网络流量分类

第1章 绪论

1.1

1.1.1

网络流量集合的定义：

$$S = \{f_i | i : (sip, dip, sport, dport, pro), i \in D\}$$

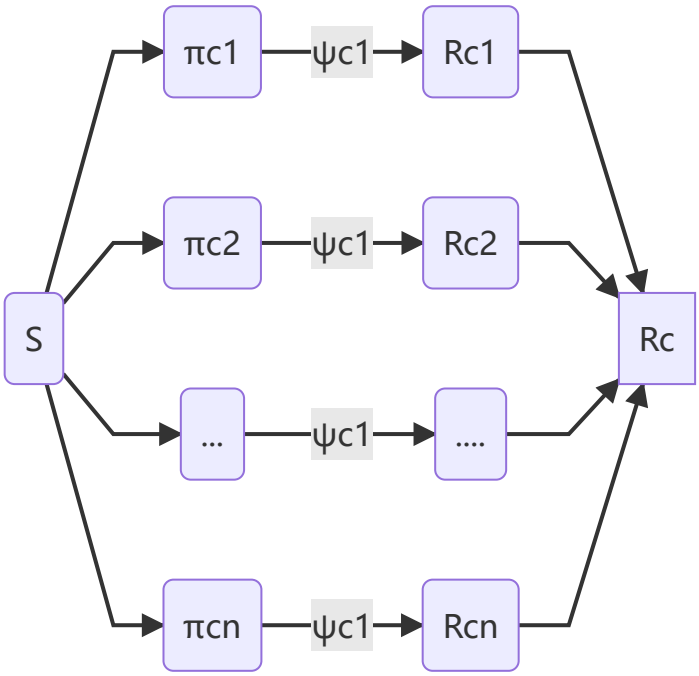
两点重要理解：

- 网络流量集合S是由一条条ip流f_i组成的
- 标志ip流有五个要素，只要这五个要素相同，则ip流相同，属于同一ip流

1.2

1.2.1

- 网络流量集合S，分类结果R_C,分类集簇π_C之间的关系如下;ψc为分类函数，不同的分类集簇不相交，互相独立



- 标志网络流量分类方法的flag主要是分类维度，同一分类维度可以有多种方法

数据粒度	分类方法	设备分类	用户行为	协议分类	服务分类	应用分类	协议加密属性*

数据粒度	分类方法	设备分类	用户行为	协议分类	服务分类	应用分类	协议加密属性*
数据报文(数据报文大小，数据报文到达时间间隔)	特征规则匹配[6]		停留时间	http	音视频	淘宝	SSL/TLS
流层面(ip流的特征)	机器学习[7,8]		跳出率	ftp	即时通信	微信	SSH
会话层面(应用流的特征:sip,dip,应用层协议)	深度学习[9]		回访者	smtp	网络游戏	抖音	IPSec(隧道流量识别)

1.2.2

- 网络流量分类的意义，主要是两方面：网络服务（流控处理和网络处理资源）和网络安全管理

1.3&1.4

明密文分类，协议分类，应用分类，行为分类