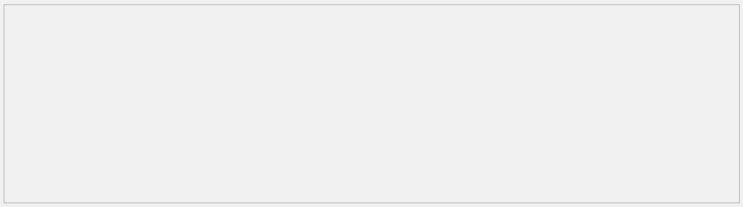
MSR-G2系列路由器 IPSEC 野蛮方式的典型配置

高贵贤 2013-07-22 发表

MSR-G2系列路由器 IPSEC 野蛮方式的典型配置

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.Router1和Router3均使用PSK认证方法；
3.IKE第一阶段的协商模式为野蛮模式。
设备清单：MSR G2路由器3台
二、 组网图：



图一 MSR-G2路由器 IPSEC野蛮模式典型配置组网图

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
#
//Router1的GigabitEthernet0/0接口调用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，加密方式为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，调用了IKE profile、IPSEC提议、安全ACL以及指定对端地址
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 local-address 12.1.1.1
 remote-address 23.1.1.2
 ike-profile 123
#
//标识本端身份的方式为user-fqdn
ike identity user-fqdn
#
//配置IKE profile，定义使用野蛮模式，本端名字为Router1，对端名字为Router3
ike profile 123
 keychain 1
```

```
 exchange-mode aggressive
 local-identity user-fqdn Router1
 match remote identity user-fqdn Router3
#
//配置IKE 的钥匙链，对端地址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==
Router3配置：
//配置环回口模拟内用用户
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
//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的内用地址，和Router1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，加密算法使用3des-cbc，认证方式使用MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用Ike profile、IPSEC提议、安全ACL，并指定对端地址为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
 ike-profile 123
#
//标识本端身份的方式为user-fqdn
 ike identity user-fqdn
#
//配置Ike profile，指定使用野蛮模式，调用钥匙链1
ike profile 123
 keychain 1
 exchange-mode aggressive
 local-identity user-fqdn Router3
 match remote identity user-fqdn Router1
#
//配置钥匙链1，密码配置为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            //第一个包丢掉
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.436 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.184 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=0.185 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.162 ms
```

```
<Router1>display ike sa verbose
  ----------------------------------------------------
  Connection ID: 11
  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): 86379
  Exchange-mode: Aggressive        //野蛮模式
  Diffie-Hellman group: Group 1
  NAT traversal: Not detected      //网络中不存在NAT设备
```

四、 配置关键点：

1. 保证Router1和Router3路由可达；
2. Router1和Router3的安全ACL，最好互为镜像；
3. IKE模式默认为主模式，在Ike profile配置为野蛮模式，V5设备中实在ike peer中进行配置；
4. 预共享密钥在Ike keychain中进行配置，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。