策略路由中调用 FQDN 地址对象不稳定问题。

总结一下问题：
0:首先 FQDN 地址对象有两种方式获取：
1.设备自己使用配置的 DNS
2.DNS 的流量经过设备，设备记下来的。

版本：
V6.2.4
1.通过策略路由诊断命令查看装载的 FQDN 地址

```
HUB-1 # diagnose    firewall    proute list
list route policy info(vf=root):

id=2 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0:0 iif=3 dport=0-65535 oif=6
source(1): 0.0.0.0-255.255.255.255
destination fqdn(1):
      www.baidu.com ID(5) ADDR(192.168.10.100)
hit_count=1 last_used=2021-01-07 16:32:01
```

2.观察 FQDN 的对应的地址条目和 TTL

```
config firewall address
      edit "www.baidu.com"
            set uuid d7d6b380-50b2-51eb-2a95-024ae4a2369e
            set type fqdn <---
            set allow-routing enable
            set fqdn "www.baidu.com" <---
            set cache-ttl 86400
      next
      edit "news.baidu.com"
            set uuid 079cc6ba-50ca-51eb-3ee5-a232eec6d748
            set type fqdn <---
            set fqdn "news.baidu.com" <---
      next
      edit "tieba.baidu.com"
            set uuid 0b148714-50cb-51eb-a4ed-1eee006006f7
            set type fqdn <---
            set fqdn "tieba.baidu.com" <---
      next
end
```

HUB-1 # diagnose test application dnsproxy 6
worker idx: 0
vfid=0 name=news.baidu.com ver=IPv4 timer running, min_ttl=3600:2233, cache_ttl=0 , slot=-1, num=1, wildcard=0
192.168.10.111 (ttl=3600:2239:2239)
vfid=0 name=tieba.baidu.com ver=IPv4 timer running, min_ttl=3600:2223, cache_ttl=0 , slot=-1, num=0, wildcard=0
vfid=0 name=www.baidu.com ver=IPv4 timer running, min_ttl=3600:2223, cache_ttl=86400 , slot=-1, num=1, wildcard=0
192.168.10.100 (ttl=3600:2229:85029)

其中 ttl=3600:2229:85029 含义：3600 是 DNS 服务器返回的 TTL，2229 是从 3600 减到的值，85029 是手工在设备上配置的这个 cache-tts 减的值。

如果配置的 cache-ttl> dns 服务器返回的 TTL，认为该 FQDN 下面配置的 cache-ttl 时间优先
如果 cache-ttl<dns 服务器返回的 TTL DNS 服务器返回的 TTL 优先。
如果没有没配置 cache-ttl（0）,以 DNS 服务器返回的 TTL 为准。
一句话：以大的值为准。

配置 86400，我们可以认为手工配置的 cache-ttl 优先。
如果 cache-ttl 计数器减到 0，该 FQDN 对应的地址条目消失。

4.目前是通过修改 fqdn 地址下的 cache-ttl 调整成 86400 解决

```
config firewall address
    edit "www.baidu.com"
        set uuid d7d6b380-50b2-51eb-2a95-024ae4a2369e
        set type fqdn <---
        set allow-routing enable
        set fqdn "www.baidu.com" <---
        set cache-ttl 86400
    next
```

5..另外 FQDN 地址缓存条目与缓存时间与 config system dns
下的无关。

```
config system dns
    set primary 192.168.10.16
    set dns-cache-limit 2     //FQDN 地址与这个无关
    set dns-cache-ttl 2000 // FQDN 地址与这个无关
end
```

这里面配置的是 DNS cache，可以通过以下方式观察。

```
HUB-1 # diagnose    test application      dnsproxy    7
worker idx: 0
vfid=0, name=www.huagai.com, ttl=595:575:1980
        106.75.164.205 (ttl=595)
vfid=0, name=ipbl.fortinet.com, ttl=76978:76938:1960
        208.91.113.75 (ttl=76978)
CACHE num=2
```


李威峰

中国区技术支持工程师

Best Regards
WeiFeng Li 李威峰 |TAC Engineer,China
Floor 12th, Founder International Building, No.52,
North 4th Ring West Road,Haidian district, BJ 100080, China
O: 400-600-5255 | E:wfli@fortinet.com
北京市海淀区北四环西路 52 号方正国际大厦 12 层