# 利用dns snooping功能实现基于域名的安全策略V2.0

域间策略/安全域 孔凡安 2024-02-24 发表

## 组网及说明

DNS Snooping功能适用于基于域名做策略的场景（如安全策略、带宽策略等）。设备使用基于域名的策略过滤用户流量时，需要获取域名对应的IP地址才能真正实现流量过滤。开启DNS Snooping功能后，设备会监听过路的DNS请求报文和DNS应答报文，如果DNS请求报文中的域名与策略中的域名相同，设备会在收到该域名的响应报文时记录域名解析结果，并上报给策略，使得策略可以基于此域名对应的IP地址实现流量过滤。如果DNS请求报文中的域名与过滤规则中的域名不同，设备不会记录域名解析结果。

## 告警信息

不涉及

## 问题描述

现网中遇到一些客户利用dns snooping功能实现基于域名做安全策略过滤的场景，实际使用过程中可能遇到一些问题。

针对dns snooping使用过程中遇到的问题总结并说明如下。

V1.0版本可见链接：https://zhiliao.h3c.com/theme/details/214164

其余基于域名的安全策略功能的实现可以参考本人其他案例，关键词“域名”

## 过程分析

Q1: 实现基于域名的安全策略需要下发的配置能有哪些?

A1:安全策略放通dns解析流量；配置域名对象组；安全策略调用该域名对象组；开启dns snooping功能。示例如下：

```
#
 dns snooping enable
#
object-group ip address dns_snooping
 0 network host name dysmsapi.aliyuncs.com
#
#
security-policy ip
 rule 0 name dns
  action pass
  service dns-udp
 rule 1 name dns_snooping
  action pass
  destination-ip dns_snooping
#
```

Q2：如何查看FW记录的解析结果

A2：参考命令如下：

```
#
RBM_P<FW_01>disp object-group ip host object-group-name dns_snooping    ---显示主机名对应IP地址的相关信息
object group : dns_snooping
  Object ID       : 0
    Host name     : dysmsapi.aliyuncs.com
    VPN instance  : -
    Updated at    : 2024-02-23 18:40:16
    IP addresses  :
      106.11.45.35
      106.11.211.236       ---域名对应的IP，该表项存在则安全策略生效
#
RBM_P[FW_01-probe]disp system internal dns snooping host  ---显示DNS Snooping记录的域名解析信息，该表项的老化时间由dns回应报文的老化时间决定
```

```
Total number: 1
No.  Host name                Server                TTL          QType
IP addresses
1    dysmsapi.aliyuncs.com    114.114.114.114       104          A
106.11.45.35
#
RBM_P[FW_01-probe]disp system internal dns kernel snooping-rule host   ---显示内核中DNS Snooping监听域名解析结果的规则，查看配置是否生效
Slot: 1
Type:
 D: Domain    S: Subdomain

No.   VPN instance          Domain/Subdomain      Rule-type QTYPE IgnoreVpn
1                           dysmsapi.aliyuncs.com D         A     N
```

实际使用中，前两条命令经常会用到，以对比终端dns解析结果和FW上记录表项是否一致。

Q3：域名老化时间很短，终端访问过程中没有触发FW dns snooping记录表项并上报策略，导致终端访问时断时续，如何解决?
A3：配置对象组主机名对应IP地址的老化时间，对应命令：**object-group dns-aging。**设置一个合适的时间即可。

**object-group dns-aging**命令用来开启主机名对应IP地址的老化功能。

**undo object-group dns-aging**命令用来关闭主机名对应IP地址的老化功能。

【命令】

**object-group dns-aging** [ **time** *aging-time* ]

**undo object-group dns-aging**

【缺省情况】

主机名对应IP地址的老化功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

**time** *aging-time*：主机名对应IP地址的老化时间，取值范围为1～70000000，单位为分钟，缺省值为120。

【使用指导】

非缺省vSystem不支持本命令。

在同一主机名对应多个IP地址的负载均衡场景中，DNS解析主机名获得的IP地址会在多个IP地址之间进行不断切换。缺省情况下，每次切换，对象组模块都会通告相关策略（如安全策略）变更IP地址，会造成相关策略频繁提交加速，大量耗费设备内存，此时可通过开启主机名对应IP地址的老化功能解决此问题。

开启该功能后，对象组针对每个主机名维护一个IP地址组。当通过DNS解析该主机名获得的IP地址不在该组内，会将新的IP地址添加至组内，并将该组新的IP地址范围告知相关策略；当获得的IP地址在该组内，则不会告知相关策略，并更新该IP地址的老化时间。若组内某个IP地址达到老化时间，则会将其从组内删除，并告知相关策略。从而减少相关策略加速次数，降低设备内存占用。

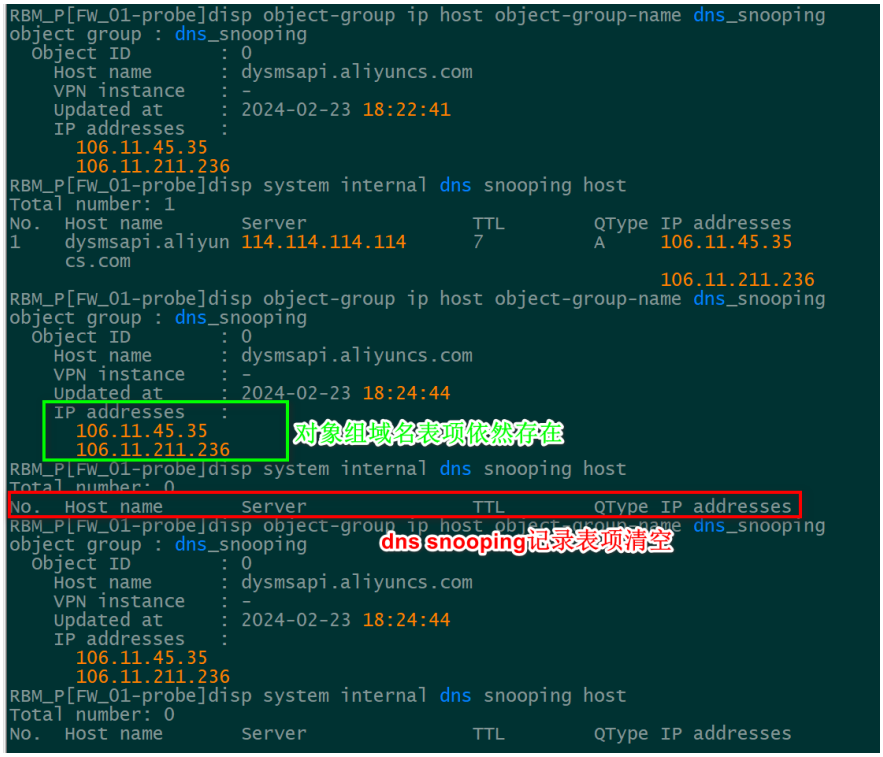
建议所配置主机名对应IP地址的老化时间大于DNS服务器上配置的解析记录生存时间（TTL）。

【举例】

# 配置主机名对应IP地址的老化时间为5分钟。

```
<Sysname> system-view
[Sysname] object-group dns-aging
[Sysname] object-group dns-aging time 5
```

Q4：配置了**object-group dns-aging**命令之后，域名老化时间按照哪个解析结果来算?
A4：以disp object-group ip host object-group-name xxx的解析结果为准。
测试条件如下：域名的老化时间2分钟，设置域名对象组老化时间为30min。2min后查看结果：




## 解决方法

DNS Snooping功能处于不断优化的过程，现网使用过程中建议使用最新版本。

以上。