0

使用也可一起使用。IKE 则提供加密算法、密钥等的协商。

1. 安全关联和安全策略

安全关联(Security Association, SA)是指提供通信安全服务的发送方和接收方之间的一种单向关系。安全关联是构成 IPSec 的基础,它是进行通信的双方经协商建立起来的一种协定。安全关联可以用一个 32 位的安全参数索引(Security Parameter Index,SPI)来唯一标识,一个 SPI 值决定一个特定的 SA,它通常放在 AH 或 ESP 头中;安全关联是单向的,如果要对两台主机 A与 B实现双向安全,则需要两个安全关联,每个方向一个:(A,B)、(B,A)。安全关联的内容包含了 IP 数据包是否加密、认证,以及加密、认证采用的算法、密钥等相关信息。所有的 SA 记录都存放在安全关联数据库中,按散列方式存取。

安全策略(Security Policy)定义了两个 IPSec 系统之间的安全通信特征,并决定在该通信中为数据包提供的安全服务。一个 IPSec 系统的所有安全策略都存放在安全策略数据库中,根据选择符(包括源地址、目的地址、协议、端口等)进行检索。安全策略通常与SA合作,共同作用于通信的数据包。

2. AH

AH 协议先将数据进行校验和加密,然后封装为 IP 包,从而实现无连接通信的数据完整性、数据源认证和防止重放攻击。AH 能完成除数据加密外的所有的 ESP 所能提供的功能。在认证机制上,它所覆盖的范围比 ESP 的广,包括对 IP 头中一些选项的认证。

为了应用 IPSec 协议, IP 数据包的格式要有所改变, 即在 IP 头和被保护的数据之间插入一个 AH 头, 如图 16-3 所示。

Ib矛	AH头	被保护的数据
11-5	An	10000000000000000000000000000000000000

图 16-3 用 AH 保护的 IP 数据包格式示意图

AH 头的格式如图 16-4 所示,包括:下一报头、有效载荷长度、保留位、安全参数索引、序列号、认证数据。

下一个报头	有效载荷长度	保留位		
安全参数索引 (SPI)				
序列号				
	认证数据(AD)			

图 16-4 AH 头的格式

AH 使用的典型的认证算法是一种迭代型的消息摘要算法。AH 中采用 MD5 算法,可以提供完整性服务。从前面的讲述可以知道 MD5 可以对任意长度的信息进行散列运算产生一个唯一的 128 位消息摘要。由于消息摘要是唯一的,所以对信息的任何修改都将得到另一个不同的消息摘要,因此能防止消息被篡改,从而保证了数据的完整性。AH 也可以采用 SHA 算法提供更强的抗攻击能力,SHA 是在 MD5 的基础上,增加了分组处理的迭代次数