路由器应用ACL和防火墙的区别 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/270/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E5_c67_270367.htm 一、两种设备产生和存在的背景不同 1、两种设备产生的根源不同 路由器的产生是基于对网络数据包路由而产生的。路由器需要完成的是将不同网络的数据包进行有效的路由，至于为什么路由、是否应该路由、路由过后是否有问题等根本不关心，所关心的是：能否将不同的网段的数据包进行路由从而进行通讯。 防火墙是产生于人们对于安全性的需求。数据包是否可以正确的到达、到达的时间、方向等不是防火墙关心的重点，重点是这个（一系列）数据包是否应该通过、通过后是否会对网络造成危害。 2、根本目的不同 路由器的根本目的是：保持网络和数据的“ 通 ”。 防火墙根本的的目的是：保证任何非允许的数据包“ 不通 ”。 二、核心技术的不同 Cisco路由器核心的ACL列表是基于简单的包过滤，从防火墙技术实现的角度来说，NetEye防火墙是基于状态包过滤的应用级信息流过滤。 一个最为简单的应用：企业内网的一台主机，通过路由器对内网提供服务（假设提供服务的端口为tcp 1455）。为了保证安全性，在路由器上需要配置成：外-》内 只允许client访问 server的tcp 1455端口，其他拒绝。 针对现在的配置，存在的安全脆弱性如下： 1、IP地址欺骗（使连接非正常复位） 2、TCP欺骗（会话重放和劫持） 存在上述隐患的原因是，路由器不能监测TCP的状态。如果在内网的client和路由器之间放上NetEye防火墙，由于NetEye防火墙能够检测 TCP的状态，并且可以重新随机生成TCP的序列号，则可以彻底消除这

样的脆弱性。同时，NetEye 防火墙的一次性口令认证客户端功能，能够实现在对应用完全透明的情况下，实现对用户的访问控制，其认证支持标准的Radius协议和本地认证数据库，可以完全与第三方的认证服务器进行互操作，并能够实现角色的划分。 虽然，路由器的"Lock-and-Key"功能能够通过动态访问控制列表的方式，实现对用户的认证，但该特性需要路由器提供Telnet服务，用户在使用使也需要先Telnet到路由器上，使用起来不很方便，同时也不够安全（开放的端口为黑客创造了机会）。 三、安全策略制定的复杂程度不同 路由器的默认配置对安全性的考虑不够，需要一些高级配置才能达到一些防范攻击的作用，安全策略的制定绝大多数都是基于命令行的，其针对安全性的规则的制定相对比较复杂，配置出错的概率较高。 NetEye 防火墙的默认配置既可以防止各种攻击，达到既用既安全，安全策略的制定是基于全中文的GUI的管理工具，其安全策略的制定人性化，配置简单、出错率低。 四、对性能的影响不同 路由器是被设计用来转发数据包的，而不是专门设计作为全特性防火墙的，所以用于进行包过滤时，需要进行的运算非常大，对路由器的CPU和内存的需要都非常大，而路由器由于其硬件成本比较高，其高性能配置时硬件的成本都比较大。 NetEye防火墙的硬件配置非常高（采用通用的INTEL芯片，性能高且成本低），其软件也为数据包的过滤进行了专门的优化，其主要模块运行在操作系统的内核模式下，设计之时特别考虑了安全问题，其进行数据包过滤的性能非常高。 由于路由器是简单的包过滤，包过滤的规则条数的增加，NAT规则的条数的增加，对路由器性能的影响都相应的增加，而NetEye防火墙采用的是

状态包过滤，规则条数，NAT的规则数对性能的影响接近于零。 五、审计功能的强弱差异巨大 路由器本身没有日志、事件的存储介质，只能通过采用外部的日志服务器（如syslog，trap）等来完成对日志、事件的存储；路由器本身没有审计分析工具，对日志、事件的描述采用的是不太容易理解的语言；路由器对攻击等安全事件的相应不完整，对于很多的攻击、扫描等操作不能够产生准确及时的事件。审计功能的弱化，使管理员不能够对安全事件进行及时、准确的响应。 NetEye防火墙的日志存储介质有两种，包括本身的硬盘存储，和单独的日志服务器；针对这两种存储，NetEye 防火墙都提供了强大的审计分析工具，使管理员可以非常容易分析出各种安全隐患；NetEye 防火墙对安全事件的响应的及时性，还体现在他的多种报警方式上，包括蜂鸣、trap、邮件、日志；NetEye 防火墙还具有实时监控功能，可以在线监控通过防火墙的连接，同时还可以捕捉数据包进行分析，非分析网络运行情况，排除网络故障提供了方便。 六、防范攻击的能力不同 对于像Cisco这样的路由器，其普通版本不具有应用层的防范功能，不具有入侵实时检测等功能，如果需要具有这样的功能，就需要生级升级IOS为防火墙特性集，此时不单要承担软件的升级费用，同时由于这些功能都需要进行大量的运算，还需要进行硬件配置的升级，进一步增加了成本，而且很多厂家的路由器不具有这样的高级安全功能。可以得出：。具有防火墙特性的路由器成本 > 防火墙 路由器 。具有防火墙特性的路由器功能 。具有防火墙特性的路由器可扩展性 综上所述，可以得出结论：用户的网络拓扑结构的简单与复杂、用户应用程序的难易程度不是决定是否应该使用防火墙的

标准，决定用户是否使用防火墙的一个根本条件是用户对网络安全的需求！即使用户的网络拓扑结构和应用都非常简单，使用防火墙仍然是必需的和必要的；如果用户的环境、应用比较复杂，那么防火墙将能够带来更多的好处，防火墙将是网络建设中不可或缺的一部分，对于通常的网络来说，路由器将是保护内部网的第一道关口，而防火墙将是第二道关口，也是最为严格的一道关口。