Konfigurieren eines Secure Sockets Layer Virtual Private Network (SSL VPN) auf dem Router RV340 oder RV345

Besonderer Hinweis: Lizenzierungsstruktur - Firmware-Versionen 1.0.3.15 und höher Für AnyConnect wird künftig nur noch eine Gebühr für Client-Lizenzen berechnet.

Weitere Informationen zur AnyConnect-Lizenzierung auf Routern der Serie RV340 finden Sie im Artikel AnyConnect-Lizenzierung für Router der Serie RV340.

Ziel

Das Secure Sockets Layer Virtual Private Network (SSL VPN)-Gateway ermöglicht es Remote-Benutzern, mithilfe eines Webbrowsers einen sicheren VPN-Tunnel einzurichten. Diese Funktion ermöglicht den einfachen Zugriff auf eine Vielzahl von Webressourcen und webfähigen Anwendungen über die native HTTP-Browserunterstützung (Hypertext Transfer Protocol Secure) über SSL.

SSL VPN ermöglicht Benutzern den Remote-Zugriff auf Netzwerke mit Zugangsbeschränkungen über einen sicheren und authentifizierten Pfad, indem der Netzwerkverkehr verschlüsselt wird.

Die Router RV340 und RV345 unterstützen den Cisco AnyConnect VPN-Client oder auch AnyConnect Secure Mobility Client. Diese Router unterstützen standardmäßig zwei SSL VPN-Tunnel, und der Benutzer kann eine Lizenz für die Unterstützung von bis zu 50 Tunneln registrieren. Nach der Installation und Aktivierung richtet das SSL VPN einen sicheren Remote-Access-VPN-Tunnel ein.

In diesem Artikel wird erläutert, wie Sie SSL VPN auf dem RV340- oder dem RV345-Router konfigurieren.

Unterstützte Geräte

- RV340
- RV345
- Cisco Secure Mobility-Client

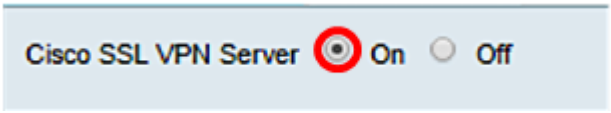
Software-Version

- 1.0.3.15 — RV340, RV345
- 4.4.01054 - AnyConnect Secure Mobility Client

Konfigurieren von SSL VPN

Schritt 1: Öffnen Sie das webbasierte Dienstprogramm des Routers, und wählen Sie VPN > SSL VPN aus.

Schritt 2: Klicken Sie auf das Optionsfeld Ein, um Cisco SSL VPN Server zu aktivieren.

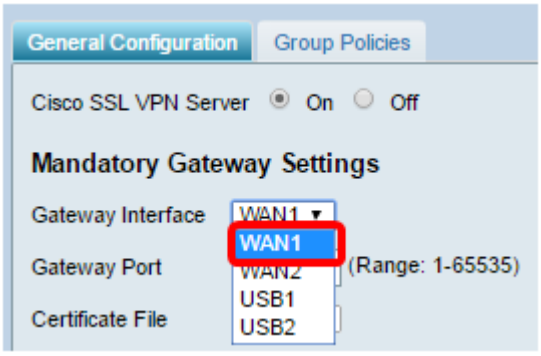


Obligatorische Gateway-Einstellungen

Die folgenden Konfigurationseinstellungen sind obligatorisch:

Schritt 3: Wählen Sie die Gateway-Schnittstelle aus der Dropdown-Liste 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

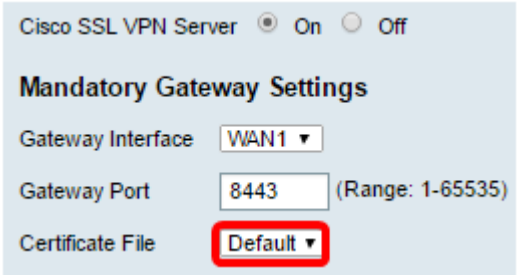


Anmerkung: In diesem Beispiel wird WAN1 ausgewählt.

Schritt 4: Geben Sie die Portnummer für das SSL VPN-Gateway in das Feld Gateway-Port zwischen 1 und 65535 ein.

Anmerkung: In diesem Beispiel wird 8443 als Portnummer verwendet.

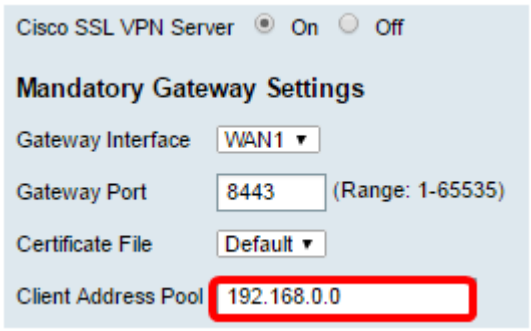
Schritt 5: Wählen Sie die Zertifikatsdatei aus der Dropdown-Liste aus. Dieses Zertifikat authentifiziert Benutzer, die versuchen, über die SSL-VPN-Tunnel auf die Netzwerkressource zuzugreifen. Die Dropdown-Liste enthält ein Standardzertifikat und die importierten Zertifikate.



Anmerkung: In diesem Beispiel wird "Default" (Standard) ausgewählt.

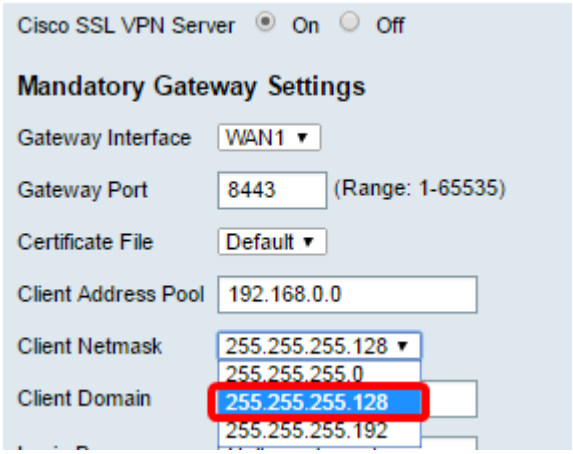
Schritt 6: Geben Sie die IP-Adresse des Client-Adresspools in das Feld Client-Adresspool ein. Dieser Pool ist der Bereich der IP-Adressen, der Remote-VPN-Clients zugewiesen wird.

Anmerkung: Stellen Sie sicher, dass der IP-Adressbereich nicht mit Adressen im lokalen Netzwerk überlappt.



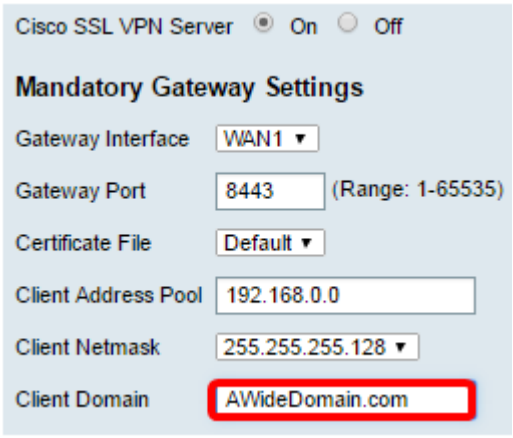
Anmerkung: In diesem Beispiel wird 192.168.0.0 verwendet.

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



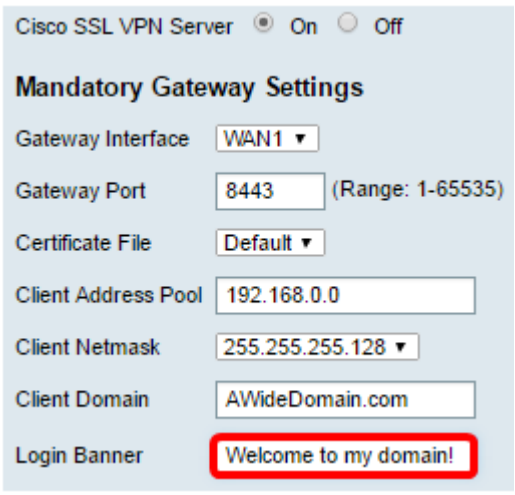
Anmerkung: In diesem Beispiel wird 255.255.255.128 ausgewählt.

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



Anmerkung: In diesem Beispiel wird AWideDomain als Client-Domänenname verwendet.

Schritt 9: Geben Sie den Text ein, der als Anmeldebanner im Feld Anmeldebanner angezeigt wird. Dieses Banner wird bei jeder Anmeldung eines Clients angezeigt.



Anmerkung: In diesem Beispiel, Willkommen in meiner Domäne! als Anmeldebanner verwendet.

Optionale Gateway-Einstellungen

Die folgenden Konfigurationseinstellungen sind optional:

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

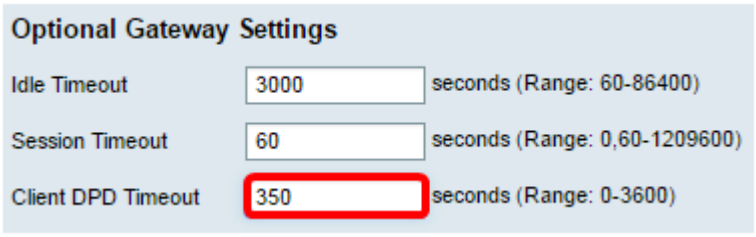
Anmerkung: In diesem Beispiel wird 3000 verwendet.

Schritt 2: Geben Sie im Feld Sitzungstimeout 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.

Anmerkung: In diesem Beispiel wird 60 verwendet.

Schritt 3: Geben Sie im Feld "ClientDPD Timeout" einen Wert in Sekunden von 0 bis 3600 ein. Dieser Wert gibt das regelmäßige Senden von HELLO/ACK-Nachrichten zur Prüfung des Status des VPN-Tunnels an.

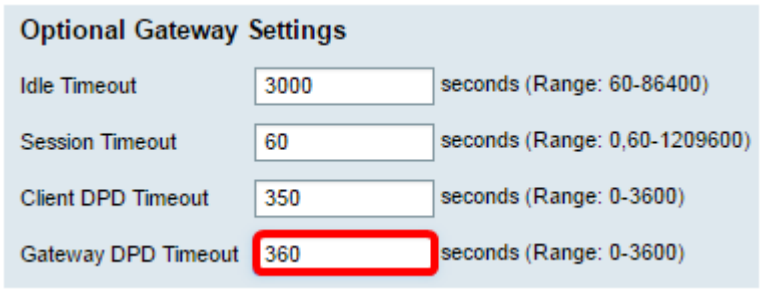
Anmerkung: Diese Funktion muss an beiden Enden des VPN-Tunnels aktiviert sein.



Anmerkung: In diesem Beispiel wird 350 verwendet.

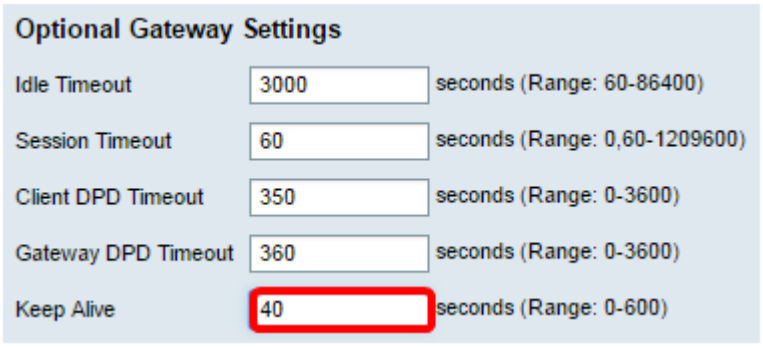
Schritt 4: Geben Sie im Feld GatewayDPD-Zeitüberschreitung einen Wert in Sekunden von 0 bis 3600 ein. Dieser Wert gibt das regelmäßige Senden von HELLO/ACK-Nachrichten zur Prüfung des Status des VPN-Tunnels an.

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



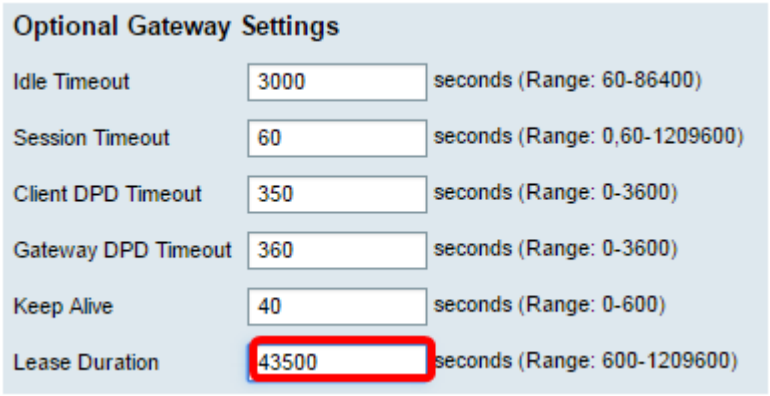
Anmerkung: In diesem Beispiel wird 360 verwendet.

Schritt 5: Geben Sie im Feld Verbindung aufrecht halten einen Wert in Sekunden von 0 bis 600 ein. Mit dieser Funktion wird sichergestellt, dass Ihr Router immer mit dem Internet verbunden ist. Sie versucht, eine getrennte VPN-Verbindung wiederherzustellen.



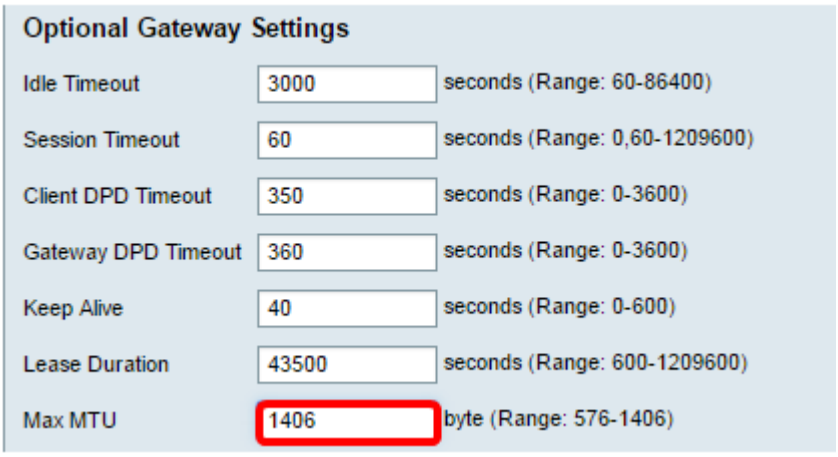
Anmerkung: In diesem Beispiel wird 40 verwendet.

Schritt 6: Geben Sie im Feld "Leasedauer" einen Wert in Sekunden für die Dauer des anzuschließenden Tunnels ein. Möglich sind Werte im Bereich von 600 bis 1209600 Sekunden.



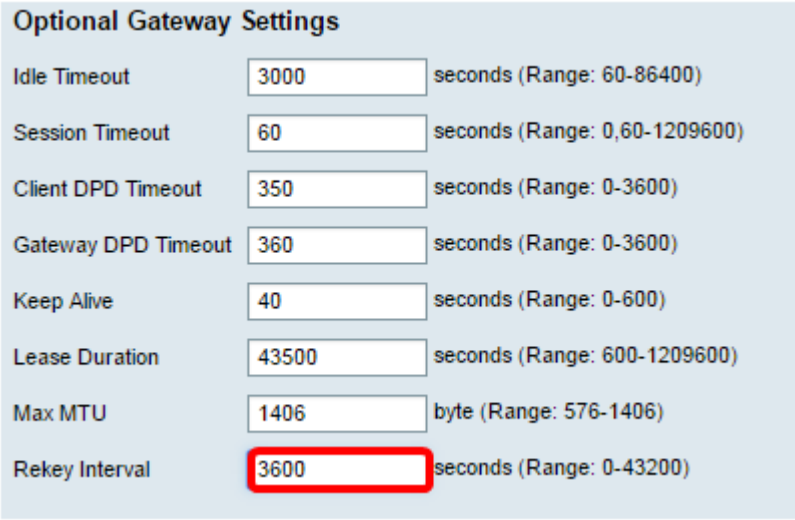
Anmerkung: In diesem Beispiel wird 43500 verwendet.

Schritt 7: Geben Sie die Paketgröße in Byte ein, die über das Netzwerk gesendet werden kann. Der Bereich liegt zwischen 576 und 1406.



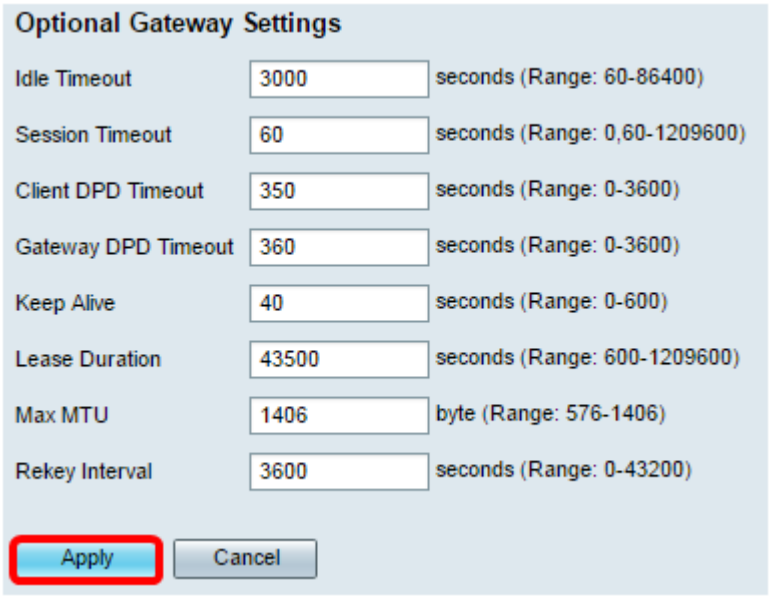
Anmerkung: In diesem Beispiel wird 1406 verwendet.

Schritt 8: Geben Sie im Feld "Rekey Interval" (Intervall für erneute Schlüsselerstellung) die Zeitspanne 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.



Anmerkung: In diesem Beispiel wird 3600 verwendet.

Schritt 9: Klicken Sie auf Anwenden.



Schritt 10. (Optional) Um die Konfiguration dauerhaft zu speichern, klicken Sie auf das blinkende 

Symbol.

Sie sollten nun SSL VPN auf Ihrem RV34x-Router 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.