RV016、RV042、RV042G和RV082 VPN路由器上的VPN隧道设置

目标

虚拟专用网络(VPN)是两个终端之间的安全连接。通过VPN隧道建立在这两个位置或网络之间安全地发送数据的专用网络。VPN隧道连接两个人计算机或网络并且允许数据传输在互联网，好象端点就在网络内。VPN是适合员工经常出差或经常在LAN外的公司的好解决方案。使用VPN，这些员工可以访问LAN并使用可用资源完成工作。此外，VPN可以连接两个或多个站点，因此拥有不同分支机构的公司可以相互通信。

注意：RV有线路由器系列提供两种VPN类型：网关到网关和客户端到网关。要使VPN连接正常工作，连接两端的IPSec值必须相同。此外，连接的两端必须属于不同的LAN。后续步骤说明如何在RV有线路由器系列上配置VPN。

在本文中，VPN配置将是网关到网关。

本文介绍如何在RV016 RV042、RV042G和RV082 VPN路由器上建立VPN隧道。

适用设备

·RV016
· RV042
· RV042G
· RV082

软件版本

•v4.2.1.02

VPN设置

步骤1.登录Web Configuration Utility页面，然后选择**VPN > Gateway to Gateway**。“网关*至网关*”页面打开：

注意：要配置客户端到网关VPN隧道，请选择**VPN > Client to Gateway**。

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	TestTunnel
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	156.26.31.119
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only
IP Address :	192.0.2.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 1 - 768 bit
Phase 1 Encryption :	DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☑
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5

步骤2.在Tunnel Name字段中，输入VPN隧道的名称。

步骤3.在Interface下拉列表中，选择一个可用的WAN接口。这是将与另一端建立VPN隧道的接口。

步骤4.在Local Group Setup（本地组设置）下，在Local Security Gateway Type下拉列表中，选择Listed（列出）选项之一：

·仅IP — 如果路由器配置了用于Internet连接的静态IP地址，请选择此选项。

·IP +域名(FQDN)身份验证 — 如果路由器配置了静态IP地址和用于Internet连接的注册域名，请选择此选项。

·IP +电子邮件地址（用户FQDN）身份验证 — 如果路由器配置了用于Internet连接的静态IP地址，并且将使用电子邮件地址进行身份验证，请选择此选项。

·动态IP +域名(FQDN)身份验证 — 如果路由器配置了动态IP地址，且将使用动态域名进行身份验证，请选择此选项。

·动态IP +邮件地址（用户FQDN）身份验证 — 如果路由器具有用于Internet连接的动态IP地址，但没有用于身份验证的动态域名，而将使用邮件地址进行身份验证，请选择此选项。

步骤5.在Local Group Setup（本地组设置）下，在Local Security Group Type下拉列表中，选择以下选项之一：

·IP Address — 此选项允许您指定一台可使用此VPN隧道的设备。您只需输入设备的IP地址。

·子网 — 选择此选项可允许属于同一子网的所有设备使用VPN隧道。您需要输入网络IP地址及其各自的子网掩码。

·IP Range — 选择此选项可指定可使用VPN隧道的设备范围。您需要输入设备范围的第一个IP地址和最后一个IP地址。

步骤6.在Remote Group Setup（远程组设置）下，在Remote Local Security Gateway Type（远程本地安全网关类型）下拉列表中，选择以下选项之一：

·仅IP — 如果路由器配置了用于Internet连接的静态IP地址，请选择此选项。

·IP +域名(FQDN)身份验证 — 如果路由器配置了静态IP地址和用于Internet连接的注册域名，请选择此选项。

·IP +电子邮件地址（用户FQDN）身份验证 — 如果路由器配置了用于Internet连接的静态IP地址，并且将使用电子邮件地址进行身份验证，请选择此选项。

·动态IP +域名(FQDN)身份验证 — 如果路由器配置了动态IP地址，且将使用动态域名进行身份验证，请选择此选项。

·动态IP +邮件地址（用户FQDN）身份验证 — 如果路由器具有用于Internet连接的动态IP地址，但没有用于身份验证的动态域名，而将使用邮件地址进行身份验证，请选择此选项。

步骤7.如果选择IP Only作为远程本地安全网关类型，请从下拉列表中选择以下选项之一：

·IP — 选择此选项以在相邻字段中输入IP地址。

·IP by DNS Resolved — 如果您不知道远程网关的IP地址，请选择此选项，然后在相邻字段

中输入另一台路由器的名称。

步骤8.在Remote Group Setup下，在Remote Security Group Type下拉列表中，选择以下选项之一：

·IP Address — 此选项允许您指定一台可使用此VPN隧道的设备。您只需输入设备的IP地址。

·子网 — 选择此选项可允许属于同一子网的所有设备使用VPN隧道。您需要输入网络IP地址及其各自的子网掩码。

·IP Range — 选择此选项可指定可使用VPN隧道的设备范围。您需要输入设备范围的第一个IP地址和最后一个IP地址。

步骤9.在IPSec Setup下，在Keying Mode下拉列表中，选择以下选项之一：

·手动 — 此选项允许您手动配置密钥，而不是与VPN连接中的其他路由器协商密钥。

·具有预共享密钥的IKE — 选择此选项以启用在VPN隧道中设置安全关联的互联网密钥交换协议(IKE)。IKE使用预共享密钥对远程对等体进行身份验证。

步骤 10DH(Diffie - Hellman)是允许VPN隧道两端共享加密密钥的密钥交换协议。在第1阶段DH组和第2阶段DH组下拉列表中，选择以下选项之一：

·组1 - 768位 — 提供更快的交换速度，但安全性较低。如果需要VPN会话快速且安全性不是问题，则选择此选项。

·组2 - 1024位 — 提供比组1更高的安全性，但处理时间更长。在安全性和速度方面，这是一个更加平衡的选项。

·组3 - 1536位 — 速度更慢，安全性更高。如果需要VPN会话安全且速度不是问题，则选择此选项。

步骤11.在第1阶段加密和第2阶段加密下拉列表中，选择以下选项之一来加密和解密密钥：

·DES — 数据加密标准，这是加密数据的基本算法，用于加密56位数据包中的密钥。

·3DES — 三重数据加密标准，此算法加密三个64位数据包中的密钥。它比DES更安全。

·AES-128 — 高级加密标准，此算法使用相同的密钥进行加密和解密。它提供比DES更高的安全性。其密钥大小为128位

·AES-192 — 类似于AES-128，但其密钥大小为192位。

·AES-256 — 类似于AES-128，但其密钥大小为256位。这是最安全的加密算法。

步骤12.在Phase 1 Authentication和Phase 2 Authentication下拉列表中，选择以下选项之一：

·SHA1 — 此算法生成160位的哈希值。使用此值，算法会检查交换的数据的完整性，并确保数据未更改。

·MD5 — 这是用于身份验证的算法设计。此算法检查VPN隧道两端之间共享信息的完整性。它生成一个哈希值，该哈希值用于对VPN隧道两端的密钥进行身份验证。

步骤13.在Phase 1 SA生存期和Phase 2 SA生存期字段中，输入VPN隧道在某个阶段处于活动状态的时间（以秒为单位）。第1阶段的默认值为28800秒。第2阶段的默认值为3600秒。

注意：两台路由器的第1阶段和第2阶段配置必须相同。

步骤14.（可选）选中Perfect Forward Secrecy**复选框**以启用完全向前保密(PFS)。 使用PFS时，IKE第2阶段协商将生成用于加密和身份验证的新数据，从而实施更高的安全性。

步骤15.在预共享密钥中，输入两台路由器将共享的密钥进行身份验证。

步骤16.（可选）选中**Minimum Preshared Key Complexity**复选框以启用Preshared Key Strength Meter，该计量器将告诉您所创建密钥的强度。

步骤17.（可选）要配置更高级的加密选项，请单击**Advanced+**。

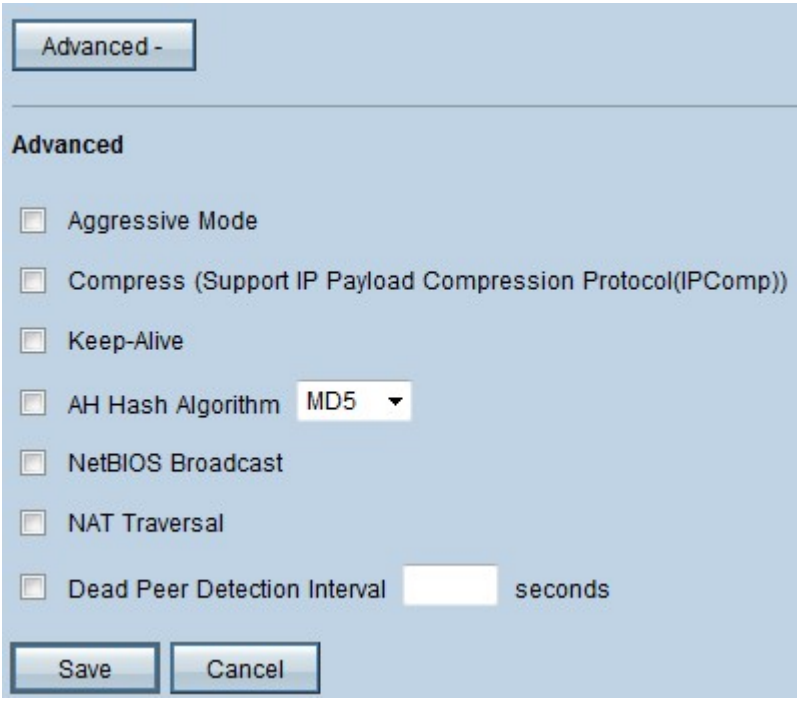
步骤18.单击“保**存”保存**配置。

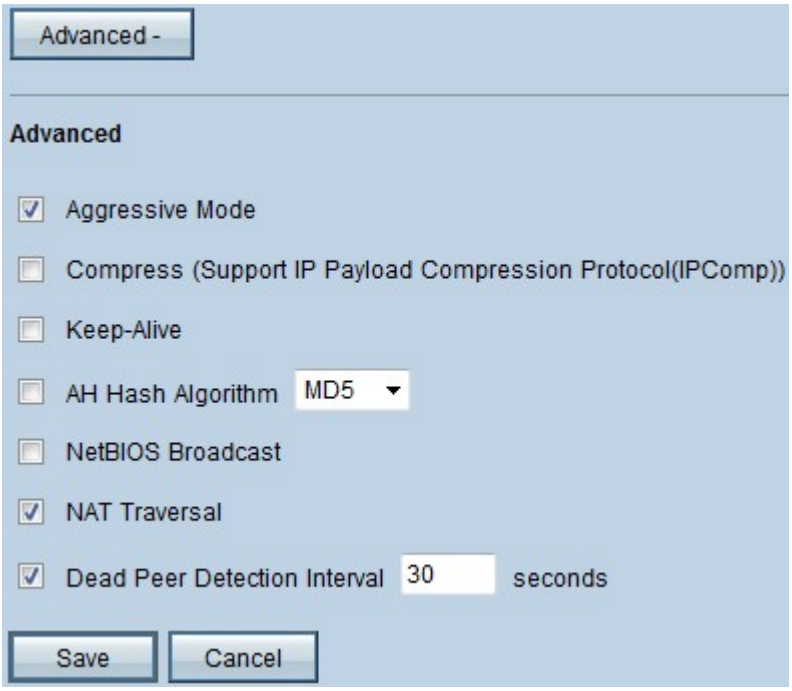
高级VPN选项

如果您想要为VPN设置添加更多功能，RV有线路由器系列提供高级选项。这些选项可增强VPN隧道的安全功能。这些选项是可选的，但如果您在一台路由器上设置了高级选项，请确保在另一台路由器上设置相同的选项。下一节将介绍这些选项。

步骤1.在IPSec字段中，单击“高**级+”**按钮。“高级”页面打开：

注意：要配置客户端到网关VPN隧道的高级选项，请选择**VPN > Client to Gateway**。然后单击**Advanced+**。





上图显示了高级选项的配置示例。

步骤2.在“高级”下，检查要添加到VPN设置的选项：

·主动模式 — 使用此选项，密钥协商更快，从而降低安全性。如果要提高VPN隧道的速度，请选中**Aggressive Mode**复选框。

·压缩(支持IP负载压缩协议（IP压缩协议）) — 使用此选项，IP压缩协议将减小IP数据报的大小。 选中**Compress(Support IP Payload Compression Protocol(IP Comp))(压缩(支持IP负载压缩协议（IP压缩）))**复选框以启用此选项

·保持连接 — 此选项尝试在VPN会话被丢弃时重新建立该会话。选中保**持连接**复选框以启用此选项。

·AH散列算法 — 此选项将保护扩展到IP报头，以验证整个数据包的完整性。MD5或SHA1均可用于此目的。选中**AH Hash Algorithm**复选框，从下拉列表中选择MD5或SHA1，以启用整个数据包的身份验证。

·NetBIOS广播 — 这是一种Windows协议，它提供有关插入LAN中的不同设备（如打印机、计算机和文件服务器）的信息。通常，VPN不传输此信息。选中**NetBIOS Broadcast**复选框以通过VPN隧道发送这些信息。

·NAT穿越 — 网络地址转换使私有LAN中的用户能够使用公有IP地址作为源地址访问互联网资源。如果路由器位于NAT网关后面，请选中**NAT Traversal**复选框。

·Dead Peer Detection Interval — 选中**Dead Peer Detection Interval**复选框，并输入（以秒为单位）路由器发送其他数据包以检查VPN隧道的连通性之前的间隔。

步骤3.单击“保**存**”保存配置。