某局点F1000-AI配置基于域名的策略不成功的经验案例

域间策略/安全域 **徐玉娟** 2023-04-14 发表

问题描述

防火墙配置dns代理，dns服务器是公网服务器8.8.8.8，配置完成之后终端上查看解析出的地址和防火墙上解析出的地址一样，但是终端无法访问百度网站

过程分析

1，查看配置接口是否加入安全域，放通安全域的情况没有问题

```
ip vpn-instance ceshi1
#
dns proxy enable
dns server 8.8.8.8
dns server 114.114.114.114
dns server 8.8.8.8 vpn-instance ceshi1
 #
object-group ip address baidu域名
  0 network host name www.baidu.com
 #
interface GigabitEthernet1/0/10
  port link-mode route
  ip binding vpn-instance ceshi1
  ip address 10.X.X.X 24
#
interface GigabitEthernet1/0/11
  port link-mode route
  ip binding vpn-instance ceshi1
  ip address 10.X.X.Y 24
 #
security-zone name intra1
  import interface GigabitEthernet1/0/10
 #
security-zone name extra1
  import interface GigabitEthernet1/0/11
 #
rule 118 name ceshi-dns
   action pass
   counting enable
   vrf ceshi1
   source-ip-host 172.16.1.1
   destination-ip baidu域名
 #
rule 117 name local-ceshi1
   action pass
   vrf ceshi1
   source-zone Local
   destination-ip-host 8.8.8.8
   destination-ip-host 114.114.114.114
 #
rule 115 name 阻断所有
   counting enable
   vrf ceshi1
   source-zone intra1
   destination-zone Extra1
```

2，终端解析地址和防火墙上的一致，查看web界面的安全策略匹配情况发现，测试时的流量匹配了rule115的阻断策略，而没有匹配位置靠前的rule118策略

匹配了拒绝所有的rule115，报文示踪提示被策略阻断：

经确认，dns解析带有vpn实例，display dns host也需要加vpn实例，这种场景地址对象组也需绑定vpn实例，才能获取到解析出来的地址。

dns server 8.8.8.8 vpn-instance ceshi1

#

object-group ip address baidu域名

0 network host name www.baidu.com vpn-instance ceshi1

<H3C>dis dns host vpn-instance ceshi1

Type: D: Dynamic S: Static

Total number: 1

No.	Host name	Type	TTL	Query type	IP addresses
1	www.baidu.com	D	56	A	120.X.X.X

[H3C]dis object-group ip host object-group-name baidu域名

object group :baidu域名

Object ID : 0

Host name :www.baidu.com

VPN instance : ceshi1

Updated at : 2023-03-28 14:33:38

IP addresses : 120.X.X.X