链滴

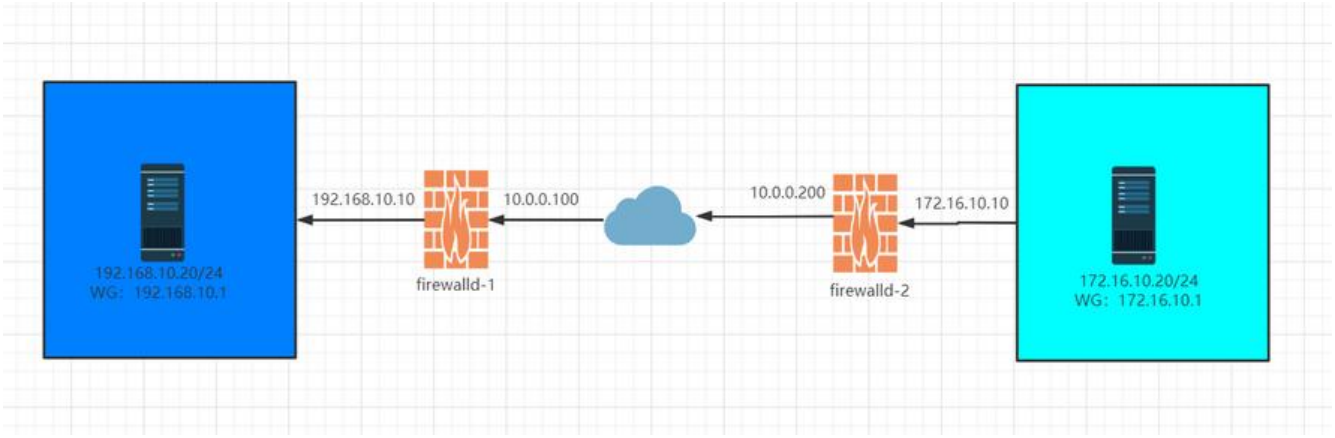
3- 综合案例 两个私有网络的互相通迅

作者：Carey

原文链接：https://ld246.com/article/1611578793508

来源网站：链滴

环境示例：俩个私有网络的主机都有http服务需要可以互相通信



1 主机网络环境准备

```
#web-1
[20:07:44 root@web-1 ~]#hostname -I
192.168.10.71
[20:08:37 root@web-1 ~]#route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.10.10   0.0.0.0         UG    100    0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0

#firewalld-1
[20:10:37 root@firewalld-1 network-scripts]#hostname -I
192.168.10.10 10.0.0.100
[20:10:42 root@firewalld-1 network-scripts]#route -n
Kernel IP routing table
```

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     101    0        0 eth1
192.168.10.0    0.0.0.0         255.255.255.0   U     102    0        0 eth0

#firewalld-2
[20:07:17 root@firewalld-2 ~]#hostname -I
172.16.10.10 10.0.0.200
[20:11:28 root@firewalld-2 ~]#route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     103    0        0 eth1
172.16.10.0     0.0.0.0         255.255.255.0   U     102    0        0 eth0

#web-2
[20:07:42 root@web-2 ~]#hostname -I
172.16.10.20
[20:11:46 root@web-2 ~]#route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.16.10.10    0.0.0.0         UG    100    0        0 eth0
172.16.10.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

2 firewalld开启路由转发

```
[20:13:03 root@firewalld-1 ~]#echo 1 >/proc/sys/net/ipv4/ip_forward
[20:11:33 root@firewalld-2 ~]#echo 1 >/proc/sys/net/ipv4/ip_forward
```

3 配置SNAT实现内网主机可以访问互联网

```
#允许firewalld-1内网访问互联网
[20:13:25 root@firewalld-1 ~]#iptables -t nat -APOSTROUTING -s 192.168.10.0/24 -j MASQU
RADE

[20:08:51 root@web-1 ~]#ping 10.0.0.200
PING 10.0.0.200 (10.0.0.200) 56(84) bytes of data.
64 bytes from 10.0.0.200: icmp_seq=1 ttl=63 time=1.30 ms
64 bytes from 10.0.0.200: icmp_seq=2 ttl=63 time=0.739 ms

[20:22:50 root@firewalld-2 ~]#tcpdump -i eth1
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:23:10.487634 IP 10.0.0.100 > firewalld-2: ICMP echo request, id 1638, seq 146, length 64
20:23:10.487656 IP firewalld-2 > 10.0.0.100: ICMP echo reply, id 1638, seq 146, length 64

#允许firewalld-1内网访问互联网
[20:13:58 root@firewalld-2 ~]#iptables -t nat -APOSTROUTING -s 172.16.10.0/24 -j MASQUE
ADE

[20:18:24 root@web-2 ~]#ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100) 56(84) bytes of data.
64 bytes from 10.0.0.100: icmp_seq=1 ttl=63 time=1.13 ms
64 bytes from 10.0.0.100: icmp_seq=2 ttl=63 time=0.678 ms
```

```
[20:24:06 root@firewalld-1 ~]#tcpdump  -i eth1
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:24:13.061897 IP 10.0.0.200 > firewalld-1: ICMP echo request, id 1640, seq 19, length 64
20:24:13.061922 IP firewalld-1 > 10.0.0.200: ICMP echo reply, id 1640, seq 19, length 64
```

配置完成后内网的主机是可以访问10.0.0.0互联网网段的

4 配置DNAT实现俩个私网主机可以互相访问对方的http务

```
#firewalld-1配置
[20:29:34 root@firewalld-1 ~]#iptables -t nat -APREROUTING -d 10.0.0.100 -p tcp --dport 80 -
 DNAT --to-destination 192.168.10.71:80

[20:30:07 root@web-2 ~]#curl 10.0.0.100
httpd 192.168.10.71

#firewalld-2配置
[20:23:21 root@firewalld-2 ~]#iptables -t nat -APREROUTING -d 10.0.0.200 -p tcp --dport 80 -
 DNAT --to-destination 172.16.10.20:80

[20:23:52 root@web-1 ~]#curl 10.0.0.200
httpd 172.16.10.20
```

5 配置DNAT实现俩个主机可以互相访问

```
[20:35:49 root@firewalld-1 ~]#iptables -t nat -IPREROUTING -d 10.0.0.100   -j DNAT --to-dest
nation 192.168.10.71
[20:23:21 root@firewalld-2 ~]#iptables -t nat -APREROUTING -d 10.0.0.200   -j DNAT --to-des
ination 172.16.10.20
```

即使是其他服务主要访问10.0.0.100都会映射到192.168.71主机，访问10.0.0.200映射到172.16.10.2
包扣ping