在RV016、RV042、RV042G和RV082 VPN路由器上配置网关VPN的网关

目标

虚拟专用网络(VPN)用于在公共或共享互联网上的两个终端之间通过所谓的VPN隧道建立安全连接。更具体地说，网关到网关VPN连接允许两个路由器安全地彼此连接，并且一端上的客户端在逻辑上看起来好像是另一端网络的一部分。这使得数据和资源能够更轻松、更安全地通过Internet共享。

必须在两台路由器上完成配置才能启用网关到网关VPN。在两台路由器之间，应该颠倒在本地组设置和远程组设置部分中完成的配置，以便其中一个的本地组成为另一个的远程组。

本文档的目标是解释如何在RV016、RV042、RV042G和RV082 VPN系列路由器上配置网关到网关VPN。

适用设备

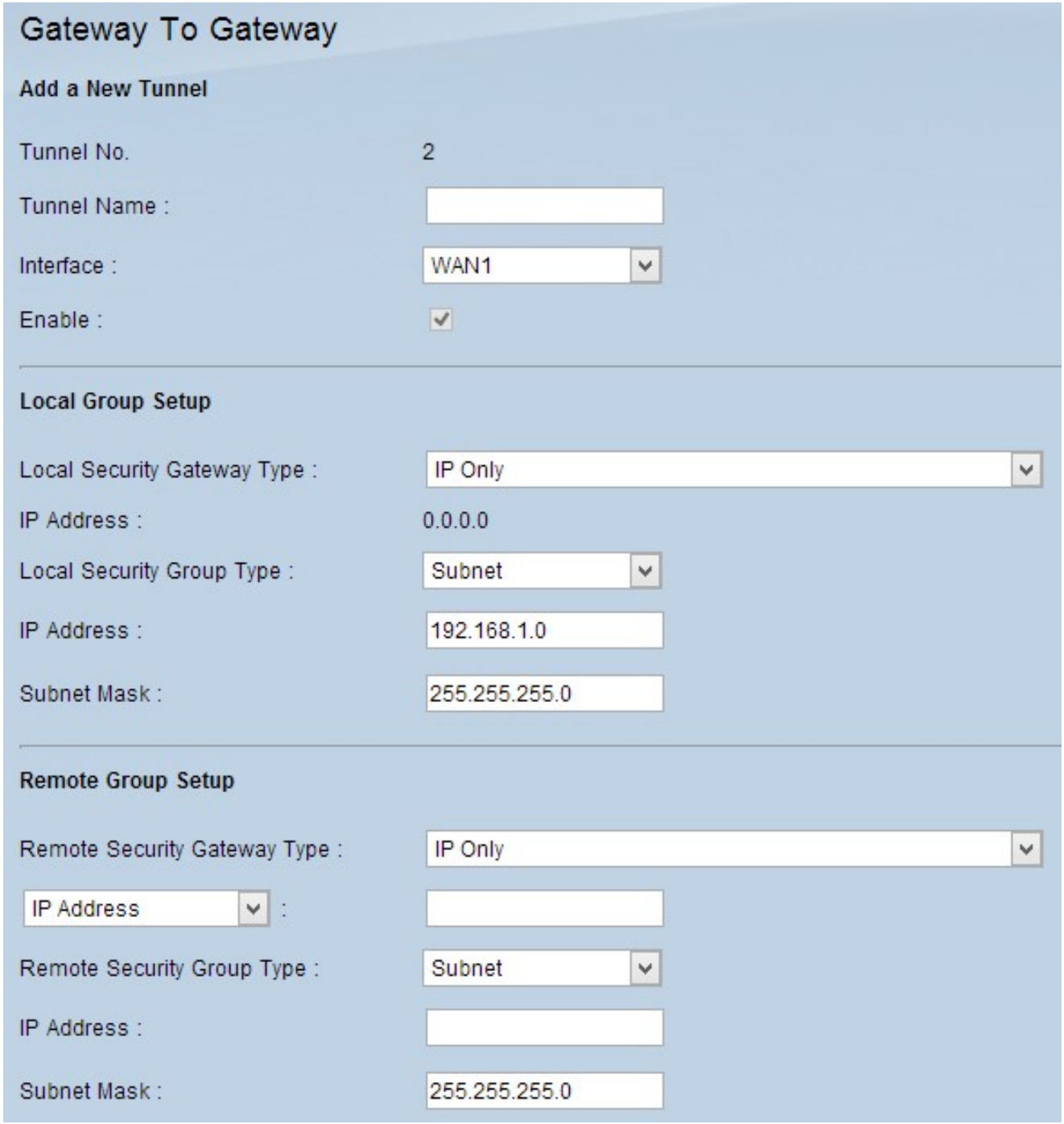
- RV016
- RV042
· RV042G
- RV082

软件版本

•v4.2.2.08

配置网关到网关VPN

步骤1:登录路由器配置实用程序并选择VPN > Gateway to Gateway。Gateway to Gateway页面打开：



要配置网关VPN的网关，需要配置以下功能：

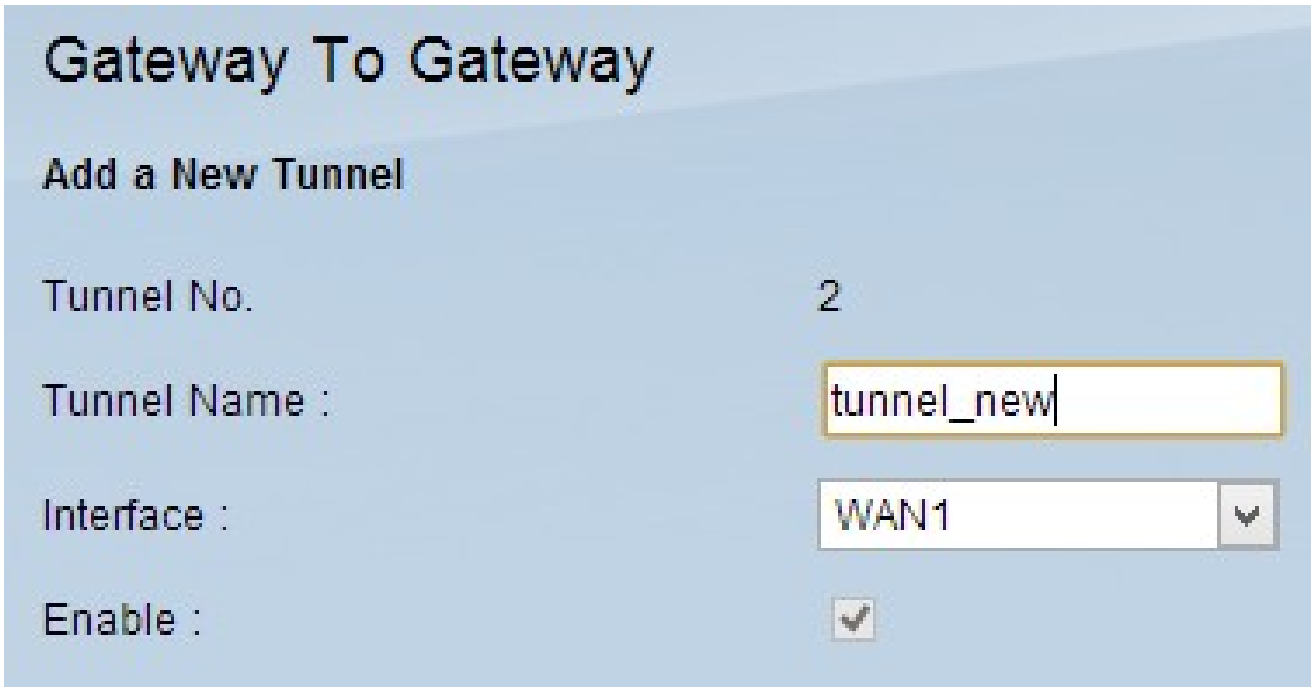
1.添加新隧道

2.本地组设置

3.远程组设置

4. IPSec设置

添加新隧道



Tunnel No.是一个只读字段，显示要创建的当前隧道。

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。

第二步：从Interface下拉列表中，选择要用于隧道的广域网(WAN)端口。

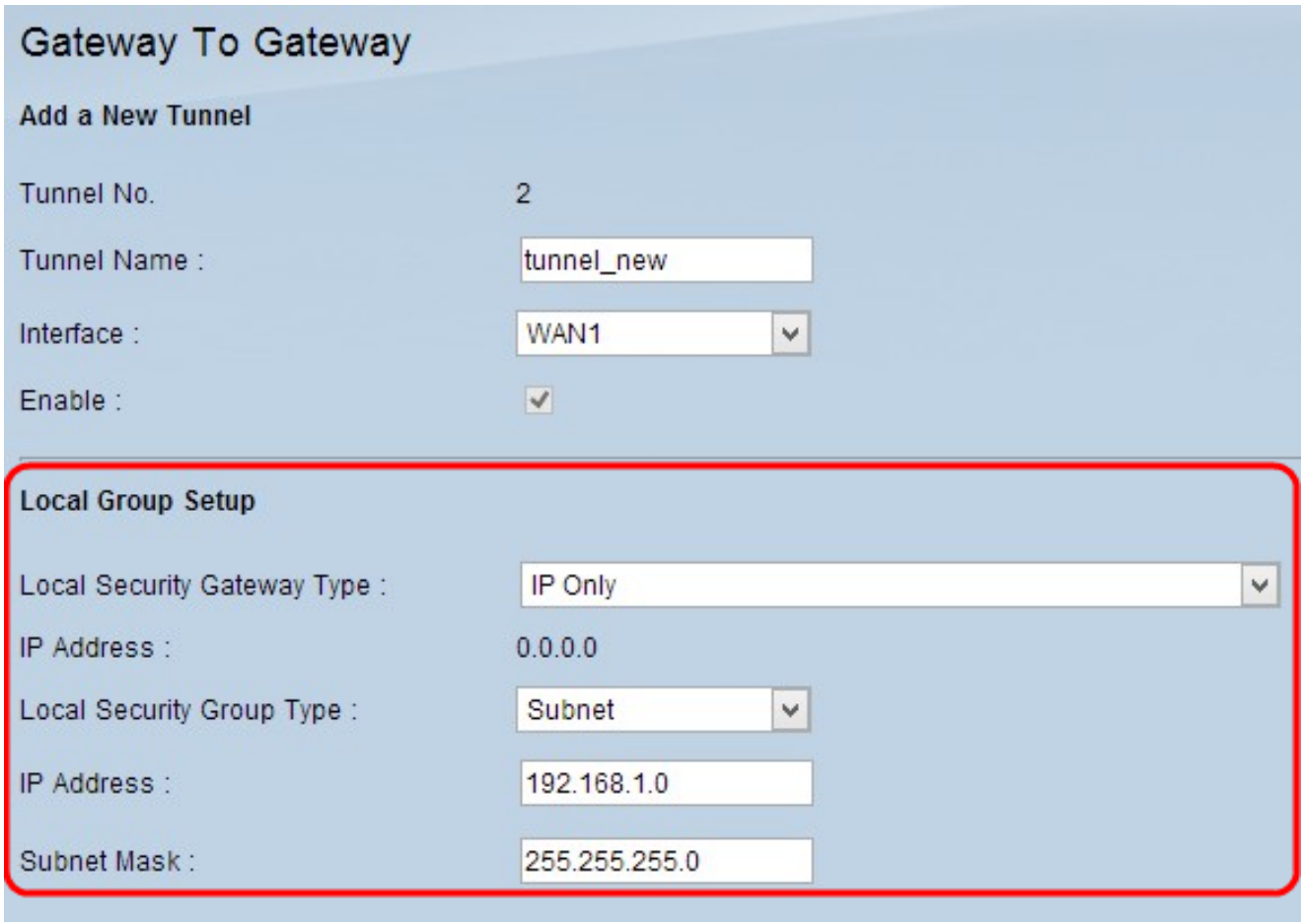
· WAN1 - RV0XX系列VPN路由器的专用WAN端口。

· WAN2 - RV0XX系列VPN路由器的WAN2/DMZ端口。仅当将其配置为WAN而非非军事区(DMZ)端口时，才会显示在下拉菜单中。

第 3 步：（可选）要启用 VPN，请选中“Enable”（启用）字段中的复选框。默认情况下，VPN处于启用状态。

本地组设置

注意：一台路由器上本地组设置的配置应与另一台路由器上远程组设置的配置相同。



步骤1: 从Local Security Gateway Type下拉列表中选择适当的路由器标识方法以建立VPN隧道。

·仅IP — 使用静态IP地址识别本地路由器（此路由器）。只有当路由器具有静态WAN IP时，才能选择此选项。静态WAN IP地址会自动显示在IP Address字段中。

· IP +域名(FQDN)身份验证 — 通过静态IP地址和注册域可以访问隧道。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地址会自动显示在IP Address字段中。

· IP +邮件地址（用户FQDN）身份验证 — 通过静态IP地址和邮件地址可以访问隧道。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地址会自动显示在IP Address字段中。

·动态IP +域名(FQDN)身份验证 — 通过动态IP地址和注册域可以访问隧道。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 — 通过动态IP地址和邮件地址可以访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。

第二步：从Local Security Group下拉列表中选择可访问VPN隧道的相应本地LAN用户或用户组。默认为子网。

· IP — 只有一个LAN设备可以访问VPN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。

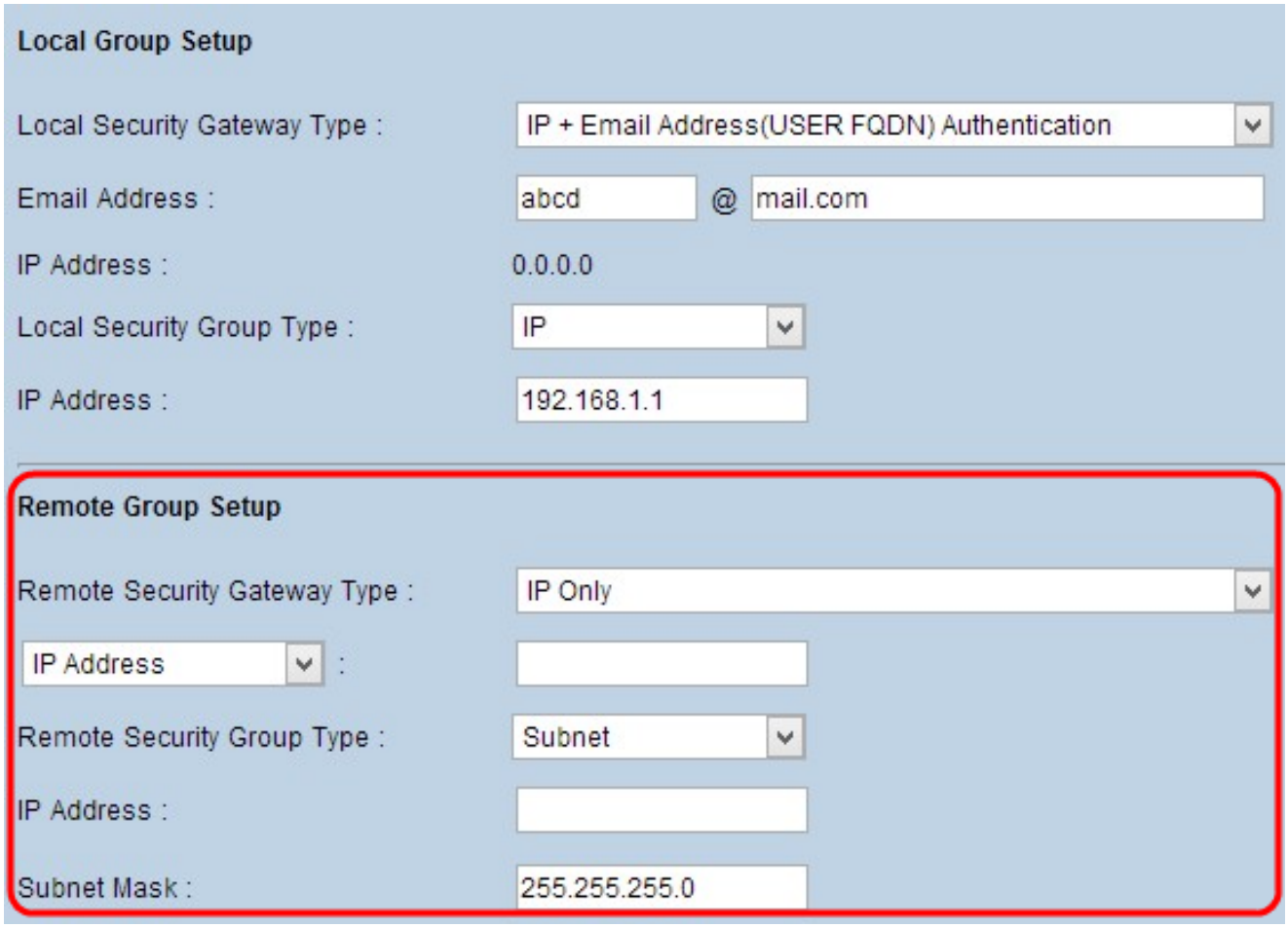
·子网 — 特定子网上的所有LAN设备均可访问隧道。如果选择此选项，请在IP地址和子网掩码字段中分别输入LAN设备的子网IP地址和子网掩码。默认掩码为 255.255.255.0。

· IP范围 — 一系列LAN设备可以访问隧道。如果选择此选项，请分别在“Begin IP”（起始 IP）和“End IP”（结束 IP）字段中输入起始和结束 IP 地址。

第三步：点击 Save（保存），以保存设置。

远程组设置

注意：一台路由器上远程组设置的配置应与另一台路由器上本地组设置的配置相同。



步骤1:从Remote Security Gateway Type下拉列表中，选择标识远程路由器以建立VPN隧道的方法。

·仅IP — 可通过静态WAN IP访问隧道。如果您知道远程路由器的IP地址，请从远程安全网关类型(Remote Security Gateway Type)字段正下方的下拉列表中选择IP地址并输入IP地址。如果您不知道IP地址但知道域名，请选择IP by DNS Resolved（按DNS解析IP），并在IP by DNS Resolved（按DNS解析IP）字段中输入路由器的域名。

· IP +域名(FQDN)身份验证 — 通过路由器的静态IP地址和注册域可以访问隧道。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，请选择IP by DNS Resolved（按DNS解析IP），并在IP by DNS Resolved（按DNS解析IP）字段中输入路由器的域名。在Domain Name（域名）字段中输入路由器的域名，无论您选择使用哪种方法识别它。

· IP +邮件地址（用户FQDN）身份验证 — 通过静态IP地址和邮件地址可以访问隧道。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，请选择IP by DNS Resolved（按DNS解析IP），并在IP by DNS Resolved（按DNS解析IP）字段中输入路由器的域名。在Email Address字段中输入电子邮件地址。

·动态IP +域名(FQDN)身份验证 — 通过动态IP地址和注册域可以访问隧道。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 — 通过动态IP地址和邮件地址可以访问隧道。如果选择此选项，请在“Email Address”（邮件地址）字段中输入邮件地址。

第二步：从Remote Security Group Type下拉列表中选择可访问VPN隧道的适当远程LAN用户或用户组。

· IP — 只有一台特定的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。

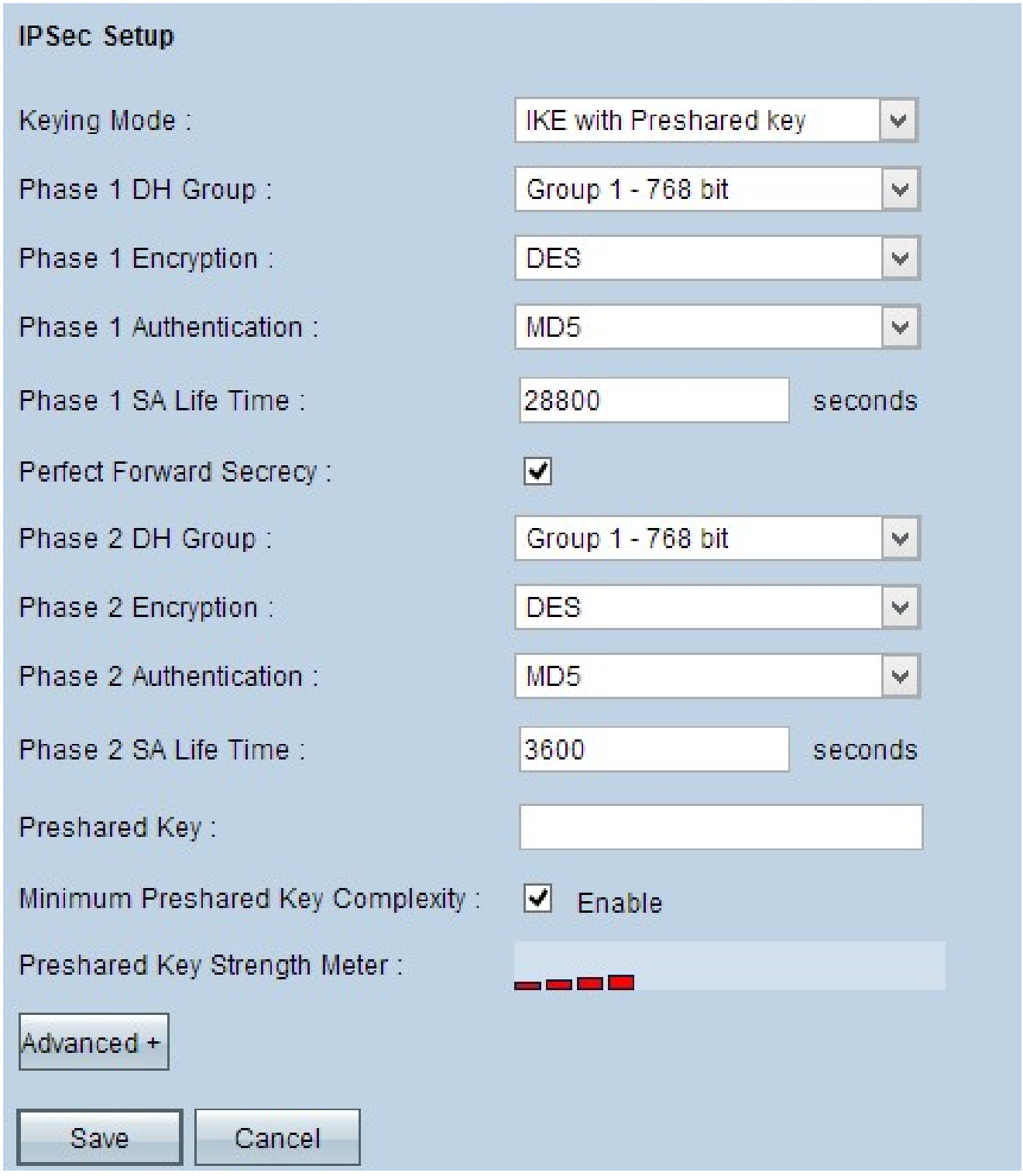
·子网 — 特定子网上的所有LAN设备均可访问隧道。如果选择此选项，请在IP地址和子网掩码字段中分别输入LAN设备的子网IP地址和子网掩码。

· IP范围 — 一系列LAN设备可以访问隧道。如果选择此选项，请分别在“Begin IP”（起始IP）和“End IP”（结束 IP）字段中输入起始和结束 IP 地址。

注意：隧道两端的两台路由器不能位于同一子网上。

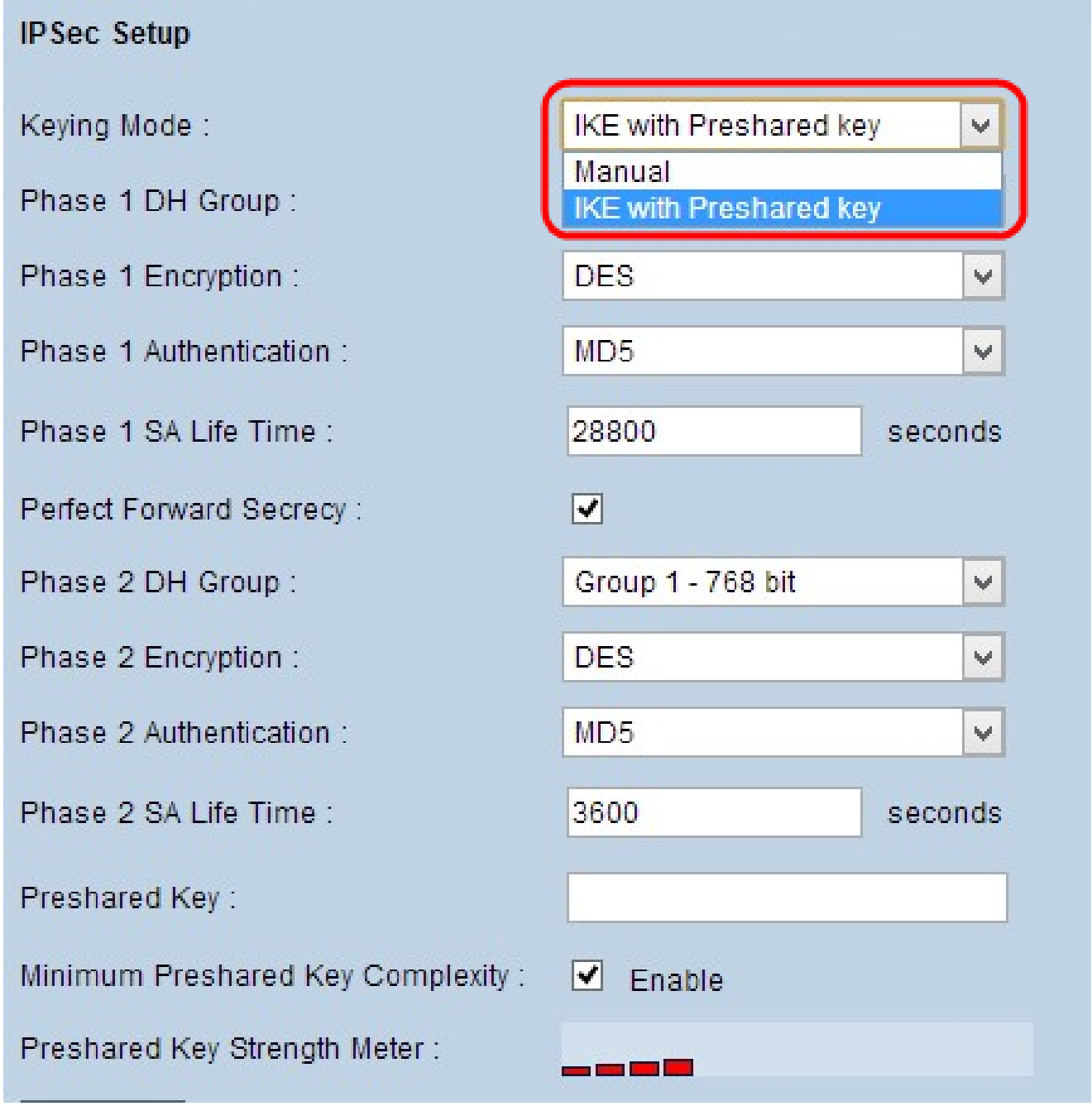
第三步：点击 Save（保存），以保存设置。

IPSec 设置选项



互联网协议安全（IPSec）是一种互联网层安全协议，其在任何通信会话期间通过身份验证和加密提供端到端安全。

注意：VPN的两端都需要使用相同的加密、解密和身份验证方法才能正常工作。为两台路由器输入相同的IPSec设置设置。

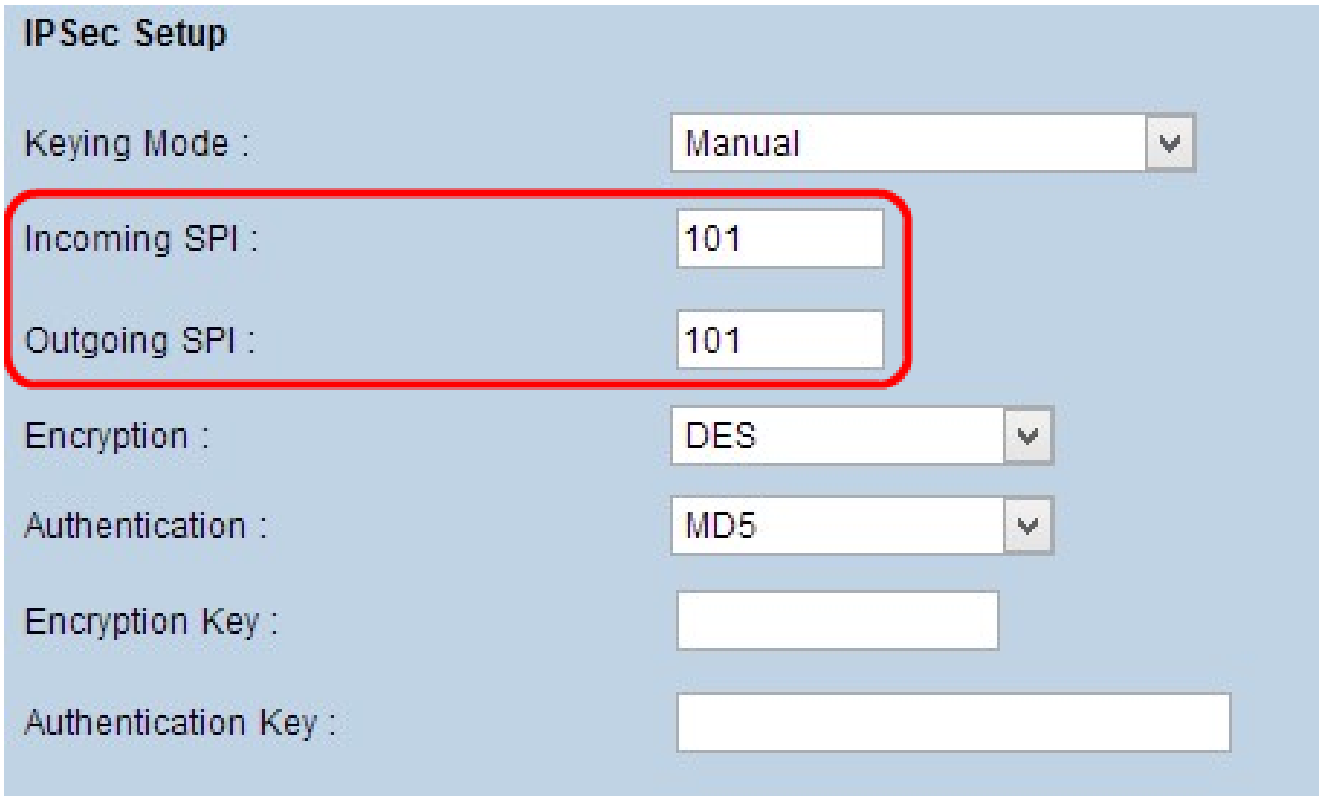


步骤1:从Keying Mode下拉列表中选择适当的密钥管理模式以确保安全性。默认模式为 IKE with Preshared key（带预共享密钥的 IKE）。

· 手动 — 自定义安全模式，可自行生成新的安全密钥，而无需与密钥协商。在故障排除期间和小型静态环境中最好使用该工具。

· 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，以建立隧道的身份验证通信。

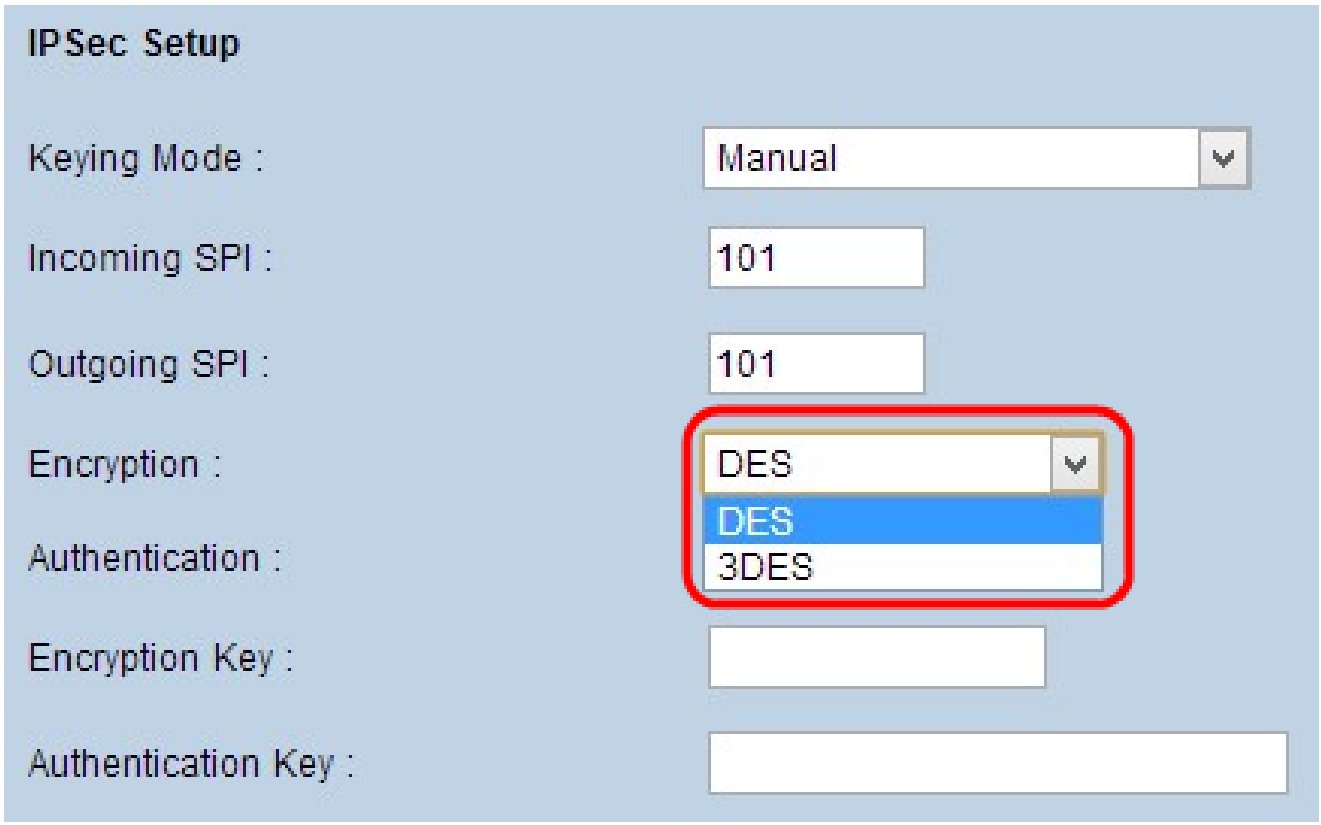
手动键控模式的IPSec设置



步骤1:在Incoming 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)报头中传输，并确定对传入数据包的保护。您可以输入一个介于100到ffffff之间的值。本地路由器的传入SPI必须与远程路由器的传出SPI匹配。

第二步：在Outgoing SPI字段中输入传出安全参数索引(SPI)的唯一十六进制值。 您可以输入一个介于100到ffffff之间的值。远程路由器的传出 SPI 需要与本地路由器的传入 SPI 匹配。

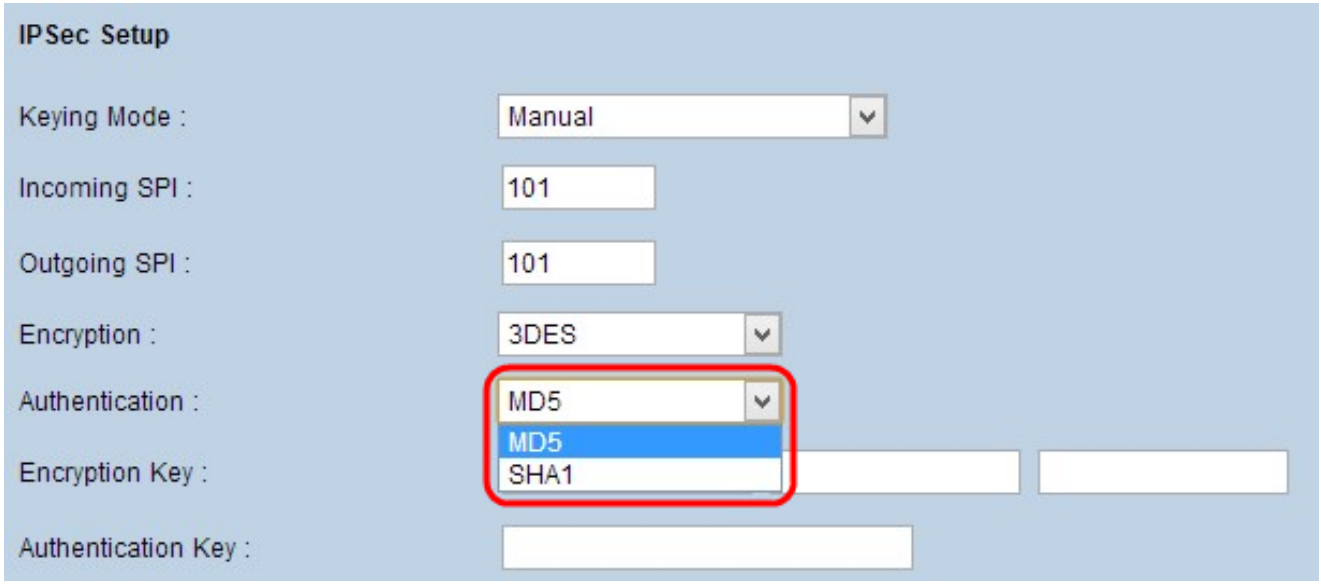
注意：两个隧道不能具有相同的SPI。



第三步：从Encryption下拉列表中选择数据的适当加密方法。推荐的加密方法为 3DES。VPN隧道需要在两端使用相同的加密方法。

· DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持 DES 时，才应使用此方法。

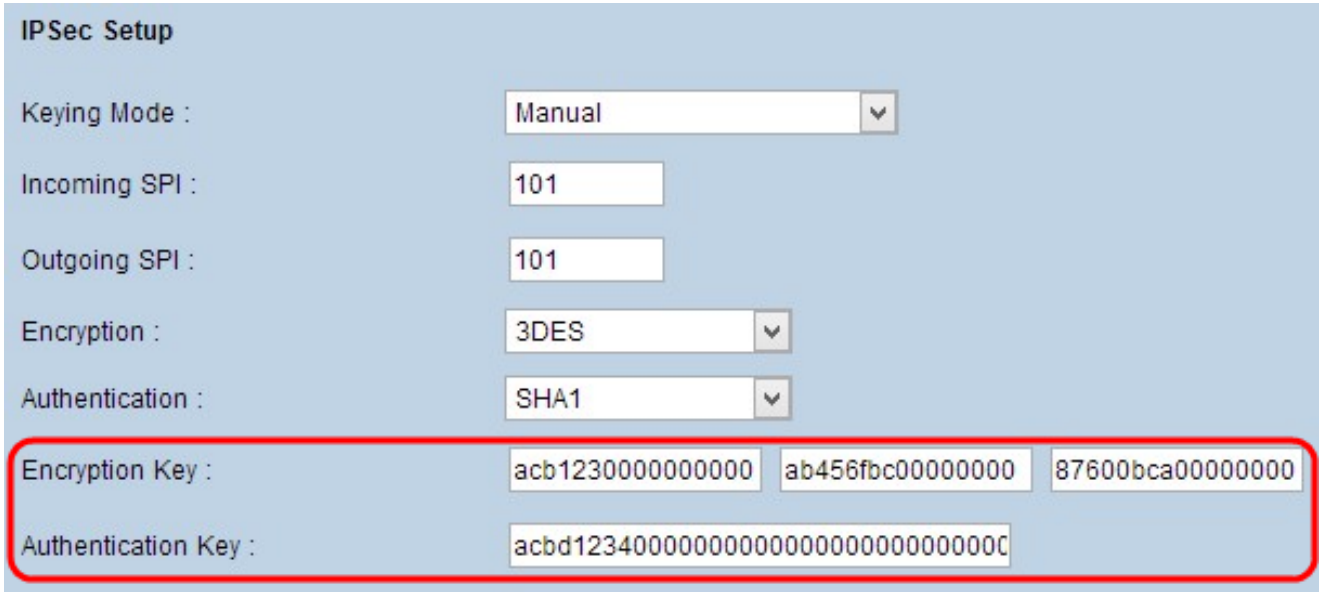
· 3DES — 三重数据加密标准(3DES)是一种168位、简单的加密方法。3DES 对数据进行三次加密，可提供比 DES 更高的安全性 。



第四步： 从Authentication下拉列表中选择数据的相应身份验证方法。推荐的身份验证是SHA1，因为它比MD5更安全。 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)是一个128位的哈希函数，通过计算校验和来保护数据免受恶意攻击。

· SHA1 — 安全散列算法版本1(SHA1)是一个160位散列函数，比MD5更安全，但计算时间更长。

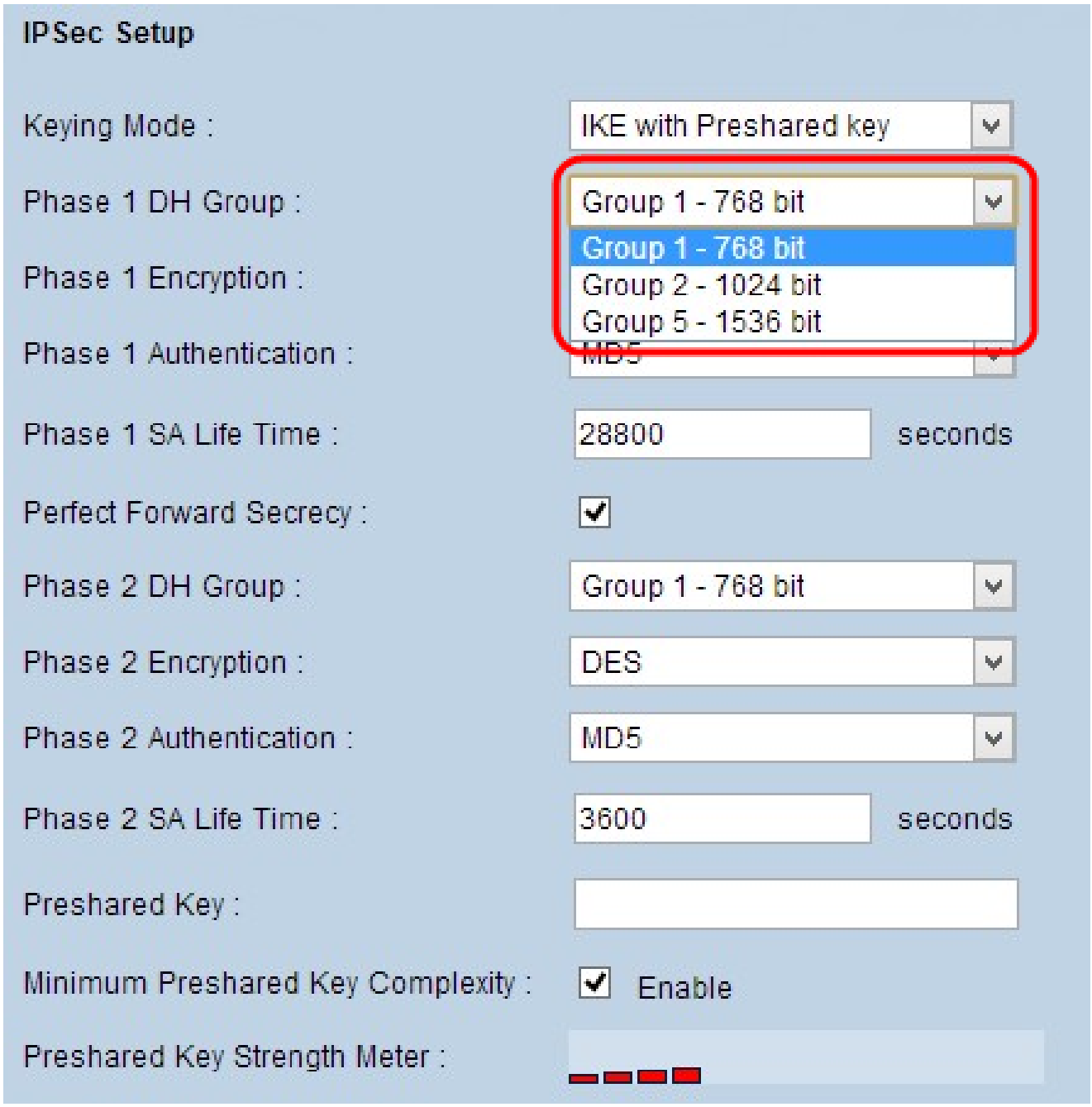


第五步：在Encryption Key字段中输入要加密和解密数据的密钥。如果您在第 3 步中选择 DES 作为加密方法，请输入 16 位十六进制值。如果您在第 3 步中选择 3DES 作为加密方法，请输入 40 位十六进制值。

第六步：在Authentication Key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。如果在步骤4中选择SHA1作为身份验证方法，请输入40位十六进制值。如果添加的数字不足，则在数字不足之前会附加零。VPN隧道需要为两端使用相同的预共享密钥。

步骤 7.点击 Save（保存），以保存设置。

带预共享密钥的 IKE 模式配置

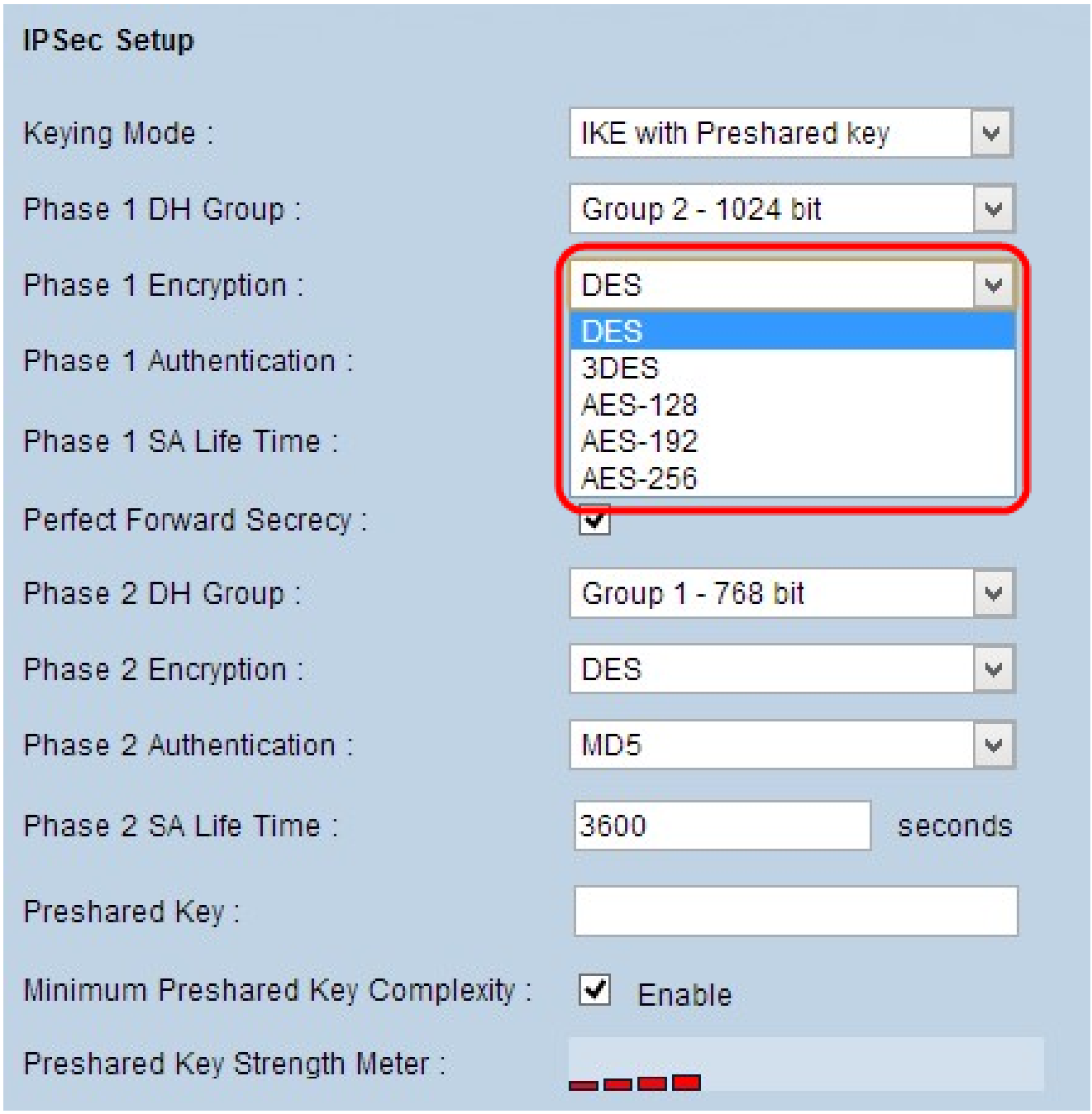


步骤1:从Phase 1 DH Group下拉列表中选择适当的阶段1 DH组。第 1 阶段用于在隧道两端之间建立单工逻辑安全关联 (SA)，以支持安全的身份验证通信。Diffie-hellman (DH) 是一种加密密钥交换协议，用于在第 1 阶段确定密钥强度并共享密钥以验证通信。

·组1 - 768位 — 强度最低的密钥和最不安全的身份验证组，但计算IKE密钥所需的时间最少。如果网络速度较慢，则首选此选项。

·组2 - 1024位 — 比组1强度更高的密钥和更安全的身份验证组，但计算IKE密钥需要更多时间。

·组5 - 1536位 — 强度最高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。



第二步： 从Phase 1 Encryption下拉列表中选择相应的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。

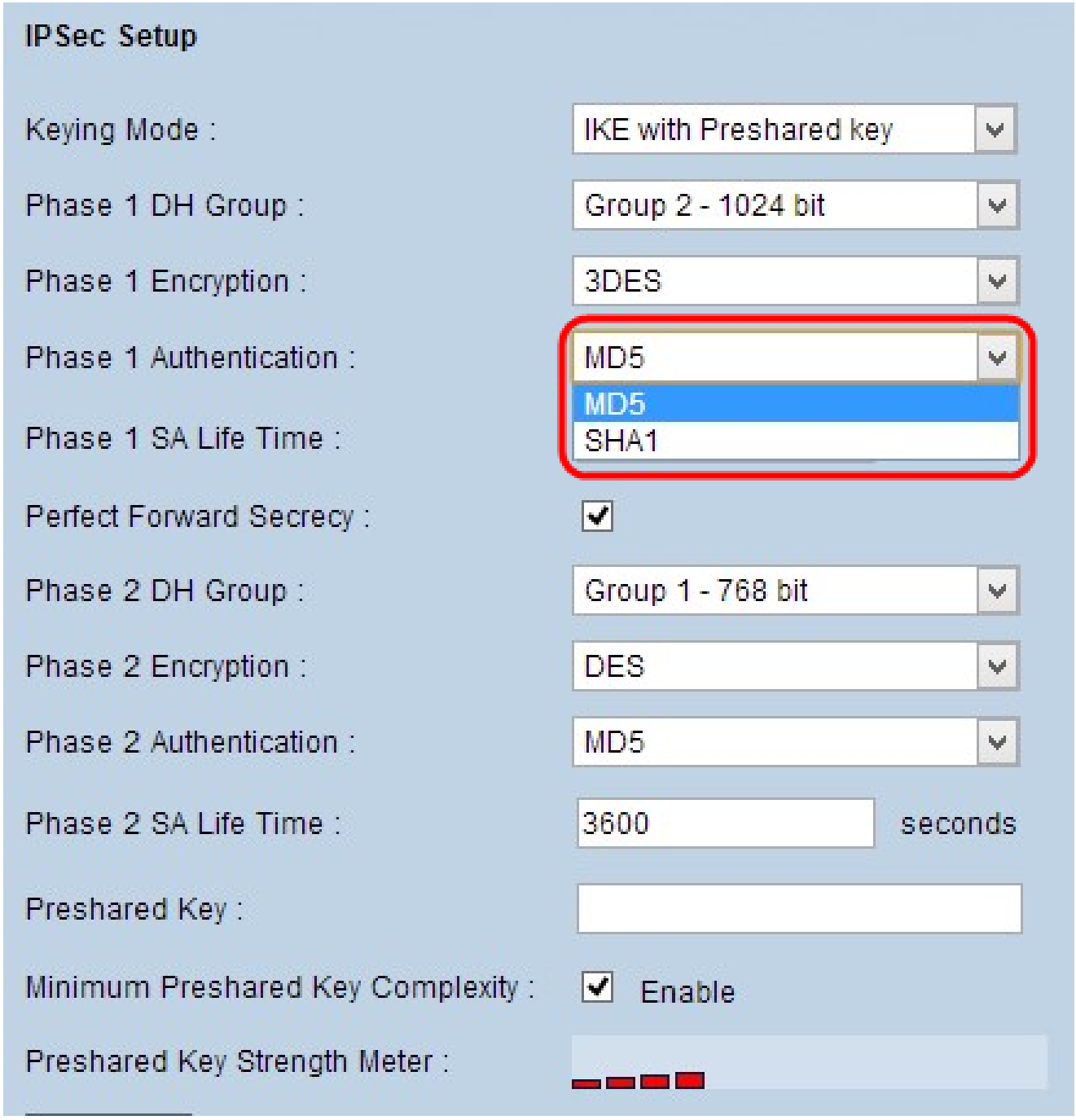
· DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持 DES 时，才应使用此方法。

· 3DES — 三重数据加密标准(3DES)是一种168位、简单的加密方法。3DES 对数据进行三次加密，可提供比 DES 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个周期的重复将纯文本转换为加密文本。

· AES-192 — 高级加密标准(AES)是192位加密方法，它通过12个周期的重复将纯文本转换为加密文本。AES-192 比 AES-128 更安全。

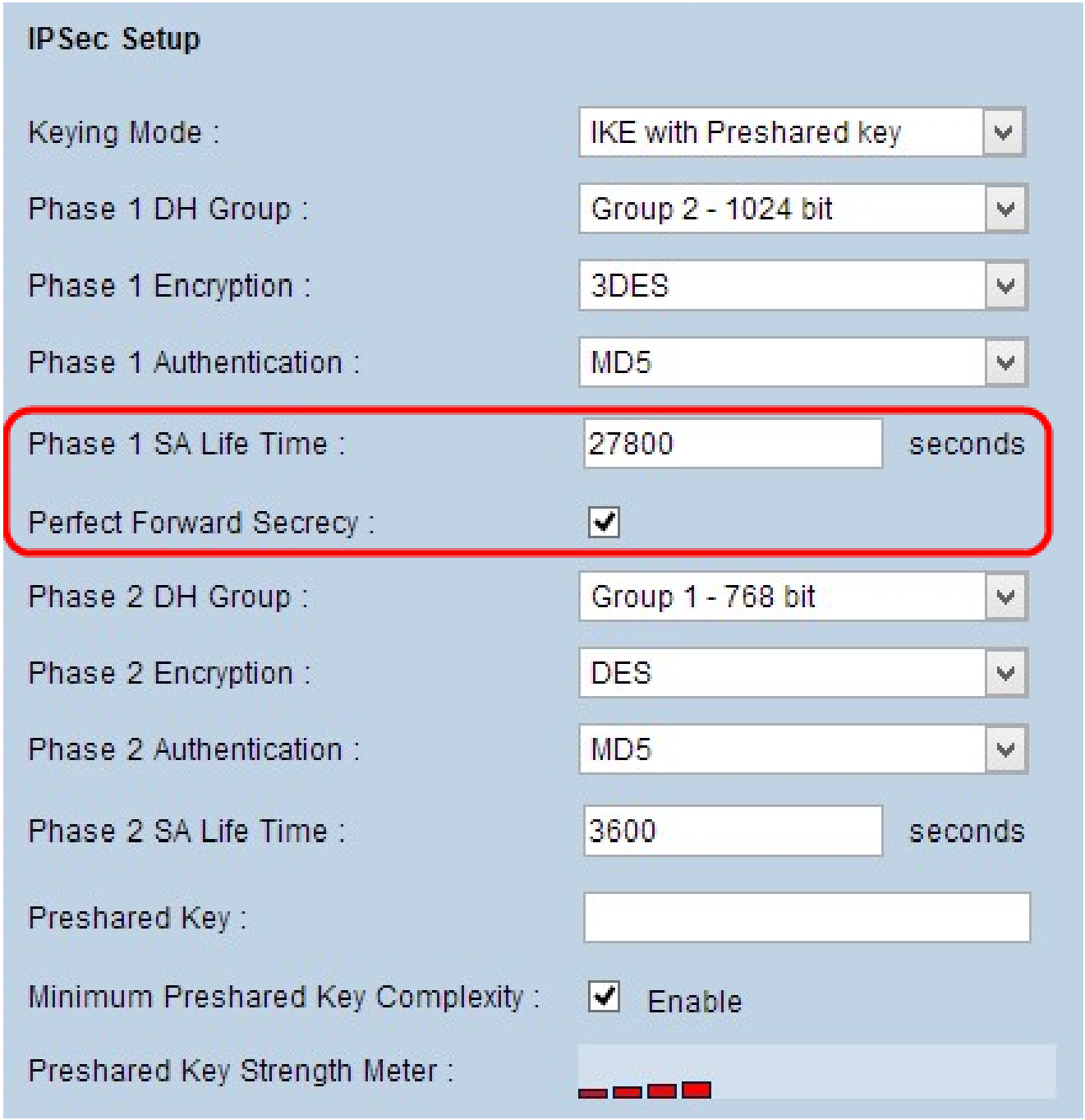
· AES-256 — 高级加密标准(AES)是256位加密方法，它通过14个周期的重复将纯文本转换为加密文本。AES-256 是最安全的加密方法。



第三步：从Phase 1 Authentication下拉列表中选择适当的阶段1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。

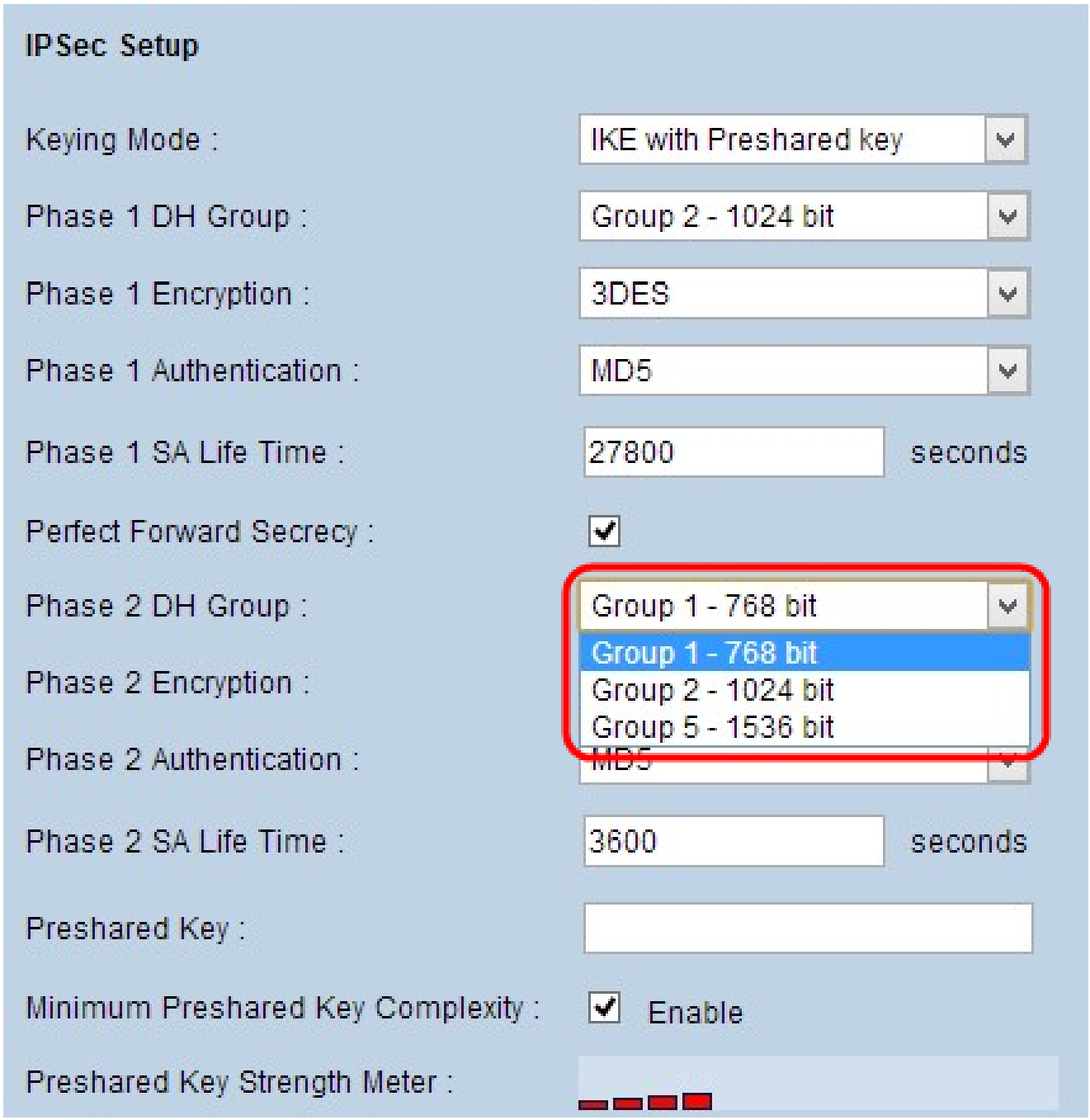
· MD5 — 消息摘要算法–5(MD5)是一个128位的哈希函数，通过计算校验和来保护数据免受恶意攻击。

· SHA1 — 安全散列算法版本1(SHA1)是一个160位散列函数，比MD5更安全，但计算时间更长。



第四步：在Phase 1 SA Life Time字段中，输入第1阶段密钥有效且VPN隧道保持活动状态的时间量（以秒为单位）。

第五步：选中 Perfect Forward Secrecy（完全向前保密）复选框，为密钥提供更多保护。如果任何密钥被盗取，此选项允许路由器生成新密钥。加密的数据只会通过被盗取的密钥泄露。推荐采取此操作，因为它可以提供更高的安全性。

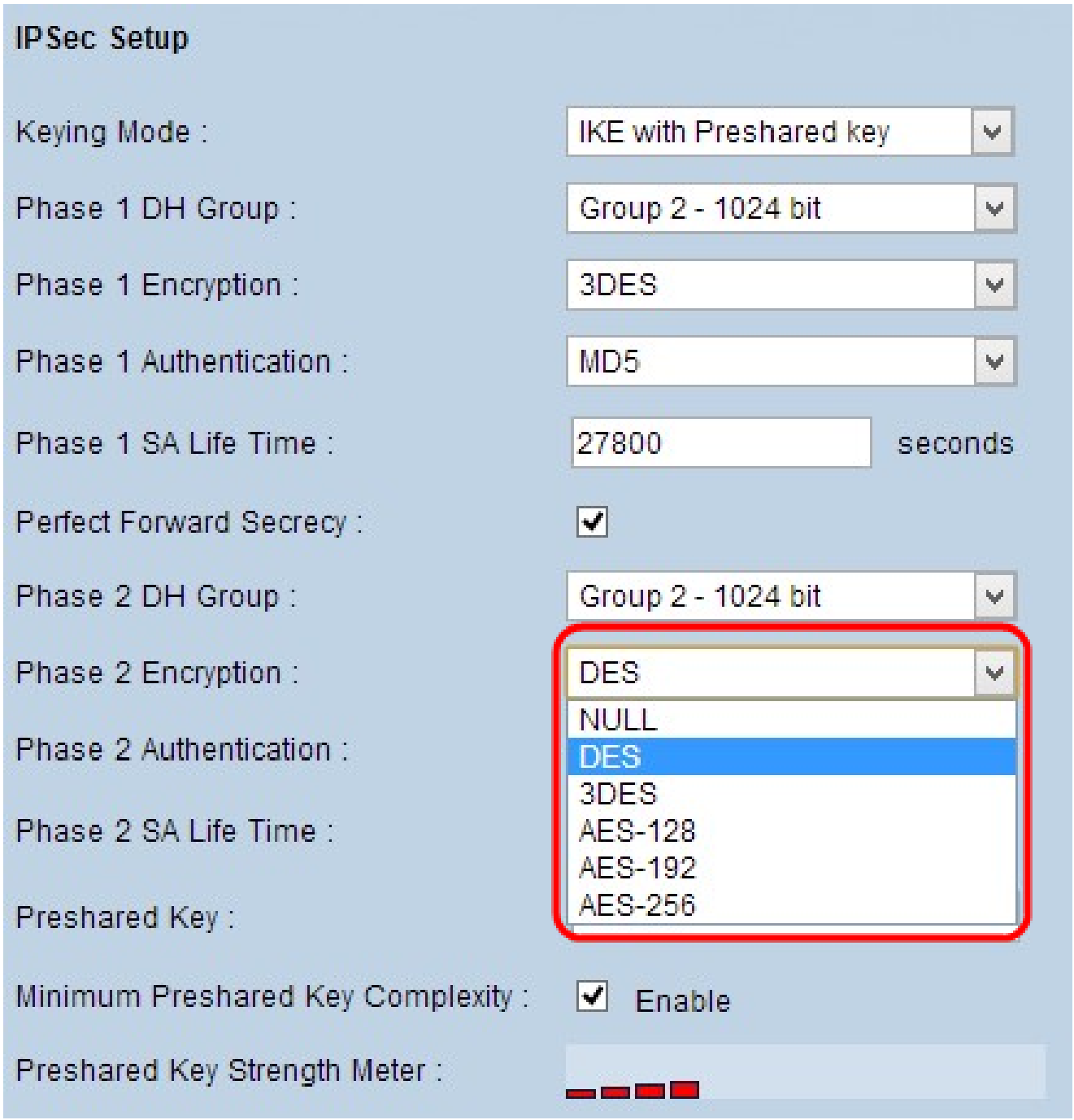


第六步： 从Phase 2 DH Group下拉列表中选择适当的第2阶段DH组。第2阶段使用安全关联，用于确定数据包经过两个端点时的安全性。

·组1 - 768位 — 强度最低的密钥和最不安全的身份验证组，但计算IKE密钥所需的时间最少。如果网络速度较慢，则首选此选项。

·组2 - 1024位 — 比组1强度更高的密钥和更安全的身份验证组，但计算IKE密钥需要更多时间。

·组5 - 1536位 — 强度最高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 7. 从Phase 2 Encryption下拉列表中选择相应的Phase 2 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。

· NULL — 不使用加密。

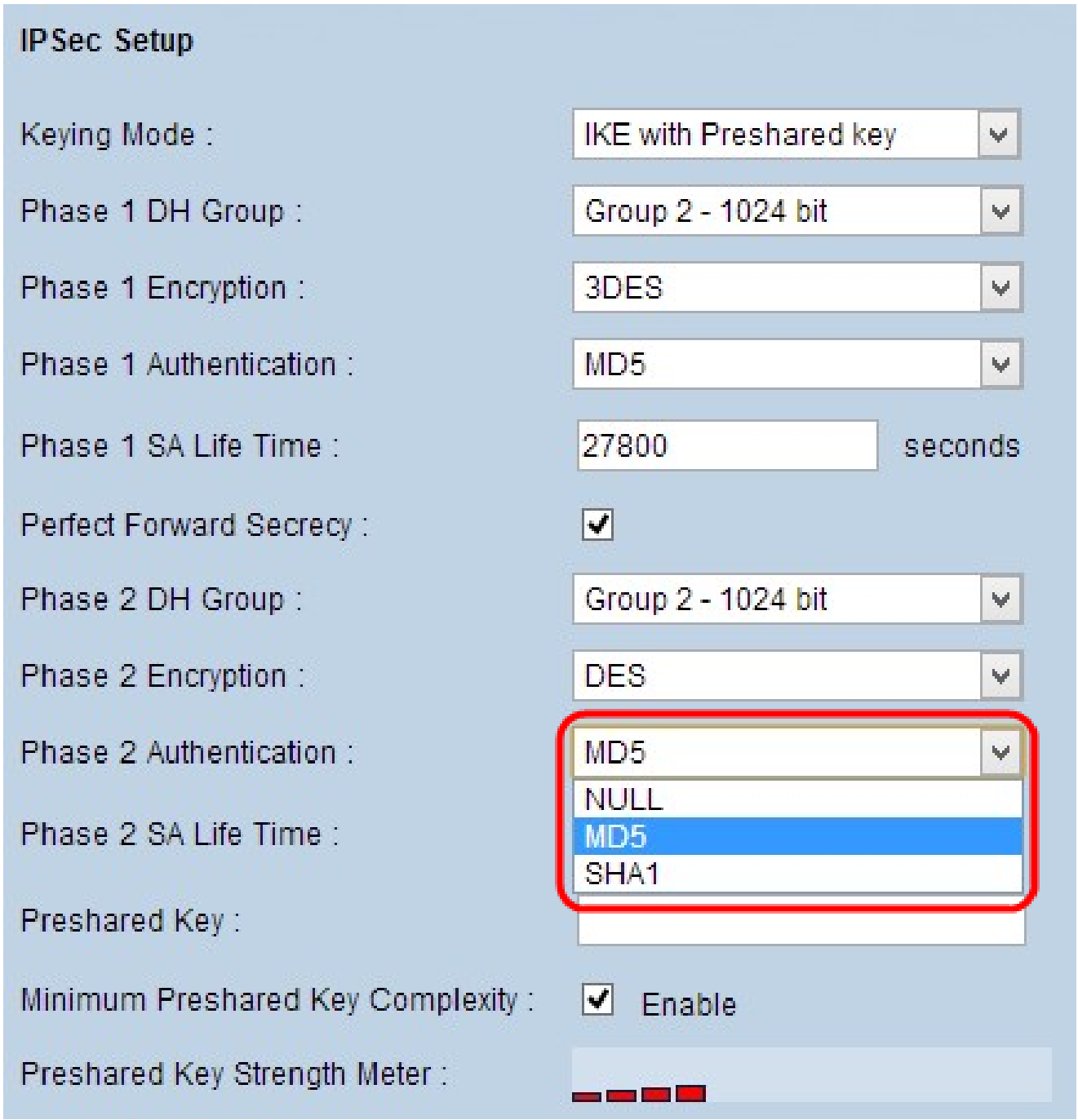
· DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持 DES 时，才应使用此方法。

· 3DES — 三重数据加密标准(3DES)是一种168位、简单的加密方法。3DES 对数据进行三次加密，可提供比 DES 更高的安全性 。

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

· AES-192 — 高级加密标准(AES)是192位加密方法，通过12个循环重复将纯文本转换为加密文本。AES-192比AES-128更安全。

· AES-256 — 高级加密标准(AES)是256位加密方法，它通过14个循环重复将纯文本转换为加密文本。AES-256 是最安全的加密方法。

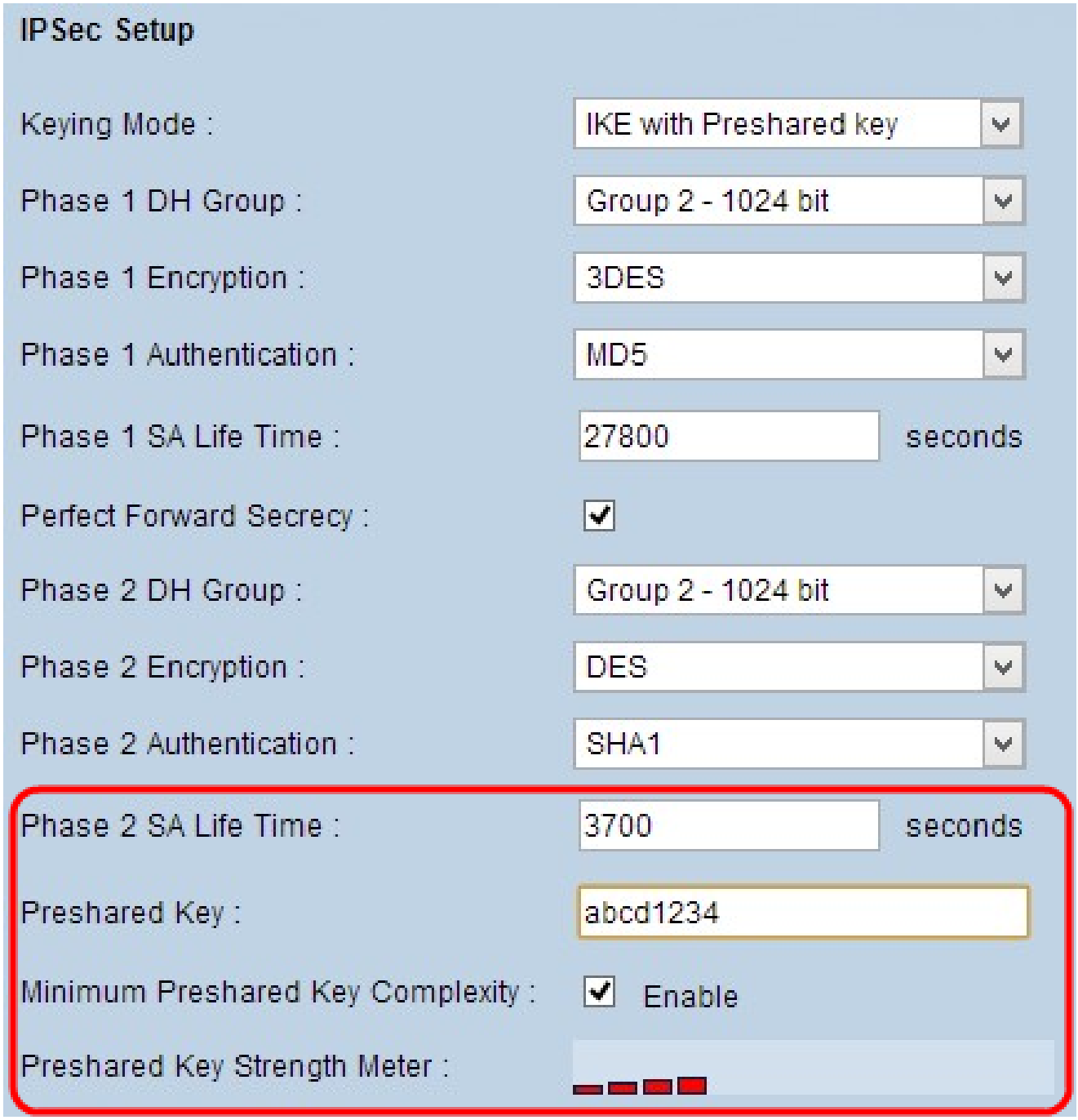


步骤 8从Phase 2 Authentication下拉列表中选择适当的身份验证方法。 VPN 隧道的两端需要使用相同的身份验证方法。建议使用SHA1。

· MD5 — 消息摘要算法–5(MD5)是一个128位的十六进制哈希函数，通过计算校验和来保护数据免受恶意攻击。

· SHA1 — 安全散列算法版本1(SHA1)是一个160位散列函数，比MD5更安全，但计算时间更长。

· Null — 不使用身份验证方法。



步骤 9在Phase 2 SA Life Time字段中，输入第2阶段密钥有效且VPN隧道保持活动状态的时间量（以秒为单位）。

步骤 10在Preshared Key字段中输入之前在IKE对等体之间共享的密钥，以对对等体进行身份验证。最多可以使用 30 个十六进制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：强烈建议经常更改IKE对等体之间的预共享密钥，以使VPN保持安全。

步骤11.（可选）如果要启用预共享密钥的强度计，请选中Minimum Preshared Key Complexity复选框。它用于通过颜色条确定预共享密钥的强度。

·预共享密钥强度表 — 通过彩色条形图显示预共享密钥的强度。红色表示弱强度，黄色表示可接受强度，绿色表示强强度。

步骤 12点击 Save（保存），以保存设置。

注意：如果要配置Advanced部分中可用的网关到网关VPN选项，请参阅文章在RV016、RV042、RV042G和RV082 VPN路由器上配置网关到网关VPN的高级设置。

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）。