MSR V7系列路由器和MSR V5系列路由器主模式对接IPSec over GRE典型配置

IPsec ipoe 朱玉广 2015-01-04 发表

一、 组网需求：

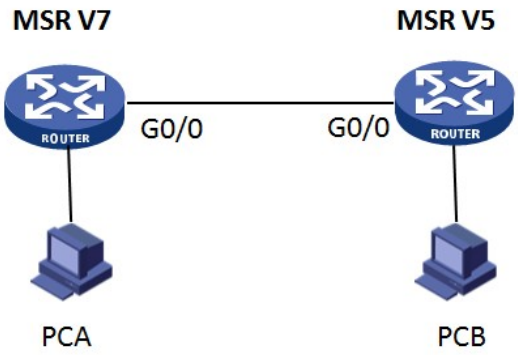
要求MSR3020和MSR3620之间路由可达，PCA使用MSR3620上的loopback 0口代替，PCB由MSR3020上的loopback 0口代替，并且有如下要求：

1、双方使用主模式建立IPsec隧道；

2、双方使用预共享密钥的方式建立IPsec；

3、双方采用IPSec over GRE的方式。

二、 组网图：



三、 配置步骤：

MSR3620（V7平台）配置：

#配置出接口地址：

[H3C] interface GigabitEthernet0/0

[H3C-GigabitEthernet0/0] port link-mode route

[H3C-GigabitEthernet0/0] description to V5

[H3C-GigabitEthernet0/0] combo enable copper

[H3C-GigabitEthernet0/0] ip address 10.34.136.93 255.255.255.252

#使用一个Loopback地址，用来模仿内部PCA：

[H3C] interface LoopBack0

[H3C-LoopBack0] ip address 10.34.140.27 255.255.255.255

#设备上起OSPF，区域ID设为34，并指定区域内的网段地址

[H3C]ospf 1

[H3C-ospf-1] silent-interface GigabitEthernet0/0

[H3C-ospf-1] area 0.0.0.34

[H3C-ospf-1-area-0.0.0.34] network 10.34.0.0 0.0.255.255

#创建IKE Keychain,配置预共享密钥为123456

[H3C] ike keychain 123

[H3C-ike-keychain-123]pre-shared-key address 10.34.142.94 255.255.255.252 key simple 123456

#配置IKE Profile，并配置match地址

[H3C] ike profile 123

[H3C-ike-profile-123] keychain 123

[H3C-ike-profile-123] match remote identity address 10.34.142.94

[H3C-ike-profile-123] dpd interval 10 periodic

#配置ACL感兴趣流：

[H3C] acl number 3000

[H3C-acl-adv-3000] description IPSec ACL for VPN to V5

[H3C-acl-adv-3000] rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 10.0.0.0 0.255.255.255

#配置IPSec安全提议，加密算法设置为3DES，验证算法设置为MD5：

[H3C]ipsec transform-set 123

[H3C-ipsec-transform-set-123] esp encryption-algorithm 3des-cbc

[H3C-ipsec-transform-set-123] esp authentication-algorithm md5

#配置IPSec策略，指定ACL、安全提议和IKE Profile，并指定对端公网地址。

[H3C] ipsec policy tov5 1 isakmp

[H3C-ipsec-policy-isakmp-tov5-1] transform-set 123

[H3C-ipsec-policy-isakmp-tov5-1] security acl 3000

[H3C-ipsec-policy-isakmp-tov5-1] remote-address 10.34.142.94

[H3C-ipsec-policy-isakmp-tov5-1] ike-profile 123

#设备上起Tunnel口，指定给源和目的地址分别为本端和对端的出口地址，并在接口上应用IPSec策略：

[H3C] interface Tunnel1 mode gre

[H3C-Tunnel1] description VPN Tunnel to V5

[H3C-Tunnel1] ip address 10.34.142.93 255.255.255.252

[H3C-Tunnel1] keepalive 10 3

[H3C-Tunnel1] ospf cost 100

[H3C-Tunnel1] source 10.34.136.93

[H3C-Tunnel1] destination 10.34.136.94

[H3C-Tunnel1] ipsec apply policy tov5

MSR3020配置：

#配置出接口地址：

[H3C] interface GigabitEthernet0/0

[H3C-GigabitEthernet0/0] description to V7

[H3C-GigabitEthernet0/0] ip address 10.34.136.94 255.255.255.252

#创建loopback 0口，模拟内网的终端设备PCB

[H3C] interface LoopBack0

[H3C-LoopBack0] ip address 10.34.140.129 255.255.255.255

#设备启用OSPF，区域ID指定为34，并指定该区域包含的网段地址

[H3C] ospf 1

[H3C-ospf-1] silent-interface GigabitEthernet0/0

[H3C-ospf-1] area 34

[H3C-ospf-1-area-0.0.0.34] network 10.34.0.0 0.0.255.255

#配置DPD，名字设为123

[H3C] ike dpd 123

#创建ike peer，使用默认的主模式，并开启DPD检测

[H3C] ike peer 123

[H3C-ike-peer-123] pre-shared-key simple 123456

[H3C-ike-peer-123] remote-address 10.34.142.93

[H3C-ike-peer-123] dpd 123

#创建IPSec感兴趣流，并指定源网段和目的网段

[H3C] acl number 3000

[H3C-acl-adv-3000] description IPSec ACL for VPN-V7

[H3C-acl-adv-3000] rule 0 permit ip source 10.0.0.0 0.255.255.255 destination 10.0.0.0 0.255.255.255

#创建IPSec安全提议，使用隧道模式，封装模式选择ESP方式，加密方式为3des，验证方式为md5

[H3C] ipsec transform-set 123

[H3C-ipsec-transform-set-123] encapsulation-mode tunnel

[H3C-ipsec-transform-set-123] transform esp

[H3C-ipsec-transform-set-123] esp authentication-algorithm md5

[H3C-ipsec-transform-set-123] esp encryption-algorithm 3des

#创建IPsec策略，指定ACL、IKE Peer和安全提议

[H3C] ipsec policy tov7 1 isakmp

[H3C-ipsec-policy-isakmp-tov7-1] security acl 3000

[H3C-ipsec-policy-isakmp-tov7-1] ike-peer 123

[H3C-ipsec-policy-isakmp-tov7-1] transform-set 123

#建立tunnel口，指定源和目的分别为两端设备的出口地址，并在该接口下发IPSec策略

[H3C] interface Tunnel0

[H3C-Tunnel0] description VPN Tunnel to V7

[H3C-Tunnel0] ip address 10.34.142.94 255.255.255.252

[H3C-Tunnel0] source 10.34.136.94

[H3C-Tunnel0] destination 10.34.136.93

[H3C-Tunnel0] keepalive 10 3

[H3C-Tunnel0] ospf cost 100

[H3C-Tunnel0] ipsec policy tov7

配置结果：

触发建立IPSec之后，在MSR3020上使用display ike sa，可以看到如下：

[H3C]dis ike sa

```
  total phase-1 SAs: 1
  connection-id  peer                 flag       phase   doi
 ----------------------------------------------------------------------
   9            10.34.142.93          RD|ST      1       IPSEC
   15           10.34.142.93          RD         2       IPSEC
```

四、 配置关键点：

1、设备两端的感兴趣流acl一定要互为镜像；

2、V7侧ike profile下须要配置match remote命令，否则会导致DPD探测异常；

3、V7侧非IPSec模板方式，IPSec策略下须配置remote address命令，否则会导致无法触发IPSec触发；

4、在IPSec over GRE中，IPSec应用在Tunnel口上；

5、IPSec安全提议中的认证和加密算法默认为空，需手工配置。