函数，通过校验和计算保护数据免受恶意攻击。
- SHA1 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全。

步骤6.如果要允许不可路由的流量通过VPN隧道，请选中**NetBIOS Broadcast**复选框。默认情况下为未选中状态。NetBIOS用于通过软件应用和Windows功能（如Network Neighborhood）检测网络中的打印机、计算机等网络资源。

步骤7. ( 可选 ) 如果要通过公有IP地址从私有LAN访问Internet，请选中**NAT Traversal**复选框。NAT穿越用于使内部系统的私有IP地址显示为公有IP地址，以保护私有IP地址免受任何恶意攻击或发现。

步骤8.单击“**保存**”以保存设置。