

在RV34x系列路由器上配置IKEv2

本文檔的目的是向您展示如何在RV34x系列路由器上使用IKEv2配置IPsec配置檔案。

RV34x系列路由器的韌體版本1.0.02.16現在支援站點到站點VPN和客戶端到站點VPN的網際網路金鑰交換版本2(IKEv2)。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仍使用UDP埠500，但需要注意一些更改。失效對等體檢測(DPD)的管理方式不同，現在已內建。將安全關聯(SA)協商最小化到4條消息。此新更新還支援可擴展身份驗證協定(EAP)身份驗證，此身份驗證現在能夠利用AAA伺服器 and 拒絕服務保護。

下表進一步說明IKEv1和IKEv2之間的差異

| IKEv1 | IKEv2 |
|-----------------------|--------------|
| SA兩階段協商 (主模式與主動模式) | SA單相協商(簡化) |
| | 本地/遠端憑證支援 |
| | 改進的衝突處理 |
| | 改進的金鑰更新機制 |
| | NAT穿越內建 |
| | AAA伺服器的EAP支援 |

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通常用於虛擬私有網路(VPN)，並在IP層實作，這有助於為許多不安全的應用增加安全性。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。它還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中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，其定義諸如加密、驗證和在自動模式下為第I階段和第II階段交涉以及手動鍵控模式使用的Diffie-Hellman(DH)群組等演演算法。階段I建立預共用金鑰以建立安全的身份驗證通訊。階段II是加密流量的位置。您可以設定大部分IPsec引數，例如通訊協定(封裝安全負載(ESP))、驗證標頭(AH)、模式(通道、傳輸)、演演算法(加密、完整性、Diffie-Hellman)、完全向前保密(PFS)、SA存留期和金鑰管理通訊協定(Internet金鑰交換(IKE)-IKEv1和IKEv2)。

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](#)。

必須注意的是，配置站點到站點VPN時，遠端路由器需要與本地路由器相同的IPsec配置檔案配置。

下面是本地路由器和遠端路由器的配置表。在本檔案中，我們將使用路由器A配置本地路由器。

| 欄位 | 本地路由器 (路由器A) | 遠端路由器(路 由器B) |
|-------|-----------------|-----------------|
| 配置檔名稱 | 家庭辦公室 | 遠端辦公室 |
| 鍵控模式 | 自動 | 自動 |

| IKE版本 | IKEv2 | IKEv2 |
|----------------|----------------|----------------|
| 第一階段選項 | 第一階段選項 | 第一階段選項 |
| DH組 | Group2 - 1024位 | Group2 - 1024位 |
| 加密 | AES-192 | AES-192 |
| 驗證 | SHA2-256 | SHA2-256 |
| SA生存期 | 28800 | 28800 |
| III階段選項 | III階段選項 | III階段選項 |
| 通訊協定選擇 | ESP | ESP |
| 加密 | AES-192 | AES-192 |
| 驗證 | SHA2-256 | SHA2-256 |
| SA生存期 | 3600 | 3600 |
| 完全向前保密 | 已啟用 | 已啟用 |
| DH組 | Group2 - 1024位 | Group2 - 1024位 |

要瞭解如何在RV34x上配置站點到站點VPN，請按一下連結：[在RV34x上配置站點到站點VPN。](#)

- RV34x

- 1.0.02.16

IKEv2IPsec

步驟1. 登入到本地路由器 (路由器A) 的Web配置頁。



Router

cisco

●●●●●●●●

English

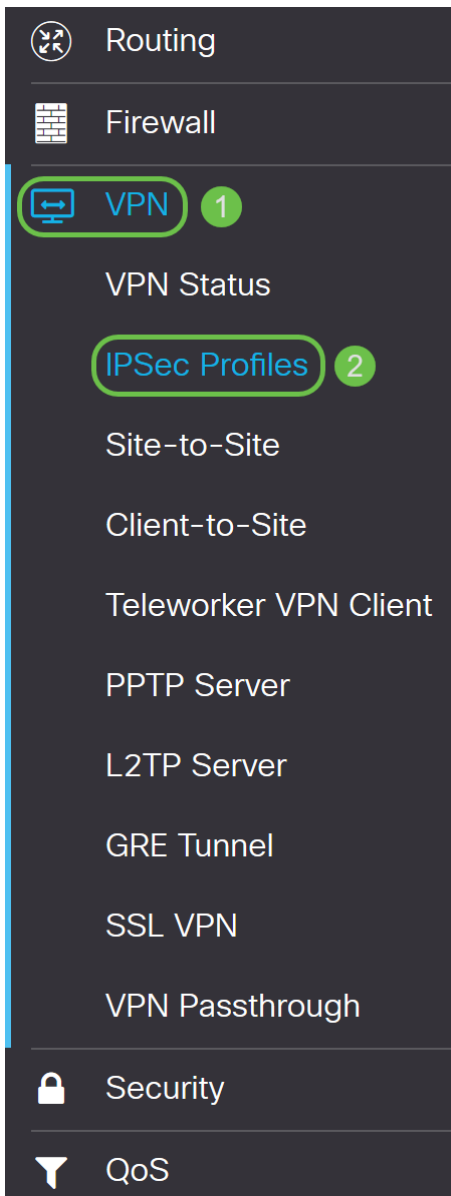


Login

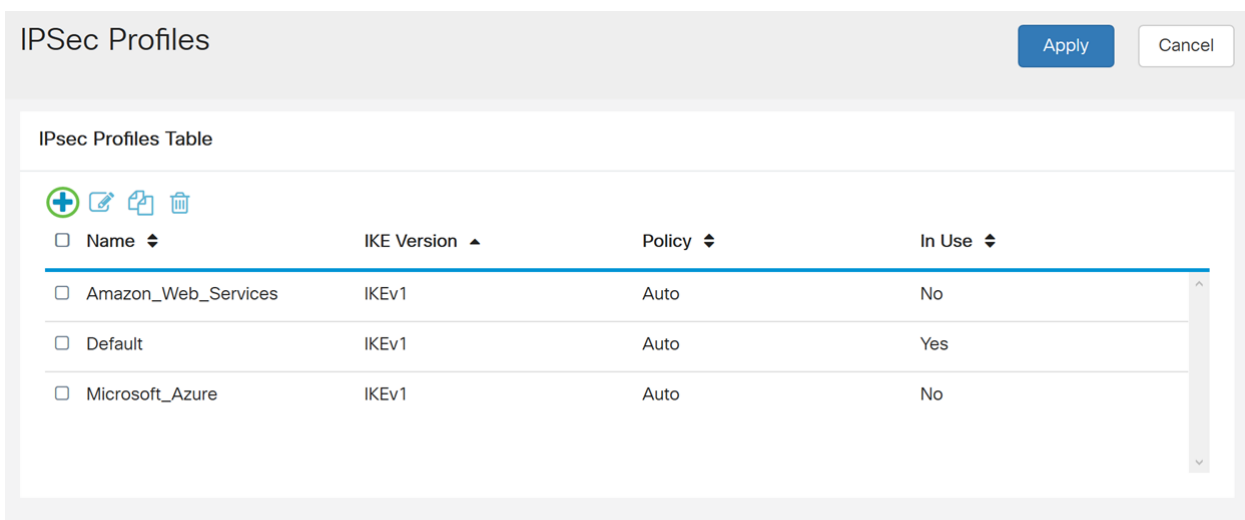
©2017-2018 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

步驟2.導覽至VPN > IPSec Profiles。



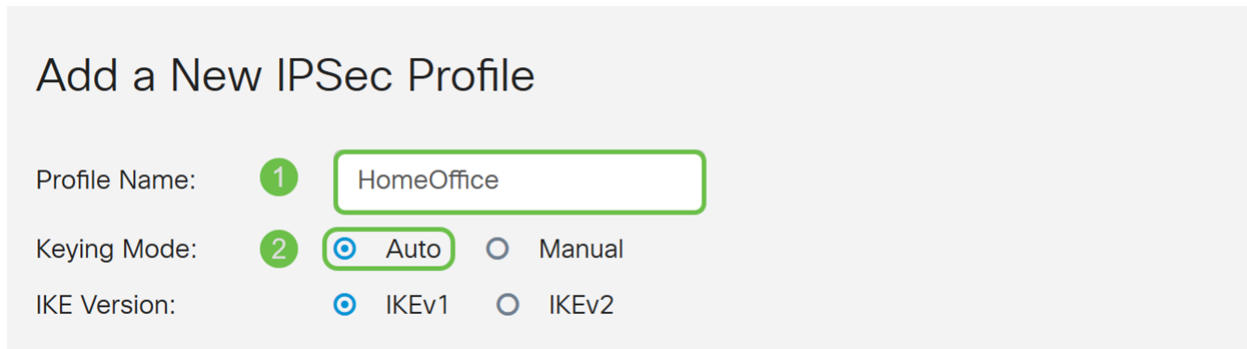
步驟3.在IPSec配置檔案表中，按一下**Add**以建立新的IPsec配置檔案。還可以選擇編輯、刪除或克隆配置檔案。通過克隆配置檔案，可以快速複製IPsec配置檔案表中已存在的配置檔案。如果您需要使用相同的配置建立多個配置檔案，克隆將為您節省一些時間。



步驟4.輸入配置檔名稱並選擇鍵入模式（自動或手動）。配置檔名稱不必與您的其他路由器匹配，但金鑰模式需要匹配。

輸入HomeOffice作為配置文件名稱。

為鍵控模式選擇自動。



Add a New IPsec Profile

Profile Name:

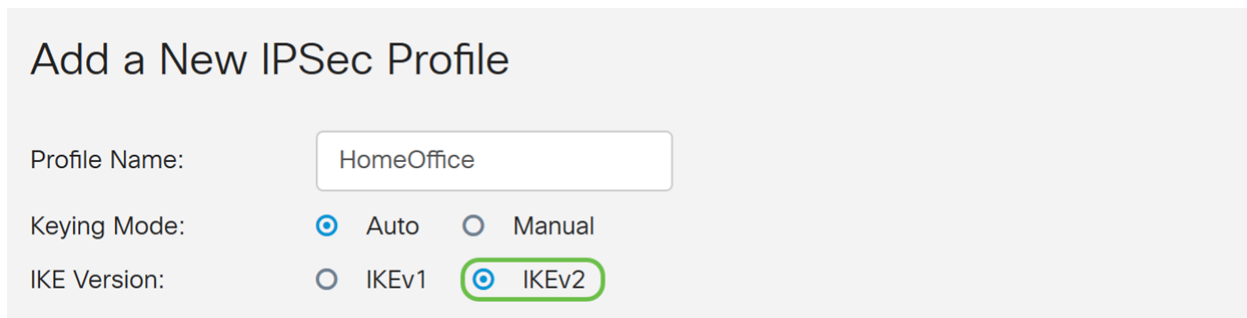
Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

步驟5.選擇IKEv1或IKEv2作為IKE版本。IKE是在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都定義了如何獲取經過驗證的金鑰材料，但Skeme還包括快速金鑰更新。IKEv2效率更高，因為它需要更少的資料包來進行金鑰交換，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IKEv2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。



Add a New IPsec Profile

Profile Name:

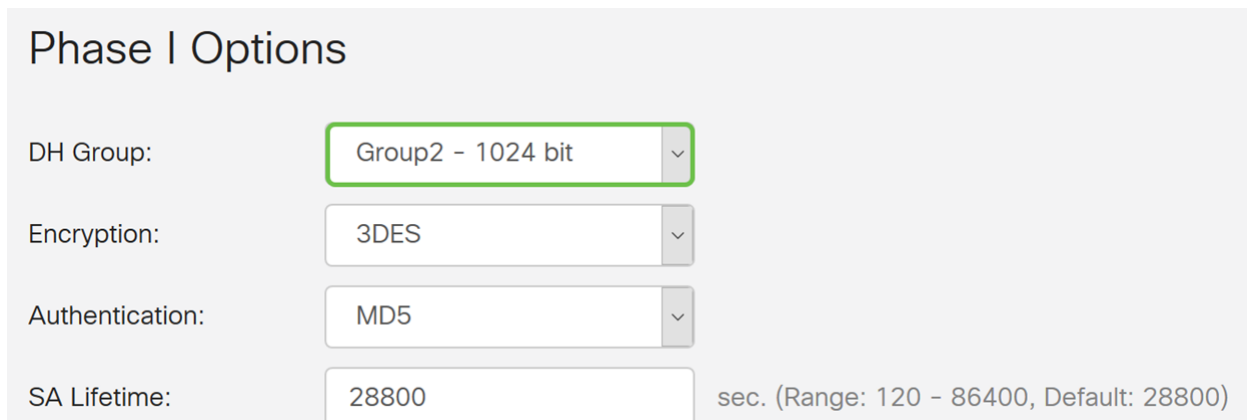
Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

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。在階段I部分，選擇一個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)。

為此演示選擇了組2 - 1024位。

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。



Phase I Options

DH Group:

Encryption:

Authentication:

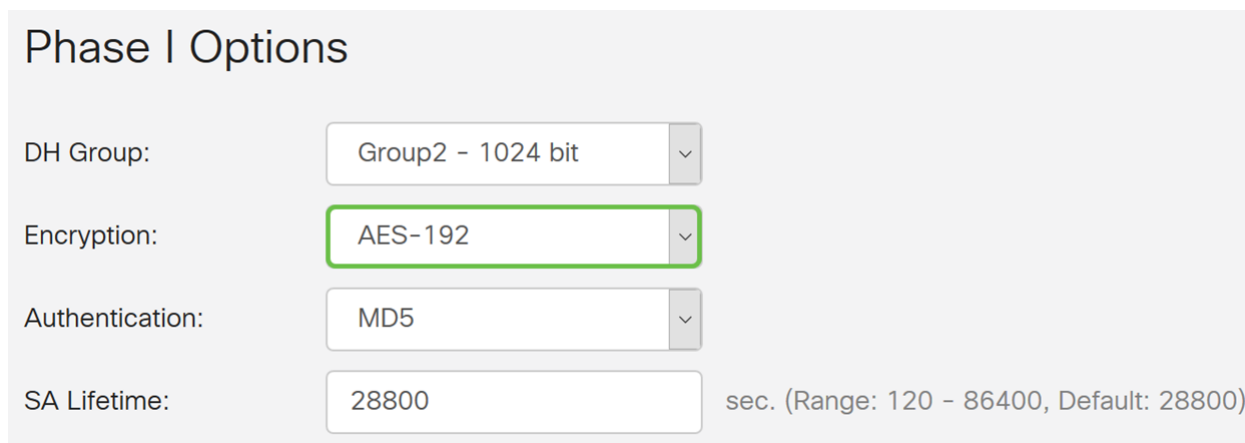
SA Lifetime: sec. (Range: 120 - 86400, Default: 28800)

步驟7.從下拉選單中選擇加密選項(3DS、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，但現在是一個傳統演算法，並且只有在沒有其他替代方案時才應使用，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。如果您的裝置可以支援，建議使用AES。

在本例中，我們選擇**AES-192**作為加密選項。

附註：按一下超連結以瞭解有關[使用IPsec或下一代加密配置VPN安全的更多資訊](#)。

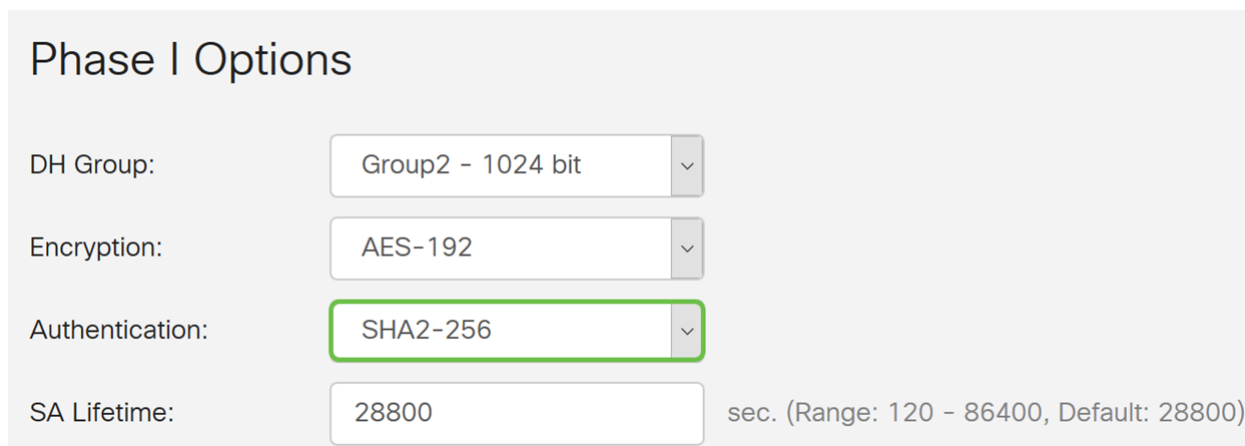


Phase I Options

| | | |
|-----------------|-------------------|---|
| DH Group: | Group2 - 1024 bit | ▼ |
| Encryption: | AES-192 | ▼ |
| Authentication: | MD5 | ▼ |
| SA Lifetime: | 28800 | sec. (Range: 120 - 86400, Default: 28800) |

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。



Phase I Options

| | | |
|-----------------|-------------------|---|
| DH Group: | Group2 - 1024 bit | ▼ |
| Encryption: | AES-192 | ▼ |
| Authentication: | SHA2-256 | ▼ |
| SA Lifetime: | 28800 | sec. (Range: 120 - 86400, Default: 28800) |

步驟9. SA生存期(秒)會顯示IKE SA在此階段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。

Phase I Options

| | | |
|-----------------|-------------------|---|
| DH Group: | Group2 - 1024 bit | ▼ |
| Encryption: | AES-192 | ▼ |
| Authentication: | SHA2-256 | ▼ |
| SA Lifetime: | 28800 | sec. (Range: 120 - 86400, Default: 28800) |

步驟10。在第II階段，您將加密來回傳送的資料。在 *Phase 2 Options* 中，從下拉選單中選擇協定：

- 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。

Phase II Options

| | | |
|--------------------------|--|--|
| Protocol Selection: | ESP | ▼ |
| Encryption: | 3DES | ▼ |
| Authentication: | MD5 | ▼ |
| SA Lifetime: | 3600 | sec. (Range: 120 - 28800, Default: 3600) |
| Perfect Forward Secrecy: | <input checked="" type="checkbox"/> Enable | |
| DH Group: | Group2 - 1024 bit | ▼ |

步驟11.從下拉式清單中選擇加密選項(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-192**作為加密選項。

附註：按一下超連結以瞭解有關[使用IPsec或下一代加密配置VPN安全的更多資訊。](#)

Phase II Options

| | | |
|--------------------------|--|--|
| Protocol Selection: | ESP | ▼ |
| Encryption: | AES-192 | ▼ |
| Authentication: | MD5 | ▼ |
| SA Lifetime: | 3600 | sec. (Range: 120 - 28800, Default: 3600) |
| Perfect Forward Secrecy: | <input checked="" type="checkbox"/> Enable | |
| DH Group: | Group2 - 1024 bit | ▼ |

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。

Phase II Options

| | | |
|--------------------------|--|--|
| Protocol Selection: | ESP | ▼ |
| Encryption: | AES-192 | ▼ |
| Authentication: | SHA2-256 | ▼ |
| SA Lifetime: | 3600 | sec. (Range: 120 - 28800, Default: 3600) |
| Perfect Forward Secrecy: | <input checked="" type="checkbox"/> Enable | |
| DH Group: | Group2 - 1024 bit | ▼ |

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。

Phase II Options

| | | |
|--------------------------|--|--|
| Protocol Selection: | ESP | sec. (Range: 120 - 28800, Default: 3600) |
| Encryption: | AES-192 | |
| Authentication: | SHA2-256 | |
| SA Lifetime: | 3600 | |
| Perfect Forward Secrecy: | <input checked="" type="checkbox"/> Enable | |
| DH Group: | Group2 - 1024 bit | |

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。如果您的裝置可以支援此功能，則建議這樣做。

Phase II Options

| | | |
|--------------------------|--|--|
| Protocol Selection: | ESP | sec. (Range: 120 - 28800, Default: 3600) |
| Encryption: | AES-192 | |
| Authentication: | SHA2-256 | |
| SA Lifetime: | 3600 | |
| Perfect Forward Secrecy: | <input checked="" type="checkbox"/> Enable | |
| DH Group: | Group2 - 1024 bit | |

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」。

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 28800, Default: 3600)

Perfect Forward Secrecy: Enable

DH Group:

步驟16. 按一下Apply新增新的IPsec配置檔案。

IPSec Profiles

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 86400, Default: 28800)

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime: sec. (Range: 120 - 28800, Default: 3600)

Perfect Forward Secrecy: Enable

DH Group:

步驟17. 按一下Apply後，應新增新的IPsec配置檔案。

IPSec Profiles

IPsec Profiles Table

| <input type="checkbox"/> Name | <input type="checkbox"/> IKE Version | <input type="checkbox"/> Policy | <input type="checkbox"/> In Use |
|--|--------------------------------------|---------------------------------|---------------------------------|
| <input type="checkbox"/> Amazon_Web_Services | IKEv1 | Auto | No |
| <input type="checkbox"/> Default | IKEv1 | Auto | Yes |
| <input type="checkbox"/> Microsoft_Azure | IKEv1 | Auto | No |
| <input type="checkbox"/> HomeOffice | IKEv2 | Auto | No |

步驟18.在頁面頂部，按一下**Save**圖示導航到*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19.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。

| Configuration File Name | Last Change Time |
|-------------------------|---------------------------|
| Running Configuration: | 2018-Dec-08, 00:17:01 GMT |
| Startup Configuration: | 2018-Dec-07, 21:54:43 GMT |
| Mirror Configuration: | 2018-Dec-07, 21:54:33 GMT |
| Backup Configuration: | N/A |

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source: Running Configuration 1

Destination: Startup Configuration 2

Save Icon Blinking: Enabled

步驟20.再次執行所有步驟以設定路由器B。

現在，您應該已經成功建立了一個新的IPsec配置檔案，使用IKEv2作為兩台路由器的IKE版本。您已準備好配置站點到站點VPN。