MSR-G2系列路由器 IPSEC OVER GRE功能的典型配置

高贵贤 2013-07-22 发表

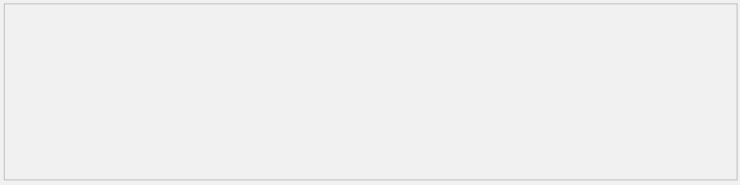
MSR-G2系列路由器 IPSEC OVER GRE功能的典型配置

一、组网需求

Router1和Router2之间建立GRE隧道，Router1和Router2下挂网段间流量走GRE，在GRE中对流量进行加密

设备清单：MSR G2路由器2台

二、组网图



图一 MSR-G2路由器 IPSEC over GRE典型配置组网图

三、配置步骤

使用版本：E0006P05

Router1配置：

```
//配置环回口模拟内网用户
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
//配置物理接口地址
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.1.1.1 255.255.255.0
//配置tunnel0口，模式选择gre，并在此接口下调用IPSEC策略
#
interface Tunnel0 mode gre
 ip address 20.1.1.1 255.255.255.0
 source 10.1.1.1
 destination 10.1.1.2
 ipsec apply policy 123
#
//配置静态路由，下一跳指向tunnel0口
 ip route-static 2.2.2.2 32 Tunnel0
//配置安全ACL，保护两侧内网用户
#
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 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，调用安全ACL、IPSEC提议、指定对端地址为对端tunnel口地址
#
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 20.1.1.2
#
//配置Ike钥匙链，地址为对端tunnel口地址，PSK为123
ike keychain 1
 pre-shared-key address 20.1.1.2 255.255.255.255 key cipher $c$3$dltAoRlNnJ5Dkff
kQH0itp5yUcHL0g==
#
```

Return

Router2配置：

```
//配置环回口模拟内网用户
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
//配置物理接口地址
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.1.1.2 255.255.255.0
//配置tunnel0口，模式为gre，在此接口调用IPSEC策略
#
interface Tunnel0 mode gre
 ip address 20.1.1.2 255.255.255.0
 source 10.1.1.2
 destination 10.1.1.1
 ipsec apply policy 123
#
//配置安全ACL，报文内网用户数据
acl number 3000
 rule 0 permit ip source 2.2.2.2 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，调用安全ACL，IPSEC提议，指定对端地址为对端tunnel口地址
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 20.1.1.1
#
//配置Ike要是链，地址为对端tunnel口地址，PSK为123
ike keychain 1
 pre-shared-key address 20.1.1.1 255.255.255.255 key cipher
$c$3$TVH6oqoopQnGt53BjIUFIA5IeOecHw==
#
Return
```

四、测试过程：

```
<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=255 time=0.474 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=255 time=0.260 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=255 time=0.239 ms
56 bytes from 2.2.2.2: icmp_seq=4 ttl=255 time=0.239 ms
```

五、配置关键点：

1. 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；
2. 远端地址是对方的GRE隧道口的IP地址，不是物理接口的IP地址；
3. IPSEC策略绑定在GRE隧道上；
4. 定义静态路由或策略路由将需要加密的流量引入到GRE隧道上；
5. V7设备配置tunnel虚接口，需要预先指定模式，不同于V5设备；
6. V7设备预共享密钥的配置需要在ike keychain中配置，不同于V5设备。