配置在一个RV34x系列路由器的一个互联网协议安全(IPSec)配置文件

客观

互联网协议安全(IPSec)提供在两个对等体之间的安全隧道，例如两路由器。被认为敏感，并且应该通过这些安全隧道发送的参数应该通过指定这些隧道的特性定义的信息包，以及应该使用保护这些敏感信息包。然后，当IPSec对等体看到这样一个敏感信息包时，它设置适当的安全隧道并且通过此隧道发送信息包到远端对等体。

当IPsec在防火墙或路由器时实现，提供可以适用于交叉周界的所有数据流的强有力的安全保障。在公司或工作组内的数据流不导致与安全相关处理的开销。

本文目标将显示您如何配置在一个RV34x系列路由器的IPSec配置文件。

可适用的设备

- RV34x系列

软件版本

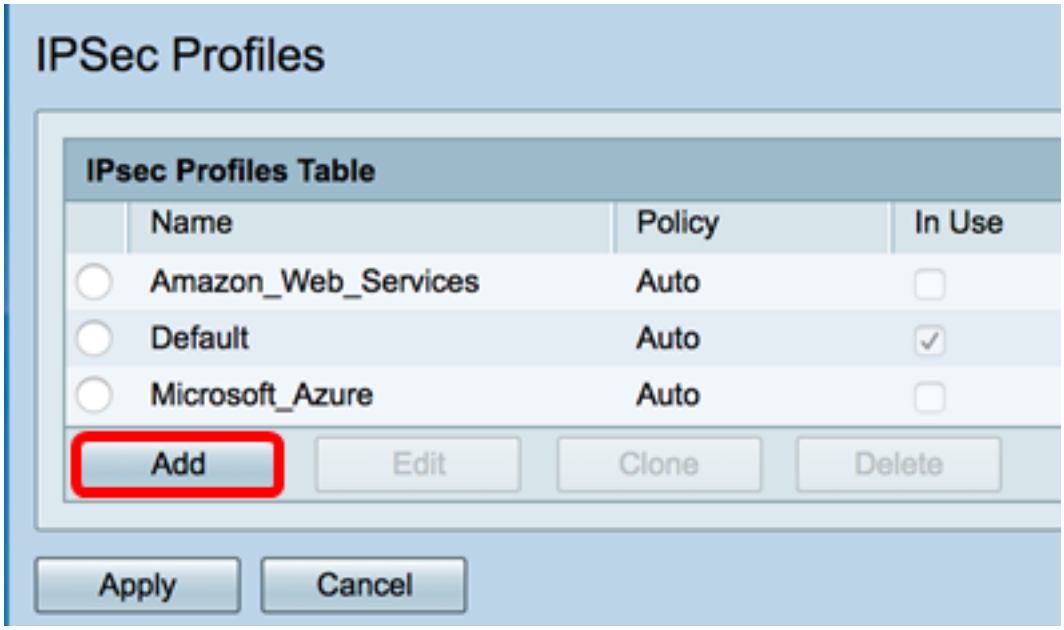
- 1.0.1.16

配置IPSec配置文件

创建IPSec配置文件

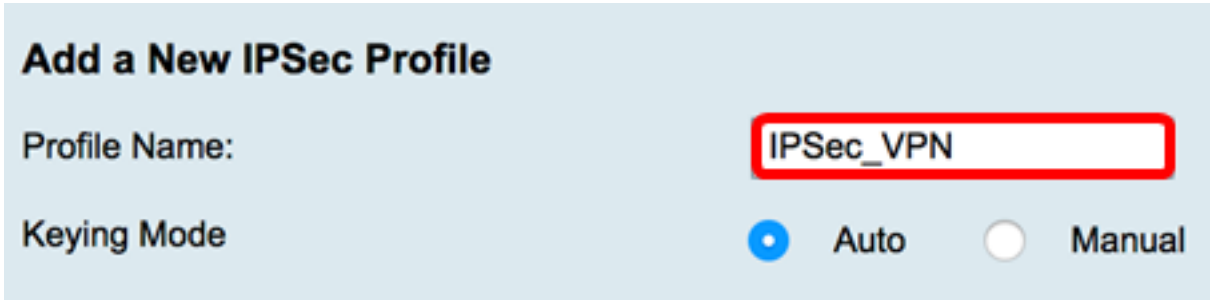
步骤1.登陆到路由器的基于Web的工具并且选择**VPN > IPSec配置文件**。

Step 2.IPSec配置文件表显示现有的配置文件。点击**添加**创建新配置文件。



步骤3.创建一个名字对于在*配置文件名字*字段的配置文件。配置文件名字必须包含字母或数字字符和仅一条下划线(_)特殊字符的。

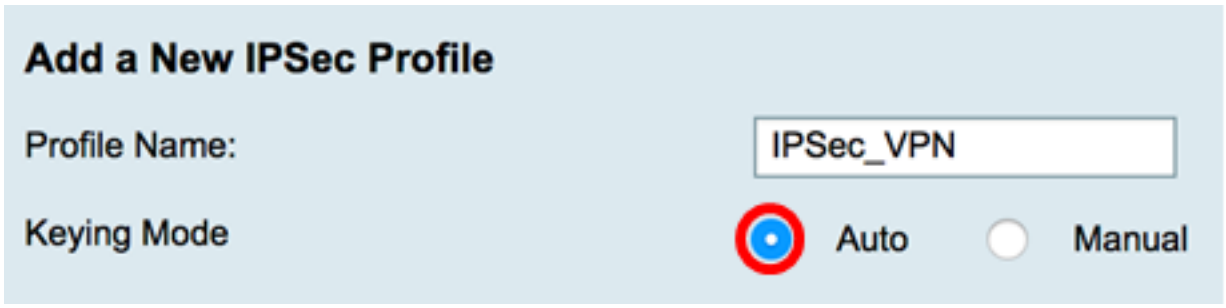
Note:在本例中， IPSec_VPN使用作为IPSec配置文件名字。



步骤4.点击一个单选按钮确定配置文件将使用验证的密匙交换方法。选项是：

- 自动—自动地设置策略参数。此选项使用一个Internet Key Exchange (IKE)策略数据完整性和加密密钥交换。如果这被选择，在自动策略参数范围下的配置设置是启用的。点击此处配置自动设置。
- 手工—此选项允许您手工配置数据加密和完整性的键虚拟专用网络(VPN)隧道的。如果这被选择，在手工的策略参数范围下的配置设置是启用的。点击此处配置手工的设置。

Note:对于此示例，自动被选择了。



配置自动设置

第 1 步：在阶段1选项地区中，请选择适当的Diffie-Hellman (DH)组与键一起使用在从DH组下拉列表的阶段1。Diffie-Hellman是用于连接交换预共享密钥集的一个加密密钥交换协议。位取

决于算法的力量。选项是：

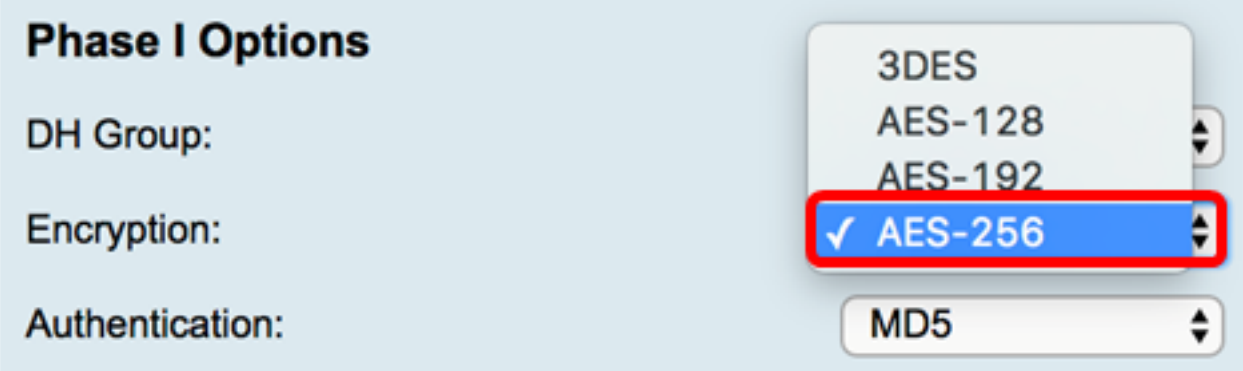
- Group2 - 1024位—比Group1计算关键慢，但是安全。
- Group5 - 1536位—计算键最慢，但是最安全。

Note:在本例中， Group2-1024位被选择。

Step 2.从加密下拉列表，请选择适当的加密方法加密和解码封装安全有效载荷(ESP)和互联网安全协会和密钥管理协议(ISAKMP)。选项是：

- 3DES —三重数据加密标准。
- AES-128 —高级加密标准使用一个128-bit键。
- AES-192 —高级加密标准使用一个192-bit键。
- AES-256 —高级加密标准使用一个256-bit键。

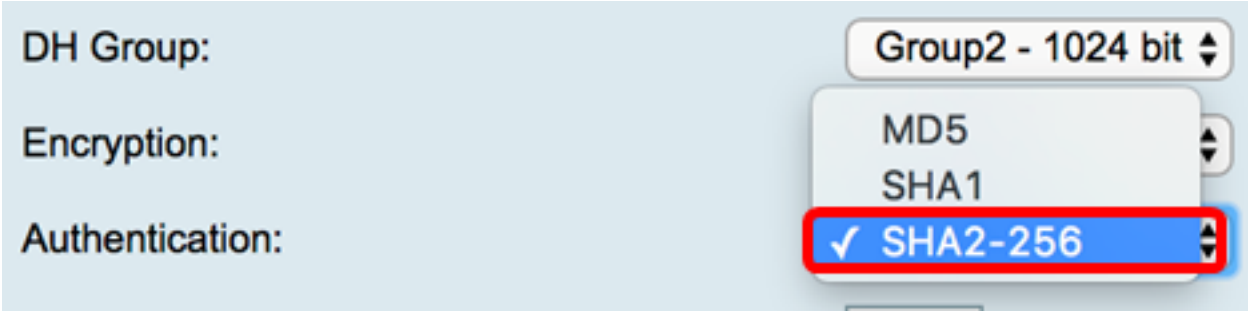
Note: AES是加密标准方法在DES和3DES的其更加巨大的性能和安全的。加长AES键将强化与下落在性能的安全。对于此示例， AES-256被选择。



第 3 步：从认证下拉菜单，请选择将确定的认证方法ESP和ISAKMP如何验证。选项是：

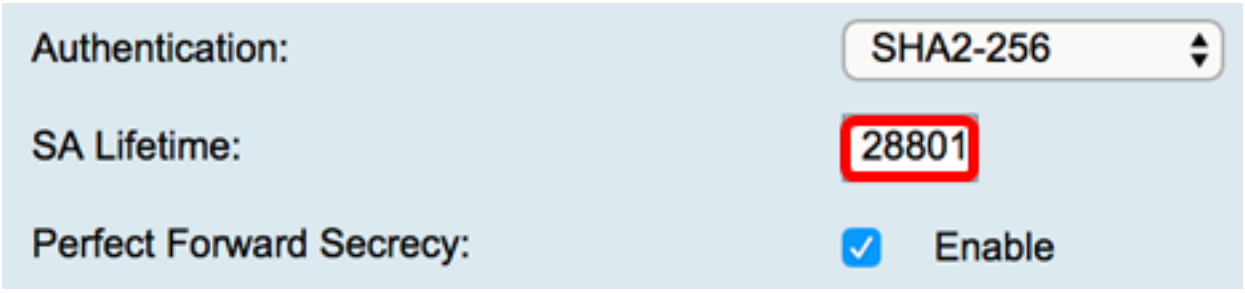
- MD5 —消息分类算法有一个128-bit Hash值。
- SHA-1 —安全散列算法有一个160-bit Hash值。
- SHA2-256 —与256-bit Hash值的安全散列算法。

Note: MD5和SHA是两个密码散列函数。他们采取数据部分，变紧密它，并且创建不典型地是再现的一个唯一十六进制输出。在本例中， SHA2-256被选择。

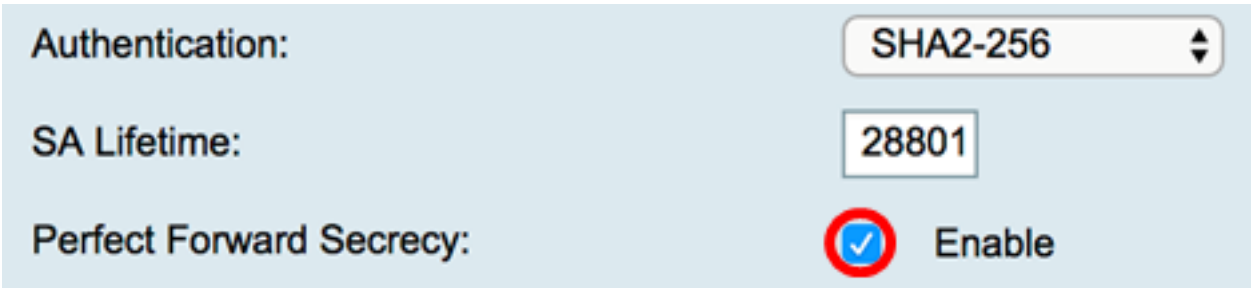


第 4 步：在*SA寿命*字段，请输入在120到86400之间的值范围。这是Internet Key Exchange (IKE)安全关联(SA)在此阶段内将依然是活动的时间长度。DEFAULT值是28800。

Note:在本例中，使用28801。

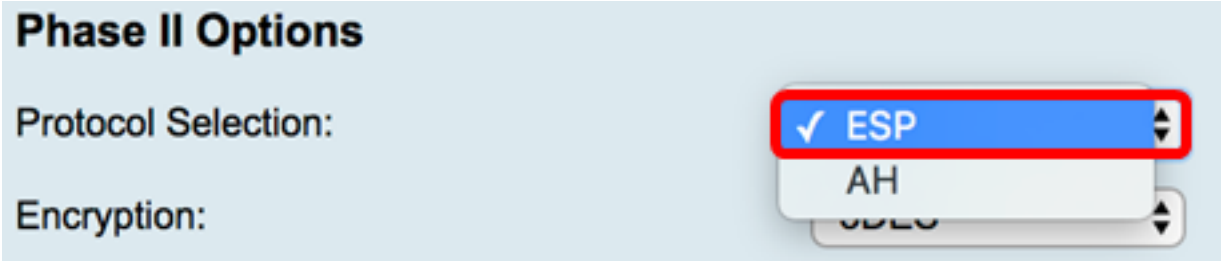


第5.步(可选的)检查生成IPSec数据流加密和认证的一新密钥的**Enable (event)优秀的转发保密性**复选框。



第6.步。从协议选择下拉菜单在第II阶段选项地区，请选择协议类型适用于协商的第二阶段。选项是：

- ESP —如果这被选择，请跳到第7步选择关于怎样的一个加密方法ESP信息包将被加密并且解码。提供数据保密性服务和可选的数据验证的安全协议和反重放服务。ESP封装将保护的数据。
- AH —认证报头(AH)是提供数据验证和可选的反重放服务的安全协议。AH在将保护的数据被嵌入(充分的IP数据包)。如果这被选择了，请跳到第8步。

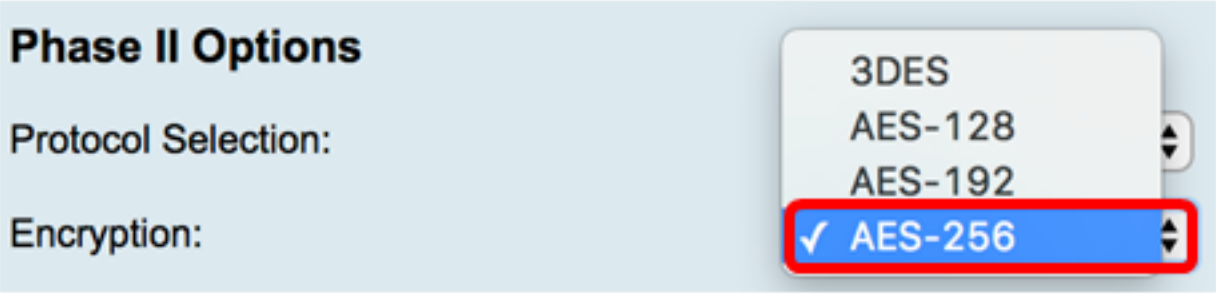


第 7 步：如果ESP在第6步被选择了，请选择适当的加密方法加密和解码ESP和ISAKMP从加密下拉列表。选项是：

- 3DES —三重数据加密标准。

- AES-128 —高级加密标准使用一个128-bit键。
- AES-192 —高级加密标准使用一个192-bit键。
- AES-256 —高级加密标准使用一个256-bit键。

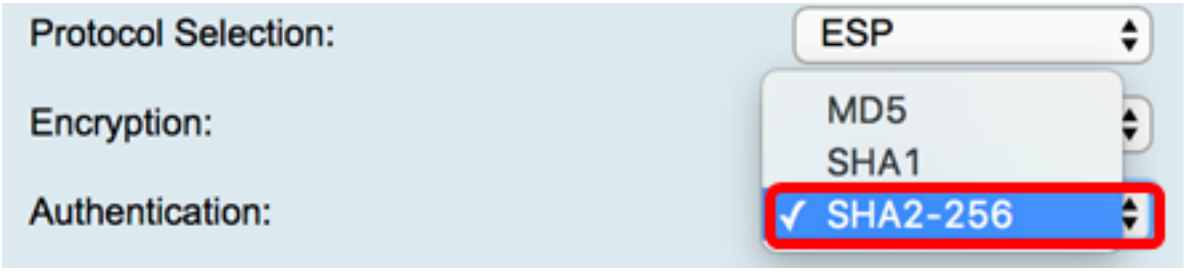
Note:在本例中， AES-256被选择。



第8.步。从认证下拉菜单，请选择将确定的认证方法ESP和ISAKMP如何验证。选项是：

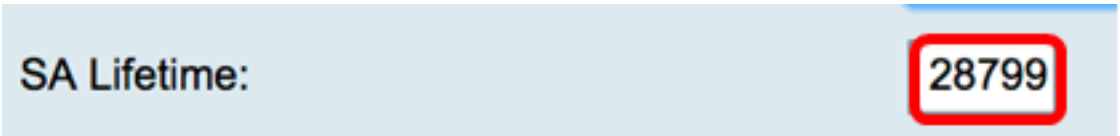
- MD5 —消息分类算法有一个128-bit Hash值。
- SHA-1 —安全散列算法有一个160-bit Hash值。
- SHA2-256 —与256-bit Hash值的安全散列算法。

Note:在本例中，使用SHA2-256。



第9.步。在*SA寿命*字段，请输入在120到28800之间的值范围。这是IKE SA在此阶段内将保持活动的时间长度。DEFAULT值是3600。

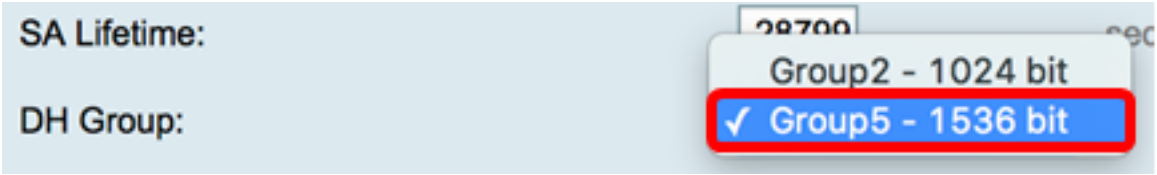
Note:在本例中，使用28799。

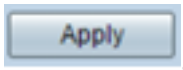


第10.步。从DH组下拉列表，请选择适当的Diffie-Hellman (DH)组与键一起使用在第2阶段。选项是：

- Group2 – 1024位—比Group1计算关键慢，但是安全。
- Group5 – 1536位—计算键最慢，但是最安全。

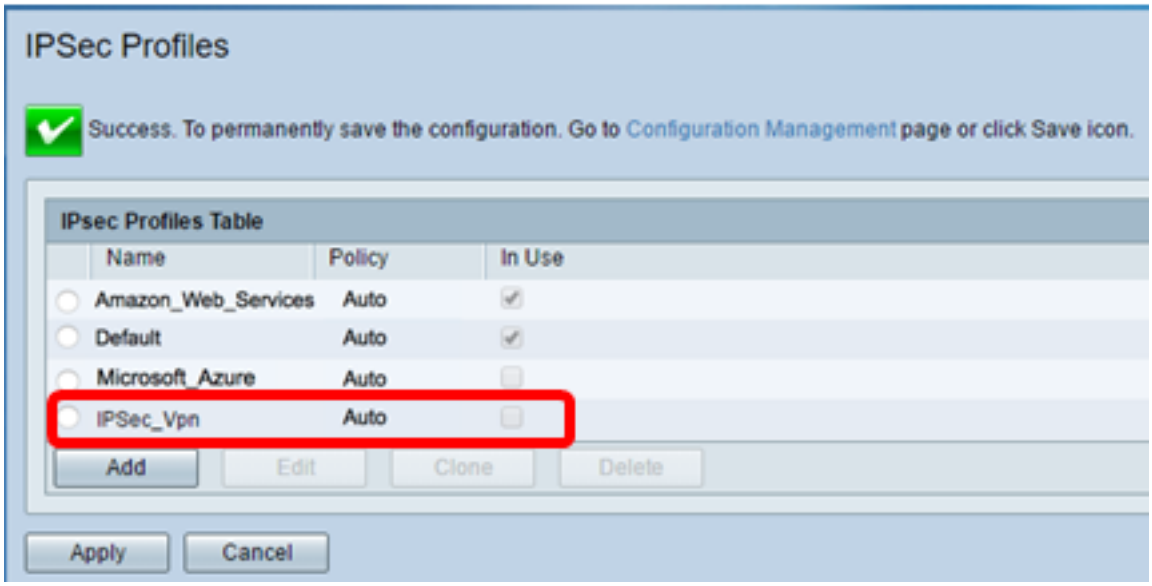
Note:在本例中， Group5 – 1536位被选择。



步骤11.点击 

。

Note:您将被采取回到IPSec配置文件表，并且新建立的IPSec配置文件应该当前出现。



步骤12。(可选)永久保存配置，请去复制/保存配置页或点击 

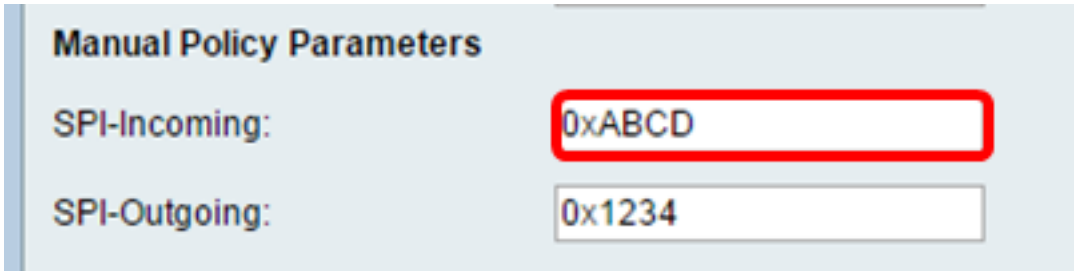
图标在页的上面的部分。

您应该成功当前配置了在一个RV34x系列路由器的自动IPSec配置文件。

配置手工的设置

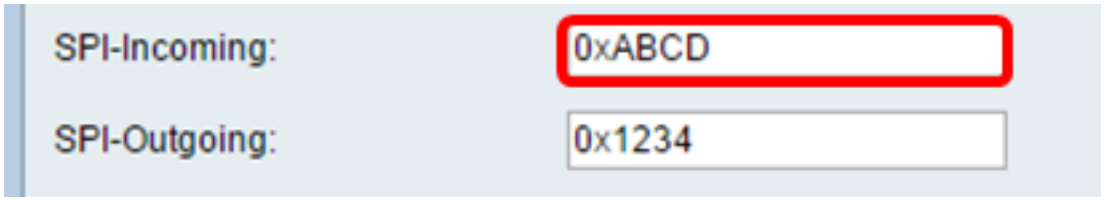
第 1 步：在SPI*流入*字段，从100请输入一个十六进制数字范围到安全参数索引(SPI)标记的FFFFFFF在VPN连接的流入的数据流的。SPI标记用于与其他会话数据流区分一次会话数据流。

Note:对于此示例，使用0xABCD。



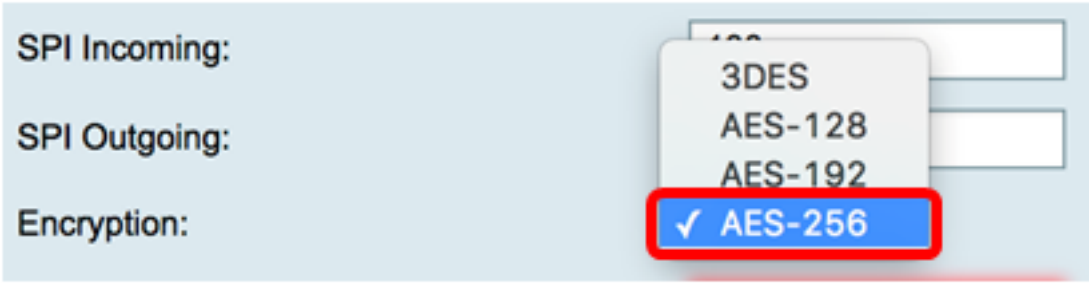
Step 2.在SPI*流出的*字段，从100请输入一个十六进制数字范围到SPI标记的FFFFFFF在VPN连接的流出的数据流的。

Note:对于此示例，使用0x1234。



步骤3.从加密下拉列表选择选项。选项是3DES、AES-128、AES-192和AES-256。

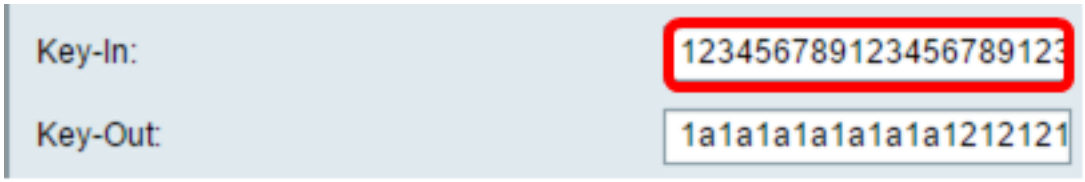
Note:在本例中， AES-256被选择。



第 4 步：在KEY*在*字段，请输入Inbound政策的一个键。密钥长度取决于在选择的算法第3.步。

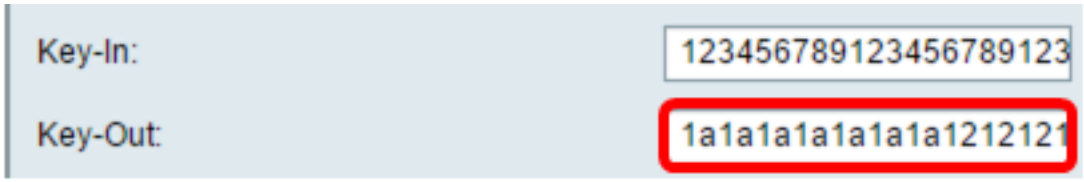
- 3DES使用一个48字符键。
- AES-128使用一个32字符键。
- AES-192使用一个48字符键。
- AES-256使用一个64字符键。

Note:在本例中，…使用12345678912345678912 3。



第 5 步：在*KEY*字段，请输入流出的策略的一个键。密钥长度取决于在选择的算法第3.步。

Note:在本例中，…使用1a1a1a1a1a1a1a121212。



步骤6.从手工的完整性算法下拉列表选择选项。

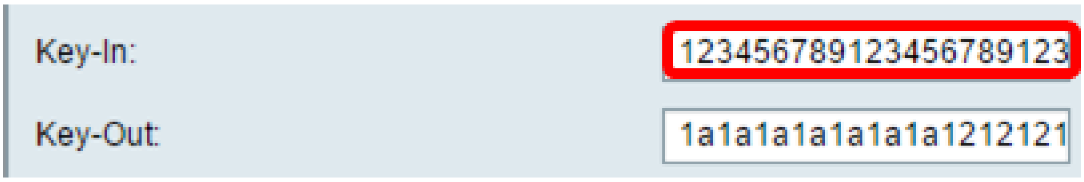
- MD5 —使用一个128-bit Hash值数据完整性。MD5比SHA-1和SHA2-256较不安全，但是快速地。
- SHA-1 —使用一个160-bit Hash值数据完整性。SHA-1比MD5更慢，但是安全，并且SHA-1比SHA2-256更加快速，但是巩固。
- SHA2-256 —使用一个256-bit Hash值数据完整性。SHA2-256比MD5和SHA-1是慢，但是巩固。

Note:在本例中， MD5被选择。

第 7 步：在KEY*在字段*，请输入Inbound政策的一个键。密钥长度取决于在选择的算法第6.步。

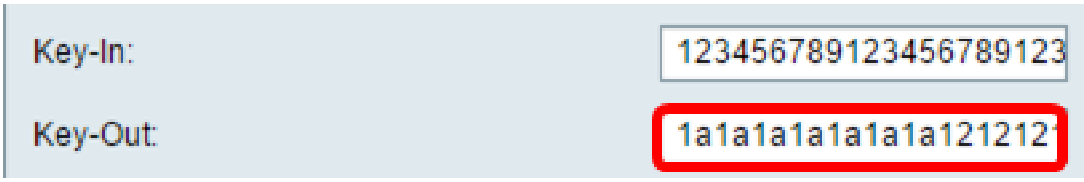
- MD5使用一个32字符键。
- SHA-1使用一个40字符键。
- SHA2-256使用一个64字符键。

Note:在本例中，…使用123456789123456789123。



第8.步。在*KEY字段*，请输入流出的策略的一个键。密钥长度取决于在选择的算法第6.步。

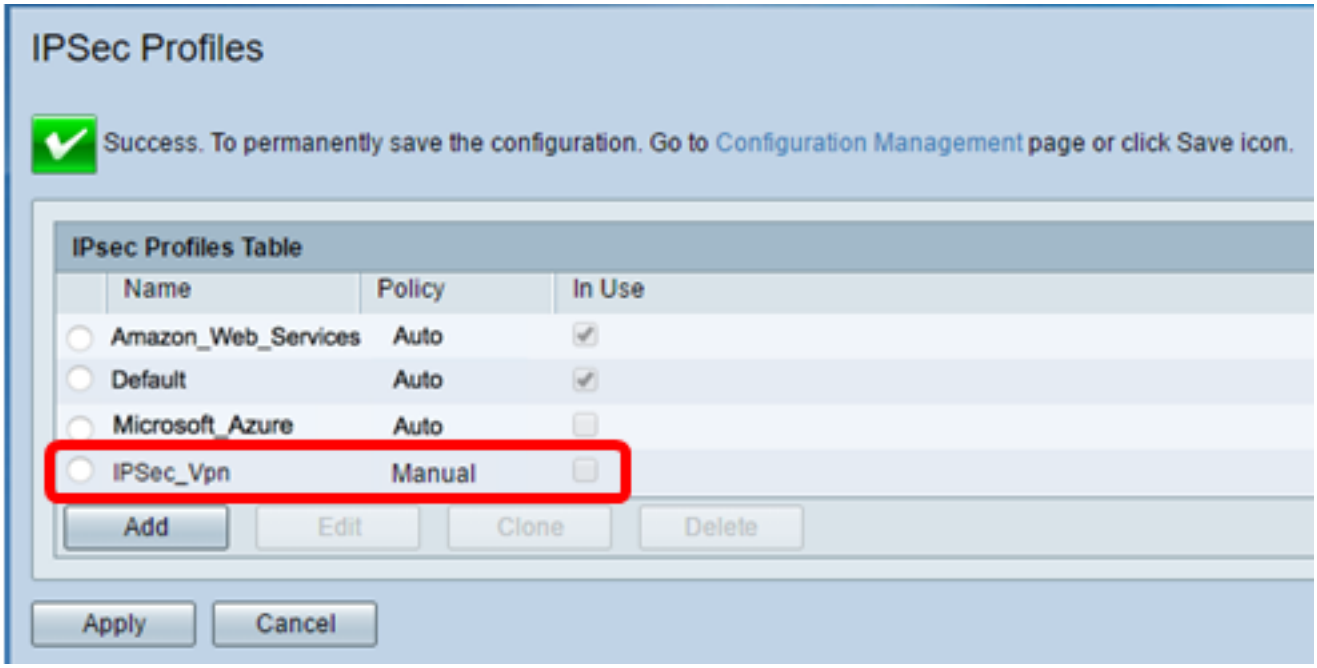
Note:在本例中，…使用1a1a1a1a1a1a1a121212。



步骤9.点击 

。

Note:您将被采取回到IPSec配置文件表，并且新建立的IPSec配置文件应该当前出现。



第10.步(可选)永久保存配置，去复制/保存配置页或点击 

图标在页的上面的部分。

您应该成功当前配置了在一个RV34x系列路由器的手工的IPSec配置文件。