

# 在RV160和RV260系列路由器上配置訪問規則

## 目標

您的路由器負責從外部網路接收資料，並且是您的本地網路安全的第一道防線。通過在路由器上啟用訪問規則，可以根據特定引數（如IP地址或埠號）過濾資料包。透過下列步驟，本文旨在指導您如何設定存取規則，以更好地控制進入網路的封包。本文檔還將重點介紹一些使用訪問規則以實現最佳安全性的最佳實踐。

## 適用裝置

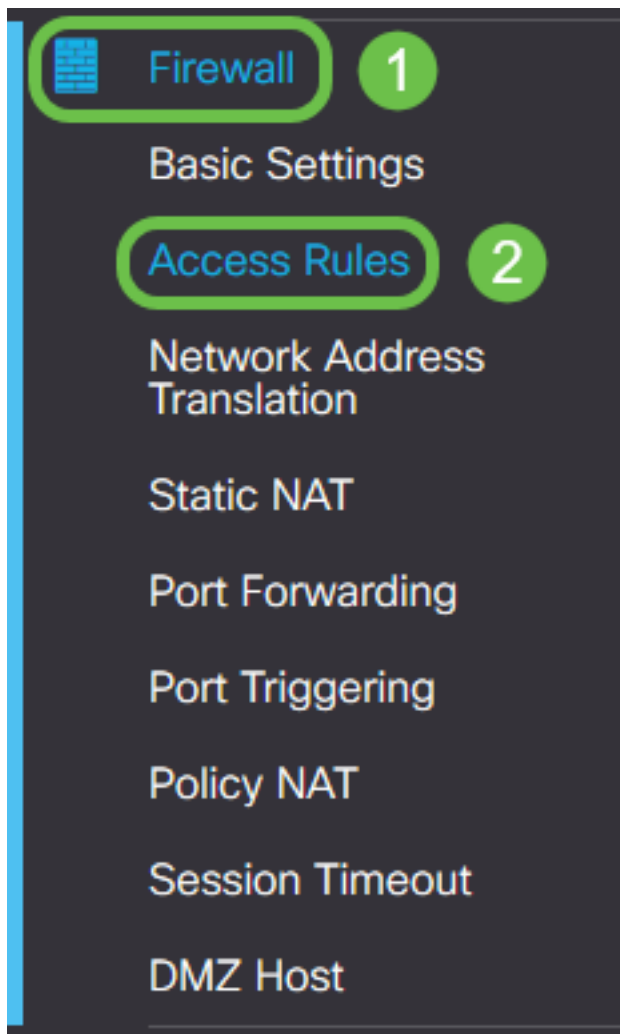
- RV160x
- RV260x

## 軟體版本

- 1.0.00.13

## 配置訪問規則

步驟1. 從配置實用程式左側的導航窗格中，選擇Firewall > Access Rules。



系統將顯示Access Rules頁面。在此頁上有一些表，分別包含IPv4和IPv6的訪問規則及其屬性的清

單。您可以在此處新增新訪問規則、編輯現有規則或刪除現有規則。

## 新增/編輯訪問規則

步驟2.要新增新的訪問規則，請根據要應用規則的協定，在IPv4訪問規則或IPv6訪問規則表中按一下要新增的藍色圖示。此案例使用IPv4。

### IPv4 Access Rules Table



要編輯現有條目，請選中要修改的訪問規則旁邊的覈取方塊。然後選擇相應表格頂部的藍色編輯圖示。一次只能選擇一個規則進行編輯。

### IPv4 Access Rules Table



<input checked="" type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	Any	Any	Any
<input type="checkbox"/>	201	Enabled	Allowed	All Traffic	VLAN	Any	WAN
<input type="checkbox"/>	202	Enabled	Denied	All Traffic	WAN	Any	VLAN

系統將顯示Add/Edit Access Rules頁面。

步驟3.選中/取消選中Rule Status覈取方塊以在操作期間啟用或禁用訪問規則。當您擁有想要儲存以在以後應用的訪問規則時，這很有用。

## Add/Edit Access Rules

Rule Status:  Enable

Action:  Allow  Deny

Services:  IPv4  IPv6 All Traffic

步驟4.在Action欄位中，選擇規則應允許還是拒絕對要指定的傳入網路流量的訪問。

Rule Status:  Enable

Action:  Allow  Deny

Services:  IPv4  IPv6 All Traffic

Log:  Always  Never

Source Interface: Any

**附註：**為了獲得最佳安全性，建議設定僅允許預期接收的流量的訪問規則，而不是嘗試僅拒絕不需要的流量。這將更好地保護您的網路免受未知威脅。

步驟5.在服務欄位中，從下拉選單中選擇您想要應用存取規則的網路服務型別。

## Add/Edit Access Rules

Rule Status:  Enable

Action:  Allow  Deny

Services:  IPv4  IPv6  ▼

Log:  Always  Never

Source Interface:  ▼

**附註：** IPv4或IPv6單選按鈕將根據您在*Access Rules*頁面中選擇要應用訪問規則的表自動選擇。

步驟6. 從*Log*欄位選擇是否希望路由器在進入網路的資料包與應用的規則匹配時生成日誌消息。

Rule Status:  Enable

Action:  Allow  Deny

Services:  IPv4  IPv6  ▼

Log:  Always  Never

Source Interface:  ▼

步驟7. 從*Source Interface*下拉選單中，為訪問規則將應用的傳入資料包選擇網路介面。

Log:  Always  Never

Source Interface: Any

Source Address: WAN  
USB  
VLAN1  
Any

Destination Interface: Any

Destination Address: Any

步驟8.從 *Source Address* 下拉選單中選擇訪問規則將應用的傳入地址型別。選項如下：

- Any — 規則將應用於任何傳入IP地址
- Single — 規則將應用於單個定義的IP地址
- 子網 — 規則將應用於網路的已定義子網
- IP範圍 — 規則將應用於已定義的IP地址範圍

**附註：**如果選擇Single、Subnet或IP Range，相應的欄位將顯示在下拉選單的右側，您可以在其中輸入地址詳細資訊。在此示例中，輸入了一個IP範圍以演示。

Source Interface: Any

Source Address: IP Range 1.2.3.1 To 1.2.3.100 (1.2.3.1 To 1.2.3.4)

Destination Interface: Any  
Single  
Subnet  
IP Range

Destination Address:

步驟9.從 *Destination Interface* 下拉選單中，為訪問規則將應用的傳出資料包選擇網路介面。

Log:  Always  Never

Source Interface: Any

Source Address: Any

Destination Interface: Any

Destination Address: Any

Schedule

步驟10.從*Destination Address* 下拉選單中選擇訪問規則將應用的傳出地址型別。選項如下：

- Any — 規則將應用於任何傳出IP地址
- Single — 規則將應用於單個定義的IP地址
- 子網 — 規則將應用於網路的已定義子網
- IP範圍 — 規則將應用於已定義的IP地址範圍

**附註：**如果選擇Single、Subnet或IP Range，相應的欄位將顯示在下拉選單的右側，您可以在其中輸入地址詳細資訊。在此示例中，輸入子網進行演示。

Destination Interface: Any

Destination Address: Subnet 1.2.3.4 / 16 (1.2.3.4 / 32)

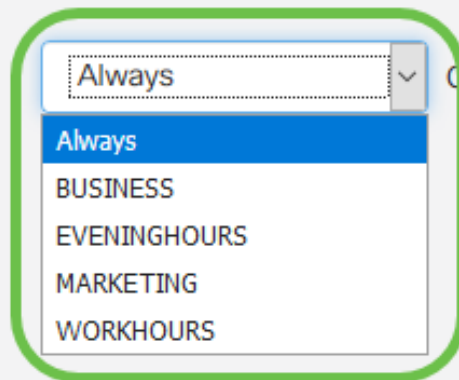
Schedule

Schedule Name: Always Click [here](#) to configure the schedules.

步驟11.從*Schedule Name*下拉選單中，選擇要應用訪問規則的時間計畫。

## Schedule

Schedule Name:

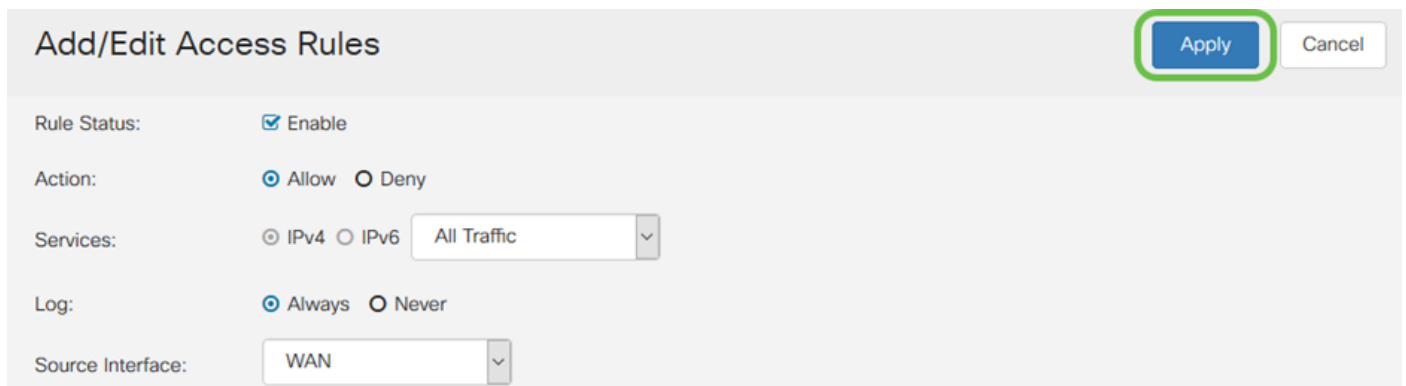


[Click here to configure the schedules.](#)

**附註：**為了提高安全性，最佳實踐是限制非關鍵網路在工作時間訪問，以確保在您的企業未運行時拒絕不需要的連線。

**附註：**如果要為訪問規則配置計畫時間，請按一下 *Schedule Name* 下拉選單右側的連結。有關如何配置這些計畫的詳細資訊，請參閱[此處](#)。

步驟12. 對訪問規則配置感到滿意後，按一下 **Apply** 進行確認。



Add/Edit Access Rules Apply Cancel

Rule Status:  Enable

Action:  Allow  Deny

Services:  IPv4  IPv6  ▼

Log:  Always  Never

Source Interface:  ▼

現在將返回到 *Access Rules* 主頁。

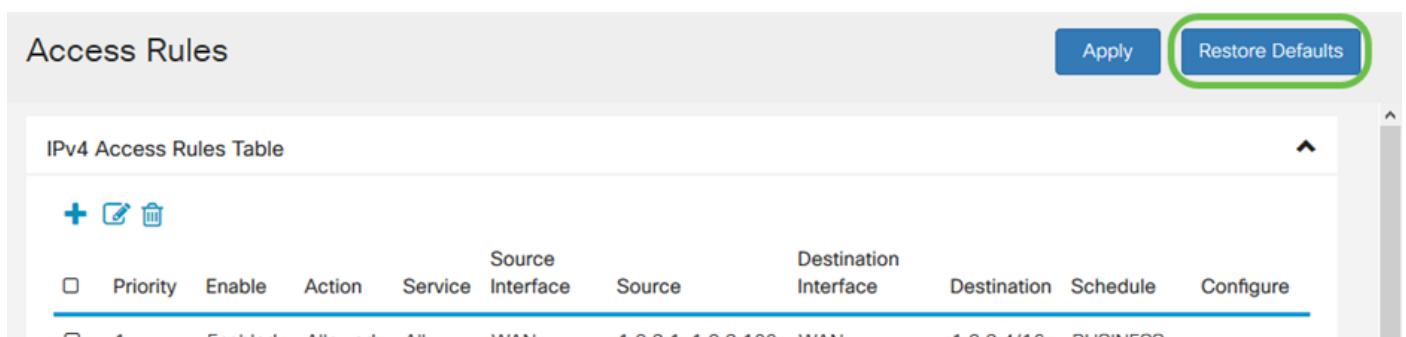
**附註：**當建立新的訪問規則時，其優先順序將置於清單的底部。這意味著如果訪問規則與特定引數上的其他規則衝突，則優先順序較高的規則的限制將優先。要優先向上或向下移動規則，可以使用 *Configure* 列中的藍色箭頭。

IPv4 Access Rules Table ▲



<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	<span>▲</span> <span>▼</span>

步驟13 ( 可選 )。 如果要將訪問規則清單恢復為預設值，請按一下頁面右上角的 **Restore Defaults**。



Access Rules Apply Restore Defaults

IPv4 Access Rules Table ▲

+ ✎ 🗑️

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	

## 刪除訪問規則

步驟14. 要從清單中刪除訪問規則，只需選中您要刪除的相應規則的覈取方塊。然後選擇清單頂部的藍色垃圾桶圖示。可以一次刪除多個訪問規則條目。

IPv4 Access Rules Table

<input type="checkbox"/>	Priority	Enable	Action	Service	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
<input checked="" type="checkbox"/>	1	Enabled	Allowed	All Traffic	WAN	1.2.3.1-1.2.3.100	WAN	1.2.3.4/16	BUSINESS	▲ ▼

## 服務管理

服務管理允許您按現有網路服務的埠號、協定和其他詳細資訊新增或編輯這些服務。配置訪問規則時，這些網路服務將在「服務」下拉選單中可用。通過服務管理清單的配置選單，您可以建立自定義服務，然後這些服務可以應用於訪問規則，以更好地控制進入網路的流量。要詳細瞭解如何配置服務管理，請按一下[此處](#)。

## 結論

適當應用訪問規則是保護WAN連線的寶貴工具。使用上述指南和所討論的方法，您應該擁有為RV160x或RV260x路由器正確配置安全訪問規則所需的一切。