DNS 服务 Serv

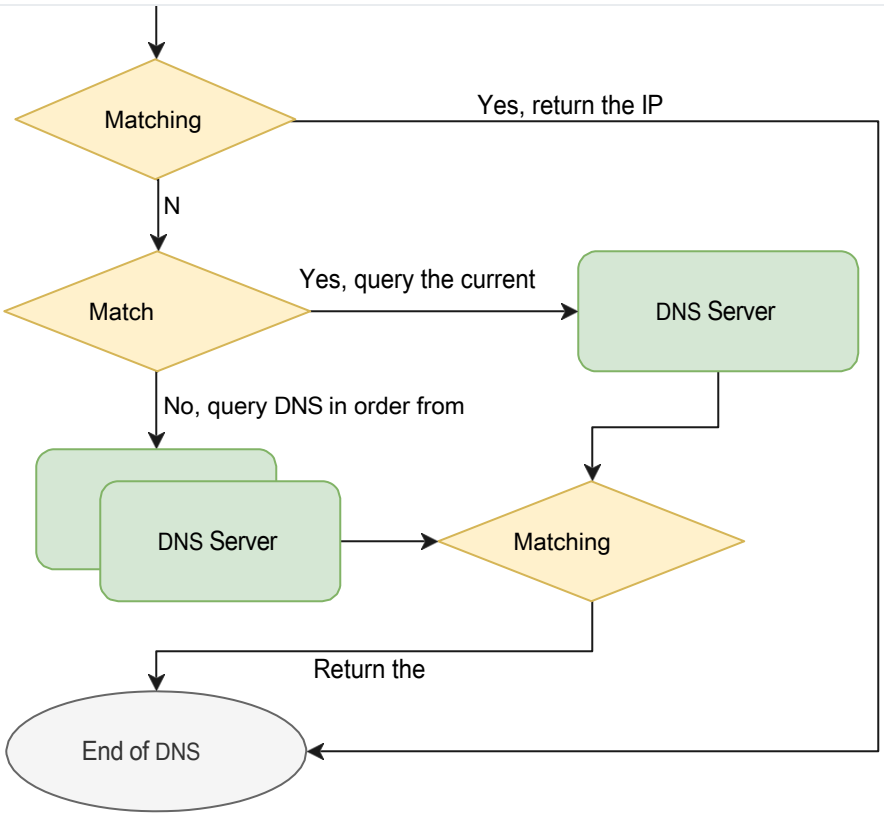
V2Ray's built-in DNS service, which resolves IPs, is often used first to match routing rules, and if not configured properly, requests can take a while to resolve on DNS requests.

The "`domainStrategy`" mode of routing is closely related to the DNS function, so here is a special section on it.

- `"AsIs"`, when the endpoint requests a domain name, the domain inside the route is matched and the routing rules are followed directly regardless of whether it matches or not.
- `"IPIfNonMatch"` , when the terminal requests a domain name, the domain in the route is matched, if it cannot be matched
  If the result is obtained, a DNS query is performed for the domain name, and the resulting IP address is used to re-route the IP match.
- `"IPOnDemand"` , when matching any IP-based rule, resolves the domain name to IP immediately for matching.

`AsIs` are the fastest, but the least accurate in terms of routing results, while `IPOnDemand` is the most accurate, but the slowest.

DNS 流程 Proc



Basic 基础配置

```json
{
 "dns": {
   "servers": [
     "1.1.1.1".
     "localhost"
   ]
 }
}
```

The basic use of the DNS module is not particularly complicated. It is to specify one or more DNS servers, which V2ray will use in turn (the next one will be queried when the query fails). The meaning of "localhost" is special, as the local program uses the system's DNS to send requests, rather than V2ray communicating directly with DNS servers, which is not controlled by modules such as Routing.

新 V2Ray 白话文指南 White Paper Guide

进阶配置 Advance

Although this is a basic article, I don't want to start another DNS article on the high-level side, so I'll write it here.

客户端分流配置 Passenger side

```json
{
 "dns": {
   "servers": [
     {
       "address": "119.29.29.29".
       "port": 53.
       "domains": [
         "geosite:cn"
       ].
       "expectIPs": [
         "geoip:cn"
       ]
     }.
     {
       "address": "8.8.8.8".
       "port": 53.
       "domains": [
         "geosite:geolocation-!cn",
         "geosite:speedtest",
         "ext:h2y.dat:gfw"
       ]
     },
     "1.1.1.1".
     "localhost"
   ]
 }
}
```

The DNS service can be used for triage. The general idea is that "which domain names should be resolved by which DNS servers, and you want to get the IP addresses that belong to them. The

configuration rules are similar to those used in routing mode, so please refer to the official file for details.

If the domain name is not a domestic domain, it will match the second configuration and use the new result. Domains that are not domestic will be matched to the second configuration, so use 8.8.8.8 to query, this time without
If you are expecting a special IP address, you can use the one returned directly; if there is a problem with any of the above processes, query 1.1.1.1 directly, or let the local DNS try again.

服务器配置

```json
{
 "dns": {
   "servers": [
     "https+local://1.1.1.1/dns-query",
     "localhost"
   ]
 }
}
```

DNS on the server side generally requires no complex configuration. If configured, note that the outbound of `freedom` should be configured
The built-in DNS is used only when `"domainStrategy"` is `"UseIP" | "UseIPv4" | "UseIPv6"`, and the default `AsIs are` left to the operating system to resolve and connect.

The DOH function added in the new version 4.22.0+ can be easily used when deployed on the server side.

对外开放 DNS for v2ray 服务

The author of Kitsunebi, in "A Discussion of the Use of Various Bashful DNS Technologies in Proxy Environments," describes how to open up the v2ray DNS through the Dokodemo inbound protocol and the DNS outbound protocol to take full advantage of the power of the v2ray's built-in DNS, such as allowing other system applications to obtain DNS without a proxy. In this article, Kitsunebi describes how to open the v2ray DNS through `the Dokodemo` inbound protocol and the `DNS` outbound protocol, so that the power of the v2ray built-in DNS can be fully utilized, for example, by allowing other non-proxy affiliates of the system to obtain the power of DNS-

level wireless filtering, and by taking over the system DNS in a transparent proxy.

The core idea of this method is to use the `Dokodemo` inbound protocol to receive DNS request traffic and forward it to the `DNS outbound protocol.` The `DNS outbound` protocol intercepts `Type A` and `Type AAAA` DNS queries and passes them to the v2ray built-in DNS for processing, which returns the query results; otherwise, the query traffic is sent to the target DNS server according to `Dokodemo`'s configuration.

Basic 客户端基本配置

```
        {
            "tag": "dns-in",
            "port": 53.
            "protocol": "dokodemo-door".
            "settings": {
                "address": "8.8.8.8".
                "port": 53,
                "network": "tcp,udp",
                "userLevel": 1
            }
        }
    ].
    "outbounds": [
        {
            "protocol": "dns".
            "tag": "dns-out"
        }
    ].
    "routing": {
        "rules": [
            {
                "type": "field",
                "inboundTag": [
                    "dns-in"
                ].
                "outboundTag": "dns-out"
            }
        ]
    }
}
```

However, there is a problem with this configuration. For DNS queries that are not `Type A` and `Type AAAA`, v2ray will forward directly to the destination DNS server set in `dns-in`. When the domain name is contaminated, the result returned is naturally the contaminated result; if you want v2ray's built-in DNS to act as a `DNSCrypt-Proxy`, this will undoubtedly lead to DNS query content leakage.

There are two solutions:

The AAAA's DNS query traffic is forwarded to the remote end via a proxy and sent outbound via the remote v2ray's `freedom` to `8.8.8.8:53` Return uncontaminated results from the

```
{
    "outbounds": [
        {
            "protocol": "dns".
            "tag": "dns-out",
            "proxySettings": {
                "tag": "remote-proxy-out"
            }
        }
    ]
}
```

Set up other reliable DNS servers in `dns-in`. For example, using only v2ray built-in DNS to achieve DNS triage.

The `dnscrypt-proxy` is used to resolve the data.

If the demand for `non-Type A` and `Type AAAA` DNS queries is low, the above improvements can be ignored.

DNS over HTTPS

V2Ray 4.22.0 is a new feature, and there is no special configuration, except that the DNS address in the above configuration is written as a DOH service address. In ~~general, only~~ `https+local` ~~mode is~~ used on ~~the server side, but there seems to be no stable~~ DOH provider within the ~~wall, only~~ `1.1.1.1` is ~~available, and the result is not stable~~. https://223.5.5.5/dns-query.

```
{                                                                    "
 "dns": {                                                            l
   "servers": [                                                      o
     "https+local://1.1.1.1/dns-query",                              c
                                                                     a
```

```
        lhost"
      }
    }
```

json

Note that the tls certificate of DOH of most service providers does not issue authentication for IP address, and the actual domain name must be written, but there are also

Some DoH providers can be accessed directly using IP as the host name, such as CloudFlare's `1.1.1.1` and Arium Cloud Public

The DNS is `223.5.5.5`.

DOH incorporates DNS requests into regular https traffic, so that the outgoing ISP does not know the domain name you are accessing by using DOH. However, it should be noted that only when both the client and server use DOH protocol (https mode on the client side and https+local mode on the server side), traditional UDP DNS requests will not appear on the VPS outlet.

The resolution time of DOH is much higher than traditional UDP, you can see the specific domain name resolution time by setting the log level of V2Ray to info.

```
2019/11/28 17:34:55 [Info] v2ray.com/core/app/dns: UDP:1.1.1.1:53 got answere: w
...
2019/11/28 17:42:50 [Info] v2ray.com/core/app/dns: DOH:1.1.1.1:443 got answere.
```

The following are reference values for parsing time consumption:

- US VPS UDP 1.1.1.1: 1ms~5ms
- US VPS DOHL 1.1.1.1: 10ms~100ms
- V2Ray guest and terminal Domestic UDP
- 1.1.1.1: 200ms~1s V2Ray guest and terminal Domestic DOH 1.1.1.1: 200ms~3s

However, in practice, due to problems with the network, DOH may take less time than UDP. I feel that this time consumption is different, but it is a small gap, and I rarely notice it in practice.

You can choose to use it as you wish.

参考阅读 Reference

If you have a need for transparent proxies, I think it's worth a look. If not, feel free to do so.

新 V2Ray White Paper Guide 白话文指南

DNS 答疑 Ans

Q: DOH 是什么 What

A: DOH is short for DNS Over HTTPS, which uses https requests to complete DNS requests.

DOH has gone through several draft versions in its history, and V2ray supports RFC8484.

Q: DOHL 又是什么 What's

A: DOHL is not a standard name, it is just a name within V2ray. V2ray has two modes of DOH operation, DOHL means writing `https+local://1.1.1.1/dns-query` in the configuration, which is sent directly by the program without routing rules; instead of writing `https://1.1.1.1/dns- query` will follow the routing rules.

Q: 都要走 DNSHTTPS，那不是很慢 All of , that's not very slow

A: Yes. While traditional UDP will basically respond at the 10ms level, DOH response times are typically 100ms+. In
DOHL mode benefits from the long distance links of http2, and can also respond for several dozen ms. However, personally, these ms-level delays are not perceptible.

Q: DOH 是 HTTPS 可以防污染，传统 DNS 我代理也不爱污染，两者有区别吗 is there can be anti-pollution, traditional the crown agents are

A: There is no difference in effect. The main purpose of DOH is to solve the privacy problem, not some great black and white technology.

Q: The DNS 的 configuration of V2ray 配置好像很复杂 seems to be very complicated

A: There are two main uses of V2ray's DNS, and it is easy to confuse the public:

- One is at the outbound point of the outbound freedom protocol, just like a normal proxy server, where the proxy requests end up, which can be called "endpoint DNS";
- Before matching routing rules, the domain name requested by the terminal needs to be

resolved into an IP, and then the routing rules are matched according to the IP, which can be called "matching DNS".

Instead, "matching DNS" is handled by the built-in DNS. "Matching DNS is not essential to the entire proxy process, and is not even used when routing's "domainStrategy":AsIs are used; even in other modes, it only affects efficiency: if the built-in DNS is not configured correctly, each request will ask for an incorrect "matching DNS" until it times out before being forwarded. Even in other modes, this only affects efficiency: if the built-in DNS configuration is incorrect, each request will ask for an incorrect "match DNS" until it times out and is forwarded, but the data is normal throughout the forwarding process.

问：里面还有 "domians" in the DNS..." expectIPs"

Q: There are also

A: After understanding the two major functions of "terminating DNS" and "matching DNS", you can select these parameters according to the file as needed.

问：压根没写 DNS 配置，好像也是正常的

Q: not write the DNS configuration, it seems to be normal

A: If you do not write a dns configuration, a `"localhost"` configuration will be defaulted as a built-in proxy. On the guest side, the built-in DNS only serves to "match DNS", and even if the local DNS returns a polluted result, it often does not affect the flow of the v2ray crown proxy. The program, so "also normal".

问：文档推荐在服务器侧使用 DOHL on the server side and DOHL on the in 在墙内客户端侧使用 Mat 可以吗

Q: It is recommended to use

is it

wall client side.

A: You can use some of the service providers available in your country, such as `https+local://1.1.1.1/dns-query`.

`https+local://dns.rubyfish.cn/dns-query` , `https+local://dns.alidns.com/dns-query` . However, if these services are not available within the country, you will have to either go into DOH mode or create your own DOH service.

It is not too complicated to build DOH, and V2ray can also use non-standard ports and custom paths, or even "hide" behind an individual site (similar to the tls+ws+web model). These are some of the ways to explore.

Q: V2ray as DNS 服务端时是什么模式

A: V2ray can provide DNS service responses through dokodemo's inbound, using the built-in DNS service configuration. This process is ultimately sent as UDP to the outgoing external DNS request, and is not part of the "terminating DNS" and "matching DNS" process described above.

Q: In the use of transparent proxies, how the work

Some of them use V2ray as a DNS server and are subject to the built-in service.

The caching and matching impact of the server.

更新历史

- 2019-12-30 QA.
- 2019-11-28 First edition.
- 2019-11-29 Add description.
- 2017-12-05 Merged with ToutyRater original content

Edit this page on GitHub

Last update: 5/30/2020, 12:38:24 AM

← HTTP

Japanese language files →