Konfigurieren von AnyConnect Virtual Private Network (VPN)-Konnektivität auf dem Router der RV34x-Serie

Ziel

Dieses Dokument soll Ihnen zeigen, wie AnyConnect-VPN-Verbindungen auf dem Router der RV34x-Serie konfiguriert werden.

Vorteile bei der Verwendung des AnyConnect Secure Mobility Client:

1. Sichere und kontinuierliche Netzwerkverbindungen
2. Durchgängige Sicherheit und Richtliniendurchsetzung
3. Bereitstellbar über die Adaptive Security Appliance (ASA) oder über Systeme für die Bereitstellung von Unternehmenssoftware
4. Anpassbar und übersetzbar
5. Einfach zu konfigurieren
6. Unterstützt sowohl Internet Protocol Security (IPSec) als auch Secure Sockets Layer (SSL)
7. Unterstützt das Internet Key Exchange-Protokoll der Version 2.0 (IKEv2.0)

Einleitung

Über eine Virtual Private Network (VPN)-Verbindung können Benutzer auf ein privates Netzwerk zugreifen und darüber Daten senden und empfangen. Die Verbindung erfolgt über ein öffentliches oder gemeinsam genutztes Netzwerk wie das Internet, ist aber dennoch eine sichere Verbindung zu einer zugrunde liegenden Netzwerkinfrastruktur. So werden das private Netzwerk und die zugehörigen Ressourcen geschützt.

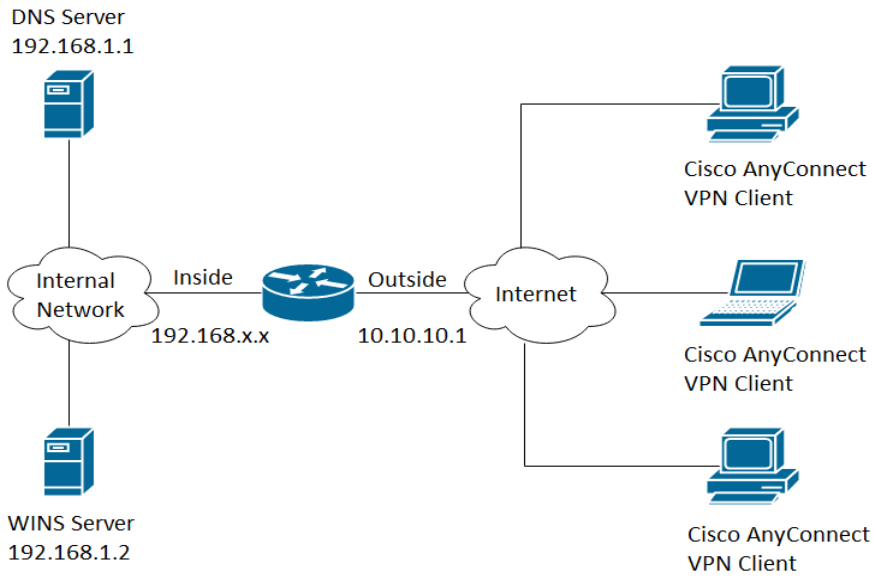
Ein VPN-Client ist eine Software, die auf einem Computer installiert und ausgeführt wird, der sich mit dem Remote-Netzwerk verbinden möchte. Diese Client-Software muss mit derselben Konfiguration wie der VPN-Server eingerichtet werden, z. B. die IP-Adresse und die Authentifizierungsinformationen. Diese Authentifizierungsinformationen umfassen den Benutzernamen und den vorab freigegebenen Schlüssel, die zum Verschlüsseln der Daten verwendet werden. Abhängig vom physischen Standort der zu verbindenden Netzwerke kann ein VPN-Client auch ein Hardware-Gerät sein. Dies geschieht normalerweise, wenn über die VPN-Verbindung zwei Netzwerke miteinander verbunden werden, die sich an unterschiedlichen Standorten befinden.

Der Cisco AnyConnect Secure Mobility Client ist eine Softwareanwendung für die Verbindung mit einem VPN, die mit verschiedenen Betriebssystemen und Hardwarekonfigurationen ausgeführt werden kann. Mit dieser Softwareanwendung kann so auf Remoteressourcen eines anderen Netzwerks zugegriffen werden, als wäre der Benutzer direkt mit seinem Netzwerk verbunden – auf sichere Weise. Der Cisco AnyConnect Secure Mobility Client nutzt innovative neue Ansätze, um durchgängige Sicherheit für den mobilen Netzwerkzugriff mit Computern oder Smartphones für Endbenutzer zu gewährleisten und IT-Administratoren die Durchsetzung umfassender IT-Richtlinien zu ermöglichen.

Auf dem RV34x-Router ist ab Firmware-Version 1.0.3.15 keine AnyConnect-Lizenzierung

erforderlich. Nur für Client-Lizenzen wird eine Gebühr erhoben.

Weitere Informationen zur AnyConnect-Lizenzierung für die Router der RV340-Serie finden Sie im folgenden Artikel: AnyConnect-Lizenzierung für die Router der RV340-Serie.



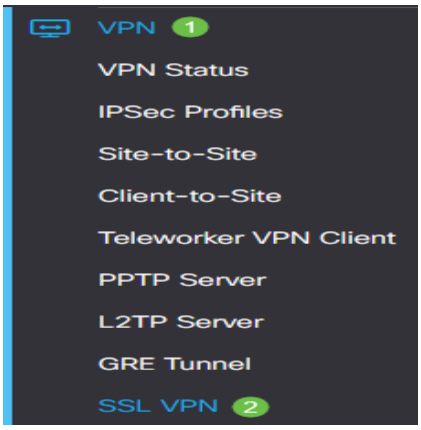
Unterstützte Geräte | Firmware-Version

- Cisco AnyConnect Secure Mobility Client | 4.4 (Aktuelle Version herunterladen)
- RV34x-Serie | 1.0.03.15 (Aktuelle Version herunterladen)

AnyConnect-VPN-Verbindungen auf dem RV34x konfigurieren

SSL VPN auf dem RV34x konfigurieren

Schritt 1: Greifen Sie auf das webbasierte Dienstprogramm des Routers zu und wählen Sie **VPN > SSL VPN** aus.



Schritt 2: Klicken Sie auf das Optionsfeld **On** (Ein), um Cisco SSL VPN-Server zu aktivieren.

Obligatorische Gateway-Einstellungen

Die folgenden Konfigurationseinstellungen sind obligatorisch:

Schritt 3: Wählen Sie aus der Dropdown-Liste die Gateway-Schnittstelle aus. Dies ist der Port, der für die Weiterleitung von Datenverkehr durch die SSL-VPN-Tunnel verwendet wird. Folgende Optionen sind verfügbar:

- WAN1
- WAN2
- USB1
- USB2

Hinweis: In diesem Beispiel wird WAN1 ausgewählt.

Schritt 4: Geben Sie die Portnummer, die für das SSL-VPN-Gateway verwendet wird, in das Feld *Gateway Port* ein. Sie sollte zwischen 1 und 65535 liegen.

Hinweis: In diesem Beispiel wird 8443 als Portnummer verwendet.

Schritt 5: Wählen Sie aus der Dropdown-Liste die Zertifikatsdatei aus. Dieses Zertifikat authentifiziert Benutzer, die versuchen, über die SSL-VPN-Tunnel auf die Netzwerkressource zuzugreifen. Die Dropdown-Liste enthält ein Standardzertifikat und die importierten Zertifikate.

Hinweis: In diesem Beispiel ist Default (Standard) ausgewählt.

Schritt 6: Geben Sie in das Feld *Client Address Pool* (Client-Adressen-Pool) die IP-Adresse des Client-Adressen-Pools ein. Dieser Pool ist der Bereich der IP-Adressen, der Remote-VPN-Clients zugewiesen wird.

Hinweis: Stellen Sie sicher, dass sich der IP-Adressbereich nicht mit einer der IP-Adressen im lokalen Netzwerk überschneidet.

Hinweis: In diesem Beispiel wird „192.168.0.0“ verwendet.

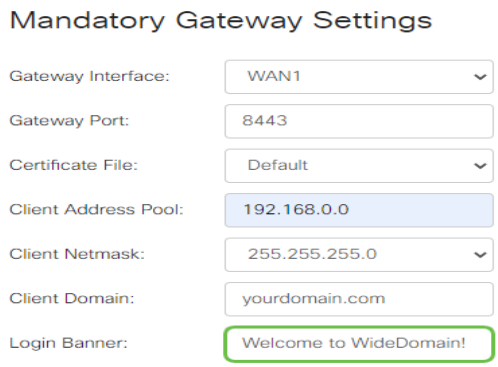
Schritt 7. Wählen Sie aus der Dropdown-Liste die Client-Netzmaske aus.

Hinweis: In diesem Beispiel wird 255.255.255.128 ausgewählt.

Schritt 8: Geben Sie in das Feld *Client Domain* (Client-Domäne) den Client-Domänennamen ein. Dies ist der Domänenname, der an SSL-VPN-Clients übertragen werden soll.

Hinweis: In diesem Beispiel wird WideDomain.com als Client-Domänenname verwendet.

Schritt 9. Geben Sie in das Feld *Login Banner* (Anmeldebanner) den Text ein, der als Anmeldebanner angezeigt werden soll. Dieses Banner wird bei jeder Anmeldung eines Clients angezeigt.

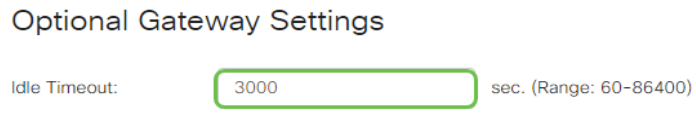


Hinweis: In diesem Beispiel wird Welcome to Widedomain! als Anmeldebanner verwendet.

Optionale Gateway-Einstellungen

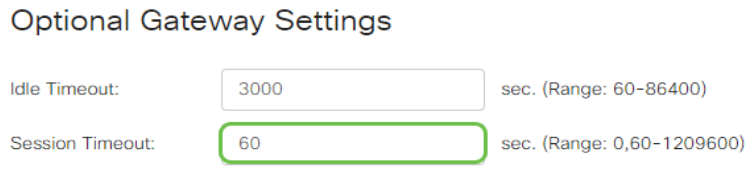
Die folgenden Konfigurationseinstellungen sind optional:

Schritt 1: Geben Sie einen Wert für die Leerlaufzeitüberschreitung in Sekunden zwischen 60 und 86400 ein. Dies ist die Zeitdauer, die die SSL-VPN-Sitzung inaktiv bleiben kann.



Hinweis: In diesem Beispiel wird 3000 verwendet.

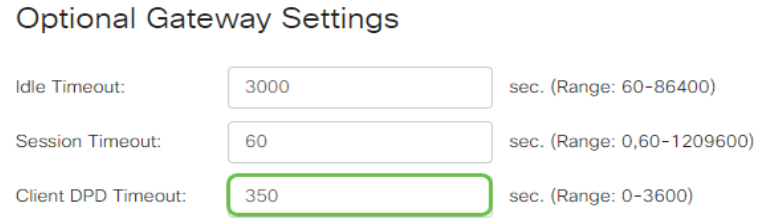
Schritt 2: Geben Sie in das Feld *Session Timeout* (Sitzungs-Timeout) einen Wert in Sekunden ein. Dies ist die Zeit, die es dauert, bis die Sitzung des Transmission Control Protocol (TCP) oder User Datagram Protocol (UDP) nach der angegebenen Leerlaufzeit abläuft. Möglich sind Werte im Bereich von 60 bis 1209600 Sekunden.



Hinweis: In diesem Beispiel wird 60 verwendet.

Schritt 3: Geben Sie in das Feld *ClientDPD Timeout* (ClientDPD-Zeitüberschreitung) einen Wert in Sekunden zwischen 0 und 3600 ein. Dieser Wert gibt das regelmäßige Senden von HELLO/ACK-Nachrichten zur Prüfung des Status des VPN-Tunnels an.

Hinweis: Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert sein.

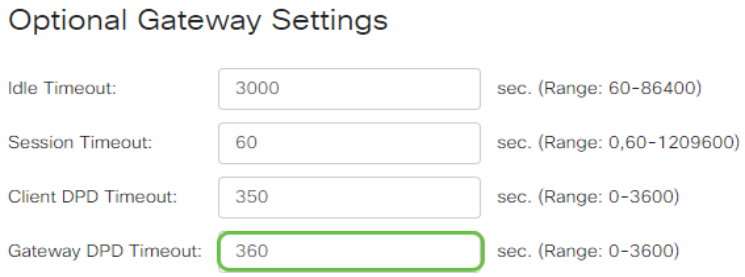


Hinweis: In diesem Beispiel wird 350 verwendet.

Schritt 4: Geben Sie in das Feld *GatewayDPD Timeout* (GatewayDPD-Zeitüberschreitung) einen Wert in Sekunden zwischen 0 und 3600 ein. Dieser Wert gibt das regelmäßige Senden von

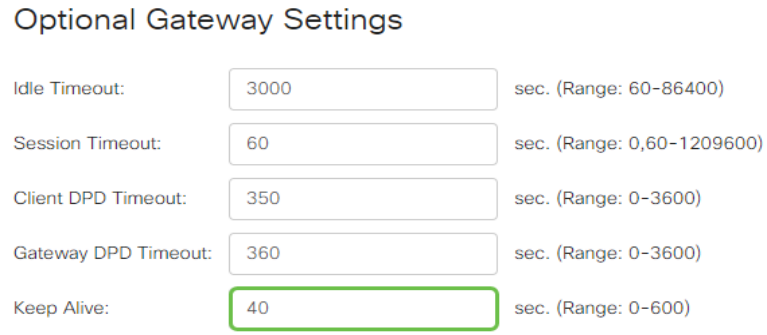
HELLO/ACK-Nachrichten zur Prüfung des Status des VPN-Tunnels an.

Hinweis: Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert sein.



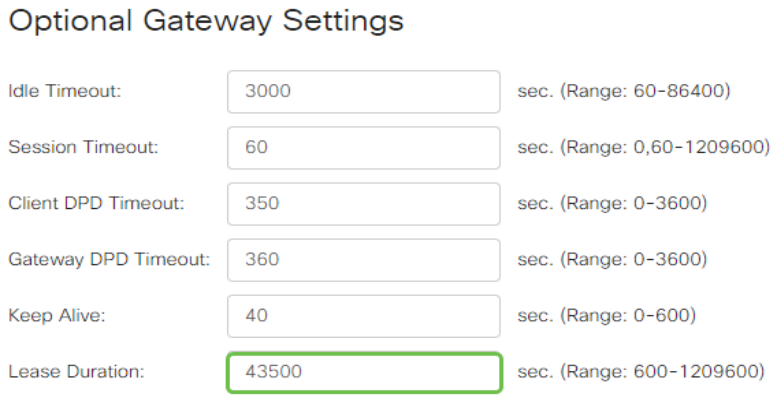
Hinweis: In diesem Beispiel wird 360 verwendet.

Schritt 5: Geben Sie in das Feld *Keep Alive* einen Wert in Sekunden zwischen 0 und 600 ein. Mit dieser Funktion wird sichergestellt, dass der Router immer mit dem Internet verbunden ist. Sie versucht, eine getrennte VPN-Verbindung wiederherzustellen.



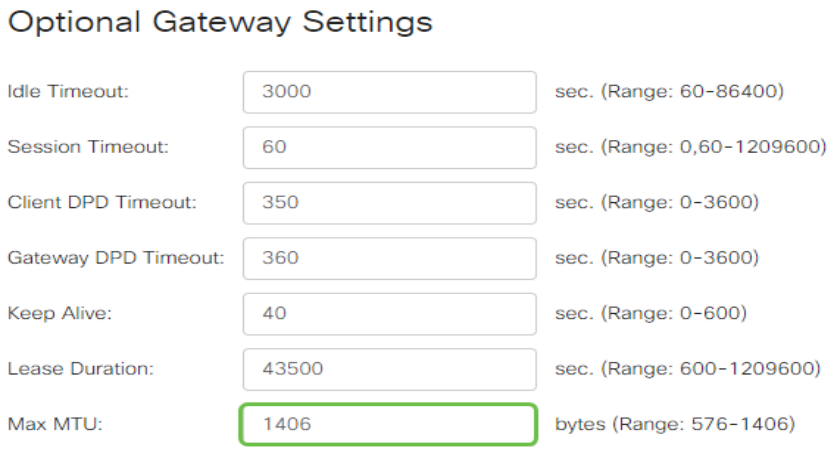
Hinweis: In diesem Beispiel wird 40 verwendet.

Schritt 6: Geben Sie in das Feld *Lease-Duration* (Lease-Dauer) einen Wert in Sekunden für die Dauer des zu verbindenden Tunnels ein. Möglich sind Werte im Bereich von 600 bis 1209600 Sekunden.



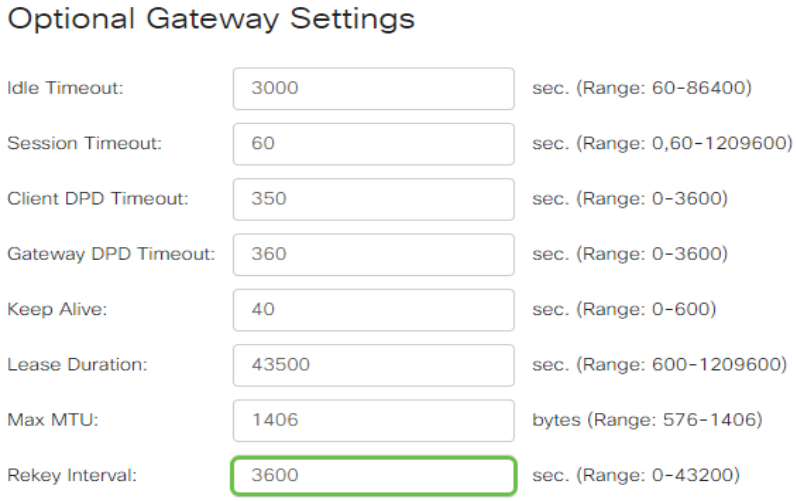
Hinweis: In diesem Beispiel wird 43500 verwendet.

Schritt 7. Geben Sie die Paketgröße in Byte ein, das über das Netzwerk gesendet werden kann. Möglich sind Werte im Bereich von 576 bis 1406.



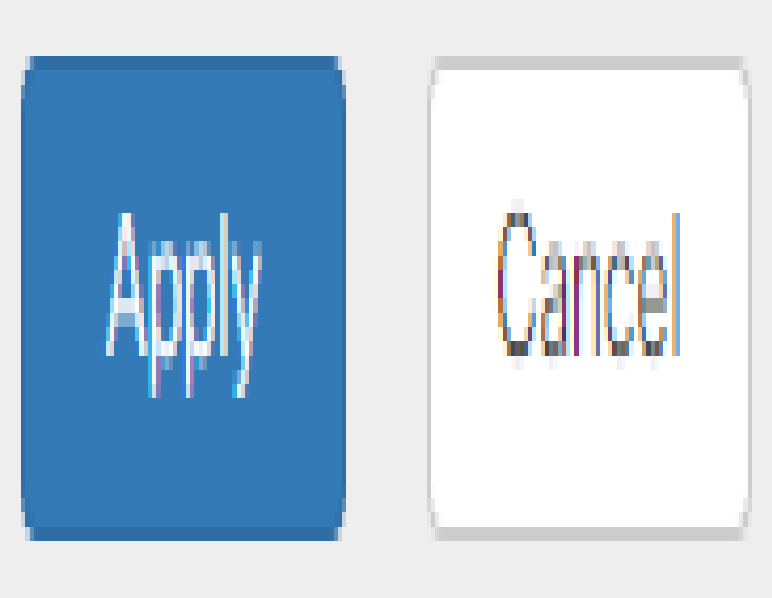
Hinweis: In diesem Beispiel wird 1406 verwendet.

Schritt 8: Geben Sie in das Feld *Rekey Interval* (Intervall für Schlüsselneueingabe) die Zeit für das Relay-Intervall ein. Die Funktion zur Schlüsselneueingabe ermöglicht es den SSL-Schlüsseln Neuverhandlungen nach der Einrichtung der Sitzung durchzuführen. Möglich sind Werte im Bereich von 0 bis 43200.



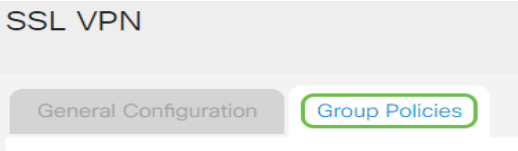
Hinweis: In diesem Beispiel wird 3600 verwendet.

Schritt 9. Klicken Sie auf **Apply** (Anwenden).

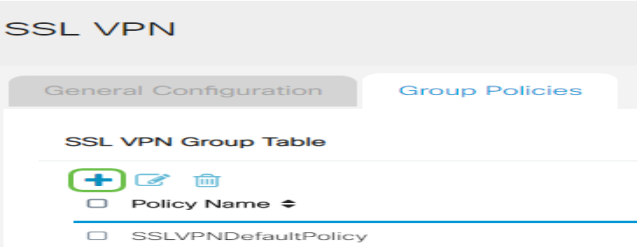


Gruppenrichtlinien konfigurieren

Schritt 1: Klicken Sie auf die Registerkarte **Group Policies** (Gruppenrichtlinien).



Schritt 2: Klicken Sie unter der Tabelle "SSL VPN Group" (SSL-VPN-Gruppe) auf die Schaltfläche **Add** (Hinzufügen), um eine Gruppenrichtlinie hinzuzufügen.

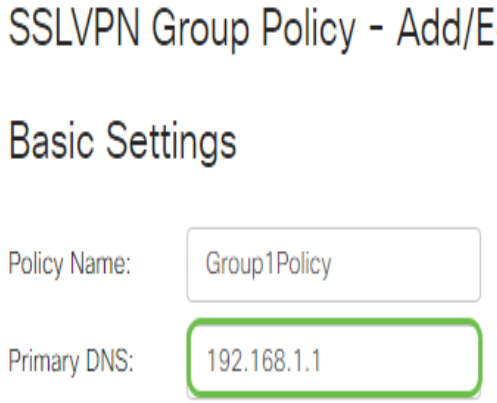


Hinweis: Die Tabelle mit den SSL VPN-Gruppen zeigt die Liste der Gruppenrichtlinien auf dem Gerät an. Sie können auch die erste Gruppenrichtlinie in der Liste mit dem Namen SSLVPNDefaultPolicy bearbeiten. Dies ist die vom Gerät bereitgestellte Standardrichtlinie.

Schritt 3: Geben Sie in das Feld *Policy Name* (Richtlinienname) Ihren bevorzugten Richtliniennamen ein.

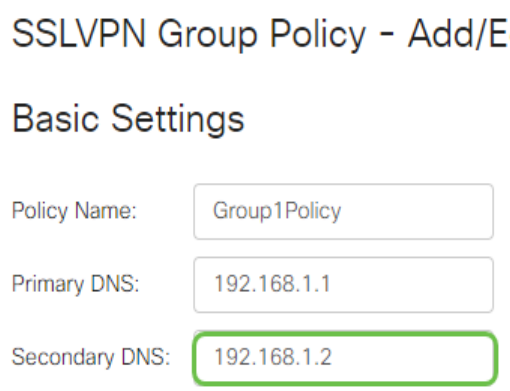
Hinweis: In diesem Beispiel wird die Group 1-Richtlinie verwendet.

Schritt 4: Geben Sie die IP-Adresse des primären DNS-Servers in das entsprechende Feld ein. Standardmäßig ist diese IP-Adresse bereits angegeben.



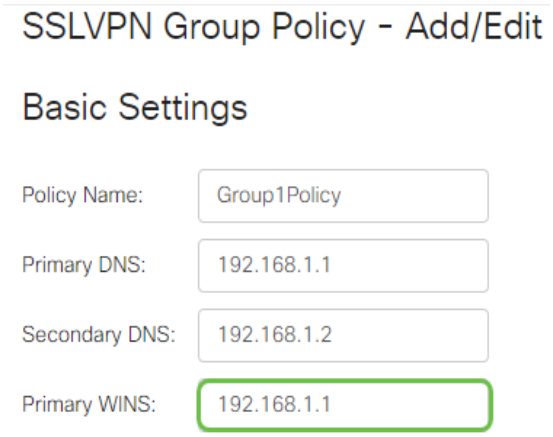
Hinweis: In diesem Beispiel wird „192.168.1.1“ verwendet.

Schritt 5: Geben Sie optional die IP-Adresse des sekundären DNS in das dafür vorgesehene Feld ein. Dies dient als Backup, sollte der primäre DNS-Server ausfallen.



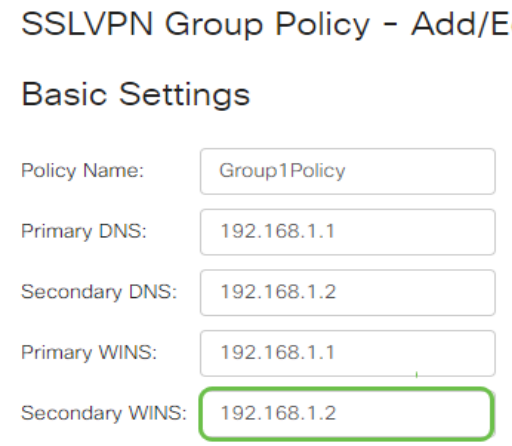
Hinweis: In diesem Beispiel wird „192.168.1.2“ verwendet.

Schritt 6: Geben Sie optional die IP-Adresse des primären WINS-Servers in das entsprechende Feld ein.



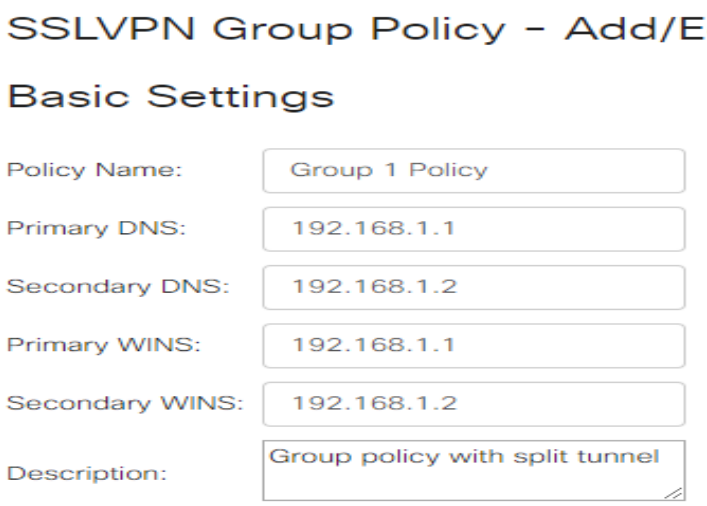
Hinweis: In diesem Beispiel wird „192.168.1.1“ verwendet.

Schritt 7: Geben Sie optional die IP-Adresse des sekundären WINS-Servers in das entsprechende Feld ein.



Hinweis: In diesem Beispiel wird „192.168.1.2“ verwendet.

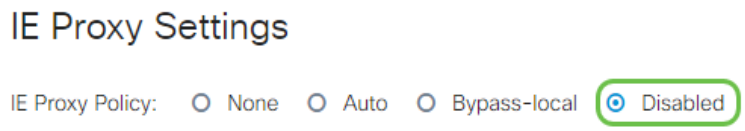
Schritt 8. (Optional) Geben Sie eine Beschreibung der Richtlinie in das Feld *Beschreibung ein*.



Hinweis: In diesem Beispiel wird eine Gruppenrichtlinie mit Split-Tunnel verwendet.

Schritt 9. (Optional) Klicken Sie auf ein Optionsfeld, um die IE-Proxy-Richtlinie auszuwählen und die Microsoft Internet Explorer (MSIE)-Proxy-Einstellungen für die Einrichtung eines VPN-Tunnels zu aktivieren. Folgende Optionen sind verfügbar:

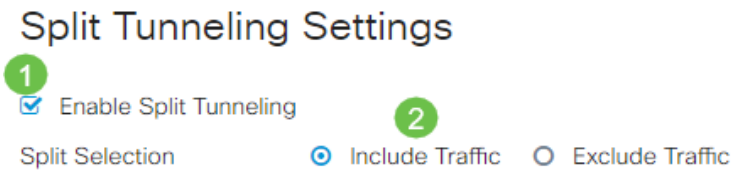
- None – Ermöglicht dem Browser, keine Proxy-Einstellungen zu verwenden.
- Auto – Ermöglicht dem Browser, die Proxy-Einstellungen automatisch zu erkennen.
- Bypass-local – Ermöglicht dem Browser, die für den Remote-Benutzer konfigurierten Proxy-Einstellungen zu umgehen.
- Disabled – Deaktiviert die MSIE-Proxy-Einstellungen.



Hinweis: In diesem Beispiel wird Disabled (Deaktiviert) ausgewählt. Dies ist die Standardeinstellung.

Schritt 10. (Optional) Aktivieren Sie im Bereich Split Tunneling Settings (Split Tunneling-Einstellungen) das Kontrollkästchen **Enable Split Tunneling,** um zu ermöglichen, dass Internet-Datenverkehr unverschlüsselt direkt an das Internet gesendet wird. Mit Full Tunneling wird der gesamte Verkehr an das Endgerät gesendet und von dort an die Zielressourcen weitergeleitet. Dabei muss das Unternehmensnetzwerk nicht im Pfad für den Webzugriff enthalten sein.

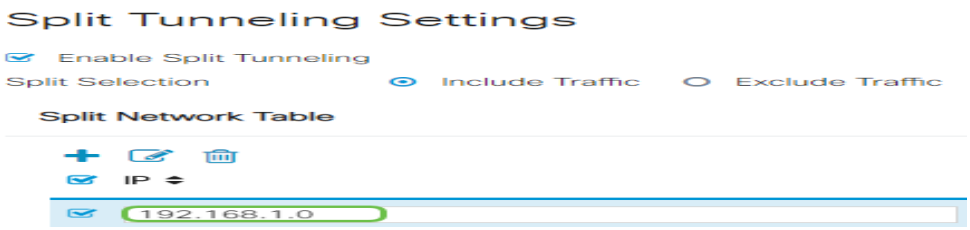
Schritt 11. (Optional) Klicken Sie auf ein Optionsfeld, um zu wählen, ob Datenverkehr beim Anwenden des Split-Tunneling ein- oder ausgeschlossen werden soll.



Hinweis: In diesem Beispiel wird "Datenverkehr einschließen" ausgewählt.

Schritt 12: Klicken Sie in der Tabelle "Split Network" (Netzwerk aufteilen) auf die Schaltfläche **Add** (Hinzufügen), um eine Ausnahme für aufgeteilte Netzwerke hinzuzufügen.

Schritt 13: Geben Sie die IP-Adresse in das entsprechende Feld ein.



Hinweis: In diesem Beispiel wird „192.168.1.0“ verwendet.

Schritt 14: Klicken Sie in der Tabelle "Split DNS" (DNS aufteilen) auf die Schaltfläche **Add** (Hinzufügen), um eine Ausnahme für aufteilte DNS hinzuzufügen.

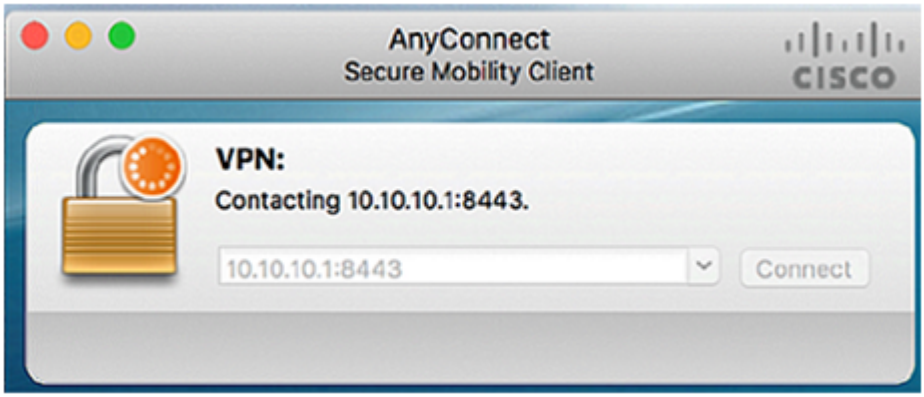
Schritt 15: Geben Sie den Domänennamen in das entsprechende Feld ein und klicken Sie auf **Apply** (Anwenden).

AnyConnect-VPN-Verbindung überprüfen

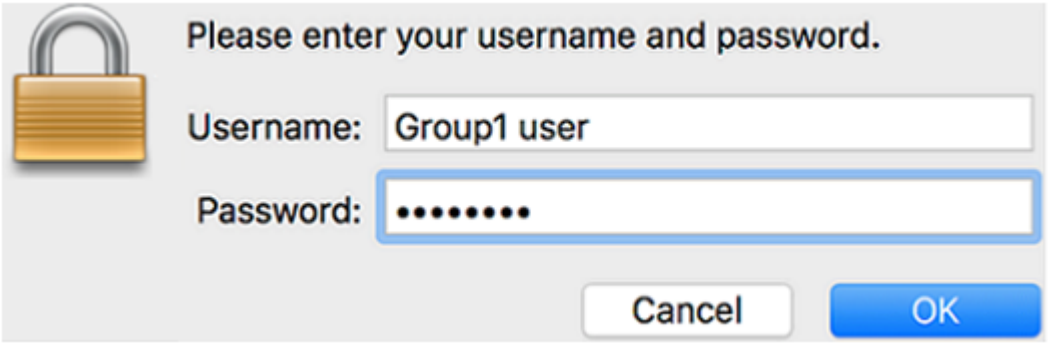
Schritt 1: Klicken Sie auf das Symbol **AnyConnect Secure Mobility Client**.

Schritt 2: Geben Sie im Fenster "AnyConnect Secure Mobility Client" die IP-Adresse und die Portnummer des Gateways getrennt durch einen Doppelpunkt (:) ein, und klicken Sie dann auf **Connect** (Verbinden).

Hinweis: In diesem Beispiel wird „10.10.10.1:8443“ verwendet. Die Software zeigt jetzt an, dass sie das Remote-Netzwerk kontaktiert.

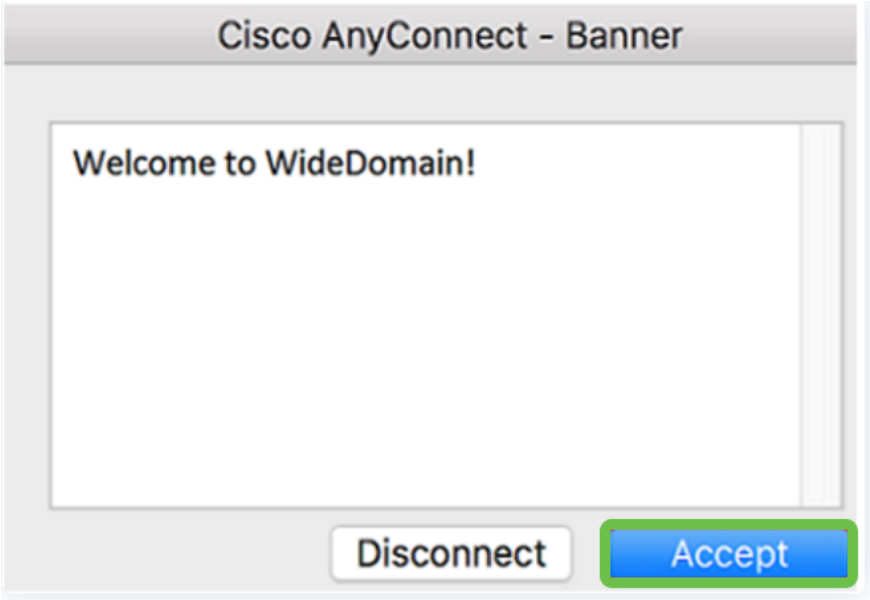


Schritt 3: Geben Sie Ihren Server-Benutzernamen und Ihr Kennwort in die entsprechenden Felder ein und klicken Sie dann auf **OK**.

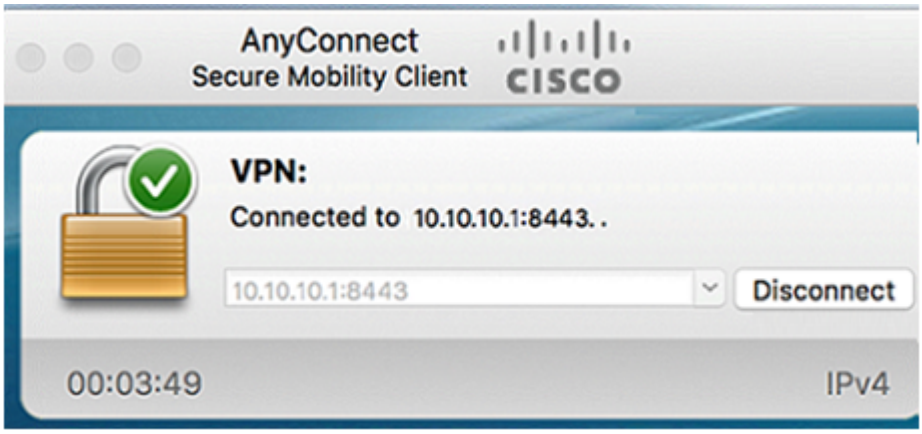


Hinweis: In diesem Beispiel wird der Benutzer Group1 als Benutzername verwendet.

Schritt 4: Sobald die Verbindung hergestellt ist, wird das Anmeldebanner angezeigt. Klicken Sie auf **Accept** (Akzeptieren).



Das AnyConnect-Fenster sollte jetzt die erfolgreiche VPN-Verbindung zum Netzwerk anzeigen.



Schritt 5: (Optional) Klicken Sie auf **Trennen**, um die Verbindung zum Netzwerk zu trennen.

Sie müssten die AnyConnect-VPN-Verbindung mit einem Router der RV34x-Serie jetzt erfolgreich konfiguriert haben.

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.