# 关于M9000-S系列防火墙虚墙抓包的经验案例

其他 叶靖 2022-05-31 发表

## 组网及说明

某客户局点购买了一台我司的M9012-S防火墙设备作为出口设备，对网络进行安全防护。防火墙的版本为R9724P3003。

## 问题描述

现场客户在防火墙上配置了虚墙服务，现在客户有需求，需要在虚墙上进行抓包。

## 过程分析

由于M9000系列防火墙设备在D032新分支版本后，web页面需要实现抓包，需要先将流量镜像到blade板卡。另外由于现场配置了虚墙服务，想在虚墙上进行抓包，需要先在防火墙的根墙中配置镜像，将流量镜像到blade板卡，然后再登录虚墙的web页面，通过“报文捕获功能”进行抓包。

具体配置如下：

(1)登录到根墙，即缺省Context

(2)配置流镜像功能

# 配置IPv4高级ACL 3001，匹配抓包对应的报文，如匹配源地址为10.1.1.0/24网段的用户。

```
<Device> system-view
[Device] acl advanced 3001
[Device-acl-ipv4-adv-3001] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 20.1.1.0 0.0.0.255
 [Device-acl-ipv4-adv-3001] quit
```

# 创建流分类abc，并配置报文匹配规则为ACL 3001。

```
[Device] traffic classifier abc
[Device-classifier-abc] if-match acl 3001
[Device-classifier-abc] quit
```

# 创建流行为abc，并配置流镜像到Context所进驻安全引擎组的主安全引擎上（本举例假设此主安全引擎的Blade接口为Blade 4/0/1。

```
[Device] traffic behavior abc
[Device-behavior-abc] mirror-to interface blade 4/0/1
[Device-behavior-abc] quit
```

# 创建QoS策略abc，在策略中为流分类abc指定采用流行为abc。

```
[Device] qos policy abc
[Device-qospolicy-abc] classifier abc behavior abc
[Device-qospolicy-abc] quit
```

# 将QoS策略abc应用到抓包流量对应的接口，如接口GigabitEthernet1/0/1的inbound和outbound方向上，且必须开启enhancement功能。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy abc inbound enhancement
[Device-GigabitEthernet1/0/1] qos apply policy abc outbound enhancement
[Device-GigabitEthernet1/0/1] quit
```

(3)登录到虚墙即非缺省context的web管理页面上

（4）在web页面上 系统—诊断中心—报文捕获 菜单中进行抓包，注意上面的提示“* 此功能必须与流镜像功能配合使用才能捕获报文。”调用与之前流镜像相同的ACL3001进行抓包即可。

## 解决方法

针对M9000-S系列防火墙，如果有虚墙抓包的需求，需要先在根墙配置流镜像，将流量镜像到blade板卡，然后登陆到虚墙web进行抓包。