某局点F1020防火墙IPSEC建立失败问题处理经验案例

IPSec VPN zhiliao_l6nhL 2018-11-08 发表

组网及说明

客户总部和分支两台我司防火墙互联，接口均为固定公网地址。

问题描述

IKE SA和IPSEC SA均无法建立

过程分析

1、由于目前第一阶段都建立失败，重点关注IKE参数设置和公网连通性。

beijing:

ike profile profile2

keychain keychin2

local-identity address 43.254.X.X

match remote identity address 222.76.X.X 255.255.255.248

xiamen:

ike profile profile2

keychain keychin2

local-identity address 222.76.X.X

match remote identity address 43.254.X.X 255.255.255.224

两边均使用默认proposal，没有问题。

2、beijing侧开启Debugging调试

Retransmit phase 1 packet. //**重传阶段1的报文**

91.166, remote = 222.76.241.20/500

Sending packet to 222.76.X.X remote port 500, local port 500.

....

Retransmission of phase 1 packet timed out. //**重传超时**

3、 为什么会重传阶段1的报文，怀疑是设备做了策略，测试公网可以互相PING通，没有对IPSEC做限制。

但仔细检测发现xiamen公网口有NAT SERVER配置，将500和4500端口映射到了内网地址。

解决方法

将针对500和4500端口的映射删除问题解决，IPSEC建立成功。

nat server protocol udp global 222.76.X.X 500 inside 192.168.40.40 500

nat server protocol udp global 222.76.X.X 4500 inside 192.168.40.40 4500

在遇到IPSEC建立失败问题的时候思路要清晰，对IPSEC建立的每一个阶段烂熟于心。