在RV016、RV042、RV042G和RV082 VPN路由器的VPN隧道设置

客观

虚拟专用网络(VPN)是两个终端之间的一个安全连接。一个专用网络，那安全地发送数据在这两个位置之间或网络，由VPN隧道建立。VPN隧道连接两个人计算机或网络并且允许数据在互联网传输，好象终端在网络内。VPN是有员工必须经常传播或是在LAN外面的公司的一个好解决方案。使用VPN，这些员工能访问LAN和使用可用的资源做他们的工作。并且， VPN能连接两个或多个站点，因此用不同的分组的公司能与彼此联络。

Note:RV有线路由器系列为网关提供VPN，网关到网关和客户端的两种类型。为了VPN连接能适当地工作， IPSec值在连接的两边必须是相同的。此外，连接的两边必须属于不同的LAN。以下步骤解释如何配置在RV有线路由器系列的VPN。

为此条款的目的， VPN配置网关到网关。

此条款说明如何设置在RV016 RV042、RV042G和RV082 VPN路由器的一条VPN隧道。

可适用的设备

- RV016
- RV042
- RV042G
- RV082

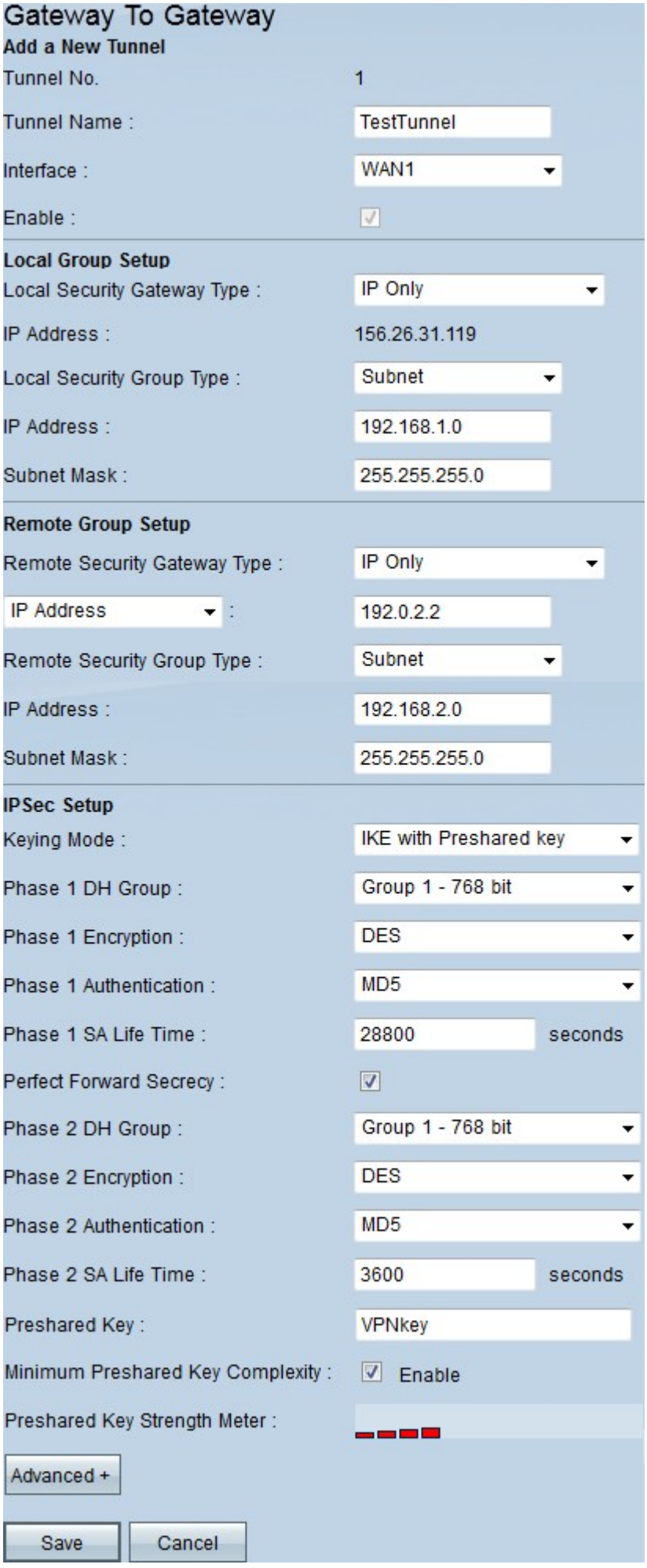
软件版本

- v4.2.1.02

VPN设置

步骤1.登陆对Web配置实用工具页并且选择**VPN >网关到网关**。*网关到网关的*页打开：

Note:要配置客户端到网关VPN隧道，请选择**VPN >客户端到网关**。


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
Phase 2 SA Life Time :
3600
seconds
Preshared Key :
VPNkey
Minimum Preshared Key Complexity :
Enable
Preshared Key Strength Meter :
Advanced +
Save
Cancel

Step 2.在隧道名字段，请输入VPN隧道的名字。

第 3 步：在接口下拉列表中，请选择其中一可用的广域网接口。这是将设立有另一边的VPN隧道的接口。

第 4 步：在本地组设置下，在本地安全网关类型下拉列表，请选择其中一种列表选项：

•仅IP —，如果您的路由器配置有互联网连通性的，一个静态IP地址请选择此选项。

•IP+域名(FQDN)认证—，如果您的路由器配置有一个静态IP地址和一个注册的域名互联网连通性的，请选择此选项。

•IP+电子邮件地址(用户FQDN)认证—请选择此选项，如果您的路由器配置有互联网连通性的一个静态IP地址，并且电子邮件地址将是认证的使用。

•动态IP+域名(FQDN)认证—请选择此选项，如果您的路由器配置有一个动态IP地址，并且一个动态域名将使用认证。

•动态IP+电子邮件地址(用户FQDN)认证—请选择此选项，如果您的路由器有互联网连通性的一个动态IP地址，但是没有认证的一个动态域名，并且电子邮件地址使用认证。

第 5 步：在本地组设置下，在安全组类型下拉列表，请选择其中一个选项：

•IP地址—此选项让您指定能使用此VPN隧道的一个设备。您只需要输入设备的IP地址。

•子网—选择此选项允许属于相同子网使用VPN隧道的所有设备。您需要输入网络IP地址和其各自子网掩码。

•IP范围—选择此选项指定能使用VPN隧道设备的范围。您需要输入第一个IP地址和设备的范围的最后IP地址。

第6.步。在远程组建立下，在远程本地安全网关类型下拉列表，请选择下列之一：

•仅IP —，如果您的路由器配置有互联网连通性的，一个静态IP地址请选择此选项。

•IP+域名(FQDN)认证—，如果您的路由器配置有一个静态IP地址和一个注册的域名互联网连通性的，请选择此选项。

•IP+电子邮件地址(用户FQDN)认证—请选择此选项，如果您的路由器配置有互联网连通性的一个静态IP地址，并且电子邮件地址将是认证的使用。

•动态IP+域名(FQDN)认证—请选择此选项，如果您的路由器配置有一个动态IP地址，并且一个动态域名将使用认证。

•动态IP+电子邮件地址(用户FQDN)认证—请选择此选项，如果您的路由器有互联网连通性的一个动态IP地址，但是没有认证的一个动态域名，并且电子邮件地址使用认证。

第 7 步：如果仅选择IP作为远程本地安全网关类型，从如下下拉列表请选择这些选项之一：

•IP —选择此选项输入IP地址在相邻字段。

•由被解决的DNS的IP —请选择此选项，如果不认识远程网关的IP地址，然后输入另一个路由器的名字在相邻字段。

第8.步。在远程组建立下，在远程安全组类型下拉列表，请选择下列之一：

•IP地址—此选项让您指定能使用此VPN隧道的一个设备。您只需要输入设备的IP地址。

•子网—选择此选项允许属于相同子网使用VPN隧道的所有设备。您需要输入网络IP地址和其各自子网掩码。

•IP范围—选择此选项指定能使用VPN隧道设备的范围。您需要输入第一个IP地址和设备的范围的最后IP地址。

第9.步。在IPSec设置下，在密钥模式下拉列表，请选择其中一个选项：

•手工—此选项让您手工配置键而不是协商键与在VPN连接的另一个路由器。

•IKE用预共用的键—选择此选项对enable (event)设置VPN隧道的一个安全关联的互联网密钥交换协议(IKE)。IKE使用一个预共用的键验证远端对等体。

步骤10. DH (Diffie-Hellman)是允许VPN隧道两端共享一个被加密的键的一个密钥交换协议。在阶段1 DH组和第2阶段DH组下拉列表，选择下列之一：

•Group1 - 768位—提供快速地交换速度，但是低安全。如果需要VPN会话快速，并且安全不是问题，则请选择此选项。

•第2组-第1024组位—比Group1提供更多安全，但是它有更多处理时间。这是一个更加平衡的选项根据安全和速度。

•Group3 - 1536位—提供较少速度，但是更多安全。如果需要VPN会话安全，并且速度不是问题，则选择此选项。

第11.步。在阶段1加密和第2阶段加密下拉列表中，请选择其中一以下键的加密和解密的：

•DES —数据加密标准，这是加密在一个56位信息包的键数据的加密的一个基本算法。

•3DES —三重数据加密标准，此算法加密在三64个位信息包的键。它比DES安全。

•AES-128 —高级加密标准，此算法使用同一个键加密和解密。它比DES提供更多安全。其密钥大小是128位

•AES-192 —类似于AES-128，但是其密钥大小192位。

•AES-256 —类似于AES-128，但是其密钥大小256位。这是可用最安全的加密算法。

步骤12。在阶段1认证和第2阶段认证下拉列表中，请选择这些选项之一：

•SHA1 —此算法导致160位的一个Hash值。使用此值，算法检查在被交换的数据的完整性，并且保证数据未更改。

•MD5 —这为认证的目的是算法设计。此算法检查共有的信息的完整性在VPN隧道之间的二末端的。它导致共享验证在VPN隧道的两端的键的一个Hash值。

第13步。在SA阶段1寿命和SA第2阶段寿命字段，请输入时间(以秒钟) VPN隧道是活跃的在阶段。DEFAULT值阶段1的是28800秒。DEFAULT值第2阶段的是3600秒。

Note:阶段1和第2阶段配置必须是相同的在两路由器。

步骤14。(可选)请检查**优秀的转发保密性**复选框对enable (event)完整转发安全性(PFS)。使用PFS， IKE第2阶段协商将生成新的数据为加密和认证，强制执行更多安全。

第15步。在预共用的键中，请输入两路由器为认证将共享的键。

第16步。(可选)请检查**最低的预共用的关键复杂性**复选框对enable (event)告诉您键力量您创

建的预共用的密钥强度公尺。

第17步。(可选)配置更多高级加密选项，请点击**Advanced+**。

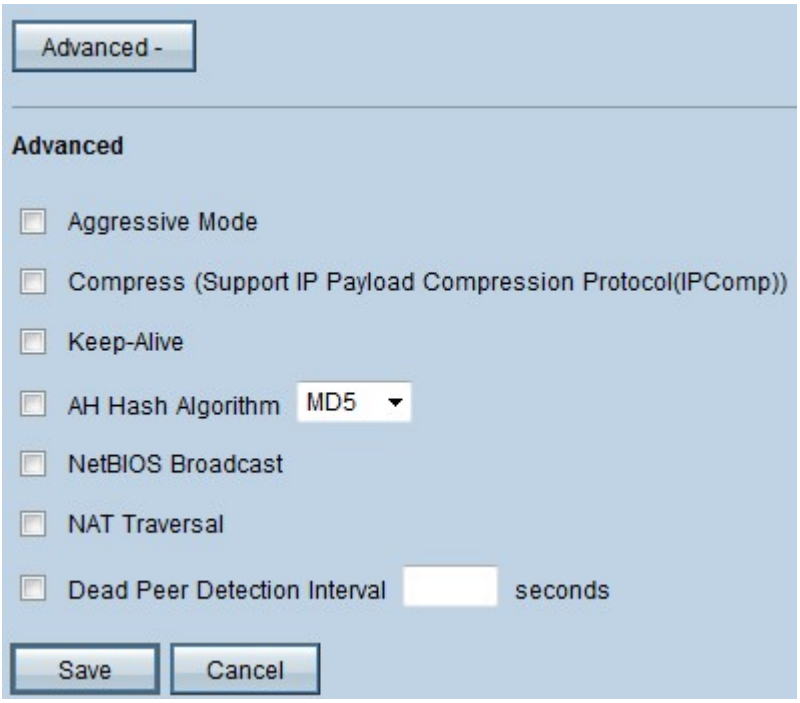
第18步。点击**“Save”保存**您的配置。

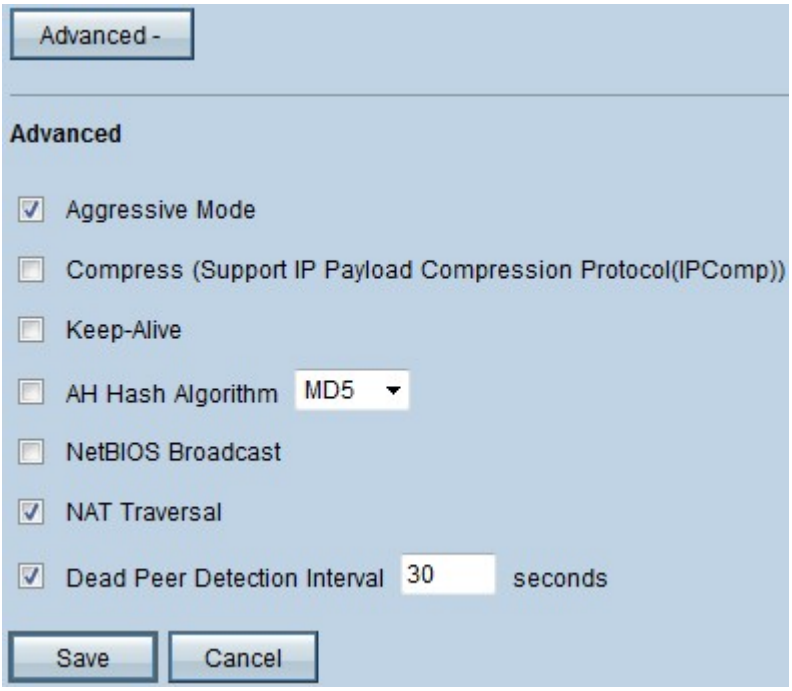
先进的VPN选项

如果要添加更多功能到您的VPN设置， RV有线路由器系列提供高级选项。这些选项提高您的VPN隧道安全功能。这些选项是可选的，但是，如果设置在一个路由器的高级选项，保证设置在另一个路由器的同样选项。下个部分说明这些选项。

第 1 步：在IPSec字段请点击**Advanced+**按钮。*Advanced页*打开：

Note:要配置客户端的高级选项到网关VPN隧道，请选择**VPN >客户端到网关**。然后请点击**Advanced+**。





以上的图片显示高级选项的配置的示例。

Step 2.在先进下，请检查您希望添加到您的VPN设置的选项：

•积极模式—使用此选项，键的协商更加快速，减少安全。如果要改进VPN隧道的速度请检查**积极模式**复选框。

• 压缩(支持IP有效负载压缩协议(IP Comp)) —与此选项， IP Comp协议将减少IP数据包的大小。 检查**压缩(支持IP有效负载压缩协议(IP Comp))**对enable (event)的复选框此选项

• 保活—，如果被撤销，此选项尝试重建VPN会话。检查**保活**复选框对enable (event)此选项。

•AH Hash算法—此选项对IP头扩大保护验证整个数据包的完整性。可以为此使用MD5或SHA1。检查**AH Hash算法**复选框和从下拉列表，选择MD5或SHA1，对整个数据包的启用认证。

• NetBIOS广播—这是提供关于不同的设备的信息接通LAN，例如打印机、计算机和文件服务器的Windows协议。通常， VPN不传播此信息。检查**NetBIOS广播**复选框发送这些在VPN隧道间的信息。

•NAT横越—网络地址转换访问与使用的互联网资源的专用LAN的enable (event)用户一个公共IP地址作为源地址。如果您的路由器是在NAT网关后，请检查**NAT横越**复选框。

• 对端死机检测间隔—检查**对端死机检测间隔**复选框并且输入(以秒钟)间隔，在路由器发送另一个信息包检查VPN隧道的连接前。

步骤3.点击**"Save"**保存您的配置。