在RV160和RV260上配置VPN設定嚮導

本文檔介紹如何在RV160和RV260上配置VPN設定嚮導。

技術不斷發展，業務通常在辦公室之外進行。裝置移動性更強，員工通常在家中或出差時工作。這可能會導致一些安全漏洞。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。

VPN通過網際網路等安全性較低的網路建立加密連線。它確保連線系統的適當安全級別。隧道是作為私有網路建立的，可以通過使用行業標準的加密和身份驗證技術安全地傳送資料，以確保傳送的資料安全。遠端訪問VPN通常依賴網際網路協定安全(IPsec)或安全套接字層(SSL)來保護連線。

VPN提供對目標網路的第2層訪問；這需要跨基本IPsec連線執行的通道通訊協定，例如點對點通道通訊協定(PPTP)或第2層通道通訊協定(L2TP)。IPsec VPN支援網關到網關隧道的站點到站點VPN。例如，使用者可以在分支機構站點配置VPN隧道以連線到公司站點的路由器，以便分支機構站點可以安全地訪問公司網路。IPsec VPN還支援主機到網關隧道的客戶端到伺服器VPN。從家用筆記型電腦/PC通過VPN伺服器連線到公司網路時，客戶端到伺服器VPN非常有用。

RV160系列路由器支援10條隧道，RV260系列路由器支援20條隧道。在為站點到站點IPsec隧道配置安全連線時，VPN設定嚮導會引導使用者。這通過避免複雜和可選引數簡化了配置，因此任何使用者都可以快速高效地設定IPsec隧道。

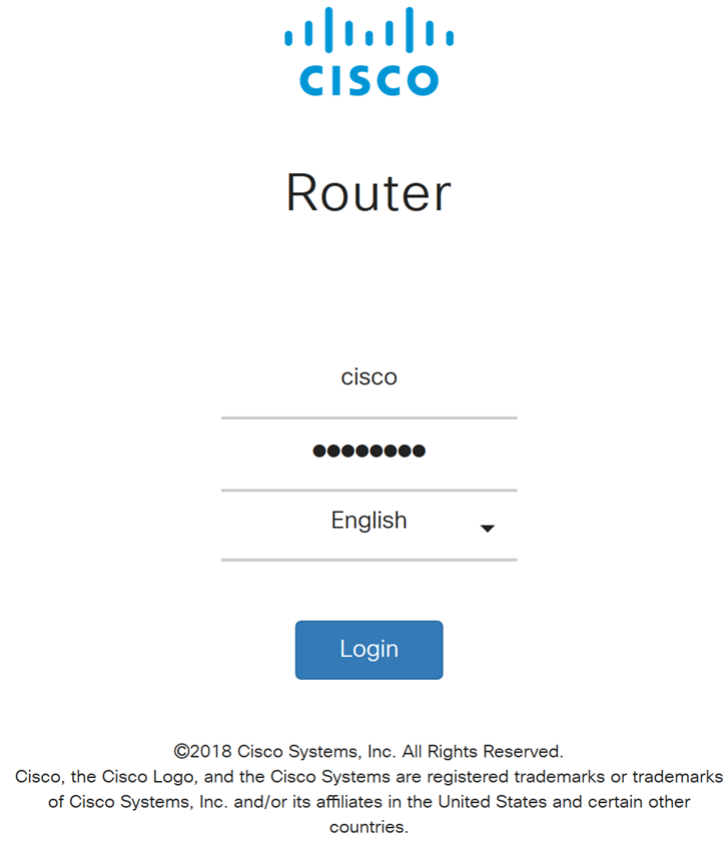
- RV160
- RV260

- 1.0.0.13

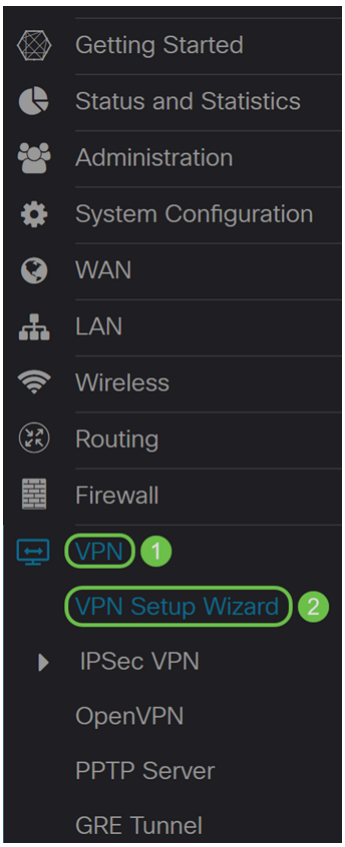
VPN

步驟1.登入到本地路由器上的Web配置頁。

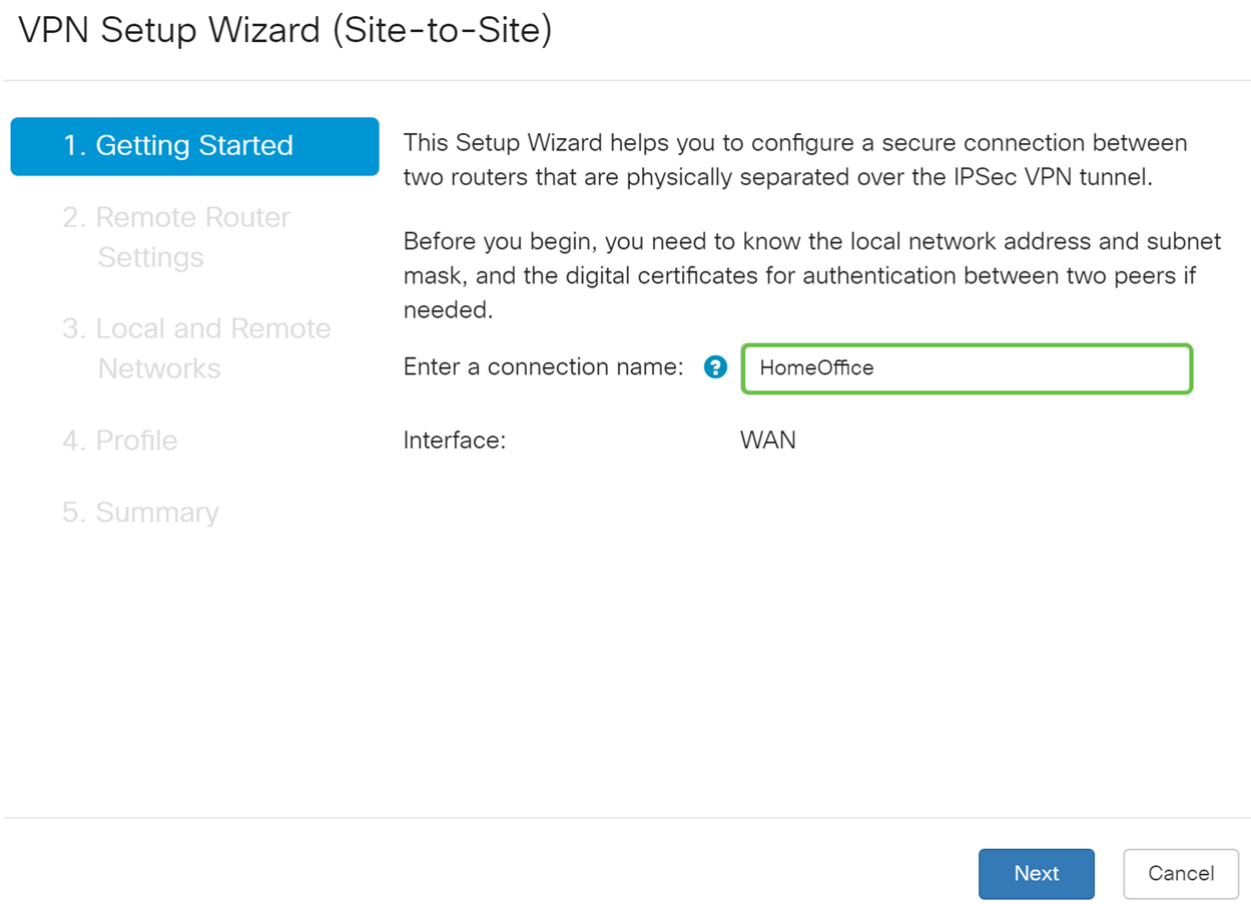
附註：我們將本地路由器稱為路由器A，遠端路由器稱為路由器B。在本文檔中，我們將使用兩個RV160來演示VPN設定嚮導。



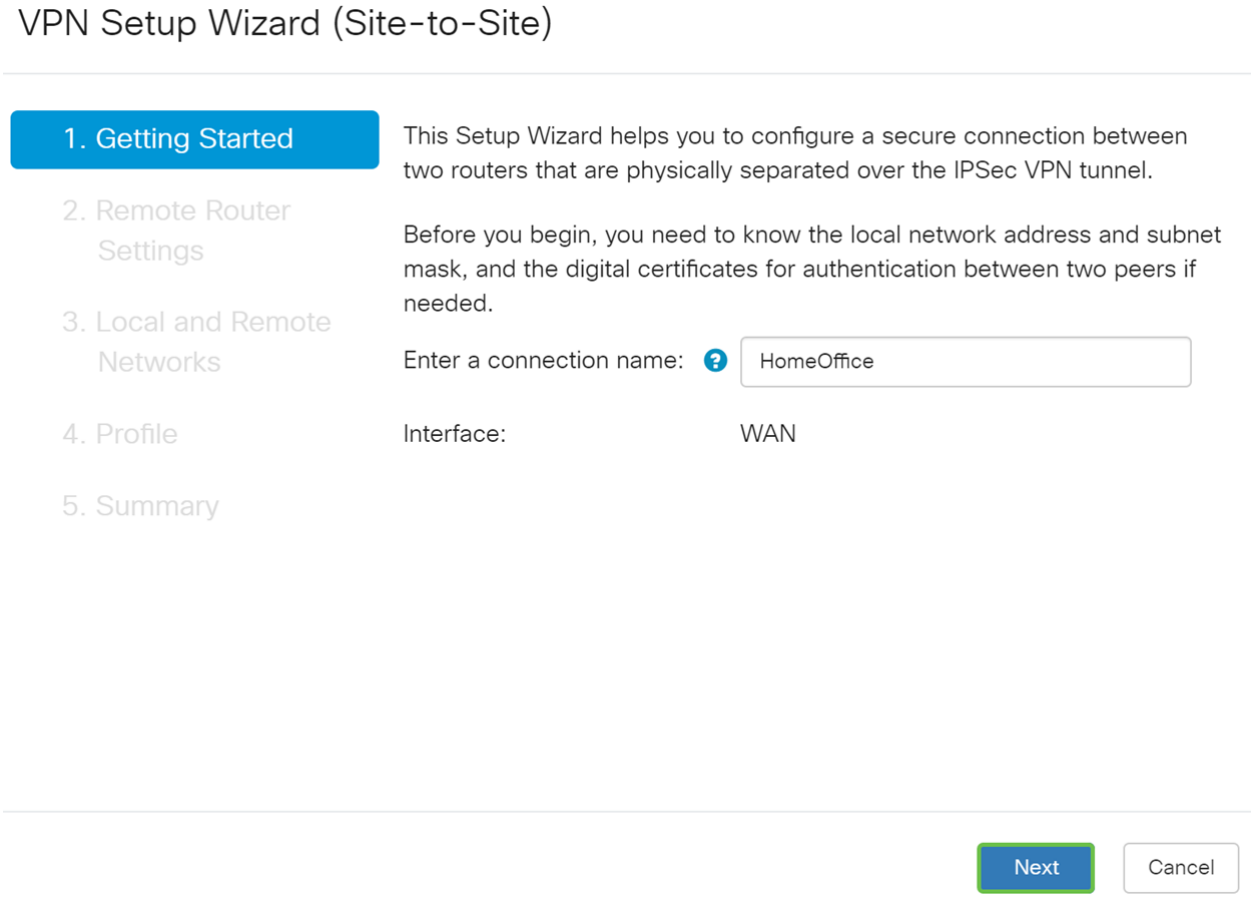
步驟2.導覽至**VPN > VPN Setup Wizard**。



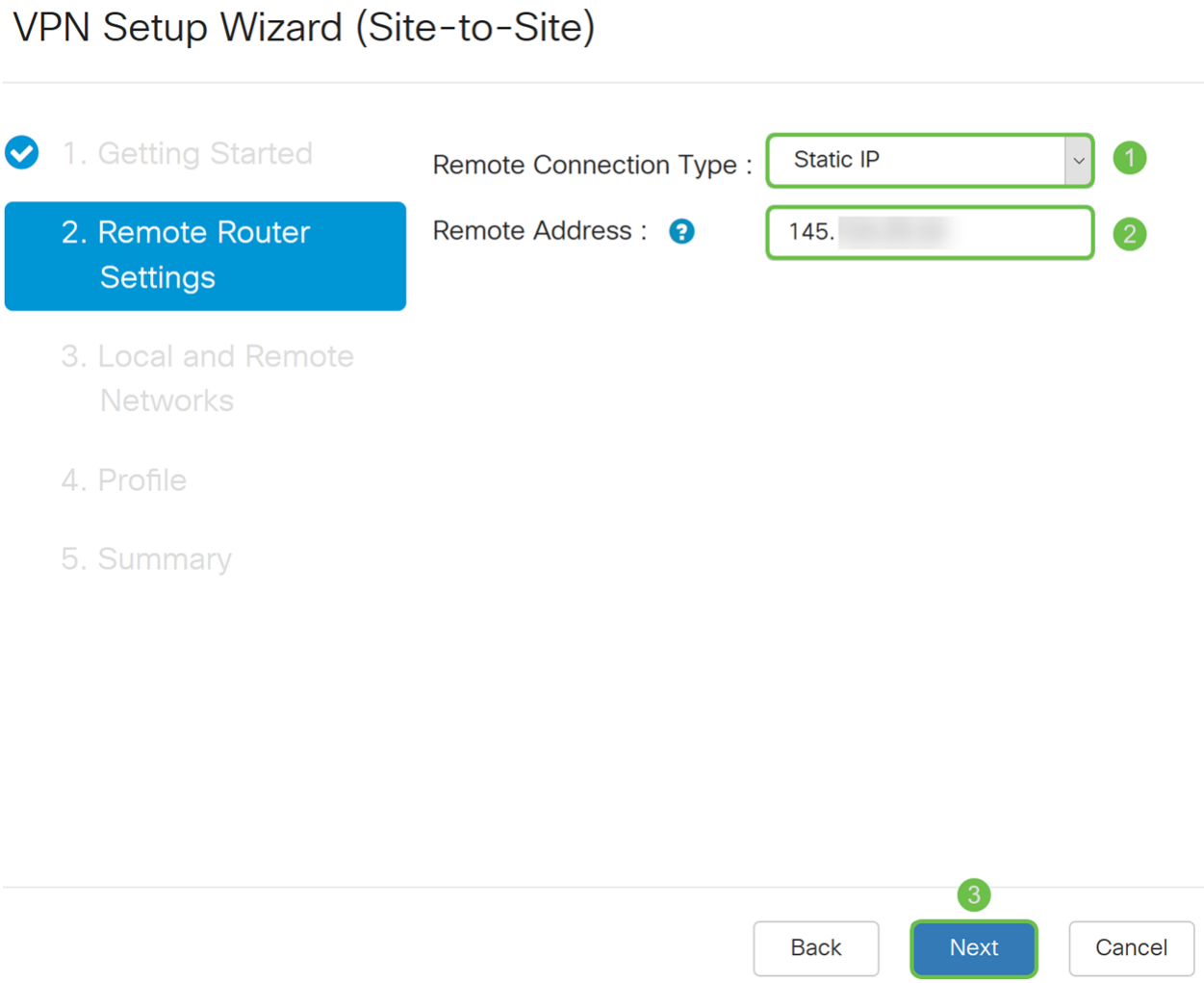
步驟3.在*Getting Started*部分的**Enter a connection name**欄位中輸入連線名稱。我們在**HomeOffice**中輸入了連線名稱。



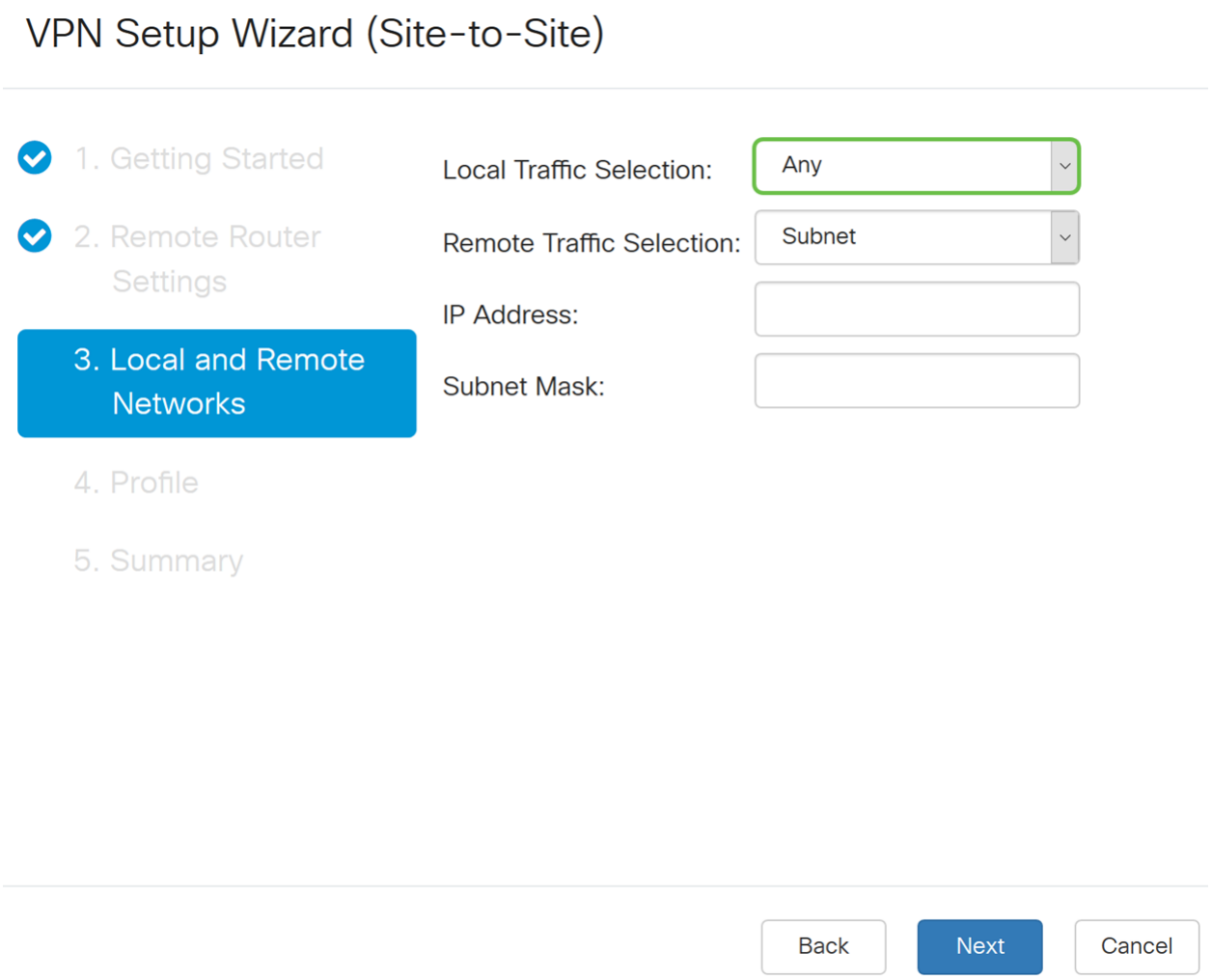
步驟4.如果您使用的是RV260，請在「*Interface*」欄位中選擇一個介面。RV160隻有WAN連結，因此您將無法從下拉式清單中選擇一個介面。按一下**下一步**以轉到*遠端路由器設定*部分。



步驟5.從下拉選單中選擇*Remote Connection Type*。選擇**靜態IP**或**FQDN**（完全限定域名），然後在*遠端地址*欄位中輸入要連線的網關的WAN IP地址或FQDN。在本示例中，選擇了**Static IP**，並輸入了遠端路由器WAN IP地址（路由器B）。然後按一下**Next**移動到下一部分。

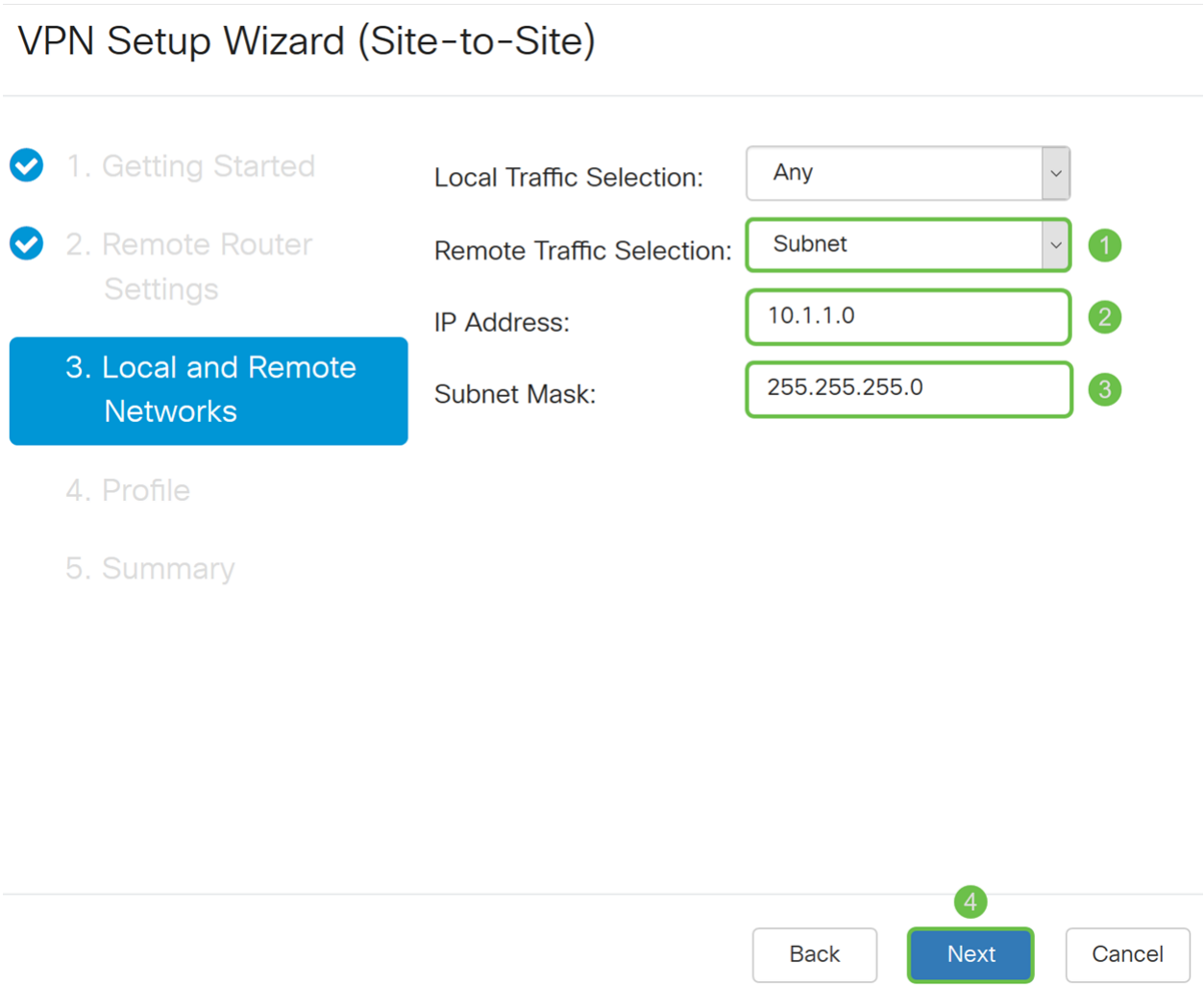


步驟6.在*Local and Remote Network*部分的*Local Traffic Selection*下，從下拉選單中選擇本地IP(**Subnet**、**Single**或*Any*)。如果選擇**Subnet**，請輸入子網IP地址和子網掩碼。如果選擇**Single**，請輸入IP地址。如果選擇**Any**，請轉到下一步以配置*Remote Traffic Selection*。

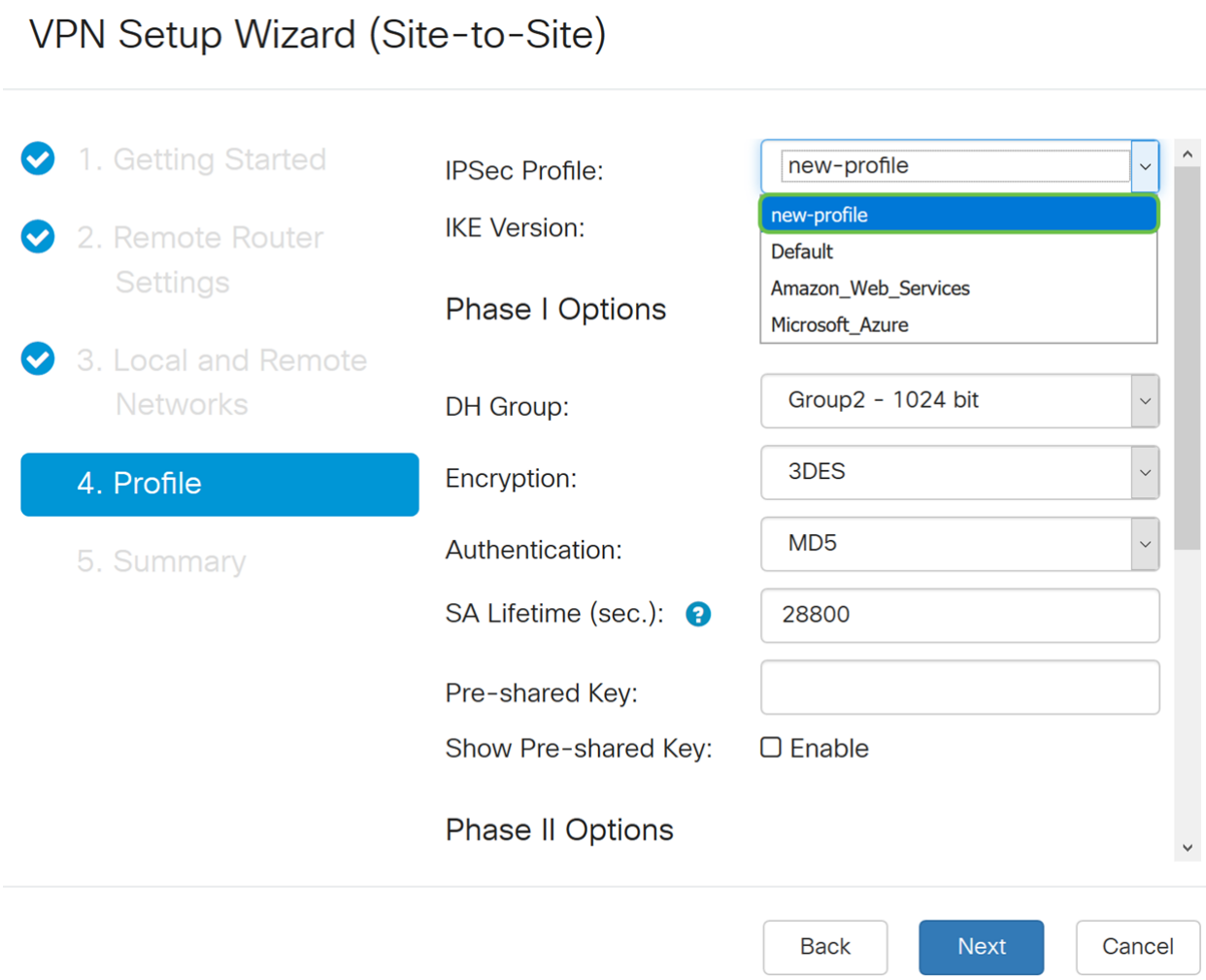


步驟7.在*Remote Traffic Selection*中，從下拉選單中選擇*Remote IP*(**Subnet**、Single或**Any**)。如果選擇**Subnet**，請輸入遠端路由器（路由器B）的子網IP地址和子網掩碼。 如果選擇**Single**，請輸入IP地址。然後按一下**Next**配置*Profile*部分。

附註：如果為*Local Traffic Selection*選擇了Any，則必須為Remote Traffic Selection選擇**Subnet** 或Single。

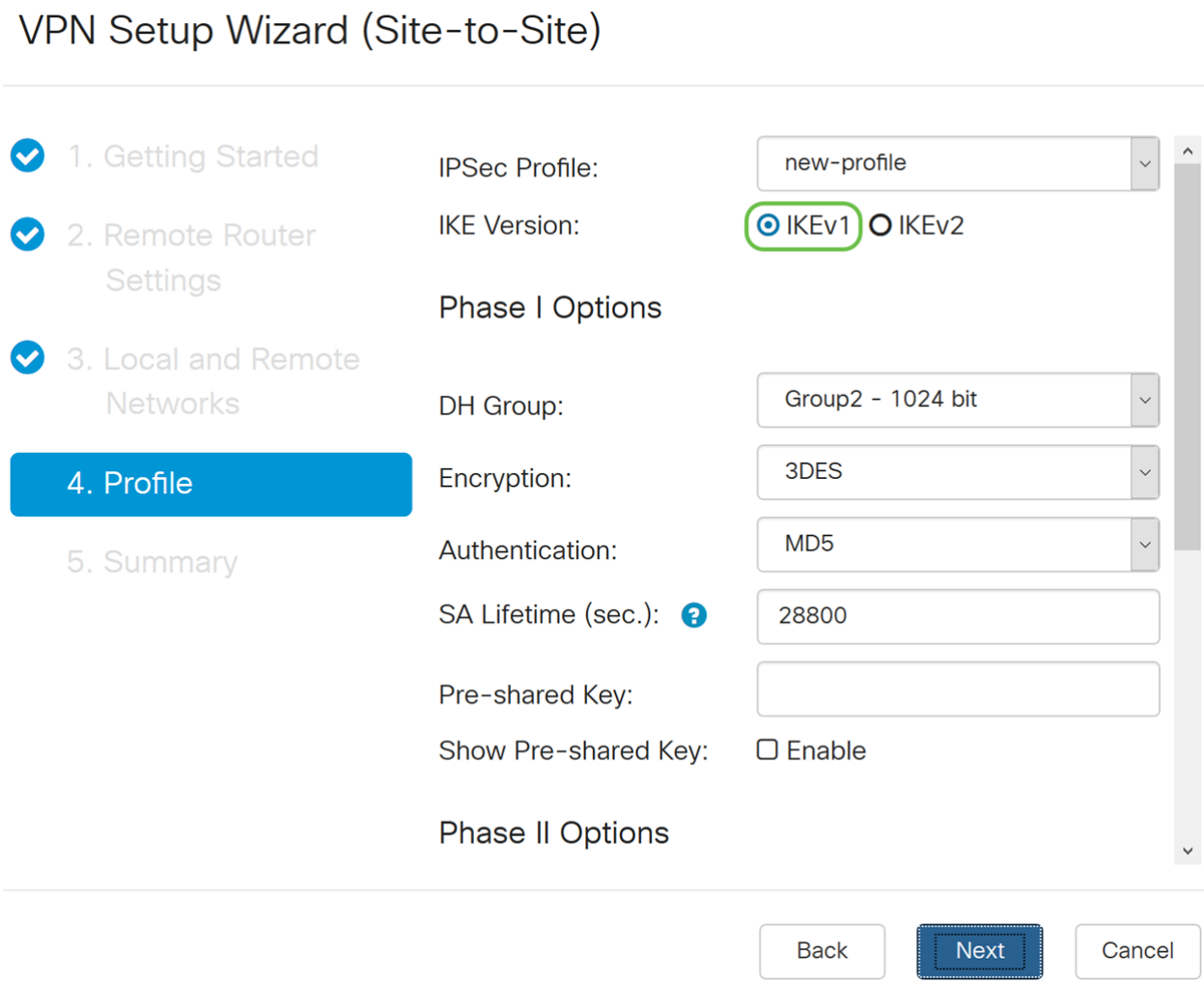


步驟8.在*Profile*部分，從下拉選單中選擇IPsec配置檔案的名稱。在本演示中，選擇了**new-profile**作為IPsec配置檔案。



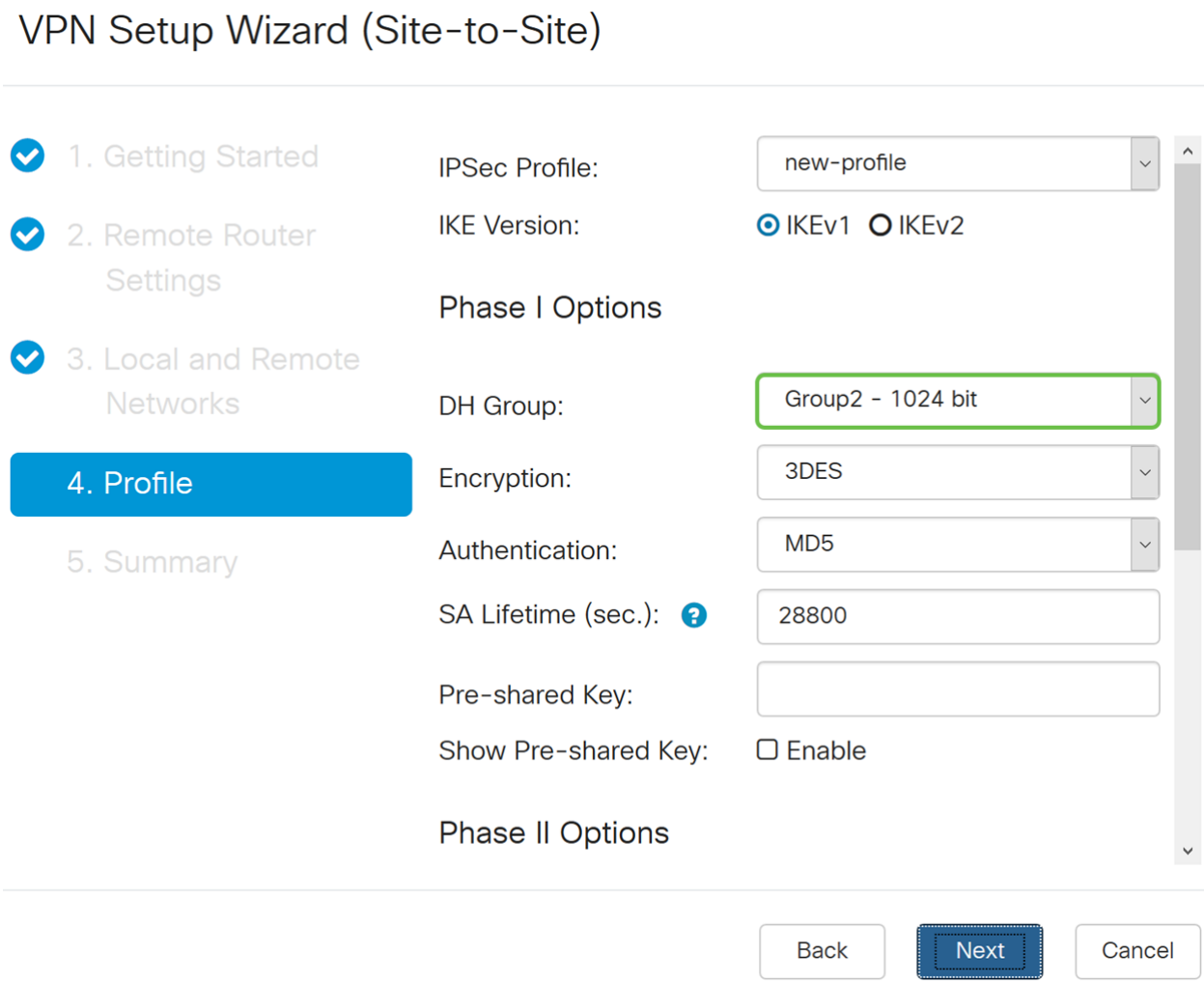
步驟9.選擇**IKEv1**（Internet金鑰交換版本1）或**IKEv2**（Internet金鑰交換版本2）作為*IKE版本*。IKE是在Internet安全關聯和金鑰管理協定(ISAKMP)框架中實現Oakley金鑰交換和Skeme金鑰交換的混合協定。IKE提供IPsec對等體的身份驗證、協商IPsec金鑰和協商IPsec安全關聯。IKEv2效率更高，因為它執行金鑰交換所需的資料包更少，並且支援更多的身份驗證選項，而IKEv1僅執行共用金鑰和基於證書的身份驗證。在本示例中，選擇**IKEv1**作為我們的IKE版本。

附註：如果您的裝置支援IKEv2，則建議使用IKEv2。如果您的裝置不支援IKEv2，則使用IKEv1。路由器（本地和遠端）都需要使用相同的IKE版本和安全設定。



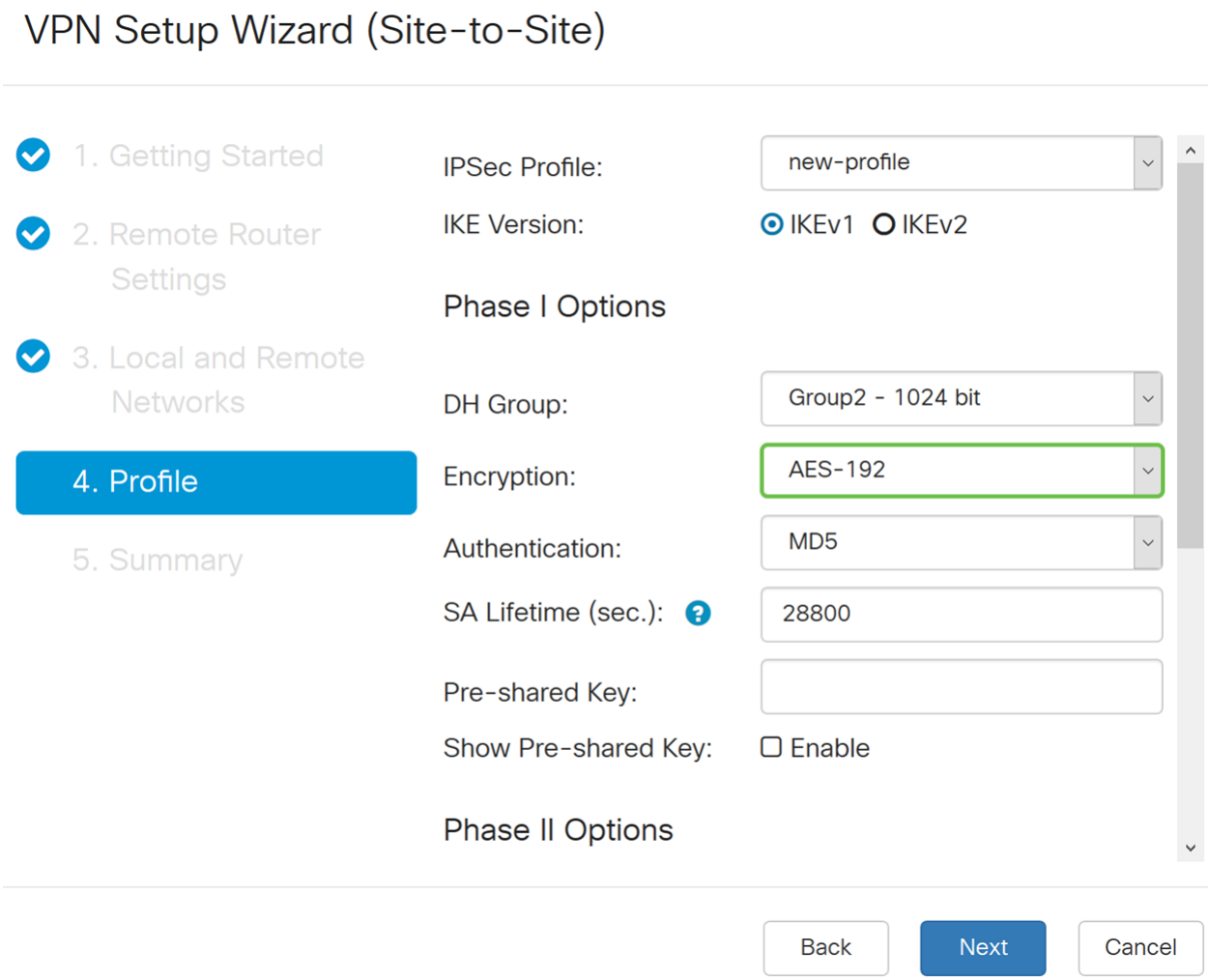
步驟10.在「*Phase 1 Options*」區段中，從下拉選單中選擇DH(Diffie-Hellman)組(**Group 2 - 1024 bit** 或**Group 5 - 1536 bit**)。DH是金鑰交換協定，具有兩組不同主金鑰長度：組2最多有1,024位，組5最多有1,536位。在本演示中，**我們將使用Group 2** - 1024位。

附註：要獲得更快的速度和更低的安全性，請選擇「組2」。要獲得更慢的速度和更高的安全性，請選擇「組5」。預設情況下會選擇「組2」。

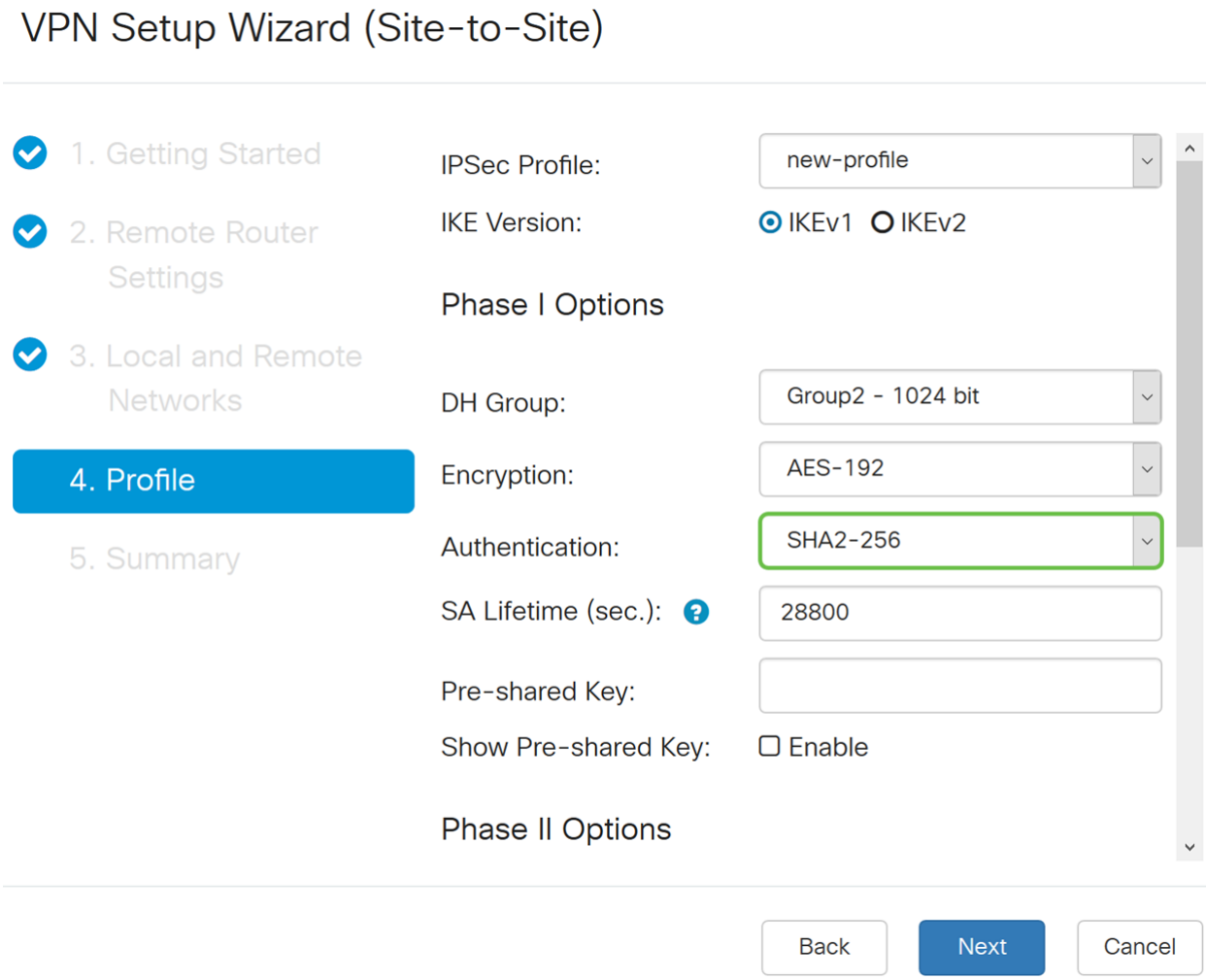


步驟11.從下拉選單中選擇加密選項(**3DES、AES-128、AES-192**或**AES-256**)。此方法確定用於加密或解密封裝安全負載(ESP)/Internet安全關聯和金鑰管理協定(ISAKMP)資料包的演算法。三重資料加密標準(3DES)使用DES加密三次，但現在是傳統演算法。這意味著只有當沒有更好的替代方法時才應該使用它，因為它仍提供邊緣但可接受的安全級別。使用者應僅在需要向後相容性時才使用它，因為它容易受到某些「塊衝突」攻擊。高級加密標準(AES)是一種加密演算法，旨在比DES更安全。AES使用較大的金鑰大小，確保唯一已知解密消息的方法是讓入侵者嘗試所有可能的金鑰。建議使用AES而不是3DES。在本例中，我們將使用**AES-192**作為加密選項。

附註：以下是一些可能有幫助的其他資源：使用IPSec和下一代加密配置VPN安全。

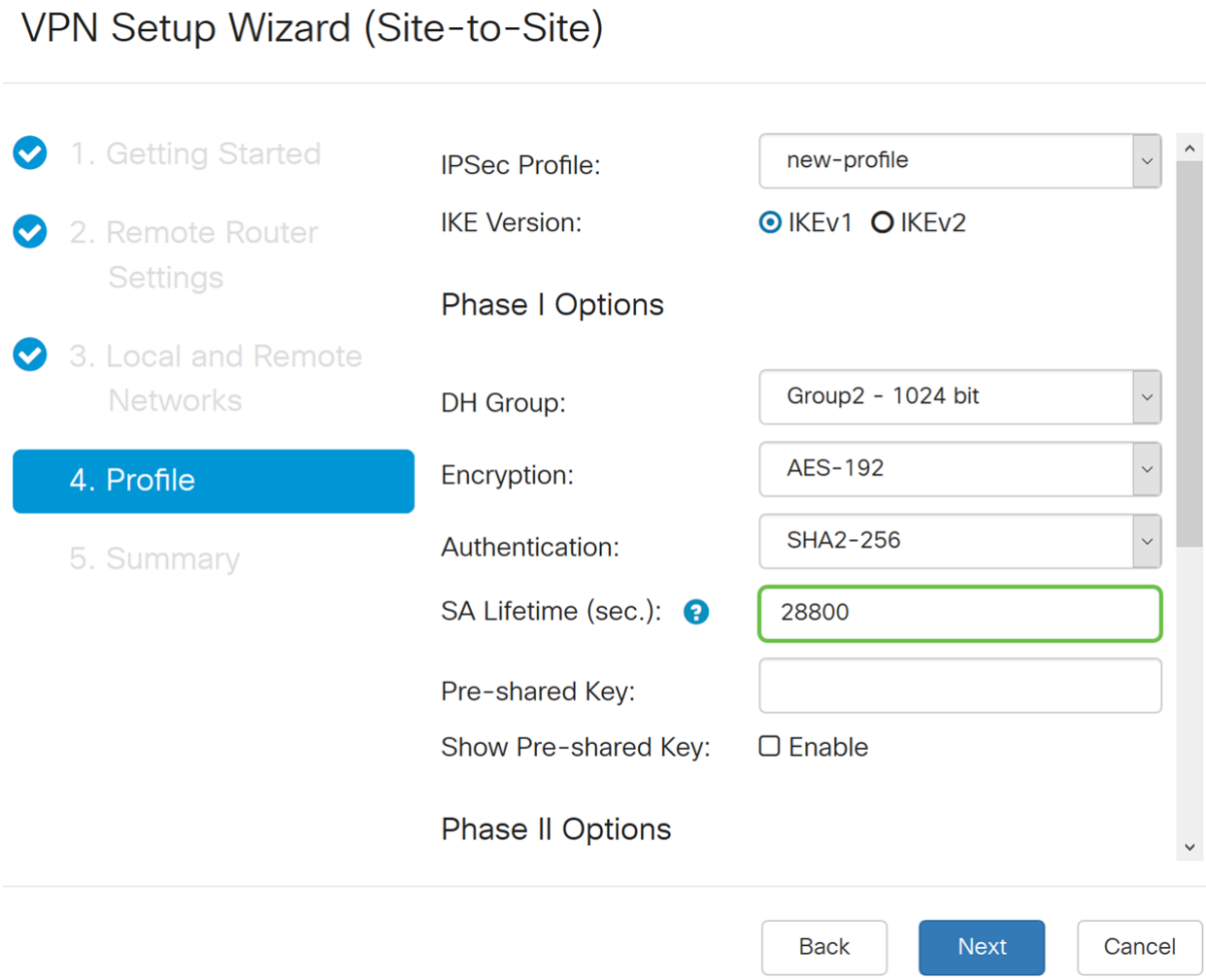


步驟12.驗證方法決定如何驗證封裝安全負載通訊協定(ESP)標頭封包。MD5是產生128位摘要的單向雜湊演算法。SHA1是產生160位摘要的單向雜湊演算法，而SHA2-256產生256位摘要。建議使用SHA2-256，因為它更安全。確保VPN隧道的兩端使用相同的身份驗證方法。選擇驗證**(MD5、SHA1或SHA2-256)**。**本示例選**擇了SHA2-256。



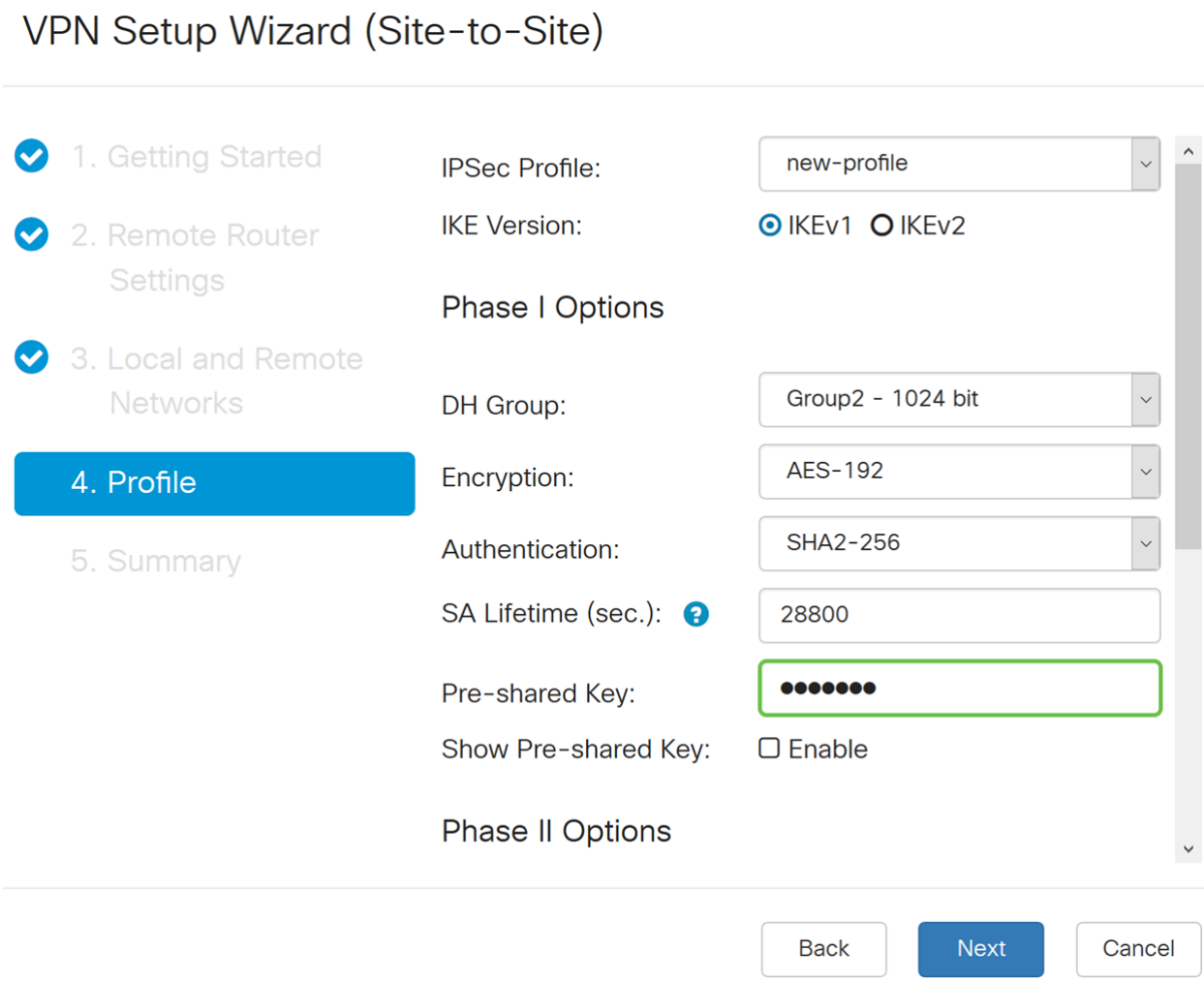
步驟13. *SA Lifetime(Sec)*告訴您在此階段中IKE SA處於活動狀態的時間量（以秒為單位）。在生存期到期之前協商新的安全關聯(SA)，以確保在舊的SA到期時可以使用新的SA。預設值為28800，範圍為120到86400。我們將使用預設值**28800**秒作為階段I的SA生存期。

附註：建議您在階段I的SA生存時間長於階段II SA生存時間。如果您使第I階段比第II階段短，那麼您將不得不頻繁地來回重新協商隧道，而不是資料隧道。資料隧道需要更高的安全性，因此最好在II階段具有比I階段更短的生存期。



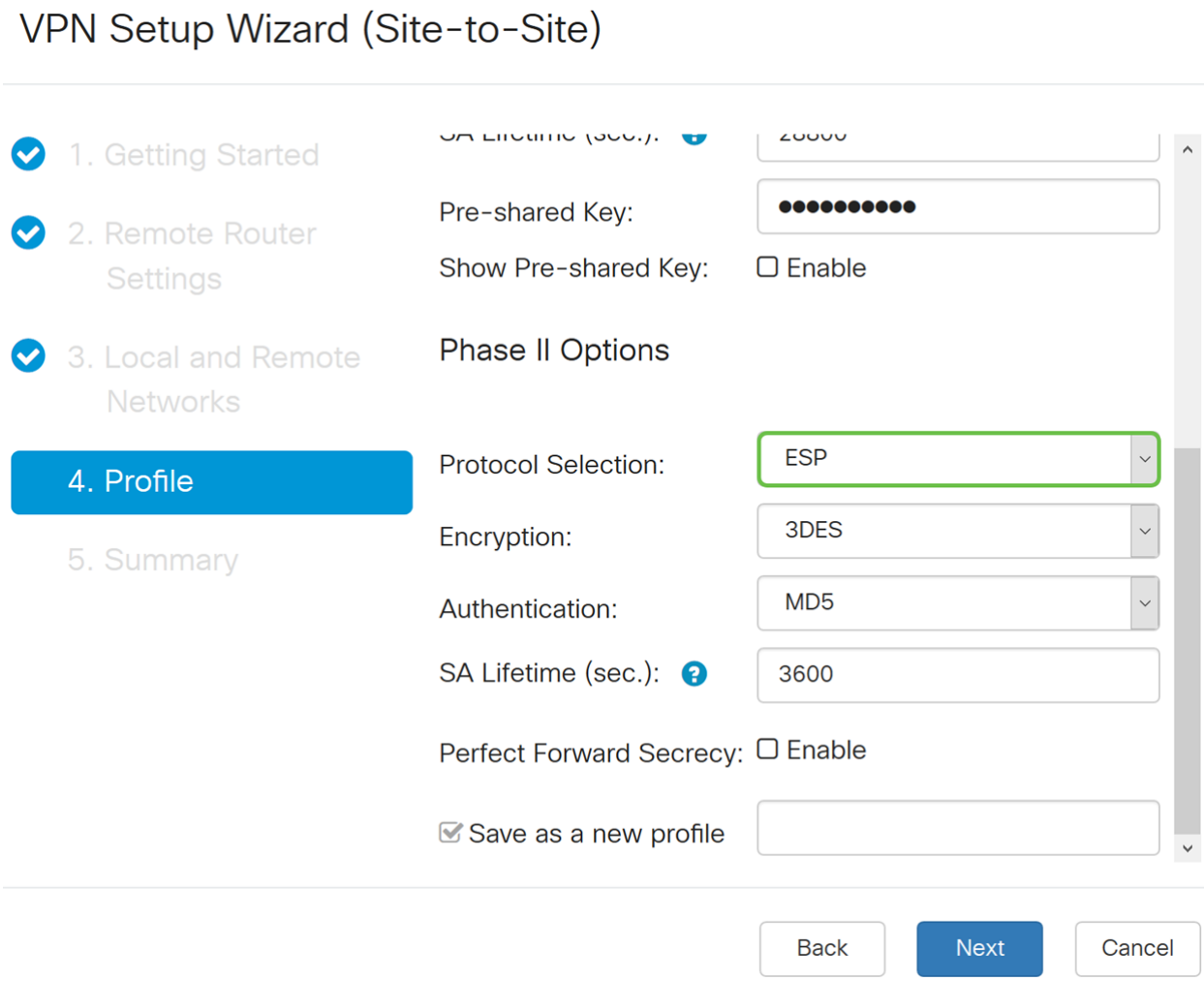
步驟14.輸入**Pre-shared Key**以用於對遠端IKE對等體進行身份驗證。最多可輸入30個鍵盤字元或十六進位制值，如My_@123或4d795f40313233。VPN隧道的兩端必須使用相同的預共用金鑰。

附註：我們建議您定期更改預共用金鑰以最大化VPN安全性。



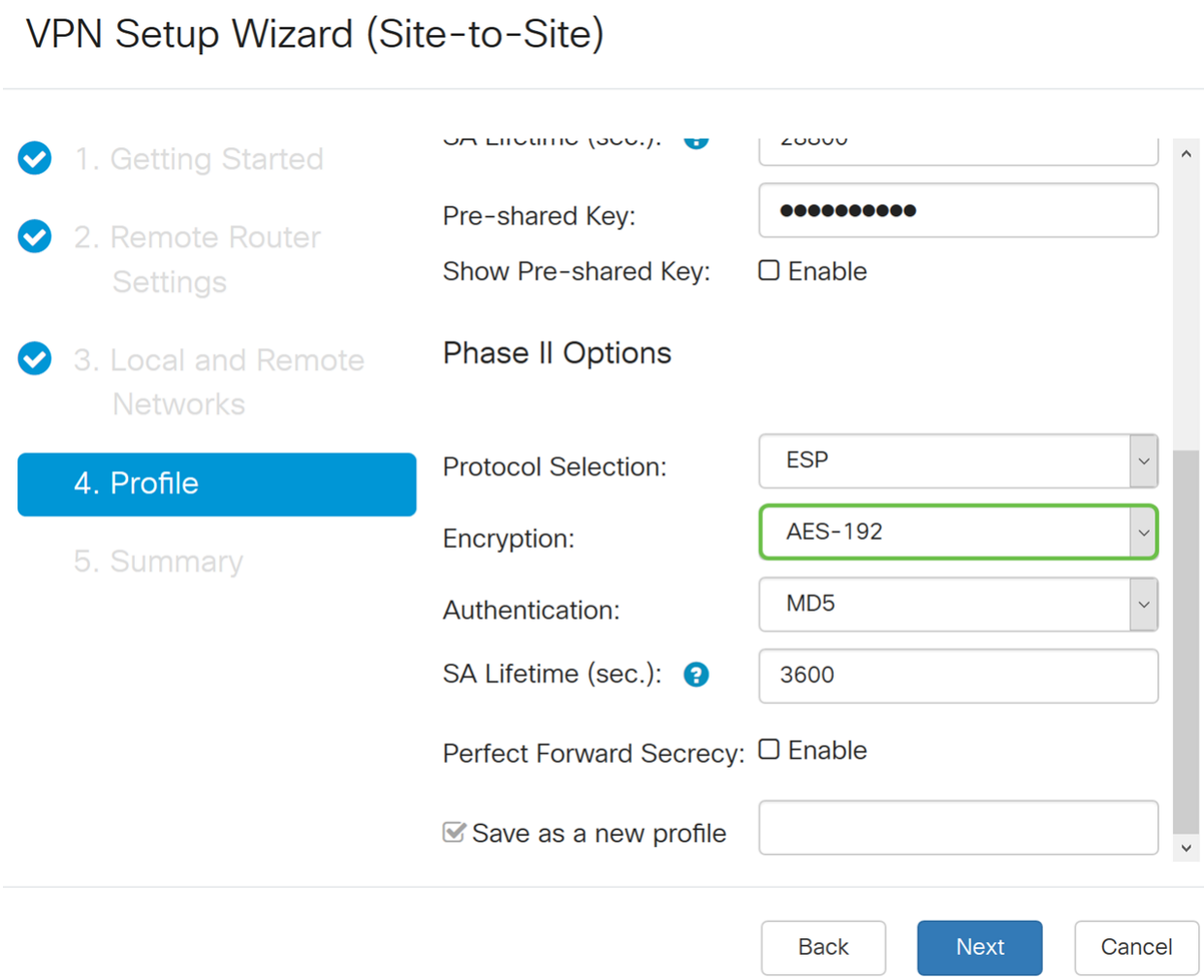
步驟15.在*Phase II Options*部分，從下拉選單中選擇協定。

- **ESP** — 選擇用於資料加密的ESP並輸入加密。
- **啊** — 如果資料不是機密資料，但必須經過身份驗證，則選擇此項以確保資料完整性。

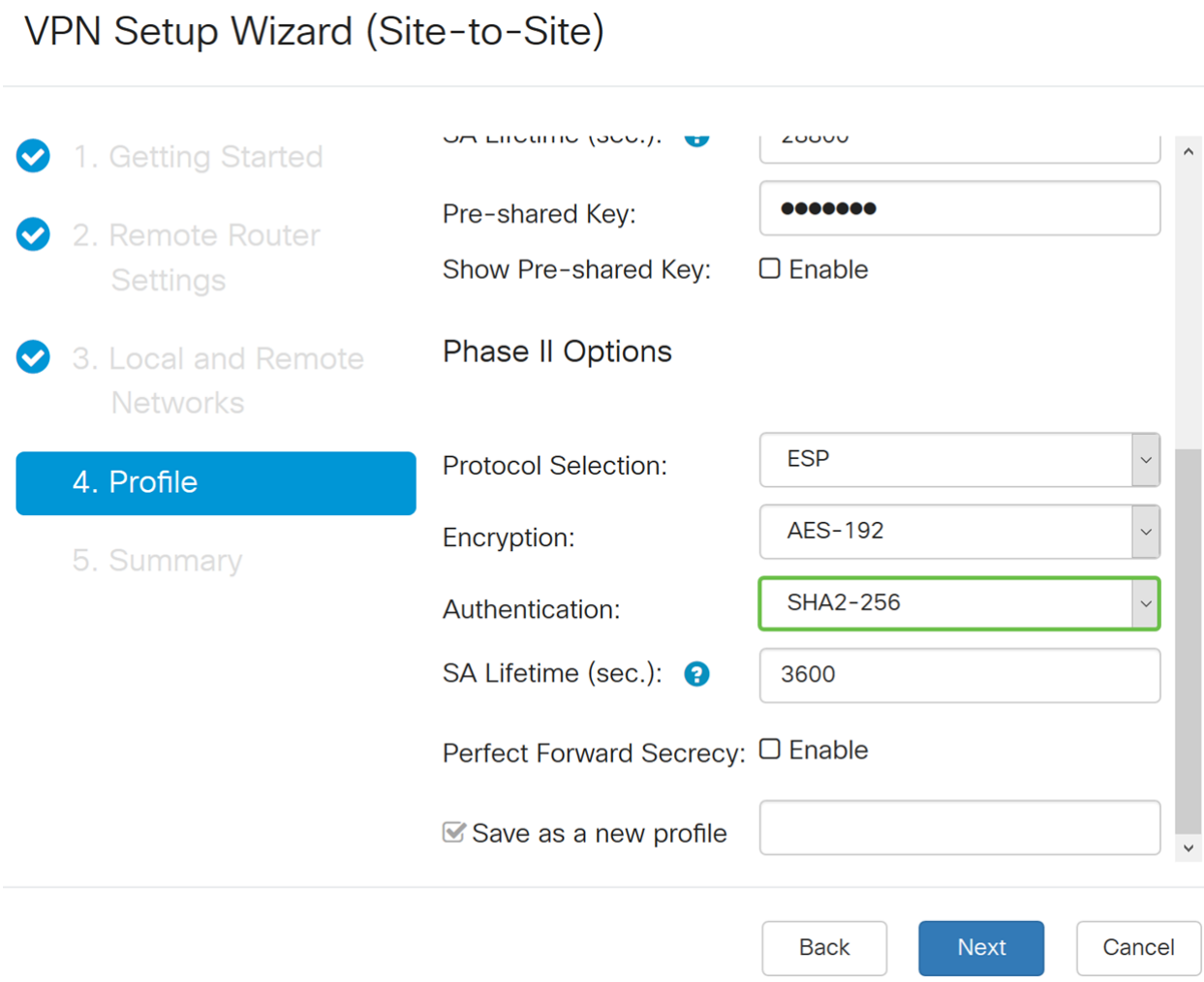


步驟16.從下拉選單中選擇加密選項(**3DES、AES-128、AES-192**或**AES-256**)。此方法確定用於加密或解密封裝安全負載(ESP)/Internet安全關聯和金鑰管理協定(ISAKMP)資料包的演算法。三重資料加密標準(3DES)使用DES加密三次，但現在是傳統演算法。這意味著只有當沒有更好的替代方法時才應該使用它，因為它仍提供邊緣但可接受的安全級別。使用者應僅在需要向後相容性時才使用它，因為它容易受到某些「塊衝突」攻擊。高級加密標準(AES)是一種加密演算法，旨在比DES更安全。AES使用較大的金鑰大小，確保唯一已知解密消息的方法是讓入侵者嘗試所有可能的金鑰。建議使用AES而不是3DES。在本例中，我們將使用**AES-192**作為加密選項。

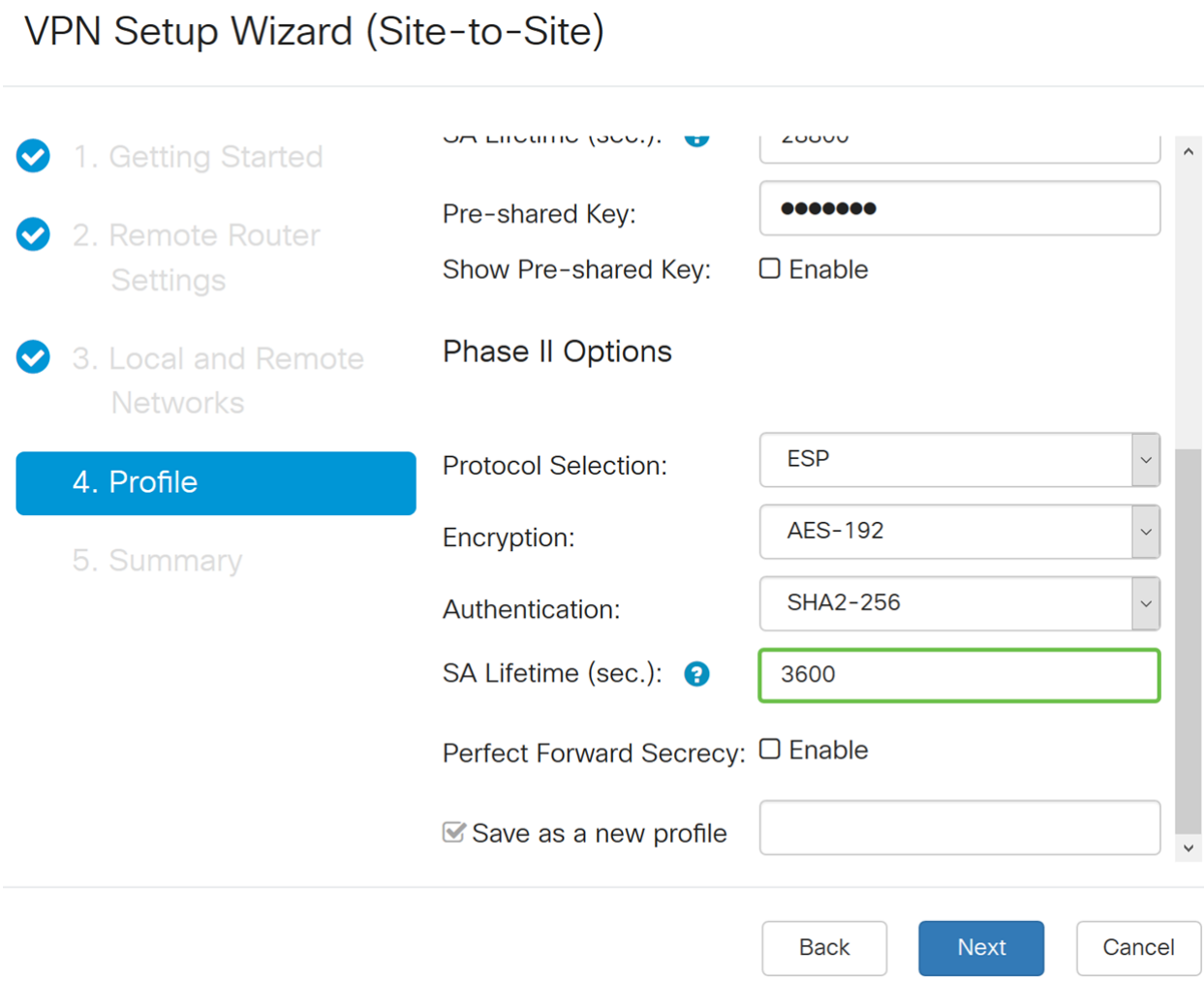
附註：以下是一些可能有幫助的其他資源：使用IPSec和下一代加密配置VPN安全。



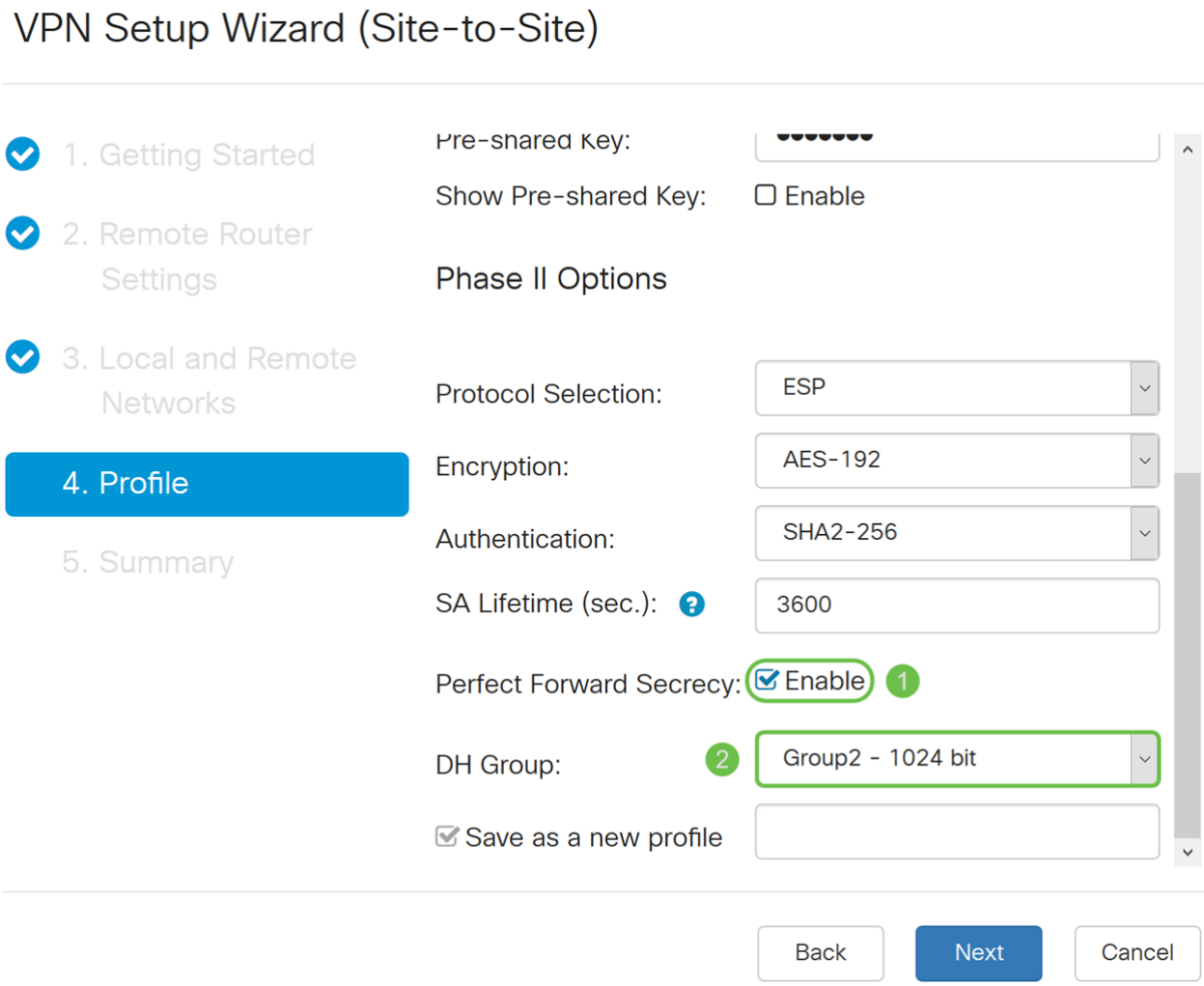
步驟17.驗證方法確定如何驗證封裝安全負載協定(ESP)報頭資料包。MD5是產生128位摘要的單向雜湊演算法。SHA1是產生160位摘要的單向雜湊演算法，而SHA2-256產生256位摘要。建議使用SHA2-256，因為它更安全。確保VPN隧道的兩端使用相同的身份驗證方法。選擇驗證**(MD5、SHA1或SHA2-256)。本示例選擇了**SHA2-256。



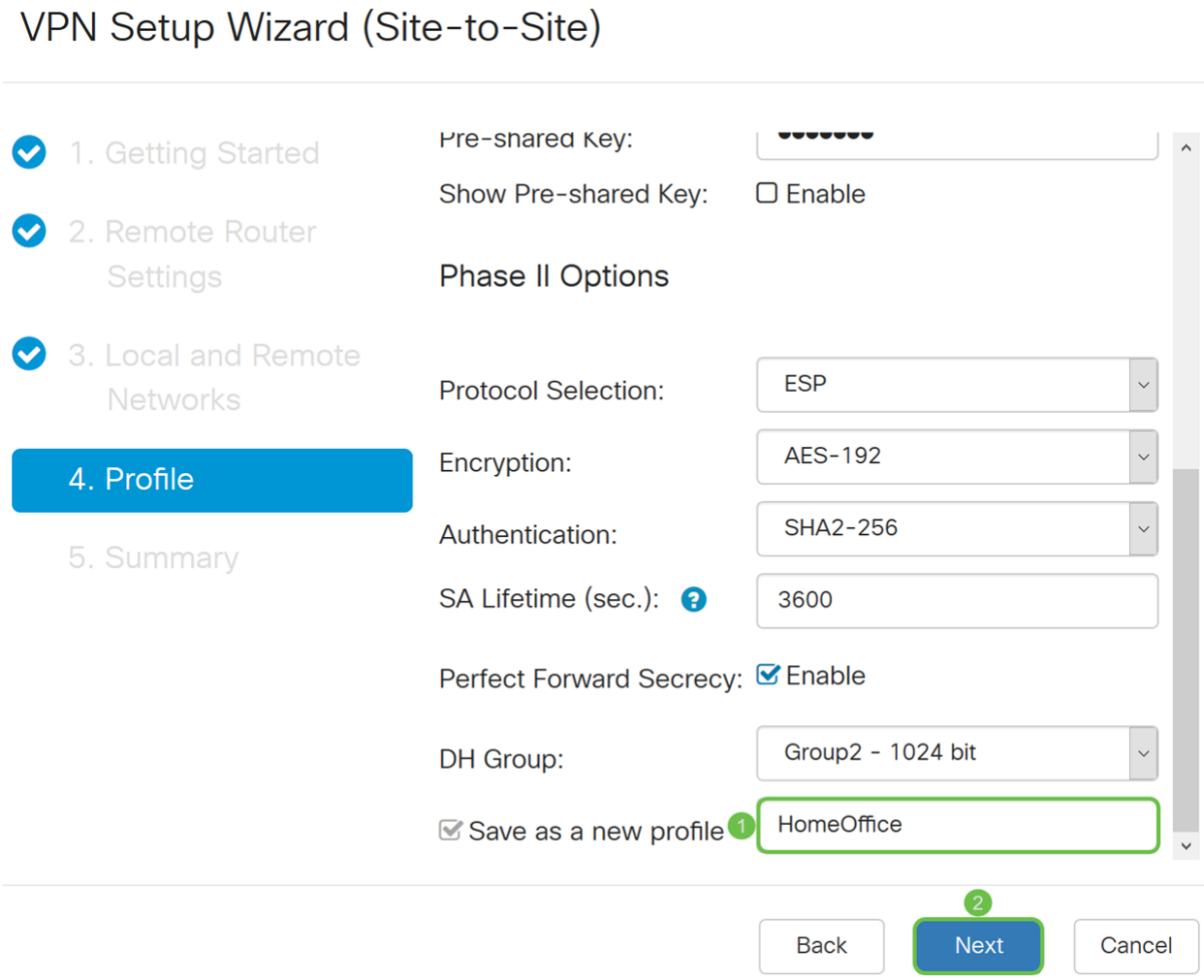
步驟18.輸入*SA Lifetime(Sec)*，即VPN隧道(IPsec SA)在此階段中處於活動狀態的時間量（秒）。階段2的預設值為3600秒。



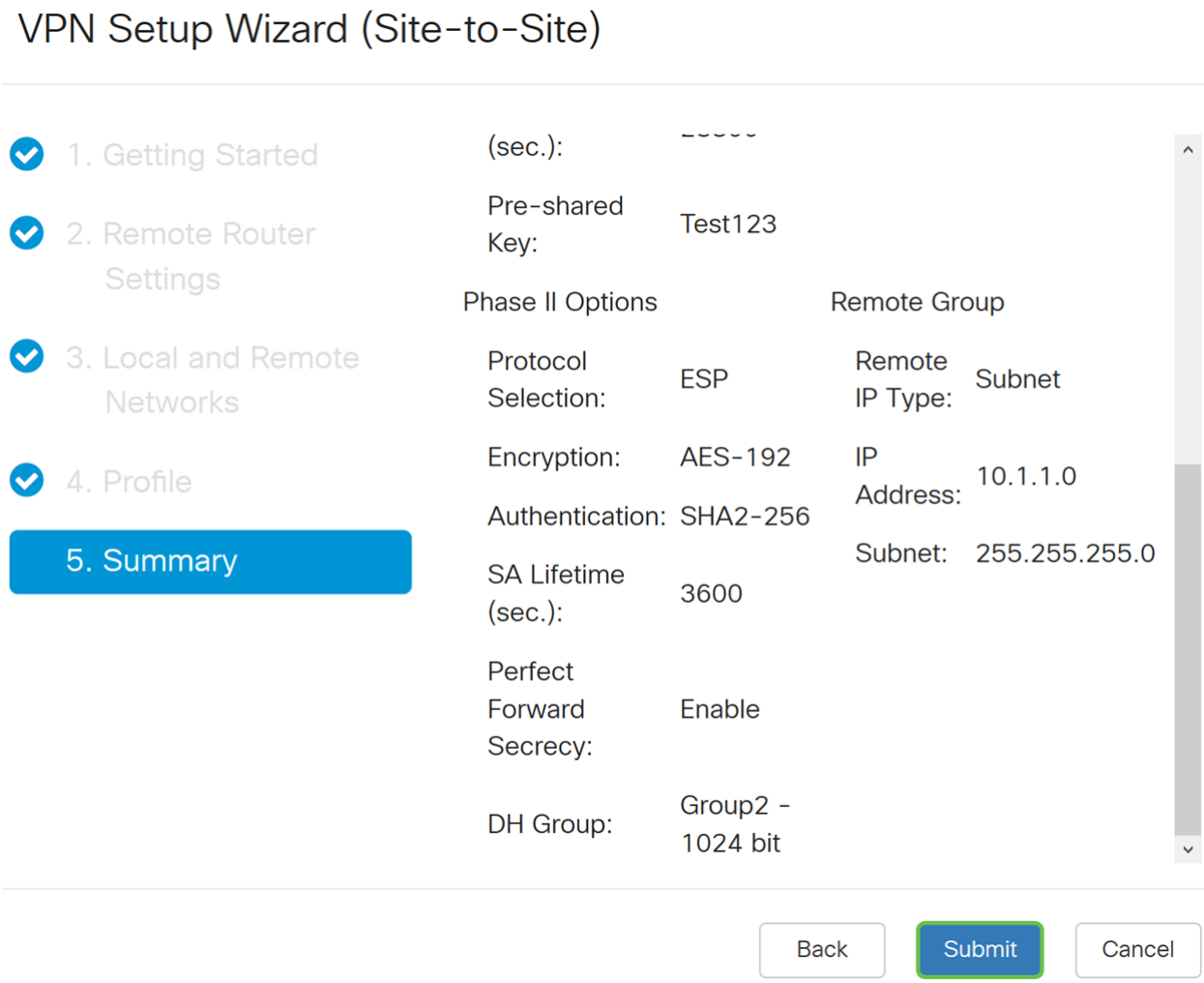
步驟19.啟用完全轉發保密(PFS)時，IKE第2階段協商會生成用於IPsec流量加密和身份驗證的新金鑰材料。完全轉發保密技術用於使用公鑰密碼技術提高通過網際網路傳輸的通訊的安全性。選中此框以啟用此功能，或取消選中此框以禁用此功能。建議使用此功能。如果選中，請選擇*DH組*。在本示例**中使用Group2 -** 1024位。



步驟20.在*另存為新配置檔案*中，為剛建立的新配置檔案輸入名稱。按一下**下一步**檢視VPN配置的摘要。



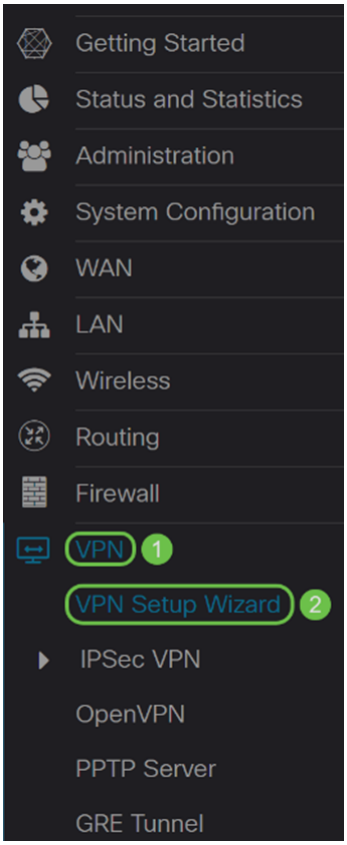
步驟21.驗證資訊，然後按一下**Submit**。



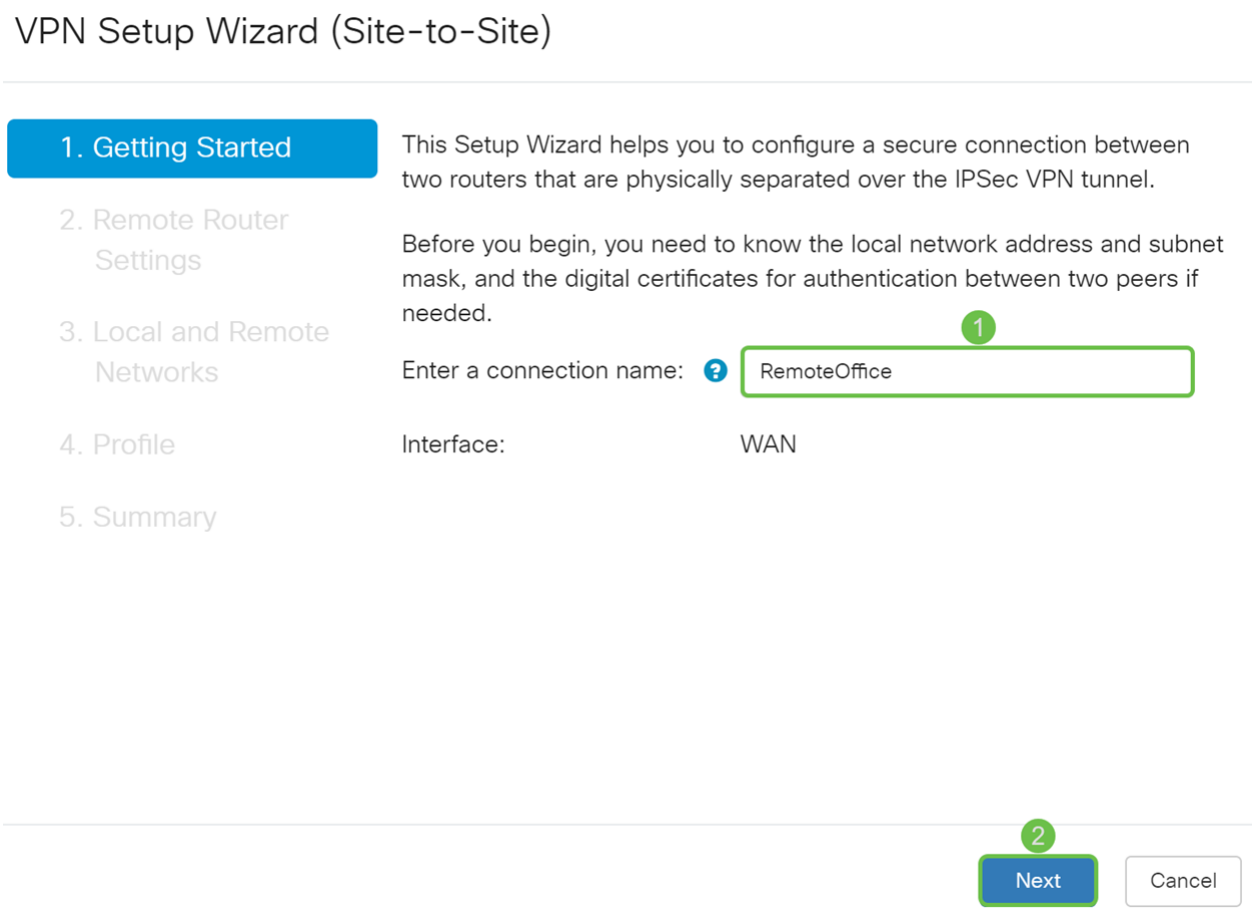
VPN

在遠端路由器上，您需要配置與本地路由器相同的安全設定，但使用本地路由器IP地址作為遠端流量。

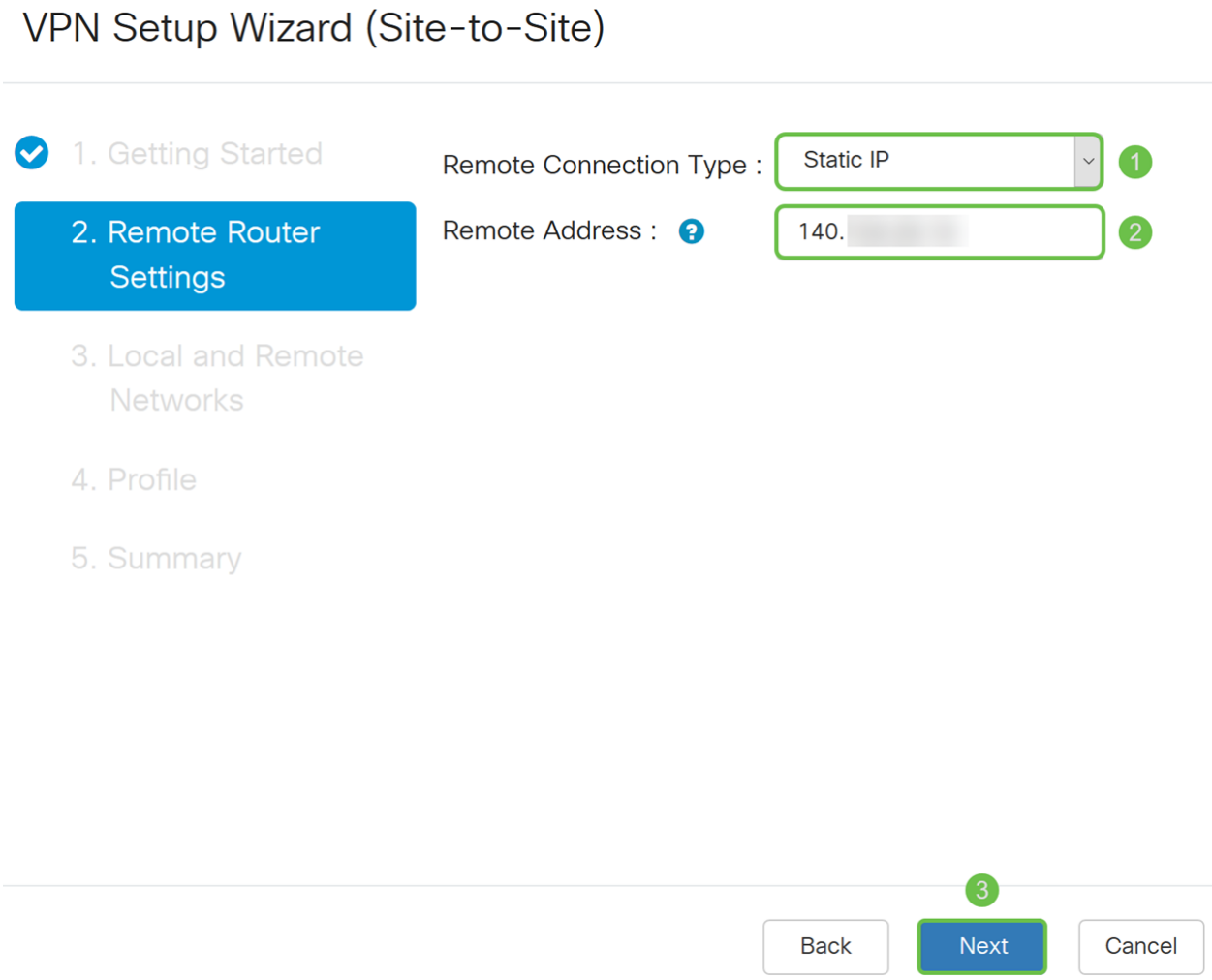
步驟1.登入到遠端路由器（路由器B）上的Web配置頁面，然後導航至**VPN > VPN Setup Wizard**。



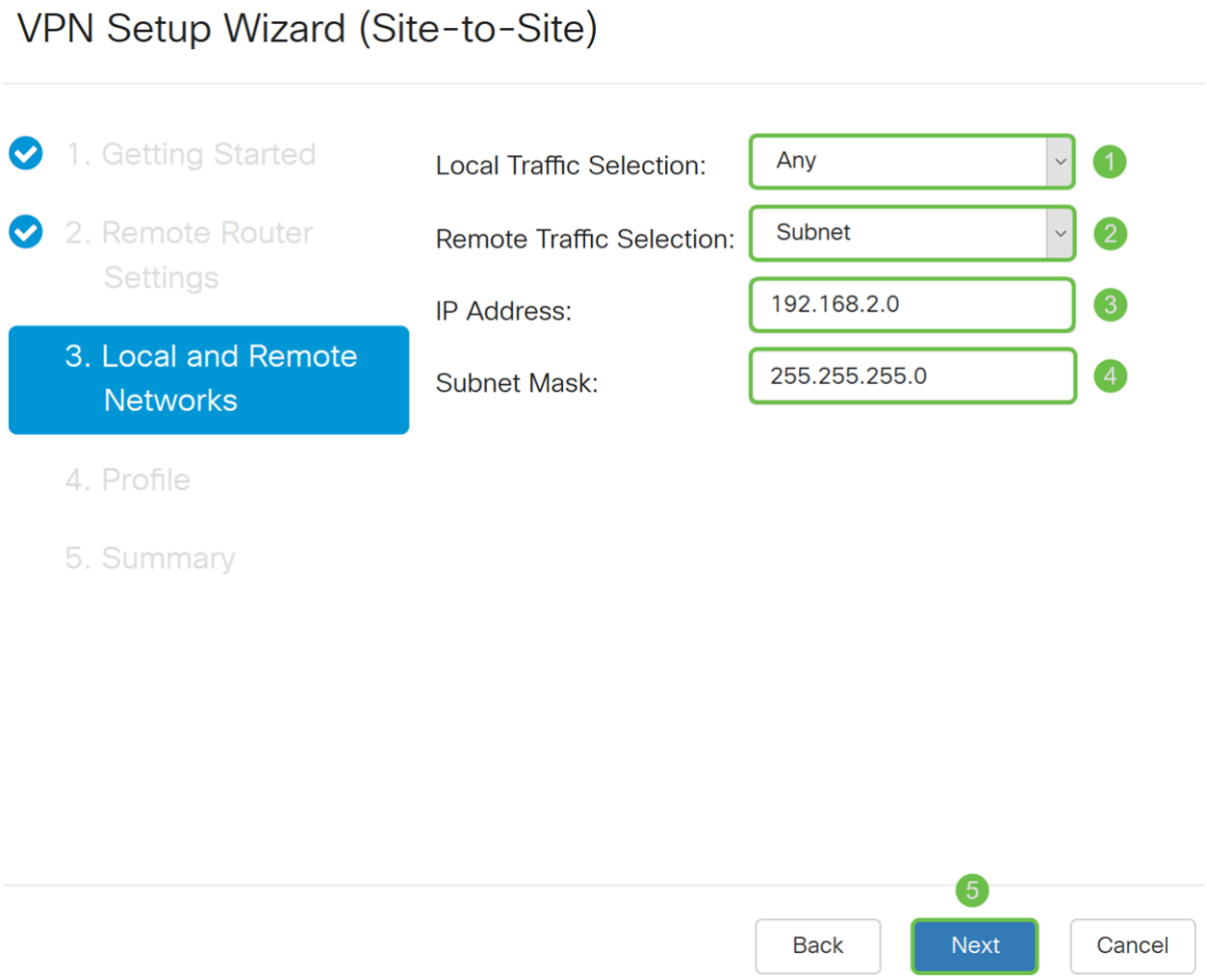
步驟2.輸入連線名稱，如果您使用的是RV260，則選擇將用於VPN的介面。RV160隻有WAN鏈路，因此您將無法從下拉選單中選擇介面。然後按一下**Next**繼續。



步驟3.在*Remote Router Settings*中選擇*Remote Connection Type*，然後輸入路由器A的WAN IP地址。然後按一下**下一步**繼續下一部分。

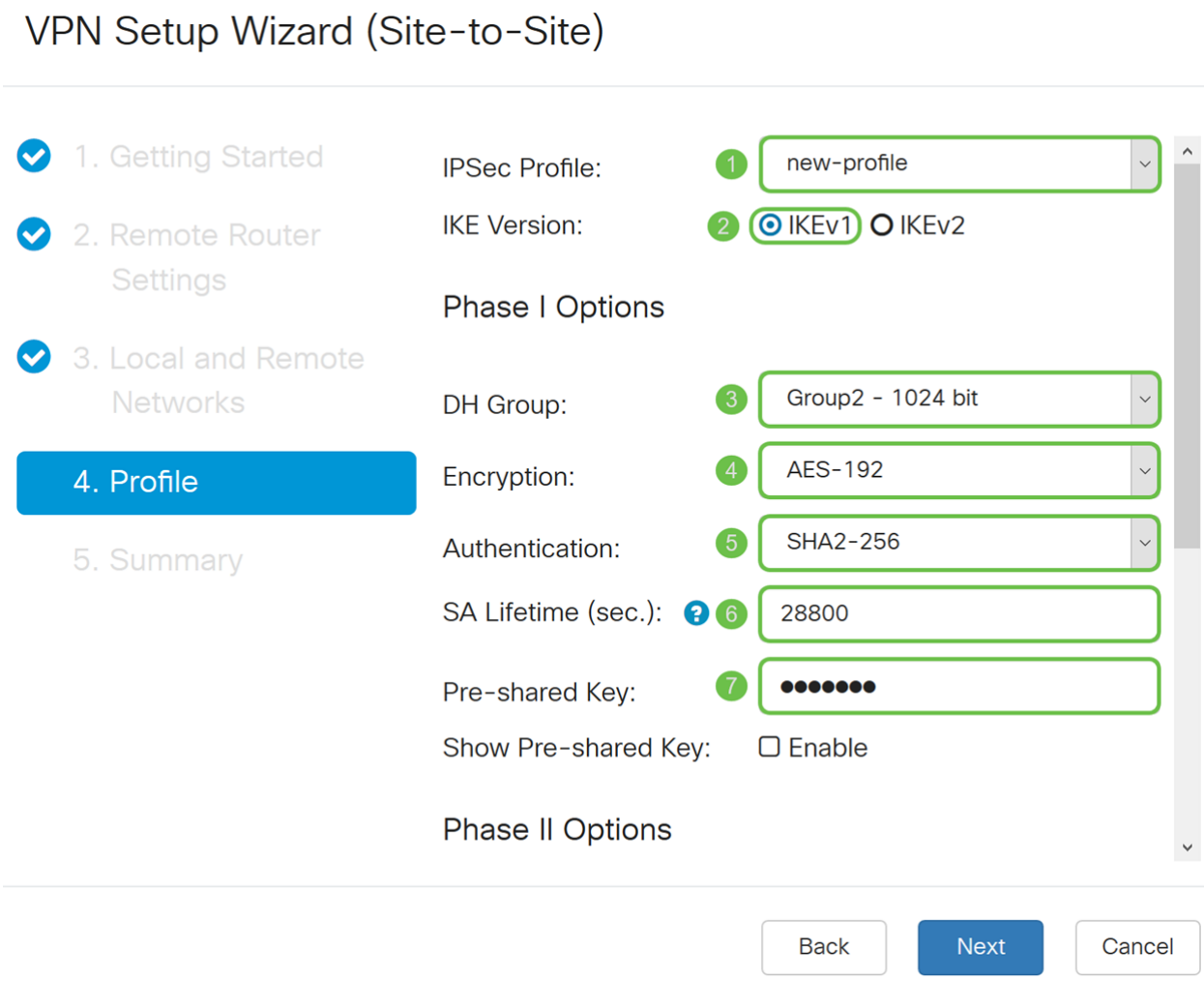


步驟4.選擇本地和遠端流量。如果在*Remote Traffic Selection*欄位中選擇了**Subnet**，請輸入路由器A的專用IP地址子網。然後按一下**Next**配置*Profile*部分。

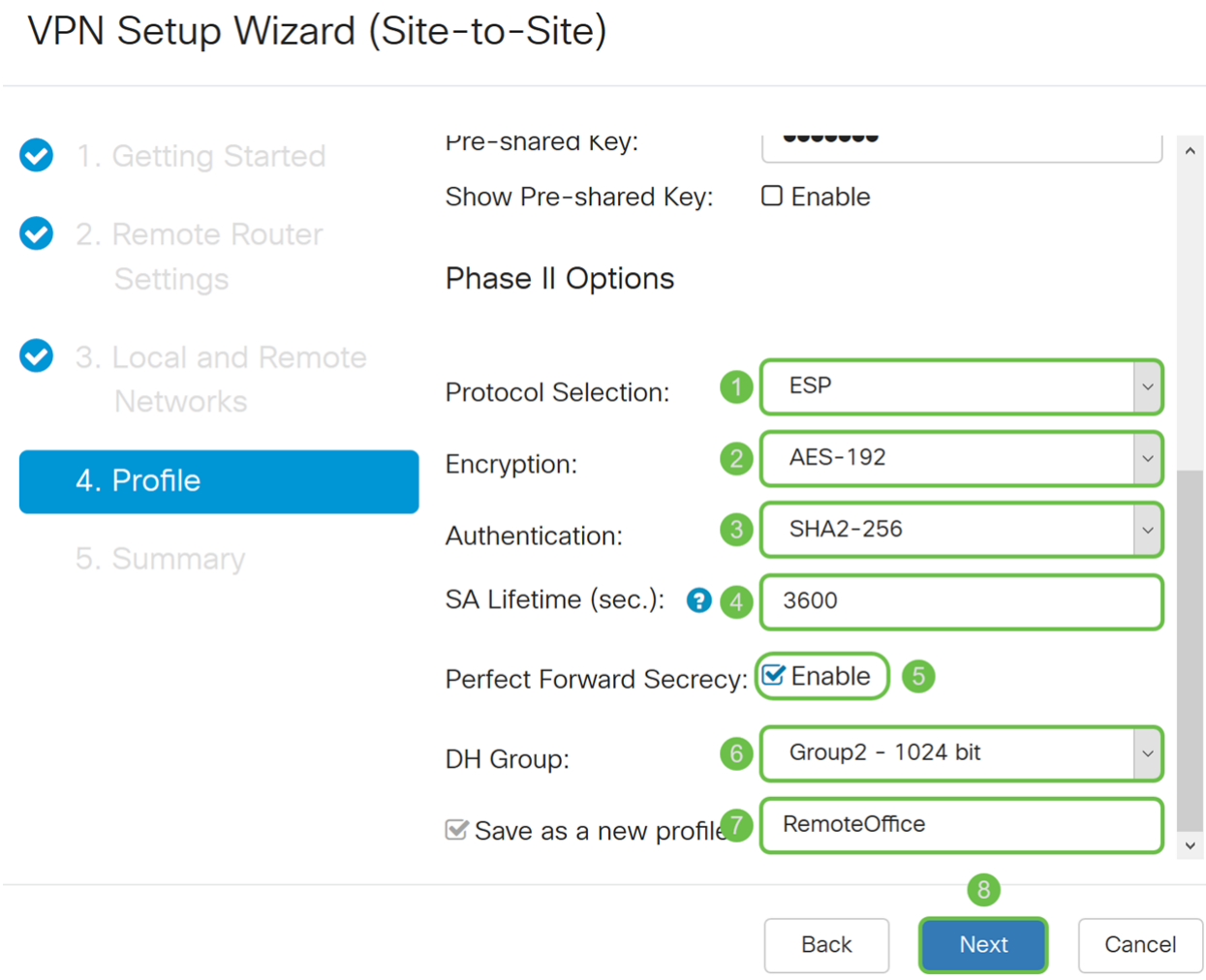


步驟5.在*設定檔*區段中，選擇與路由器A相同的安全設定。我們還輸入了與路由器A相同的預共用金鑰。然後按一下**Next**轉到*Summary*頁面。

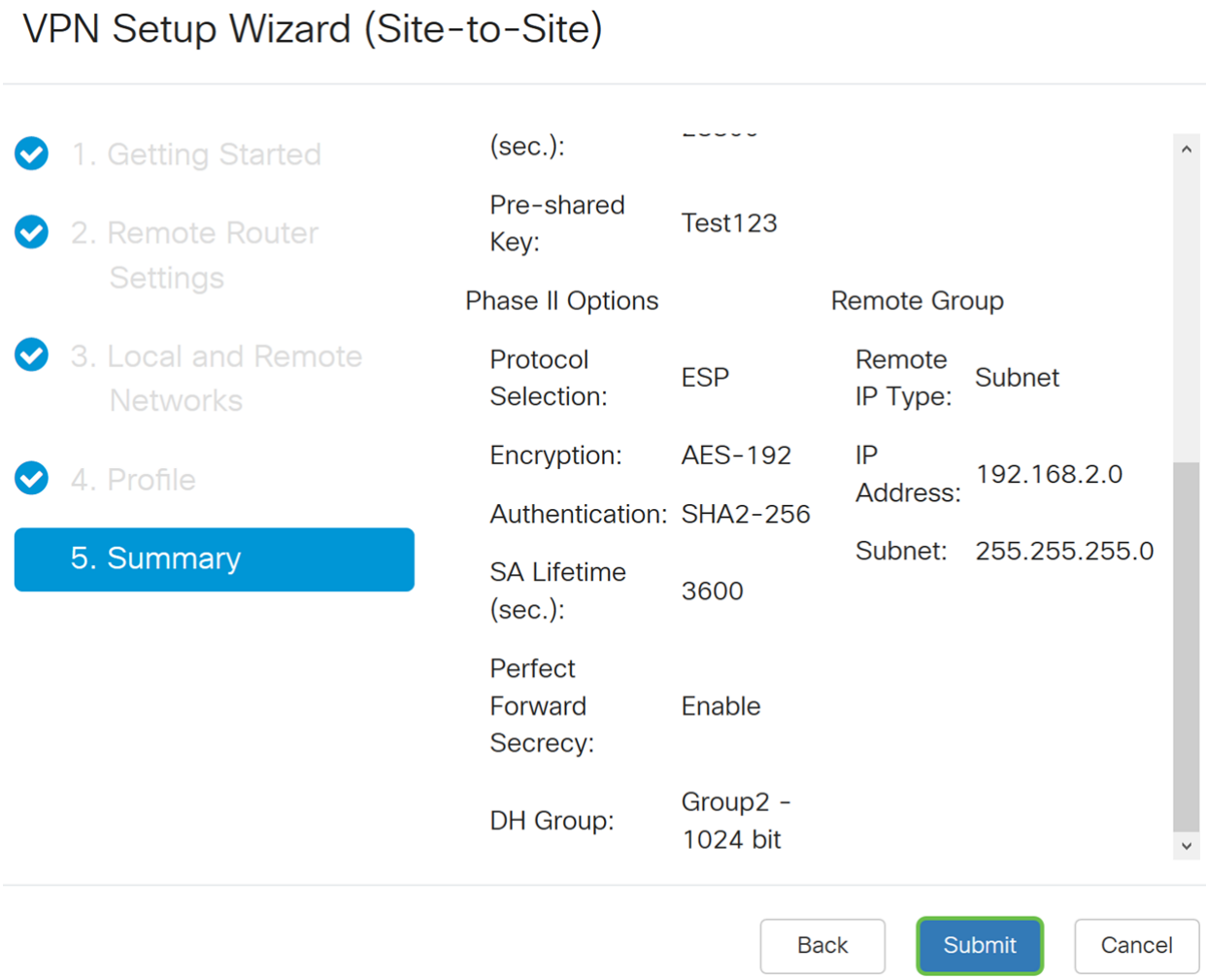
I階段選項：


VPN Setup Wizard (Site-to-Site)
1. Getting Started
2. Remote Router Settings
3. Local and Remote Networks
4. Profile
5. Summary
IPSec Profile:
1
new-profile
IKE Version:
2
IKEv1
IKEv2
Phase I Options
DH Group:
3
Group2 - 1024 bit
Encryption:
4
AES-192
Authentication:
5
SHA2-256
SA Lifetime (sec.):
6
28800
Pre-shared Key:
7
Show Pre-shared Key:
Enable
Phase II Options
Back
Next
Cancel

II階段選項：



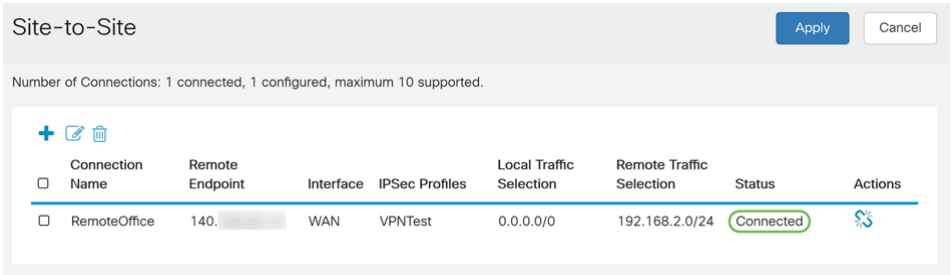
步驟6.在*Summary*頁面中，驗證您剛才配置的資訊是否正確。然後按一下**Submit**建立站點到站點VPN。



附註：路由器當前使用的所有配置都位於運行配置檔案中，該檔案是易失性檔案，在重新啟動後不會保留。要在重新啟動後保留配置，請確保在完成所有更改後將運行配置檔案複製到啟動配置檔案。為此，請按一下頁面頂部的**Save**按鈕，或導航到**Administration > Configuration Management**。接下來，請確認*來源*是**執行組態**，而**目的地**是**啟動組態**。按一下「**Apply**」。

您應該已經使用VPN安裝嚮導成功配置了站點到站點VPN。按照以下步驟驗證您的站點到站點VPN是否已連線。

步驟1。若要確認連線是否已建立，導航到**VPN > IPSec VPN > Site-to-Site**時，應該會看到*Connected*狀態。



步驟2.導覽至**Status and Statistics > VPN Status**，並確保點對點通道為*Enabled*和*UP*。

VPN Status

Site-to-Site Tunnel Status

1	Tunnel(s) Used	9	Tunnel(s) Available
1	Tunnel(s) Enabled	1	Tunnel(s) Defined

Connection Table

Column Display Selection

No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140.	