第 32 卷 第 4 期 计 算 机 工 程 2006 年 2 月
Vol.32 № 4 Computer Engineering February 2006
·安全技术· 文章编号：1000—3428(2006)04—0163—03 文献标识码：A 中图分类号：TP309

IPv4/IPv6 双栈防火墙的设计与实现

肖文曙，陈 雷，张玉军
(中国科学院计算技术研究所信息网络研究室，北京 100080)

摘 要： IPv6 的新特点和应用对现有的安全设备结构提出了挑战。同时，从 IPv4 升级到 IPv6 是一个长期的过程，两种协议在一定时间内将共同存在。因此，需要设计支持 IPv4、IPv6 双协议的防火墙以适应过渡时期的需要和 IPv6 新特点对防火墙的要求。论述了 IPv4/IPv6 防火墙的设计需要考虑的防火墙位置、IPv6 与 IPv4 的差异及性能，然后介绍防火墙实现的步骤和将要进行的工作。
关键词： 防火墙；IPv6；IPSec

Design and Implementation of IPv4/IPv6 Firewall

XIAO Wenshu, CHEN Lei, ZHANG Yujun
(Information Network Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

【Abstract】 The adoption of IPv6 will impact today's network security architecture. Firewall is one of the main points of security architecture. This paper discusses how to design firewall to match the requirement of next generation network based on IPv6. This paper focuses on the problems that should be taken into consideration when designing firewall system for the network environment that both IPv4 and IPv6 exist. Then, the work on firewall is introduced and the following work is presented.
【Key words】 Firewall; IPv6; IPSec

随着 Internet 的迅速增长和无线设备的激增，现行的 Internet 协议 IPv4 在地址空间、端到端的 IP 连接、服务质量、网络安全和移动性等方面都暴露出了不足，极大地限制了 IP 网络的进一步发展。而 IPv6 所提供的巨大的地址空间以及所具有的诸多优势和功能，获得了普遍关注和广泛认可。

然而，从 IPv4 升级到 IPv6 不是一二天内完成的，IPv4 与 IPv6 系统在一段时期共存是不可避免的事实。IPv6 协议的一个重要设计目标是与 IPv4 兼容。在这个阶段，IPv6 节点之间的通信依赖于现有 IPv4 网络的设施，而且 IPv6 结点也必不可少地要与 IPv4 结点通信，对于同时支持两种协议的主机，攻击者可以同时使用两种协议协调作战，对于安全产品，应该同时支持两种协议，并联系起来分析，才能真正起到保障安全的作用。这对于网络安全提出了新的要求。研究 IPv4/IPv6 过渡阶段下的新的安全体系设计是非常必要的。IPv6 利用 IPsec 实现了网络层的加密与认证，部分解决了现有网络协议 IPv4 存在的安全问题，但是，相关的密钥交换、加密算法等标准都不成熟，IPSec 的提出仍然替代不了传统安全设备，如防火墙和入侵检测系统。已有公司开始进行基于 IPv6 防火墙的研究和开发。设计 IPv4/IPv6 过渡阶段的防火墙，是构造过渡阶段安全体系结构的重要部分，对保障 IPv6 的实现有着重要的意义。

1 防火墙的设计思想

防火墙的设计需要考虑防火墙的位置，即其与网关的相对位置，此外，防火墙 IPv6 部分与 IPv4 部分的差异和防火墙性能也是必需的考虑。

1.1 过渡阶段防火墙的位置

在 IPv4、IPv6 共存的环境下，针对 IPv6 小岛之间的通信以及 IPv6 小岛和 IPv4 海洋之间的通信，需要网关支持隧道技术和协议转换技术，防火墙实施安全策略时要考虑与网关的交互。

针对 IPv6 小岛之间通信的解决方案，这些方案都是在隧道的基础上实施的，出口路由器是隧道的起点或终点，路由器通向外网的数据包格式都是同一类型的隧道包格式，内网的数据包是普通的 IPv6 包，因此防火墙可以统一实施安全策略，根据防火墙的位置不同，实施的安全检测也不同：

·防火墙放置在出口路由器(隧道端点)外面，可以保护路由器免遭攻击，流经防火墙的数据包是普通的 IPv4 数据包或 IPv4/IPv6 隧道包，如果隧道包没有被 IPSec 协议进行加密处理，防火墙可以读取隧道包内的 IPv6 报头分析过滤；

·防火墙位于出口路由器(隧道端点)与内部网络之间，流经防火墙的数据包是普通的 IPv4 数据包(内部 IPv4 主机或双栈主机之间的 IPv4 通信数据)或 IPv6 数据包，防火墙直接对 IPv6 报头分析过滤；

·防火墙与出口路由器(隧道端点)集成在一起，防火墙在数据包进入隧道封装之前或从隧道解包出来时对数据包分析过滤，此时防火墙分析的数据包是 IPv6 数据。

我们的防火墙针对 IPv6 小岛之间的通信要求，放置在出口路由器与内部网络之间，流经防火墙的数据包是普通的 IPv4 数据包(内部 IPv4 主机或双栈主机间的 IPv4 通信数据)或 IPv6 数据包(内部 IPv6 主机或双栈主机之间的 IPv6 通信数据)。

1.2 防火墙需要考虑的 IPv6 与 IPv4 的差异

IPv4/IPv6 环境下，防火墙 IPv6 部分的设计需要考虑 IPv6

基金项目： 国家计算机网络与信息安全管理中心招标项目“IPv6 信息过滤技术”
作者简介： 肖文曙(1980—)，女，博士生，主研方向：信息网络安全；陈 雷，硕士生；张玉军，博士
收稿日期： 2005-02-06 **E-mail：** wsxiao@ict.ac.cn

不同于 IPv4 的特点：

IPv6 报头与 IPv4 报头的差异是对 IPv6 包进行过滤时需要考虑的，IPv4 防火墙的过滤器在工作的时候对于 IPv4 选择性包头部分并无考虑，在 IPv6 下，确定特定扩展报头的有无是过滤时必须考虑的，同时，IPv4 的 IP 报头和 TCP/UDP 报头紧接在一起，且长度基本固定，防火墙很容易找到 IP 地址和 TCP/UDP 端口信息，进行过滤，而 IPv6 的扩展报头存在于两者之间，对过滤器寻找地址及端口信息带来麻烦，影响效率。

IPsec 是 IPv6 必需的功能，如果 IPsec 要在 IPv6 的环境中使用，经过加密的数据如何过滤是必须解决的问题，一个加密的通道允许使用者跳过安全性的检查。IPsec 也是 IPv4 可选的功能，在现在的 IPv4 网络中，IPsec 一般用于 VPN 环境中，设置于两个网关之间，而没有用于两个端系统之间。在 IPv6 环境下，要实现端对端的 IPsec 安全首先必须解决如何过滤加密数据的问题。为解决这个问题，有人提出在防火墙处打断连接。这样将有两个加密通道：一个从外部主机到防火墙；一个是从防火墙到内部主机，这个办法的主要问题是会打破端到端的模式。

对移动的更好的支持是 IPv6 的重要应用。这同时会给防火墙带来过滤上的困难，因为对过滤器来看网络变得分散。一个外地的主机移动到本地，防火墙要能判断出这个移动节点而不能把它当成非法的，为做到这一点防火墙要能分析协议并具有授权功能。

我们的防火墙在实现中，考虑到 IPv4 和 IPv6 的这些差异，实现了通过地址端口号等信息对 IPv6 数据包的过滤，对 IPsec 和移动的支持在防火墙的下一步工作中进行。

1.3 防火墙性能考虑

在 IPv4/IPv6 过渡阶段的网络环境下，网络流量大大增加，而防火墙处于内部网络通向外部网络的出口处，过滤通信数据包将付出性能代价，CPU 的大量时间将用来检查规则表，当更快的通信抵达时这个问题会变得更严重。因此应该尽量减轻防火墙负担。首先，防火墙在 Linux 系统下实现，首先需要精简系统的内核。同时，从过滤方法考虑，我们采用状态包过滤防火墙辅助少量应用层控制策略，同时由入侵检测系统辅助防火墙实施访问控制策略，达到安全性与性能的折中。

2 防火墙系统的初步实现

要实现 IPv4/IPv6 防火墙，首先就是要实现防火墙对双协议栈的支持，使防火墙具备 IPv4、IPv6 包处理的能力；要设计防火墙的安全策略，包括网络的划分，网络间通信的基本策略；要实现防火墙的管理部分，提供对用户的接口，并提供通过 IPv4、IPv6 两种地址对防火墙访问的能力。下面介绍我们设计的防火墙总体结构和实现步骤。

2.1 防火墙结构

防火墙由 Web 管理系统和内核部分组成，Web 管理系统通过通用网关接口为用户提供一个管理配置的接口，也给防火墙提供一种控制存储防火墙规则的脚本。这个部分包括 Web 管理界面、通用网关接口、Web 服务器。内核部分实现网络数据包处理、分发的核心工作，包括安全策略模块、包过滤模块、日志统计模块以及其他功能模块。

(1) Web 管理系统

Web 管理系统负责与用户的交互。用户通过浏览器登陆管理界面，设置防火墙的参数，进行过滤规则的配置，用户输入的数据通过该接口传回防火墙系统，应用程序将这些数据作为参数，写入相应的配置文件中。

(2) 安全策略设计

防火墙安全性的基础是首先要建立一套合理的科学的可操作的安全策略。本防火墙系统采用了一种适用于混和军用网络的新型的安全策略，具有较高的安全性和开放性。防火墙区分 3 个不同的网络，分别为绿网--内网、红网--外网、橙网--非军事化区。最基本的安全策略是：允许内网的用户访问非军事区，允许可信站点的外网用户访问非军事区，允许内网用户访问外网可信站点，不允许外网用户访问内网。

(3) 防火墙过滤模块

防火墙过滤模块包过策略表和会话状态表，依据策略表规则进行过滤，这些规则告诉防火墙数据包是否合法以及对于来自某个源、至某个目的地或具有某种协议类型的网络流量要做些什么，而会话状态表使得同一会话的数据包无须逐个匹配过滤规则，提高性能。

2.2 防火墙的实现步骤

按照防火墙设计时的考虑，为提高性能，首先进行精简内核的工作，然后实现管理、包过滤、日志模块。

2.2.1 精简内核

防火墙实现在一个小型 Linux 上，为提高防火墙的性能，首先精简 Linux 系统内核。如果不需要的模块被放在 Linux 的系统内核中，每次在系统启动时这些没有的内核模块会加载到系统内核中，系统内核的运行效率会大打折扣。

重新编译内核，在内核配置时去除所有可以拿掉的选项，并且要注意选中 IPv6 相关选项。要大幅度精简核心，就需要裁剪文件系统。Linux 的 VFS 简化了档案系统的设计，增加了系统的效率。但这些嵌入系统根本就用处不大，把它们去除。编译内核和模块，将编译好的文件移到启动目录下，用新内核替换原有内核。

2.2.2 实现管理模块部分

配置 apache 服务器，从而可以通过 IPv6 地址访问防火墙，进行管理操作。

假定防火墙内部 IPv4 地址设为 192.168.6.10，IPv6 地址为 2002:250:f007:1::400,Web 服务端口号为 81，则在浏览器中键入 HTTP://192.168.6.10:81 或 HTTP://[2002:250:取 f007:1::400]:81 可以登录到防火墙。

我们使用 Perl 语言编写管理页面及响应程序，该部分由核心管理程序和功能模块组成。核心管理程序有 Perl 脚本和几个 CGI 脚本，分包括核心库、管理中心的首页和模块管理。

功能模块完成某一特定功能的参数设置或数据的显示等。模块的一般结构如表 1 所示。

表 1 功能模块列表

目录或文件	说明
functionnanme.cgi	该模块的首页
config	缺省的配置文件
config.info	对配置文件中置选项的说明
image/	存放模块中用到的图片
lange/	页面信息中的各种语言版本

2.2.3 实现包过滤模块部分

该部分实现网络数据包处理、分发的核心工作，实现采用 C 语言和脚本语言编程。

防火墙内核的开发建立在 Linux netfilter 架构的基础上。Netfilter 是 Linux2.4 内核实现数据包过滤/数据包处理/NAT 等的功能框架，Netfilter 提供了一个抽象、通用化的框架，为每种网络协议(IPv4、IPv6 等)定义一套钩子函数，这些钩子函数在数据报流过协议栈的几个关键点被调用。在这几个

点中，协议栈将把数据报及钩子函数标号作为参数调用 netfilter 框架。

防火墙过滤表通过钩子函数 NF_IP_LOCAL_IN, NF_IP_FORWARD 及 NF_IP_LOCAL_OUT 接入 netfilter 框架。因此对于任何一个数据报只有一个地方对其进行过滤。

防火墙对数据包过滤的过程是: 系统首先根据 IP 协议版本确定其通过 IPv4 协议栈还是 IPv6 协议栈，然后检查接收数据包的校验和是否正确，字段数据值是否合法。如果数据包没有错误，系统对会话表进行搜索，寻找与当前会话匹配的条目，如果没有搜索到匹配的会话，系统根据数据包的属性检查策略表以判断对当前数据包实施的策略，如果策略允许数据包通过，当前会话就被加入会话表。

如果系统在会话表中搜索到匹配的会话，系统检查序列号的合法性，以确保当前数据包是会话的一部分。数据包会话状态检查有效后，系统对数据包进行地址翻译或者计算路由，然后发送数据包。如果不通过，系统就丢弃当前数据包并记录日志信息。

2.2.4 实现日志统计和流量分析

在过滤规则设置时，对于要被丢弃的数据包，首先送到目标 LOG，LOG 将匹配的数据报传递给 syslog()进行记录，写入系统日志文件。应用程序读取文件，根据模式匹配找出希望显示的记录显示在管理页面的“日志”页。

流量分析使用了一个生成流量分析图表的工具 rrdtool，和定时执行任务的软件 cron。在 crontab 文件中，写入命令

*/30 * * * * root /usr/local/bin/rrdtool.pl > /dev/null

此命令每隔 30min 调用一次 rrdtool.pl，获取网卡的数据包进出流量信息，调用 rrdtool，将流量信息反映到管理界面的流量图页。该页有若干张流量图，分别是 3 个网卡一天、一个月、一年的流量状况图。根据这些图表，可以对经过防火墙的流量进行分析统计。

4 防火墙系统说明

防火墙配置部分主要有如下模块:

(1) 防火墙接口参数设置该功能模块用于进行内网，非军事区，外网的地址参数配置。根据管理员的输入，将接口的 IPv6 地址、IPv4 地址等数据写入配置文件，后台程序读取该文件，执行实际的配置操作。

(2) IPv6 包过滤规则设置。模块用于 IPv6 包过滤策略设定，本设置用于添加、修改、删除防火墙规则链，根据数据包的输入输出接口、源地址、源端口、目的地址、目的端口、协议类型来过滤(图 1)。

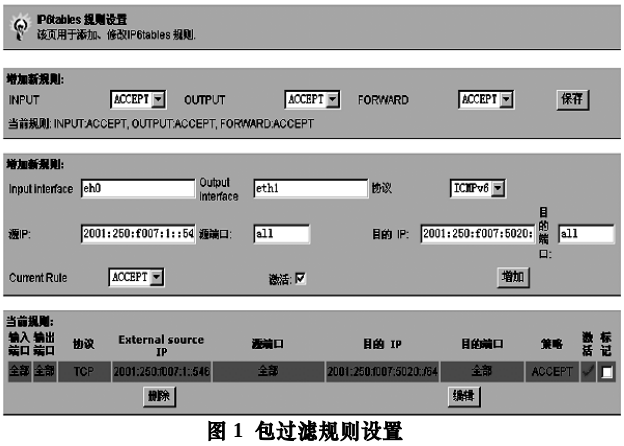

图 1 包过滤规则设置

(3) IPv6 路由配置。我们的防火墙属于分组过滤路由器防火墙系统。在此处进行系统的路由设置。对防火墙的 IPv6 路由表进行操作，对防火墙进行路由设置。对于IPv6的功能模块，防火墙有相应的IPv4模块: IPv4 包过滤规则设置，IPv4 路由配置。

(4) 日志查询模块。防火墙有完善的日志功能，对防火墙所控制的活动进行记录。有对外部主机的访问的日志，对被阻断的 v6 或 v4 数据包有确切的记录。日志的实现是通过程序调用系统命令将被阻断的数据包信息写入日志文件并将信息显示出来。

(5) 防火墙流量分析模块。防火墙有流量分析功能，对通过防火墙的流量状况进行统计分析，并形成直观的图表。

5 防火墙性能指标

测试防火墙得到使用千兆网卡，在流量大于 200Mbps 时，丢包率<0.05%；使用百兆网卡，在流量大于 60Mbps 时，丢包率<0.01%(在 P4 Xeon 2 GHz x 2，2GB DDR mem, GEnic 配置下)。百兆网卡 60%负载丢包率表见表 2。千兆网卡 20%负载丢包率见表 3。

表 2 测试数据 1

Frame size	Rate Tested(%)	(01,07,01)to (01,09,01)(%) 100～1000MB	Average
64	30.00	0.000	0.000
64	60.00	0.145	0.145
128	30.00	0.000	0.000
128	60.00	0.003	0.003
256	30.00	0.000	0.000
256	60.00	0.000	0.000

表 3 测试数据 2

Frame size	Rate Tested(%)	(01,07,01)to (01,09,01)(%)	Average
64	10.00	0.000	0.000
64	20.00	1.386	1.386
128	10.00	0.000	0.000
128	20.00	0.012	0.012
128	30.00	1.816	1.816
256	20.00	0.000	0.000
256	40.00	0.000	0.000
256	60.00	2.213	2.213

6 防火墙的进一步实现

我们的防火墙已经完成了初步的实现，即第一版的开发，在今后的防火墙实现中，重点需要考虑 IPv6 不同于 IPv4 的特点，以适应新的要求和提高防火墙的处理能力。

IPsec 是 IPv6 支持的功能。如果使用 IPsec 传输模式进行端到端的加密，则防火墙无法对分组所采用的传输层协议、TCP/IP 的端口号进行过滤，因为其接收的是加密的数据包，这些信息无法获得，降低了防火墙的性能。因此，如何在加密的环境下过滤数据包，将是需要解决的问题的重点。研究如何将 IPsec 与防火墙结合是下一步要完成的工作。

参考文献

1 Jacques J, Gundol B, Jacques F. Firewalls and IPv6[R]. AFNIC, 2002-10-30.

2 Ellermann U. IPv6 and Firewalls[A]. Proc. of 14th International Congress on Computer and Communications Security Protection, 1996-06.

3 Dobrucki M. The Effects of the Transition to IPv6 on Internet Security[R]. Nixu Ltd., 1999-12.

4 Gamage C. Encyrpted Message Authentication by Firewalls[A]. Proc. of PKC' 99, LNCS, Springer-Verlag, 1999, 1560: 69-81.

5 Nicolas G R. VPN and Firewall Traversal[A]. Seminar on Network Security Tik-110.501 2000, 2000-11.

6 贾　贺, 张　旭. 防火墙原理与实用技术[M]. 北京: 电子工业出版社, 2002.