在RV34x系列路由器上配置端口转发/端口触发 /NAT

目标

解释端口转发和端口触发的用途,并提供在RV34x系列路由器上设置这些功能的说明。

- •比较端口转发和端口触发
- 设置端口转发和端口触发
- 设置网络地址转换(NAT)

适用设备

• RV34x路由器系列

软件版本

• 1.0.01.17

比较端口转发和端口触发

这些功能允许某些互联网用户访问您网络上的特定资源,同时保护您要保持私有的资源。使用 时的一些示例:托管Web/电子邮件服务器、报警系统和安全摄像头(将视频发回非现场计算 机)。 端口转发会打开端口以响应指定服务的入站流量。

在设置向导的"服务管理"部分输入信息时,将设置这些端口及其说明的列表。设置这些设置时 ,端口转发和端口触发不能使用相同的端口号。

端口转发

端口转发是一种技术,它允许公众访问局域网(LAN)上网络设备上的服务,方法是为服务打开 特定端口以响应入站流量。这可确保数据包具有到达目标的清晰路径,从而实现更快的下载速 度和更低的延迟。这是为网络上的一台计算机设置的。您需要添加特定计算机的IP地址,但该 地址无法更改。

这是一种静态操作,它打开您选择的特定端口范围且不更改。这可能会增加安全风险,因为配 置的端口始终处于打开状态。

想象一下,在分配给该设备的端口上,门总是打开。

端口触发

端口触发类似于端口转发,但更加安全。区别在于,触发器端口并非总是为特定流量打开。在 LAN上的资源通过触发端口发送出站流量后,路由器会侦听通过指定端口或端口范围的入站流 量。当没有活动时,触发端口会关闭,这会增加安全性。另一个好处是,网络上的多台计算机 可以在不同时间访问此端口。因此,您不需要知道提前触发该IP地址的计算机,它会自动执行 此操作。

想想你给了某人一个通行证,但那里有一名门卫,每次你进门时,门卫都会检查你的通行证

,然后把门关上,直到下一个领着通行证的人到来。

设置端口转发和端口触发

端口转发

要配置端口转发,请执行以下步骤:

步骤1.登录Web配置实用程序。在搜索/地址栏中输入路由器的IP地址。浏览器可能会发出网 站不受信任的警告。继续访问网站。有关此步骤的更多指导,请单<u>击此处</u>。

输入路由器的用户名和密码,然后单击Log In。默认用户名和密码为cisco。

		Usemame:	ctangular Snip
		Password:	
cisco	Router	Language: English	<u>~</u>
		Log In	

步骤2.从左侧的主菜单中,单击Firewall > Port Forwarding

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

在端口转发表中,单击**添加**或选择该行,然后单击**编辑**以配置以下内容:

外部服务 从下拉列表中选择外部服务。(如果未列出服务,您可以按照"服务管理"部分的说明添加或修

内部服务 从下拉列表中选择内部服务。(如果未列出服务,您可以按照"服务管理"部分的说明添加或修

内部 IP 输入服务器的内部IP地址。

接口 从下拉列表中选择接口,以应用端口转发。

启用或禁用端口转发规则。

Port	Forward	dina						
_								
P	ort Forwardi	ing Table						
	Enable	External Service		Internal Service		Internal IP Address	Interfaces	
		All Traffic	~	All Traffic	~		WAN1	~
		Edit Delet	le Ser	vice Management				
		Cancel						

例如,公司在其LAN上托管Web服务器(内部IP地址为192.0.2.1)。可以启用HTTP流量的端 口转发规则。这将允许从Internet请求进入该网络。公司将端口号80(HTTP)设置为转发到IP地 址192.0.2.1,然后来自外部用户的所有HTTP请求将转发到192.0.2.1。它为网络中的特定设备 设置。

步骤3.单击"服务管理"

在"服务表"中,单**击"添**加"或选择一行,然后单**击"编**辑"并配置以下内容:

- 应用名称 服务或应用的名称
- •协议 所需协议。请参阅您托管的服务的文档
- •端口开始/ICMP类型/IP协议—为此服务保留的端口号范围
- 端口结束 为此服务保留的端口的最后一个编号

Service Management	t			
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	y Port Forwarding / Port Tr	iggering settings, this	service can not apply ICMP/IP on the Protocol T	ype.
Add Edit	Delete			
Apply Back	Cancel			

步骤4.单击"应**用"**

端口触发

要配置端口触发,请执行以下步骤:

步骤1.登录Web配置实用程序。从左侧的主菜单中,单击Firewall > Port Triggering

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

步骤2.要向端口触发表添加或编辑服务,请配置以下内容:

应用程序名称	输入应用的名称。
触发服务	从下拉列表中选择服务。(如果未列出服务,您可以按照"服务管理"部分的说明添加或修
传入服务	从下拉列表中选择服务。(如果未列出服务,您可以按照"服务管理"部分的说明添加或修
接口	从下拉列表中选择接口。
状态	启用或禁用端口触发规则。

单击Add(或选择行并单击Edit),然后输入以下信息:

F	Port	Triggerii	ng			
	Por	rt Triggering	g 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			

第3步:单击Service Management,以在Service列表中添加或编辑条目。

在"服务表"中,单击"**添加**"或**"编**辑"并配置以下内容:

- 应用名称 服务或应用的名称
- •协议 所需协议。请参阅您托管的服务的文档

- •端口开始/ICMP类型/IP协议—为此服务保留的端口号范围
- •端口结束 为此服务保留的端口的最后一个编号

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
2 1	TCP	V 10000	10000
When a service is in use by Port Forward	ding / Port Triggering settings	, this service can not apply ICMP/IP on the Prot	tocol Type.

步骤4.单击"应**用"**

网络地址转换

网络地址转换(NAT)使具有未注册IP地址的私有IP网络能够连接到公有网络。这是大多数网络 中常用的配置协议。NAT将内部网络的私有IP地址转换为公有IP地址,然后将数据包转发到公 有网络。这允许内部网络中的大量主机通过有限数量的公有IP地址访问Internet。这还有助于 保护私有IP地址免受任何恶意攻击或发现,因为私有IP地址被隐藏。

要配置NAT,请执行以下步骤

步骤1.单击"防火墙">"网络地址转换"

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

步骤2.在NAT表中,选中Enable NAT for ach applicable Interface on the list以启用

etwork Address	Translation
NAT Table	
Interface	Enable NAT
WAN1	
WAN2	
USB1	
USB2	
Apply Cance	el

步骤3.单击"应用"

您现在已成功配置端口转发、端口触发和NAT。

其它资源

- •要配置静态NAT,请单击<u>此处</u>
- 有关路由器(包括RV3xx系列)的许多问题的答案,请单击<u>此处</u>
- •有关RV34x系列的常见问题,请单击<u>此处</u>
- 有关RV345和RV345P的详细信息,请单击<u>此处</u>
- 有关在RV34x系列上配置服务管理的详细信息,请单击<u>此处</u>

查看与本文相关的视频……

<u>单击此处查看思科提供的其他技术讲座</u>