

在RV130和RV130W上新增和配置訪問規則

目標

網路裝置提供基本的流量過濾功能和訪問規則。存取規則是存取控制清單(ACL)中的單一專案，它根據通訊協定、來源和目的地IP位址或網路組態來指定允許或拒絕規則（轉送或捨棄封包）。

本文檔的目的是向您展示如何在RV130和RV130W上新增和配置訪問規則。

適用裝置

- RV130
- RV130W

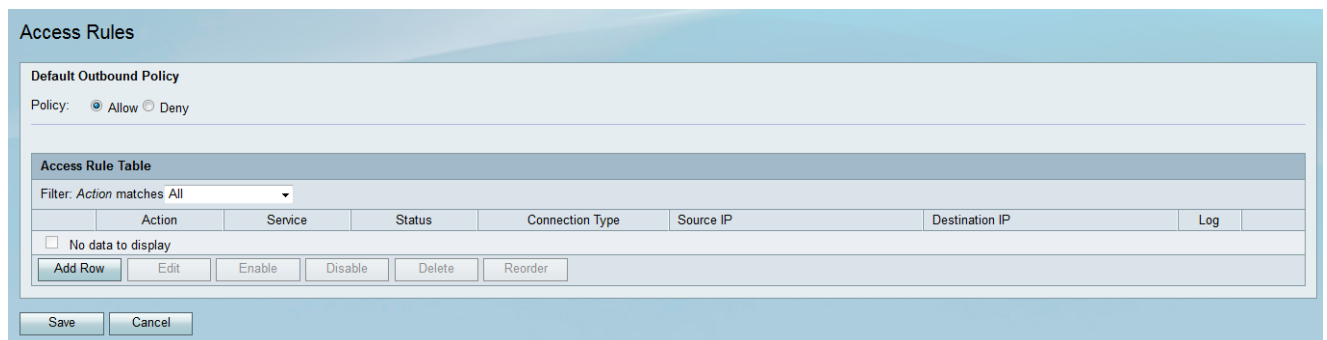
軟體版本

- 版本1.0.1.3

新增和配置訪問規則

設定預設出站策略

步驟1.登入到Web配置實用程式並選擇**Firewall > Access Rules**。*Access Rules*頁面隨即開啟：



The screenshot shows the 'Access Rules' configuration page. At the top, there is a section for 'Default Outbound Policy' with a radio button for 'Allow' selected and 'Deny' unselected. Below this is the 'Access Rule Table' section, which includes a filter dropdown set to 'Action matches All'. The table has columns for Action, Service, Status, Connection Type, Source IP, Destination IP, and Log. Below the table, there are buttons for 'Add Row', 'Edit', 'Enable', 'Disable', 'Delete', and 'Reorder'. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

步驟2.在*Default Outbound Policy*區域中，按一下所需的單選按鈕為出站流量選擇策略。當沒有配置任何訪問規則或Internet訪問策略時，應用該策略。預設設定為**Allow**，允許所有到Internet的流量通過。

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

可用選項定義如下：

- 允許 — 允許所有型別的流量從LAN傳到Internet。
- 拒絕 — 阻止所有型別的流量從LAN傳到Internet。

步驟3.按一下**Save**以儲存設定。

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

新增訪問規則

步驟1.登入到Web配置實用程式並選擇**Firewall > Access Rules**。Access Rules視窗開啟：

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

No data to display

步驟2.按一下Access Rule Table中的**Add Row**以新增新的訪問規則。

Access Rules

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

Action	Service	Status	Connection Type	Source IP	Destination IP	Log
No data to display						

將開啟Add Access Rule頁面：

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步驟3.從Connection Type下拉選單中，選擇規則適用的流量型別。

Connection Type: Outbound (LAN > WAN) ▾
Outbound (LAN > WAN)
Inbound (WAN > LAN)
Inbound (WAN > DMZ)

Action:

Schedule: ▾

Services: All Traffic ▾

Source IP: Any ▾

Start:

Finish:

可用選項定義如下：

- 傳出(LAN > WAN) — 規則影響來自本地網路(LAN)並傳出到網際網路(WAN)的資料包。
- 入站(WAN > LAN) — 規則影響來自Internet(WAN)並進入本地網路(LAN)的資料包。
- 傳入(WAN > DMZ) — 規則影響來自網際網路(WAN)並進入非軍事區(DMZ)子網的資料包。

步驟4.從Action下拉選單中，選擇匹配規則時要執行的操作。

Connection Type: Outbound (LAN > WAN) ▾

Action: Always block ▾

Schedule: Schedules

Services: Configure Services

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用選項定義如下：

- 始終阻止 — 如果條件匹配，則始終拒絕訪問。跳至步驟6。
- 始終允許 — 如果條件匹配，則始終允許訪問。跳至步驟6。
- 按計畫阻止 — 如果在預配置的計畫期間條件匹配，則拒絕訪問。
- 按時間表允許 — 如果在預配置的計畫期間條件匹配，則允許訪問。

步驟5.如果您在步驟4中選擇了按進度表阻止或按進度表允許，請從Schedule下拉選單中選擇相應的進度表。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: test_schedule_1 ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

附註：要建立或編輯排程，請按一下配置排程。如需詳細資訊和准則，請參閱[在RV130和RV130W上設定時間表](#)。

步驟6.從服務下拉選單中選擇訪問規則適用的服務型別。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services:

- All Traffic ▾
- All Traffic
- DNS
- FTP
- HTTP
- HTTP Secondary
- HTTPS
- HTTPS Secondary
- TFTP
- IMAP
- NNTP
- POP3
- SNMP
- SMTP
- TELNET
- TELNET Secondary
- TELNET SSL
- Voice(SIP)

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

附註：如果要新增或編輯服務，請按一下配置服務。如需詳細資訊和准則，請參閱[RV130和RV130W上的服務管理組態](#)。

為出站流量配置源和目標IP

如果在新增訪問規則的第3步中選擇了出站(LAN > WAN)作為連線型別，請按照本節中的步驟操作。

附註：如果在新增訪問規則的步驟3中選擇了入站連線型別，請跳至下一部分：[為入站流量配置源和目標IP](#)。

步驟1。從Source IP下拉選單中選擇要定義源IP的方式。對於出站流量，來源IP是指防火牆規則將應用的一個或多個地址（在LAN中）。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Any ▾
Any
Single Address
Address Range

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用選項定義如下：

- Any — 適用於來自本地網路中任何IP地址的流量。因此，請將*Start*和*Finish*欄位留空。如果選擇此選項，請跳至步驟4。
- 單個地址 — 適用於來自本地網路中單個IP地址的流量。在*Start*欄位中輸入IP地址。
- 地址範圍 — 適用於來自本地網路中IP地址範圍的流量。在*開始*欄位中輸入範圍的開始IP地址，在*完成*欄位中輸入結束IP地址以設定範圍。

步驟2.如果您在步驟1中選擇了**單個地址**，請在*開始*欄位中輸入要應用於訪問規則的IP地址，然後跳至步驟4。如果您在步驟1中選擇了**地址範圍**，請在*開始*欄位中輸入要應用於訪問規則的開始IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Single Address ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步驟3.如果您在步驟1中選擇了**地址範圍**，請在**完成欄位**中輸入用於封裝訪問規則的IP地址範圍的結束IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

步驟4.從**Destination IP**下拉選單中選擇要定義目標IP的方式。對於出站流量，目標IP是指本地網路中允許或拒絕流量的地址（在WAN中）。

Connection Type:	Outbound (LAN > WAN) ▾	
Action:	Allow by schedule ▾	
Schedule:	test_schedule ▾	<input type="button" value="Configure Schedules"/>
Services:	VOIP ▾	<input type="button" value="Configure Services"/>
Source IP:	Address Range ▾	
Start:	<input type="text" value="10.10.14.100"/>	(Hint: 192.168.1.100)
Finish:	<input type="text" value="10.10.14.175"/>	(Hint: 192.168.1.200)
Destination IP	Any ▾	
Start:	<input type="text"/>	
Finish:	<input type="text"/>	
Log:	Never ▾	
Rule Status:	<input type="checkbox"/> Enable	

可用選項定義如下：

- Any — 適用於流向公共Internet中任何IP地址的流量。因此，請將*Start*和*Finish*欄位留空。
- 單一地址 — 適用於通向公共Internet中單個IP地址的流量。在*Start*欄位中輸入IP地址。
- 地址範圍 — 適用於流向公共Internet中一系列IP地址的流量。在*開始*欄位中輸入範圍的開始IP地址，在*完成*欄位中輸入結束IP地址以設定範圍。

步驟5.如果您在步驟4中選擇了**Single Address**，請在*Start*欄位中輸入將應用於訪問規則的IP地址。如果您在**步驟4**中選擇了地址範圍(Address Range)，請在*Start*欄位中輸入將應用於訪問規則的起始IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Single Address ▾

Start: 192.168.1.100

Finish:

Log: Never ▾

Rule Status: Enable

步驟6.如果您在步驟4中選擇了地址範圍，請在完成欄位中輸入用於封裝訪問規則的IP地址範圍的結束IP地址。

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

配置入站流量的源和目標IP

如果在[新增訪問規則](#)的步驟3中選擇了入站(WAN > LAN)或入站(WAN > DMZ)作為連線型別，請按照本節中的步驟操作。

步驟1。從Source IP下拉選單中選擇要定義源IP的方式。對於入站流量，源IP是指應用防火牆規則的一個或多個地址（在WAN中）。

Connection Type: Inbound (WAN > LAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: All Traffic ▾

Source IP: Any ▾

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP: Any ▾

Start:

Finish:

Log: Never ▾

Rule Status: Enable

可用選項定義如下：

- Any — 適用於源自公共Internet中任何IP地址的流量。因此，請將*Start*和*Finish*欄位留空。如果選擇此選項，請跳至步驟4。
- 單個地址 — 適用於來自公共Internet中單個IP地址的流量。在*Start*欄位中輸入IP地址。
- 地址範圍 — 適用於源自公共Internet中一系列IP地址的流量。在*開始*欄位中輸入範圍的開始IP地址，在*完成*欄位中輸入結束IP地址以設定範圍。

步驟2.如果您在步驟1中選擇了**單個地址**，請在*開始*欄位中輸入要應用於訪問規則的IP地址，然後跳至步驟4。如果您在步驟1中選擇了**地址範圍**，請在*開始*欄位中輸入要應用於訪問規則的開始IP地址。

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

步驟3.如果您在步驟1中選擇了**地址範圍**，請在**完成**欄位中輸入用於封裝訪問規則的IP地址範圍的結束IP地址。

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

步驟4.在**Destination IP**下拉選單下方的**Start**欄位中輸入目標IP的單個地址。對於入站流量，目標IP是指允許或拒絕來自公共Internet的流量的地址（在LAN中）。

Connection Type:

Action:

Schedule:

Services:

Source IP:

Start: (Hint: 192.168.1.100)

Finish: (Hint: 192.168.1.200)

Destination IP:

Start:

Finish:

Log:

Rule Status: Enable

附註：如果在新增訪問規則的步驟3中選擇了入站(WAN > DMZ)作為連線型別，則目標IP的單個地址將自動配置為啟用的DMZ主機的IP地址。

記錄和啟用訪問規則

步驟1。如果您希望路由器在資料包與規則匹配時建立日誌，請在Log下拉選單中選擇Always。如果希望匹配規則時永不進行記錄，請選擇Never。

Start:

Finish:

Log:

Rule Status: Enable

步驟2.選中Enable 覈取方塊以啟用訪問規則。

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

步驟3.按一下**Save**以儲存設定。

Add Access Rule

Connection Type: Outbound (LAN > WAN) ▾

Action: Allow by schedule ▾

Schedule: test_schedule ▾

Services: VOIP ▾

Source IP: Address Range ▾

Start: 10.10.14.100 (Hint: 192.168.1.100)

Finish: 10.10.14.175 (Hint: 192.168.1.200)

Destination IP: Address Range ▾

Start: 192.168.1.100

Finish: 192.168.1.170

Log: Never ▾

Rule Status: Enable

訪問規則表將使用新配置的訪問規則進行更新。

Access Rules



Configuration settings have been saved successfully

Default Outbound Policy

Policy: Allow Deny

Access Rule Table

Filter: Action matches All

	Action	Service	Status	Connection Type	Source IP	Destination IP	Log
<input type="checkbox"/>	Allow by schedule	VOIP	Enabled	Outbound (LAN > WAN)	10.10.14.100 ~ 10.10.14.175	192.168.1.100 ~ 192.168.1.170	Never

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）。