RV320和RV325 VPN路由器系列上的网关到网关虚拟专用网络(VPN)配置

目标

VPN用于通过公共或共享互联网通过称为VPN隧道的两个终端形成非常安全的连接。更具体地说，网关到网关VPN连接允许两台路由器安全地彼此连接，并且一端的客户端在逻辑上看起来是另一端同一远程网络的一部分。这使数据和资源能够更轻松、更安全地通过互联网共享。必须在连接的两端进行配置，才能成功建立网关到网关VPN连接。本文的目的是指导您在RV32x VPN路由器系列上配置网关到网关VPN连接。

适用设备

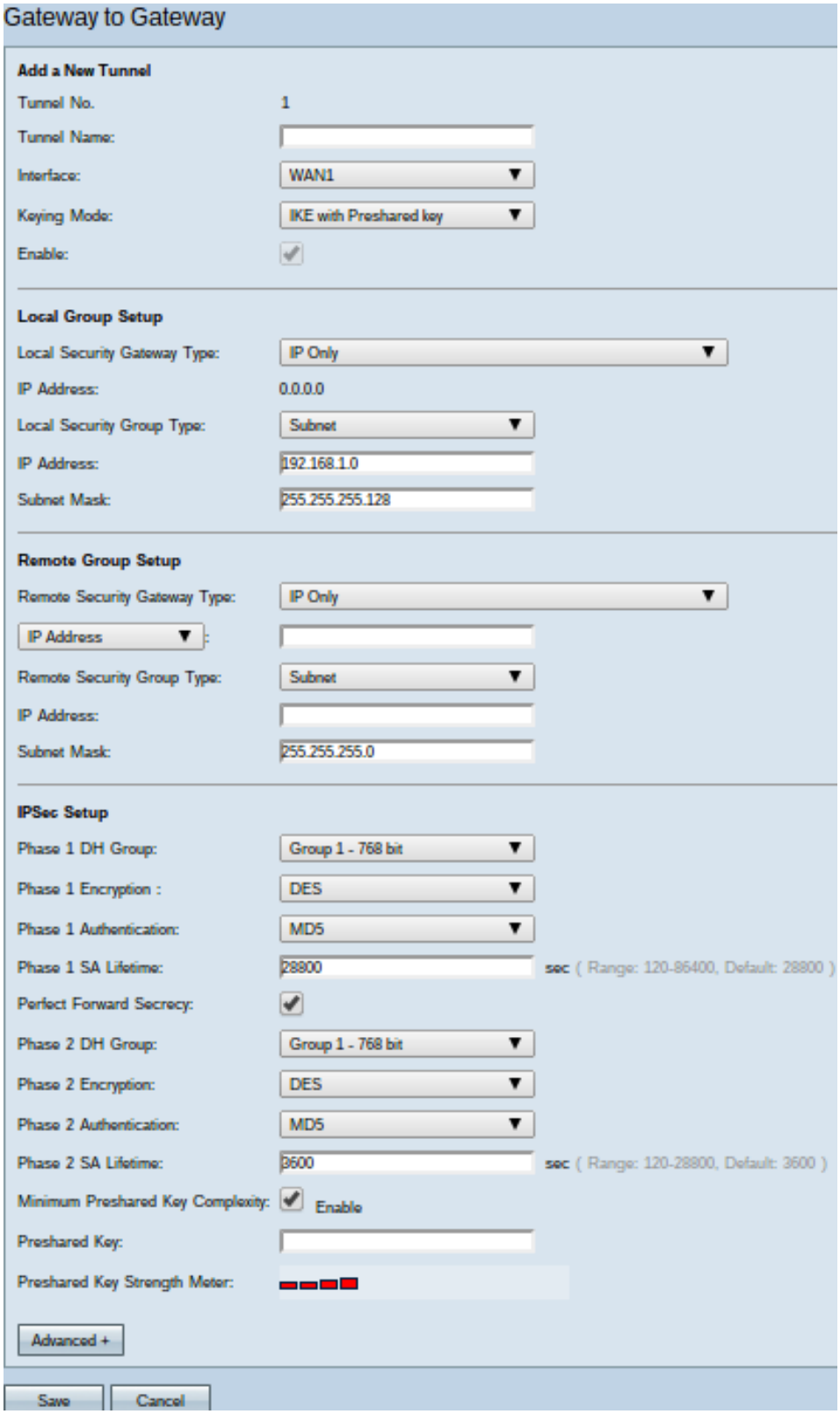
·RV320双WAN VPN路由器
· RV325千兆双WAN VPN路由器

软件版本

•v1.1.0.09

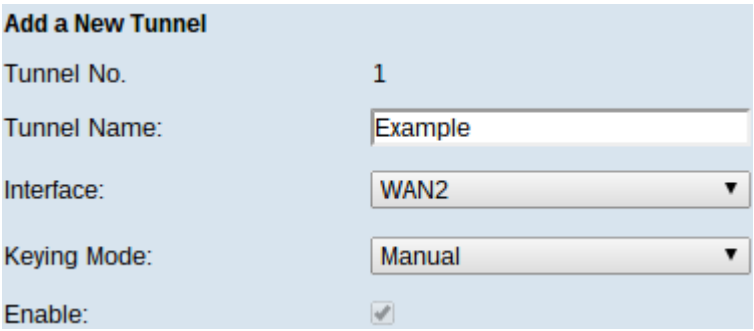
网关到网关

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



为使VPN连接正常工作，连接两端的Internet协议安全(IPSec)值必须相同。连接的两端必须属于不同的局域网(LAN)，并且至少有一台路由器可以通过静态IP地址或动态DNS主机名来识别。

添加新隧道



·隧道编号 — 显示将要创建的当前隧道。路由器支持100个隧道。

步骤1.在Tunnel Name字段中输入VPN隧道的名称。它不必与隧道另一端使用的名称匹配。

步骤2.从Interface下拉列表中选择用于隧道的广域网(WAN)端口。

·WAN1 — 路由器的专用WAN端口。

·WAN2 — 路由器的WAN2/DMZ端口。仅当配置为WAN而非非军事化区域(DMZ)端口时，才会显示在下拉菜单中。

·USB1 — 路由器的USB1端口。只有在端口上连接了3G/4G/LTE USB转换器时才能正常工作。

·USB2 — 路由器的USB2端口。只有在端口上连接了3G/4G/LTE USB转换器时才能正常工作。

步骤3.从Keying Mode下拉列表中选择要使用的隧道安全。

·手动 — 此选项允许您手动配置密钥，而不是与VPN连接的另一端协商密钥。

·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。

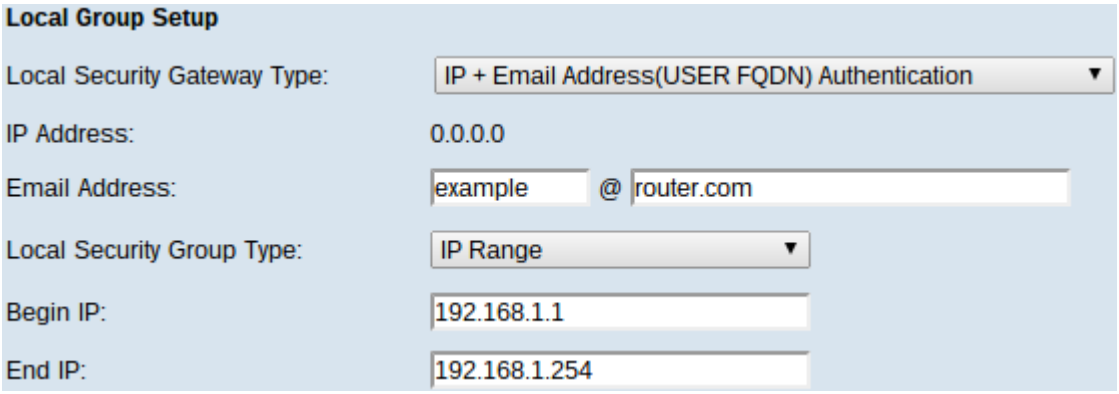
·带证书的IKE — 选择此选项可启用带证书的互联网密钥交换(IKE)协议，该协议提供更安全的方法来自动生成和交换预共享密钥，以便为隧道建立更经过身份验证和安全的通信。

步骤4.选中Enable复选框以启用VPN隧道。默认情况下，它处于启用状态。

本地组设置

这些设置应与VPN隧道另一端路由器的“远程组设置”设置匹配。

注意：如果从步骤1的步骤3的“添加新隧道”步骤3的“键控模式”下拉列表中选择了手动或预共享密钥的IKE，并跳过步骤2到4。如果选择了带证书的IKE，则跳过步骤1。



步骤1.从Local Security Gateway Type下拉列表中，选择标识路由器以建立VPN隧道的方法。

·仅IP — 只能通过静态WAN IP访问隧道。如果路由器有任何静态WAN IP，则可以选择此选项。静态 WAN IP 地址是自动生成的字段。

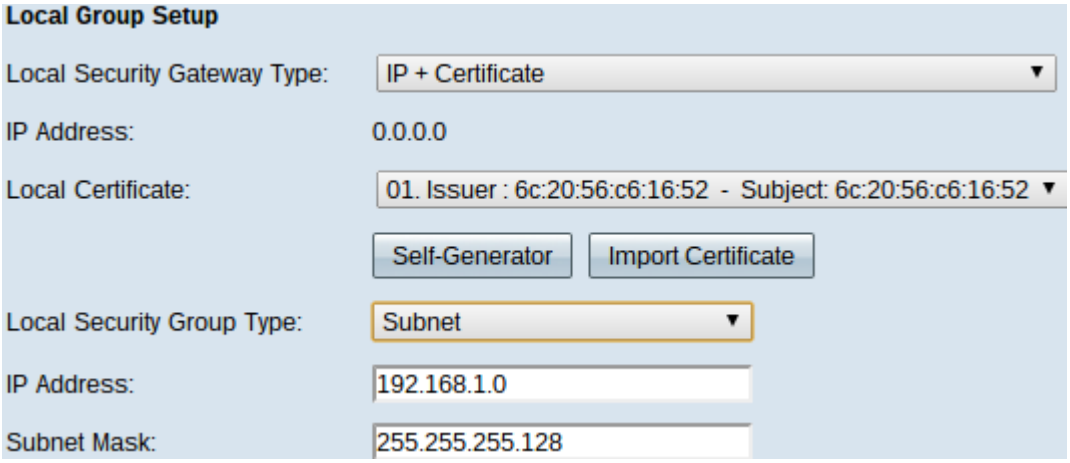
·IP +域名(FQDN)身份验证 — 可通过静态IP地址和注册域访问隧道。如果选择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。静态 WAN IP 地址是自动生成的字段。

·IP +电子邮件地址（用户FQDN）身份验证 — 可通过静态IP地址和电子邮件地址访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。静态 WAN IP 地址是自动生成的字段。

·动态IP +域名(FQDN)身份验证 — 可通过动态IP地址和注册域访问隧道。如果选择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。

·动态IP +邮件地址（用户FQDN）身份验证 — 可通过动态IP地址和邮件地址访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。

注意：使用IKE和证书时，本地组设置区域的以下更改会发生更改。



本地安全网关类型(Local Security Gateway Type)下拉列表变为不可编辑，并显示IP +证书(IP + Certificate)。这是可以使用隧道的LAN资源。
IP Address字段显示设备的WAN IP地址。用户不可编辑。

步骤2.从Local Certificate下拉列表中选择证书。证书在VPN连接上提供更强的身份验证安全。

步骤3.（可选）单击Self-Generator**按钮，显**示Certificate Generator窗*口，以*配置和生成证书。

第4步。（可选）单击“导入证**书”按**钮以显示“*我的证*书”窗口，以查看和配置证书。

步骤5.从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。您只需在IP地址字段中输入设备的IP地址。

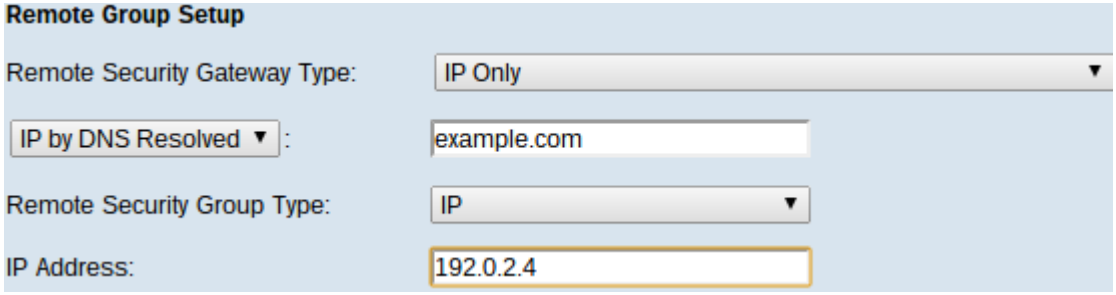
·子网 — 选择此选项可允许属于同一子网的所有设备使用VPN隧道。您需要在IP Address字段中输入网络IP地址，在Subnet Mask字段中输入相应的子网掩码。

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

远程组设置

这些设置应与VPN隧道另一端路由器的“本地组设置”设置匹配。

注意：如果从步骤1的“添加新隧道”步骤3的“键控模式”下拉列表中选择了手动或预共享密钥的IKE，并跳过步骤2到5。或者，如果选择了带证书的IKE，则跳过步骤1。



步骤1.从Remote Security Gateway Type下拉列表中，选择确定另一路由器以建立VPN隧道的方法。

·仅IP — 只能通过静态WAN IP访问隧道。如果知道远程路由器的IP地址，请在Remote Security Gateway Type字段正下方的下拉列表中选择IP地址并输入地址。如果您不知道IP地址但知道域名，并在IP by DNS Resolved字段中输入路由器的域名，请选择IP by DNS Resolved。

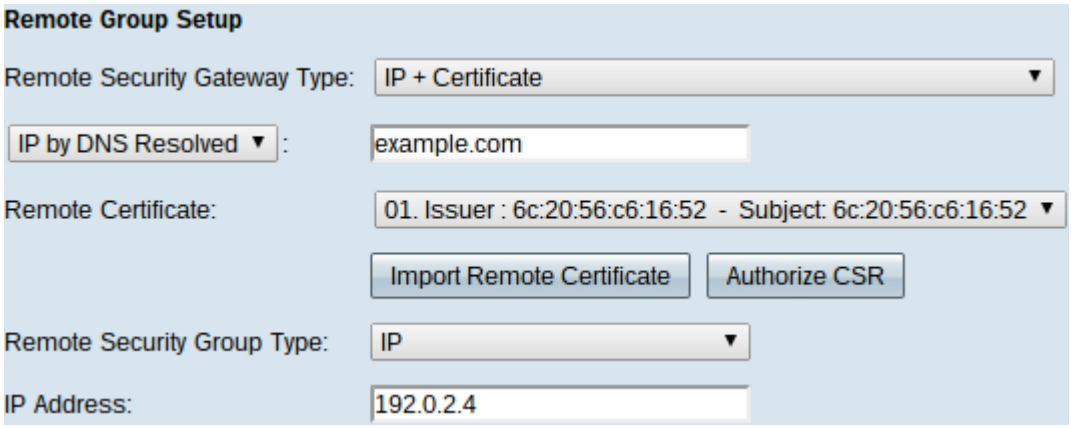
·IP +域名(FQDN)身份验证 — 可通过静态IP地址和路由器的注册域访问隧道。如果知道远程路由器的IP地址，请在Remote Security Gateway Type字段正下方的下拉列表中选择IP地址并输入地址。如果您不知道IP地址但知道域名，并在IP by DNS Resolved字段中输入路由器的域名，请选择IP by DNS Resolved。如果选择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。

·IP +邮件地址(USER FQDN)身份验证 — 可以通过静态IP地址和邮件地址访问隧道。如果知道远程路由器的IP地址，请在Remote Security Gateway Type字段正下方的下拉列表中选择IP地址，然后输入地址。如果您不知道IP地址但知道域名，并在IP by DNS Resolved字段中输入路由器的域名，请选择IP by DNS Resolved。在电子邮件地址字段中输入电子邮件地址。

·动态IP +域名(FQDN)身份验证 — 可通过动态IP地址和注册域访问隧道。如果选择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。

·动态IP +邮件地址（用户FQDN）身份验证 — 可通过动态IP地址和邮件地址访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。
注意：如果两台路由器都有动态IP地址，请勿为两个网关选择动态IP +邮件地址。

注意：使用IKE和证书时，远程组设置区域的以下更改会更改。



“远程安全网关类型”(Remote Security Gateway Type)下拉列表变为不可编辑，并显示IP +证书(IP + Certificate)。这是可以使用隧道的LAN资源。

步骤2.如果您知道远程路由器的IP地址，请在Remote Security Gateway Type字段正下方的下拉列表中选择IP地址并输入地址。如果您不知道IP地址但知道域名，并在IP by DNS Resolved字段中输入远程路由器的域名，请选择IP by DNS Resolved

步骤3.从Remote Certificate下拉列表中选择证书。证书在VPN连接上提供更强的身份验证安全。

步骤4.（可选）单击Import Remote Certificate**按钮以**导入新证书。

第5步。（可选）单击Authorize CSR**按钮**，用数字签名请求标识证书。

步骤6.从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。您只需在IP地址字段中输入设备的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。您需要在IP Address字段中输入网络IP地址，在Subnet Mask字段中输入相应的子网掩码。

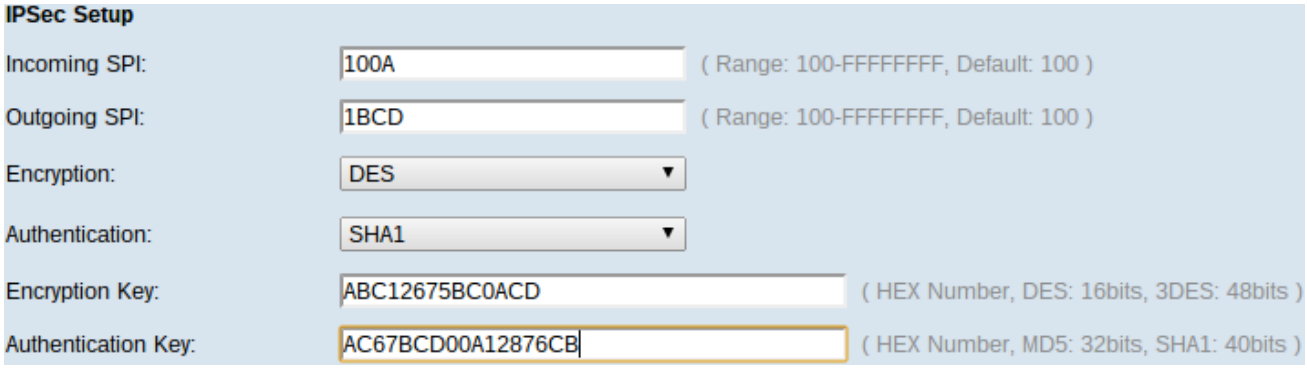
·IP Range — 选择此选项可指定可使用VPN隧道的设备范围。您需要输入设备范围的第一个IP地址和最后一个IP地址。在Begin IP（开始IP）字段和End IP字段中。

IPSec 设置选项

要在VPN隧道两端之间正确设置加密，它们必须具有完全相同的设置。在这种情况下，IPSec会在两台设备之间创建安全身份验证。它分两个阶段完成。

手动键控模式的IPSec设置

仅当从Step 3 of Add a New Tunnel（添加新隧道的步骤3）的Keying Mode（键控模式）下拉列表中选择Manual（手动）时才可用。这是自定义安全模式，可自行生成新安全密钥，不与密钥协商。最好在故障排除和小型静态环境中使用。



第 1 步： 在 Incoming SPI（传入 SPI）字段中，输入传入安全参数索引 (SPI) 的唯一十六进制值。SPI在封装安全负载(ESP)协议报头中传输，这些报头共同确定对传入数据包的保护。您可以输入 100 到 ffffffff。

步骤2.在Outgoing SPI字段中输入SPI的唯一十六进制值。SPI在ESP报头中传输，这些报头共同决定对传出数据包的保护。您可以输入 100 到 ffffffff。

注意：传入和传出SPI应在两端相匹配，以建立隧道。

步骤3.从Encryption下拉列表中选择适当的加密方法。推荐的加密方法为 3DES。VPN 隧道的两端需要使用相同的加密方法。

·DES - DES（数据加密标准）是一种56位旧的、更向后兼容的加密方法，其安全性不如易被破解。

·3DES - 3DES（三重数据加密标准）是168位的简单加密方法，通过加密数据三次来增加密钥大小，比DES更安全。

步骤4.从Authentication下拉列表中选择适当的身份验证方法。建议的身份验证是SHA1。VPN隧道两端需要使用相同的身份验证方法。

·MD5 - MD5（消息摘要算法–5）表示32位十六进制哈希函数，通过校验和计算保护数据免受恶意攻击。

·SHA1 — SHA1（安全散列算法版本1）是160位散列函数，比MD5更安全。

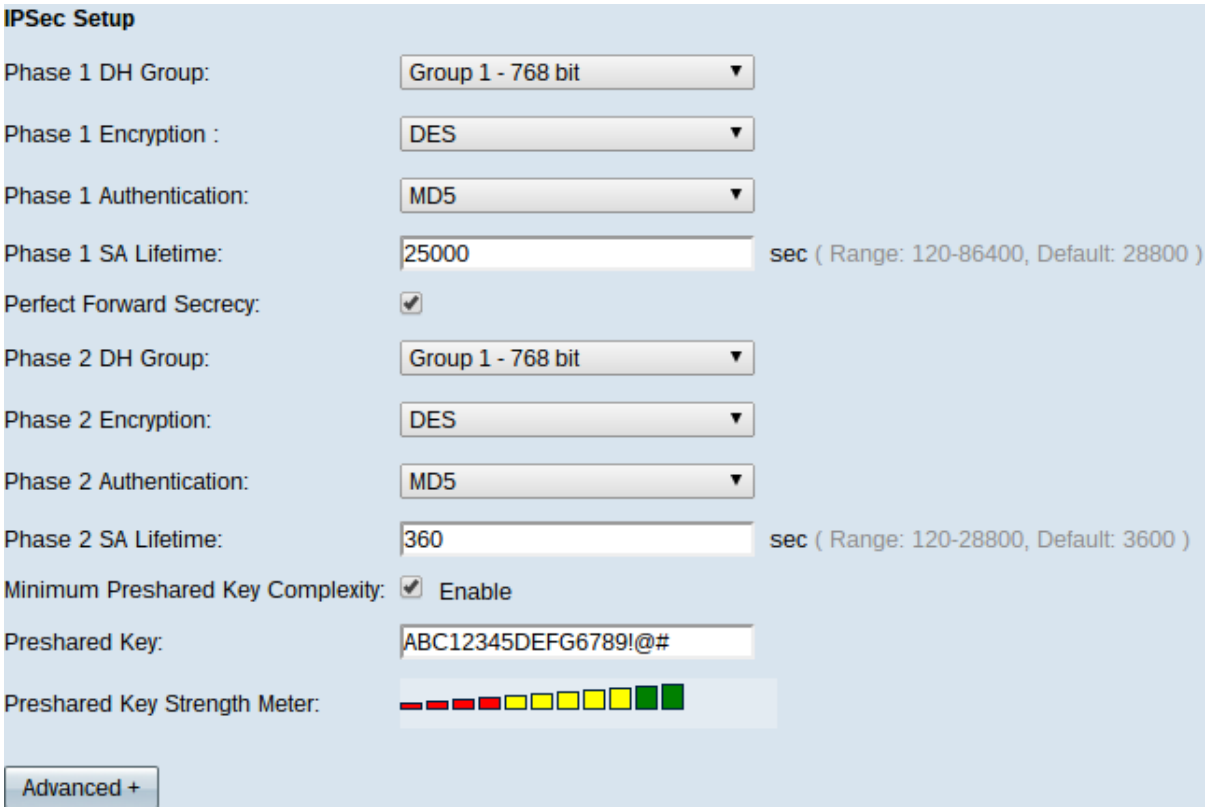
第 5 步： 在 Encryption Key（加密密钥）字段中输入密钥，以加密和解密数据。如果您在第 3 步中选择 DES 作为加密方法，请输入 16 位十六进制值。如果您在第 3 步中选择 3DES 作为加密方法，请输入 40 位十六进制值。

步骤6.在Authentication Key字段中输入预共享密钥以验证流量。如果在步骤4中选择MD5作为身份验证方法，请输入32位十六进制值。如果在步骤4中选择SHA作为身份验证方法，请输入40位十六进制值。VPN 隧道的两端需要使用相同的预共享密钥。

第 7 步： 点击 **Save（保存），以保存设置。**

使用预共享密钥的IKE的IPSec设置

仅当从Add a New Tunnel的Step 3的Keying Mode下拉列表中选择了带预共享密钥的IKE时，才可用。



第 1 步： 从 Phase 1 DH Group（第 1 阶段 DH 组）下拉列表中选择适当的第 1 阶段 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(DH)是密码密钥交换协议，在第1阶段连接期间用于共享密钥以验证通信。

·组1 - 768位 — 表示最高强度的密钥和最安全的身份验证组。它需要更多时间来计算 IKE 密钥。如果网络速度较快，则首选此选项。

·组2 - 1024位 — 表示更高强度的密钥和更安全的身份验证组。计算IKE密钥需要一些时间。

·组5 - 1536位 — 表示强度最低的密钥和最不安全的身份验证组。计算IKE密钥所需的时间更少。如果网络速度较慢，则首选此选项。

步骤2.从Phase 1 Encryption下拉列表中选择适当的Phase 1 Encryption以加密密钥。建议使用AES-128、AES-192或AES-256。VPN 隧道的两端需要使用相同的加密方法。

·DES — 数据加密标准(DES)是56位旧式加密方法，在当今世界，这种加密方法并不十分安全。

·3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，通过对数据进行三次加密来增加密钥大小，比DES提供更高的安全性。

·AES-128 — 高级加密标准(AES)是128位加密方法，通过10次循环重复将纯文本转换为密文。

·AES-192 — 是192位加密方法，通过12次循环重复将纯文本转换为密文。

·AES-256 — 是一种256位加密方法，通过14次循环重复将纯文本转换为密文。

步骤3.从Phase 1 Authentication下拉列表中选择适当的身份验证方法。VPN 隧道的两端需要使用相同的身份验证方法。建议使用SHA1。

·MD5 — 消息摘要算法5(MD5)表示32位十六进制哈希函数，通过校验和计算保护数据免受恶意攻击。

·SHA1 — 比MD5更安全的160位哈希函数。

步骤4.在Phase 1 SA Life Time字段中输入VPN隧道保持活动状态的时间量（以秒为单位）。

步骤5.选中Perfect Forward Secrecy复选框，为密钥提供更多保护。此选项允许在任何密钥被破坏时生成新密钥。加密的数据只会通过被盗取的密钥泄露。因此，它可提供更安全的通信并对其进行身份验证，其原因在于即使一个密钥被盗取，它也能保护其他密钥。推荐采取此操作，因为它可以提供更高的安全性。

步骤6.从第2阶段DH组下拉列表中选择适当的第2阶段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。DH是在第1阶段连接期间用于共享密钥以验证通信的加密密钥交换协议。

·组1 - 768位 — 表示最高强度的密钥和最安全的身份验证组。它需要更多时间来计算 IKE 密钥。如果网络速度较快，则首选此选项。

·组2 - 1024位 — 表示更高强度的密钥和更安全的身份验证组。 计算IKE密钥需要一些时间。

·组5 - 1536位 — 表示强度最低的密钥和最不安全的身份验证组。计算IKE密钥所需的时间更少。如果网络速度较慢，则首选此选项。

注意：由于未生成任何新密钥，因此如果在步骤5中取消选中完全向前保密，则无需配置第2阶段DH组。

第 7 步： 从 Phase 2 Encryption（第 2 阶段加密）下拉列表中选择适当的第 2 阶段加密来加密密钥。建议使用AES-128、AES-192或AES-256。VPN 隧道的两端需要使用相同的加密方法。

·DES - DES是56位旧式加密方法，在当今世界，这种加密方法并不十分安全。

·3DES - 3DES是一种168位的简单加密方法，通过加密数据三次来增加密钥大小，比DES提供更高的安全性。

·AES-128 - AES是128位加密方法，通过10次循环重复将纯文本转换为密文。

·AES-192 — 是192位加密方法，通过12次循环重复将纯文本转换为密文。

·AES-256 — 是一种256位加密方法，通过14次循环重复将纯文本转换为密文。

第 8 步： 从 Phase 2 Authentication（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 隧道的两端需要使用相同的身份验证方法。

·MD5 - MD5表示32位十六进制哈希函数，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。

·空 — 不使用身份验证方法。

步骤9.在Phase 2 SA Life Time字段中输入VPN隧道保持活动状态的时间（以秒为单位）。

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

步骤11.在预共享密钥(Preshared Key)字段中输入之前在IKE对等体之间共享的密钥。最多30个十六进制和字符可用作预共享密钥。VPN 隧道的两端需要使用相同的预共享密钥。

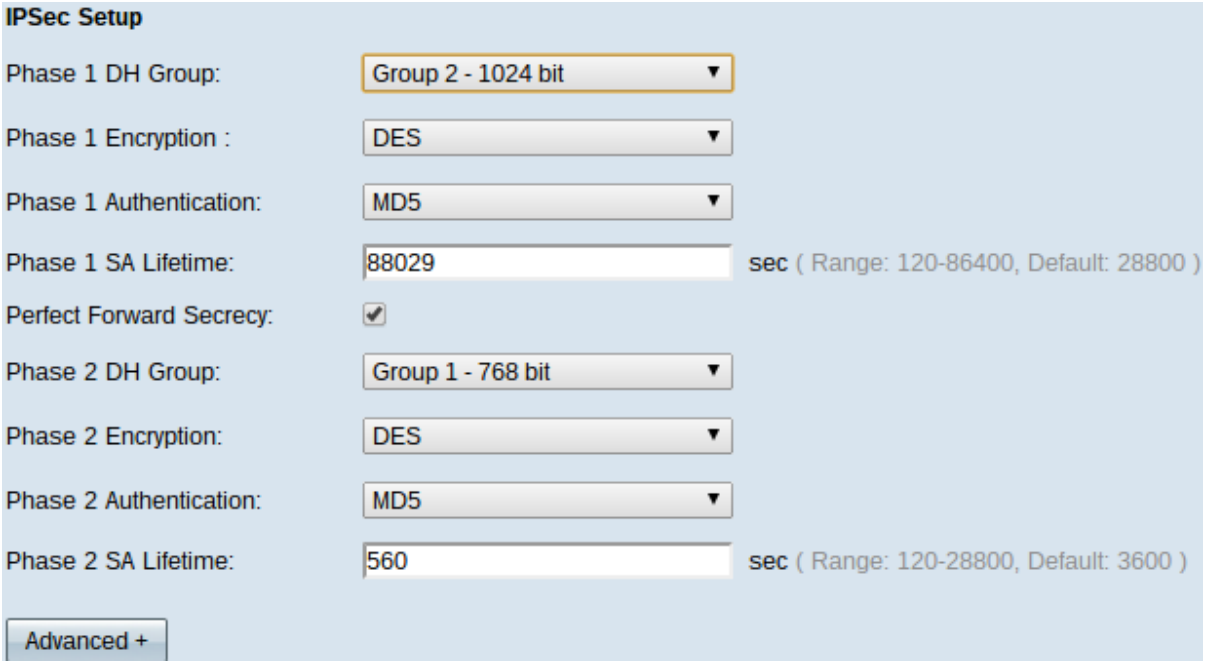
注意：强烈建议频繁更改IKE对等体之间的预共享密钥，以便VPN保持安全。

预共享密钥强度计通过颜色条显示预共享密钥的强度。红色表示强度弱，黄色表示强度可接受，绿色表示强度高。

步骤12.单击“**保存**”以保存设置。

带证书的IKE的IPSec设置

仅当从Add a New Tunnel的Step 3的Keying Mode下拉列表中选择了带证书的IKE时才可用。



第 1 步： 从 Phase 1 DH Group（第 1 阶段 DH 组）下拉列表中选择适当的第 1 阶段 DH 组。第1阶段用于在隧道两端之间建立单工逻辑SA（安全关联），以支持安全身份验证通信。DH是在第1阶段连接期间用于共享密钥以验证通信的加密密钥交换协议。

·组1 - 768位 — 表示最高强度的密钥和最安全的身份验证组。但是，它需要更多时间来计算IKE密钥。如果网络速度较快，则首选此选项。

·组2 - 1024位 — 表示更高强度的密钥和更安全的身份验证组。但是，它需要一些时间来计算 IKE 密钥。

·组5 - 1536位 — 表示强度最低的密钥和最不安全的身份验证组。计算IKE密钥所需的时间更少。如果网络速度较慢，则首选此选项。

步骤2.从Phase 1 Encryption下拉列表中选择适当的Phase 1 Encryption以加密密钥。建议使用AES-128、AES-192或AES-256。VPN 隧道的两端需要使用相同的加密方法。

·DES - DES是56位旧式加密方法，在当今世界，这种加密方法并不十分安全。

·3DES - 3DES是一种168位的简单加密方法，通过加密数据三次来增加密钥大小，比DES提供更高的安全性。

·AES-128 - AES是128位加密方法，通过10次循环重复将纯文本转换为密文。

·AES-192 — 是192位加密方法，通过12次循环重复将纯文本转换为密文。

·AES-256 — 是一种256位加密方法，通过14次循环重复将纯文本转换为密文。

步骤3.从Phase 1 Authentication下拉列表中选择适当的身份验证方法。VPN 隧道的两端需要使用相同的身份验证方法。建议使用SHA1。

·MD5 - MD5表示32位十六进制哈希函数，通过校验和计算保护数据免受恶意攻击。

·SHA1 — 比MD5更安全的160位哈希函数。

步骤4.在Phase 1 SA Life Time字段中输入VPN隧道保持活动状态的时间量（以秒为单位）。

步骤5.选中Perfect Forward Secrecy复选框，为密钥提供更多保护。此选项允许在任何密钥被破坏时生成新密钥。加密的数据只会通过被盗取的密钥泄露。因此，当另一个密钥被入侵时，它可以保护其他密钥，从而提供更安全且更经过身份验证的通信。推荐采取此操作，因为它可以提供更高的安全性。

步骤6.从第2阶段DH组下拉列表中选择适当的第2阶段DH组。第1阶段用于建立隧道两端之间的单工逻辑SA，以支持安全认证通信。DH是在第1阶段连接期间用于共享密钥以验证通信的加密密钥交换协议。

·组1 - 768位 — 表示最高强度的密钥和最安全的身份验证组。但是，它需要更多时间来计算IKE密钥。如果网络速度较快，则首选此选项。

·组2 - 1024位 — 表示更高强度的密钥和更安全的身份验证组。但是，它需要一些时间来计算 IKE 密钥。

·组5 - 1536位 — 表示强度最低的密钥和最不安全的身份验证组。计算IKE密钥所需的时间更少。如果网络速度较慢，则首选此选项。

注意：由于没有生成任何新密钥，因此如果在步骤5中未选中完全向前保密，则无需配置第2阶段DH组。

第 7 步： 从 Phase 2 Encryption（第 2 阶段加密）下拉列表中选择适当的第 2 阶段加密来加密密钥。建议使用AES-128、AES-192或AES-256。VPN 隧道的两端需要使用相同的加密方法。

·DES - DES是56位旧式加密方法，在当今世界，这种加密方法并不十分安全。

·3DES - 3DES是一种168位的简单加密方法，通过加密数据三次来增加密钥大小，比DES提供更高的安全性。

·AES-128 - AES是128位加密方法，通过10次循环重复将纯文本转换为密文。

·AES-192 — 是192位加密方法，通过12次循环重复将纯文本转换为密文。

·AES-256 — 是一种256位加密方法，通过14次循环重复将纯文本转换为密文。

第 8 步： 从 Phase 2 Authentication（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 隧道的两端需要使用相同的身份验证方法。

·MD5 - MD5表示32位十六进制哈希函数，通过校验和计算保护数据免受恶意攻击。

·SHA1 — SHA1是160位哈希函数，比MD5更安全。

·空 — 不使用身份验证方法。

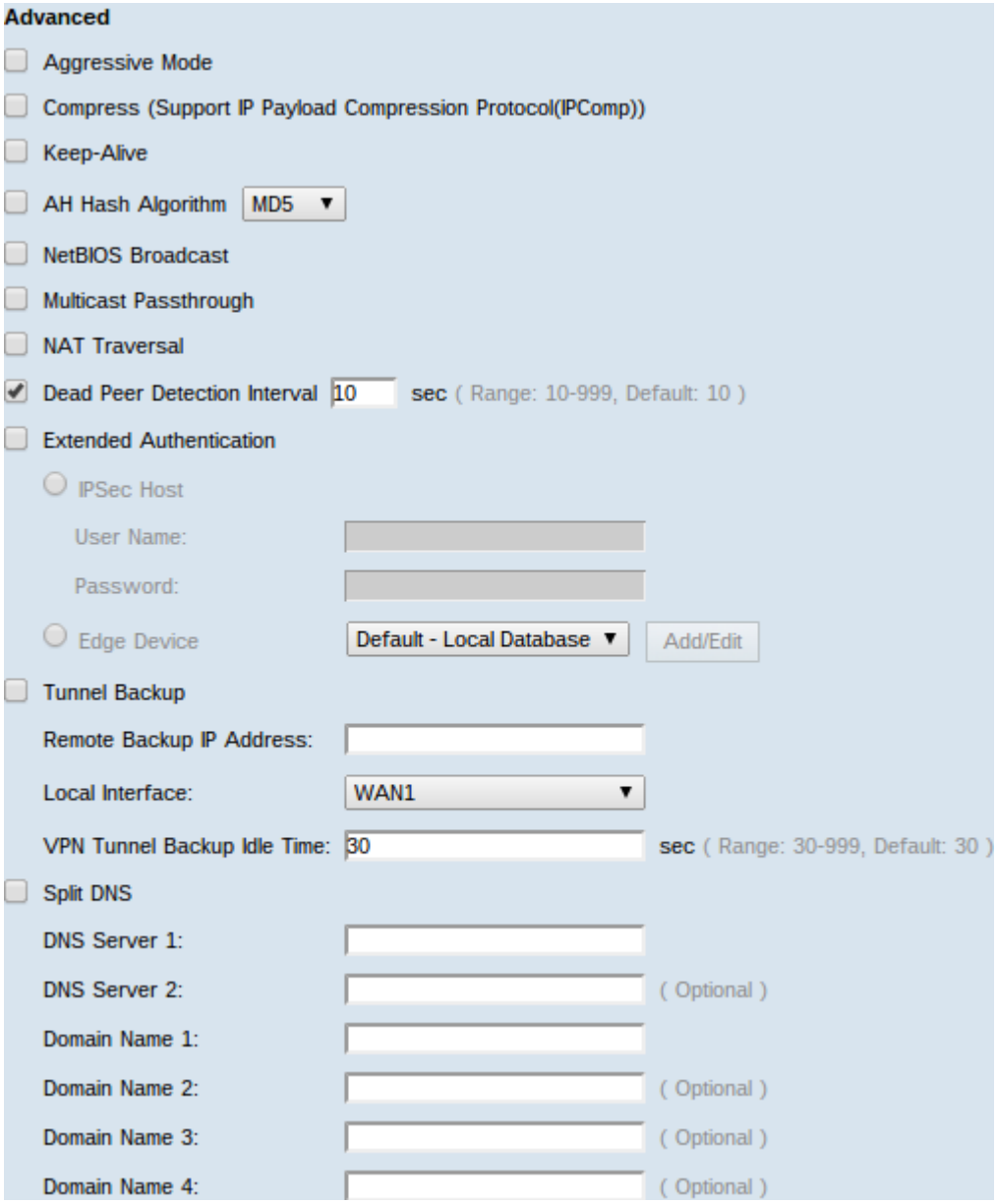
步骤9.在Phase 2 SA Life Time字段中输入VPN隧道保持活动状态的时间（以秒为单位）。

步骤10.单击“**保存**”以保存设置。

（可选）IKE的IPSec高级设置（带证书）和IKE的预共享密钥

如果从Add a New Tunnel的Step 3的Keying Mode下拉列表中选择了带证书的IKE或带预先密钥的IKE，则高级选项可用。两种类型的键控模式都可使用相同的设置。

步骤1.单击“高**级+**”按钮以显示高级IPSec选项。



步骤2.如果网络速度较低，请选中Aggressive Mode复选框。它在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.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、用户希望通过缓慢的网络快速传输数据而不丢失数据时压缩IP数据报的大小。

步骤4.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。如果任何连接变为非活动状态，它有助于立即重新建立连接。

步骤5.如果要对身份验证报头(AH)进行身份验证，请选中AH Hash Algorithm复选框。AH为数据源提供身份验证，通过校验和实现数据完整性并将保护扩展到IP报头。隧道两端的算法应相

同。

·MD5 - MD5表示128位十六进制哈希函数，通过校验和计算保护数据免受恶意攻击。

·SHA1 — SHA1是160位哈希函数，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。默认情况下为未选中状态。NetBIOS 用于通过一些软件应用和网上邻居等 Windows 功能来检测网络中的网络资源，例如打印机、计算机等。

步骤7.如果VPN路由器位于NAT网关后面，请选中此框以启用NAT穿越。网络地址转换(NAT)使具有私有LAN地址的用户能够使用公有可路由的IP地址作为源地址来访问Internet资源。但是，对于入站流量，NAT网关没有自动方法将公有IP地址转换到专用LAN上的特定目标。此问题会阻止IPSec交换成功。NAT遍历设置此入站转换。隧道两端必须使用相同的设置。

步骤8.检查Dead Peer Detection Interval以定期检查通过Hello或ACK的VPN隧道的活动性。如果选中此复选框，请输入所需问候消息的持续时间或间隔（以秒为单位）。

步骤9.选中Extended Authentication（扩展身份验证）以使用IPSec主机用户名和密码对VPN客户端进行身份验证或使用在User Management（用户管理）中找到的数据库。必须在两台设备中启用此功能，才能使其正常工作。单击**IPSec Host**单选按钮以使用IPSec主机和用户名，并在User Name字段和Password字段中输入用户名和密码。或单击“边**缘设备**”单选按钮以使用数据库。从边缘设备下拉列表中选择所需的数据库。

步骤10.选中Tunnel Backup复选框以启用隧道备份。当Dead Peer Detection Interval已检查时，此功能可用。该功能使设备能够通过备用WAN接口或IP地址重新建立VPN隧道。

·远程备份IP地址 — 远程对等体的备用IP。在此字段中输入它或已为远程网关设置的WAN IP。

·本地接口 — 用于重新建立连接的WAN接口。从下拉列表中选择所需的接口。

·VPN Tunnel Backup Idle Time — 在主隧道未连接时选择何时使用备份隧道的时间。以秒为单位输入。

步骤11.选中Split DNS复选框以启用拆分DNS。此功能允许根据指定域名向定义的DNS服务器发送DNS请求。在DNS Server 1和DNS Server 2字段中输入DNS服务器名称，并在Domain Name #字段中输入域名。

步骤12.单击“保**存”**完成设备的配置。