基于 Netfilter 架构的网络防火墙设计与实现

冯雁辉[1]　陆华英[1]　蒋彭[2*]
（1. 上海开放大学静安分校　上海市　200040　2. 上海市静安区业余大学　上海市　200040）

摘　要：本文基于 Netfilter 架构网络防火墙的研究，其主要设计的思路是在一个现实的网络环境中，使用 Netfilter 的配置工具 iptables 来设置一系列防火墙系统的管理命令，用于建立一套处理数据转发和过滤的规则，并能够依据这个预先设定的数据转发过滤规则，来检测内外网络之间所传输数据的网络层报头中的信息源，比如用于控制数据包流的源地址、目的地址、传输的数据类型等信息，从而确保用户的网络能够安全、稳定、顺畅地运行。

关键词：网络防火墙；数据包过滤；通用架构；内核模块

Web Server 的浏览访问不仅增加了数据流量，也同时大大增加了网络被攻击的可能性。在传统的网络架构中，对网络的管控通常采用加密、用户认证、访问控制或是行为审计和事件日志等形式，从而实现集中而统一的网络安全管理。但是在 Internet 网络环境中，网络的架构相对复杂，网络访问形式多样，网络中交互的数据量巨大，所以 Internet 的网络安全技术需要把在传统网络中的所采用的安全技术与分布式网络的安全技术相结合，这样的集成化网络安全管理系统才能实现在 Internet 中安全的数据通信，同时保护用户内部的网络环境不受外部非法访问。正是基于这样的目的，网络防火墙技术才得到了深入的研究。

基于 Netfilter 架构的网络防火墙的研究是在当下网络宽带工程的进展日新月异，网络应用深入普及的背景下，利用在用户的网络系统内核中嵌入了 Linux 所提供的防火墙系统软件的方式，从而来确保用户的网络能够安全、稳定、顺畅地运行。这种网络防火墙实现技术是建立在首先对通信数据包进行检测，再完成转发过滤。所以使用 Netfilter 设置防火墙，就是使用其中的配置工具 iptables 来设置一系列防火墙管理命令，用于管理用户设置的数据转发和过滤规则。

本文主要介绍了一种基于 Linux 的内核软件包来构建一种网络防火墙的设计方法，依据用户预先设定的数据转发过滤规则来检查通信双方数据包中的地址信息和连接状态信息。这样就可以在现有的用户网络系统基础上，很方便的构建一个理想的、实用的网络防火墙系统，实现对用户内部网络环境的安全保护。

1　安全的网络体系结构

Netfilter 是 Linux 内核中一种常见的体系结构，通过提供一个抽象的、通用化的框架，来建构一套基于通信数据包转发过滤的网络防火墙系统。其设计思想是根据网络层报头中的源地址、目的地址和传输数据类型来控制数据包的流向。在数据传递的过程中，可以依据指定的数据转发和过滤规则，检测所传递的数据包的源端口、目的端口和连接状态。其中 Netfilter 建立了一系列的数据处理规则表，这些表由一些完成相应数据处理的数据链构成。每个链可以由一个或多个进行数据包转发和过滤的规则组成，这些规则决定了接收到的数据是转发还是过滤。用户的网络架构如图 1 所示。

在这个安全的用户网络环境中，可以实现如下的一些功能。通过线路①将服务器集群接入用户网络的中心交换机，用户网络环境中的所有用户均可访问到相应的服务器集群，从而实现了网内用户与各类服务器主机之间的数据传递，并

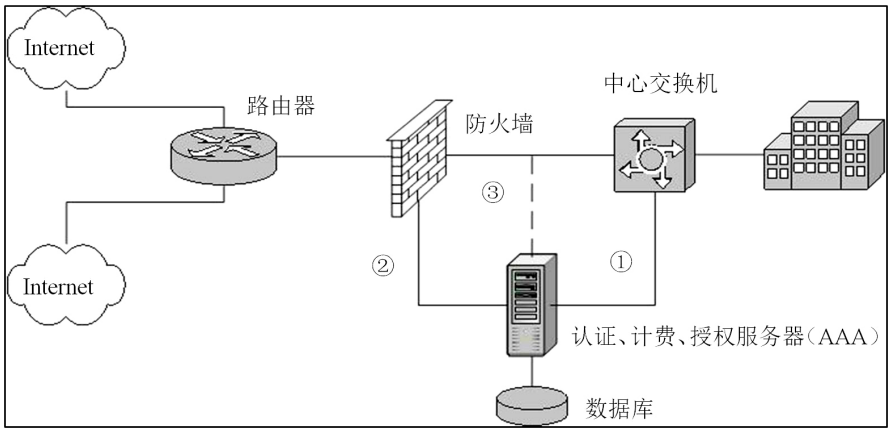

图 1：网络架构

● 基金项目：上海开放大学 2019 年学科创新项目“系统构建开放教育综合素质课实践研究”（项目编号：XK1904）阶段性成果；2021 年上海市静安区教育科研重点课题（项目编号：ZS202102）阶段性成果。

表 1：系统实现的主要功能

线路	实现功能
①	将认证、授权服务器接入用户网络的中心交换机，网内用户均可访问到相应的服务器集群，实现了网内用户与服务器主机之间的数据传递，并为用户完成安全认证。
②	沟通了防火墙与认证、授权服务器，便于由服务器集群来控制防火墙，完成相应的配置和管理，为授权提供了通讯条件。
③	此线路不用于网络通讯，而是为认证、授权服务器捕获数据（防火墙 <-> 中心交换机）提供条件。

表 2：钩子函数位置

PREROUTING	在路由选择的决策之前
INPUT	数据包将要被转发到本地 socket 之前
FORWORD	经过本地转发的数据包
OUTPUT	本地发出的数据包
POSTROUTING	路由选择决策后转交给硬件处理之前

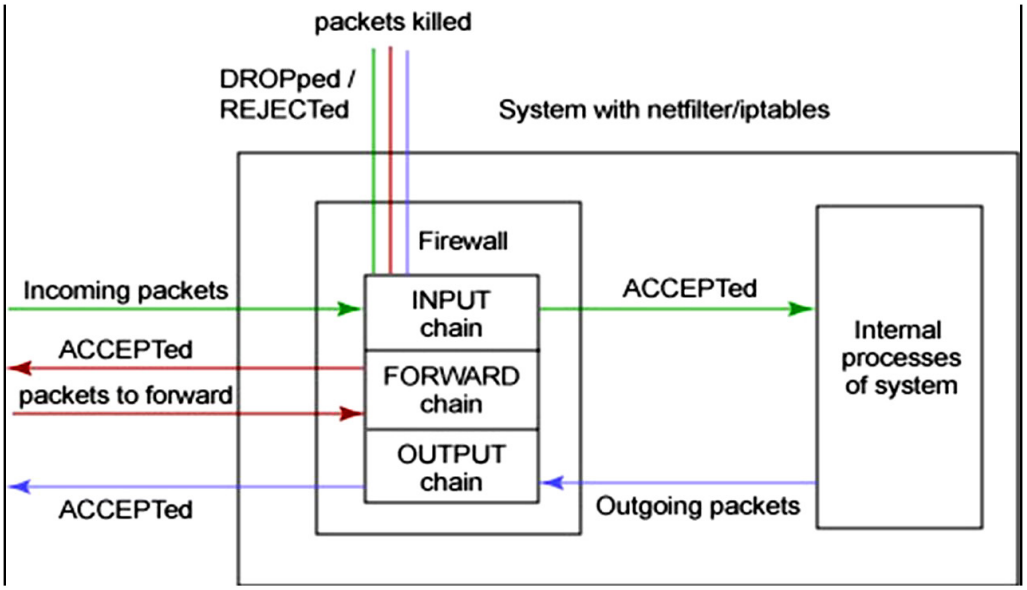

图 2：数据包转发过滤过程

使用相应的服务功能，为用户安全认证提供了通讯条件；通过线路②实现了防火墙与服务器集群之间的数据交互，并可以由服务器集群来控制防火墙，完成配置和管理，为网内用户的对外授权数据传递提供了通讯条件；线路③为服务器集群捕获数据（位于防火墙与中心交换机之间）提供条件。系统实现的功能如表 1 所示。

2 基于Netfilter的防火墙策略设计

2.1 使用配置工具iptables建立规则和链

Netfilter 架构中数据包转发过滤系统为各种协议提供了一组操作函数，也称为钩子函数。这些函数设置在通信双方传输数据包的线路上。根据数据包的来源地址和目的地址，可以将数据包分为接收数据、转发数据、流转数据三种类型。通过路由选择可以区分出这些相应的数据包类型，确定是接收、转发还是流转的数据。在通信路径中这些钩子函数对应的位置，分别如表 2 所示。

在 Netfilter 架构中，数据包转发过滤系统由名为 Netfilter 和 Iptables 的两部分组成。可以使用这两个组件设计数据包的转发过滤规则，这些规则是防火墙系统所遵循的依据，以便防火墙系统对接收到的数据进行进一步的操作。其中的 Netfilter 组件，是 Linux 系统内核组成的一部分，主要的构成元素被称之为表，在这些表中包含了用户定制的用来控制数据包转发和过滤的一系列的操作规则。

而 Iptables 组件则是完成对这些表中的数据处理规则进行插入、修改、删除等操作的工具，也称为用户空间。在网络环境中，通信双方在进行数据传递的过程中，通过向防火墙系统提供依据数据包的地址或控制协议等信息来进行数据处理的指令，以此来确定数据的转发和过滤。

可以使用 Netfilter /iptables 系统提供的 iptables 命令来创建和编辑这些数据转发过滤规则，并将它们添加到内核空间

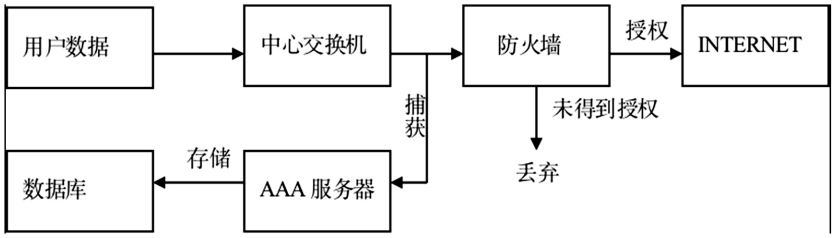

图 3：系统中数据包的操作过程

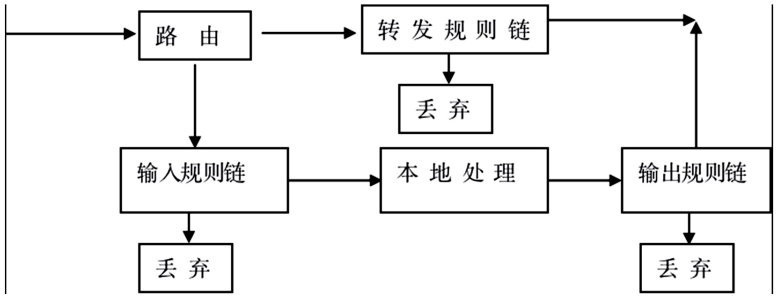

图 4：Netfilter 系统中数据包传输数据流向

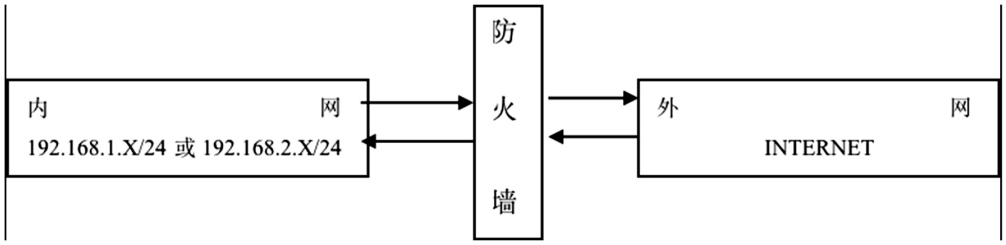

图 5：网络结构简图

的数据包转发过滤表中的数据处理链中。数据包转发过滤过程如图 2 所示。

如前所述，利用 Iptables 组件可以建立针对用户的数据包转发过滤规则，这些对数据包的数据处理规则存储在 Netfilter 组件的数据包转发过滤表中。根据所处理的数据包的类型，可以将这些数据包处理规则分组，并分类归并到相应的数据处理链中。其中，处理本地接收的数据包的规则，也称为入站数据包，被添加到输入规则的数据处理链中。输出规则的数据处理链中添加了处理发送到外部网络的数据包的规则，也称为出站数据包。转发规则的数据处理链中加入了对正在进行路由的数据包的处理规则。

这里的数据包转发过滤的处理过程是将所接收到的数据包的头信息提取出来，与它所在的数据处理链中的每个规则进行比较，看它是否完全匹配某一转发过滤规则。如果与其中的处理规则相匹配，那么将会对依据该规则显式指定的数据包执行对应的操作，也就是对这个数据包完成相应的授权操作。如果数据包的头信息与当前的这个处理规则相互不匹配，那么就会再与数据处理链中的下一条规则进行比较。最后，如果数据包与这个数据处理链中任意的规则都不匹配，那么最终将会引用数据处理链的策略来决定如何处理这个数据包。在系统中对接收到的数据包的操作过程如图 3 所示。

2.2 Netfilter的数据包传输

Netfilter 的 iptables 组件使用这些预先编辑的数据包转发过滤规则来控制接收到的数据包处理操作。这样就可以决定所有进行数据通信的数据包是发送给本地主机输入规则数据处理链，还是选择路由后转发规则数据处理链。

如果这些数据包的目的地址是本地的，则这些数据包在输入规则的数据处理链中被转发过滤规则接受，并在本地接收。如果目的地址是外网中的某个主机，那么这些数据包就会被转发规则链中的规则所接受，并被发送到相应的接口，经过路由选择后转发到外部网络中。用户内部网络中对外发送的出站数据包会被送到输出规则链。如果这个数据包能够被接受，则将被发送给相应的接口，也是经过相应的路由选择后转发出去。Netfilter 系统中数据包传输数据流向如图 4 所示。

3 配置防火墙套件

3.1 网络环境部署

在搭建的用户内部网络环境中已经建立以下服务：web 应用服务，域名为 www.mysite.com；ftp 文件传输服务，域名为 ftp.mysite.com；用于实现防火墙功能的计算机上的网络地址分别设置为 :Eth0(218.197.93.115)、Eth1(192.168.1.1)

、Eth2(192.168.2.1)；服务器 Server 计算机的网络地址为：C（192.168.1.2）；用户内部网络中客户机 A 上的网络地址为：A（192.168.2.2）；客户机 B 上的网络地址为：B（218.197.93.161）。系统的网络结构简图如图 5 所示。

在这个用户网络环境中，防火墙主机既是用户内部网络中的成员，也是外部网络的成员。接外网的网卡可以对用户内部网络传出的数据包做 IP 地址的伪装，这样在内部网络中传出的数据包会将其网络地址转换为一个 Internet 中真正的公网 IP 地址。在本网络环境中使用的 Internet 公网的 IP 地址为 218.197.93.115，在连接内部网络的时候，使用局域网内部的 IP 地址为 192.168.1.1，内部网络中其它用户的计算机可以使用的 IP 地址范围是 192.168.1.2~192.168.1.254。

预期实现的功能包括实现防火墙的地址转换功能，让客户机 A 能访问外部网络（218.197.93.254），在服务器主机上开启 ftp 和 web 服务，使得客户机 A 和 B 能够正常访问服务器主机 C。开启防火墙功能，使得防火墙可以进行网络内部用户数据包的源地址转换，实现用户的内部网络可以正常访问外部网络。并且内部网络用户可以访问 DMZ 区域，实现对 DMZ 区域中服务器的配置和管理。外部网络不能直接访问内部网络中的用户内部数据，但是外部网络由防火墙完成对外网地址到服务器实际地址的转换后，可以访问用户的 DMZ 区域中的服务。

在 /etc/sysconfig/network-scripts 中建立 ifcfg-eth0 文件，编辑如下内容，配置基本的用户网络环境，并配置为自启动状态：

```
# DEVICE=eth0
# IPADDR=192.168.1.1
# NETMASK=255.255.255.0
# NETWORK=192.168.1.0
# BROADCAST=192.168.1.255
# GATEWAY=218.197.93.115
```

3.2 建立规则

实现以下功能：通过防火墙的网络地址转换功能让客户机 A 能访问外部网络（218.197.93.254），在服务器主机上开启 ftp 和 web 服务，使得客户机 A 和 B 主机能够正常访问服务器主机 C，通过防火墙系统进行网络地址转换后实现用户内部网络可以访问外网。编辑如下内容：

```
# establish a static firewall // 建立脚本文件指定开放的端口
Open_ports="80 25 110 10 20 21"  // 设置本地服务器对外开放的端口
Allow_ports="53 80 20 21"  // 允许外部网络访问的本地服务器端口
iptables -A FORWARD -p tcp -d 192.168.1.1 --dport www -i eth1 -j ACCEPT
// 对 www 服务器设置数据包过滤规则
iptables -A FORWARD -p udp -d 192.168.1.0/24 -i eth1 -j ACCEPT
// 对内部网络用户设置数据包转发过滤规则
iptables -A FORWARD -s 192.168.1.0/24 -i eth1 -j ACCEPT
// 对内部网络中传输的数据包进行转发过滤
```

通过编辑用户防火墙系统的数据包转发过滤规则，完成相关安全设置，就建立了一个相对完整的 netfilter 防火墙系统，提供了一种有效的防护手段。对外部的网络服务可以通过某些指定的端口来实现数据交互，同时也提供了用户网络内部对 Internet 的无缝访问，这样也基本实现了外部网络对内部访问时候的入侵检测功能。

4 结束语

在 Linux 内核中使用内置的针对 IP 地址进行处理的数据包过滤工具 Netfilter/ Iptables 系统，使得配置网络防火墙，进行数据包过滤的实现过程相对方便。并且 Netfilter/Iptables 系统不仅为用户提供了对网络防火墙的配置和数据包转发过滤的完全控制，还允许为网络防火墙定制控制数据包转发过滤的规则。

本文主要研究了如何建立一种在系统内核中用于扩展各种网络服务的结构化框架，综合应用网络通信技术和集中化管理技术，其想法是生成一个易于扩展的模块化结构。此外，新的策略和模块规则被添加到系统的内核中，而不需要重新启动内核。所以，通过对系统内核模块的定制编辑，就能够实现对一些网络新特性的扩展。

参考文献

[1] 韩少云编 . 网络与 Linux 安全攻防 [M]. 西安电子科技大学出版社 , 2022.
[2] 赵尔丹，张照枫，袁洲编著 .Linux 系统与网络管理 [M]. 机械工业出版社 , 2022.
[3] 余华兵著 .Linux 内核深度解析 [M]. 人民邮电出版社 , 2019.
[4] 母中旭 .IPTables/Netfilter 技术在中小微企业局域网防火墙的应用 [J]. 科学技术创新 , 2017.
[5] 吴勇杰 .Linux 内核防火墙 Netfilter 架构实现与应用研究 [J]. 电脑编程技巧与维护 , 2013.
[6] 刘飞霞 .Linux 内核中 Netfilter/Iptables 防火墙设置分析 [J]. 西安电子科技大学 , 2012.

作者简介

冯雁辉（1964-），男，工程硕士，讲师。研究方向为程序设计，软件测试。
陆华英（1981-），女，硕士学位，讲师。研究方向为软件工程，教育技术。
蒋彭（1974-）（通讯作者），男，硕士学位，副教授。研究方向为软件工程，教育技术。