F1070 是否可以使用策略路由进行基于目的域名的指导转发

outbound链路负载均衡 策略路由 **杨玉琦** 2021-11-18 发表

问题描述

当前现场业务针对大量目的域名进行链路负载，因该方式会导致dns缓存过高因此设备运行异常。是否可以使用策略路由替代负载均衡针对大量目的域名进行指导转发?

解决方法

经确认，可以用策略路由基于域名转发，具体配置关系为：策略路由可以通过匹配acl实现，acl中可以调用对象组，对象组中可以匹配主机名。

其实现方式是防火墙去主动解析域名，然后将解析的得到的IP地址替换域名，报文上到设备时查策略路由中对应的IP可以匹配上。这种方式需要配置和终端一样的dns服务器，且防火墙会维护dns动态表项，dns动态表项的缓存时间由dns服务器决定，老化后会继续查询dns，因此也要消耗性能去维护dns缓存表。

通过负载均衡和策略路由这两种方式实现都会缓存dns表，但负载均衡的dns由负载均衡模块处理，缓存时间缺省60min可以手动设置，策略路由方式的dns表项动态缓存，缓存时间无法手动设置。当域名过多时，两种方式都会维护大量的dns表项，因此不建议配置过多，还是建议基于IP方式的负载策略。