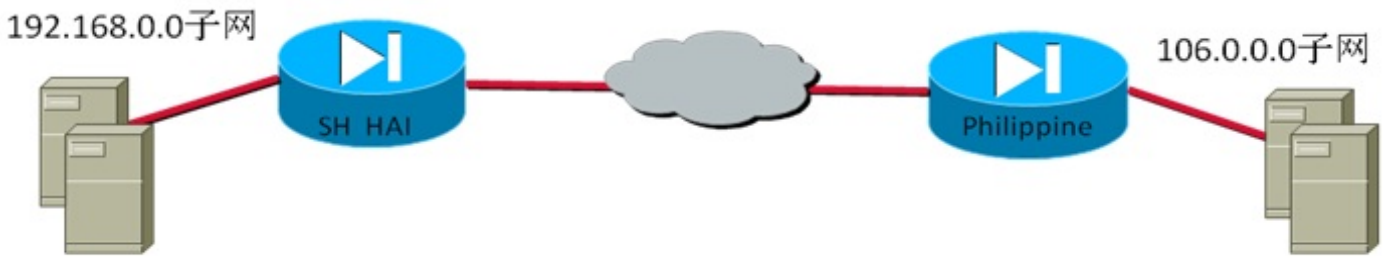
IPsec VPN 服务中断诊断案例

目录

案例分析网络拓扑结构



目的

学习完本案例后，对于IPsec vpn服务中断的故障排错有一个基本的思路。

地址介绍

SH Hai ASA的public IP 地址为10.10.10.10, Philippine ASA的public IP 地址为 11.11.11.11.（因涉及真实案例，故本案例中所有的公口地址都采用私网地址）

案例描述

用户自述并未对网络做任何变动，但突然就发现从上海到菲律宾的ipsec vpn不通了。从上海到菲律宾的公网IP是可达的。现要找出故障原因，使得从上海的192.168.0.0子网到菲律宾的 106.0.0.0子网可以通过 VPN 通讯。

排错工具

Show crypto isakmp sa
Show crypto ipsec sa
Capture命令
Show logging

故障排错过程

1. 通过远程访问进入SH Hai ASA, 请求用户发起从 A子网到B子网的兴趣流，通过下面的

命令察看show的结果：

```
Show crypto isakmp sa
Show crypto ipsec sa   peer  11.11.11.11
```
输出结果为：”There are no ipsec sas for peer 11.11.11.11”

注意ASA的Isakmp sa和Ipsec SA 是紧密绑定在一起的，两者必须同时存在，这点是和路由器不一样的。从上可以发现，兴趣流并没有触发第一阶段isakmp Sa的成功建立。

2. 检查两端ASA的IKE proposal和pre-shared 密钥，双方匹配，没有发现任何错误。
3. 通过capture命令察看是否兴趣流到达SH ASA的内口。

```
SH-5520(config)# access-list cs permit ip  192.168.0.0 255.255.128.0  106.0.0.0
255.255.255.0
SH-5520(config)# access-list cs perm ip  106.0.0.0 255.255.255.0  192.168.0.0
255.255.128.0

SH-5520(config)# capture  cs  access-list cs in  LAN
SH-5520(config)# show capture cs

19 packets captured

   1: 13:34:37.443611 192.168.0.9 > 106.0.0.251: icmp: echo request
   2: 13:34:37.443892 192.168.0.9 > 106.0.0.251: icmp: echo request
```
：从上我们可以看出，SH Hai ASA已经成功收到了来自192.168.0.0子网的数据包。但是并没有收到来自106.0.0.0子网的数据包。

同样在Philippine ASA作capture发现，show的结果为：

```
Philippine(config)# show capture cs
   0 packets captured
```
从以上抓包可以发现，上海的包应该没有送达菲律宾的ASA.

4. 检查双方路由：

```
 SH-5520# show route
  C    192.168.0.0 255.255.255.0 is directly connected, LAN
  S*   0.0.0.0 0.0.0.0 [1/0] via 20x.xx.xx.xx, Outside1
```
没有问题。

```
Philippine# show route
  C    106.0.0.0 255.255.255.0 is directly connected, inside
  S*   0.0.0.0 0.0.0.0 [1/0] via 20x.xx.xx.xx, Outside
```
也没有问题。

5. 上海的公口和菲律宾的公口互 Ping

```
SH-5520# ping  11.11.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.55.79.161, timeout is 2 seconds:
!!!!!

Philippine# ping  10.10.10.10
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 122.55.79.161, timeout is 2 seconds:
```

…..可以看到单向通讯

6. capture双方公口的包

```
access-list  cs1   permit ip host  10.10.10.10  host  11.11.11.11
access-list  cs1   permit ip host  11.11.11.11 host   10.10.10.10

capture  cs1  access-list  cs1   in LAN
```

同样在Philippine方也做同样的capture,命令略。

观测结果：
如从SH 发往Phillippine的公口的Ping包，可以看到在SH端有echo request的包可以捕捉到，但是没有echo reply的包被捕捉到，在菲律宾端，没有任何包可以在公口捕捉到。

如从Phillippine 发往SH的公口的Ping包，可以看到在Phillippine端有echo request的包可以捕捉到，但是没有echo reply的包被捕捉到，在SH端，既有echo request的包可以捕捉到，也有echo reply的包被捕捉到。 从双向的观测结果可以看到，问题出在了SH这一端的下一条，或者整个公网的路由或者其他方面。
在SH 端show arp:

```
Outside1 20x.1x4.x1.x49     000f.23d5.2c20   32
Outside1 20x.x36.x16.2x9   000f.23d5.2c20  1270
Outside1 2x2.1x6.2x8.x4     000f.23d5.2c20   11262
Outside1 2xx.x.1x8.x7           000f.23d5.2c20  11268
```

发现有四个不同的IP 地址（下一跳）都映射到了同一个MAC 地址。

7. 电话和客户沟通，请他和SP沟通，同时检查下一跳的连接方式和路由等。
8. 客户电话回馈，是SH下一跳的问题，已经解决了。（因不是本案例的重点内容， 故细节省略。）
9. SH和Philippine再次互Ping,互通成功，抓包也是正常的。
10. 但是兴趣流依旧没有触发成功的isakmp SA的建立。
    在SH ASA上启动系统日志:

```
Logging on
Logging buffered informational
Logging timestamp
```

然后show logging 发现SH ASA 报错：”……..no acceptable ipsec SA”.

检查双方的ipsec proposal，完全匹配。再检查双方的crypto map的配置：

SH ASA的配置：

```
crypto map Outside1_map 1 match address Outside1_1_cryptomap
crypto map Outside1_map 1 set pfs group1
crypto map Outside1_map 1 set peer  11.11.11.11
crypto map Outside1_map 1 set transform-set ESP-3DES-SHA
```

Philippine ASA的配置：

```
crypto map outside-1_map 25 match address outside-1_60_cryptomap
crypto map outside-1_map 25 set peer 10.10.10.10
crypto map outside-1_map 25 set transform-set ESP-3DES-SHA
```

问题找到，SH ASA启动了pfs group1, 而 Philippine ASA 没有启动。

11. 解决方案
    在SH ASA上: “no crypto map Outside1_map 1 set pfs group1”.

案例结果

SH ASA和Philippine ASA最终可以成功建立SA，两个子网之间的流量通过VPN通讯。

```
SH-5520# show crypto ipsec sa peer  11.11.11.11
peer address: 11.11.11.11
    Crypto map tag: Outside1_map, seq num: 1, local addr: 10.10.10.10

      access-list Outside1_1_cryptomap permit ip 192.168.0.0 255.255.128.0 106.0.0.0
255.255.255.0
      local ident (addr/mask/prot/port): (192.168.0.0/255.255.128.0/0/0)
      remote ident (addr/mask/prot/port): (106.0.0.0/255.255.255.0/0/0)
      current_peer: 11.11.11.11
      #pkts encaps: 1888599, #pkts encrypt: 1888599, #pkts digest: 1888599
      #pkts decaps: 1681578, #pkts decrypt: 1681578, #pkts verify: 1681578
      #pkts compressed: 0, #pkts decompressed: 0
```