设置好NAT地址转换网络安全更有保障 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E8_AE_BE_E7_BD_AE_E5_A5_BDN_c101_260874.htm 随着计算机网络迅速发展，目前有许多的企业或单位同时拥有自己的内部网和Internet网。其实如果不想让外部网络用户知道自己的网络内部结构，可以通过NAT将内部网络与外部Internet 隔离开，则外部用户根本不知道通过NAT设置的内部IP地址，而内部计算机却可以随时访问这两个网络中的资源。 配置NAT的重要性 当我们尝试着改变网络的IP地址时，考虑这样做会给网络中已有的安全机制带来什么样的影响。比如：防火墙根据IP报头中包含的TCP端口号、信宿地址、信源地址以及其它一些信息来决定是否让该数据包通过。任何一个淘气的黑客，只要他能够使NAT误以为他的连接请求是被允许的，都可以以一个授权用户的身份对你的网络进行访问。如果企业正在迈向网络技术的前沿，并正在使用IP安全协议（IPSec）来构造一个虚拟专用网（VPN）时，错误地放置NAT设备会毁了计划。由此可见，对于这样网络环境，正确配置NAT地址转换非常有必要。 NAT定义 NAT(Network Address Translation)的功能，就是指在一个网络内部，根据需要可以随意自定义的IP地址，而不需要经过申请。在网络内部，各计算机间通过内部的IP地址进行通讯。而当内部的计算机要与外部internet网络进行通讯时，具有NAT功能的设备（比如：路由器）负责将其内部的IP地址转换为合法的IP地址（即经过申请的IP地址）进行通信。NAT主要的处理方式是通过修改UDP或TCP报文头部地址信息实现地址的转换。 NAT设

置分类 根据NAT设置类型，大致可以分为静态地址转换、动态地址转换、复用动态地址转换。 一、静态地址转换：静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有E-mail服务器或FTP服务器等可以为外部用户提供的服务，这些服务器的IP地址必须采用静态地址转换，以便外部用户可以使用这些服务。静态地址转换基本配置步骤：（1）、在内部本地地址与内部合法地址之间建立静态地址转换。在全局设置状态下输入：ip nat inside source static 内部本地地址 内部合法地址。（2）、指定连接网络的内部端口 在端口设置状态下输入：ip nat inside。（3）、指定连接外部网络的外部端口 在端口设置状态下输入：ip nat outside。可以根据实际需要,定义多个内部端口及多个外部端口。我们也可以通过一个实例，来观察如何配置NAT的设置（在Windows 2003 Server系统环境下）。 首先需要安装两块网卡，分别配置两个网段地址(内网网卡配10.1.153.1.外网网卡配222.210.213.109)。通过“ 控制面板 ”或者“ 管理工具 ”进入“ 路由和远程访问 ”。如果原先没有启用配置过路由(如果原先已经启用了静态路由等其他功能，建议先禁用服务)访问，进入配置向导，按照向导，选择“ Internat连接服务 ”→“ 设置有网络地址转换(NAT)路由协议的路由器 ”→“ 使用选择的Internat连接 ”，下面的列表框里显示了两个连接(见图1左窗口，本地连接和本地连接2)，选择配置了外网IP的那个连接(比如配置了公网IP的连接)，再点击下一步就完成了。打开本机树，您会看到四个子项(见图1):路由接口、IP路由选择、远程访问策略、远程访问记录。 图1 100Test 下载频道开通，各类考试题目直