IPSec

1.简介

IPsec（IP Security）是IETF制定的三层隧道加密协议，它为Internet上传输的数据提供了高质量的、可互操作的、基于密码学的安全保证。特定的通信方之间在IP层通过加密与数据源认证等方式，提供了以下的安全服务：

  数据机密性（Confidentiality）：IPsec发送方在通过网络传输包前对包进行加密。

   数据完整性（Data Integrity）：IPsec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。

   数据来源认证（Data Authentication）：IPsec在接收端可以认证发送IPsec报文的发送端是否合法。

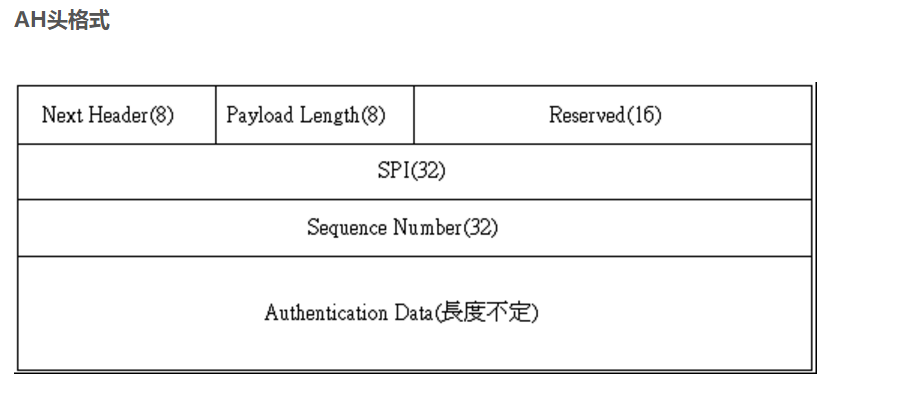
防重放（Anti-Replay）：IPsec接收方可检测并拒绝接收过时或重复的报文。

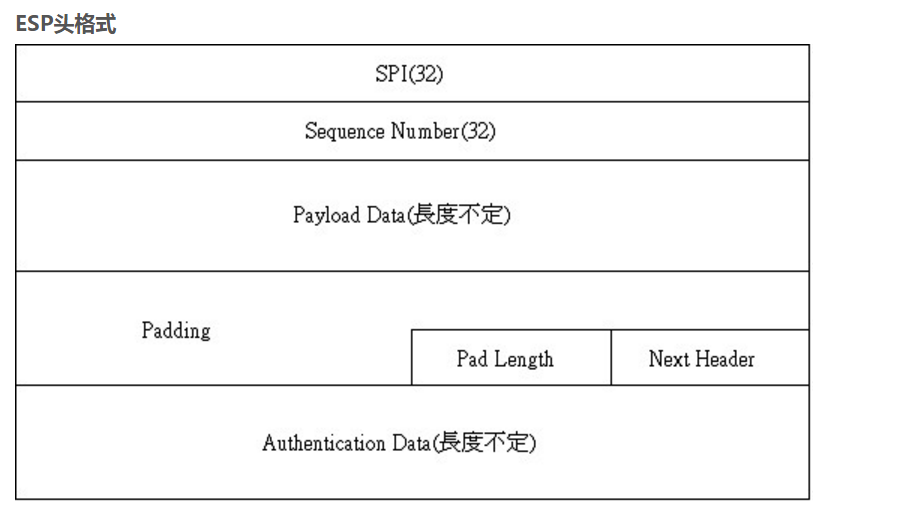
IPsec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构，包括网络认证协议AH（Authentication Header，认证头）、ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，因特网密钥交换）和用于网络认证及加密的一些[算法](http://lib.csdn.net/base/datastructure" \o "算法与数据结构知识库" \t "http://blog.csdn.net/tantexian/article/details/_blank)等。其中，AH协议和ESP协议用于提供安全服务，IKE协议用于密钥交换。

1. AH与ESP

IPsec协议中的AH协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP协议定义了加密和可选认证的应用方法，提供数据可靠性保证。

AH协议（IP协议号为51）提供数据源认证、数据完整性校验和防报文重放功能，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。



(2) ESP协议（IP协议号为50）提供加密、数据源认证、数据完整性校验和防报文重放功能。

3.传输模式和隧道模式



4安全联盟（Security Association，SA）

SA是IPsec的基础，也是IPsec的本质。SA是通信对等体间对某些要素的约定，例如，使用哪种协议（AH、ESP还是两者结合使用）、协议的封装模式（传输模式和隧道模式）、加密算法（DES、3DES和AES）、特定流中保护数据的共享密钥以及密钥的生存周期等。建立SA的方式有手工配置和IKE自动协商两种。

(1).SA是单向的，在两个对等体之间的双向通信，最少需要两个SA来分别对两个方向的数据流进行安全保护。

(2)协商方式:有如下两种协商方式建立SA：

             手工方式（manual）配置比较复杂，创建SA所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖IKE而单独实现IPsec功能。

              IKE自动协商（isakmp）方式相对比较简单，只需要配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护SA。

5.IKE在实施IPsec的过程中，可以使用IKE（Internet Key Exchange，因特网密钥交换）协议来建立SA，该协议建立在由ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）定义的框架上。IKE为IPsec提供了自动协商交换密钥、建立SA的服务，能够简化IPsec的使用和管理，大大简化IPsec的配置和维护工作。

IKE使用了两个阶段为IPsec进行密钥协商并建立SA：

        第一阶段，通信各方彼此间建立了一个已通过身份认证和安全保护的通道，即建立一个ISAKMP SA。第一阶段有主模式（Main Mode）和野蛮模式（Aggressive Mode）两种IKE交换方法。

     第二阶段，用在第一阶段建立的安全隧道为IPsec协商安全服务，即为IPsec协商具体的SA，建立用于最终的IP数据安全传输的IPsec SA。