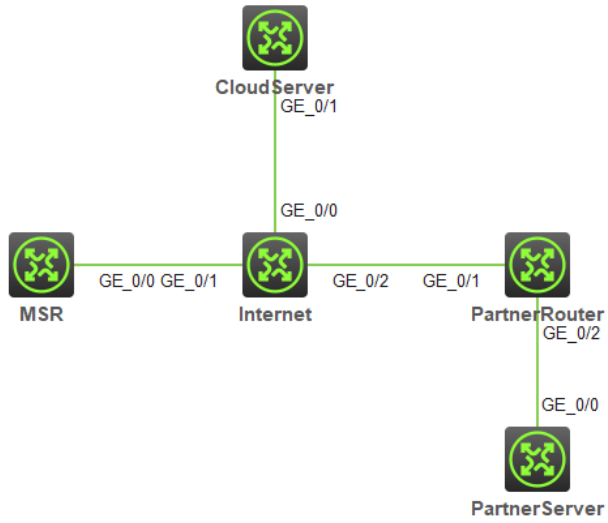
MSRG2路由器 ipsec+双向NAT 实现访问云端服务器与远端服务器互访案例

IPSec VPN NAT 林宇阳 2020-02-21 发表

组网及说明



客户需求如下：

1.CloudServer与PartnerServer之间可以双向主动触发tcp访问连接。

2.MSR与PartnerRouter之间建立IPSec vpn隧道。PartnerServer的流量经过隧道传到MSR路由器，再由MSR进行NAT转换后和与CloudServer实现交互。

3.CloudServer对PartnerServer真实地址不可知，通过访问MSR提供的地址实现与PartnerServer的通信。

4.Partner要求与其通信的地址为MSR内网地址192.168.85.137/29；

5.因业务应用需求，服务器要求仅与其指定TCP端口通信

实际组网中PartnerRouter为第三方IPSec VPN网关设备。

问题描述

客户按照双向NAT映射的思路自行配置后发现虽然IPSec sa可以成功建立，但从云端进行流量触发测试，却无法与合作方服务器实现通信。

附客户关键配置：

```
nat address-group 1 name PTMQ154snat
 address 192.168.85.137 192.168.85.137
#
nat address-group 2 name SJZHGMQ1snat
 address 220.194.201.28 220.194.201.28
#
interface GigabitEthernet0/0
 port link-mode route
 description Multiple_Line
 bandwidth 10000
 ip address 220.194.201.28 255.255.255.240
 packet-filter name GigabitEthernet0/0 inbound
 nat inbound name PTMQ154 address-group name PTMQ154snat counting
 nat inbound name SJZHGMQ1 address-group name SJZHGMQ1snat counting
 nat server protocol tcp global 192.168.85.137 1410 inside 47.95.71.154 1410 counting
 nat server protocol tcp global current-interface 1410 inside 172.16.244.11 22 counting
 ipsec apply policy test
#
 ip route-static 0.0.0.0 0 GigabitEthernet0/0 220.194.201.17
 ip route-static 192.168.85.137 32 GigabitEthernet0/0 220.194.201.17
#
acl basic name PTMQ154
 rule 0 permit source 47.95.71.154 0 logging
#
acl basic name SJZHGMQ1
 rule 0 permit source 172.16.244.11 0 logging
#
acl advanced 3002  //IPSec保护流量
 rule 0 permit ip source 192.168.85.136 0.0.0.7 destination 172.16.0.0 0.0.255.255
#
acl advanced name GigabitEthernet0/0
 rule 0 permit tcp destination-port eq 1410
#
IPSec基础配置方法非本案例重点，不额外赘述
```

过程分析

1.定位报文交互失败原因：

a)在MSR路由器上开启debug ip packet ACL XXX (匹配从源目为云端地址或者源目为合作方服务器地址的报文)观察，发现流量在经过NAT转换后已通过IPSec隧道达到合作方，但合作方的回程报文在达到MSR后出现问题：反向报文从ipsec隧道返回后直接走黑洞路由丢弃报文而再不会匹配接口的转换策略.

```
*Nov 29 18:59:42:096 2019 2600 IPSEC/7/PACKET:
Inbound ESP IPsec processing: Sent packet back to IP forwarding. Pkt len is 84.
*Nov 29 18:59:42:096 2019 2600 IPFW/7/IPFW_PACKET:
Receiving, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 15, offset = 0, ttl = 254, protocol = 1,
checksum = 1612, s = 172.16.244.11, d = 192.168.85.137
prompt: Receiving IP packet.

*Nov 29 18:59:42:096 2019 2600 IPFW/7/IPFW_PACKET:
Discarding, interface = GigabitEthernet0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 15, offset = 0, ttl = 253, protocol = 1,
checksum = 1868, s = 172.16.244.11, d = 192.168.85.137
prompt: FIB BLACKHOLE.
```

b)查看黑洞路由的生成原因——当接口配置一条nat-server时，若global地址不是接口地址即会自动生成一条路由优先级为1的直连黑洞路由：

nat server protocol tcp global 192.168.85.137 1410 inside 47.95.71.154 1410 counting

192.168.85.137/32 Direct 1 0 0.0.0.0 NULL0

在有此黑洞路由存在的情况下，任何目的地址是192.168.85.137的转发流量都会直接被黑洞丢弃。

在删去导致出错的冗余配置：为反向流量配置的一条nat in 和nat server的情况下，可以实现转换。

~~nat server protocol tcp global 192.168.85.137 1410 inside 47.95.71.154 1410 counting~~

~~nat inbound name SJZHCMQ1 address-group name SJZHCMQ1snat counting~~

附模拟器验证结果,使用Telnet代替1041端口：

```
<aliyun>
<aliyun>tel 220.194.201.28
Trying 220.194.201.28 ...
Press CTRL+K to abort
Connected to 220.194.201.28 ...

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: abc
Password:
<hezuoQMserver>
<hezuoQMserver>
<hezuoQMserver>
```

至此云端访问合作方的流量已可以实现交互。

2.随后客户进行合作方发起访问测试，发现反向触发依旧处于失败。

通过开启debug IP packet acl XXX和debug nat packet 观察，可以确认原因为：

当前配置下，NAT相关功能均在G0/0接口配置生效，而实际上流量经过IPSec隧道到达MSR后不会进行目的地址的转换而是仅进行源地址转换。报文最终以私网IP为目的地址发出MSR设备，被外部网络设备直接丢弃。

解决方法

从上述分析中可以发现，通过在接口进行两个natServer+两个nat inbound实现转换的思路是不可行的。

需要调整NAT部署的方法为静态NAT+NAT Outbound+NAT Server方式实现过IPSec隧道转发的需求：

```
 nat static inbound 60.205.228.184 192.168.85.138
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 220.194.201.28 255.255.255.0
 nat outbound 3998
 nat server protocol tcp global current-interface 23 inside 172.16.244.11 23
 nat server protocol tcp global current-interface 1410 inside 172.16.244.11 1410
 nat static enable
 ipsec apply policy test
#
 ip route-static 0.0.0.0 0 220.194.201.1
 ip route-static 192.168.85.137 32 220.194.201.1
#
interface LoopBack0 （触发IPSec用）
 ip address 192.168.85.141 255.255.255.255
#
acl advanced 3002
 rule 0 permit ip source 192.168.85.136 0.0.0.7 destination 172.16.0.0 0.0.255.255
#
acl advanced 3998
 rule 0 permit tcp source 172.16.244.11 0 destination-port eq telnet
 rule 5 permit tcp source 172.16.244.11 0 destination-port eq 1410
#
IPSec基础配置方法非本案例重点，不额外赘述
```

验证测试：

云端——>合作方

```
<yunshang>tel 220.194.201.28 1410
Trying 220.194.201.28 ...
Press CTRL+K to abort
Connected to 220.194.201.28 ...

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: abc
Password:
<hezuoQMserver>
```

合作方——>云端

```
<hezuoQMserver>tel 192.168.85.137 1410
Trying 192.168.85.137 ...
Press CTRL+K to abort
Connected to 192.168.85.137 ...

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Password:
<yunshang>
```