 ESP 的协议号为50 AH 协议号为51 一、ESP详解 （一）ESP提供：confidentiality，data integrity，optional data origin authentication，anti-replay services （二）ESP结构为： 1、Security Parameter Index（SPI） 2、Sequence Number 3、Payload Data（Variable） 4、Padding（0-255）Bytes 5、Pad length 6、Report Handler 7、Authentication Data（varaible） SPI： 1、destination address 2、protocol 3、identify the security association（SA） SPI number是在Internet Key Exchange（IKE）协商过程中，可以任意指定的。利用这个number可以在security association database（SADB）中查询相关信息。 Sequence number： 提供anti-replay services.这点在AH中也是同样的 原理是通过increasing序号 Payload data： 被保护的数据，加密算法需要一个initialization vector（IV），注意IV需要认证，但是不是加密的，DES使用前8个字节做为IV，3DES、AES也使用8字节的IV. Padding Bytes： 根据加密算法不同，补足的字节也不同。 二、AH详解 （一）AH提供：connectionless integrity，data authentication，optional replay protection，但是不提供confidentiality（加密） （二）AH的包结构： 1、Next header 2、Payload Length 3、Reserved 4、Security Parameter Index（SPI） 5、Sequence Number 6、Authentication Data（Variable） 三、ESP、AH对比 1、AH没有ESP的加密特性 2、AH的authtication是对整个数据包做出的，包括IP头部分，因为IP头部分包含很多变量，比

如type of service（TOS），flags，fragment offset，TTL以及header checksum.所以这些值在进行authtication前要全部清零。否则hash会mismatch导致丢包。 相反，ESP是对部分数据包做authentication，不包括IP头部分。 