

配置Shrew Soft VPN客户端以连接到RV34X系列路由器

目标

本文档的目的是展示如何使用Shrew Soft VPN客户端连接到RV340系列路由器。

您可以从以下位置下载最新版本的Shrew Soft VPN客户端软件：

<https://www.shrew.net/download/vpn>

适用设备 | 软件版本

RV340 | 1.0.3.17 ([下载最新](#))

RV340W | 1.0.3.17(下载[最新版](#))

RV345 | 1.0.3.17(下载[最新版](#))

RV345P | 1.0.3.17(下载[最新版](#))

简介/使用案例

IPSec VPN (虚拟专用网络) 允许您通过在Internet上建立加密隧道来安全地获取远程资源。RV34X系列路由器用作IPSEC VPN服务器，并支持Shrew Soft VPN客户端。本指南将向您展示如何配置路由器和Shrew Soft Client以保护与VPN的连接。

本文档包含两部分：

配置RV340系列路由器

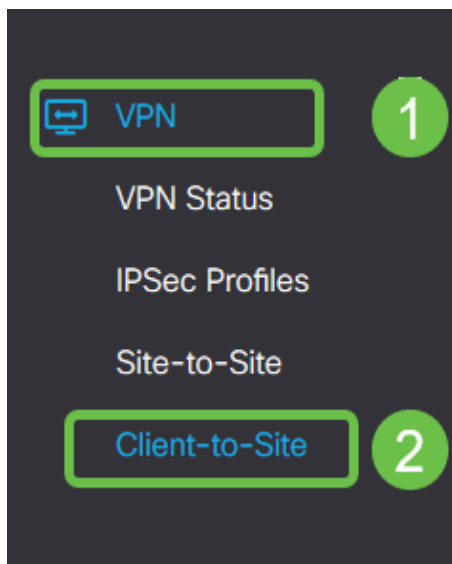
配置Shrew Soft VPN客户端

配置RV34X系列路由器：

首先，我们将在RV34x上配置客户端到站点VPN

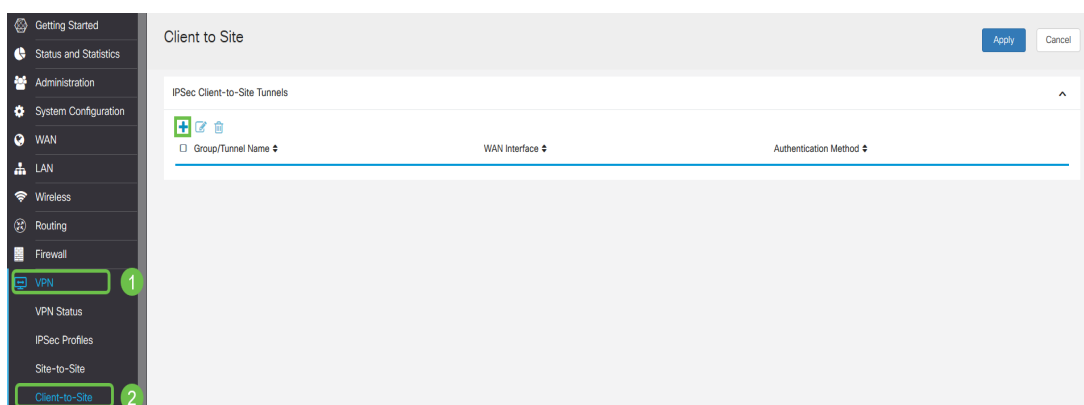
第 1 步

在VPN > Client-to-Site中，



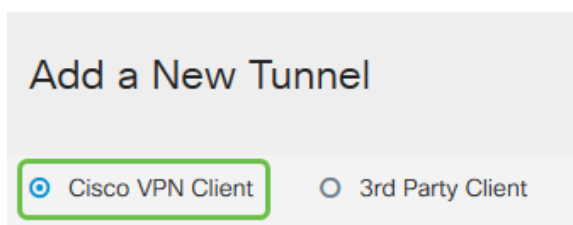
步骤 2

添加客户端到站点VPN配置文件



步骤 3

选择Cisco VPN Client选项。



步骤 4

选中Enable框，使VPN客户端配置文件处于活动状态。我们还将配置组名称，选择WAN接口，并输入预共享密钥。

注意： 请注意组名和预共享密钥，它们稍后将在配置客户端时使用。

Enable:

Group Name:

Interface:

IKE Authentication Method

Pre-shared Key:

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

步骤 5

暂时将**用户组表**留空。这是用于**路由器**上的用户组，但我们尚未对其进行配置。确保**模式**设置为**客户端**。输入**客户端LAN的池范围**。我们将使用172.16.10.1到172.16.10.10。

注意：池范围应使用网络中其他位置未使用的唯一子网。

User Group:

User Group Table

+

Group Name

Mode: Client NEM

Pool Range for Client LAN

Start IP:

End IP:

步骤 6

此处是配置**模式配置设置**的位置。我们将使用以下设置：

主 DNS 服务器：如果您有内部DNS服务器或想使用外部DNS服务器，可以在此处输入。否则，默认设置为RV340 LAN IP地址。我们将在示例中使用默认值。

分割隧道：选中以启用分割隧道。这用于指定哪些流量将通过VPN隧道。我们将在示例中使用分割隧道。

拆分隧道表：输入VPN客户端应通过VPN访问的网络。本示例使用RV340 LAN网络。

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

步骤 7

单击**Save**后，我们可以在IPSec Client-to-Site Groups列表中看到Profile。

Client to Site

IPSec Client-to-Site Tunnels

Group/Tunnel Name	WAN Interface	Authentication Method
Clients	WAN1	Pre-shared Key

步骤 8

现在，我们将配置用于验证VPN客户端用户的用户组。在**系统配置 > 用户组**中，单击“+”以添加用户组。

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- System
- Time
- Log
- Email
- User Accounts
- User Groups

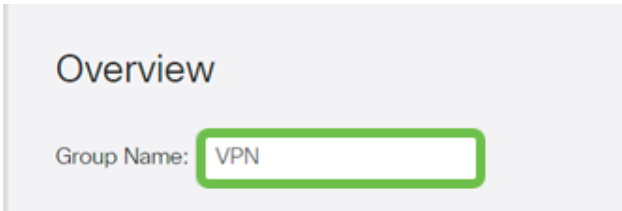
User Groups

User Groups Table

Group	Web Login/NETCONF/RESTCONF
admin	Admin
guest	Disabled

步骤 9

输入组名称。

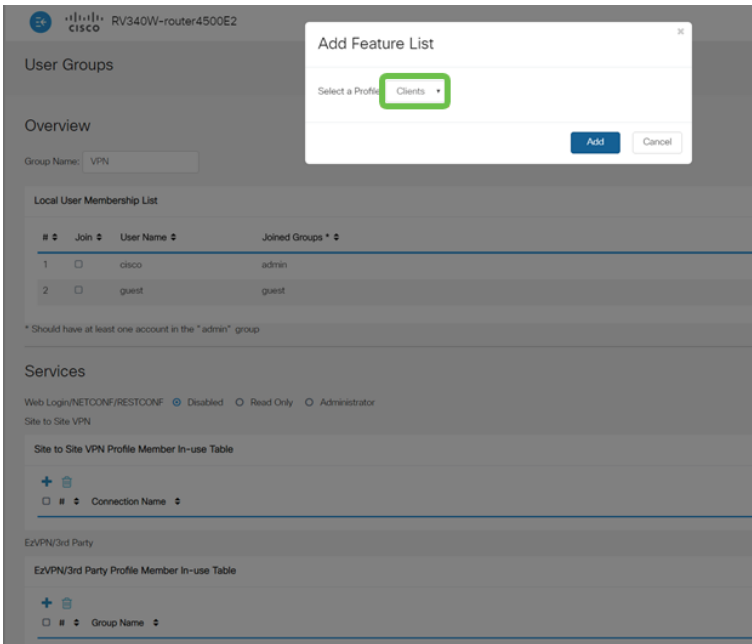


Overview

Group Name:

步骤 10

在**Services**部分 > **EzVPN/第3方**中，单击**Add** 将此用户组链接到之前配置的**客户端到站点配置文件**。



RV340W-router4500E2

User Groups

Overview

Group Name: VPN

Local User Membership List

#	Join	User Name	Joined Groups
1	<input type="checkbox"/>	cisco	admin
2	<input type="checkbox"/>	guest	guest

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

Services

Web Login/NETCONF/RESTCONF Disabled Read Only Administrator

Site to Site VPN

Site to Site VPN Profile Member In-use Table

#	Connection Name
---	-----------------

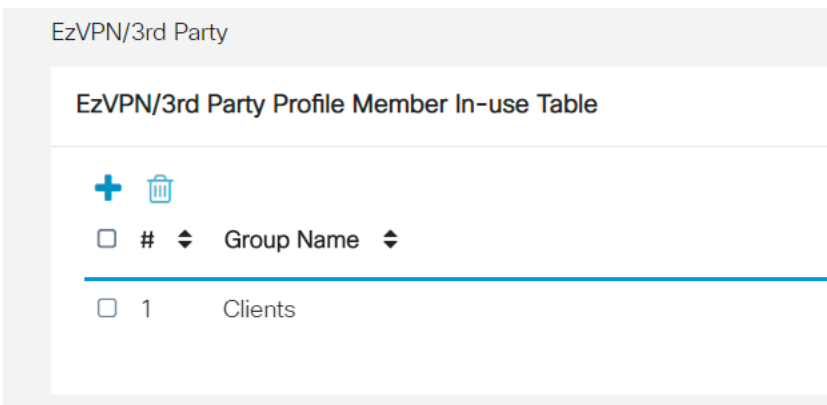
EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

#	Group Name
---	------------

步骤 11

您现在应该在**EzVPN/第三方的**列表中看到“**客户端到站点组名称**”



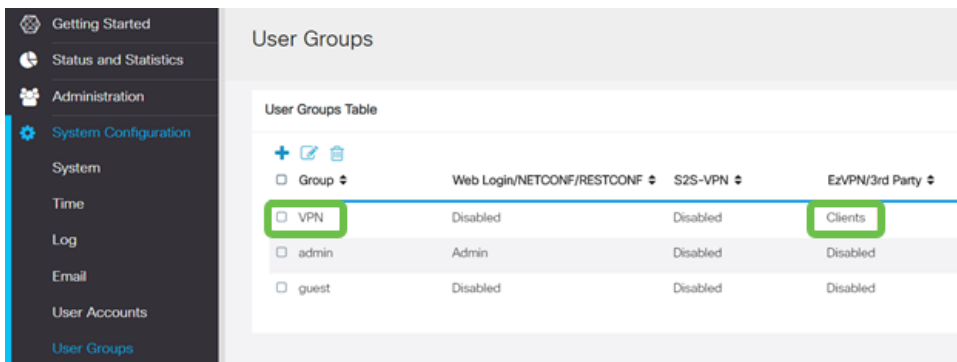
EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

#	Group Name
1	Clients

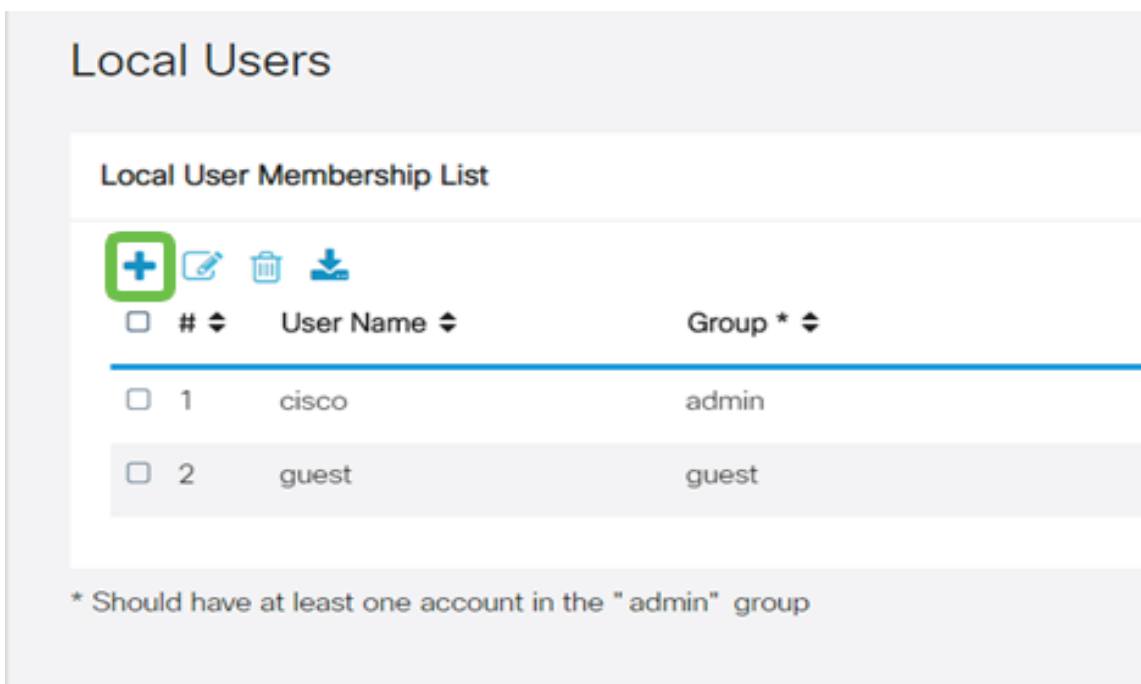
步骤 12

应用用户组配置后，您将在**用户组**列表中看到该配置，并显示新用户组将与我们之前创建的**客户端到站点配置文件**一起使用。



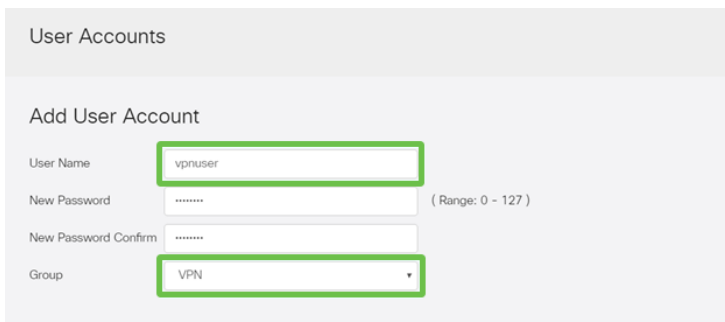
步骤 13

现在，我们将在“系统配置”(System Configuration)>“用户帐户”(User Accounts)中配置新用户。单击 '+' 创建新用户。



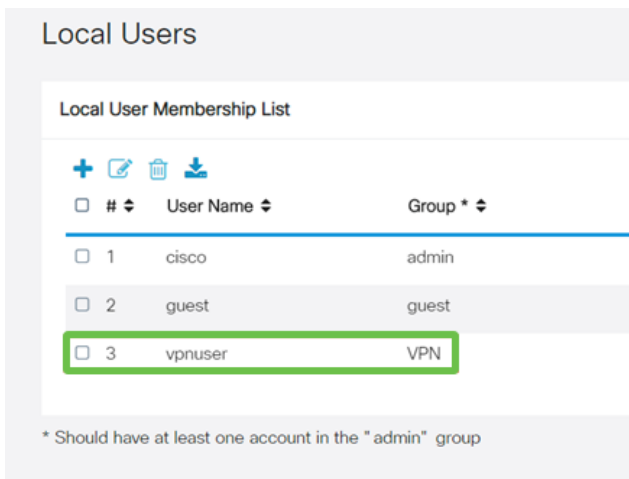
步骤 14

输入新用户名和新密码。验证组已设置为我们刚配置的新用户组。完成后单击“应用”。



步骤 15

新用户将显示在本地用户列表中。



RV340系列路由器的配置完成。现在，我们将配置Shrew Soft VPN客户端。

配置ShrewSoft VPN客户端

现在，我们将配置Shrew Soft VPN客户端。

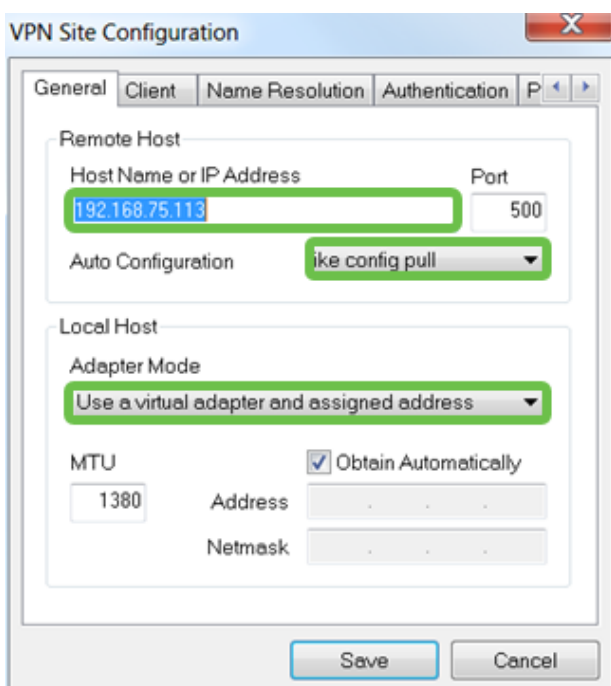
第 1 步

打开ShrewSoft VPN Access Manager，然后单击“添加”添加配置文件。在显示的VPN Site Configuration窗口中，配置General选项卡：

主机名或 IP 地址:使用WAN IP地址 (或RV340的主机名)

自动配置:选择ike config pull

适配器模式:选择使用虚拟适配器和分配的地址



步骤 2

配置“客户端”选项卡。我们只使用默认设置。

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. The 'Firewall Options' section is expanded, showing the following settings:

- NAT Traversal: enable
- NAT Traversal Port: 4500
- Keep-alive packet rate: 15 Secs
- IKE Fragmentation: enable
- Maximum packet size: 540 Bytes

The 'Other Options' section is also expanded, showing the following checked options:

- Enable Dead Peer Detection
- Enable ISAKMP Failure Notifications
- Enable Client Login Banner

At the bottom of the dialog box, there are 'Save' and 'Cancel' buttons.

步骤 3

在“名称解析”选项卡> DNS选项卡中，选中启用DNS框，并保持选中自动获取框。

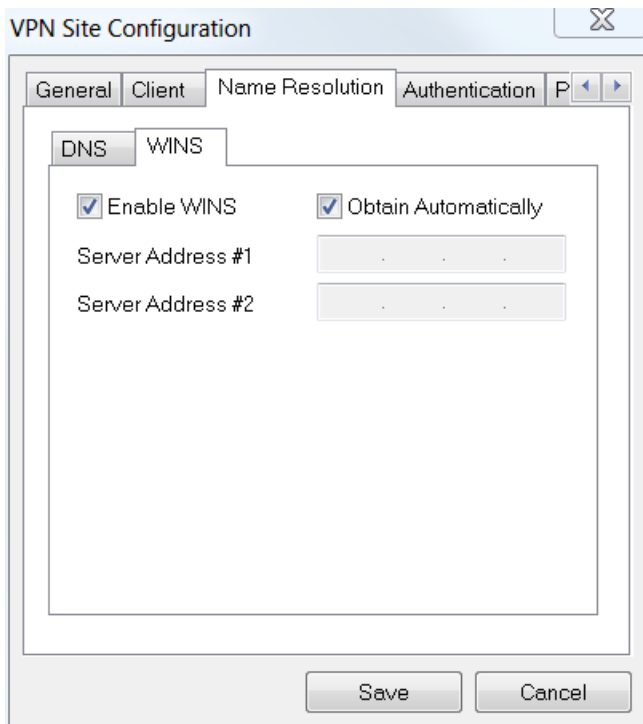
The screenshot shows the 'VPN Site Configuration' dialog box with the 'Name Resolution' tab selected. The 'DNS' sub-tab is active, showing the following settings:

- Enable DNS
- Obtain Automatically
- Server Address #1: . . .
- Server Address #2: . . .
- Server Address #3: . . .
- Server Address #4: . . .
- Obtain Automatically
- DNS Suffix:

At the bottom of the dialog box, there are 'Save' and 'Cancel' buttons.

步骤 4

在“名称解析”选项卡> WINS选项卡中，选中启用WINS框，并保持选中自动获取框。

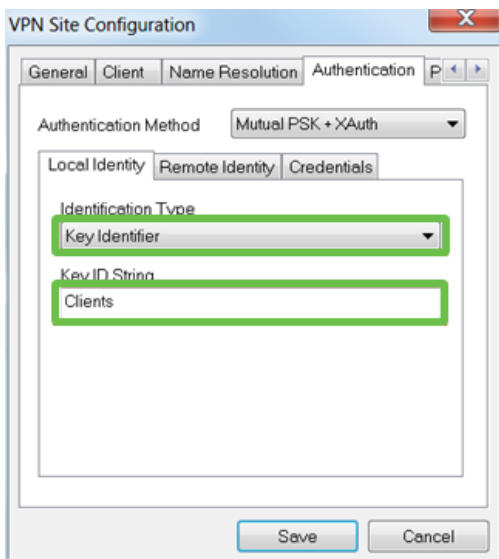


步骤 5

配置“身份验证”选项卡>“本地身份”选项卡：

标识类型:选择密钥标识符

密钥ID字符串:输入在RV34x上配置的组名



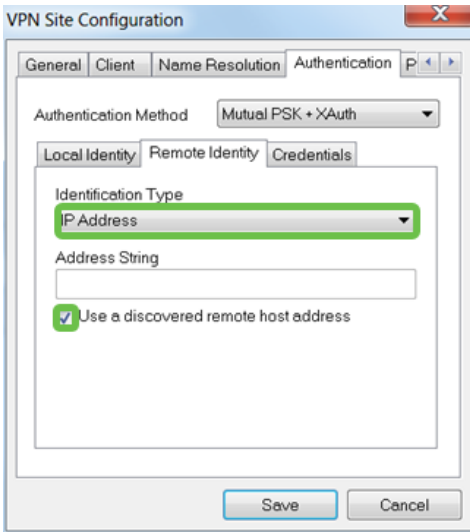
步骤 6

在“身份验证”选项卡>“远程身份”选项卡中，我们将保留默认设置。

标识类型:IP Address

地址字符串:<blank>

使用已发现的远程主机地址框：已选中

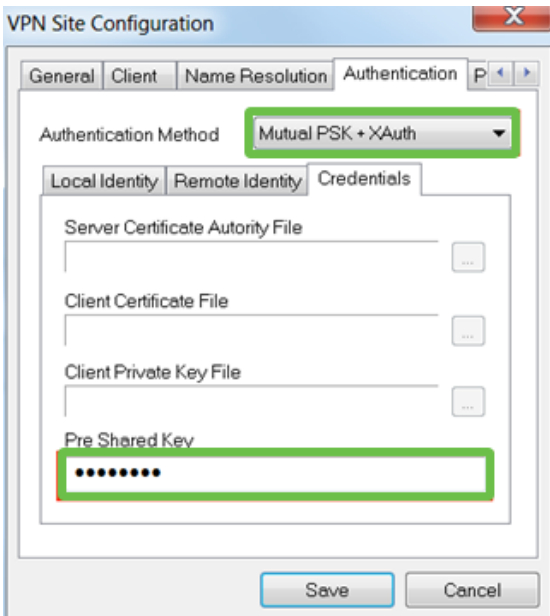


步骤 7

在“身份验证”选项卡>“凭证”选项卡中，配置以下内容：

认证方法:选择Mutual PSK +扩展验证

预共享密钥:输入在RV340客户端配置文件中配置的预共享密钥



步骤 8

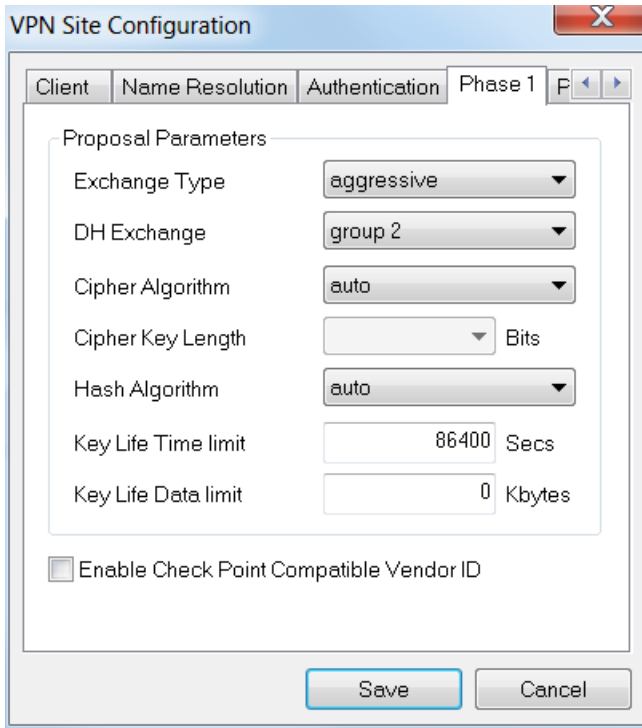
对于“第1阶段”(Phase 1)选项卡，我们将保留默认设置：

交换类型：攻击性

DH交换：第 2 组

密码算法：自动

散列算法:自动



步骤 9

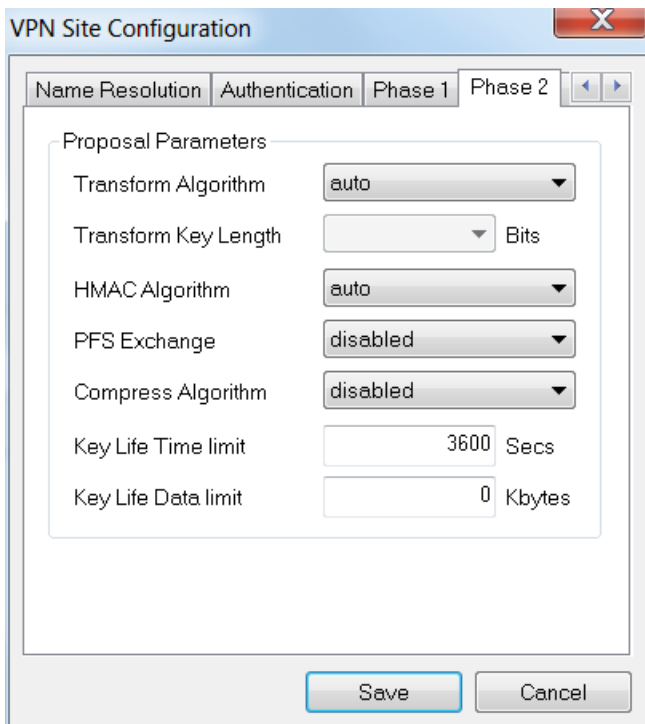
我们还将使用“第2阶段”(Phase 2)选项卡的默认值：

转换算法：自动

HMAC算法：自动

PFS交换：禁用

压缩算法：禁用



步骤 10

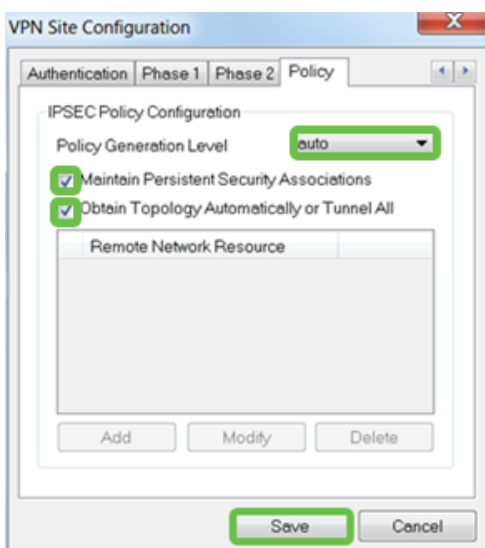
对于Policy选项卡，我们将使用以下设置：

策略生成级别：自动

维护持续安全关联：已选中

自动获取拓扑或全部隧道：已选中

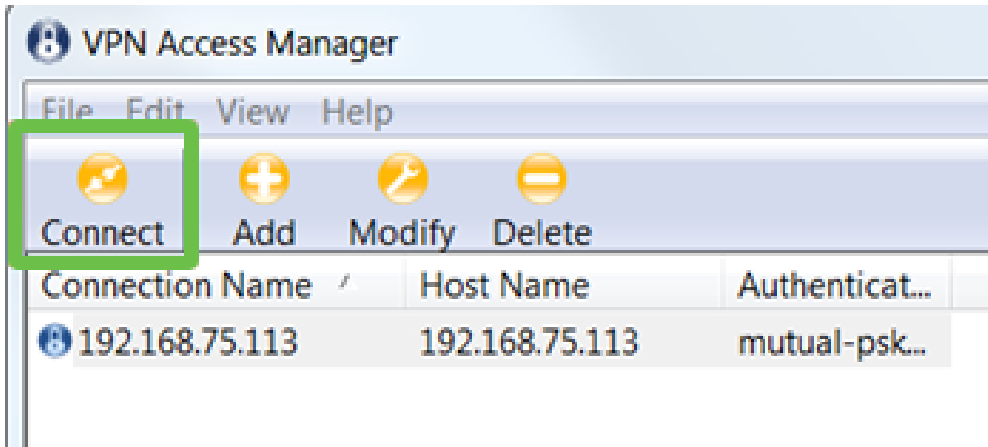
由于我们在RV340上配置了分割隧道，因此我们无需在此处进行配置。



完成后，单击 Save（保存）。

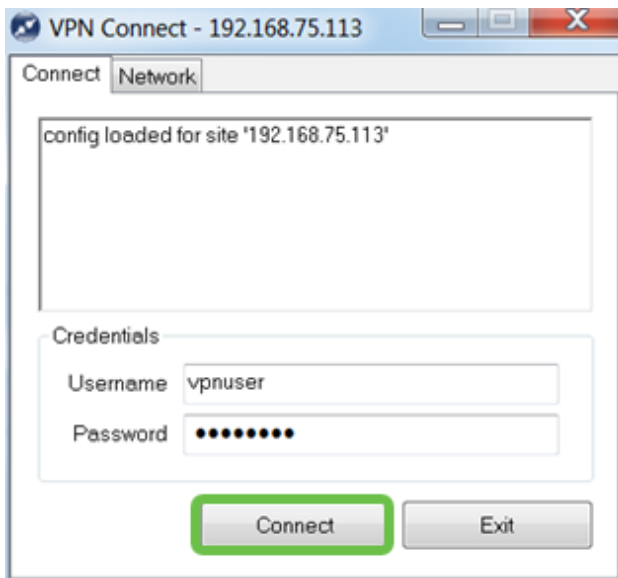
步骤 11

现在，我们已准备好测试连接。在“VPN Access Manager(VPN访问管理器)”中，突出显示连接配置文件并单击“Connect(连接)”按钮。



步骤 12

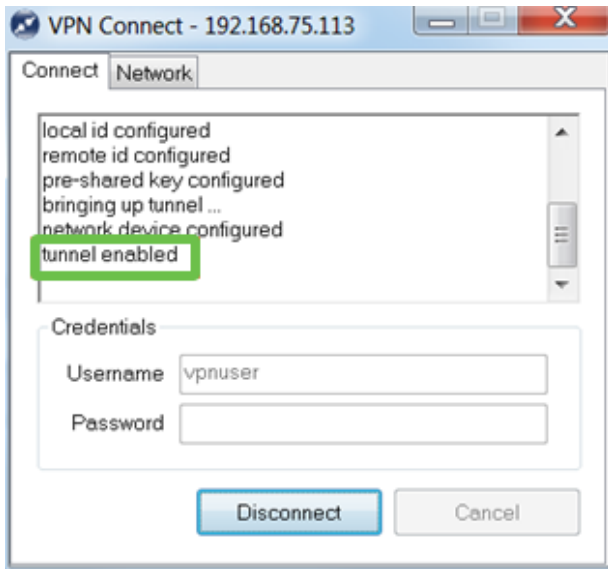
在出现的VPN Connect窗口中，使用我们在RV340上创建的用户帐户的凭证输入用户名和密码（步骤13和14）。



完成后，单击Connect。

步骤 13

验证隧道是否已连接。您应该看到隧道已启用。



结论

现在，您已设置通过VPN连接到网络。