RV320和RV325 VPN路由器上的訪問規則配置

目標

存取控制清單(ACL)是封鎖或允許流量從某些使用者傳送過來的清單。可以將Access Rules配置為 始終生效或基於定義的計畫。根據各種標準配置訪問規則,以便允許或拒絕對網路的訪問。訪問規 則根據訪問規則需要應用到路由器的時間進行排程。本文概述並描述了用於確定是否允許流量通過 路由器的防火牆進入網路以確保網路安全的訪問規則設定嚮導。

適用裝置 | 韌體版本

- RV320 Dual WAN VPN路由器 | 1.1.0.09版(下載<u>最新版</u>)
- RV325 Gigabit Dual WAN VPN路由器 | 1.1.0.09版(下載<u>最新版</u>)

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。將開啟訪問規則頁:

Access	ccess Rules								
IPv4 IP	v6								
Access	Rules Table							Items 1-5 of 5	5 -
	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time Day	
0		V	Allow	All Traffic [1]	LAN	Any	Any	Always	
0		V	Deny	All Traffic [1]	USB1	Any	Any	Always	
0		V	Deny	All Traffic [1]	USB2	Any	Any	Always	
0		\checkmark	Deny	All Traffic [1]	WAN1	Any	Any	Always	
0			Deny	All Traffic [1]	WAN2	Any	Any	Always	
Add	Edit Delete	Restore to Defa	ult Rules S	ervice Management				Page 1 🔻 of	1 🕨 🕨

訪問規則表包含以下資訊:

- 優先順序 顯示訪問規則的優先順序
- Enable 顯示是否啟用或禁用訪問規則
- Action 顯示允許或拒絕訪問規則。
- •服務 顯示服務型別。
- SourceInterface 顯示訪問規則應用於哪個介面。
- 源 顯示源裝置的IP地址
- 目標 顯示目標裝置的IP地址
- 時間 顯示應用訪問規則的時間
- 天 在一週內應用訪問規則時顯示

服務管理

步驟1.按一下Service Management新增新服務。將開啟Service Management表頁:

Servi	ce Management Table		ltems1-5 of 21 5 ▼ per page
	Service Name	Protocol	Port Range
	All Traffic	TCP&UDP	1~65535
	DNS	UDP	53~53
	FTP	TCP	21~21
	HTTP	TCP	80~80
	HTTP Secondary	TCP	8080~8080
Add	Edit Delete		📕 🛃 Page 1 🔻 of 5 🕨 🕨

步驟2.按一下Add新增新服務。

Servi	ice Management Table		Items1-5 of 21 5 ▼ per page
	Service Name	Protocol	Port Range
	All Traffic	TCP&UDP	1~65535
	DNS	UDP	53~53
	FTP	TCP	21~21
	HTTP	TCP	80~80
	HTTP Secondary	TCP	8080~8080
	Database	TCP 🔻	520 ~ 520
Add	Edit Delete		M Page 1 - of 5
Save	e Cancel		

步驟3.配置以下欄位。

- •服務名稱 根據您的要求,為服務指定一個名稱
- Protocol 為您的服務選擇協定TCP或UDP
- 埠範圍 根據您的要求輸入埠號範圍,埠號必須在範圍(1-65536)內。

步驟4.按一下Save以儲存變更

IPv4上的存取規則組態

Ac	Access Rules									
	Access Rules Table Items 1-5 of 5 🔻 per pag								5 🔻 perpage	
		Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
			√	Allow	All Traffic [1]	LAN	Any	Any	Always	
				Deny	All Traffic [1]	USB1	Any	Any	Always	
			V	Deny	All Traffic [1]	USB2	Any	Any	Always	
			1	Deny	All Traffic [1]	WAN1	Any	Any	Always	
			V	Deny	All Traffic [1]	WAN2	Any	Any	Always	
	Add	Edit Delete	Restore to Def	fault Rules	Service Management				🛃 🗹 Page	e 1 🔻 of 1 🕨 💌

步驟1.按一下Add配置新的訪問規則。將出現Edit Access Rules視窗。

Edit Access Rules			
Services			
Action:	Allow		
Service:	Allow Deny TCP&UDP/1~65535]		
Log:	No Log 🗸		
Source Interface:	LAN 👻		
Source IP:	ANY -		
Destination IP:	ANY -		
Scheduling			
Time:	Always 👻		
From:	(hh:mm)		
To:	(hh:mm)		
Effective on:	🗹 Everyday 🗌 Sun 🗌 Mon 🗌 Tue 🗌 Wed 🗌 Thu 🗌 Fri 🗌 Sat		
Save Car	ncel Back		

步驟2.從「操作」下拉選單中選擇相應的選項,以允許或限制要設定的規則的流量。訪問規則根據 各種值限制對網路的訪問。

- Allow 允許所有流量。
- 拒絕 限制所有流量。

Services		
Action:	Allow 🔻	
Service:	All Traffic [TCP&UDP/1~65535]	•
Log:	All Traffic [TCP&UDP/1~65535] DNS [UDP/53~53] ETP [TCP/21~21]	
Source Interface:	HTTP [TCP/80~80] HTTP Secondary [TCP/8080~8080]	
Source IP:	HTTPS [TCP/443~443] HTTPS Secondary [TCP/8443~8443]	
Destination IP:	TFTP [UDP/69~69] IMAP [TCP/143~143] NNTP [TCP/119~119]	
Scheduling	POP3 [TCP/110~110] SNMP [UDP/161~161] SMTP [TCP/25~25]	
Time:	TELNET [TCP/23~23] TELNET Secondary [TCP/8023~8023]	
From:	DHCP [UDP/67~67] L2TP [UDP/1701~1701]	
To:	PPTP [TCP/1723~1723] IPSec [UDP/500~500]	
Effective on:	Ping [ICMP/255~255]	J 🗌 Thu 🗌 Fri 🗌 S

步驟3.從Service下拉選單中選擇需要過濾的適當服務。

Edit Access Rules			
Services			
Action:	Allow 🔻		
Service:	All Traffic [TCP&UDP/1~65535]		
Log:	Log packets matching this rule 👻		
Source Interface:	No Log Log packets matching this rule		
Source IP:	ANY -		
Destination IP:	ANY -		
Scheduling			
Time:	Always -		
From:	(hh:mm)		
To:	(hh:mm)		
Effective on:	🗹 Everyday 🗌 Sun 🗌 Mon 🗌 Tue 🗌 Wed 🗌 Thu 🗌 Fri 🗌 Sat		
Save Car	ncel Back		

步驟4.從Log下拉選單中選擇適當的Log選項。log選項確定裝置是否保留與訪問規則集對應的流量日 誌。

•記錄與此訪問規則匹配的資料包 — 路由器會保留跟蹤所選服務的日誌。

• 未記錄 — 路由器不保留訪問規則的日誌。

Edit Access Rules			
Services			
Action:	Allow -		
Service:	All Traffic [TCP&UDP/1~65535]		
Log:	Log packets matching this rule 💌		
Source Interface:	LAN 👻		
Source IP:	LAN WAN1		
Destination IP:	WAN2 USB 1 USB 2 ANY		
Scheduling			
Time:	Always 🔻		
From:	(hh:mm)		
To:	(hh:mm)		
Effective on:	Everyday Sun Mon Tue Wed Thu Fri Sat		
Save Ca	ncel Back		

步驟5.從Interface下拉選單中,選擇適當的源介面。此介面是執行訪問規則的地方。

- LAN 訪問規則僅影響LAN流量。
- WAN 1 訪問規則僅影響WAN 1流量。
- WAN 2 訪問規則僅影響WAN 2流量。
- Any 訪問規則會影響裝置的任何介面中的所有流量。

Edit Access Rules			
Services			
Action:	Allow -		
Service:	All Traffic [TCP&UDP/1~65535]		
Log:	Log packets matching this rule 🔻		
Source Interface:	LAN -		
Source IP:	ANY -		
Destination IP:	ANY Single Range		
Scheduling			
Time:	Always -		
From:	(hh:mm)		
To:	(hh:mm)		
Effective on:	🗹 Everyday 🗌 Sun 🗌 Mon 🗌 Tue 🗌 Wed 🗌 Thu 🗌 Fri 🗌 Sat		
Save Ca	ncel Back		

步驟6.從Source IP下拉選單中選擇將訪問規則應用到的適當源IP型別。

- Any 裝置網路的任何IP地址都應用了規則。
- 單一 只有裝置網路上的一個指定IP地址應用了該規則。在相鄰欄位中輸入所需的IP地址。
- 範圍 只有裝置網路上的指定IP地址範圍才應用規則。如果選擇Range,則需要在相鄰的欄位 中輸入該範圍的第一個和最後一個IP地址。

Services	
Action:	Allow 👻
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Log packets matching this rule 🔻
Source Interface:	LAN 👻
Source IP:	Range - 192.168.1.10 To 192.168.1.100
Destination IP:	ANY ANY Single Range
Time:	Always 🔻
From:	(hh:mm)
To:	(hh:mm)
Effective on:	Everyday Sun Mon Tue Wed Th

步驟7.從可用下拉選單中選擇將訪問規則應用到的適當目標IP型別。

- Any 任何目標IP地址都應用了規則。
- 單個 只有單個指定的IP地址應用了規則。在相鄰欄位中輸入所需的IP地址。
- 範圍 只有裝置網路外部的指定IP地址範圍才應用規則。如果選擇Range,則需要在相鄰的欄 位中輸入該範圍的第一個和最後一個IP地址。

- 0 <u>-</u>	
Scheduling	
Time:	Always 👻
From:	Always Interval (hh:mm)
To:	(hh:mm)
Effective on:	🗹 Everyday 🗌 Sun 🗌 Mon 🗌 Tue 🗌 Wed 🗌 Thu 🗌 Fri 🗌 Sat
Save	Cancel Back

Timesaver:預設情況下,時間設定為「始終」。如果要將訪問規則應用於特定時間或日期,請執行 步驟8至步驟11。否則,請跳至步驟12。

步驟8.從下拉選單中選擇Interval,訪問規則在特定時間處於活動狀態。您需要輸入實施訪問規則的時間間隔。

Scheduling Time:	Interval 🔻
From: To:	3:00 (hh:mm) 7:00 (hh:mm)
Effective on:	Everyday Sun Mon Tue Wed Thu Fri Sat
Save Ca	ncel Back

步驟9.在「自」欄位中輸入開始應用訪問清單的時間。時間格式為hh:mm。

步驟10.在「至」欄位中輸入您不再應用訪問清單的時間。時間格式為hh:mm。

Scheduling	
Time:	Interval 🔻
From:	3:00 (hh:mm)
To:	7:00 (hh:mm)
Effective on:	🗹 Everyday 🗌 Sun 🗌 Mon 🗌 Tue 🗌 Wed 🗌 Thu 🗌 Fri 🗌 Sat
Save Ca	ancel Back

步驟11.選中要應用訪問清單的特定日期的覈取方塊。

步驟12.按一下Save以儲存變更。

A	CCESS F Pv4 IPv	Rules ¹⁶								
	Access	Rules Table							Items	s 1-5 of 6 5 🔻
		Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
	٥	1 🕶		Allow	All Traffic [1]	LAN	192.168.1.10 ~ 192.168.1.100			All week
			\checkmark	Allow	All Traffic [1]	LAN	Any	Any	Always	
			\checkmark	Deny	All Traffic [1]	USB1	Any	Any	Always	
			\checkmark	Deny	All Traffic [1]	USB2	Any	Any	Always	
				Deny	All Traffic [1]	WAN1	Any	Any	Always	
	Add	Edit De	lete Restore	to Default Rules	Service Man	agement			📕 🛃 Page	1 🔻 of 2 🕨 💌

步驟13。(可選)如果要恢復預設規則,請按一下**Restore to Default Rules**。您配置的所有訪問規 則都將丟失。

IPv6上的訪問規則配置

Access R	tules								
Access R	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day perpage
0		1	Allow	All Traffic [1]	LAN	Any	Any	Always	
0			Deny	All Traffic [1]	USB1	Any	Any	Always	
0		V	Deny	All Traffic [1]	USB2	Any	Any	Always	
0		V	Deny	All Traffic [1]	WAN1	Any	Any	Always	
0		V	Deny	All Traffic [1]	WAN2	Any	Any	Always	
Add	Edit Delete	Restore to	Default Rules	Service Management				Pa	age 1 🔻 of 1 🕨 💌

步驟1.按一下IPv6頁籤配置IPv6訪問規則。

Acce	ess Rules								
Ac	ccess Rules Table							Items 1-5 of	f5 5 🔻 perpage
	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time	Day
(V	Allow	All Traffic [1]	LAN	Any	Any	Always	
(Deny	All Traffic [1]	USB1	Any	Any	Always	
e			Deny	All Traffic [1]	USB2	Any	Any	Always	
($\overline{\mathbf{v}}$	Deny	All Traffic [1]	WAN1	Any	Any	Always	
(V	Deny	All Traffic [1]	WAN2	Any	Any	Always	
A	dd Edit Delete	Restore to De	fault Rules	Service Management				🛃 🗹 Pa	ige 1 🔻 of 1 🕨 💌

步驟2.單擊Add新增新的IPv6訪問規則。將出現Edit Access Rules視窗。

Edit Access Rules	
Services	
Action:	Allow -
Service:	Deny [TCP&UDP/1~65535]
Log:	No Log 🔻
Source Interface:	LAN 👻
Source IP / Prefix Length:	ANY -
Destination IP / Prefix Length:	ANY -
Save Cancel	Back

步驟3.從「活動」下拉選單中選擇相應的選項,以允許或限制您需要設定的規則。 訪問規則通過允 許或拒絕來自特定服務或裝置的流量訪問來限制對網路的訪問。

- Allow 允許所有流量。
- 拒絕 限制所有流量。

Edit Access Rules	
Services	
Action:	Allow 🔫
Service:	All Traffic [TCP&UDP/1~65535]
Log:	All Traffic [TCP&UDP/1~65535] DNS [UDP/53~53]
Source Interface:	FTP [TCP/21~21] HTTP [TCP/80~80]
Source IP / Prefix Length:	HTTP Secondary [TCP/8080~8080] HTTPS [TCP/443~443]
Destination IP / Prefix Length:	HTTPS Secondary [TCP/8443~8443] TFTP [UDP/69~69] IMAP ITCP/143~143]
	NNTP [TCP/143~143]
Save Cancel	SNMP [UDP/161~161]
	TELNET [TCP/25~25]
	TELNET Secondary [TCP/8023~8023] TELNET SSL [TCP/992~992]
	DHCP [UDP/67~67] L2TP [UDP/1701~1701]
	PPTP [TCP/1723~1723]
	Ping [ICMP/255~255] data ITCP/520~5211

步驟4.從「服務」下拉選單中選擇需要過濾的相應服務。

附註:若要允許所有流量,如果操作已設定為「允許」,請從服務下拉選單中選擇All Traffic [TCP&UDP/1~65535]。該清單包含您可能要過濾的所有型別的服務。

Edit Access Rules	
Services	
Action:	Allow -
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Enabled -
Source Interface:	Enabled
Source IP / Prefix Length:	ANY -
Destination IP / Prefix Length:	ANY -
Save Cancel	Back

步驟5.從Log下拉選單中選擇適當的Log選項。log選項確定裝置是否保留與訪問規則集對應的流量日誌。

- •已啟用 使路由器能夠保持對所選服務的日誌跟蹤。
- Not Log 禁用路由器以保持日誌跟蹤。

Edit Access Rules	
Services	
Action:	Allow -
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Enabled -
Source Interface:	
Source IP / Prefix Length:	LAN WAN1
Destination IP / Prefix Length:	ANY
Save Cancel	Back

步驟6.點選Interface下拉選單並選擇適當的源介面。此介面是執行訪問規則的地方。

- LAN 訪問規則僅影響LAN流量。
- WAN 1 訪問規則僅影響WAN 1流量。
- WAN 2 訪問規則僅影響WAN 2流量。
- Any 訪問規則會影響裝置的任何介面中的所有流量。

Edit Access Rules	
Services	
Action:	Allow 🔻
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Enabled -
Source Interface:	LAN 🔻
Source IP / Prefix Length:	ANY
Destination IP / Prefix Length:	ANY Single Subnet
Save Cancel	Back

步驟7.從Source IP/ Prefix Length下拉選單中選擇將訪問規則應用到的適當源IP型別。

• ANY — 從裝置網路接收的任何資料包都應用了規則。

Edit Access Rules	
Services	
Action:	Allow -
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Enabled -
Source Interface:	LAN -
Source IP / Prefix Length:	Single - 2607:f0d0:1002:51::4 / 128
Destination IP / Prefix Length:	ANY -
Save Cancel	Back

• 單個 — 只有裝置網路中的單個指定IP地址應用了規則。在相鄰欄位中輸入所需的IPv6地址。

Edit Access Rules	
Services	
Action:	Allow -
Service:	All Traffic [TCP&UDP/1~65535]
Log:	Enabled -
Source Interface:	LAN -
Source IP / Prefix Length:	Subnet - 2607:f0d0:1002:51::4 / 45
Destination IP / Prefix Length:	ANY 🔻
Save Cancel	Back

o

• 子網 — 只有子網的IP地址才應用規則。在相鄰欄位中輸入所需子網的IPv6網路地址和字首長度

ction: Allow =
Allow +
vice: All Traffic [TCP&UDP/1~65535]
j: Enabled -
Source Interface: LAN -
Source IP / Prefix Length: Subnet - 2607:f0d0:1002:51::4
Antipotion ID / Drafix Langth:

步驟8.從Destination IP / Prefix Length下拉選單中選擇將訪問規則應用到的適當目標IP型別。

- Any 任何目標IP地址都應用了規則。
- 單一 只有裝置網路上的一個指定IP地址應用了該規則。輸入所需的IPv6地址。
- 子網 只有子網的IP地址才應用規則。在相鄰欄位中輸入所需子網的IPv6網路地址和字首長度。

步驟9.按一下Save,變更就會生效。

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