

知 vty在起了vpn实例的情况下限制客户端之后访问不了

VPN实例 姚一鸣 2019-12-17 发表

组网及说明



server直连client，也可以跨设备

问题描述

SERVER的0/0口地址为12.1.1.1/24,接口绑定到vpn实例1, clientg0/0地址为12.1.1.2/24, 现想通过telnet server后面加acl对上到设备的数据包做限制

```
#
acl basic 2000
 rule 0 permit source 12.1.1.2 0
#
telnet server acl 2000
调用之后发现client telnet访问不了12.1.1.1，但是可以ping通12.1.1.1
```

过程分析

因为起了vpn实例跑虚层面所以数据的转发会和实例有关

telnet server后没加acl可以正常访问且可以ping通

```
<H3C>ping 12.1.1.1
Ping 12.1.1.1 (12.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 12.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 12.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 12.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 12.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 12.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 12.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.200/1.000/0.400 ms
<H3C>%Dec 17 19:26:51:851 2019 H3C PING/6/PING_STATISTICS: Ping statistics for 12.1.1.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.200/1.000/0.400 ms
.

<H3C>telnet 12.1.1.1
Trying 12.1.1.1 ...
Press CTRL+K to abort
Connected to 12.1.1.1 ...

*****
*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,*
* no decompiling or reverse-engineering shall be allowed.*
*****
*****

login: 123
Password:
<H3C>
<H3C>
```

加了acl之后里面没有调用vpn参数telnet访问被拒，但是可以ping通

```
<H3C>telnet 12.1.1.1
Trying 12.1.1.1 ...
Press CTRL+K to abort
Connected to 12.1.1.1 ...

The connection was closed by the remote host!
<H3C>
<H3C>
```

加了一条rule 5 permit vpn-instance 1 source 12.1.1.2 0后可以访问

```
[H3C]qui
<H3C>
<H3C>tel
<H3C>telnet 12.1.1.1
Trying 12.1.1.1 ...
Press CTRL+K to abort
Connected to 12.1.1.1 ...

*****
*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,*
*   *
* no decompiling or reverse-engineering shall be allowed.*
*   *
*****
*****

login: █
```

解决方法

acl加了一条rule 5 permit vpn-instance 1 source 12.1.1.2 0后解决