



**【装包过程】**

1. 在IP数据报文的末尾添加ESP尾部信息。尾部包含三部分，分别是padding、padding length、next=ip
   1. Padding：当加密算是块加密时，数据的长度需要是每块长度的整数倍，此时当数据长度不够整数倍时，需要进行填充，直至可以分成若干完整的块。
   2. Padding length：是上述padding的长度记录，方便在后期的拆包过程中找到非原始数据
   3. Next=ip：当前报⽂的类型，如next=tcp
2. 对IP数据报文与ESP尾部使用加密密钥以及加密算法（SA安全关联）进⾏加密
3. 在原IP头和第2步得到的结果中间添加ESP头。ESP头包含两部分，分别是:SPI和 序列号。
   1. SPI：安全参数索引，使用这个数值判断对应的安全关联
   2. 序列号：通过序列号判断当前的包的状态，检查回放攻击
4. 对ESP 头和第2步得到的结果使用验证密钥和验证算法生成authentication data，添加到最后方作为ESP MAC
5. 装包过程完成，最后的结构为：原始IP头->第3步生成的ESP头->第2步得到的加密结果->第4步得到的ESP MAC

**【拆包过程**:】

（对装包的部分进行反向验证）

1. 对ESP头、密文、ESP尾三个部分计算摘要，并与ESP MAC部分进⾏对比，如果对比结果不同，就证明与装包过程时进行的验证结果是不同的，也就是说数据被篡改了
2. 检查ESP头的两个组成部分
   1. SPI：利用这个数值判断对应的安全关联SA
   2. 序列号：检查是否是回放攻击。
3. 根据第2步中的SPI对应的SA得到加密算法与密钥，同时完成解密，得到在装包过程中第2步操作的IP数据报文与ESP尾部
4. 根据ESP尾部中的padding length得到后续添加的padding部分的长度，并将这部分截去，同时将next=iP中的IP类型记为真正的IP类型后，得到的最终结果就是拆包后的结果。