

某局点MSR810-W使用NQA ICMP-echo进行IPsec VPN保活不生效处理经验案例

IPSec VPN

俞璐

2018-06-21 发表

组网及说明

略。

问题描述

现场分支采用MSR810-W和总部其他厂商设备建立IPsec VPN，客户在使用过程中出现分支总部VPN终端，需要分支侧Reset ipsec sa、ike sa后重新建立IPsec VPN网络才能恢复。由于总部不支持DPD检测，故现场采用NQA ICMP-echo来实现IPsec隧道保活。现场配置如下：

```
#
nqa entry admin idcvpn
type icmp-echo
destination ip 192.168.102.1
history-record enable
history-record number 10
probe count 10
probe timeout 1000
source ip 192.168.32.1

#
nqa entry admin zbvpn
type icmp-echo
destination ip 192.168.2.254
history-record enable
history-record number 10
probe count 10
probe timeout 1000
source ip 192.168.32.1

#
nqa schedule admin idcvpn start-time now lifetime forever
nqa schedule admin zbvpn start-time now lifetime forever

#
```

过程分析

现场配置完NQA测试组功能后依旧现场IPsec不通的故障，查看NQA测试结果都是失败的。

[MSR810]dis nqa result

NQA entry (admin admin, tag zbvpn) test results:

```
Send operation times: 10      Receive response times: 0
Min/Max/Average round trip time: 0/0/0
Square-Sum of round trip time: 0
Last succeeded probe time: 0000-00-00 00:00:00.0
```

Extended results:

```
Packet loss ratio: 100%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 10
```

NQA entry (admin admin, tag idcvpn) test results:

```
Send operation times: 10      Receive response times: 0
Min/Max/Average round trip time: 0/0/0
Square-Sum of round trip time: 0
Last succeeded probe time: 0000-00-00 00:00:00.0
```

Extended results:

```
Packet loss ratio: 100%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 10
```

现场将NQA删除重新配置后，NQA ICMP-echo探测成功，此时IPsec vpn恢复。

[MSR810]undo nqa schedule admin idcvpn

[MSR810]undo nqa schedule admin zbvpn

```

[MSR810]undo nqa entry admin idcvpn
[MSR810]undo nqa entry admin zbvpn
[MSR810]nqa entry admin idcvpn
[MSR810-nqa-admin-idcvpn] type icmp-echo
[MSR810-nqa-admin-idcvpn-icmp-echo] destination ip 192.168.102.1
[MSR810-nqa-admin-idcvpn-icmp-echo] history-record enable
[MSR810-nqa-admin-idcvpn-icmp-echo] history-record number 10
[MSR810-nqa-admin-idcvpn-icmp-echo] probe count 10
[MSR810-nqa-admin-idcvpn-icmp-echo] probe timeout 1000
[MSR810-nqa-admin-idcvpn-icmp-echo] source ip 192.168.32.1
[MSR810-nqa-admin-idcvpn-icmp-echo]#
[MSR810-nqa-admin-idcvpn-icmp-echo]nqa entry admin zbvpn
[MSR810-nqa-admin-zbvpn] type icmp-echo
[MSR810-nqa-admin-zbvpn-icmp-echo] destination ip 192.168.2.254
[MSR810-nqa-admin-zbvpn-icmp-echo] history-record enable
[MSR810-nqa-admin-zbvpn-icmp-echo] history-record number 10
[MSR810-nqa-admin-zbvpn-icmp-echo] probe count 10
[MSR810-nqa-admin-zbvpn-icmp-echo] probe timeout 1000
[MSR810-nqa-admin-zbvpn-icmp-echo] source ip 192.168.32.1
[MSR810-nqa-admin-zbvpn-icmp-echo] nqa schedule admin idcvpn start-time now lifetime forever
[MSR810] nqa schedule admin zbvpn start-time now lifetime forever
[MSR810]dis nqa result

```

NQA entry (admin admin, tag zbvpn) test results:

```

Send operation times: 10      Receive response times: 10
Min/Max/Average round trip time: 4/7/5
Square-Sum of round trip time: 271
Last succeeded probe time: 2011-01-17 11:10:43.5

```

Extended results:

```

Packet loss ratio: 0%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0

```

NQA entry (admin admin, tag idcvpn) test results:

```

Send operation times: 10      Receive response times: 10
Min/Max/Average round trip time: 2/3/2
Square-Sum of round trip time: 85
Last succeeded probe time: 2011-01-17 11:10:43.4

```

Extended results:

```

Packet loss ratio: 0%
Failures due to timeout: 0
Failures due to internal error: 0
Failures due to other errors: 0

```

[MSR810]dis nqa his

[MSR810]dis nqa history

NQA entry (admin admin, tag zbvpn) history records:

Index	Response	Status	Time
10	4	Succeeded	2011-01-17 11:10:43.5
9	4	Succeeded	2011-01-17 11:10:43.5
8	5	Succeeded	2011-01-17 11:10:43.5
7	4	Succeeded	2011-01-17 11:10:43.5
6	6	Succeeded	2011-01-17 11:10:43.5
5	6	Succeeded	2011-01-17 11:10:43.5
4	6	Succeeded	2011-01-17 11:10:43.5
3	4	Succeeded	2011-01-17 11:10:43.4
2	5	Succeeded	2011-01-17 11:10:43.4
1	7	Succeeded	2011-01-17 11:10:43.4

NQA entry (admin admin, tag idcvpn) history records:

Index	Response	Status	Time
10	3	Succeeded	2011-01-17 11:10:43.4
9	2	Succeeded	2011-01-17 11:10:43.4
8	3	Succeeded	2011-01-17 11:10:43.4
7	3	Succeeded	2011-01-17 11:10:43.4
6	3	Succeeded	2011-01-17 11:10:43.4
5	3	Succeeded	2011-01-17 11:10:43.4

4	3	Succeeded	2011-01-17 11:10:43.4
3	3	Succeeded	2011-01-17 11:10:43.4
2	3	Succeeded	2011-01-17 11:10:43.4
1	3	Succeeded	2011-01-17 11:10:43.4

既然配置了NQA探测，IPsec VPN隧道应该处于永久保活状态，为何还会出现IPsec不通的情况。我们仔细分析命令手册，发现有这样一条说明：

【命令】

frequency interval

undo frequency

【缺省情况】

在NQA测试类型视图下，Voice、Path-jitter测试中连续两次测试开始时间的时间间隔为60000毫秒；其他类型的测试中连续两次测试开始时间的时间间隔为0毫秒，即只进行一次测试。

也就是说，NQA ICMP-echo缺省只进行了一次测试，将其删除重新配置后，又重新进行一次测试，流量重新触发IPsec建立。

解决方法

#

```
nqa schedule admin idcvpn start-time now lifetime forever
```

```
nqa schedule admin zbvpn start-time now lifetime forever
```

#

很多人认为配置nqa schedule XXX forever就会一直进行测试，但是实际NQA ICMP-echo只进行了一次测试。如需进行永久测试增加以下配置即可：

```
[Sysname-nqa-admin-idcvpn] type icmp-echo
```

```
[Sysname-nqa-admin-idcvpn-icmp-echo] frequency 1000
```