防火墙安全策略没生效

域间策略/安全域 王听宇 2023-04-05 发表

组网及说明

fw--- ntp服务器

防火墙从ntp服务器同步时间失败

告警信息

无

告警信息

问题描述

防火墙从ntp服务器同步时间失败 /客户端-服务器模式

dis ntp status

Clock status unsynchronized

过程分析

debugging ntp-service all 看ntp报文没有发出，没有产生到ntp服务器的会话，web上抓出口也没有抓到发出的ntp报文

由于没有产生会话，怀疑ntp报文被防火墙阻断了

定义acl xxx，匹配不通流量源目的IP，双向报文配置两个rule

<H3C>debugging security-policy packet ip acl xxx

<H3C>debugging ip info acl XXX # 如果有丢包则会打印信息丢包的具体模块，如果没有丢包则不打印

<H3C>debugging aspf packet acl xxx

<H3C>debugging ip packet acl xxx

<FW>debugging session session-table all acl 3XXX # 可以查看会话被删除的具体情况

收集如上debug，发现被 Rule-ID=100阻断了

Apr 5 00:07:08:249 2023 H3C-FW FILTER/7/PACKET: -COntext=1; The packet is denied. Src-ZOne=Local, Dst-ZOne=Untrust;If-In=InLoopBack0(132), If-Out=GigabitEthernet1/0/15(17); Packet Info:Src-IP=a.a.a.a Dst-IP=b.b.b.b, VPN-Instance=, Src-MacAddr=0000-0000-0000,Src-Port=123, Dst-Port=123, Protocol=UDP(17), Application=ntp(47),Terminal=invalid(0), SecurityPolicy=any, Rule-ID=100.

如下策略配置在web安全策略最上面，正常应该最优先匹配

```
rule 108 name ntp
  action pass
  counting enable
  source-zone Trust
  source-zone Local
  destination-zone Untrust
  service dns-udp
  service-port udp destination eq 123
```

service port和service 是两种属性， 是且的关系，都要满足才行

Ntp的流量没匹配上如上策略，匹配了下面的rule100 被丢弃了

同一属性是或的关系，比如如下:

```
source-zone Trust
 source-zone Local
```

解决方法

将service dns-udp 去掉正常

```
rule 108 namentp
  action pass
  counting enable
  source-zone Trust
  source-zone Local
  destination-zone Untrust
  service-port udp destination eq 123
```