
NAT 虚拟服务器实验

1.实验目的

网络地址转换(NAT,Network Address Translation)属接入广域网(WAN)技术,是一种将私有(保留)地址转化为合法 IP 地址的转换技术,它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单,NAT 不仅完美地解决了 IP 地址不足的问题,而且还能够有效地避免来自网络外部的攻击,隐藏并保护网络内部的计算机。

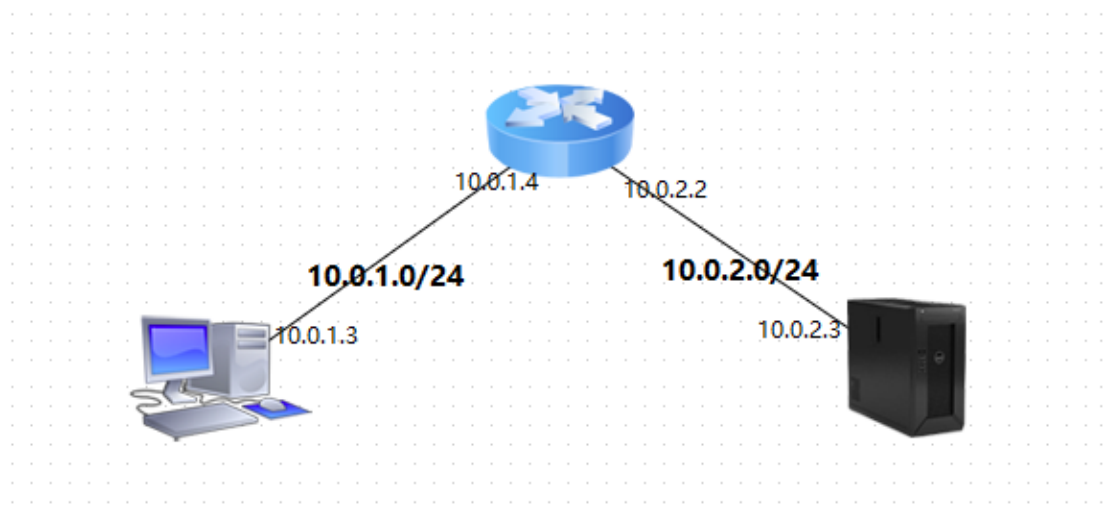
通过在路由器上配置 NAT 静态端口映射了解 NAT 的虚拟服务器功能是如何实现的。

2.知识补充

虚拟服务器可以使多台服务器共享一个公网 IP,假设我们现在有一个 202.197.61.123 的公网 IP,我们将此 IP 分配给路由器,然后将路由器的内网 IP 设为 192.168.1.1,再将分别载有 a 项目的服务器 A 和载有 b 项目的服务器 B 与路由器相连,并分别设内网 IP 为 192.168.1.2 和 192.168.1.3。然后通过路由器 NAT 静态端口映射将外网的 2222 端口映射至 192.168.1.2:80,将外网的 3333 端口映射至 192.168.1.3:80;当我们访问 202.197.61.123:2222 的时候我们访问到的是 a 项目,当我们访问 202.197.61.123:3333 的时候我们访问到的是 b 项目;这样 NAT 可以为我们节省很多的公网 IP 资源。

3.实验步骤

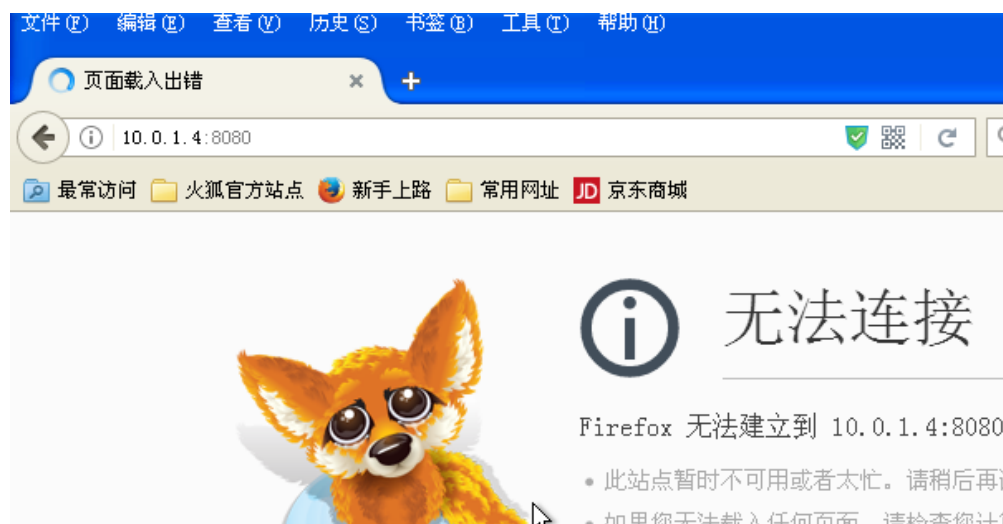
在右上方的实验拓扑图中选择配置 NAT 虚拟服务器实验,点击连线配置子网网段,实验拓扑如下图所示:



然后点击提交实验，等待资源分配成功后，点击图标按全屏访问即可进入设备。

首先我们进入 ApplicationServer(用户名: centos 密码: centos)，输入命令 `sudo service httpd start` 启动 http 服务。

然后我们进入 PC，在 PC 上登录浏览器输入 10.0.1.4:8080,发现无法载入界面



为了模拟真实的环境，我们需要把 10.0.2.0/24 定义为局域网，把 10.0.1.0/24 定义为广域网，PC 是不能直接访问应用服务器的，但是通过 NAT 可以实现此功能。

然后在 PC 上登录浏览器输入 10.0.1.4，账号和密码都是 root，登录路由器管理界面。

进入路由器后点击最上面一行选择 NETWORK，再选择 Firewall，将 reject 选项都改为 accept 选项。然后再最下方选择 Save & Apply。

Enable SYN-flood protection ☒

Drop invalid packets ☒

Input

accept

Output

accept

Forward

accept

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	<div>accept</div>	<div>accept</div>	<div>accept</div>	<input type="checkbox"/>	<input type="checkbox"/>	<div>Edit</div>
wan: wan: wan6: ⇒ REJECT	<div>accept</div>	<div>accept</div>	<div>accept</div>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<div>Edit</div>

Add

然后选择 NETWORK，选择 Interfaces，再选择 eth0，点击 edit 选项，再在 common Configuration 中选择 Firewall Settings, 将 NET1 归入 wan:

Common Configuration

General Setup

Advanced Settings

Physical Settings

Firewall Settings

Create / Assign firewall-zone

lan: lan:

wan: wan: wan6:

unspecified -or- create:

Choose the firewall zone you want to assign to this i

zone or fill out the create field to define a new zone and

然后再最下方选择 **Save & Apply**。

同理再将 eth1 归入 lan，这样就把 PC 和应用服务器的网络隔离了，这时候在网页中访问 10.0.2.3 是访问不通的。

接下来我们选择 NETWORK，再选择 Firewall，选择 Port Forwards 进入了虚拟服务器的端口转发界面。再在下方的配置区域，配置端口转发信息，然后点击 Add 按钮。（Tips: 同学们有没有发现 Internal IP address 这里没有 10.0.2.3 这个选项呢？（需要手动填写）自己先想想为什么，答案将在此文档的最后出现。）

General Settings

Port Forwards

Traffic Rules

Custom Rules

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
Forward8080	IPv4-tcp, udp From any host in wan Via any router IP at port 8080	IP 10.0.2.3 , port 80 in lan	<input checked="" type="checkbox"/>	<div><div></div><div></div></div> <div>EditDelete</div>

Port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
Forward8080	TCP+UDP	wan	8080	lan	10.0.2.3 (FA:16)	80

Add

完成之后，会出现如下信息

Port Forwards

Name	Match	Forward to	Enable	Sort
Forward8080	IPv4-tcp, udp From any host in wan Via any router IP at port 8080	IP 10.0.2.3 , port 80 in lan	<input checked="" type="checkbox"/>	<div><div></div><div></div></div> <div>Edit</div>

配置成功后我们就可以在最下方选择 **Save & Apply** 保存配置。
然后再在外层的配置页面继续点击 **Save & Apply** 保存配置。
接下来就是见证奇迹的时刻：



下面就来揭晓为何 Internal IP address 这里没有 10.0.2.3 这个选项，原因在于路由器是基于学习机制的，一开始它也不知道它有哪些邻居，所以可以先进入服务器 ping 10.0.2.2 让路由器知道它有这么一个邻居。之后再去路由器看就能看到 10.0.2.3 这个地址了。

温馨提示：实验资源宝贵，实验结束后记得点击结束实验

