IPSEC双向穿越建立不成功问题

IPSec VPN 聂骋 2023-01-12 发表

组网及说明

无具体组网，可以参考普通的IPSEC,只是两端都在内网，外面有个NAT设备。
本次是192.168.1.1为私网，对应的NAT上的公网为1.1.1.1
对端是172.16.1.1为私网，对应的NAT上的公网地址为2.2.2.2

告警信息

无

告警信息

问题描述

无法建立第一阶段，ike sa始终没有。

过程分析

1.debugging查看收发包情况，发行第五个包发过去后，对端就一直不回复了。可以看到重传的记录。并且前面可以看到debugging到主模式第五个包。

*Jan 10 22:04:00:217 2023 UNIS IKE/7/EVENT: -COntext=1; vrf = 0, local = 1.1.1.1 remote = 2.2.2.2/4500 IKE SA state changed from IKE_P1_STATE_SEND3 to IKE_P1_STATE_SEND5.
*Jan 10 22:04:05:604 2023 UNIS IKE/7/PACKET: -COntext=1; vrf = 0, local = 1.1.1.1, remote = 2.2.2.2/4500 Retransmit phase 1 packet.
*Jan 10 22:04:05:604 2023 UNIS IKE/7/PACKET: -COntext=1; vrf = 0, local = 1.1.1.1, remote = 2.2.2.2/4500 Sending packet to 2.2.2.2 remote port 4500, local port 4500.

2.检查ikeprofile下的配置，由于主模式第5个包是身份认证报文。因此判断是identity配置错误。检查现场配置发现。

```
ike profile pro1
 keychain key1 dpd interval 10 retry 3 on-demand
 local-identity address 192.168.1.1
 match remote identity address 2.2.2.2 255.255.255.255
 match local address GigabitEthernet1/0/4
 proposal 1
```

现场的local-identity是用的私网地址，而对端的identity写的对端的公网地址。而在对端由于也有NAT，对端写是的local-identity是私网地址172.16.1.1，对端地址写的是1.1.1.1，这就会出现异常。两端不是对称配置。

解决方法

identity改为对称即可，但是这样对后续其他运维人员其实是有难度的，所以直接改为fqdn即可。
原因为ike profile下的identity仅仅是一个身份信息而已，和接口地址没有任何关系，写地址是因为一般地址可以在网络设备中代表一个唯一的设备。可以理解为这个配置的意思是，我人为写了一个identity的身份信息，格式是地址格式，内容就是我认为敲的东西，因此只要两端的配置对称，那么这个ikeProfile的身份识别就是没问题的，而这个地址是否存在，是否接口地址，都无所谓。

注意！！！，在IPSEC中，有且仅有IKE 中的identity的地址是可以随便写的，其他涉及地址的配置，都不能随便写，比如keychain或者IPSEC下的local和remote。