某局点新增安全策略导致业务中断问题分析

域间策略/安全域 **孔凡安** 2023-04-23 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

背景：某局点版本老旧依旧使用的是传统的包过滤策略，后续客户要求替换为更为先进的安全策略。
现场在安全策略使能的情况下，发现新增rule之后，OSPF邻居中断，业务异常。
日志记录如下：

> %Apr 12 21:18:05:804 2023 M9006 SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.107.239.237-User=dnt; Command is security-policy ip
> %Apr 12 21:18:09:883 2023 M9006 SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.107.239.237-User=dnt; Command is display this
> %Apr 12 21:19:00:307 2023 M9006 SHELL/6/SHELL_CMD: -Line=vty0-IPAddr=10.107.239.237-User=dnt; Command is rule name 20210605_local-SERVER ----防火墙安全策略动作缺省为drop，匹配条件为空，ospf报文匹配到该策略，被丢弃
> %Apr 12 21:19:07:157 2023 M9006 OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 10.101.34.2 Local address: 10.101.39.118 Remote address: 10.101.39.117 Reason: DeadInterval timer expired.
> %Apr 12 21:19:07:157 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.117(Route-Aggregation20.4033) changed from FULL to DOWN.
> %Apr 12 21:19:08:157 2023 M9006 OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 10.101.34.45 Local address: 10.101.39.102 Remote address: 10.101.39.101 Reason: DeadInterval timer expired.
> %Apr 12 21:19:08:157 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.101(Route-Aggregation1) changed from FULL to DOWN.
> %Apr 12 21:19:08:157 2023 M9006 OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 10.101.34.1 Local address: 10.101.39.114 Remote address: 10.101.39.113 Reason: DeadInterval timer expired.
> %Apr 12 21:19:08:157 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.113(Route-Aggregation10.4032) changed from FULL to DOWN.
> %Apr 12 21:19:08:158 2023 M9006 OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 10.101.34.46 Local address: 10.101.39.106 Remote address: 10.101.39.105 Reason: DeadInterval timer expired.
> %Apr 12 21:19:08:158 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.105(Route-Aggregation2) changed from FULL to DOWN.
> %Apr 12 21:21:02:415 2023 M9006 SSHS/6/SSHS_DISCONNECT: SSH user dnt (IP: 10.107.239.237) disconnected from the server.
> %Apr 12 21:21:02:425 2023 M9006 SHELL/5/SHELL_LOGOUT: dnt logged out from 10.107.239.237.
> %Apr 12 21:21:05:586 2023 M9006 SHELL/6/SHELL_CMD: -Line=-IPAddr=**-User=**; Command is undo debugging all
> %Apr 12 21:23:49:123 2023 M9006 SHELL/5/SHELL_LOGIN: dnt logged in from con1/0.
> %Apr 12 21:23:51:505 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is sys
> %Apr 12 21:23:55:980 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is display interface Reth 1
> %Apr 12 21:24:18:901 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is security-policy ip
> %Apr 12 21:24:20:128 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is display this
> %Apr 12 21:24:25:541 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is rule 0
> %Apr 12 21:24:31:737 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is display this
> %Apr 12 21:24:38:146 2023 M9006 CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=12-CommandSource=snmp-COnfigSource=startup-COnfigDestination=running; Configuration changed.
> %Apr 12 21:24:40:957 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is source-zone local
> %Apr 12 21:24:52:734 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is source-zone SERVER

%Apr 12 21:24:59:889 2023 M9006 SHELL/6/SHELL_CMD: -Line=con1/0-IPAddr=**-User=dnt; Command is destination-zone SERVER ---添加匹配条件后，ospf报文可以正常匹配包过滤测试

%Apr 12 21:25:06:540 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.105(Route-Aggregation2) changed from LOADING to FULL.

%Apr 12 21:25:07:194 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.105(Route-Aggregation1) changed from FULL to DOWN.

%Apr 12 21:25:08:202 2023 M9006 OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.101.39.105(Route-Aggregation2) changed from LOADING to FULL.

过程分析：

首先，需要明确的是当安全策略与包过滤策略同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以请合理配置安全策略和包过滤策略，否则可能会导致配置的包过滤策略不生效。

根据日志记录可以看出，新增安全策略后，OSPF立即中断，分析原因应该是防火墙安全策略缺省动作为drop，匹配条件为空（即所有流量均能匹配到该规则），OSPF报文匹配到该策略，被丢弃导致邻居中断。后续再安全策略中添加匹配条件后，OSPF报文无法匹配安全策略，继续匹配原来的包过滤策略，邻居状态变为FULL状态。

解决方法

解决方案：先disable安全策略，等安全策略的配置完成后，重新使能安全策略。

此外，还需要注意：安全策略功能与对象策略功能在设备上不能同时使用，首次进入安全策略视图后，对象策略功能立即失效。这一点要和包过滤策略做区分。安全策略缺省动作为拒绝，使用对象策略的场景下使能安全策略后有业务全部中断的风险！