

# 在RV016、RV042、RV042G和RV082 VPN路由器上阻止來自兩個不同網路的Ping資料包的防火牆訪問規則配置

## 目標

一台路由器可能需要兩個不同的網路，才能為與路由器不在同一網路中的裝置提供Internet訪問。這可以通過基於各種標準的訪問規則來實現，以便允許或拒絕對任何網路或IP地址範圍的訪問。訪問規則有助於路由器確定允許哪些流量通過防火牆，也有助於提高路由器的安全性。

本文說明如何通過訪問規則阻止來自RV016、RV042、RV042G和RV082 VPN路由器上兩個不同網路的ping資料包。

## 適用裝置

- RV016
- RV042
- RV042G
- RV082

## 軟體版本

- v4.2.1.02

## 訪問規則配置

步驟 1. 登入到Web配置實用程式，然後選擇Firewall > Access Rules。Access Rules頁面隨即開啟：

Access Rules

IPv4 IPv6

Item 1-3 of 3 Rows per page : 5

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time	Day	Delete
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always		
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always		

Add Restore to Default Rules

Page 1 of 1

步驟 2. 按一下Add新增訪問規則。將開啟Access Rules Services頁面：

Access Rules

Services

Action : Allow

Service : All Traffic [TCP&UDP/1~65535]

Service Management

Log : Log packets match this rule

Source Interface : LAN

Source IP : Single 192.168.0.1

Destination IP : Range 10.10.10.1 to 10.10.10.30

步驟 3. 從Action下拉選單中選擇相應的操作，如果選擇了Allow，則允許流量通過。否則，請選擇Deny以拒絕流量。

步驟 4. 從Service下拉選單中選擇相應的服務。

注意：如果所需服務可用，請跳至步驟10。

步驟 5. 如果相應的服務不可用，請按一下Service Management，此時將顯示Service Management視窗：

Service Name :

Protocol :

Port Range :  to

- All Traffic [TCP&UDP/1~65535]
- DNS [UDP/53~53]
- FTP [TCP/21~21]
- HTTP [TCP/80~80]
- HTTP Secondary [TCP/8080~8080]
- HTTPS [TCP/443~443]
- HTTPS Secondary [TCP/8443~8443]
- TFTP [UDP/69~69]
- IMAP [TCP/143~143]
- NNTP [TCP/119~119]
- POP3 [TCP/110~110]
- SNMP [UDP/161~161]

步驟 6. 在Service Name欄位中輸入所需的服務名稱。

步驟 7. 從Protocol下拉選單中選擇適當的協定型別：

- TCP — 傳輸控制協定是要求有保證傳輸的應用程式使用的協定。
- UDP — 使用者資料包協定使用資料包套接字建立主機到主機的通訊。
- IPv6 — 在資料包中的主機之間引導Internet流量，這些資料包將通過路由地址指定的網路進行路由。

步驟 8. 在Port Range欄位中輸入將應用於服務的埠範圍。

步驟 9.按一下Add to List，將服務新增到Access Rules頁面上的Service下拉選單中。

步驟 10.按一下「OK」以關閉視窗，這樣會將使用者帶回「Access Rules」頁面。

The screenshot shows the 'Access Rules' configuration window. The 'Services' section is expanded, showing a list of services including 'Service Management'. The 'Action' is set to 'Allow', 'Service' is 'All Traffic [TCP&UDP/1~65535]', 'Log' is 'Log packets match this rule', 'Source Interface' is 'LAN', 'Source IP' is 'Single' with '192.168.0.1', and 'Destination IP' is 'Range' with '10.10.10.1 to 10.10.10.30'.

步驟 11.選擇Log packets match this rule，在Log下拉選單中記錄與訪問規則匹配的傳入資料包。

步驟 12.從Source Interface下拉選單中選擇受此規則影響的介面。來源介面是從中啟動流量的介面。

- LAN — 區域網埠連線緊鄰網路（如辦公樓或學校）中的電腦。
- WAN1 — 廣域網埠連線網路上大面積的電腦。這可以是連線一個地區甚至一個國家的任何網路。企業和政府用它來連線其他地點。
- WAN2 — 與埠WAN1相同，只是它是第二個網路。
- DMZ — 允許外部流量訪問網路上的電腦，而不暴露區域網。
- ANY — 允許使用任何介面。

## Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP :   to

步驟 13.從Source IP下拉選單中選擇一個選項來指定網路將用於通過介面的流量的源IP地址：

- Any — 任何IP地址都將用於轉發流量。下拉選單右側沒有任何欄位可用。
- 單一 — 使用單個IP地址轉發流量。在下拉選單右側的欄位中輸入所需的IP地址。
- 範圍 — 範圍IP地址將用於轉發流量。在下拉選單右側的欄位中輸入所需的IP地址範圍。

步驟 14.從Destination IP下拉選單中選擇一個選項，以指定網路將用於通過介面的流量的目標IP地址：

- Any — 任何IP地址都將用於轉發流量。下拉選單右側沒有任何欄位可用。
- 單一 — 使用單個IP地址轉發流量。在下拉選單右側的欄位中輸入所需的IP地址。
- 範圍 — 範圍IP地址將用於轉發流量。在下拉選單右側的欄位中輸入所需的IP地址範圍。

步驟 15.按一下Save以應用設定。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。