某局点通过M9000-V防火墙限制内网只能访问某个网站不生效的经验案例

域间策略/安全域 **叶靖** 2021-01-27 发表

组网及说明

某客户局点购买了一台M9016防火墙作为网络出口设备，现场客户想通过防火墙对网络流量做限制，实现内网用户只能访问部分网站（www.aaa.com）的需求。其中M9016-V的版本为version 7.1.064, Ess 9153P1216。

问题描述

由于www.aaa.com对应的IP地址在不断变化，所以无法针对IP放通策略，只能针对域名放通策略，于是现场在防火墙上配置了DNS服务器，另外在策略中放通了对应的安全策略。

```
#
ip vpn-instance VPN1
#
interface Route-Aggregation1
 description to-waiwang
 ip binding vpn-instance VPN1
#
interface Route-Aggregation2
 description To-neiwang
 ip binding vpn-instance VPN1
#
object-group ip address wangzhan//配置网站域名
 0 network host name www.aaa.com
dns server 114.114.114.114//配置防火墙的DNS服务器地址
object-group ip address DNS
 0 network host address 114.114.114.114
#
security-policy ip
 rule 16 name Local-Untrust-GW-DNS//放通本地到外网的DNS流量
  action pass
  vrf VPN1
  source-zone local
  destination-zone Untrust_GW
  destination-ip DNS

rule 14 name Trust-Untrust-GW//放通内网到外网的DNS流量和访问www.aaa.com的流量
  action pass
  vrf VPN1
  source-zone Trust_GW
  destination-zone Untrust_GW
  destination-ip wangzhan
  destination-ip DNS
```

但是现场测试发现，内网用户无法访问www.aaa.com。

过程分析

通过测试发现，现场内网用户可以ping通DNS服务器114.114.114.114，也可以正常解析www.aaa.com的IP地址；在防火墙上可以ping通DNS服务器114.114.114.114，但是ping www.aaa.com时提示uknown host，无法正常解析出www.aaa.com的IP地址。

我们怀疑是防火墙解析www.aaa.com域名失败，导致访问www.aaa.com的流量无法正常匹配上安全策略，我们测试，将防火墙的地址组配置修改为

```
object-group ip address wangzhan
 0 network host address 1.1.1.1//直接配置为IP地址。
```

这时候我们测试发现，内网终端就可以正常访问www.aaa.com了。通过该测试，我们进一步确认是防火墙本地解析域名失败导致该问题。

那么为什么防火墙本地可以ping通DNS服务器，但是却无法正常解析www.aaa.com的Ip地址呢?
我们注意到，现场设备的内外网端口都是绑定了VPN实例的，在安全策略的配置中也都是正确的添加了VPN实例的相关配置。我们注意到，在防火墙上pingDNS测试时，是带VPN实例来ping测试的，但是防火墙解析域名时，设备本身是不会带VPN实例信息的。我们发现，现场在配置DNS服务器时，未指定DNS服务器，通过查看命令手册发现：

dns server

dns server命令用来配置域名服务器的IPv4地址。
undo dns server命令用来删除域名服务器的IPv4地址。

【命令】

dns server *ip-address* [**vpn-instance** *vpn-instance-name*]

设备指定DNS服务器时可以添加VPN实例后缀。但是现场并没有添加。现场修改DNS配置为
dns server 114.114.114.114 vpn-instance VPN1
之后，测试正常，防火墙本地能正常解析域名，且内网可以正常访问www.aaa.com。

解决方法

在外网口绑定了VPN实例的情况下，我们再配置DNS服务器时，需要注意指定VPN实例信息，如下：
dns server 114.114.114.114 vpn-instance VPN1