在RV160和RV260上配置站點到站點VPN高級設定和故障切換

目標

本文檔的目標是向您展示如何在RV160和RV260上配置站點到站點VPN高級設定和故障切換。

簡介

虛擬專用網路(VPN)是將遠端工作人員連線到安全網路的理想方式。VPN允許遠端主機像連線到現場安全網路一樣工作。在站點到站點VPN中，一個位置的本地路由器通過VPN隧道連線到遠端路由器。此隧道使用行業標準的加密和身份驗證技術安全地封裝資料，以保護傳送的資料。必須在連線的兩端執行相同的配置，才能成功建立站點到站點VPN連線。高級站點到站點VPN配置可靈活配置VPN隧道的可選配置。

故障切換是一項功能強大的功能，可確保這兩個站點之間的持續連線。當容錯很重要時，這很有用。當主路由器關閉時，會發生故障轉移。此時，輔助路由器或備用路由器將接管並提供連線。這將有助於防止單點故障。

適用裝置

- RV160
- RV260

軟體版本

- 1.0.00.13

必要條件

在RV160和RV260上配置站點到站點VPN的高級設定和故障轉移之前，需要在本地和遠端路由器上配置IPsec配置檔案和站點到站點VPN。以下是可幫助您配置這些內容的文章清單。您可以選擇使用VPN設定嚮導，該嚮導將幫助您配置IPsec配置檔案以及站點到站點VPN，或者您可以單獨配置它們，並遵循下面提供的兩個文檔。

1. 在RV160和RV260上配置VPN設定嚮導

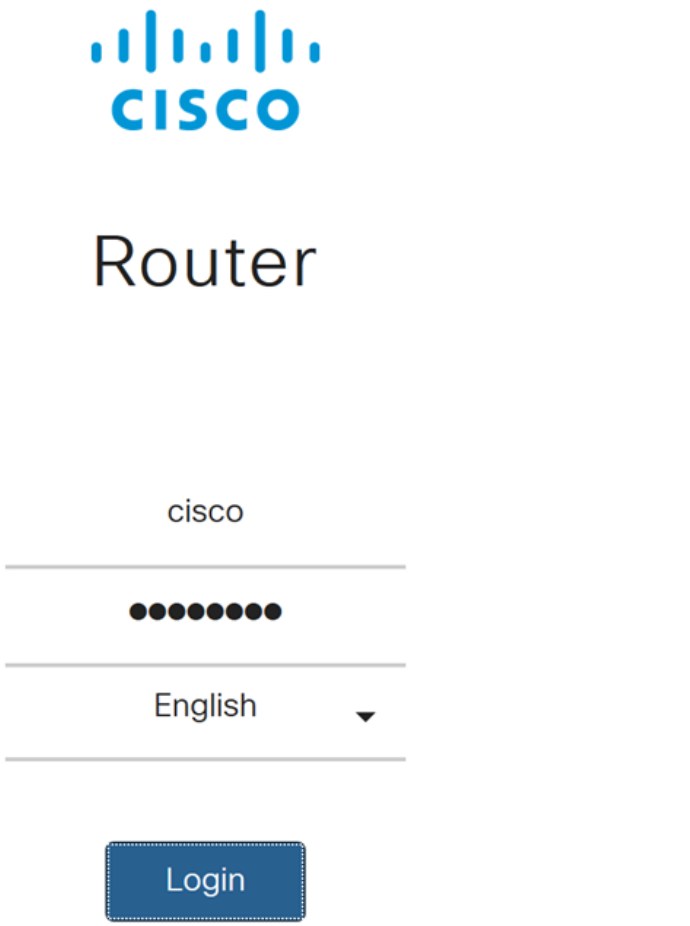
或

1. 在RV160和RV260上配置IPSec配置檔案(自動金鑰模式)（可選）
2. 在RV160和RV260上配置站點到站點VPN

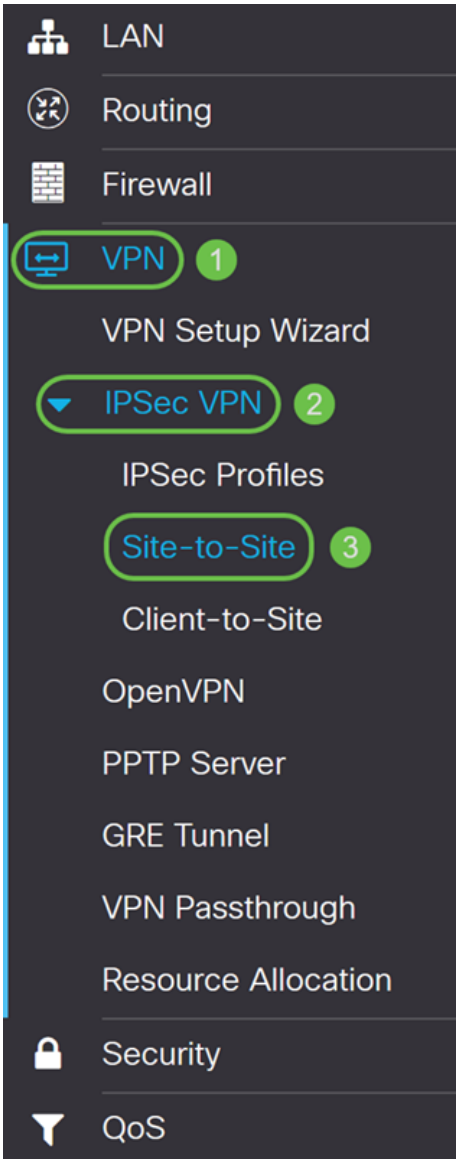
配置站點到站點VPN高級設定

在VPN連線的兩端，高級設定的配置應該相同。

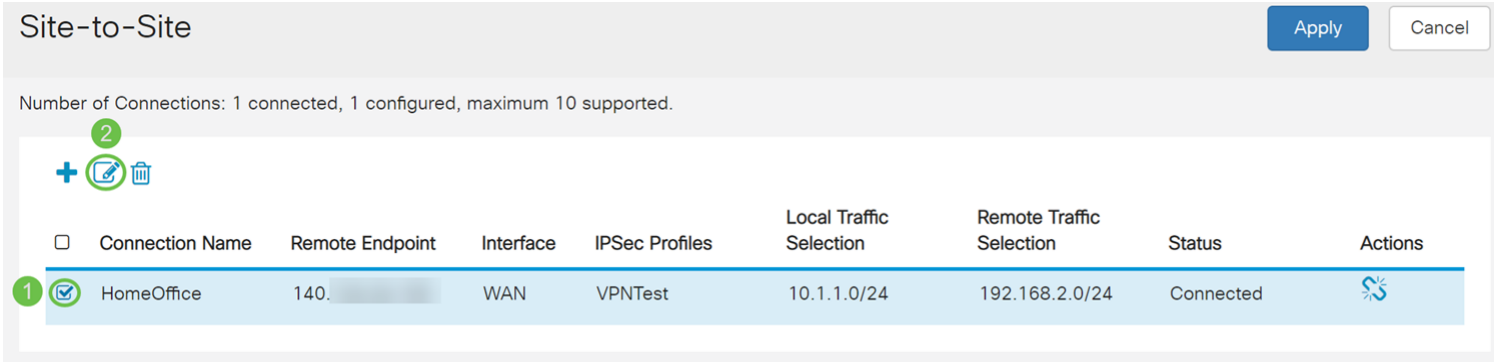
步驟1.登入到Web配置實用程式。



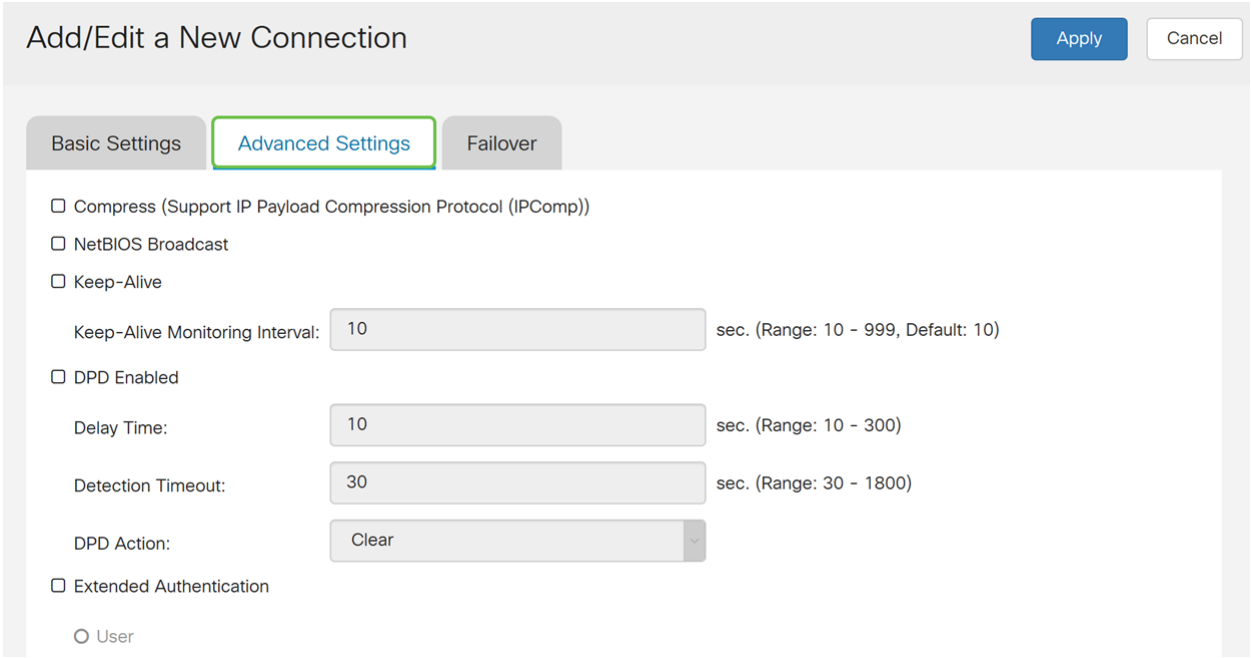
步驟2.導覽至**VPN > IPSec VPN > Site-to-Site**。



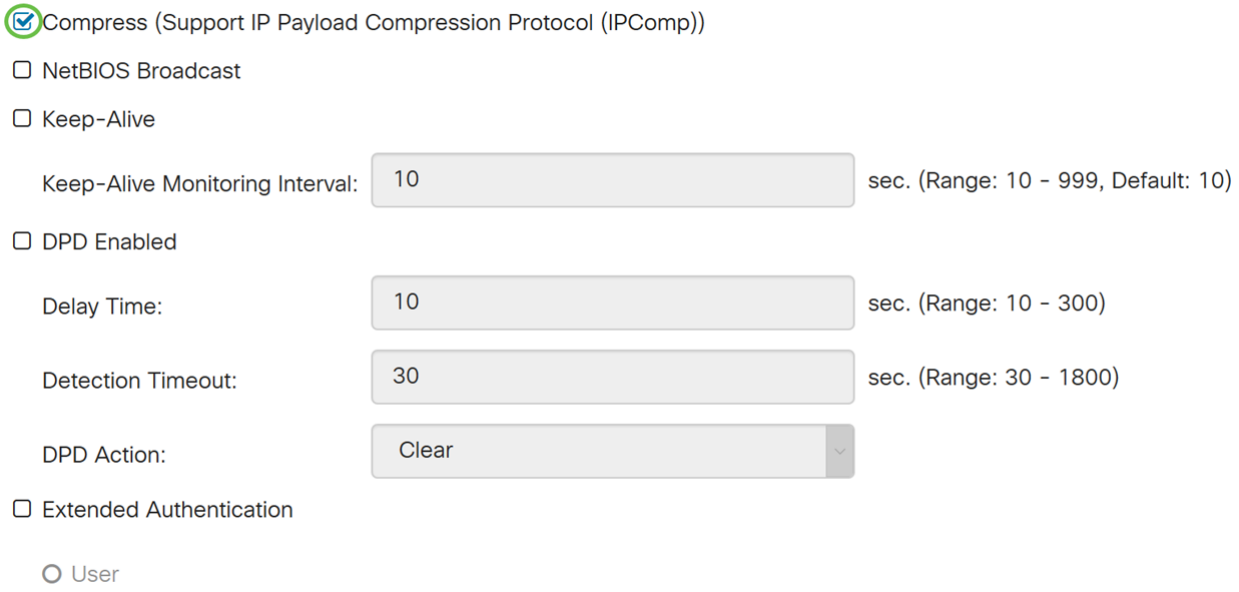
步驟3.選中要編輯的連線覈取方塊。然後按筆**和紙張圖**標編輯連線。在此示例中，選擇了名為HomeOffice的連線。



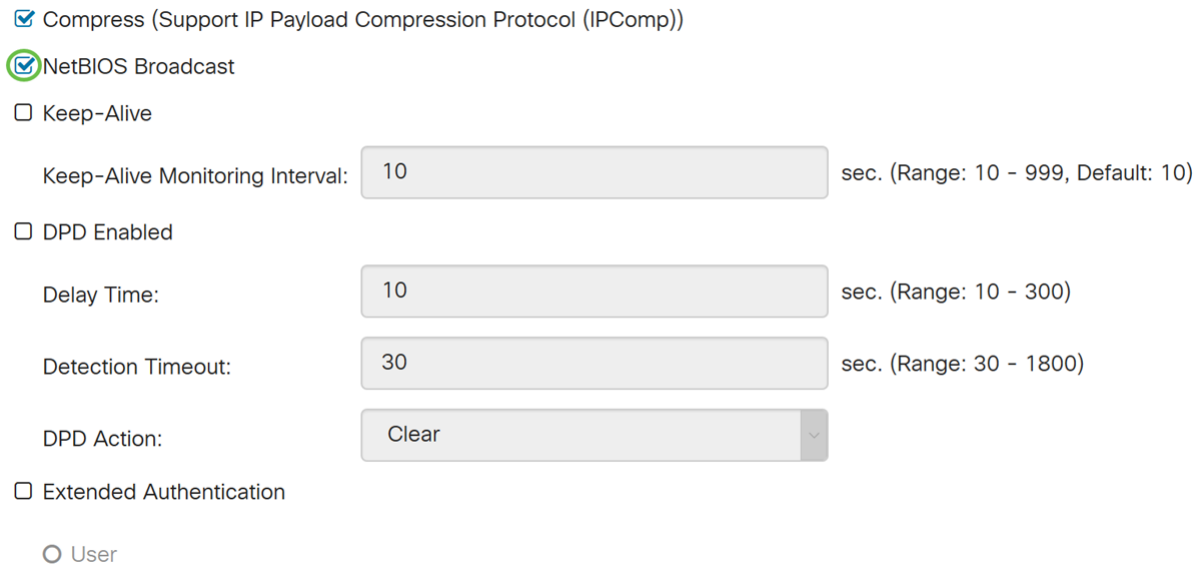
步驟4.按一下**Advanced Settings**選項卡。



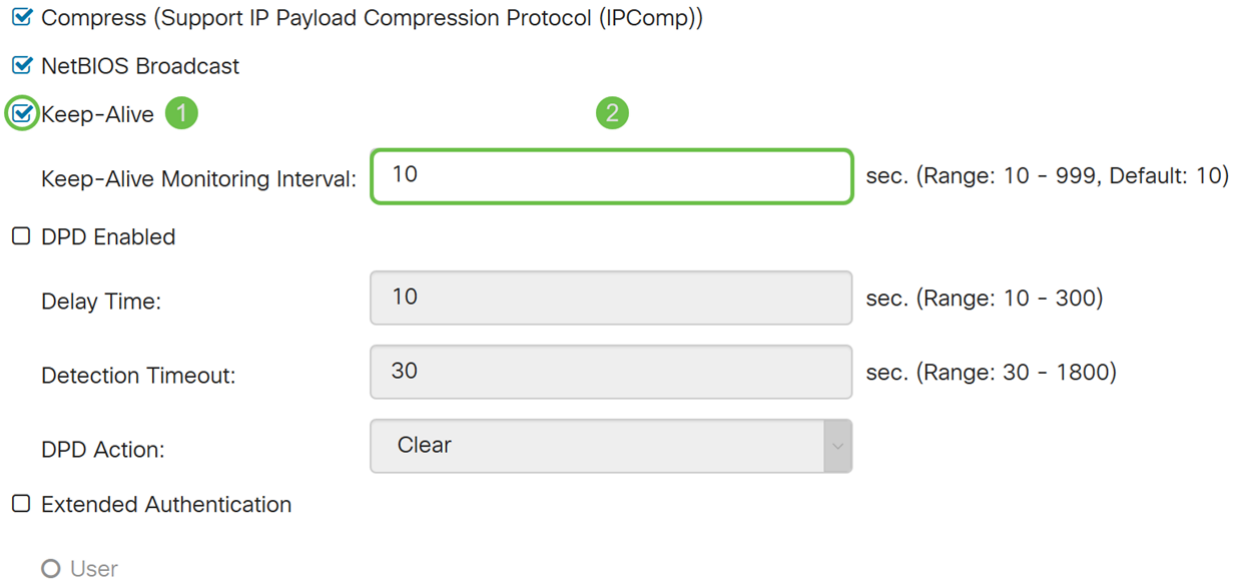
步驟5.選中**Compress(Support IP Payload Compression Protocol(IPComp))**覈取方塊，使路由器能夠在啟動連線時建議壓縮。此通訊協定降低IP資料包的大小。如果響應方拒絕此提議，則路由器不會實施壓縮。當路由器是響應方時，它接受壓縮，即使未啟用壓縮。如果為此路由器啟用此功能，則需要在遠端路由器（隧道的另一端）上啟用它。



步驟6.廣播消息用於Windows網路中的名稱解析，以標識電腦、印表機和檔案伺服器等資源。某些軟體應用程式和Windows功能（例如Network Neighborhood）會使用這些消息。LAN廣播流量通常不會通過VPN隧道轉發。但是，您可以選中此框以允許從隧道的一端向另一端重新廣播NetBIOS廣播。選中**NetBIOS Broadcast**覈取方塊以啟用。

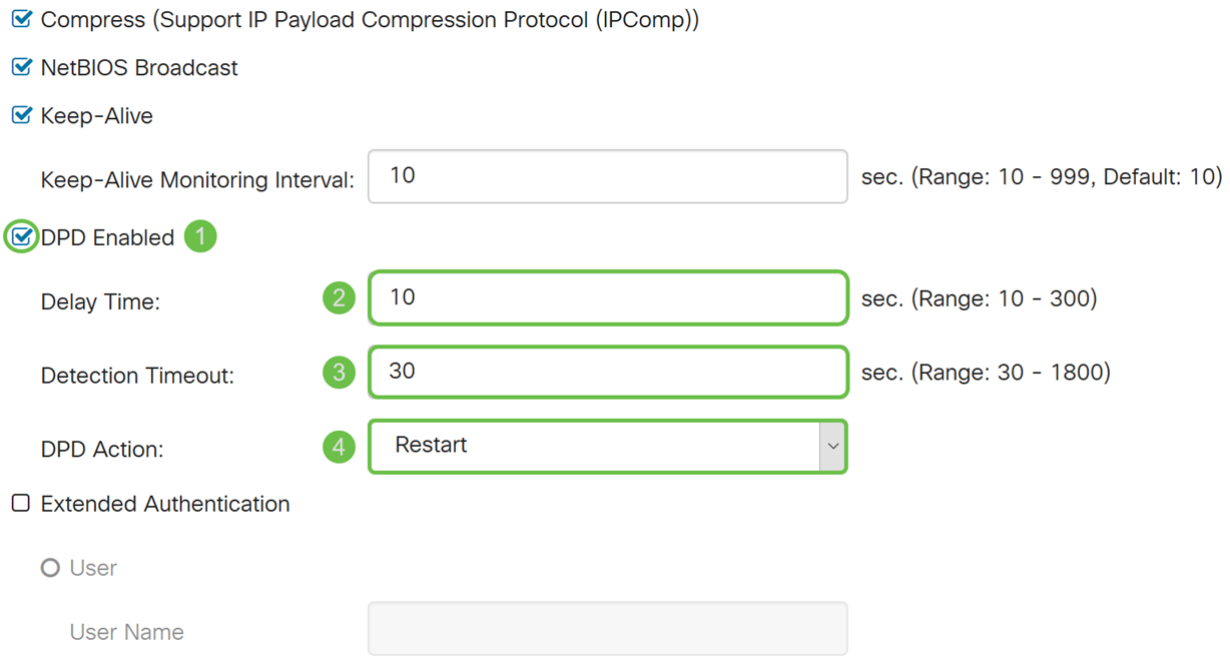


步驟7.選中**Keep-Alive**覈取方塊，使路由器能夠嘗試定期重新建立VPN連線。在*Keep-Alive Monitoring Interval*欄位中輸入設定保持連線監視間隔的秒數。範圍為10-999秒。



步驟8.選中**Dead Peer Detection(DPD)Enabled**以啟用DPD。它會定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。必須在VPN隧道的兩端啟用DPD選項。在Interval欄位中通過輸入以下內容來指定HELLO/ACK消息之間的時間間隔：

- Delay Time — 輸入每個Hello消息之間的時間延遲（以秒為單位）。範圍為10 - 300秒，預設值為10。
- Detection Timeout — 輸入超時（以秒為單位），以宣告對等體已停機。範圍是從30到1800秒。
- DPD操作 — DPD超時後要執行的操作。從下拉選單中選擇**Clear**或**Restart**。

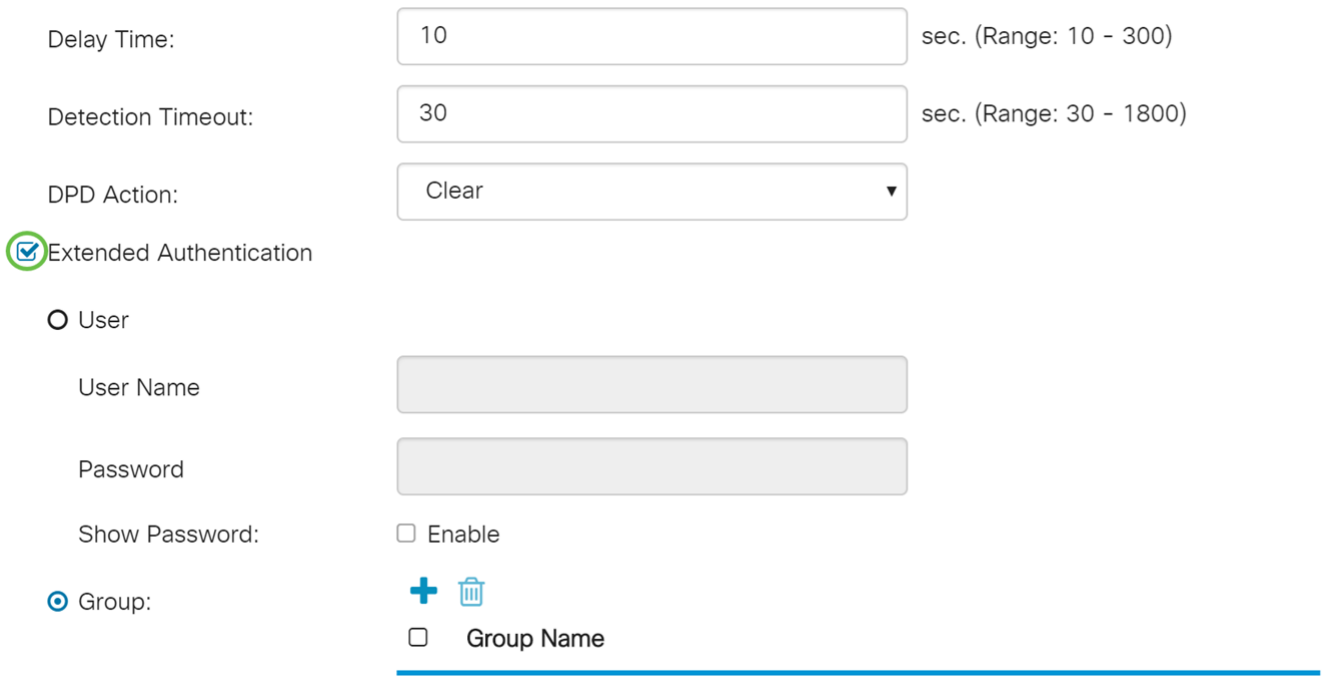


步驟9.如果要啟用擴展身份驗證，請選中**Extended Authentication**。這將提供額外的身份驗證級別，要求遠端使用者在獲得對VPN的訪問許可權之前輸入其憑據。要使擴展身份驗證起作用，主站點必須使用組身份驗證，遠端站點必須使用使用者身份驗證。在接下來的幾個步驟中，我們將配置主站點以使用組身份驗證。

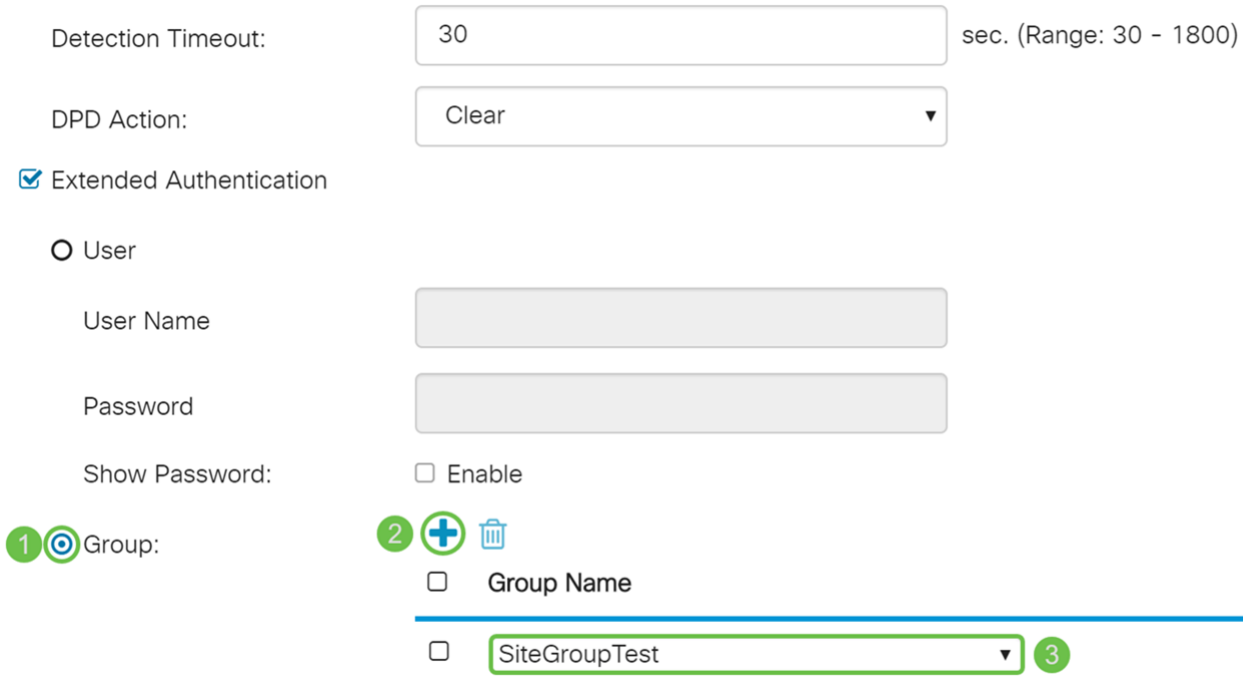
附註：建議配置客戶端到站點以進行使用者身份驗證，而不是擴展身份驗證。

如果尚未建立主網站的使用者組，請按一下連結瞭解如何建立位於本文中的使用者組：正在為擴展身份驗證建立使用者組。

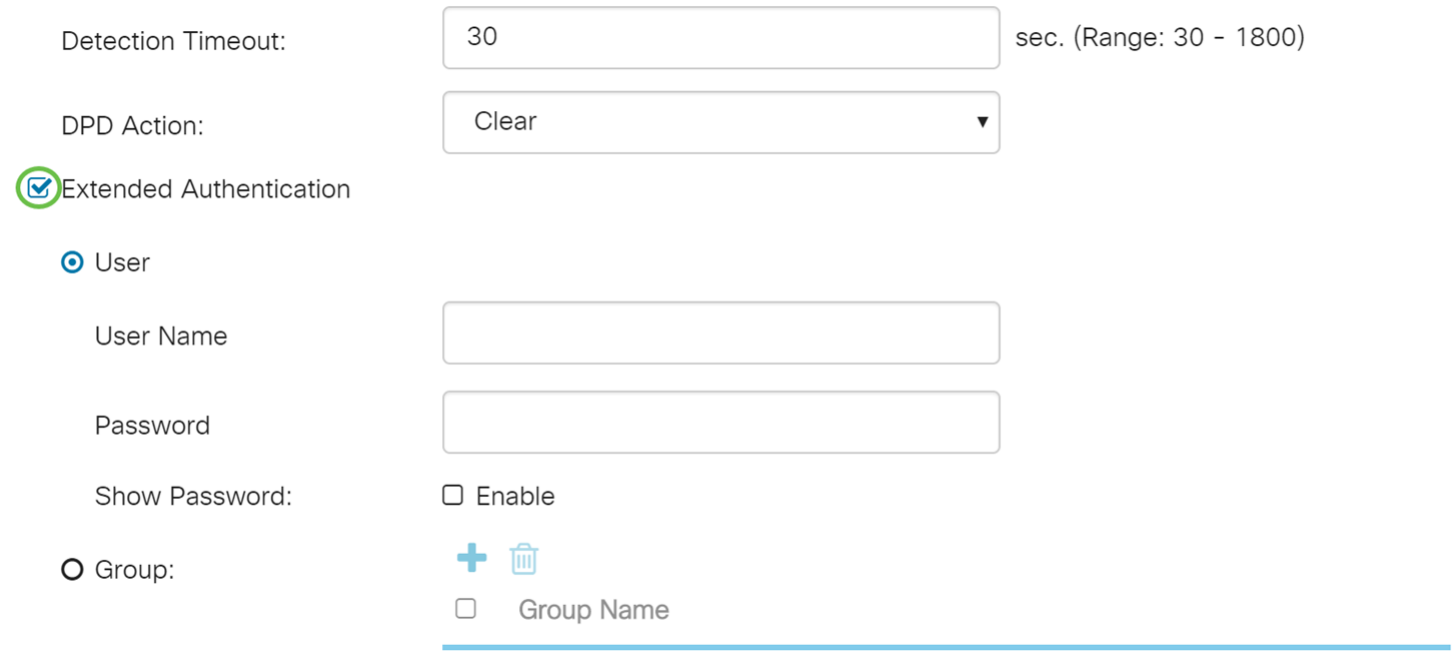
如果您想瞭解如何建立使用者帳戶，請按一下連結重定向到以下部分：正在為擴展身份驗證建立使用者帳戶。



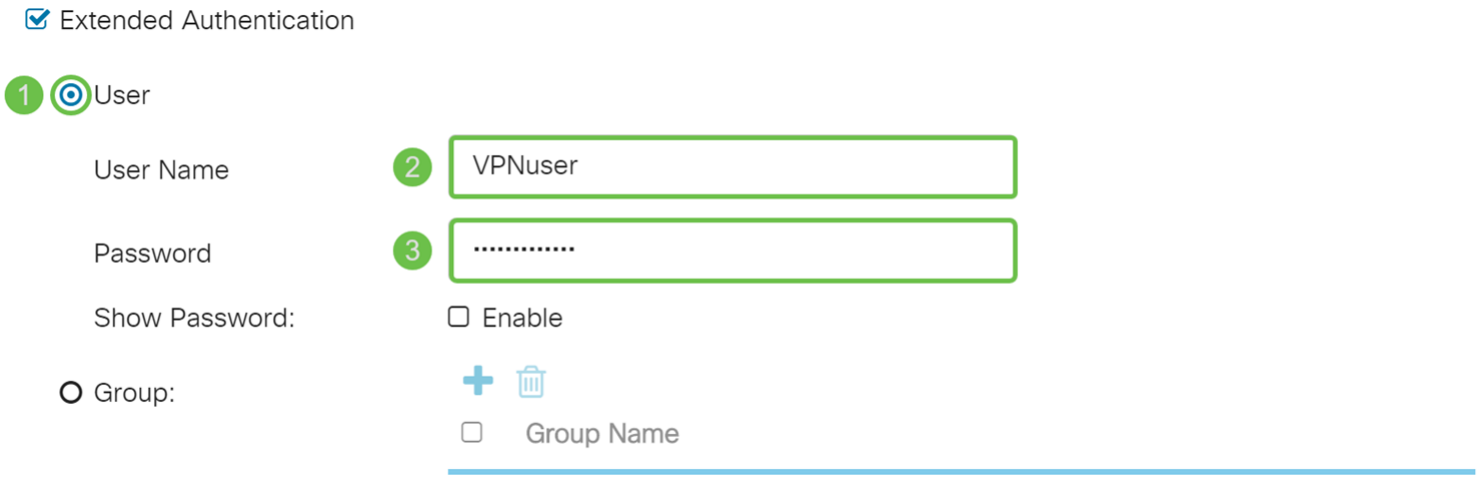
步驟10.選擇**Group**作為擴展身份驗證，然後按**plus**圖示新增新組。從下拉選單中選擇要用於身份驗證的組。確保所需的使用者位於該組中。



步驟11.在接下來的幾個步驟中，我們將配置遠端路由器以使用使用者身份驗證。在遠端路由器中，選中**Extended Authentication**覈取方塊以啟用擴展身份驗證。



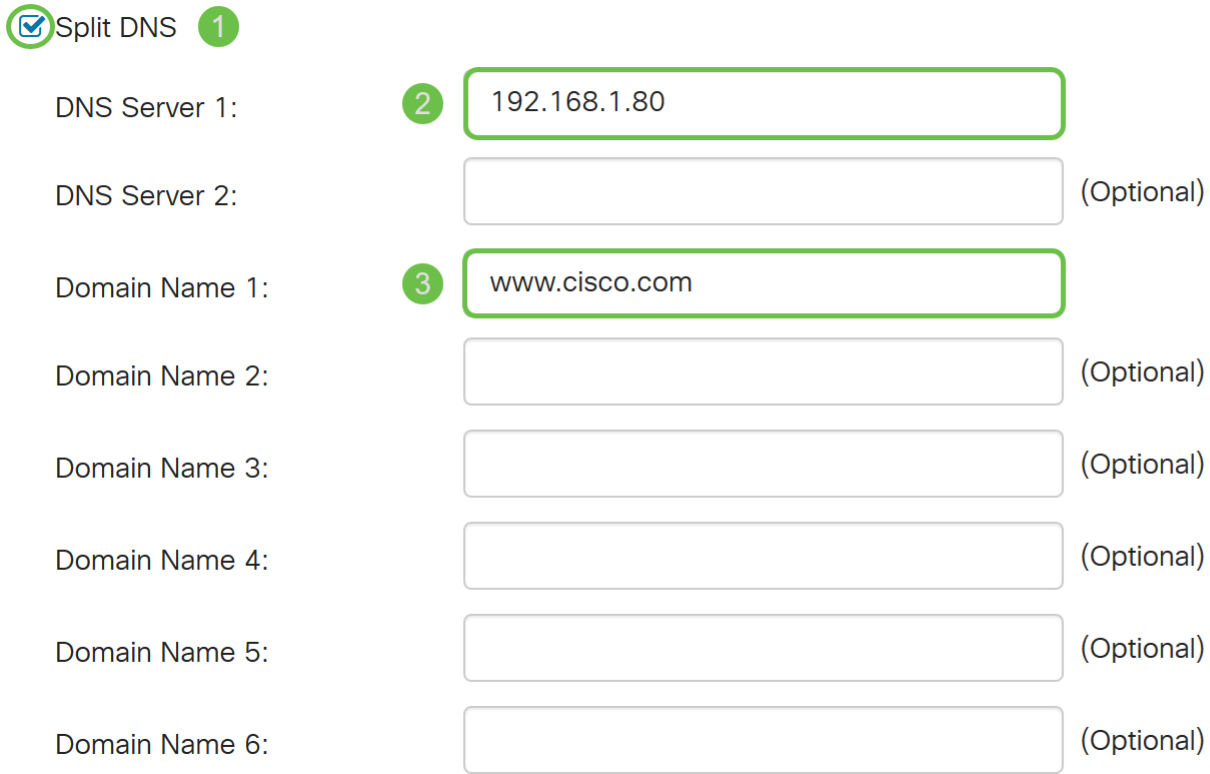
步驟12.選擇**User**作為擴展身份驗證。輸入在主路由器中選擇的組中使用者的**使用者名稱**和**密碼**。在本示例中，VPNuser和CiscoTest123!已輸入。



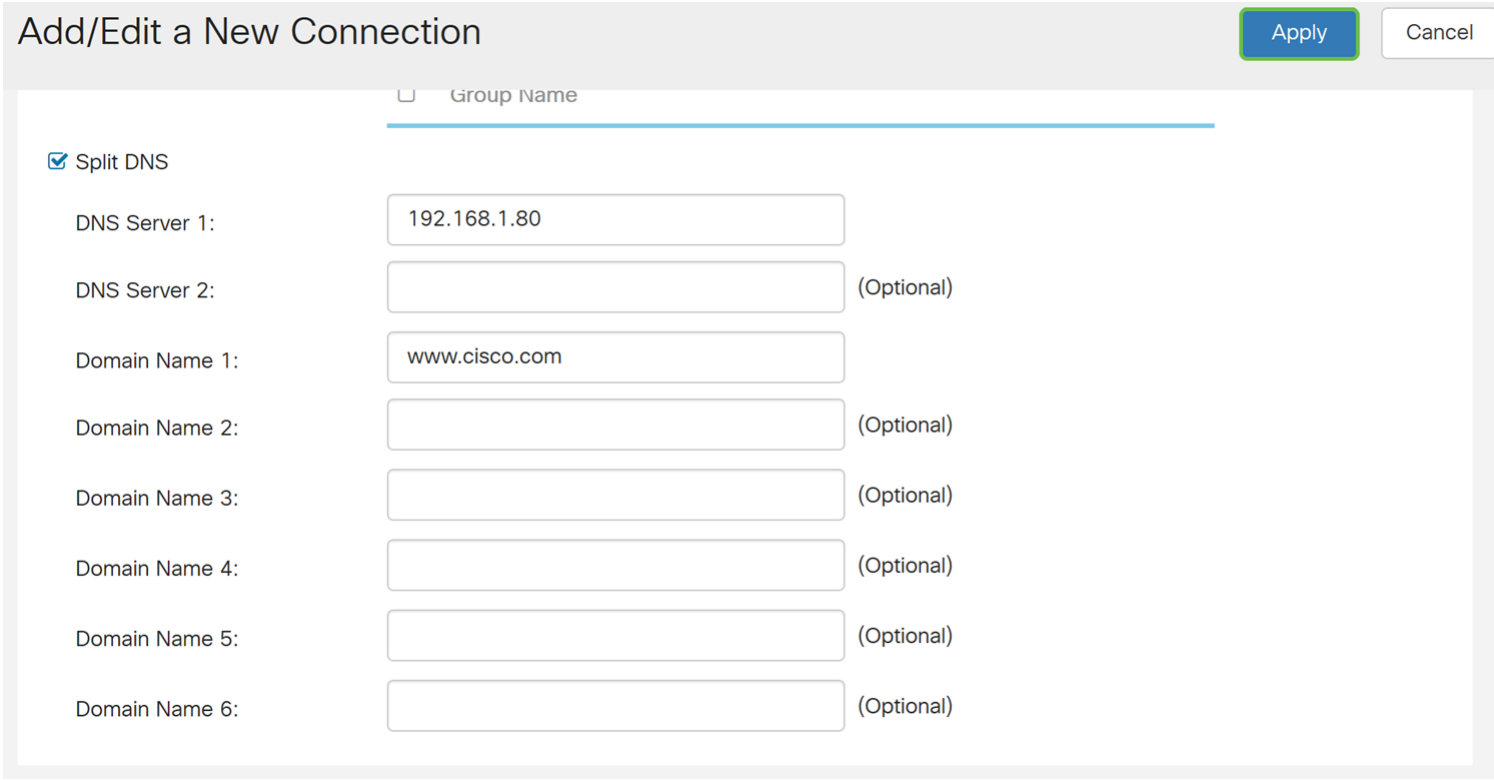
步驟13.選中**Split DNS**以啟用。這會根據指定的域名拆分域名系統(DNS)伺服器和對其他DNS伺服器的其他DNS請求。當路由器收到地址解析請求時，它會檢查域名。如果域名與拆分DNS設定中的域名匹配，則會將請求傳遞到VPN伺服器網路中的指定DNS伺服器。否則，該請求會被傳遞到WAN介面設定中指定的DNS伺服器（即ISP DNS伺服器）。

拆分DNS被分為同一域的兩個區域。一個用於內部網路，另一個用於外部網路。拆分DNS將內部主機定向到內部DNS以進行名稱解析，而外部主機定向到外部DNS以進行名稱解析。

如果您已啟用*Split DNS*，請輸入要用於指定域的DNS伺服器的IP地址。或者，在*DNS Server 2*欄位中指定輔助DNS伺服器。在*域名1-6*中，輸入DNS伺服器的域名。域請求被傳遞到指定的DNS伺服器。

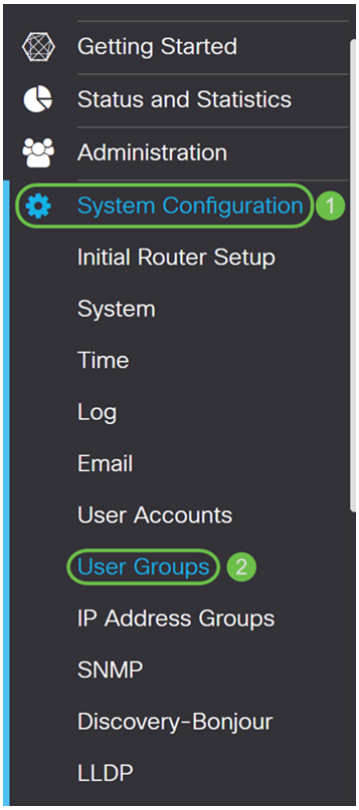


步驟14.按一下**Apply**。

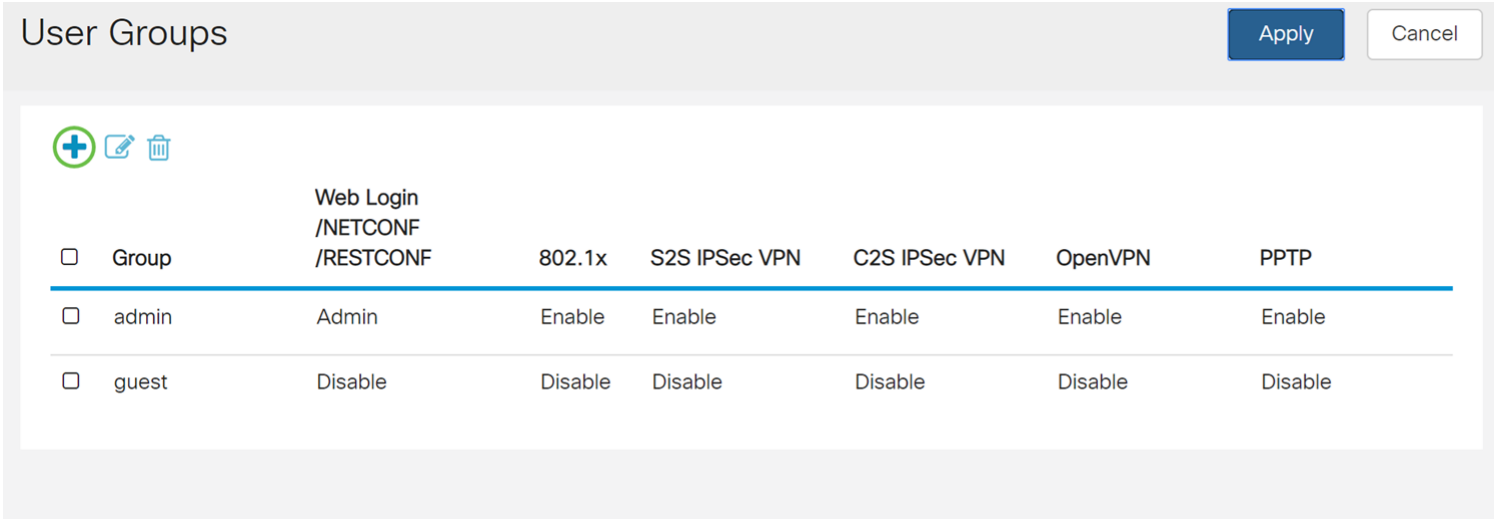


建立使用者組以進行擴展身份驗證

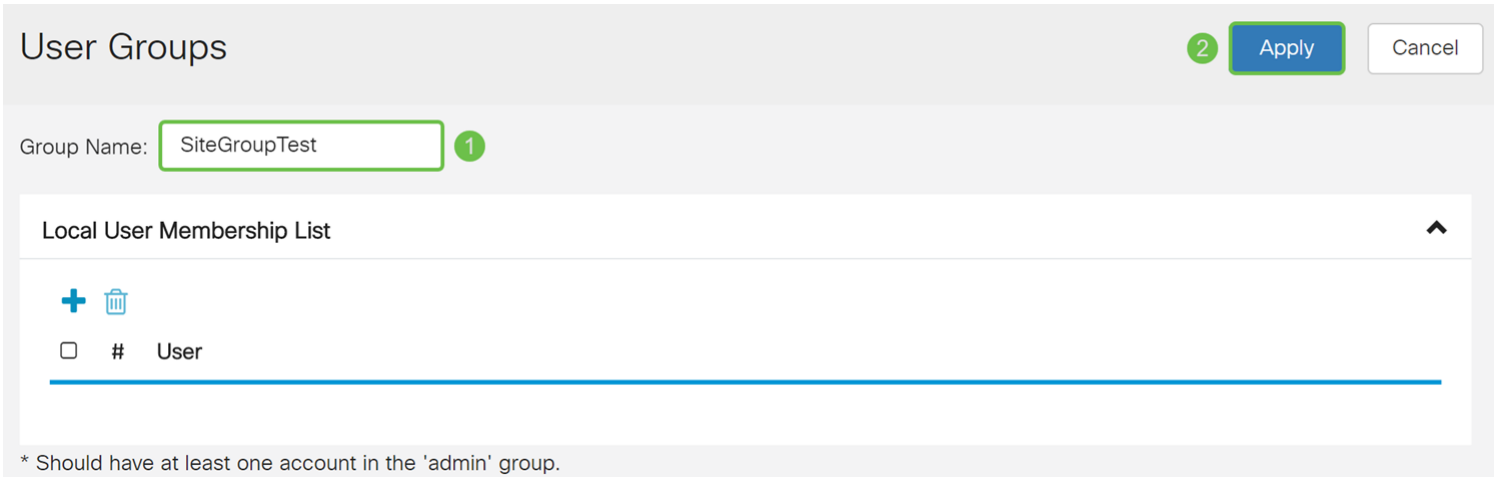
步驟1.導覽至System Configuration > User Groups。



步驟2.按一下plus圖示新增新使用者組。



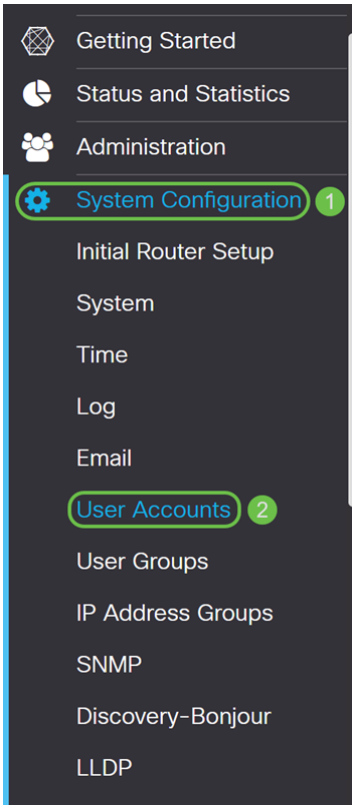
步驟3.在*Group Name*欄位中輸入名稱，然後按**Apply**。在本示例中，輸入了SiteGroupTest作為組名。



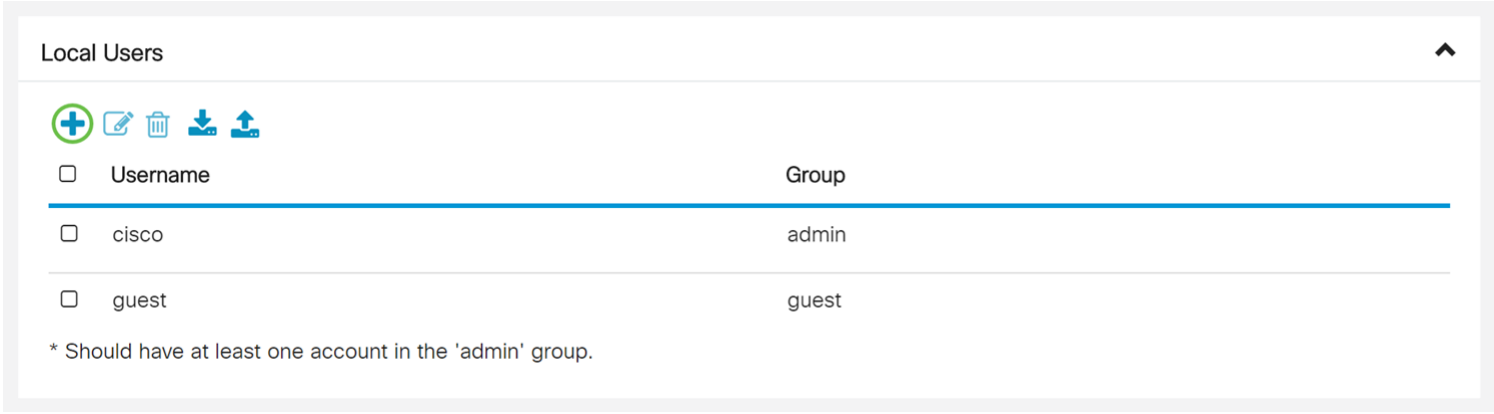
配置擴展身份驗證的使用者帳戶

重要附註：請將預設管理員帳戶保留在管理組中，並為Shrew Soft建立新的使用者帳戶和使用者組。如果將管理員帳戶移動到不同的組，您將阻止自己登入路由器。

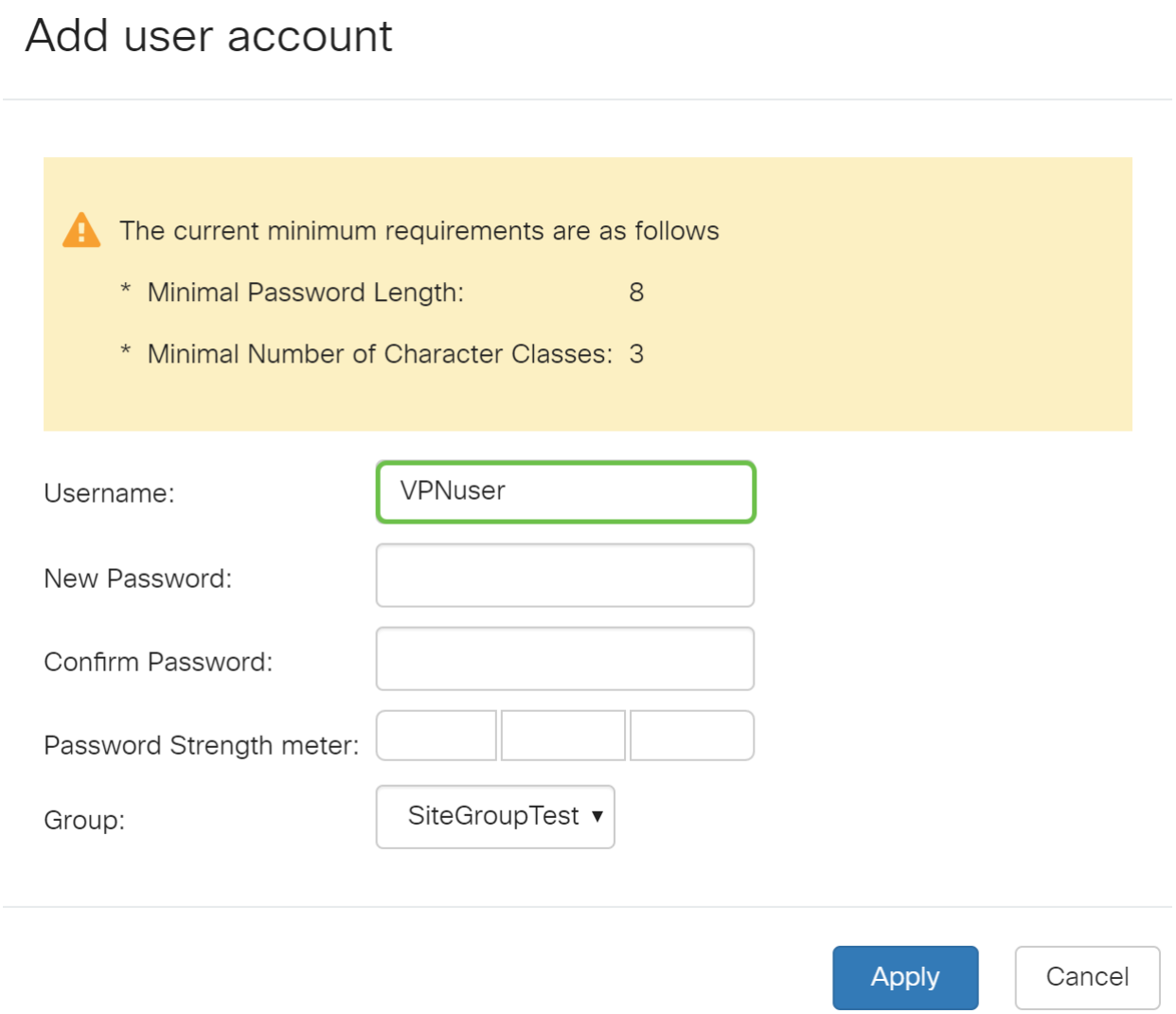
步驟1.導覽至**System Configuration > User Accounts**。



步驟2.向下滾動頁面至*Local Users*。按一下**plus**圖示新增新的本地使用者。

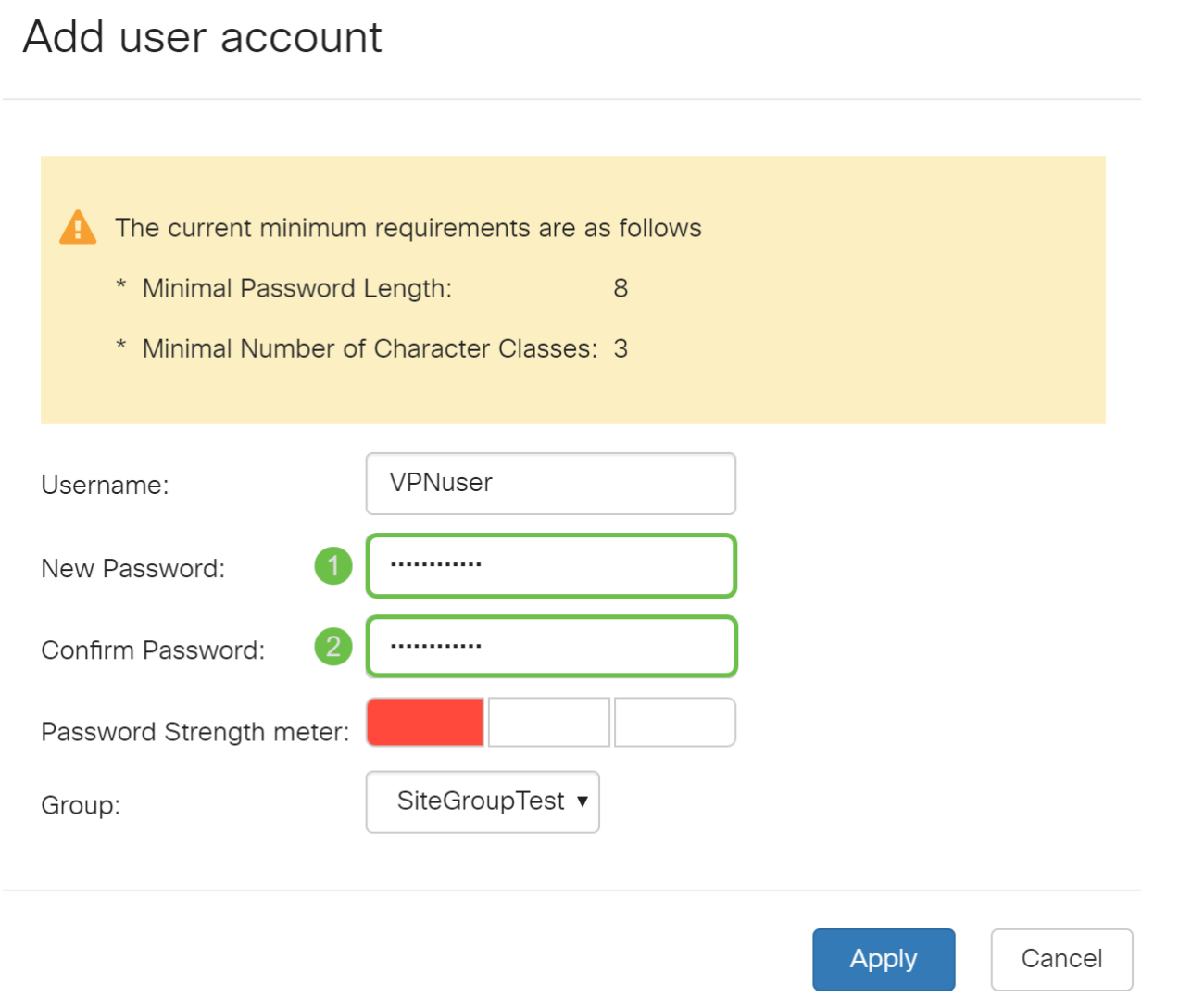


步驟3. *Add user account*頁面隨即開啟。在*Username*欄位中輸入使用者名稱。在此示例中，輸入了VPNuser作為使用者名稱。

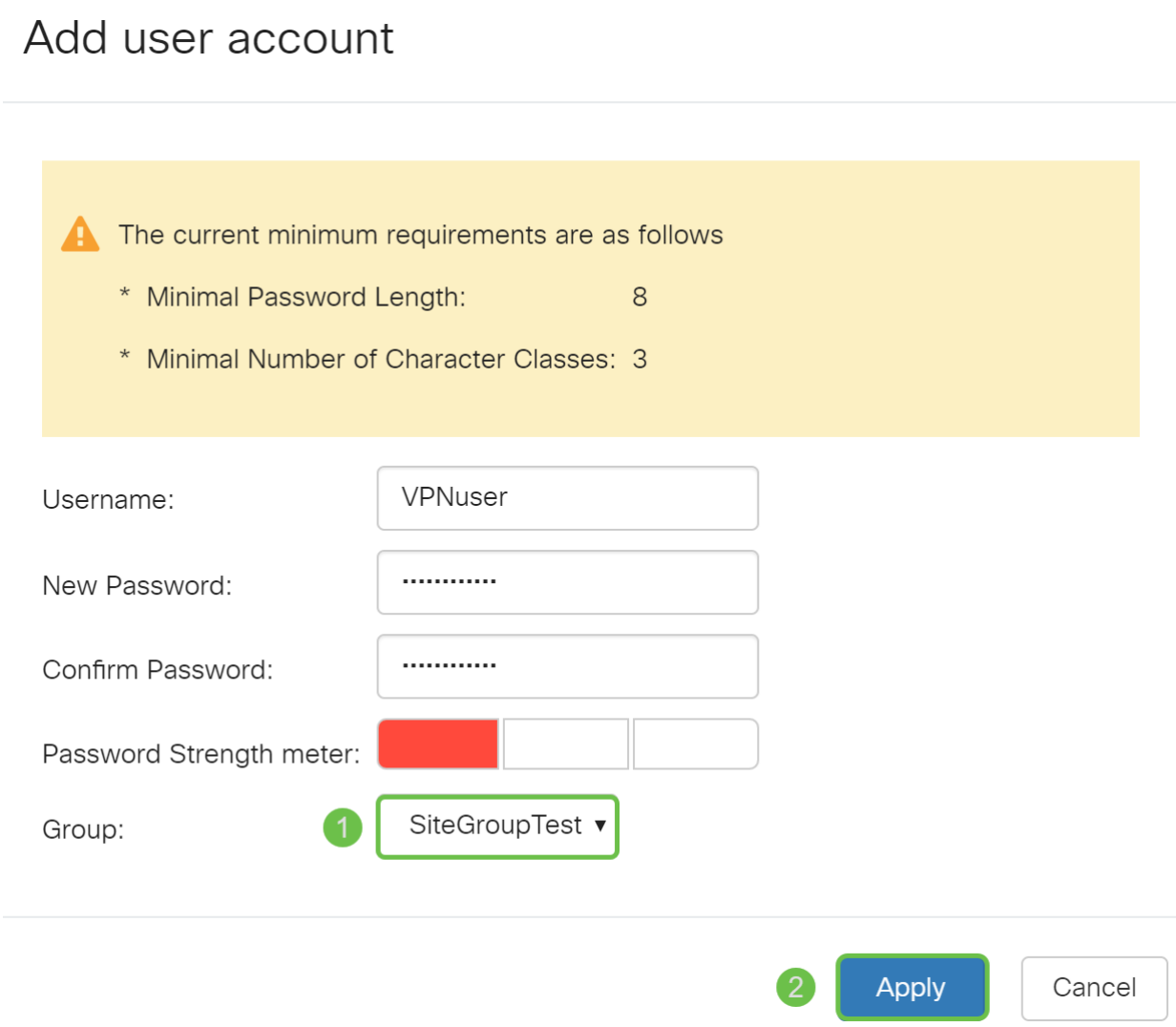


步驟4.在*New Password* 和*Confirm Password* 欄位中輸入密碼。在本例中，CiscoTest123!已輸入。

附註：此密碼用作示例，但建議使用更複雜的密碼。



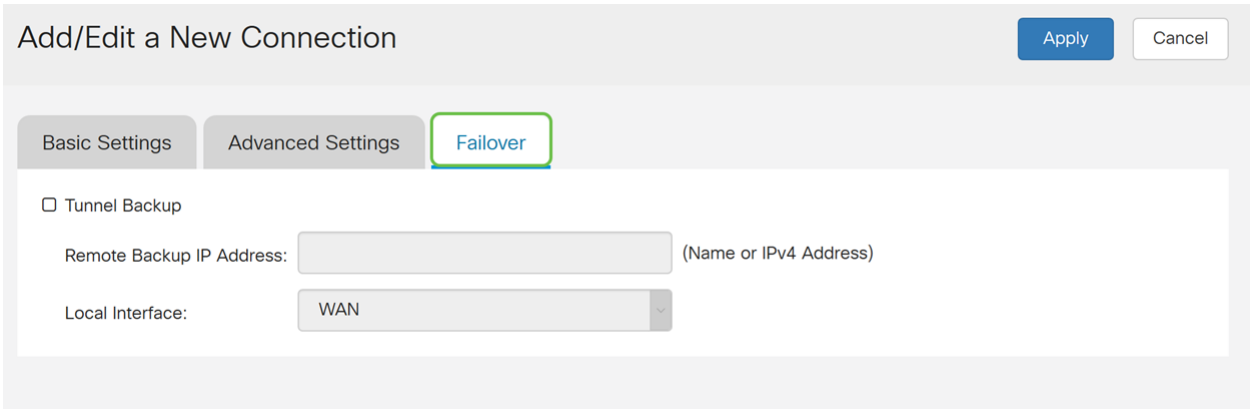
步驟5.選擇組，然後按**Apply**建立新使用者帳戶。在此示例中，選擇了SiteGroupTest作為組。



配置故障轉移

要啟用站點到站點故障切換，必須在*高級設定*頁籤上啟用keep-alive。

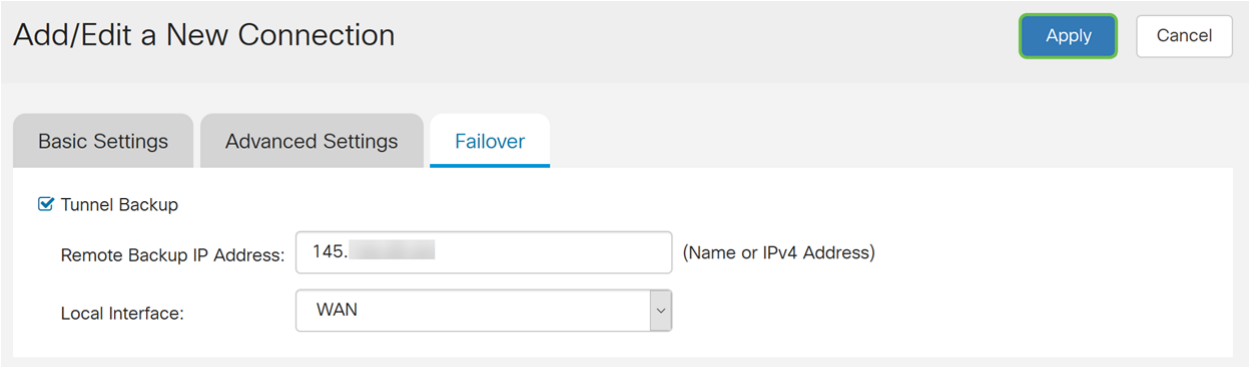
步驟1.按一下**Failover**頁籤配置故障切換。



步驟2.檢查**Tunnel Backup** 以啟用。當主隧道關閉時，此功能允許路由器通過使用遠端對等體的備用IP地址或備用本地WAN來重新建立VPN隧道。此功能僅在啟用DPD時可用。

步驟3.在*Remote Backup IP Address*欄位中，輸入遠端對等體的IP地址，或重新輸入已為遠端網關設定的WAN IP地址。然後從下拉選單中選擇本地介面(**WAN1**、**WAN2**、**USB1**或**USB2**)。

步驟4.按一下**Apply**。



結論

現在，您應該已經成功在RV160和RV260上為站點到站點VPN配置高級設定和故障切換。您的站點到站點VPN仍然應該連線。

檢視與本文相關的影片……

[按一下此處檢視思科的其他技術對話]