在RV130和RV130W上配置IPSec VPN服务器

目标

通过IPSec VPN（虚拟专用网络），您可以建立互联网上的加密隧道，从而安全地远程访问公司资源。

本文档的目标是向您展示如何在RV130和RV130W上配置IPSec VPN服务器。

注意：有关如何在RV130和RV130W上使用Shrew Soft VPN Client配置IPSec VPN服务器的信息，请参阅*在RV130和RV130W上使用Shrew Soft VPN Client with IPSec VPN Server*。

适用设备

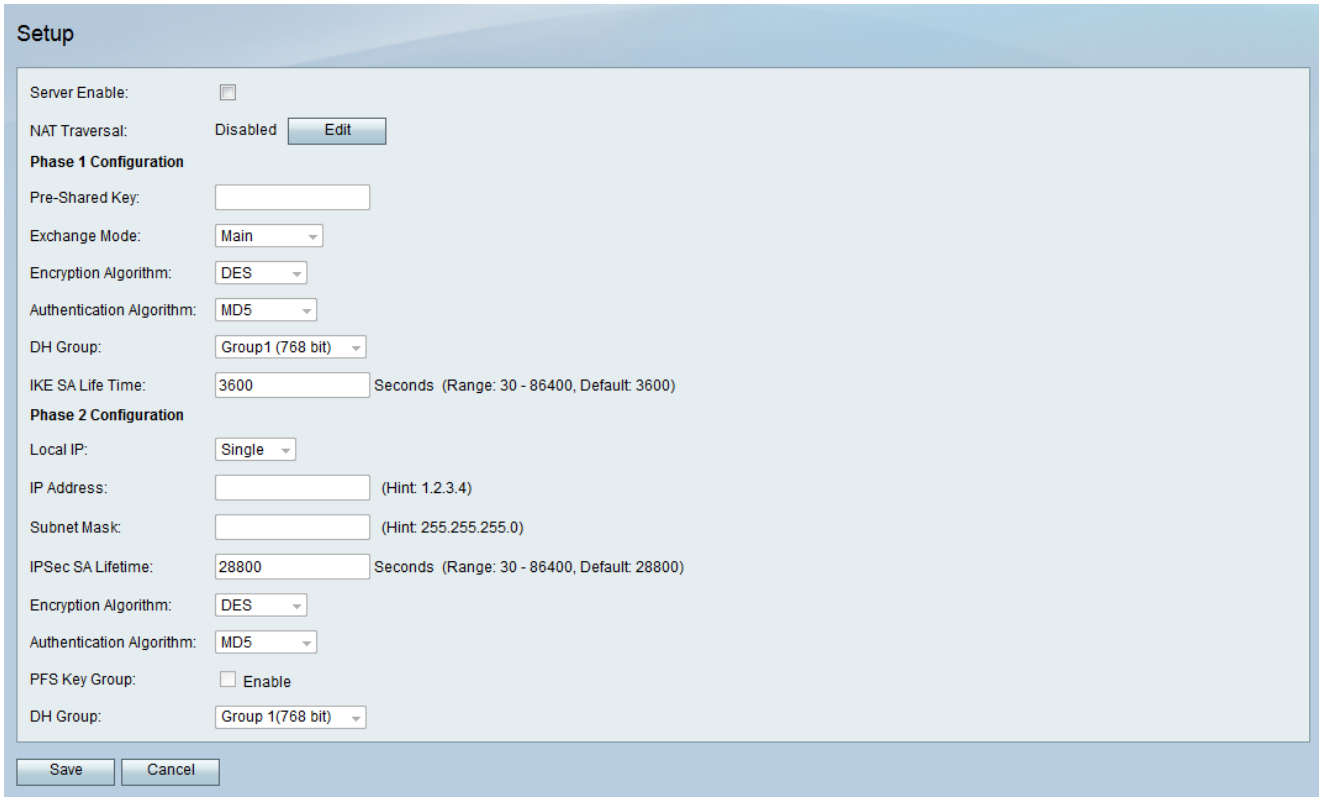
·RV130W Wireless-N VPN防火墙
· RV130 VPN防火墙

软件版本

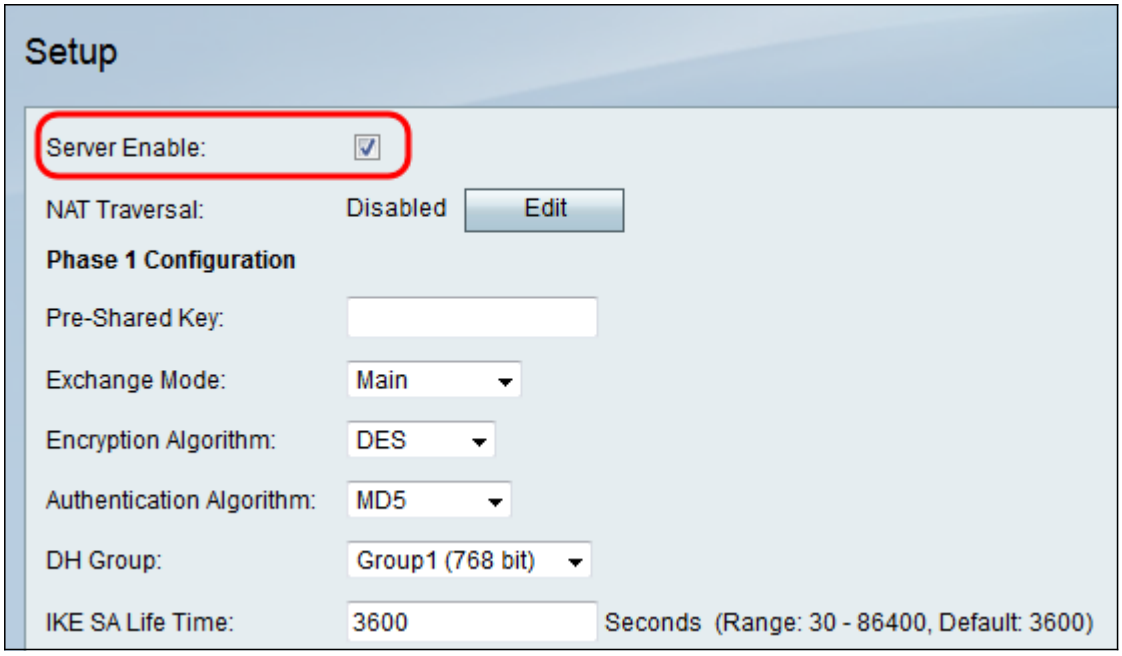
•v1.0.1.3

设置IPSec VPN服务器

步骤1.登录到Web配置实用程序并选择**VPN > IPSec VPN Server > Setup**。系统将打开“设置”(Setup)页面。

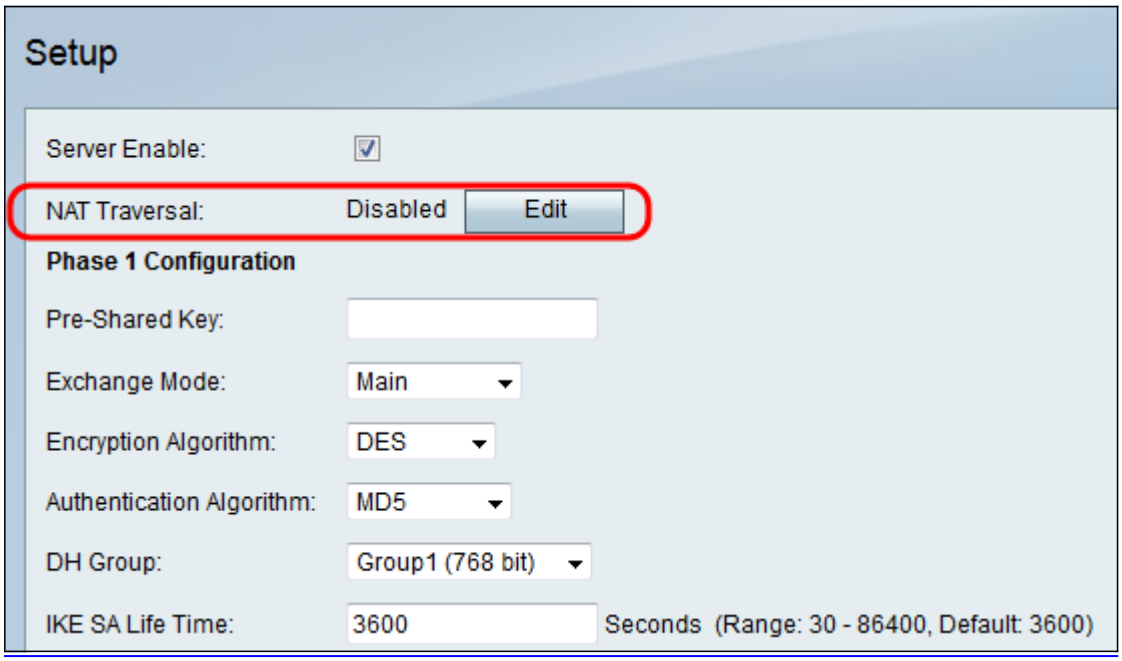


步骤2.选中**Server Enable**复选框以启用证书。

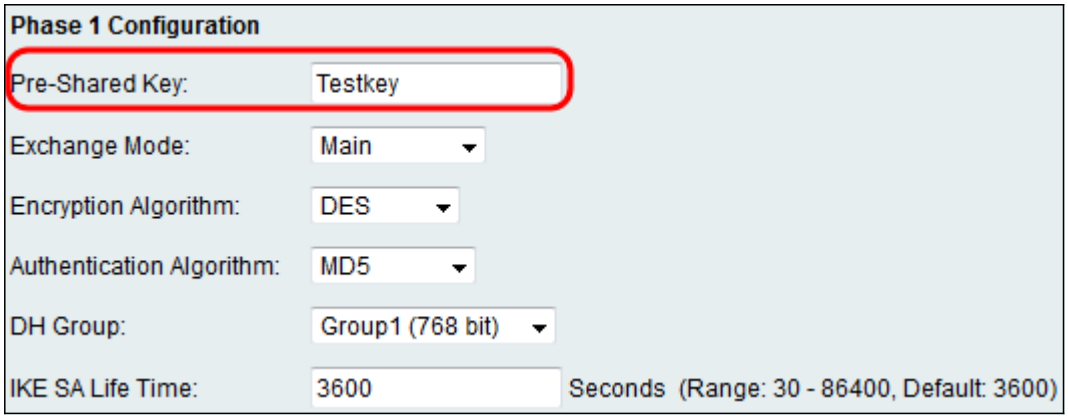


步骤3.（可选）如果VPN路由器或VPN客户端位于NAT网关后面，请单击**Edit**以配置NAT穿越。否则，请禁用NAT穿越。

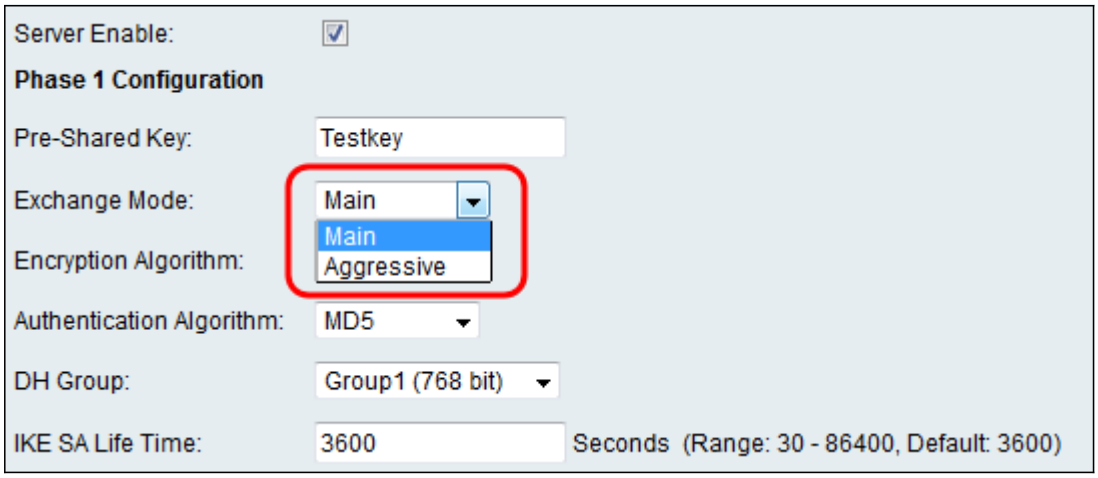
注意：有关如何配置NAT遍历设置的详细信息，请参阅*RV130和RV130W VPN路由器上的互联网密钥交换(IKE)策略设置*。



步骤4.在*预共享密钥*字段中输入一个密钥，该密钥长度介于8到49个字符之间，并且将在您的设备和远程终端之间交换。

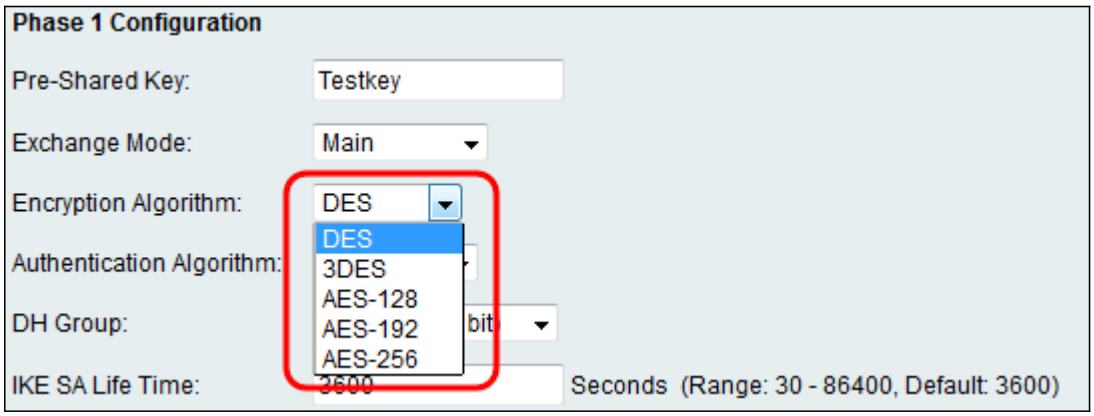


步骤5.从*Exchange Mode*下拉列表中，选择IPSec VPN连接的模式。**Main**是默认模式。但是，如果您的网络速度较低，请选择**主动**模式。



注意：主动模式在连接期间以明文形式交换隧道终端的ID，交换时间较少，但安全性较低。

步骤6.从**Encryption Algorithm**下拉列表中，选择适当的加密方法以加密第1阶段的预共享密钥。建议使用AES-128来实现其高安全性和快速性能。VPN隧道两端都需要使用相同的加密方法。



可用选项定义如下：

·DES — 数据加密标准(DES)是56位旧加密方法，它不是很安全，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。

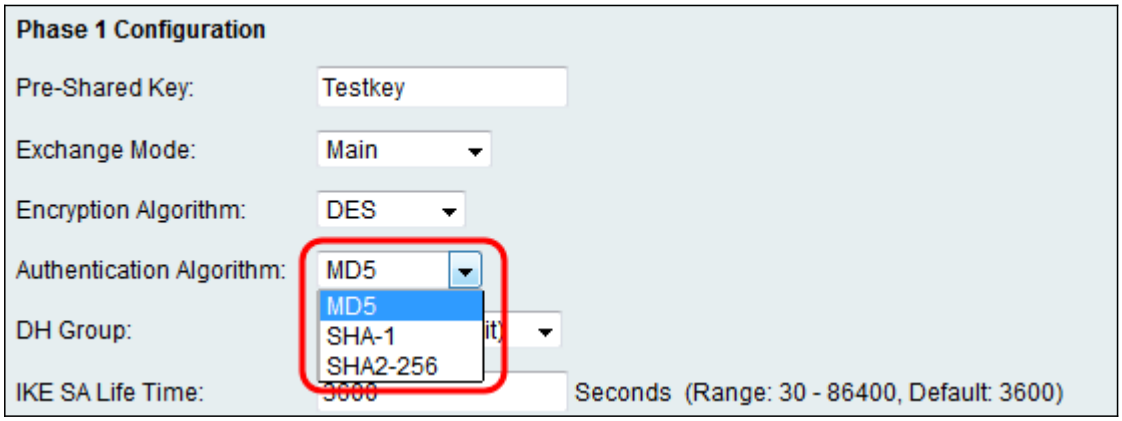
·AES-128 — 具有128位密钥的高级加密标准(AES-128)使用128位密钥进行AES加密。

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。

步骤7.从*Authentication Algorithm*下拉列表中，选择适当的身份验证方法以确定如何在第1阶段验证封装安全负载(ESP)协议报头数据包。VPN隧道需要为连接的两端使用相同的身份验证方法。



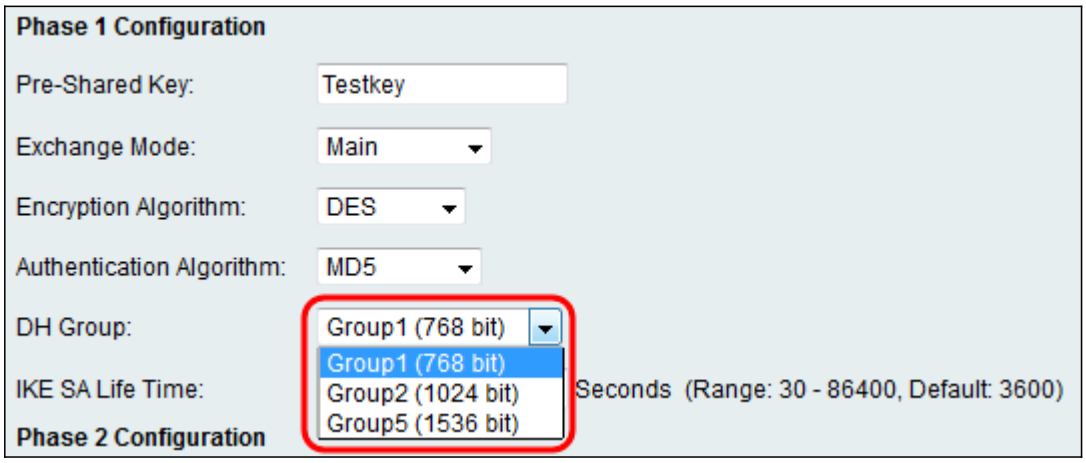
可用选项定义如下：

·MD5 - MD5是产生128位摘要的单向散列算法。MD5的计算速度比SHA-1快，但比SHA-1安全性低。不推荐MD5。

·SHA-1 — SHA-1是产生160位摘要的单向散列算法。SHA-1计算速度比MD5慢，但比MD5更安全。

·SHA2-256 — 指定具有256位摘要的安全散列算法SHA2。

第8步：从*DH Group*下拉列表中，选择要与阶段1中的密钥一起使用的相应Diffie-Hellman(DH)组。Diffie-Hellman是用于交换预共享密钥集的连接中的加密密钥交换协议。算法的强度由比特决定。



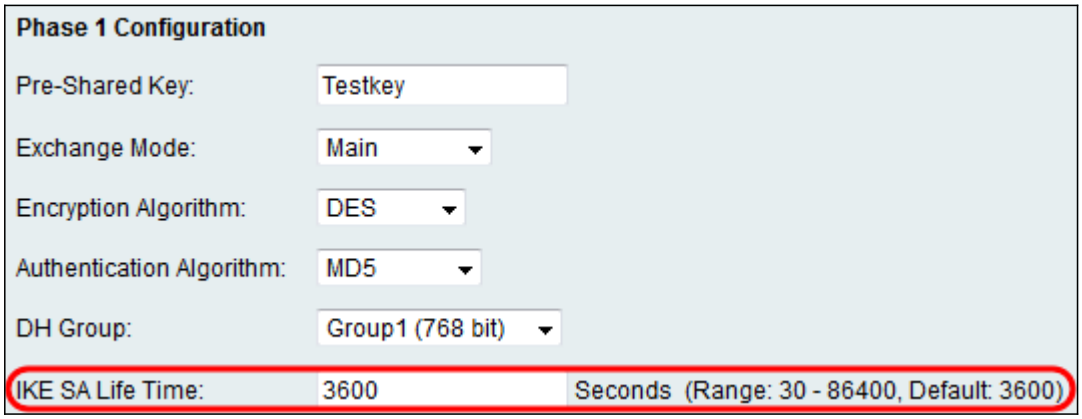
可用选项定义如下：

·Group1（768位）— 以最快的速度计算密钥，但最不安全。

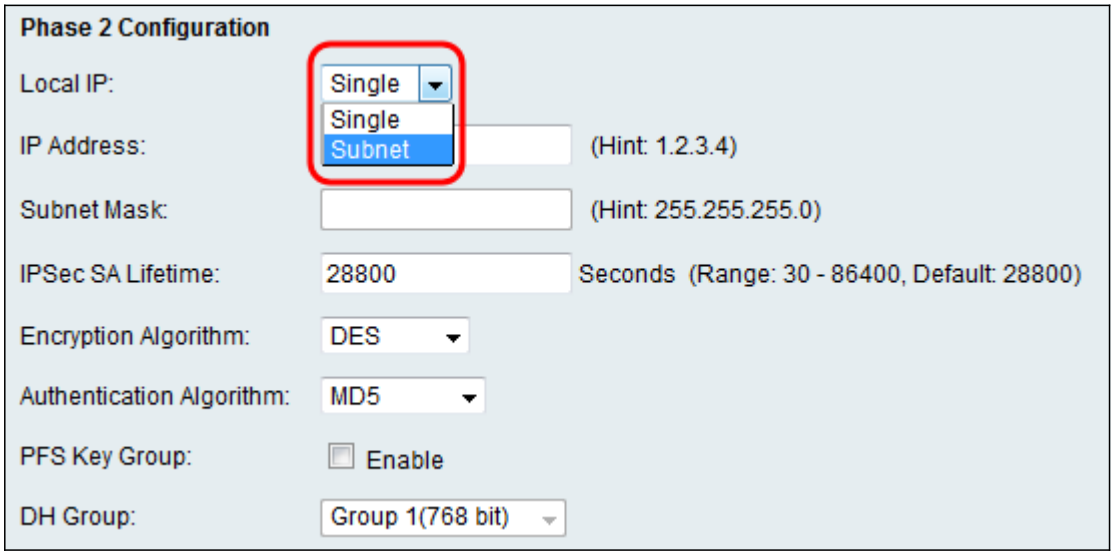
·Group2（1024位）— 计算密钥的速度较慢，但比Group1更安全。

·组5（1536位）— 计算最慢但最安全的密钥。

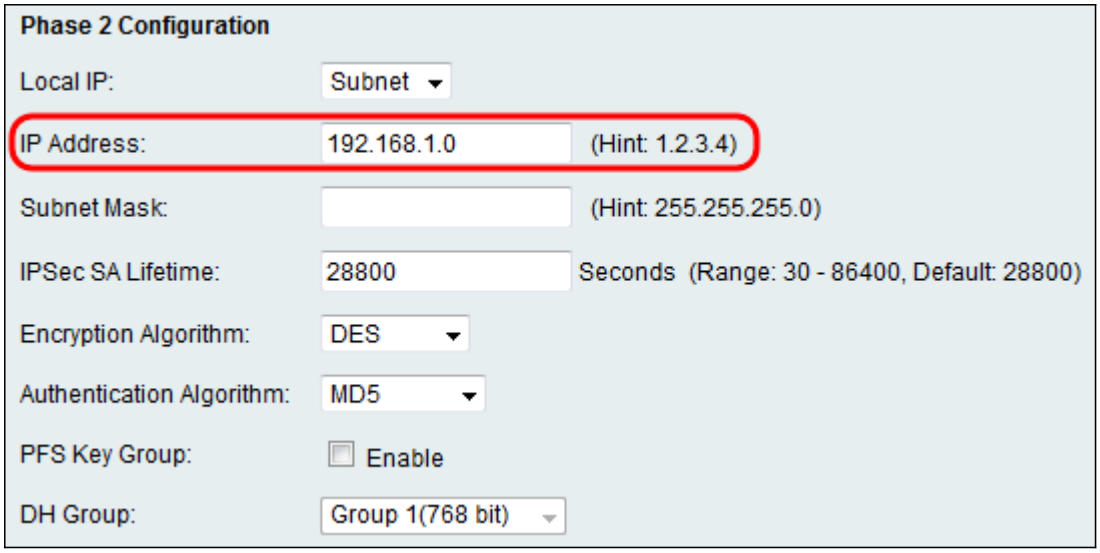
步骤9.在*IKE SA Life Time*字段中，输入自动IKE密钥有效的时间（以秒为单位）。此时间到期后，将自动协商新密钥。



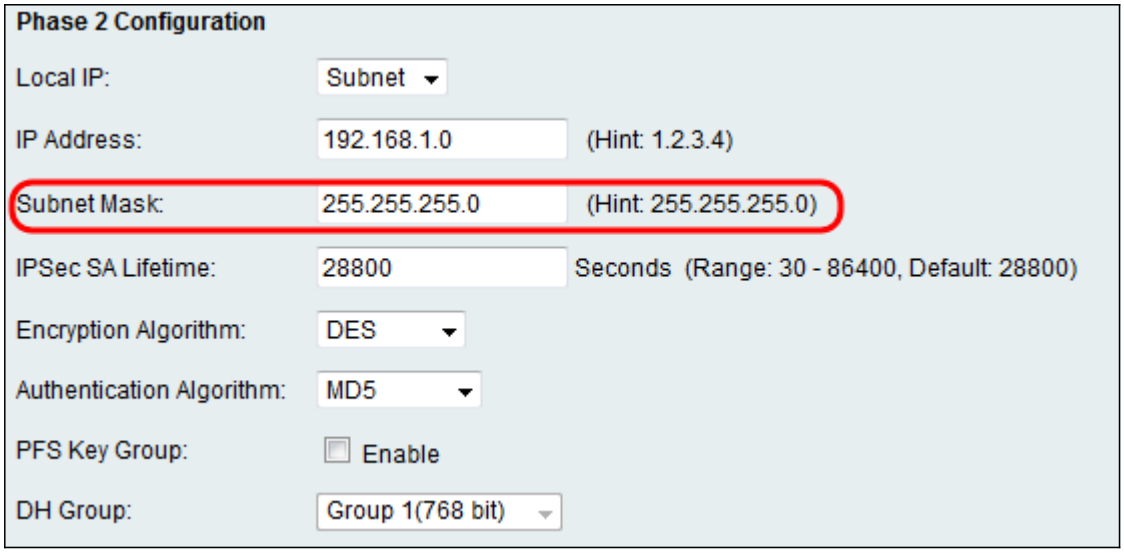
步骤10.从*本地IP*下拉列表中，如果您希望单个本地LAN用户访问VPN隧道，请选择**Single**；如果您希望多个用户能够访问**Subnet**。



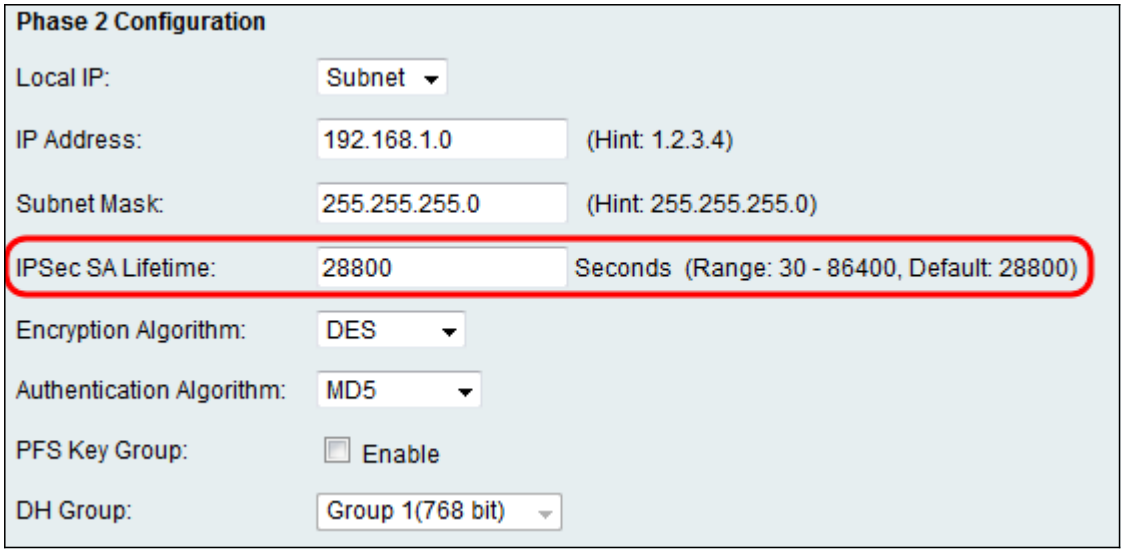
步骤11.如果在步骤10中选择了**Subnet**，请在IP Address字段中输入子网的网络IP地址。如果在步骤10中选择了**Single**，请输入单个用户的IP地址并跳至步骤13。



步骤12.（可选）如果在步骤10中选择了**子网**，请在*子网掩码*字段中输入本地网络的子网掩码。

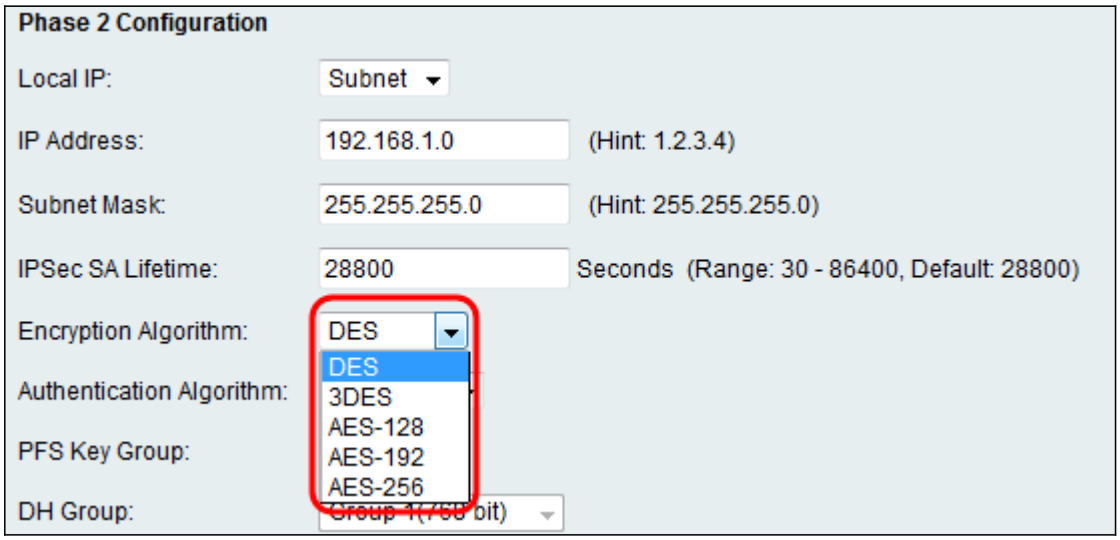


步骤13.在*IPSec SA Lifetime*字段中，输入VPN连接在第2阶段保持活动状态的时间（以秒为单位）。此时间到期后，将重新协商VPN连接的IPSec安全关联。



步骤14.从*Encryption Algorithm*下拉列表中，选择适当的加密方法以加密第2阶段的预共享密钥。建议使用AES-128来实现其高安全性和快速性能。VPN隧道两端都需要使用相同的加密方

法。



可用选项定义如下：

·DES — 数据加密标准(DES)是56位旧加密方法，虽然最不安全，但为了向后兼容，可能需要这种方法。

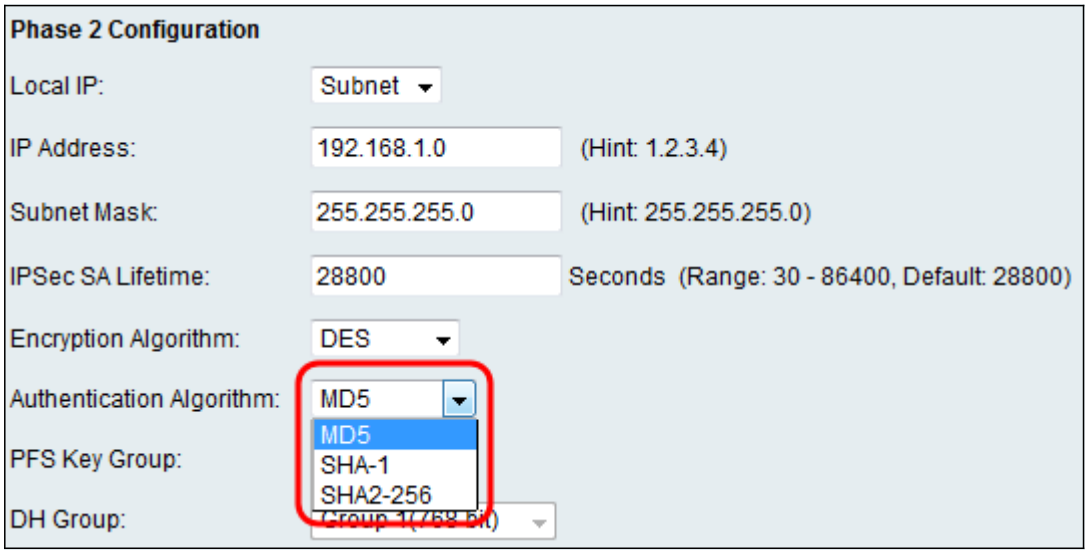
·3DES — 三重数据加密标准(3DES)是一种168位、简单的加密方法，用于增加密钥大小，因为它将数据加密三次。这提供了比DES更高的安全性，但比AES更低的安全性。

·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。

步骤15.从*Authentication Algorithm*下拉列表中，选择适当的身份验证方法，以确定如何在第2阶段验证封装安全负载(*Encapsulating Security Payload， ESP)协议报头数据包。VPN隧道的两端都需要使用相同的身份验证方法。*



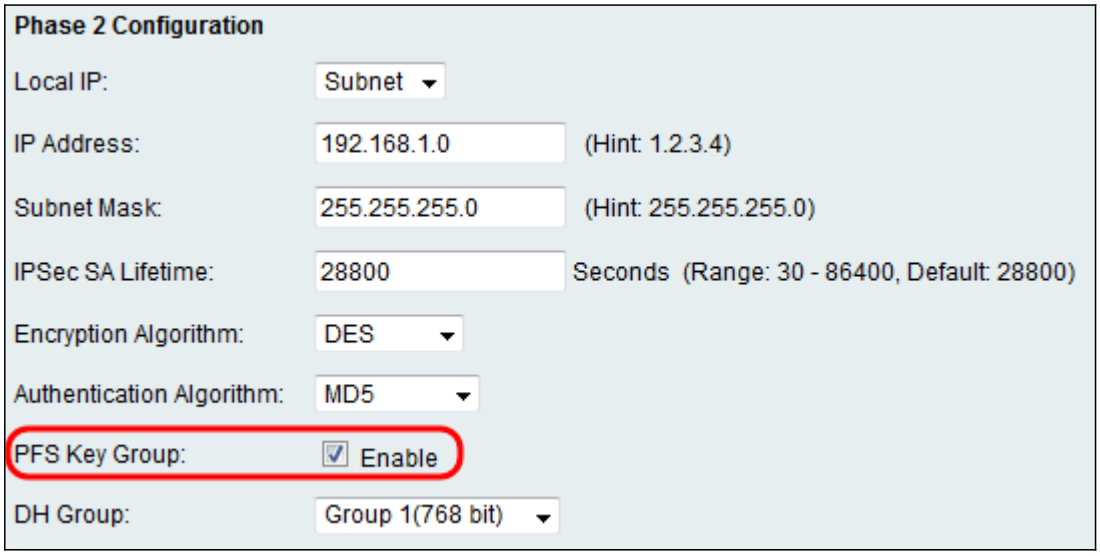
可用选项定义如下：

·MD5 - MD5是产生128位摘要的单向散列算法。MD5的计算速度比SHA-1快，但比SHA-1安全性低。不推荐MD5。

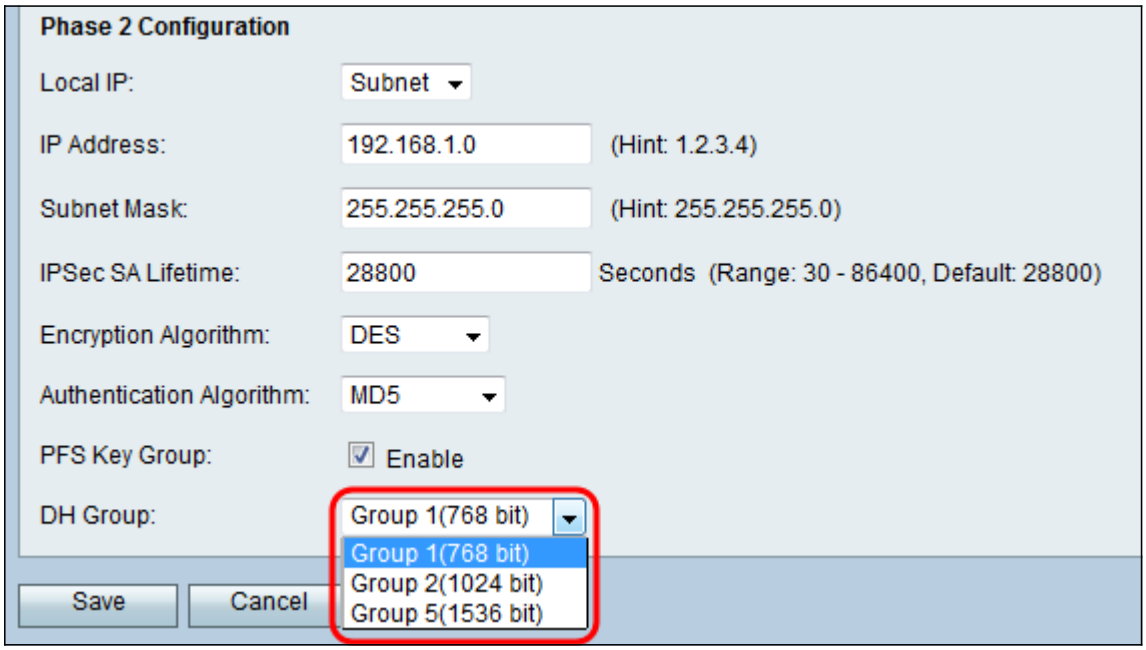
·SHA-1 — SHA-1是产生160位摘要的单向散列算法。SHA-1计算速度比MD5慢，但比MD5更安全。

·SHA2-256 — 指定具有256位摘要的安全散列算法SHA2。

第16步。（可选）在*PFS Key Group字段*中，选中**Enable复**选框。完全向前保密(PFS)通过确保在第2阶段使用新的DH密钥来保护您的数据创建额外的安全层。此过程会在传输过程中发生第1阶段生成的DH密钥泄露时完成。



第17步：从*DH Group*下拉列表中，选择要与阶段2中的密钥一起使用的相应Diffie-Hellman(DH)组。



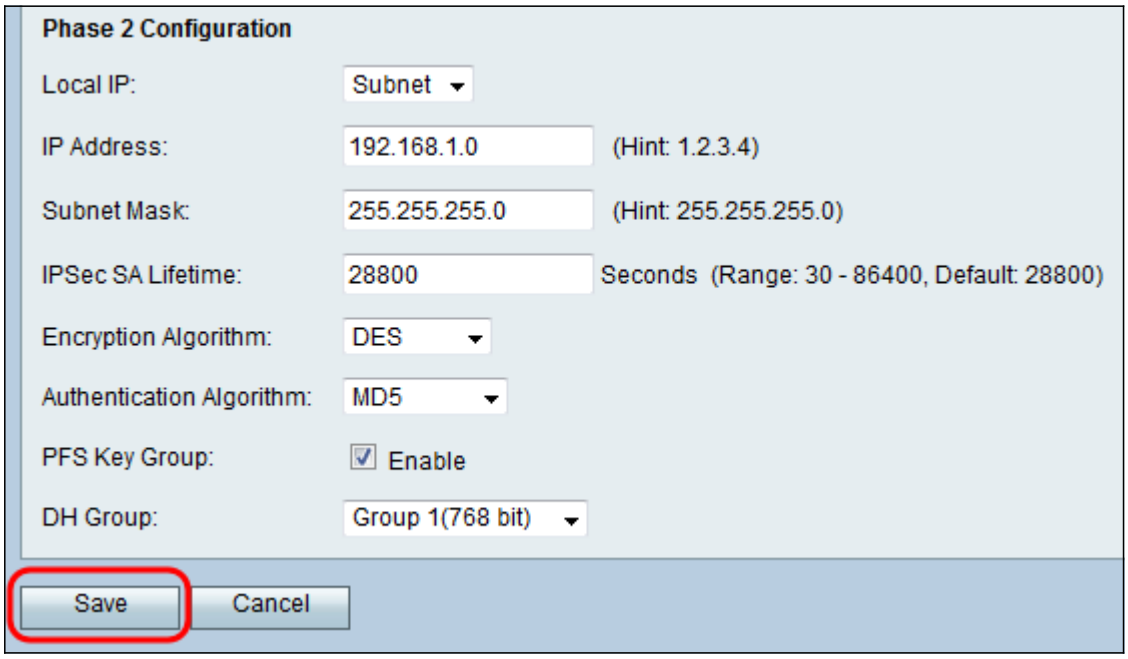
可用选项定义如下：

·Group1（768位）— 以最快的速度计算密钥，但最不安全。

·Group2（1024位）— 计算密钥的速度较慢，但比Group1更安全。

·组5（1536位）— 计算最慢但最安全的密钥。

步骤18.单击Save保存设置。



有关详细信息，请参阅以下文档：

- RV130产品手册 — 介绍RV130系列路由器的VPN功能
- RV130产品页面 — 包含思科所有RV130文章的链接

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）。