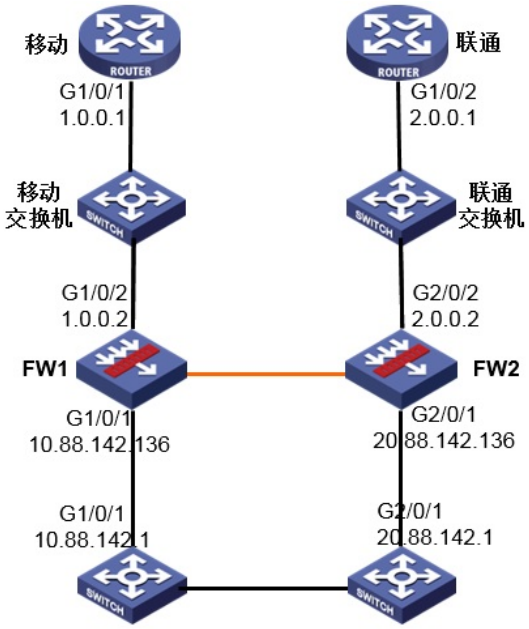
H3C V7防火墙在目标IP地址不可达的情况下实现流量切换

NQA 冗余组 冗余口 **杨海严** 2017-08-31 发表



H3C V7防火墙部署在出口，连接移动和联通的路由器，H3C V7防火墙和运营商路由器之间部署二层交换机，当移动路由器出现故障接口DOWN，H3C V7防火墙无法感知接口仍然UP，无法实现切换。本案例讲述track结合nqa探测实现切换：

（1）当FW1的接口G1/0/2（1.0.0.2）和目标IP地址1.0.0.1不可达的情况下，流量发生切换，走FW2；

（2）当故障消除，FW1的接口G1/0/2（1.0.0.2）和目标IP地址1.0.0.1可达的情况下，流量回切，走FW1。

接口配置、安全域、域间策略等基础配置不再累述，关键配置如下：

#创建ICMP-echo类型的NQA测试组（管理员为yhy，操作标签为123），并配置探测报文的目的地址为1.0.0.1，建立联动项。

```
<H3C>system-view
[H3C]nqa entry yhy 123
[H3C-nqa-yhy-123] type icmp-echo
[H3C-nqa-yhy-123-icmp-echo]destination ip 1.0.0.1
[H3C-nqa-yhy-123-icmp-echo]frequency 1000
[H3C-nqa-yhy-123-icmp-echo]next-hop ip 1.0.0.1
[H3C-nqa-yhy-123-icmp-echo]reaction 1 checked-element probe-fail threshold-type consecutive 1 acti
on-type trigger-only
[H3C-nqa-yhy-123-icmp-echo]quit
# 启动ICMP-echo测试操作，并一直进行测试。
[H3C]nqa schedule yhy 123 start-time now lifetime forever

#配置Track，监测上、下行接口的状态，track2关联nqa探测项
[H3C]track 1 interface GigabitEthernet1/0/1 physical
[H3C]track 2 nqa entry yhy 123 reaction 1
[H3C]track 3 interface GigabitEthernet2/0/1 physical
[H3C]track 4 interface GigabitEthernet2/0/2 physical

#配置冗余组
[H3C]redundancy group aaa
#创建Node 1，Node 1和FW1绑定，为主节点，成员接口为GE1/0/1和GE1/0/2。关联的Track项为1和2。
[H3C-redundancy-group-aaa]node 1
[H3C-redundancy-group-aaa-node-1]bind slot 1
[H3C-redundancy-group-aaa-node-1]priority 100
[H3C-redundancy-group-aaa-node-1]track 1 interface GigabitEthernet1/0/1
```

[H3C-redundancy-group-aaa-node-1]track 2 interface GigabitEthernet1/0/2
[H3C-redundancy-group-aaa-node-1]node-member interface GigabitEthernet1/0/1
[H3C-redundancy-group-aaa-node-1]node-member interface GigabitEthernet1/0/2
[H3C-redundancy-group-aaa-node-1]quit
#创建Node 2，Node 2和FW2绑定，为主节点，成员接口为GE2/0/1和GE2/0/2。关联的Track项为3和4。
[H3C-redundancy-group-aaa]node 2
[H3C-redundancy-group-aaa-node-2]bind slot 2
[H3C-redundancy-group-aaa-node-2]priority 50
[H3C-redundancy-group-aaa-node-2]track 3 interface GigabitEthernet2/0/1
[H3C-redundancy-group-aaa-node-2]track 4 interface GigabitEthernet2/0/2
[H3C-redundancy-group-aaa-node-2]node-member interface GigabitEthernet2/0/1
[H3C-redundancy-group-aaa-node-2]node-member interface GigabitEthernet2/0/2
[H3C-redundancy-group-aaa-node-2]quit

测试步骤：

（1）和目标IP 1.0.0.1 可达

<H3C>ping 1.0.0.1 //和目标IP 1.0.0.1 可达
Ping 1.0.0.1 (1.0.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.0.0.1: icmp_seq=0 ttl=255 time=1.109 ms
56 bytes from 1.0.0.1: icmp_seq=1 ttl=255 time=0.979 ms
56 bytes from 1.0.0.1: icmp_seq=2 ttl=255 time=0.975 ms
56 bytes from 1.0.0.1: icmp_seq=3 ttl=255 time=0.767 ms
56 bytes from 1.0.0.1: icmp_seq=4 ttl=255 time=0.997 ms
--- Ping statistics for 1.0.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.767/0.965/1.109/0.111 ms

<H3C>dis track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 18 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet1/0/1
    Protocol: None
Track ID: 2
  State: Positive   // track2是Positive
  Duration: 0 days 0 hours 0 minutes 21 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: yhy 123
    Reaction: 1
    Remote IP/URL: 1.0.0.1
    Local IP: --
    Interface: --
Track ID: 3
  State: Positive
  Duration: 0 days 1 hours 18 minutes 14 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/1
    Protocol: None
Track ID: 4
  State: Positive
  Duration: 0 days 1 hours 7 minutes 45 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/2
Protocol: None

<H3C>display redundancy group
Redundancy group aaa (ID 1):
  Node ID   Slot   Priority   Status   Track weight

```
 1          Slot1        100        Primary       255
 2          Slot2        50         Secondary     255

Preempt delay time remained     : 0    min
Preempt delay timer setting     : 1    min
Remaining hold-down time        : 0    sec
Hold-down timer setting         : 1    sec
Manual switchover request       : No

Member interfaces:

Node 1:
  Node member     Physical status
    GE1/0/1       UP
    GE1/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    1        Positive     255                GE1/0/1
    2        Positive     255                GE1/0/2
Node 2:
  Node member     Physical status
    GE2/0/1       UP
    GE2/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    3        Positive     255                GE2/0/1
    4        Positive     255                GE2/0/2
```

（2）和目标IP 1.0.0.1 不可达，流量切换

```
<H3C>ping 1.0.0.1    //和目标IP 1.0.0.1 不可达
Ping 1.0.0.1 (1.0.0.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
--- Ping statistics for 1.0.0.1 ---
4 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss

*Aug 23 21:38:21:859 2017 H3C NQA/7/Event: -COntext=1; NQA entry (yhy-123): Probe timed out.
*Aug 23 21:38:21:860 2017 H3C NQA/7/Reaction: -COntext=1; NQA entry (yhy-123) reaction (1): Sta
tus changed from below-threshold to over-threshold.
*Aug 23 21:38:21:860 2017 H3C NQA/7/Reaction: -COntext=1; NQA entry (yhy-123) reaction (1):
Trigger notified.
%Aug 23 21:38:21:864 2017 H3C RDDC/5/RDDC_ACTIVENODE_CHANGE: -COntext=1; Redundan
cy group aaa active node changed to node 2 (slot 2), because of node&＃39;s weight changed.  //冗
余组切换到node2
%Aug 23 21:38:21:908 2017 H3C IFNET/3/PHY_UPDOWN: -COntext=1; Physical state on the
interface GigabitEthernet1/0/1 changed to down.  //联动下行口DOWN
%Aug 23 21:38:21:908 2017 H3C IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on the i
nterface GigabitEthernet1/0/1 changed to down.



<H3C>dis track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 43 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet1/0/1
    Protocol: None
Track ID: 2
  State: Negative   // track2是Negative
  Duration: 0 days 0 hours 0 minutes 43 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
```

```
    NQA entry: yhy 123
    Reaction: 1
    Remote IP/URL: 1.0.0.1
    Local IP: --
    Interface: --
Track ID: 3
  State: Positive
  Duration: 0 days 1 hours 16 minutes 41 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/1
    Protocol: None
Track ID: 4
  State: Positive
  Duration: 0 days 1 hours 6 minutes 12 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/2
    Protocol: None

<H3C>
*Aug 23 21:38:25:859 2017 H3C NQA/7/Event: -COntext=1; NQA entry (yhy-123): Probe timed out.
*Aug 23 21:38:29:859 2017 H3C NQA/7/Event: -COntext=1; NQA entry (yhy-123): Probe timed out.
*Aug 23 21:38:33:859 2017 H3C NQA/7/Event: -COntext=1; NQA entry (yhy-123): Probe timed out.
<H3C>display redundancy group
Redundancy group aaa (ID 1):
  Node ID      Slot          Priority   Status        Track weight
  1            Slot1         100        Secondary     -255 //权值改变，状态切换成功
  2            Slot2         50         Primary       255

Preempt delay time remained     : 0     min
Preempt delay timer setting     : 1     min
Remaining hold-down time        : 0     sec
Hold-down timer setting         : 1     sec
Manual switchover request       : No

Member interfaces:

Node 1:
  Node member     Physical status
    GE1/0/1       DOWN(redundancy down)  //联动下行口DOWN
    GE1/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    1        Negative     255                GE1/0/1
    2        Negative     255                GE1/0/2(Fault)  //故障口
Node 2:
  Node member     Physical status
    GE2/0/1       UP
    GE2/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    3        Positive     255                GE2/0/1
    4        Positive     255                GE2/0/2

<H3C>debug ip icmp
This command is CPU intensive and might affect ongoing services. Are you sure you want to
continue? [Y/N]:Y
<H3C>
*Aug 23 21:39:42:852 2017 H3C SOCKET/7/ICMP: -COntext=1;
ICMP Output:   //发出请求，但是未回应
 ICMP Packet: src = 1.0.0.2, dst = 1.0.0.1
              type = 8, code = 0 (echo)
*Aug 23 21:39:46:852 2017 H3C SOCKET/7/ICMP: -COntext=1;
```

```
ICMP Output:
 ICMP Packet: src = 1.0.0.2, dst = 1.0.0.1
              type = 8, code = 0 (echo)
```

（3）和目标IP 1.0.0.1 恢复成可达状态，流量回切

```
<H3C>ping 1.0.0.1  //和IP 1.0.0.1 恢复可达
Ping 1.0.0.1 (1.0.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.0.0.1: icmp_seq=0 ttl=255 time=1.109 ms
56 bytes from 1.0.0.1: icmp_seq=1 ttl=255 time=0.979 ms
56 bytes from 1.0.0.1: icmp_seq=2 ttl=255 time=0.975 ms
56 bytes from 1.0.0.1: icmp_seq=3 ttl=255 time=0.767 ms
56 bytes from 1.0.0.1: icmp_seq=4 ttl=255 time=0.997 ms

--- Ping statistics for 1.0.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.767/0.965/1.109/0.111 ms

*Aug 23 21:40:15:869 2017 H3C NQA/7/Event: -COntext=1; NQA entry (yhy-123): Probe timed out.
*Aug 23 21:40:16:866 2017 H3C NQA/7/Reaction: -COntext=1; NQA entry (yhy-123) reaction (1): Sta
tus changed from over-threshold to below-threshold.
*Aug 23 21:40:16:866 2017 H3C NQA/7/Reaction: -COntext=1; NQA entry (yhy-123) reaction (1):
Trigger notified.
%Aug 23 21:40:20:017 2017 H3C IFNET/3/PHY_UPDOWN: -COntext=1; Physical state on the
interface GigabitEthernet1/0/1 changed to up. //联动下行口UP
%Aug 23 21:40:20:017 2017 H3C IFNET/5/LINK_UPDOWN: -COntext=1; Line protocol state on the i
nterface GigabitEthernet1/0/1 changed to up.

<H3C>display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 18 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet1/0/1
    Protocol: None
Track ID: 2
  State: Positive  //track2状态变为Positive
  Duration: 0 days 0 hours 0 minutes 21 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: yhy 123
    Reaction: 1
    Remote IP/URL: 1.0.0.1
    Local IP: --
    Interface: --
Track ID: 3
  State: Positive
  Duration: 0 days 1 hours 18 minutes 14 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/1
    Protocol: None
Track ID: 4
  State: Positive
  Duration: 0 days 1 hours 7 minutes 45 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    Interface: GigabitEthernet2/0/2
    Protocol: None

<H3C>display redundancy group
Redundancy group aaa (ID 1):
  Node ID      Slot          Priority   Status        Track weight
  1            Slot1         100        Secondary     255  //权值正常，状态暂未切换
```

```
 2           Slot2        50         Primary     255

Preempt delay time remained     : 1     min
Preempt delay timer setting     : 1     min
Remaining hold-down time        : 0     sec
Hold-down timer setting         : 1     sec
Manual switchover request       : No

Member interfaces:

Node 1:
  Node member     Physical status
    GE1/0/1       UP
    GE1/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    1        Positive     255                GE1/0/1
    2        Positive     255                GE1/0/2
Node 2:
  Node member     Physical status
    GE2/0/1       UP
    GE2/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    3        Positive     255                GE2/0/1
    4        Positive     255                GE2/0/2

<H3C>
%Aug 23 21:41:17:671 2017 H3C RDDC/5/RDDC_ACTIVENODE_CHANGE: -COntext=1; Redundan
cy group aaa active node changed to node 1 (slot 1), because of node&＃39;s weight changed.  //冗
余组回切成功
<H3C>display redundancy group
Redundancy group aaa (ID 1):
  Node ID      Slot          Priority   Status        Track weight
  1            Slot1         100        Primary       255   //状态切换成功
  2            Slot2         50         Secondary     255

Preempt delay time remained     : 0     min
Preempt delay timer setting     : 1     min
Remaining hold-down time        : 0     sec
Hold-down timer setting         : 1     sec
Manual switchover request       : No

Member interfaces:

Node 1:
  Node member     Physical status
    GE1/0/1       UP
    GE1/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    1        Positive     255                GE1/0/1
    2        Positive     255                GE1/0/2
Node 2:
  Node member     Physical status
    GE2/0/1       UP
    GE2/0/2       UP
  Track info:
    Track    Status       Reduced weight     Interface
    3        Positive     255                GE2/0/1
4        Positive     255                GE2/0/2
```

（1）NQA一定要配置正确，要记得启动ICMP-echo测试操作；

（2）track项要调用nqa探测项，而track 1 interface GigabitEthernet1/0/1 protocol ipv4监控的是本设备接口状态，无法监控对端设备的接口状态。