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

目标

本文档旨在向您展示如何在RV32x系列VPN路由器上配置单个客户端到网关虚拟专用网络(VPN)。

简介

VPN是专用网络，用于通过公共网络虚拟连接远程用户。一种VPN类型是客户端到网关VPN。客户端到网关VPN是远程用户与网络之间的连接。客户端在用户设备中配置了VPN客户端软件。它允许用户远程安全地连接到网络。

适用设备

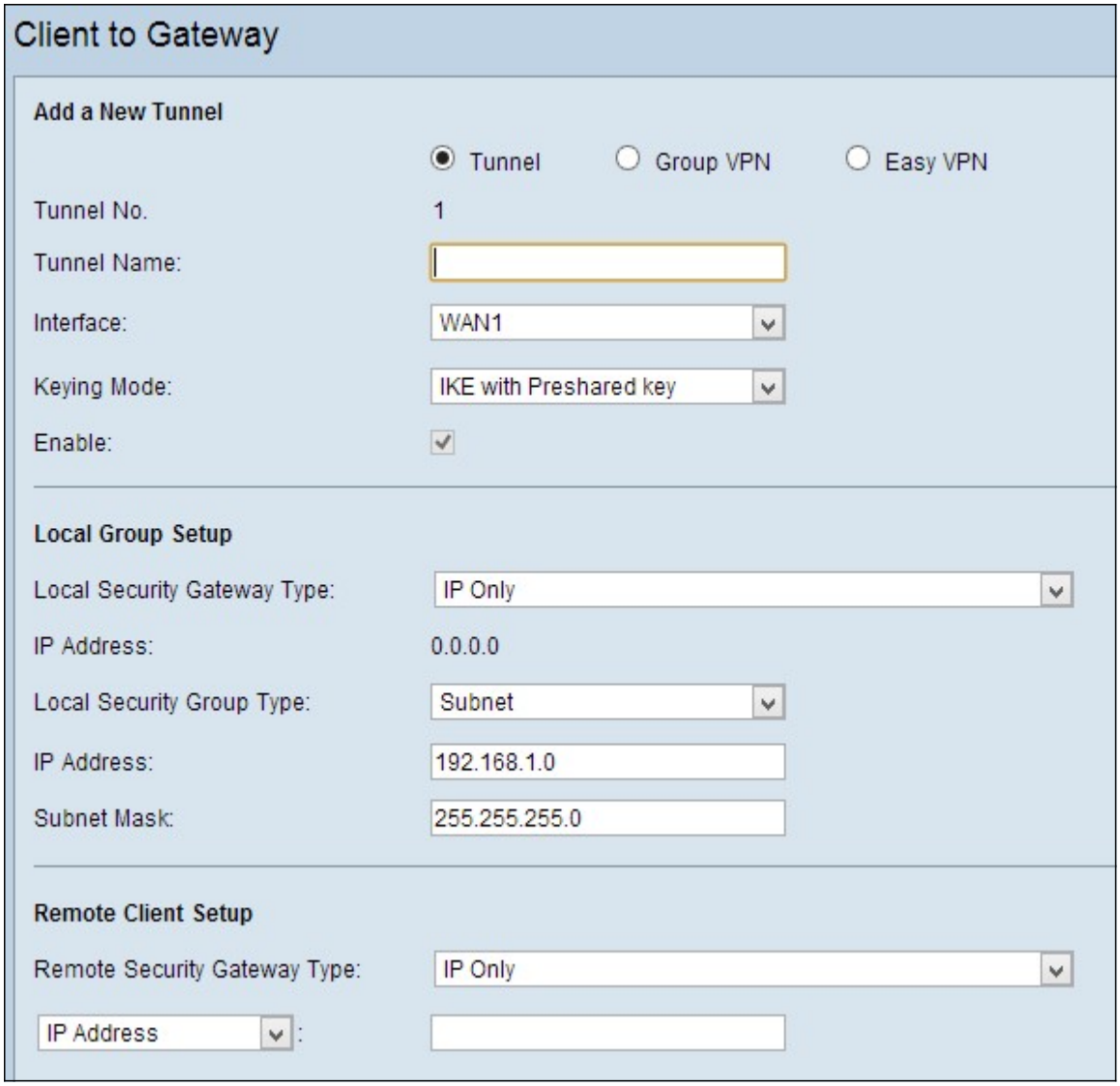
- RV320双WAN VPN路由器
- RV325千兆双WAN VPN路由器

软件版本

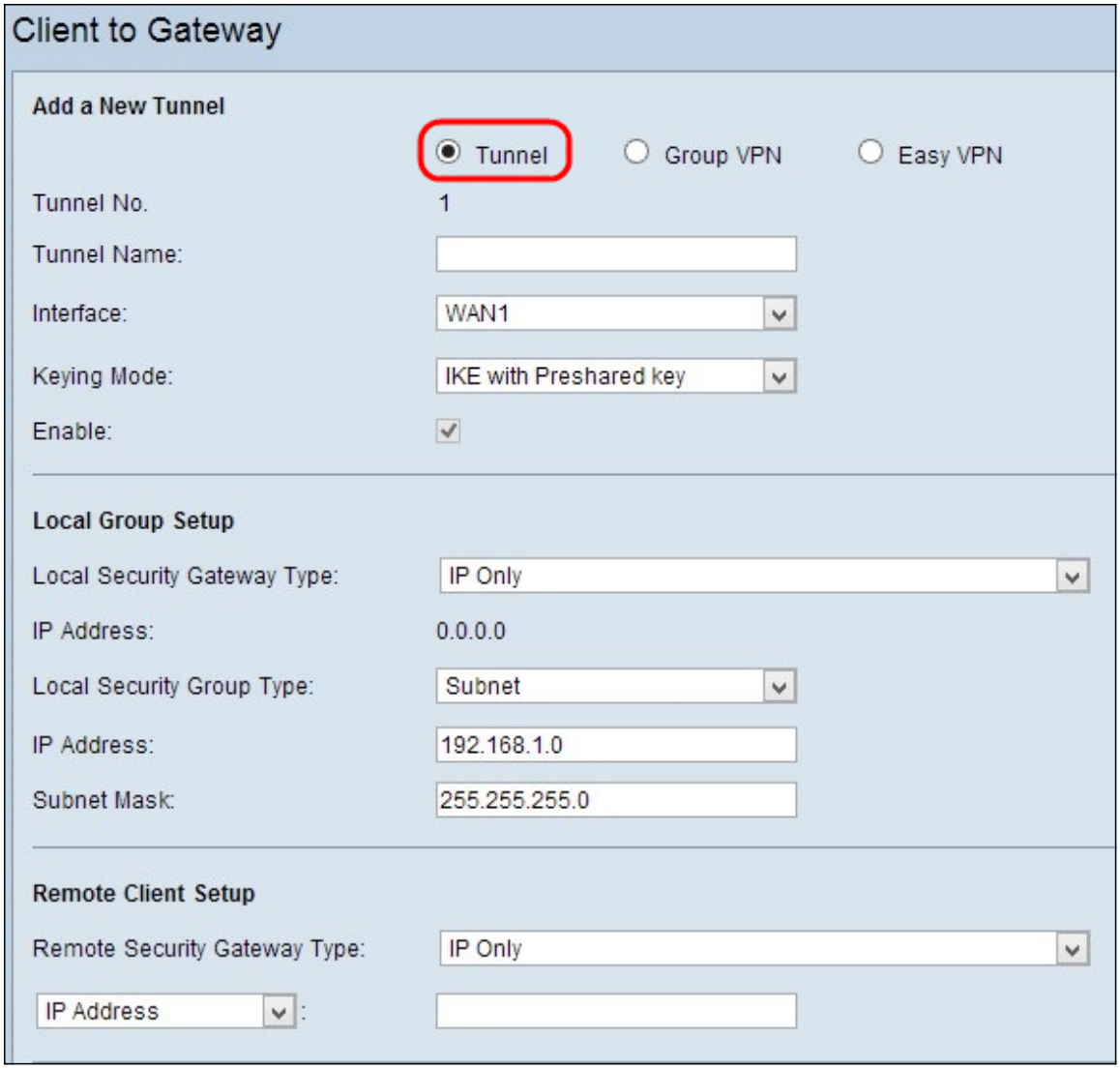
- v1.1.0.09

配置单客户端到网关VPN

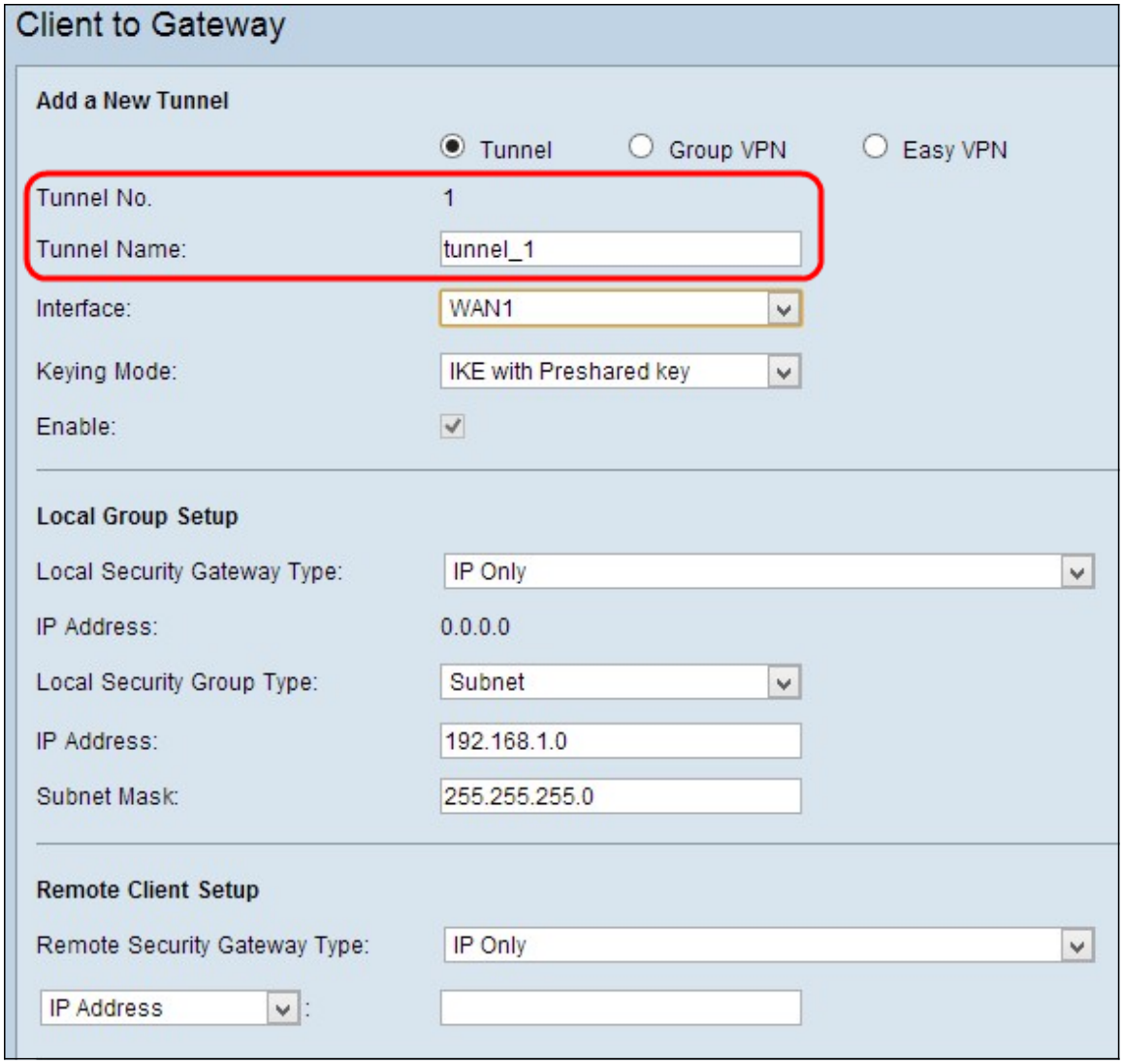
第 1 步： 登录到 Web 配置实用程序，然后选择 VPN > Client to Gateway（客户端到网关）。系统将打开 *Client to Gateway（客户端到网关）页面：*



步骤2.单击**Tunnel**单选按钮，为客户端到网关VPN添加单个隧道。


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
:

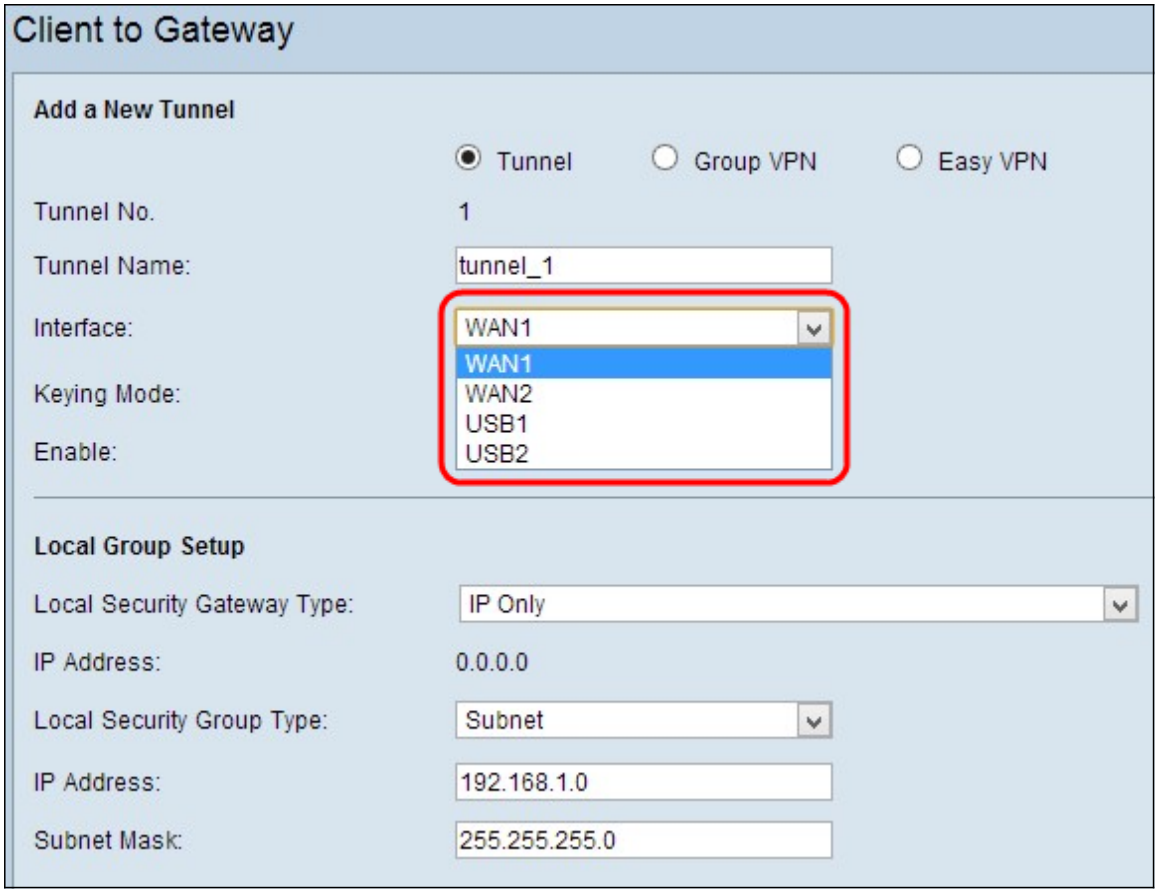
添加新隧道



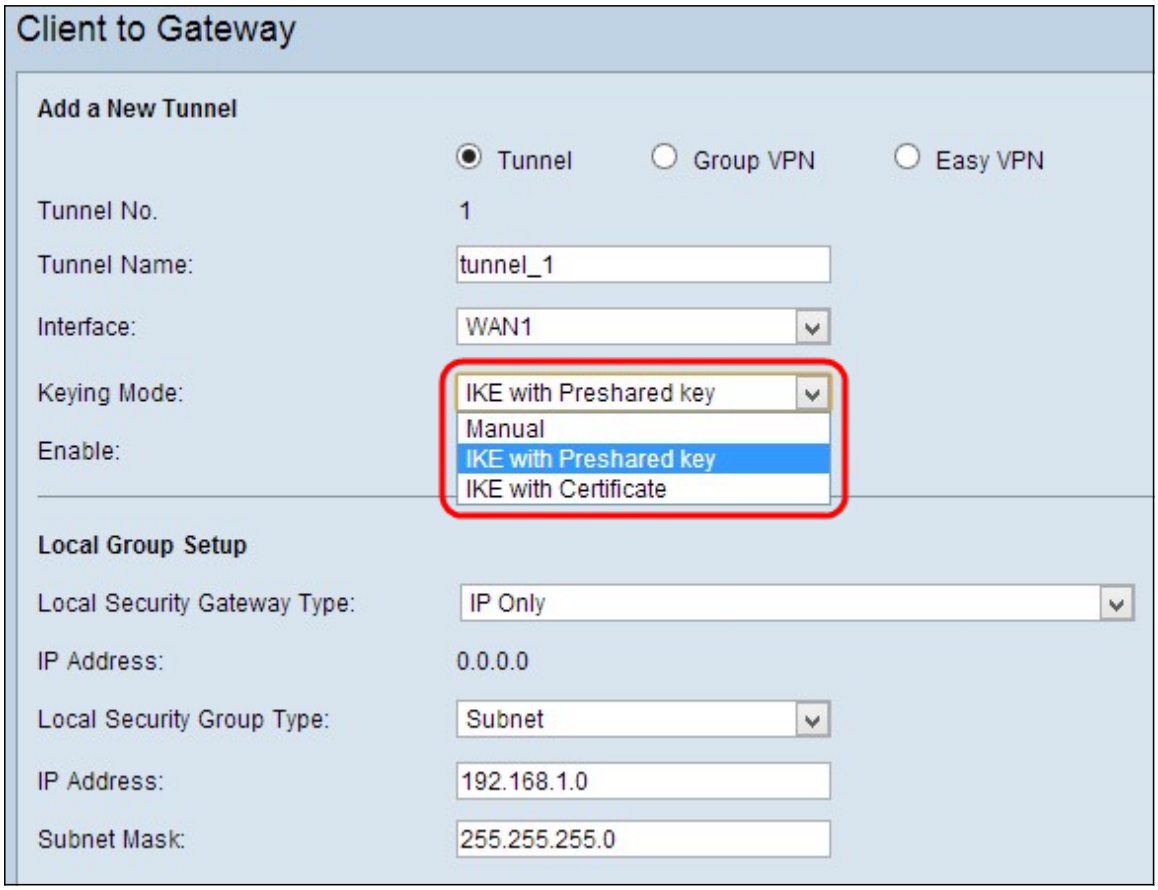
注意：隧道编号 — 表示隧道的编号。此号码会自动生成。

步骤1.在Tunnel Name字段中输入隧*道的名*称。

步骤2.从*接口*下拉列表中选择远程客户端访问VPN所通过的接口。



第 3 步： 从 *Keying Mode（密钥模式）*下拉列表中选择适当的密钥管理模式，以确保安全。默认模式为 IKE with Preshared key（带预共享密钥的 IKE）。



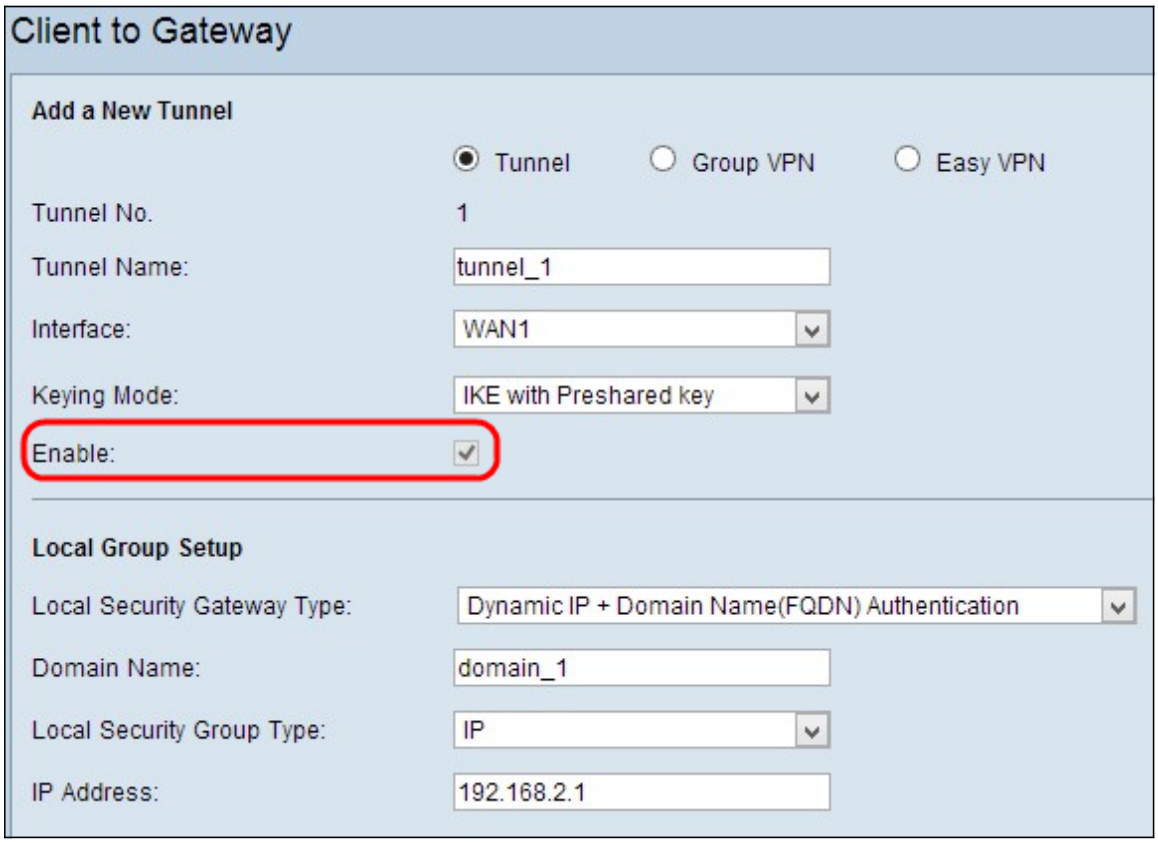
选项定义如下：

- 手动 — 自定义安全模式，可自行生成新的安全密钥，且不与密钥协商。它最适合在故障排除期

间或小型静态环境中使用。

- 带预共享密钥的IKE — 互联网密钥交换(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。
- 带证书的IKE — 带证书的互联网密钥交换(IKE)协议是一种更安全的方法，可自动生成和交换预共享密钥，以便为隧道建立更安全的通信。

步骤4.选中**Enable**复选框以启用客户端到网关VPN。默认情况下启用。



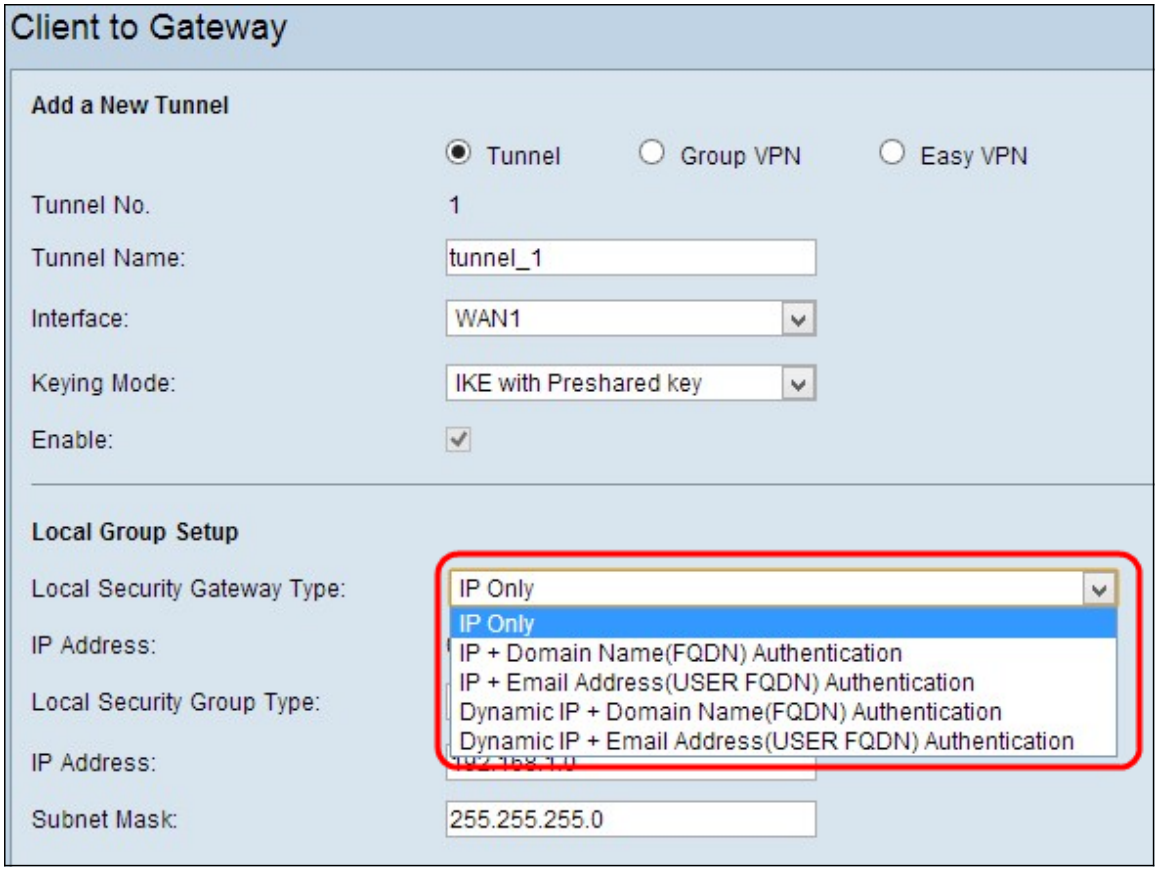
步骤5.如果要保存到目前为止的设置，请向下滚动并单击“保**存**”以保存设置。

本地组设置

使用手动设置本地组或使用预共享密钥的IKE

注意：如果从Add a New Tunnel（添加新隧道）部分的Step 3的*Keying Mode*（键控模式）下拉列表中选择Manual（手动）或IKE with Preshared（预共享）*密钥，请执行以下*步骤。

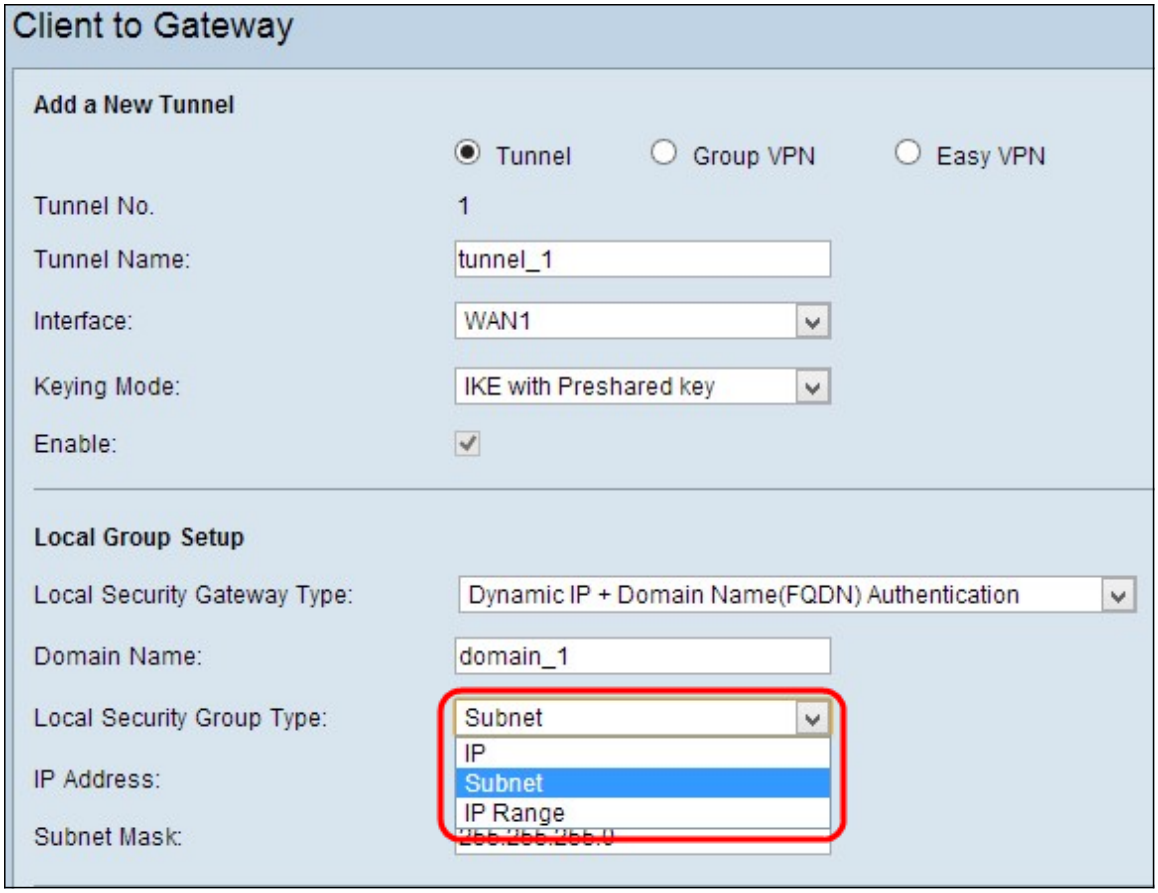
步骤1.从Local Security Gateway（本地安全网关）下拉列*表中选择*适当的路由器标识方法，以建立VPN隧道。



选项定义如下：

- 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地址会自动生成。
- 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地址会自动生成。
- 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地址会自动生成。
- 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。
- IP Address — 表示WAN接口的IP地址。它是只读字段。

步骤2.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。

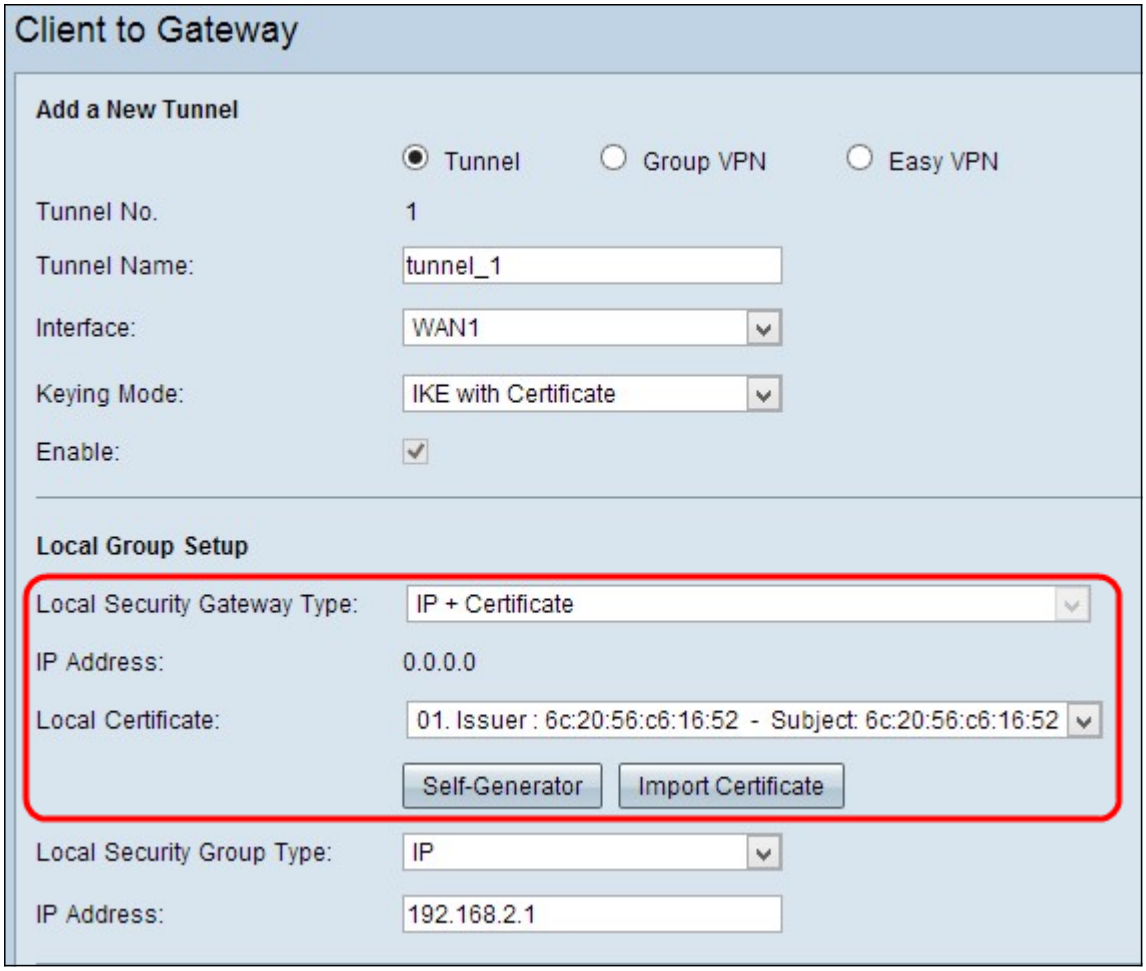


- IP — 只有一个特定LAN设备可以访问隧道。如果选择此选项，请在“IP Address”（IP 地址）字段中输入 LAN 设备的 IP 地址。默认 IP 地址为 192.168.1.0。
- 子网 — 特定子网上的所有LAN设备都可以访问隧道。如果选择此选项，请分别在“IP Address”（IP 地址）和“Subnet Mask”（子网掩码）字段中输入 LAN 设备的 IP 地址和子网掩码。默认掩码为 255.255.255.0。
- IP范围 — 一系列LAN设备可以访问隧道。如果选择此选项，请在“开始IP”和“结束IP”字*段中分*别输*入起始IP*地址和结束IP。默认范围为 192.168.1.0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

步骤3.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

使用带有隧道VPN证书的IKE的本地组设置

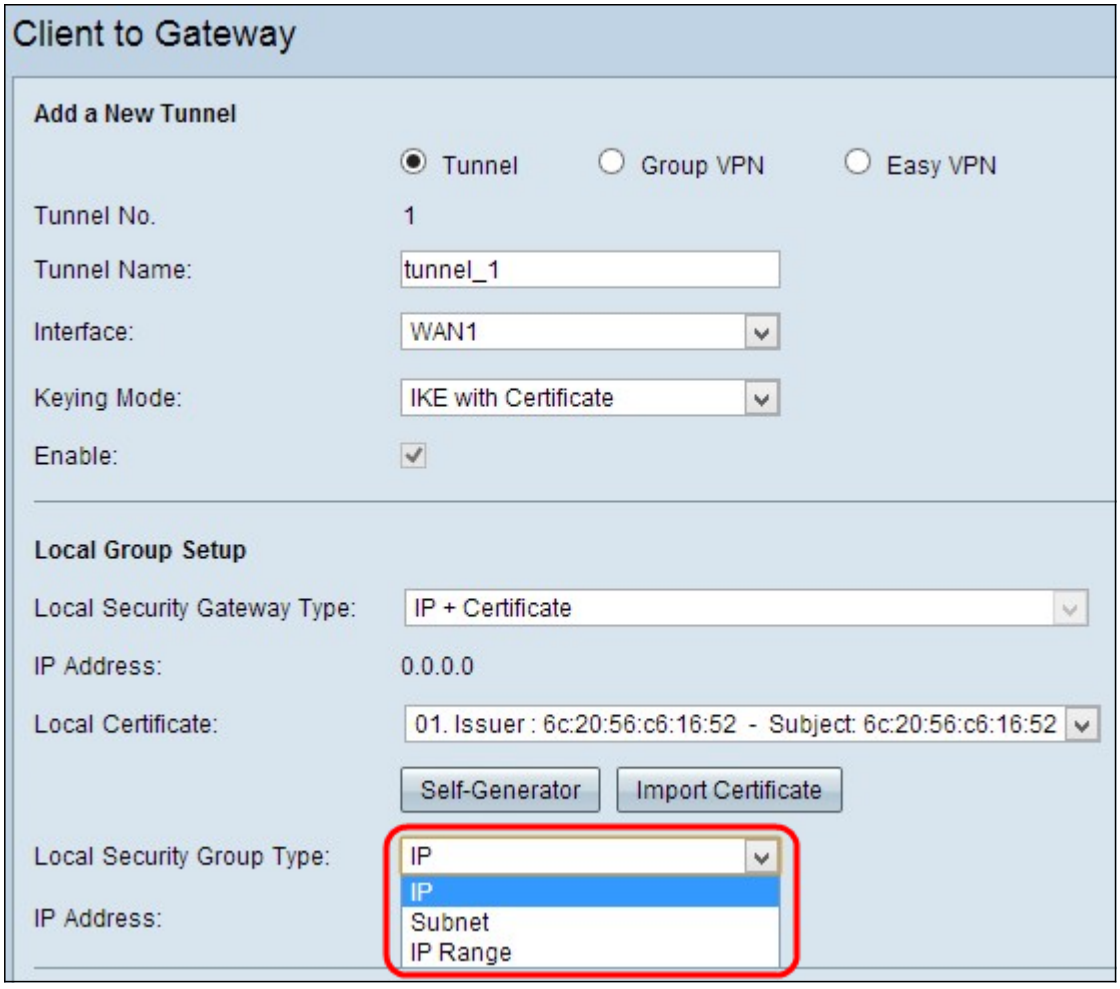
注意：如果从Add a New Tunnel（添加新隧道）部分的Step 3的*Keying Mode（键控模式）*下拉列表中选择IKE with Certificate（带证书），请*执行以下*步骤。



- 本地安全网关类型 — 可通过带证书的IP访问隧道。
- IP Address — 表示WAN接口的IP地址。它是只读字段。

步骤1.从Local Certificate下拉列表中选择适当的本地证*书以*标识路由器。单击**Self-Generator(自**生成器)自动生成证书，或单**击Import Certificate(导**入证书)导入新证书。

注意：要了解有关如何自动生成证书的详细信息，请参阅*在RV320路由器上生成证书*，以及如何导入证书，请参阅*在RV320路由器上配置我的证书*。



步骤2.从Local Security Group Type下拉列表中选择可以访问VPN隧道的适当类型的本地LAN *用户或*用户组。默认为子网。

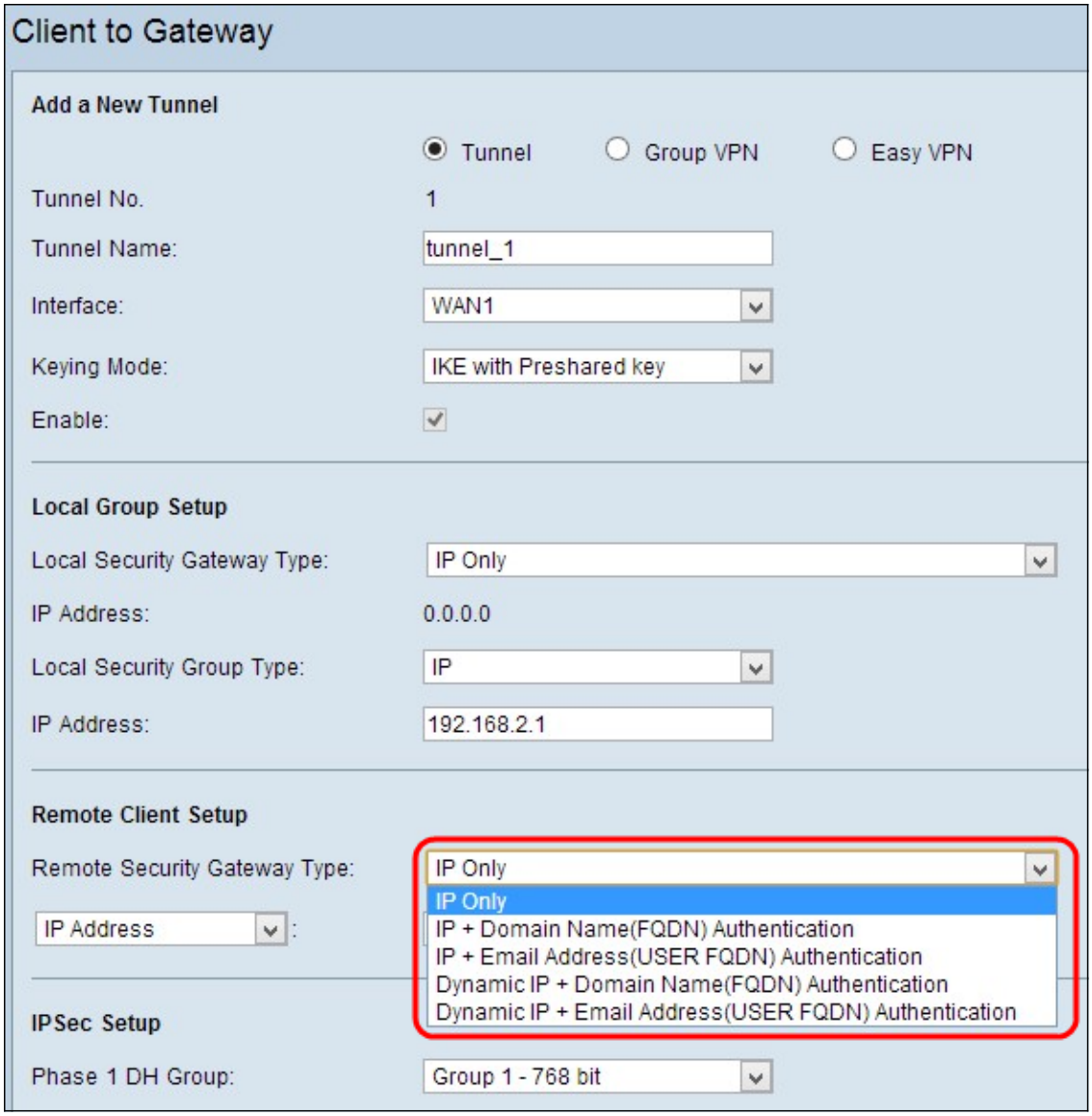
- IP — 只有一个特定LAN设备可以访问隧道。如果选择此选项，请在“IP Address”（IP 地址）字段中输入 LAN 设备的 IP 地址。默认 IP 地址为 192.168.1.0。
- 子网 - 特定子网上的所有 LAN 设备都可以访问隧道。如果选择此选项，请分别在“IP Address”（IP 地址）和“Subnet Mask”（子网掩码）字段中输入 LAN 设备的 IP 地址和子网掩码。默认掩码为 255.255.255.0。
- IP 范围 - 一些 LAN 设备可以访问隧道。如果选择此选项，请在Start IP和End IP字段中输入起始和结束IP地址。默认范围为 192.168.1.0 到 192.168.1.254。

步骤3.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

远程客户端设置

使用手动或IKE使用预共享密钥的远程客户端设置

注：如果在“添加新隧道”部分的步骤3中从“键控模式”下拉列表中选*择*“手动”或“使用预共享密钥的IKE”，*请执行以下*步骤。



步骤1.从Remote Security Gateway（远程安全网关）下拉列表中，选择适当的客户*端标识方*法来建立VPN隧道。默认设置为“IP Only”（仅 IP）。

- 仅 IP - 仅通过客户端的静态 WAN IP 即可访问隧道。仅当您知道客户端的静态WAN IP或域名时，才能选择此选项。从下拉列表中选择IP地址，并在相邻字段中输入客户端的静态IP，或从下拉列表中选择IP by DNS Resolved并在相邻字段中输入客户端的域名。通过IP地址的本地DNS服务器，路由器可以自动检索IP地址。

  注意：如果从Add a New Tunnel Through Tunnel or Group VPN部分的步骤3的*Keying Mode* 下拉列表中选择Manual，这将是唯一可用的选项。

- IP + 域名 (FQDN) 身份验证 - 可以通过客户端的静态 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。从下拉列表中选择IP地址，并在相邻字段中输入客户端的静态IP，或从下拉列表中选择IP by DNS Resolved并在相邻字段中输入客户端的域名。通过IP地址的本地DNS服务器，路由器可以自动检索IP地址。
- IP +电子邮件地址（用户FQDN）身份验证 — 可通过客户端的静态IP地址和电子邮件地址访问隧道。如果选择此选项，请在“电子邮件地址”字段中输入电子邮件地址。从下拉列表中选择IP地址并在相邻字段中输入客户端的静态IP，或从下拉列表中选择IP by DNS Resolved并在相邻字段中输入IP地址的域名。通过IP地址的本地DNS服务器，路由器可以自动检索IP地址。
- 动态 IP + 域名 (FQDN) 身份验证 - 可以通过客户端的动态 IP 地址和注册域访问隧道。如果选

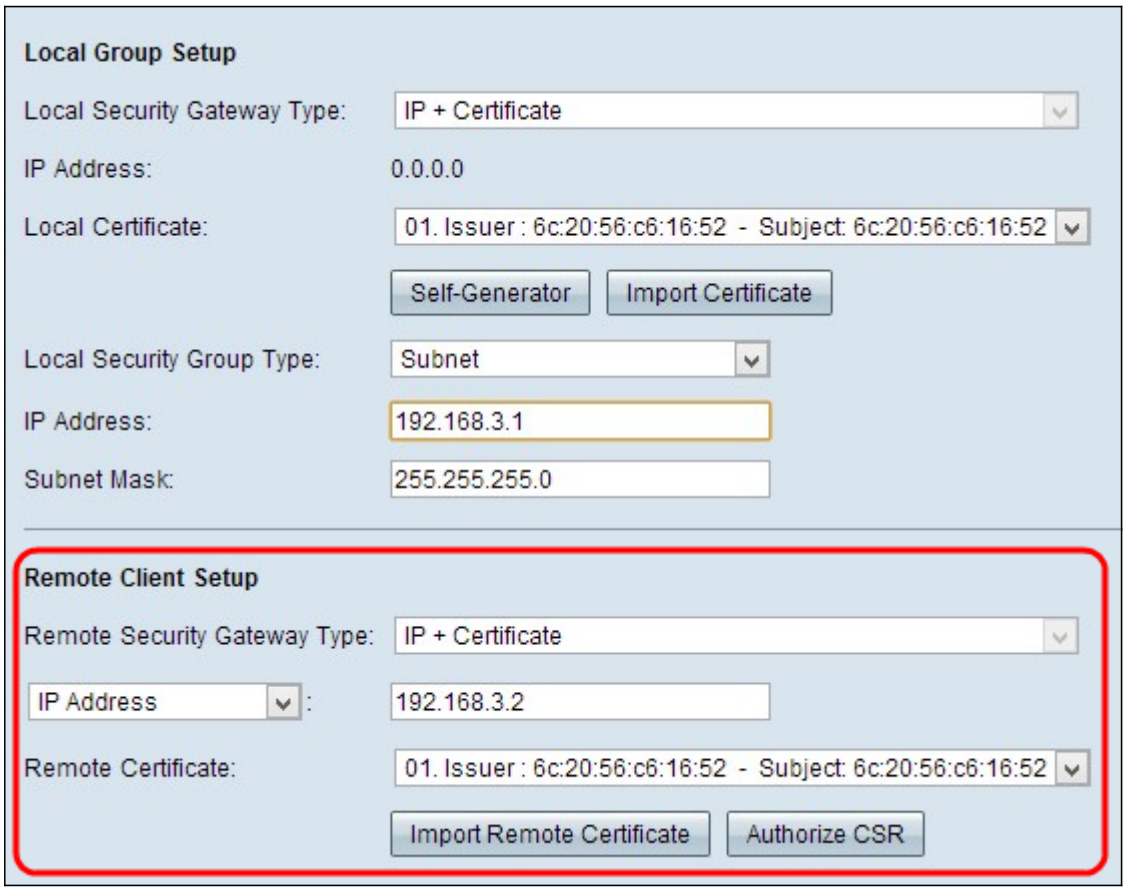
择此选项，请在“Domain Name”（域名）字段中输入注册域的名称。

- 动态IP +邮件地址（用户FQDN）身份验证 — 可通过客户端的动态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。

步骤2.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

使用带证书的IKE的远程组设置

注：如果从Add a New Tunnel（添加新隧道）部分的Step 3的Keying Mode(键控模式*)*下拉列表中选择IKE with Certificate（带证书），请执行*以下*步骤。



- 远程安全网关类型 — 客户端标识可通过带证书的IP建立VPN连接。

步骤1.从下**拉列**表中**选择IP Address**或IP by DNS Resolved。

- IP地址 — 只能通过客户端的静态WAN IP访问隧道。只有知道客户端的静态WAN IP时，才可选择此选项。在IP地址字段中输入客户*端的静*态IP。
- IP By DNS Resolved — 如果您不知道客户端的IP地址，但知道该IP地址的域，则此功能非常有用。输入IP地址的域名。通过IP地址的本地DNS服务器，路由器可以自动检索IP地址。

步骤2.从Remote Certificate下拉列表中选*择相*应的远程证书。单击**Import Remote Certificate(导**入远程证书)导入新证书，或单**击Authorize CSR**（授权CSR）以识别带有数字签名请求的证书。

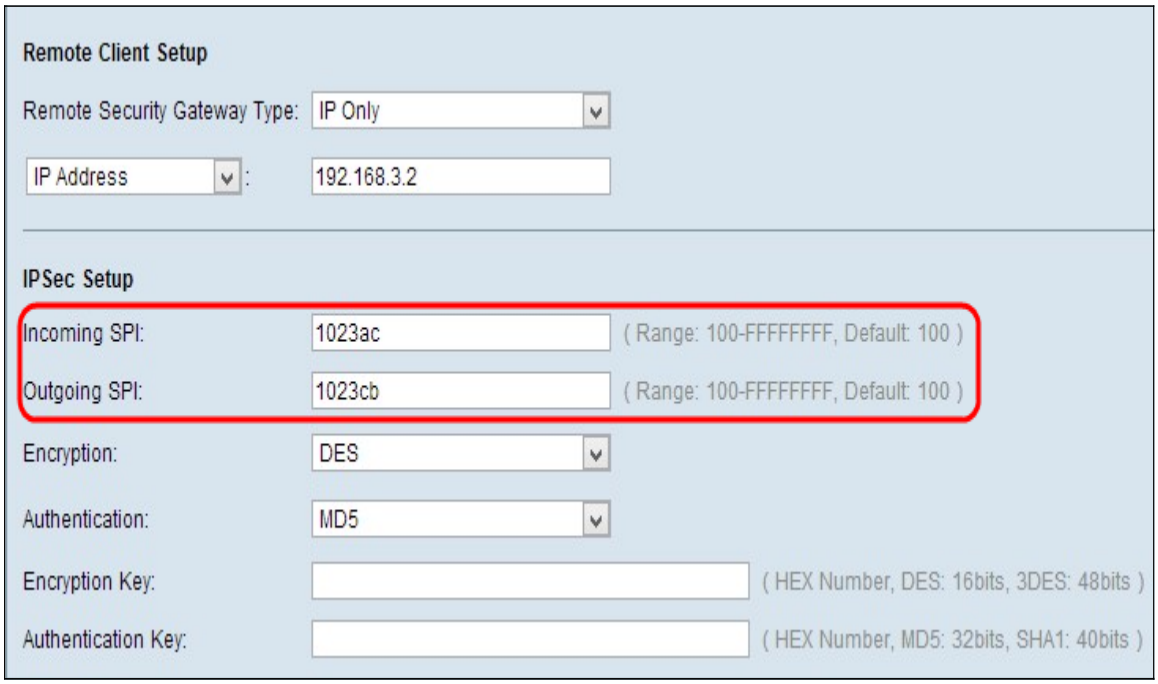
注意：如果想了解有关如何导入新证书的详细信息，请参阅*查看/添加RV320路由器上的受信任SSL证书*，并了解有关授权CSR的详细信息，请参阅*RV320路由器上的证书签名请求(CSR)*。

步骤3.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

IPSec 设置选项

IPSec设置（手动键）

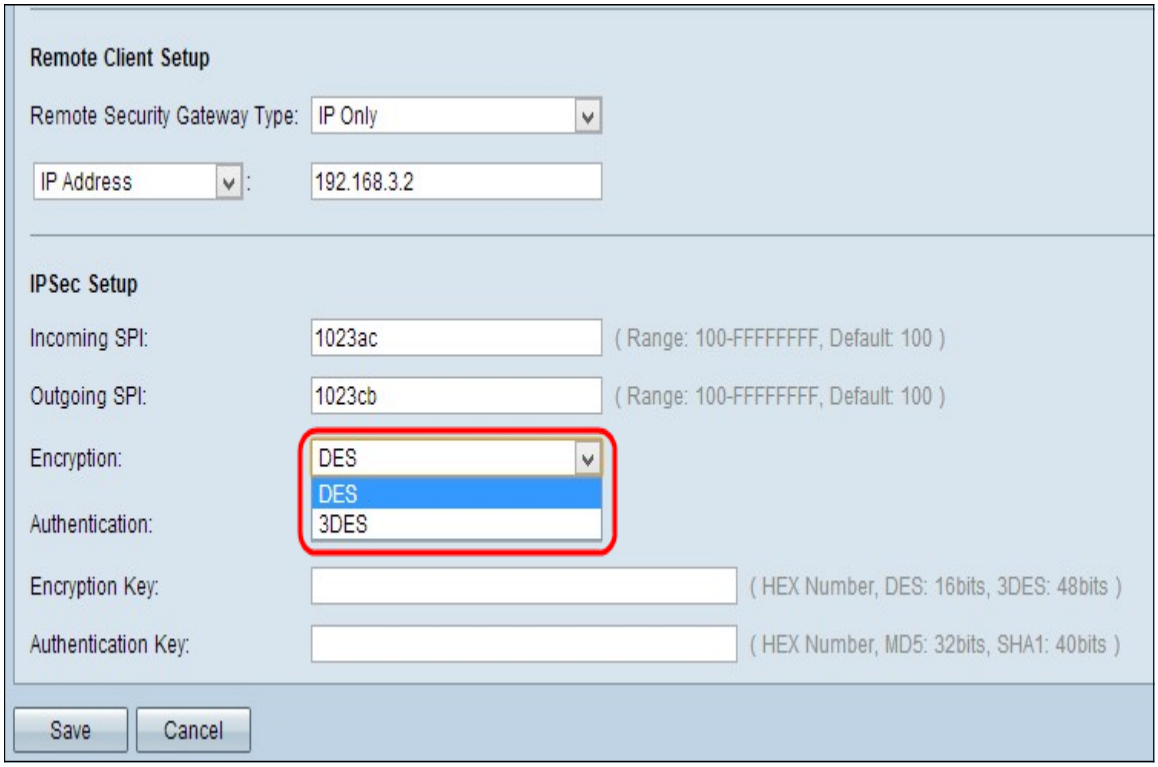
注：如果从“添加新隧道”部分的步骤3*的*“键控模式”下拉列表中选择了“手*动*”，*请执行以*下步骤。



步骤1.在传入SPI字段中输入传入安全参数索引(SPI)的*唯一十六进制*值。SPI在封装安全负载协议(ESP)报头中携带，ESP报头共同确定传入数据包的安全关联(SA)。范围是100到ffffffff，默认为100。

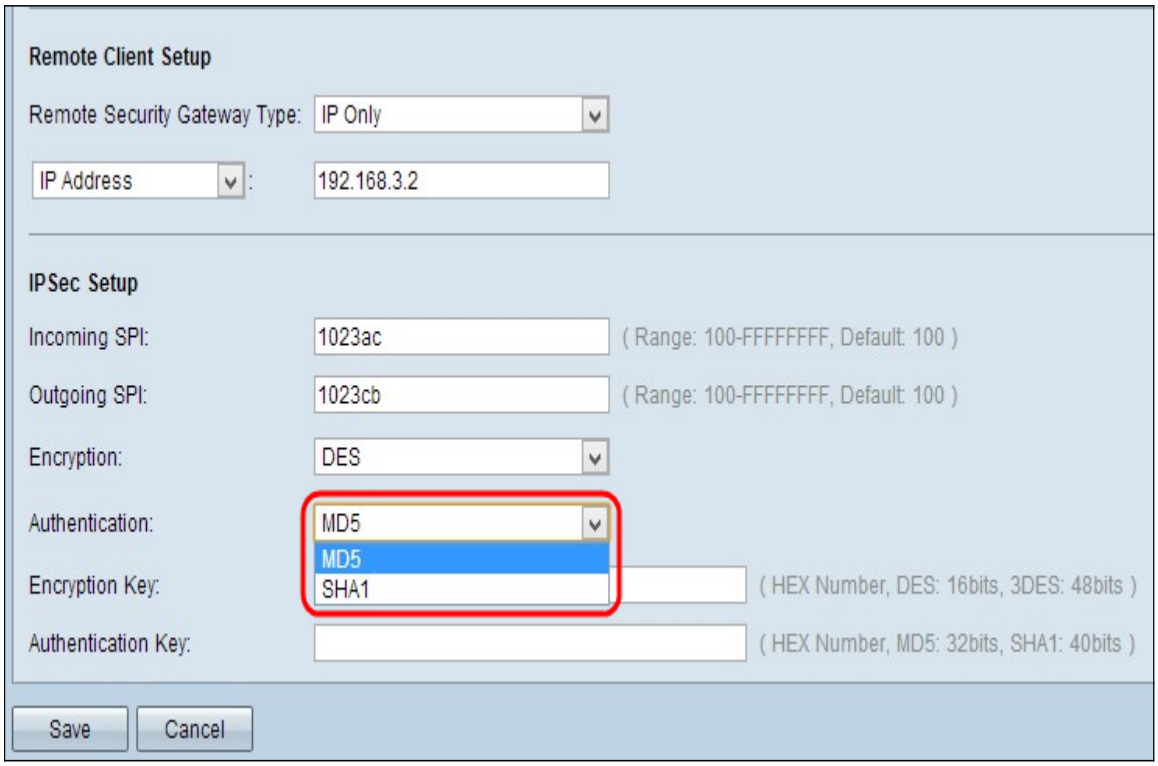
步骤2.在传出SPI字段中输入传出安全参数索引(SPI)的唯一*十六进制*值。SPI在封装安全负载协议(ESP)报头中传输，ESP报头共同确定传出数据包的安全关联(SA)。范围是100到ffffffff，默认为100。

注意：连接的设备的传入SPI和隧道另一端的传出SPI应相匹配以建立隧道。



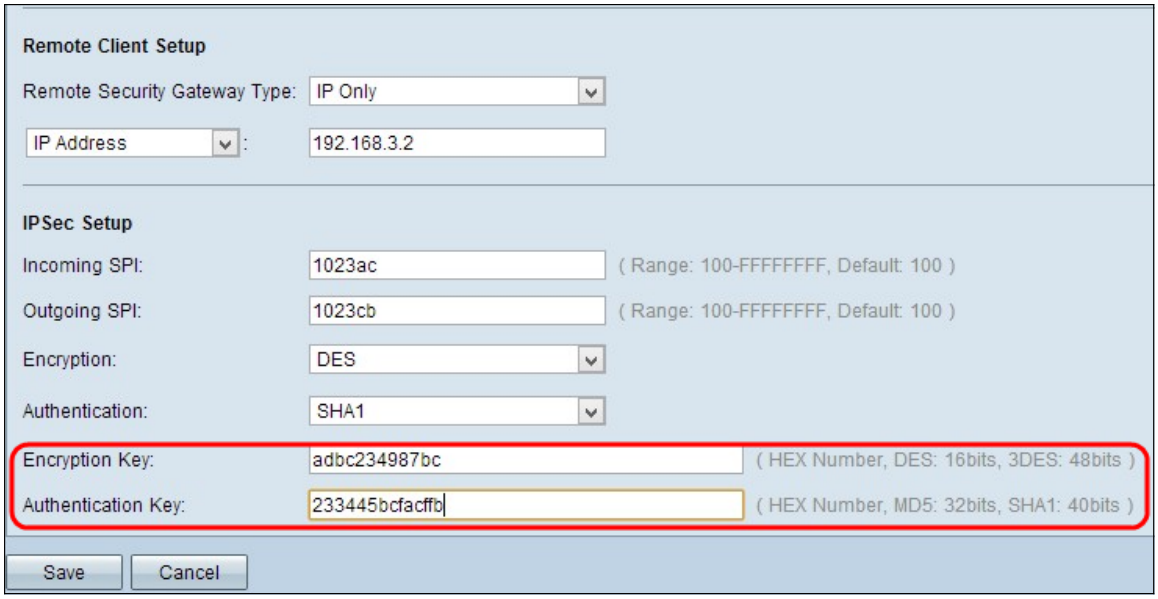
步骤3.从Encryption下拉列表中选择适*当的*加密方法。推荐的加密方法为 3DES。VPN 隧道的两端需要使用相同的加密方法。

- DES — 数据加密标准(DES)是一种56位的、较旧、向后兼容的加密方法，并不安全。
- 3DES — 三重数据加密标准(3DES)是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 — 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 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全。



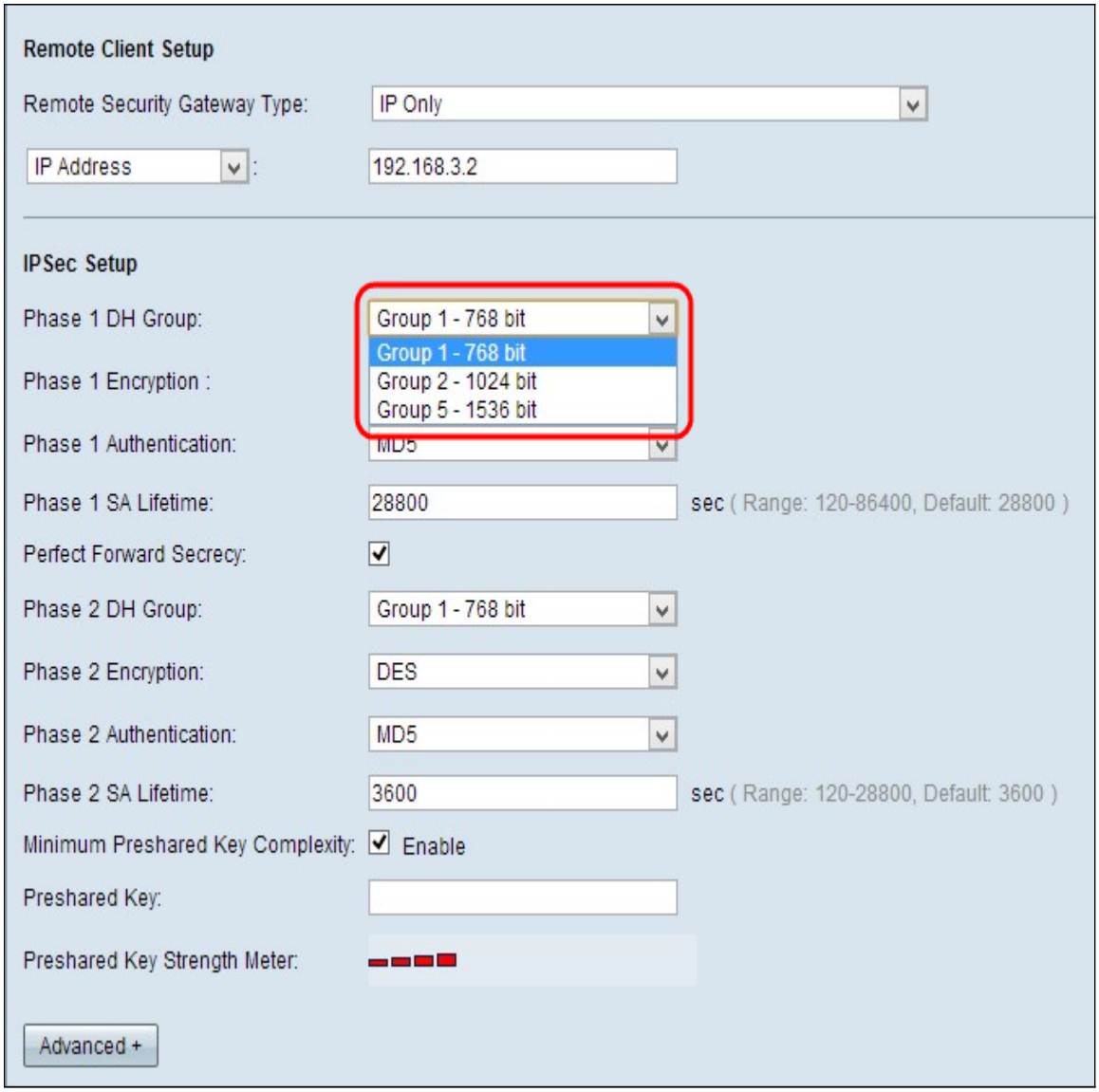
第 5 步： 在 *Encryption Key (加密密钥) 字段中输入密钥，以加密和解密数据。*如果在步骤3中选择DES作为加密方法，请输入16位十六进制值。如果在步骤3中选择3DES作为加密方法，请输入40位十六进制值。

第 6 步： 在 *Authentication Key (身份验证密钥)* 字段中输入预共享密钥，以对流量进行身份验证。如果您在第 4 步中选择 MD5 作为身份验证方法，请输入 32 位十六进制值。如果您在第 4 步中选择 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。

步骤7.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

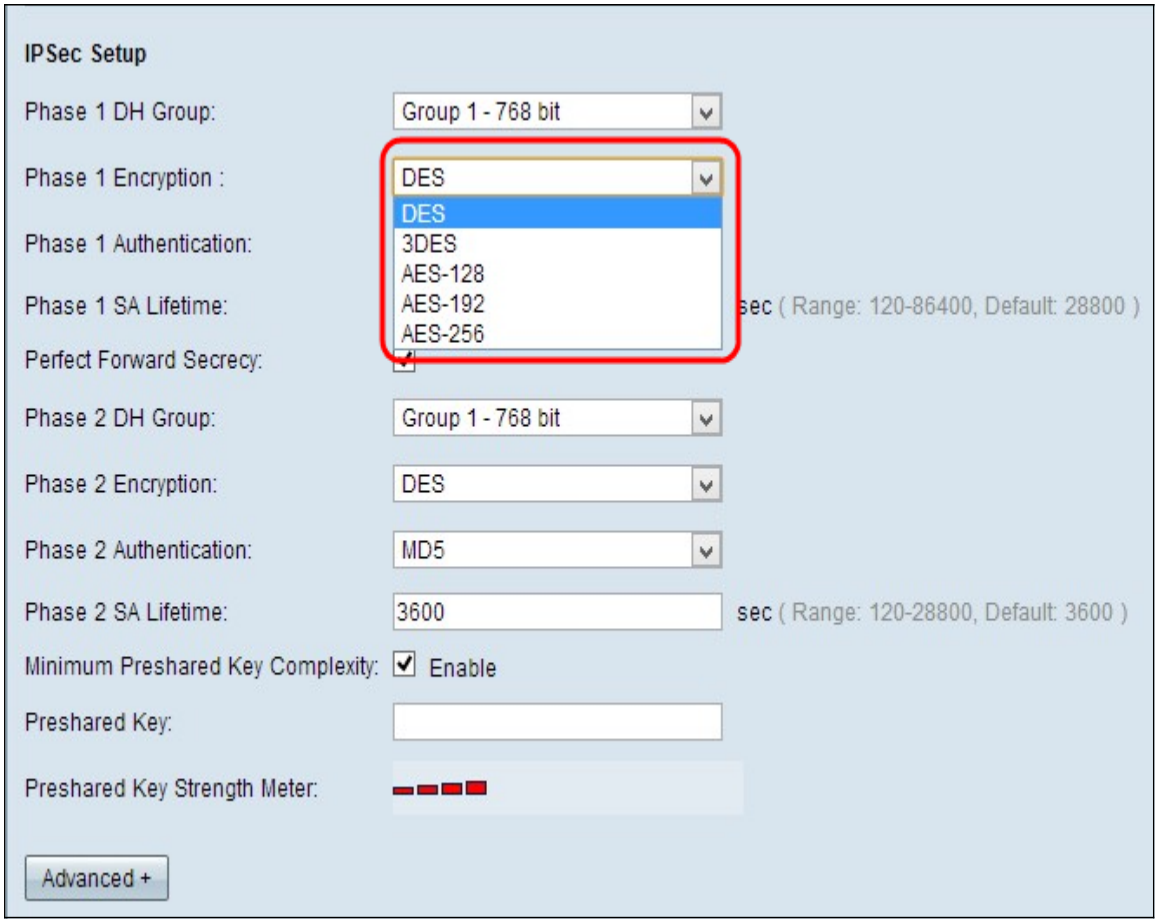
IPSec设置，使用带预共享密钥的IKE或带证书的IKE

注意：如果从“添加新隧道”(Add a New Tunnel)部分的步骤3中的“键控模式”(Keying Mode)下拉列表中选择了带预共享密钥的IKE或带证书的IKE，请执行*以下*步骤。



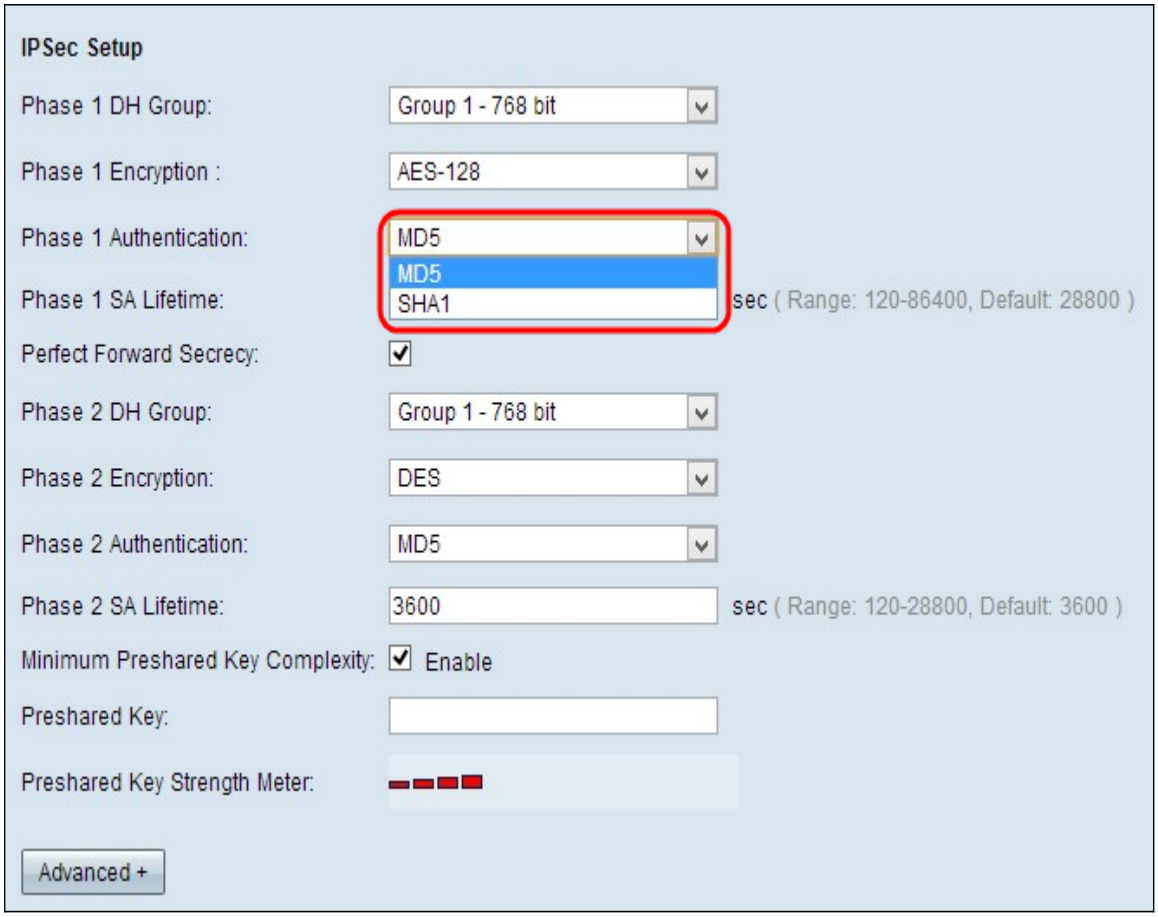
第 1 步：从 *Phase 1 DH Group（第 1 阶段 DH 组）下拉列表中选择适当的第 1 阶段 DH 组*。第1阶段用于在隧道两端之间建立单工逻辑安全关联(SA)，以支持安全可信通信。Diffie-Hellman(DH)是在第1阶段连接期间用于共享密钥以验证通信的加密密钥交换协议。

- 第 1 组 - 768 位 - 表示最低强度的密钥和最不安全的身份验证组。但是，它需要更少的时间来计算 IKE 密钥。如果网络速度较慢，则首选此选项。
- 第 2 组 - 1024 位 - 表示较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。
- 第 5 组 - 1536 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。



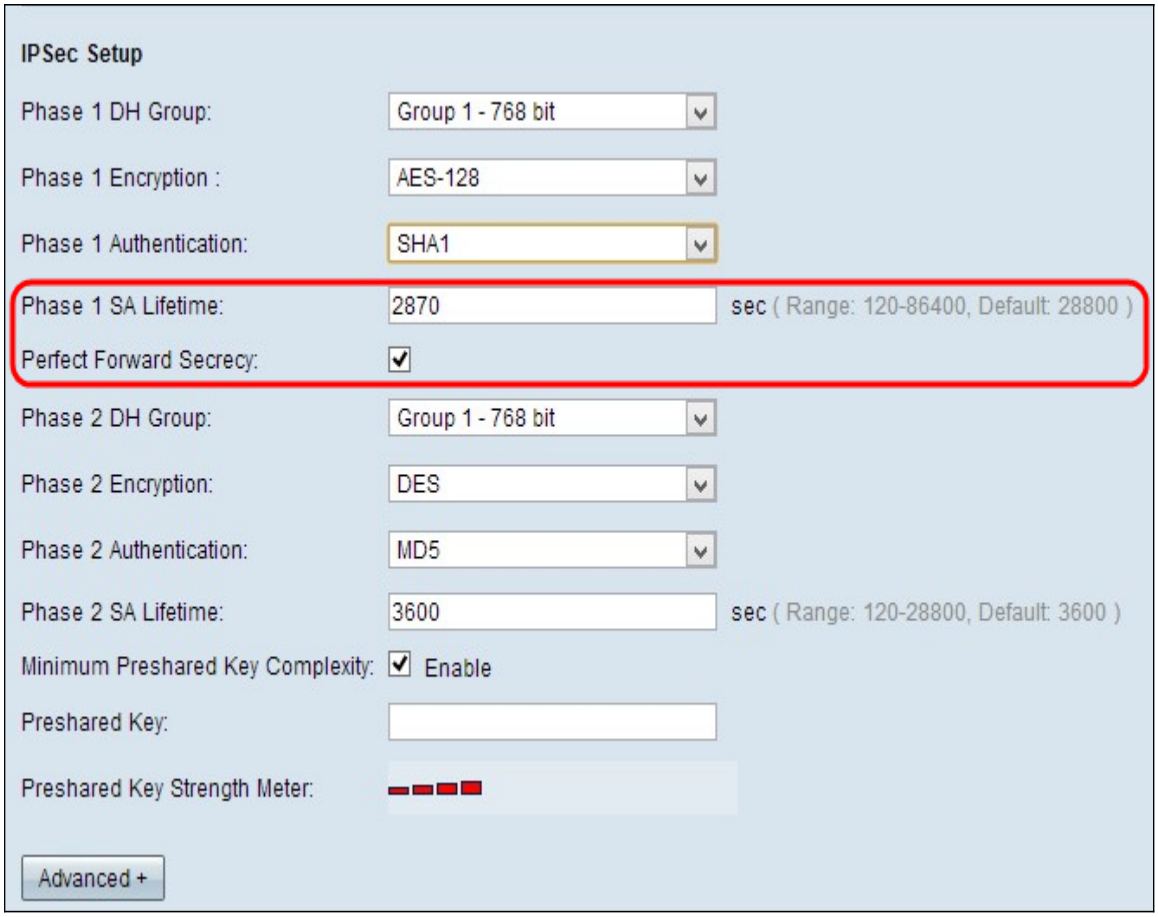
步骤2.从Phase 1 Encryption下拉列表中选择适当的Phase 1 Encryption*以加密*密钥。推荐使用 AES-256，因为它是最安全的加密方法。VPN 隧道的两端需要使用相同的加密方法。

- DES — 数据加密标准(DES)是56位，旧的加密方法，并不是非常安全的加密方法。
- 3DES — 三重数据加密标准(3DES)是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更安全。
- AES-128 — 高级加密标准(AES)是128位加密方法，通过10个重复周期将纯文本转换为密文。
- AES-192 — 高级加密标准(AES)是192位加密方法，通过12个重复周期将纯文本转换为密文。
- AES-256 — 高级加密标准(AES)是256位加密方法，通过14个重复周期将纯文本转换为密文。



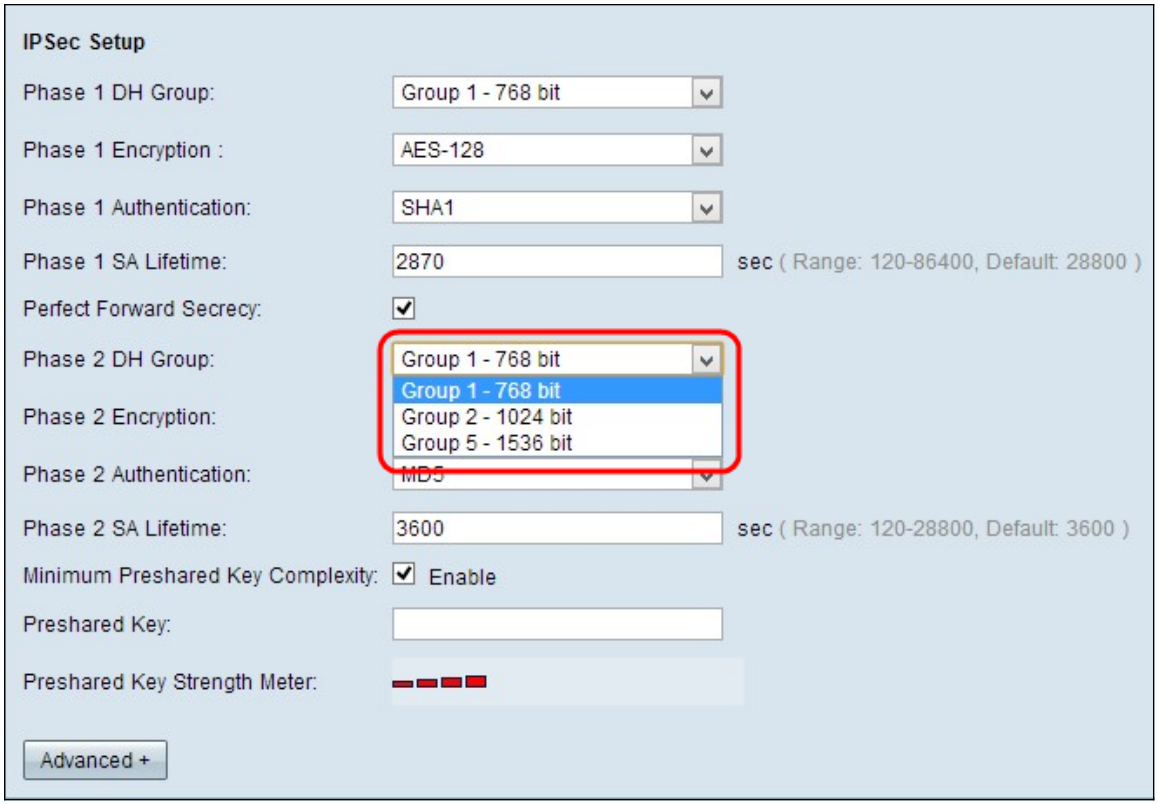
步骤3.从Phase 1 Authentication下拉列表中*选择适*当的身份验证方法。VPN 隧道的两端需要使用相同的身份验证方法。

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



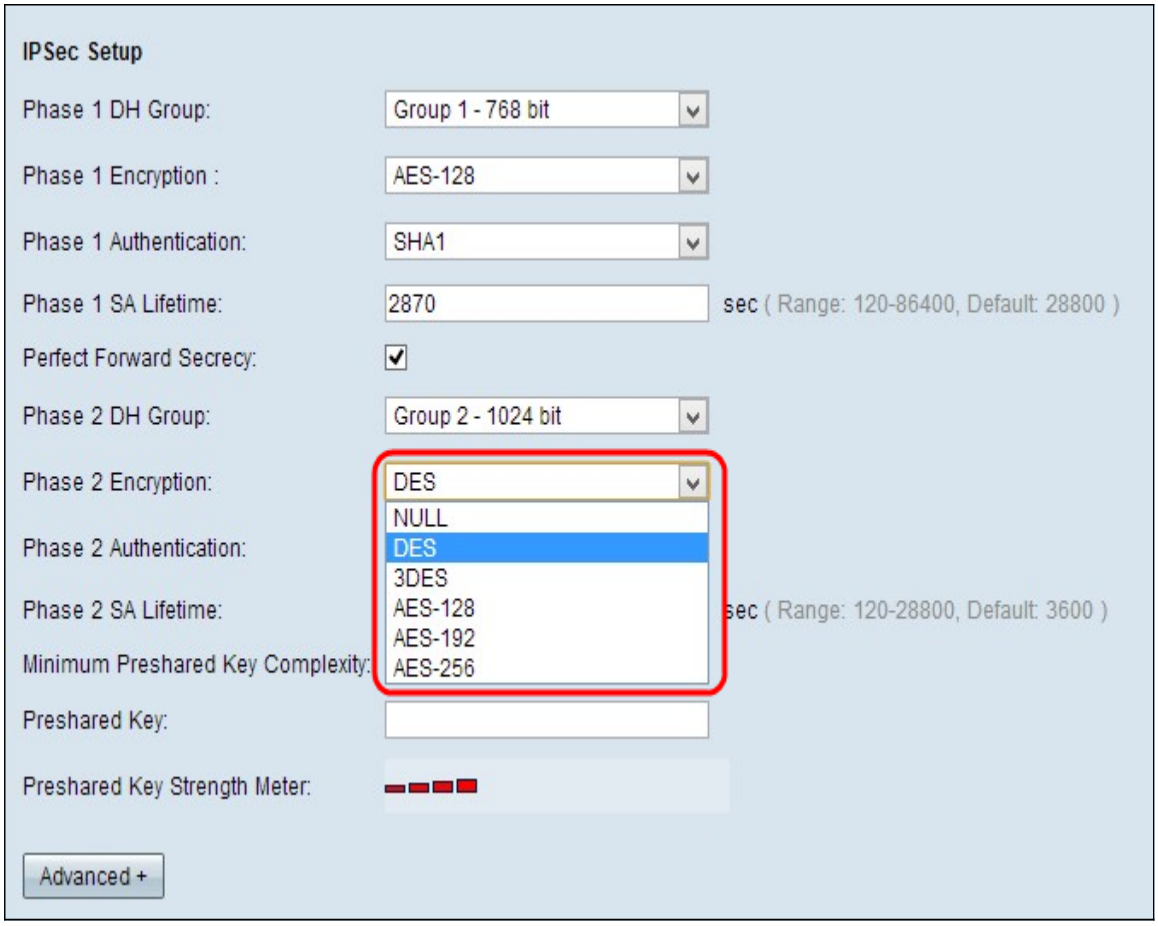
步骤4.在第1阶段，VPN隧道在第1阶段SA生命期字段中保持活*动状态，以秒*为单位。 默认时间为 28800 秒。

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。



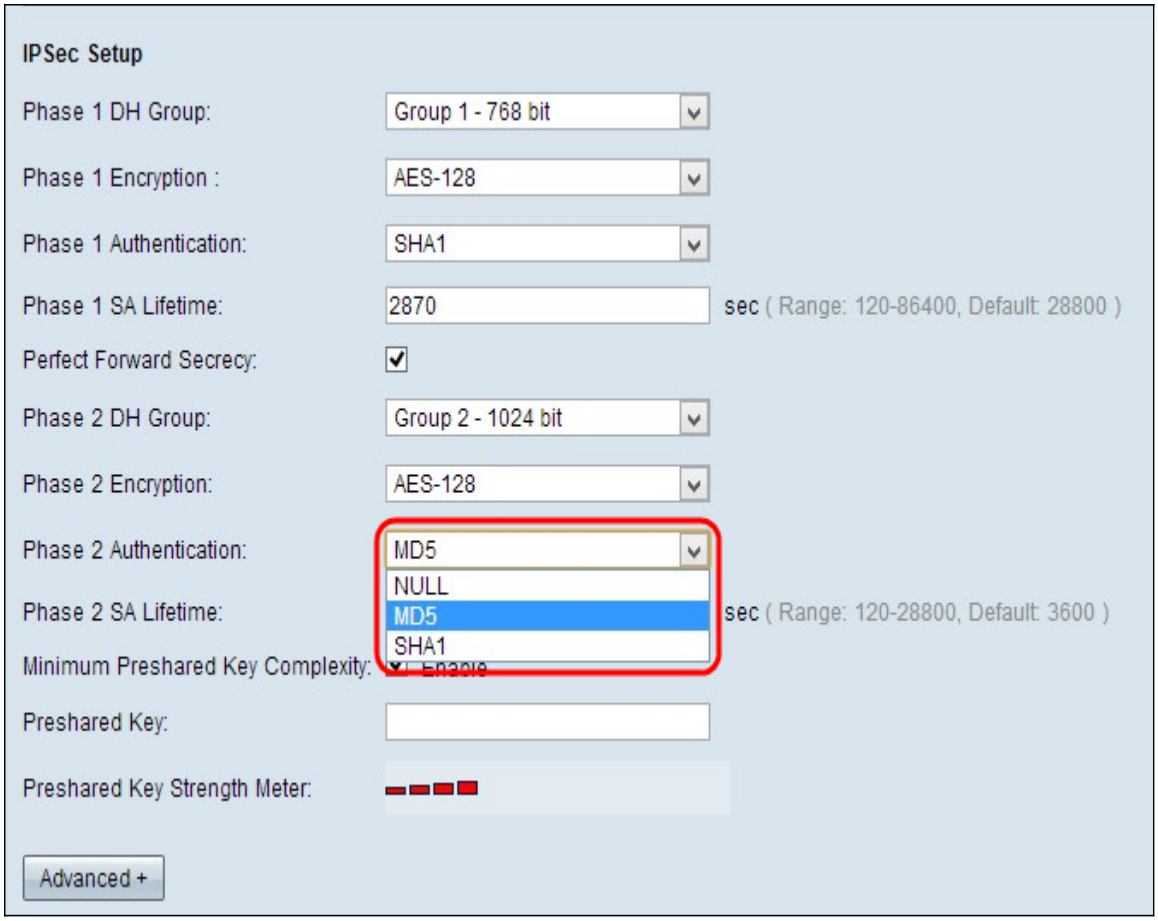
步骤6.从第2阶段DH组下拉列表中*选择适当*的第2阶段DH组。第 1 阶段用于在隧道两端之间建立单工逻辑安全关联 (SA)，以支持安全的身份验证通信。Diffie-Hellman(DH)是在第1阶段连接期间用于共享密钥以验证通信的加密密钥交换协议。

- 第 1 组 - 768 位 - 表示最低强度的密钥和最不安全的身份验证组。但是，它需要更少的时间来计算 IKE 密钥。如果网络速度较慢，则首选此选项。
- 第 2 组 - 1024 位 - 表示较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。
- 第 5 组 - 1536 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。



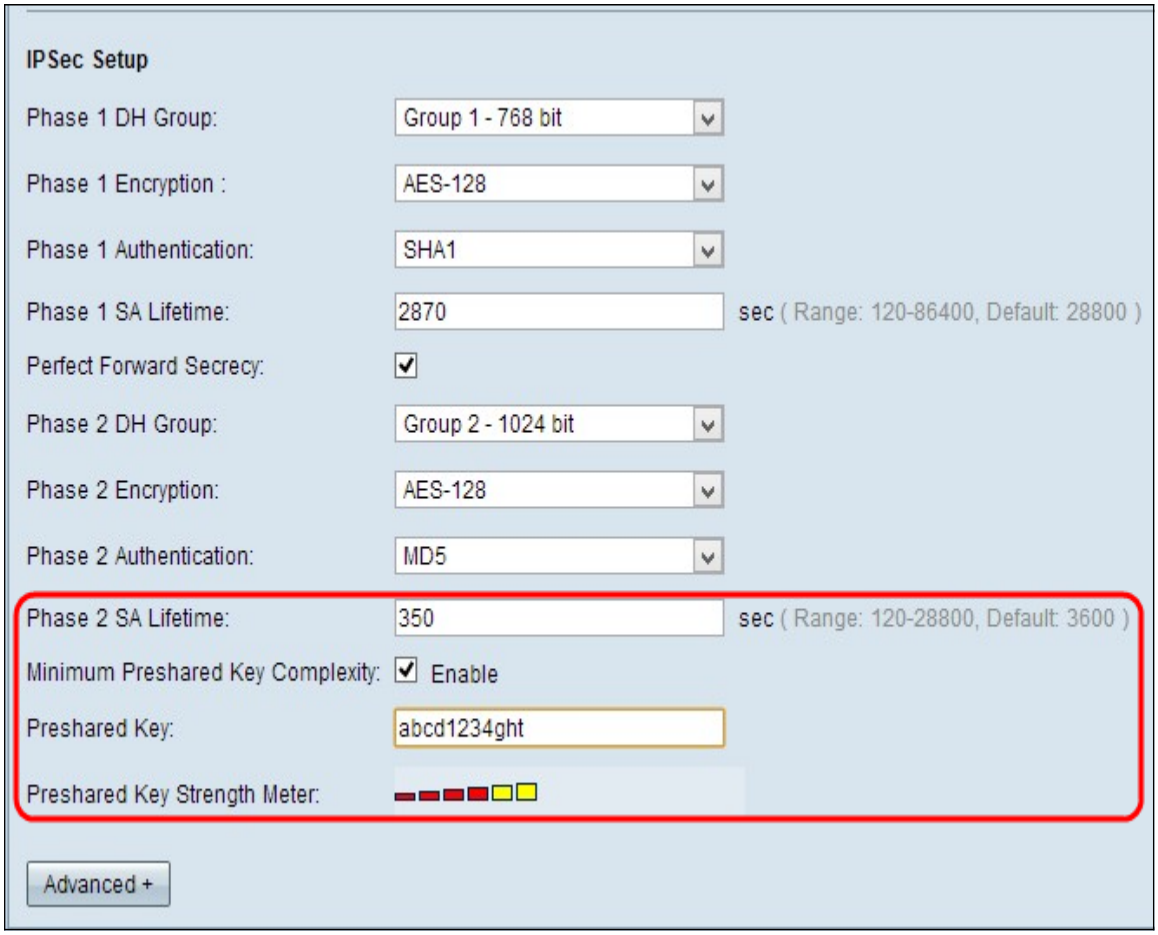
第 7 步： 从 *Phase 2 Encryption（第 2 阶段加密）下拉列表中选择适当的第 2 阶段加密来加密密钥*。推荐使用 AES-256，因为它是最安全的加密方法。VPN 隧道的两端需要使用相同的加密方法。

- DES — 数据加密标准(DES)是56位，旧的加密方法，并不是非常安全的加密方法。
- 3DES — 三重数据加密标准(3DES)是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更安全。
- 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 — 高级加密标准(AES)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 — 高级加密标准(AES)是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 — 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 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全。
- 空值 - 不使用任何验证方法。



步骤9.在第2阶段，VPN隧道在第2阶段SA生命期字段中保持活*动状态，以秒*为单位。 默认时间为 3600 秒。

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。最多可使用30个字母数字字符作为预共享密钥。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，以便VPN保持安全。

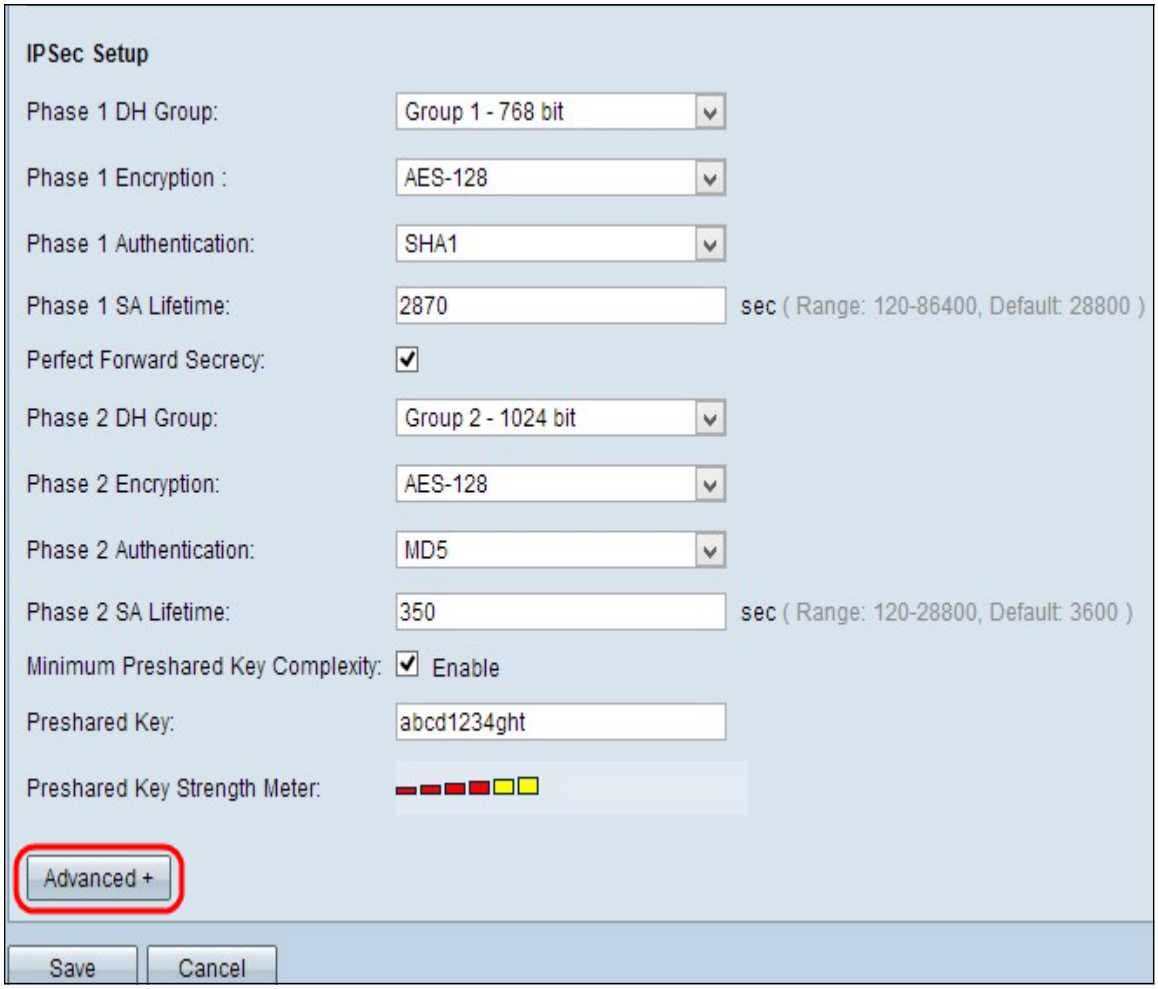
- 预共享密钥强度计 — 通过彩色条显示预共享密钥的强度。红色表示强度弱，黄色表示强度可接受，绿色表示强度高。如果在IPSec设置**步骤10中选中Minimum Preshared Key Complexity**复选框，则仅显示Preshared Key Strength Meter。

注意：如果从步骤3的*Keying Mode* 下拉列表中为*Add a New Tunnel*部分选择具有预共享密钥的IKE，则只有您可以选择配置步骤10、步骤11和查看预共享密钥强度计。

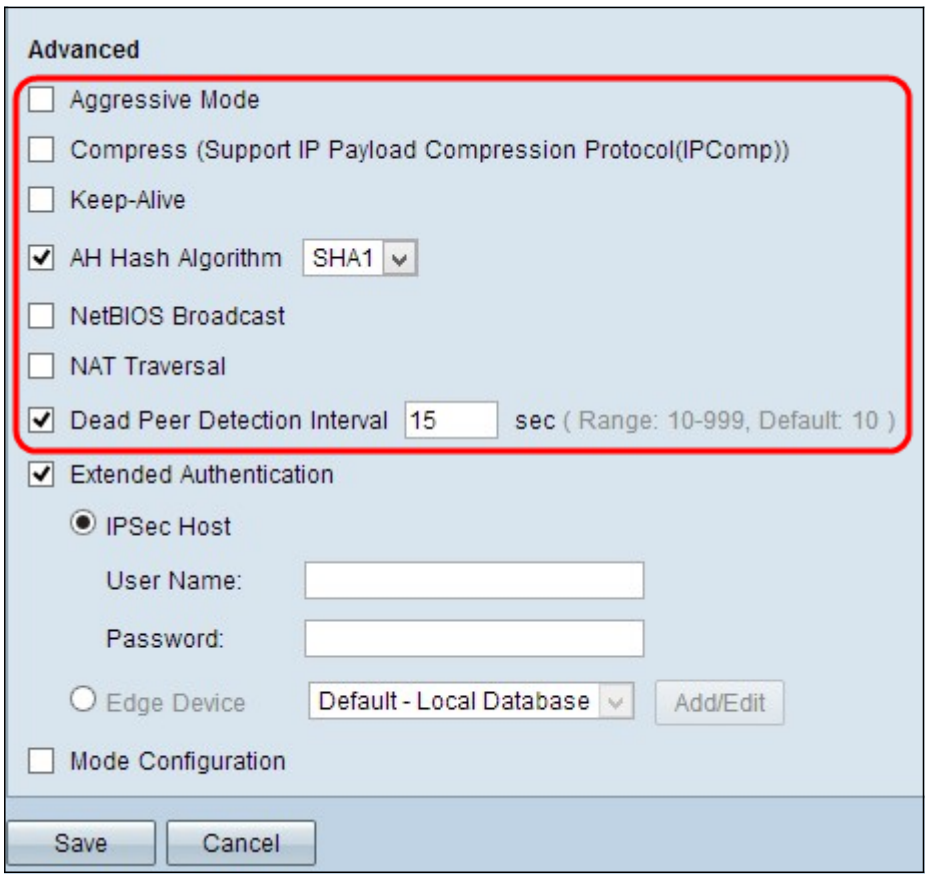
步骤12.如果要保存到目前为止的设置，请向下滚动并单击“保**存”**以保存设置。

使用带预共享密钥的IKE或带证书的IKE的高级设置

高级设置仅可用于具有预共享密钥的IKE和具有认证密钥的IKE。手动键设置没有任何高级设置。



步骤1.单击**Advanced**以获取具有预共享密钥的IKE的高级设置。



步骤2.如果网络速**度低**，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。

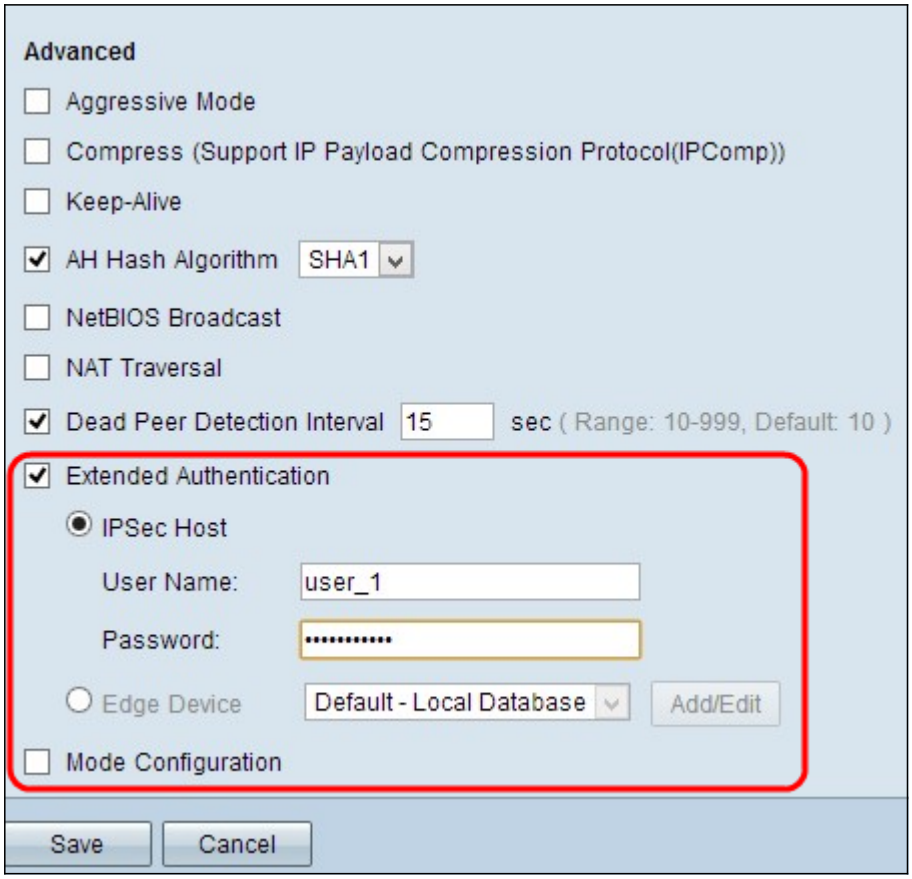
步骤5.如果要对Authenticate Header(AH)**进行身份验**证，请选中AH Hash Algorithm复选框。AH为数据源提供身份验证，通过校验和实现数据完整性并将保护扩展到IP报头。隧道两端的算法应相同。

- MD5 — 消息摘要算法5(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 — 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广播。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穿越用于将内部系统的私有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.选中**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。



步骤9.选中**Extended Authentication** ，为VPN连接提供更高的安全性和身份验证。点击适当的单选按钮以扩展VPN连接的身份验证。

- IPSec主机 — 通过IPSec主机进行扩展身份验证。如果选择此选项，请在User Name字段中输入IPSec主机的用户名，在Password字段中输入密码。
- 边缘设备 — 通过边缘设备进行扩展身份验证。如果选择此选项，请从下拉列表中选择包含边缘设备的数据库。如果要添加或编辑数据库，请单击“添加/**编辑**”。

注意：要了解有关如何添加或编辑本地数据库的详细信息，请*参阅RV320路由器上的用户和域管理配置*。

步骤 10选中**Mode Configuration**，为传入隧道请求方提供IP地址。

注意：第9步到第11步可用于隧道VPN的IKE预共享密钥模式。

步骤11.单击“**保存**”保存设置。

结论

您现在已学习了在RV32x系列VPN路由器上配置单个客户端到网关VPN的步骤

查看与本文相关的视频……

单击此处查看思科提供的其他技术讲座