

知 SR66路由器作为LNS vpdn用户拨入后无法访问内网经验案例

PPPoE

L2TP VPN

VPDN

孙兆强

2020-04-15 发表

组网及说明



图中组网为运营商VPDN实际组网，ip地址考虑到安全性做了替换处理。用户pppoe拨号到运营商LAC，然后LAC拨l2tp到LNS。

问题描述

Client为专用终端VPDN拨号到LAC，然后l2tp拨到LNS。客户要求特殊，要求流量从LNS发往内网时要做源地址转换。用户拨号能成功但是无法访问内网。

过程分析

用户关键配置

```
interface GigabitEthernet0/0
```

```
port link-mode route
```

```
combo enable copper
```

```
ip address 1.1.2.2 255.255.255.0
```

```
interface Virtual-Template1
```

```
ppp authentication-mode chap domain system
```

```
remote address 172.16.8.2
```

```
ip address unnumbered interface GigabitEthernet0/0
```

```
nat inbound 3000 address-group 4
```

```
#
```

```
l2tp-group 1 mode lns
```

```
allow l2tp virtual-template 1 remote LAC
```

```
tunnel name LNS
```

```
tunnel password cipher $c$3$C4xazIHkSNV8aZMhPF0tdeMWPw6DBaDj
```

```
acl advanced 3000
```

```
rule 0 permit ip source 172.16.8.2 0
```

```
nat address-group 4
```

```
address 40.0.210.88 40.0.210.95
```

```
ip route-static 40.0.210.88 29 1.1.2.1
```

```
ospf 1
```

```
import-route static
```

```
area 0.0.0.0
```

```
network 192.168.0.0 0.0.0.255
```

在内网设备上查看路由表，已通过ospf学习到nat地址池路由

```
40.0.210.88/29 O_ASE2 150 1 192.168.0.1 GE0/0
```

在内网设备上debug ip icmp报文有收有发。

```
*Apr 14 08:53:02:917 2020 neiwang SOCKET/7/ICMP:
```

```
ICMP Input:
```

```
ICMP Packet: vpn = PUBLIC(0), src = 40.0.210.90, dst = 192.168.0.2
```

```
type = 8, code = 0 (echo)
```

```
*Apr 14 08:53:02:917 2020 neiwang SOCKET/7/ICMP:
```

```
ICMP Output:
```

```
ICMP Packet: vpn = PUBLIC(0), src = 192.168.0.2, dst = 40.0.210.90
```

```
type = 0, code = 0 (echo-reply)
```

在LNS上查看路由表

```
40.0.210.88/29 Static 60 0 1.1.2.1 GE0/0
```

```
172.16.8.2/32 Direct 0 0 172.16.8.2 BAS0
```

Nat地址池的路由指向了公网出口下一跳。用户的本意是想将回程流量指向VT口，所以地址借用了公网口，且下一跳指向公网下一跳。

实际上设备上会生成一个虚拟BAS口，并形成用户32位主机路由，出接口将流量指向BAS口。用户的配置方式无法将流量指向BAS口。

V7设备里的VT口一直保持down状态，也无法通过路由将流量指向VT口。

解决方法

1、保持用户nat inbound方式配置，将nat地址池流量指向172.16.8.2，通过路由迭代指到BAS口。ip route-static 40.0.210.88 29 172.16.8.2

查看LNS上路由表

40.0.210.88/29	Static	60	0	172.16.8.2	BAS0
----------------	--------	----	---	------------	------

172.16.8.2/32	Direct	0	0	172.16.8.2	BAS0
---------------	--------	---	---	------------	------

限制：此方法只适用于一个client的场景，多个client就会形成多个32位主机路由。用静态路由的方式会形成等价路由。流量回到错误用户势必导致业务异常。

2、在LNS的内网口配置nat outbound 3000 address-group 4，LNS上生成NULL0的直连路由，

40.0.210.88/30	Direct	1	0	0.0.0.0	NULL0
----------------	--------	---	---	---------	-------

40.0.210.92/30	Direct	1	0	0.0.0.0	NULL0
----------------	--------	---	---	---------	-------

在ospf里引入直连即可