安全路由器组网及IPSec技术介绍Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/563/2021_2022__E5_AE_89_E5_85_A8_E8_B7_AF_E7_c101_563568.htm 一个大的企业/公司需要把分布在全国的各个分公司或办事处通过广域网联系起来，做到相互之间共享信息资源，由于需要在公用的数据网上传输数据，众所周知在公用的数据网上传输数据信息并不是特别的安全。为了提高所传输的数据的安全性可以考虑使用安全路由器。安全路由器可以隐藏公司内部的网络拓扑结构图，同时还可以加密需要传输的数据，从而做到即使传输的数据在公网上给其它用户拦截到时，他们也不能通过IP包来获取公司内部的网络IP地址及了解到内部的网络拓扑结构图，经过加密的数据，没有专门的解密工具一般的用户是不可能知道所传输的数据包的内容。使用安全路由器的网络拓扑图如下图所示： 图 利用安全路由器组网 由于安全路由器具有数据加密的功能，局域网上的需要传输的数据在通过安全路由器向外发送时，安全路由器会根据一定的加密算法把数据加密，接收到该数据的对端也要使用相同的算法才能把数据还原。 安全路由器的IPSec的隧道模式还具有隐藏内部网络拓扑结构图的功能，安全路由器对所有需要发送的IP包，进行重新封装，在原来的IP包上封装源和目的网关的IP地址；目的路由器对接收到的IP包，先去掉IPSec所增加的IP包头，然后再根据IP包的源和目的地址，把该IP包发送到局域网上的目的主机上。 当局域网A上的用户要给局域网B上的用户发送数据时，首先A用户的IP报文通过出口安全路由器时被重新打包，在原来的IP包上封装源和目的网关的IP地址，封装后

的IP报文传送到目的地B端的安全路由器时，可被自动识别出来，同时IP报文重新被解包，最终传送到B端用户。 IPSec技术介绍 IPSec是一个开放式标准的框架。基于IETF开发的标准，IPSec可以在一个公共IP网络上确保数据通讯的可靠性和完整性。IPSec对于实现通用的安全策略所需要的基于标准的灵活的解决方案提供了一个必备的要素。 TCP/IP协议簇提供了一个开放式协议平台，正将越来越多的部门和人员用网络连接起来，网络正在快速地改变着我们工作和生活的方式，但是安全性的缺乏已经减慢了联网的发展速度。目前网络面临的各种威胁包括保密数据的泄露、完整性的破坏、身份伪装和拒绝服务等。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com