H3C F1020(V7) 新部署安全策略日志记录不同步刷新案例

Flow日志 域间策略/安全域 丁犁 2019-07-01 发表

组网及说明

不涉及

问题描述

H3C 防火墙 F1020，版本R9333P17

用户某流量，前期匹配FW Web界面中，安全策略ID=9规则执行转发。后续新增安全策略ID=11的规则，且将该规则调整至 ID=9 规则前，使得流量根据新增安全策略ID=11的规则转发，如图1所示：

图1

在F1020 命令行界面中，观察相关流量会话统计信息，确认相关流量已按照新策略（ID=11，Name=“微信HIS”）转发：

```
display session table ipv4 source-ip 192.168.x.x destination-ip  192.168.y.y verbose

Slot 1:
Initiator:
  Source      IP/port: 192.168.x.x/1
  Destination IP/port: 192.168.y.y/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/8
  Source security zone: 微信服务器
Responder:
  Source      IP/port: 192.168.y.y/1
  Destination IP/port: 192.168.x.x/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: 网闸外端机
State: ICMP_REPLY
Application: ICMP
Rule ID: 11
Rule name: 微信HIS     //会话统计中，流量匹配新的安全策略，rule id和name正确
Start time: 2019-05-11 12:00:46  TTL: 29s
Initiator->Responder:        1867 packets     112020 bytes
Responder->Initiator:        1867 packets     112020 bytes

Total sessions found: 1
```

F1020 Web 界面，安全策略日志中，发现相关流量的源安全域、目的安全域，已经调整为修改后的安全策略“微信HIS”相关内容（蓝色），但**“规则编号”和“安全策略”名称，却未刷新出现异常。**及，仍然显示为修改前的“微信服务器”名称（红色），出现异常（正常应该显示为“微信HIS”名称）.如图2所示：

图2

过程分析

不涉及

解决方法

目前，V7平台防火墙对于安全策略日志默认有延迟发送功能，对于相同的日志，5分钟只发送一条。用户使用ping测试观察日志刷新变化情况，ICMP的安全策略日志只携带ICMP Type 和ICMP Code，每次ping， ICMP Type 和ICMP Code 都相同。

安全策略配置变更后一段时间内还会收到延迟发送的日志，显示为以前的ID和相同的五元组。

若不希望延迟发送日志，可以**开启命令[H3C]aspf log sending-realtime enable** 解决。