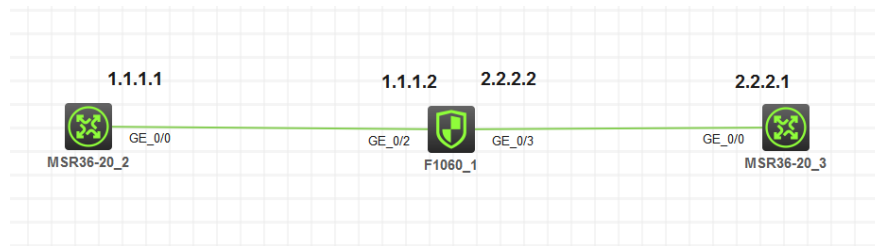


知 NGFW防火墙bfd echo会话down原因分析

BFD 胡伟 2020-02-20 发表

组网及说明



```
#
bfd echo-source-ip 100.100.100.100
#
track 1 bfd echo interface GigabitEthernet1/0/2 remote ip 1.1.1.1 local ip 1.1.1.2

#
nat address-group 1
address 1.1.1.10 1.1.1.12

#
interface GigabitEthernet1/0/2
port link-mode route
combo enable copper
ip address 1.1.1.2 255.255.255.0
#
```

问题描述

bfd echo会话down

过程分析

1. 在没有配置nat outbound时的会话

```
[H3C-GigabitEthernet1/0/2]display bfd session
Total Session Num: 1   Up Session Num: 1   Init Mode: Active
IPv4 Session Working Under Echo Mode:
LD      SourceAddr  DestAddr  State  Holdtime  Interface
97      1.1.1.2    1.1.1.1   Up     1629ms   GE1/0/2

display session table ipv4 verbose
Slot 1:
Initiator:
Source  IP/port: 100.100.100.100/49248
Destination IP/port: 1.1.1.2/3785
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: InLoopBack0
Source security zone: Local
Responder:
Source  IP/port: 1.1.1.2/3785
Destination IP/port: 100.100.100.100/49248
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Trust
State: UDP_OPEN
```

Application: GENERAL_UDP
Rule ID: 0
Rule name: 0
Start time: 2019-01-24 10:33:38 TTL: 30s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes
Total sessions found: 1

2. 在配置nat outbound后

```
[H3C-GigabitEthernet1/0/2]nat outbound  
[H3C-GigabitEthernet1/0/2]#Jan 24 11:26:59:212 2019 H3C BFD/5/BFD_CHANGE_FSM: -COntext=  
1; Sess[1.1.1.2/1.1.1.1, LD/RD:97/97, Interface:GE1/0/2, SessType:Echo, LinkType:INET], Ver:1, Sta  
: UP->DOWN, Diag: 1
```

```
[H3C-GigabitEthernet1/0/2]display bfd session  
Total Session Num: 1 Up Session Num: 0 Init Mode: Active  
IPv4 Session Working Under Echo Mode:  
LD SourceAddr DestAddr State Holdtime Interface  
97 1.1.1.2 1.1.1.1 Down 0ms GE1/0/2
```

```
[H3C-GigabitEthernet1/0/2]display session table ipv4 verbose
```

Slot 1:

Initiator:

```
Source IP/port: 100.100.100.100/49248  
Destination IP/port: 1.1.1.2/3785  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: -/-/  
Protocol: UDP(17)  
Inbound interface: InLoopBack0  
Source security zone: Local
```

Responder:

```
Source IP/port: 1.1.1.2/3785  
Destination IP/port: 1.1.1.2/1024  
DS-Lite tunnel peer: -  
VPN instance/VLAN ID/Inline ID: -/-/  
Protocol: UDP(17)  
Inbound interface: GigabitEthernet1/0/2  
Source security zone: Trust
```

State: UDP_OPEN

Application: GENERAL_UDP

Rule ID: 0

Rule name: 0

Start time: 2019-01-24 11:26:57 TTL: 29s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

源目地址一致，报文被丢弃。

3. 创建一个ACL屏蔽bfd echo-source-ip 100.100.100.100

#

```
acl advanced 3999  
rule 0 deny ip source 100.100.100.100 0  
rule 5 permit ip
```

```
[H3C-GigabitEthernet1/0/2]undo nat outbound
```

```
[H3C-GigabitEthernet1/0/2]#Jan 24 11:31:44:299 2019 H3C BFD/5/BFD_CHANGE_FSM: -COntext=  
1; Sess[1.1.1.2/1.1.1.1, LD/RD:97/97, Interface:GE1/0/2, SessType:Echo, LinkType:INET], Ver:1, Sta  
: DOWN->INIT, Diag: 0
```

```
%Jan 24 11:31:44:302 2019 H3C BFD/5/BFD_CHANGE_FSM: -COntext=1; Sess[1.1.1.2/1.1.1.1, LD/  
RD:97/97, Interface:GE1/0/2, SessType:Echo, LinkType:INET], Ver:1, Sta: INIT->UP, Diag: 0
```

```
[H3C-GigabitEthernet1/0/2]nat outbound 3999
```

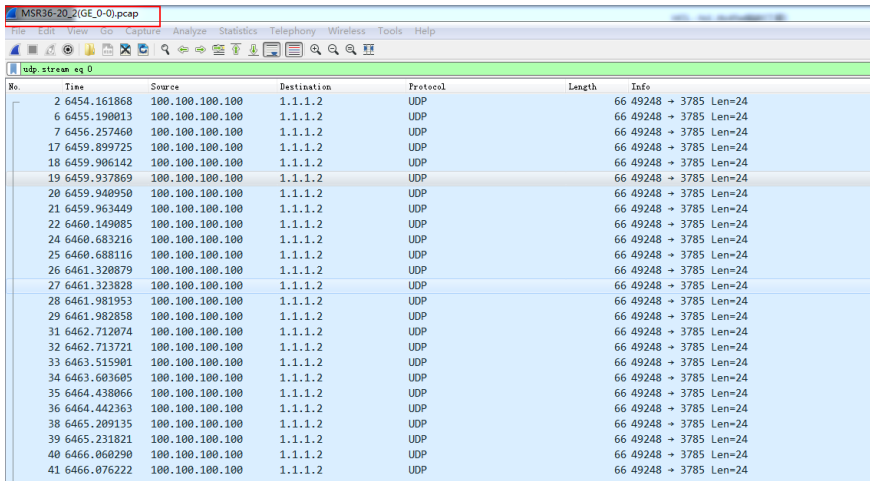
```
[H3C-GigabitEthernet1/0/2]display bfd session
```

```
Total Session Num: 1 Up Session Num: 1 Init Mode: Active
```

```
IPv4 Session Working Under Echo Mode:
```

LD SourceAddr DestAddr State Holdtime Interface
97 1.1.1.2 1.1.1.1 Up 1751ms GE1/0/2

4. 在路由器G0/0/0接口抓包



No.	Time	Source	Destination	Protocol	Length	Info
2	6454.161868	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
6	6455.190813	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
7	6456.257460	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
17	6459.899725	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
18	6459.906142	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
19	6459.937869	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
20	6459.940950	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
21	6459.963449	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
22	6460.149085	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
24	6460.683216	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
25	6460.688116	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
26	6461.320879	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
27	6461.323828	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
28	6461.981953	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
29	6461.982858	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
31	6462.712074	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
32	6462.713721	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
33	6463.515901	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
34	6463.603605	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
35	6464.438066	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
36	6464.442363	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
38	6465.209135	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
39	6465.231821	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
40	6466.060290	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24
41	6466.076222	100.100.100.100	1.1.1.2	UDP	66	49248 - 3785 Len=24

解决方法

可以这样理解，echo报文：封装在UDP报文中传送，其UDP目的端口号为3785。本端发送echo报文建立BFD会话，对端链路进行检测。对端不建立BFD会话，只需把收到的echo报文转发回本端。