在RV160和RV260上配置IPSec配置檔案（自動金鑰模式）

本文檔將演示如何在RV160和RV260系列路由器上使用自動金鑰模式建立新的網際網路協定安全(IPsec)配置檔案。

IPsec可確保您通過Internet進行安全的專用通訊。它為通過Internet傳輸敏感資訊提供了兩個或多個主機的隱私、完整性和真實性。IPsec通常用於虛擬私人網路(VPN)，且是在IP層實作，其使用可協助許多缺乏安全的應用程式。VPN用於為通過不安全網路（例如網際網路）傳輸的敏感資料和IP資訊提供安全通訊機制。它為遠端使用者和企業提供靈活的解決方案，以保護來自同一網路上其他方的任何敏感資訊。

為了成功加密和建立VPN隧道的兩端，雙方需要就加密、解密和身份驗證的方法達成一致。IPsec設定檔是IPsec中的中央組態，定義加密、驗證和Diffie-hellman(DH)群組等演演算法，用於自動模式以及手動鍵控模式下的第I階段和II階段交涉。第1階段建立預共用金鑰以建立安全的經過身份驗證的通訊。階段2是流量加密的位置。可以配置大多數IPsec引數，如協定、模式、演算法、完全轉發保密(PFS)、安全關聯(SA)生存期和金鑰管理協定。

請注意，配置站點到站點VPN時，遠端路由器需要具有與本地路由器相同的配置檔案設定。

可以在以下連結中找到有關Cisco IPsec技術的更多資訊：Cisco IPSec技術簡介。

要使用VPN設定嚮導配置IPsec配置檔案和站點到站點VPN，請按一下連結：在RV160和RV260上配置VPN設定嚮導。

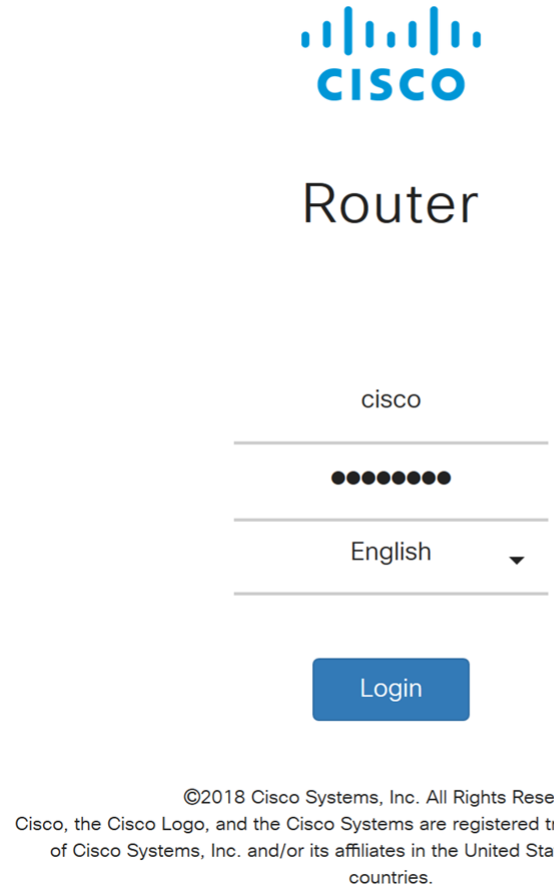
要配置站點到站點VPN，請參閱文檔：在RV160和RV260上配置站點到站點VPN。

- RV160
- RV260

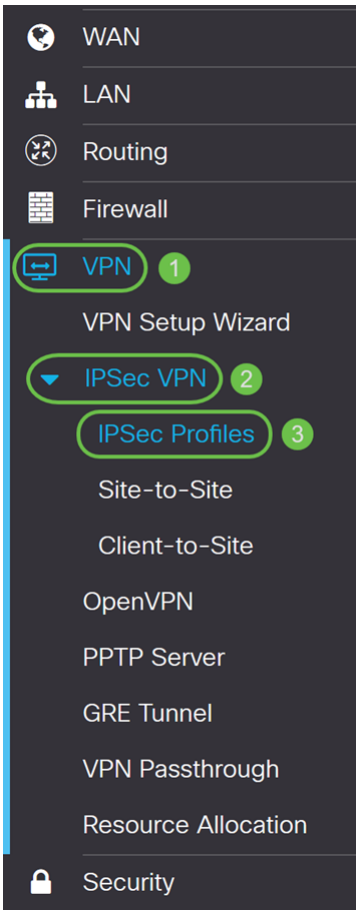
•1.0.00.13

IPsec

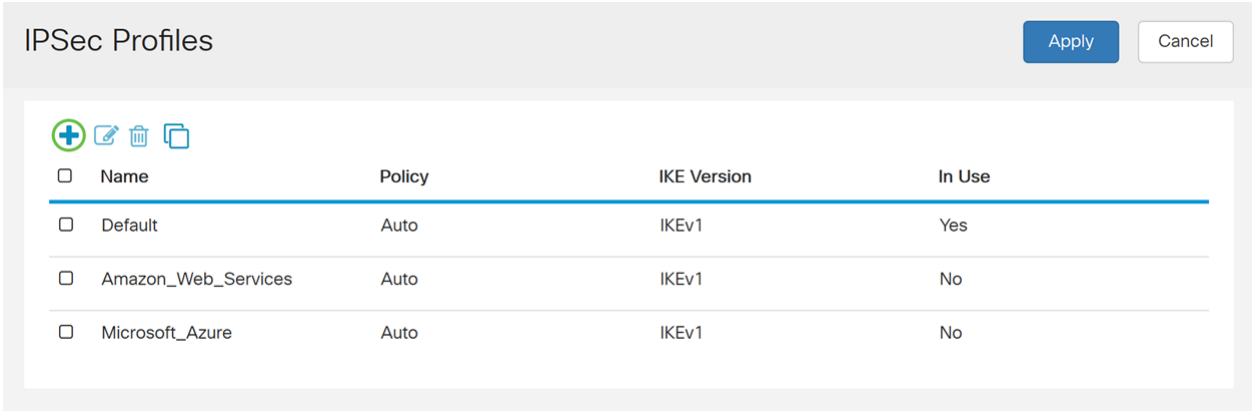
步驟1.登入路由器上的Web組態頁面。



步驟2.導覽至**VPN > IPSec VPN > IPSec Profiles**。



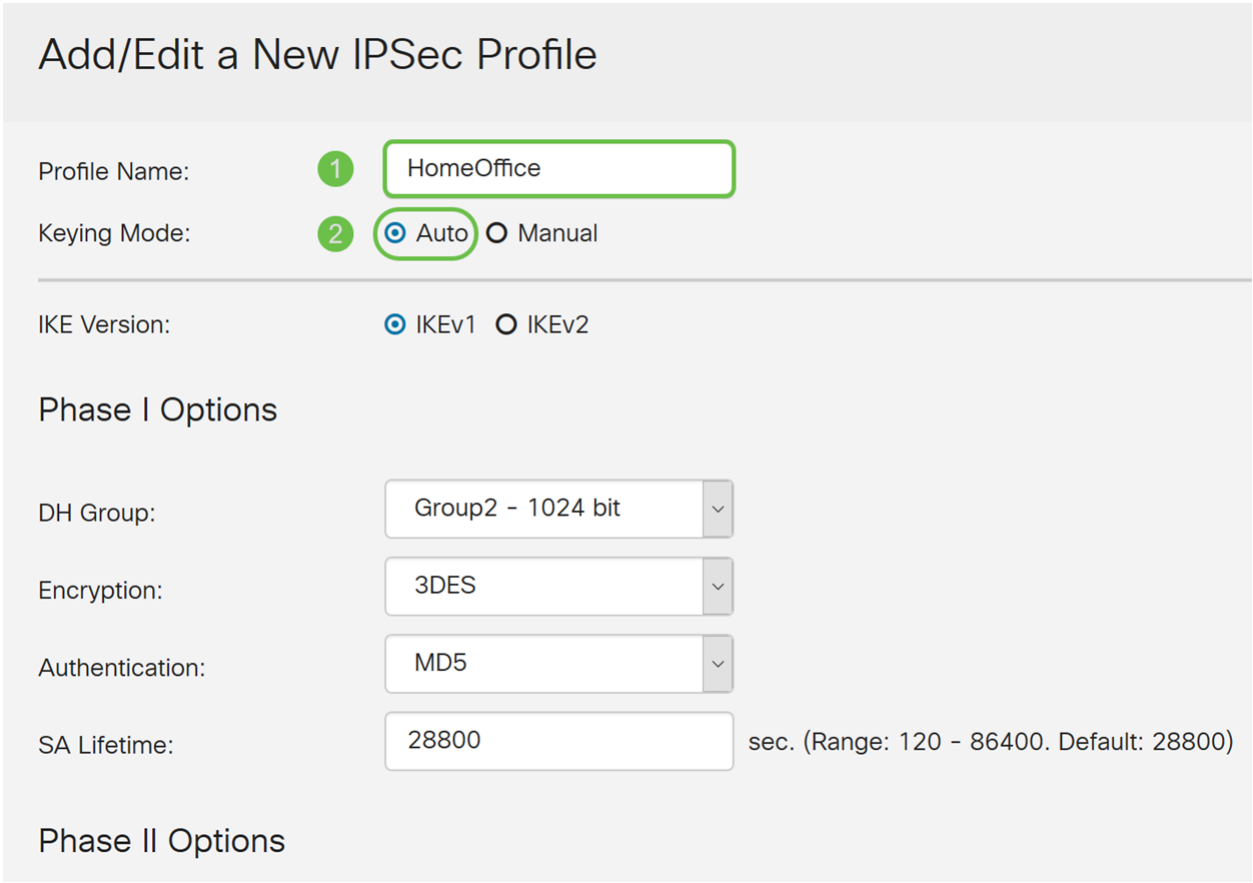
步驟3.在*IPSec配置檔案*表中，按一下**Add**以建立新的IPsec配置檔案。還可以選擇編輯、刪除或克隆配置檔案。



步驟4.輸入配置檔名稱並選擇鍵入模式（自動或手動）。

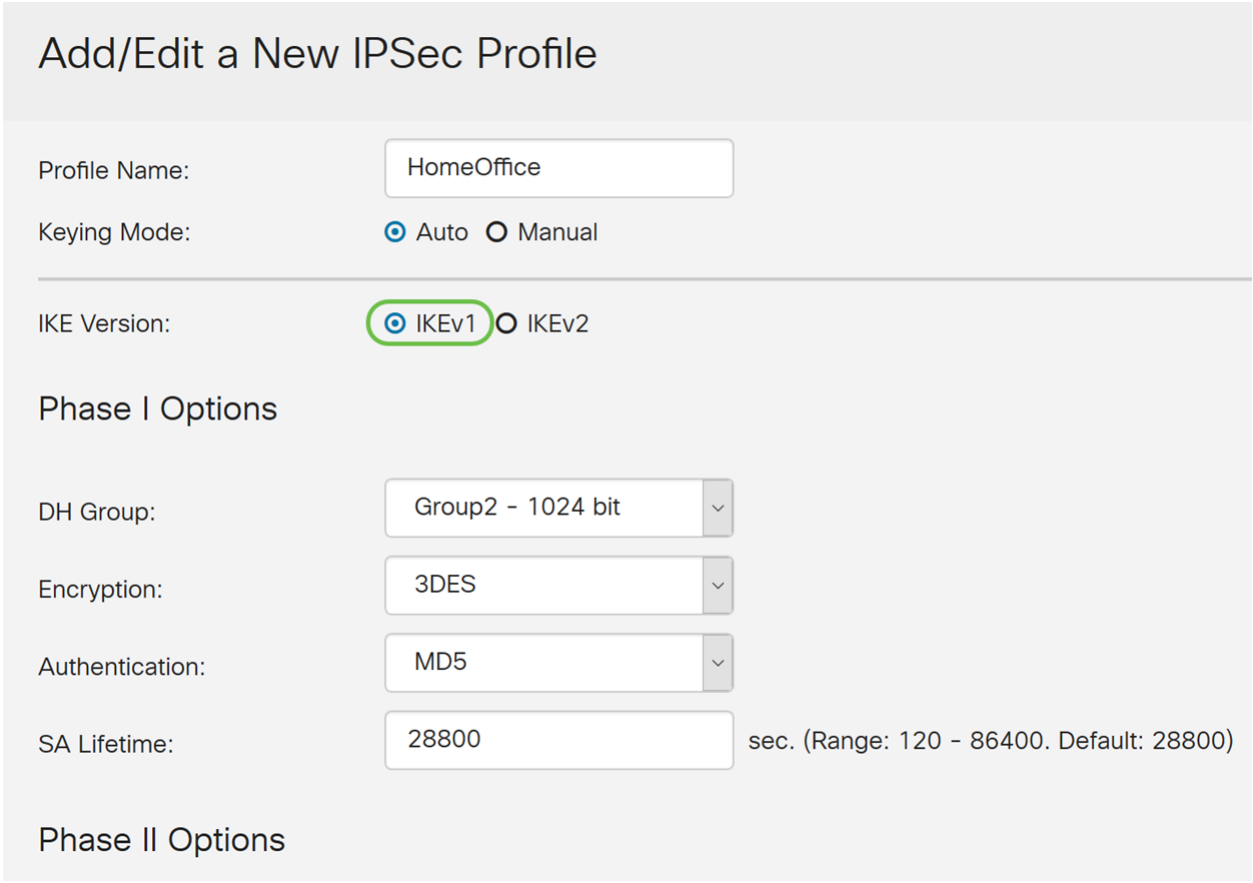
輸入HomeOffice作為配置文*件名稱*。

為鍵控模式選*擇自動*。



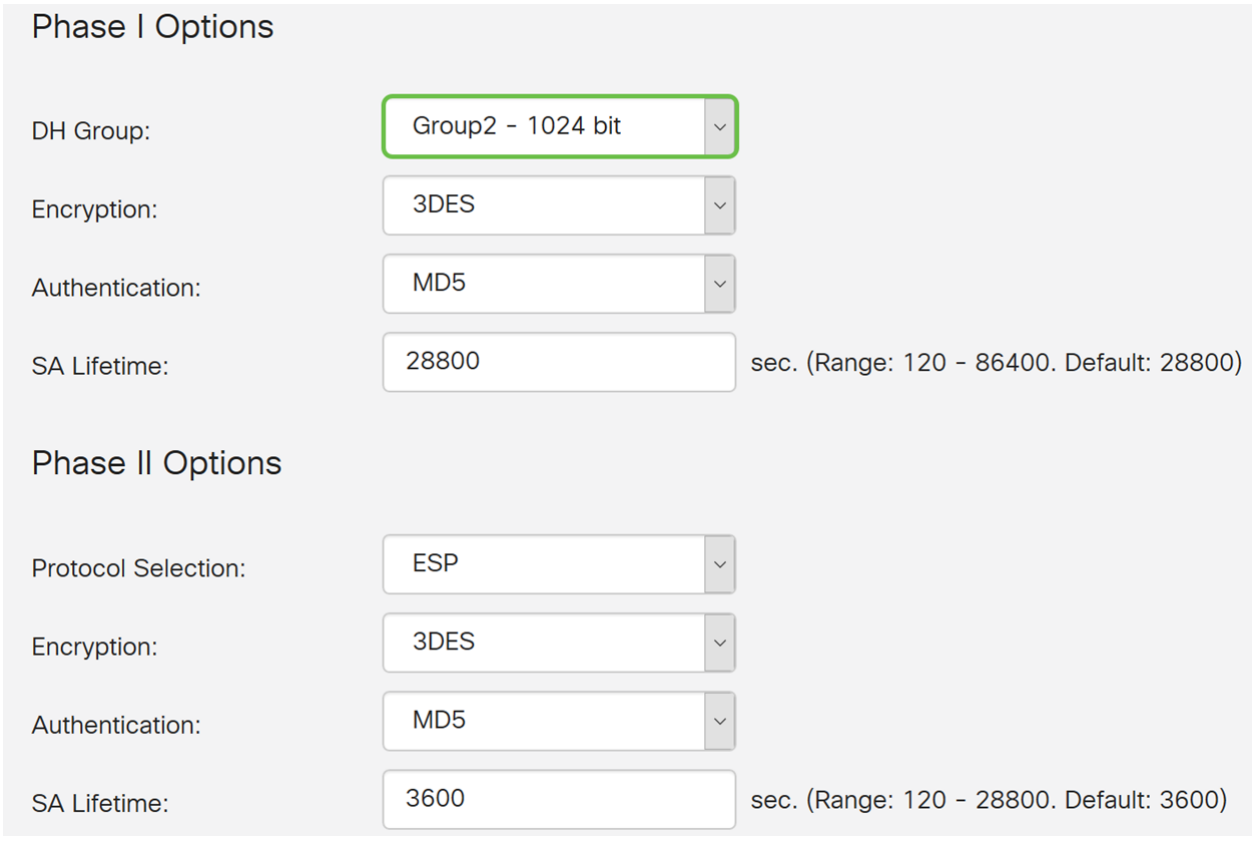
步驟5.選擇*Internet Key Exchange Version 1(IKEv1)*或*Internet Key Exchange Version 2(IKEv2)*作為IKE版本。IKE是在Internet安全關聯和金鑰管理協定(ISAKMP)框架中實現Oakley金鑰交換和Skeme金鑰交換的混合協定。Oakley和Skeme都定義了如何派生經過驗證的金鑰材料，但Skeme還包括快速金鑰更新。IKE提供IPsec對等體的身份驗證、協商IPsec金鑰和協商IPsec安全關聯。IKEv2效率更高，因為它需要更少的資料包來進行金鑰交換，支援更多的身份驗證選項，而IKEv1僅執行共用金鑰和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。



步驟6.階段I設定和交換您將在階段II用於加密資料的金鑰。在「*Phase I*」區段中，選擇Diffie-Hellman(DH)組。DH是一種金鑰交換協定，具有兩組不同主金鑰長度(**組2 - 1024位和組**5 - **1536位)**。在本演示中，我們選擇了**Group 2 - 1024 bit** 。

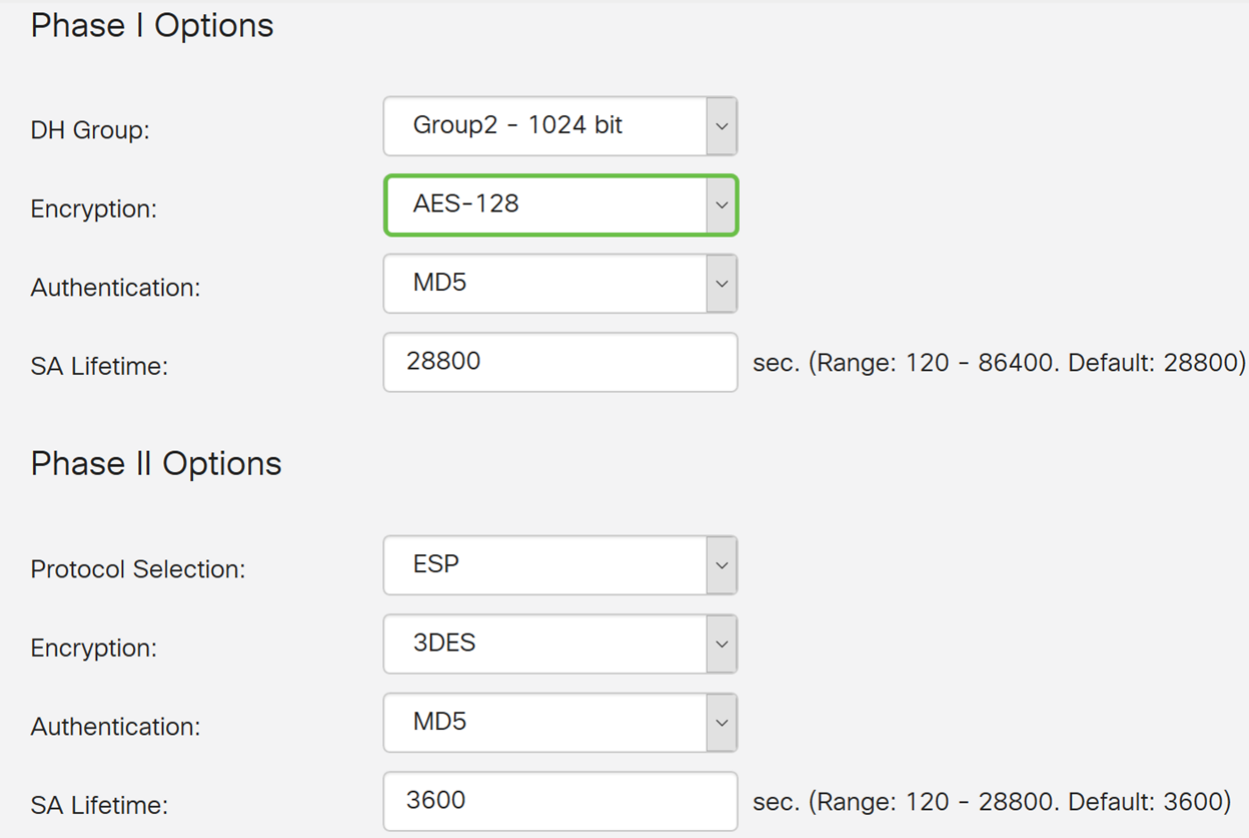
附註：為獲得更快的速度和更高的安全性，請選擇「組2」。為獲得更慢的速度和安全性，請選擇「組5」。預設情況下會選擇組2。



步驟7.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

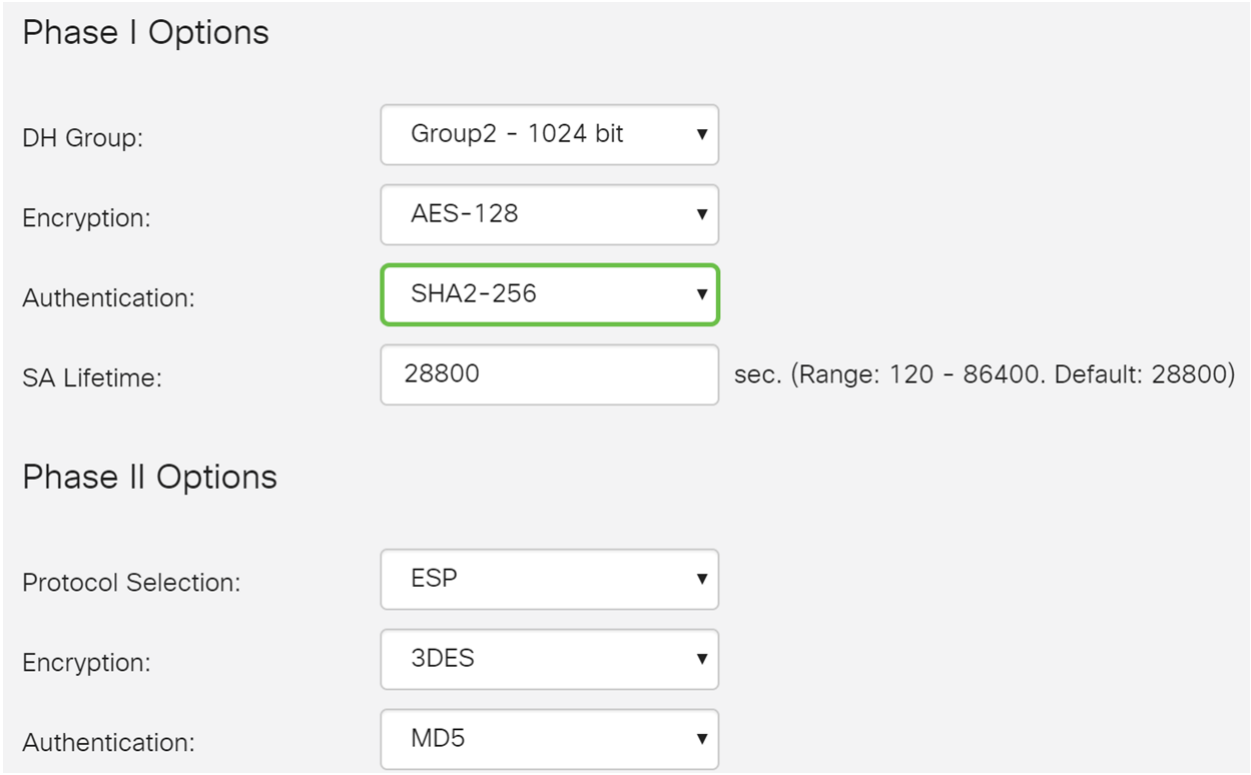
於加密和解密ESP/ISAKMP資料包的演算法。三重資料加密標準(3DES)使用DES加密三次，但現在是傳統演算法。這意味著只有當沒有更好的替代方法時才應該使用它，因為它仍提供邊緣但可接受的安全級別。使用者應僅在需要向後相容性時才使用它，因為它容易受到某些「塊衝突」攻擊。建議不要使用3DES，因為它被認為不安全。高級加密標準(AES)是一種加密演算法，旨在比DES更安全。AES使用較大的金鑰大小，確保唯一已知解密消息的方法是讓入侵者嘗試所有可能的金鑰。如果您的裝置可以支援，建議使用AES。在本例中，我們選擇**AES-128**作為加密選項。

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的安全。



步驟8.驗證方法確定ESP報頭資料包的驗證方式。這是身份驗證中使用的雜湊演算法，用於驗證端A和端B確實是它們所說的。MD5是產生128位摘要的單向雜湊演算法，比SHA1快。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)**。

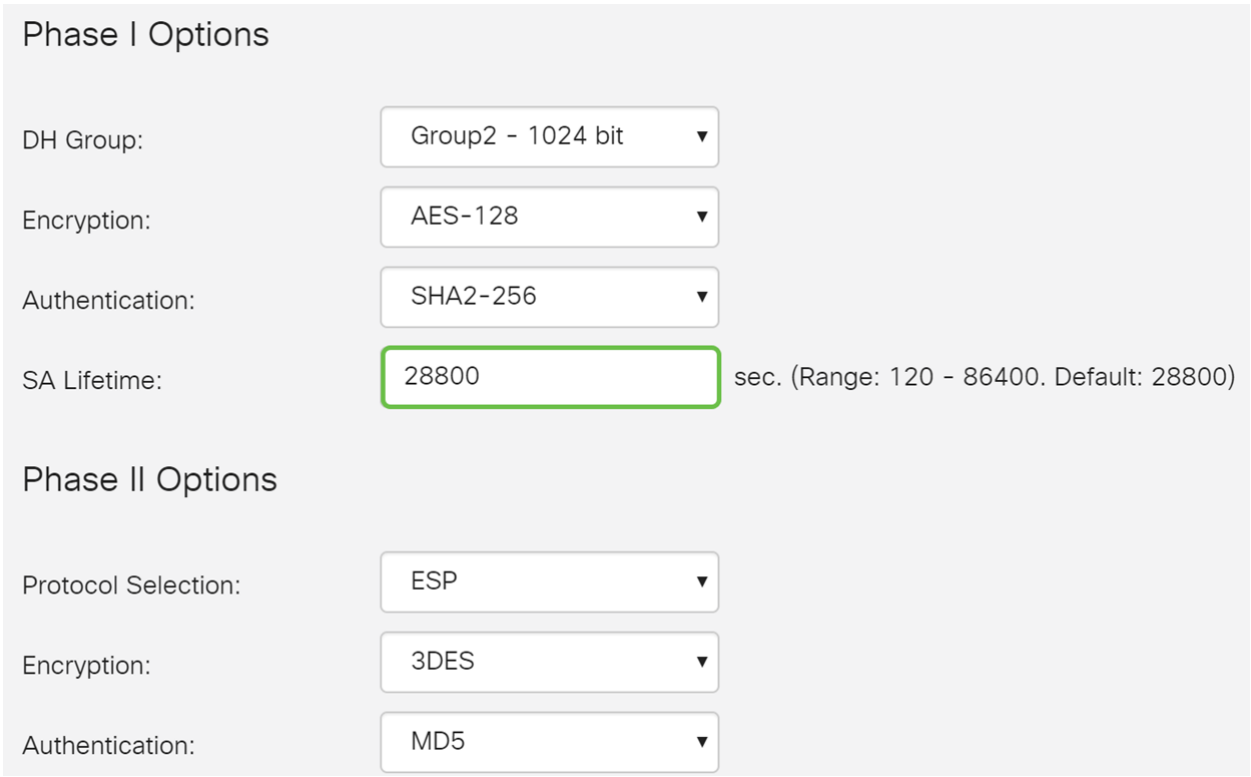
本示例選擇了SHA2-256。



步驟9. *SA Lifetime(Sec)*會顯示IKE SA在此階段中處於活動狀態的時間量。當SA在各自的生存期之後到期時，新的協商將開始。範圍為120到86400，預設值為28800。

我們將使用預設值**28800**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。

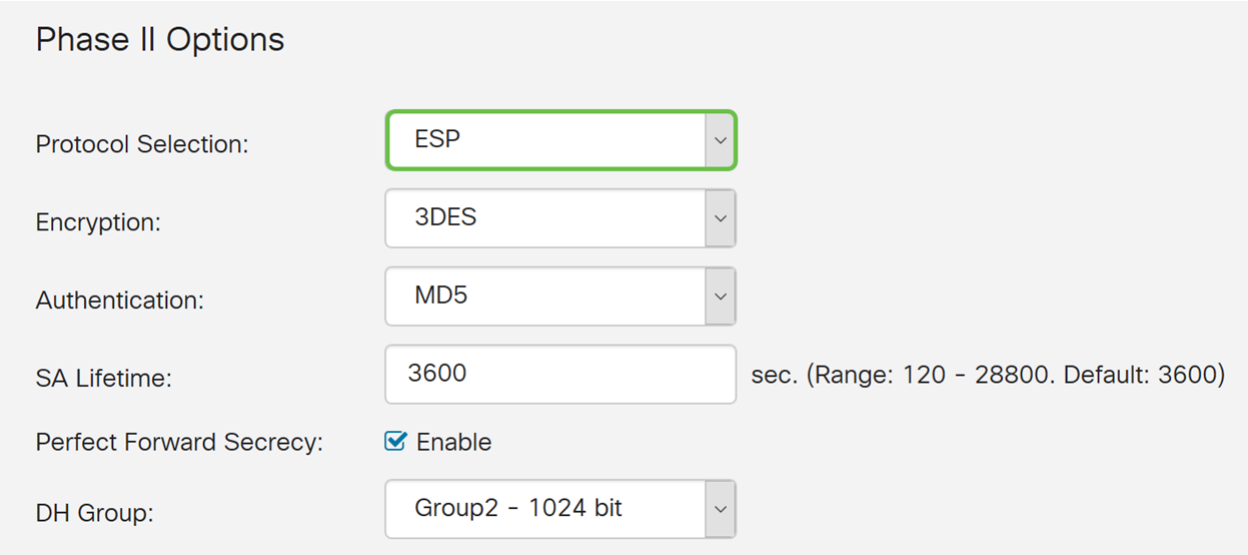


步驟10.階段II是對來回傳送的資料進行加密。在*Phase 2 Options*中，從下拉選單中選擇協定，選項為：

- 封裝安全負載(ESP) — 選擇用於資料加密的ESP並輸入加密。

• Authentication Header(AH) — 選擇此項，可在資料不是機密的情況下保證資料完整性，也就是說，資料不是加密的，但必須經過身份驗證。它僅用於驗證流量的來源和目的地。

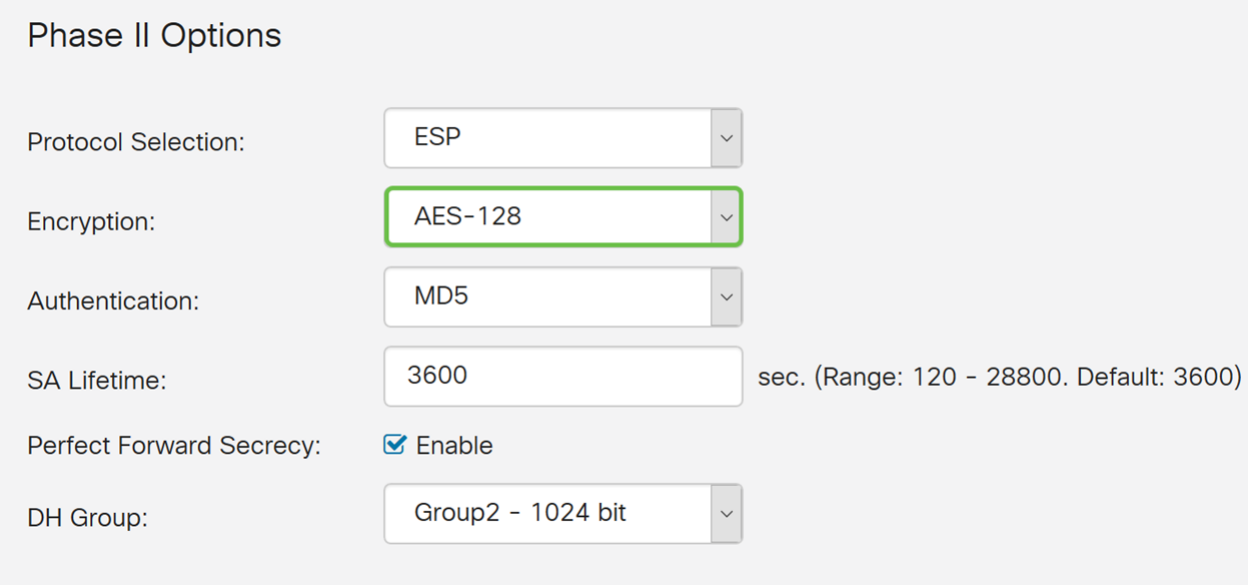
在本例中，我們將使用**ESP**作為我們的*協定選擇*。



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和解密ESP/ISAKMP資料包的演算法。

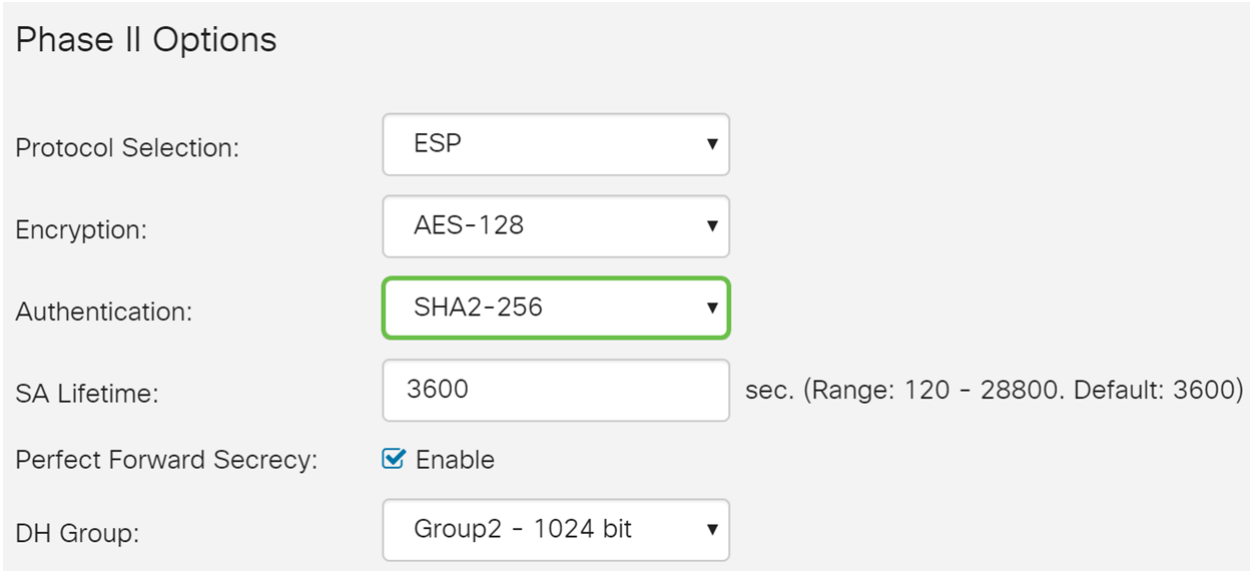
在本例中，我們將使用**AES-128**作為加密選項。

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的安全](#)。

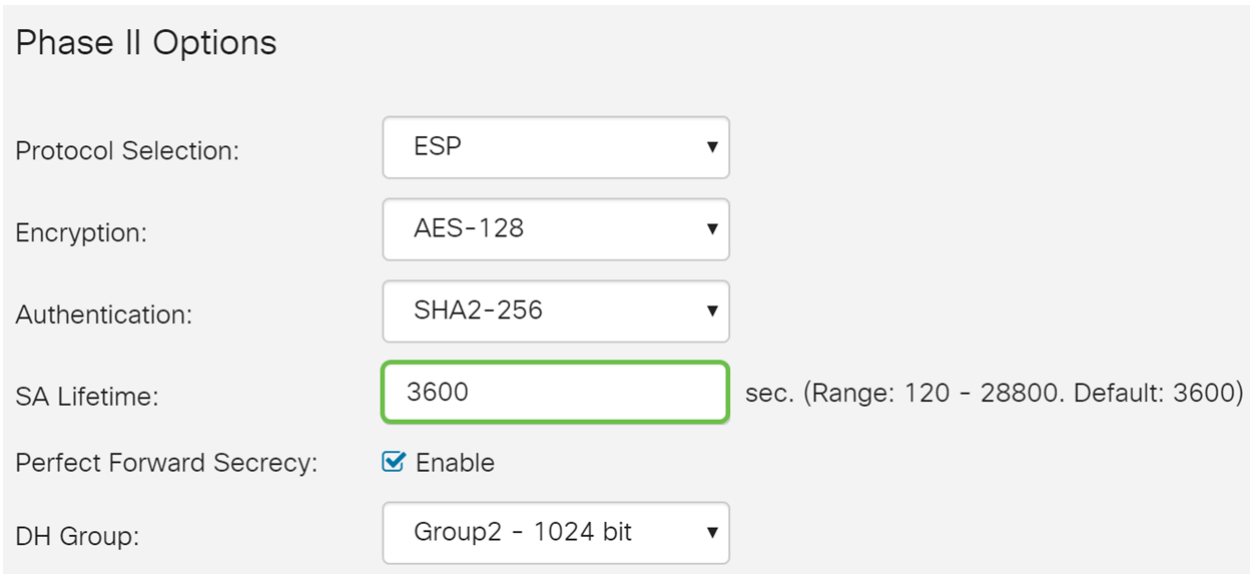


步驟12.驗證方法決定如何驗證封裝安全負載通訊協定(ESP)標頭封包。選擇驗證(**MD5、SHA1**或**SHA2-256**)。

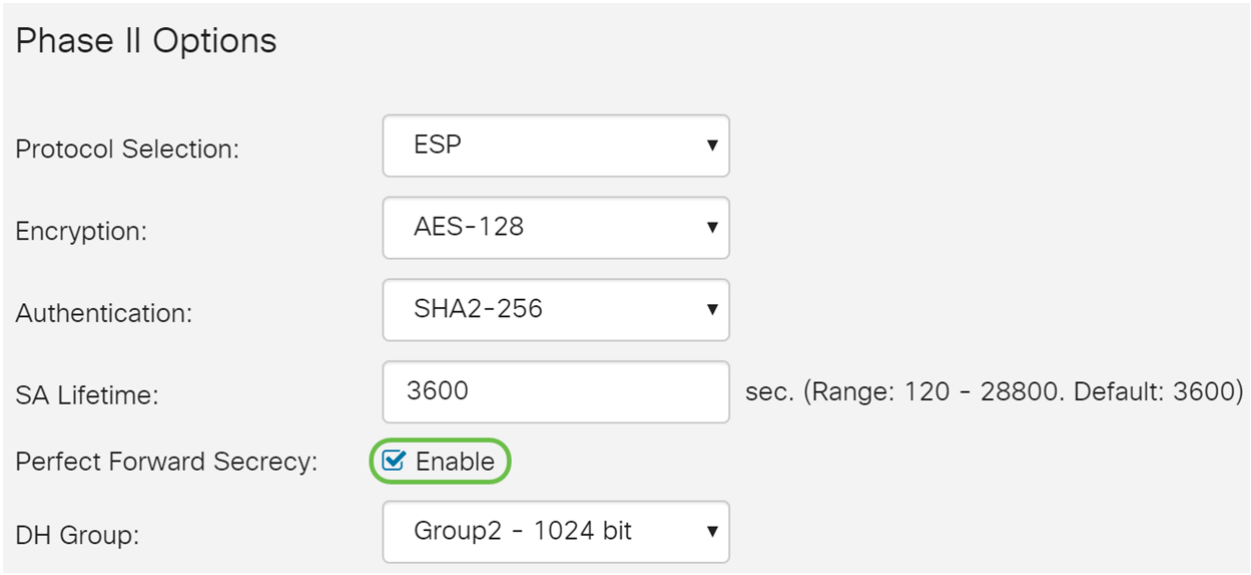
本示例選擇了SHA2-256。



步驟13.輸入VPN隧道(IPsec SA)在此階段的活動時間。階段2的預設值為3600秒。我們將使用此演示的預設值。

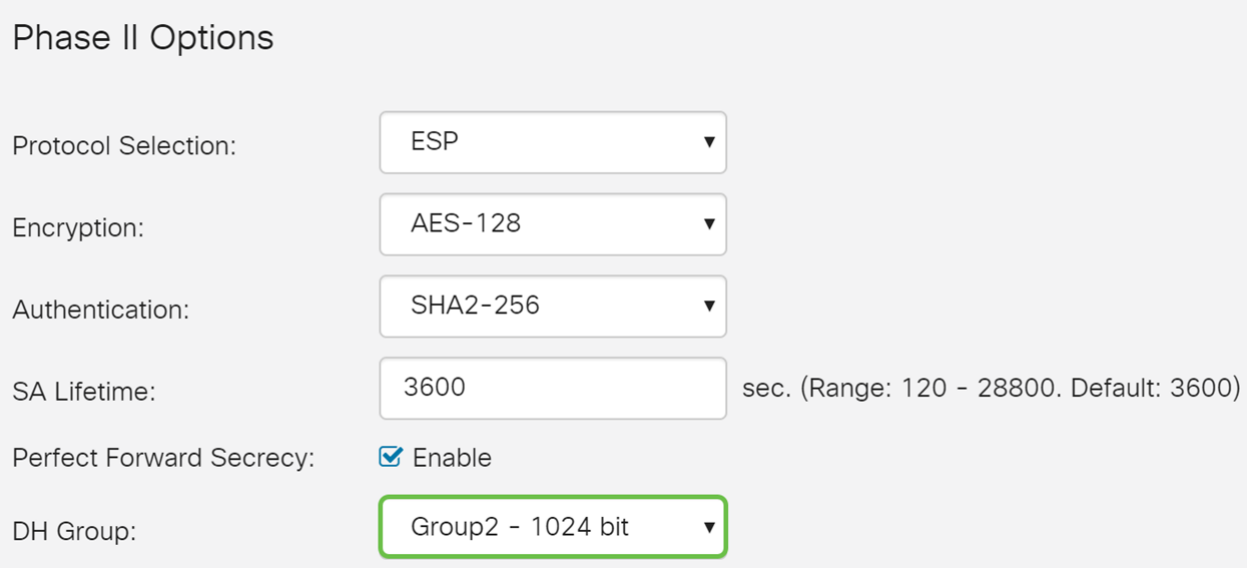


步驟14.選中**Enable**以啟用完全向前保密功能。啟用完全轉發保密(PFS)時，IKE第2階段協商會生成用於IPsec流量加密和身份驗證的新金鑰材料。PFS用於使用公鑰加密技術提高通過Internet傳輸的通訊的安全性。如果您的裝置支援，建議這樣做。

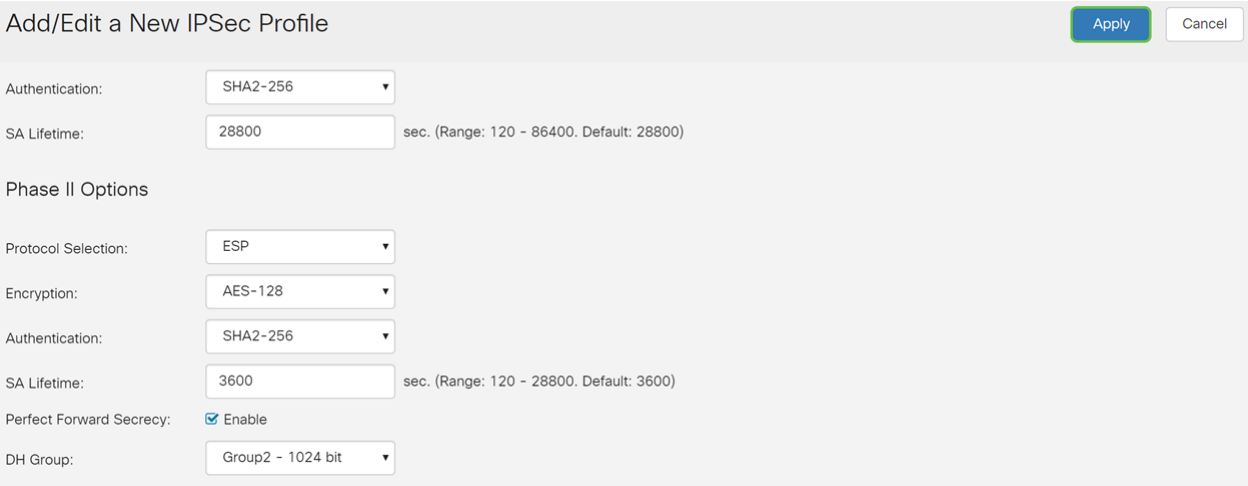


步驟15.選擇Diffie-hellman(DH)組。DH是一種金鑰交換協定，具有兩組不同主金鑰長度(**組2 - 1024位和組**5 **- 1536位)**。在本演示中，我們選擇了**Group 2 - 1024 bit** 。

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」。

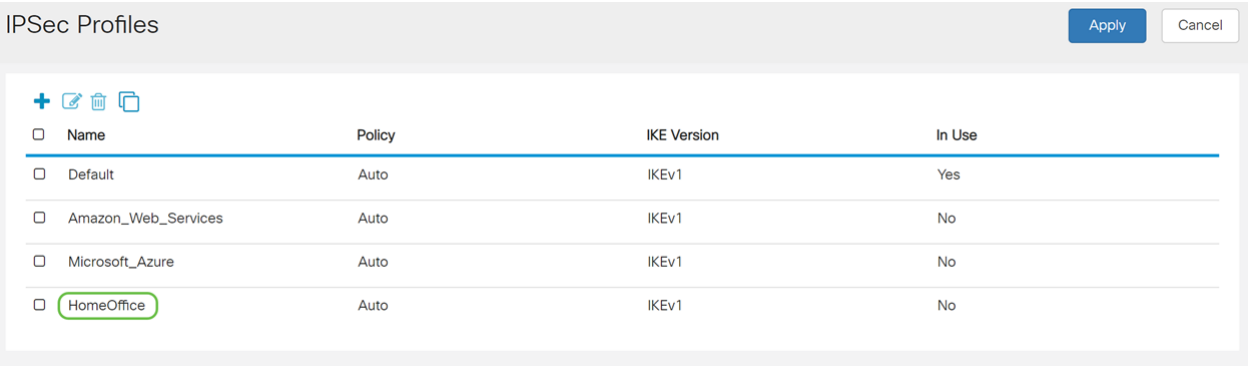


步驟16.按一下**Apply**新增新的IPsec配置檔案。

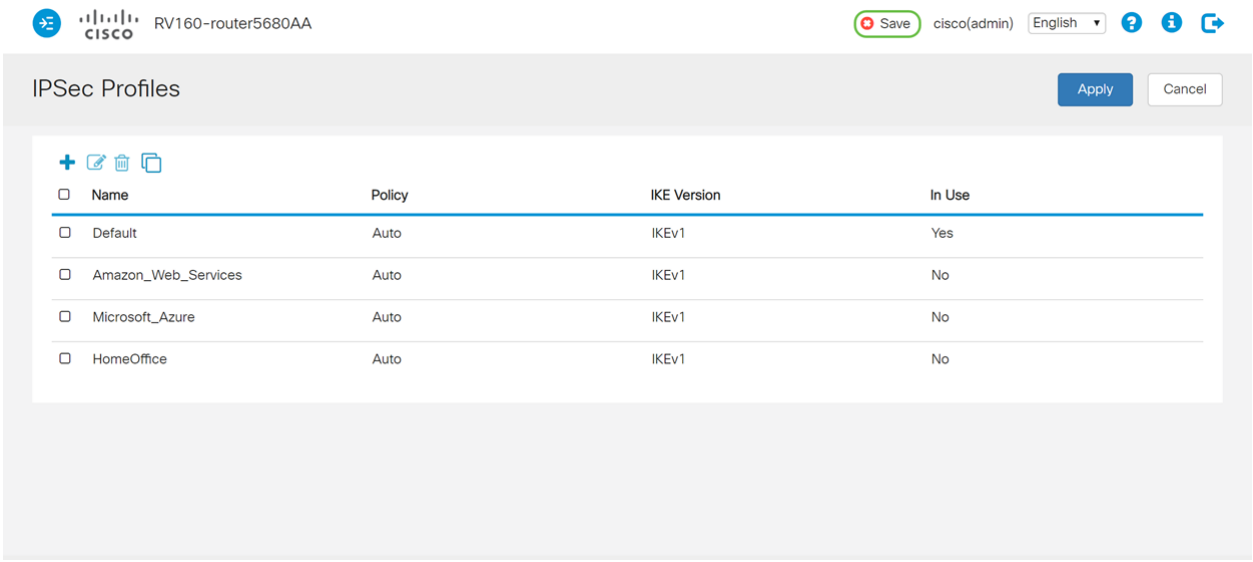


現在，您應該已經成功建立了新的IPsec配置檔案。請在下面繼續驗證是否已新增您的IPsec配置檔案。您也可以按照步驟將運行配置檔案複製到啟動配置檔案，以便在重新啟動後保留所有配置。

步驟1.按一下*Apply*後，應新增新的IPsec配置檔案。



步驟2.在頁面頂部，按一下**Save**按鈕導航到*Configuration Management*，將運行配置儲存到啟動配置。這是為了在重新啟動之間保留配置。



步驟3.在組態管理中，請確認*來源*是**執行組態**，而*目的地*是**啟動組態**。然後按下Apply將運行配置儲存到啟動配置。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。將運行配置檔案複製到啟動配置檔案會在重新啟動之間保留所有配置。