MB的分散式部署，利用客户端的限制资源处理客户端的流量

挑战：

1客户端必须被信任

2admin需要能控制MB的功能

endbox在客户端可以收信任的执行MB

本文：可以在源头或者目的地都识别流量

INTEL SGX：intel提供的。安全区内存存储在称为安全区页面缓存（EPC）的系统保留的内存范围内，该范围已进行透明加密

可以支持本地和远程验证

endbox：在客户机上执行MB（基于SGX---TEE），数据包的加解密都发生在TEE中

唯一入口：仅接受使用正确的endboxclient端加密的流量。确保没有流量可以绕过endbox。绕过的流量也不可读

endbox取消了MB的验证，而是把对流量的验证工作前置到客户端，具体方式是使用SGX这种安全飞地的方式。由intel的背书

-------------------------------------------------------------------------------------------------------------------

endbox的客户端组成

数据的分装等功能在安全区外执行，加密解密在安全区内执行

为了确保流量都被检测，用户不能直接连接到网络，只能通过vpn连接到网络。

vpn客户端对报文进行进一步的处理（在安全区内）

1.可以根据设置由一个或多个MB进行处理

2.根据特定的功能，包头或者payload可能会被更改。甚至整个数据包有可能被丢弃

2.数据包被签名并加密到TEE外面，被传递会vpn客户端的不可信任空间

4.传输数据包

serv端进行反向处理。

vpn客户端分为两部分：可信的和不可信的

--------------------------------------------------------------------------------------------------------------------

证书和密钥管理

私钥从不离开安全区

--------------------------------------------------------------------------------------------------------------------

处理网络加密流量

对网络加密流量从处理

假设：用户使用不受信任的tls库，且这些会话密钥被发送给诚实的Clieck接口，并且在endbox的客户端运行了。这些密钥被用于解密一些特殊的数据包

通过蟹盖openssl中的一个自定义函数，这个自定义函数通过openvpn调用会话密钥。

使用这种方法，endbox可以解密流量（客户并不知道），client不需要信任ca挥着其他提供接入服务的机构。通过endbox转移会话密钥并不会造成风险

--------------------------------------------------------------------------------------------------------------------

安全保证：用户不适用vpn和endbox连接的话，流量会被防火墙丢弃------------------【这点可以借鉴，当流量不符合时MB直接丢弃，省去serv端的种种操作（包括不限于对数据包头的处理）】

client和serv周期性的交换信息，客户端可以使中间盒一直有效，保持最新状态

由于并非集种部署MB，对于拒绝服务攻击由很好的阻拦效果，得益于分布式部署，当发生故障时，影响不至于扩散致整个网络

【感想】：减少serv端的处理，丢弃不合理流量，在serv端的验证工作在endbox中几乎为0，值得借鉴。通过在MB端的发送验证信息，使得serv端只需要做很少的处理即可验证流量已经被check是个好办法。