在RV130或RV130W路由器上配置高级虚拟专用网络(VPN)设置

目标

虚拟专用网络(VPN)是在网络内部或网络之间建立的安全连接。VPN用于将指定主机和网络之间的流量与未经授权的主机和网络的流量隔离。站点到站点（网关到网关）VPN将整个网络相互连接，通过在公共域（也称为Internet）上创建隧道来维护安全性。每个站点只需要一个到同一公共网络的本地连接，因此节省了使用较长的专用租用线-的费用。

VPN对公司非常有益，因为它具有高度可扩展性，简化了网络拓扑，并通过减少远程用户的差旅时间和成本提高了工作效率。

互联网密钥交换(IKE)是用于为VPN中的通信建立安全连接的协议。此安全连接称为安全关联(SA)。 您可以创建IKE策略来定义此过程中要使用的安全参数，例如对等体的身份验证、加密算法等。要使VPN正常工作，两个终端的IKE策略应该相同。

本文旨在展示如何在RV130或RV130W路由器上配置高级VPN设置，其中涵盖IKE策略设置和VPN策略设置。

适用设备

·RV130
· RV130W

软件版本

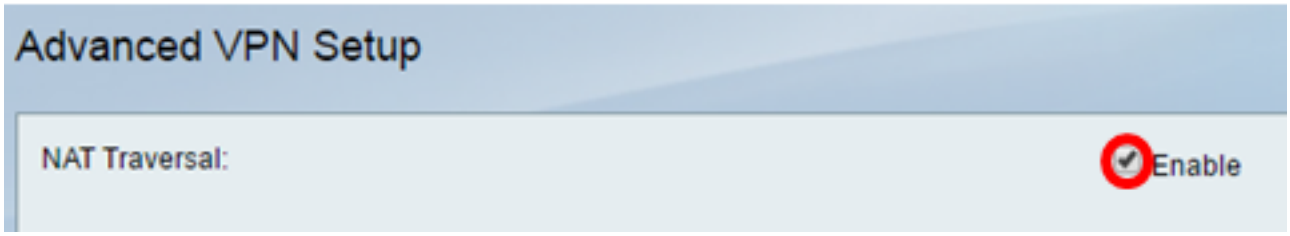
•1.0.3.22

配置高级VPN设置

添加/编辑Internet密钥交换(IKE)策略设置

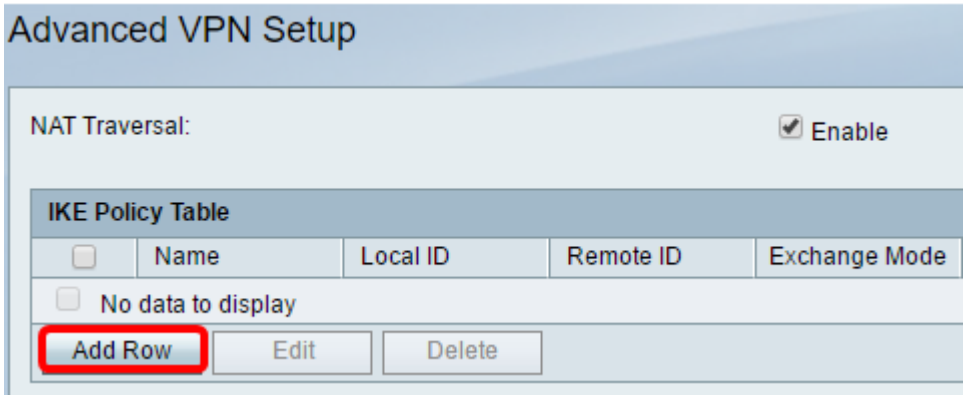
步骤1.登录到基于Web的实用程序，并选择**VPN > Site-to-Site IPSec VPN >Advanced VPN Setup**。

步骤2.（可选）如果要为VPN连接启用网络地址转换(NAT)遍历，请选中NAT遍历中的**Enable**复选框。NAT遍历允许在使用NAT的网关之间建立VPN连接。如果VPN连接通过启用了NAT的网关，请选择此选项。



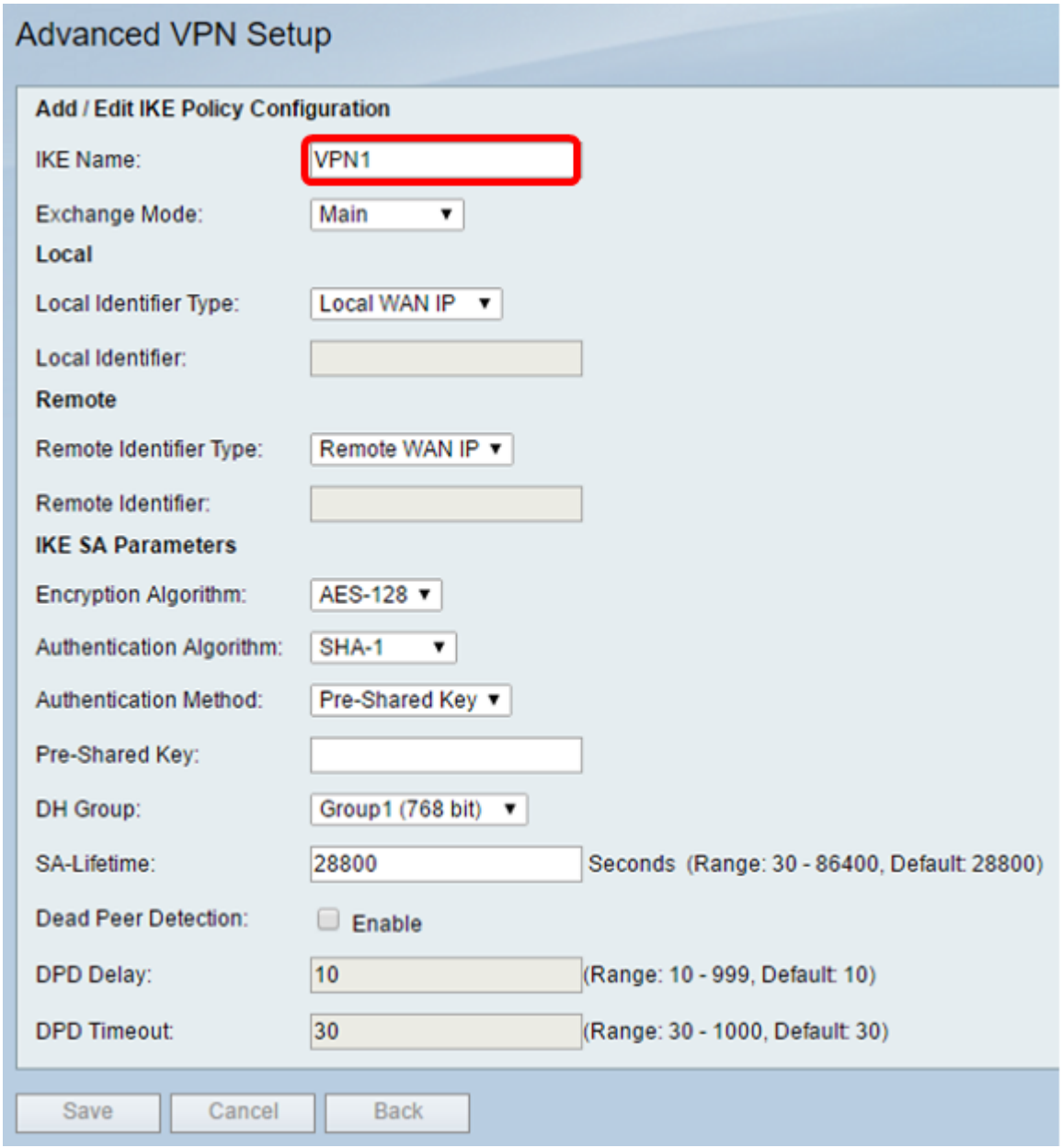
步骤3.在IKE策略表中，单击**Add Row**以创建新的IKE策略。

注意：如果已配置基本设置，则下表将包含创建的基本的VPN设置。可以通过选中策略的复选框并点击**编辑**来编辑现有的IKE策略。“高级VPN设置”(Advanced VPN Setup)页面将更改：



步骤4.在*IKE Name*字段中，输入IKE策略的唯一名称。

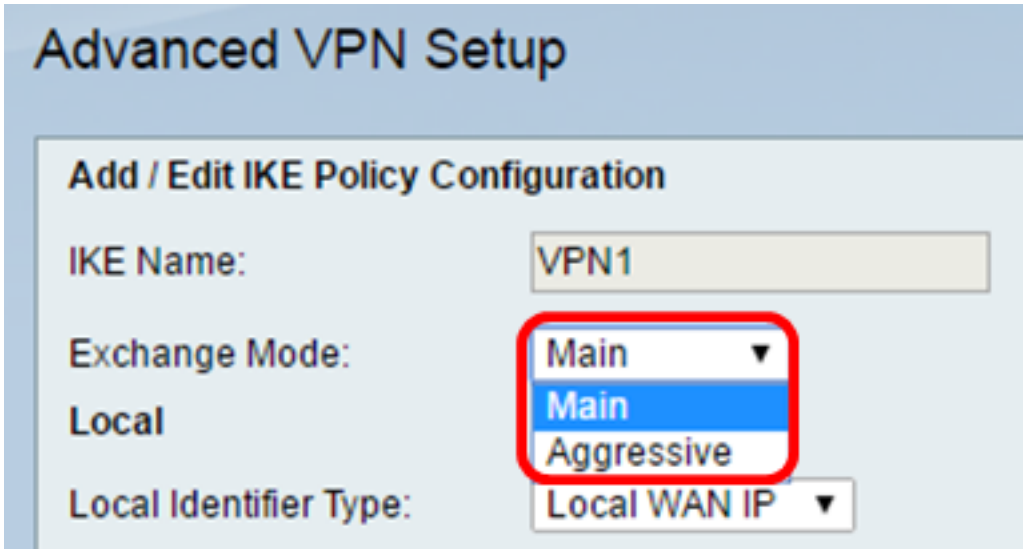
注意：如果已配置基本设置，则创建的连接名称将设置为IKE名称。在本示例中，VPN1是所选IKE名称。



步骤5.从Exchange模式下拉列表中选择一个选项。

- Main — 此选项允许IKE策略以比主动模式更高的安全性协商VPN隧道。如果更安全的VPN连接优先于协商速度，请单击此选项。
- 主动 — 此选项允许IKE策略建立比主模式更快但安全性较低的连接。如果更快的VPN连接比高安全性优先，请单击此选项。

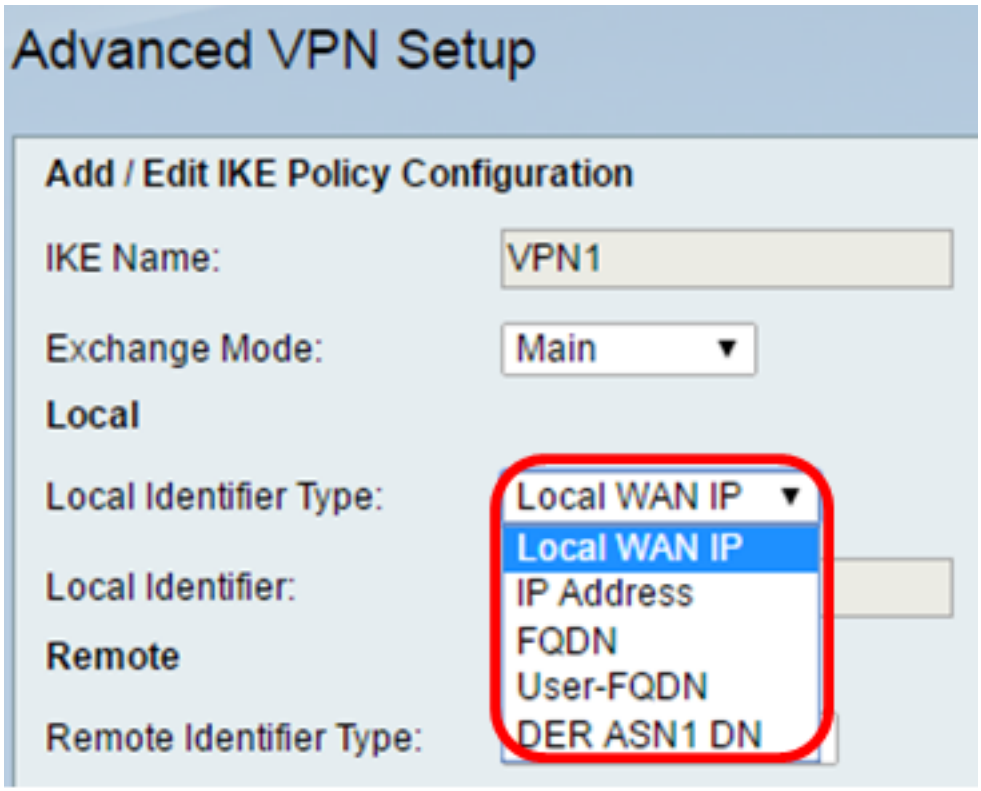
注意：在本示例中，选择Main。



步骤6.从Local Identifier Types下拉列表中进行选择，以确定或指定本地路由器的Internet安全关联和密钥管理协议(ISAKMP)。选项有：

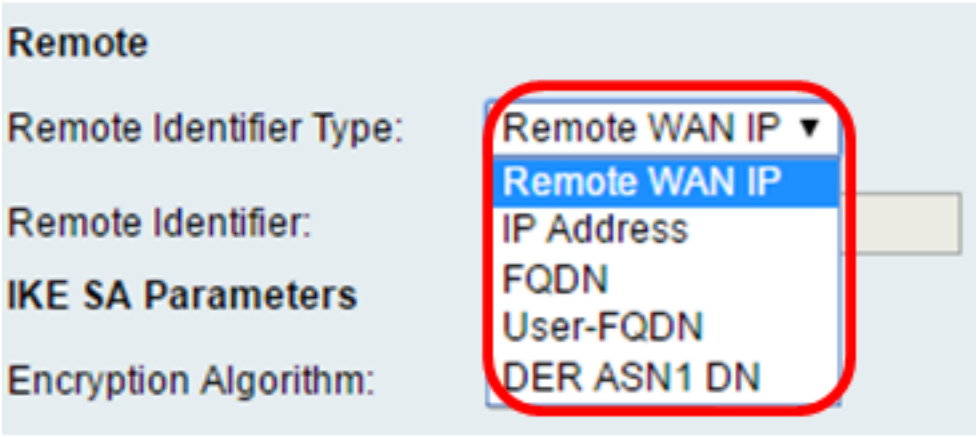
- 本地WAN IP — 路由器使用局域网(WAN)IP作为主要标识符。此选项通过Internet连接。选择此选项会使下面的*本地标识符*字段变灰。
- IP地址 — 点击此选项可在*本地标识符*字段中输入IP地址。
- FQDN — 完全限定域名(FQDN)或域名(例如http://www.example.com)允许您在*本地标识符(Local Identifier)字段中输入域名或IP地*址。
- User-FQDN — 此选项是用户邮件地址，例如user@email.com。在*Local Identifier*字段中输入域名或IP地址。
- DER ASN1 DN — 此选项是可分辨名称(DN)的标识符类型，它使用可分辨编码规则Abstract Syntax Notation One(DER ASN1)传输信息。当VPN隧道与用户证书关联时会发生这种情况。如果选择此项，请在*本地标识符*字段中输入域名或IP地址。

注意：在本示例中，选择本地WAN IP。



步骤7.从Remote Identifier Type下拉列表中选择，以标识或指定远程路由器的Internet安全关联和密钥管理协议(ISAKMP)。选项包括Remote WAN IP、IP Address、FQDN、User FQDN和DER ASN1 DN。

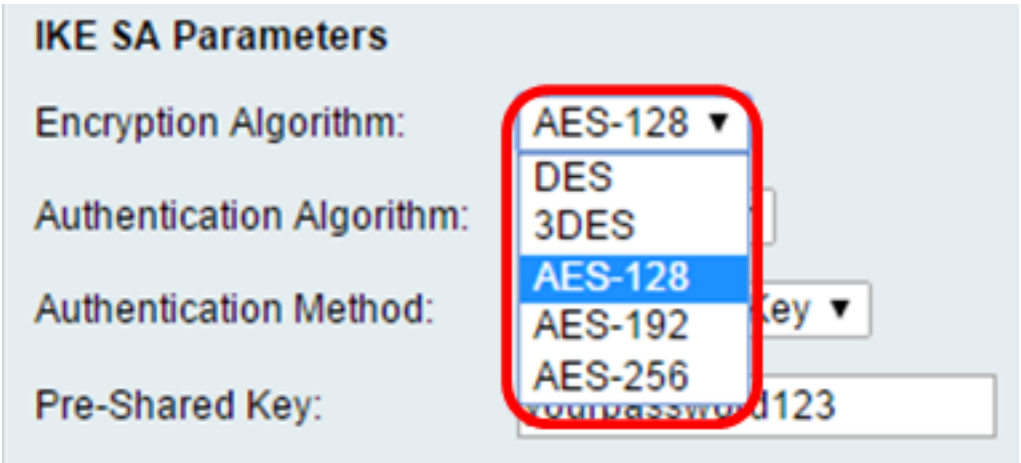
注意：在本示例中，选择远程WAN IP。



步骤8.从Encryption Algorithm下拉列表中选择一个选项。

- DES — 数据加密标准(DES)是一种56位旧加密方法，它不是非常安全的加密方法，但为了向后兼容，可能需要它。
- 3DES — 三重数据加密标准(3DES)是一种168位、简单的加密方法，用于增加密钥大小，因为它将数据加密三次。这提供了比DES更高的安全性，但比AES更低的安全性。
- AES-128 — 具有128位密钥的高级加密标准(AES-128)使用128位密钥进行AES加密。AES比DES更快且更安全。一般来说，AES也比3DES更快、更安全。AES-128是默认加密算法，比AES-192和AES-256更快但安全性低。
- AES-192 — AES-192使用192位密钥进行AES加密。AES-192比AES-128更慢但更安全，比AES-256更快但更安全。
- AES-256 — AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192更慢，但更安全。

注意：在本示例中，选择AES-128。



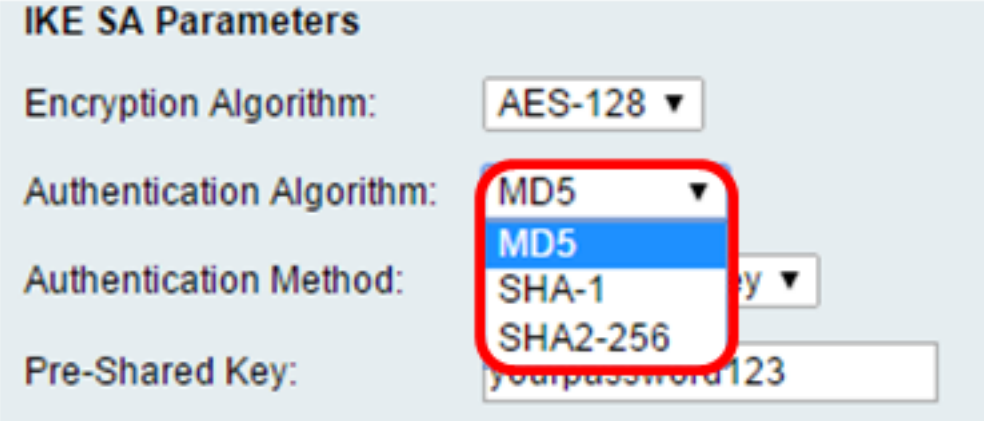
步骤9.从Authentication Algorithm下拉列表中，选择以下选项：

- MD5 — 消息摘要5(MD5)是一种使用128位散列值进行身份验证的身份验证算法。MD5的安全性较低，但比SHA-1和SHA2-256更快。
- SHA-1 — 安全哈希函数1(SHA-1)使用160位哈希值进行身份验证。SHA-1比MD5更慢但更安全

。SHA-1是默认身份验证算法，比SHA2-256更快但更安全。

- SHA2-256 — 具有256位哈希值(SHA2-256)的安全哈希算法2使用256位哈希值进行身份验证。SHA2-256比MD5和SHA-1更慢，但更安全。

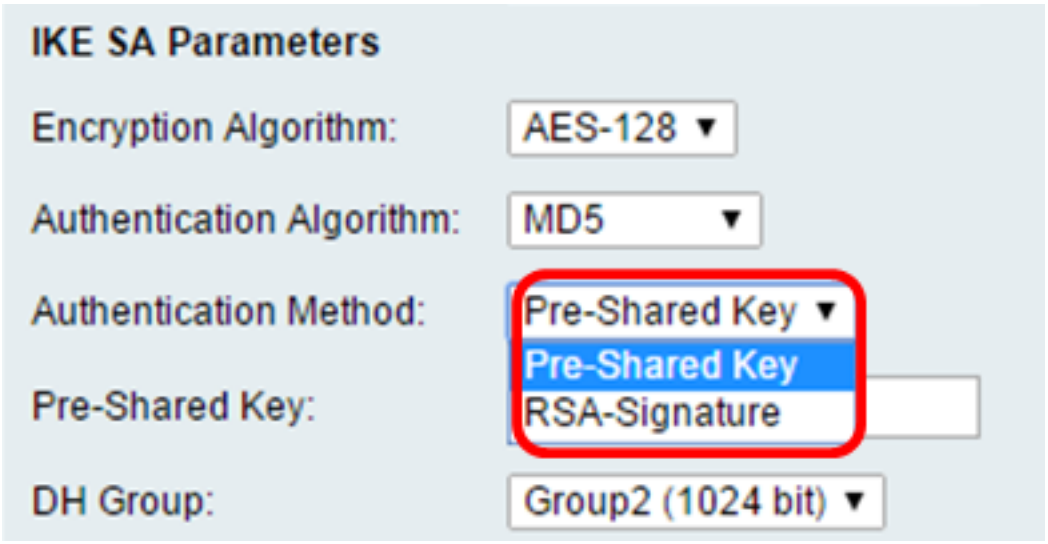
注意：在本例中，选择MD5。



步骤10.在Authentication Method下拉列表中，选择以下选项：

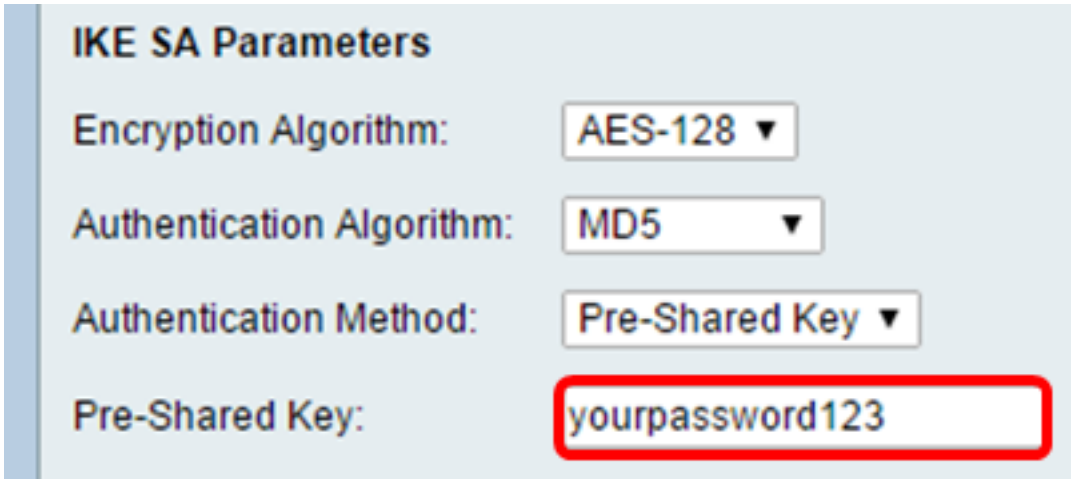
- Pre-Shared Key — 此选项需要与IKE对等体共享的密码。
- RSA签名 — 此选项使用证书对连接进行身份验证。如果选择此项，Pre-Shared Key字段将被禁用。跳至步骤12。

注意：在本示例中，选择预共享密钥。



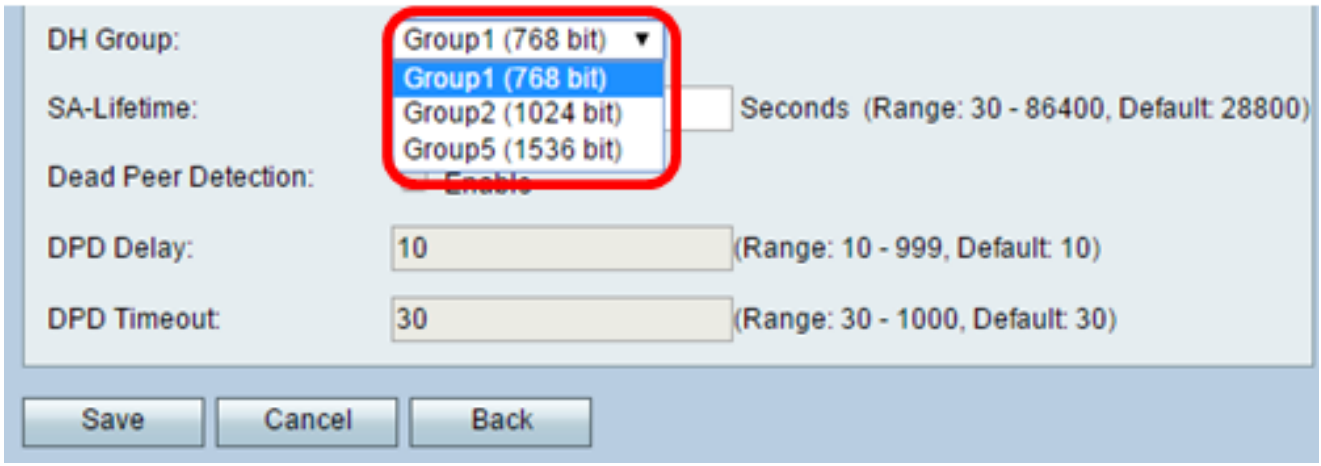
步骤11.在*预共享密钥*字段中，输入长度介于8到49个字符之间的密码。

注意：在本例中，使用yourpassword123。

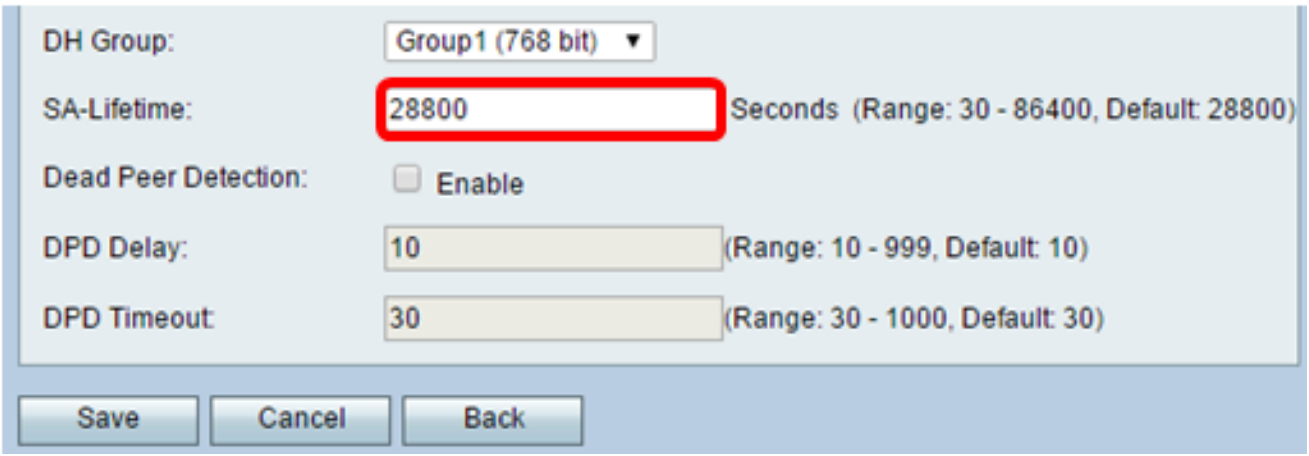


第12步：从DH Group下拉列表中，选择IKE使用哪个Diffie-Hellman(DH)组算法。DH组中的主机可以在彼此不知情的情况下交换密钥。组比特数越高，安全性越好。

注意：在本示例中，选择Group1。

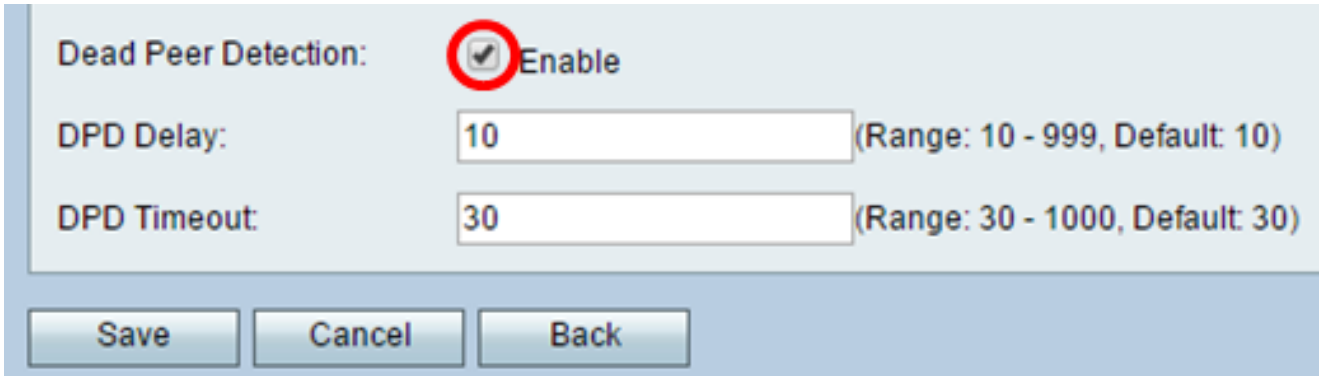


步骤13.在*SA-Lifetime*字段中，输入VPN的SA在续订SA之前持续的时间（以秒为单位）。超时的范围是从 30 到 86400 秒。默认值为 28800。



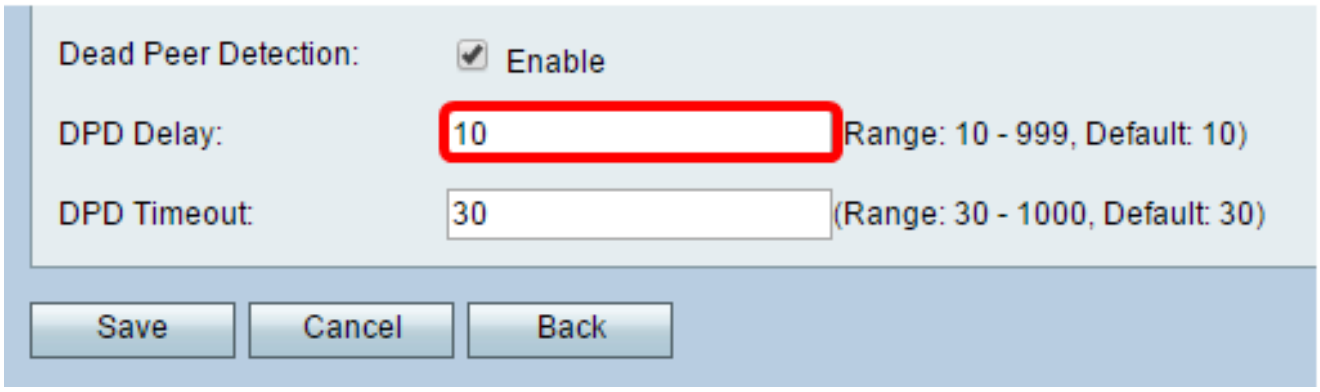
第14步(可选)选中**Enable** Dead Peer Detection复选框以启用Dead Peer Detection(DPD)。DPD监控IKE对等体，以查看对等体是否停止运行或仍然处于活动状态。如果检测到对等体已停机，设备将删除IPsec和IKE安全关联。DPD可防止非活动对等体上的网络资源浪费。

注意：如果不希望启用Dead Peer Detection，请跳至步骤17。



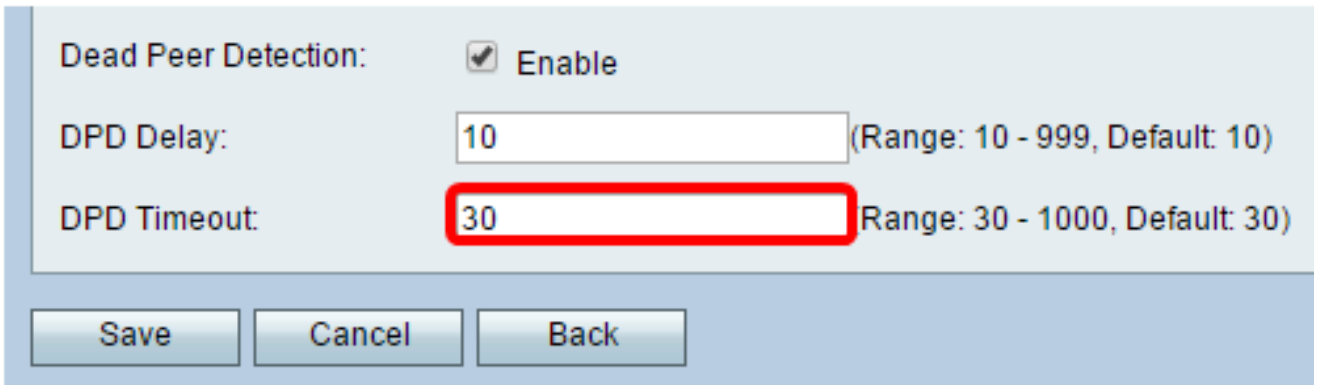
第15步。（可选）如果在第14步中启用DPD，请在*DPD延迟*字段中输入检查对等体活动的频率（以秒为单位）。

注意：DPD Delay是连续DPD R-U-THERE消息之间的间隔（以秒为单位）。DPD R-U-THERE消息仅在IPsec流量空闲时发送。默认值为 10。

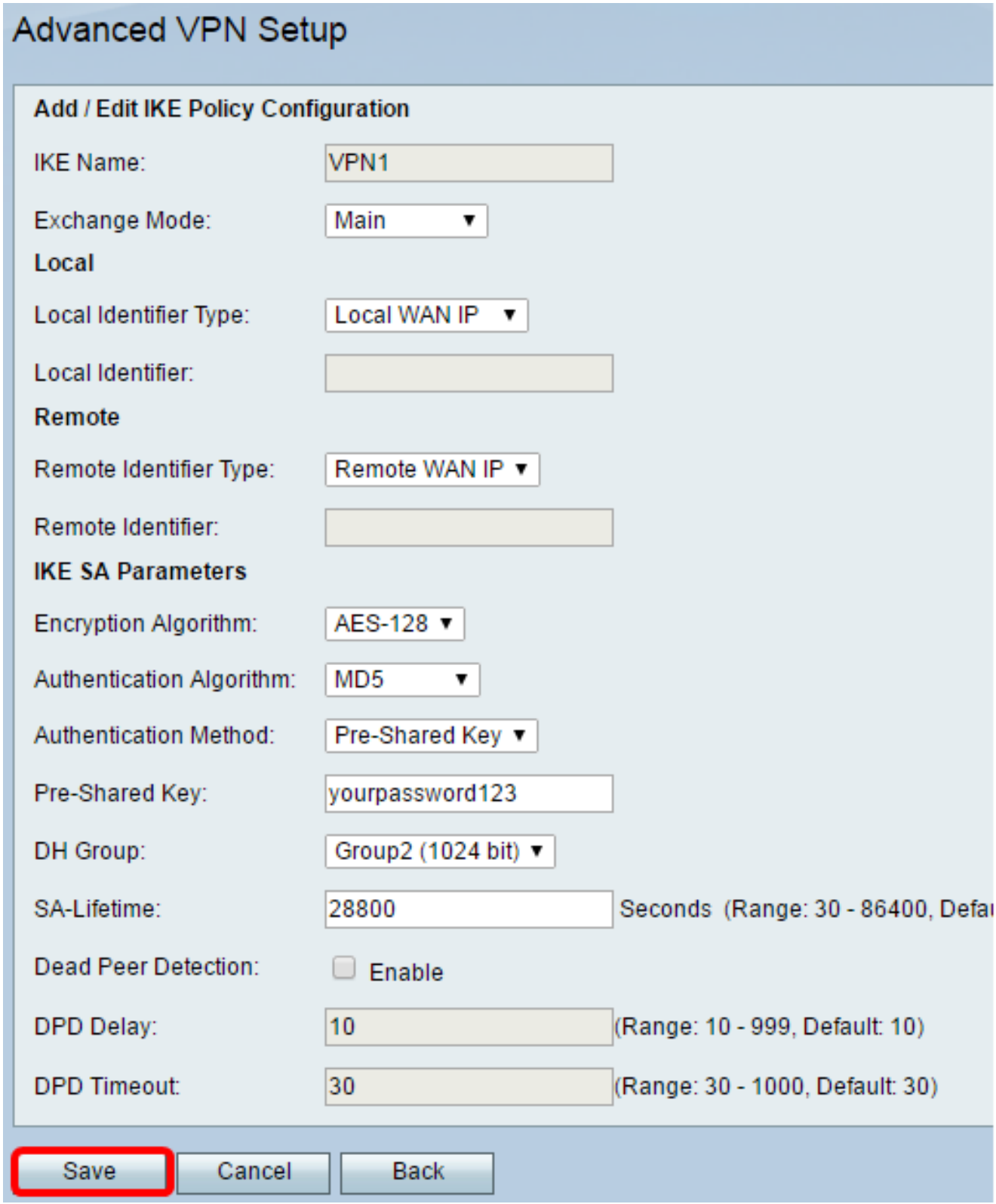


步骤16.（可选）如果在步骤14中启用DPD，请在*DPD超时*字段中输入非活动对等体被丢弃之前等待的秒数。

注意：这是设备在认为对等体失效之前应等待接收对DPD消息的响应的最长时间。默认值为30。



步骤17.点击**保存**。



注意：系统将重新显示Advanced VPN Setup主页。

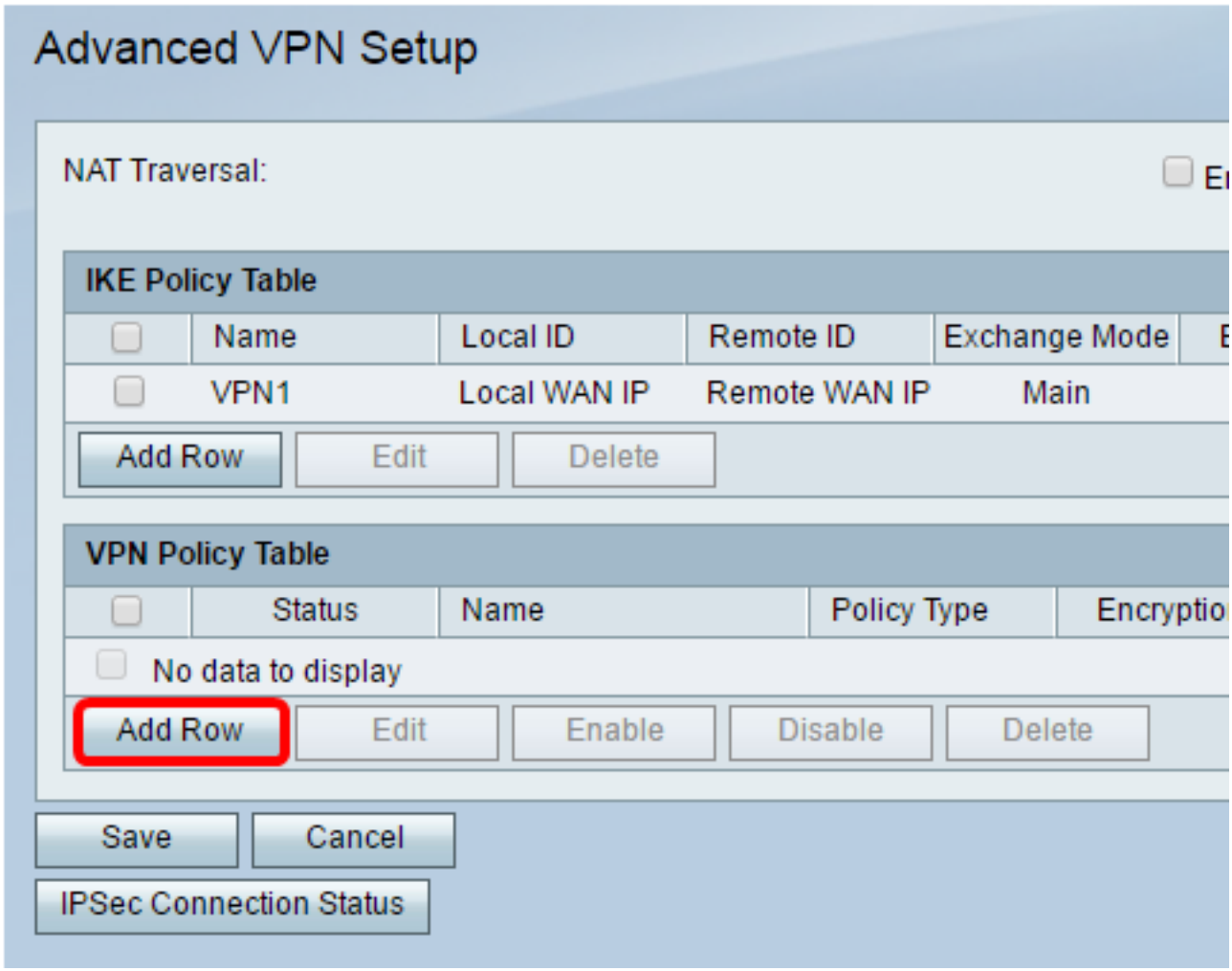
现在，您应该在路由器上成功配置IKE策略设置。

配置VPN策略设置

注意:要使VPN正常工作，两个端点的VPN策略应该相同。

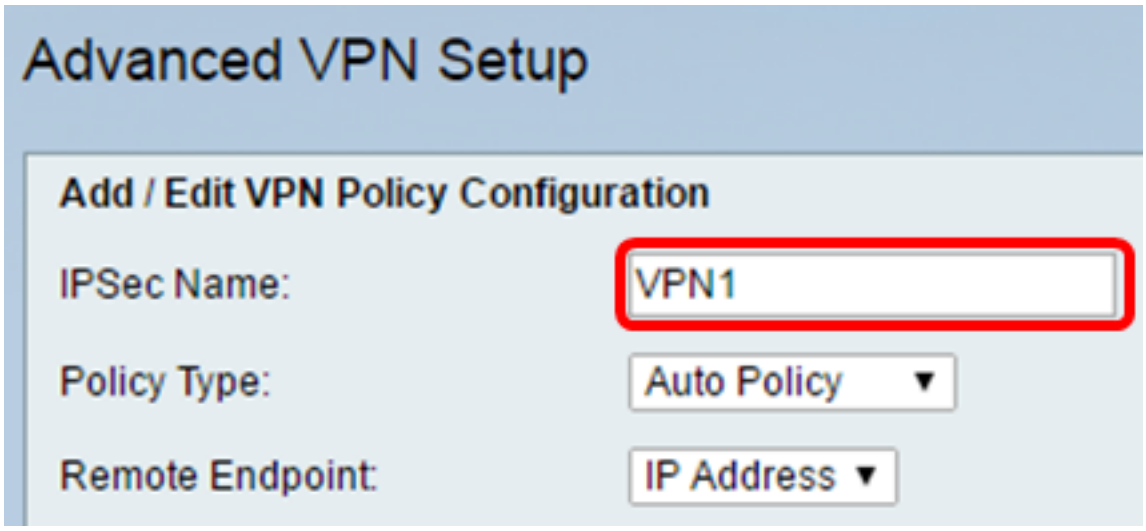
步骤1.在VPN策略表中，单击**Add Row**以创建新的VPN策略。

注意：您还可以通过选中策略的复选框编辑VPN策略，然后单击**Edit**。系统将显示Advanced VPN Setup页面：



步骤2.在Add/Edit VPN Configuration区域下的*IPSec Name*字段中，输入VPN策略的名称。

注意：在本示例中，使用VPN1。



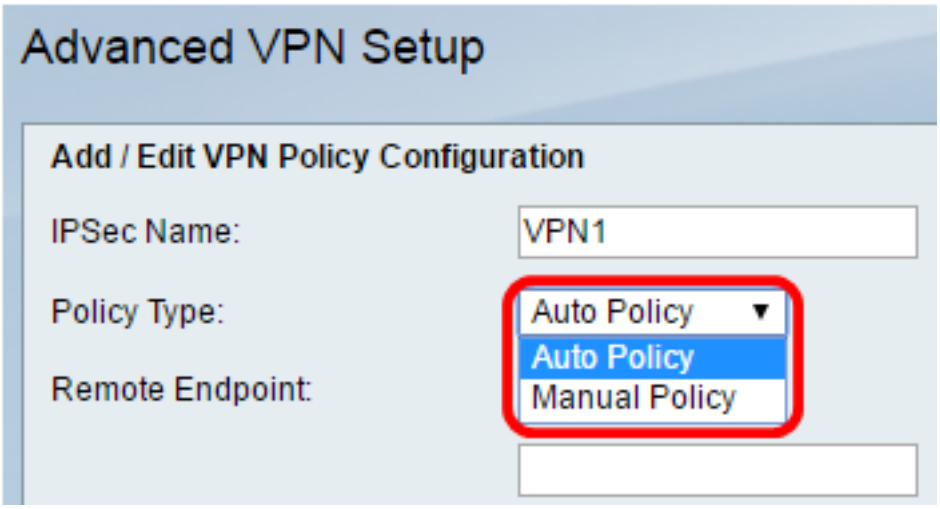
步骤3.从Policy Type下拉列表中，选择一个选项。

- Manual Policy — 此选项允许您为VPN隧道手动配置数据加密和完整性的密钥。如果选择此项，则会启用Manual Policy Parameters区域下的配置设置。继续这些步骤，直到选择远程流量。

单击此处了解这些步骤。

- 自动策略 — 自动设置策略参数。此选项使用IKE策略进行数据完整性和加密密钥交换。如果选择此项，则会启用Auto Policy Parameters区域下的配置设置。单击此处了解这些步骤。确保IKE协议在两个VPN终端之间自动协商。

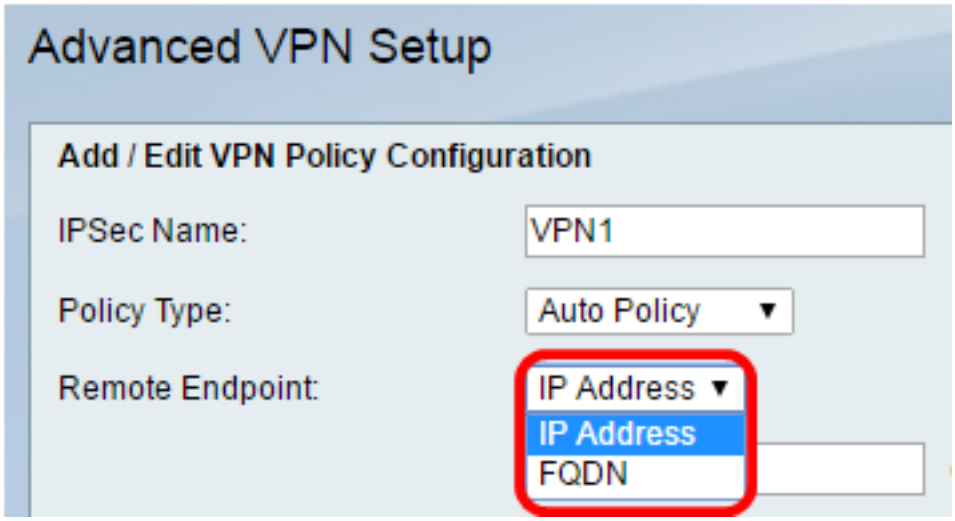
注意：在本示例中，选择Auto Policy。



步骤4.从Remote Endpoint下拉列表中选择一个选项。

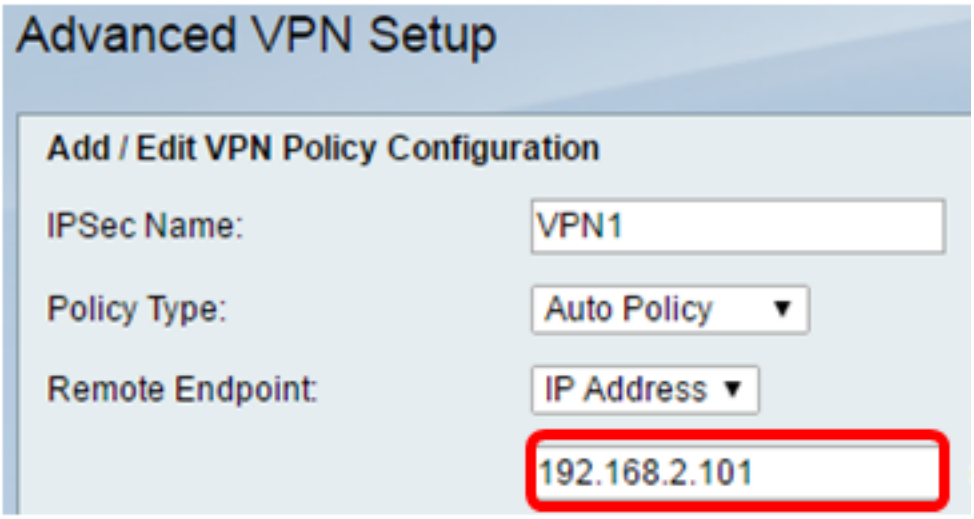
- IP地址 — 此选项通过公有IP地址标识远程网络。
- FQDN — 特定计算机、主机或Internet的完整域名。FQDN由两部分组成：主机名和域名。只有在步骤3中选择了**Auto Policy**时，才能启用此选项。

注意：在本示例中，选择IP地址。

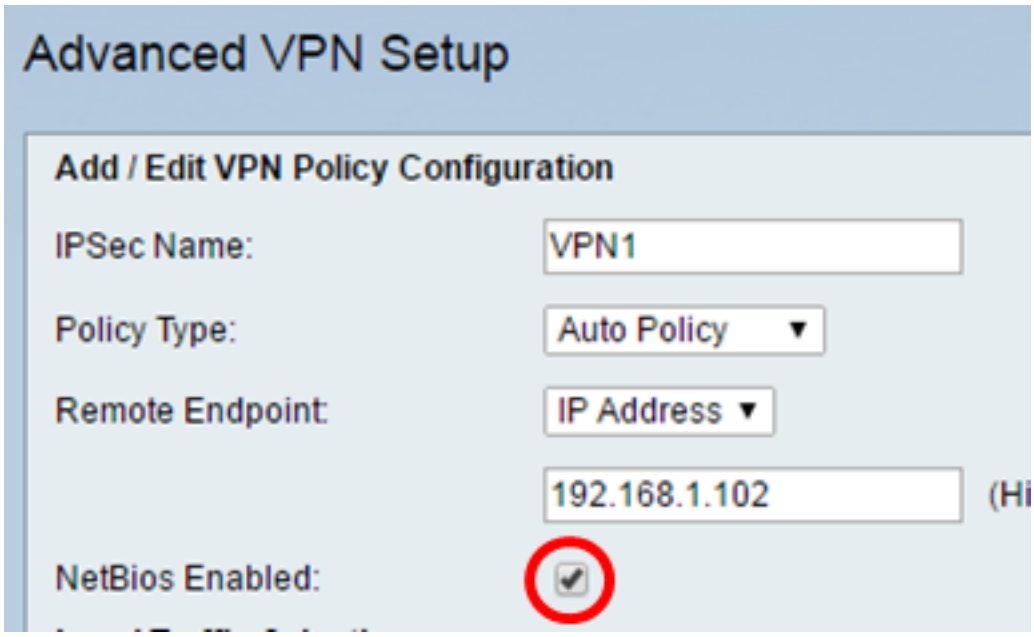


步骤5.在*远程终端*字段中，输入远程地址的公用IP地址或域名。

注意：在本例中，使用192.168.2.101。



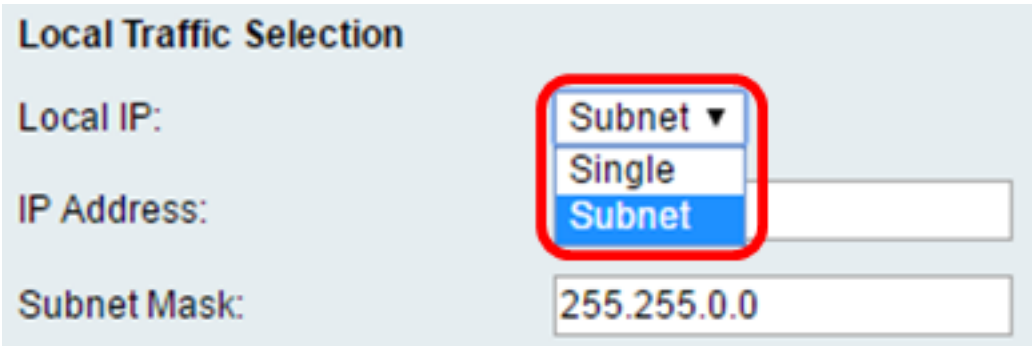
步骤6.（可选）如果要启用要通过VPN连接发送的网络基本输入/输出系统(NetBIOS)广播，请选中**NetBios Enabled**复选框。NetBIOS允许主机在局域网(LAN)中相互通信。



步骤7.从Local Traffic Selection区域下的Local IP下拉列表中，选择一个选项。

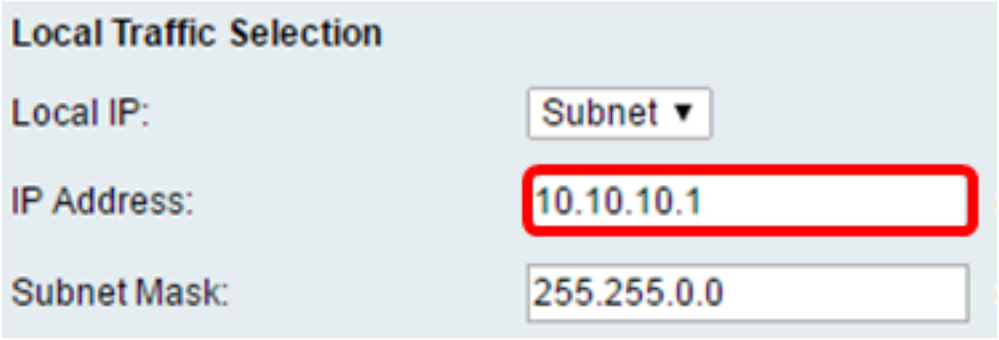
- 单个 — 将策略限制为一个主机。
- 子网 — 允许IP地址范围内的主机连接到VPN。

注意：在本示例中，选择子网。



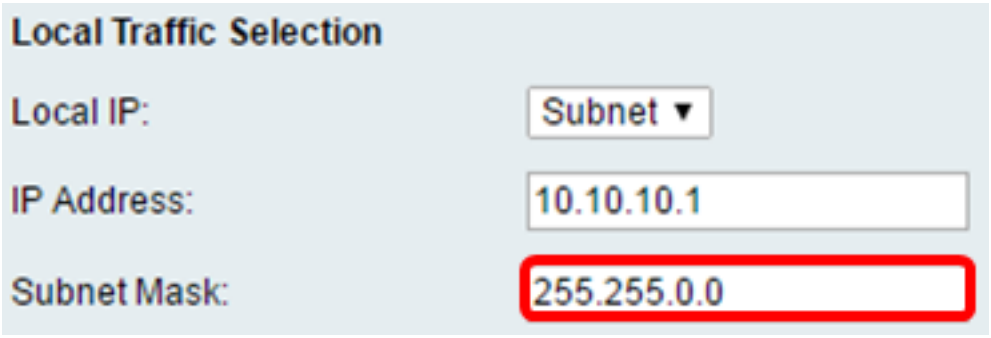
步骤8.在IP地址字段中输入本地子网或主机的主机或子网IP地址。

注意：在本示例中，使用本地子网IP地址10.10.10.1。



步骤9.（可选）如果在步骤7中选择了子网，请在*子网掩码*字段中输入客户端的子网掩码。如果在步骤1中选择了Single，则禁用Subnet Mask字段。

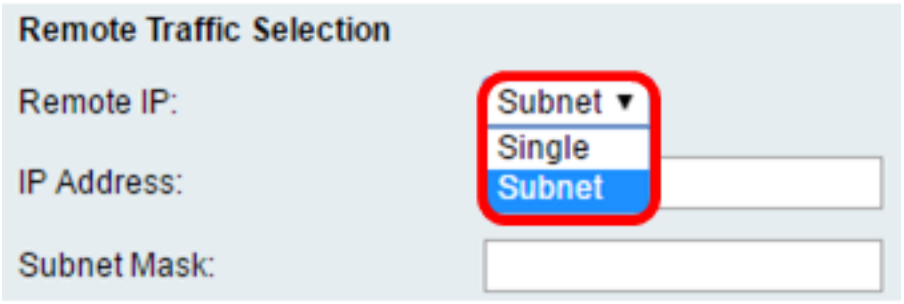
注意：本例中使用子网掩码255.255.0.0。



步骤10.从Remote Traffic Selection区域下的Remote IP下拉列表中，选择一个选项。

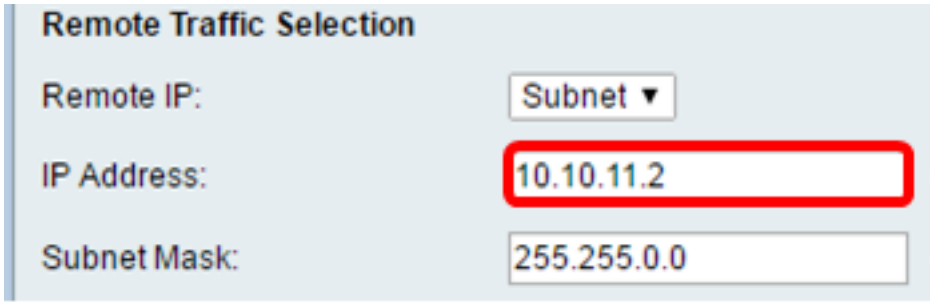
- 单个 — 将策略限制为一个主机。
- 子网 — 允许IP地址范围内的主机连接到VPN。

注意： 在本示例中，选择子网。



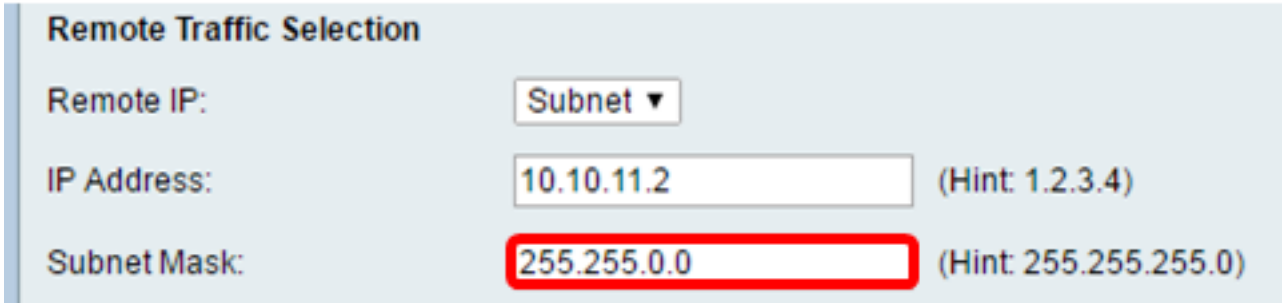
步骤11.在*IP Address*字段中输入将成为VPN一部分的主机的IP地址*范*围。如果在步骤10中选择了**Single**，请输入IP地址。

注意：在下面的示例中，使用10.10.11.2。



步骤12.（可选）如果在步骤10中选择了**子网**，请在子网掩码字段中输入子网IP地址的子网掩码。

注意：在下面的示例中，使用了255.255.0.0。

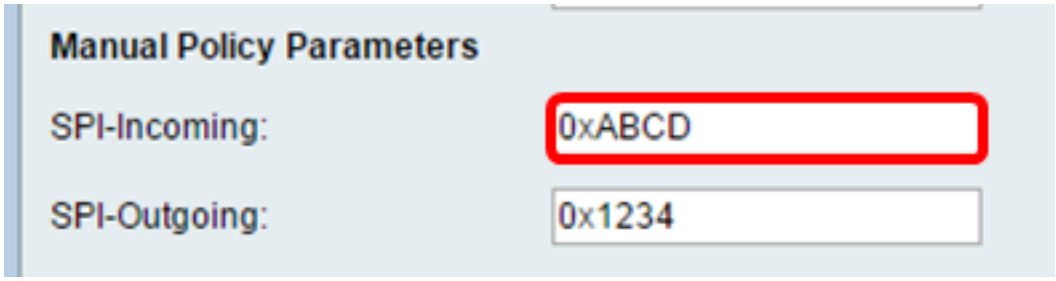


手动策略 参数

注意：只有选择“手动策略”(**Manual Policy**)，**才能编辑**这些字段。

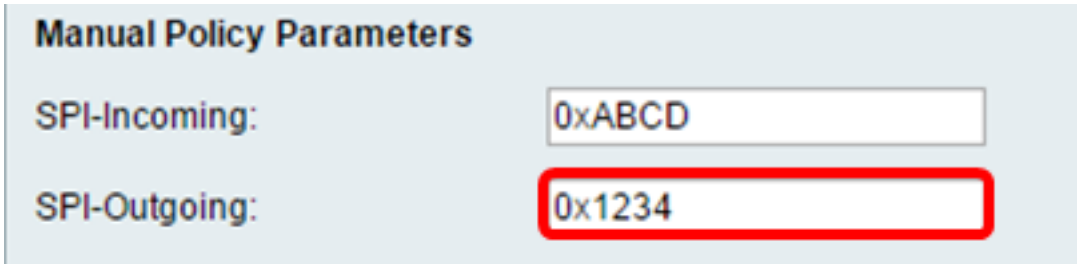
步骤1.在*SPI-Incoming*字段中，为VPN连接上传入流量的安全参数索引(SPI)标记输入三到八个十六进制字符。SPI标记用于区分一个会话的流量和其他会话的流量。

注意：在本例中，使用0xABCD。



步骤2.在*SPI-Outgoing*字段中，为VPN连接上的传出流量的SPI标记输入三到八个十六进制字符。

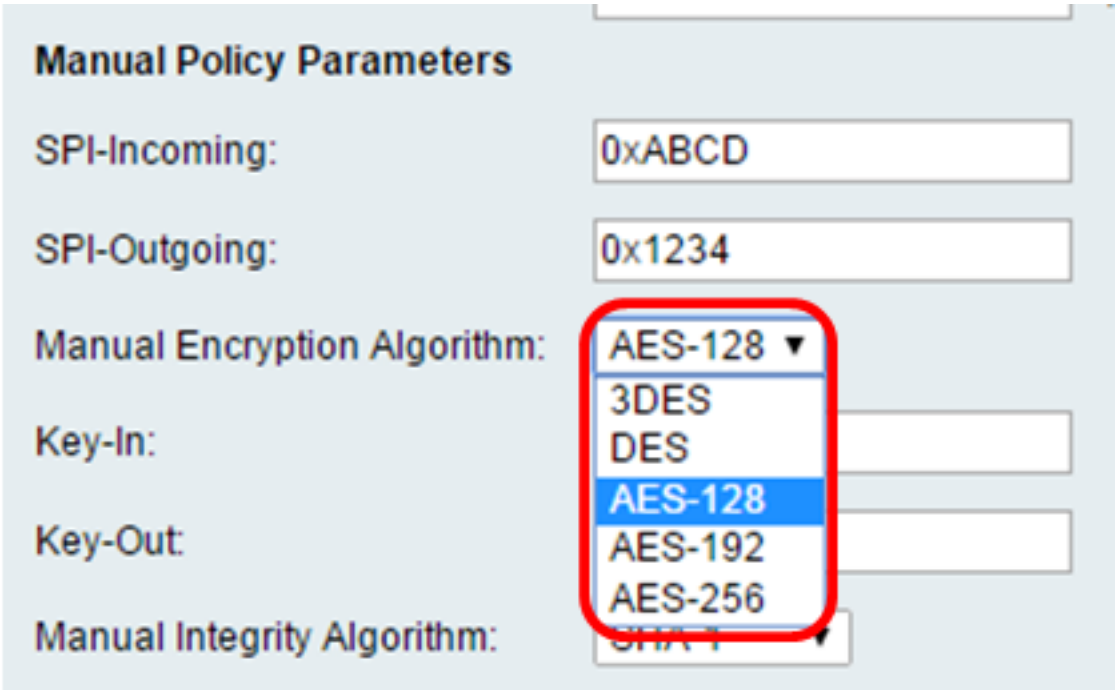
注意：在本示例中，使用0x1234。



步骤3.从Manual Encryption Algorithm下拉列表中选择一个选项。选项包括DES、3DES、

AES-128、AES-192和AES-256。

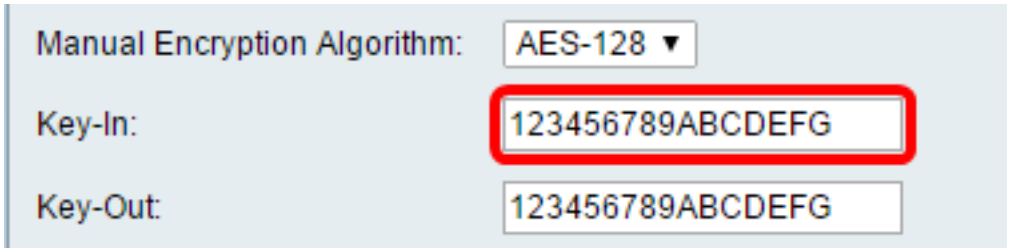
注意：在本例中，选择AES-128。



步骤4.在*Key-In*字段中，输入入站策略的密钥。密钥长度取决于步骤3中选择的算法。

- DES使用8个字符的密钥。
- 3DES使用24个字符的密钥。
- AES-128使用16个字符的密钥。
- AES-192使用24个字符的密钥。
- AES-256使用32个字符的密钥。

注意：在本例中，123456789ABCDEFG。



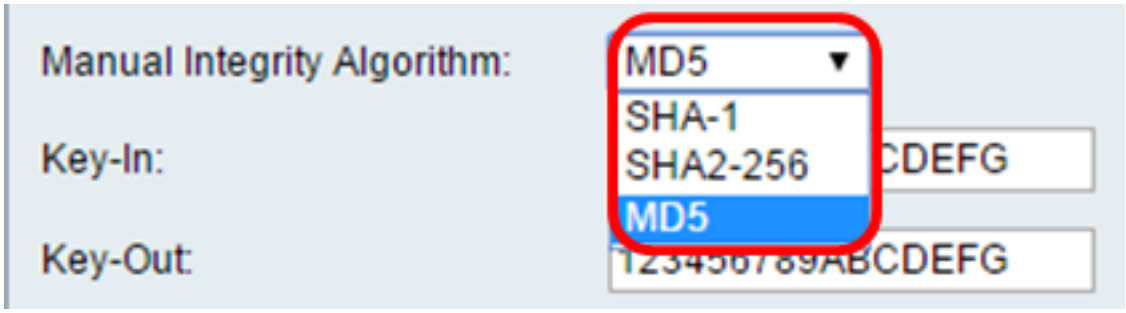
步骤5.在*Key-Out*字段中，输入传出策略的密钥。密钥长度取决于步骤3中选择的算法。

注意：在本例中，123456789ABCDEFG。

步骤6.从Manual Integrity Algorithm下拉列表中，选择一个选项。

- MD5 — 使用128位哈希值实现数据完整性。MD5的安全性较低，但比SHA-1和SHA2-256更快。
- SHA-1 — 使用160位哈希值实现数据完整性。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。
- SHA2-256 — 使用256位哈希值实现数据完整性。SHA2-256比MD5和SHA-1更慢，但更安全。

注意：在本例中，选择MD5。



步骤7.在*Key-In*字段中，输入入站策略的密钥。密钥长度取决于步骤6中选择的算法。

- MD5使用16个字符的密钥。
- SHA-1使用20字符的密钥。
- SHA2-256使用32个字符的密钥。

注意：在本例中，123456789ABCDEFG。

步骤8.在*Key-Out*字段中，输入传出策略的密钥。密钥长度取决于步骤6中选择的算法。

注意：在本例中，123456789ABCDEFG。

自动o策略参数

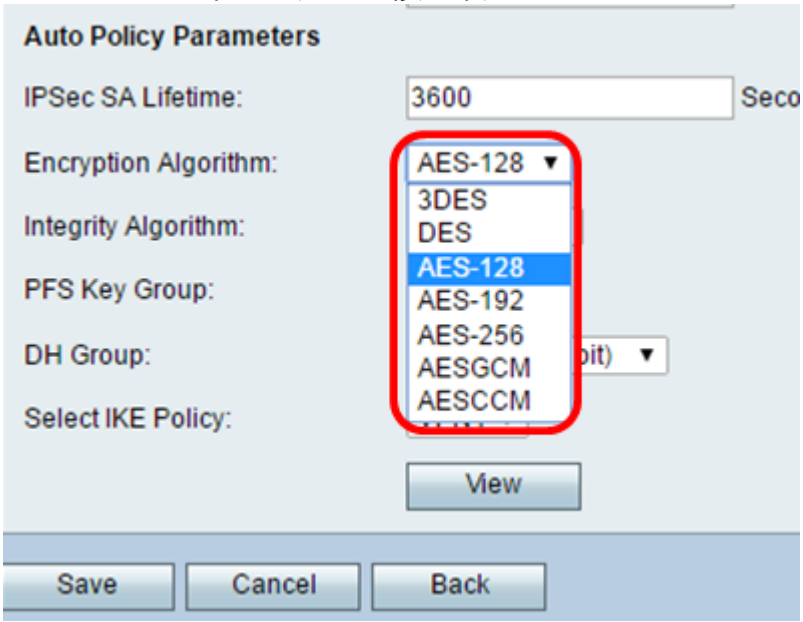
注意：在创建自动VPN策略前，请确保创建要基于其创建自动VPN策略的IKE策略。仅当在第3步中选择了**Auto Policy**时，才能编辑这些字段。

第1步：在*IPSec SA-Lifetime*字段中，输入SA在续订前持续的时间（以秒为单位）。范围为30-86400。默认值为3600。

步骤2.从加密算法下拉列表中选择一个选项。选项有：

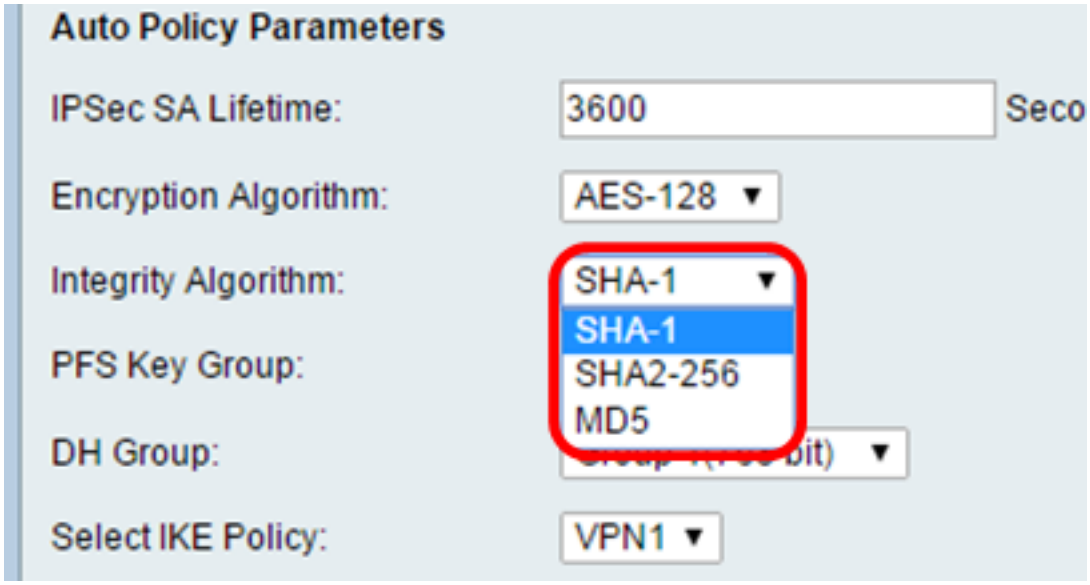
注意：在本例中，选择AES-128。

- DES — 一种56位旧加密方法，它不是非常安全的加密方法，但为了向后兼容，可能需要它。
- 3DES — 一种168位、简单的加密方法，用于增加密钥大小，因为它将数据加密三次。这提供了比DES更高的安全性，但比AES更低的安全性。
- AES-128 — 使用128位密钥进行AES加密。AES比DES更快且更安全。一般来说，AES也比3DES更快、更安全。AES-128比AES-192和AES-256更快，但安全性较低。
- AES-192 — 使用192位密钥进行AES加密。AES-192比AES-128更慢但更安全，比AES-256更快但更安全。
- AES-256 — 使用256位密钥进行AES加密。AES-256比AES-128和AES-192更慢，但更安全。
- AESGCM — 高级加密标准伽罗瓦计数器模式是经过身份验证的通用加密块密码模式。GCM身份验证使用特别适合在硬件中高效实施的操作，使其特别适用于高速实施或高效紧凑电路中的实施。
- AESCCM — 采用CBC-MAC模式的高级加密标准计数器是经过身份验证的通用加密块密码模式。CCM非常适合用于紧凑的软件实施中。

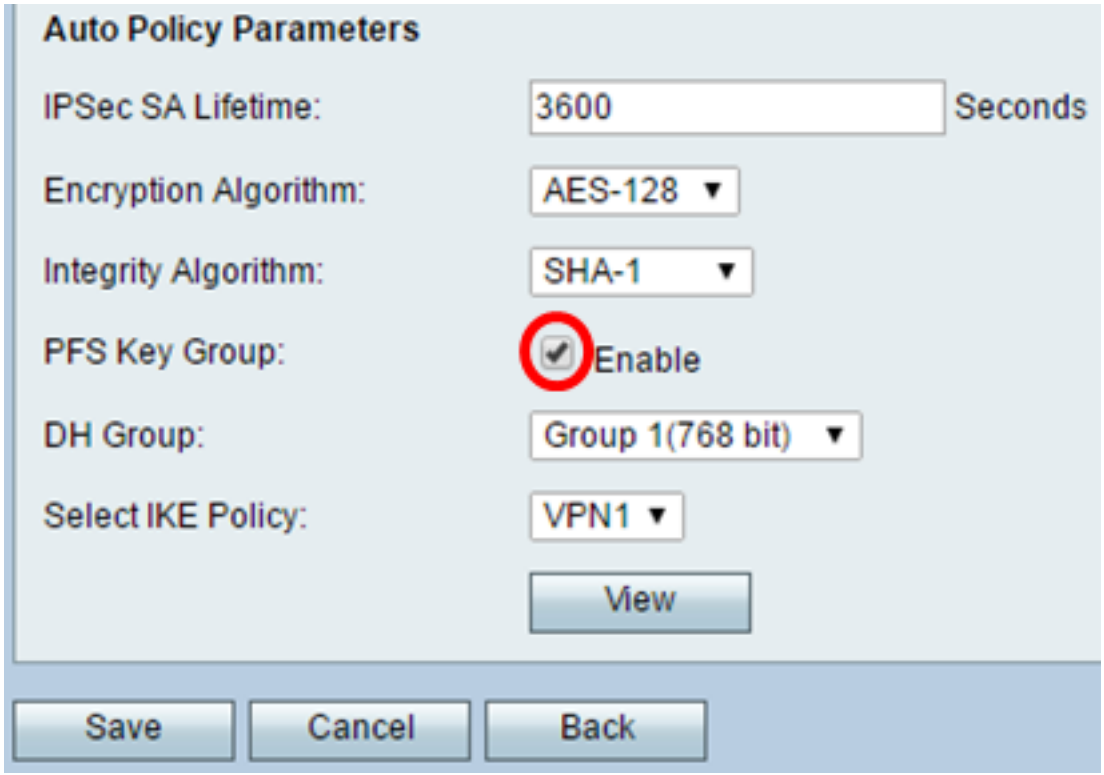


步骤3.从完整性算法下拉列表中选择一个选项。选项包括MD5、SHA-1和SHA2-256。

注意：在本示例中，选择SHA-1。

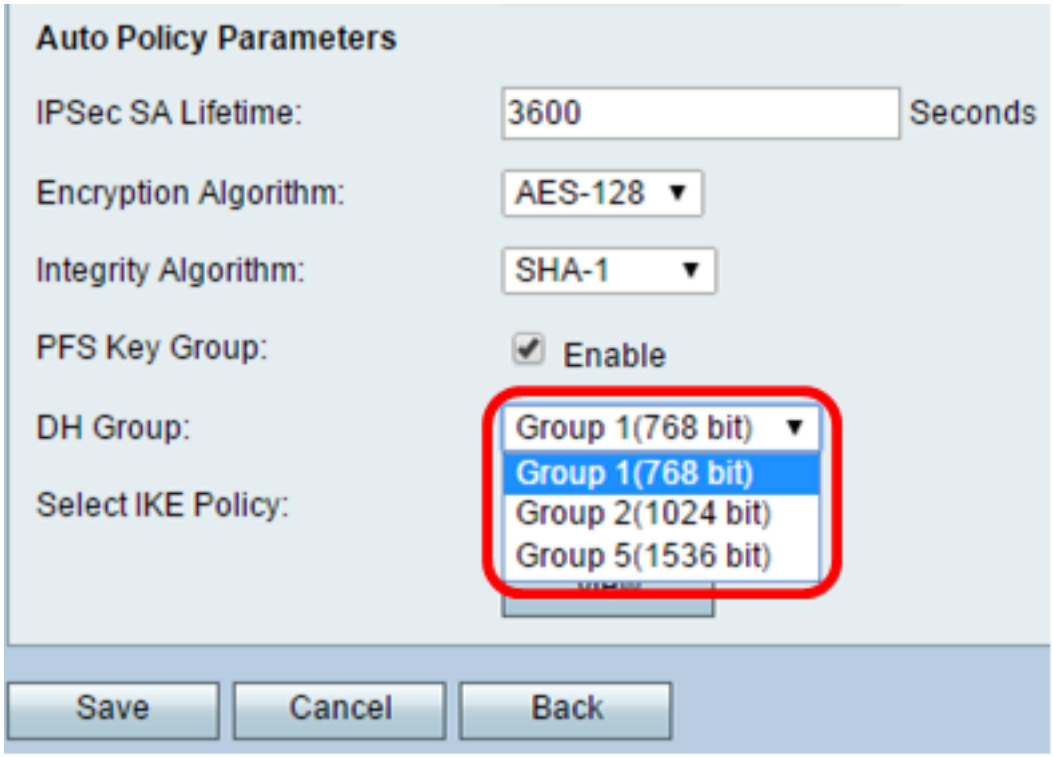


步骤4.选中PFS密钥组中的**Enable**复选框以启用完全向前保密(PFS)。PFS提高了VPN安全性，但降低了连接速度。



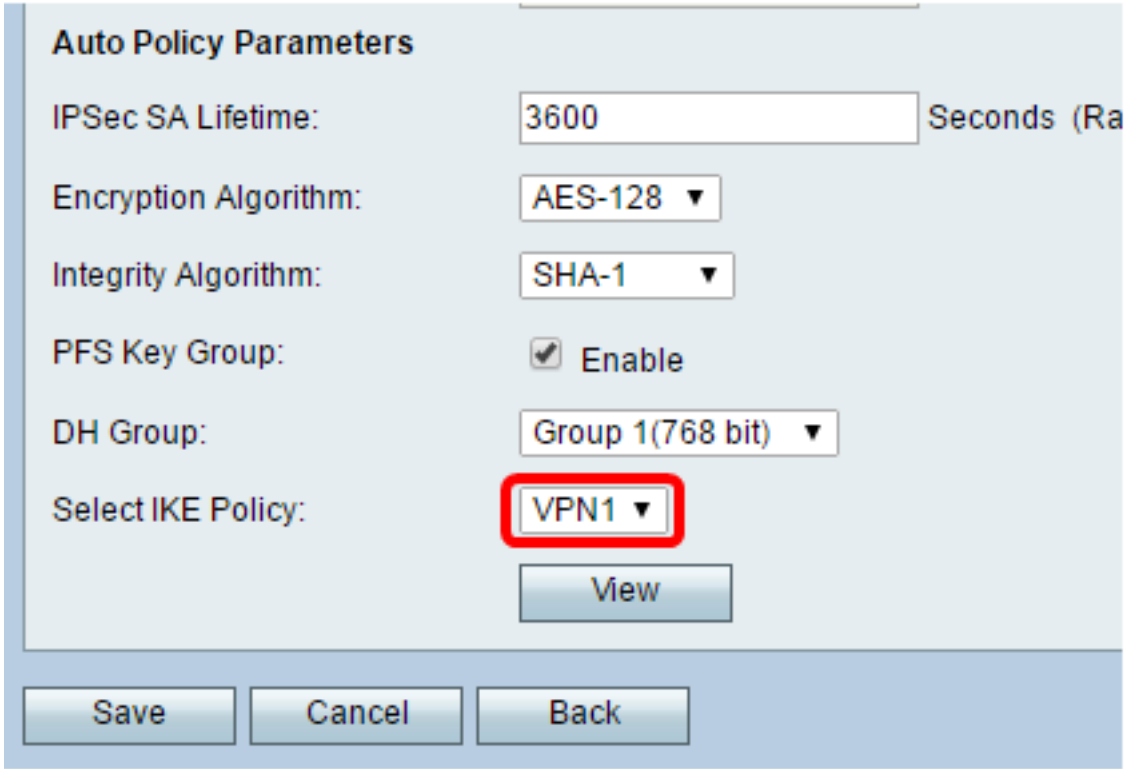
步骤5.（可选）如果在步骤4中选择启用PFS，请从DH组下拉列表中选择要加入的DH组。组编号越高，安全性越好。

注意：在本示例中，选择组1。

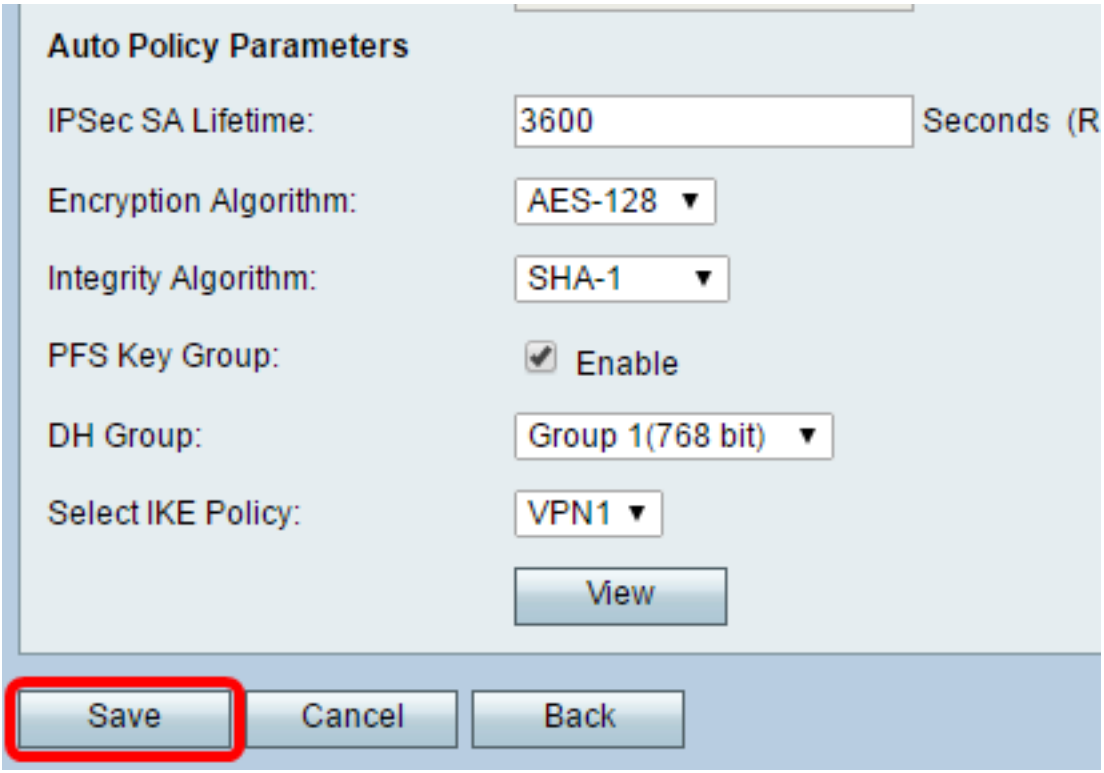


第6步：从选择IKE策略(Select IKE Policy)下拉列表中，选择要用于VPN策略的IKE策略。

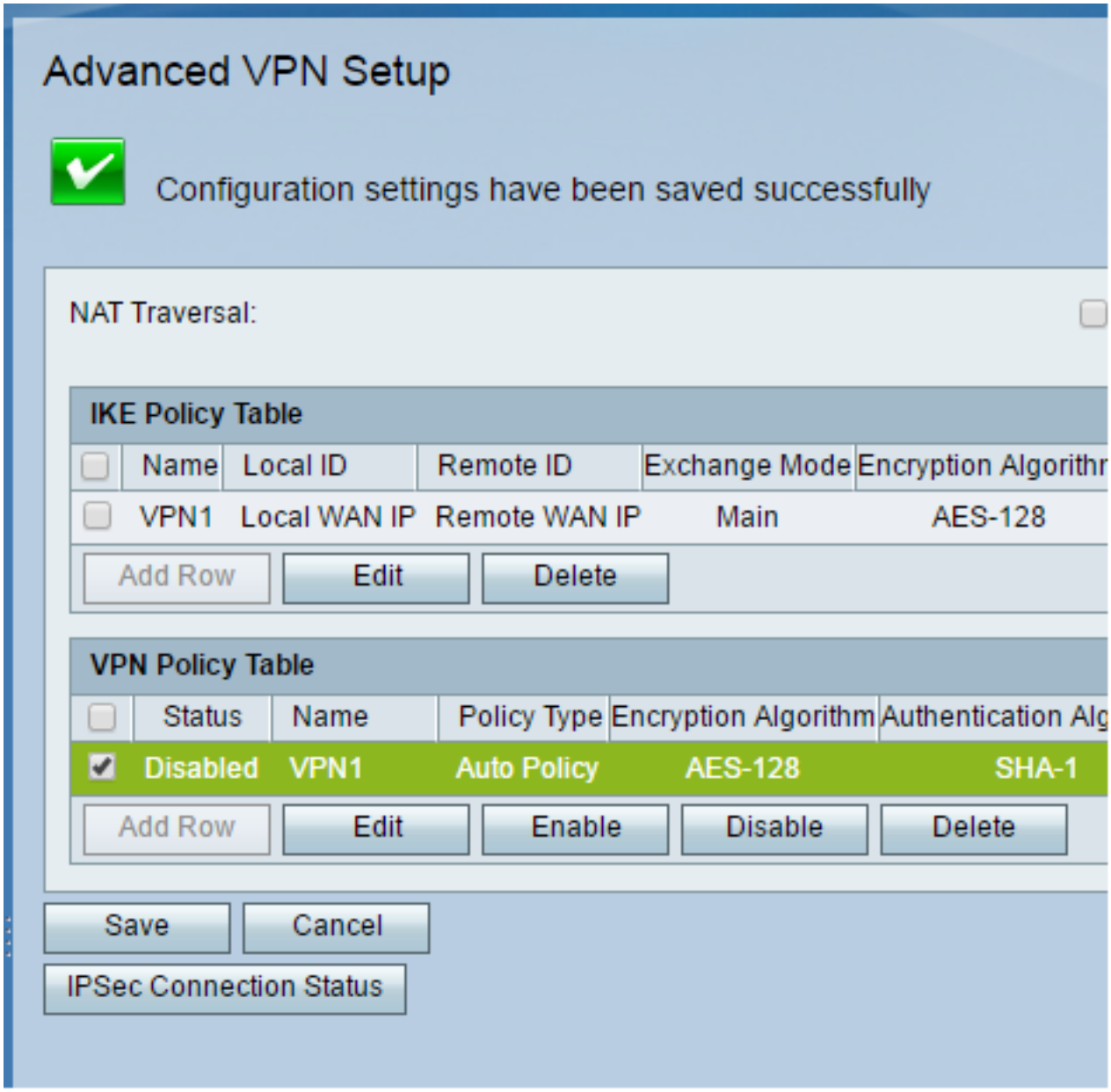
注意：在本示例中，只配置了一个IKE策略，因此只显示一个策略。



步骤7.单击**Save**。

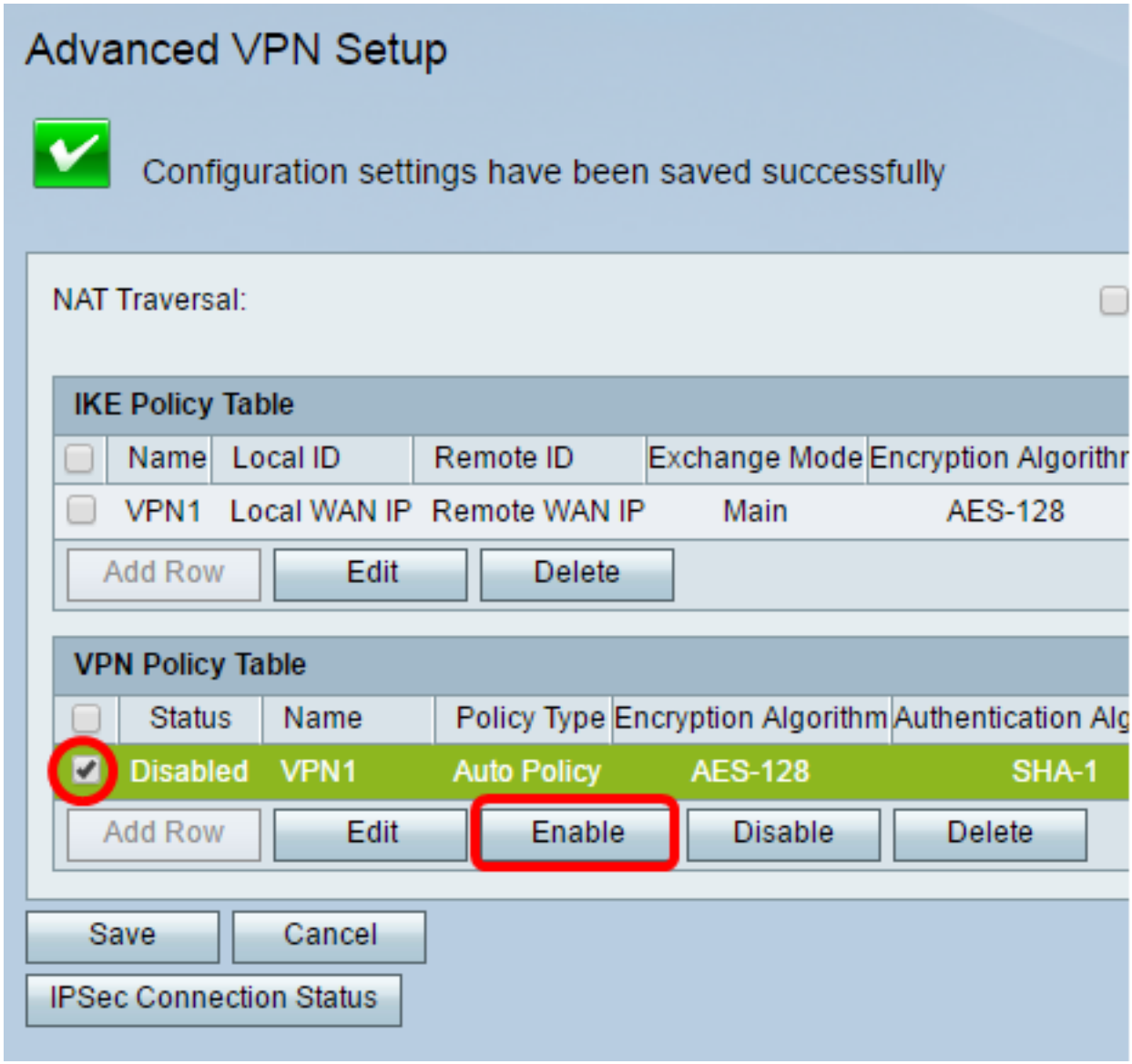


注意：系统将重新显示Advanced VPN Setup主页。系统将显示确认消息，确认配置设置已成功保存。

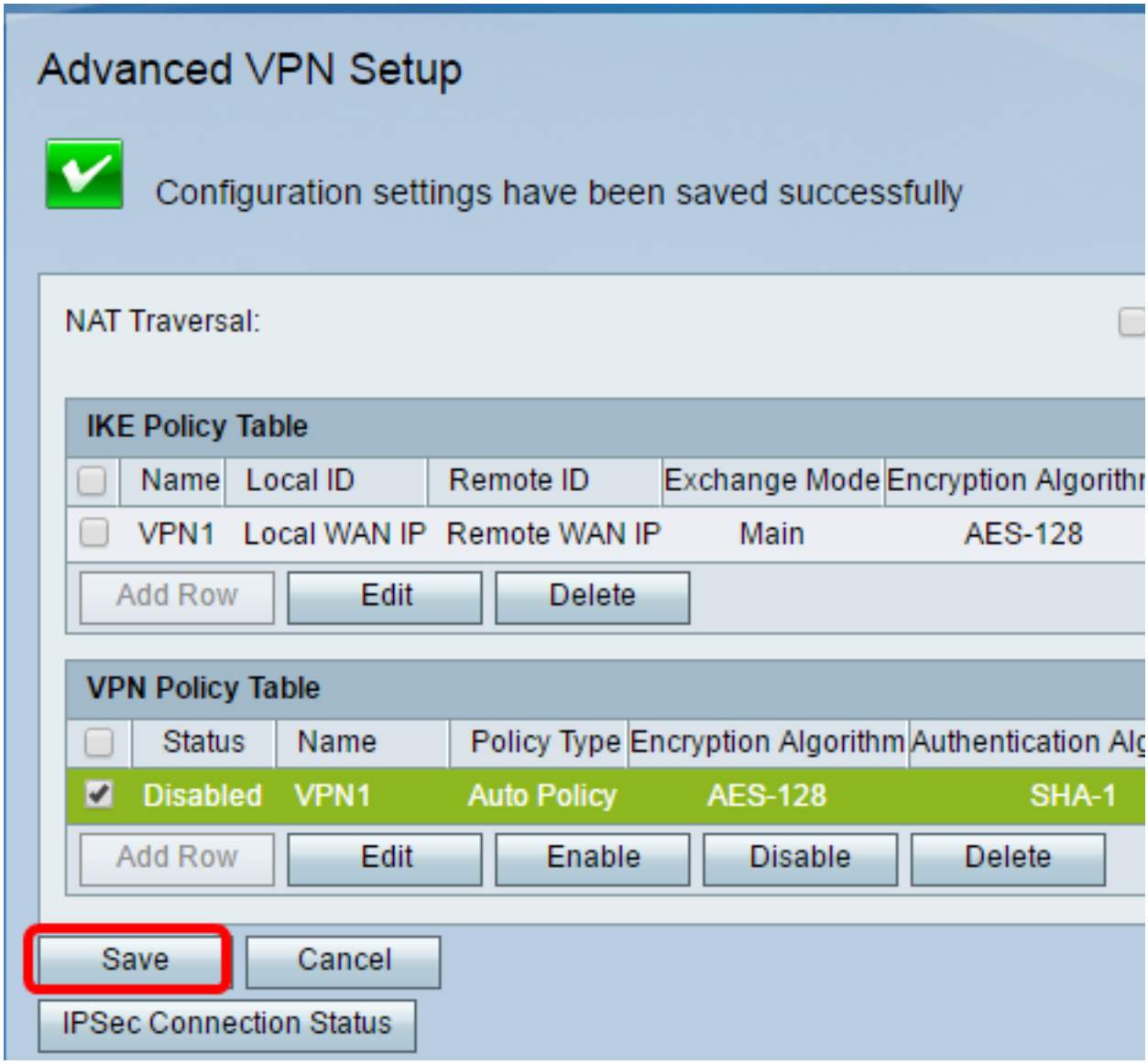


步骤8.在VPN策略表下，选中一个复选框以选择VPN，然后单击**Enable**。

注意：默认情况下禁用配置的VPN策略。


Advanced VPN Setup
Configuration settings have been saved successfully
NAT Traversal:
IKE Policy Table
Name
Local ID
Remote ID
Exchange Mode
Encryption Algorithr
VPN1
Local WAN IP
Remote WAN IP
Main
AES-128
Add Row
Edit
Delete
VPN Policy Table
Status
Name
Policy Type
Encryption Algorithm
Authentication Alg
Disabled
VPN1
Auto Policy
AES-128
SHA-1
Add Row
Edit
Enable
Disable
Delete
Save
Cancel
IPSec Connection Status

步骤9.单击**Save**。



您现在应该已经在RV130或RV130W路由器上成功配置了VPN策略。

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）。