

Verbindung mit IPSec VPN Server auf RV130 und RV130W über Shrew Soft VPN Client

Ziel

IPSec VPN (Virtual Private Network) ermöglicht die sichere Bereitstellung von Remote-Ressourcen über einen verschlüsselten Tunnel im Internet.

Der RV130 und der RV130W arbeiten als IPSec VPN Server und unterstützen den Shrew Soft VPN Client.

Laden Sie die neueste Version der Client-Software herunter.

- Shrew Soft (<https://www.shrew.net/download/vpn>)

Anmerkung: Um den Shrew Soft VPN Client erfolgreich mit einem IPSec VPN Server einrichten und konfigurieren zu können, müssen Sie zuerst den IPSec VPN Server konfigurieren. Weitere Informationen hierzu finden Sie im Artikel [Konfiguration eines IPSec VPN Servers auf RV130 und RV130W](#).

In diesem Dokument wird erläutert, wie Sie den Shrew Soft VPN-Client für die Verbindung mit einem IPSec VPN-Server der RV130 und RV130W verwenden.

Unterstützte Geräte

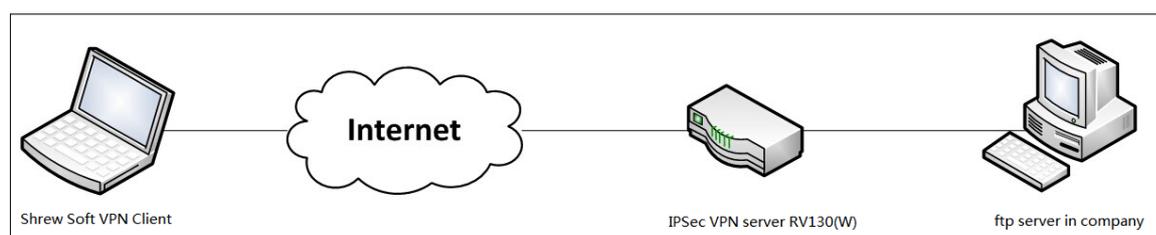
- RV130W Wireless-N VPN Firewall
- RV130 VPN-Firewall

Systemanforderungen

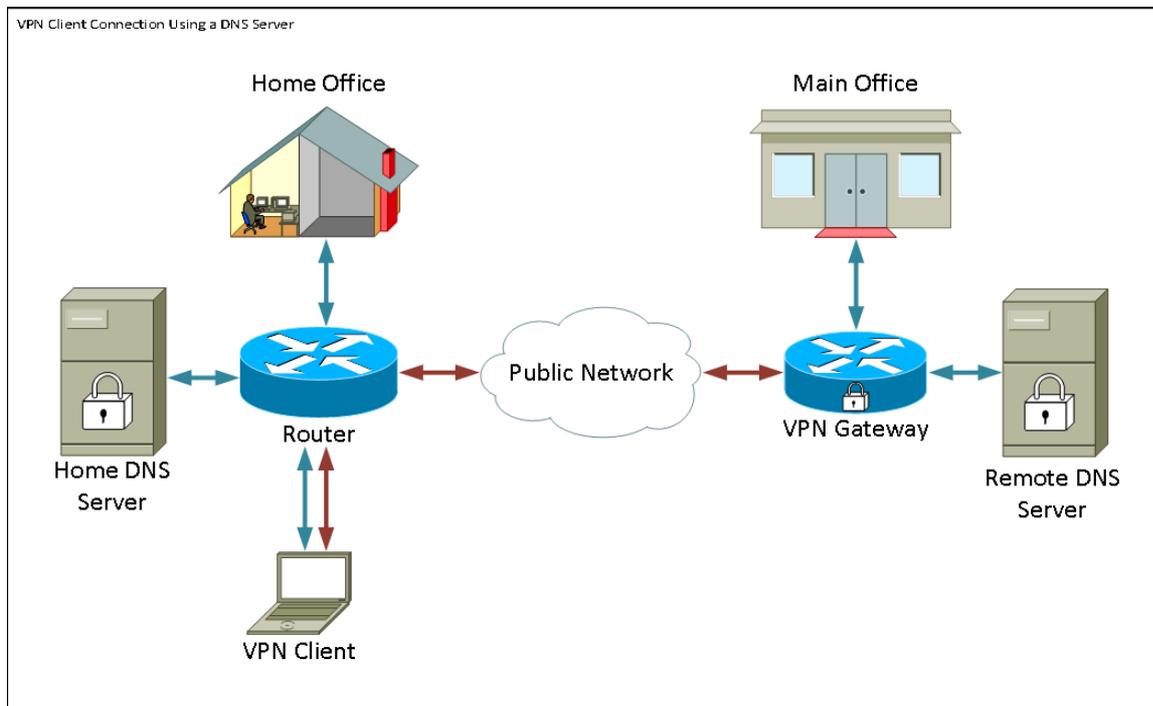
- 32- oder 64-Bit-Systeme
- Windows 2000, XP, Vista oder Windows 7/8

Topologie

Nachfolgend wird eine Topologie der obersten Ebene dargestellt, die die Geräte veranschaulicht, die an einer Konfiguration zwischen Client und Standort beteiligt sind.



Im Folgenden finden Sie ein detailliertes Flussdiagramm, das die Rolle von DNS-Servern in einer Netzwerkumgebung für kleine und mittlere Unternehmen veranschaulicht.



Software-Version

•1.0.1.3

Shrew Soft VPN-Client einrichten

IPSec-VPN-Einrichtung und -Benutzerkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > IPSec VPN Server > Setup**. Die Seite *Setup* wird geöffnet.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

Schritt 2: Überprüfen der ordnungsgemäßen Konfiguration des IPSec VPN-Servers für den RV130 Wenn der IPSec VPN Server nicht konfiguriert oder falsch konfiguriert ist, lesen Sie [Konfiguration eines IPSec VPN Servers auf RV130 und RV130W](#), und klicken Sie auf **Speichern**.

Setup

 Configuration settings have been saved successfully

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

IKE SA Life Time: Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

IPSec SA Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm:

Authentication Algorithm:

PFS Key Group: Enable

DH Group:

Anmerkung: Die obigen Einstellungen sind ein Beispiel für eine RV130/RV130W IPSec VPN Server-Konfiguration. Die Einstellungen basieren auf dem Dokument "[Configuration of an IPSec VPN Server on RV130 and RV130W](#)" und werden in den nachfolgenden Schritten beschrieben.

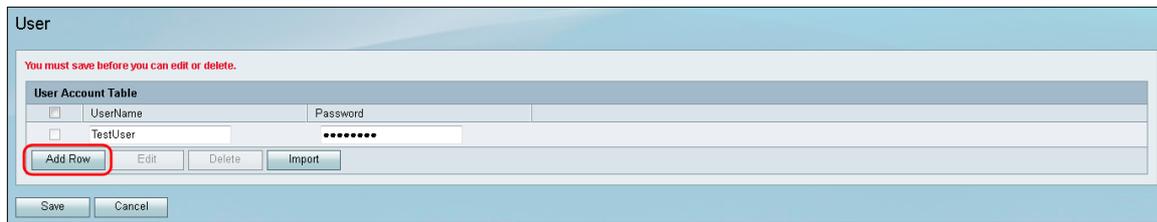
Schritt 3: Navigieren Sie zu **VPN > IPSec VPN Server > User**. Die Seite *Benutzer* wird angezeigt.

User

User Account Table

<input type="checkbox"/>	UserName	Password
<input type="checkbox"/>	No data to display	

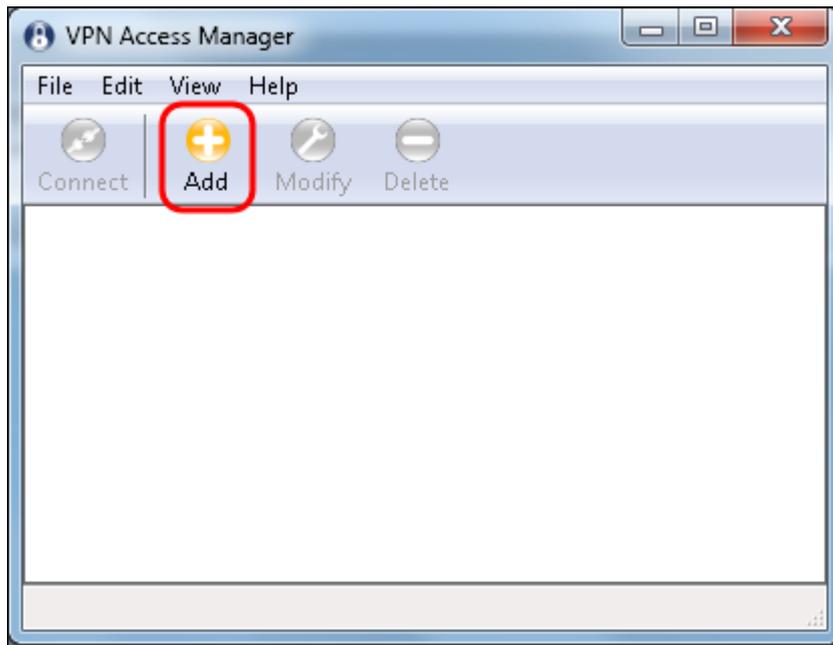
Schritt 4: Klicken Sie auf **Zeile hinzufügen**, um Benutzerkonten hinzuzufügen, die zur Authentifizierung der VPN-Clients verwendet werden (erweiterte Authentifizierung), und geben Sie den gewünschten Benutzernamen und das gewünschte Kennwort in die dafür vorgesehenen Felder ein.



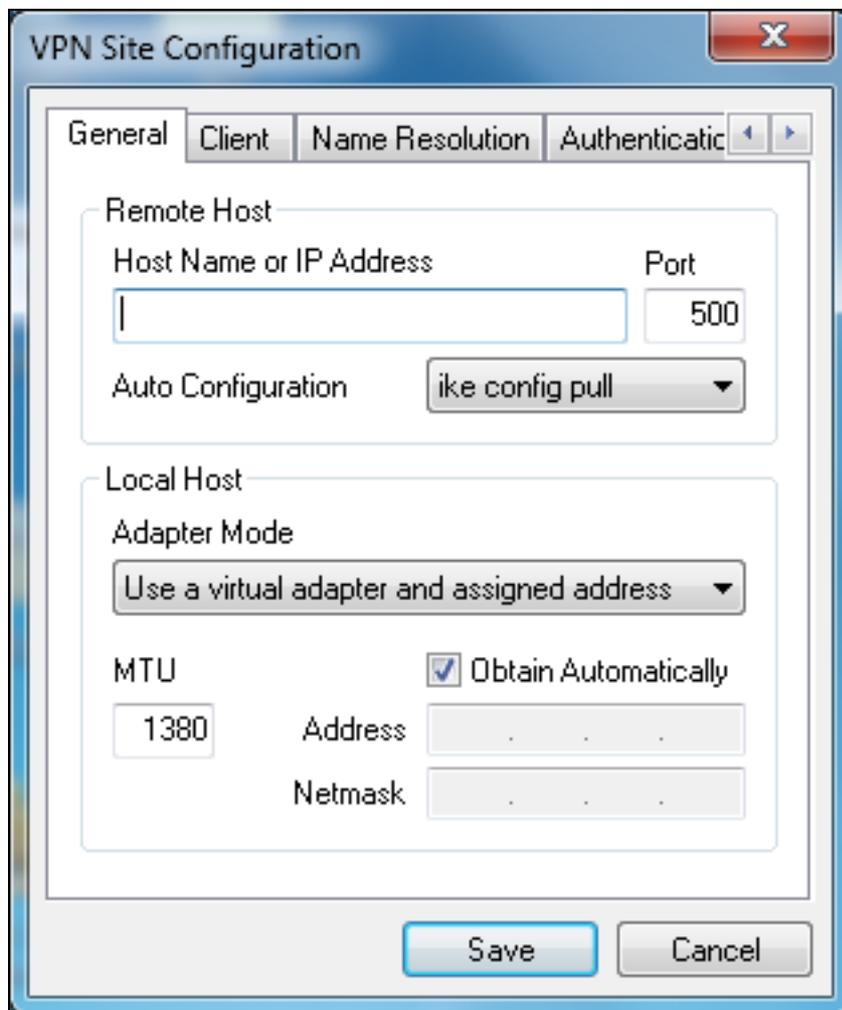
Schritt 5: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Konfiguration des VPN-Clients

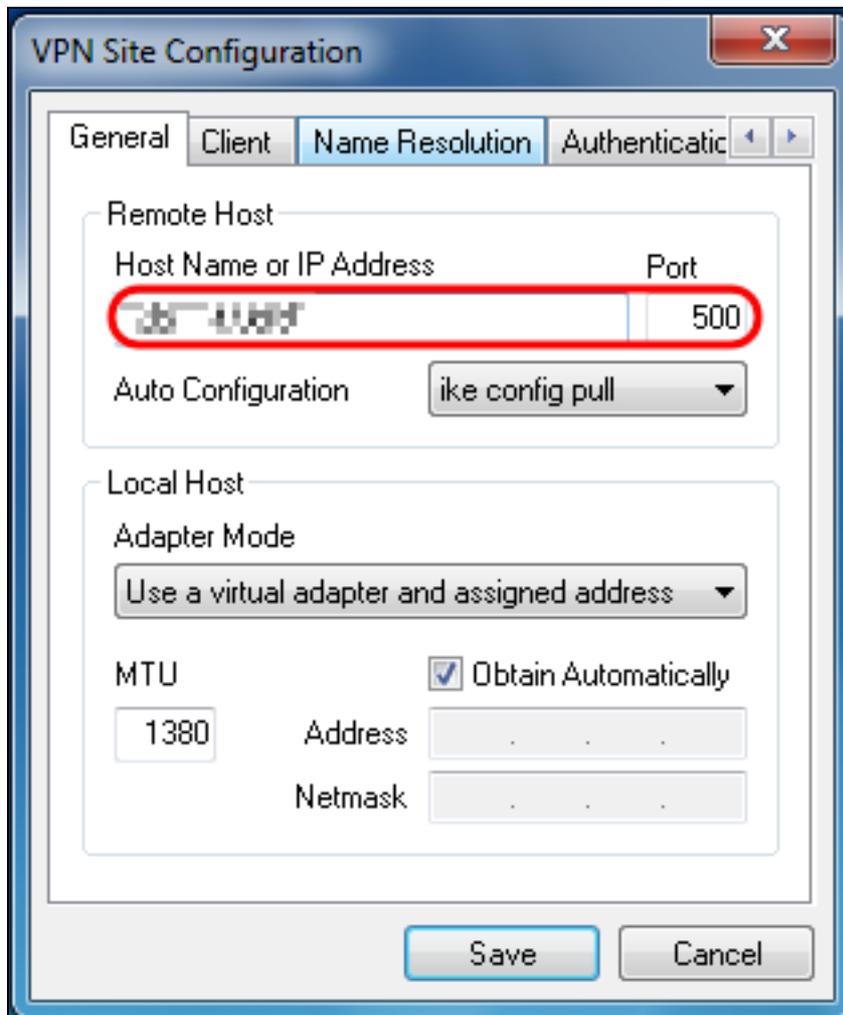
Schritt 1: Öffnen Sie SHREW VPN Access Manager, und klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen.



Das Fenster *VPN-Standortkonfiguration* wird angezeigt.

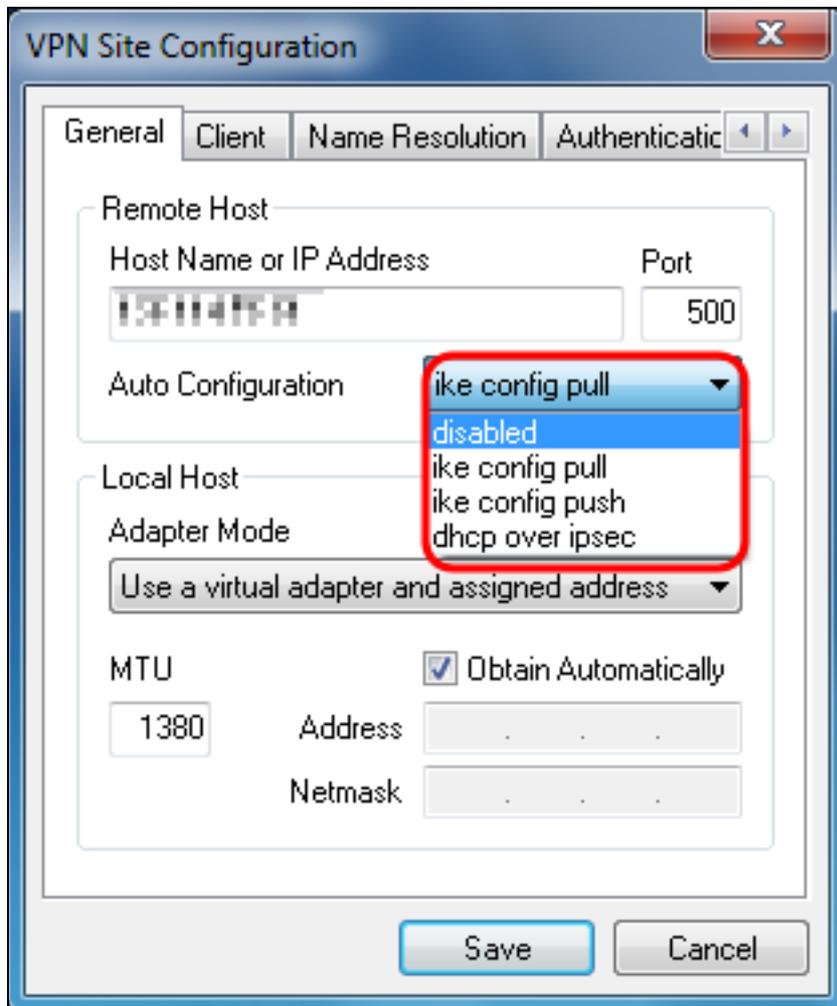


Schritt 2: Geben Sie im Abschnitt *Remote Host* auf der Registerkarte *General (Allgemein)* den öffentlichen Hostnamen oder die IP-Adresse des Netzwerks ein, mit dem Sie eine Verbindung herstellen möchten.



Anmerkung: Stellen Sie sicher, dass die Portnummer auf den Standardwert 500 festgelegt ist. Damit das VPN funktioniert, verwendet der Tunnel den UDP-Port 500, der so festgelegt werden sollte, dass ISAKMP-Datenverkehr an die Firewall weitergeleitet werden kann.

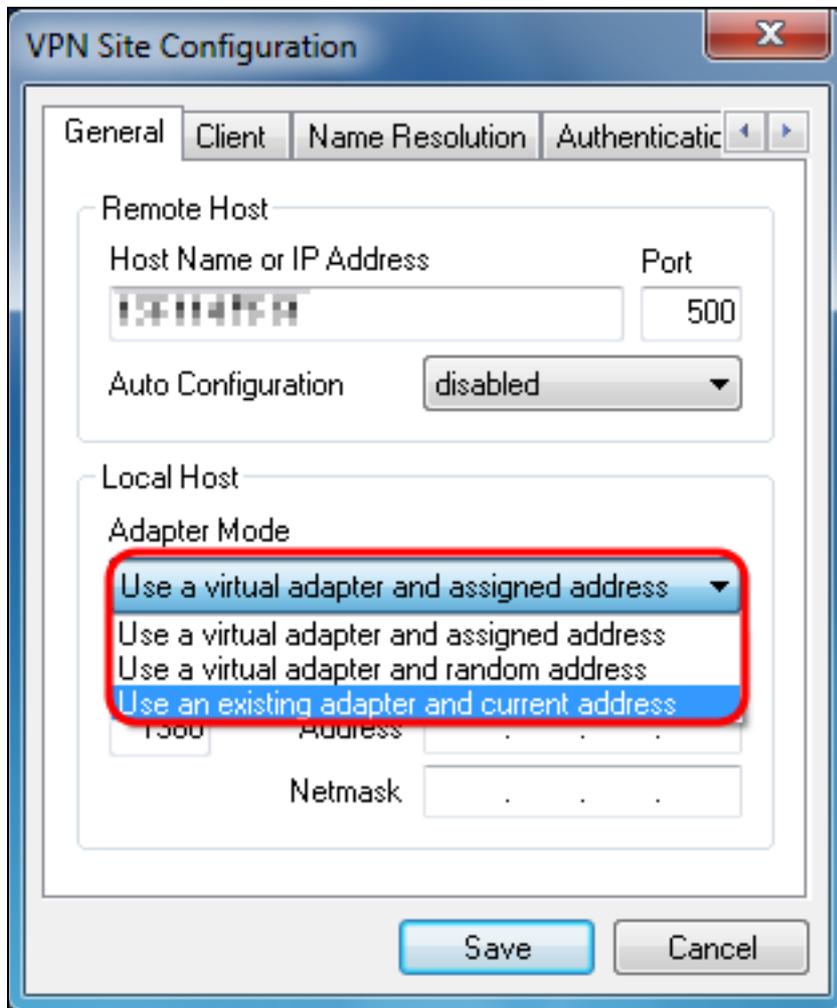
Schritt 3: Wählen Sie in der Dropdown-Liste "*Automatische Konfiguration*" die Option **Deaktiviert aus**.



Die verfügbaren Optionen sind wie folgt definiert:

- Deaktiviert - Deaktiviert alle automatischen Client-Konfigurationen.
- IKE Config Pull - Ermöglicht das Einstellen von Anforderungen eines Computers durch den Client. Mit der Unterstützung der Pull-Methode durch den Computer gibt die Anforderung eine Liste von Einstellungen zurück, die vom Client unterstützt werden.
- IKE Config Push - Bietet einem Computer die Möglichkeit, dem Client während des Konfigurationsprozesses Einstellungen anzubieten. Mit der Unterstützung der Push-Methode durch den Computer gibt die Anforderung eine Liste von Einstellungen zurück, die vom Client unterstützt werden.
- DHCP Over IPsec - Ermöglicht dem Client, Einstellungen vom Computer über DHCP over IPsec anzufordern.

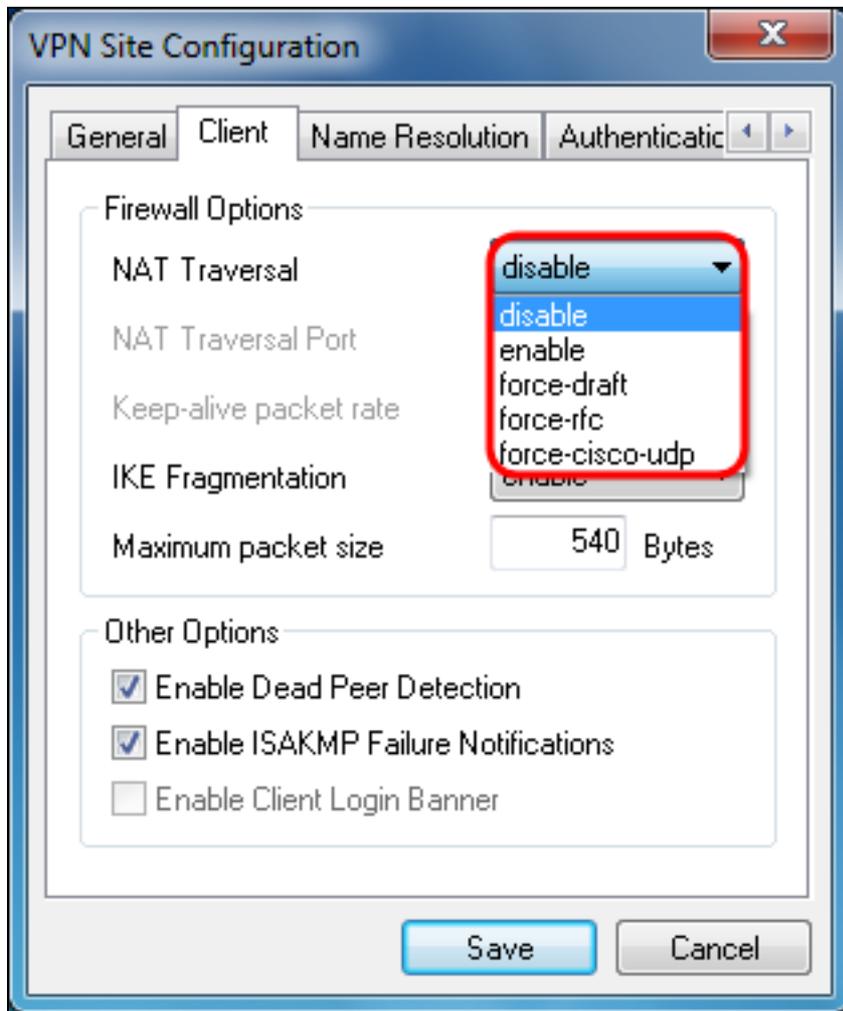
Schritt 4: Wählen Sie im Abschnitt "*Lokaler Host*" in der Dropdown-Liste "*Adaptermodus*" die Option **Vorhandenen Adapter und aktuelle Adresse verwenden**.



Die verfügbaren Optionen sind wie folgt definiert:

- Virtuellen Adapter und zugewiesene Adresse verwenden — Ermöglicht dem Client, einen virtuellen Adapter mit einer angegebenen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.
- Verwendung eines virtuellen Adapters und einer zufälligen Adresse — Ermöglicht dem Client, einen virtuellen Adapter mit einer zufälligen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.
- Vorhandenen Adapter und aktuelle Adresse verwenden — Ermöglicht dem Client, nur den vorhandenen physischen Adapter mit der aktuellen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.

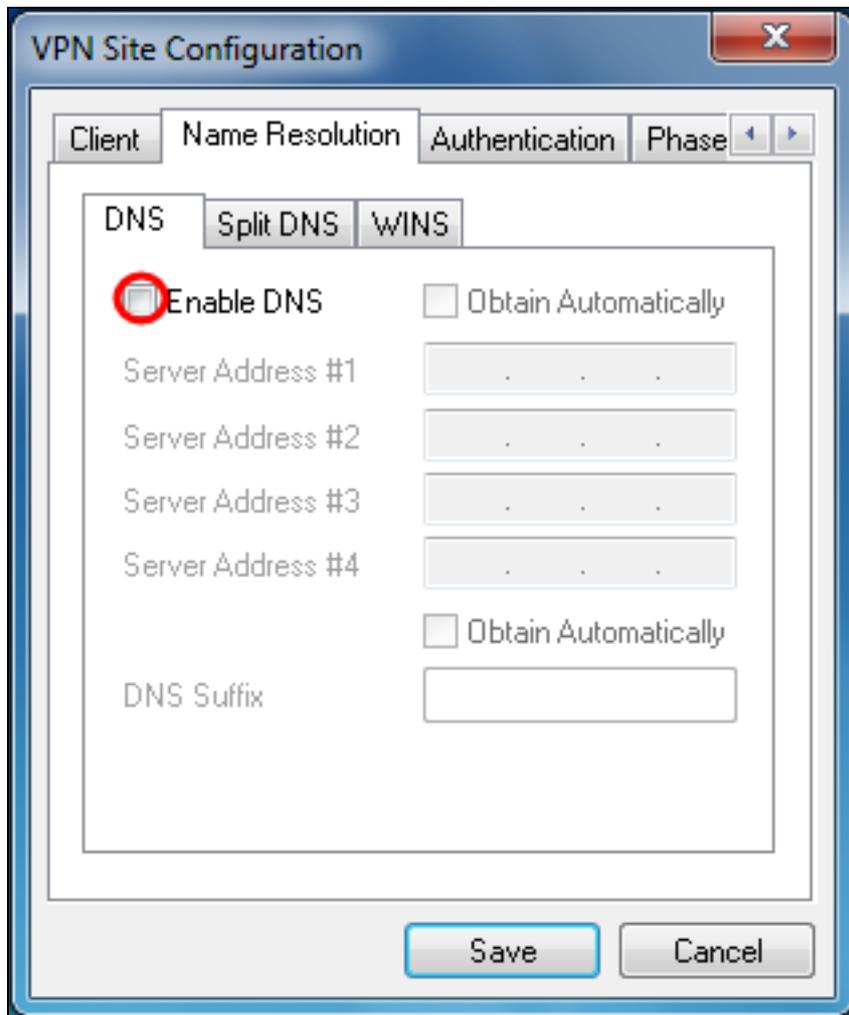
Schritt 5: Klicken Sie auf die Registerkarte *Client*. Wählen Sie in der Dropdown-Liste *NAT Traversal* im Artikel [Configuration of an IPsec VPN Server on RV130 and RV130W \(Konfiguration eines IPsec VPN Servers auf RV130 und RV130W\)](#) die gleiche Einstellung aus, die Sie auf dem *RV130W* konfiguriert haben.



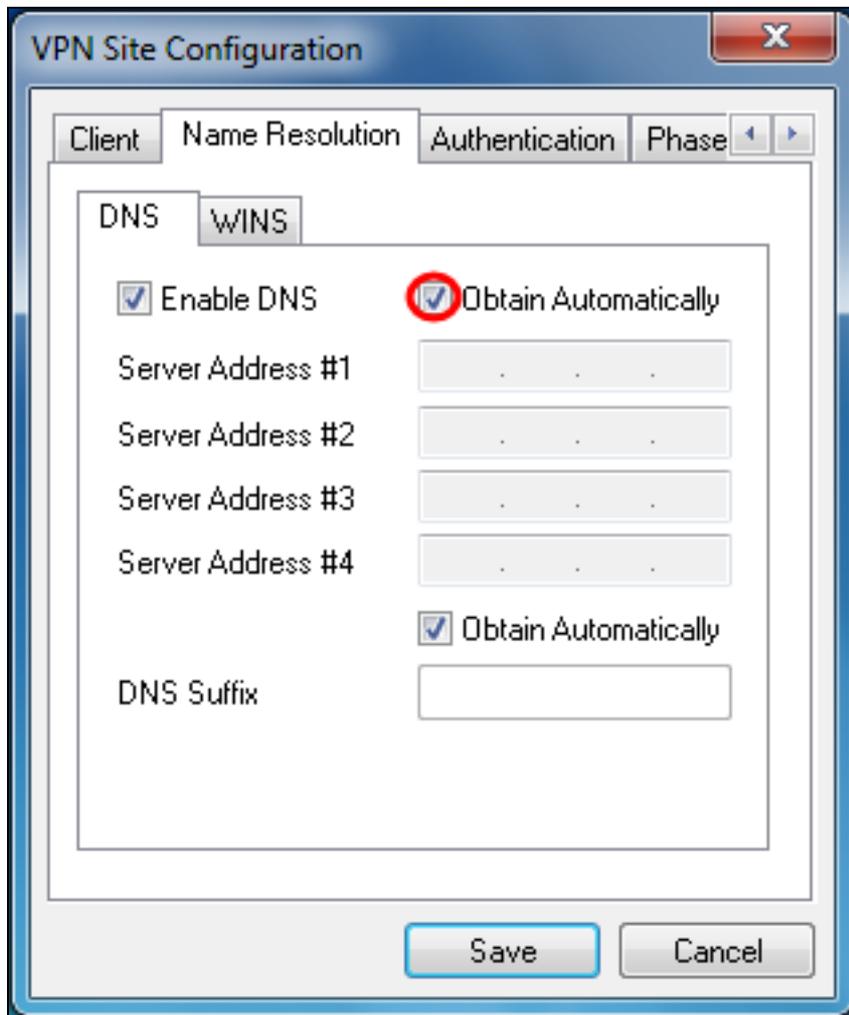
Die verfügbaren NAT-Menüoptionen (Network Address Translation Traversal) sind wie folgt definiert:

- Disable (Deaktivieren) - Die NAT-Protokollerweiterungen werden nicht verwendet.
- Aktivieren - Die NAT-Protokollerweiterungen werden nur verwendet, wenn das VPN-Gateway Unterstützung während der Aushandlung anzeigt und NAT erkannt wird.
- Force-Draft - Die Draft-Version der NAT-Protokoll-Erweiterungen wird verwendet, unabhängig davon, ob das VPN-Gateway Unterstützung bei Verhandlungen anzeigt oder NAT erkannt wird.
- Force-RFC - Die RFC-Version des NAT-Protokolls wird unabhängig davon verwendet, ob das VPN-Gateway Unterstützung während der Aushandlung anzeigt oder ob NAT erkannt wird.
- Force-Cisco-UDP: Erzwingt die UDP-Kapselung für VPN-Clients ohne NAT.

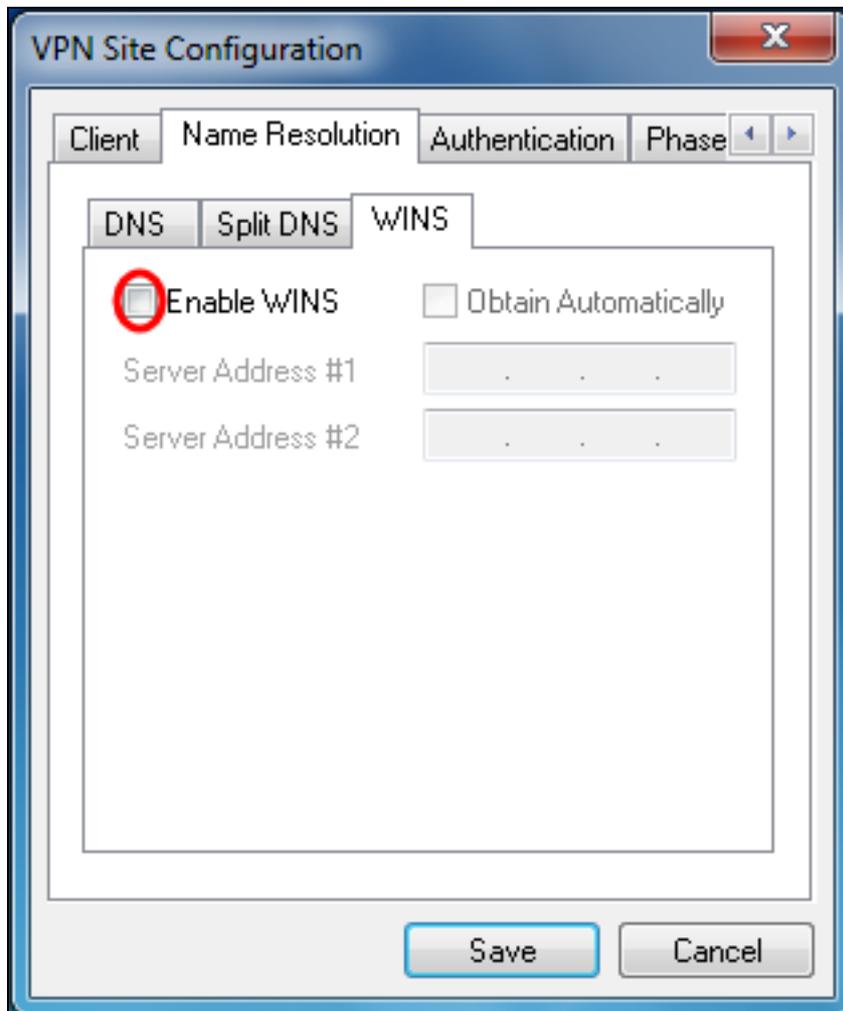
Schritt 6. Klicken Sie auf die Registerkarte *Namensauflösung* und aktivieren Sie das Kontrollkästchen **DNS aktivieren**, wenn Sie DNS aktivieren möchten. Wenn für die Standortkonfiguration keine spezifischen DNS-Einstellungen erforderlich sind, deaktivieren Sie das Kontrollkästchen **DNS aktivieren**.



Schritt 7: (Optional) Wenn Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway die DNS-Einstellungen automatisch bereitstellen. Wenn nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige DNS-Serveradresse ein.

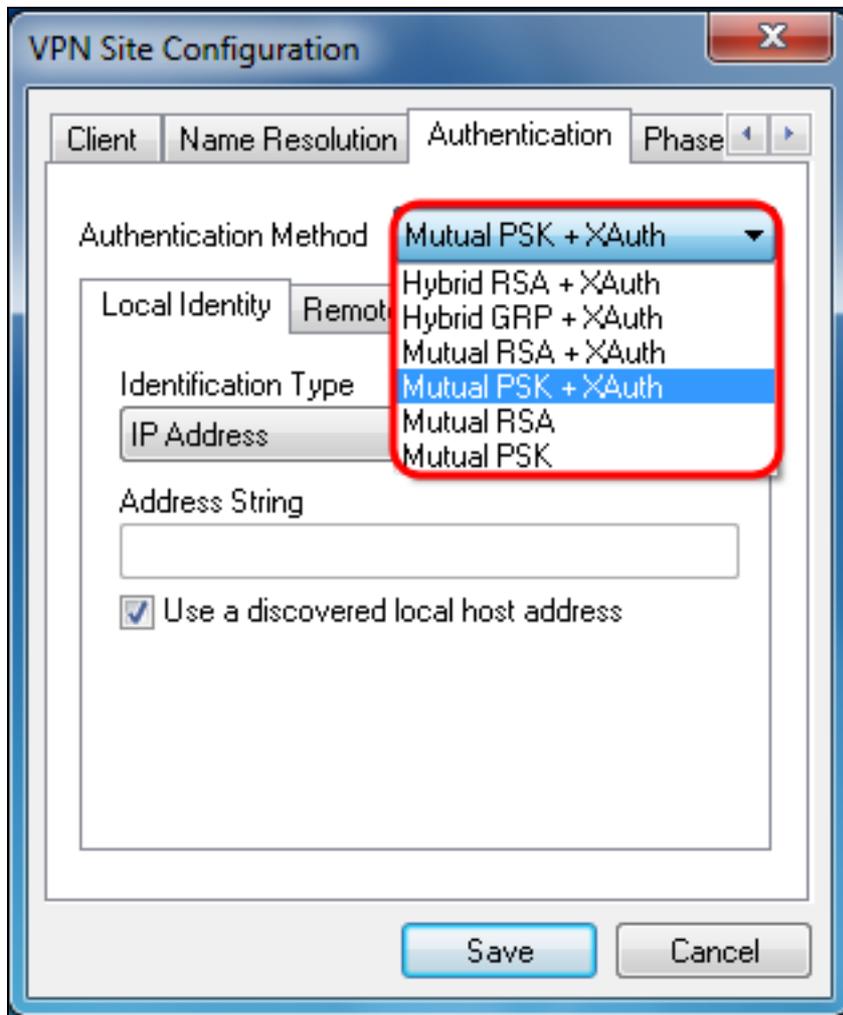


Schritt 8. (Optional) Klicken Sie auf die Registerkarte *Namensauflösung*, aktivieren Sie das Kontrollkästchen **WINS aktivieren**, wenn Sie den Windows Internet Name Server (WINS) aktivieren möchten. Wenn Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway die WINS-Einstellungen automatisch bereitstellen. Wenn nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige WINS-Serveradresse ein.



Anmerkung: Durch die Bereitstellung von WINS-Konfigurationsinformationen kann ein Client WINS-Namen mithilfe eines Servers auflösen, der sich im privaten Remote-Netzwerk befindet. Dies ist nützlich, wenn Sie versuchen, über einen Pfadnamen für die Uniform Naming Convention auf Remote-Windows-Netzwerkressourcen zuzugreifen. Der WINS-Server gehört normalerweise zu einem Windows-Domänencontroller oder einem Samba-Server.

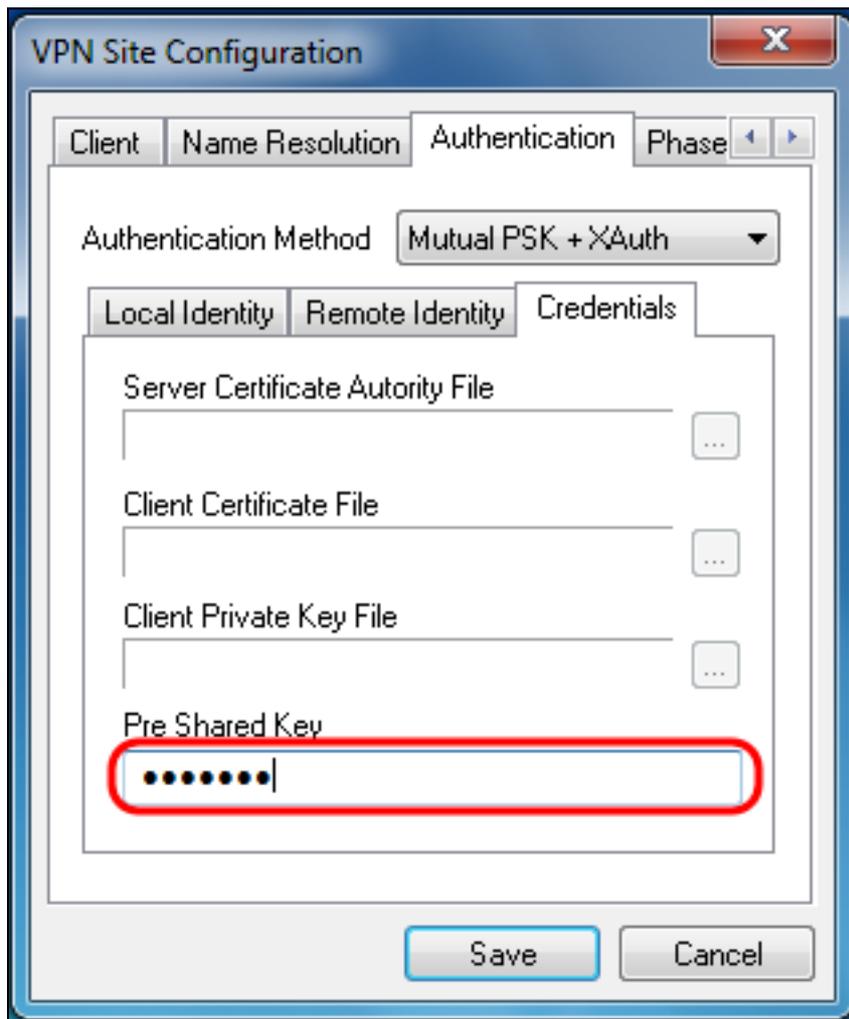
Schritt 9: Klicken Sie auf die Registerkarte *Authentication* (*Authentifizierung*), und wählen Sie **Mutual PSK + XAuth** in der Dropdown-Liste *Authentication Method* (*Authentifizierungsmethode*) aus.



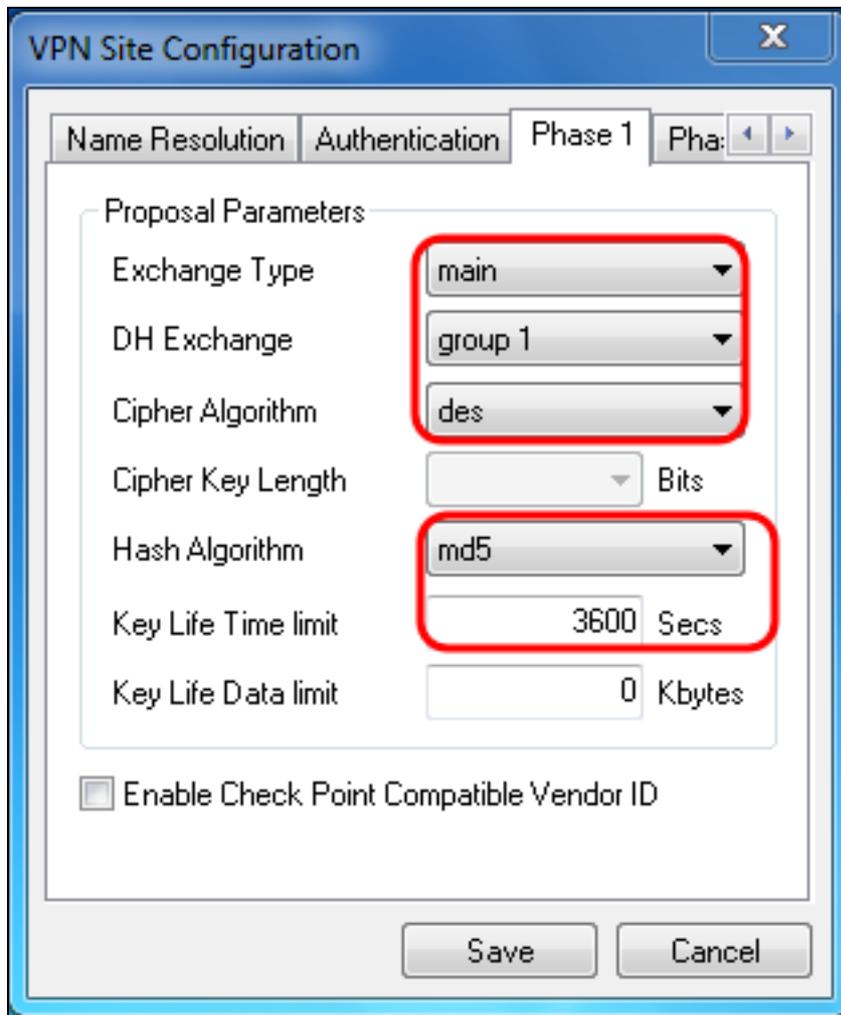
Die verfügbaren Optionen sind wie folgt definiert:

- Hybrid-RSA + XAuth — Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseldateitypen bereitgestellt.
- Hybrid GRP + XAuth — Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form einer PEM- oder PKCS12-Zertifikatsdatei und einer Zeichenfolge mit gemeinsamem Schlüssel bereitgestellt.
- Gegenseitiges RSA + XAuth — Client und Gateway benötigen beide Anmeldeinformationen zur Authentifizierung. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.
- Gegenseitiges PSK + XAuth — Client und Gateway benötigen beide Anmeldeinformationen, um sich zu authentifizieren. Die Anmeldeinformationen werden in Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt.
- Gegenseitiges RSA - Client und Gateway benötigen zur Authentifizierung Anmeldeinformationen. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.
- Gegenseitiges PSK: Client und Gateway benötigen zur Authentifizierung Anmeldeinformationen. Die Anmeldeinformationen werden in Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt.

Schritt 10: Klicken Sie im Abschnitt "Authentifizierung" auf die Unterregisterkarte "Anmeldedaten" und geben Sie den gleichen vorinstallierten Schlüssel ein, den Sie auf der Seite "IPsec VPN Server Setup" im Feld "Vorinstallierter Schlüssel" konfiguriert haben.



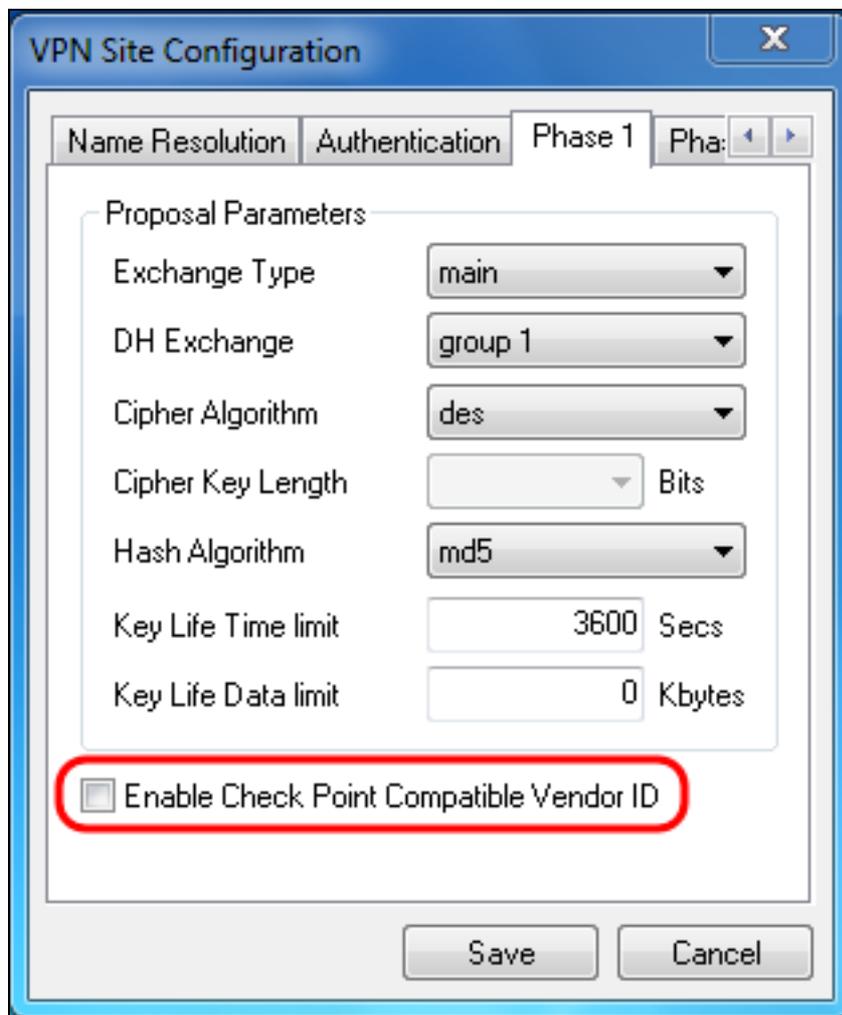
Schritt 11: Klicken Sie auf die Registerkarte *Phase 1*. Konfigurieren Sie die folgenden Parameter so, dass sie die gleichen Einstellungen aufweisen, die Sie in [Schritt 2 des Abschnitts "IPSec VPN Server User Configuration"](#) für den RV130/RV130W konfiguriert haben.



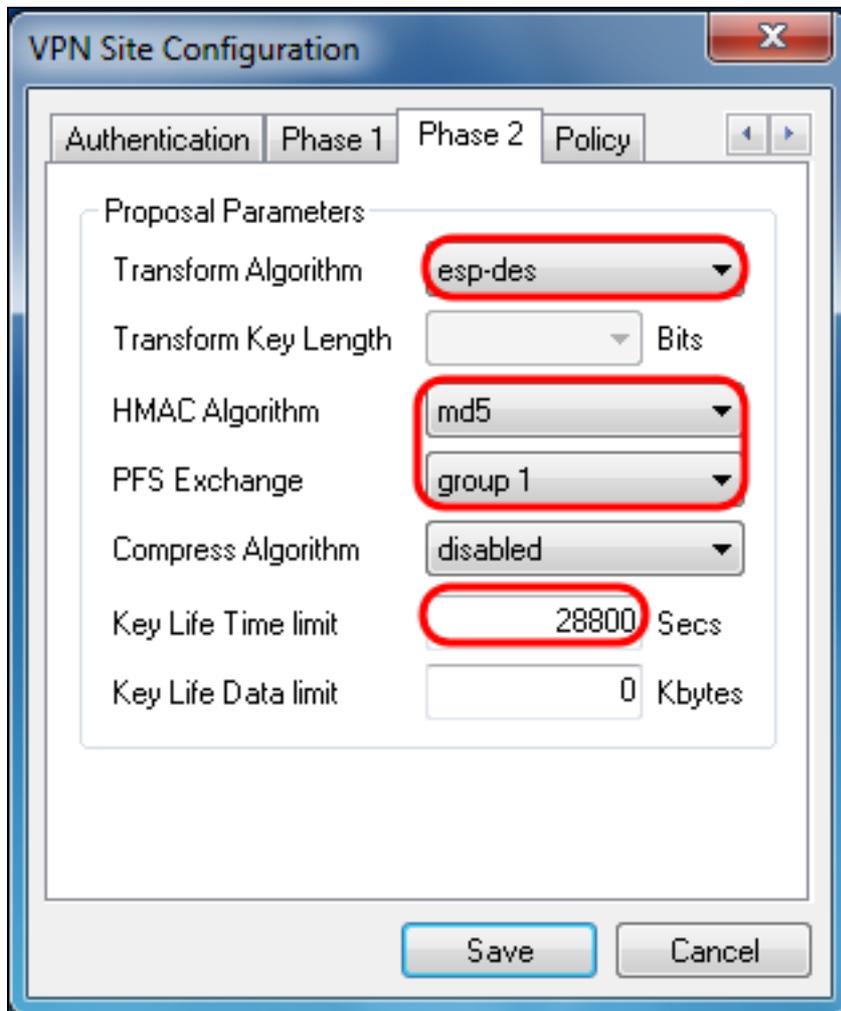
Die Parameter in Shrew Soft müssen mit den RV130/RV130W-Konfigurationen in Phase 1 übereinstimmen:

- "Exchange Type" sollte mit "Exchange Mode" übereinstimmen.
- "DH Exchange" sollte mit "DH Group" übereinstimmen.
- "Cipher Algorithm" sollte mit "Encryption Algorithm" übereinstimmen.
- "Hash Algorithm" sollte mit "Authentication Algorithm" übereinstimmen.

Schritt 12: Wenn Ihr Gateway während der Phase-1-Verhandlungen eine mit Cisco kompatible Anbieter-ID anbietet, aktivieren Sie das Kontrollkästchen **Enable Check Point Compatible Vendor ID (Check Point-kompatible Anbieter-ID aktivieren)**. Wenn das Gateway dies nicht tut, oder wenn Sie sich nicht sicher sind, lassen Sie das Kontrollkästchen deaktiviert.



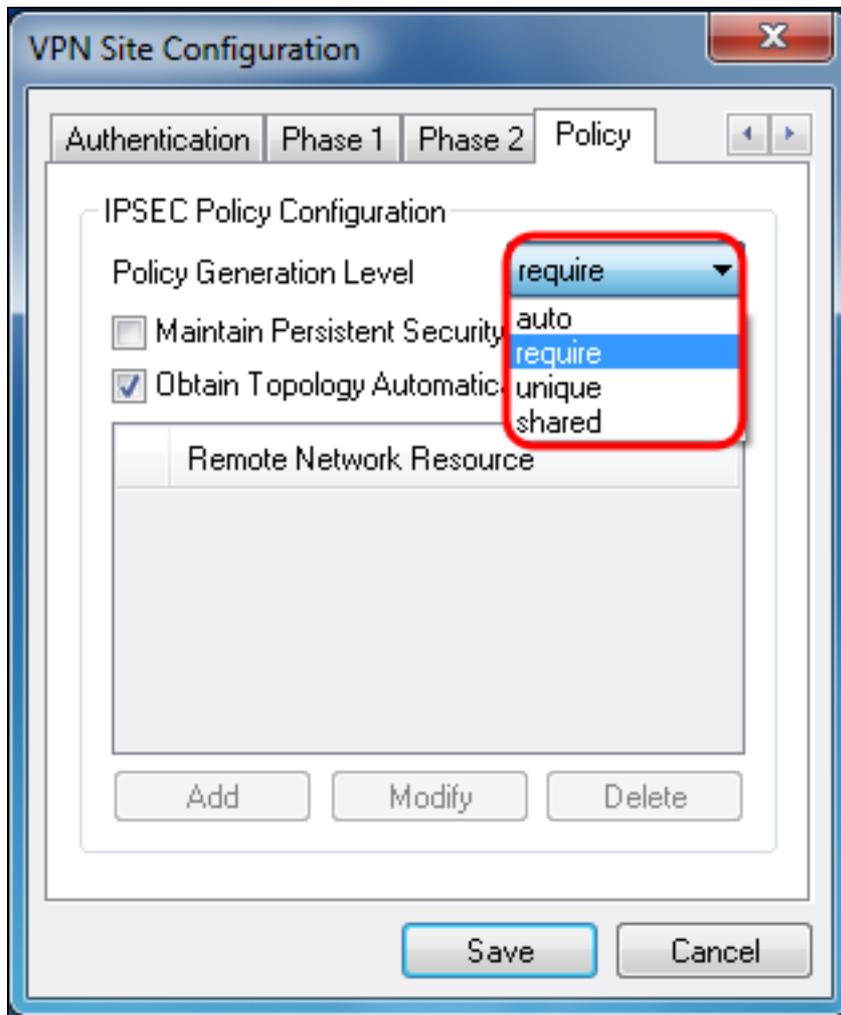
Schritt 13. Klicken Sie auf die Registerkarte *Phase 2*. Konfigurieren Sie die folgenden Parameter so, dass sie die gleichen Einstellungen aufweisen, die Sie in [Schritt 2 des Abschnitts "IPSec VPN Server User Configuration"](#) für den RV130/RV130W konfiguriert haben.



Die Parameter in Shrew Soft müssen mit den RV130/RV130W-Konfigurationen in Phase 2 übereinstimmen:

- "Transform Algorithm" sollte mit "Encryption Algorithm" übereinstimmen.
- "HMAC Algorithm" sollte mit "Authentication Algorithm" übereinstimmen.
- "PFS Exchange" sollte mit "DH Group" übereinstimmen, wenn PFS Key Group auf dem RV130/RV130W aktiviert ist. Andernfalls wählen Sie **Disabled (Deaktiviert)**.
- "Key Life Time limit" sollte mit "IPSec SA Lifetime" übereinstimmen.

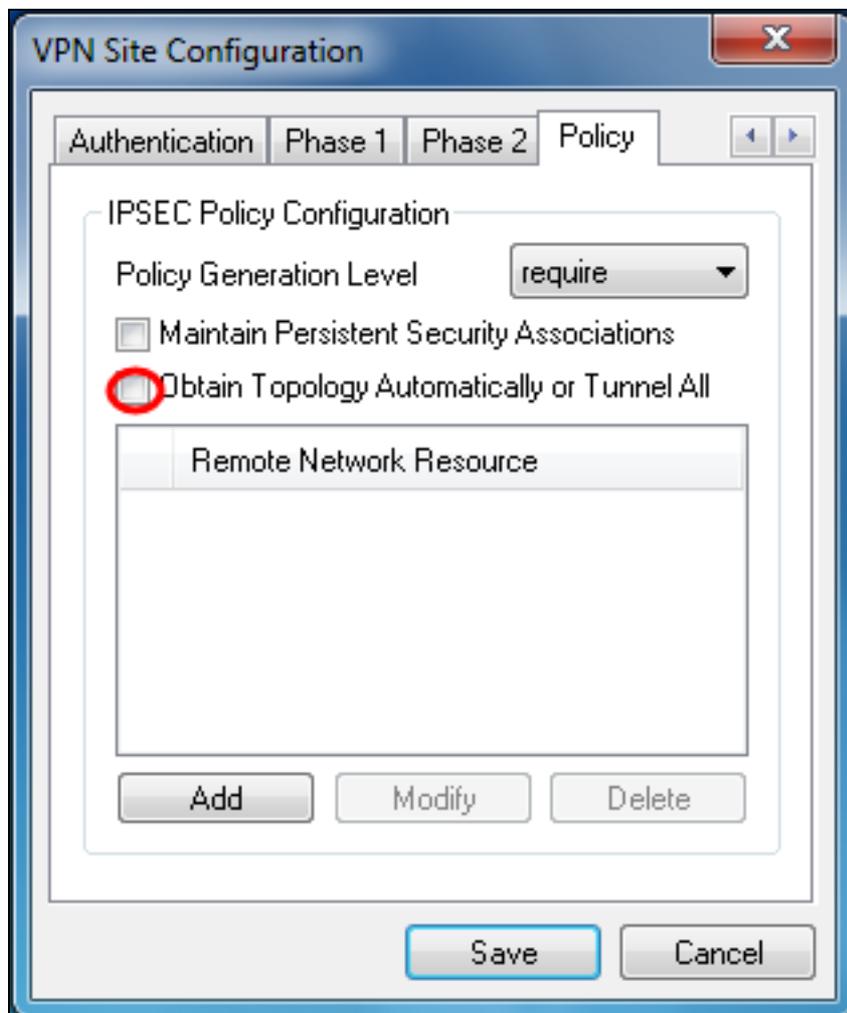
Schritt 14: Klicken Sie auf die Registerkarte *Policy (Richtlinie)*, und wählen Sie in der Dropdown-Liste *Policy Generation Level (Richtlinienerstellungsebene)* die Option **require** aus. Mit der Option *Richtlinienerstellungsebene* wird die Ebene geändert, auf der IPsec-Richtlinien generiert werden. Die verschiedenen Ebenen in der Dropdown-Liste entsprechen dem IPsec SA-Verhalten, das von verschiedenen Anbieterimplementierungen implementiert wurde.



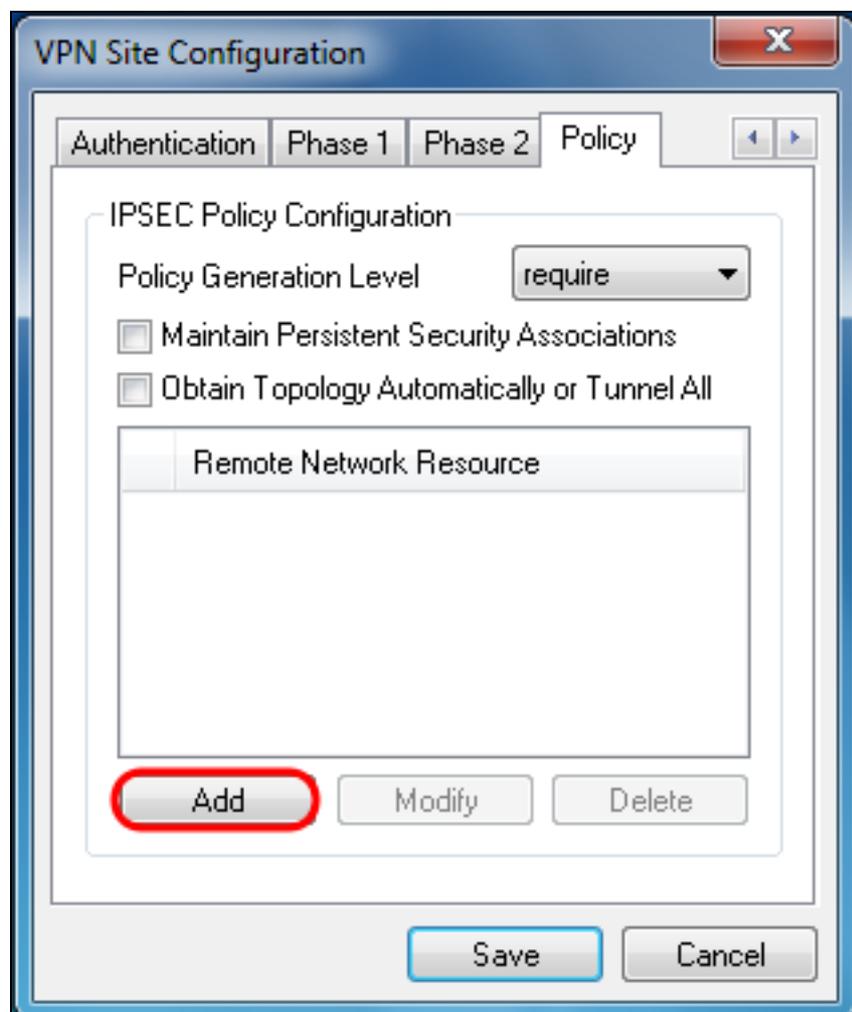
Die verfügbaren Optionen sind wie folgt definiert:

- Auto - Der Client bestimmt automatisch die entsprechende IPSec-Richtlinienebene.
- Erforderlich - Der Client handelt keine eindeutige Sicherheitszuordnung (Security Association, SA) für jede Richtlinie aus. Richtlinien werden unter Verwendung der lokalen öffentlichen Adresse als lokale Richtlinien-ID und der Remote-Netzwerkressourcen als Remote-Richtlinien-ID generiert. Bei dem Vorschlag für Phase 2 werden die Richtlinien-IDs während der Verhandlung verwendet.
- Eindeutig - Der Client handelt für jede Richtlinie eine eindeutige Sicherheitszuordnung aus.
- Freigegeben - Richtlinien werden auf der erforderlichen Ebene erstellt. Im Vorschlag für Phase 2 wird die lokale Richtlinien-ID als lokale ID und Any (0.0.0.0/0) als Remote-ID während der Verhandlung verwendet.

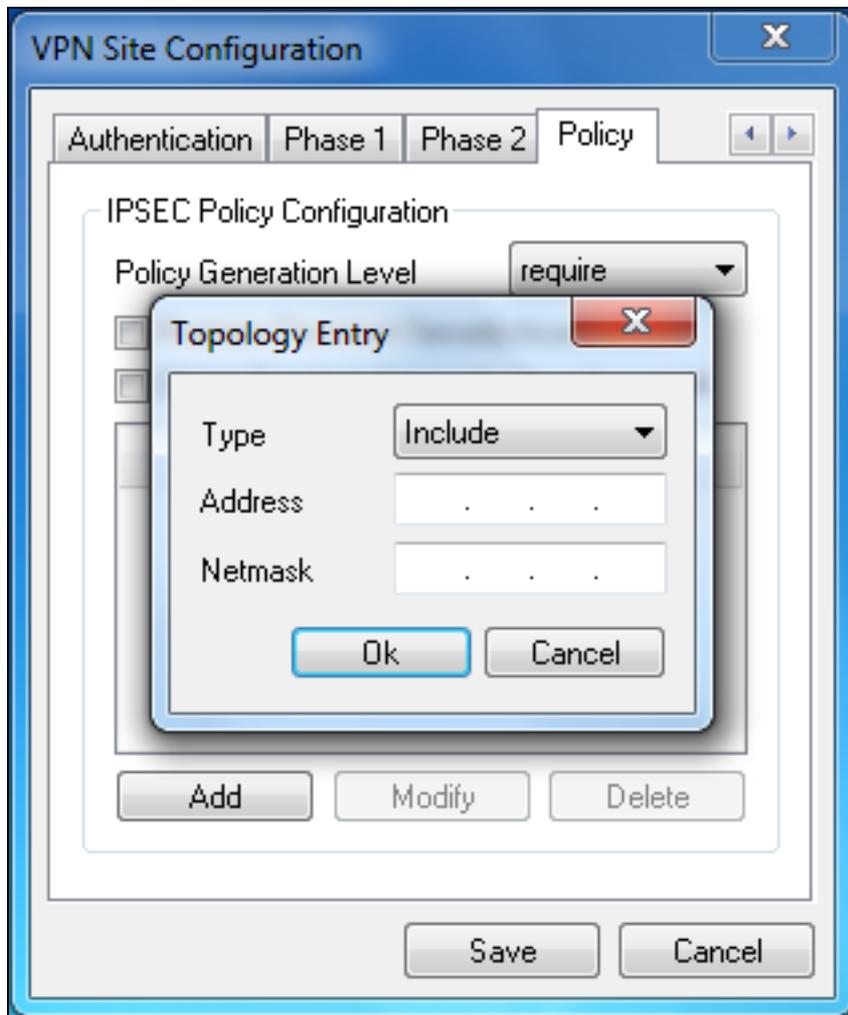
Schritt 15: Deaktivieren Sie das Kontrollkästchen **Topologie automatisch beziehen oder Tunnel All**. Mit dieser Option wird die Konfiguration von Sicherheitsrichtlinien für die Verbindung geändert. Wenn deaktiviert, muss eine manuelle Konfiguration durchgeführt werden. Wenn diese Option aktiviert ist, wird die automatische Konfiguration durchgeführt.



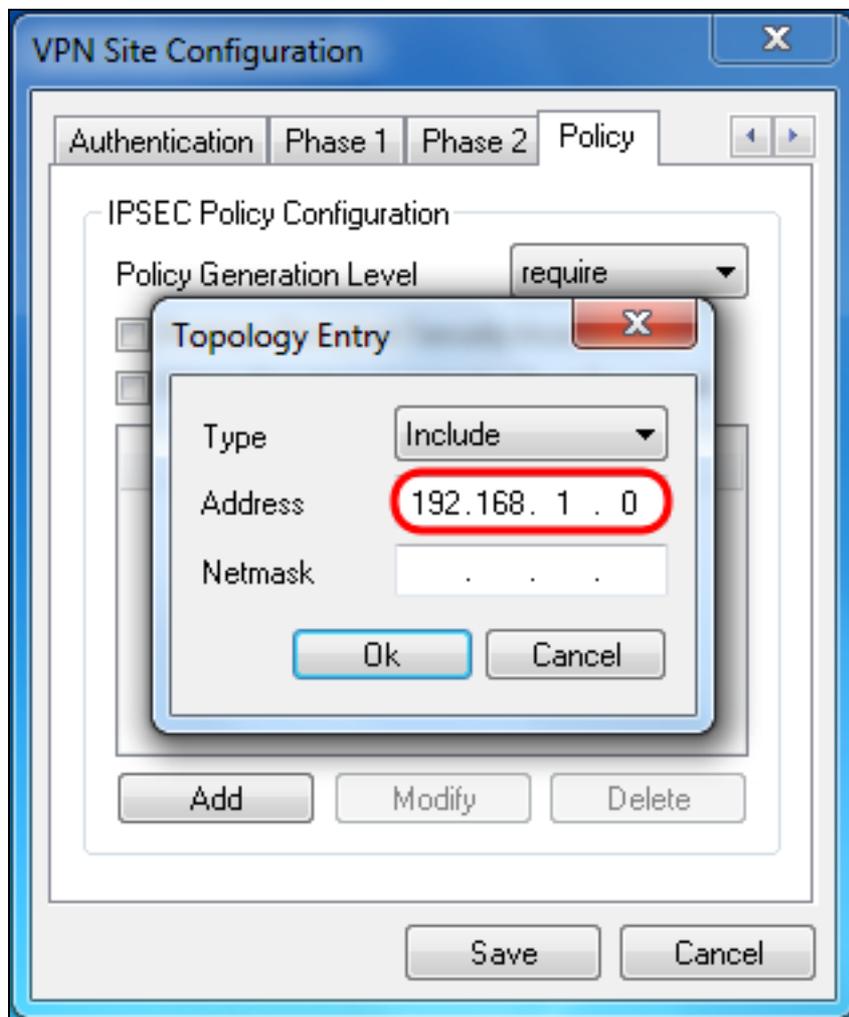
Schritt 16. Klicken Sie auf **Hinzufügen**, um die Remote-Netzwerkressource hinzuzufügen, mit der Sie eine Verbindung herstellen möchten. Zu den Remote-Netzwerkressourcen gehören der Remote-Zugriff auf Desktops, Abteilungsressourcen, Netzlaufwerke und gesicherte elektronische Post.



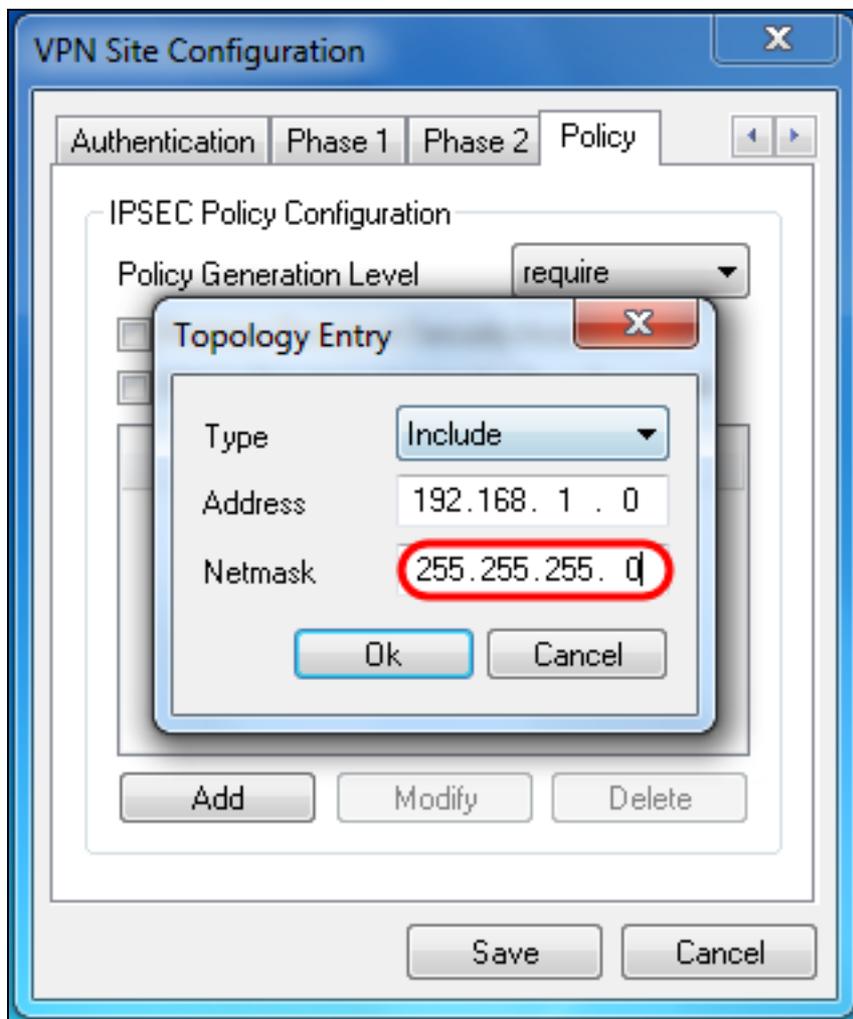
Das Fenster *Topologieeintrag* wird angezeigt:



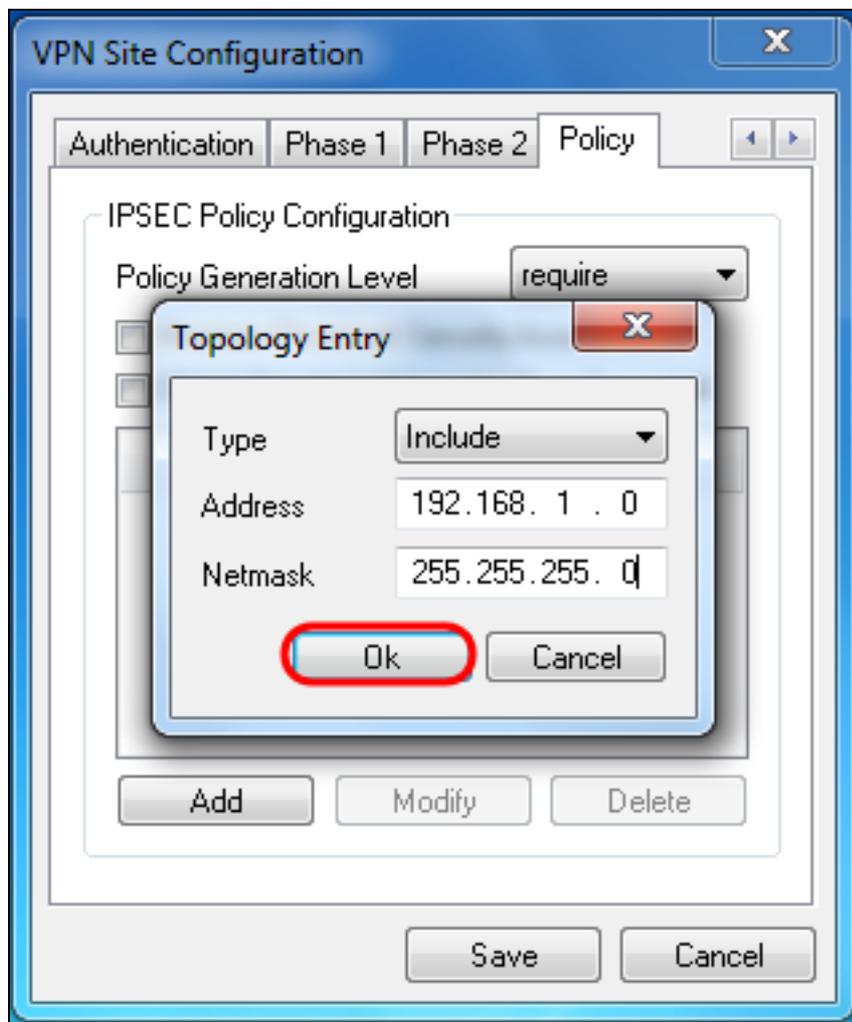
Schritt 17: Geben Sie im Feld *Adresse* die Subnetz-ID des RV130/RV130W ein. Die Adresse muss mit dem Feld *IP-Adresse* in [Schritt 2 des Abschnitts "IPSec VPN Server Setup and User Configuration"](#) dieses Dokuments übereinstimmen.



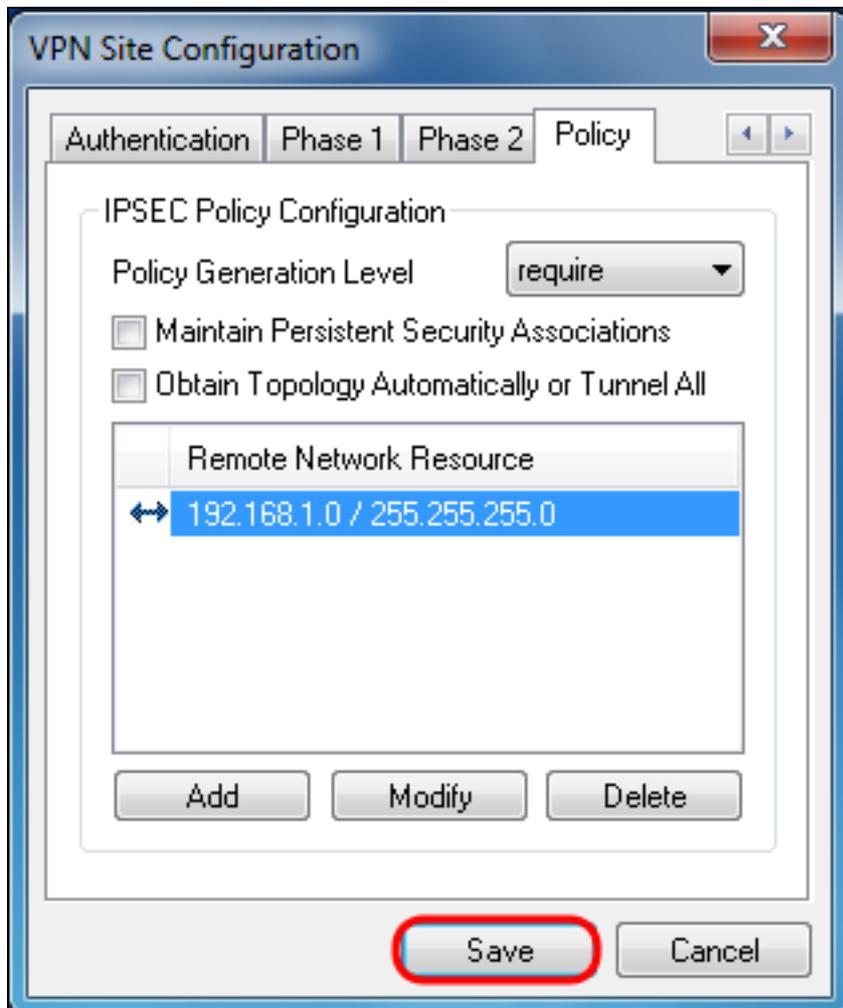
Schritt 18: Geben Sie in das Feld *Netzmaske* die Subnetzmaske für das lokale Netzwerk des RV130/RV130W ein. Die Netzmaske muss mit dem Feld *Subnetzmaske* in [Schritt 2 des Abschnitts "IPSec VPN Server User Configuration"](#) dieses Dokuments übereinstimmen.



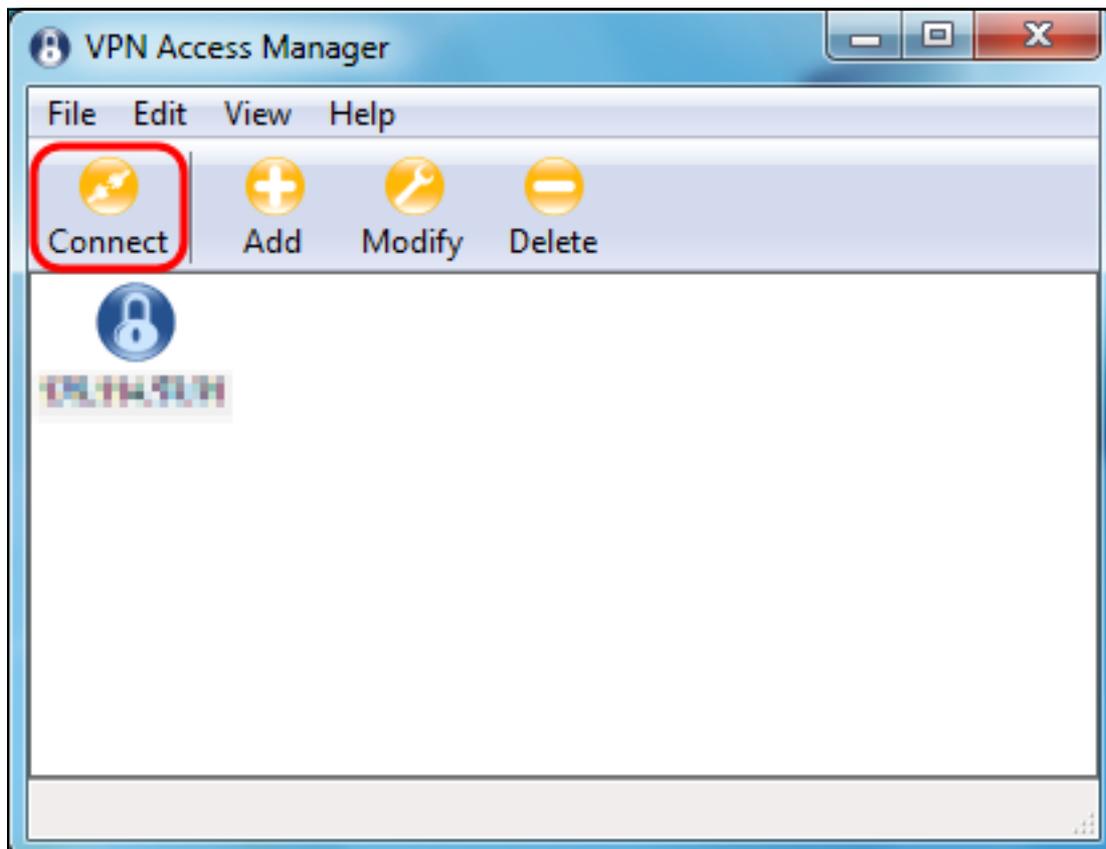
Schritt 19: Klicken Sie auf **OK**, um die Remote-Netzwerkressource hinzuzufügen.



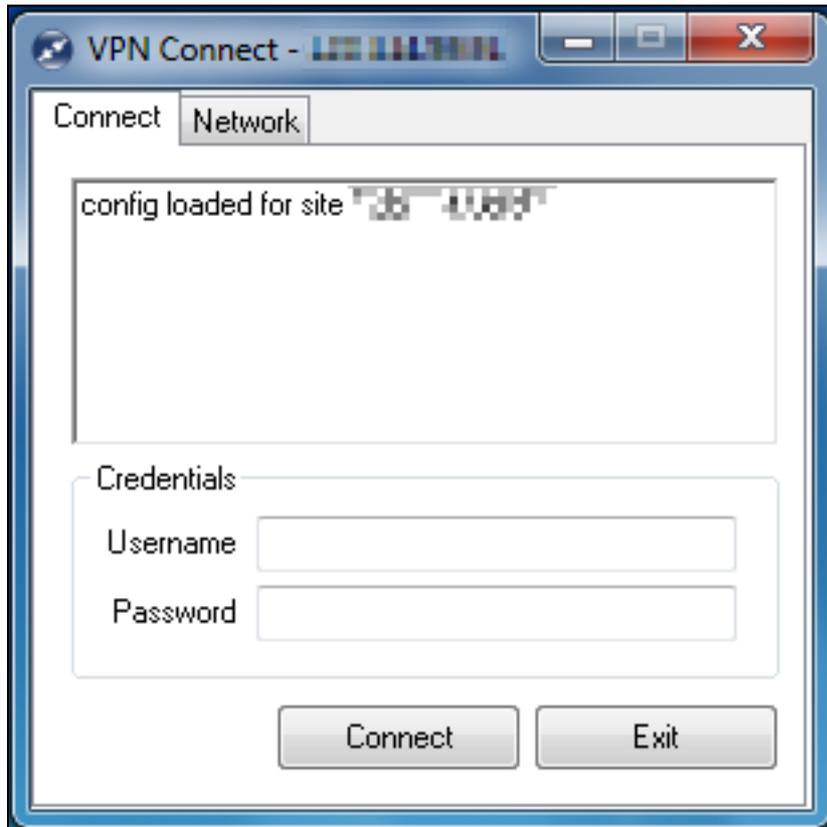
Schritt 20: Klicken Sie auf **Speichern**, um die Konfigurationen für die Verbindung mit der VPN-Site zu speichern.



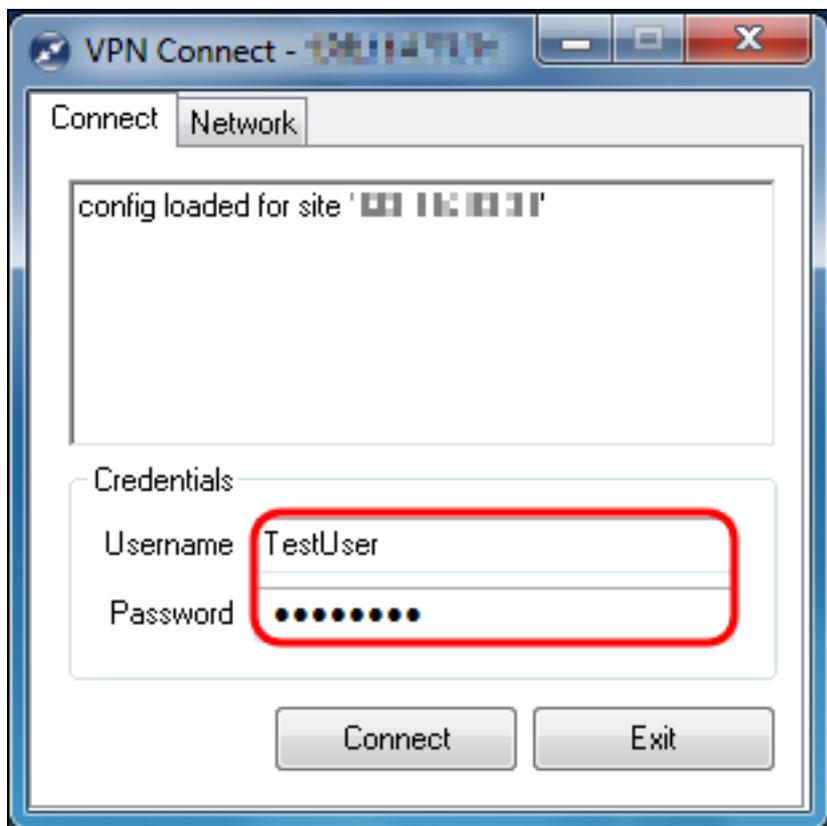
Schritt 21: Kehren Sie zum Fenster *VPN Access Manager* zurück, um den von Ihnen konfigurierten VPN-Standort auszuwählen, und klicken Sie auf die Schaltfläche **Verbinden**.



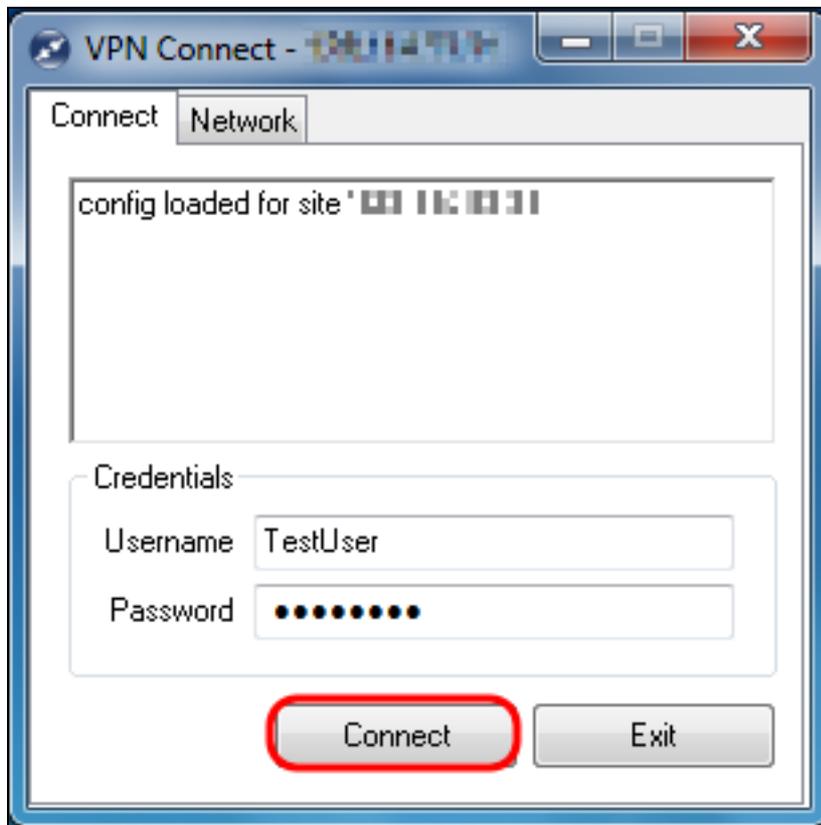
Das Fenster *VPN Connect* (VPN-Verbindung) wird angezeigt.



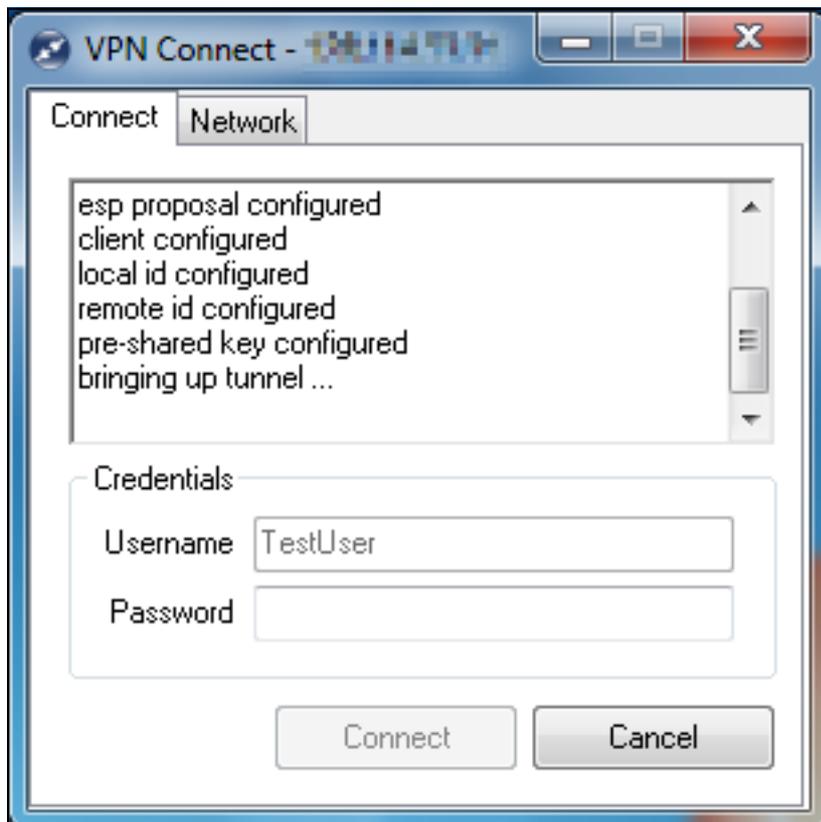
Schritt 22. Geben Sie im Abschnitt *Anmeldedaten* den Benutzernamen und das Kennwort des Kontos ein, das Sie in [Schritt 4 des Abschnitts "IPSec VPN Server-Benutzerkonfiguration"](#) dieses Dokuments eingerichtet haben.

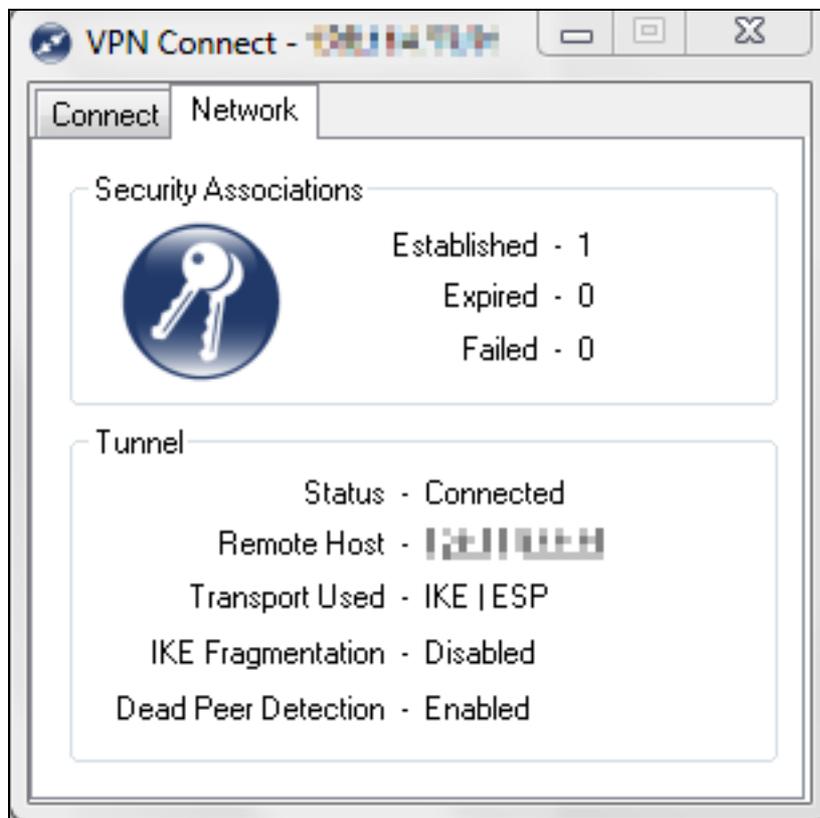


Schritt 23: Klicken Sie auf **Connect** to VPN into the RV130/RV130W.



Der IPSec-VPN-Tunnel ist eingerichtet, und der VPN-Client kann auf die Ressource hinter dem RV130/RV130W-LAN zugreifen.





[Video zu diesem Artikel anzeigen ...](#)

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.