

知 SR6608 设备端口流量处理方式是先过滤还是先镜像

firewall packe 镜像 朱新建 2021-09-10 发表

组网及说明

(G(G0/0/2)SR6602X(G0/0/0, 6.6.6.6)-----6.6.6.5)MSR56

问题描述

不涉及

过程分析

66接口配置如下，调用3000的包过滤在inbound方向

```
interface GigabitEthernet0/0/0
firewall packet-filter 3001 inbound
ip address 6.6.6.6 255.255.255.0
mirroring-group 1 mirroring-port inbound
#
acl number 3001 name forrekey
rule 0 deny ip
```

在msr56上ping66对接地址

```
[MSR5660-2] ping -c 100000 -m 10 -t 10 -s 8100 6.6.6.6
Ping 6.6.6.6 (6.6.6.6): 8100 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
```

66上镜像组配置inbound方向

```
[SR6602X-1]dis mirroring-group all
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet0/0/0 inbound
  monitor port: GigabitEthernet0/0/3
```

```
[SR6602X-1]dis int g 0/0/0
```

```
Last 5 seconds input rate 396793.62 bytes/sec, 3174344 bits/sec, 285.60 packets/sec
Last 5 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
```

```
[SR6602X-1]dis int g 0/0/3
```

```
Last 5 seconds input rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Last 5 seconds output rate 397178.00 bytes/sec, 3177424 bits/sec, 286.19 packets/sec
```

测试接口入方向被packet filter deny的流量能被镜像出来，接口inbound方向先进行镜像，后包过滤

在66接口配置出方向的镜像

```
[SR6602X-1]dis mirroring-group all
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet0/0/0 outbound
  monitor port: GigabitEthernet0/0/3
```

接口配置如下调用3000的包过滤

```
interface GigabitEthernet0/0/0
firewall packet-filter 3001 outbound
ip address 6.6.6.6 255.255.255.0
mirroring-group 1 mirroring-port outbound
#
```

```
[SR6602X-1]dis int g 0/0/0
```

```
Last 5 seconds input rate 398460.78 bytes/sec, 3187680 bits/sec, 286.79 packets/sec
Last 5 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
```

```
[SR6602X-1]dis int g 0/0/3
```

```
Last 5 seconds input rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
Last 5 seconds output rate 319.59 bytes/sec, 2552 bits/sec, 0.39 packets/sec
```

接口出方向被packet filter deny的流量不能被镜像出来，出方向先包过滤后镜像

解决方法

接口入方向被packet filter deny的流量能被镜像出来，接口出方向被packet filter deny的流量不能被镜像出来

