

Konfigurieren des Shrew Soft VPN Clients mit dem RV160 und RV260

Ziel

In diesem Dokument wird erläutert, wie Sie die erforderlichen Einstellungen für die Verbindung des Shrew Soft VPN-Clients über Router der Serie RV160 oder RV260 konfigurieren.

Einführung in die Grundlagen von VPN

Ein Virtual Private Network (VPN) ist eine hervorragende Möglichkeit, Remote-Benutzer mit einem sicheren Netzwerk zu verbinden. Sie stellt eine verschlüsselte Verbindung über ein weniger sicheres Netzwerk wie das Internet her.

Ein VPN-Tunnel richtet ein privates Netzwerk ein, das Daten sicher mit Verschlüsselung und Authentifizierung senden kann. Unternehmensbüros verwenden häufig eine VPN-Verbindung, da es sowohl nützlich als auch notwendig ist, ihren Mitarbeitern den Zugriff auf ihre internen Ressourcen zu ermöglichen, selbst wenn sie sich außerhalb des Büros befinden.

Der RV160-Router unterstützt bis zu 10 VPN-Tunnel und der RV260 bis zu 20.

In diesem Artikel werden die Schritte zur Konfiguration des RV160/RV260-Routers und des Shrew Soft VPN-Clients beschrieben. Sie erfahren, wie Sie eine Benutzergruppe, ein Benutzerkonto, ein IPsec-Profil und ein Client-to-Site-Profil erstellen. Auf dem Shrew Soft VPN-Client wird die Konfiguration der Registerkarten Allgemein, Client, Namensauflösung, Authentifizierung, Phase 1 und Phase 2 erläutert.

Was sind die Vor- und Nachteile, wenn ich ein VPN verwenden möchte?

VPNs eignen sich für Anwendungsfälle, die in vielen Branchen und Geschäftsbereichen üblich sind. Die folgende Tabelle zeigt einige Vor- und Nachteile der Verwendung eines VPN.

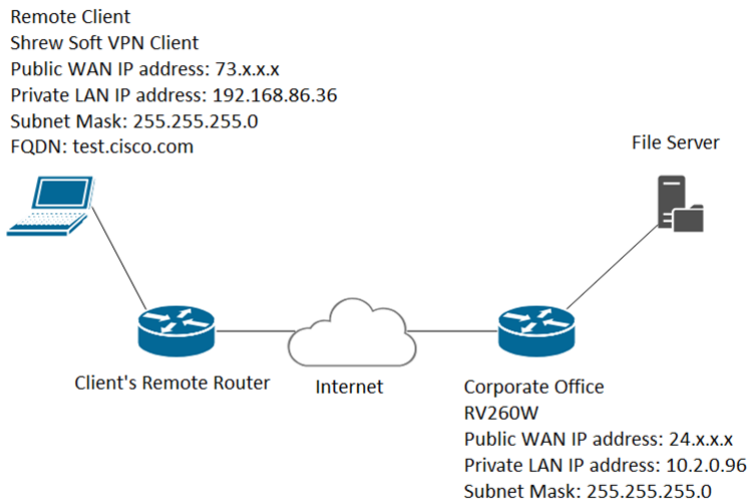
Vorteile	Verbindungen
Bietet sichere Kommunikation, Komfort und Zugriffsmöglichkeiten mit Zugriffsrechten, die auf einzelne Benutzer wie Mitarbeiter, Auftragnehmer oder Partner zugeschnitten sind.	Eine langsame Verbindungsgeschwindigkeit kann auftreten. Eine stärkere Verschlüsselung erfordert Zeit und Ressourcen, um Anonymität und Sicherheit zu gewährleisten. Die Verschlüsselung des Netzwerkverkehrs erfordert in der Regel etwas mehr Overhead. Sie können vielleicht ein paar VPN-

	Anbieter finden, die eine gute Verbindungsgeschwindigkeit bei gleichzeitiger Wahrung der Anonymität und Sicherheit bieten, aber es handelt sich in der Regel um bezahlte Services.
Steigerung der Produktivität durch Erweiterung des Unternehmensnetzwerks und der Unternehmensanwendungen	Potenzielles Sicherheitsrisiko durch Fehlkonfigurationen Das Entwerfen und Implementieren eines VPNs kann kompliziert sein. Ein erfahrener Experte muss das VPN so konfigurieren, dass eine Beeinträchtigung des Netzwerks vermieden wird.
Reduziert Kommunikationskosten und erhöht die Flexibilität.	Wenn eine Situation eintritt, in der eine neue Infrastruktur oder eine neue Gruppe von Konfigurationen hinzugefügt werden muss, können technische Probleme aufgrund der Inkompatibilität entstehen, insbesondere, wenn es sich um andere Produkte oder Anbieter als die handelt, die Sie bereits verwenden.
Der tatsächliche geografische Standort der Benutzer ist geschützt und nicht öffentlichen oder gemeinsam genutzten Netzwerken wie dem Internet ausgesetzt.	
Schützt vertrauliche Netzwerkdaten und -ressourcen.	
Mit einem VPN können neue Benutzer oder eine Benutzergruppe hinzugefügt werden, ohne dass zusätzliche Komponenten oder eine komplizierte Konfiguration erforderlich sind.	

Topologie

Dies ist eine einfache Topologie des Netzwerks.

Hinweis: Die öffentliche WAN-IP-Adresse wurde verwischt.



Unterstützte Geräte

- RV160
- RV260

Software-Version

- 1.0.0.xx (RV160 und RV260)
- 2.2.1 wird empfohlen, da 2.2.2 Verbindungsprobleme mit unseren Routern aufweisen kann ([Shrew Soft VPN Client Download](#)).

Inhalt

1. [Erstellen von Benutzergruppen](#)
2. [Erstellen von Benutzerkonten](#)
3. [Konfigurieren des IPsec-Profiles](#)
4. [Konfigurieren von Client-zu-Site](#)
5. [Konfigurieren des Shrew Soft VPN-Clients](#)
6. [Shrew Soft VPN-Client: Registerkarte Allgemein](#)
7. [Shrew Soft VPN-Client: Registerkarte "Client"](#)
8. [Shrew Soft VPN-Client: Registerkarte "Namensauflösung"](#)
9. [Shrew Soft VPN-Client: Registerkarte Authentifizierung](#)
10. [Shrew Soft VPN-Client: Registerkarte für Phase 1](#)
11. [Shrew Soft VPN-Client: Registerkarte "Phase 2"](#)

12. [Shrew Soft VPN-Client: Verbindung](#)
13. [Tipps zur Fehlerbehebung bei VPN-Verbindungen](#)
14. [Überprüfung](#)
15. [Fazit](#)

Erstellen von Benutzergruppen

Wichtiger Hinweis: Bitte lassen Sie das Standard-Admin-Konto in der Admin-Gruppe und erstellen Sie ein neues Benutzerkonto und eine neue Benutzergruppe für Shrew Soft. Wenn Sie Ihr Admin-Konto in eine andere Gruppe verschieben, können Sie sich nicht beim Router anmelden.

Schritt 1: Melden Sie sich bei der Webseite für die Konfiguration an.



Router

cisco

●●●●●●●●

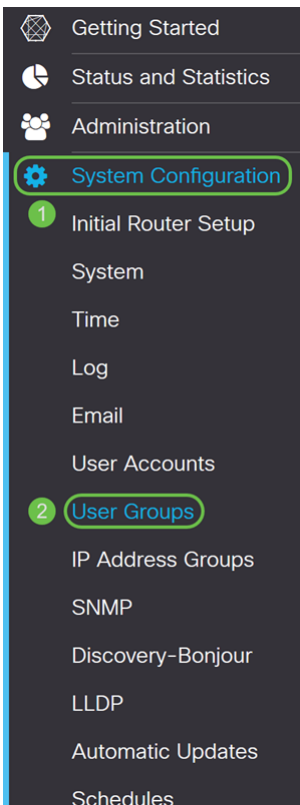
English ▼

Login

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Schritt 2: Navigieren Sie zu **Systemkonfiguration > Benutzergruppen**.



Schritt 3: Klicken Sie auf das **Plus**-Symbol, um eine neue Benutzergruppe hinzuzufügen.

User Groups Apply Cancel

<input type="checkbox"/>	Group	Web Login /NETCONF /RESTCONF	Lobby Ambassad...	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP	Captive Portal
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Enable	Disable	Disable	Disable

Schritt 4: Geben Sie im Feld *Gruppenname* einen Namen für die Gruppe ein.

Wir verwenden als Beispiel **ShrewSoftGroup**.

User Groups Apply Cancel

Group Name:

Local User Membership List ^

<input type="checkbox"/>	#	User
--------------------------	---	------

Schritt 5: Drücken Sie **Apply**, um eine neue Gruppe zu erstellen.

User Groups

Apply

Cancel

Group Name:

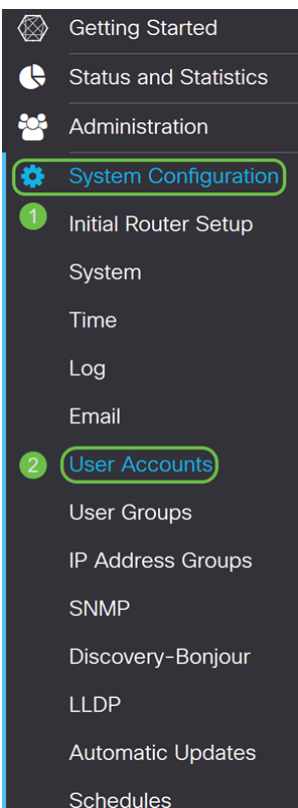
Local User Membership List



User

Erstellen von Benutzerkonten

Schritt 1: Navigieren Sie zu **Systemkonfiguration > Benutzerkonten**.



Schritt 2: Blättern Sie nach unten zur Tabelle *Lokale Benutzer*, und drücken Sie das **Plus**-Symbol, um einen neuen Benutzer hinzuzufügen.

Local Users




<input type="checkbox"/>	Username	Group
<input type="checkbox"/>	cisco	admin
<input type="checkbox"/>	guest	guest

* Should have at least one account in the 'admin' group.

Schritt 3: Die Seite *Benutzerkonten hinzufügen* wird geöffnet. Geben Sie einen Benutzernamen für den Benutzer ein.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter:

Group:


Apply

Cancel

Schritt 4: Geben Sie ein Kennwort in das Feld *Neues Kennwort ein*. Geben Sie im Feld *Kennwort bestätigen* dasselbe Kennwort erneut ein. In diesem Beispiel wird **CiscoTest123** als Kennwort verwendet.

Hinweis: Das hier verwendete Kennwort ist ein Beispiel. Es wird empfohlen, Ihr Kennwort zu vereinfachen.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

1


Confirm Password:

2

Password Strength meter:



Group:


 

Apply

Cancel

Schritt 5: Wählen Sie in der Dropdown-Liste *Gruppe* eine Gruppe aus, in der der Benutzer sein soll.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:


New Password:

Confirm Password:

Password Strength meter:



Group:


 

Apply

Cancel

Schritt 6: Drücken Sie **Apply**, um ein neues Benutzerkonto zu erstellen.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:


New Password:

Confirm Password:

Password Strength meter:



Group:

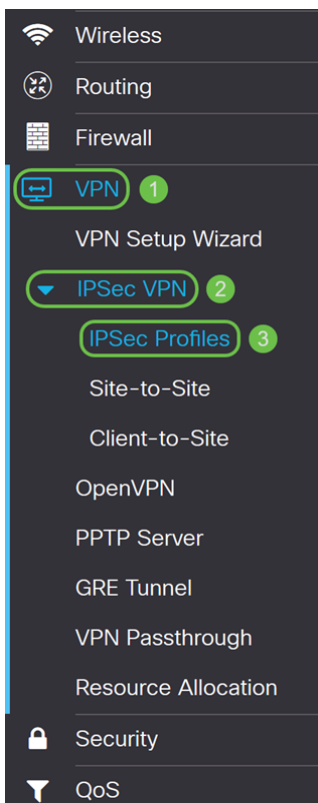
 

Apply

Cancel

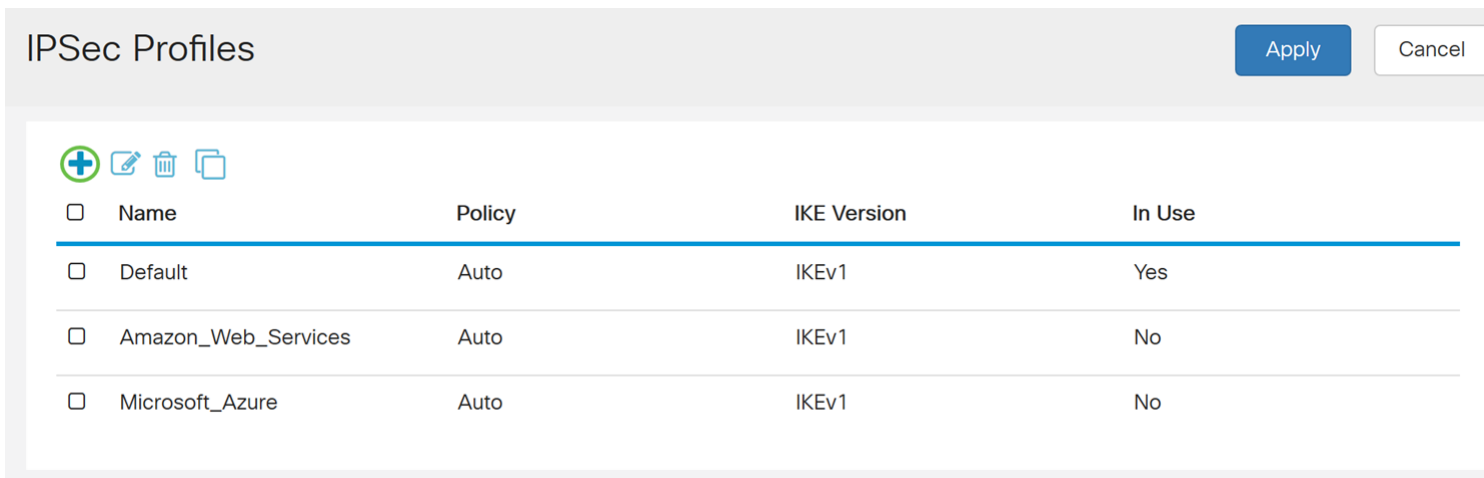
Konfigurieren des IPsec-Profiles

Schritt 1: Navigieren Sie zu **VPN > IPsec VPN > IPsec Profiles**.



Hinweis: Weitere Informationen zum Konfigurieren von IPsec-Profilen erhalten Sie, wenn Sie auf den Link klicken, um den Artikel anzuzeigen: [Konfigurieren von IPsec-Profilen \(Auto Keying Mode\) auf dem RV160 und RV260](#)

Schritt 2: Klicken Sie auf das **Plus**-Symbol, um ein neues IPsec-Profil hinzuzufügen.



Schritt 3: Geben Sie im Feld *Profilname* einen Namen für das Profil ein. Wir geben **ShrewSoftProfile** als unseren Profilnamen ein.

Add/Edit a New IPSec Profile

Apply

Cancel

Profile Name:

ShrewSoftProfile

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Schritt 4: Wählen Sie **Auto (Automatisch)** als *Keying Mode* aus.

Add/Edit a New IPSec Profile

Apply

Cancel

Profile Name:

ShrewSoftProfile

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Schritt 5: Wählen Sie entweder **IKEv1** oder **IKEv2** als *IKE-Version* aus. In diesem Beispiel wurde IKEv1 ausgewählt.

Add/Edit a New IPSec Profile

Apply

Cancel

Profile Name:

ShrewSoftProfile

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

sec. (Range: 120 - 86400. Default: 28800)

Schritt 6. Im Abschnitt "Optionen für Phase I" wurde dieser Artikel konfiguriert.

DH-Gruppe: **Gruppe 2 - 1024 Bit**

Verschlüsselung: **AES-256**

Authentifizierung: **SHA2-256**

SA-Lebensdauer: **28800**

Phase I Options

DH Group:

1 Group2 - 1024 bit

Encryption:

2 AES-256

Authentication:

3 SHA2-256

SA Lifetime:

4 28800

sec. (Range: 120 - 86400. Default: 28800)

Schritt 7. Unter den *Optionen für Phase II* haben wir diesen Artikel konfiguriert.

Protokollauswahl: **ESP**

Verschlüsselung: **AES-256**

Authentifizierung: **SHA2-256**

SA-Lebensdauer: **3600**

Perfekte Rufweiterleitung: **Aktiviert**

DH-Gruppe: **Gruppe 2 - 1024 Bit**

Phase II Options

Protocol Selection: 1 ESP

Encryption: 2 AES-256

Authentication: 3 SHA2-256

SA Lifetime: 4 3600 sec. (Range: 120 - 28800. Default: 3600)

Perfect Forward Secrecy: 5 Enable

DH Group: 6 Group2 - 1024 bit

Schritt 8: Klicken Sie auf **Apply**, um Ihr neues IPsec-Profil zu erstellen.

Add/Edit a New IPsec Profile

Apply

Cancel

Encryption: AES-256

Authentication: SHA2-256

SA Lifetime: 28800 sec. (Range: 120 - 86400. Default: 28800)

Phase II Options

Protocol Selection: ESP

Encryption: AES-256

Authentication: SHA2-256

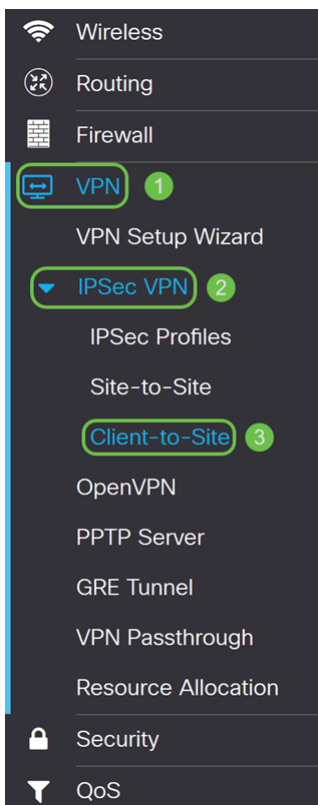
SA Lifetime: 3600 sec. (Range: 120 - 28800. Default: 3600)

Perfect Forward Secrecy: Enable

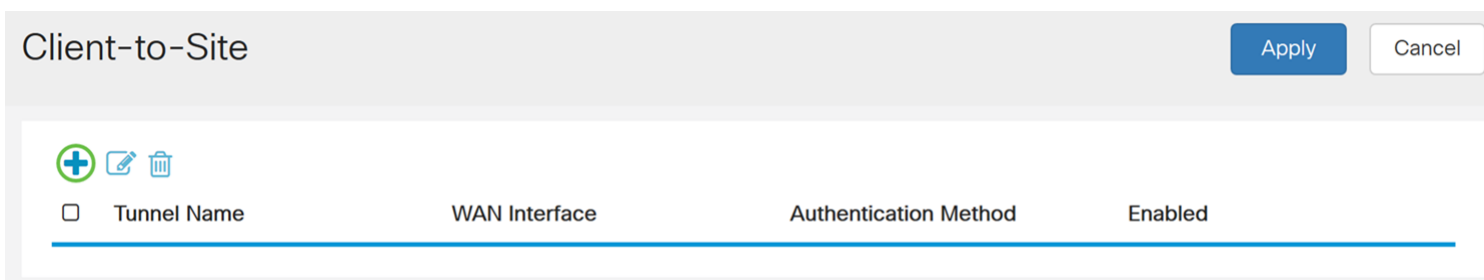
DH Group: Group2 - 1024 bit

Konfigurieren von Client-zu-Site

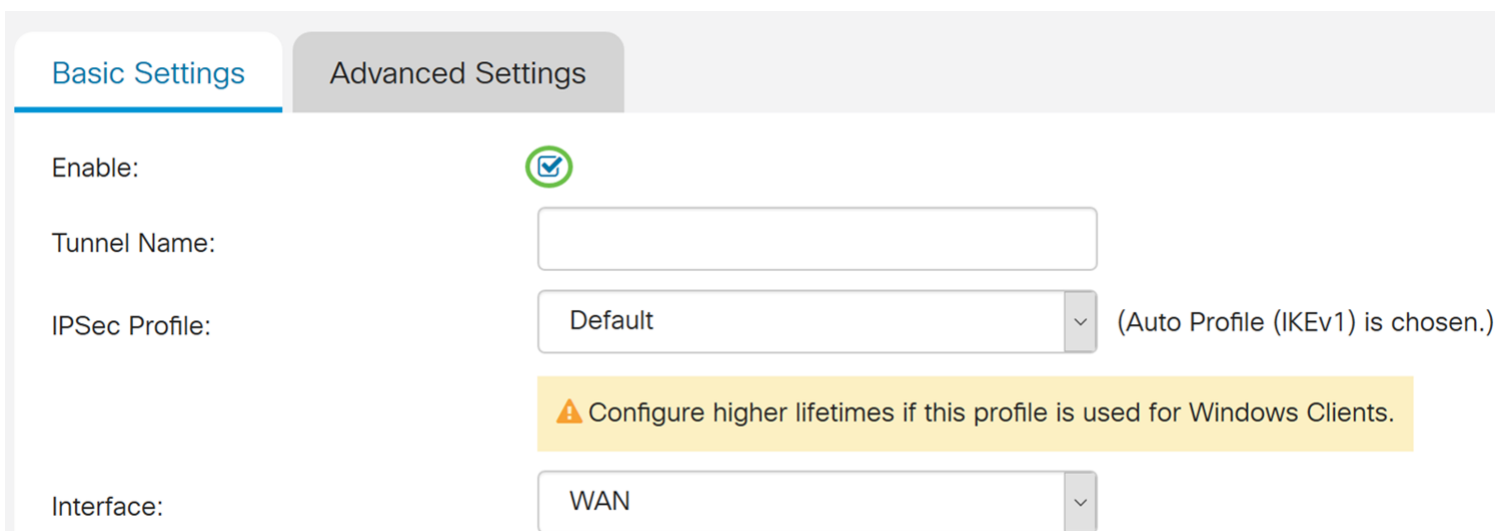
Schritt 1: Navigieren Sie zu **VPN > IPsec VPN > Client-to-Site**.



Schritt 2: Klicken Sie auf das **Plus**-Symbol, um einen neuen Tunnel hinzuzufügen.



Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Tunnel zu aktivieren.



Schritt 4: Geben Sie im Feld *Tunnel Name* einen Namen für den Tunnel ein.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

ShrewSoftTest

IPSec Profile:

Default

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Schritt 5: Wählen Sie in der Dropdown-Liste *IPSec Profile* (IPSec-Profil) ein Profil aus, das Sie verwenden möchten. Wählen Sie *ShrewSoftProfile* aus, das im vorherigen Abschnitt erstellt wurde: [Konfigurieren des IPSec-Profiles](#).

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

ShrewSoftTest

IPSec Profile:

ShrewSoftProfile

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Schritt 6: Wählen Sie aus der Dropdown-Liste *Interface (Schnittstelle)* die Schnittstelle aus, die Sie verwenden möchten. Wir verwenden **WAN** als Schnittstelle, um den Tunnel zu verbinden.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

ShrewSoftTest

IPSec Profile:

ShrewSoftProfile

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Schritt 7: Wählen Sie im Abschnitt *IKE-Authentifizierungsmethode* entweder *Pre-shared Key* oder *Certificate* aus. Wir verwenden **Pre-shared Key** als IKE-Authentifizierungsmethode.

Hinweis: IKE-Peers authentifizieren sich gegenseitig durch Computing und Senden eines

verschlüsselten Hashs von Daten, der den Pre-shared Key enthält. Wenn der empfangende Peer in der Lage ist, den gleichen Hash mit seinem Pre-shared Key unabhängig zu erstellen, weiß er, dass beide Peers denselben geheimen Schlüssel teilen und so den anderen Peer authentifizieren müssen. Vorinstallierte Schlüssel lassen sich nicht gut skalieren, da jeder IPsec-Peer mit den Pre-Shared Keys jedes anderen Peers konfiguriert werden muss, mit dem er eine Sitzung aufbaut.

Das Zertifikat verwendet ein digitales Zertifikat, das Informationen wie den Namen, die IP-Adresse, die Seriennummer, das Ablaufdatum des Zertifikats und eine Kopie des öffentlichen Schlüssels des Inhabers des Zertifikats enthält.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Schritt 8: Geben Sie den Pre-shared Key ein, den Sie für die Authentifizierung verwenden möchten. Pre-Shared Key kann sein, was immer Sie wollen. Der auf dem Shrew Soft VPN-Client konfigurierte Pre-Shared Key muss mit dem hier beim Konfigurieren identisch sein.

In diesem Beispiel verwenden wir **CiscoTest123!** als Pre-Shared Key.

Hinweis: Der hier eingegebene vorinstallierte Schlüssel ist ein Beispiel. Es wird empfohlen, einen komplexeren vorinstallierten Schlüssel einzugeben.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Schritt 9: Wählen Sie den *lokalen Bezeichner* aus der Dropdown-Liste aus. Die folgenden Optionen sind definiert als:

- Local WAN IP - Diese Option verwendet die IP-Adresse der WAN-Schnittstelle (Wide Area Network) des VPN-Gateways.
- IP-Adresse - Mit dieser Option können Sie eine IP-Adresse für die VPN-Verbindung

manuell eingeben. Sie müssen die WAN-IP-Adresse des Routers am Standort (Büro) eingeben.

- FQDN: Bei dieser Option wird beim Herstellen der VPN-Verbindung der FQDN (Fully Qualified Domain Name) des Routers verwendet.
- User FQDN - Mit dieser Option können Sie einen vollständigen Domännennamen für einen bestimmten Benutzer im Internet verwenden.

In diesem Beispiel wählen wir **Local WAN IP** als lokale ID aus.

Hinweis: Die lokale WAN-IP des Routers wird automatisch ausgefüllt.

Local Identifier:

1 Local WAN IP

2 24. [redacted]

Remote Identifier:

IP Address

[redacted]

Schritt 10: Wählen Sie in der Dropdown-Liste *Remote Identifier* entweder **IP Address**, **FQDN** oder **User FQDN** aus. Geben Sie dann die entsprechende Antwort von dem ein, was Sie ausgewählt haben. In diesem Beispiel wählen wir **FQDN** und geben **test.cisco.com** ein.

Local Identifier:

Local WAN IP

24. [redacted]

Remote Identifier:

1 FQDN



2 test.cisco.com

Schritt 11: Aktivieren Sie das Kontrollkästchen **Erweiterte Authentifizierung**, um die Funktion zu aktivieren. Dadurch wird eine zusätzliche Authentifizierungsstufe bereitgestellt, bei der Remote-Benutzer ihre Anmeldeinformationen eingeben müssen, bevor sie Zugriff auf das VPN erhalten.

Wenn Sie die *erweiterte Authentifizierung* aktiviert haben, klicken Sie auf das **Plus-Symbol**, um eine Benutzergruppe hinzuzufügen. Wählen Sie die Gruppe aus der Dropdown-Liste aus, die Sie für die erweiterte Authentifizierung verwenden möchten. Wir wählen **ShrewSoftGroup** als Gruppe aus.

Extended Authentication

1

2  

Group Name

3 ShrewSoftGroup

Schritt 12: Geben Sie im Feld *Pool Range for Client LAN* (Pool-Bereich für Client-LAN) den

IP-Adressbereich ein, der einem VPN-Client im Feld *Start IP (IP starten)* und *End IP (IP beenden)* zugewiesen werden kann. Dabei muss es sich um einen Adresspool handeln, der sich nicht mit den Standortadressen überschneidet.

Wir geben **10.2.1.1** als *Start-IP* und **10.2.1.254** als *End-IP* ein.

Pool Range for Client LAN:

Start IP:

1

10.2.1.1

End IP:

2

10.2.1.254

Schritt 13: (Optional) Klicken Sie auf die Registerkarte **Erweiterte Einstellungen**.

The screenshot shows the 'Advanced Settings' tab selected. Under 'Remote Endpoint', a dropdown menu is set to 'Dynamic IP'. Below this, the 'Local Group Setup' section contains a 'Local IP Type' dropdown set to 'Any'. The 'Mode Configuration' section includes three input fields: 'Primary DNS Server' with the value '10.2.0.96', 'Secondary DNS Server' which is empty, and 'Primary WINS Server' which is also empty.

Schritt 14: (Optional) Hier können Sie die IP-Adresse des Remote-Endpunkts angeben. In diesem Leitfaden wird **dynamische IP** verwendet, da die IP-Adresse für den Endclient nicht festgelegt ist.

Sie können auch angeben, welche internen Ressourcen im *Local Group Setup* verfügbar sind.

Wenn Sie **Any (Beliebig)** auswählen, stehen alle internen Ressourcen zur Verfügung.

Sie können auch Interne DNS- und WINS-Server verwenden. Dazu müssen Sie sie unter *Moduskonfiguration* angeben.

Sie können auch Voll- oder Split-Tunnel und Split-DNS verwenden.

Blättern Sie nach unten zu *Zusätzliche Einstellungen*. Aktivieren Sie das Kontrollkästchen

Aggressive Mode, um den aggressiven Modus zu aktivieren. Der aggressive Modus ist der Fall, wenn die Aushandlung für IKE SA in drei Pakete komprimiert wird, wobei alle SA-erforderlichen Daten vom Initiator übergeben werden müssen. Die Verhandlung ist schneller, aber sie haben eine Verwundbarkeit des Austauschs von Identitäten im Klartext.

Hinweis: Weitere Informationen zum Hauptmodus und aggressiven Modus finden Sie unter: [Hauptmodus vs. aggressiver Modus](#)

In diesem Beispiel aktivieren wir den **aggressiven Modus**.

Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Schritt 15: (Optional) Aktivieren Sie das Kontrollkästchen **Compress (Support IP Payload Compression Protocol (IPComp))**, damit der Router beim Start einer Verbindung Komprimierung vorschlagen kann. Dieses Protokoll reduziert die Größe von IP-Datagrammen. Wenn der Befrager dieses Angebot ablehnt, implementiert der Router keine Komprimierung. Wenn der Router der Responder ist, akzeptiert er Komprimierung, auch wenn die Komprimierung nicht aktiviert ist.

Wir lassen *Compress* ungeprüft.

Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Schritt 16: Klicken Sie auf **Apply**, um den neuen Tunnel hinzuzufügen.

Add/Edit a New Tunnel

Apply

Delete

Cancel

Secondary VPN Server:

Default Domain:

Split Tunnel: On Off



IP Address Netmask

Split DNS: On Off



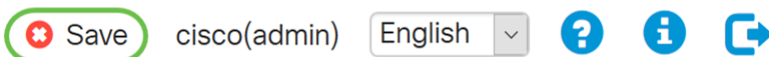
Domain Name

Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Schritt 17: Klicken Sie oben auf der Webseite auf das blinkende Symbol **Speichern**.



Schritt 18: Die Seite *Konfigurationsverwaltung* wird geöffnet. Stellen Sie im Abschnitt *"Konfiguration kopieren/speichern"* sicher, dass das Feld *Quelle* über **Konfiguration ausführen** und das Feld *Ziel* über **Startkonfiguration** verfügt. Drücken Sie dann **Apply**. Alle Konfigurationen, die der Router derzeit verwendet, befinden sich in der Running Configuration-Datei, die flüchtig ist und zwischen Neustarts nicht beibehalten wird. Beim Kopieren der Running Configuration-Datei in die Startkonfigurationsdatei wird die Konfiguration zwischen Neustarts beibehalten.

Configuration Management

Last Change Time

Running Configuration: 2019-Feb-14, 16:39:11 UTC

Startup configuration: --

Mirror Configuration: 2019-Feb-15, 13:00:11 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source: 1

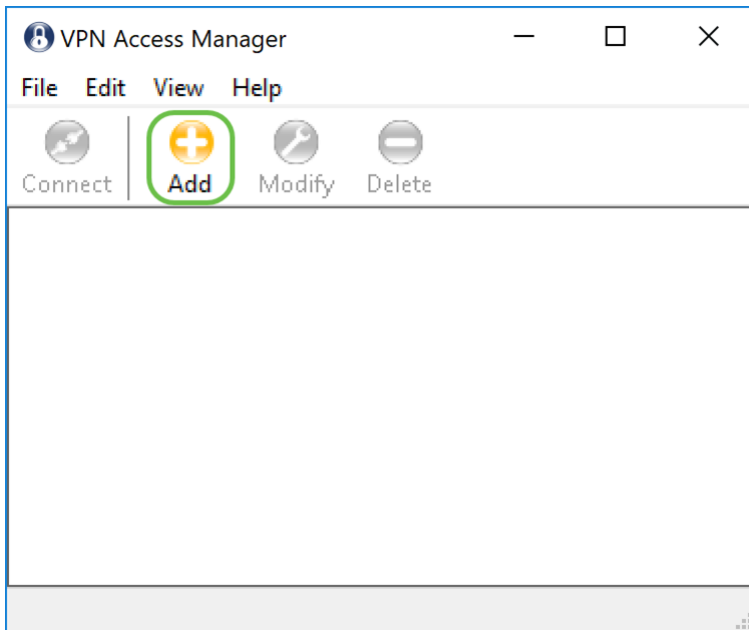
Destination: 2

Konfigurieren des Shrew Soft VPN-Clients

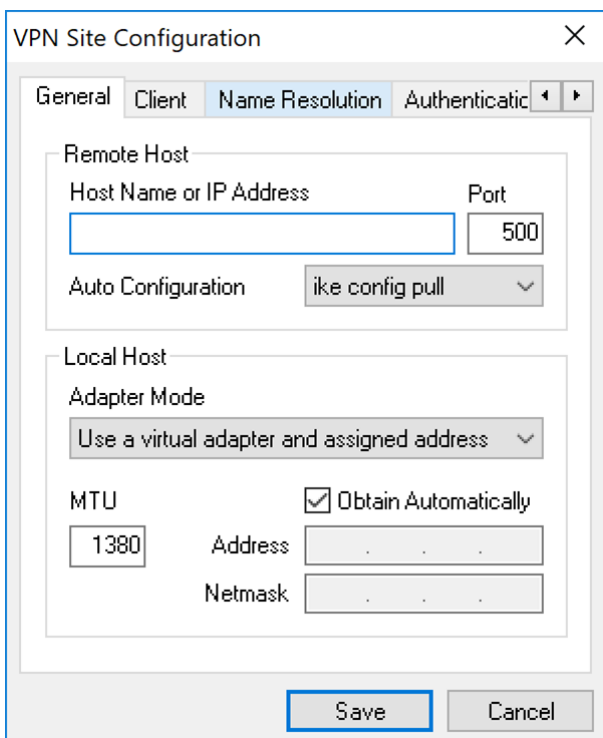
Wenn Sie den Shrew Soft VPN-Client noch nicht heruntergeladen haben, können Sie den Client über folgenden Link herunterladen: [Shrew Soft VPN Client für Windows](#). Wir verwenden die Standard Edition. Wenn Sie bereits einen Shrew Soft VPN-Client heruntergeladen haben, können Sie gerne mit dem ersten Schritt fortfahren.

Shrew Soft VPN-Client: Registerkarte Allgemein

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



Das Fenster *VPN Site Configuration* (Konfiguration des VPN-Standorts) wird angezeigt.



Schritt 2: Geben Sie im Abschnitt *Remote Host* unter der Registerkarte *Allgemein* den öffentlichen Hostnamen oder die öffentliche IP-Adresse des Netzwerks ein, mit dem Sie eine Verbindung herstellen möchten. In diesem Beispiel geben Sie die WAN-IP-Adresse des RV160/RV260 vor Ort ein, um die Verbindung herzustellen.

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

VPN Site Configuration

General Client Name Resolution Authenticatic

Remote Host

Host Name or IP Address Port

24.220. 500

Auto Configuration ike config pull

Local Host

Adapter Mode

Use a virtual adapter and assigned address

MTU Obtain Automatically

1380 Address . . .

Netmask . . .

Save Cancel

Schritt 3: Wählen Sie in der Dropdown-Liste *Automatische Konfiguration* eine Option aus. Die verfügbaren Optionen sind wie folgt definiert:

- **Deaktiviert** - Deaktiviert jede automatische Client-Konfiguration
- **Ike Config Pull** - Ermöglicht das Festlegen von Anforderungen von einem Computer durch den Client. Mit 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 über den Konfigurationsprozess Einstellungen anzubieten. Mit Unterstützung der Push-Methode durch den Computer gibt die Anforderung eine Liste der vom Client unterstützten Einstellungen zurück.
- **DHCP Over IPsec** - Bietet dem Client die Möglichkeit, Einstellungen über DHCP over IPsec vom Computer anzufordern.

In diesem Beispiel wählen wir **z. B. "config Pull"**.

VPN Site Configuration

General Client Name Resolution Authenticatic

Remote Host

Host Name or IP Address: 24.220. Port: 500

Auto Configuration: ike config pull

Local Host

Adapter Mode: Use a virtual adapter and assigned address

MTU: 1380 Obtain Automatically

Address: . . .

Netmask: . . .

Save Cancel

Schritt 4: Wählen Sie im Abschnitt *Lokaler Host* in der Dropdown-Liste **Adaptermodus und zugewiesene Adresse** verwenden die Option **Virtueller Adapter und zugewiesene Adresse** verwenden, und aktivieren Sie das **Kontrollkästchen Automatisch beziehen**. Die verfügbaren Optionen sind wie folgt definiert:

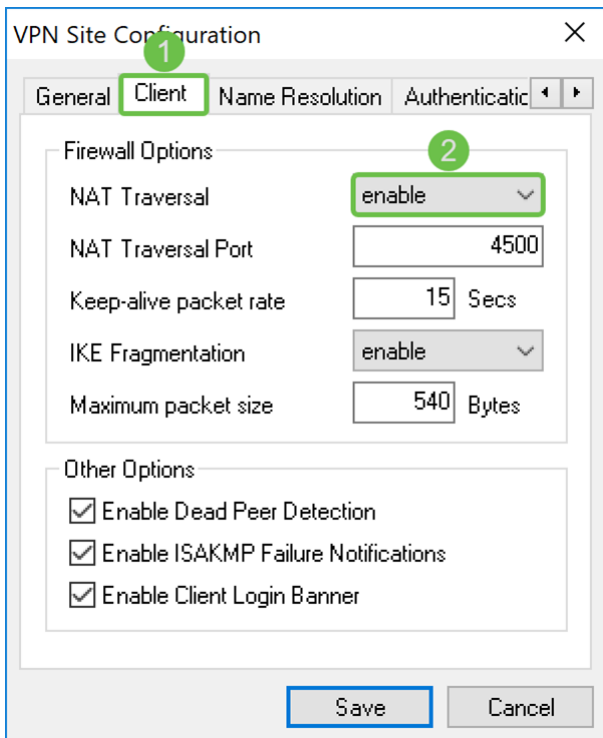
- **Virtueller Adapter und zugewiesene Adresse** - Ermöglicht dem Client, einen virtuellen Adapter mit einer angegebenen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.
- **Virtueller Adapter und zufällige Adresse** - Ermöglicht dem Client, einen virtuellen Adapter mit einer zufälligen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.
- **Vorhandenen Adapter und aktuelle Adresse verwenden** - Ermöglicht dem Client, nur seinen vorhandenen physischen Adapter mit seiner aktuellen Adresse als Quelle für seine IPsec-Kommunikation zu verwenden.

Shrew Soft VPN-Client: Registerkarte "Client"

Schritt 1: Klicken Sie auf die Registerkarte *Client*. Wählen Sie in der Dropdown-Liste *NAT Traversal* die gleiche Einstellung aus, die Sie für den RV160/RV260 für NAT Traversal konfiguriert haben. Die verfügbaren Menüoptionen für Network Address Traversal (NATT) sind wie folgt definiert:

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

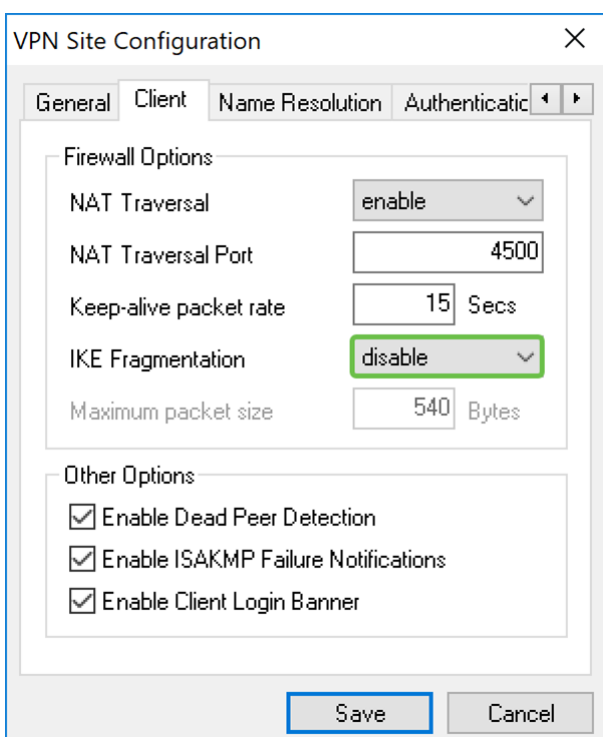
In diesem Dokument wird **enable** für NAT Traversal ausgewählt und *NAT Traversal Port* und *Keep-Alive Packet Rate* als Standardwert belassen.



Schritt 2: Wählen Sie in der Dropdownliste *IKE-Fragmentierung* entweder **Disable**, **Enable** oder **Force** aus. Die Optionen sind wie folgt definiert:

- **Disable (Deaktivieren)** - Die Erweiterung des IKE-Fragmentierungsprotokolls wird nicht verwendet.
- **Aktivieren** - Die Erweiterung des IKE-Fragmentierungsprotokolls wird nur verwendet, wenn das VPN-Gateway bei Verhandlungen die Unterstützung anzeigt.
- **Force** - Die Erweiterung des IKE-Fragmentierungsprotokolls wird unabhängig davon verwendet, ob das VPN-Gateway während der Verhandlungen Unterstützung anzeigt.

Wir haben die **Deaktivierung** für die *IKE-Fragmentierung* ausgewählt.



Schritt 3: Aktivieren Sie das Kontrollkästchen **Dead Peer Detection** aktivieren, um das

Protokoll Dead Peer Detection zu aktivieren. Wenn diese Option aktiviert ist, wird sie nur verwendet, wenn der Router sie unterstützt. Dadurch können der Client und der Router den Tunnelstatus überprüfen, um festzustellen, wann eine Seite nicht mehr reagieren kann. Diese Option ist standardmäßig aktiviert.

In diesem Beispiel wird die Dead Peer Detection überprüft.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Client' tab selected. Under 'Firewall Options', 'NAT Traversal' is set to 'enable', 'NAT Traversal Port' is 4500, 'Keep-alive packet rate' is 15 Secs, 'IKE Fragmentation' is 'disable', and 'Maximum packet size' is 540 Bytes. Under 'Other Options', three checkboxes are checked: 'Enable Dead Peer Detection', 'Enable ISAKMP Failure Notifications', and 'Enable Client Login Banner'. The 'Save' button is highlighted with a blue border.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable ISAKMP Failure Notification (ISAKMP-Fehlerbenachrichtigung aktivieren)**, um die ISAKMP-Fehlerbenachrichtigung vom VPN Client IPsec-Daemon zu aktivieren. Dies ist standardmäßig aktiviert.

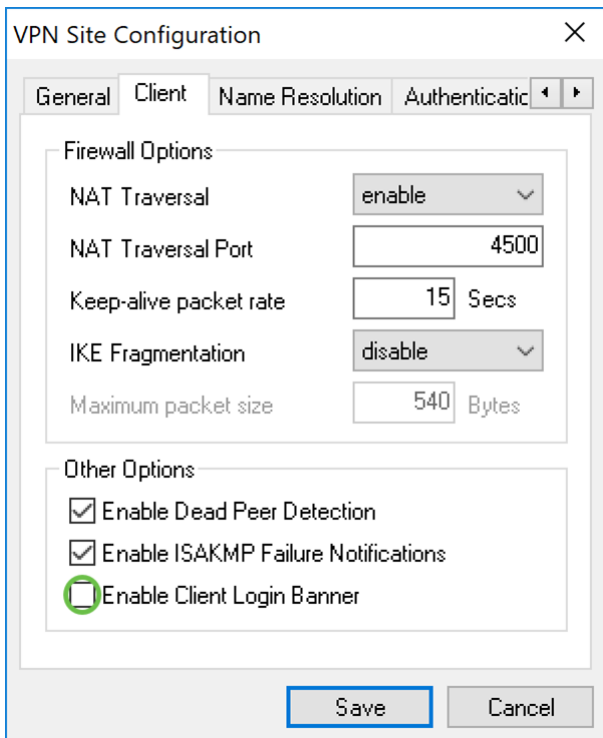
In diesem Beispiel wird die ISAKMP-Fehlerbenachrichtigung überprüft.

This screenshot is identical to the previous one, but the 'Enable Client Login Banner' checkbox is now unchecked, while 'Enable ISAKMP Failure Notifications' remains checked. The 'Save' button is still highlighted with a blue border.

Schritt 5: Deaktivieren Sie das **Banner Client-Anmeldung aktivieren**, um die Funktion zu deaktivieren. Es wird ein Anmeldebanner angezeigt, nachdem der Tunnel mit dem Router

erstellt wurde. Der Router muss die Transaction Exchange unterstützen und für die Weiterleitung eines Anmeldebanners an den Client konfiguriert sein. Dieser Wert ist standardmäßig aktiviert.

Wir deaktivieren das Client Login Banner.



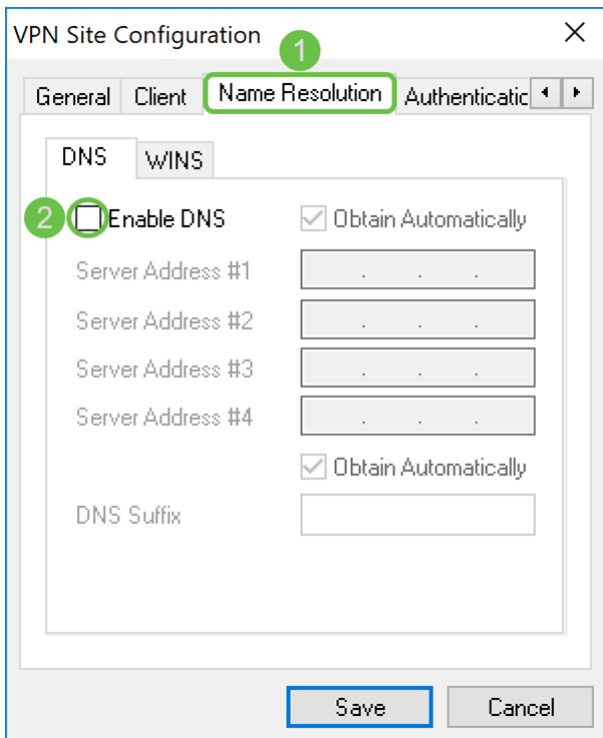
The image shows a screenshot of the 'VPN Site Configuration' dialog box, specifically the 'Client' tab. The dialog has a title bar with a close button (X) and a tabbed interface with 'General', 'Client', 'Name Resolution', and 'Authenticatic' tabs. The 'Client' tab is active. It contains two sections: 'Firewall Options' and 'Other Options'. In the 'Firewall Options' section, there are five settings: 'NAT Traversal' (enable), 'NAT Traversal Port' (4500), 'Keep-alive packet rate' (15 Secs), 'IKE Fragmentation' (disable), and 'Maximum packet size' (540 Bytes). In the 'Other Options' section, there are three checkboxes: 'Enable Dead Peer Detection' (checked), 'Enable ISAKMP Failure Notifications' (checked), and 'Enable Client Login Banner' (unchecked). At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

Shrew Soft VPN-Client: Registerkarte "Namensauflösung"

Schritt 1: 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**.

Wenn *DNS aktivieren* aktiviert ist und Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway automatisch DNS-Einstellungen bereitstellen. Falls nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige DNS-Server-Adresse ein.

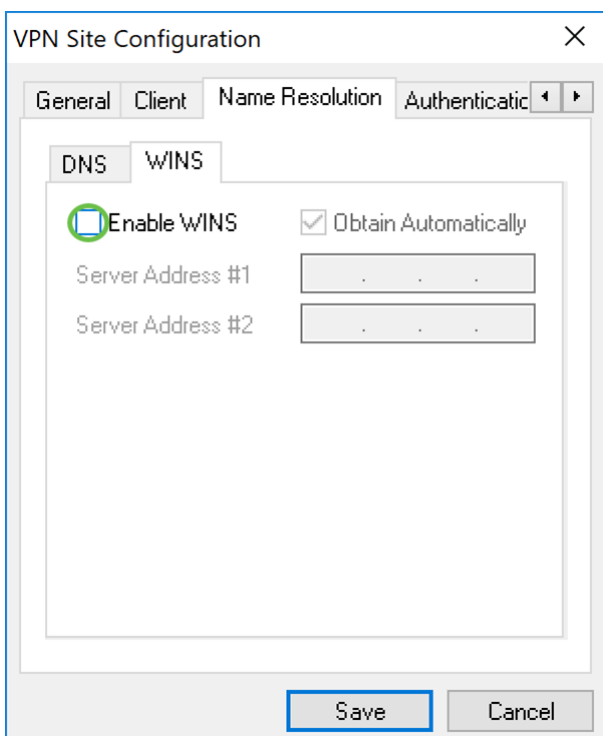
In diesem Beispiel ist **Enable DNS** deaktiviert.



Schritt 2: Aktivieren Sie das Kontrollkästchen **WINS aktivieren**, wenn Sie Windows Internet Name Server (WINS) aktivieren möchten. Wenn Ihr Remote-Gateway für die Unterstützung von Configuration Exchange konfiguriert ist, kann das Gateway automatisch WINS-Einstellungen bereitstellen. Falls nicht, stellen Sie sicher, dass das Kontrollkästchen **Automatisch beziehen** deaktiviert ist, und geben Sie manuell eine gültige WINS-Serveradresse ein.

Hinweis: Durch Bereitstellen von WINS-Konfigurationsinformationen kann ein Client WINS-Namen mithilfe eines Servers auflösen, der sich im privaten Remote-Netzwerk befindet. Dies ist nützlich, wenn versucht wird, mithilfe eines einheitlichen Namenskonventionen-Pfadnamens auf die Netzwerkressourcen von Remote-Fenstern zuzugreifen. Der WINS-Server gehört in der Regel zu einem Windows Domain Controller oder einem Samba-Server.

In diesem Beispiel ist **Enable WINS** deaktiviert.



Shrew Soft VPN-Client: Registerkarte Authentifizierung

Schritt 1: Klicken Sie auf die Registerkarte *Authentifizierung*, und wählen Sie **Mutual PSK + XAuth** in der Dropdown-Liste *Authentication Method* 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 vergeben.
- **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 gemeinsam genutzten geheimen Zeichenfolge bereitgestellt.
- **Mutual RSA + XAuth** - Sowohl der Client als auch das Gateway benötigen Anmeldeinformationen für die Authentifizierung. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen vergeben.
- **Gegenseitiges PSK + XAuth** - Sowohl der Client als auch das Gateway benötigen Anmeldeinformationen für die Authentifizierung. Die Anmeldeinformationen werden in Form einer freigegebenen geheimen Zeichenfolge bereitgestellt.
- **Mutual RSA** - Sowohl der Client als auch das Gateway benötigen Anmeldeinformationen für die Authentifizierung. Die Anmeldeinformationen werden in Form von PEM- oder PKCS12-Zertifikatsdateien oder Schlüsseltypen vergeben.
- **Gegenseitiges PSK** - Sowohl der Client als auch das Gateway benötigen Anmeldeinformationen für die Authentifizierung. Die Anmeldeinformationen werden in Form einer freigegebenen geheimen Zeichenfolge bereitgestellt.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected (marked with a green circle 1). The 'Authentication Method' dropdown is set to 'Mutual PSK + XAuth' (marked with a green circle 2). Below this, the 'Local Identity' sub-tab is active, showing 'Identification Type' set to 'Fully Qualified Domain Name' and an empty 'FQDN String' text box. At the bottom, the 'Save' button is highlighted with a blue border.

Schritt 2: Wählen Sie auf der Registerkarte *Lokale Identität* den Identifizierungstyp aus, und geben Sie dann die entsprechende Zeichenfolge in das leere Feld ein. Die folgenden

Optionen sind definiert als:

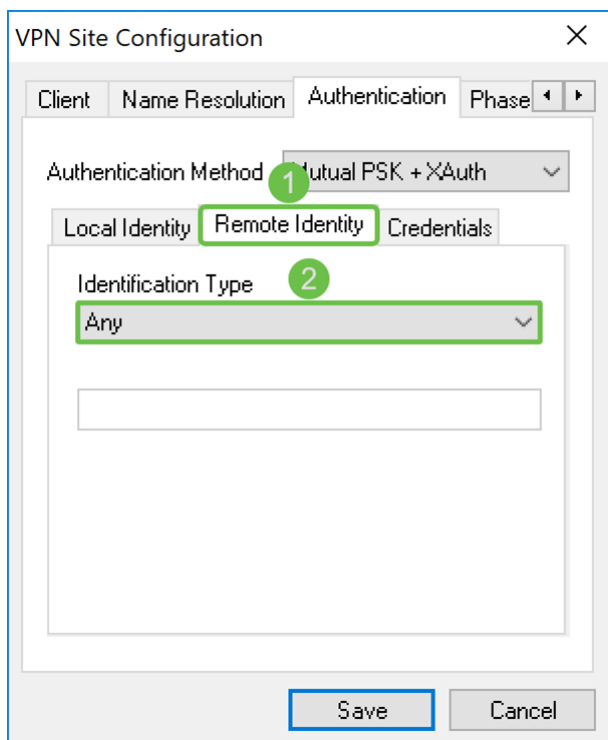
- **Any (Beliebig):** Dies wird nur auf der Registerkarte "Remote-Identität" akzeptiert. Der Client akzeptiert alle ID-Typen und -Werte. Diese Vorgehensweise sollte mit Vorsicht verwendet werden, da sie einen Teil des IKE-Phase-1-Identifizierungsprozesses umgeht.
- **Vollqualifizierter Domänenname:** Bei dieser Option müssen Sie eine FQDN-Zeichenfolge in Form einer DNS-Domänenzeichenfolge bereitstellen. Beispielsweise wäre "cisco.com" ein akzeptabler Wert. Der Client lässt diese Option nur zu, wenn ein PSK-Authentifizierungsmodus verwendet wird.
- **vollqualifizierter Domänenname:** Sie müssen eine Benutzer-FQDN-Zeichenfolge in Form einer user@domain-Zeichenfolge bereitstellen. Beispiel: "dave@cisco.com" wäre ein akzeptabler Wert. Der Client lässt diese Option nur zu, wenn ein PSK-Authentifizierungsmodus verwendet wird.
- **IP-Adresse** - Wenn die IP-Adresse ausgewählt ist, *wird das* Kontrollkästchen *Entdeckte lokale Hostadresse* verwenden standardmäßig aktiviert. Dies bedeutet, dass der Wert automatisch bestimmt wird. Deaktivieren Sie das Kontrollkästchen, wenn Sie eine andere Adresse als die Adapteradresse für die Kommunikation mit dem Client-Gateway verwenden möchten. Geben Sie dann eine bestimmte Adresszeichenfolge ein. Der Client lässt diese Option nur zu, wenn ein PSK-Authentifizierungsmodus verwendet wird.
- **Key Identifier:** Wenn diese Option aktiviert ist, müssen Sie eine Identifikationszeichenfolge angeben.

In diesem Beispiel wählen wir **Vollqualifizierter Domänenname** und geben **test.cisco.com** in das Feld *FQDN-Zeichenfolge* ein.

The screenshot shows the 'VPN Site Configuration' dialog box with the 'Authentication' tab selected. Under 'Authentication Method', 'Mutual PSK + XAuth' is chosen. The 'Remote Identity' sub-tab is active, showing 'Identification Type' set to 'Fully Qualified Domain Name' (marked with a green circle '1') and 'FQDN String' set to 'test.cisco.com' (marked with a green circle '2'). 'Save' and 'Cancel' buttons are at the bottom.

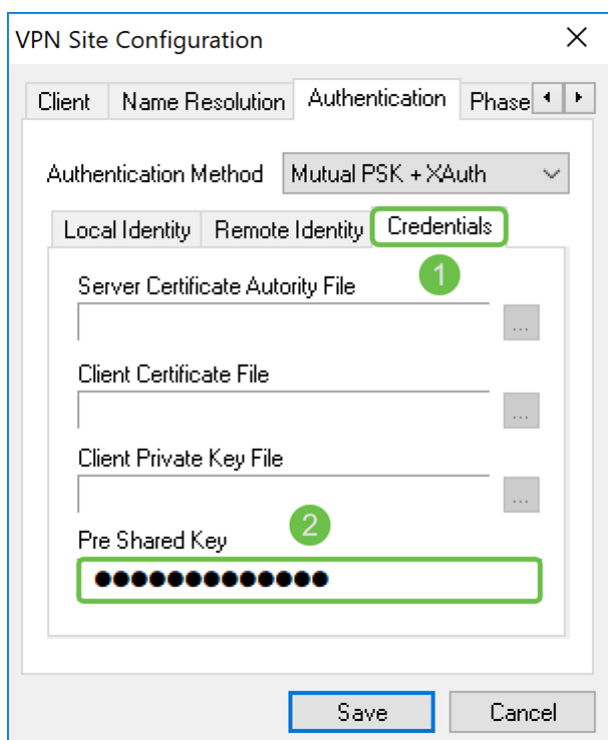
Schritt 3: Klicken Sie auf die Registerkarte *Remote Identity (Remote-Identität)*, und wählen Sie den Identifizierungstyp aus. Folgende Optionen sind verfügbar: Alle vollständig qualifizierten Domännennamen, vollständig qualifizierten Domännennamen von Benutzern, IP-Adressen oder Key-Identifier.

In diesem Dokument wird **Any** als Identifizierungstyp verwendet.



Schritt 4: Klicken Sie auf die Registerkarte "Anmeldeinformationen", und geben Sie den gleichen vorinstallierten Schlüssel ein, den Sie für den RV160/RV260 konfiguriert haben.

Wir geben **CiscoTest123 ein!** im Feld *Vorinstallierter Schlüssel*.



Shrew Soft VPN-Client: Registerkarte für Phase 1

Schritt 1: Klicken Sie auf die Registerkarte *Phase 1*. Konfigurieren Sie die folgenden Parameter so, dass sie dieselben Einstellungen haben, die Sie für den RV160/RV260 konfiguriert haben.

Die Parameter in Shrew Soft müssen mit der in [Phase 1](#) ausgewählten RV160/RV260-

Konfiguration übereinstimmen. In diesem Dokument werden die Parameter in Shrew Soft wie folgt festgelegt:

- Exchange-Typ: **aggressiv**

- DH Exchange: **Gruppe 2**

- Cipher-Algorithmus: **AES**

Schlüssellänge des •: **256**

- Hash-Algorithmus: **sha2-256**

- Lebenszeitlimit: **28800**

- Limit wichtiger Lebensdaten: **0**

VPN Site Configuration

Name Resolution Authentication **Phase 1** Pha: ◀ ▶

Proposal Parameters

Exchange Type 2 aggressive

DH Exchange 3 group 2

Cipher Algorithm 4 aes

Cipher Key Length 5 256 Bits

Hash Algorithm 6 sha2-256

Key Life Time limit 7 28800 Secs

Key Life Data limit 8 0 Kbytes

Enable Check Point Compatible Vendor ID

Save Cancel

Schritt 2: (Optional) 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 Vendor-ID aktivieren)**. Wenn das Gate keine mit Cisco kompatible Anbieter-ID anbietet oder Sie sich nicht sicher sind, lassen Sie das Kontrollkästchen deaktiviert. Wir lassen das Kontrollkästchen deaktiviert.

VPN Site Configuration

Name Resolution Authentication Phase 1 Pha: ◀ ▶

Proposal Parameters

Exchange Type aggressive

DH Exchange group 2

Cipher Algorithm aes

Cipher Key Length 256 Bits

Hash Algorithm sha2-256

Key Life Time limit 28800 Secs

Key Life Data limit 0 Kbytes

Enable Check Point Compatible Vendor ID

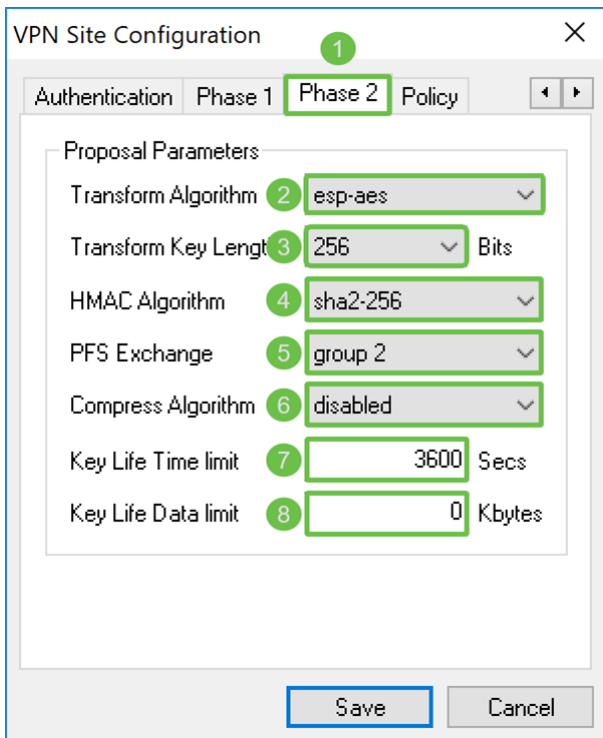
Save Cancel

Shrew Soft VPN-Client: Registerkarte "Phase 2"

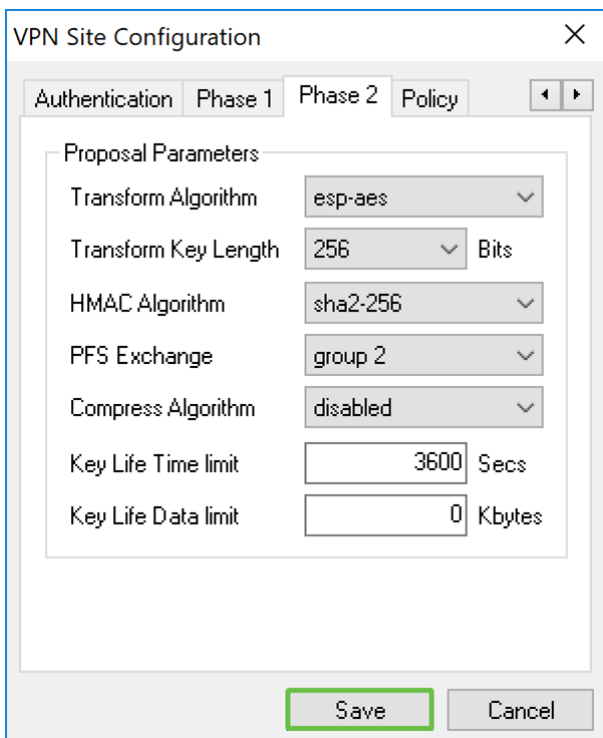
Schritt 1: Klicken Sie auf die Registerkarte *Phase 2*. Konfigurieren Sie die folgenden Parameter so, dass sie dieselben Einstellungen haben, die Sie für den RV160/RV260 konfiguriert haben.

Die Parameter sollten mit der RV160/260-Konfiguration in [Phase 2](#) wie folgt übereinstimmen:

- Umwandlungsalgorithmus: **ESP-aes**
- Schlüssellänge umwandeln: **256**
- HMAC-Algorithmus: **sha2-256**
- PFS Exchange: **Gruppe 2**
- Komprimierungsalgorithmus: **deaktiviert**
- Lebenszeitlimit: **3600**
- Limit wichtiger Lebensdaten: **0**



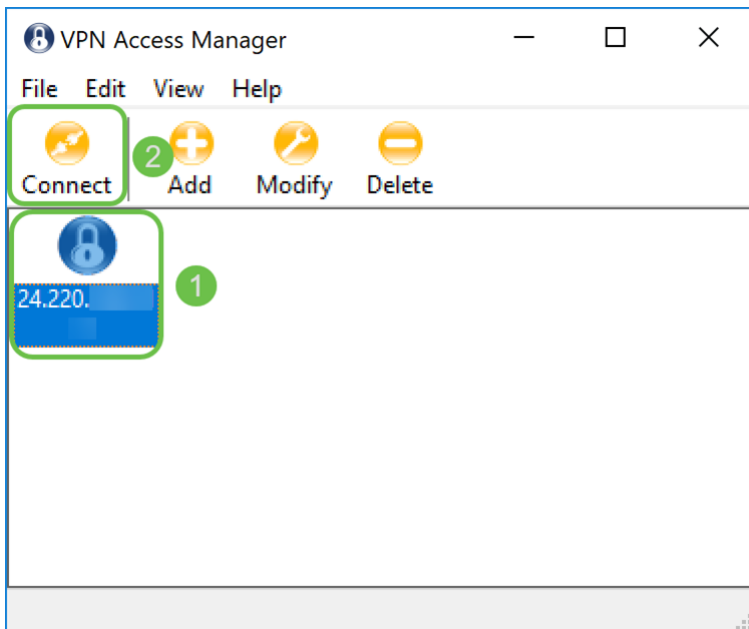
Schritt 2: Drücken Sie die **Save** (Speichern)-Taste am unteren Seitenrand, um die Konfiguration zu speichern.



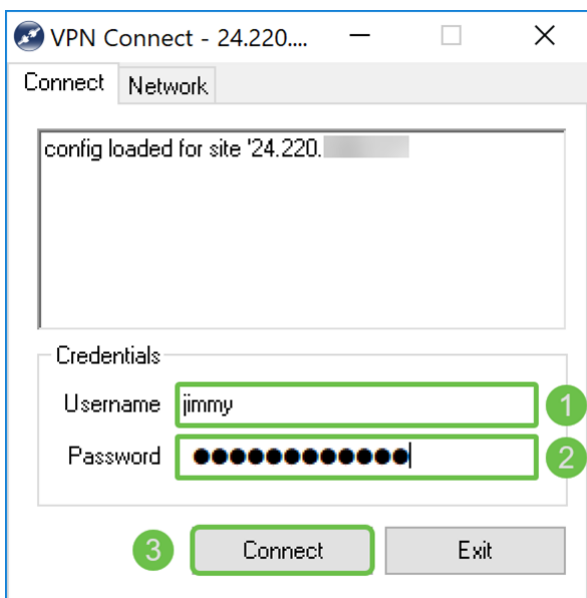
Shrew Soft VPN-Client: Verbindung

Schritt 1: Wählen Sie im *VPN Access Manager* das soeben erstellte VPN-Profil aus. Drücken Sie anschließend **Verbinden**.

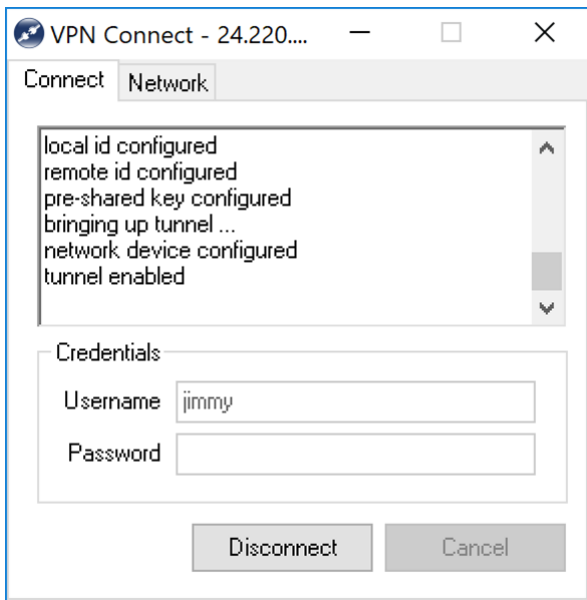
Hinweis: Wenn Sie das VPN-Profil umbenennen möchten, klicken Sie mit der rechten Maustaste darauf, und wählen Sie **Umbenennen** aus. Ein Teil der IP-Adresse im Profil ist verschwommen, um das Netzwerk zu schützen.



Schritt 2: Ein Fenster *VPN Connect* wird angezeigt. Geben Sie den Benutzernamen und das Kennwort ein, die im Abschnitt [Erstellen eines Benutzerkontos](#) erstellt wurden. Drücken Sie anschließend **Verbinden**.

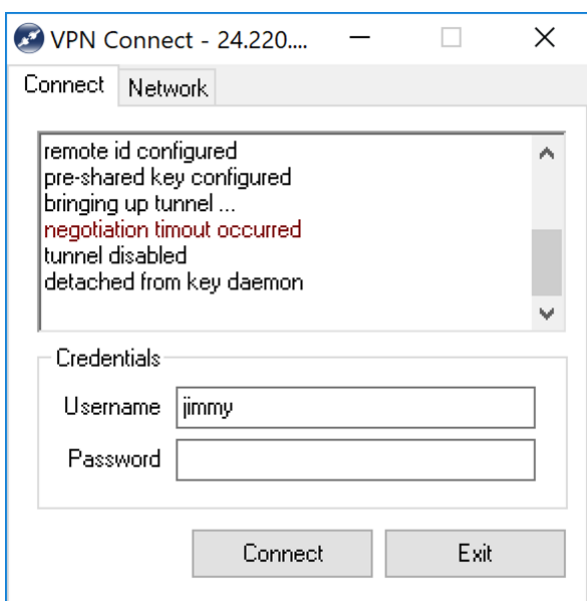


Schritt 3: Nach dem Drücken von *Connect* (Verbinden) werden die Konfigurationsinformationen zusammen mit einer Anforderung zur Kommunikation an den IKE-Daemon weitergeleitet. Im Ausgabefenster werden verschiedene Meldungen des Verbindungsstatus angezeigt. Wenn die Verbindung erfolgreich hergestellt wird, erhalten Sie die Meldung "Netzwerkgerät konfiguriert" und "Tunnel aktiviert". Die *Verbindungstaste* wechselt zu einer *Verbindungstaste*.

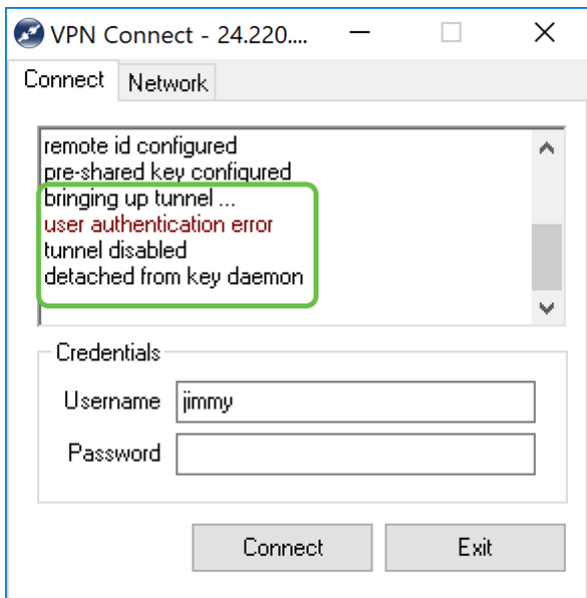


Tipps zur Fehlerbehebung bei VPN-Verbindungen

Wenn Sie Fehlermeldungen erhalten, die Folgendes enthalten: "Aushandlung-Timeout aufgetreten", "Tunnel deaktiviert" und "vom Schlüsseldaeomon getrennt". Sie können Ihre Konfiguration auf Ihrem Router und dem Shrew Soft VPN-Client überprüfen, um sicherzustellen, dass sie übereinstimmen.

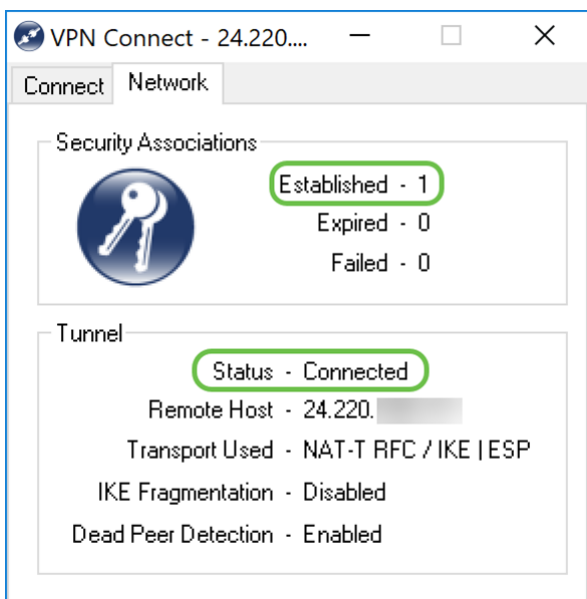


Wenn Sie eine Fehlermeldung erhalten, die besagt: "user authentication error" (Benutzerauthentifizierungsfehler), bedeutet dies, dass Sie das falsche Kennwort für diesen Benutzernamen eingegeben haben. Überprüfen Sie die Benutzeranmeldeinformationen, und stellen Sie sicher, dass sie korrekt konfiguriert und eingegeben wurden.



Überprüfung

Schritt 1: Klicken Sie im Fenster *VPN-Verbindung* auf die Registerkarte *Netzwerk*. Auf dieser Registerkarte sollten Sie die aktuellen Netzwerkstatistiken für die Verbindung anzeigen können. Im Abschnitt *Tunnel* sollte *Connected* als Status angezeigt werden.



Schritt 2: Navigieren Sie auf Ihrem Router zu **Status und Statistik > VPN Status**. Scrollen Sie auf der Seite *VPN-Status* nach unten zum Abschnitt *Client-to-Site-VPN-Status*. In diesem Abschnitt können Sie alle Verbindungen zwischen Client und Standort anzeigen. Klicken Sie auf das Symbol für **die** Augen, um weitere Details anzuzeigen.

Schritt 3: Navigieren Sie zu Ihrer Suchleiste in der Taskleiste, und suchen Sie nach Eingabeaufforderung.

Hinweis: Die folgenden Anweisungen werden unter einem Windows 10-Betriebssystem verwendet. Dies kann je nach Betriebssystem variieren, das Sie verwenden.

Schritt 4: Geben Sie den Befehl ohne die Anführungszeichen ein: "**ping [private IP-Adresse des Routers]**", aber geben Sie die private IP-Adresse anstelle der Wörter ein. Sie sollten in der Lage sein, die private IP-Adresse des Routers erfolgreich zu pinggen.

In diesem Beispiel geben wir **ping 10.2.0.96** ein. 10.2.0.96 ist die private IP-Adresse unseres Routers.

```
Command Prompt
Microsoft Windows [Version 10.0.17134.523]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\ >ping 10.2.0.96

Pinging 10.2.0.96 with 32 bytes of data:
Reply from 10.2.0.96: bytes=32 time=91ms TTL=64
Reply from 10.2.0.96: bytes=32 time=95ms TTL=64
Reply from 10.2.0.96: bytes=32 time=84ms TTL=64
Reply from 10.2.0.96: bytes=32 time=84ms TTL=64

Ping statistics for 10.2.0.96:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 95ms, Average = 88ms

C:\Users\ >
```

Fazit

Sie sollten Ihren Shrew Soft VPN-Client jetzt erfolgreich mit RV160 oder RV260 verbunden haben.