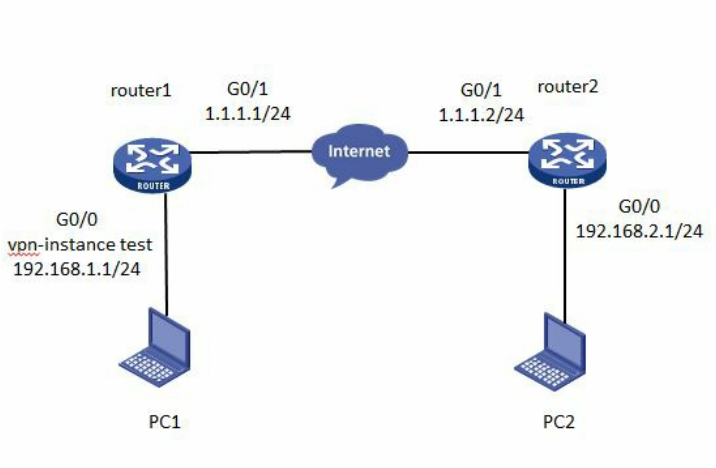
MSR5660系列路由器ipsec vpn无法建立的案例分析

IPsec 李聪 2016-09-19 发表



一、 组网：

如图所示，两台路由器router1和router2分别部署在两个不同的局点。之前两台路由器之间建立ipsec vpn进行两个局点的私网地址互通的，两台路由器都是使用的主模式建立的ipsec vpn，之前ipsec vpn的业务一直正常使用。现在由于router1这边的局点增加了几个网段，使用不同的业务需求，现在客户要求使用vpn实例隔离的方式实现。因此，本案例中将router1的接口G0/0加入了vpn实例test。但是我们发现一个问题，将内网接口G0/0加入vpn实例之后发现ipsec vpn全部断开，业务中断。

本案例涉及的路由器的型号均为MSR5660，版本为Version 7.1.059, Release 0306P52。

二、 原因分析：

接下来从客户配置、网络情况、以及debug方面进行分析。

1. 检查配置

```
#
ip vpn-instance test
 route-distinguisher 10:1
 vpn-target 10:1 import-extcommunity
 vpn-target 10:1 export-extcommunity   //vpn实例的配置
#
interface GigabitEthernet0/0
 ip binding vpn-instance test  //将接口加入vpn实例test
 ip address 192.168.1.1 255.255.255.0
#
acl advanced 3010 //配置的acl匹配的流量
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
//以下是ipsec vpn的配置
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy h3c 1 isakmp
 transform-set 1
```

security acl 3010

local-address 1.1.1.1

remote-address 1.1.1.2

ike-profile h3c

#

ike profile h3c

keychain 1

match remote identity address 1.1.1.2 255.255.255.255

#

ike proposal 1

encryption-algorithm 3des-cbc

authentication-algorithm md5

#

ike keychain 1

pre-shared-key address 1.1.1.2 255.255.255.255 key cipher c3$TXgO9EZW+xdt1XqF6O/u0/h6j83RSXHukphu

#

interface GigabitEthernet/0/1

ip address 1.1.1.1 255.255.255.0 //配置外网接口的ip地址

ipsec apply policy h3c //在接口上面调用ipsec策略

#

ip route-static 192.168.2.0 24 1.1.1.2 //配置静态路由

以上配置主要就是router1增加vpn实例之后的配置，可以看出客户主要增加的配置就是内网接口G0/0下面增加的绑定vpn实例的配置。根据现场反馈，之前没有在G0/0接口下面增加绑定VPN实例的时候是可以正常使用的，目前就只是在router1的G0/0接口下面增加绑定vpn实例的配置，router2上面的配置没动过。现在的现象就是ipsec vpn不通了。从以上的简单初步的分析可以看出应该是配置问题导致的。

2. 分析问题原因

通过以上的简单分析，我们初步怀疑是配置问题导致的，因此我们再重新检查配置发现ipsec vpn配置参数里面有关于vpn实例的解释。下面我们针对配置使用debug工具对配置进行验证。

2.1 ipsec对不同vpn实例的处理机制

我们查询手册资料之后发现ipsec对不同vpn实例的处理机制，其中本功能就是在ike profile里面进行配置的。对于内部MPLS L3VPN实例，当IPsec解封装后得到的报文需要继续转发到不同的VPN中去时，设备需要知道在哪个VPN实例中查找相应的路由。缺省情况下，设备在与外网相同的VPN中查找路由，如果不希望在与外网相同的VPN中查找路由去转发报文，则可以指定一个内部VPN实例，通过查找该内部VPN实例中的路由来转发报文。其中配置参数为：

在ike profile视图下面配置inside-vpn vpn-instance [vpn-name]。

2.2 尝试修改配置以及通过debug工具进行验证

从以上的分析我们看出如果设备需要转发到不同的vpn实例的话，ike profile里面是需要配置inside-vpn vpn-instance这个参数的。如下配置：

#

ike profile h3c

keychain 1

match remote identity address 1.1.1.2 255.255.255.255

inside-vpn vpn-instance test //增加这部分配置

#

配置上以上参数我们通过display ike sa以及display ipsec sa发现还是没有ipsec的建立。因此通过debugging ike all发现也没有ike的协商报文过程。因此怀疑没有触发ipsec的协商。

接下来，我们还可以发现没有触发协商一般就是acl的问题，现在内网接口G0/0加入了vpn实例，那么acl的配置也应该有所修改：

acl advanced 3010

rule 0 permit ip vpn-instance test source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

接下来，还需要检查路由的配置，内网的报文需要经过设备封装ipsec出外网，那么我们之前配置的静态路由也是需要修改的：

ip route-static vpn-instance test 192.168.2.0 24 1.1.1.2 public

通过以上配置之后，我们发现重新reset ike sa以及reset ipsec sa，然后触发ipsec协商发现debug能够抓取到协商的报文以及协商过程。通过display ike sa以及display ipsec sa能够看到ipsec建立成功。

三、 解决办法：

通过以上的分析，我们总结了以下几点：

1．配置acl，需要带有vpn实例，保证内网访问发出的协商报文能够触发ipsec协商。

2．配置路由，带上vpn实例，然后指向对方的地址，需要带有public的参数。

3．配置ike profile，里面需要配置inside-vpn vpn-instance test。

4．如果发现ipsec不能建立，建议两边设备的ike sa以及ipsec sa都需要清除一下，然后重新协商就可以了。因此，本案例最后还建议这种组网的情况下配置dpd检测功能。