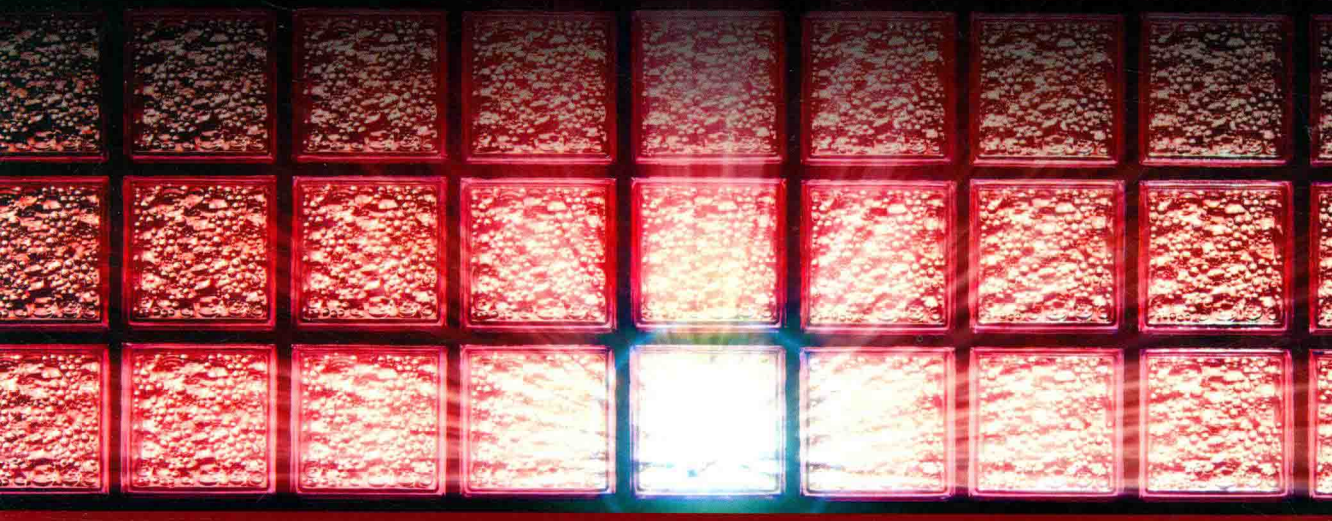
Pearson



Linux 防火墙

（第4版）

[美] Steve Suehring 著　　王文烨 译

LINUX® FIREWALLS

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

Linux 防火墙

（第4版）

[美] Steve Suehring 著　　王文烨 译

LINUX® FIREWALLS

人民邮电出版社
北京

图书在版编目（CIP）数据

Linux防火墙 : 第4版 / (美) 史蒂夫·苏哈林
(Steve Suehring) 著 ; 王文烨译. -- 北京 : 人民邮电
出版社, 2016.11
ISBN 978-7-115-43633-7

Ⅰ. ①L… Ⅱ. ①史… ②王… Ⅲ. ①Linux操作系统
②计算机网络－防火墙 Ⅳ. ①TP316.89②TP393.08

中国版本图书馆CIP数据核字(2016)第243346号

版权声明

◆ 著　[美] Steve Suehring
译　王文烨
责任编辑　傅道坤
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

◆ 开本：800×1000　1/16
印张：22.25
字数：490 千字　2016 年 11 月第 1 版
印数：1－2 000 册　2016 年 11 月北京第 1 次印刷

著作权合同登记号　图字：01-2016-2070 号

定价：79.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315

内容提要

本书是构建 Linux 防火墙的权威指南，包括如何使用 Linux iptables/nftables 来实现防火墙安全的主题。本书共分三大部分。第 1 部分为数据包过滤以及基本的安全措施，其内容有：数据包过滤防火墙的预备知识、数据包过滤防火墙概念、传统的 Linux 防火墙管理程序 iptables、新的 Linux 防火墙管理程序 nftables、构建和安装独立的防火墙。第 2 部分为 Linux 防火墙的高级主题、多个防火墙和网络防护带，其内容有：防火墙的优化、数据包转发、NAT、调试防火墙规则、虚拟专用网络。第 3 部分则讲解了 iptables 和 nftables 之外的主题，包括入侵检测和响应、入侵检测工具、网络监控和攻击检测、文件系统完整性等内容。

本书适合 Linux 系统管理员、网络安全专业技术人员阅读。

序言

欢迎阅读本书。本书介绍了在运行 Linux 的计算机上建立防火墙所需要的各方面内容。在开始介绍 Linux 下的防火墙 iptables 以及最新的 nftables 之前，本书会介绍一些基础的内容，包括网络、IP 以及安全。

本书的读者应该使用一台运行着 Linux 的计算机，不论该计算机是单机的还是作为防火墙亦或是作为互联网网关。本书讲解了如何为单一的计算机例如台式主机构建防火墙，同时也展示了如何为可以托管多台计算机的本地网络构建防火墙。

本书最后的部分介绍了除 iptables 和 nftables 之外的计算机和网络安全相关的因素。这部分包括了入侵检测、文件系统监控以及监听网络流量。本书很大程度上是与 Linux 版本无关的，这意味着任何流行的 Linux 发行版都可以使用书中的内容，只需要很小的调整或无须调整。

关于作者

Steve Suehring 是一位擅长 Linux 和 Windows 系统以及开发的技术架构师。Steve 在技术领域著有多本书籍和杂志，涉及方面颇广。在他担任 *LinuxWorld* 杂志的编辑期间，他编著和修订了关于 Linux 安全方面的文章和综述，以及 Linux 在一级方程式赛车中的使用的专题报道。

致谢

我要感谢我的妻子、家庭以及朋友们，感谢他们无尽的支持。同时也感谢 Robert P.J. Day 和 Andrew Prowant，感谢他们审阅本书的草稿。

目录

第 1 部分

数据包过滤以及基本安全措施

第1章

数据包过滤防火墙的预备知识

一个小型站点可能会通过多种方式连接到互联网，如T1专线、电缆调制解调器、DSL、无线、PPP、综合业务数字网（ISDN）或者其他的方式。直接连接到互联网的计算机通常是安全问题的焦点。无论是一台计算机还是由连接起来的多台计算机所组成的局域网（LAN），对于小型站点来说，最初的焦点将是直接连接到互联网的那台计算机。这台计算机将被用来搭建防火墙。

防火墙（firewall）这个术语根据其实现方式和使用目的不同而有多种不同的含义。在本书中，防火墙意味着直接连接到互联网的计算机。防火墙也是针对Internet访问实施安全策略的地方。防火墙计算机的外部网卡便是连接到互联网的连接点，或称为网关（gateway）。防火墙存在的意义是保护网关内部的站点免受外部威胁。

一个简单的防火墙设置有时被称作“堡垒防火墙”，因为它是您抵御外部攻击的主要防线。您的许多安全措施都建立在这位保卫您领地的“卫士”之上。它会尽一切可能来保护系统安全。

在这条防线之后的是您的一台或一组计算机。充当防火墙的计算机所扮演的角色可能只是简单地作为您局域网中其他计算机连接到互联网的连接点。您可以在防火墙后的计算机上运行本地的私有服务，例如共享的打印机或者共享的文件系统，或者让您所有的计算机都能连接到互联网。您的某台计算机上可能会存放着您的私人财务记录。您也许想让这台计算机访问Internet，但您不会想让任何人来访问这台计算机。有时，您可能希望向互联网提供您自己的服务。局域网中的某台计算机可能会托管着您的个人站点，另外一台计算机则可能会作为邮件服务器或者网关。您的设置和目的将决定您的安全策略。

防火墙存在的目的是为了执行您定义的安全策略。这些策略反映了您所做出的决策：允许哪些Internet服务访问您的机器，通过您的计算机向外提供哪些服务，哪些服务只为特定的远程用户或站点提供，哪些服务和程序您只希望在本地运行以便仅供您私人使用。安全策略实际上就是访问控制和授权使用私有及受保护的服务、程序以及您计算机上的文件。

虽然家庭和小型企业系统并不会遇到大型公司站点所面临的全部安全问题，但设置安全策略的基本思路和步骤仍是相同的。只是无需考虑那么多的因素，而且安全策略通常没有大型企业站点那样严格，其重点在于保护您的站点免受互联网上不速之客的访问。数据包过滤防火墙

是一种常用的保护网络安全和控制外部访问的方法。

当然，拥有防火墙并不意味着您拥有了全面的防护。安全是一个过程，而不是一块硬件。例如，尽管有防火墙的存在，仍有可能通过下载间谍软件、广告软件或点击恶意邮件，使计算机的防护之门大开，继而招致外部对网络的攻击。采取措施以消除外部攻击所带来的危害与在防火墙上花费资源同样重要。在您的网络中使用最佳实践将有助于减少您的计算机被恶意使用的机会，并给予您的网络以弹性。

需要记住的一点是，互联网模式（Internet paradigm）是基于端到端透明这一前提的。对于正在通信的两台计算机来说，两者通信所使用的网络对二者来说是不可见的。实际上，如果通信路径上的某个网络设备失效，则两台计算机之间的流量会在两台计算机不知道的情况下通过新的通信线路继续传输。

理想情况下，防火墙应该是透明的。然而，防火墙可以通过在两台端点计算机之间的网络内引入单一故障点，来破坏互联网模式（Internet paradigm）。而且，并不是所有的网络应用程序使用的通信协议都能轻易通过一个简单的数据包过滤防火墙。如果没有额外的应用程序支持或更加复杂的防火墙技术，则不可能使特定流量穿越防火墙。

更加复杂的问题就是网络地址转换（Network Address Translation[NAT]，Linux 的说法是地址伪装）了。NAT 使得一台计算机能够通过转换多台计算机的请求并将它们转发至相应的目的地从而代表很多其他的计算机。NAT 和 RFC 1918 定义的私有 IP 地址的使用有效地减轻了即将出现的 IPv4 地址短缺。但 NAT 和 RFC 1918 私有地址空间的结合会使得某些类型的网络流量要么难以传输，要么需要复杂的技术或昂贵的成本才能完成传输。

> 注意：
>
> 很多路由器设备，尤其是那些用于 DSL、电缆调制解调器和无线通信设备，通常以防火墙的名义出售，但它们实际上顶多算一个启用了 NAT 的路由器。它们并不会执行许多真正的防火墙所能够实现的功能，但它们确实将内部和外部的网络隔离开了。在购买路由器时，请警惕那些号称是防火墙但只提供 NAT 功能的产品。尽管它们中的有些设备拥有一些不错的功能，但通常没有更为高级的配置功能。

最后一个复杂的地方来源于多媒体和点对点（P2P）协议的广泛使用，它们在实时通信软件和网络游戏中都有应用。这些协议与当今的防火墙技术相互对立。现如今，特定的防火墙解决方案必须对每一个应用协议单独进行建立和部署。而那种简单地、经济地处理这些协议的防火墙架构仍处在标准委员会的工作组的讨论中。

我们应该牢记，混合使用防火墙、DHCP 和 NAT 会引入复杂性，导致站点为了满足用户使用某些网络服务的要求，不得不对系统的安全性做出一定程度的让步，理解这一点至关重要。小型企业通常不得不部署多个局域网和更复杂的网络配置，以满足不同本地用户的多种安全需求。

在深入了解开发防火墙的细节之前，本章将先介绍数据包过滤防火墙的基础概念以及机制。