关于防火墙必须知道的几点 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/0/2021_2022__E5_85_B3_E4_BA_8E_E9_98_B2_E7_c99_422.htm 提到防火墙，顾名思义，就是防火的一道墙。防火墙的最根本工作原理就是数据包过滤。实际上在数据包过滤的提出之前，都已经出现了防火墙。 数据包过滤，就是通过查看题头的数据包是否含有非法的数据，我们将此屏蔽。 举个简单的例子，假如体育中心有一场刘德华演唱会，检票员坐镇门口，他首先检查你的票是否对应，是否今天的，然后撕下右边的一条，将剩余的给你，然后告诉你演唱会现场在哪里，告诉你怎么走。这个基本上就是数据包过滤的工作流程吧。 你也许经常听到你们老板说：要增加一台机器它可以禁止我们不想要的网站，可以禁止一些邮件它经常给我们发送垃圾邮件和病毒等，但是没有一个老板会说：要增加一台机器它可以禁止我们不愿意访问的数据包。实际意思就是这样。接下来我们推荐几个常用的数据包过滤工具。 最常见的数据包过滤工具是路由器。另外系统中带有数据包过滤工具，例如LinuxTCP/IP中带有的ipchain等windows2000带有的TCP/IPFiltering筛选器等，通过这些我们就可以过滤掉我们不想要的数据包。 防火墙也许是使用最多的数据包过滤工具了，现在的软件防火墙和硬件防火墙都有数据包过滤的功能。接下来我们会重点介绍防火墙的。 防火墙通过一下方面来加强网络的安全： 1、策略的设置 策略的设置包括允许与禁止。允许例如允许我们的客户机收发电子邮件，允许他们访问一些必要的网站等。例如防火墙经常这么设置，允许内网的机器访问网站、收发电子邮件、从FTP

下载资料等。这样我们就要打开80、25、110、21端口，开HTTP、SMTP、POP3、FTP等。 禁止就是禁止我们的客户机去访问哪些服务。例如我们禁止邮件客户来访问网站，于是我们就给他打开25、110，关闭80。 2、NAT NAT，即网络地址转换，当我们内网的机器在没有公网IP地址的情况下要访问网站，这就要用到NAT。工作过程就是这样，内网一台机器 192.168.0.10要访问新浪，当到达防火墙时，防火墙给它转变成一个公网IP地址出去。一般我们为每个工作站分配一个公网IP地址。 防火墙中要用到以上提到的数据包过滤和代理服务器，两者各有优缺点，数据包过滤仅仅检查题头的内容，而代理服务器除了检查标题之外还要检查内容。当数据包过滤工具瘫痪的时候，数据包就都会进入内网，而当代理服务器瘫痪的时候内网的机器将不能访问网络。 另外，防火墙还提供了加密、身份验证等功能。还可以提供对外部用户VPN的功能。 编辑特别推荐: #0000ff>如何在xp下通过命令行对防火墙进行配置 #0000ff>详细配置CiscoPIX防火墙 #0000ff>利用防火墙来防止DOS攻击的实例解析 