设置并使用GreenBow IPsec VPN客户端与RV160和RV260路由器连接

目标

本文档的目标是设置并使用TheGreenBow IPsec VPN客户端与RV160和RV260路由器连接。

简介

虚拟专用网络(VPN)连接允许用户通过公共或共享网络（如Internet）访问、发送和接收数据到专用网络和从专用网络接收数据，但仍确保与底层网络基础设施的安全连接以保护专用网络及其资源。

VPN隧道建立一个专用网络，该专用网络可以使用加密和身份验证安全地发送数据。公司办公室通常使用VPN连接，因为即使员工不在办公室，也允许其访问其专用网络既有用也有必要。

VPN允许远程主机或客户端像位于同一本地网络一样工作。RV160路由器最多支持10个VPN隧道，RV260最多支持20个。在路由器配置了Internet连接后，可以在路由器和终端之间建立VPN连接。VPN客户端完全依赖于VPN路由器的设置才能建立连接。设置必须完全匹配，否则无法通信。

GreenBow VPN Client是第三方VPN客户端应用，它使主机设备能够通过RV160和RV260系列路由器为客户端到站点IPsec隧道配置安全连接。

使用VPN连接的优势

使用VPN连接有助于保护机密网络数据和资源。

它为远程员工或公司员工提供方便和可访问性，因为他们将能够轻松访问总部，而不必在现场，同时维护专用网络及其资源的安全。

与其他远程通信方法相比，使用VPN连接的通信提供了更高级别的安全性。高级加密算法使这成为可能，从而保护专用网络免受未经授权的访问。

用户的实际地理位置受到保护，不会暴露于公共或共享网络（如Internet）。

VPN允许添加新用户或用户组，而无需额外组件或复杂的配置。

使用VPN连接的风险

配置错误可能会带来安全风险。由于VPN的设计和实施可能非常复杂，因此需要将连接配置任务委托给知识丰富且经验丰富的专业人员，以确保专用网络的安全不会受到损害。

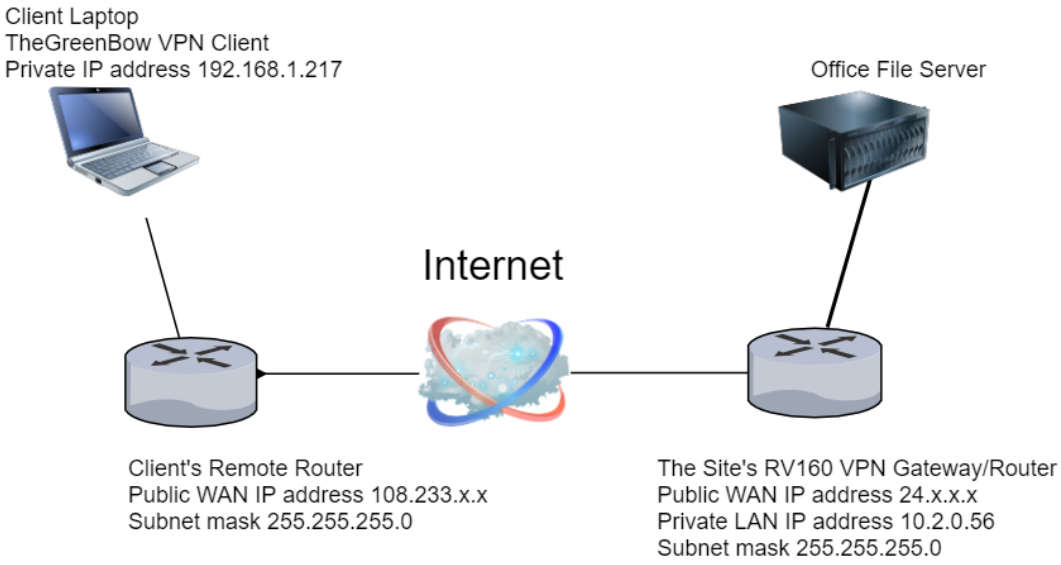
它可能不太可靠。由于VPN连接需要Internet连接，因此必须拥有信誉经过验证和测试的提供商来提供卓越的Internet服务，并保证最短甚至不出现停机。

如果出现需要添加新基础架构或新配置集的情况，则可能会因不兼容而出现技术问题，尤其是如果不兼容的产品或供应商与您已经使用的产品或供应商不同。

连接速度可能会慢。如果您使用的VPN客户端提供免费VPN服务，则可能预期连接速度也会很慢，因为这些提供商不会优先处理连接速度。在本文中，我们将使用付费的第三方来消除此问题。

客户端到站点网络的基本拓扑

这是用于设置的网络的基本布局。公有WAN IP地址已部分模糊，或者显示**x**代替实际数字，以保护此网络免受攻击。



本文将介绍在站点配置RV160或RV260路由器所需的步骤，以实现以下目的：

- 用户组 — **VPNUsers**
- 允许作为客户端访问的用户帐户（一个或多个用户）
- IPsec配置文件 — **TheGreenBow**
- 客户端到站点配置文件 — **客户**
- 您还将看到客户端连接后如何查看站点的VPN状态

注意：您可以为用户组、IPsec配置文件和客户端到站点配置文件使用任何名称。列出的名称只是示例。

本文还说明了每个客户端在其计算机上配置TheGreenBow VPN的步骤：

- 下载并设置TheGreenBow VPN客户端软件
- 配置客户端的第1阶段和第2阶段设置
- 启动并验证VPN连接作为客户端

现场路由器上的每个设置都必须与客户端设置匹配。如果您的配置未导致VPN连接成功，请检查所有设置以确保它们匹配。本文所示的示例只是建立连接的一种方式。

目录

在站点的RV160或RV260路由器上配置

创建客户端到站点配置文件

在客户端位置配置

配置第1阶段设置

配置隧道设置

作为客户端启动VPN连接

检查RV160或RV260上的连接

验证站点上的VPN状态

适用设备

- RV160
- RV260

软件版本

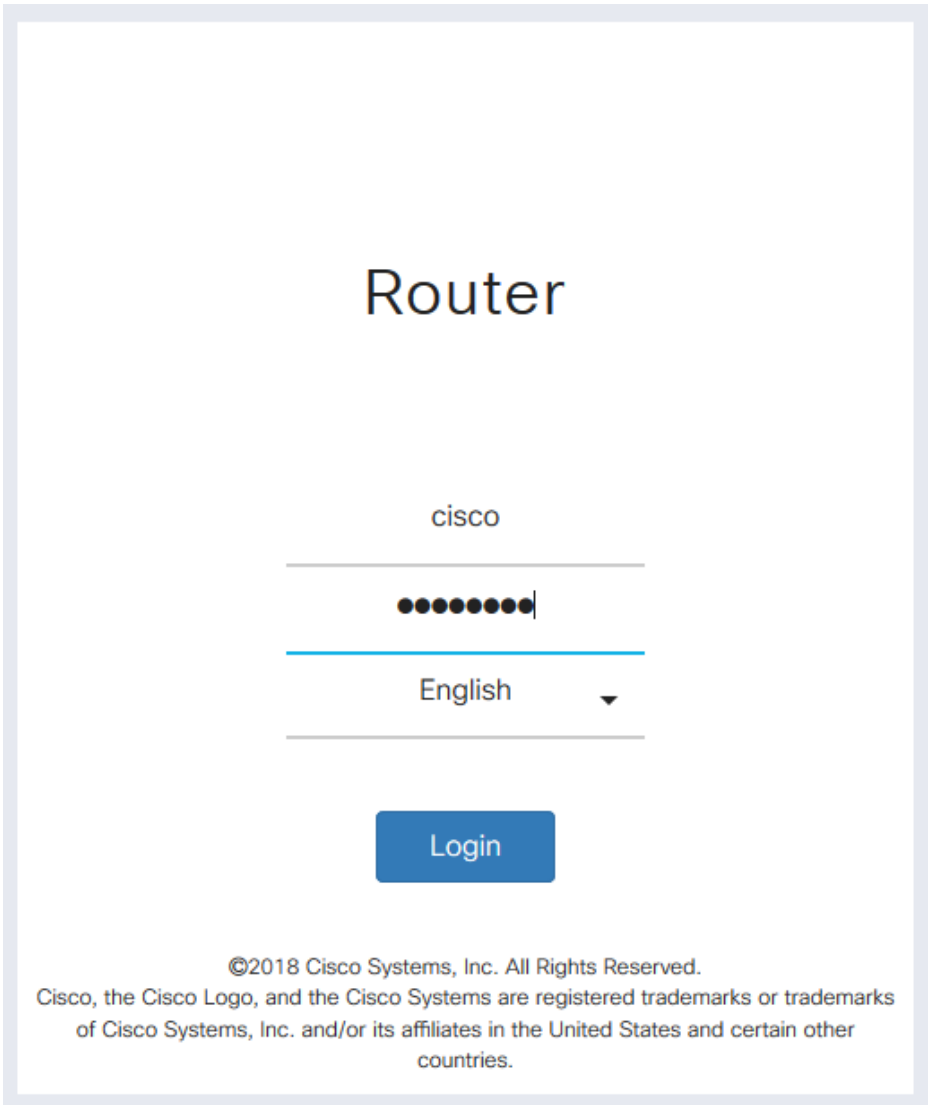
- 1.0.00.15

在RV160或RV260路由器的站点上配置VPN客户端

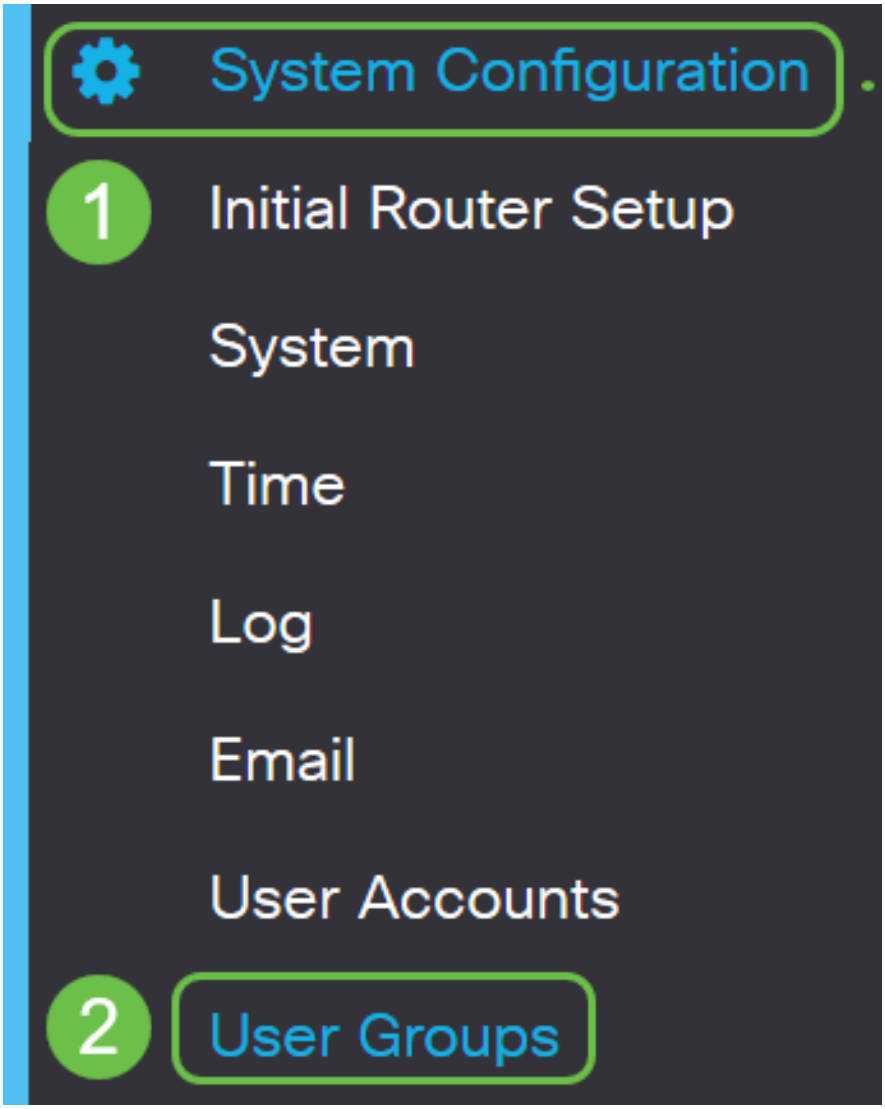
创建用户组

重要说明：请将默认管理员帐户保留在管理员组中，并为TheGreenBow创建新用户帐户和用户组。如果将管理员帐户移至其他组，则会阻止您登录路由器。

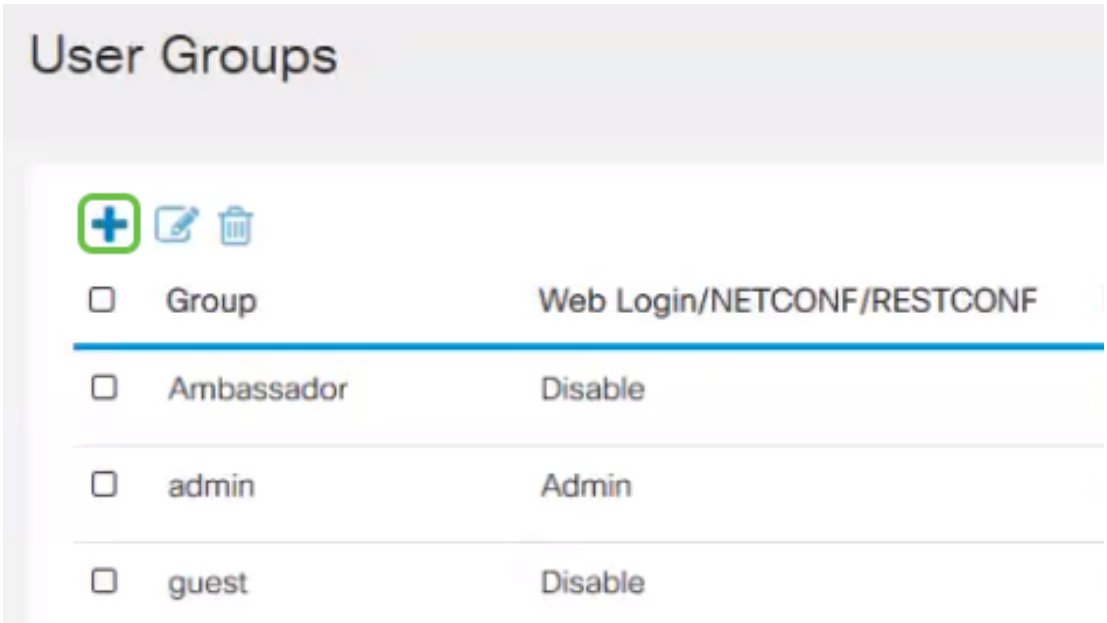
步骤1.登录路由器的基于Web的实用程序。



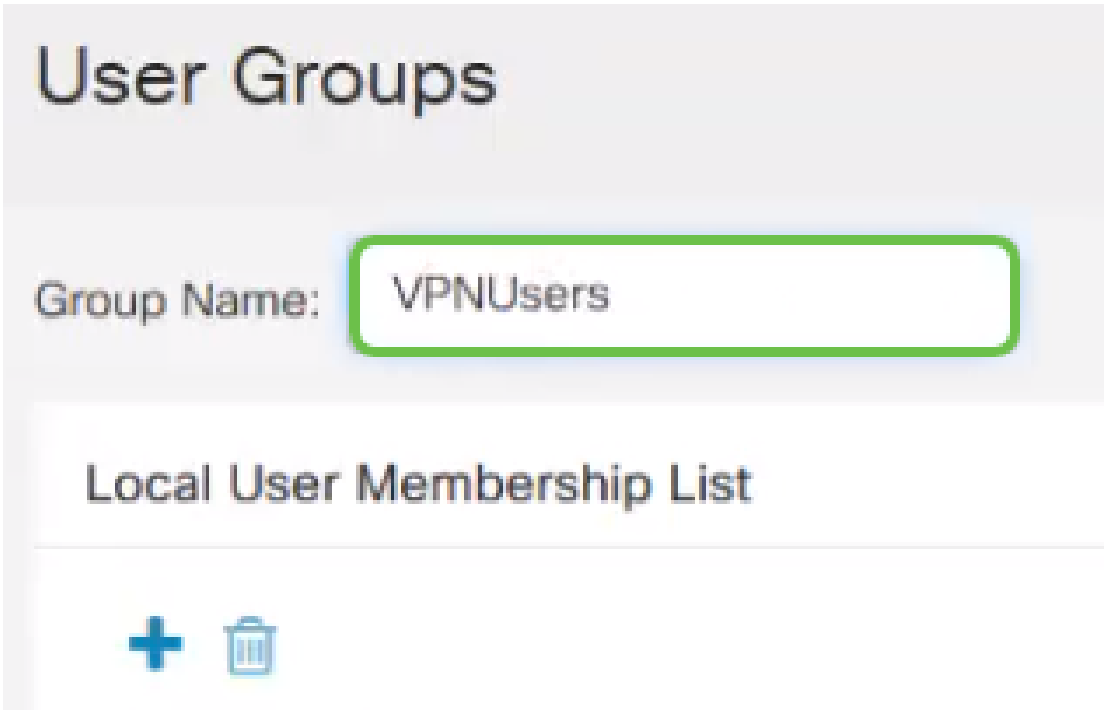
步骤2.选择System Configuration > User Groups。



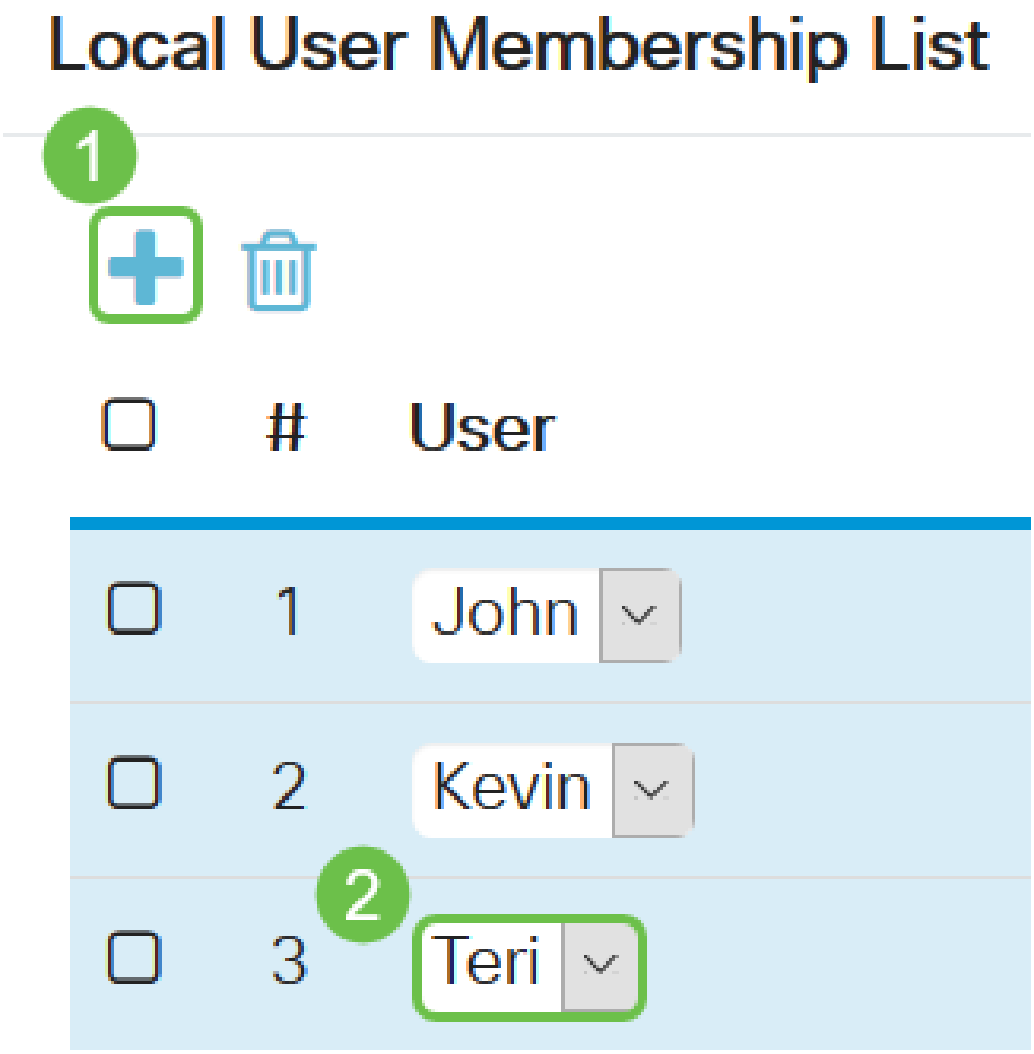
步骤3.单击加号图标添加用户组。



步骤4.在“概述”区域的“组名”字*段中输*入组。

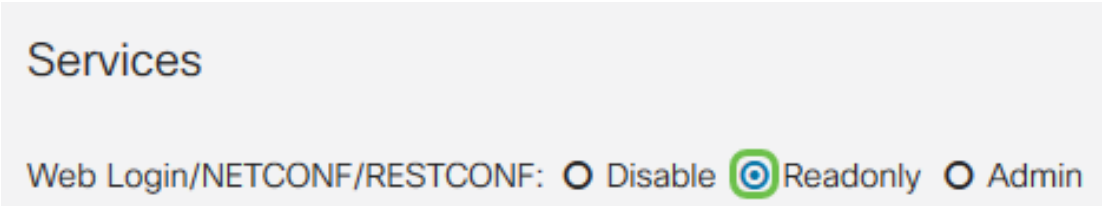


步骤5.在Local User *Membership List*下，单击**加号**图标，然后从下拉列表中选择用户。如果要添加更多，请再次按加**号**图标并选择要添加的其他成员。成员只能是一个组的一部分。如果尚未输入所有用户，则可以在“创建用户帐户”部分添加更多用户。

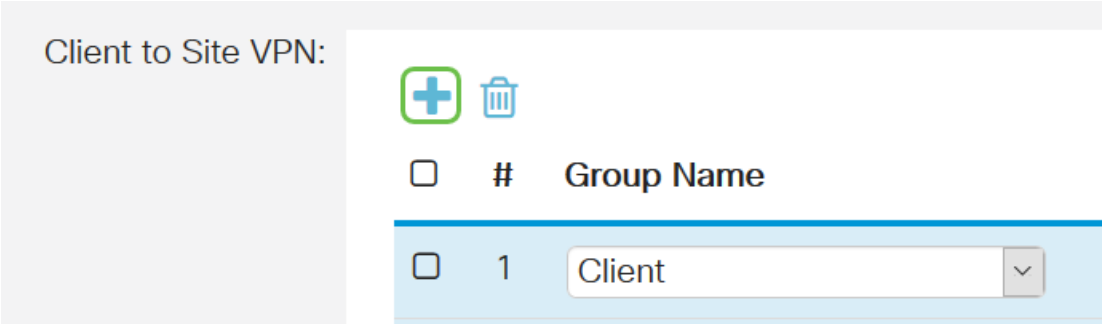


步骤6.在*Services*下，选择要授予组中用户的权限。选项有：

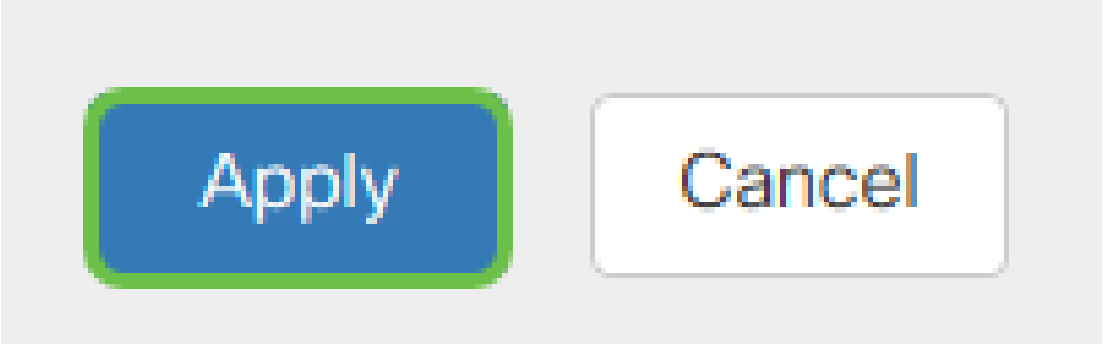
- 已禁用 — 此选项表示不允许组成员通过浏览器访问基于Web的实用程序。
- 只读 — 此选项表示组成员只能在登录后读取系统的状态。它们无法编辑任何设置。
- Admin — 此选项为组成员提供读和写权限，并且能够配置系统状态。



步骤7.单击**加号**图标添加现有的客户端到站点VPN。如果尚未配置此配置，您可以在“创建客户端到站点配置文件”一节中找到本文中的信息。

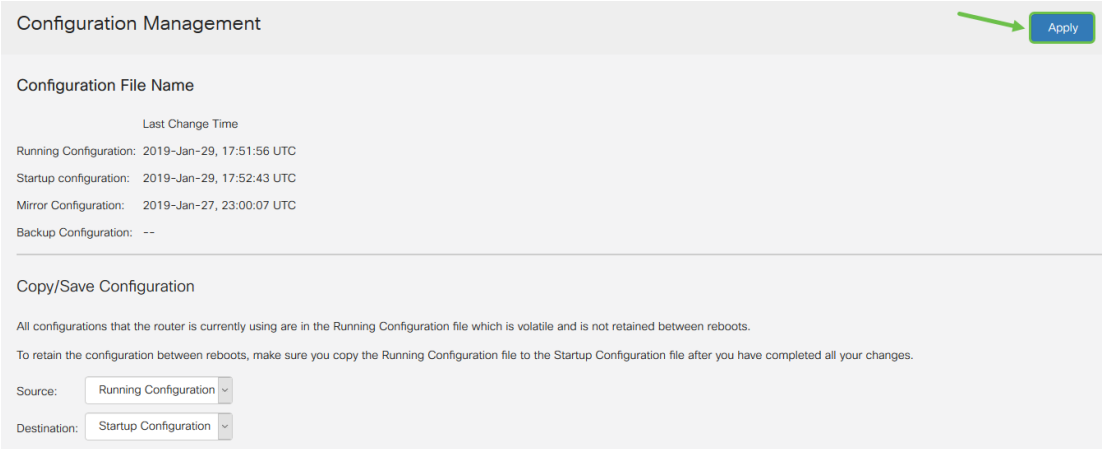


步骤8.单击“**应用**”。

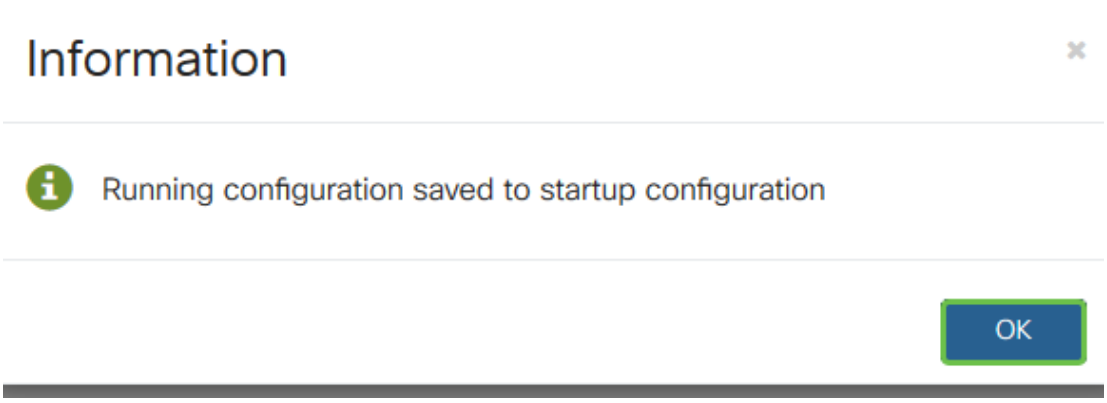


步骤9.单击“保**存**”。

步骤10.再次单击**Apply**，将运行配置保存到启动配置。



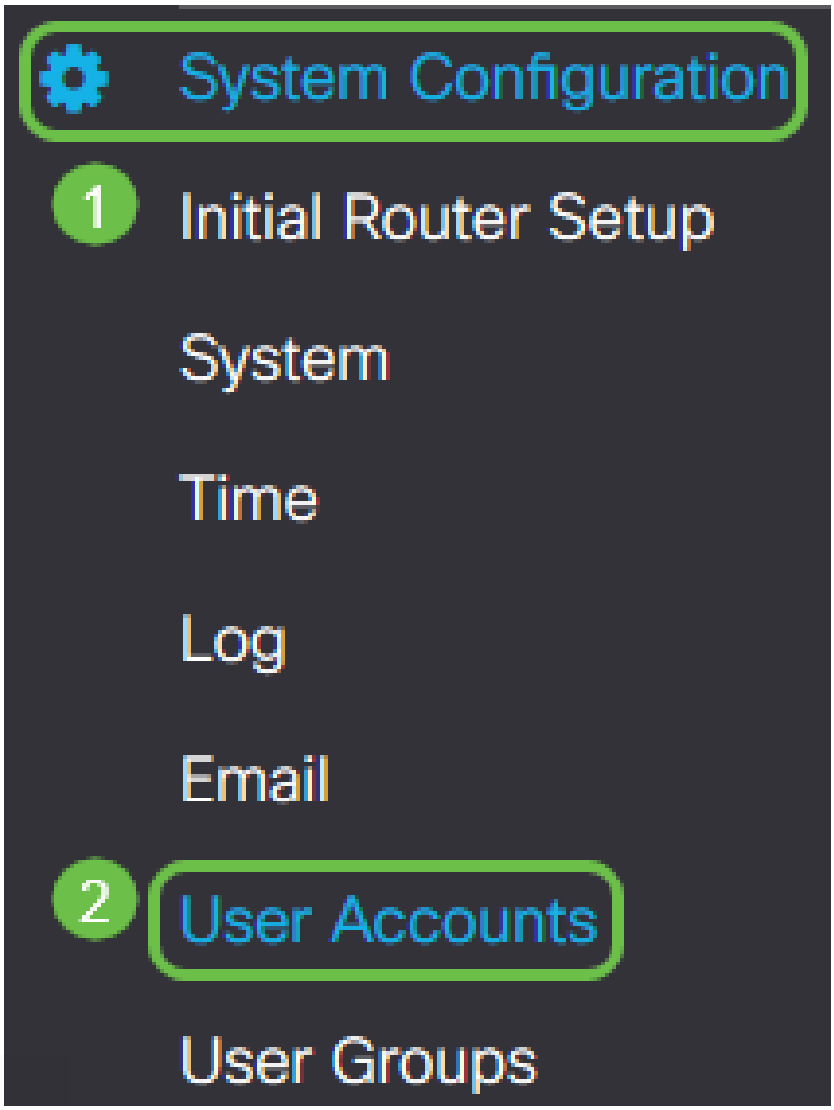
步骤11.收到确认信息后，单击“确**定**”。



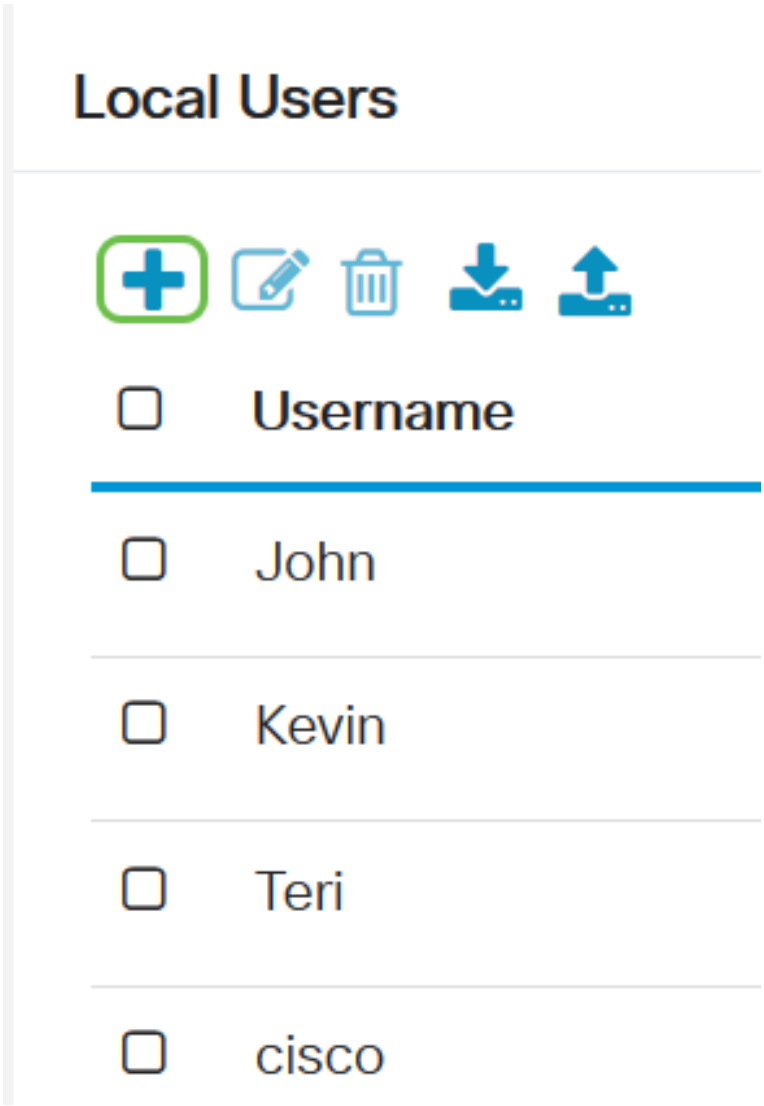
您现在应该已在RV160或RV260系列路由器上成功创建了用户组。

创建用户帐户

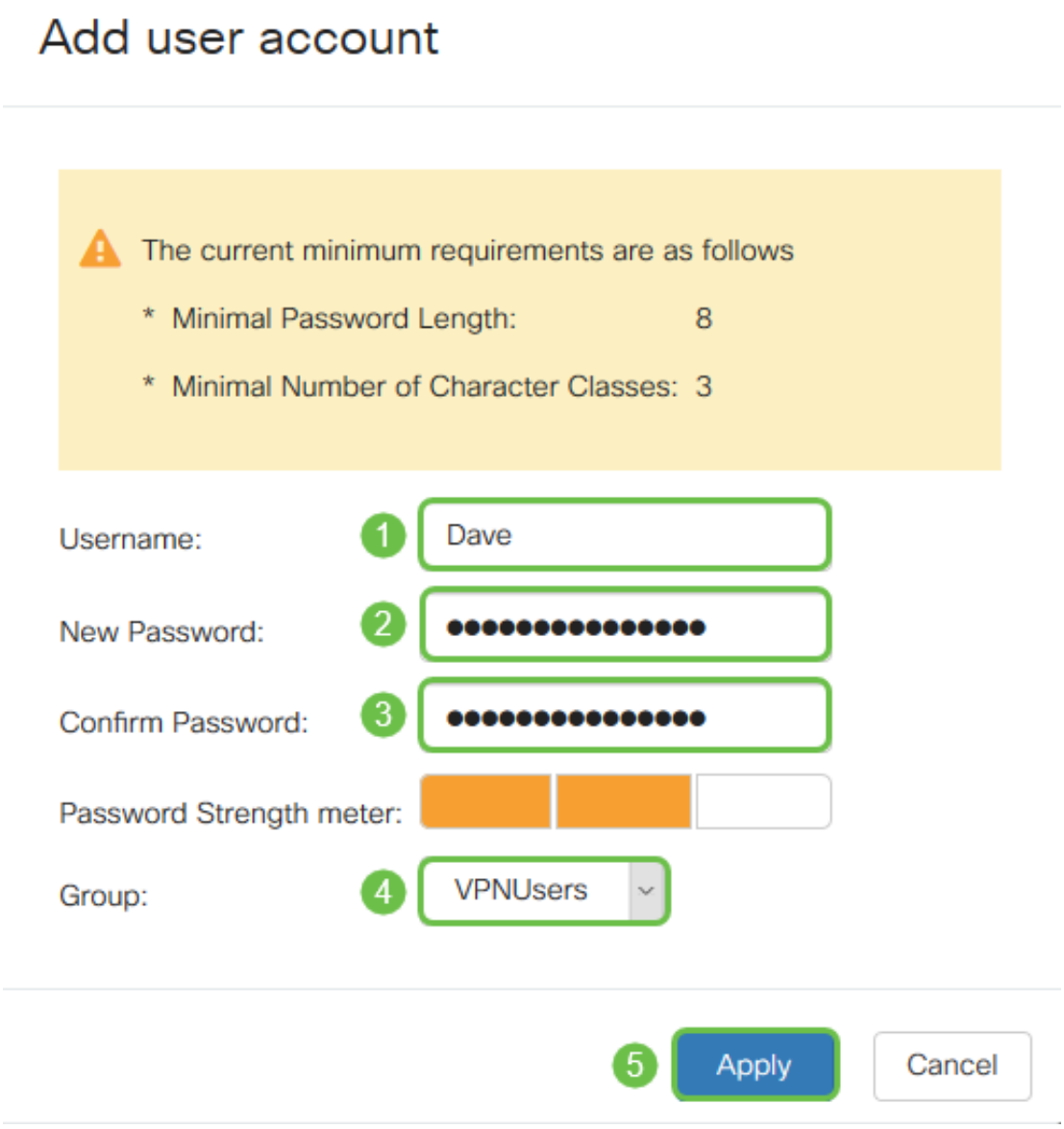
步骤1.登录到路由器的基于Web的实用程序，然后选择System Configuration > **User Accounts**。



步骤2.在Local Users区*域中*，单击添加**图**标。



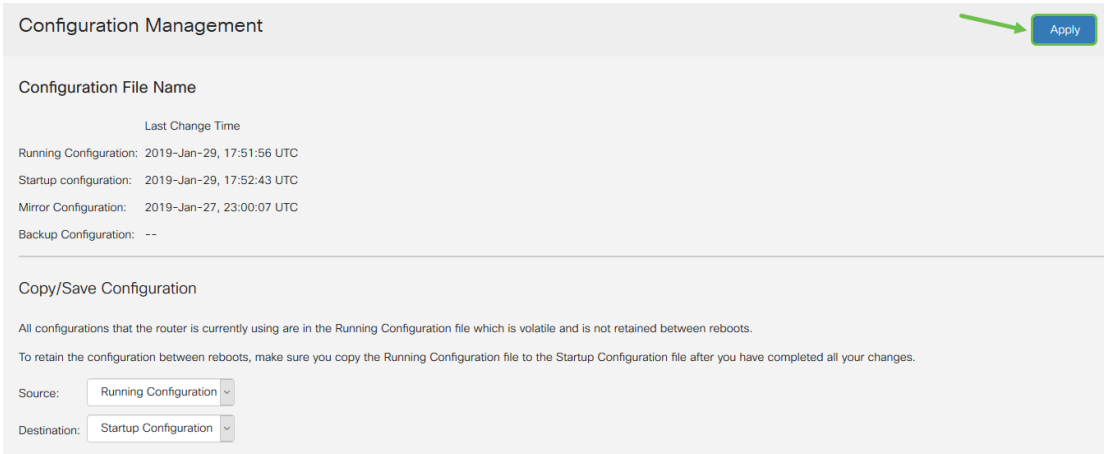
步骤3.在*用户名*字段中输入用户的名称、密码以及要从下拉菜单中将用户添加到的组。单击 **Apply**。



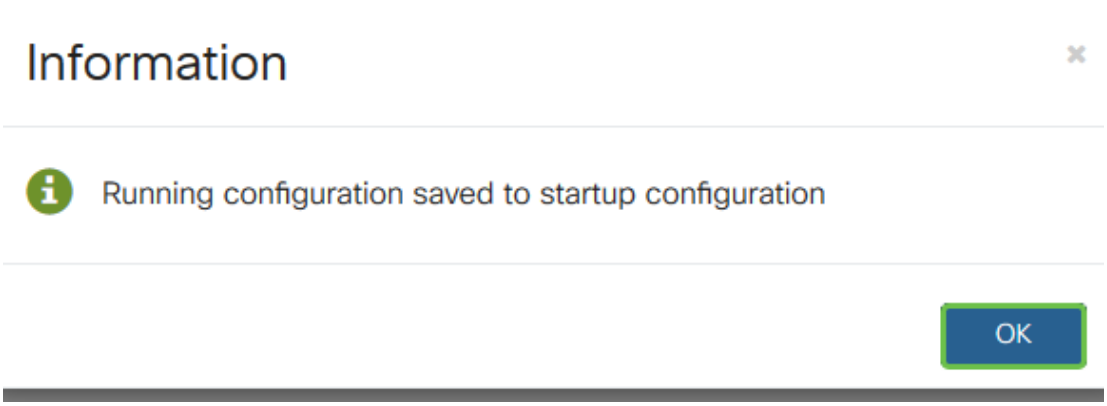
注意：当客户端在其计算机上设置TheGreenBow客户端时，他们将使用相同的用户名和密码登录。

步骤4.单击“保**存**”。

步骤5.再次单**击Apply**，将运行配置保存到启动配置。



步骤6.收到确认信息后，单击“确**定**”。

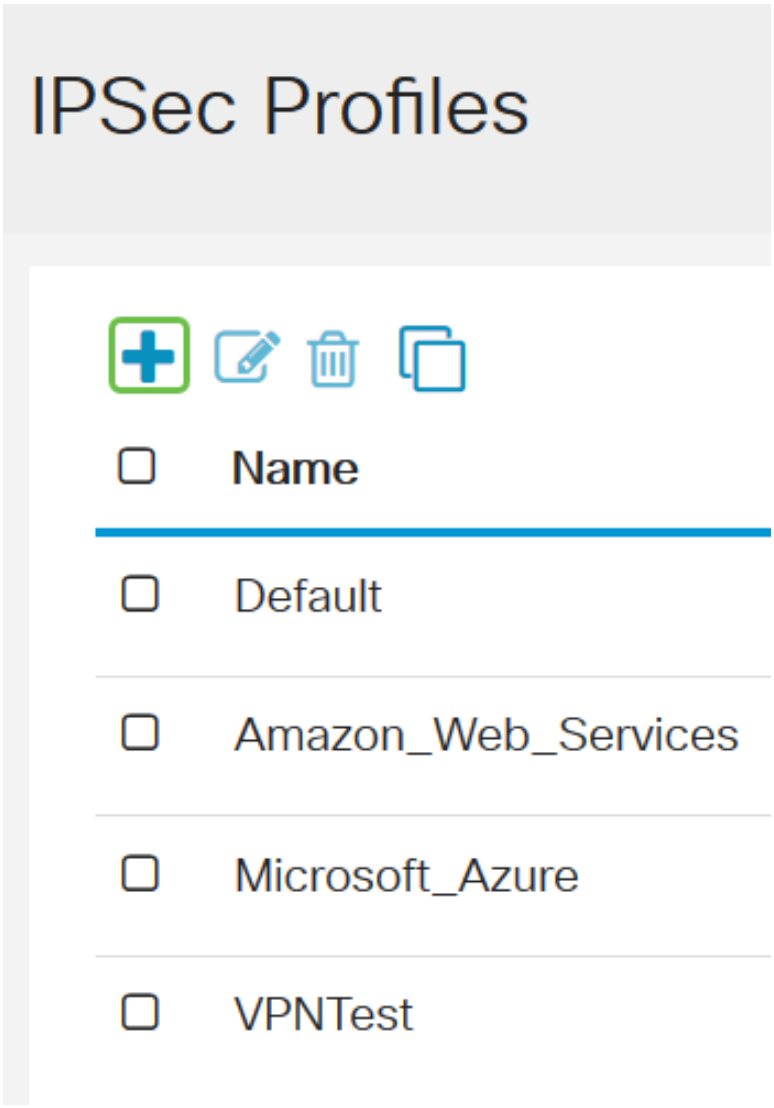


现在，您应该已在RV160或RV260路由器上创建用户帐户。

配置IPsec配置文件

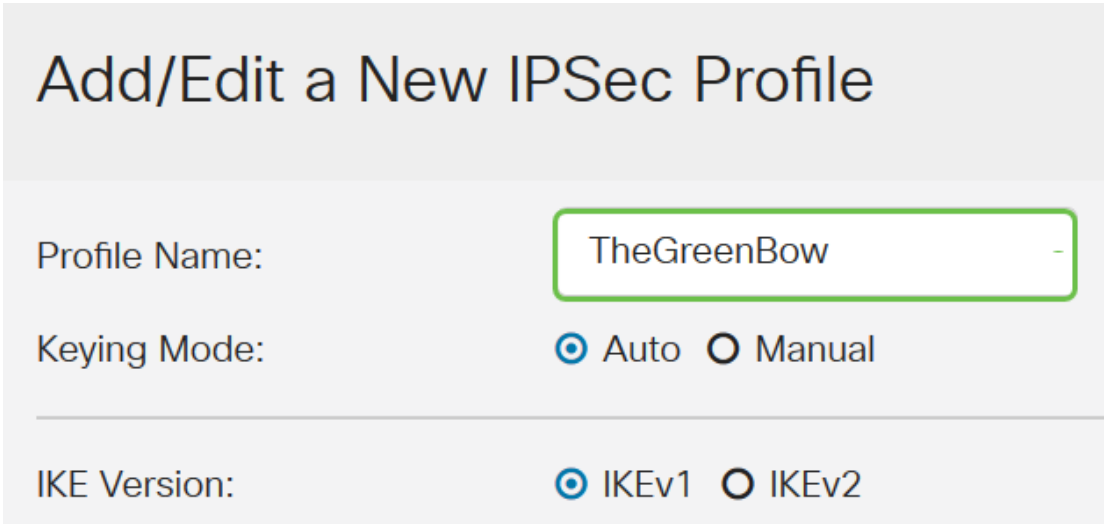
步骤1.登录到RV160或RV260路由器的基于Web的实用程序，然后选择**VPN > IPSec VPN > IPSec Profiles**。

步骤2. IPSec配置文件表显示现有配置文件。单击加**号**图标创建新配置文件。



注意：Amazon_Web_Services、Default和Microsoft_Azure是默认配置文件。

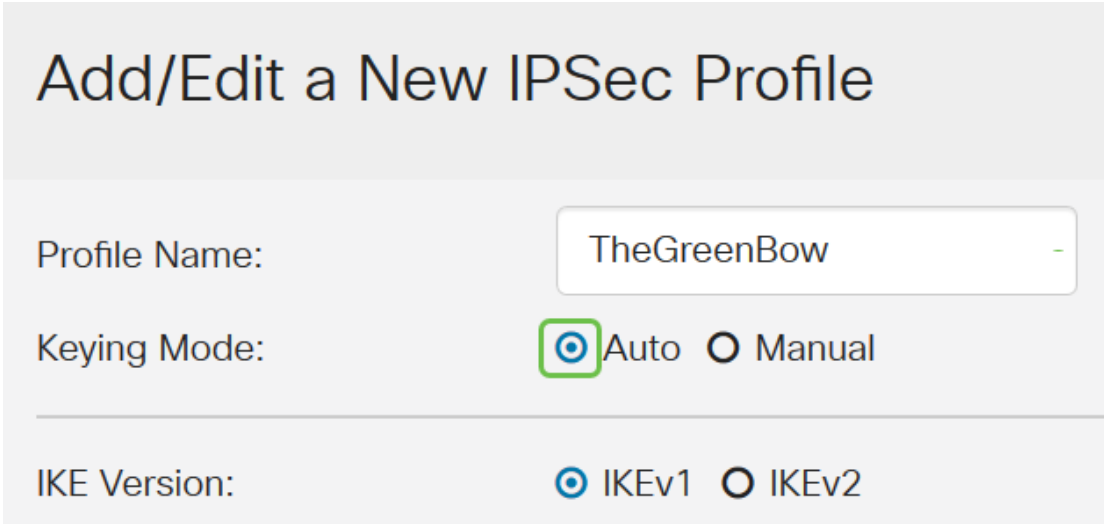
步骤3.在Profile Name字段中为配置文件*创建名*称。配置文件名称只能包含字母数字字符和特殊字符的下划线(_)。



步骤4.单击单选按钮确定配置文件将用于验证的密钥交换方法。选项有：

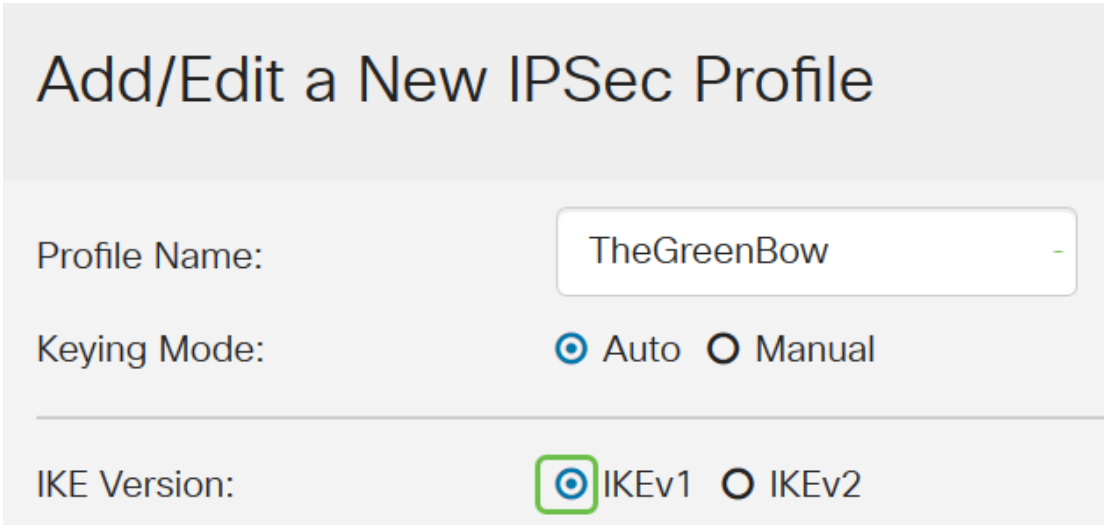
- 自动 — 策略参数自动设置。此选项使用互联网密钥交换(IKE)策略实现数据完整性和加密密钥交换。如果选择此选项，则启用Auto Policy Parameters区域下的配置设置。
- 手动 — 此选项允许您手动配置密钥以用于VPN隧道的数据加密和完整性。如果选择此选

项，则Manual Policy Parameters区域下的配置设置将启用。这并不广泛使用。



注意：在本例中，选**择了**Auto。

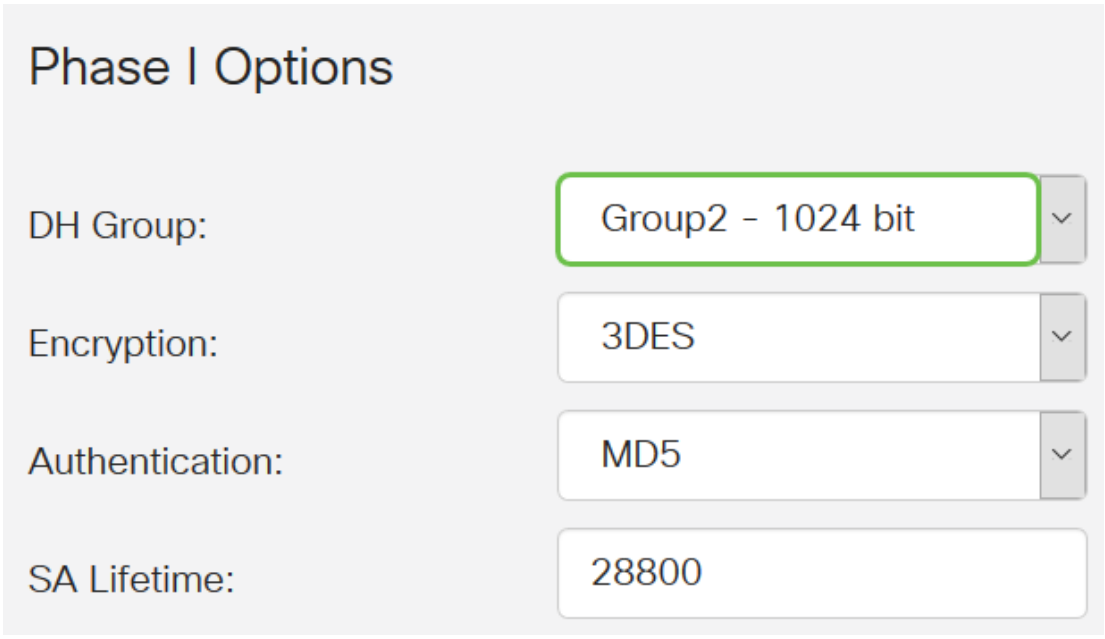
步骤5.选择IKE版本。在客户端上设置TheGreenBow时，请确保选择相同版本。



配置第1阶段和第2阶段设置

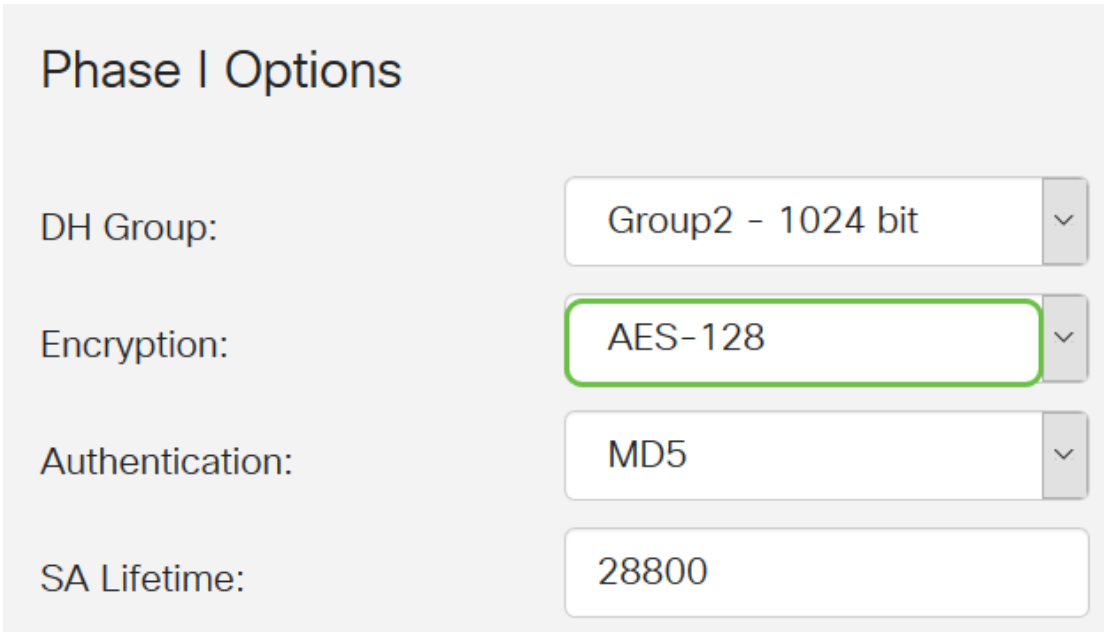
步骤1.在Phase 1 Options区域，从DH Group下拉列表中选择与Phase 1中的密钥一起使用的相应Diffie-Hellman(DH)组。Diffie-Hellman是用于交换预共享密钥集的连接中使用的加密密钥交换协议。算法的强度由位决定。选项有：

- 组2-1024位 — 此选项计算密钥的速度较慢，但比组1更安全。
- 组5-1536位 — 此选项计算最慢的密钥，但是最安全的密钥。



步骤2.从*加密*下拉列表中，选择加密方法以加密和解密封装安全负载(ESP)和互联网安全关联和密钥管理协议(ISAKMP)。 选项有：

- 3DES — 三重数据加密标准。不推荐.仅当需要向后兼容时才使用它，因为它容易受到某些“阻止冲突”攻击。
- AES-128 — 高级加密标准使用128位密钥。高级加密标准(AES)是一种加密算法，旨在比DES更安全。AES使用更大的密钥大小，确保只有入侵者才能尝试所有可能的密钥才能解密消息。
- AES-192 — 高级加密标准使用192位密钥。
- AES-256 — 高级加密标准使用256位密钥。这是最安全的加密选项。



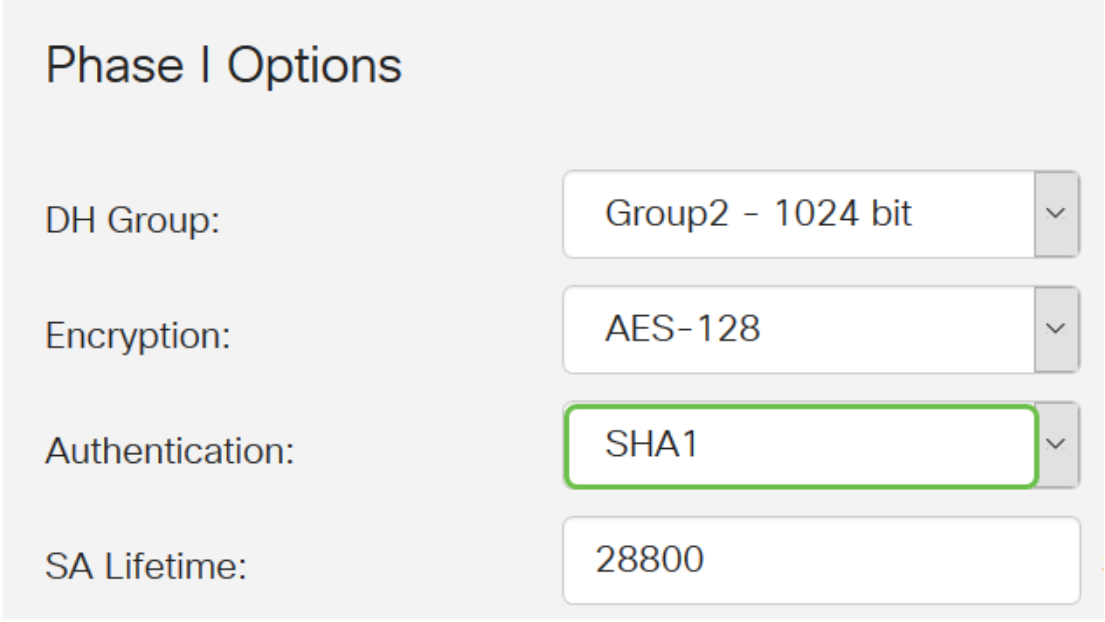
注意：AES是DES和3DES上的标准加密方法，因为其性能和安全性更高。加长AES密钥将提高安全性，性能会降低。

步骤3.从*Authentication*下拉列表中，选择确定如何对ESP和ISAKMP进行身份验证的身份验证方法。选项有：

- MD5 — 消息摘要算法有128位哈希值。
- SHA-1 — 安全散列算法有160位散列值。

- SHA2-256 — 安全散列算法，带256位散列值。这是最安全和推荐的算法。

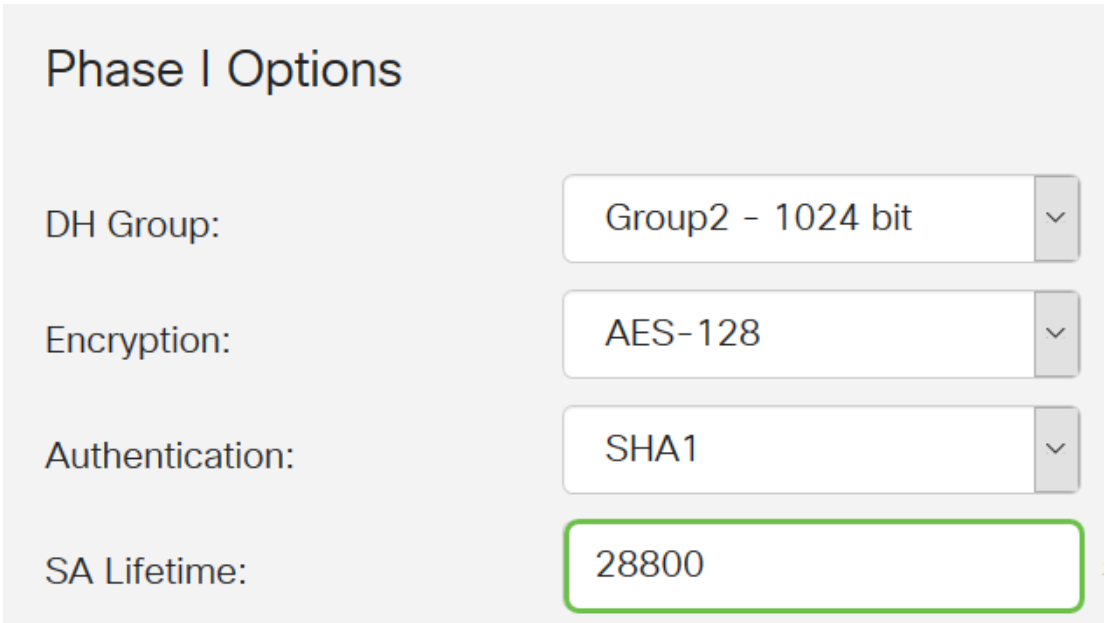
注意：确保VPN隧道两端使用相同的身份验证方法。



注意：MD5和SHA都是加密哈希函数。它们提取一段数据，将其压缩，并创建通常无法复制的唯一十六进制输出。在本例中，选择SHA1。

步骤4.在*SA Lifetime*字段中，输入一个介于120和86400之间的值。默认值为28800。*SA Lifetime(Sec)*告诉您IKE SA在此阶段处于活动状态的时间量（以秒为单位）。新安全关联(SA)在生命期到期前协商，以确保新SA在旧SA到期时就可使用。默认值为28800，范围为120到86400。我们将使用28800秒作为第I阶段的SA生存期。

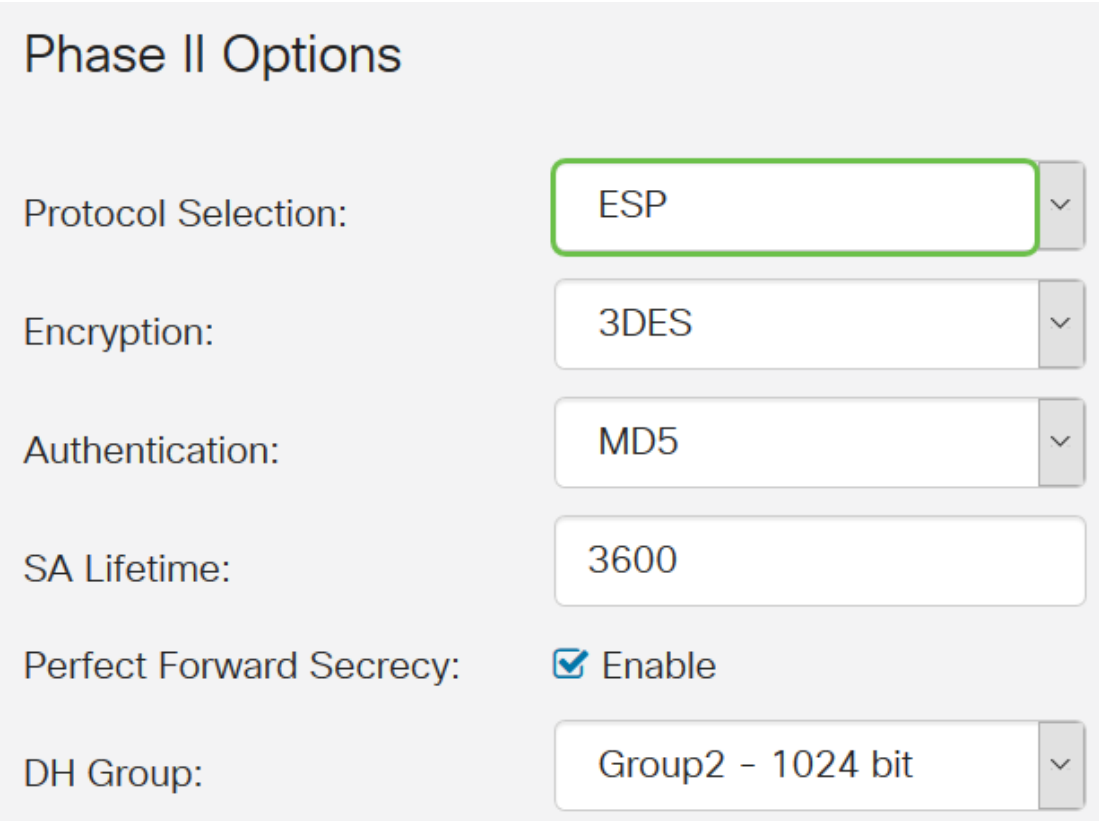
注意：建议您的SA生命周期在第I阶段比您的第II SA生命期长。如果将第I阶段缩短到第II阶段，则您将不得不频繁重新协商隧道，而不是数据隧道。数据隧道需要更高的安全性，因此最好在第II阶段使寿命短于第I阶段。



步骤5.从“第II阶段选项”区域的*“协议选择”*下拉列表中，选择要应用于协商第二阶段的协议类型。选项有：

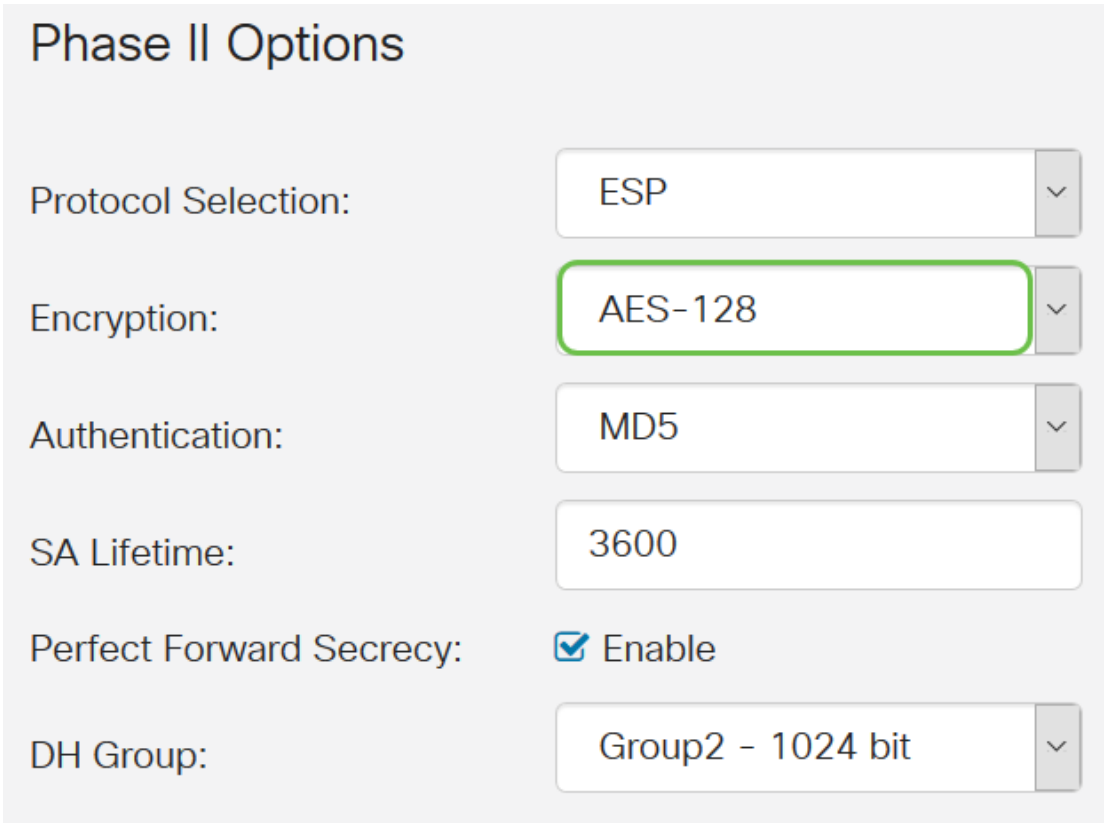
- ESP — 此选项也称为封装安全负载。此选项封装要保护的数据。如果选择此选项，请继续步骤6以选择加密方法。

- AH — 此选项也称为身份验证报头(AH)。 它是一种安全协议，提供数据身份验证和可选的反重播服务。AH嵌入到要保护的IP数据报中。如果选择此选项，请跳至步骤7。



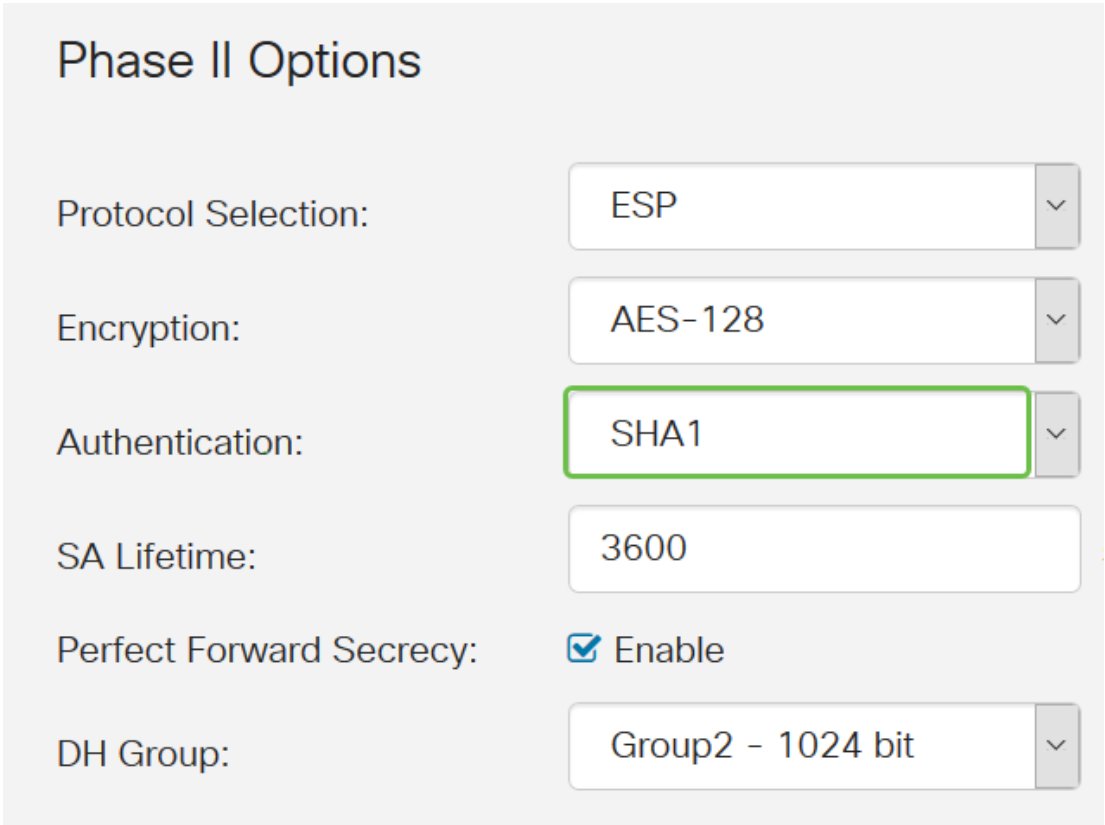
步骤6.如果在步骤6中选择了ESP，请选择加密。选项有：

- 3DES — 三重数据加密标准
- AES-128 — 高级加密标准使用128位密钥。
- AES-192 — 高级加密标准使用192位密钥。
- AES-256 — 高级加密标准使用256位密钥。

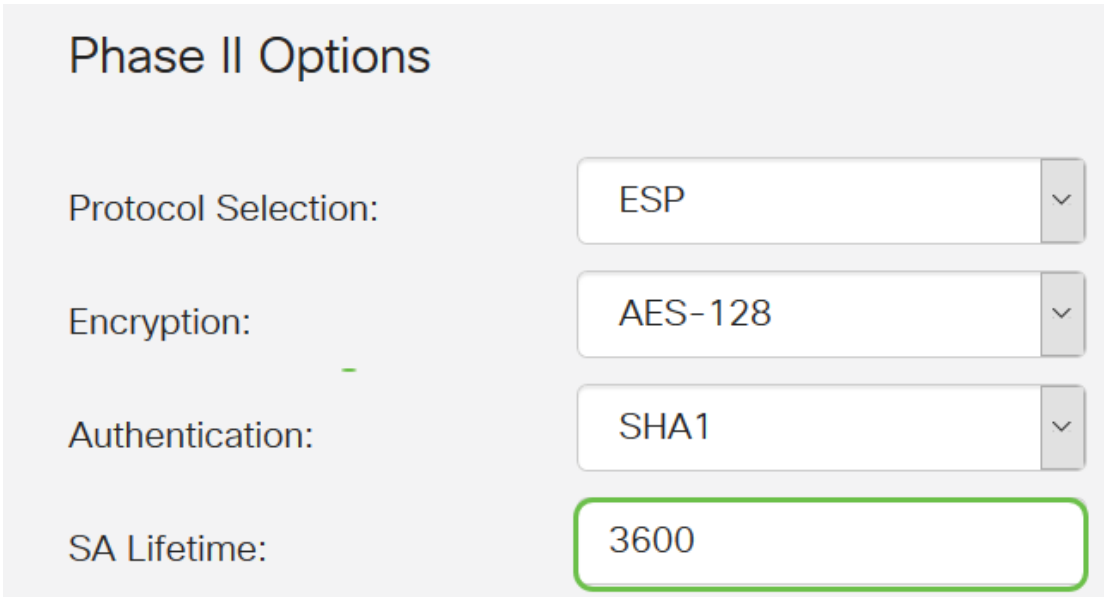


步骤7.从*Authentication*下拉列表中，选择确定如何对ESP和ISAKMP进行身份验证的身份验证方法。选项有：

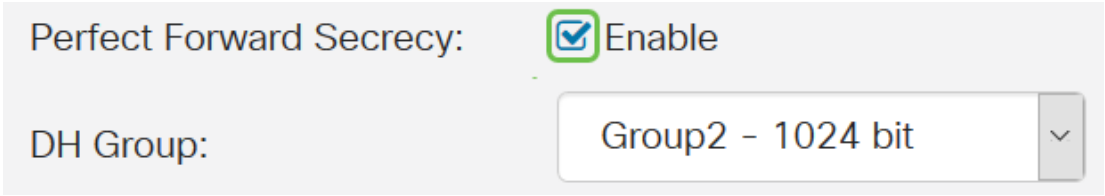
- MD5 — 消息摘要算法有128位哈希值。
- SHA-1 — 安全散列算法有160位散列值。
- SHA2-256 — 安全散列算法，带256位散列值。



步骤8.在*SA Lifetime*字段中，输入一个介于120和28800之间的值。这是IKE SA在此阶段保持活动状态的时间长度。默认值为 3600。

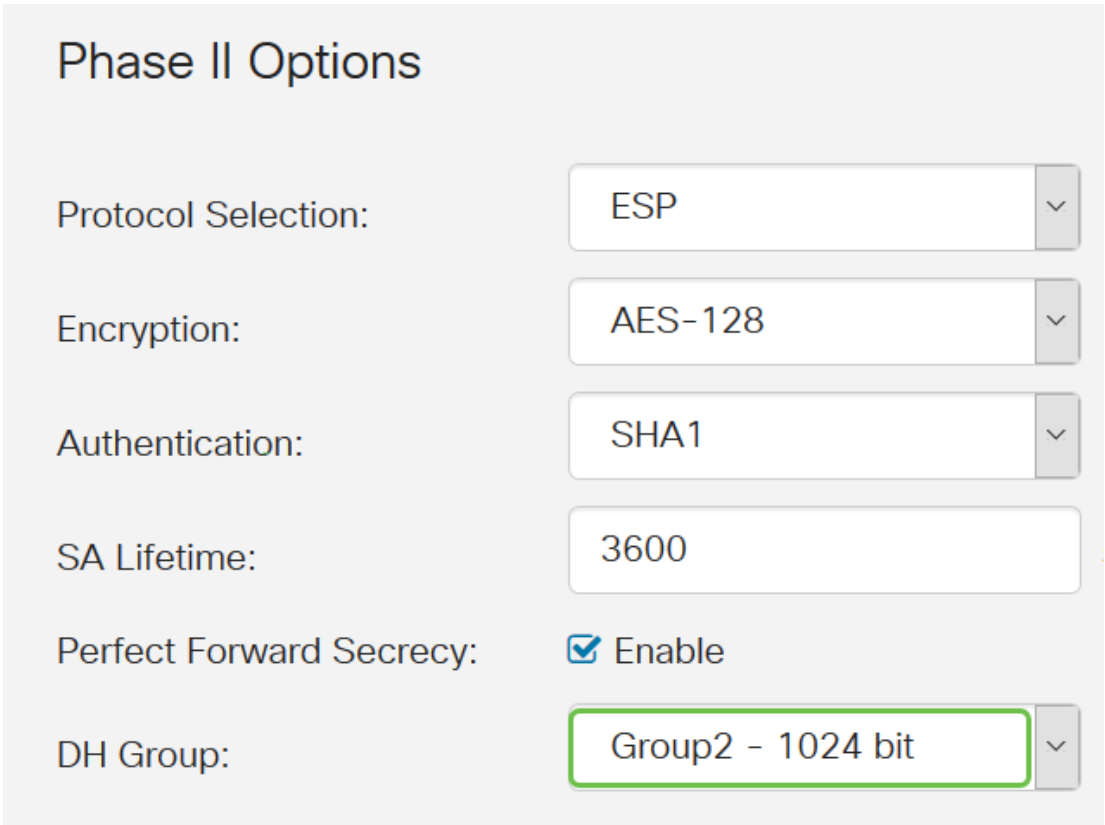


第9步。（可选）选中**Enable** Perfect Forward Secrecy复选框，为IPsec流量加密和身份验证生成新密钥。使用完全前向保密(Perfect Forward Secrecy)来提高通过Internet传输的通信的安全性。选中此框可启用此功能，或取消选中此框可禁用此功能。建议使用此功能。

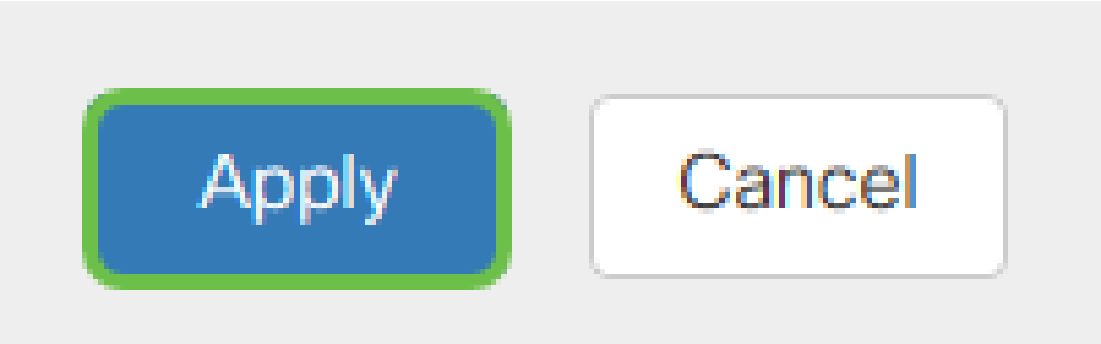


步骤10.从*DH组*下拉列表中，选择要与第2阶段的密钥一起使用的DH组。选项包括：

- 组2-1024位 — 此选项计算密钥的速度较快，但安全性较低。
- 组5-1536位 — 此选项计算最慢的密钥，但是最安全的密钥。

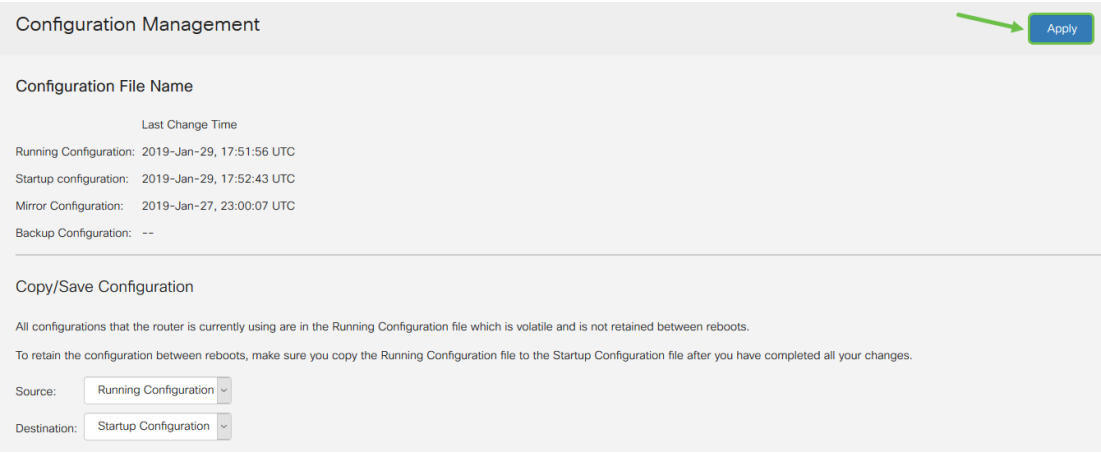


步骤11.单击“**应用**”。

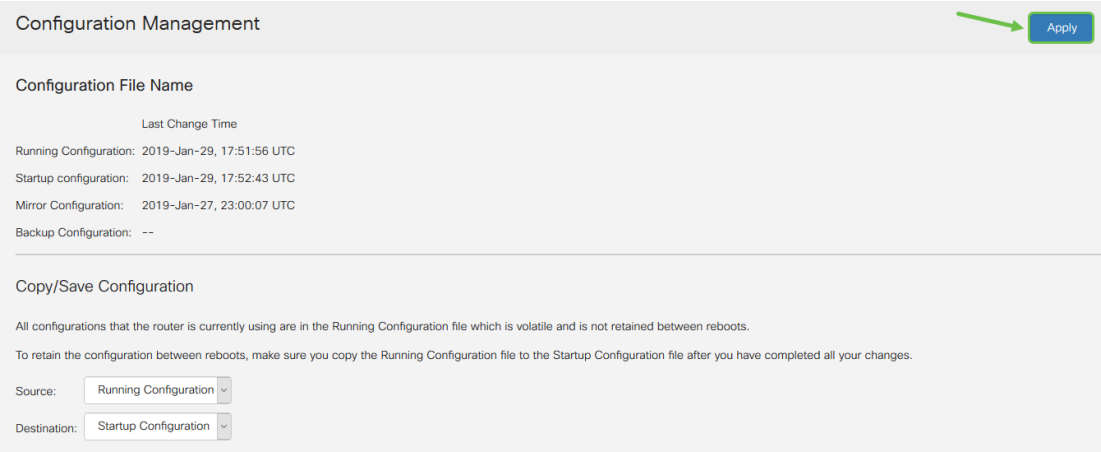


步骤12.单击“**保存**”永久保存配置。

步骤13.再次单击**Apply**，将运行配置保存到启动配置。



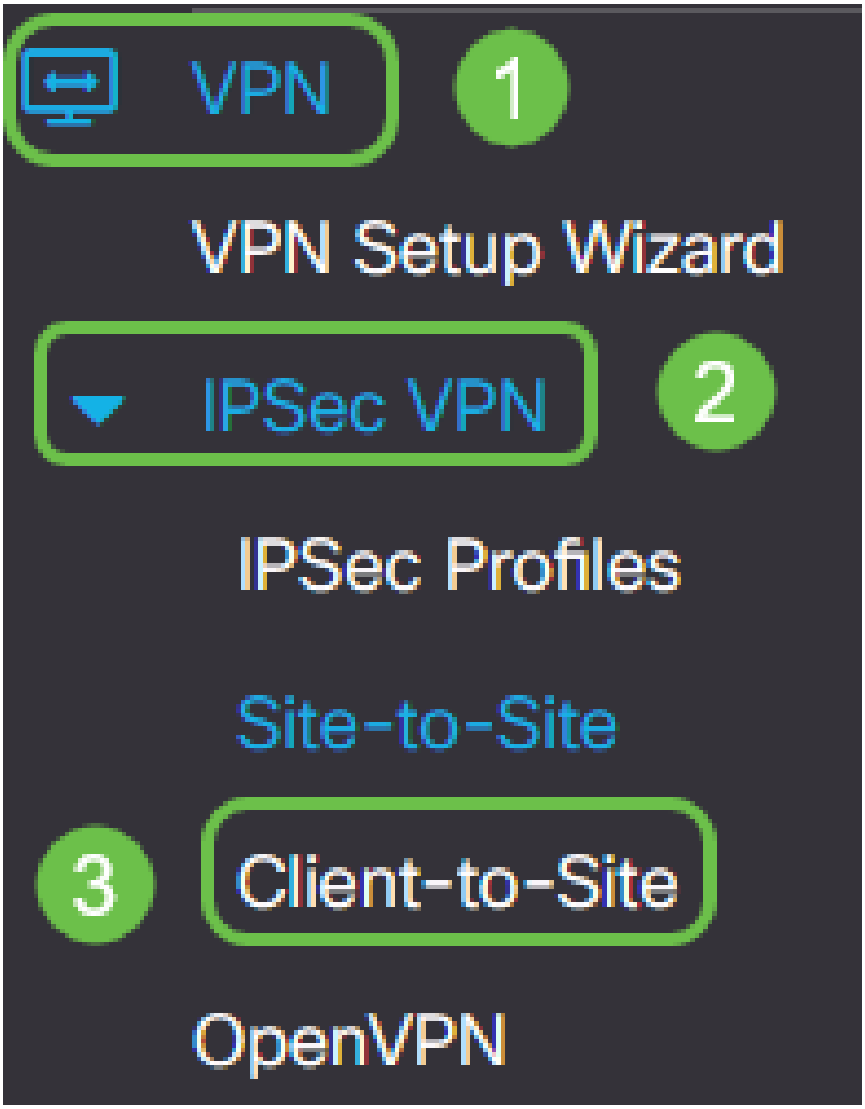
步骤14.收到确认信息后，单击“**确定**”。



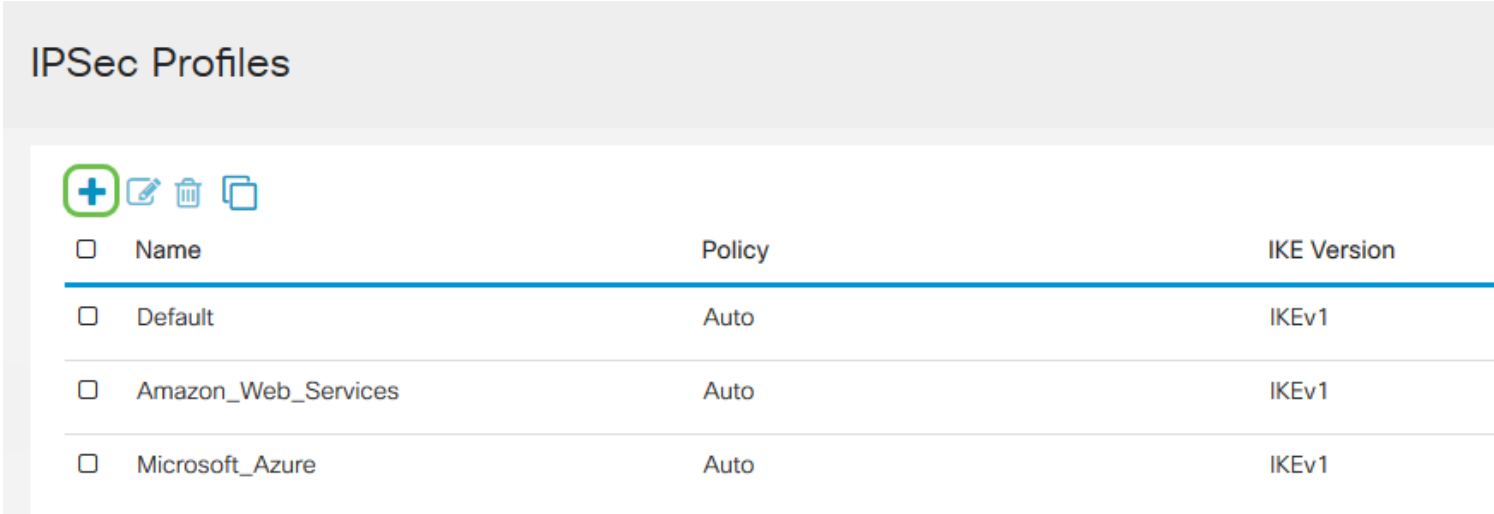
现在，您应该已在RV160或RV260路由器上成功配置了IPsec配置文件。

创建客户端到站点配置文件

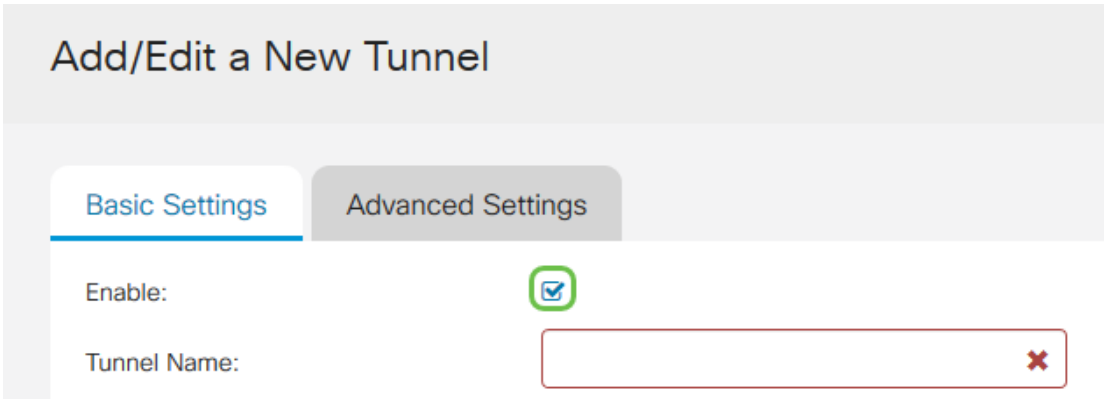
步骤1.选**择VPN > IPSec VPN > Client-to-Site**。



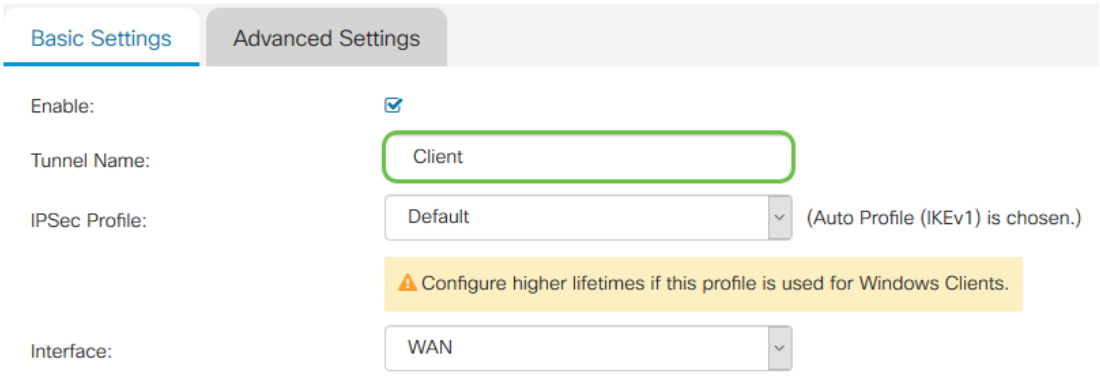
步骤2.单击加号图标。



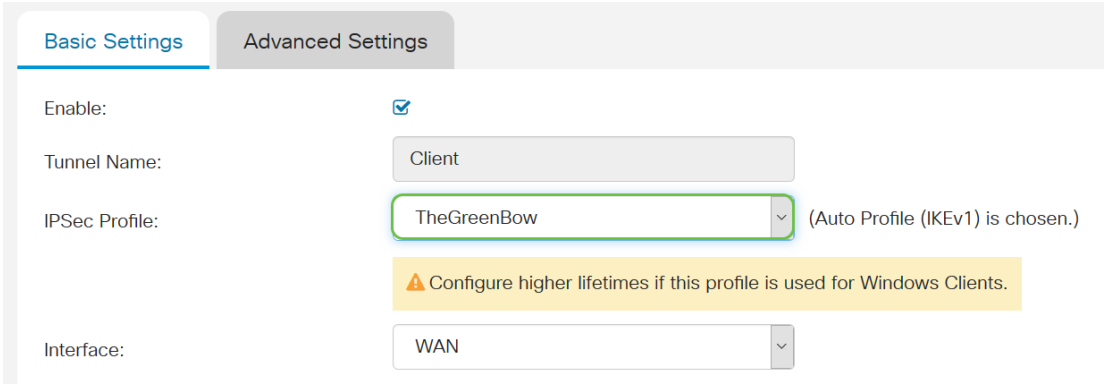
步骤3.在Basic Settings（基本设置）选项卡下，选中**Enable**（启用）复选框以确保VPN配置文件处于活动状态。



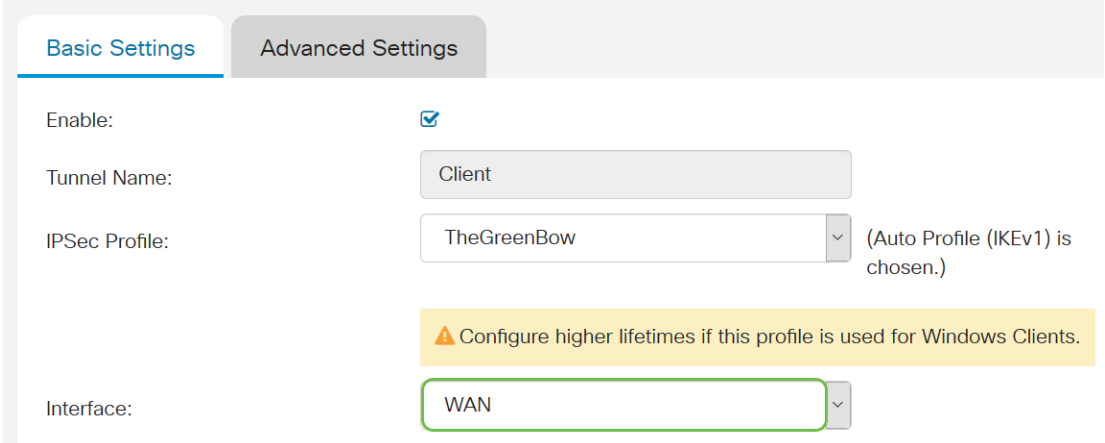
步骤4.在Tunnel Name字段中输入VPN连*接的名*称。



步骤5.从IPsec下拉列表中选择要使用的*IPsec*配置文件。



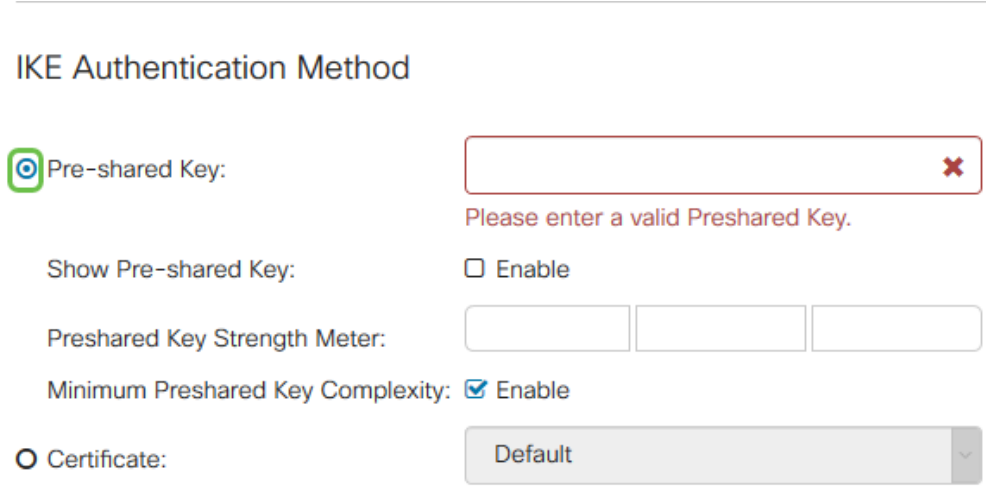
步骤6.从接口下拉列*表中*选择接口。



注意：这些选项取决于您使用的路由器型号。在本例中，选择WAN。

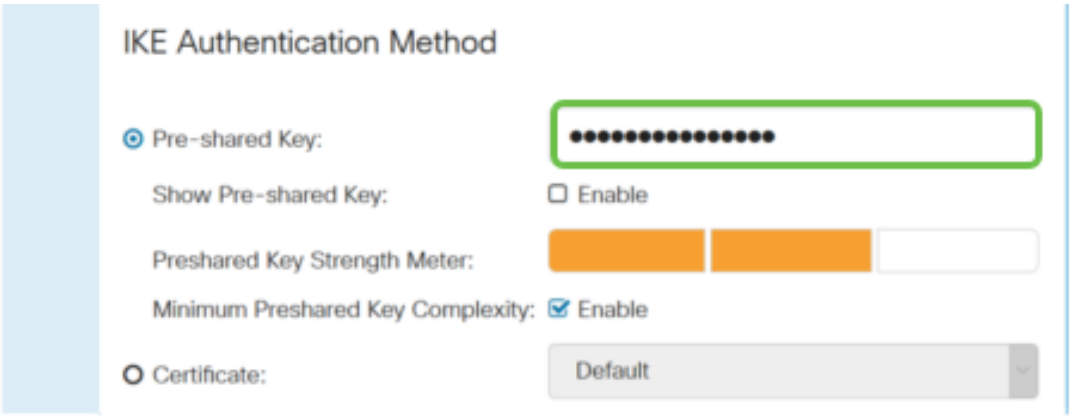
步骤7.选择IKE身份验证方法。选项有：

- 预共享密钥 — 此选项允许我们使用VPN连接的共享密码。
- 证书 — 此选项使用数字证书，该证书包含诸如证书名称或IP地址、序列号、证书到期日期以及证书持有者的公钥副本等信息。

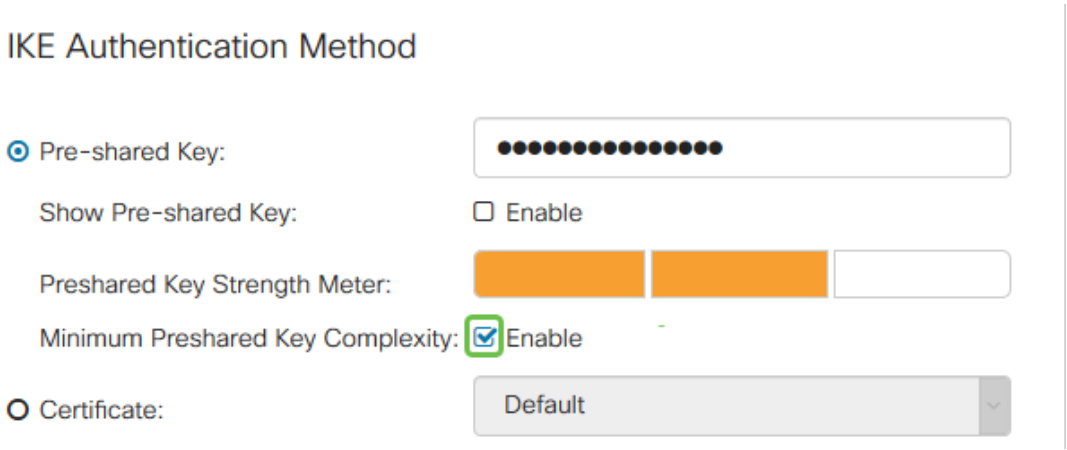


注意：预共享密钥可以是您想要的任何密钥，只需在站点和客户端上匹配即可，当他们在其计算机上设置TheGreenBow客户端时。

步骤8.在Pre-shared Key字段中输入*连接密码*。

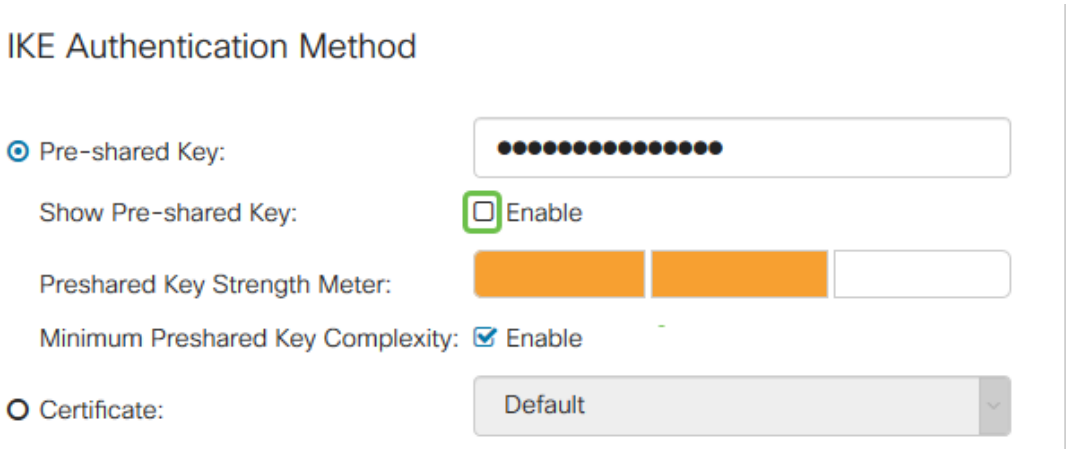


第9步。（可选）取消选中*Minimum Pre-shared Key Complexity Enable*复选框，以便能够使用简单密码。



注意：在本例中，“最小预共享密钥复杂性”(Minimum Pre-shared Key Complexity)处于启用状态。

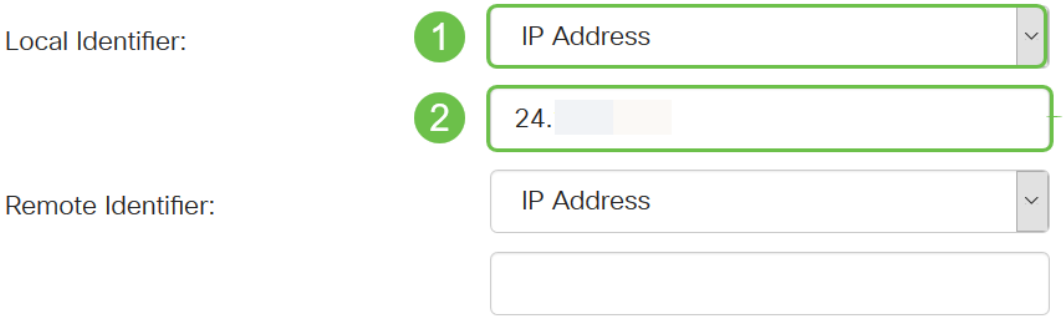
步骤10.（可选）选中*Show Pre-shared Key Enable*复选框以明文显示密码。



注意：在本例中，Show Pre-shared key（显示预共享密钥）保持禁用状态。

步骤11.从Local Identifier下拉列表中选择本地标识符。选项有：

- 本地WAN IP — 此选项使用VPN网关广域网(WAN)接口的IP地址。
- IP Address — 此选项允许您手动输入VPN连接的IP地址。这是站点（办公室）路由器的WAN IP地址。
- FQDN — 此选项也称为完全限定域名(FQDN)。 它允许您为Internet上的特定计算机使用完整的域名。
- 用户FQDN — 此选项允许您为Internet上的特定用户使用完整的域名。

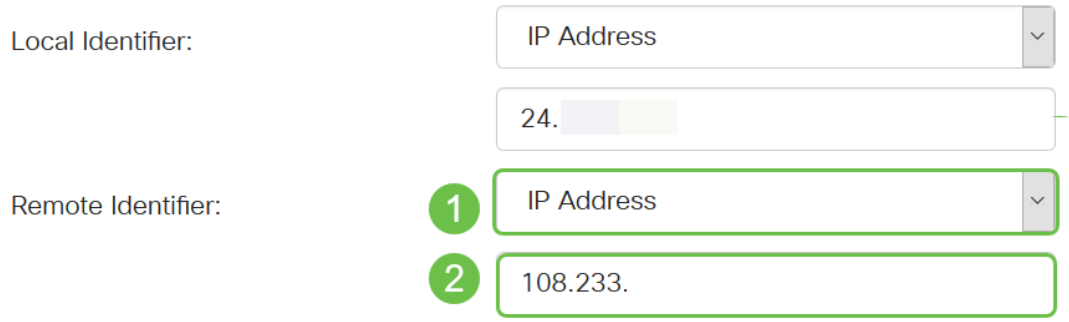


注意：在本例中，选择IP地址，并输入站点路由器的WAN IP地址。在本例中，已输入24.x.x.x。出于隐私考虑，完整地址已模糊。

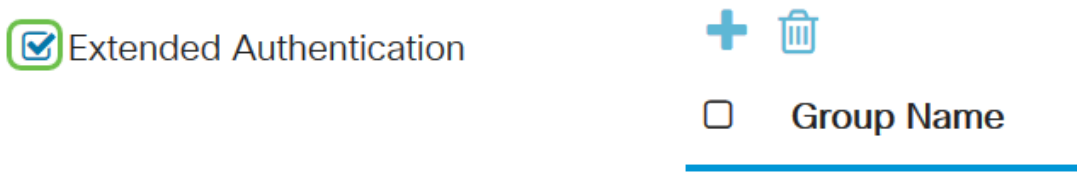
步骤12.选择远程主机的标识符。选项有：

- IP地址(IP Address) — 此选项使用VPN客户端的WAN IP地址。要查找WAN IP地址，您可以在Web浏览器中输入“我的IP是什么”。这是客户端IP地址。
- FQDN — 完全限定域名。此选项允许您为Internet上的特定计算机使用完整的域名。
- 用户FQDN — 此选项允许您为Internet上的特定用户使用完整的域名。

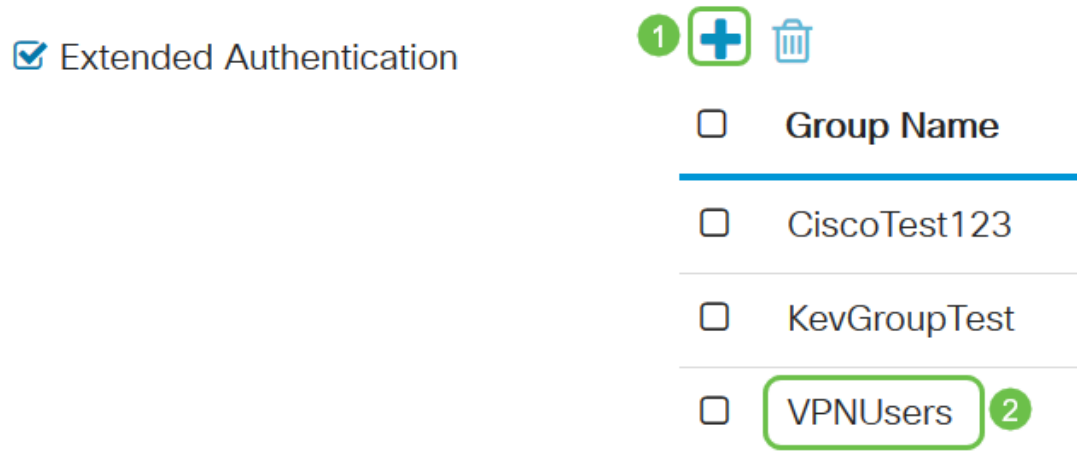
注意：在本例中，选择IP地址，并输入路由器在客户端位置的当前IPv4地址。这可以通过在Web浏览器中搜索“我的IP地址是什么”来确定。此地址可能会更改，因此，如果在配置成功后出现连接问题，则此区域可以在客户端和站点上进行检查和更改。



步骤13.（可选）选中Extended Authentication**复选框**以激活该功能。激活后，这将提供额外的身份验证级别，要求远程用户在授予VPN访问权限之前在其凭证中进行密钥。



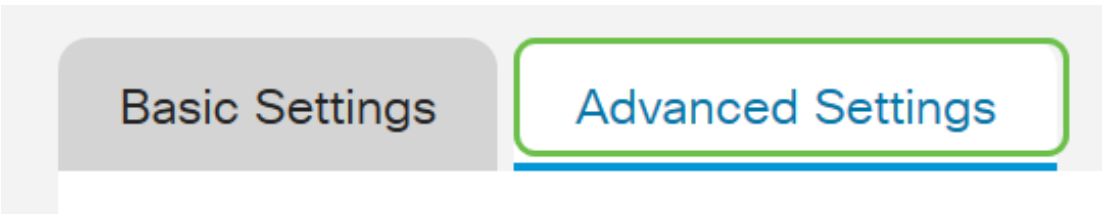
第14步。（可选）单击加号图标，选择将使用扩展身份验证的组，然后从下拉列表中选**择该**用户。



注意：在本例中，选**择VPNUsers**。

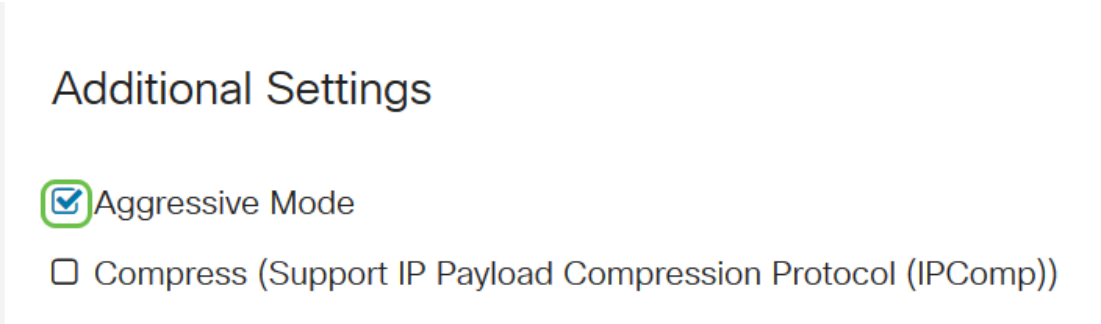
步骤15.在Pool *Range for Client LAN*下，输入可分配给VPN客户端的第一个IP地址和结束IP地址。这必须是一个地址池，与站点地址不重叠。这些接口可称为虚拟接口。如果您收到需要更改虚拟接口的消息，您将在此修复该消息。

步骤16.选择Advanced Settings(**高级设置**)选项卡



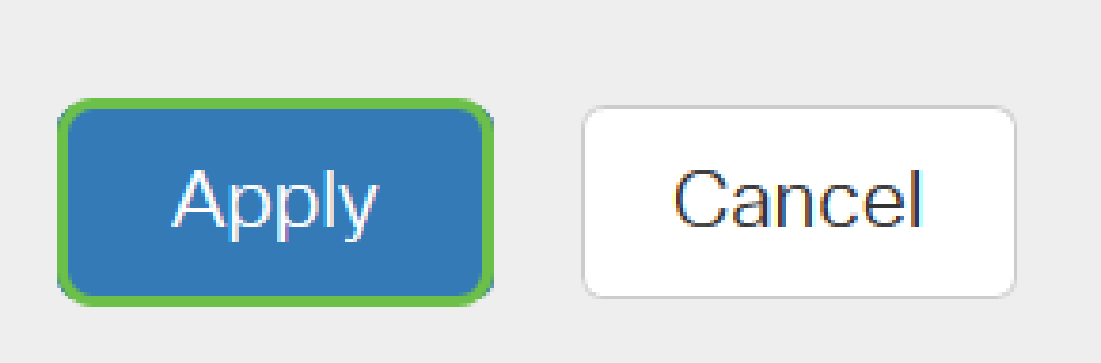
步骤17.（可选）向下滚动到页面底部并选择**Aggressive Mode**。主动模式功能允许您为IP安全(IPsec)对等体指定RADIUS隧道属性，并启动与隧道的互联网密钥交换(IKE)主动模式协商。有关主

动模式与主模式的详细信息，请单击此处。

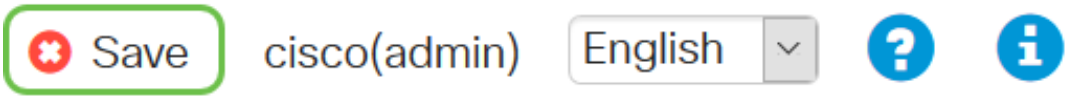


注意：Compress复选框使路由器在开始连接时能够建议压缩。此协议可减小IP数据报的大小。如果响应方拒绝此建议，则路由器不实施压缩。当路由器是响应方时，它接受压缩，即使未启用压缩。如果为此路由器启用此功能，则需要在远程路由器（隧道的另一端）上启用此功能。 在本例中，未选中*Compress*。

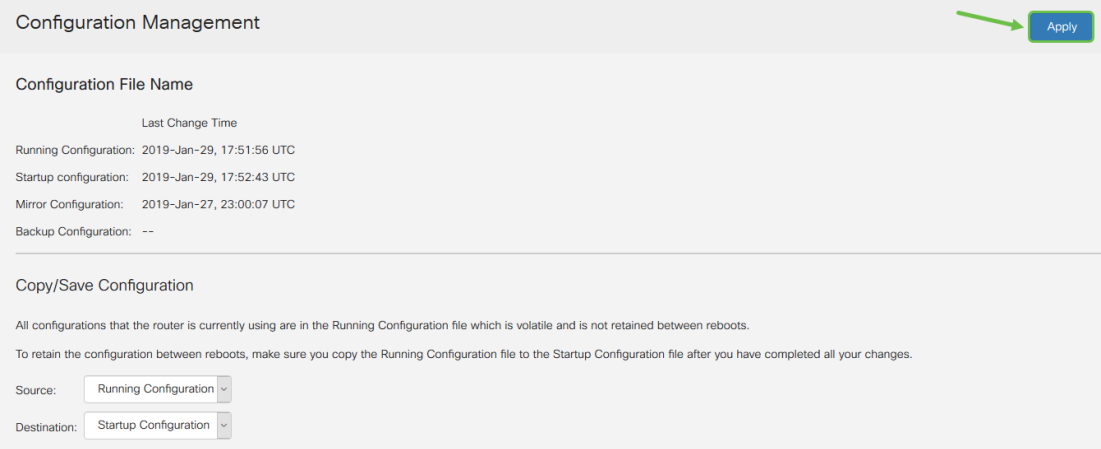
步骤18.单击“**应用**”。



步骤19.单击“保**存**”。



步骤20.再次单击**Apply**，将运行配置保存到启动配置。



步骤21.收到确认信息后，单击“确**定**”。

现在，您应该已在路由器上为GreenBow VPN客户端配置了客户端到站点隧道。

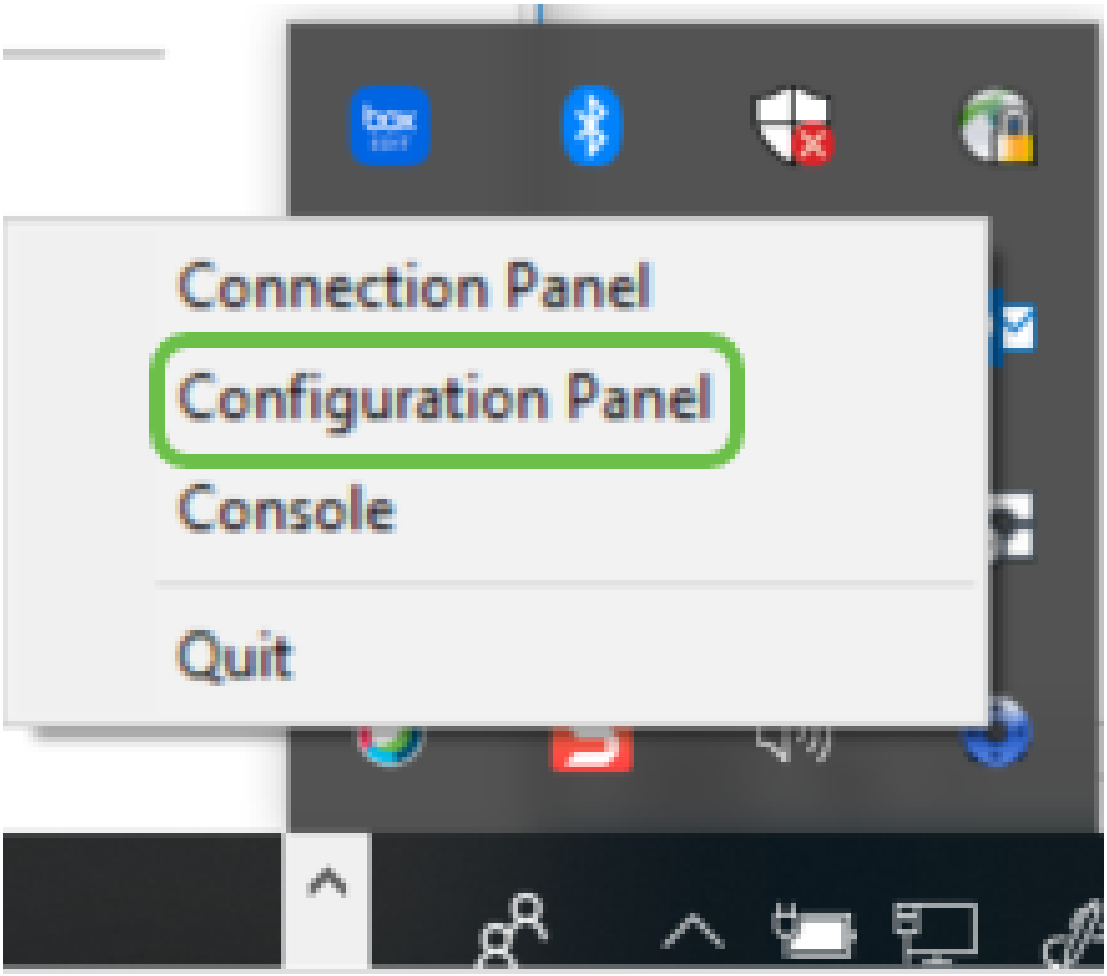
在远程工作人员的计算机上配置GreenBow VPN客户端

配置第1阶段设置

要下载TheGreenBow IPsec VPN客户端软件的最新版本，请单击此处。

步骤1.右键点击GreenBow VPN客户端图标。此按钮位于任务栏的右下角。

步骤2.选择“**配置面板**”。



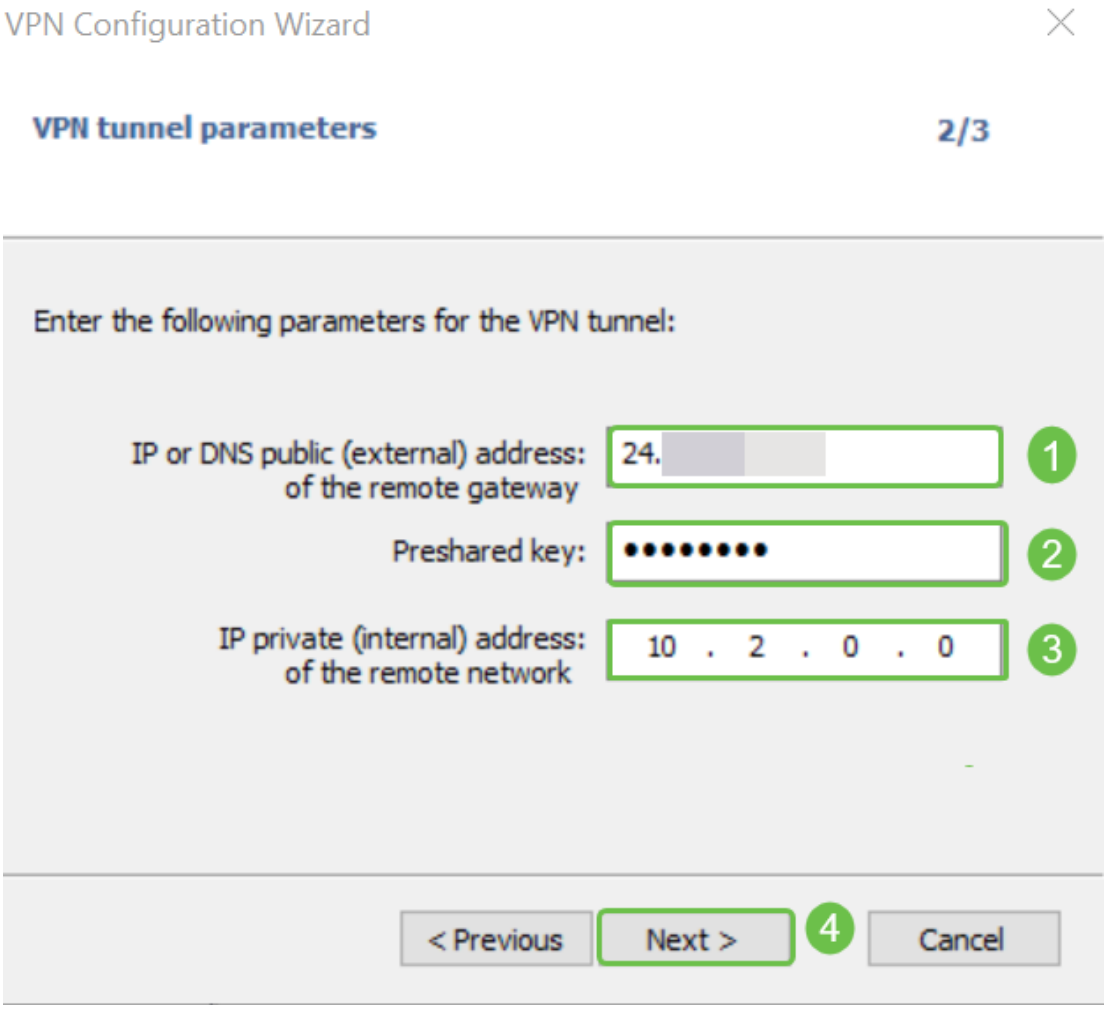
注意：这是Windows计算机上的一个示例。这取决于您使用的软件。

步骤3.选择**IKE V1 IPsec隧道创建向导**。

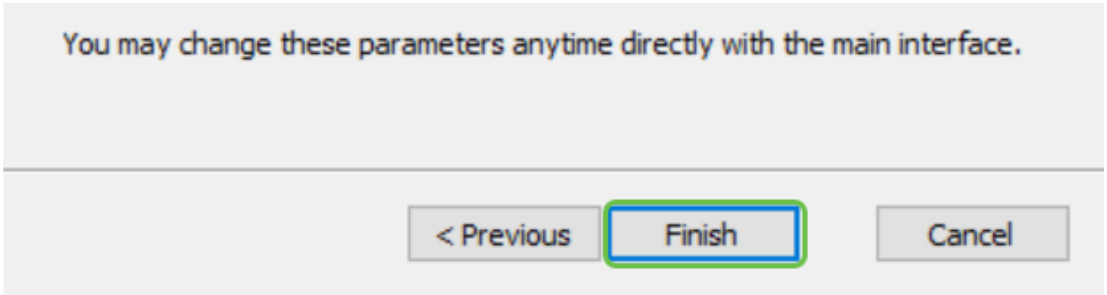
注意：在本例中，正在配置IKE版本1。如果要配置IKE版本2，您将执行相同的步骤，但右键点击IKE V2文件夹。您还需要为站点上的路由器上的IPsec配置文件选择IKEv2。

步骤4.填写文件服务器所在站点（办公室）路由器的公有WAN IP地址、预共享密钥和现场远程网络的私有内部地址。单击 **Next**。在本例中，站点为24.x.x.x。最后三个二进制八位数（此IP地址中的

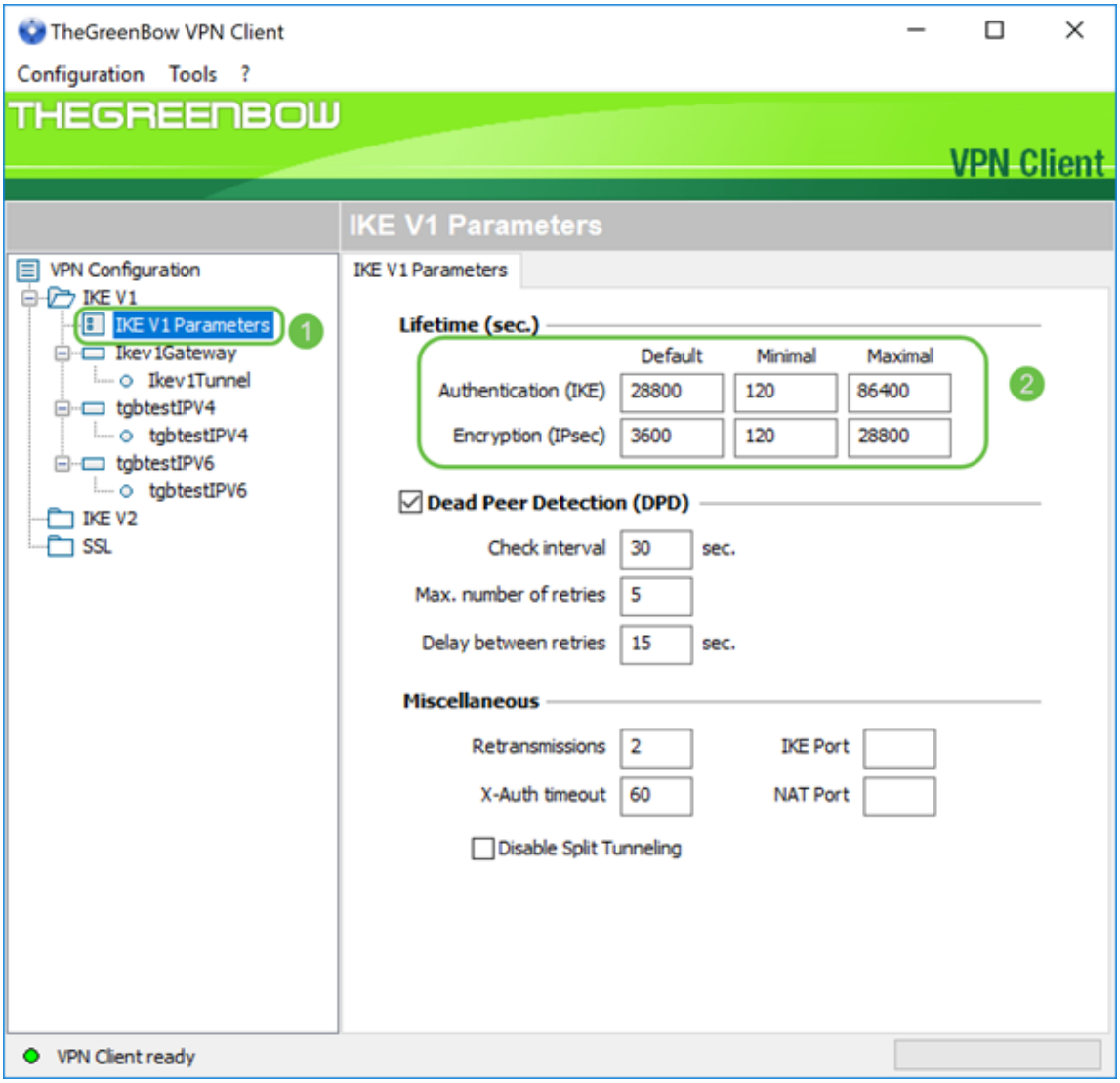
数字集）已替换为x以保护此网络。您可以输入完整的IP地址。



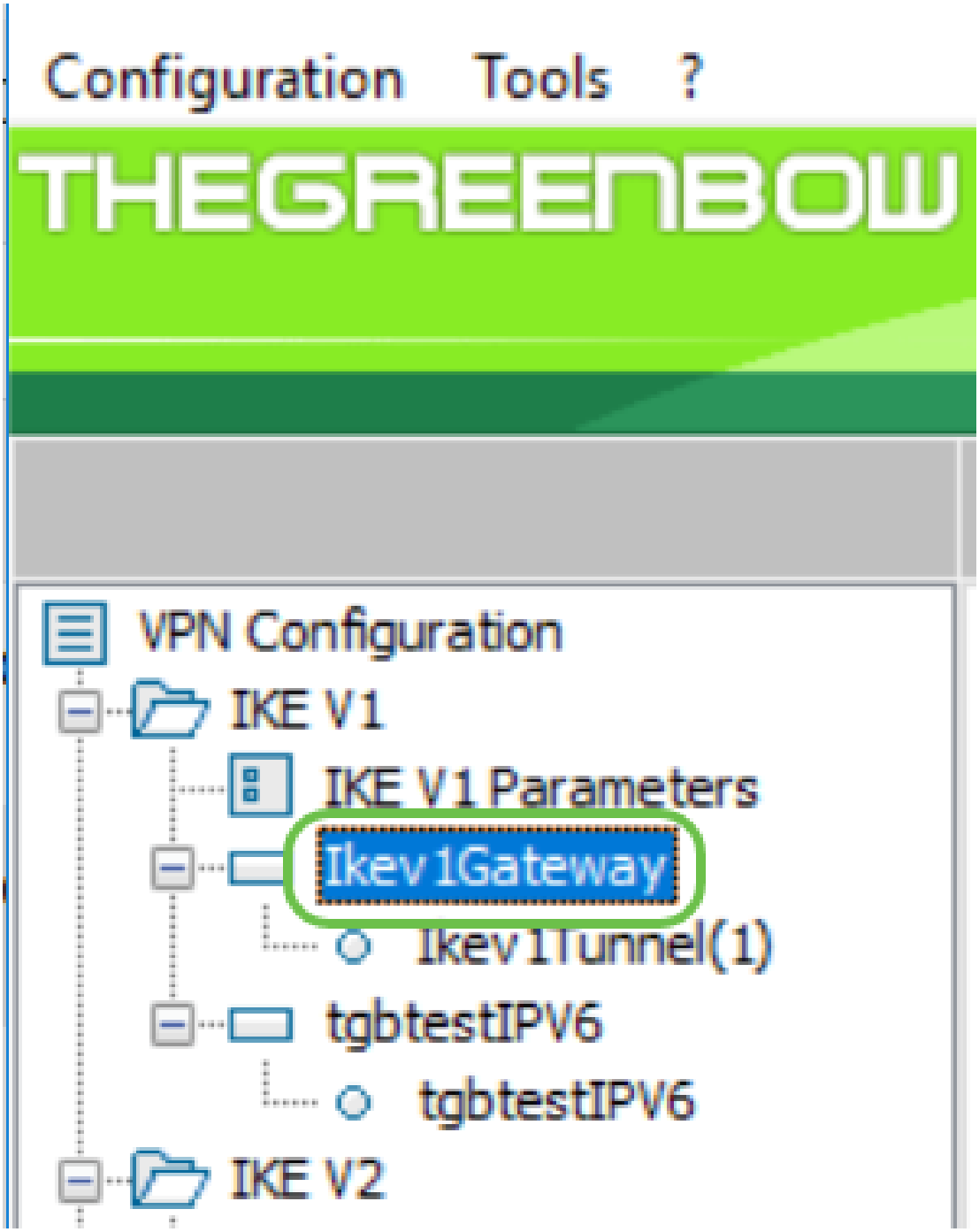
步骤5.单击“完**成**”。



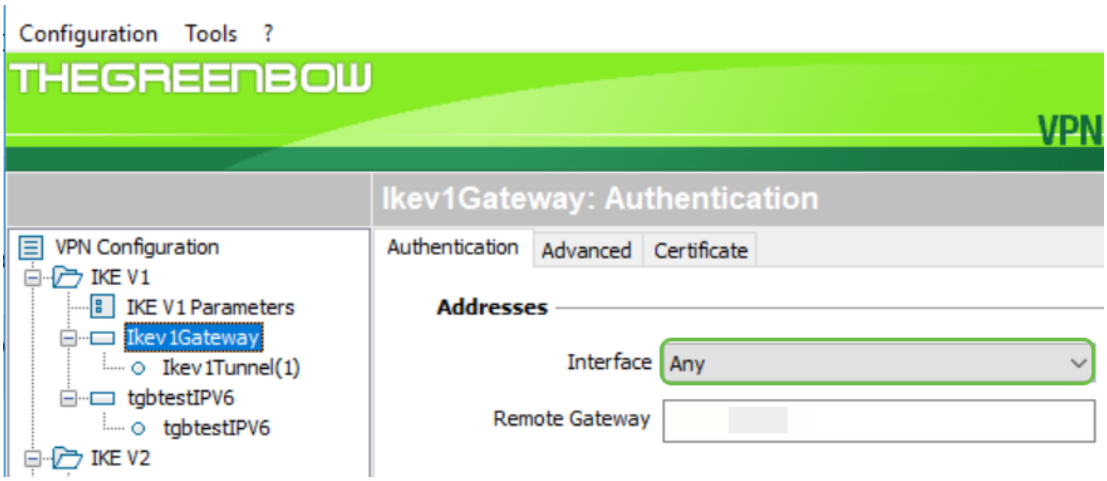
第6步（可选）您可以更改IKE V1参数。可以调整GreenBow Default、Minimal和Maximal寿命。在此位置，您可以输入路由器接受的生命期范围。



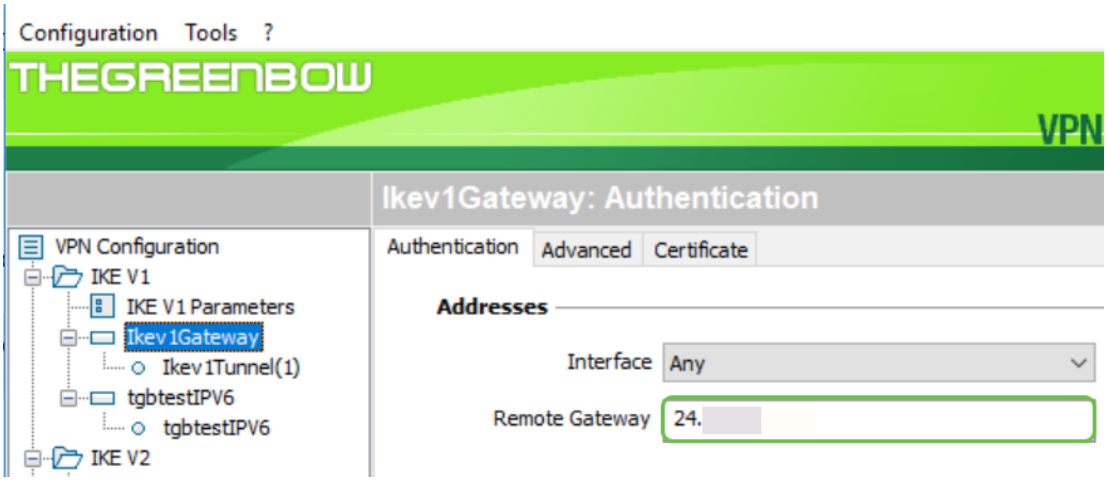
步骤7.点击您创建的网关。



步骤8.在*Addresses*下的Authentication*选项*卡中，您将看到本地地址的下拉列表。您可以选择一个或选**择任**意，如下所示。

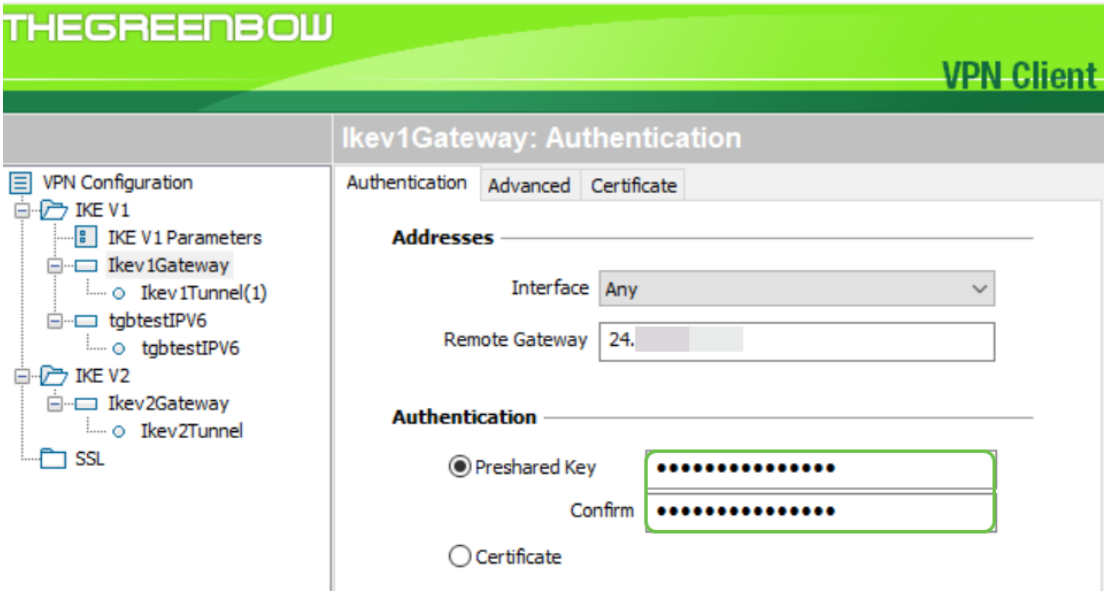


步骤9.在Remote Gateway（远程网关）字段中输入远程*网关的*地址。这可以是IP地址或DNS名称。这是站点（办公室）路由器的公有IP地址。



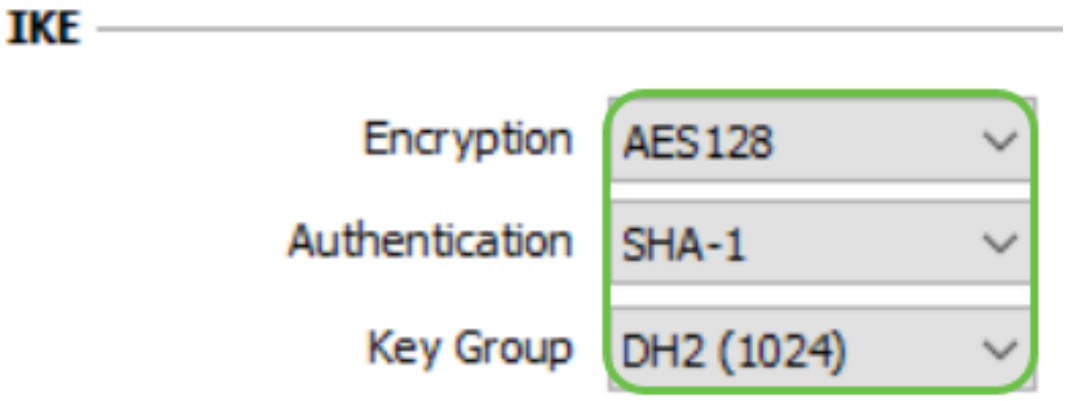
步骤10.在*Authentication*下，选择身份验证类型。选项有：

- 预共享密钥 — 此选项将允许用户使用已在VPN网关上配置的密码。用户必须匹配密码才能建立VPN隧道。
- Certificate — 此选项将使用证书完成VPN客户端和VPN网关之间的握手。

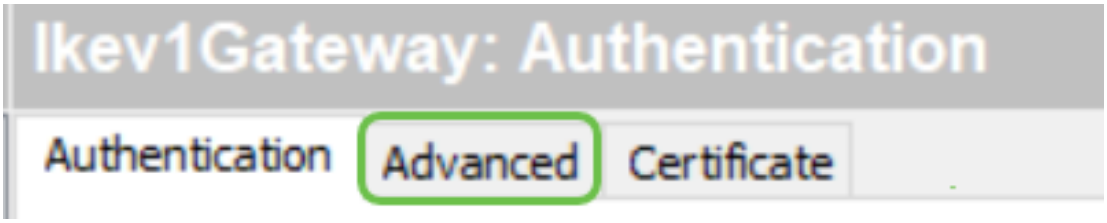


注意：在本例中，输入并确认了路由器上配置的预共享密钥。

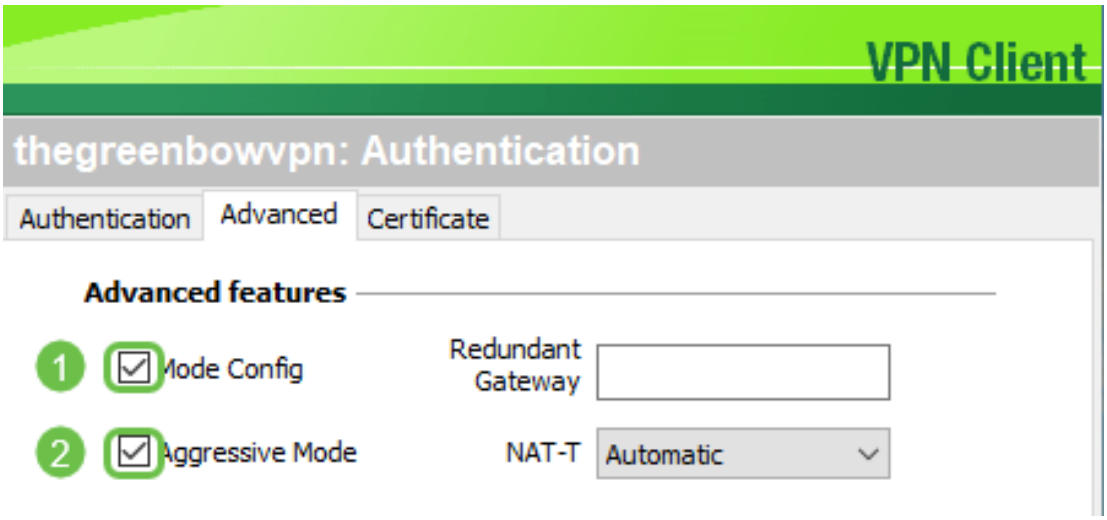
步骤11.在*IKE*下，设置Encryption、Authentication和Key Group设置以匹配路由器的配置。



步骤12.单击“高级”**选项**卡。

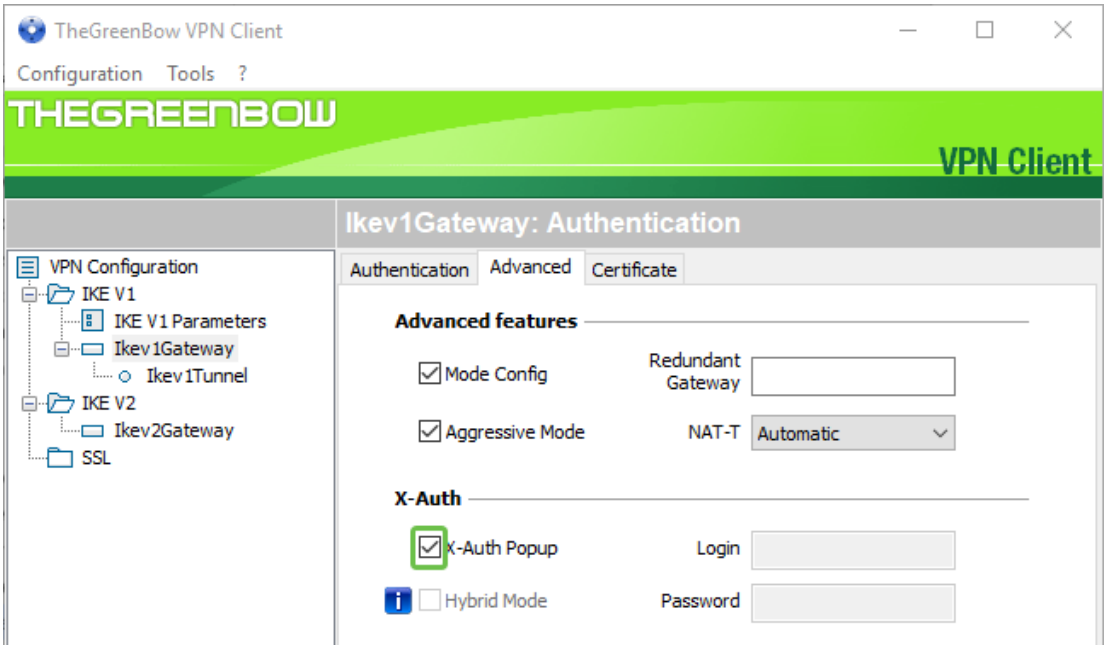


步骤13.在“高级功能”下，选中“模式**配置”**和“主**动模式**”复选框。在RV160上，在本示例的客户端到站点配置文件中选择了主动模式。将NAT-T设置保留为Automatic。

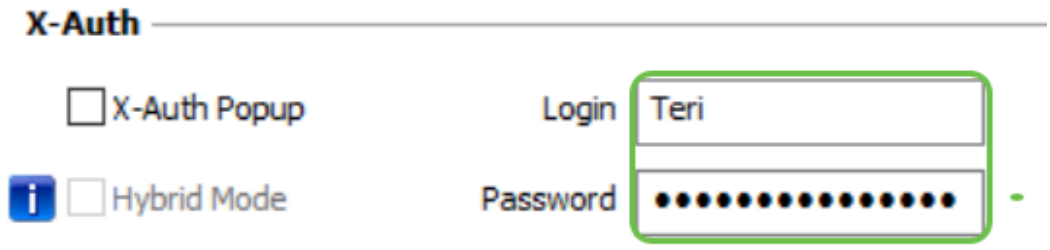


注意：启用模式配置后，GreenBow VPN客户端将从VPN网关提取设置以尝试建立隧道。NAT-T可加快连接建立。

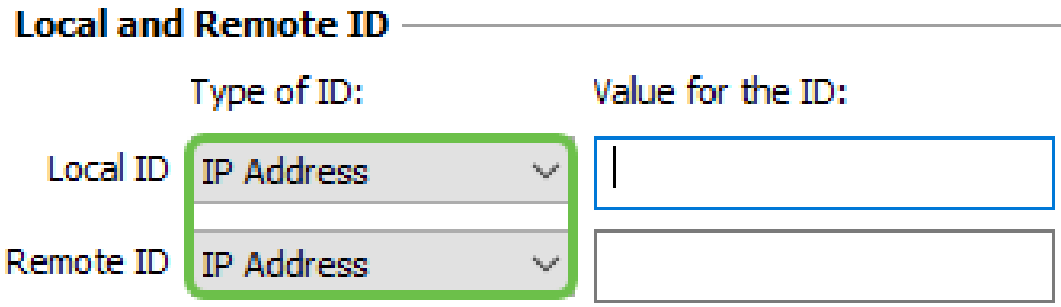
第14步。（可选）在*X-Auth*下，可以选中**X-Auth Popup复选框，以在启动连接时自动拉出登录窗口**。登录窗口是用户输入凭证以完成隧道的位置。



步骤15.（可选）如果未选择X-Auth弹出*窗口，请*在“登录”字段中输入*您的*用户名。这是在VPN网关和站点密码中创建用户帐户时输入的用户名。

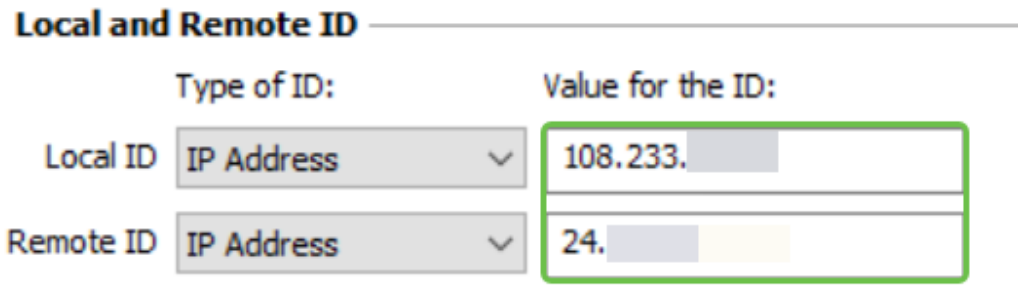


步骤16.在*Local ID和Remote ID*下，设置Local ID和Remote ID以匹配VPN网关的设置。

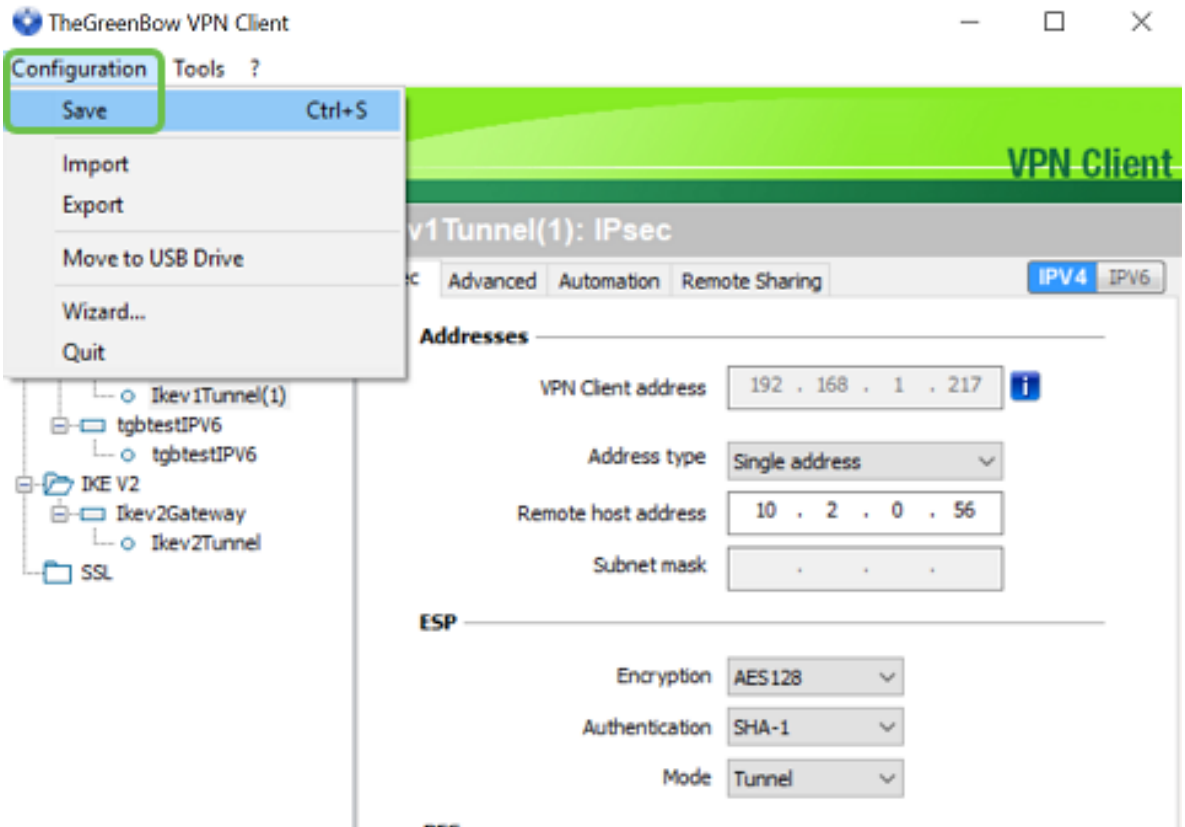


注意：在本例中，本地ID和远程ID均设置为IP地址，以匹配RV160或RV260 VPN网关的设置。

步骤17.在ID*的Value下*，在各自的字段中输入本地ID和远程ID。本地ID是客户端的WAN IP地址。通过搜索“我的IP是什么”可以找到此信息。远程ID是站点路由器的WAN IP地址。

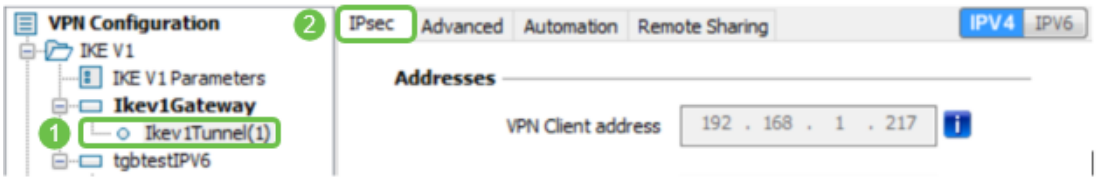


步骤18.单击“**配置**”并选择“**保存**”。

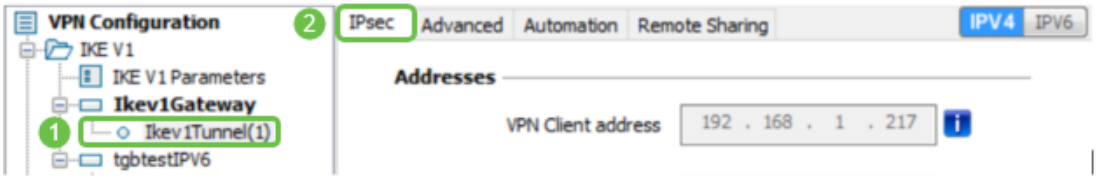


配置隧道设置

步骤1.单击IKev1Tunnel(**1)(您**的可能有其他名称)和IPsec**选项**卡。如果在Ikev1Gateway高级设置中选择了Mode Config，VPN Client地址将自动填充。这显示远程位置的计算机/笔记本电脑的本地IP地址。

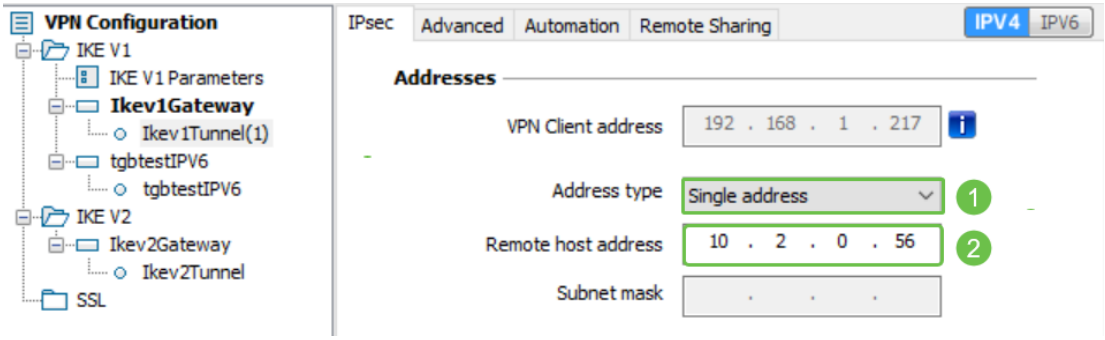


步骤2.从Address type下拉列表中选择VPN客户端可以访问*的地*址类型。这可以是单个地址、地址范围或子网地址。默认的子网地址自动包括VPN客户端地址（计算机的本地IP地址）、远程LAN地址和子网掩码。如果选择“单个地址”或“地址范围”，则需要手动填写这些字段。在“远程LAN地址”字段中输入VPN隧道应访问的网络地址，在“子网掩码”*字段中输入远程*网络的子网掩*码和子网*掩码。

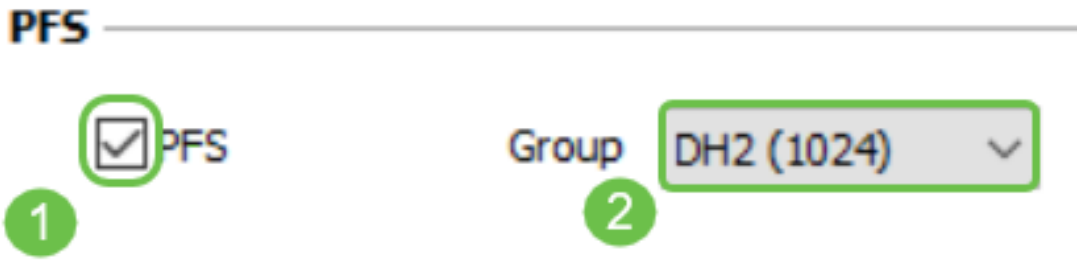


注意：在本例中，选择了单个地址，并输入了站点上路由器的本地IP地址。

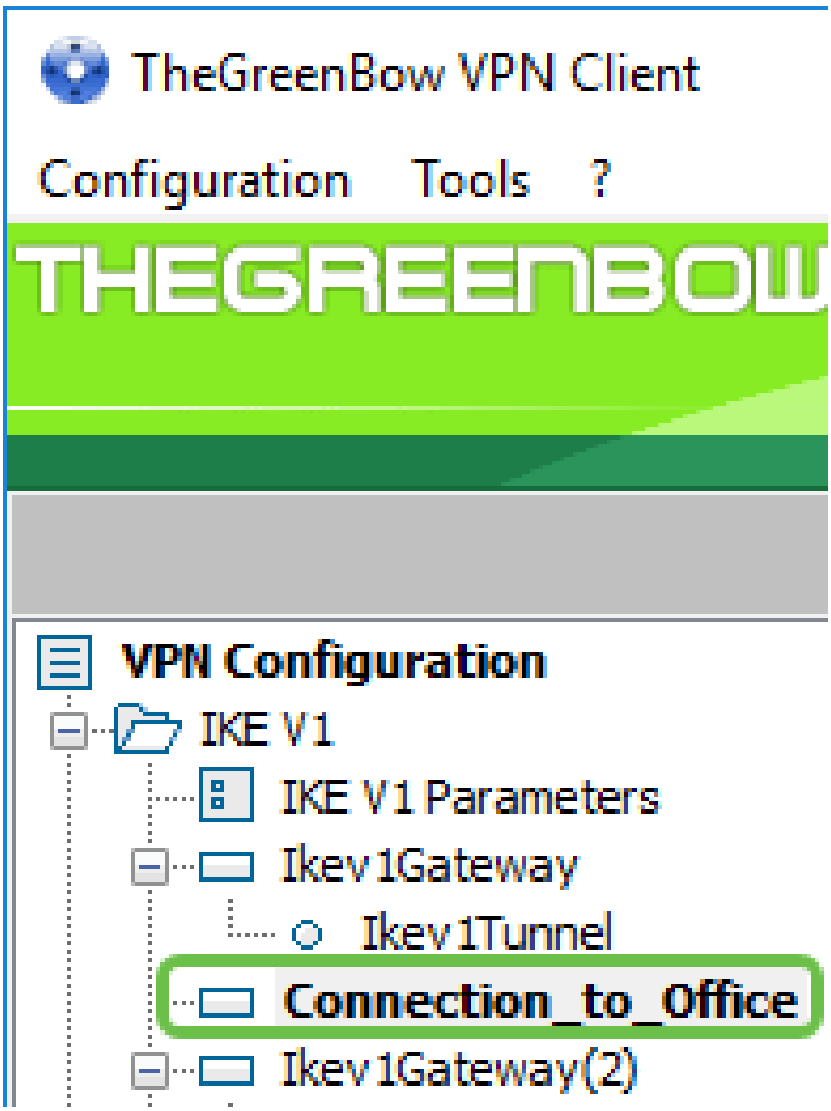
步骤3.在*ESP*下，设置Encryption、Authentication和Mode以匹配站点（办公室）的VPN网关设置。



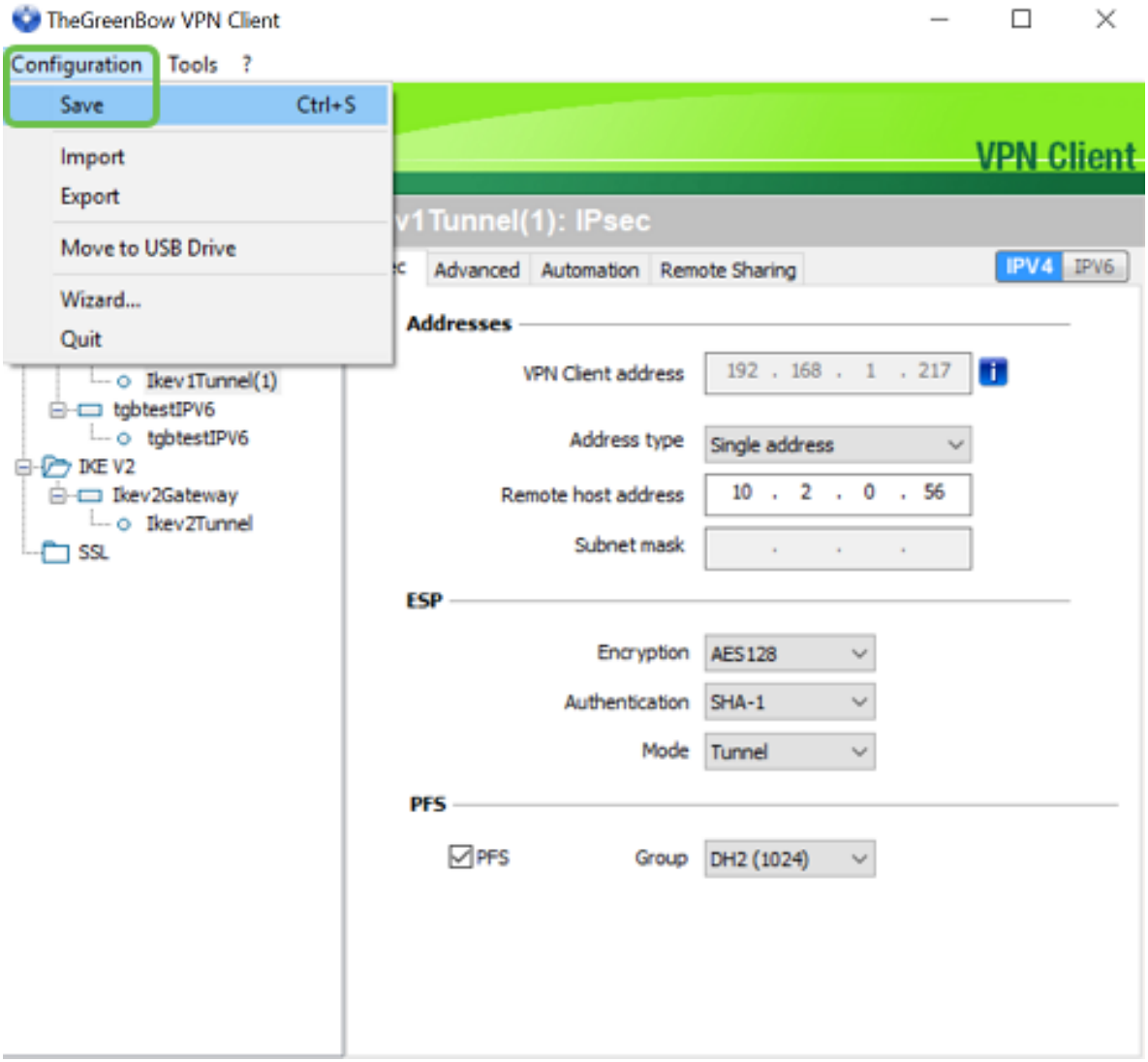
步骤4.（可选）在PFS下，选中**PFS** 复选框以启用完全向前保密(PFS)。PFS生成用于加密会话的随机密钥。从Group下拉列表中选择*PFS* 组设置。如果已在路由器上启用，也应在此处启用。



步骤5.（可选）右键单击Ikev1Gateway的名称，如果要重命名，请点击重命名部分。



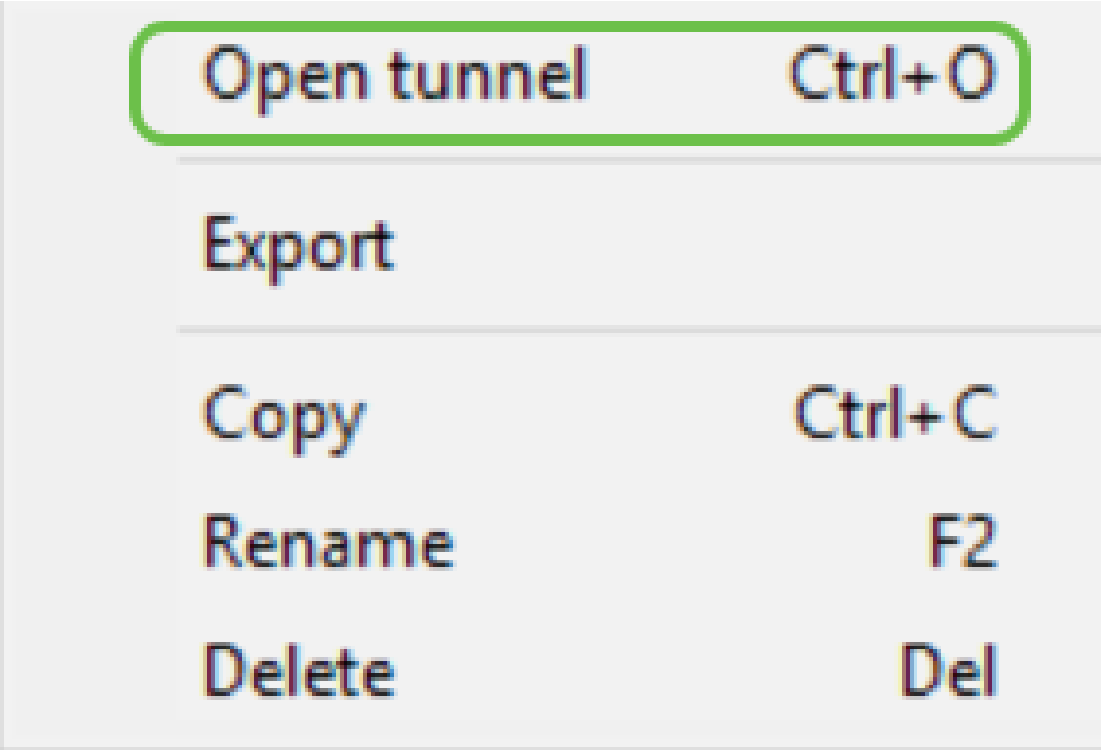
步骤6.单击“配置”并选择“保存”。



您现在应该已成功配置TheGreenBow VPN客户端，以通过VPN连接到RV160或RV260路由器。

作为客户端启动VPN连接

步骤1.由于GreenBow已打开，因此可以右键单击隧道并选择“打开**隧道”以开始连接**。

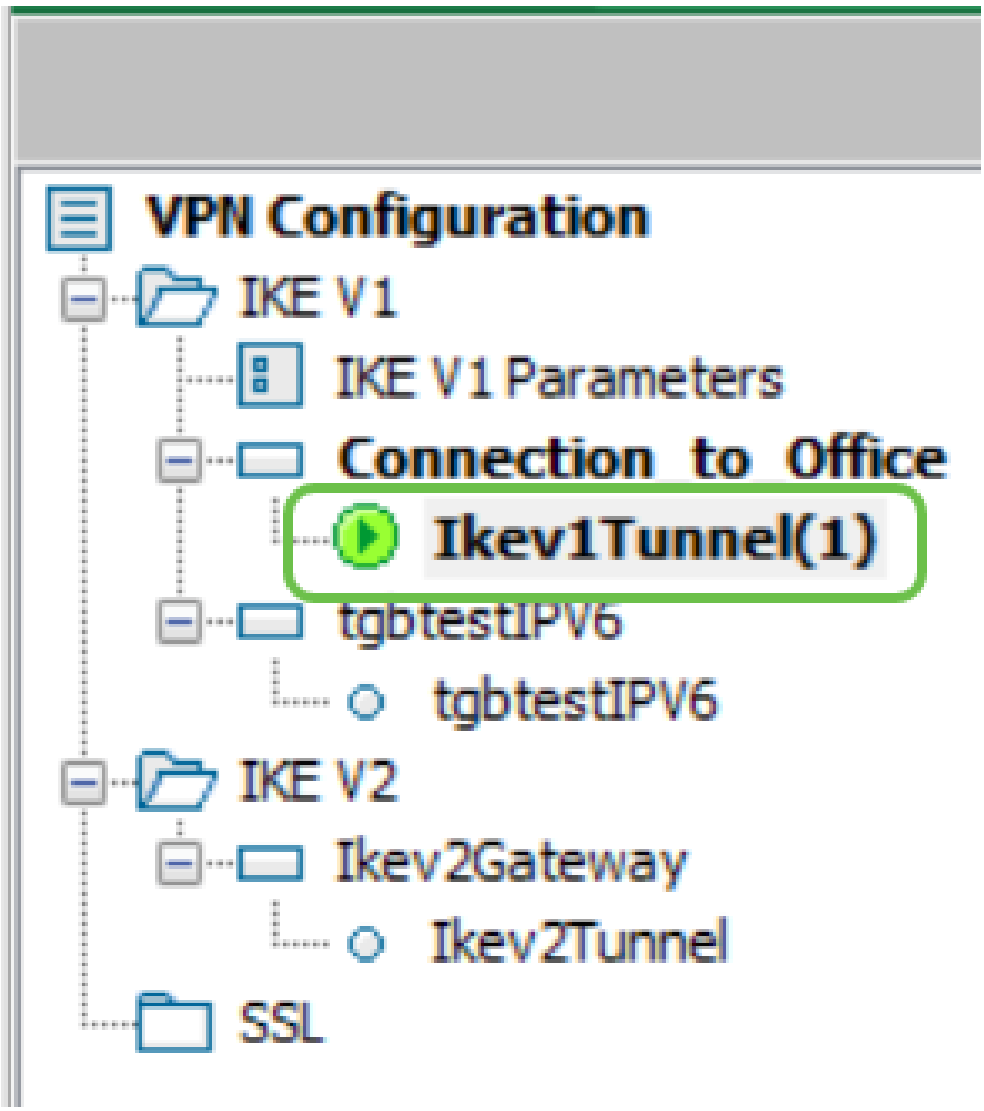


注意：您也可以双击隧道来打开隧道。

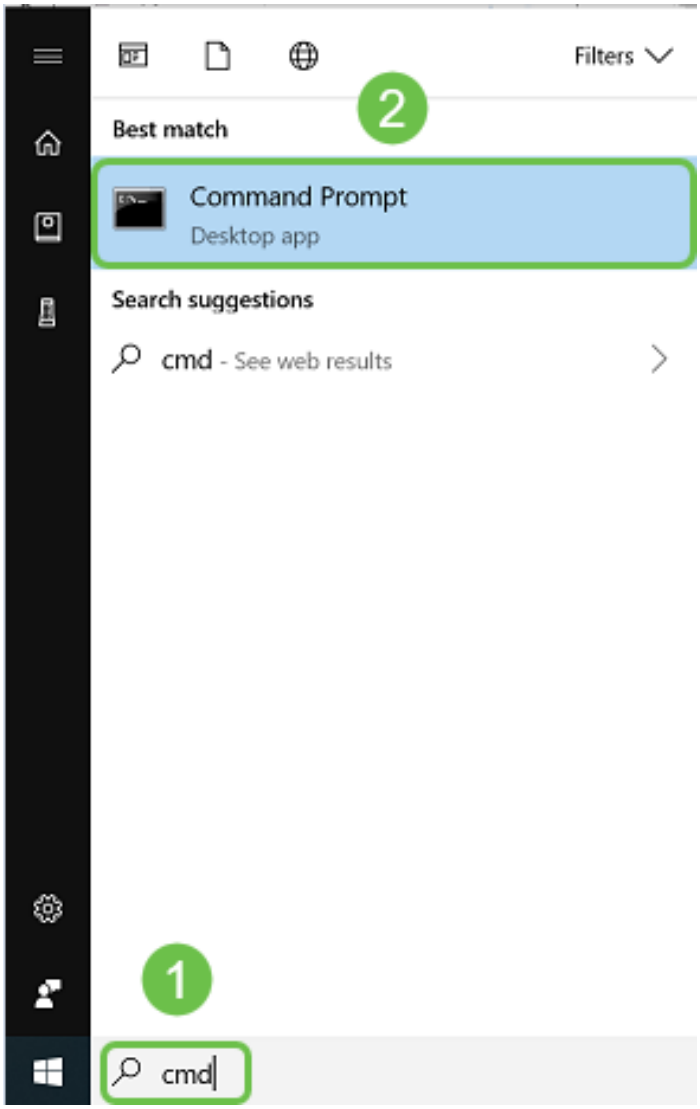
步骤2.（可选）如果您正在开始新会话并已关闭TheGreenBow，请单击屏幕右侧的**TheGreenBow VPN Client**图标。

步骤3.（可选）只有在设置新会话并遵循步骤2时，才需要执行此步骤。选择需要使用的VPN连接，然后单击“打**开**”。VPN连接应自动启动。

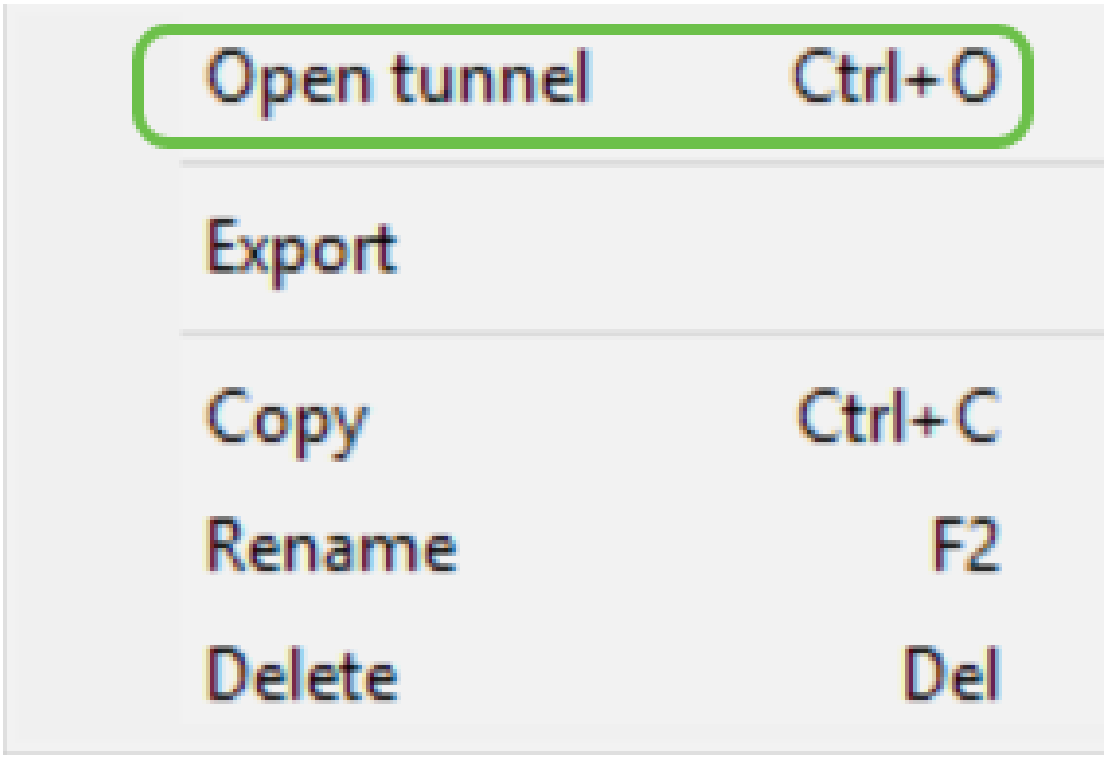
步骤4.当隧道连接时，隧道旁会显示一个绿色圆圈。如果您看到感叹号，可以单击它查找错误。



步骤5.（可选）要验证您已连接，请从客户端计算机访问命令提示符。



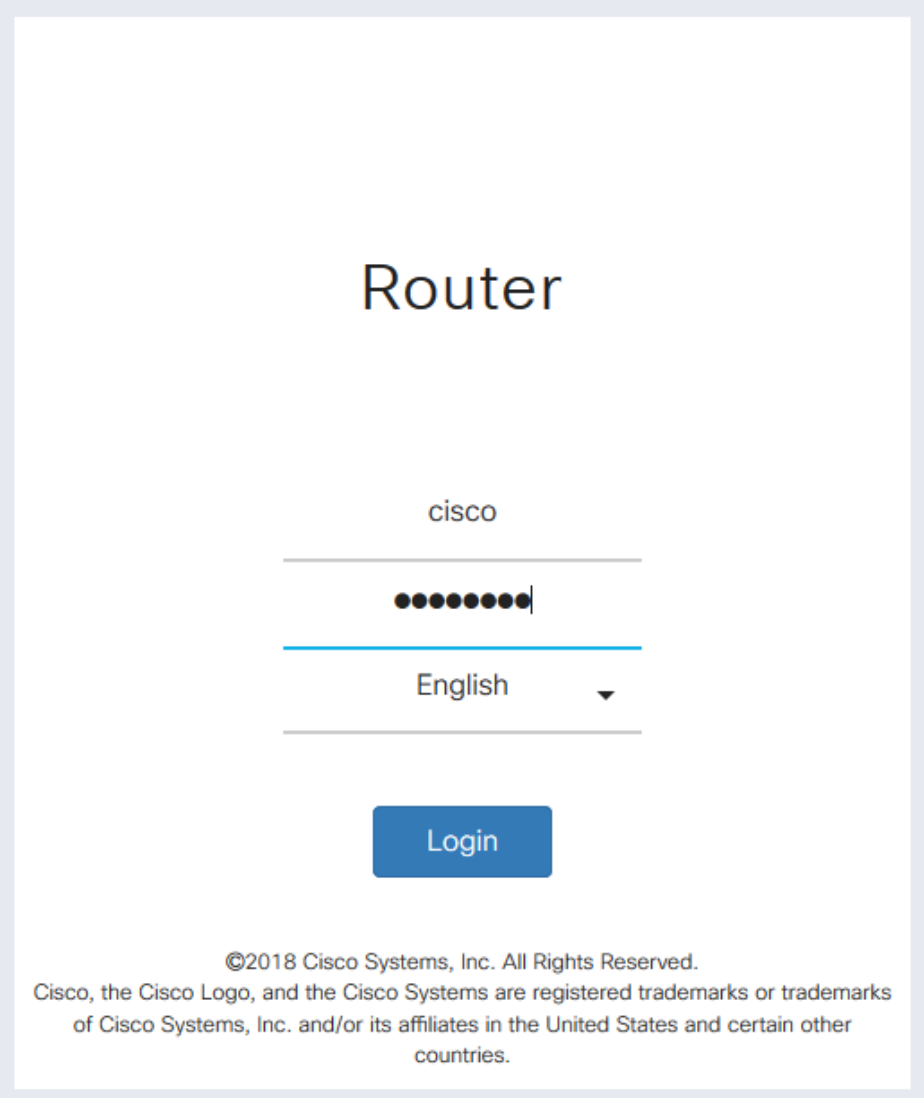
步骤6.（可选）输入ping，然后输入站点路由器的专用LAN IP地址。如果收到回复，则表明您已连接。



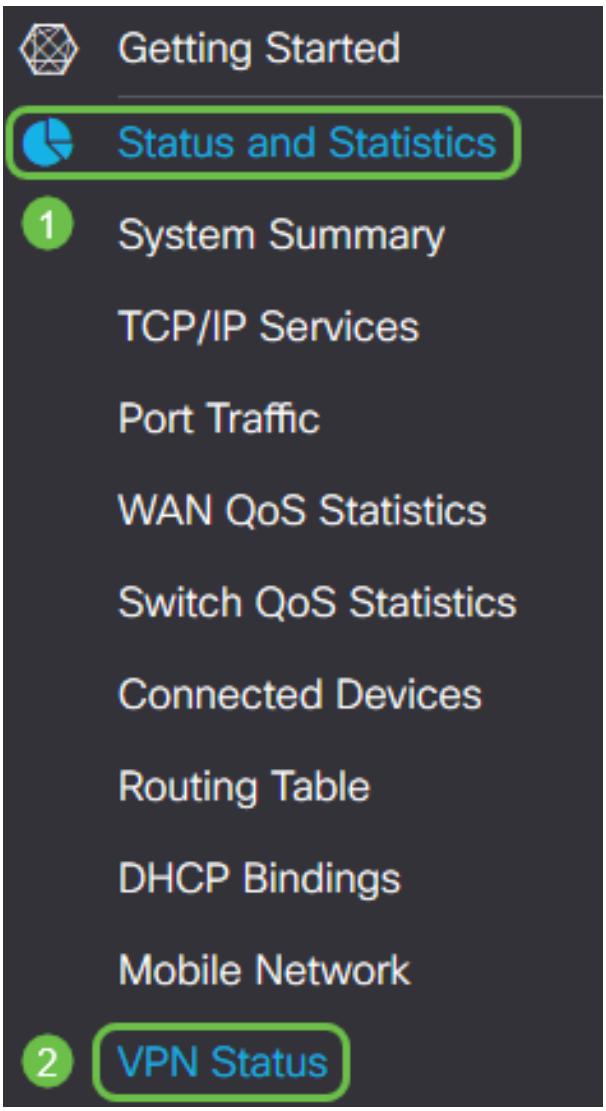
验证VPN状态

验证站点上的VPN状态

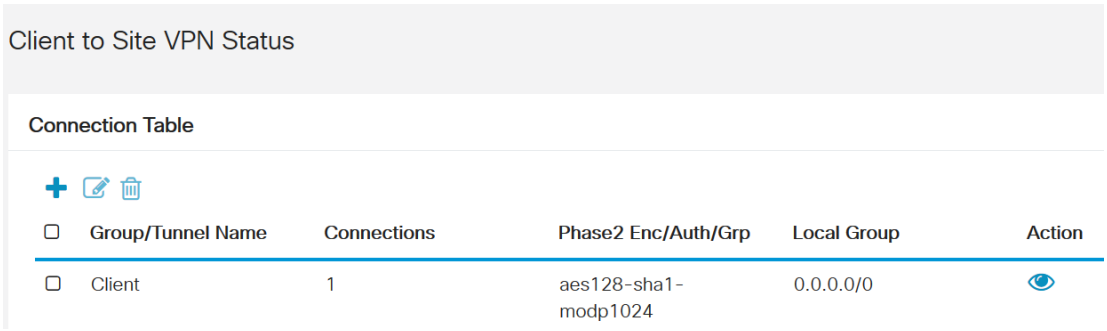
步骤1.登录RV160或RV260的VPN网关的基于Web的实用程序。



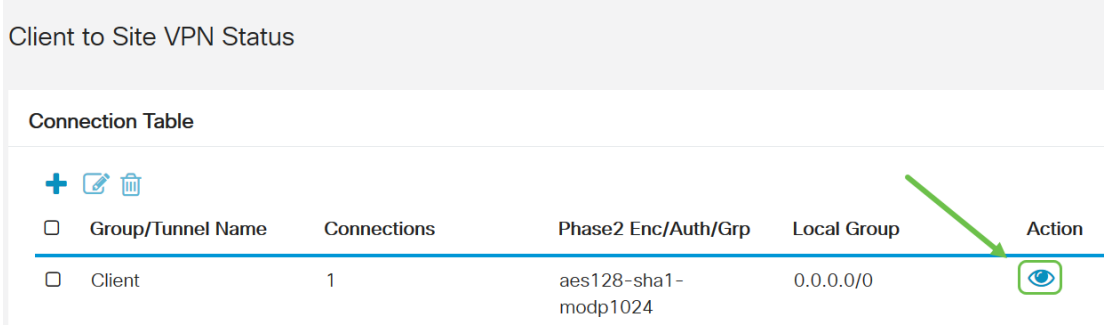
步骤2.选择Status **and Statistics >** VPN Status。



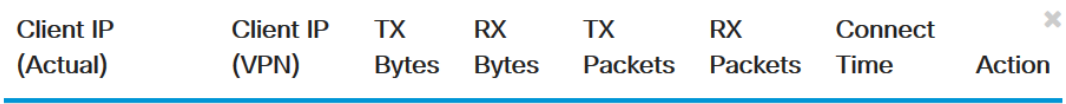
步骤3.在“*客户端到站点隧道状态*”下，选中“*连接表*”*的*“*连接*”*列*。您应该看到VPN连接已确认。



步骤4.单击眼睛图**标查**看更多详细信息。



步骤5.客户端到站点VPN状态的详细信息如下所示。您会注意到客户端的WAN IP地址，即从设置时配置的地址池分配的本地IP地址。它还显示发送和接收的字节和数据包以及连接时间。如果要断开客户端连接，请单击“操作”下**的蓝色**断链*图标*。单击右上**角**的x在检查后关闭。



结论

现在，您应该已成功在RV160或RV260路由器上设置并验证VPN连接，并且已将GreenBow VPN客户端配置为通过VPN连接到路由器。