Konfiguration des Shrew VPN Clients auf den Routern RV042, RV042G und RV082 VPN über Windows

Ziel

Ein Virtual Private Network (VPN) ist eine Methode, mit der sich Remote-Benutzer virtuell über das Internet mit einem privaten Netzwerk verbinden können. Ein Client-to-Gateway-VPN verbindet den Desktop oder Laptop eines Benutzers mithilfe von VPN-Client-Software mit einem Remote-Netzwerk. Client-to-Gateway-VPN-Verbindungen sind für Mitarbeiter an Remote-Standorten nützlich, die eine sichere Remote-Verbindung mit dem Büronetzwerk herstellen möchten. Der Shrew VPN Client ist eine auf einem Remote-Host-Gerät konfigurierte Software, die eine einfache und sichere VPN-Verbindung ermöglicht.

In diesem Dokument wird erläutert, wie Sie den Shrew VPN Client für einen Computer konfigurieren, der mit einem RV042-, RV042G- oder RV082-VPN-Router verbunden ist.

Hinweis: In diesem Dokument wird davon ausgegangen, dass Sie den Shrew VPN Client bereits auf den Windows-Computer heruntergeladen haben. Andernfalls müssen Sie eine Client-To-Gateway-VPN-Verbindung konfigurieren, bevor Sie mit der Konfiguration des Shrew VPN beginnen können. Weitere Informationen zum Konfigurieren von Client für Gateway-VPN finden Sie unter *Richten Sie einen Remote-Zugriffstunnel (Client für Gateway) für VPN-Clients auf RV042-, RV042G- und RV082-VPN-Routern ein*.

Unterstützte Geräte

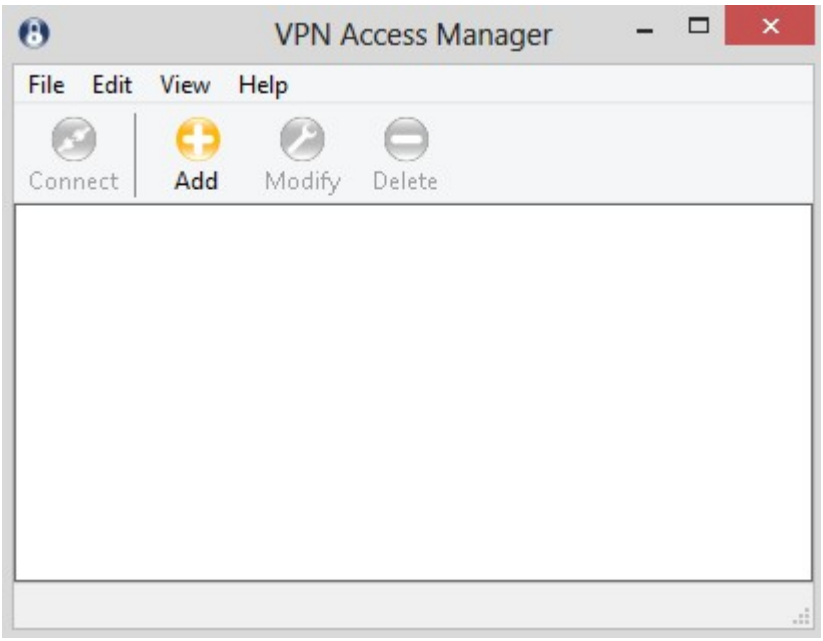
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

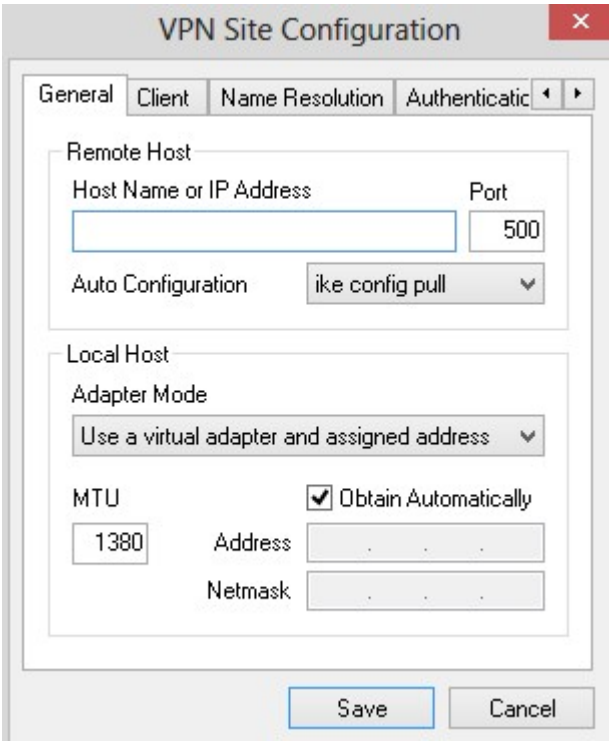
ãƒ» v4.2.2.08

Konfigurieren der Shrew VPN-Clientverbindung unter Windows

Schritt 1: Klicken Sie auf dem Computer auf **Shrew VPN Client**, und öffnen Sie ihn. Das Fenster *Shrew Soft VPN Access Manager* wird geöffnet:

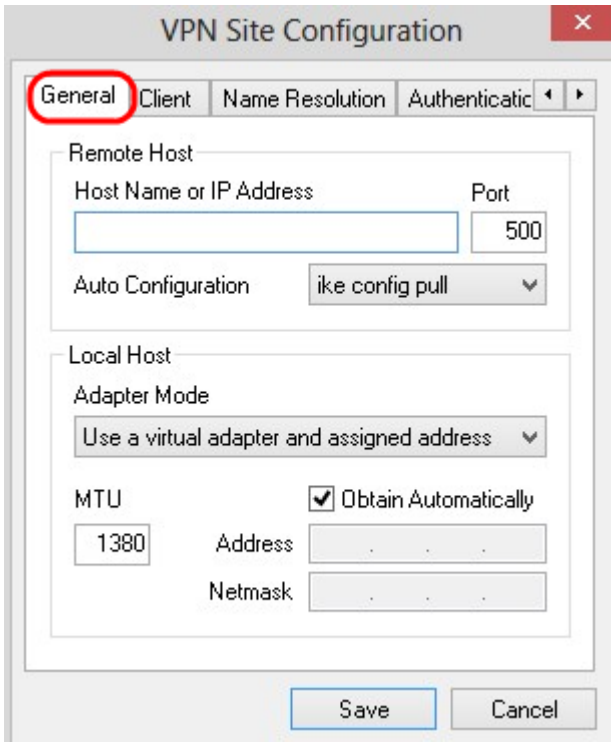


Schritt 2: Klicken Sie auf **Hinzufügen**. Das Fenster *VPN-Standortkonfiguration* wird angezeigt:



Allgemeine Konfiguration

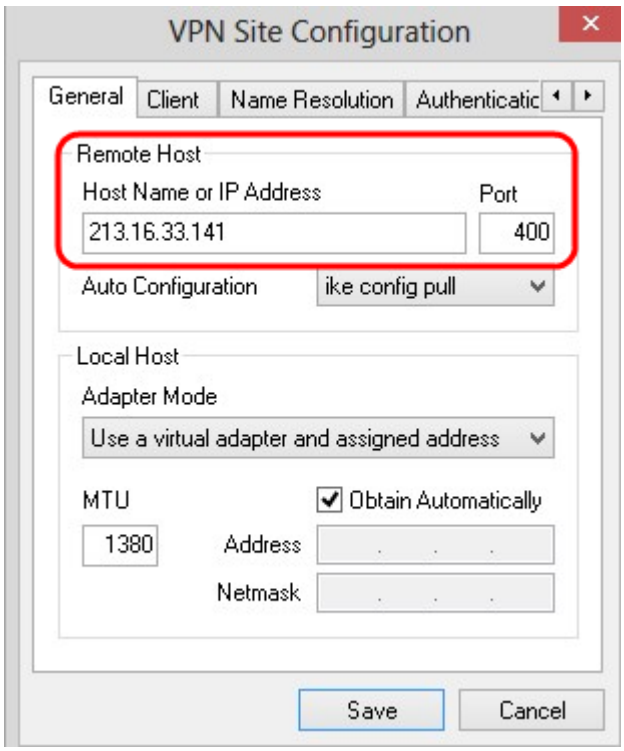
Schritt 1: Klicken Sie auf die Registerkarte **Allgemein**.



Hinweis: Im Abschnitt *"Allgemein*" werden die IP-Adressen des Remote- und des lokalen Hosts konfiguriert. Diese dienen zur Definition der Netzwerkparameter für die Verbindung zwischen Client und Gateway.

Schritt 2: Geben Sie im Feld *Host Name or IP Address (Hostname oder IP-Adresse) die IP-Adresse des Remote-Hosts ein, die der IP-Adresse des konfigurierten WAN entspricht.*

Schritt 3: Geben Sie im Feld *Port* die Nummer des Ports ein, der für die Verbindung verwendet werden soll. Die im abgebildeten Beispiel verwendete Portnummer lautet 400.



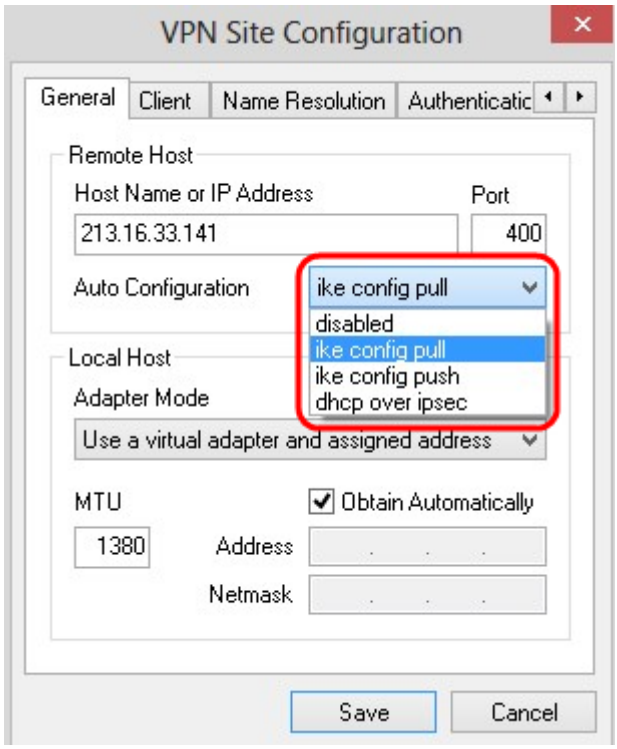
Schritt 4: Wählen Sie aus der Dropdown-Liste *Auto Configuration* (Automatische Konfiguration) die gewünschte Konfiguration aus.

ãƒ» Disabled (Deaktiviert): Die Deaktivierung deaktiviert alle automatischen Client-Konfigurationen.

ãƒ» 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.

ãƒ» 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.

ãƒ» DHCP Over IPSec - Ermöglicht dem Client, Einstellungen vom Computer über DHCP over IPSec anzufordern.

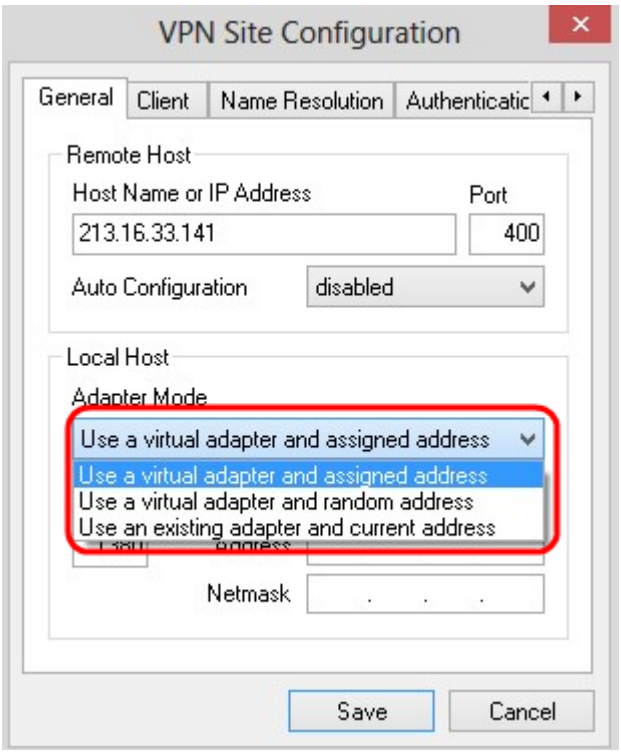


Schritt 5: Wählen Sie aus der Dropdown-Liste *Adaptermodus* den gewünschten Adaptermodus für den lokalen Host auf Basis der automatischen Konfiguration aus.

ãƒ» Virtuellen Adapter und zugewiesene Adresse verwenden â€" Ermöglicht dem Client, einen virtuellen Adapter mit einer angegebenen Adresse zu verwenden.

ãƒ» Virtuellen Adapter und zufällige Adresse verwenden â€" Ermöglicht dem Client, einen virtuellen Adapter mit zufälliger Adresse zu verwenden.

ãƒ» Vorhandenen Adapter und aktuelle Adresse verwenden â€" Verwendet einen vorhandenen Adapter und seine Adresse. Es müssen keine zusätzlichen Informationen eingegeben werden.

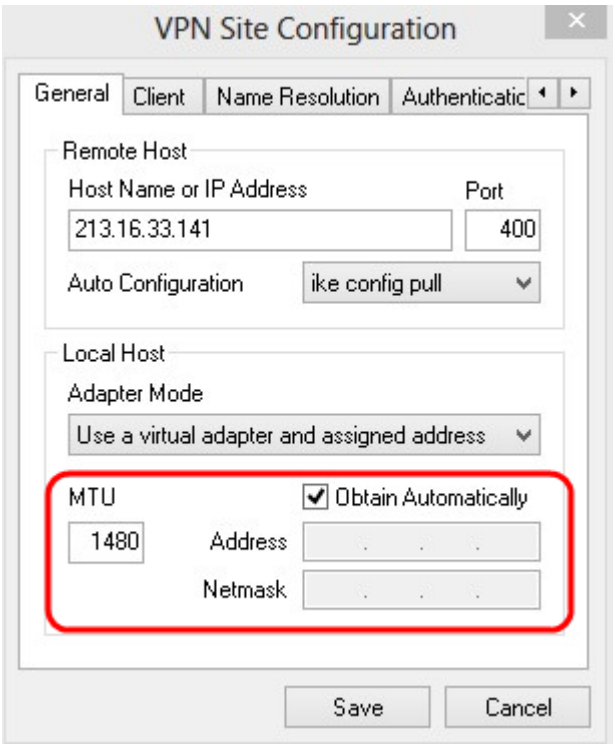


Schritt 6: Geben Sie die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) in das Feld *MTU (MTU) ein,* wenn Sie in Schritt 5 in der Dropdown-Liste *Adaptermodus die* Option **Virtuellen Adapter und zugewiesene Adresse verwenden** auswählen. Die maximale Übertragungseinheit trägt zur Behebung von IP-Fragmentierungsproblemen bei. Der Standardwert ist 1380.

Schritt 7: (Optional) Um die Adresse und die Subnetzmaske automatisch über den DHCP-Server zu erhalten, aktivieren Sie das Kontrollkästchen **Automatisch beziehen**. Diese Option ist nicht für alle Konfigurationen verfügbar.

Schritt 8: Geben Sie die IP-Adresse des Remote-Clients in das *Adressfeld ein,* wenn Sie in Schritt 5 in der *Adaptermodus*-Dropdown-Liste die Option **Virtuellen Adapter und zugewiesene Adresse verwenden** ausgewählt haben.

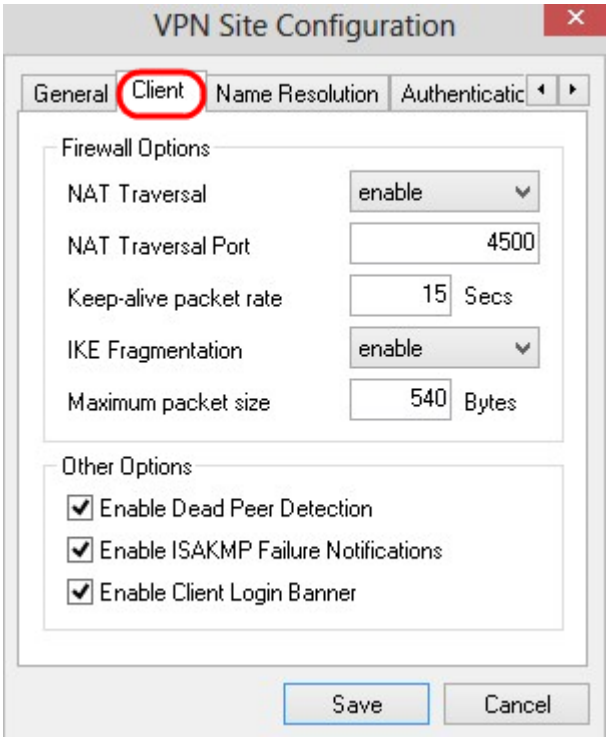
Schritt 9. Geben Sie Subnetzmaske der IP-Adresse des Remote-Clients in das Feld *Netzmaske* ein, wenn Sie in Schritt 5 in der Dropdown-Liste *Adaptermodus die* Option **Virtuellen Adapter und zugewiesene Adresse verwenden** ausgewählt haben.



Schritt 10. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Client-Konfiguration

Schritt 1: Klicken Sie auf die Registerkarte **Client**.



Hinweis: Im Abschnitt "*Client*" können Sie die Firewall-Optionen, die Dead Peer Detection und ISAKMP-Fehlerbenachrichtigungen (Internet Security Association and Key Management Protocol) konfigurieren. Die Einstellungen legen fest, welche Konfigurationsoptionen manuell konfiguriert und welche automatisch bezogen werden.

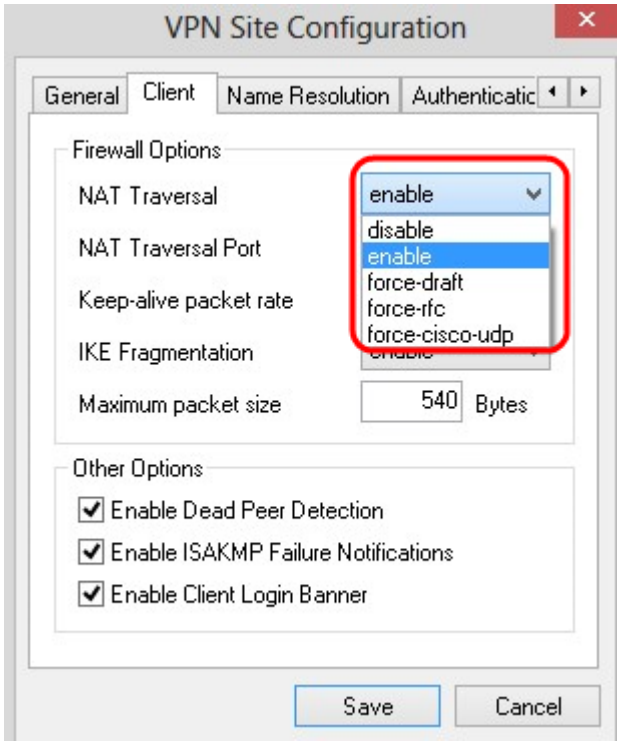
Schritt 2: Wählen Sie in der Dropdown-Liste NAT Traversal die entsprechende NAT-Traversal-Option (Network Address Translation) aus.

ãƒ» Disable (Deaktivieren) - NAT-Protokoll ist deaktiviert.

ãƒ» Aktivieren - IKE-Fragmentierung wird nur verwendet, wenn das Gateway Unterstützung durch Verhandlungen anzeigt.

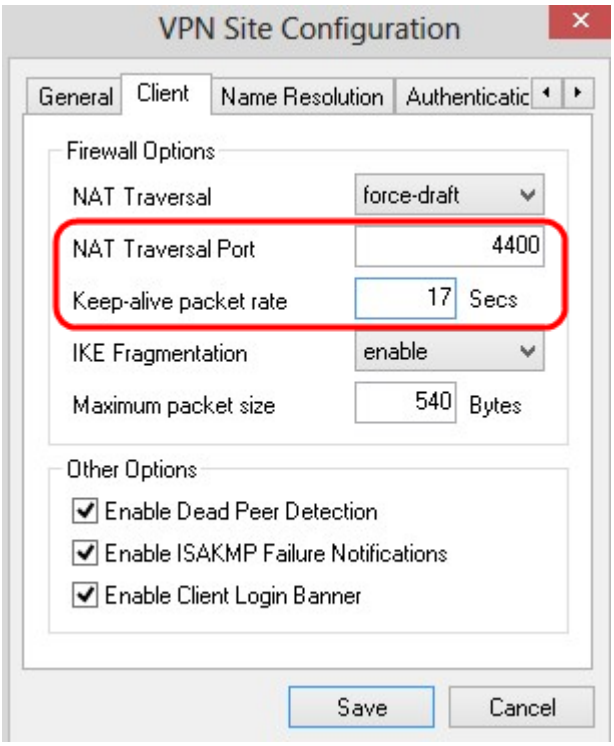
ãƒ» Entwurf erzwingen â€" Der Entwurf des NAT-Protokolls. Sie wird verwendet, wenn das Gateway Unterstützung durch die Aushandlung oder die Erkennung der NAT anzeigt.

ãƒ» Force RFC - Die RFC-Version des NAT-Protokolls. Sie wird verwendet, wenn das Gateway Unterstützung durch die Aushandlung oder die Erkennung der NAT anzeigt.



Schritt 3: Geben Sie den UDP-Port für NAT in das Feld *NAT Traversal Port (NAT-Überbrückungsport*) ein. Der Standardwert ist 4500.

Schritt 4: Geben Sie im Feld *Keep-Alive-Paketrate* einen Wert für die Rate ein, mit der Keepalive-Pakete gesendet werden. Der Wert wird in Sekunden gemessen. Der Standardwert ist 30 Sekunden.

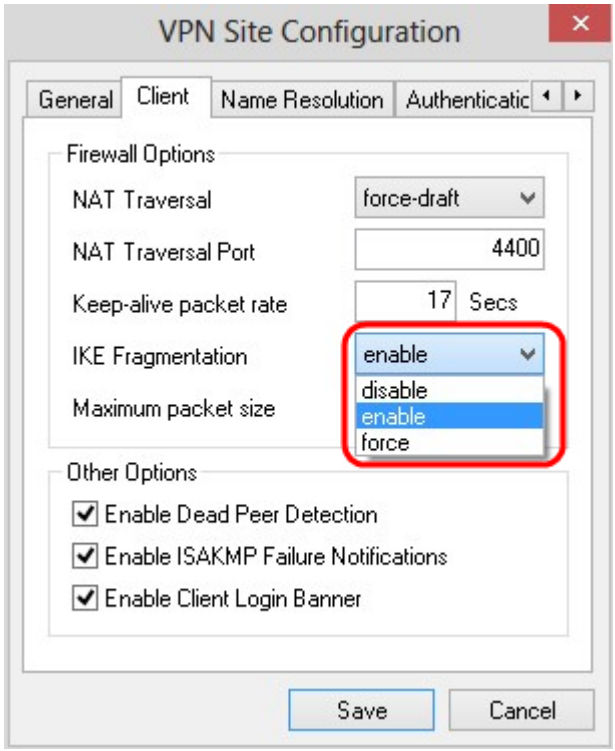


Schritt 5: Wählen Sie in der Dropdown-Liste *IKE Fragmentation* (*IKE-Fragmentierung*) die gewünschte Option aus.

ãƒ» Deaktivieren - IKE-Fragmentierung wird nicht verwendet.

ãƒ» Aktivieren - IKE-Fragmentierung wird nur verwendet, wenn das Gateway Unterstützung durch Verhandlungen anzeigt.

ãƒ» Force â€" IKE-Fragmentierung wird unabhängig von Indikationen oder Erkennung verwendet.



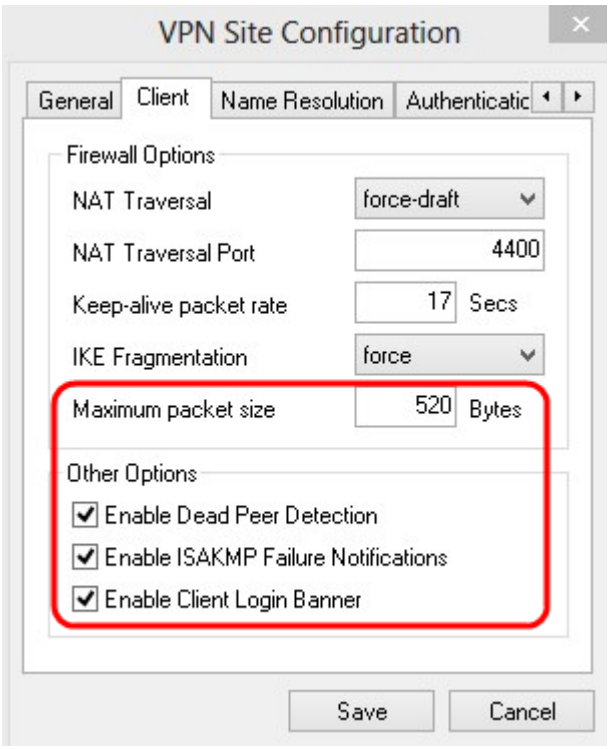
Schritt 6: Geben Sie die maximale Paketgröße in das Feld *Maximale Paketgröße* in Byte ein. Ist die Paketgröße größer als die maximale Paketgröße, wird eine IKE-Fragmentierung durchgeführt. Der

Standardwert ist 540 Byte.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Dead Peer Detection aktivieren,** um dem Computer und dem Client die Erkennung zu ermöglichen, wenn der andere nicht mehr reagieren kann.

Schritt 8: Aktivieren Sie das Kontrollkästchen **ISAKMP-Fehlerbenachrichtigungen aktivieren,** um Fehlerbenachrichtigungen vom VPN-Client **zu** senden.

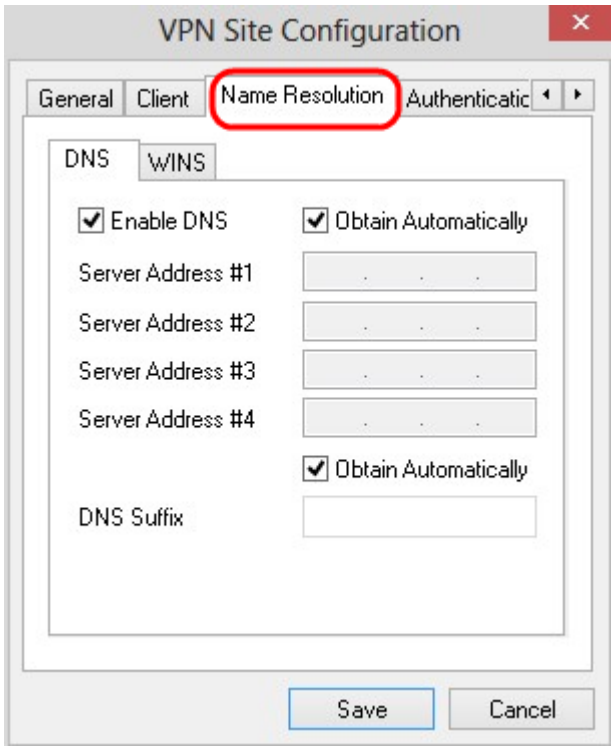
Schritt 9. (Optional) Um ein Anmeldebanner für den Client anzuzeigen, wenn die Verbindung mit dem Kabelmodem hergestellt wurde, aktivieren Sie das Kontrollkästchen **Clientanmeldung aktivieren**.



Schritt 10. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

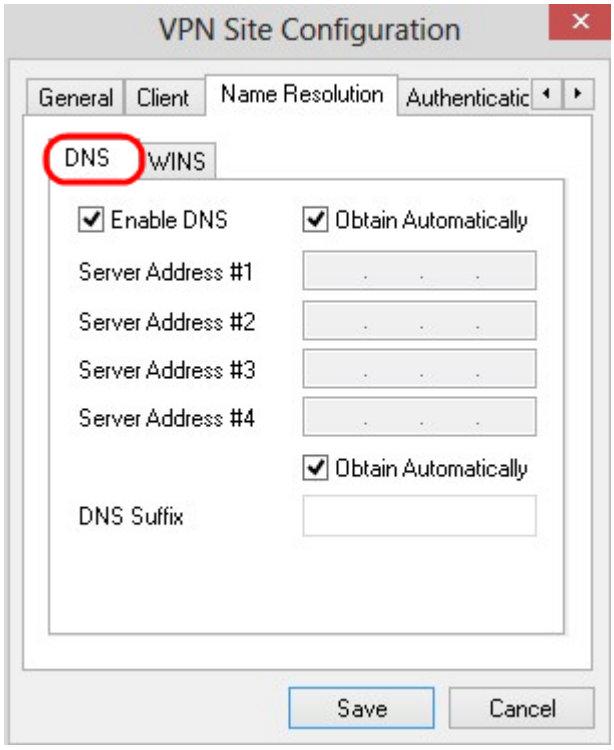
Konfiguration der Namensauflösung

Schritt 1: Klicken Sie auf die Registerkarte **Namensauflösung**.



Hinweis: Im Abschnitt *Namensauflösung* werden die DNS- (Domain Name System) und WIN-Einstellungen (Windows Internet Name Service) konfiguriert.

Schritt 2: Klicken Sie auf die Registerkarte **DNS**.

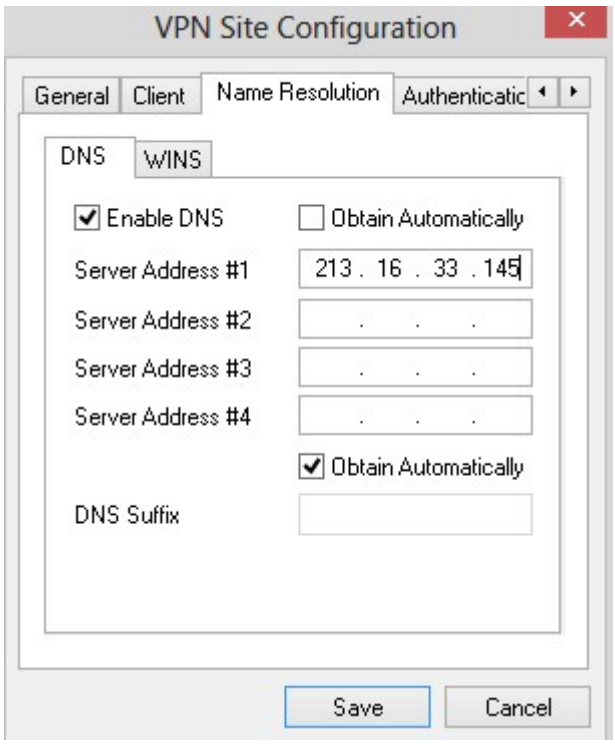


Schritt 3: Markieren Sie **DNS aktivieren**, um das Domain Name System (DNS) zu aktivieren.

Schritt 4: (Optional) Um die DNS-Serveradresse automatisch abzurufen, aktivieren Sie das Kontrollkästchen **Automatisch abrufen**. Wenn Sie diese Option verwenden, fahren Sie mit Schritt 6 fort.

Schritt 5: Geben Sie die DNS-Serveradresse in das Feld *Serveradresse 1 ein*. Wenn ein anderer DNS-

Server vorhanden ist, geben Sie die Adresse dieser Server in die übrigen Felder *Serveradresse* ein.



Schritt 6. (Optional) Um das Suffix des DNS-Servers automatisch abzurufen, aktivieren Sie das Kontrollkästchen **Automatisch abrufen**. Wenn Sie diese Option verwenden, fahren Sie mit Schritt 8 fort.

Schritt 7. Geben Sie das Suffix des DNS-Servers in das Feld *DNS-Suffix* ein.

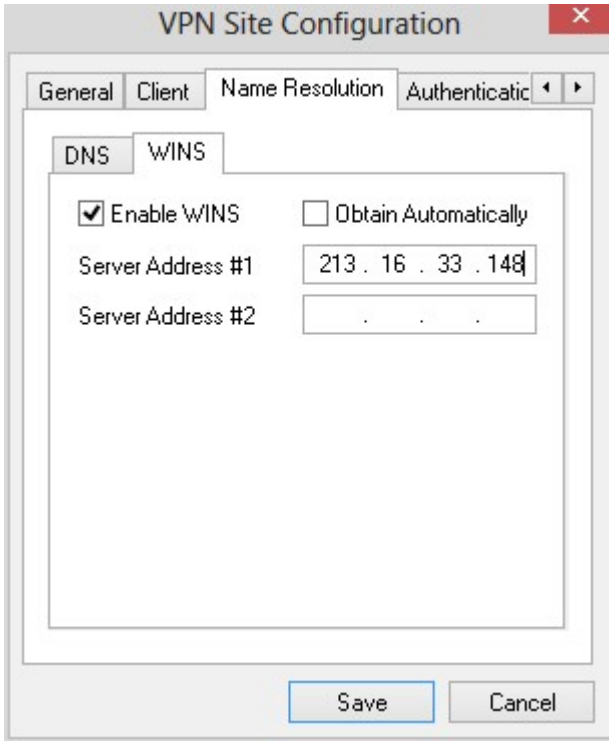
Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Schritt 9. Klicken Sie auf die Registerkarte **WINS**.

Schritt 10. Aktivieren Sie **WINS aktivieren**, um Windows Internet Name Server (WINS) zu aktivieren.

Schritt 11. (Optional) Um die DNS-Serveradresse automatisch abzurufen, aktivieren Sie das Kontrollkästchen **Automatisch abrufen**. Wenn Sie diese Option verwenden, fahren Sie mit Schritt 13 fort.

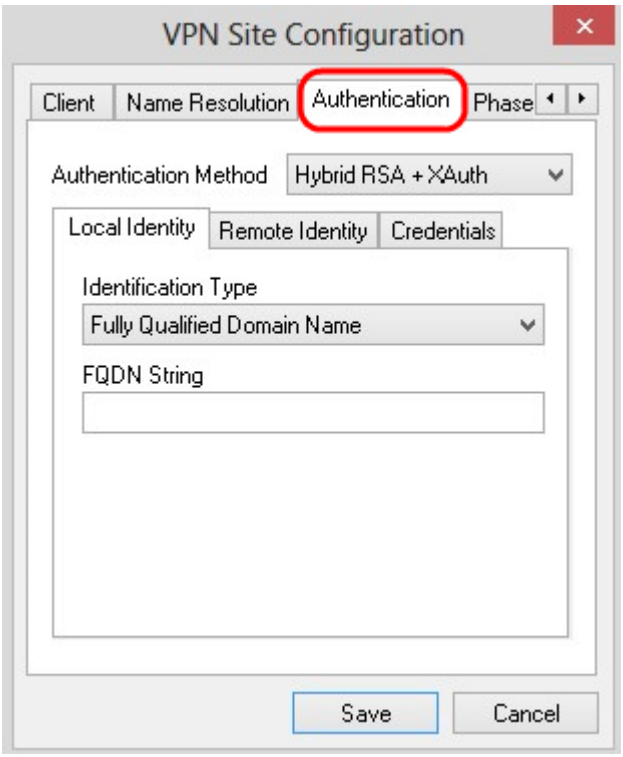
Schritt 12: Geben Sie die Adresse des WINS-Servers in das Feld *Serveradresse 1 ein*. Wenn andere DNS-Server vorhanden sind, geben Sie die Adresse dieser Server in die übrigen Felder *Serveradresse* ein.



Schritt 13: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Authentifizierung

Schritt 1: Klicken Sie auf die Registerkarte **Authentifizierung**.



Hinweis: Im Abschnitt *Authentifizierung* können Sie die Parameter für den Client konfigurieren, der die Authentifizierung behandelt, wenn er versucht, eine ISAKMP-SA einzurichten.

Schritt 2: Wählen Sie in der Dropdown-Liste "*Authentication Method*" die entsprechende Authentifizierungsmethode aus.

ãƒ» Hybrid-RSA + XAuth â€" Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseldateitypen bereitgestellt.

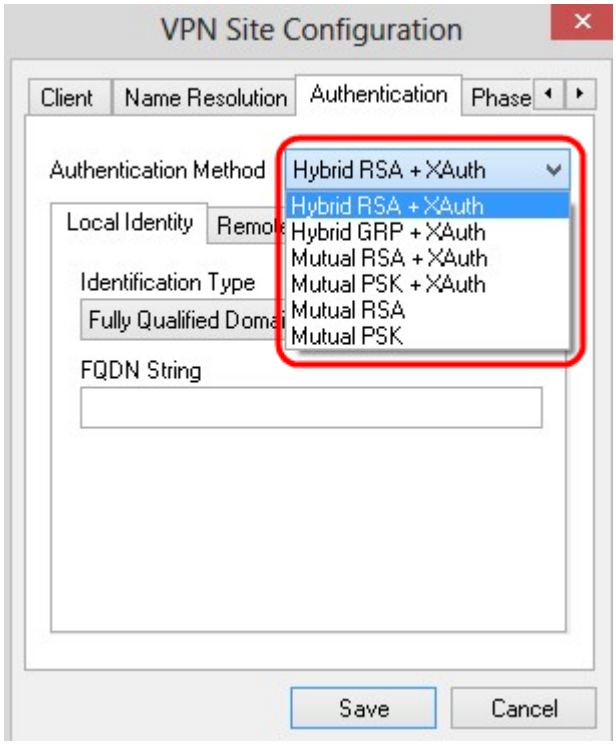
ãƒ» Hybrid GRP + XAuth â€" Die Client-Anmeldeinformationen werden nicht benötigt. Der Client authentifiziert das Gateway. Die Anmeldeinformationen werden in Form einer PEM- oder PKCS12-Zertifikatsdatei und einer Zeichenfolge mit gemeinsamem geheimen Schlüssel bereitgestellt.

ãƒ» Gegenseitiges RSA + XAuth â€" Client und Gateway benötigen beide Anmeldeinformationen zur Authentifizierung. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.

ãƒ» Gegenseitiges PSK + XAuth â€" Client und Gateway benötigen beide Anmeldeinformationen, um sich zu authentifizieren. Die Anmeldeinformationen werden in Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt.

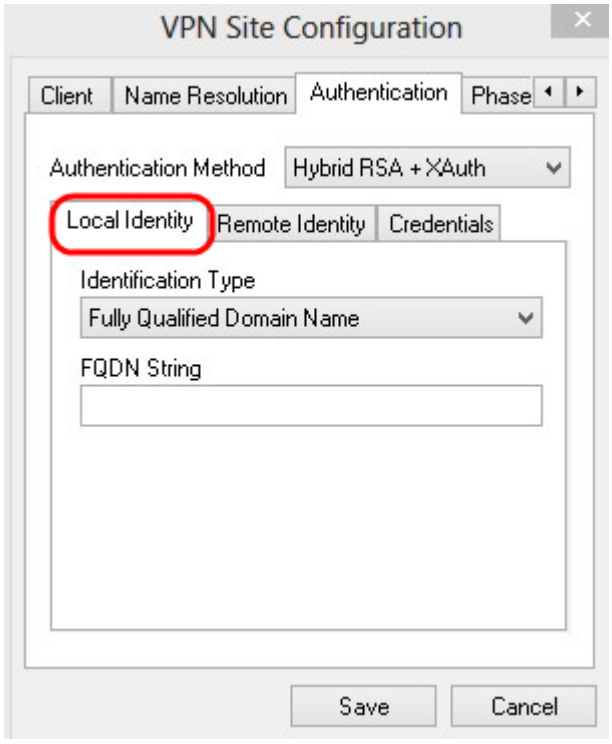
ãƒ» Gegenseitiges RSA - Client und Gateway benötigen zur Authentifizierung Anmeldeinformationen. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen bereitgestellt.

ãƒ» Gegenseitiges PSK - Client und Gateway benötigen beide Anmeldeinformationen, um sich zu authentifizieren. Die Anmeldeinformationen werden in Form einer Zeichenfolge für den gemeinsamen geheimen Schlüssel bereitgestellt.



Lokale Identitätskonfiguration

Schritt 1: Klicken Sie auf die Registerkarte **Lokale Identität**.



Hinweis: Die lokale Identität legt die ID fest, die zur Überprüfung an das Gateway gesendet wird. Im Abschnitt "*Lokale Identität*" werden Identifikationstyp und FQDN-Zeichenfolge (Fully Qualified Domain Name) konfiguriert, um zu bestimmen, wie die ID gesendet wird.

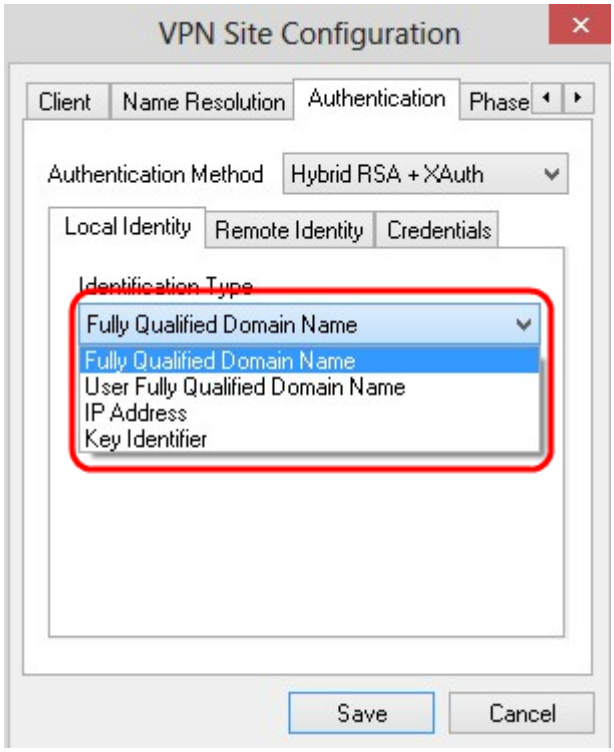
Schritt 2: Wählen Sie in der Dropdown-Liste *Identification Type (Identifikationstyp*) die entsprechende Identifizierungsoption aus. Nicht alle Optionen sind für alle Authentifizierungsmodi verfügbar.

ãƒ» Vollqualifizierter Domänenname: Die Client-Identifizierung der lokalen Identität basiert auf einem vollqualifizierten Domänennamen. Wenn Sie diese Option auswählen, folgen Sie Schritt 3, und fahren Sie dann mit Schritt 7 fort.

ãƒ» Vollqualifizierter Domänenname des Benutzers - Die Client-Identifizierung der lokalen Identität basiert auf dem vollqualifizierten Domänennamen des Benutzers. Wenn Sie diese Option auswählen, folgen Sie Schritt 4, und fahren Sie dann mit Schritt 7 fort.

ãƒ» IP-Adresse - Die Client-Identifizierung der lokalen Identität basiert auf der IP-Adresse. Wenn Sie **Eine erkannte lokale Hostadresse verwenden** aktivieren, wird die IP-Adresse automatisch erkannt. Wenn Sie diese Option auswählen, befolgen Sie Schritt 5, und fahren Sie dann mit Schritt 7 fort.

ãƒ» Key Identifier â€" Die Client-Identifikation des lokalen Clients wird anhand eines Key Identifier identifiziert. Wenn Sie diese Option auswählen, befolgen Sie die Schritte 6 und 7.



Schritt 3: Geben Sie den vollqualifizierten Domänennamen als DNS-Zeichenfolge in das Feld *FQDN-Zeichenfolge* ein.

Schritt 4: Geben Sie den vollqualifizierten Domänennamen des Benutzers als DNS-Zeichenfolge in das Feld *UFQDN-Zeichenfolge ein*.

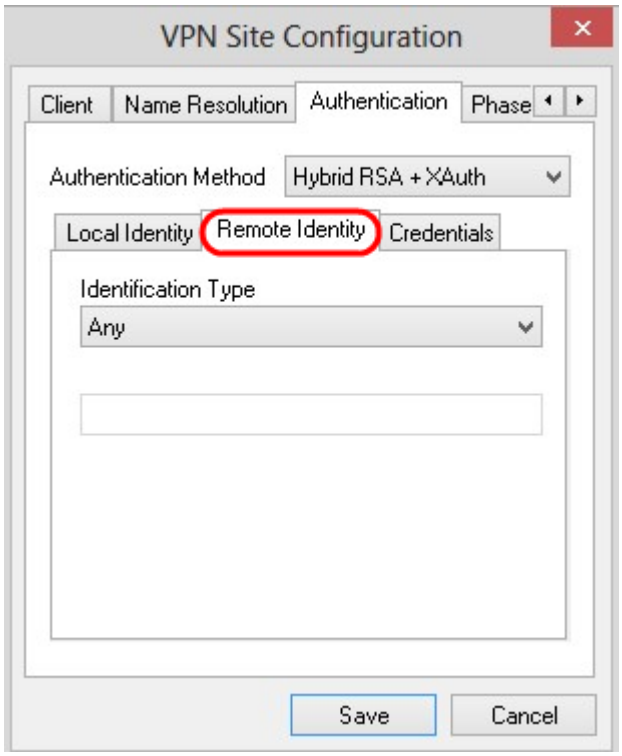
Schritt 5: Geben Sie die IP-Adresse in das Feld *UFQDN-Zeichenfolge* ein.

Schritt 6: Geben Sie die Schlüsselkennung ein, um den lokalen Client in der *Schlüssel-ID-Zeichenfolge* zu identifizieren.

Schritt 7. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Remote-Identitätskonfiguration

Schritt 1: Klicken Sie auf die Registerkarte **Remote Identity**.



Hinweis: Die Remote-Identität verifiziert die ID des Gateways. Im Abschnitt "*Remote Identity*" (*Remote-Identität*) wird der Identifikationstyp konfiguriert, um zu bestimmen, wie die ID verifiziert wird.

Schritt 2: Wählen Sie in der Dropdown-Liste *Identification Type (Identifikationstyp*) die entsprechende Identifizierungsoption aus.

ãƒ» Beliebig - Der Remote-Client kann jeden Wert oder jede ID zur Authentifizierung akzeptieren.

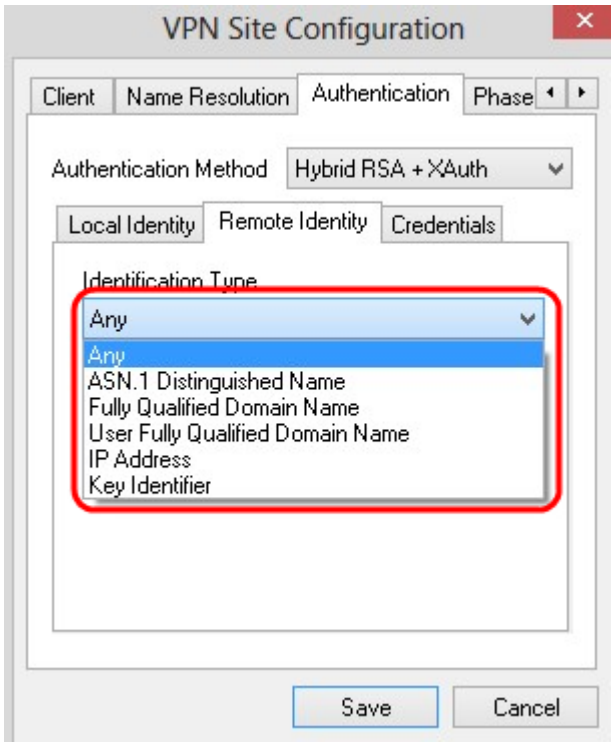
ãƒ» ASN.1 Distinguished Name: Der Remote-Client wird automatisch anhand einer PEM- oder PKCS12-Zertifikatsdatei identifiziert. Sie können diese Option nur wählen, wenn Sie in Schritt 2 des Abschnitts "*Authentifizierung"* eine RSA-Authentifizierungsmethode auswählen. Aktivieren Sie das Kontrollkästchen **Betreff im empfangenen Zertifikat verwenden, aber nicht mit einem bestimmten Wert vergleichen,** um das Zertifikat automatisch zu erhalten. Wenn Sie diese Option wählen, folgen Sie Schritt 3 und fahren dann mit Schritt 8 fort.

ãƒ» Vollqualifizierter Domänenname: Die Client-Identifizierung der Remote-Identität basiert auf dem vollqualifizierten Domänennamen. Sie können diese Option nur wählen, wenn Sie in Schritt 2 des Abschnitts "*Authentifizierung"* eine PSK-Authentifizierungsmethode auswählen. Wenn Sie diese Option auswählen, folgen Sie Schritt 4, und fahren Sie dann mit Schritt 8 fort.

ãƒ» Vollqualifizierter Domänenname des Benutzers - Die Client-Identifizierung der Remote-Identität basiert auf dem vollqualifizierten Domänennamen des Benutzers. Sie können diese Option nur wählen, wenn Sie in Schritt 2 des Abschnitts "*Authentifizierung"* eine PSK-Authentifizierungsmethode auswählen. Wenn Sie diese Option wählen, folgen Sie Schritt 5 und fahren dann mit Schritt 8 fort.

ãƒ» IP-Adresse - Die Client-Identifizierung der Remote-Identität basiert auf der IP-Adresse. Wenn Sie **Eine erkannte lokale Hostadresse verwenden** aktivieren, wird die IP-Adresse automatisch erkannt. Wenn Sie diese Option wählen, folgen Sie Schritt 6 und fahren dann mit Schritt 8 fort.

ãƒ» Key Identifier â€" Die Client-Identifikation des entfernten Clients basiert auf einem Key Identifier. Wenn Sie diese Option auswählen, befolgen Sie die Schritte 7 und 8.



Schritt 3: Geben Sie die DN-Zeichenfolge ASN.1 in das Feld *DN-Zeichenfolge ASN.1 ein*.

Schritt 4: Geben Sie den vollqualifizierten Domänennamen als DNS-Zeichenfolge in das Feld *FQDN-Zeichenfolge* ein.

Schritt 5: Geben Sie den vollqualifizierten Domänennamen des Benutzers als DNS-Zeichenfolge in das Feld *UFQDN-Zeichenfolge* ein.

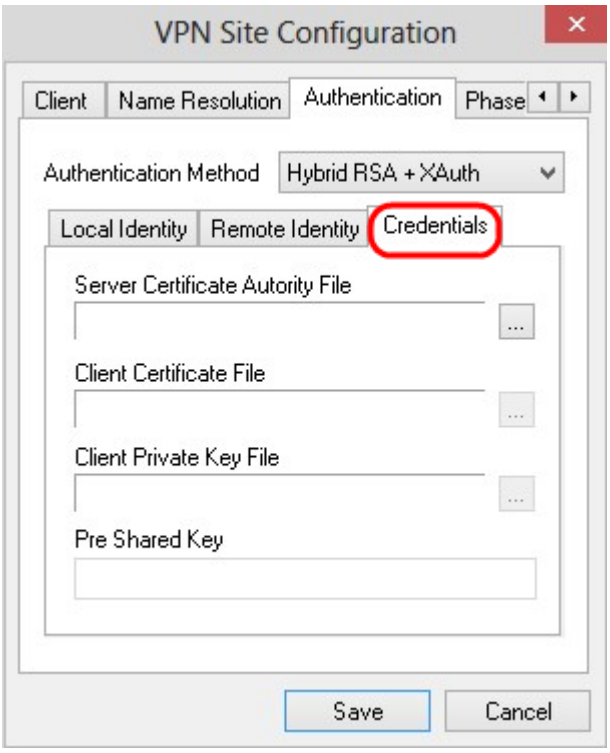
Schritt 6: Geben Sie die IP-Adresse in das Feld *UFQDN-Zeichenfolge* ein.

Schritt 7. Geben Sie die Schlüsselkennung ein, um den lokalen Client im Feld *Schlüssel-ID-Zeichenfolge* zu identifizieren.

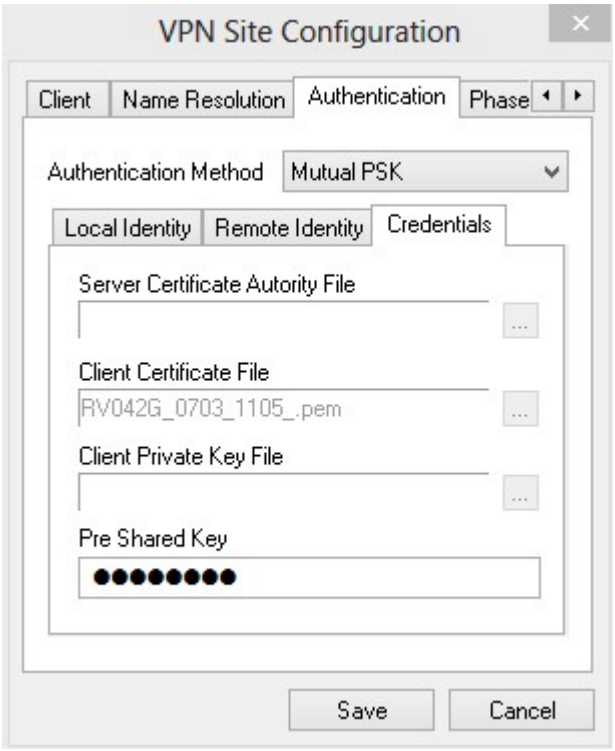
Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Konfiguration der Anmeldeinformationen

Schritt 1: Klicken Sie auf die Registerkarte **Anmeldedaten**.



Hinweis: Im Abschnitt "*Anmeldedaten*" wird der vorinstallierte Schlüssel konfiguriert.



Schritt 2: Um die Serverzertifikatdatei auszuwählen, klicken Sie auf **...** neben dem Feld *Datei* der *Serverzertifikatbehörde* und wählen Sie den Pfad aus, unter dem Sie die Serverzertifikatdatei auf Ihrem PC gespeichert haben.

Schritt 3: Um die Client-Zertifikatsdatei auszuwählen, klicken Sie auf **...** neben dem Feld *Client Certificate File (Client-Zertifikatdatei*) und wählen Sie den Pfad aus, unter dem Sie die Client Certificate File (Client-Zertifikatdatei) auf Ihrem PC gespeichert haben.

Schritt 4: Um die Datei für den privaten Clientschlüssel auszuwählen, klicken Sie auf **...** -Symbol

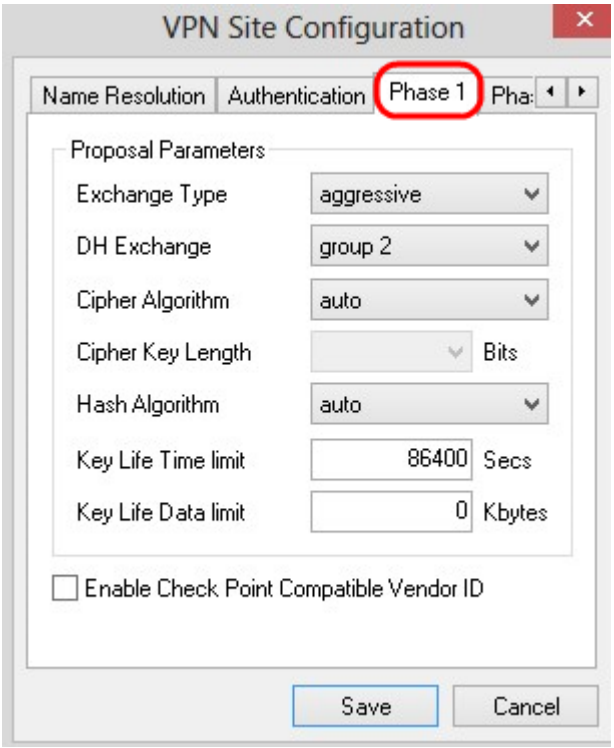
neben dem Feld *Client Private Key File* (Datei für privaten Client-Schlüssel) und wählen Sie den Pfad aus, unter dem Sie die Datei für privaten Client-Schlüssel auf Ihrem PC gespeichert haben.

Schritt 5: Geben Sie den vorinstallierten Schlüssel in das Feld *Vorinstallierter Schlüssel* ein. Dabei sollte es sich um denselben Schlüssel handeln, den Sie auch bei der Konfiguration des Tunnels verwenden.

Schritt 6: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Konfiguration von Phase 1

Schritt 1: Klicken Sie auf die Registerkarte **Phase 1**.

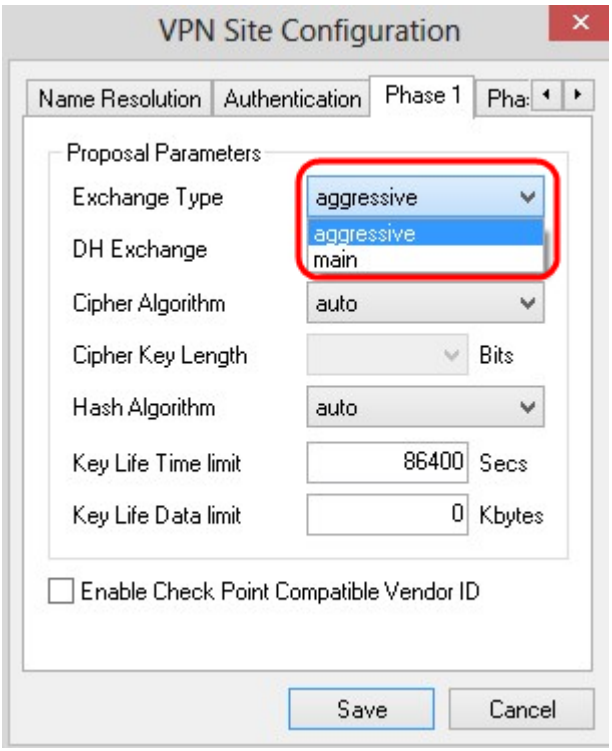


Hinweis: Im Abschnitt zu *Phase 1* können Sie die Parameter so konfigurieren, dass eine ISAKMP-SA mit dem Client-Gateway erstellt werden kann.

Schritt 2: Wählen Sie den entsprechenden Schlüsselaustauschtyp aus der Dropdown-Liste *Exchange Type (Austauschtyp*) aus.

ãƒ» Main (Hauptmodus): Die Identität der Peers ist gesichert.

ãƒ» Aggressive (Aggressiv): Die Identität der Peers ist nicht gesichert.



Schritt 3: Wählen Sie in der Dropdown-Liste *DH Exchange* (*DH-Austausch*) die Gruppe aus, die Sie während der Konfiguration der VPN-Verbindung ausgewählt haben.

Schritt 4: Wählen Sie in der Dropdown-Liste *Cipher Algorithm* (*Verschlüsselungsalgorithmus*) die entsprechende Option aus, die während der Konfiguration der VPN-Verbindung ausgewählt wurde.

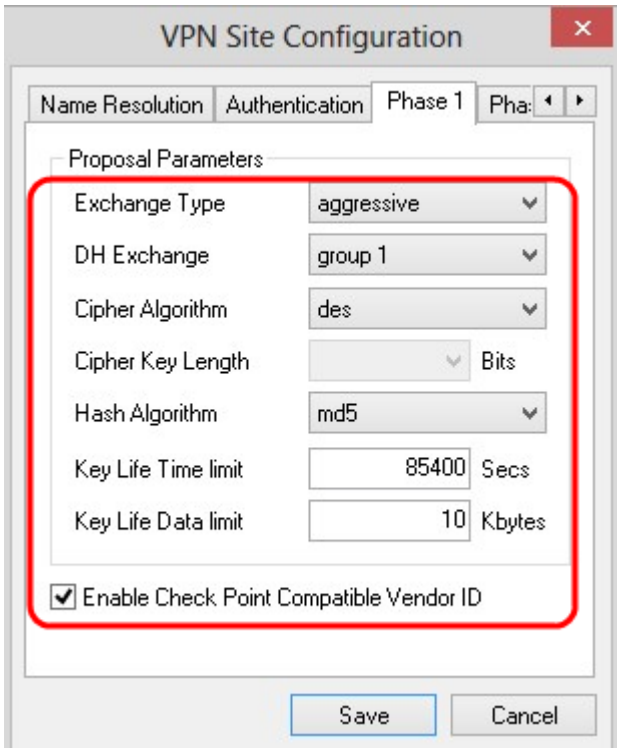
Schritt 5: Wählen Sie in der Dropdown-Liste *Cipher Key Length* (Länge des Schlüssels) die Option aus, die der Schlüssellänge der Option entspricht, die Sie während der Konfiguration der VPN-Verbindung ausgewählt haben.

Schritt 6: Wählen Sie in der Dropdown-Liste *Hash Algorithm* (Hash-Algorithmus) die Option aus, die Sie während der Konfiguration der VPN-Verbindung gewählt haben.

Schritt 7. Geben Sie im Feld *Key Life Time* (Limit für die Schlüssellebensdauer) den Wert ein, der während der Konfiguration der VPN-Verbindung verwendet wird.

Schritt 8: Geben Sie im Feld *Key Life Data* limit (Limit für Lebensdauerdaten) den zu schützenden Wert in Kilobyte ein. Der Standardwert ist 0, wodurch die Funktion deaktiviert wird.

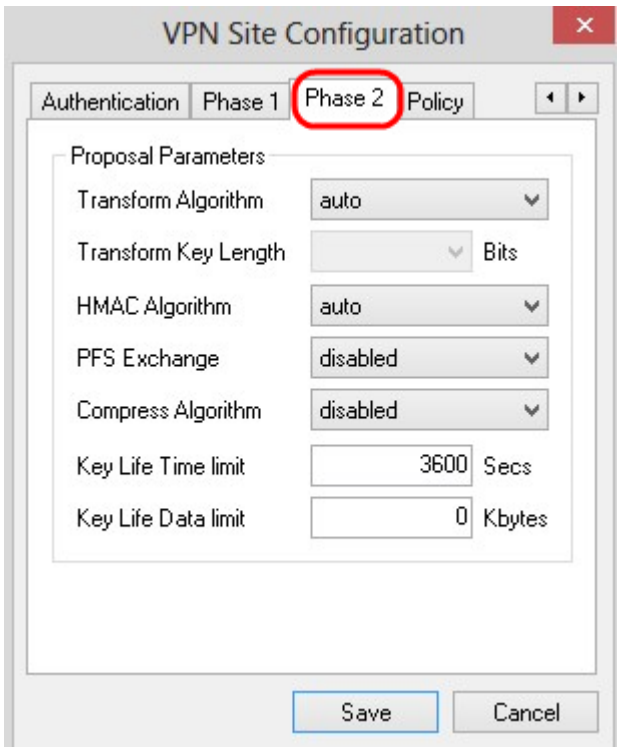
Schritt 9: Aktivieren Sie optional das Kontrollkästchen **Enable Check Point Compatible Vendor ID (Prüfpunkt-kompatible Lieferanten-ID aktivieren**).



Schritt 10. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Konfiguration von Phase 2

Schritt 1: Klicken Sie auf die Registerkarte **Phase 2**.



Hinweis: Im Abschnitt zu *Phase 2* können Sie die Parameter so konfigurieren, dass eine IPsec-Sicherheitszuordnung mit dem Remote-Client-Gateway eingerichtet werden kann.

Schritt 2: Wählen Sie in der Dropdown-Liste *Transform Algorithm (Umwandlungsalgorithmus*) die Option aus, die während der Konfiguration der VPN-Verbindung ausgewählt wurde.

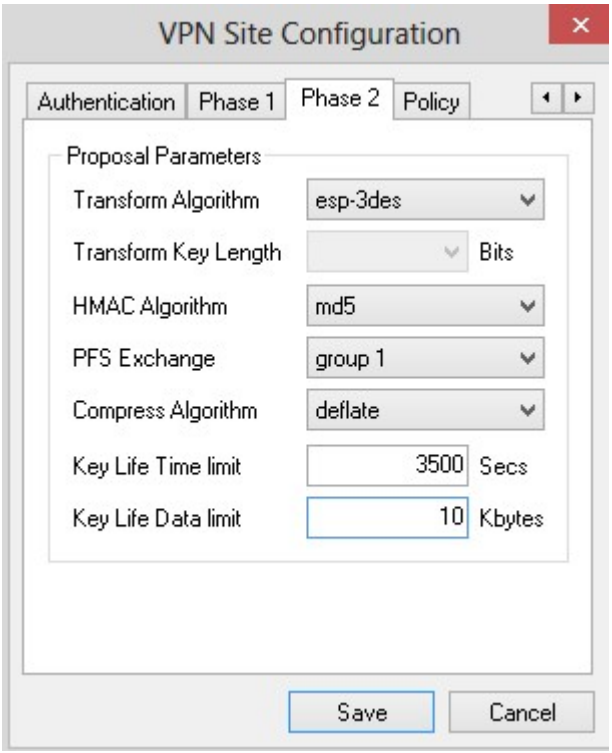
Schritt 3: Wählen Sie in der Dropdown-Liste "*Transform Key Length*" (Schlüssellänge umwandeln) die Option aus, die der Schlüssellänge der Option entspricht, die während der Konfiguration der VPN-Verbindung ausgewählt wurde.

Schritt 4: Wählen Sie in der Dropdown-Liste *HMAC Algorithm* (HMAC-Algorithmus) die Option aus, die während der Konfiguration der VPN-Verbindung ausgewählt wurde.

Schritt 5: Wählen Sie in der Dropdown-Liste *PFS Exchange* die Option aus, die während der Konfiguration der VPN-Verbindung ausgewählt wurde.

Schritt 6: Geben Sie in das Feld *Key Life Time (Schlüssellaufzeit*) den Wert ein, der während der Konfiguration der VPN-Verbindung verwendet wird.

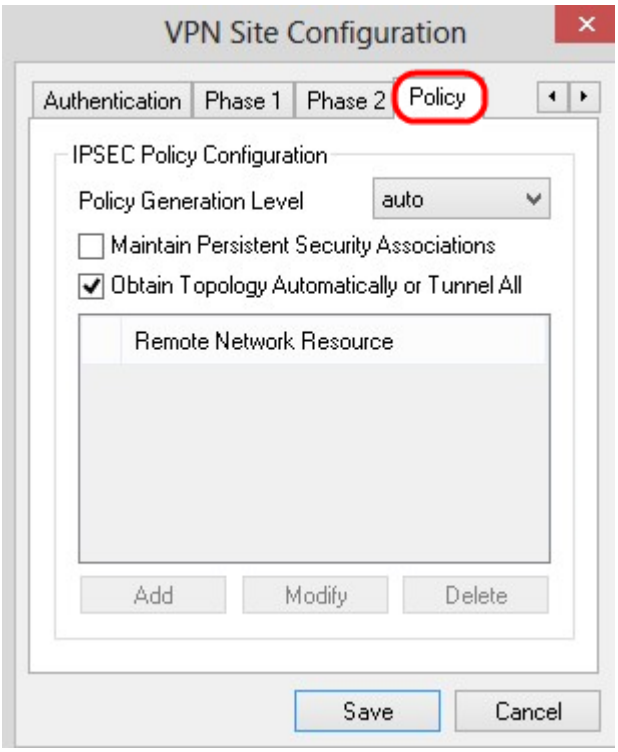
Schritt 7. Geben Sie im Feld *Limit für wichtige Lebensdauerdaten* den zu schützenden Wert in Kilobyte ein. Der Standardwert ist 0, wodurch die Funktion deaktiviert wird.



Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Richtlinienkonfiguration

Schritt 1:Klicken Sie auf die Registerkarte **Policy**.



Hinweis: Im Abschnitt "*Policy*" (Richtlinie) wird die IPSEC-Richtlinie definiert, die erforderlich ist, damit der Client für die Standortkonfiguration mit dem Host kommunizieren kann.

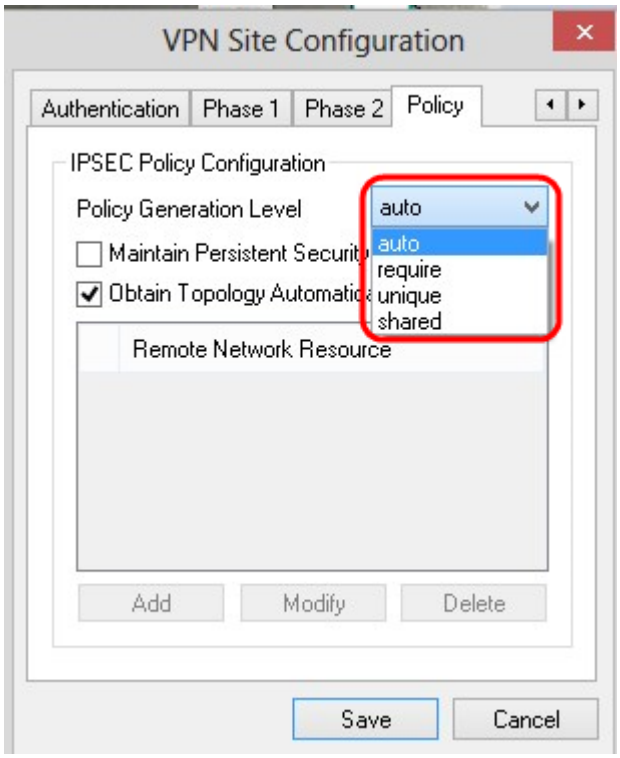
Schritt 2: Wählen Sie in der Dropdown-Liste *Policy Generation Level (Richtlinienerstellungsebene*) die gewünschte Option aus.

ãƒ» Auto â€" Die erforderliche IPsec-Richtlinienebene wird automatisch bestimmt.

ãƒ» Erforderlich - Es wird keine eindeutige Sicherheitszuordnung für jede Richtlinie ausgehandelt.

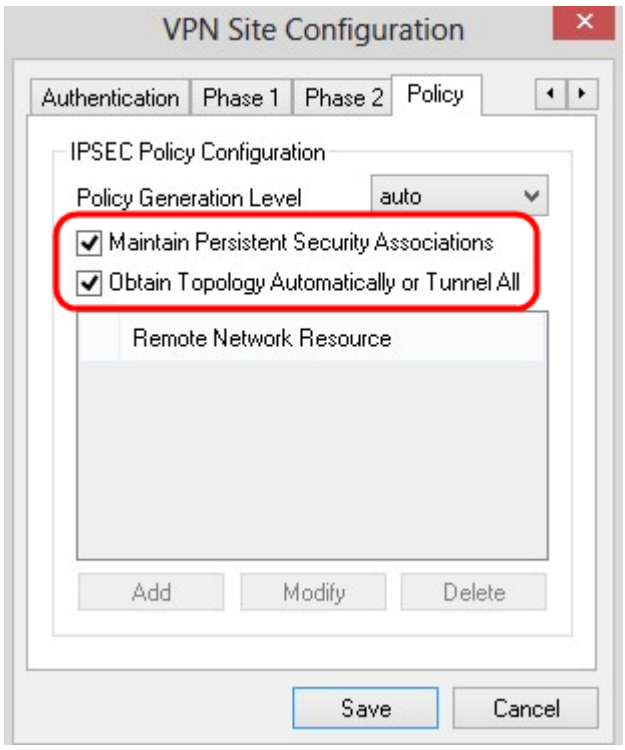
ãƒ» Eindeutig - Für jede Richtlinie wird eine eindeutige Sicherheitszuordnung ausgehandelt.

ãƒ» Shared (Gemeinsam genutzt): Die entsprechende Richtlinie wird auf der erforderlichen Ebene erstellt.

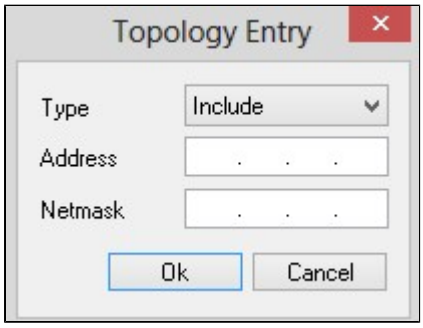


Schritt 3. (Optional) Um die IPSec-Aushandlungen zu ändern, aktivieren Sie das Kontrollkästchen **Permanente Sicherheitszuordnungen verwalten**. Wenn diese Option aktiviert ist, wird die Verhandlung für jede Richtlinie direkt nach dem Herstellen der Verbindung durchgeführt. Wenn die Option deaktiviert ist, wird die Verhandlung nach Bedarf durchgeführt.

Schritt 4. (Optional) Um eine automatisch bereitgestellte Liste der Netzwerke vom Gerät zu erhalten oder alle Pakete standardmäßig an den RV0XX zu senden, aktivieren Sie das Kontrollkästchen **Topologie automatisch beziehen oder Tunnel All (Alle Tunnel)**. Ist das Kontrollkästchen deaktiviert, muss die Konfiguration manuell durchgeführt werden. Ist diese Einstellung markiert, fahren Sie mit Schritt 10 fort.



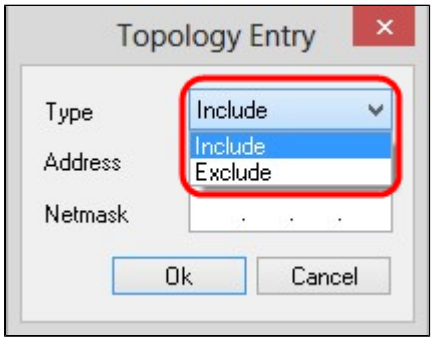
Schritt 5: Klicken Sie auf **Hinzufügen**, um der Tabelle einen Topologieeintrag hinzuzufügen. Das Fenster *Topologieeintrag* wird angezeigt.



Schritt 6: Wählen Sie in der Dropdown-Liste *Typ* die gewünschte Option aus.

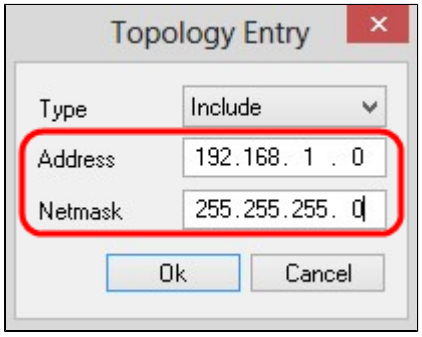
ãƒ» Einschließen - Der Netzwerkzugriff erfolgt über ein VPN-Gateway.

ãƒ» Ausschließen - Der Zugriff auf das Netzwerk erfolgt über lokale Verbindungen.

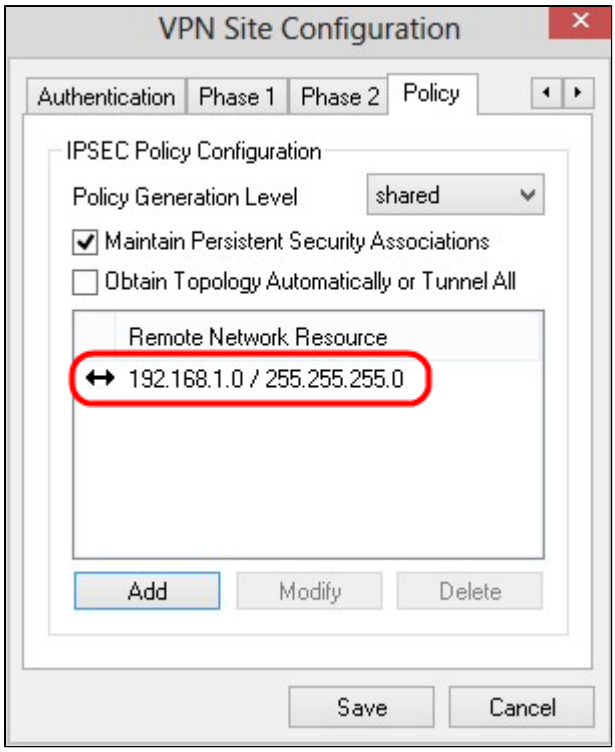


Schritt 7. Geben Sie im Feld *Adresse* die IP-Adresse des RV0XX ein.

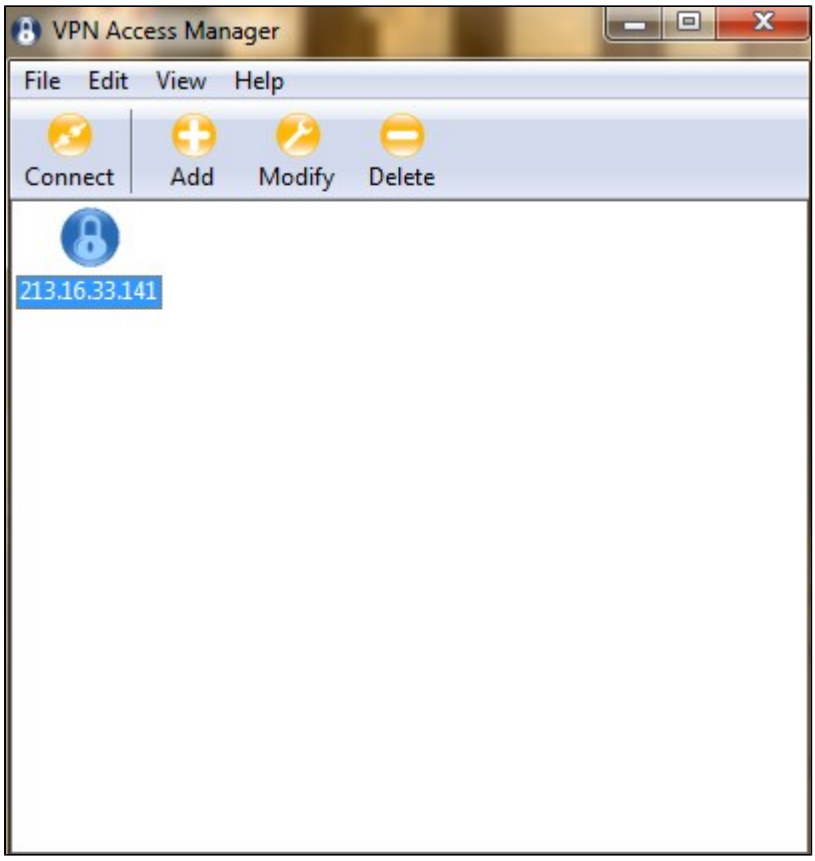
Schritt 8: Geben Sie in das Feld *Netzmaske* die Adresse der Subnetzmaske des Geräts ein.



Schritt 9. Klicken Sie auf **OK**. Die IP-Adresse und die Subnetzmaskenadresse des RV0XX werden in der Liste der Remote-Netzwerkressourcen angezeigt.



Schritt 10. Klicken Sie auf **Speichern**, um den Benutzer zum Fenster *VPN Access Manager* zurückzukehren, in dem die neue VPN-Verbindung angezeigt wird.

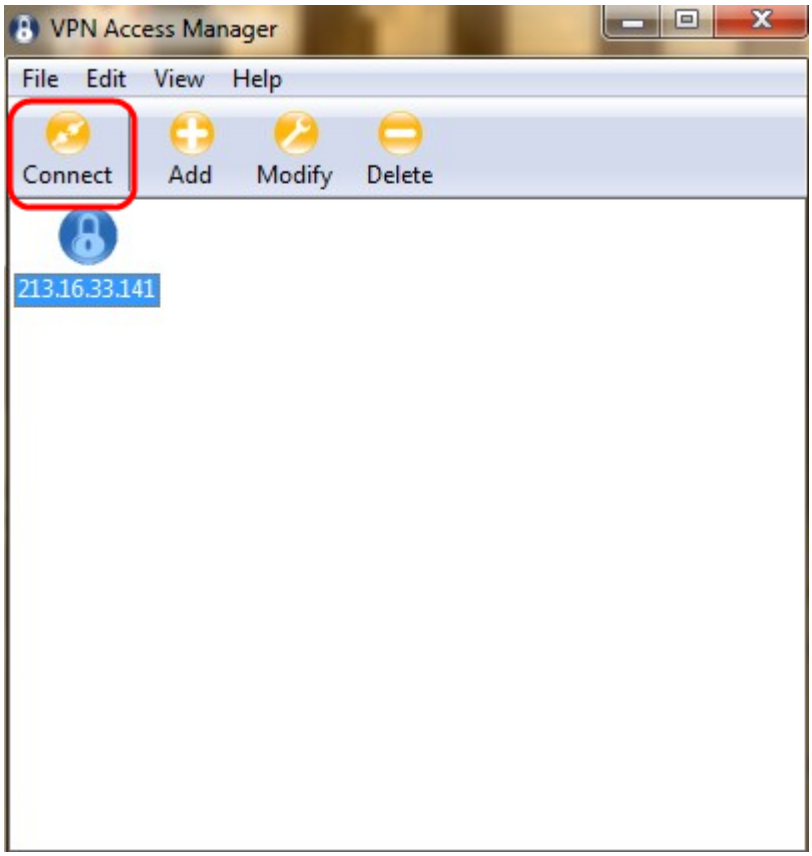


Verbinden

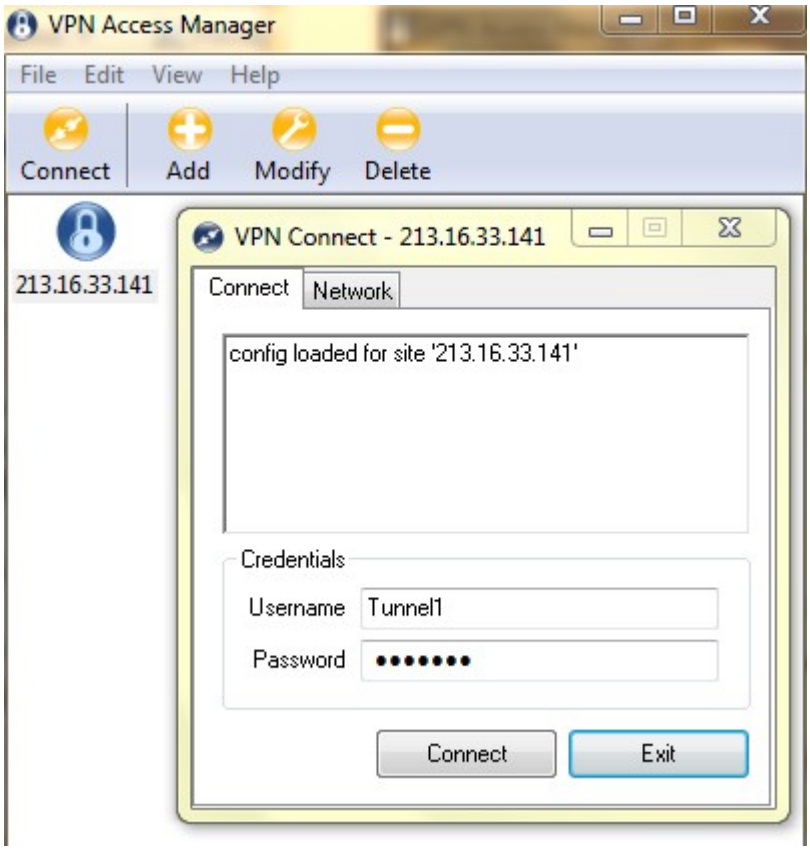
In diesem Abschnitt wird erläutert, wie Sie die VPN-Verbindung nach der Konfiguration aller Einstellungen einrichten. Die erforderlichen Anmeldeinformationen entsprechen denen des auf dem Gerät konfigurierten VPN-Clientzugriffs.

Schritt 1: Klicken Sie auf die gewünschte VPN-Verbindung.

Schritt 2: Klicken Sie auf **Verbinden.**



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



Schritt 3: Geben Sie den Benutzernamen für das VPN in das Feld *Username (Benutzername*) ein.

Schritt 4: Geben Sie das Kennwort für das VPN-Benutzerkonto in das Feld *Kennwort ein*.

Schritt 5: Klicken Sie auf **Verbinden**. Das Fenster *Shrew Soft VPN Connect* wird angezeigt:

Schritt 6. (Optional) Klicken Sie auf **Trennen**, um die Verbindung zu deaktivieren.

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.