安全策略匹配错误

域间策略/安全域 ASPF 聂骋 2022-12-06 发表

组网及说明

不涉及

告警信息

无

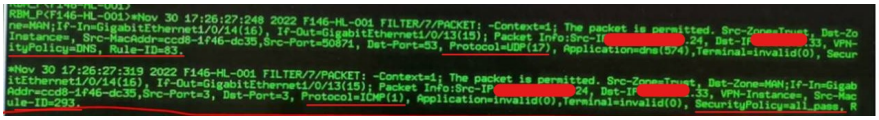
告警信息

问题描述

防火墙配置了安全策略放通某一条流量，但是看会话，发现匹配的是最后的全通，并且全通删除后就正常匹配了。

过程分析

检查debugging情况，发现24访问33的DNS流量，第一个过来后是正常匹配DNS规则，但是立即就有一条ICMP的流量，也是这个地址，重新匹配了all_pass的策略，会话也一直显示all_pass。



从debugging可以看到，ICMP报文端口是3，一般是差错报文，而差错报文分为外层IP头和内层IP头，防火墙对于这类报文处理逻辑是，外层IP去匹配策略，匹配后用内层去查找会话，如果会话存在，就刷新会话的策略信息。因此现场放全通后，ICMP差错报文被放通，而且无法匹配DNS，只能匹配全通，匹配后刷新了老会话，导致会话中一直显示匹配策略错误。

解决方法

正常情况，无需关注，如果需要排除掉，现场的情况如果想确认什么设备发出的报文，可以用ACL抓包去看看外层的IP是什么设备发的。然后策略阻断掉即可。

acl advanced 3XXX

rule 0 permit icmp icmp-type port-unreachable //这个根据现场实际情况可以更改。