

问题描述

【MVS】Citrix NetScaler 负载均衡设备抓包分析方法

解决方法

官网链接说明:

<https://docs.netScaler.com/zh-cn/citrix-adc/current-release/system/troubleshooting-citrix-adc/how-to-record-a-packet-trace-on-citrix-adc.html>

关于Filter Expression的使用方法:

如果需要通过抓包客户端IP为192.168.1.120, 虚服务IP为192.168.1.40, 虚服务端口为8090的报文, 可以使用下面的过滤表达式

```
CONNECTION.SRCIP.EQ(192.168.1.120)&&  
(CONNECTION.DSTIP.EQ(192.168.1.40) && CONNECTION.DSTPORT.EQ(8090))
```

如果需要通过同时抓包负载均衡与后端服务器之间交互的报文, 可以勾选【Trace filtered connection's peer traffic】选项

The screenshot shows the configuration interface for packet capture on a Citrix NetScaler device. The 'Merge' dropdown is set to 'ONSTOP'. Under the 'Trace filtered connection's peer traffic' section, the checkbox is checked and highlighted with a red box. Other options include 'Do Runtime cleanup', 'Skip RPC', and 'Capture Dropped Packets'. The 'Capturing Mode' section includes options for 'Packets buffered for transmission (TXB)', 'Received packets before NIC pipelining (RX)', 'MPTCP master flow (MPTCP)', 'Packets are not captured in flow receiver', 'Citrix Web App Firewall', 'Transmitted packets (TX)', 'Received packets after NIC pipelining (NEW_RX)', 'Translated IPv6 packets', and 'Capture C2C message'. At the bottom, there are 'Start' and 'Close' buttons.