在 RV34x 系列路由器上設定 AnyConnect Virtual Private Network (VPN) 連線

目標

本文件的目標是為您說明如何在 RV34x 系列路由器上設定 AnyConnect VPN 連線功能。

使用AnyConnect安全移動客戶端的優勢：

1. 安全且持久的連線
2. 持久的安全和策略實施
3. 可以從自適應安全裝置(ASA)或從企業軟體部署系統部署
4. 可定製和可翻譯的
5. 易於配置
6. 支援網際網路協定安全(IPSec)和安全套接字層(SSL)
7. 支援Internet金鑰交換版本2.0(IKEv2.0)協定

簡介

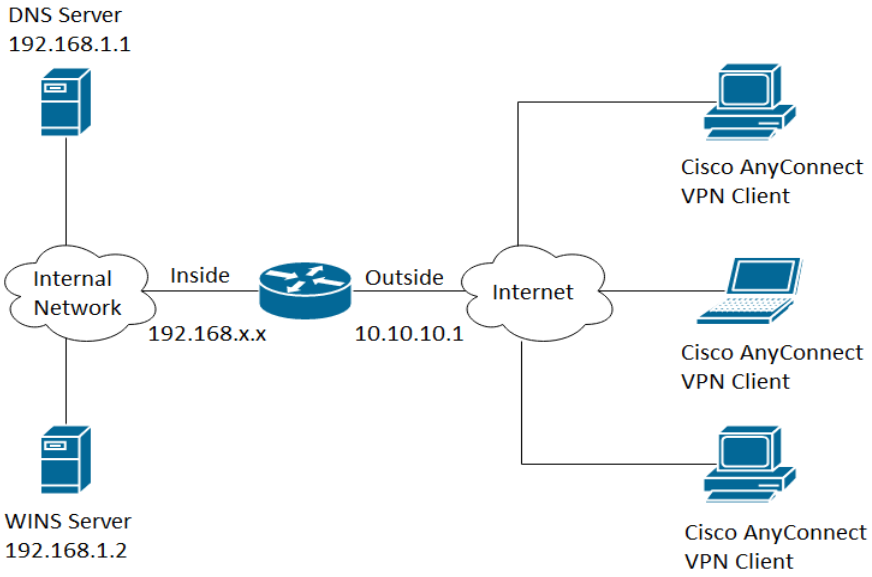
虛擬專用網路(VPN)連線允許使用者通過公共或共用網路（例如Internet）來訪問、傳送和從專用網路接收資料，但仍確保與底層網路基礎設施的安全連線，以保護專用網路及其資源。

VPN客戶端是在要連線到遠端網路的電腦上安裝並運行的軟體。此客戶端軟體的設定配置必須與VPN伺服器的配置相同，例如IP地址和身份驗證資訊。此驗證資訊包括將用於加密資料的使用者名稱和預共用金鑰。根據要連線的網路的物理位置，VPN客戶端也可以是硬體裝置。如果使用VPN連線連線位於不同位置的兩個網路，通常會發生這種情況。

Cisco AnyConnect Security Mobility Client是一種軟體應用程式，用於連線到在各種作業系統和硬體配置上工作的VPN。此軟體應用程式使使用者能夠像直接連線到其網路一樣安全地訪問另一個網路的遠端資源。Cisco AnyConnect Security Mobility Solution提供了一種創新方法，可在基於電腦或智慧電話平台上保護移動使用者，為終端使用者提供更加無縫、始終受保護的體驗，並為IT管理員提供全面的策略實施。

在RV34x路由器上，從韌體版本1.0.3.15開始，無需進行AnyConnect許可。僅對客戶端許可證收費。

有關RV340系列路由器上的AnyConnect許可的其他資訊，請參閱RV340系列路由器的AnyConnect許可文章。



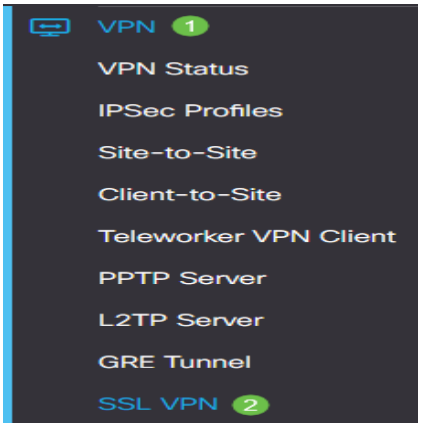
適用裝置 |韌體版本

- Cisco AnyConnect Security Mobility Solution — 遠端存取 | 4.4(下載最新版本)
- RV34x系列 | 1.0.03.15(下載最新版本)

在RV34x上配置AnyConnect VPN連線

在RV34x上配置SSL VPN

步驟1.訪問路由器基於Web的實用程式並選擇**VPN > SSL VPN**。



步驟2.按一下**On**單選按鈕以啟用Cisco SSL VPN伺服器。

強制網關設定

必須使用以下配置設定：

步驟3.從下拉選單中選擇Gateway Interface。此埠將用於通過SSL VPN隧道傳輸流量。選項包括：

- WAN1

- WAN2
- USB1
- USB2

注意：在本例中，選擇了WAN1。

步驟4.在*Gateway Port*欄位中輸入用於SSL VPN網關的埠號，範圍為1到65535。

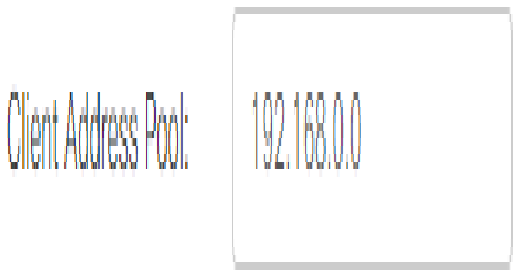
注意：在本示例中，8443用作埠號。

步驟5.從下拉選單中選擇Certificate File。此證書對嘗試通過SSL VPN隧道訪問網路資源的使用者進行身份驗證。下拉選單包含預設證書和匯入的證書。

注意：**在**本示例中，選擇了「預設」(Default)。

步驟6.在*Client Address Pool*欄位中輸入客戶端地址池的IP地址。此池將是分配給遠端VPN客戶端的IP地址範圍。

注意：確保IP地址範圍不會與本地網路上的任何IP地址重疊。



注意：本示例使用192.168.0.0。

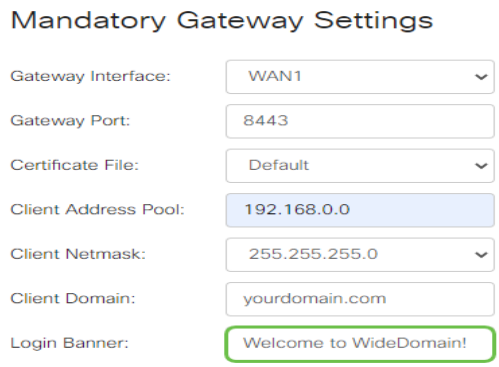
步驟7.從下拉選單中選擇Client Netmask。

注意：在本例中，選擇了255.255.255.128。

步驟8.在*Client Domain*（客戶端域）欄位中*輸入客戶端*域名。這是應推送到SSL VPN客戶端的域名。

注意：在本示例中，WideDomain.com用作客戶端域名。

步驟9.在*Login Banner*欄位中輸入顯示為登入標語的文本。這將是在每次客戶端登入時顯示的標語。



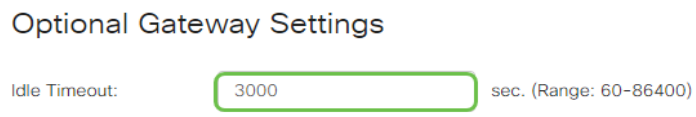
注意：在本示例中，歡迎使用Widedomain！用作登入標語。

可選網關設定

以下配置設定是可選的：

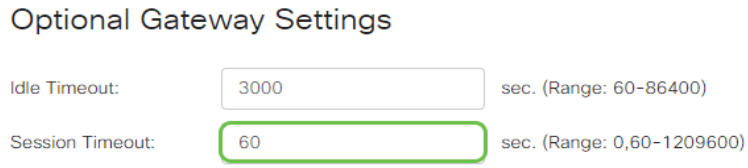
步驟1.輸入介於60到86400之間的空閒超時值（以秒為單位）。這是SSL VPN會話可以保持空閒的

持續時間。



註：在此示例中，使用3000。

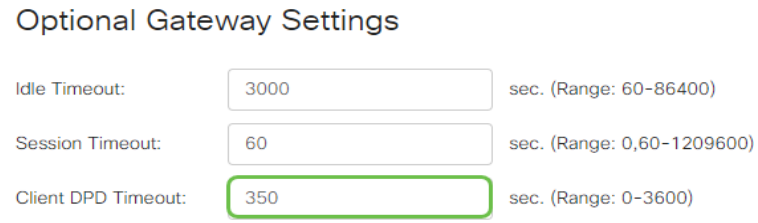
步驟2.在*Session Timeout*（會話超時）欄位中輸入一*個以秒為*單位的值。這是傳輸控制通訊協定(TCP)或使用者資料包通訊協定(UDP)作業階段在指定的閒置時間之後逾時的時間。範圍為60到1209600。



註：在此示例中，使用60。

步驟3.在*ClientDPD Timeout*欄位中輸入一個值（以秒為單位），範圍為0到3600。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。

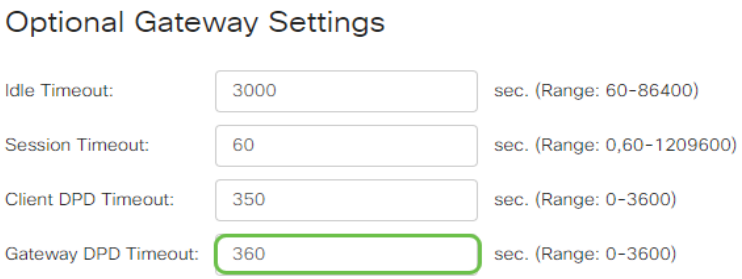
注意：必須在VPN隧道的兩端啟用此功能。



注意：在本示例中，使用350。

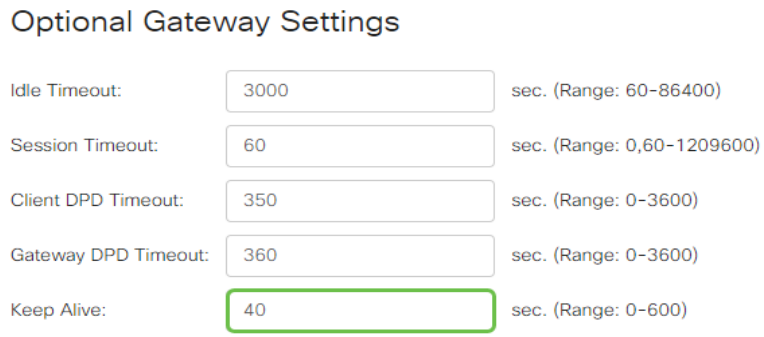
步驟4.在*GatewayDPD Timeout*欄位中輸入一個0到3600之間的值（以秒為單位）。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。

注意：必須在VPN隧道的兩端啟用此功能。



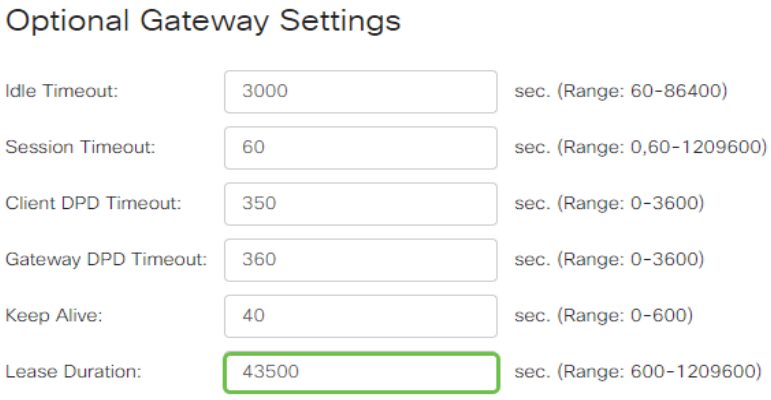
注意：在本示例中，使用360。

步驟5.在*Keep Alive*欄位中輸入一個0到600之間的值（以秒為單位）。此功能可確保您的路由器始終連線到Internet。如果斷開，它將嘗試重新建立VPN連線。



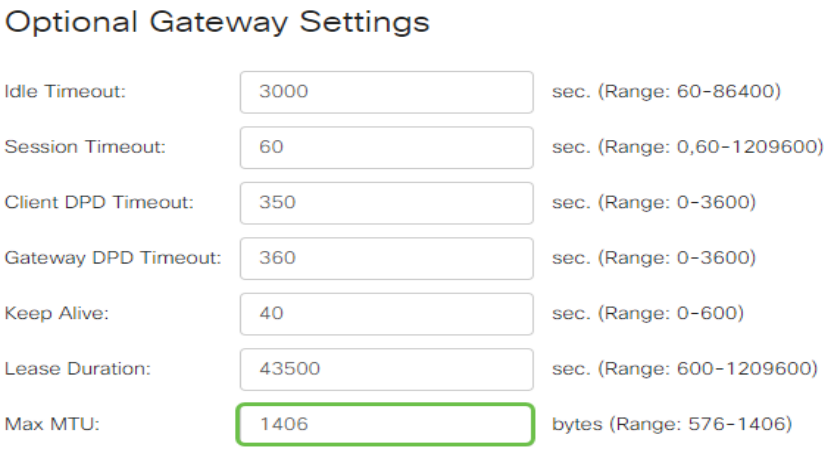
注意：在本示例中，使用40。

步驟6.在*Lease Duration*欄位中輸入要連線的隧道的持續時間值（以秒為單位）。範圍為600到1209600。



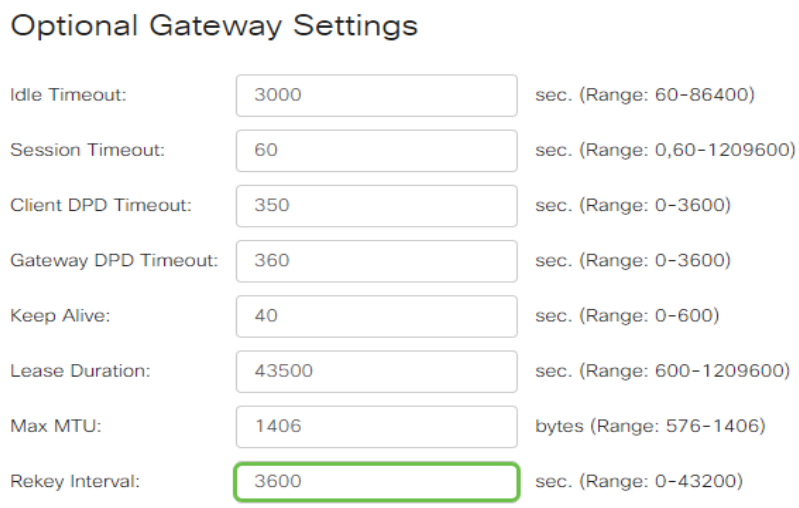
注意：在本示例中，使用43500。

步驟7.輸入可通過網路傳送的資料包大小（以位元組為單位）。範圍為576至1406。



注意：在本示例中，使用1406。

步驟8.在*Rekey Interval*欄位中輸入中繼間隔時間。Rekey功能允許SSL金鑰在會話建立後重新協商。範圍是從0到43200。

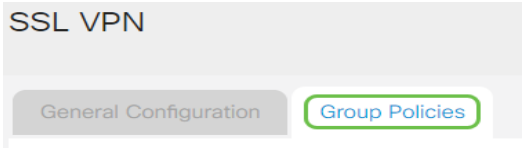


註：本例中使用的是3600。

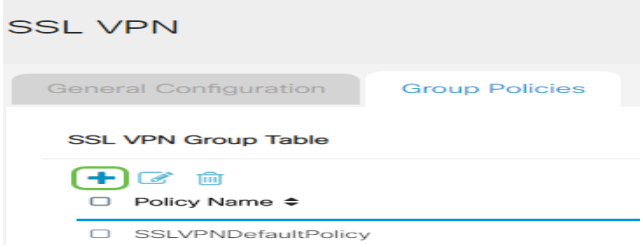
步驟9.按一下「**Apply**」。

配置組策略

步驟1.按一下**Group Policies**頁籤。



步驟2.按一下SSL VPN Group Table下的**Add**按鈕以新增組策略。



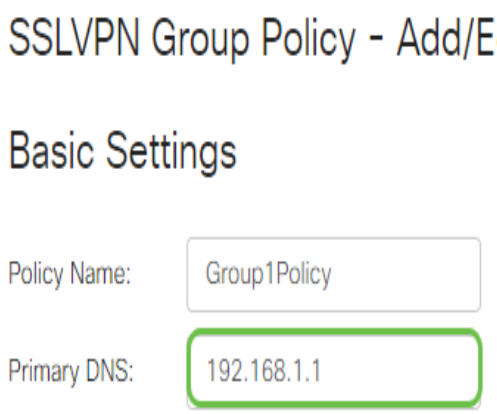
注意：「SSL VPN組」(SSL VPN Group)表格將顯示裝置上的組策略清單。您還可以編輯清單中的

第一個組策略，該策略名為SSLVPNDefaultPolicy。這是裝置提供的預設策略。

步驟3.在*Policy Name*欄位中輸入您的首選策略名稱。

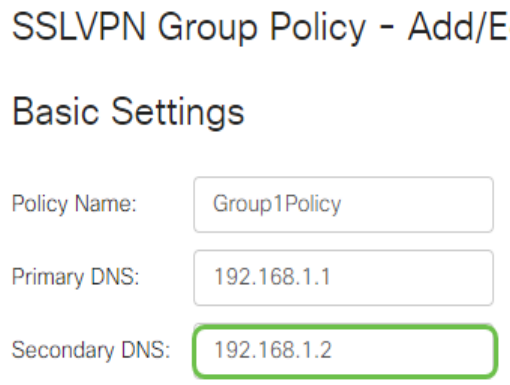
注意：在本示例中，使用組1策略。

步驟4.在提供的欄位中輸入主DNS的IP地址。預設情況下，已提供此IP地址。



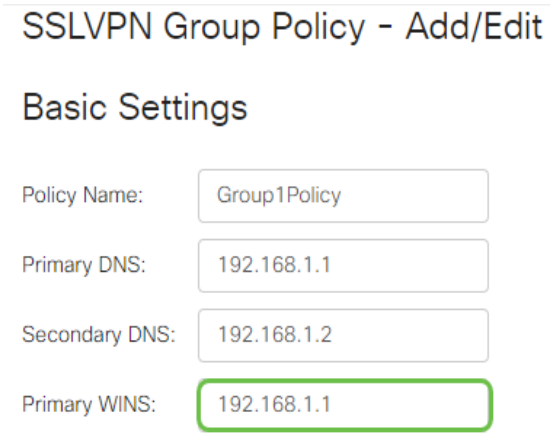
注意：在本例中使用的是192.168.1.1。

步驟5.（可選）在所提供的欄位中輸入輔助DNS的IP地址。這將在主DNS出現故障時用作備份。



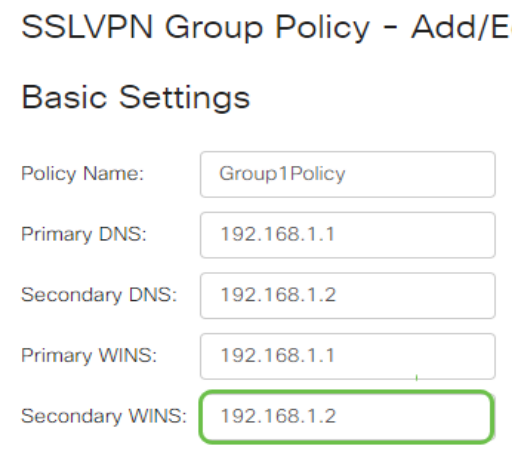
注意：在本例中使用的是192.168.1.2。

步驟6.（可選）在提供的欄位中輸入主WINS的IP地址。



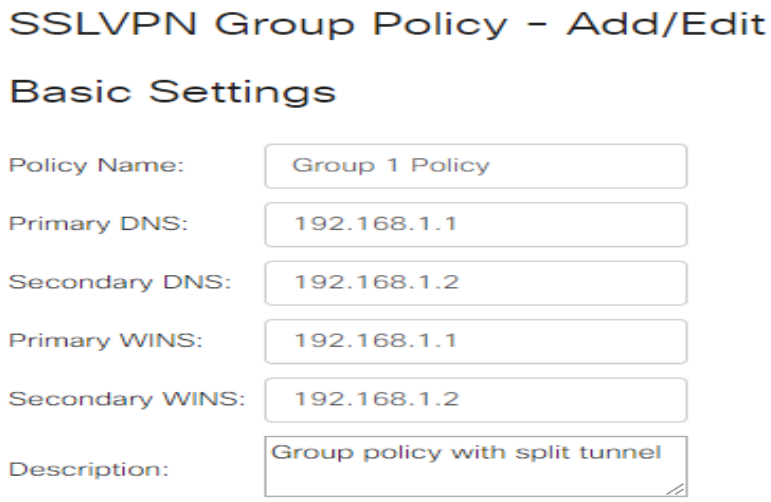
注意：在本例中使用的是192.168.1.1。

步驟7.（可選）在提供的欄位中輸入輔助WINS的IP地址。



注意：在本例中使用的是192.168.1.2。

步驟8。（可選）在*說明*欄位中輸入策略的說明。

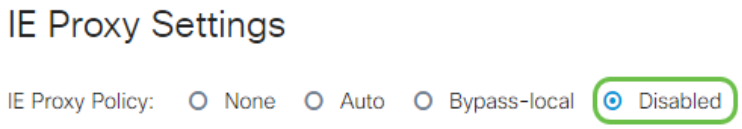


注意：在本示例中，使用具有拆分隧道的組策略。

步驟9.（可選）按一下單選按鈕選擇IE代理策略以啟用Microsoft Internet Explorer(MSIE)代理設定來建立VPN隧道。選項包括：

- None — 允許瀏覽器不使用代理設定。

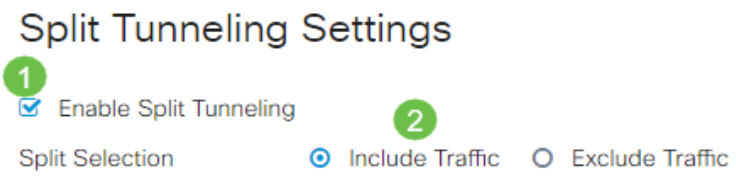
- 自動 — 允許瀏覽器自動檢測代理設定。
- Bypass-local — 允許瀏覽器繞過在遠端使用者上配置的代理設定。
- 已禁用 — 禁用MSIE代理設定。



注意：在本例中，選擇了Disabled。這是預設設定。

步驟10。（可選）在Split Tunneling Settings區域中，選中**Enable Split Tunneling**覈取方塊，允許以未加密方式將目的地為Internet的流量直接傳送到Internet。全通道會將所有流量傳送到終端裝置，然後將其路由到目的地資源，如此一來，就可以將企業網路從用於Web存取的路徑中移除。

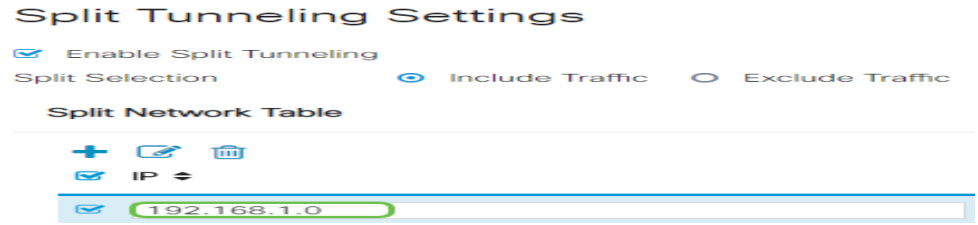
步驟11。（可選）按一下單選按鈕，選擇應用分割隧道時是包括流量還是排除流量。



注意：**在**本示例中，選擇包括流量。

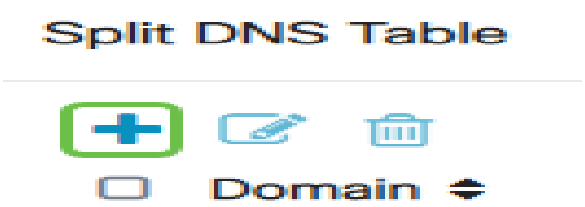
步驟12.在Split Network Table中，按一下**Add**按鈕以新增split Network例外。

步驟13.在提供的欄位中輸入網路的IP地址。



注意：本示例使用192.168.1.0。

步驟14.在拆分DNS表中，按一下**Add**按鈕新增拆分DNS例外。



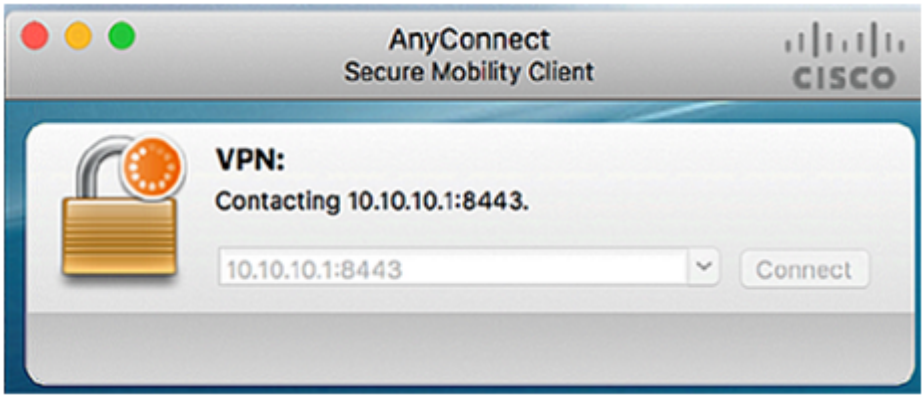
步驟15.在提供的欄位中輸入域名，然後按一下**Apply**。

驗證AnyConnect VPN連線

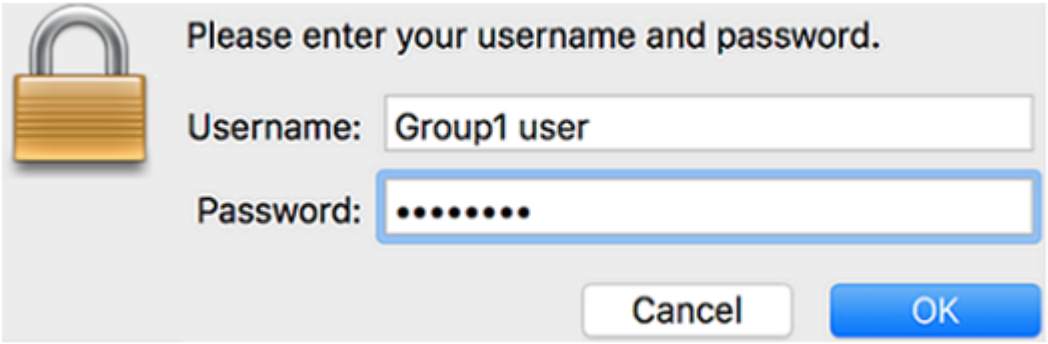
步驟1.點選**AnyConnect Secure Mobility Client**圖標。

步驟2.在AnyConnect Secure Mobility Client（AnyConnect安全移動客戶端）視窗中，輸入網關IP地址和網關埠號(用冒號(:)分隔)，然後按一下**Connect**。

注意：在本示例中，使用10.10.10.1:8443。軟體現在將顯示它正在聯絡遠端網路。

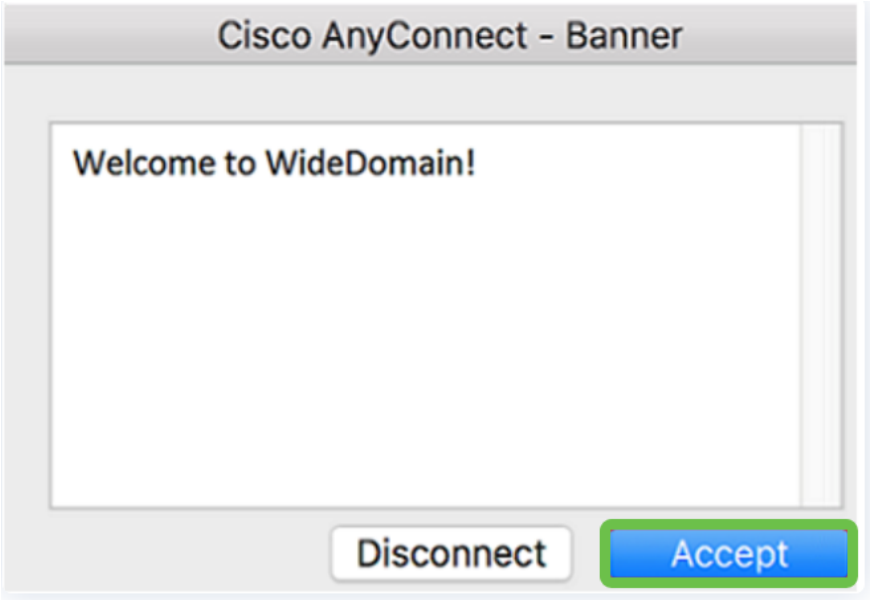


步驟3.在相應的欄位中輸入您的伺服器使用者名稱和密碼，然後按一下**OK**。

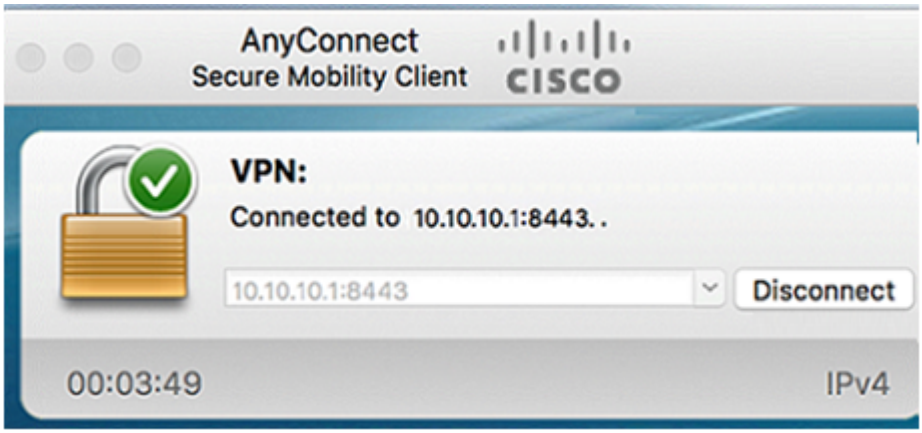


注意：在本示例中，Group1使用者用作使用者名稱。

步驟4.一旦建立連線，就會顯示登入橫幅。按一下「**Accept**」。



AnyConnect視窗現在應指示到網路的VPN連線是否成功。



步驟5.（可選）要斷開網路連線，請按一下**斷開連線**。

現在，您應該已經使用RV34x系列路由器成功配置了AnyConnect VPN連線。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。