

在RV34x系列路由器上配置客戶端到站點的虛擬專用網路(VPN)連線

目標

在客戶端到站點虛擬專用網路(VPN)連線中，來自Internet的客戶端可以連線到伺服器，以訪問伺服器後面的公司網路或區域網(LAN)，但仍維護網路及其資源的安全。此功能非常有用，因為它建立了一個新的VPN隧道，允許遠端工作人員和商務旅行者使用VPN客戶端軟體訪問您的網路，而不會損害隱私和安全性。

本文檔的目的是向您展示如何在RV34x系列路由器上配置客戶端到站點VPN連線。

適用裝置

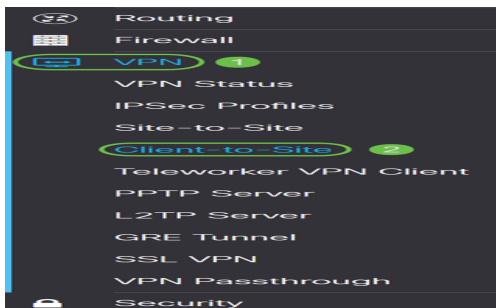
- RV34x系列

軟體版本

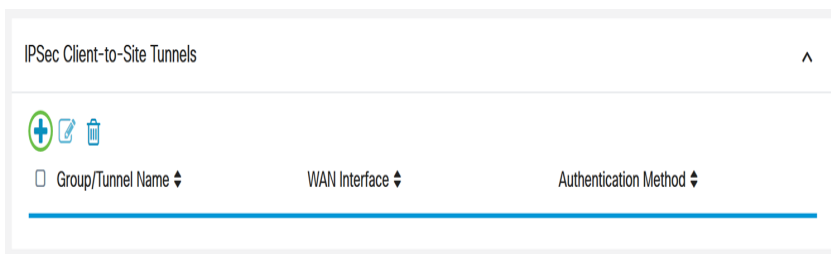
- 1.0.01.16

配置客戶端到站點VPN

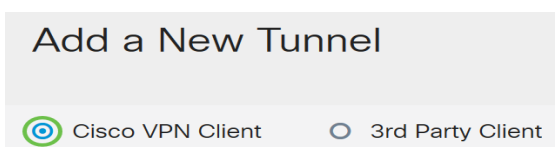
步驟1. 登入到路由器基於Web的實用程式，然後選擇VPN > Client-to-Site。



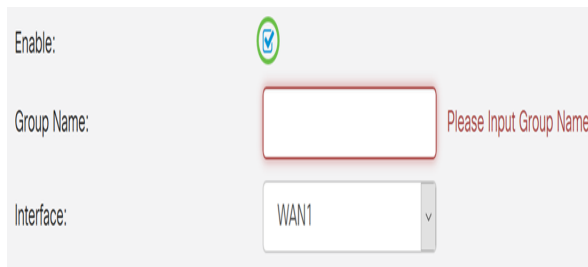
步驟2. 按一下IPSec Client-to-Site Tunnels部分下的Add按鈕。



步驟3. 在Add a New Tunnel區域中，按一下Cisco VPN Client單選按鈕。



步驟4. 勾選**Enable**覈取方塊以啟用組態。

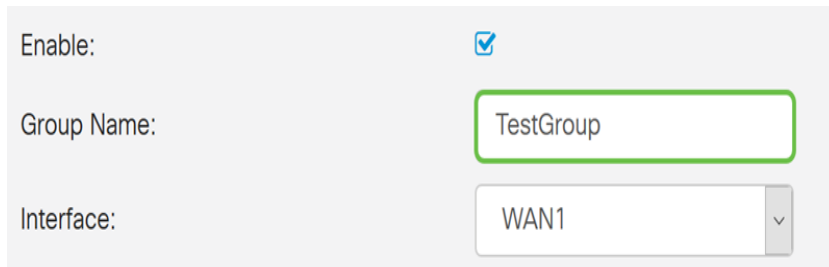


Enable:

Group Name: Please Input Group Name

Interface: WAN1

步驟5. 在所提供的欄位中輸入組名稱。在Internet金鑰交換(IKE)協商過程中，該識別符號將用作此組所有成員的識別符號。



Enable:

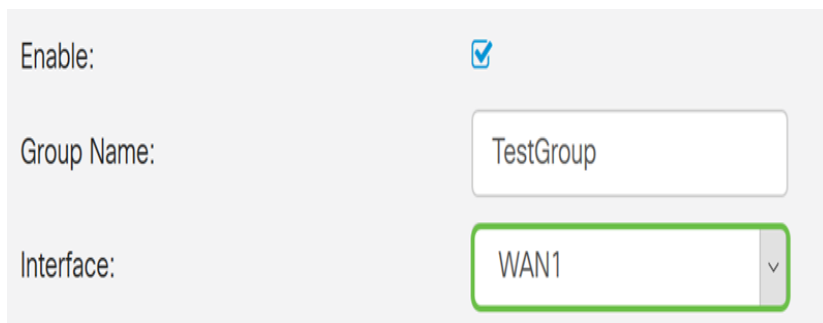
Group Name: TestGroup

Interface: WAN1

附註：輸入介於A到Z或0到9之間的字元。組名稱不允許使用空格和特殊字元。本示例使用TestGroup。

步驟6. 點選下拉選單選擇介面。選項包括：

- WAN1
- WAN2
- USB1
- USB2



Enable:

Group Name: TestGroup

Interface: WAN1


附註：在本示例中，選擇了WAN1。這是預設設定。

步驟7. 在IKE Authentication Method區域中，選擇在基於IKE的隧道中的IKE協商中使用的身份驗證方法。選項包括：

- 預共用金鑰 — IKE對等體通過計算和傳送包含預共用金鑰的資料的金鑰雜湊來相互進行身份驗證。如果接收對等體能夠使用其預共用金鑰獨立建立相同的雜湊，則它知道兩個對等體必須共用相同的金鑰，從而驗證另一個對等體。預共用金鑰不能很好地擴展，因為每個IPSec對等體必須使用與其建立會話的其他對等體的預共用金鑰進行配置。
- 證書(Certificate) — 數位證書是一個包，其中包含諸如持有人的證書標識等資訊：名稱或IP地址、證書的序列號到期日期以及證書持有人的公鑰的副本。標準數位證書格式在X.509規範中定義。X.509版本3定義了憑證的資料結構。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable


Certificate:

附註：在本例中，選擇預共用金鑰。這是預設設定。

步驟8.在提供的欄位中輸入預共用金鑰。這將是IKE對等體組中的身份驗證金鑰。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable


Certificate:

步驟9. (可選) 選中**Enable**覈取方塊，選中Minimum Pre-shared Key Complexity可檢視預共用金鑰強度表，並確定金鑰強度。金鑰的強度定義如下：

- 紅色，密碼很弱。
- 橙色 — 密碼相當強。
- 綠色 — 密碼為強。

IKE Authentication Method

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

附註：您可以選中*Show Pre-shared Key*欄位中的**Enable**覈取方塊，以純文字檔案格式檢查您的密碼。

IKE Authentication Method

Pre-shared Key: 2

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: 1 Enable

Certificate:

步驟10。(可選) 按一下「使用者組」(User Group)表格中的**plus**圖示以新增組。

User Group Table


Group Name 

步驟11。(可選) 從下拉選單中選擇使用者組是用於admin還是用於訪客。如果您使用使用者帳戶建立了自己的使用者組，則可以選擇它。在本例中，我們將選擇TestGroup。

附註： TestGroup是我們在System Configuration > User Groups中建立的使用者組。

User Group Table

Group Name 

TestGroup

Mode: admin

Pool Range: guest

附註： 在本示例中，選擇了TestGroup。您還可以選中使用者組旁邊的框，然後如果要刪除使用者組，請按一下**Delete**按鈕。

步驟12.按一下單選按鈕選擇模式。選項包括：

- 客戶端 — 此選項允許客戶端請求IP地址，伺服器提供已配置地址範圍中的IP地址。
- 網路擴展模式(NEM) — 此選項允許客戶端建議其子網，對於該子網，需要在伺服器後的LAN和客戶端建議的子網之間的流量應用VPN服務。

Mode: Client NEM

附註： 在本例中，選擇了Client。

步驟13.在Start IP欄位中輸入起始IP地址。這是池中第一個可以分配給客戶端的IP地址。

Pool Range for Client LAN

Start IP:

End IP:

附註：本示例使用192.168.100.1。

步驟14.在*End IP*欄位中輸入結尾IP地址。這是池中可分配給客戶端的最後一個IP地址。

Pool Range for Client LAN

Start IP:

End IP:

附註：本例中使用的是192.168.100.100。

步驟15。(可選)在*Mode Configuration*區域下，在提供的欄位中輸入主DNS伺服器的IP地址。

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

附註：本示例使用192.168.1.1。

步驟16。(可選)在提供的欄位中輸入輔助DNS伺服器的IP地址。

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

附註：本示例使用192.168.1.2。

步驟17。(可選)在提供的欄位中輸入主WINS伺服器的IP地址。

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text"/>

附註： 本示例使用192.168.1.1。

步驟18。（可選）在提供的欄位中輸入輔助WINS伺服器的IP地址。

Mode Configuration

Primary DNS Server:	<input type="text" value="192.168.1.1"/>
Secondary DNS Server:	<input type="text" value="192.168.1.2"/>
Primary WINS Server:	<input type="text" value="192.168.1.1"/>
Secondary WINS Server:	<input type="text" value="192.168.1.2"/>

附註： 本示例使用192.168.1.2。

步驟19。（可選）在提供的欄位中輸入要在遠端網路中使用的預設域。

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

附註： 在此示例中，使用sample.com。

步驟20。（可選）在*Backup Server 1*欄位中，輸入備份伺服器的IP地址或域名。如果主IPSec VPN伺服器發生故障，裝置可在此啟動VPN連線。您最多可以在提供的欄位中輸入三個備份伺服器。在三台伺服器中，備份伺服器1的優先順序最高，而備份伺服器3的優先順序最低。

Default Domain:	<input type="text" value="sample.com"/>	
Backup Server 1:	<input type="text" value="example.com"/>	(IP Address or Domain Name)
Backup Server 2:	<input type="text"/>	(IP Address or Domain Name)
Backup Server 3:	<input type="text"/>	(IP Address or Domain Name)

附註： 在此示例中，Example.com用於備份伺服器1。

步驟21。（可選）選中**Split Tunnel**覈取方塊以啟用分割隧道。分割通道允許您同時存取私人網路和Internet的資源。

Split Tunnel:

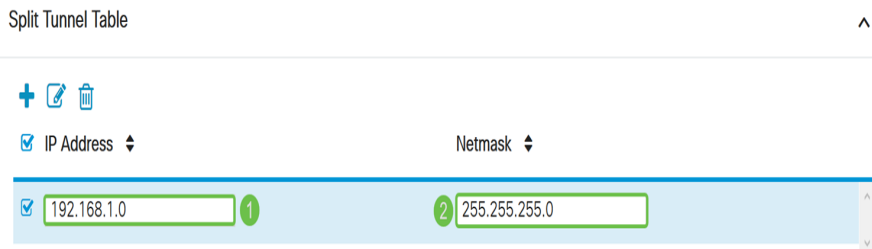


步驟22。(可選)在*Split Tunnel Table*下，按一下**plus**圖示為拆分隧道新增IP地址。

Split Tunnel Table

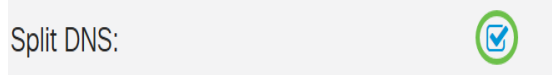


步驟23。(可選)在提供的欄位中輸入拆分隧道的IP地址和網路掩碼。



附註：本範例中使用的是192.168.1.0和255.255.255.0。您還可以選中該框並按一下**Add**、**Edit**和**Delete**按鈕分別新增、編輯或刪除拆分隧道。

步驟24。(可選)選中**Split DNS**竅取方塊以啟用分割DNS。拆分DNS允許您為內部和外部網路建立單獨的DNS伺服器，以維護網路資源的安全和隱私。



步驟25。(可選)按一下*Split DNS Table*下的**plus**圖示為拆分DNS新增域名。

Split DNS Table



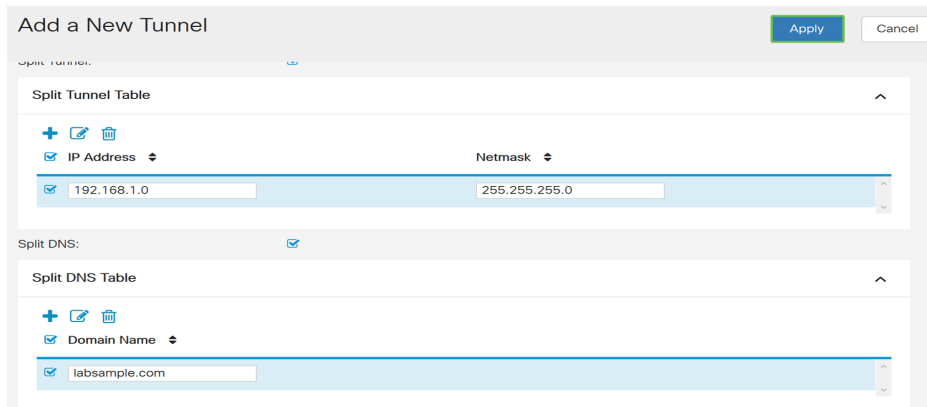
步驟26。(可選)在提供的欄位中輸入拆分DNS的域名。

Split DNS Table



附註：在此示例中，使用labsample.com。您還可以選中該框並按一下**Add**、**Edit**和**Delete**按鈕分別新增、編輯或刪除拆分DNS。

步驟27.按一下**Apply**。



結論

您現在應該已經在RV34x系列路由器上成功配置了客戶端到站點連線。

按一下以下文章以瞭解有關以下主題的詳細資訊：

- [在RV34x系列路由器上配置Teleworker VPN客戶端](#)
- [使用GreenBow VPN客戶端連線RV34x系列路由器](#)
- [為RV34x路由器上的VPN客戶端設定建立使用者帳戶](#)
- [為RV34x路由器上的VPN設定建立使用者組](#)

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](#)