**信而泰BGP Flow Spec防攻击测试解决方案**

随着互联网行业的迅猛发展，越来越多的业务都从线下走到了线上。互联网在给大家生活带来便利的同时也面临着防护自身安全的各种挑战。DoS/DDoS攻击是对网络安全的重大威胁，攻击者通过多个控制端控制成千上万的攻击设备对同一个目的地址、网段或服务器同时发起流量攻击，导致网络拥塞或服务器CPU占用过高无法提供服务。现在的路由器除了具备流量转发的功能外，还可以通过BGP Flow Specification对流量进行分类、限速、过滤和重定向等操作，这对防御DoS/DDoS攻击非常重要。目前，Renix软件平台支持BGP Flow Spec的相关功能测试。本文的主要内容也是说明Renix对于BGP Flow Spec测试的支持度以及相关测试操作举例。

# BGP Flow Specification介绍

先简单介绍一下什么是BGP Flow Specification。BGP Flow Specification（简称BGP Flow Spec）是一种用于防止DoS（Denial of Service）/DDoS（Distributed Denial of Service）攻击的方法，可以提高网络安全性和可用性。传统预防DoS/DDoS攻击的方法有两种，分别是流分类技术和对攻击流量重定向，但是这两种方法都存在缺陷，如表1所示。

表1传统预防DoS/DDoS攻击方法的比较

|  |  |  |
| --- | --- | --- |
| **预防方法** | **方法概述** | **缺点** |
| 流分类技术 | 在设备上手工配置流量匹配规则和相应的QoS策略，用来缓解DoS/DDoS的攻击。 | 该方法存在如下缺点：   * 无法保证防御攻击的实时性，需要在多个网络服务供应商之间进行协调，以标识出攻击源。 * 维护工作难度大，需要手工修改流量过滤策略。 |
| 对攻击流量重定向 | 通过路由策略修改指向受攻击目标的路由的下一跳：   * 将下一跳设置为一个黑洞，将流量丢弃。 * 将下一跳设置到一台流量清洗设备上，对攻击流量进行清洗，保护正常的业务流量。 | 该方法存在如下缺点：   * 流量过滤的匹配条件单一，即只能通过目的IP地址进行过滤。 * 控制流量过滤的信息和转发流量的路由信息混合在一起，增加维护难度。 |

BGP Flow Spec可以解决上述缺点：

* 可维护性好。使用标准协议定义的BGP网络层可达信息类型来传递流量过滤信息，因此路由信息和流量过滤信息独立存在。
* 提供丰富的过滤条件和处理动作，可以更有针对性地实现对流量的控制。

此外，BGP Flow Spec的应用可以大大提高用户网络的安全性与可靠性，具体如下：

* 实时监控：BGP Flow Specification可以以定时采样的方式对攻击流量进行快速响应，实现对攻击流量的控制。
* 预先防护：根据常见的攻击流量的特点，手工部署防护策略，使常见的攻击流量没有机会对用户网络造成危害，防患于未然。
* 降低成本：不需要在每台设备上单独建立流量控制策略，提高可维护性。
* 限制攻击范围：BGP Flow Specification支持跨域传播功能，可以在尽可能靠近攻击源的设备上消除攻击流量对网络的危害，大大降低了攻击流量对网络的影响。

# Renix平台BGP Flow Spec配置介绍

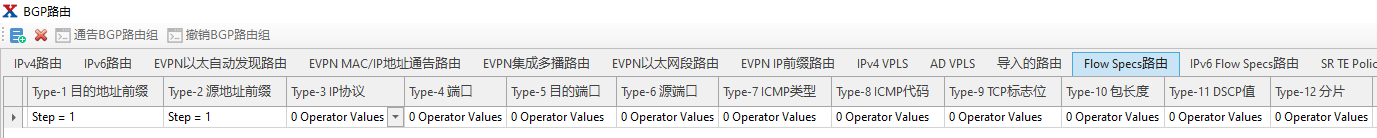
在RFC 5575中定义了解码Flow Spec的标准程序，使BGP路由具备更为丰富的属性并可执行限速、过滤和重定向等行为。接下来介绍Renix对于BGP Flow Spec测试的支持度。

1. 支持IPv4 Flow Spec和IPv6 Flow Spec。





1. IPv4 Flow Spec支持12种匹配规则。

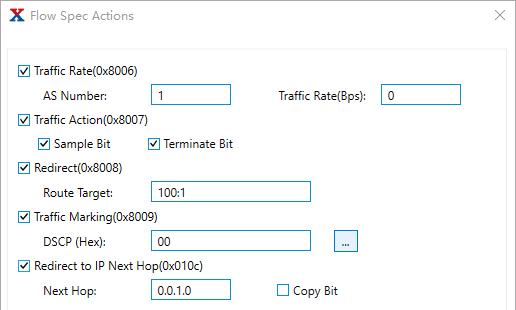


不同Type对应不同的字段，具体匹配规则内容如表2

表2 IPv4 Flow Spec支持的匹配规则

|  |  |  |
| --- | --- | --- |
| **Type类型** | **匹配字段** | **作用** |
| Type-1 | 目的地址前缀 | 指定匹配的目的地址前缀。 |
| Type-2 | 源地址前缀 | 指定匹配的源地址前缀。 |
| Type-3 | IP协议 | 指定匹配的IP协议号。 |
| Type-4 | 端口 | 指定匹配端口。 |
| Type-5 | 目的端口 | 指定匹配的目的端口。 |
| Type-6 | 源端口 | 指定匹配的源端口。 |
| Type-7 | ICMP类型 | 指定匹配的ICMP类型。 |
| Type-8 | ICMP代码 | 指定匹配的ICMP代码。 |
| Type-9 | TCP标志位 | 指定匹配的TCP标志位。 |
| Type-10 | 包长度 | 指定匹配的数据包长度。 |
| Type-11 | DSCP值 | 指定匹配的DSCP值。 |
| Type-12 | DSCP值 | 指定匹配的分片标志。 |

1. IPv4 Flow Spec支持5种路由策略。

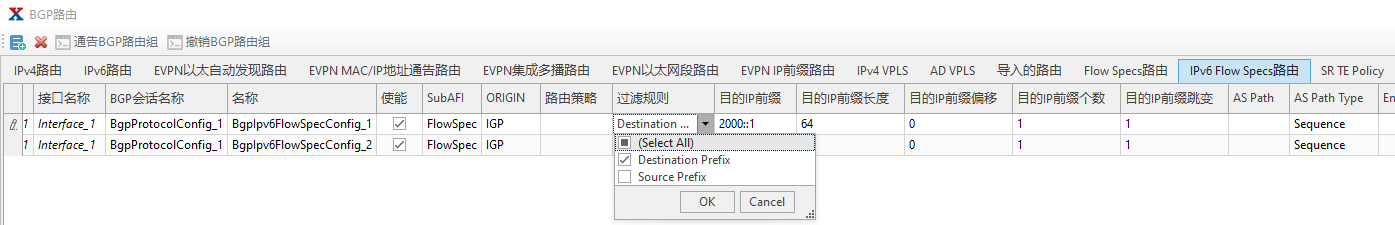


每一种路由策略的具体作用如:3：

表3 IPv4 Flow Spec支持的路由策略

|  |  |
| --- | --- |
| **Type类型** | **作用** |
| Traffic Rate(0x8006) | 流量限速动作。指定AS号和指定流量的最大传输速率。当配置为0时对流量执行丢弃动作。 |
| Traffic Action(0x8007) | 选中Sample Bit时启用流量抽样记录。选中Terminate Bit时撤销已生效的匹配规则。 |
| Redirect(0x8008) | 流量重定向到指定的路由目标动作。 |
| Traffic Marking(0x8009) | 重新标记报文DSCP值的动作。 |
| Redirect to IP Next Hop(0x010c) | 重定向到下一跳动作。选中Copy Bit时，会复制一份规则匹配的流量，并执行重定向到下一跳动作。 |

1. IPv6 Flow Spec支持2种匹配规则。

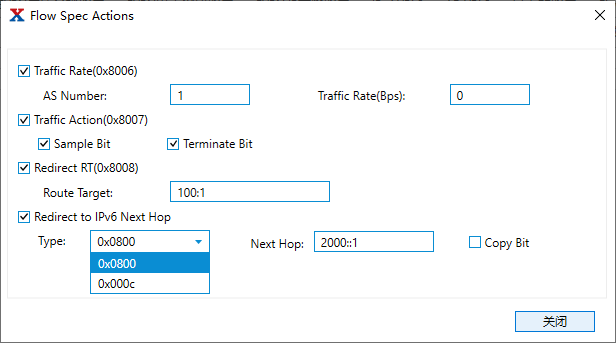


每一种规则具体匹配的内容如表4：

表4 IPv6 Flow Spec支持的匹配规则

|  |  |  |
| --- | --- | --- |
| **Type类型** | **匹配字段** | **作用** |
| Destination Prefix | 目的地址前缀 | 指定匹配的目的地址前缀。 |
| Source Prefix | 源地址前缀 | 指定匹配的源地址前缀。 |

1. IPv6 Flow Spec支持4种路由策略。



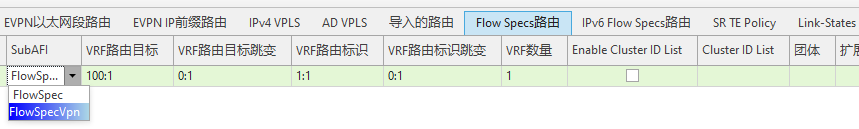
每一种路由策略的具体作用如表5：

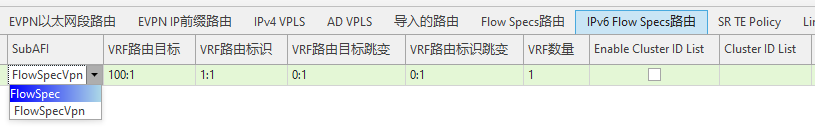
表5 IPv6 Flow Spec支持的路由策略

|  |  |
| --- | --- |
| **Type类型** | **作用** |
| Traffic Rate(0x8006) | 流量限速动作。指定AS号和指定流量的最大传输速率。当配置为0时对流量执行丢弃动作。 |
| Traffic Action(0x8007) | 选中Sample Bit时启用流量抽样记录。选中Terminate Bit时撤销已生效的匹配规则。 |
| Redirect(0x8008) | 流量重定向到指定的路由目标动作。 |
| Redirect to IPv6 Next Hop(0x0800) | 重定向到下一跳动作。选中Copy Bit时，会复制一份规则匹配的流量，并执行重定向到下一跳动作。 |
| Redirect to IPv6 Next Hop(0x000c) | 重定向到下一跳动作。选中Copy Bit时，会复制一份规则匹配的流量，并执行重定向到下一跳动作。 |

1. SubAFI支持配置为FlowSpecVpn。

将SubAFI配置为FlowSpecVpn时，可以配置VRF的相关参数，如指定VRF路由目标、指定VRF路由标识符等配置。





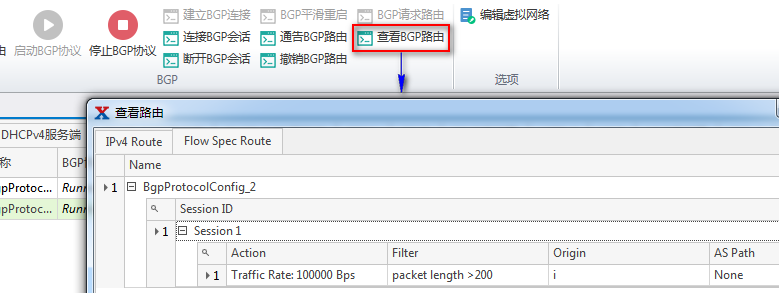
1. 支持配置Multi Exit Discriminator、Local Preference、Cluster ID List等参数。

当使能Multi Exit Discriminator为选中状态时配置MULTI\_EXIT\_DISC属性；当Enable Local preference为选中状态时配置Local\_PREF的值；当仿真路由器作为BGP路由反射器时配置uster ID list的值。



1. 支持查看学到的Flow Spec路由策略和匹配规则。

BGP会话使能查看路由，运行测试，点击查看BGP路由，可以查看学到的Flow Spec路由策略和匹配规则



# BGP Flow Spec测试示例

说完Renix平台BGP Flow Spec的相关配置之后，接下来以BGP Flow Spec防攻击测试为例，演示如何使用Renix平台进行测试。主要是在测试仪A、B端口之间建立正常业务流量和攻击流量，对比设备在使能BGP Flow Spec功能前后流量的收发情况，验证被测设备BGP Flow Spec功能。

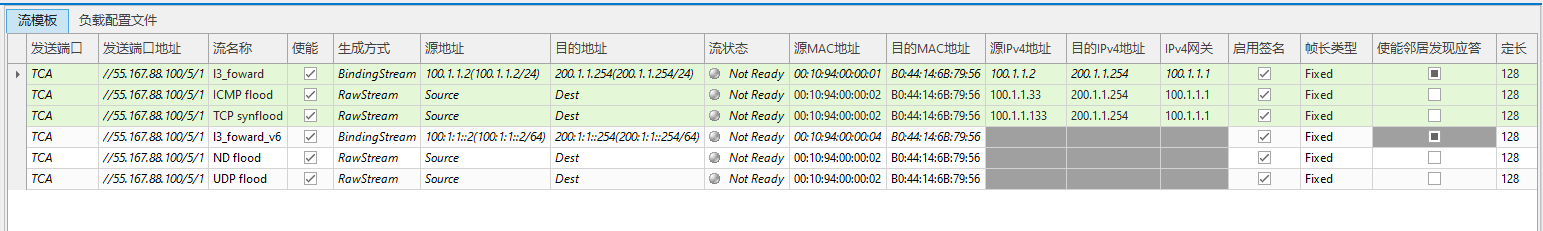
主要步骤如下

1. 按照如下测试拓扑进行组网：

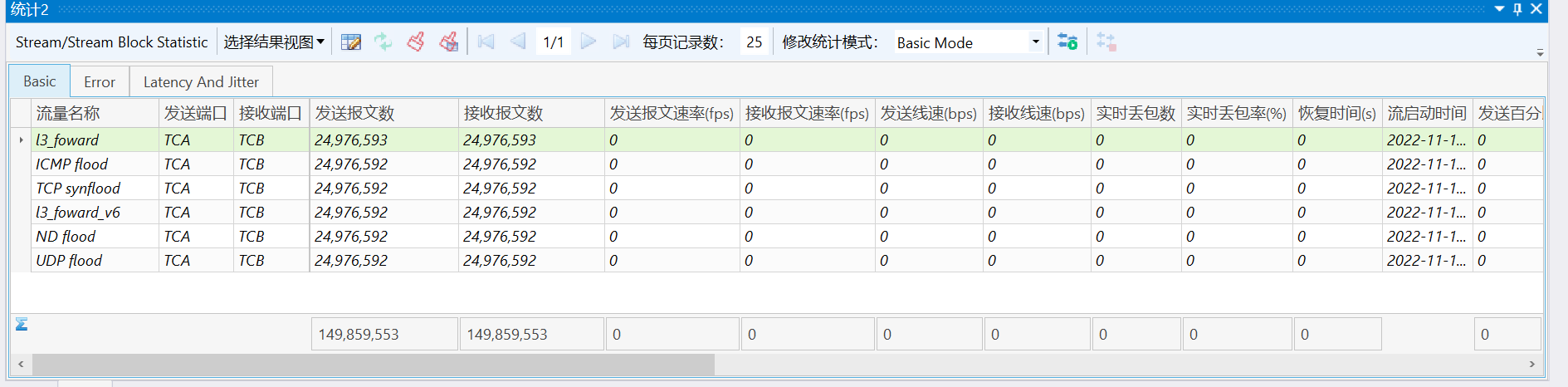
DUT1和DUT2建立双栈IBGP，DUT2为路由反射器，DUT1为客户端



1. 在测试仪表A、B端口之间构造3条IPv4流量：第1条流为正常业务流，源IP为100.1.1.2，目的IP为200.1.1.254（测试仪端口B），目的端口80；第2条流模拟ICMP FLOOD攻击，目的地址为200.1.1.254；第3条流模拟TCP SYNFLOOD攻击，源IP为100.1.1.133, 目的IP为200.1.1.254，目的端口80。

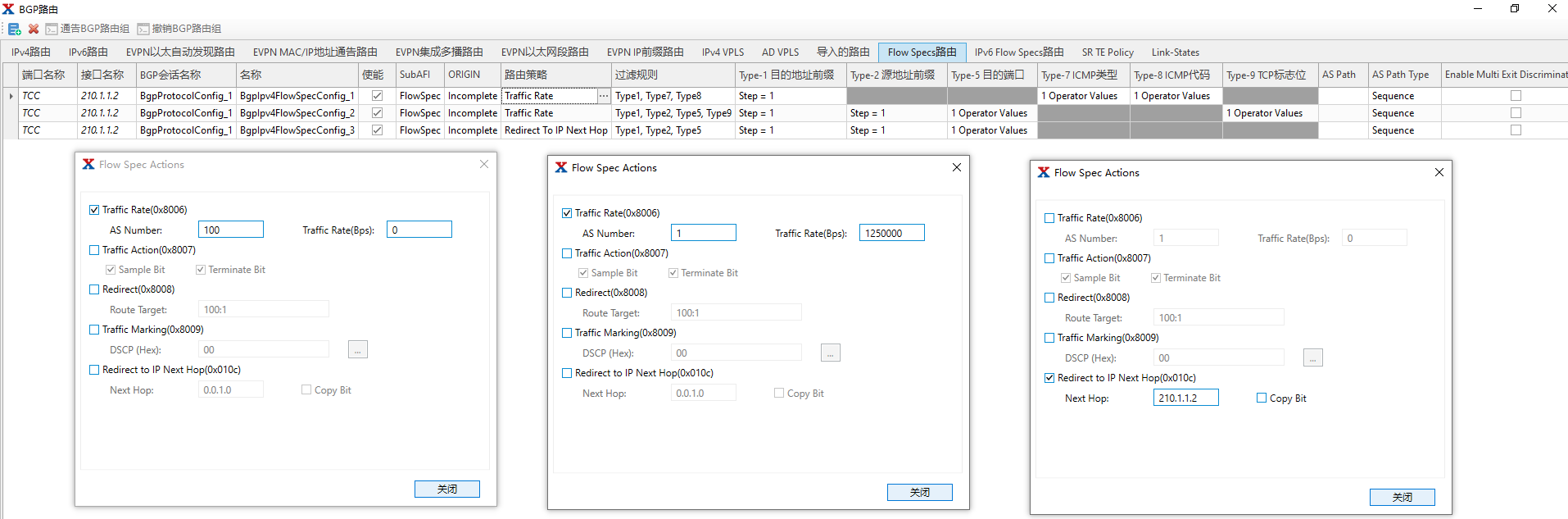


1. 发送所有流量，在测试仪B端口可以正常收到所有流量。

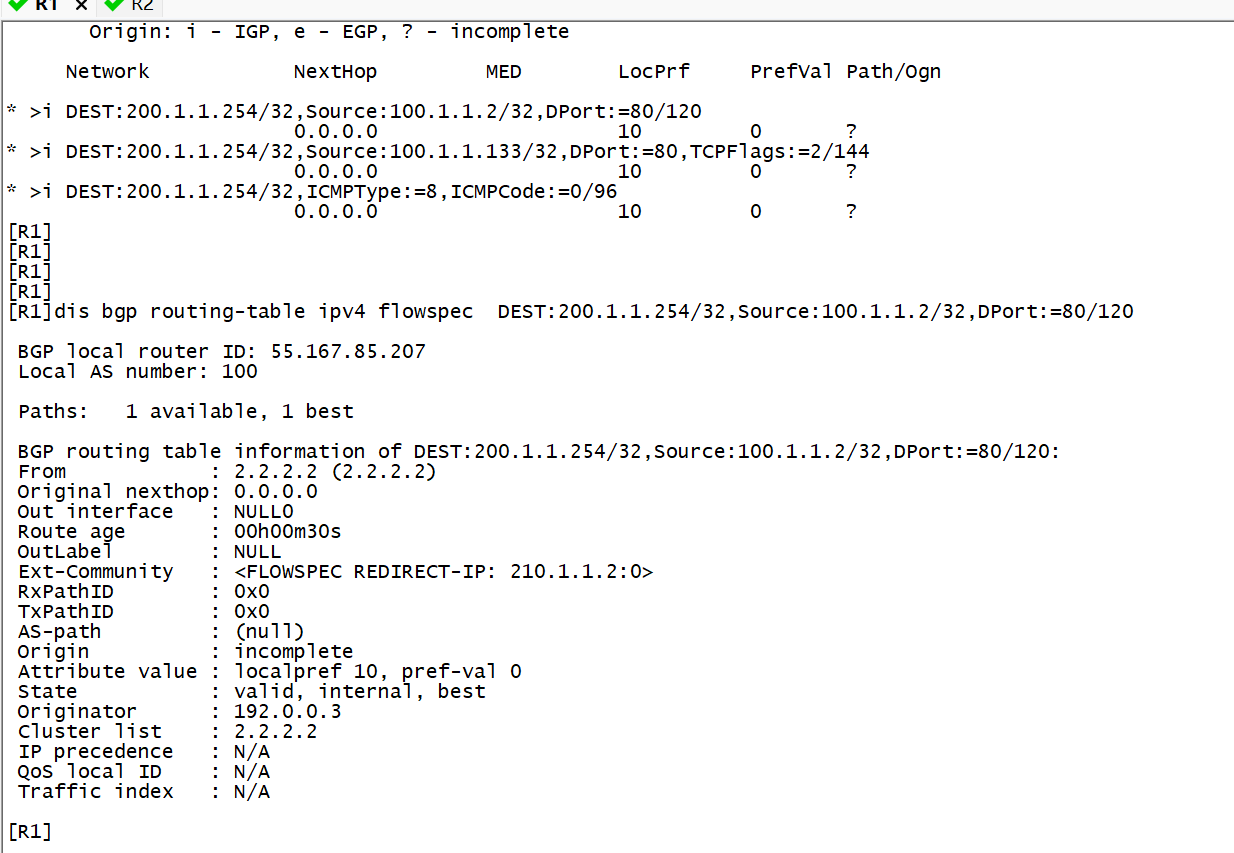


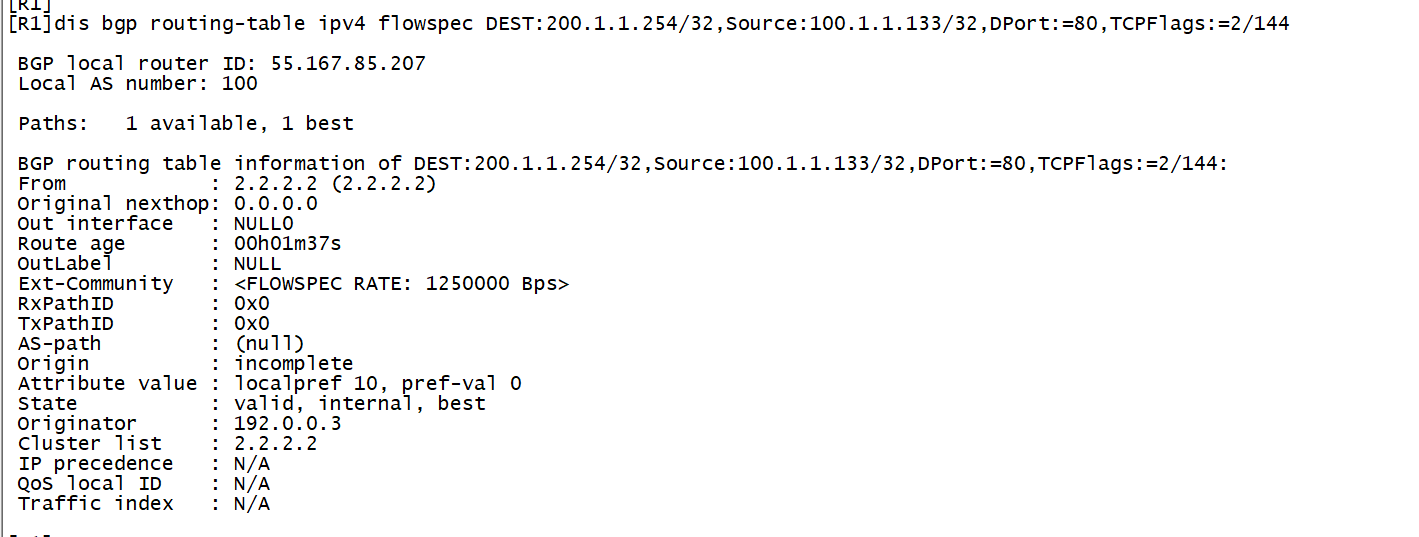
1. 配置DUT1和DUT2使能BGP FLOWSPEC功能。仪表端口C与DUT2建立BGP邻居关系，并通过BGP FLOWSPEC向DUT2配置流量信息，通告DUT1对步骤3中的ICMP/ND FLOOD、TCP SYNFLOOD和UDP FLOOD攻击流量进行过滤。对ICMP/ND FLOOD攻击进行阻断，对TCP/SYNFLOOD和UDP FLOOD攻击限制速度为10Mb/s。

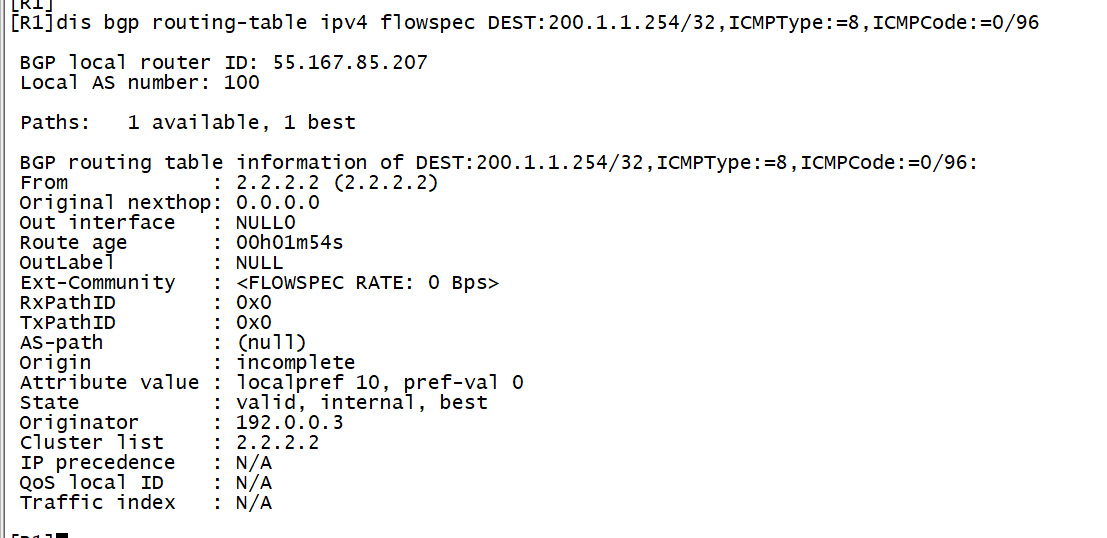
测试仪C端口通告的BGP Flow Spec路由



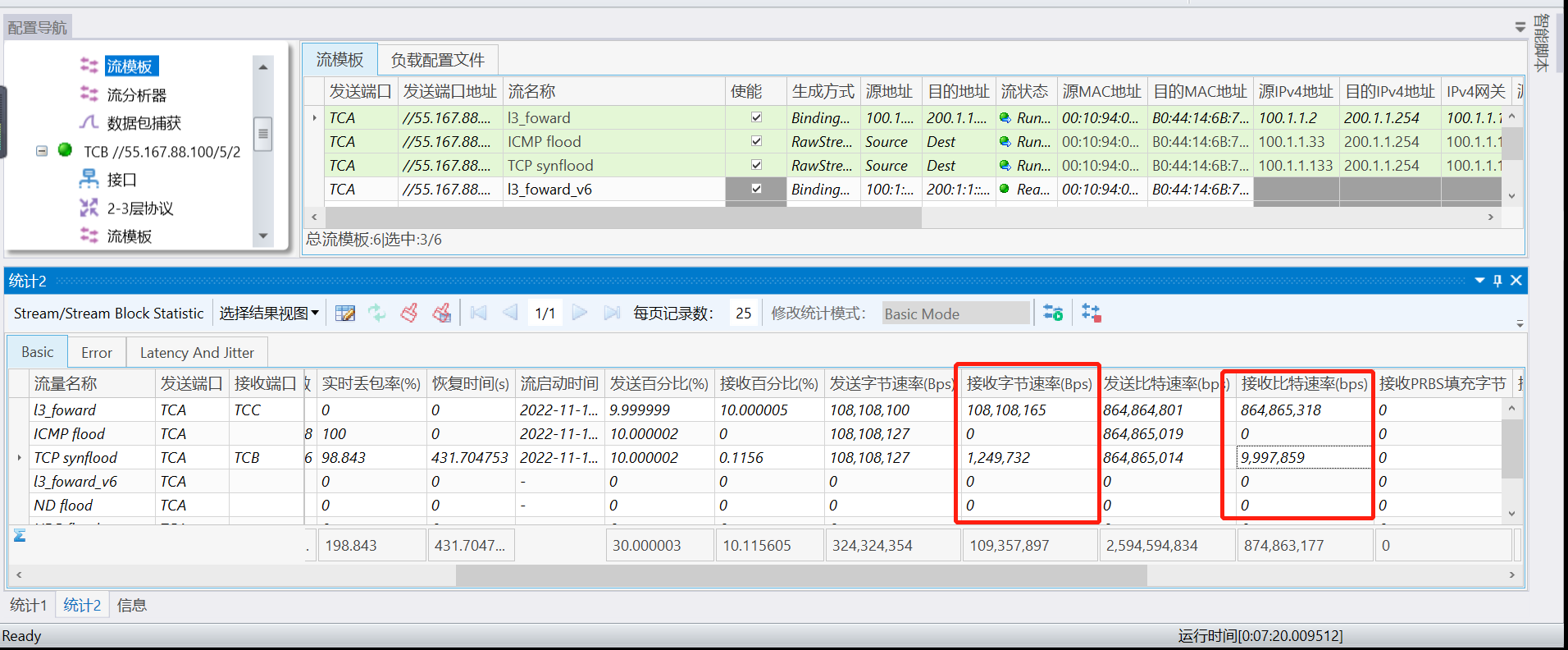
被测设备学习到的IPv4 BGP Flow Spec路由信息

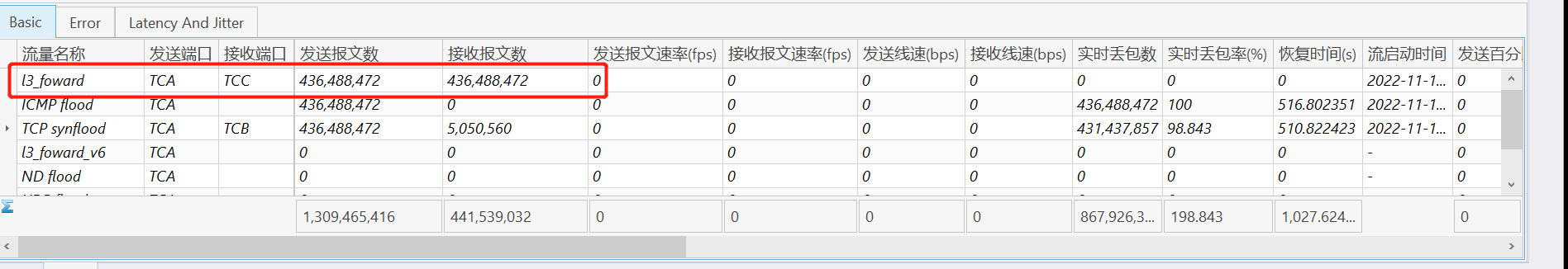






1. 再次发送建立的3条IPv4流量，可以看到IPv4正常业务流量收发一致且能正常重定向到Port TCC，ICMP攻击流量不通，TCP攻击流量限速到10Mb/s且接收端口为Port TCB。





当前，Renix 软件BGP Flow Spec除了支持匹配多个字段、定义对匹配字段执行的操作等基本功能测试外，也具备对该协议的扩展和开发的能力。