RV215W上的高级VPN设置

目标

虚拟专用网络(VPN)是在网络内或网络之间建立的安全连接。VPN用于隔离指定主机和网络之间的流量与未授权主机和网络的流量。本文介绍如何在RV215W上配置高级VPN设置。

适用设备

·RV215W

软件版本

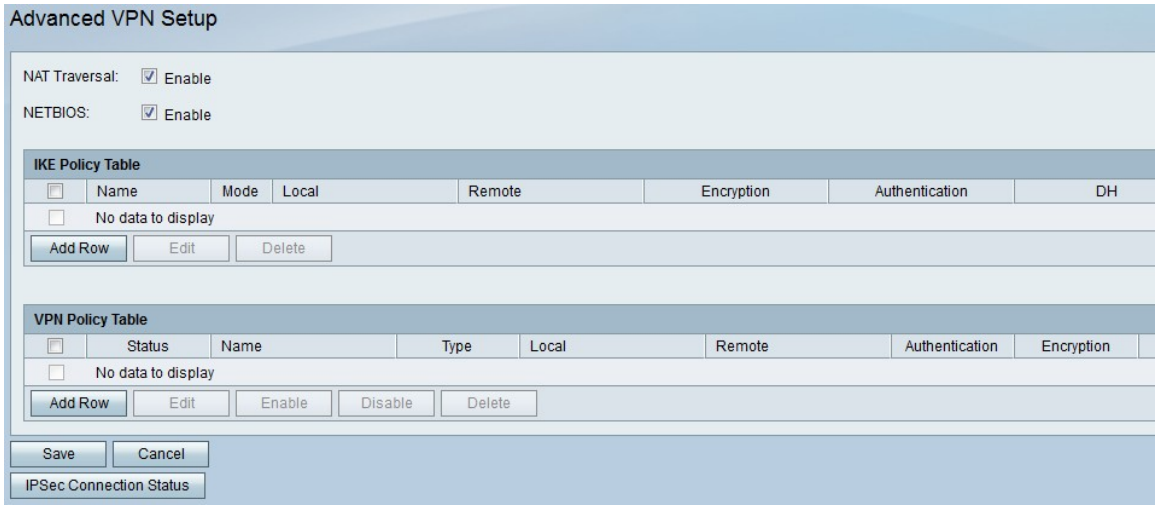
•1.1.0.5

高级VPN设置

初始设置

此过程说明如何配置高级VPN设置的初始设置。

步骤1.登录到Web配置实用程序，然后选择**VPN > Advanced VPN Setup**。“*高级VPN设置*”页打开：



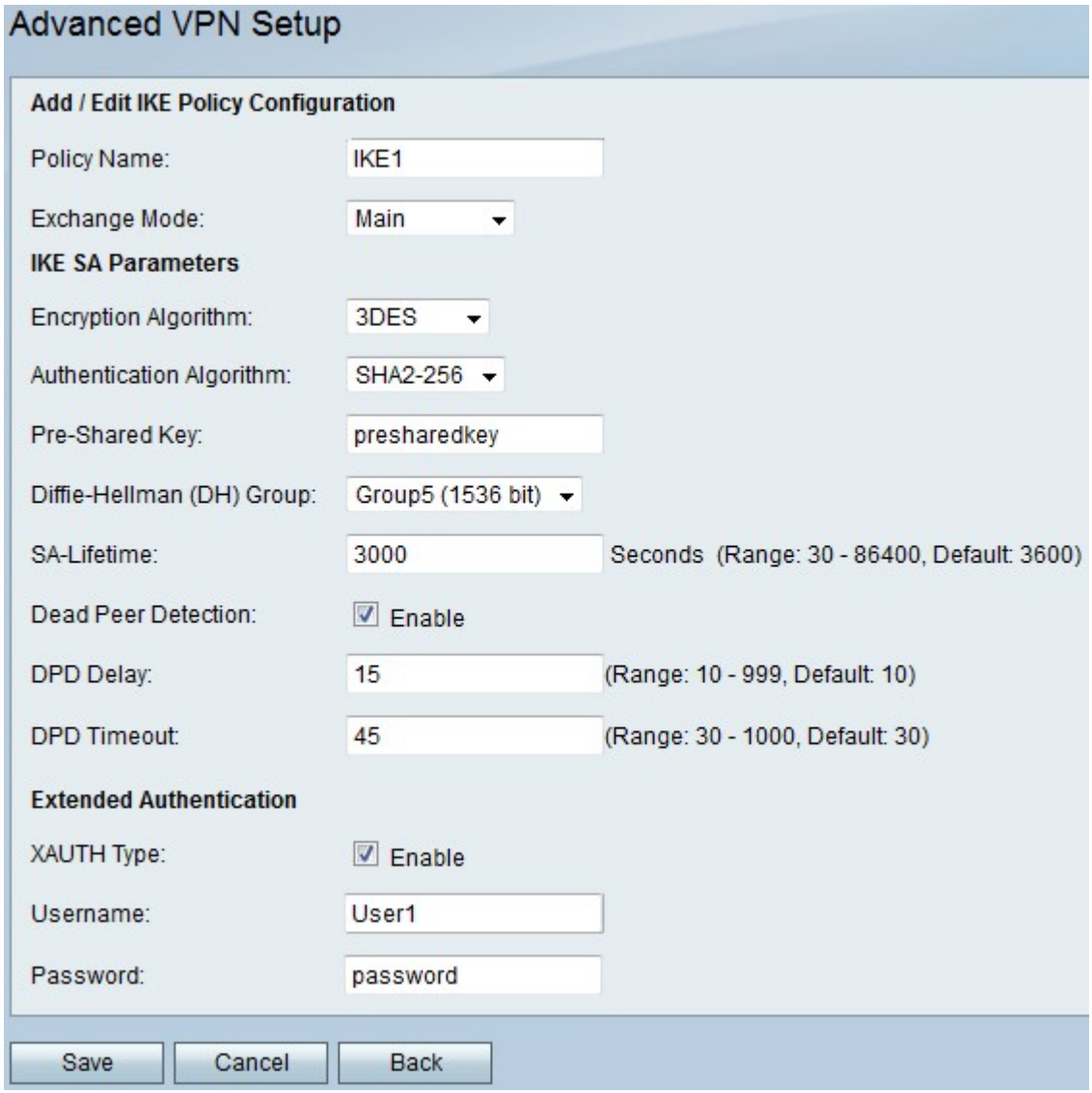
步骤2.（可选）如果要为VPN连接启用网络地址转换(NAT)遍历，请选中NAT遍历字段中的**启用**复选框。NAT穿越允许在使用NAT的网关之间建立VPN连接。如果VPN连接通过启用NAT的网关，请选择此选项。

步骤3.（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字段中的**启用**复选框。NetBIOS允许主机在LAN内相互通信。

IKE策略设置

互联网密钥交换(IKE)是用于在VPN中建立通信安全连接的协议。此已建立的安全连接称为安全关联(SA)。 此过程说明如何为VPN连接配置IKE策略以用于安全。要使VPN正常运行，两个端点的IKE策略应相同。

步骤1.在IKE策略表中，单击**添加行**以创建新的IKE策略。要编辑IKE策略，请选中该策略的复选框，然后单击**Edit**。“高级*VPN设置*”页更改：

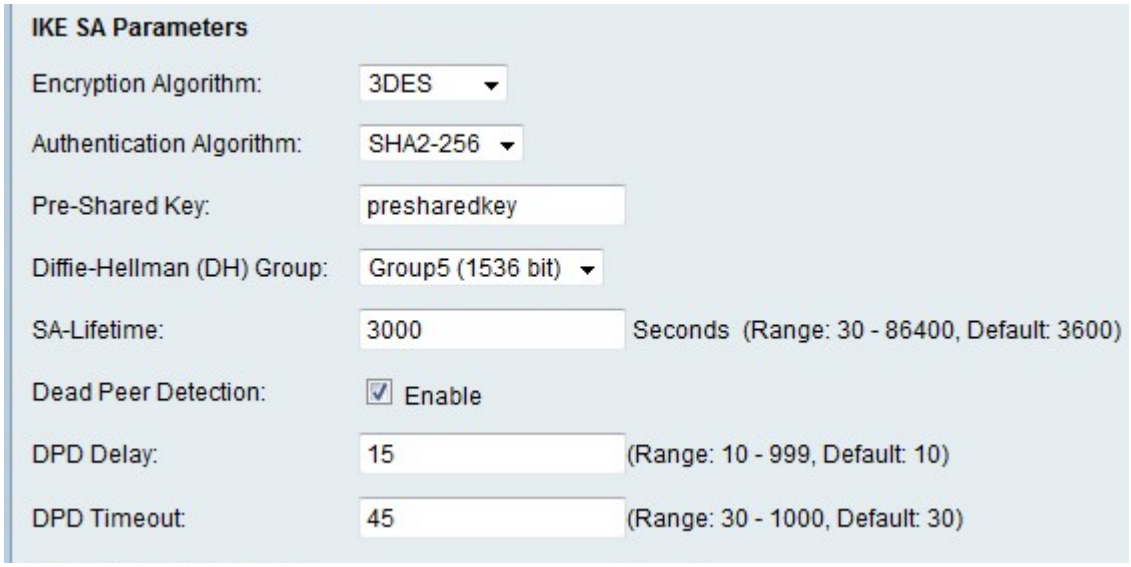


步骤2.在Policy Name字段中，输入IKE策略的名称。

步骤3.从Exchange Mode下拉列表中，选择一个选项。

·Main — 此选项允许IKE策略比主动模式更安全但更慢地运行。如果需要更安全的VPN连接，请选择此选项。

·主动 — 此选项允许IKE策略比主模式运行更快但安全性较低。如果需要更快的VPN连接，请选择此选项。



步骤4.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位旧式加密方法，它不是一种非常安全的加密方法，但可能需要它才能向后兼容。

·3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，用于增加密钥大小，因为它对数据加密三次。这比DES提供更高的安全性，但比AES安全性更低。

·AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，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 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，比AES-256快但不安全。

·AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步骤5.从Authentication Algorithm下拉列表中，选择一个选项。

·MD5 — 消息摘要算法5(MD5)使用128位哈希值进行身份验证。MD5的安全性较低，但比SHA-1和SHA2-256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慢但更安全，而SHA-1比SHA2-256快但不安全。

·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慢但安全。

步骤6.在Pre-Shared Key字段中，输入IKE策略使用的预共享密钥。

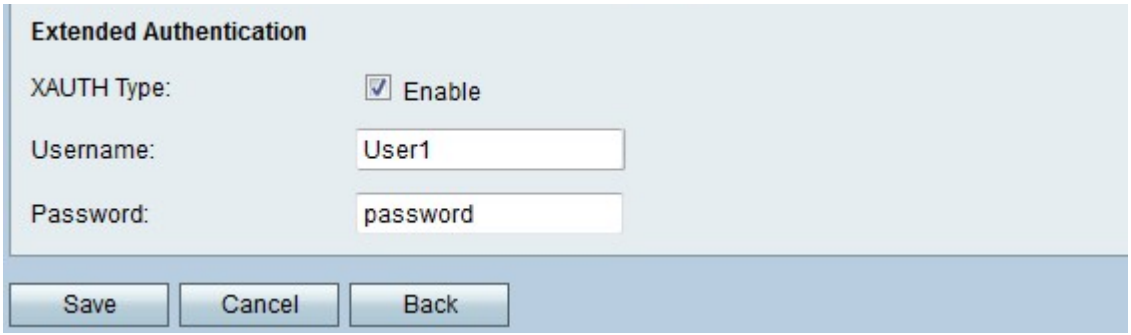
步骤7.从Diffie-Hellman(DH)组下拉列表中，选择IKE使用的DH组。DH组中的主机可以在彼此不知情的情况下交换密钥。组位数越高，组就越安全。

步骤8.在SA-Lifetime字段中，输入VPN的SA在续约SA之前的持续时间（以秒为单位）。

第9步。（可选）选中Dead Peer Detection字段中的**Enable**复选框以启用Dead Peer Detection(DPD)。DPD监控IKE对等体，以查看对等体是否已停止运行。DPD可防止在非活动对等体上浪费网络资源。

第10步。（可选）如果在第9步中启用DPD，请在DPD Delay字段中输入检查对等体活动的频率（以秒为单位）。

第11步。（可选）如果在第9步中启用了DPD，请在DPD Timeout字段中输入在丢弃非活动对等体之前等待的秒数。



第12步。（可选）选中XAUTH Type字段中的**Enable**复选框以启用扩展身份验证(XAUTH)。XAUTH允许多个用户使用单个VPN策略，而不是每个用户的VPN策略。

第13步。（可选）如果在第12步中启用XAUTH，请在Username字段中输入要用于策略的用户名。

第14步。（可选）如果在第12步中启用XAUTH，请在Password字段中输入用于策略的密码。

步骤15.单击“**保存**”。系统将重*新显示原*始的“高级VPN设置”页。

VPN策略设置

此过程说明如何配置VPN连接的VPN策略。要使VPN正常运行，两个终端的VPN策略应相同。

步骤1.在VPN策略表中，单击**添加行**以创建新的VPN策略。要编辑VPN策略，请选中该策略的复选框，然后单击**Edit**。“高*级VPN设置*”页更改：

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

步骤2.在Policy Name字段中，输入VPN策略的名称。

步骤3.从Policy Type下拉列表中，选择一个选项。

·手动策略 — 此选项允许您配置密钥以进行数据加密和完整性。

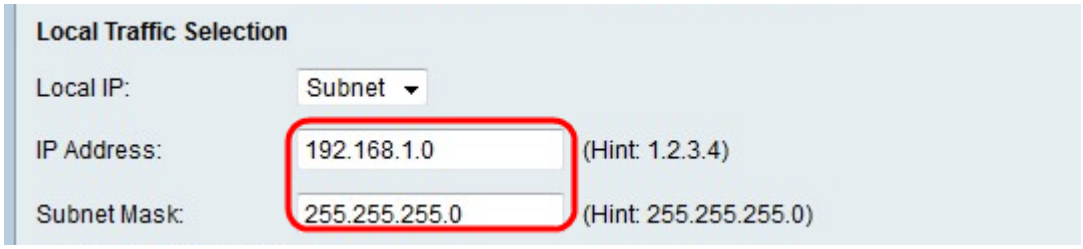
·自动策略(Auto Policy) — 此选项使用IKE策略进行数据完整性和加密密钥交换。

步骤4.从Remote Endpoint下拉列表中，选择一个选项。

·IP Address — 此选项通过公有IP地址标识远程网络。

·FQDN — 此选项使用完全限定域名(FQDN)来标识远程网络。

步骤5.在Remote Endpoint下拉列表下的文本输入字段中，输入远程地址的公有IP地址或域名。



步骤6.从Local IP下拉列表中，选择一个选项。

·单个 — 此选项使用单台主机作为本地VPN连接点。

·子网 — 此选项使用本地网络的子网作为本地VPN连接点。

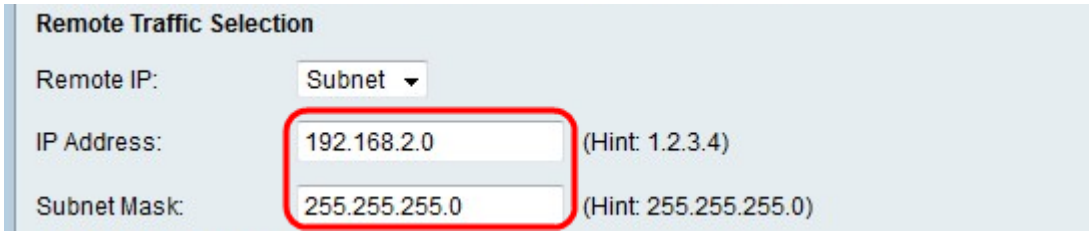
步骤7.在IP Address字段中，输入本地子网或主机的主机或子网IP地址。

步骤8.（可选）如果在步骤6中选择了子网，请在子网掩码字段中输入本地子网的子网掩码。

步骤9.从Remote IP下拉列表中，选择一个选项。

·单个 — 此选项使用单台主机作为远程VPN连接点。

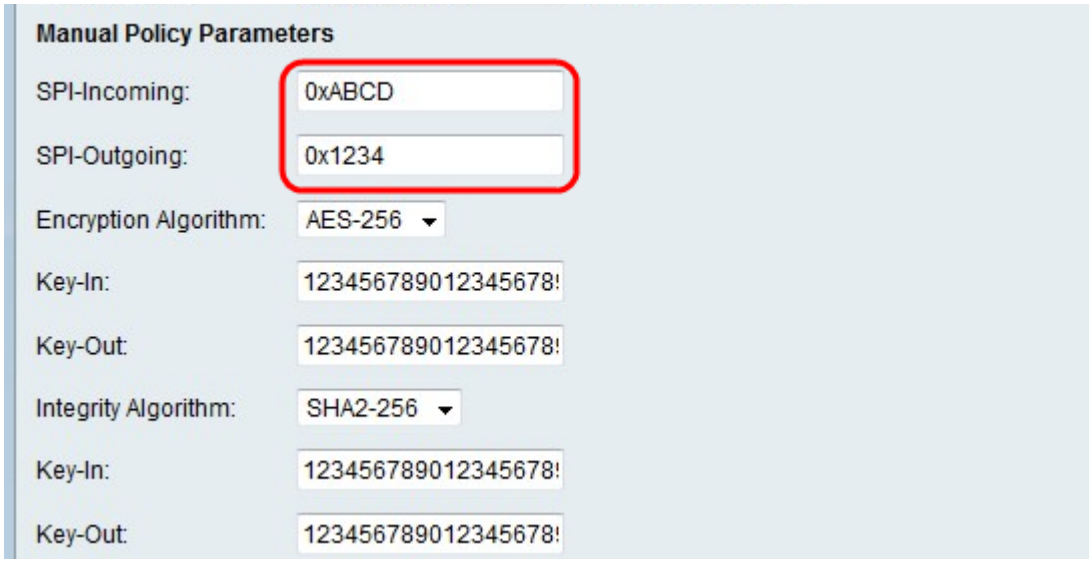
·子网 — 此选项使用远程网络的子网作为远程VPN连接点。



步骤10.在IP Address字段中，输入远程子网或主机的主机或子网IP地址。

步骤11.（可选）如果在步骤9中选择了子网，请在子网掩码字段中输入远程子网的子网掩码。

注意：如果在步骤3中选择手动策略，请执行步骤12至步骤19;否则，请跳过步骤20。



步骤12.在SPI-Incoming字段中，为VPN连接上的传入流量输入安全参数索引(SPI)标记的三到八个十六进制字符。SPI标记用于区分一个会话的流量与其他会话的流量。

步骤13.在SPI-Outgoing字段中，为VPN连接上的传出流量输入SPI标记的三到八个十六进制字符。

步骤14.从Encryption Algorithm下拉列表中，选择一个选项。

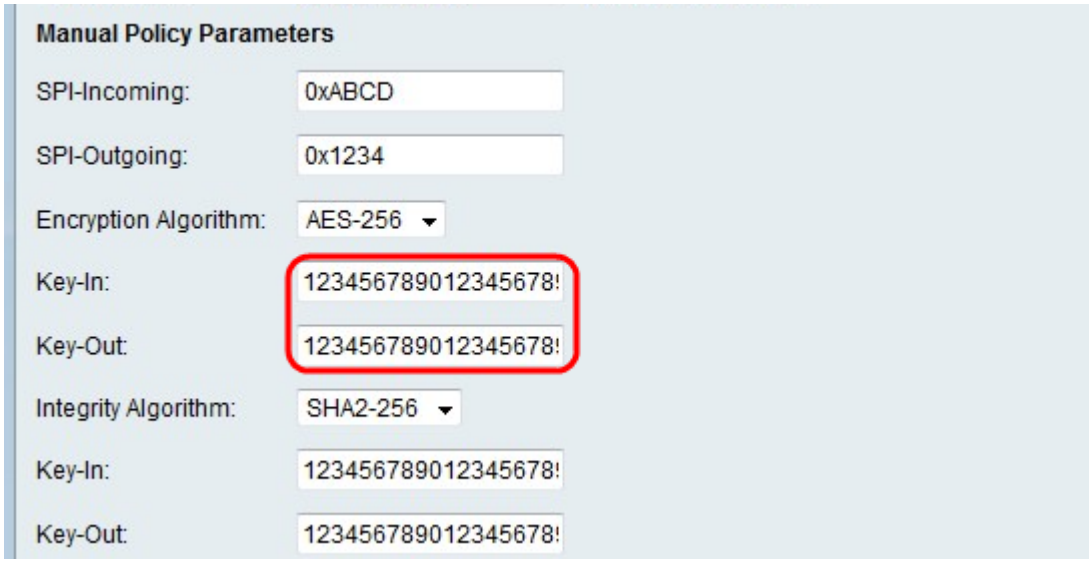
·DES — 数据加密标准(DES)是一种56位旧式加密方法，它不是一种非常安全的加密方法，但可能需要它才能向后兼容。

·3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，用于增加密钥大小，因为它对数据加密三次。这比DES提供更高的安全性，但比AES安全性更低。

·AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，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 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，比AES-256快但不安全。

·AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。



步骤15.在Key-In字段中，输入入站策略的密钥。密钥长度取决于步骤14中选择的算法。

·DES使用8个字符的密钥。

·3DES使用24个字符的键。

·AES-128使用12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。

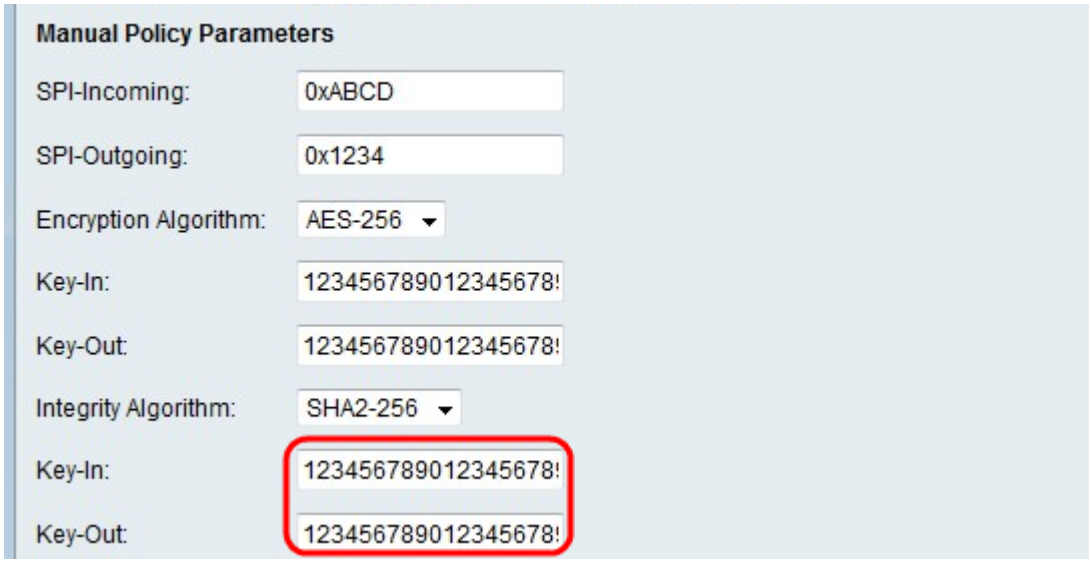
步骤16.在Key-Out字段中，输入传出策略的密钥。密钥长度取决于步骤14中选择的算法。密钥长度与步骤15相同。

步骤17.从Integrity Algorithm下拉列表中，选择一个选项。

·MD5 — 消息摘要算法5(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快。

·SHA-1 — 安全散列函数1(SHA-1)使用160位散列值来实现数据完整性。SHA-1比MD5慢但更安全，而SHA-1比SHA2-256快但不安全。

·SHA2-256 — 具有256位哈希值(SHA2-256)的安全哈希算法2使用256位哈希值来实现数据完整性。SHA2-256比MD5和SHA-1慢但安全。



步骤18.在Key-In字段中，输入入站策略的密钥。密钥长度取决于步骤17中选择的算法。

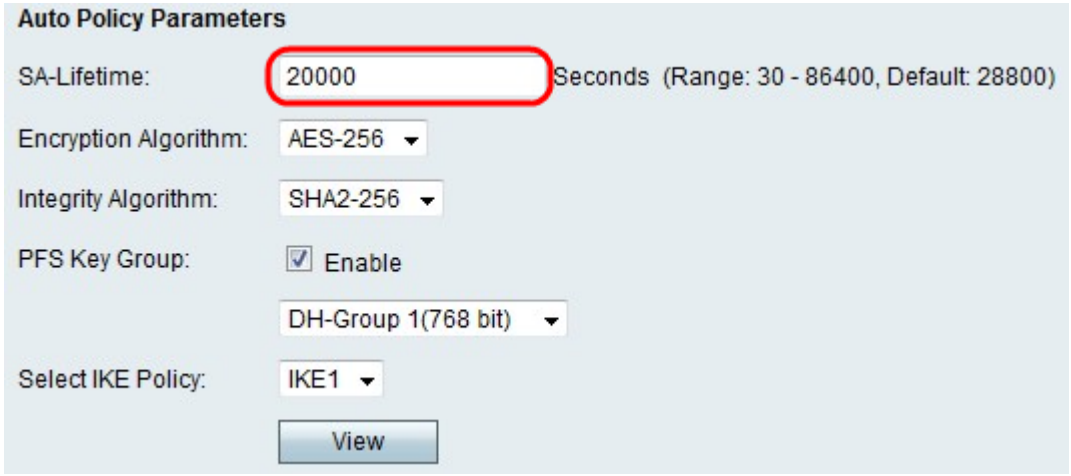
·MD5使用16个字符的键。

·SHA-1使用20个字符的密钥。

·SHA2-256使用32个字符的密钥。

步骤19.在Key-Out字段中，输入传出策略的密钥。密钥长度取决于步骤17中选择的算法。密钥长度与步骤18相同。

注意：如果在步骤3中选择Auto Policy，请执行步骤20至步骤25;否则，请跳至步骤26。



步骤20.在SA-Lifetime字段中，输入SA在续约前持续的时间（以秒为单位）。

步骤21.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位旧式加密方法，它不是一种非常安全的加密方法，但可能需要它才能向后兼容。

·3DES — 三重数据加密标准(3DES)是一种168位的简单加密方法，用于增加密钥大小，因为它对数据加密三次。这比DES提供更高的安全性，但比AES安全性更低。

·AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，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 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，比AES-256快但不安全。

·AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步骤22.从Integrity Algorithm下拉列表中，选择一个选项。

·MD5 — 消息摘要算法5(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快。

·SHA-1 — 安全散列函数1(SHA-1)使用160位散列值来实现数据完整性。SHA-1比MD5慢但更安全，而SHA-1比SHA2-256快但不安全。

·SHA2-256 — 具有256位哈希值(SHA2-256)的安全哈希算法2使用256位哈希值来实现数据完整性。SHA2-256比MD5和SHA-1慢但安全。

步骤23.选中PFS密钥组中的**Enable**复选框以启用完全转发保密(PFS)。PFS提高了VPN安全性，但降低了连接速度。

第24步。（可选）如果您选择在第23步中启用PFS，请为以下下拉列表选择要加入的Diffie-Hellman(DH)组。组编号越高，组就越安全。

步骤25.从Select IKE Policy下拉列表中，选择要用于VPN策略的IKE策略。

注意：如果单击“**View**”，则会指向“Advanced VPN Setup”页面的“IKE*配置*”部分。

步骤26.单击“**保存**”。系统将重*新显示原*始的“高级VPN设置”页。

步骤27.单击“**保存**”。