在RV34x系列路由器上配置埠轉發/埠觸發/NAT

目標

解釋埠轉發和埠觸發的目的,並提供在RV34x系列路由器上設定這些功能的說明。

- •比較埠轉發和埠觸發
- 設定埠轉發和埠觸發
- 設定網路地址轉換(NAT)

適用裝置

• RV34x路由器系列

軟體版本

• 1.0.01.17

比較埠轉發和埠觸發

這些功能允許某些Internet使用者訪問您網路上的特定資源,同時保護您想要保持私有性的資源。以下為使用此類命令時的一些示例:託管web/電子郵件伺服器、警報系統和安全監視器 (將影片傳送回非現場電腦)。 埠轉發開啟埠以響應指定服務的入站流量。

當您在設定嚮導的「服務管理」部分輸入資訊時,將會設定這些埠的清單及其說明。設定這些 埠時,不能將相同的埠號同時用於埠轉發和埠觸發。

連線埠轉送

連線埠轉送是一種技術,可透過為服務開啟特定連線埠來回應傳入流量,允許公眾存取區域網路(LAN)上網路裝置上的服務。這可確保資料包具有到達預定目標的清晰路徑,從而加快下載 速度並降低延遲。這是為網路中的一台電腦設定的。您需要新增特定電腦的IP地址,但無法更 改。

這是一種靜態操作,用於開啟您選擇且不更改的特定埠範圍。這可能會增加安全風險,因為已 配置的埠總是開啟的。

想象一下,該埠上總是開啟一個門,用於指定該埠的裝置。

連線埠觸發

埠觸發類似於埠轉發,但更加安全。不同之處在於,觸發埠並不總是針對該特定流量開啟。 LAN上的資源透過觸發連線埠傳送傳出流量後,路由器會監聽透過指定連線埠或連線埠範圍的 傳入流量。觸發埠在沒有活動時關閉,這增加了安全性。另一個優點是,您網路上的多台電腦 可以在不同的時間訪問此埠。因此,您無需事先知道將觸發它的電腦的IP地址,它會自動執行 此操作。

想象一下,你給別人一個通行證,但是那裡有一個門衛,他會在你每次進來時檢查你的通行證 ,然後關上門,直到有通行證的下一個人來到這裡為止。

設定埠轉發和埠觸發

連線埠轉送

要配置埠轉發,請執行以下步驟:

步驟1.登入到Web配置實用程式。在搜尋/位址列中輸入路由器的IP地址。瀏覽器可能會發出 警告,指出該網站不可信。繼續瀏覽網站。如需此步驟的詳細指南,請按一下<u>此處</u>。

輸入路由器的使用者名稱和密碼,然後按一下Log In。預設使用者名稱和密碼為cisco。

		Username:
	_	Password:
cisco	Router	Language: English V
		Log In

步驟2.在左側的主選單中,按一下Firewall >Port Forwarding



在埠轉發表中,按一下Add或選擇行,然後按一下Edit以配置以下內容:

外部服務	從下拉選單中選擇一個外部服務。(如果未列出服務,您可以按照「服務管理」部分中的詞
內部服務	從下拉選單中選擇一個內部服務。(如果未列出服務,您可以按照「服務管理」部分中的記
內部IP地址	輸入伺服器的內部IP地址。
介面	從下拉選單中選擇介面,以應用埠轉發。
狀態	啟用或禁用埠轉發規則。

Ρ	ort	Forwardi	ing			
	Por	rt Forwardin	g Table			
		Enable	External Service	Internal Service	Internal IP Address	Interfaces
			All Traffic V	All Traffic 🔍		WAN1 👻
			Edit Delete Se	arvice Management		
		Apply	Cancel			

例如,某公司在其LAN上託管Web伺服器(內部IP地址為192.0.2.1)。可以啟用HTTP流量的 埠轉發規則。這將允許來自Internet的請求進入該網路。公司將埠號80(HTTP)設定為轉發到 IP地址192.0.2.1,然後將外部使用者的所有HTTP請求轉發到192.0.2.1。它是針對網路中的特 定裝置設定的。

第3步。按一下**服務管理**

在服務表中,按一下Add或選擇行,然後按一下Edit並配置以下內容:

- Application Name 服務或應用程式的名稱
- Protocol 必需協定。請參閱您託管服務的文檔
- Port Start/ICMP Type/IP Protocol 為此服務保留的埠號範圍
- Port End 為該服務保留的埠的最後一個編號

Service Management			
Service Table			
Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
SMTP	TCP	25	25
SNMP-TCP	TCP	161	161
SNMP-TRAPS-TCP	TCP	162	162
SNMP-TRAPS-UDP	UDP	162	162
SNMP-UDP	UDP	161	161
SSH-TCP	TCP	22	22
SSH-UDP	UDP	22	22
TACACS	TCP	49	49
TELNET	TCP	23	23
TFTP	UDP	69	69
	TCP	10000	10000
* When a service is in use by Port Forwarding	/ Port Triggering setting	s, this service can not apply ICMP/IP on the Prot	ocol Type.
Low Control Delete			
Apply Back Cancel			

步驟4.按一下Apply

連線埠觸發

要配置埠觸發,請執行以下步驟:

步驟1.登入到Web配置實用程式。從左側的主選單中,按一下Firewall > Port Trigger

	Getting Started
•	Status and Statistics
•	Administration
•	System Configuration
•	WAN
•	QoS
•	LAN
•	Routing
•	Firewall
	Basic Settings
	Buolo Octango
	Access Rules
	Access Rules Network Address Translation
	Access Rules Network Address Translation Static NAT
	Access Rules Network Address Translation Static NAT Port Forwarding
	Access Rules Network Address Translation Static NAT Port Forwarding (Port Triggering)
	Access Rules Network Address Translation Static NAT Port Forwarding (Port Triggering) Session Timeout
	Access Rules Network Address Translation Static NAT Port Forwarding (Port Triggering) Session Timeout DMZ Host
Þ	Access Rules Network Address Translation Static NAT Port Forwarding (Port Triggering) Session Timeout DMZ Host

步驟2.要向埠觸發表新增或編輯服務,請配置以下內容:

應用程式名稱	輸入應用程式的名稱。
觸發服務	從下拉選單中選擇服務。(如果未列出服務,您可以按照「服務管理」部分中的說明新步
傳入服務	從下拉選單中選擇服務。(如果未列出服務,您可以按照「服務管理」部分中的說明新步
介面	從下拉選單中選擇介面。
狀態	啟用或禁用埠觸發規則。

按一下Add(或選擇行並按一下Edit)並輸入以下資訊:

F	Port	Triggerir	ng			
	Por	rt Triggering	Table			
		Enable	Application Name	Trigger Service	Incoming Service	Interfaces
			c	All Traffic	FTP	WAN1
			d	All Traffic	FTP	WAN1
		Add		Service Management		
	Ap	ply	Cancel			

步驟3。按一下Service Management,在Service清單中新增或編輯條目。

在「服務表」中,按一下Add或Edit,然後配置以下內容:

• Application Name — 服務或應用程式的名稱

• Protocol — 必需協定。請參閱您託管服務的文檔

- Port Start/ICMP Type/IP Protocol 為此服務保留的埠號範圍
- Port End 為該服務保留的埠的最後一個編號

Service Management			
Service Table			
Application Name	Protocol *	Port Start/ICMP Type/IP Protocol	Port End
SMTP	TCP	25	25
SNMP-TCP	TCP	161	161
SNMP-TRAPS-TCP	TCP	162	162
SNMP-TRAPS-UDP	UDP	162	162
SNMP-UDP	UDP	161	161
SSH-TCP	TCP	22	22
SSH-UDP	UDP	22	22
TACACS	TCP	49	49
TELNET	TCP	23	23
TFTP	UDP	69	69
	TCP	10000	10000
* When a service is in use by Port Forwarding / Port T	riggering settings, this	service can not apply ICMP/IP on the Protocol Typ	pe.
Add Edit Delete			
Apply Back Cancel			

步驟4.按一下Apply

網路位址轉譯

網路地址轉換(NAT)允許具有未註冊IP地址的私有IP網路連線到公共網路。這是大多數網路中 通常設定的通訊協定。在將資料包轉發到公共網路之前,NAT將內部網路的私有IP地址轉換為 公有IP地址。這允許內部網路上的大量主機通過有限的公有IP地址訪問Internet。這也有助於 保護私有IP地址免受任何惡意攻擊或發現,因為私有IP地址始終處於隱藏狀態。

要配置NAT,請執行以下步驟

步驟1.按一下Firewall> Network Address Translation

	Getting Started
•	Status and Statistics
•	Administration
•	System Configuration
•	WAN
•	QoS
•	LAN
•	Routing
•	Firewall
	Basic Settings
	Access Rules
	Network Address Translation
	Static NAT
	Port Forwarding
	Port Forwarding Port Triggering
	Port Forwarding Port Triggering Session Timeout
	Port Forwarding Port Triggering Session Timeout DMZ Host
•	Port Forwarding Port Triggering Session Timeout DMZ Host VPN

步驟2.在NAT表中,為清單中要啟用的每個適用介面選中Enable NAT

NAT Table		
Interface	Enable NAT	
WAN1		
WAN2		
USB1		
USB2		

步驟3.按一下Apply

現在您已成功配置埠轉發、埠觸發和NAT。

其他資源

- 要配置靜態NAT,請點選此處
- 有關包括RV3xx系列在內的路由器的許多問題的答案,請點選此處
- 有關RV34x系列的常見問題,請點選此<u>處</u>
- 有關RV345和RV345P的詳細資訊,請按一下此處
- 有關在RV34x系列上配置服務管理的詳細資訊,請點選此處

檢視與本文相關的影片……

<u>按一下此處檢視思科的其他技術對話</u>