✡✡✡MSR-G2 系列路由器 IPSEC 穿越NAT的典型配置

NAT 高贵贤 2013-07-22 发表

MSR-G2 系列路由器 IPSEC 穿越NAT的典型配置

一、 组网需求：

Router1在NAT安全网关内网侧。要求在Router1和Router3之间建立一个IPsec隧道，对Router1所在的子网（1.1.1.1/32）和Router3所在的子网（3.3.3.3/32）之间的数据流进行安全保护。具体需要求如下：

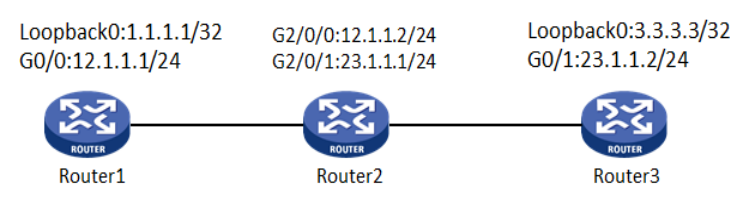
1．协商双方使用缺省的IKE提议

2．协商模式为野蛮模式协商

3．第一阶段协商的认证方法为预共享密钥认证

设备清单：MSR G2路由器3台

二、 组网图：



图一 MSR-G2路由器 IPSEC穿越NAT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
#
//配置静态路由，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，保护两侧内网网段
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 3.3.3.3 0
#
//配置IPSEC提议，加密算法使用3des-cbc，认证使用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、ike安全框架并指定对端地址为23.1.1.2
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 23.1.1.2
 ike-profile 123
#
//标识设备的方式为user-fqdn
 ike identity user-fqdn
#
//配置ike profile,使用野蛮模式，本端标识为Router1
ike profile 123
```

```
 keychain 1
 exchange-mode aggressive
 local-identity user-fqdn Router1
 match remote identity address 23.1.1.2 255.255.255.0
#
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$3$fKzT3ddqs0YYoUQlGYOT9yUX4RlKkw==
Router2配置：
[Router2-GigabitEthernet2/0/1]display this
#
//接口GigabitEthernet2/0/1配置NAT
interface GigabitEthernet2/0/1
 port link-mode route
 combo enable copper
 ip address 23.1.1.1 255.255.255.0
 nat outbound
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
#
//在接口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
#
//配置静态路由，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
#
//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 3.3.3.3 0 destination 1.1.1.1 0
#
//配置IPSEC提议，加密算法使用3des-cbc，认证算法使用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、ike安全框架并指定对端地址为23.1.
1.1
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 local-address 23.1.1.2
 remote-address 23.1.1.1
 ike-profile 123
#
//配置ike profile，调用IKE钥匙链、使用野蛮模式、隧道对端名称为Router1
ike profile 123
 keychain 1
 exchange-mode aggressive
 match remote identity user-fqdn Router1
#
//配置IKE 钥匙链，密钥为123
ike keychain 1
 pre-shared-key address 23.1.1.1 255.255.255.255 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      //第一个包丢掉
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.365 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.190 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=0.182 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.168 ms

[Router1]display ike  sa verbose
  -----------------------------------------------
  Connection ID: 12
  Outside VPN:
  Inside VPN:
  Profile: 123
  Transmitting entity: Initiator
  -----------------------------------------------
  Local IP: 12.1.1.1
  Local ID type: USER_FQDN
  Local ID: Router1

  Remote IP: 23.1.1.2
  Remote ID type: USER_FQDN
  Remote ID: Router3

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

  Life duration(sec): 86400
  Remaining key duration(sec): 86380
  Exchange-mode: Aggressive           //野蛮模式
  Diffie-Hellman group: Group 1
  NAT traversal: Detected             //检测到了NAT设备的存在

[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: 1435
  Tunnel:
      local  address: 12.1.1.1
      remote address: 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: 2772268438 (0xa53d7596)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3562
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: Y
    Status: active
```

[Outbound ESP SAs]
SPI: 402158417 (0x17f87351)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3562
Max sent sequence-number: 4
UDP encapsulation used for nat traversal: Y
Status: active

四、 配置关键点：

1. IPSEC NAT穿越的配置，需要指定IKE第一阶段使用野蛮模式；
2. V7设备配置IKE框架（profile），调用Ike keychain、启用野蛮模式、匹配对端设备User-fqdn，在V5设备中直接在ike peer中完成；
3. V7设备配置Ike keychain，配置预共享密钥；V5设备直接在Ike Peer中完成。
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。