无线portal过程中，流量到达设备后被异常放通/deny/重定向异常问题

Portal 林东良 2024-06-20 发表

组网及说明

STA---云AP or STA---AP---AC

告警信息

无

问题描述

无线终端（安卓）接入无线后，无法自动弹出portal页面。如果手动打开浏览器，或手动输入ip或域名，可以弹出portal页面。

过程分析

电脑手机等终端在接入网络后，会发出大量的探测报文，有的是探测微软服务，有的是探测谷歌服务。这些探测报文按理说可以触发portal重定向动作。

客户的终端在手动打开浏览器时，可以弹出portal页面，也可以正常登录。因此可判断不是DNS问题或者portal服务器问题，猜测是portal过程处理问题。

在设备（云AP或者AC）上debug portal all，有如下log。

```
[Outbound] permit the packet on the outbound {MatchRes = [Rule2-Permit]}.
IfName = WLAN-BSS1/0/3, PortName = WLAN-BSS1/0/3, Vlan = 1, DstMAC = 725e-3250-4ca6,
SrcIP = 23.192.223.165, DstIP = 192.168.1.8
L4Protocol = 6, SrcPort = 443, DstPort = 54776, VrfIndex = 0

*Apr 30 08:24:47:705 2024 PRUEBAS POLANCO PORTAL/7/RULE:
 [Outbound] permit the packet on the outbound {MatchRes = [Rule1-Permit]}.
 IfName = WLAN-BSS1/0/3, PortName = WLAN-BSS1/0/3, Vlan = 1, DstMAC = 725e-3250-4ca6,
 SrcIP = 192.178.52.138, DstIP = 192.168.1.8
 L4Protocol = 6, SrcPort = 443, DstPort = 42102, VrfIndex = 0

*Apr 30 08:24:47:705 2024 PRUEBAS POLANCO PORTAL/7/RULE:
 [Outbound] permit the packet on the outbound {MatchRes = [Rule2-Permit ]}.
 IfName = WLAN-BSS1/0/3, PortName = WLAN-BSS1/0/3, Vlan = 1, DstMAC = 725e-3250-4ca6,
 SrcIP = 192.178.57.14, DstIP = 192.168.1.8
 L4Protocol = 6, SrcPort = 443, DstPort = 34588, VrfIndex = 0

*Apr 30 08:24:47:705 2024 PRUEBAS POLANCO PORTAL/7/RULE:
[Outbound] permit the packet on the outbound {MatchRes = [Rule1-Permit]}.
IfName = WLAN-BSS1/0/3, PortName = WLAN-BSS1/0/3, Vlan = 1, DstMAC = 725e-3250-4ca6,
SrcIP = 192.178.52.170, DstIP = 192.168.1.8
 L4Protocol = 6, SrcPort = 443, DstPort = 36446, VrfIndex = 0

*Apr 30 08:24:47:705 2024 PRUEBAS POLANCO PORTAL/7/RULE:
 [Outbound] permit the packet on the outbound {MatchRes = [Rule2-Permit]}.
 IfName = WLAN-BSS1/0/3, PortName = WLAN-BSS1/0/3, Vlan = 1, DstMAC = 725e-3250-4ca6,
 SrcIP = 192.168.1.1, DstIP = 192.168.1.8
 L4Protocol = 1, SrcPort = 0, DstPort = 0, VrfIndex = 0
```

可以看到一些访问https的流量匹配上 Rule1-Permit。

汇总一下portal debug中遇到的各种rule

```
  [Outbound] permit the packet on the outbound {MatchRes = [Rule4-Deny]}.
 [Inbound] execute full rule match, { MatchRes = [Rule1-Permit] }
 [Outbound] execute full rule match, { MatchRes = Pre-Rule1-Permit }
 [Outbound] permit the packet on the outbound {MatchRes = [Rule2-Permit]}.
 [Inbound] execute full rule match, { MatchRes = [Rule3-Redirect] }
```

各个rule的意义：

Rule1   free rule放行，free rule放行的IP都可以从配置看到

Rule2   用户已经通过认证，或者触发临时放行.

Rule3   默认配置，HTTP/HTTPS流量被重定向

Rule4　默认配置，流量默认deny。或者通过配置portal deny 配置下发的

上面看到443端口的流量被Rule1放通，因此怀疑安卓终端探测流量匹配到free-rule而导致被放通，所以未能触发portal重定向而自动弹出portal页面。

portal free-rule配置如下，但是放通的是域名，无法和被放通的流量对应上。

```
#
 portal user log enable
 portal client-gateway interface Vlan-interface1
 portal free-rule 501 destination ip 114.114.114.114 255.255.255.255
 portal free-rule 502 destination ip any udp 53
 portal free-rule 503 destination ip any tcp 53
 portal free-rule 504 destination ip any tcp 5223
 portal free-rule 520 destination oasisauth.h3c.com
 portal free-rule 521 destination short.weixin.qq.com
 portal free-rule 522 destination mp.weixin.qq.com
 portal free-rule 523 destination long.weixin.qq.com
 portal free-rule 524 destination dns.weixin.qq.com
 portal free-rule 525 destination minorshort.weixin.qq.com
 portal free-rule 526 destination extshort.weixin.qq.com
 portal free-rule 527 destination szshort.weixin.qq.com
 portal free-rule 528 destination szlong.weixin.qq.com
 portal free-rule 529 destination szextshort.weixin.qq.com
 portal free-rule 530 destination isdspeed.qq.com
 portal free-rule 531 destination wx.qlogo.cn
 portal free-rule 532 destination wifi.weixin.qq.com
 portal free-rule 533 destination login.live.com
 portal free-rule 534 destination login.microsoftonline.com
 portal free-rule 535 destination browser.events.data.microsoft.com
 portal free-rule 536 destination aadcdn.msauth.net
 portal free-rule 537 destination connect.facebook.net
 portal free-rule 538 destination staticxx.facebook.com
 portal free-rule 539 destination graph.facebook.com
 portal free-rule 540 destination www.facebook.com
 portal free-rule 541 destination m.facebook.com
 portal free-rule 542 destination facebook.com
 portal free-rule 543 destination static.xx.fbcdn.net
 portal free-rule 544 destination *.xx.fbcdn.net
 portal free-rule 545 destination scontent-lax3-2.xx.fbcdn.net
 portal free-rule 546 destination scontent-hkg3-1.xx.fbcdn.net
 portal free-rule 547 destination *.facebook.com
 portal free-rule 548 destination *.facebook.net
 portal free-rule 549 destination accounts.google.com
 portal free-rule 550 destination gstatic.google.com
 portal free-rule 551 destination fonts.gstatic.com
 portal free-rule 552 destination accounts.youtube.com
 portal free-rule 553 destination play.google.com
 portal free-rule 554 destination lh3.googleusercontent.com
 portal free-rule 555 destination ssl.gstatic.com
 portal free-rule 556 destination clients1.google.com
 portal free-rule 557 destination www.google.com
 portal free-rule 558 destination accounts.google.com.sg
 portal free-rule 559 destination content-autofill.googleapis.com
 portal free-rule 560 destination www3.l.google.com
 portal free-rule 561 destination www.googleapis.com
 portal free-rule 562 destination accounts-cctld.l.google.com
 portal free-rule 563 destination api.twitter.com
 portal free-rule 564 destination abs-0.twimg.com
 portal free-rule 565 destination pbs.twimg.com
 portal free-rule 566 destination ton.twimg.com
 portal safe-redirect enable
 portal safe-redirect method get post
 portal safe-redirect user-agent Android
 portal safe-redirect user-agent CFNetwork
 portal safe-redirect user-agent CaptiveNetworkSupport
 portal safe-redirect user-agent Chrome
 portal safe-redirect user-agent Firefox
 portal safe-redirect user-agent MicroMessenger
 portal safe-redirect user-agent MicrosoftNCSI
 portal safe-redirect user-agent Mosilla
 portal safe-redirect user-agent Safari
 portal safe-redirect user-agent WeChat
 portal safe-redirect user-agent android
 portal safe-redirect user-agent iPhone
 portal safe-redirect user-agent micromessenger

#
```

如果free-rule是域名的，可以从display portal dns free-rule-host 查看域名和IP对应关系。

最后证实，该https流量匹配上了fonts.gstatic.com的free-rule，导致被放通。

解决方法

删除多余的free-rule后，问题解决，终端可以在接入WIFI后自动弹出portal页面。