

使用GreenBow VPN客户端连接RV34x系列路由器

特别通知：许可结构 — 固件版本1.0.3.15及更高版本。今后，AnyConnect将仅对客户端许可证收取费用。

有关RV340系列路由器上AnyConnect许可的其他信息，请参阅[RV340系列路由器的AnyConnect许可文章](#)。

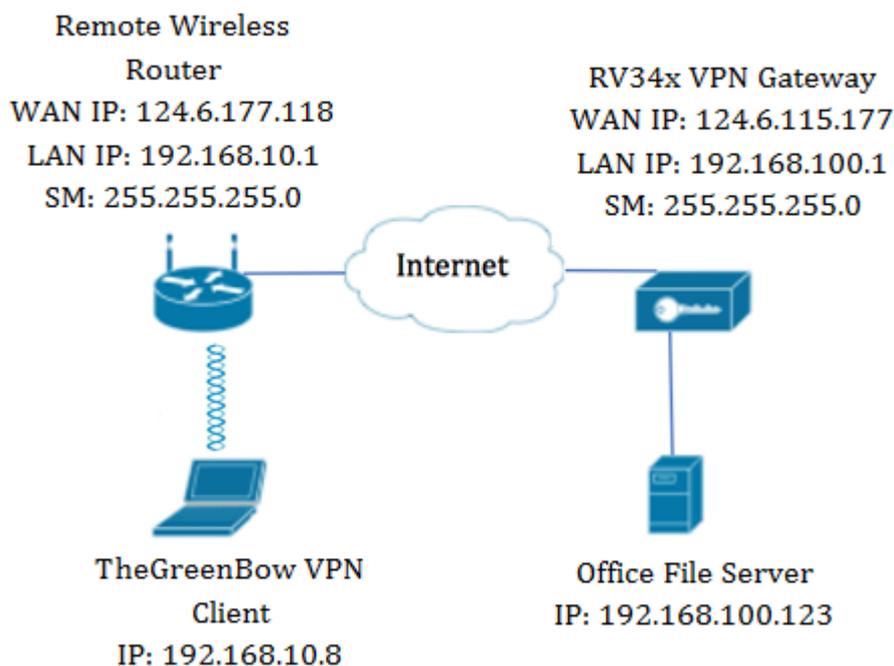
简介

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。公司办公室大多使用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是必要的。

VPN允许远程主机像位于同一本地网络一样工作。该路由器最多支持50个隧道。在路由器配置了Internet连接后，可以在路由器和终端之间设置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。

GreenBow VPN客户端是第三方VPN客户端应用，使主机设备能够通过RV34x系列路由器为站点到站点IPSec隧道配置安全连接。



在图中，计算机将连接到其网络外部办公室中的文件服务器以访问其资源。为此，计算机中的TheGreenBow VPN Client将以从RV34x VPN网关提取设置的方式进行配置。

使用VPN连接的优势

1. 使用VPN连接有助于保护机密网络数据和资源。
2. 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，而无需在现场，同时仍能维护专用网络及其资源的安全。
3. 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。当今先进的技术使这成为可能，从而保护专用网络免受未经授权的访问。
4. 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）。
5. 将新用户或用户组添加到网络很容易，因为VPN易于扩展。无需额外的组件或复杂的配置，即可实现网络扩展。

使用VPN连接的风险

1. 配置错误导致的安全风险。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。
2. 可靠性。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。
3. 可扩展性。如果遇到需要添加新基础设施或新配置集的情况，则可能会出现技术问题，因为不兼容，尤其是当您使用的产品或供应商以外的其他产品或供应商时。
4. 移动设备的安全问题。当在移动设备上启动VPN连接时，安全问题可能出现，特别是当移动设备无线连接到本地网络时。
5. 连接速度慢。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。

使用GreenBow VPN客户端的必备条件

必须先要在VPN路由器上配置以下项，并通过单击[此处](#)建立连接来应用到GreenBow VPN客户端。

1. [在VPN网关上创建客户端到站点配置文件](#)
2. [在VPN网关上创建用户组](#)
3. [在VPN网关上创建用户帐户](#)
4. [在VPN网关上创建IPSec配置文件](#)
5. [在VPN网关上配置I阶段和II阶段设置](#)

适用设备

- RV34x系列

软件版本

- 1.0.01.17

使用GreenBow VPN客户端

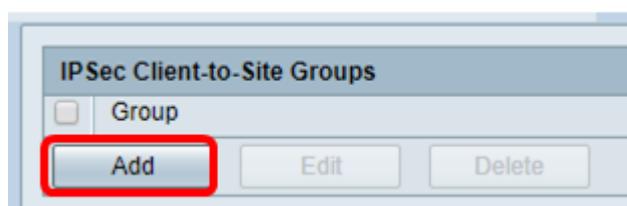
[在路由器上创建客户端到站点配置文件](#)

步骤1.登录到RV34x路由器的基于Web的实用程序，然后选择VPN > Client-to-Site。



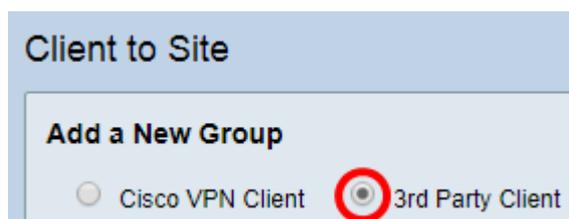
注意：本文中的图像是从RV340路由器拍摄的。选项可能因设备型号而异。

步骤2.单击“添加”。



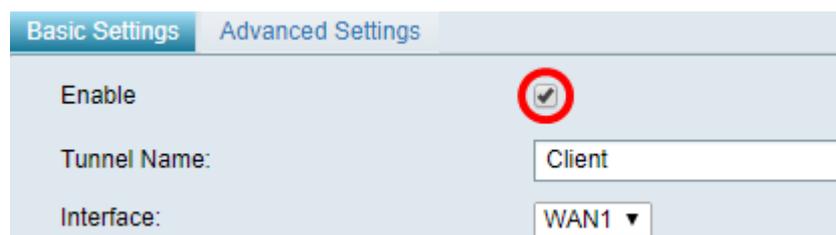
步骤3.单击第3方客户端。

注意：AnyConnect是Cisco VPN客户端的示例，而GreenBow VPN客户端是第三方VPN客户端的示例。



注意：在本例中，选择第3方客户端。

步骤4.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。



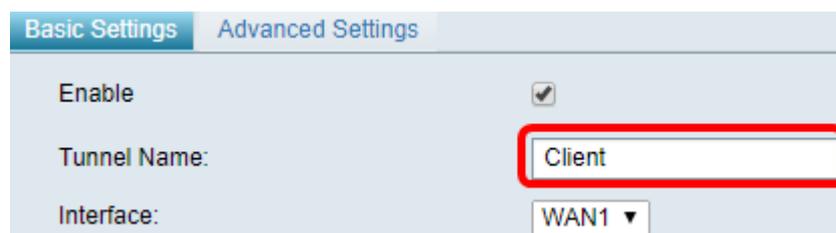
Basic Settings | Advanced Settings

Enable

Tunnel Name: Client

Interface: WAN1 ▼

步骤5.在Tunnel Name字段中输入VPN连接的名称。



Basic Settings | Advanced Settings

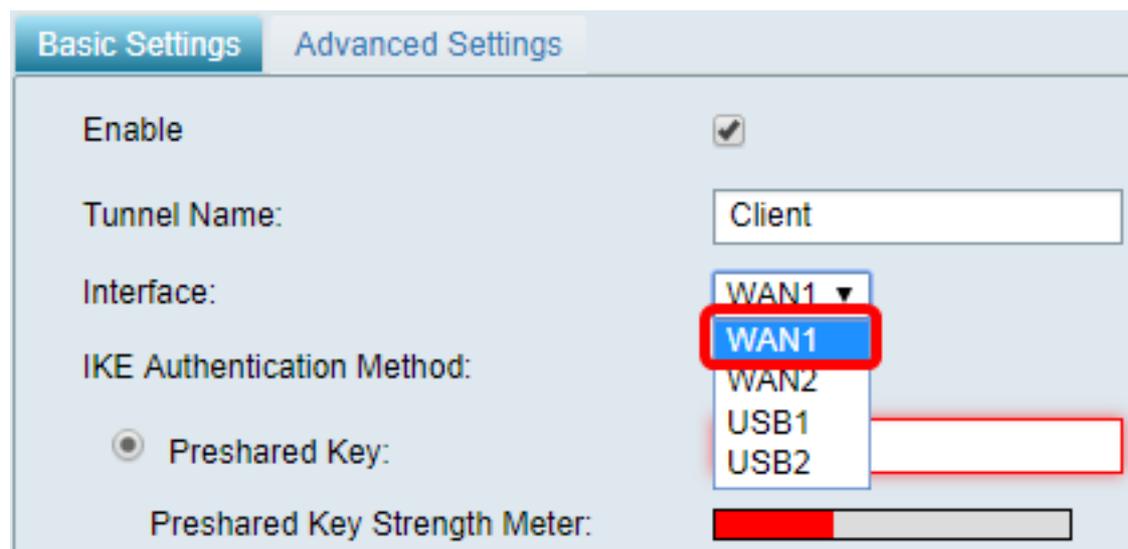
Enable

Tunnel Name: Client

Interface: WAN1 ▼

注意：在本例中，输入Client。

步骤6.从Interface下拉列表中选择要使用的接口。WAN1、WAN2、USB1和USB2将使用路由器上的相应接口进行VPN连接。



Basic Settings | Advanced Settings

Enable

Tunnel Name: Client

Interface: WAN1 ▼

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

注意：这些选项取决于您使用的路由器型号。在本例中，选择WAN1。

步骤7.选择IKE身份验证方法。选项有：

- 预共享密钥 — 此选项将允许我们使用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。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

Certificate:

注意：在本例中，选择预共享密钥。

步骤8.在Preshared Key字段中输入连接密码。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

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

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

注意：在本例中，“最低预共享密钥复杂性”(Minimum Preshared Key Complexity)处于启用状态。

步骤10.（可选）选中Show plain text when edit **Enable**复选框以以纯文本形式显示口令。

IKE Authentication Method:

Preshared Key:

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Show plain text when edit: Enable

注意：在本例中，当编辑处于禁用状态时显示纯文本。

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。
- 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。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

FQDN

User FQDN

注意：在本例中，选择本地WAN IP。使用此选项，会自动检测本地WAN IP。

步骤12. (可选) 为远程主机选择标识符。选项有：

- IP地址(IP Address) — 此选项使用VPN客户端的WAN IP地址。
- FQDN — 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。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

FQDN

User FQDN

注意：在本例中，选择IP地址。

步骤13.在Remote Identifier字段中输入远程标识符。

Local Identifier: Local WAN IP 124.6.115.177

Remote Identifier: IP Address 124.6.177.118

注意：在本例中，输入124.6.115.177。

步骤14. (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。

Extended Authentication:

Group Name

Add Delete

注意：在本例中，未选中扩展身份验证。

步骤15.在“组名”下，单击“添加”。

Extended Authentication:

Group Name

步骤16.从Group Name下拉列表中选择将使用扩展身份验证的组。

Group Name

admin

admin

guest

IPSecVPN

VPN

注意：在本例中，选择VPN。

步骤17.在Pool Range for Client LAN下，在Start IP（开始IP）字段中输入可分配给VPN客户端的第一个IP地址。

Pool Range for Client LAN:

Start IP:

End IP:

注意：在本例中，输入10.10.100.100。

步骤18.在End IP（结束IP）字段中输入可分配给VPN客户端的最后一个IP地址。

Pool Range for Client LAN:

Start IP:

End IP:

注意：在本例中，输入10.10.100.245。

步骤19.单击“应用”。

Pool Range for Client LAN:

Start IP:

End IP:

步骤20.单击“保存”。

cisco (admin) Log Out About Help

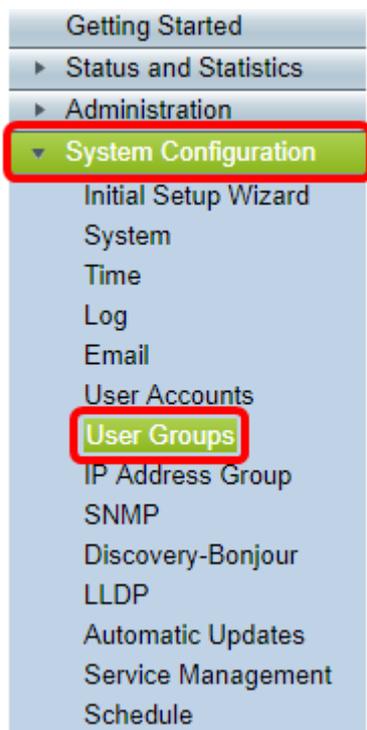
现在，您应该已在路由器上为GreenBow VPN客户端配置了客户端到站点配置文件。

创建用户组

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 Groups

。

注意：本文中的映像来自RV340路由器。选项可能因设备型号而异。



步骤2.单击Add添加用户组。



步骤3.在“概述”区域的“组名”字段中输入组名。

User Groups

Overview

Group Name:

Local User Membership List

#	Join	User Name	Joined Groups *
1	<input checked="" type="checkbox"/>	CiscoTest	VPN
2	<input type="checkbox"/>	cisco	admin
3	<input type="checkbox"/>	guest	guest
4	<input checked="" type="checkbox"/>	vpnuser	VPN

* Should have at least one account in the "admin" group

注意：在本例中，使用VPN。

步骤4.在Local Membership List下，选中需要处于同一组中的用户名的复选框。

User Groups

Overview

Group Name:

Local User Membership List

#	Join	User Name	Joined Groups *
1	<input checked="" type="checkbox"/>	CiscoTest	VPN
2	<input type="checkbox"/>	cisco	admin
3	<input type="checkbox"/>	guest	guest
4	<input checked="" type="checkbox"/>	vpnuser	VPN

* Should have at least one account in the "admin" group

注意：在本例中，选择CiscoTest和vpnuser。

步骤5.在“服务”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。
- 管理员 — 此选项为组成员提供读和写权限，并能够配置系统状态。

Services

Web Login Disabled Read Only Administrator

注意：在本例中，选择只读。

步骤6.在EzVPN/第3方配置文件成员使用中表中，单击Add。

EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table	
#	Group Name

步骤7.从Select a Profile下拉列表中选择配置文件。选项可能因VPN网关上配置的配置文件而异。

Add Feature List

Select a Profile:

注意：在本例中，选择Clients。

步骤8.单击“添加”。

Add Feature List

Select a Profile:

步骤9.单击“应用”。

SSL VPN

PPTP VPN Permit

L2TP Permit

802.1x Permit

步骤10.单击“保存”。

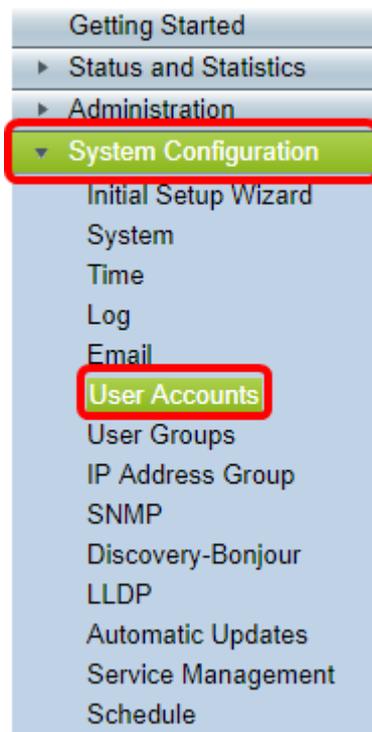


您现在应该已在RV34x系列路由器上成功创建了用户组。

[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**。

注意：本文中的图像是从RV340路由器拍摄的。选项可能因设备型号而异。



步骤2. 在Local User Membership List区域，单击**Add**。

User Accounts

Local Users Password Complexity

Password Complexity Settings: Enable

Local Users

Local User Membership List			
<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	guest	VPN
<input type="checkbox"/>	2	cisco	admin

* Should have at least one account in the "admin" group

步骤3.在User Name字段中输入用户的名称。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group ▼

注意：在本例中，输入CiscoTest。

步骤4.在New Password字段中输入用户密码。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

步骤5.在New Password Confirm框中确认密码。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

步骤6.从Group下拉列表中选择组。这是用户将与之关联的组。

Group

注意：在本例中，选择VPN。

步骤7.单击“应用”。

User Accounts

Add User Account

User Name

New Password

New Password Confirm

Group

步骤8.单击“保存”。



您现在应该已在RV34x系列路由器上创建用户帐户。

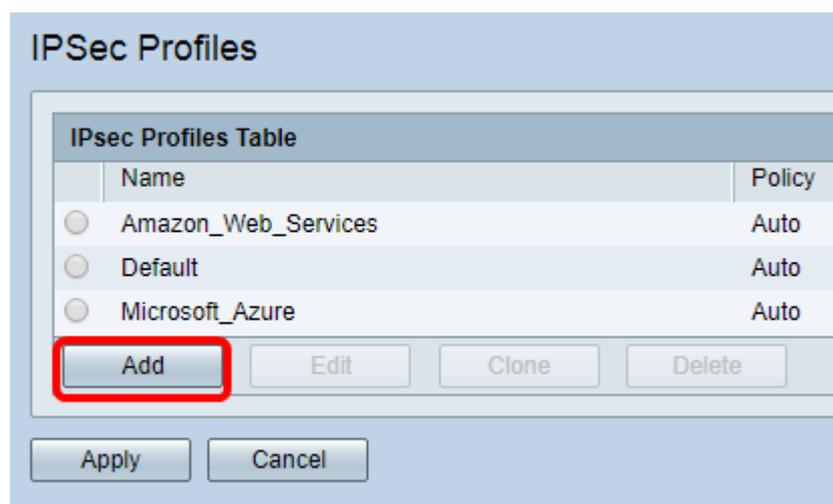
[配置IPSec配置文件](#)

步骤1.登录到RV34x路由器的基于Web的实用程序，然后选择VPN > IPSec Profiles(VPN > IPSec Profiles)。



注意：本文中的图像是从RV340路由器拍摄的。选项可能因设备型号而异。

步骤2. IPSec配置文件表显示现有配置文件。单击**Add**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(_)。

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode: Auto Manual

注意：在本例中，输入Client。

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。如果选择此选项，请跳至[配置自动设置](#)。
- 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。如果选择此选项，请跳至[配置手动设置](#)。

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode: Auto Manual

注意：在本例中，选择了Auto。

[配置第I阶段和第II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适当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。

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

注意：在本例中，选择组5-1536位。

步骤2.从Encryption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Internet安全关联和密钥管理协议(ISAKMP)。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。

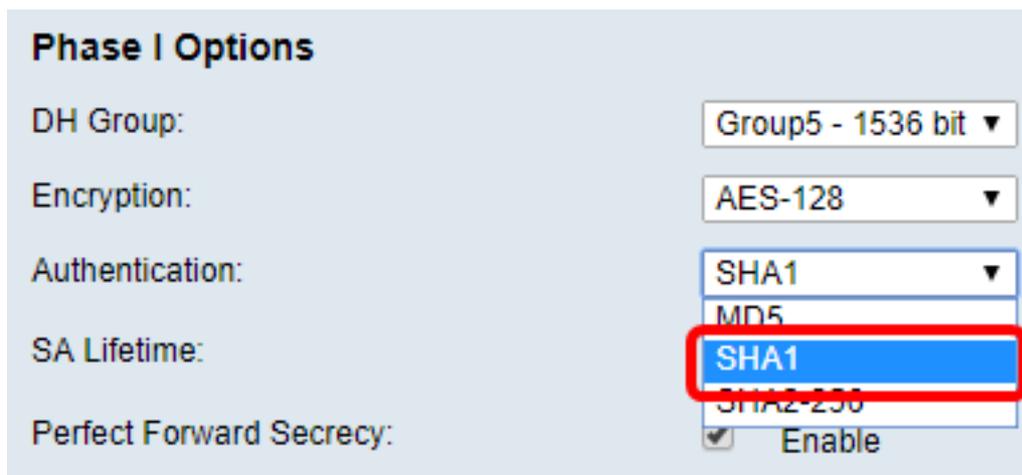


The screenshot shows the 'Phase I Options' configuration window. The 'DH Group' is set to 'Group5 - 1536 bit'. The 'Encryption' dropdown menu is open, showing options: AES-128, 3DES, AES-128 (highlighted with a red box), AES-192, and AES-256. The 'Authentication' field is empty. The 'SA Lifetime' field is empty. The 'Perfect Forward Secrecy' checkbox is checked and labeled 'Enable'.

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。在本例中，选择AES-128。

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。



The screenshot shows the 'Phase I Options' configuration window. The 'DH Group' is set to 'Group5 - 1536 bit'. The 'Encryption' dropdown menu is set to 'AES-128'. The 'Authentication' dropdown menu is open, showing options: SHA1 (highlighted with a red box), MD5, and SHA2-256. The 'SA Lifetime' field is empty. The 'Perfect Forward Secrecy' checkbox is checked and labeled 'Enable'.

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。这是Internet密钥交换(IKE)安全关联(SA)在此阶段将保持活动状态的时间长度。默认值为 28800。



Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

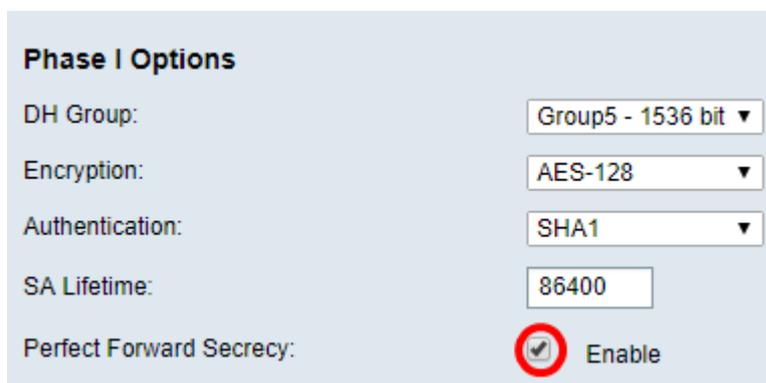
Authentication: SHA1 ▼

SA Lifetime: 86400

Perfect Forward Secrecy: Enable

注意：在本例中，输入86400。

步骤5. (可选) 选中Enable **Perfect Forward Secrecy**复选框以生成用于IPSec流量加密和身份验证的新密钥。



Phase I Options

DH Group: Group5 - 1536 bit ▼

Encryption: AES-128 ▼

Authentication: SHA1 ▼

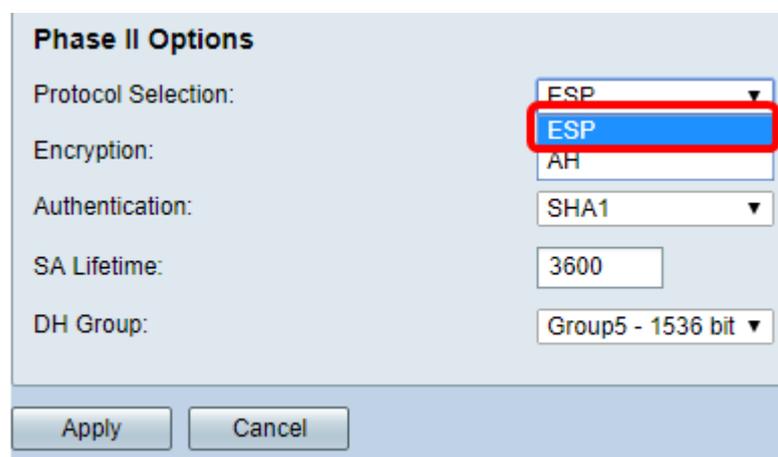
SA Lifetime: 86400

Perfect Forward Secrecy: Enable

注意：在本例中，启用完全向前保密。

步骤6.从Phase II Options区域的Protocol Selection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 — 此选项封装要保护的数据。如果选择此选项，请继续[步骤7](#)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8](#)。



Phase II Options

Protocol Selection: ESP ▼

Encryption: ESP ▼

Authentication: SHA1 ▼

SA Lifetime: 3600

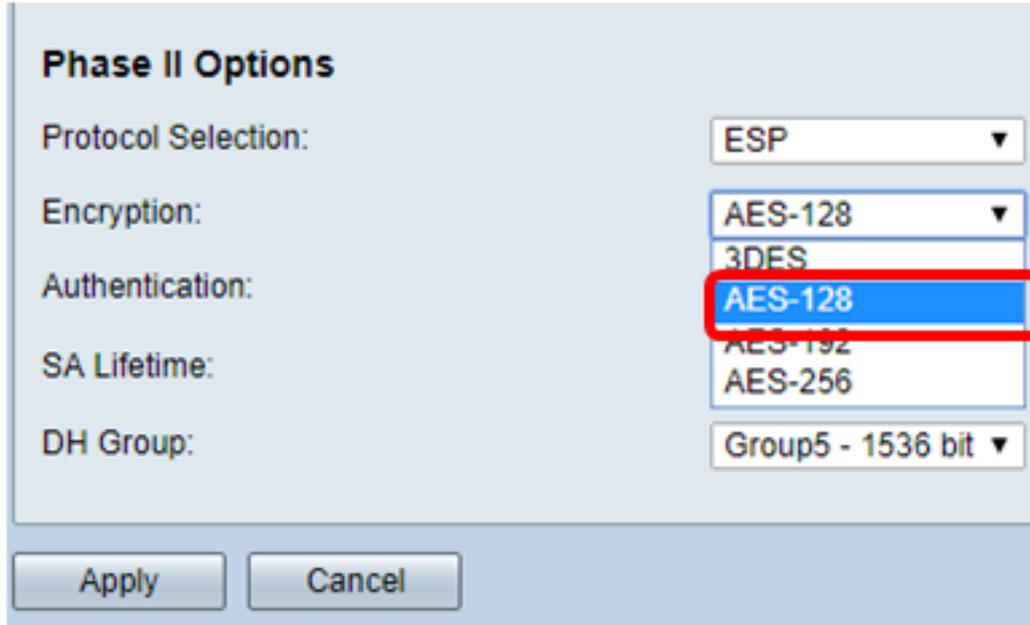
DH Group: Group5 - 1536 bit ▼

Apply Cancel

注意：在本例中，选择ESP。

步骤7.如果在步骤6中选择了ESP，请选择确定如何对ESP和ISAKMP进行身份验证的身份验证方法。选项有：

- 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。

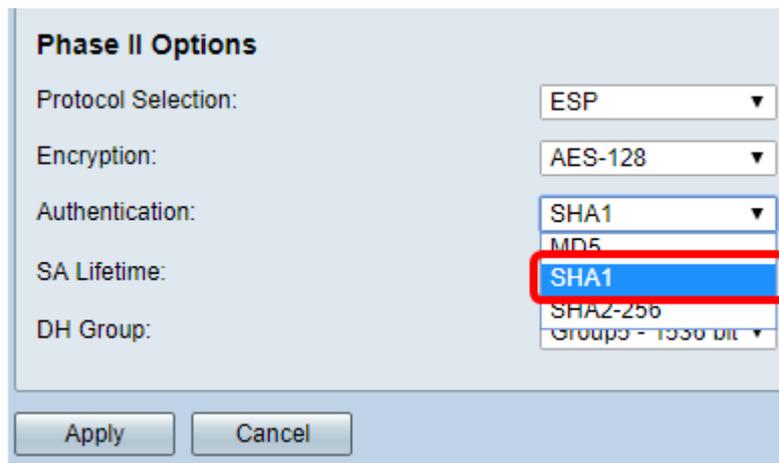


The screenshot shows the 'Phase II Options' dialog box. The 'Protocol Selection' dropdown is set to 'ESP'. The 'Encryption' dropdown is set to 'AES-128'. The 'Authentication' dropdown is open, showing options: '3DES', 'AES-128' (highlighted with a red box), 'AES-192', and 'AES-256'. The 'SA Lifetime' field is empty. The 'DH Group' dropdown is set to 'Group5 - 1536 bit'. At the bottom, there are 'Apply' and 'Cancel' buttons.

注意：在本例中，选择AES-128。

步骤8.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。



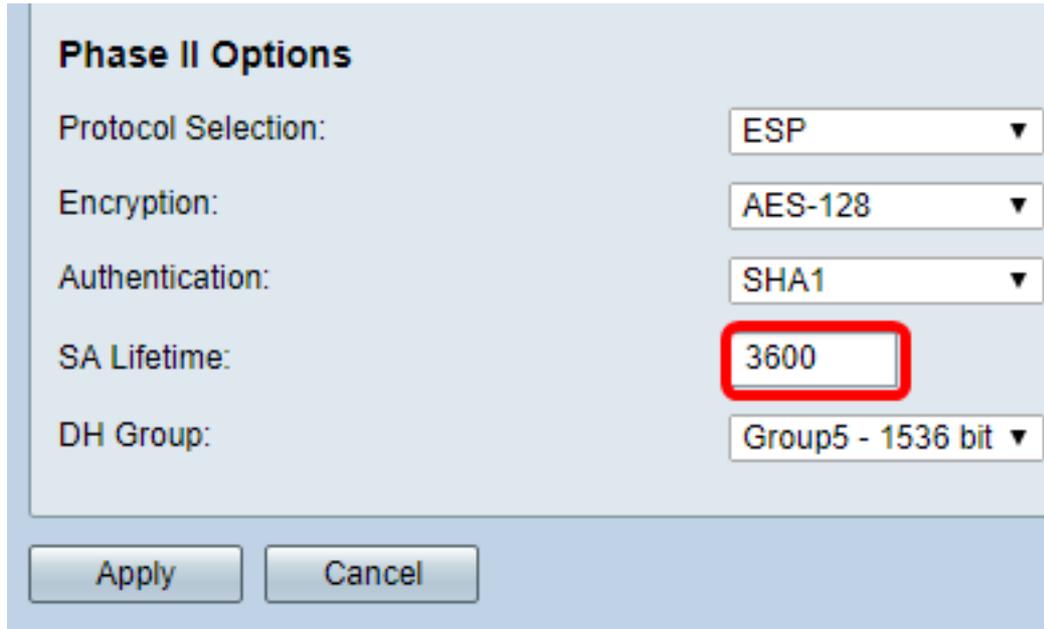
The screenshot shows the 'Phase II Options' dialog box. The 'Protocol Selection' dropdown is set to 'ESP'. The 'Encryption' dropdown is set to 'AES-128'. The 'Authentication' dropdown is open, showing options: 'SHA1' (highlighted with a red box), 'MD5', 'SHA2-256', and 'Group5 - 1536 bit'. The 'SA Lifetime' field is empty. The 'DH Group' dropdown is set to 'Group5 - 1536 bit'. At the bottom, there are 'Apply' and 'Cancel' buttons.

注意：在本例中，选择SHA1。

步骤9.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。

步骤10.从DH组下拉列表中，选择要与第2阶段中的密钥一起使用的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。



The image shows a configuration window titled "Phase II Options". It contains several settings:

Setting	Value
Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	SHA1
SA Lifetime:	3600
DH Group:	Group5 - 1536 bit

At the bottom of the window, there are two buttons: "Apply" and "Cancel". The "SA Lifetime" field, which contains the value "3600", is highlighted with a red rectangular border.

注意：在本例中，输入3600。

步骤11.单击“应用”。

IPSec Profiles

Add a New IP Sec Profile

Profile Name:

Keying Mode Auto Manual

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime:

DH Group:

步骤12.单击“保存”永久保存配置。



现在，您应该已在RV34x系列路由器上成功配置了自动IPSec配置文件。

[配置手动设置](#)

步骤1.在 *SPI-Incoming* 字段中，为VPN连接上的传入流量输入从100到FFFFFFFF的安全参数索引(SPI)标记的十六进制值。SPI标记用于区分一个会话的流量与其他会话的流量。

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

注意：在本例中，输入0xABCD。

步骤2.在 *SPI-Outgoing* 字段中，为VPN连接上的传出流量的SPI标记输入从100到FFFFFFF的十六进制值。

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

注意：在本例中，输入0x1234。

步骤3.从下拉列表中选择加密值。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。

SPI Incoming: [input field]

SPI Outgoing: [input field]

Encryption: [dropdown menu]

- 3DES
- AES-128
- AES-192
- ✓ AES-256

注意：在本例中，选择AES-256。

步骤4.在 *Key-In* 字段中，输入入站策略的密钥。密钥的长度取决于步骤3中选择的算法。

Key-In: 123456789123456789123...

Key-Out: 1a1a1a1a1a1a1a1a1212121...

注意：在本例中，输入123456789123456789123...

步骤5.在 *Key-Out* 字段中，输入传出策略的密钥。密钥的长度取决于步骤3中选择的算法。

Key-In: 123456789123456789123...

Key-Out: 1a1a1a1a1a1a1a1a1212121...

注意：在本例中，输入1a1a1a1a1a1a1a1a12121212...

步骤6.从Authentication下拉列表中选择身份验证方法。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。



Authentication: MD5
 SHA1
 SHA2-256

Key-In

Key-Out

注意：在本例中，选择MD5。

步骤7.在Key-In字段中，输入入站策略的密钥。密钥的长度取决于步骤6中选择的算法。

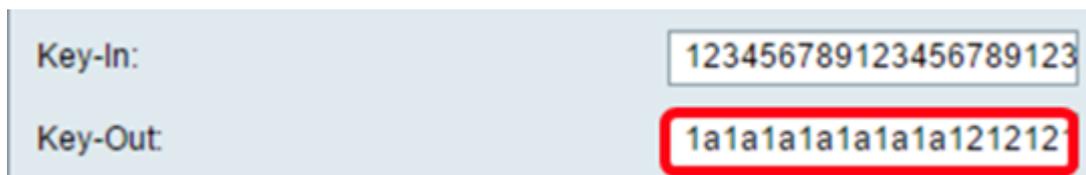


Key-In: 123456789123456789123

Key-Out: 1a1a1a1a1a1a1a1a1212121

注意：在本例中，输入123456789123456789123...

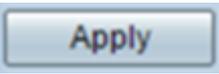
步骤8.在Key-Out字段中，输入传出策略的密钥。密钥的长度取决于步骤6中选择的算法。



Key-In: 123456789123456789123

Key-Out: 1a1a1a1a1a1a1a1a1212121

注意：在本例中，输入1a1a1a1a1a1a1a1a12121212...

步骤9.单击 。

步骤10.单击“保存”永久保存配置。



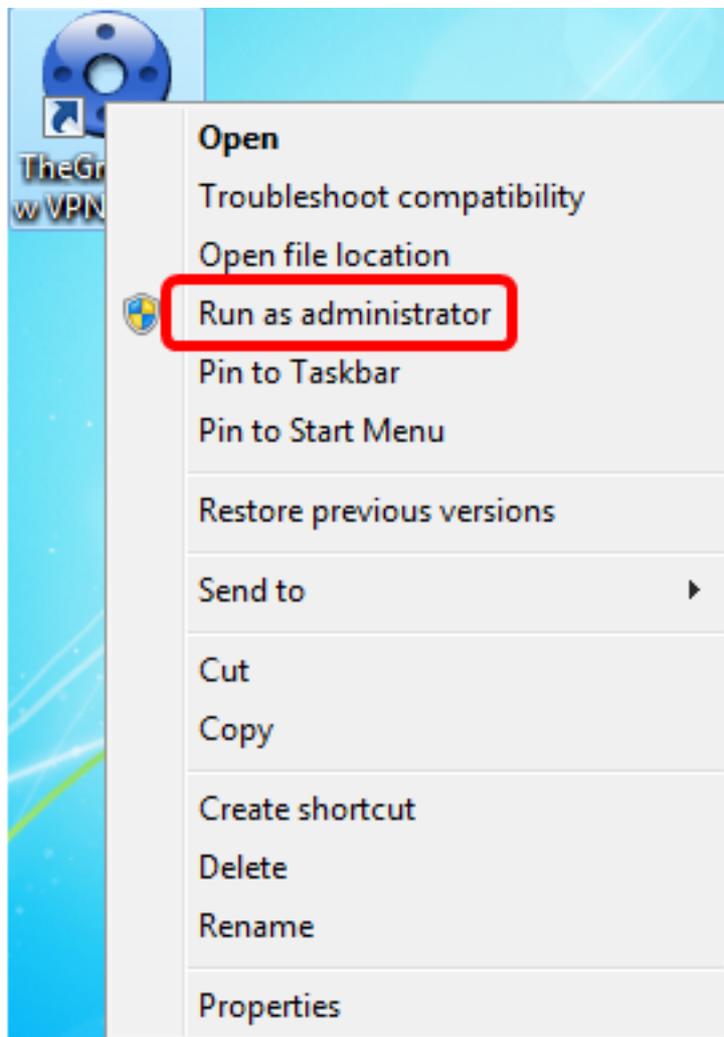
cisco (admin) Log Out About Help

现在，您应该已在RV34x系列路由器上成功配置了手动IPSec配置文件。

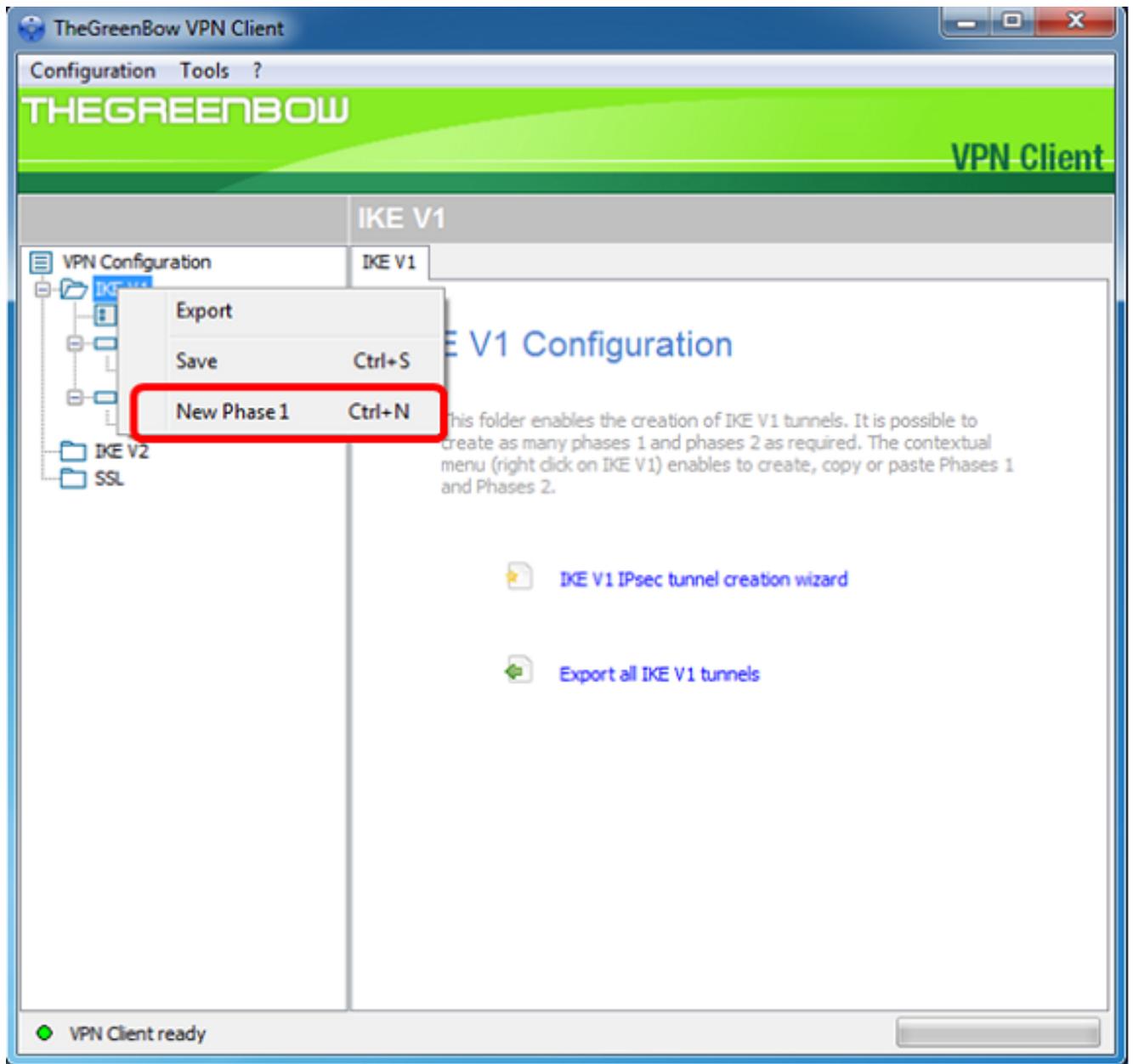
配置GreenBow VPN客户端软件

配置第1阶段设置

步骤1.右键单击GreenBow VPN Client图标，然后选择Run as administrator(以管理员身份运行)。

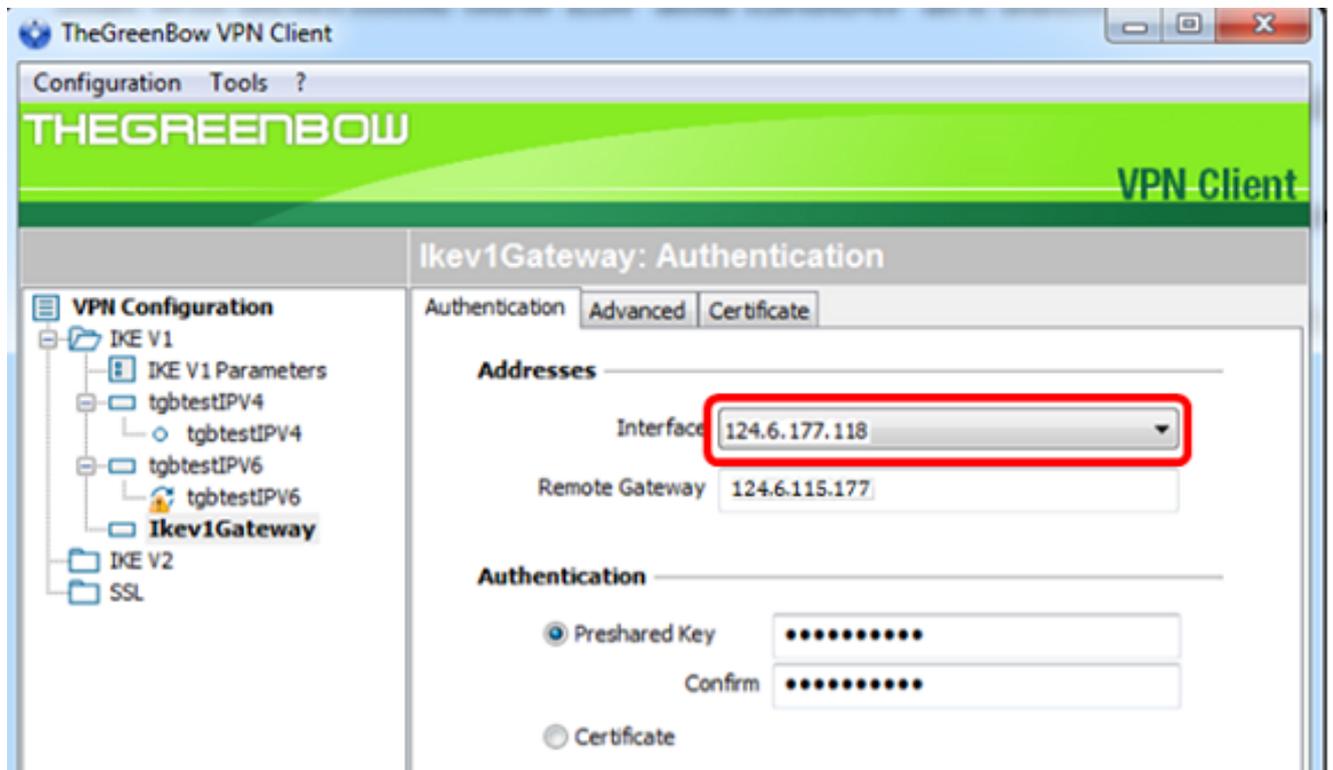


步骤2.在VPN配置下的左窗格中，右键单击IKE V1并选择New Phase 1。



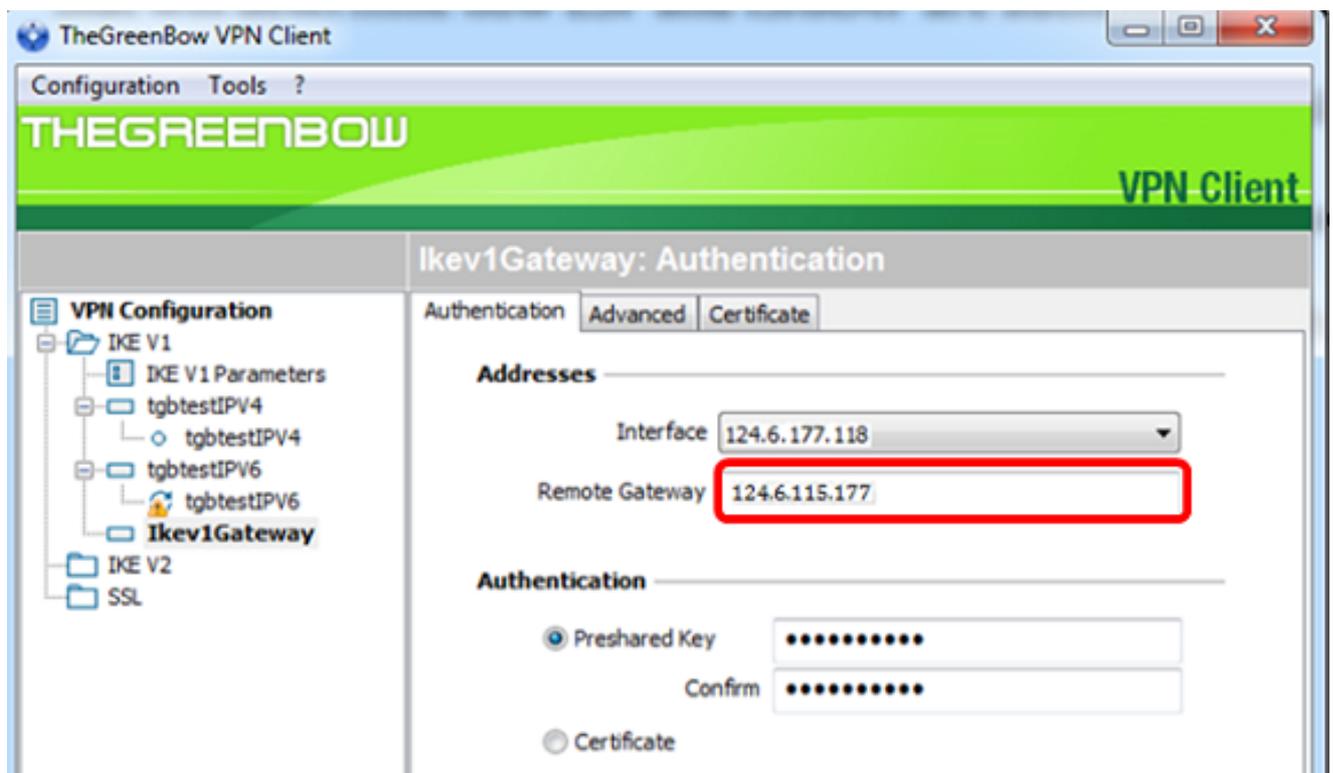
步骤3.在Addresses下的Authentication选项卡中，验证Interface区域中的IP地址与安装GreenBow VPN客户端的计算机的WAN IP地址相同。

注意：在本示例中，IP 地址是 124.6.177.118。



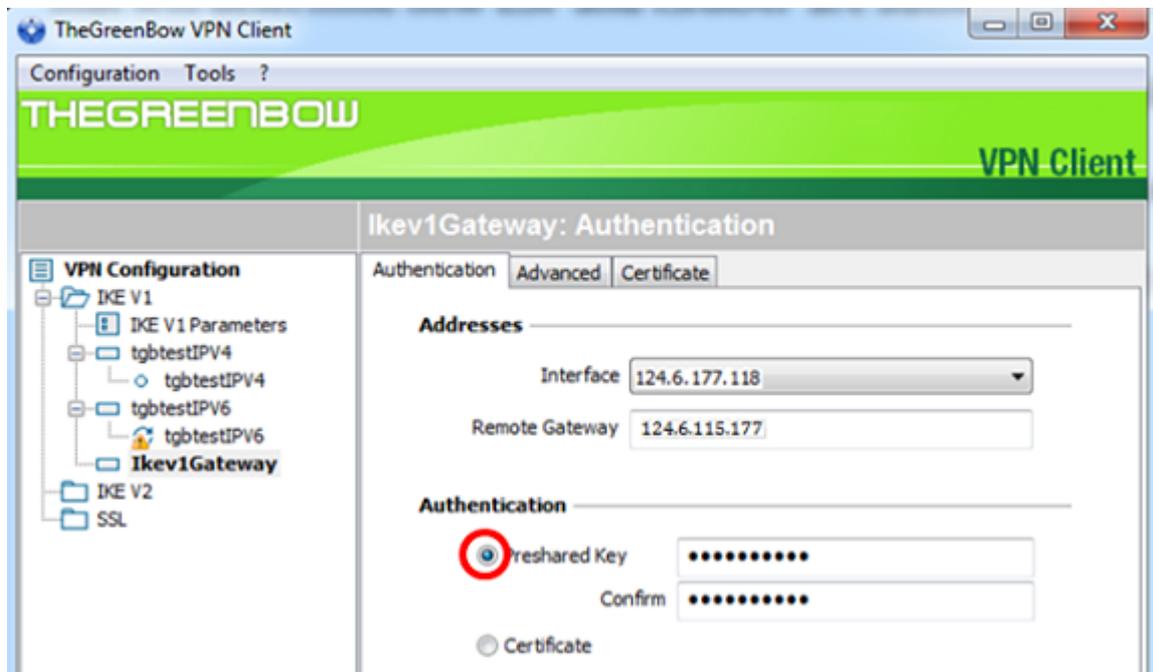
步骤4.在Remote Gateway (远程网关) 字段中输入远程网关的地址。

注意：在本例中，远程RV34x路由器的IP地址为124.6.115.177。



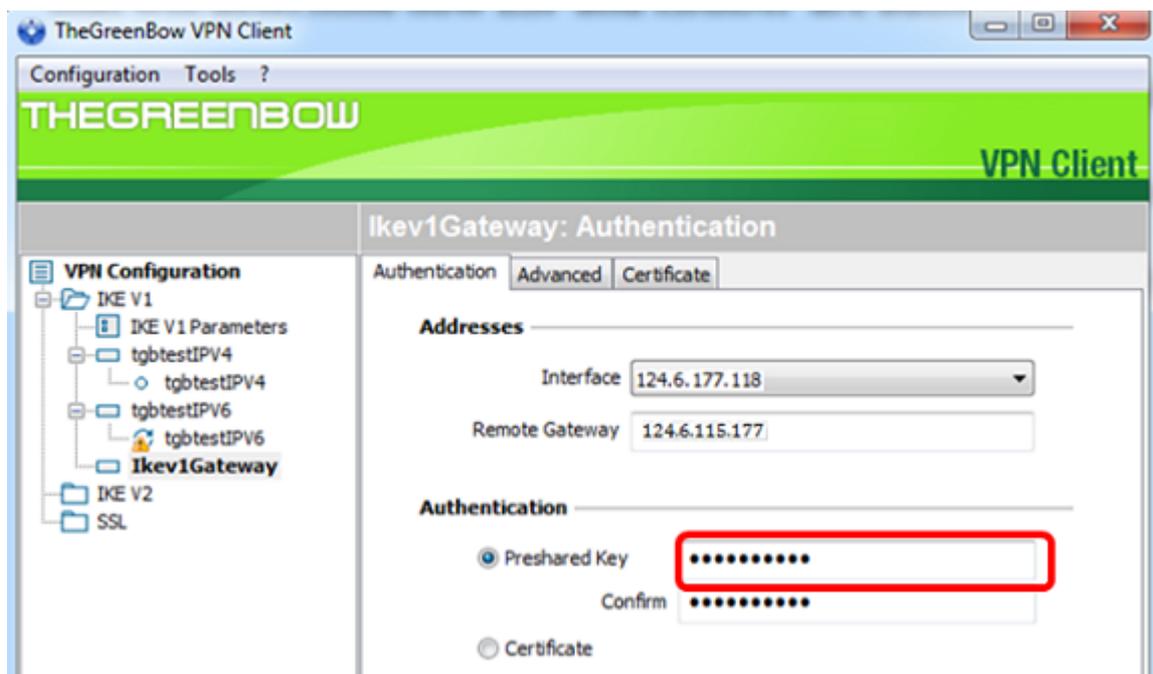
步骤5.在Authentication下，选择身份验证类型。选项有：

- 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。

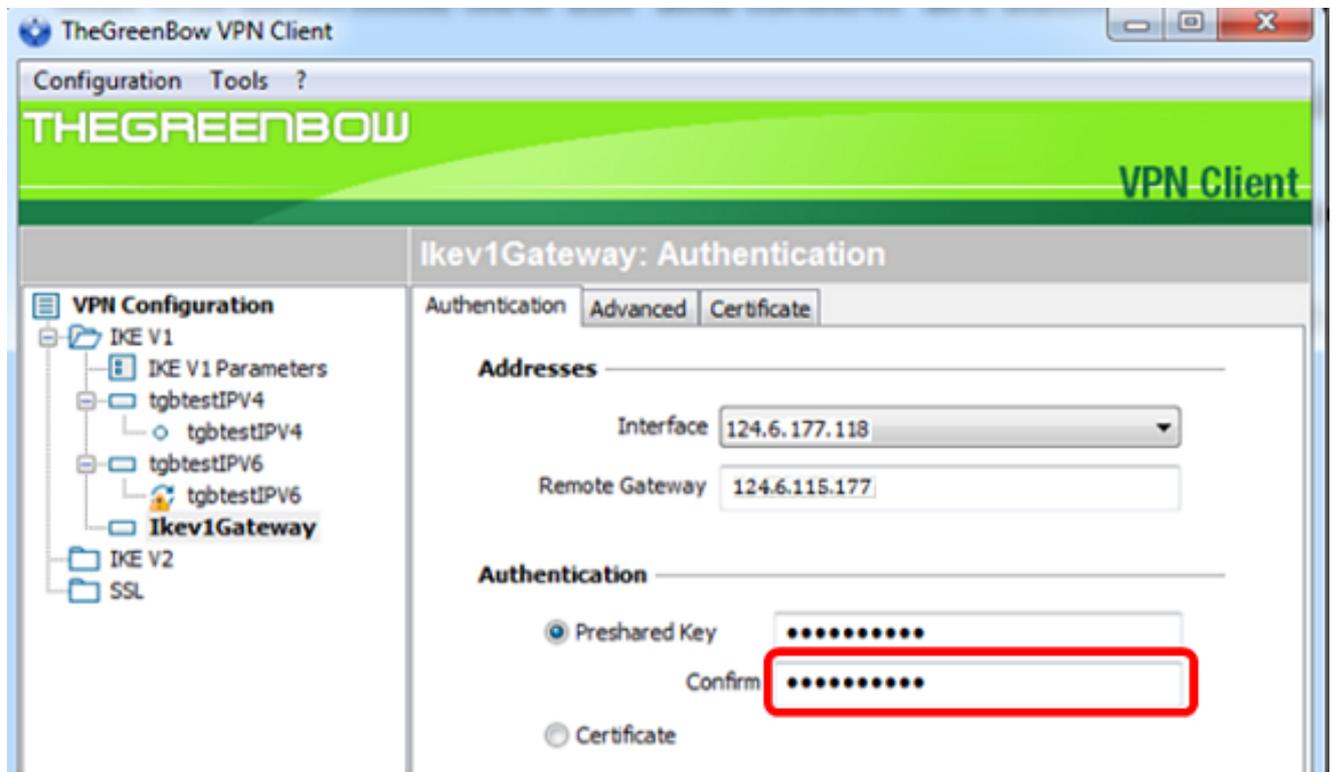


注意：在本示例中，选择预共享密钥以匹配RV34x VPN网关的配置。

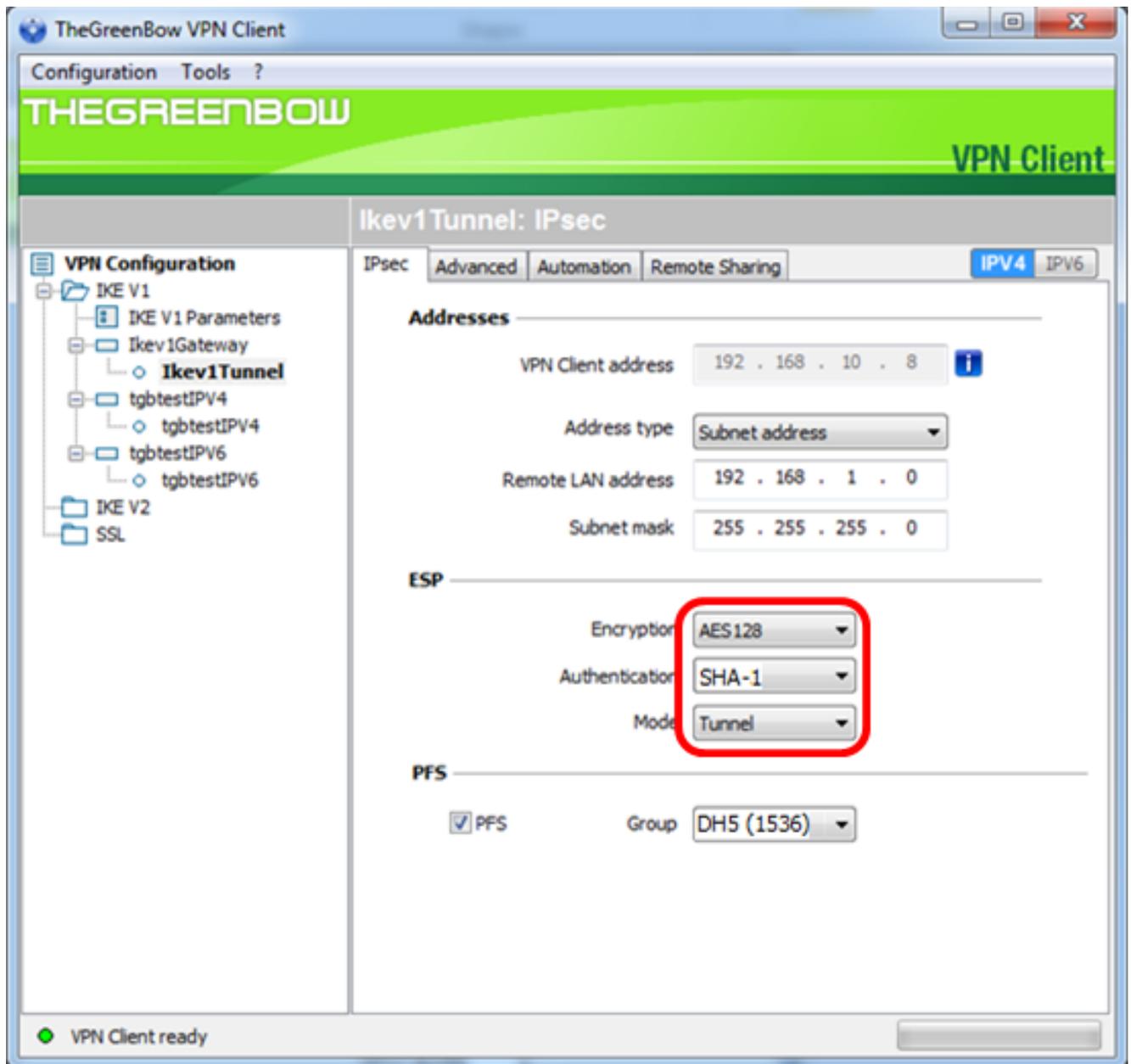
步骤6.输入路由器中配置的预共享密钥。



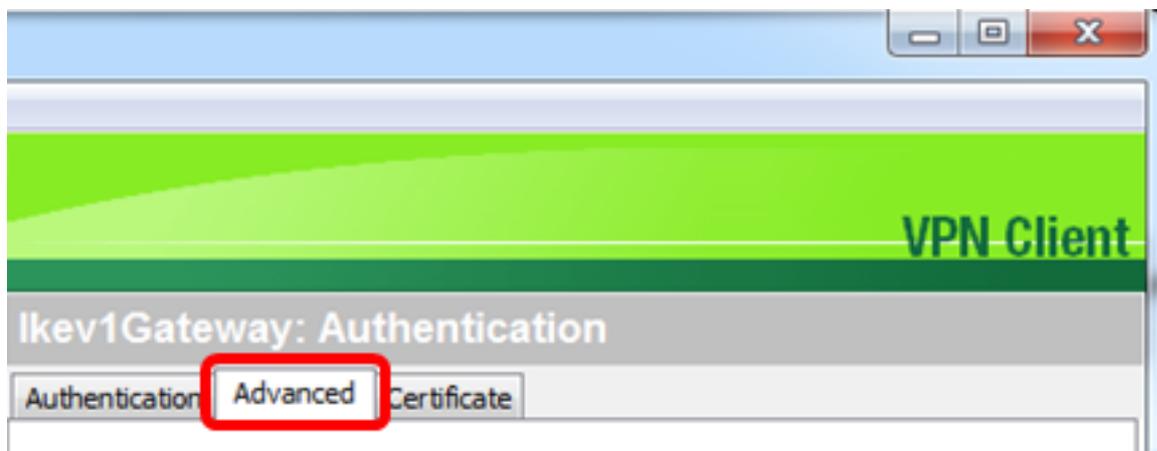
步骤7.在“确认”字段中输入相同的预共享密钥。



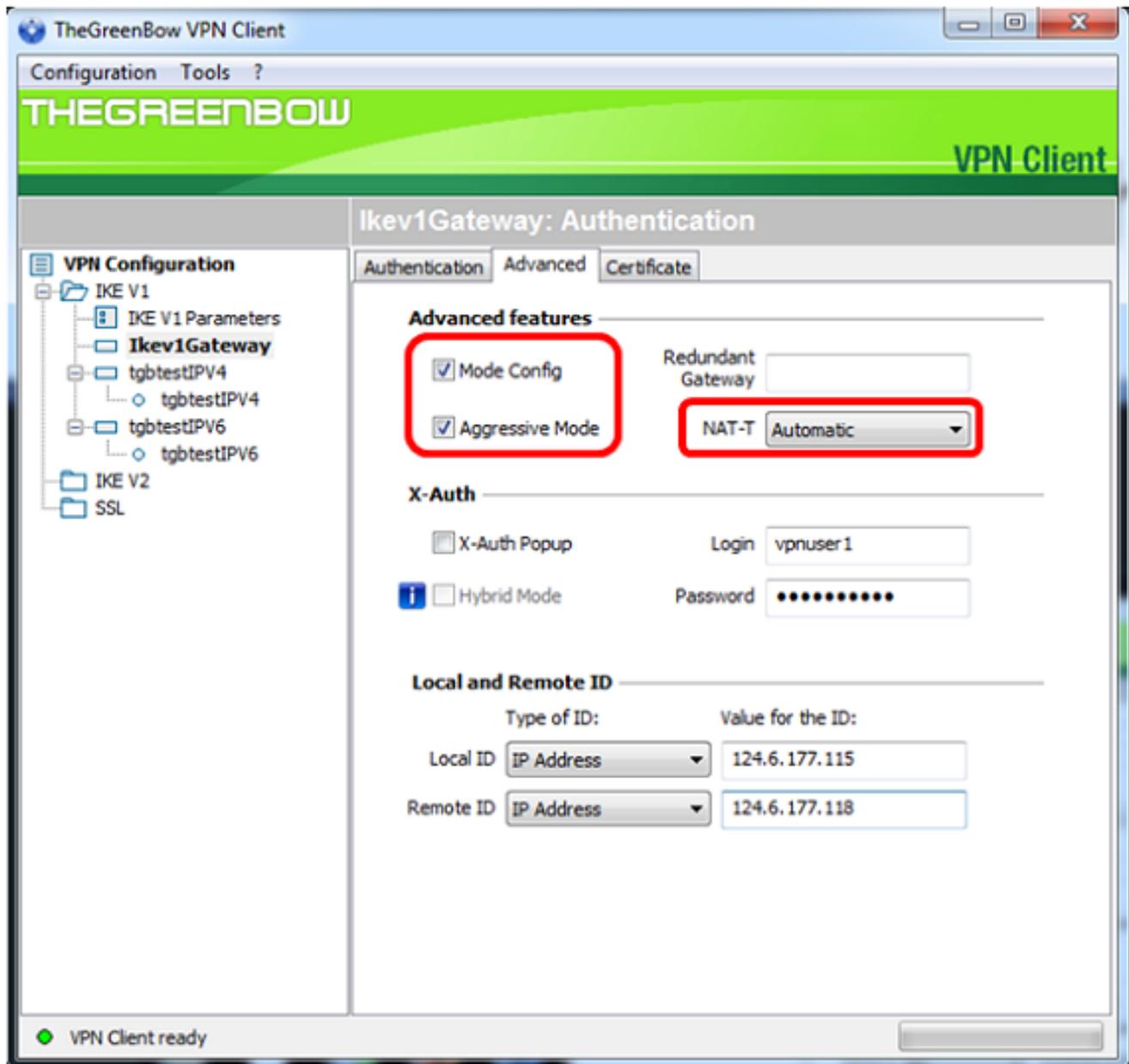
步骤8.在IKE下，设置加密、身份验证和密钥组设置以匹配路由器的配置。



步骤9.单击“高级”选项卡。

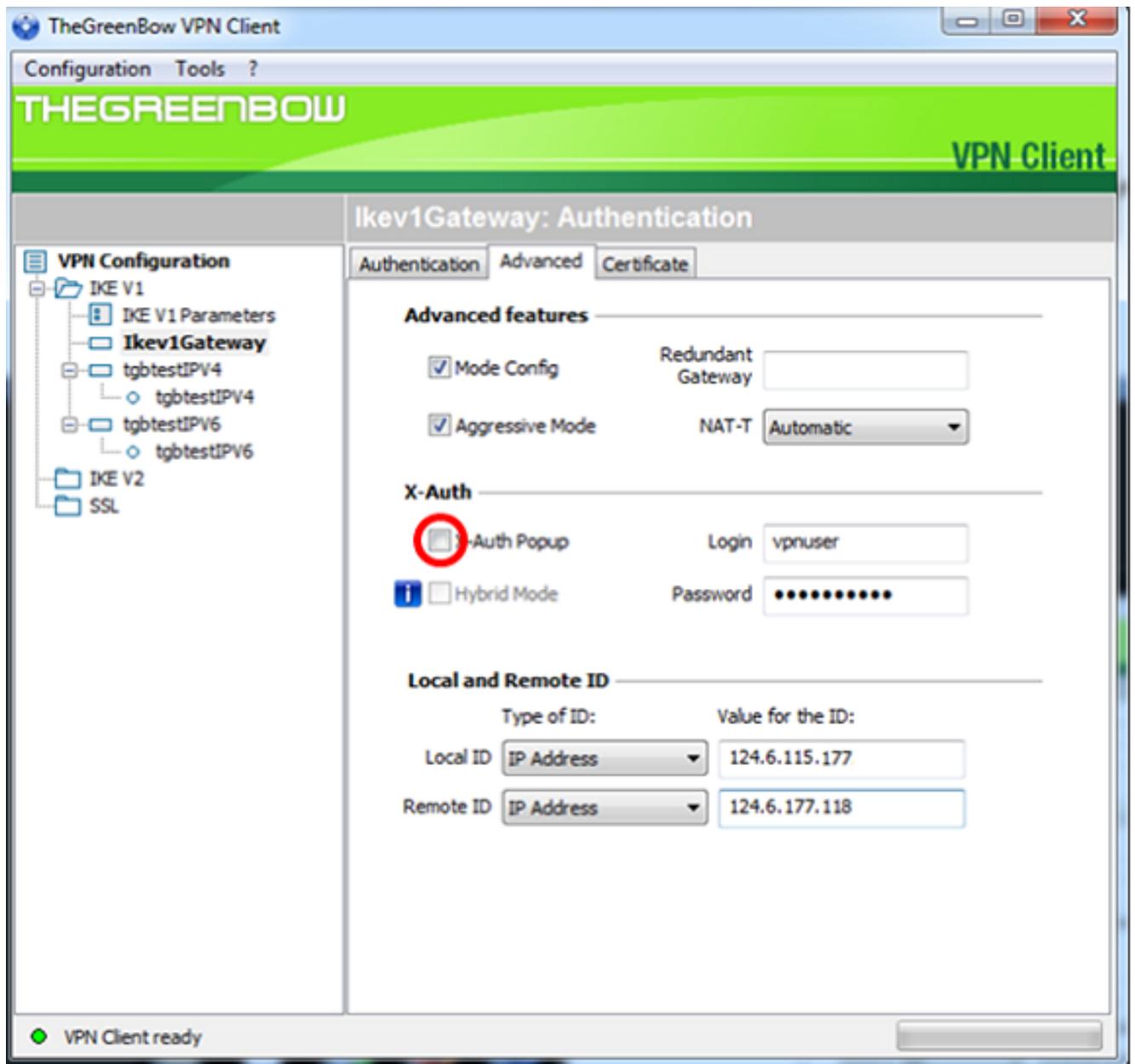


步骤10. (可选) 在Advanced features下，选中Mode Config 和Aggressive Mode 复选框，并将NAT-T设置设置为Automatic。



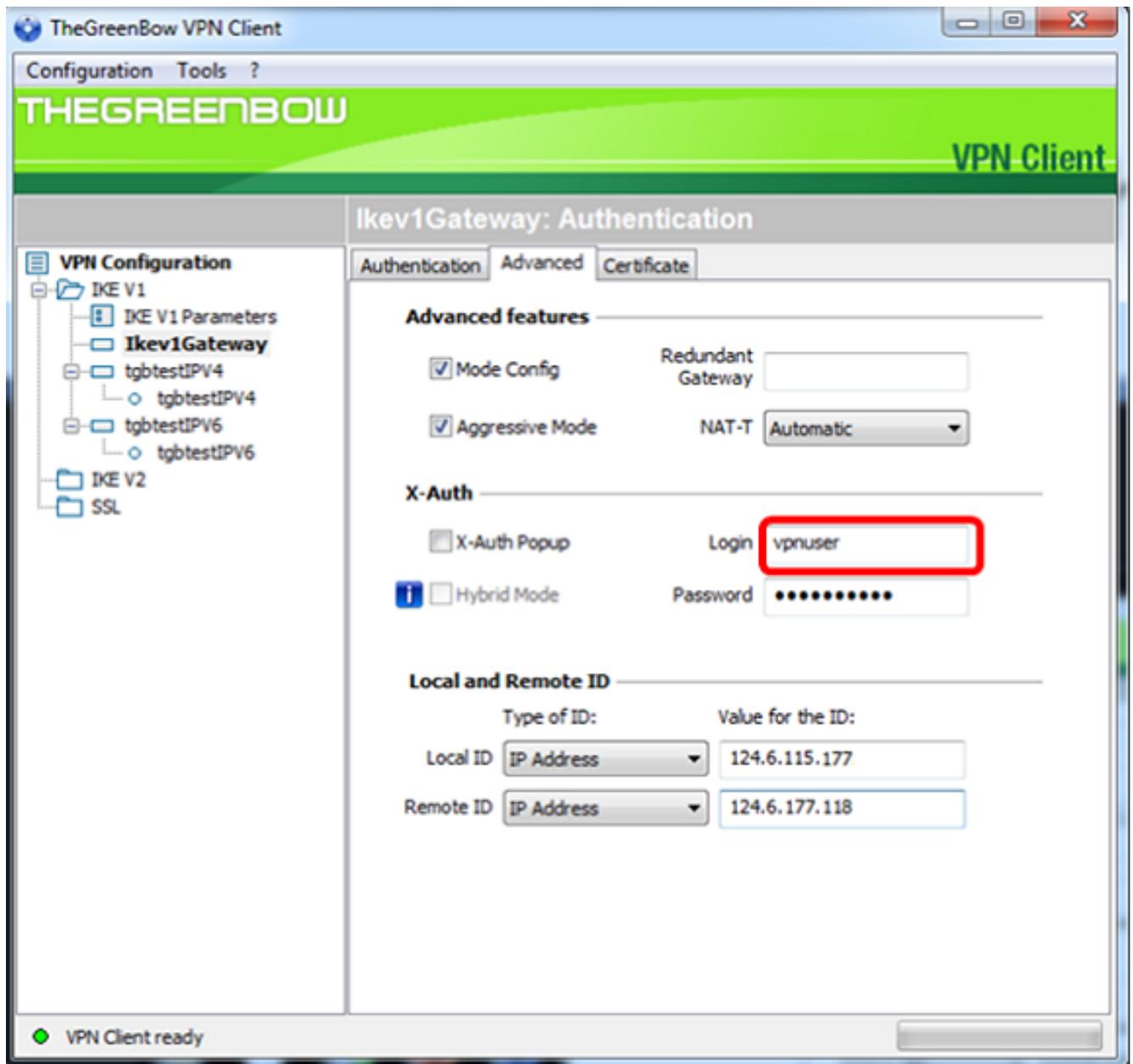
注意：启用模式配置后，GreenBow VPN客户端将从VPN网关提取设置以尝试建立隧道，同时启用主动模式和NAT-T可加快建立连接。

第11步。（可选）在X-Auth下，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。

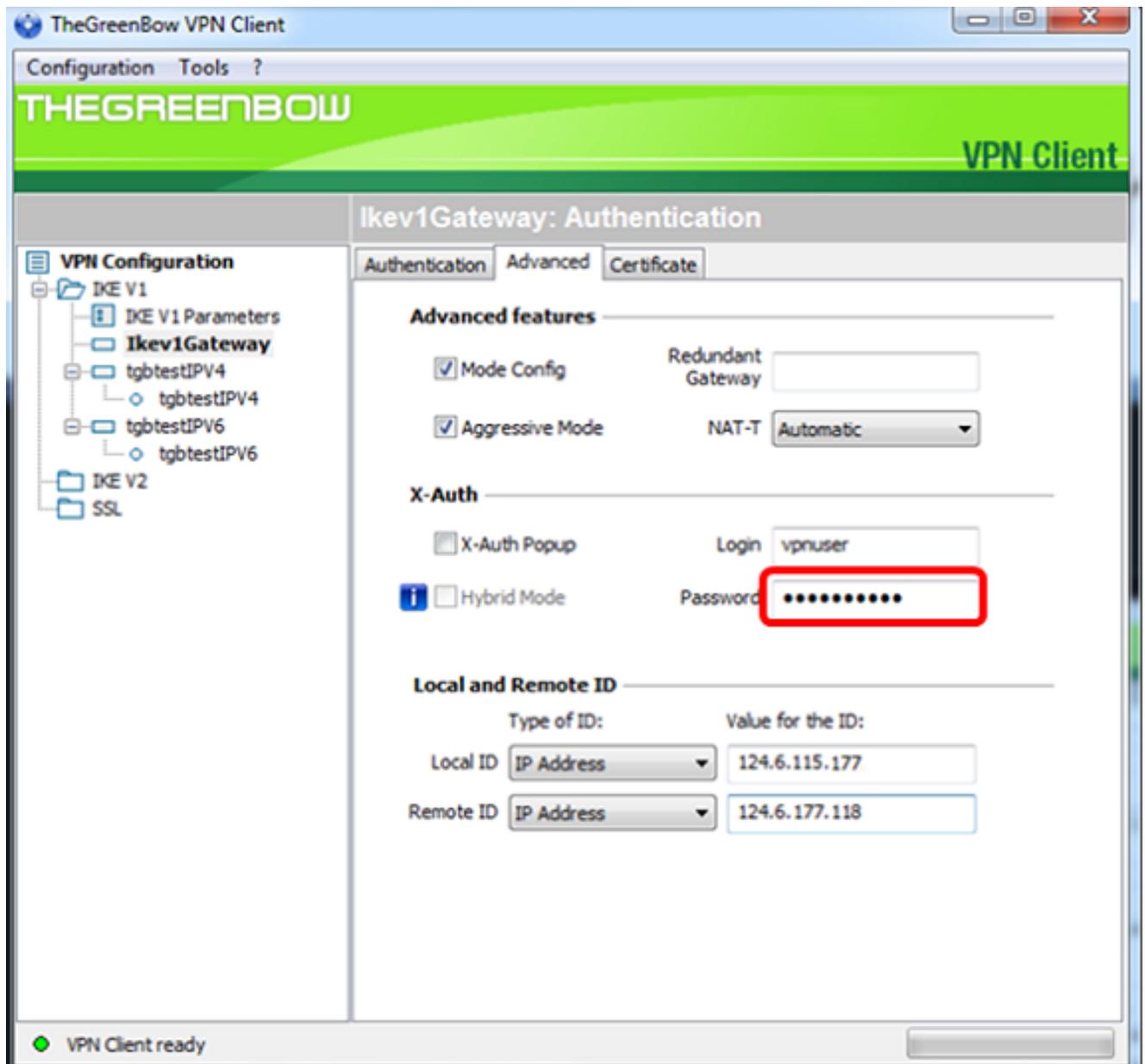


注意：在本例中，未选中X-Auth弹出窗口。

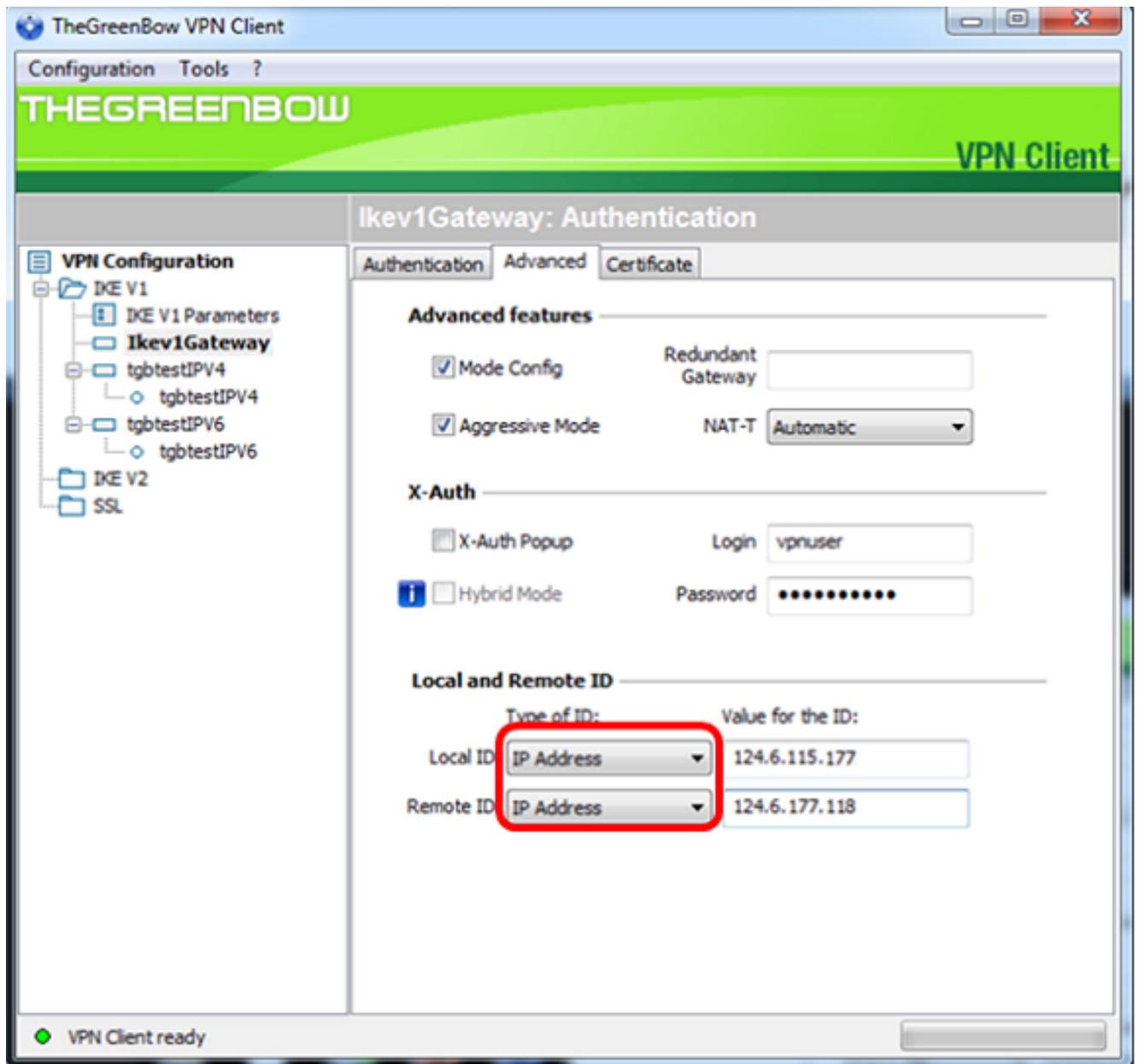
步骤12.在Login字段中输入您的用户名。这是为在VPN网关中创建用户组而配置的用户名。



步骤13.在Password字段中输入密码。

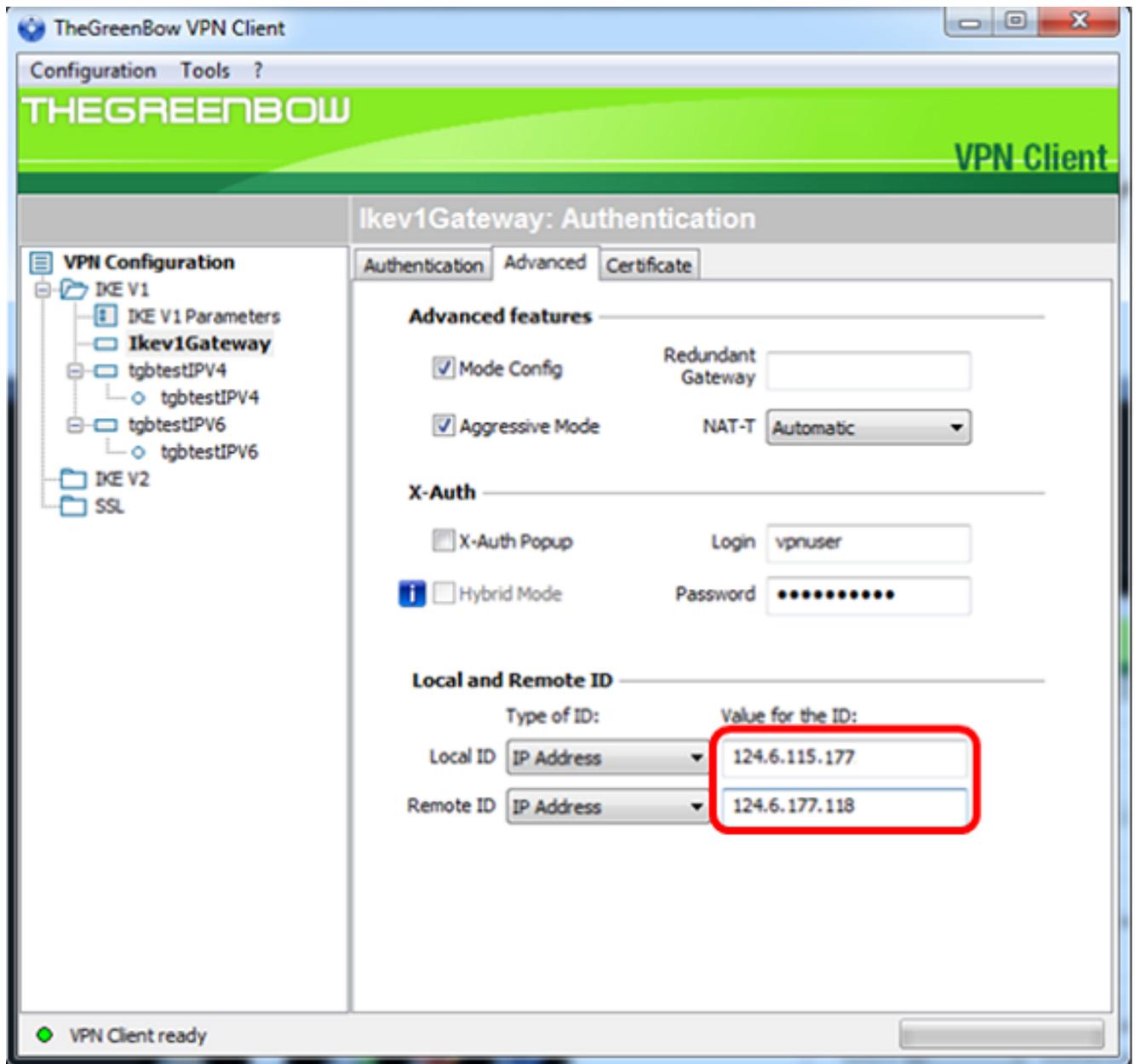


步骤14.在Local ID和Remote ID下，设置Local ID和Remote ID以匹配VPN网关的设置。

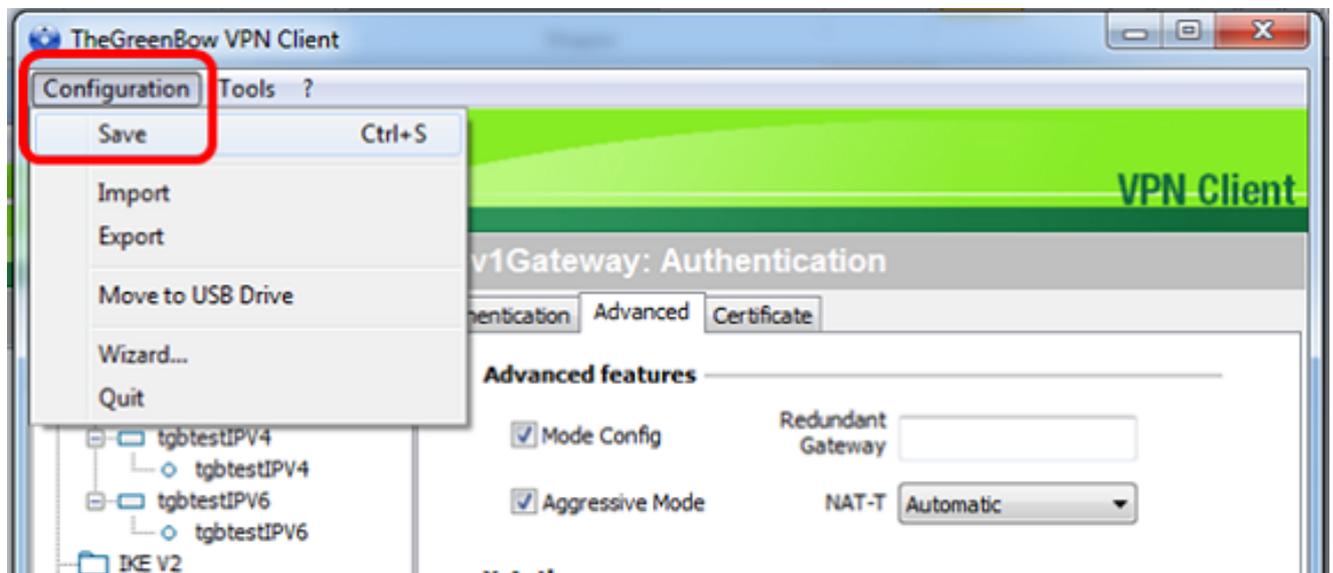


注意：在本例中，本地ID和远程ID均设置为IP地址以匹配RV34x VPN网关的设置。

步骤15.在ID的Value下，在各自的字段中输入本地ID和远程ID。

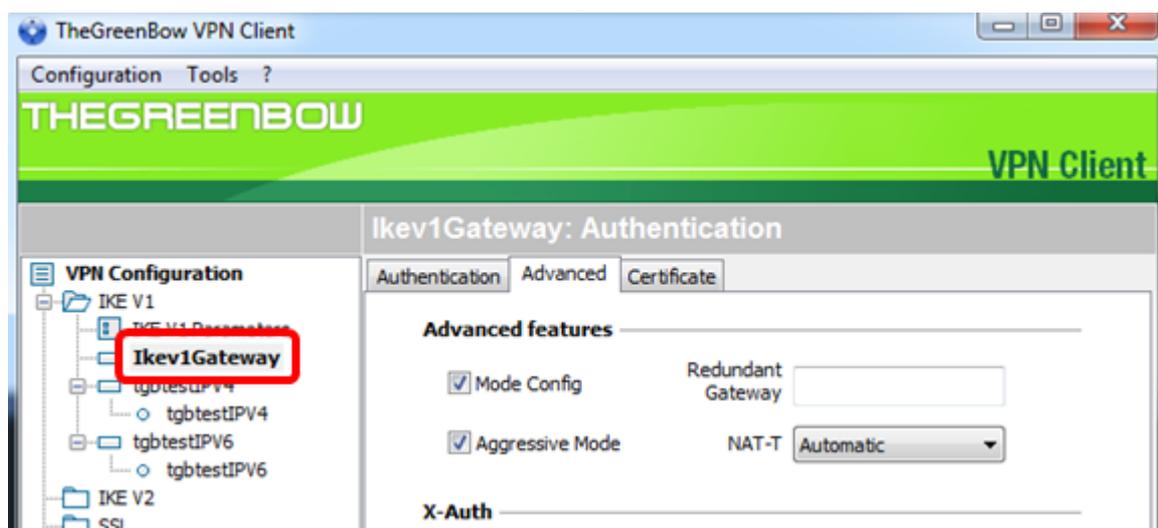


步骤16. 单击Configuration > Save以保存设置。

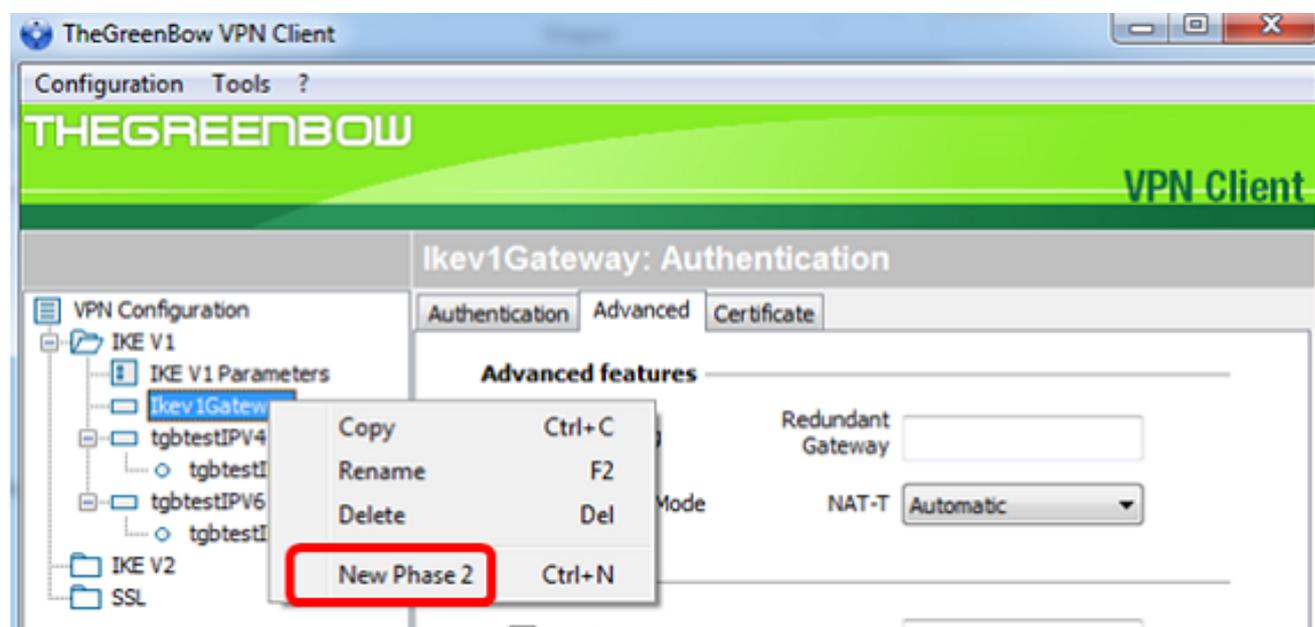


配置第2阶段设置

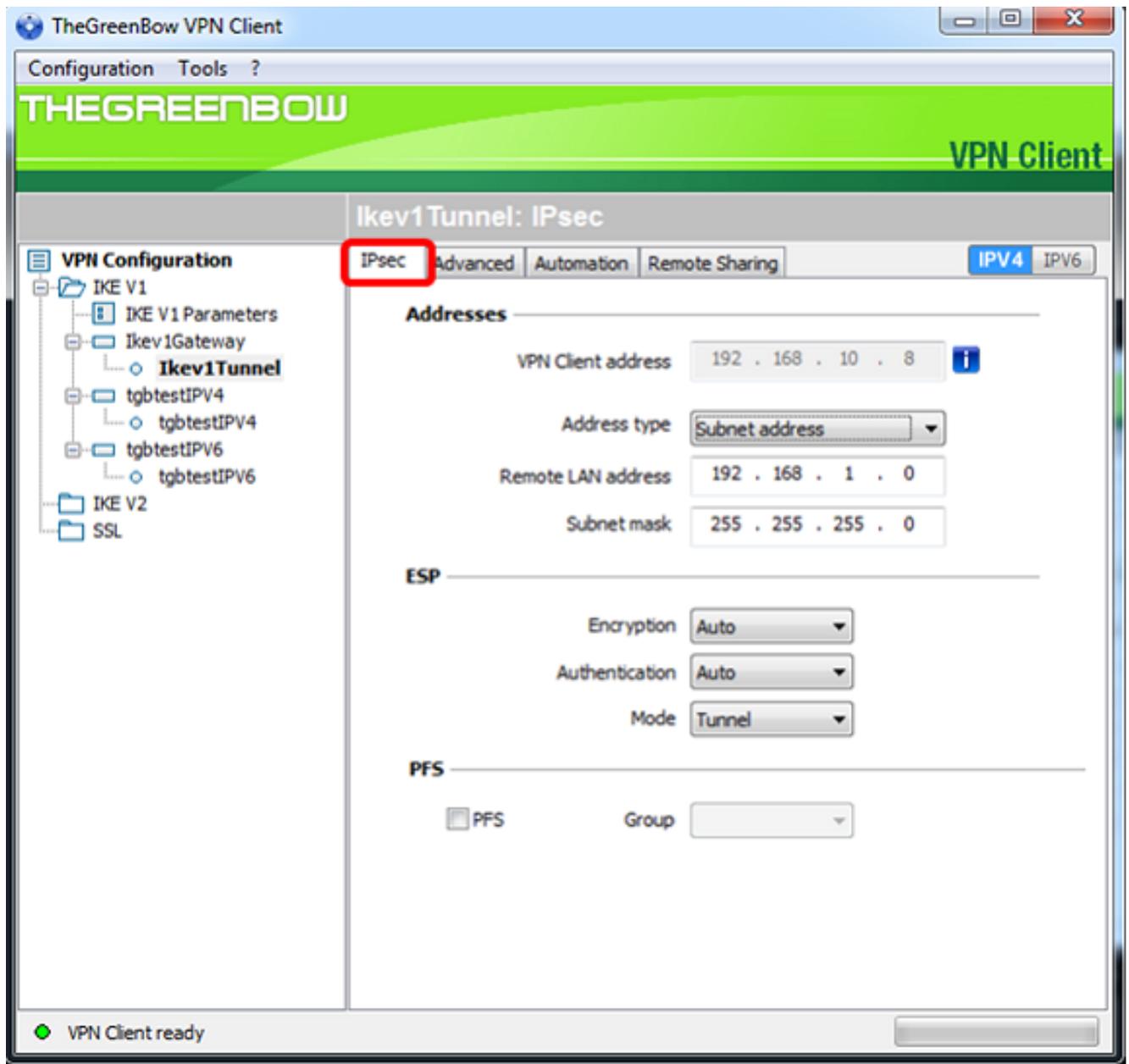
步骤1.右键单击Ikev1 Gateway。



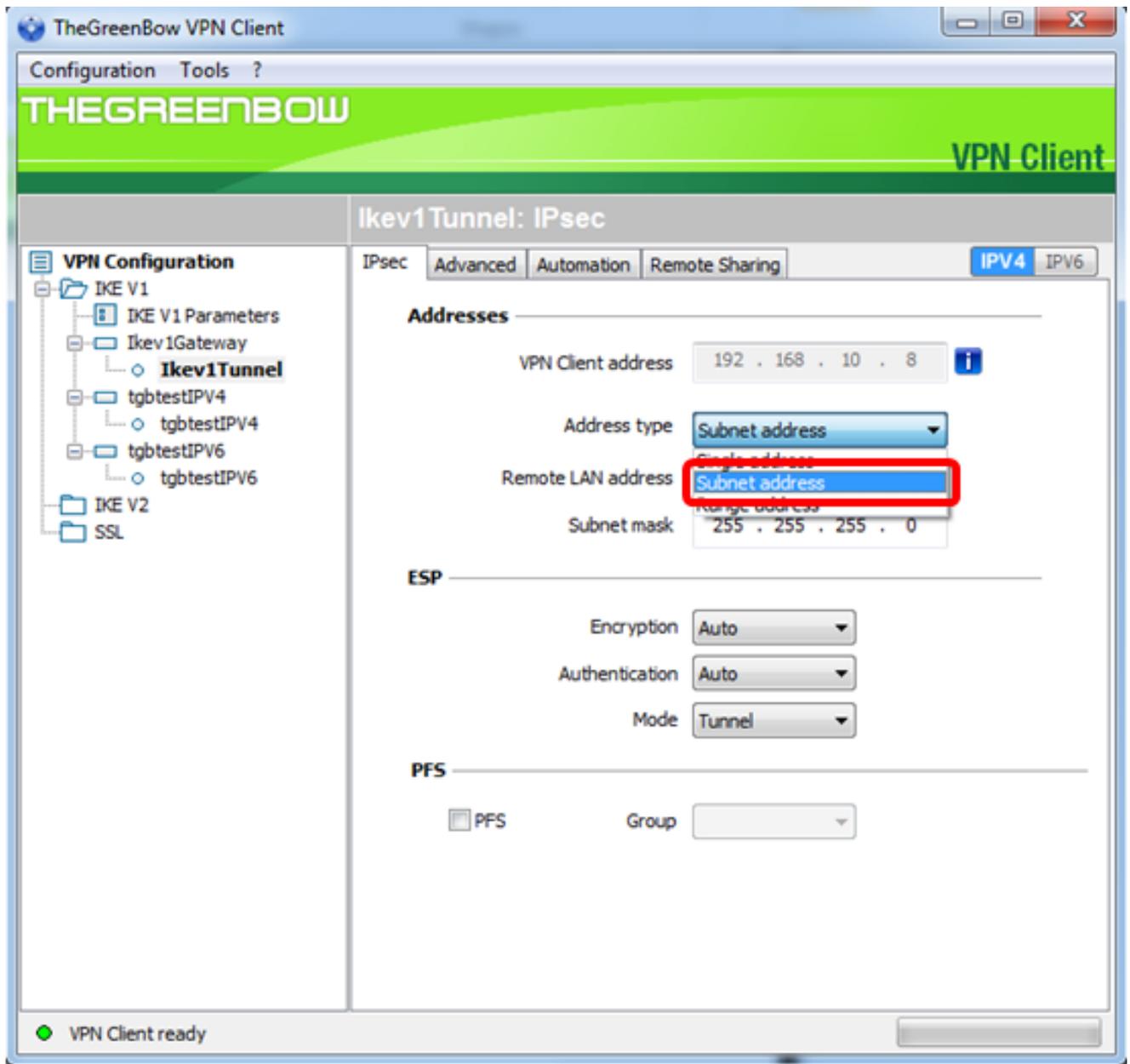
步骤2.选择新阶段2。



步骤3.单击IPsec选项卡。

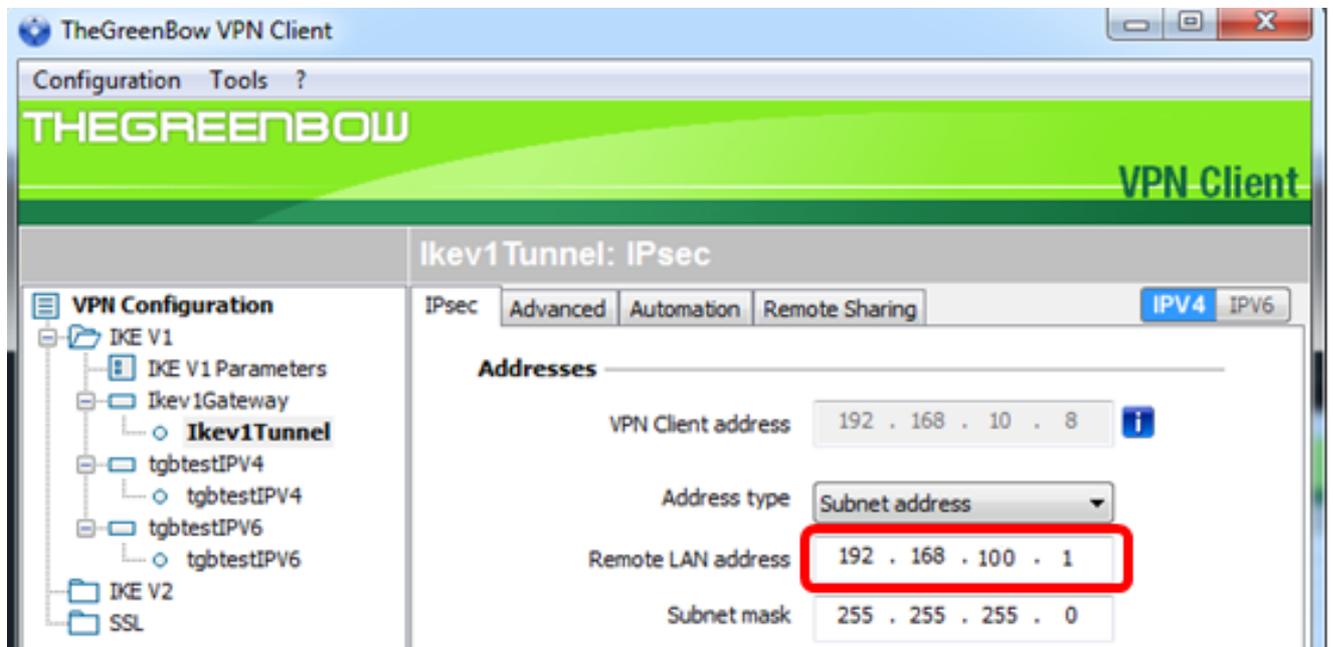


步骤4.从Address type (地址类型) 下拉列表中选择VPN客户端可以访问的地址类型。



注意：在本例中，选择子网地址。

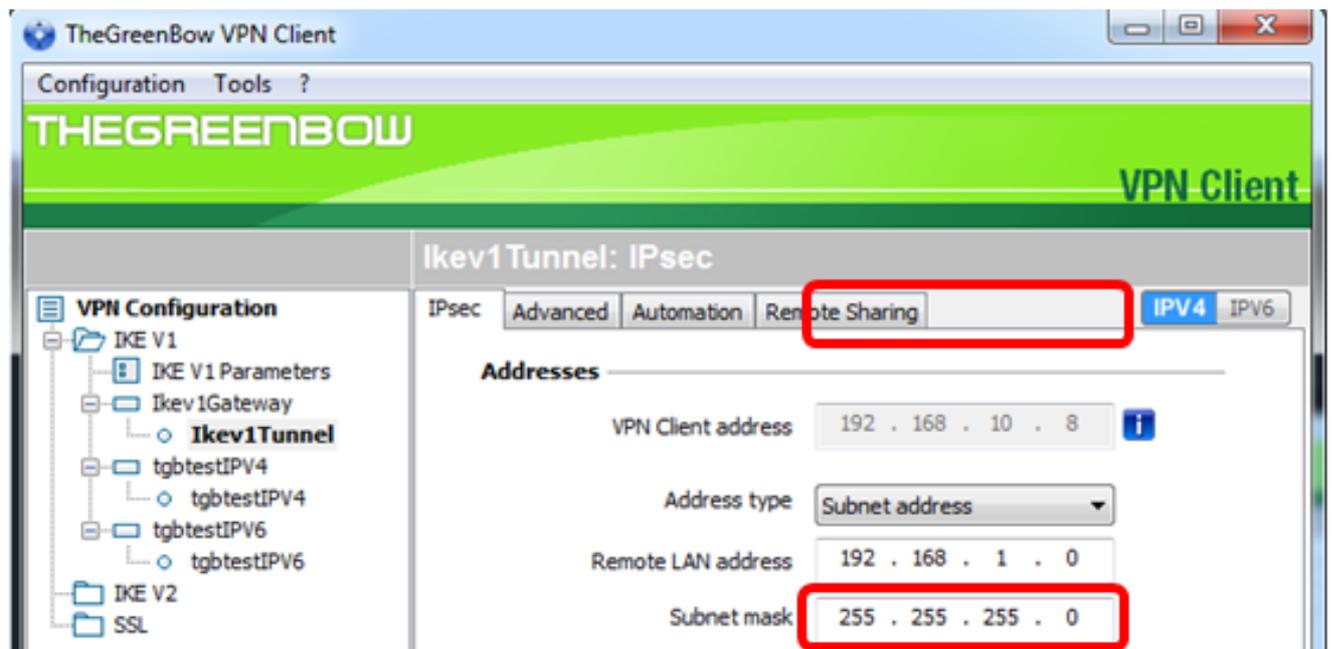
步骤5.在Remote LAN address字段中输入VPN隧道应访问的网络地址。



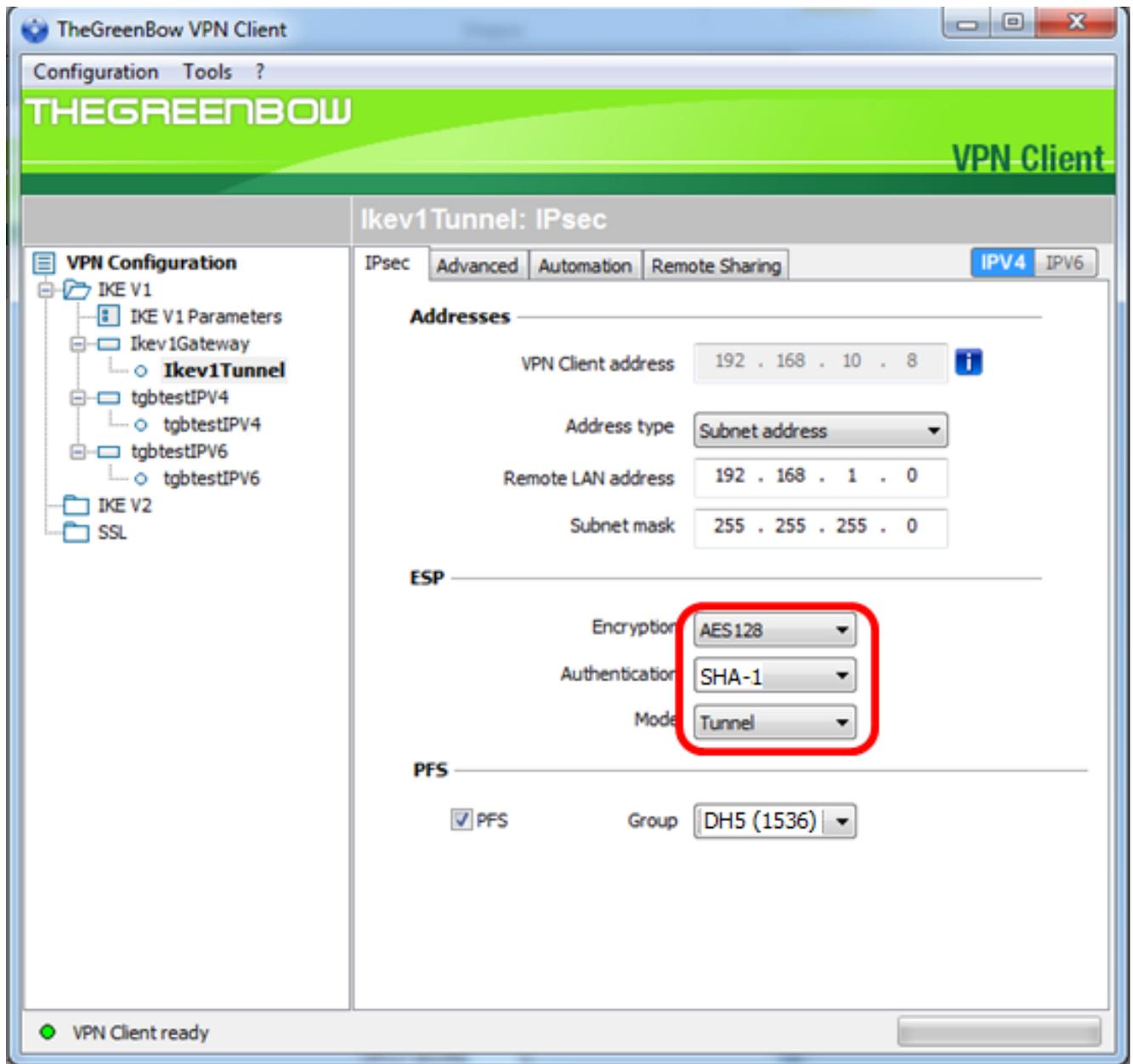
注意：在本例中，输入192.168.100.1。

步骤6.在“子网掩码”字段中输入远程网络的子网掩码。

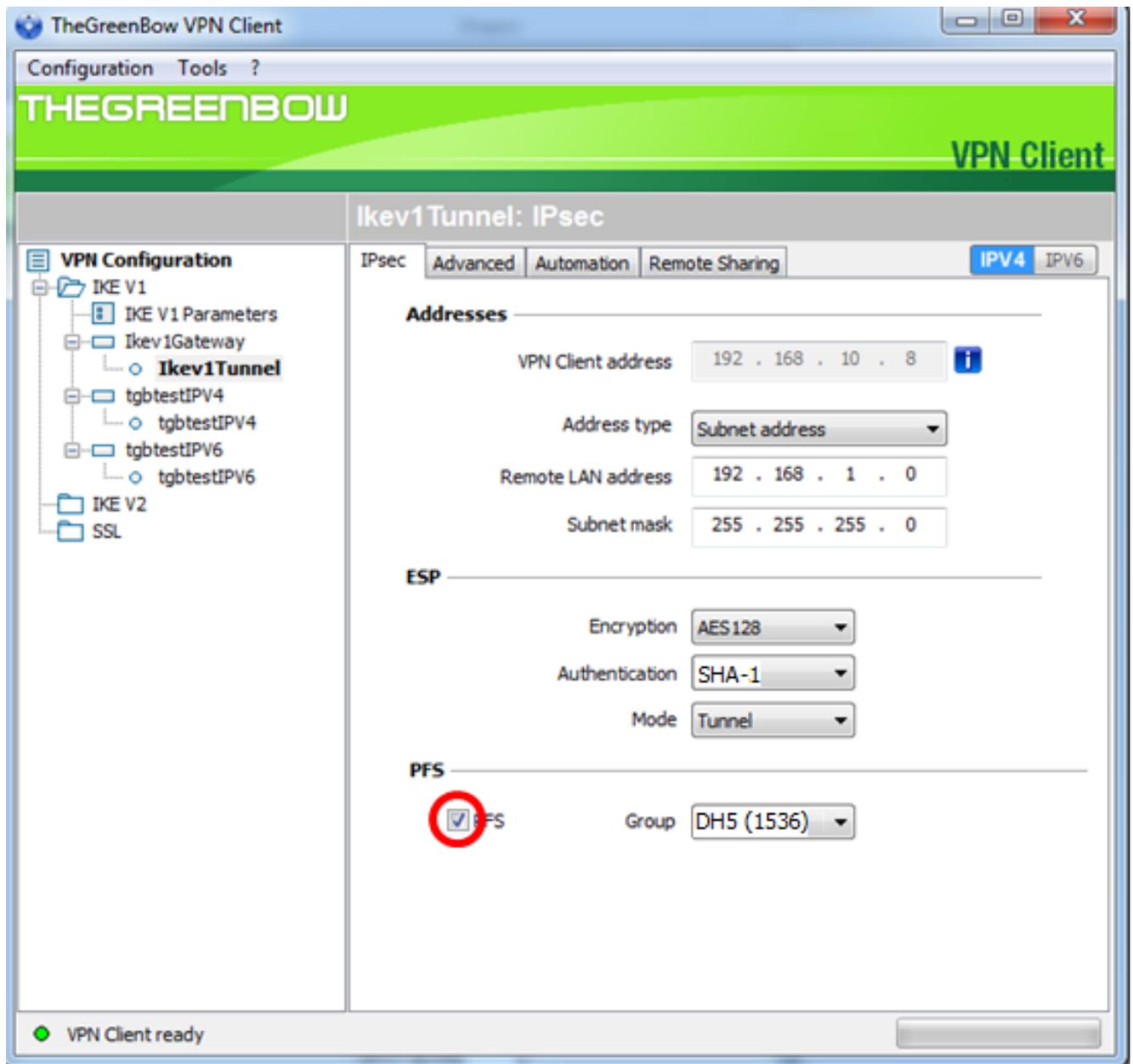
注意：在本例中，输入255.255.255.0。



步骤7.在ESP下，设置Encryption、Authentication和Mode以匹配VPN网关的设置。

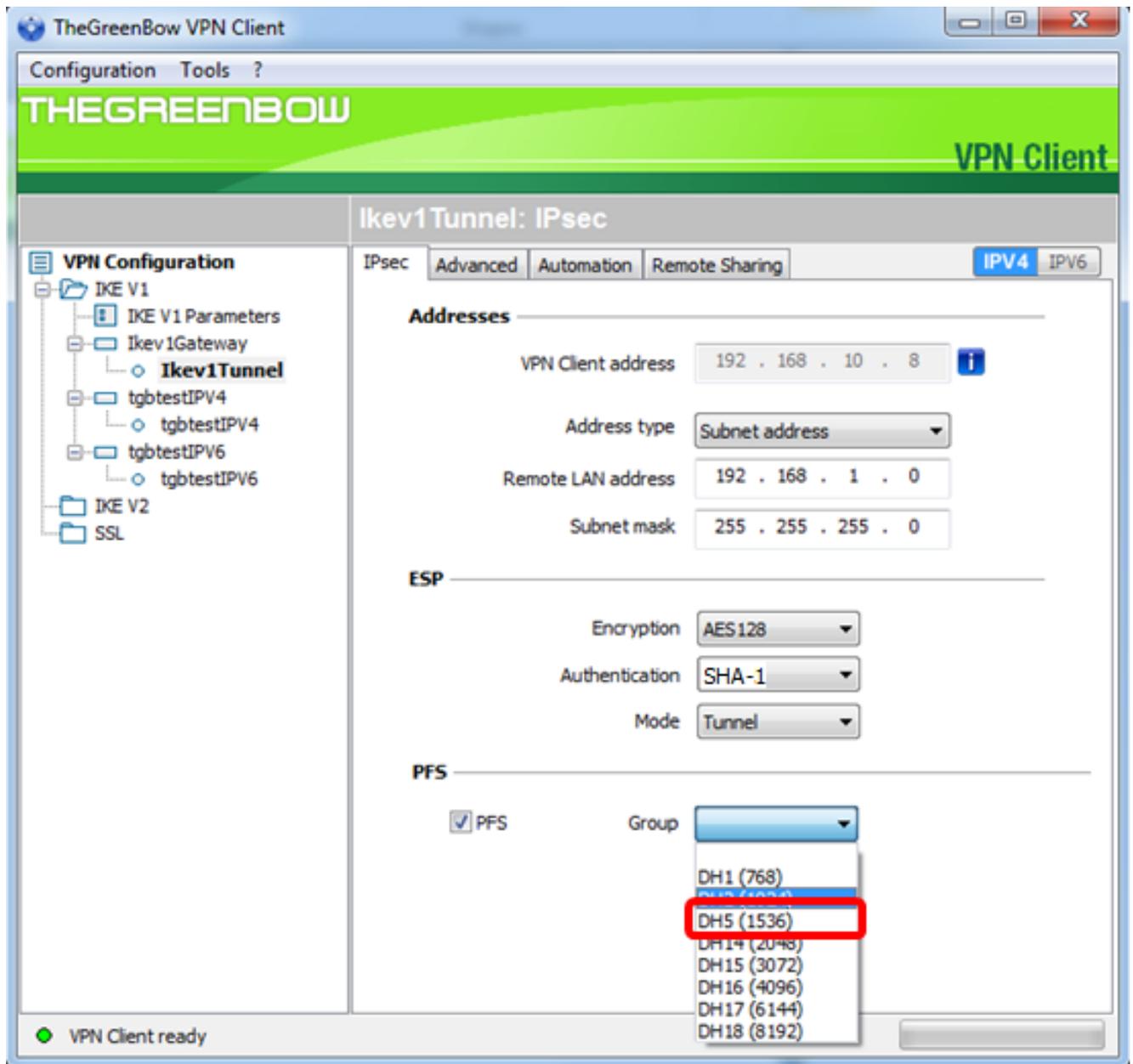


步骤8. (可选) 在PFS下，选中PFS复选框以启用完全向前保密(PFS)。PFS生成用于加密会话的随机密钥。

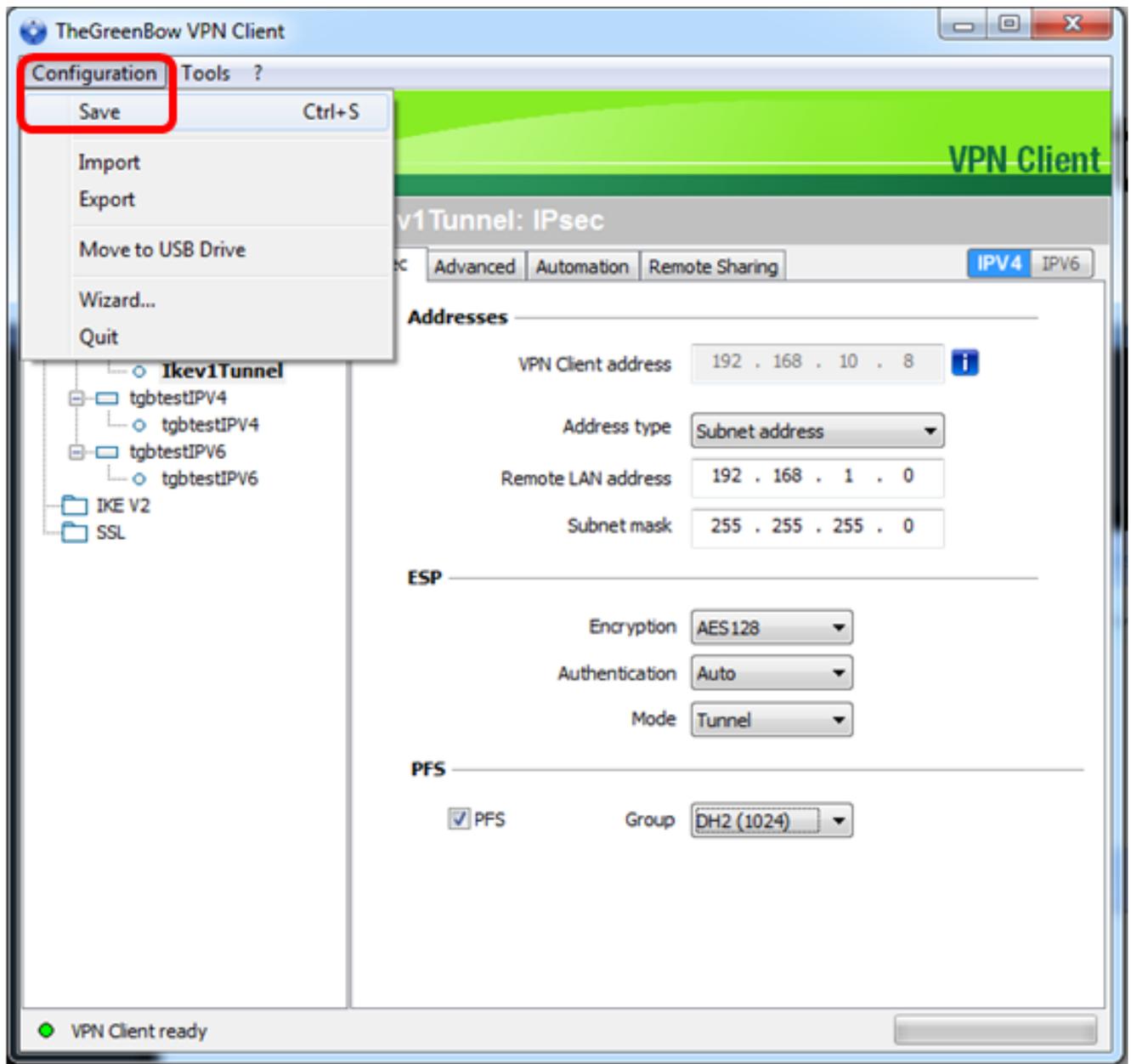


步骤9.从Group下拉列表中选择PFS组设置。

注意：在本例中，选择DH5(1536)以匹配路由器的DH组设置。



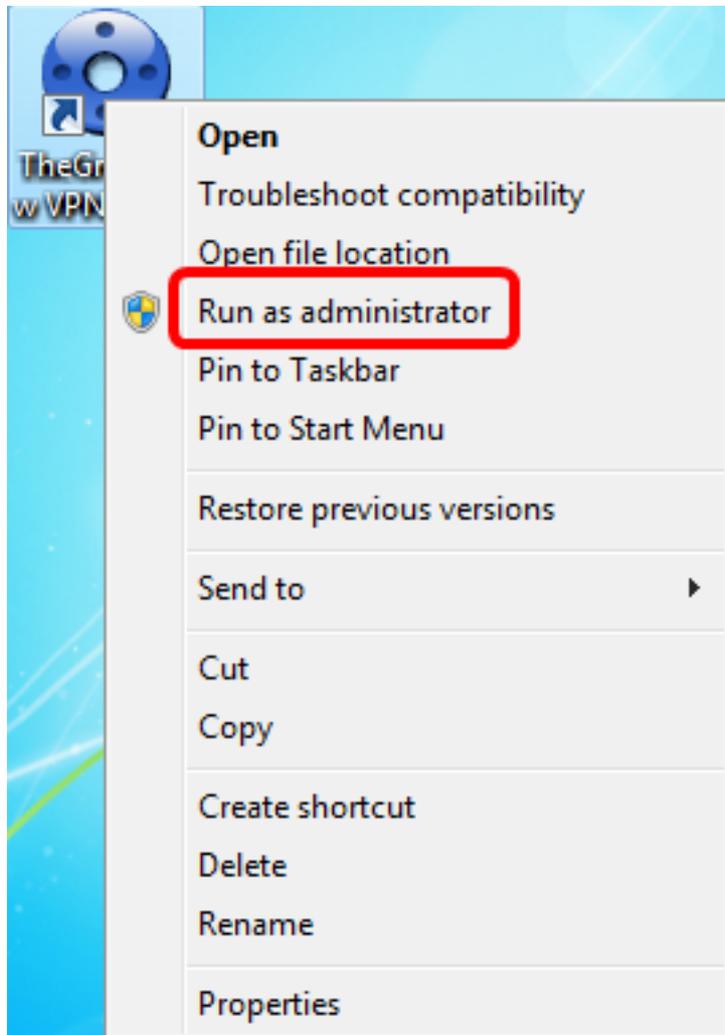
步骤10.右键单击Configuration并选择Save。



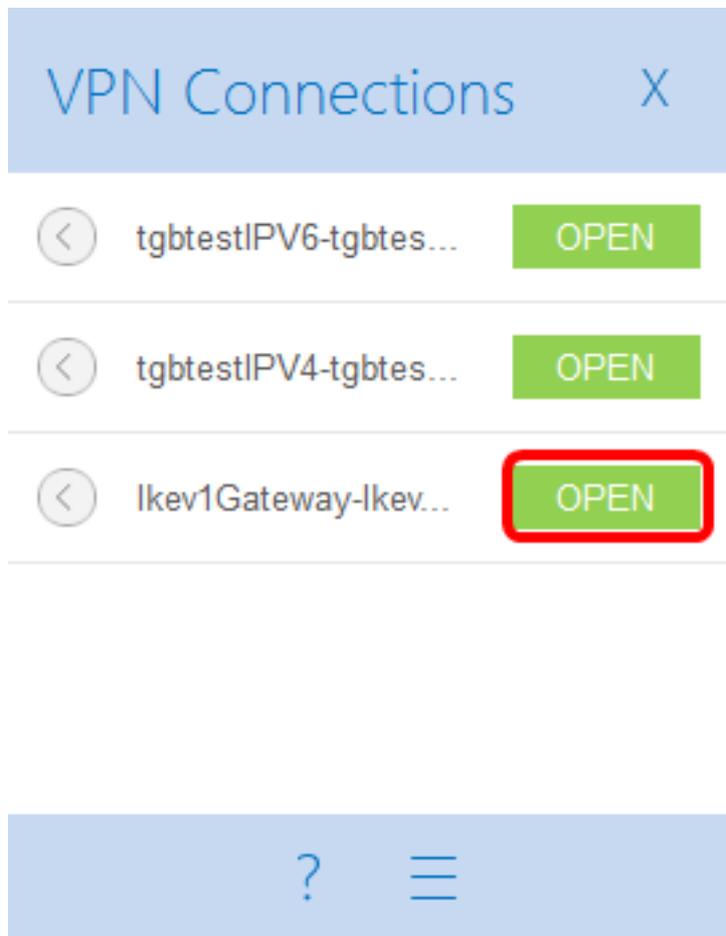
您现在应该已成功配置GreenBow VPN客户端，以通过VPN连接到RV34x系列路由器。

启动VPN连接

步骤1. 右键单击TheGreenBow VPN Client，然后选择“以管理员身份运行”。



步骤2.选择需要使用的VPN连接，然后单击**OPEN**。VPN连接应自动启动。

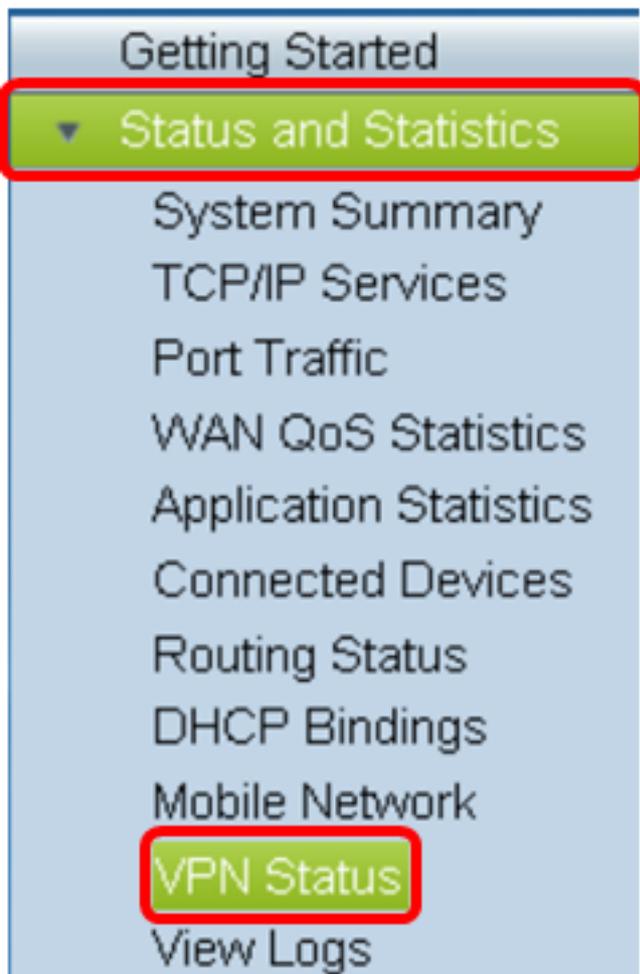


注意：在本例中，选择了已配置的Ikev1Gateway。

验证VPN状态

步骤1.登录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Client-to-Site Tunnel Status下，检查Connection Table的Connections列。

注意：在本例中，已建立一个VPN连接。

Connections
1

您现在应该已成功验证RV34x系列路由器上的VPN连接状态。GreenBow VPN客户端现在配置为通过VPN连接到路由器。