

Linux 或 Windows 上實現端口映射

varlemon 運維 昨天

作者: varlemon

鏈接: <https://www.cnblogs.com/connect/p/server-port-proxy.html>

通常服務器會有許多塊網卡，因此也可能會連接到不同的網絡，在隔離的網絡中，某些服務可能會需要進行通信，此時服務器經過配置就可以承擔起了轉發數據包的功能。

一、Windows 下實現端口映射

1. 查詢端口映射情況

```
1 netsh interface portproxy show v4tov4
```

2. 查詢某一個IP的所有端口映射情況

```
1 netsh interface portproxy show v4tov4 | find "[IP]"  
2 例：  
3 netsh interface portproxy show v4tov4 | find "192.168.1.1"
```

3. 增加一個端口映射

```
1 netsh interface portproxy add v4tov4 listenaddress=[外网IP] listenport=[外网  
2 例 :  
3 netsh interface portproxy add v4tov4 listenaddress=2.2.2.2 listenport=8080
```

4. 刪除一個端口映射

```
1 interface portproxy delete v4tov4 listenaddress=[外网IP] listenport=[外网端口]  
2  
3 interface portproxy delete v4tov4 listenaddress=2.2.2.2 listenport=8080
```

二、Linux下端口映射

1. 允許數據包轉發

```
1 echo 1 >/proc/sys/net/ipv4/ip_forward  
2 iptables -t nat -A POSTROUTING -j MASQUERADE  
3 iptables -A FORWARD -i [内网网卡名称] -j ACCEPT
```

```
4 iptables -t nat -A POSTROUTING -s [內網網段] -o [外網网卡名称] -j MASQUERADE
5
6 例：
7 echo 1 >/proc/sys/net/ipv4/ip_forward
8 iptables -t nat -A POSTROUTING -j MASQUERADE
9 iptables -A FORWARD -i ens33 -j ACCEPT
10 iptables -t nat -A POSTROUTING -s 192.168.50.0/24 -o ens37 -j MASQUERADE
```

2. 設置端口映射

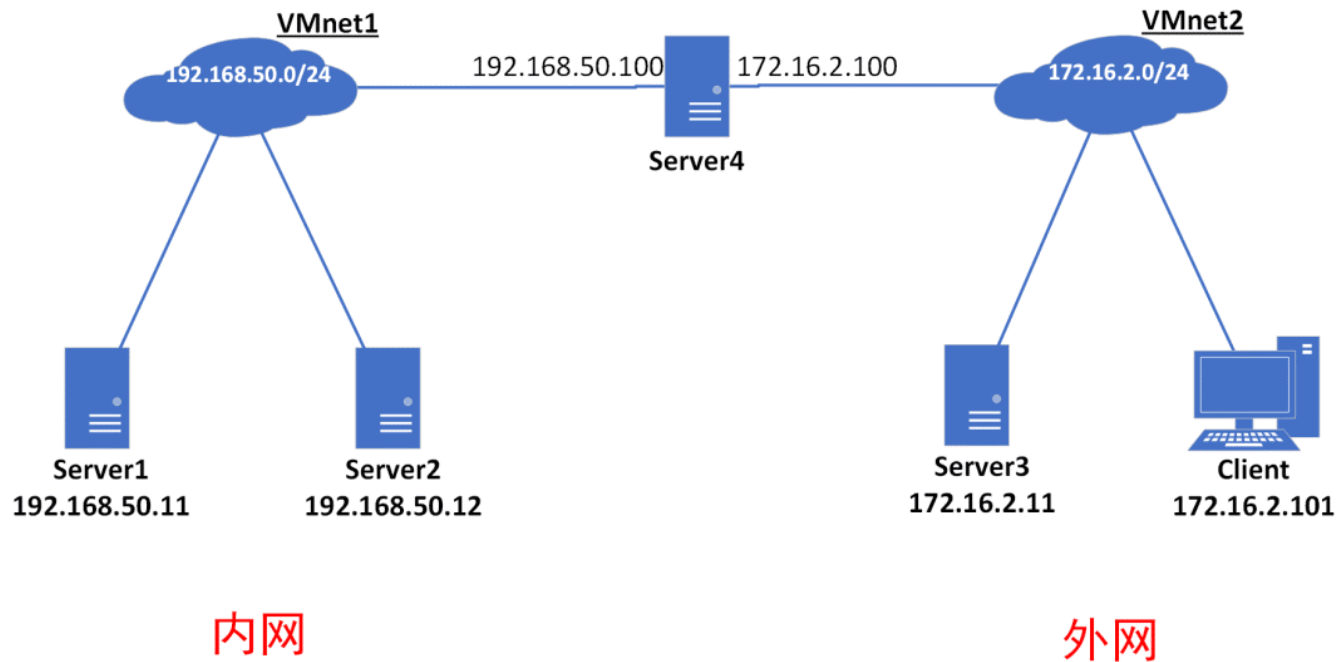
```
1 iptables -t nat -A PREROUTING -p tcp -m tcp --dport [外網端口] -j DNAT --to-
2 例：
3 iptables -t nat -A PREROUTING -p tcp -m tcp --dport 6080 -j DNAT --to-desti
```

實驗：將部署在內網的服務映射到外網

實驗環境

1. VMWare Workstation Pro
2. 5台最小化安裝的centos 7虛擬機

實驗拓撲



內網和外網是相對Server4來說的。

Server1和Server2為內網環境的兩台服務器；

Server3為外網環境下的一台服務器；

Server4為一台雙網卡主機，分別連接192.168.50.0/24和172.16.2.0/24兩個網絡。

配置實驗環境

1. Server1,2,3上搭建HTTP服務

用Python在Server1上搭建一個簡單的HTTP服務

```
1 cd ~
2 echo "server1" > index.html
3 python -m SimpleHTTPServer 8080
```

```
[root@server1 ~]# cd ~  
[root@server1 ~]# echo "server1" > index.html  
[root@server1 ~]# python -m SimpleHTTPServer 8080  
Serving HTTP on 0.0.0.0 port 8080 ...  
█
```

Server2、Server3同理

對照實驗

在client上訪問Server1的資源

```
1 curl http://192.168.50.11:8080/index.html
```

```
[root@client ~]# curl http://192.168.50.11:8080/index.html  
curl: (7) Failed to connect to 192.168.50.11: Network is unreachable  
[root@client ~]# █
```

在client上訪問Server2的資源

```
1 curl http://192.168.50.12:8080/index.htm
```

```
[root@client ~]# curl http://192.168.50.12:8080/index.html
curl: (7) Failed to connect to 192.168.50.12: Network is unreachable
[root@client ~]#
```

在client上訪問Server3的資源

```
1 curl http://172.16.2.11:8080/index.html
```

```
[root@client ~]# curl http://172.16.2.11:8080/index.html
server3
[root@client ~]#
```

可以看到，外網的client是無法訪問內網Server1,Server2的資源的。

在Server4上配置端口映射

臨時配置

```
1 #允许数据包转发
2 echo 1 >/proc/sys/net/ipv4/ip_forward
3 iptables -t nat -A POSTROUTING -j MASQUERADE
4 iptables -A FORWARD -i ens33 -j ACCEPT
5 iptables -t nat -A POSTROUTING -s 192.168.50.0/24 -o ens37 -j MASQUERADE
6 #设置端口映射
7 iptables -t nat -A PREROUTING -p tcp -m tcp --dport 8081 -j DNAT --to-desti
```

```
8 iptables -t nat -A PREROUTING -p tcp -m tcp --dport 8082 -j DNAT --to-desti
```

永久配置

如果需要永久配置，則將以上命令追加到/etc/rc.local文件。

檢查效果

在client上訪問Server1的資源

```
1 curl http://172.16.2.100:8081/index.html
```

```
[root@client ~]# curl http://172.16.2.100:8081/index.html
server1
[root@client ~]#
```

在client上訪問Server2的資源

```
1 curl http://172.16.2.100:8082/index.html
```

```
[root@client ~]# curl http://172.16.2.100:8082/index.html
server2
[root@client ~]#
```

在client上訪問Server3的資源

```
1 curl http://172.16.2.11:8080/index.html
```

```
[root@client ~]# curl http://172.16.2.11:8080/index.html
server3
[root@client ~]#
```

如果Server4為Windows，替換一下相應的命令即可

Windows的IP信息如下

網卡	IP地址	子網掩碼	默認網關	備註
Ethernet0	192.168.50.105	255.255.255.0	-	內網網卡
Ethernet1	172.16.2.105	255.255.255.0	-	外網網卡


```
管理员: C:\Windows\system32\cmd.exe

C:\>ipconfig

Windows IP 配置

以太网适配器 Ethernet1:

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址 . . . . . : fe80::298a:9b97:e517:61ad%24
    IPv4 地址 . . . . . : 172.16.2.105
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : 
    本地链接 IPv6 地址 . . . . . : fe80::a46e:b333:64b8:6922%12
    IPv4 地址 . . . . . : 192.168.50.105
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 

隧道适配器 isatap.{307740C4-B907-4256-900A-5A9095071F09}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 

隧道适配器 isatap.{414FF7D0-E6F8-46D1-BA22-CB7C76DB0732}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 

C:\>
C:\>
```

配置並查看端口映射情况

```
1 netsh interface portproxy add v4tov4 listenaddress=172.16.2.105 listenport=
2 netsh interface portproxy add v4tov4 listenaddress=172.16.2.105 listenport=
3 netsh interface portproxy show v4tov4
```

```
C:\>netsh interface portproxy add v4tov4 listenaddress=172.16.2.105 listenport=8081 connectaddress=192.168.50.11 connectport=8080

C:\>netsh interface portproxy add v4tov4 listenaddress=172.16.2.105 listenport=8082 connectaddress=192.168.50.12 connectport=8080

C:\>netsh interface portproxy show v4tov4

侦听 ipv4:                连接到 ipv4:
地址          端口          地址          端口
-----
172.16.2.105  8081          192.168.50.11 8080
172.16.2.105  8082          192.168.50.12 8080

C:\>
C:\>
```

檢查效果

在client節點上

```
1 curl http://172.16.2.105:8081/index.html
2 curl http://172.16.2.105:8082/index.html
3 curl http://172.16.2.11:8080/index.html
```

```
[root@client ~]# curl http://172.16.2.105:8081/index.html
server1
[root@client ~]# curl http://172.16.2.105:8082/index.html
server2
[root@client ~]# curl http://172.16.2.11:8080/index.html
server3
[root@client ~]#
[root@client ~]#
[root@client ~]#
[root@client ~]#
```

推薦：計算機網絡工程師



網絡通信技術分享

閱讀原文

喜歡此內容的人還喜歡

懂了！VMware/KVM/Docker原來是這麼回事兒

編程技術宇宙



Linux 環境變量配置全攻略

Linux學習



Linux之《荒島餘生》（五）網絡篇

小姐姐味道

