基于Linux的分布式防火墙设计与实现 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__E5_9F_BA_E4_BA_8ELinu_c103_260892.htm 摘要：防火墙在网络安全中起着重要作用。但是，目前传统的边界防火墙暴露出越来越多的缺陷，无法适应新的网络应用。分布式防火墙是对传统防火墙的改进。文中介绍了分布式防火墙的概念，并给出了其在Linux上的设计与实现。 关键字：分布式防火墙；KeyNote信任管理系统；安全策略；安全凭证；Linux平台。 1 传统防火墙及其缺陷 防火墙是指设置在不同网络或网络安全域之间，根据一定的安全策略对网络间的通信实施访问控制的一系列部件的组合。 传统意义上的防火墙就是指边界防火墙，它将网络分为内网和外网两部分。它是网络间信息传输的唯一出入口，能够根据安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的重要的、基本的安全装置。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监控了内部网和Internet之间的任何活动，保证了内部网络的安全。 传统防火墙依赖于网络的拓扑限制，它假定内网上的所有主机都是可信任的，而外网上的所有主机都是不可信的。当网络遵照拓扑限制时，这种模型工作得很好；但是，随着网络连接的扩充和新的网络应用的发展，这种模型暴露出了越来越多的缺陷，面临着极大的挑战。主要表现在： (1) 对绕过防火墙的攻击无能为力；如果防火墙的规则设置不当，内网上的所有主机将暴露在外部攻击的直接威胁之下。 (2) 由于信任内网上的所有主机，而

对来自网络内部的恶意攻击、未授权访问或无意的误操作“视而不见”。(3) 是潜在的通信瓶颈和单一故障点。(4) 与端到端加密（如VPN）有冲突。(5) 由于依赖于网络拓扑，无法支持移动计算。为了克服上述缺陷，产生了“分布式防火墙”（Distributed Firewall）的概念。2 分布式防火墙 多台基于主机但受集中管理和配置的防火墙组成了分布式防火墙。在分布式防火墙中，安全策略仍然被集中定义，但是在每一个单独的网络端点（例如主机、路由器）上实施。分布式防火墙中含有三个必需的组件：(1) 描述安全策略的语言。(2) 安全地发布策略的机制。(3) 应用、实施策略的机制。安全策略语言规定了哪些通信被允许，哪些通信被禁止，它应该支持多种类型的应用，还应支持权利委派和身份鉴别。策略制定后被发布到网络端点上。策略发布机制应该保证策略在传输过程中的完整性和真实性。策略发布有多种方式，可以直接“推”到终端系统上，可以由终端按需获取，也可以以证书的形式提供给用户。策略实施机制位于要保护的主机上，在处理出入的通信之前，它查询本地策略再做出允许或禁止的决定。分布式防火墙克服了传统防火墙的缺陷，它的优势在于：(1) 在网络内部增加了另一层安全。(2) 有效抵御来自内部的攻击。(3) 消除网络边界上的通信瓶颈和单一故障点。(4) 支持基于加密和认证的网络应用。(5) 与拓扑无关，支持移动计算。3 总体设计 分布式防火墙的前两个组件从本质上说是安全授权问题。传统的授权机制包括访问控制列表（ACL）和公钥证书体系（X.509、PKI）。但是ACL不适用于开放、动态的分布式环境，证书体系在授予权限、信任模式、委托权利等方面也不能很好地满足分布式防火墙的要求。