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)是两个端点之间的安全连接。在这两个位置或网络之间安全地发送数据的专用网络由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传输在互联网，好象端点就在网络内。对于员工经常需要出差或离开LAN的公司来说，VPN是一个不错的解决方案。通过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，因此具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类型的VPN：网关到网关和客户端到网关。为了使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。接下来的步骤将介绍如何在RV有线路由器系列上配置VPN。

为本文的目的，VPN配置将是Gateway to Gateway。

本文解释如何在RV016 RV042、RV042G和RV082 VPN路由器上设置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:登录到Web Configuration Utility页面，然后选择VPN > Gateway to Gateway。Gateway to Gateway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

第二步：在Tunnel Name字段中，输入VPN隧道的名称。

第三步：在Interface下拉列表中，选择其中一个可用的WAN接口。这是将与另一端建立VPN隧道的接口。

第四步：在Local Group Setup下的Local Security Gateway Type下拉列表中，选择下列选项之一：

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

· IP +域名(FQDN)身份验证 — 如果您的路由器配置了静态IP地址和注册域名以实现Internet连接，请选择此选项。

· IP +邮件地址（用户FQDN）身份验证 — 如果您的路由器配置了用于Internet连接的静态IP地址，并且邮件地址将用于身份验证，请选择此选项。

·动态IP +域名(FQDN)身份验证 — 如果您的路由器配置了动态IP地址，并且动态域名将用于身份验证，请选择此选项。

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

第五步：在Local Group Setup下的Local Security Group Type下拉列表中，选择以下选项之一：

· IP地址 — 通过此选项，可以指定一个可以使用此VPN隧道的设备。您只需要输入设备的IP地址。

·子网 — 选择此选项以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范围 — 选择此选项可指定可以使用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。

第六步：在Remote Group Setup下的Remote Local Security Gateway Type下拉列表中，选择以下选项之一：

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

· IP +域名(FQDN)身份验证 — 如果您的路由器配置了静态IP地址和注册域名以实现Internet连接，请选择此选项。

· IP +邮件地址（用户FQDN）身份验证 — 如果您的路由器配置了用于Internet连接的静态IP地址，并且邮件地址将用于身份验证，请选择此选项。

·动态IP +域名(FQDN)身份验证 — 如果您的路由器配置了动态IP地址，并且动态域名将用于身份验证，请选择此选项。

·动态IP +邮件地址（用户FQDN）身份验证 — 如果您的路由器具有用于Internet连接的动态IP地址，但没有用于身份验证的动态域名，并且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，请从下面的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其他路由器的名称。

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

· IP地址 — 通过此选项，可以指定一个可以使用此VPN隧道的设备。您只需要输入设备的IP地址。

·子网 — 选择此选项以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范围 — 选择此选项可指定可以使用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下的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。

· IKE with Preshared Key — 选择此选项以启用Internet密钥交换协议(IKE)，该协议在VPN隧道中设置安全关联。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Phase 1 DH Group和Phase 2 DH Group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，但安全性更低。如果您需要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，但它的处理时间更长。在安全性和速度方面，这是一个更平衡的选择。

·组3 - 1536位 — 速度较慢，但安全性较高。如果您需要VPN会话是安全的，并且速度不是问题，则选择此选项。

步骤 11在Phase 1 Encryption和Phase 2 Encryption下拉列表中，为密钥的加密和解密选择以下选项之一：

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

· 3DES — 三重数据加密标准，该算法将密钥加密为三个64位数据包。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。它比DES提供更高的安全性。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 — 此算法产生160位的散列值。使用此值，算法将检查所交换数据的完整性，并确保数据未发生更改。

· 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，该值被共享以对VPN隧道两端的密钥进行身份验证。

步骤 13在Phase 1 SA Lifetime和Phase 2 SA Lifetime字段中，输入VPN隧道在某个阶段中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：两台路由器上的第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，IKE第2阶段协商将生成用于加密和身份验证的新数据，从而增强安全性。

步骤 15在Preshared Key中，输入两台路由器将共享用于身份验证的密钥。

步骤16.（可选）选中Minimum Preshared Key Complexity复选框，以启用Preshared Key Strength Meter，它告诉您创建的密钥的强度。

步骤17.（可选）要配置更多高级加密选项，请点击Advanced+。

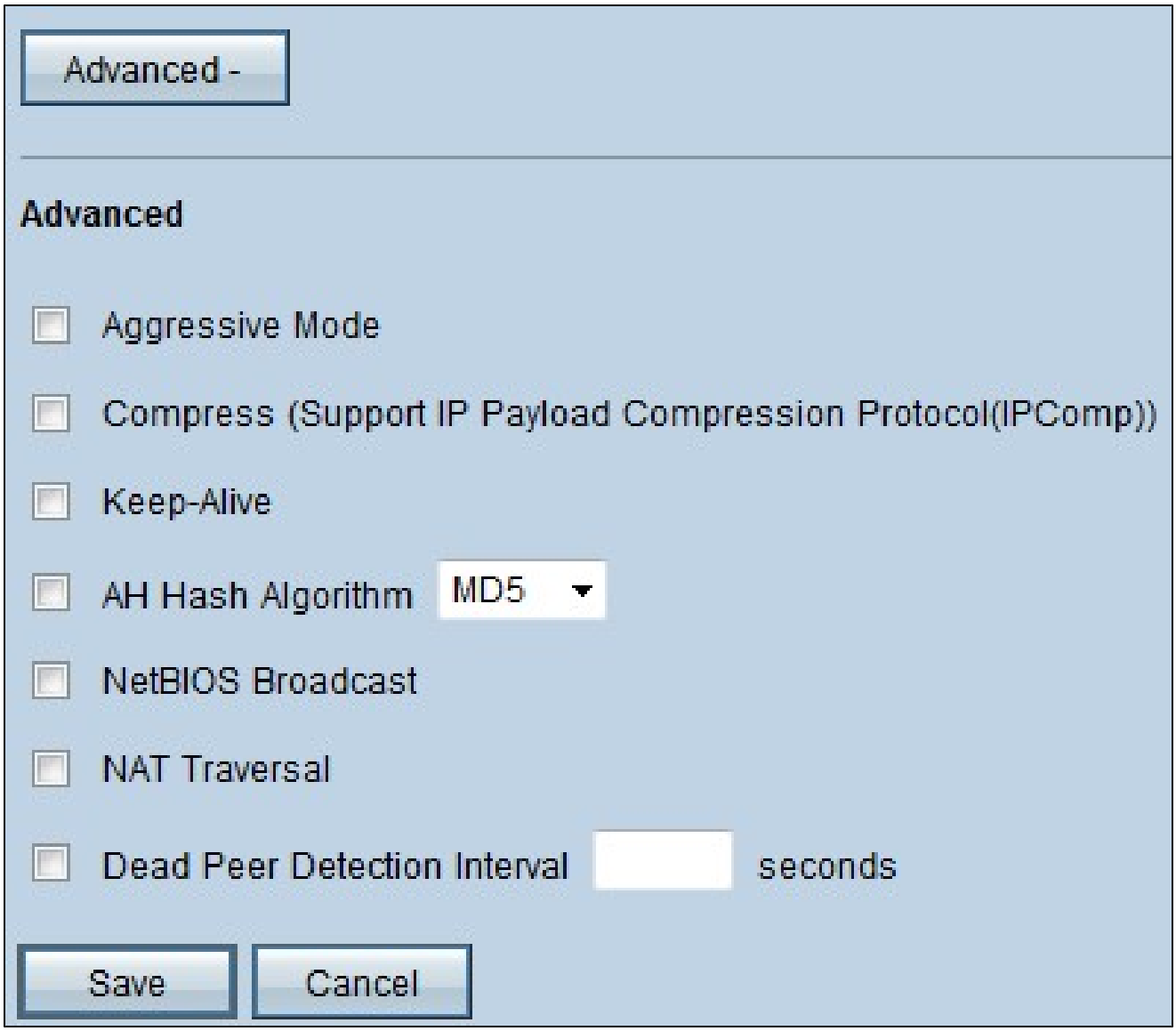
步骤 18.单击Save保存配置。

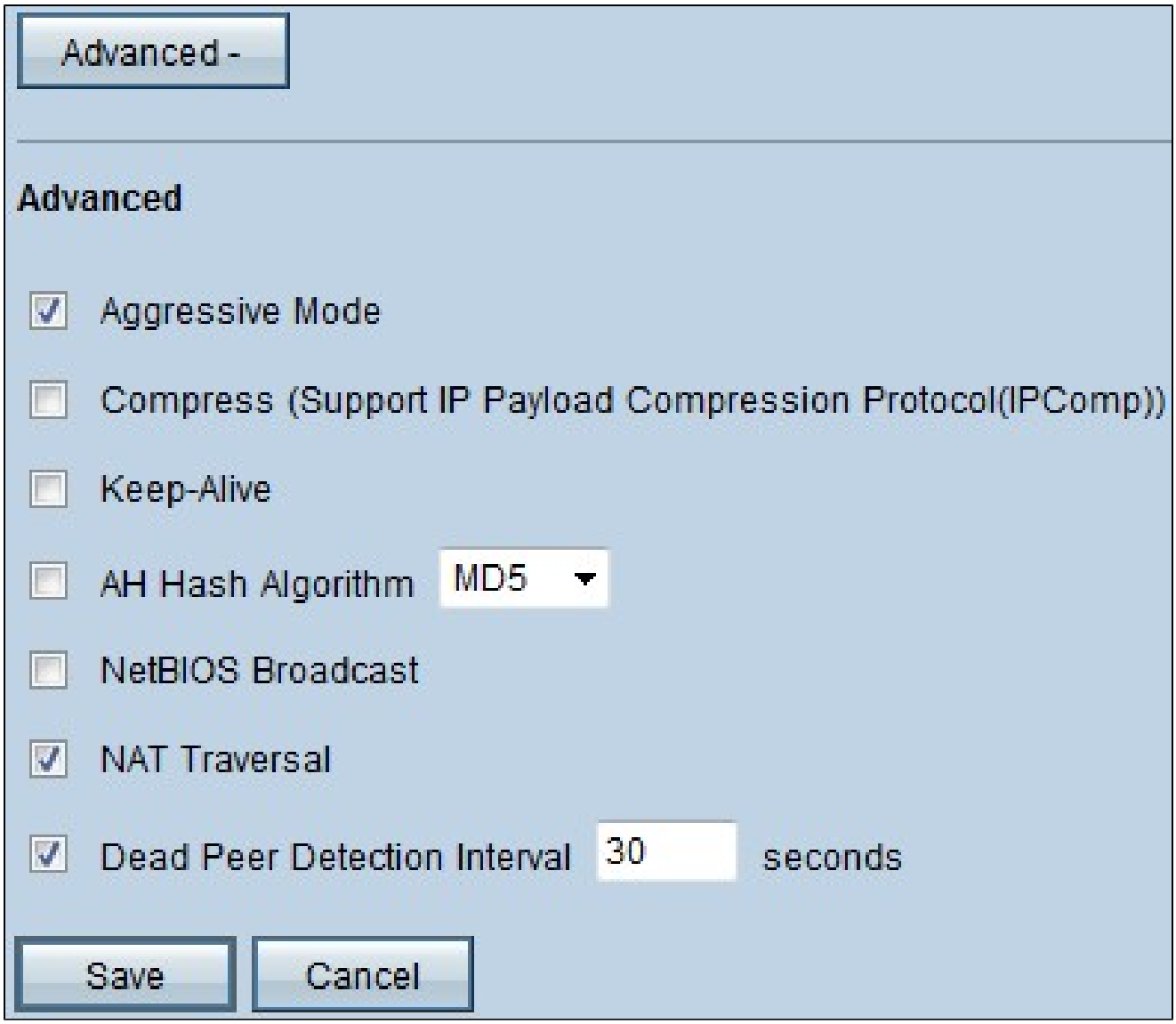
高级VPN选项

如果您希望在VPN设置中添加更多功能，RV有线路由器系列可提供高级选项。这些选项增强了VPN隧道的安全功能。这些选项是可选的，但如果您在一个路由器上设置高级选项，请确保在另一个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Advanced+按钮。将打开Advanced页面：

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+。


Advanced -
Advanced
Aggressive Mode
Compress (Support IP Payload Compression Protocol(IPComp))
Keep-Alive
AH Hash Algorithm
MD5
NetBIOS Broadcast
NAT Traversal
Dead Peer Detection Interval
seconds
Save
Cancel



上图显示了高级选项的配置示例。

第二步：在Advanced下，选中要添加到VPN设置的选项：

·主动模式 — 使用此选项时，密钥协商速度更快，从而降低安全性。如果要提高VPN隧道的速度，请选中主动模式复选框。

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

·保持连接 — 此选项尝试重新建立VPN会话（如果它被丢弃）。选中Keep Alive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都

可用于此目的。选中AH Hash Algorithm复选框，然后从下拉列表中选择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，提供插入LAN的不同设备（如打印机、计算机和文件服务器）的相关信息。通常，VPN不会传输此信息。选中NetBIOS Broadcast复选框以通过VPN隧道发送这些信息。

· NAT穿越 — 网络地址转换使专用LAN中的用户可以使用公有IP地址作为源地址来访问Internet资源。如果路由器位于NAT网关之后，请选中NAT Traversal复选框。

· Dead Peer Detection Interval — 选中Dead Peer Detection Interval复选框，并输入路由器发送其他数据包以检查VPN隧道连接之前的时间间隔（以秒为单位）。

第三步：单击Save保存配置。

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）。

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）。