MSR 系列路由器 IPsec with VRRP 典型配置举例

目 录

1 简介

本文档介绍 IPsec with VRRP 的典型配置举例。

IPsec 支持隧道一端采用 VRRP 的虚拟 IP 地址进行 IKE 协商。利用 DPD 的特性，还可以做到在使用 VRRP 地址的隧道一端，当 Master 故障时，IKE 重新与 Slave 进行协商，重新建立 IPsec 隧道。

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。

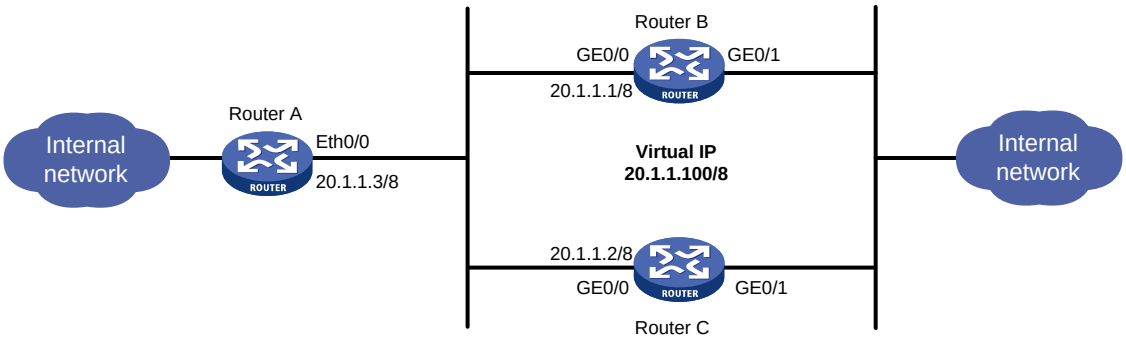
本文档假设您已了解 IPsec 和 VRRP 特性。

3 配置举例

3.1 组网需求

如 图 1 所示，RouterA是分支的接入路由器，RouterB和RouterC分别是总部的主用和备用路由器，分支机构在 40.0.0.0 网段，总部在 30.0.0.0 网段，要求：RouterA与VRRP的虚拟地址建立IPsec隧道，配合DPD特性，实现在主用路由器故障时的动态切换。

图1 IPsec with VRRP 配置组网图



3.2 配置思路

- 为了让 Router B 成为 Master，需要为 Router B 配置较高的优先级（默认优先级为 100）；
- 为了与备份组建立 IPsec 隧道，Router A 上 IKE 指定对端地址为 VRRP 虚地址；

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

配置 VRRP 虚地址的一端如果作为发起方，还是会选取接口的主地址进行协商，因此在 IPsec 与 VRRP 的组合应用环境中，应该让配置 VRRP 的一方作为 IKE 协商的响应方，而非发起方。

3.5 配置步骤

3.5.1 RouterA的配置

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
<RouterA> system-view
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 40.0.0.0 0.255.255.255 destination 30.0.0.0
0.255.255.255
[RouterA-acl-adv-3000] quit
```

创建一个 DPD 并采用默认配置。

```
[RouterA] ike dpd 1
[RouterA-ike-dpd-1] quit
```

配置 IKE 对等体。

```
[RouterA] ike peer vrrp
[RouterA-ike-peer-vrrp] pre-shared-key vrrp
[RouterA-ike-peer-vrrp] remote-address 20.1.1.100
[RouterA-ike-peer-vrrp] dpd 1
[RouterA-ike-peer-vrrp] quit
```

采用 IPsec 安全提议的缺省配置。

```
[RouterA] ipsec proposal vrrp
[RouterA-ipsec-proposal-vrrp] quit
```

配置 IPsec 策略。

```
[RouterA] ipsec policy vrrp 1 isakmp
[RouterA-ipsec-policy-isakmp-vrrp-1] security acl 3000
[RouterA-ipsec-policy-isakmp-vrrp-1] ike-peer vrrp
[RouterA-ipsec-policy-isakmp-vrrp-1] proposal vrrp
[RouterA-ipsec-policy-isakmp-vrrp-1] quit
```

在接口 Ethernet0/0 上应用 IPsec 策略。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] port link-mode route
[RouterA-Ethernet0/0] ip address 20.1.1.3 255.0.0.0
[RouterA-Ethernet0/0] ipsec policy vrrp
[RouterA-Ethernet0/0] quit
[RouterA] ip route-static 30.0.0.0 255.0.0.0 20.1.1.100
```

3.5.2 RouterB的配置

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
<RouterB> system-view
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 30.0.0.0 0.255.255.255 destination 40.0.0.0
0.255.255.255
[RouterB-acl-adv-3000] quit
```

配置 IKE 对等体。

```
[RouterB] ike peer vrrp
[RouterB-ike-peer-vrrp] pre-shared-key vrrp
[RouterB-ike-peer-vrrp] remote-address 20.1.1.3
[RouterB-ike-peer-vrrp] quit
```

配置 IPsec 安全提议。

```
[RouterB] ipsec proposal vrrp
[RouterB-ipsec-proposal-vrrp] encapsulation-mode tunnel
[RouterB-ipsec-proposal-vrrp] transform esp
[RouterB-ipsec-proposal-vrrp] esp encryption-algorithm des
[RouterB-ipsec-proposal-vrrp] esp authentication-algorithm md5
[RouterB-ipsec-proposal-vrrp] quit
```

配置 IPsec 策略。

```
[RouterB] ipsec policy vrrp 1 isakmp
[RouterB-ipsec-policy-isakmp-vrrp-1] security acl 3000
[RouterB-ipsec-policy-isakmp-vrrp-1] ike-peer vrrp
[RouterB-ipsec-policy-isakmp-vrrp-1] proposal vrrp
[RouterB-ipsec-policy-isakmp-vrrp-1] quit
```

配置 VRRP。

```
[RouterB] interface gigabitethernet 0/0
[RouterB-GigabitEthernet0/0] vrrp vrid 100 virtual-ip 20.1.1.100
[RouterB-GigabitEthernet0/0] vrrp vrid 100 priority 150
```

在接口 GigabitEthernet0/0 上应用 IPsec 策略。

```
[RouterB-GigabitEthernet0/0] ipsec policy vrrp
[RouterB-GigabitEthernet0/0] quit
[RouterB] ip route-static 40.0.0.0 255.0.0.0 20.1.1.3
```

3.5.3 RouterC的配置

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
<RouterC> system-view
[RouterC] acl number 3000
[RouterC-acl-adv-3000] rule 0 permit ip source 30.0.0.0 0.255.255.255 destination 40.0.0.0
0.255.255.255
[RouterC-acl-adv-3000] quit
```

配置 IKE 对等体。

```
[RouterC] ike peer vrrp
[RouterC-ike-peer-vrrp] pre-shared-key vrrp
```

```
[RouterC-ike-peer-vrrp] remote-address 20.1.1.3
[RouterC-ike-peer-vrrp] quit
```
配置 IPSec 安全提议。
```
[RouterC] ipsec proposal vrrp
[RouterC-ipsec-proposal-vrrp] encapsulation-mode tunnel
[RouterC-ipsec-proposal-vrrp] transform esp
[RouterC-ipsec-proposal-vrrp] esp encryption-algorithm des
[RouterC-ipsec-proposal-vrrp] esp authentication-algorithm md5
[RouterC-ipsec-proposal-vrrp] quit
```
配置 IPsec 策略。
```
[RouterC] ipsec policy vrrp 1 isakmp
[RouterC-ipsec-policy-isakmp-vrrp-1] security acl 3000
[RouterC-ipsec-policy-isakmp-vrrp-1] ike-peer vrrp
[RouterC-ipsec-policy-isakmp-vrrp-1] proposal vrrp
[RouterC-ipsec-policy-isakmp-vrrp-1] quit
```
配置 VRRP。
```
[RouterC] interface eigabitethernet 0/0
[RouterC-GigabitEthernet0/0] vrrp vrid 100 virtual-ip 20.1.1.100
```
在接口 GigabitEthernet0/0 上应用 IPsec 策略。
```
[RouterC-GigabitEthernet0/0] ipsec policy vrrp
[RouterC-GigabitEthernet0/0] quit
[RouterC] ip route-static 40.0.0.0 255.0.0.0 20.1.1.3
```

3.6 验证配置

查看 VRRP 状态，RouterB 拥有更高的 VRRP 优先级，因此 VRRP 协商状态应为 Master，RouterC 为 Backup。
```
%Jun 12 10:48:39:160 2006 RouterB VRRP/5/MasterChange:
 IPv4 GigabitEthernet0/0/0 | Virtual Router 100 :  BACKUP --> MASTER    reason:Timer fired
%Jun 12 10:48:42:744 2006 RouterC VRRP/5/MasterChange:
IPv4 GigabitEthernet0/0/0 | Virtual Router 100 :  MASTER --> BACKUP    reason:Received VRRP
packet
```
从分支机构 ping 总部的 IP 地址，IKE 协商成功后可以 ping 通。
```
<RouterA> ping -a 40.1.1.1 30.1.1.1
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

通过 diplay ike sa 和 display ipsec sa brief 命令可以在 RouterA 和 RouterB 上查看到 sa 建立情况：

```
<RouterA> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  --------------------------------------------------------
       19          20.1.1.100      RD|ST         2     IPSEC
       18          20.1.1.100      RD|ST         1     IPSEC

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

<RouterA> display ipsec sa brief
 total phase-2 SAs: 2
Src Address     Dst Address     SPI        Protocol  Algorithm
-------------------------------------------------------------
20.1.1.3        20.1.1.100      1795685915 ESP       E:DES
                                                     A:HMAC-MD5-96;
20.1.1.100      20.1.1.3        1353813377 ESP       E:DES
                                                     A:HMAC-MD5-96;

<RouterB> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  --------------------------------------------------------
       9           20.1.1.3        RD            2     IPSEC
       8           20.1.1.3        RD            1     IPSEC

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

<RouterB> display ipsec sa brief
 total phase-2 SAs: 2
Src Address     Dst Address     SPI        Protocol  Algorithm
-------------------------------------------------------------
20.1.1.3        20.1.1.100      1795685915 ESP       E:DES
                                                     A:HMAC-MD5-96;
20.1.1.100      20.1.1.3        1353813377 ESP       E:DES
                                                     A:HMAC-MD5-96;
```

关闭 RouterB 的 GigabitEthernet0/0 接口，RouterB 的 VRRP 状态切换到 backup，RouterC 的 VRRP 状态切换到 Master。重新从分支机构 ping 总部的 IP 地址，DPD 监测到对端 SA 不存在，重试 3 次后，会删除本端 SA，重新与 RouterC 进行 IKE 协商，建立 SA 后，可以 ping 通。

```
%Jun 12 10:59:10:291 2006 RouterB VRRP/5/MasterChange:
IPv4 GigabitEthernet0/0/0 | Virtual Router 100 :  MASTER --> INITIALIZE    reason: Received
interface event
%Jun 12 10:59:15:151 2006 RouterC VRRP/5/MasterChange:
IPv4 GigabitEthernet0/0/0 | Virtual Router 100 :  BACKUP --> MASTER    reason:Timer fired

<RouterA> ping -a 40.1.1.1 30.1.1.1
```

```
  PING 30.1.1.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 30.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

<RouterC> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  --------------------------------------------------------------
        5          20.1.1.3        RD            2     IPSEC
        6          20.1.1.3        RD            1     IPSEC

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

<RouterC> display ipsec sa brief
 total phase-2 SAs: 2
Src Address     Dst Address     SPI        Protocol  Algorithm
-----------------------------------------------------------------
20.1.1.3        20.1.1.100      483652851  ESP       E:DES
                                                     A:HMAC-MD5-96;
20.1.1.100      20.1.1.3        1727023681 ESP       E:DES
                                                     A:HMAC-MD5-96;
```

当 RouterB 的 GigabitEthernet0/0 接口重新 UP 时，VRRP 状态切换会 MASTER，从分支到总部的数据流会重新发送到 RouterB 上，DPD 发现 SA 不存在重传超时后，RouterA 删除 SA 重新与 RouterB 进行 IKE 协商，协商成功后分支到总部的数据流会在新的 IPSec 隧道上得以传输。

3.7 配置文件

- Router A：

```
#
acl number 3000
 rule 0 permit ip source 40.0.0.0 0.255.255.255 destination 30.0.0.0 0.255.255.255
#
ike dpd 1
```

```
#
ike peer vrrp
 pre-shared-key cipher kswMMJ0oAIg=
 remote-address 20.1.1.100
 dpd 1
#
ipsec proposal vrrp
#
ipsec policy vrrp 1 isakmp
 security acl 3000
 ike-peer vrrp
 proposal vrrp
#
interface Ethernet0/0
 port link-mode route
 ip address 20.1.1.3 255.0.0.0
 ipsec policy vrrp
#
ip route-static 30.0.0.0 255.0.0.0 20.1.1.100
#
```

- Router B：

```
#
acl number 3000
 rule 0 permit ip source 30.0.0.0 0.255.255.255 destination 40.0.0.0 0.255.255.255
#
ike peer vrrp
 pre-shared-key cipher kswMMJ0oAIg=
 remote-address 20.1.1.3
#
ipsec proposal vrrp
 encapsulation-mode tunnel
 transform esp
 esp encryption-algorithm des
 esp authentication-algorithm md5
#
ipsec policy vrrp 1 isakmp
 security acl 3000
 ike-peer vrrp
 proposal vrrp
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 20.1.1.1 255.0.0.0
 vrrp vrid 100 virtual-ip 20.1.1.100
 vrrp vrid 100 priority 150
 ipsec policy vrrp
#
ip route-static 40.0.0.0 255.0.0.0 20.1.1.3
```

```
#
```

- Router C：

```
#
acl number 3000
 rule 0 permit ip source 30.0.0.0 0.255.255.255 destination 40.0.0.0 0.255.255.255
#
ike peer vrrp
 pre-shared-key cipher kswMMJ0oAIg=
 remote-address 20.1.1.3
#
ipsec proposal vrrp
 encapsulation-mode tunnel
 transform esp
 esp encryption-algorithm des
 esp authentication-algorithm md5
#
ipsec policy vrrp 1 isakmp
 security acl 3000
 ike-peer vrrp
 proposal vrrp
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 20.1.1.2 255.0.0.0
 vrrp vrid 100 virtual-ip 20.1.1.100
 ipsec policy vrrp
#
ip route-static 40.0.0.0 255.0.0.0 20.1.1.3
#
```

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