安全策略里边调用URL导致icmp每30个包丢一个包// url-category url-permit

域间策略/安全域 URL过滤 **李瑞** 2023-03-02 发表

组网及说明

icmp过墙纯转发

告警信息

不涉及

问题描述

icmp报文过墙纯转发，每30个报文丢一个包

过程分析

debug看到，由于无法匹配中rule 18的策略，安全策略模块通知ASPF删除会话，下一个报文重新匹配安全策略：

```
*Mar  1 15:53:58:407 2023 M9006-01 FILTER/7/PACKET: -Slot=2.1; The packet is denied. Src-Zone=Trust, Dst-Zone=Untrust;If-In=Route-Aggregation1.38(7014), If-Out=Route-Aggregation2(7009); Packet Info:Src-IP=1.1.1.1, Dst-IP=2.2.2.2, VPN-Instance=,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), Url-category=invalid(65535), ACL=none, Rule-ID=none.
*Mar  1 15:53:58:407 2023 M9006-01 ASPF/7/PACKET: -Slot=2.1; The non-first packet was dropped by packet filter or object-policy. Src-Zone=Trust, Dst-Zone=Untrust;If-In=Route-Aggregation1.38(7014), If-Out=Route-Aggregation2(7009); Packet Info:Src-IP=1.1.1.1, Dst-IP=2.2.2.2, VPN-Instance=none, Src-Port=1, Dst-Port=2048. Protocol=ICMP(1).
*Mar  1 15:53:58:407 2023 M9006-01 SESSION/7/TABLE: -Slot=2.1; Tuple5(EVENT): 1.1.1.1/1-->2.2.2.2/2048(ICMP(1)) Module ASPF  set deleted flag.
*Mar  1 15:53:58:407 2023 M9006-01 IPFW/7/IPFW_INFO: -Slot=2.1; MBUF was intercepted! Phase Num is 9(post routing beforefrag), Service ID is 3(interzone), Bitmap is 1000000000000000, return 1(0:continue, 1:dropped, 2:consumed, 3:enqueued, 4:relay)! Interface is Route-Aggregation2, s=1.1.1.1, d= 2.2.2.2, protocol= 1, pktid = 24710.
*Mar  1 15:53:58:435 2023 M9006-01 SESSION/7/TABLE: -Slot=2.1; Tuple5(EVENT): 1.1.1.1/1-->2.2.2.2/2048(ICMP(1)) Session entry was deleted.
*Mar  1 15:54:03:114 2023 M9006-01 SESSION/7/TABLE: -Slot=2.1; Tuple5(EVENT): 1.1.1.1/1-->2.2.2.2/2048(ICMP(1)) Session entry was created.
*Mar  1 15:54:03:114 2023 M9006-01 SESSION/7/TABLE: -Slot=2.1; Tuple5  (FSM): 1.1.1.1/1-->2.2.2.2/2048(ICMP(1)) FSM:NONE-->ICMP_REQUEST, dir:ORIGIN, PacketType:REQUEST(8)
*Mar  1 15:54:03:114 2023 M9006-01 FILTER/7/PACKET: -Slot=2.1; The packet is permitted. Src-Zone=Trust, Dst-Zone=Untrust;If-In=Route-Aggregation1.38(7014), If-Out=Route-Aggregation2(7009); Packet Info:Src-IP=1.1.1.1, Dst-IP=2.2.2.2, VPN-Instance=, Src-MacAddr=642f-c7c8-ae01,Src-Port=8, Dst-Port=0, Protocol=ICMP(1), Application=ICMP(22742), Url-category=initial-category(65533), SecurityPolicy=url-permit, Rule-ID=18.
*Mar  1 15:54:03:114 2023 M9006-01 SESSION/7/TABLE: -Slot=2.1; Tuple5(EVENT): 1.1.1.1/1-->2.2.2.2/2048(ICMP(1)) Session entry was backuped.
```

相关配置如下：

```
#
Security-policy ip
rule 18 name url-permit
  action pass
  logging enable
  counting enable
  source-zone Trust
  destination-zone Untrust
 url-category url-permit

#
url-filter category url-permit severity 1000
 rule 1 host www.baidu.com
 rule 2 host text aiqiyi.com
```

分析结论及问题原因：

安全策略里边调用URL，这个URL过滤是且的关系，URL模块会等待30个报文左右用来识别，如果是icmp的报文，那么30个之后还是识别不出url，那么直接被安全策略阻断。

解决方法

需要重新创建优先级更高的rule放通icmp等不携带URL的报文。