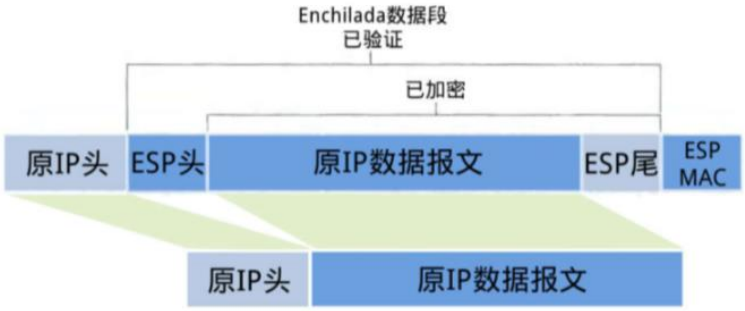
Q：准确描述 IPSec 传输模式下 ESP 报文的装包与拆包过程

1. 传输模式与隧道模式的区别

与隧道模式不同，当 IPsec 工作在传输模式时，新的 IP 头并不会被生成，而是采用原来的 IP 头，保护的也仅仅是真正传输的数据，而不是整个 IP 报文。在处理方法上，原来的 IP 报文会先被解开，再在数据前面加上新的 ESP 或 AH 协议头，最后再装回原来的 IP 头，即原来的 IP 包被修改过再传输。

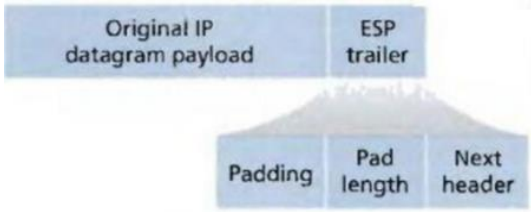
2. 传输模式下 IPsec (ESP) Datagram



3. 传输模式下 ESP 报文装包过程

（1）将原本的 IP 报文拆开成 IP 头和报文数据。

（2）对报文数据进行填充 ESP 尾（填充、填充长度、next header：标明加密数据报文的类型）。

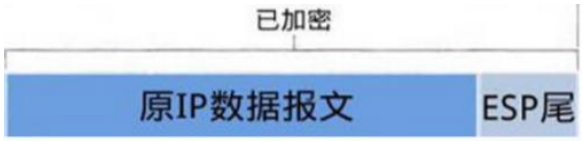


填充（padding）：字段长范围为 0-255，用于将明文扩充到需要加密的长度，同时隐藏载荷数据的真实长度。

填充长度（padding lenght）(8 位)表示填充的字节数方便解包时顺利找出用来填充的那一段数据。

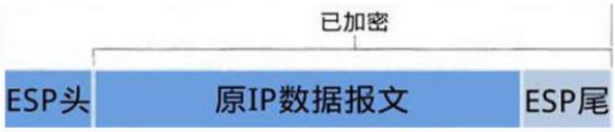
下一头部（Next header）(8 位)：标志下一头部的类型(被加密的数据类型)。

（3）加密填充后的报文数据。



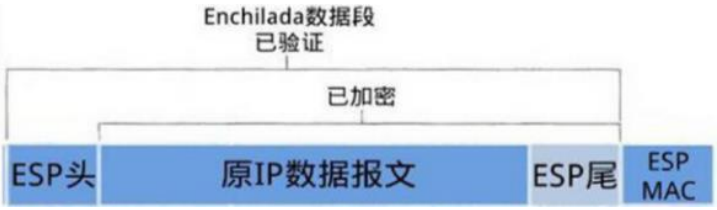
将原 IP 报文以及第 1 步得到的 ESP 尾部作为一个整体进行加密。具体的加密算法与密钥由 SA 给出。

（4）为第 3 步得到的加密数据添加 ESP 头部。



ESP 头由两部分组成，SPI 和 seq#（Sequence number）。加密数据与 ESP 头合称为“enchilada”。

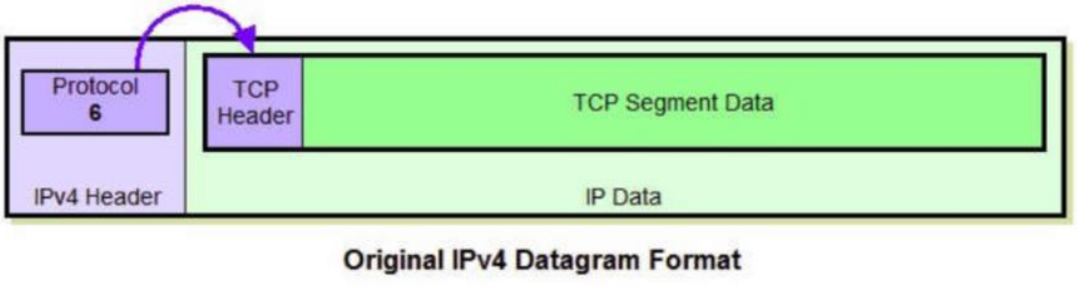
（5）附加完整性度量结果（ICV，Integrity check value）。



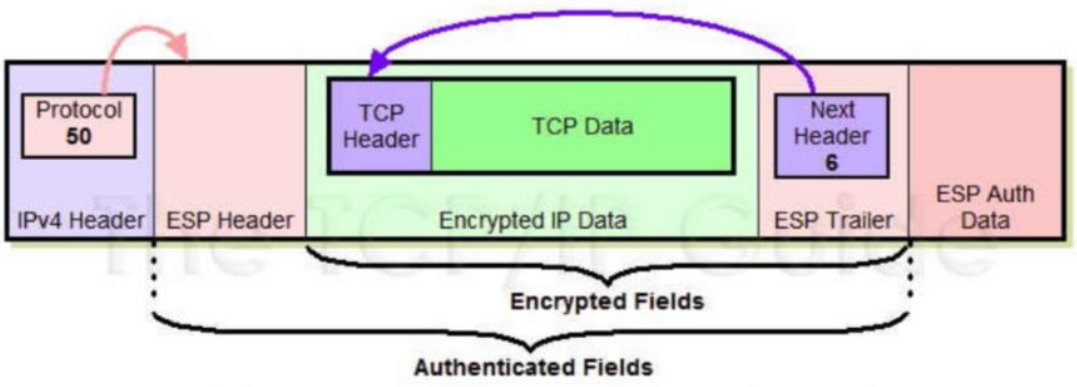
对第 4 步得到的“enchilada”做摘要，得到一个完整性度量值，并附在 ESP 报文的尾部（即图中的 ESP MAC）。

（6）获得原本的 ip 头，并将协议类型改为 50，说明它里面装的是一个 IPsec 报文。

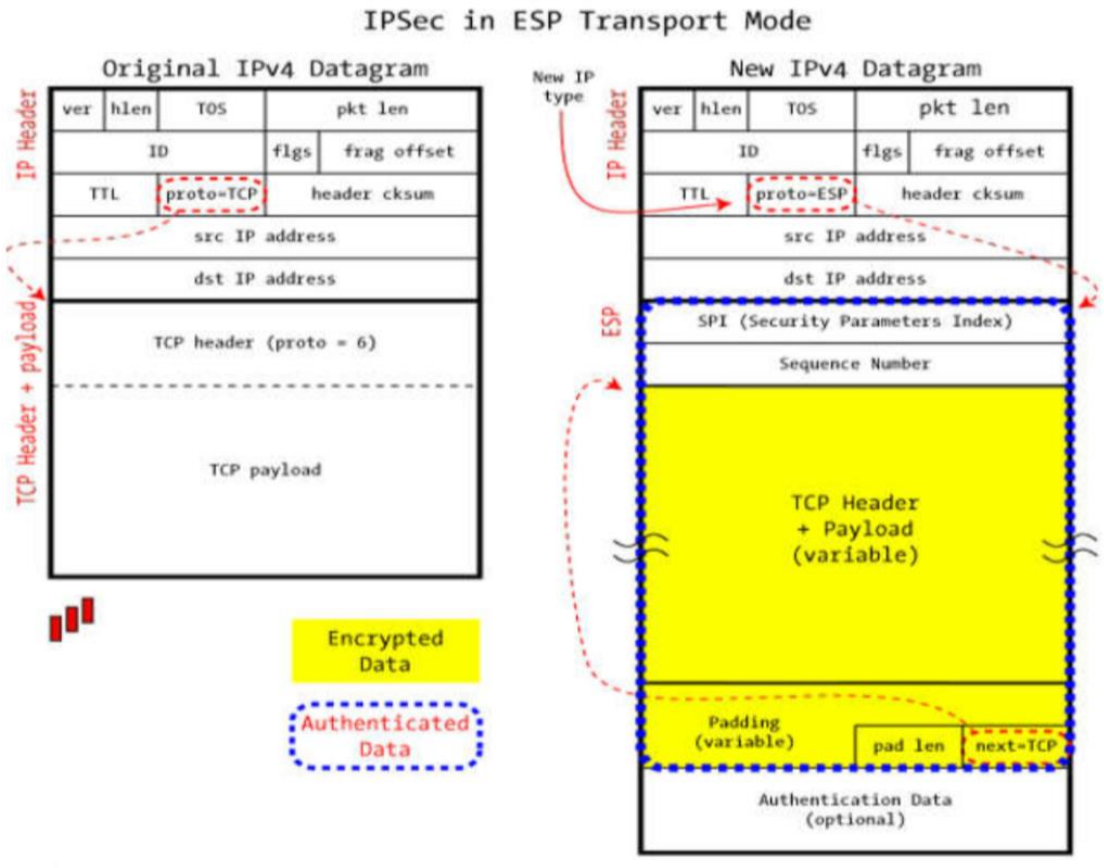
装包前后示意图：



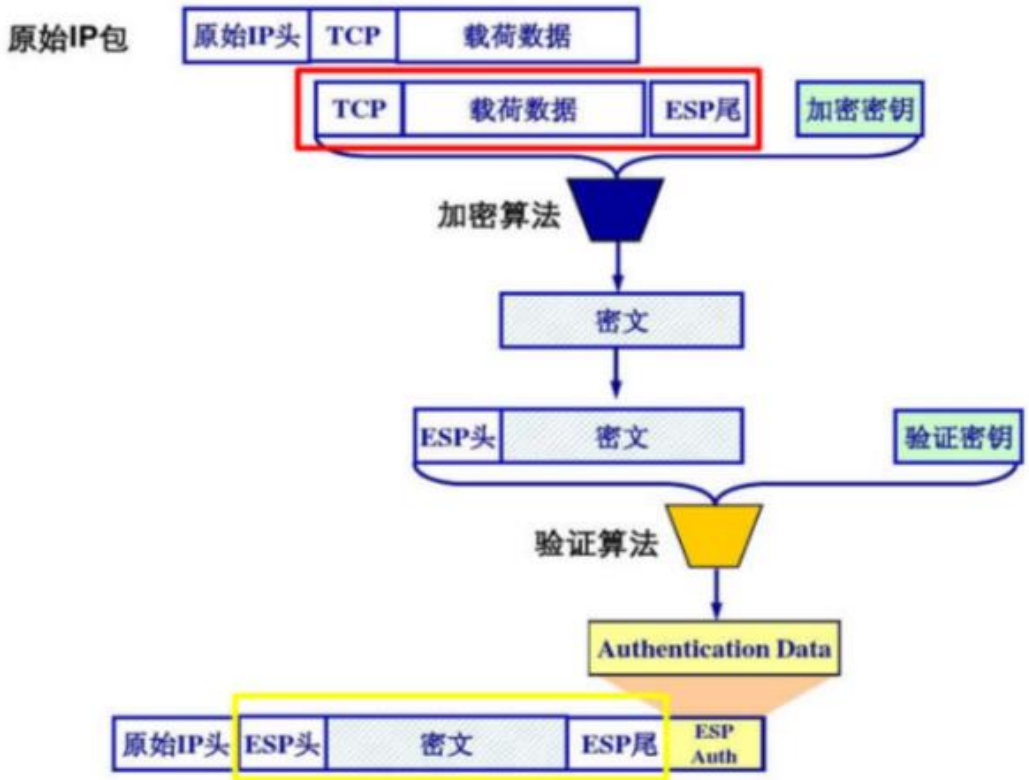
Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Transport Mode



传输模式下的认证和传输区域：
（红色区域是加密区，黄色区域是验证区）



3. 传输模式下 ESP 报文拆包过程

（1）收到数据报文后，发现协议类型是 50，表明这是一个 IPsec 包。首先查看 ESP 头，通过安全参数索引号 SPI 决定数据报文所对应的 SA，获得对应的模式（隧道或传输模式）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"的摘要值，与附在 IP 报文最后的 ICV 进行对比，二者相同则数据完整性未被破坏。

（3）检查 ESP 头中的 Seq # 里的序列号，保证数据是新的，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，即“enchilada”。得到原 IP 报文与 ESP 尾部（trailer）。

（5）根据 ESP 尾部里的填充长度信息，找出填充字段的长度，删除填充字段后就得到原来的 IP 报文。

（6）最后转让到一个高一级的协议层—比如 TCP 或 UDP—由它们对这个包进行处理。