**（1）有状态防火墙需求**

1. 非正常的ACK报文检测（未发送该序列号报文）；
2. 已接受syn报文并回复syn-ack，但未收到ack报文，同时连接超时。
3. 内网可以访问外网，外网不能访问内网。
4. 只允许http 报文通过（web服务器的防护）。（基本事件）
5. 窗口外的报文丢弃。（基本事件）

**（2）需添加的事件**

增添自定义事件：

ABNORMAL\_ACK、ABNORMAL\_SEQ、ABNORMAL\_SYS\_ACK、OUT\_TO\_IN、IN\_TO\_OUT

添加基本事件：HTTP\_PACKET

**（3）模块间接口信息**



①自定义事件信息{parent\_event, filter, arg}

②事件处理函数信息{event,callback}

③配置信息{流过滤表达式，事件过滤表达式}

④配置信息{流过滤表达式，事件过滤表达式}

⑤基本事件信息{event, connection, \*pkt}

⑥状态回写{connection}

**（4）事件管理工作流程**

在事件管理中维护多棵事件生成树，以每个基本事件为树的根节点，有多少个基本事件就有多少棵事件生成树。用户自定义事件都是从一个基本事件出发，逐步过滤生成的。生成树的每个节点包含（event\_id, filter, callback），其中event\_id指事件的id,filter为生成该事件的过滤函数，callback指该事件的处理回调函数。根据用户编写的事件自定义函数和事件处理函数，完成整个事件生成树的建立。从TCP流管理模块接收到产生的基本事件后，根据事件生成树产生自定义事件，并根据处理函数处理这些自定义事件。