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）

2. 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。

3. 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

4. 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。

5. 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。