防火墙ipsec单通问题

IPSec VPN　彭钦　2022-08-17 发表

组网及说明

无

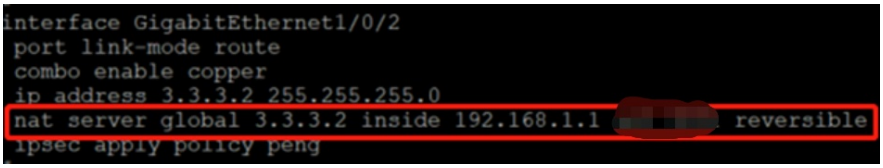
告警信息

无

问题描述

现场存在源地址转换、目的地址转换、ipsec业务、sip业务，但存在较为特殊的情况。现场192.168.1.1是内网服务器，需要给外网提供服务（通过nat server映射）；同时192.168.1.1也有ipsec业务，属于感兴趣流的源地址；同时192.168.1.1还需要通过nat server reversible去访问外网。但192.168.1.1去ping10.0.0.1不通，而10.0.0.1可ping通192.168.1.1（ipsec单通）。

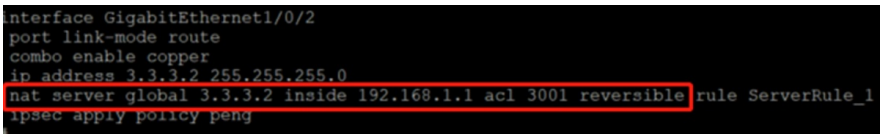
nat server global 3.3.3.2 inside 192.168.1.1 reversible

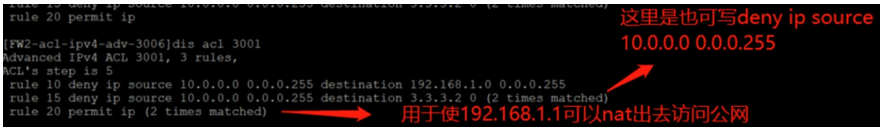


过程分析

通过查看会话及debug nat packet发现192.168.1.1去ping10.0.0.1匹配reversible进行了源地址转换，导致不通。需在nat server中加入acl进行过滤， 由于这里是反向匹配，当192.168.1.1 ping 10.0.0.1时，acl里的deny需要写源是10.0.0.0 0.0.0.255（或者明细 源是10.0.0.0 0.0.0.255 目的是3.3.3.2 0 global地址）。 同时由于现场192.168.1.1需要去访问公网以及外网需要映射进来，所以还需写个permit ip。

若deny 10.0.0.0 0.0.0.255 到 192.168.1.0 0.0.0.255（即感兴趣反向），此时是不匹配的。





解决方法

见上，关键是acl的写法。