MSR 系列路由器利用 NQA 探测在固定时间段内保持 IPsec 隧道的连通性配置举例

目 录

1 简介

本文档介绍利用 NQA 探测在固定时间段内保持 IPsec 隧道的连通性的典型配置举例。

2 配置前提

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解 NQA、NTP、防火墙和 IPsec 的相关特性。

3 配置举例

3.1 组网需求

如 图 1 所示，Router A和Router B是企业总部和分支的安全网关，两者之间已建立IPsec VPN隧道，并且Router A和Router B已配置了内网到外网的NAT转换，Router A已通过DHCP服务器自动获取了地址。要求在Router A上配置NQA探测来刷新链路状态，保持隧道的连通性，并通过防火墙来控制进行NQA探测的时段。

图1 利用 NQA 探测在固定时间段内保持 IPsec 隧道的连通性配置组网图

3.2 配置思路

- 要在固定时间段进行 NQA 的探测必须要先配置时间段。为了保证时间的准确性，可以先设置系统的时区，并用 NTP 与知名的网络时间服务器进行时间同步。
- 为了保证在规定时间内进行探测，可以利用防火墙来控制进行 NQA 探测的时间段。
- 为了方便统计与查看 NQA 的探测情况，可开启 NQA 测试组的历史记录功能。

3.3 使用版本

本举例是在 Release 2317 版本上进行配置和验证的。

3.4 配置注意事项

- IPsec 响应端使用野蛮模式的时候不用配置 ACL。

- 在进行 UDP-echo 测试之前，需要在 NQA 服务器端配置 UDP 监听功能。
- IPsec 安全提议缺省配置中，未配置 ESP 协议的认证算法，需手动指定。

3.5 配置步骤

3.5.1 Router A的配置

配置 NTP 功能进行时间同步。

```
<RouterA> system-view
[RouterA] ntp-service unicast-server 207.46.232.182
[RouterA] ntp-service unicast-server 207.46.197.32
[RouterA] ntp-service unicast-server 192.43.244.18
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ip address 1.1.1.1 255.255.255.0
[RouterA-Ethernet0/0] quit
```

配置系统所在的时区为美国东部时区。

```
[RouterA] clock timezone EST minus 5
```

创建名为 time 的时间段，范围为每天的 8 点到 12 点。

```
[RouterA] time-range time 08:00 to 12:00 daily
```

创建 ACL3001，只允许在规定的时间范围内进行 NQA 的探测。

```
[RouterA] acl number 3001
[RouterA-acl-adv-3001] rule 0 permit udp destination 1.1.1.2 0 destination-port eq
 8000 time-range time
[RouterA-acl-adv-3001] quit
```

创建一个 IKE 对等体，并进入 IKE-Peer 视图。

```
[RouterA] ike peer peer
```

配置 IKE 第一阶段的协商模式为野蛮模式。

```
[RouterA-ike-peer-peer] exchange-mode aggressive
```

配置预共享密钥。

```
[RouterA-ike-peer-peer] pre-shared-key 123
```

配置对端安全网关 IP 地址。

```
[RouterA-ike-peer-peer] remote-address 1.1.1.2
```

启用 NAT 穿越功能。

```
[RouterA-ike-peer-peer] nat traversal
[RouterA-ike-peer-peer] quit
```

采用安全提议的缺省配置。

```
[RouterA] ipsec proposal def
```

配置 ESP 协议采用 md5 认证算法。

```
[RouterA-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterA-ipsec-transform-set-def] quit
```

创建 IPsec 安全策略 policy，其协商方式为 isakmp。

```
[RouterA] ipsec policy policy 1 isakmp
```

配置 IPsec 安全策略引用的访问控制列表。

```
[RouterA-ipsec-policy-isakmp-policy-1] security acl 3001
```

配置 IPsec 安全策略所引用的 IPsec 安全提议。

```
[RouterA-ipsec-policy-isakmp-policy-1] transform-set def
```

在 IPsec 安全策略中引用 IKE 对等体。

```
[RouterA-ipsec-policy-isakmp-policy-1] ike-peer peer
[RouterA-ipsec-policy-isakmp-policy-1] quit
```

利用防火墙来控制进行 NQA 探测的时间段。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] firewall packet-filter 3001 outbound
```

在接口上应用安全策略。

```
[RouterA-Ethernet0/0] ipsec policy policy
[RouterA-Ethernet0/0] quit
```

创建 UDP-echo 类型的测试组。

```
[RouterA] nqa entry admin test
[RouterA-nqa-admin-test] type udp-echo
```

配置测试操作的目的地址为 1.1.1.2，目的端口号为 8000。

```
[RouterA-nqa-admin-test-udp-echo] destination ip 1.1.1.2
[RouterA-nqa-admin-test-udp-echo] destination port 8000
```

测试组连续两次测试开始时间的时间间隔为 3000 毫秒。

```
[RouterA-nqa-admin-test-udp-echo] frequency 3000
```

开启 NQA 测试组的历史记录保存功能。

```
[RouterA-nqa-admin-test-udp-echo] history-record enable
```

配置一次 NQA 测试中进行探测的次数为 2。

```
[RouterA-nqa-admin-test-udp-echo] probe count 2
```

配置 NQA 探测超时时间为 50000 毫秒。

```
[RouterA-nqa-admin-test-udp-echo] probe timeout 50000
[RouterA-nqa-admin-test-udp-echo] quit
```

立即启动测试操作，并一直进行测试。

```
[RouterA] nqa schedule admin test start-time now lifetime forever
```

3.5.2 Router B的配置

配置 NTP 功能进行时间同步。

```
<RouterB> system-view
[RouterB] ntp-service unicast-server 207.46.232.182
[RouterB] ntp-service unicast-server 207.46.197.32
[RouterB] ntp-service unicast-server 192.43.244.18
```

配置系统所在的时区为美国东部时区。

```
[RouterB] clock timezone EST minus 5
```

配置接口 Ethernet0/0 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface ethernet 0/0
```

```
[RouterB-Ethernet0/0] ip address 1.1.1.2 255.255.255.0
[RouterB-Ethernet0/0] quit
```
创建一个 IKE 对等体，并进入 IKE-Peer 视图。
```
[RouterB] ike peer peer
```
配置 IKE 第一阶段的协商模式为野蛮模式。
```
[RouterB-ike-peer-peer] exchange-mode aggressive
```
配置预共享密钥。
```
[RouterB-ike-peer-peer] pre-shared-key 123
```
启用 NAT 穿越功能。
```
[RouterB-ike-peer-peer] nat traversal
[RouterB-ike-peer-peer] quit
```
采用安全提议的缺省配置。
```
[RouterB] ipsec proposal def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterB-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterB-ipsec-transform-set-def] quit
```
创建 IPsec 安全策略模板 policy，并进入 IPsec 安全策略模板视图。
```
[RouterB] ipsec policy-template policy 1
```
在 IPsec 安全策略中引用 IKE 对等体。
```
[RouterB-ipsec-policy-template-policy-1] ike-peer peer
```
配置 IPsec 安全策略所引用的 IPsec 安全提议。
```
[RouterB-ipsec-policy-template-policy-1] proposal def
```
引用 IPsec 安全策略模板创建一条 IPsec 安全策略。
```
[RouterB-ipsec-policy-template-policy-1] ipsec policy policy1 1 isakmp template
Policy
[RouterB-ipsec-policy-template-policy-1] quit
```
在接口 Ethernet0/0 上应用安全策略。
```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ipsec policy policy1
[RouterB-Ethernet0/0] quit
```
开启 NQA 服务器功能，配置监听的 IP 地址为 1.1.1.2，UDP 端口号为 8000。
```
[RouterB] nqa server enable
[RouterB] nqa server udp-echo 1.1.1.2 8000
```

3.6 验证配置

完成以上配置后，Router A 到达配置的时间范围内，开始进行 NQA 探测，并触发 IKE 进行协商建立 SA。IKE 协商成功后便可以创建 IPsec SA，从而保持 VPN 的连通性。

显示 UDP-echo 测试的历史记录。
```
[RouterA] display nqa history
  NQA entry (admin admin, tag test) history record(s):
    Index      Response     Status           Time
    1218       11           Succeeded        2013-06-05 10:58:31.4
```

```
    1217       8            Succeeded        2013-06-05 10:58:31.4
    1216       10           Succeeded        2013-06-05 10:58:28.4
    1215       8            Succeeded        2013-06-05 10:58:28.4
    1214       10           Succeeded        2013-06-05 10:58:25.4
    1213       7            Succeeded        2013-06-05 10:58:25.4
    1212       10           Succeeded        2013-06-05 10:58:22.4
    1211       8            Succeeded        2013-06-05 10:58:22.4
    1210       10           Succeeded        2013-06-05 10:58:19.4
    1209       8            Succeeded        2013-06-05 10:58:19.4
```

可以通过如下显示信息看到，Router A 作为发起方已与 Router B 协商生成了两个阶段的 SA。

```
 [RouterA] display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  -----------------------------------------------------------------
     1             1.1.1.2                 RD|ST       1       IPSEC
     2             1.1.1.2                 RD|ST       2       IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK—REKEY
```

可以通过如下显示信息查看协商生成的 IPsec SA。

```
[RouterA] display ipsec sa
==============================
Interface: Ethernet0/0
    path MTU: 1500
==============================

  ----------------------------
  IPsec policy name: "policy"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 1.1.1.2
    flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: UDP
        dest addr: 1.1.1.2/255.255.255.255  port: 8000  protocol: UDP

    [inbound ESP SAs]
      spi: 0xBD7257D2(3178387410)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 1
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843177/3332
      anti-replay detection: Enabled
```

```
    anti-replay window size(counter based): 32
  udp encapsulation used for nat traversal: N

[outbound ESP SAs]
  spi: 0xEA170DA6(3927379366)
  transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
  in use setting: Tunnel
  connection id: 2
  sa duration (kilobytes/sec): 1843200/3600
  sa remaining duration (kilobytes/sec): 1843177/3332
  anti-replay detection: Enabled
    anti-replay window size(counter based): 32
  udp encapsulation used for nat traversal: N
```

3.7 配置文件

- Router A：

```
#
clock timezone EST minus 05:00:00
#
time-range time 08:00 to 12:00 daily
#
acl number 3001
 rule 0 permit udp destination 1.1.1.2 0 destination-port eq 8000 time-range tim
e
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$y3TA3pnujTdYAJ+OmZcOpjnhzzFwkQ==
 remote-address 1.1.1.2
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy policy 1 isakmp
 security acl 3001
 ike-peer peer
 transform-set def
#
interface Ethernet0/0
 port link-mode route
firewall packet-filter 3001 outbound
 ip address 1.1.1.1 255.255.255.0
 ipsec policy policy
#
```

```
nqa entry admin test
 type udp-echo
  destination ip 1.1.1.2
  destination port 8000
  frequency 3000
  history-record enable
  probe count 2
  probe timeout 50000
#
 nqa schedule admin test start-time now lifetime forever
#
 ntp-service unicast-server 207.46.232.182
 ntp-service unicast-server 207.46.197.32
 ntp-service unicast-server 192.43.244.18
#
```

- Router B：

```
#
clock timezone EST minus 05:00:00
#
ike peer peer
 exchange-mode aggressive
 pre-shared-key cipher $c$3$LGxdivAwVW08EdMCk3IZLKGChom9aQ==
 nat traversal
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy-template policy 1
 ike-peer peer
 transform-set def
#
ipsec policy policy1 1 isakmp template policy
#
interface Ethernet0/0
 port link-mode route
ip address 1.1.1.2 255.255.255.0
 ipsec policy policy1
#
nqa server enable
 nqa server udp-echo 1.1.1.2 8000
#
ntp-service unicast-server 207.46.232.182
ntp-service unicast-server 207.46.197.32
ntp-service unicast-server 192.43.244.18
#
```

4 相关资料

- H3C MSR 系列路由器 命令参考(V5)-R2311
- H3C MSR 系列路由器 配置指导(V5)-R2311