2006行业新闻浅谈防火墙技术与网络安全 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/63/2021_2022_2006_E8_A1_8C_E4_B8_9A_c40_63774.htm 网络已经成为了人类所构建的最丰富多彩的虚拟世界，网络的迅速发展，给我们的工作和学习生活带来了巨大的改变。我们通过网络获得信息，共享资源。如今， Internet遍布世界任何一个角落，并且欢迎任何一个人加入其中，相互沟通，相互交流。随着网络的延伸，安全问题受到人们越来越多的关注。在网络日益复杂化，多样化的今天，如何保护各类网络和应用的安全，如何保护信息安全，成为了本文探讨的重点。 几乎所有接触网络的人都知道网络中有一些费尽心机闯入他人计算机系统的人，他们利用各种网络和系统的漏洞，非法获得未授权的访问信息。不幸的是如今攻击网络系统和窃取信息已经不需要什么高深的技巧。网络中有大量的攻击工具和攻击文章等资源，可以任意使用和共享。不需要去了解那些攻击程序是如何运行的，只需要简单的执行就可以给网络造成巨大的威胁。甚至部分程序不需要人为的参与，非常智能化的扫描和破坏整个网络。这种情况使得近几年的攻击频率和密度显著增长，给网络安全带来越来越多的安全隐患。 // 请保留本文完整.REISTLIN.Blog.Cnunder.com. 我们可以通过很多网络工具，设备和策略来保护不可信任的网络。其中防火墙是运用非常广泛和效果最好的选择。它可以防御网络中的各种威胁，并且做出及时的响应，将那些危险的连接和攻击行为隔绝在外。从而降低网络的整体风险。 防火墙的基本功能是对网络通信进行筛选屏蔽以防止未授权的访问进出计算机网络，简单

的概括就是，对网络进行访问控制。绝大部分的防火墙都是放置在可信任网络（Internal）和不可信任网络（Internet）之间。 防火墙一般有三个特性： A．所有的通信都经过防火墙 B．防火墙只放行经过授权的网络流量 C．防火墙能经受的住对其本身的攻击 我们可以看成防火墙是在可信任网络和不可信任网络之间的一个缓冲，防火墙可以是一台有访问控制策略的路由器（Route ACL），一台多个网络接口的计算机，服务器等，被配置成保护指定网络，使其免受来自于非信任网络区域的某些协议与服务的影响。所以一般情况下防火墙都位于网络的边界，例如保护企业网络的防火墙，将部署在内部网络到外部网络的核心区域上。 为什么要使用防火墙？很多人都会有这个问题，也有人提出，如果把每个单独的系统配置好，其实也能经受住攻击。遗憾的是很多系统在缺省情况下都是脆弱的。最显著的例子就是Windows系统，我们不得不承认在Windows 2003以前的时代， Windows默认开放了太多不必要的服务和端口，共享信息没有合理配置与审核。如果管理员通过安全部署，包括删除多余的服务和组件，严格执行NTFS权限分配，控制系统映射和共享资源的访问，以及帐户的加固和审核，补丁的修补等。做好了这些，我们也可以非常自信的说，Windows足够安全。也可以抵挡住网络上肆无忌惮的攻击。但是致命的一点是，该服务器系统无法在安全性，可用性和功能上进行权衡和妥协。 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