

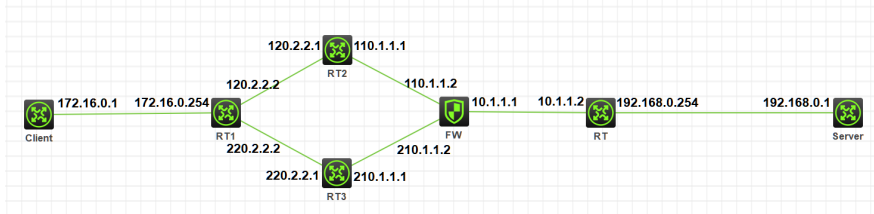
从协议说起 (2) ——ICMP (Tracert)

Tracert 胡伟 2020-10-15 发表

组网及说明

组网如下: Client 172.16.0.1 需要访问Server 192.168.0.1, FW将192.168.0.1分别映射为两条链路的外网地址

链路1: nat server global 110.1.1.3 inside 192.168.0.1



涉及的所有设备开启下面两个功能

ip ttl-expires enable

ip unreachable enable

配置步骤

Tracert根据百度百科的解释是(跟踪路由)是路由跟踪实用程序,用于确定IP数据包访问目标所采取的路径。Tracert命令用IP生存时间(TTL)字段和ICMP错误消息来确定从一个主机到网络上其他主机的路由。其工作原理为通过向目标发送不同IP生存时间(TTL)值的“Internet控制消息协议(ICMP)”回应数据包,Tracert诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的TTL递减1。数据包上的TTL减为0时,路由器应该将“ICMP已超时”的消息发回源系统。

tracert是Windows下常用的命令行工具(基于ICMP协议),UNIX下与之对应的是traceroute(基于UDP协议)。

Comware基于Linux系统开发,使用tracert命令,基于UDP协议。在客户端tracert FW链路1的nat server global地址110.1.1.3回显如下:

```
[H3C]tracert 110.1.1.3
traceroute to 110.1.1.3 (110.1.1.3), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1 172.16.0.254 (172.16.0.254) 1,000 ms 0,000 ms 1,000 ms
 2 120.2.2.1 (120.2.2.1) 1,000 ms 1,000 ms 0,000 ms
 3 110.1.1.2 (110.1.1.2) 2,000 ms 2,000 ms 1,000 ms
 4 110.1.1.3 (110.1.1.3) 3,000 ms 5,000 ms 3,000 ms
 5 110.1.1.3 (110.1.1.3) 4,000 ms 4,000 ms 3,000 ms
[H3C]
```

FW上抓包流量图分析如下

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------------------|--------------|-------------|----------|--------|--|
| 1 | 1978-03-01 01:12:16.40987 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33434 len=12 |
| 2 | 1978-03-01 01:12:16.41811 | 172.16.0.254 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 3 | 1978-03-01 01:12:16.41845 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33435 len=12 |
| 4 | 1978-03-01 01:12:16.41992 | 172.16.0.254 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 5 | 1978-03-01 01:12:16.41926 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33436 len=12 |
| 6 | 1978-03-01 01:12:16.41959 | 172.16.0.254 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 7 | 1978-03-01 01:12:16.41982 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33437 len=12 |
| 8 | 1978-03-01 01:12:16.41962 | 120.2.2.1 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 9 | 1978-03-01 01:12:16.41944 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33438 len=12 |
| 10 | 1978-03-01 01:12:16.41906 | 120.2.2.1 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 11 | 1978-03-01 01:12:16.41602 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33439 len=12 |
| 12 | 1978-03-01 01:12:16.41636 | 120.2.2.1 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 13 | 1978-03-01 01:12:16.41604 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33440 len=12 |
| 14 | 1978-03-01 01:12:16.41781 | 110.1.1.2 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 15 | 1978-03-01 01:12:16.41826 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33441 len=12 |
| 16 | 1978-03-01 01:12:16.41888 | 110.1.1.2 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 17 | 1978-03-01 01:12:16.41942 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33442 len=12 |
| 18 | 1978-03-01 01:12:16.41976 | 110.1.1.2 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 19 | 1978-03-01 01:12:16.41963 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33443 len=12 |
| 20 | 1978-03-01 01:12:16.42197 | 110.1.1.2 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 21 | 1978-03-01 01:12:16.42172 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33444 len=12 |
| 22 | 1978-03-01 01:12:16.42297 | 110.1.1.3 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 23 | 1978-03-01 01:12:16.42300 | 110.1.1.3 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 24 | 1978-03-01 01:12:16.42407 | 110.1.1.3 | 172.16.0.1 | ICMP | 78 | Time-to-live exceeded (Time to live exceeded in transit) |
| 25 | 1978-03-01 01:12:16.42418 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33446 len=12 |
| 26 | 1978-03-01 01:12:16.42455 | 110.1.1.3 | 172.16.0.1 | ICMP | 0 | Destination unreachable (Port unreachable) |
| 27 | 1978-03-01 01:12:16.42676 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33447 len=12 |
| 28 | 1978-03-01 01:12:16.42694 | 110.1.1.3 | 172.16.0.1 | ICMP | 0 | Destination unreachable (Port unreachable) |
| 29 | 1978-03-01 01:12:16.42645 | 172.16.0.1 | 110.1.1.3 | UDP | 54 | 33815 → 33448 len=12 |
| 30 | 1978-03-01 01:12:16.42924 | 110.1.1.3 | 172.16.0.1 | ICMP | 78 | Destination unreachable (Port unreachable) |

| 时间 | 172.16.0.1 | 192.168.0.1 | 172.16.0.254 | 192.2.2.1 | 110.1.1.3 | 注释 |
|----------------------------|------------|---------------|--------------|-------------|-------------|-------------------------|
| 1970-05-01 01:12:16.409887 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.411111 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.412945 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.412992 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.413241 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.413550 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.413811 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.414661 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.414944 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.415700 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.416022 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.416359 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.416628 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.416926 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.417181 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.417412 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.417654 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.417975 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.418206 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.418497 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.418768 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.420145 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.420445 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.420645 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.420944 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |
| 1970-05-01 01:12:16.420944 | 2002 | → 192.168.0.1 | → 172.16.0.1 | → 192.2.2.1 | → 110.1.1.3 | ICMP: 2002 = 2048 Len=2 |

由于FW上默认开启nat alg icmp-error, 会对服务器内网返回的icmp-error报文中的IP地址进行修改, 这就导致了Client上tracert无法显示NAT后的私网地址。

```

29 1970-01-01 01:06:13.942275      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
30 1970-01-01 01:06:13.942410      110.1.1.3       172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)

<
> Frame 29: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface unknown, id 0
> Ethernet II, Src: 56:8a:46:a1:07:05 (56:8a:46:a1:07:05), Dst: 56:89:13:5b:01:07 (56:89:13:5b:01:07)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 172.16.0.1
  Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xf949 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.16.0.1, Dst: 192.168.0.1
    User Datagram Protocol, Src Port: 33014, Dst Port: 33448

29 1970-01-01 01:06:13.942275      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
30 1970-01-01 01:06:13.942410      110.1.1.3       172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)

Frame 30: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface unknown, id 0
Ethernet II, Src: 56:89:13:5b:01:05 (56:89:13:5b:01:05), Dst: 56:8d:13:8c:02:06 (56:8d:13:8c:02:06)
Internet Protocol Version 4, Src: 110.1.1.3, Dst: 172.16.0.1
  Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0xf949 [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 172.16.0.1, Dst: 110.1.1.3
    User Datagram Protocol, Src Port: 33014, Dst Port: 33448

```

将FW使能undo nat alg icmp-error, 使得icmp-error报文IP不发生修改, 这样Client即可显示NAT后的私网地址, 如下:

```

[H3C]tracert 110.1.1.3
tracroute to 110.1.1.3 (110.1.1.3), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1 172.16.0.254 (172.16.0.254) 0.000 ms 1.000 ms 0.000 ms
 2 120.2.2.1 (120.2.2.1) 1.000 ms 1.000 ms 1.000 ms
 3 110.1.1.2 (110.1.1.2) 0.000 ms 1.000 ms 1.000 ms
 4 10.1.1.2 (10.1.1.2) 1.000 ms 2.000 ms 0.000 ms
 5 192.168.0.1 (192.168.0.1) 1.000 ms 2.000 ms 1.000 ms
[H3C]

62 1970-01-01 01:48:58.556326      172.16.0.1      110.1.1.3      UDP      54 33030 → 33446 Len=12
63 1970-01-01 01:48:58.556523      172.16.0.1      192.168.0.1    UDP      54 33030 → 33446 Len=12
64 1970-01-01 01:48:58.557338      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
65 1970-01-01 01:48:58.557534      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
66 1970-01-01 01:48:58.559263      172.16.0.1      110.1.1.3      UDP      54 33030 → 33447 Len=12
67 1970-01-01 01:48:58.559460      172.16.0.1      192.168.0.1    UDP      54 33030 → 33447 Len=12
68 1970-01-01 01:48:58.560213      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
69 1970-01-01 01:48:58.560424      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
70 1970-01-01 01:48:58.561741      172.16.0.1      110.1.1.3      UDP      54 33030 → 33448 Len=12
71 1970-01-01 01:48:58.562019      172.16.0.1      192.168.0.1    UDP      54 33030 → 33448 Len=12
72 1970-01-01 01:48:58.562782      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)
73 1970-01-01 01:48:58.562846      192.168.0.1      172.16.0.1      ICMP      70 Destination unreachable (Port unreachable)

```

配置关键点

附件下载: Client-tracert.rar