**中神通大地云控——多WAN路由解析功能介绍**

在线文档： http://www.trustcomputing.com.cn/bbs/viewthread.php?tid=2125

Word文档：https://www.trustcomputing.com.cn/help/zst\_mwan\_route\_dns.docx

## 客户需求

客户自建国际网（或其它单独路由、计费的专网专线）出口通道，再把之前的互联网出口通道改成国内网出口通道，要求局域网内无线、有线终端不受干扰，不修改终端OS已有的网络配置，也不另外安装任何软件/APP/插件/配置文件，达到国内网、国际网智能无感分流的目的，并且要保证直去直回，不绕路。

## 二、解决方案



**图1 多WAN路由解析示意图**

**1.1 出网流程**

将客户需求简化为以下两种出网流程：

1、国内流量出网流程

① 用户访问 www.baidu.com
② 网关拦截DNS查询流量并重定向到网关自身DNS服务器

③ 网关DNS服务器查询域名所属集合，决定使用国内DNS服务器114.114.114.114进行解析

④ 网关OS查询114.114.114.114所属IP集合，决定路由至国内网关出口

⑤ 得到DNS解析，是国内IP 153.3.238.127，并继续访问

⑥ 网关OS查询153.3.238.127所属IP集合，决定使用国内网关出口进行路由

2、国际流量出网流程

① 用户访问 ai.com
② 网关拦截DNS查询流量并重定向到网关自身DNS服务器

③ 网关DNS服务器查询域名所属集合，决定使用国际DNS服务器8.8.8.8进行解析

④ 网关OS查询8.8.8.8所属IP集合，决定路由至国际网关出口

⑤ 得到DNS解析，是国际IP 104.21.96.1，并继续访问

⑥ 网关OS查询104.21.96.1所属IP集合，决定使用国际网关出口进行路由

**1.2解决方案**

架设一台中神通大地云控TrustGate硬件网关，或者在硬件、虚拟化平台、云主机上安装一套中神通大地云控系统，硬件设备/母机的多个网卡分别连接局域网交换机、国内网光猫、国际网路由器、管理员PC等，再按照以下步骤进行设置：

1、自定义DNS策略

 国际域名集（GLOBAL）交由8.8.8.8解析，中国域名集（CHINA）交由114.114.114.114解析（可选），其它域名交由114.114.114.114解析，如图2所示。



**图2 自定义DNS策略**

2、DNAT端口映射

在网关局域网网卡处做DNAT端口映射，将去往任意地址UDP 53端口的流量映射到本机的53端口，即本机的DNS服务器处，如图3所示。这样可以保证在不修改客户端网络设置的前提下，仍然可以将本机DNS解析设置应用到客户端的DNS解析中。



**图3 DNAT端口映射**

3、静态路由

 默认网关是两个出口网卡（eth0,eth1），国际IP集（US\_ipv4）的出口网关指向国际网路由器IP（192.168.100.1, eth0），其它流量的出口网关指向国内网光猫IP（192.168.100.254, eth1），如图4所示。



**图4 静态路由**

4、NAT策略

 分别在默认网关的成员网卡处（eth0、eth1）对所有流量做来源NAT，转换后的地址是该网卡的IP，如图5所示。



**图5 NAT策略**

## 三、方案说明

**3.1 关键功能介绍**

中神通大地云控系统（以下简称“大地云控”）的DNS服务器和静态路由功能都具备处理大规模数据集的能力，均为网关级应用，可以用于多WAN、多VPN、SD-WAN接入时的路由解析分流，具体来说是以下四个功能：

1、基于大规模分区IP地址集的分区智能权威DNS解析服务

为来自电信、联通、移动、铁通、教育、外网的用户分别设置其所在区域的权威域名解析服务，例如：同一个域名，国内用户得到服务器的国内IP，国外用户得到服务器的国外IP，再配合多WAN接入以及基于大规模分区IP地址集的智能无感分流路由功能，使得客户端访问网站等服务时不绕路（入网方向）。

2、基于大规模分区域名集的智能递归DNS解析服务

为各个域名集提供其所在区域的递归转发域名解析服务，例如：国内域名用114.114.114.114解析，国外域名用8.8.8.8解析，再配合多WAN接入以及基于大规模分区IP地址集的智能无感分流路由功能，使得客户端访问网站等服务时不绕路（出网方向）。

3、基于大规模分区IP地址集的智能无感分流路由功能

在多WAN、多VPN、SDWAN接入时，提供智能无感分流，用于客户端出网或服务器接入：

1）当客户端出网时，实现国内IP走国内网关、国外IP走国外网关，还需要配合基于大规模分区域名集的智能递归DNS解析服务，实现国内网站、国外网站分流访问

2）当接入服务器时，需要配合基于大规模分区IP地址集的智能分区权威域名解析功能，实现电信、联通、移动、铁通、教育、外网用户访问最近的服务器IP资源

4、大规模域名库和大规模IP库

大规模域名库包括国别库，例如：中国域名库包含“cn”ltd，即所有“.cn”结尾的域名，基本上都是1000~10000条的规模。

大规模IP库包括国别库和中国运营商库，分为IPv4和IPv6两种，都是从权威机构的数据库中提取出来的，基本上都是100~10000条的规模。

另外还有取反IP库，例如：

1）NOT\_CHINA\_ipv4 就是CHINA\_ipv4库的取反，即所有不是CHINA\_ipv4库的IP。

2）ALL\_OTHER\_ipv4是保底库，用于最后一条路由规则，匹配所有不是之前库的IP。

**3.2传统多WAN接入方案的缺点**

传统多WAN接入是将多个出口IP一起作为默认路由，如图6所示，实际运行时，网关只能起到负载均衡的作用，无法区别对待国内、国际域名和IP，无法保证不绕路，无法达到客户的要求。

****

**图6 传统多WAN接入路由**

另外，传统出口方案还有使用TCP代理、旁路由的技术，其缺点是需要在各个客户端OS里安装、更新代理软件/APP/浏览器插件/PAC、json配置文件，无法做到无感分流，同时存在认证数据非授权异地使用、敏感信息泄露的风险，而且TCP层（第四层）代理原理上比纯路由（第三层）的方案低效且耗费资源。

## 四、总结

**大地云控系统 + 多WAN + 客户端 = 智能无感分流出网路由系统
大地云控系统 + 多WAN + 服务器 = 智能无感分流应用发布系统**

“智能路由 + IP集”实现国内IP、国外IP（或国内各大ISP）走不同的出口网关，“智能DNS + 域名集”解决国内域名、国外域名分别按照各自地域的DNS服务器（114.114.114.114、8.8.8.8）做解析，双剑合璧、缺一不可，是人工智能+大数据在互联互通、网络优化领域的最新应用。

## 联系方式

武汉中神通信息技术有限公司

联系人：胡先生

手 机：+86-13607188723

QQ号：390226588

QQ群：233482006

官 网：http://www.trustcomputing.com.cn/bbs

微信公众号名称：中神通信息

微信号：utmwall

