IPSec VPN服务器的配置在RV130和RV130W的

目标

IPSec VPN (虚拟专用网络)使您通过设立在互联网间的一加密隧道安全地获取对公司资源的远程访问。

本文目标将显示您如何配置在RV130和RV130W的IPSec VPN服务器。

注意：关于如何配置有泼妇软的VPN客户端的IPSec VPN服务器的信息RV130和RV130W的，参考条款*使用泼妇软的VPN客户端用在RV130和RV130W的IPSec VPN服务器*。

可适用的设备

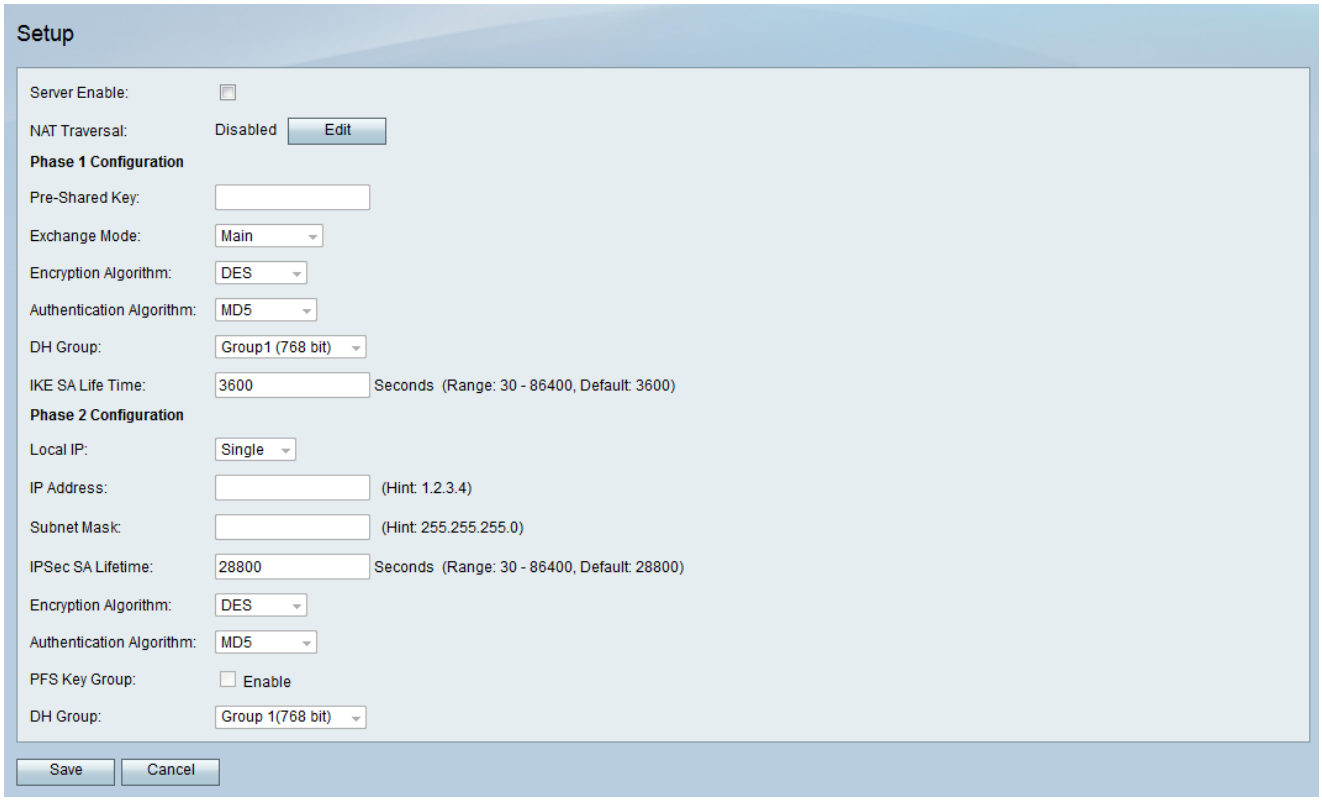
•RV130W Wireless-N VPN防火墙
•RV130 VPN防火墙

软件版本

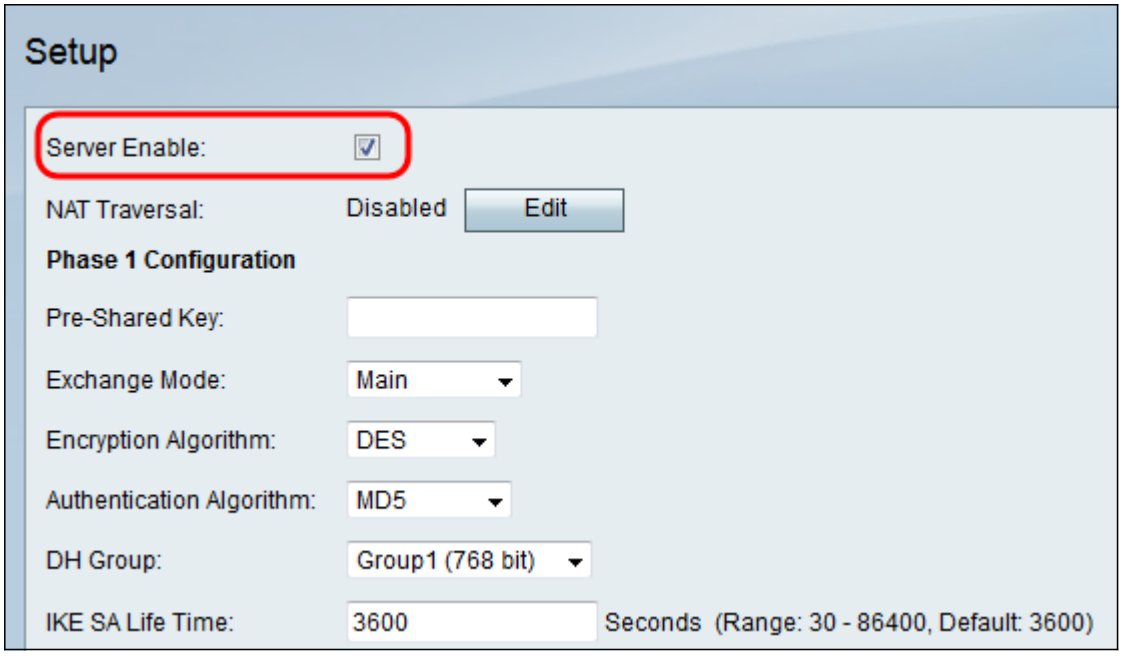
•v1.0.1.3

设置IPSec VPN服务器

步骤1.登陆到Web配置工具并且选择**VPN > IPSec VPN Server>设置**。设置页打开。

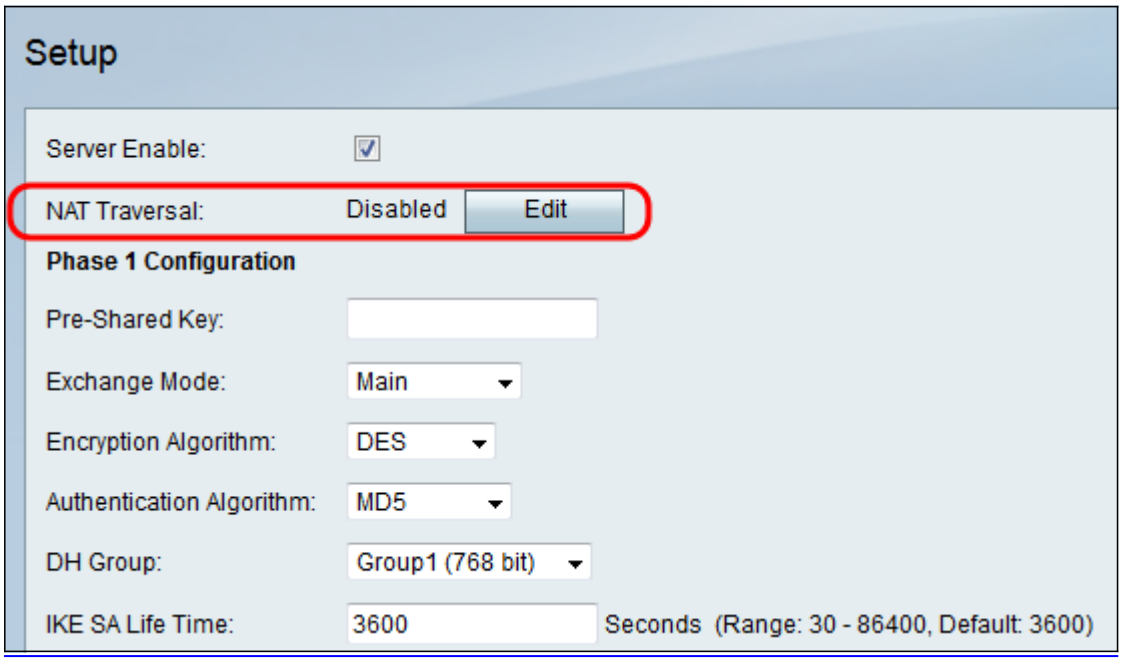


第二步：检查**Enable复选框的服务器**启用证书。

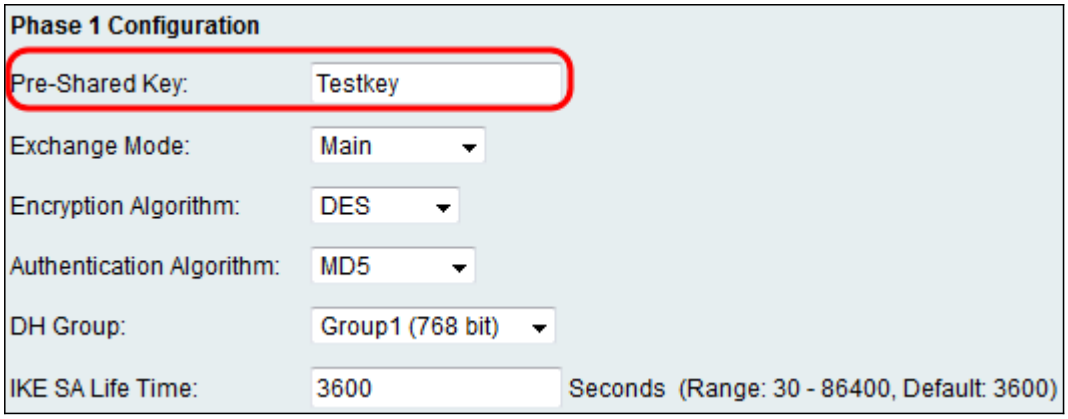


步骤3. (可选)，如果您的VPN路由器或VPN客户端是在NAT网关后，单击**编辑**配置NAT横越。否则，禁用的事假NAT横越。

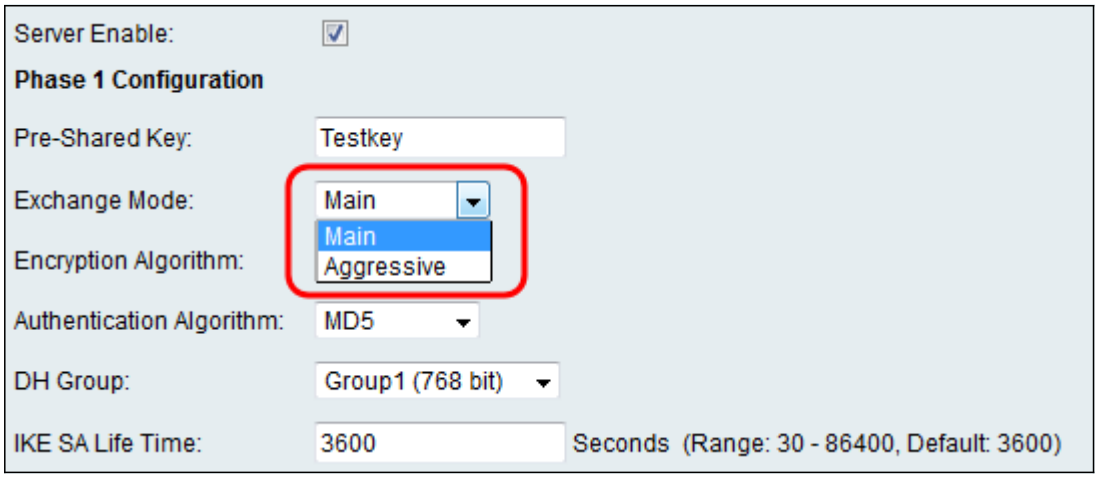
注意：关于如何配置NAT横越设置的更多信息，参考*Internet Key Exchange (IKE)在RV130和RV130W VPN路由器的策略设置。*



步骤4.输入密钥在将交换在您的设备和远程终点之间在*Pre-Shared Key字段*长的8个到49个的字符之间。

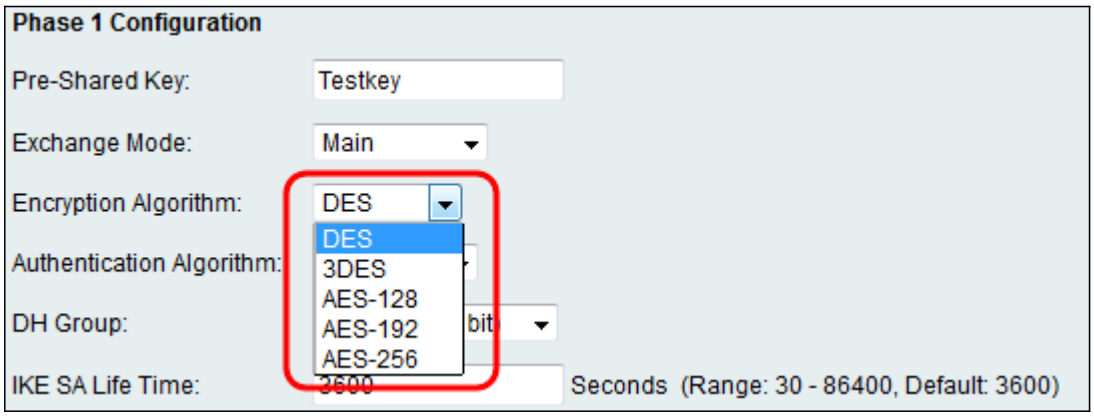


第 5 步：从*Exchange模*式丢弃下来列表，请选择IPSec VPN连接的模式。**主**是默认模式。然而，如果您的网络速度低，请选择**积极模式**。



注意：积极模式在连接时交换通道的端点的ID在明文的，需要较少时刻交换，但是安全的较少。

第六步：从**加密算法**下拉列表，请选择适当的加密方法加密在相位1. AES-128的预先共享密钥为其高安全性和快速性能推荐。VPN通道需要使用同一个加密方法两个其末端。



可用的选项定义如下：

•DES —数据加密标准(DES)是56位，不安全的旧有加密方法，但是可能为向后兼容性要求。

•3DES —，因为加密数据三次，三重数据加密标准(3DES)是168-bit，用于的简单加密方法增加密钥大小。这比DES提供更多安全，但是较少安全比AES。

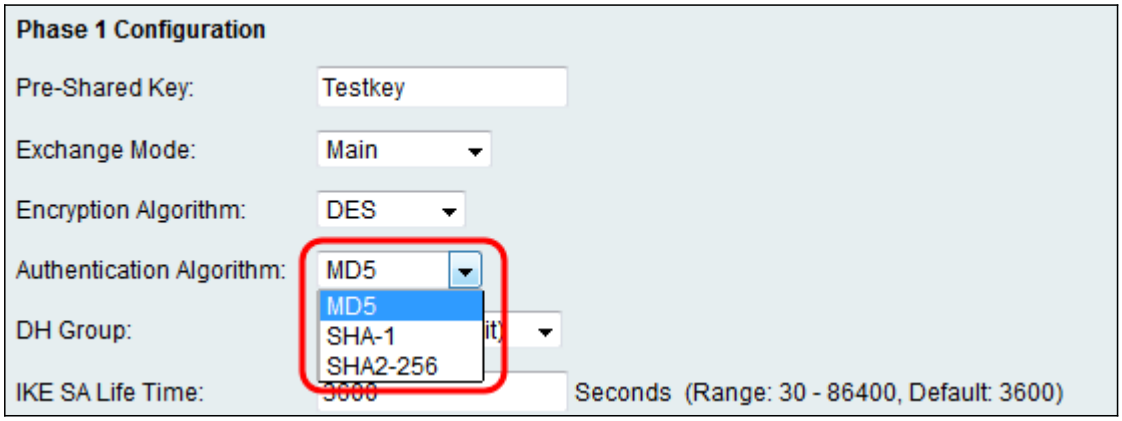
•AES-128 —与128-bit密钥(AES-128)的高级加密标准使用一128-bit密钥AES加密。AES比

DES是安全快速等等的。一般来说， AES比3DES也是安全快速等等的。的AES-128比AES-192和AES-256是安全更加快速，但是的较少。

•AES-192 — AES-192使用一192-bit密钥AES加密。的AES-192比AES-128是更加快速更加慢，但是的更多安全和，但是较少比AES-256巩固。

•AES-256 — AES-256使用一256-bit密钥AES加密。的AES-256比AES-128和AES-192是安全更加慢，但是的更多。

第 7 步：从*验证算法*下拉列表，请选择适当的认证方法确定封装安全有效载荷(ESP)协议报头数据包如何在阶段1验证。VPN通道需要使用同一认证方法连接的两端。



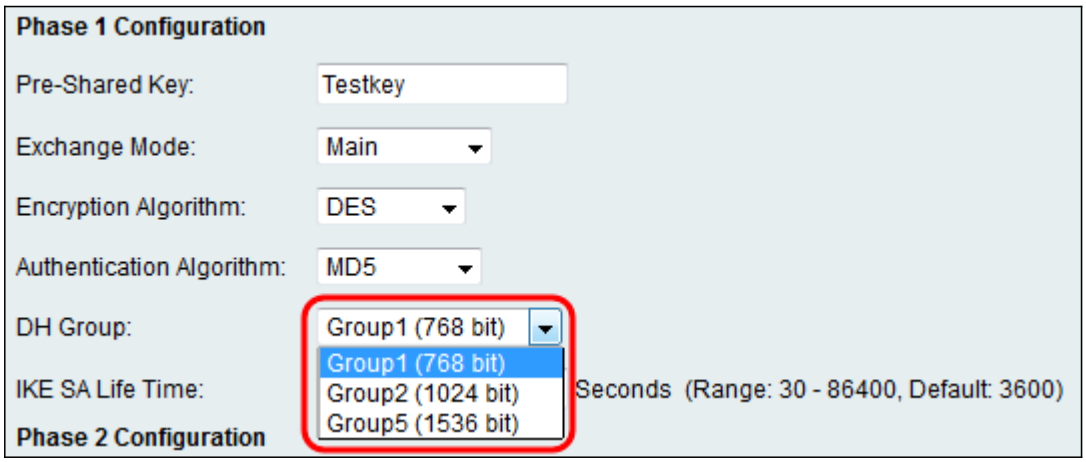
可用的选项定义如下：

•MD5 — MD5是生产一128-bit摘要的一单程哈希算法。MD5比SHA-1计算快速，但是安全的较少比SHA-1。没有推荐MD5。

•SHA-1 — SHA-1是生产一160-bit摘要的一单程哈希算法。SHA-1比MD5计算慢，但是安全的更多比MD5。

•SHA2-256 —指定与256-bit摘要的安全散列算法SHA2。

步骤 8从*DH组*下拉列表，请选择适合的Diffie-Hellman (DH)组与密钥一起使用在相位1. Diffie-Hellman是用于连接交换预先共享密钥集的加密密钥交换协议。位取决于算法的优点。



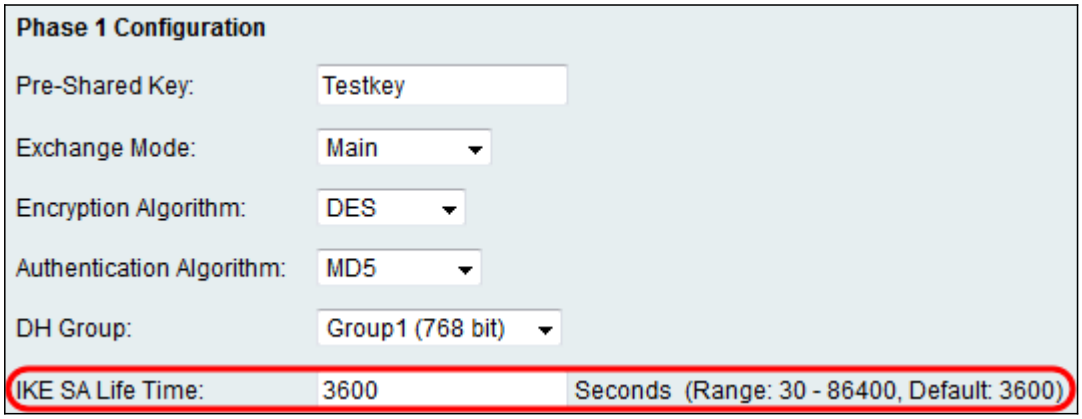
可用的选项定义如下：

•Group1 (768-bit) —计算密钥最快速，但是安全的最少。

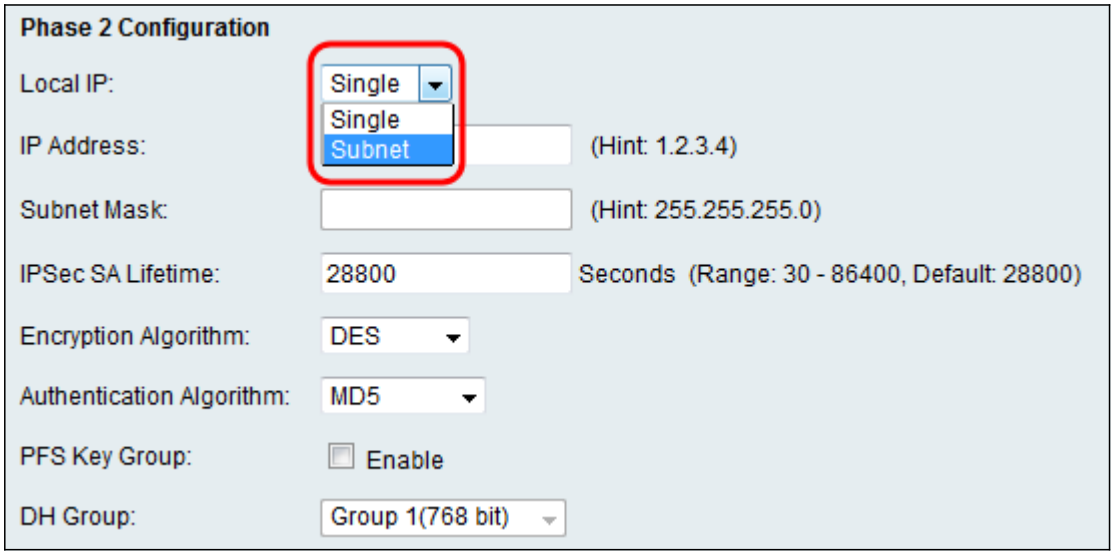
•第2组(1024位) —比Group1计算关键慢，但是安全的更多。

•Group5 (1536位) —计算密钥最慢，但是安全的多数。

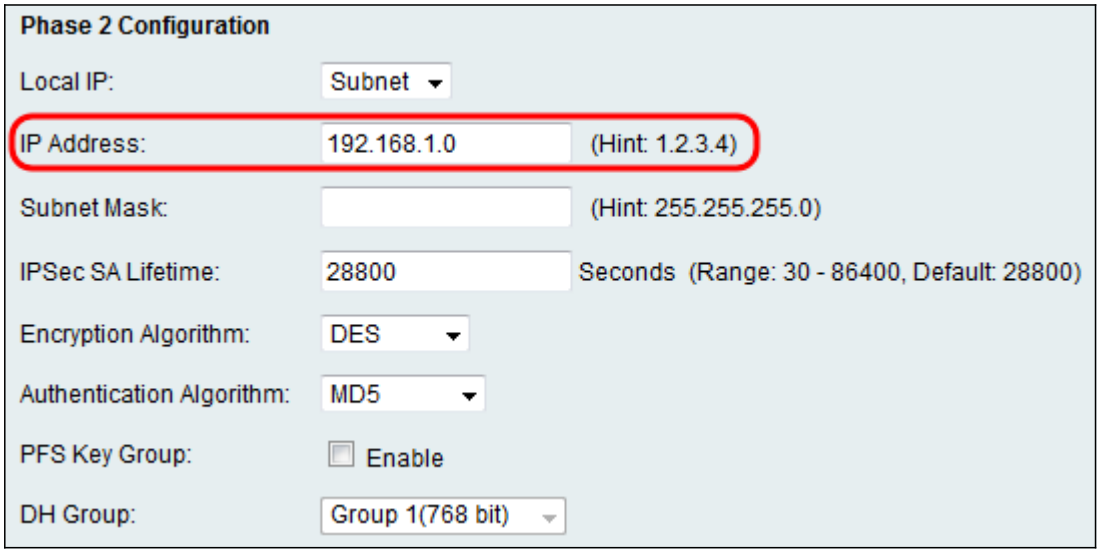
步骤 9在*SA IKE生命时间*字段，请以秒钟进入时间，自动IKE密钥有效。一旦这次超时，新密钥自动地协商。



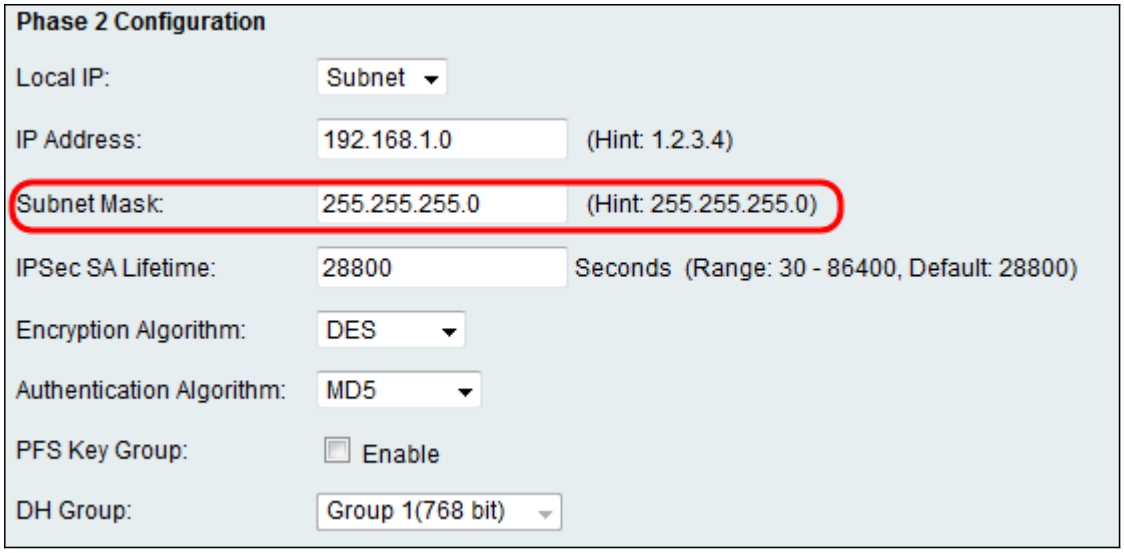
步骤 10从下来*本地IP*丢弃列表，请选择**单个**，如果类似会访问单个本地LAN的用户VPN通道，或者选择**子网**，如果希望多个用户能访问它。



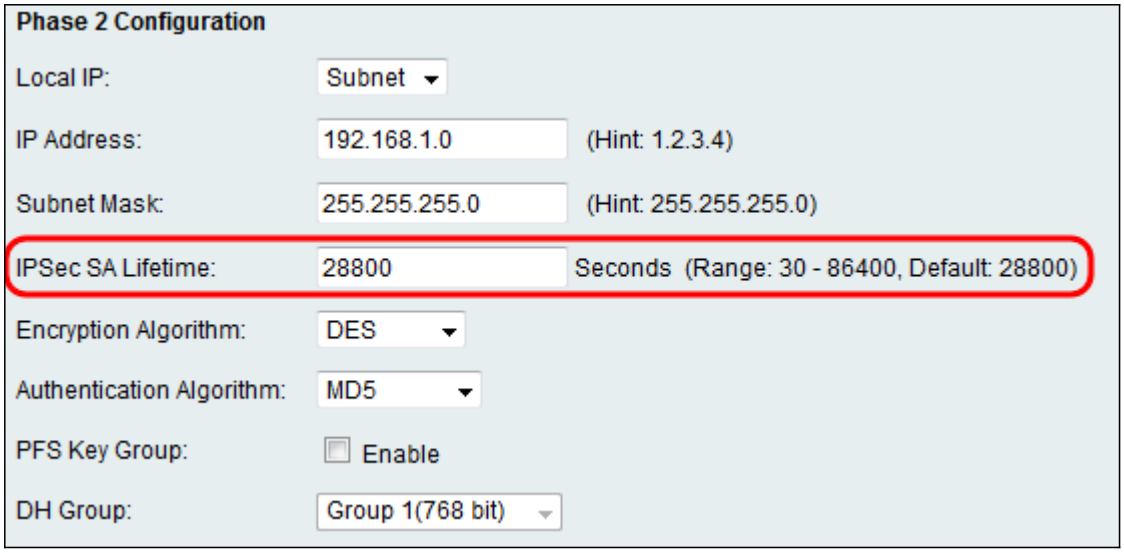
步骤 11如果**子网**在步骤10选择，请进入子网络的网络IP地址在IP地址字段的。如果**单个**在步骤10选择，输入单个用户和跳过的IP地址对步骤13。



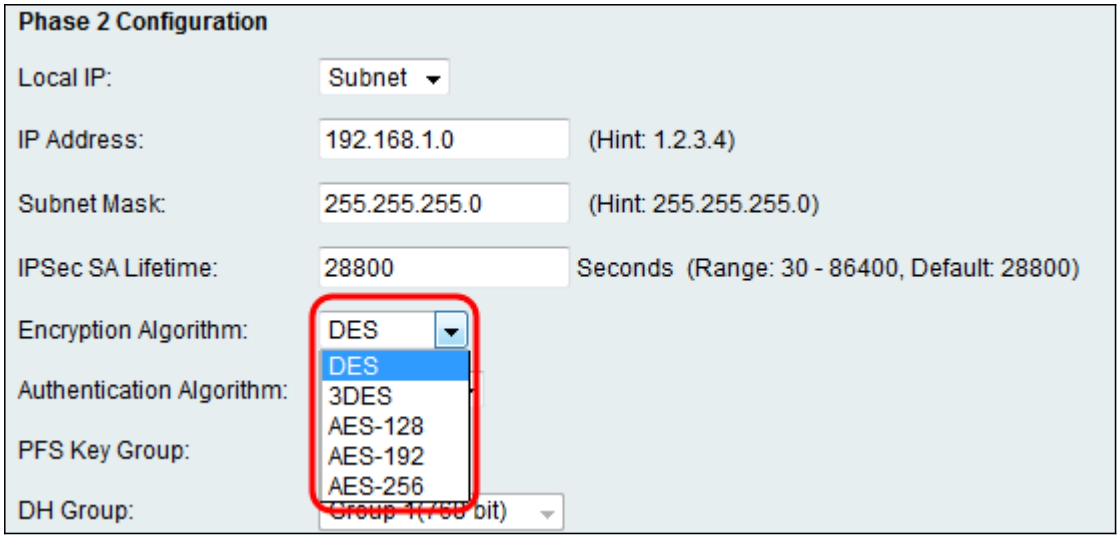
步骤 12(可选)，如果**子网**在步骤10选择，请在*子网掩码*字段输入本地网络的子网掩码。



步骤 13在*SA IPSec寿命*字段，请以秒钟进入时间VPN连接在第2阶段依然是活动。一旦这次超时， VPN连接的IPSec安全关联重新协商。



步骤 14从*加密算法*下拉列表，请选择适当的加密方法加密在相位2. AES-128的预先共享密钥为其高安全性和快速性能推荐。VPN通道需要使用同一个加密方法两个其末端。



可用的选项定义如下：

•DES —数据加密标准(DES)是56位，是安全的最少的旧有加密方法，但是可能为向后兼容

性要求。

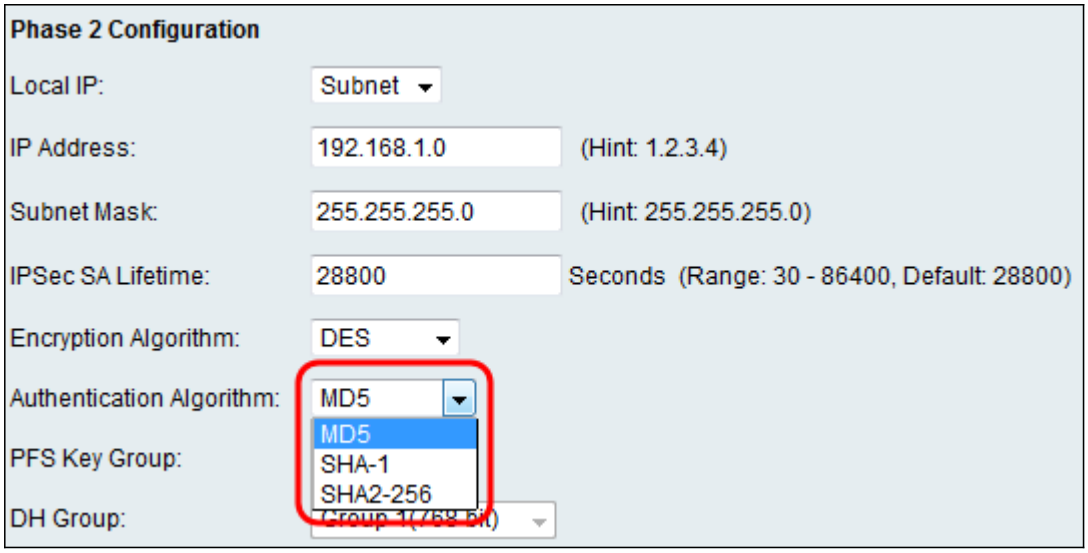
•3DES —，因为加密数据三次，三重数据加密标准(3DES)是168-bit，用于的简单加密方法增加密钥大小。这比DES提供更多安全，但是较少安全比AES。

•AES-128 —与128-bit密钥(AES-128)的高级加密标准使用一128-bit密钥AES加密。AES比DES是安全快速等等的。一般来说， AES比3DES也是安全快速等等的。的AES-128比AES-192和AES-256是安全更加快速，但是的较少。

•AES-192 — AES-192使用一192-bit密钥AES加密。的AES-192比AES-128是更加快速更加慢，但是的更多安全和，但是较少比AES-256巩固。

•AES-256 — AES-256使用一256-bit密钥AES加密。的AES-256比AES-128和AES-192是安全更加慢，但是的更多。

步骤 15从*验证算法*下拉列表，请选择适当的认证方法确定封装安全有效载荷(ESP)协议报头数据包如何在相位2.The VPN通道需要验证使用同一认证方法两个其末端。



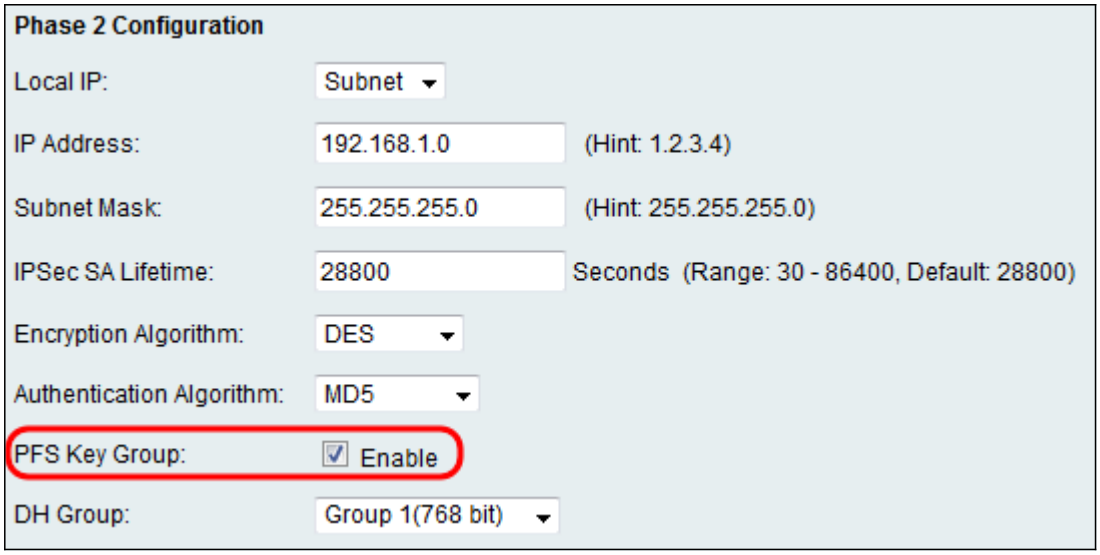
联机选项定义如下：

•MD5 — MD5是生产一128-bit摘要的一单程哈希算法。MD5比SHA-1计算快速，但是安全的较少比SHA-1。没有推荐MD5。

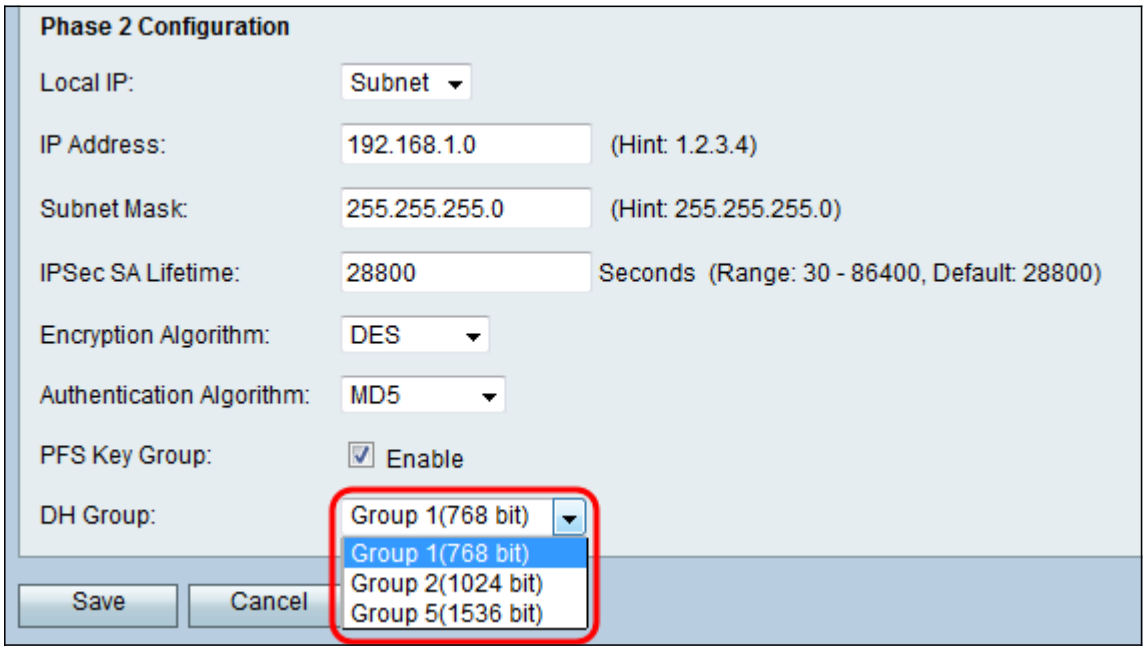
•SHA-1 — SHA-1是生产一160-bit摘要的一单程哈希算法。SHA-1比MD5计算慢，但是安全的更多比MD5。

•SHA2-256 —指定与256-bit摘要的安全散列算法SHA2。

步骤 16(可选)在*PFS密钥Group字段*，请检查**Enable复选框**。完整转发安全性(PFS)通过保证在第2阶段的一新的DH密钥创建安全一块另外的层在保护您的数据的。万一在阶段1生成的DH密钥在运送中，减弱进程完成。



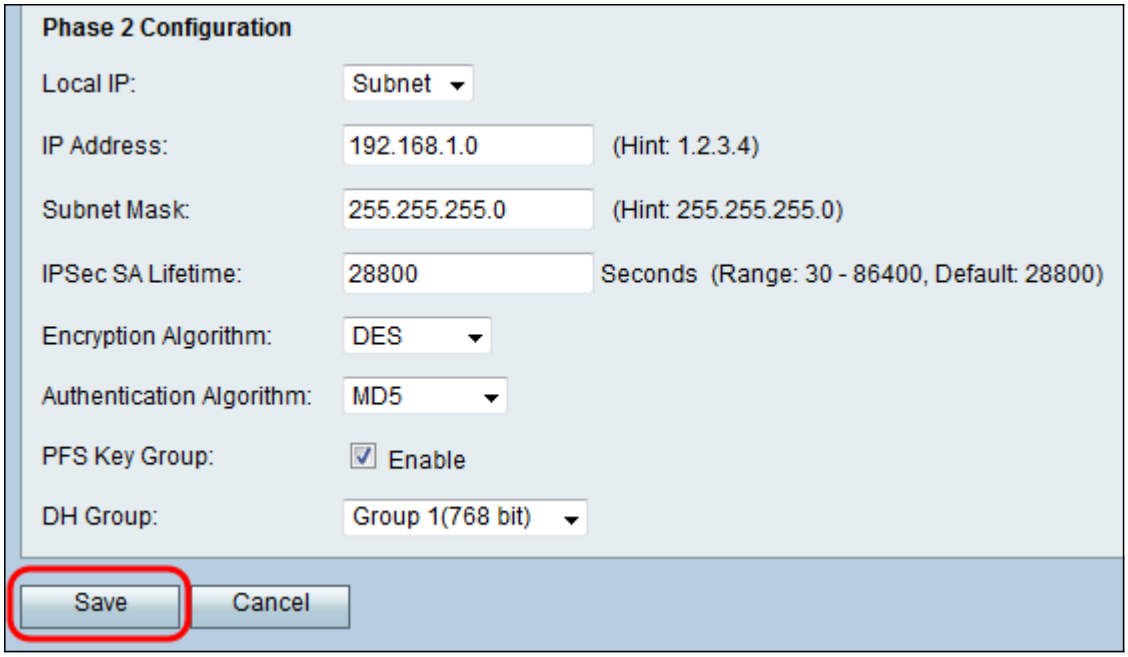
步骤 17从*DH组*下拉列表，请选择适合的Diffie-Hellman (DH)组与密钥一起使用在第2阶段。



联机选项定义如下：

- Group1 (768-bit) —计算密钥最快速，但是安全的最少。
- 第2组(1024位) —比Group1计算关键慢，但是安全的更多。
- Group5 (1536位) —计算密钥最慢，但是安全的多数。

步骤18。点击**“Save”**保存您的设置。



欲知更多信息，请检查以下文档：

- RV130数据表或宣传单页-解释RV130系列路由器的VPN功能
- RV130产品网页-包括所有RV130条款的链路从Cisco