**流特征(Flow Features)：**

1. srcip源IP **√**
2. sport源端口号 **√**
3. dstip目的IP **√**
4. dsport目的端口号 **√**
5. **proto**协议 **√**

**基础特征(Base Features)：**

1. state其他协议类型，ACC, CLO, CON, ECO, ECR, FIN, INT, MAS, PAR, REQ, RST, TST, TXD, URH, URN, (-) -----》 需要根据协议proto特征进行判断
2. **dur**连接总持续时间 **√**
3. **sbytes**源端口向目的端口发送的字节数 **√**
4. **dbytes**目的端口向源端口发送的字节数**√**
5. **sttl** 源到目的地的生存时间**√**
6. **dttl** 目的地到源的生存时间**√**
7. sloss 源数据包转发或丢失（个数）
8. dloss 目的数据包转发或丢失（个数）
9. **service** 应用层服务（http, ftp,smtp,ssh,dns,ftp-data,irc, -）**√**
10. **Sload** 每秒发送源字节数（源发出）**√**
11. **Dload** 每秒发送目的字节数（目的发出）**√**
12. **Spkts** 源到目的数据包总数 **√**
13. **Dpkts** 目的到源数据包总数 **√**

**内容特征(Content Feautres)**

1. **Swin** 源TCP窗口大小 **√**
2. **Dwin** 目的TCP窗口大小 **√**
3. **Stcpb** 源TCP队列数 **√**
4. **Dtcpb** 目的TCP队列数 **√**
5. **Smeansz** 源发送的流数据包大小的平均值 **√**
6. **Dmeansz** 目的发送的流数据包大小的平均值 **√**
7. Trans\_depth http请求/响应事务的连接深度
8. **Res\_bdy\_len**从服务器的http服务传输的数据的内容大小。（从服务器传回给源的数据大小之和）**√**

**时间特征(Time Features)**

1. Sjit 源网络抖动(mSec)
2. Djit 目的网络抖动(mSec)
3. Stime 记录开始时间 **√**
4. Ltime 记录结束时间 **√**
5. **Sintpkt** Source inter-packet arrival time(mSec) **√**
6. **Dintpkt** Destination inter-packet arrival time(mSec) **√**
7. **Tcprtt** synack+ackdat的总和 需要防火墙端发来状态信息，比如三次握手中的第几次 **√**
8. **Synack** 在SYN和TCP的SYN ACK数据包之间的时间 **√**
9. **Ackdat** SYN\_ACK和TCP的ACK数据包之间的时间。**√**

**附加生成特征(Additional Generated Features)**

**通用特征**

1. **Is\_sm\_ips\_ports** 如果源IP（1）等于目的IP（3），同时源端口（2）等于目的端口（4），此值为1，否则为0 **√**
2. Ct\_state\_ttl 根据源/目标生存时间（10）（11）的特定值范围，为每个状态（6）分配编号。
3. **Ct\_flw\_http\_mthd** 根据流中具有诸如http服务中的Get和Post之类的方法数进行编号**√**
4. Is\_ftp\_login 如果通过用户和密码访问ftp会话，则返回1，否则返回0。
5. Ct\_ftp\_cmd 根据流在ftp中的指令条数进行编号

**连接特征**

1. Ct\_srv\_src 根据上次（26），在100个连接中包含相同服务（14）和源地址（1）的连接数。进行编号
2. Ct\_srv\_dst 根据上次（26），在100个连接中包含相同服务（14）和目标地址（3）的连接数。进行编号
3. Ct\_dst\_ltm 根据上次（26），在100个连接中具有相同目标地址（3）的连接数。进行编号
4. Ct\_src\_ltm 根据上次（26），在100个连接中具有相同源地址（1）的连接数。进行编号
5. Ct\_src\_dport\_ltm 根据上次（26），在100个连接中具有相同源地址（1）和目标端口（4）的连接数。
6. Ct\_dst\_sport\_ltm 根据上次(26) ，在100个连接中没有相同目的地址(3)和源端口(2)的连接。
7. Ct\_dst\_src\_ltm 根据上次时间（26），在100个连接中，相同源（1）和目标（3）的连接数。