**IPSec传输模式下ESP 报文的装包与拆包过程**

**一、装包过程**

1. **在原IP报文末尾添加ESP尾部信息。**

ESP尾部信息包含三部分：

1. Padding：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

（2）Pad Length：说明填充的字节数

（3）Next Header：标志下一头部的类型（被加密的数据类型）

1. **将原 IP 报文的数据部分与第1步得到的ESP尾部作为整体进行加密，加密算法与密钥由SA给出。**
2. **为第2步得到的加密数据添加ESP头部信息。加密数据与ESP头合称为“Enchilada” 。**

ESP头部信息包含两部分：

（1）SPI：Security Parameter Index，安全参数索引，用于将收到的IPsec数据包与其对应的SA进行关联，从SAD中获得关于该IPsec包一些信息如协议所有的算法和密钥

（2）序列号：Sequence numbe，占32比特，SA初次建立时置0，每发送一个数据包加1，用于抵抗重放攻击

1. **对前面的加密数据与ESP头的组合体做一个摘要，得到一个完整性度量值（ICV），并添加到该组合体尾部。**
2. **把原IP头加到ESP头前面，修改协议类型为50。这样基于ESP协议的传输模式下装包便完成了。**

**二、拆包过程**

1. **接收方收到数据报文后，发现协议类型是 50，知道这是一个IPsec包。查看ESP头部信息，通过里面的SPI得到数据报文对应的SA。**
2. **计算前面说到的Enchilada部分的ICV，与附在末尾的完整性度量值做对比，如果一样的话说明数据是完整的，否则可以断定所收到的报文已经不是原来的报文了。**
3. **检查序列号，保证数据是“新鲜的”而不是重放攻击。**
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报文的数据部分与ESP尾。**
5. **根据ESP尾里的Padding填充长度信息，我们可以找出填充字段，删去后就得到原IP报文的数据部分。**
6. **将 IP头和IP数据部分组合即得到完整的原IP报文。然后根据原IP头的目的地址进行转发。**