Konfigurieren des Shrew Soft VPN-Clients für die Verbindung mit dem Router der Serie RV34X

Ziel

Dieses Dokument soll zeigen, wie der Shrew Soft VPN-Client für die Verbindung mit einem Router der Serie RV340 verwendet wird.

Sie können die neueste Version der Shrew Soft VPN-Clientsoftware hier herunterladen:

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

Unterstützte Geräte | Softwareversion

RV340 | 1.0.3.17 (neueste Version herunterladen)

RV340 W | 1.0.3.17 (neueste Version herunterladen)

RV345 | 1.0.3.17 (neueste Version herunterladen)

RV345P | 1.0.3.17 (neueste Version herunterladen)

Einführung/Anwendungsfall

Mit IPSec VPN (Virtual Private Network) können Sie Remote-Ressourcen sicher abrufen, indem Sie einen verschlüsselten Tunnel im Internet einrichten. Die Router der Serie RV34X fungieren als IPSEC VPN-Server und unterstützen den Shrew Soft VPN-Client. Dieser Leitfaden zeigt Ihnen, wie Sie Ihren Router und den Shrew Soft Client konfigurieren, um eine Verbindung mit einem VPN zu sichern.

Dieses Dokument besteht aus zwei Teilen:

Konfigurieren des Routers der Serie RV340

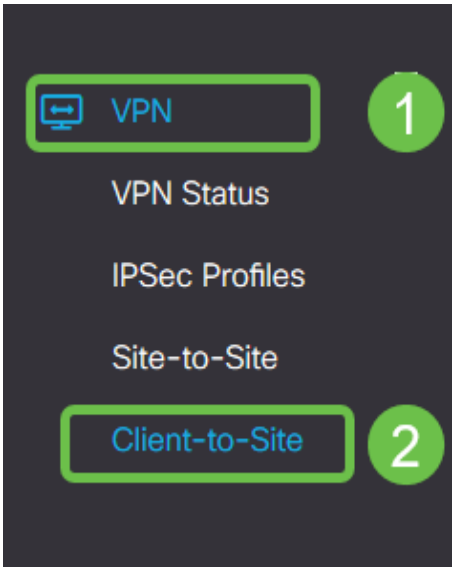
Konfigurieren des Shrew Soft VPN-Clients

Konfigurieren des Routers der Serie RV34X:

Zunächst konfigurieren Sie das **Client-to-Site-VPN** auf dem RV34x.

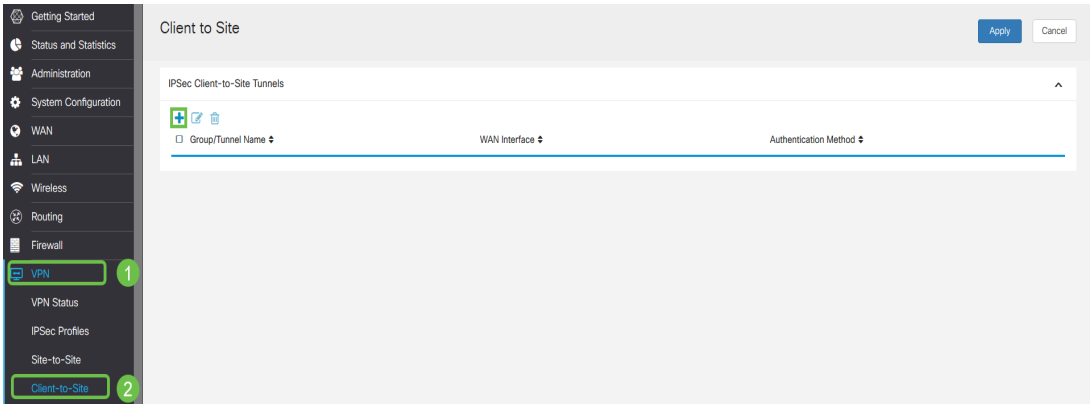
Schritt 1

In **VPN > Client-to-Site**,



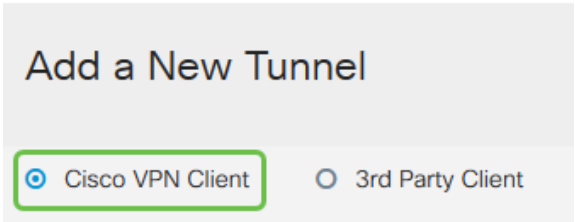
Schritt 2

Hinzufügen eines **Client-to-Site**-VPN-Profils



Schritt 3

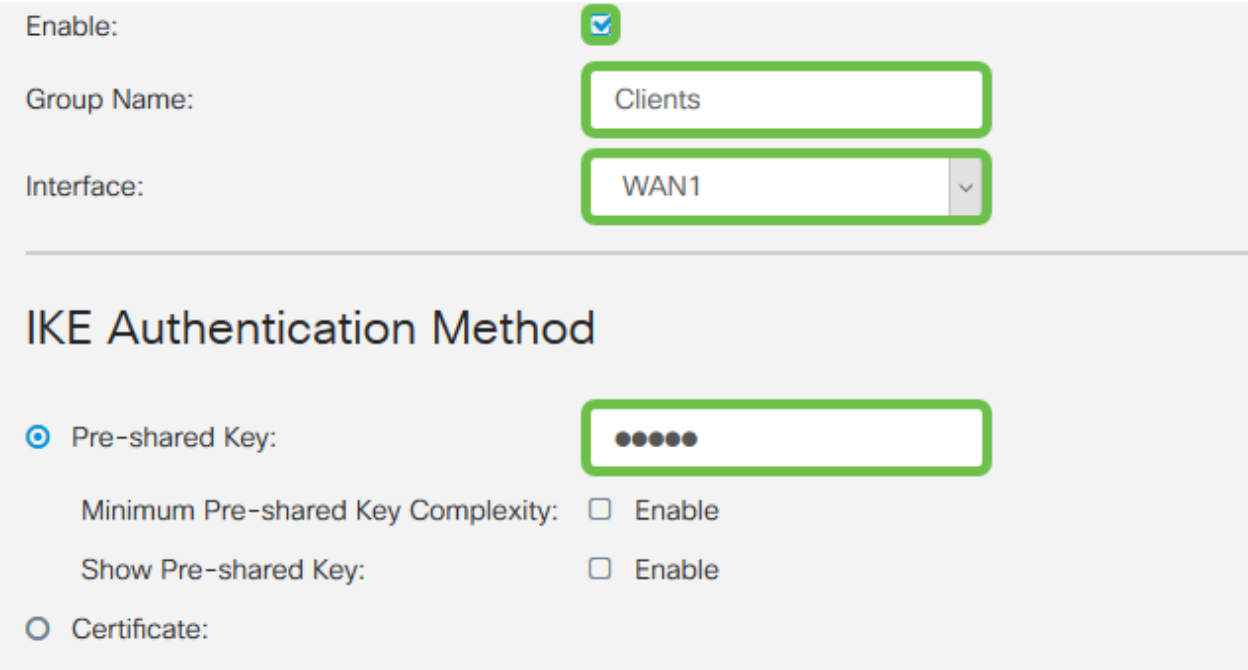
Wählen Sie die Option **Cisco VPN Client** aus.



Schritt 4

Aktivieren Sie das **Kontrollkästchen Aktivieren**, um das VPN-Clientprofil zu aktivieren. Außerdem konfigurieren Sie den *Gruppennamen*, wählen die **WAN-Schnittstelle aus** und geben einen **Pre-shared Key ein**.

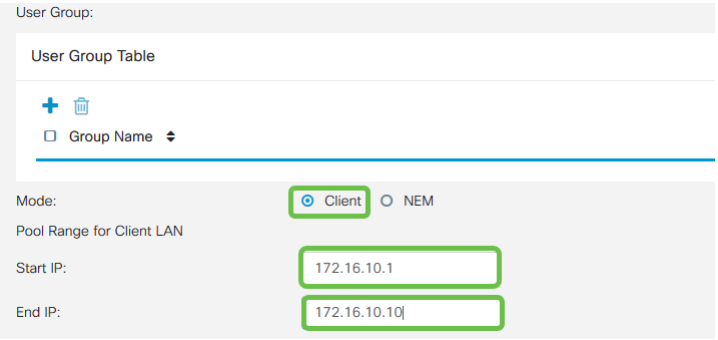
Hinweis: Beachten Sie den *Gruppennamen* und den *vorinstallierten Schlüssel*, die bei der Konfiguration des Clients später verwendet werden.



Schritt 5

Lassen Sie die **Benutzergruppentabelle** jetzt leer. Dies gilt für die *Benutzergruppe* auf dem Router, wurde jedoch noch nicht konfiguriert. Stellen Sie sicher, dass der **Modus** auf **Client** eingestellt ist. Geben Sie den **Pool-Bereich für Client-LAN ein**. Wir verwenden die Nummern 172.16.10.1 bis 172.16.10.10.

Hinweis: Der Pool-Bereich sollte ein eindeutiges Subnetz verwenden, das an keiner anderen Stelle im Netzwerk verwendet wird.



Schritt 6

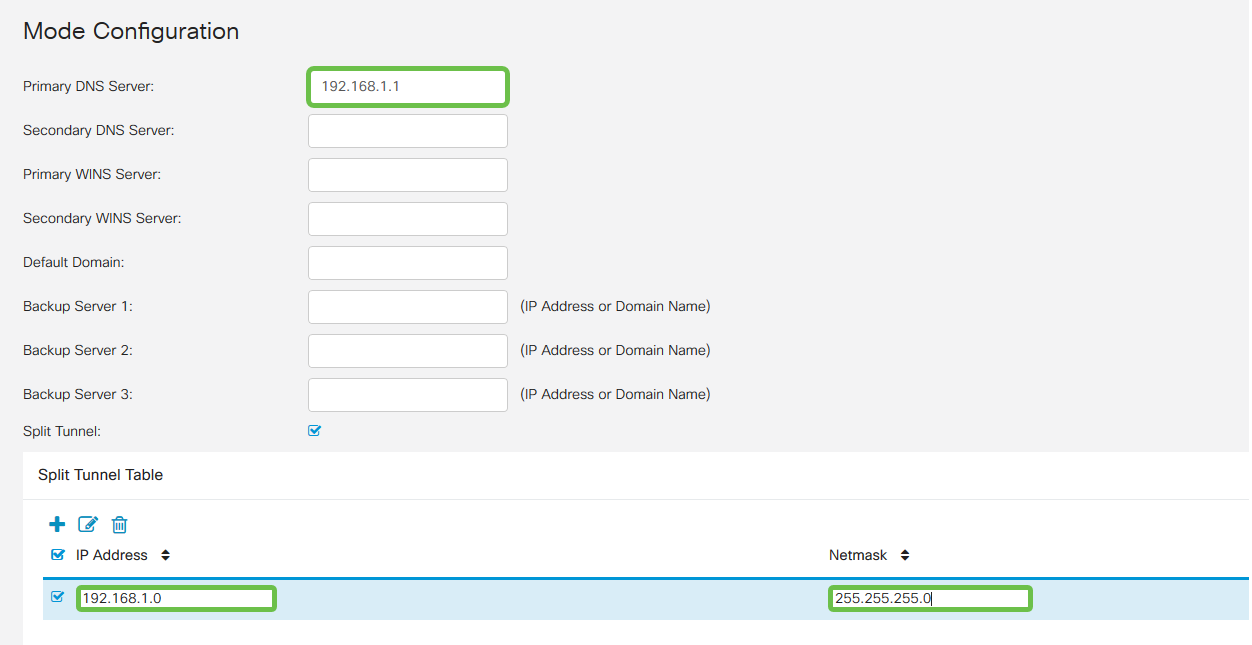
Hier konfigurieren Sie die Einstellungen für die **Moduskonfiguration**. Hier sind die Einstellungen, die wir verwenden werden:

Primärer DNS-Server: Wenn Sie einen internen DNS-Server haben oder einen externen DNS-Server verwenden möchten, können Sie diesen hier eingeben. Andernfalls wird der Standardwert auf die RV340 LAN-IP-Adresse festgelegt. In unserem Beispiel verwenden wir die Standardeinstellung.

Split-Tunnel: Aktivieren Sie Split Tunneling. Mit diesem Parameter wird festgelegt, welcher

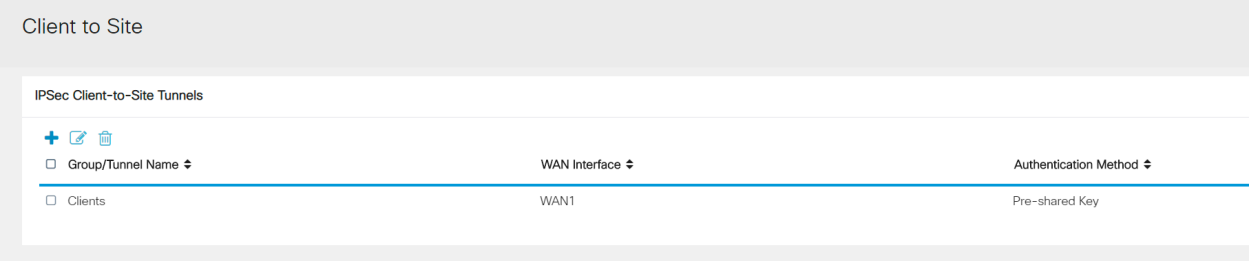
Datenverkehr über den VPN-Tunnel geleitet wird. In unserem Beispiel wird Split Tunnel verwendet.

Tunneltabelle aufteilen: Geben Sie die Netzwerke ein, auf die der VPN-Client über das VPN zugreifen soll. In diesem Beispiel wird das LAN-Netzwerk RV340 verwendet.



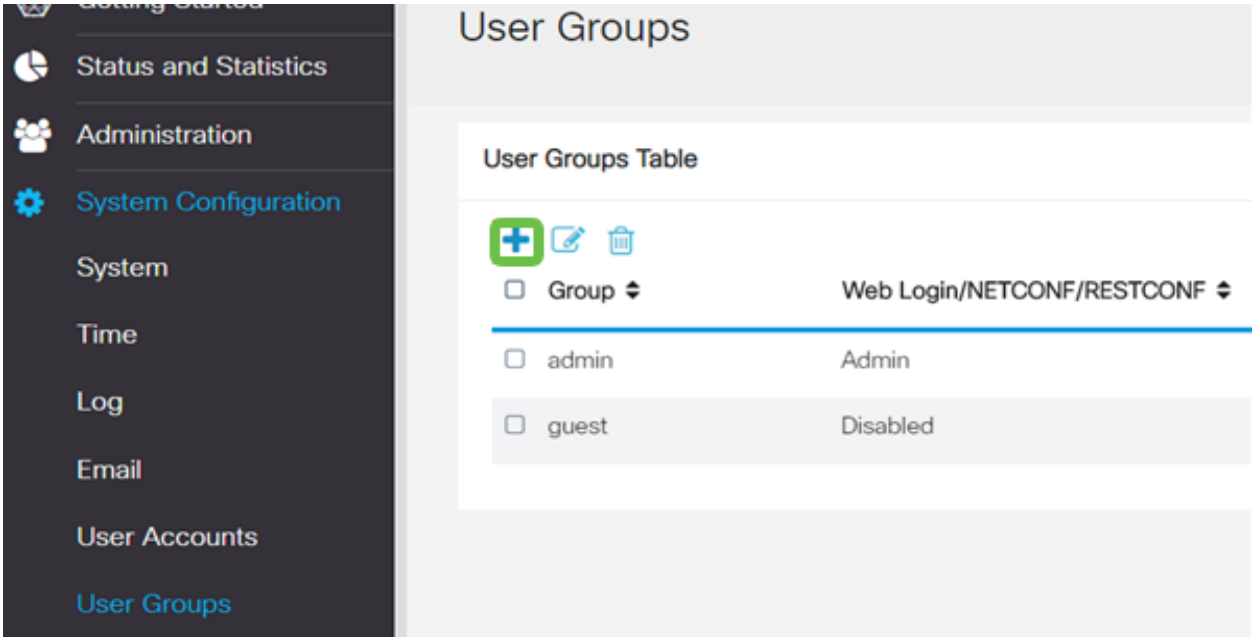
Schritt 7

Wenn Sie auf **Speichern** klicken, wird das Profil in der Liste **IPSec-Client-to-Site-Gruppen** angezeigt.



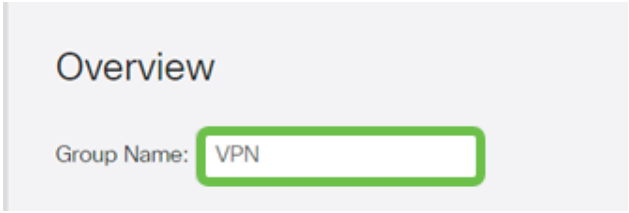
Schritt 8

Wir konfigurieren nun eine **Benutzergruppe** für die Authentifizierung von VPN-Client-Benutzern. Klicken Sie unter **Systemkonfiguration > Benutzergruppen** auf ", um eine Benutzergruppe hinzuzufügen.



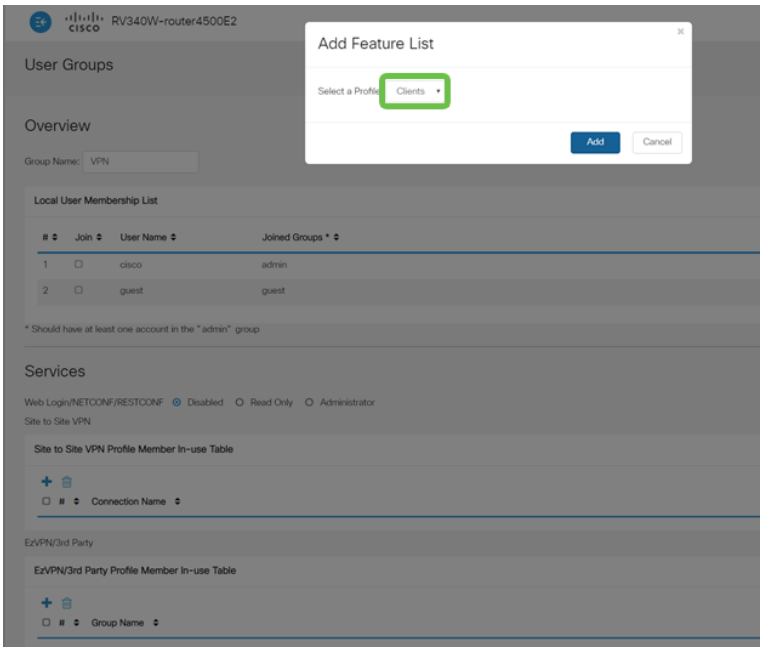
Schritt 9

Geben Sie einen **Gruppennamen ein**.



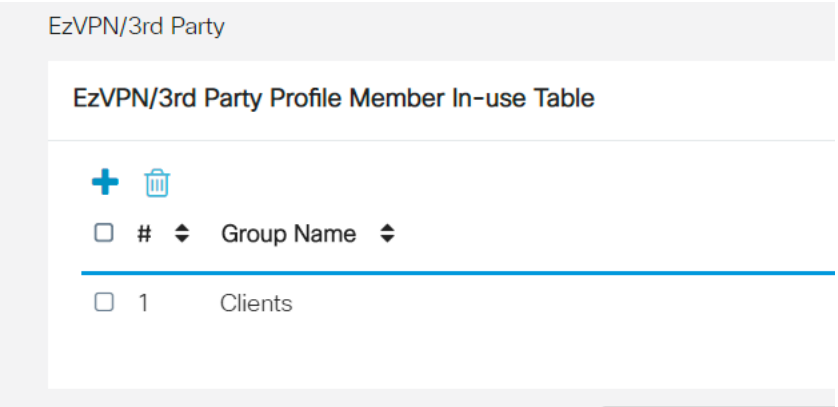
Schritt 10

Klicken Sie im **Services**-Abschnitt > **EzVPN/Drittanbieter** auf **Hinzufügen**, um diese Benutzergruppe mit dem **Client-to-Site**-Profil zu verknüpfen, das Sie zuvor konfiguriert haben.



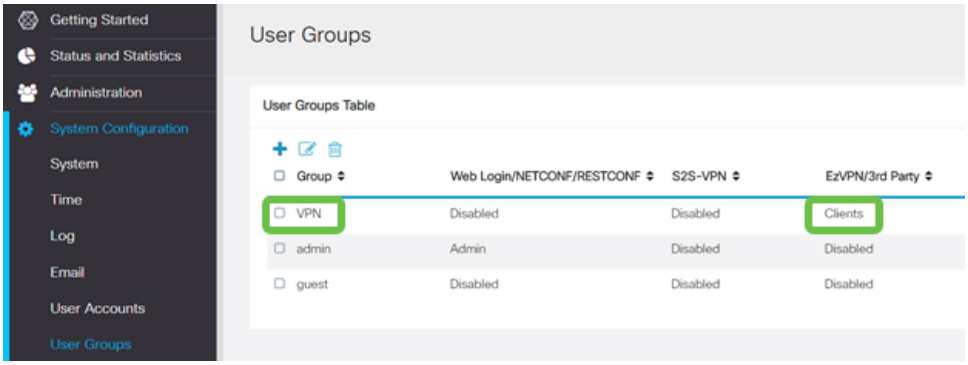
Schritt 11

Sie sollten nun den **Client-to-Site-**Gruppennamen in der Liste für **EzVPN/Drittanbieter** sehen.



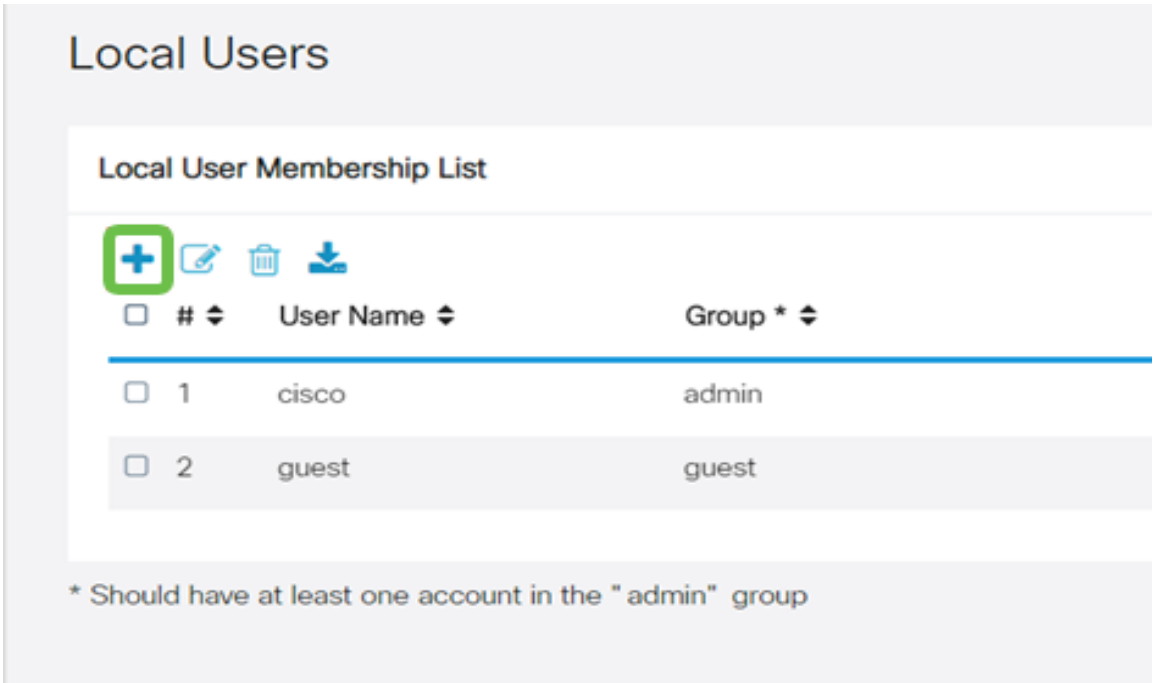
Schritt 12

Nachdem Sie die Benutzergruppenkonfiguration **angewendet** haben, wird diese in der Liste **Benutzergruppen** angezeigt. Die neue Benutzergruppe wird mit dem zuvor erstellten Client-to-Site-Profil verwendet.



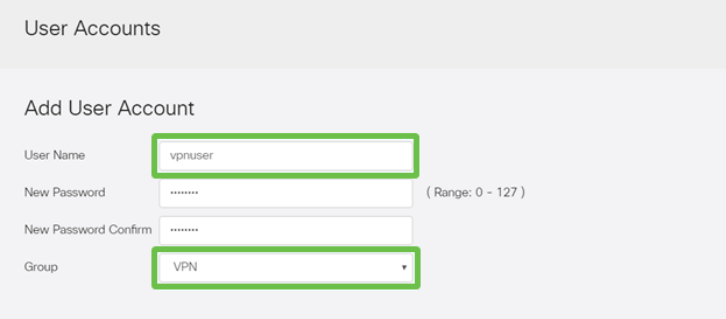
Schritt 13

Jetzt konfigurieren Sie einen neuen Benutzer in **Systemkonfiguration** > **Benutzerkonten**. Klicken Sie auf **"+"**, um einen neuen Benutzer zu erstellen.



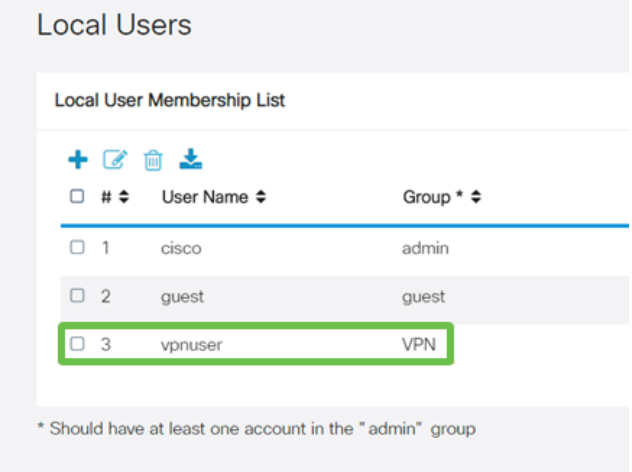
Schritt 14

Geben Sie den neuen **Benutzernamen** zusammen mit dem **neuen Kennwort ein**. Überprüfen Sie, ob die **Gruppe** auf die neue soeben konfigurierte **Benutzergruppe** eingestellt ist. Klicken Sie abschließend auf **Übernehmen**.



Schritt 15

Der neue **Benutzer** wird in der Liste der **lokalen Benutzer** angezeigt.



Damit ist die Konfiguration des Routers der Serie RV340 abgeschlossen. Jetzt wird der Shrew Soft VPN-Client konfiguriert.

Konfigurieren des ShrewSoft VPN-Clients

Jetzt wird der Shrew Soft VPN-Client konfiguriert.

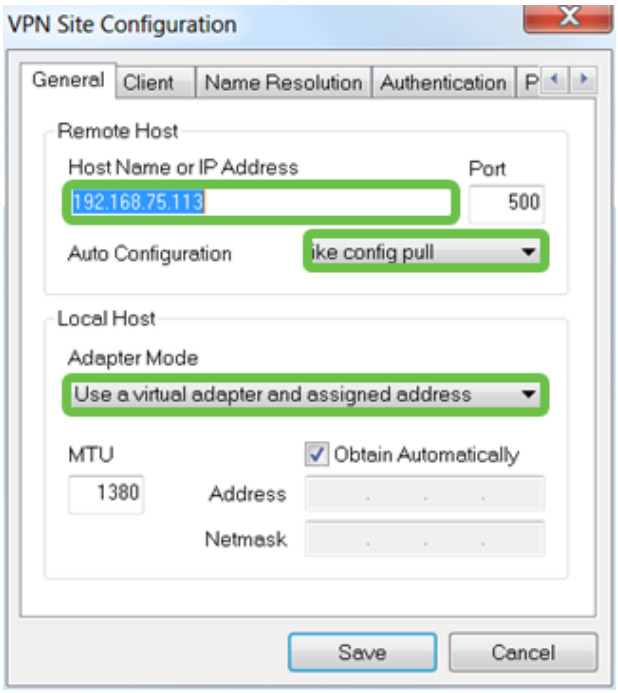
Schritt 1

Öffnen Sie den ShrewSoft *VPN Access Manager*, und klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen. Im sich öffnenden Fenster *VPN Site Configuration* konfigurieren Sie die Registerkarte **General**:

Hostname oder IP-Adresse: Verwenden Sie die WAN-IP-Adresse (oder den Hostnamen des RV340).

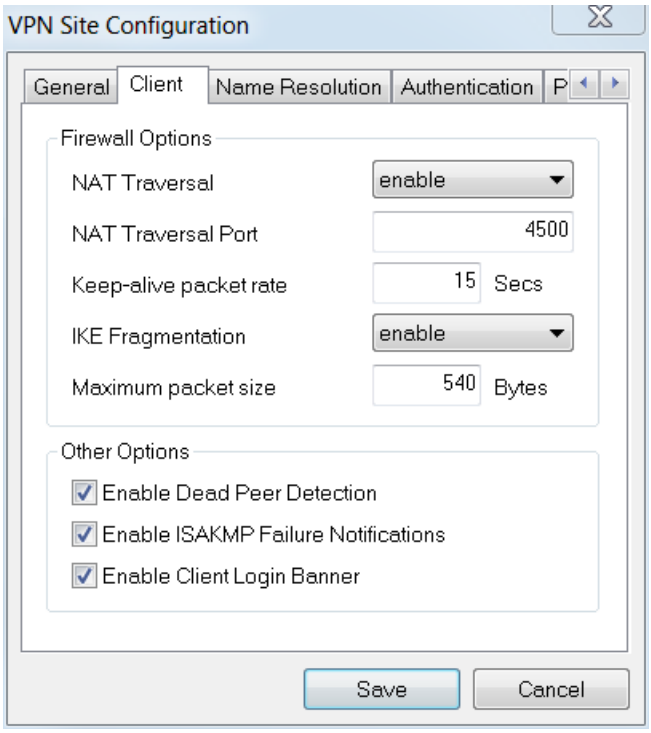
Automatische Konfiguration: Wählen Sie **die Option Konfigurationsanfrage aus.**

Adaptermodus: Wählen Sie **Einen virtuellen Adapter und zugewiesene Adresse verwenden.**



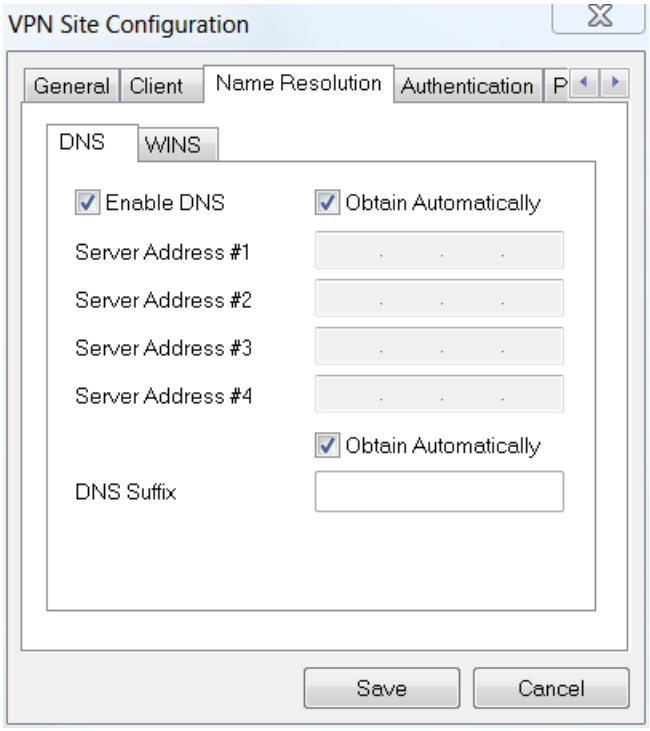
Schritt 2

Konfigurieren Sie die Registerkarte **Client**. Wir verwenden nur die Standardeinstellungen.



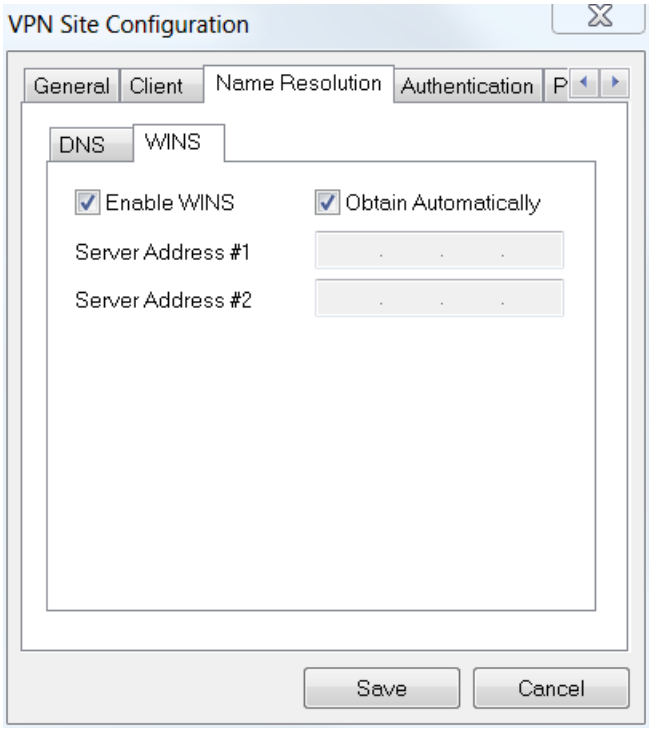
Schritt 3

Aktivieren Sie auf der Registerkarte **Namensauflösung > DNS** das **Kontrollkästchen DNS aktivieren,** und lassen Sie die **Kontrollkästchen Automatisch beziehen** aktiviert.



Schritt 4

Aktivieren Sie auf der Registerkarte **Namensauflösung > WINS** das **Kontrollkästchen WINS aktivieren,** und lassen Sie das **Kontrollkästchen Automatisch beziehen** aktiviert.



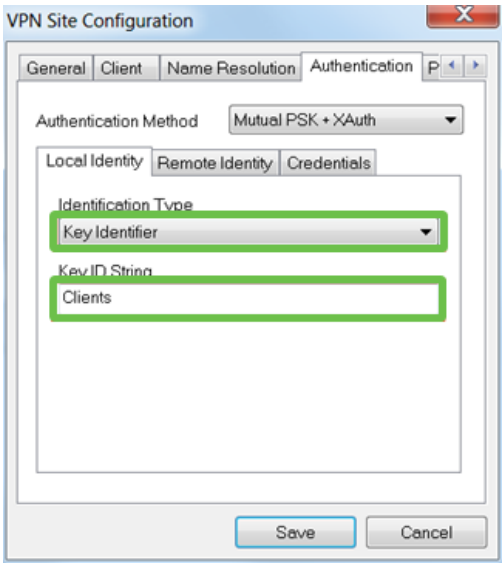
Schritt 5

Konfigurieren Sie die Registerkarte **Authentifizierung > Lokale Identität**:

Identifizierungstyp: **Schlüsselkennung** auswählen

Schlüssel-ID-Zeichenfolge: Geben Sie den **Gruppennamen ein**, der auf dem RV34x

konfiguriert wurde.



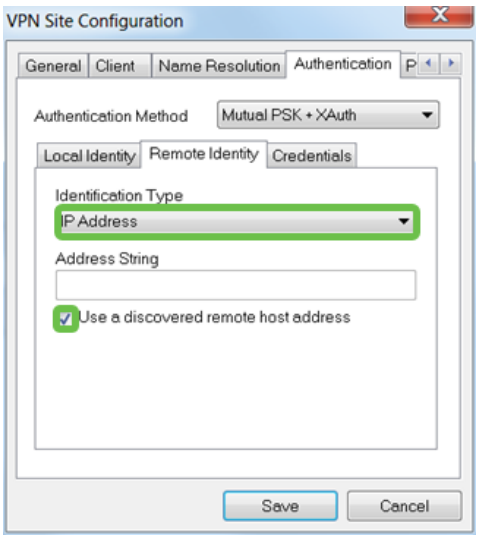
Schritt 6

Im Register **Authentifizierung** > **Remote Identity** bleiben die Standardeinstellungen unverändert.

Identifizierungstyp: IP-Adresse

Adresszeichenfolge: <leer>

Verwenden Sie ein erkanntes Adressfeld **des Remotehosts**: Aktiviert

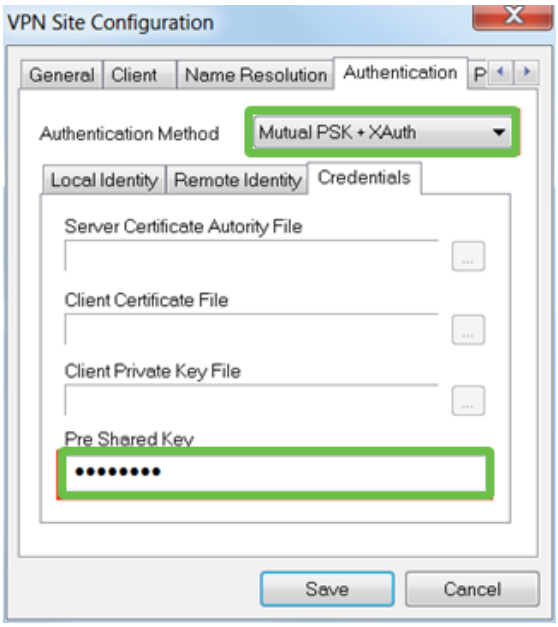


Schritt 7

Konfigurieren Sie auf der Registerkarte **Authentifizierung** > **Anmeldeinformationen** Folgendes:

Authentifizierungsmethode: Wählen Sie **Mutual PSK + XAuth aus**

Vorinstallierter Schlüssel: Geben Sie den im RV340-Clientprofil konfigurierten **Preshared Key** ein.



Schritt 8

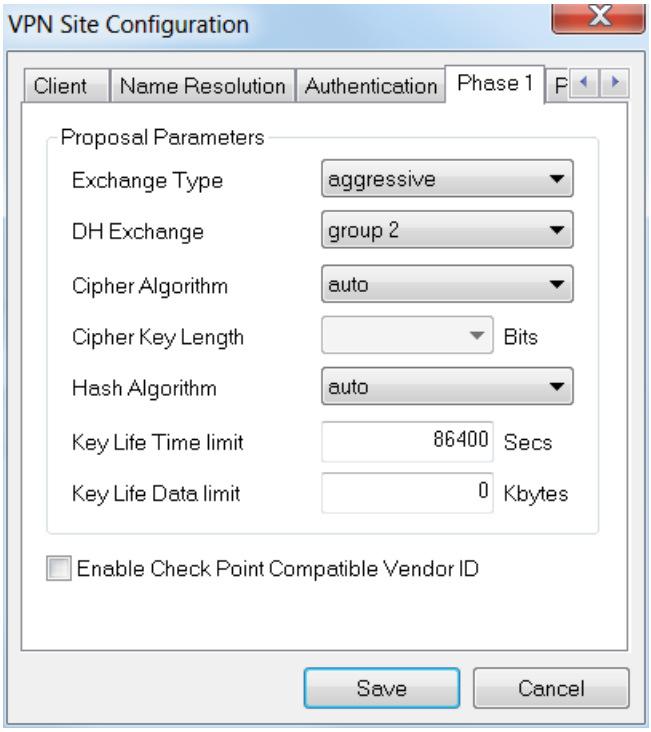
Für die Registerkarte **Phase 1** bleiben die Standardeinstellungen unverändert:

Exchange-Typ: aggressiv

DH Exchange: Gruppe 2

Verschlüsselungsalgorithmus: Automatisch

Hash-Algorithmus: Automatisch



Schritt 9

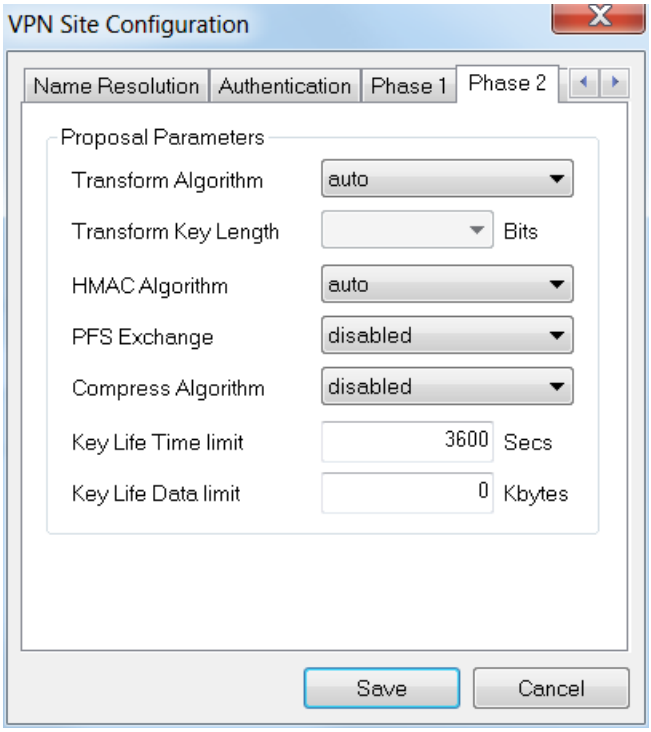
Außerdem werden die Standardwerte für die Registerkarte **Phase 2** verwendet:

Transform Algorithm: Automatisch

HMAC-Algorithmus: Automatisch

PFS Exchange: Deaktiviert

Komprimierungsalgorithmus: Deaktiviert



Schritt 10

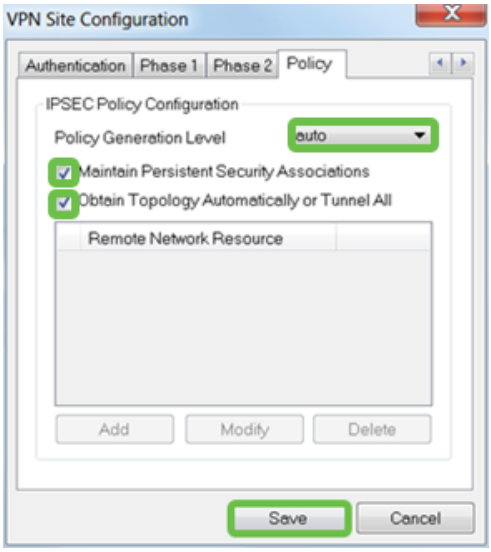
Für die Registerkarte **Richtlinien** verwenden wir die folgenden Einstellungen:

Ebene der Richtliniengenerierung: Automatisch

Beibehalten von permanenten Sicherheitszuordnungen: Aktiviert

Topologie automatisch abrufen oder Alle tunneln: Aktiviert

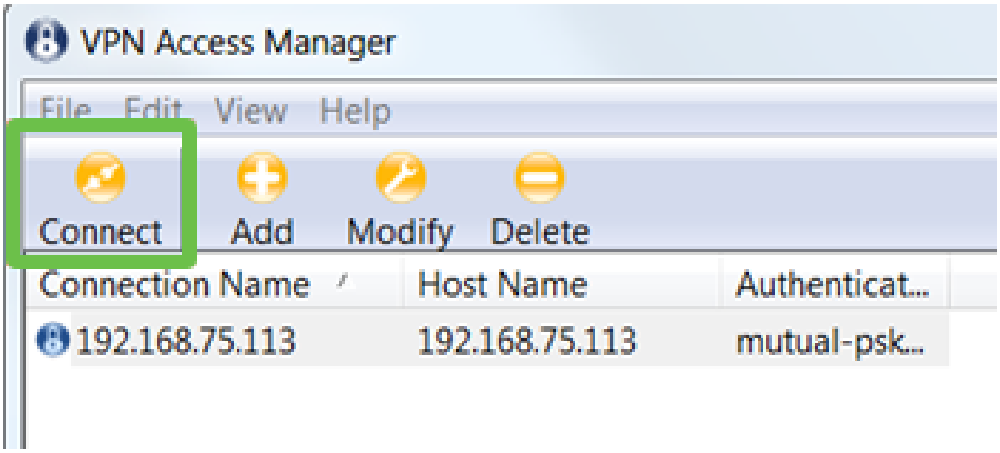
Da **Split-Tunneling** auf dem RV340 konfiguriert wurde, muss er hier nicht konfiguriert werden.



Klicken Sie abschließend auf **Speichern**.

Schritt 11

Jetzt können wir die Verbindung testen. Markieren Sie im *VPN Access Manager* das Verbindungsprofil, und klicken Sie auf die Schaltfläche **Connect**.



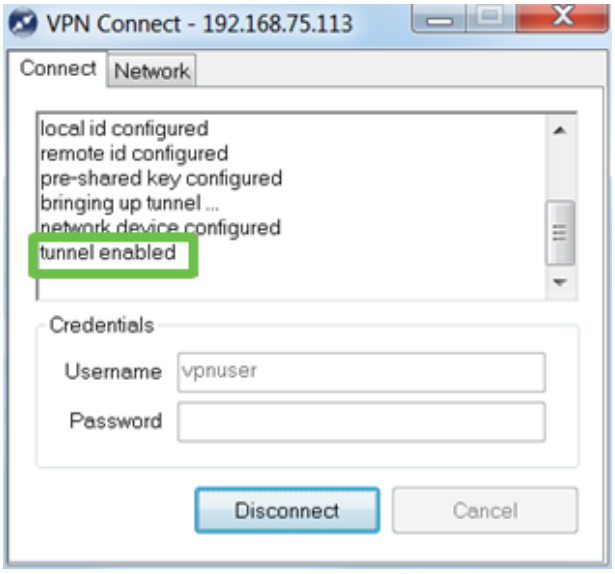
Schritt 12

Geben Sie im **VPN Connect-**Fenster, das angezeigt wird, den **Benutzernamen** und **das Kennwort** mit den Anmeldeinformationen für das **Benutzerkonto** ein, das wir auf dem RV340 erstellt haben (Schritte 13 und 14).

Wenn Sie fertig sind, klicken Sie auf **Verbinden**.

Schritt 13

Überprüfen Sie, ob der Tunnel angeschlossen ist. Der **Tunnel** sollte **aktiviert sein**.



Fazit

Sie sind nun für die VPN-Verbindung mit Ihrem Netzwerk eingerichtet.