MSR-G2系列路由器 IPSEC 主模式的典型配置

高贵贤 2013-07-22 发表

MSR-G2系列路由器 IPSEC 主模式的典型配置

一、 组网需求：
在Router1和Router3之间建立一个IPsec隧道，对Router1所在的子网（1.1.1.1/32）与Router3所在的子网（3.3.3.3/32）之间的数据流进行安全保护
1. Router1和Router3之间采用IKE协商方式建立IPsec SA
2. 使用缺省的IKE提议
3. 使用缺省的预共享密钥认证方法
设备清单：MSR G2路由器3台
二、 组网图：

图1 MSR-G2路由器 IPSEC主模式典型配置组网图

三、 配置步骤
设备版本：E0006P05
Router1配置：

```
//配置环回接口Loopback0模拟内网用户
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
//接口GigabitEthernet0/0调用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 12.1.1.1 255.255.255.0
 ipsec apply policy 123
#
//配置默认路由，下一跳指向对端地址12.1.1.2
ip route-static 0.0.0.0 0 12.1.1.2
#
//配置安全ACL，保护数据流为Router1和Router3的内网地址
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 3.3.3.3 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IPSEC提议、安全ACL、指定隧道对端地址为23.1.1.2
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 local-address 12.1.1.1
 remote-address 23.1.1.2
#
//配置IKE钥匙链，对端地址为23.1.1.2，密钥为123
ike keychain 1
 pre-shared-key address 23.1.1.2 255.255.255.255 key cipher
$c$3$fKzT3ddqs0YYoUQIGYOT9yUX4RIKkw==
```

Router3配置：

```
//配置环回口，模拟内网用户
#
```

```
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
//配置接口GigabitEthernet0/1，调用IPSEC策略
interface GigabitEthernet0/1
 port link-mode route
 ip address 23.1.1.2 255.255.255.0
 ipsec apply policy 123
#
//配置默认路由，下一跳指向对端地址23.1.1.1
ip route-static 0.0.0.0 0 23.1.1.1
#
//安全ACL，保护数据流为Router3和Router1的内网用户地址，和对端配置互为镜像
acl number 3000
 rule 0 permit ip source 3.3.3.3 0 destination 1.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc，认证方式为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用IPSEC提议、安全ACL、指定对端地址为12.1.1.1
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 local-address 23.1.1.2
 remote-address 12.1.1.1
#
//配置IKE钥匙链，指定对端地址为12.1.1.1，密钥为123
ike keychain 1
 pre-shared-key address 12.1.1.1 255.255.255.255 key cipher
$c$3$XCU5kp2dS69DM/qa7fi4S9WxUfNeWA==
测试过程：
[Router1]ping -a 1.1.1.1 3.3.3.3
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press escape sequence to brea
k
Request time out          //会先丢一个包
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.434 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.182 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=0.180 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.171 ms
[Router1]display ike  sa
   Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------------
   3             23.1.1.2            RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
[Router1]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: 12.1.1.1       //封装后源地址为12.1.1.1
        remote address: 23.1.1.2       //封装后目的地址为23.1.1.2
```

```
    Flow:
    sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1383692956 (0x52797a9c)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3571
      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: 2694185529 (0xa0960239)
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3571
      Max sent sequence-number: 4
      UDP encapsulation used for nat traversal: N
      Status: active
[Router1]display  ike  sa verbose
  -----------------------------------------------
  Connection ID: 3
  Outside VPN:
  Inside VPN:
  Profile:
  Transmitting entity: Initiator
  -----------------------------------------------
  Local IP: 12.1.1.1
  Local ID type: IPV4_ADDR
  Local ID: 12.1.1.1

  Remote IP: 23.1.1.2
  Remote ID type: IPV4_ADDR
  Remote ID: 23.1.1.2

  Authentication-method: PRE-SHARED-KEY
  Authentication-algorithm: SHA1
  Encryption-algorithm: DES-CBC

  Life duration(sec): 86400
  Remaining key duration(sec): 86315
  Exchange-mode: Main       //主模式
  Diffie-Hellman group: Group 1
  NAT traversal: Not detected   //没有NAT设备，故未检测
四、 配置关键点：
1. 保证Router1和Router3之间路由可达；
2. Router1和Router3两侧的安全ACL配置，最好是互为镜像；
3. V7设备预共享密钥的配置在ike keychain中，V5设备在ike  peer中配置；
4. 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。
```