

知 在IPSec中PFS是什么含义?

刘军 2006-10-25 发表

在IPSEC中PFS是什么含义?

PFS (Perfect Forward Secrecy, 完善的前向安全性) 是一种安全特性, 指一个密钥被破解, 并不影响其他密钥的安全性, 因为这些密钥间没有派生关系。此特性是通过在IKE阶段2的协商中增加密钥交换来实现的。