IPSec的两种工作模式及其报文封装格式

姚忆斌 2007-01-23 发表

IPSec的两种工作模式及其报文封装格式

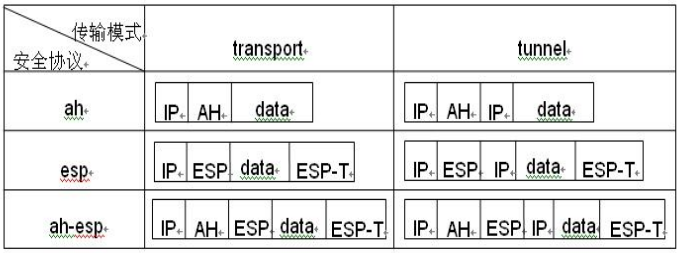
Q: IPSec有几种工作模式,它们报文封装格式有什么区别?

A: IPsec有如下两种工作模式:

隧道（tunnel）模式：用户的整个IP数据包被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被封装在一个新的IP数据包中。通常，隧道模式应用在两个安全网关之间的通讯。

传输（transport）模式：只是传输层数据被用来计算AH或ESP头，AH或ESP头以及ESP加密的用户数据被放置在原IP包头后面。通常，传输模式应用在两台主机之间的通讯，或一台主机和一个安全网关之间的通讯。

在tunnel和transport模式下的数据封装形式如下图所示，图中data为原IP报文。



传输模式
transport
tunnel
ah
esp
ah-esp
IP
AH
data
IP
AH
data
IP
IP
ESP
data
ESP-T
IP
ESP
data
ESP-T
IP
IP
ESP
data
ESP-T
AH
IP
ESP
data
ESP-T
AH
IP