防火墙基于域名的安全策略无法匹配

域间策略/安全域 **彭钦** 2023-03-29 发表

组网及说明

无

告警信息

无

问题描述

现场配置了基于域名的安全策略，但是无法匹配策略。

过程分析

详细分析见下：

（1）基本配置：

```
dns server 8.8.8.8 vpn-instance wai

object-group ip address xxx
0 network host name ai.yyyyyy.com vpn-instance wai

interface GigabitEthernet1/0/9
 port link-mode route
 ip binding vpn-instance wai
 ip address 10.1.1.1 255.255.255.0
```

（2）查看域名解析情况，发现可正常解析：

```
RBM_P<H3C>dis dns host  vpn-instance  wai
Type:
  D: Dynamic    S: Static

Total number: 1
No.  Host name                Type  TTL        Query type  IP addresses
1    iai.tencentcloudapi.com D     56         A           120.x.x.x
                                                          49.x.x.x
                                                          120.y.y.y
```

（3）查看地址对象组获取地址情况，发现无法获取到地址：

```
RBM_P[H3C]dis object-group  ip host  object-group-name   xxx
object group : xxx
  Object ID        : 0
    Host name      : ai.yyyyyy.com
    VPN instance   :
    Updated at     : 2023-03-28 14:33:38
    IP addresses   :
```

解决方法

出口带vpn实例，dns server也带vpn实例，设备dns解析带vpn实例，地址对象组若要从其中获取地址，相应域名也需带vpn实例。

object-group ip address xxx

0 network host name ai.yyyyyy.com vpn-instance wai

```
RBM_P[H3C]dis object-group  ip host  object-group-name   xxx
object group : xxx
  Object ID         : 0
    Host name       : ai.yyyyyy.com
    VPN instance    : wai
    Updated at      : 2023-03-28 14:40:38
    IP addresses    :
      49.x.x.x
      120.x.x.x
      120.y.y.y
```