IPSec 传输模式下 ESP 报文的装包与拆包过程

15331191 廖颖泓

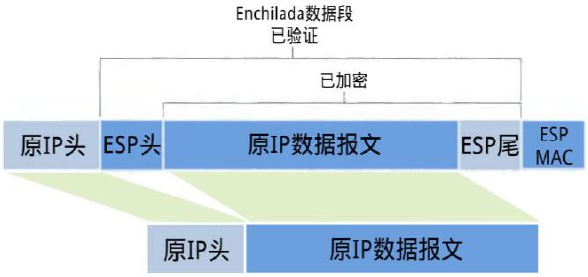
一、IPSec传输模式

传输模式下IPsec保护的仅仅是原IP报文的数据内容部分(有效载荷)，而不是整个原报文。在这个过程中原报文结构被修改。

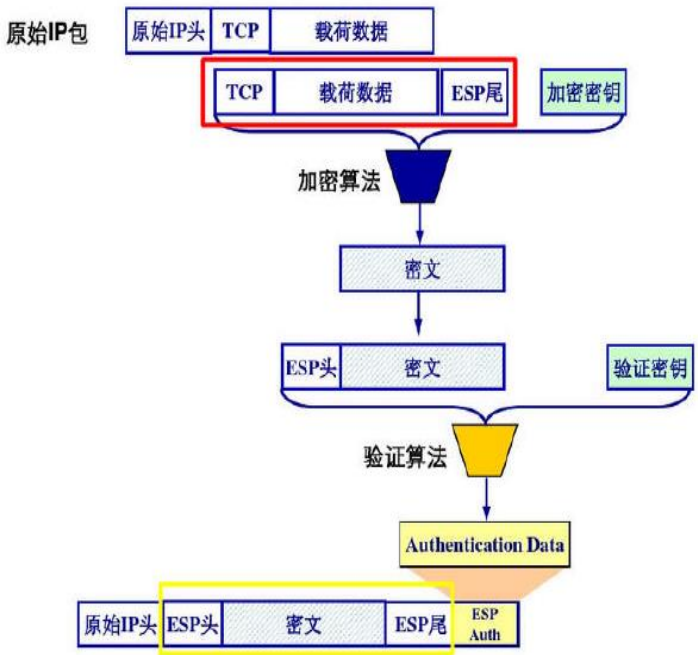
在处理方法上，原IP报文被拆解，在其有效载荷前面加上新的ESP或AH协议头，再装回原来的IP地址，形成IPsec报文。

二、IPSec传输模式下的装包过程

IPSec传输模式下的报文结构如下



装包过程的总体流程图如下(红色区域便是加密区，黄色区域是验证区)

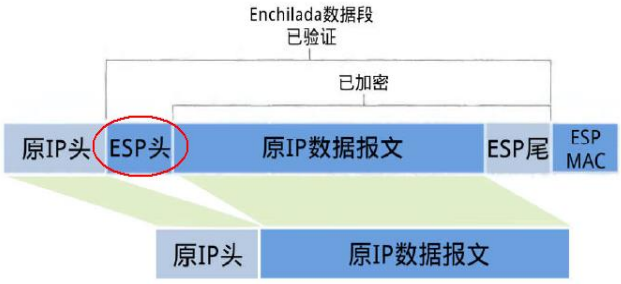


1. 拆解原始IP报文，将原始IP头与原IP报文分开，并在报文末尾添加ESP trailer(尾部/挂载) 信息。

ESP trailer包含三部分。由于所选加密算法可能是块加密，当最后一块长度不足时就需要填充(padding)，附上填充长度(Padlength)方便解包时顺利找出用来填充的那一段数据。Next header用来标明被封装的原报文的协议类型，例如6=TCP。

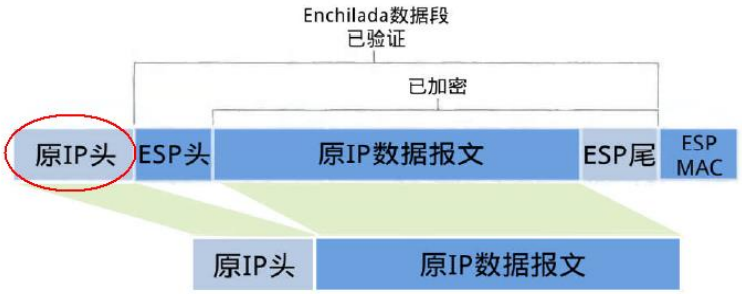
2. 将拆解后的IP报文以及第1步得到的ESP trailer作为一个整体进行加密封装。具体的加密算法与密钥由安全关联SA给出。

3. 为第2步得到的加密数据添加ESP header。ESP header由SPI和Seq #两部分组成。加密数据与ESP header合称为“enchilada”，构成认证部分。注意到被封装的原报文的协议类型受到保护，没有在ESP header给出，而由加密的ESP trailer的Next header声明。

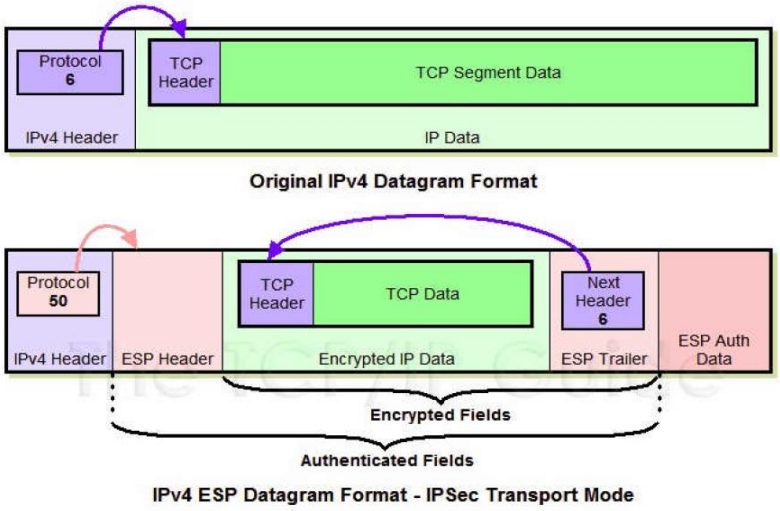


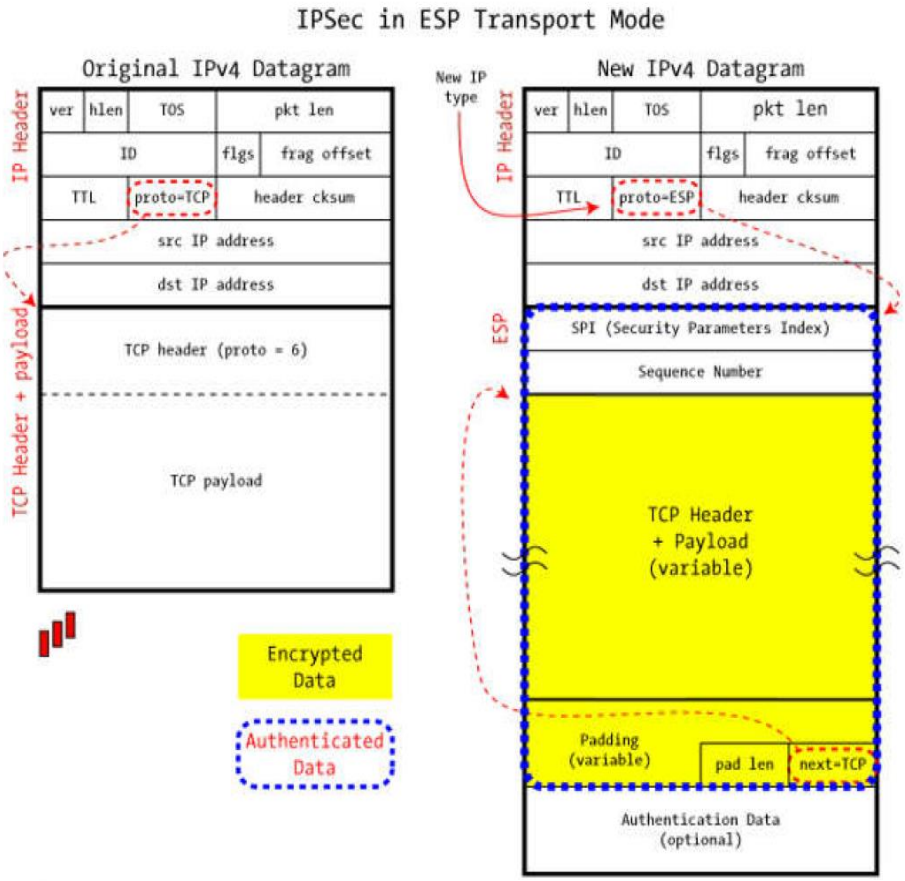
4. 附加完整性度量结果(ICV，Integrity check value)。对第3步得到的“enchilada”认证部分做摘要，得到一个32位整数倍的完整性度量值，并附在ESP报文的尾部。完整性度量算法包括验证密钥由SA给出。

5.将原始的 IP 报文头中的协议号改为 50(代表 ESP)，然后将 IP 报文头加到第 4 步的结果之前构成 IPsec 报文。



最终得到的报文结构如下





三、IPSec传输模式下的拆包过程

1. 接收方收到IP报文后，发现协议类型是50，表明这是一个ESP包。首先查看ESP header，通过SPI决定数据报文所对应的SA，获得对应的模式(tunnel/transport mode) 以及安全规范。
2. 根据SA指定的摘要算法和验证密钥计算“enchilada”部分的摘要，与附在末尾的ICV做对比，验证数据完整性。
3. 检查ESP header中Seq #里的顺序号，保证数据是“新鲜”的，避免重放攻击。
4. 根据SA所提供的加密算法和密钥，解密被加密过的数据，得到原IP报文与ESP trailer。
5. 根据ESP trailer的填充长度信息，找出填充字段的长度，删去后得到原来的IP报文。
6. 最后根据得到的原IP报文的目的地址进行转发。