现场IPSEC隧道建立后单通

IPSec VPN NAT 聂骋 2022-05-30 发表

组网及说明

普通的IPSEC组网，不多做赘述

告警信息

无

告警信息

问题描述

现场做IPSEC隧道后，发现流量单通

过程分析

通过debugging内层也是就感兴趣流的流量
发现如下情况

发现设备做了NAT出去了，但是接口的NAT outbound是无法匹配的，现场正常做了deny的配置。
acl advanced 3001
rule 0 deny ip source 10.5.48.0 0.0.7.255 destination 10.5.0.0 0.0.3.255
进一步检查接口的NAT，发现现场还有NAT server的reversible功能
nat server protocol udp global current-interface 6060 inside 10.5.5X.X 6060 reversible rule SIP中继6060udp description SIP中继6060udp
nat server protocol tcp global current-interface 6060 inside 10.5.5X.X 6060 reversible rule SIP中继6060tcp description SIP中继6060tcp
由于nat server的reversible参数配置后，是不看端口的，因此取消了一个UDP相关的reversible，测试后发现现象还是一样。进一步关闭TCP的nat server的reversible之后才正常。

解决方法

接口的NAT server如果配置了reversible 也就可以出方向做源地址转换，并且不看端口，同时nat server 的reversible参数 配置后，也不看协议了，也就是说，只要一条nat server 配置了reversible参数，出方向做源地址转换既不看端口也不看协议，只要地址匹配就能发出去。因此这种情况下必须取消所有reversible相关的NAT server才行。

如果是外网访问内网的话，正常匹配协议和端口，不会受到reversible参数影响。