

知

MER5200配置上网行为管理后部分应用异常经验案例

攻击防范及检测

特征库

郭昊

2021-03-30 发表

组网及说明

MER5200作为中小企业出口设备，配置上网行为管理。

问题描述

MER5200设备配置上网行为管理，需求为允许微信、有道词典等指定应用访问外网，不允许其他应用访问外网。配置上网行为管理后，微信、qq、有道词典等应用均无法正常使用。

过程分析

类问题多是由于上网行为管理策略禁止了应用软件发出的特定报文导致，常见现象包括应用连接不到外网，web页面验证码显示不全，应用特定功能无法使用（例如qq无法使用qq群功能、群消息不显示图片）等等。遇到此类问题排查方法有以下两种。

第一种，将上网行为管理的应用控制策略，勾选“记录”，之后当应用报文被策略过滤时，设备logbuffer/logfile会有日志。我们可以找一台电脑测试，根据测试电脑地址过滤日志，就可以确认是哪条策略过滤了应用，之后将该上网行为管理策略改为放通即可。以有道词典无法连接外网为例，设备日志会记录下面内容（可以根据display logbuffer reverse | include 10.10.15.113过滤日志，10.10.15.113为测试电脑地址）：

```
%Mar 23 12:26:43:440 2021 Fast UFLT/6/UFLT_MATCH_IPV4_LOG: Protocol(1001)=TCP;
```

```
Application(1002)=YouDaoDict;
```

```
URL(1093)=dict.youdao.com/fsearch;
```

```
URLCategory(1094)=OthersLife;
```

```
PolicyName(1079)=1;
```

```
SrcIPAddr(1003)=10.10.15.113;
```

```
SrcPort(1004)=56582;
```

```
DstIPAddr(1007)=220.181.76.82;
```

```
DstPort(1008)=80;
```

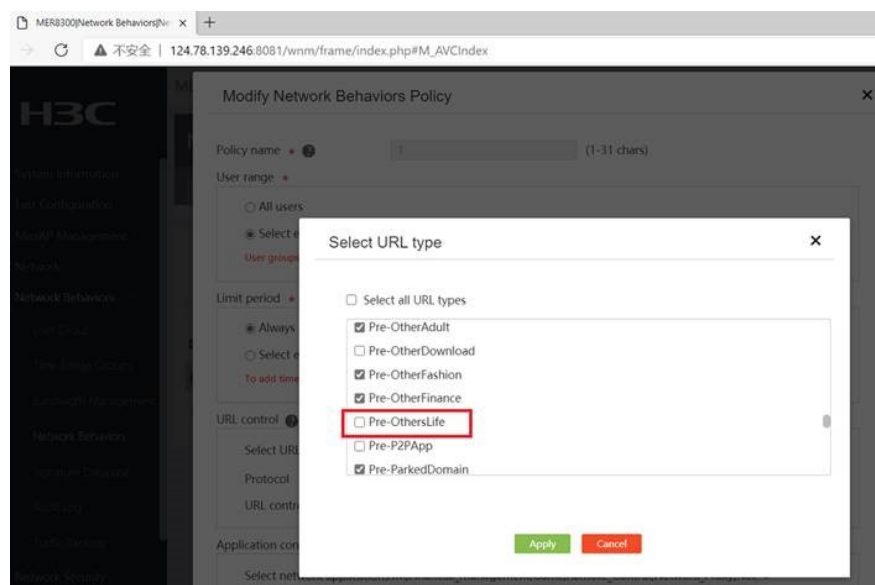
```
SrcZoneName(1025)=Any;
```

```
DstZoneName(1035)=Any;
```

```
UserName(1113)=10.10.15.113;
```

```
Action(1053)=Drop;
```

其中application=YouDaoDict为测试相关报文，action=drop说明策略过滤了该报文，UrlCategory=OthersLife为具体生效的策略名。在设备web页面修改上述策略时，为了方便找到OthersLife策略，可以将设备web页面先改为英文，之后在上网行为管理策略—>网址控制中，找到OthersLife去勾选，改为不过滤此类url。之后测试有道词典正常。



第二种方法，根据测试终端地址做debug，确认哪条策略过滤了报文。以测试终端地址192.168.1.201为例，

```
[H3C]acl advanced 3999
```

```
[H3C-acl-ipv4-adv-3999]rule permit ip source 192.168.1.201 0
```

```
<H3C>debugging object-policy packet ip acl 3999
```

```
<H3C>t m
```

```
<H3C>t d
```

之后关注被denied报文。以下述情况为例，被过滤的报文匹配到策略的应用分类TencentResource，rule-id=280表示TencentResource所属app-group中的第280个drop策略。之后在web页面将对应drop策略改为放通即可。

*Aug 21 06:25:08:826 2020 H3C FILTER/7/PACKET: The packet is denied, Src-
解决方法
ZOne=Trust(matched=Any), Dst-ZOne=Untrust(matched=Any):If-In=Vlan-interface1(17413), If-Out=D
根据日志或debug信息，确认将过滤应用报文的策略，并将其改为放通。
ialero(17414), Packet Info:Src IP=192.168.1.201, Dst IP=122.228.66.158, VPN-Instance=, Src-Port=6
5534, Dst-Port=443, Protocol=TCP(6), Application=TencentResource(22126), ObjectPolicy=Any-Any,
Rule-ID=280.

