MSR 系列路由器与 VRRP 虚地址建立 IPsec 功能的配置举例

目 录

1 简介

本文档介绍 MSR 系列路由器与 VRRP 虚地址建立 IPsec 功能的典型配置举例。

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。

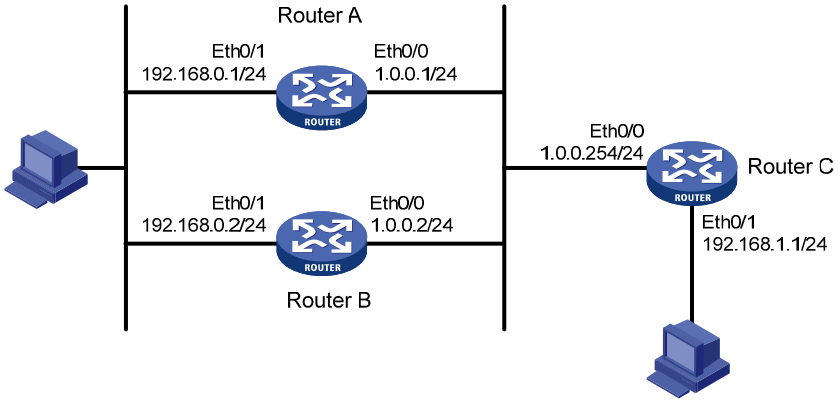
本文档假设您已了解 IPsec 和 VRRP 特性。

3 配置举例

3.1 组网需求

如 图 1 所示，Router A和Router B同属于一个VRRP备份组，Router A作为Master，Router B作为Backup，要求：Router C和VRRP备份组之间建立基于IKE的IPsec隧道。

图1 MSR 系列路由器与 VRRP 虚地址建立 IPSec 功能的配置组网图



3.2 配置思路

- 为了让 Router A 成为 Master，需要为 Router B 配置较低的优先级（默认优先级为 100）；
- 为了与备份组建立 IPsec 隧道，Router C 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 配置步骤

3.4.1 Router A的配置

配置接口 Ethernet0/1 的 IP 地址。

```
<RouterA> system-view
[RouterA] interface ethernet 0/1
[RouterA-Ethernet0/1] ip address 192.168.0.1 255.255.255.0
[RouterA-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] ip address 1.0.0.1 255.255.255.0
[RouterA-Ethernet0/0] quit
```

配置到 192.168.1.0 的静态路由。

```
[RouterA] ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterA] acl number 3000
[RouterA-acl-adv-3000] rule 0 permit ip source 192.168.0.0 0.0.0.255 destination
 192.168.1.0 0.0.0.255
[RouterA-acl-adv-3000] quit
```

创建一个 DPD 并采用默认配置。

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

配置 IKE 对等体。

```
[RouterA] ike peer branch
[RouterA-ike-peer-branch] pre-shared-key 123
[RouterA-ike-peer-branch] remote-address 1.0.0.254
```

引用指定的 DPD。

```
[RouterA-ike-peer-branch] dpd vrrp
[RouterA-ike-peer-branch] 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
```

配置 IPsec 安全策略 branch，其协商方式为 isakmp。

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

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 1.0.0.128。

```
[RouterA] interface ethernet 0/0
[RouterA-Ethernet0/0] vrrp vrid 1 virtual-ip 1.0.0.128
```

#在接口 Ethernet0/0 上应用安全策略。

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

3.4.2 Router B的配置

配置接口 Ethernet0/1 的 IP 地址。

```
<RouterB> system-view
[RouterB] interface ethernet 0/1
[RouterB-Ethernet0/1] ip address 192.168.0.2 255.255.255.0
[RouterB-Ethernet0/1] quit
```

配置接口 Ethernet0/0 的 IP 地址。

```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] ip address 1.0.0.2 255.255.255.0
[RouterB-Ethernet0/0] quit
```

配置到 192.168.1.0 的静态路由。

```
[RouterB] ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
```

创建 ACL3000,定义需要 IPsec 保护的数据流。

```
[RouterB] acl number 3000
[RouterB-acl-adv-3000] rule 0 permit ip source 192.168.0.0 0.0.0.255 destination
 192.168.1.0 0.0.0.255
[RouterB-acl-adv-3000] quit
```

创建一个 DPD 并采用默认配置。

```
[RouterB] ike dpd vrrp
[RouterB-ike-dpd-vrrp] quit
```

配置 IKE 对等体。

```
[RouterB] ike peer branch
[RouterB-ike-peer-branch] pre-shared-key 123
[RouterB-ike-peer-branch] remote-address 1.0.0.254
```

引用指定的 DPD。

```
[RouterB-ike-peer-branch] dpd vrrp
[RouterB-ike-peer-branch] 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
```

配置 IPsec 安全策略 branch，其协商方式为 isakmp。

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

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 1.0.0.128。

```
[RouterB] interface ethernet 0/0
[RouterB-Ethernet0/0] vrrp vrid 1 virtual-ip 1.0.0.128
```
配置 Router B 在备份组 1 中的优先级为 80，以保证 Router A 成为 Master 负责转发流量。
```
[RouterB-Ethernet0/0] vrrp vrid 1 priority 80
```
在接口 Ethernet0/0 上应用安全策略。
```
[RouterB-Ethernet0/0] ipsec policy branch
[RouterB-Ethernet0/0] quit
```

3.4.3 Router C的配置

配置接口 Ethernet0/0 的 IP 地址。
```
<RouterC> system-view
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ip address 1.0.0.254 255.255.255.0
[RouterC-Ethernet0/0] quit
```
配置接口 Ethernet0/1 的 IP 地址。
```
[RouterC] interface ethernet 0/1
[RouterC-Ethernet0/1] ip address 192.168.1.1 255.255.255.0
[RouterC-Ethernet0/1] quit
```
配置到 192.168.0.0 的静态路由。
```
[RouterC] ip route-static 192.168.0.0 255.255.255.0 1.0.0.128
```
创建 ACL3000,定义需要 IPsec 保护的数据流。
```
[RouterC] acl number 3000
[RouterC-acl-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
 192.168.0.0 0.0.0.255
[RouterC-acl-adv-3000] quit
```
创建一个 DPD 并采用默认配置。
```
[RouterC] ike dpd vrrp
[RouterC-ike-dpd-vrrp] quit
```
配置 IKE 对等体。
```
[RouterC] ike peer center
[RouterC-ike-peer-center] pre-shared-key 123
[RouterC-ike-peer-center] remote-address 1.0.0.128
```
引用指定的 DPD。
```
[RouterC-ike-peer-center] dpd vrrp
[RouterC-ike-peer-center] quit
```
采用安全提议的缺省配置。
```
 [RouterC] ipsec proposal def
```
配置 ESP 协议采用 md5 认证算法。
```
[RouterC-ipsec-transform-set-def] esp authentication-algorithm md5
[RouterC-ipsec-transform-set-def] quit
```
配置 IPsec 安全策略 center，其协商方式为 isakmp。
```
[RouterC] ipsec policy center 1 isakmp
[RouterC-ipsec-policy-isakmp-center-1] security acl 3000
```

```
[RouterC-ipsec-policy-isakmp-center-1] proposal def
[RouterC-ipsec-policy-isakmp-center-1] ike-peer center
[RouterC-ipsec-policy-isakmp-center-1] quit
```

在接口 Ethernet0/0 上应用安全策略。

```
[RouterC] interface ethernet 0/0
[RouterC-Ethernet0/0] ipsec policy center
[RouterC-Ethernet0/0] quit
```

3.5 验证配置

完成以上配置后，正常情况下，Router C 与 Router A 建立 IPsec 隧道实现加密通信，当 Router A 断开后，Router C 切换到与 Router B 的隧道继续进行加密通信，从而避免了通信的中断。

可以通过以下显示信息，看到正常情况下 Router C 与备份组的通信经过 Router A。

```
<RouterC> ping -a 192.168.1.1 192.168.0.1
  PING 192.168.0.1: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 192.168.0.1: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 192.168.0.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.0.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.0.1: bytes=56 Sequence=4 ttl=255 time=2 ms

  --- 192.168.0.1 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
round-trip min/avg/max = 2/2/2 ms
```

可以通过以下显示查看 Router A 上生成的主用 IPsec SA。

```
<RouterA> display ipsec sa
===============================
Interface: Ethernet0/0
    path MTU: 1500
===============================

  ----------------------------
  IPsec policy name: "branch"
  sequence number: 1
  acl version: ACL4
  mode: isakmp
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.0.0.128
        remote address: 1.0.0.254
    flow:
        sour addr: 192.168.0.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
```

```
    [inbound ESP SAs]
      spi: 0xF697493(258569363)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 3
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3430
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N

    [outbound ESP SAs]
      spi: 0xD70F31D5(3608097237)
      transform: ESP-ENCRYPT-NULL ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 4
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843199/3430
      anti-replay detection: Enabled
        anti-replay window size(counter based): 32
      udp encapsulation used for nat traversal: N
```

可以通过如下显示信息查看 Router A 上生成的主用 IKE SA 的摘要信息。

```
<RouterA> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi
  --------------------------------------------------------------------
     6             1.0.0.254               RD          1       IPSEC
     7             1.0.0.254               RD          2       IPSEC

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

显示 Router A 上备份组 1 的详细信息。

```
<RouterA> display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Ethernet0/0
     VRID           : 1               Adver Timer : 1
     Admin Status   : Up              State       : Master
     Config Pri     : 100             Running Pri : 100
     Preempt Mode   : Yes             Delay Time  : 0
     Auth Type      : None
     Virtual IP     : 1.0.0.128
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 1.0.0.1
```

显示 Router B 上备份组 1 的详细信息。

```
<RouterB>display vrrp verbose
```

```
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Ethernet0/0
     VRID           : 1               Adver Timer : 1
     Admin Status   : Up              State       : Backup
     Config Pri     : 80              Running Pri : 80
     Preempt Mode   : Yes             Delay Time  : 0
     Become Master  : 3650ms left
     Auth Type      : None
     Virtual IP     : 1.0.0.128
     Master IP      : 1.0.0.1
```

可以通过以下显示信息，当 Router A 出现故障后，Router C 与备份组的报文传输经过 Router B,IPsec 隧道不变。

```
<RouterC> ping -a 192.168.1.1 192.168.0.2
  PING 192.168.0.2: 56  data bytes, press CTRL_C to break
    Request time out
    Reply from 192.168.0.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 192.168.0.2: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.0.2: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.0.2: bytes=56 Sequence=4 ttl=255 time=2 ms

  --- 192.168.0.2 ping statistics ---
    5 packet(s) transmitted
    4 packet(s) received
    20.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
```

通过 Router B 上的 debug 信息可以看到切换信息。

```
<RouterB>
%Jun 25 13:24:07:226 2013 RouterB VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4
virtual router 1 (configured on Ethernet0/3) changed from Backup to Master: Time
r expired.
```

显示 Router B 上备份组 1 的详细信息，可以看到 Router B 已从备用变为主用。

```
<RouterB>display vrrp verbose
 IPv4 Standby Information:
     Run Mode       : Standard
     Run Method     : Virtual MAC
 Total number of virtual routers : 1
   Interface Ethernet0/0
     VRID           : 1               Adver Timer : 1
     Admin Status   : Up              State       : Master
     Config Pri     : 80              Running Pri : 80
     Preempt Mode   : Yes             Delay Time  : 0
     Auth Type      : None
     Virtual IP     : 1.0.0.128
     Virtual MAC    : 0000-5e00-0101
```

```
    Master IP      : 1.0.0.2
```

3.6 配置文件

- Router A：

```
acl number 3000
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ike dpd vrrp
#
ike peer branch
 pre-shared-key cipher $c$3$IvTMTzU5wB6rzFXH1F8jo56jbcd43g==
 remote-address 1.0.0.254
 dpd vrrp
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy branch 1 isakmp
 security acl 3000
 ike-peer branch
 transform-set def
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.0.1 255.255.255.0
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.0.0.128
 ipsec policy branch
#
 ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
#
```

- Router B：

```
acl number 3000
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ike dpd vrrp
#
ike peer branch
 pre-shared-key cipher $c$3$x8Ebm7JcEpRhPMShxDkeQvAeR124xA==
 remote-address 1.0.0.254
 dpd vrrp
#
```

```
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy branch 1 isakmp
 security acl 3000
 ike-peer branch
 transform-set def
#
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.0.0.128
 vrrp vrid 1 priority 80
 ipsec policy branch
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.0.2 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 1.0.0.254
#
```

- Router C：

```
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
#
ike dpd vrrp
#
ike peer center
 pre-shared-key cipher $c$3$/ZioTZcnjBYt3MNHRDeXdWfn1vstOQ==
 remote-address 1.0.0.128
 dpd vrrp
#
ipsec transform-set def
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
#
ipsec policy center 1 isakmp
 security acl 3000
 ike-peer center
 transform-set def
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
```

```
interface Ethernet0/0
 port link-mode route
 ip address 1.0.0.254 255.255.255.0
 ipsec policy center
#
ip route-static 192.168.0.0 255.255.255.0 1.0.0.128
#
```

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