《现代通信与网络工程实用教程》

图书基本信息

书名：《现代通信与网络工程实用教程》

13位ISBN编号：9787121174780

10位ISBN编号：7121174782

出版时间：2012-9

出版社：电子工业出版社

作者：刘正华 编

页数：305

《现代通信与网络工程实用教程》

内容概要

《现代通信与网络工程实用教程》

书籍目录

章节摘录

版权页： 插图： 8.3.4项目4三层隧道协议——IPSec协议配置的实现 1.IPSec协议基础 1）IPSec概述 （1）定义。IPSec是一个工业标准网络安全协议，是一种由IETF设计的端到端的、确保基于IP通信的数据安全性的机制。它支持对数据加密，为网络通信提供透明的安全服务，保护TCP／IP通信免遭窃听和篡改，同时确保数据的完整性。 （2）基本工作原理。发送方在数据传输前对数据实施加密，在整个传输过程中，报文都以密文方式传输，直到数据到达目的节点，才由接收端对其进行解密。IPSec对数据的加密以数据包而不是整个数据流为单位，这不仅更灵活，也有助于进一步提高IP数据包的安全性。通过提供强有力的加密保护，IPSec可以有效防范网络攻击，保证专用数据在公共网络环境下的安全性。 （3）内容。IPSec不是单独协议，是一整套体系结构。①AH（Authentication Header）协议。②ESP（Encapsulating Security Payload）协议。③IKE（Internet Key Exchange）协议。④用于网络验证及加密的一些算法。IPSec规定了如何选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源验证、数据加密等网络安全服务。 （4）安全机制与协商安全关联的概念。①安全机制：可以把IPSec想象成位于TCPfiP协议栈的下层协议，该层由每台计算机上的安全策略和发送、接收方协商的安全关联（Security Association，SA）进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的IP地址、协议和端El号都满足一个过滤机制，那么这个数据包将要遵守关联的安全行为。②协商安全关联（Negotiated Security Association）：第一个满足过滤机制的数据包将会引发发送和接收方对安全关联进行协商。ISAKMP／OAKLEY是这种协商采用的标准协议。在一个ISAKMP／OAKLEY交换过程中，两台机器对验证和数据安全方式达成一致，进行相互验证，然后生成一个用于随后的数据加密的共享密钥。 （5）验证报头（AH）。通过一个位于IP报头和传输报头之间的验证报头可以提供IP负载数据的完整性和数据验证。验证报头包括验证数据和一个序列号，共同用来验证发送方身份，确保数据在传输过程中没有被改动，防止受到第三方的攻击。IPSec验证报头不提供数据加密；信息将以明文方式发送。 （6）封装安全负载（ESP）。为了保证数据的保密性并防止数据被第三方窃取，封装安全负载提供了一种对IP负载进行加密的机制。另外，ESP还可以提供数据验证和数据完整性服务。 （7）IPSec是第三层的协议标准。支持IP网络上数据的安全传输。除了对IP数据流的加密机制进行了规定之外，IPSec还制定了隧道模式的数据包格式，一般被称做IPSec隧道模式。一个IPSec隧道由一个隧道客户和隧道服务器组成，两端都配置使用IPSec隧道技术，采用协商加密机制。

《现代通信与网络工程实用教程》

编辑推荐

《现代通信与网络工程实用教程》

版权说明