MSR-G2系列路由器 VRRP虚地址建立IPSCE的配置

高贵贤 2013-07-22 发表

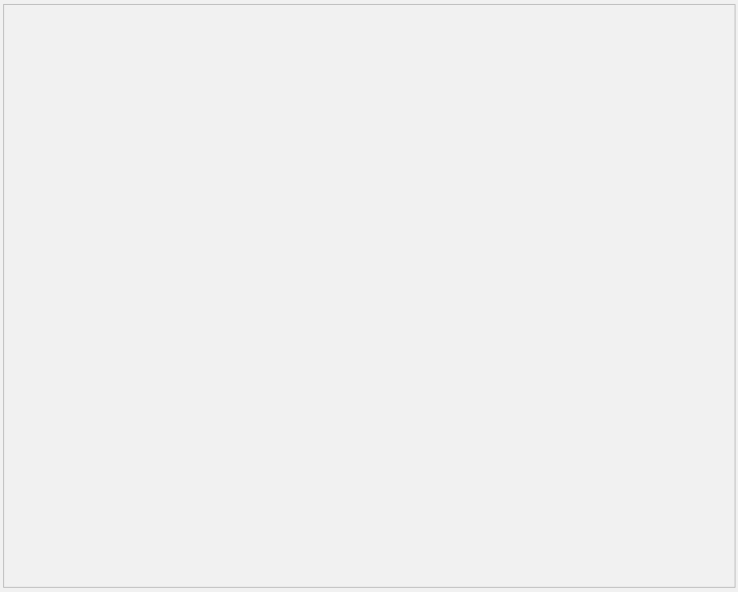
MSR G2系列路由器 VRRP虚地址建立IPSCE的配置

一、组网需求

Router1、Router2、Router3都连接在一台交换机上，Router2和Router3组VRRP，虚地址为10.1.1.254，Router3作为VRRP master,Router2作为backup;Router1和VRRP虚地址之间建立基于IKE的IPSEC，实际应用中，Router2和Router3的内网口也建议使用VRRP，对内提供统一网关

设备清单：MSR G2路由器3台

二、组网图



图一 MSR-G2路由器 VRRP虚地址建立IPSEC典型配置组网图

三、配置步骤

使用版本：E0006P05

Router1配置：

```
//配置环回接口，模拟内网用户
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
//接口GigabitEthernet2/0/0调用IPSEC策略123
interface GigabitEthernet2/0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
 ipsec apply policy 123
#
//配置静态路由，下一跳指向VRRP虚地址
 ip route-static 2.2.2.2 32 10.1.1.254
#
//配置安全ACL，保护内网地址
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
//配置IPSEC提议，使用的加密算法为3des-cbc,认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用安全ACL，指定对端地址为VRRP虚地址
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
```

```
remote-address 10.1.1.254
#
//配置ike钥匙链，使用密码为123
ike keychain 1
 pre-shared-key address 10.1.1.254 255.255.255.255 key cipher $c$3$bcRFrReUFq
eqvvA6k2S42Zta86dnzA==
```

Router2配置：

```
//接口GigabitEthernet0/0调用IPSEC策略并在接口配置VRRP组，虚地址为10.1.1.254
#
interface GigabitEthernet0/0
 port link-mode route
ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.254
 ipsec apply policy 123
#
//配置静态路由，下一跳地址为10.1.1.1
ip route-static 1.1.1.1 32 10.1.1.1
#
//配置安全ACL，保护两侧内网地址
acl number 3000
 rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc，认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用安全ACL，IPSEC提议，指定对端地址为10.1.1.1，本端地址
为VRRP虚地址10.1.1.254
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
local-address 10.1.1.254
 remote-address 10.1.1.1
#
//配置ike钥匙链，指定PSK为123
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher
$c$3$Ncp7fPbgq2AhRBH60bDTJXgJbv8DOQ==
#
```

Router3配置：

```
//在接口GigabitEthernet0/0调用IPSEC策略并在接口配置VRRP组，虚地址为10.1.1.2
54
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.1.1.3 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.254
 ipsec apply policy 123
#
//配置静态路由，下一跳指向10.1.1.1
ip route-static 1.1.1.1 32 10.1.1.1
#
//配置安全ACL，保护两侧内网地址
acl number 3000
 rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc，认证算法是MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用安全ACL，IPSEC提议，并制定对端地址为10.1.1.1,本端地址
为VRRP虚地址10.1.1.254
ipsec policy 123 1 isakmp
```

```
 transform-set 123
 security acl 3000
local-address 10.1.1.254
 remote-address 10.1.1.1
#
//配置ike钥匙链，PSK密码为123
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher $c$3$FWEY1gp45QC
NjK8wOBmCrOY5Slv9ng==
#
```

四、验证配置

```
<Router1>ping -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press escape sequence to break
Request time out                    //第一个包丢掉
56 bytes from 2.2.2.2: icmp_seq=1 ttl=254 time=0.758 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=254 time=0.534 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=254 time=0.535 ms
56 bytes from 2.2.2.2: icmp_seq=4 ttl=254 time=0.523 ms

<Router1>display ike  sa
   Connection-ID   Remote               Flag         DOI
-------------------------------------------------------------------------
   18              10.1.1.254           RD           IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router1>display ipsec sa
-------------------------------
Interface: GigabitEthernet2/0/0
-------------------------------

  ----------------------------
  IPsec policy: 123
  Sequence number: 1
  Mode: isakmp
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 10.1.1.1          //本端地址
        remote address: 10.1.1.254        //对端地址
    Flow:
    sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1894449663 (0x70eb01ff)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3575
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for nat traversal: N
      Status: active

    [Outbound ESP SAs]
      SPI: 556617108 (0x212d4d94)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3575
      Max sent sequence-number: 4
      UDP encapsulation used for nat traversal: N
```

```
    Status: active


<Router3>display ike sa
  Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------
  12              10.1.1.1            RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router3>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

 ----------------------------
 IPsec policy: 123
 Sequence number: 1
 Mode: isakmp
 ----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 10.1.1.254     //本端地址
      remote address: 10.1.1.1       //对端地址
  Flow:
  sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip
  dest addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 556617108 (0x212d4d94)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3512
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: N
    Status: active

  [Outbound ESP SAs]
    SPI: 1894449663 (0x70eb01ff)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3512
    Max sent sequence-number: 4
    UDP encapsulation used for nat traversal: N
    Status: active

Router2不会建立表象，因为此时Router3是master，Router2作为backup不会参与数据转发
[Router2]display ike sa
  Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------

[Router2]display  vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
  Interface GigabitEthernet0/0
    VRID           : 1                 Adver Timer  : 100
    Admin Status   : Up                State        : Backup
    Config Pri     : 100               Running Pri  : 100
```

```
    Preempt Mode   : Yes                Delay Time   : 0
    Become Master  : 2640ms left
    Auth Type      : None
    Virtual IP     : 10.1.1.254
    Master IP      : 10.1.1.3

<Router3>display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
  Interface GigabitEthernet0/0
    VRID           : 1                  Adver Timer  : 100
    Admin Status   : Up                 State        : Master
    Config Pri     : 100                Running Pri  : 100
    Preempt Mode   : Yes                Delay Time   : 0
    Auth Type      : None
    Virtual IP     : 10.1.1.254
    Virtual MAC    : 0000-5e00-0101
    Master IP      : 10.1.1.3
<Router1>ping -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press escape sequence to break
Request time out                    //第一个包丢掉
56 bytes from 2.2.2.2: icmp_seq=1 ttl=254 time=0.758 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=254 time=0.534 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=254 time=0.535 ms
56 bytes from 2.2.2.2: icmp_seq=4 ttl=254 time=0.523 ms

<Router1>display ike  sa
  Connection-ID   Remote               Flag        DOI
-----------------------------------------------------------------------------
   18             10.1.1.254           RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router1>display ipsec sa
-------------------------------
Interface: GigabitEthernet2/0/0
-------------------------------

 -----------------------------
 IPsec policy: 123
 Sequence number: 1
 Mode: isakmp
 -----------------------------
   Tunnel id: 0
   Encapsulation mode: tunnel
   Perfect forward secrecy:
   Path MTU: 1443
   Tunnel:
       local  address: 10.1.1.1          //本端地址
       remote address: 10.1.1.254        //对端地址
   Flow:
   sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
   dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

   [Inbound ESP SAs]
     SPI: 1894449663 (0x70eb01ff)
     Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843199/3575
     Max received sequence-number: 4
     Anti-replay check enable: Y
     Anti-replay window size: 64
     UDP encapsulation used for nat traversal: N
     Status: active
```

```
  [Outbound ESP SAs]
    SPI: 556617108 (0x212d4d94)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3575
    Max sent sequence-number: 4
    UDP encapsulation used for nat traversal: N
    Status: active


<Router3>display ike sa
  Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------------
  12              10.1.1.1            RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router3>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

 -----------------------------
 IPsec policy: 123
 Sequence number: 1
 Mode: isakmp
 -----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 10.1.1.254     //本端地址
      remote address: 10.1.1.1       //对端地址
  Flow:
  sour addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip
  dest addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 556617108 (0x212d4d94)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3512
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: N
    Status: active

  [Outbound ESP SAs]
    SPI: 1894449663 (0x70eb01ff)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3512
    Max sent sequence-number: 4
    UDP encapsulation used for nat traversal: N
    Status: active

Router2不会建立表象，因为此时Router3是master，Router2作为backup不会参与数据转发
[Router2]display ike sa
  Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------------
```

```
[Router2]display  vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet0/0
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Backup
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Become Master  : 2640ms left
     Auth Type      : None
     Virtual IP     : 10.1.1.254
     Master IP      : 10.1.1.3

<Router3>display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 2
   Interface GigabitEthernet0/0
     VRID           : 1                 Adver Timer  : 100
     Admin Status   : Up                State        : Master
     Config Pri     : 100               Running Pri  : 100
     Preempt Mode   : Yes               Delay Time   : 0
     Auth Type      : None
     Virtual IP     : 10.1.1.254
     Virtual MAC    : 0000-5e00-0101
     Master IP      : 10.1.1.3
```

五、配置关键点

1. Router2和Router3的VRRP详细配置，可以参见VRRP典型配置；
2. Router2和Router3的IPSEC配置一致，指定的本段地址都为VRRP虚拟地址；
3. Router1上指定的地址为VRRP虚地址；
4. V7设备预共享密钥在Ike keychain中配置，V5设备在Ike peer中配置；
5. ipsec安全策略下（ipsec transform-set）默认是没有加密和认证方法的，这点需要注意。