防火墙路由、专业防火墙应用对比分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E9_98_B2_E7_81_AB_E5_A2_99_E8_c101_461669.htm 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！ 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。 